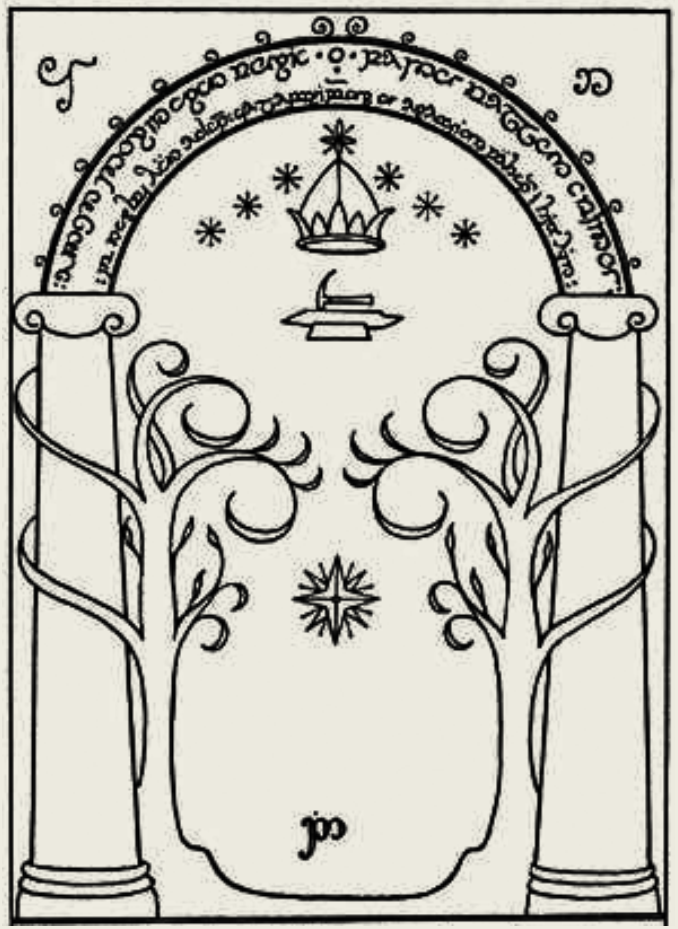
NEW SSO FEATURES IN CYPRESS

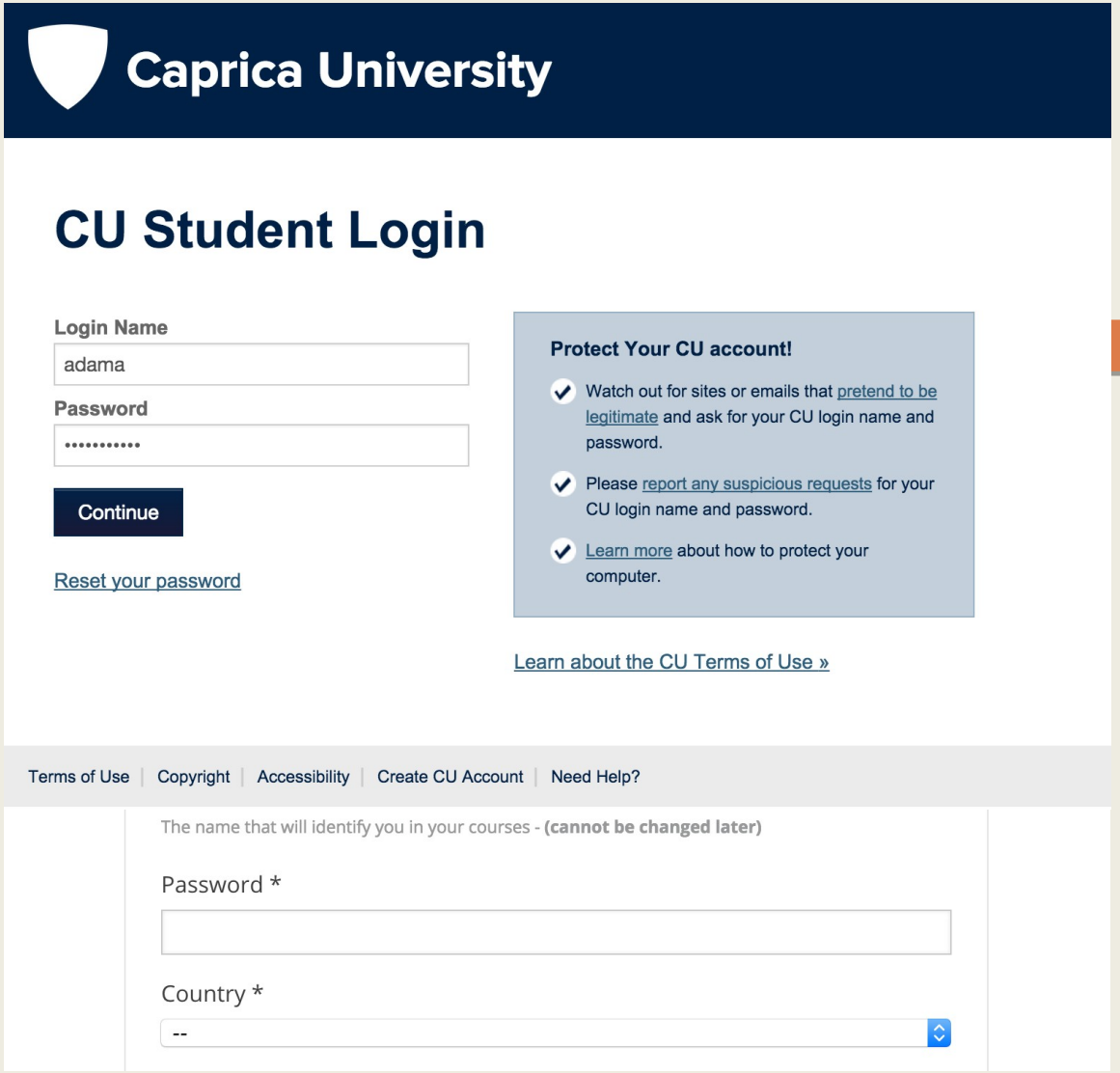
OpenCraft

HOW IT WORKS

SAML 2.0 AND SHIBBOLETH



STUDENT REGISTRATION FLOW



STUDENT REGISTRATION FLOW

RelayState=testshib&SAMLResponse=PD94bWwgdm
Vyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJwO
lJlc3BvbnNlIHhtbG5zOnNhbWwycD0idXJuOm9hc2lzOm5hb
WVzOnRjOlNBTUw6Mi4wOnByb3RvY29sIiBEZXN0aW5hdGl
vbj0iaHR0cDovL2V4YW1wbGUubm9uZS9hdXRoL2NvbXBs
ZXRlL3RwYS1zYW1sLyIgSUQ9Il9hMDdmZDlhMDg0ODM3M
2U1NTMyMGRjMzQyNDk0ZWY1ZCIgSW5SZXNwb25zZVRvP
SJURVNUSUQiIElzc3VlSW5zdGFudD0iMjAxNS0wNi0xNVQw
MDowNzoxNS4xODhaIiBWZXJzaW9uPSIyLjAiPjxzYW1sMjpJc
3N1ZXIgeG1sbnM6c2FtbDI9InVybjpvYXNpczpuYW1lczp0Yz
pTQU1MOjIuMDphc3NlcnRpb24iIEZvcm1hdD0idXJuOm9hc
2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtY
XQ6ZW50aXR5Ij5odHRwczovL2lkcC50ZXN0c2hpYi5vcmcv
aWRwL3NoaWJib2xldGg8L3NhbWwyOklzc3Vlcj48c2FtbDJw
OlN0YXR1cz48c2FtbDJwOlN0YXR1c0NvZGUgVmFsdWU9In
VybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpzdGF0dXM6U
3VjY2VzcyIvPjwvc2FtbDJBkMk9RdTlRdmpnNllPdFlQNlBOM2
o3ZUs3CnBVY3hRIdVdF...

STUDENT REGISTRATION FLOW

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="http://example.none/auth/complete/tpa-
saml/" ID="_a07fd9a0848373e55320dc342494ef5d" InResponseTo="TESTID" IssueInstant="2015-06-15T00:07:15.188Z"
Version="2.0">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://idp.testshib.org/idp/shibboleth</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="_dc77827bf5dc3b6f4d3693ee3156ba52"
Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" />
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <xenc:EncryptedKey Id="_978a7b6419a318d86e3314cf9b1c913f" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                    </xenc:EncryptionMethod>

<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICsDCCAhmgAwIBAg....</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
                    <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                        <xenc:CipherValue>lXA/Hb6JR1imT3c5r+kAOmhubyV/9JjMCsvDIbPDrLUGX4iaU...</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedKey>
            </ds:KeyInfo>
            <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:CipherValue>
                    TAgjvoJitsaPOHvaRPswXNhhxD2lvCKz1rsBkXnbayXe6bnpMB0x9ijE1Wj8UxbklBhA110DxaN6ZnHQyK8jb7SoUSOc...
                </xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml2:EncryptedAssertion>
</saml2p:Response>
```

<SAML2:ATTRIBUTESTATEMENT>

urn:oid:2.5.4.42:
William

urn:oid:2.5.4.4:
Adama

urn:oid:2.5.4.3:
William Adama

urn:oid:0.9.2342.19200300.100.1.3:
adama@galactica.fleet.colonies.gov

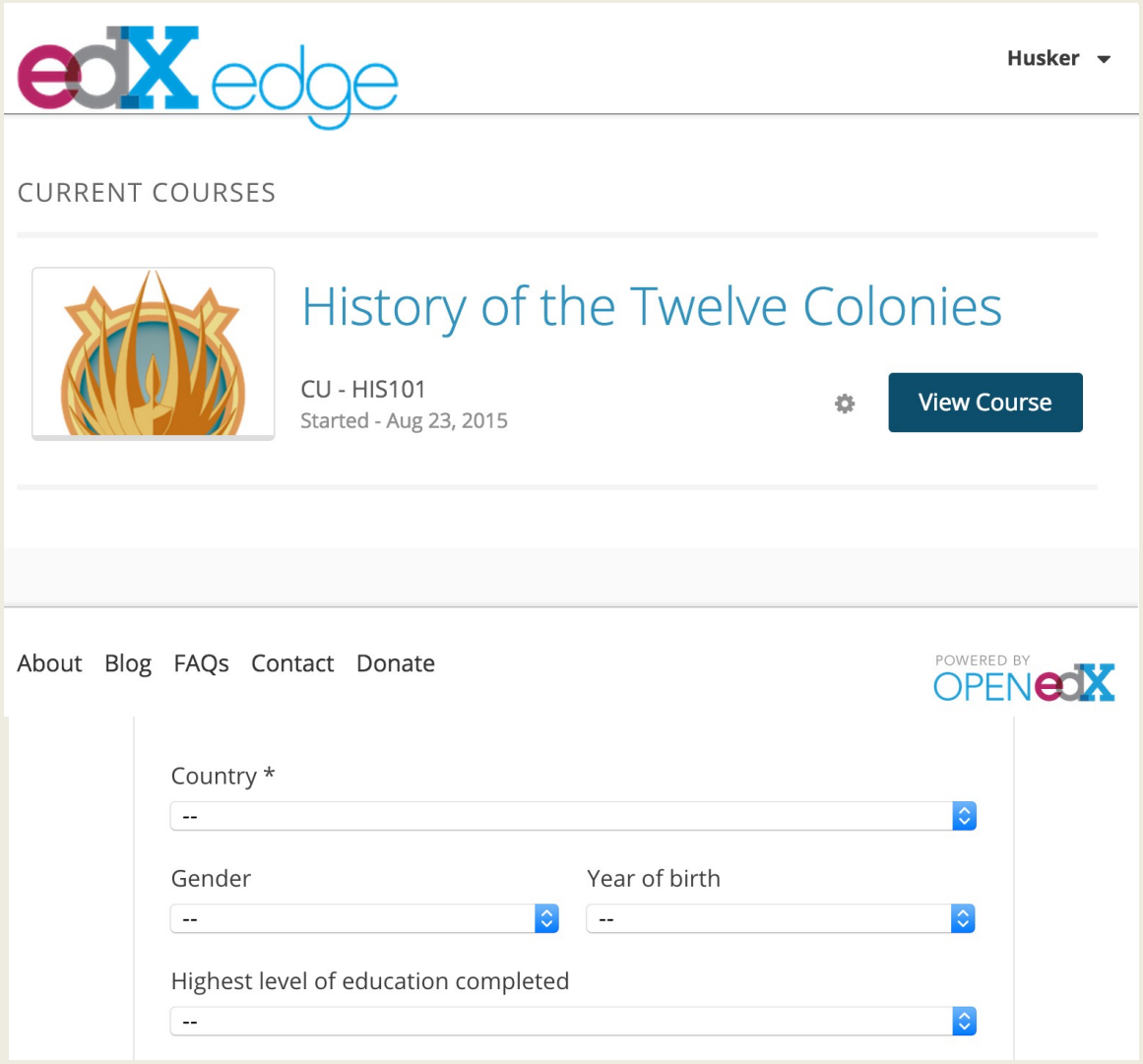
urn:oid:0.9.2342.19200300.100.1.1:
Husker

<SAML2:ATTRIBUTESTATEMENT>

urn:mace:dir:attribute-def:ubcMoocEdX:
16874621837462

urn:oid:1.3.6.1.4.1.5923.1.1.1.7:
urn:mace:ubc.ca:entl:mooc:edx:student

STUDENT REGISTRATION FLOW



STUDENT LOGIN FLOW

Part 2

HOW WE IMPLEMENTED IT

TECHNICAL GOALS

1. Add Shibboleth Provider support to third_party_auth.

2. Support many Shibboleth institutional login options

3. Allow deep links to edX Edge that indicate a preferred institutional login

4. Be able to remove the legacy Shibboleth implementation

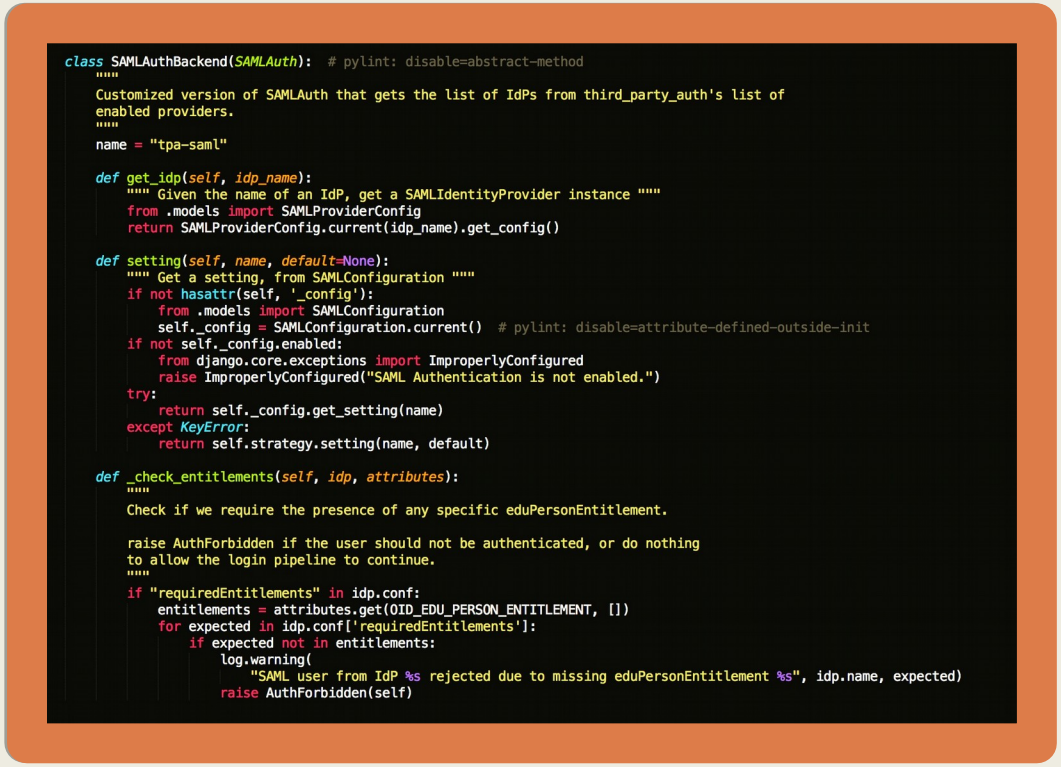
FORMING A PLAN

Discovery

Technical Spec

Discussion

Revisions



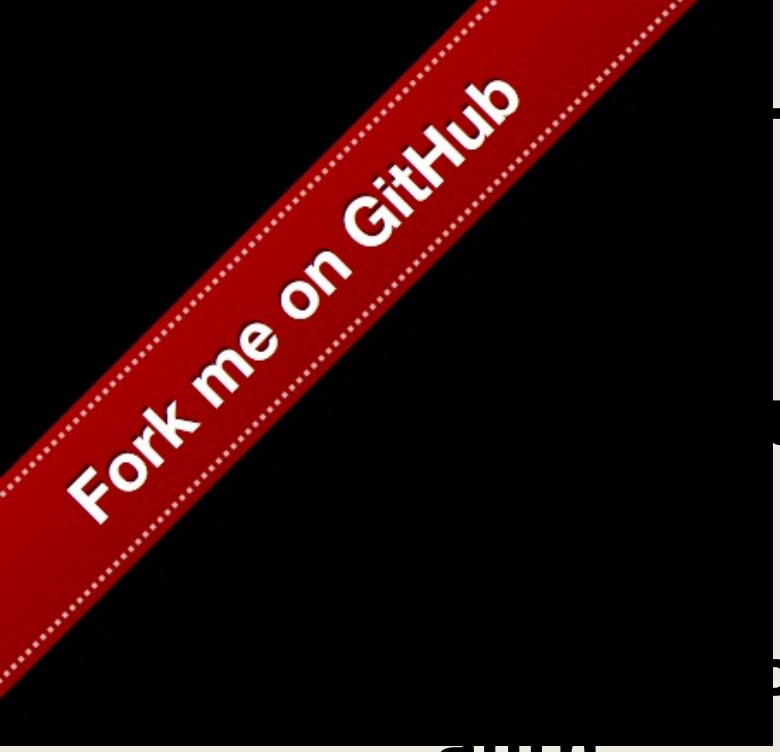
```python
class SAMLAuthBackend(SAMLAuth):  # pylint: disable=abstract-method
    """
    Customized version of SAMLAuth that gets the list of IdPs from third_party_auth's list of
    enabled providers.
    """
    name = "tpa-saml"

    def get_idp(self, idp_name):
        """ Given the name of an IdP, get a SAMLIdentityProvider instance """
        from .models import SAMLProviderConfig
        return SAMLProviderConfig.current(idp_name).get_config()

    def setting(self, name, default=None):
        """ Get a setting, from SAMLConfiguration """
        if not hasattr(self, '_config'):
            from .models import SAMLConfiguration
            self._config = SAMLConfiguration.current()  # pylint: disable=attribute-defined-outside-init
        if not self._config.enabled:
            from django.core.exceptions import ImproperlyConfigured
            raise ImproperlyConfigured("SAML Authentication is not enabled.")
        try:
            return self._config.get_setting(name)
        except KeyError:
            return self.strategy.setting(name, default)

    def _check_entitlements(self, idp, attributes):
        """
        Check if we require the presence of any specific eduPersonEntitlement.

        raise AuthForbidden if the user should not be authenticated, or do nothing
        to allow the login pipeline to continue.
        """
        if "requiredEntitlements" in idp.conf:
            entitlements = attributes.get(OID_EDU_PERSON_ENTITLEMENT, [])
            for expected in idp.conf['requiredEntitlements']:
                if expected not in entitlements:
                    log.warning(
                        "SAML user from IdP %s rejected due to missing eduPersonEntitlement %s", idp.name, expected)
                    raise AuthForbidden(self)
```



TORY 1: OPEN SOURCE COLLABORATION

ty_au Google / John Cox

ocial-auth Matías Aguirre

"Social auth made simple"

python-saml OneLogin / Sixto Martin

"Forget those complicated libraries and use the open source library provided and supported by OneLogin Inc."

TestShib Internet2

"All SAML 2.0 implementations are welcome and may be tested against Shibboleth here."

STORY 2: CRI-9 - BUG OR FEATURE?

“There has been a lot of student confusion and frustration over the social auth sign in and the new sign in page. Over the last 48 hours we have received over 70 questions from student asking what the dashboard is and how to link it to Google/Facebook.”

STORY 3: TESTING WITH UNIVERSITY PARTNERS

- University of British Columbia
- UC Berkeley
- Georgetown University

STORY 4: MISTAKES I MADE

- Scheduling reviews
- Celery Beat
- Storing secrets in the DB
- Twitter backend
- CRI-9 email validation

HOW TO SET IT UP

bit.ly/cypress-sso-setup

(+ edx-code)

PART 3: **QUESTIONS**

Consider asking…

- How did these changes affect the existing third_party_auth providers (Google/Facebook/LinkedIn)?
- How can my school be added to edge.edx.org / edx.org ?
- Can I put my school’s login button where the Google/Facebook buttons are, instead of the “institution” list?
- What is the “Dummy Provider” ?
- What sort of community contributions could improve this feature?
- Have any more features been added recently?
- Are there any advanced features not mentioned in the docs?