



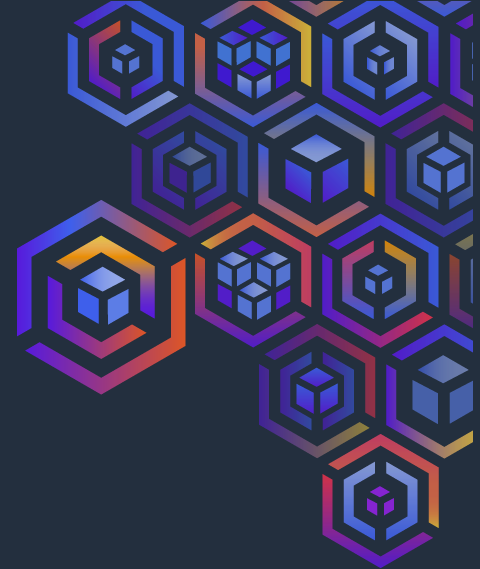
**COMMUNITY DAY**

# Building an IoT System to Protect My Lunch

**Fernando Medina Corey**

**Lead Cloud Architect – Witekio**

**@fmc\_sea**





# COMMUNITY DAY

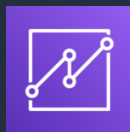
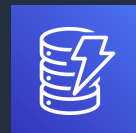
## What's the Big Deal about Cloud with IoT?

- 35 Billion connected devices today
- Customers are demanding more connected solutions
- Expiring CA root certificates
- Remotely manage updates and patches
- Predictive maintenance and alerting
- Automating and optimizing data collection and storage
- Business intelligence reporting

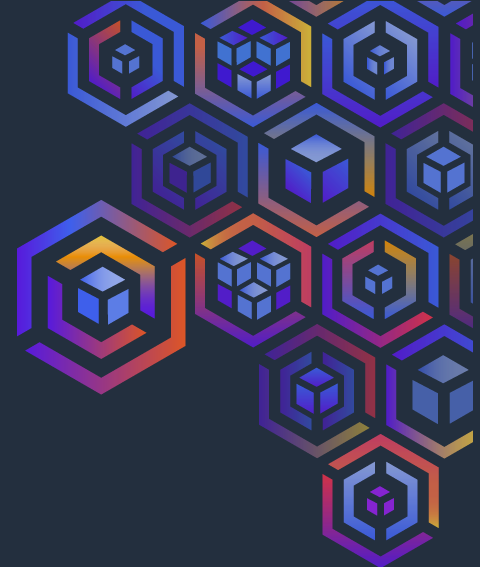




# COMMUNITY DAY



Why IoT on AWS?





# COMMUNITY DAY

## Authenticating IoT Devices to the Cloud

- X.509 certificates
- TPM attestation
- Other mechanisms
  - Device claiming
  - Preregistering device ids and public keys
  - Certificate Signing Requests

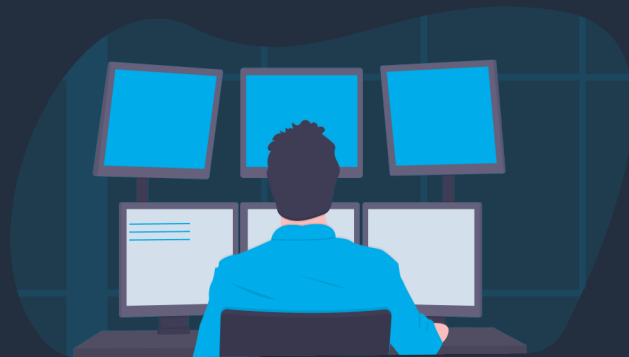




# COMMUNITY DAY

## Device Authorization Mechanisms

- IoT Core Polices
- AWS IAM Policies and Roles
- Amazon Cognito
- STS Tokens





# COMMUNITY DAY



## Root Certificate

- Creates signing certificates
- Registered with the AWS



## Signing Certificate(s)

- Creates trusted device certificates



## Leaf/Device Certificates

- Authenticates the device
- Stored securely on the device

# X.509 Authentication



# COMMUNITY DAY

AWS IoT Core

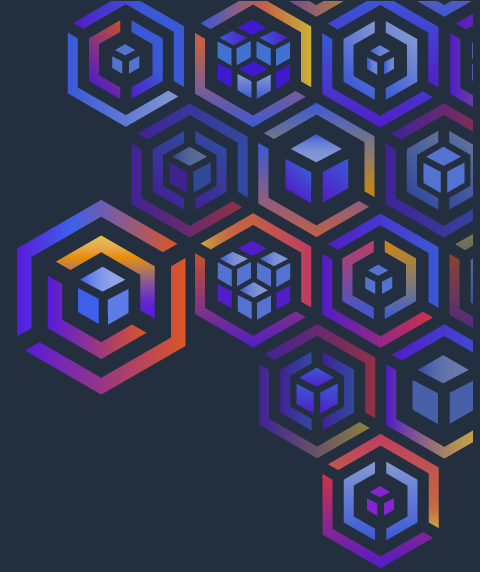


Root Certificate



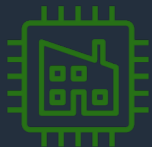
Signing Certificate

## X.509 Authentication





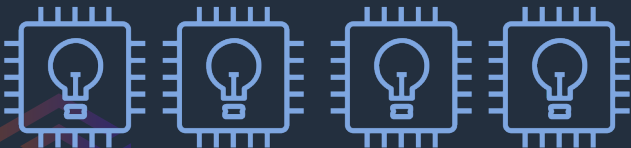
# COMMUNITY DAY



Device Manufacturing Process



Signing Certificate

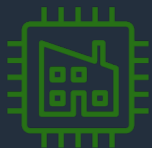


## X.509 Authentication





# COMMUNITY DAY



Device Manufacturing Process

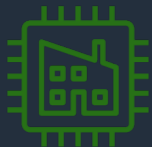


Signing Certificate

## X.509 Authentication



# COMMUNITY DAY



Device Manufacturing Process

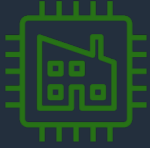


Signing Certificate

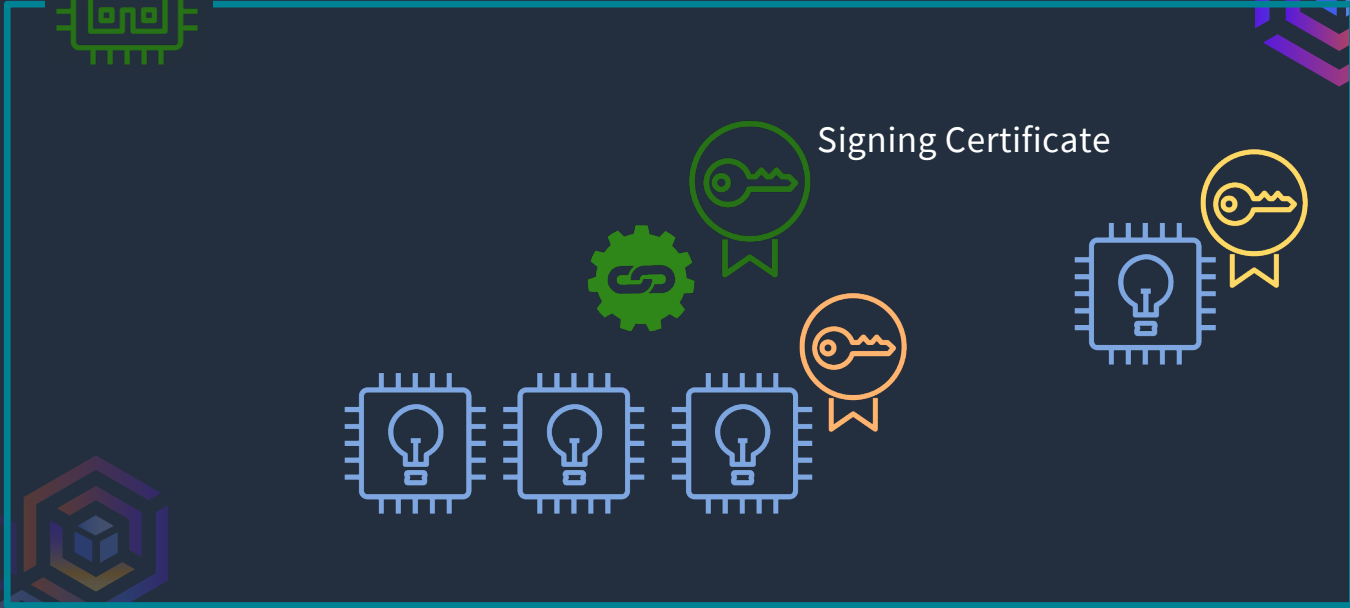
## X.509 Authentication



# COMMUNITY DAY



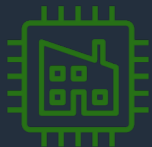
Device Manufacturing Process



## X.509 Authentication



# COMMUNITY DAY



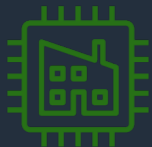
Device Manufacturing Process



## X.509 Authentication



# COMMUNITY DAY



Device Manufacturing Process



## X.509 Authentication



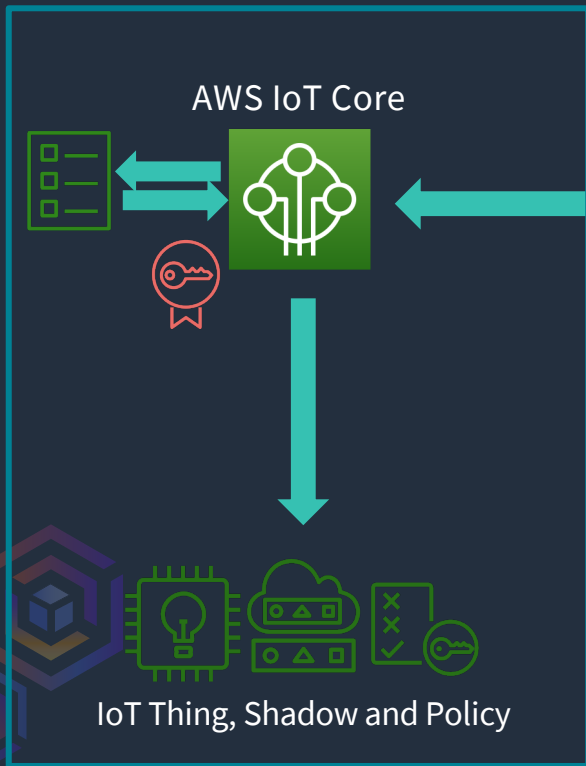
# COMMUNITY DAY

## IoT Device Provisioning on AWS

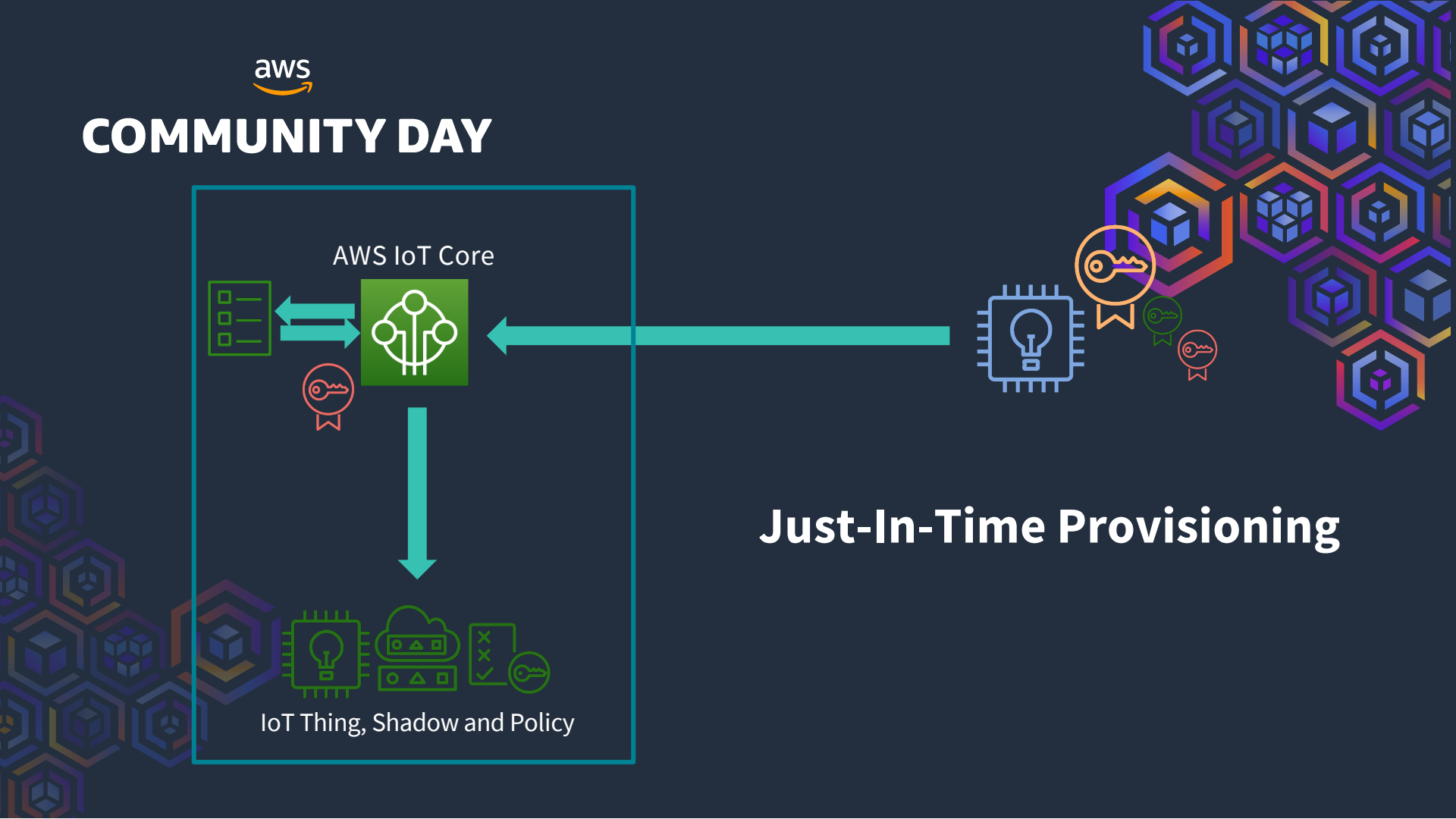
- Manually register devices and certificates in AWS IoT
- Just In Time Provisioning (JITP)
  - Devices provision with template
- Just In Time Registration (JITR)
  - Lambda processes MQTT Topic
- Provisioning via trusted user
  - Authenticated technician or customer gets certificate for device
- Provisioning via claim certificate
  - Shared claim certificate used to get a unique certificate



# COMMUNITY DAY

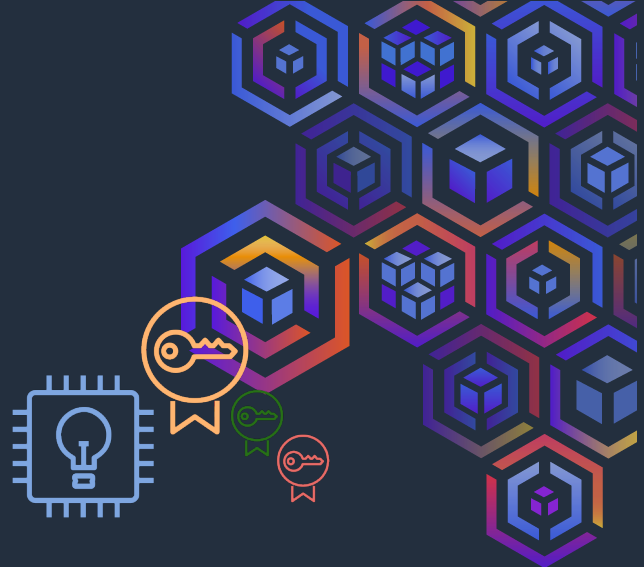
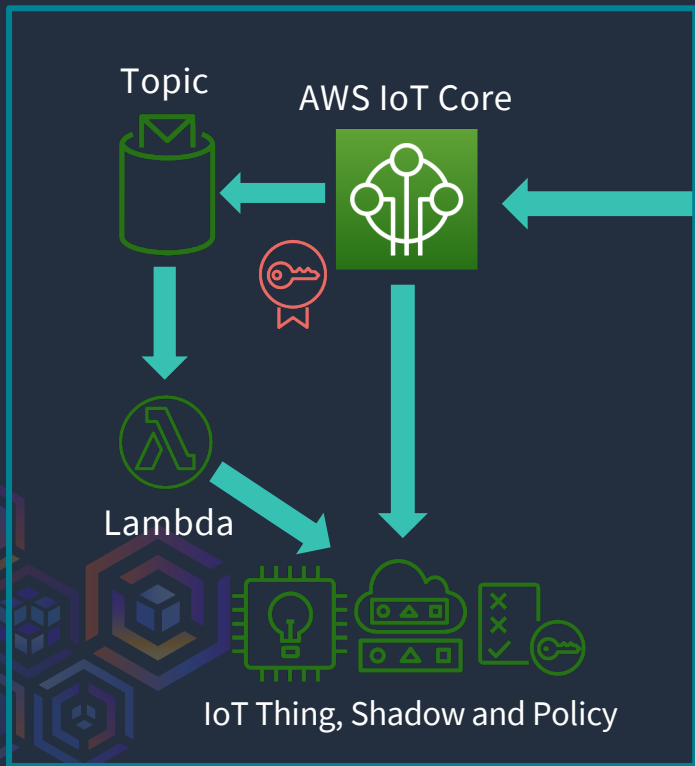


## Just-In-Time Provisioning





# COMMUNITY DAY



## Just-In-Time Registration



Demo Time!

My Snack Protection System



# COMMUNITY DAY

Text Message  
Thursday 8:30 AM

Your security system just detected motion  
at:2020-09-17 15:30:09

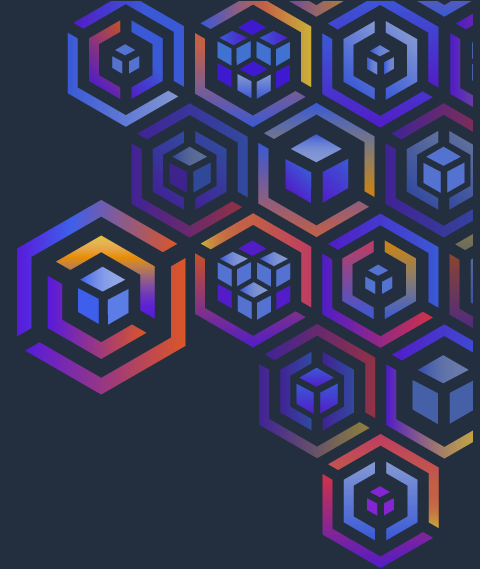
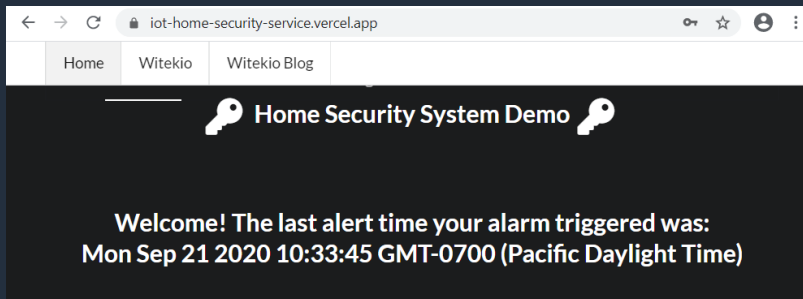
Your security system just detected motion  
at:2020-09-17 15:31:39

Today 10:33 AM

Your security system just detected motion  
at:2020-09-21 17:33:45



Text Message





# COMMUNITY DAY

Standard PIR Sensor

Raspberry Pi Device



Easily stolen chocolate



# COMMUNITY DAY



```
$ tree -L 1
```

```
.  
├── backend  
├── frontend  
└── manufacturing
```

Our  
Application  
Code



COMMUNITY DAY

# Manufacturing



```
# In ./manufacturing
```

```
$ tree
```

```
.
├── connection_attempt.bash
├── create_and_register_ca_cert.bash
├── create_device_cert.bash
├── permissive-provisioning-template.json
├── raspi_cert_transfer.bash
└── run.py
```



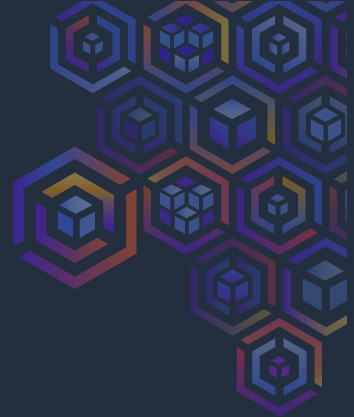
# COMMUNITY DAY



```
# In ./frontend  
$ tree
```

```
.  
├── css  
│   └── main.css  
├── index.html  
└── js  
    └── app.js
```

## Frontend





# COMMUNITY DAY

## Backend



```
# In ./backend
$ tree
.
├── handlers
│   ├── get_device_shadow.py
│   ├── jit_provisioning.js
│   └── process_alarm.py
├── resources
│   ├── cognito.yml
│   ├── dynamodb.yml
│   └── iot_provisioning_role.yml
└── serverless.yml
```

And now...

A live demo!



Getting Started Guides:

[fernandomc.com](http://fernandomc.com)

[witekio.com/blog](http://witekio.com/blog)