Generating Required Keys Guide

For each Producer a pub/priv RSA 2048 keypair is required in two formats. These keys will be used in the Bluetooth Beacon and Verification Server:

- Private Producer key in PEM format
- Private Producer key in DER format
- Public Producer key in PEM format
- Public Producer key in DER format

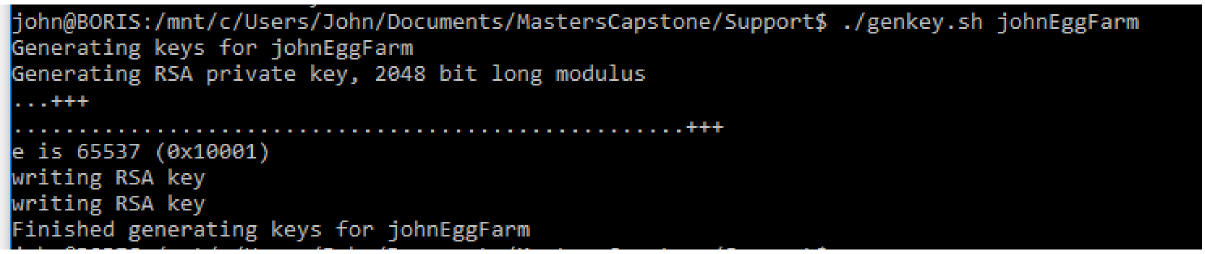
A simple shell script has been produced to assist in generating these keys using openSSL.

Note: The script needs to run on a *unix based machine with openssl installed.

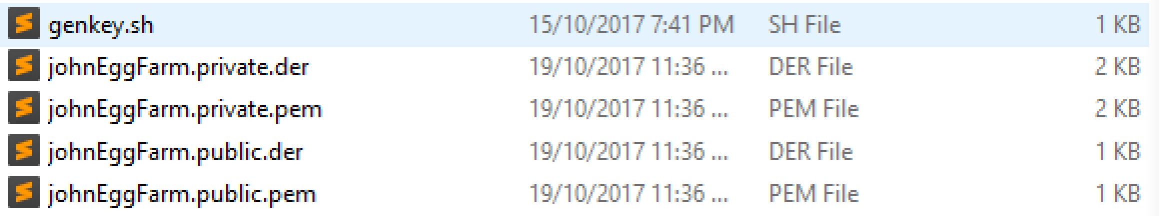
The genkey.sh script can be executed as following:

./genkey.sh producerName

producerName being the name of the Producer to create the keys for. If the script succeeds four keys should appear in the folder and will appear as below:



```
john@BORIS:/mnt/c/Users/John/Documents/MastersCapstone/Support$ ./genkey.sh johnEggFarm
Generating keys for johnEggFarm
Generating RSA private key, 2048 bit long modulus
...+++
....................................................+++
e is 65537 (0x10001)
writing RSA key
writing RSA key
Finished generating keys for johnEggFarm
```



genkey.sh	15/10/2017 7:41 PM	SH File	1 KB
johnEggFarm.private.der	19/10/2017 11:36 ...	DER File	2 KB
johnEggFarm.private.pem	19/10/2017 11:36 ...	PEM File	2 KB
johnEggFarm.public.der	19/10/2017 11:36 ...	DER File	1 KB
johnEggFarm.public.pem	19/10/2017 11:36 ...	PEM File	1 KB