November 28, 2017

AWS re:INVENT

Serverless Authentication and Authorization

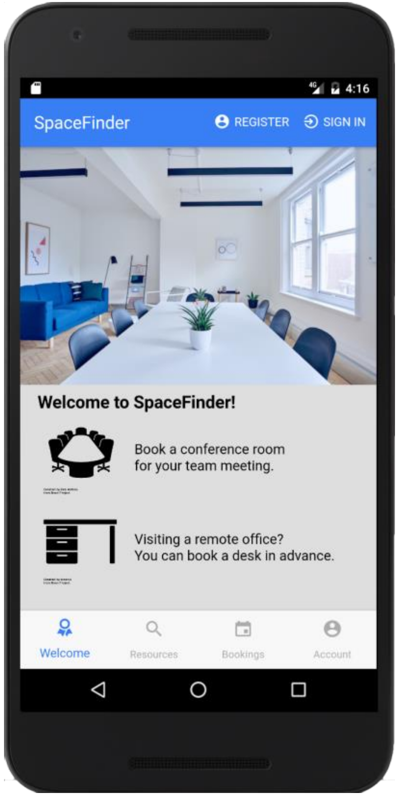
Justin Pirtle and Vladimir Budilov, Senior Solutions Architects

What to expect from the session

- Assumes high-level familiarity with Serverless API architectures (API Gateway, Lambda)

- Learn how to implement **identity management** for your **serverless apps**, using
  - Amazon Cognito User Pools
  - Amazon Cognito Federated Identities
  - Amazon API Gateway
  - AWS Lambda
  - AWS Identity and Access Management (IAM)

SpaceFinder



Welcome to SpaceFinder!

Book a conference room for your team meeting.

Visiting a remote office? You can book a desk in advance.

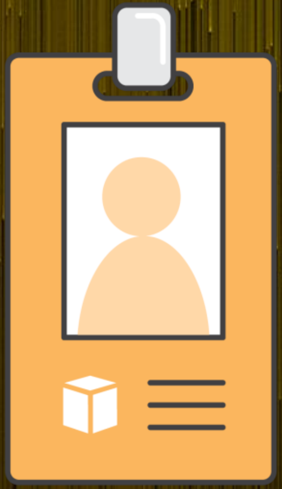
Hybrid mobile app

- Runs in web browser, Android, Apple iOS devices
- Built using Ionic 3 Framework
- Angular 4 / TypeScript
- AWS SDKs for JavaScript

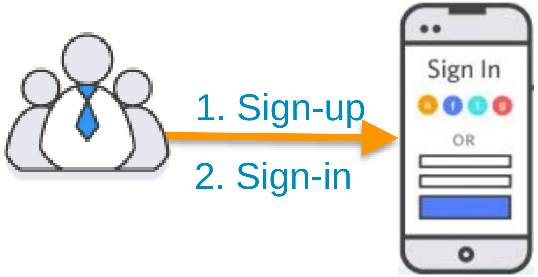
Do try this at home

- Mobile app + API are open-sourced (Apache 2.0 license)
- **https://github.com/awslabs/aws-serverless-auth-reference-app**

Managing Identities



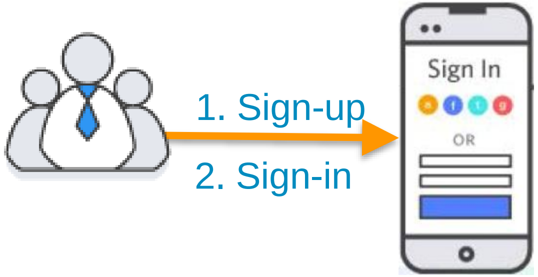
Sign-up and Sign-in



1. Sign-up

2. Sign-in

Sign-up and Sign-in

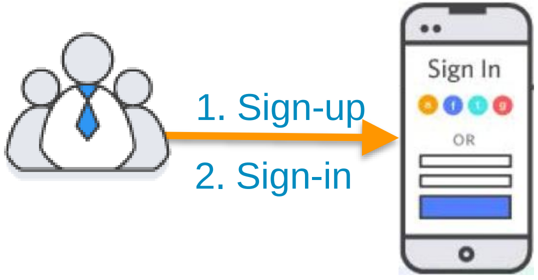


1. Sign-up

2. Sign-in

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

Sign-up and Sign-in



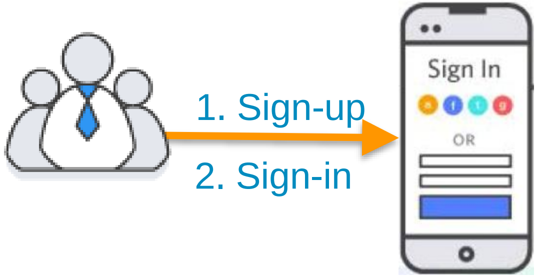
1. Sign-up

2. Sign-in

Username	Email	Password
beverly123	beverly123@example.com	Pa [illegible] 23
pilotjane	pilotjane@example.com	a##eroplan [illegible]
sudhir1977	sudhir197@example.com	m [illegible] a

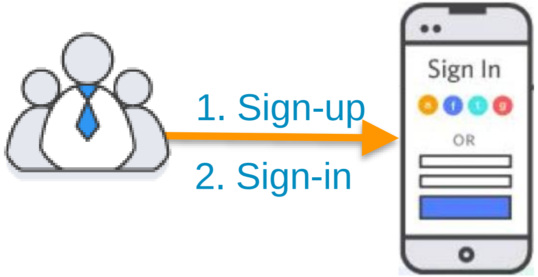
- Never store passwords in plaintext!
- Vulnerable to rogue employees
- A hacked DB results in all passwords being compromised

Sign-up and Sign-in



Username	Email	Hashed Password
beverly123	beverly123@example.com	21a730e7d6cc9d715efcc0514ed69a1f
pilotjane	pilotjane@example.com	fea74fde863cd38f88b3393f590ae883
sudhir1977	sudhir197@example.com	6ce6be14f0c775cc9b3dbe4e18d9fc7d

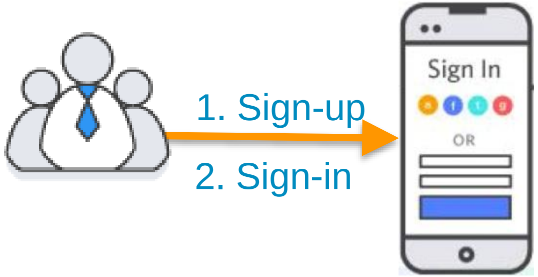
Sign-up and Sign-in



Username	Email	Hashed Password
beverly123	beverly123@example.com	21a [illegible] d715efc [illegible] 1f
pilotjane	pilotjane@example.com	fea74fde862 [illegible] 90ae883
sudhir1977	sudhir197@example.com	[illegible] c775cc9b3dbe4e [illegible]

- MD5/SHA1 collisions
- Rainbow Tables
- Dictionary attacks, brute-force (GPUs can compute billions of hashes/sec)

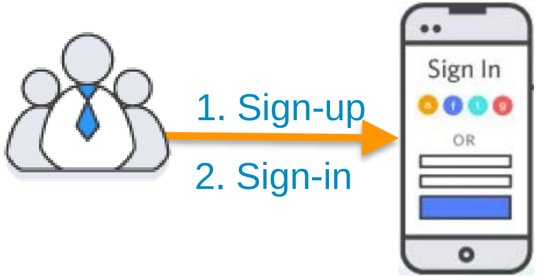
Sign-up and Sign-in



Username	Email	Salted Hash
beverly123	beverly123@example.com	1e66f9358530620b2bcae79dada717c…
pilotjane	pilotjane@example.com	88fccd9cf82377d11d2fede177457d47…
sudhir1977	sudhir197@example.com	08a5981de4fecf04b1359a179962a48...

- Incorporate app-specific salt + random user-specific salt
- Use algorithm with configurable # of iterations (e.g. bcrypt, PBKDF2), to slow down brute force attacks

Sign-up and Sign-in

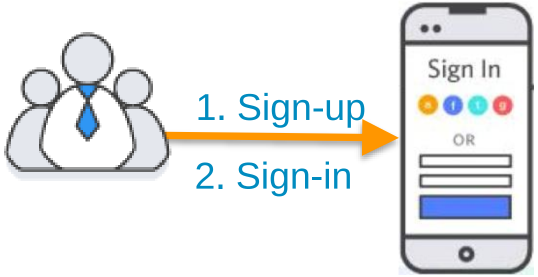


1. Sign-up

2. Sign-in

Username	Email	SRP Verifier function
beverly123	beverly123@example.com	<password-specific verifier>
pilotjane	pilotjane@example.com	<password-specific verifier>
sudhir1977	sudhir197@example.com	<password-specific verifier>

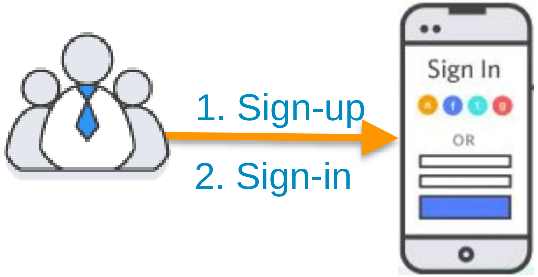
Sign-up and Sign-in



Username	Email	SRP Verifier function
beverly123	beverly123@example.com	<password-specific verifier>
pilotjane	pilotjane@example.com	<password-specific verifier>
sudhir1977	sudhir197@example.com	<password-specific verifier>

- **Secure Remote Password (SRP) Protocol**
- Verifier-based protocol
- Passwords never travel over the wire
- Resistant to several attack vectors
- Perfect Forward Secrecy

Sign-up and Sign-in



1. Sign-up

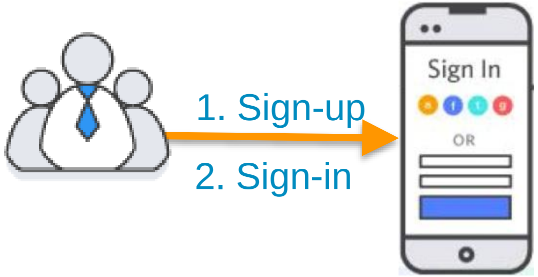
2. Sign-in

Username	Email	SRP Verifier function
beverly123	beverly123@example.com	<password-specific verifier>
pilotjane	pilotjane@example.com	<password-specific verifier>
sudhir1977	sudhir197@example.com	<password-specific verifier>

Security Requirements

☑ Secure password handling

Sign-up and Sign-in


1. Sign-up

2. Sign-in

Username	Email	SRP Verifier function
beverly123	beverly123@example.com	<password-specific verifier>
pilotjane	pilotjane@example.com	<password-specific verifier>
sudhir1977	sudhir197@example.com	<password-specific verifier>

Security Requirements

☑ Secure password handling

□ Multi-Factor Authentication

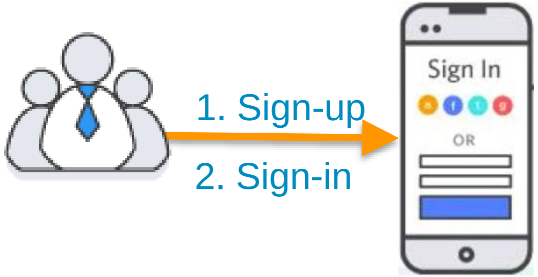
□ Enforce password policies

□ Encrypt all data server-side

□ Support custom authentication flows

□ Scalable to 100s of millions of users

Sign-up and Sign-in



Username	Email	SRP Verifier function
beverly123	beverly123@example.com	<password-specific verifier>
pilotjane	pilotjane@example.com	<password-specific verifier>
sudhir1977	sudhir197@example.com	<password-specific verifier>

User Flows

- □ Registration
- □ Verify email/phone
- □ Secure sign-in
- □ Forgot password
- □ Change password
- □ Sign-out

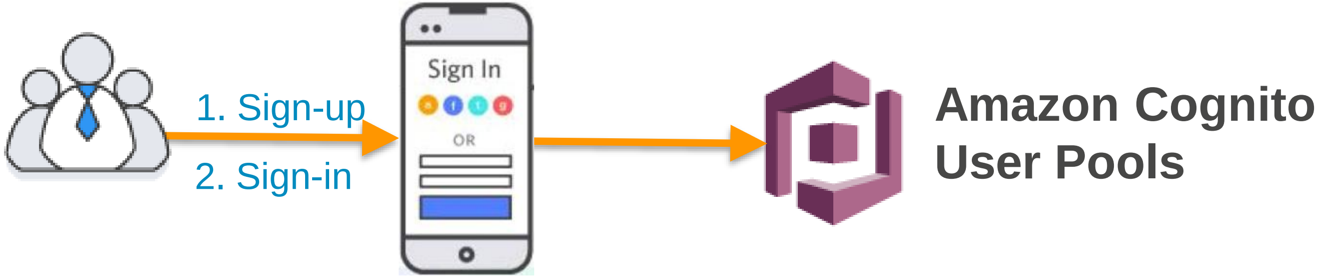
Security Requirements

- ☑ Secure password handling
- □ Multi-Factor Authentication
- □ Enforce password policies
- □ Encrypt all data server-side
- □ Support custom authentication flows
- □ Scalable to 100s of millions of users

AWS re:Invent

aws

Sign-up and Sign-in



1. Sign-up

2. Sign-in

Amazon Cognito User Pools

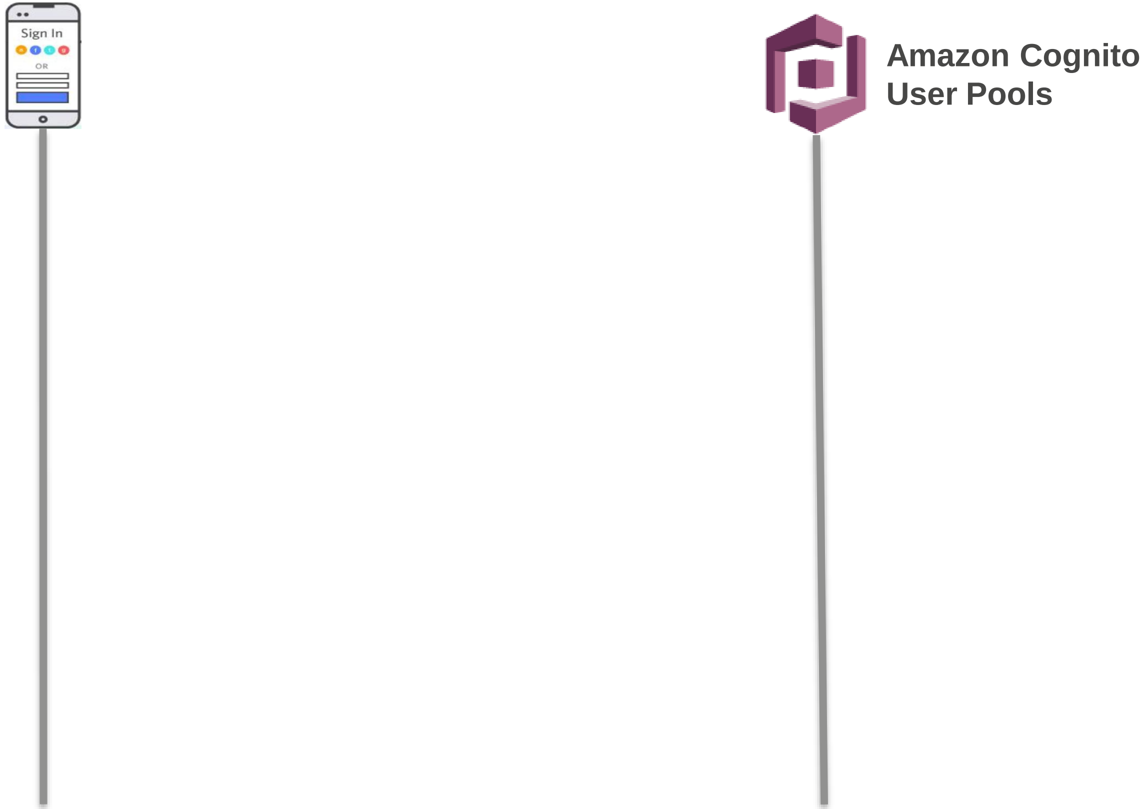
User Flows

- ☑ Registration
- ☑ Verify email/phone
- ☑ Secure sign-in
- ☑ Forgot password
- ☑ Change password
- ☑ Sign-out

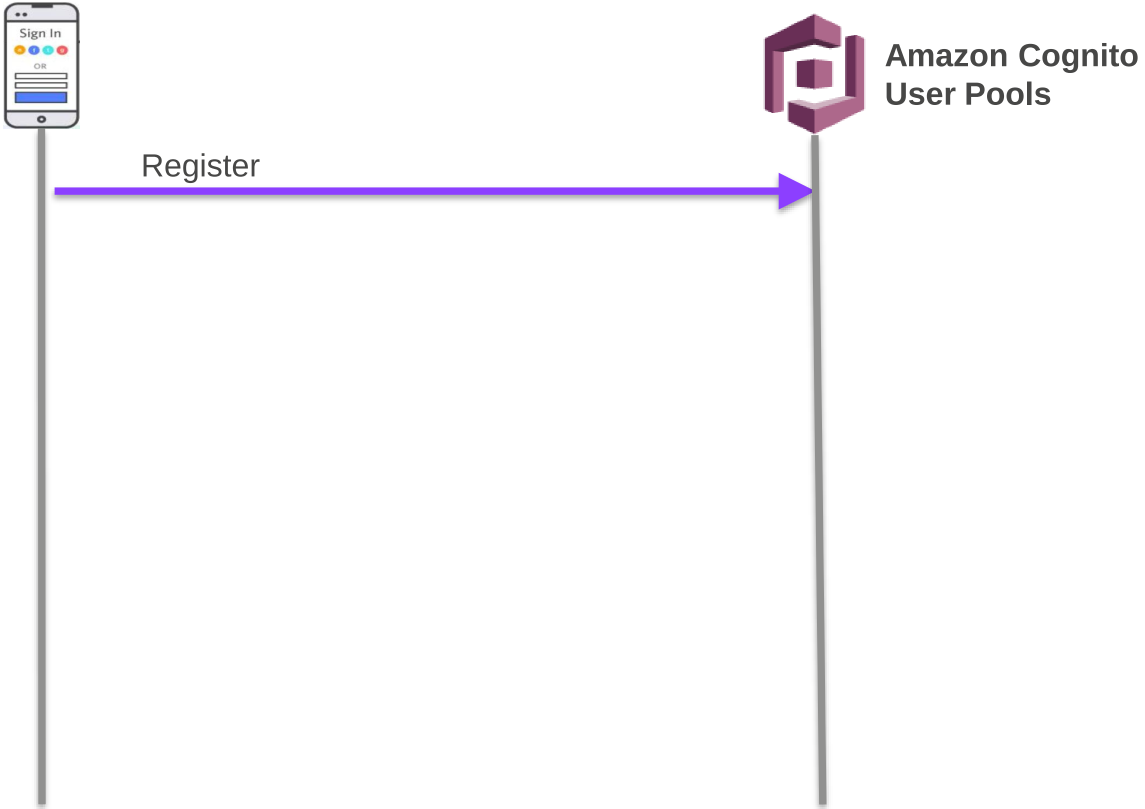
Security Requirements

- ☑ Secure password handling
- ☑ Multi-Factor Authentication
- ☑ Enforce password policies
- ☑ Encrypt all data server-side
- ☑ Support custom authentication flows
- ☑ Scalable to 100s of millions of users

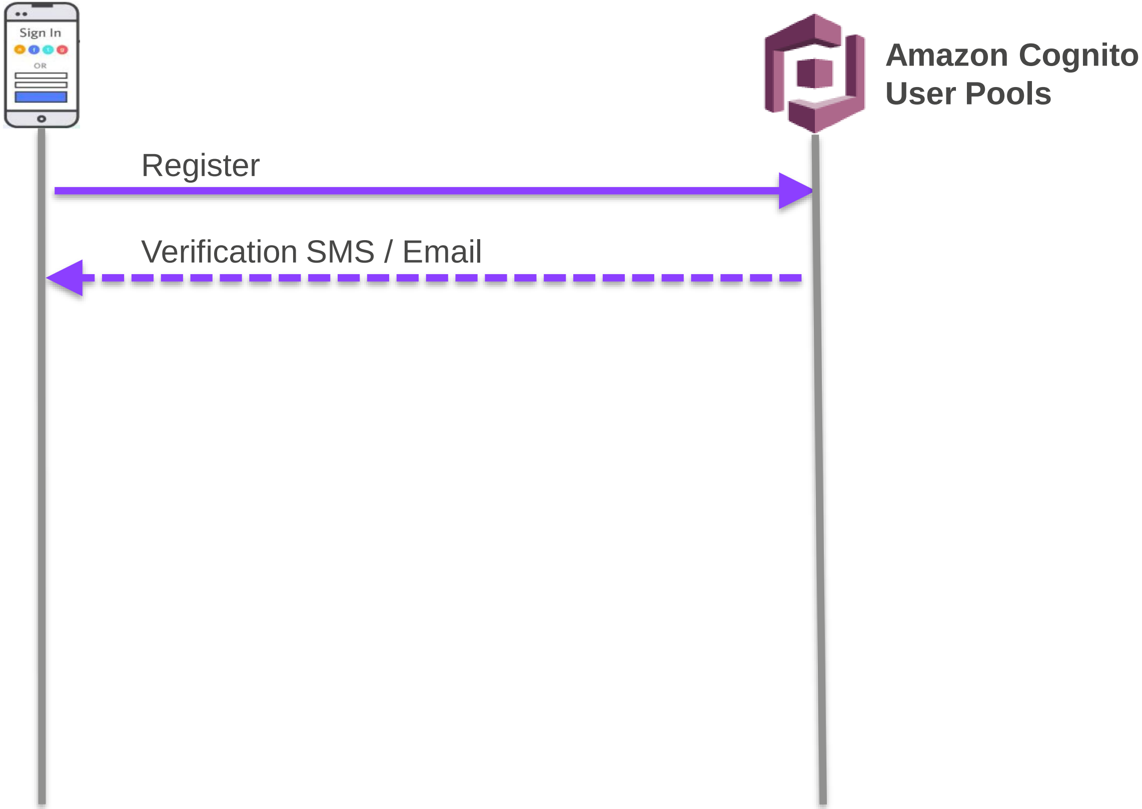
Sign-up and Sign-in



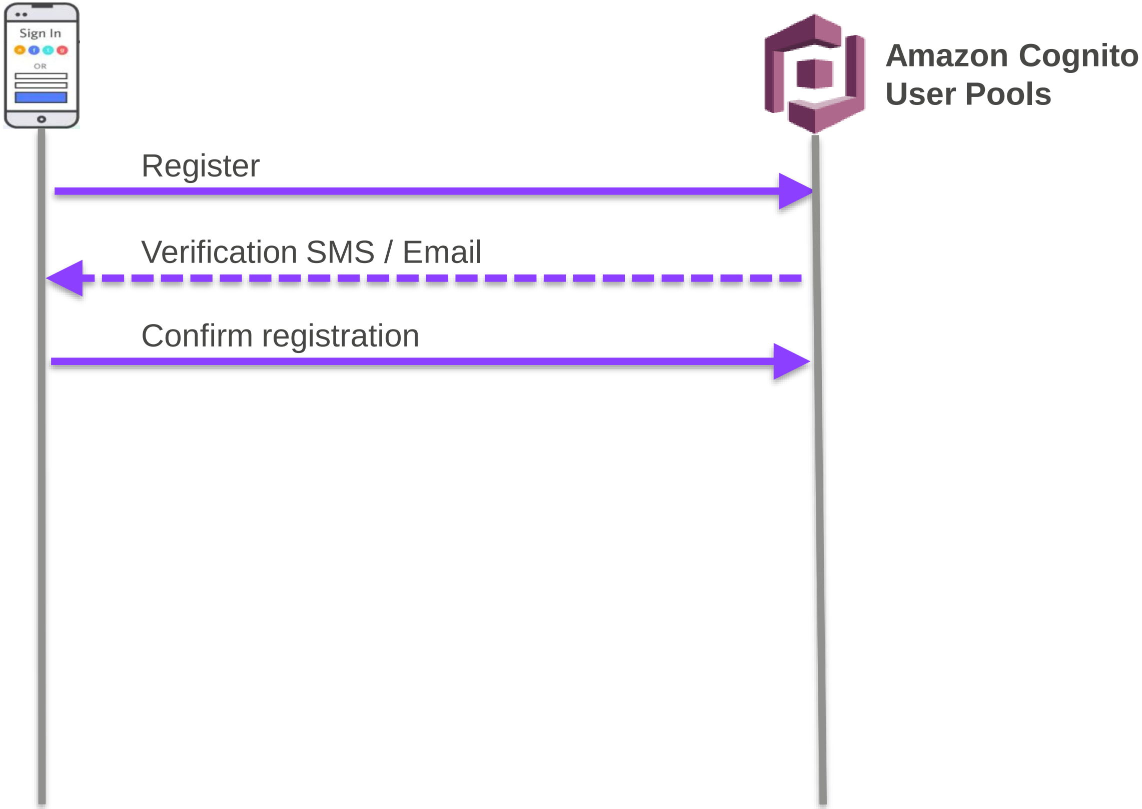
Sign-up and Sign-in



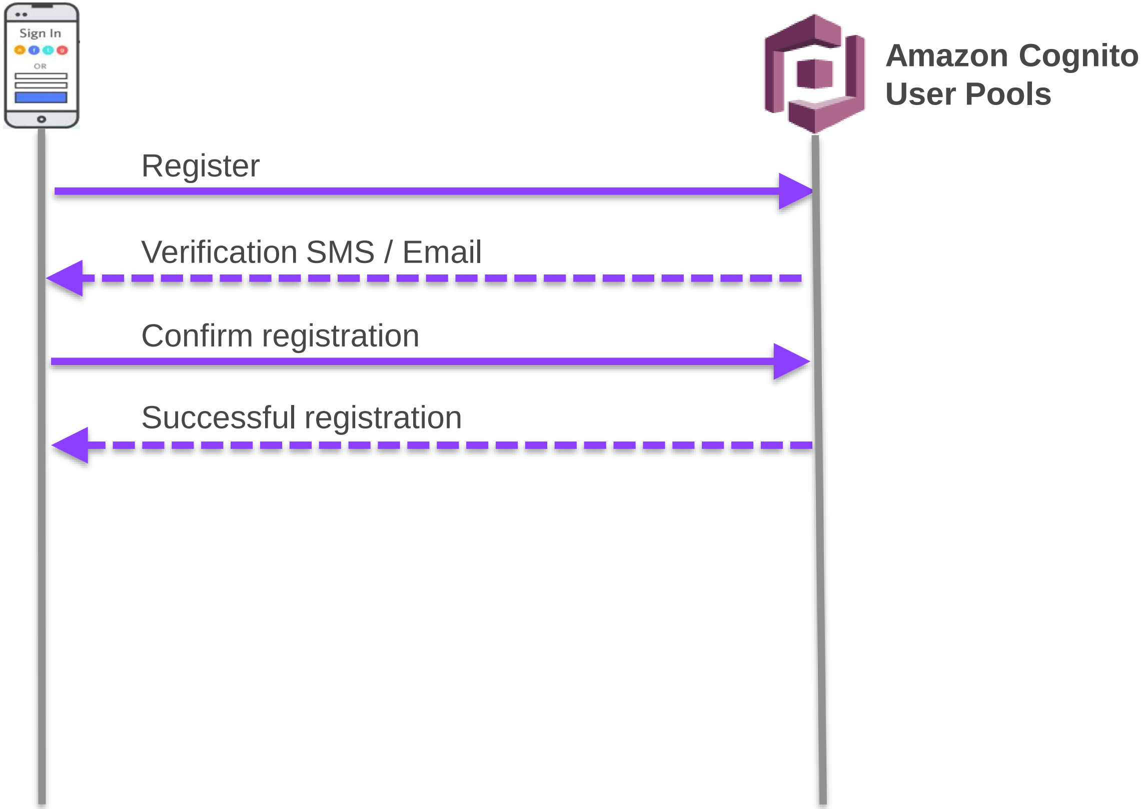
Sign-up and Sign-in



Sign-up and Sign-in



Sign-up and Sign-in



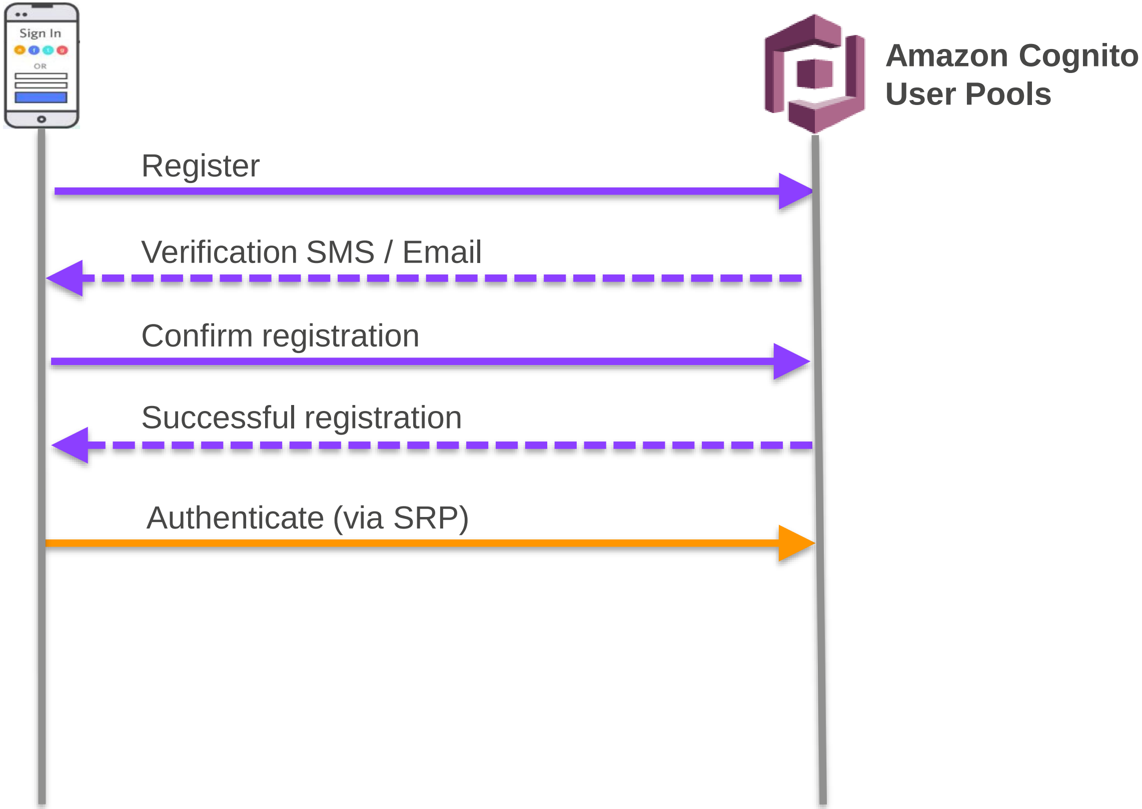
Register

Verification SMS / Email

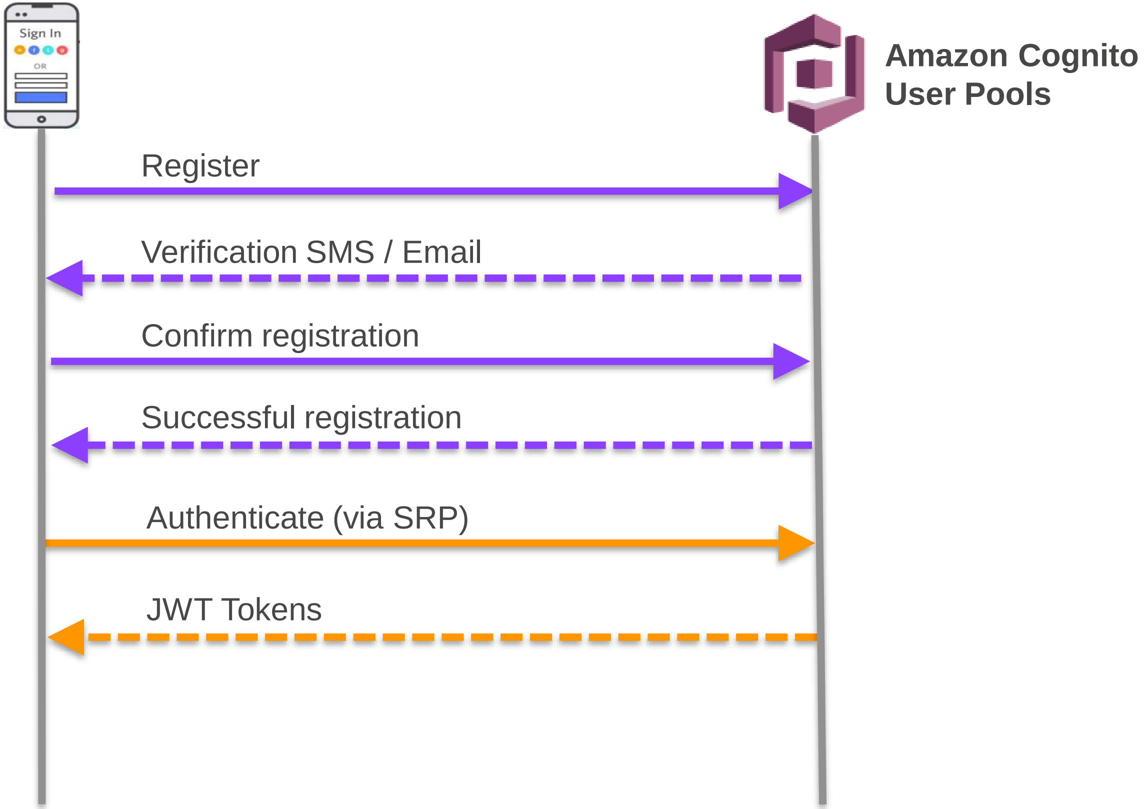
Confirm registration

Successful registration

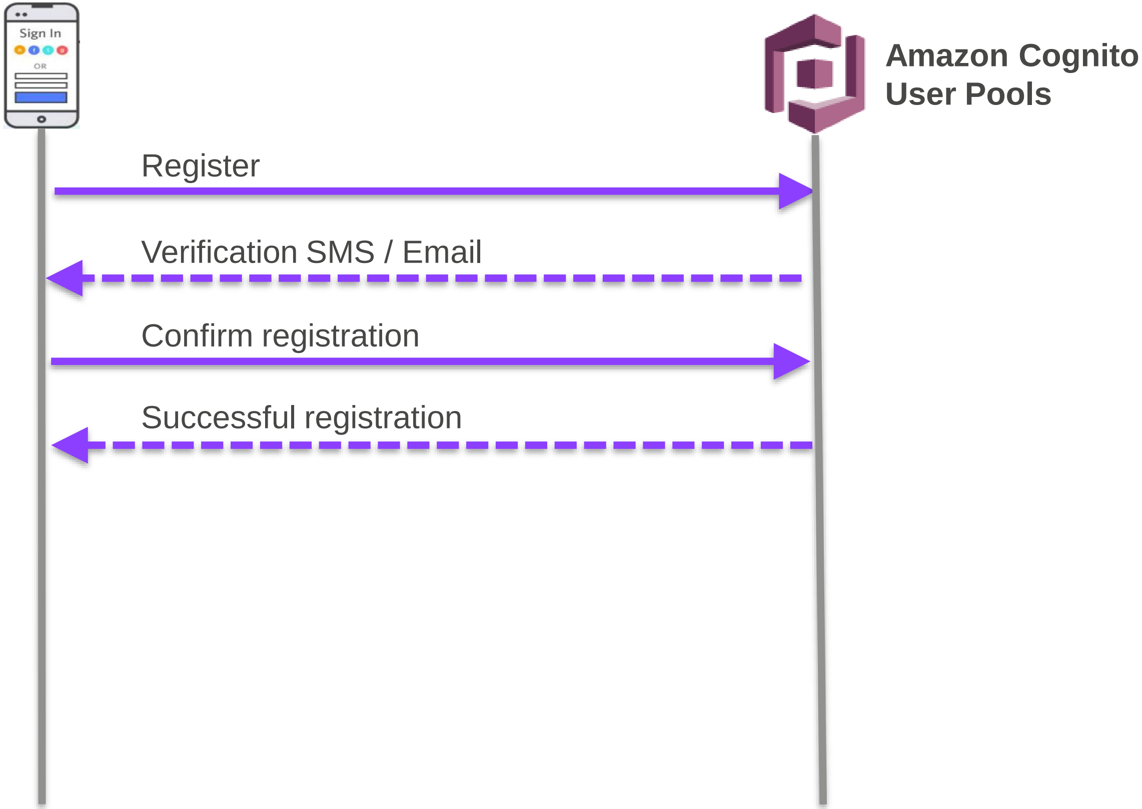
Sign-up and Sign-in



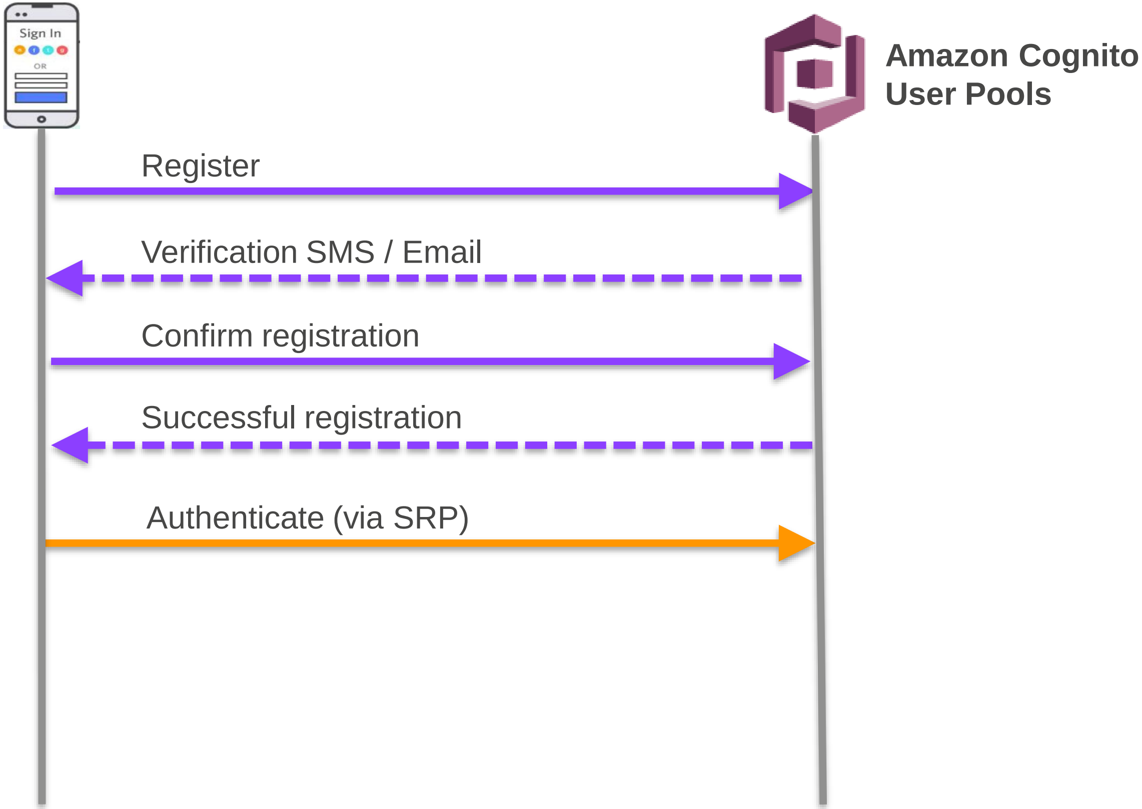
Sign-up and Sign-in



Sign-up and Sign-in

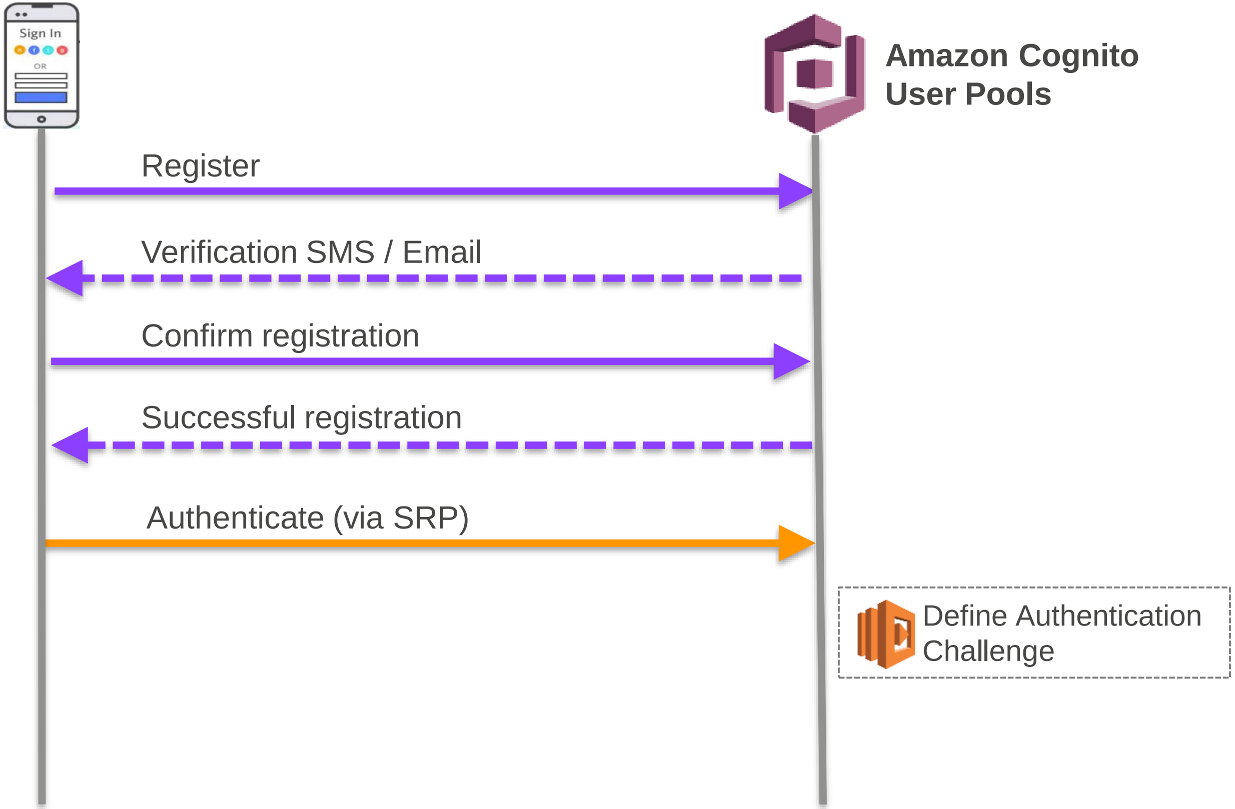


Sign-up and Sign-in



AWS re:Invent

Sign-up and Sign-in



Amazon Cognito User Pools

Register

Verification SMS / Email

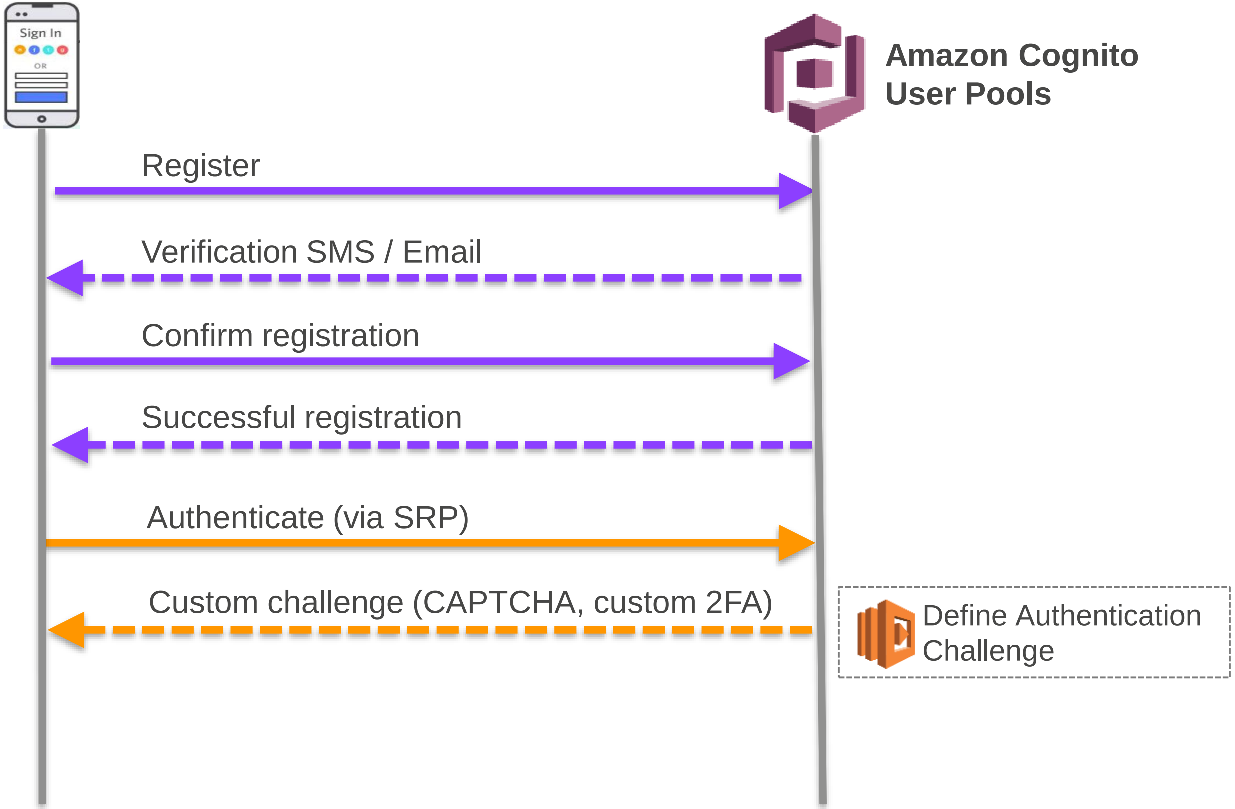
Confirm registration

Successful registration

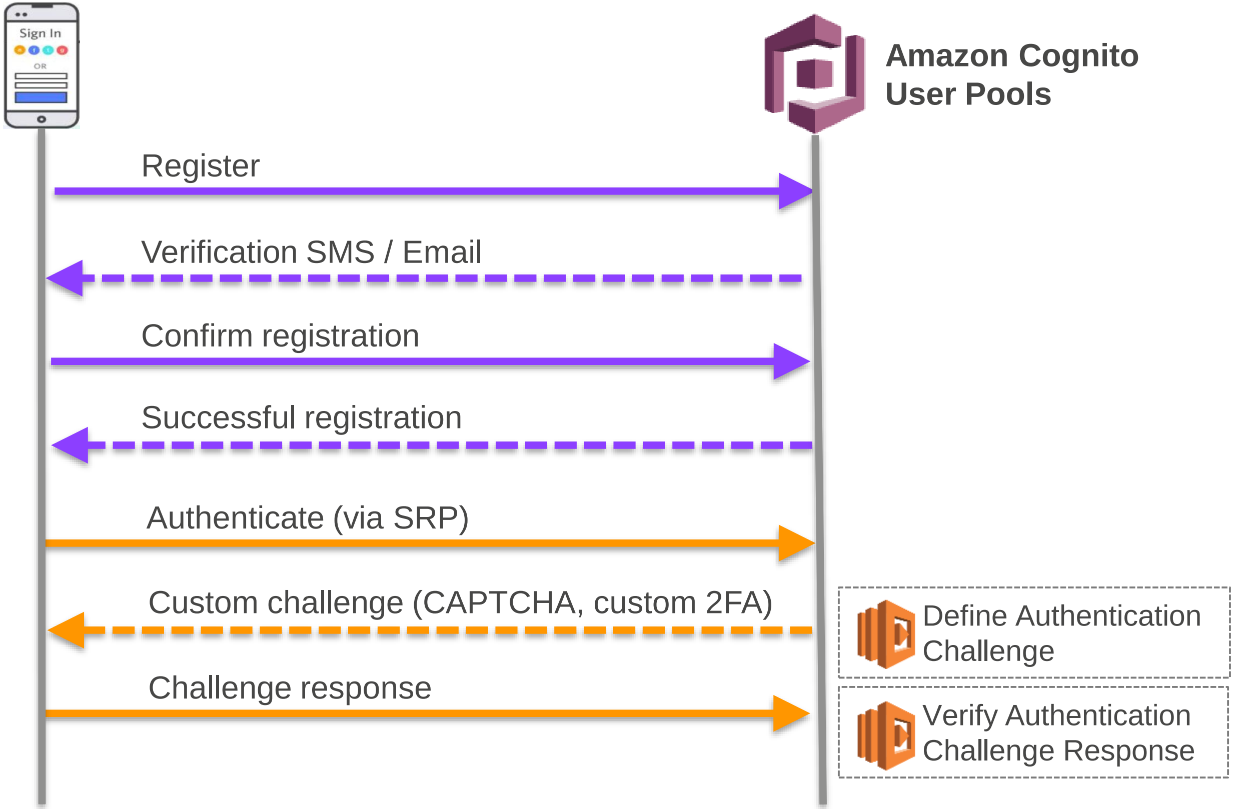
Authenticate (via SRP)

Define Authentication Challenge

Sign-up and Sign-in



Sign-up and Sign-in



Register

Verification SMS / Email

Confirm registration

Successful registration

Authenticate (via SRP)

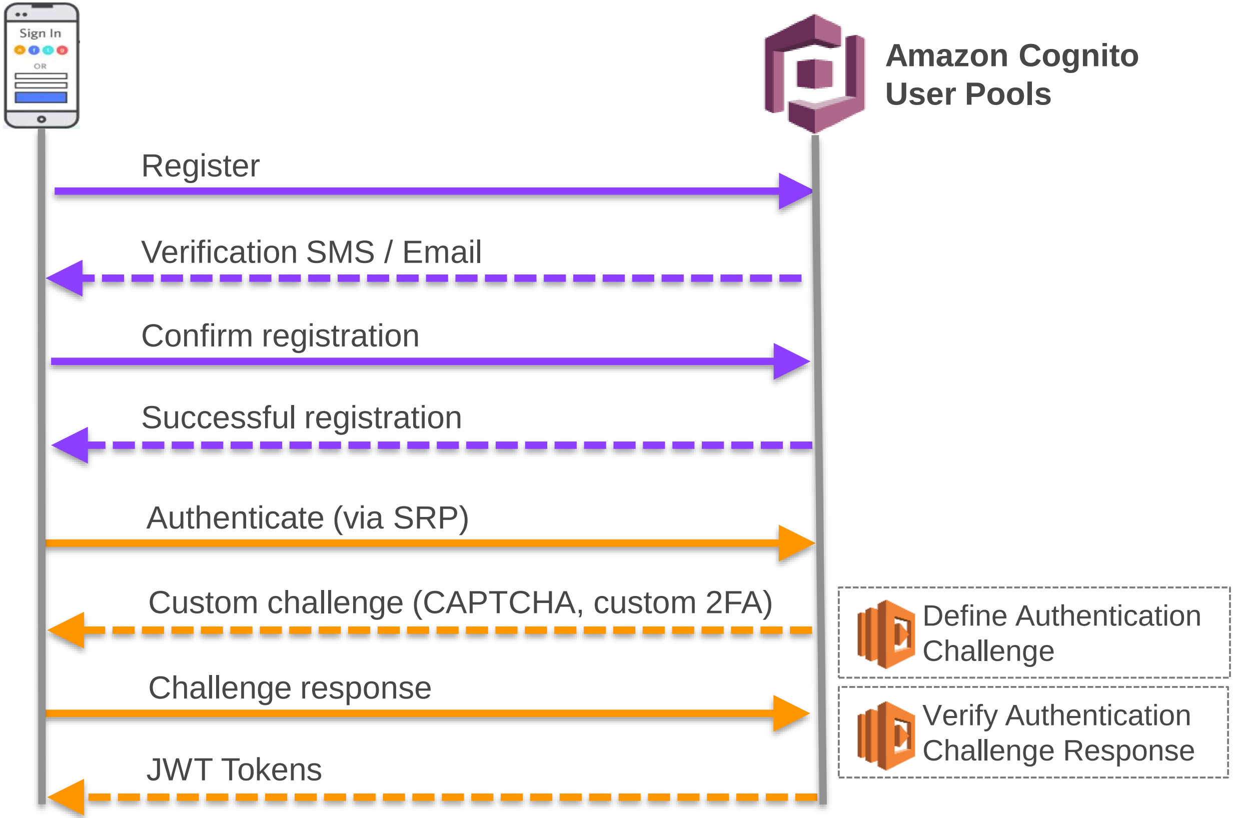
Custom challenge (CAPTCHA, custom 2FA)

Challenge response

Define Authentication Challenge

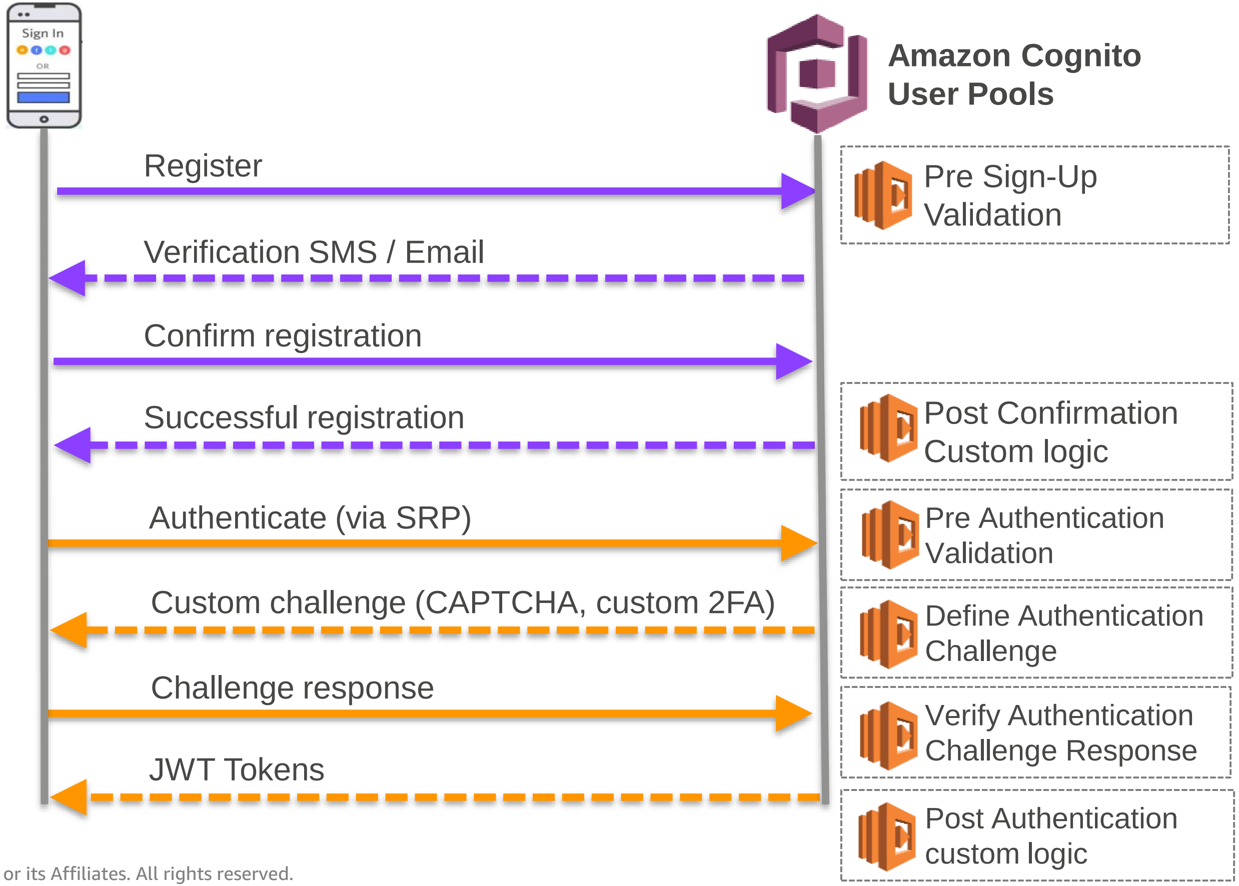
Verify Authentication Challenge Response

Sign-up and Sign-in

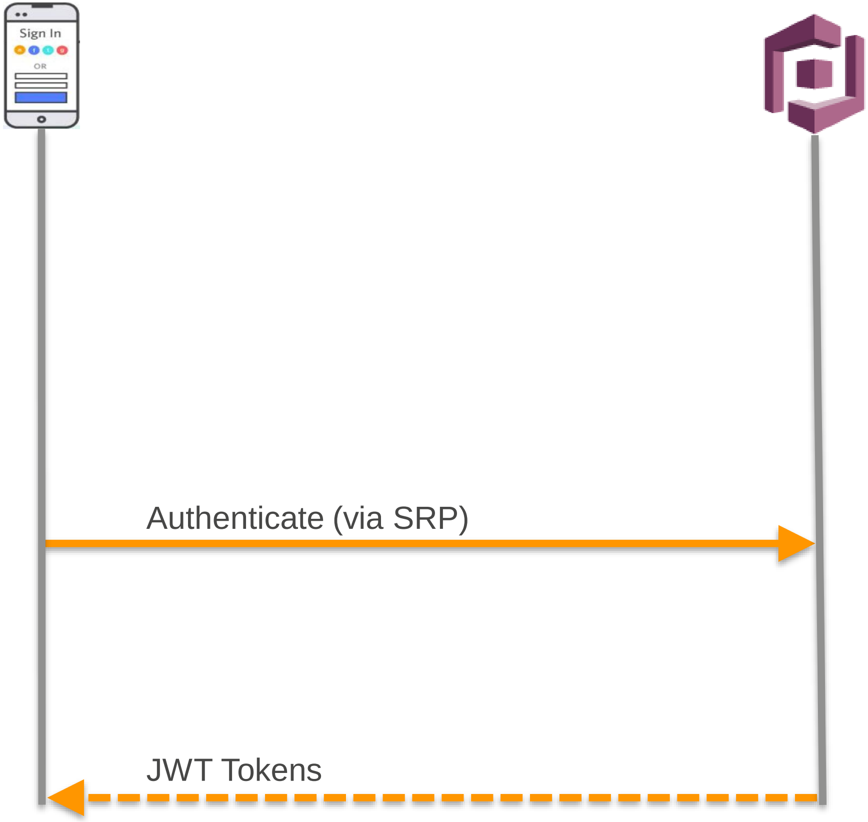


Sign In
OR
Amazon Cognito User Pools
Register
Verification SMS / Email
Confirm registration
Successful registration
Authenticate (via SRP)
Custom challenge (CAPTCHA, custom 2FA)
Challenge response
JWT Tokens
Define Authentication Challenge
Verify Authentication Challenge Response

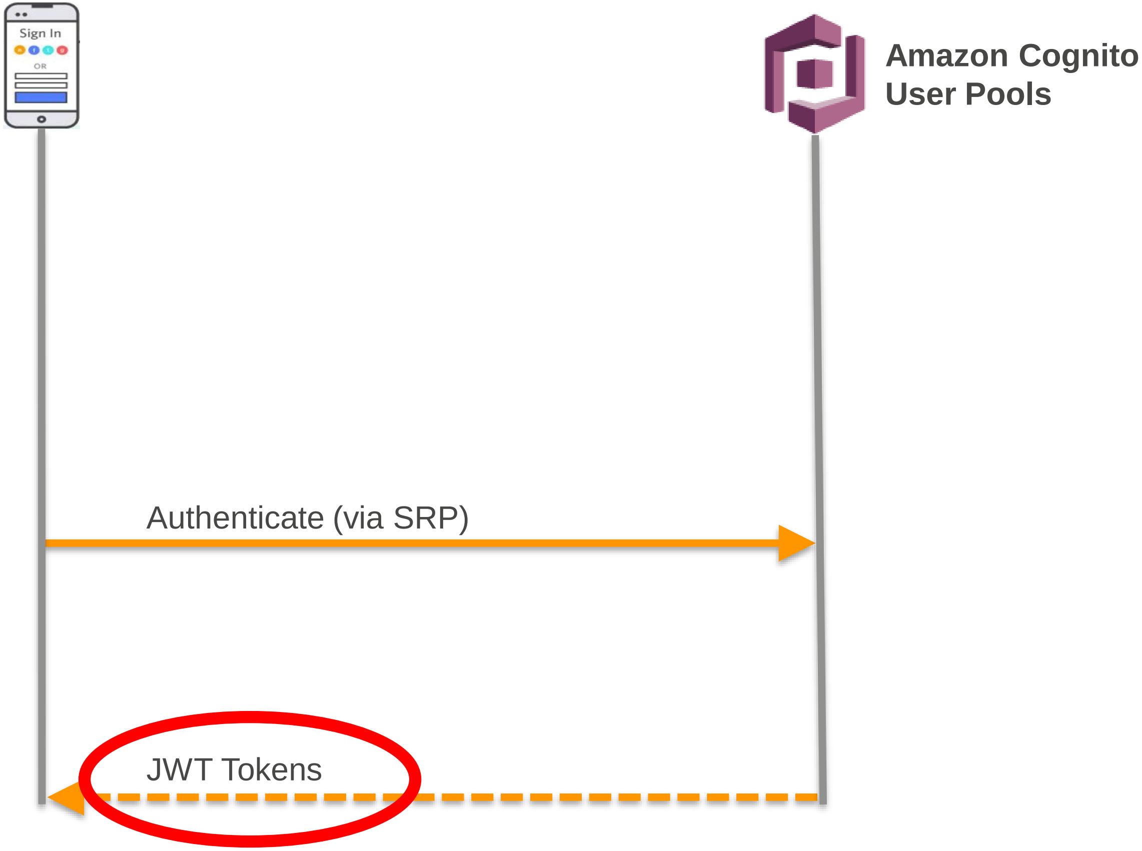
Sign-up and Sign-in


Sign In
OR
Amazon Cognito User Pools
Register
Pre Sign-Up Validation
Verification SMS / Email
Confirm registration
Post Confirmation Custom logic
Successful registration
Authenticate (via SRP)
Pre Authentication Validation
Custom challenge (CAPTCHA, custom 2FA)
Define Authentication Challenge
Challenge response
Verify Authentication Challenge Response
JWT Tokens
Post Authentication custom logic

Sign-up and Sign-in



Sign-up and Sign-in



JWT token

```
eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cy1lYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXN0IiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazx1cbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ
```

JWT token

```
eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cy1lYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXN0IiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazx1cbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ
```

Header

```
{
  "kid":"9errtDKltq8YwaJy2GZtObykRDEA9SB4iDT6vWmTeQE=",
  "alg":"RS256”
}
```

JWT token

```
eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cy1lYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXN0IiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazx1cbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ
```

Payload

```
{
  "sub":"6f557368-a884-484e-b662-9fc69f3c3802",
  "aud":"6lkfs70rovkubirh1qtntvj012",
  "email_verified":true,
  "token_use":"id",
  "auth_time":1478449060,
  "iss":"https:\/\/cognito-idp.us-east-1.amazonaws.com
        \/us-east-1_XMlUW9sUy",
  "cognito:username":"test123",
  "exp":1478452660,
  "given_name”:"Test",
  "iat":1478449060,
  "family_name":"Test",
  "email":”test@example.com"
}
```

AWS re:Invent

JWT token

eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cy1lYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXN0IiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazx1cbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ

Signature

HMACSHA256(base64UrlEncode(header) + "." +
base64UrlEncode(payload), {secret});

AWS re:Invent

JWT token

```
eyJraWQiOiI5ZXJydERLbHRxOFl3YUp5MkdadE9ieWtSREVB
OVNCNGlEVDZ2V21UZVFFPSIsImFsZyI6IlJTMjU2In0.eyJz
dWIiOiI2ZjU1NzM2OC1hODg0LTQ4NGUtYjY2Mi05ZmM2OWYz
YzM4MDIiLCJhdWQiOiI2bGtmczcwcm92a3ViaXJoMXF0bnR2
ajAxMiIsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJ0b2tlbl91
c2UiOiJpZCIsImF1dGhfdGltZSI6MTQ3ODQ0OTA2MCwiaXNz
IjoiaHR0cHM6XC9cL2NvZ25pdG8taWRwLnVzLWVhc3QtMS5h
bWF6b25hd3MuY29tXC91cy1lYXN0LTFfWE1sVVc5c1V5Iiwi
Y29nbml0bzp1c2VybmFtZSI6InRlc3QxMjMiLCJleHAiOjE0
Nzg0NTI2NjAsImdpdmVuX25hbWUiOiJUZXN0IiwiaWF0Ijox
NDc4NDQ5MDYwLCJmYW1pbHlfbmFtZSI6IlRlc3QiLCJlbWFp
bCI6InRyYW5qaW1AYW1hem9uLmNvbSJ9.atQO0SJg9V97d6t
YonHNx0q7Zuof8-d-q0u69zNnuSJtmzGvOAW97tP2e3GydY9
K8q_2kG2IzkpEMUEdaeWjz2qG5dS328Scm6pRDPpC5pOkU8y
mjH7DBPfVXhtgS3iOhyleFhtmaTaYb_lYLpaaV10m8sVFOMH
tjdfrAm26Fq7zyjWYTSfzhqud29Ti4zn9PhcE7aL3s7BB8CJ
18_yFXSoG5CYCpLszvHazx1cbmPoXFrlFlPvZ07Oy8EbOaGs
4CukmoYiV-5RnZsA9JXj405Kp50k-v8HCL6ZACDw3OYMV87P
e6PuEqbzQLlc8BufKThm0xBiO6NJtvI7iC2sEIQ
```

Header

```
{
  "kid":"9errtDKltq8YwaJy2GZtObykRDEA9SB4iDT6vWmTeQE=",
  "alg":"RS256”
}
```

Payload

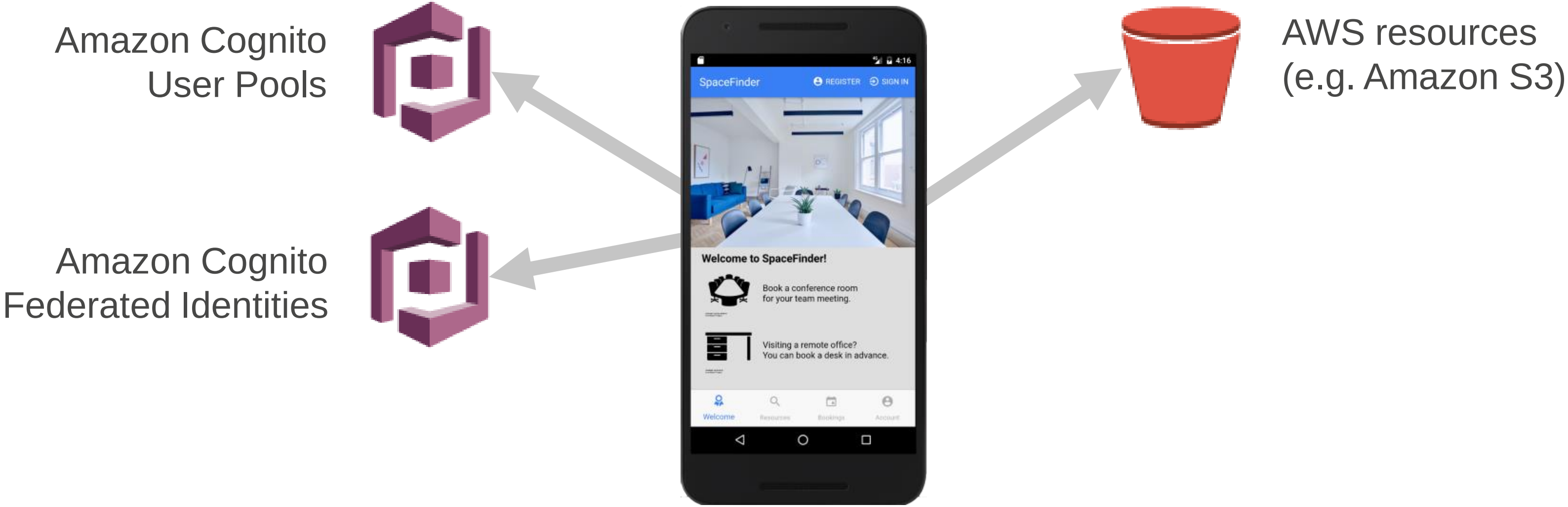
```
{
  "sub":"6f557368-a884-484e-b662-9fc69f3c3802",
  "aud":"6lkfs70rovkubirh1qtntvj012",
  "email_verified":true,
  "token_use":"id",
  "auth_time":1478449060,
  "iss":"https:\/\/cognito-idp.us-east-1.amazonaws.com
        \/us-east-1_XMlUW9sUy",
  "cognito:username":"test123",
  "exp":1478452660,
  "given_name”:"Test",
  "iat":1478449060,
  "family_name":"Test",
  "email":”test@example.com"
}
```

Signature

```
HMACSHA256(base64UrlEncode(header) + "." +
base64UrlEncode(payload), {secret});
```

AWS re:Invent

Application so far...



Amazon Cognito User Pools

Amazon Cognito Federated Identities

AWS resources (e.g. Amazon S3)

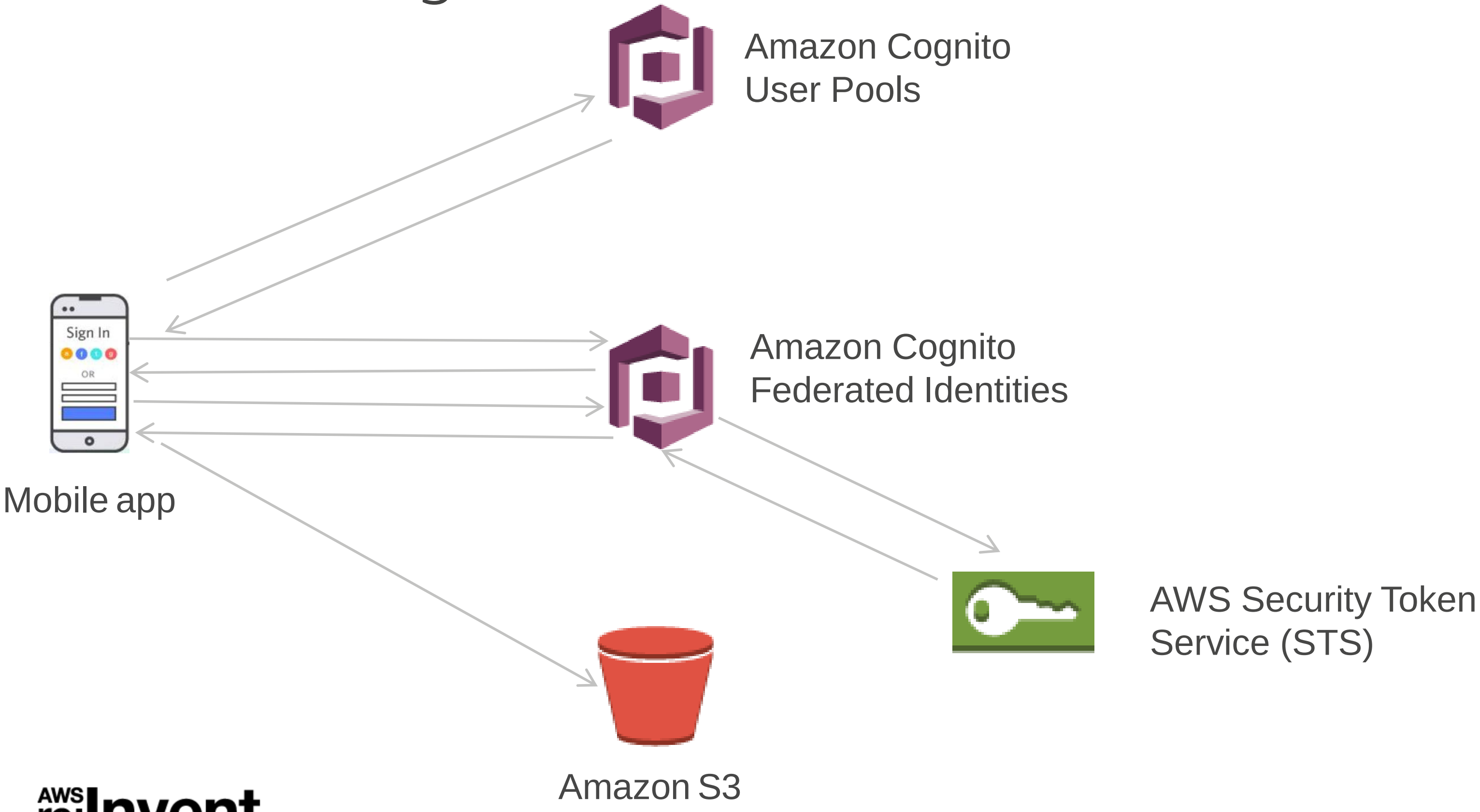
SpaceFinder

Welcome to SpaceFinder!

Book a conference room for your team meeting.

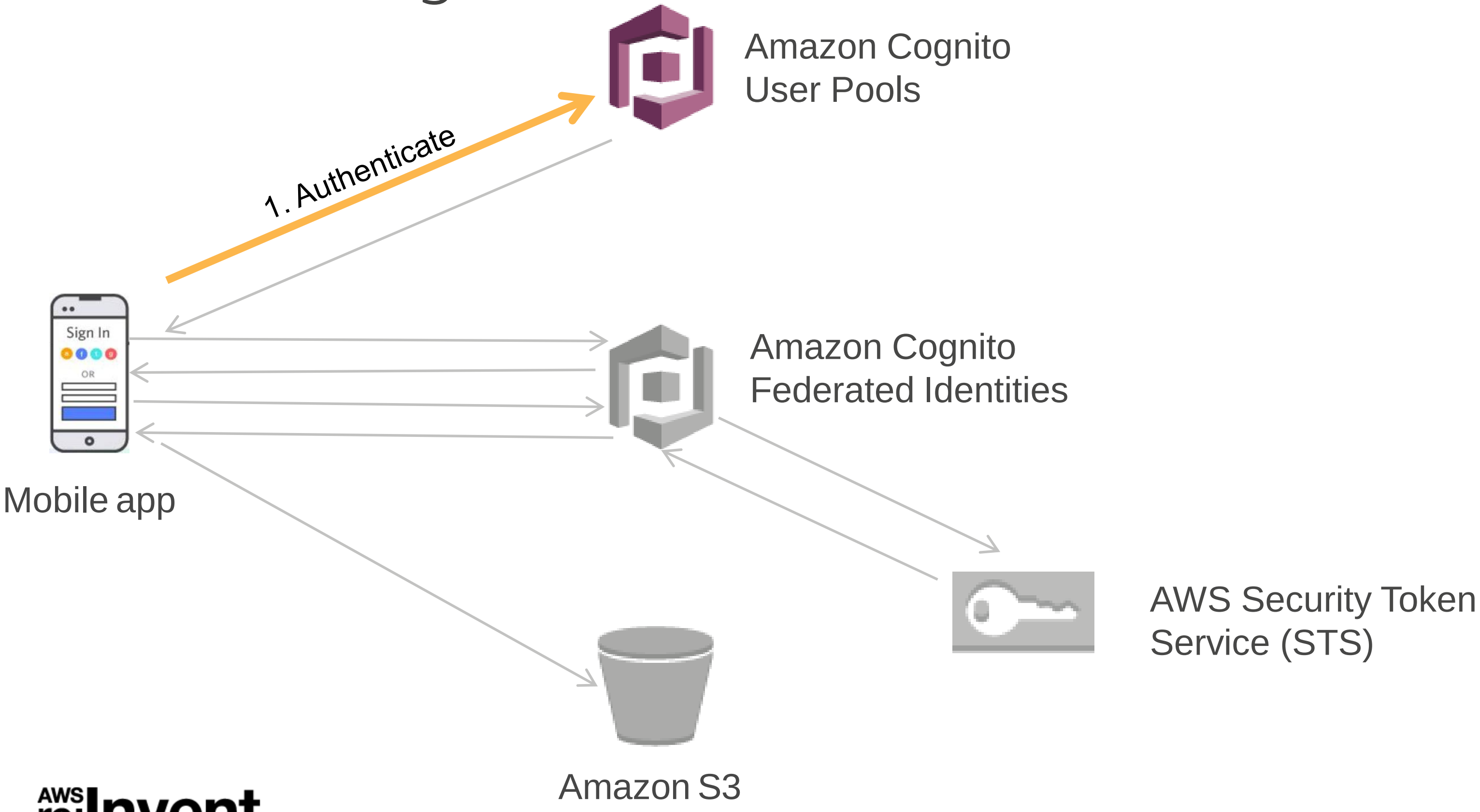
Visiting a remote office? You can book a desk in advance.

Federating access to AWS resources

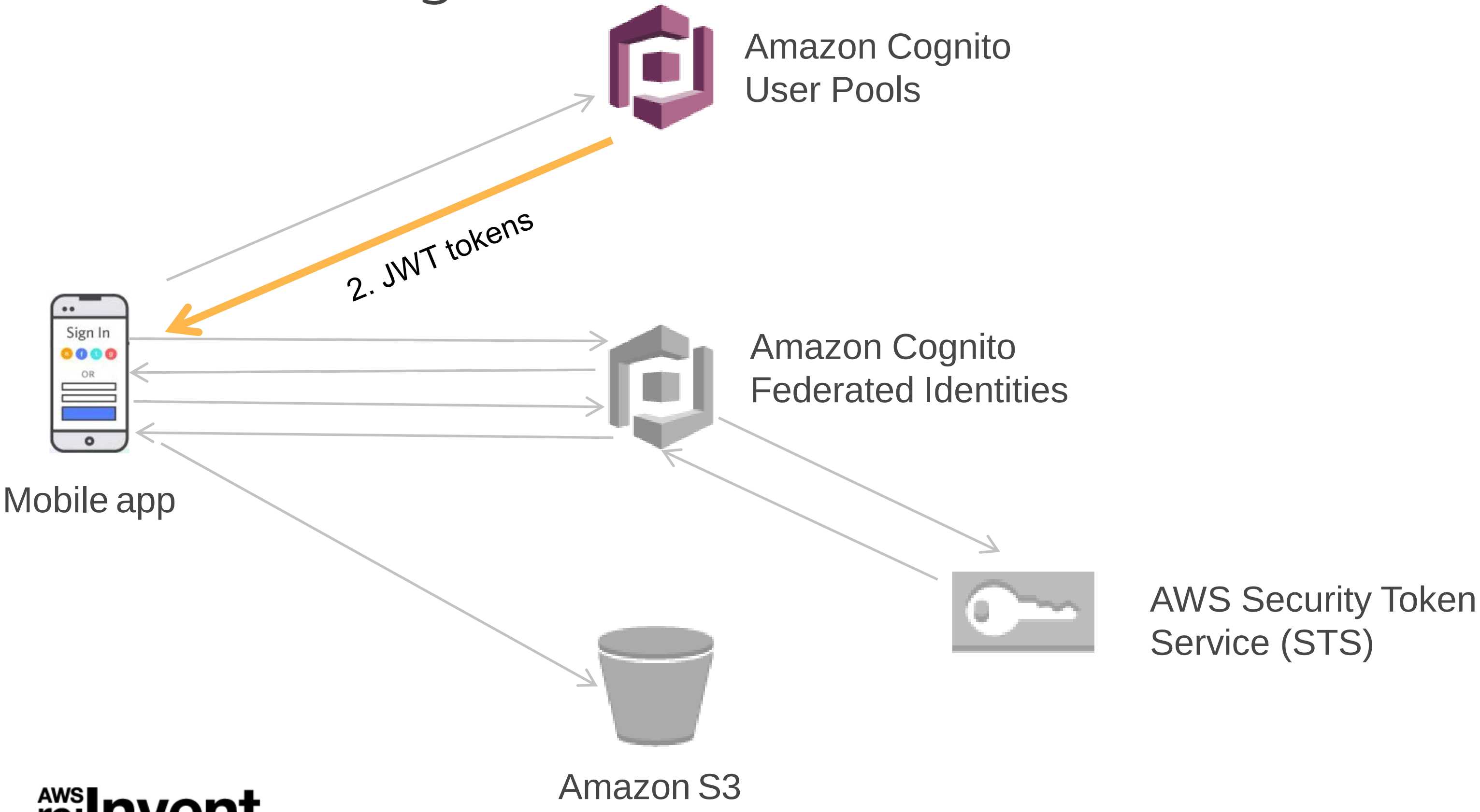


Amazon Cognito User Pools
Amazon Cognito Federated Identities
Sign In
OR
Mobile app
AWS Security Token Service (STS)
Amazon S3

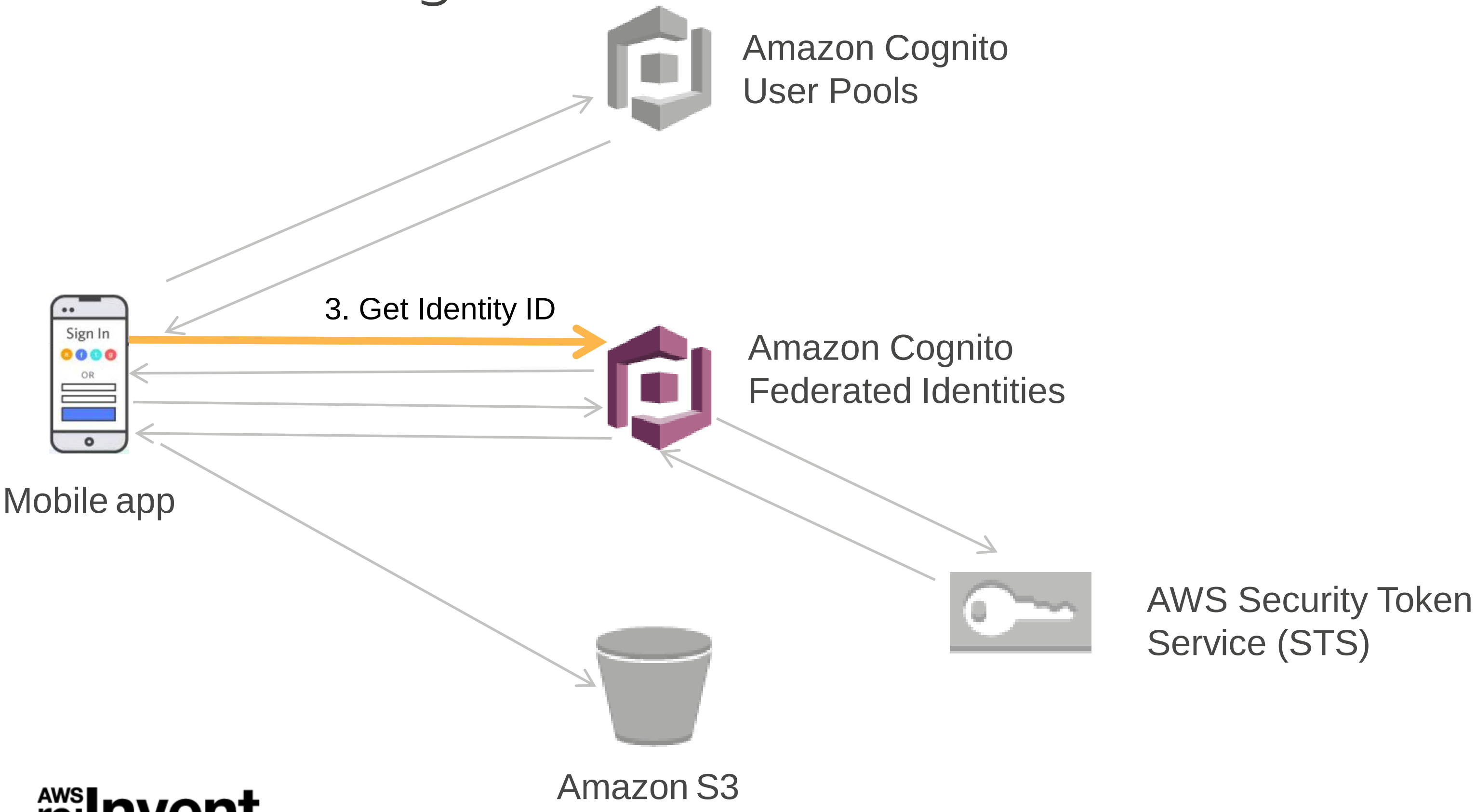
Federating access to AWS resources



Federating access to AWS resources



Federating access to AWS resources



Amazon Cognito User Pools

3. Get Identity ID

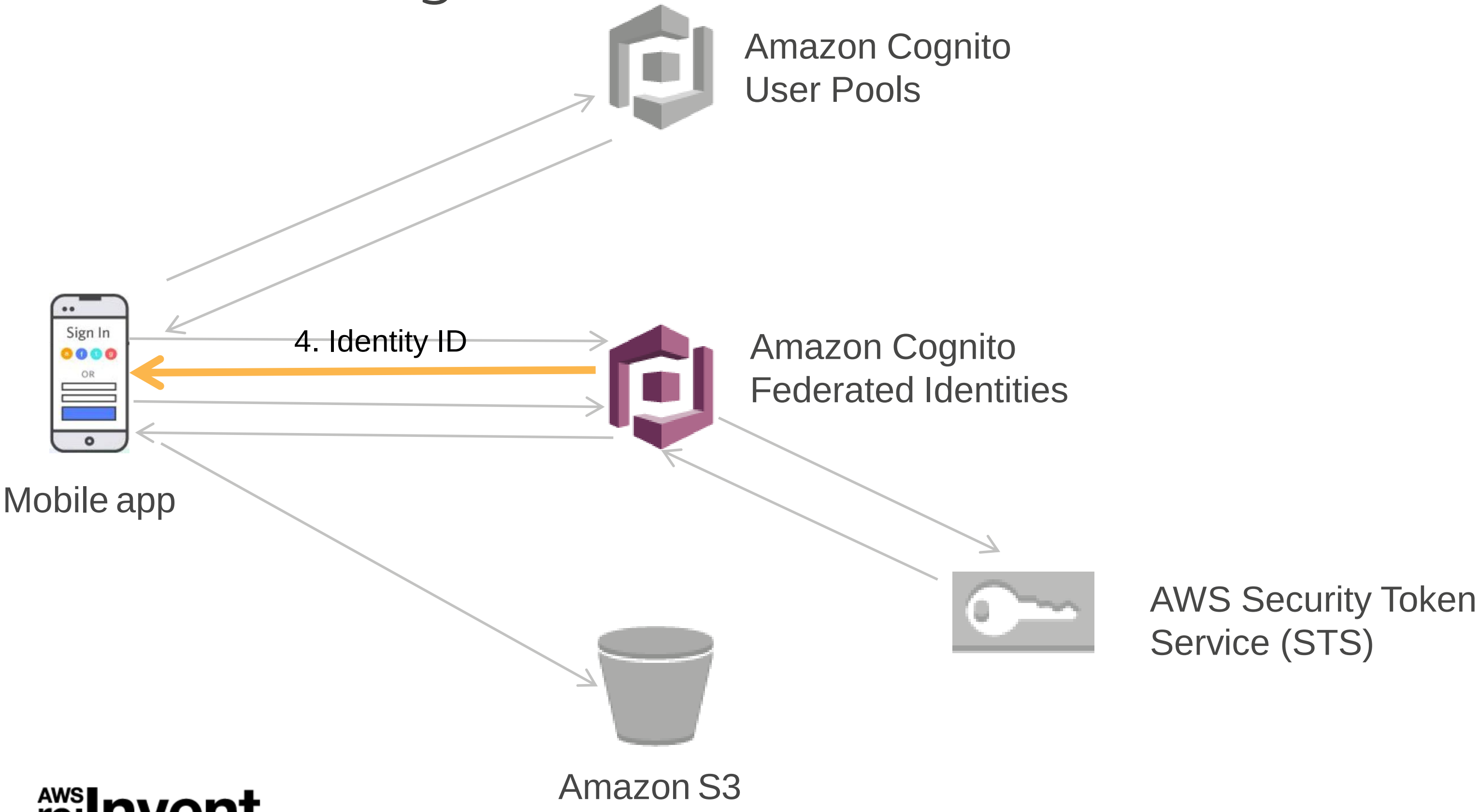
Amazon Cognito Federated Identities

Mobile app

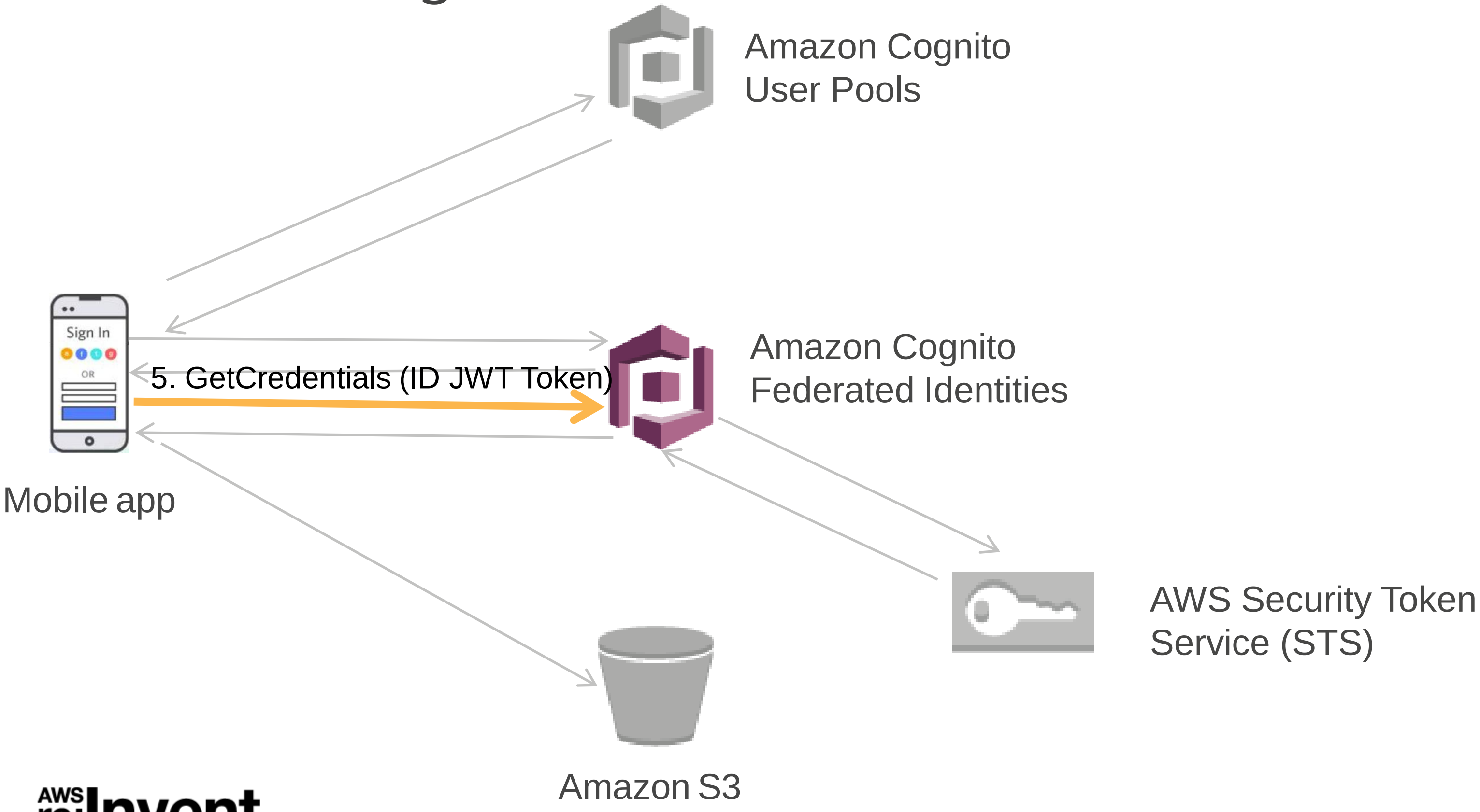
AWS Security Token Service (STS)

Amazon S3

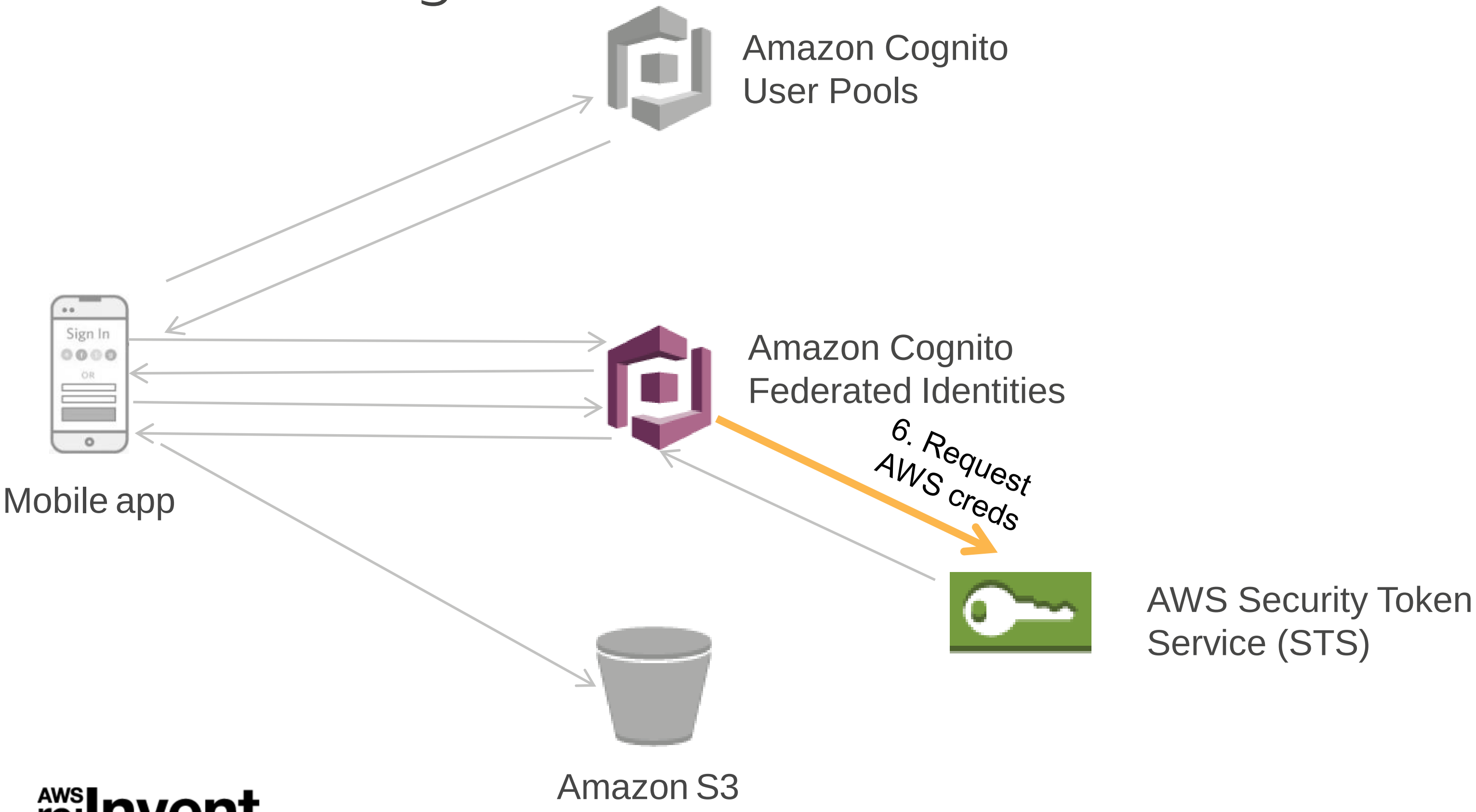
Federating access to AWS resources



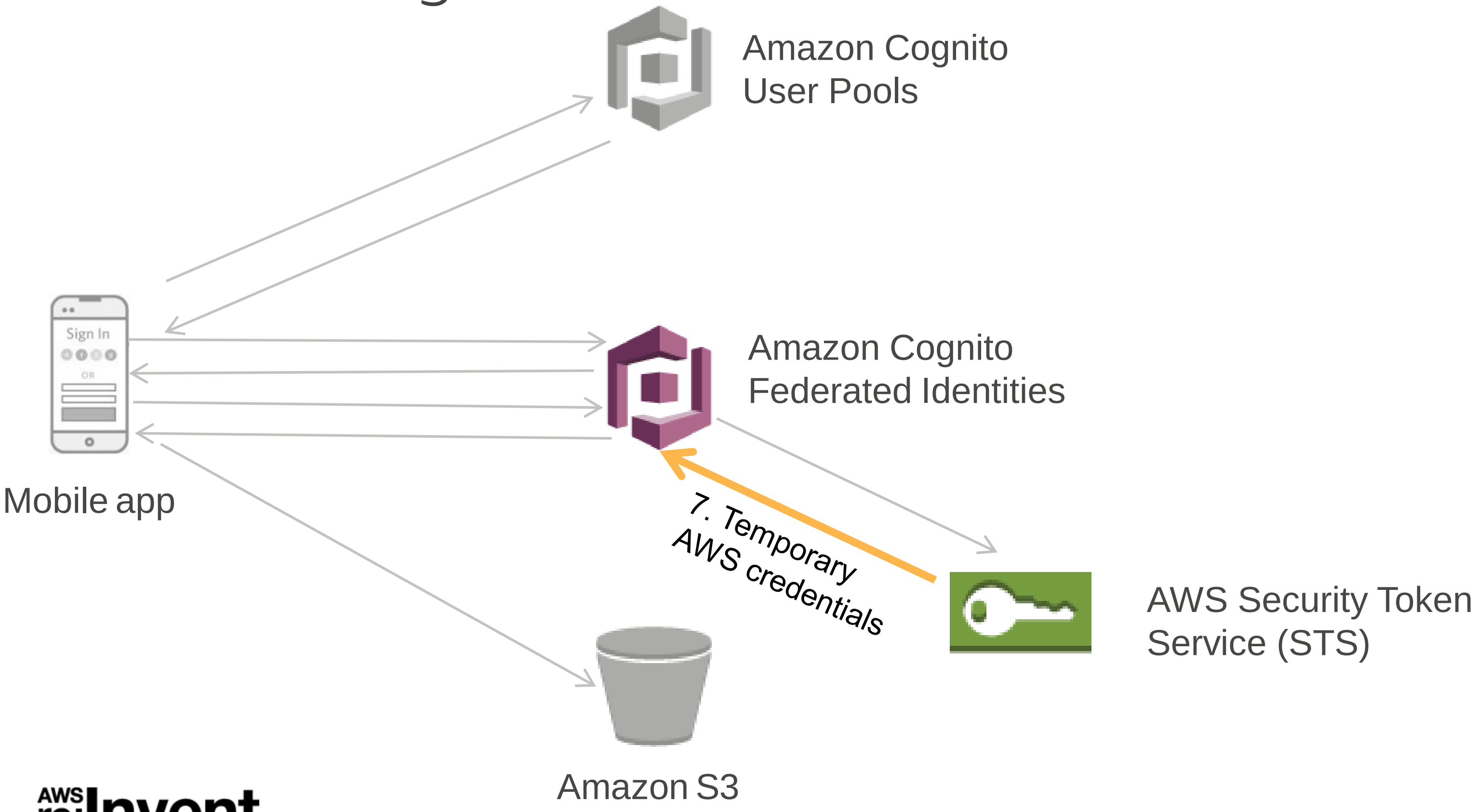
Federating access to AWS resources



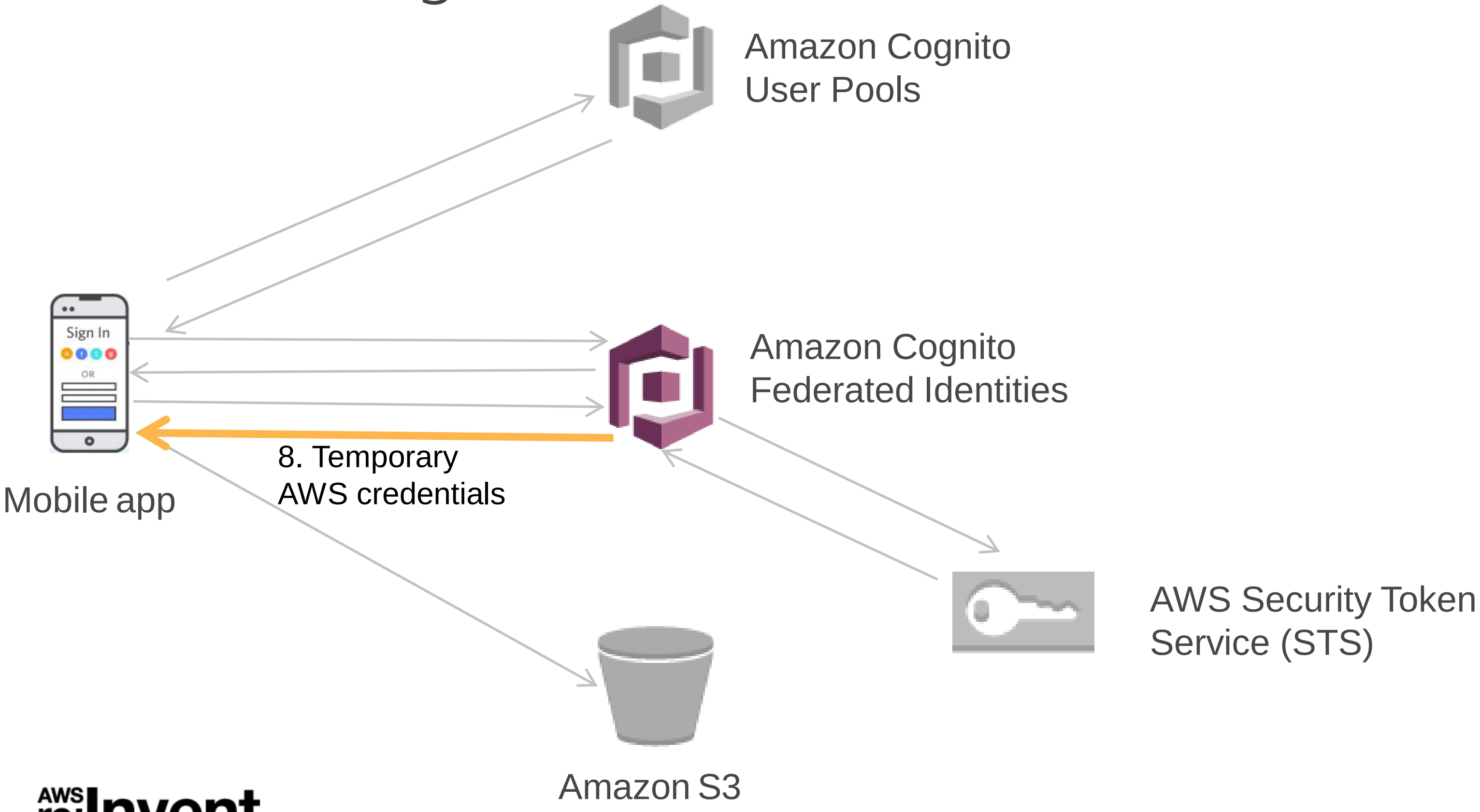
Federating access to AWS resources


Amazon Cognito User Pools
Sign In
OR
Mobile app
Amazon Cognito Federated Identities
6. Request AWS creds
AWS Security Token Service (STS)
Amazon S3

Federating access to AWS resources



Federating access to AWS resources



Amazon Cognito User Pools

Amazon Cognito Federated Identities

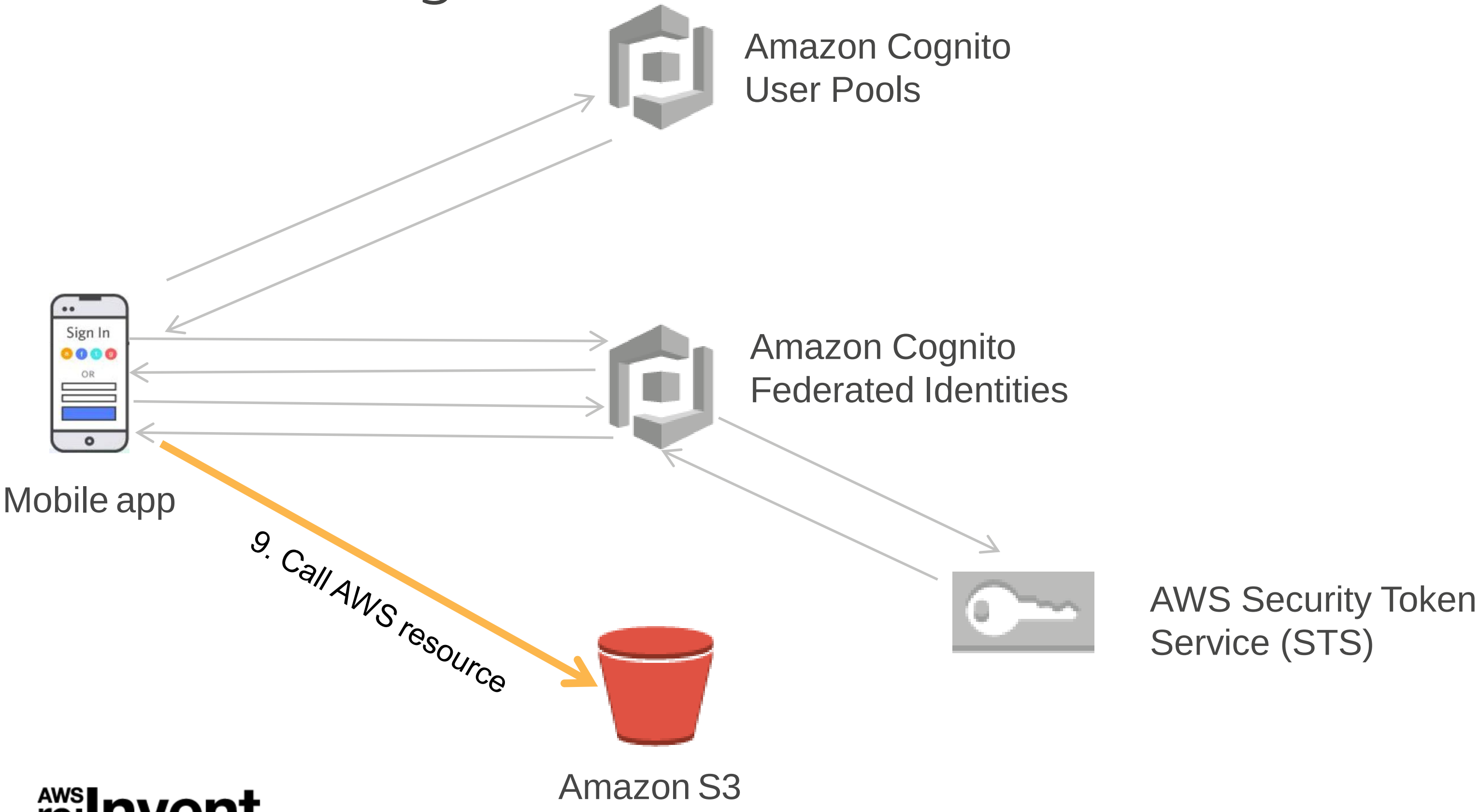
8. Temporary AWS credentials

Mobile app

AWS Security Token Service (STS)

Amazon S3

Federating access to AWS resources



“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

Fine-grained Role-Based Access Control

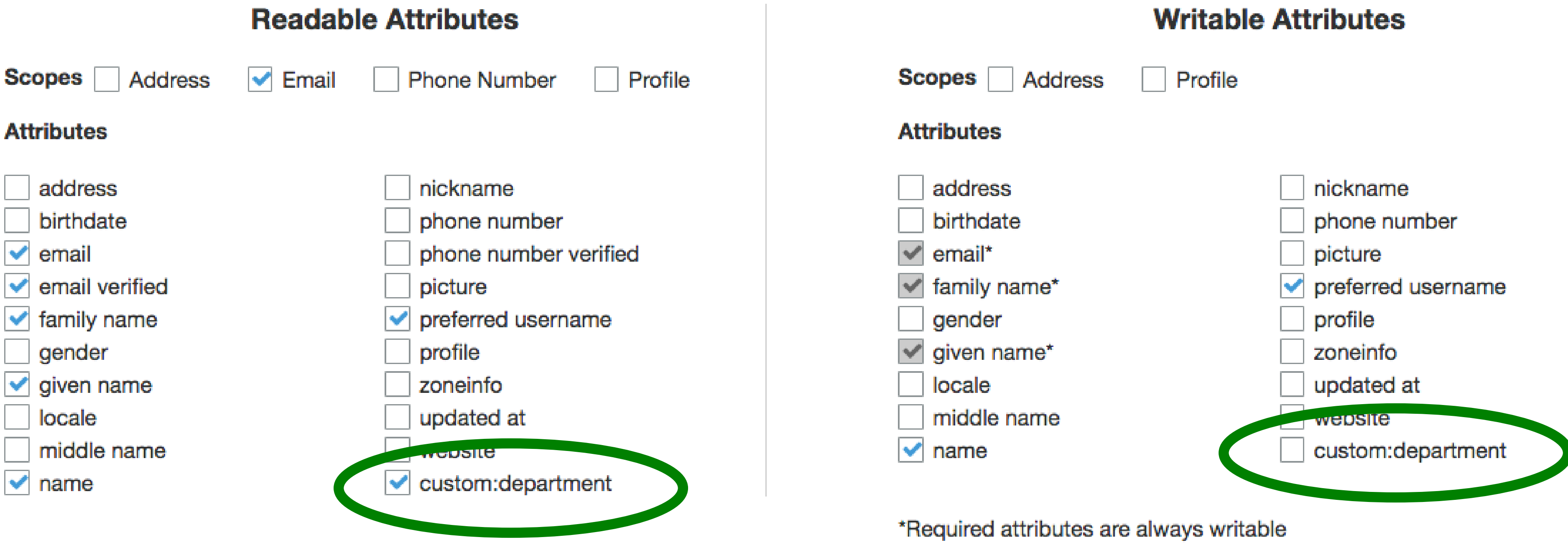
Unauthenticated users:

- Default role

Authenticated users

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

Fine-grained RBAC (role from rule)



Readable Attributes

Scopes □ Address ☑ Email □ Phone Number □ Profile

Attributes

□ address
□ birthdate
☑ email
☑ email verified
☑ family name
□ gender
☑ given name
□ locale
□ middle name
☑ name

□ nickname
□ phone number
□ phone number verified
□ picture
☑ preferred username
□ profile
□ zoneinfo
□ updated at
□ website
☑ custom:department

Writable Attributes

Scopes □ Address □ Profile

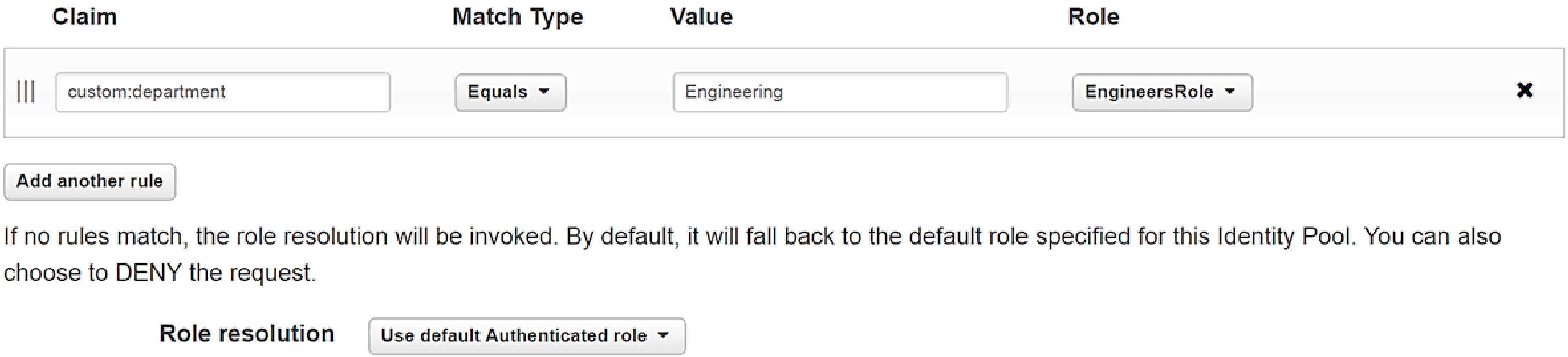
Attributes

□ address
□ birthdate
☑ email*
☑ family name*
□ gender
☑ given name*
□ locale
□ middle name
☑ name

□ nickname
□ phone number
□ picture
☑ preferred username
□ profile
□ zoneinfo
□ updated at
□ website
□ custom:department

*Required attributes are always writable

Fine-grained RBAC (role from rule)

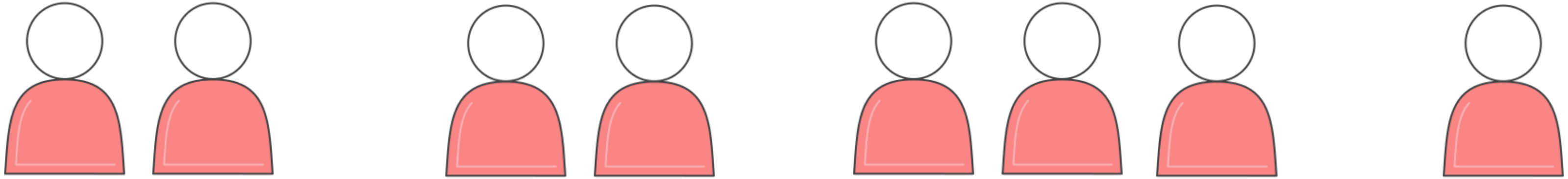


Claim	Match Type	Value	Role
custom:department	Equals ▾	Engineering	EngineersRole ▾

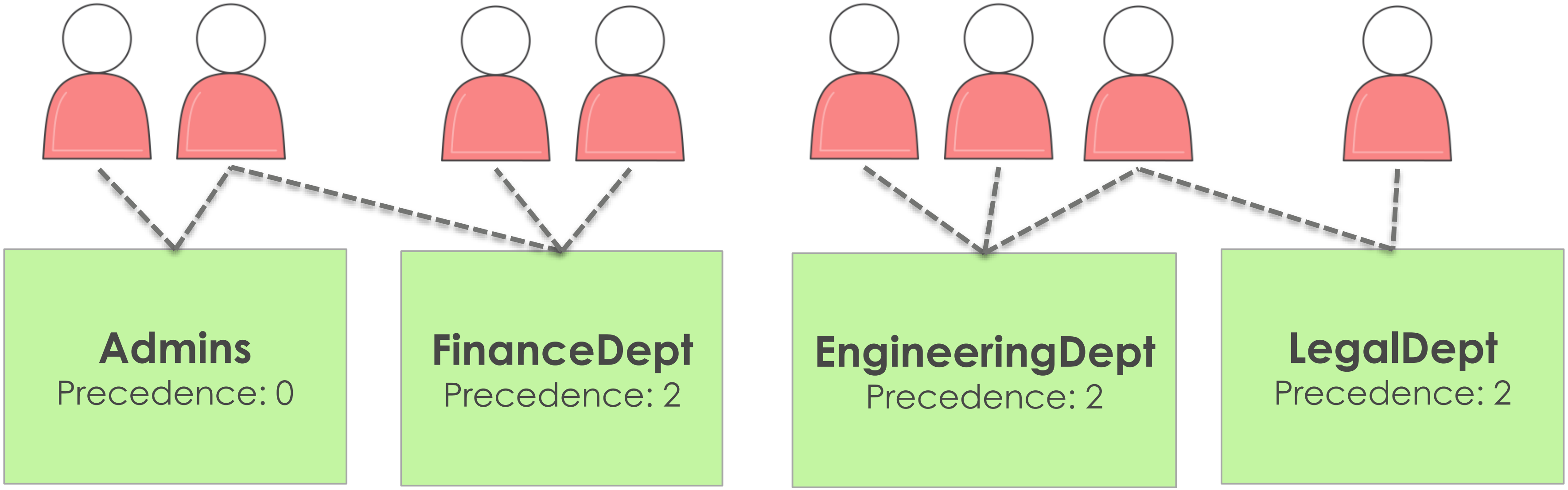
If no rules match, the role resolution will be invoked. By default, it will fall back to the default role specified for this Identity Pool. You can also choose to DENY the request.

Role resolution: Use default Authenticated role ▾

Fine-grained RBAC (role from token)



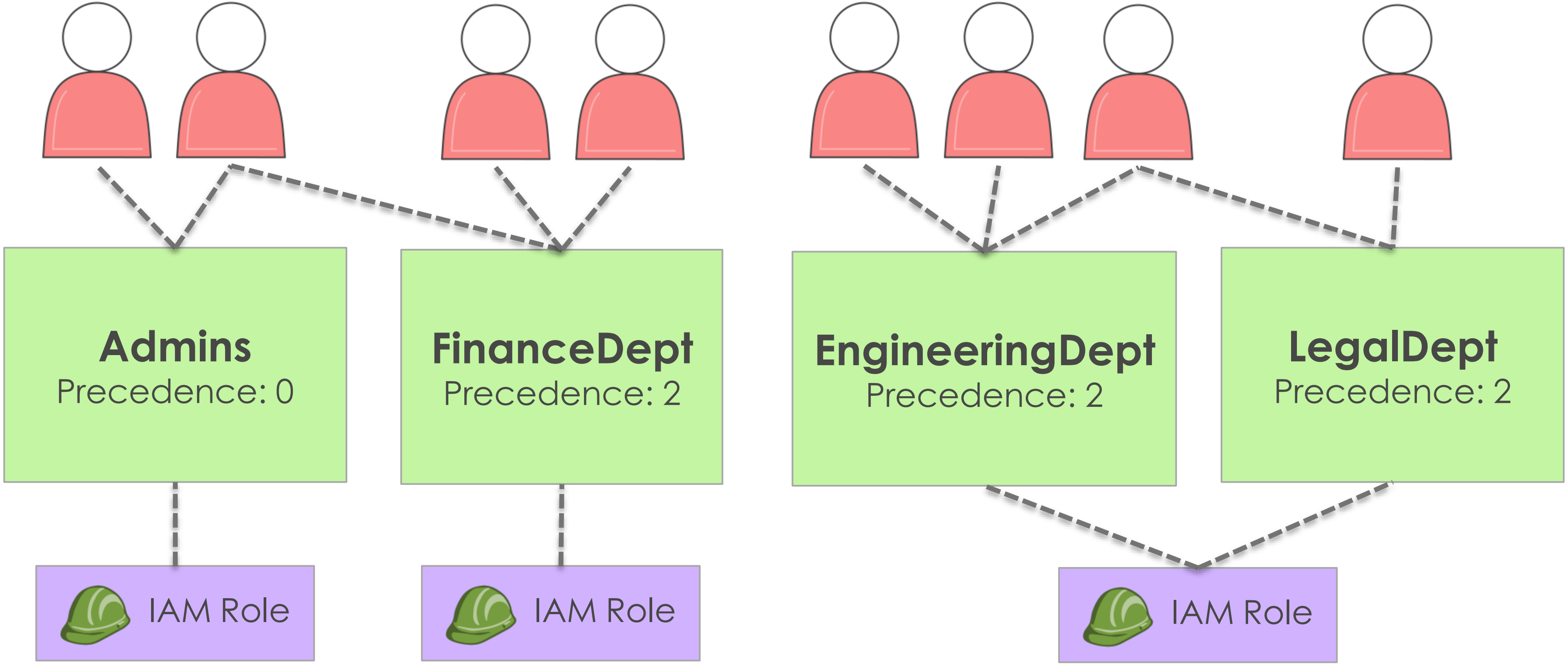
Fine-grained RBAC (role from token)



AWS re:Invent

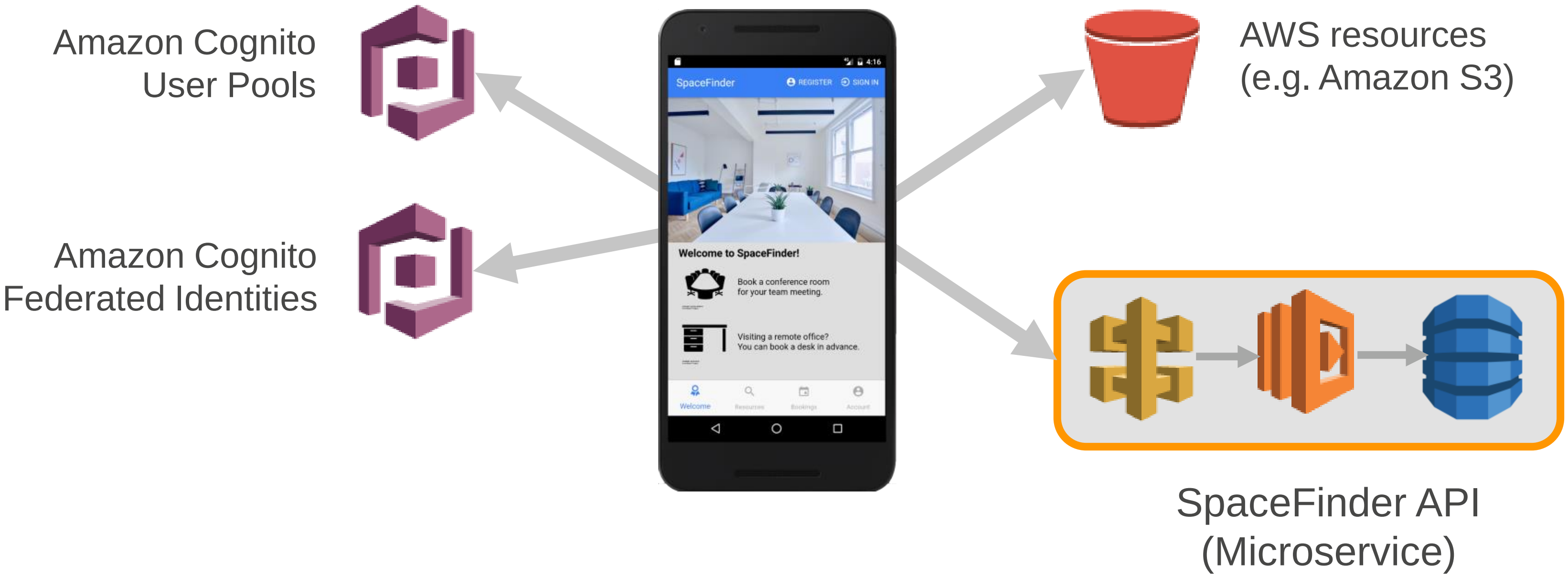
aws

Fine-grained RBAC (role from token)



DEMO

Application so far…



Welcome to SpaceFinder!

Book a conference room
for your team meeting.

Visiting a remote office?
You can book a desk in advance.

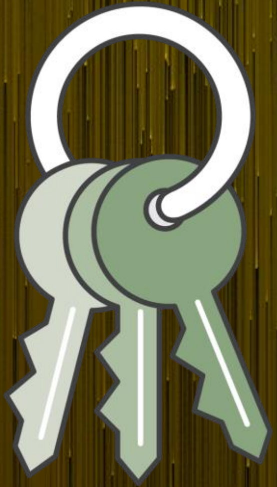
Amazon Cognito
User Pools

Amazon Cognito
Federated Identities

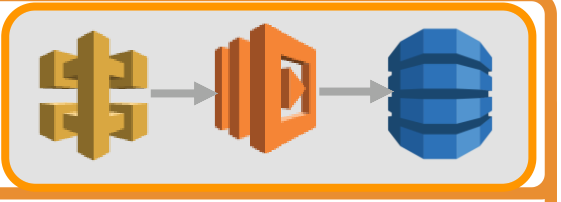
AWS resources
(e.g. Amazon S3)

SpaceFinder API
(Microservice)

Authorizing Serverless APIs

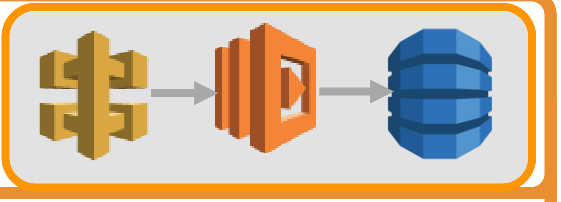


SpaceFinder API



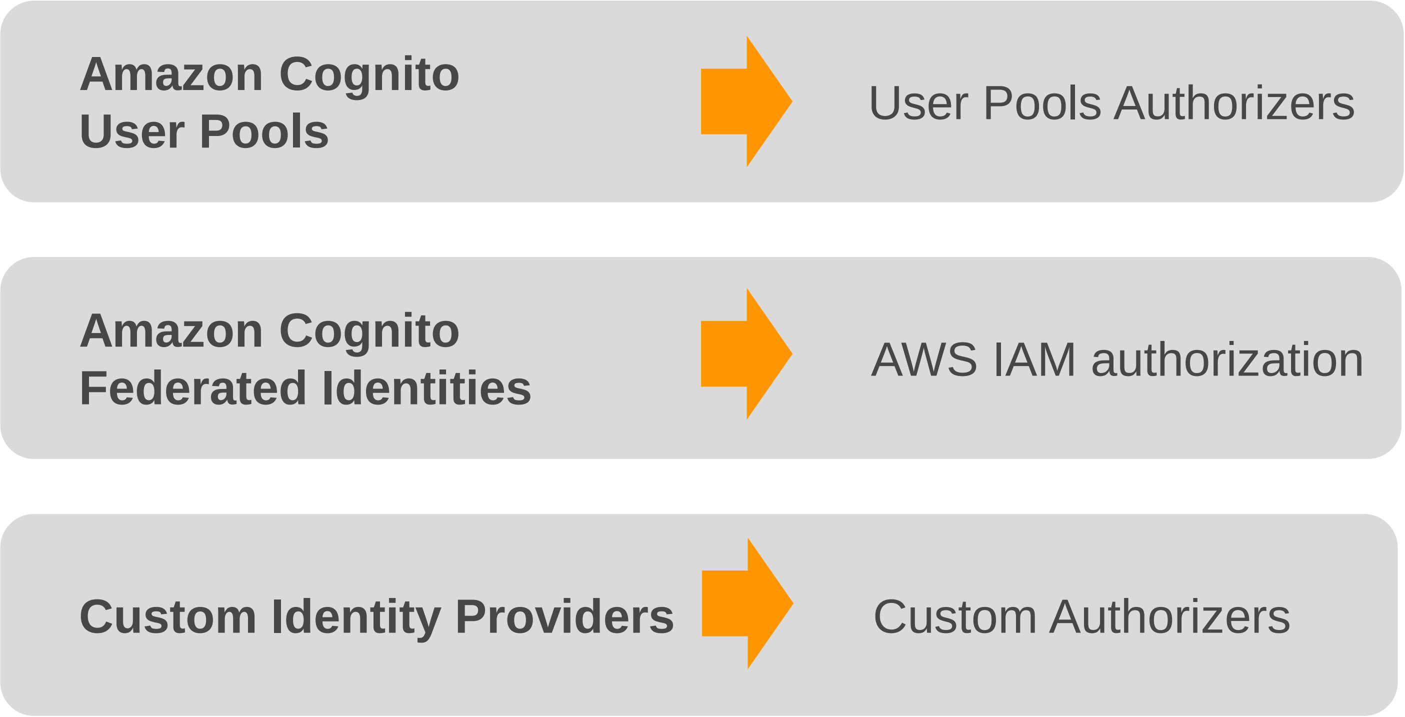
POST	/locations
GET	/locations
GET	/locations/{locationId}
DELETE	/locations/{locationId}
GET	/locations/{locationId}/resources
POST	/locations/{locationId}/resources
DELETE	/locations/{locationId}/resources/{resourceId}
GET	/locations/{locationId}/resources/{resourceId}/bookings
GET	/users/{userId}/bookings
POST	/users/{userId}/bookings
DELETE	/users/{userId}/bookings/{bookingId}

SpaceFinder API



Admin only	POST	/locations
	GET	/locations
	GET	/locations/{locationId}
Admin only	DELETE	/locations/{locationId}
	GET	/locations/{locationId}/resources
Admin only	POST	/locations/{locationId}/resources
Admin only	DELETE	/locations/{locationId}/resources/{resourceId}
	GET	/locations/{locationId}/resources/{resourceId}/bookings
	GET	/users/{userId}/bookings
	POST	/users/{userId}/bookings
	DELETE	/users/{userId}/bookings/{bookingId}

API Gateway: three types of authorization

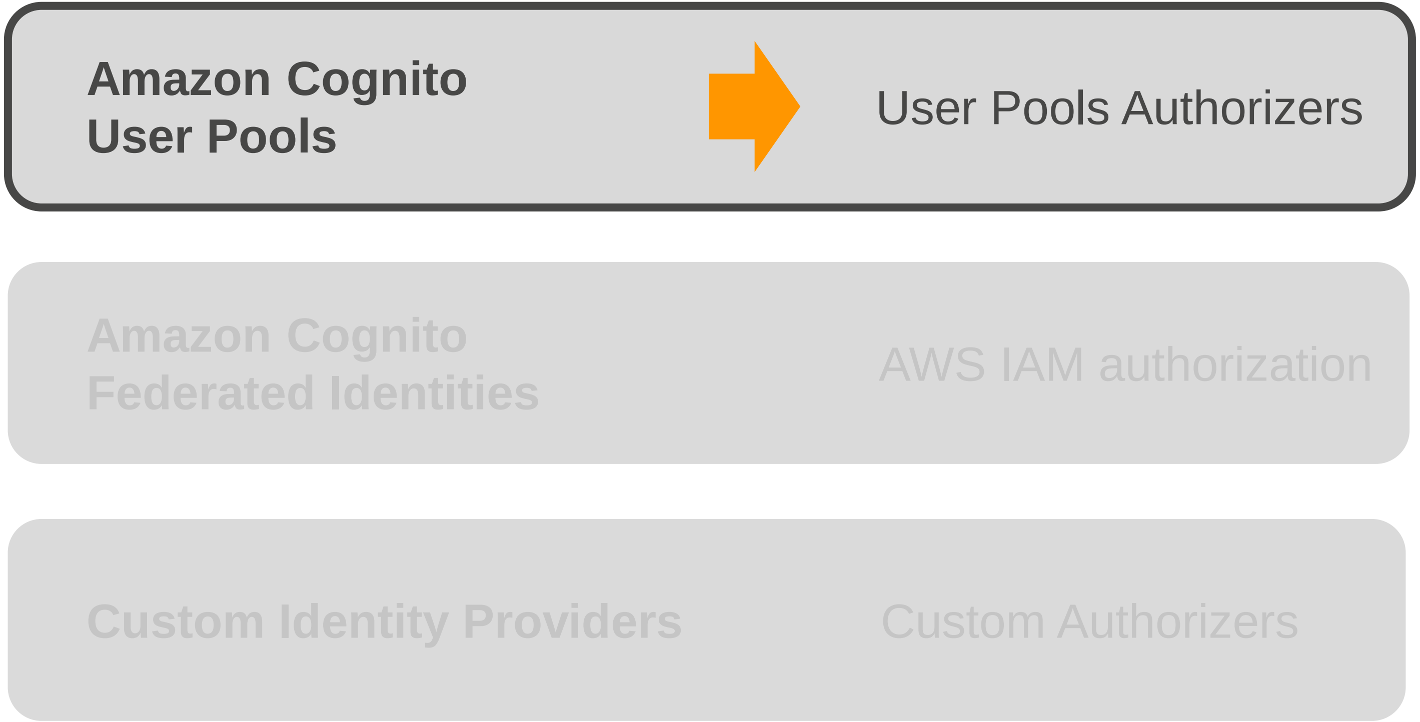


Amazon Cognito User Pools → User Pools Authorizers

Amazon Cognito Federated Identities → AWS IAM authorization

Custom Identity Providers → Custom Authorizers

API Gateway: three types of authorization

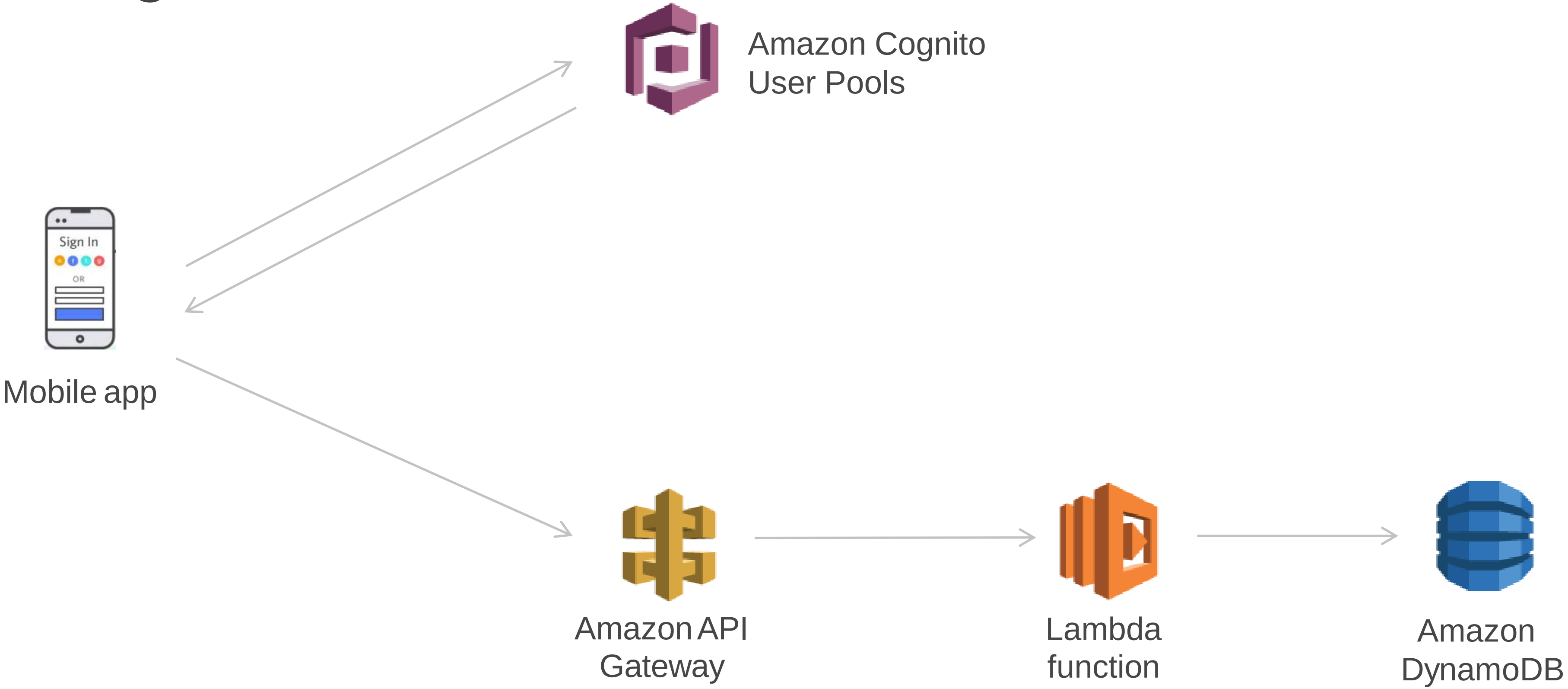


Amazon Cognito User Pools → User Pools Authorizers

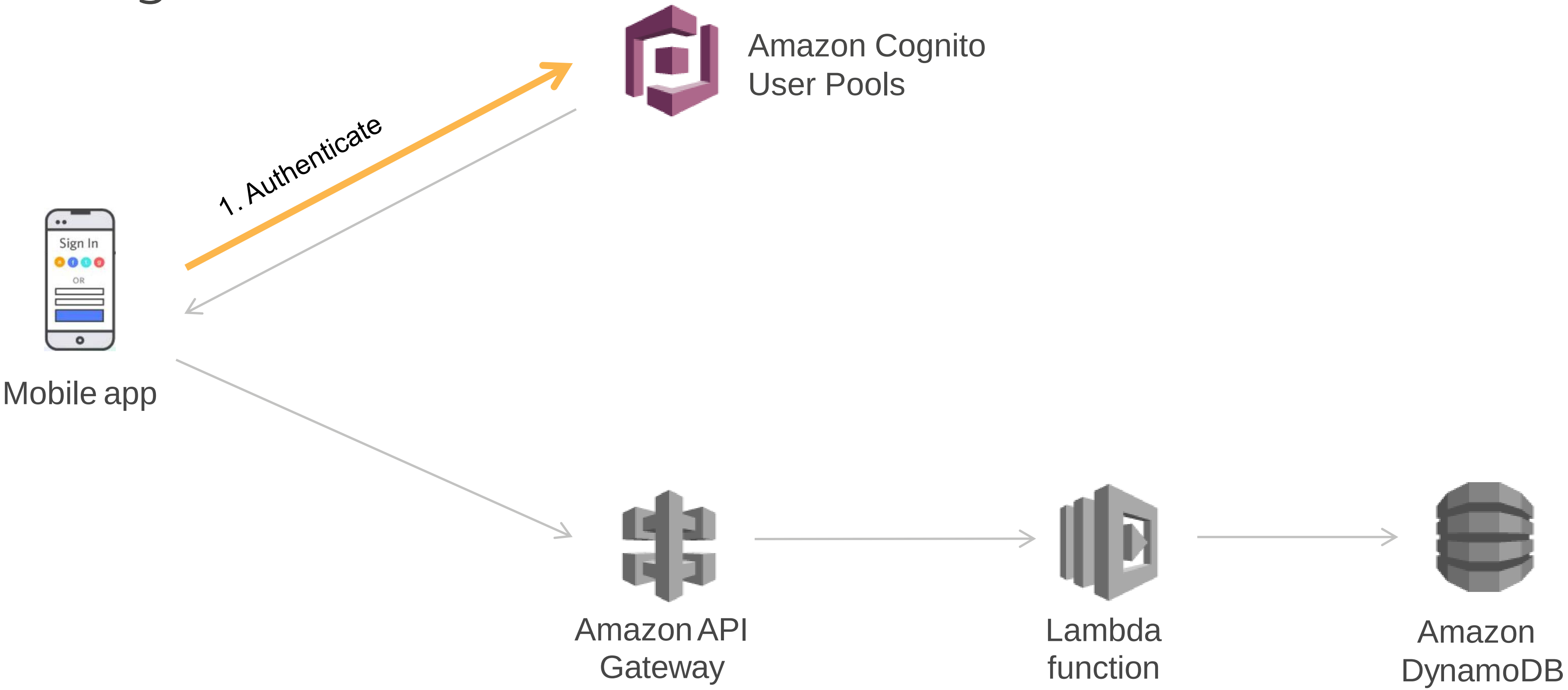
Amazon Cognito Federated Identities AWS IAM authorization

Custom Identity Providers Custom Authorizers

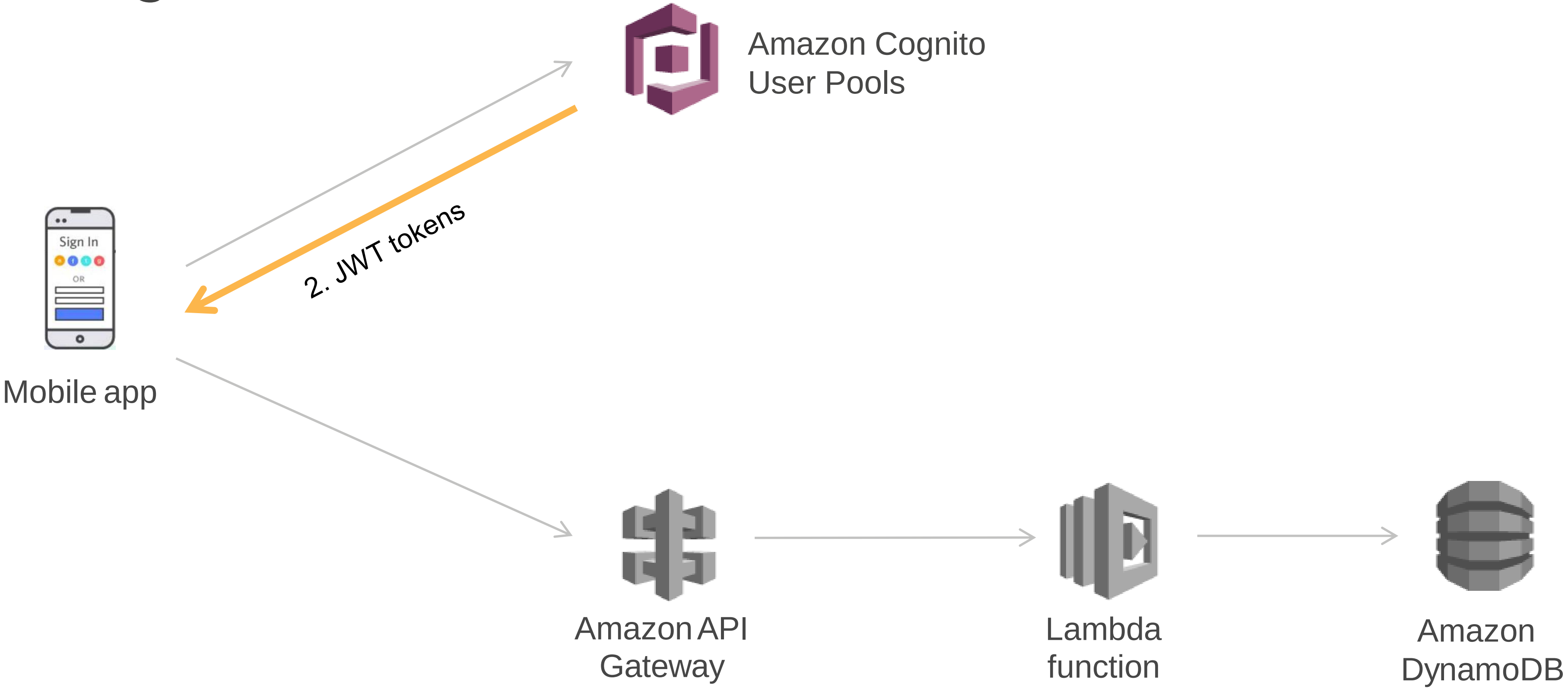
Cognito User Pools Authorizers



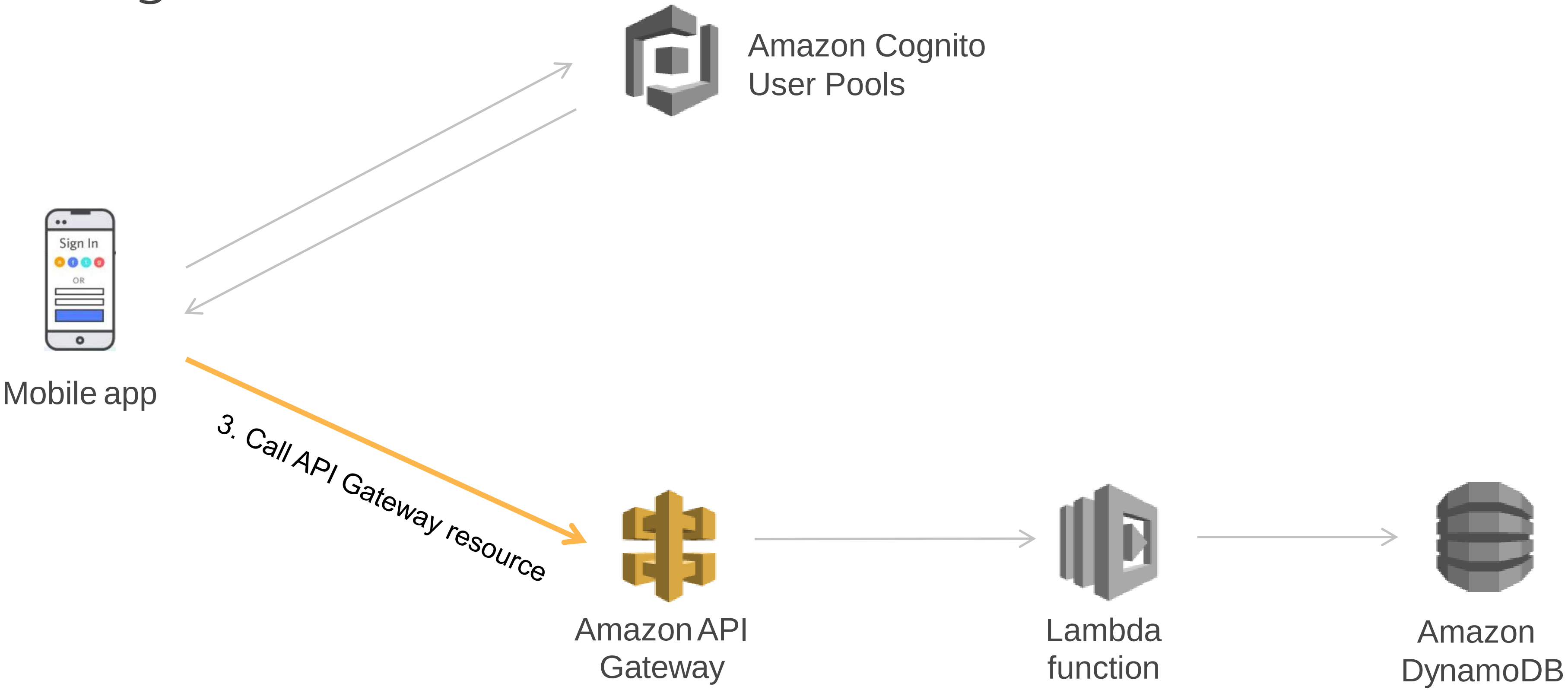
Cognito User Pools Authorizers



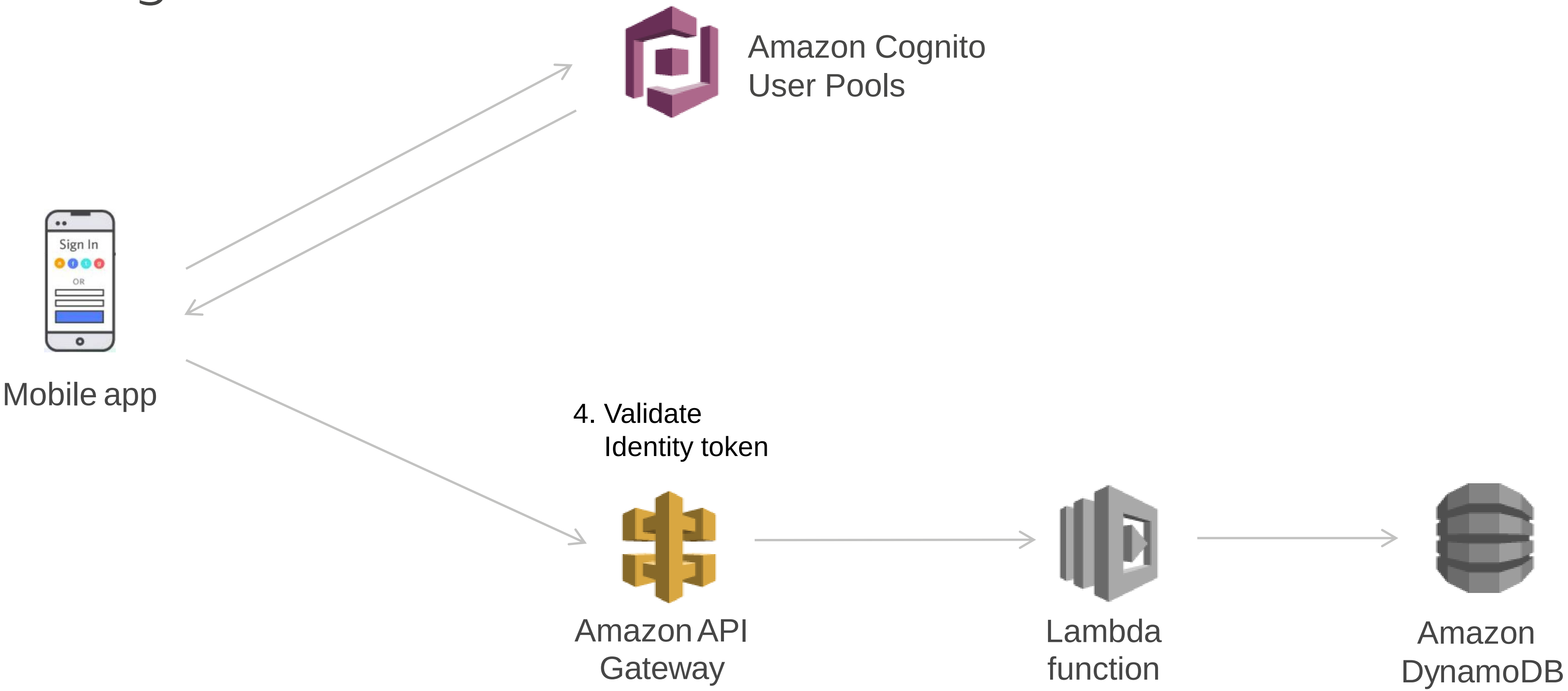
Cognito User Pools Authorizers



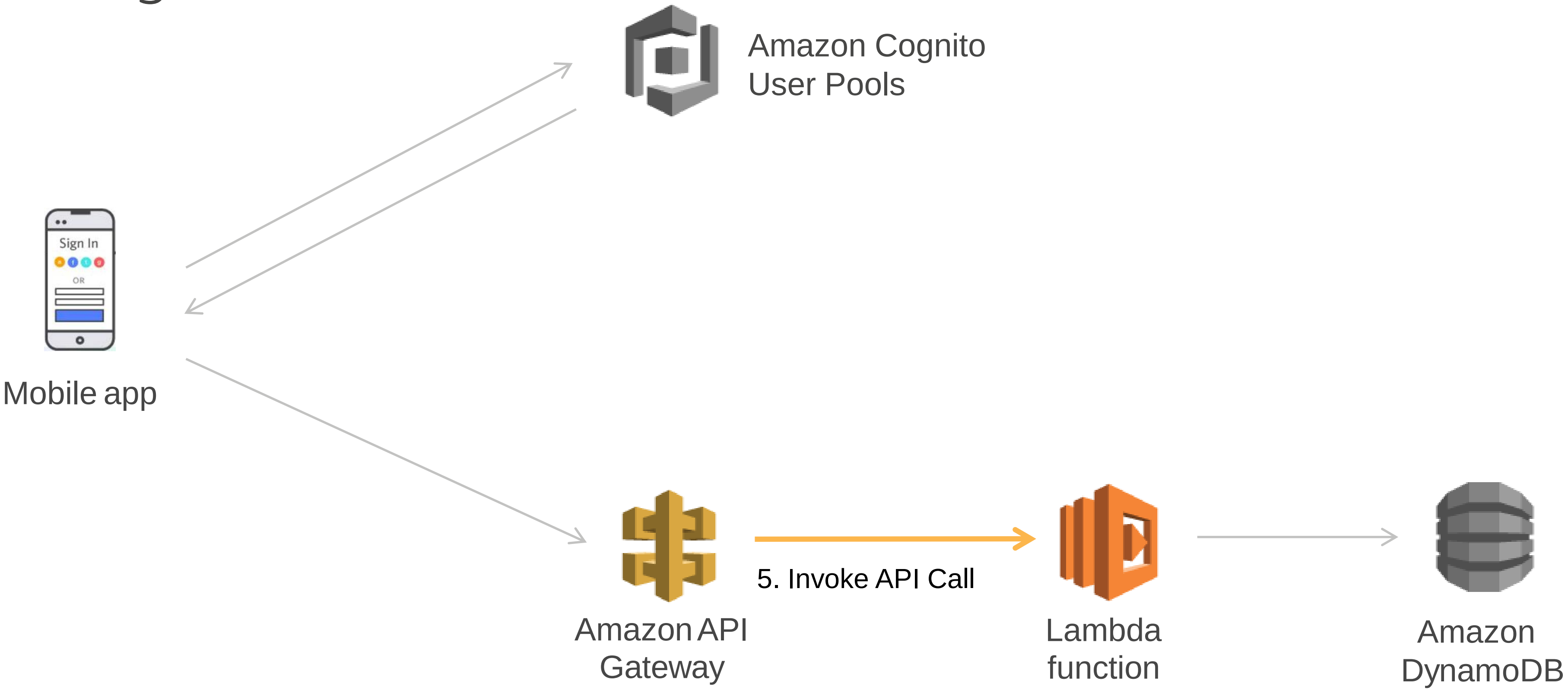
Cognito User Pools Authorizers



Cognito User Pools Authorizers



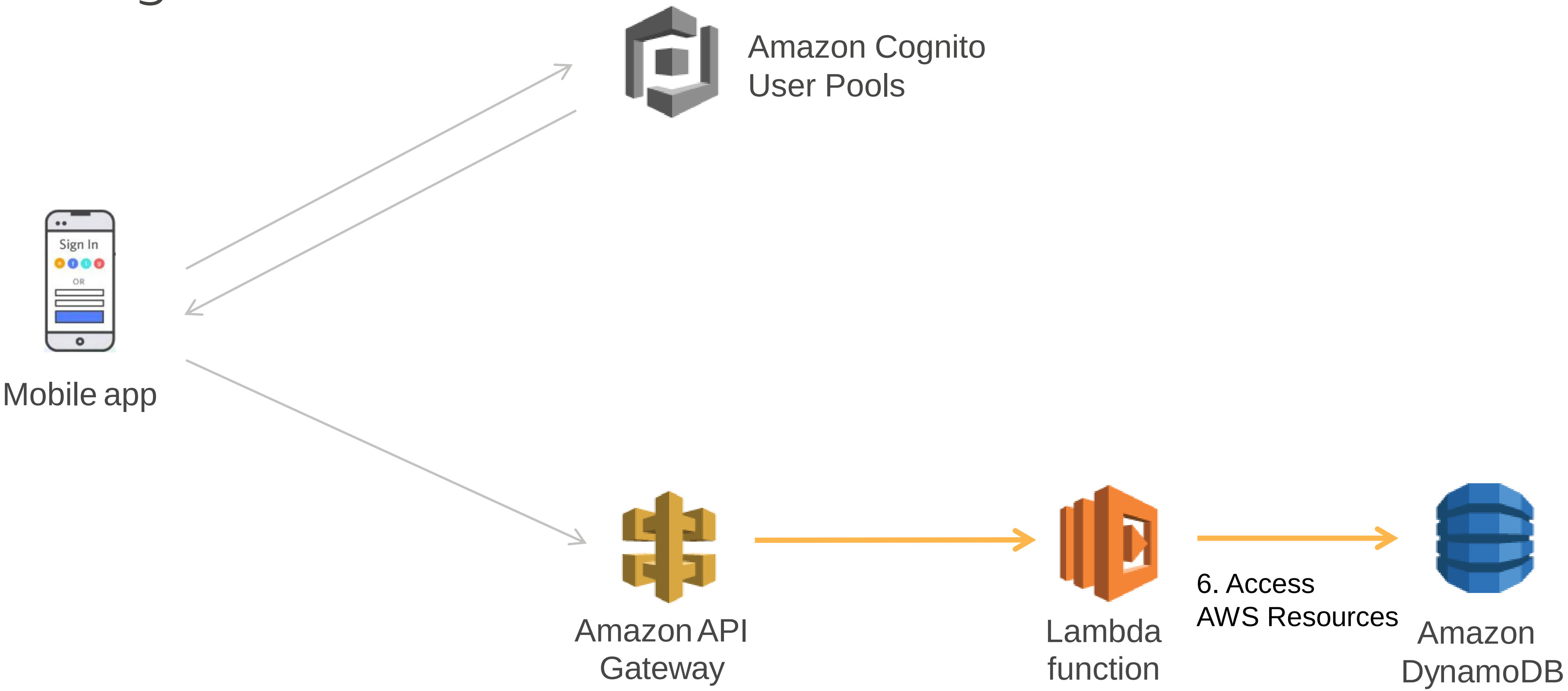
Cognito User Pools Authorizers



AWS re:Invent

aws

Cognito User Pools Authorizers



Amazon Cognito
User Pools

Mobile app

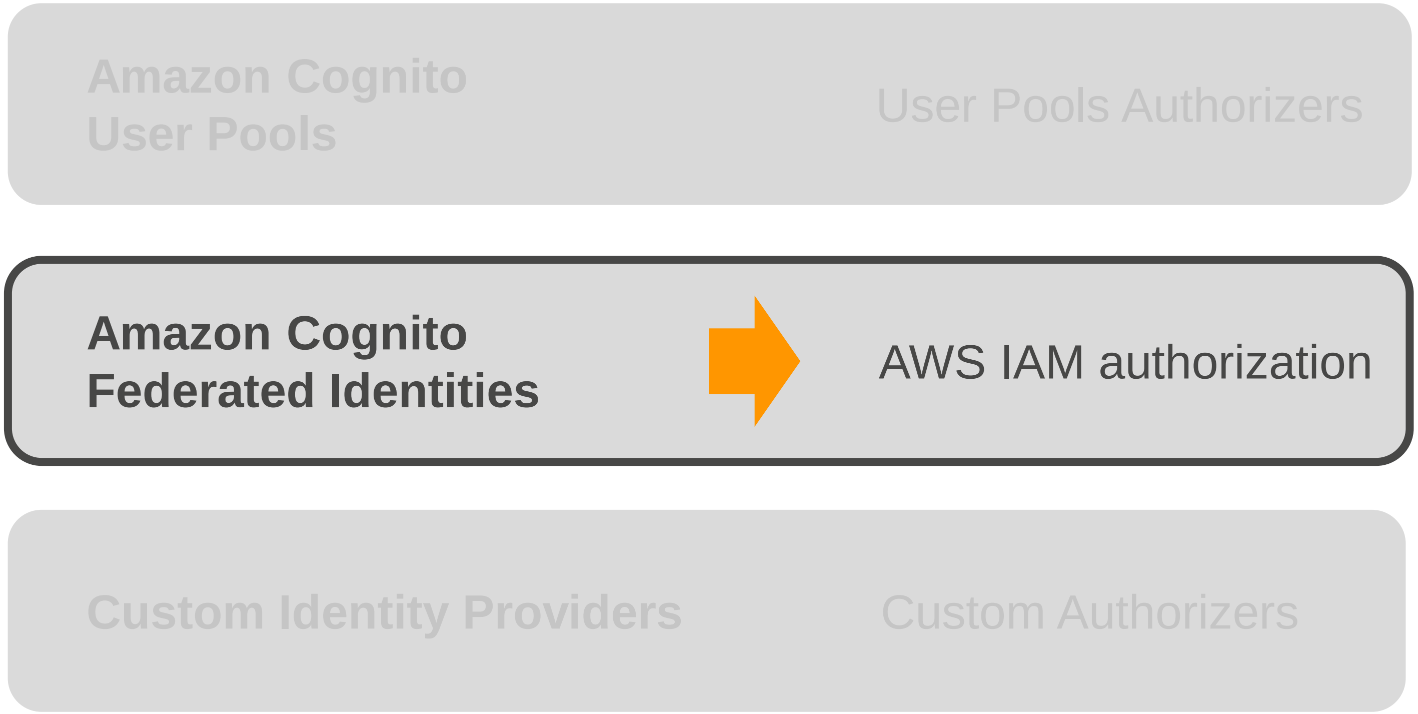
Amazon API
Gateway

Lambda
function

6. Access
AWS Resources

Amazon
DynamoDB

API Gateway: three types of authorization

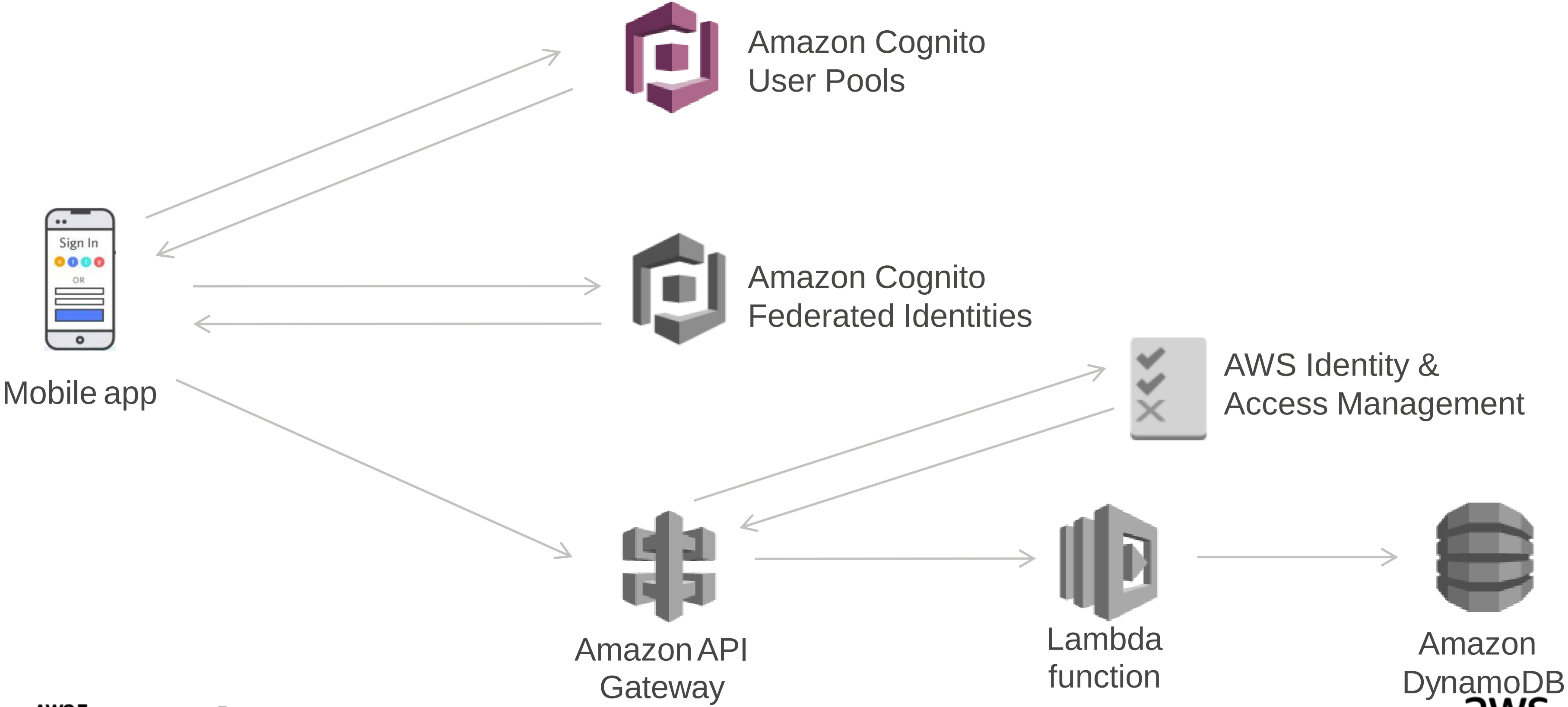


Amazon Cognito User Pools → User Pools Authorizers

Amazon Cognito Federated Identities → AWS IAM authorization

Custom Identity Providers → Custom Authorizers

IAM-based authorization



Amazon Cognito User Pools

Amazon Cognito Federated Identities

AWS Identity & Access Management

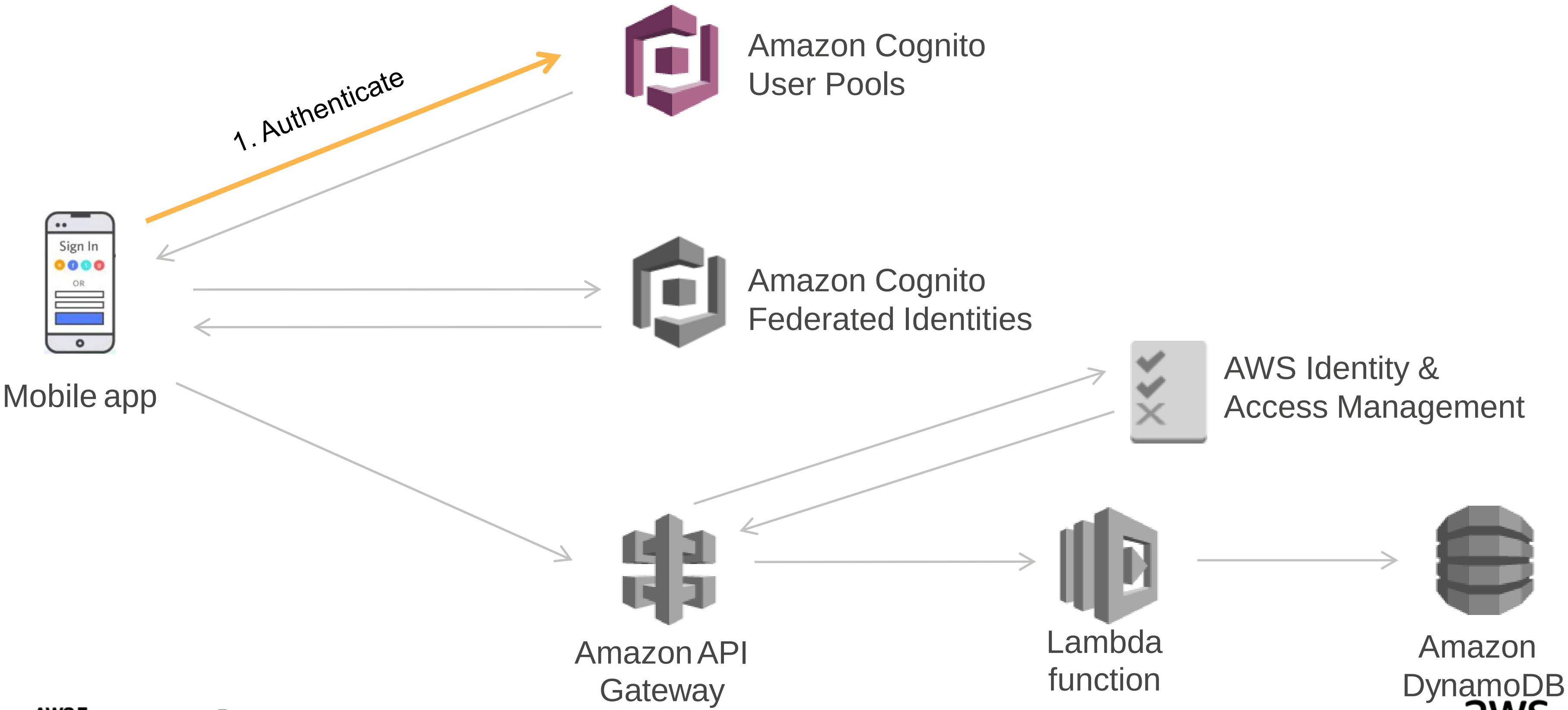
Mobile app

Amazon API Gateway

Lambda function

Amazon DynamoDB

IAM-based authorization

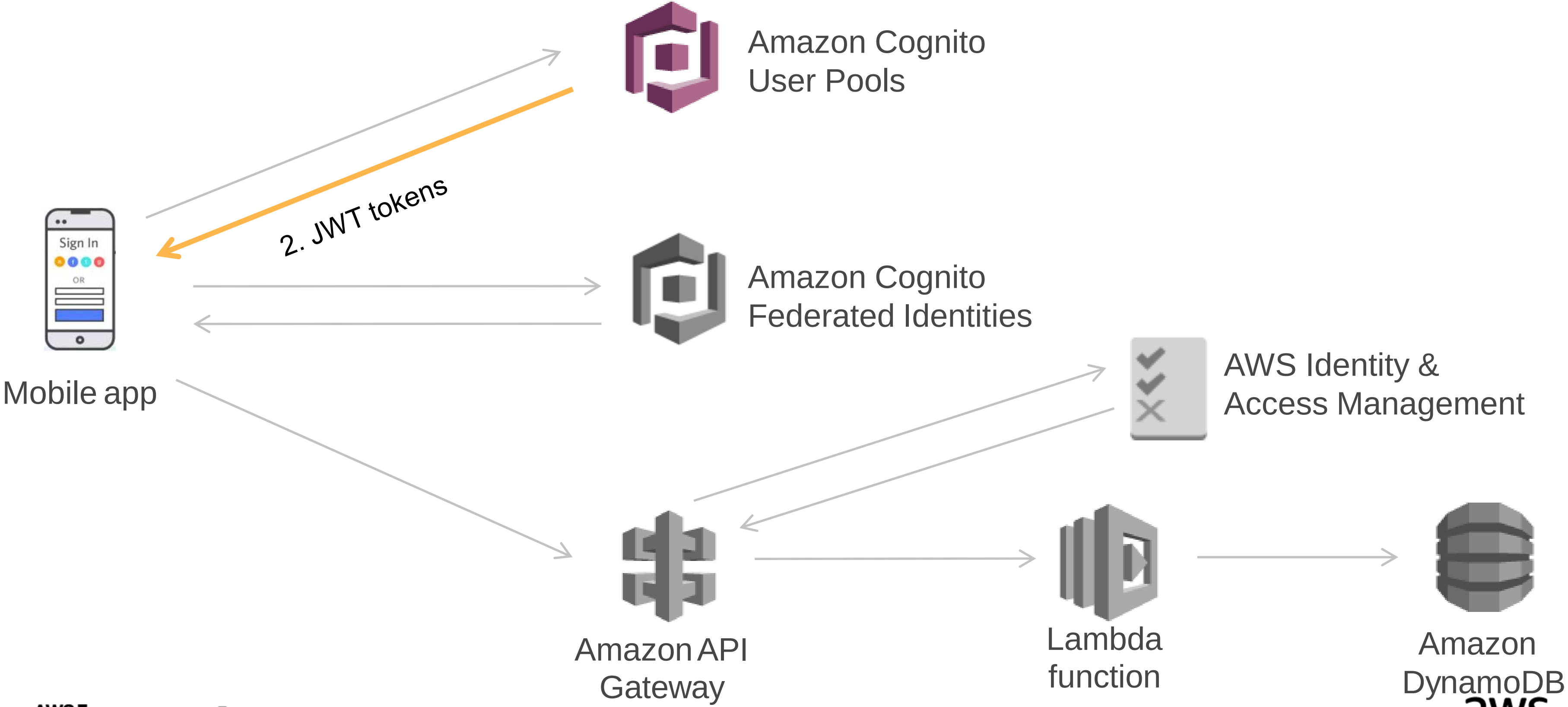


1. Authenticate
Amazon Cognito User Pools
Sign In
OR
Mobile app
Amazon Cognito Federated Identities
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

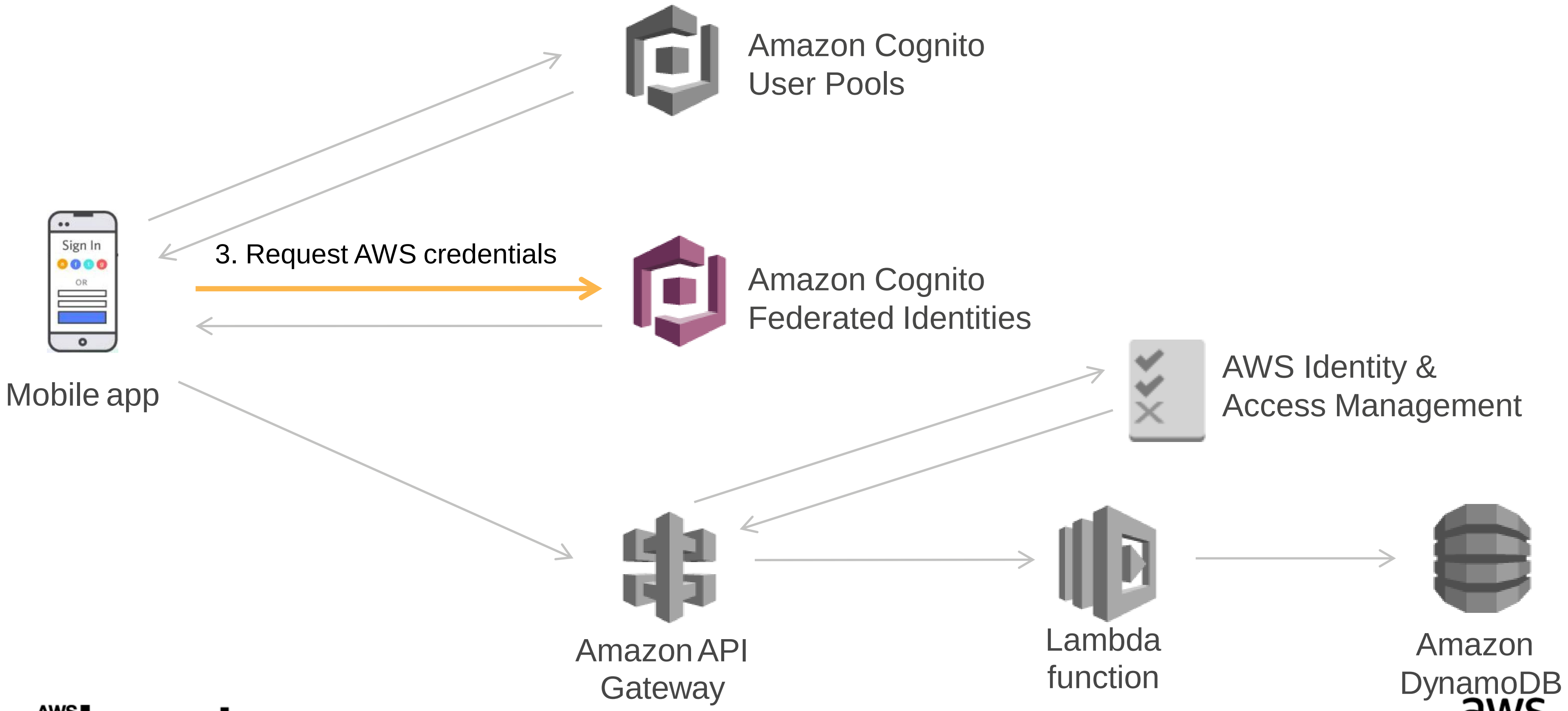
AWS re:Invent

aws

IAM-based authorization


Amazon Cognito User Pools
2. JWT tokens
Sign In
OR
Mobile app
Amazon Cognito Federated Identities
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

IAM-based authorization



Amazon Cognito User Pools

3. Request AWS credentials

Amazon Cognito Federated Identities

Mobile app

AWS Identity & Access Management

Amazon API Gateway

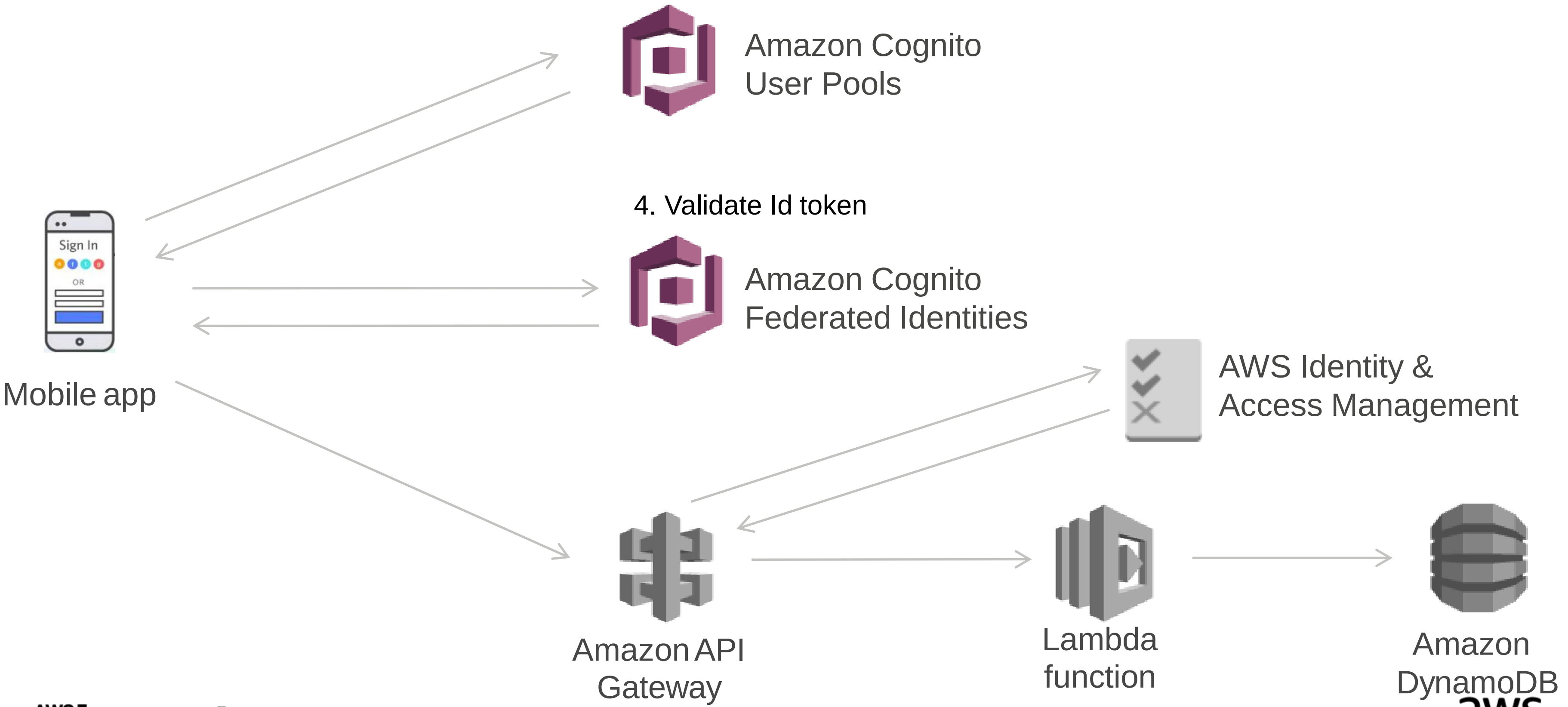
Lambda function

Amazon DynamoDB

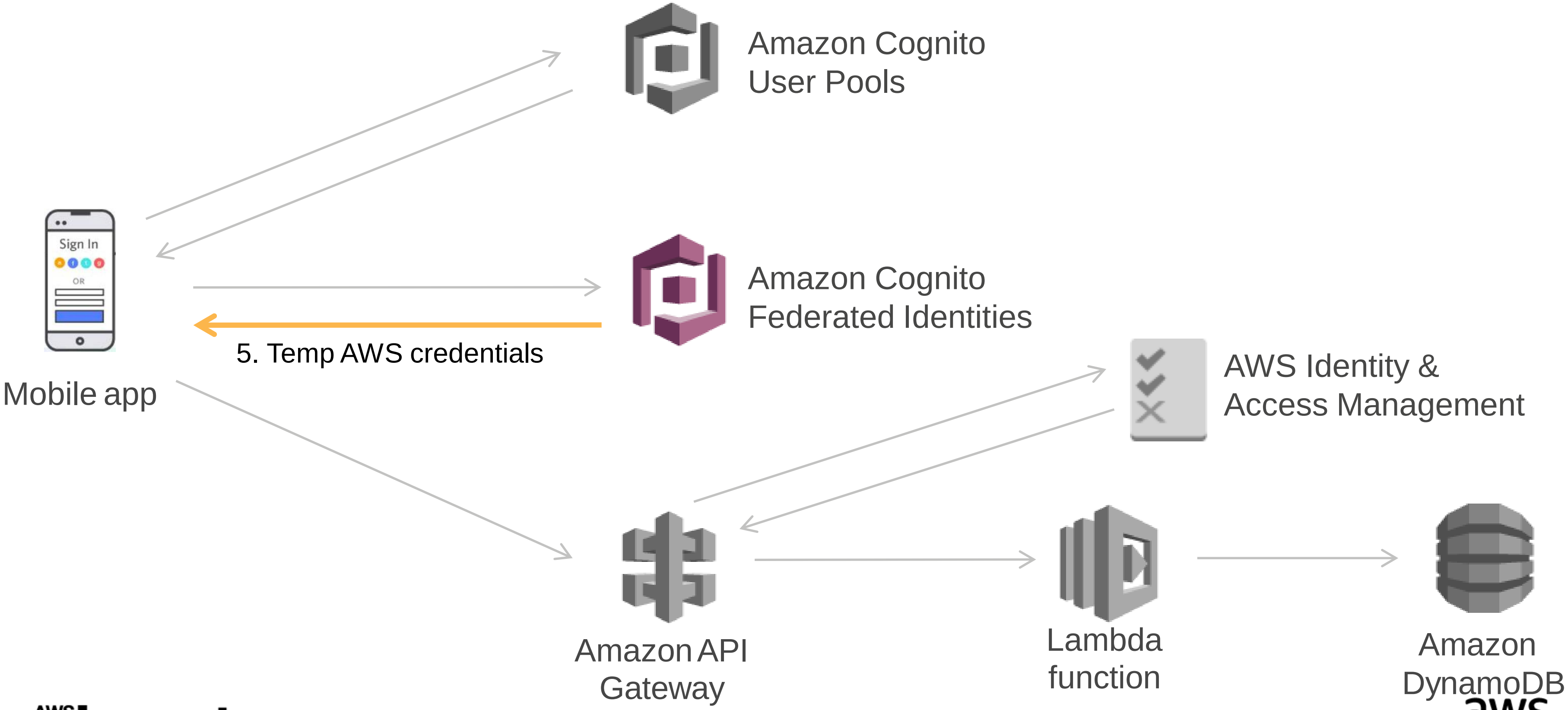
AWS re:Invent

aws

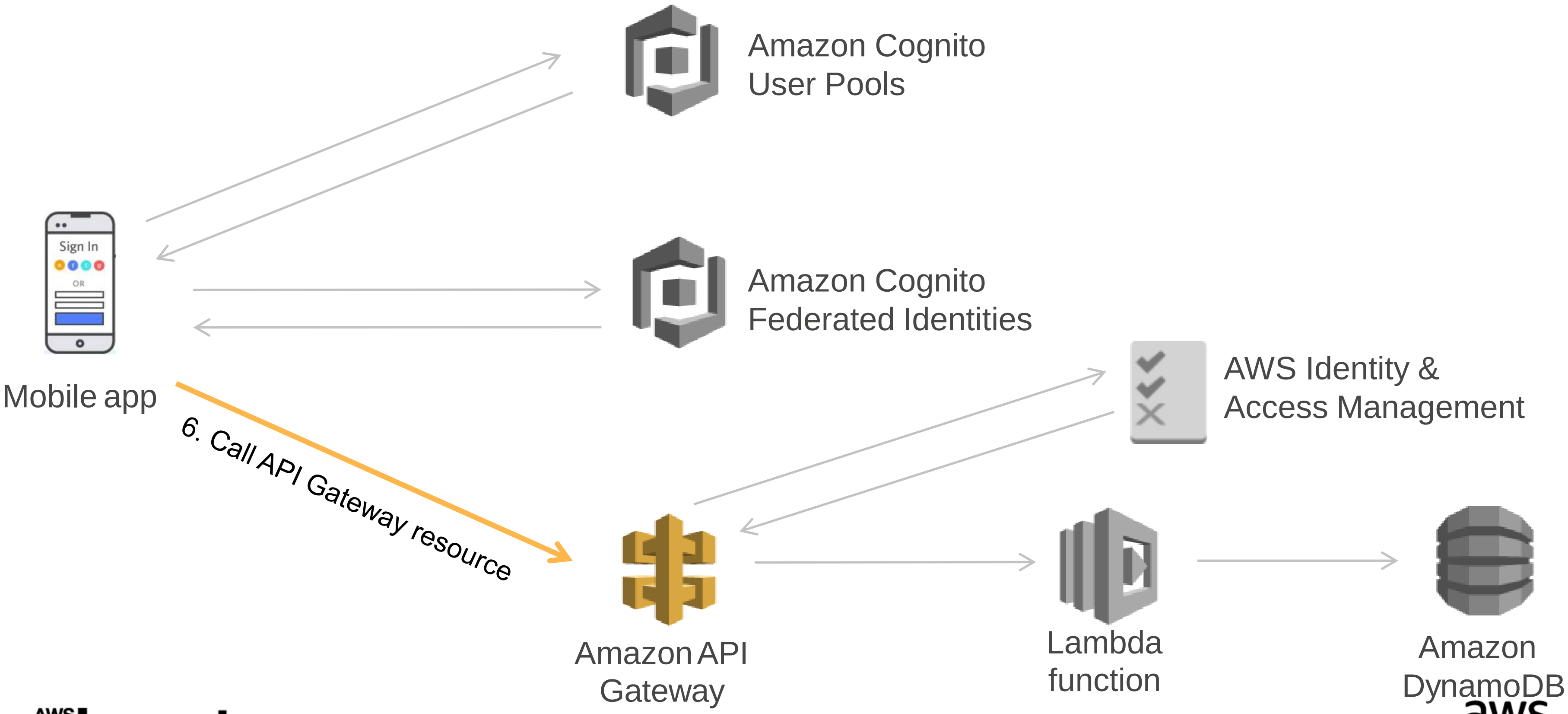
IAM-based authorization



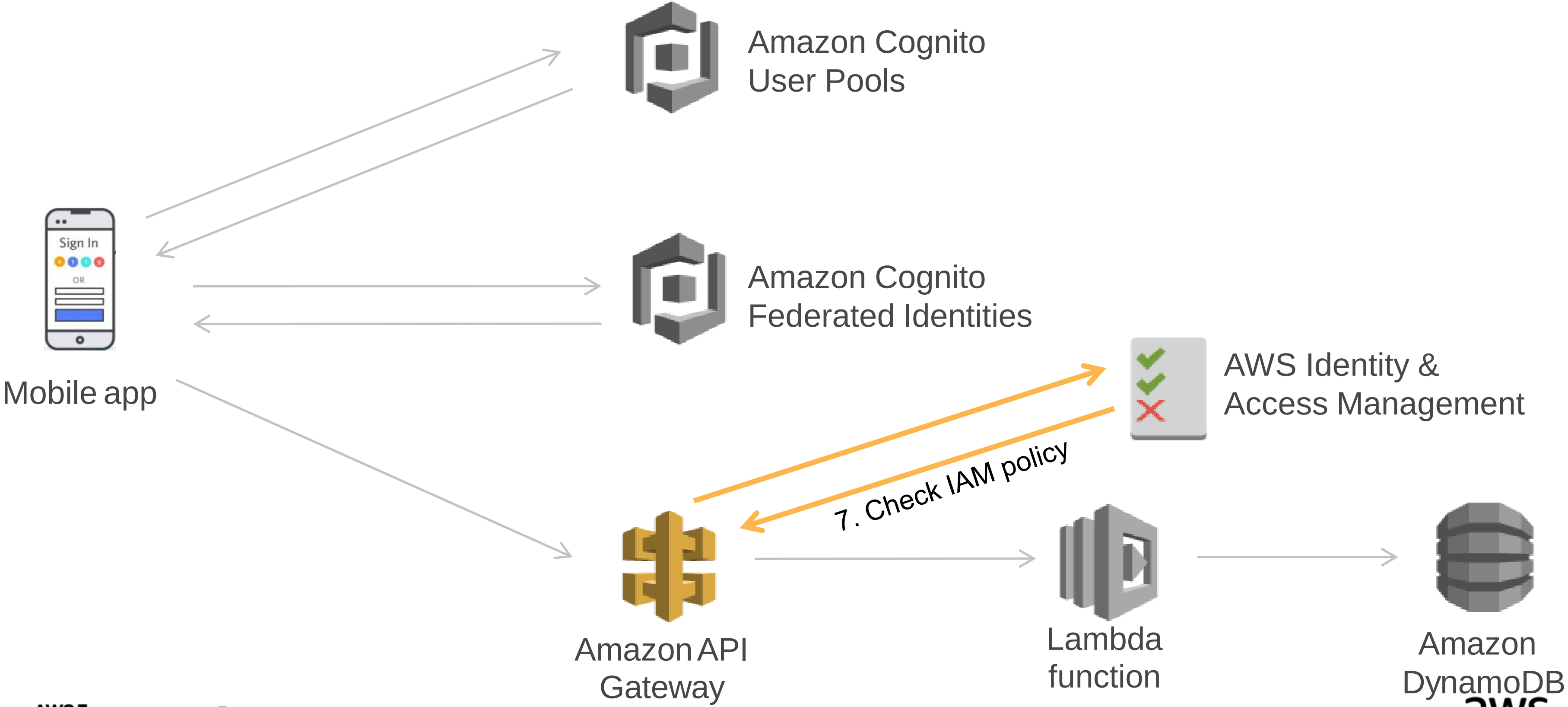
IAM-based authorization


Amazon Cognito User Pools
Sign In
OR
Mobile app
Amazon Cognito Federated Identities
5. Temp AWS credentials
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

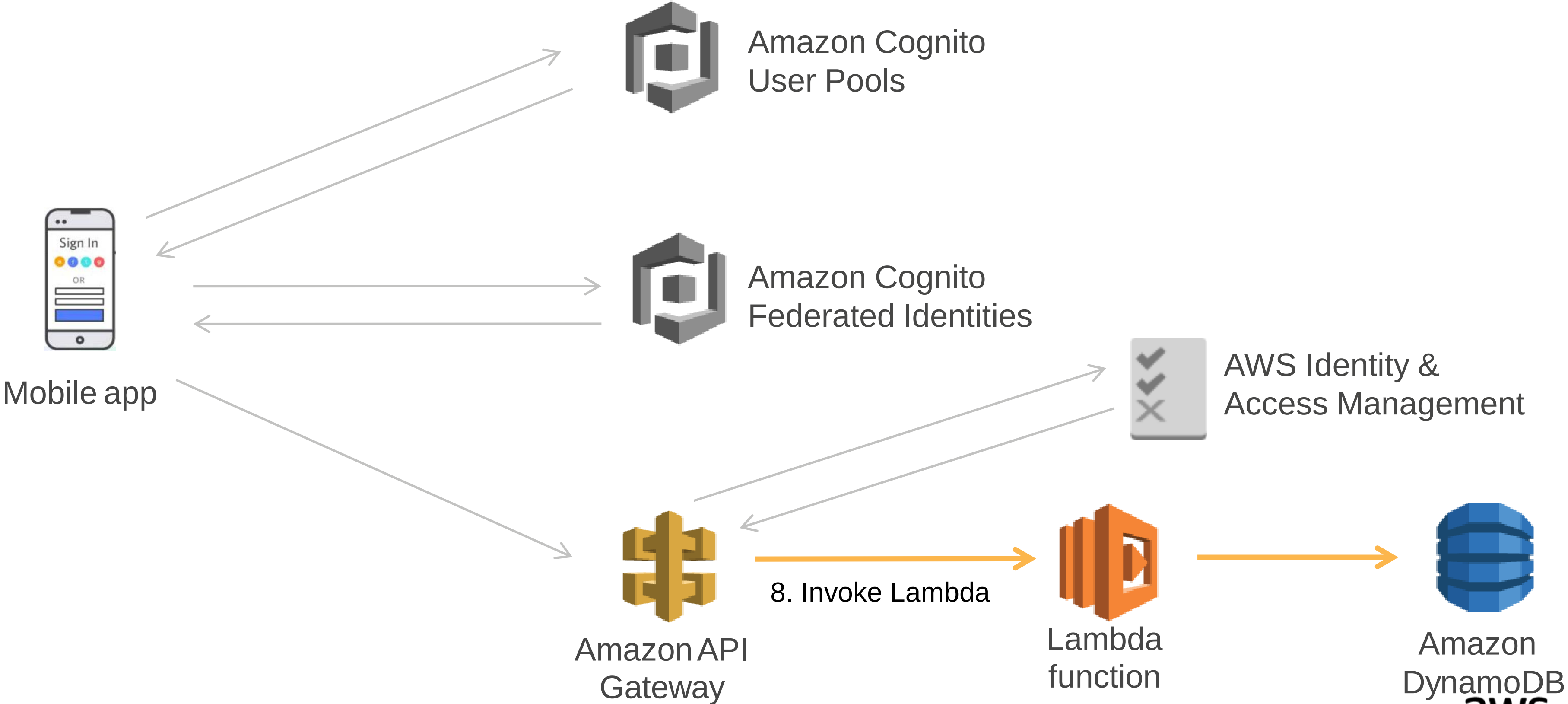
IAM-based authorization


Amazon Cognito User Pools
Sign In
OR
Mobile app
Amazon Cognito Federated Identities
AWS Identity & Access Management
6. Call API Gateway resource
Amazon API Gateway
Lambda function
Amazon DynamoDB

IAM-based authorization



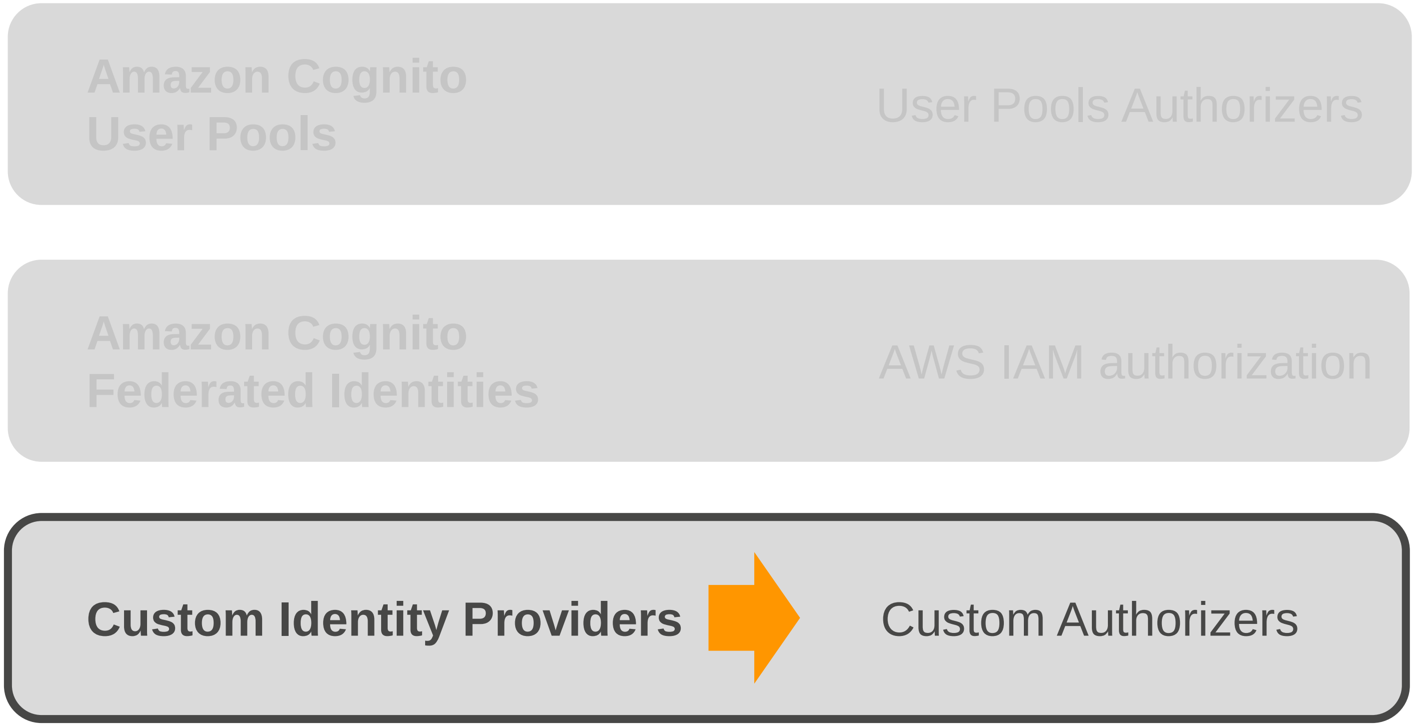
IAM-based authorization



IAM Policy Detail

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "execute-api:Invoke",
            "Effect": ”Allow",
            "Resource": "arn:aws:execute-api:*:*:ff5h9tpwfh/*"
        },
        {
            "Action": "execute-api:Invoke",
            "Effect": "Deny",
            "Resource": "arn:aws:execute-api:*:*:ff5h9tpwfh/*/POST/locations/*"
        }
    ]
}
```

API Gateway: three types of authorization



Amazon Cognito User Pools

User Pools Authorizers

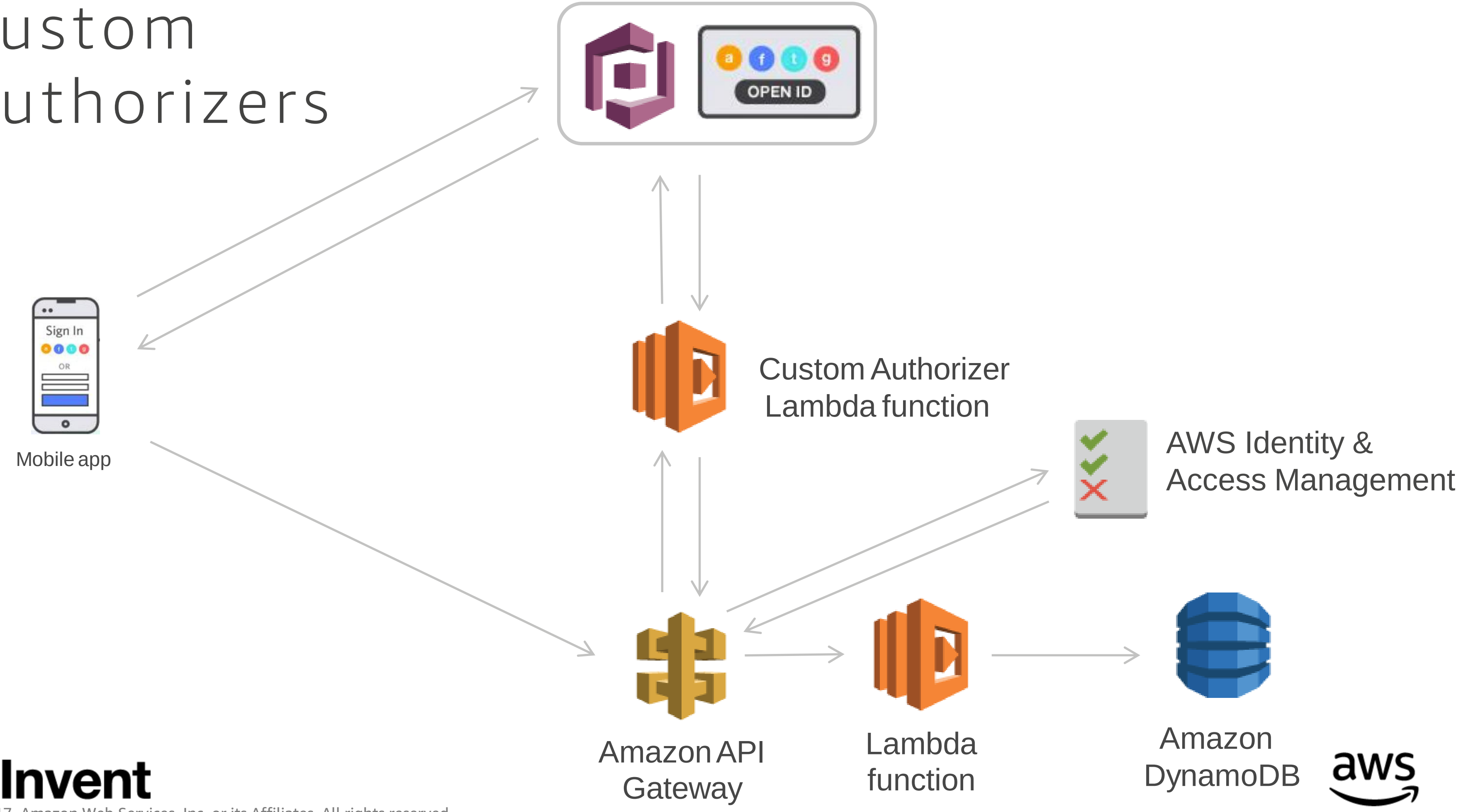
Amazon Cognito Federated Identities

AWS IAM authorization

Custom Identity Providers

Custom Authorizers

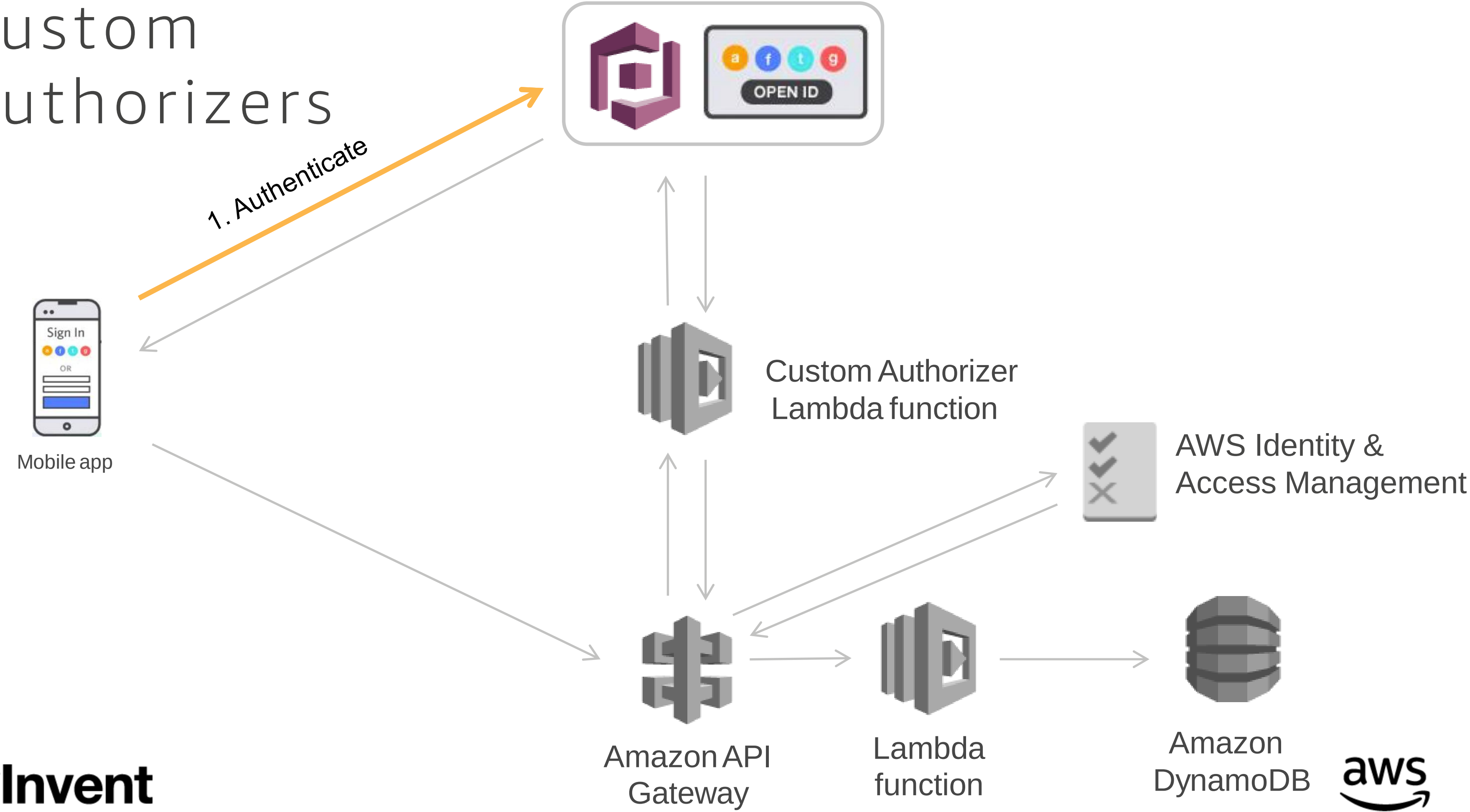
Custom Authorizers



AWS re:Invent

aws

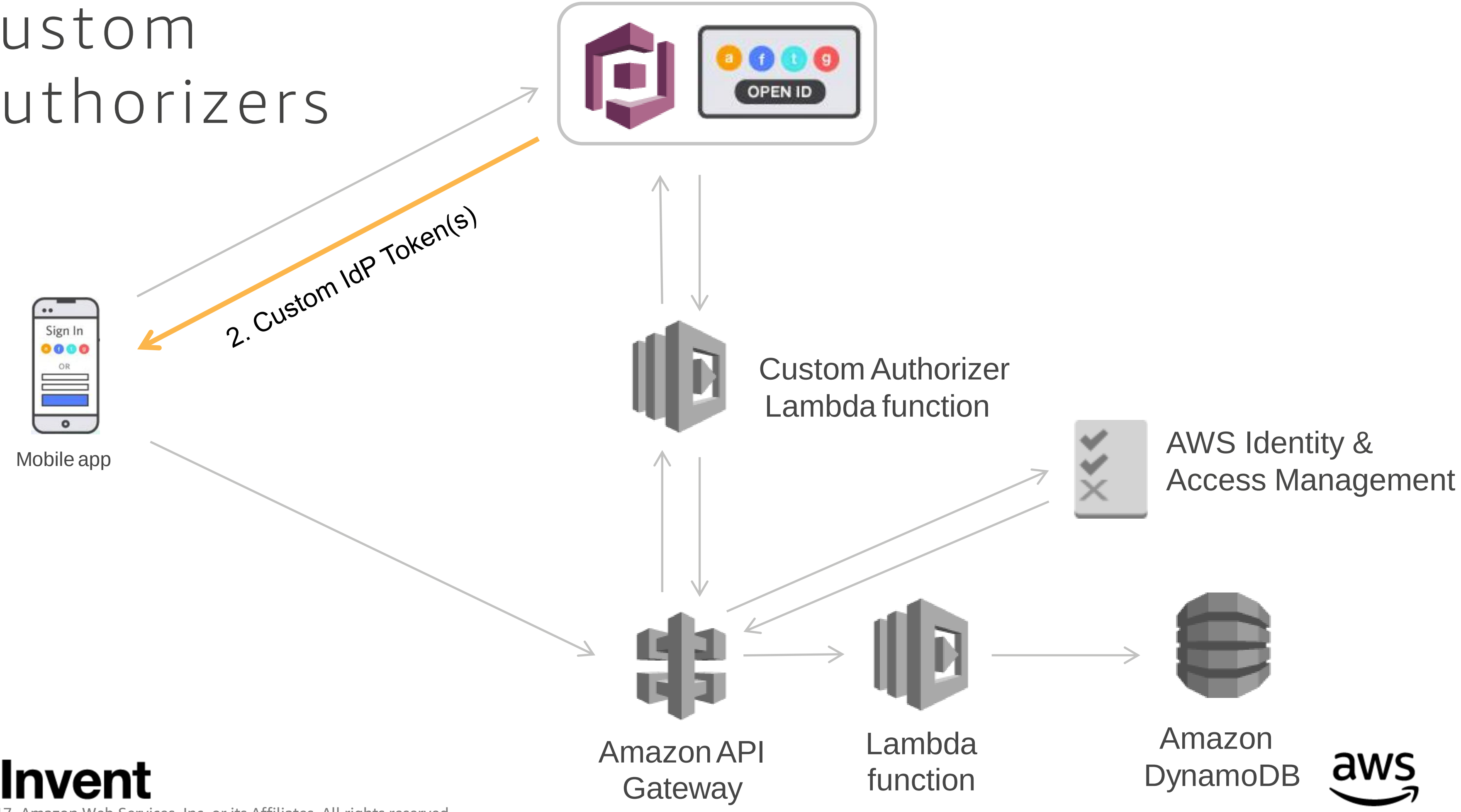
Custom Authorizers



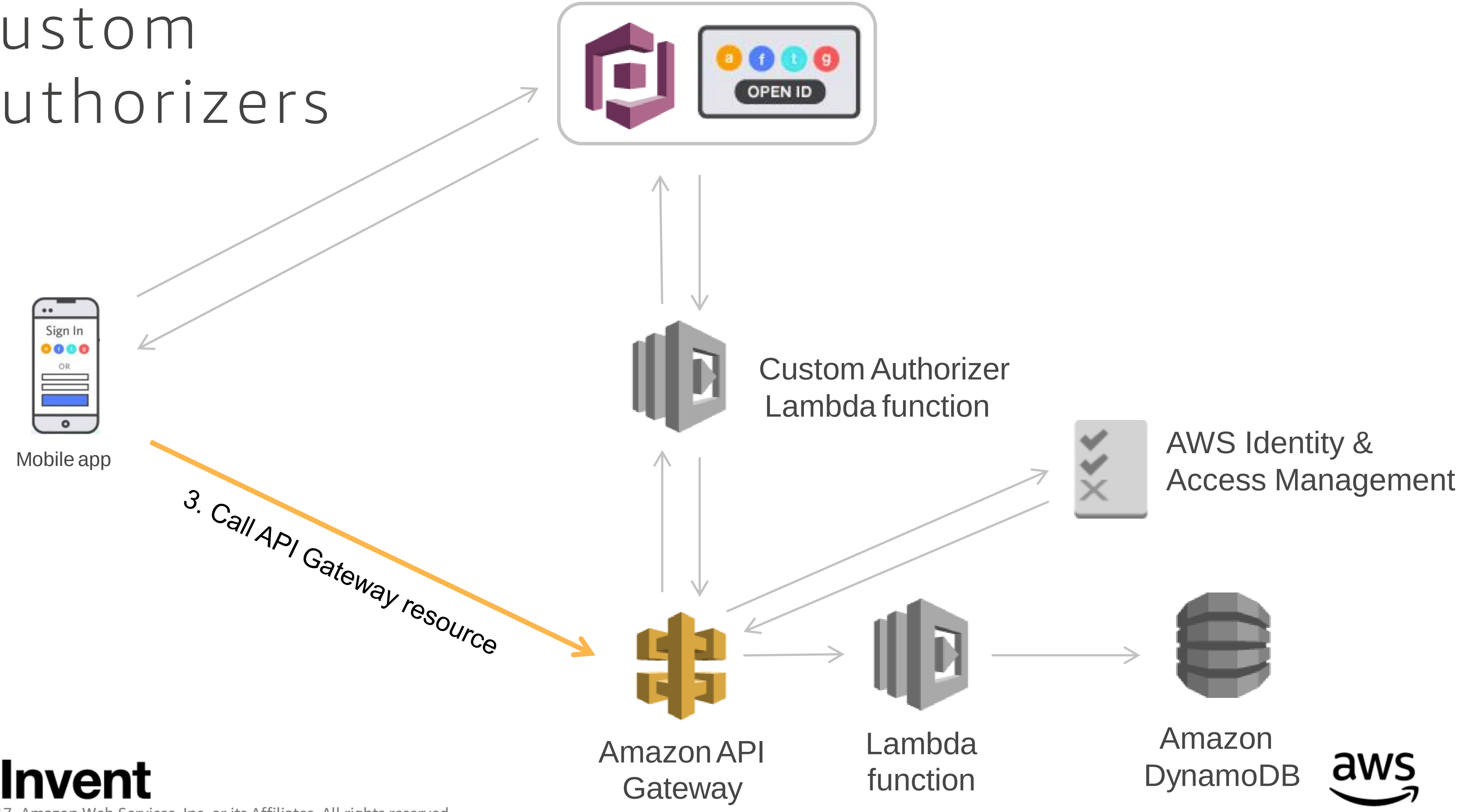
AWS re:Invent

aws

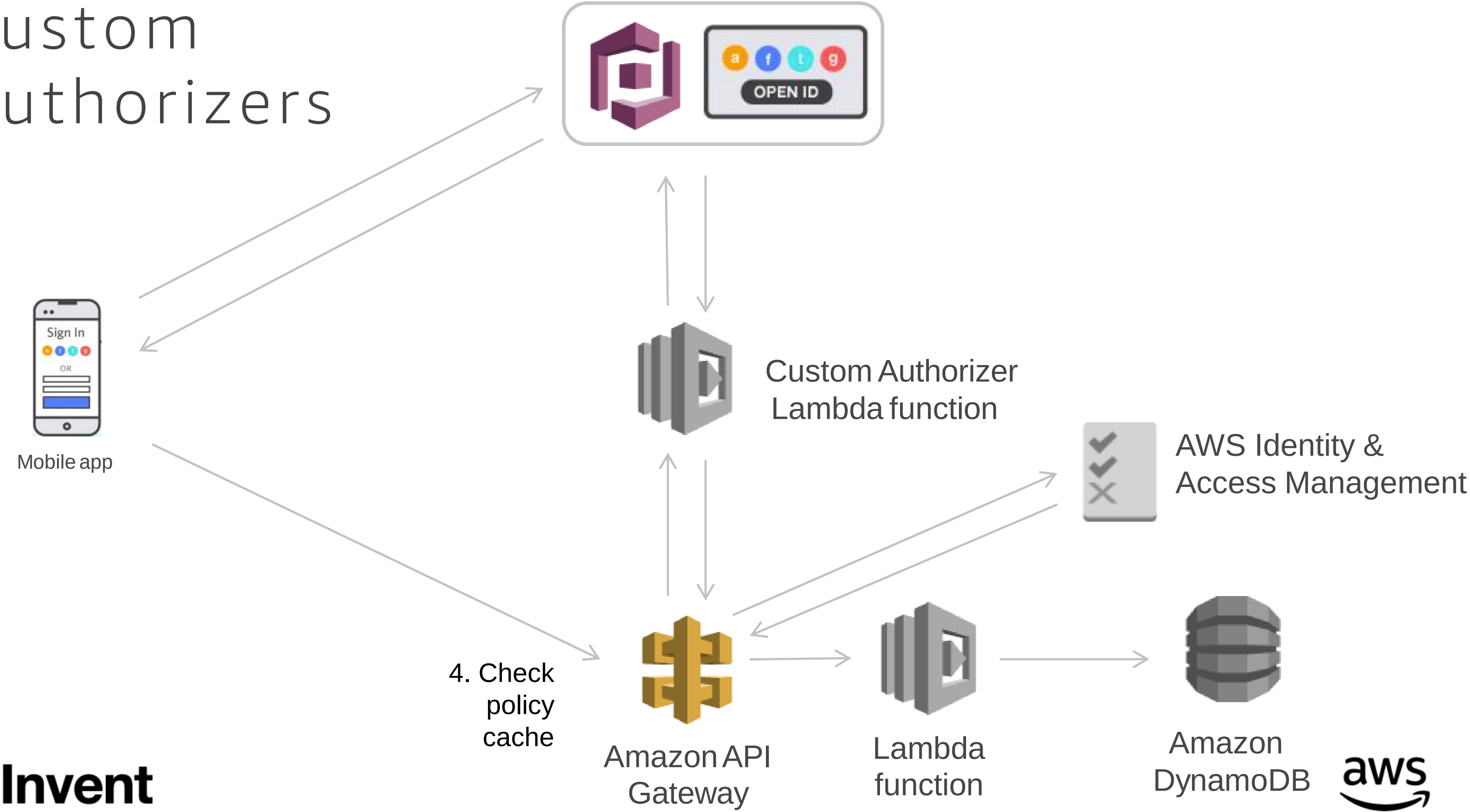
Custom Authorizers



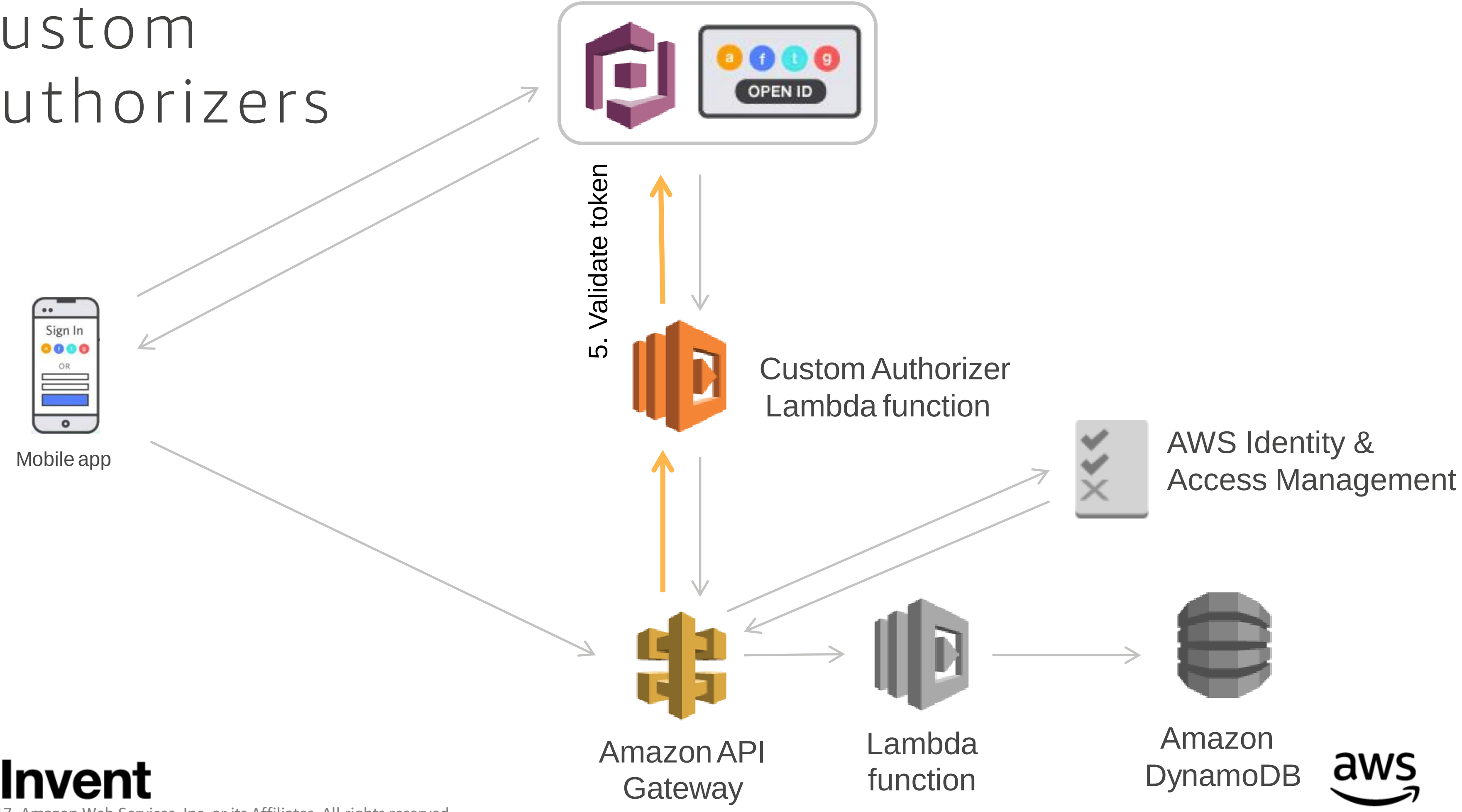
Custom Authorizers


OPEN ID
Sign In
OR
Mobile app
3. Call API Gateway resource
Custom Authorizer Lambda function
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

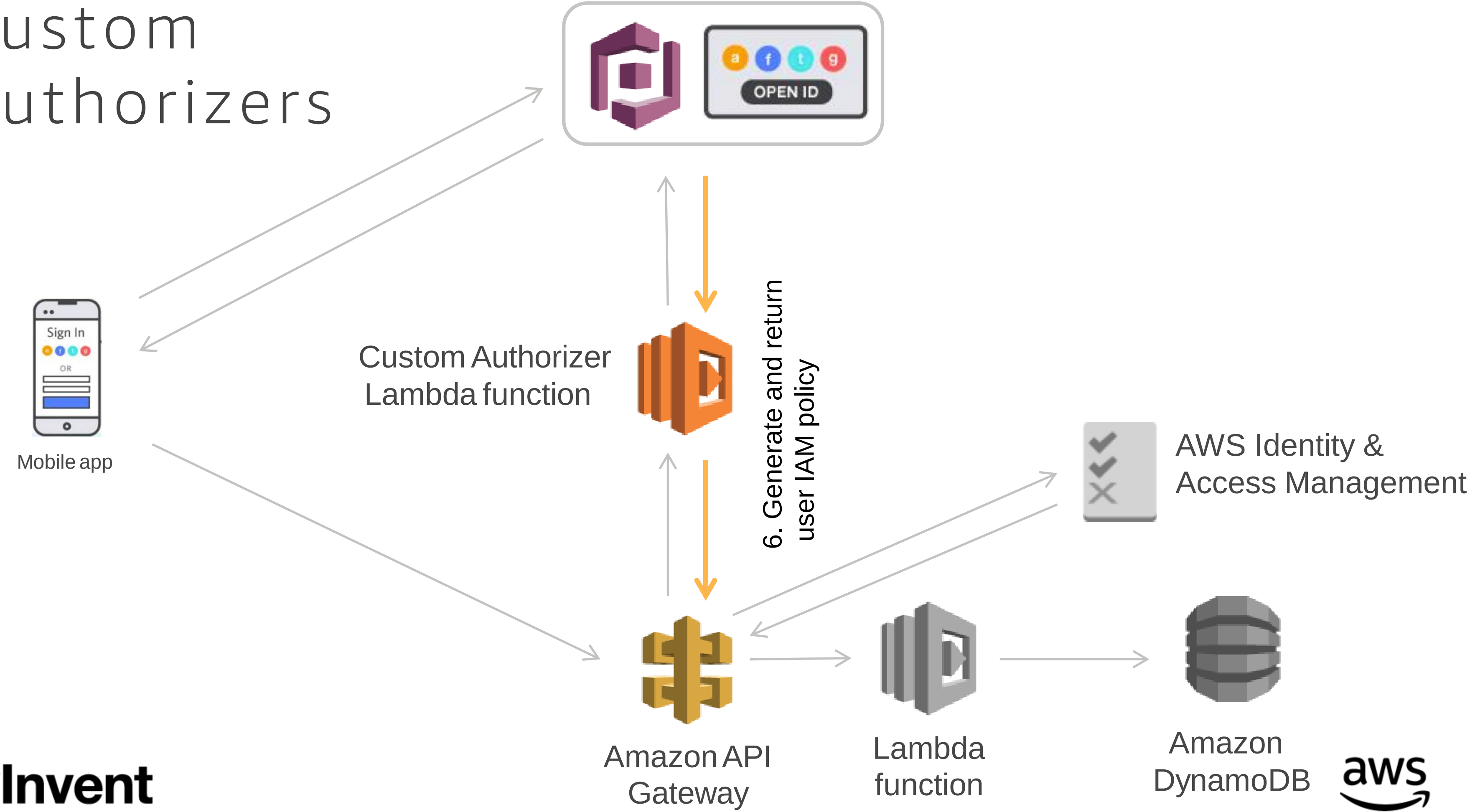
Custom Authorizers



Custom Authorizers

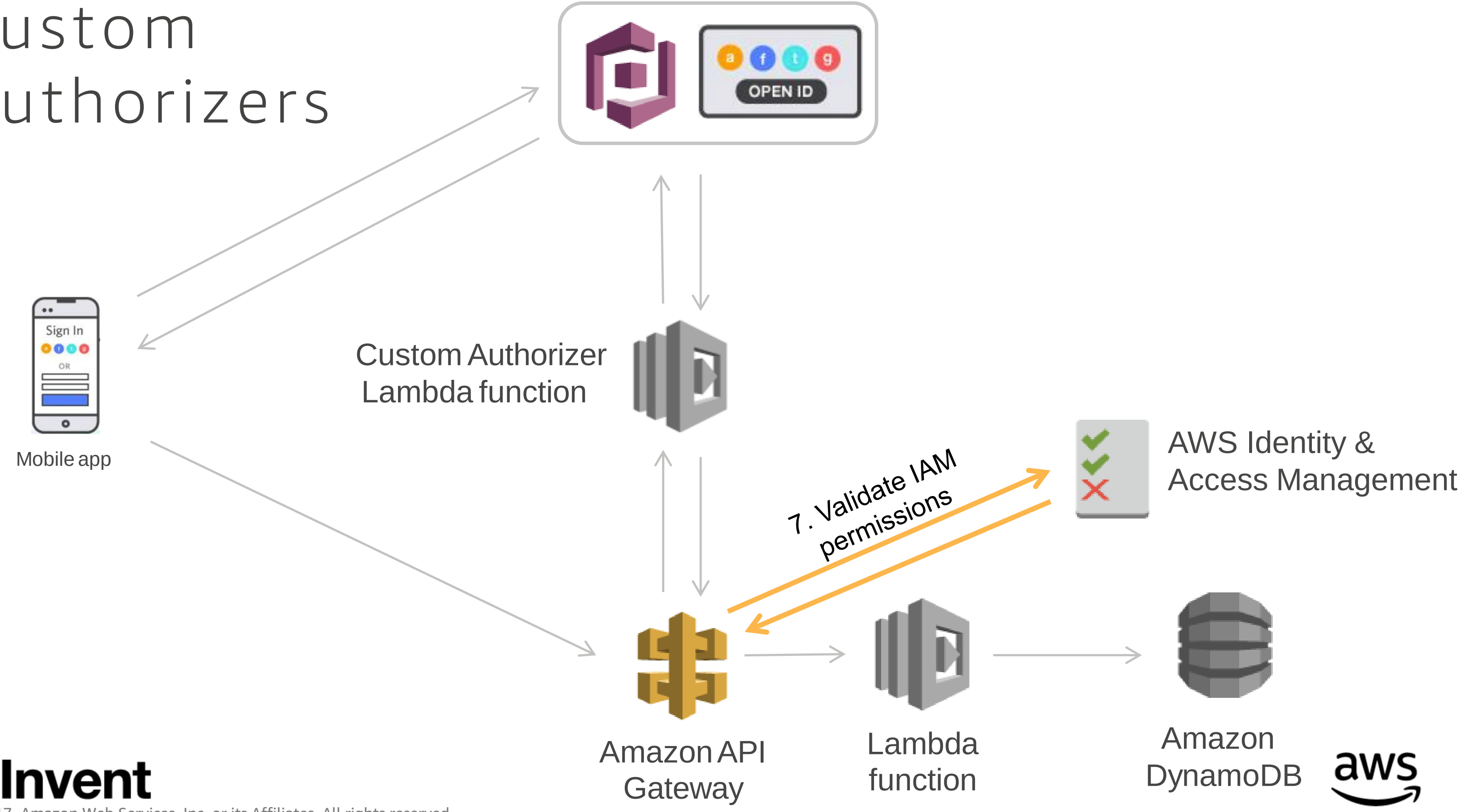


Custom Authorizers


a f t g
OPEN ID
Sign In
OR
Mobile app
Custom Authorizer Lambda function
6. Generate and return user IAM policy
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

AWS re:Invent

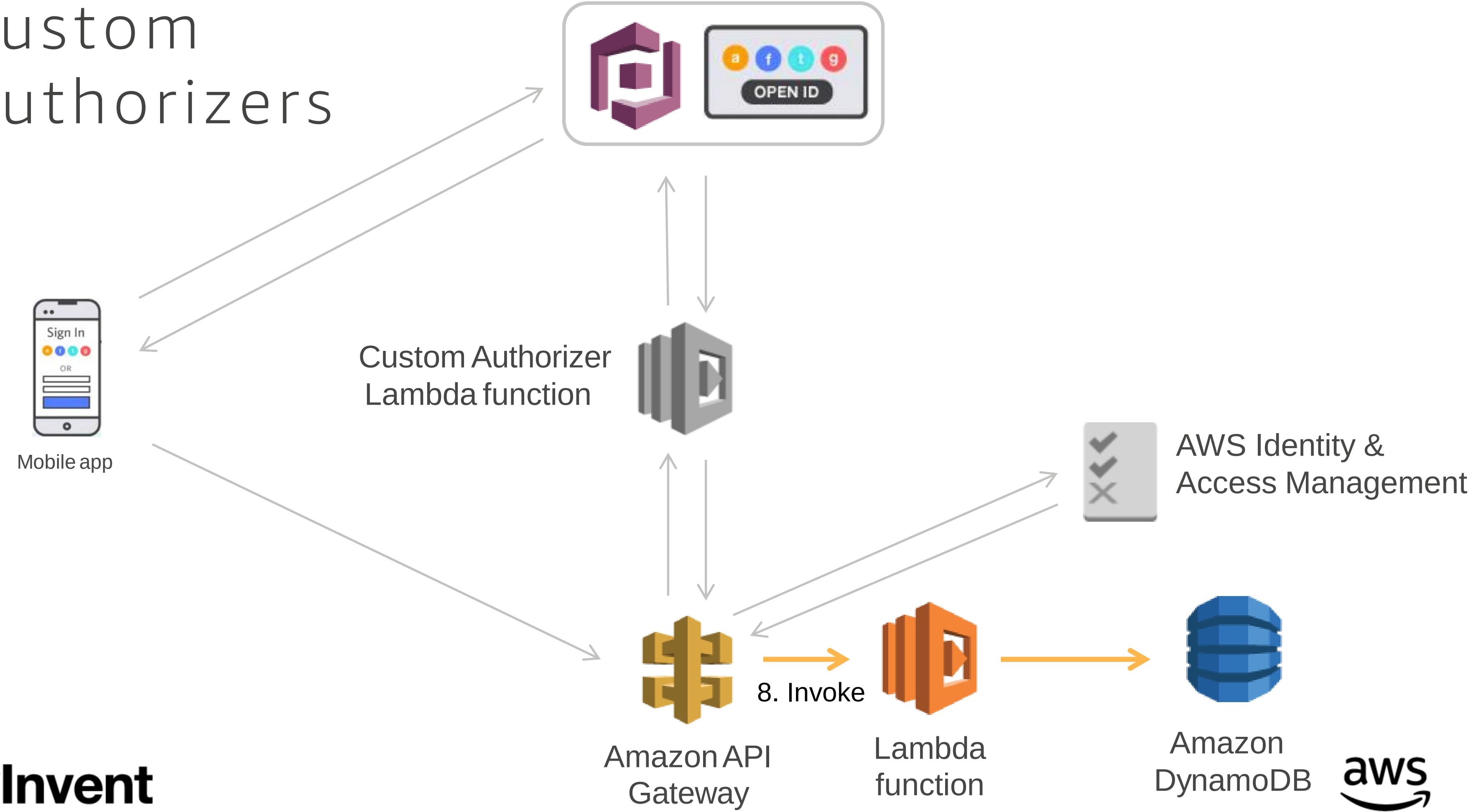
Custom Authorizers



a f t g
OPEN ID
Sign In
OR
Mobile app
Custom Authorizer Lambda function
7. Validate IAM permissions
AWS Identity & Access Management
Amazon API Gateway
Lambda function
Amazon DynamoDB

AWS re:Invent

Custom Authorizers



Custom Authorizer Lambda function

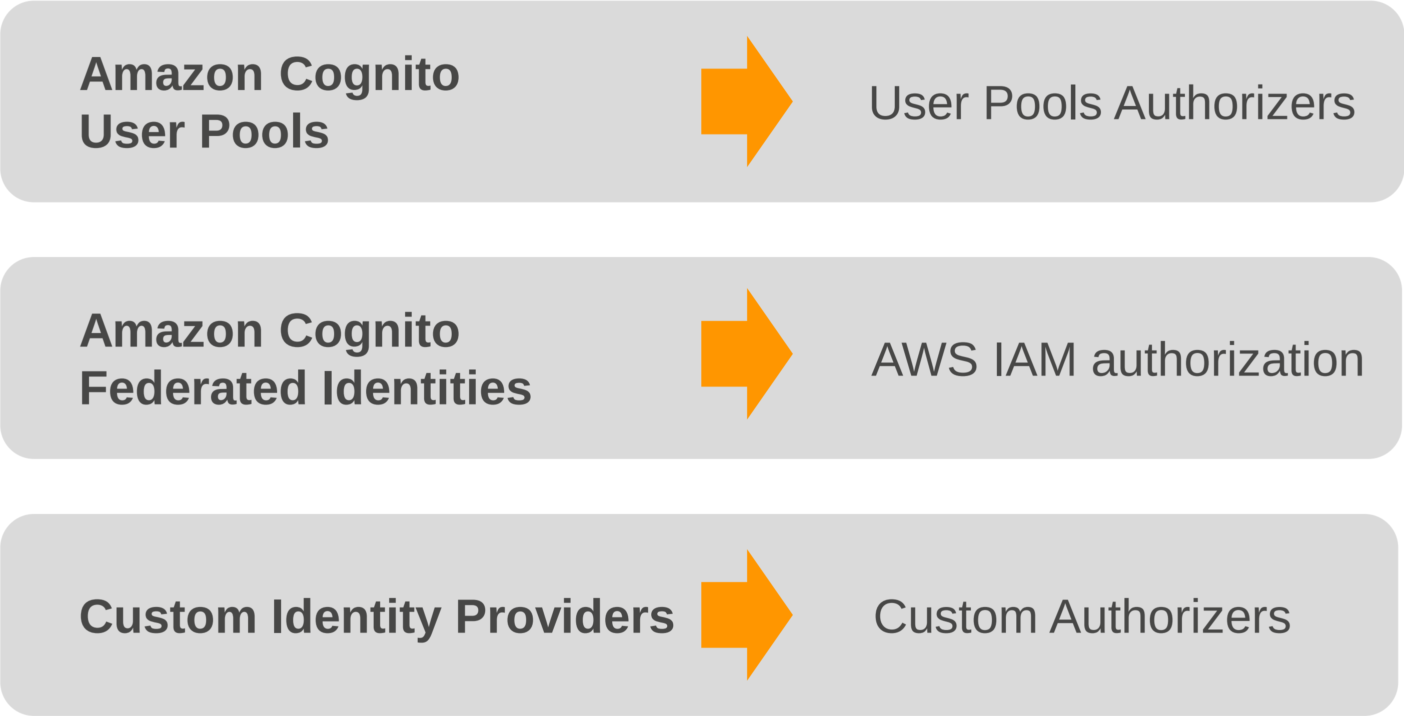
Sample Code

```
var testPolicy = new AuthPolicy(”userIdentifier", "XXXXXXXXXXXX", apiOptions);

testPolicy.allowMethod(AuthPolicy.HttpVerb.POST,   "/locations/*");
testPolicy.allowMethod(AuthPolicy.HttpVerb.DELETE, "/locations/*");

callback(null, testPolicy.getPolicy());
```

API Gateway: three types of authorization



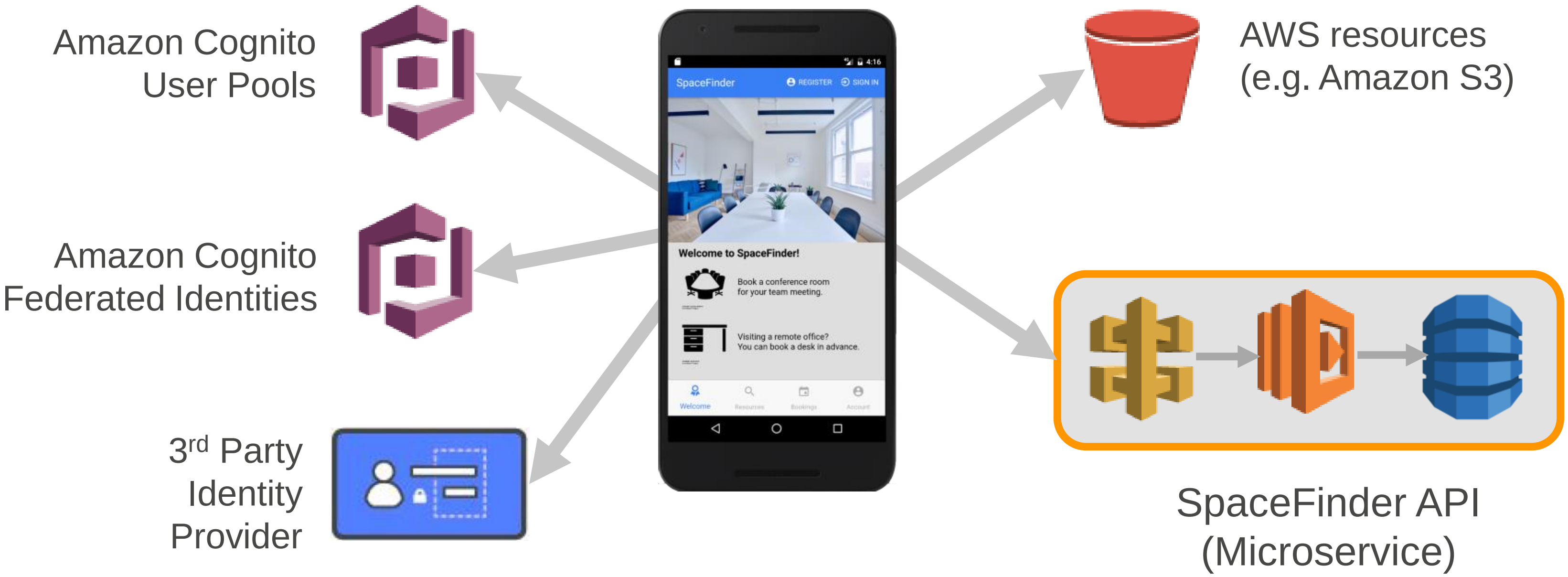
Amazon Cognito User Pools → User Pools Authorizers

Amazon Cognito Federated Identities → AWS IAM authorization

Custom Identity Providers → Custom Authorizers

DEMO

Architecture so far…



Amazon Cognito User Pools

Amazon Cognito Federated Identities

3rd Party Identity Provider

AWS resources (e.g. Amazon S3)

SpaceFinder API (Microservice)

4:16
SpaceFinder
REGISTER
SIGN IN
Welcome to SpaceFinder!
Book a conference room for your team meeting.
Visiting a remote office? You can book a desk in advance.
Welcome
Resources
Bookings
Account

3rd Party Federation

App Integration and Federation

1

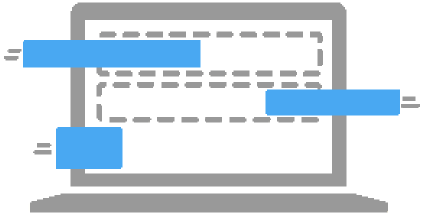
Built-in, Customizable User Interface for Sign up / Sign in

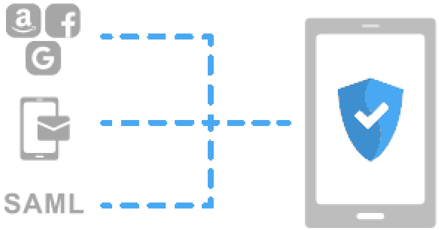
2

Federation with Facebook, Login with Amazon, Google, and SAML2 providers

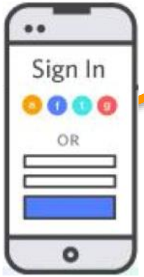
3

OAuth 2.0 Support

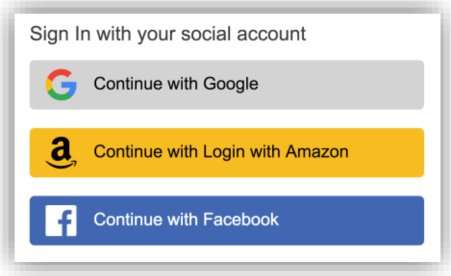




Integrating with Social IdPs



1. Initiate sign-in



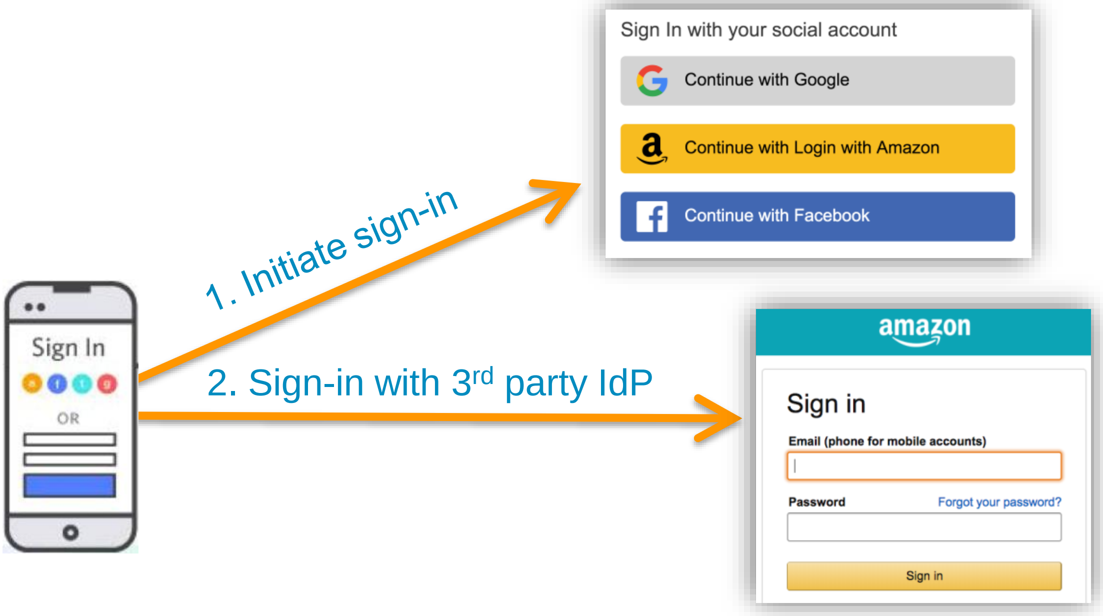
Sign In with your social account

Continue with Google

Continue with Login with Amazon

Continue with Facebook

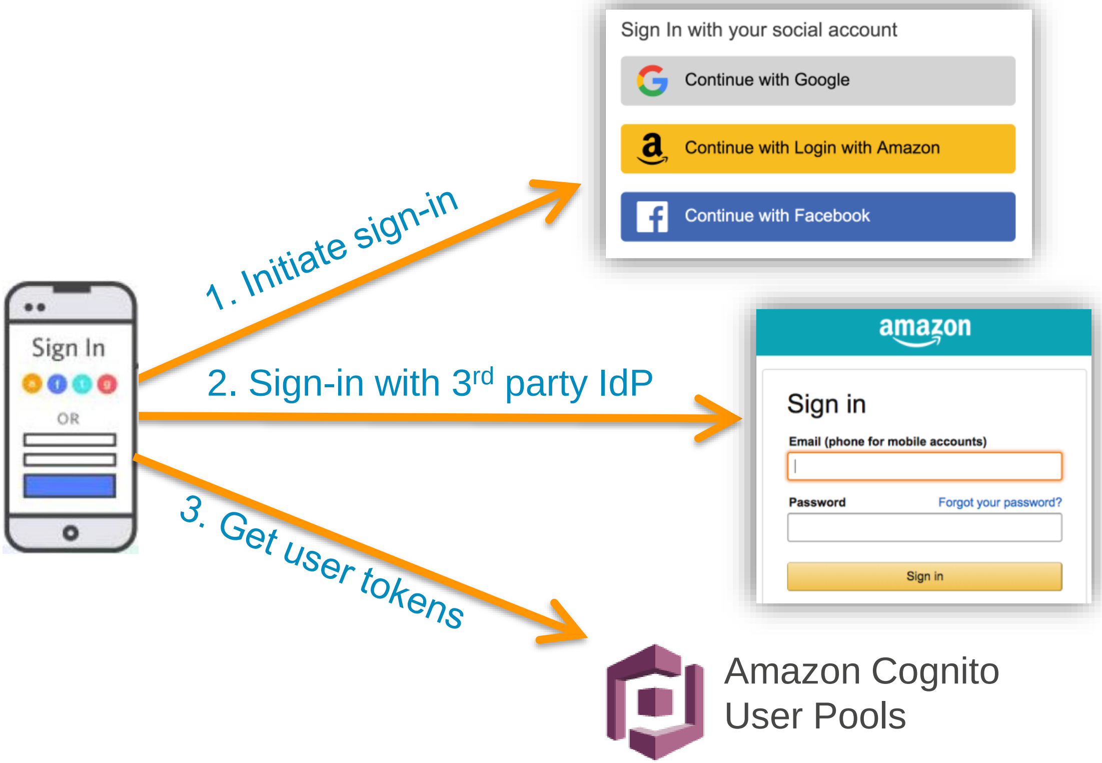
Integrating with Social IdPs



1. Initiate sign-in

2. Sign-in with 3rd party IdP

Integrating with Social IdPs



1. Initiate sign-in

2. Sign-in with 3rd party IdP

3. Get user tokens

Sign In with your social account

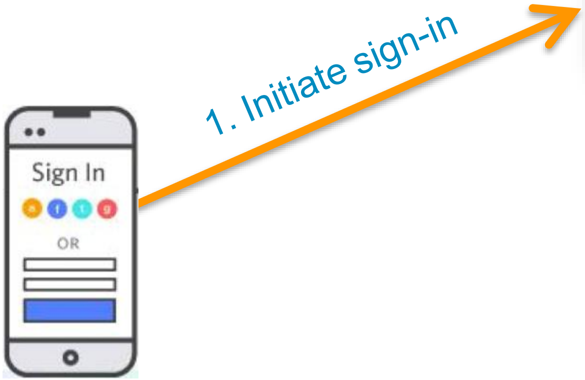
Sign in

Email (phone for mobile accounts)

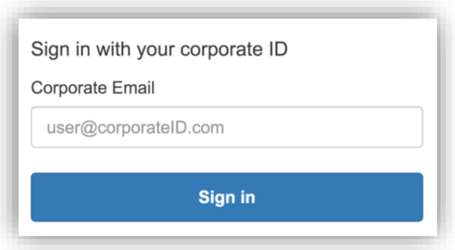
Password

Amazon Cognito User Pools

Integrating with Enterprise IdPs



1. Initiate sign-in

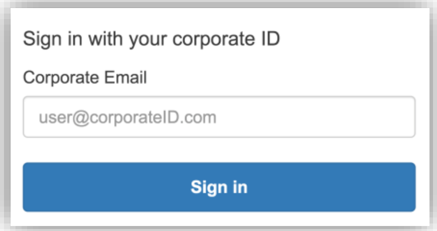


Sign in with your corporate ID

Corporate Email

user@corporateID.com

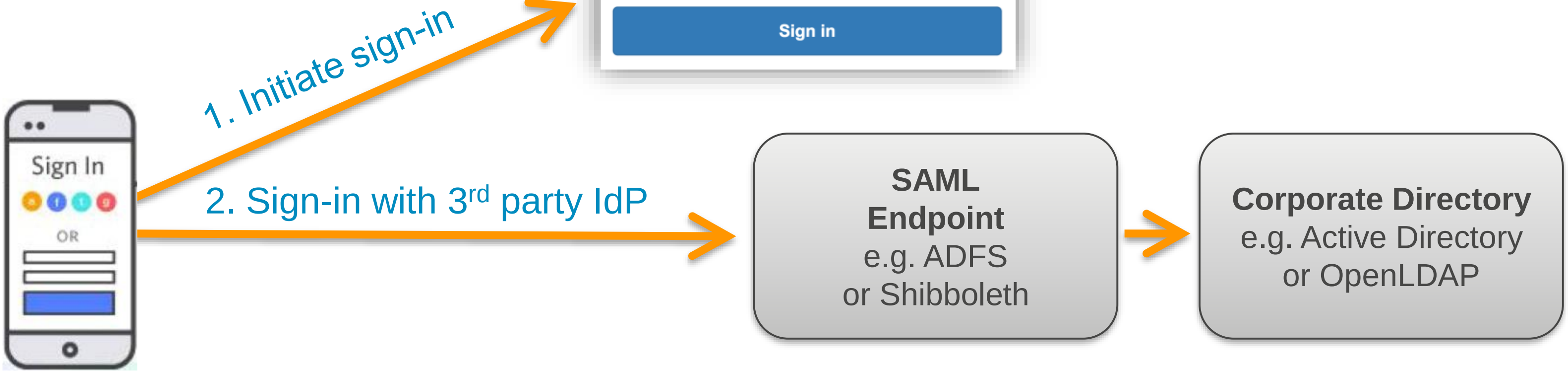
Integrating with Enterprise IdPs



Sign in with your corporate ID

Corporate Email

user@corporateID.com



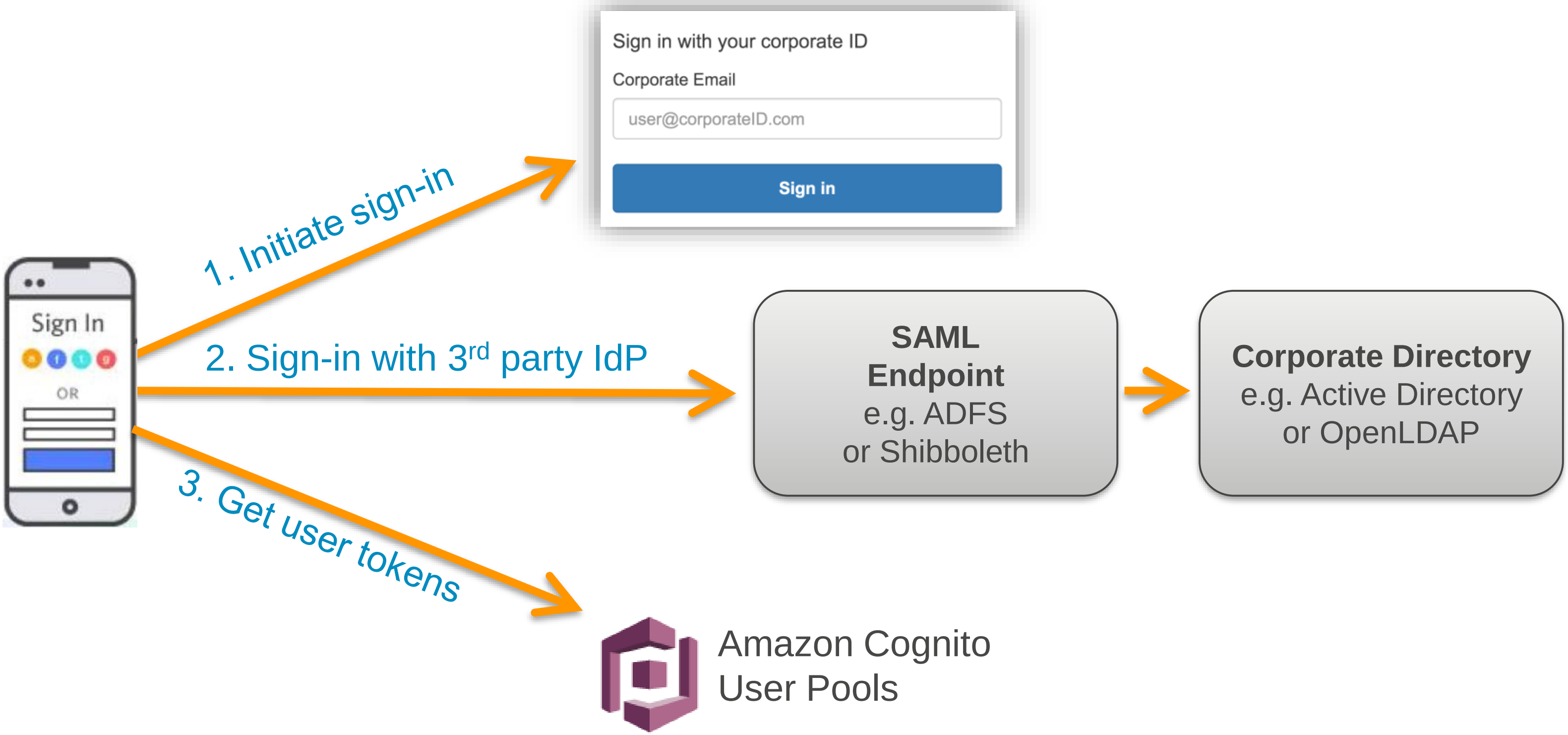
1. Initiate sign-in

2. Sign-in with 3rd party IdP

SAML Endpoint
e.g. ADFS
or Shibboleth

Corporate Directory
e.g. Active Directory
or OpenLDAP

Integrating with Enterprise IdPs



Sign in with your corporate ID

Corporate Email

user@corporateID.com

DEMO

Migrating to Cognito User Pools

Migration approach #1: Bulk import

(1) Create CSV

- Doesn’t contain passwords
- Max 100,000 users at a time

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

```
$ 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
```

AWS re:Invent

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

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

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

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

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

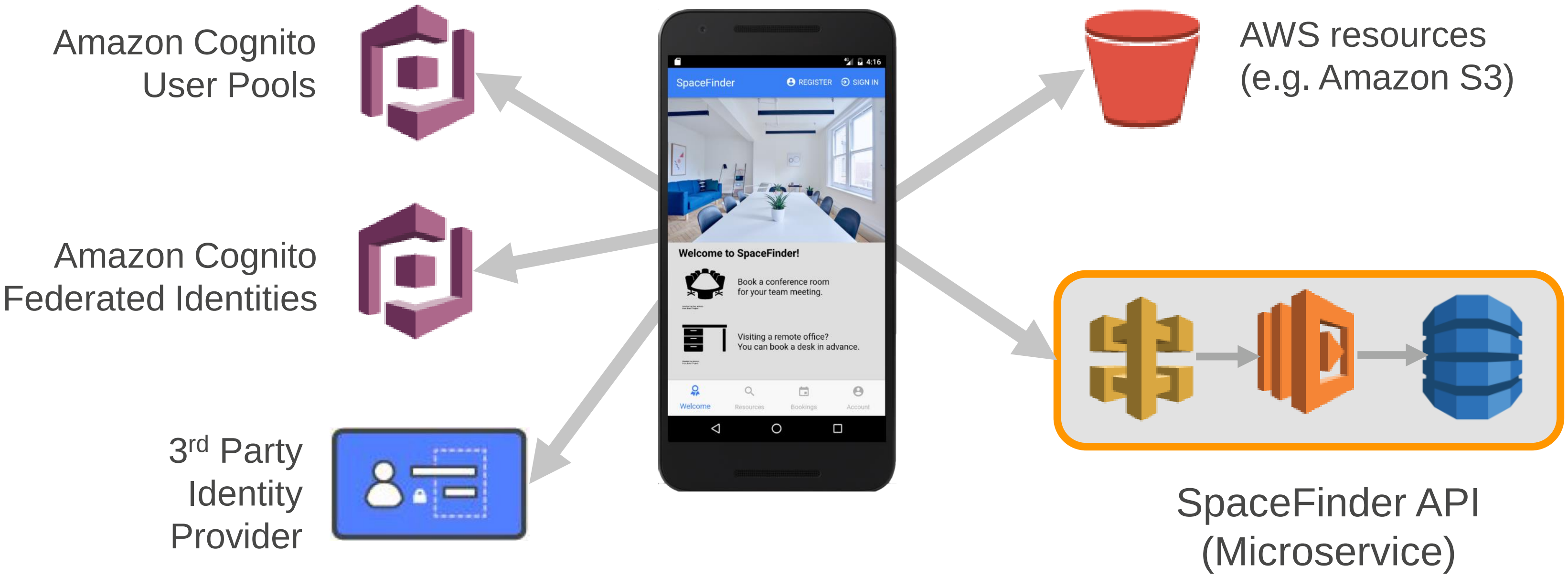
(1) First, try authenticating against Cognito User Pools

(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

Wrap up

SpaceFinder mobile app



Amazon Cognito User Pools

Amazon Cognito Federated Identities

3rd Party Identity Provider

AWS resources (e.g. Amazon S3)

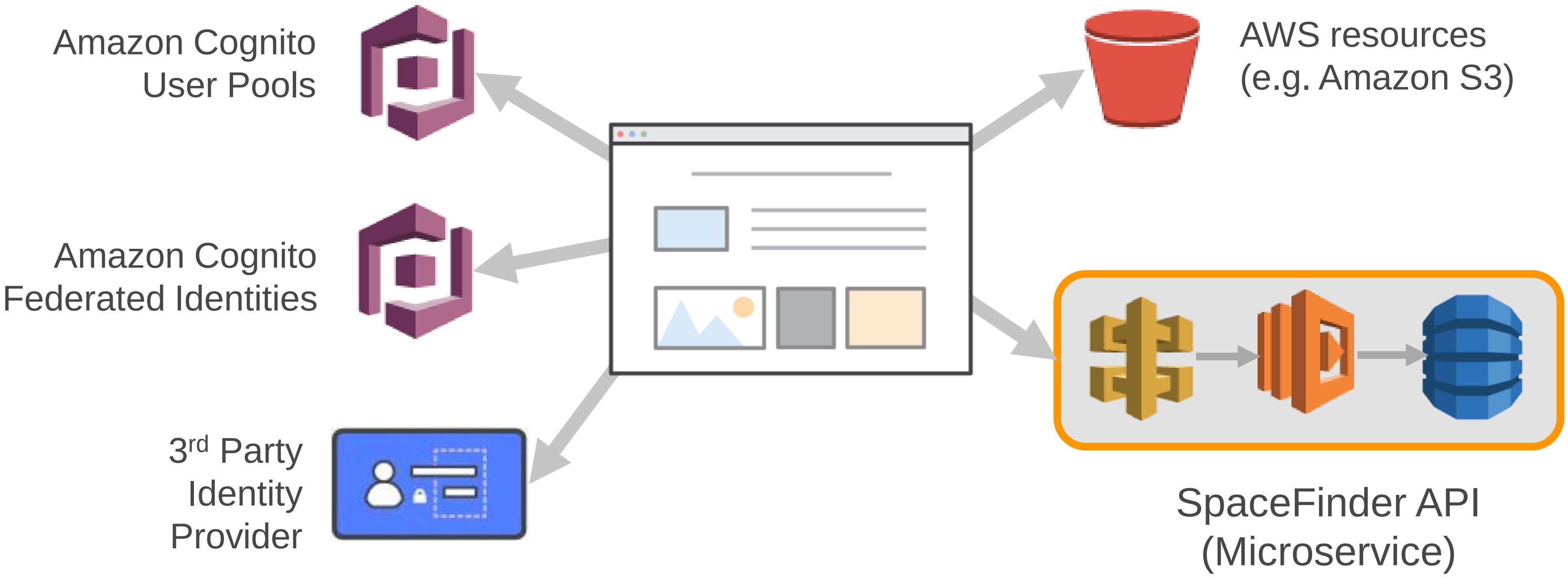
SpaceFinder API (Microservice)

Welcome to SpaceFinder!

Book a conference room for your team meeting.

Visiting a remote office? You can book a desk in advance.

SpaceFinder web app



Amazon Cognito User Pools

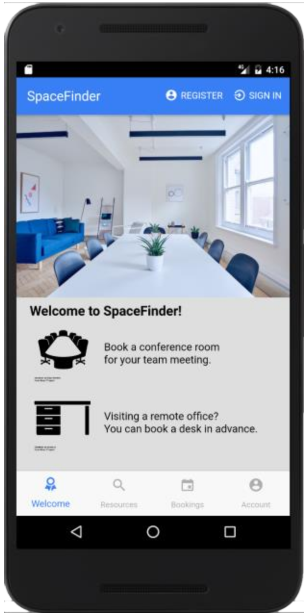
Amazon Cognito Federated Identities

3rd Party Identity Provider

AWS resources (e.g. Amazon S3)

SpaceFinder API (Microservice)

SpaceFinder



Welcome to SpaceFinder!

Book a conference room for your team meeting.

Visiting a remote office? You can book a desk in advance.

Do try this at home

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

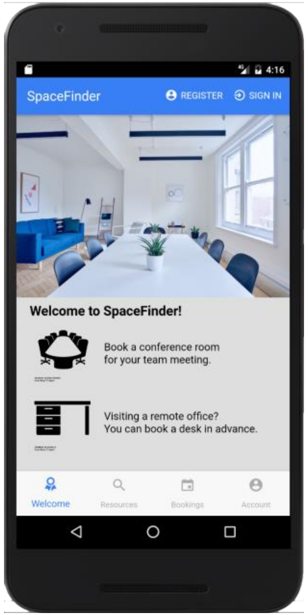
https://github.com/awslabs/aws-serverless-auth-reference-app

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

Remember to complete your evaluations

SpaceFinder



Welcome to SpaceFinder!

Book a conference room
for your team meeting.

Visiting a remote office?
You can book a desk in advance.

Do try this at home

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

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

CLICK TO ADD TEXT

AWS re:Invent

THANK YOU!

CLICK TO ADD TEXT

AWS re:Invent

aws