AWS COGNITO

APPLICATION

AUTHENTICATION

AUTHENTICATION
AND AUTHORIZATION

IDP

SOCIAL
PROVIDERS

AWS
COGNITO

- **Bruno Fuzetti Penso**
- **+ 10 years of experience**
- **Solution Architect @ Grupo Boticário**

https://github.com/brunopenso

https://www.linkedin.com/in/brunopenso/

AUTHENTICATION AND AUTHORIZATION

AUTHENTICATION

- Validate user identity
- Normally has a username – that identify the user
- And some complemente such as Password – that confirms if the user is the user

AUTHORIZATION

- Allow access to specific resources
- Based on the User identity

IDP – Identity Provider

- Authentication service
- Cognito is identity provider
- Normally integrates with external providers like: Facebook, Google
- Federate with Saml and oAuth protocols

SOCIAL and OTHERS PROVIDERS

- External database for Authentication
- Responsable to ensure that the user identitifed is valid
- Generate trust in the use of your system
- Security simplified for your application

COGNITO – WHAT IS?

- Amazon Cognito allows you to handle users, make login and access control for your web and mobile applications faster and easy
- Standards: Oauth 2.0, SAML 2.0 and OpenID Connect.
- Multifactor authentication and cryptography for in traffic data
- Access Resource Control for AWS

COGNITO - PRICE

Level of price definition(MAUs)	Price per MAU
First 50.000	Free
Next 50.000	0,00550 USD
Next 900.000	0,00460 USD
Next 9.000.000	0,00325 USD
More than 10.000.000	0,00250 USD

SAML Authentication = 0,015 USD

MAU = Monthly Active User

Prices from 02/01/2020

COGNITO

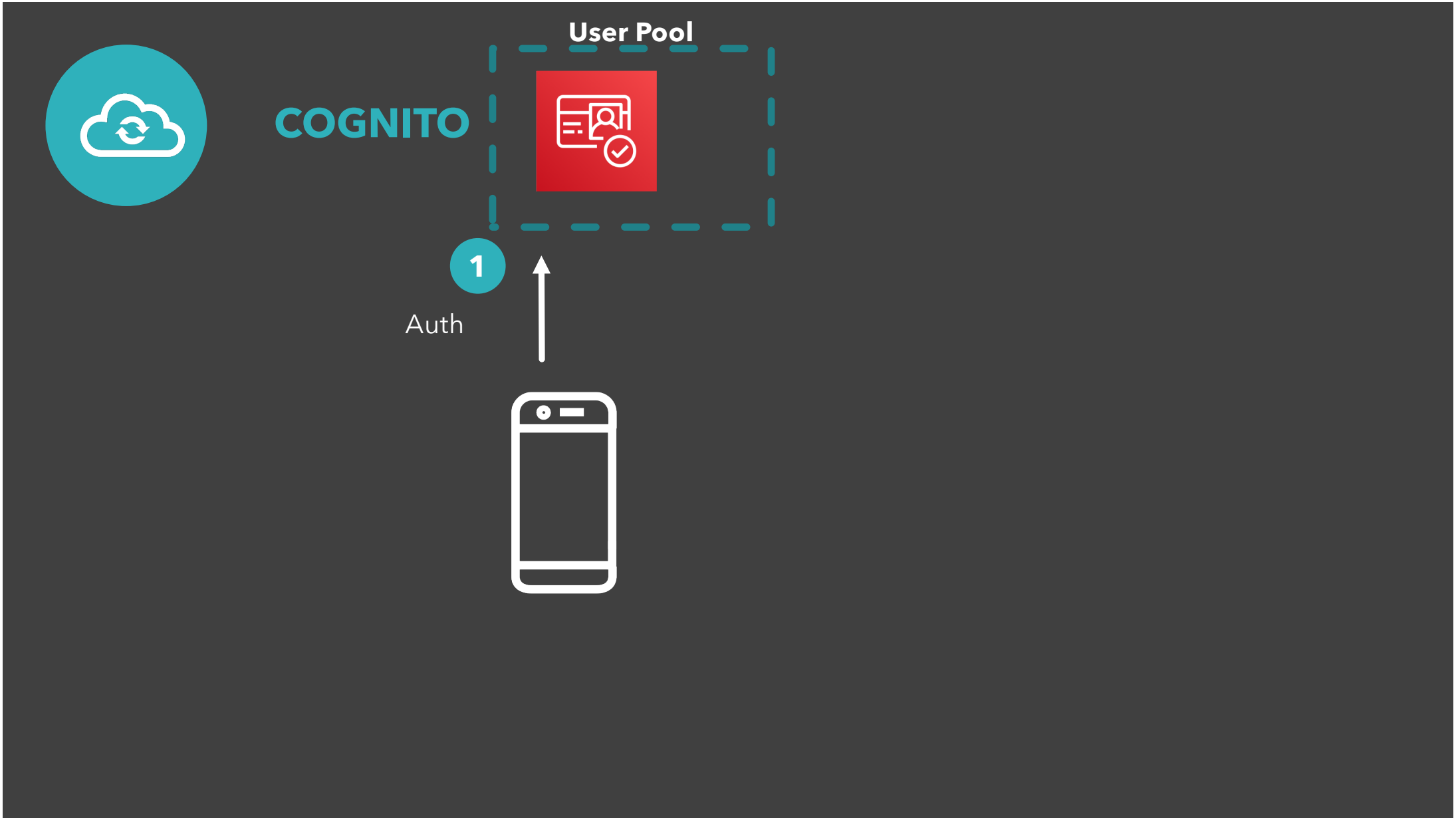
USER POOL

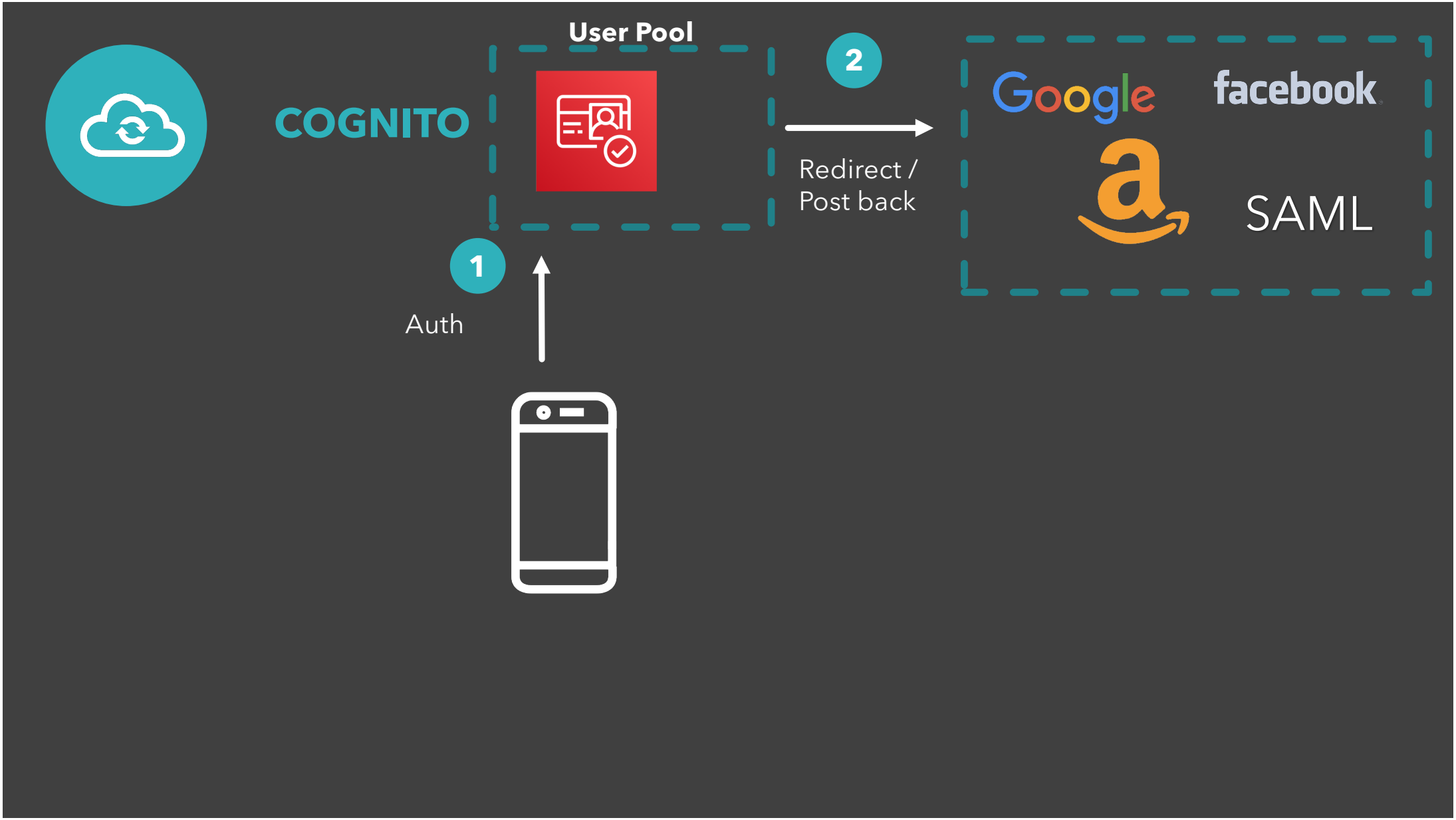
- User directory
- SignUp, signin, signout
- Group Management
- Supply information for authorization
- Is the identity provider
- External Resource Server Integration

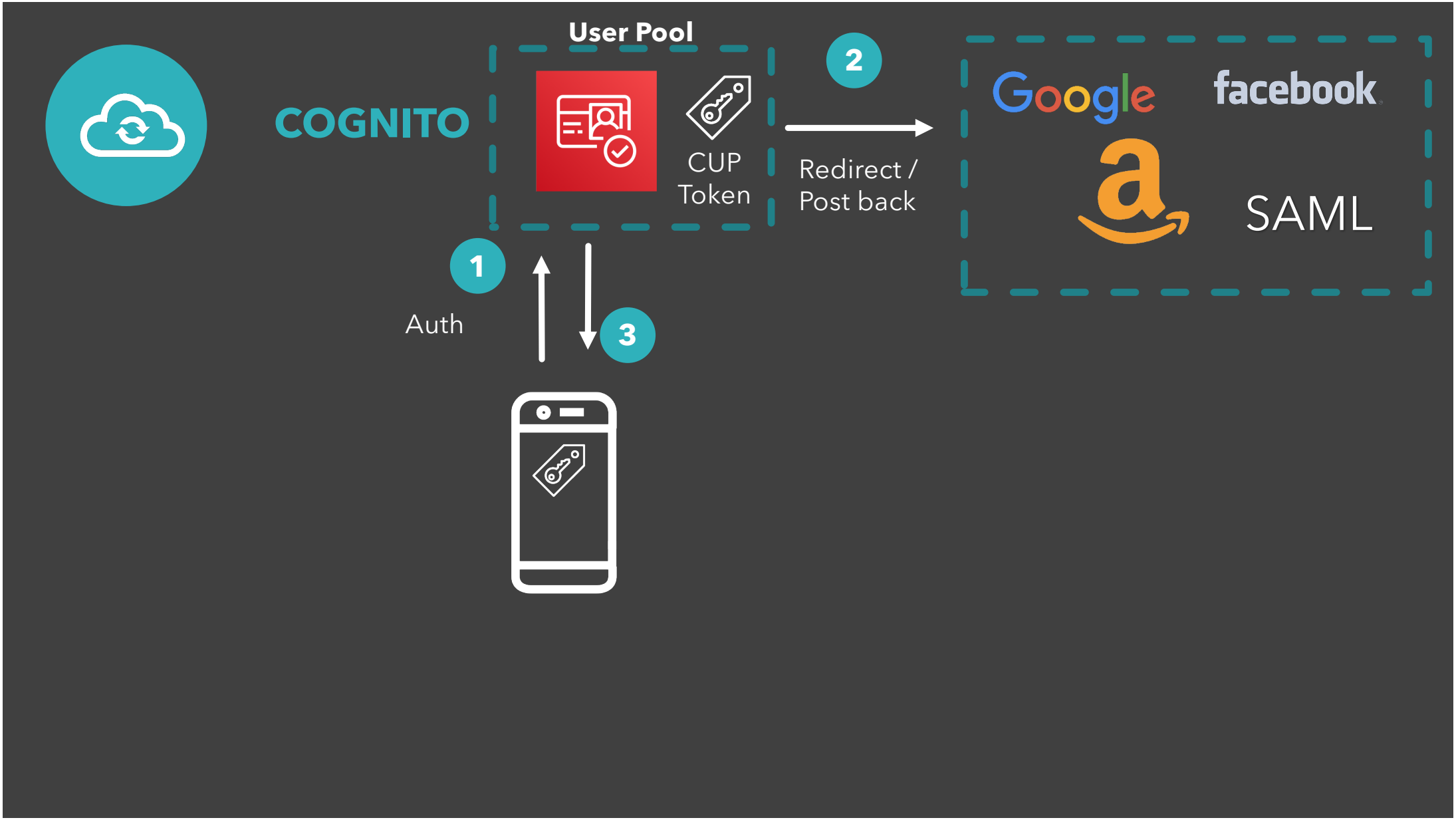
IDENTITY POOL

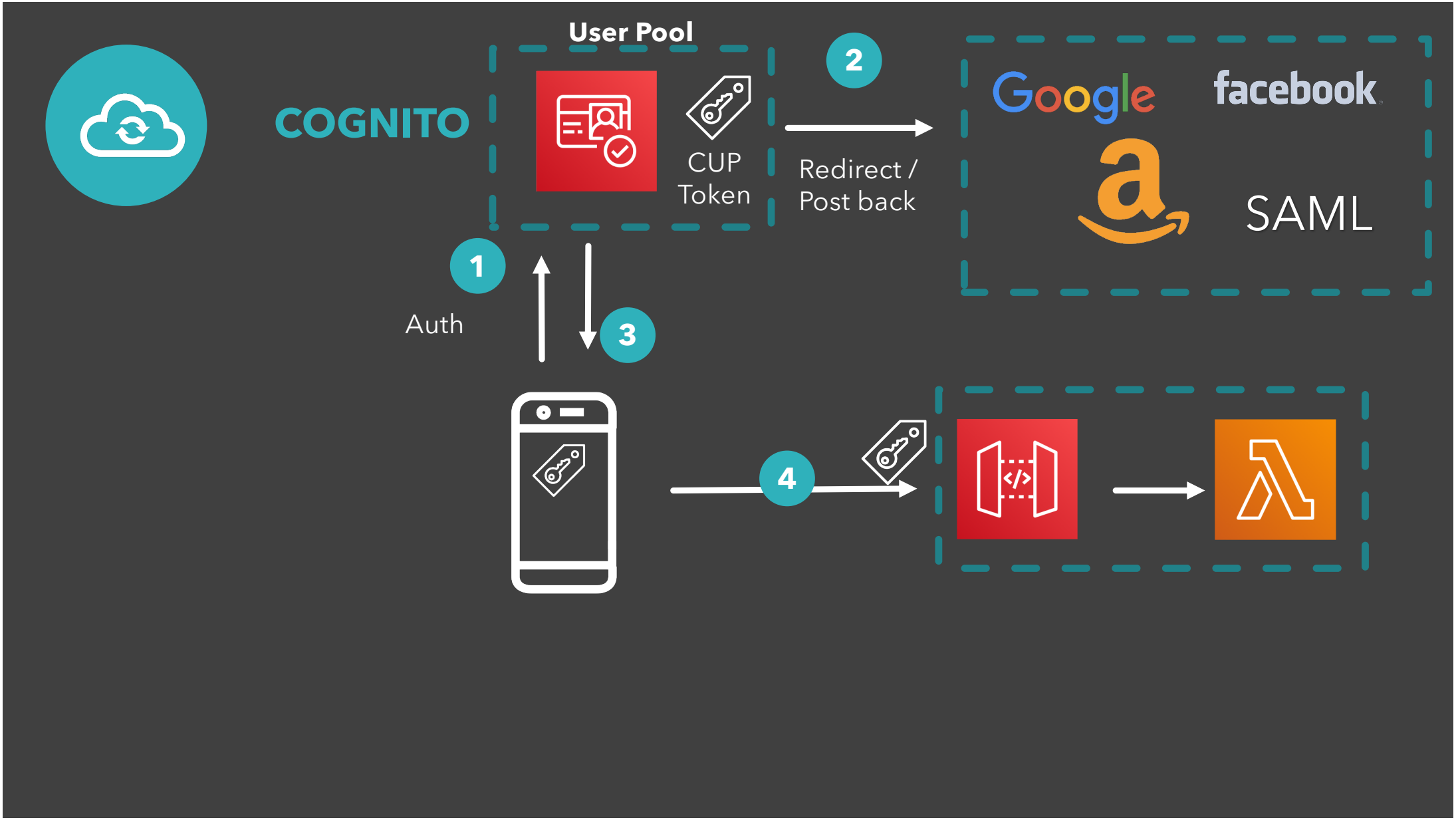
- Link and IAM role with Users for AWS Services
- Control acess to AWS resources
- Don`t have a User Directory

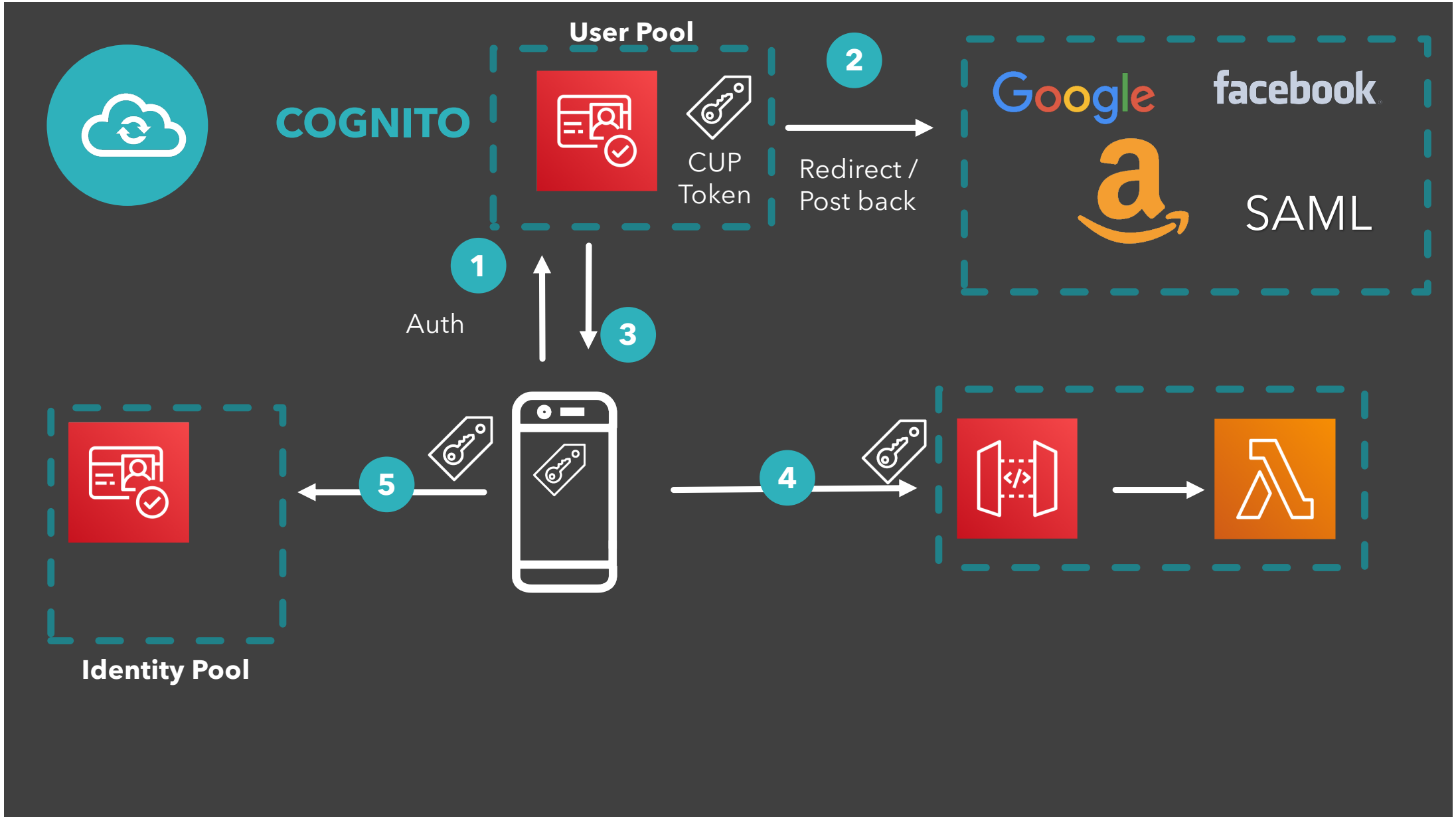
Possbile to combine RBAC with IAM

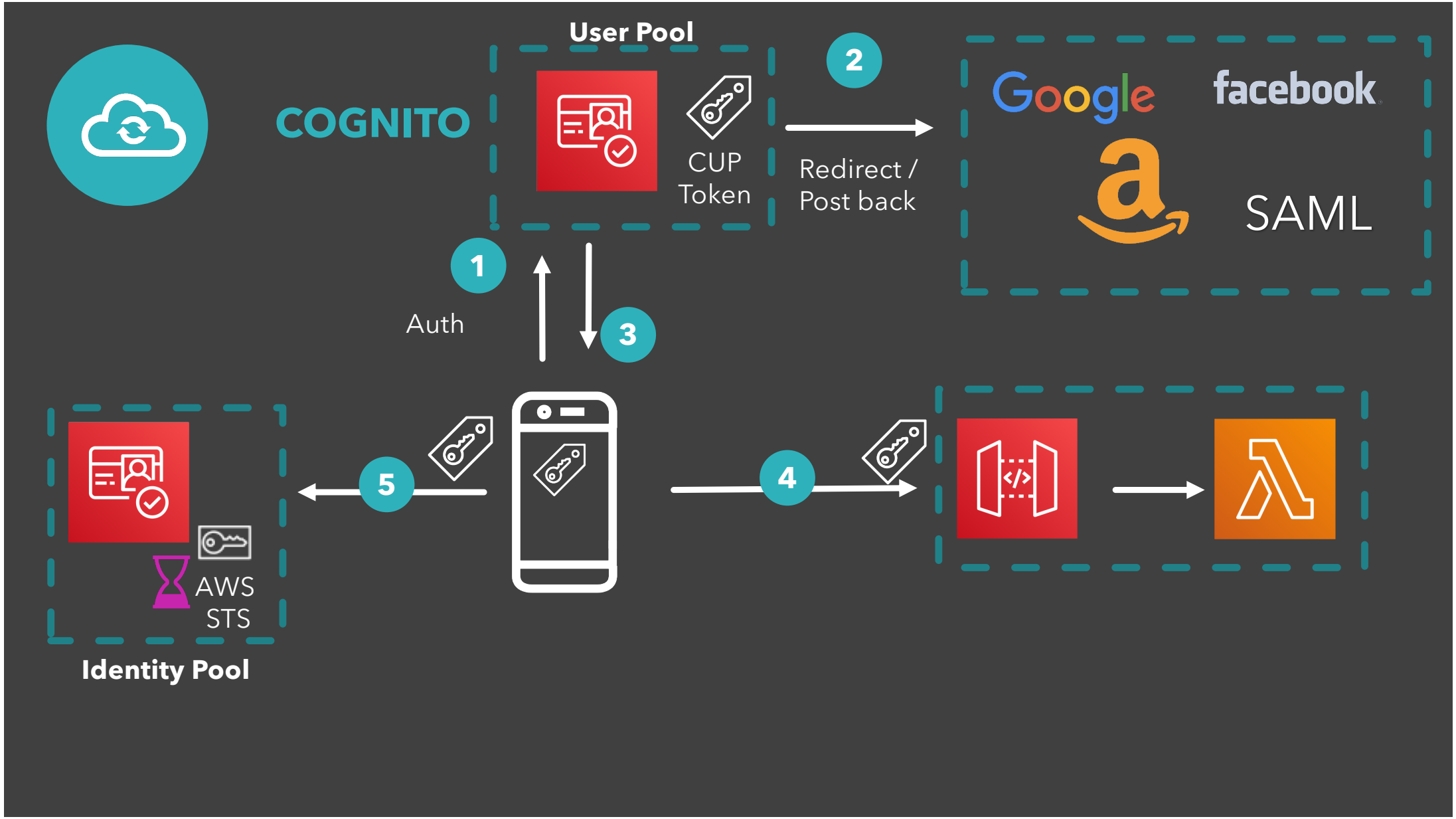

User Pool
COGNITO
1
Auth

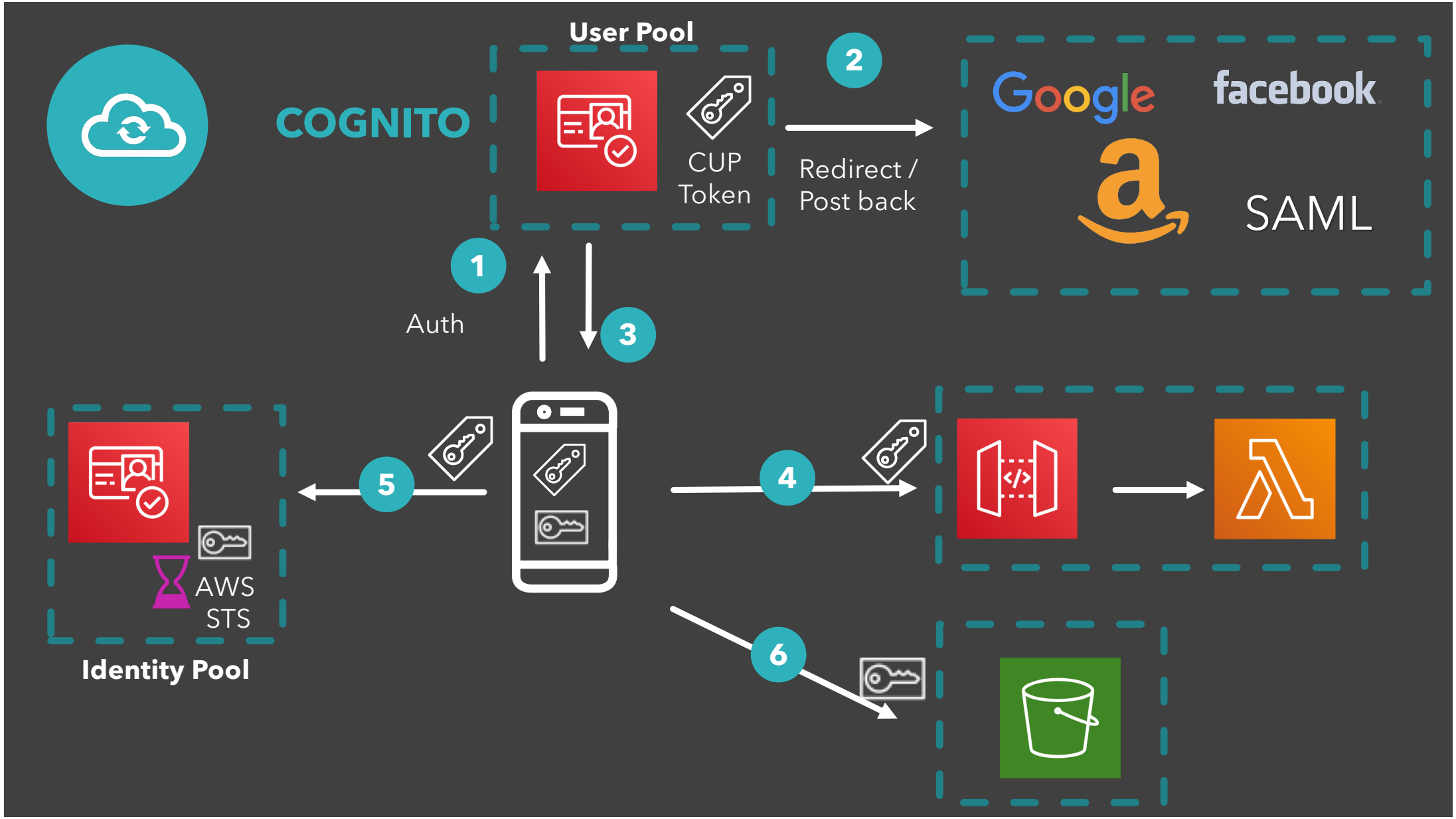

COGNITO
User Pool
2
Redirect /
Post back
Google
facebook
SAML
1
Auth


COGNITO
User Pool
CUP
Token
2
Redirect /
Post back
Google
facebook
SAML
1
Auth
3


COGNITO
User Pool
CUP
Token
2
Redirect /
Post back
Google
facebook
SAML
1
Auth
3
4


COGNITO
User Pool
CUP
Token
2
Redirect /
Post back
Google
facebook
SAML
1
Auth
3
4
5
Identity Pool

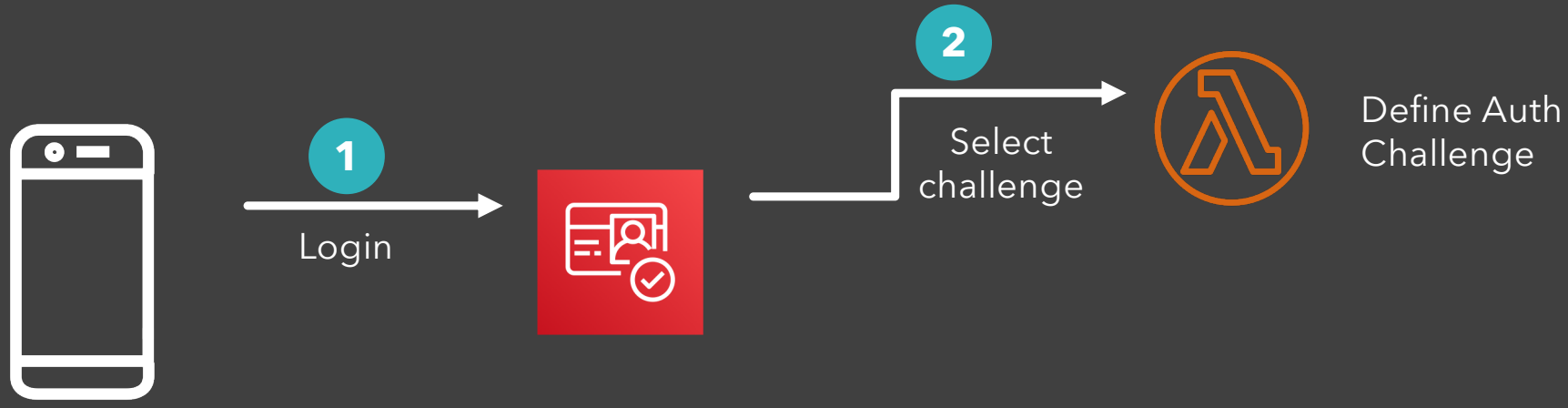

COGNITO
User Pool
CUP
Token
2
Redirect /
Post back
Google
facebook
SAML
1
Auth
3
5
4
AWS
STS
Identity Pool

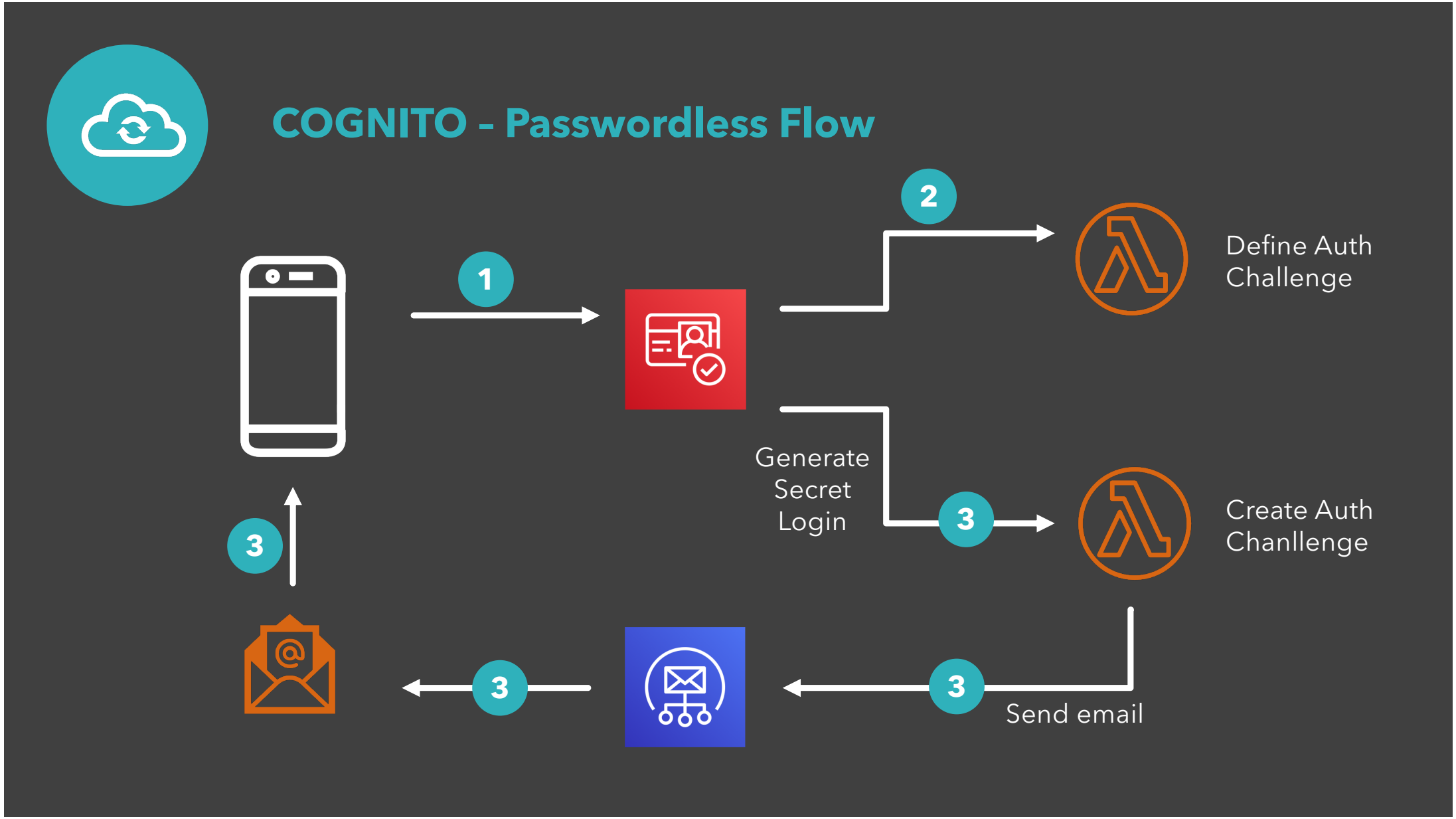

COGNITO
User Pool
CUP
Token
2
Redirect /
Post back
Google
facebook
SAML
1
Auth
3
5
4
6
AWS
STS
Identity Pool

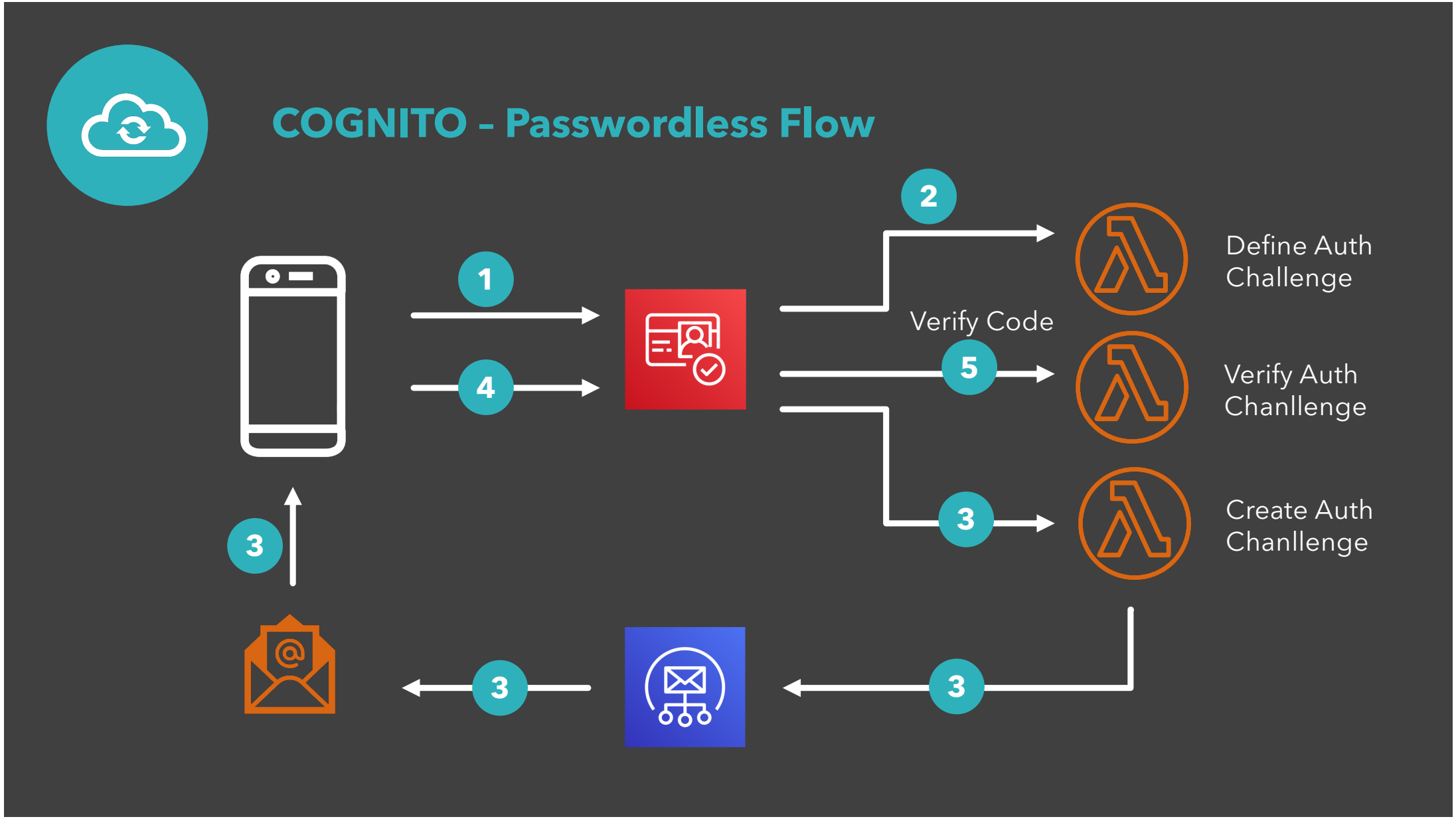
COGNITO

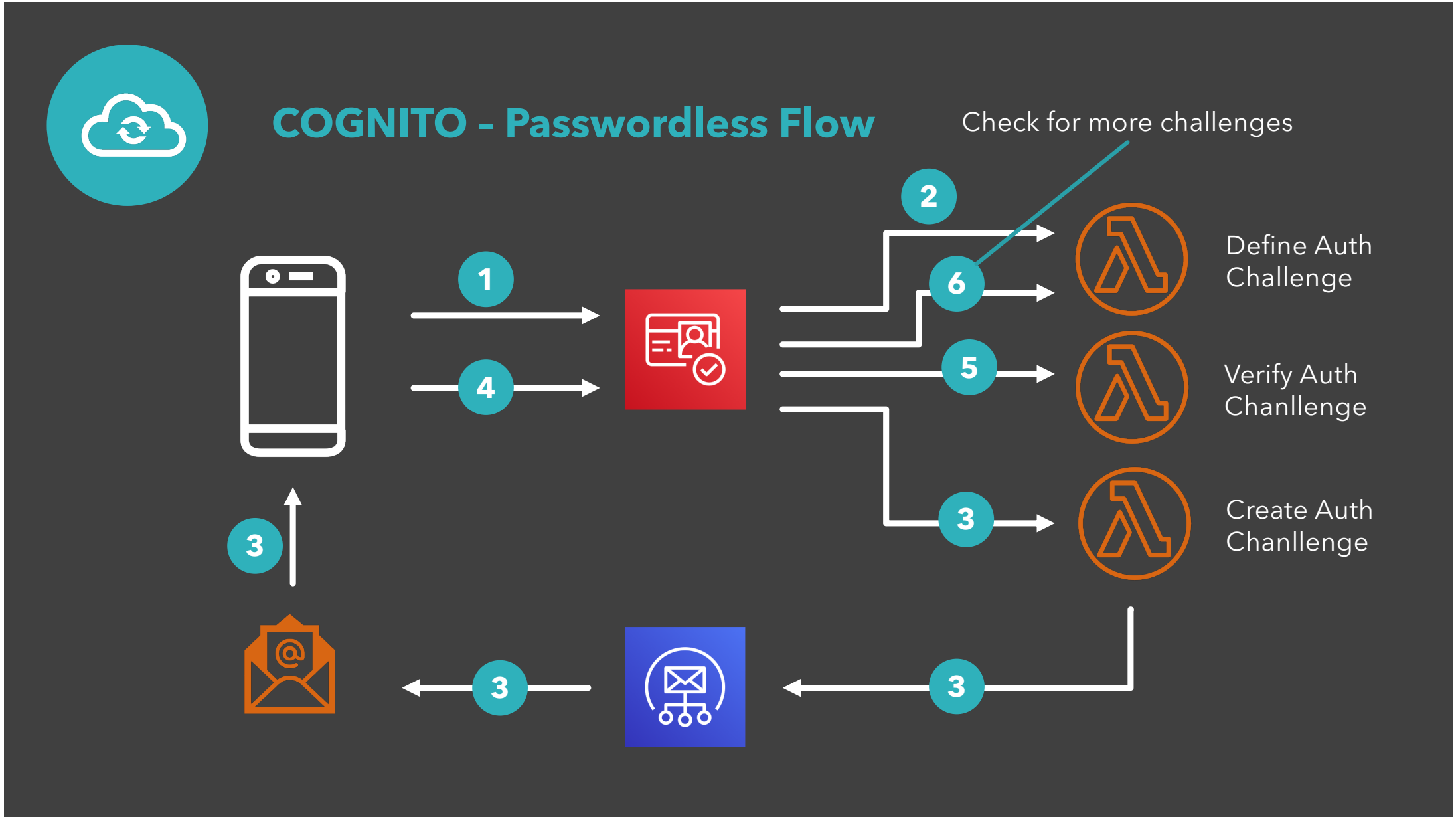
Demo

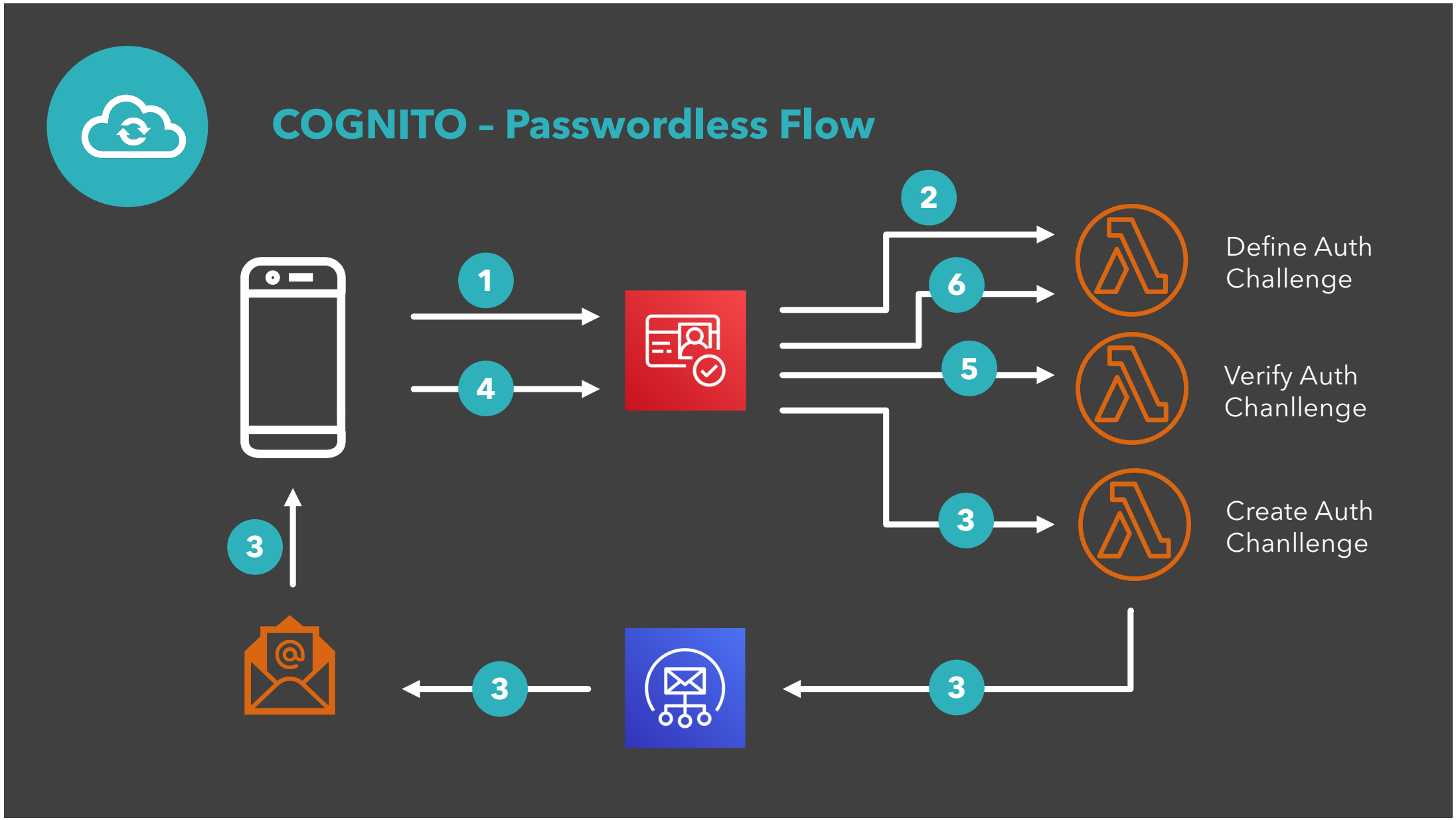
COGNITO - Passwordless Flow




COGNITO - Passwordless Flow
1
2
Define Auth
Challenge
Generate
Secret
Login
3
Create Auth
Chanllenge
3
3
Send email
3


COGNITO - Passwordless Flow
1
2
3
4
5
Verify Code
Define Auth Challenge
Verify Auth Chanllenge
Create Auth Chanllenge
3
3
3


COGNITO - Passwordless Flow
Check for more challenges
Define Auth Challenge
Verify Auth Chanllenge
Create Auth Chanllenge
1
2
3
4
5
6
3
3
3


COGNITO - Passwordless Flow
1
2
3
4
5
6
3
3
3
Define Auth Challenge
Verify Auth Chanllenge
Create Auth Chanllenge

COGNITO - Passwordless Flow

Demo

Code

Presentation

https://github.com/brunopenso/awscognitodemo-webapp

REFERENCES

https://thenewstack.io/understanding-aws-cognito-user-and-identity-pools-for-serverless-apps/

https://github.com/aws-samples/

https://youtu.be/VZqG7HjT2AQ

https://youtu.be/OAR4ZHP8DEg

https://docs.aws.amazon.com/cognito/latest/developerguide/amazon-cognito-integrating-user-pools-with-identity-pools.html

https://auth0.com/docs/api-auth/which-oauth-flow-to-use

https://aws.amazon.com/blogs/mobile/customizing-your-user-pool-authentication-flow/

https://aws.amazon.com/blogs/mobile/implementing-passwordless-email-authentication-with-amazon-cognito/

https://github.com/aws-samples/amazon-cognito-passwordless-email-auth/tree/master/cognito/lambda-triggers

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html