moz://a

Developer Roadshow 2017

Mozilla PDX | March 7, 2017

Overview

Hi.

We’re Mozilla, the proudly non-profit champions of the Internet, helping to keep it healthy, open and accessible to all.

Tweet at Us!

#mozilla

#DevRoadshow

TAKE 3 MIN to Tell Us What you think!

And be entered to win sweet swag.

mzl.la/devsurvey

Code of Conduct

A primary goal of Mozilla's Developer Roadshow (Roadshow) is to be inclusive to the largest number of participants, with the most varied and diverse backgrounds possible. As such, we are committed to providing a friendly, safe and welcoming environment for all, regardless of gender, sexual orientation, ability, age, ethnicity, socioeconomic status, and religion (or lack thereof).

This Code of Conduct outlines our expectations for all those who participate in our conference community, as well as the consequences for unacceptable behavior.
We invite all those who participate in the Roadshow to help us create safe and positive experiences for everyone.

Please find the full text here: https://mzl.la/devroadshowcoc

And contact Sandra Persing (sandra@mozilla.com; @sandrapersing) for any issues, questions, concerns.

Major Things to Look Forward to in 2017

New Web Standards

1. WebAssembly
2. WebGL 2
3. WebVR
4. CSS Grid

DevTools

1. Rewriting the DevTools into standard HTML/CSS/JS
2. Hosting the DevTools on GitHub as individual add-ons, allowing faster updates and easier outside contributions
3. CSS Grid Inspector

Performance

1. Electrolysis (e10s)
2. Multiple content processes (e10s-multi)
3. Project Quantum (announcement)

Major Things to Look Forward to in 2017

Privacy + Security

1. The Tor Uplift
2. Strong sandboxing on all platforms

Firefox Features

1. Activity Stream graduating from Test Pilot
2. More Test Pilot experiments
3. Container Tabs
4. (Maybe!) Eliminating the Aurora release channel so features can get from Nightly to Release more quickly

Web Extensions

1. Standardizing add-on APIs between Firefox, Chrome, Edge, and Opera
2. Supporting the devtools.* APIs
3. Supporting the storage.sync API
4. New Firefox-specific APIs for theming the browser
5. Finishing Chrome-compat and landing more Firefox-specific APIs

Speakers

Michael Van Kleeck:

Identity and Access

Management at Mozilla

moz://a

Identity and Access Management

Michael Van Kleeck
Mozilla Enterprise Solutions Architect

Me.

I am Michael Van Kleeck

I work on Enterprise Architecture

Twitter @michaelvkpdx

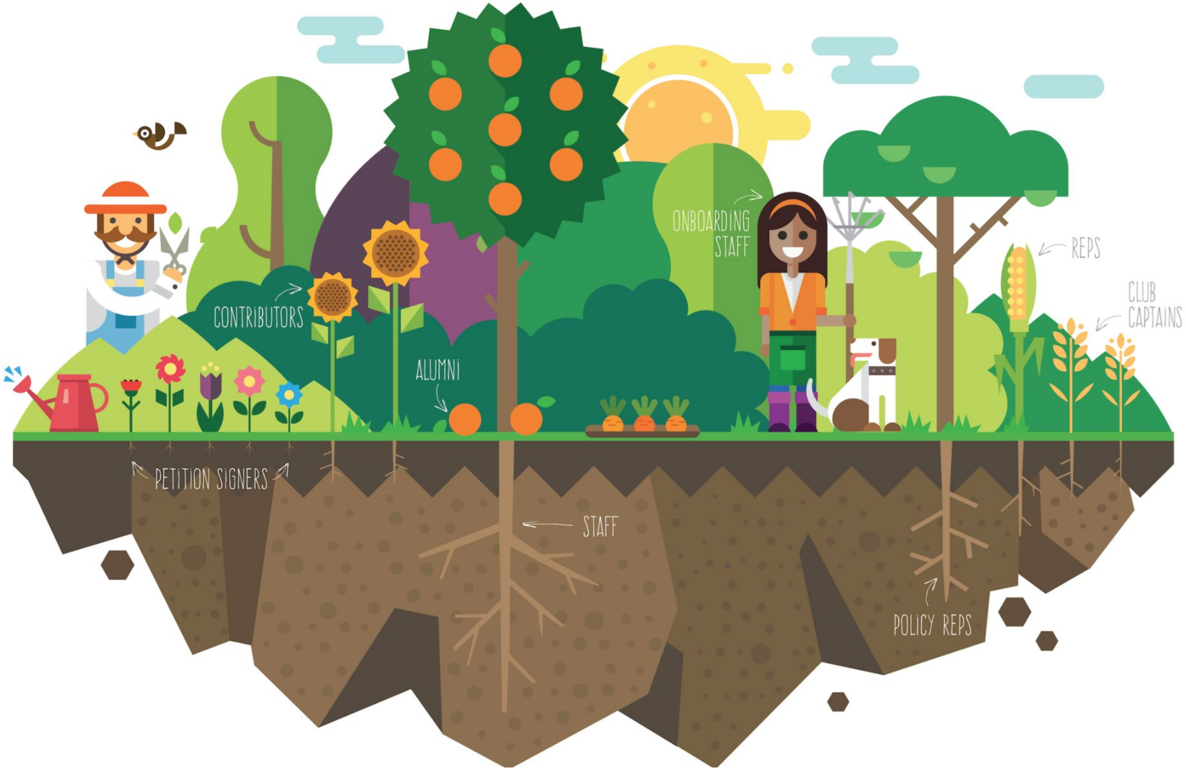
Major assistance provided by:

I am Andrew Krug

I work on Security Engineering

Twitter @andrewkrug

The Mozilla Community Garden



Identity and Access Management- Vision

> **All Mozillians (paid staff and contributors) have convenient and appropriate access to Mozilla services through a unified, authoritative, integrated identity system that empowers them to build a better Internet**

Identity and Access Management- Summary

IAM efforts improve security and productivity of Mozillians by streamlining IAM management tasks while providing visibility and auditability.

IAM provides an easier and significantly safer experience for the user and for services in need of authentication.

Identity and Access Management- Sample Use Cases

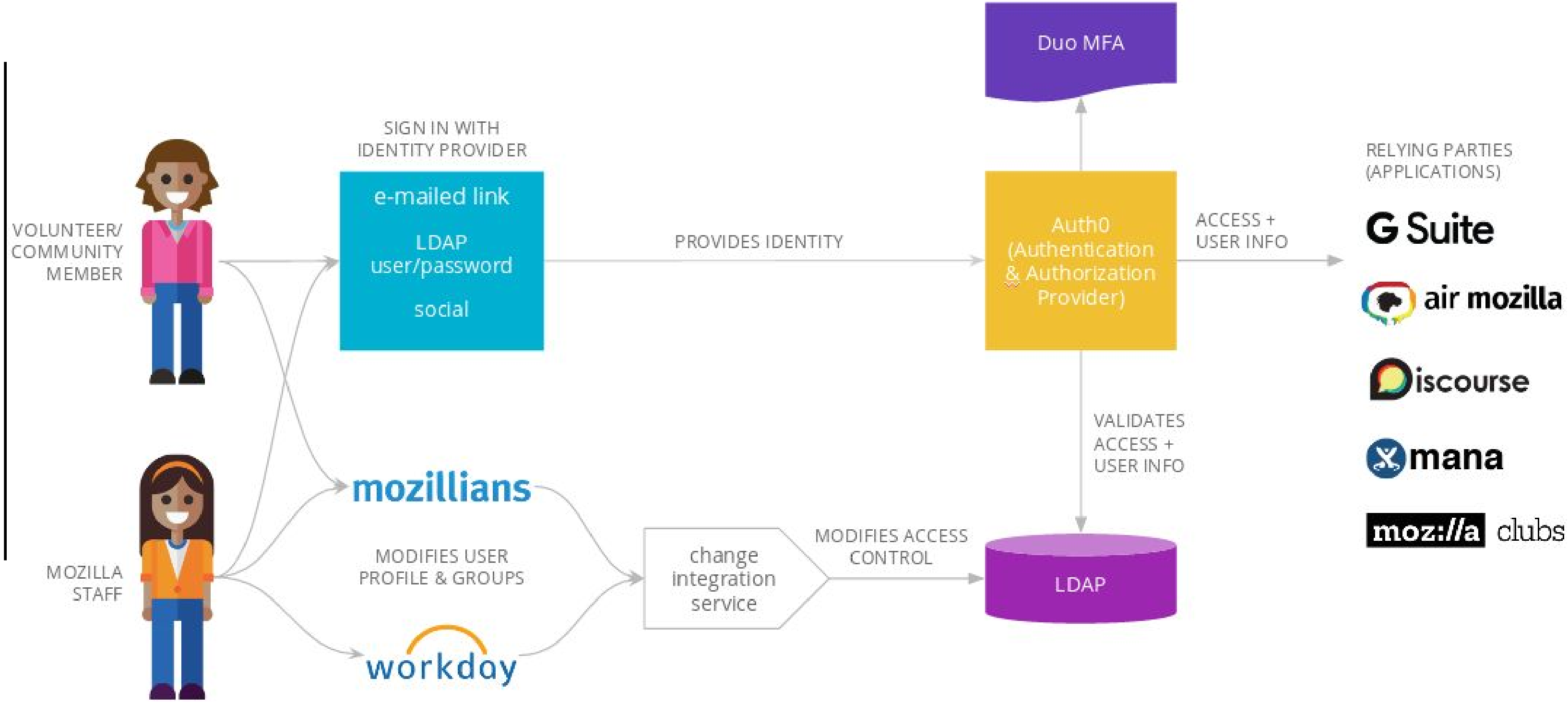
As staff or community:

- I would like to be able to collaborate easily on Mozilla Google docs.
- I would like to read documentation on Mozilla wikis and help improve it

As a developer:

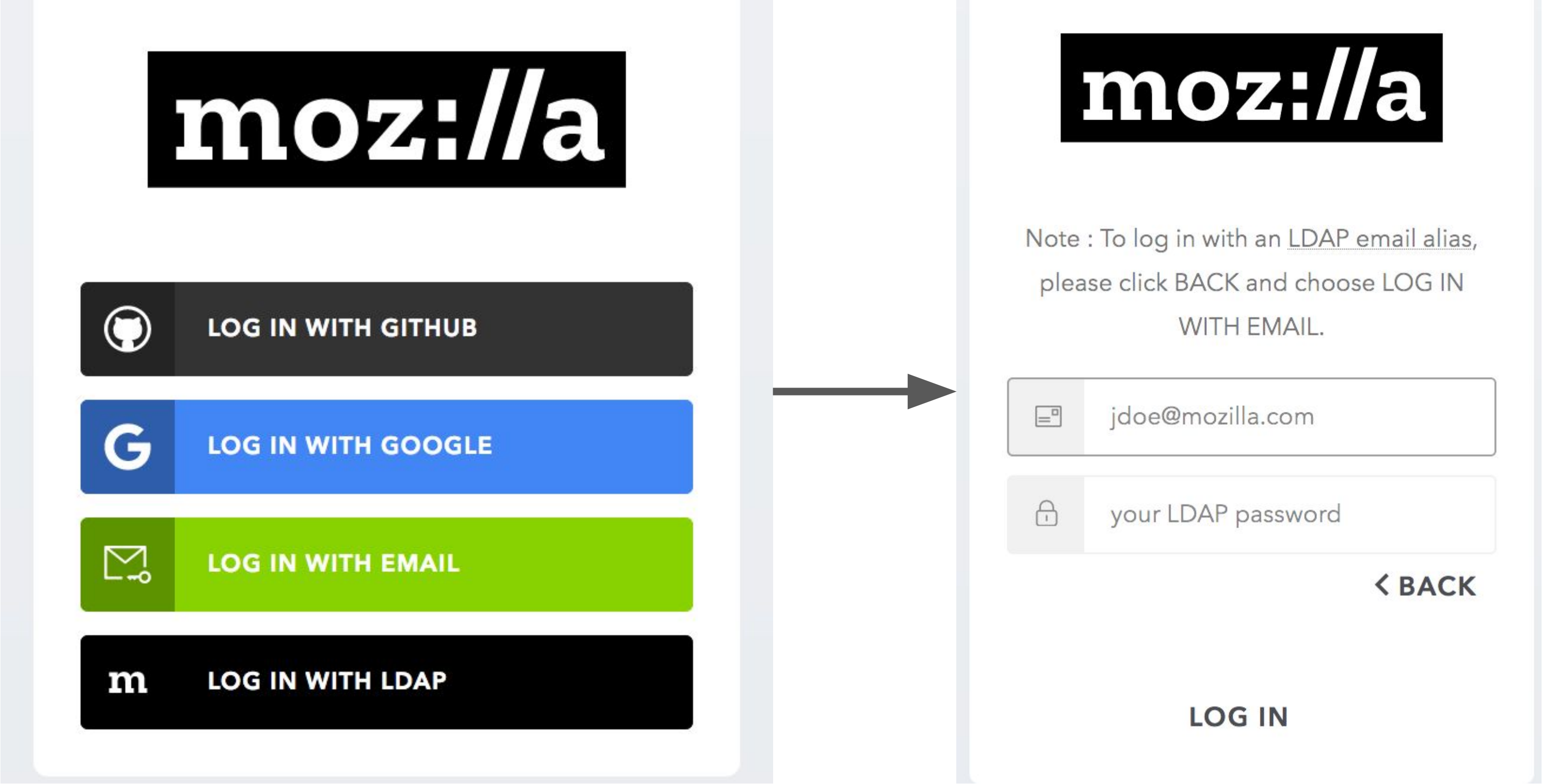
- I would like to easily enable collaboration with my web app or service.
- I would like to control who has write access to my codebase.

Identity and Access Management- High Level


Duo MFA
SIGN IN WITH IDENTITY PROVIDER
e-mailed link
LDAP user/password
social
PROVIDES IDENTITY
Auth0 (Authentication & Authorization Provider)
ACCESS + USER INFO
RELYING PARTIES (APPLICATIONS)
G Suite
air mozilla
Discourse
mana
moz://a clubs
VOLUNTEER/ COMMUNITY MEMBER
MOZILLA STAFF
mozillians
MODIFIES USER PROFILE & GROUPS
workday
change integration service
MODIFIES ACCESS CONTROL
VALIDATES ACCESS + USER INFO
LDAP

Note: High-security services have extra checks on access control modification

Identity and Access Management- Lock screen

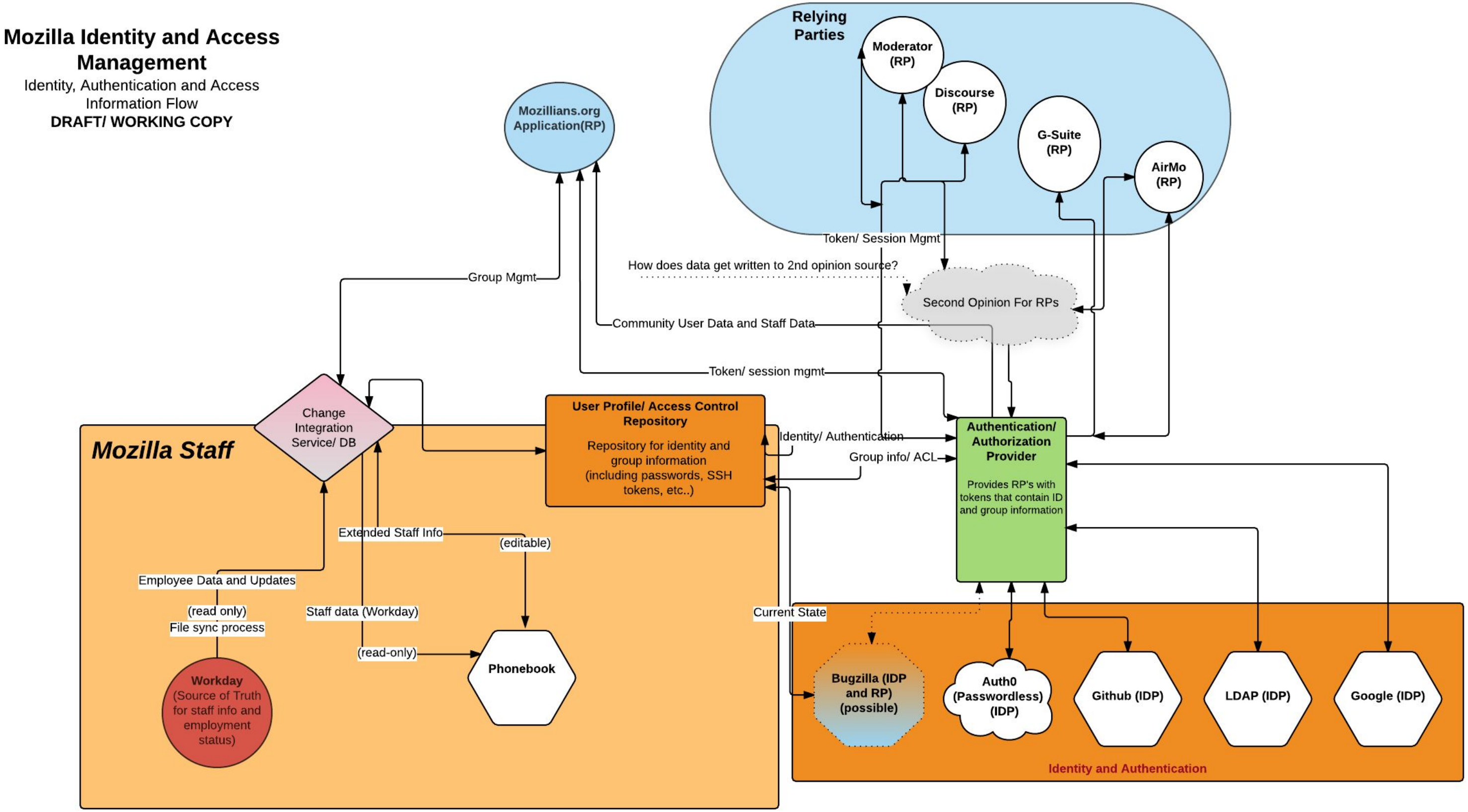


Note : To log in with an LDAP email alias, please click BACK and choose LOG IN WITH EMAIL.

jdoe@mozilla.com

your LDAP password

Identity and Access Management- Solution Architecture

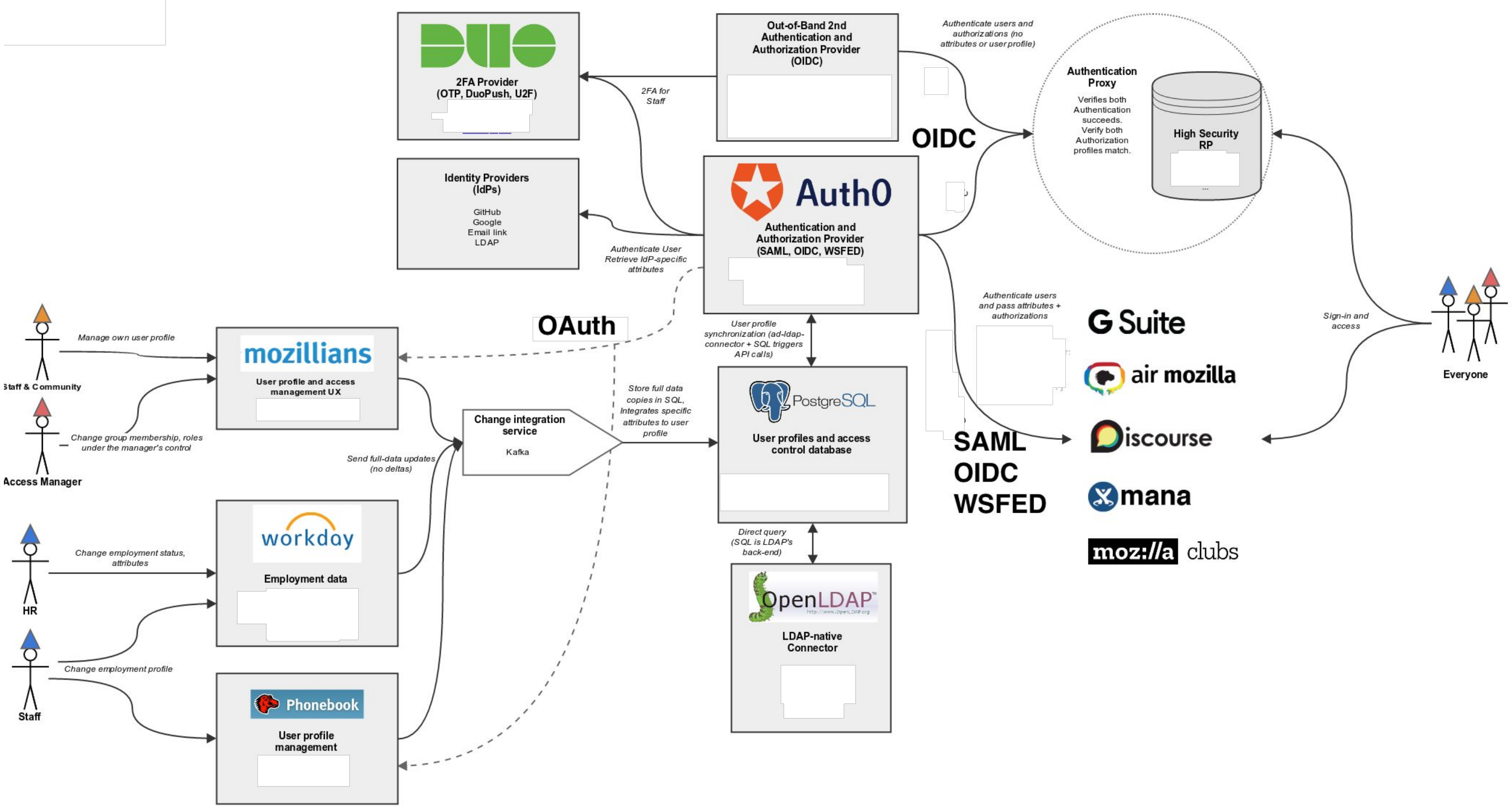


Mozilla Identity and Access Management
Identity, Authentication and Access Information Flow
DRAFT/ WORKING COPY
Relying Parties
Moderator (RP)
Discourse (RP)
G-Suite (RP)
AirMo (RP)
Mozillians.org Application(RP)
Token/ Session Mgmt
How does data get written to 2nd opinion source?
Second Opinion For RPs
Group Mgmt
Community User Data and Staff Data
Token/ session mgmt
Change Integration Service/ DB
User Profile/ Access Control Repository
Repository for identity and group information (including passwords, SSH tokens, etc..)
Identity/ Authentication
Group info/ ACL
Authentication/ Authorization Provider
Provides RP's with tokens that contain ID and group information
Mozilla Staff
Extended Staff Info
(editable)
Employee Data and Updates
(read only)
File sync process
Staff data (Workday)
(read-only)
Phonebook
Workday (Source of Truth for staff info and employment status)
Current State
Bugzilla (IDP and RP) (possible)
Auth0 (Passwordless) (IDP)
Github (IDP)
LDAP (IDP)
Google (IDP)
Identity and Authentication

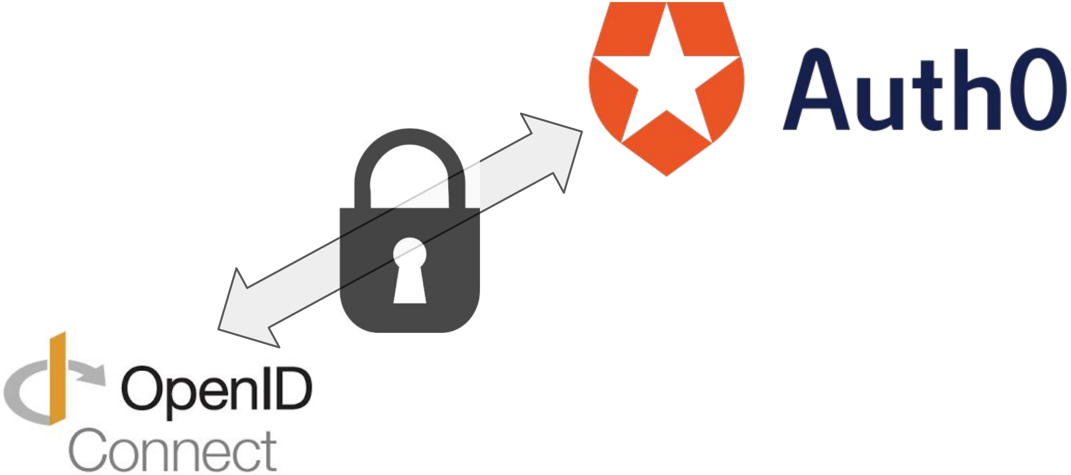
IAM Terms and Technologies

- ➔ **OAuth** Open Standard for Authentication (common!)
- ➔ **OIDC** OpenID Connect (authorization layer on OAuth)
- ➔ **SAML and WSFED** Legacy Auth technologies
- ➔ **2FA** 2-Factor Authentication (e.g., Duo, Yubikey, etc...)
- ➔ **JWT** JSON Web Tokens
- ➔ **LDAP** Lightweight Directory Access Protocol

Identity and Access Management- Tech Architecture


2FA Provider
(OTP, DuoPush, U2F)
Out-of-Band 2nd Authentication and Authorization Provider (OIDC)
2FA for Staff
Authenticate users and authorizations (no attributes or user profile)
OIDC
Authentication Proxy
Verifies both Authentication succeeds. Verify both Authorization profiles match.
High Security RP
Identity Providers (IdPs)
GitHub
Google
Email link
LDAP
Auth0
Authentication and Authorization Provider (SAML, OIDC, WSFED)
Authenticate User Retrieve IdP-specific attributes
OAuth
User profile synchronization (ad-ldap-connector + SQL triggers API calls)
Authenticate users and pass attributes + authorizations
G Suite
air mozilla
Discourse
mana
moz://a clubs
SAML
OIDC
WSFED
Sign-in and access
Everyone
Staff & Community
Manage own user profile
mozillians
User profile and access management UX
Access Manager
Change group membership, roles under the manager's control
Change integration service
Kafka
Send full-data updates (no deltas)
Store full data copies in SQL, Integrates specific attributes to user profile
PostgreSQL
User profiles and access control database
Direct query (SQL is LDAP's back-end)
OpenLDAP
LDAP-native Connector
HR
Change employment status, attributes
workday
Employment data
Staff
Change employment profile
Phonebook
User profile management

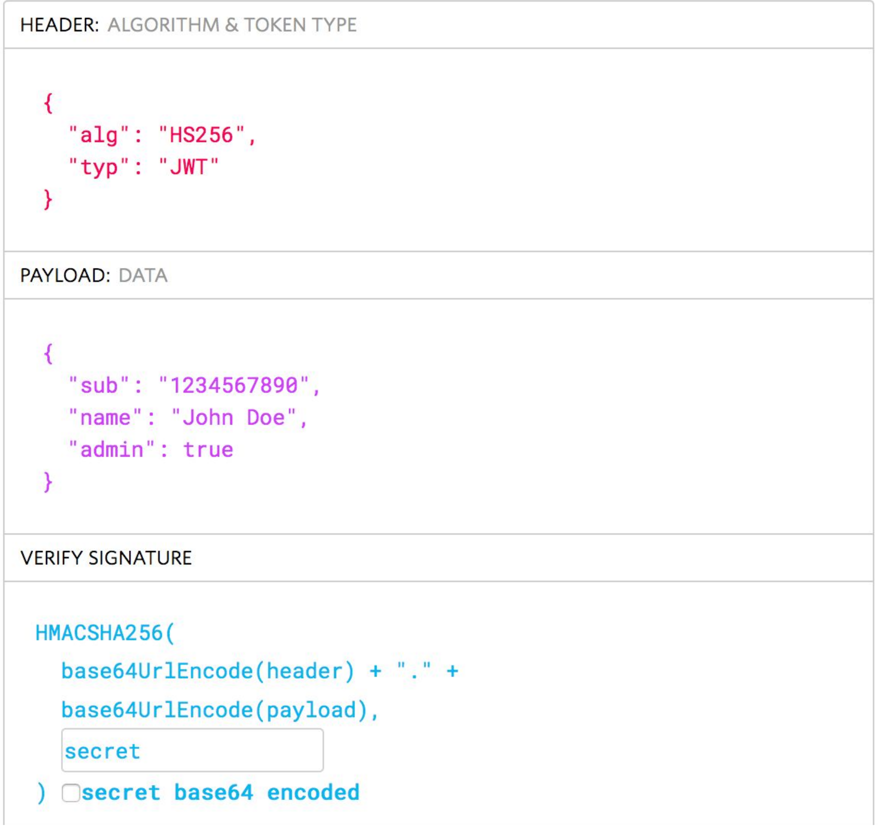
Programming Challenge



- ➔ Applications or relying parties need to talk with identity providers securely.
- ➔ Each authentication has unique messages associated.
- ➔ Those message need to be secure in transit.

JSON Web Token

Decoded



HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

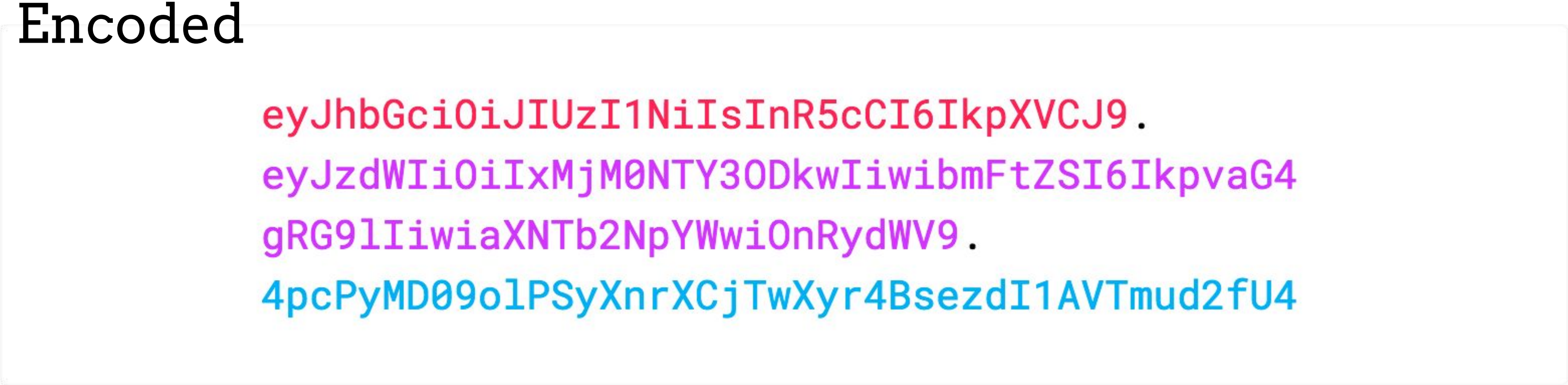
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) ☐secret base64 encoded
```

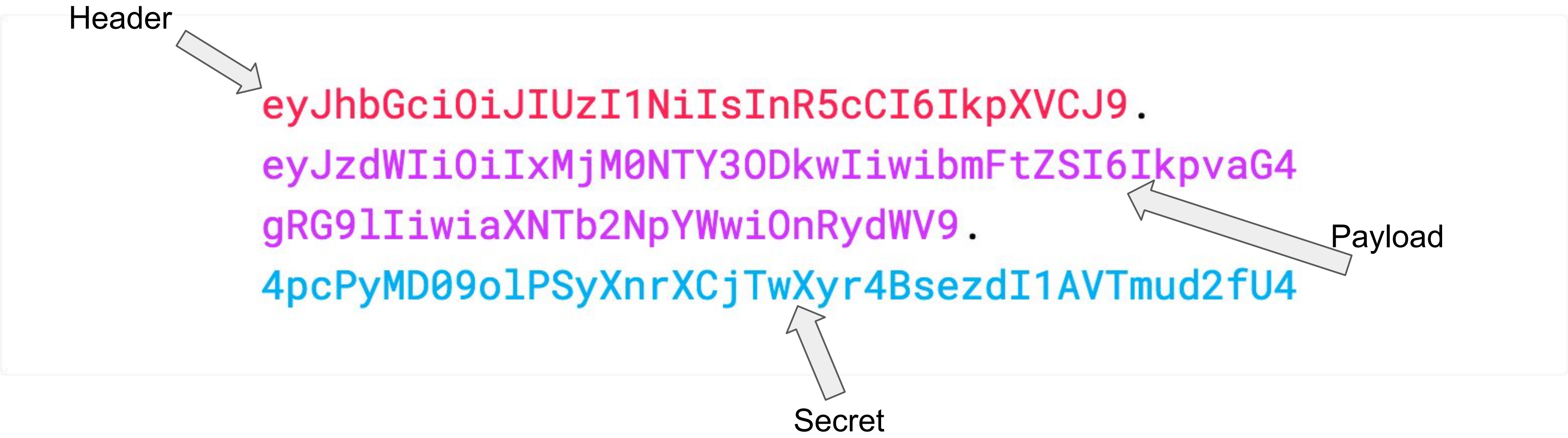
JSON Web Token

Encoded



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

What’s a digital signature?



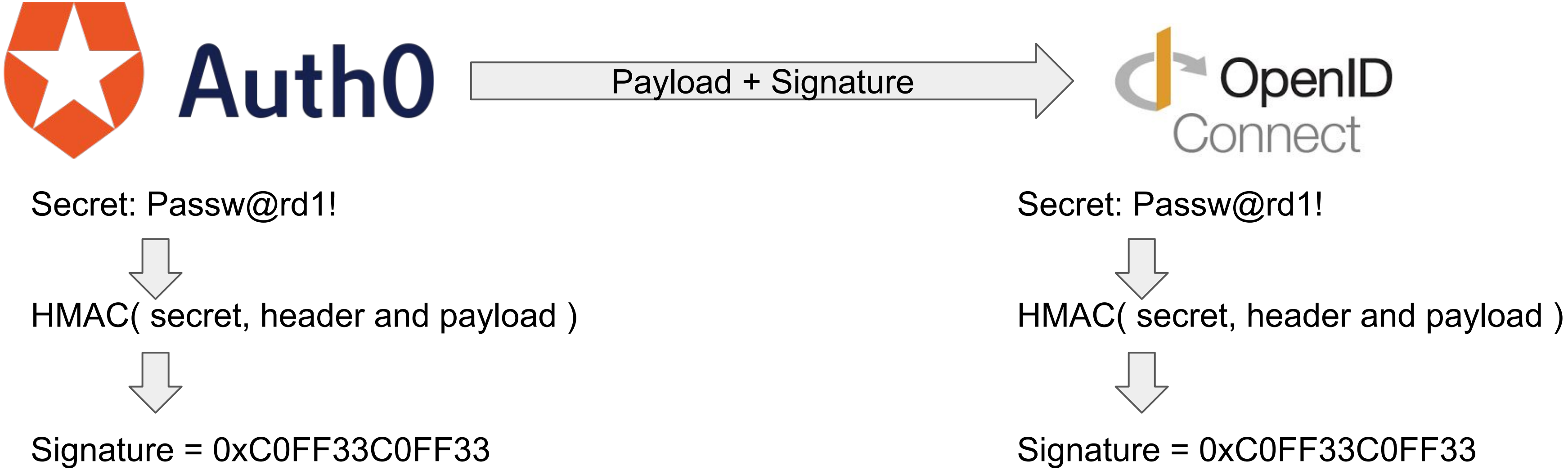
```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

Header

Payload

Secret

Digital Signatures Continued



Payload + Signature

Secret: Passw@rd1!

HMAC(secret, header and payload)

Signature = 0xC0FF33C0FF33

Secret: Passw@rd1!

HMAC(secret, header and payload)

Signature = 0xC0FF33C0FF33

If you did catch all that…

Summary :

Secure because math...

What would that look like in code?

```
#This is the payload we receive in python

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ik1pY2hhZWwgVmFuIEtsZWVrIiwiYWRtaW4iOnRydWV9.puDI94cptsSD3STETIqT4MO84nA54P2VtT_iH-mcu7I
```

First we have to split it apart…

```
#!/usr/bin/python

payload =
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ik1pY2hhZWwgVmFuIEtsZWVrIiwiYWRtaW4iOnRydWV9.puDI94cptsSD3STETIqT4MO84nA54P2VtT_iH-mcu7I

header = payload.split(‘.’)[0]

payload = payload.split(‘.’)[1]

signature = payload.split(‘.)[2]
```

Now we need to sign it…

```
#!/usr/bin/python
import hmac
import hashlib

payload = ( redacted for brevity )
secret = ByRzU2haBzT0dLwt7QZgzut4LqSPc5JW

header = payload.split(‘.’)[0]
payload = payload.split(‘.’)[1]
signature = payload.split(‘.)[2]

message = header + payload
digest_maker = hmac.new(secret, ‘ ’,hashlib.sha256)

this_signature = digest_maker.update(message).hexdigest()
```

Checking Signatures

```
#!/usr/bin/python
import hmac
import hashlib
 ** redacted for brevity **
message = header + payload
digest_maker = hmac.new(secret, ‘ ’,hashlib.sha256)

this_signature = digest_maker.update(message).hexdigest()

if this_signature == signature:
    #do things like trust the payload
else:
    #do things like access denied
```

A Defense in Depth Strategy

- → TLS Certificates
- → Application Security
- → Custom Authorizers
- → 2FA (Duo, OTP, etc.)

Applicable Developer Skills

- ➔ Cryptography Basics
- ➔ String Operations
- ➔ Different String Encoding

More Resources

JSON Web Tokens: https://jwt.io/introduction/

OpenIDC Security Best Practices:

https://wiki.mozilla.org/Security/Guidelines/OpenID_Connect

OAuth, OIDC, SAML, WS-Fed Comparison (blog by Niraj Bhatt)

Protect the Web- Get Involved With Mozilla!

Contribute to the Mozilla Code Base!

https://developer.mozilla.org/en-US/docs/Mozilla/Developer_guide

Participate In An Outreachy Project!

https://wiki.mozilla.org/Outreachy

Come work with us!

https://careers.mozilla.org/

Thanks!

Michael Van Kleeck

Twitter @michaelvkpdx

E-mail mvk@mozilla.com

Website mvk.net/officehours

moz://a

#mozilla

#DevRoadshow

on Periscope @mozilla

Q&A