**Tarea 2: AWS IoT**

*El objetivo de esta tarea es conocer con detalle el servicio AWS IoT Core y las opciones que tiene para realizar una provisión segura de certificados de forma automática mediante la opción JITR.*

***Ejercicio #1:** Conexión de dispositivo a AWS IoT manualmente(puntuación 15%)*

*Se deberá crear una CA, registrarla y publicar con certificado emitido por ella que quede en estado PENDING REGISTRATION tras una primera publicación*

*A continuación se deberá crear una regla que mediante una función Lambda active el certificado y le asocie una policy que permita la actualización del shadow del dispositivo.*

***Resultado:** capturas detalladas que permitan ver la realización de la práctica como por ejemplo: pantalla de certificado en estado PENDING REGISTRATION y posteriormente ACTIVE, captura de las publicaciones con mosquitto-client, de la pantalla de creación de la regla, del detalle de vuestra CA y de la actualización final del shadow tras la activación del certificado.*

Generando CA:

Clave privada:

openssl genrsa -aes256 -out rootCA.key 4096

```
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs> openssl genrsa -aes256 -out rootCA.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.........................++++
.....................................................................................++++
e is 65537 (0x010001)
Enter pass phrase for rootCA.key:
Verifying - Enter pass phrase for rootCA.key:
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs>
```

Certificado:

openssl req -key rootCA.key -new -x509 -days 7300 -out rootCA.pem -config C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs\openssl.cnf

```
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs> openssl req -key rootCA.key -new -x509 -days 7300 -out
rootCA.pem -config C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs\openssl.cnf
Enter pass phrase for rootCA.key:
Can't load ./.rnd into RNG
14948:error:2406F079:random number generator:RAND_load_file:Cannot open file:crypto\rand\randfile.c:98:Filename=./.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Navarra
Locality Name (eg, city) []:Pamplona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Iker
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:IoT
Email Address []:
```

Clave privada dispositivo:

openssl genrsa -out deviceCert_001.key 2048

```
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs> openssl genrsa -out deviceCert_001.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.................................+++++
.....................................................................+++++
e is 65537 (0x010001)
```

CSR:

openssl req -new -key .\deviceCert_001.key -out deviceCert_001.csr -config C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs\openssl.cnf

```
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs> openssl req -new -key .\deviceCert_001.key -out deviceC
ert_001.csr -config C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs\openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Navarra
Locality Name (eg, city) []:Pamplona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Iker
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:001
Email Address []:
```

Firmar csr:

openssl x509 -req -in .\deviceCert_001.csr -CA .\rootCA.pem -CAkey .\rootCA.key -CAcreateserial -out .\deviceCert_001.crt -days 365 -sha256

```
PS C:\Users\Admin\Documents\Tech\ENIIT\Ciberseguridad\09_Seguridad_IoT\02_Tarea\certs> openssl x509 -req -in .\deviceCert_001.csr -CA .\rootCA
.pem -CAkey .\rootCA.key -CAcreateserial -out .\deviceCert_001.crt -days 365 -sha256
Signature ok
subject=C = SP, ST = Navarra, L = Pamplona, O = Iker, CN = 001
Getting CA Private Key
Enter pass phrase for .\rootCA.key:
```

Añadir CA en AWS:

Desafio de AWS:

**Paso 1:** Genere un par de claves para el certificado de verificación de clave privada

```
openssl genrsa -out verificationCert.key 2048
```

**Paso 2:** Copie este código de registro

```
b0bf33ecba351cc3e491c049cf0835ea99bc7220fda1865d28000f9437c5a28a
```

**Paso 3:** Cree una CSR con este código de registro

```
openssl req -new -key verificationCert.key -out verificationCert.csr
```

Inserte el código de registro en el campo **Nombre común**

```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []: b0bf33ecba351cc3e491c049cf0835ea99bc7220fda1865d28000f9437c5a28a
Email Address []:
```

**Paso 4:** Use la CSR firmada con la clave privada de CA para crear un certificado de verificación de clave privada

```
openssl x509 -req -in verificationCert.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out verificationCer
```

**Paso 5:** Cargue el certificado de CA (rootCA.pem)

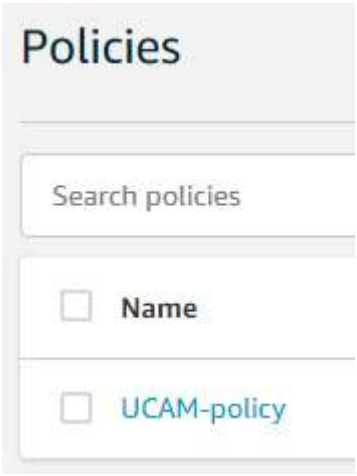
rootCA.pem

**Paso 6:** Cargue el certificado de verificación (verificationCert.crt)

verificationCert.crt

- [x] Activar certificado de CA
- [x] Habilitar el registro automático de certificados de dispositivo

Politica:




Creamos nuestro primer thing sin certificado y nos conectamos por primera vez:

mosquitto_pub --cert deviceCertAndCACert_001.crt --key deviceCert_001.key --cafile AWS-IoT.pem -h ENDPOINT PERSONALIZADO DE AWS -p 8883 -t '$aws/things/UCAM_001/shadow/update' -m "{ \"state\": {\"reported\" : { \"color\" : { \"r\" :255, \"g\": 255, \"b\": 0 } } }}" -i UCAM_001

mosquitto_pub --cert deviceCertAndCACert_001.crt --key deviceCert_001.key --cafile AWS-IoT.pem -h albq291qfo11k-ats.iot.eu-west-1.amazonaws.com -p 8883 -t "$aws/things/UCAM_001/shadow/update" -m "{ \"state\": {\"reported\" : { \"color\" : { \"r\" :255, \"g\": 255, \"b\": 0 } } }}" -i UCAM_001

Estoy teniendo este error: Error: Problem setting TLS options: File not found.

No he podido resolverlo.