RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

BORDERLESS IDENTITY

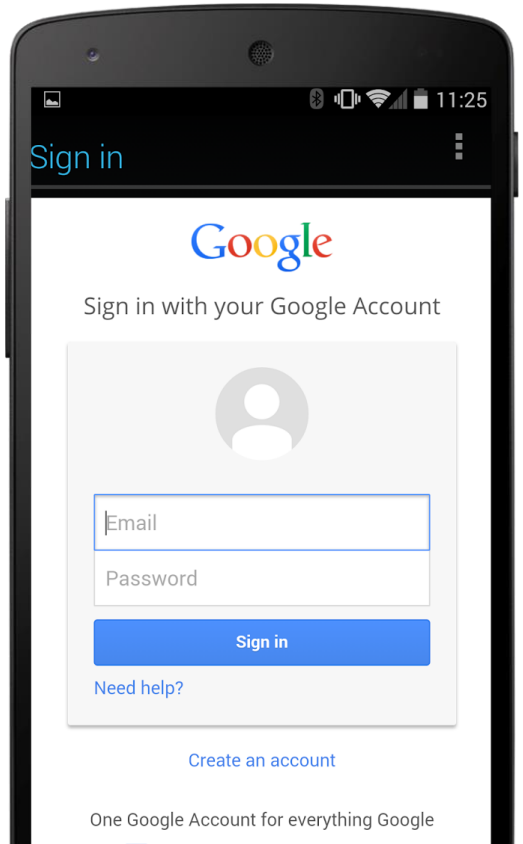
The Cutting Edge: Standards at work in Google's mobile focused future

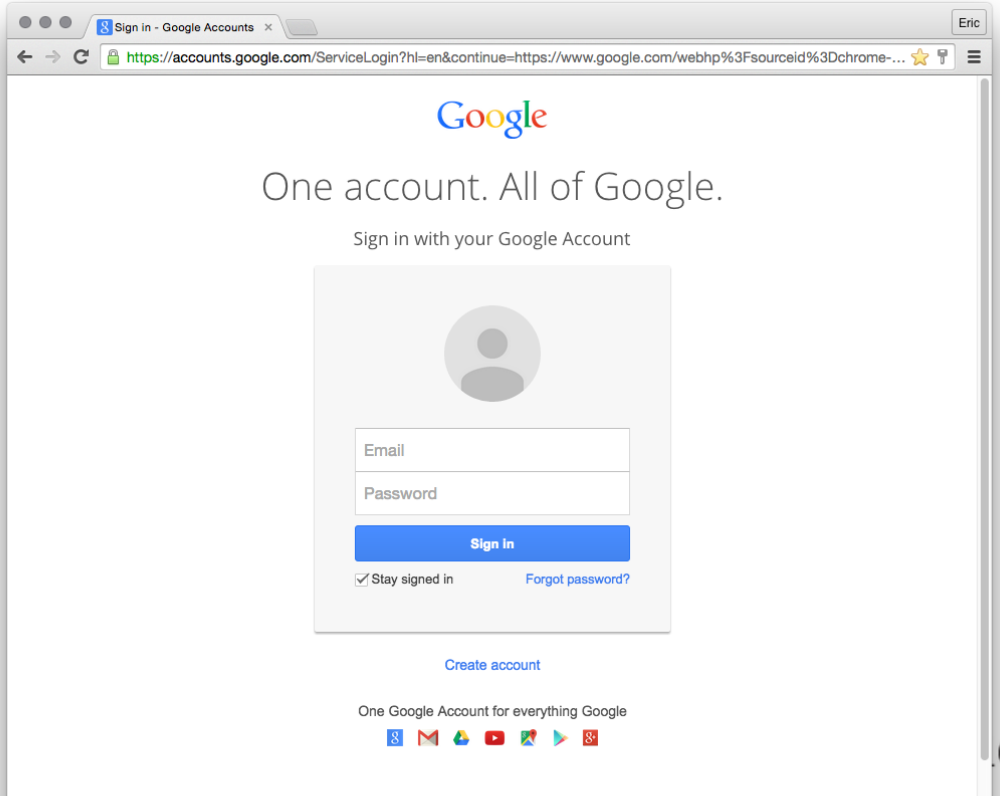
Eric Sachs

Director of Product Management
Identity, Google

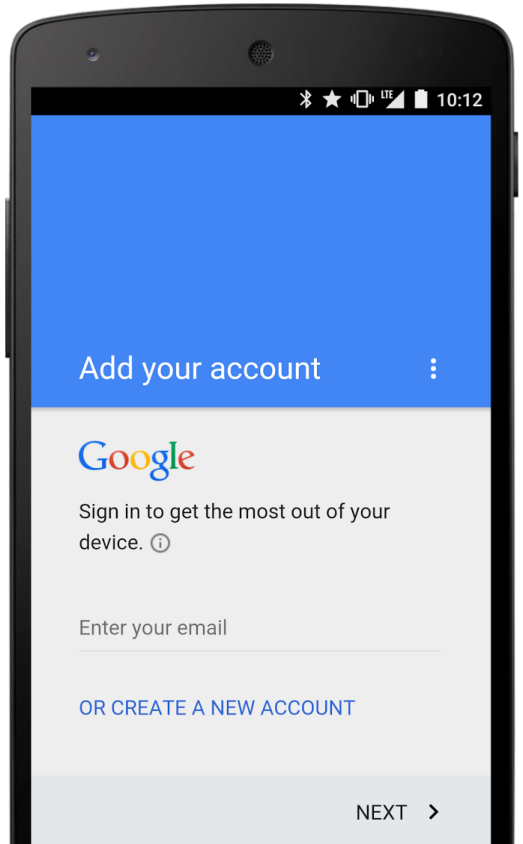
Pam Dingle

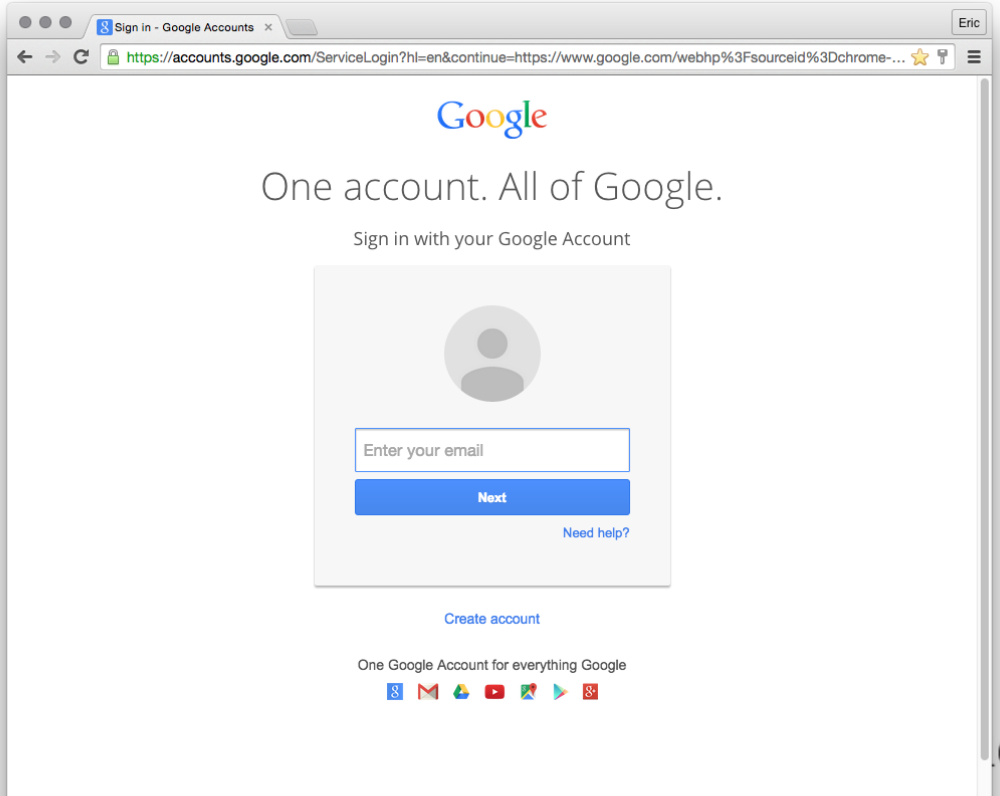
Senior Technical Architect
Office of the CTO, Ping Identity

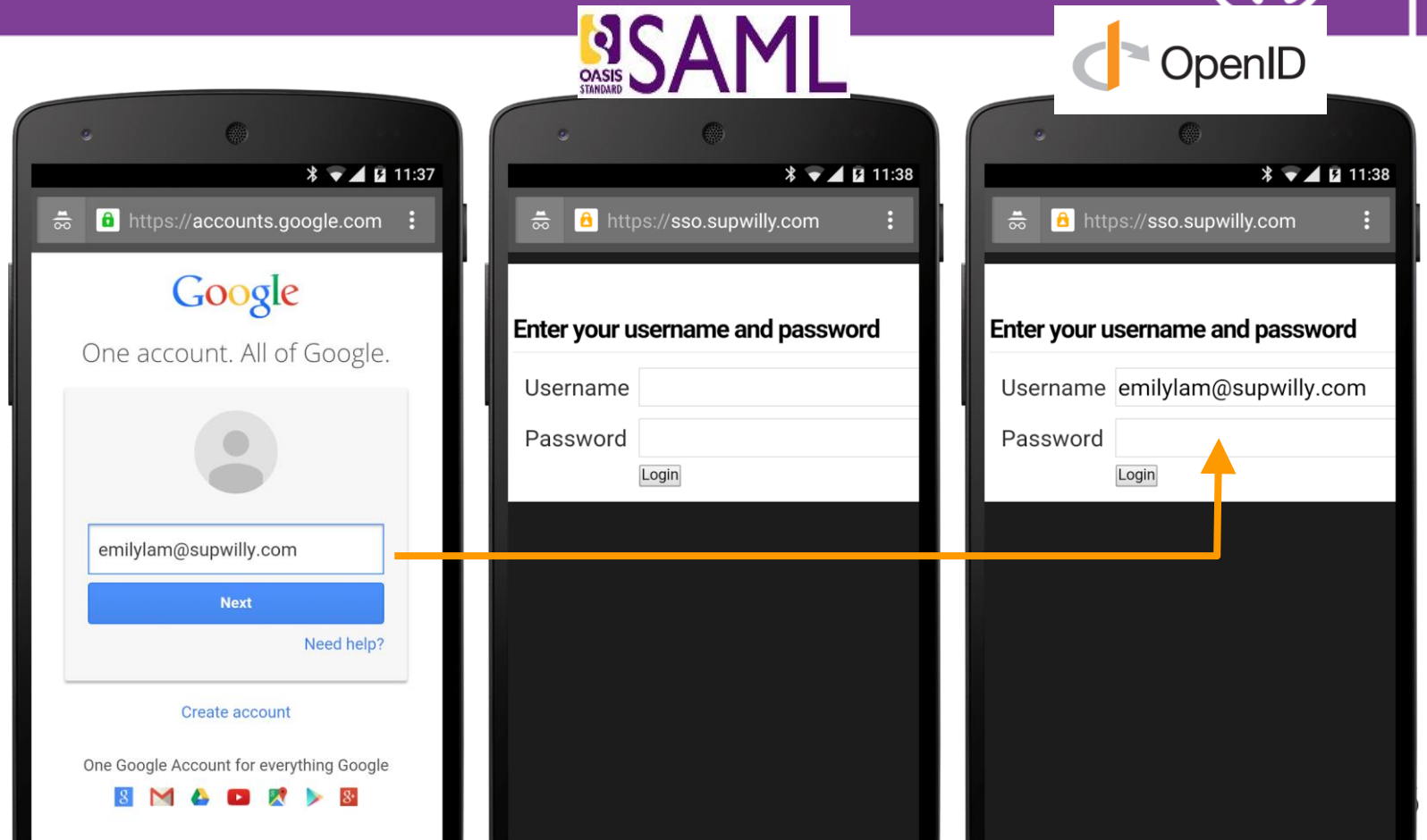

11:25
Sign in
Google
Sign in with your Google Account
Email
Password
Sign in
Need help?
Create an account
One Google Account for everything Google


Sign in - Google Accounts
Eric
https://accounts.google.com/ServiceLogin?hl=en&continue=https://www.google.com/webhp%3Fsourceid%3Dchrome-...
Google
One account. All of Google.
Sign in with your Google Account
Email
Password
Sign in
Stay signed in
Forgot password?
Create account
One Google Account for everything Google

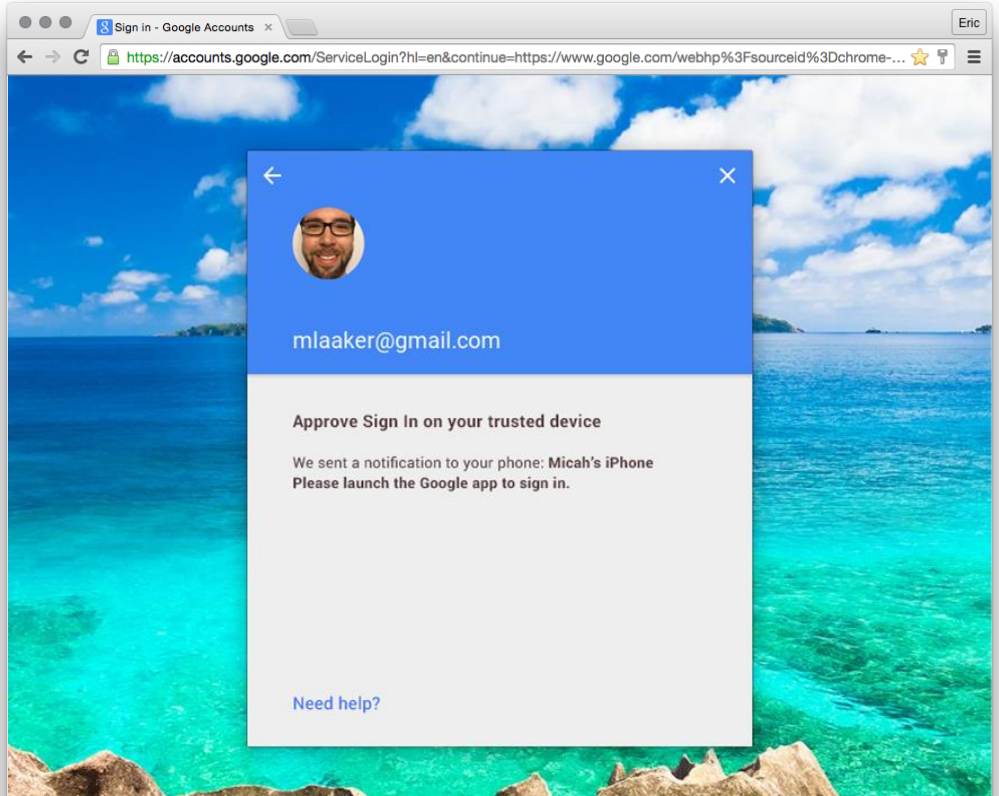
Google

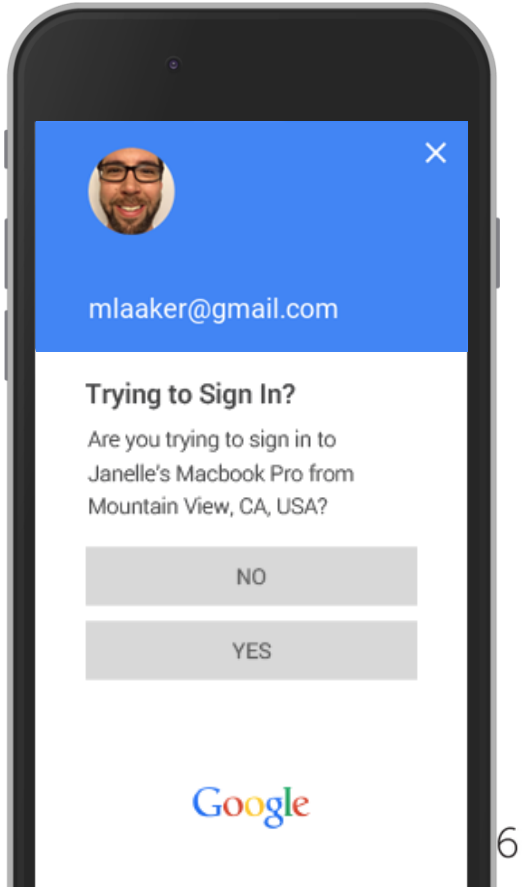

10:12
Add your account
Google
Sign in to get the most out of your device.
Enter your email
OR CREATE A NEW ACCOUNT
NEXT


Sign in - Google Accounts
Eric
https://accounts.google.com/ServiceLogin?hl=en&continue=https://www.google.com/webhp%3Fsourceid%3Dchrome-...
Google
One account. All of Google.
Sign in with your Google Account
Enter your email
Next
Need help?
Create account
One Google Account for everything Google

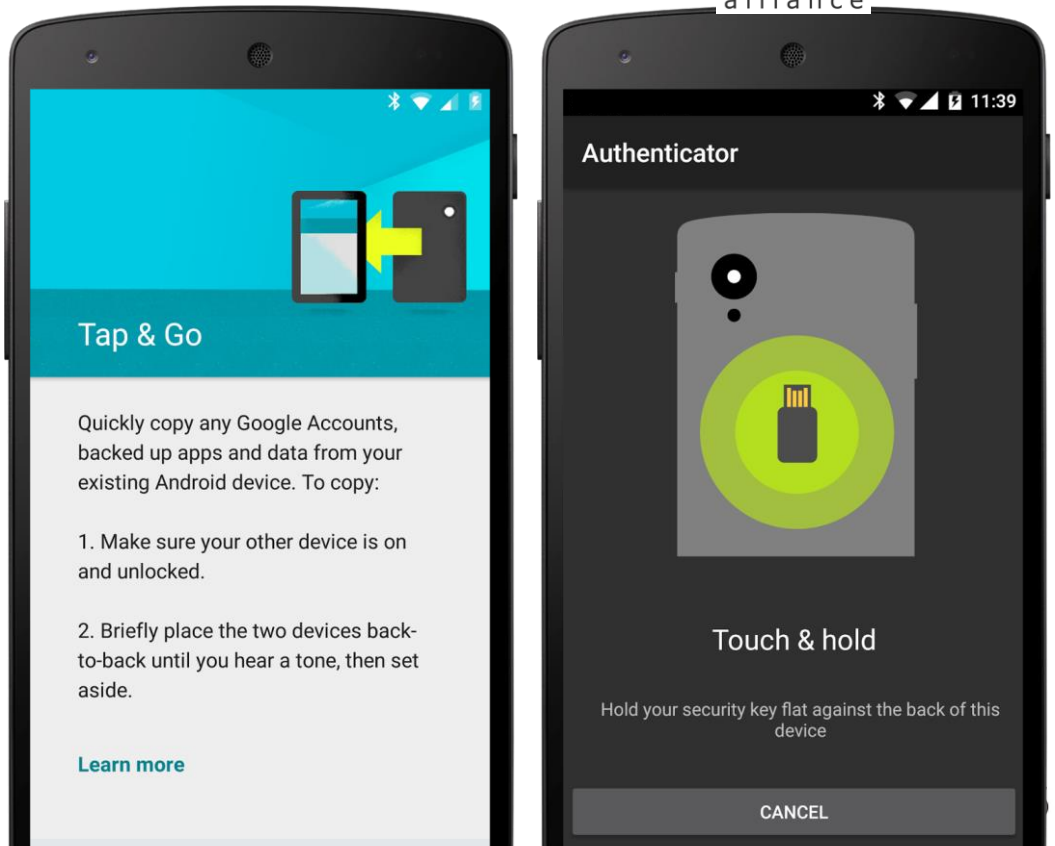

SAML
OpenID
11:37
https://accounts.google.com
Google
One account. All of Google.
emilylam@supwilly.com
Next
Need help?
Create account
One Google Account for everything Google
11:38
https://sso.supwilly.com
Enter your username and password
Username
Password
Login
11:38
https://sso.supwilly.com
Enter your username and password
Username
emilylam@supwilly.com
Password
Login

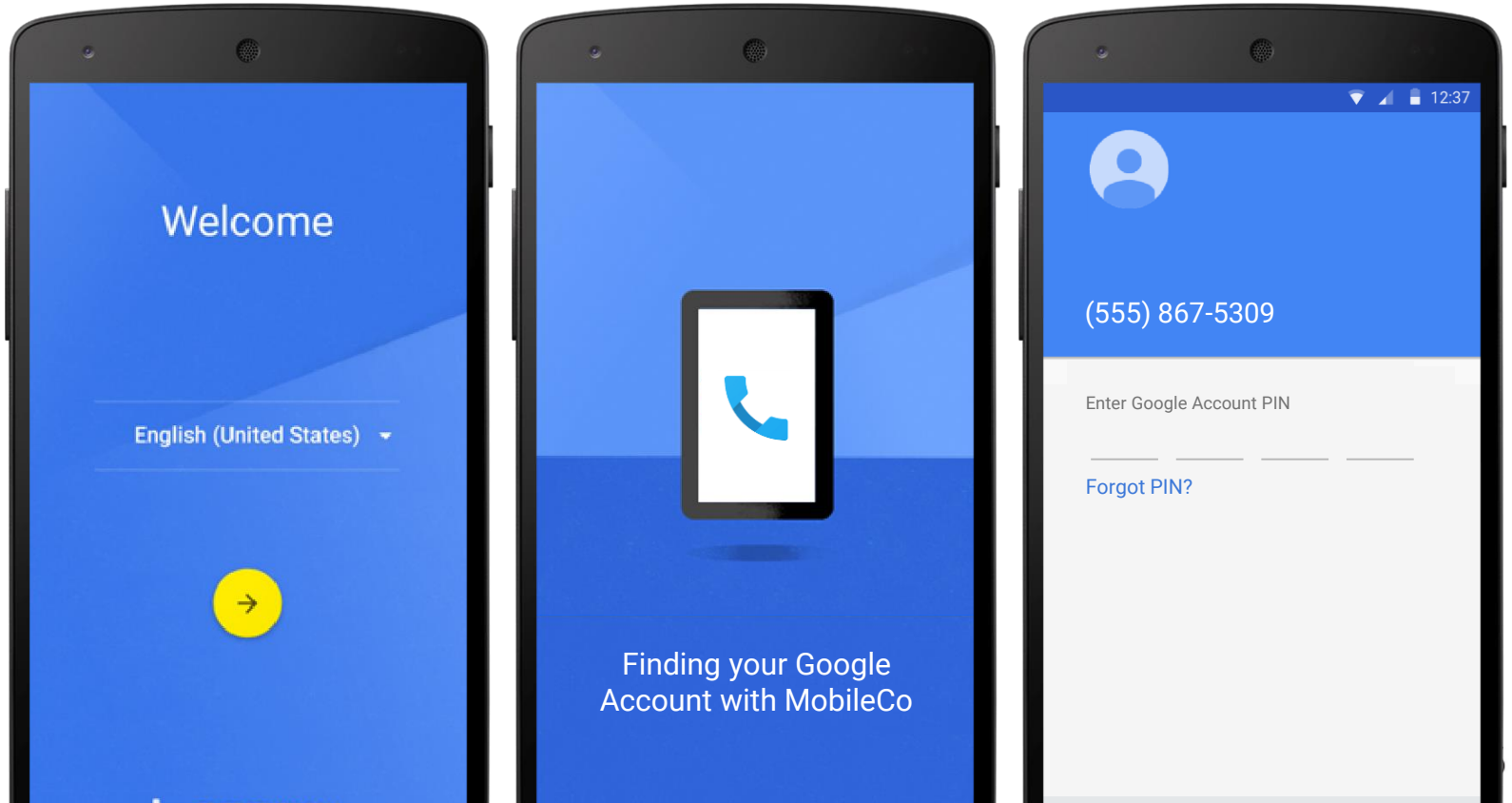
Google


Sign in - Google Accounts
Eric
https://accounts.google.com/ServiceLogin?hl=en&continue=https://www.google.com/webhp%3Fsourceid%3Dchrome-...
mlaaker@gmail.com
Approve Sign In on your trusted device
We sent a notification to your phone: Micah's iPhone
Please launch the Google app to sign in.
Need help?

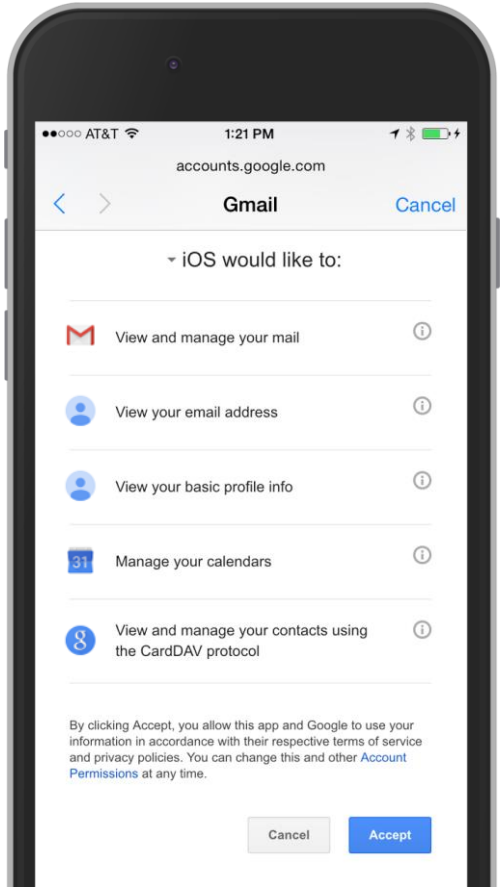

mlaaker@gmail.com
Trying to Sign In?
Are you trying to sign in to Janelle's Macbook Pro from Mountain View, CA, USA?
NO
YES
Google

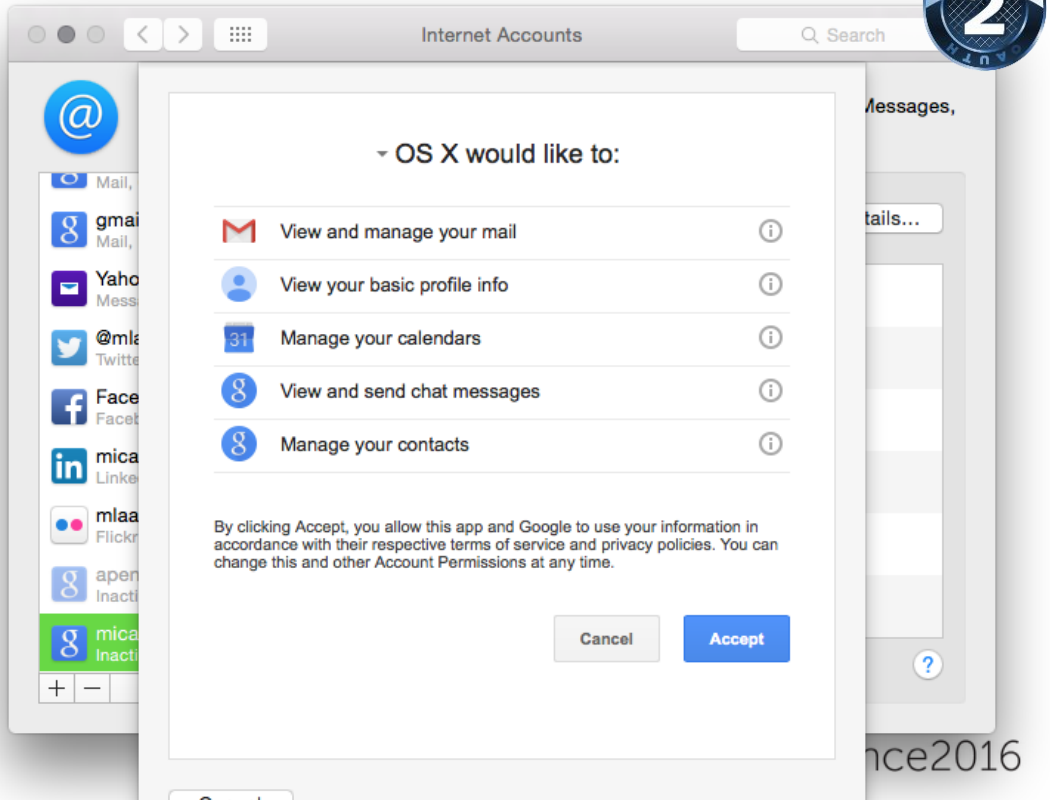
Google


Tap & Go
Quickly copy any Google Accounts, backed up apps and data from your existing Android device. To copy:
1. Make sure your other device is on and unlocked.
2. Briefly place the two devices back-to-back until you hear a tone, then set aside.
Learn more
11:39
Authenticator
Touch & hold
Hold your security key flat against the back of this device
CANCEL

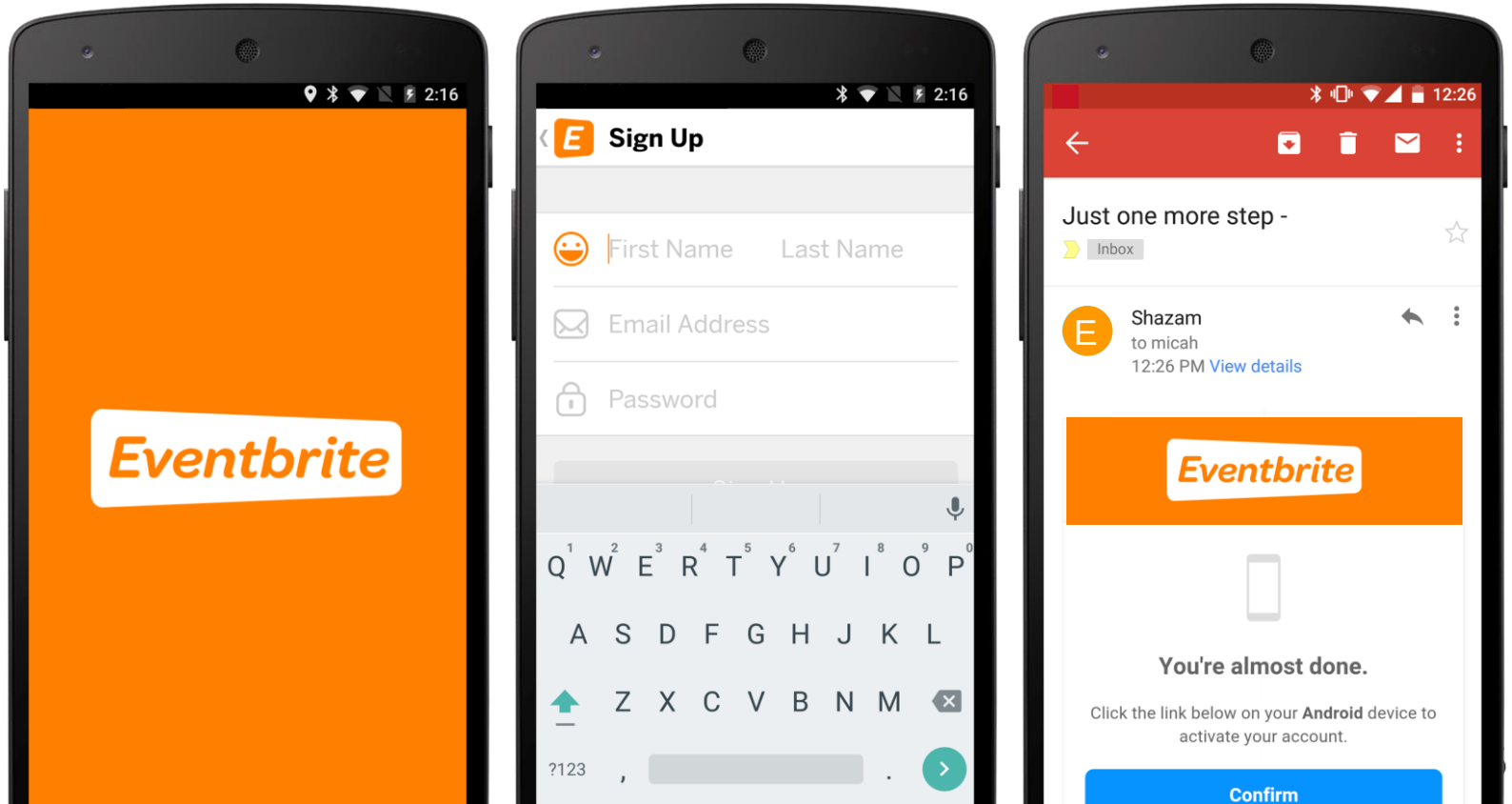

Welcome
English (United States)
Finding your Google Account with MobileCo
12:37
(555) 867-5309
Enter Google Account PIN
Forgot PIN?

Google

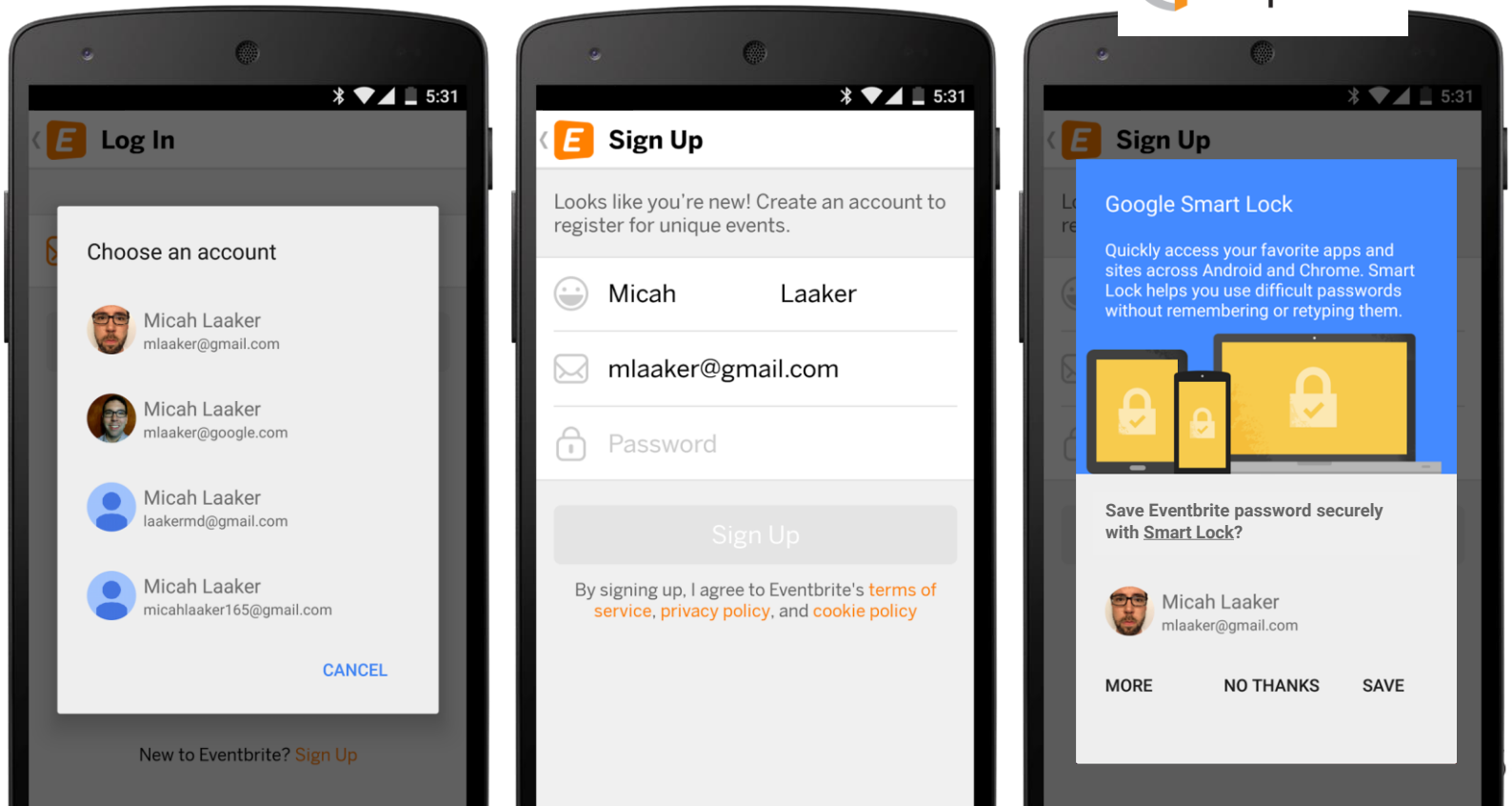

AT&T
1:21 PM
accounts.google.com
Gmail
Cancel
iOS would like to:
View and manage your mail
View your email address
View your basic profile info
Manage your calendars
View and manage your contacts using the CardDAV protocol
By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.
Cancel
Accept

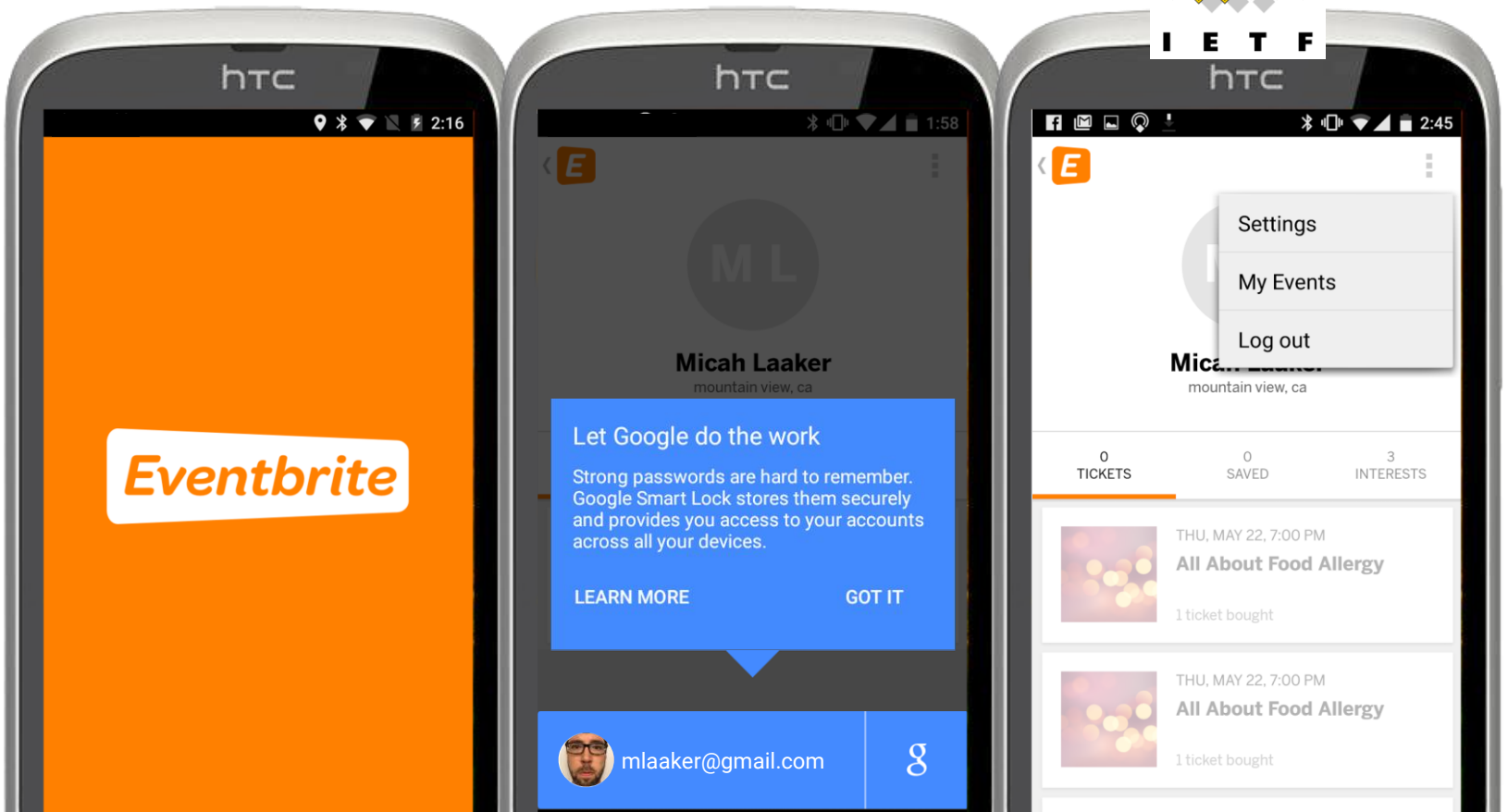

Internet Accounts
Search
OS X would like to:
View and manage your mail
View your basic profile info
Manage your calendars
View and send chat messages
Manage your contacts
By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.
Cancel
Accept

Sign in & registration on mobile is too painful



Google

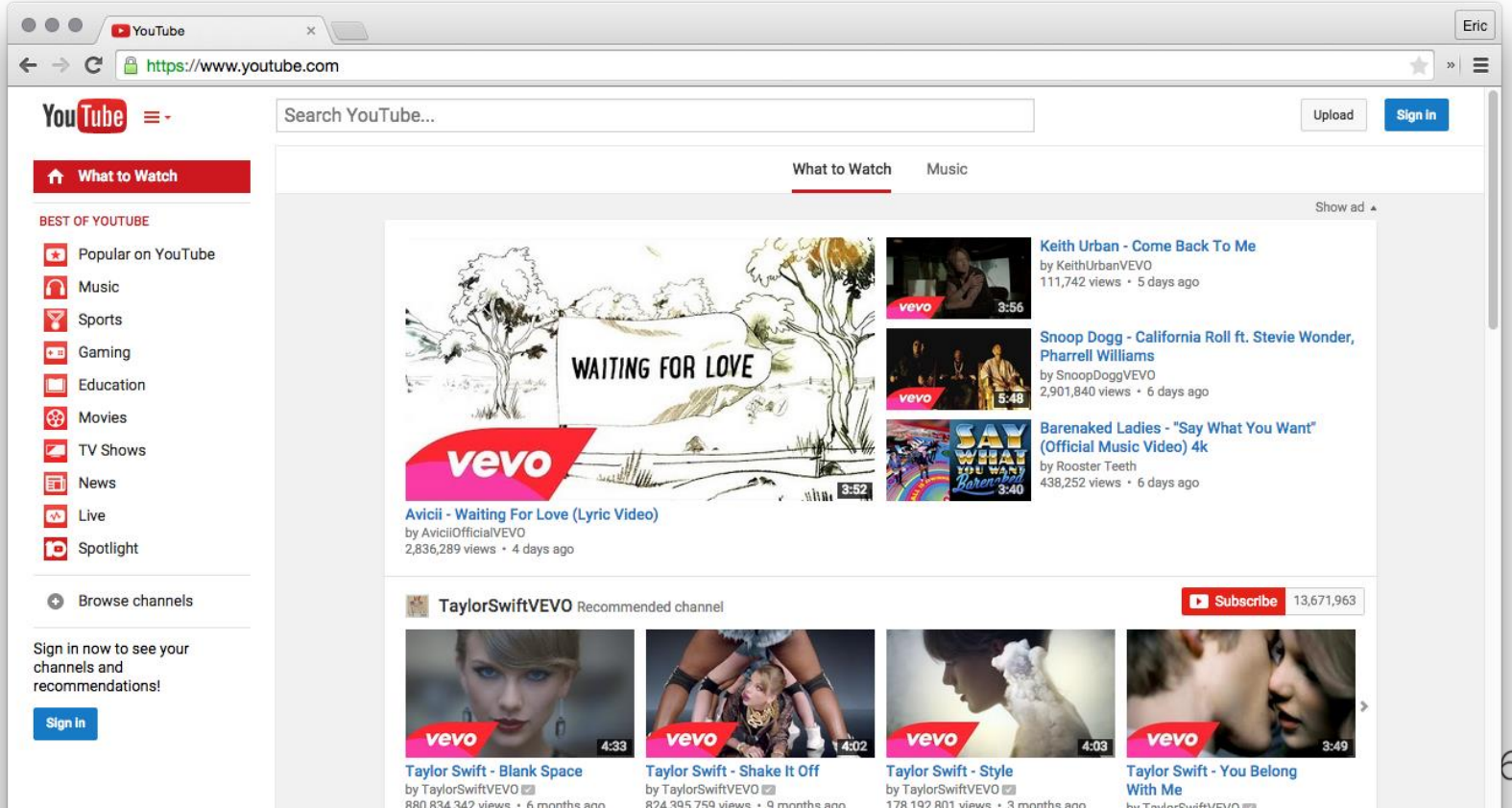

5:31
Log In
Choose an account
Micah Laaker
mlaaker@gmail.com
Micah Laaker
mlaaker@google.com
Micah Laaker
laakermd@gmail.com
Micah Laaker
micahlaaker165@gmail.com
CANCEL
New to Eventbrite? Sign Up
5:31
Sign Up
Looks like you're new! Create an account to register for unique events.
Micah
Laaker
mlaaker@gmail.com
Password
Sign Up
By signing up, I agree to Eventbrite's terms of service, privacy policy, and cookie policy
5:31
Sign Up
Google Smart Lock
Quickly access your favorite apps and sites across Android and Chrome. Smart Lock helps you use difficult passwords without remembering or retyping them.
Save Eventbrite password securely with Smart Lock?
Micah Laaker
mlaaker@gmail.com
MORE
NO THANKS
SAVE

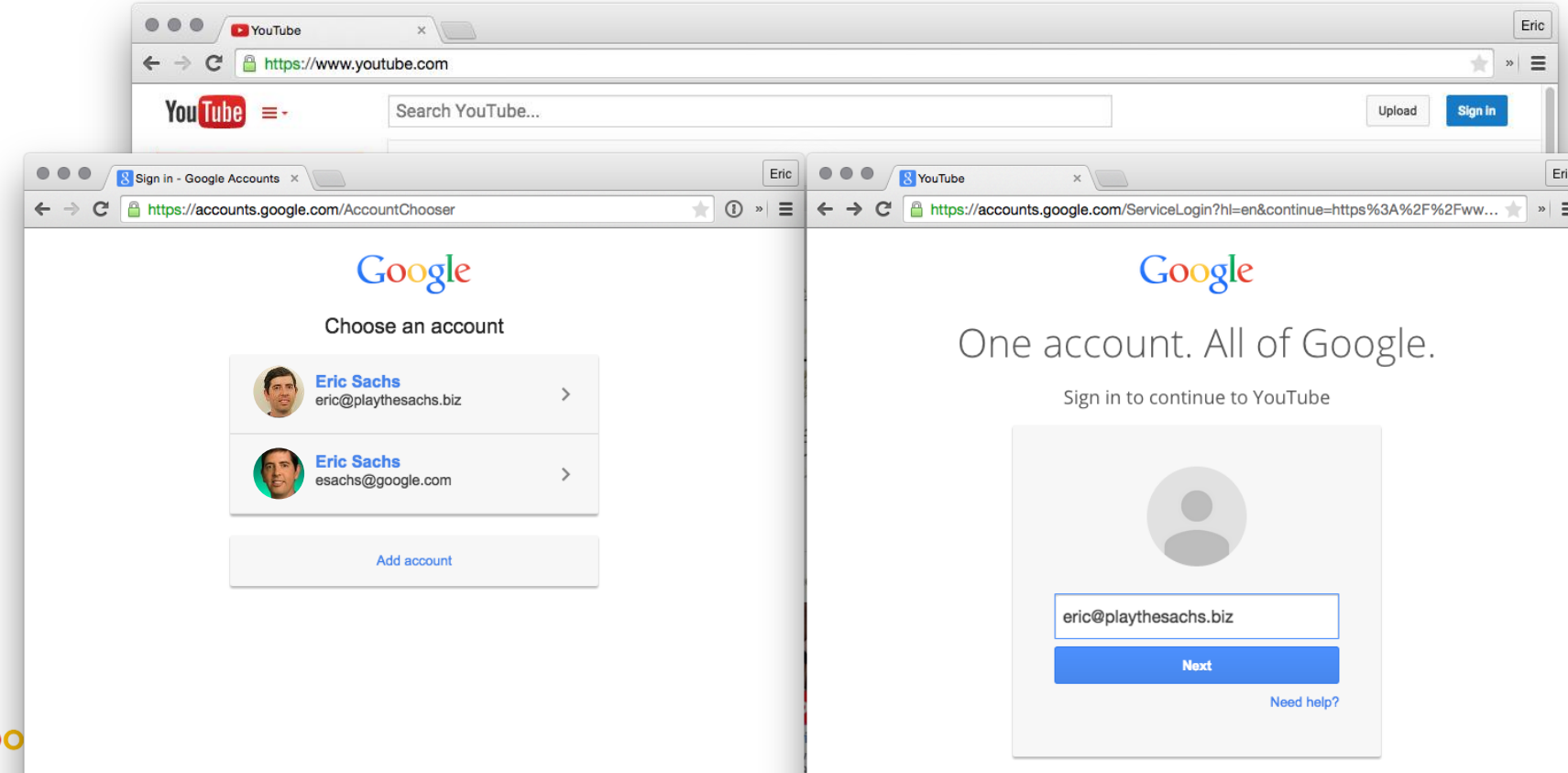

htc
2:16
Eventbrite
htc
1:58
M L
Micah Laaker
mountain view, ca
Let Google do the work
Strong passwords are hard to remember. Google Smart Lock stores them securely and provides you access to your accounts across all your devices.
LEARN MORE
GOT IT
mlaaker@gmail.com
g
htc
2:45
Settings
My Events
Log out
mountain view, ca
0
TICKETS
0
SAVED
3
INTERESTS
THU, MAY 22, 7:00 PM
All About Food Allergy
1 ticket bought
THU, MAY 22, 7:00 PM
All About Food Allergy
1 ticket bought

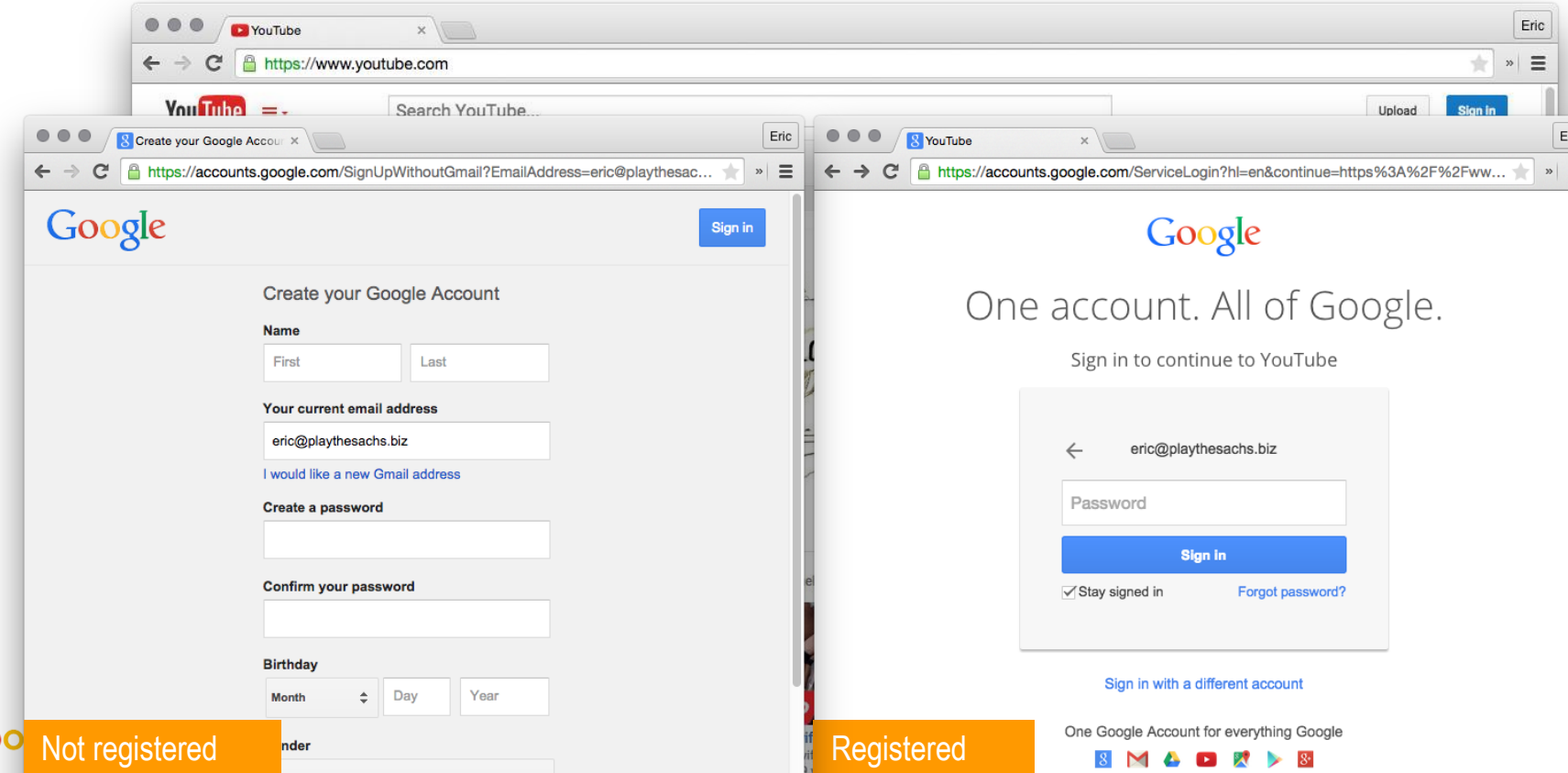
Google

I E T F

Don’t overthink

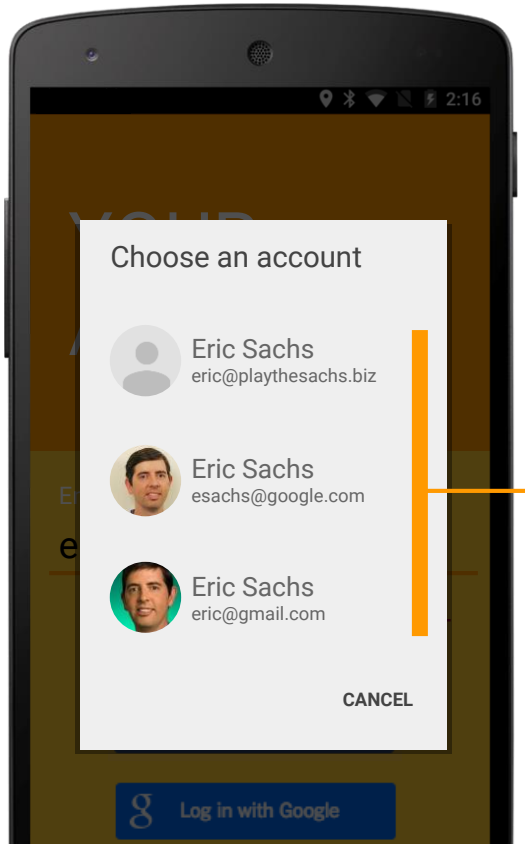



YouTube
Eric
https://www.youtube.com
YouTube
Search YouTube...
Upload
Sign in
Sign in - Google Accounts
Eric
https://accounts.google.com/AccountChooser
Google
Choose an account
Eric Sachs
eric@playthesachs.biz
Eric Sachs
esachs@google.com
Add account
YouTube
Eric
https://accounts.google.com/ServiceLogin?hl=en&continue=https%3A%2F%2Fww...
Google
One account. All of Google.
Sign in to continue to YouTube
eric@playthesachs.biz
Next
Need help?



Not registered

Registered



new user? → Select authentication method

returning user with password? → Input existing password

returning federated login user? → Authentication at Identity Provider

New UX, New Signals - backed by Standards

You can have the same UX as Google

http://accountchooser.com
- Simple Login Hints protected by consent, standards
- Overseen by OpenID Foundation http://ac.openid.net

Two added features
- Identifier-first form
- Protocol support for OpenID Connect login_hints

Cast:
- The IDP: Integral Curve
- The RP: Hipstabank
- The User: Alice

Try it:
http://hipstabank.com/business
demonstrates Federated Flows

What you Saw in the Demo

Login Hint

Hipstabank signalled Integral Curve to help initiate a login

Identifier First Login Flow

Integral Curve took the hint, only prompted for password

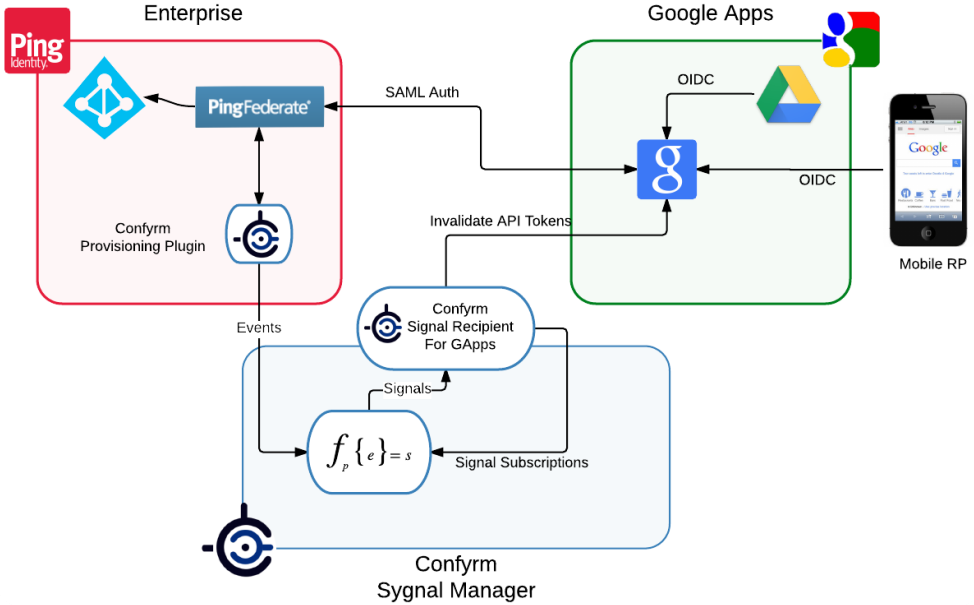
Account Record Stored

Hipstabank pushed an identifier and provider id into Account Chooser

AccountChooser Record Selected

Alice can click once to discover IDP, identify user, initiate SSO

What you Saw in the Demo

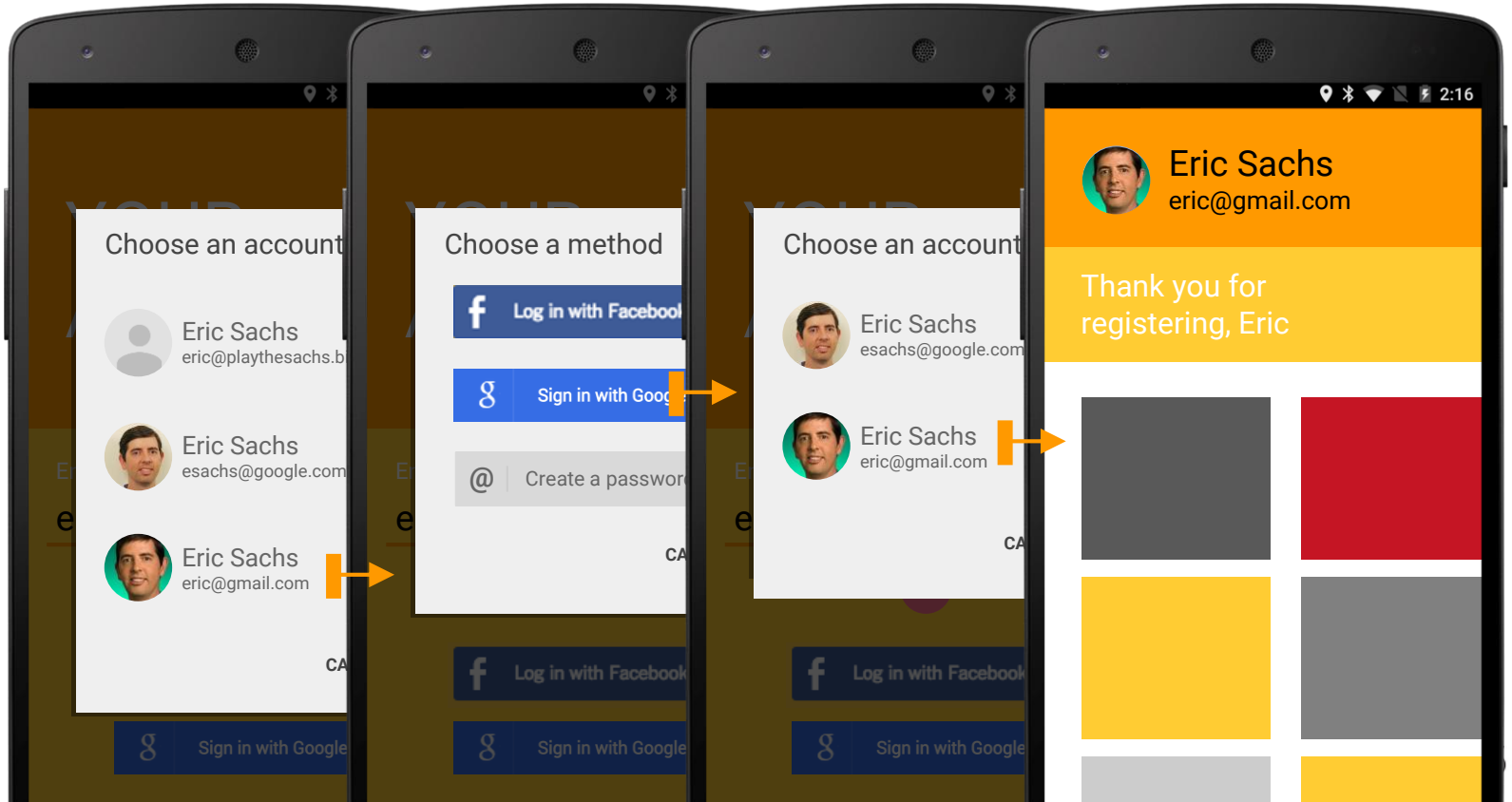


Account Event Detect & Publish

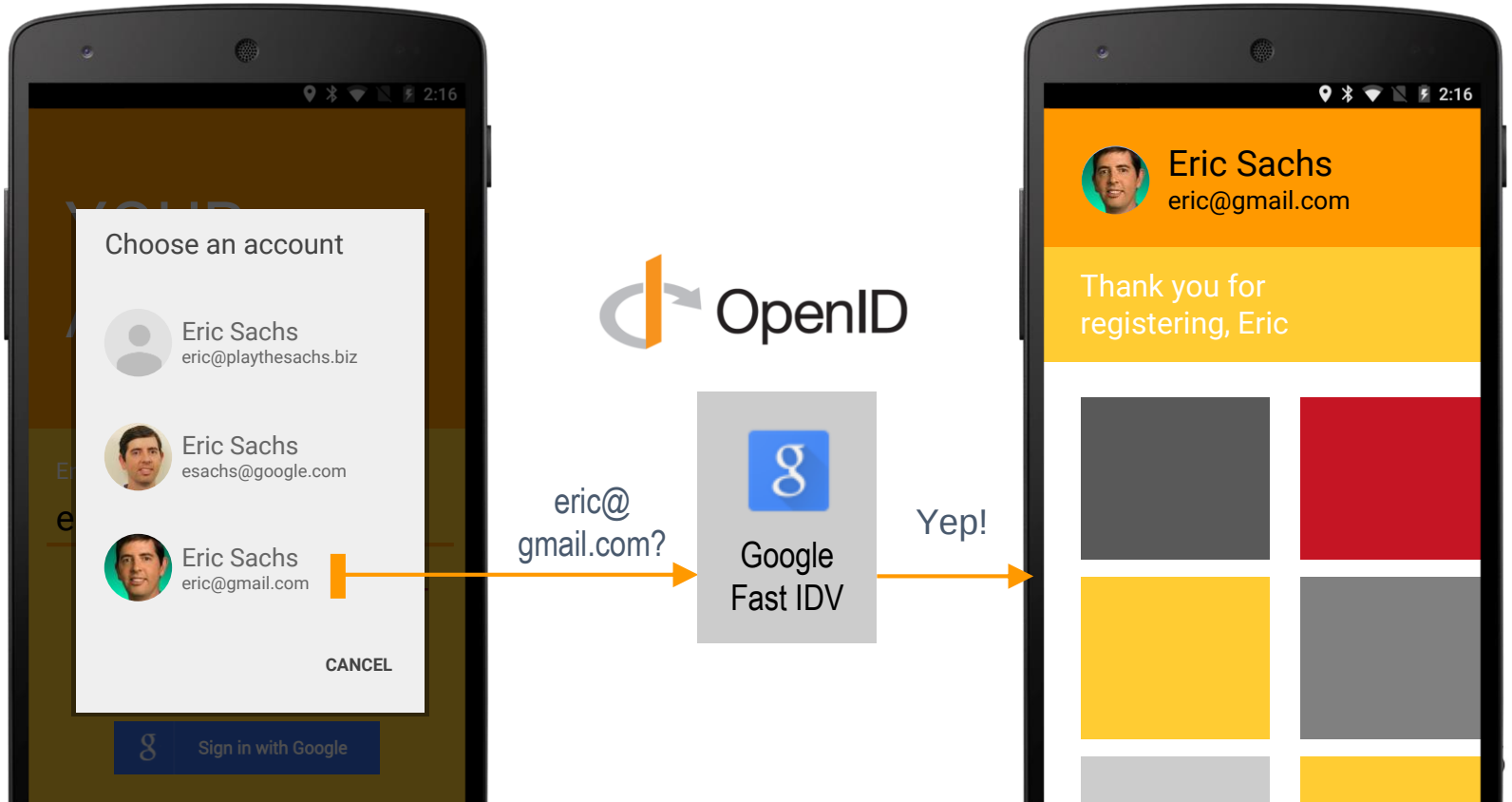
Signal Generation

Downstream Security Decisions

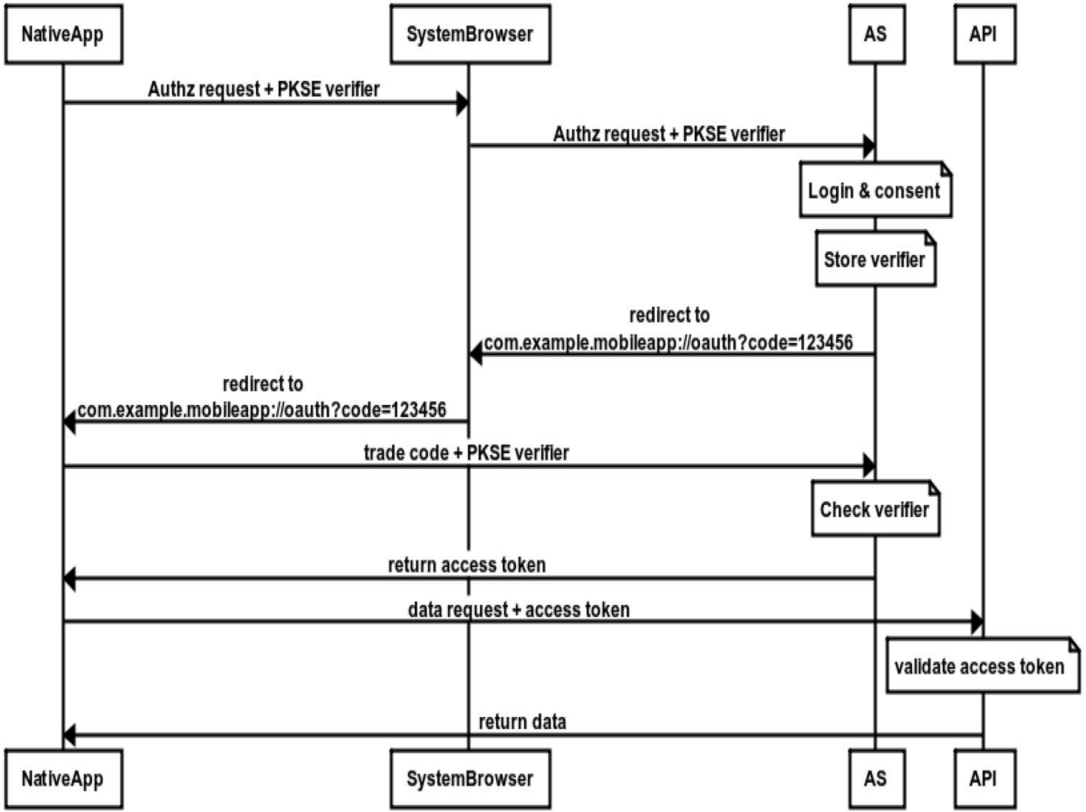
- Session invalidation
- Token Revocation

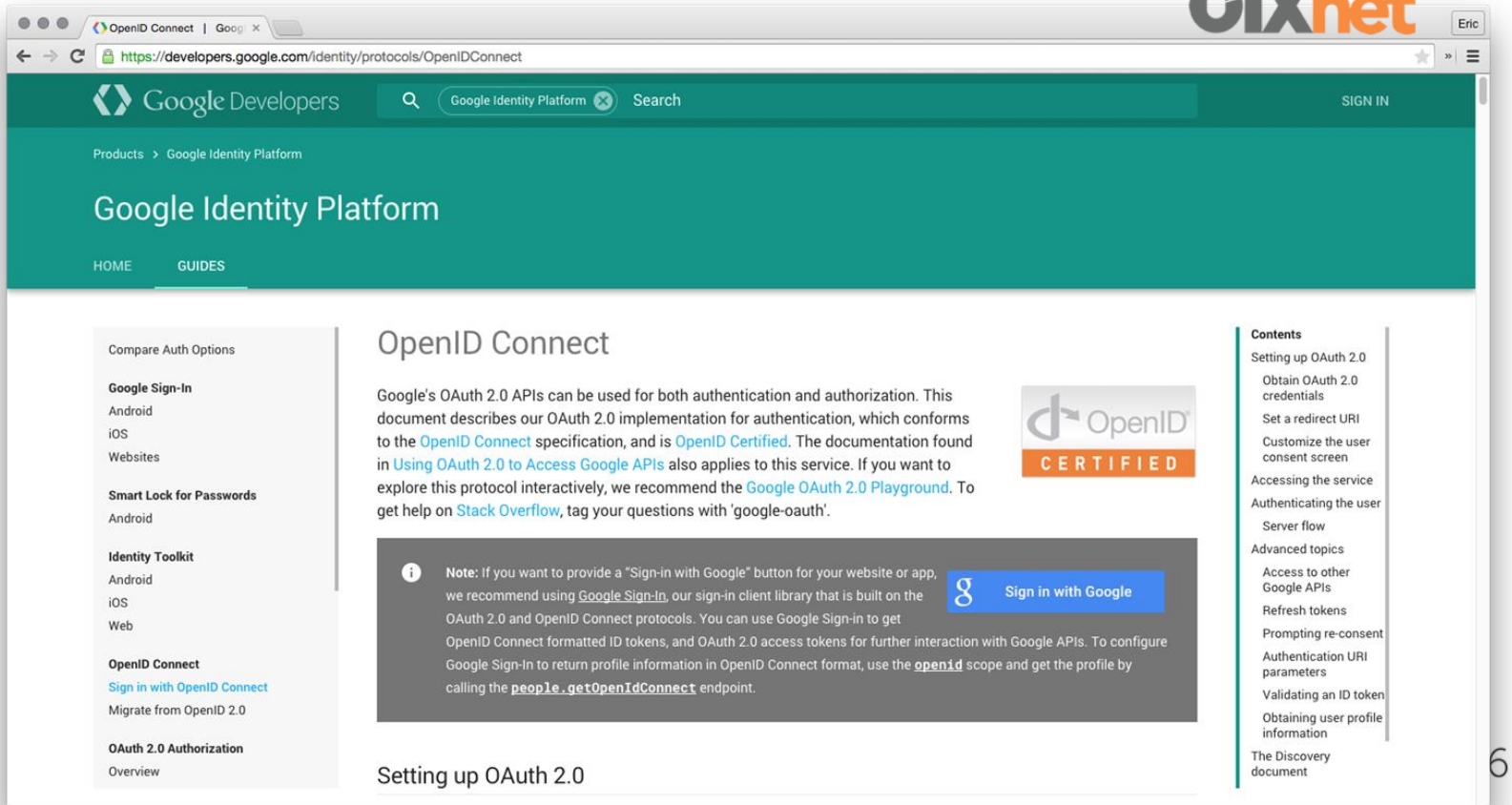

Choose an account
Eric Sachs
eric@playthesachs.b
Eric Sachs
esachs@google.com
Eric Sachs
eric@gmail.com
Sign in with Google
Choose a method
Log in with Facebook
Sign in with Goog
Create a passwor
Log in with Facebook
Sign in with Google
Choose an account
Eric Sachs
esachs@google.com
Eric Sachs
eric@gmail.com
Log in with Facebook
Sign in with Google
2:16
Eric Sachs
eric@gmail.com
Thank you for registering, Eric

Google

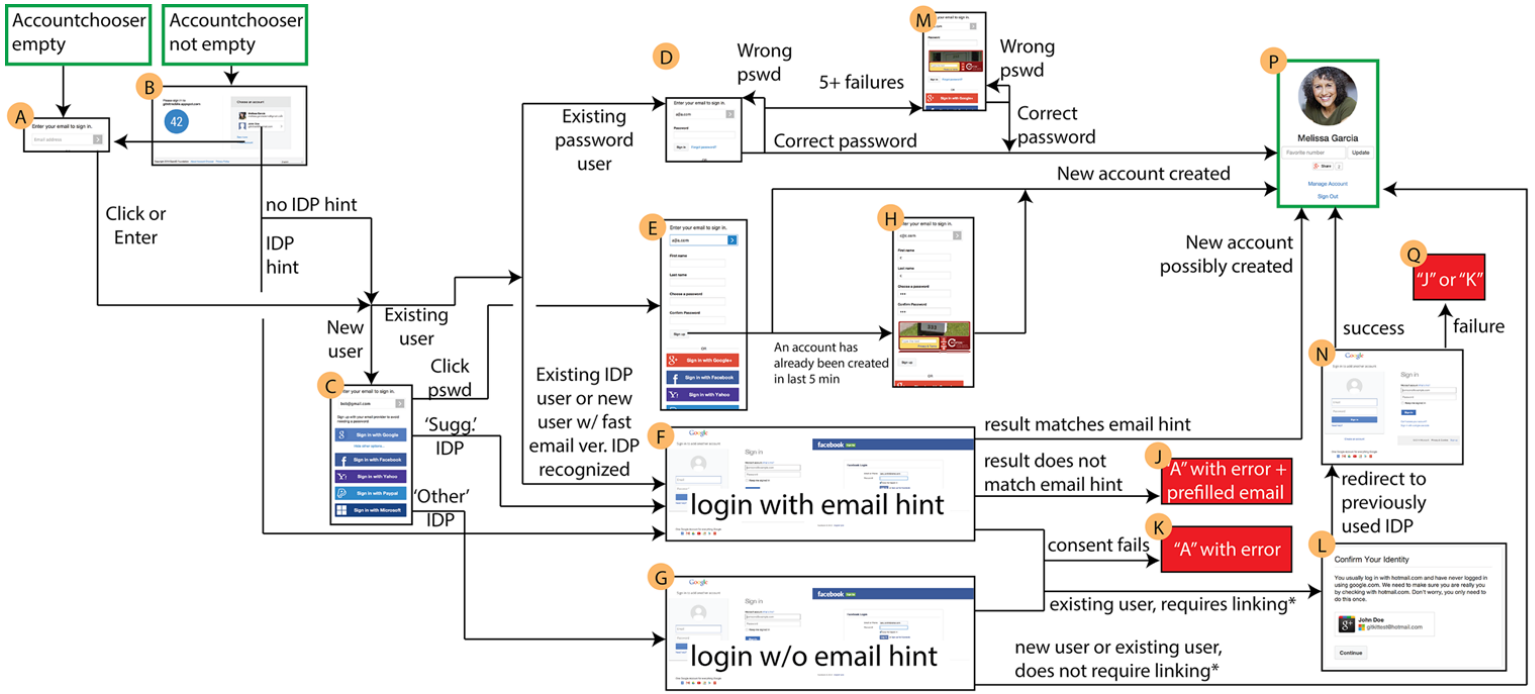

2:16
Choose an account
Eric Sachs
eric@playthesachs.biz
Eric Sachs
esachs@google.com
Eric Sachs
eric@gmail.com
CANCEL
Sign in with Google
OpenID
eric@
gmail.com?
Google
Fast IDV
Yep!
2:16
Eric Sachs
eric@gmail.com
Thank you for
registering, Eric

Google


NativeApp
SystemBrowser
AS
API
Authz request + PKSE verifier
Authz request + PKSE verifier
Login & consent
Store verifier
redirect to
com.example.mobileapp://oauth?code=123456
redirect to
com.example.mobileapp://oauth?code=123456
trade code + PKSE verifier
Check verifier
return access token
data request + access token
validate access token
return data
NativeApp
SystemBrowser
AS
API


OpenID Connect | Goog
https://developers.google.com/identity/protocols/OpenIDConnect
Eric
Google Developers
Google Identity Platform
Search
SIGN IN
Products › Google Identity Platform
Google Identity Platform
HOME
GUIDES
Compare Auth Options
Google Sign-In
Android
iOS
Websites
Smart Lock for Passwords
Android
Identity Toolkit
Android
iOS
Web
OpenID Connect
Sign in with OpenID Connect
Migrate from OpenID 2.0
OAuth 2.0 Authorization
Overview
OpenID Connect
Google's OAuth 2.0 APIs can be used for both authentication and authorization. This document describes our OAuth 2.0 implementation for authentication, which conforms to the OpenID Connect specification, and is OpenID Certified. The documentation found in Using OAuth 2.0 to Access Google APIs also applies to this service. If you want to explore this protocol interactively, we recommend the Google OAuth 2.0 Playground. To get help on Stack Overflow, tag your questions with 'google-oauth'.
OpenID CERTIFIED
Note: If you want to provide a "Sign-in with Google" button for your website or app, we recommend using Google Sign-In, our sign-in client library that is built on the OAuth 2.0 and OpenID Connect protocols. You can use Google Sign-in to get OpenID Connect formatted ID tokens, and OAuth 2.0 access tokens for further interaction with Google APIs. To configure Google Sign-In to return profile information in OpenID Connect format, use the openid scope and get the profile by calling the people.getOpenIdConnect endpoint.
Sign in with Google
Setting up OAuth 2.0
Contents
Setting up OAuth 2.0
Obtain OAuth 2.0 credentials
Set a redirect URI
Customize the user consent screen
Accessing the service
Authenticating the user
Server flow
Advanced topics
Access to other Google APIs
Refresh tokens
Prompting re-consent
Authentication URI parameters
Validating an ID token
Obtaining user profile information
The Discovery document

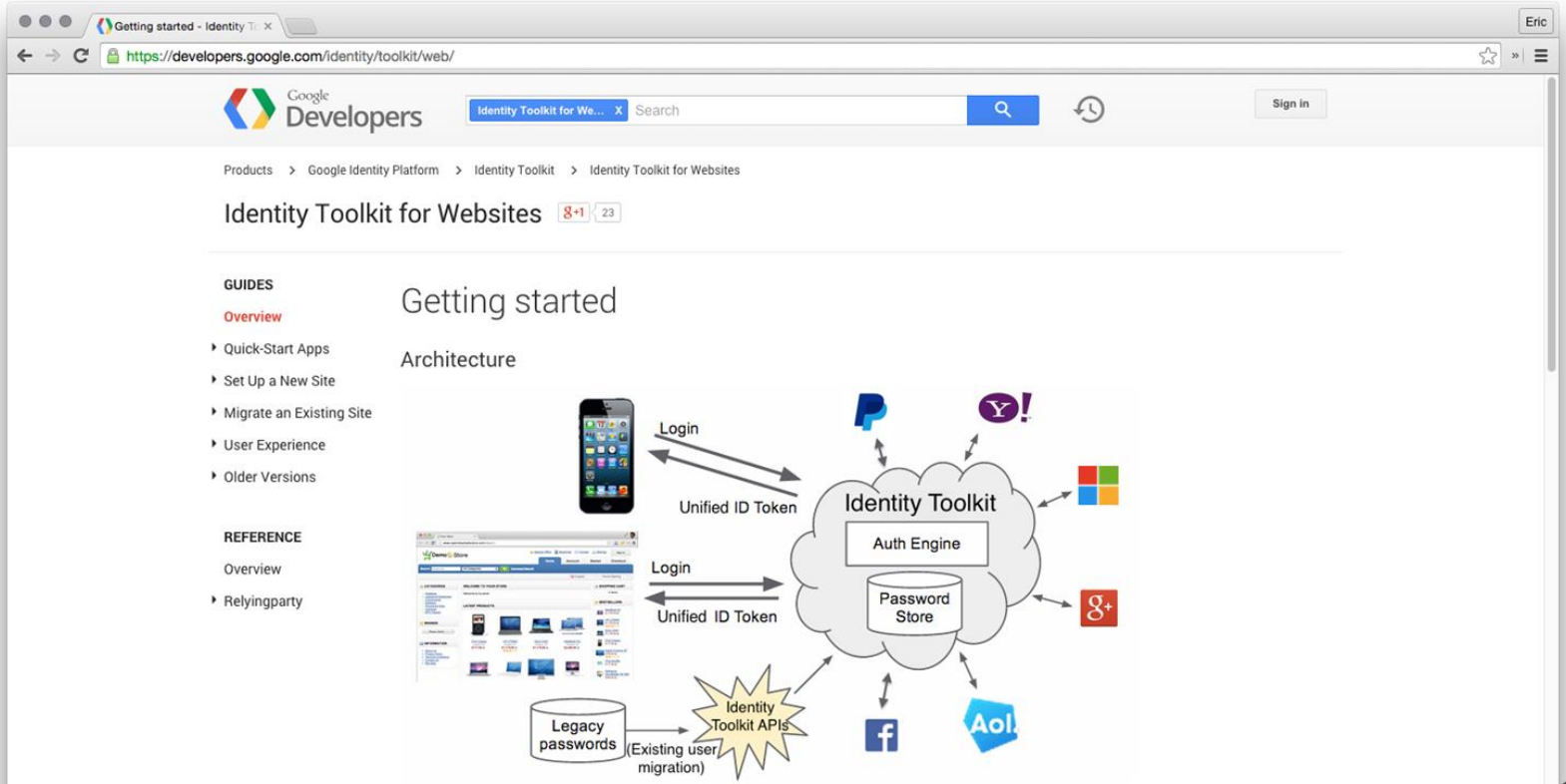
All you need to do is build this…



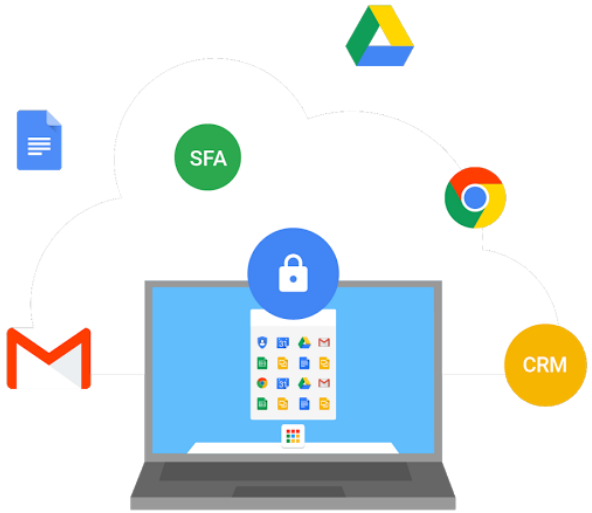
Google

*Linking is required if the email address has an existing account AND the IDP used to sign in has never been used to sign in before. This requirement is only waived if the IDP used to sign in is the email provider for the email address.

Google Identity Toolkit



For your employees...



Pick an IDaaS provider: Azure AD, Ping, Google Apps, Okta, …

Or combine them as Netflix did (Google Apps + Ping “Identity Bridge”)

Search for “Google Internet Identity Research” to find these slides and others from Google