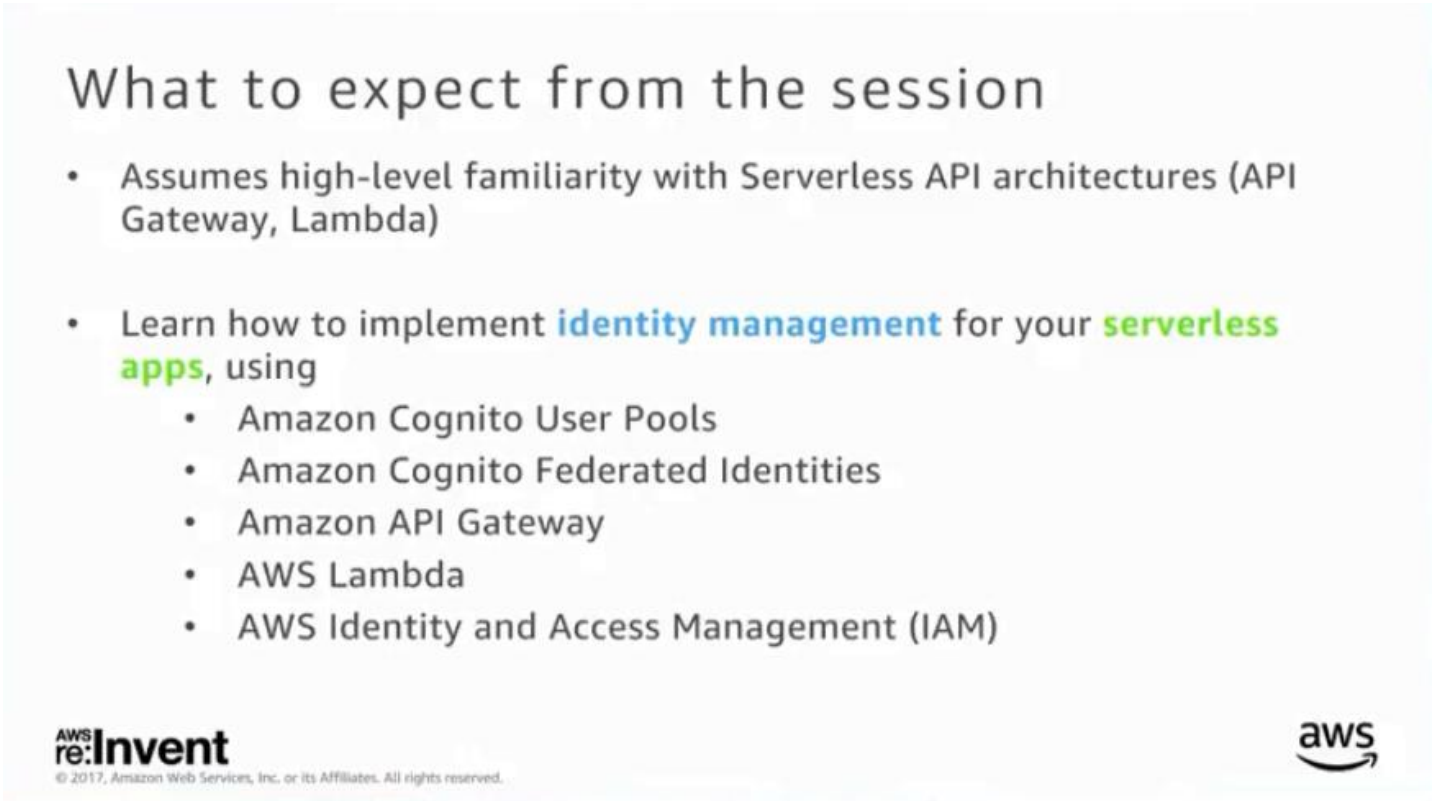
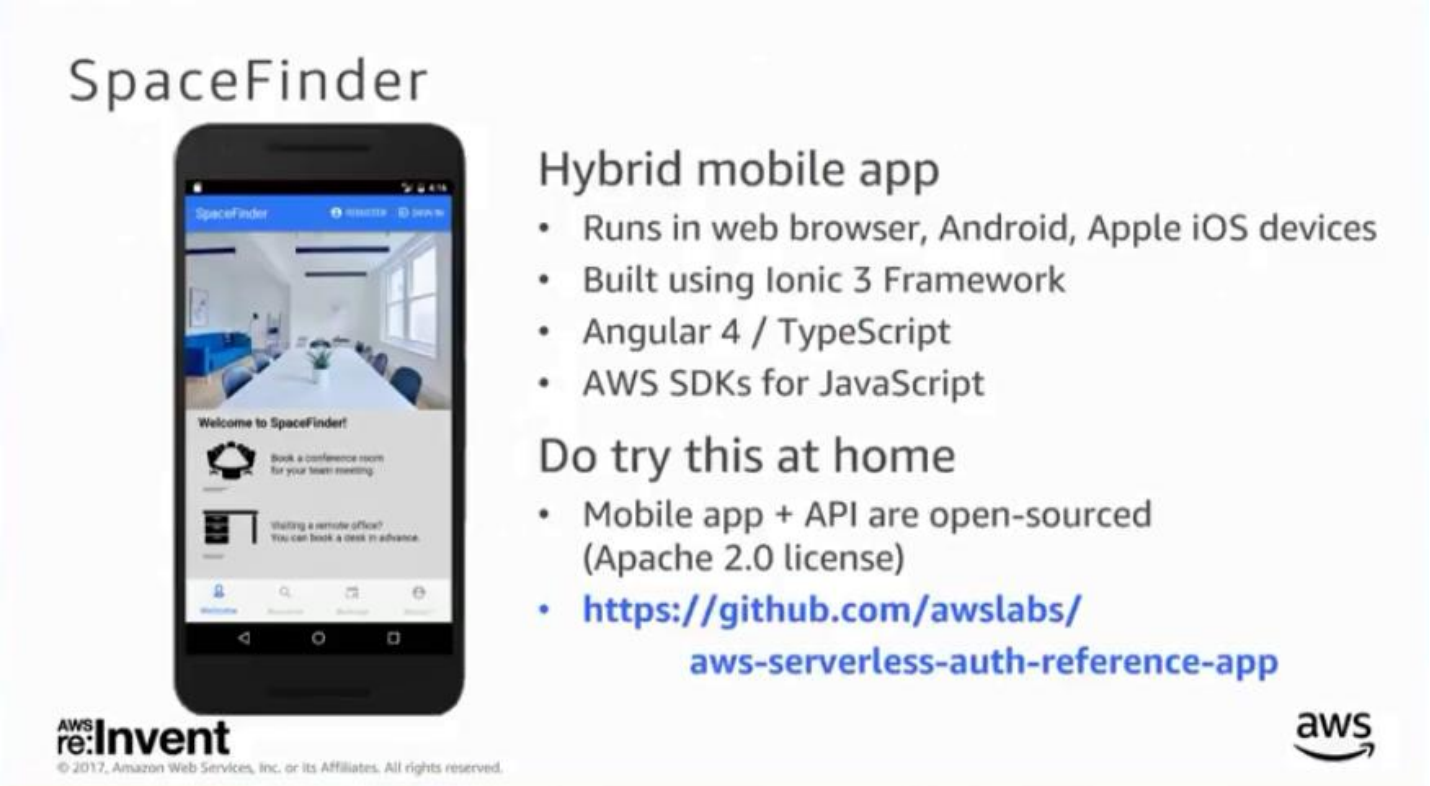
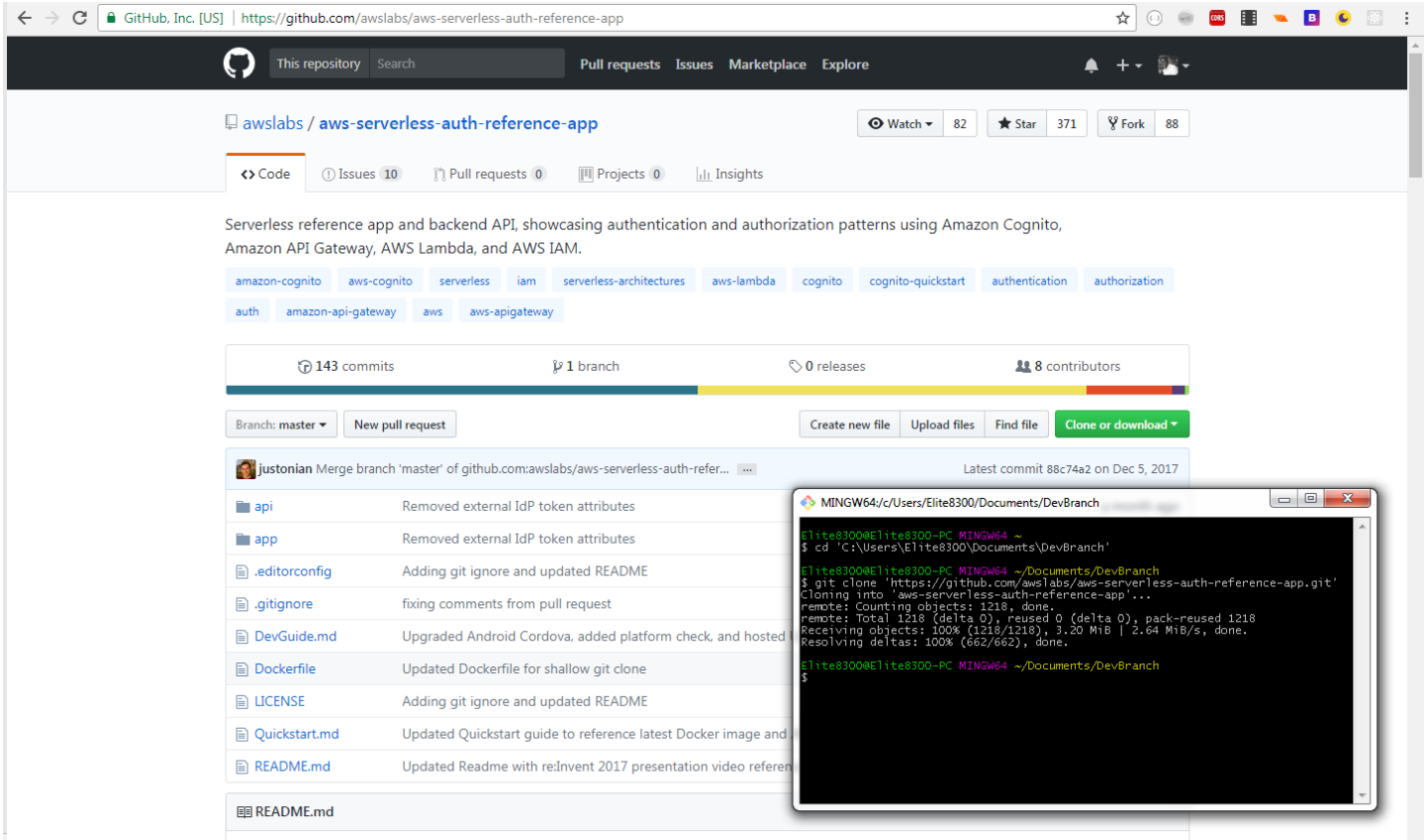
Many serverless applications need a way to manage end user identities and support sign-ups and sign-ins. Join this session to learn real-world design patterns for implementing authentication and authorization for your serverless application—such as how to integrate with social identity providers (such as Google and Facebook) and existing corporate directories. We cover how to use Amazon Cognito identity pools and user pools with API Gateway, Lambda, and IAM.

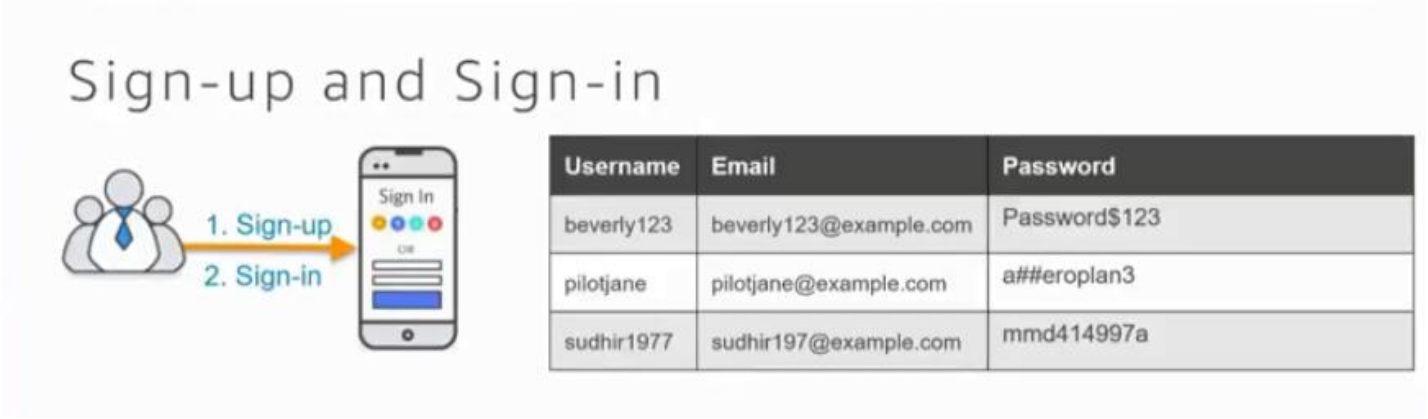




This is a conference room finder application

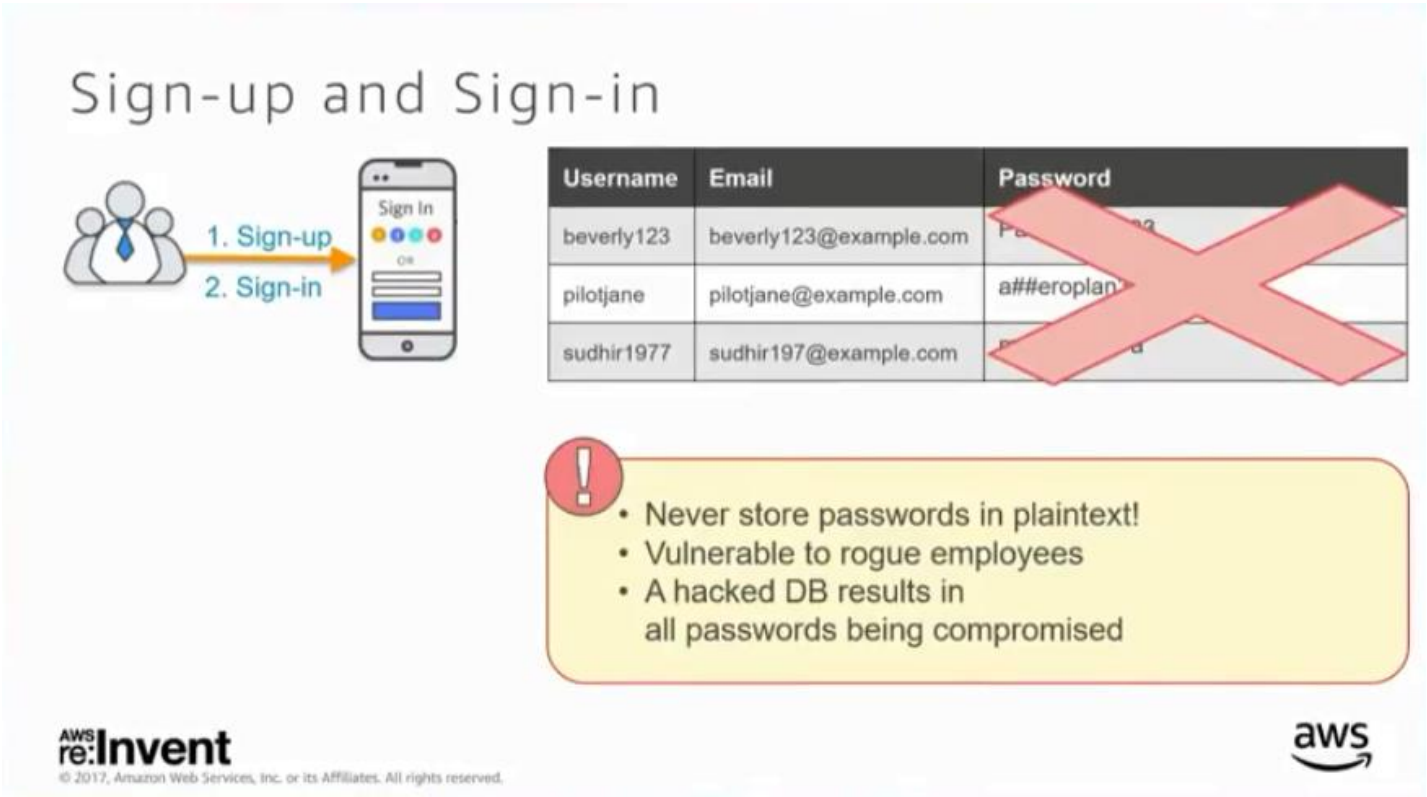


Imagine you have to create an app that allows users to sign up, sign in, upload their profile image, and search and book conference rooms. This requires managing users' identities.

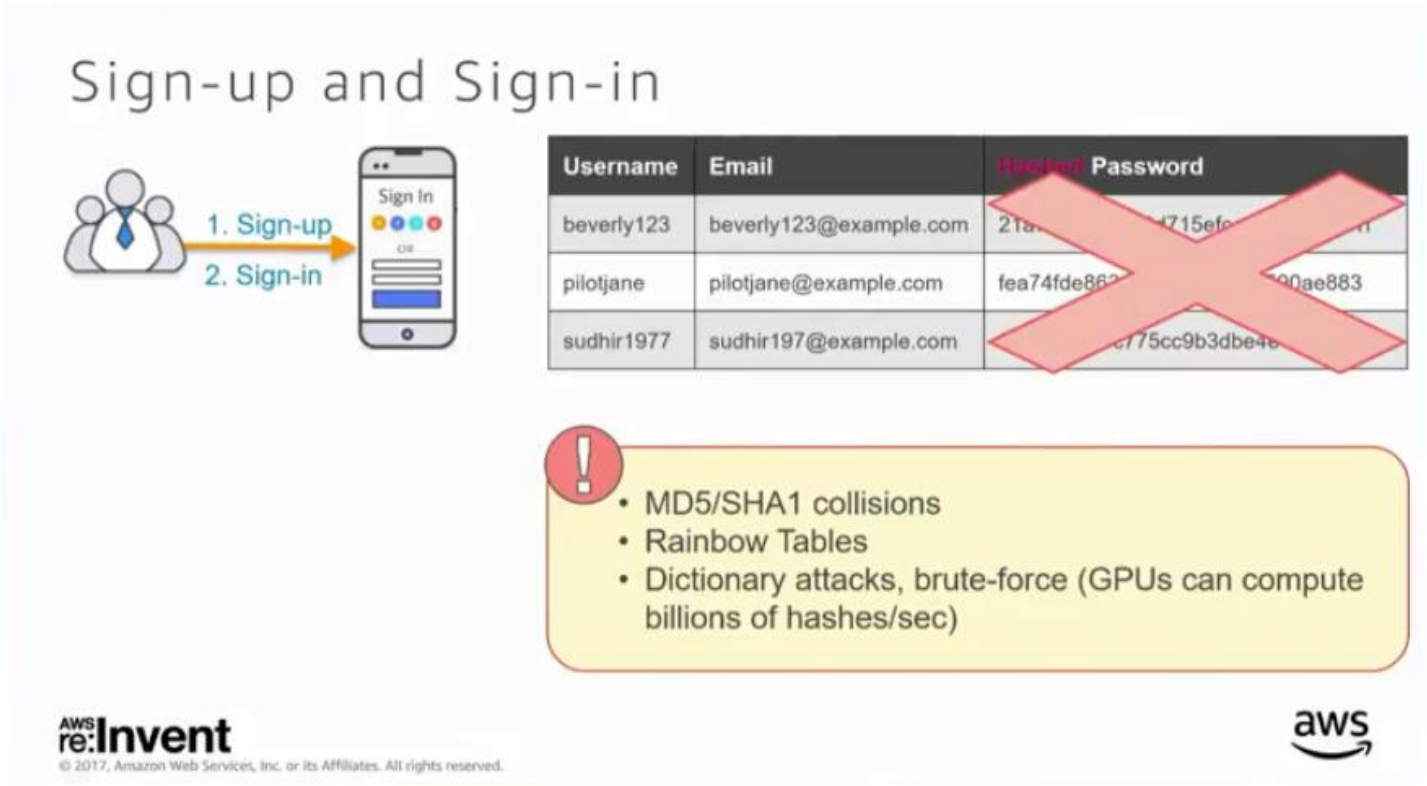


Username	Email	Password
beverly123	beverly123@example.com	Password$123
pilotjane	pilotjane@example.com	a##eroplan3
sudhir1977	sudhir197@example.com	mmd414997a

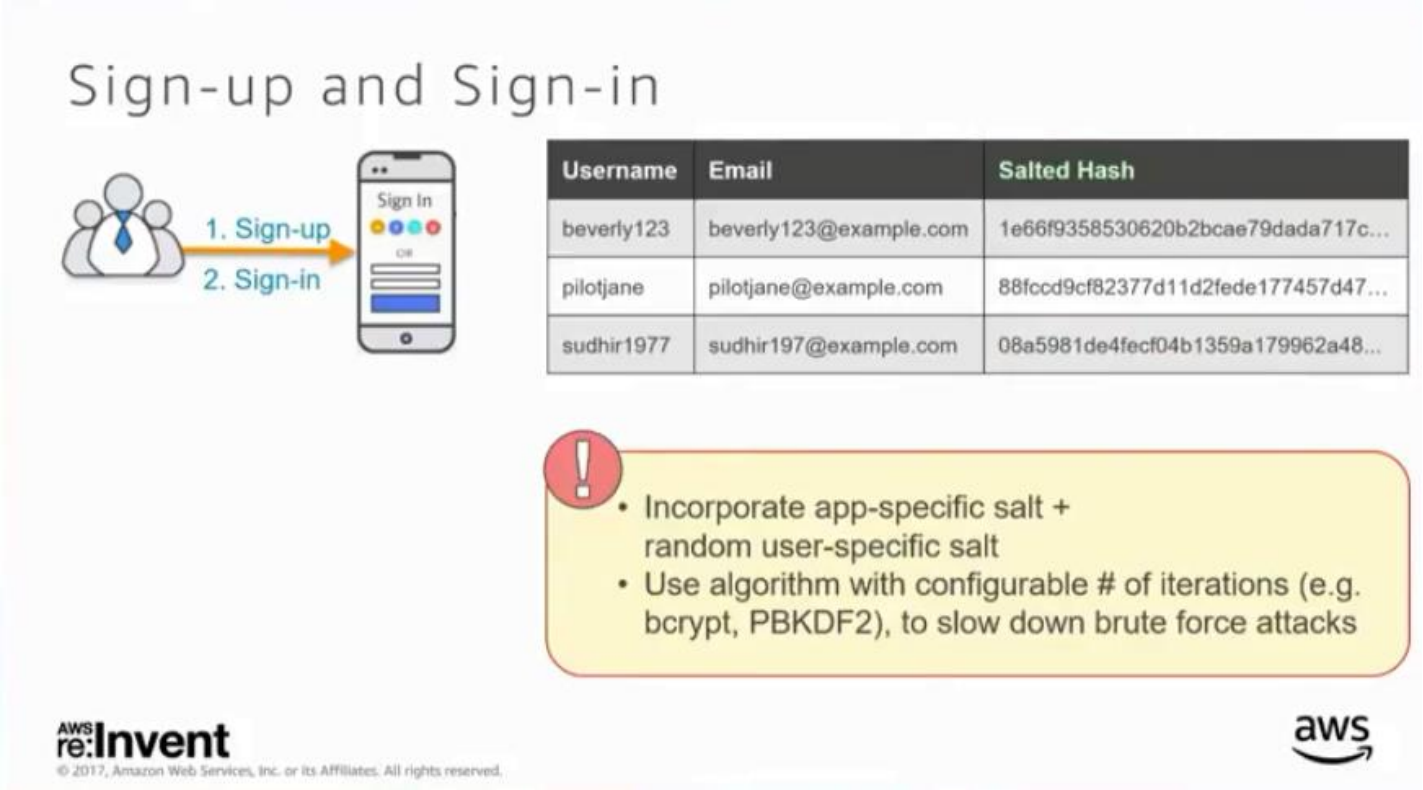
You might create the above



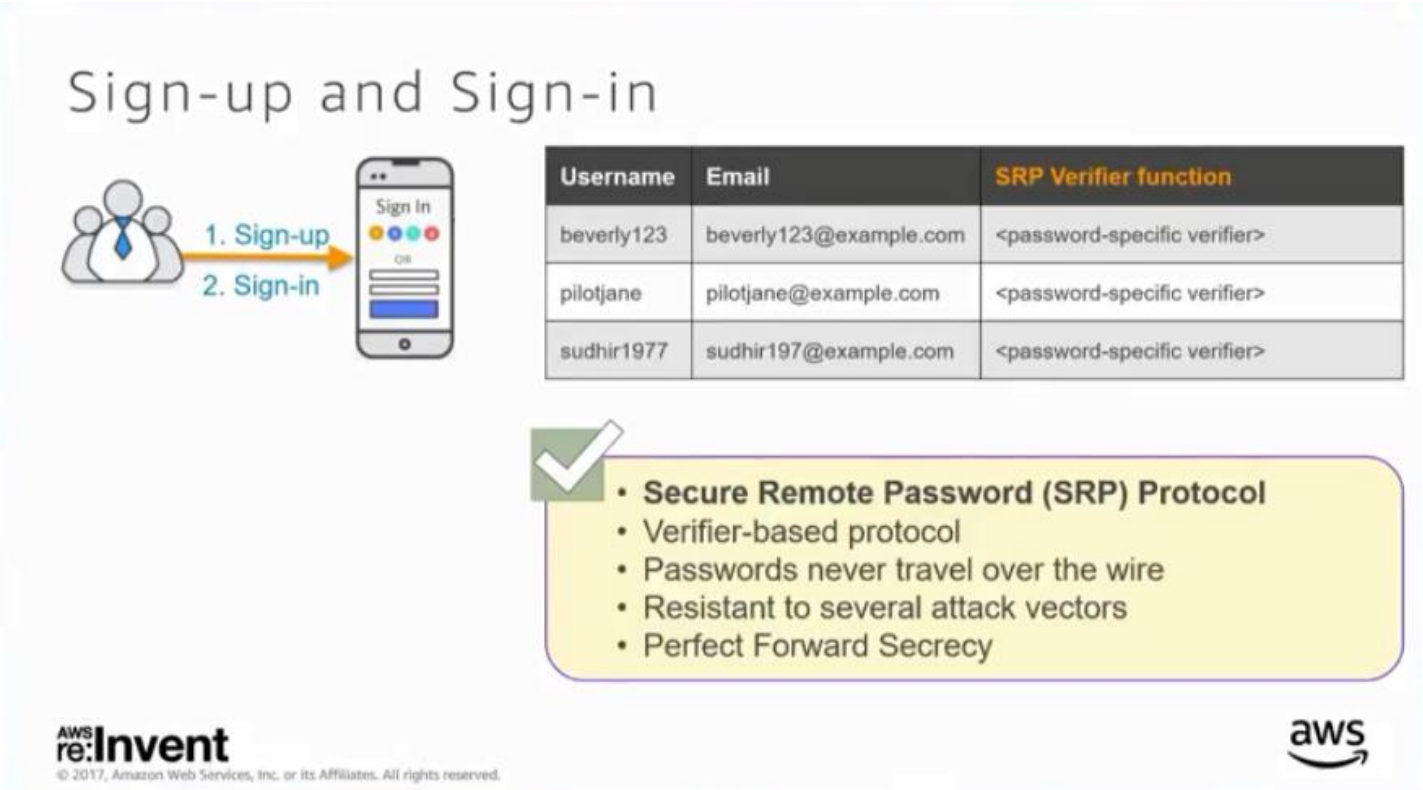
This is an antipattern



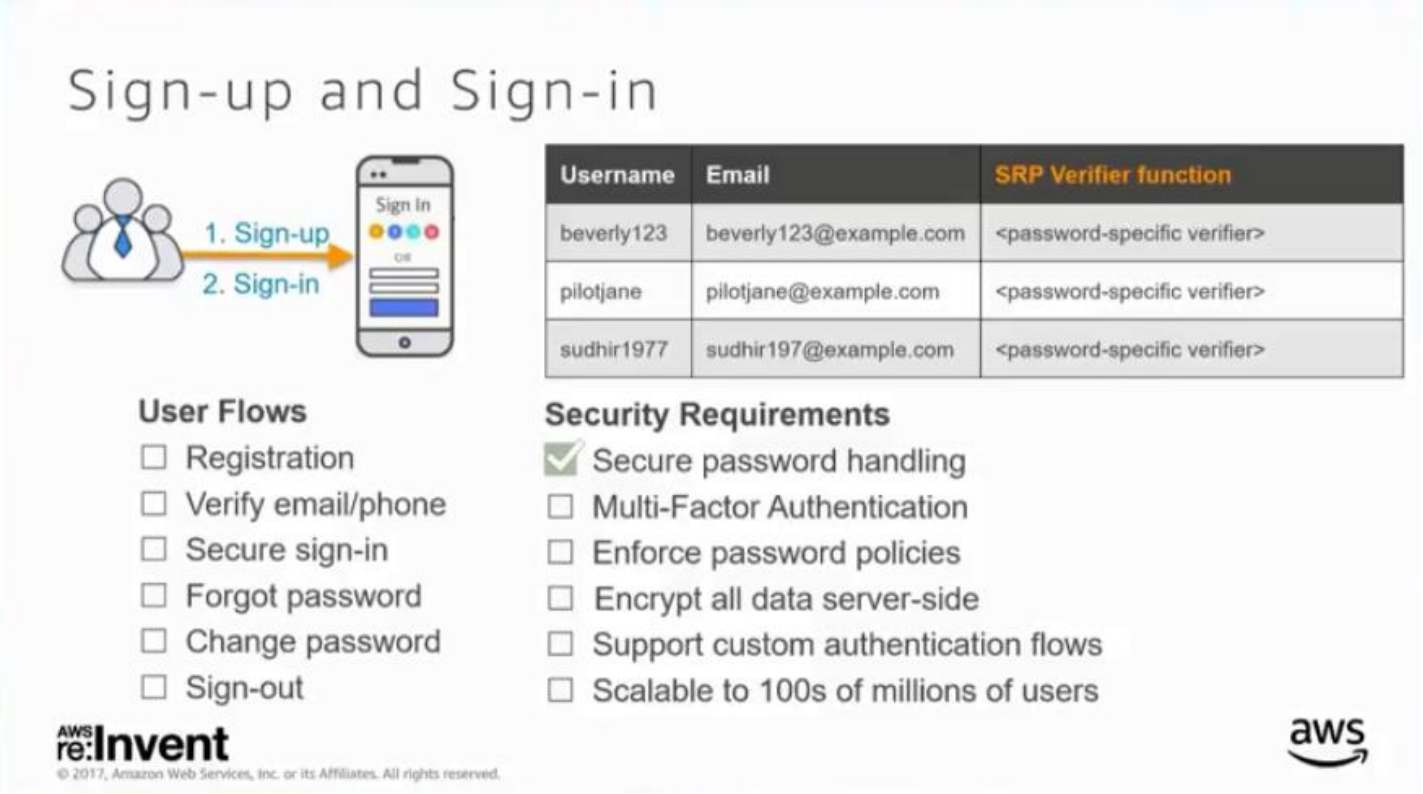
This is also a bad approach



A good approach is to salt hash the passwords but you might also not want to send the salted password over the wire for authentication

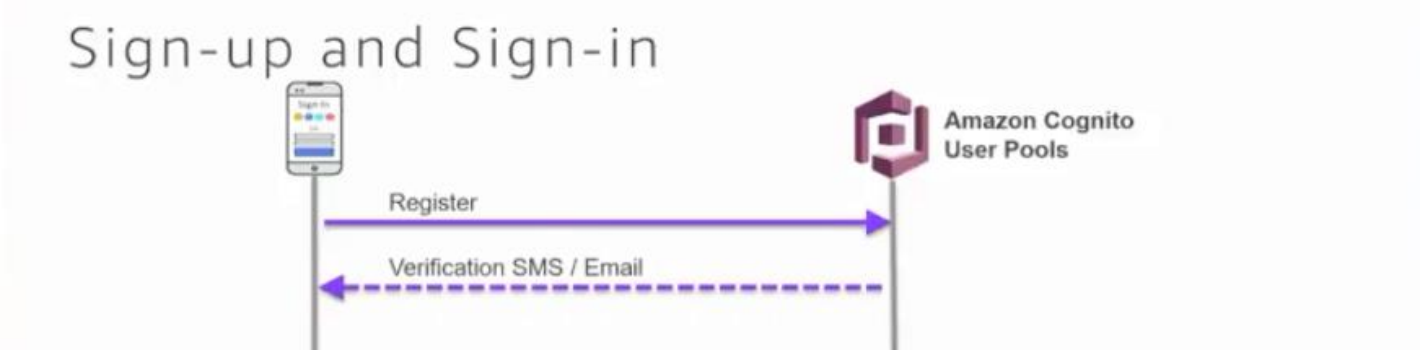


SRP allows you to transfer a verifier code created from the password and sent that over the wire instead.



What about the other factors listed above

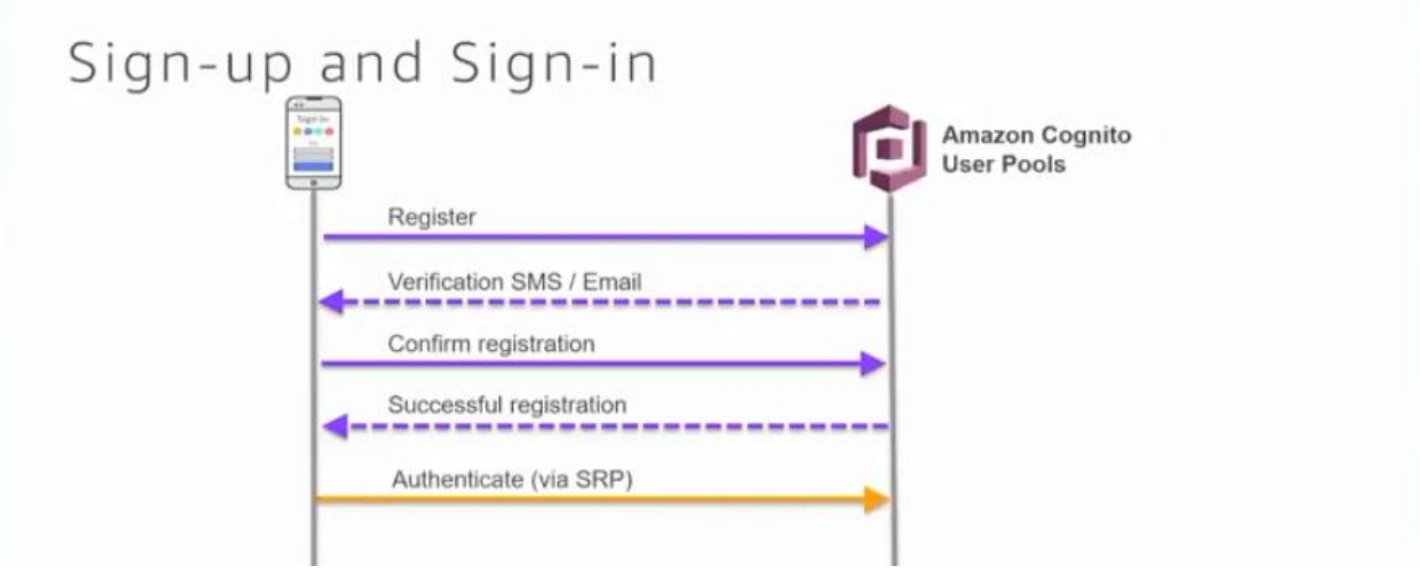
To use Cognito User Pools using our SDK, you send the users details for registration



You can also optionally set up the requirements to validate either the customers email or their SMS built into the service.

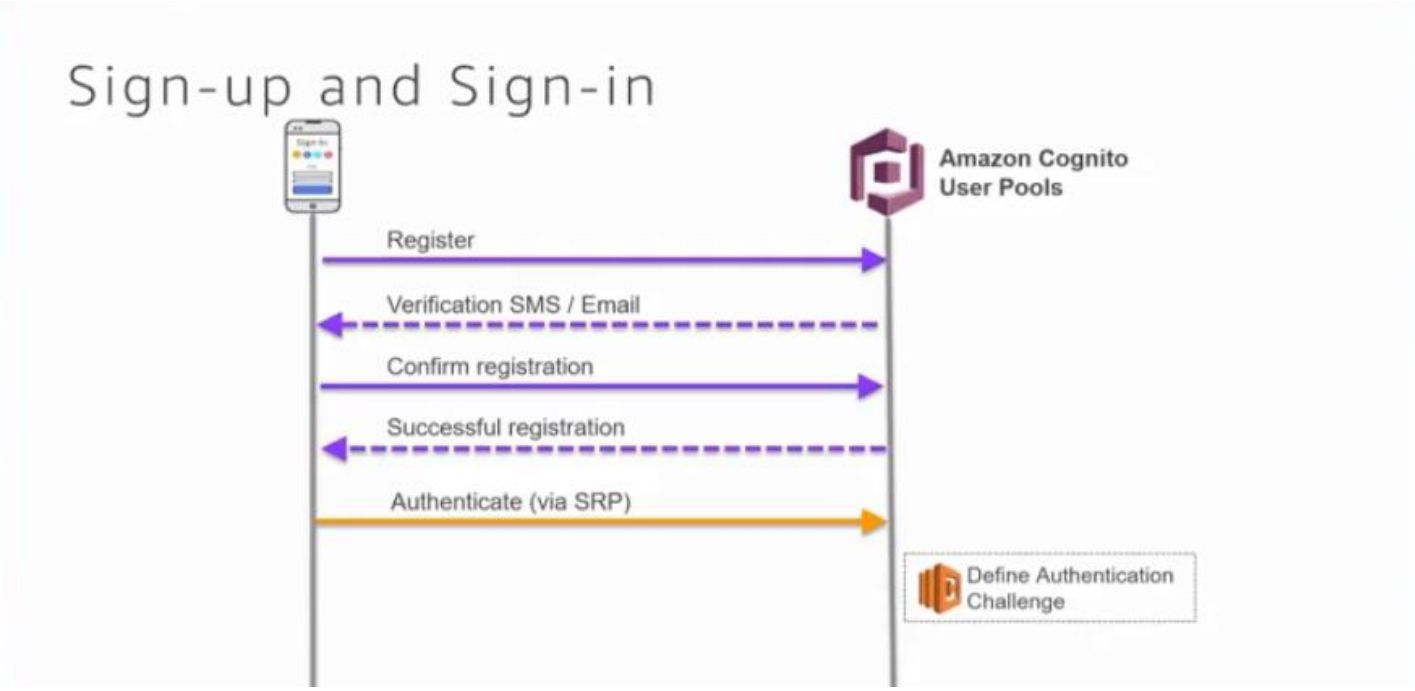
The user then has to use the code they got via email or SMS to confirm that they indeed got it

Then you have a successfully registered user that can actually authenticate with your service.

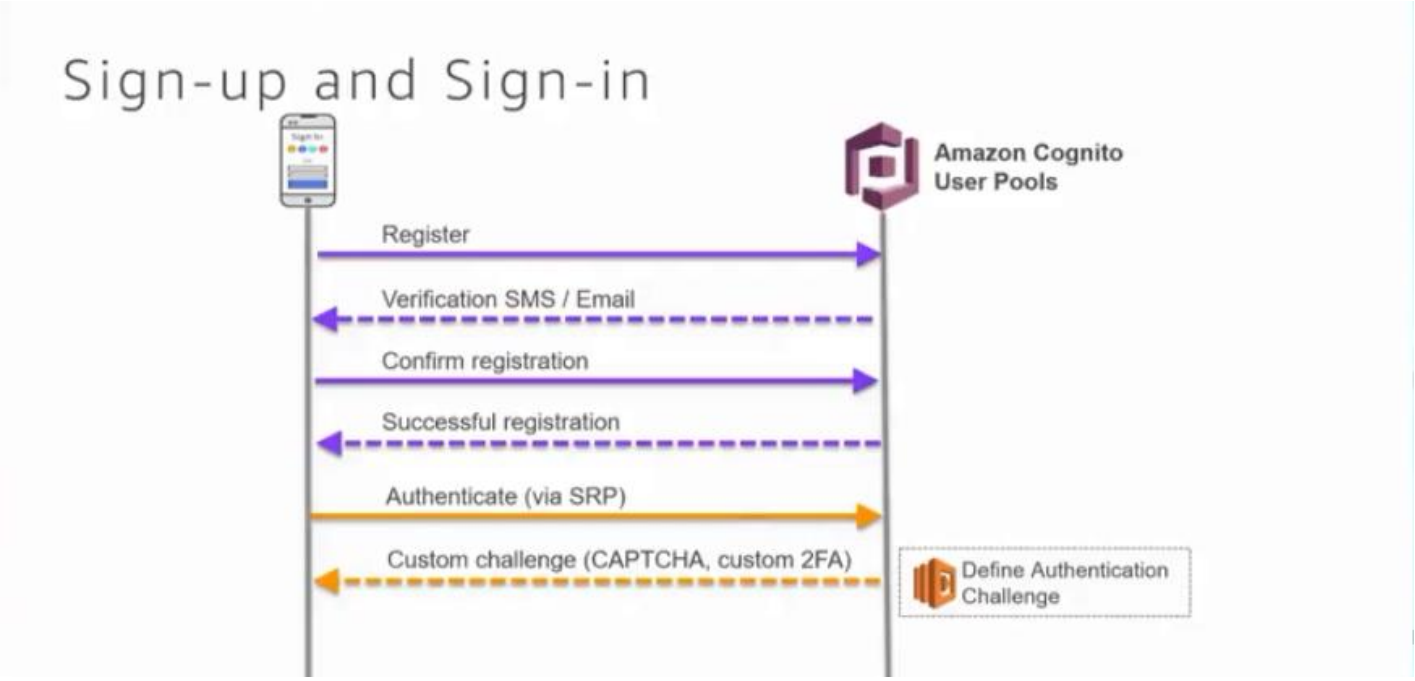


Once the user goes to authenticate during login, this is done using SRP

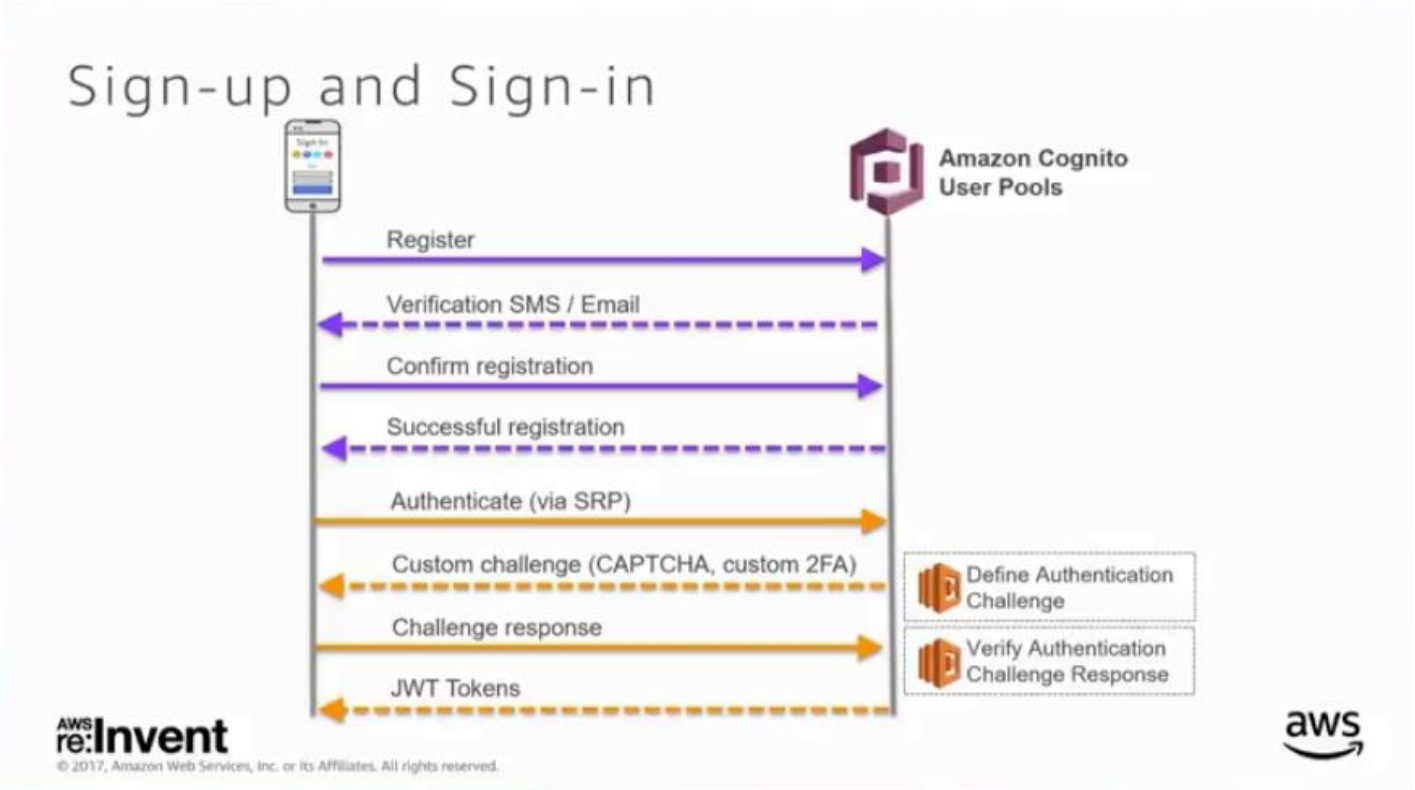
After a successful authentication, the cognito user pools service returns to you a set of JWT tokens.



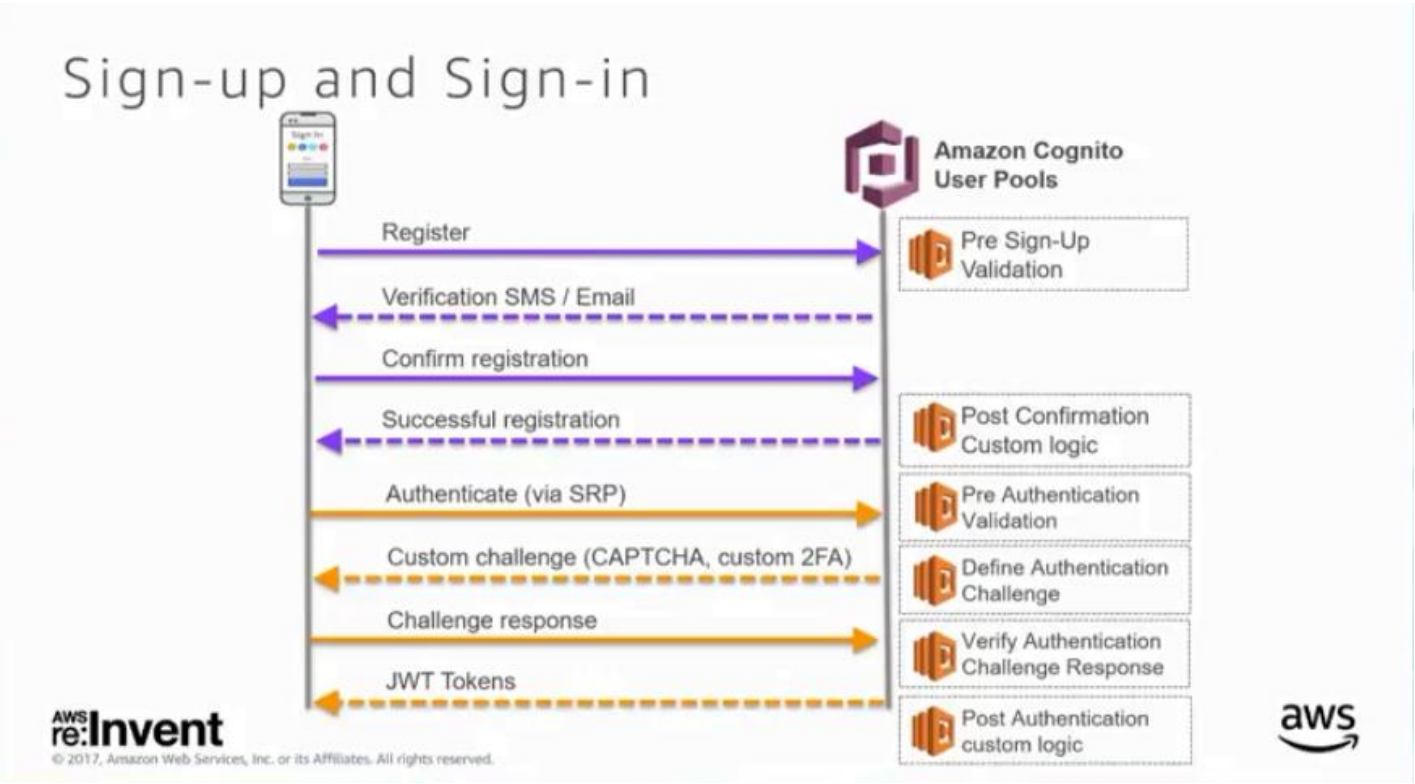
But you can also hook in and customize this authentication flow to suit your need like needing MFA option or using a CAPTHA.



You can define a custom challenge or trigger that you can hook into the workflow to generate that challenge for your users and send that challenge result back with a lambda function used to verify the challenge response.



Then you get the JWT back just as before



These are some of the available lambdas that you can hook in to customize the authentication flow.

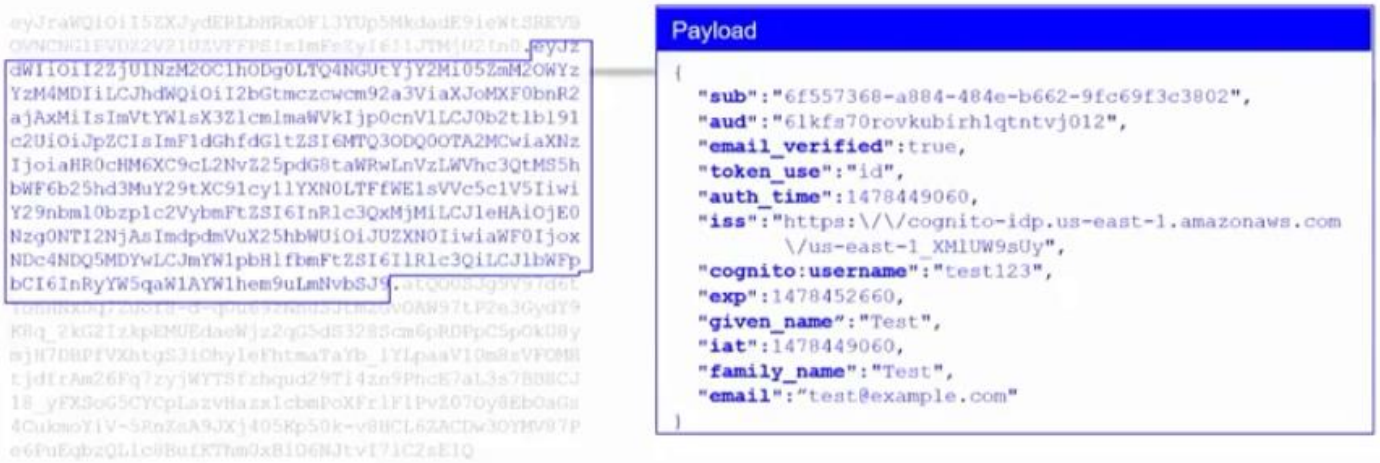
Sign-up and Sign-in

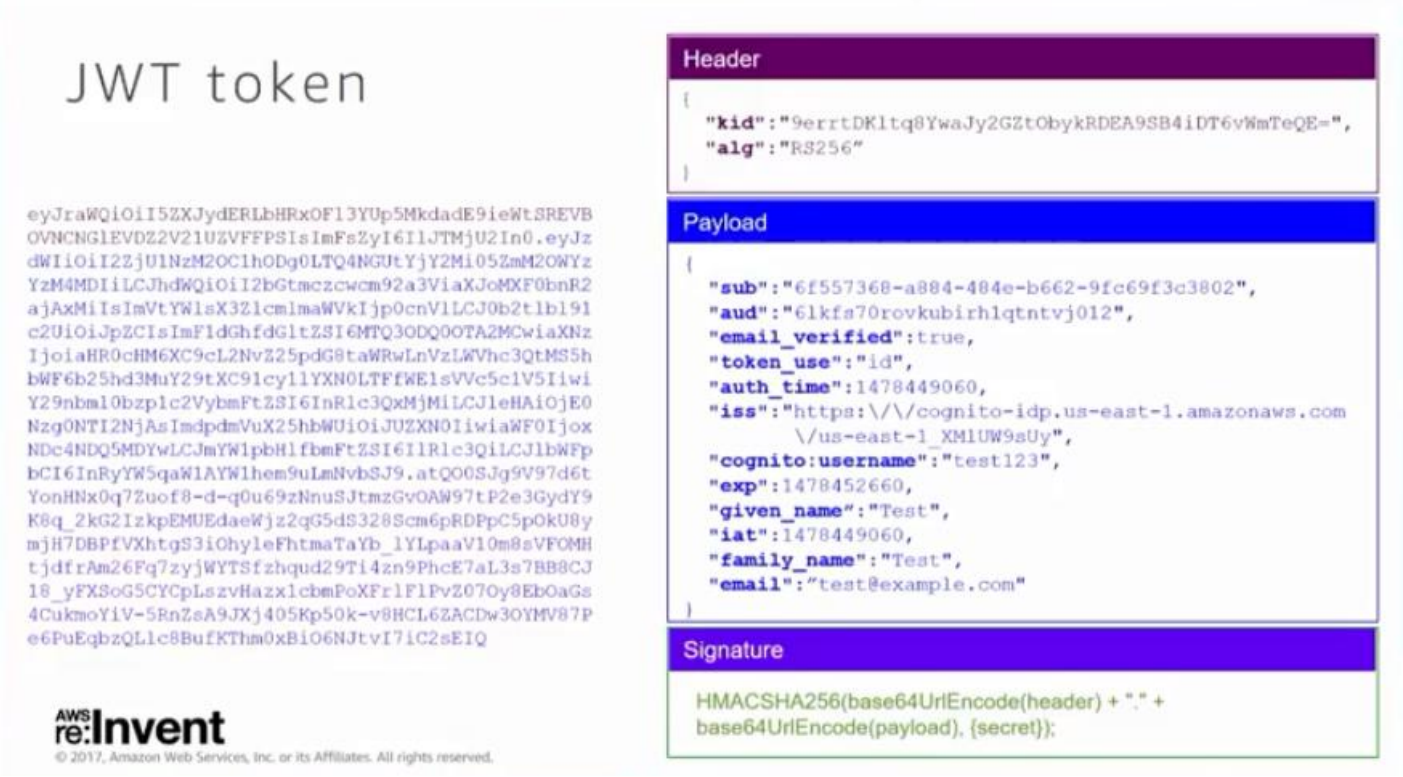
JWT token


```
eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cyllYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXNOIiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazxlcbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ
```

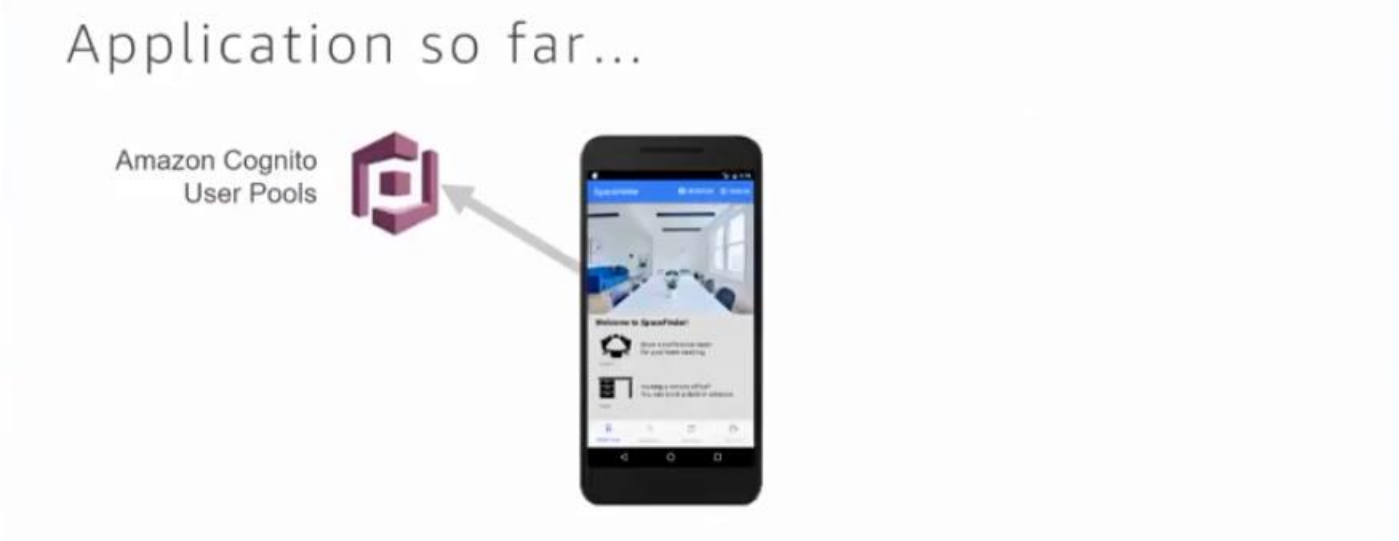
JWT token

JWT token





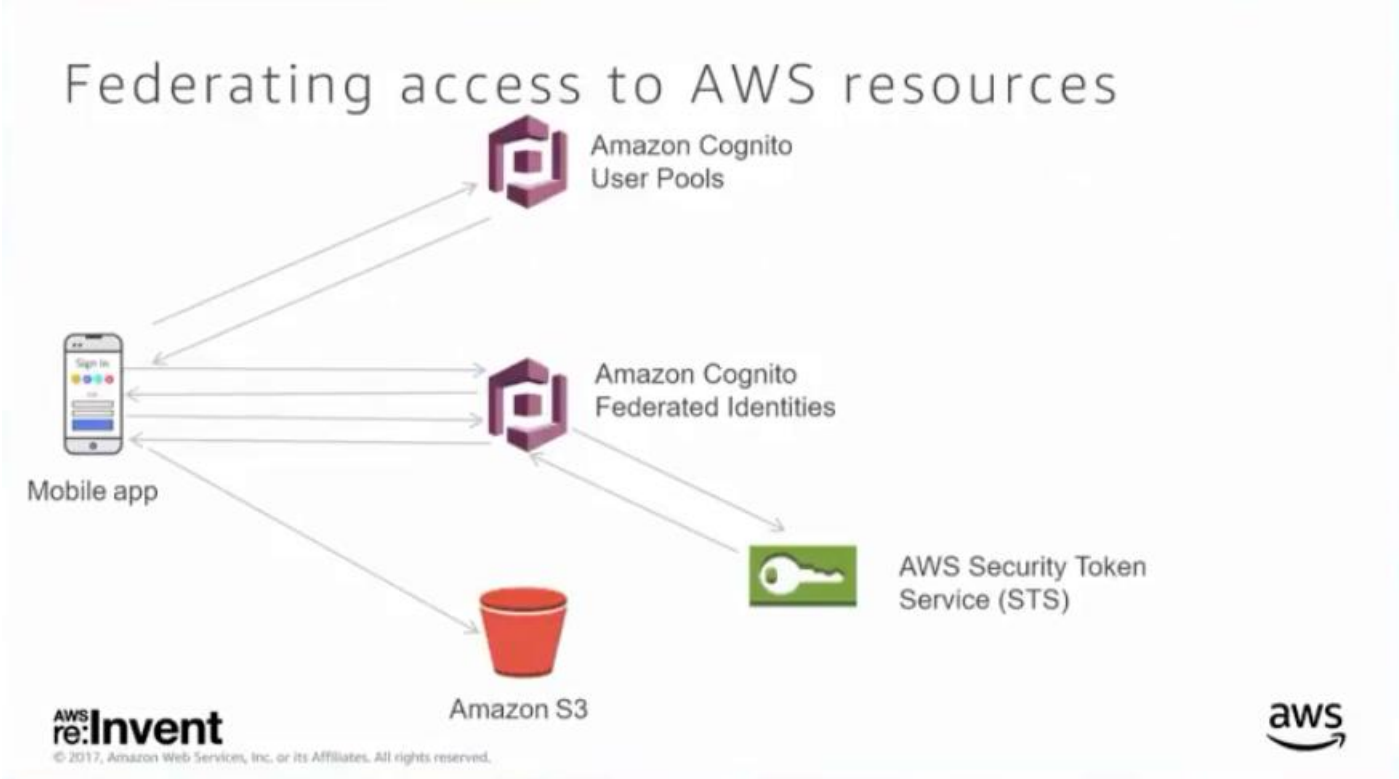
A JWT is a form of base64 encoded blob of text as an identity token with all the user details. There are 3 types of tokens you can get from the Cognito User Pools service, an Access token, Identity token, and a Refresh token. The access tokens are used to grant programmatic or API access to the user, the identity token shown above can be used for downstream or sudo-authentication for reading the claims of the user for dynamically changing the user's experience in your application using the token. The access and identity tokens are only good for 1 hour from the time they are issued, the refresh tokens can be configured to be valid for as long as 30 days. You can use a refresh token to get a new access and identity token.

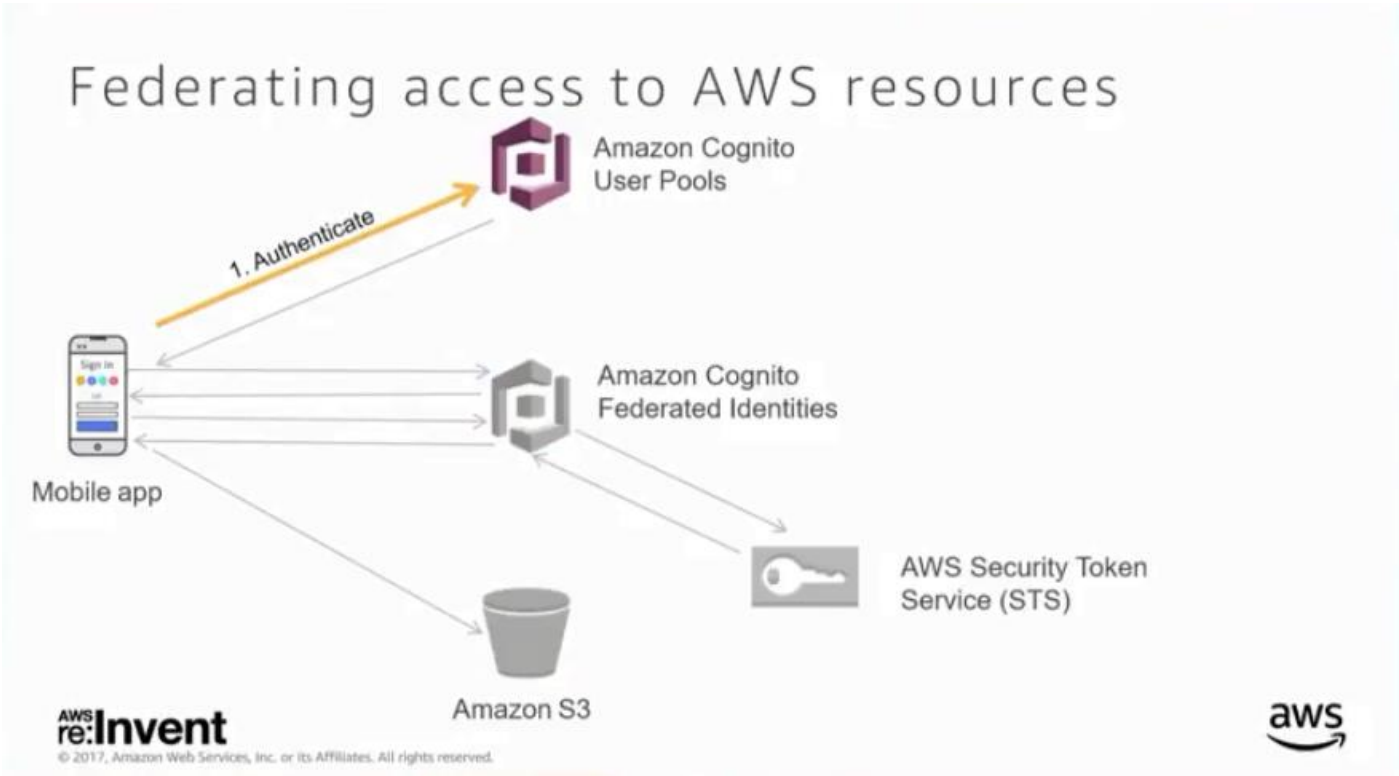


Now we have a way for our app where a user can sign in and sign out. What if they need to access AWS resources like S3 or DynamoDB.

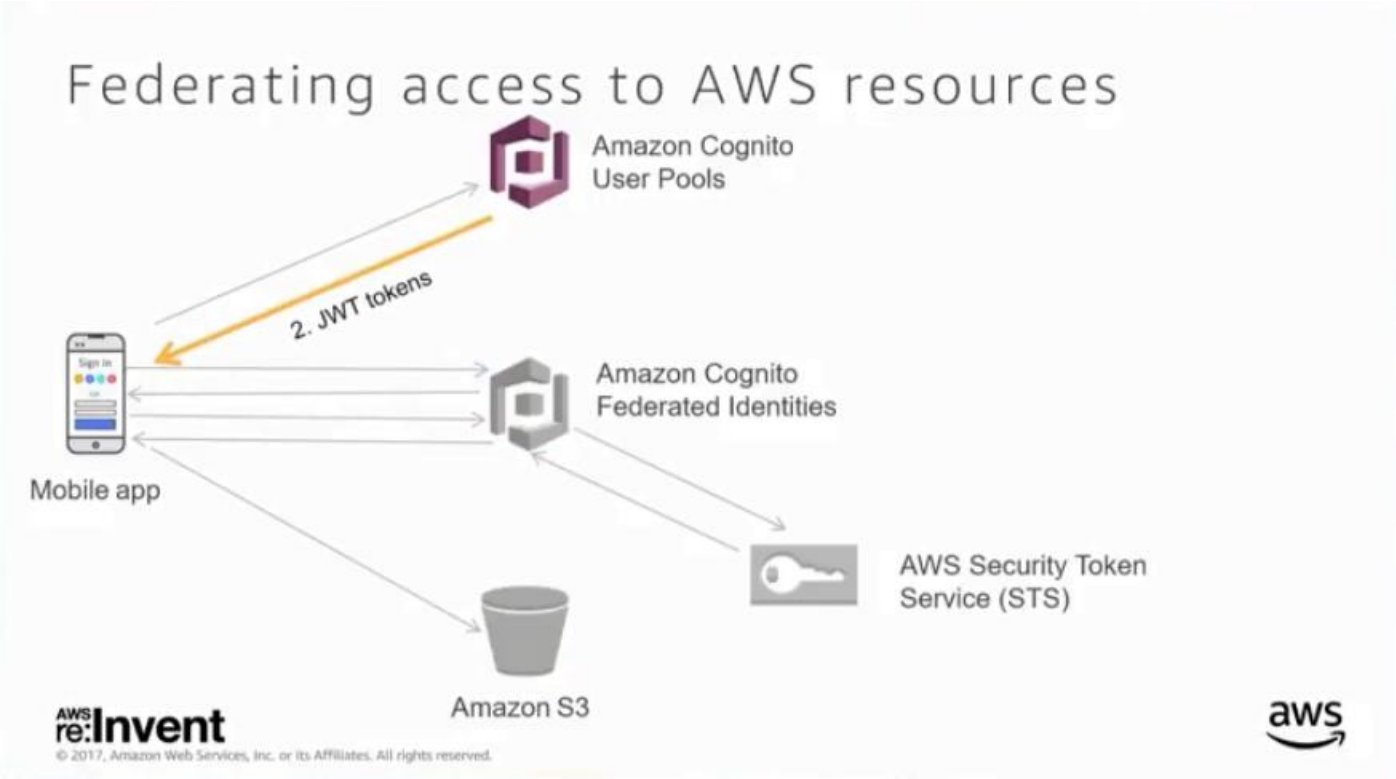
To give the user a secure, fine grain access to S3 we need something else.

The Amazon Cognito Federated Identites (CFI) allows you to exchange tokens from user pools or other bearer token based providers for AWS native credentials in the form of IAM Role.

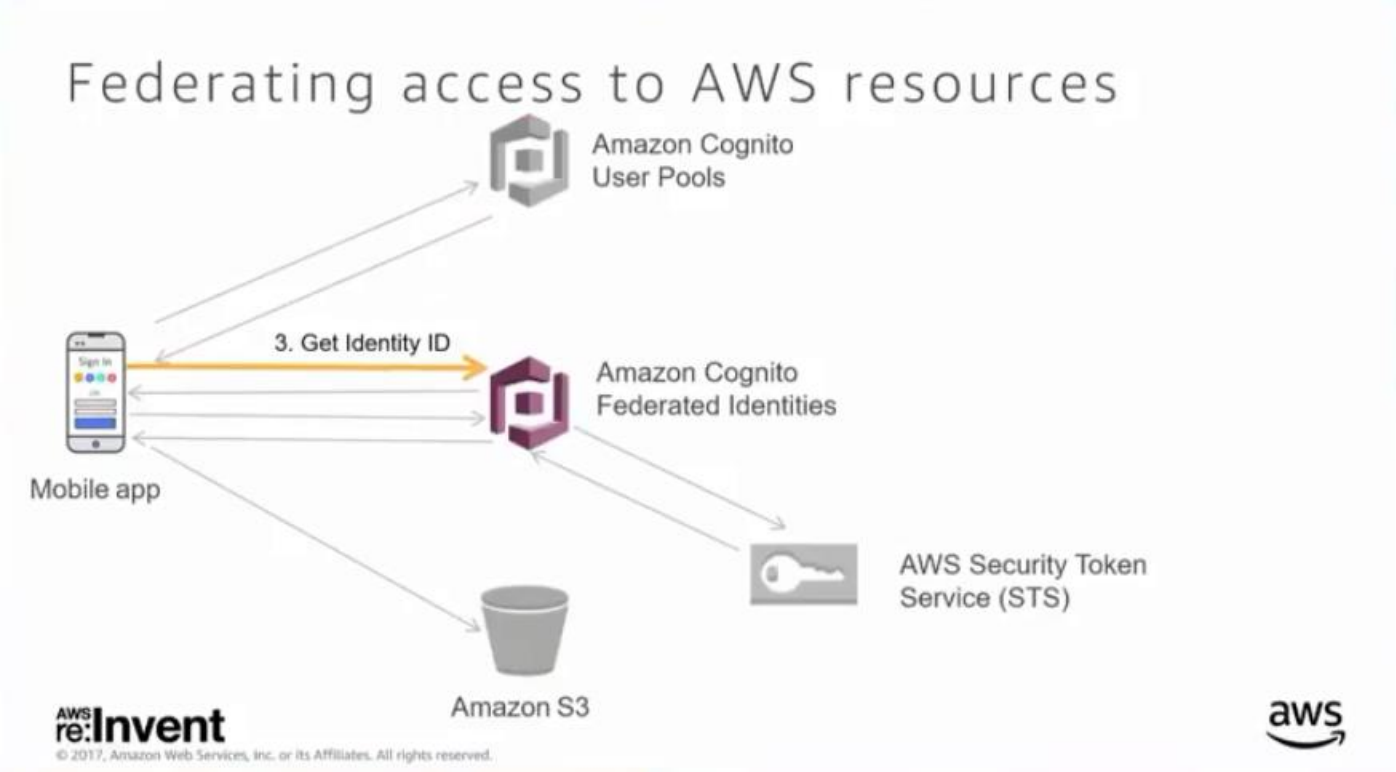




First you authenticate with Cognito User Pools

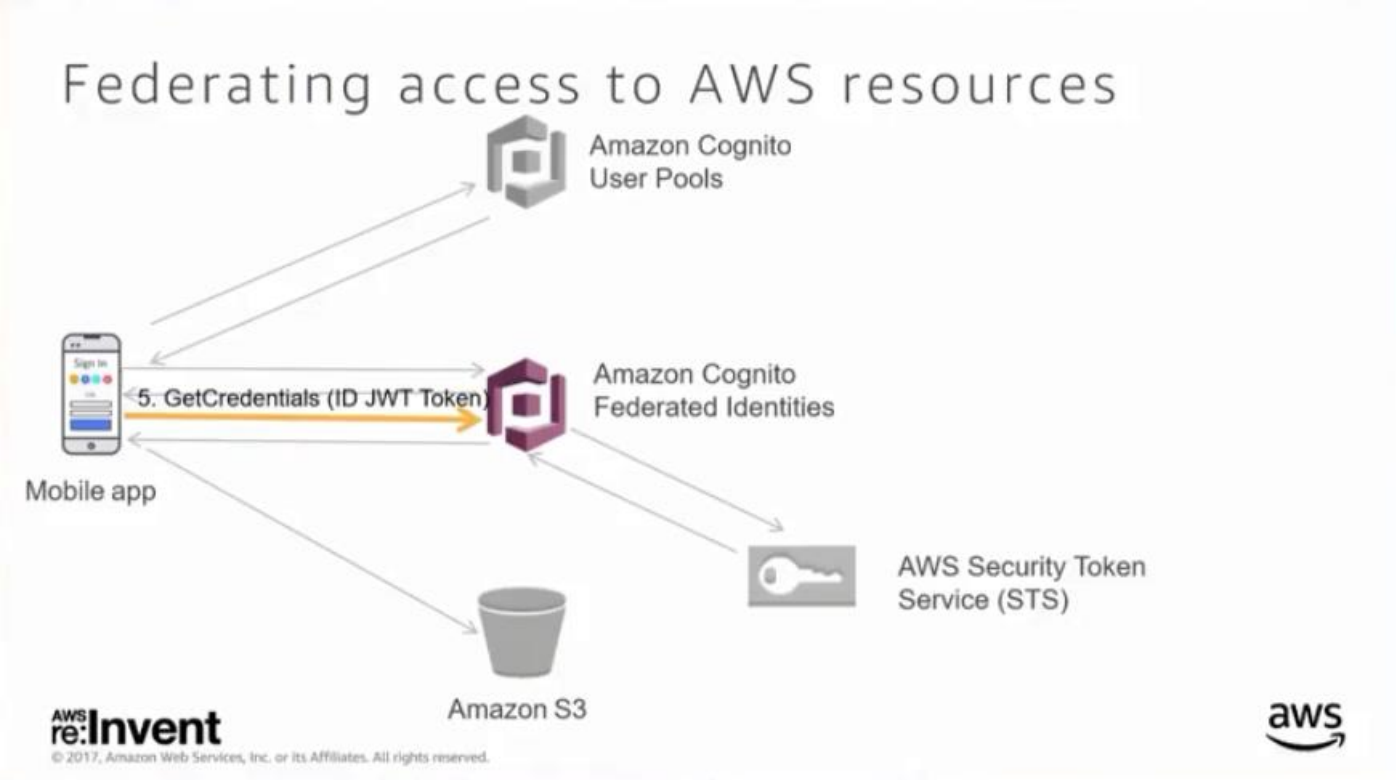


You get back a set of JWT tokens

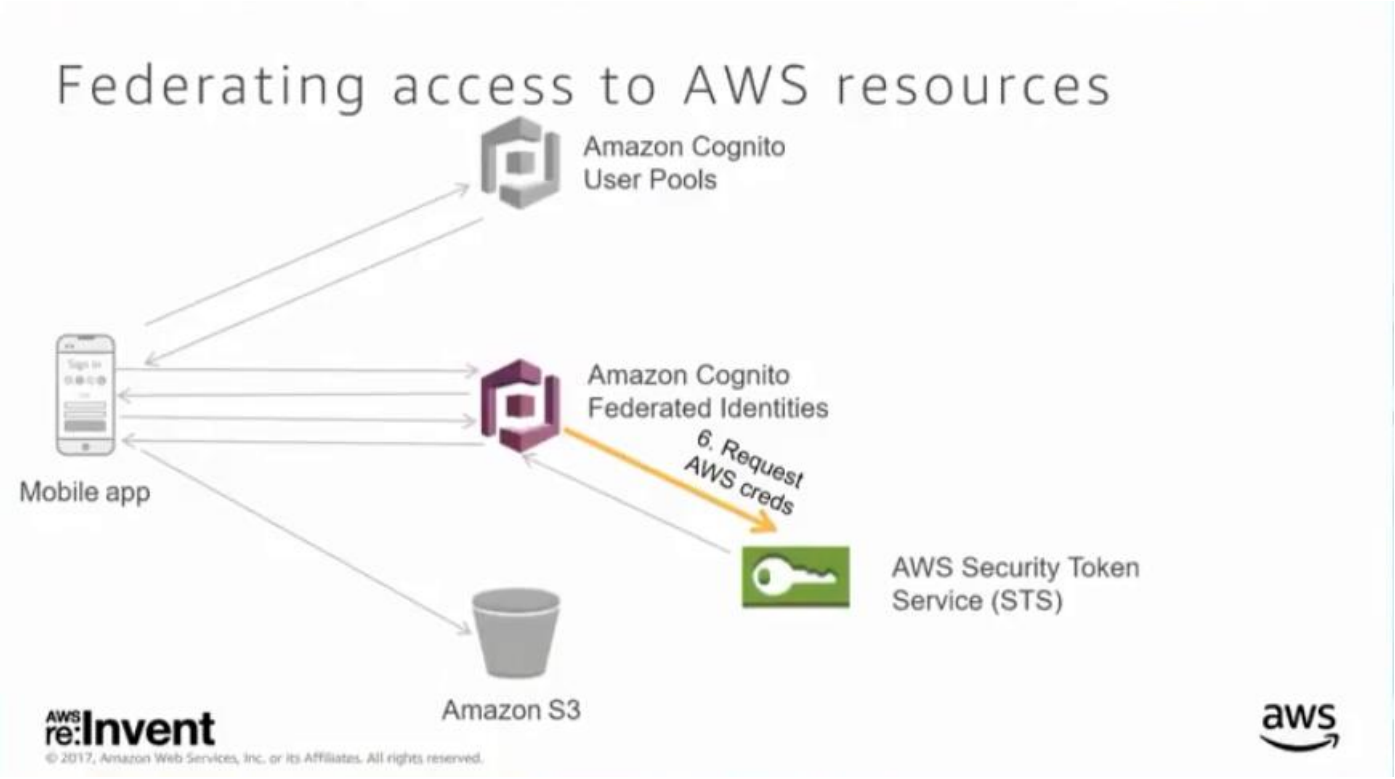


You then make a subsequent call to go ahead and pass the identity token to CFI,

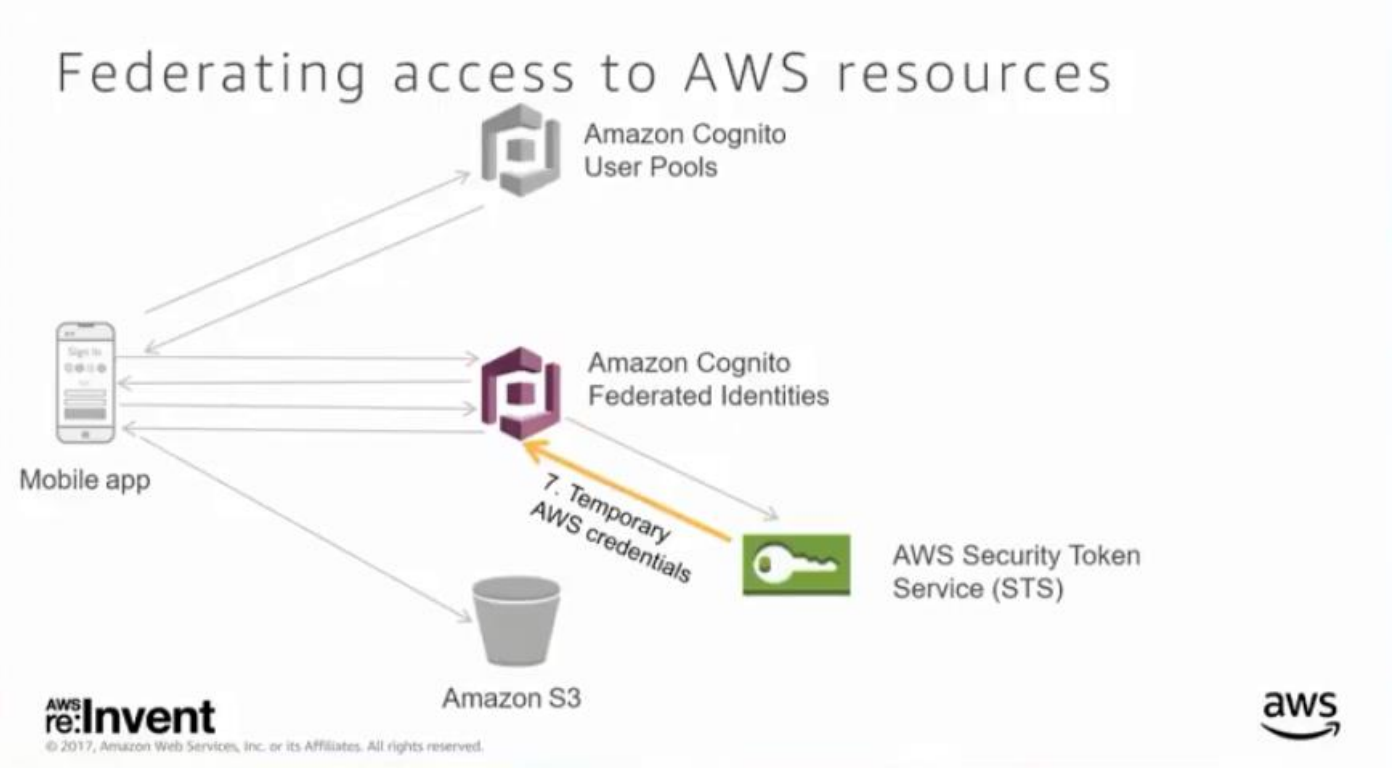
CFI will then return an Identity ID back to you.

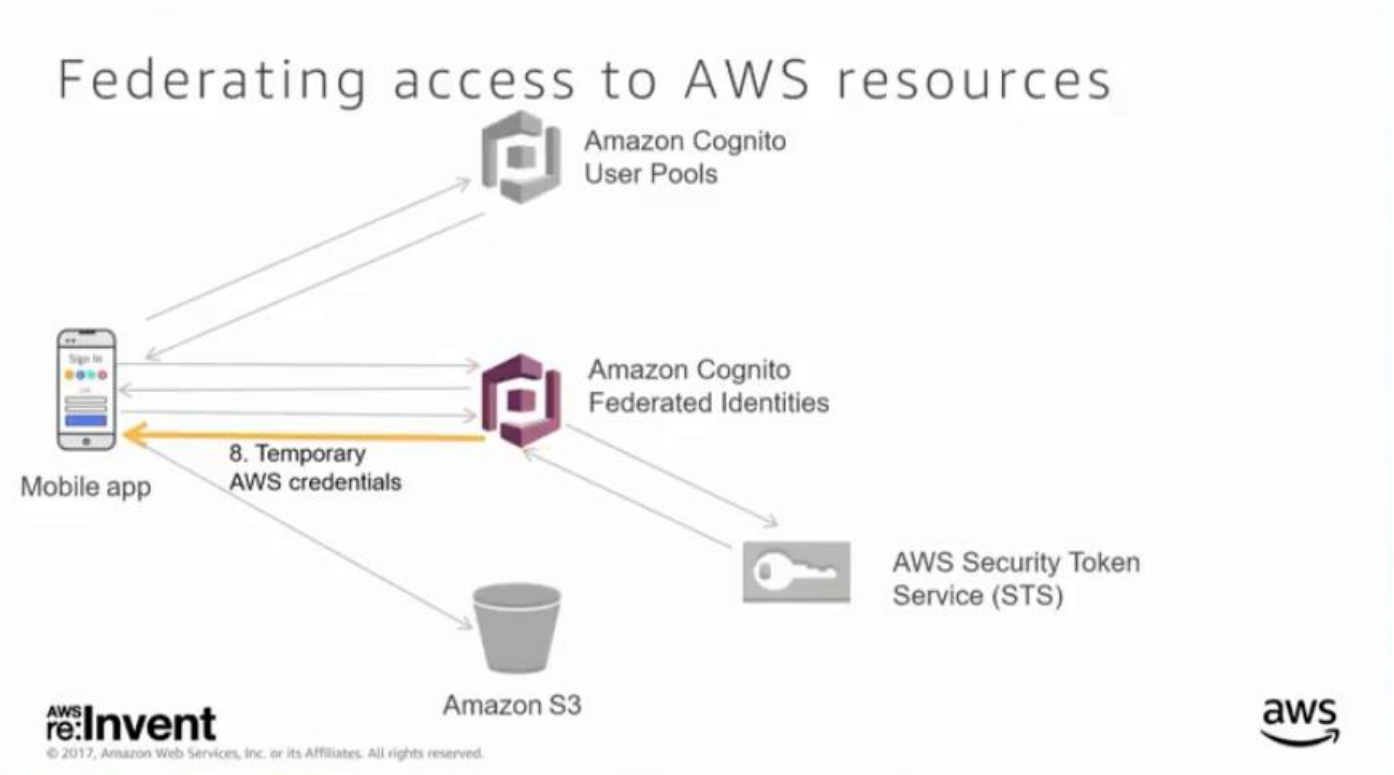


With the Identity ID and the JWT Identity Token, you can then call to the GetCredentials request as above

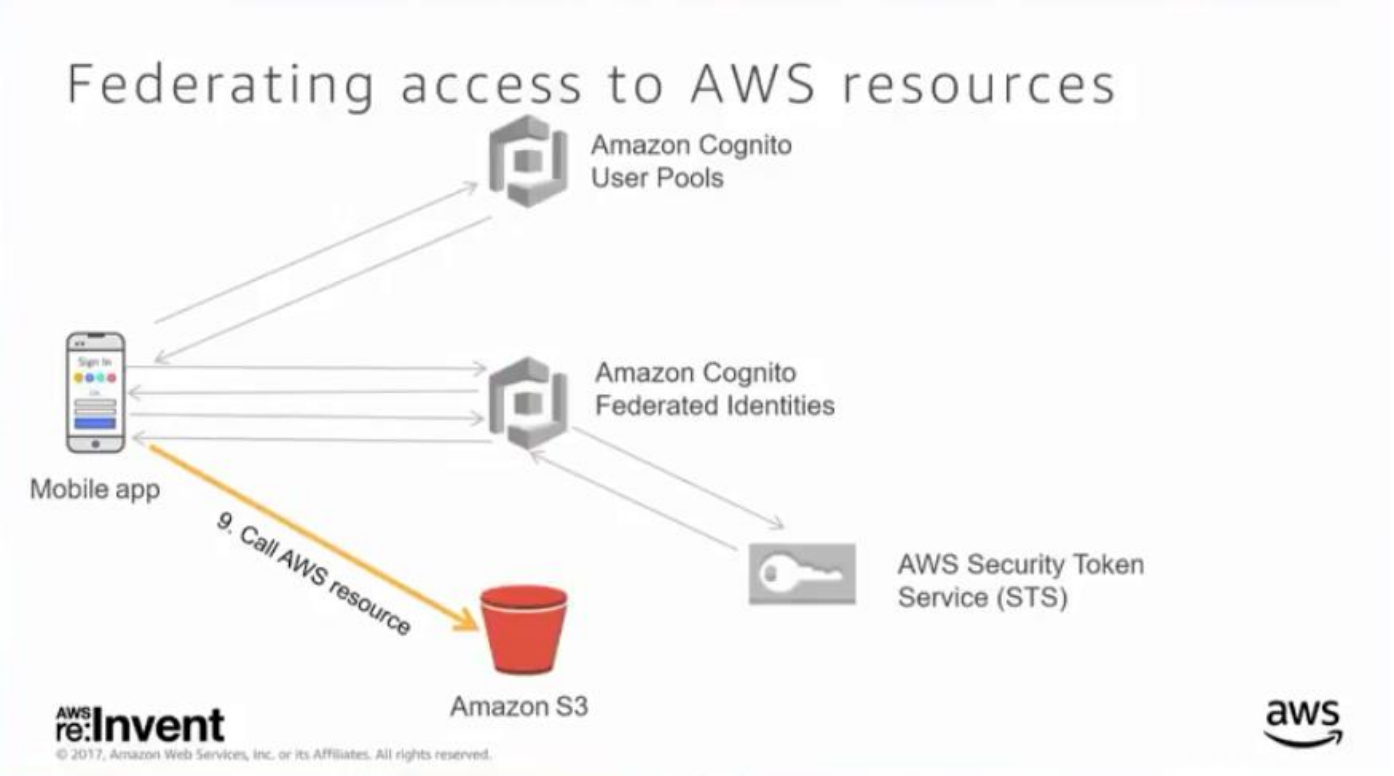


Cognito then goes to the AWS Security Token Service (STS) that will generate the particular IAM credentials for that role





Cognito then returns the IAM credentials back to the user in the form of an ***IAM Role containing an access key, secret access key, and a session token***.



Once you have the IAM Role credentials, you can then go ahead and use any AWS SDK from any language to interact with those AWS Resources like S3, DynamoDB, API Gateway, etc.

"What AWS permissions will those users have?"

"How do I give different users different AWS permissions?"

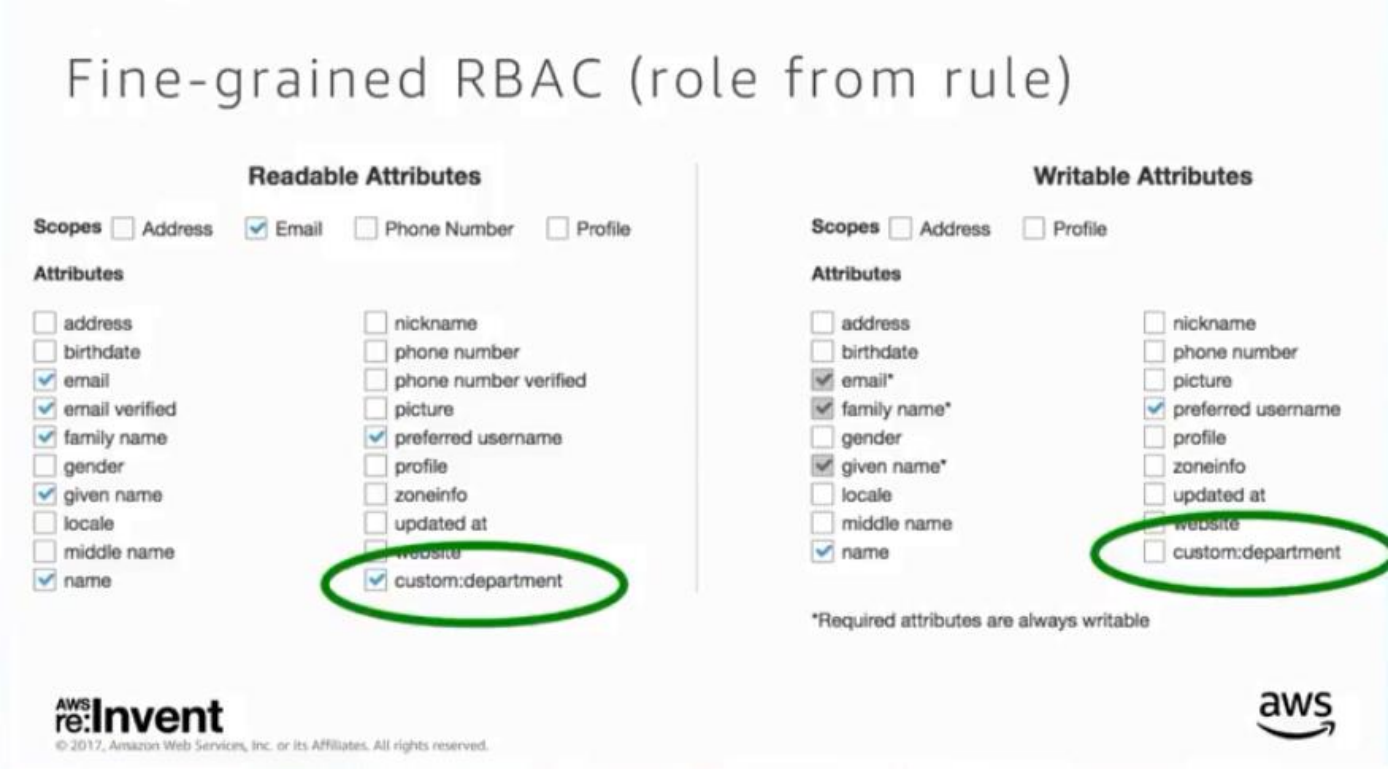
Fine-grained Role-Based Access Control

Unauthenticated users:

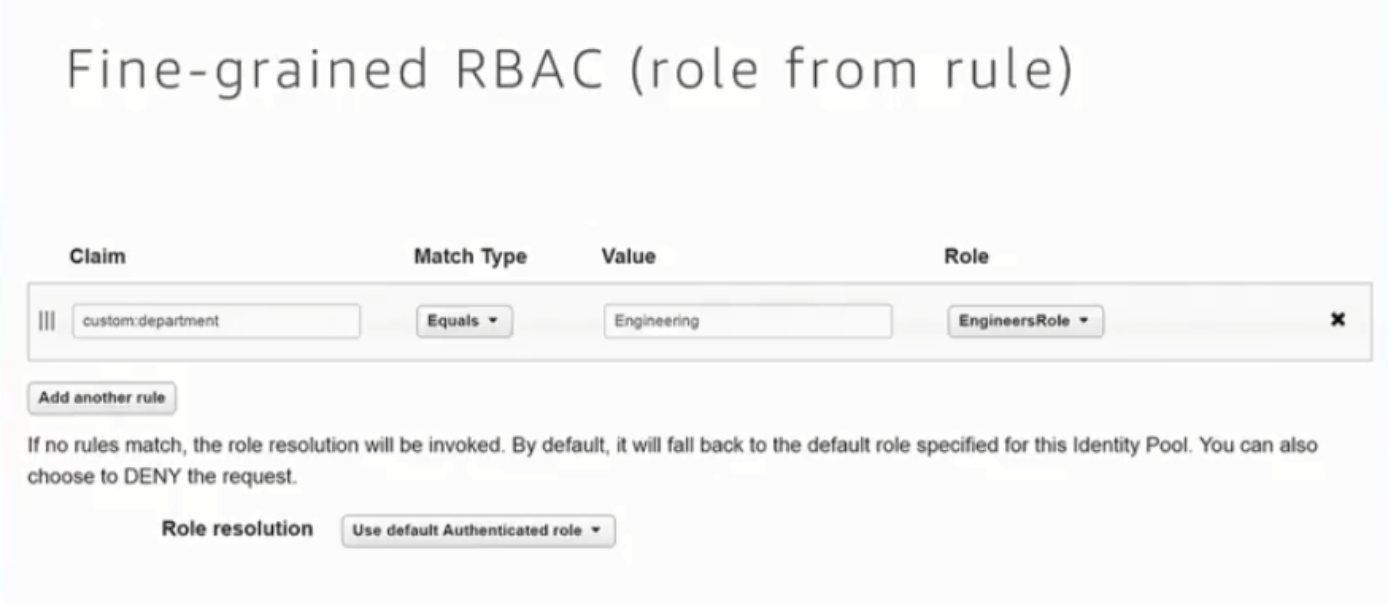
- Default role

Authenticated users

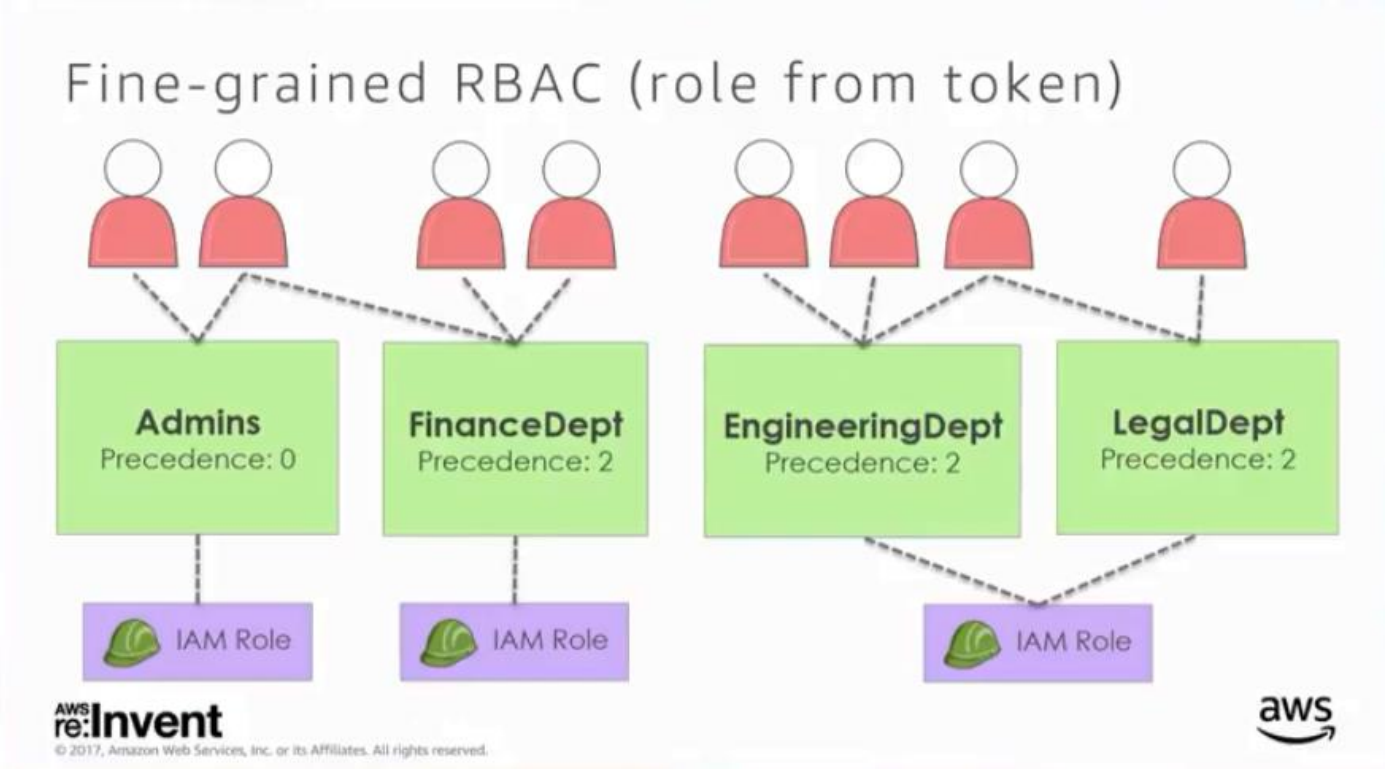
- Default role
- Choose role from rule
- Choose role from token



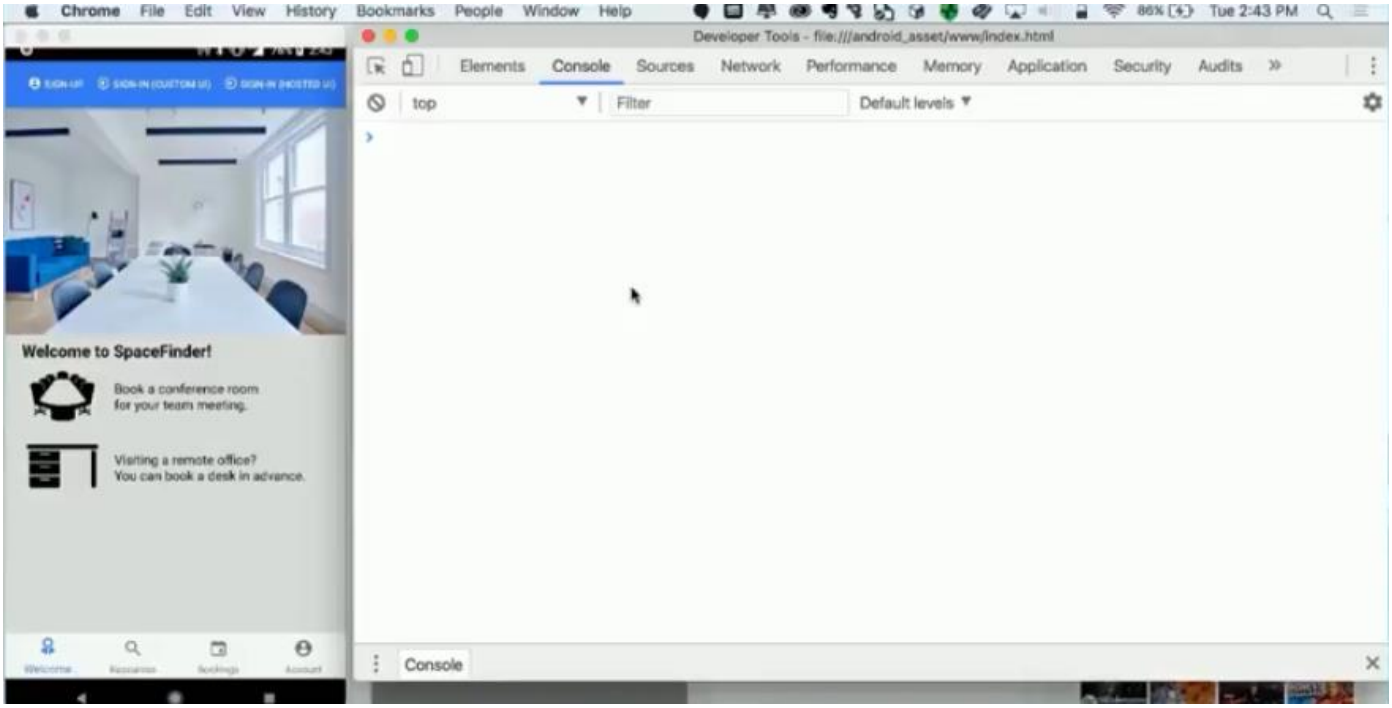
In your user pool, you can define different attributes like a department attribute above. You can then make a set of rules based on the attributes as below



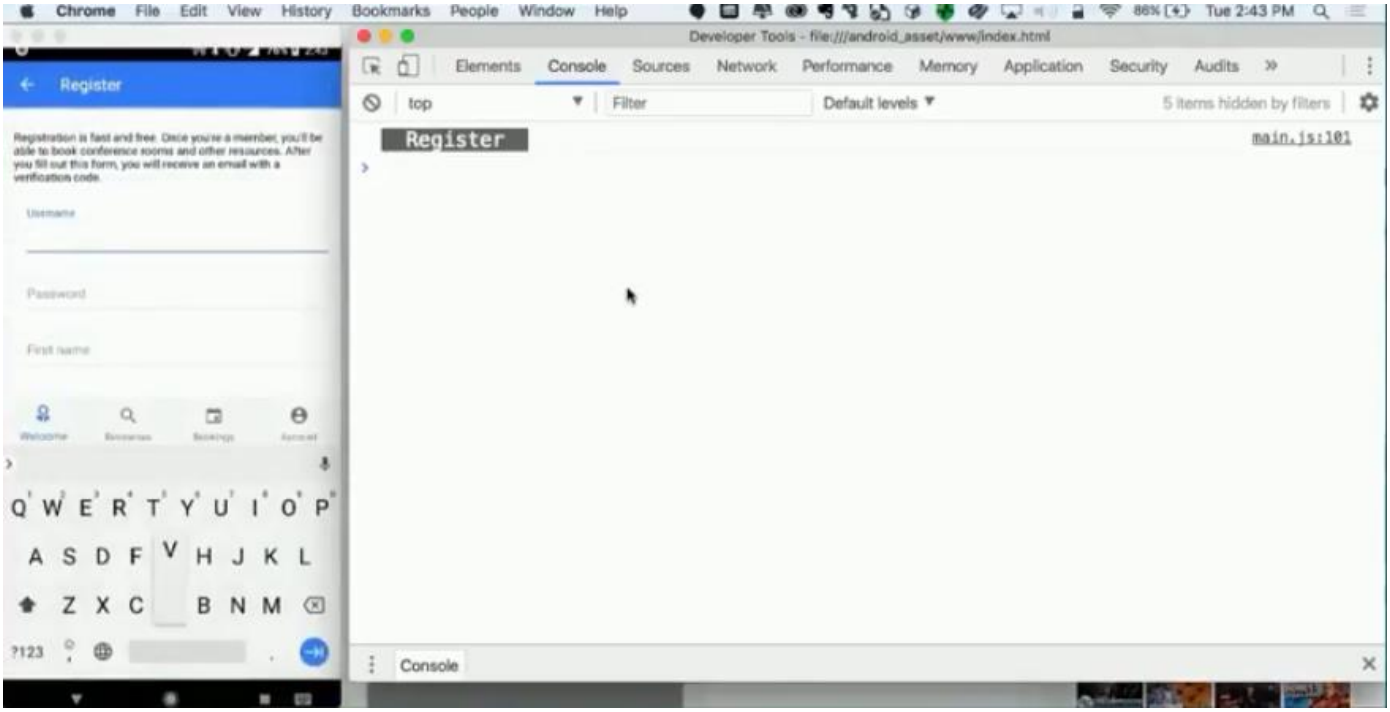
In this case we are parsing the department and if someone is a member of the engineering department, we give them the engineers role. You can define 1 or more rules that will be processed in a sequential order and the first matching role will be the effective role the user gets. ***If you have a user that does not match any of the rules, you can decide to deny access to them or give them the default unauthenticated role***.

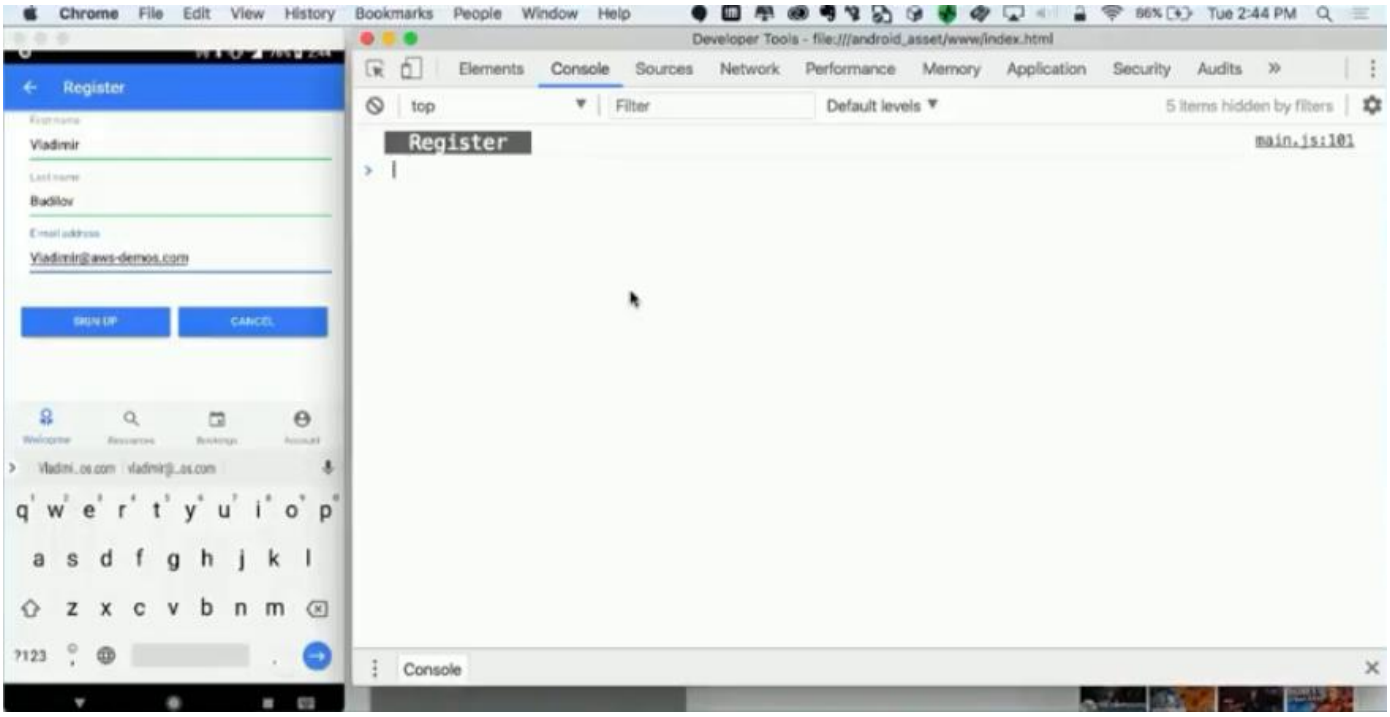


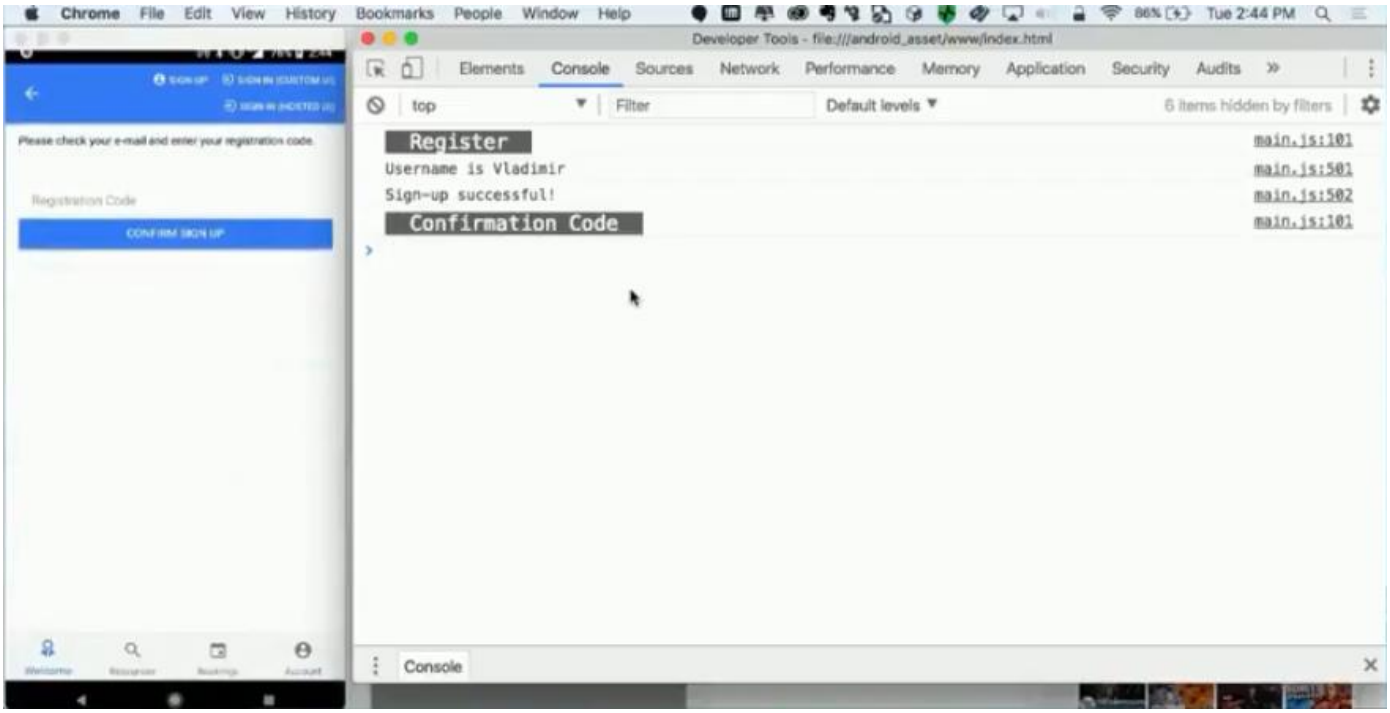
Using Cognito groups functionality, you are able to define different roles for different groups of users. A user can be in more than 1 group. With each group, you can specify an IAM Role for each group and a precedence tag. The user gets the group with the highest precedence tag if they belong to multiple groups since a user can only have 1 IAM role at any time. Cognito will then issue the appropriate token for a group dynamically.



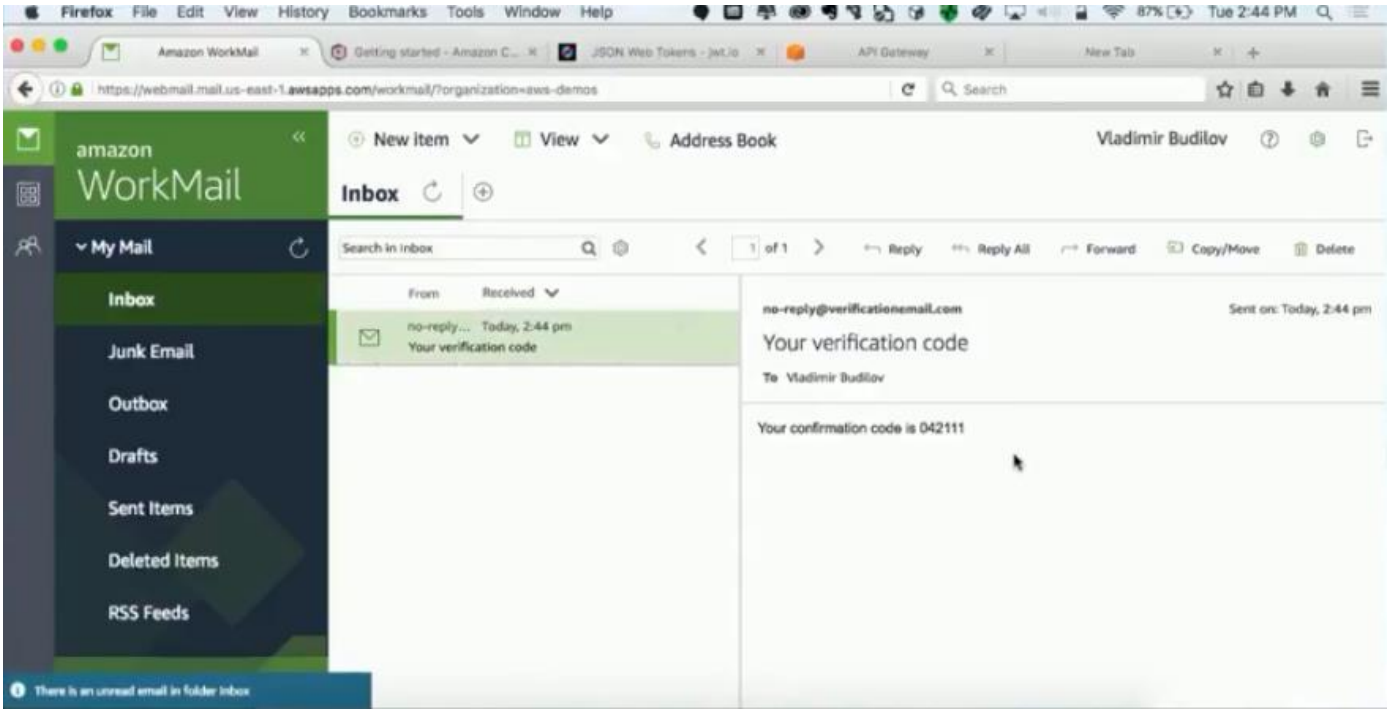
Let us start by signing up while we watch the logs that are generated

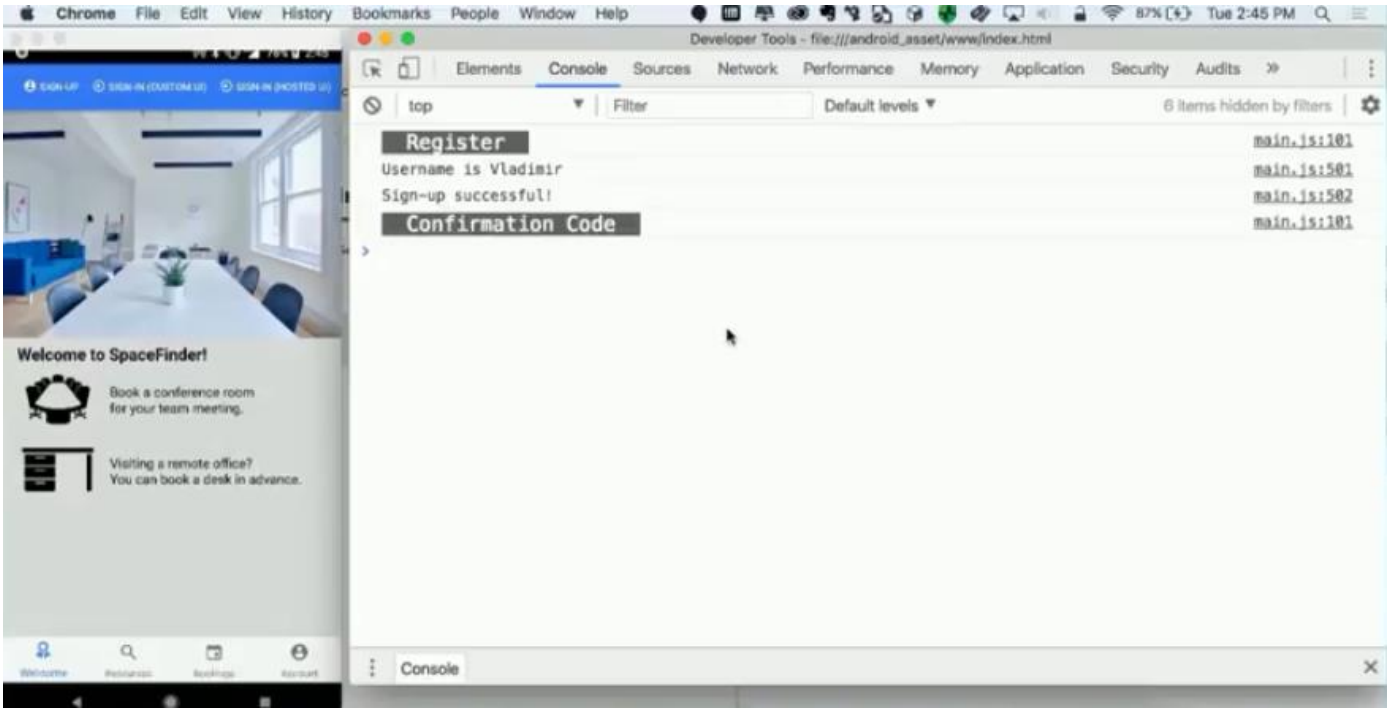




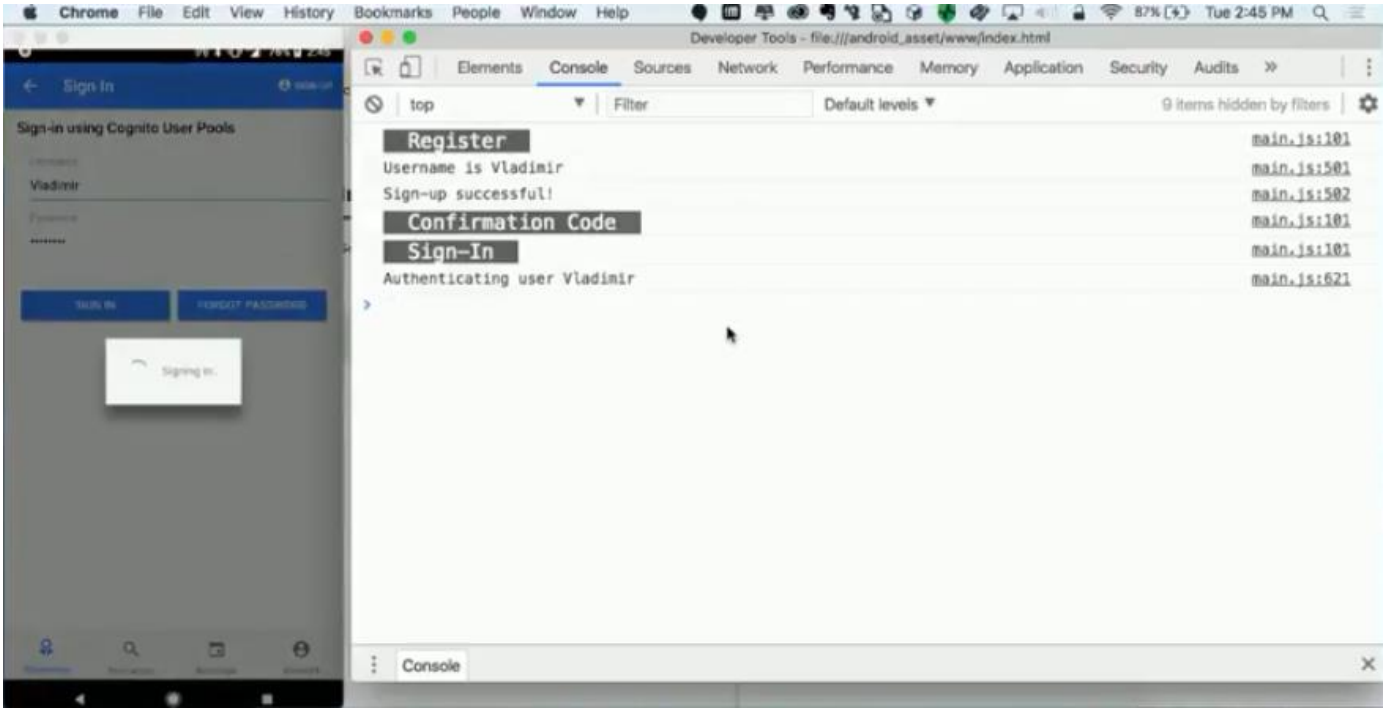


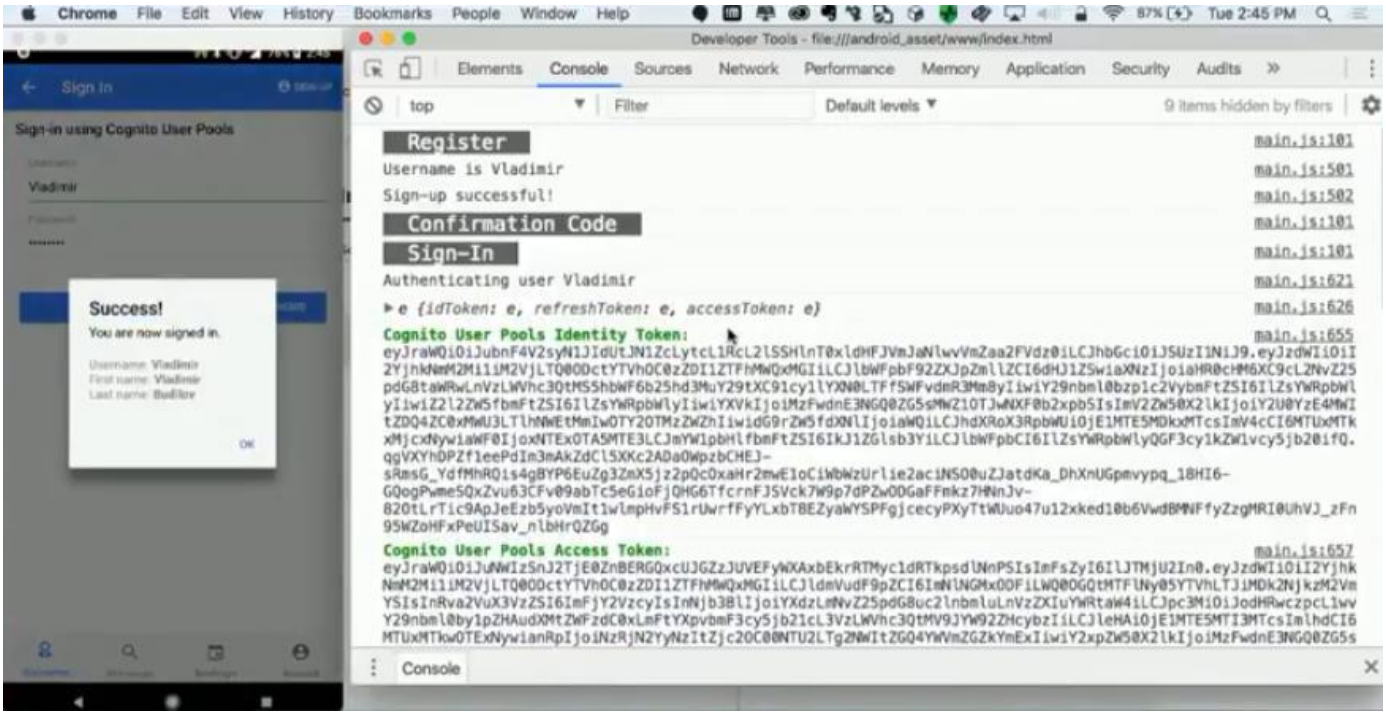
When I clicked the Register button, Cognito will sign me up but I am not confirmed yet. What is going to happen is that Cognito will send us a confirmation email to our email address with the code to confirm with.

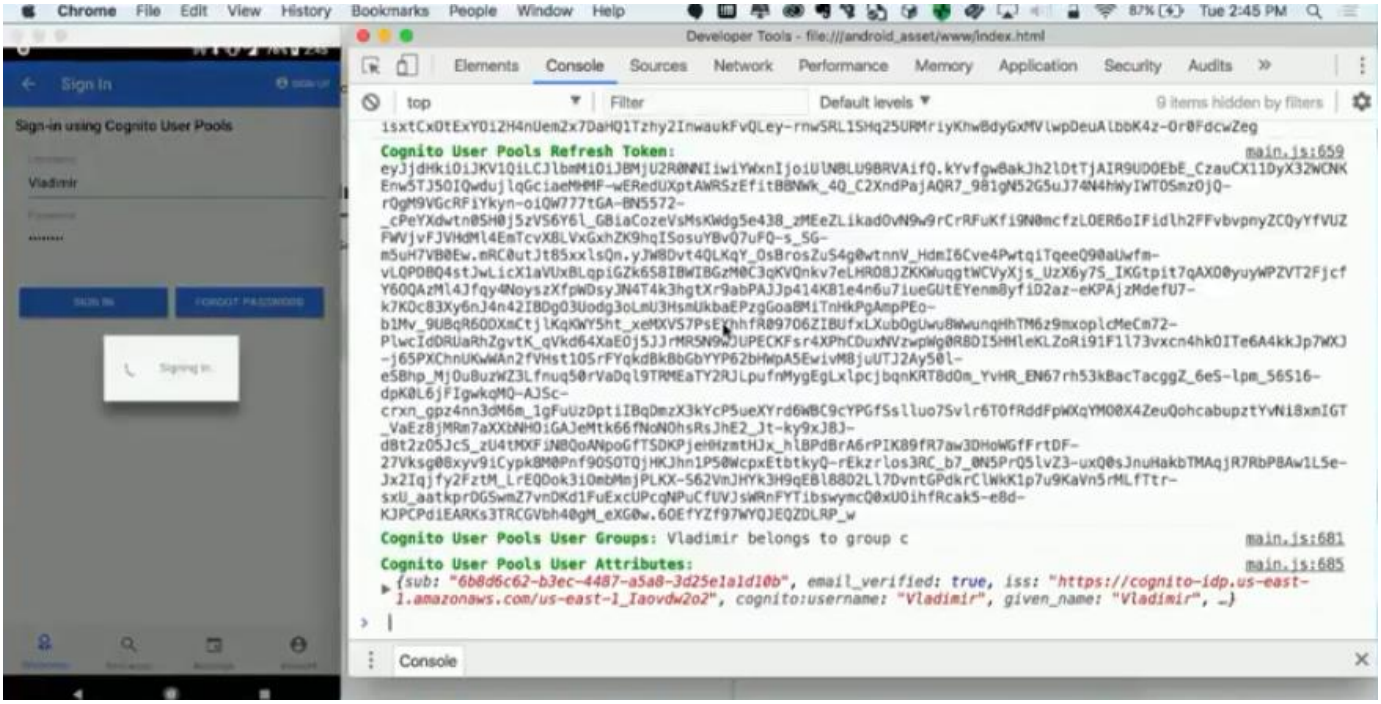


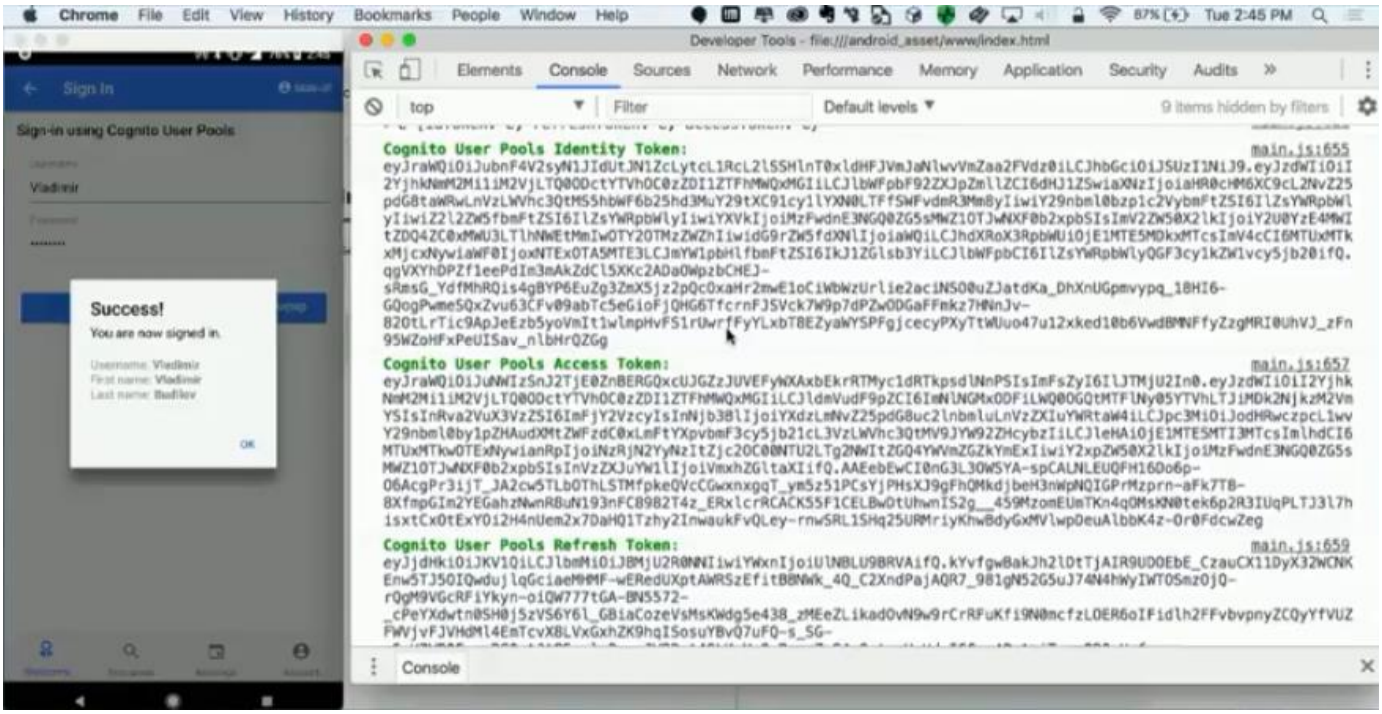


We can now use that confirmation code to get confirmed. Then we can sign into the application with our username and password.

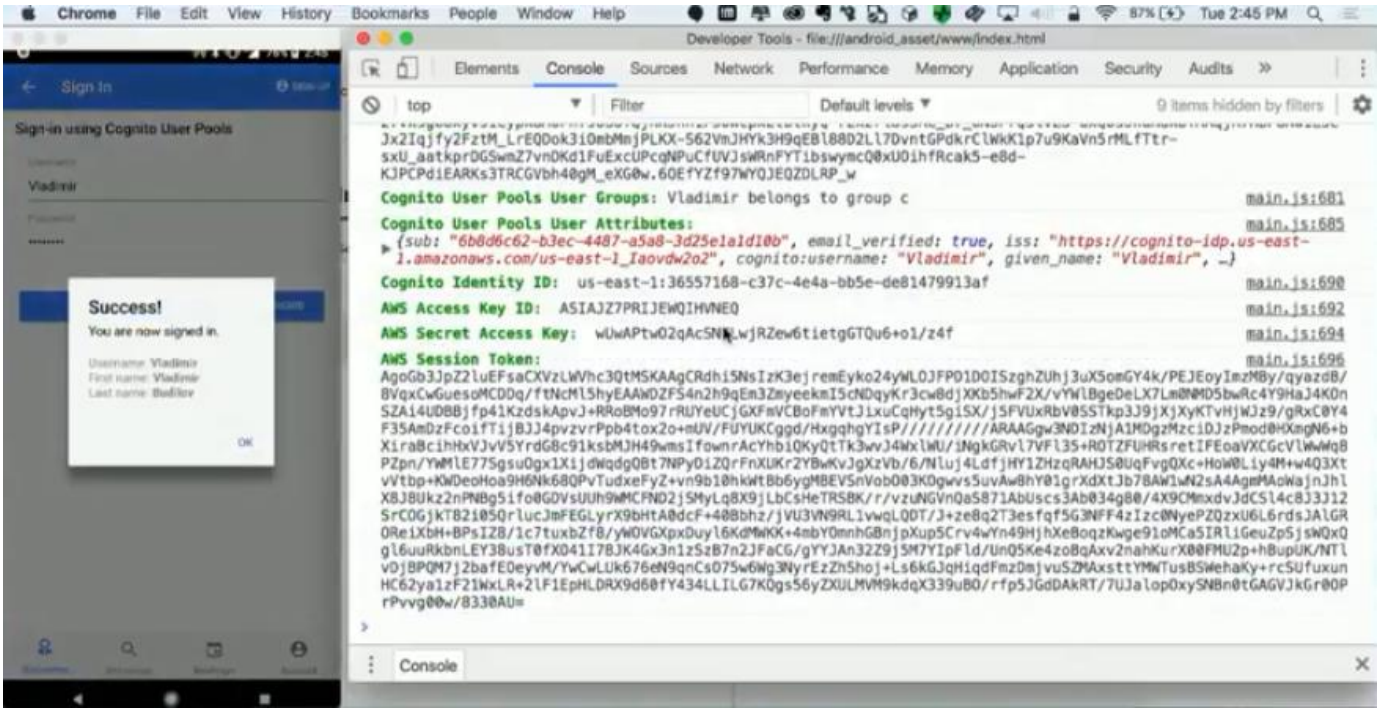

Chrome File Edit View History Bookmarks People Window Help
87% Tue 2:45 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
9 items hidden by filters
Sign In
Sign-in using Cognito User Pools
Vladimir
Register
Username is Vladimir
Sign-up successful!
Confirmation Code
Sign-In
Authenticating user Vladimir
main.js:101
main.js:501
main.js:502
main.js:101
main.js:101
main.js:621
Console


Chrome File Edit View History Bookmarks People Window Help
87% Tue 2:45 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
9 items hidden by filters
Sign In
Sign-in using Cognito User Pools
Vladimir
Success!
You are now signed in.
OK
Register
Username is Vladimir
Sign-up successful!
Confirmation Code
Sign-In
Authenticating user Vladimir
main.js:101
main.js:501
main.js:502
main.js:101
main.js:101
main.js:621
main.js:626
Cognito User Pools Identity Token:
main.js:655
Cognito User Pools Access Token:
main.js:657
Console

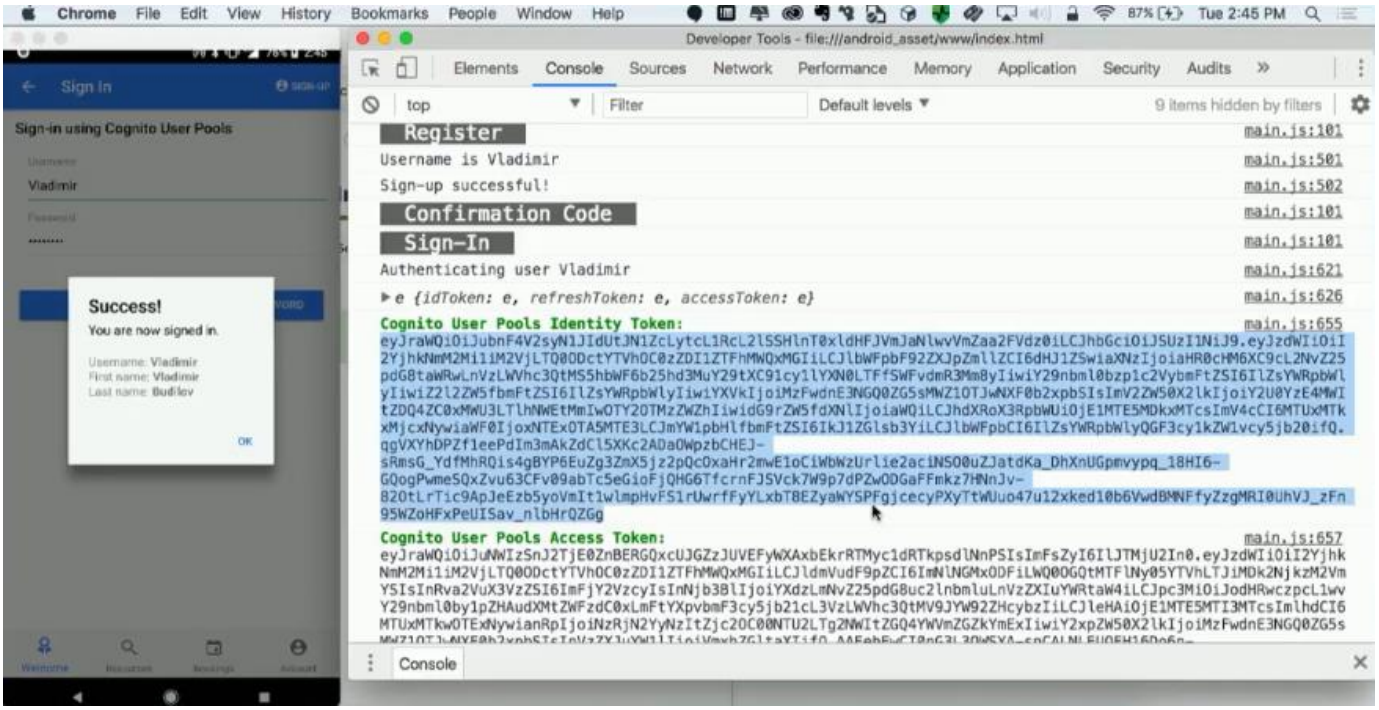


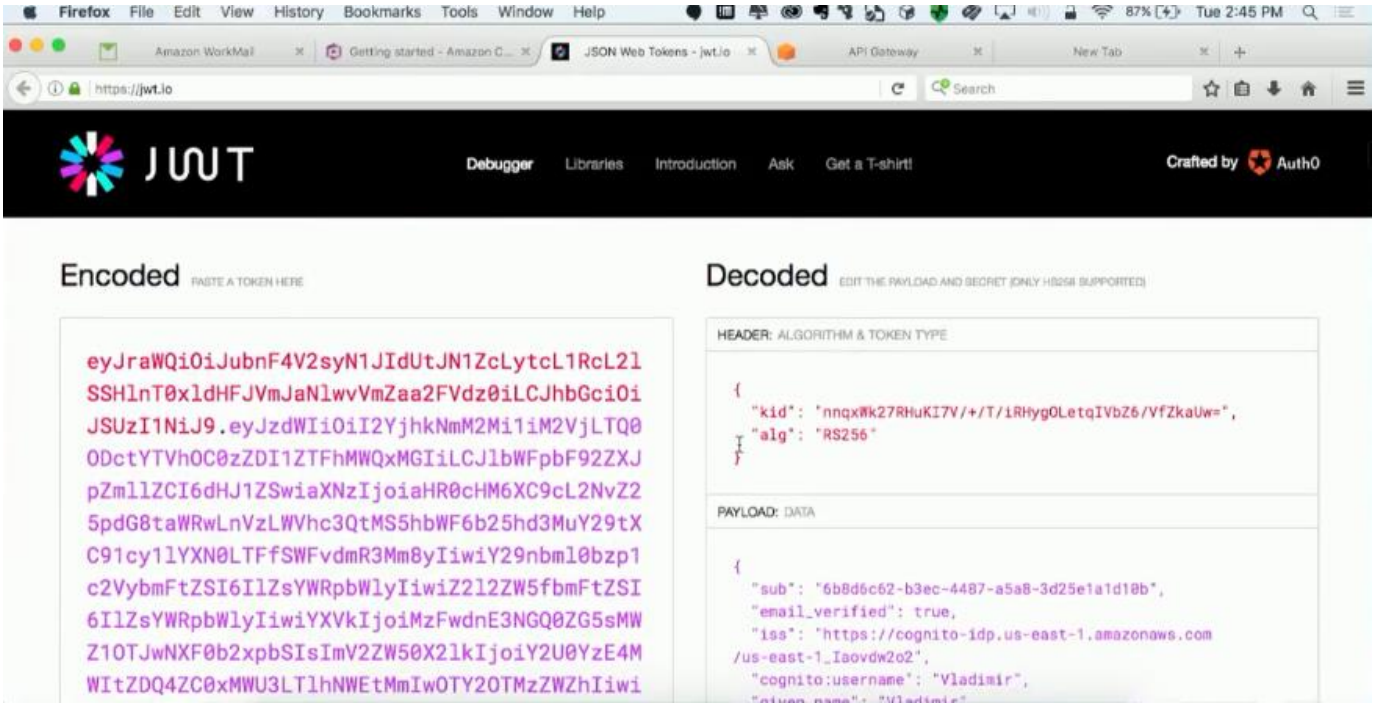


The 3 JWT tokens we mentioned earlier are printed out above

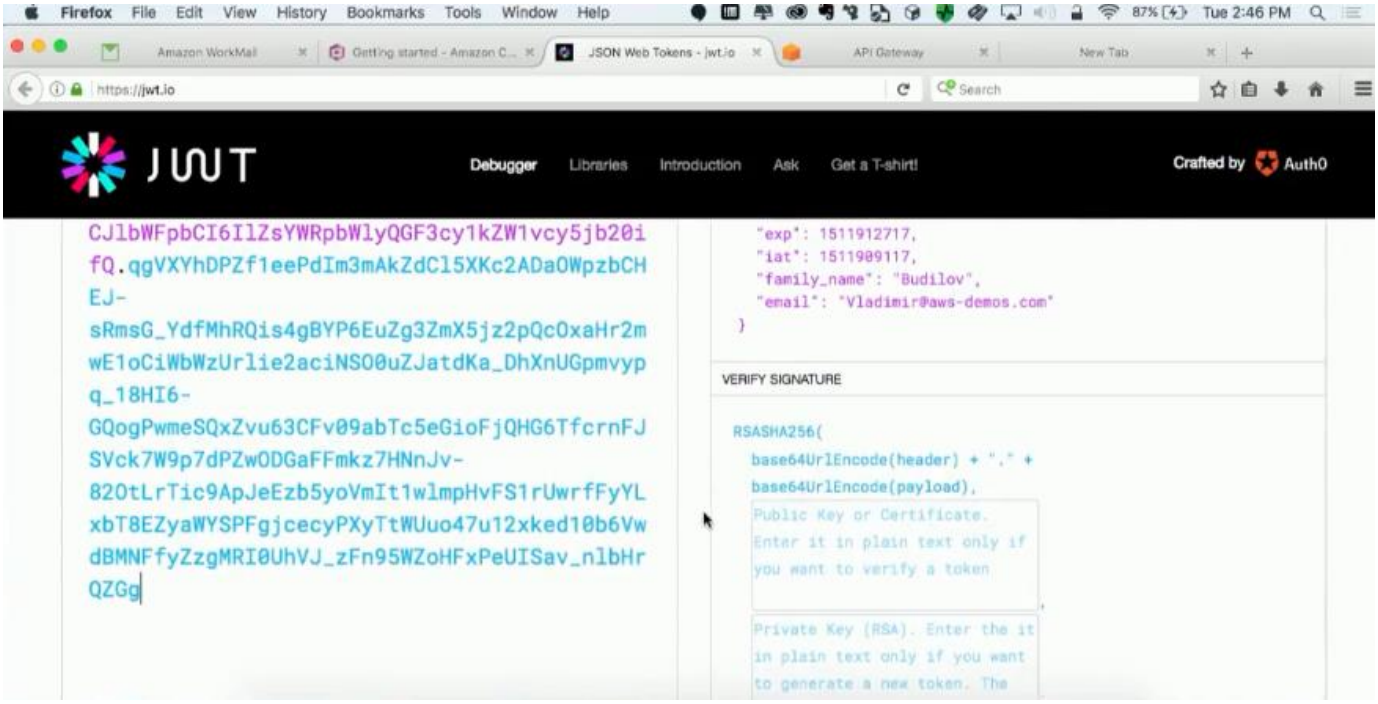


And the IAM role access credentials that are vended by STS is shown above

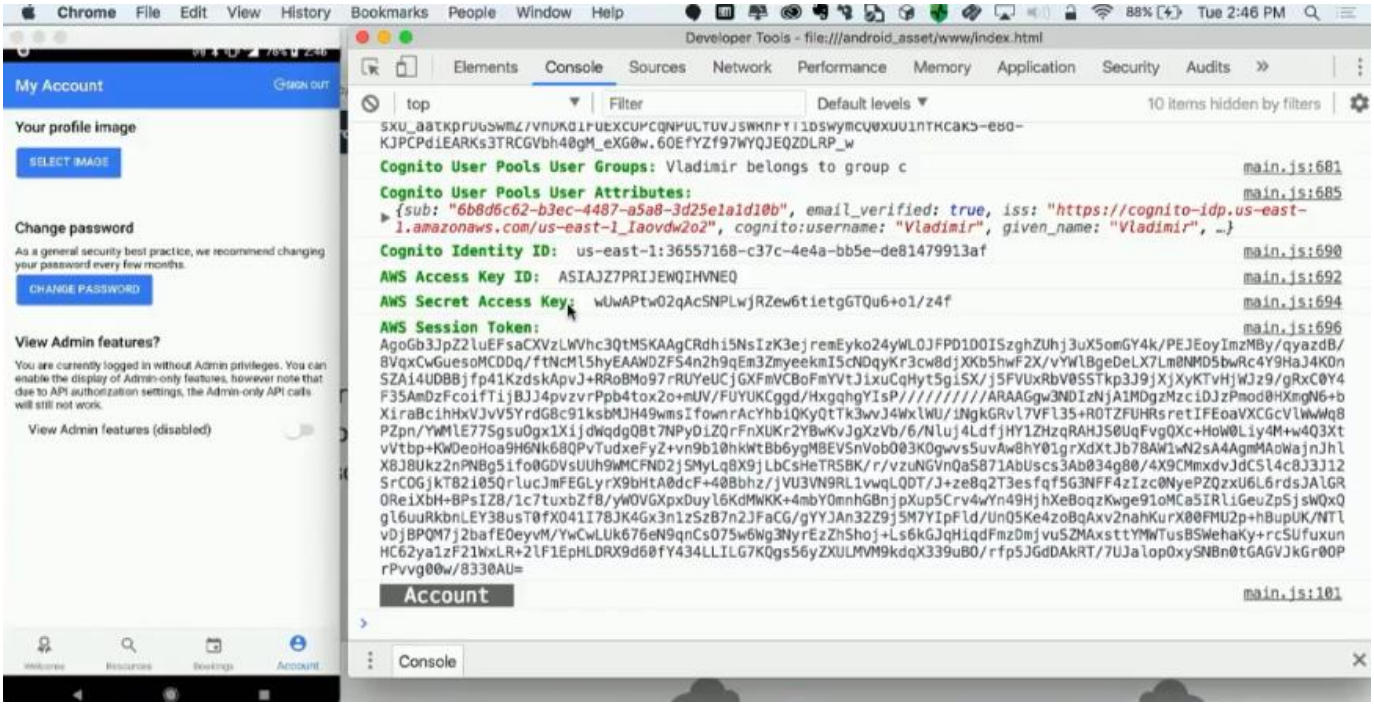




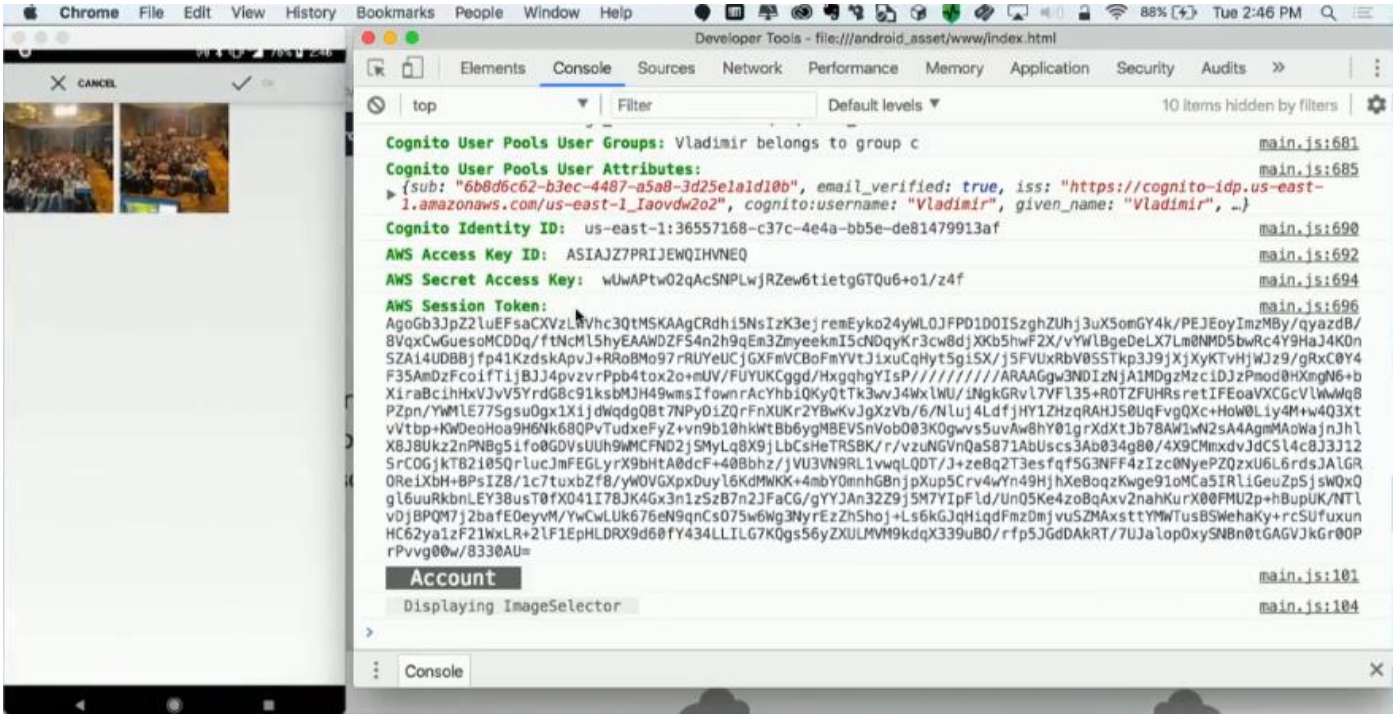
The payload in the JWT contains all the information that the user entered, we can use these details to perform authorization within the application to grant access to certain resources or not as well as in our downstream services for further customization.

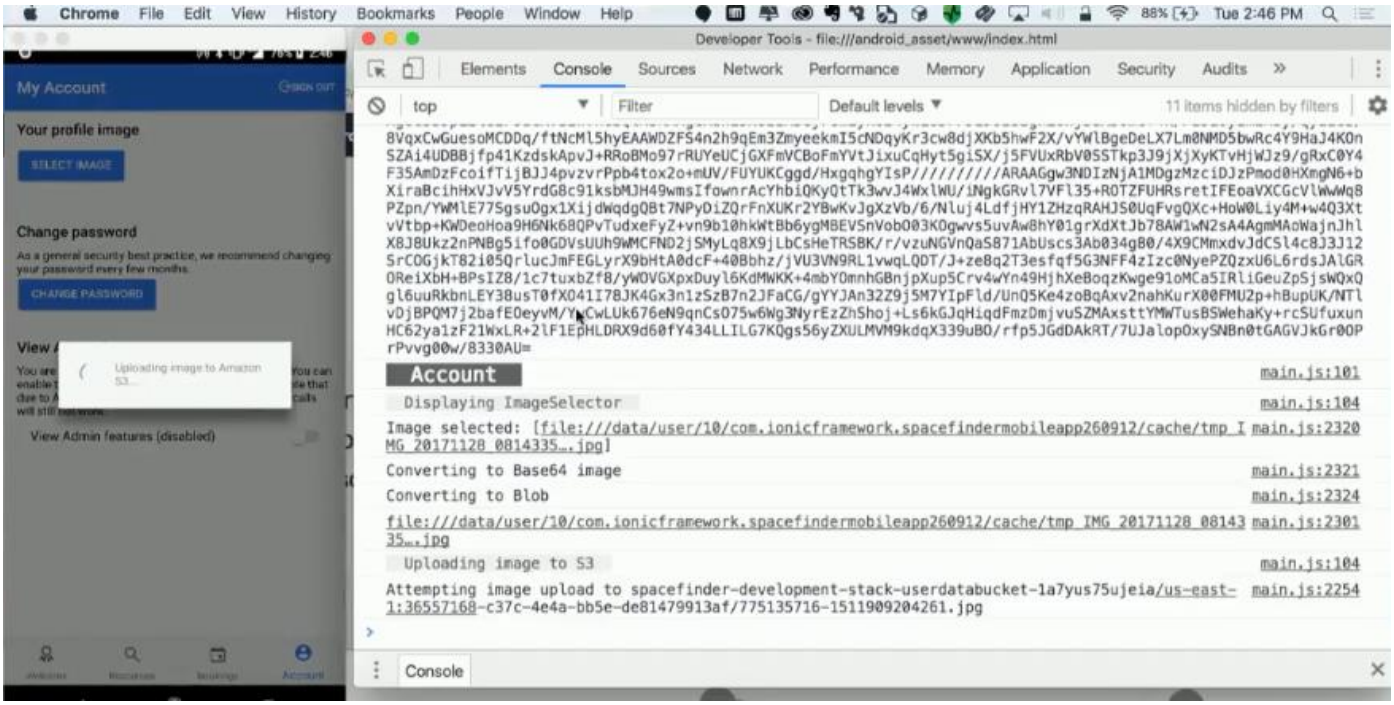


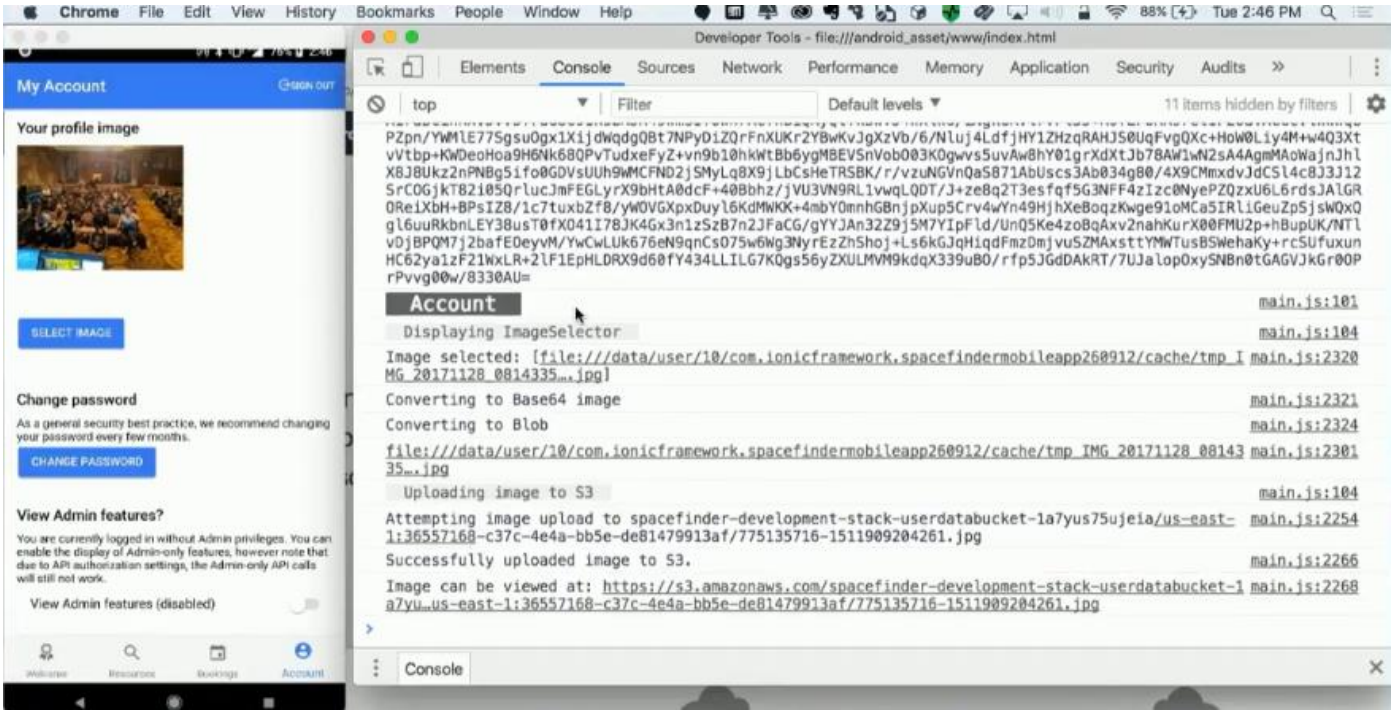
The JWT signature can also be used in our downstream services to make sure that this is a valid JWT token created by Cognito.



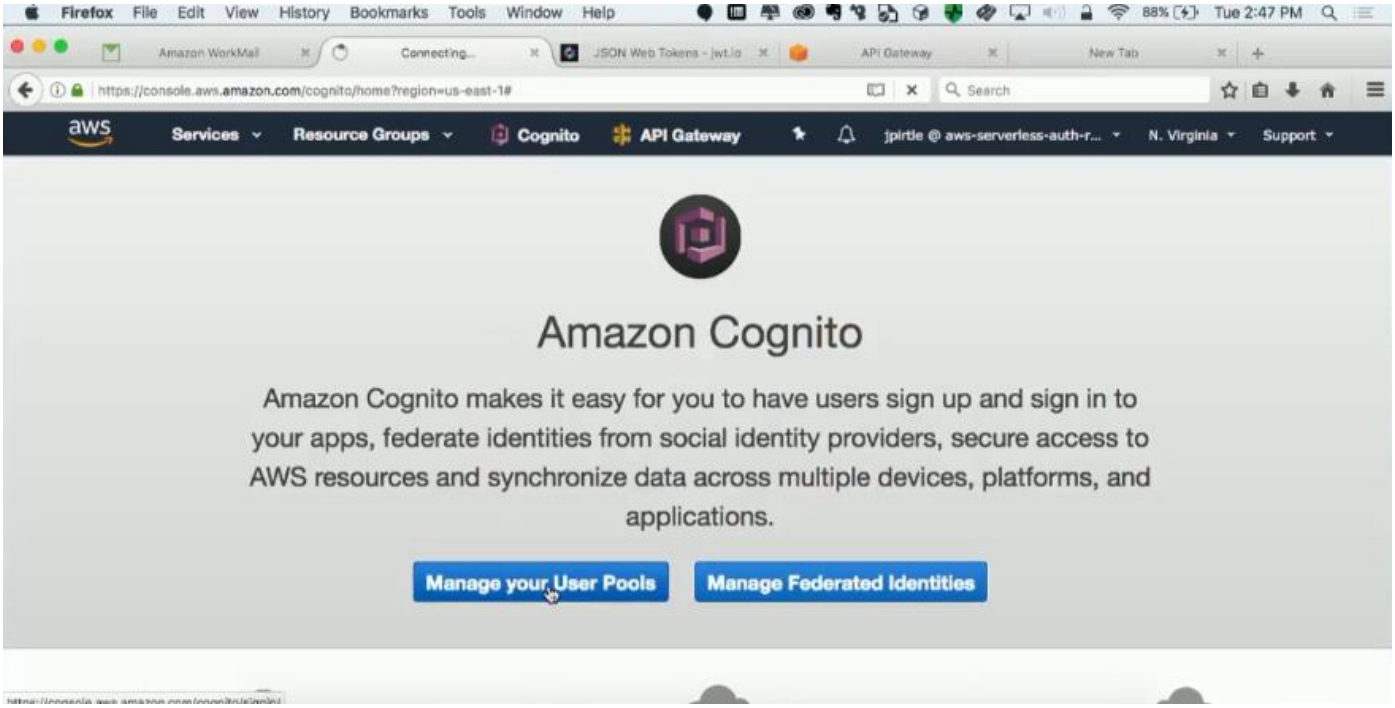
Let us now see an example of the user uploading an image

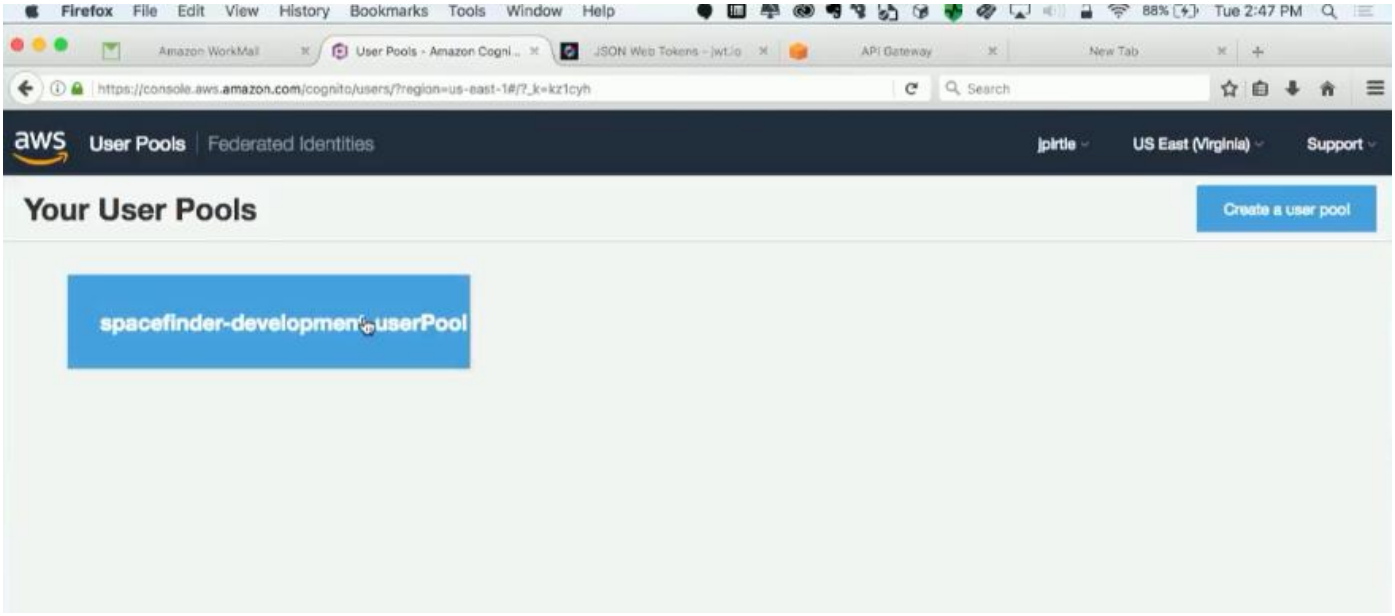

Chrome File Edit View History Bookmarks People Window Help
88% Tue 2:46 PM
CANCEL
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
10 items hidden by filters
Cognito User Pools User Groups: Vladimir belongs to group c
main.js:681
Cognito User Pools User Attributes:
main.js:685
{sub: "6b8d6c62-b3ec-4487-a5a8-3d25e1a1d10b", email_verified: true, iss: "https://cognito-idp.us-east-1.amazonaws.com/us-east-1_Iaovdw2o2", cognito:username: "Vladimir", given_name: "Vladimir", …}
Cognito Identity ID: us-east-1:36557168-c37c-4e4a-bb5e-de81479913af
main.js:690
AWS Access Key ID: ASIAJZ7PRIJEWQIHVNEQ
main.js:692
AWS Secret Access Key: wUwAPtwO2qAcSNPLwjRZew6tietgGTQu6+o1/z4f
main.js:694
AWS Session Token:
main.js:696
AgoGb3JpZ2luEFsaCXVzLWVhc3QtMSKAAgCRdhi5NsIzK3ejremEyko24yWLOJFPD1DOISzghZUhj3uX5omGY4k/PEJEoyImzMBy/qyazdB/
8VqxCwGuesoMCDDq/ftNcMl5hyEAAWDZFS4n2h9qEm3ZmyeekmI5cNDqyKr3cw8djXKb5hwF2X/vYWlBgeDeLX7Lm0NMD5bwRc4Y9HaJ4KOn
SZAi4UDBBjfp41KzdskApvJ+RRoBMo97rRUYeUCjGXFmVCBoFmYVtJixuCqHyt5giSX/j5FVUxRbV0SSTkp3J9jXjXyKTvHjWJz9/gRxC0Y4
F35AmDzFcoifTijBJJ4pvzvrPpb4tox2o+mUV/FUYUKCggd/HxgqhgYIsP//////////ARAAGgw3NDIzNjA1MDgzMzciDJzPmod0HXmgN6+b
XiraBcihHxVJvV5YrdG8c91ksbMJH49wmsIfownrAcYhbiQKyQtTk3wvJ4WxlWU/iNgkGRvl7VFl35+ROTZFUHRsretIFEoaVXCGcVlWwWq8
PZpn/YWMlE77SgsuOgx1XijdWqdgQBt7NPyDiZQrFnXUKr2YBwKvJgXzVb/6/Nluj4LdfjHY1ZHzqRAHJS0UqFvgQXc+HoW0Liy4M+w4Q3Xt
vVtbp+KWDeoHoa9H6Nk68QPvTudxeFyZ+vn9b10hkWtBb6ygMBEVSnVobO03KOgwvs5uvAw8hY01grXdXtJb78AW1wN2sA4AgmMAoWajnJhl
X8J8Ukz2nPNBg5ifo0GDVsUUh9WMCFND2jSMyLq8X9jLbCsHeTRSBK/r/vzuNGVnQaS871AbUscs3Ab034g80/4X9CMmxdvJdCSl4c8J3J12
SrCOGjkT82i05QrlucJmFEGLyrX9bHtA0dcF+40Bbhz/jVU3VN9RL1vwqLQDT/J+zeBq2T3esfqf5G3NFF4zIzc0NyePZQzxU6L6rdsJAlGR
OReiXbH+BPsIZ8/1c7tuxbZf8/yWOVGXpxDuyl6KdMWKK+4mbYOmnhGBnjpXup5Crv4wYn49HjhXeBoqzKwge91oMCa5IRliGeuZpSjsWQxQ
gl6uuRkbnLEY38usT0fXO41I78JK4Gx3n1zSzB7n2JFaCG/gYYJAn32Z9j5M7YIpFld/UnQ5Ke4zoBqAxv2nahKurX00FMU2p+hBupUK/NTl
vDjBPQM7j2bafEOeyvM/YwCwLUk676eN9qnCsO75w6Wg3NyrEzZhShoj+Ls6kGJqHiqdFmzDmjvuSZMAxsttYMWTusBSWehaKy+rcSUfuxun
HC62ya1zF21WxLR+2lF1EpHLDRX9d60fY434LLILG7KQgs56yZXULMVM9kdqX339uBO/rfp5JGdDAkRT/7UJalopOxySNBn0tGAGVJkGr0OP
rPvvg00w/8330AU=
main.js:696
Account
main.js:101
Displaying ImageSelector
main.js:104
Console

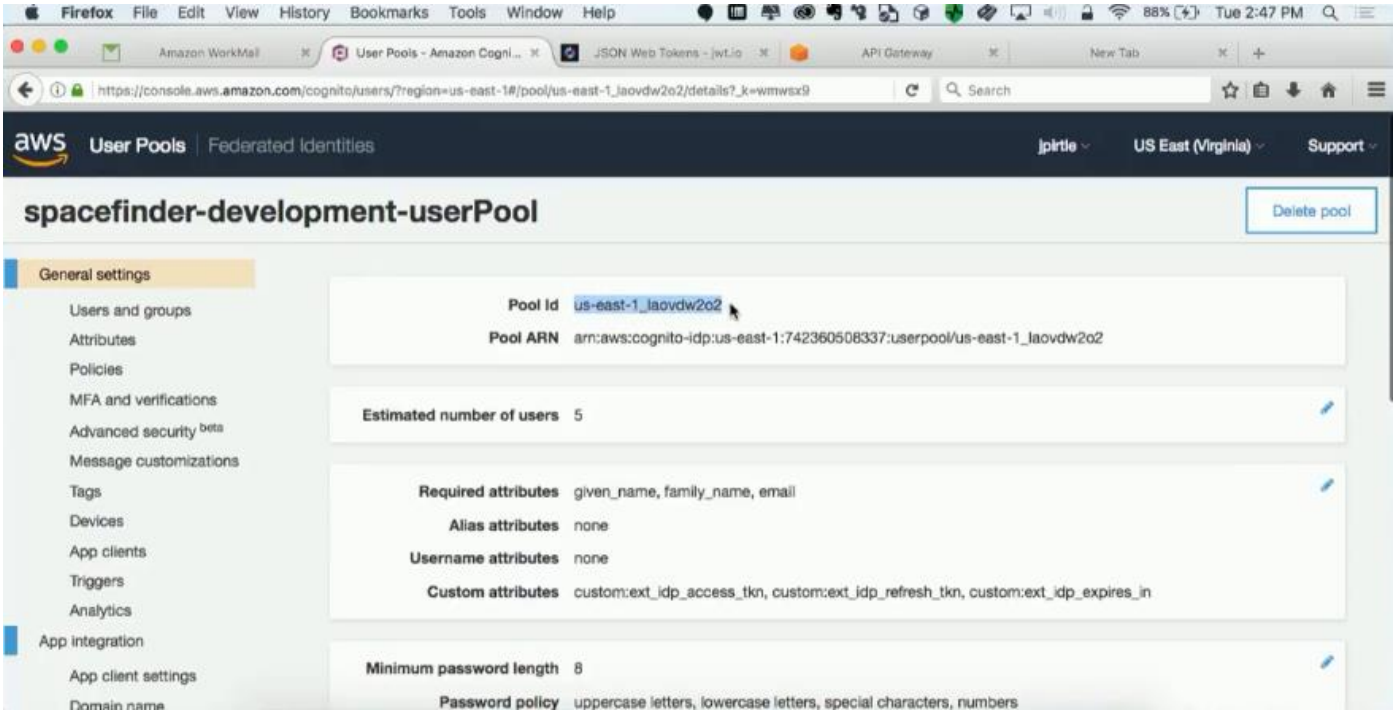

Chrome File Edit View History Bookmarks People Window Help
88% Tue 2:46 PM
My Account
SIGN OUT
Your profile image
SELECT IMAGE
Change password
As a general security best practice, we recommend changing your password every few months.
CHANGE PASSWORD
View A
Uploading image to Amazon S3...
View Admin features (disabled)
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
11 items hidden by filters
8VqxCwGuesoMCDDq/ftNcMl5hyEAAWDZFS4n2h9qEm3ZmyeekmI5cNDqyKr3cw8djXKb5hwF2X/vYWlBgeDeLX7Lm0NMD5bwRc4Y9HaJ4KOn
SZAi4UDBBjfp41KzdskApvJ+RRoBMo97rRUYeUCjGXFmVCBoFmYVtJixuCqHyt5giSX/j5FVUxRbV0SSTkp3J9jXjXyKTvHjWJz9/gRxC0Y4
F35AmDzFcoifTijBJJ4pvzvrPpb4tox2o+mUV/FUYUKCggd/HxgqhgYIsP//////////ARAAGgw3NDIzNjA1MDgzMzciDJzPmod0HXmgN6+b
XiraBcihHxVJvV5YrdG8c91ksbMJH49wmsIfownrAcYhbiQKyQtTk3wvJ4WxlWU/iNgkGRvl7VFl35+ROTZFUHRsretIFEoaVXCGcVlWwWq8
PZpn/YWMlE77SgsuOgx1XijdWqdgQBt7NPyDiZQrFnXUKr2YBwKvJgXzVb/6/Nluj4LdfjHY1ZHzqRAHJS0UqFvgQXc+HoW0Liy4M+w4Q3Xt
vVtbp+KWDeoHoa9H6Nk68QPvTudxeFyZ+vn9b10hkWtBb6ygMBEVSnVobO03KOgwvs5uvAw8hY01grXdXtJb78AW1wN2sA4AgmMAoWajnJhl
X8J8Ukz2nPNBg5ifo0GDVsUUh9WMCFND2jSMyLq8X9jLbCsHeTRSBK/r/vzuNGVnQaS871AbUscs3Ab034g80/4X9CMmxdvJdCSl4c8J3J12
SrCOGjkT82i05QrlucJmFEGLyrX9bHtA0dcF+40Bbhz/jVU3VN9RL1vwqLQDT/J+zeBq2T3esfqf5G3NFF4zIzc0NyePZQzxU6L6rdsJAlGR
OReiXbH+BPsIZ8/1c7tuxbZf8/yWOVGXpxDuyl6KdMWKK+4mbYOmnhGBnjpXup5Crv4wYn49HjhXeBoqzKwge91oMCa5IRliGeuZpSjsWQxQ
gl6uuRkbnLEY38usT0fXO41I78JK4Gx3n1zSzB7n2JFaCG/gYYJAn32Z9j5M7YIpFld/UnQ5Ke4zoBqAxv2nahKurX00FMU2p+hBupUK/NTl
vDjBPQM7j2bafEOeyvM/YwCwLUk676eN9qnCsO75w6Wg3NyrEzZhShoj+Ls6kGJqHiqdFmzDmjvuSZMAxsttYMWTusBSWehaKy+rcSUfuxun
HC62ya1zF21WxLR+2lF1EpHLDRX9d60fY434LLILG7KQgs56yZXULMVM9kdqX339uBO/rfp5JGdDAkRT/7UJalopOxySNBn0tGAGVJkGr0OP
rPvvg00w/8330AU=
main.js:696
Account
main.js:101
Displaying ImageSelector
main.js:104
Image selected: [file:///data/user/10/com.ionicframework.spacefindermobileapp260912/cache/tmp_IMG_20171128_0814335…jpg]
main.js:2320
Converting to Base64 image
main.js:2321
Converting to Blob
main.js:2324
file:///data/user/10/com.ionicframework.spacefindermobileapp260912/cache/tmp_IMG_20171128_081433…jpg
main.js:2301
Uploading image to S3
main.js:104
Attempting image upload to spacefinder-development-stack-userdatabucket-1a7yus75ujeia/us-east-1:36557168-c37c-4e4a-bb5e-de81479913af/775135716-1511909204261.jpg
main.js:2254
Console



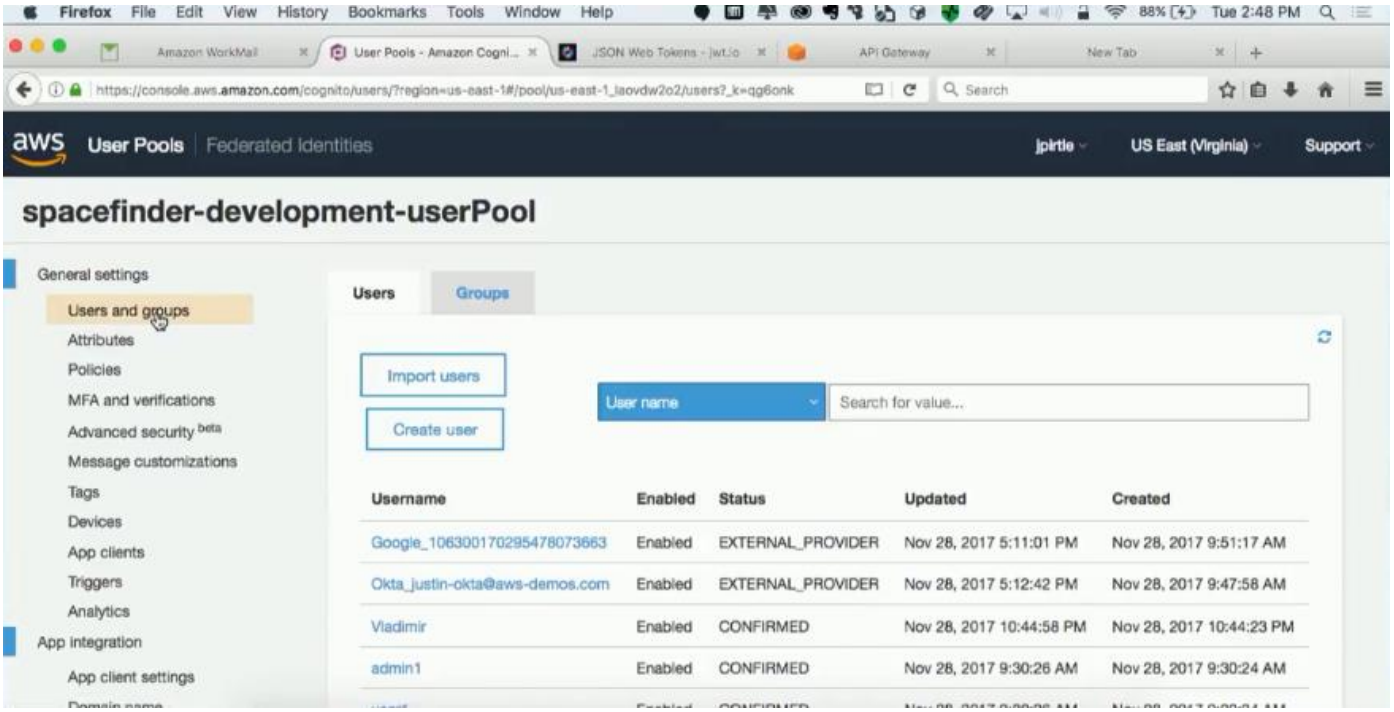
The uploaded image went directly from the mobile device to S3, it did not go through another server. That was possible using IAM Roles, and the image is stored in an S3 bucket that only this user has access to.



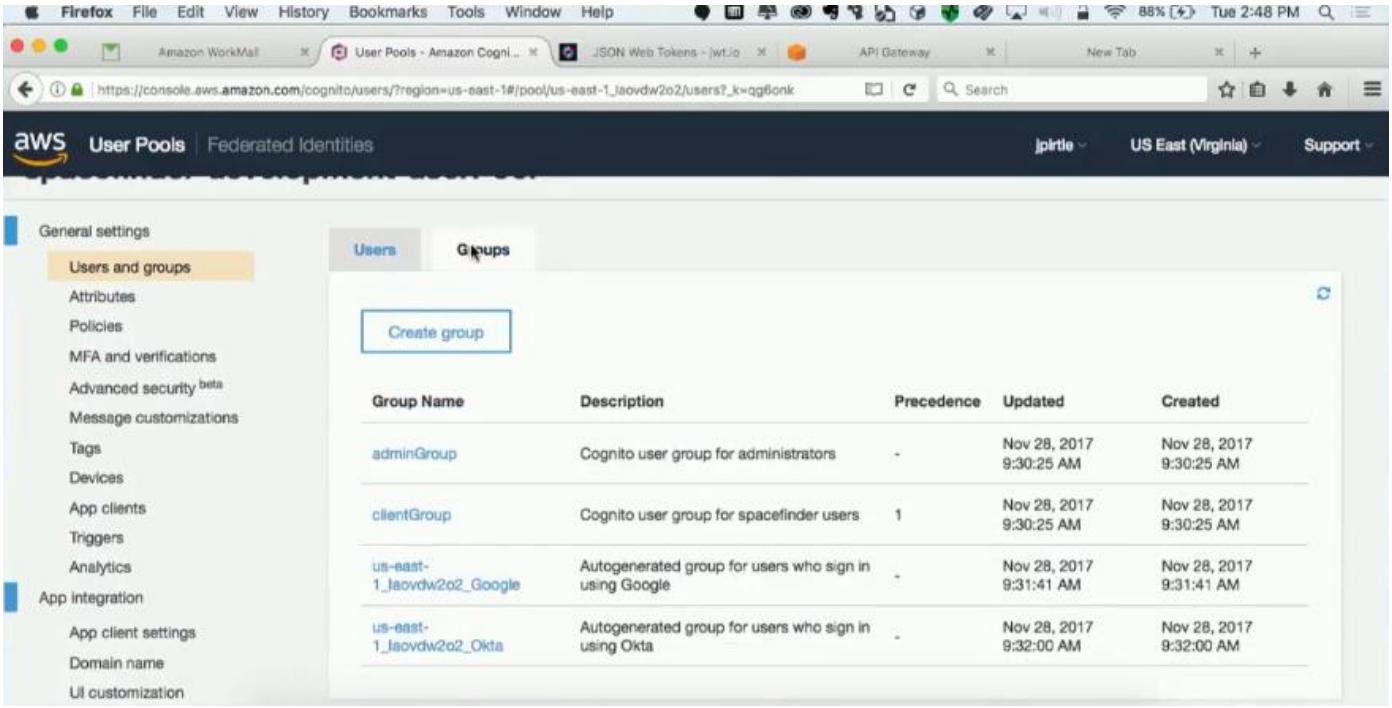




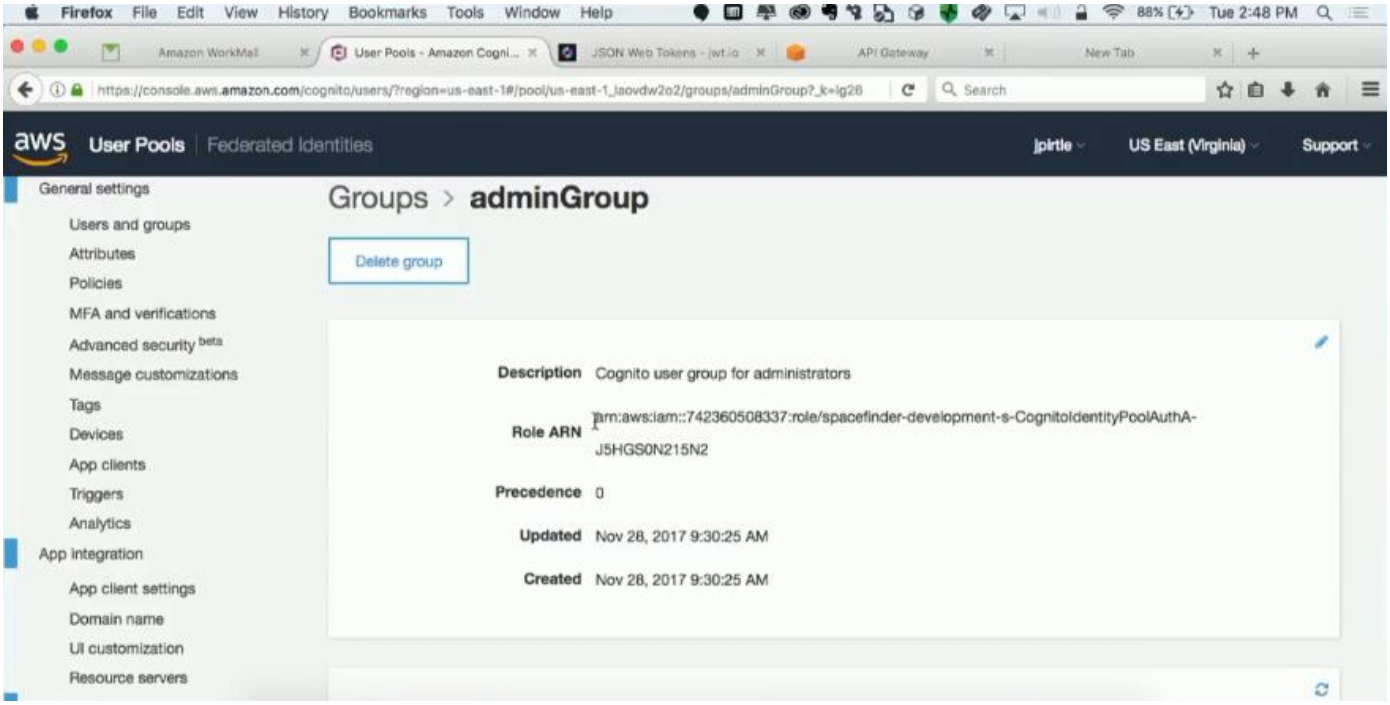
The ***Pool Id*** is the unique ID that you will be referencing throughout your application,



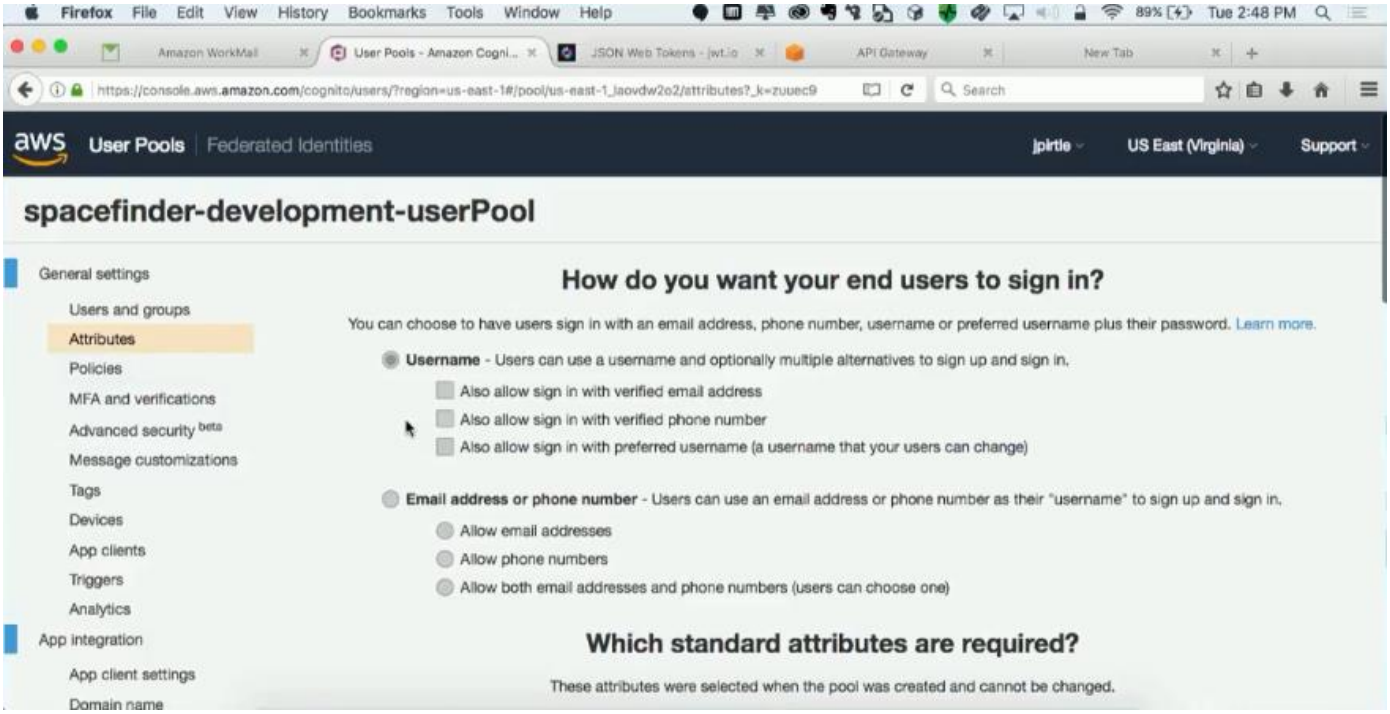
These are the users that have logged in or registered with this particular Cognito User Pool,

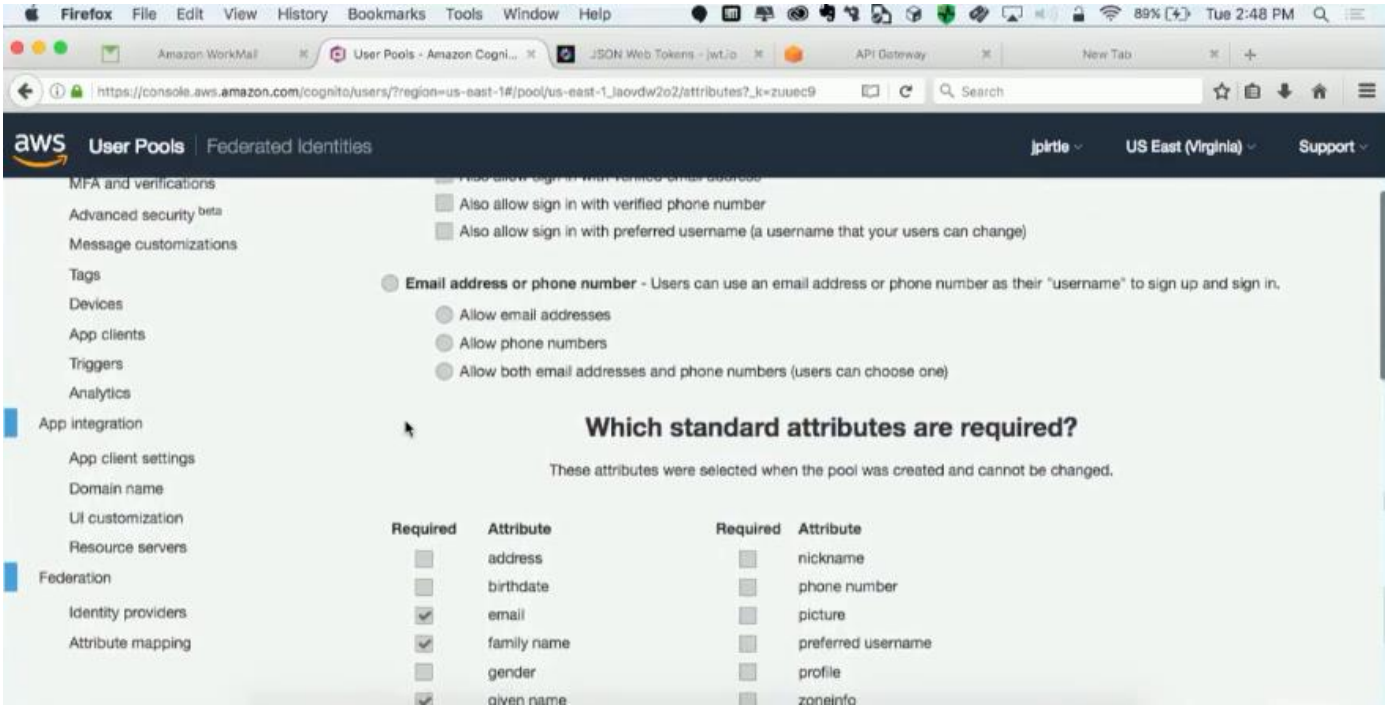


These are the groups created for use with this Cognito User Pool that users can belong to,

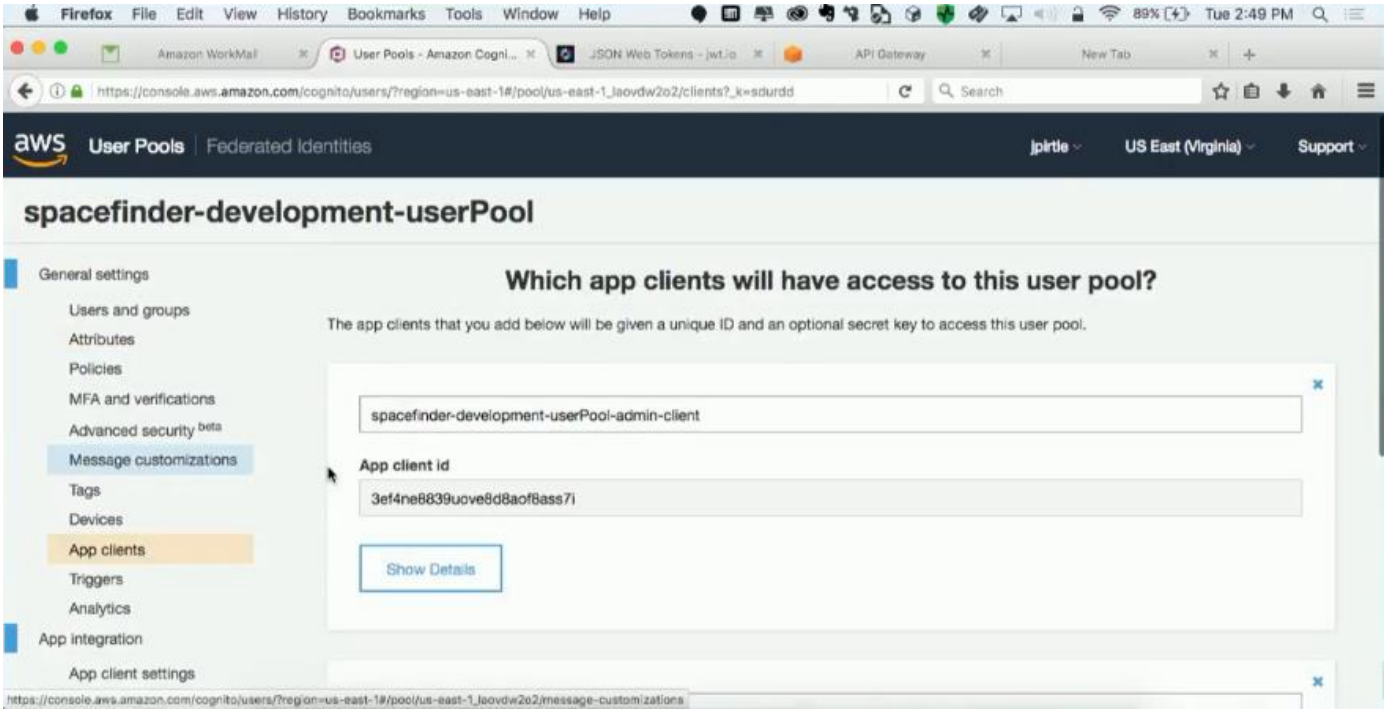


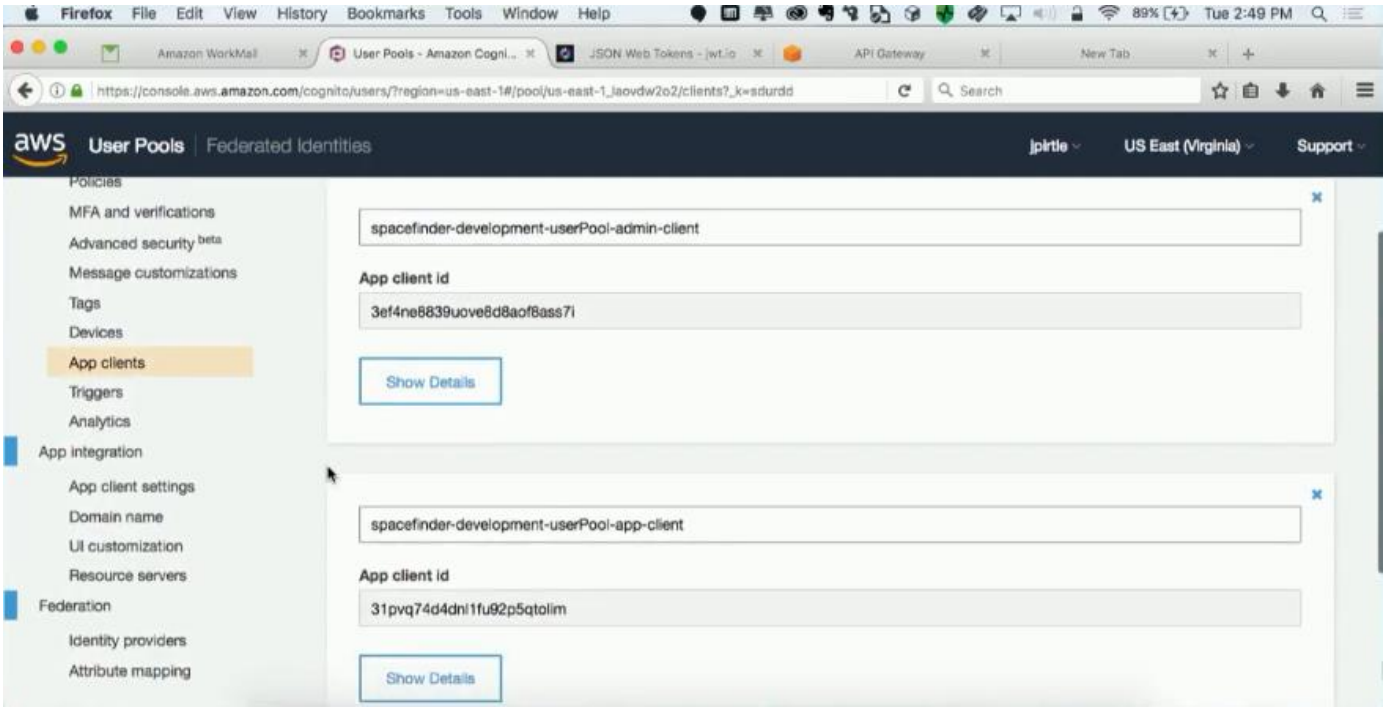
You can see that this group is associated with a particular IAM Role (Role ARN), this means that any user placed into this group will have this IAM Role as part of their token when authenticated.



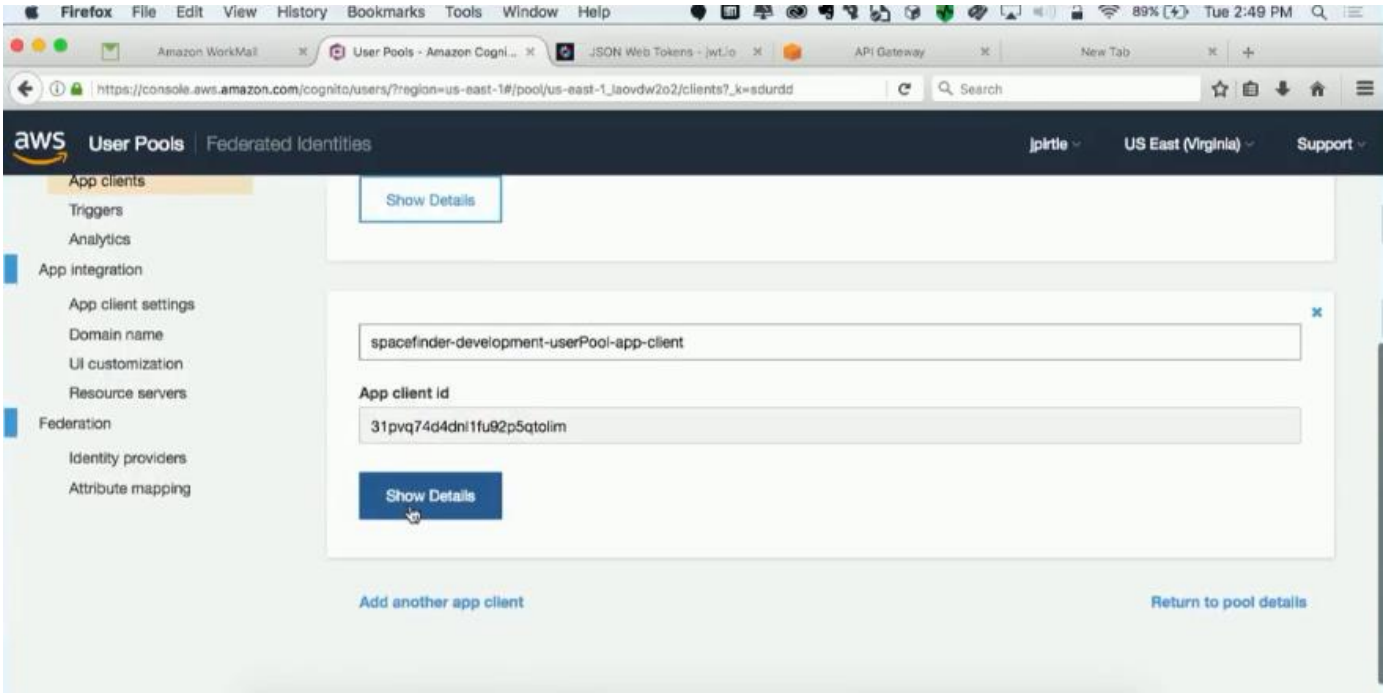


Cognito comes with default attributes but we can also create custom attributes like ‘what is your favorite color’ or ‘has the user paid?’

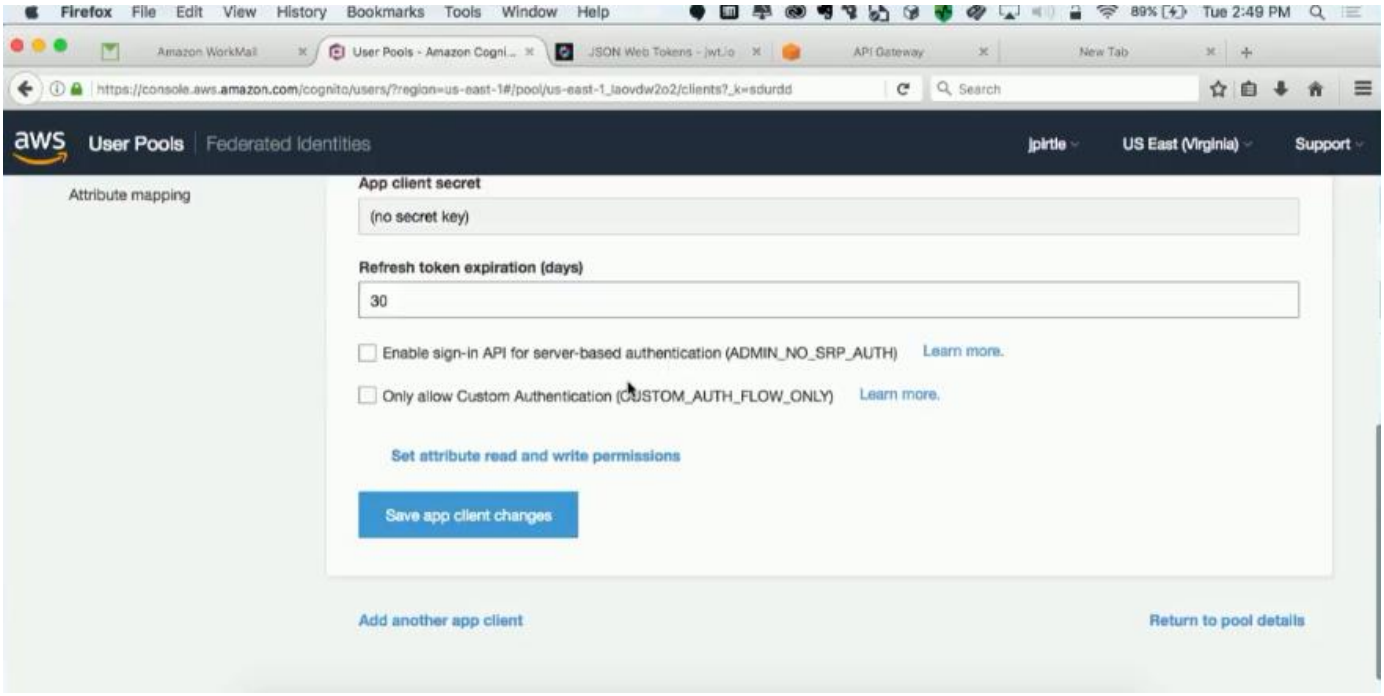


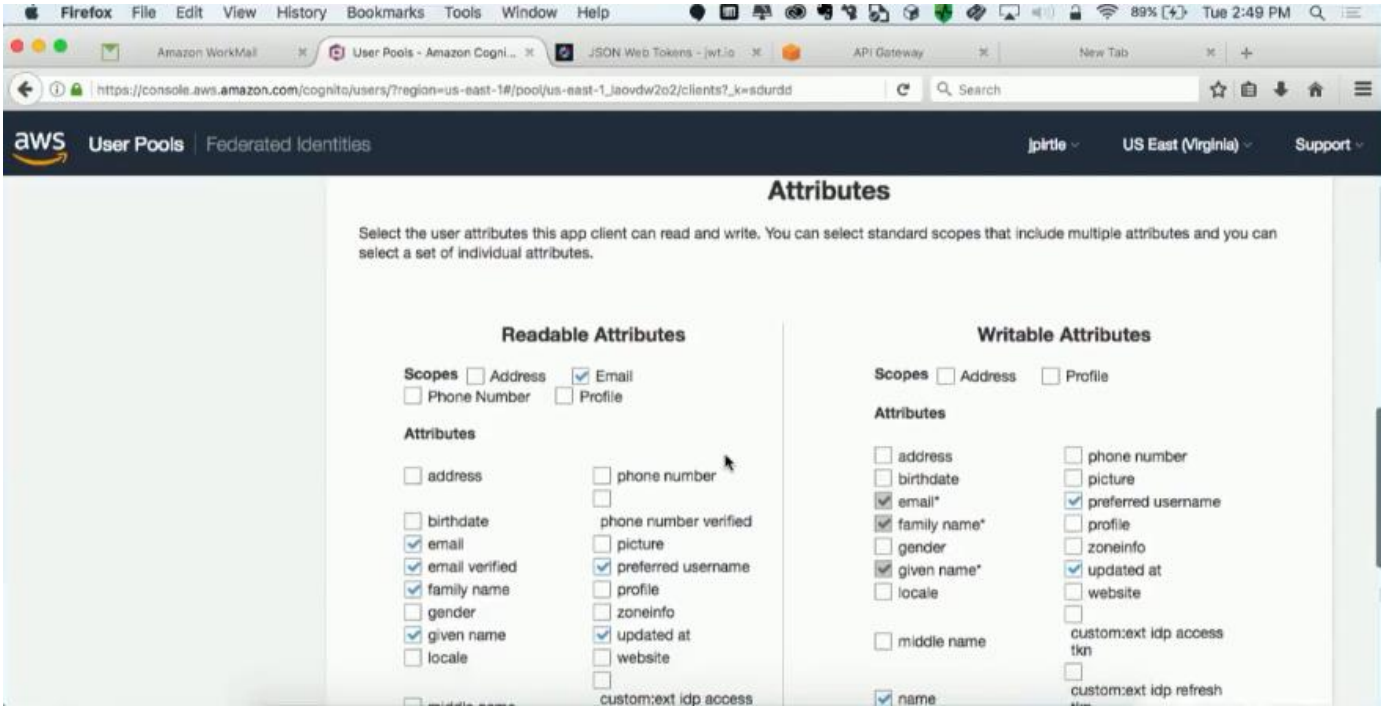


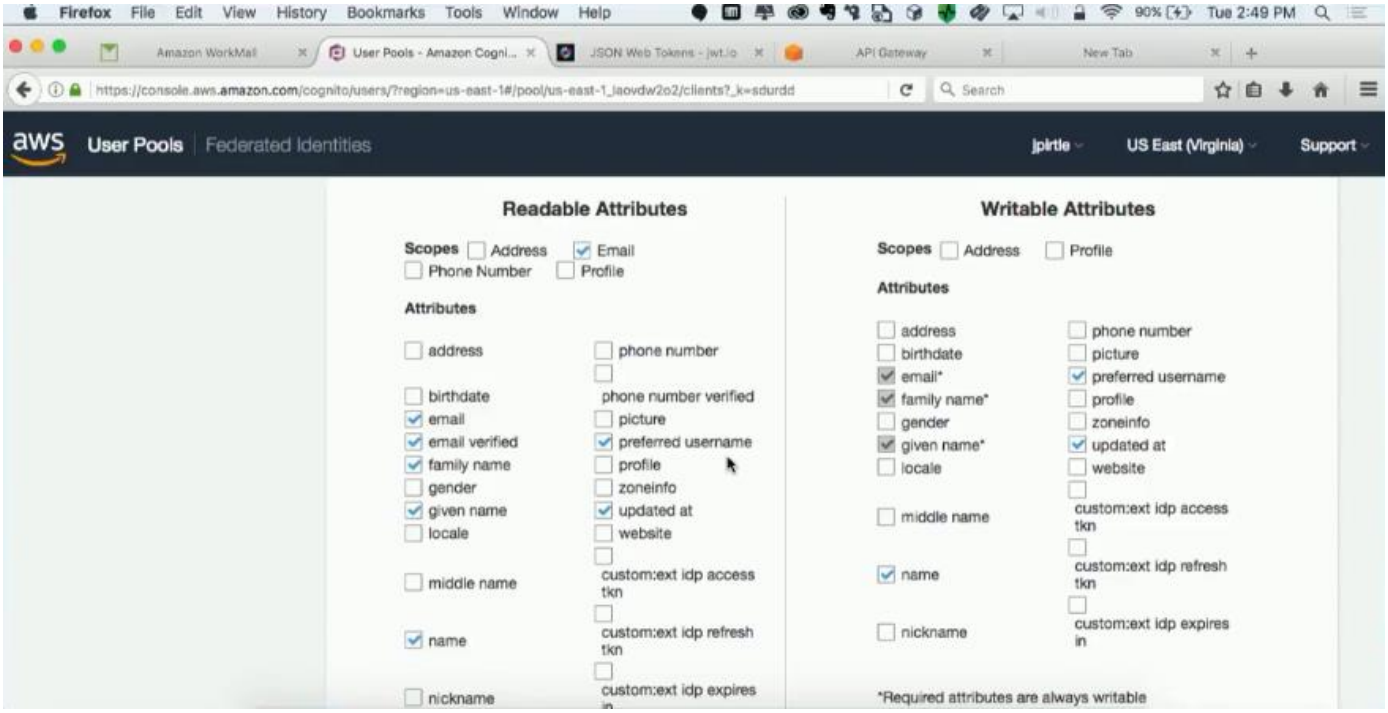
In order to actually talk to Cognito, you need an ***App ID***. Here we have configured 2 app IDs, an ***admin-client App ID*** and the ***app-client App ID*** that is being used by this Cognito application as a client.



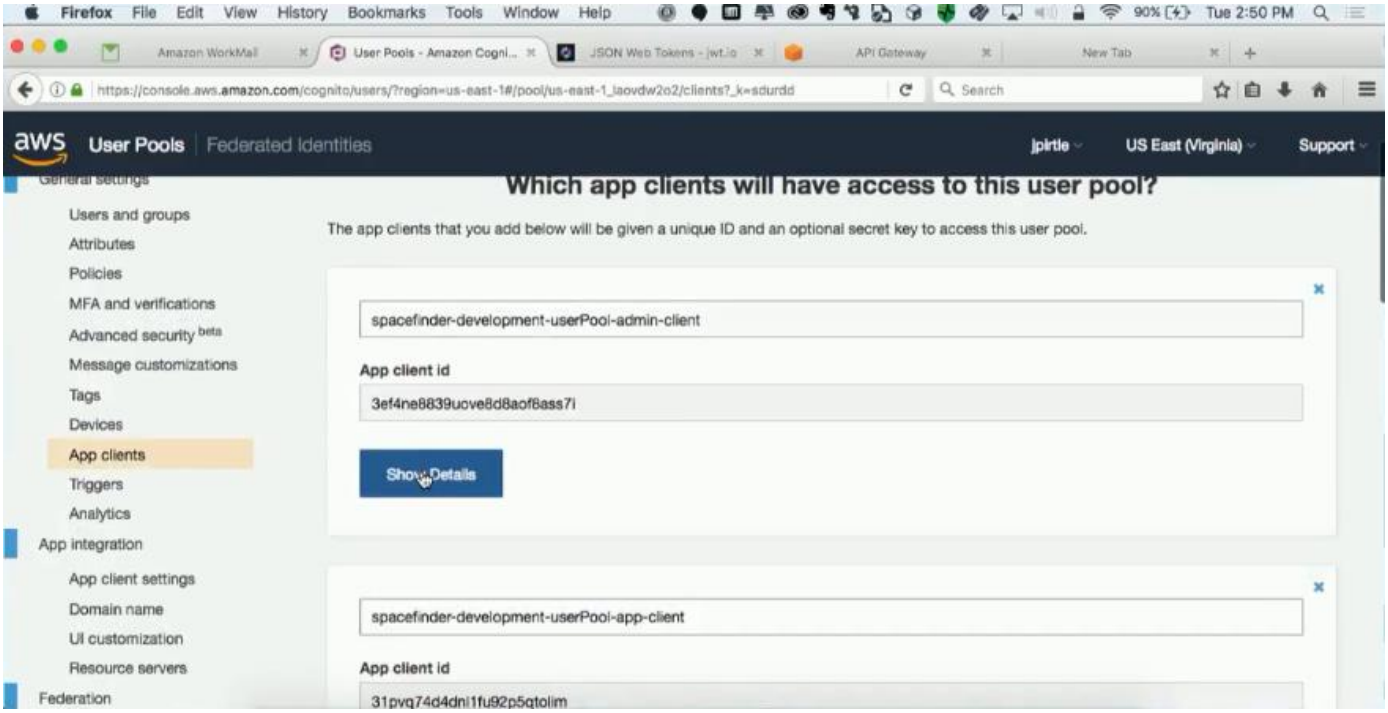
The app-client ID is configured to use SRP as below

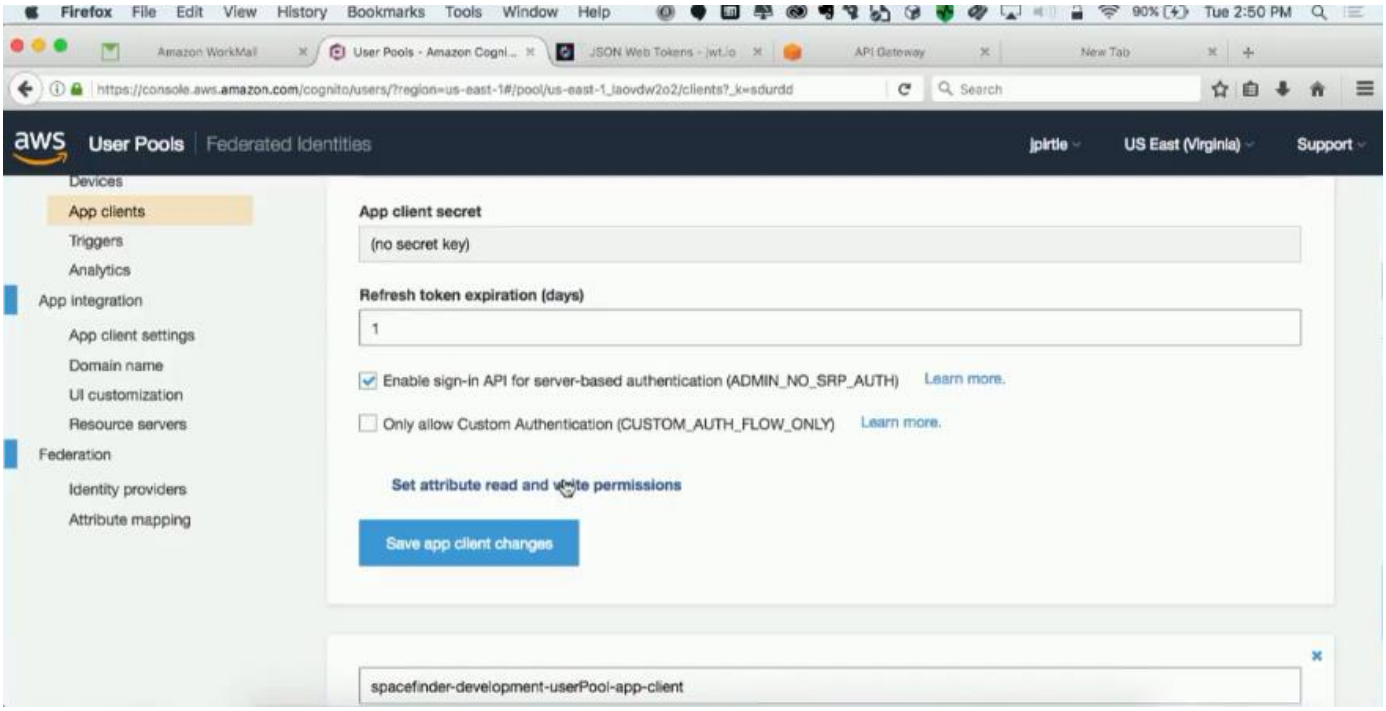

Firefox File Edit View History Bookmarks Tools Window Help
89% Tue 2:49 PM
Amazon WorkMail
User Pools - Amazon Cogni...
JSON Web Tokens - jwt.io
API Gateway
New Tab
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/clients?_k=sdurdd
Search
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Attribute mapping
App client secret
(no secret key)
Refresh token expiration (days)
30
Enable sign-in API for server-based authentication (ADMIN_NO_SRP_AUTH) Learn more.
Only allow Custom Authentication (CUSTOM_AUTH_FLOW_ONLY) Learn more.
Set attribute read and write permissions
Save app client changes
Add another app client
Return to pool details


Firefox File Edit View History Bookmarks Tools Window Help
89% Tue 2:49 PM
Amazon WorkMail
User Pools - Amazon Cogni...
JSON Web Tokens - jwt.io
API Gateway
New Tab
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/clients?_k=sdurdd
Search
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Attributes
Select the user attributes this app client can read and write. You can select standard scopes that include multiple attributes and you can select a set of individual attributes.
Readable Attributes
Scopes Address Email Phone Number Profile
Attributes
address
birthdate
email
email verified
family name
gender
given name
locale
phone number
phone number verified
picture
preferred username
profile
zoneinfo
updated at
website
custom:ext idp access
Writable Attributes
Scopes Address Profile
Attributes
address
birthdate
email*
family name*
gender
given name*
locale
middle name
name
phone number
picture
preferred username
profile
zoneinfo
updated at
website
custom:ext idp access tkn
custom:ext idp refresh

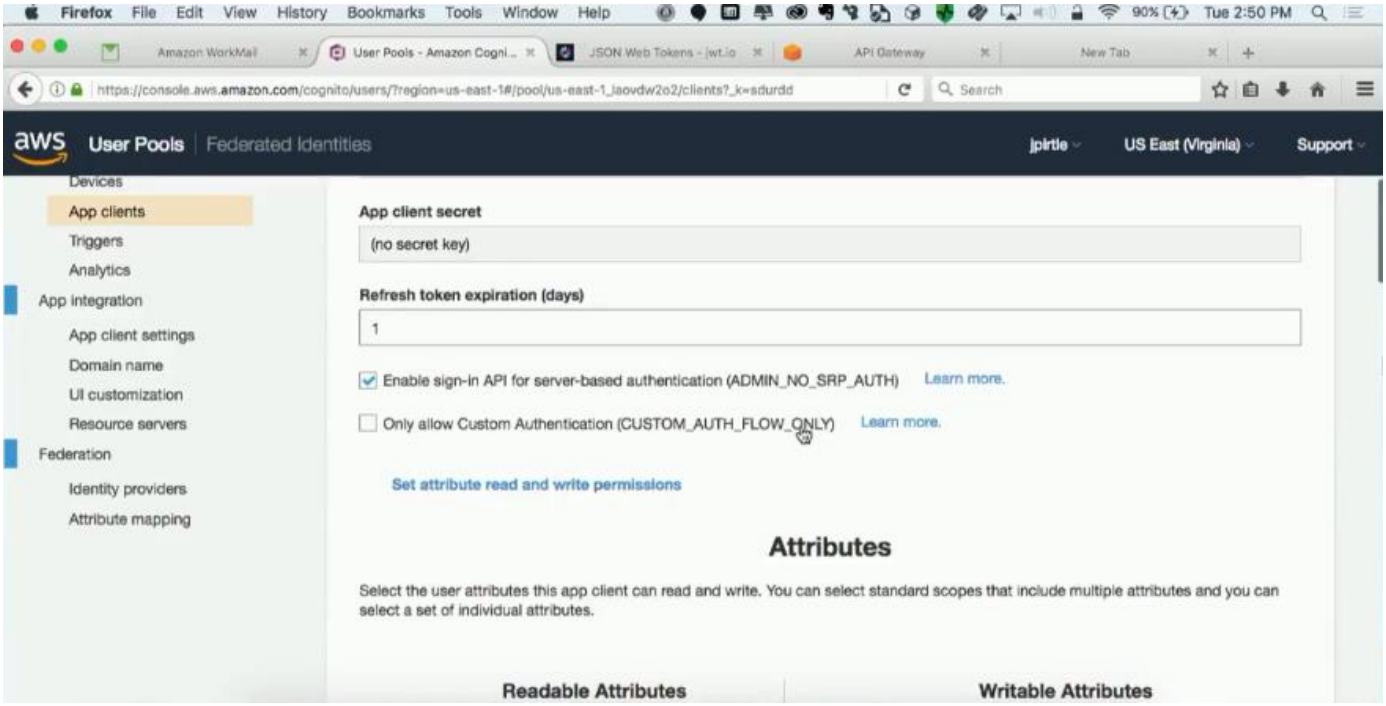


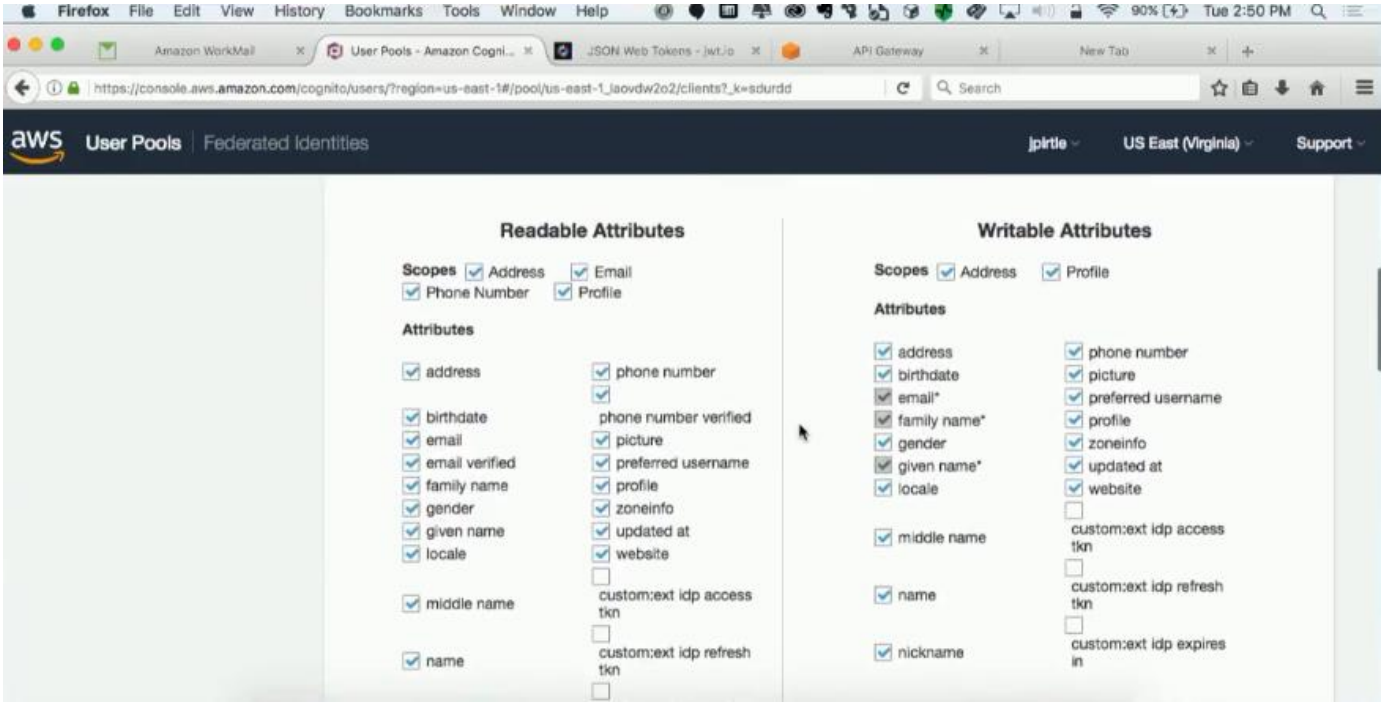
We can also set what this client has access to do in regards to reading and writing. Like preventing the client from modifying the 'paid' attribute value. We will want an admin user to be able to modify the 'paid' attribute value as below



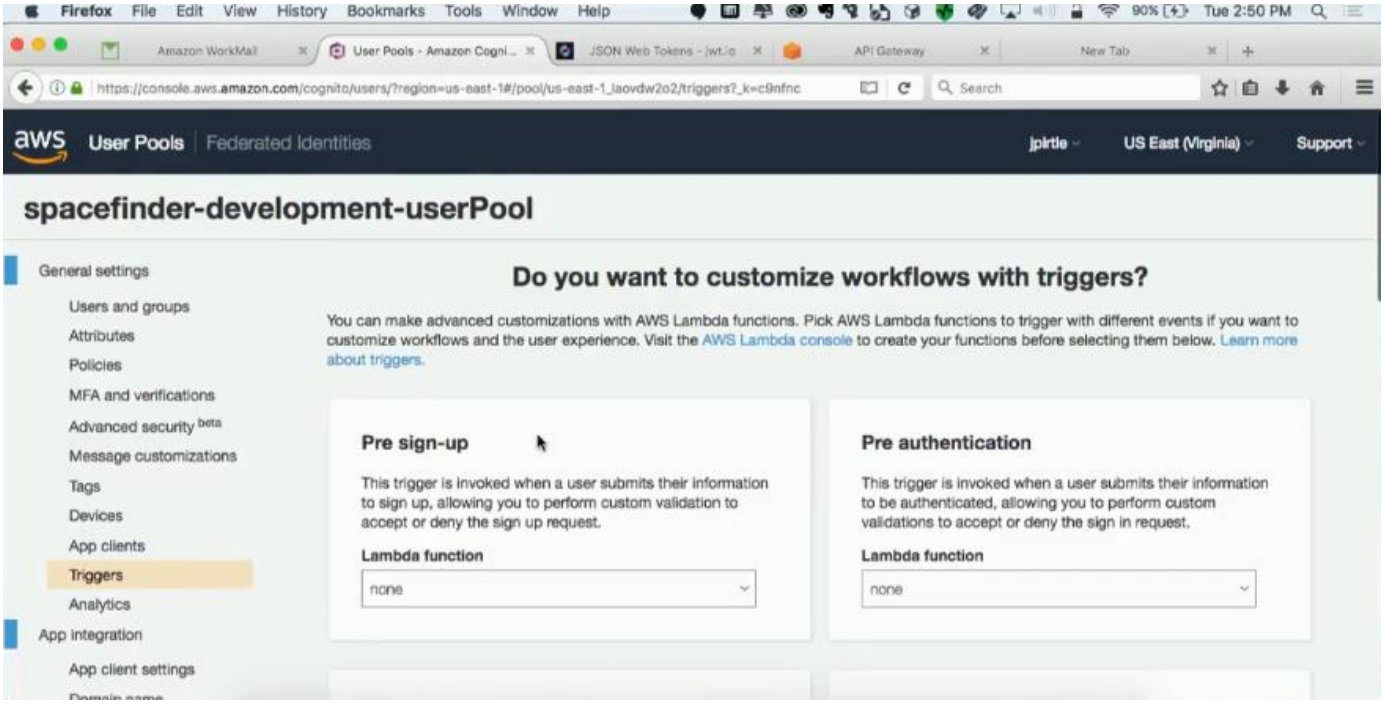


We have turned off SRP here,

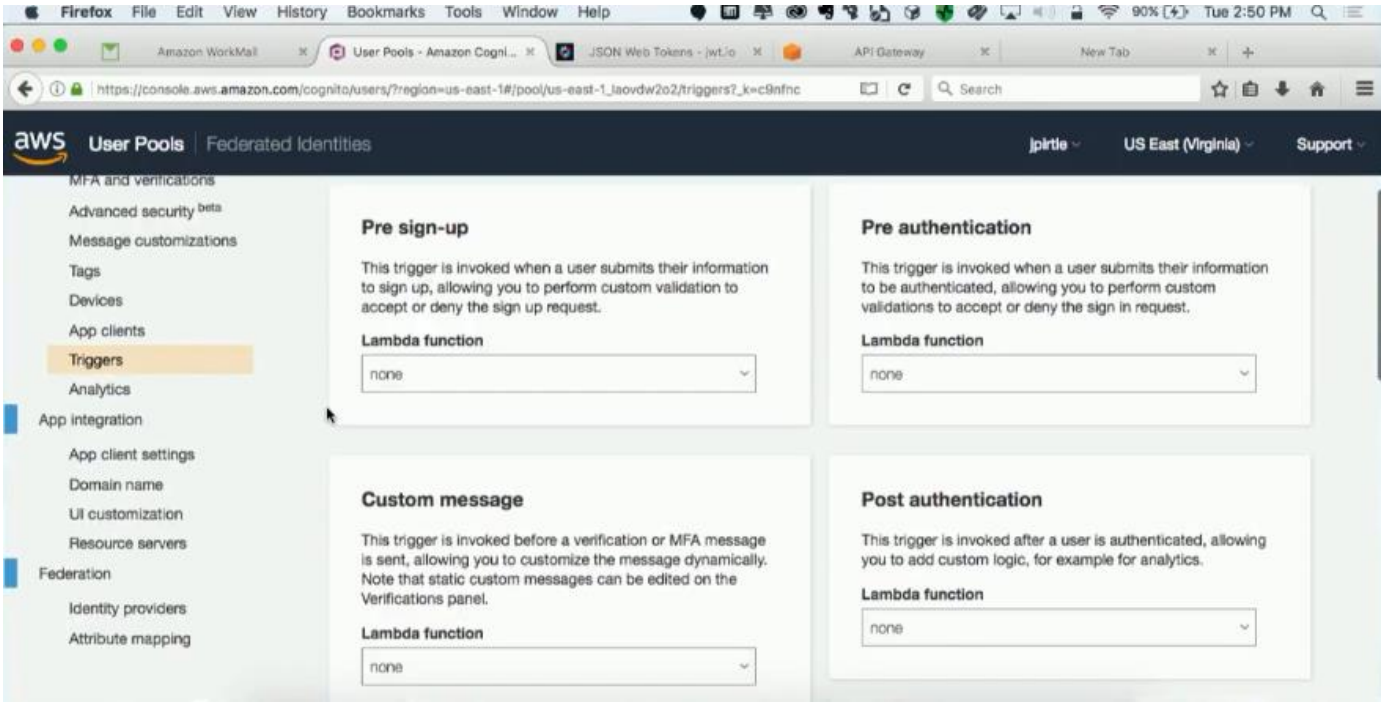




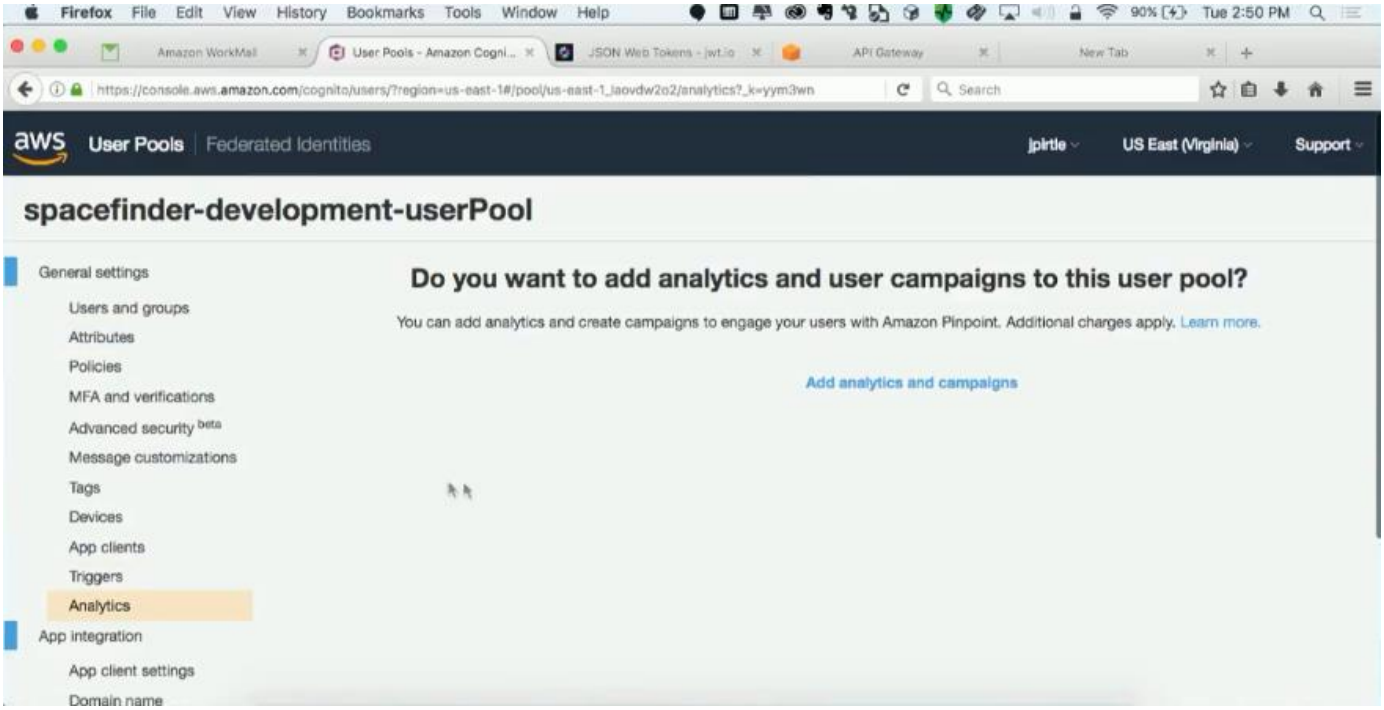
The admin app ID has access to all the available attributes.



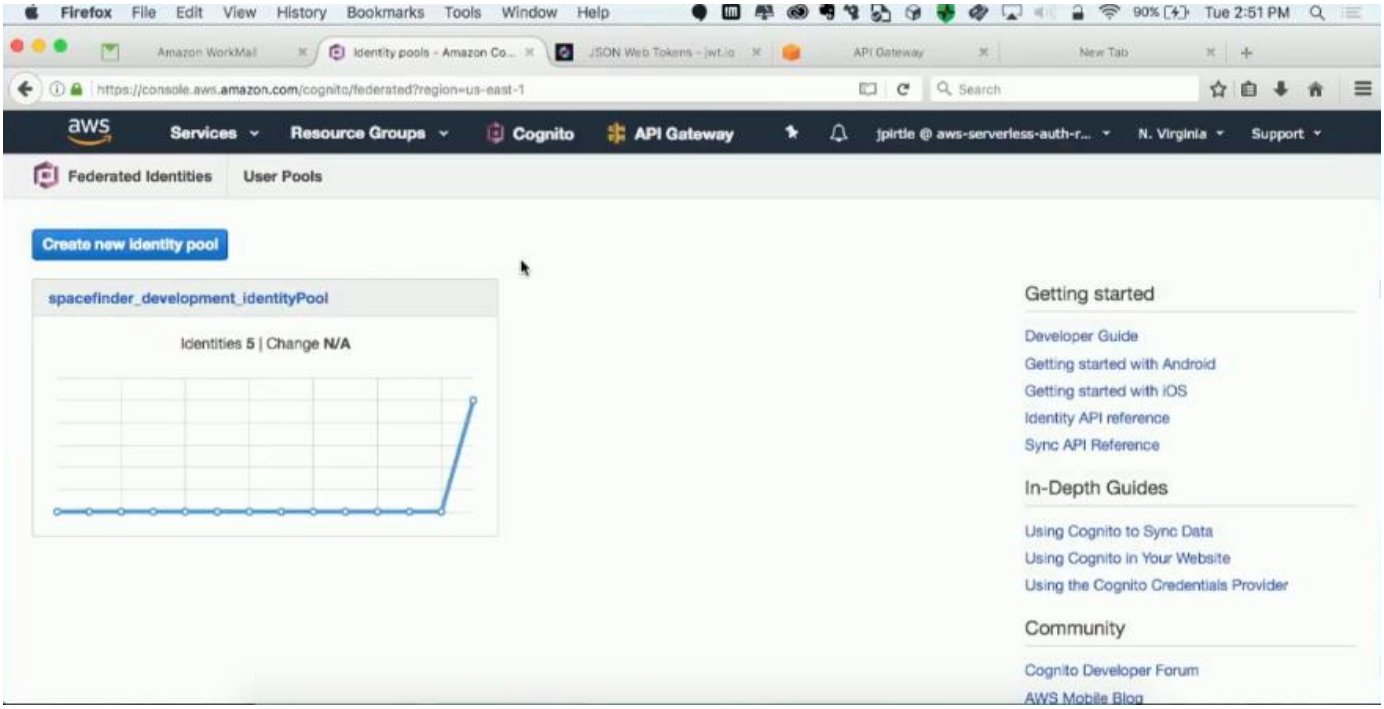
Triggers are a way for you to customize the authentication and the authorization flows,



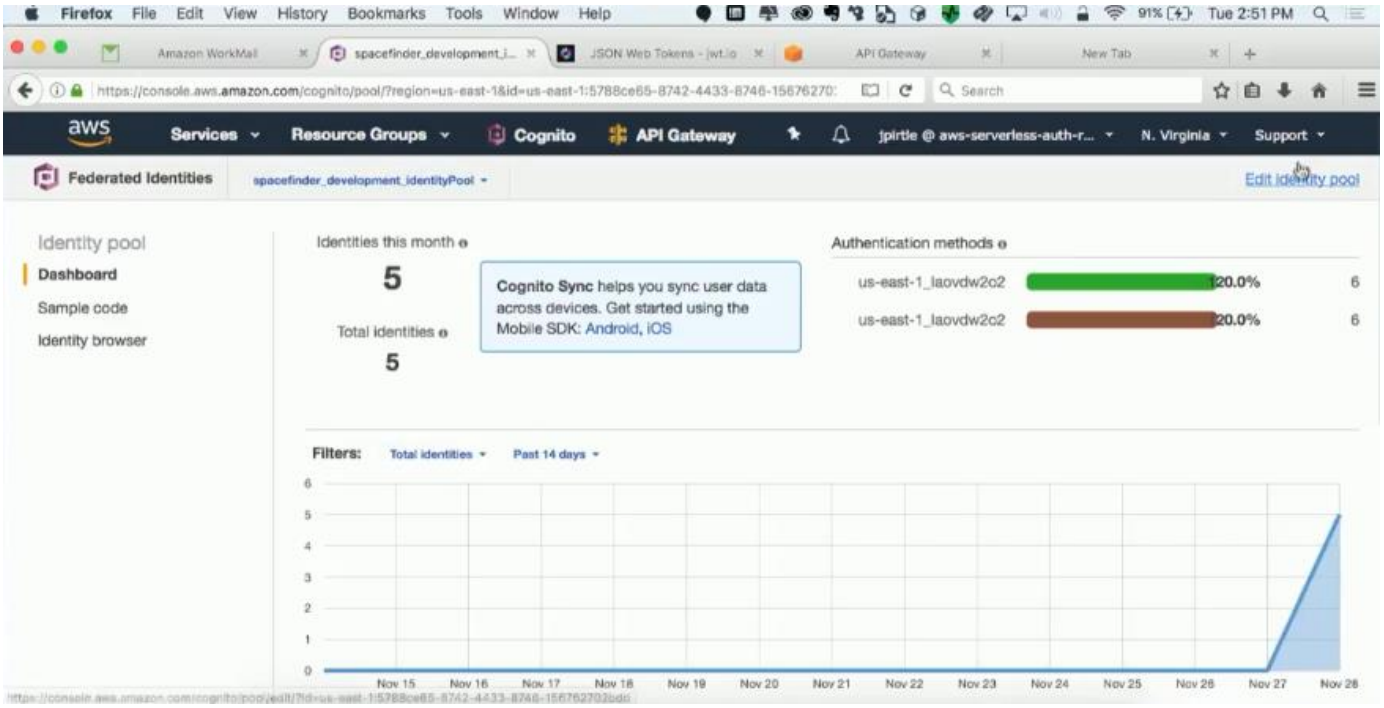
Triggers are simple lambdas that we can use

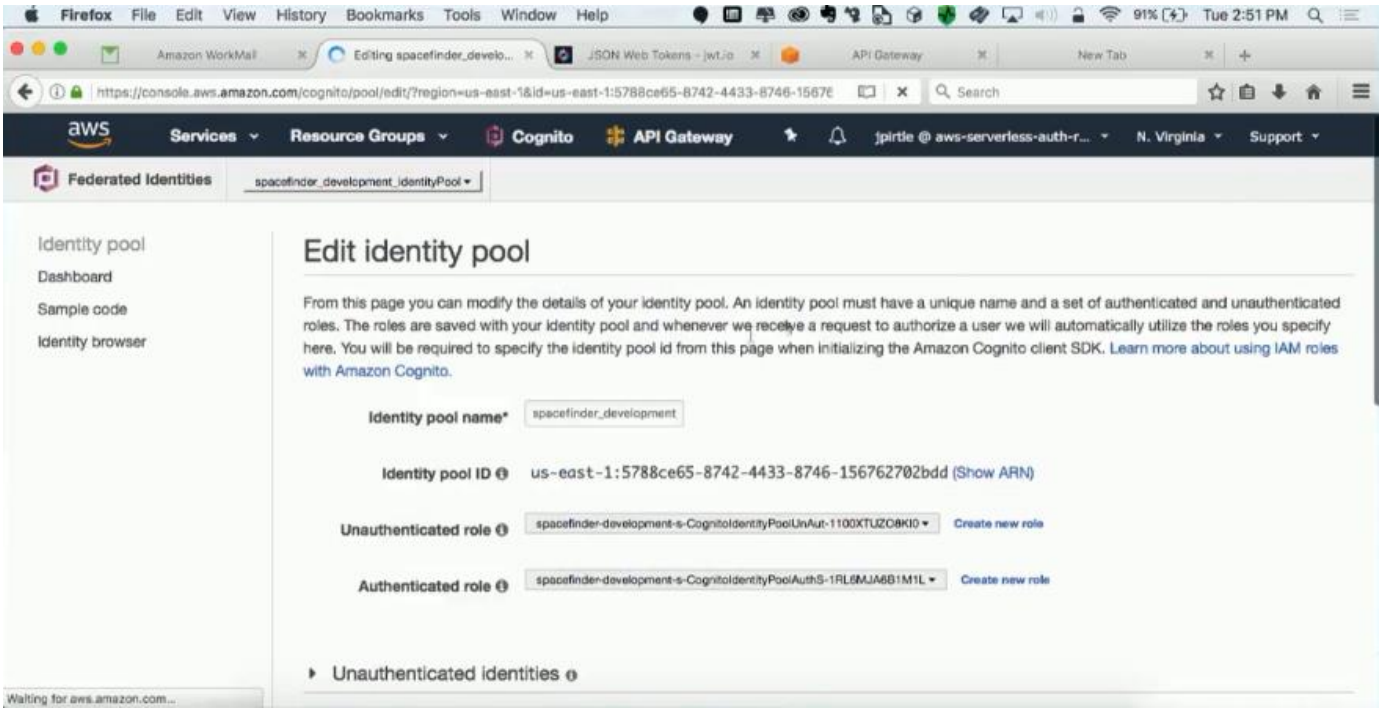


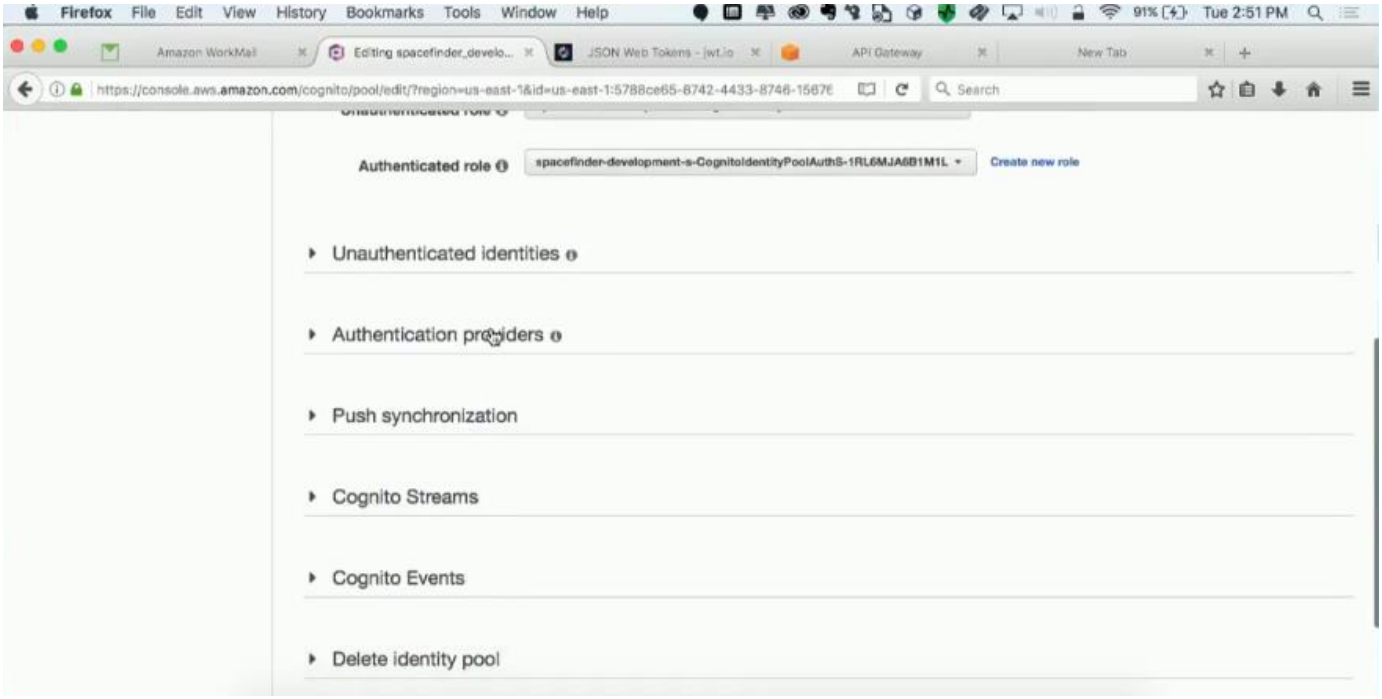
You can also turn on analytics

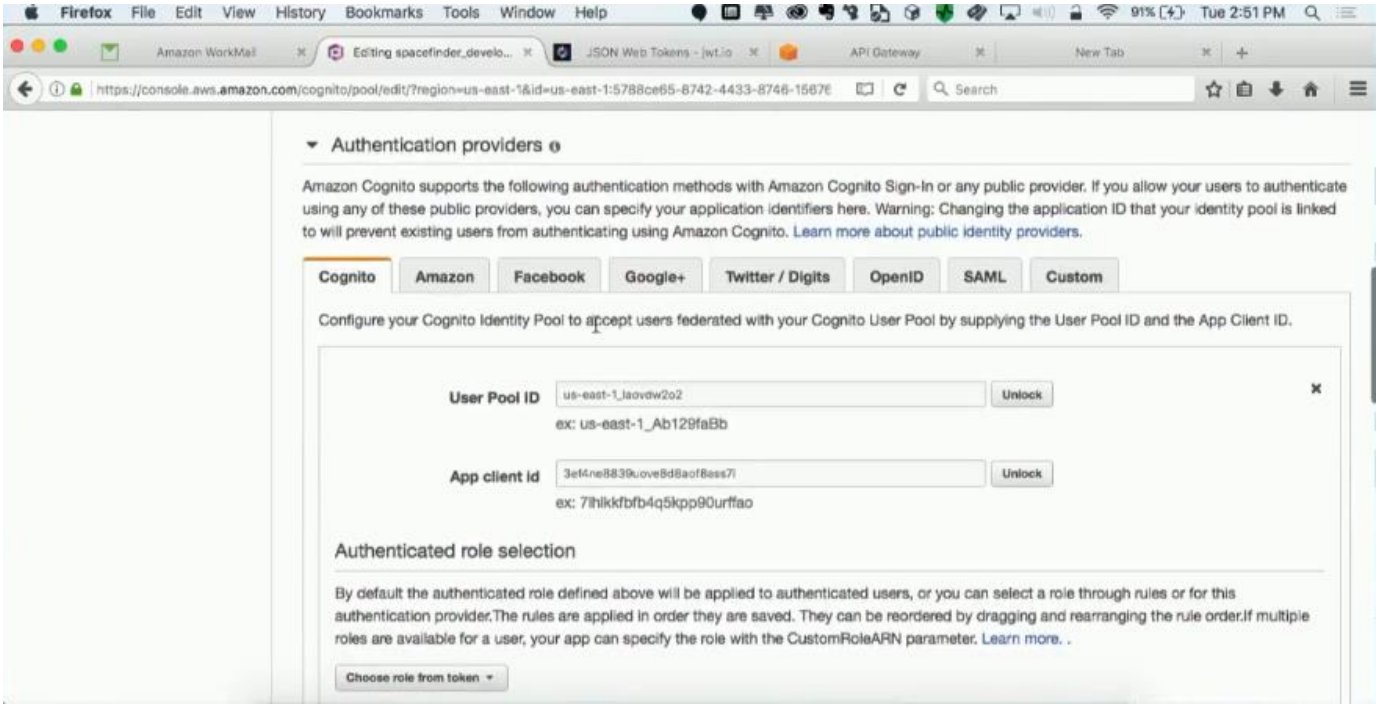


Cognito User Pools is your User directory, it stores the users and allows for an easier way to create the sign up and sign in functionalities. ***Cognito Federated Identities*** is what allows those users that have logged in with Cognito User Pools to get AWS Credentials, you exchange JWT tokens for AWS IAM Role credentials so that those users can access AWS services like S3 buckets, DynamoDB and API Gateways.

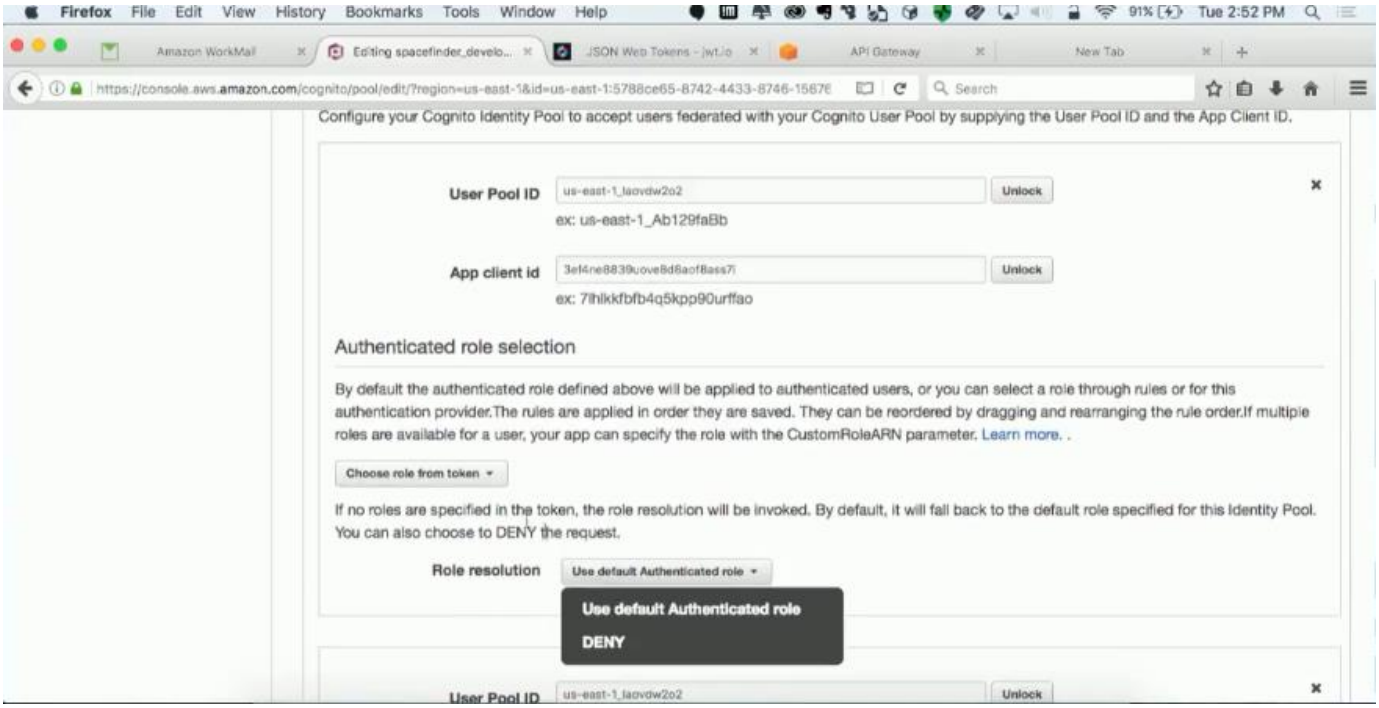


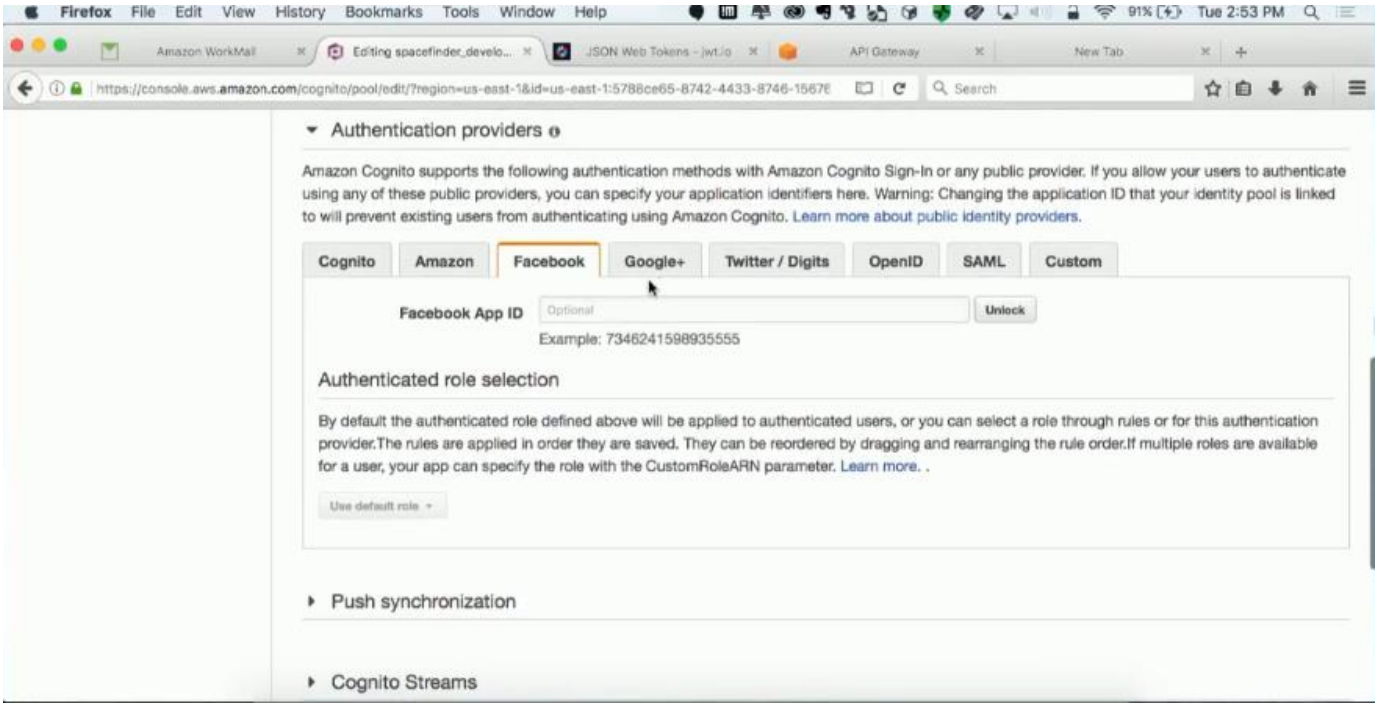

Edit identity pool
From this page you can modify the details of your identity pool. An identity pool must have a unique name and a set of authenticated and unauthenticated roles. The roles are saved with your identity pool and whenever we receive a request to authorize a user we will automatically utilize the roles you specify here. You will be required to specify the identity pool id from this page when initializing the Amazon Cognito client SDK. Learn more about using IAM roles with Amazon Cognito.
Identity pool name*
spacefinder_development
Identity pool ID
us-east-1:5788ce65-8742-4433-8746-156762702bdd (Show ARN)
Unauthenticated role
Authenticated role
Create new role
Unauthenticated identities

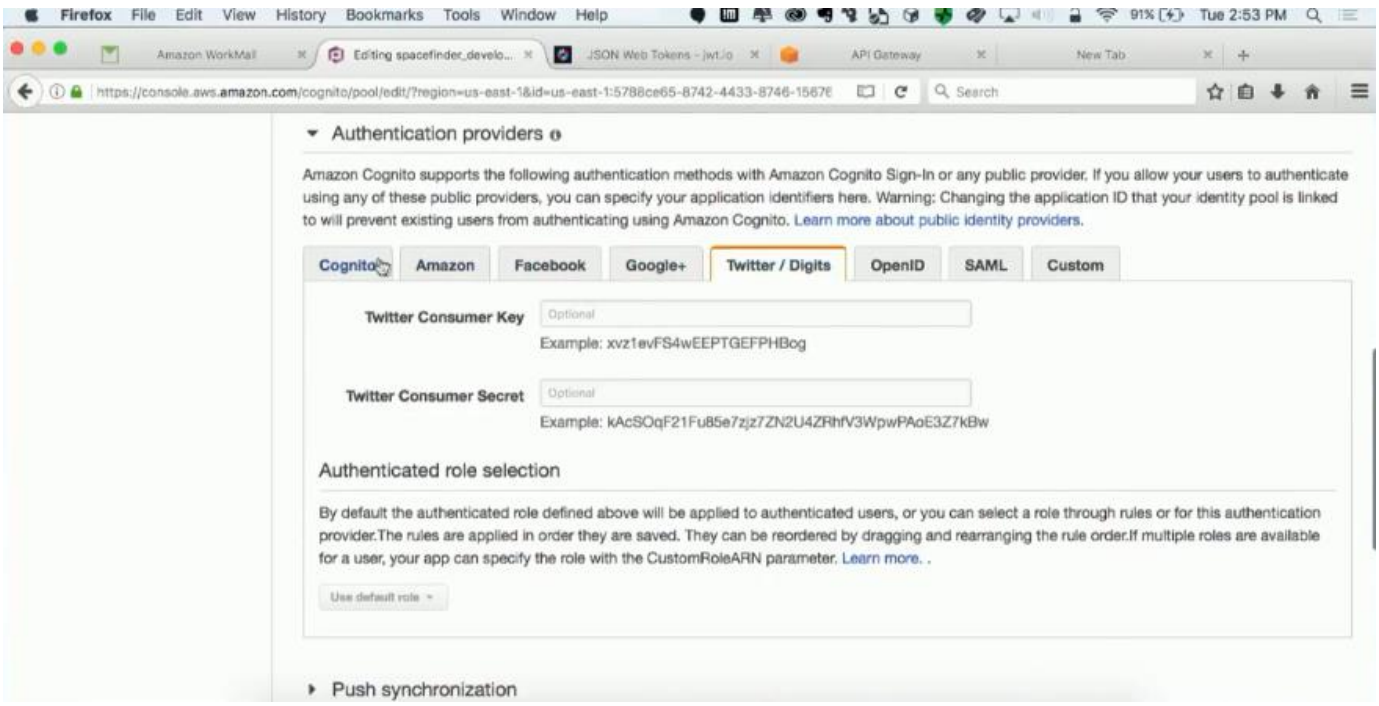

Authenticated role
Create new role
Unauthenticated identities
Authentication providers
Push synchronization
Cognito Streams
Cognito Events
Delete identity pool

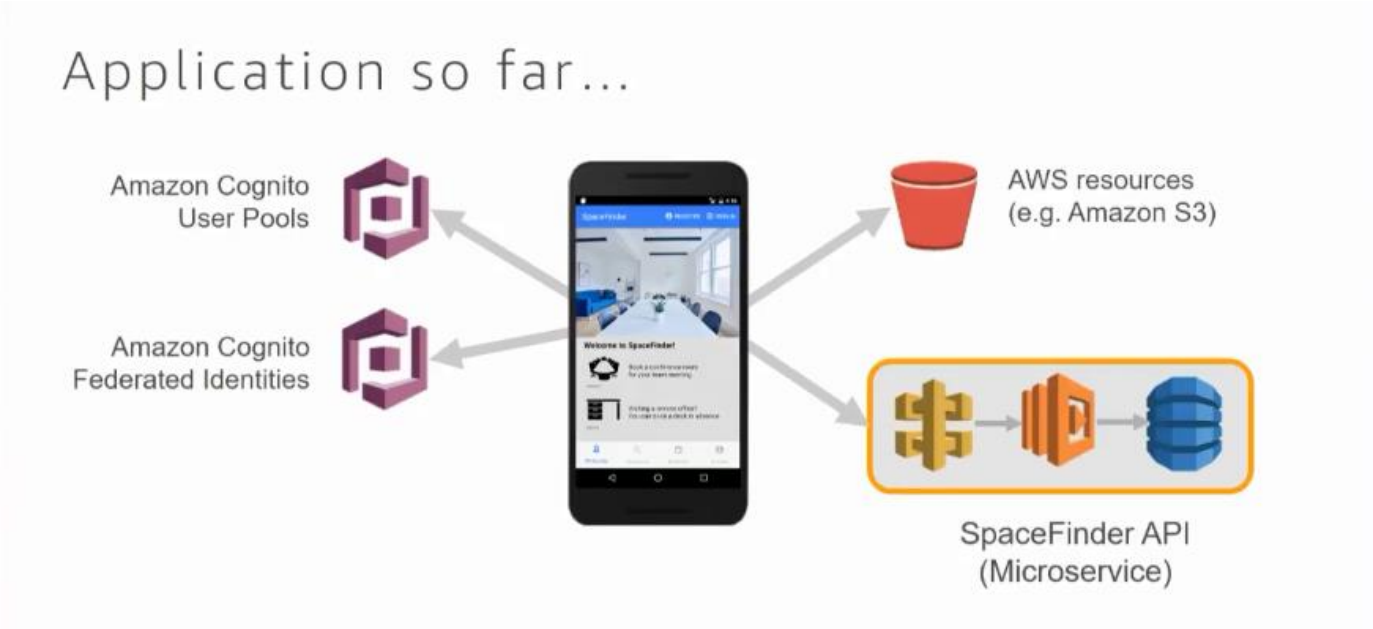


What you see here is a list of available providers that you can integrate within Federated Identities. This means that you can use Cognito to allow your users to sign up and sign in, but you can also use Facebook, Google, OpenID providers too. You can use a Custom login too.

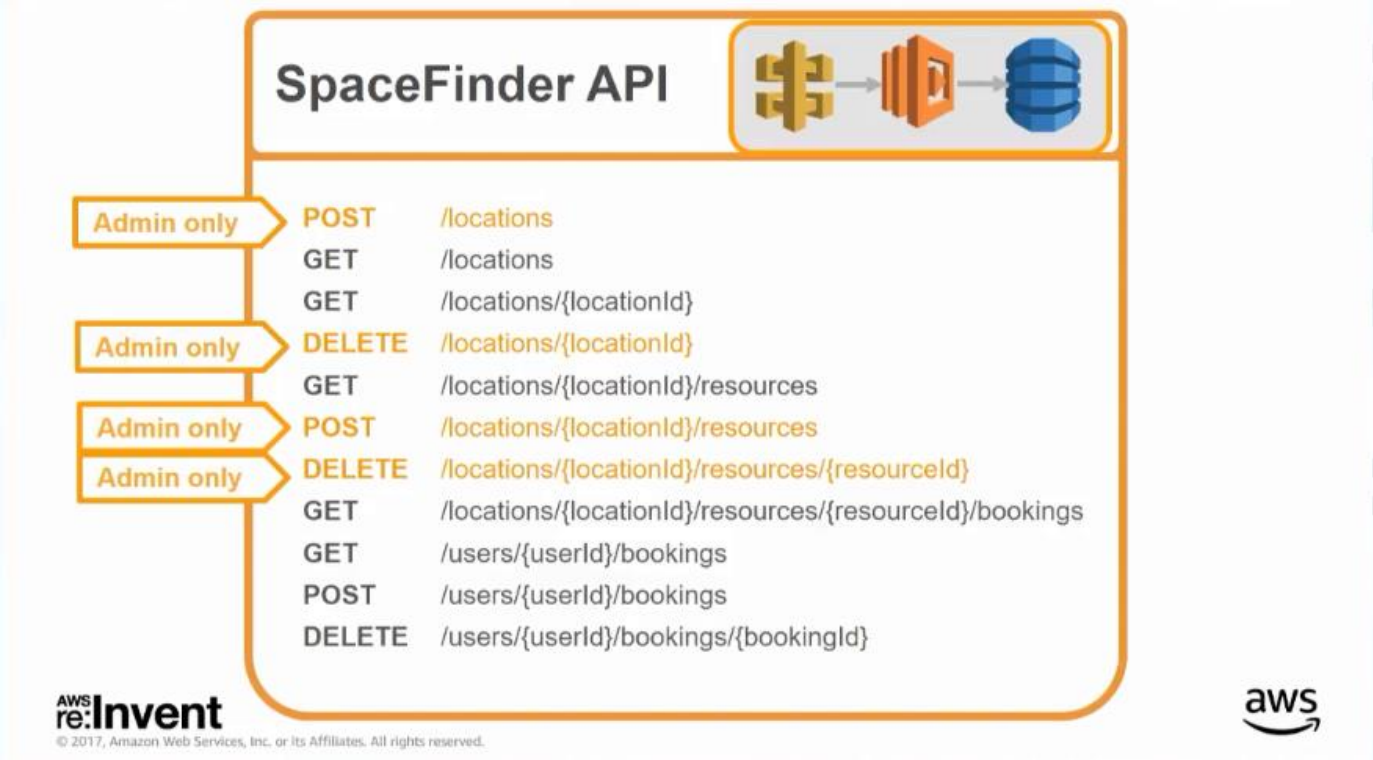



Firefox File Edit View History Bookmarks Tools Window Help
Tue 2:53 PM
Amazon WorkMail
Editing spacefinder_develo...
JSON Web Tokens - jwt.io
API Gateway
New Tab
https://console.aws.amazon.com/cognito/pool/edit/?region=us-east-1&id=us-east-1:5788ce65-8742-4433-8746-1567
Search
Authentication providers
Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.
Cognito
Amazon
Facebook
Google+
Twitter / Digits
OpenID
SAML
Custom
Facebook App ID
Optional
Unlock
Example: 734624159893555
Authenticated role selection
By default the authenticated role defined above will be applied to authenticated users, or you can select a role through rules or for this authentication provider.The rules are applied in order they are saved. They can be reordered by dragging and rearranging the rule order.If multiple roles are available for a user, your app can specify the role with the CustomRoleARN parameter. Learn more. .
Use default role
Push synchronization
Cognito Streams

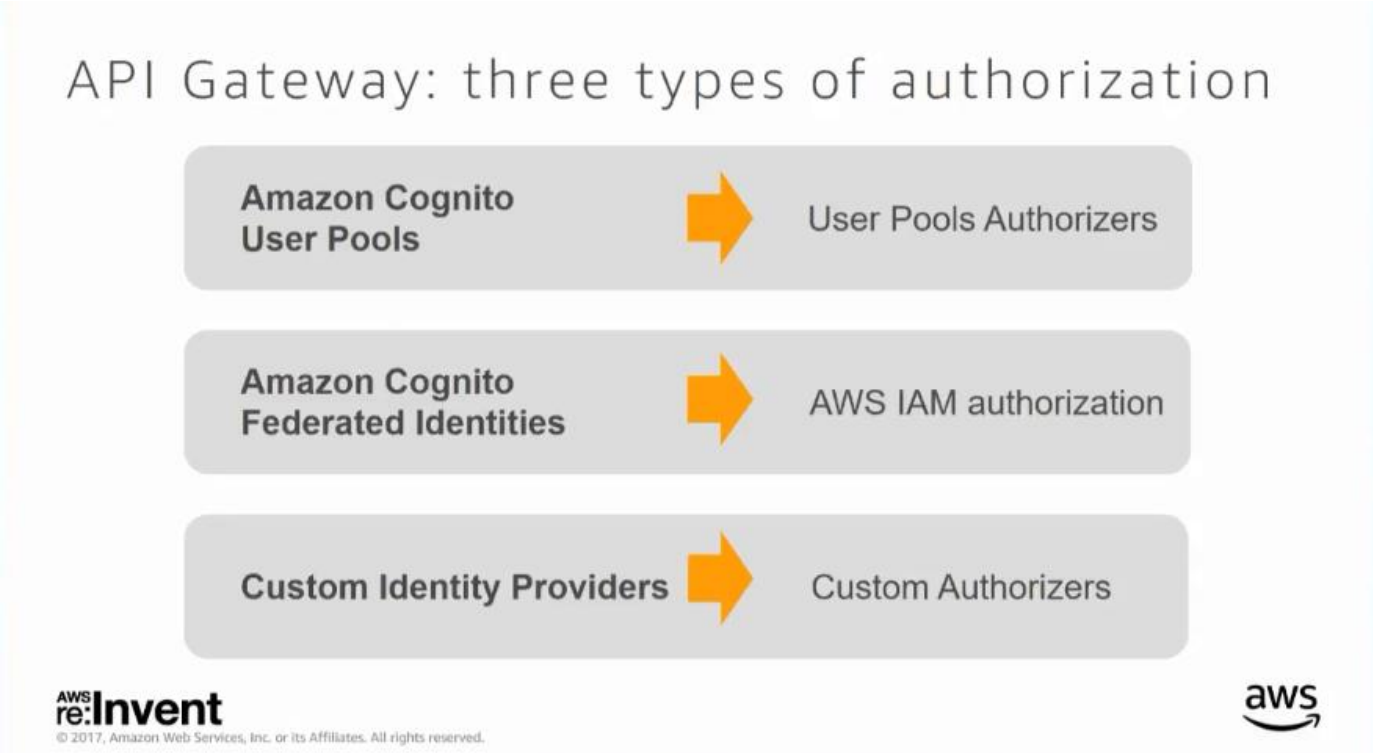

Firefox File Edit View History Bookmarks Tools Window Help
Tue 2:53 PM
Amazon WorkMail
Editing spacefinder_develo...
JSON Web Tokens - jwt.io
API Gateway
New Tab
https://console.aws.amazon.com/cognito/pool/edit/?region=us-east-1&id=us-east-1:5788ce65-8742-4433-8746-1567
Search
Authentication providers
Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you allow your users to authenticate using any of these public providers, you can specify your application identifiers here. Warning: Changing the application ID that your identity pool is linked to will prevent existing users from authenticating using Amazon Cognito. Learn more about public identity providers.
Cognito
Amazon
Facebook
Google+
Twitter / Digits
OpenID
SAML
Custom
Twitter Consumer Key
Optional
Example: xvz1evFS4wEEPTGEFPHBog
Twitter Consumer Secret
Optional
Example: kAcSOqF21Fu85e7zjz7ZN2U4ZRhfV3WpwPAoE3Z7kBw
Authenticated role selection
By default the authenticated role defined above will be applied to authenticated users, or you can select a role through rules or for this authentication provider.The rules are applied in order they are saved. They can be reordered by dragging and rearranging the rule order.If multiple roles are available for a user, your app can specify the role with the CustomRoleARN parameter. Learn more. .
Use default role
Push synchronization



Now we are ready for the business logic. We can use API Gateway, Lambda, and DynamoDB as below. You are able to offload all the authentication and authorization decisions of your business logic to the API Gateway

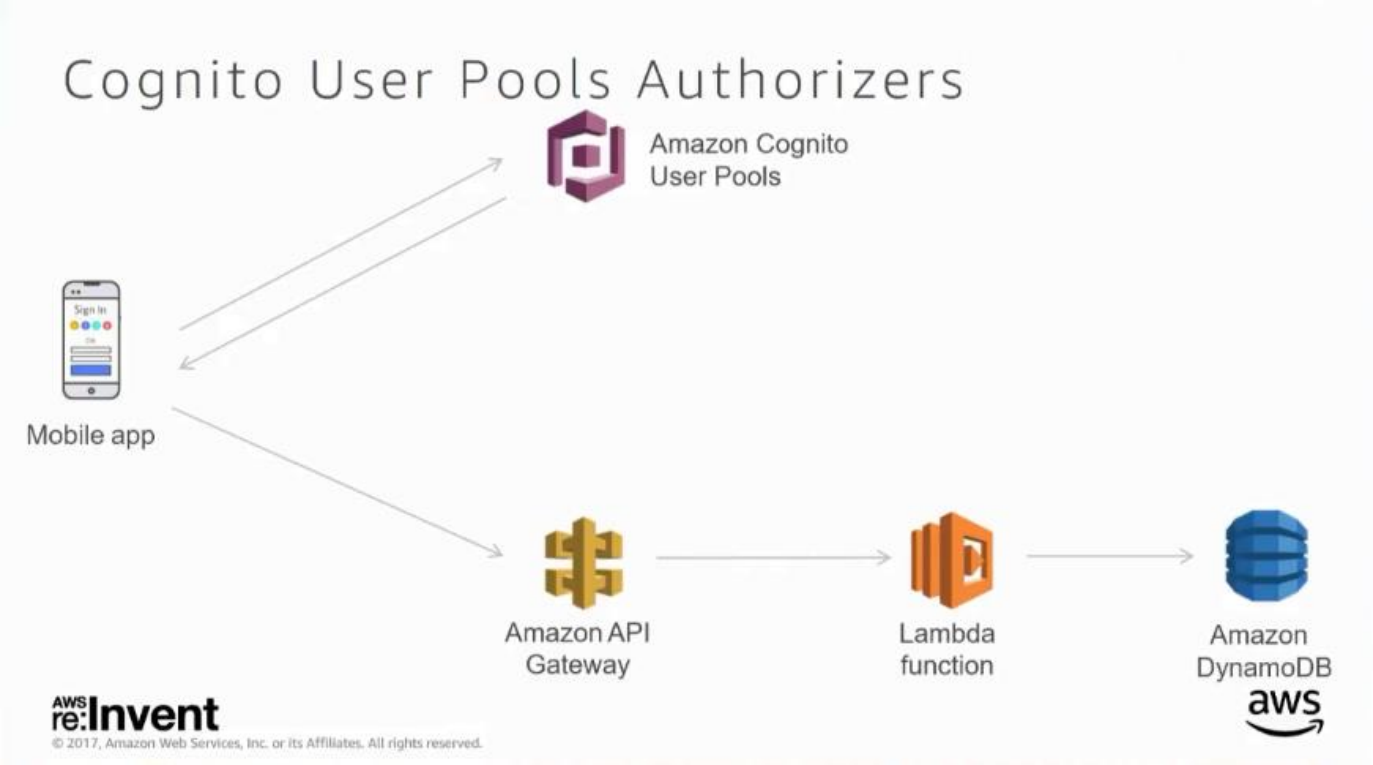


Within the API, we have admin only operations as above. We want only admin users of our User pool to be able to call and get responses from those admin-only APIs.

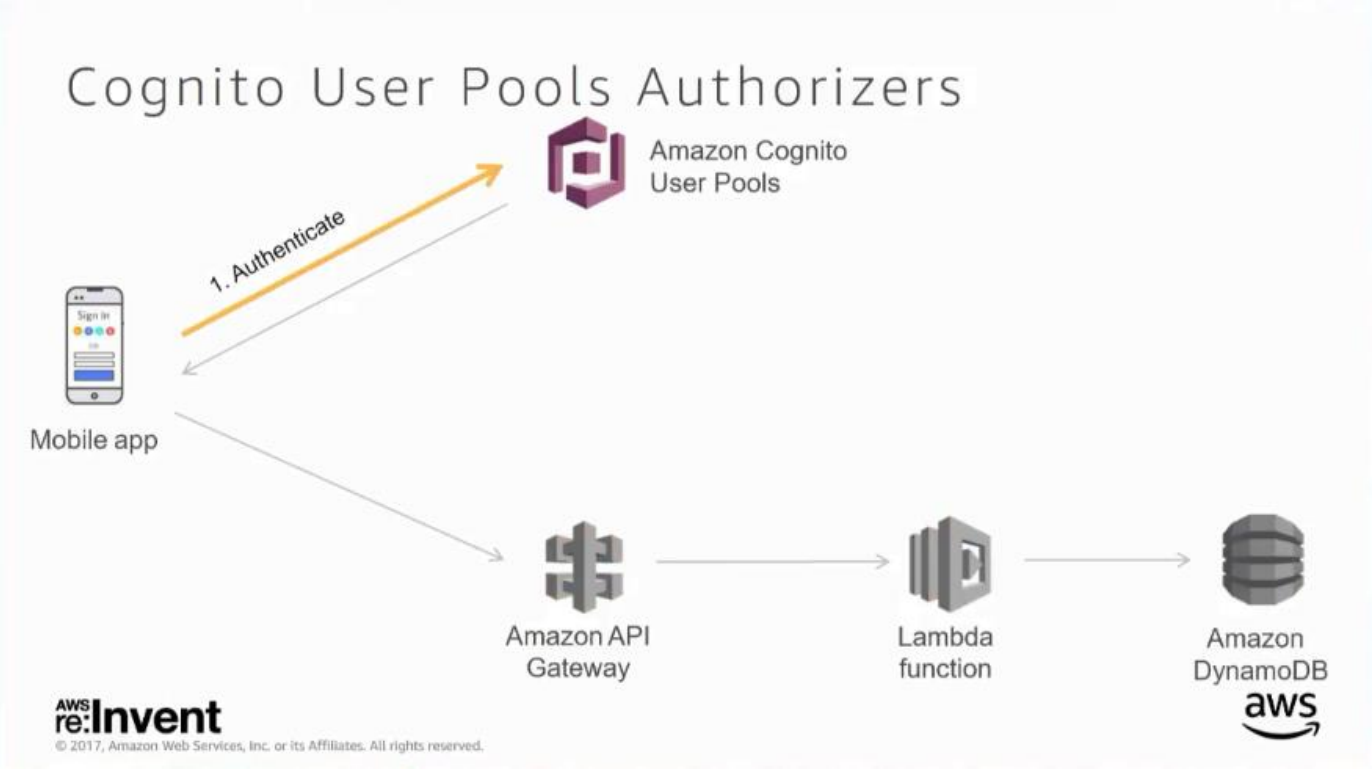


There are 3 different types of authorization options available.

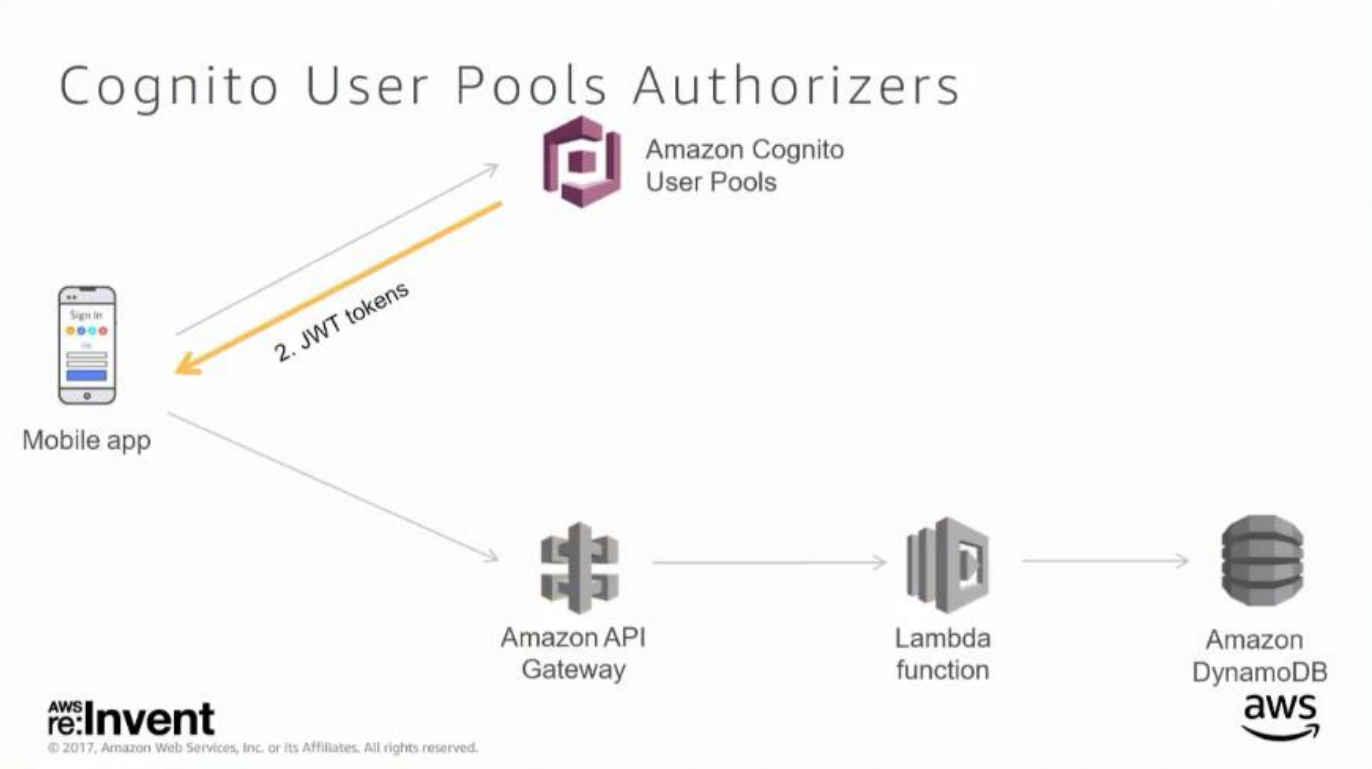
This type can only check if a user belongs to our User Pool, it is not going to be able to different our admin users from ordinary users.



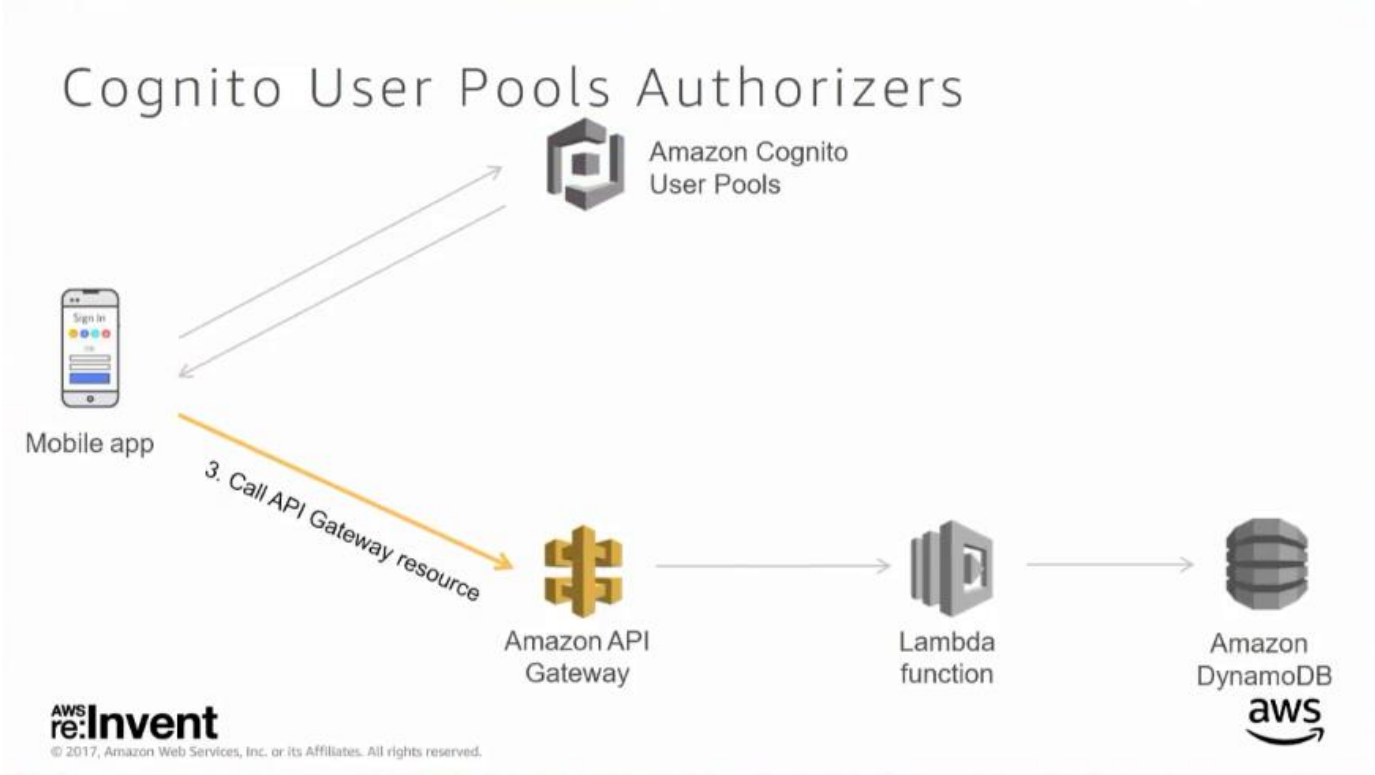
If you have users that are using Cognito User Pools, this can work as described below



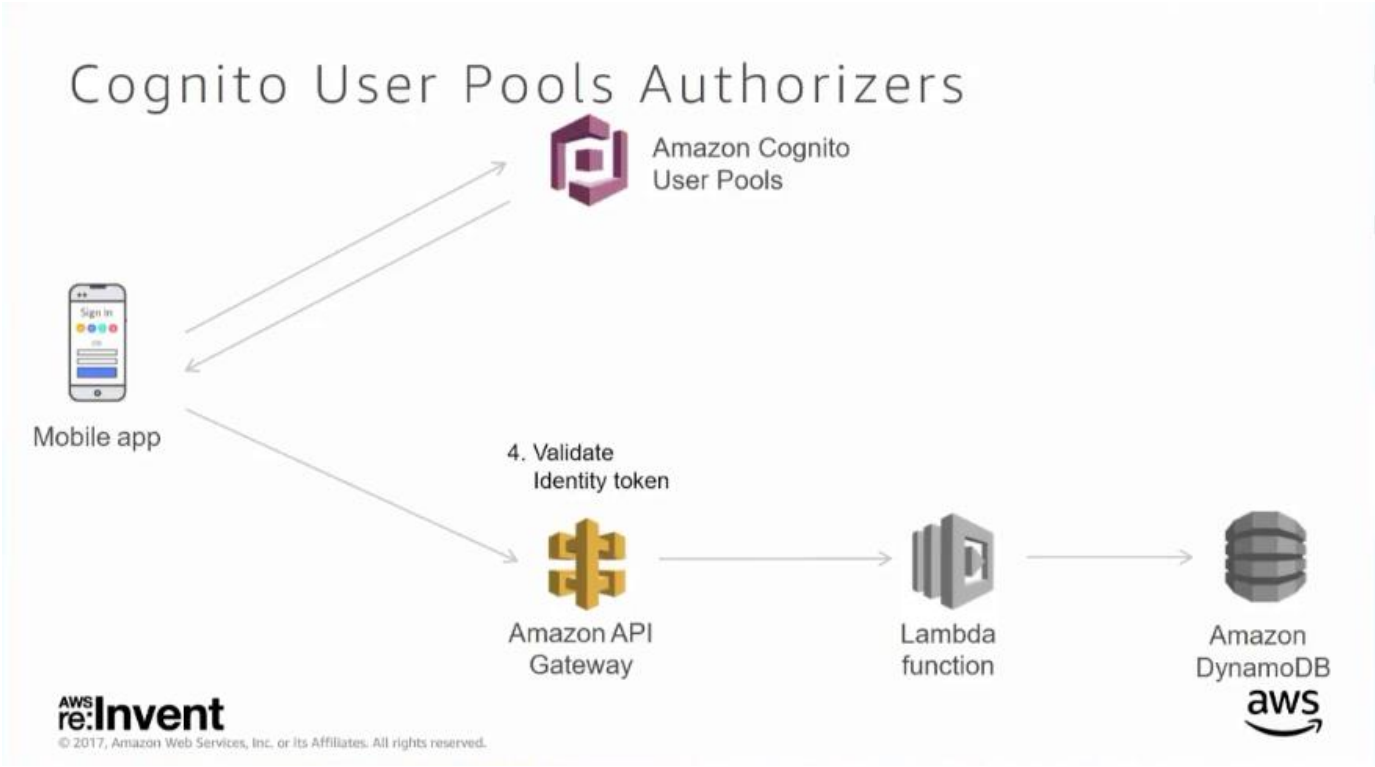
You first have those users authenticate with Cognito User Pools,



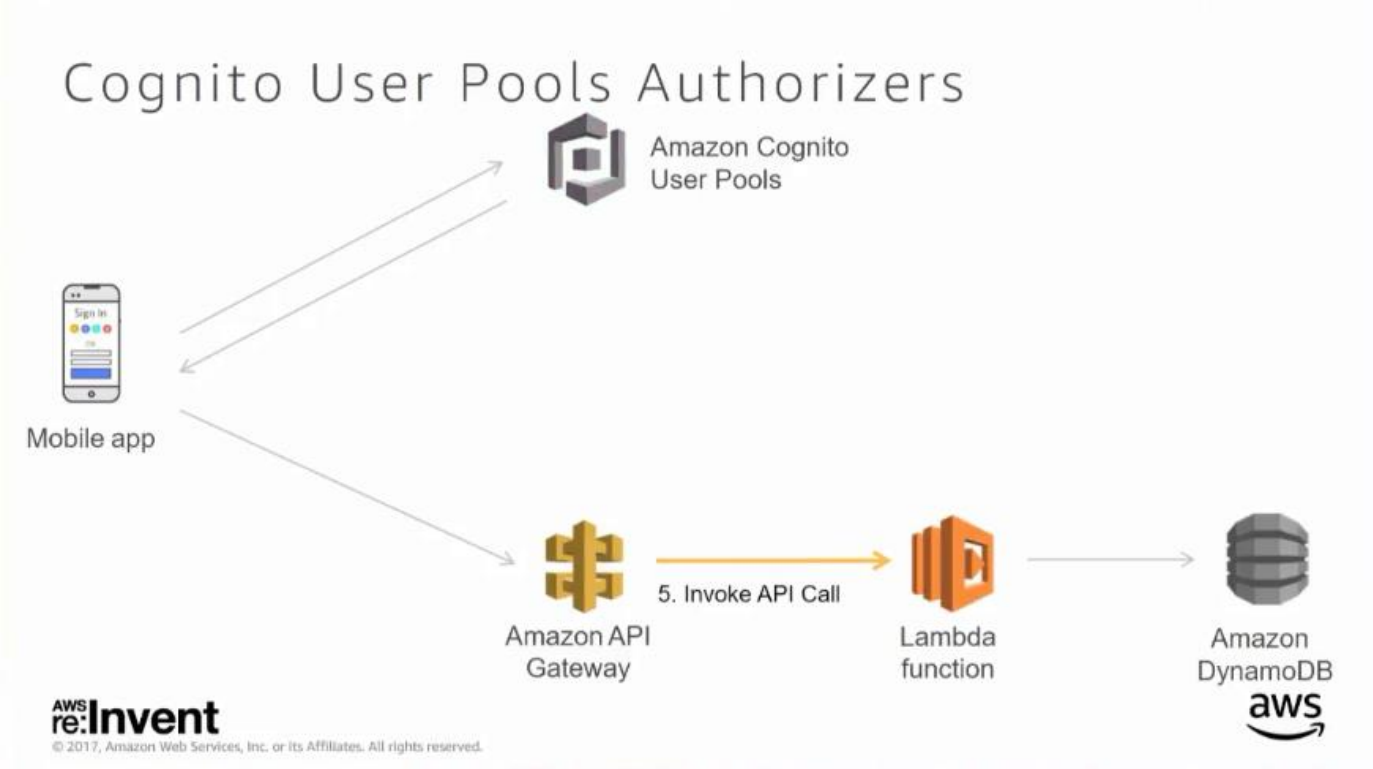
They then get back a set of JWT tokens



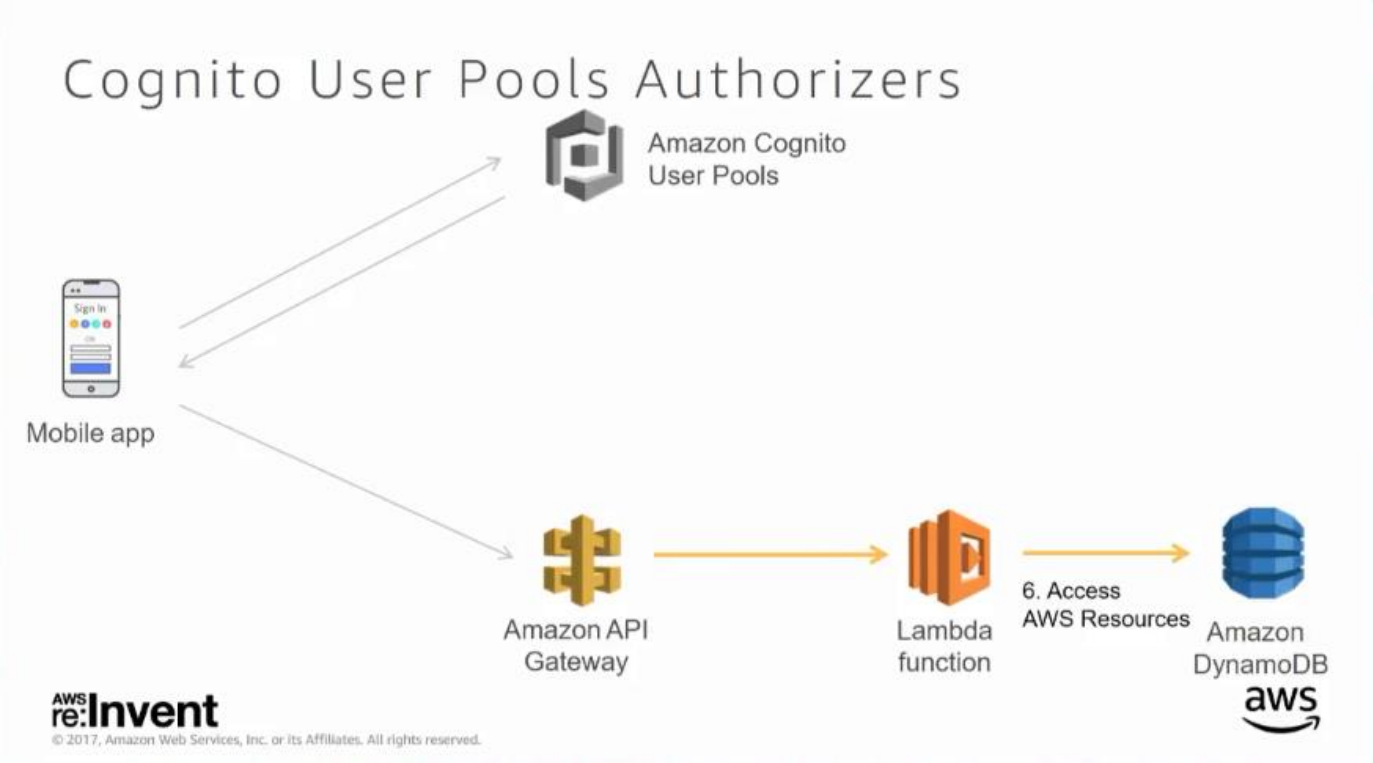
You then take the Identity token and sent it to API Gateway with the header of your choice in your request, most likely in the authorization header.



API Gateway can then read the token, check its signature, check if the token is still valid since an Identity token is only good for 1 hour,

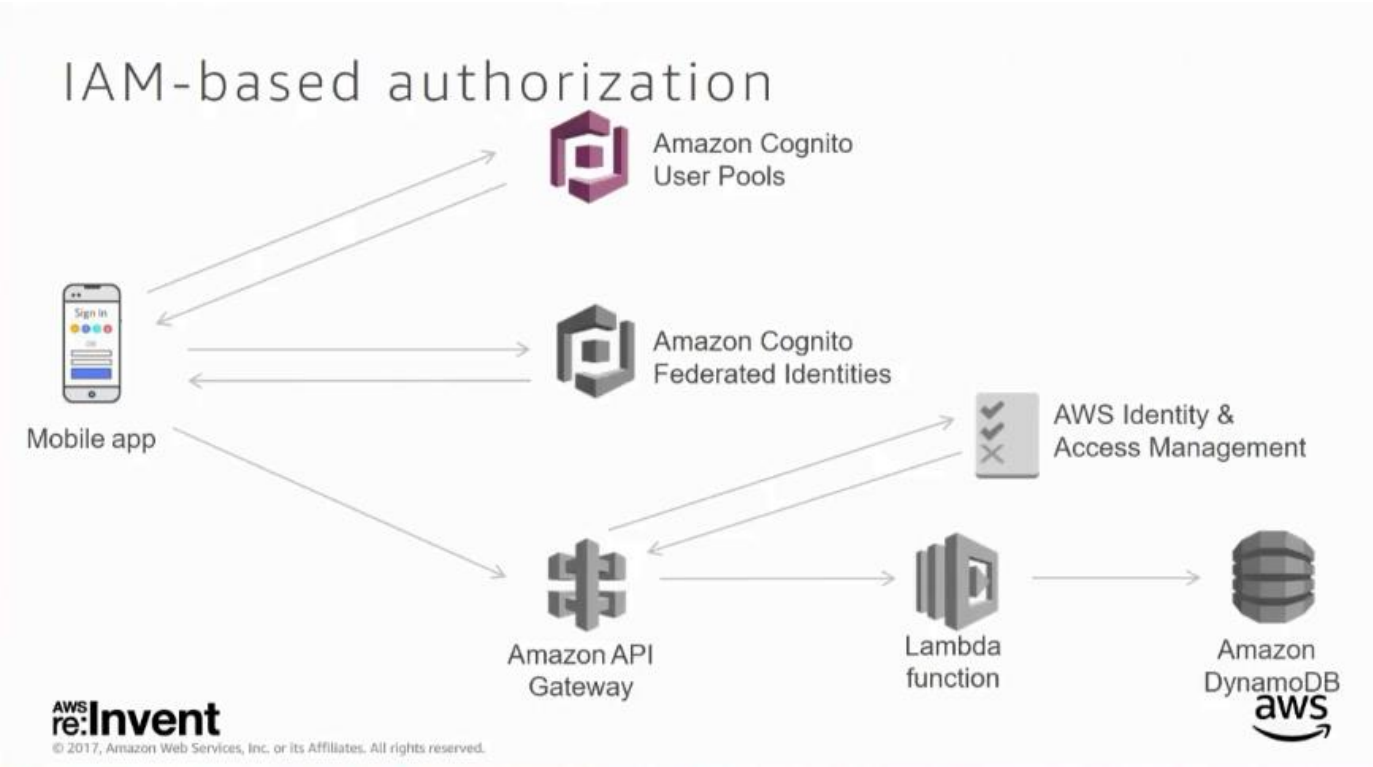


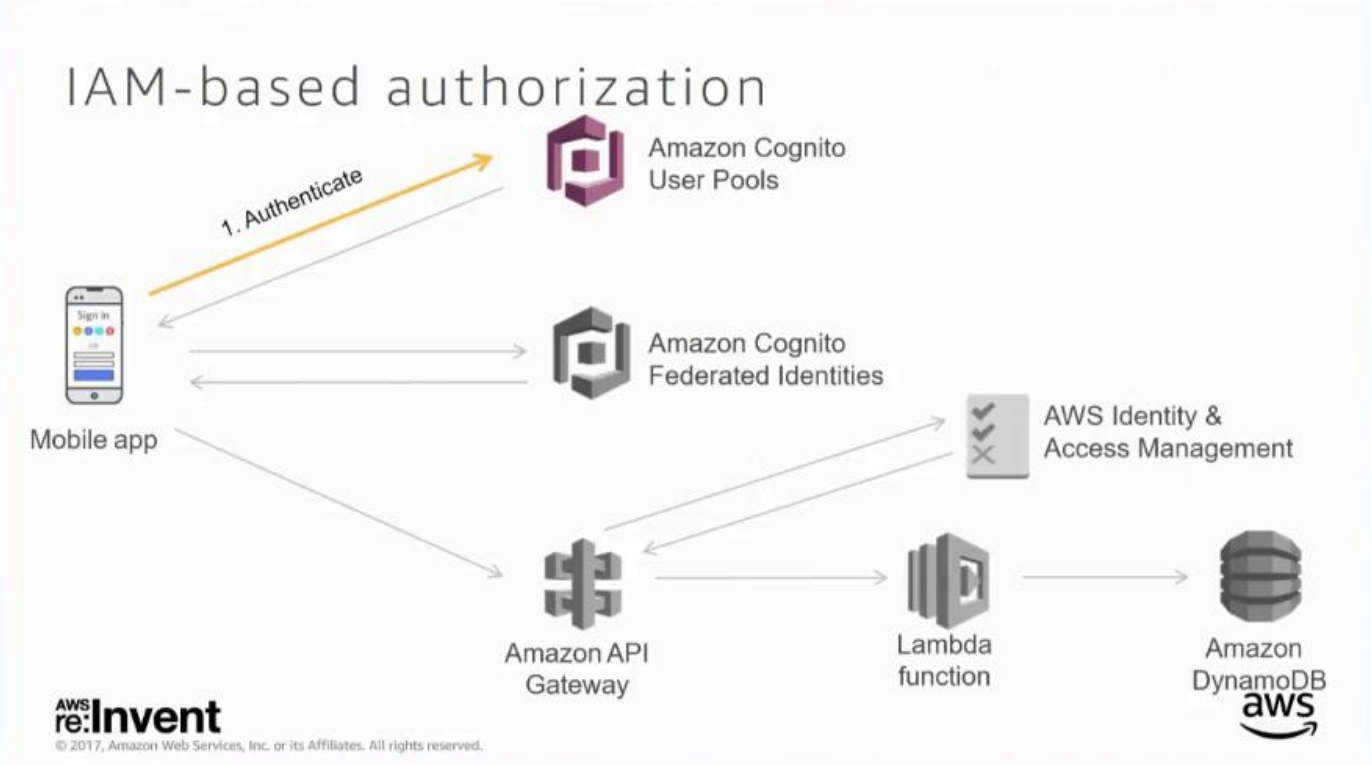
Only if the Identity token is valid will the API Gateway go ahead and invoke the lambda function of interest.

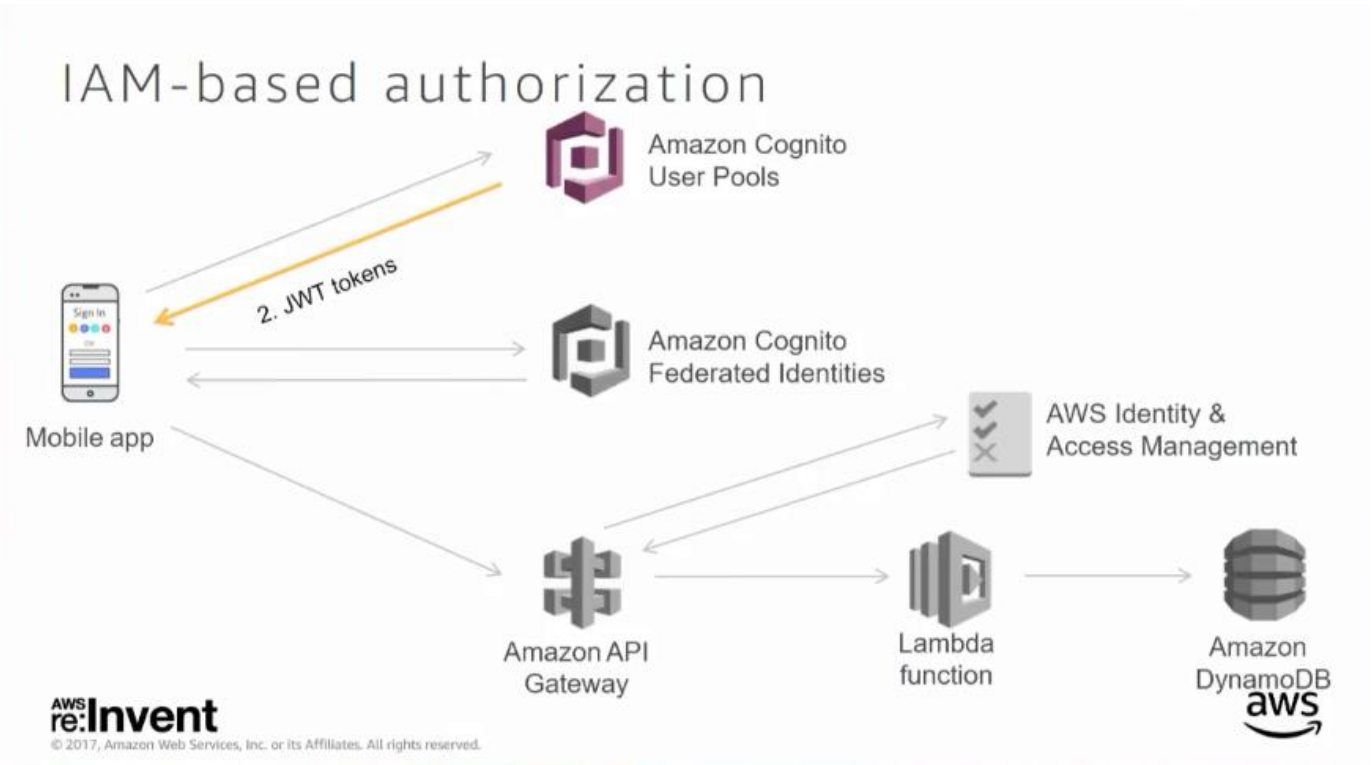


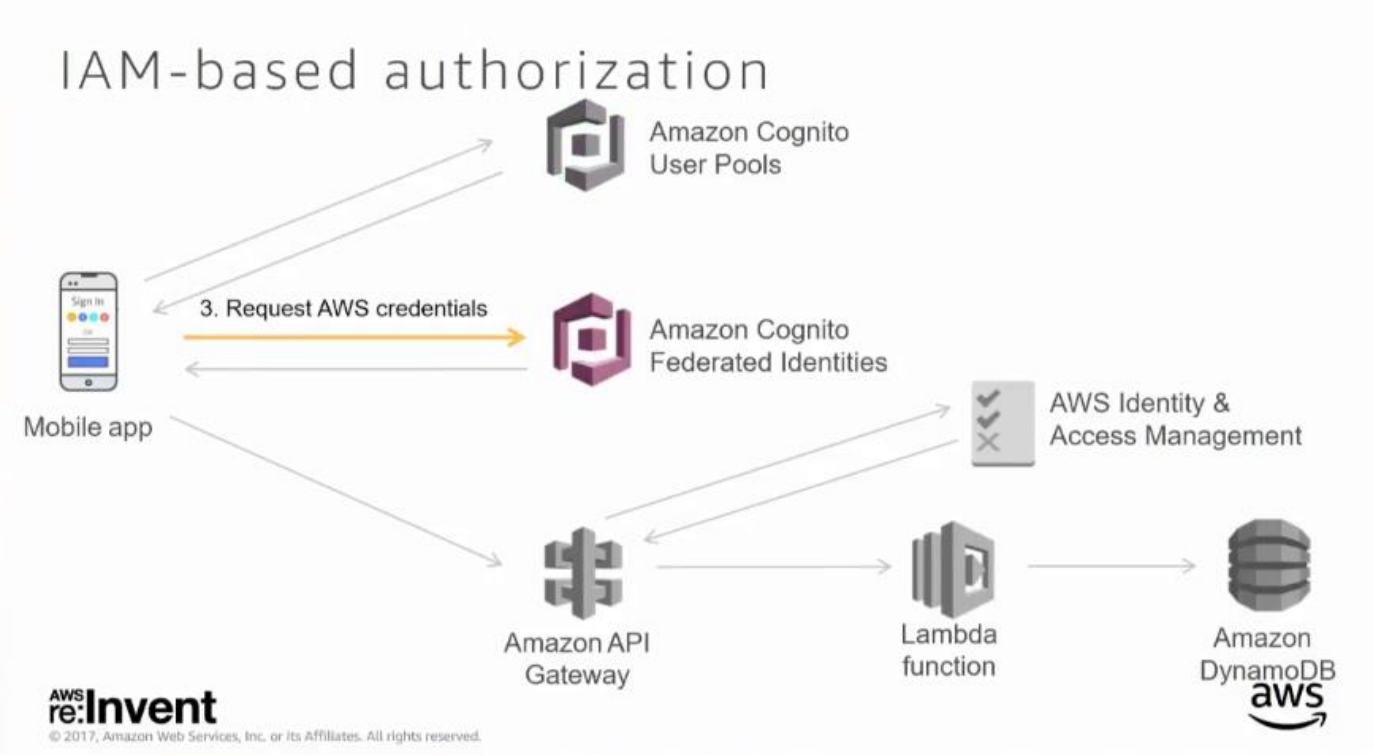
The lambda can then use the IAM execution role (specific to each lambda function) that allows it to talk to other AWS resources like DynamoDB.

AWS IAM based authorization option

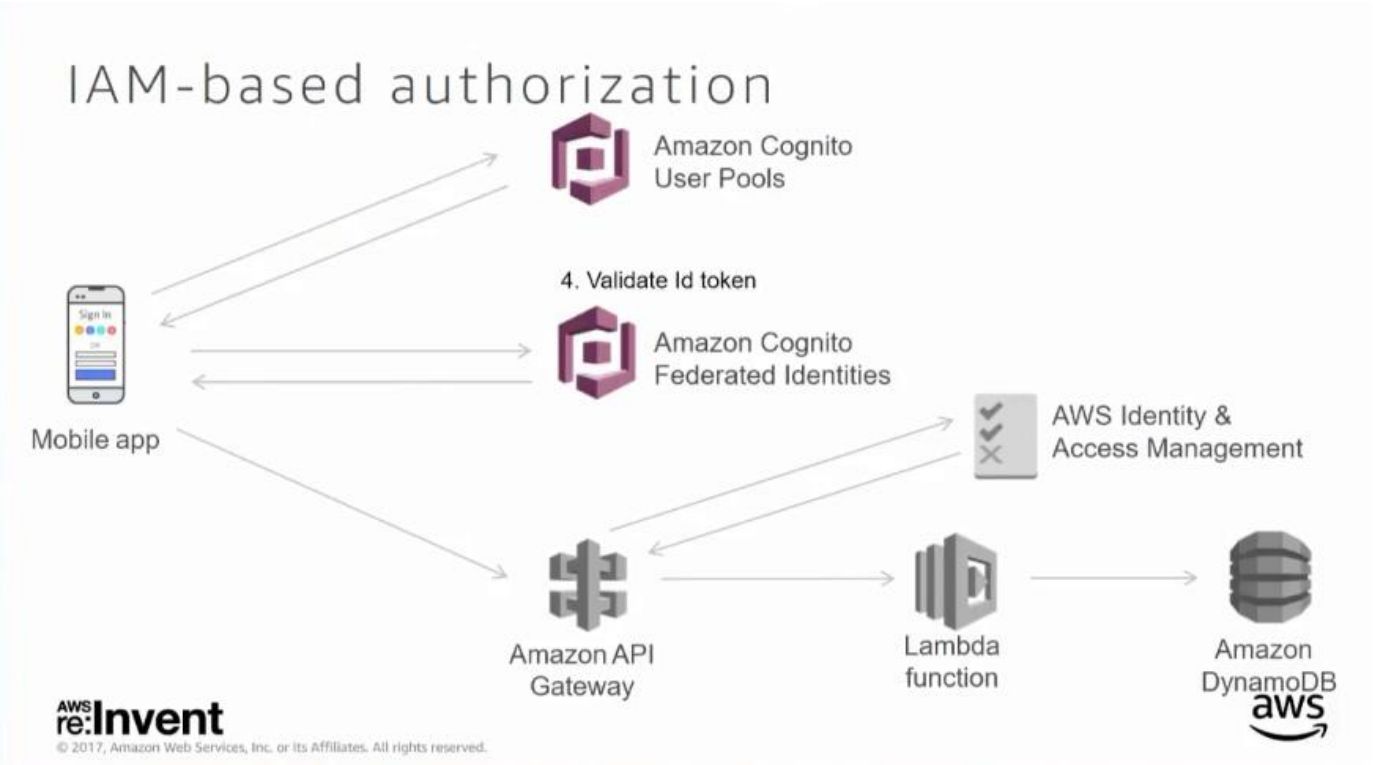



IAM-based authorization
Amazon Cognito
User Pools
1. Authenticate
Sign In
Amazon Cognito
Federated Identities
Mobile app
AWS Identity &
Access Management
Amazon API
Gateway
Lambda
function
Amazon
DynamoDB
aws
re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

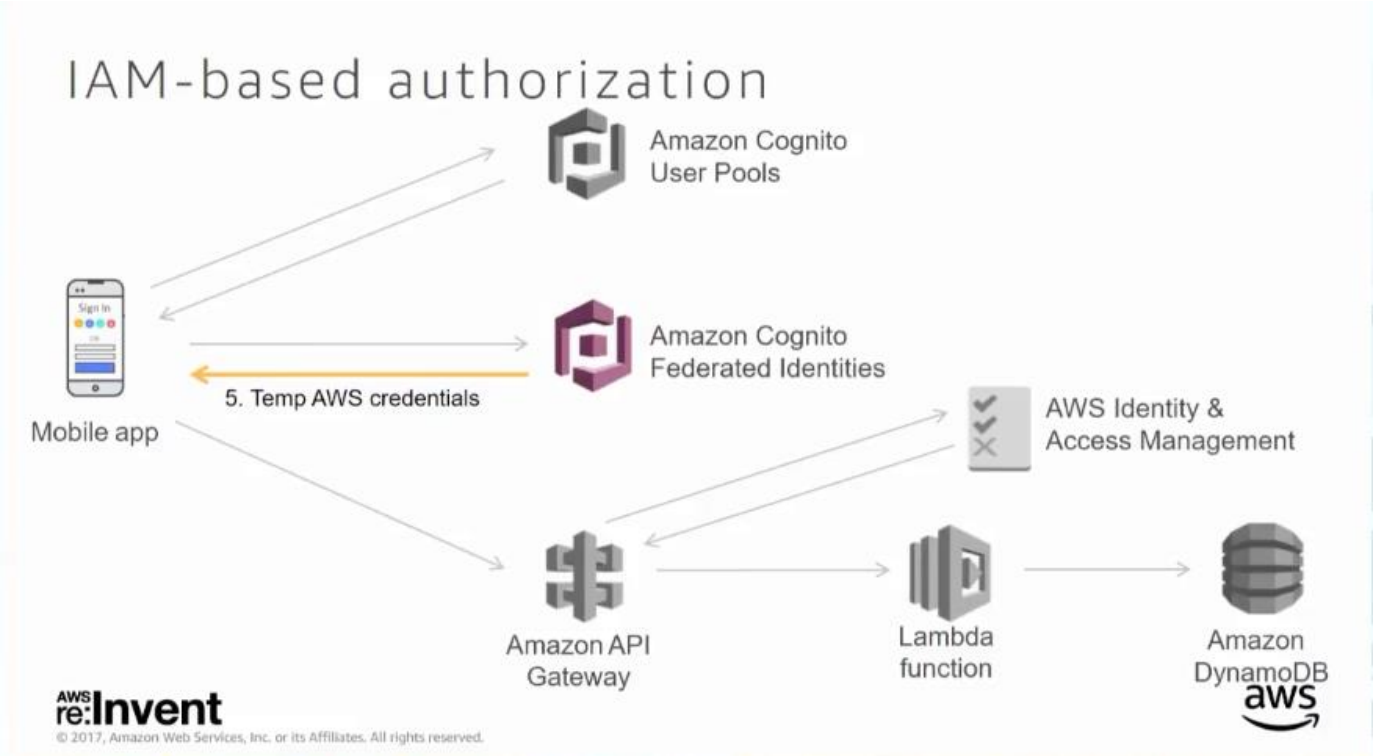

IAM-based authorization
Amazon Cognito
User Pools
2. JWT tokens
Sign In
Amazon Cognito
Federated Identities
Mobile app
AWS Identity &
Access Management
Amazon API
Gateway
Lambda
function
Amazon
DynamoDB
aws
re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

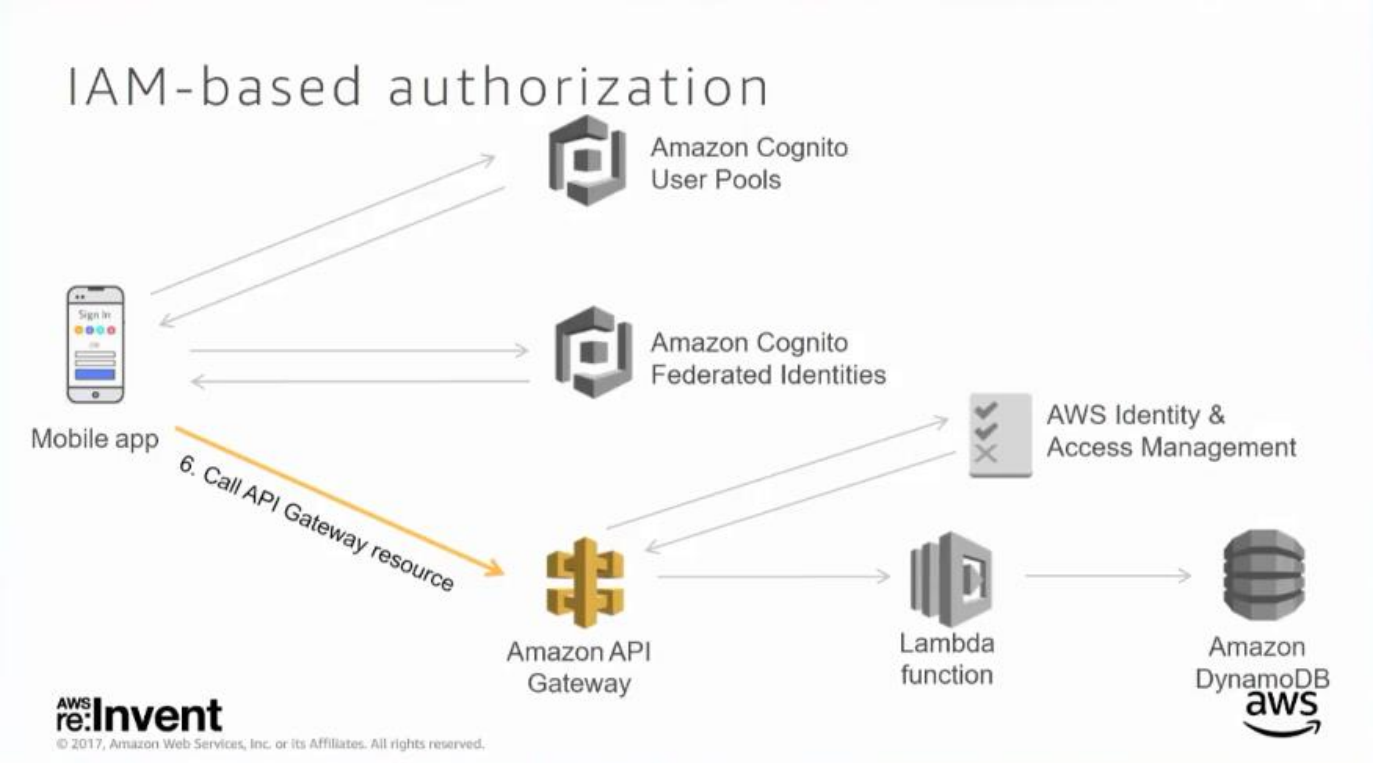


You then get your IAM Role by requesting your credentials,

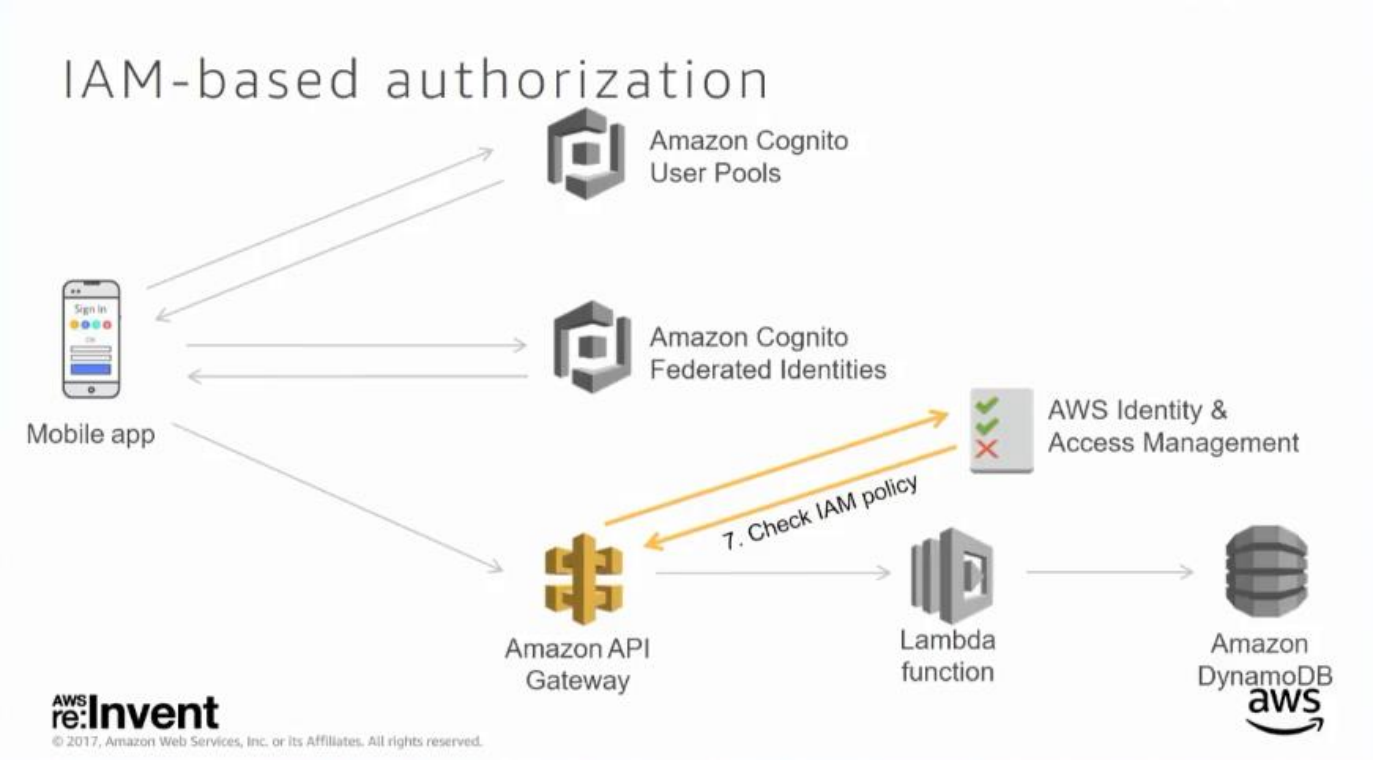


Cognito takes care of the token validation behind the scenes

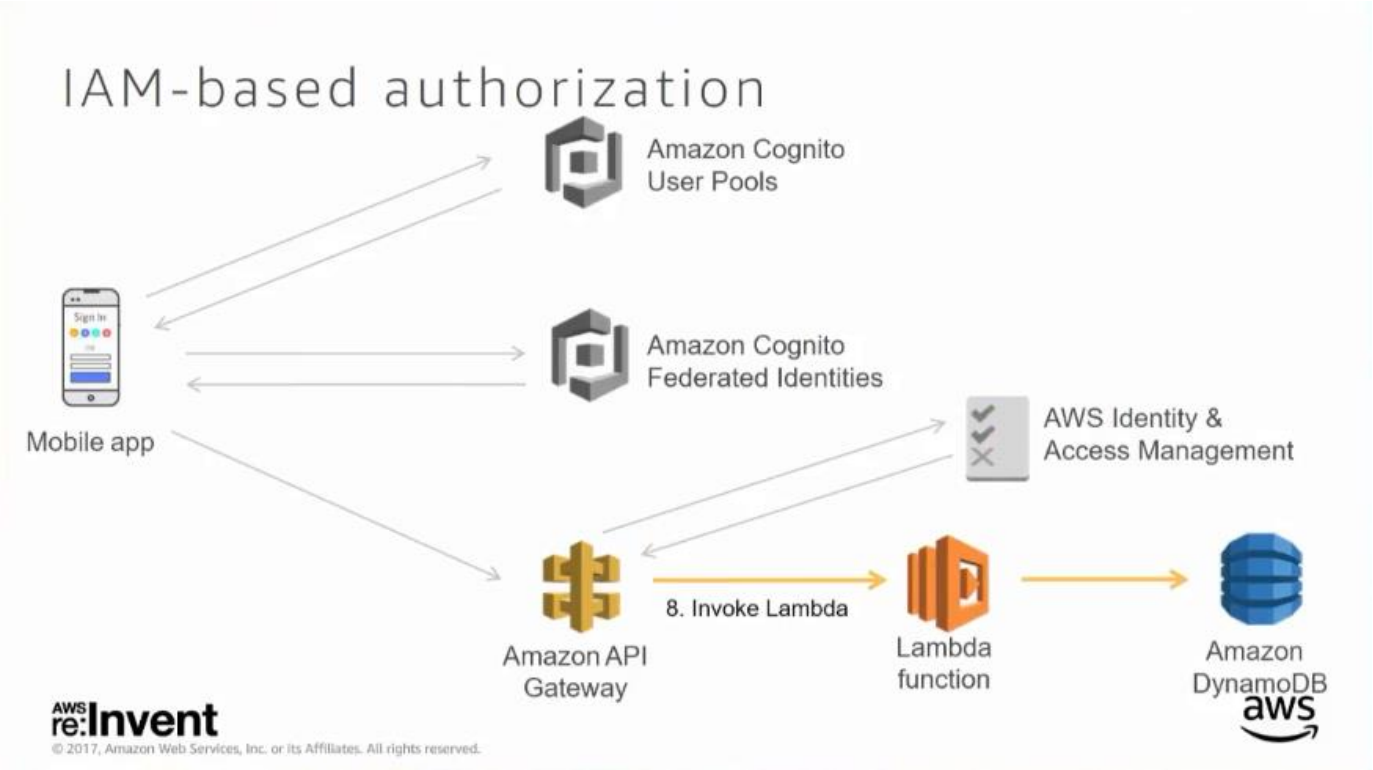




You can then send your requests to PAI Gateway, signing it with a process called ‘signature-before’.

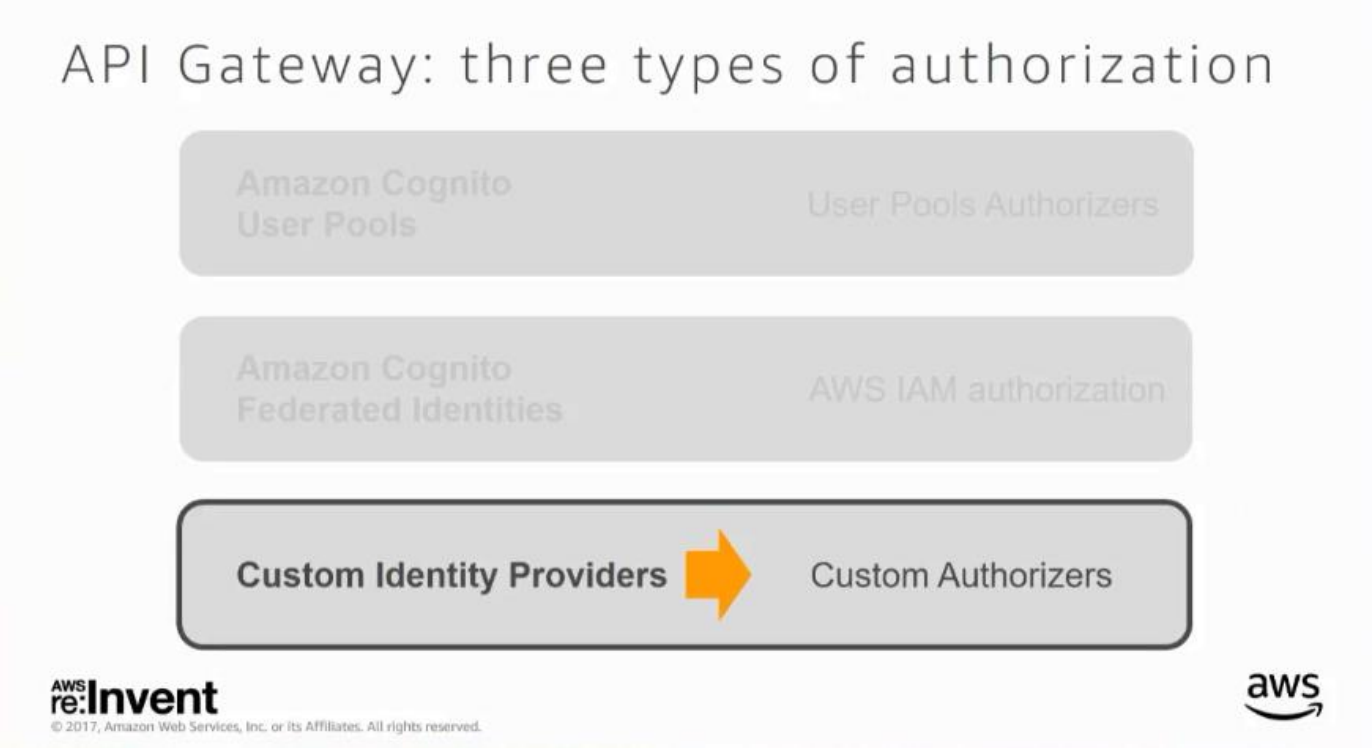


API Gateway is able to extract from the signature which role is used for singing the request, and it will check what policies that role is associated with.

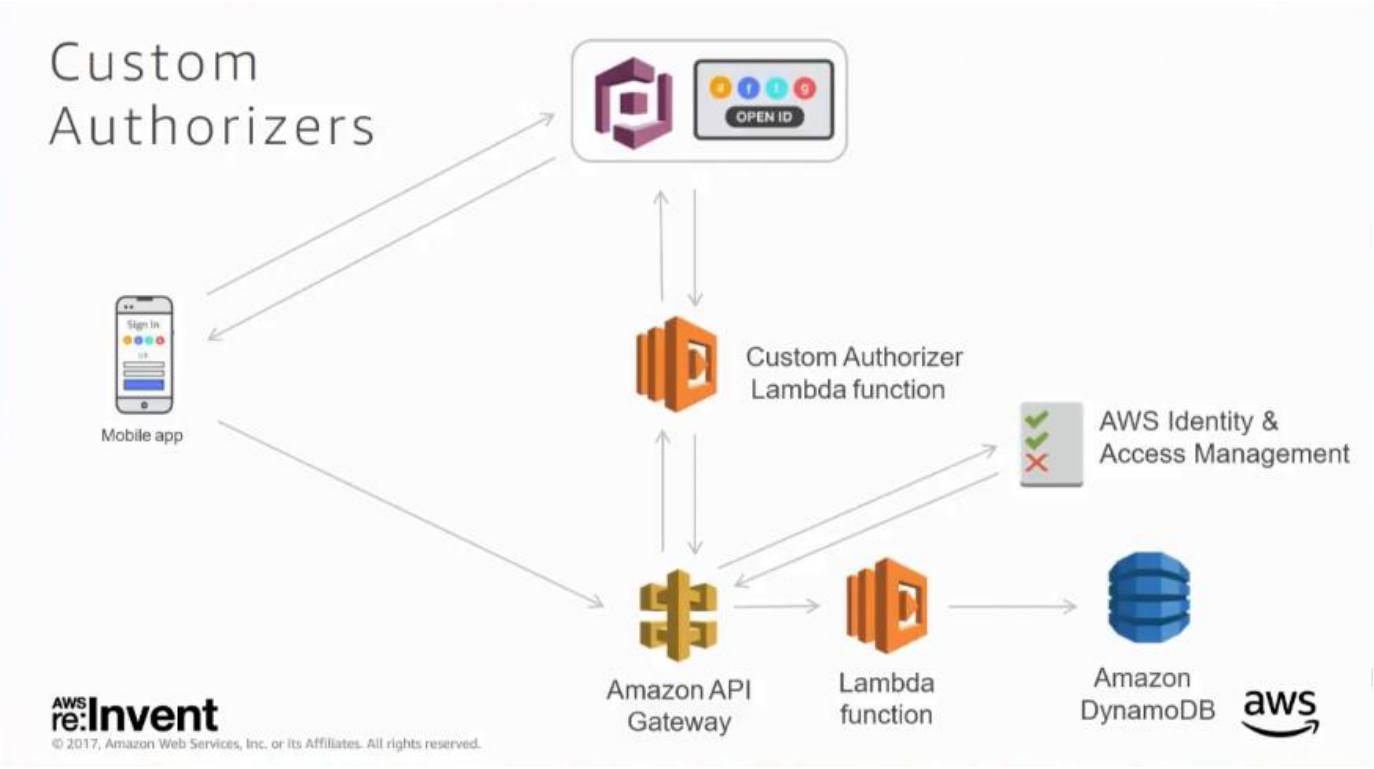


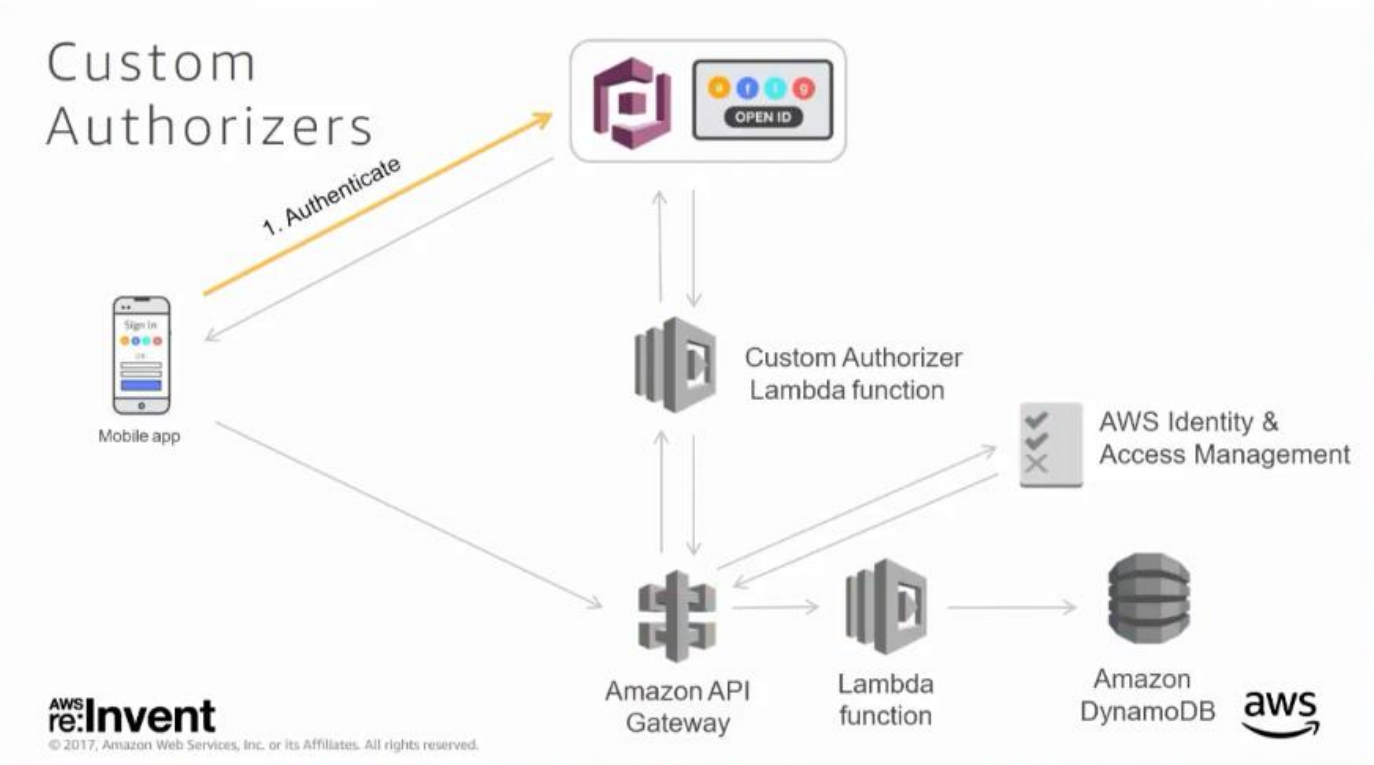
Based on the policy, API Gateway is able to determine if the user can perform the requested operation.

This is a simple IAM Policy, this policy allows the user to access all operations on the API ***except*** the specified POST on the specified path.

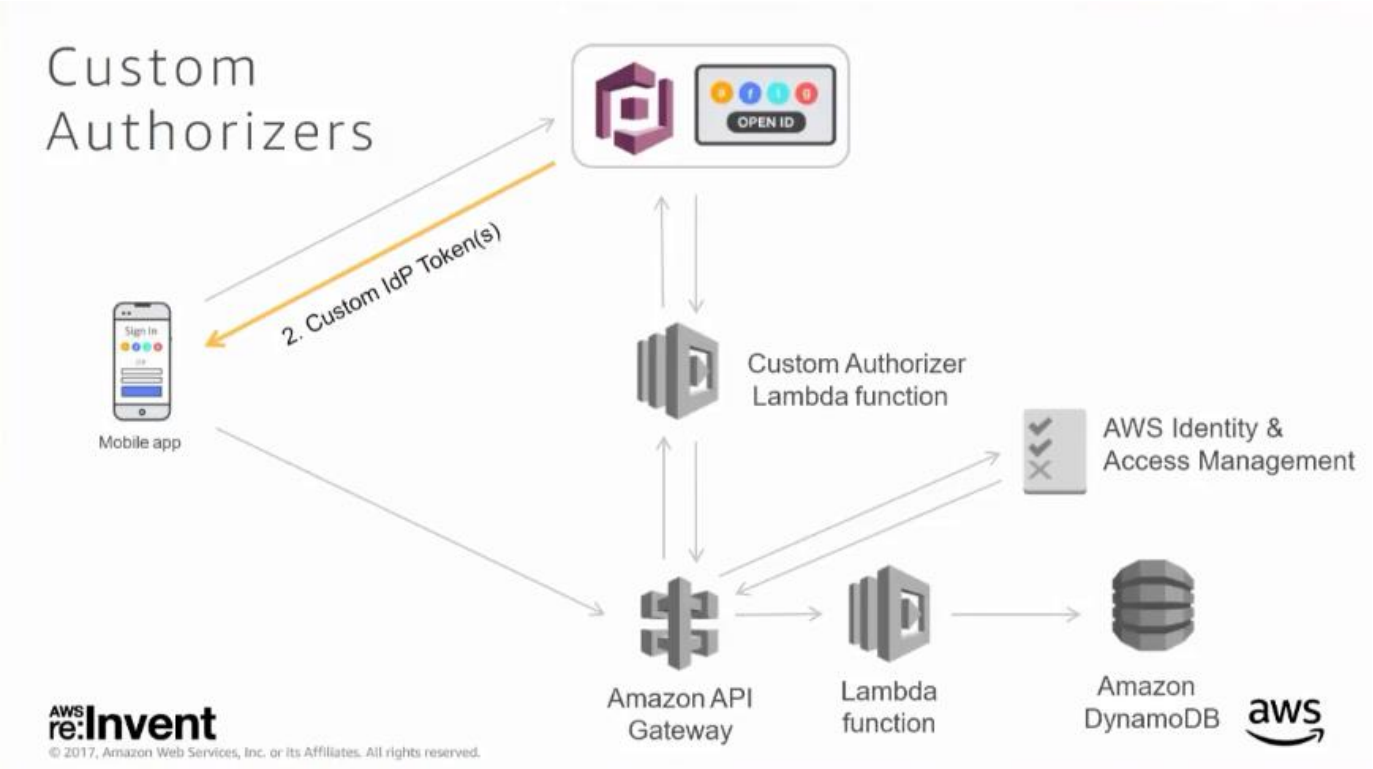


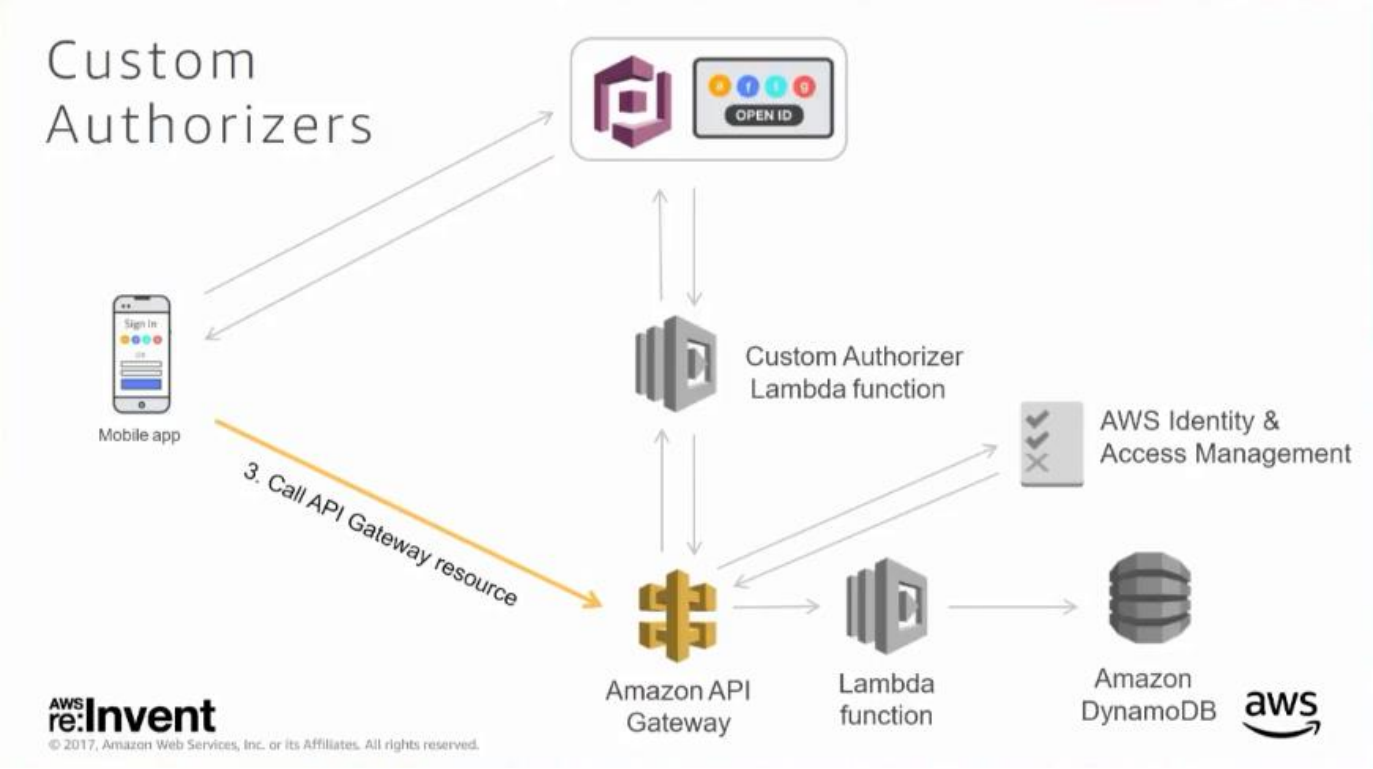
The Custom Authorizer option uses lambda functions



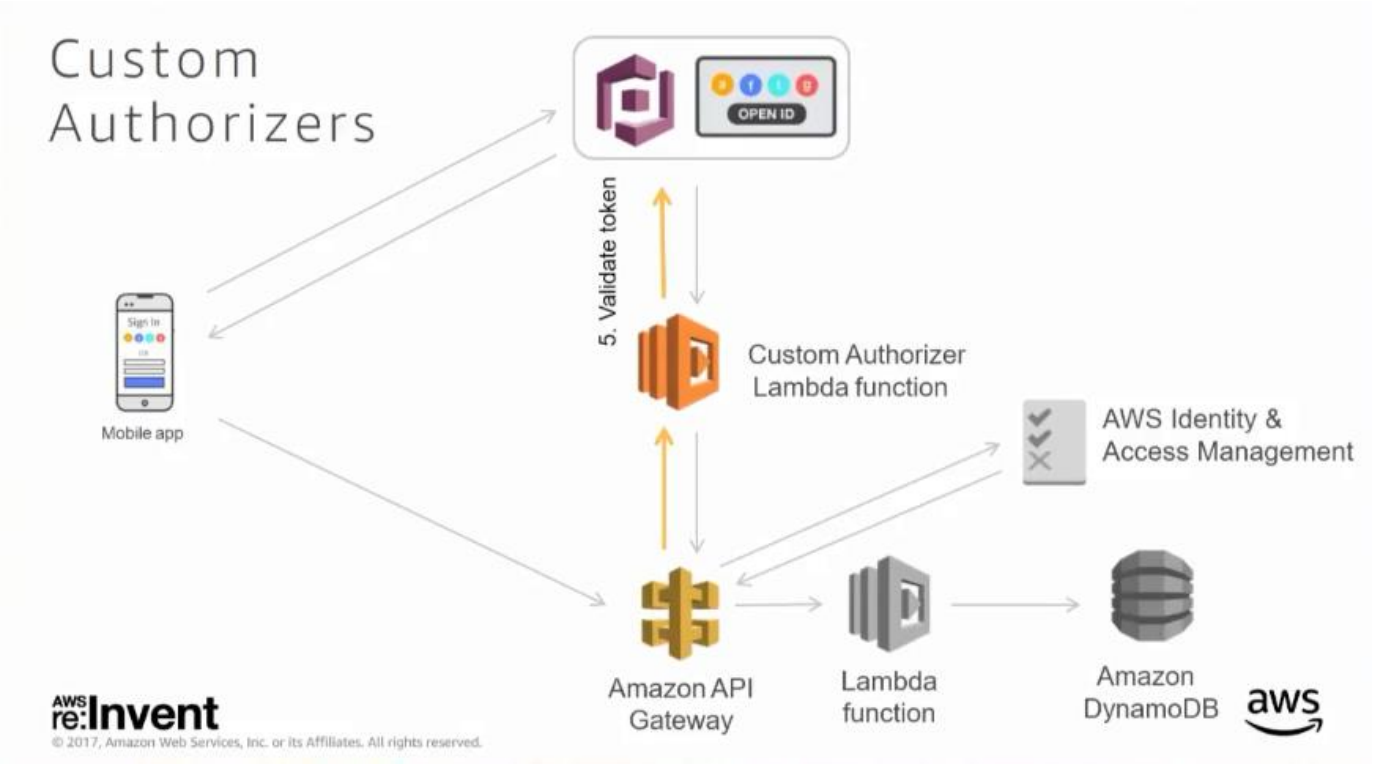


First you authenticate with your identity provider of choice, you don't have to use Cognito at all, as long s you have an identity provider that can provide a bearer token for you.

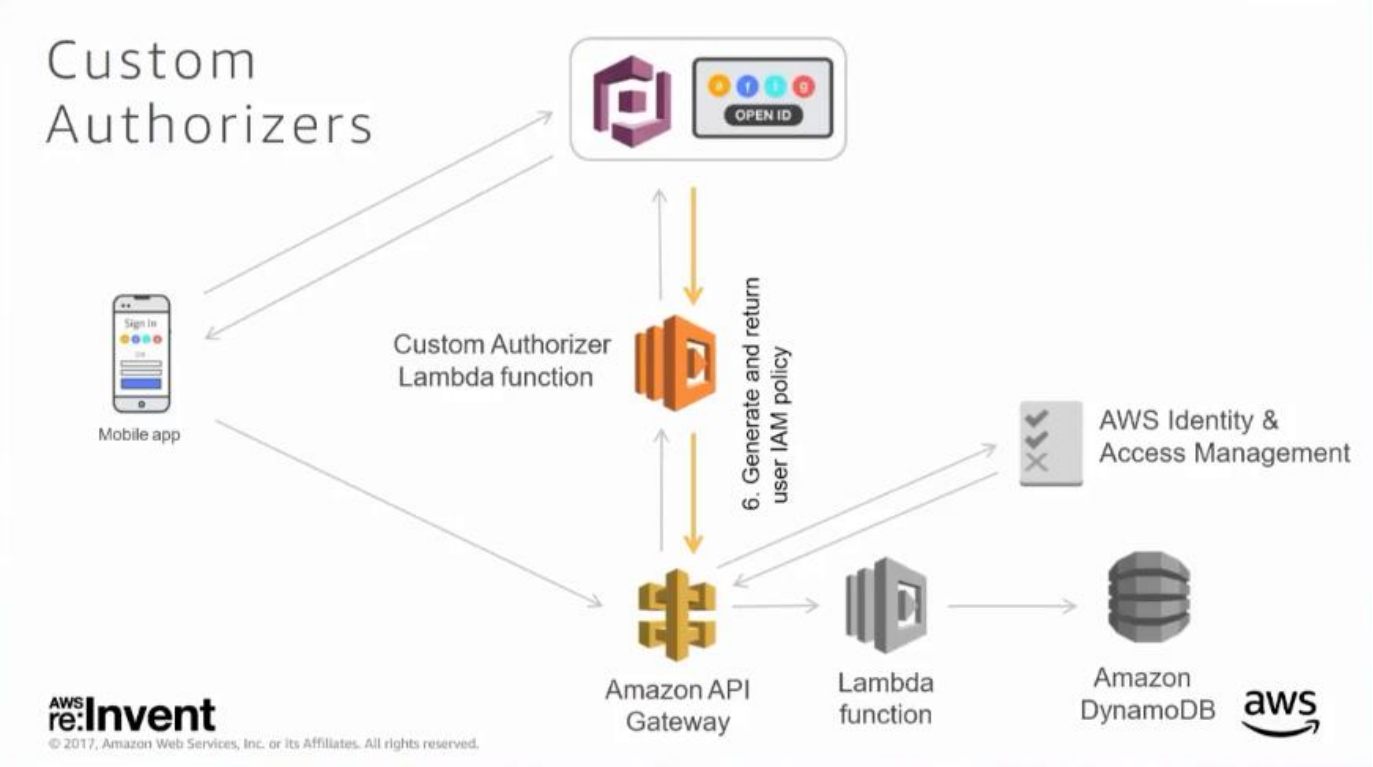




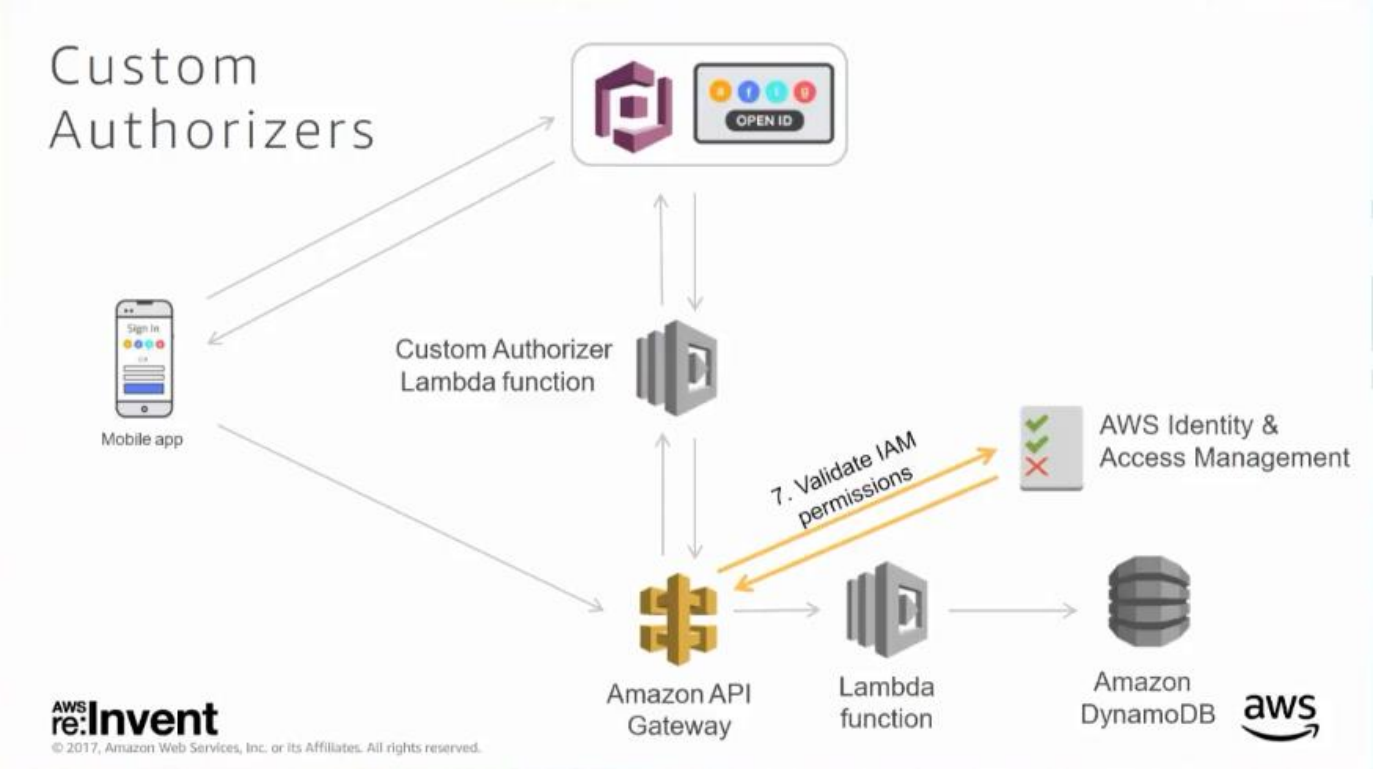
You can then send the token along to API Gateway in the header of your choice. API Gateway checks its local cache to see for that token if we have a known valid policy defined for the user via IAM credentials.



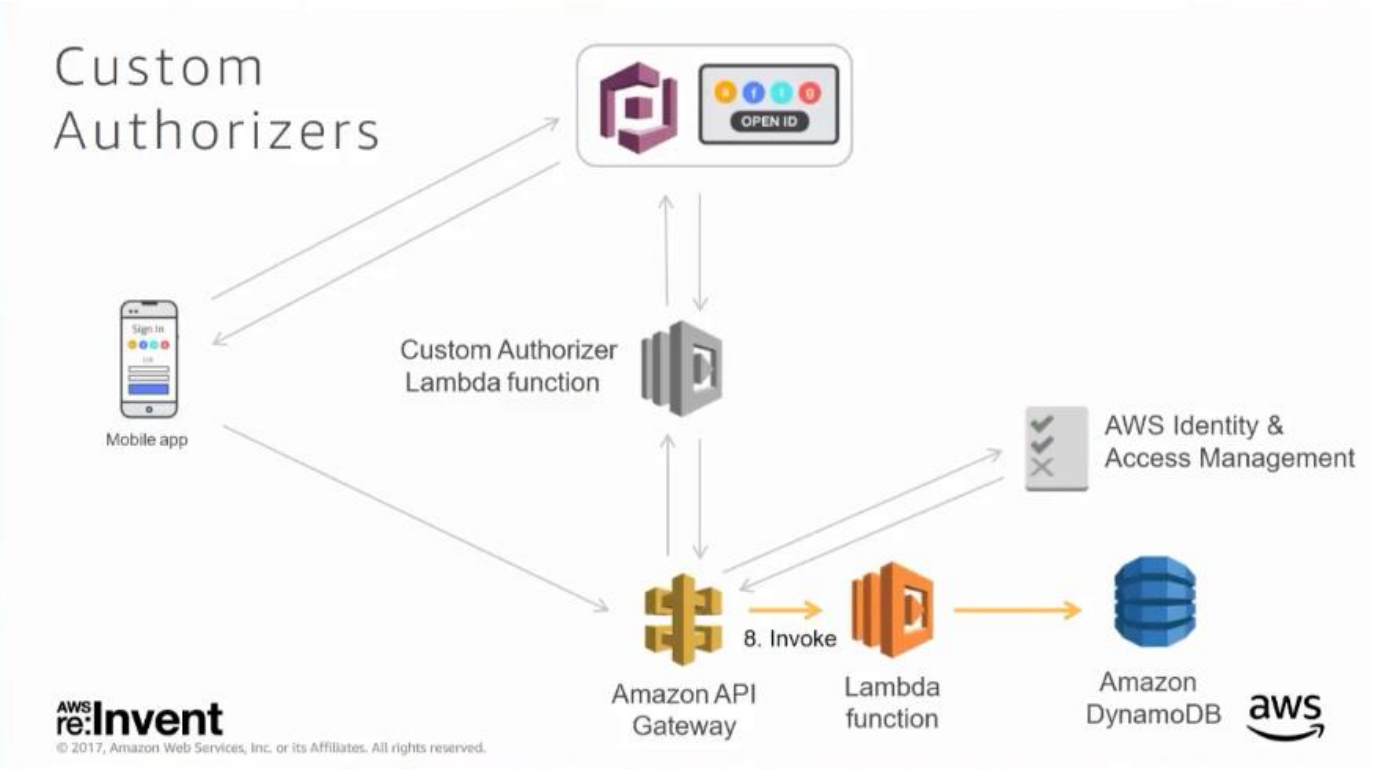
If the API Gateway does not know who the user is, it then invokes a lambda function (your custom authorizer lambda function) to run any business logic of your choice to talk to the 3rd party IDp to validate the user and determine what access they should have.

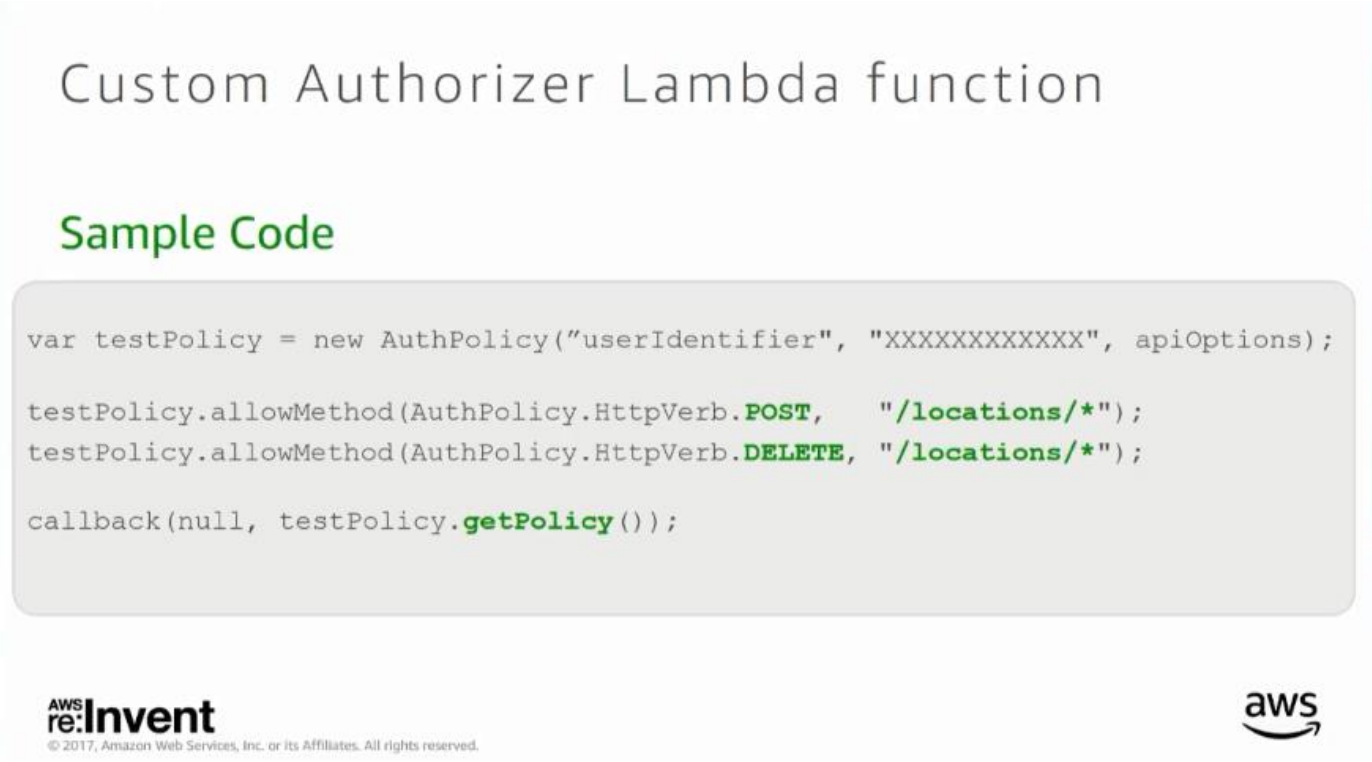


After authorization, the custom authorizer then sends back a well-formed IAM Policy back to the user. The policy is then cached locally for that user for subsequent calls, you can configure the cache duration and validity for the cached policy (the default cache duration is 5 minutes)

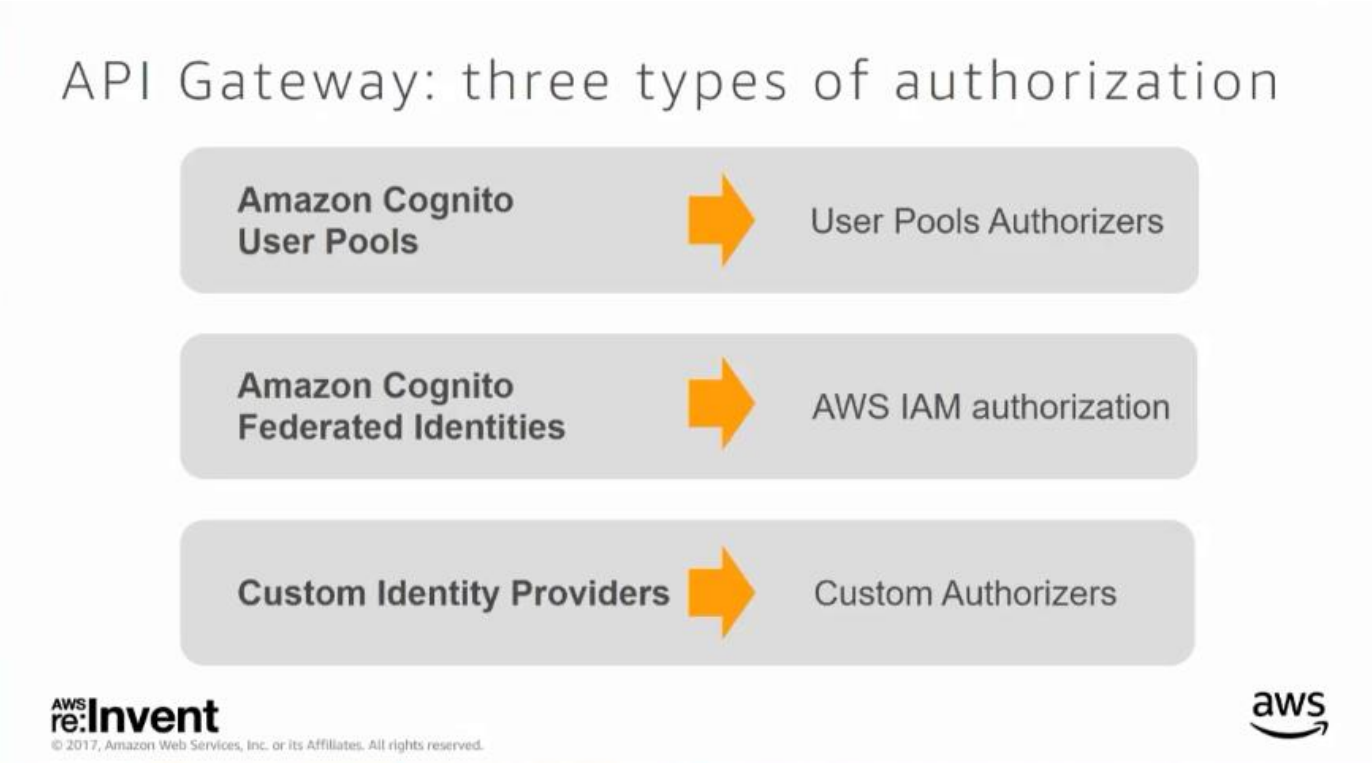


API Gateway then checks what the policy is allowed to do and compares with the intended request



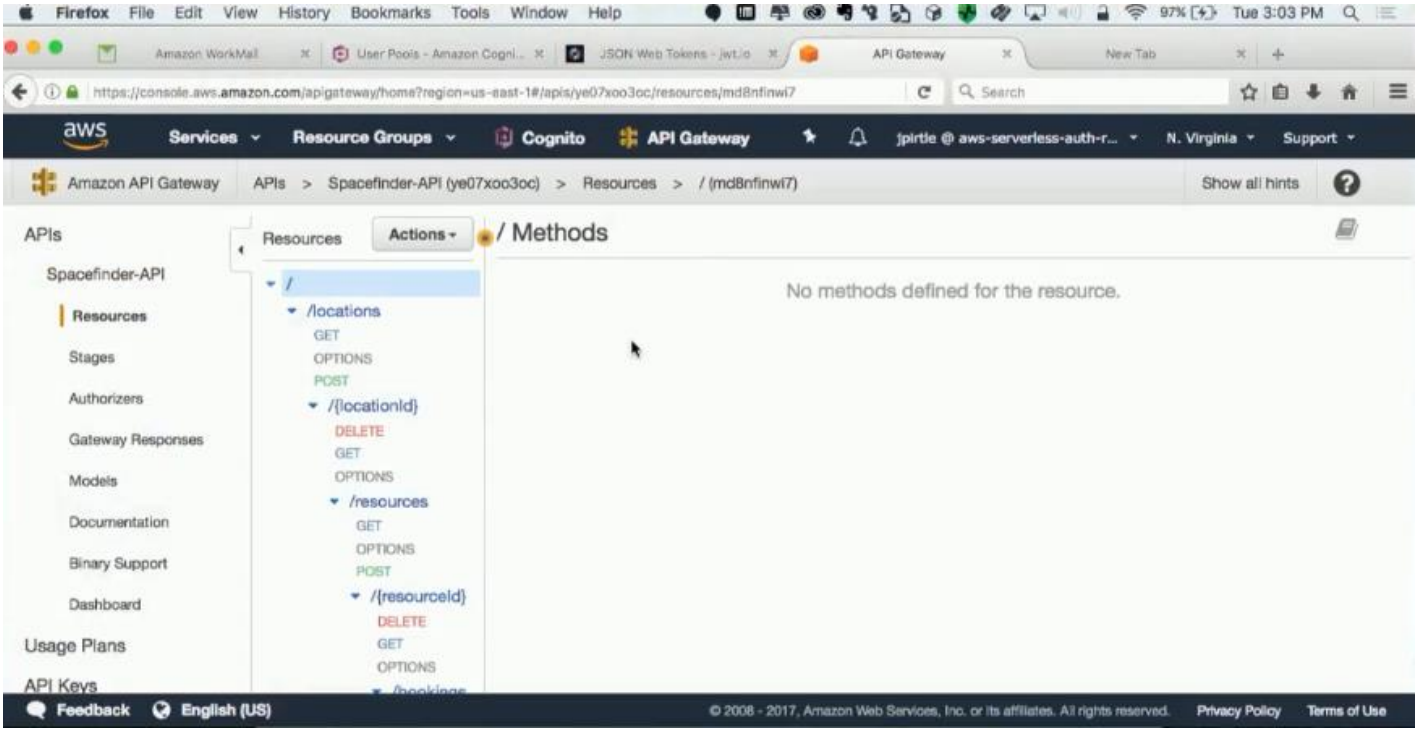


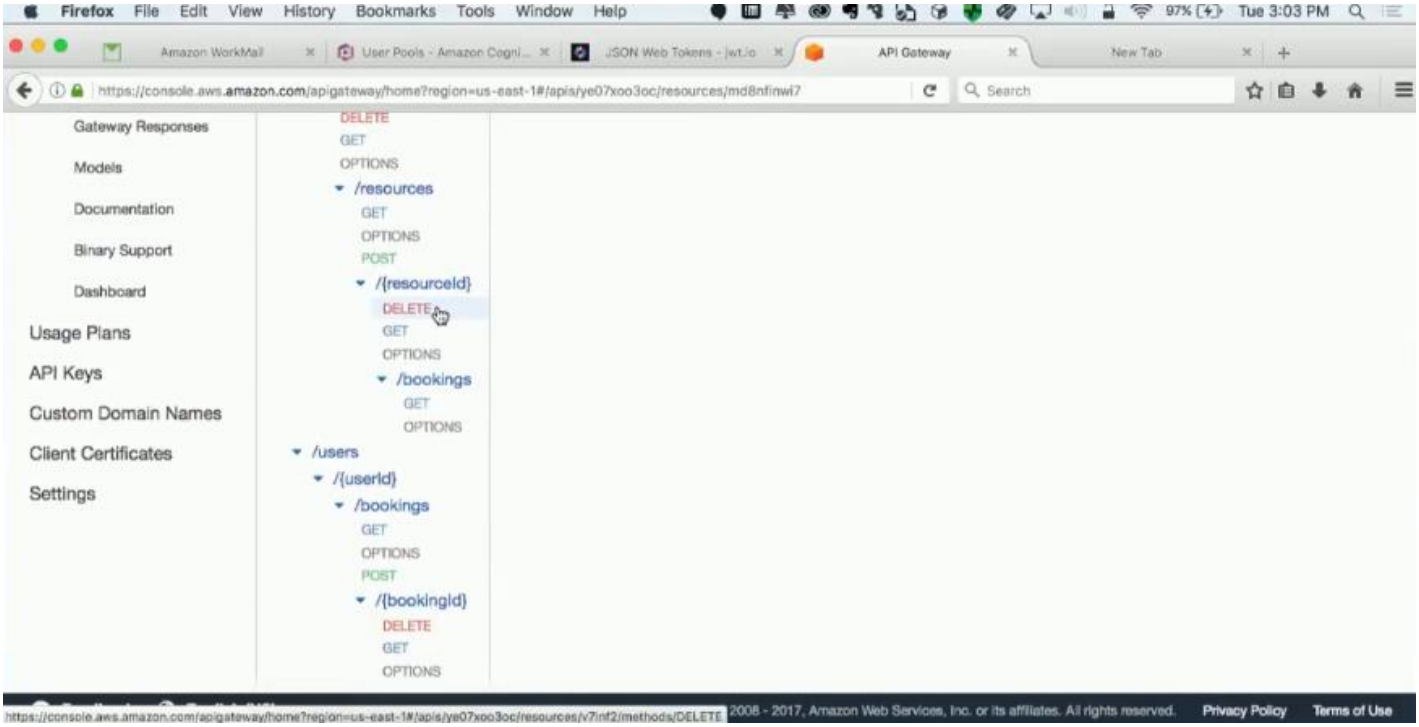
We have a lambda function blueprint in python and JavaScript that can generate a well-formed policy.

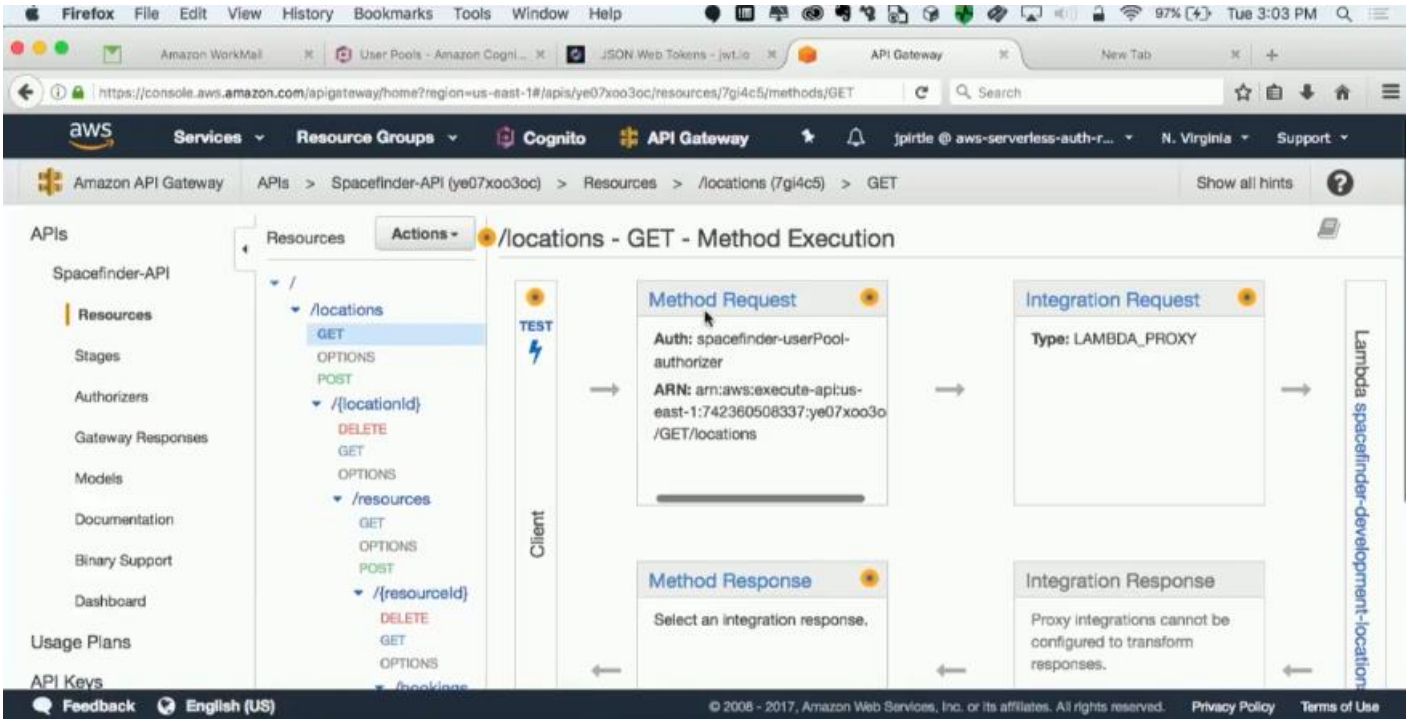


IAM based authorization is the most secure form of authorization since it uses request signing that makes the requests unique with every call.

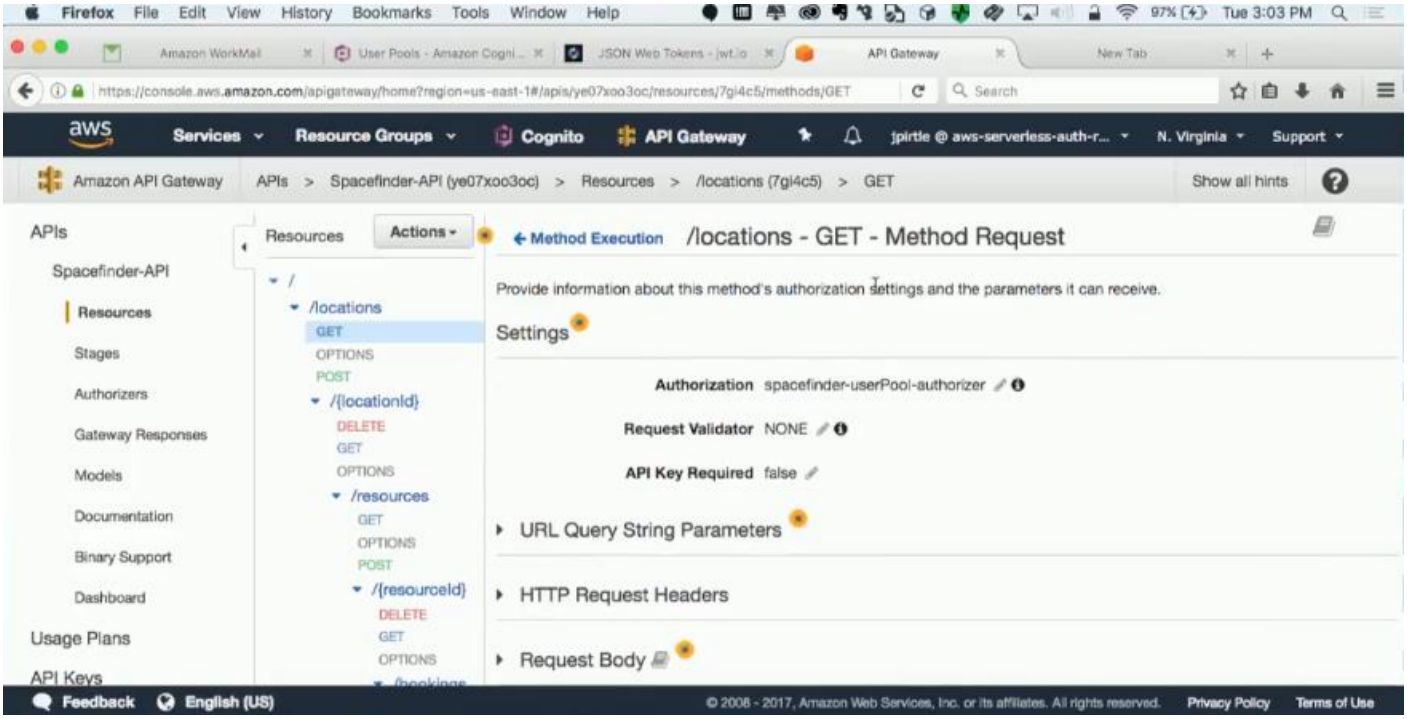
DEMO


Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:03 PM
https://console.aws.amazon.com/apigateway/home?region=us-east-1#/apis/ye07xoo3oc/resources/md8nfinwi7
Services
Resource Groups
Cognito
API Gateway
N. Virginia
Support
Amazon API Gateway
APIs > Spacefinder-API (ye07xoo3oc) > Resources > / (md8nfinwi7)
Show all hints
APIs
Spacefinder-API
Resources
Stages
Authorizers
Gateway Responses
Models
Documentation
Binary Support
Dashboard
Usage Plans
API Keys
Resources
Actions
/ Methods
No methods defined for the resource.
/
/locations
GET
OPTIONS
POST
/{locationId}
DELETE
GET
OPTIONS
/resources
GET
OPTIONS
POST
/{resourceId}
DELETE
GET
OPTIONS
Feedback
English (US)
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

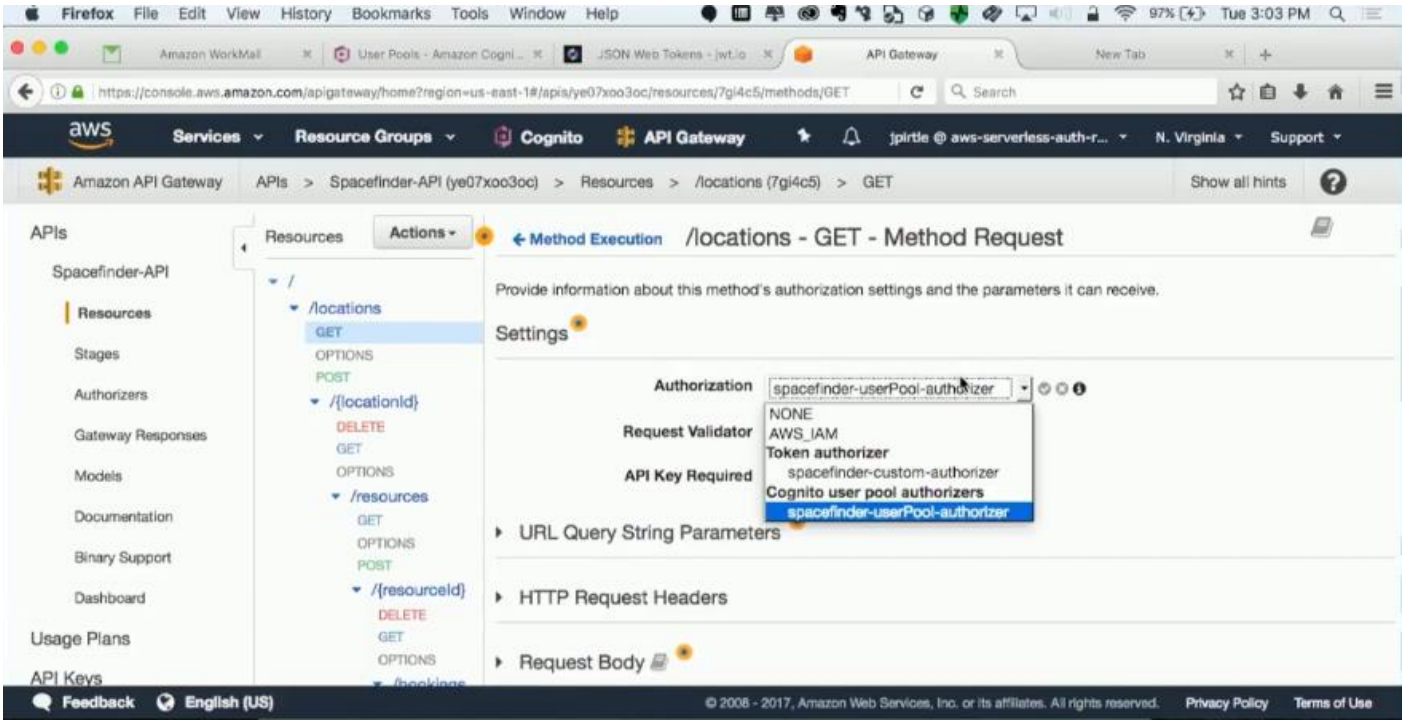

Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:03 PM
https://console.aws.amazon.com/apigateway/home?region=us-east-1#/apis/ye07xoo3oc/resources/md8nfinwi7
Gateway Responses
Models
Documentation
Binary Support
Dashboard
Usage Plans
API Keys
Custom Domain Names
Client Certificates
Settings
DELETE
GET
OPTIONS
/resources
GET
OPTIONS
POST
/{resourceId}
DELETE
GET
OPTIONS
/bookings
GET
OPTIONS
/users
/{userId}
/bookings
GET
OPTIONS
POST
/{bookingId}
DELETE
GET
OPTIONS
https://console.aws.amazon.com/apigateway/home?region=us-east-1#/apis/ye07xoo3oc/resources/v7inf2/methods/DELETE
2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use



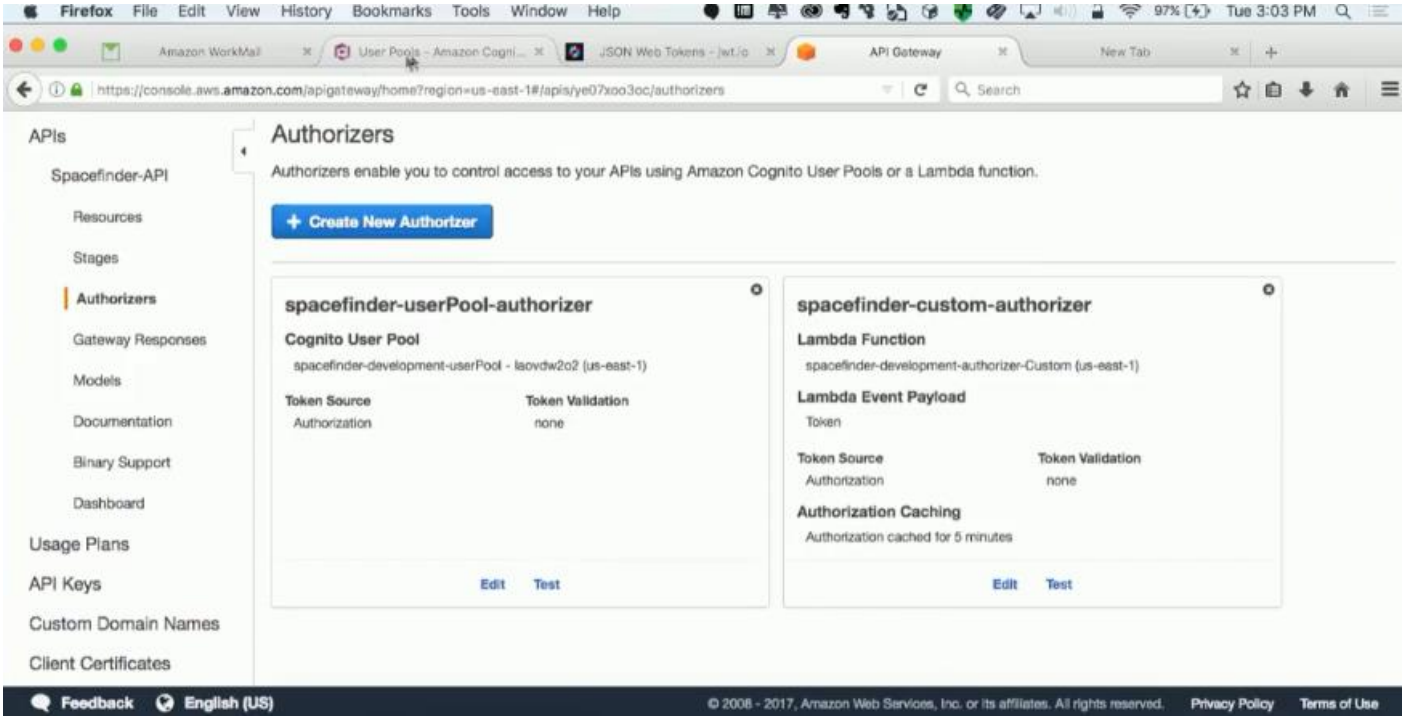
With each API endpoint, we are able to define particular authorization details needed for the request.



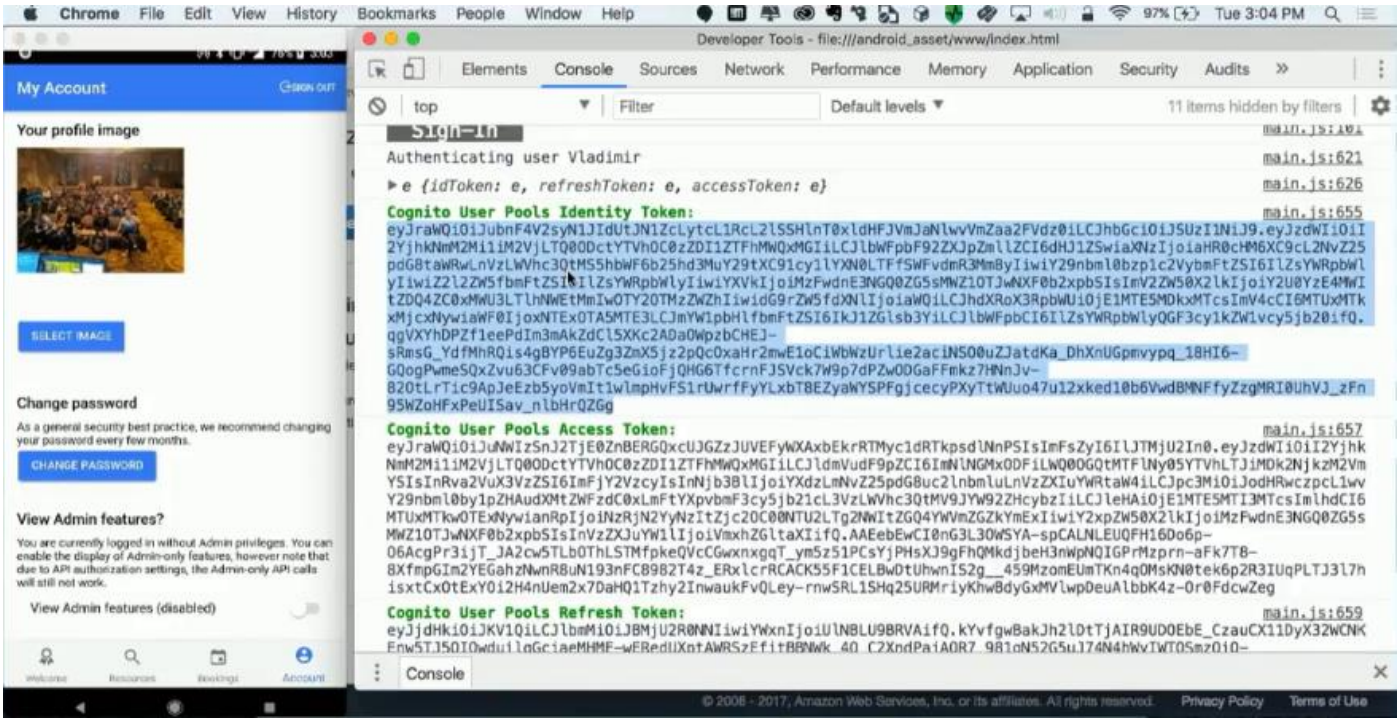
We are requiring authorization for this particular request



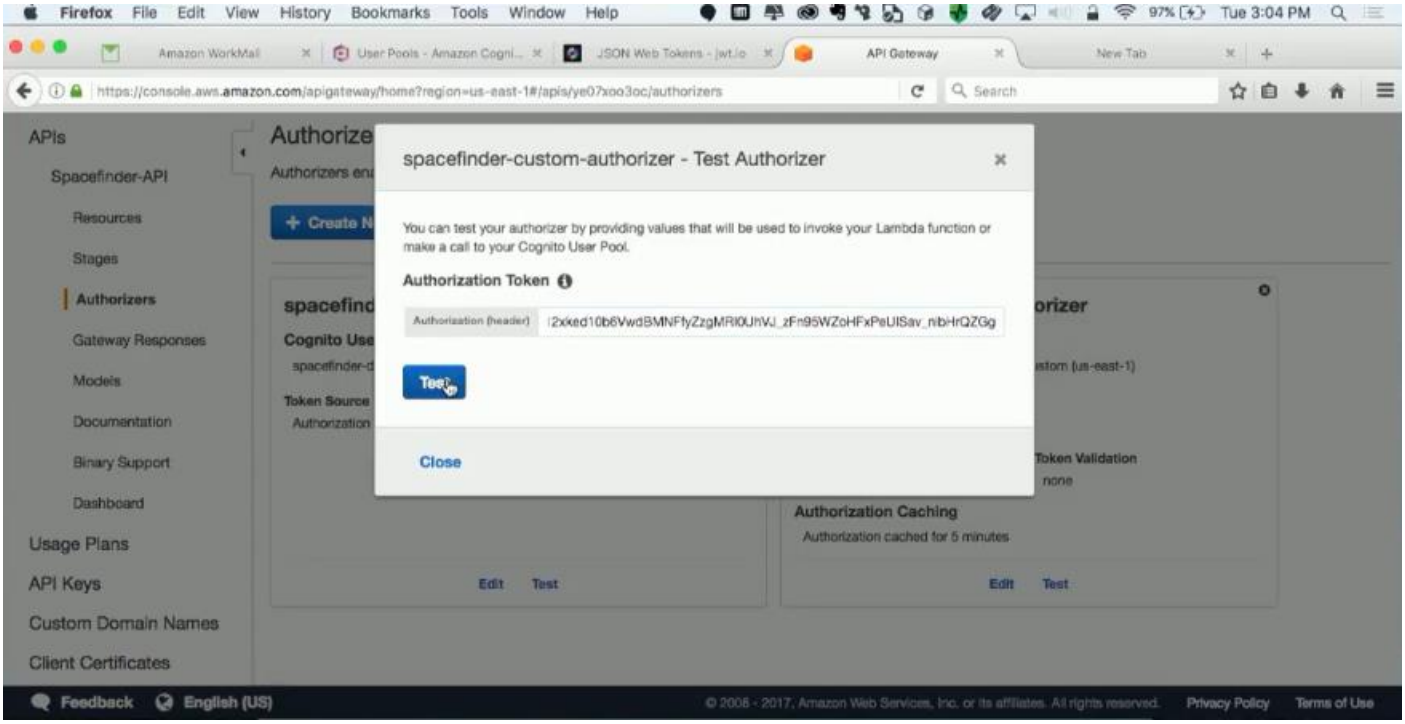
We can pick any type of authorization that we want that API request.

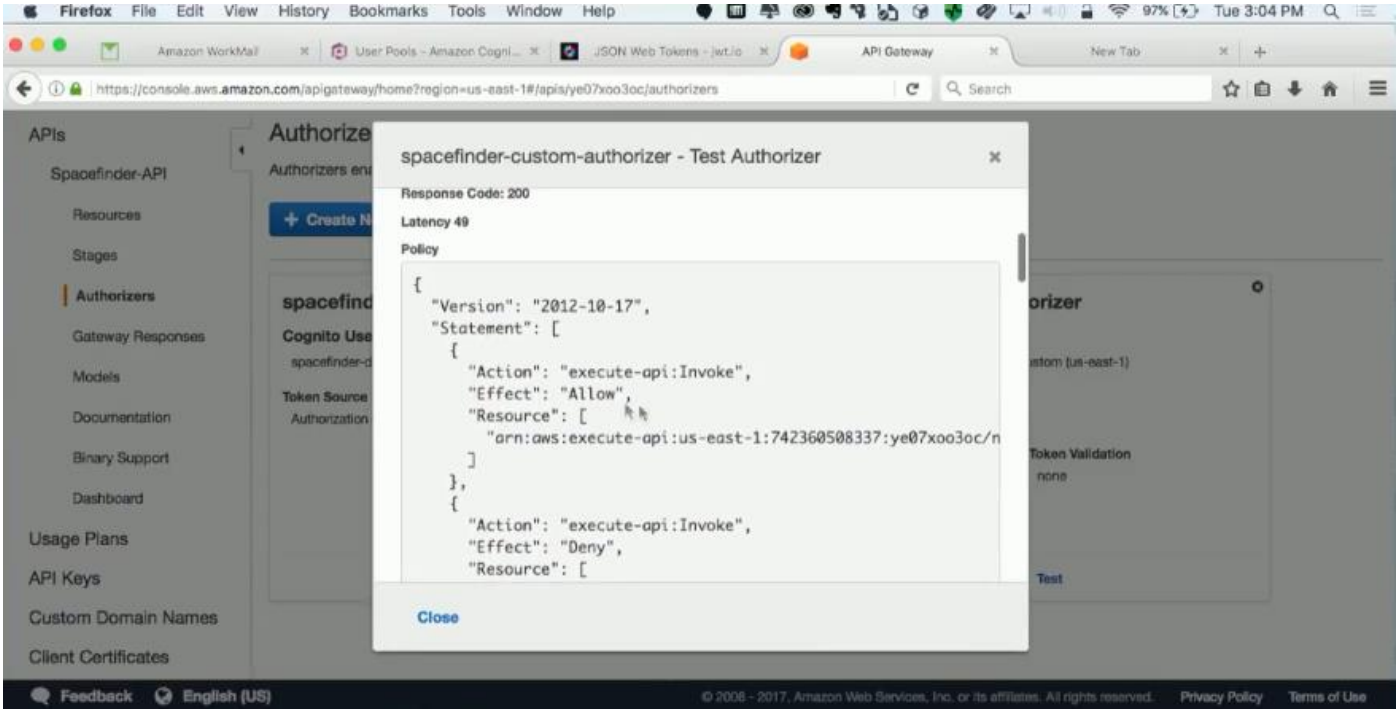


We can also define our authorizers as above.

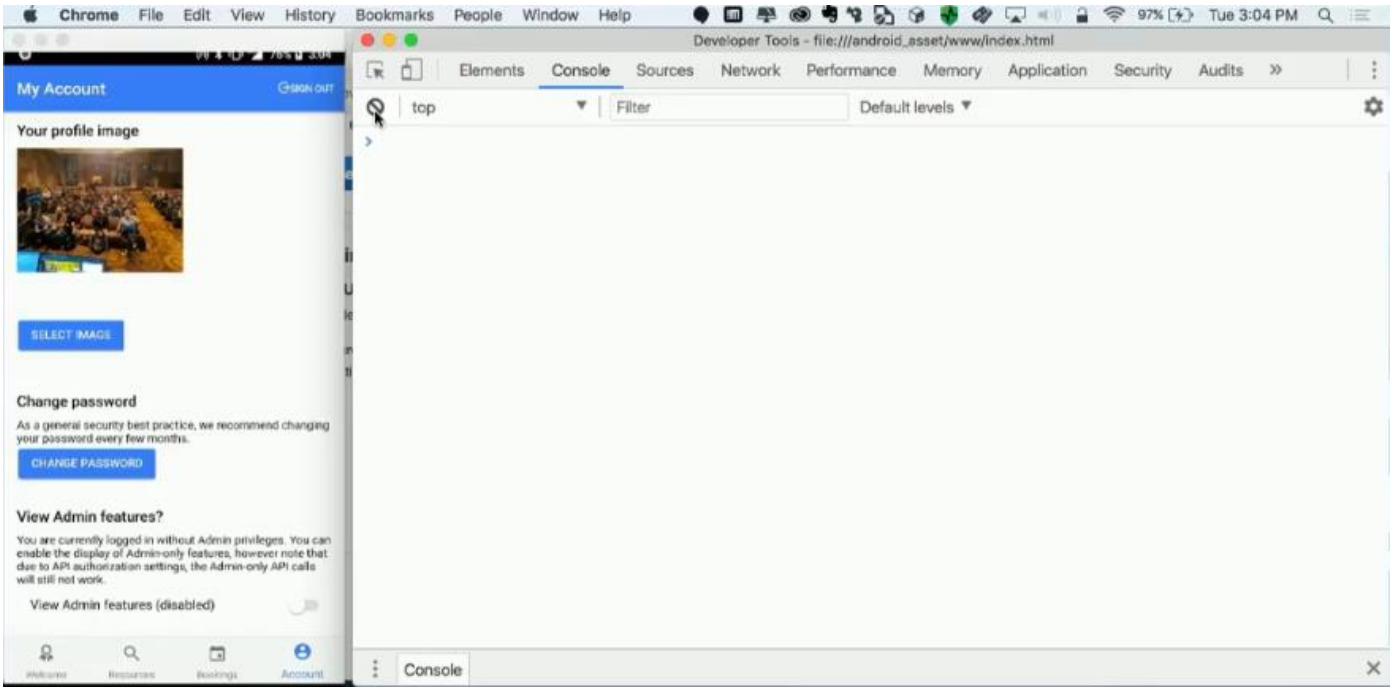


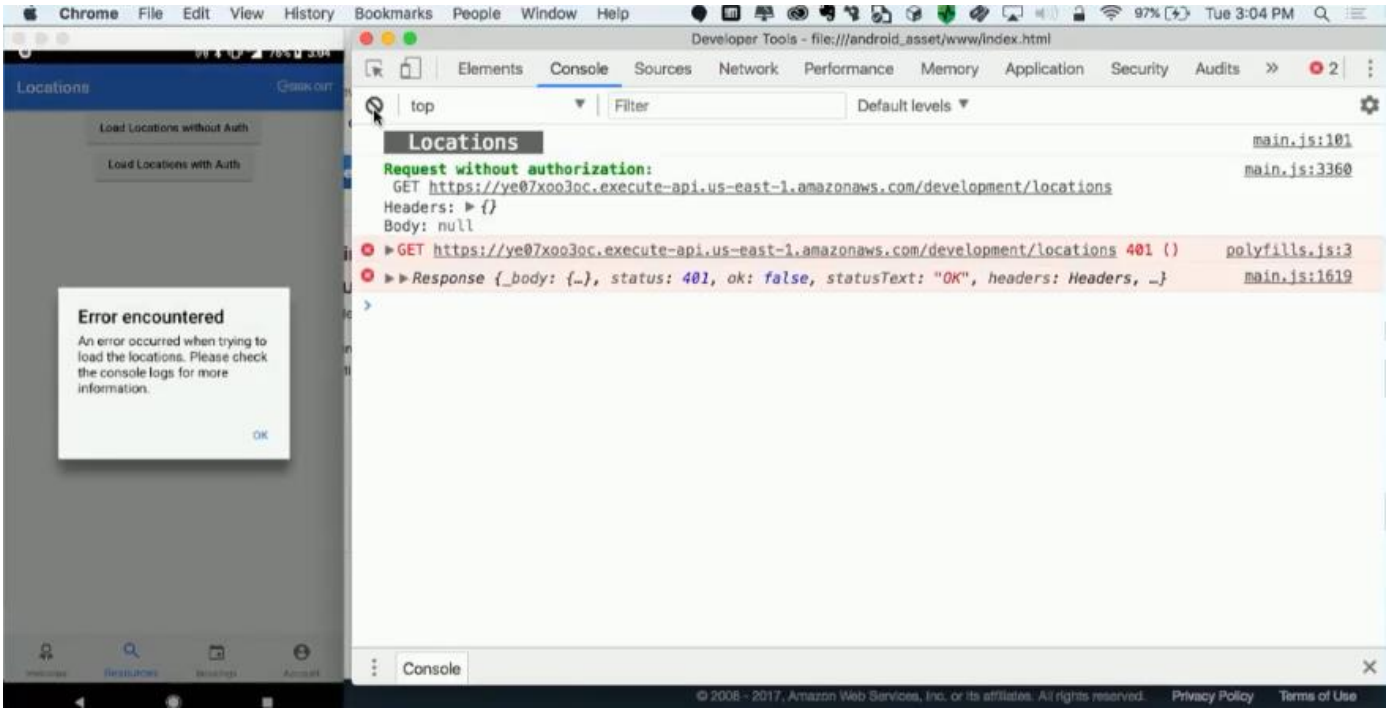
We can also take a token as above and pass it to the custom authorizer as below



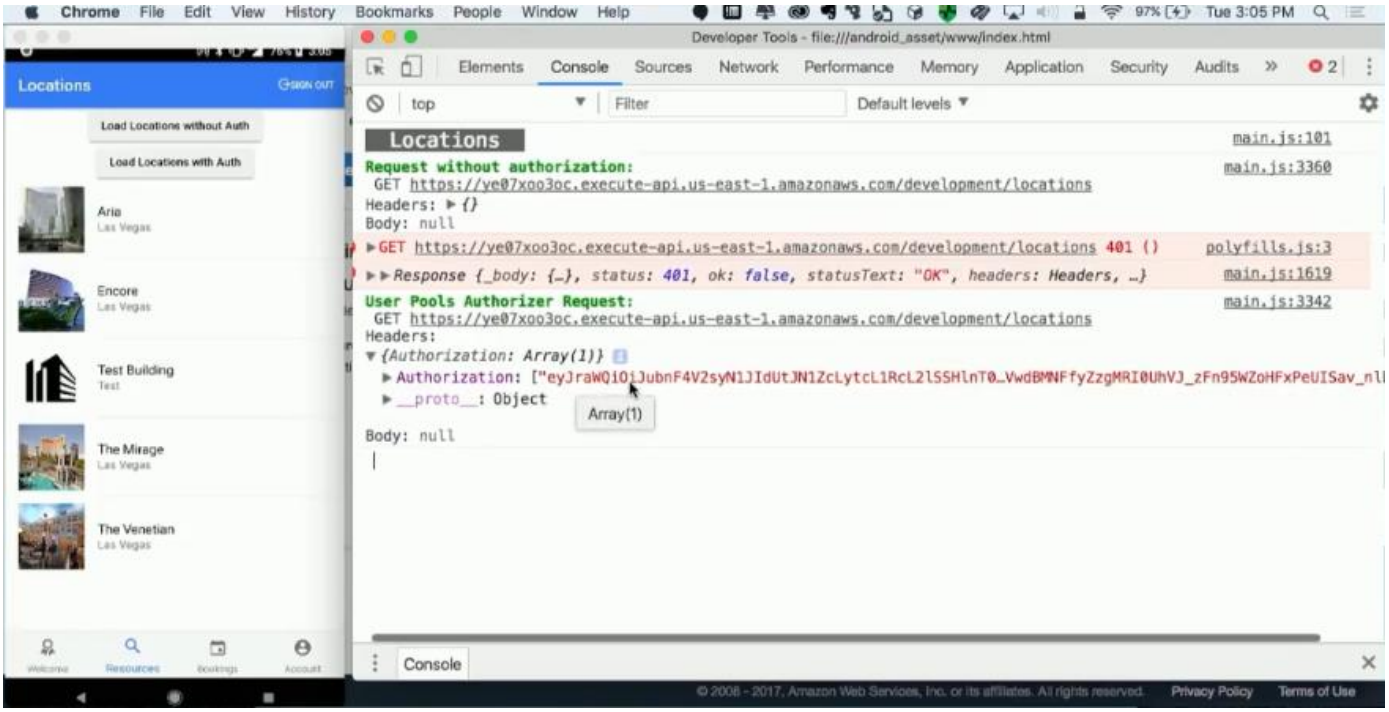


By running the custom authorizer, we can then see what the token is authorized to do

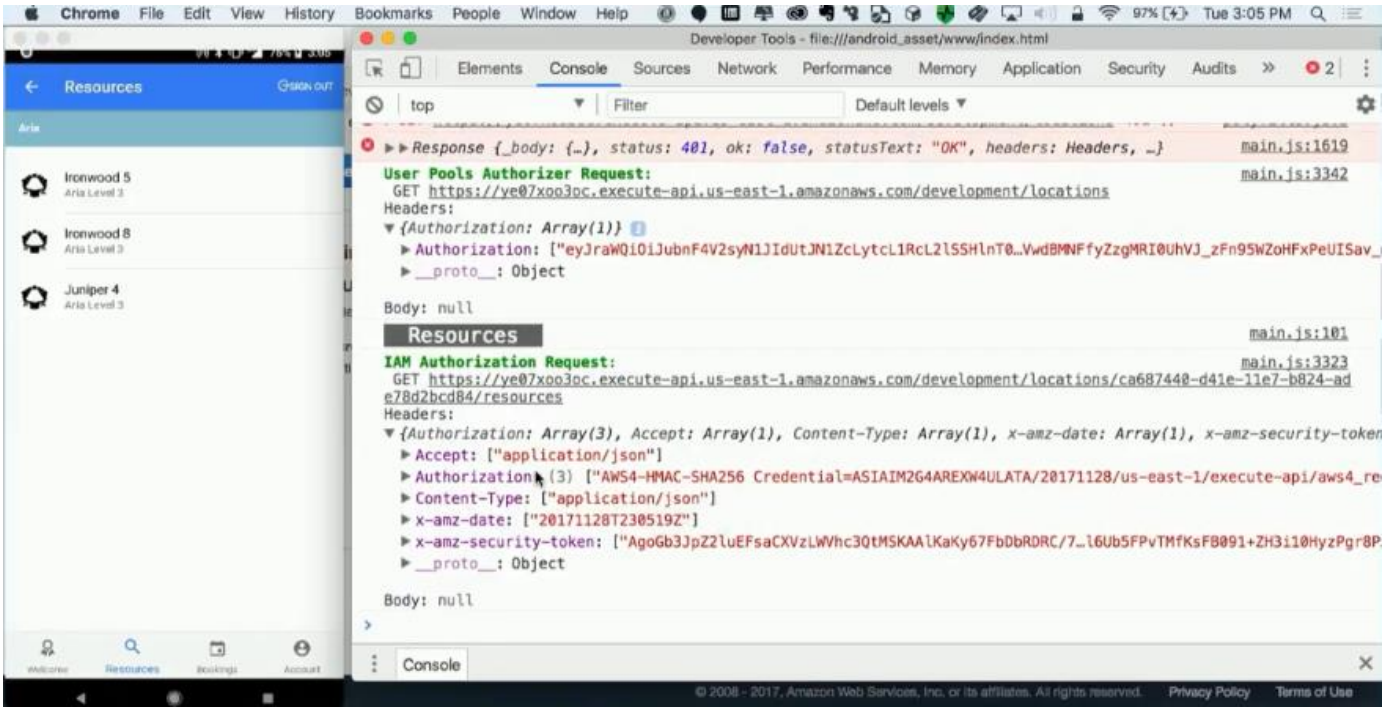




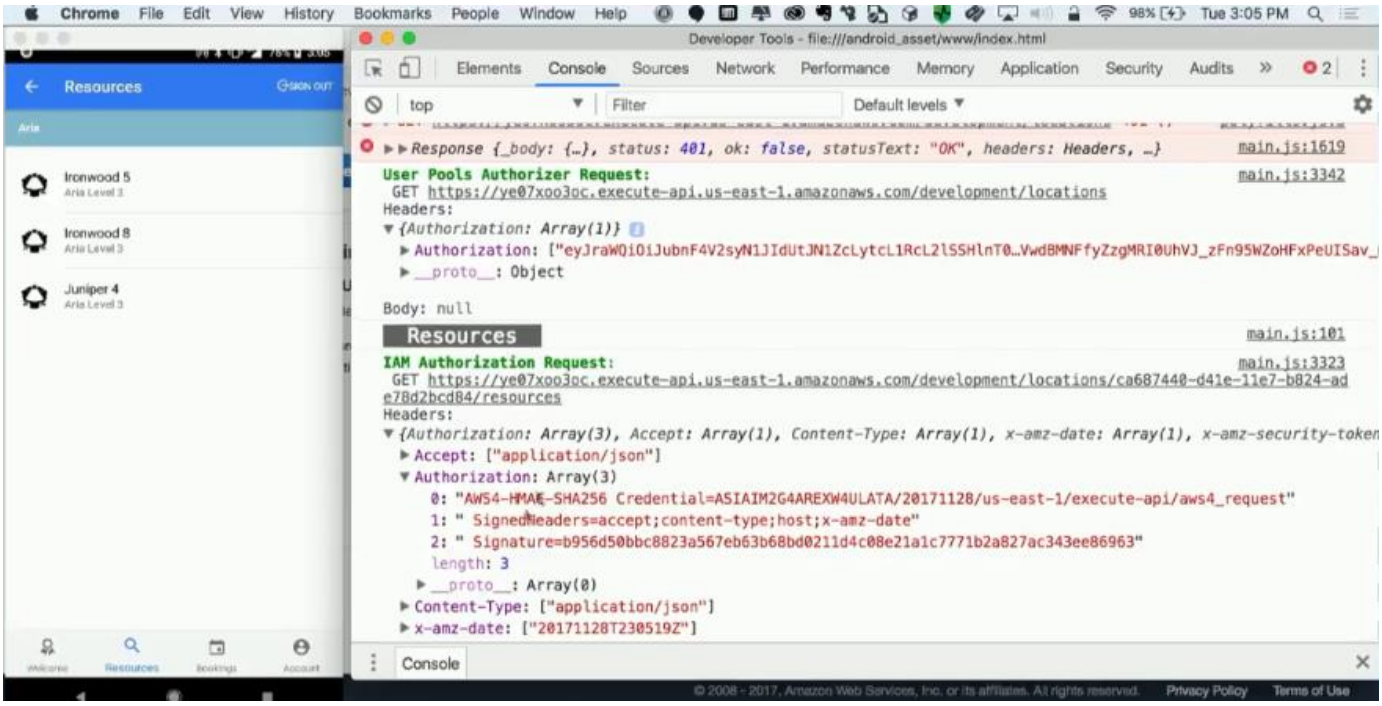
We will get a 401 error response back if there is no required header passed with the request as above.



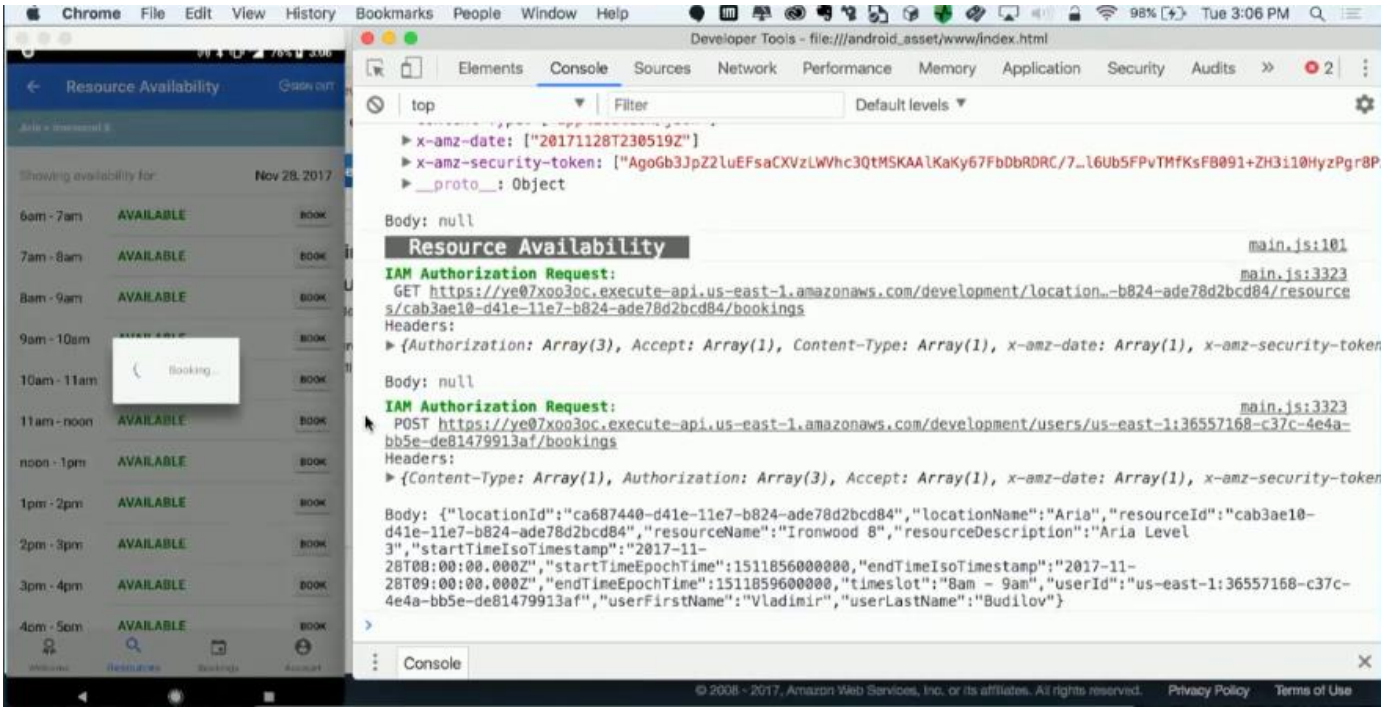
If we send a valid authorization header which is our identity token along in the request header, we get a valid response

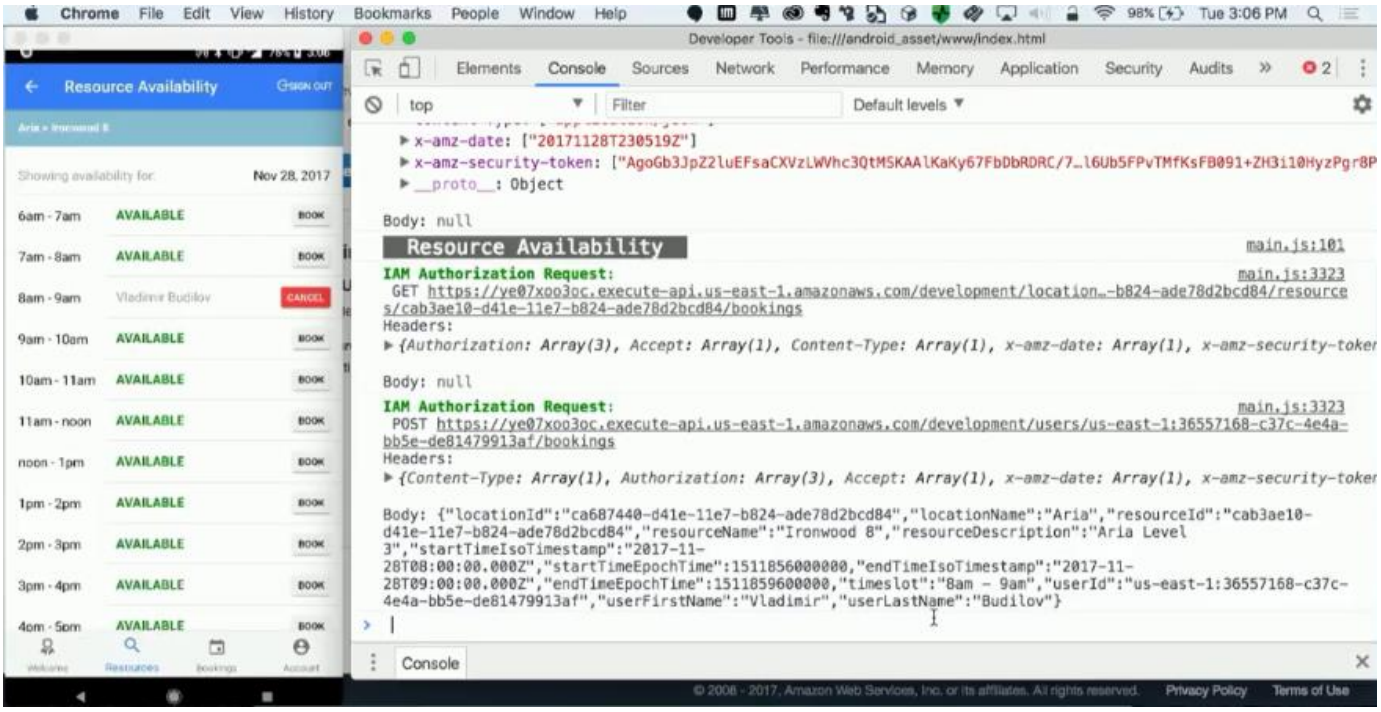


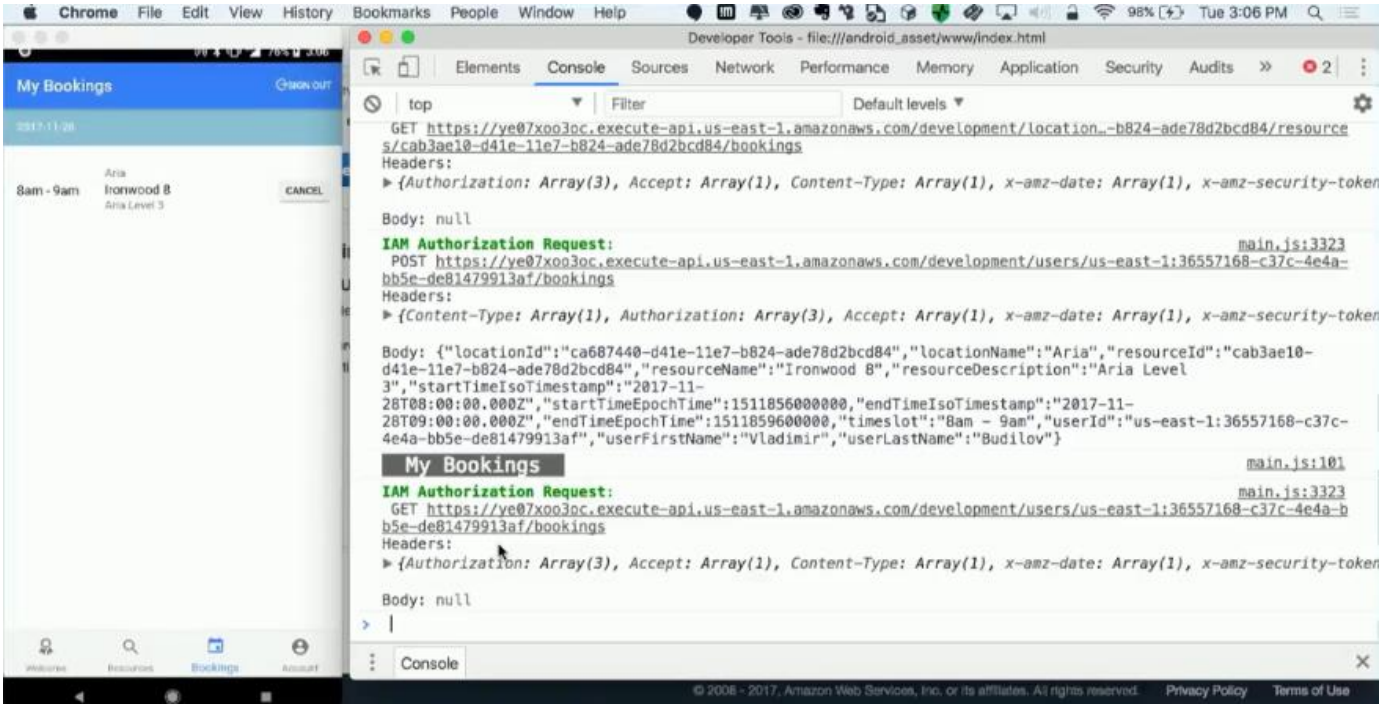
In this case we are using an IAM based authorization request where we are sending several headers along with the request

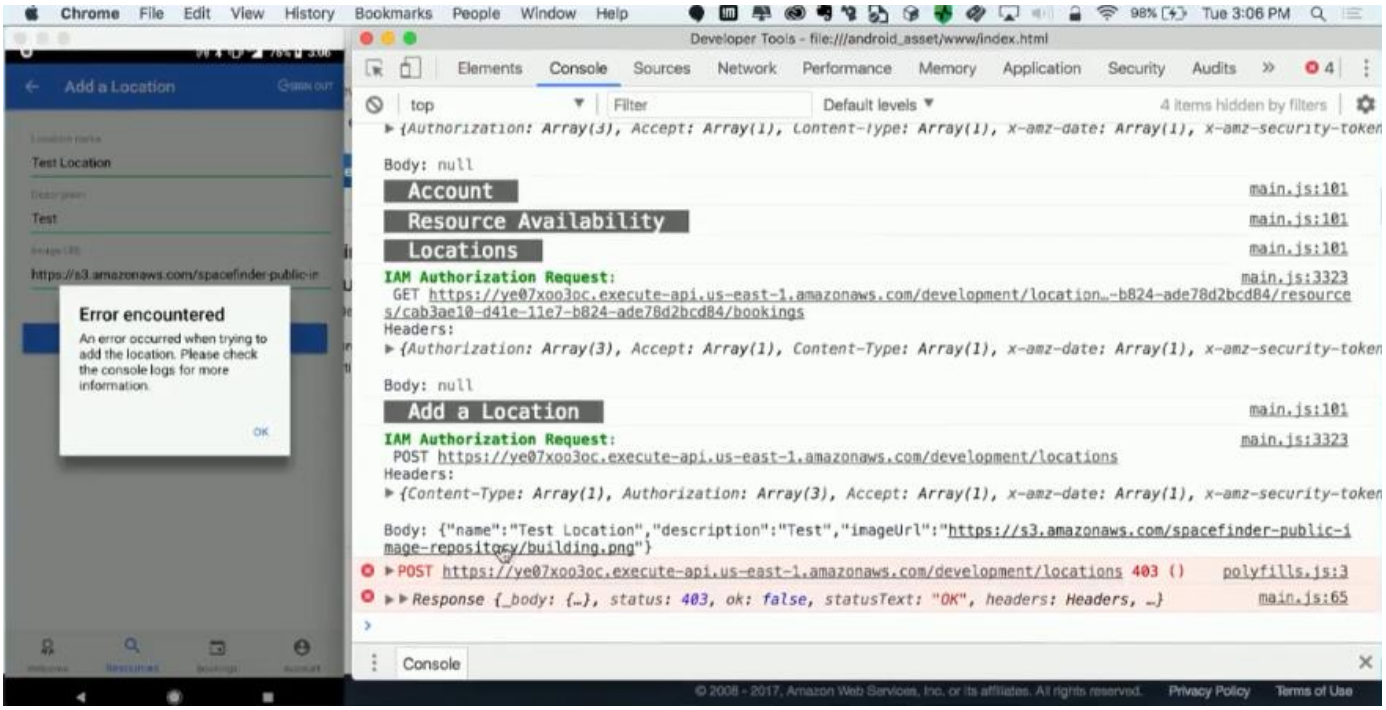


All the different headers make up the signature signing

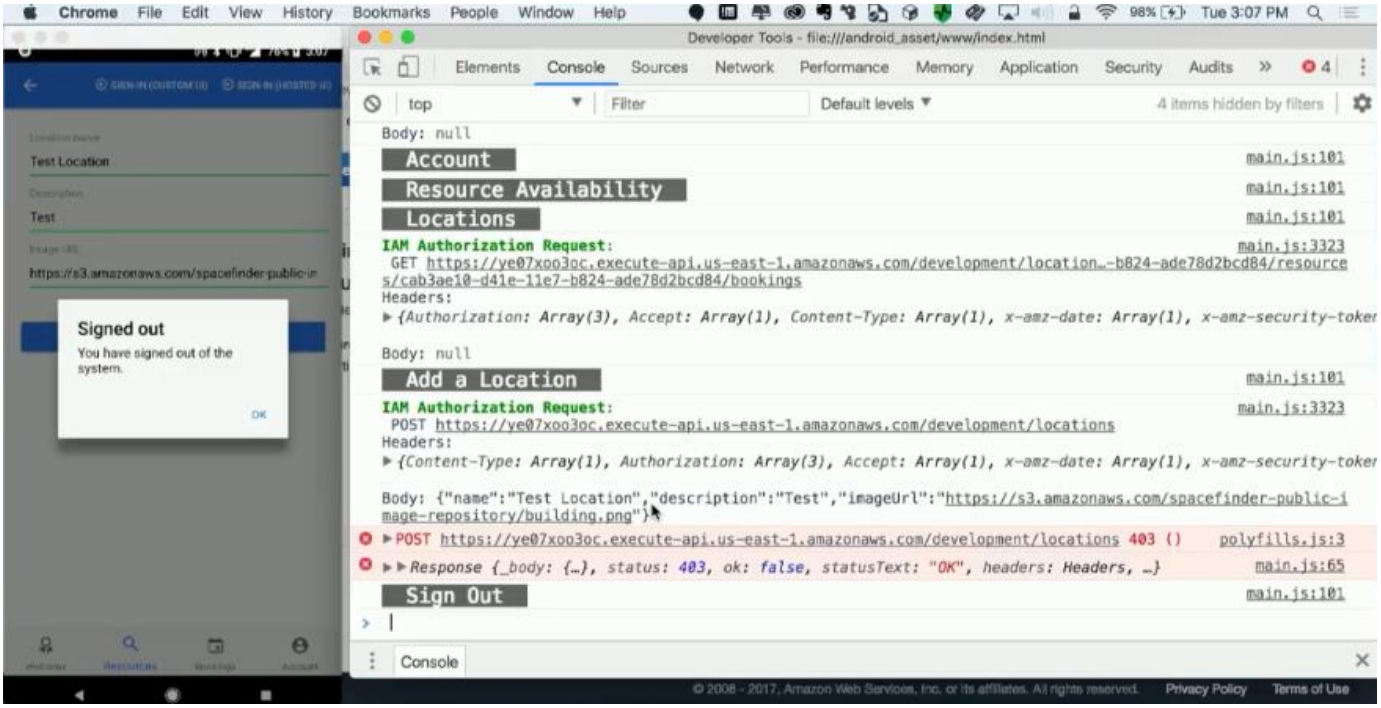

Chrome File Edit View History Bookmarks People Window Help
98% Tue 3:06 PM
Resource Availability
Showing availability for: Nov 28, 2017
6am - 7am AVAILABLE BOOK
7am - 8am AVAILABLE BOOK
8am - 9am AVAILABLE BOOK
9am - 10am AVAILABLE BOOK
10am - 11am AVAILABLE BOOK
11am - noon AVAILABLE BOOK
noon - 1pm AVAILABLE BOOK
1pm - 2pm AVAILABLE BOOK
2pm - 3pm AVAILABLE BOOK
3pm - 4pm AVAILABLE BOOK
4pm - 5pm AVAILABLE BOOK
Booking...
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top Filter Default levels
x-amz-date: ["20171128T230519Z"]
x-amz-security-token: ["AgoGb3JpZ2luEFsaCXVzLWVhc3QtMSKAAlKaKy67FbDbRDRC/7…l6Ub5FPvTMfKsFB091+ZH3i10HyzPgr8P
__proto__: Object
Body: null
Resource Availability
main.js:101
IAM Authorization Request:
main.js:3323
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/location…-b824-ade78d2bcd84/resources/cab3ae10-d41e-11e7-b824-ade78d2bcd84/bookings
Headers:
{Authorization: Array(3), Accept: Array(1), Content-Type: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: null
IAM Authorization Request:
main.js:3323
POST https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/users/us-east-1:36557168-c37c-4e4a-bb5e-de81479913af/bookings
Headers:
{Content-Type: Array(1), Authorization: Array(3), Accept: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: {"locationId":"ca687440-d41e-11e7-b824-ade78d2bcd84","locationName":"Aria","resourceId":"cab3ae10-d41e-11e7-b824-ade78d2bcd84","resourceName":"Ironwood 8","resourceDescription":"Aria Level 3","startTimeIsoTimestamp":"2017-11-28T08:00:00.000Z","startTimeEpochTime":1511856000000,"endTimeIsoTimestamp":"2017-11-28T09:00:00.000Z","endTimeEpochTime":1511859600000,"timeslot":"8am - 9am","userId":"us-east-1:36557168-c37c-4e4a-bb5e-de81479913af","userFirstName":"Vladimir","userLastName":"Budilov"}
Console
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

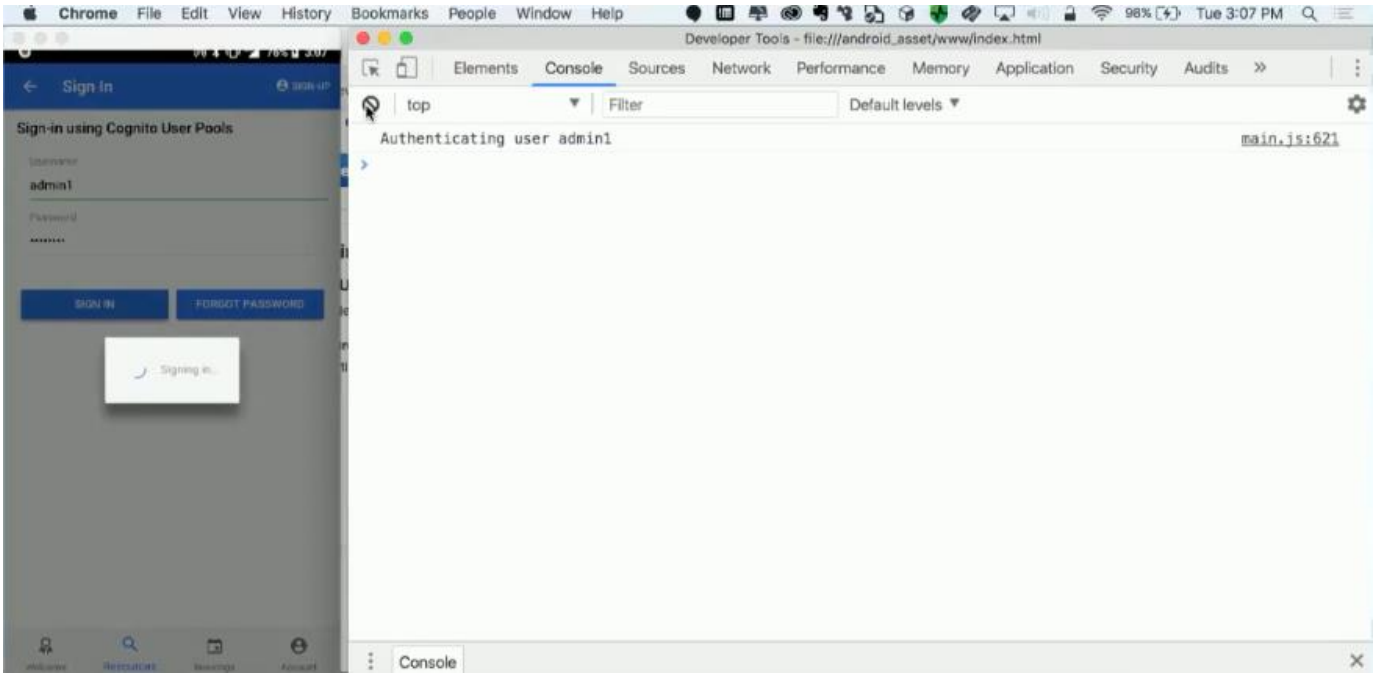

Chrome File Edit View History Bookmarks People Window Help
98% Tue 3:06 PM
Resource Availability
Showing availability for: Nov 28, 2017
6am - 7am AVAILABLE BOOK
7am - 8am AVAILABLE BOOK
8am - 9am Vladimir Budilov CANCEL
9am - 10am AVAILABLE BOOK
10am - 11am AVAILABLE BOOK
11am - noon AVAILABLE BOOK
noon - 1pm AVAILABLE BOOK
1pm - 2pm AVAILABLE BOOK
2pm - 3pm AVAILABLE BOOK
3pm - 4pm AVAILABLE BOOK
4pm - 5pm AVAILABLE BOOK
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top Filter Default levels
x-amz-date: ["20171128T230519Z"]
x-amz-security-token: ["AgoGb3JpZ2luEFsaCXVzLWVhc3QtMSKAAlKaKy67FbDbRDRC/7…l6Ub5FPvTMfKsFB091+ZH3i10HyzPgr8P
__proto__: Object
Body: null
Resource Availability
main.js:101
IAM Authorization Request:
main.js:3323
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/location…-b824-ade78d2bcd84/resources/cab3ae10-d41e-11e7-b824-ade78d2bcd84/bookings
Headers:
{Authorization: Array(3), Accept: Array(1), Content-Type: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: null
IAM Authorization Request:
main.js:3323
POST https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/users/us-east-1:36557168-c37c-4e4a-bb5e-de81479913af/bookings
Headers:
{Content-Type: Array(1), Authorization: Array(3), Accept: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: {"locationId":"ca687440-d41e-11e7-b824-ade78d2bcd84","locationName":"Aria","resourceId":"cab3ae10-d41e-11e7-b824-ade78d2bcd84","resourceName":"Ironwood 8","resourceDescription":"Aria Level 3","startTimeIsoTimestamp":"2017-11-28T08:00:00.000Z","startTimeEpochTime":1511856000000,"endTimeIsoTimestamp":"2017-11-28T09:00:00.000Z","endTimeEpochTime":1511859600000,"timeslot":"8am - 9am","userId":"us-east-1:36557168-c37c-4e4a-bb5e-de81479913af","userFirstName":"Vladimir","userLastName":"Budilov"}
Console
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

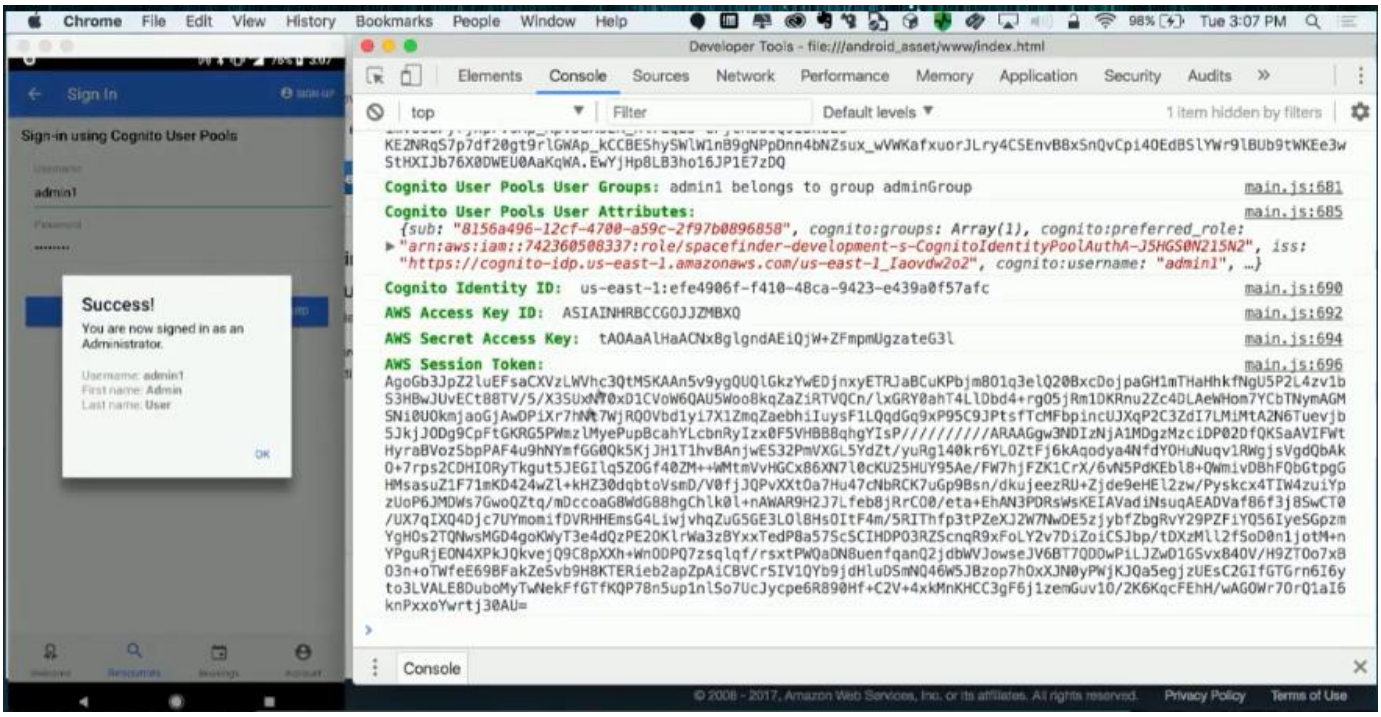




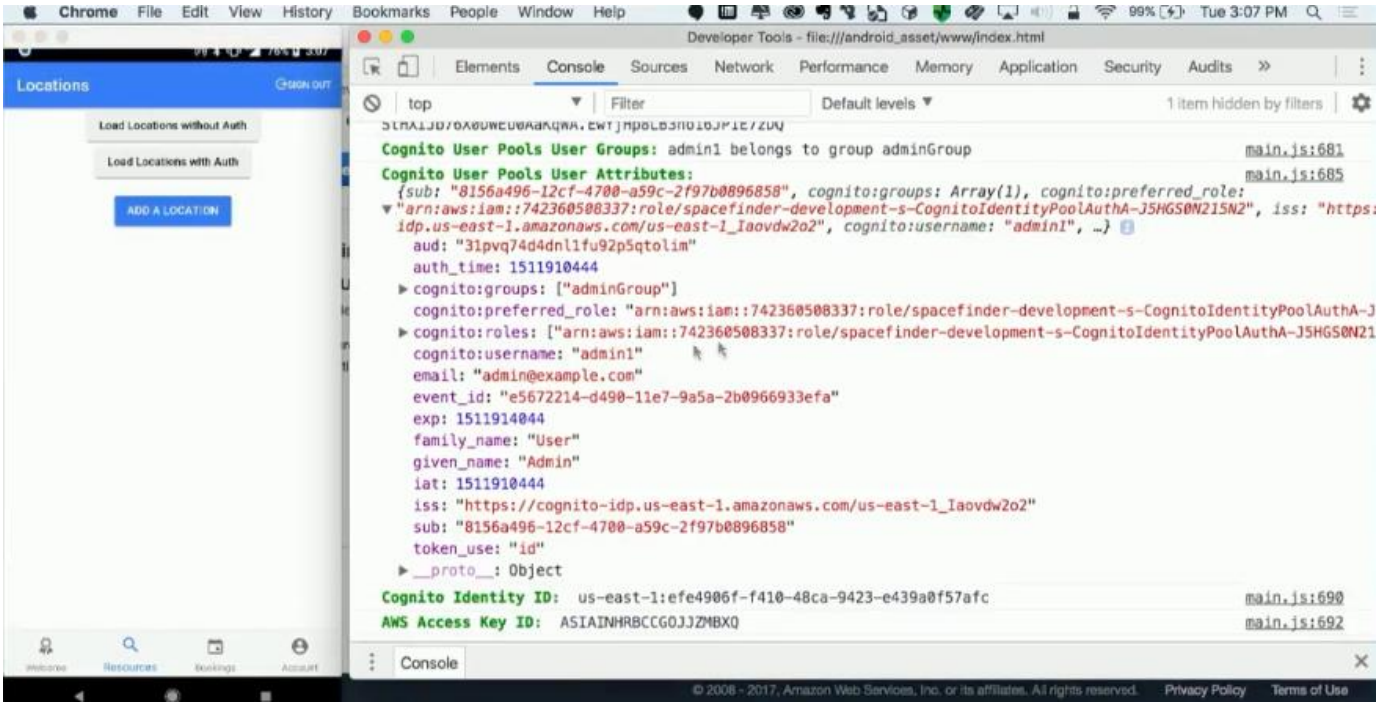
We are not an admin, so our IAM policy did not allow us to do that request

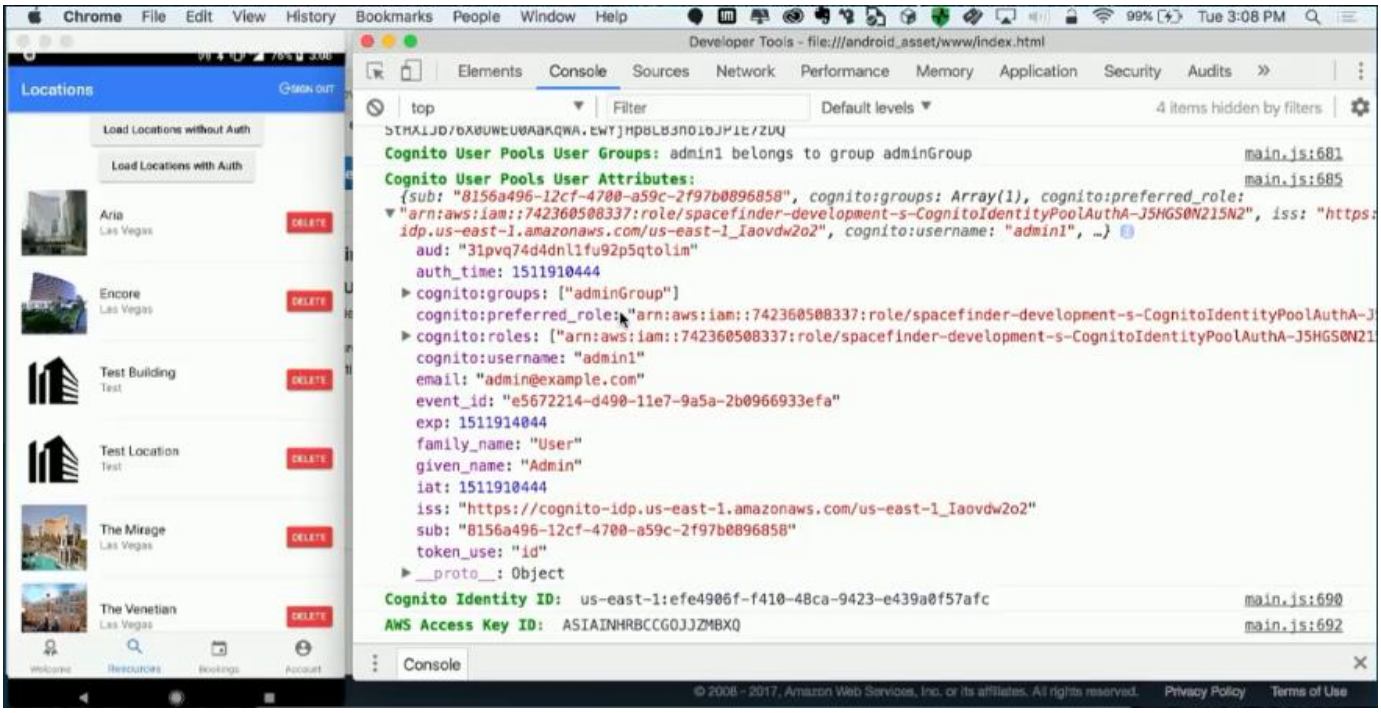

Chrome File Edit View History Bookmarks People Window Help
98% Tue 3:07 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
Test Location
Test
https://s3.amazonaws.com/spacefinder-public-ir
Signed out
You have signed out of the system.
OK
top
Filter
Default levels
4 items hidden by filters
Body: null
Account
main.js:101
Resource Availability
main.js:101
Locations
main.js:101
IAM Authorization Request:
main.js:3323
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/location…-b824-ade78d2bcd84/resources/cab3ae10-d41e-11e7-b824-ade78d2bcd84/bookings
Headers:
{Authorization: Array(3), Accept: Array(1), Content-Type: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: null
Add a Location
main.js:101
IAM Authorization Request:
main.js:3323
POST https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations
Headers:
{Content-Type: Array(1), Authorization: Array(3), Accept: Array(1), x-amz-date: Array(1), x-amz-security-token
Body: {"name":"Test Location","description":"Test","imageUrl":"https://s3.amazonaws.com/spacefinder-public-image-repository/building.png"}
POST https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations 403 ()
polyfills.js:3
Response {_body: {…}, status: 403, ok: false, statusText: "OK", headers: Headers, …}
main.js:65
Sign Out
main.js:101
Console
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


Chrome File Edit View History Bookmarks People Window Help
98% Tue 3:07 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
Sign In
Sign-in using Cognito User Pools
admin1
SIGN IN
FORGOT PASSWORD
top
Filter
Default levels
Authenticating user admin1
main.js:621
Console

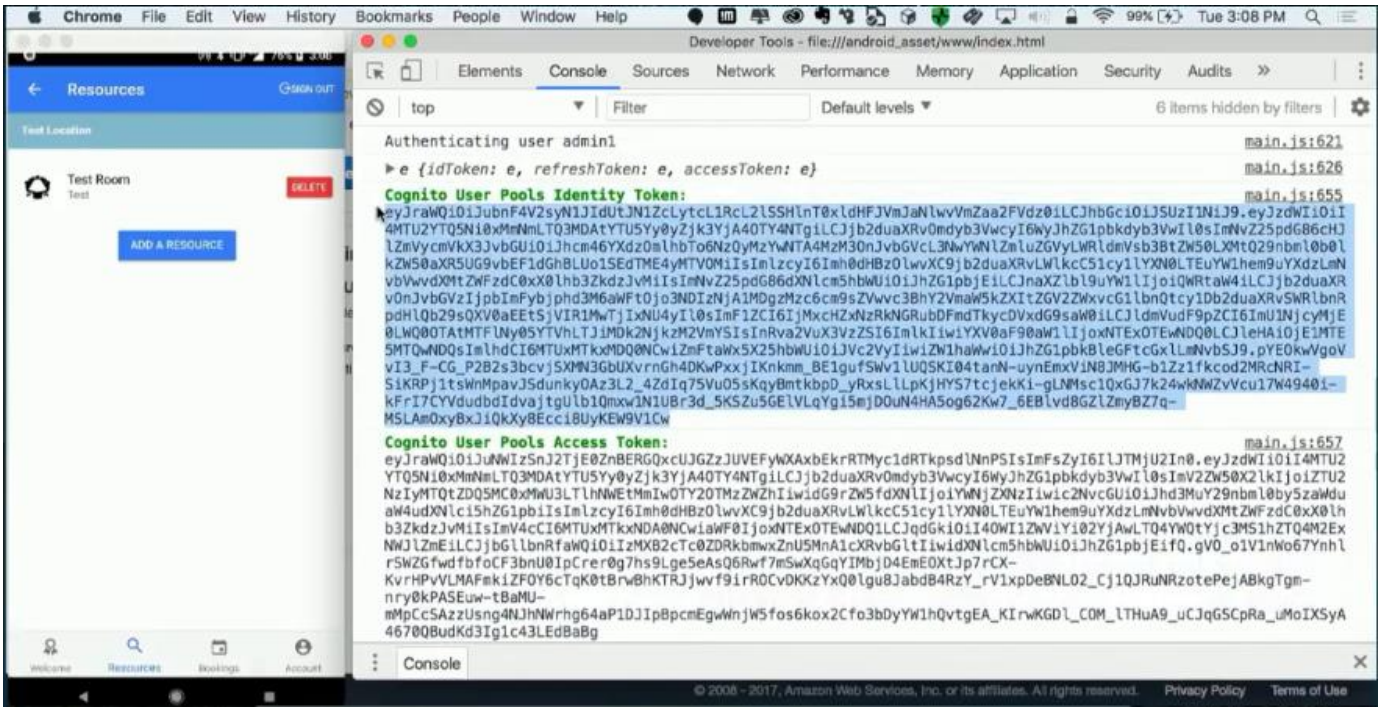


We are now an admin

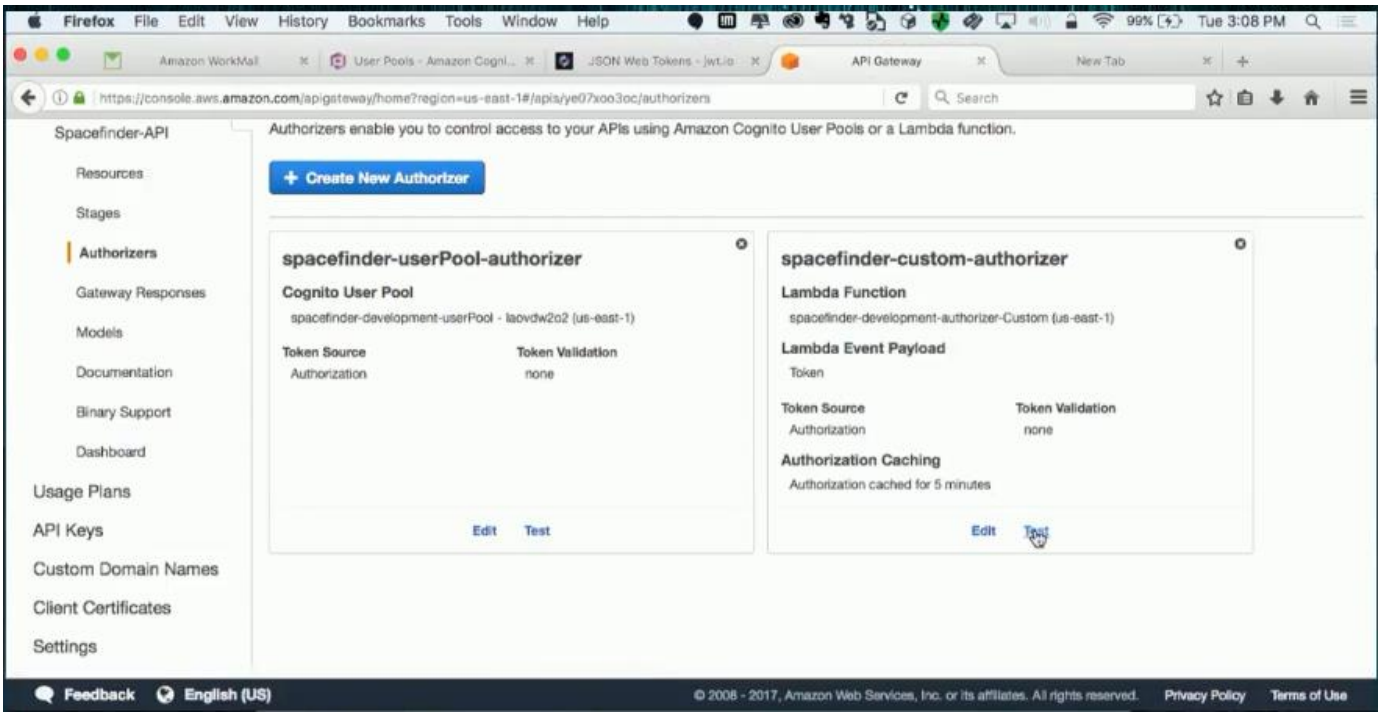


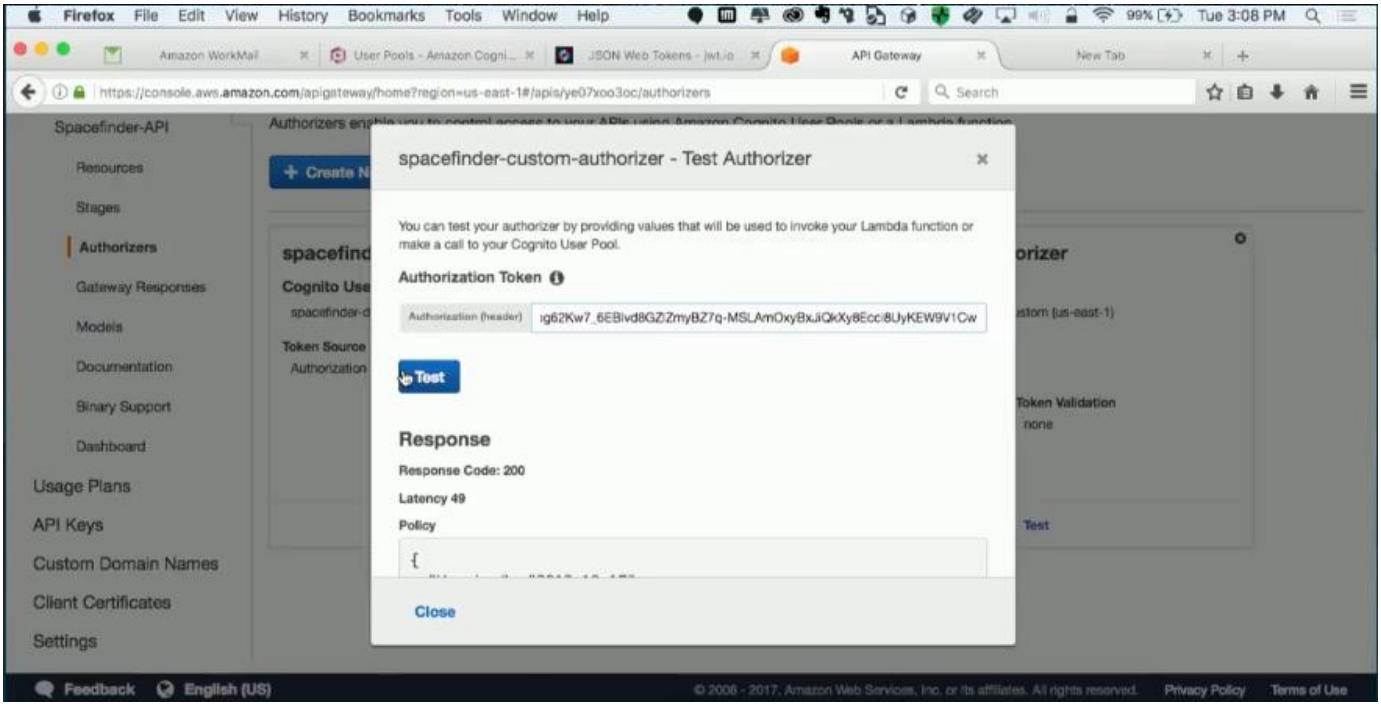


We are now able to create a resource since we are now an admin

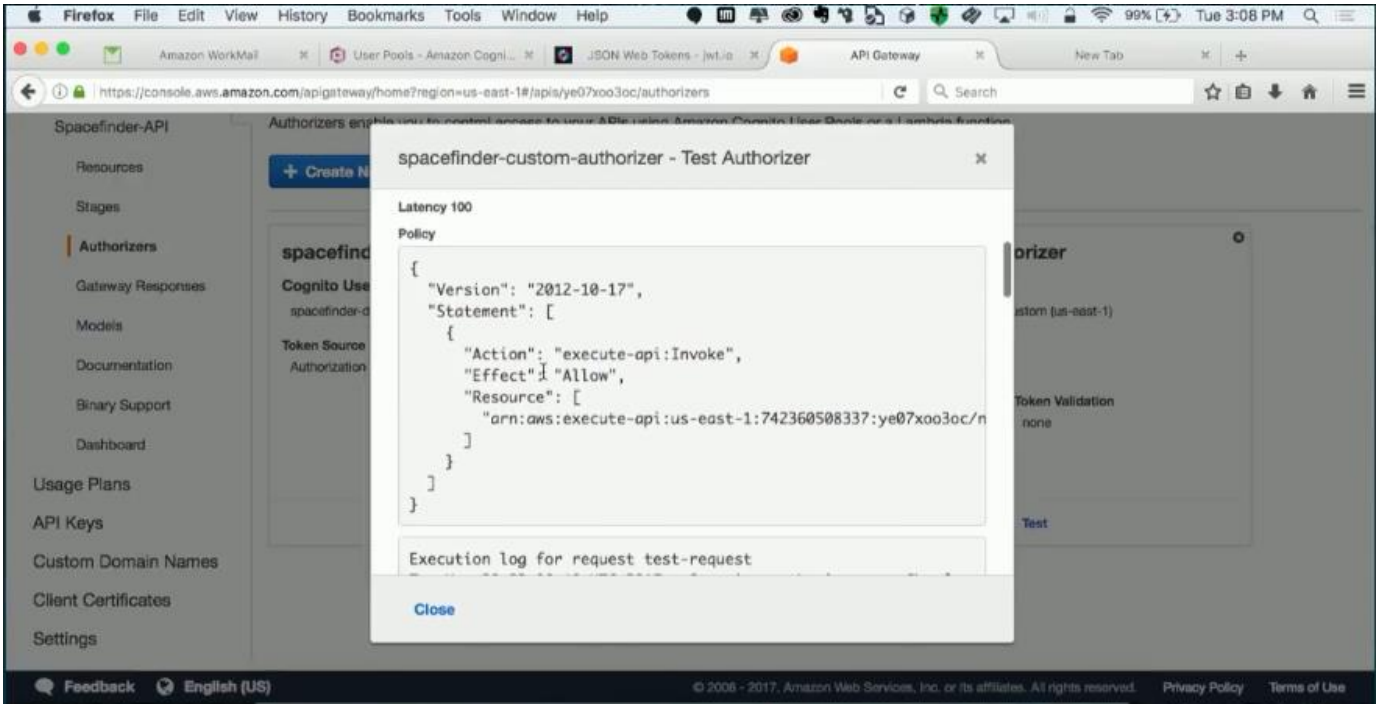


We can now copy this admin identity token and see what policy it is using as below

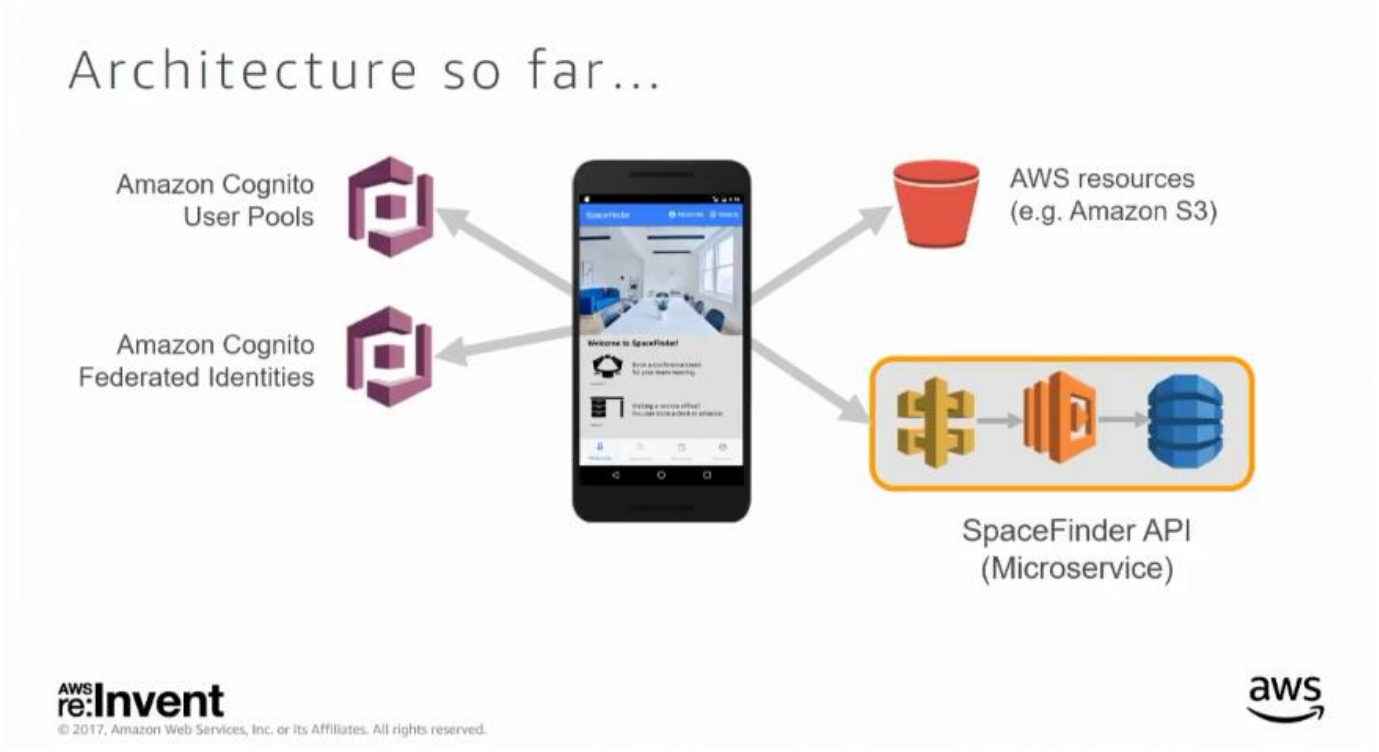




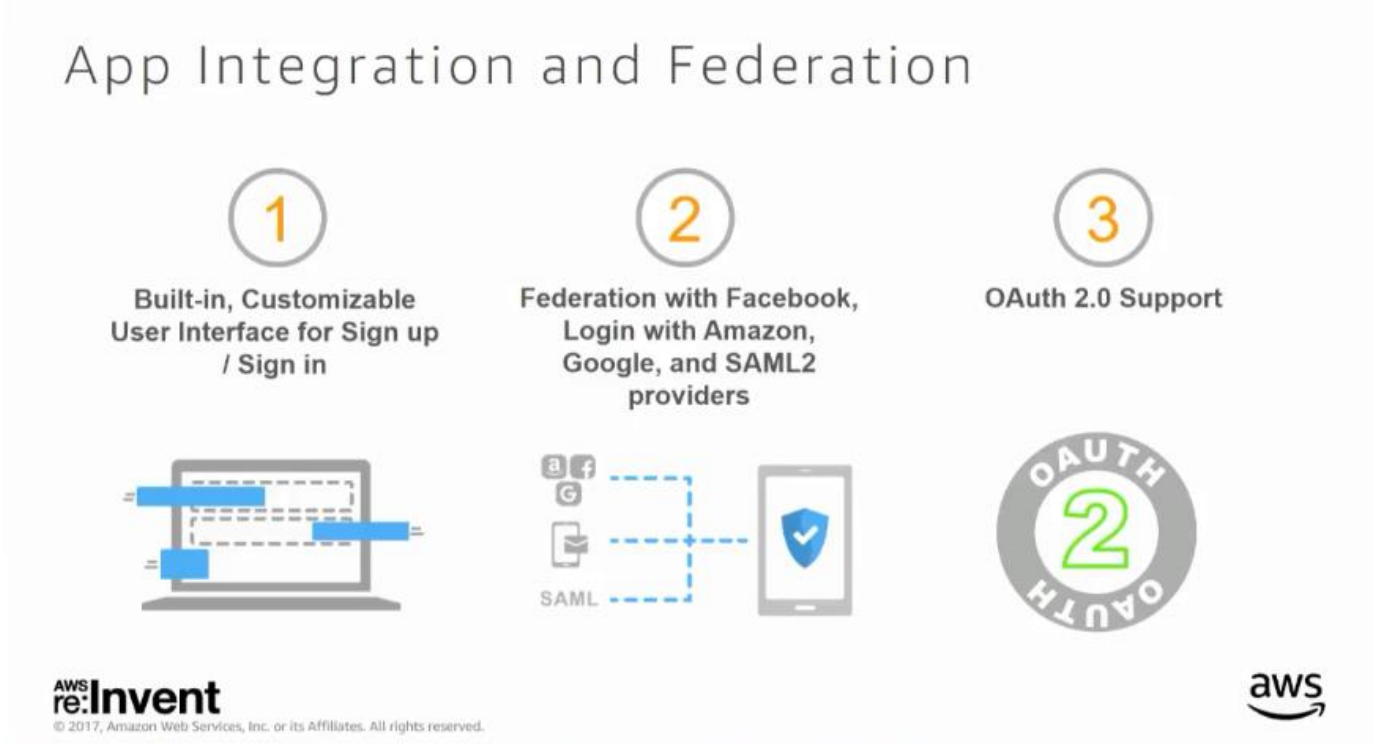
We can check this in our custom authorizer



This policy allows everything, there is no deny statement for this admin role



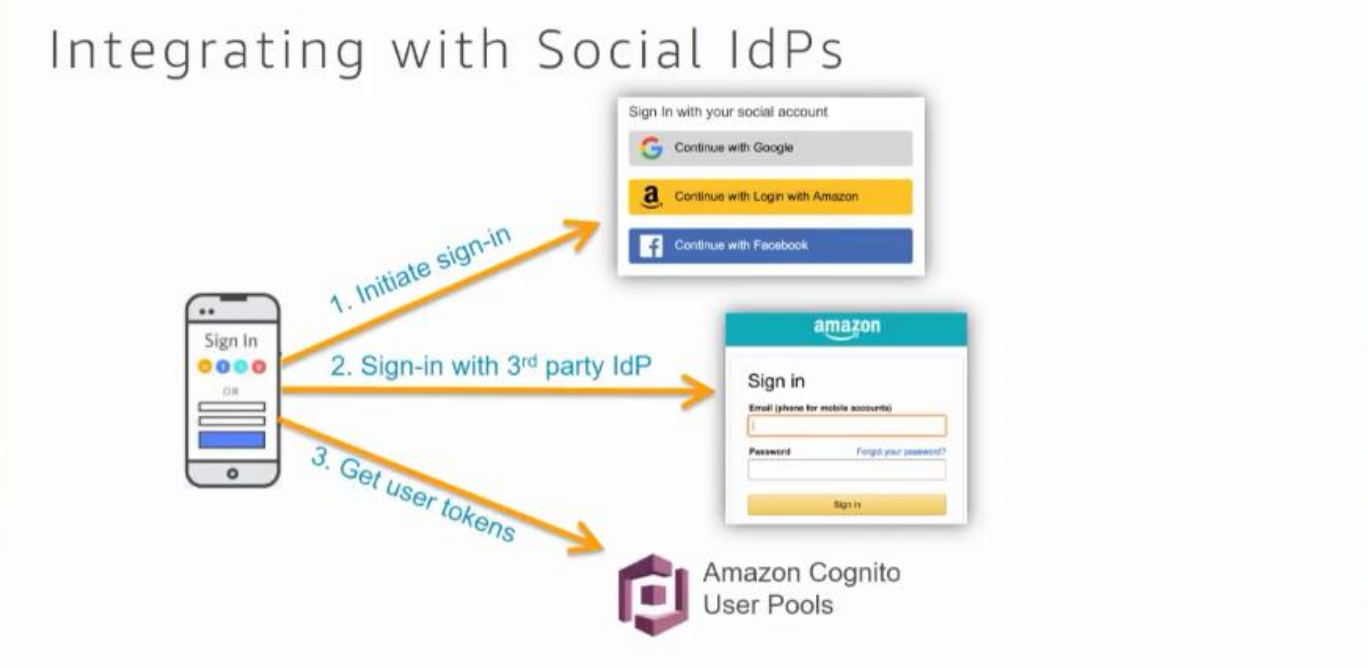
Now the microservice is complete. What is we want to allow users to federate their existing identity provider?



We have released a feature called Hosted UI that allows you to create a custom UI that federates with Facebook, Google, SAML2 providers, etc.

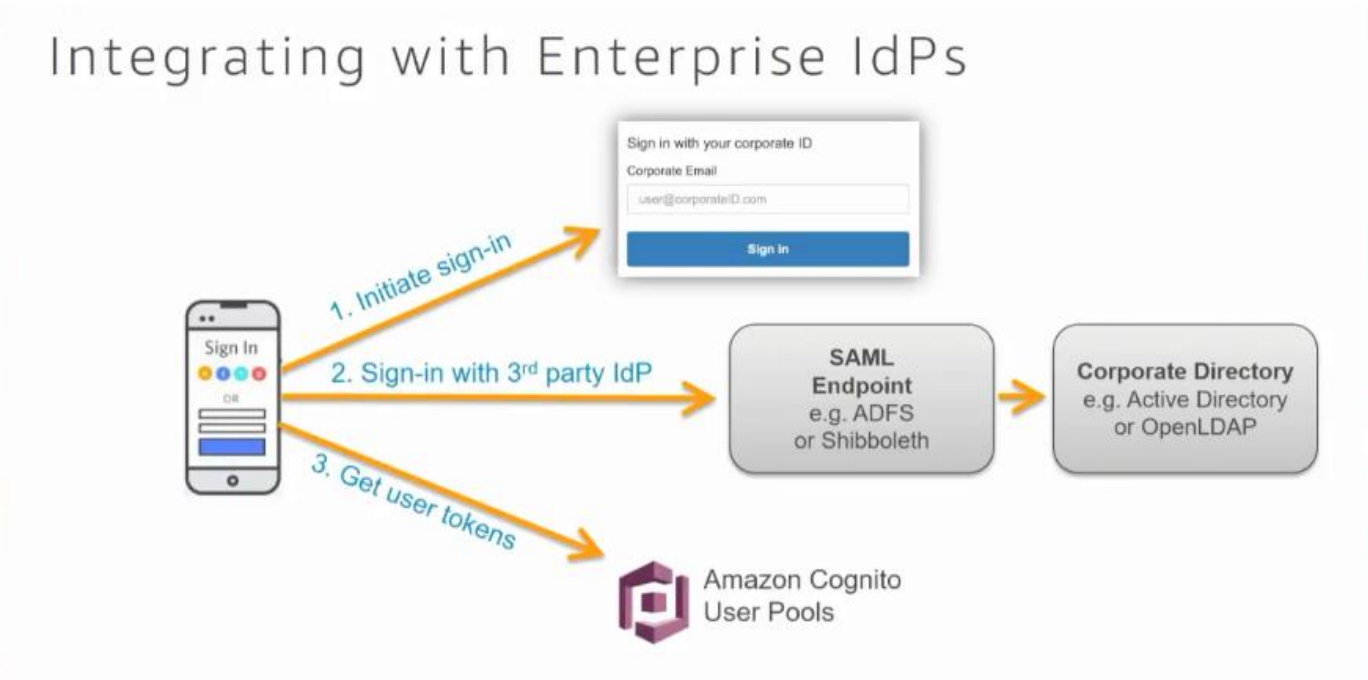
You simply have the Hosted UI presented to the user,

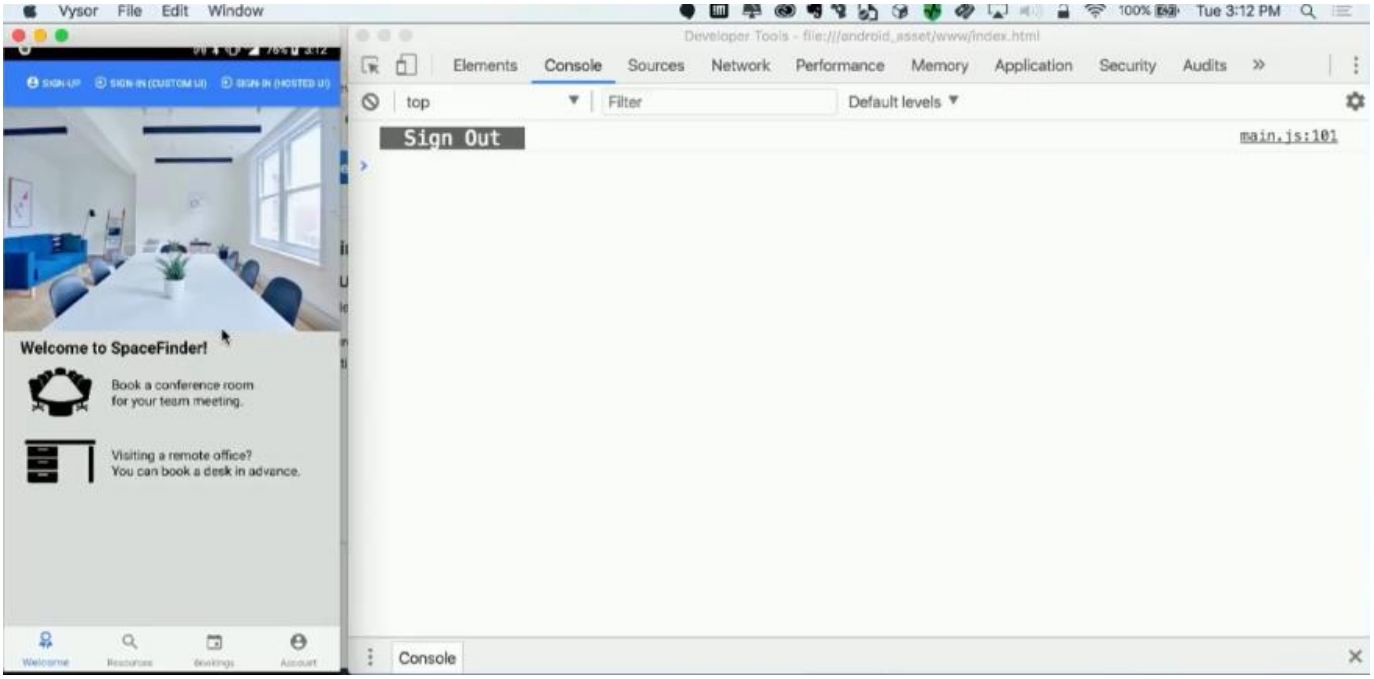
The user is then redirected to the 3rd party sign in page as above,



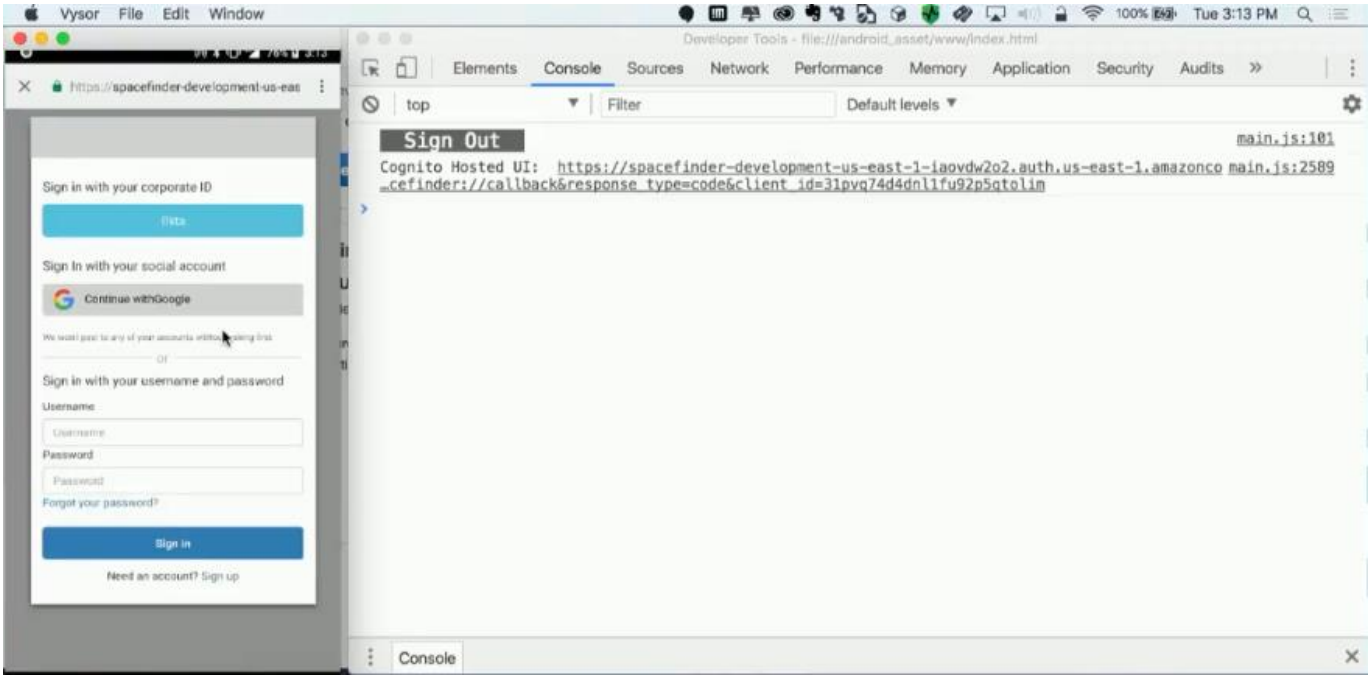
The user is then redirected to Cognito User Pools with all the credentials and and additional credentials from the 3rd party providers too.

With SAML for your enterprise IdPs, the process is similar

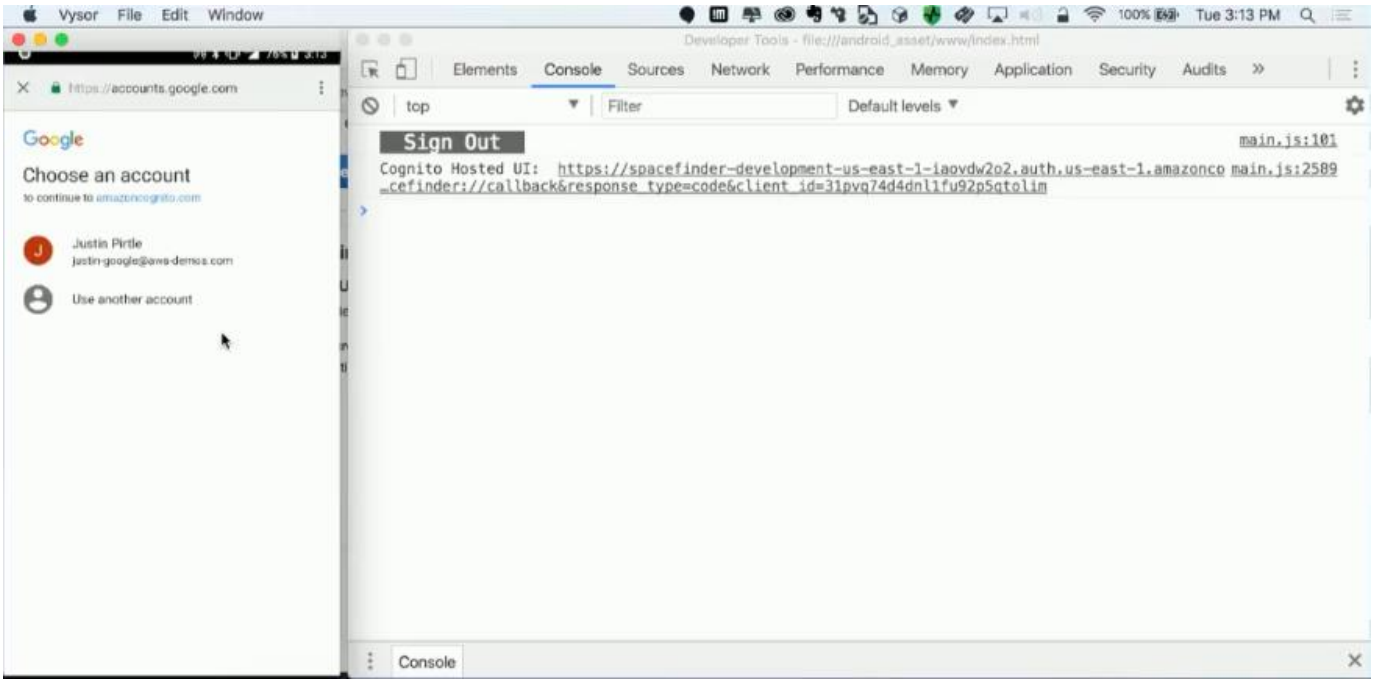


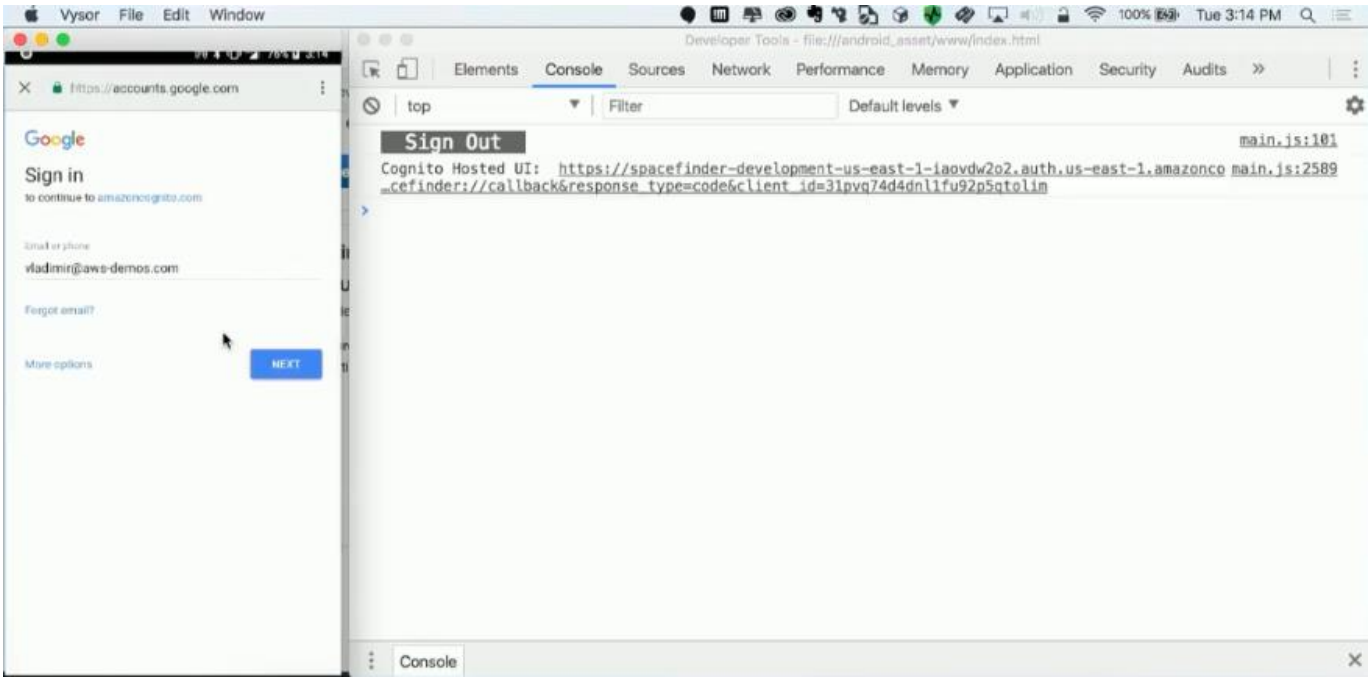


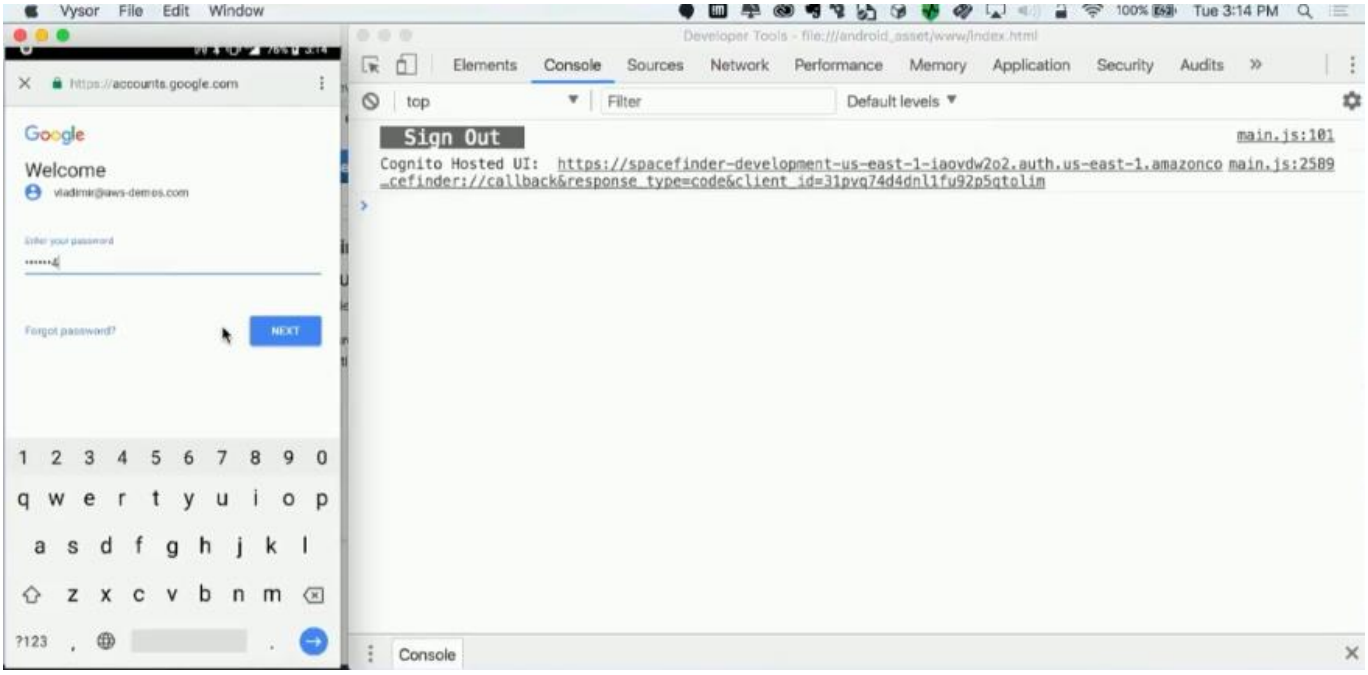
We now have a Hosted UI option that we can click on

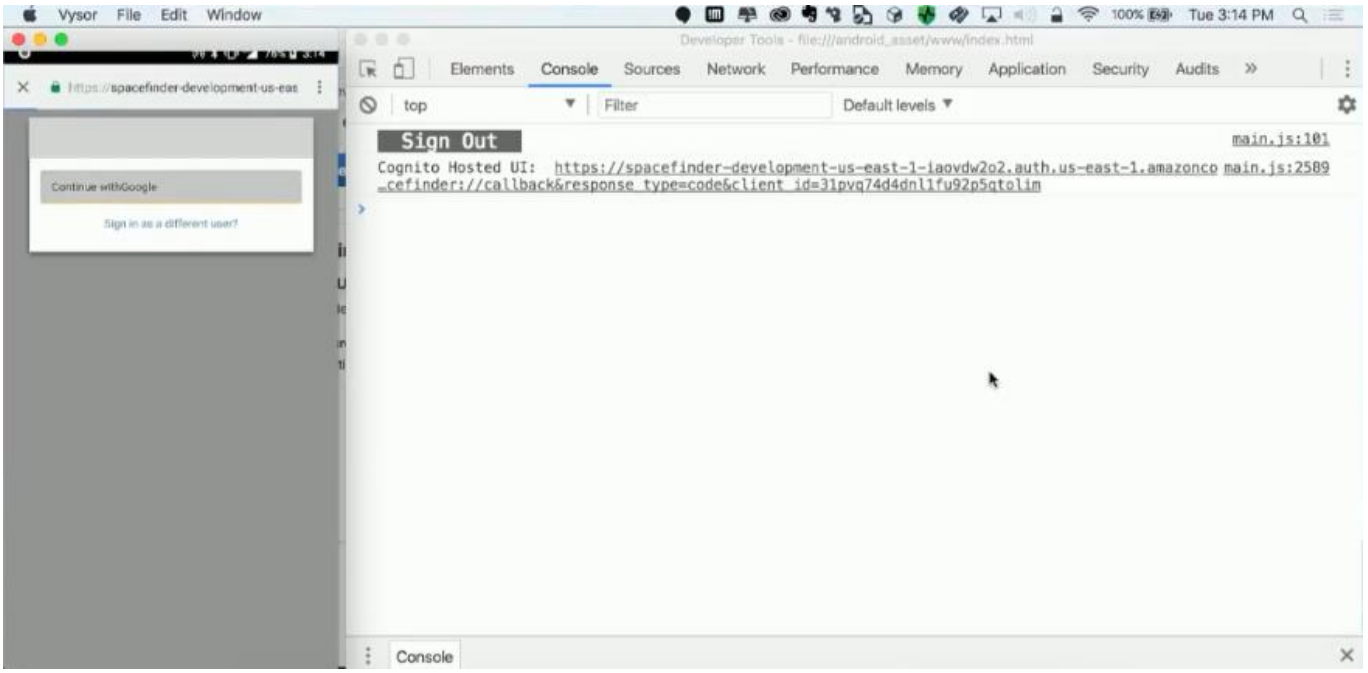


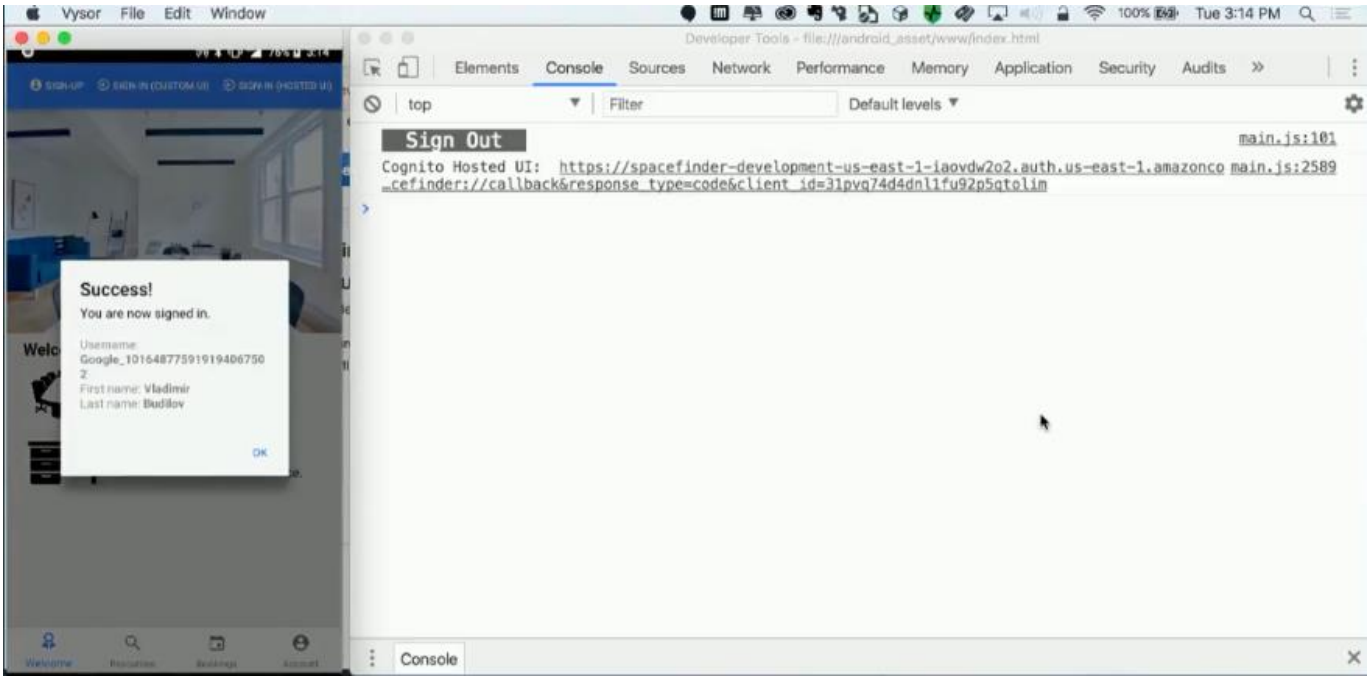
We get the above UI that is customizable. We can sign in with our username and password, or federate with any of the 3rd party providers and Cognito will take care of the coordination like mapping attributes or having an endpoint that you can receive the POST from in SAML response.


Vysor File Edit Window
Tue 3:13 PM
https://accounts.google.com
Google
Choose an account
to continue to amazoncognito.com
Justin Pirtle
justin-google@aws-demos.com
Use another account
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
…cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console

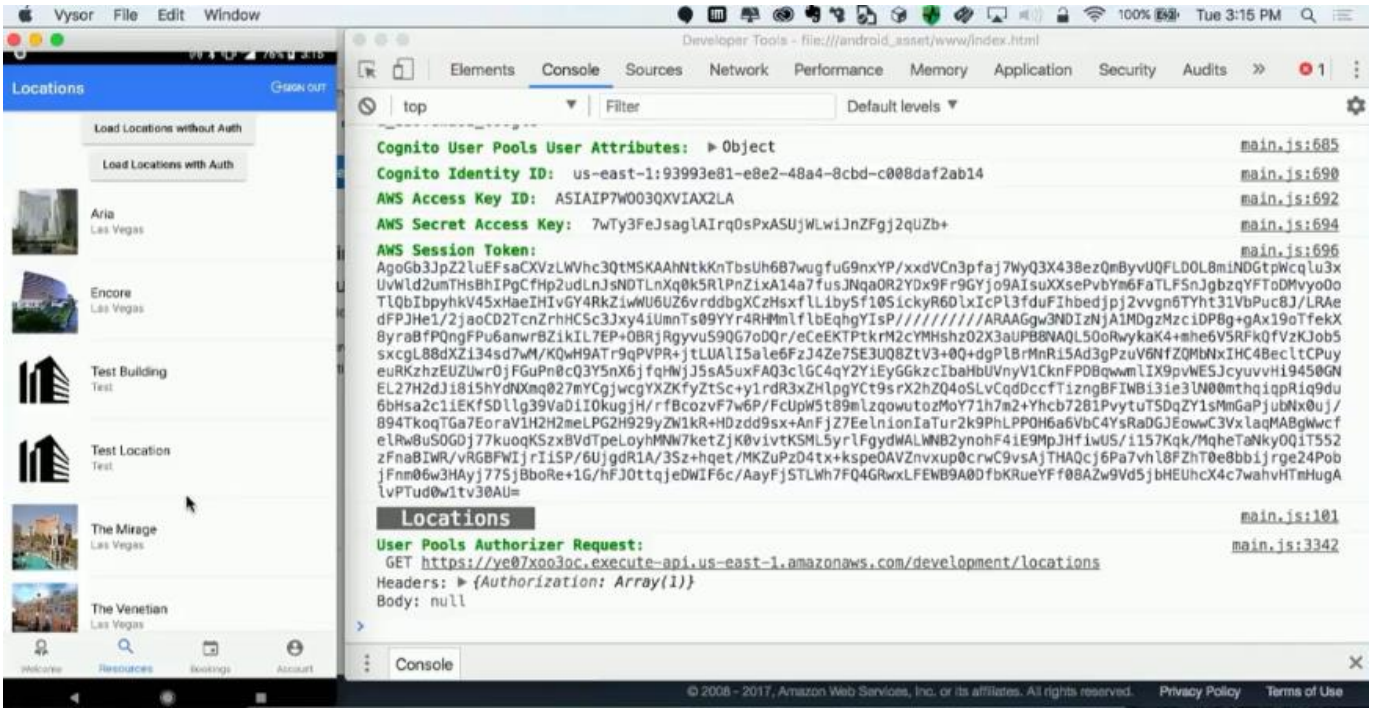

Vysor File Edit Window
Tue 3:14 PM
https://accounts.google.com
Google
Sign in
to continue to amazoncognito.com
vladimir@aws-demos.com
Forgot email?
More options
NEXT
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
…cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console


Vysor File Edit Window
Tue 3:14 PM
https://accounts.google.com
Google
Welcome
vladmir@aws-demos.com
Forgot password?
NEXT
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
_cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console

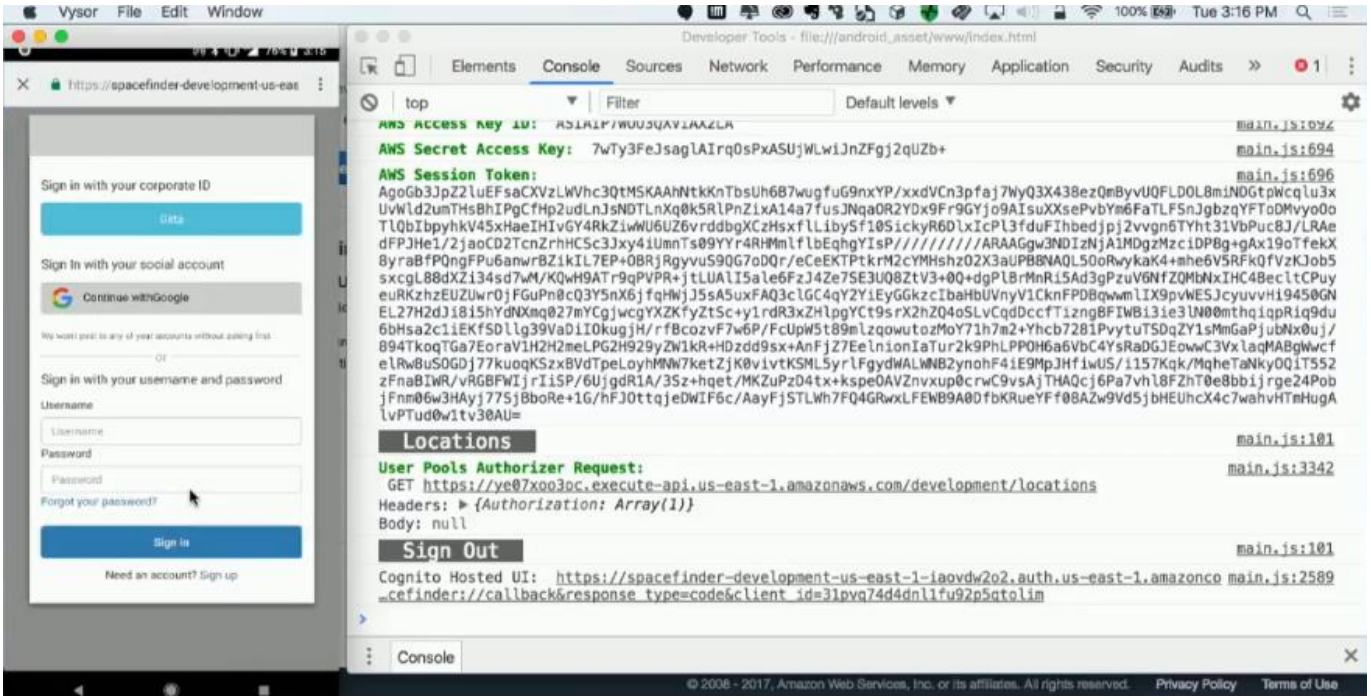

Vysor File Edit Window
Tue 3:14 PM
https://spacefinder-development-us-eas
Continue with Google
Sign in as a different user?
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
_cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console



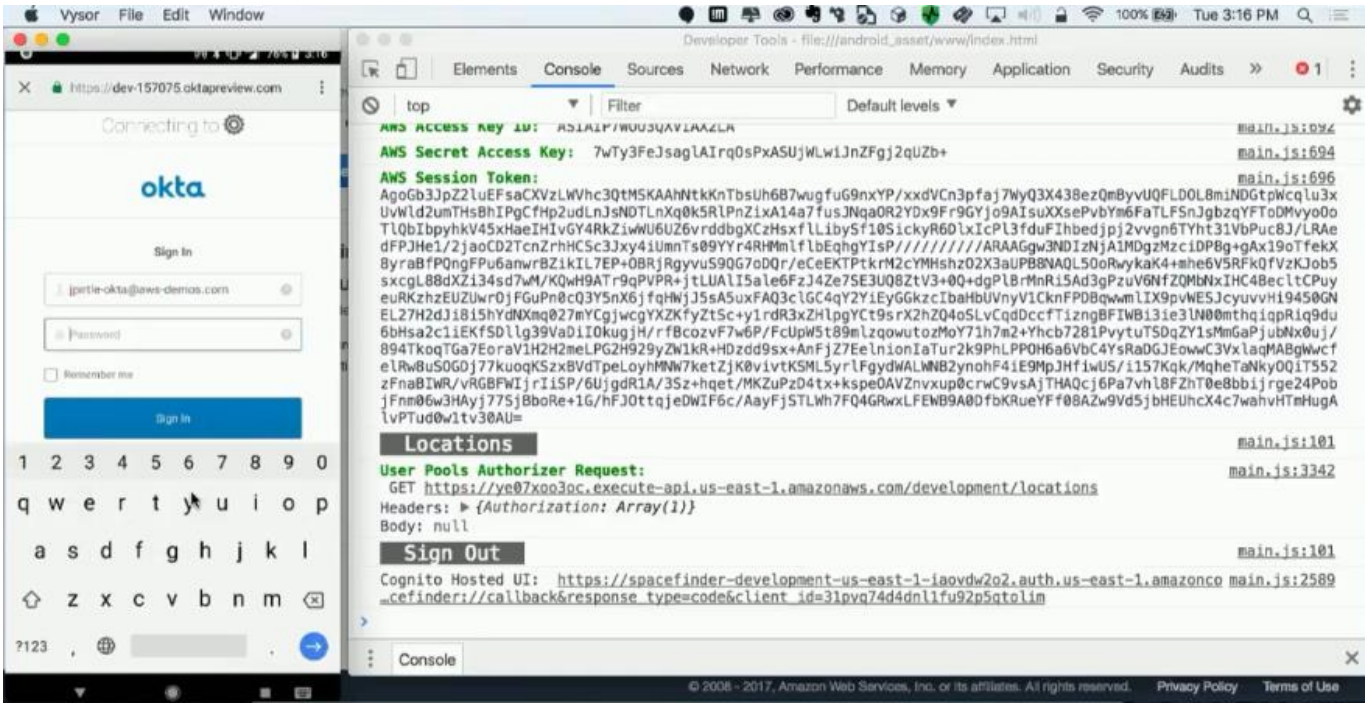
Because this is a mobile app, especially if you were doing a SAML response directly. SAML only supports a redirect response for a POST back to your client. But on a mobile device this is not an easy option. Cognito helps by intercepting that POST response from the SAML provider and provides us a standardized set of these JWT tokens that are always the same regardless of where you came from. We then get the callback from Cognito itself to actually do the sign in.

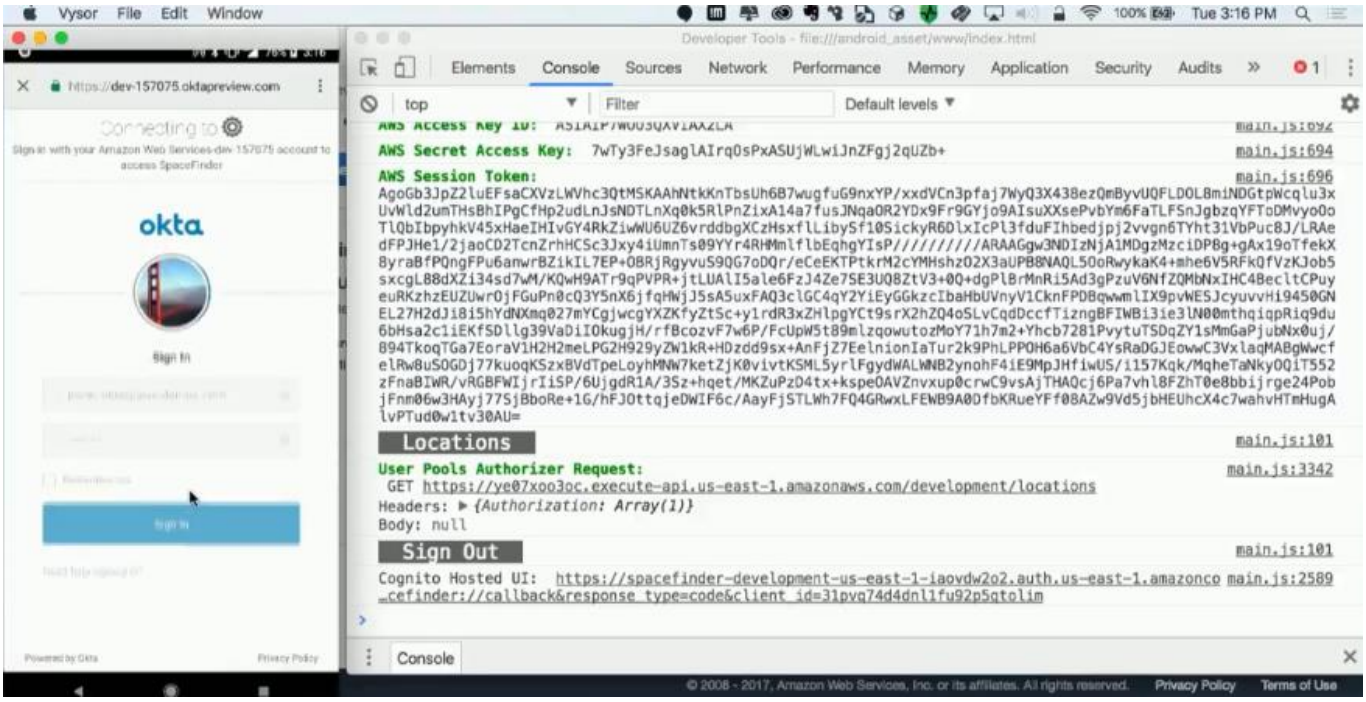


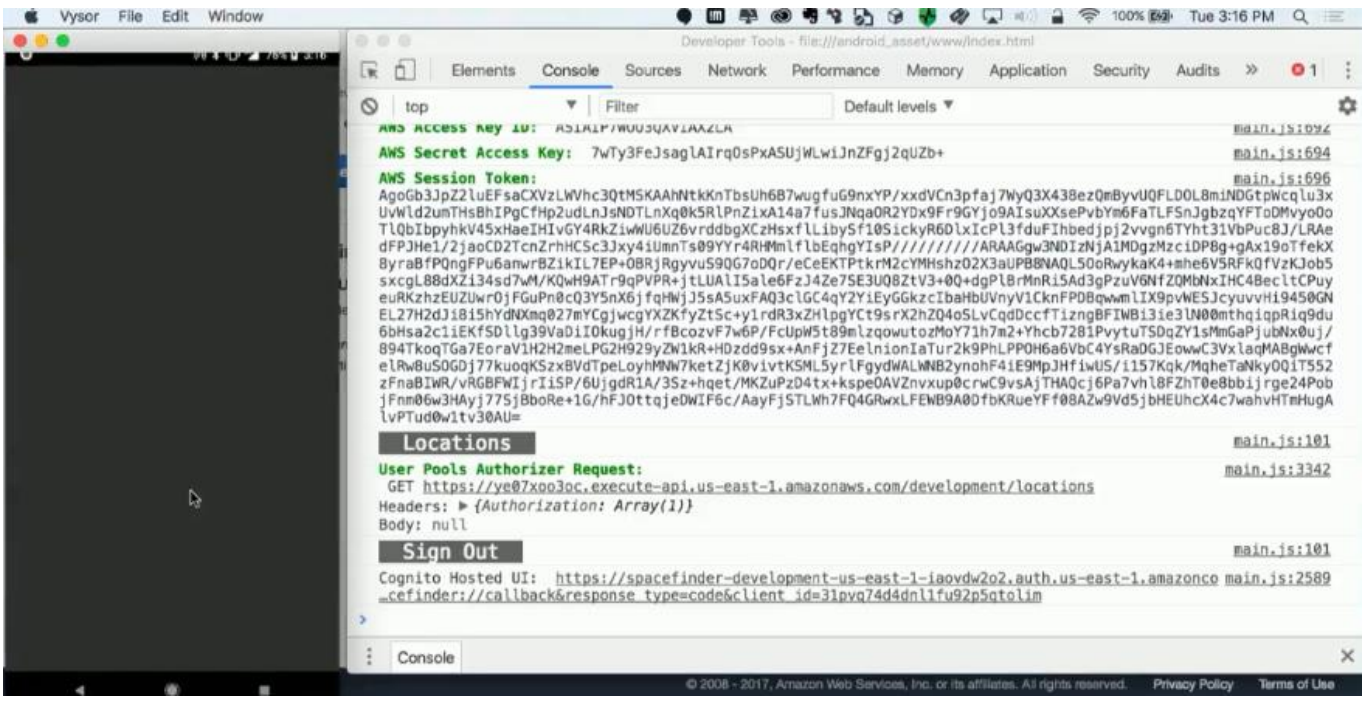
We get the same set of tokens as before.

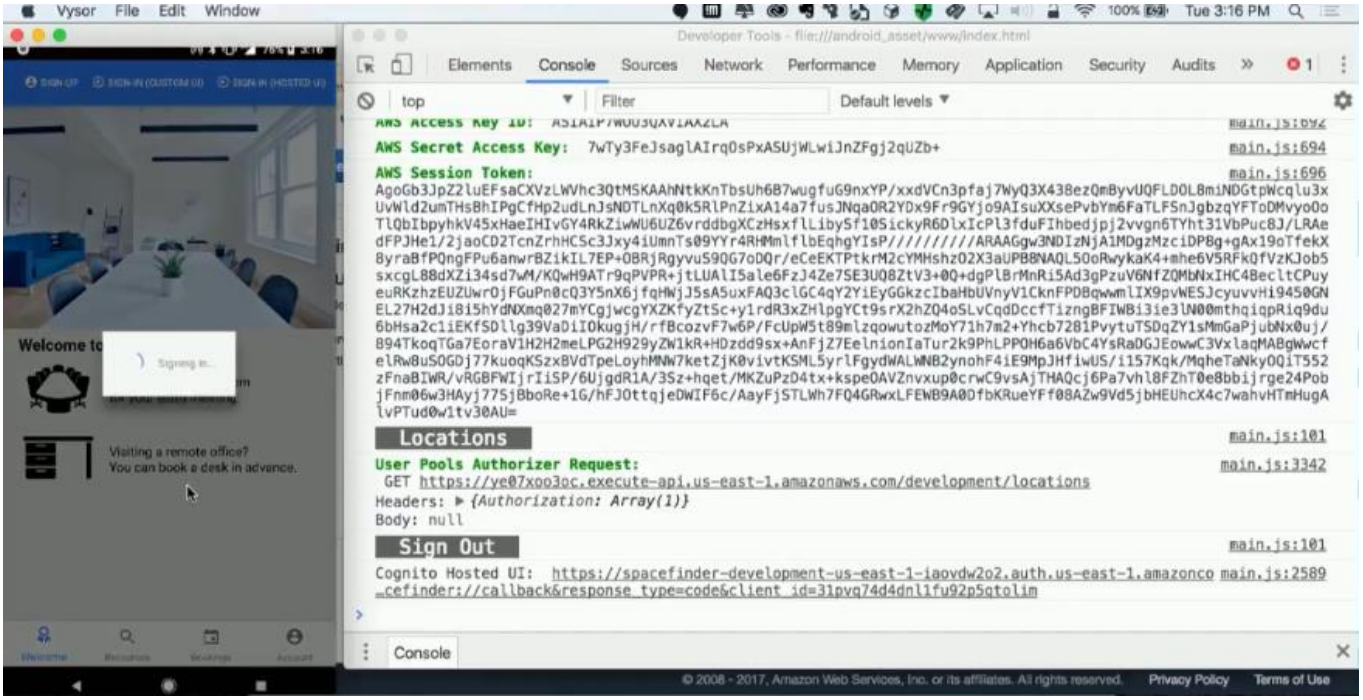


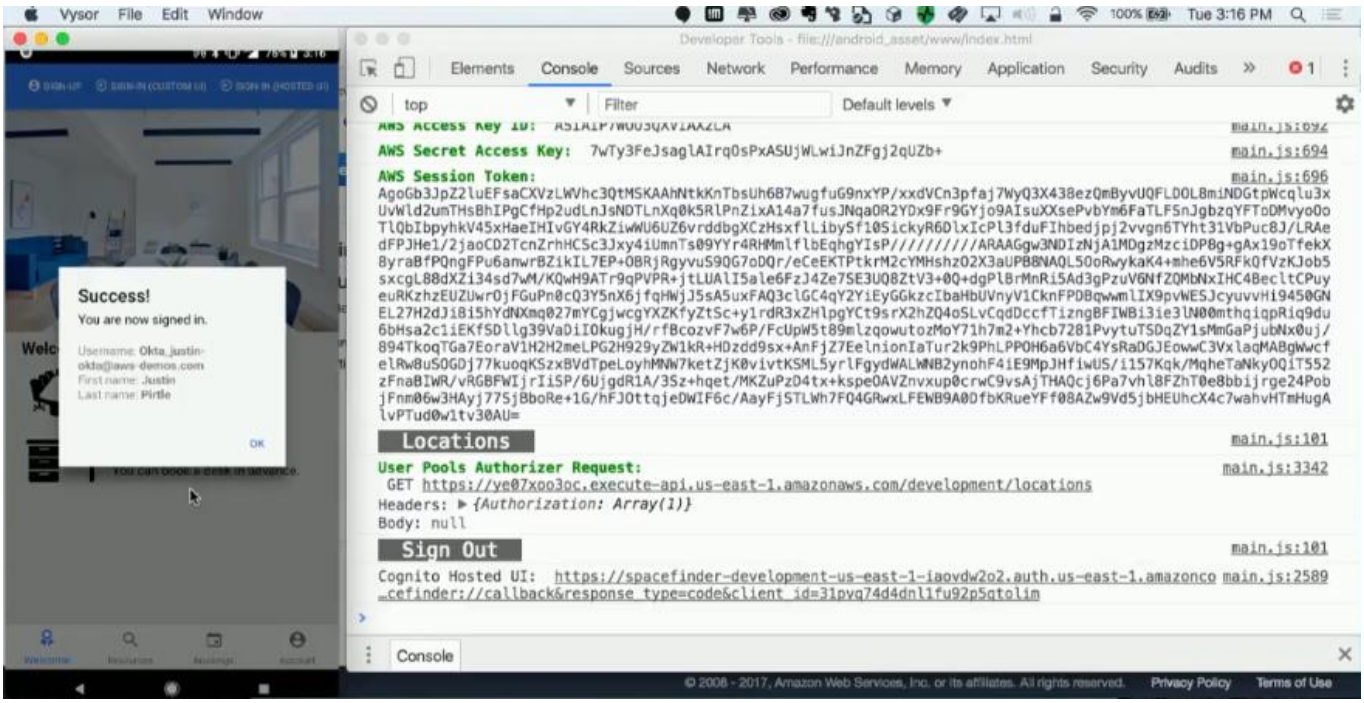
Next, let us sign out and try a SAML2.0 compliant provider like Okta below

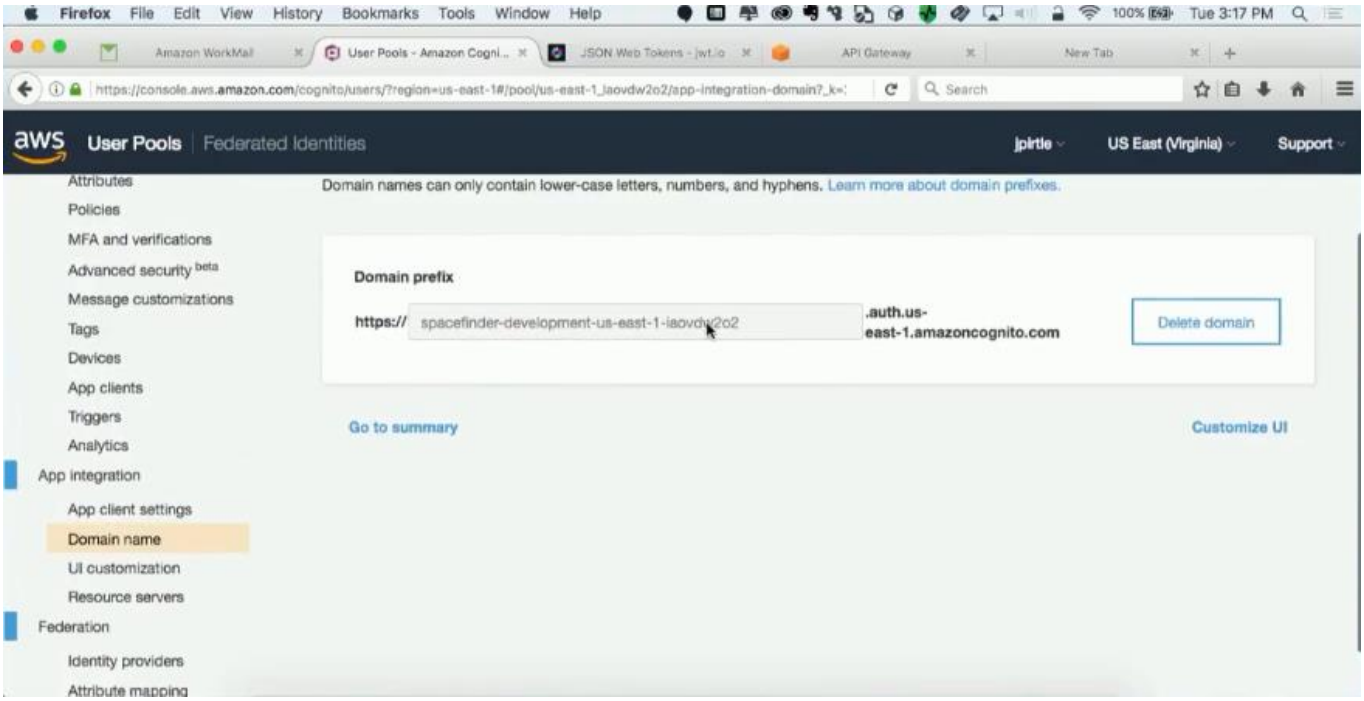


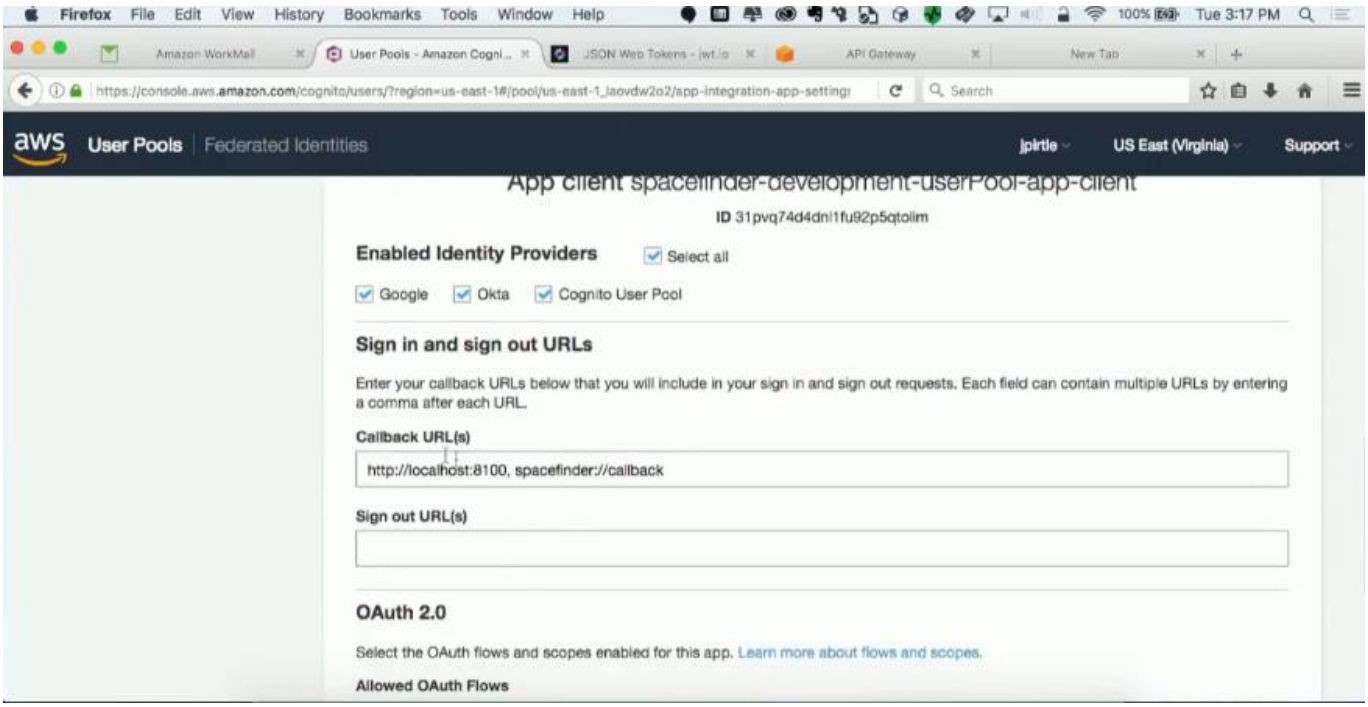

Vysor File Edit Window
Tue 3:16 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
AWS Secret Access Key: 7wTy3FeJsaglAIrqOsPxASUjWLwiJnZFgj2qUZb+
main.js:694
AWS Session Token:
main.js:696
Locations
main.js:101
User Pools Authorizer Request:
main.js:3342
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations
Headers: {Authorization: Array(1)}
Body: null
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco
main.js:2589
Console
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

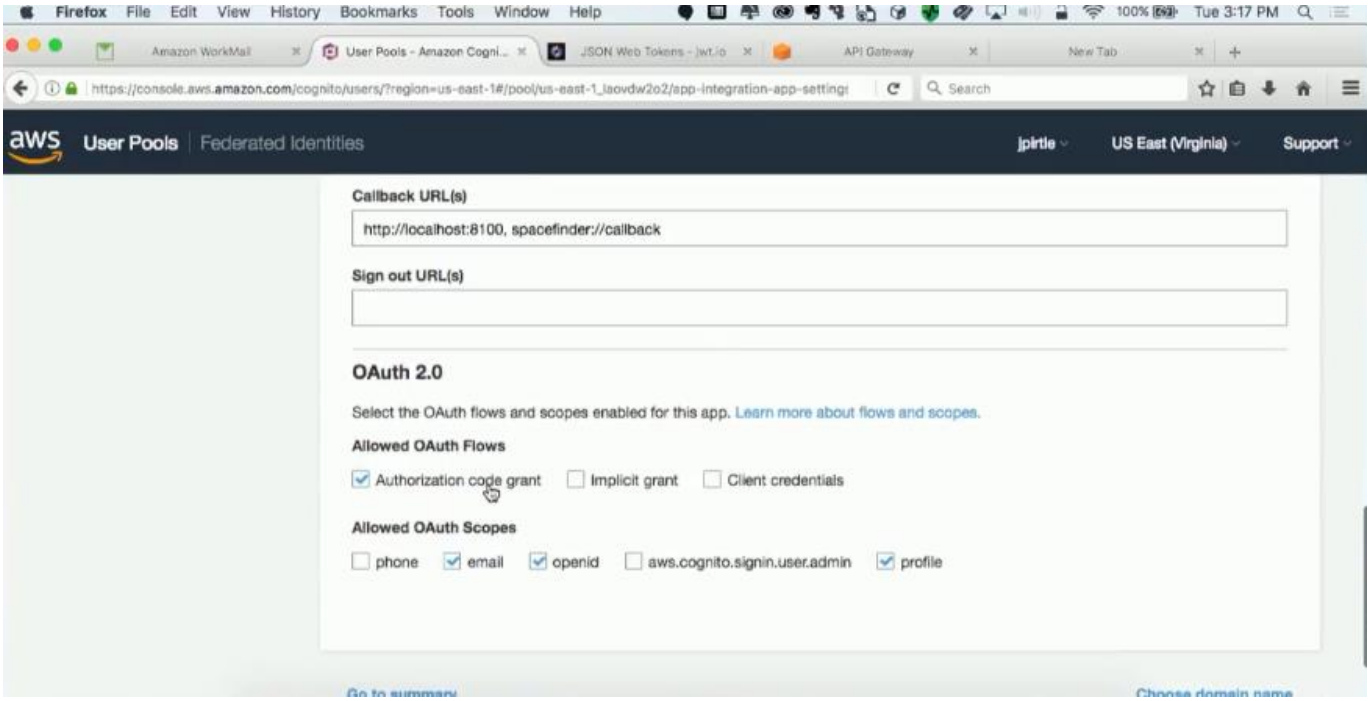

Vysor File Edit Window
Tue 3:16 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
AWS Secret Access Key: 7wTy3FeJsaglAIrqOsPxASUjWLwiJnZFgj2qUZb+
main.js:694
AWS Session Token:
main.js:696
Locations
main.js:101
User Pools Authorizer Request:
main.js:3342
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations
Headers: {Authorization: Array(1)}
Body: null
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco
main.js:2589
Console
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

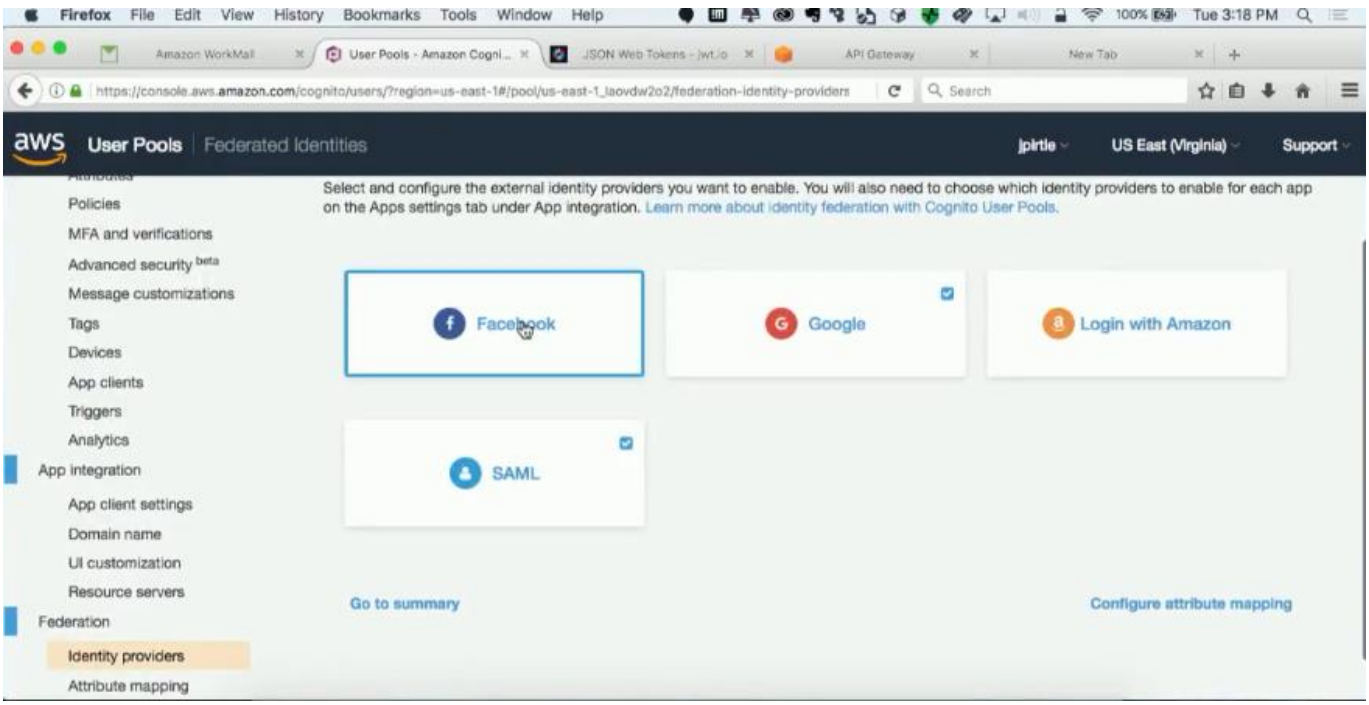

Vysor File Edit Window
Tue 3:16 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
AWS Secret Access Key: 7wTy3FeJsaglAIrqOsPxASUjWLwiJnZFgj2qUZb+
main.js:694
AWS Session Token:
main.js:696
AgoGb3JpZ2luEFsaCXVzLWVhc3QtMSKAAhNtkKnTbsUh6B7wugfuG9nxYP/xxdVCn3pfaj7WyQ3X438ezQmByvUQFLDOL8miNDGtpWcqlu3x
UvWld2umTHsBhIPgCfHp2udLnJsNDTLnXq0k5RlPnZixA14a7fusJNqaOR2YDx9Fr9GYjo9AIsuXXsePvbYm6FaTLF5nJgbzqYFToDMvyoOo
TlQbIbpyhkV45xHaeIHIvGY4RkZiwWU6UZ6vrddbgXCzHsxflLiby5f10SickyR6DlxIcPl3fduFIhbedjpj2vvgn6TYht31VbPuc8J/LRAe
dFPJHe1/2jaoCD2TcnZrhHCSc3Jxy4iUmnTs09YYr4RHMmlflbEqhgYIsP//////////ARAAGgw3NDIzNjA1MDgzMzciDPBg+gAx19oTfekX
8yraBfPQngFPu6anwrBZikIL7EP+OBRjRgyvuS9QG7oDQr/eCeEKTPtkrM2cYMHshzO2X3aUPB8NAQL5OoRwykaK4+mhe6V5RFkQfVzKJob5
sxcgL88dXZi34sd7wM/KQwH9ATr9qPVPR+jtLUAlI5ale6FzJ4Ze7SE3UQ8ZtV3+0Q+dgPlBrMnRi5Ad3gPzuV6NfZQMbNxIHC4BecltCPuy
euRKzhzEUZUwrOjFGuPn0cQ3Y5nX6jfqHWjJ5sA5uxFAQ3clGC4qY2YiEyGGkzcIbaHbUVnyV1CknFPDBqwwmlIX9pvWESJcyuvvHi9450GN
EL27H2dJi8i5hYdNXmq027mYCgjwcgYXZKfyZtSc+y1rdR3xZHlpgYCt9srX2hZQ4oSLvCqdDccfTizngBFIWBi3ie3lN00mthqipRiq9du
6bHsa2c1iEKfSDllg39VaDiIOkugjH/rfBcozvF7w6P/FcUpW5t89mlzqowutozMoY71h7m2+Yhcb7281PvytuTSDqZY1sMmGaPjubNx0uj/
894TkoqTGa7EoraV1H2H2meLPG2H929yZW1kR+HDzdd9sx+AnFjZ7EelnionIaTur2k9PhLPPOH6a6VbC4YsRaDGJEowwC3VxlaqMABgWwcf
elRw8uSOGDj77kuoqKSzxBVdTpeLoyhMNW7ketZjK0vivtKSML5yrlFgydWALWNB2ynohF4iE9MpJHfiwUS/i157Kqk/MqheTaNkyOQiT552
zFnaBIWR/vRGBFWIjrIiSP/6UjgdR1A/3Sz+hqet/MKZuPzD4tx+kspeOAVZnvxup0crwC9vsAjTHAQcj6Pa7vhl8FZhT0e8bbijrge24Pob
jFnm06w3HAyj77SjBboRe+1G/hFJOttqjeDWIF6c/AayFjSTLWh7FQ4GRwxLFEWB9A0DfbKRueYFf08AZw9Vd5jbHEUhcX4c7wahvHTmHugA
lvPTud0w1tv30AU=
Locations
main.js:101
User Pools Authorizer Request:
main.js:3342
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations
Headers: ▶ {Authorization: Array(1)}
Body: null
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
…cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console
Welcome to
Visiting a remote office?
You can book a desk in advance.
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

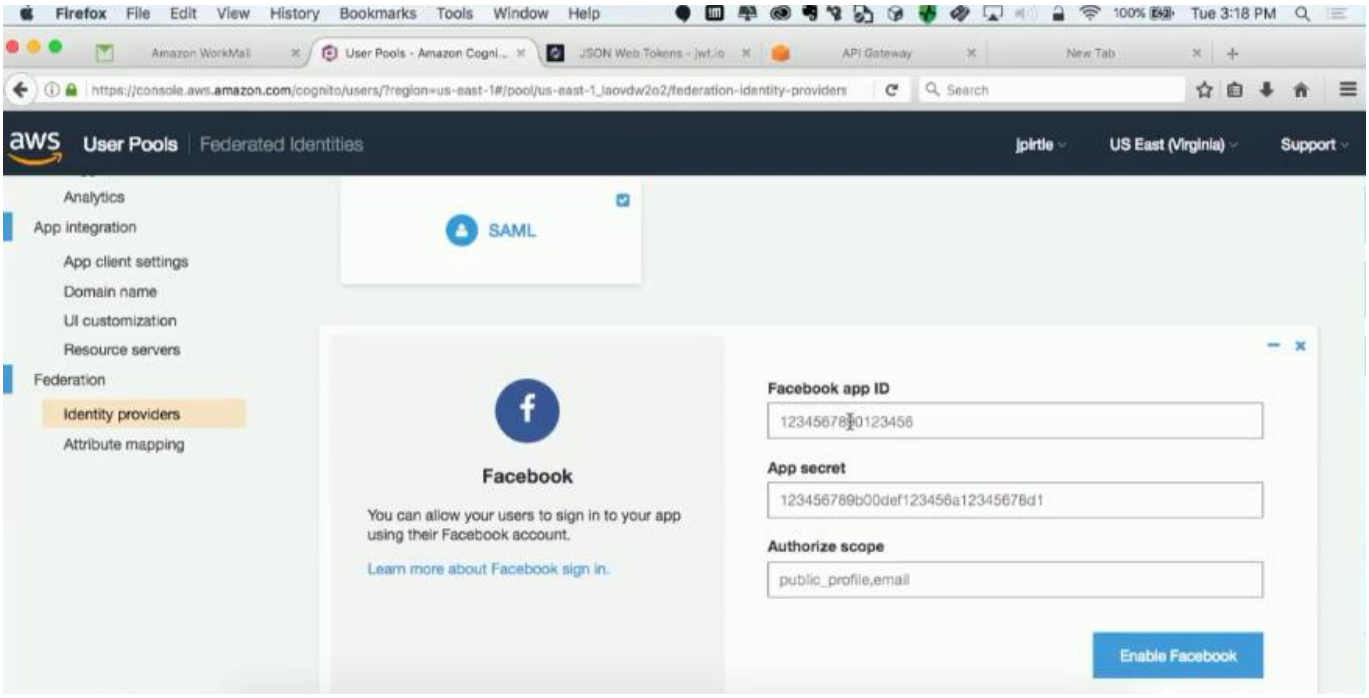

Vysor File Edit Window
Tue 3:16 PM
Developer Tools - file:///android_asset/www/index.html
Elements Console Sources Network Performance Memory Application Security Audits
top
Filter
Default levels
AWS Secret Access Key: 7wTy3FeJsaglAIrqOsPxASUjWLwiJnZFgj2qUZb+
main.js:694
AWS Session Token:
main.js:696
AgoGb3JpZ2luEFsaCXVzLWVhc3QtMSKAAhNtkKnTbsUh6B7wugfuG9nxYP/xxdVCn3pfaj7WyQ3X438ezQmByvUQFLDOL8miNDGtpWcqlu3x
UvWld2umTHsBhIPgCfHp2udLnJsNDTLnXq0k5RlPnZixA14a7fusJNqaOR2YDx9Fr9GYjo9AIsuXXsePvbYm6FaTLF5nJgbzqYFToDMvyoOo
TlQbIbpyhkV45xHaeIHIvGY4RkZiwWU6UZ6vrddbgXCzHsxflLiby5f10SickyR6DlxIcPl3fduFIhbedjpj2vvgn6TYht31VbPuc8J/LRAe
dFPJHe1/2jaoCD2TcnZrhHCSc3Jxy4iUmnTs09YYr4RHMmlflbEqhgYIsP//////////ARAAGgw3NDIzNjA1MDgzMzciDPBg+gAx19oTfekX
8yraBfPQngFPu6anwrBZikIL7EP+OBRjRgyvuS9QG7oDQr/eCeEKTPtkrM2cYMHshzO2X3aUPB8NAQL5OoRwykaK4+mhe6V5RFkQfVzKJob5
sxcgL88dXZi34sd7wM/KQwH9ATr9qPVPR+jtLUAlI5ale6FzJ4Ze7SE3UQ8ZtV3+0Q+dgPlBrMnRi5Ad3gPzuV6NfZQMbNxIHC4BecltCPuy
euRKzhzEUZUwrOjFGuPn0cQ3Y5nX6jfqHWjJ5sA5uxFAQ3clGC4qY2YiEyGGkzcIbaHbUVnyV1CknFPDBqwwmlIX9pvWESJcyuvvHi9450GN
EL27H2dJi8i5hYdNXmq027mYCgjwcgYXZKfyZtSc+y1rdR3xZHlpgYCt9srX2hZQ4oSLvCqdDccfTizngBFIWBi3ie3lN00mthqipRiq9du
6bHsa2c1iEKfSDllg39VaDiIOkugjH/rfBcozvF7w6P/FcUpW5t89mlzqowutozMoY71h7m2+Yhcb7281PvytuTSDqZY1sMmGaPjubNx0uj/
894TkoqTGa7EoraV1H2H2meLPG2H929yZW1kR+HDzdd9sx+AnFjZ7EelnionIaTur2k9PhLPPOH6a6VbC4YsRaDGJEowwC3VxlaqMABgWwcf
elRw8uSOGDj77kuoqKSzxBVdTpeLoyhMNW7ketZjK0vivtKSML5yrlFgydWALWNB2ynohF4iE9MpJHfiwUS/i157Kqk/MqheTaNkyOQiT552
zFnaBIWR/vRGBFWIjrIiSP/6UjgdR1A/3Sz+hqet/MKZuPzD4tx+kspeOAVZnvxup0crwC9vsAjTHAQcj6Pa7vhl8FZhT0e8bbijrge24Pob
jFnm06w3HAyj77SjBboRe+1G/hFJOttqjeDWIF6c/AayFjSTLWh7FQ4GRwxLFEWB9A0DfbKRueYFf08AZw9Vd5jbHEUhcX4c7wahvHTmHugA
lvPTud0w1tv30AU=
Locations
main.js:101
User Pools Authorizer Request:
main.js:3342
GET https://ye07xoo3oc.execute-api.us-east-1.amazonaws.com/development/locations
Headers: ▶ {Authorization: Array(1)}
Body: null
Sign Out
main.js:101
Cognito Hosted UI: https://spacefinder-development-us-east-1-iaovdw2o2.auth.us-east-1.amazonco main.js:2589
…cefinder://callback&response_type=code&client_id=31pvq74d4dnl1fu92p5qtolim
Console
Success!
You are now signed in.
Username: Okta_justin-okta@aws-demos.com
First name: Justin
Last name: Pirtle
OK
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:17 PM
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/app-integration-domain?_k=
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Attributes
Policies
MFA and verifications
Advanced security beta
Message customizations
Tags
Devices
App clients
Triggers
Analytics
App integration
App client settings
Domain name
UI customization
Resource servers
Federation
Identity providers
Attribute mapping
Domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.
Domain prefix
https://
spacefinder-development-us-east-1-iaovdw2o2
.auth.us-east-1.amazoncognito.com
Delete domain
Go to summary
Customize UI

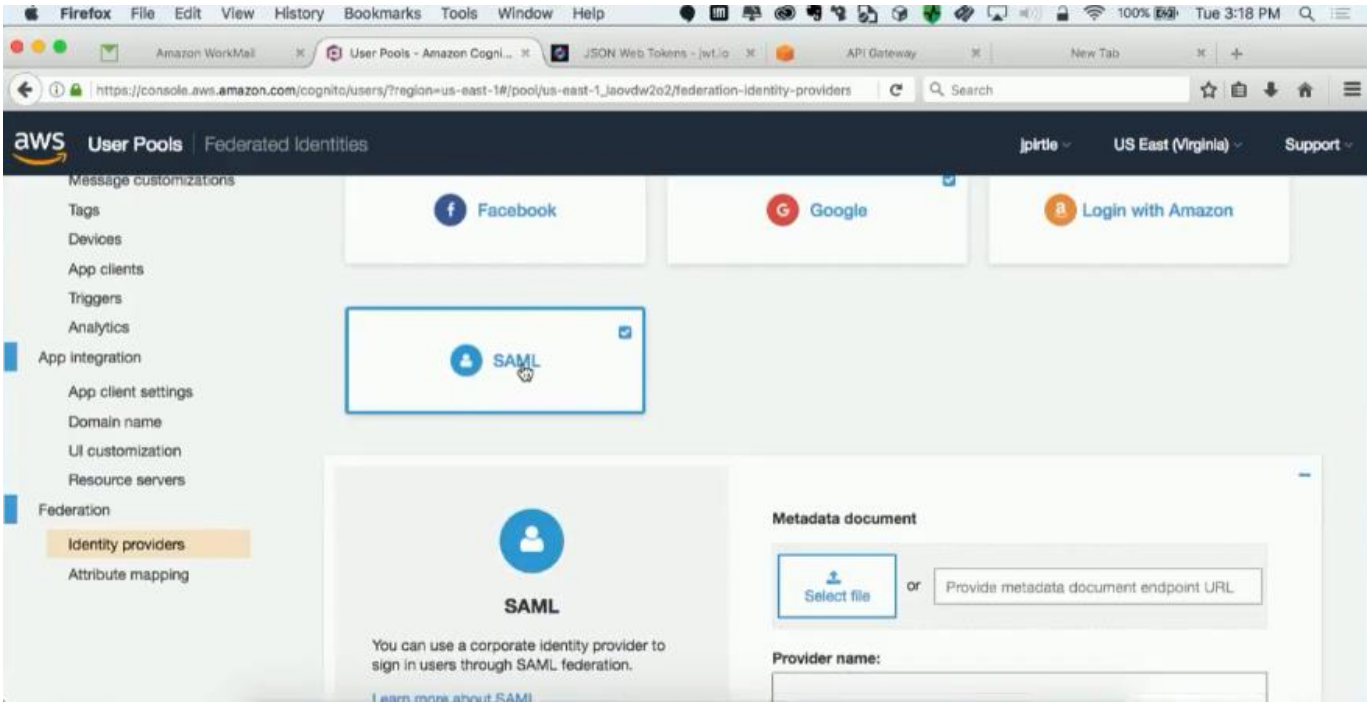

Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:17 PM
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/app-integration-app-setting
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
App client spacefinder-development-userPool-app-client
ID 31pvq74d4dnl1fu92p5qtoiim
Enabled Identity Providers
Select all
Google
Okta
Cognito User Pool
Sign in and sign out URLs
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL.
Callback URL(s)
http://localhost:8100, spacefinder://callback
Sign out URL(s)
OAuth 2.0
Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes.
Allowed OAuth Flows

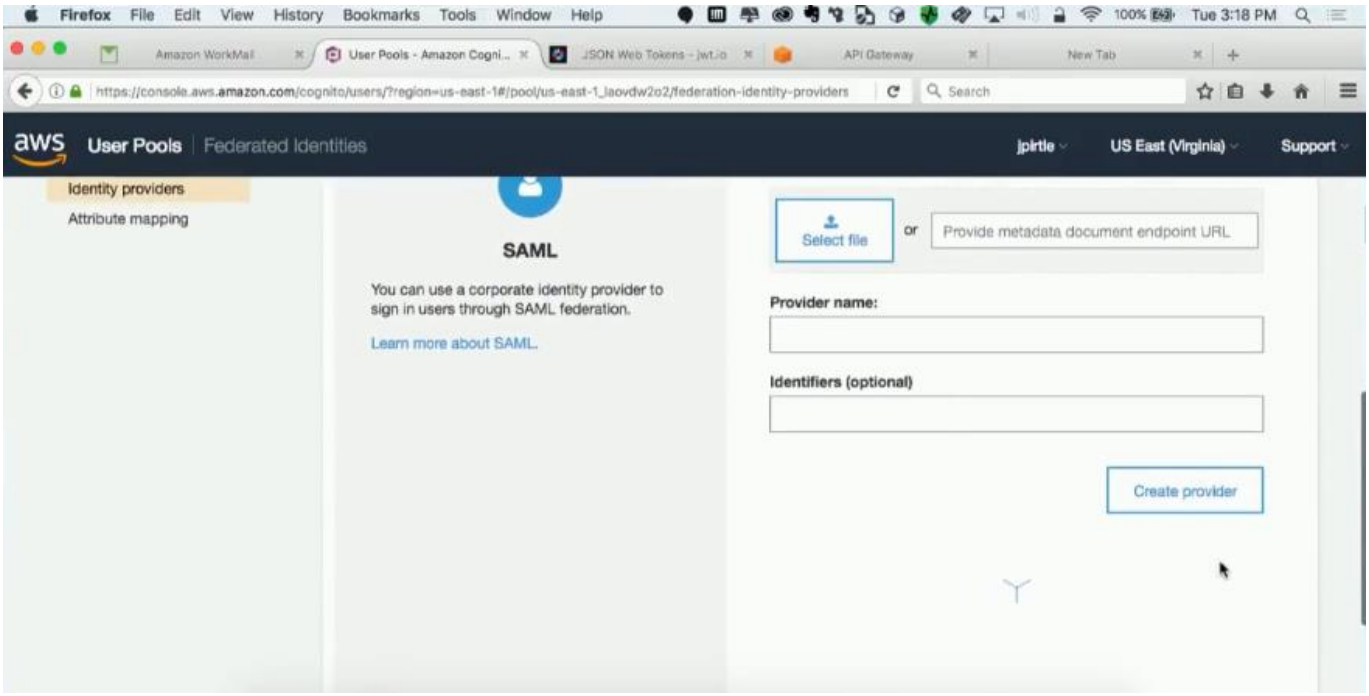

Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:17 PM
User Pools - Amazon Cogni...
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/app-integration-app-settings
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Callback URL(s)
http://localhost:8100, spacefinder://callback
Sign out URL(s)
OAuth 2.0
Select the OAuth flows and scopes enabled for this app. Learn more about flows and scopes.
Allowed OAuth Flows
Authorization code grant
Implicit grant
Client credentials
Allowed OAuth Scopes
phone
email
openid
aws.cognito.signin.user.admin
profile

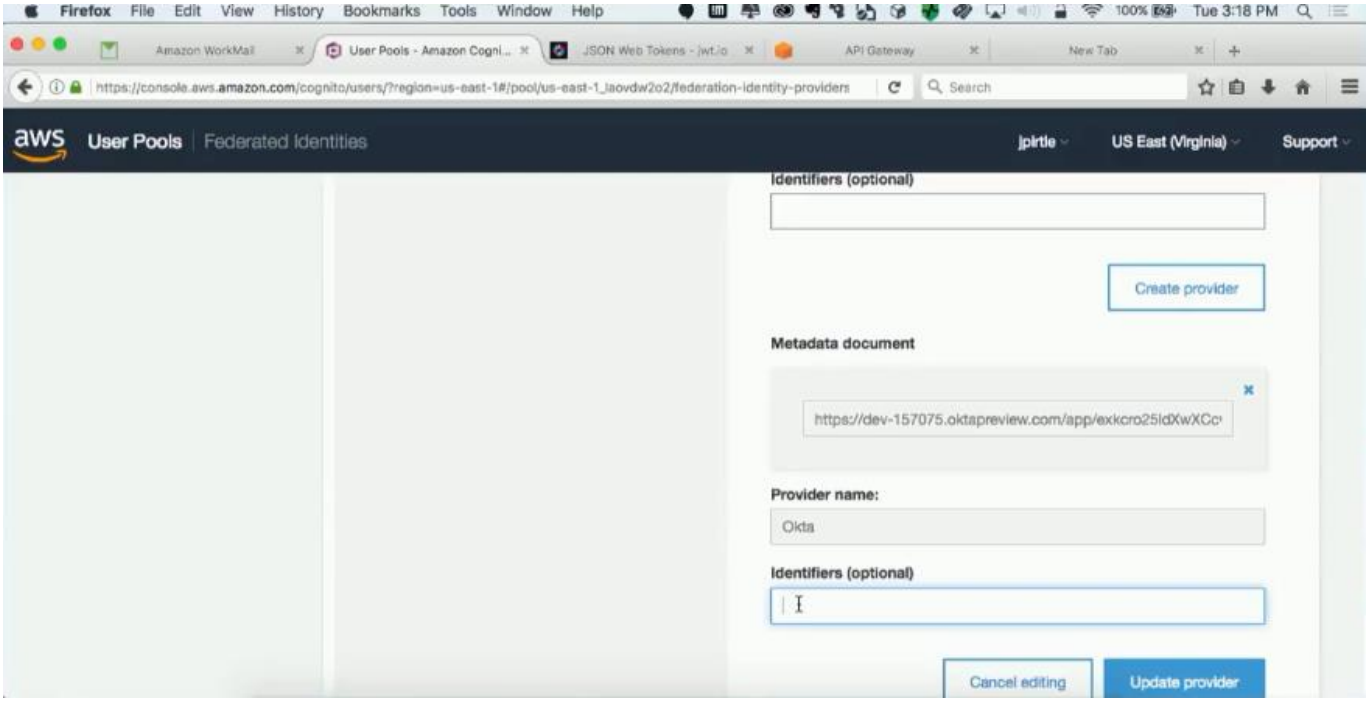

Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:18 PM
User Pools - Amazon Cogni...
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/federation-identity-providers
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Policies
MFA and verifications
Advanced security beta
Message customizations
Tags
Devices
App clients
Triggers
Analytics
App integration
App client settings
Domain name
UI customization
Resource servers
Federation
Identity providers
Attribute mapping
Select and configure the external identity providers you want to enable. You will also need to choose which identity providers to enable for each app on the Apps settings tab under App integration. Learn more about identity federation with Cognito User Pools.
Facebook
Google
Login with Amazon
SAML
Go to summary
Configure attribute mapping



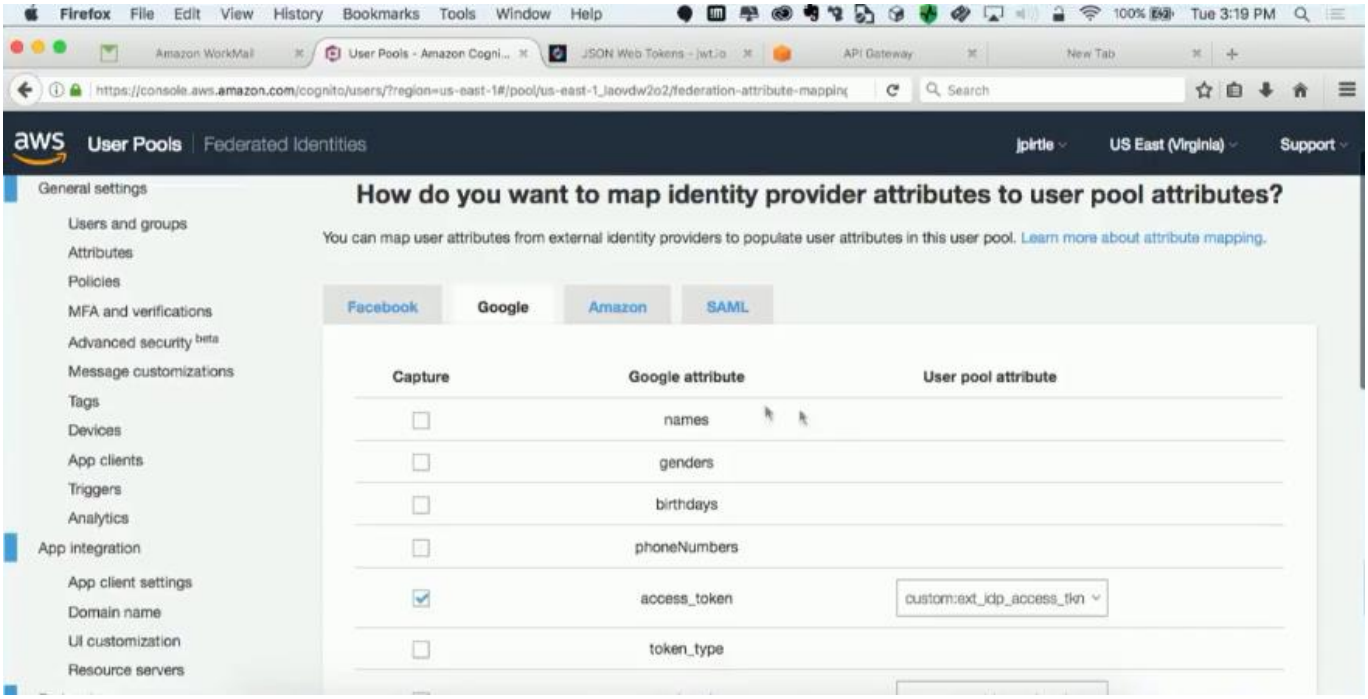
Register an application on the Facebook developer portal, then come and paste in the app ID and secret in the form above, and the scopes you want to allow.

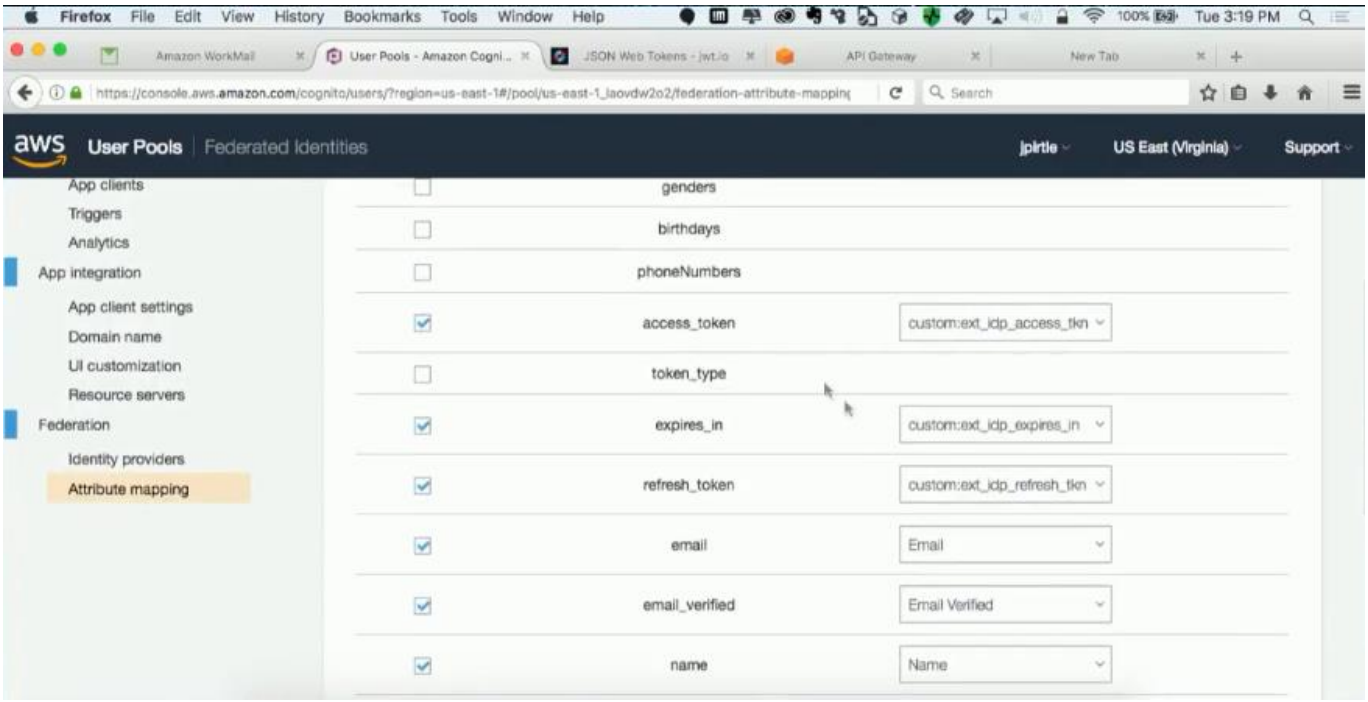




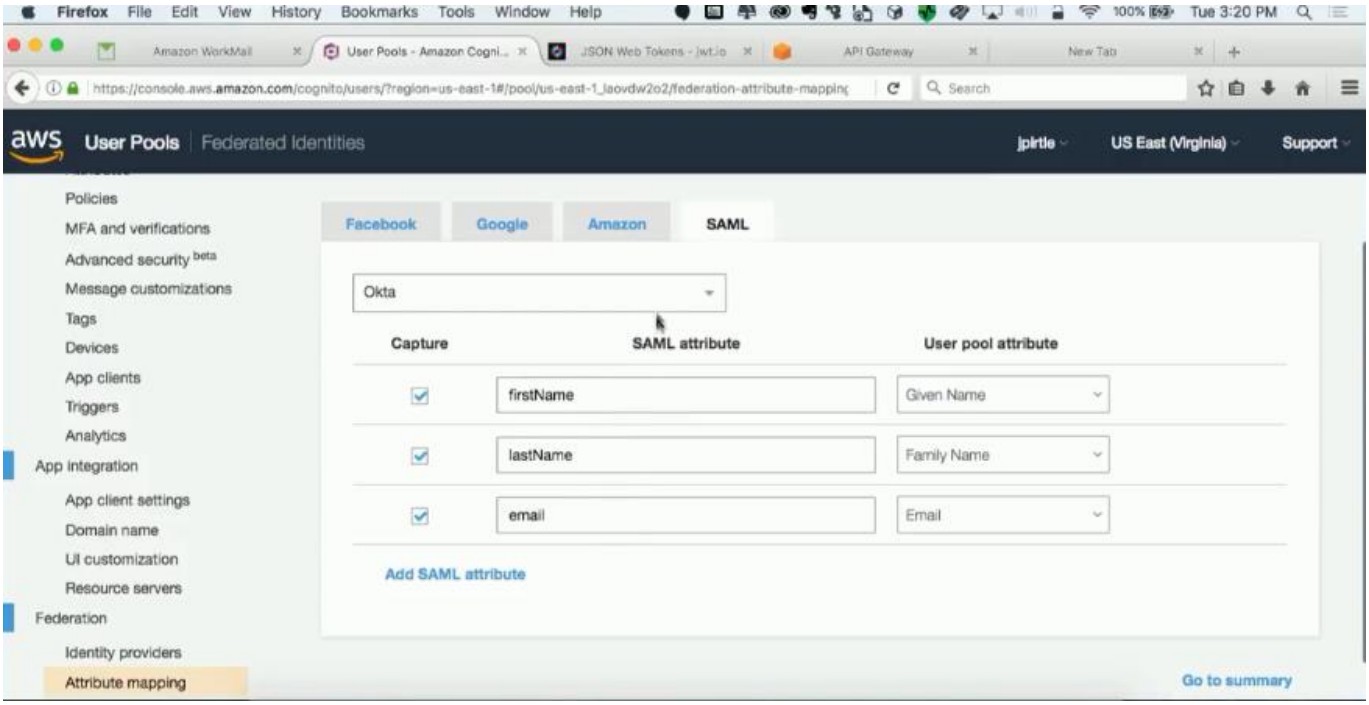


You need to provide the metadata document from your SAML2.0 provider, along with the Identifiers details that is a particular string.

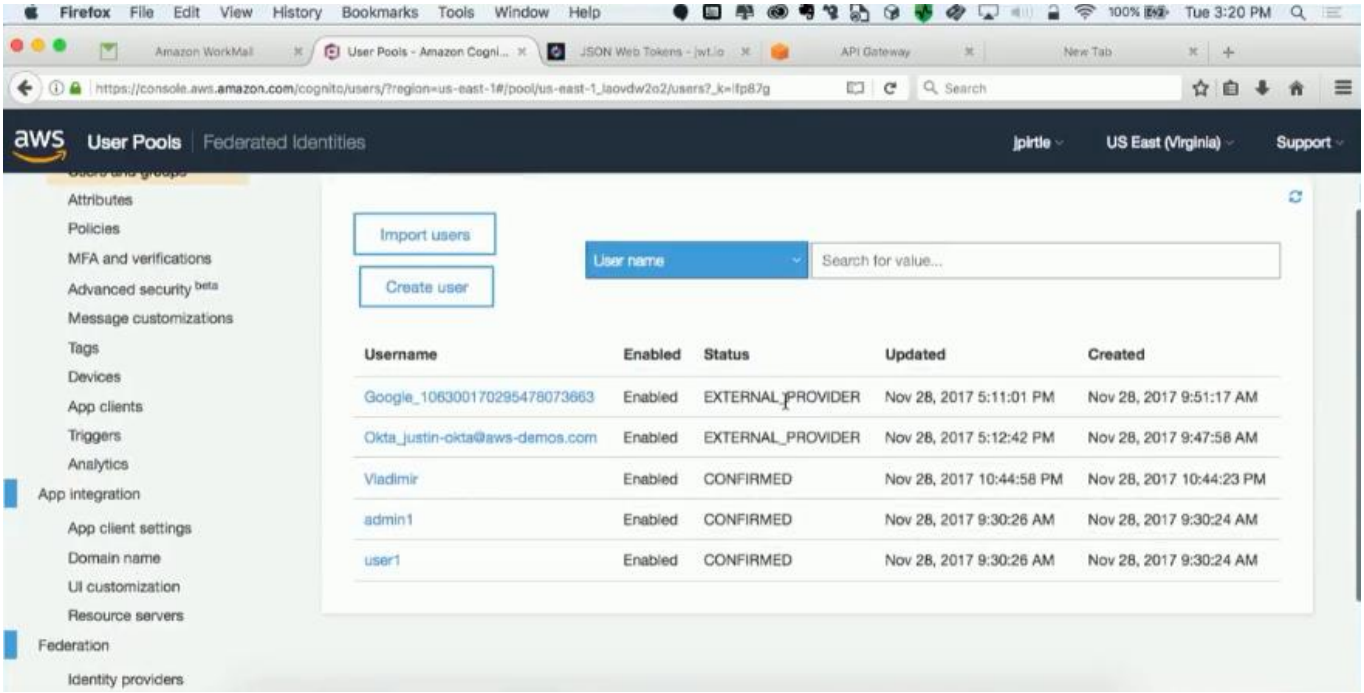




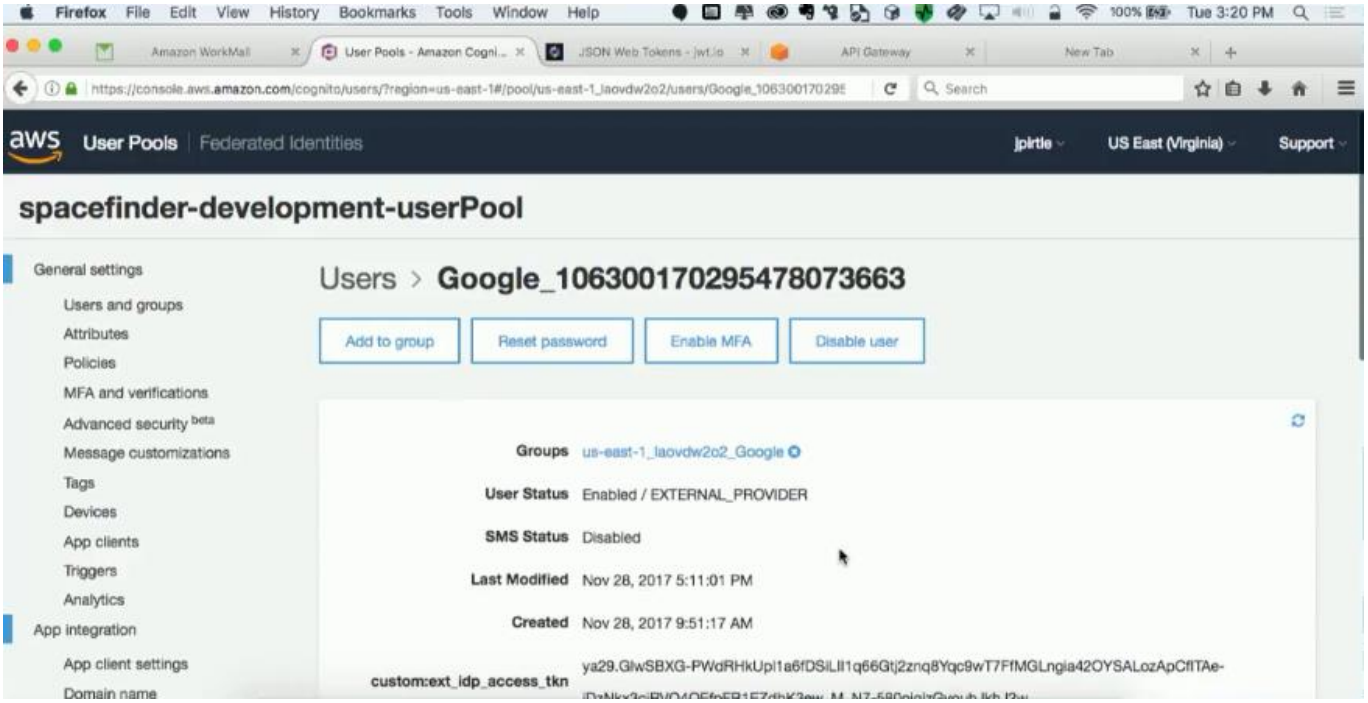
We can map Google's provided attributes to user pool attributes as above

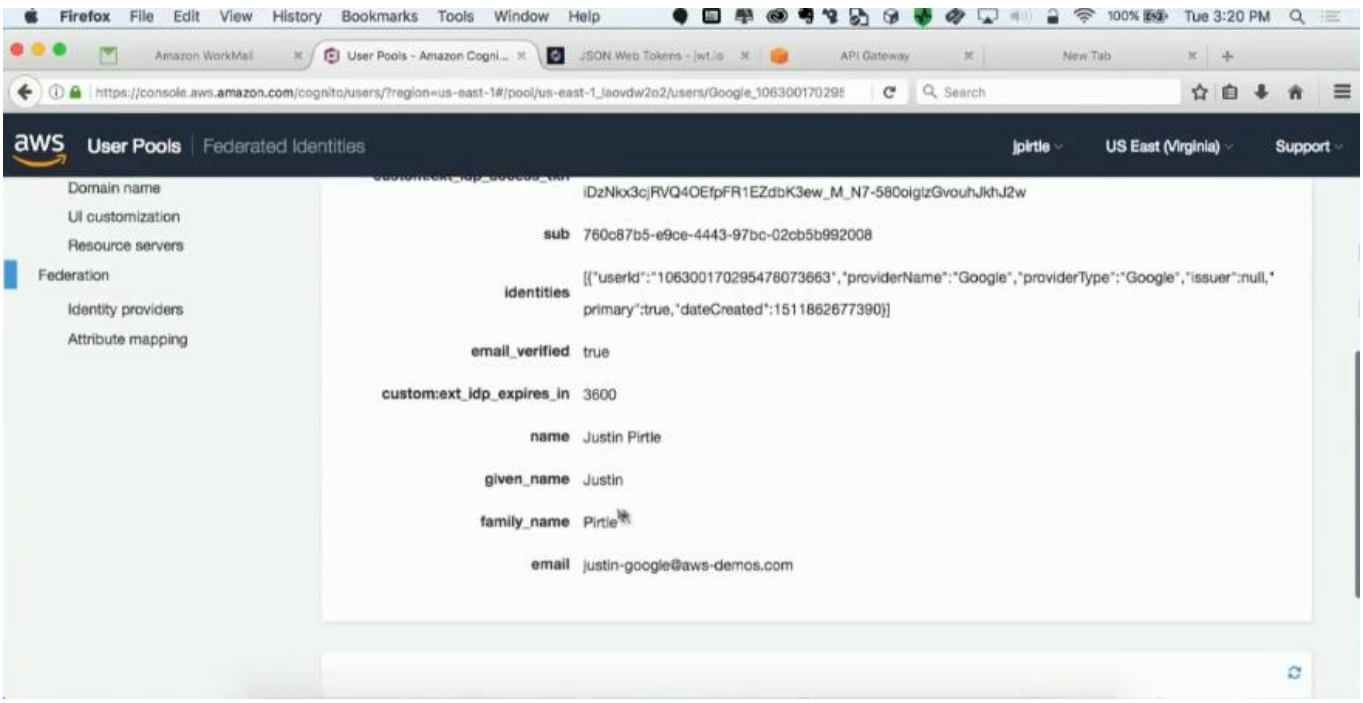


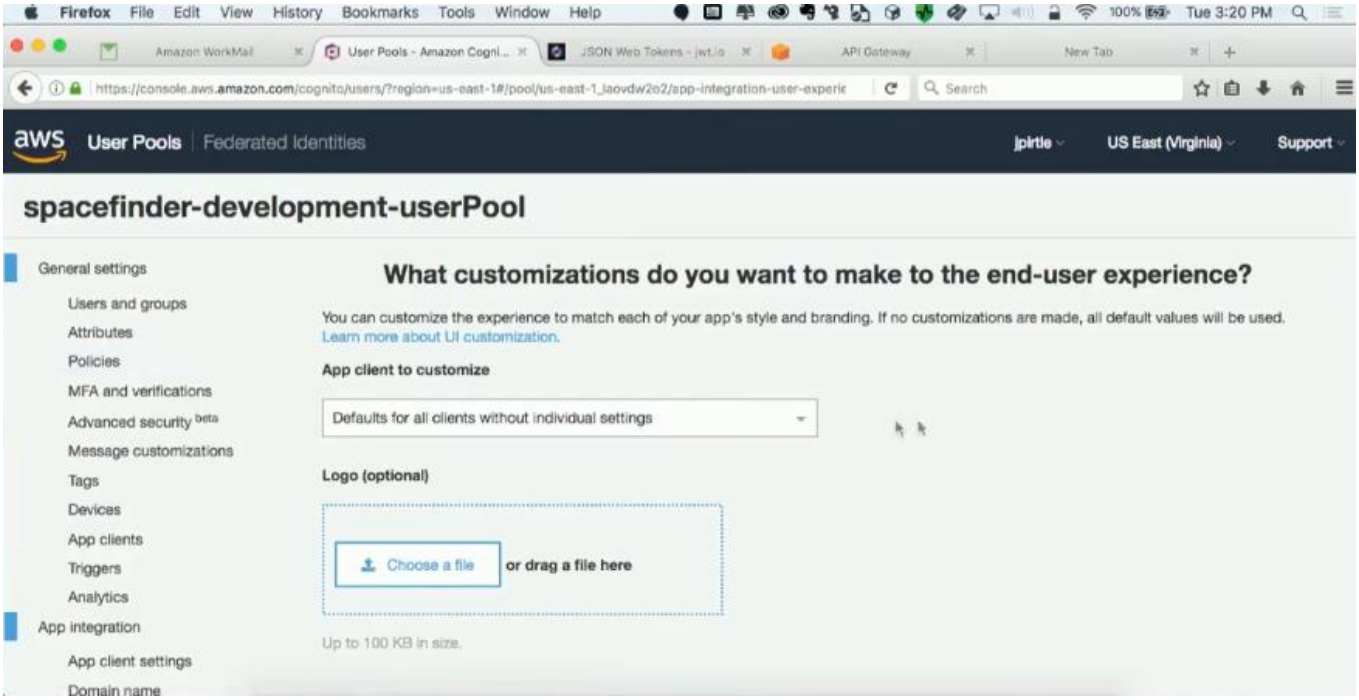
SAML attributes can also be mapped as above

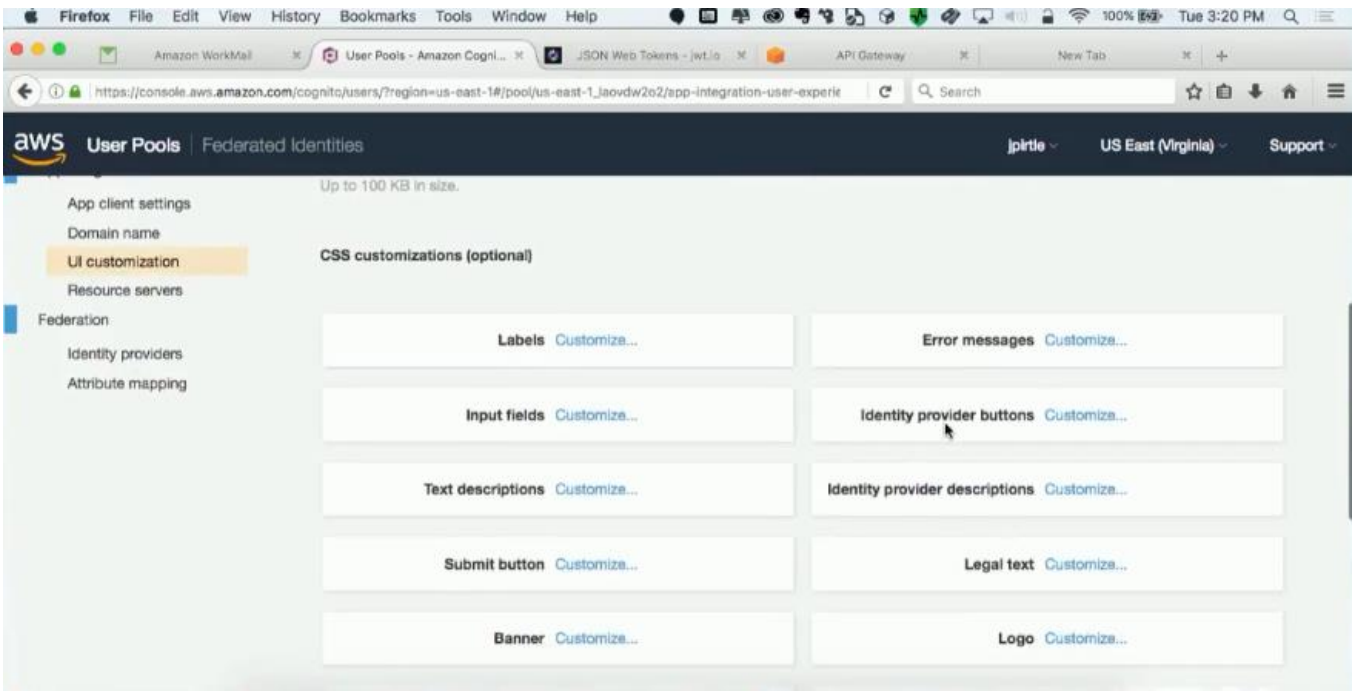


So, when we look at our users in the User Pool as above, we can see both custom attributes as well as mapped 3rd party attributes.


Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:20 PM
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/users/Google_106300170295
Search
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
spacefinder-development-userPool
General settings
Users and groups
Attributes
Policies
MFA and verifications
Advanced security beta
Message customizations
Tags
Devices
App clients
Triggers
Analytics
App integration
App client settings
Domain name
Users > Google_106300170295478073663
Add to group
Reset password
Enable MFA
Disable user
Groups us-east-1_laovdw2o2_Google
User Status Enabled / EXTERNAL_PROVIDER
SMS Status Disabled
Last Modified Nov 28, 2017 5:11:01 PM
Created Nov 28, 2017 9:51:17 AM
custom:ext_idp_access_tkn ya29.GlwSBXG-PWdRHkUpi1a6fDSiLll1q66Gtj2znq8Yqc9wT7FfMGLngia42OYSALozApCflTAe-


Firefox File Edit View History Bookmarks Tools Window Help
Tue 3:20 PM
https://console.aws.amazon.com/cognito/users/?region=us-east-1#/pool/us-east-1_laovdw2o2/users/Google_106300170295
Search
aws User Pools | Federated Identities
jpirtle
US East (Virginia)
Support
Domain name
UI customization
Resource servers
Federation
Identity providers
Attribute mapping
iDzNkx3cjRVQ4OEfpFR1EZdbK3ew_M_N7-580oiglzGvouhJkhJ2w
sub 760c87b5-e9ce-4443-97bc-02cb5b992008
identities [{"userId":"106300170295478073663","providerName":"Google","providerType":"Google","issuer":null,"primary":true,"dateCreated":1511862677390}]
email_verified true
custom:ext_idp_expires_in 3600
name Justin Pirtle
given_name Justin
family_name Pirtle
email justin-google@aws-demos.com





You can customize the Hosted UI.

Migration approach #1: Bulk import

(1) Create CSV
- Doesn't contain passwords
- Max 100,000 users at a time

(2) Run the import job

```
$ aws cognito-idp create-user-import-job

$ curl -v -T "path/to/csvfile" -H "x-amz-
server-side-encryption:aws:kms"
"PRE_SIGNED_URL"

$ aws cognito-idp start-user-import-job
```

```
cognito:mfa_enabled
cognito:username
phone_number
phone_number_verified
email
email_verified
name
given_name
family_name
middle_name
nickname
preferred_username
profile
picture
website
gender
birthdate
zoneinfo
locale
address
updated_at
```


Migration approach #1: Bulk import

(1) Create CSV
- Doesn't contain passwords
- Max 100,000 users at a time

(2) Run the import job

(3) Users change passwords on initial login

cognito:mfa_enabled
cognito:username
phone_number
phone_number_verified
email
email_verified
name
given_name
family_name
middle_name
nickname
preferred_username
profile
picture
website
gender
birthdate
zoneinfo
locale
address
updated_at

aws re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

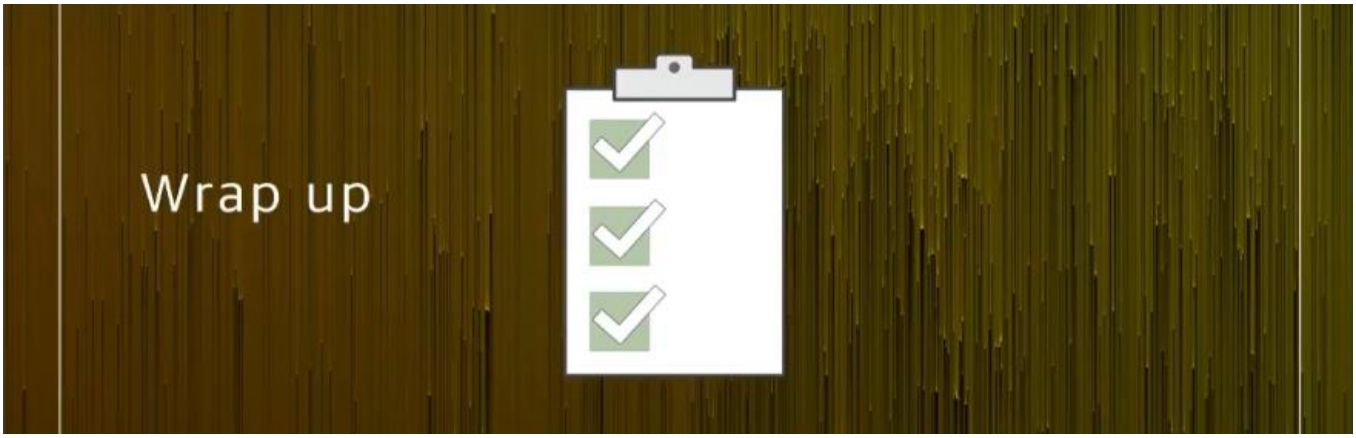
Migration approach #2: One-at-a-time

This approach migrates users one at a time as they sign-in to your app:

(1) First, try authenticating against Cognito User Pools

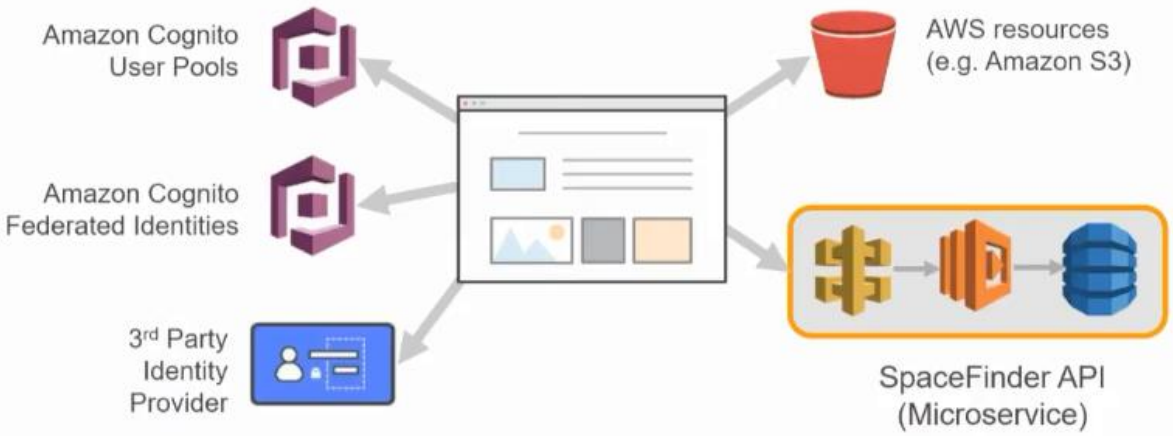
(2) If that fails because of "User Not Found", authenticate against the former IdP

(3) If authentication with former IdP is successful, then create user in the Cognito User Pool with the same username/password



SpaceFinder mobile app

SpaceFinder web app



SpaceFinder

Do try this at home

- Mobile app + API are open-sourced (Apache 2.0 license)

https://github.com/awslabs/aws-serverless-auth-reference-app

Related Sessions

- **MBL305** – Implement User Onboarding, Sign-Up, and Sign-In for Mobile and Web Applications with Amazon Cognito
- **SID332** – Identity Management for Your Users and Apps: A Deep Dive on Amazon Cognito
- **SID343** – User Management and App Authentication with Amazon Cognito
- **SRV425** – Serverless OAuth: Authorizing 3rd-party Applications to your Serverless API