Markus Afonso, Devin Kandola
Set C
March 19, 2024

(Q1) Who is the issuer of the two certificates?

The issuer is DigiCert Inc.

```
issuer=C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
```

(S1) Provide screenshots showing that the decrypted signature ends in the hash calculated in the previous step.

```
[03/19/24]seed@VM:~/Desktop$ gcc -o rsa rsa.c -lcrypto
[03/19/24]seed@VM:~/Desktop$ ./rsa
Decrypted message =  01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFF003031300D06096086480165030402010500042023898B872AD8D70B3A150A356425DD3C59CD5028AC05D648472882EC84954498
[03/19/24]seed@VM:~/Desktop$ openssl asn1parse -i -in c0.pem -strparse 4 -out
asn1parse: Option -out needs a value
asn1parse: Use -help for summary.
[03/19/24]seed@VM:~/Desktop$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout
[03/19/24]seed@VM:~/Desktop$ sha256sum c0_body.bin
23898b872ad8d70b3a150a356425dd3c59cd5028ac05d648472882ec84954498  c0_body.bin
[03/19/24]seed@VM:~/Desktop$
```

(Q2) What data does such a certificate contain?

The certificate contains information about the signer. It includes the entity's name, a special number that identifies the certificate, when the certificate starts and ends being valid, who gave out the certificate, and the entity's public key. This information helps make sure that communications over the internet are secure and that you're connecting to the right website or service.

(Q3) List the steps to manually verify that an X.509 certificate is authentic.

- Retrieve the certificate by downloading it using the following command from www.bcit.ca "openssl s_client -connect www.bcit.ca:443 –showcerts"
- To retrieve the public key of the certificate authority "openssl x509 -in c1.pem -noout –modulus" and to display the exponent use the "openssl x509 -in c1.pem -text -noout | grep "Exponent"".
- Then we decrypted the signature in digital certificate with the CA's public key and compared it to the hash of the certificate and saw that they matched which confirms that the certificate had been signed and was authentic

(Q4) If we only get one certificate after running the following command, what does that mean? where would we find the issuer's public key?

If only one certificate is retrieved using the openssl s_client -connect www.bcit.ca:443 -showcerts command, it means that the server is directly providing its certificate without any intermediate certificates. In other words, it is self-signed.