Connecting to AWS IoT Core

By: Ken Rimple
Director, Training/Mentoring
Chariot Solutions

IoT on AWS

A Philly Cloud Computing Event

CHARIOT SOLUTIONS

Outline

What is IoT Core?

Setting up your Certificates

Connecting/Authenticating to IoT Core

Defining AWS IoT Policies and Authorization Statements

CHARIOT SOLUTIONS

What is AWS IoT Core?

- A suite of AWS services
  - Defines devices as "Things" in a registry
  - Configures security via X.509 certificates
  - Associates Things with security policies
  - Defines rules to integrate Things with AWS services
  - Associates Things with shadows (state)
  - Provides a message broker with support for MQTT, HTTP and MQTT over WebSocket support

CHARIOT SOLUTIONS

AWS IoT Core: Thing Registry

Creating AWS IoT things

An IoT thing is a representation and record of your phyisical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT. Learn more.

Register a single AWS IoT thing

Create a thing in your registry

Create a single thing

Bulk register many AWS IoT things

Create things in your registry for a large number of devices already using AWS IoT, or register devices so they are ready to connect to AWS IoT.

Create many things

Cancel

Create a single thing

CHARIOT SOLUTIONS

CREATE A THING

Add your device to the thing registry

STEP 1/3

This step creates an entry in the thing registry and a thing shadow for your device.

Name

234523523452EEEFFFE

Apply a type to this thing

Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description.

Thing Type

No type selected

Create a type

Add this thing to a group

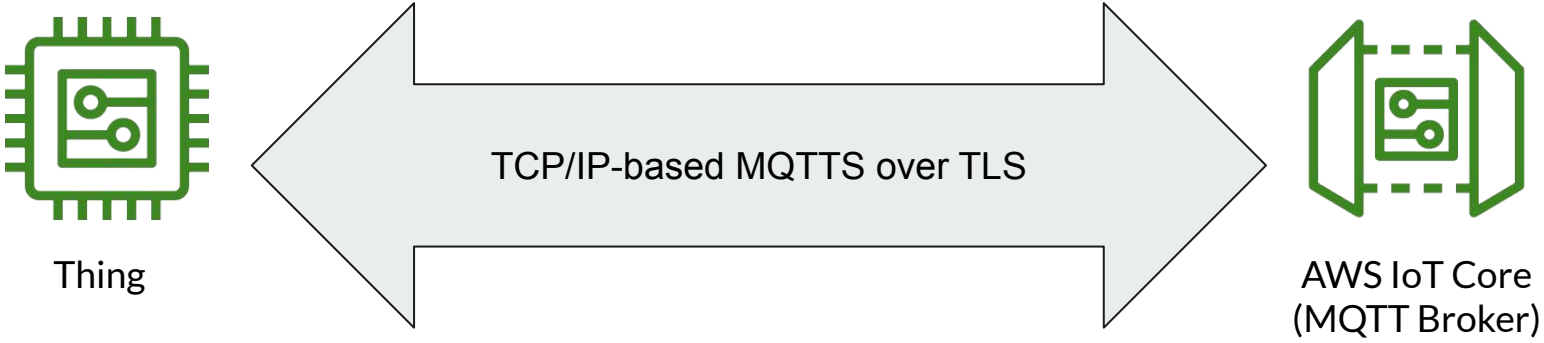
CHARIOT SOLUTIONS

Authenticating with AWS IoT Core

What to secure?	Identity associated with	Notes
IoT Devices	X.509 Certificates	Certificate establishes identity
Web, Desktop Apps, AWS CLI, Lambdas	IAM Users and Roles	
Web, Desktop Apps	Federated Identities (LDAP, etc)	For Active Directory Users
Used by Mobile, Mobile Web Applications / Amplify	Amazon Cognito Identities	Cognito and AWS Amplify work together to secure applications via temporary scoped credentials

CHARIOT SOLUTIONS

How do Things communicate?



- Private Key
- Client Certificate
- Secured destination
- Secured traffic enroute

- AWS Certificate Authority
- Contains Server Certificate
- Verify Client via Certificate

*Each IoT device must have its **own key pair** and **certificate** so that compromised keys only affect a single device!*

CHARIOT SOLUTIONS

Key Pair/Cert Generation Strategies

- AWS has a one-click Cert Generation process
  - Makes generating a cert easy
  - AWS is the CA
  - But AWS created and knows your Private Key
  - Convenience
- Some devices can create keys and generate CSRs
  - You can then only keep the key on the device
  - AWS or third party can be the CA
- Alternatively you can manage the keys yourself and associate them with the device and AWS IoT Core

CHARIOT SOLUTIONS

Creating a PK/CSR from the Thing

```
ECCX08 Serial Number = 234523523452EEEFFFE

Hi there, in order to generate a new CSR for your board, we'll need the following information ...

Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) [234523523452EEEFE]: 234523523452EEEFE

What slot would you like to use? (0 - 4) [0]: 0
Would you like to generate a new private key? (Y/n) [Y]:

Here's your CSR, enjoy!

-----BEGIN CERTIFICATE REQUEST-----
MIIBLDCB1AIBADByMQwwCgYDVQQGEwMFdXMxFTATBgNVBAgTDFBlbm5zeWx2YW5pYTEYMBYGA1UE
BxMPRm9ydCBXYXNoaW5ndG9uMRowGAYDVQQKExFDaGFyaW90IFNvbHV0aW9uczEVMBMGA1UEAxMM
UklNUExFREVWSUNFMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEHNr3AzJbv9S88rMlmZ3rpvPP
//XK4/zkORijdXfIt5Nh9q/7+IDaKs0YuOyrhweYhRkZE4WoLZRlXgLMY96tgKAAMAoGCCqGSM49
BAMCA0cAMEQCICmoB5YSFyDVi5nu5fLhBcBf5wzwfYBRp33Si5je5kkiAiAAkeXxvjDfIa/67Xon
uIdK7SXnUs9cVzaQ/Wzr0lDjbw==
-----END CERTIFICATE REQUEST-----
```

CHARIOT SOLUTIONS

Creating Key Pair / CSR from OpenSSL

```
$ openssl genrsa -out private.key 2048

$ openssl req -new -key private.key -out csr.txt
...
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) [234523523452EEEFE]: 234523523452EEEFE
...

$ cat csr.txt
-----BEGIN CERTIFICATE REQUEST-----
MIICWjCCAUICAQAwFTETMBEGA1UEAwwKTVlERVZJQ0VJRDCCASIwDQYJKoZIhvcN...
kP+QuE9q3a3rzZoYAq/ync4vXJ17r77mDPcYc39/f6IXOIF0JAuXwb2ec3Vjey2W
aXMMJBAHE/DonBl9AV7YGHn+5Ks2PHEjHRWMyIF1afQOey4nEa7qItqN2qrJC37n
HCFd+C/UoraER/VZRCDm4tcT0MUrHW51xkJwsPyQU3QFDUR3AXfljog6eNPDpVKM
cX13T5sgiVYuPb6i0FDHes5NVfVJ48UpKOrfGtqq
-----END CERTIFICATE REQUEST-----
```

CHARIOT SOLUTIONS

IoT Core
Creating a Certificate based on a CSR

CHARIOT SOLUTIONS

Use CSR to Create Certificate

CREATE A THING

Add a certificate for your thing

STEP 2/3

A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

Create certificate

Create with CSR

Upload your own certificate signing request (CSR) based on a private key you own.

09-25-2019-csr-for-demo.txt

Upload file

Use my certificate

Register your CA certificate and use your own certificates for one or many devices.

Get started

Skip certificate and create thing

You will need to add a certificate to your thing later before your device can connect to AWS IoT.

Create thing without certificate

CHARIOT SOLUTIONS

Download the Certificate

Things > RIMPLEDEVICE

THING

RIMPLEDEVICE

NO TYPE

Details

Security

Thing Groups

Billing Groups

Shadow

Interact

Activity

Jobs

Certificates

Create certificate

View other options

6d7eab80376cfdff8e...

(click on cert name)

Things > RIMPLEDEVICE > 6d7eab80376cfdff8e53...

CERTIFICATE

6d7eab80376cfdff8e53fb1527316422e968f4218f0115ea4c6e430f330017f4

ACTIVE

Actions

Activate

Deactivate

Revoke

Accept transfer

Reject transfer

Revoke transfer

Start transfer

Attach policy

Attach thing

Download

Delete

Details

Policies

Things

Non-compliance

Certificate ARN

A certificate Amazon Resource Name (ARN) uniquely identifies this certificate. **Learn more**

arn:aws:iot:us-east-1:045205798610:cert/6d7eab80376cfdff8e53fb15

Details

Issuer
OU=Amazon Web Services O\=Amazon.com Inc. L\=Seattle ST\=Washington C\=US
Subject
CN=RIMPLEDEVICE,O=Chariot Solutions,L=Fort Washington,ST=Pennsylvania,C= us
Create date
Sep 25, 2019 11:12:35 AM -0400
Effective date
Sep 25, 2019 11:10:35 AM -0400
Expiration date

Downloads

Name

6d7eab8037-certificate.pem.crt.txt

6d7eab8037-certificate.pem.c

-----BEGIN CERTIFICATE-----
MIIC4jCCAcqgAwIBAgIUbWovF+JVZ/GtT4Ny4DxlhekzRTcwDQYJKoZIhvcNAQEL
BQAwTTFlMEkGA1UECwxCQW1hem9uIFdlYiBTZXJ2aWNlcyBPPUFtYXpvbi5jb20g
SW5jLiBMPVNlYXR0bGUgU1Q9V2FzaGluZ3RvbiBDPVVTMB4XDTE5MDkyNTE1MTAz
NVoXDTQ5MTIzMTIzNTk1OVowcjEMMAoGA1UEBhMDBXVzMRUwEwYDVQQIEwxQZW5u
c3lsdmFuaWExGDAWBgNVBAcTD0ZvcnQgV2FzaGluZ3RvbjEaMBgGA1UEChMRQ2hh
cmlvdCBTb2x1dGlvbnMxFTATBgNVBAMTDFJJTVBMRURFVklDRTBZMBMGByqGSM49
AgEGCCqGSM49AwEHA0IABBza9wMyW7/UvPKzJZmd66bzz//1yuP85DkYo3V3yLeT
Yfav+/iA2irNGLjsq4cHmIUZGROFqC2UZV4CzGPerYCjYDBeMB8GA1UdIwQYMBaA
FHctI6mafvPs2+sV1QnoEsyoQF/XMB0GA1UdDgQWBBR68kUd3/X75Vg+O4P19EnV
Cbu95jAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0BAQsF
AAOCAQEAHoZ3YMCBOqwX+yZ0m8wMICsX/r1On7V0Jbohoxdjycqdpc2wSr1Cb2ae
5G8doOq13BLlSQWqW/H5lp8CYSkfvgDcp7aGlx7ntqHTu6s4J/W6TM2c3DNS6Um7
esS84GnyOroCgOGLKdewTc3GYilJ90tg3Lmo3Nk/27A7izHhsBi2T+kFywZaIHjW
EJeDhYZn6xOOlpxWHNmchmsobGQCuvLbSunIV0NqChC0fZRrh+FtA0mxYMYdnOv5
Cb1kQYBK1HSnxeSpaYGyHSxaHgPMuGOqlQ4yxAykC+bF3309T28MAwp1eWSFGbdn
fCfT8jWl2LT9w3VPAy7KE+XUaMCO0Q==
-----END CERTIFICATE-----

Next, Assign an AWS IoT Policy

IoT
policy

IoT Policy: a set of **allowed operations assigned** various IoT Core **Things**

CHARIOT SOLUTIONS

What can IoT Policies do?

- Determine what Things are allowed to do in AWS
  - Connect to IoT Core via the Broker
  - Publish to topics
  - Receive messages / Subscribe to topics
  - Filter messages in topics
- Policies can be shared across many devices
- Policies can use variables to represent information from the device via its certificate

CHARIOT SOLUTIONS

AWS IoT

Monitor

Onboard

Manage

Greengrass

Secure

Certificates

Policies

CAs

Role Aliases

Authorizers

Defend

Act

Test

Policies are managed via the Secure Iot Core menu

Create a policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the AWS IoT Policies documentation page.

Name

connect-and-access-sensor-topics

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:us-east-1:1[redacted]14:client/${iot:Certificate.Subject.CommonName}"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Receive"
      ],
      "Resource": "arn:aws:iot:us-east-1:1[redacted]4:topic/things/${iot:ClientId}/*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:us-east-1:1[redacted]14:topicfilter/things/${iot:ClientId}/*"
    }
  ]
}
```

AWS IoT

Monitor

Onboard

Manage

Greengrass

Secure

- **Certificates**
- Policies
- CAs
- Role Aliases
- Authorizers

Defend

Act

Test

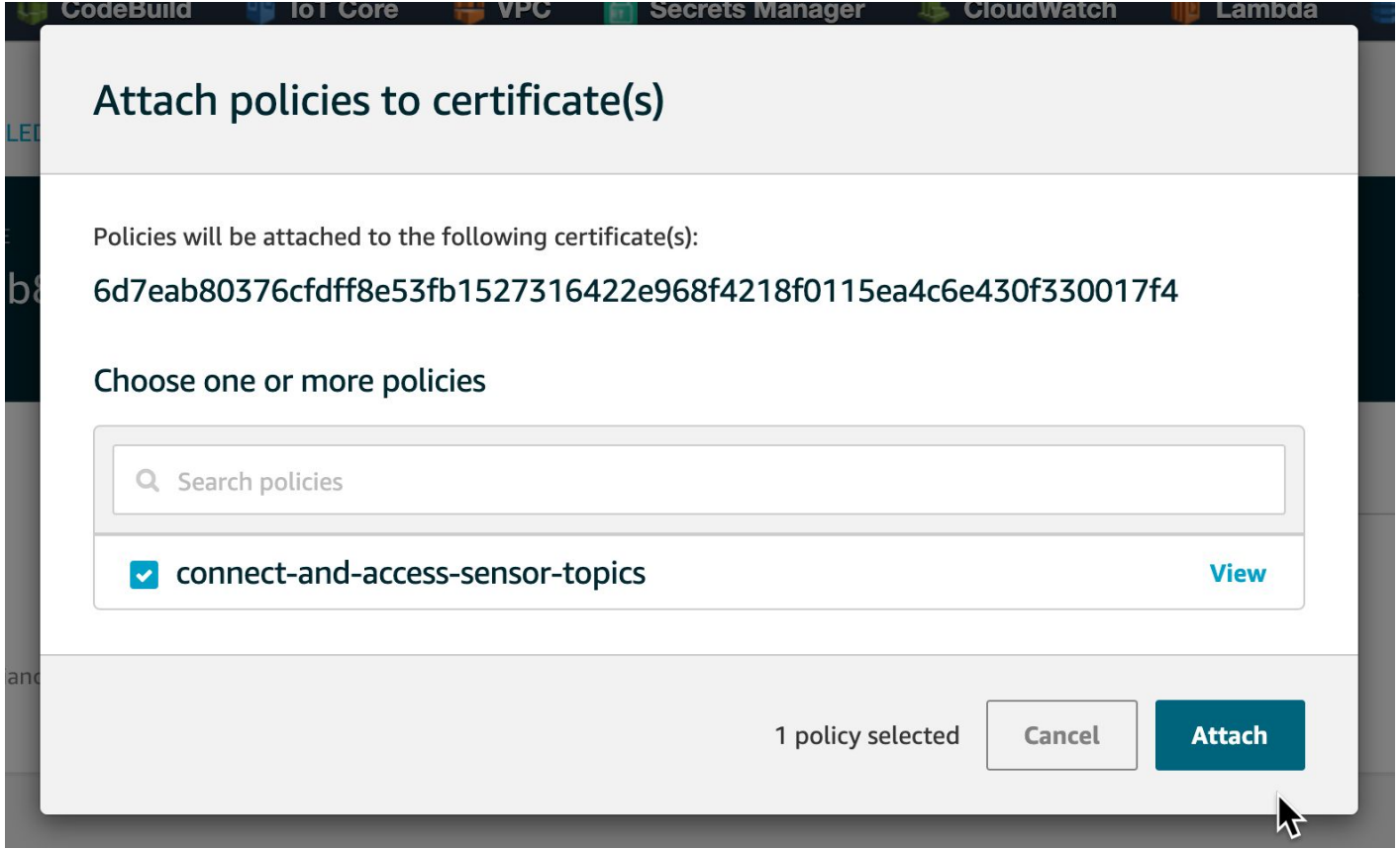
Certificates

Search certificates

6cfb917d8:
ACTIVE

Activate
Deactivate
Revoke
Accept transfer
Reject transfer
Revoke transfer
Start transfer
Attach policy
Attach thing
Download
Delete

0fbf00719b96f3b649...
ACTIVE


CodeBuild
IoT Core
VPC
Secrets Manager
CloudWatch
Lambda
Attach policies to certificate(s)
Policies will be attached to the following certificate(s):
6d7eab80376cfdff8e53fb1527316422e968f4218f0115ea4c6e430f330017f4
Choose one or more policies
Search policies
connect-and-access-sensor-topics
View
1 policy selected
Cancel
Attach

Now, Communicate!

- Attach your client certificate to the device
- Configure MQTT for TLS using the certificate
- Publish, Subscribe to MQTT Topics using Broker

CHARIOT SOLUTIONS

References

AWS - Creating and activating a Device Certificate -
https://docs.aws.amazon.com/iot/latest/developerguide/create-device-certificate.html

IOT Core Security Model -
https://aws.amazon.com/blogs/iot/understanding-the-aws-iot-security-model/

AWS - AWS IoT Policy Actions -
https://docs.aws.amazon.com/iot/latest/developerguide/create-device-certificate.html

Arduino Tutorial - Connecting to AWS IoT Core with MKR-1010 WIFI and ECCX08
https://create.arduino.cc/projecthub/Arduino_Genuino/securely-connecting-an-arduino-mkr-wifi-1010-to-aws-iot-core-a9f365

CHARIOT SOLUTIONS

Technology in the Service of Business.

Chariot Solutions is the Greater Philadelphia region's top IT consulting firm specializing in software development, systems integration, mobile application development and training.

Our team includes many of the top software architects in the area, with deep technical expertise, industry knowledge and a genuine passion for software development.

Visit us online at **chariotsolutions.com**.

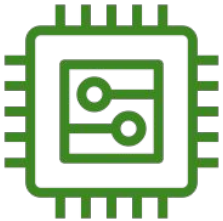
CHARIOT SOLUTIONS

TODO - what is PKI and WHY here?

- Not new
- OpenSSL, TLS, GPG - all use asymmetric (private/pblic key) pairs
- Leveraging to use for this
- Most people don't use client certs - this is what we do

CHARIOT SOLUTIONS

Authenticating clients with X.509 Certificates



IoT Device - "Thing" (example: Arduino)

X.509 private key and *certificate* installed on IoT Device

MQTT authenticate via certificate

Device gateway

X.509 certificate installed on AWS IoT

CHARIOT SOLUTIONS

Things > RIMPLEDEVICE

THING

RIMPLEDEVICE

NO TYPE

Actions

Details

Security

Thing Groups

Billing Groups

Shadow

Interact

Activity

Jobs

Violations

Defender metrics

Thing ARN

Edit

A thing Amazon Resource Name uniquely identifies this thing.

arn:aws:iot:us-east-1:04[redacted]10:thing/RIMPLEDEVICE

Type

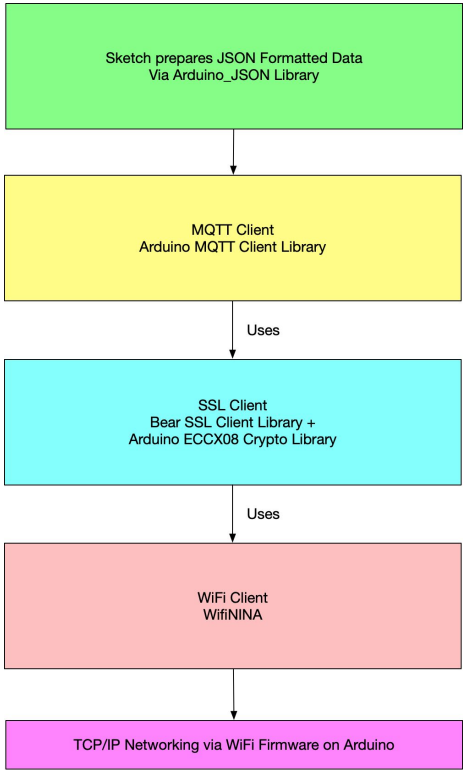
No type

Unique Amazon Resource Name for your IoT Device. Important for configuration, monitoring, etc.

View IoT Thing Details

Communicating to IoT Core via IoT Device

- Load your key pair and configure network authentication credentials, AWS IoT Core *endpoint* for MQTT traffic, and IoT Client ID in the Sketch
- Load networking stack
- Connect to Wifi, MQTT
- Send message via MQTT Client



CHARIOT SOLUTIONS

Configuring the Device

```
WiFiClient wifiClient;
BearSSLClient sslClient(wifiClient);
MqttClient mqttClient(sslClient);

unsigned long getTime() {
  return WiFi.getTime();
}

setup() {
    ArduinoBearSSL.onGetTime(getTime);
    if (!ECCX08.begin()) {
      Serial.println("No ECCX08 present!");
      while (1);
    }

    sslClient.setEccSlot(0, CERTIFICATE);
    mqttClient.setId(CLIENT_ID);
}
```

Configure the SSL and MQTT APIs

Use the wifi network for establishing the current Unix time (TLS needs this)

Effective halt with no crypto chip

Associate private key for certificate from ECC slot 0 and assign to MQTT Client (private key used to generate messages)

CHARIOT SOLUTIONS

Connecting to WIFI, MQTT

```
void connectWiFi() {
  while (WiFi.begin(WIFI_SSID, WIFI_PASS)
         != WL_CONNECTED) {
    // failed, retry
    Serial.print(".");
    delay(3000);
  }
}

void connectMQTT() {
 while (
   !mqttClient.connect(MQTT_BROKER, 8883)) {
    // failed, retry
    Serial.print(".");
    delay(5000);
  }
}
```

Provide WIFI credentials to WiFi.begin()

Provide Broker URL and Port to mqttClient.connect()

CHARIOT SOLUTIONS

Reading Sensors and Sending Data…

```
void sendSensorData() {
...
  float humidity    = ENV.readHumidity();
  float pressure    = ENV.readPressure();
…
  JSONVar payload;
…
  payload["humidity"] = humidity;
  payload["pressure"] = pressure;
…
  mqttClient.beginMessage("things/" +
       clientId + "/environment");
  mqttClient.print(JSON.stringify(payload));
  mqttClient.endMessage();
}
```

ENV is the MKRENV sensor library for our sensor shield (config not shown)

Assign properties to JSON fields

Create a message on a topic, print our JSON string to it, then end the message to send it.

CHARIOT SOLUTIONS

Creating and Using Certificates

Who creates PK / CSR?	Approach	Pros	Cons
Device (via encryption chip)	IoT Device creates CSR based on internal private key, CA signs key	• Cert uniquely identifies device • Amazon is a CA	• Need infrastructure / process to set up keys/CSR on devices
AWS	AWS Creates a KeyPair and CSR in IoT Core	• Easily managed from AWS	• Could mess up / install key on more than 1 device by mistake • Private key gets passed around

CHARIOT SOLUTIONS

The loop··· do this forever…

```
void loop() {
  if (WiFi.status() != WL_CONNECTED) {
    connectWiFi();
  }

  if (!mqttClient.connected()) {
    connectMQTT();
  }

  if (... past interval timing ...) {
    sendSensorData();
  }

  // sleep or delay here...
}
```

WiFi API can sense whether it is connected or not. If not, reconnect.

Same with MQTT Client - connect if no connection is established

We have something to say, call our sensor reading API and send the data.

CHARIOT SOLUTIONS

Advanced Users - managing your own Certs with a CA

You	CSR and Key created outside of AWS, cert installed on AWS and device	• Use existing key management infrastructure	• Movement of CSR, PK, to AWS AND Device • You have to add your CA to AWS

CHARIOT SOLUTIONS