OIDC and OAuth2 at LBNL v2

Greg Haverkamp

Where we were

- Homegrown OP/AS based on PyOIDC (productionalized example OP)
- Proprietary introspection API
- Proprietary revocation API
- Used only for IdM apps with grander plans
- Didn't trust it enough to push toward other users; too many modifications of underlying library to keep up-to-date

IdM Applications

- Account Admin API (aa)
- Account Manager (IdM/Help Desk/Cybersecurity)
- Password Change (Everyone)
- Password Reset (Not enough people)
- Account Activation (All new/returning/reactivated users)
- Activation Password Generator (HR)

Broader goals for OIDC and OAuth2

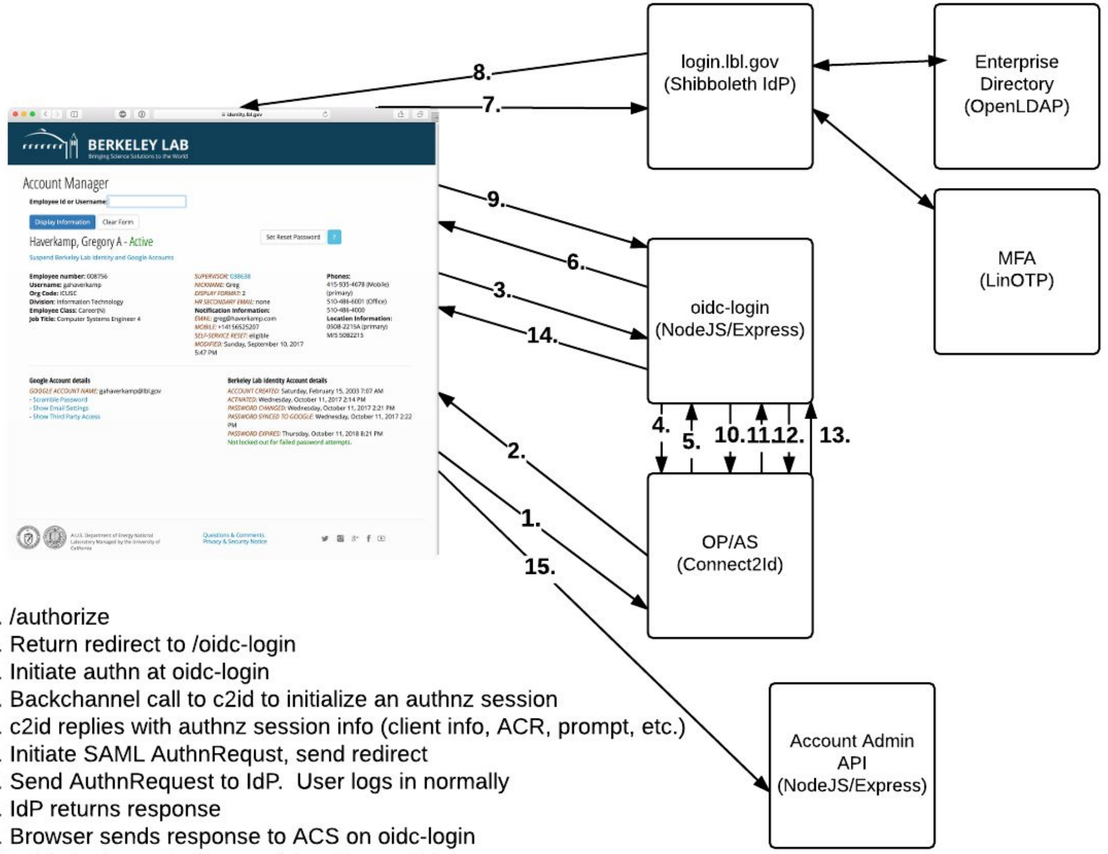
- OIDC as "easier" SSO protocol/future-hedging
- Integrate with Shibboleth IdP (don't want to duplicate efforts, esp w/MFA)
- Avoid excessive integration requirements
- Easy to integrate new protocol additions to the stack

General goals for upgrade

- OIDC Certified solution
- Expand/clean up/broaden access to Identity APIs
- Provide exemplar for others at the lab developing APIs
- Support mobile applications
- Integrate with our investments in Shibboleth MFA
- Support Account Activation Codes and Password Reset Codes (non-Shib)

How we arrived at Connect2Id

- Second choice
- Certified, and updated for new additions to OIDC and OAuth2 monthly (developed by the Nimbus developers)
- Externalized authentication and consent - easy to support all three of our required authentication methods (SAML, Activation Code, Reset Code)
- Variable token lifetime per issuance
- Pluggable UserInfo
- Pluggable JWT handling


login.lbl.gov (Shibboleth IdP)
Enterprise Directory (OpenLDAP)
MFA (LinOTP)
oidc-login (NodeJS/Express)
OP/AS (Connect2Id)
Account Admin API (NodeJS/Express)
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
identity.lbl.gov
BERKELEY LAB
Bringing Science Solutions to the World
Display Information
Clear Form
Set Reset Password
?
Questions & Comments
Privacy & Security Notice

Account Manager

Employee Id or Username:

Haverkamp, Gregory A - Active

Suspend Berkeley Lab Identity and Google Accounts

Employee number: 008756
Username: gahaverkamp
Org Code: ICUSC
Division: Information Technology
Employee Class: Career(N)
Job Title: Computer Systems Engineer 4

SUPERVISOR: 038638
NICKNAME: Greg
DISPLAY FORMAT: 2
HR SECONDARY EMAIL: none
Notification Information:
EMAIL: greg@haverkamp.com
MOBILE: +14156525207
SELF-SERVICE RESET: eligible
MODIFIED: Sunday, September 10, 2017 5:47 PM

Phones:
415-935-4678 (Mobile) (primary)
510-486-6001 (Office)
510-486-4000
Location Information:
050B-2215A (primary)
M/S 50B2215

Google Account details
GOOGLE ACCOUNT NAME: gahaverkamp@lbl.gov
- Scramble Password
- Show Email Settings
- Show Third Party Access

Berkeley Lab Identity Account details
ACCOUNT CREATED: Saturday, February 15, 2003 7:07 AM
ACTIVATED: Wednesday, October 11, 2017 2:14 PM
PASSWORD CHANGED: Wednesday, October 11, 2017 2:21 PM
PASSWORD SYNCED TO GOOGLE: Wednesday, October 11, 2017 2:22 PM
PASSWORD EXPIRES: Thursday, October 11, 2018 8:21 PM
Not locked out for failed password attempts.

A U.S. Department of Energy National Laboratory Managed by the University of California

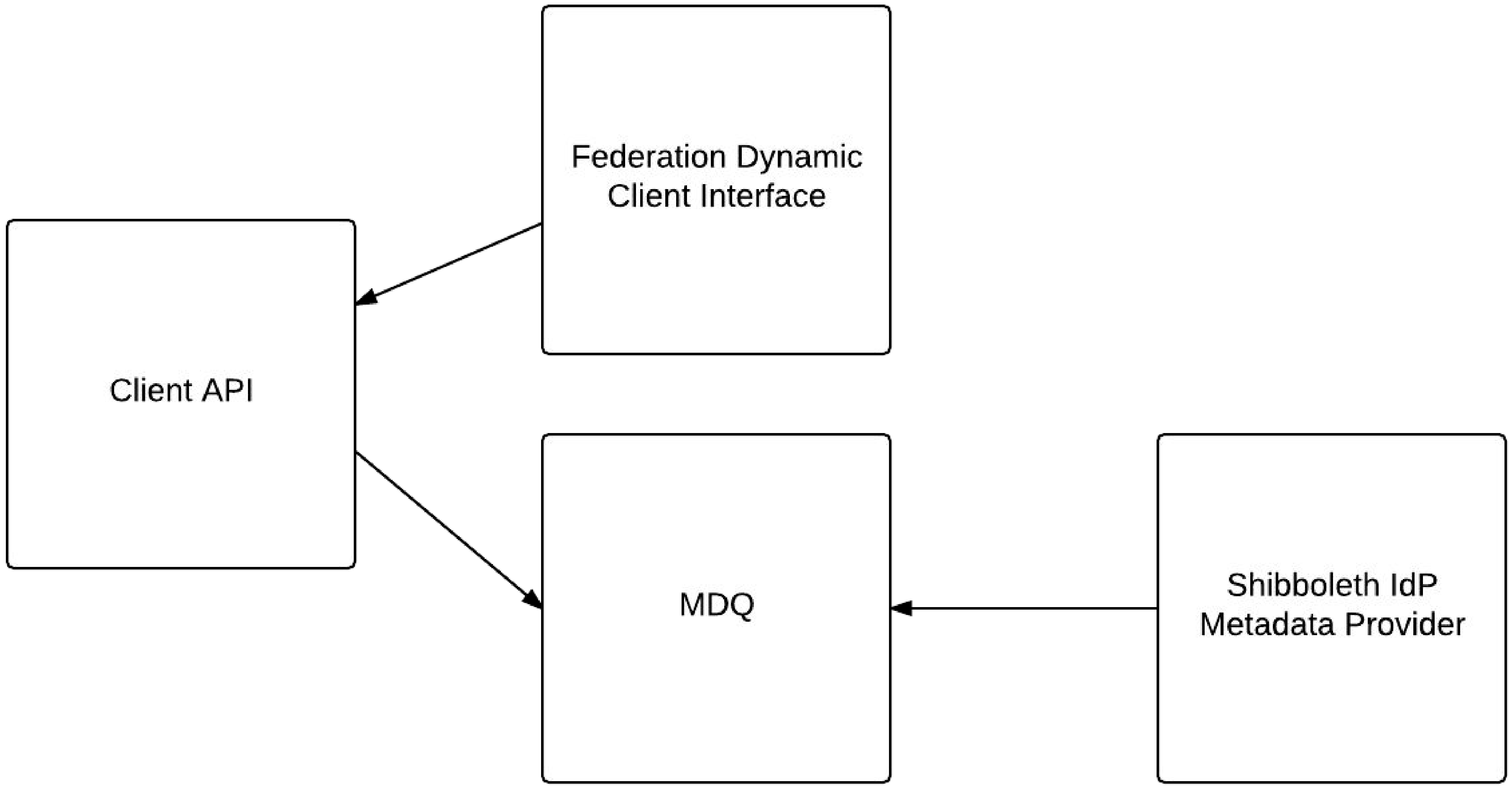
1. /authorize
2. Return redirect to /oidc-login
3. Initiate authn at oidc-login
4. Backchannel call to c2id to initialize an authnz session
5. c2id replies with authnz session info (client info, ACR, prompt, etc.)
6. Initiate SAML AuthnRequst, send redirect
7. Send AuthnRequest to IdP. User logs in normally
8. IdP returns response
9. Browser sends response to ACS on oidc-login
10. oidc-login sends successful authn to c2id
11. If c2id accepts, replies with consent info
12. Send consent (currently no consent ui)
13. c2id returns redirect_uri to oidc_login
14. oidc_login sends 302 to redirect_uri, along with access_token and id_token .
15. application beings consuming API

What haven't we gotten to?

- JWT authorization grants (service accounts)
- Client info communicated to Shib IdP
- UserInfo from Shibboleth (rather than LDAP)
- Client management for enterprise use

Questions?

gahaverkamp@lbl.gov


Federation Dynamic Client Interface
Client API
MDQ
Shibboleth IdP Metadata Provider