Witekio

AN AVNET COMPANY

AWS and Azure IoT

A Look at the Possibilities of the IoT Cloud

Overview

1.

Introduction

I've used too many tools:

- AWS, Azure

- GCP, Alibaba, Tencent

- Algolia, Stripe, Auth0, Vercel, Netlify…

Work:

- I help IoT folks leverage the cloud

Lead Cloud Architect

linkedin.com/in/fmc-sea

Embedded software
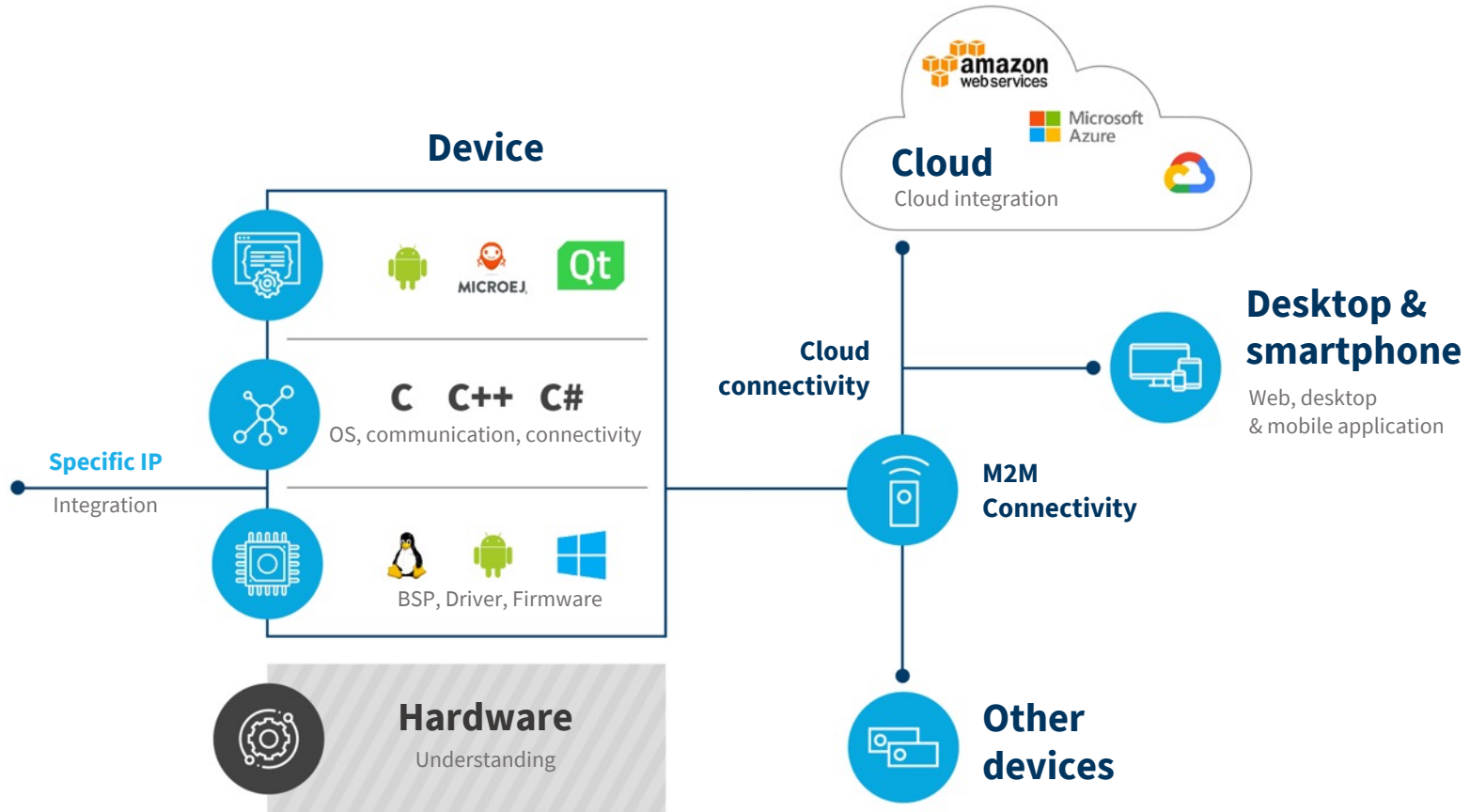## architecture and development

18 years in embedded and IoT software

135+ witekians around the world

100 customers per year

Blue-chip customers leaders in their field

SOFTWARE INDEPENDENCE

Device

Android MICROEJ Qt

C C++ C#
OS, communication, connectivity

Specific IP
Integration

BSP, Driver, Firmware

Hardware
Understanding

Cloud
Cloud integration

amazon web services
Microsoft Azure

Cloud connectivity

M2M Connectivity

Desktop & smartphone
Web, desktop
& mobile application

Other devices

What's the Big Deal about Cloud?

Context

o 35 Billion connected devices today

o Customers are demanding more connected solutions

o Expiring CA root certificates

A Few Cloud Possibilities…

o Remotely manage updates and patches

o Predictive maintenance and alerting

o Automating and optimizing data collection and storage

o Business intelligence reporting

2.

Cloud Platforms and Connected Devices

Why AWS and Azure?

Top Two Public Clouds

o **2018 ZDnet** - #1: AWS, #2: Azure

o **2019 Gartner** - #1: AWS, #2: Azure
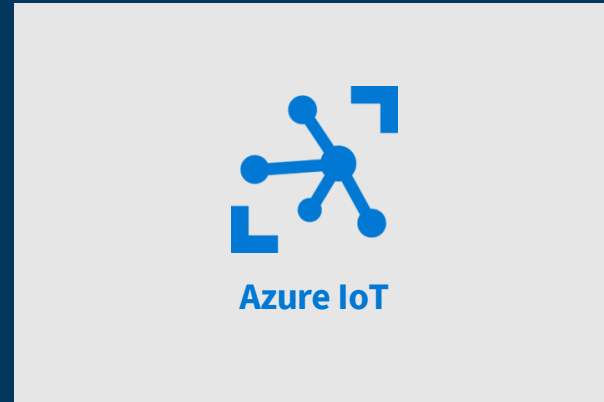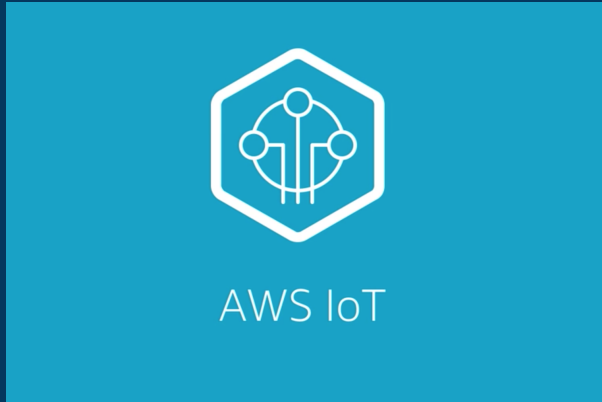
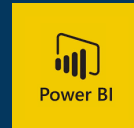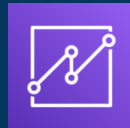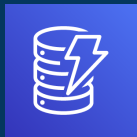o **2020 ZDnet** - #1: AWS, #2: Azure

Other IoT Options

o Google Cloud (frequently in third)

o IoT Platforms

o Other Cloud Providers

o Open Source Tools like IoT ThingsBoard

Why AWS and Azure?

AWS IoT

Azure IoT

IoT Platforms

Power BI

Authenticating IoT Devices to the Cloud

- Symmetric keys (Azure only)

- X.509 certificates

- TPM attestation

- Other mechanisms

  - Device claiming (Azure Sphere)

  - CSRs with device keys

  - Preregistering device ids and public keys

  - JSON Web Tokens (Google)

Device Authorization Mechanisms

Azure

- Shared Access Policies
- Downstream actions through IoT Hub

AWS

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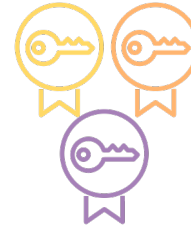- AWS IAM Policies and Roles
- STS Tokens

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
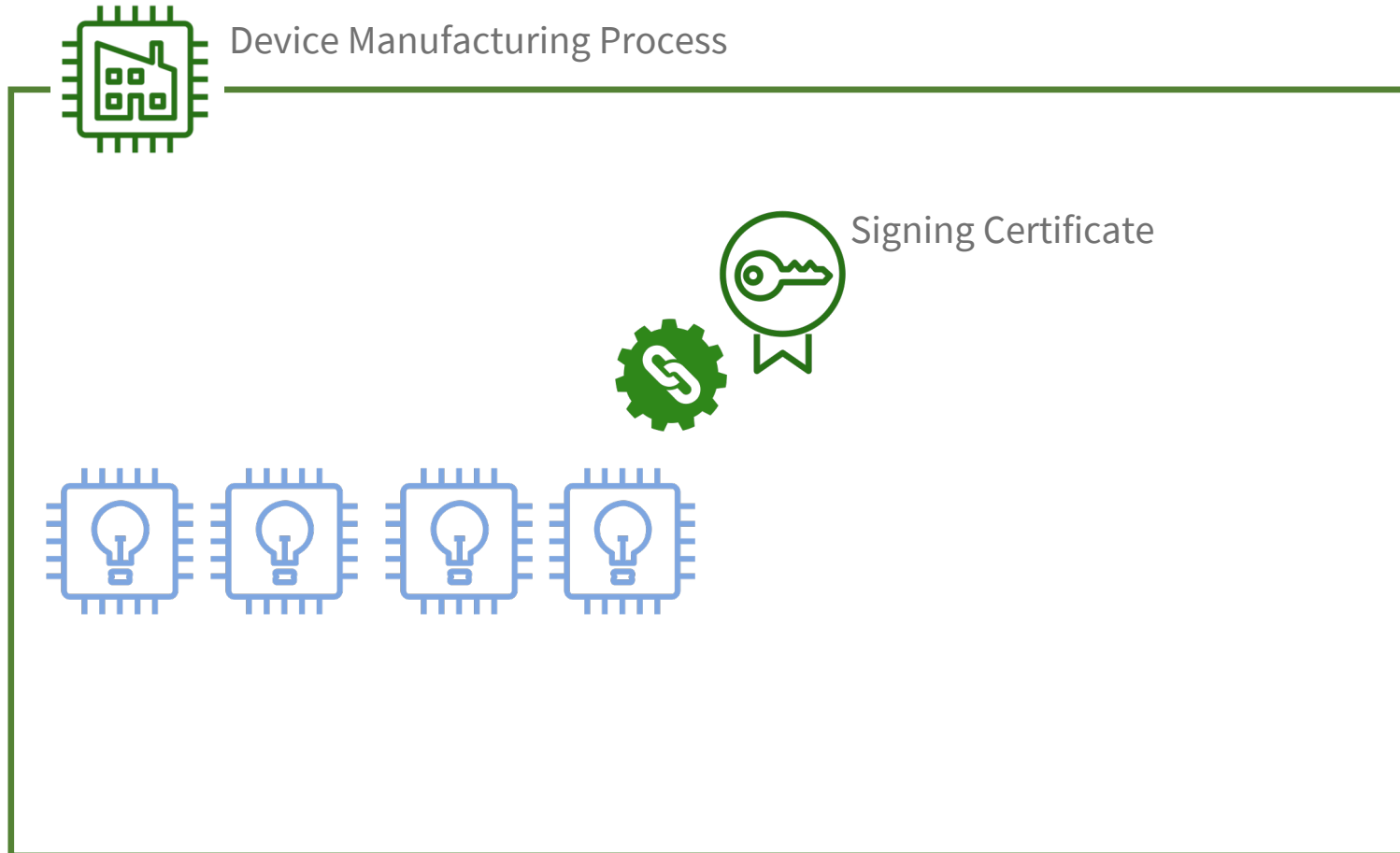
X.509 Authentication
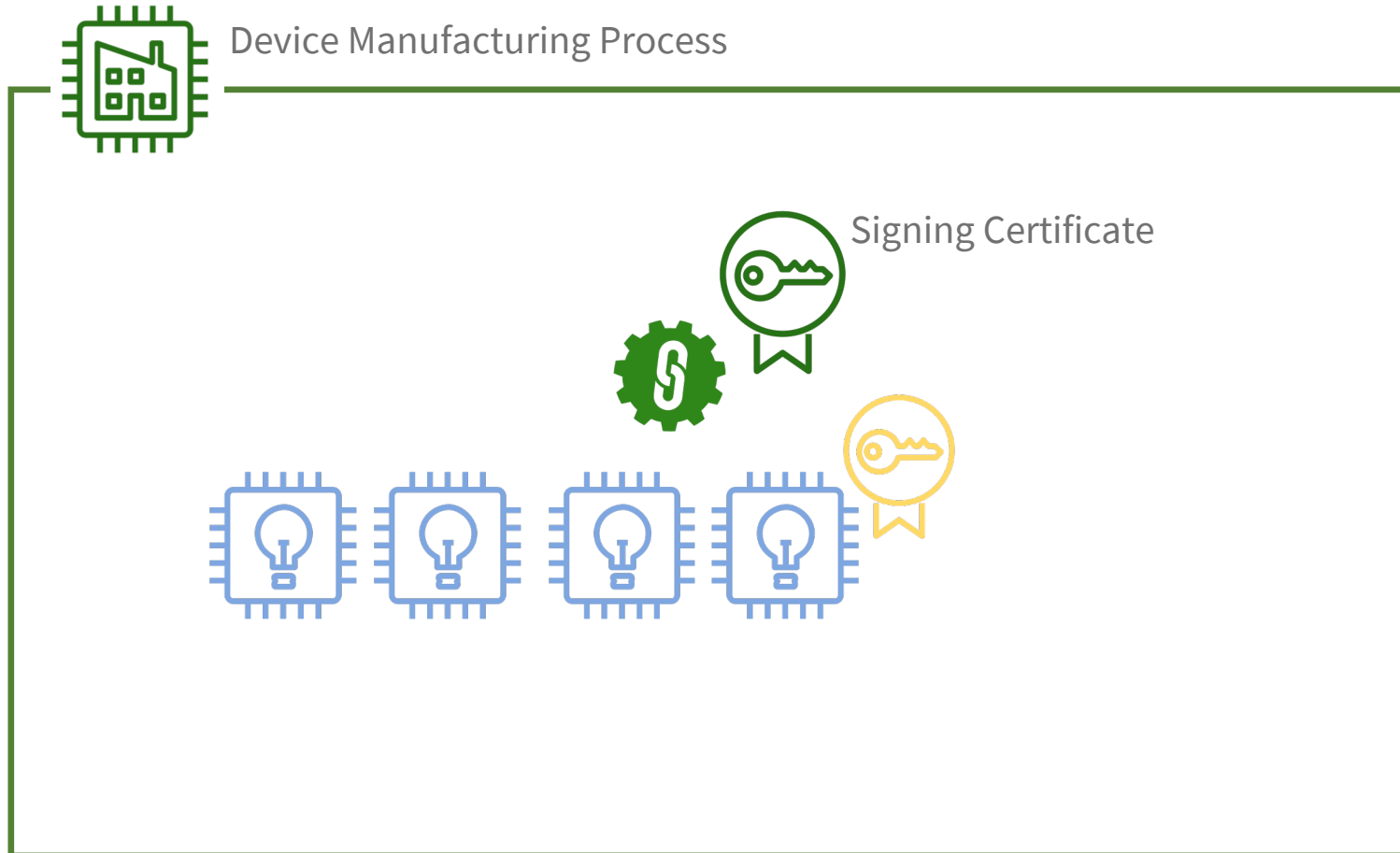

AWS IoT Core

Root Certificate
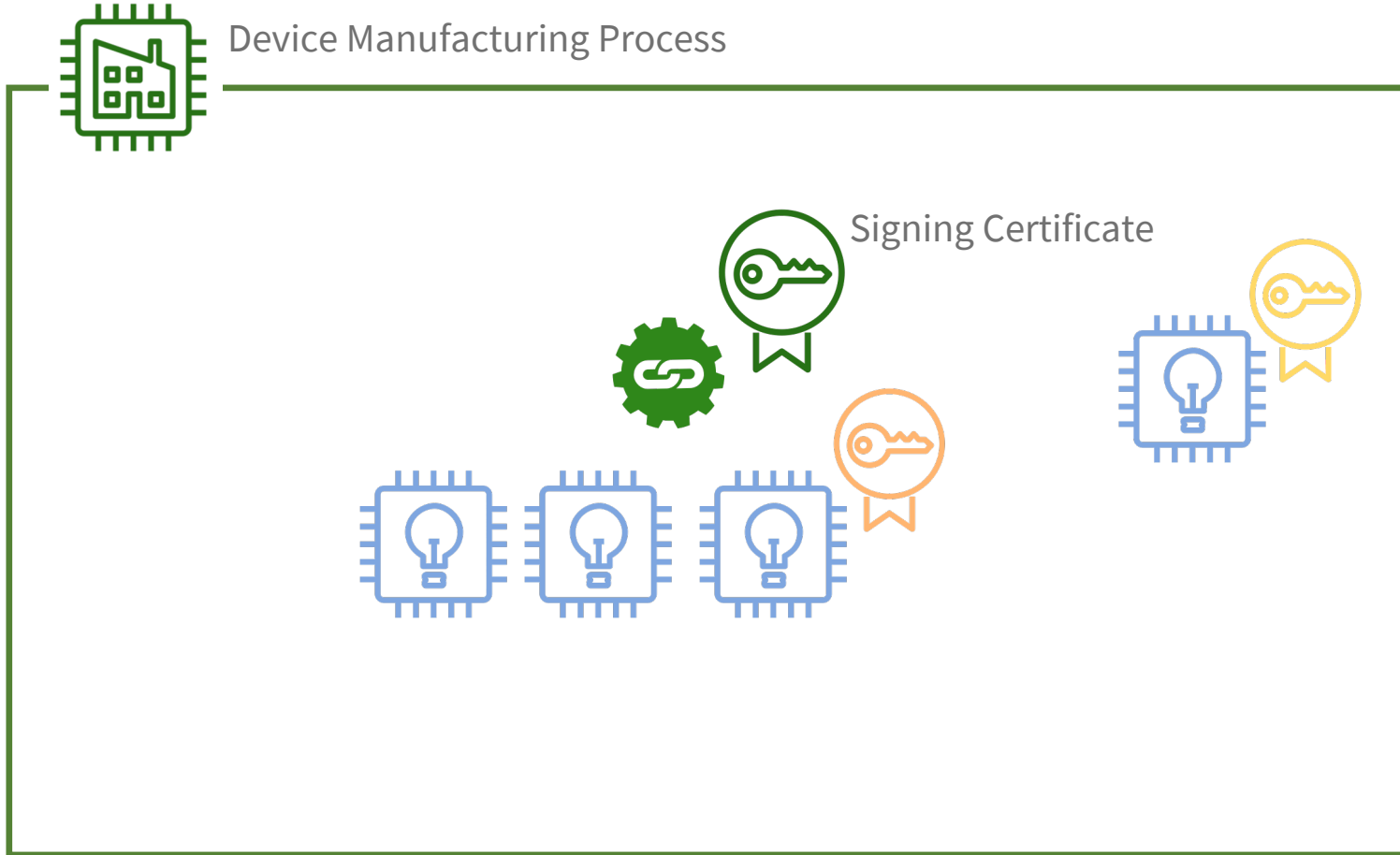
Signing Certificate

X.509 Authentication

Device Manufacturing Process

Signing Certificate

X.509 Authentication

Device Manufacturing Process

Signing Certificate

X.509 Authentication

Device Manufacturing Process

Signing Certificate

X.509 Authentication

Device Manufacturing Process

Signing Certificate

X.509 Authentication

Device Manufacturing Process

Signing Certificate

X.509 Authentication
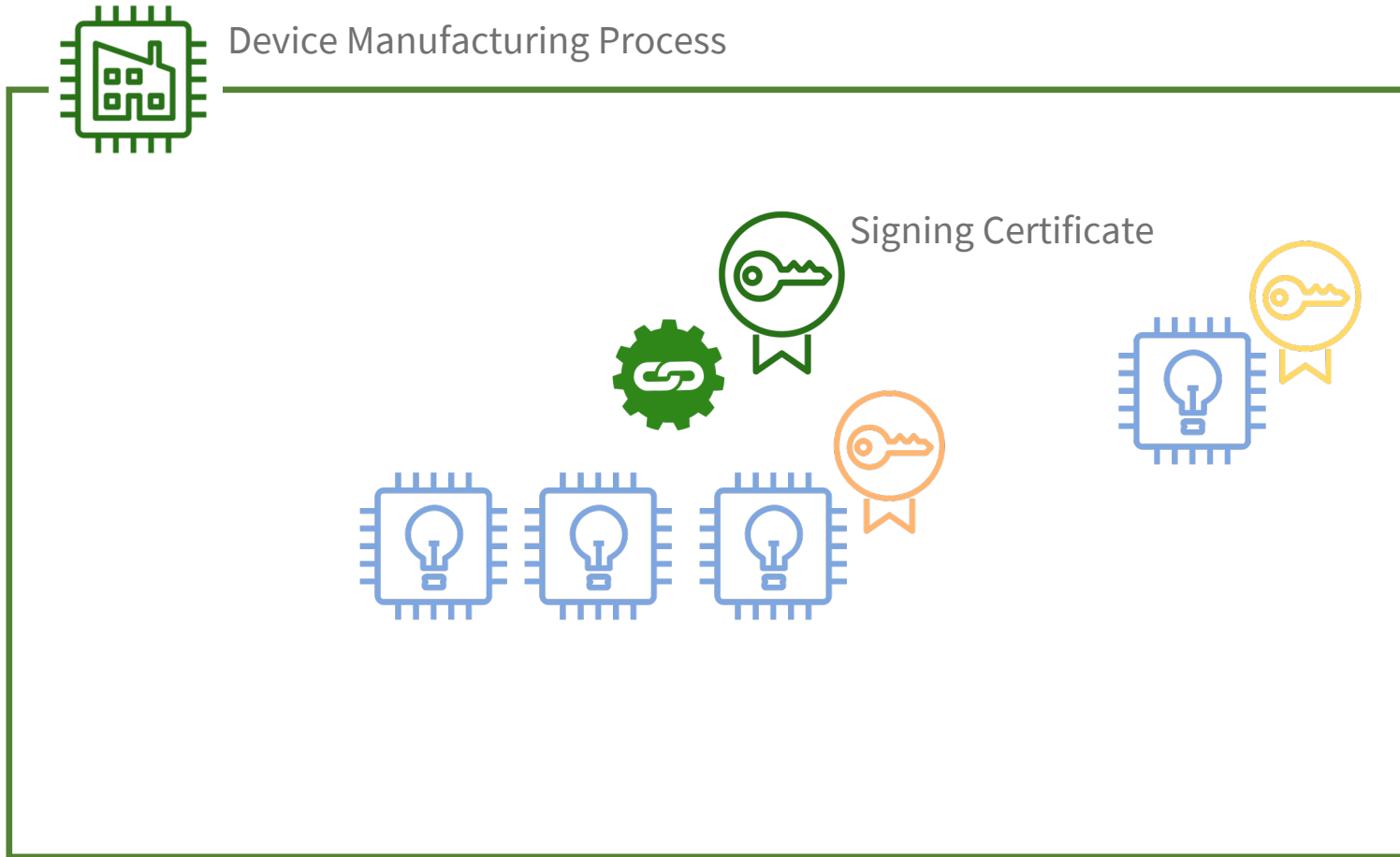
Device Manufacturing Process

Signing Certificate
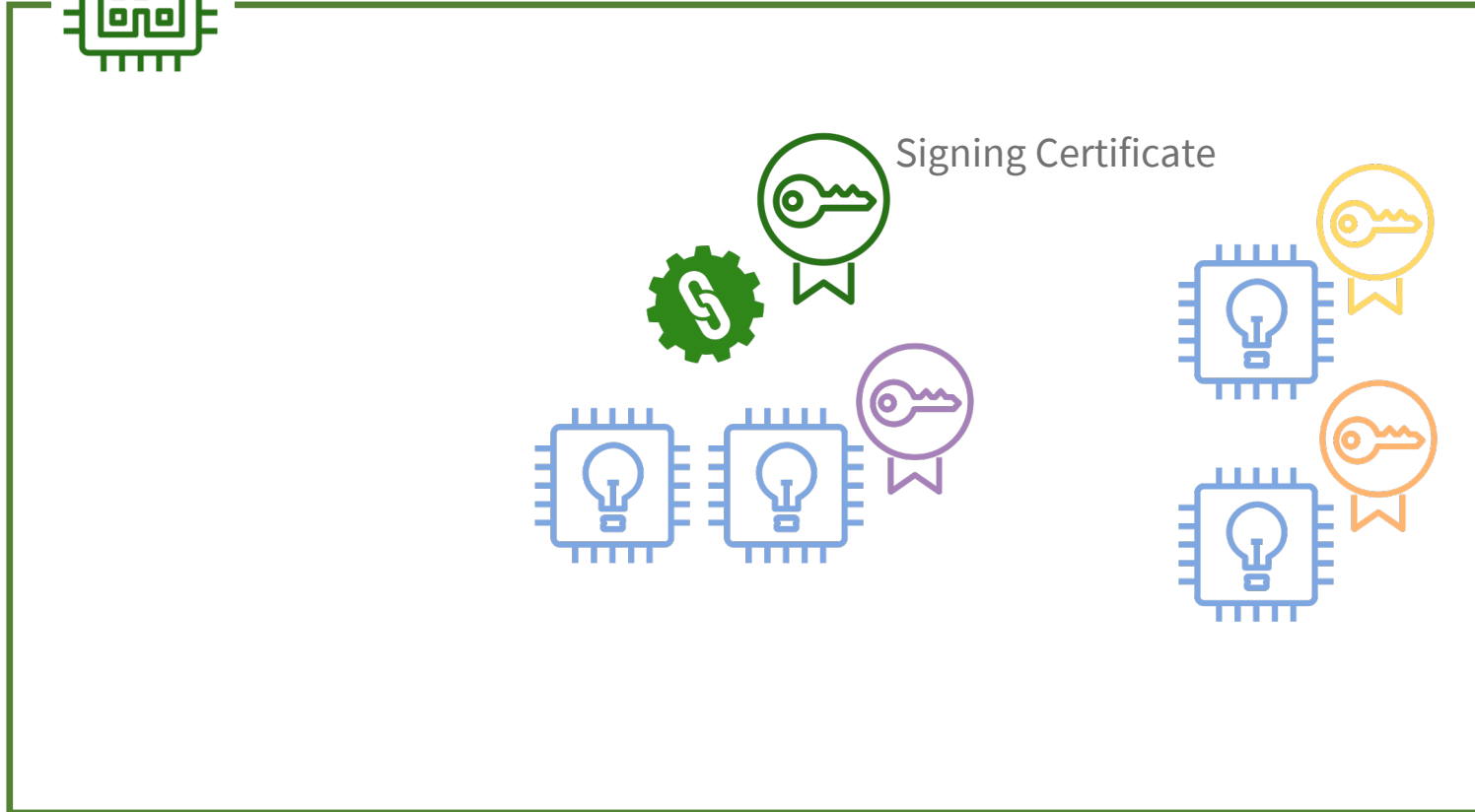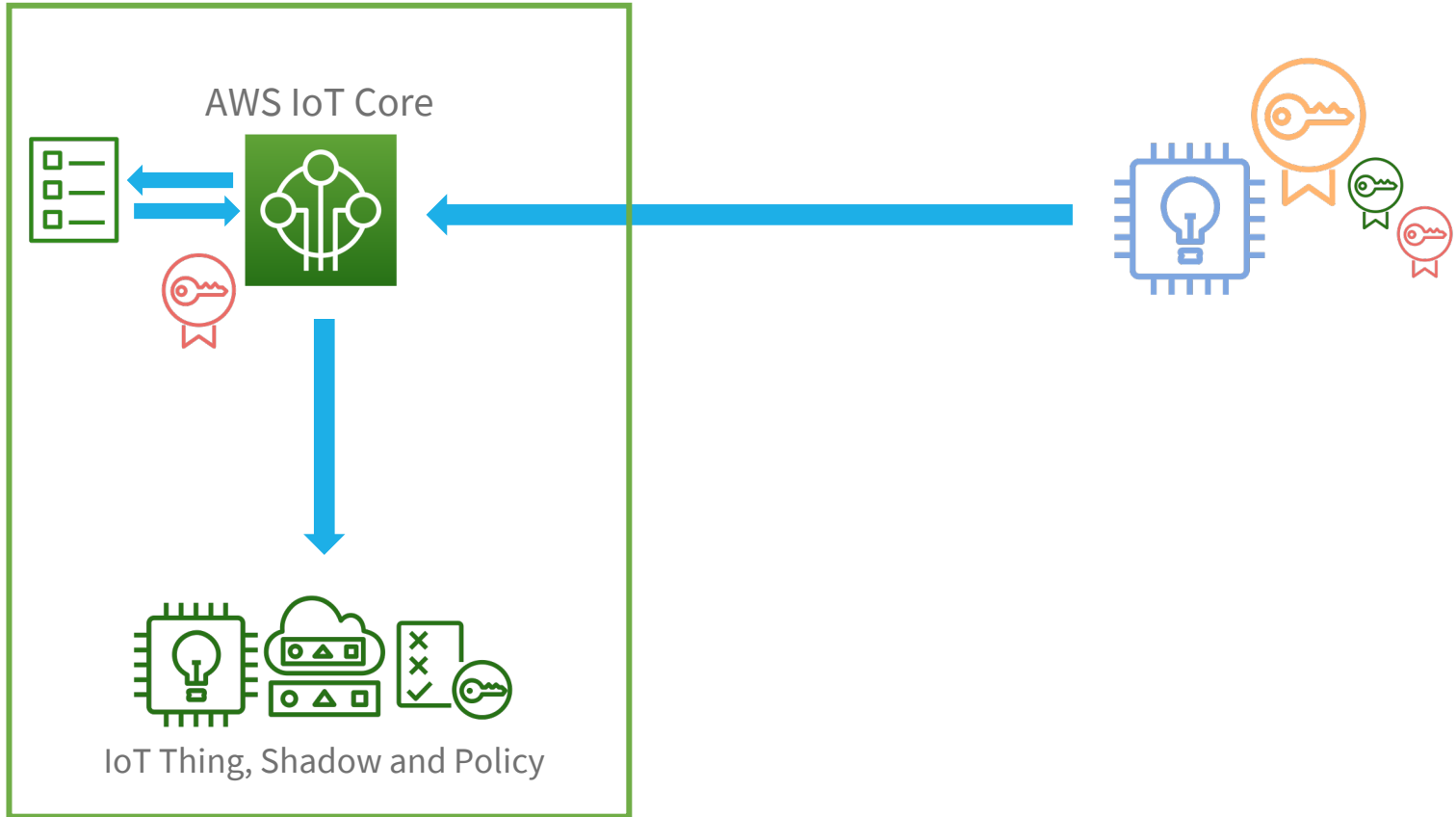
Device Provisioning

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**
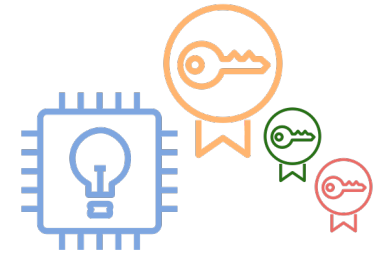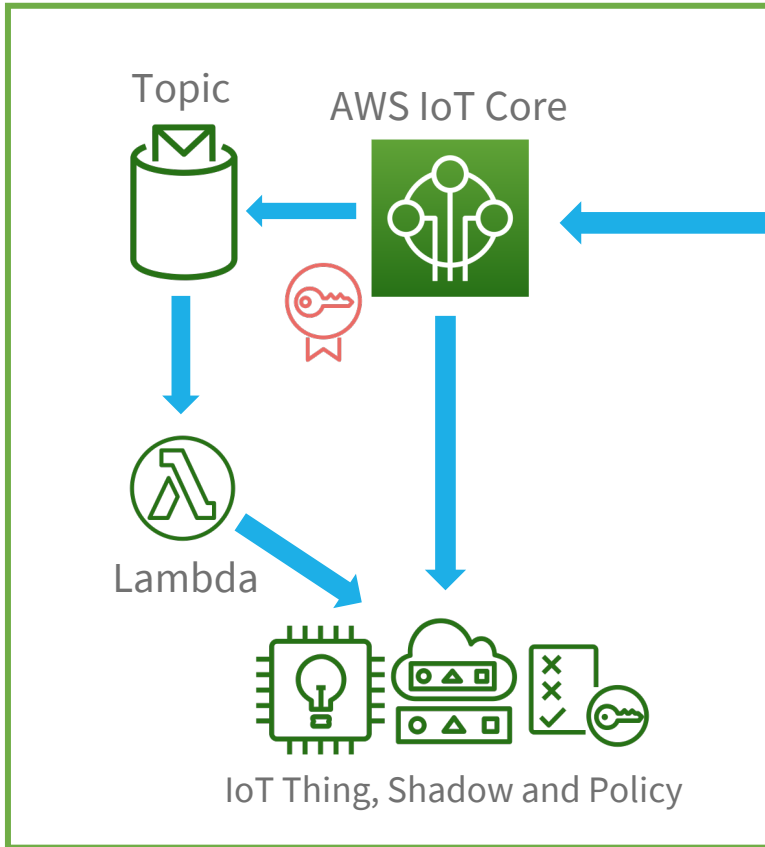 - **Key rotation**

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**
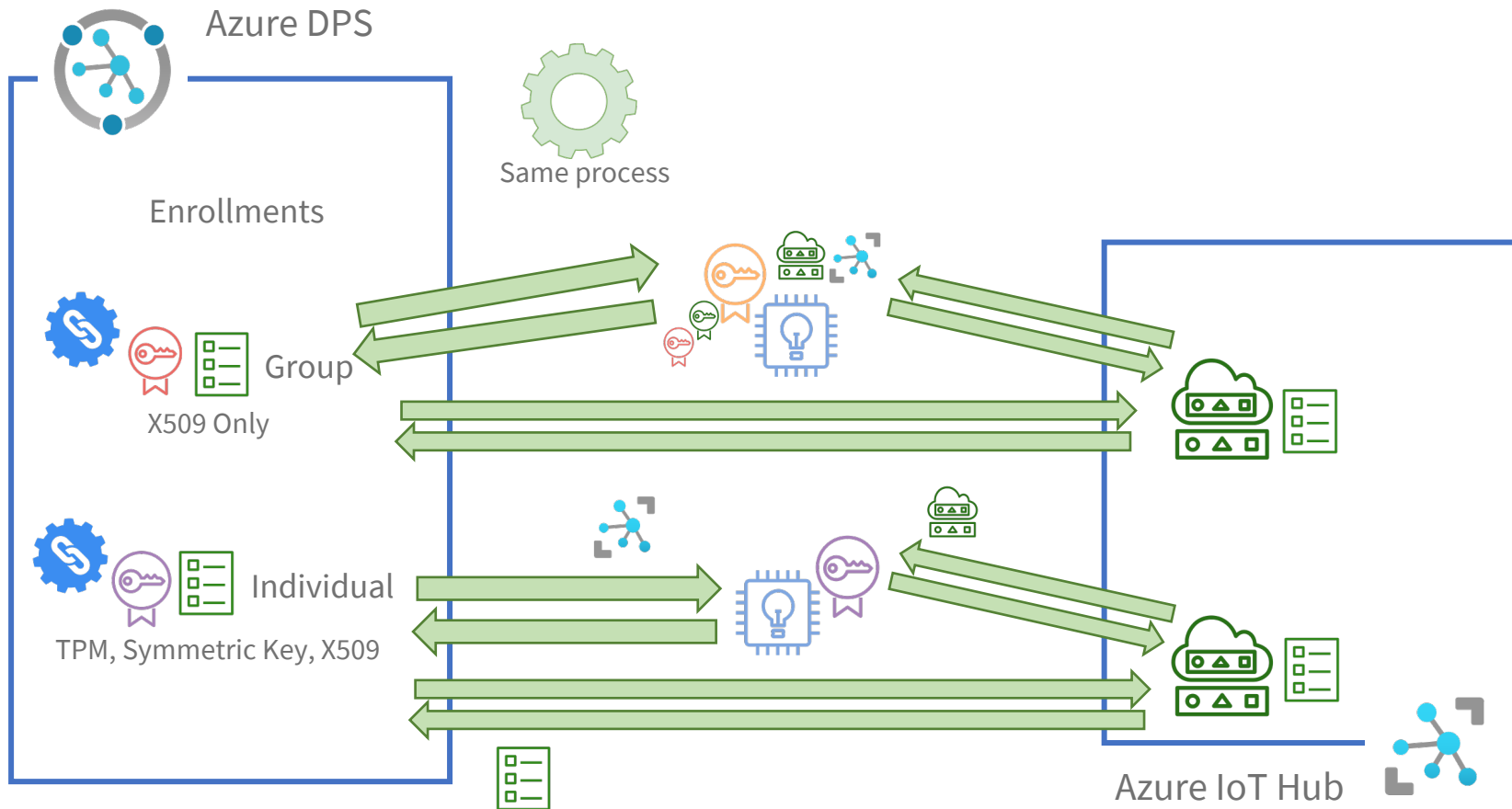 - **Shared claim certificate used to get a unique certificate**

AWS Device Provisioning – JITP

AWS IoT Core

IoT Thing, Shadow and Policy

AWS Device Provisioning – JITR

Topic

AWS IoT Core

Lambda

IoT Thing, Shadow and Policy

Azure Device Provisioning Process – DPS

Azure DPS

Same process

Enrollments

Group

X509 Only

Individual

TPM, Symmetric Key, X509

Azure IoT Hub
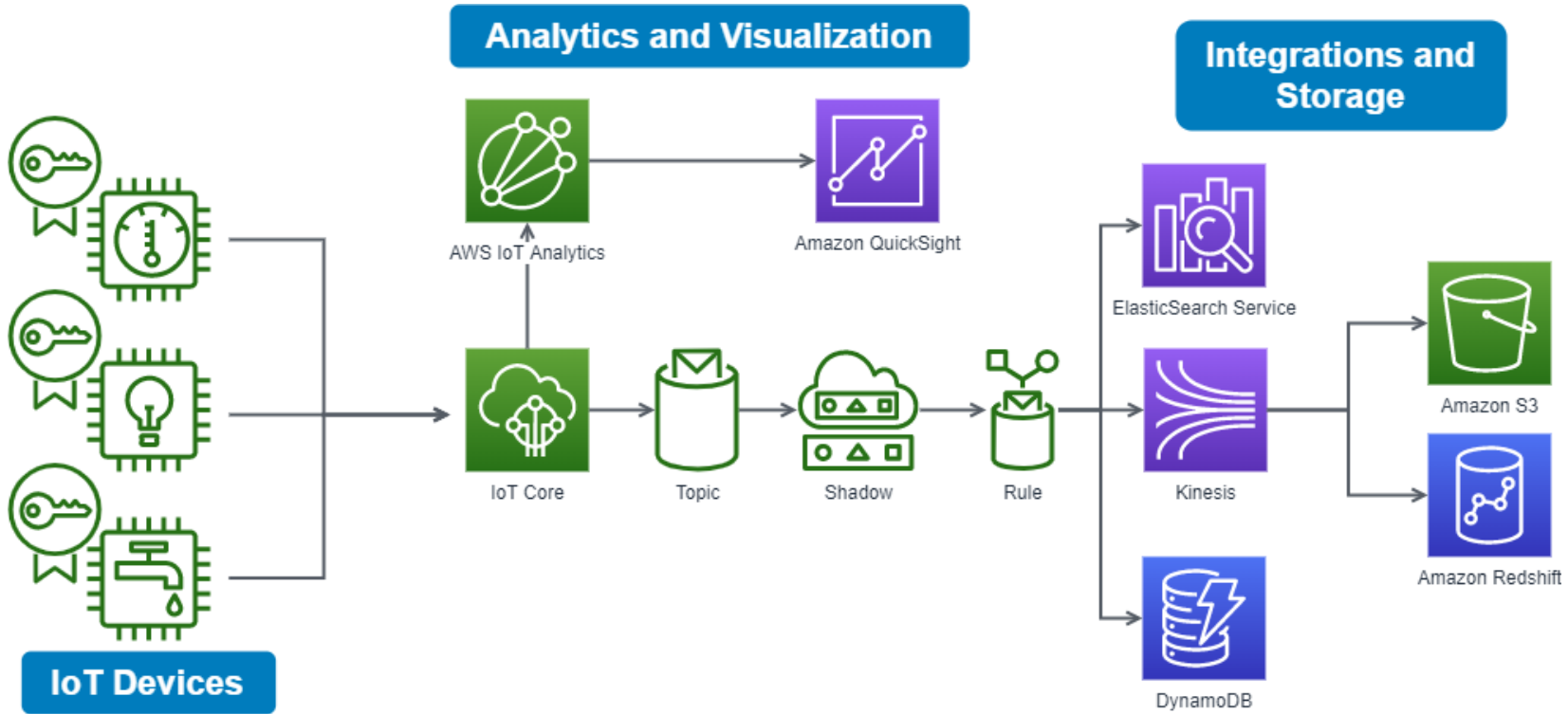
Azure Device Provisioning Process – DPS
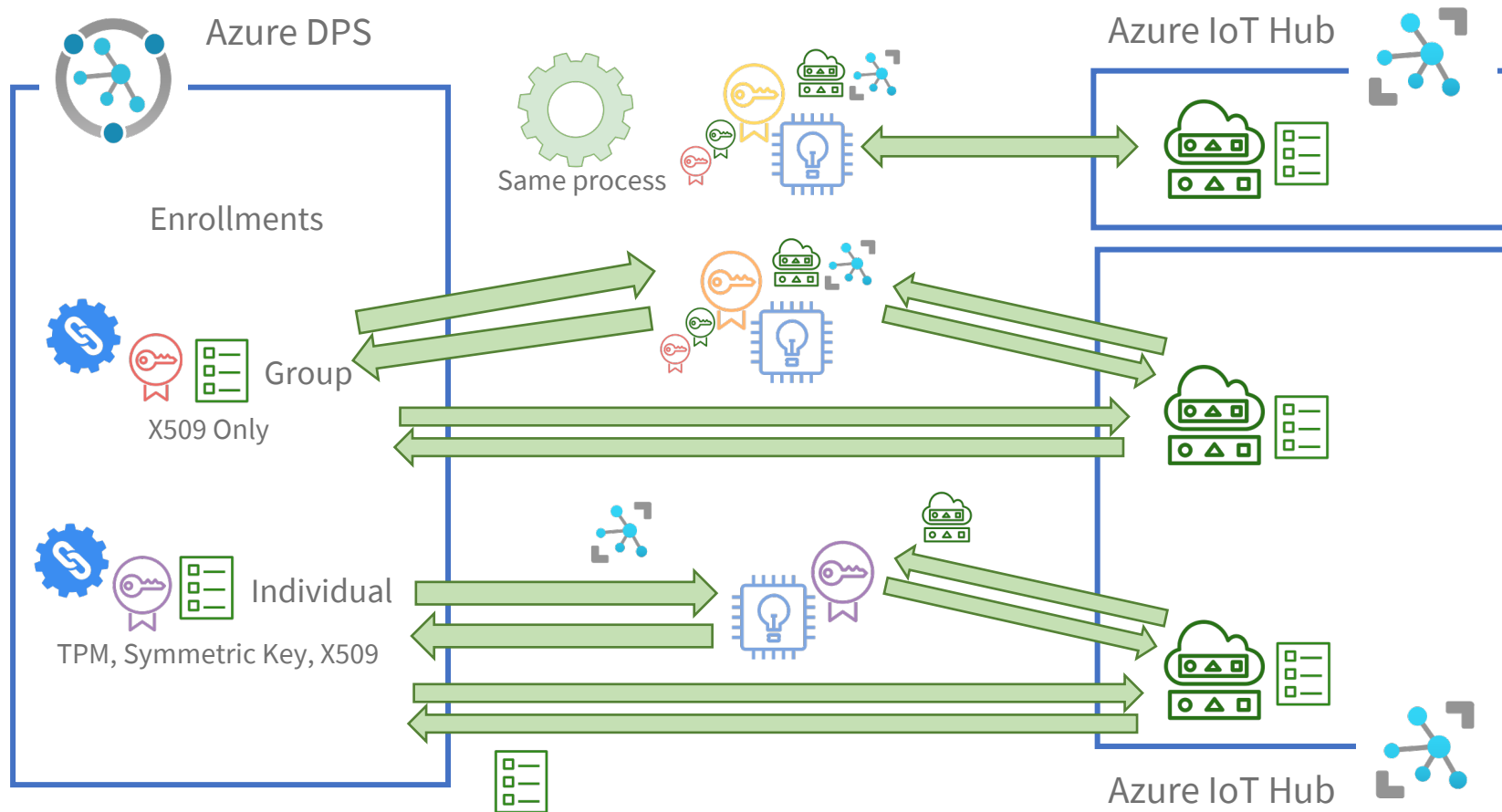
3.

Sample IoT Architectures and Use Cases

AWS Architecture: Device Fleet Analytics
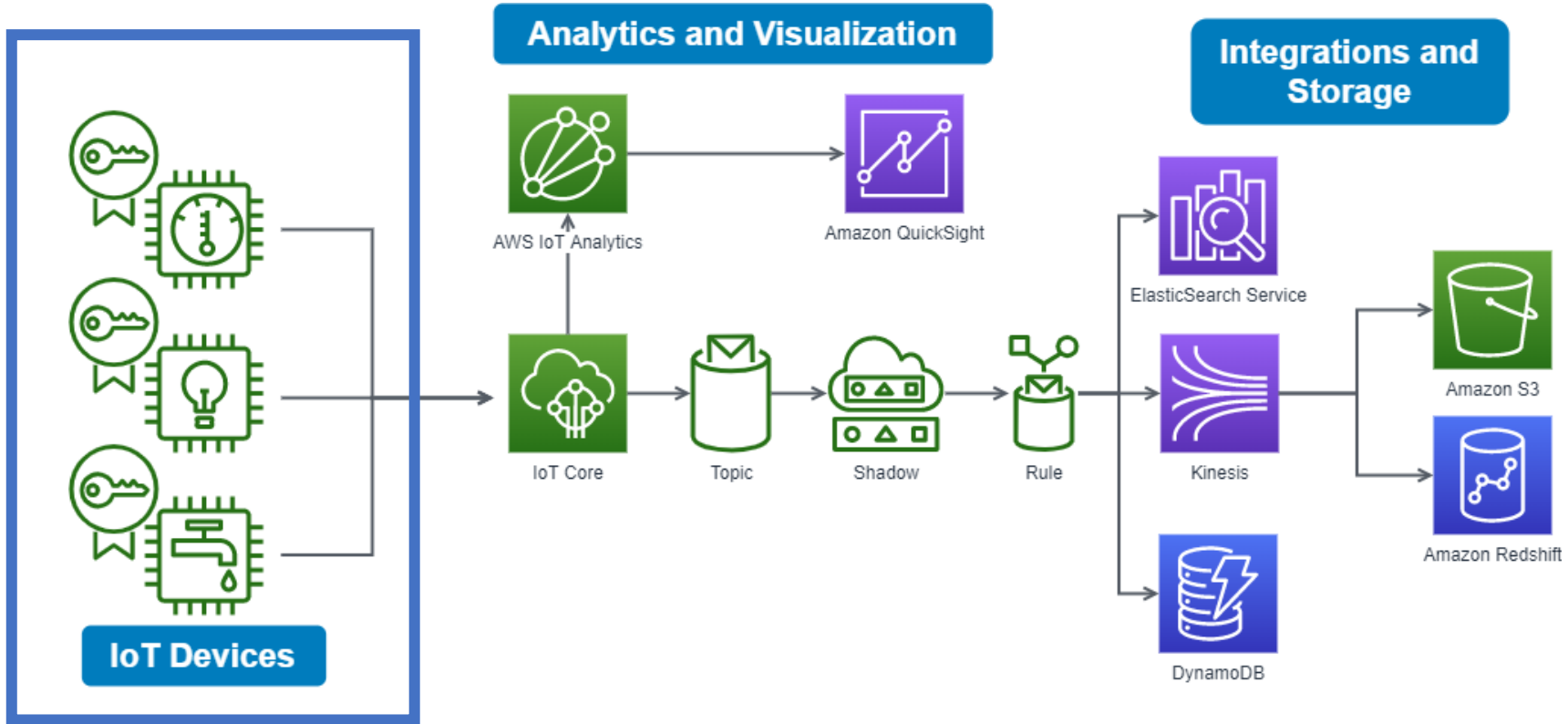
Analytics and Visualization

AWS IoT Analytics

Amazon QuickSight

Integrations and Storage

ElasticSearch Service

Amazon S3

Kinesis

Amazon Redshift

DynamoDB

IoT Core

Topic

Shadow

Rule
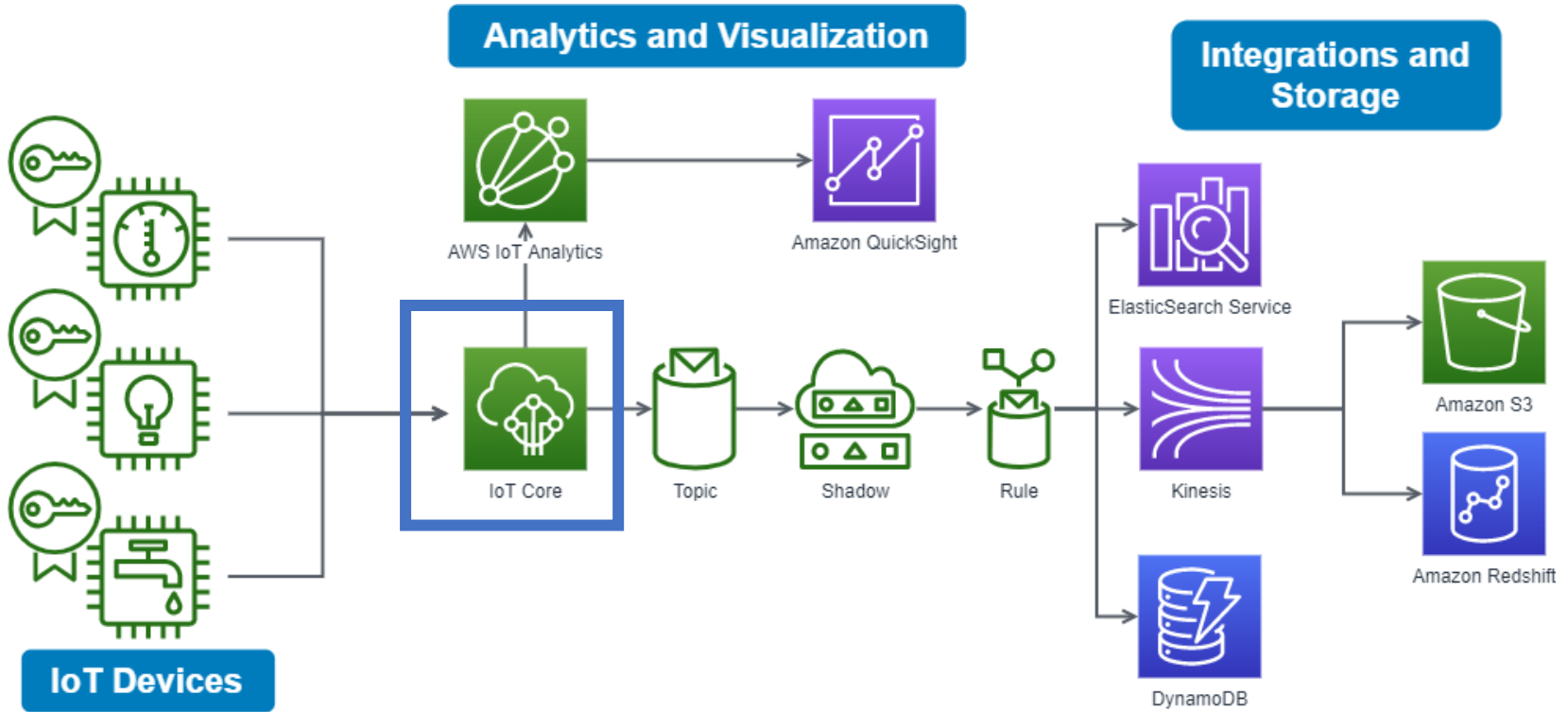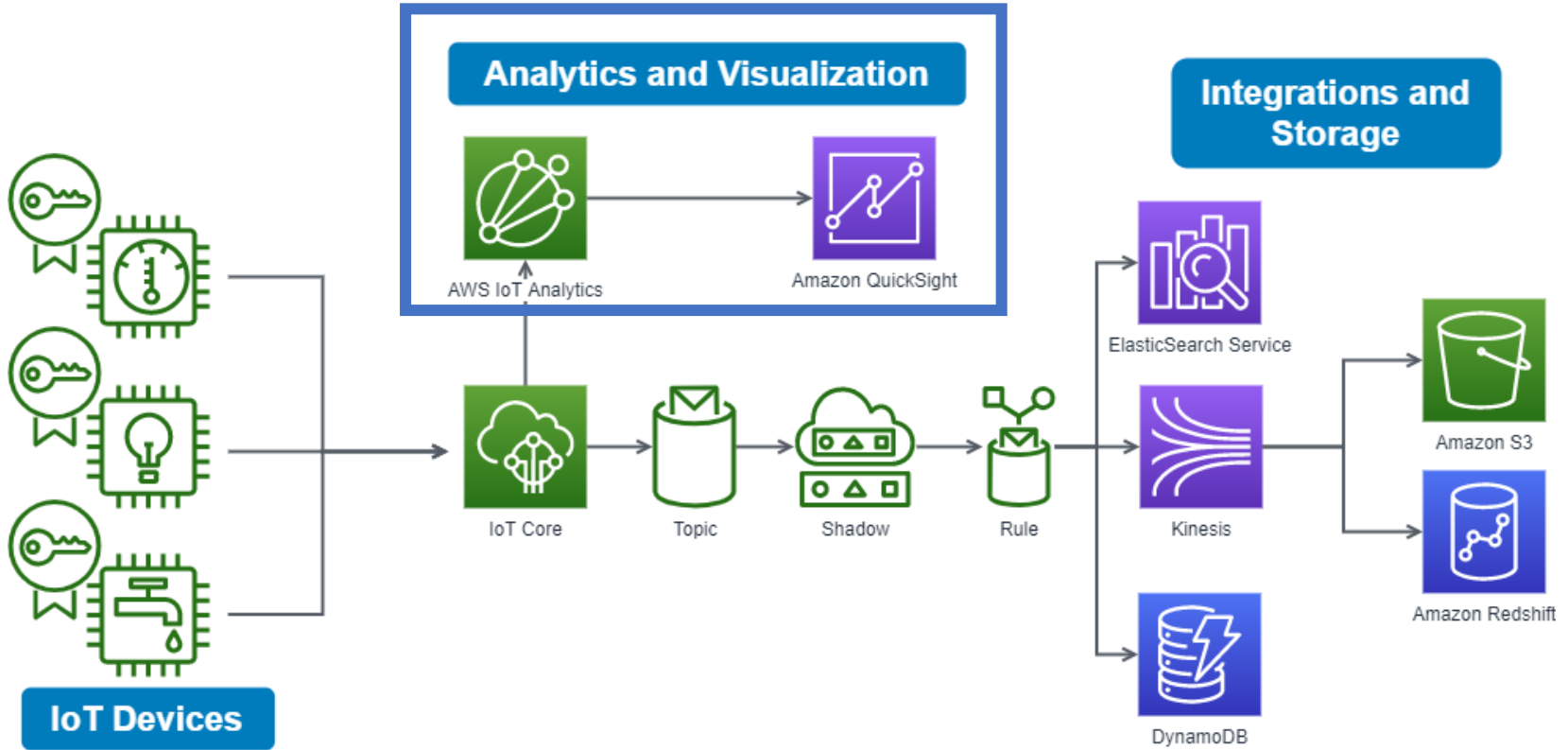
IoT Devices

AWS Architecture: Device Fleet Analytics

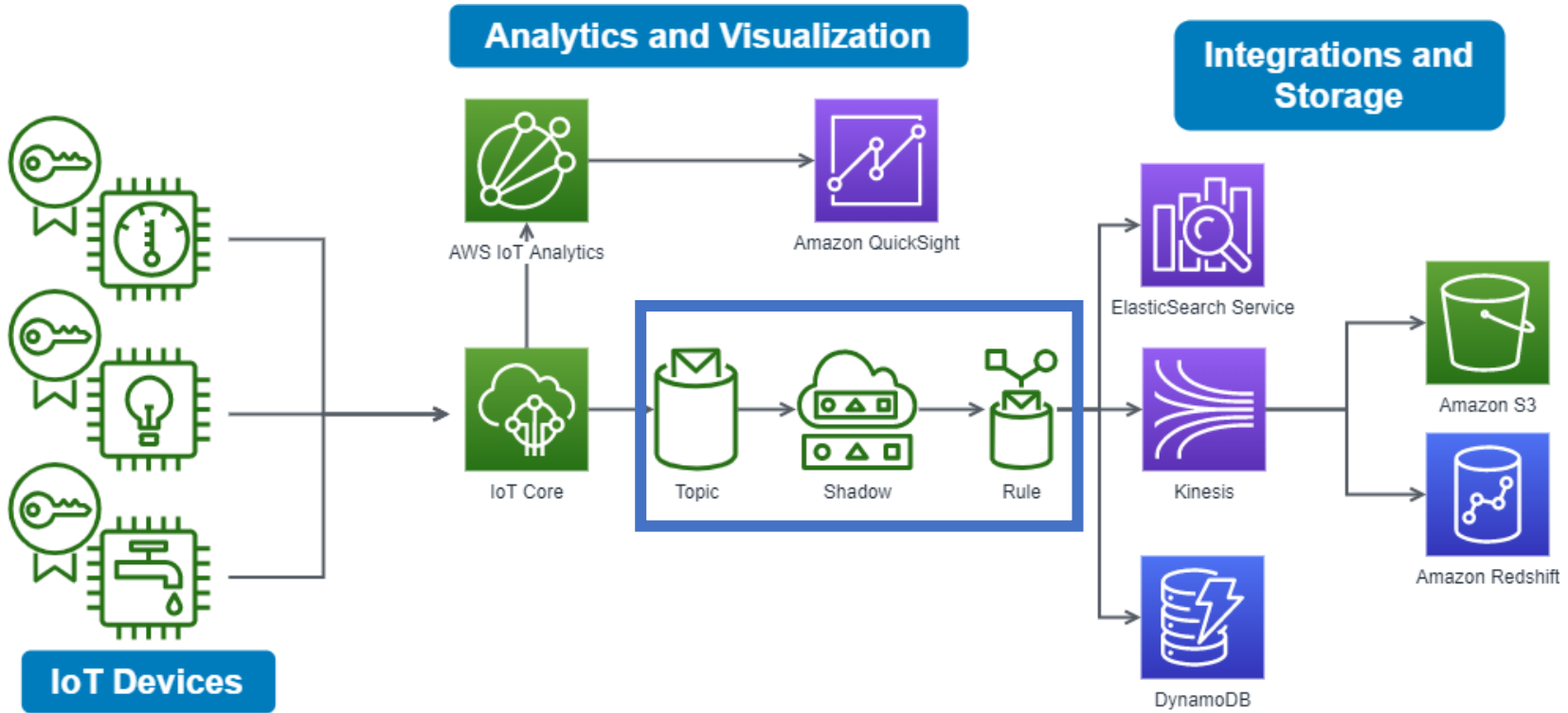# AWS Architecture: Device Fleet Analytics

AWS Architecture: Device Fleet Analytics

IoT Devices

Analytics and Visualization

AWS IoT Analytics → Amazon QuickSight

Integrations and Storage

IoT Core → Topic → Shadow → Rule

ElasticSearch Service

Kinesis → Amazon S3, Amazon Redshift

DynamoDB

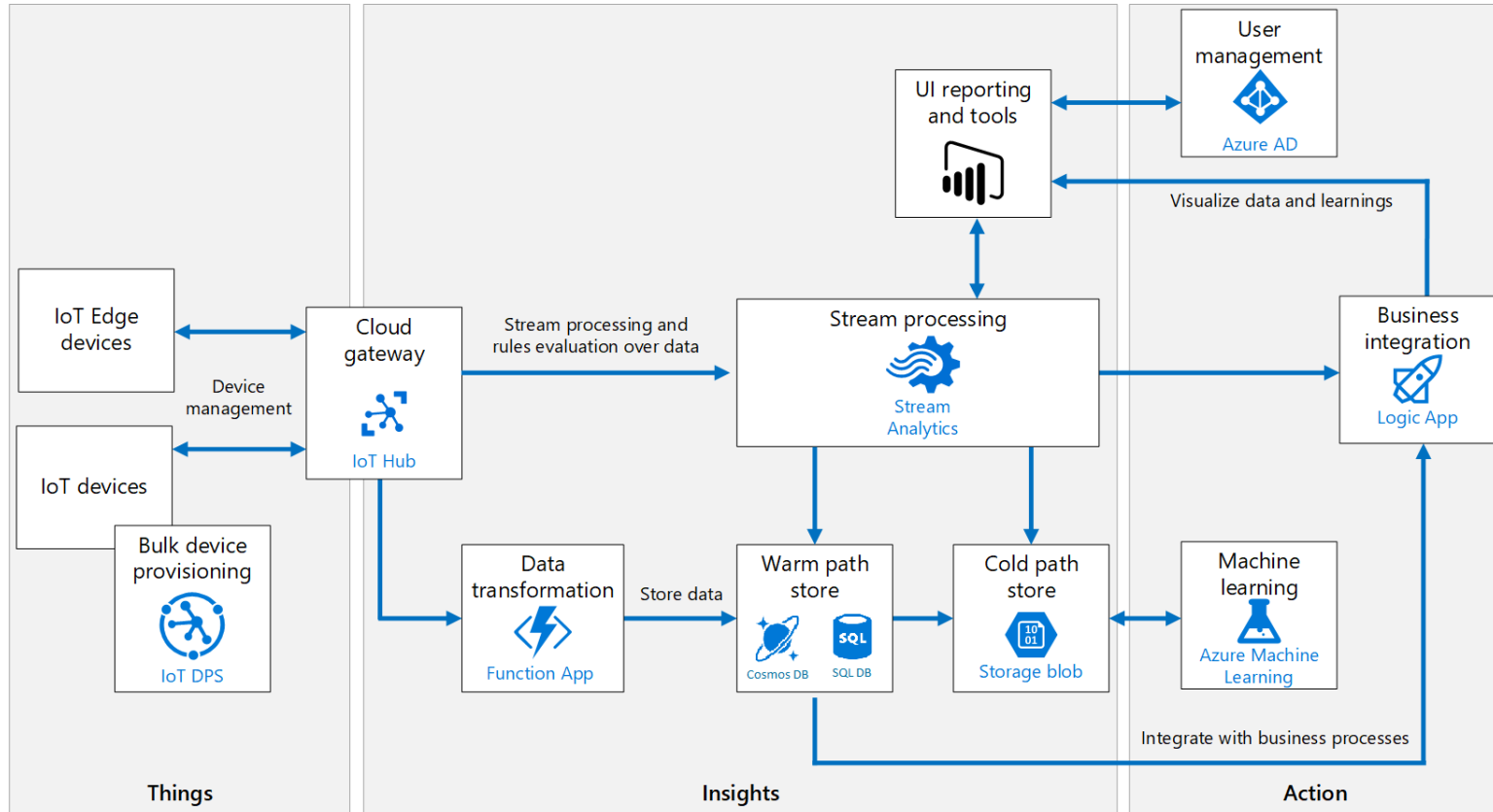# AWS Architecture: Device Fleets Analytics

AWS Architecture: Device Fleet Analytics
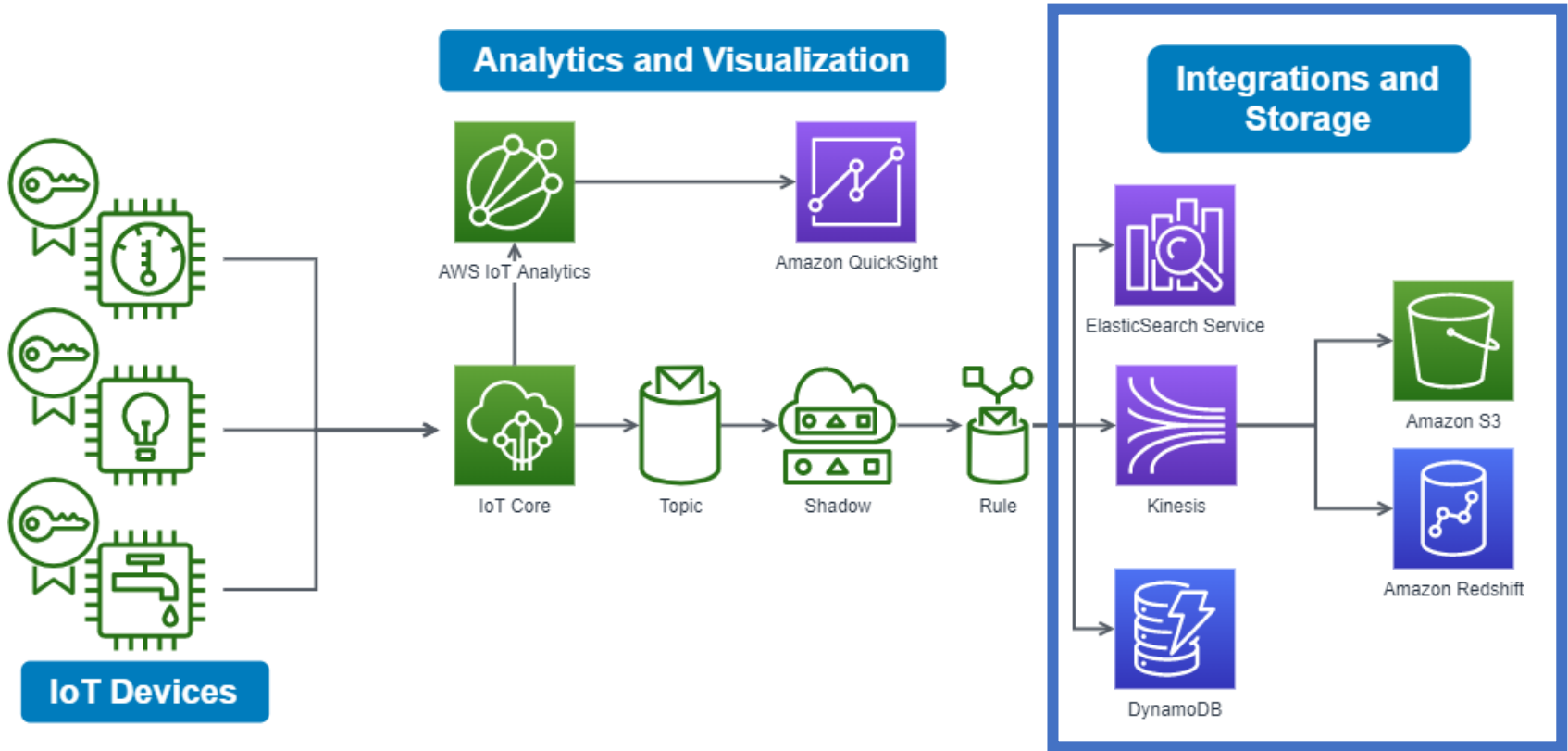
Comparable Azure Architecture

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/_images/iot.png

Bonus: Comparable GCP Architecture

https://cloud.google.com/iot-core
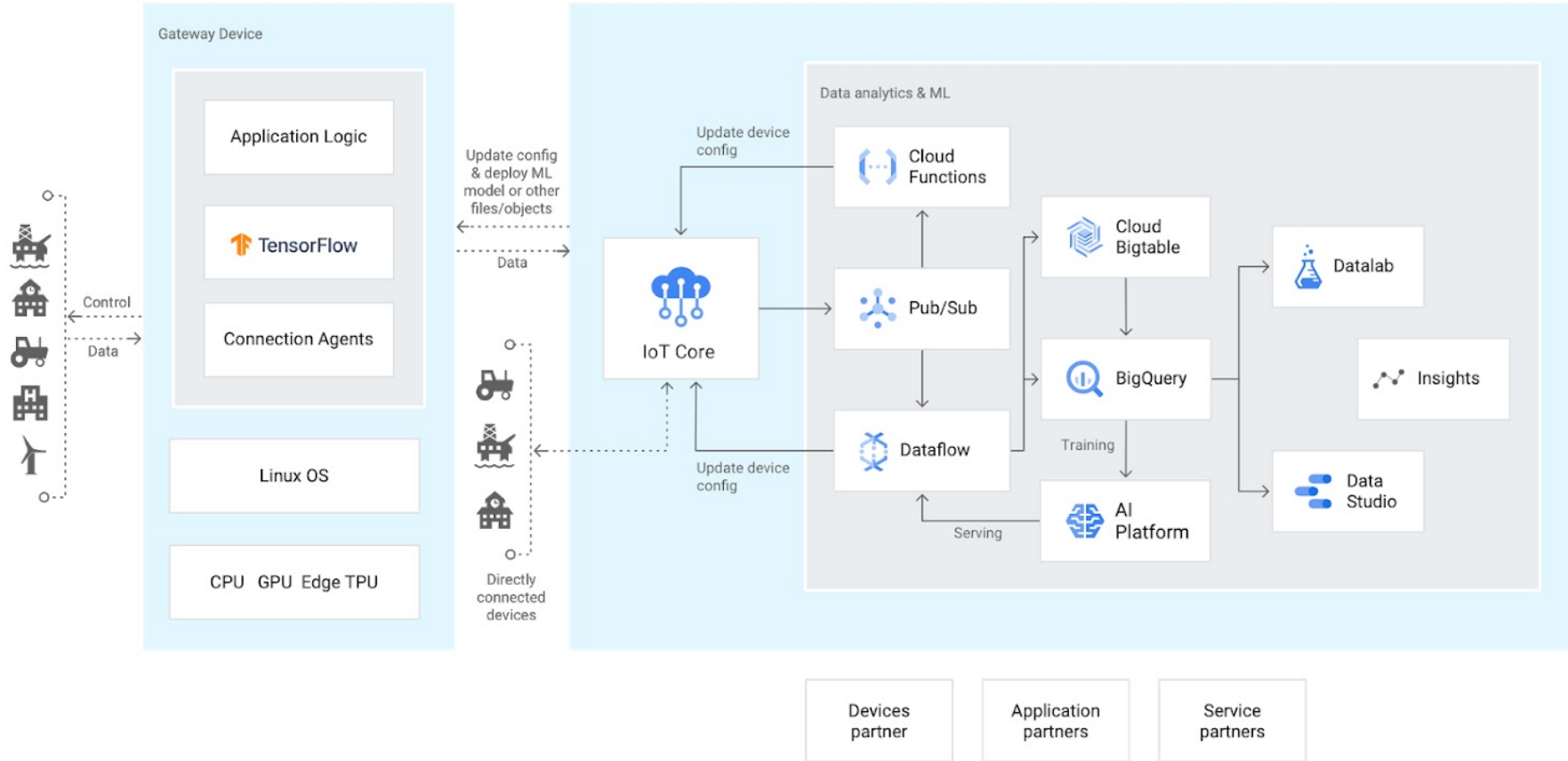
4.

Demos:
The Cloud Side of IoT

Demo 1 – Chocolate Security System with AWS
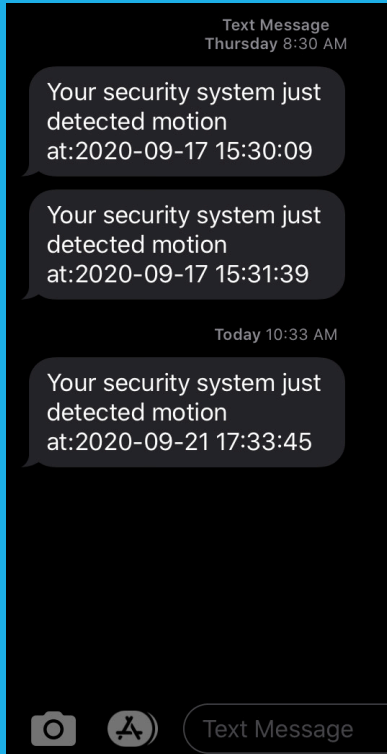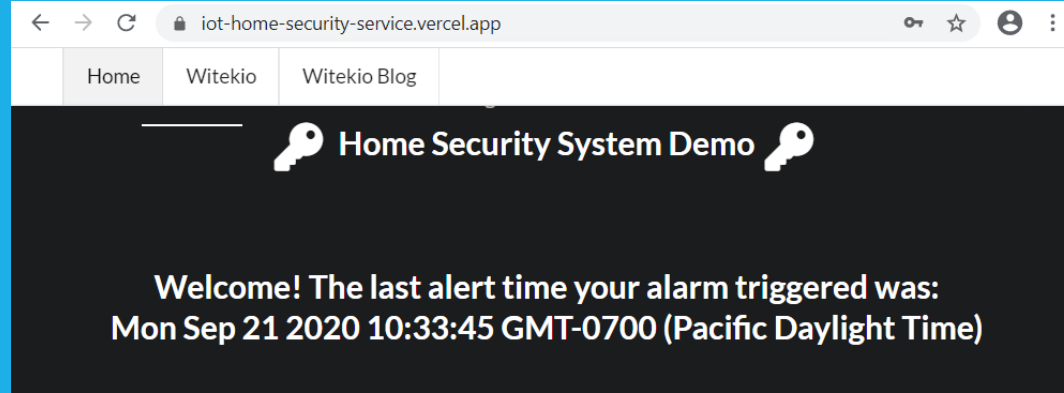
Hardware Architecture – "Chocolate Sensor"

Standard PIR Sensor

Easily stolen chocolate

Raspberry Pi Device

Cloud Architecture

HTTP APIs

Database

Customer Web Portal

DNS, Caching, Object Storage, SSL

▲ Vercel

Amazon Cognito Authentication

API Gateway

Lambda Function

DynamoDB

Lambda Function

IoT Core

Topic

Shadow

IoT Device

IoT Device

Lambda Function

SNS

Other Integrations

Device Communication

Cloud Architecture

Customer Web Portal

DNS, Caching, Object Storage, SSL

▲Vercel

Amazon Cognito Authentication

HTTP APIs

Lambda Function

Database

DynamoDB

API Gateway

Lambda Function

IoT Core

Topic

Shadow

IoT Device

IoT Device

Lambda Function

SNS

Other Integrations

Device Communication

Cloud Architecture

Cloud Architecture

Cloud Architecture

Customer Web Portal

DNS, Caching, Object Storage, SSL

▲Vercel

Amazon Cognito Authentication

HTTP APIs

Lambda Function

API Gateway

Lambda Function

Lambda Function

Database

DynamoDB

IoT Core

SNS

Other Integrations

Topic

Device Communication

IoT Device

Shadow

IoT Device

Our Code

```
├── device
│   └── run.py
├── frontend
│   ├── css
│   ├── index.html
│   └── js
├── handlers
│   ├── get_device_shadow.py
│   ├── jit_provisioning.js
│   └── process_alarm.py
├── manufacturing
│   ├── certs
│   ├── connection_attempt.bash
│   ├── create_and_register_ca_cert.bash
│   ├── create_device_cert.bash
│   ├── permissive-provisioning-template.json
│   └── raspi_cert_transfer.bash
├── resources
│   ├── cognito.yml
│   ├── dynamodb.yml
│   └── iot_provisioning_role.yml
├── serverless.yml
```
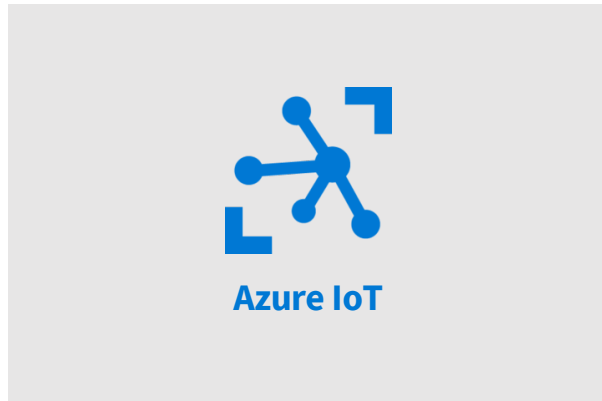
Demo 2: IoT Connected Crane

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

Azure IoT

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

AWS IoT

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
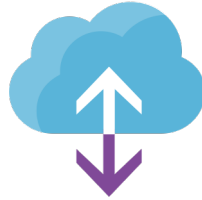
6.

Start Leveraging the Cloud for IoT

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

Ready to Get Started?

Schedule initial consultation with an architect

Cloud Workshop
- Evaluate your cloud needs and possibilities
- Spec out your applications
- Prototype cloud connected applications

CONTACT ME

@ fmedinacorey@witekio.com

in /in/fmc-sea

CONTACT SALES

www witekio.com

@ sid@witekio.com

Questions?