



Building Secure Cloud-enabled IoT Devices

A Look at the Possibilities of IoT and Cloud

Building Secure Cloud-enabled IoT Devices

Who am I?



@fmc_sea

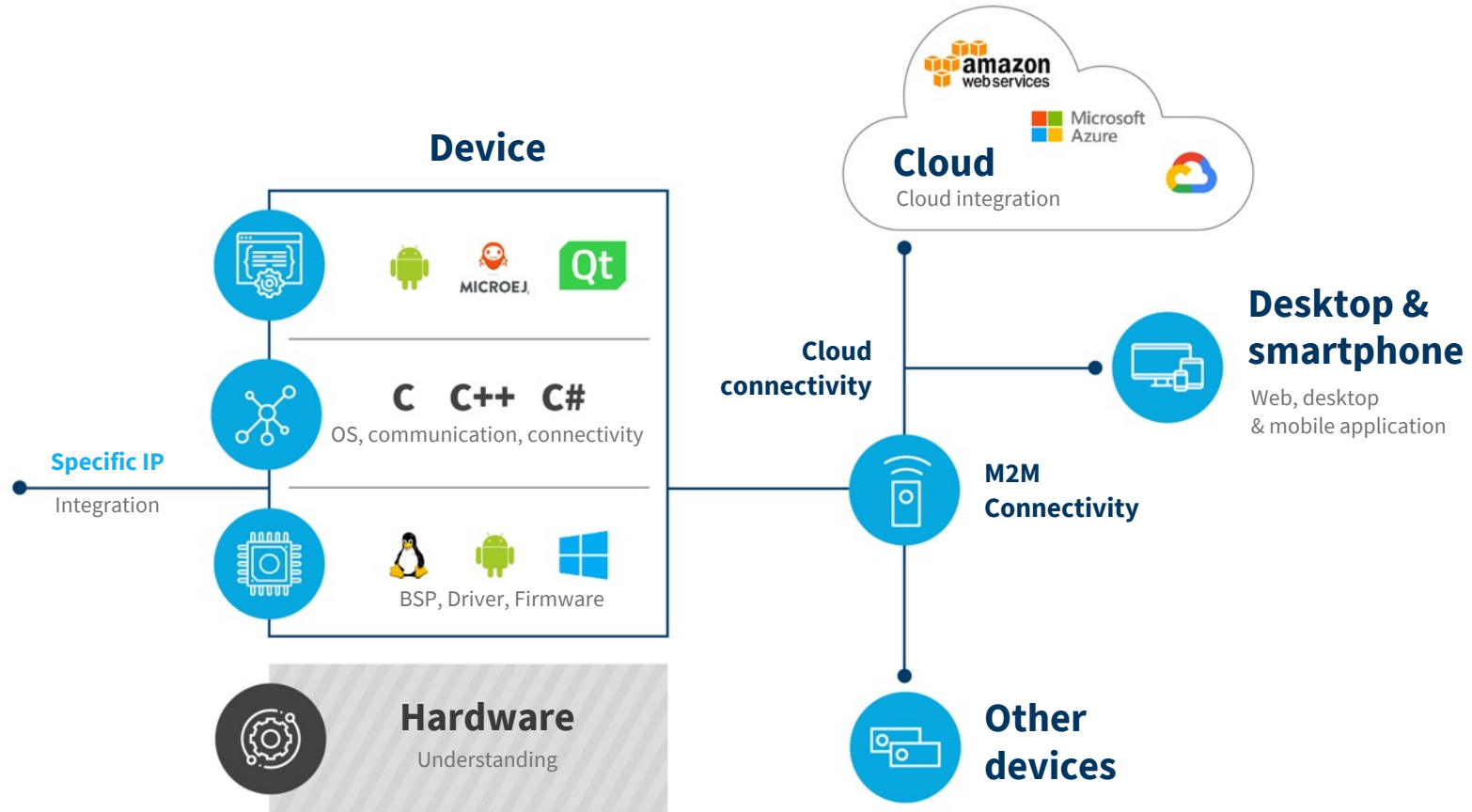
/in/fmc-sea

fernandomc.com

Fernando Medina Corey

Lead Cloud Architect

SOFTWARE INDEPENDENCE



Overview

1. Introduction
2. Cloud Platforms and Connected Devices
3. Sample IoT Architectures and Use Cases
4. Demo: The Cloud Side of IoT
5. Cost Optimization
6. Start Leveraging the Cloud for IoT





1.

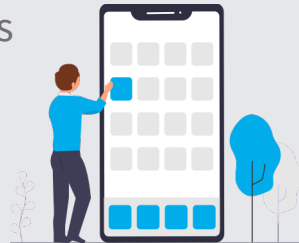
Introduction

What's the Big Deal about Cloud and IoT?

Context



- 35 Billion connected devices today
- Customers demanding more connected devices
- Expiring CA root certificates
- Numerous IoT Solutions



A Few Cloud Possibilities...

- Remotely manage updates and patches
- Predictive maintenance and alerting
- Automating and optimizing data collection and storage
- Business intelligence reporting



2.

**Cloud Platforms and
Connected Devices**



Why AWS and Azure?

Top Two Public Clouds

- [2018 ZDnet](#) - #1: AWS, #2: Azure
- [2019 Gartner](#) - #1: AWS, #2: Azure
- [2020 ZDnet](#) - #1: AWS, #2: Azure

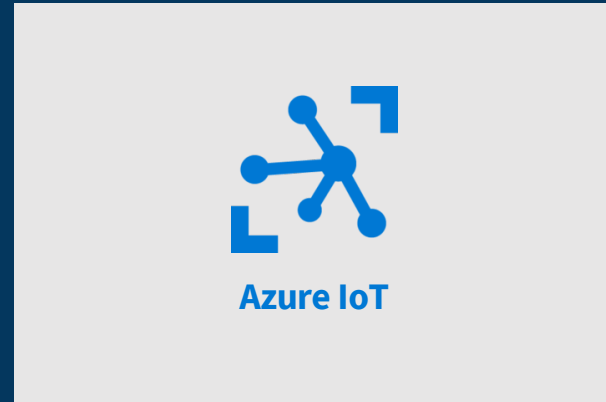
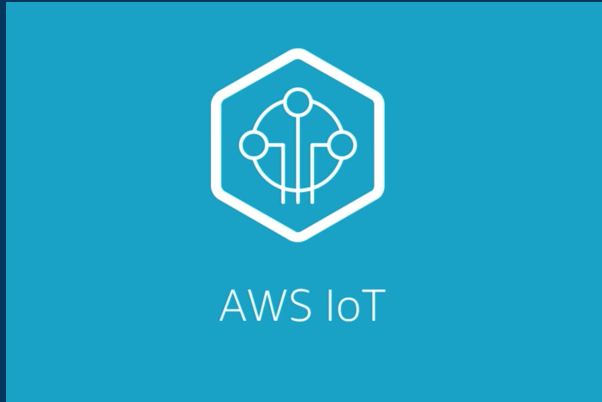


Other IoT Options

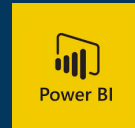
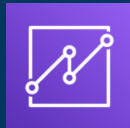
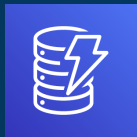
- Google Cloud (frequently in third)
- IoT Platforms
- Other Cloud Providers
- Open-Source Tools like ThingsBoard



Why AWS and Azure?



IoT Platforms





Authenticating IoT Devices to the Cloud

- Symmetric keys (Azure only)
- Standalone X.509 certificates
- X.509 certificate chain / PKI

- Other mechanisms
 - Device claiming (Azure Sphere)
 - TPM attestation



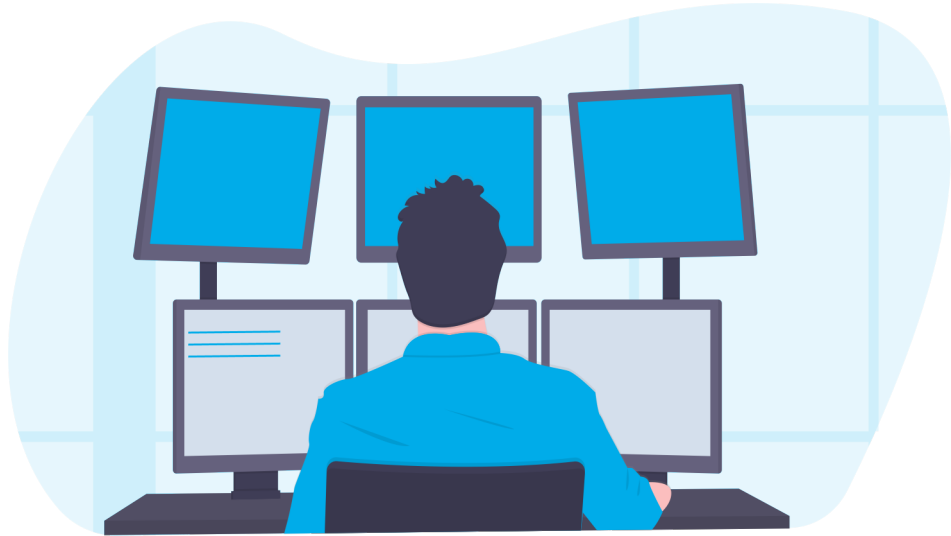
Device Authorization Mechanisms

Azure

- Shared Access Policies
- Downstream actions through IoT Hub

AWS

- IoT Core Policies
- AWS IAM Policies and Roles
- STS Tokens



X.509 Authentication



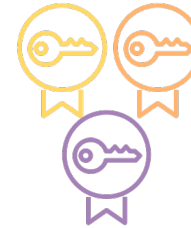
Root Certificate

- Creates signing certificates
- Registered with the cloud provider



Signing Certificate(s)

- Creates trusted device certificates



Leaf/Device Certificates

- Authenticates the device
- Stored securely on the device

X.509 Authentication

AWS IoT Core

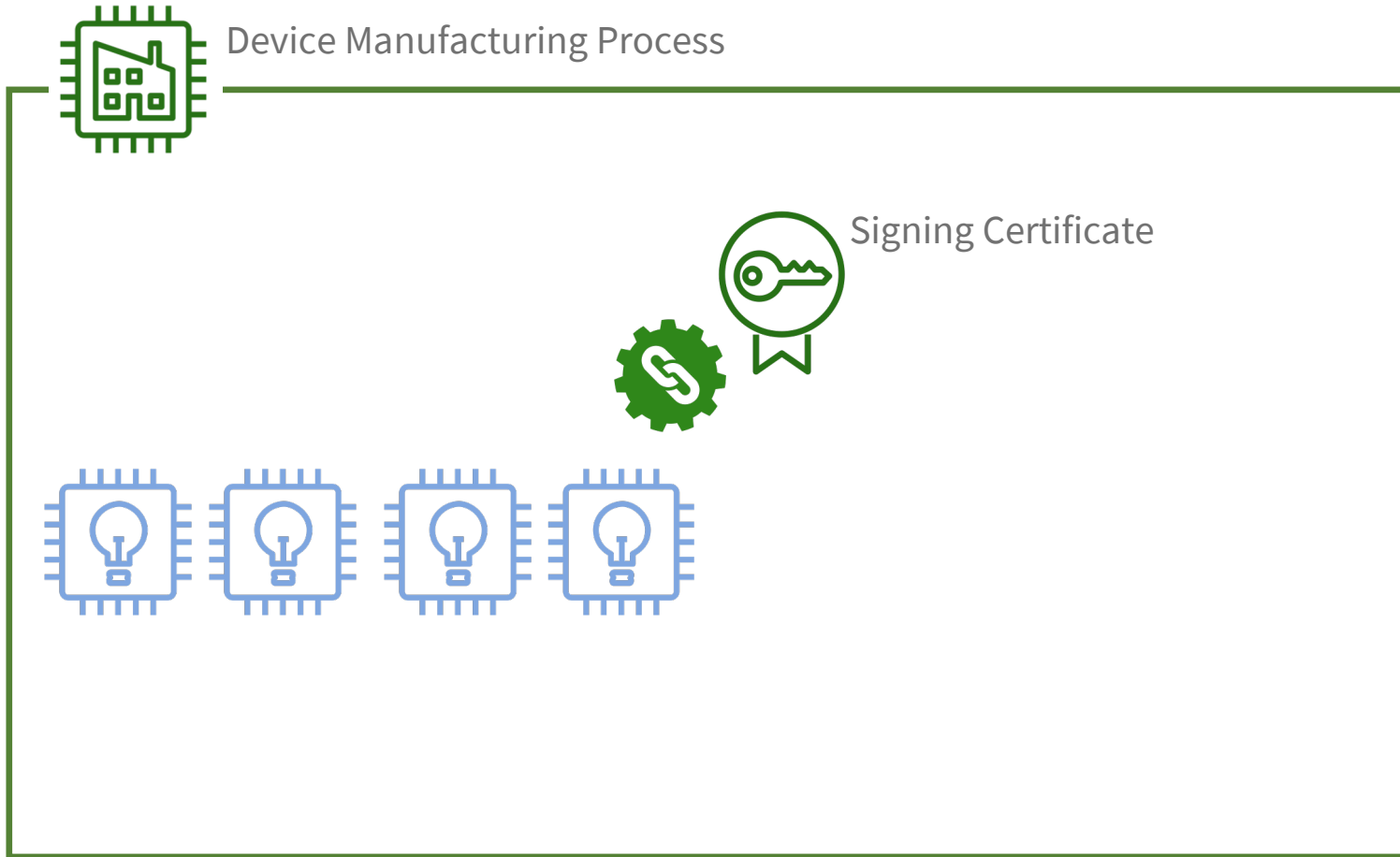


Root Certificate

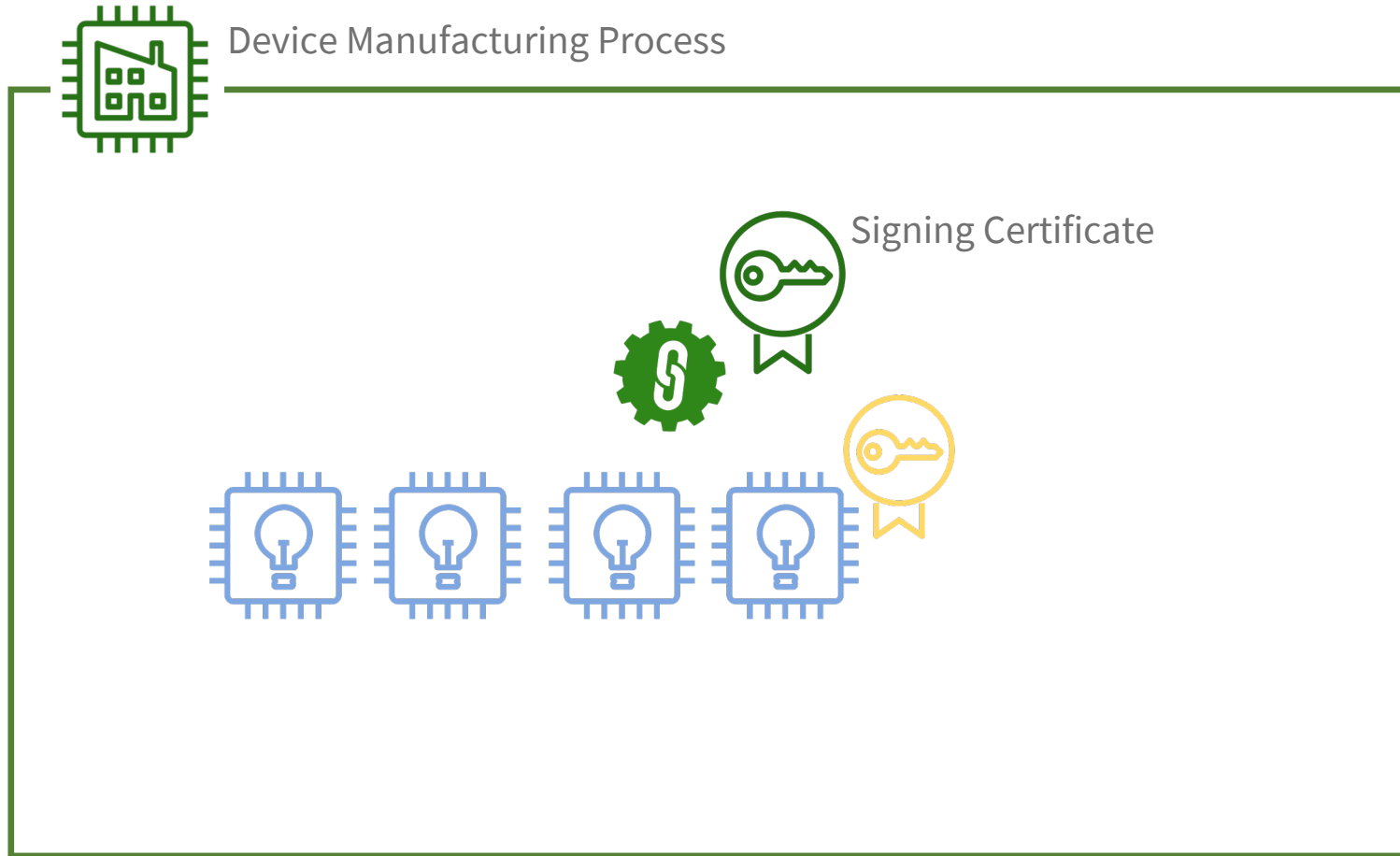


Signing Certificate

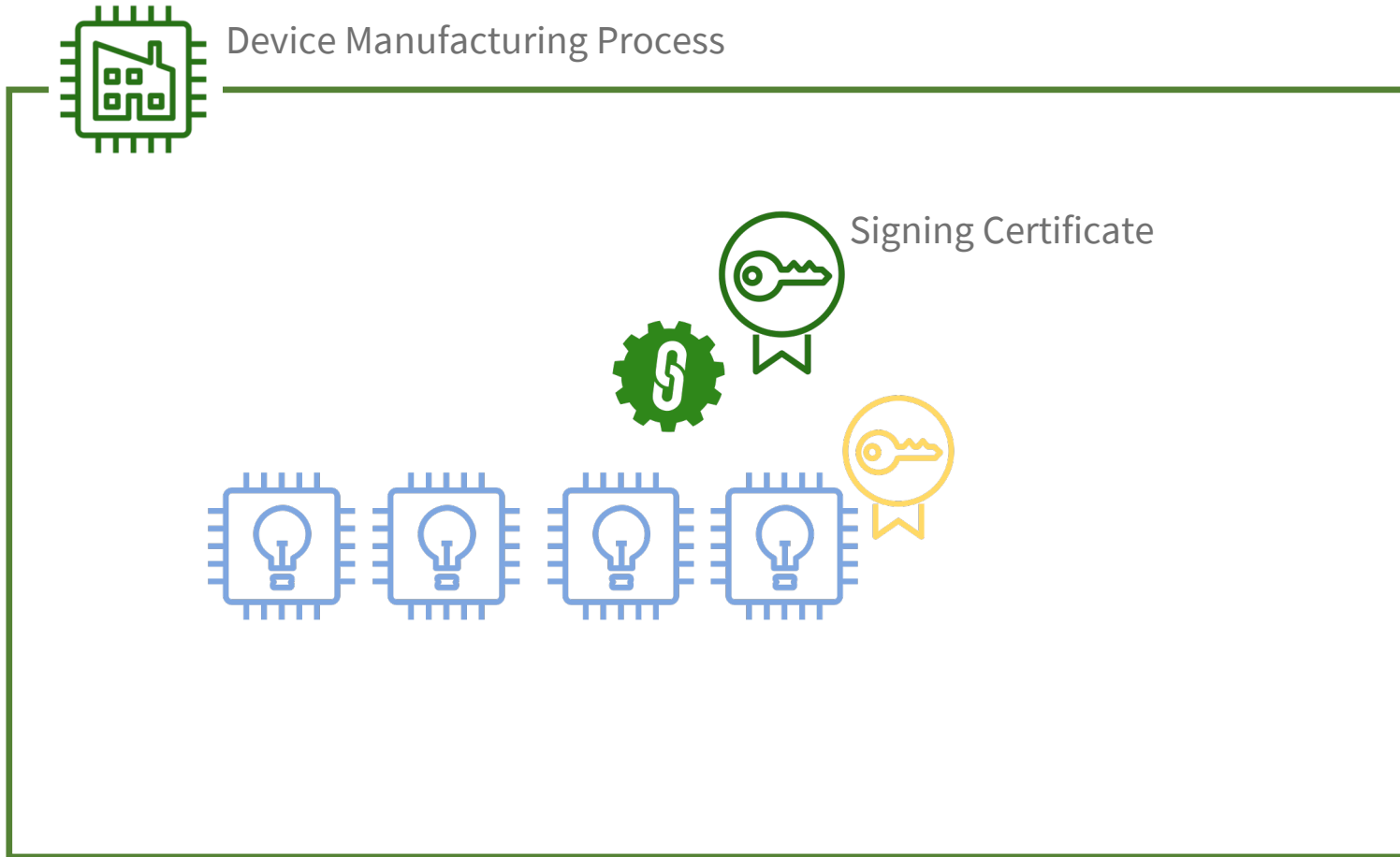
X.509 Authentication



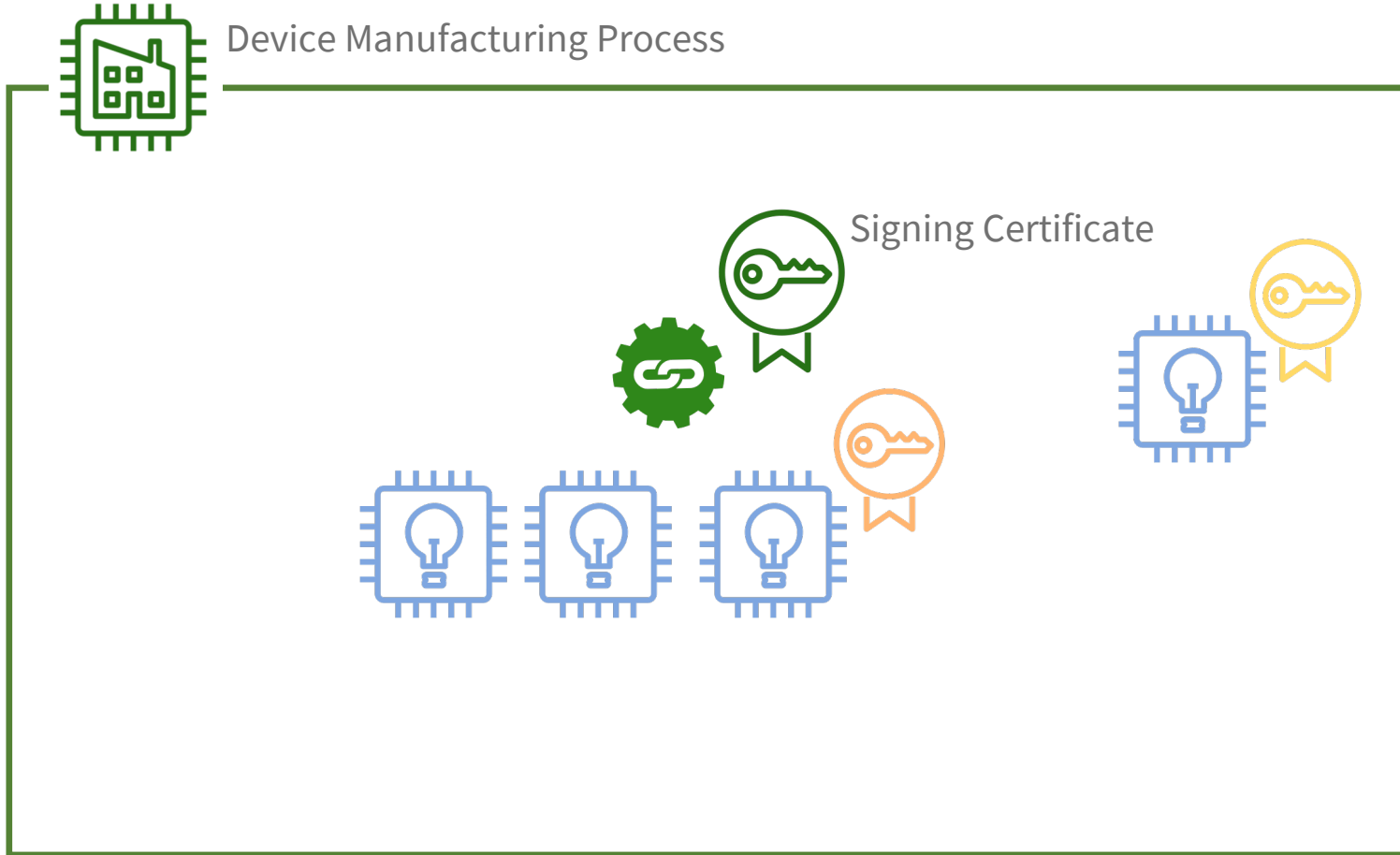
X.509 Authentication



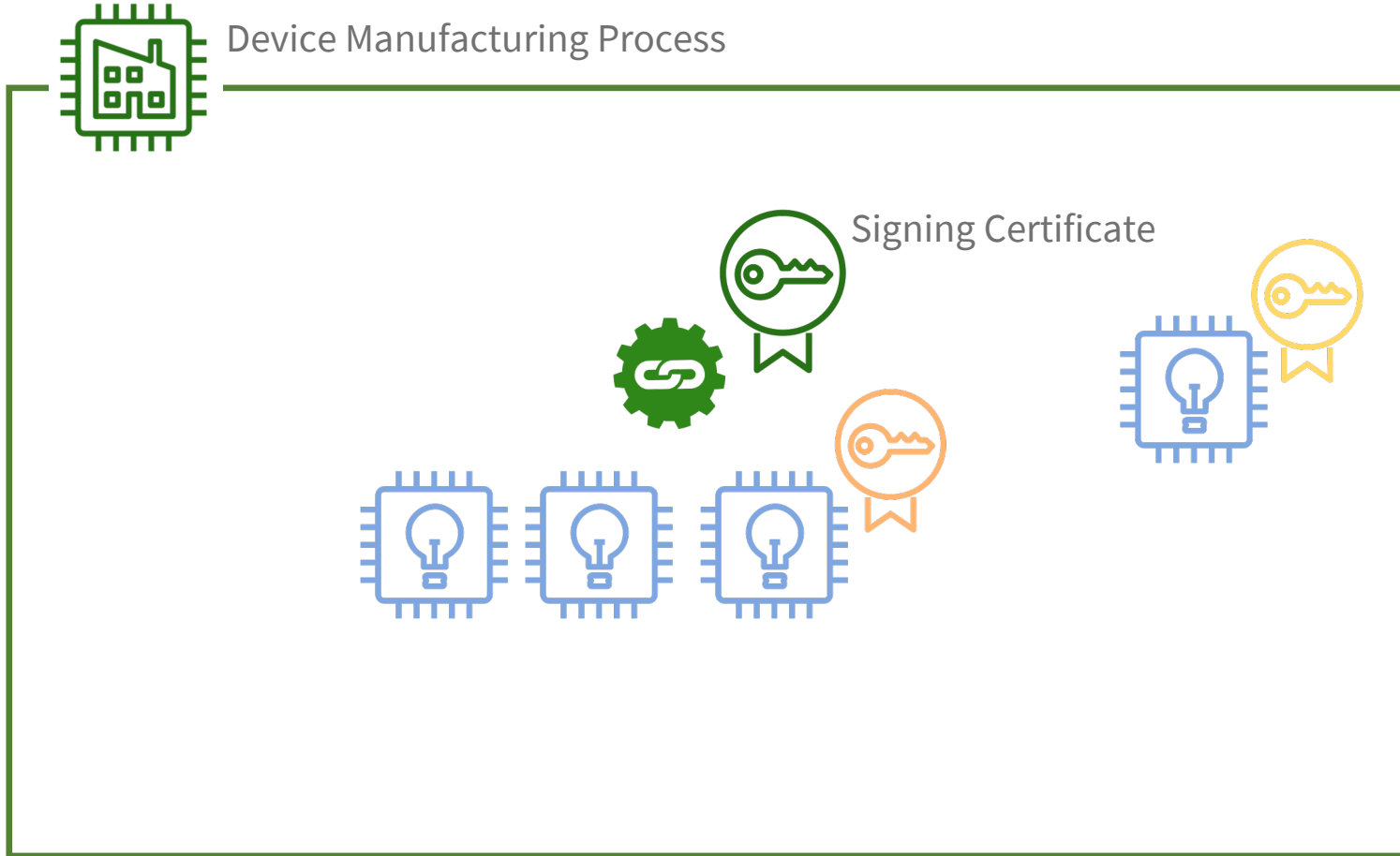
X.509 Authentication



X.509 Authentication



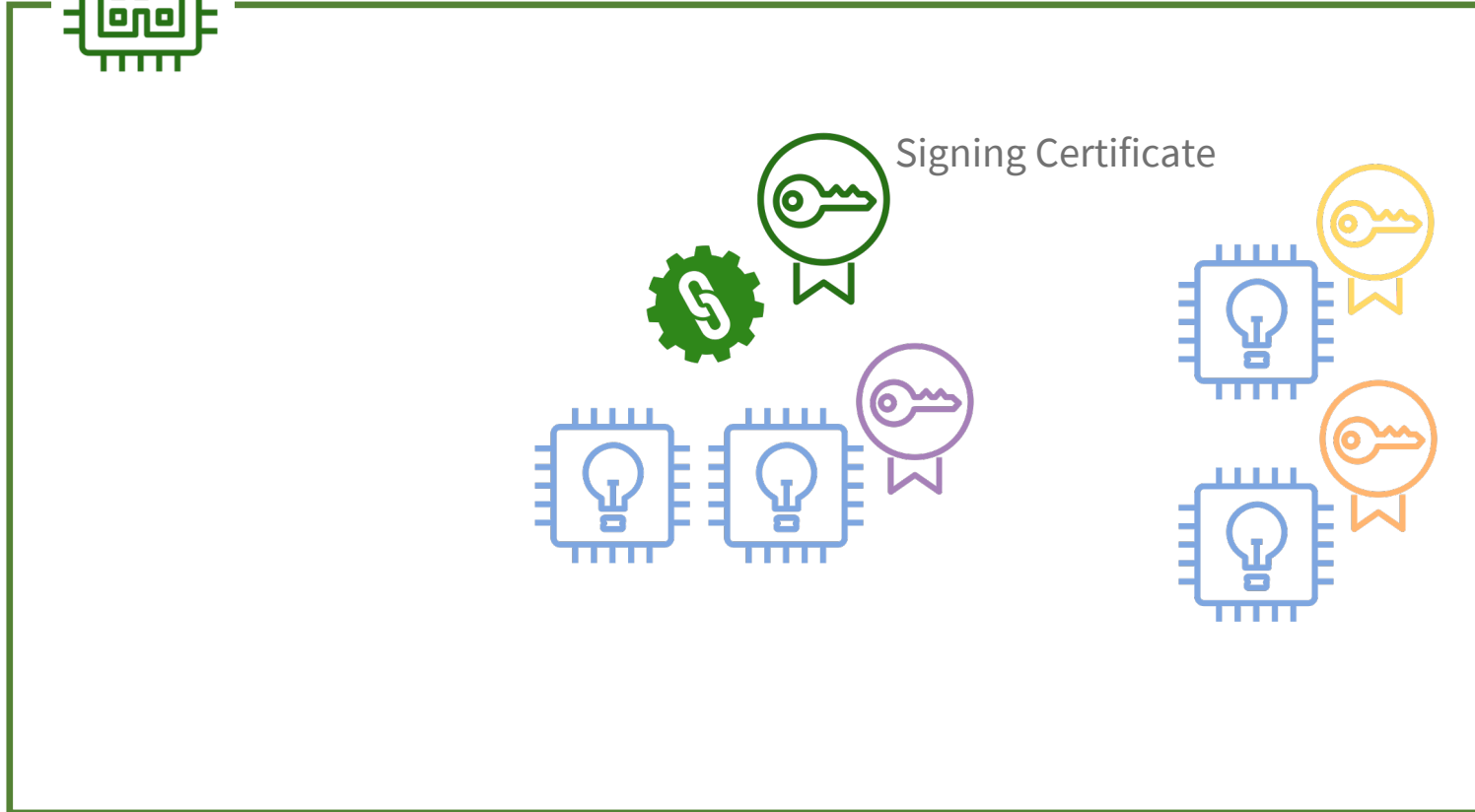
X.509 Authentication



X.509 Authentication



Device Manufacturing Process

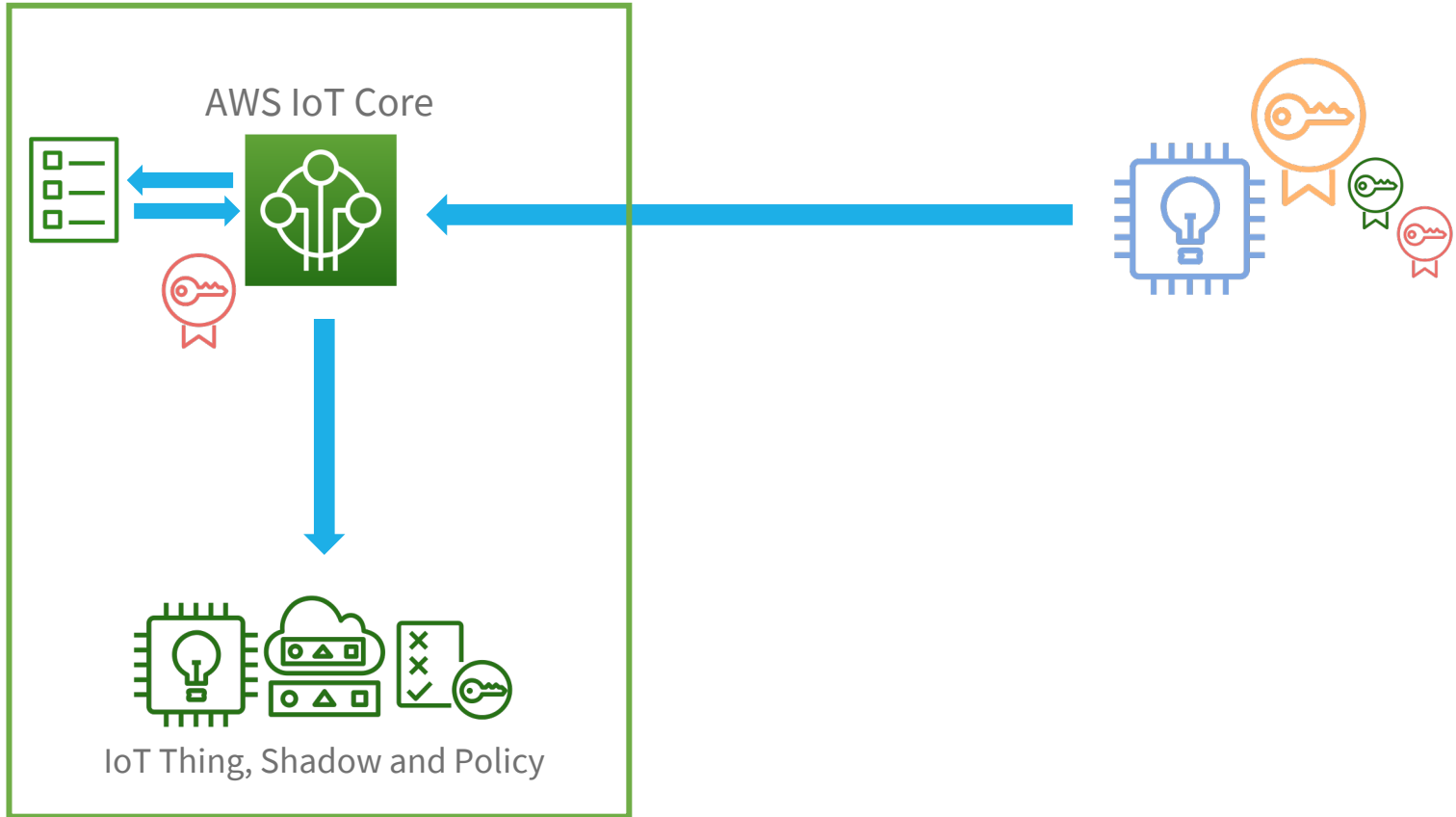


Signing Certificate

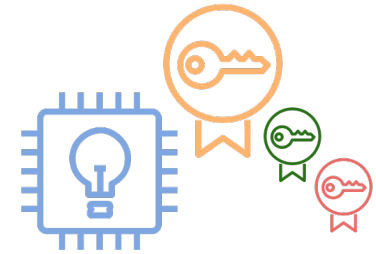
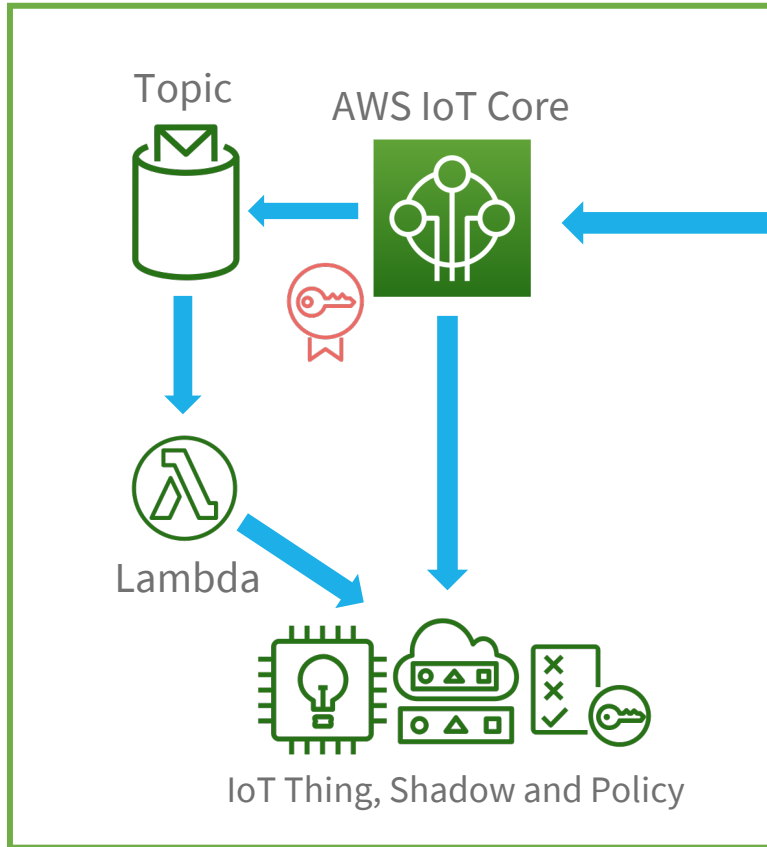
Device Provisioning - AWS

- 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

AWS Device Provisioning - JITP



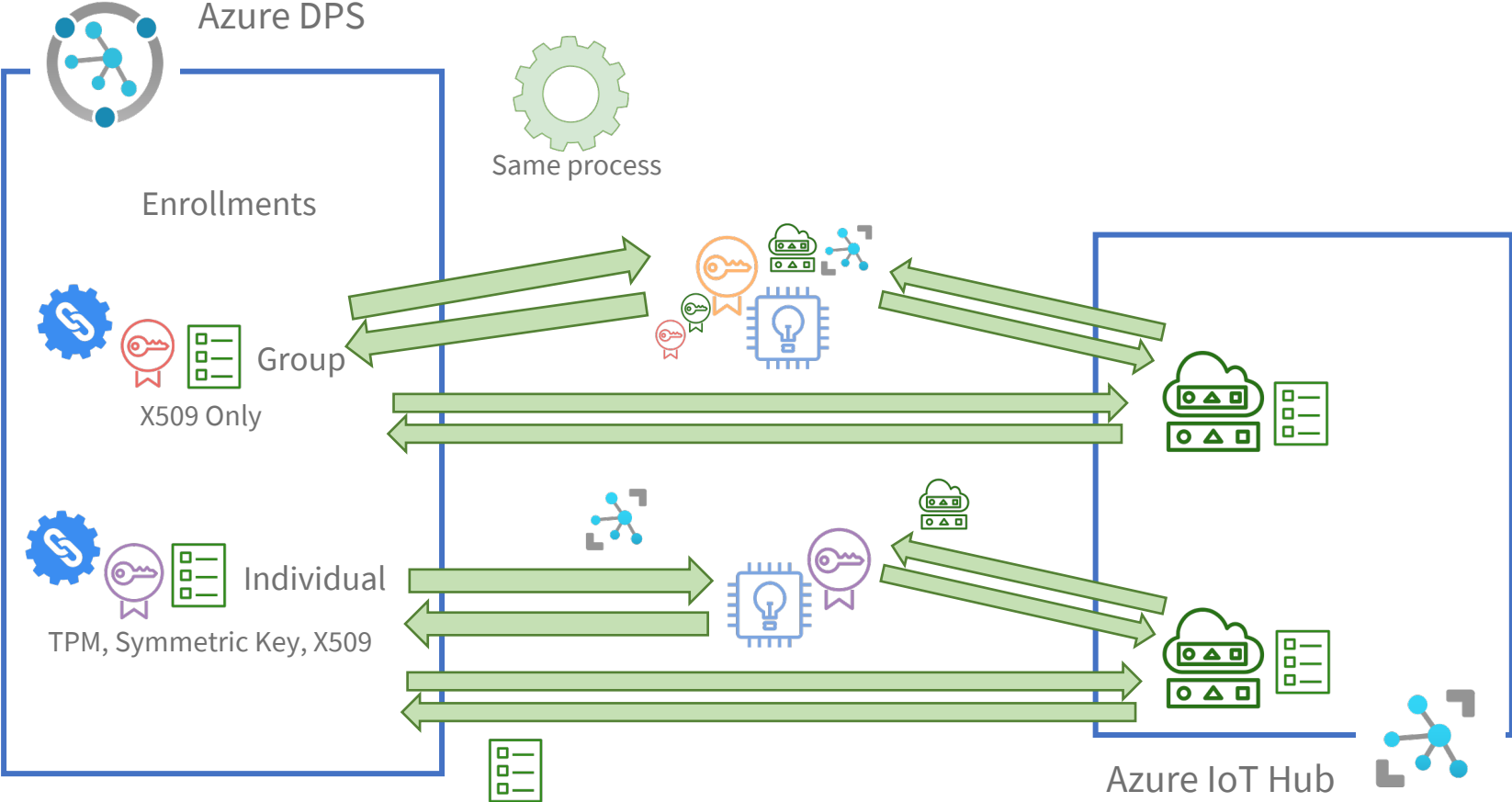
AWS Device Provisioning - JITR



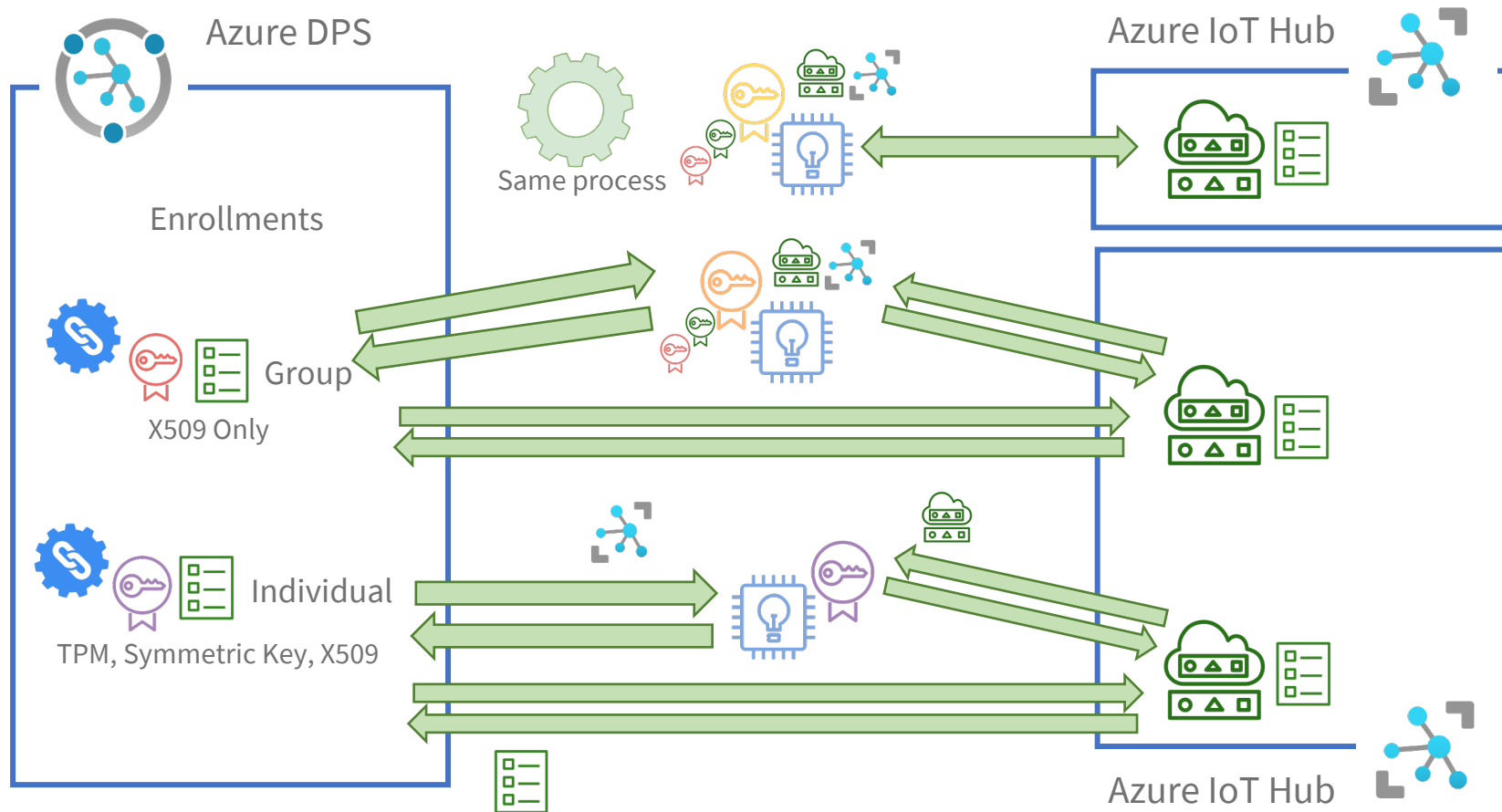
Device Provisioning - Azure

- Manually register devices and certificates in Azure IoT Hub
- Azure Device Provisioning Service
 - Enrollment lists of devices to be registered
 - Configuration of devices when they register
- Other Azure DPS benefits
 - Load balancing between IoT Hubs
 - Multitenancy provisioning
 - Latency-based provisioning
 - Key rotation

Azure Device Provisioning Process – DPS



Azure Device Provisioning Process – DPS



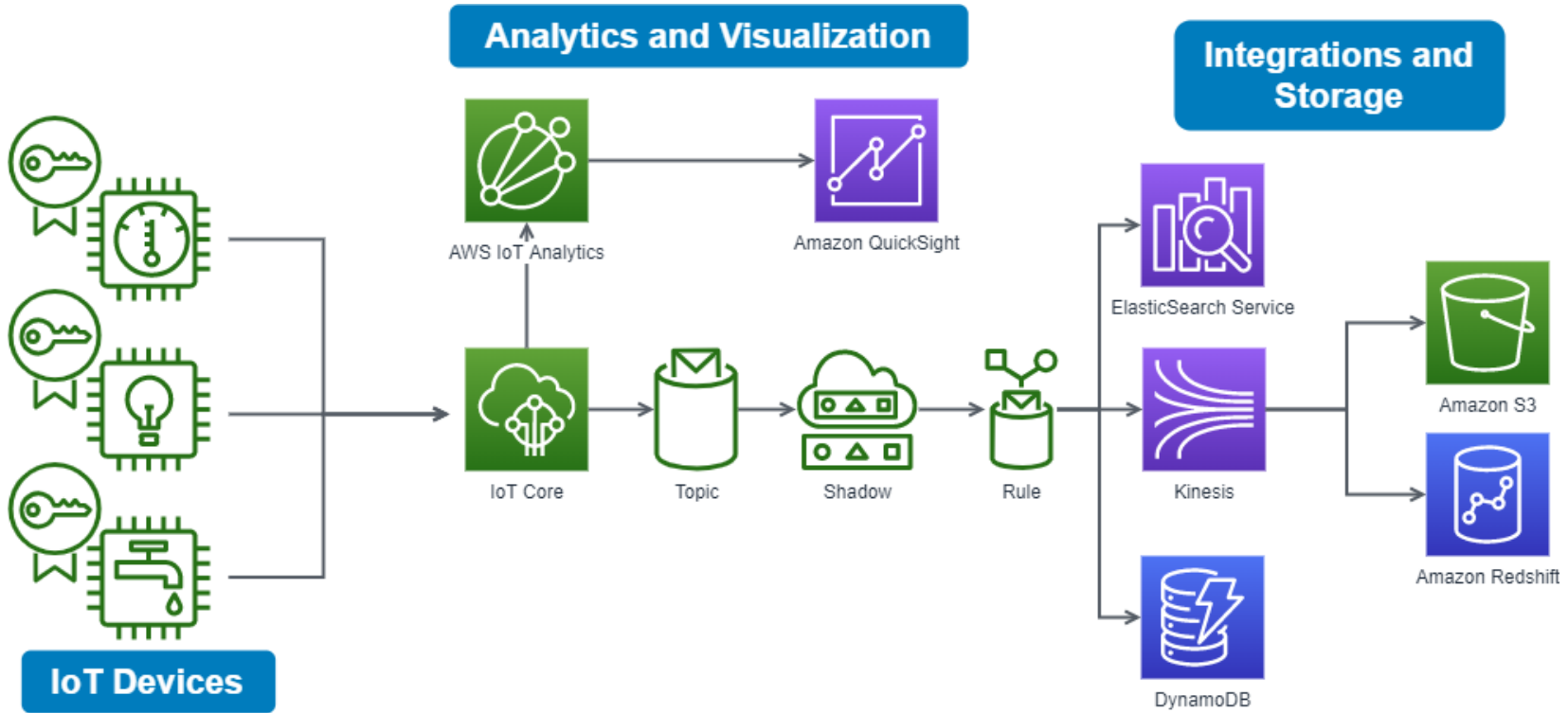


3.

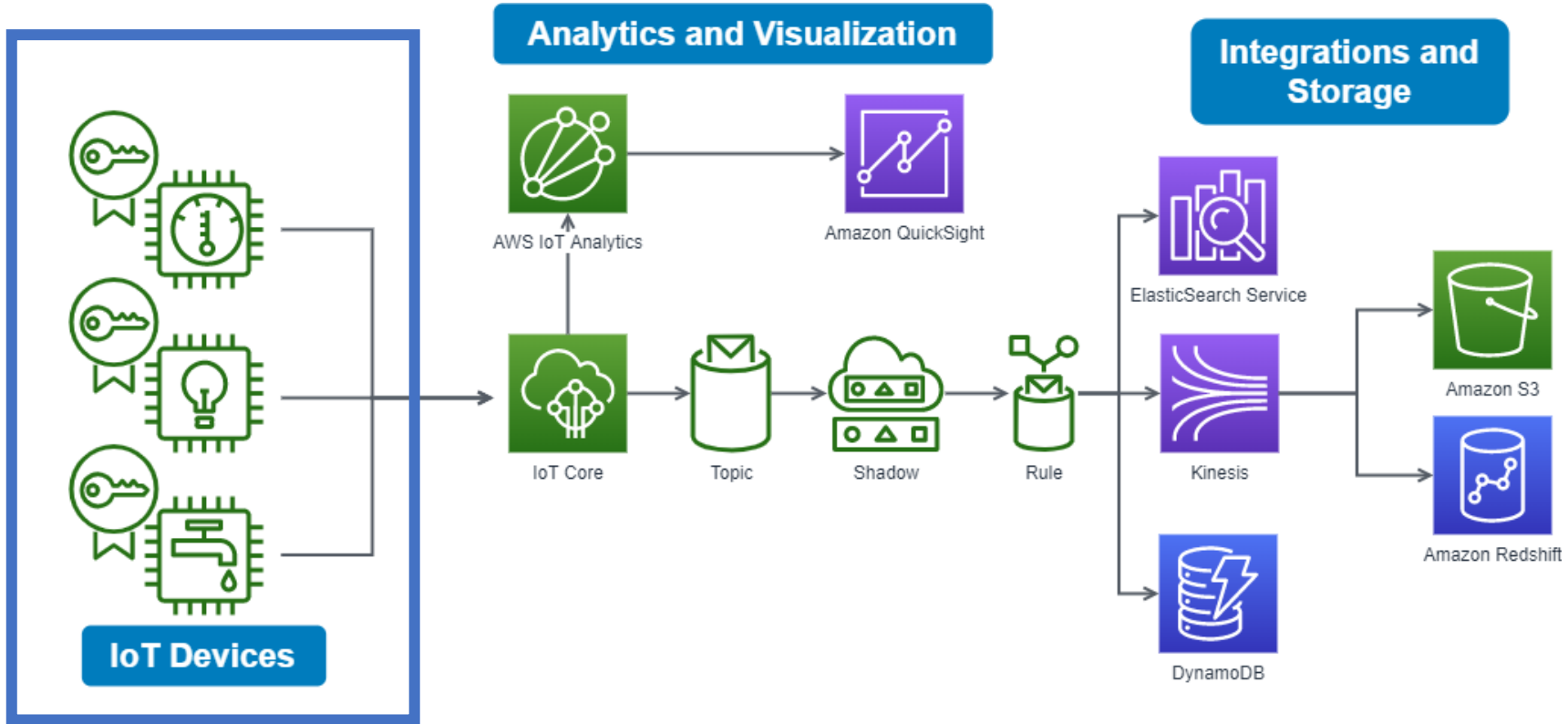
**Sample IoT Architectures
and Use Cases**



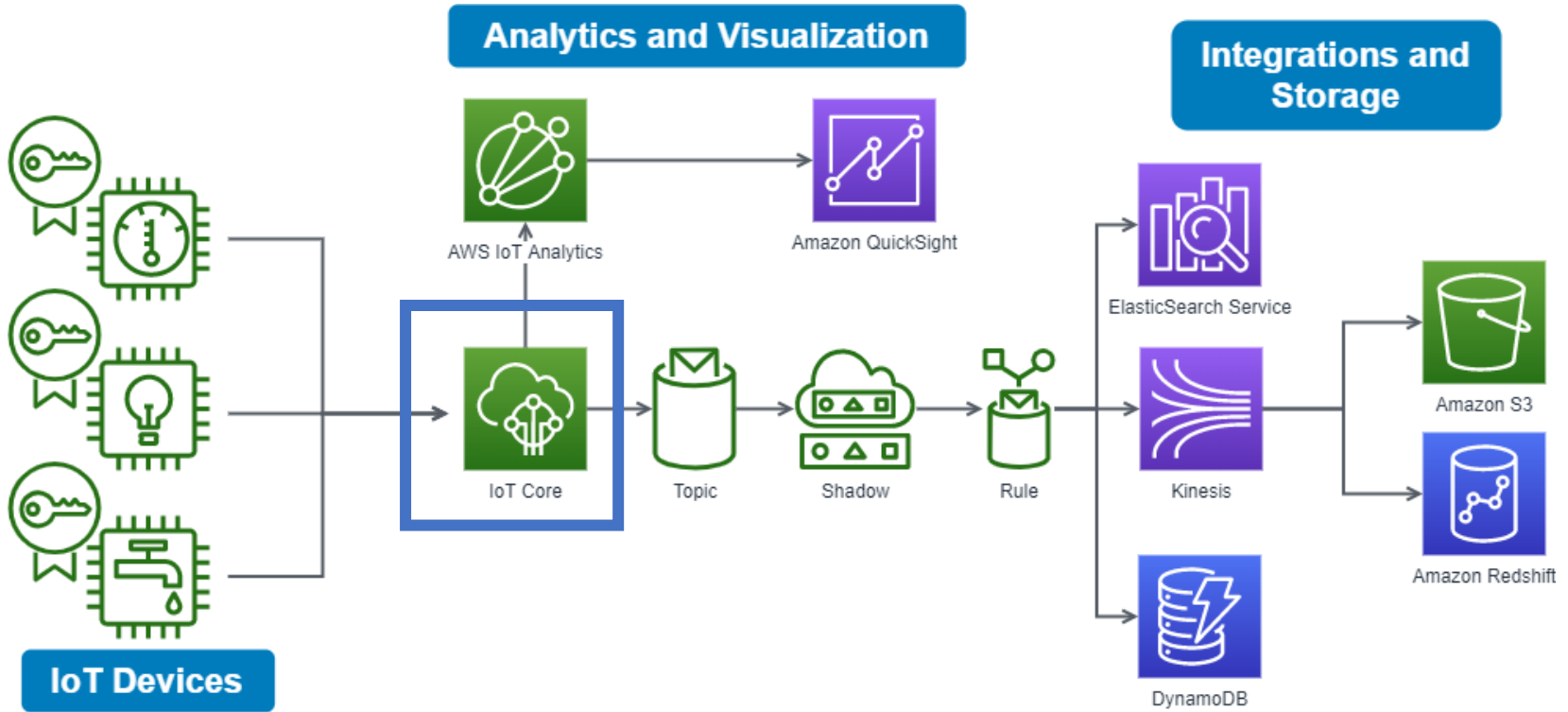
AWS Architecture: Device Fleet Analytics



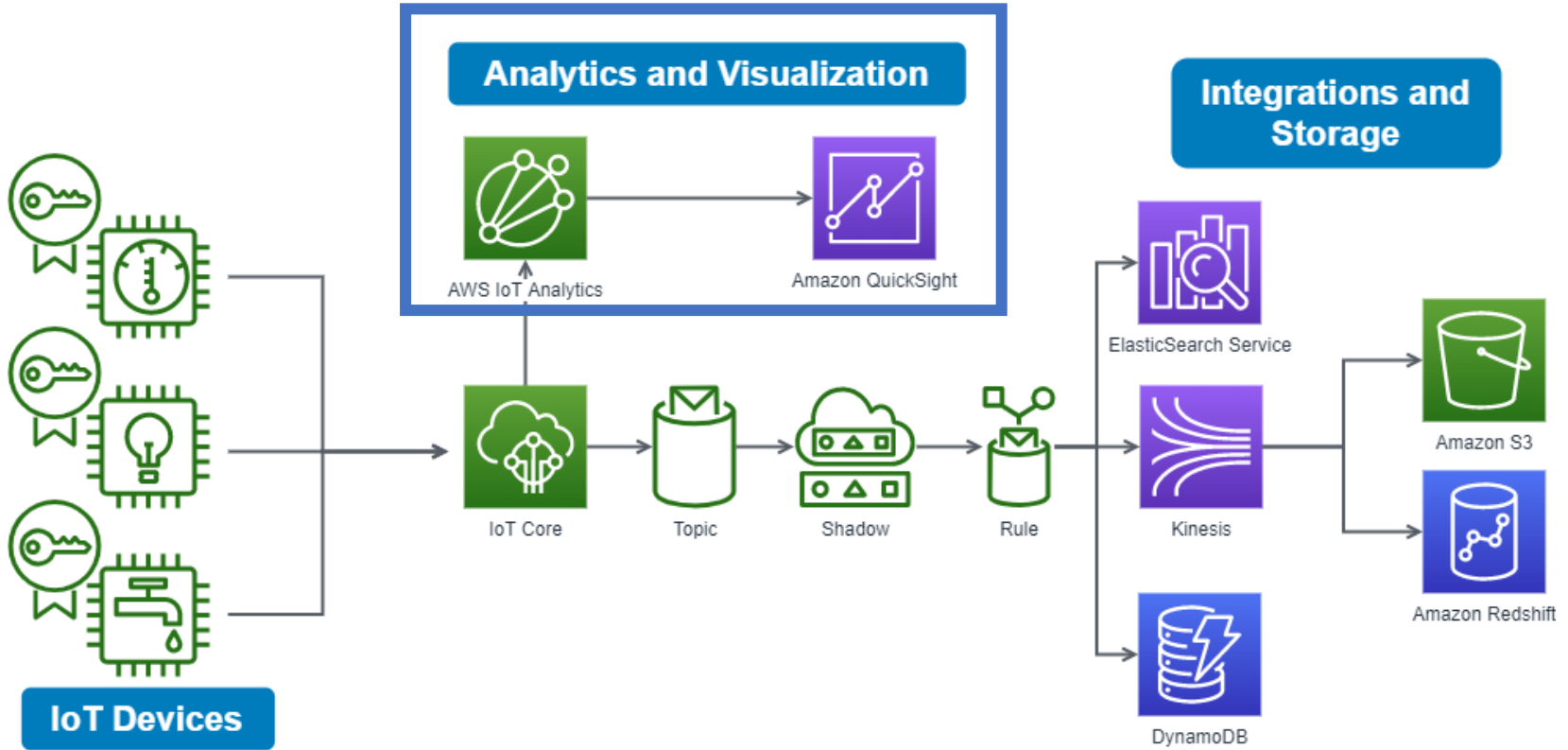
AWS Architecture: Device Fleet Analytics



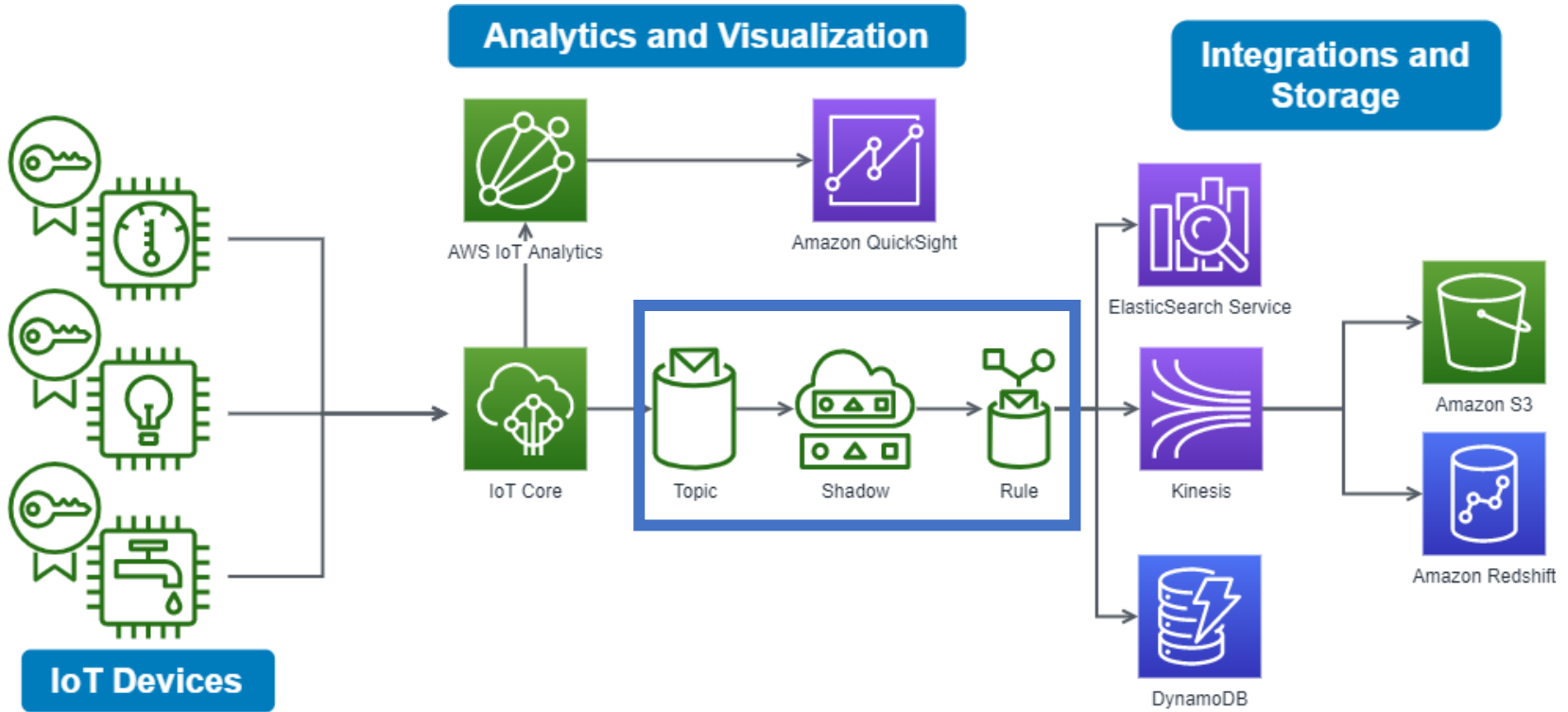
AWS Architecture: Device Fleet Analytics



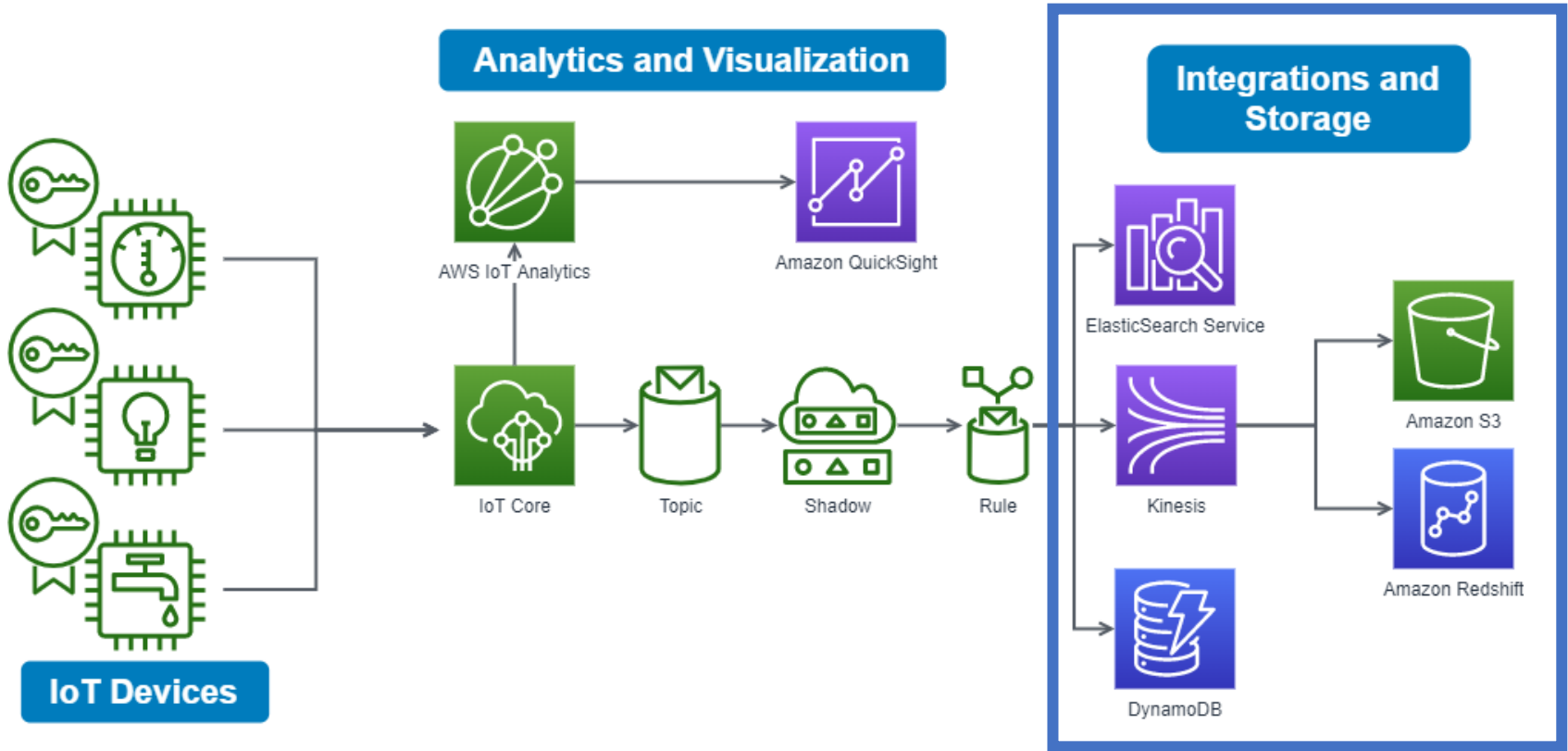
AWS Architecture: Device Fleet Analytics



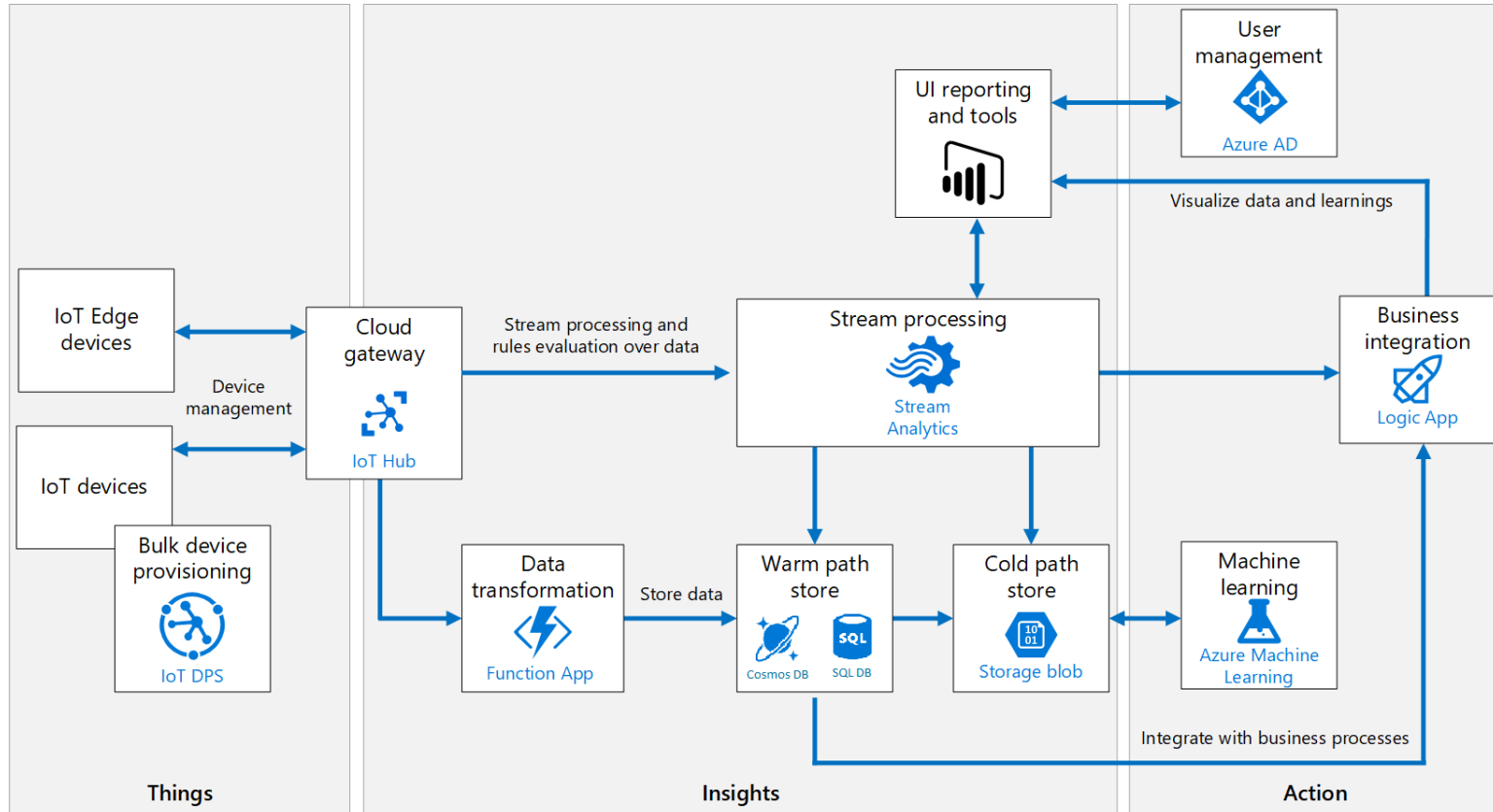
AWS Architecture: Device Fleet Analytics



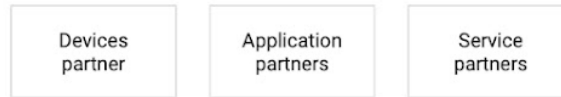
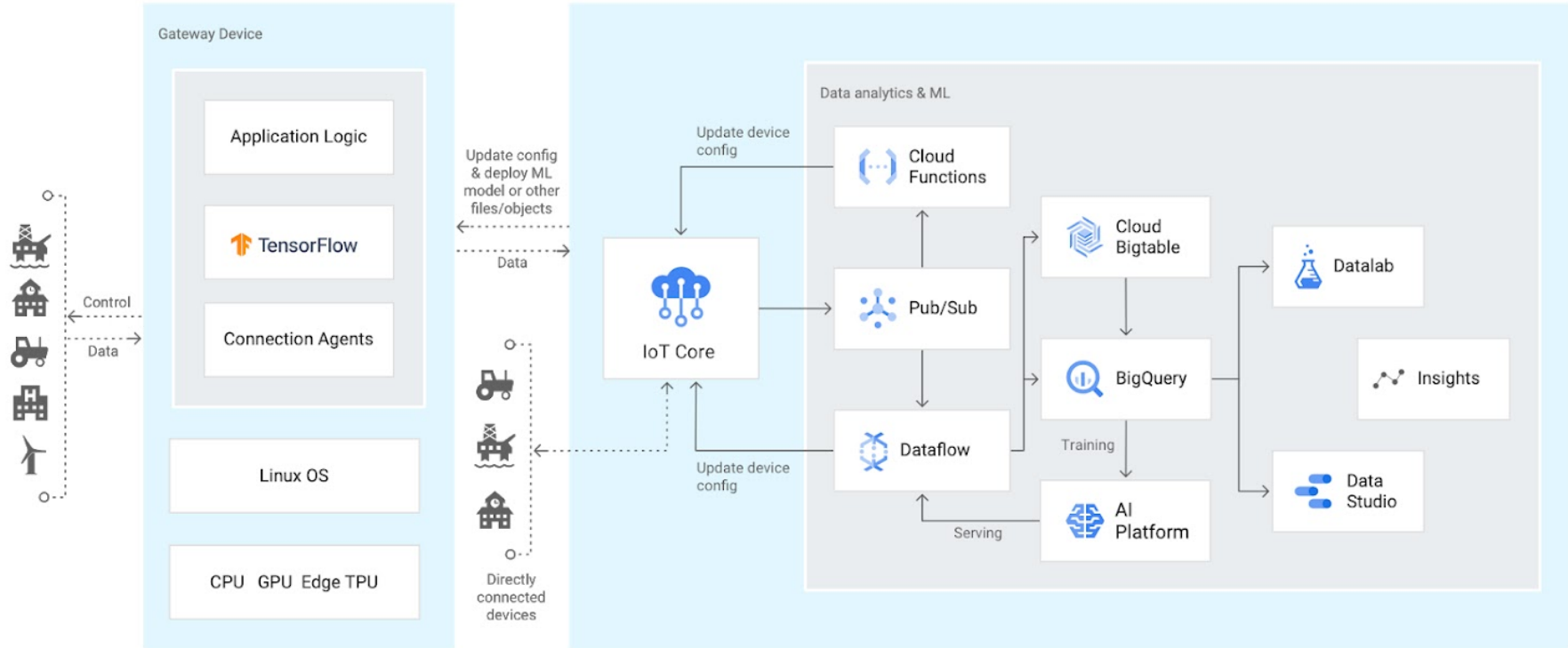
AWS Architecture: Device Fleet Analytics



Comparable Azure Architecture



Bonus: Comparable GCP Architecture



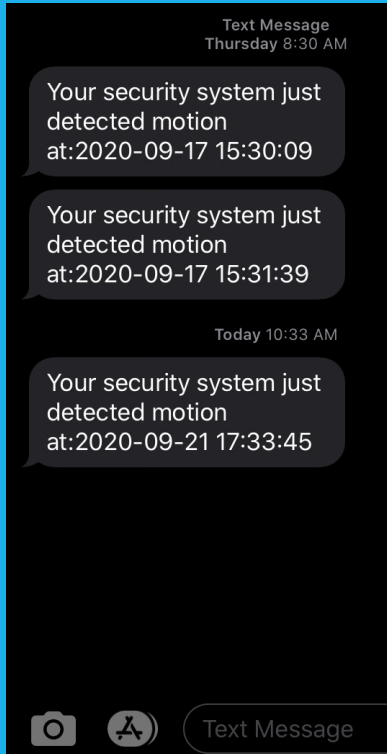
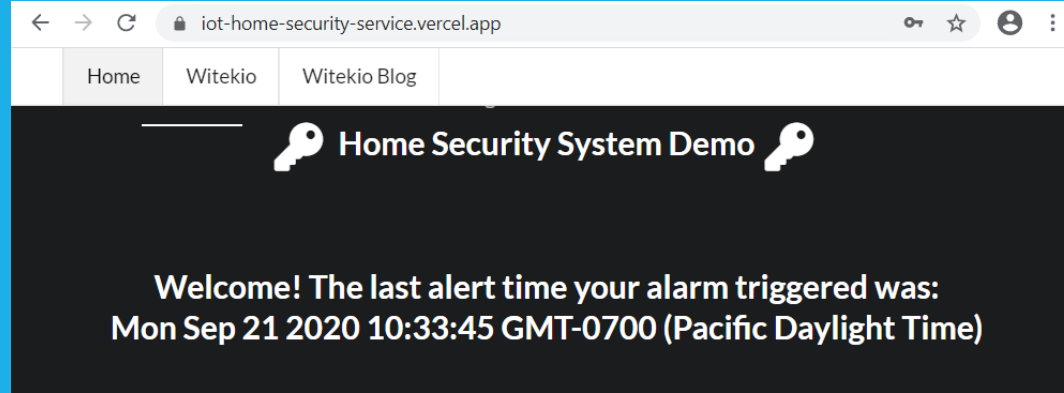
<https://cloud.google.com/iot-core>



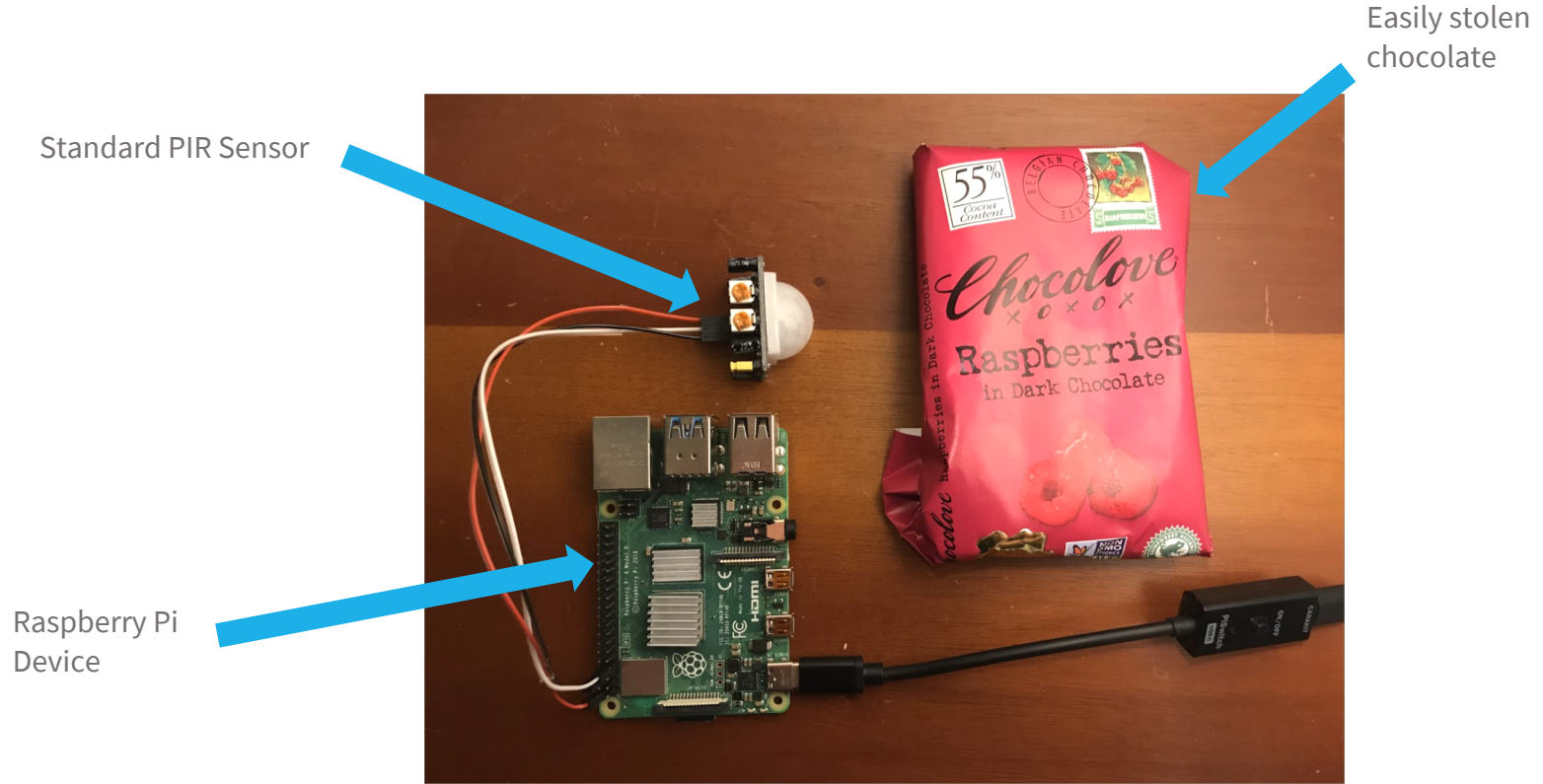
4.

**Demos:
The Cloud Side of IoT**

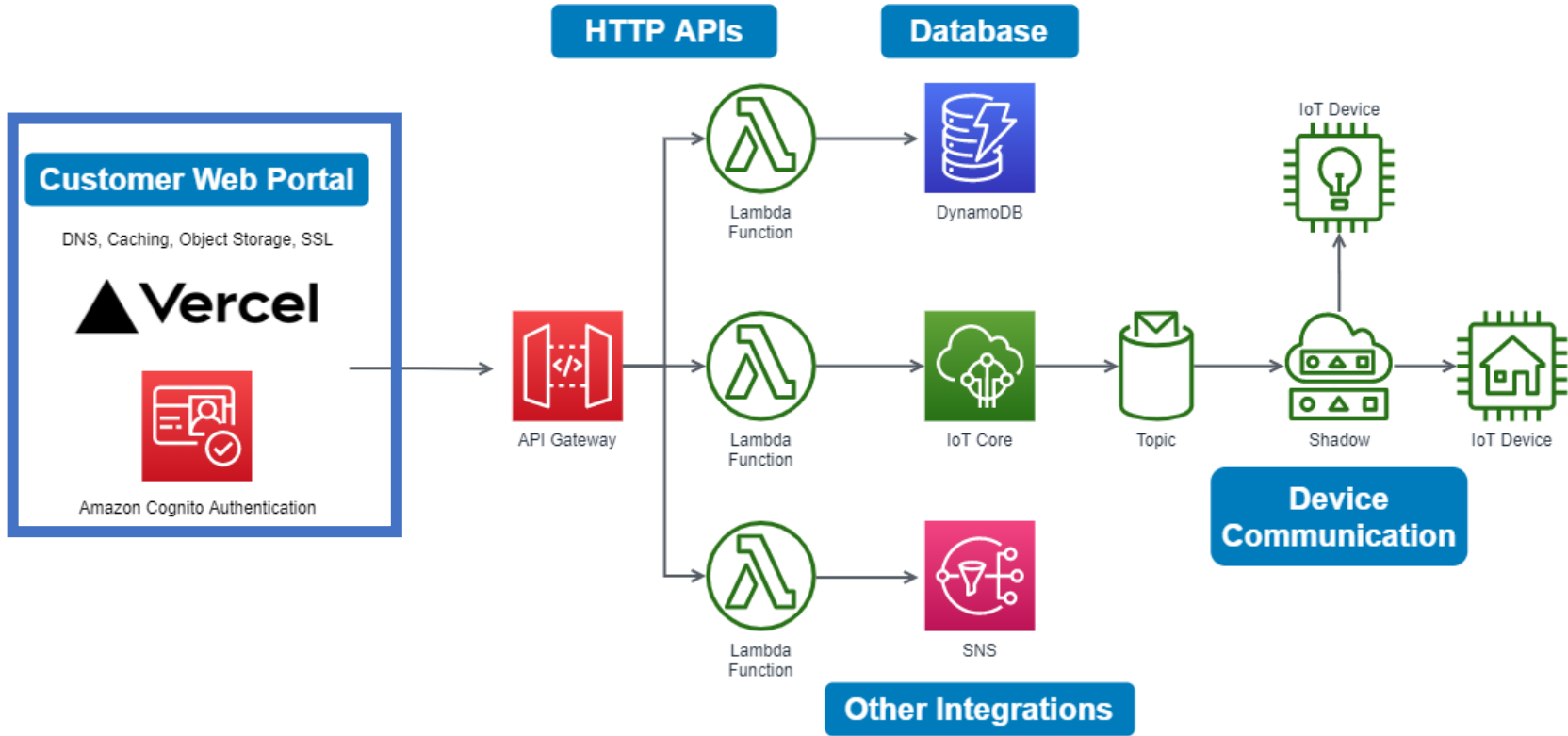
Demo 1 – Chocolate Security System with AWS



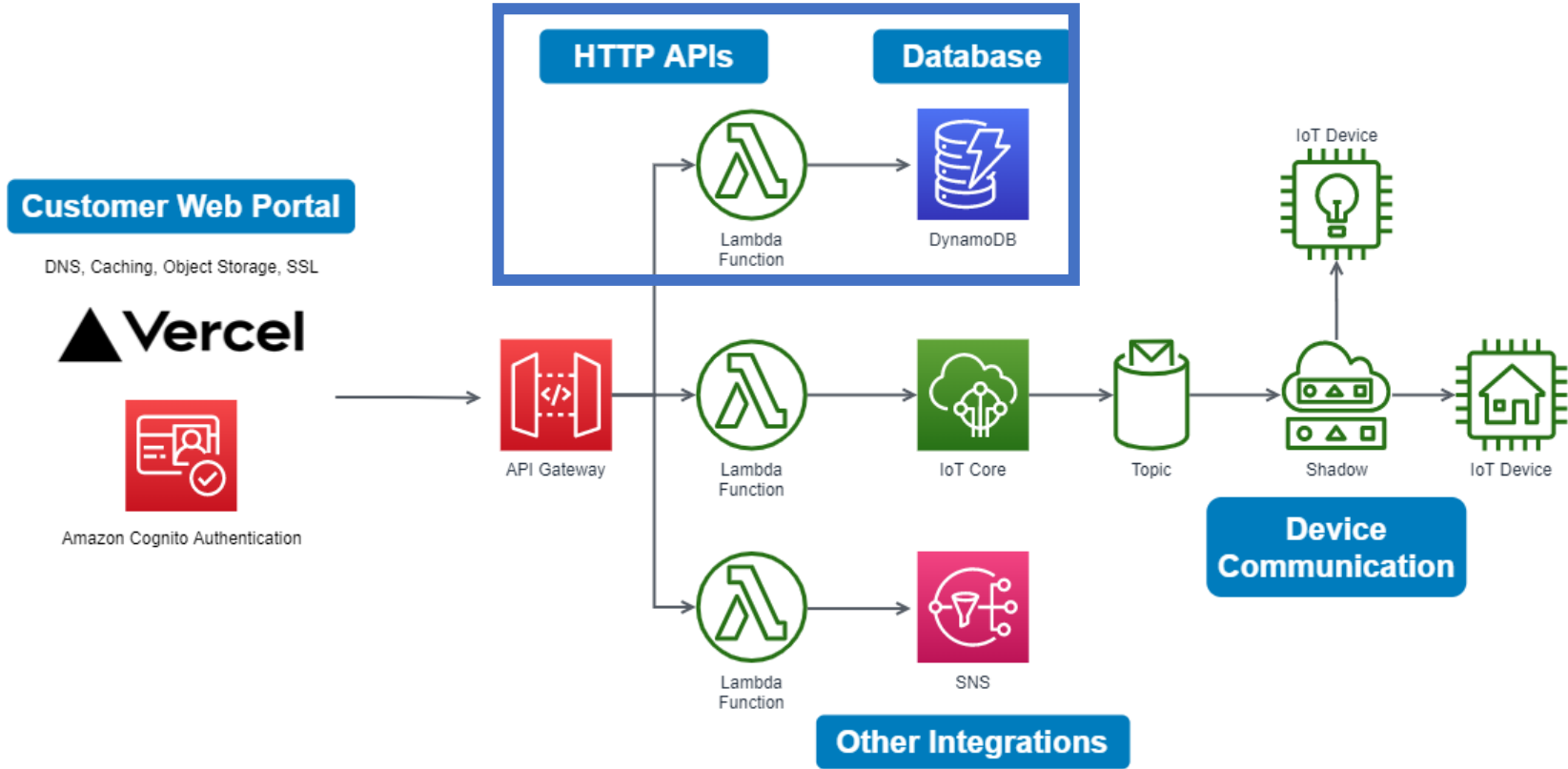
Hardware Architecture – “Chocolate Sensor”



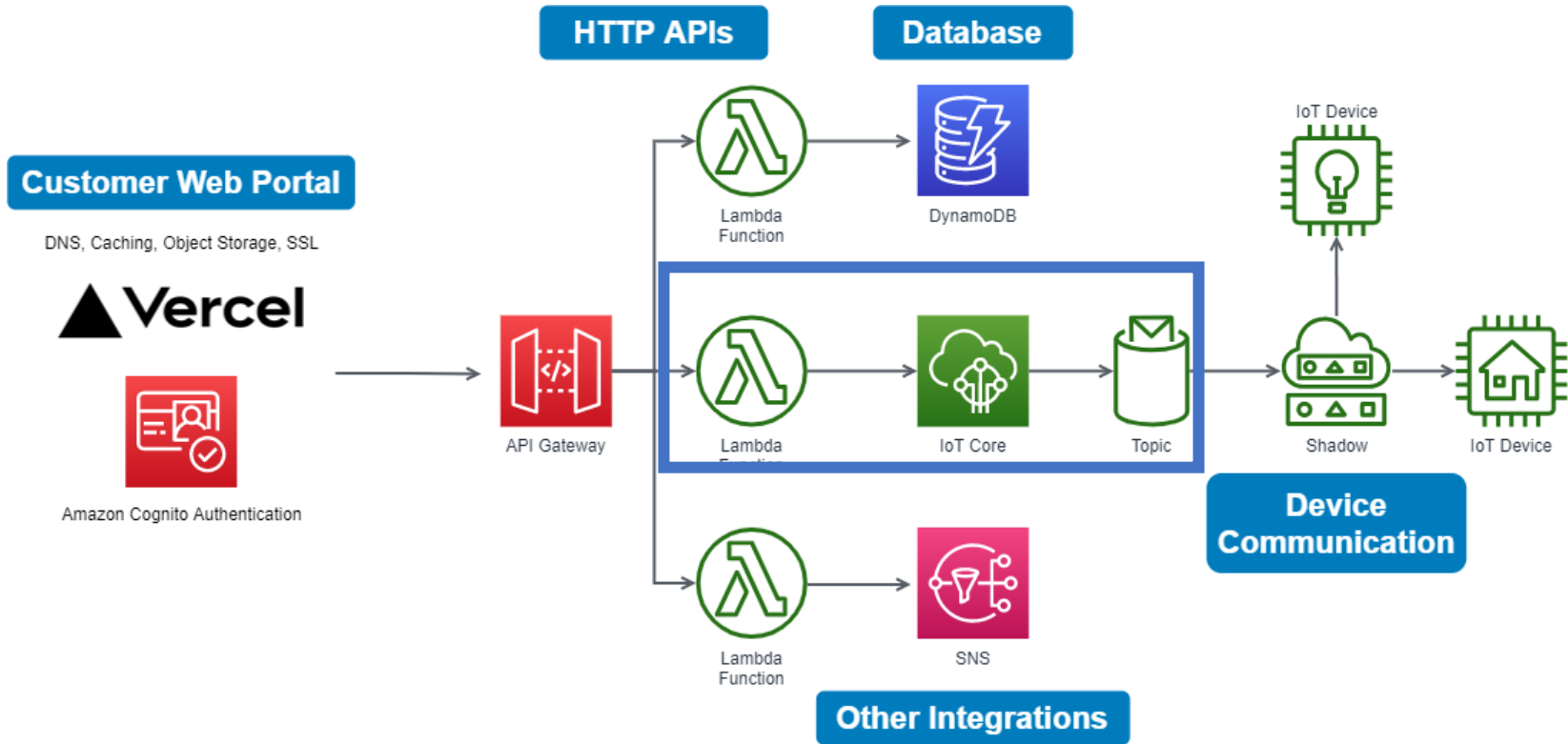
Cloud Architecture



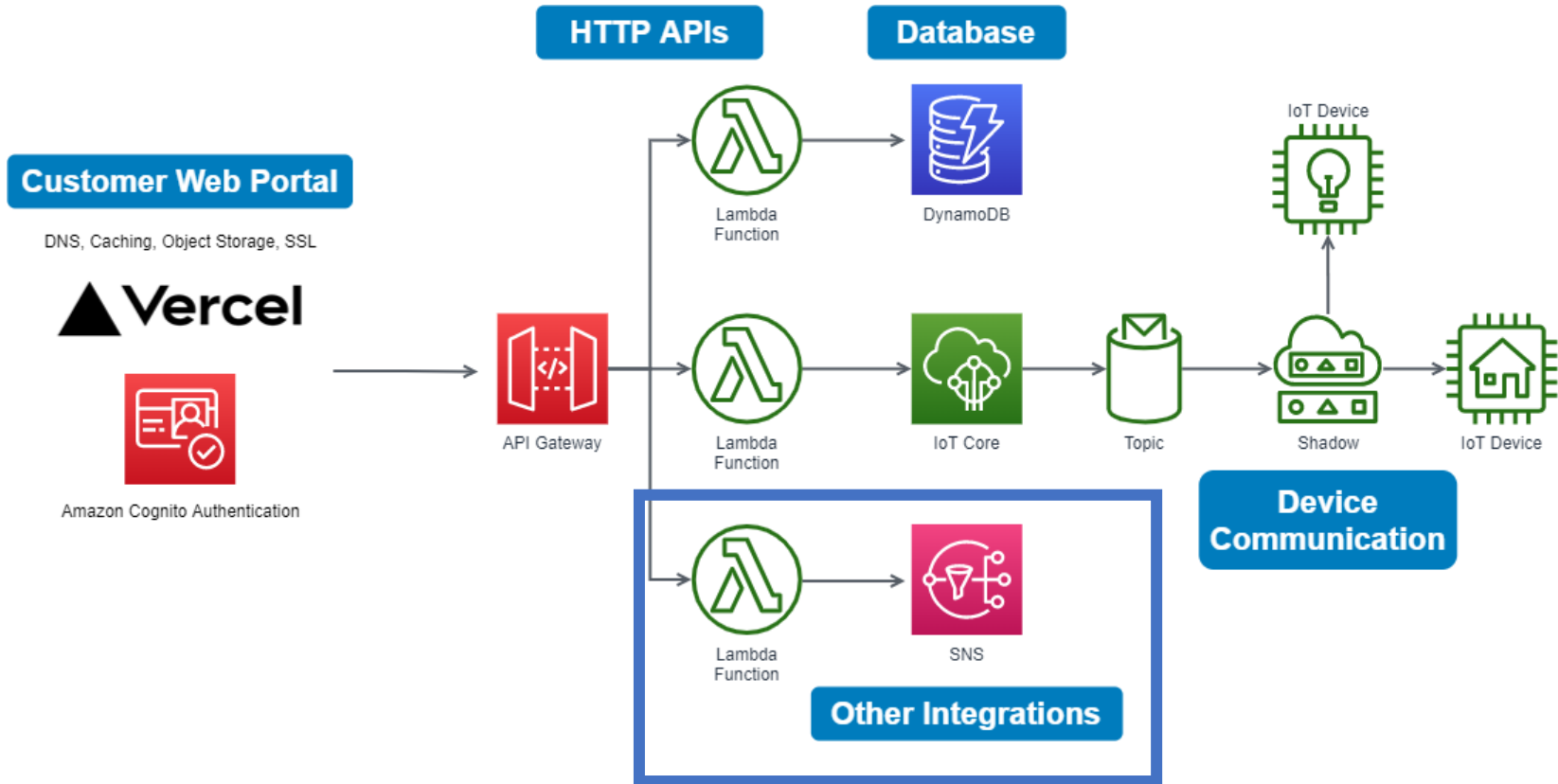
Cloud Architecture



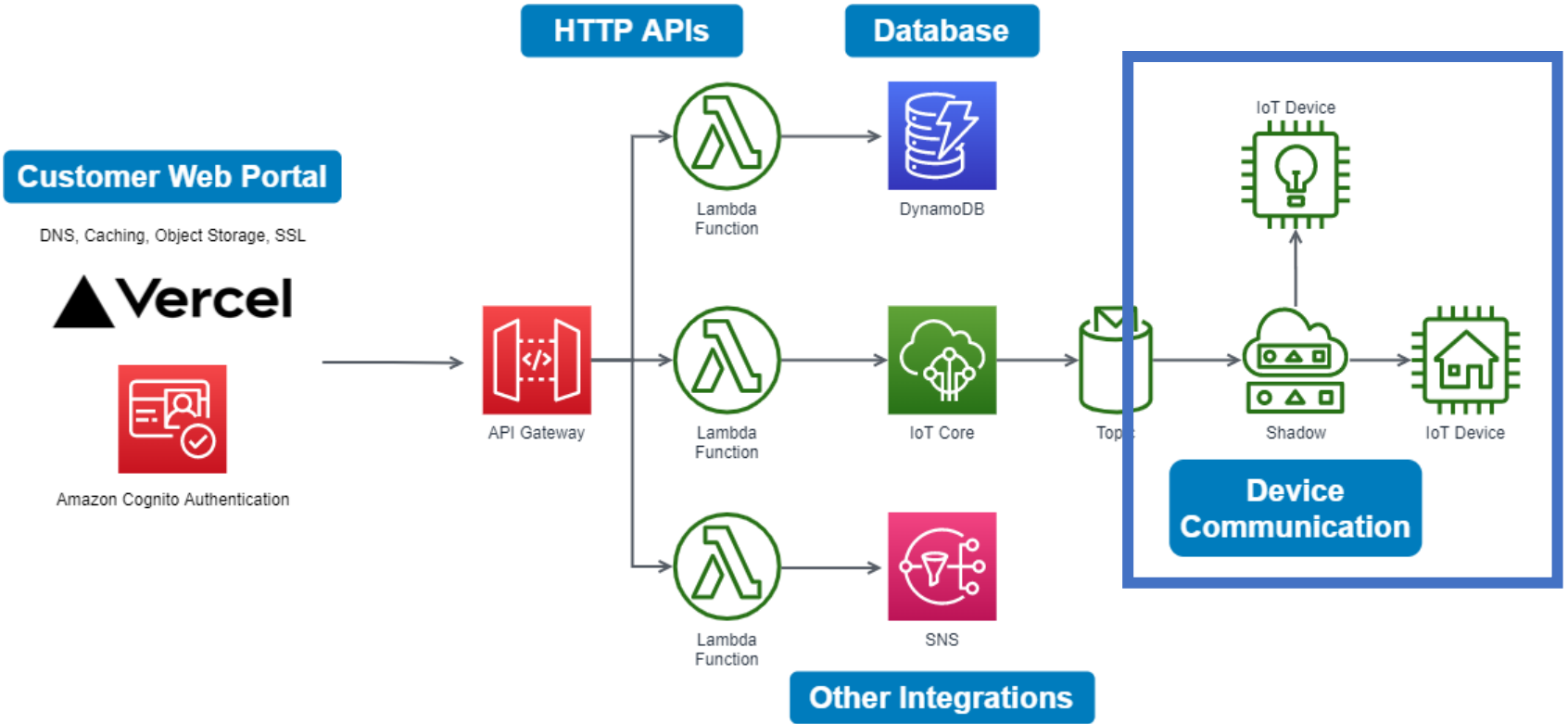
Cloud Architecture



Cloud Architecture



Cloud Architecture



Our Application Code



```
$ tree -L 1
```

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

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
```

Frontend



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

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

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
```



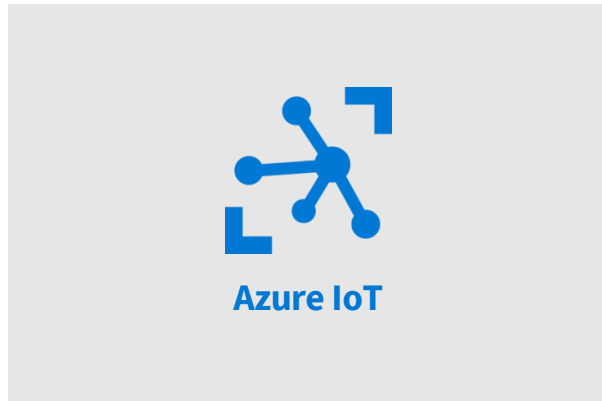
5.

Cost Optimization

Azure and AWS IoT Cost Optimization

Azure IoT Hub

- Select the tier you need (basic vs. standard)
 - Do you need bidirectional communication or not?
- Tune the number and type of IoT Hub units
- Setup auto-scaling for IoT Hub
- Tune device applications to reduce usage



AWS IoT Core

- Pay per request and feature pricing
- Reduce usage to only required features
- Reduce connectivity, messages, bundle data
- Optimize message sizes for metering
 - 8 KB message, 5 KB metering, charged at 10 KB



General Cloud Cost Optimization



Right sizing

- Appropriate instance sizes
- Appropriate capacity units

Purchasing Options

- Spot instances
- Reserved instances
- Reserved capacity

Utilization

- Managed services
- Auto scaling
- Load balancing

Buffering

- Stream data processing
- Buffer data in queues

Specific Optimization Examples

IoT Hub Tiers (Azure)

- Basic Tier Units \$10-\$500/mo
- Standard Tier S1 Units \$25-\$2500/mo
- 60-80% cost reduction

IoT Core Pricing (AWS)

- Pay per request
- Pay per utilization of specific features
- Optimize applications to reduce utilization

S3 Storage Classes (AWS)

- Standard storage - \$0.023/GB
- Glacier Deep Archive - \$0.00099/GB
- Creating appropriate lifecycle policies

Blob Storage Access Tiers (Azure)

- Premium, Hot, Cool, Archive
- Creating appropriate lifecycle policies



6.

**Start Leveraging the Cloud
for IoT**

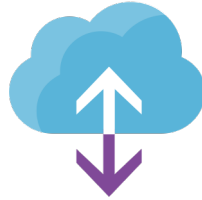


W

Leverage the Cloud for IoT



Device provisioning and management



OTA updates



Device monitoring



Telemetry and device communications



Data processing and visualization



Data storage and lifecycle management



Develop and deploy machine learning



Web applications

Questions?





Getting Started Resources:


- fernandomc.com
- witekio.com/blog

CONTACT ME

CONTACT SALES

 fmedinacorey@witekio.com

 [/in/fmc-sea](https://www.linkedin.com/company/witekio)

 witekio.com

 sid@witekio.com



**Thank
You!**

