AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC304

Machine-to-machine authentication on AWS

Chris Mercer

Security Specialist
Solutions Architect
AWS

Moumita Saha

Sr. Security Consultant
AWS

Emir Ayar

Tech Lead Solutions Architect
AWS

Samuel Folkes

Sr. Security Specialist
Solutions Architect
AWS

Jeremy Ware

Security Specialist
Solutions Architect
AWS

Agenda

Introductions

Builders’ session?

Problem statement

Authentication methods

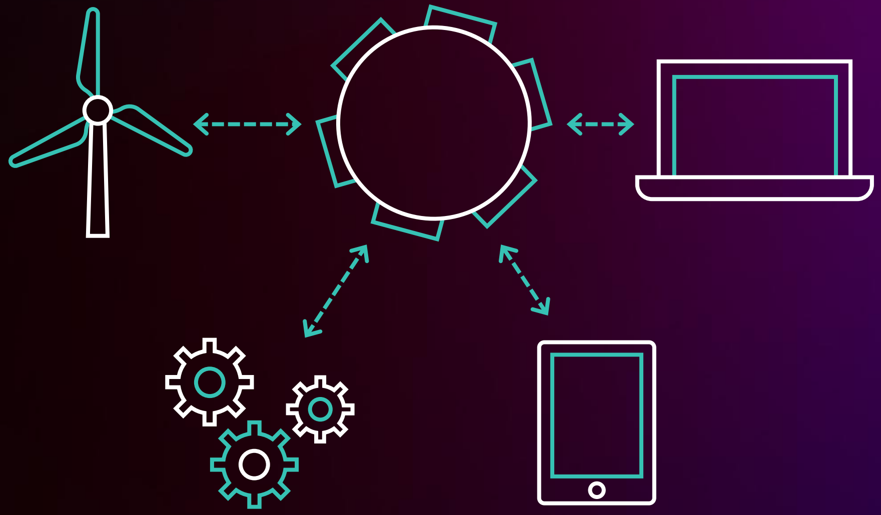
Let’s build!

What is a builders’ session?

- One-hour small-group sessions
- Build & experiment together!
- Ask AWS experts

Problem

- Machine-to-machine is hard
- Long-term credentials are risky
- Short-term credentials for the win



Why choose tokens instead of passwords?

1

Tokens are short-lived

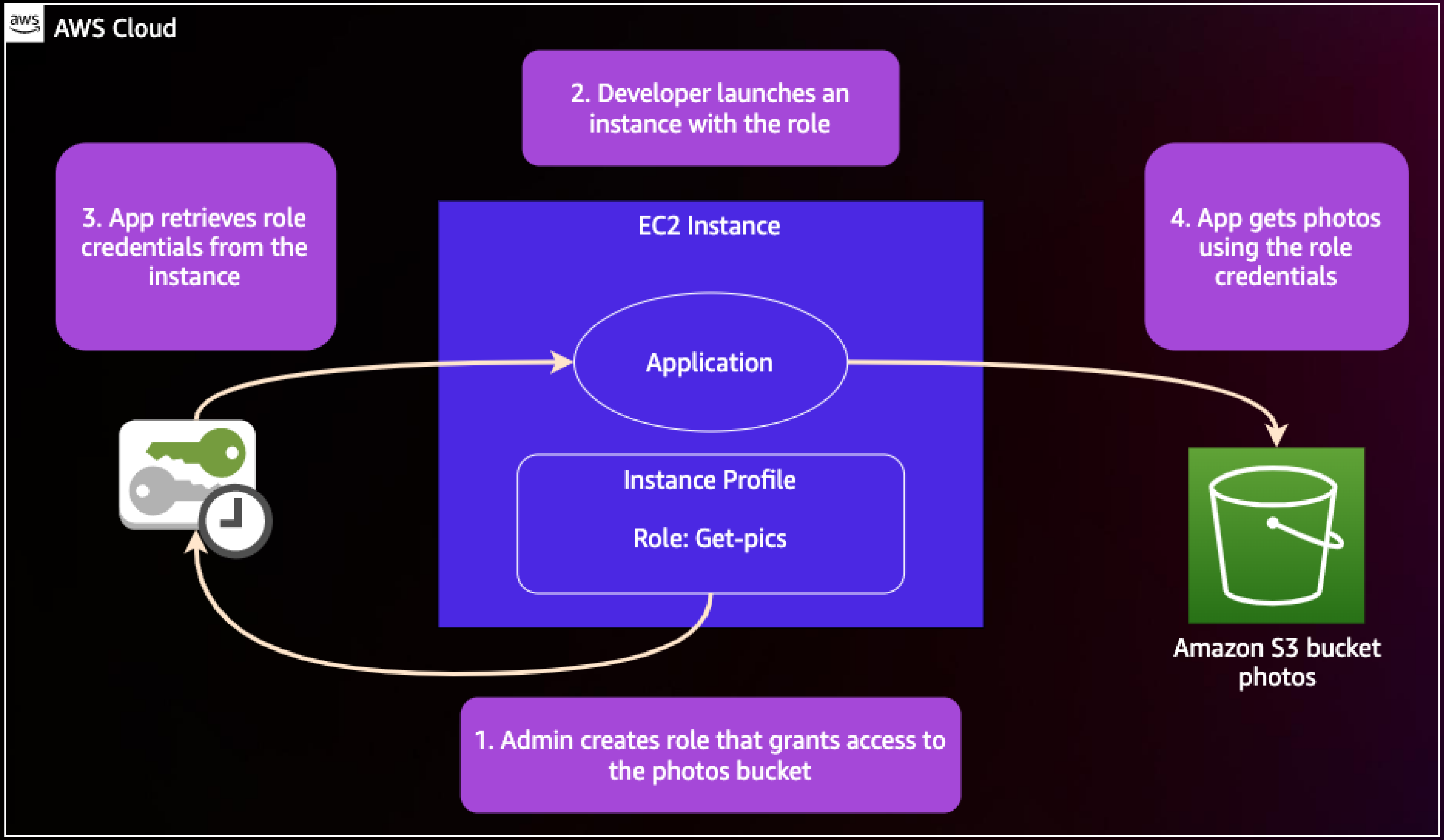
Tokens allow for granting temporary access repeatedly

2

Tokens allow for granting granular access to specific system components

Instead of a common password, tokens allow for implementing the least-privilege principle on each system component

Solution: Amazon EC2 instance profiles



AWS Cloud

2. Developer launches an instance with the role

3. App retrieves role credentials from the instance

EC2 Instance

Application

Instance Profile

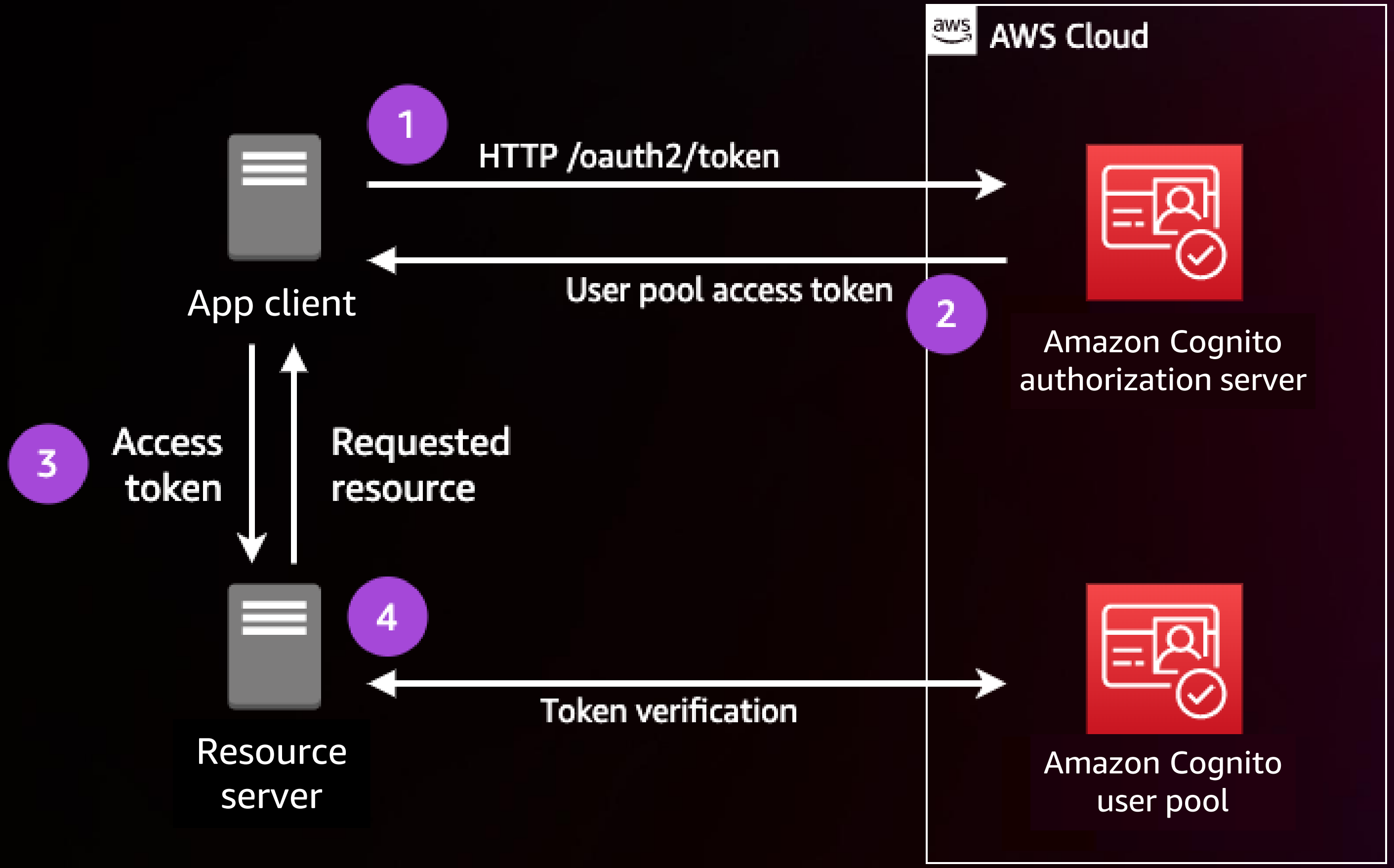
Role: Get-pics

4. App gets photos using the role credentials

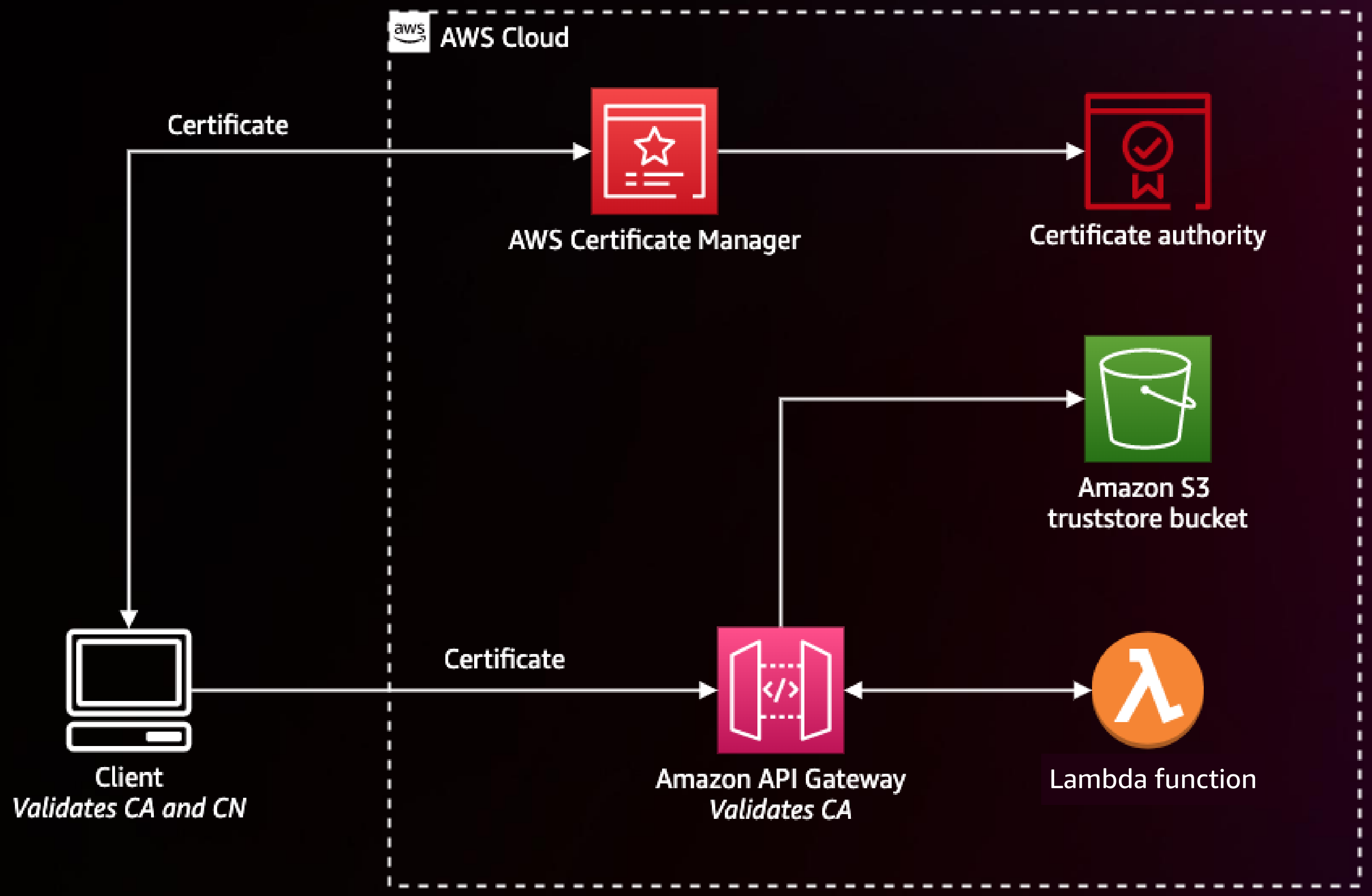
Amazon S3 bucket photos

1. Admin creates role that grants access to the photos bucket

Solution: Amazon Cognito client credentials

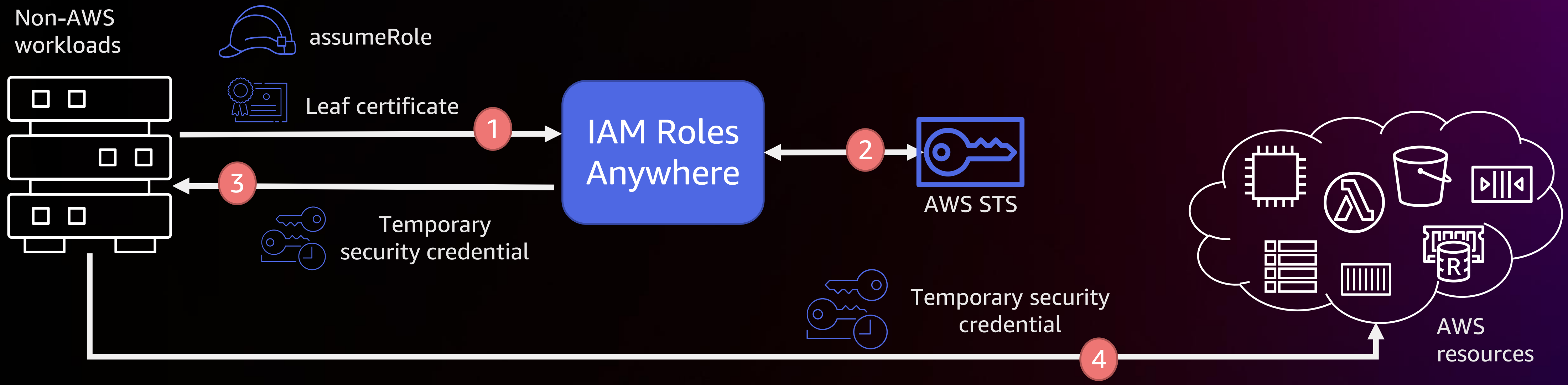


Solution: Mutual TLS (mTLS)



Solution: IAM Roles Anywhere

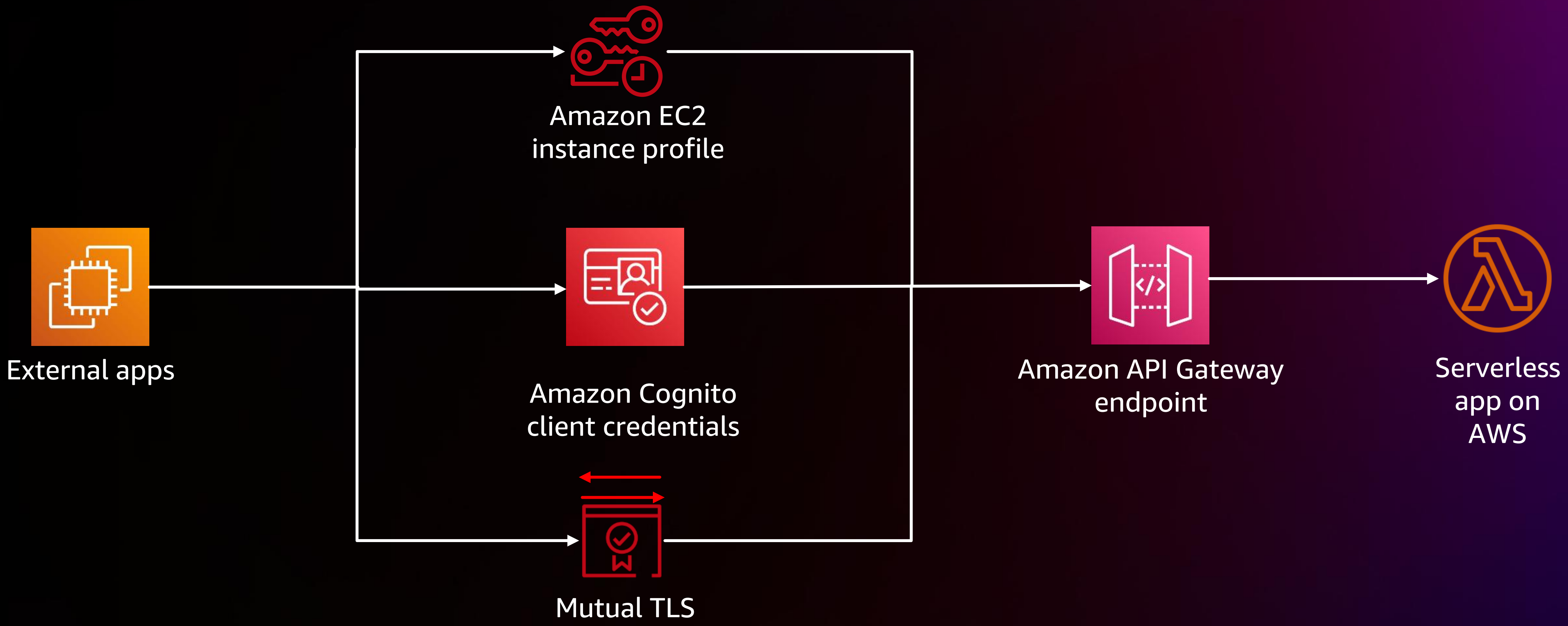
* hands-on not included in this builders' session



Solutions in comparison

Method	Pros	Cons
API key	• Quick, simple, and easy	• Sends credentials on each request • Long-lived
Instance profile	• Transparent • Credentials are stored in-memory • Short-lived	• Applicable only in AWS authentication
Client credentials	• Short-lived (communicates long-lived credentials only with Amazon Cognito)	• Requires an oAuth server (like Amazon Cognito) between apps
mTLS	• Verifies both ends of communication • No credentials are transferred	• Complicated setup: PKI management on both ends
IAM Roles Anywhere	• Short-lived • No credentials are transferred	• Requires PKI management

Workshop architecture



Let’s build!

Event link:
https://catalog.us-east-1.prod.workshops.aws/join

Access code: 1234567890QWERTYUIOP

Thank you!

Please complete the session survey in the **mobile app**