AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

IOT311

AWS IoT device connectivity and provisioning

Harish Rajagopalan (he/him)
Solutions Architect,
Amazon Web Services

Christine Samson (she/her)
Startup Solutions Architect,
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

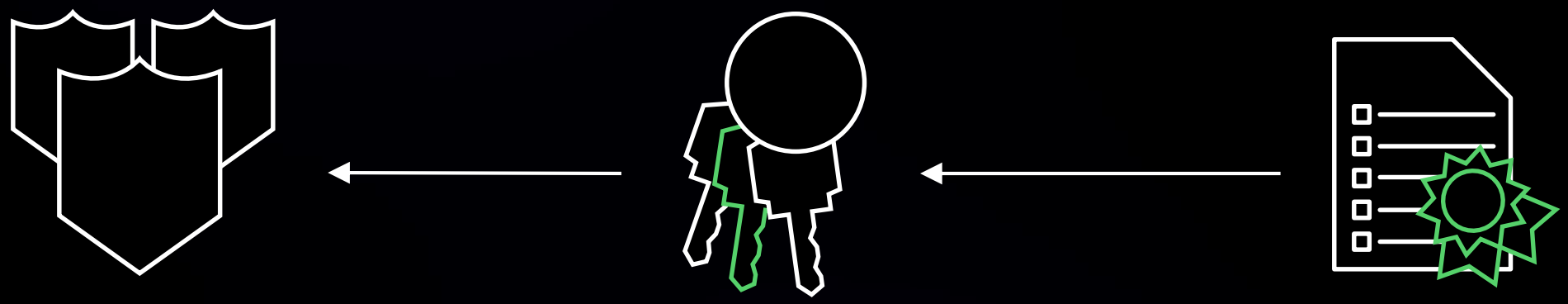
Device authentication

Device connectivity options

Device provisioning options

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Device authentication and authorization



IoT thing

IoT certificate

IoT policy

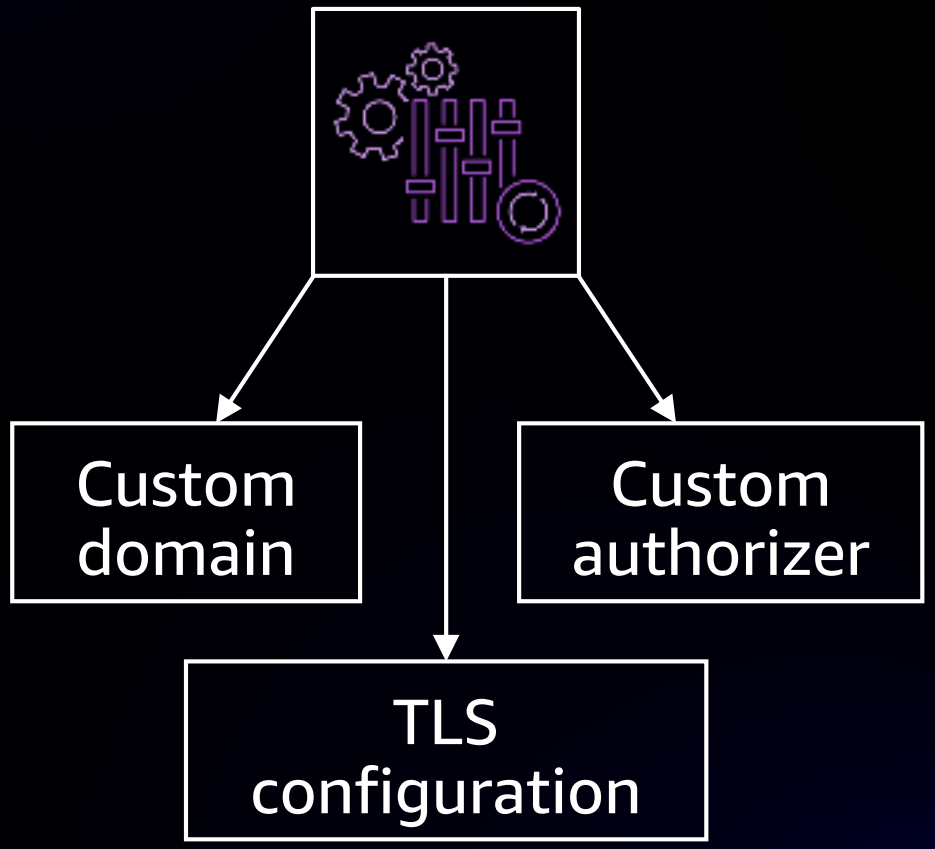
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Device connectivity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

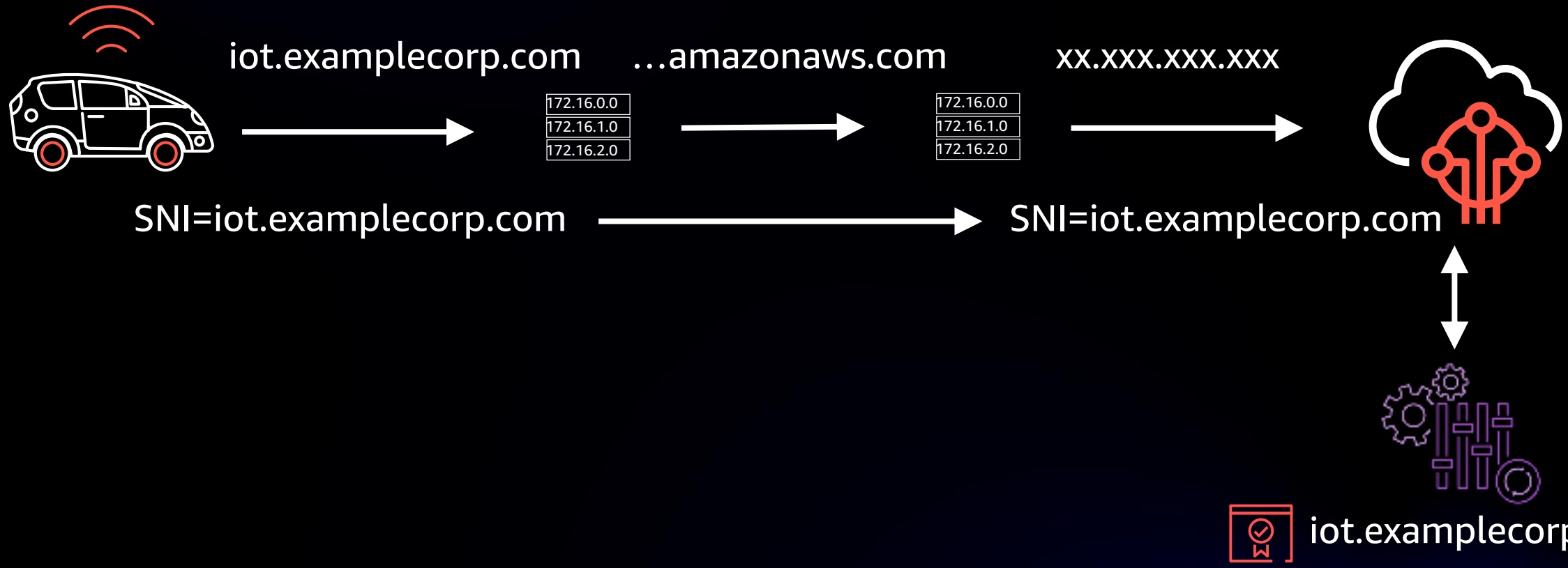
Configurable endpoints

abcd1234.iot.us-east-1.amazonaws.com



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Custom domains



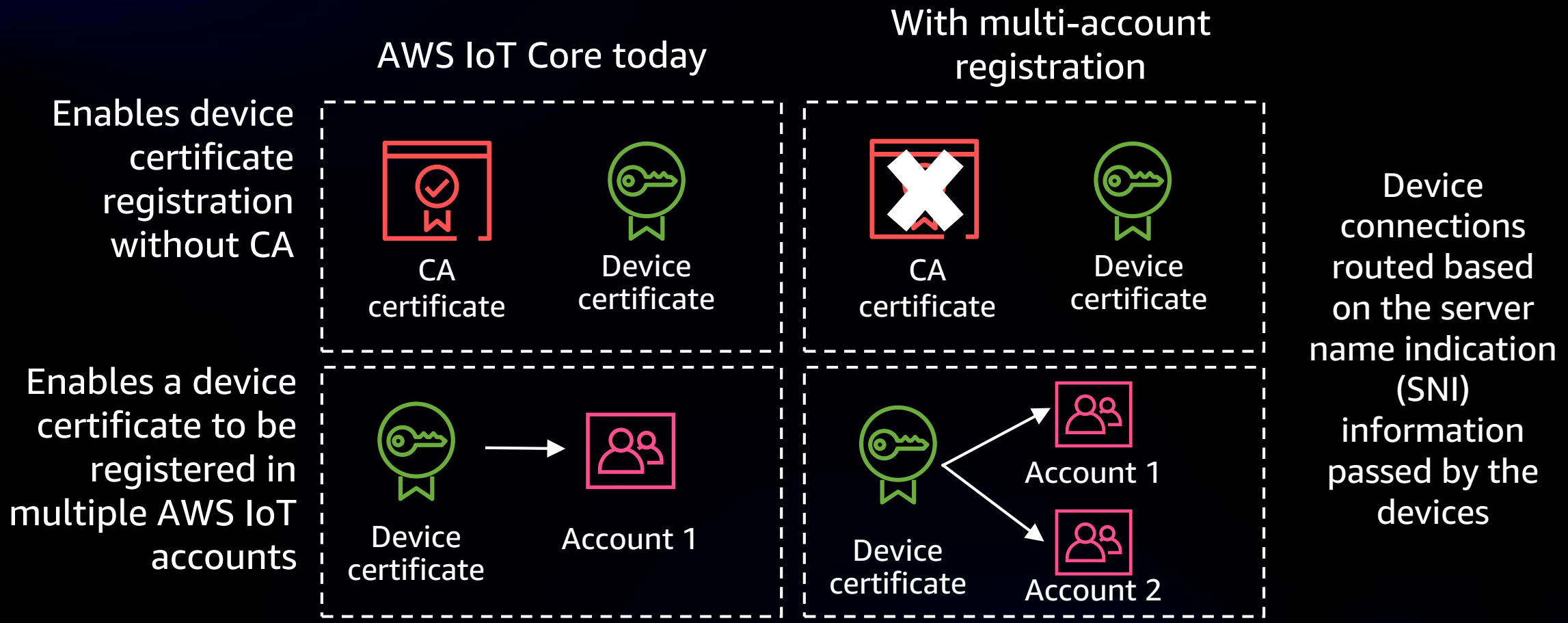
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Custom authentication enhancements

```
{"token" :"a Token",
"signatureVerified": boolean, // Indicates whether the device gateway has validated the signature.
"protocols": ["tls", "http", "mqtt"], // Indicates which protocols to expect.
"protocolData": {
        "tls" : {
                "serverName": "serverName" // The SNI string.
        },
        "http": {
                 "headers": {
                        "#{name}": "#{value}"
                 },
                "queryString": "?#{name}=#{value}"
         },
        "mqtt": {
                 "username": "myUserName",
                "password": "myPassword", // base64 encoded.
                 "clientId": "myClientId"
         }
},
"connectionMetadata": {
    "id": UUID // The connection Id. You can use this for logging.
},
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-account registration



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Device provisioning

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Device provisioning options

- Single thing provisioning
- Bulk registration
- Just-in-time provisioning (JITP)
- Fleet provisioning
  - By trusted user
  - By claim

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Single device provisioning

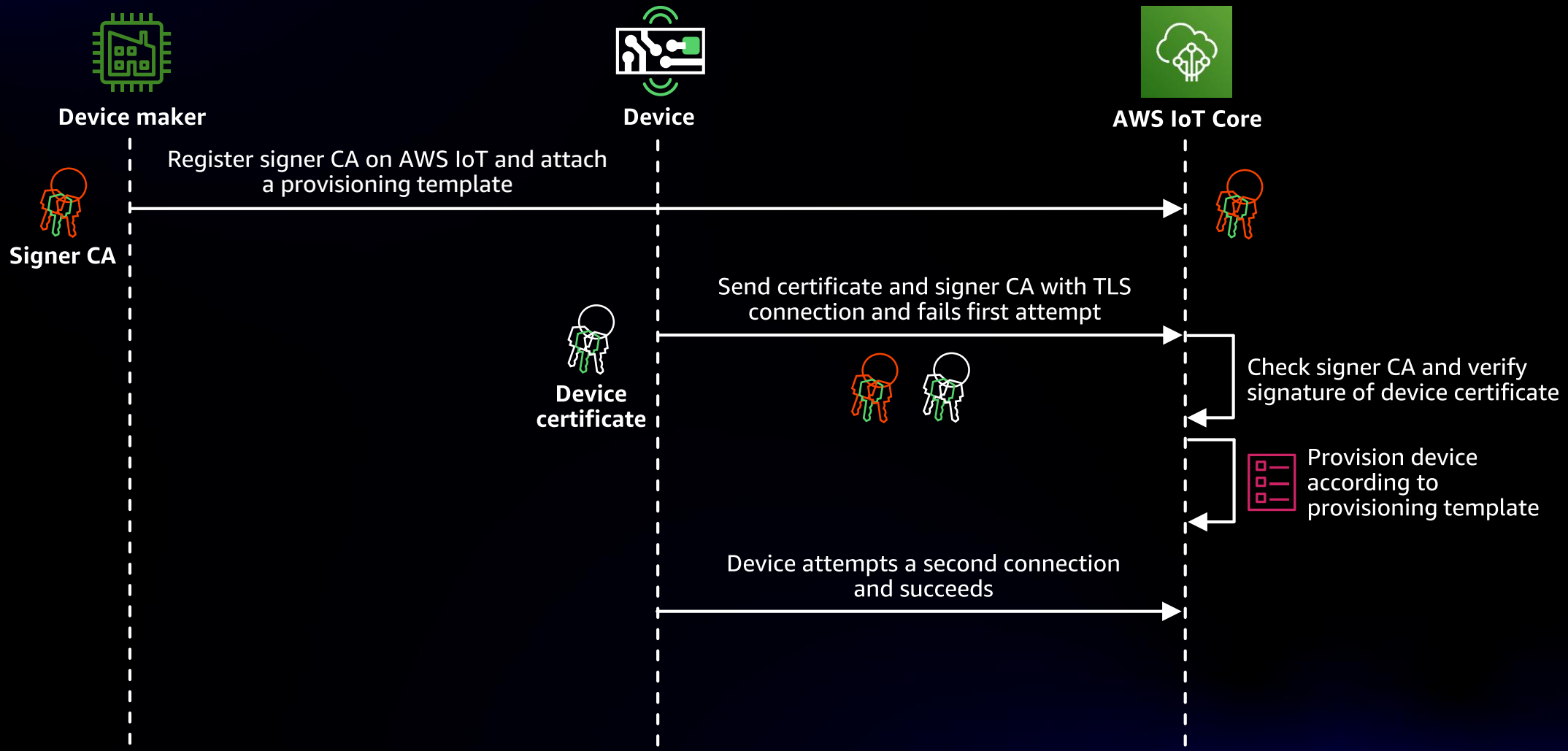
- RegisterThing API

Bulk provisioning

- start-thing-registration-task command

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Just-in-time provisioning



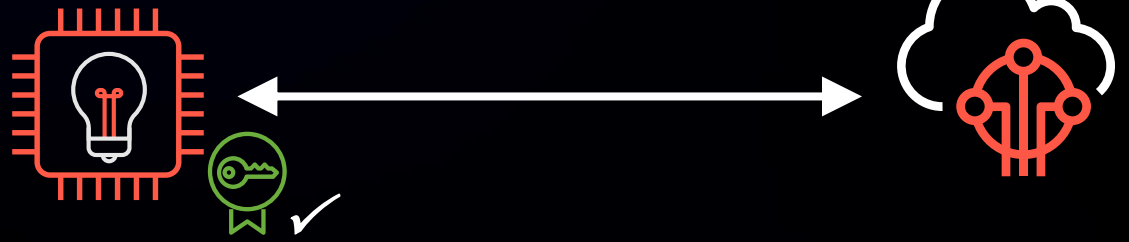
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fleet provisioning

Use case 1

"Trusted bootstrap identity"

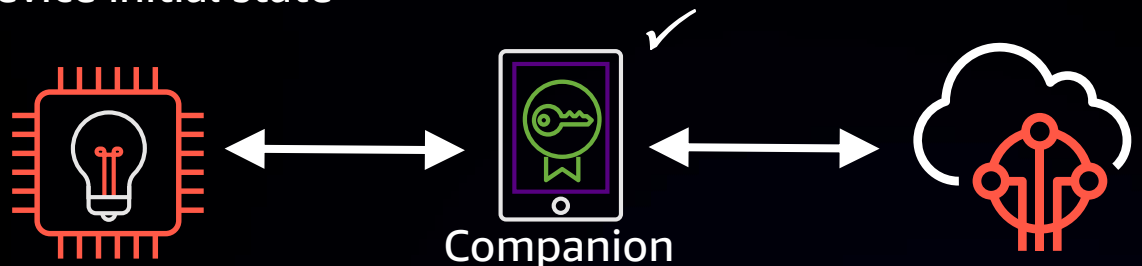
Device initial state



Use case 2

"Trusted user"

Device initial state



Device final state



Unique digital identity



IoT policy

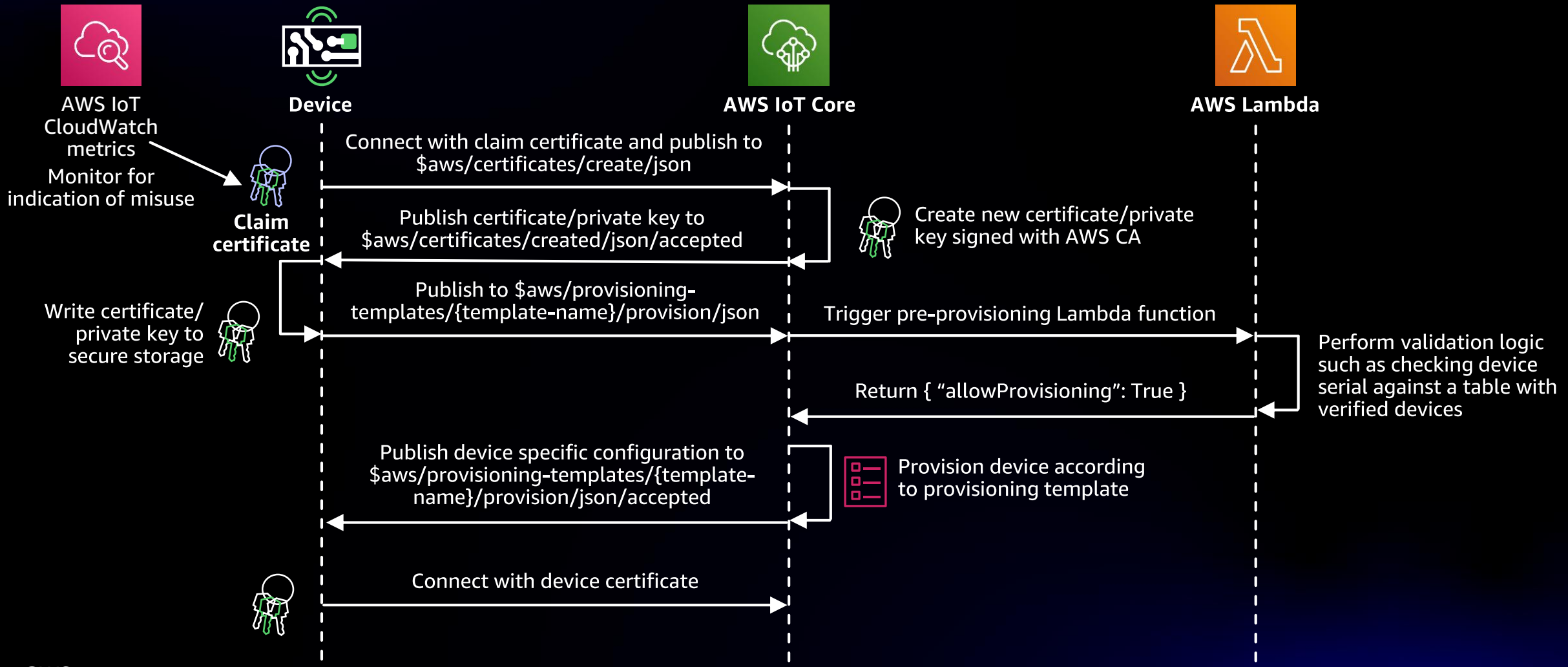


Thing registry (optional)

aws

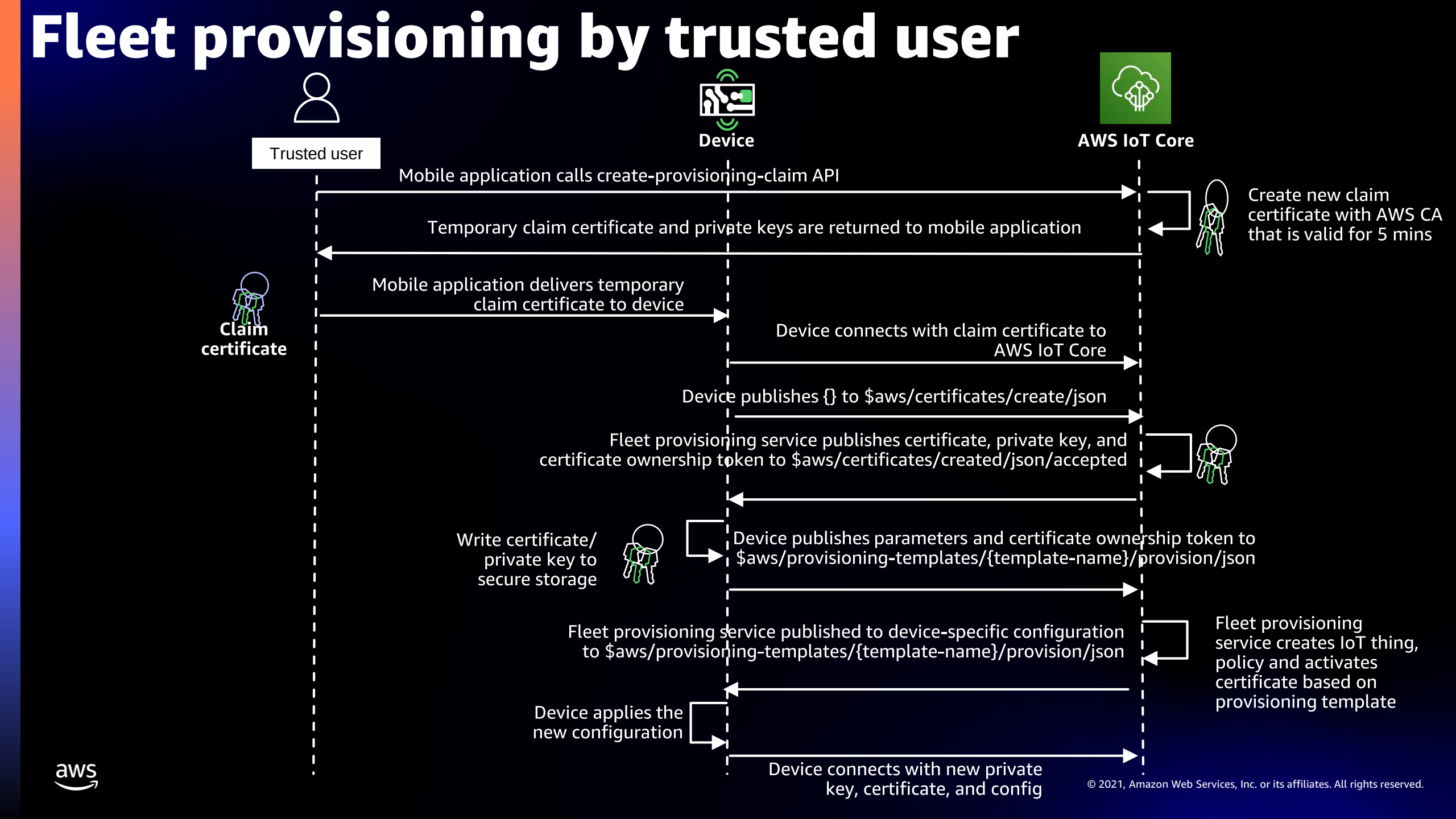
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fleet provisioning by claim



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fleet provisioning by trusted user



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Provisioning differences

	Single	Bulk	Just-In-Time	Fleet
Use Case	Device development and prototyping Testing/PoCs	When you want to use AWS CA and register devices in bulk Production/1:many	The device maker knows the account and the Region where the device will be registered Production/1:many	Devices that are not customized by the manufacturer but still need to have unique ID Production/1:many
Need to pre-provision certificates beforehand	Yes	Yes	Yes	No
Preregister certificate authority	No	No	Yes	No

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Harish Rajagopalan
rajagh@amazon.com

Christine Samson
chrsamso@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.