**TNE30024**

**Digital Certificates**

**Tutorial 3 (week 4)**

**Questions**

1. What is the certification path for swin.edu.au?

Using SSL/TLS certificate checker to investigate the URL path, for instance, this link: <https://www.digicert.com/help/>

TLS Certificate shows:

Common Name = www.swin.edu.au

Organization = Swinburne University of Technology

City/Locality = Hawthorn

State/Province = Victoria

Country = AU

Subject Alternative Names = www.swin.edu.au, swin.edu.au, swinburne.edu.au, www.swinburne.edu.au

Issuer = DigiCert Global G2 TLS RSA SHA256 2020 CA1

Serial Number = 0E8B639773B96406D9BBCFFEA89F1CDF

SHA1 Thumbprint = B26F720D588339C9C246A9DAE19049D77D2AF7B5

Key Length = 2048

Signature algorithm = SHA256-RSA

Secure Renegotiation:

Or using Mac Terminal OpenSSL command as:

openssl s\_client -connect swin.edu.au:443 -showcerts

1. What is the certification path for qantas.com.au?

Using SSL/TLS certificate checker to investigate the URL path, for instance, this link: <https://www.digicert.com/help/>

TLS Certificate shows:

Connecting to 2600:1415:10::17ce:c773

CONNECTED(00000005)

depth=2 C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

verify return:1

depth=1 C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1

verify return:1

depth=0 C=AU, ST=New South Wales, L=Mascot, O=Qantas Airways Limited, CN=\*.qantas.com.au

verify return:1

---

Certificate chain

0 s:C=AU, ST=New South Wales, L=Mascot, O=Qantas Airways Limited, CN=\*.qantas.com.au

i:C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1

a:PKEY: id-ecPublicKey, 256 (bit); sigalg: RSA-SHA256

v:NotBefore: Nov 8 00:00:00 2023 GMT; NotAfter: Nov 8 23:59:59 2024 GMT

-----BEGIN CERTIFICATE-----

MIIGBTCCBO2gAwIBAgIQCh7B25iHFFzB5XxeAs/KOzANBgkqhkiG9w0BAQsFADBP

MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE

aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMzExMDgwMDAwMDBa

Fw0yNDExMDgyMzU5NTlaMHMxCzAJBgNVBAYTAkFVMRgwFgYDVQQIEw9OZXcgU291

dGggV2FsZXMxDzANBgNVBAcTBk1hc2NvdDEfMB0GA1UEChMWUWFudGFzIEFpcndh

eXMgTGltaXRlZDEYMBYGA1UEAwwPKi5xYW50YXMuY29tLmF1MFkwEwYHKoZIzj0C

AQYIKoZIzj0DAQcDQgAEb0BCL0eCHDOQtVAnJAn3+lKGQpxHR9HTb0RQ2GxtTmFS

CKxuAMSKk+221WaG1WvL85uWevMSYYmO9pa6l8UE1aOCA4IwggN+MB8GA1UdIwQY

MBaAFLdrouqoqoSMeeq02g+YssWVdrn0MB0GA1UdDgQWBBTzyRmUrACSewYJHq52

njb5QgysYzApBgNVHREEIjAggg8qLnFhbnRhcy5jb20uYXWCDXFhbnRhcy5jb20u

YXUwPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDovL3d3

dy5kaWdpY2VydC5jb20vQ1BTMA4GA1UdDwEB/wQEAwIDiDAdBgNVHSUEFjAUBggr

BgEFBQcDAQYIKwYBBQUHAwIwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDovL2Ny

bDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS00LmNy

bDBAoD6gPIY6aHR0cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNB

U0hBMjU2MjAyMENBMS00LmNybDB/BggrBgEFBQcBAQRzMHEwJAYIKwYBBQUHMAGG

GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBJBggrBgEFBQcwAoY9aHR0cDovL2Nh

Y2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS0x

LmNydDAMBgNVHRMBAf8EAjAAMIIBfwYKKwYBBAHWeQIEAgSCAW8EggFrAWkAdgDu

zdBk1dsazsVct520zROiModGfLzs3sNRSFlGcR+1mwAAAYutqtz8AAAEAwBHMEUC

ICN2y8ql22/EgOZm3pUHs1DAKNpbXWiKa3zkRjI11PdsAiEA4wd2my6fh4Re762Z

f37UHQWWDeRfv3ACZrSsKjisNuMAdwBIsONr2qZHNA/lagL6nTDrHFIBy1bdLIHZ

u7+rOdiEcwAAAYutqtyeAAAEAwBIMEYCIQCpyog4JMZOoGN2zGPfdR5+MG39199K

gyu4i/umGsA+JAIhANb0S+sgd4CD1YVAYIqmvWzESDL65zuAHJIL4Ps1CP7EAHYA

PxdLT9ciR1iUHWUchL4NEu2QN38fhWrrwb8ohez4ZG4AAAGLrarc6wAABAMARzBF

AiEAoitCiz0IjzSEyuZpkVt1c6fnd09e6aV8n9ZsG2b5fN8CIDcUytyluRIgmxZV

c7rFv0A5cFpTEa4z0rVwIAoxw/vcMA0GCSqGSIb3DQEBCwUAA4IBAQCWP0CAJXHd

aOQh6QA0HT9xYuXtzj5yDDaKWu/RMxDHgOJrLgT3dbCz493PEBtlXOxSrn+eNxzK

WhqvOKxQOZ7y4DdEGRVefl9qWaxX4CNChsr/5Uh7ihTNsfyrF3Eh7XIuX7JQe4m8

7I8Shb8f4IKiptFHMMjbEiQoUm9aNvpNvGvDjWvlEwZykxmKIiQ2newvTJc/p5cG

WfbDuwjTiKgtpCSLnRSdFvwanQIQAhdiML8svZ9HK6rMvanh04Pah9Ixb/zILgnD

l2xDd4cEk1pux4VdCOjO8WB2siAnx9ynANNyZdahlOHuyN0piuqgZMot7t9kpy74

aicQUAG1qGxV

-----END CERTIFICATE-----

1 s:C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1

i:C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256

v:NotBefore: Apr 14 00:00:00 2021 GMT; NotAfter: Apr 13 23:59:59 2031 GMT

-----BEGIN CERTIFICATE-----

MIIEvjCCA6agAwIBAgIQBtjZBNVYQ0b2ii+nVCJ+xDANBgkqhkiG9w0BAQsFADBh

MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3

d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD

QTAeFw0yMTA0MTQwMDAwMDBaFw0zMTA0MTMyMzU5NTlaME8xCzAJBgNVBAYTAlVT

MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxKTAnBgNVBAMTIERpZ2lDZXJ0IFRMUyBS

U0EgU0hBMjU2IDIwMjAgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC

AQEAwUuzZUdwvN1PWNvsnO3DZuUfMRNUrUpmRh8sCuxkB+Uu3Ny5CiDt3+PE0J6a

qXodgojlEVbbHp9YwlHnLDQNLtKS4VbL8Xlfs7uHyiUDe5pSQWYQYE9XE0nw6Ddn

g9/n00tnTCJRpt8OmRDtV1F0JuJ9x8piLhMbfyOIJVNvwTRYAIuE//i+p1hJInuW

raKImxW8oHzf6VGo1bDtN+I2tIJLYrVJmuzHZ9bjPvXj1hJeRPG/cUJ9WIQDgLGB

Afr5yjK7tI4nhyfFK3TUqNaX3sNk+crOU6JWvHgXjkkDKa77SU+kFbnO8lwZV21r

eacroicgE7XQPUDTITAHk+qZ9QIDAQABo4IBgjCCAX4wEgYDVR0TAQH/BAgwBgEB

/wIBADAdBgNVHQ4EFgQUt2ui6qiqhIx56rTaD5iyxZV2ufQwHwYDVR0jBBgwFoAU

A95QNVbRTLtm8KPiGxvDl7I90VUwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQG

CCsGAQUFBwMBBggrBgEFBQcDAjB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGG

GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBABggrBgEFBQcwAoY0aHR0cDovL2Nh

Y2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsUm9vdENBLmNydDBCBgNV

HR8EOzA5MDegNaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vRGlnaUNlcnRH

bG9iYWxSb290Q0EuY3JsMD0GA1UdIAQ2MDQwCwYJYIZIAYb9bAIBMAcGBWeBDAEB

MAgGBmeBDAECATAIBgZngQwBAgIwCAYGZ4EMAQIDMA0GCSqGSIb3DQEBCwUAA4IB

AQCAMs5eC91uWg0Kr+HWhMvAjvqFcO3aXbMM9yt1QP6FCvrzMXi3cEsaiVi6gL3z

ax3pfs8LulicWdSQ0/1s/dCYbbdxglvPbQtaCdB73sRD2Cqk3p5BJl+7j5nL3a7h

qG+fh/50tx8bIKuxT8b1Z11dmzzp/2n3YWzW2fP9NsarA4h20ksudYbj/NhVfSbC

EXffPgK2fPOre3qGNm+499iTcc+G33Mw+nur7SpZyEKEOxEXGlLzyQ4UfaJbcme6

ce1XR2bFuAJKZTRei9AqPCCcUZlM51Ke92sRKw2Sfh3oius2FkOH6ipjv3U/697E

A7sKPPcw7+uvTPyLNhBzPvOk

-----END CERTIFICATE-----

---

Server certificate

subject=C=AU, ST=New South Wales, L=Mascot, O=Qantas Airways Limited, CN=\*.qantas.com.au

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

---

No client certificate CA names sent

Peer signing digest: SHA256

Peer signature type: ECDSA

Server Temp Key: X25519, 253 bits

---

SSL handshake has read 3152 bytes and written 401 bytes

Verification: OK

---

New, TLSv1.3, Cipher is TLS\_AES\_256\_GCM\_SHA384

Server public key is 256 bit

This TLS version forbids renegotiation.

Compression: NONE

Expansion: NONE

No ALPN negotiated

Early data was not sent

Verify return code: 0 (ok)

---

---

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS\_AES\_256\_GCM\_SHA384

Session-ID: 81903AABDB39B56374BBF7740699EDB0C547570690B4A98F6DEE7EA4717BB664

Session-ID-ctx:

Resumption PSK: 8B732AAE43A5B648F021CADA55DC462408E0461B04B44AB3D69049ECCE10E8BD496F822ECB0ED993B6C344E632178FB3

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 83100 (seconds)

TLS session ticket:

0000 - 00 03 49 bb a4 4c f1 c7-c3 7c ad 72 be c4 15 2a ..I..L...|.r...\*

0010 - 8f bc 5a 00 cb dd 27 ce-36 ad d9 e5 97 c1 34 a0 ..Z...'.6.....4.

0020 - ed df 85 b3 4f 86 8b db-90 a5 e1 7b 9f 69 0e f8 ....O......{.i..

0030 - ad bd ae 10 da a9 12 3a-18 62 67 cd 02 e7 ec cb .......:.bg.....

0040 - dc 50 30 a4 20 62 d1 5b-99 10 0c 5e ea c3 0f b3 .P0. b.[...^....

0050 - 95 e6 41 5f bd 4f db 26-fc 28 30 49 45 08 5f a5 ..A\_.O.&.(0IE.\_.

0060 - 53 f6 38 89 6f 80 c6 fb-06 9e 3b 19 6b 31 96 3b S.8.o.....;.k1.;

0070 - e4 a5 0d a2 13 4d 2d fa-30 bd 4f 38 ce 87 7f c4 .....M-.0.O8....

0080 - 74 99 7c 72 e1 bc bd 36-7d de 4e 73 2a 40 53 50 t.|r...6}.Ns\*@SP

0090 - 93 9f e6 01 da 5d fb b0-17 cb 8d cf 13 0a 60 4a .....]........`J

00a0 - d4 7e 34 b8 7c 72 6c 5b-4d f8 0f a5 e8 0f 7c 17 .~4.|rl[M.....|.

00b0 - af ae 97 b9 5f 3a 0f af-de d1 9c a7 93 3c bd 10 ....\_:.......<..

00c0 - bb b4 3d 4d db fe 36 3e-12 38 35 66 db 56 1e 3e ..=M..6>.85f.V.>

00d0 - 24 4d 78 1c 14 1c 68 2f-83 ca 8e 7e 3f 46 3f 81 $Mx...h/...~?F?.

Start Time: 1724219972

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

Max Early Data: 0

---

read R BLOCK

---

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS\_AES\_256\_GCM\_SHA384

Session-ID: F17FE8A207486025BC2E298BAE3FA70AA642E8D71C7D8C588F0581417361D771

Session-ID-ctx:

Resumption PSK: 4238B1599873B9B905C94D06B05D3E0BA93FC925035D1BC11BE14BE5D9827A6222E84E76C2AC6CFD487DEFF22330DCFF

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 83100 (seconds)

TLS session ticket:

0000 - 00 03 49 bb a4 4c f1 c7-c3 7c ad 72 be c4 15 2a ..I..L...|.r...\*

0010 - b7 c5 6f 11 86 25 3b fe-ed a5 60 dc 3a e3 11 be ..o..%;...`.:...

0020 - 28 ee 42 ca 27 fe 62 dd-9b 0b 00 84 2c 19 a2 18 (.B.'.b.....,...

0030 - d3 c4 45 45 5c 9f aa dd-13 45 2c 9a 64 25 f6 14 ..EE\....E,.d%..

0040 - 45 81 dc e5 b8 a2 33 f8-c2 f7 67 65 05 a7 db f0 E.....3...ge....

0050 - 70 43 ad 6b af cd 8b ff-7b 32 d0 fa 77 20 9e 99 pC.k....{2..w ..

0060 - 19 0f 88 cc 7e 02 b2 f3-f2 a9 cf 99 d7 2c 68 a9 ....~........,h.

0070 - 32 93 1a 49 08 ab 93 9a-e6 37 a0 f3 39 15 23 63 2..I.....7..9.#c

0080 - 41 22 92 1c 52 8b 31 e5-fa 57 b2 93 b7 1d ba b8 A"..R.1..W......

0090 - d4 bc 55 fb 22 9c 1f ea-47 dc a3 65 74 dc f8 18 ..U."...G..et...

00a0 - 35 c0 12 b6 fc 68 e5 78-93 d8 7e 22 ea f8 1f 1f 5....h.x..~"....

00b0 - e7 87 48 f2 72 d3 b1 92-c1 1a 83 2e 6e 43 e9 4c ..H.r.......nC.L

00c0 - be 93 e5 ea 57 89 6d f4-e0 cc d7 29 9f 0a 68 a3 ....W.m....)..h.

00d0 - cc 8d fb a0 02 82 1d 0b-80 fc 8f 6c ee 0f 34 14 ...........l..4.

Start Time: 1724219972

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

Max Early Data: 0

--- Or using Mac Terminal OpenSSL command as:

openssl s\_client -connect qantas.com.au:443 -showcerts

1. You have been given the following four certificates. Answer the following questions regarding them:
   1. What Canonical Names do the certificates verify?

You'd need to look at the Subject Common Name or SAN (Subject Alternative Name) fields within each certificate. This information identifies the domain or domains the certificate is authorized to secure.

* 1. Which is the root certificate?

Typically, the root certificate is self-signed and trusted by client devices. Look for a certificate where the issuer and subject are the same entity, typically a CA’s root certificate.

* 1. Which are intermediate certificates?

Intermediate certificates bridge the trust between the root certificate and the end-entity (or leaf) certificate. These certificates will have their issuer as the root or another intermediate certificate.

* 1. Which is the leaf certificate?

The leaf certificate is directly used to secure communications with the end users and is issued to the domain in question. This certificate is at the end of the certificate chain before any client or user certificates. (Or final certificate, cannot sign anyone else).

* 1. What is the certificate verification path?

The verification path would start from the leaf certificate and trace back through any intermediate certificates up to the root certificate. Each certificate in the path should be valid, with the issuer of each certificate matching the subject of the next certificate up the chain.

* 1. Are these public or private certificates?

You will need to use a certificate viewer to determine the relevant fields. You should have one installed on your PC. If not you can use an online viewer such as <https://www.sslchecker.com/certdecoder>

PUBLIC – look at the subject and issuer Organization – this show Root and Root (This is a root cert)

Certificate 1

-----BEGIN CERTIFICATE-----

MIIDezCCAmOgAwIBAgIUdx5koldD8BJ0tzzfKW9HHO35QkcwDQYJKoZIhvcNAQEL BQAwTTELMAkGA1UEBhMCQVUxDDAKBgNVBAgMA1ZpYzESMBAGA1UEBwwJTWVsYm91 cm5lMQ0wCwYDVQQKDARSb290MQ0wCwYDVQQDDARSb290MB4XDTI0MDUyMDA1NTA1 OFoXDTI1MDUyMDA1NTA1OFowTTELMAkGA1UEBhMCQVUxDDAKBgNVBAgMA1ZpYzES

MBAGA1UEBwwJTWVsYm91cm5lMQ0wCwYDVQQKDARSb290MQ0wCwYDVQQDDARSb290 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2puldQ+iRcbxyDj85uSD zcb4VG0A2bc9ZKL6dCXwdGdLTc+4+zokwZFn3VaIiJ55iJ+1WRa63eSOmqP2H0VI LpjvxLOCZxAedqunNXDUCB7JSprw9BdKbKssbVAWpNhzWiSTmgTOZHCz+rj6YaMJ kiAnrqb7H5tIVCE6/64IfB7zCUzl3R58Cmn0vYS41Hu7tl79rbf6eM+a10pHA0Px CXsdzjjaZlu+ihZlg9TkQ+x4BXH+nCZzZVoaNzk7puNr5s8a+Mn+MWafOLR1HWfw

AFL1B9mjcM9dkhc6FQ1fnX0OvDdF52z6L5gFuMyV7Eb0nZJol5OwndKmcfmiwN77

6QIDAQABo1MwUTAdBgNVHQ4EFgQUQdiYAb2TwSE7MmtMTt0yC5lsXL4wHwYDVR0j BBgwFoAUQdiYAb2TwSE7MmtMTt0yC5lsXL4wDwYDVR0TAQH/BAUwAwEB/zANBgkq hkiG9w0BAQsFAAOCAQEALnwiWZ+qnZy0QrnZqU67OaOSQbzJxKyM6kiQeJcneScW /rLUdRphe0WCmyPMXUrSywu4zXtWgZB3JQsKYx/vRVxw4KrnBnb7MegiL0DH6AWN kCSf/RgPEN265nXuVwaUFmDFpIUxxHwKyR2x6j14Nwsi+uD1DDLxna2FjSwYFnps ogB+zIMVSGZP+je9owVOCmxsJk59P3THjEYb8WSHLJXPF2Ob+Wu/keRUaD7qIuJe

W94ZKJkBldVl9mue4TiCPcYo+IVwPILN2rYfxQhMICjZWCZqMYIrPn2fNGVtY2Br

Mk09T2gEg78W9KciIakjTzAVVanmjeQsjL7+vBa4Sw==

-----END CERTIFICATE-----

PUBLIC – look at the subject and issuer Organization – this show InCertA1 and Root

Certificate 2

-----BEGIN CERTIFICATE-----

MIIDWDCCAkCgAwIBAgIBCjANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQGEwJBVTEM

MAoGA1UECAwDVmljMRIwEAYDVQQHDAlNZWxib3VybmUxDTALBgNVBAoMBFJvb3Qx DTALBgNVBAMMBFJvb3QwHhcNMjQwNTIwMDU1MzI2WhcNMjUwNTIwMDU1MzI2WjBS

MQswCQYDVQQGEwJBVTEMMAoGA1UECAwDVmljMQ0wCwYDVQQHDARNZWxiMRIwEAYD VQQKDAlJbnRDZXJ0QTExEjAQBgNVBAMMCUludENlcnRBMTCCASIwDQYJKoZIhvcN AQEBBQADggEPADCCAQoCggEBAKoDwifaFTWzNRSSYsHYijgq0FygQzg1Jx4RuTGJ OP3e3YB0bKpz+1buYQCgUCkdDdkwoebAHW/ZT2y5bh27dNy2nUutwqCYxeWBgc8S 8hCxk40u/yAkuDJFlUxDRiC/Tr2FSRAUaruddOGvJsrSYiR8w9yvXCLZlywZKNTb IkfiNCY0QyEjs4NDX+Yw3wvV8ThpBhF7aaSXgBtXA8+h4p9Ny9FxpD9G4xOYVQlz 1DVy/3zSy2/SYjLO6ocNInxMSOZiyd+XE8bu9FEwPRe68+hm0ygCxsxxkXLqPtQu J4SHLErxLr+BBLwKAyrd+USJU4kpLCQdvL9IDiZfdnk92nkCAwEAAaM+MDwwHwYD VR0jBBgwFoAUQdiYAb2TwSE7MmtMTt0yC5lsXL4wDAYDVR0TBAUwAwEB/zALBgNV HQ8EBAMCBPAwDQYJKoZIhvcNAQELBQADggEBADzznncehVYqBF4i0vnbGZSP+yt0 jb0A272smOew4RrhH0a6SLOI0B5yNDCUW0TI0tVLXzCqD5/uW6uM4y18LNjAHOR7 2Z9d3eBIukMe3vg5kR2zJ4jRFtyc1hlU5R6c1OlfYnckfbGp7OKrBzK3pAiMF1/L NnIer+PsjX7l03Qzdd0fnH9D1blIYH7Lc8PSNz15LHTPIDHyeUND99beOhSk5mYA AvOou2rN3SLHMa7Z2F681IDYJ0UK1S/DcO41a5Xr/WBSOyuU1F7bg8eiSfNEoRn9 3AclsqKCqbgak3V5mwl9u8LBHqHrJ4bBemOX3dLa01uSeIR0ZV/lCqYo5mE=

-----END CERTIFICATE-----

PRIVATE – look at the subject and issuer Organization – this show SUT (Root) and IntCertA1

Certificate 3

-----BEGIN CERTIFICATE-----

MIID2TCCAsGgAwIBAgIBFDANBgkqhkiG9w0BAQsFADBSMQswCQYDVQQGEwJBVTEM

MAoGA1UECAwDVmljMQ0wCwYDVQQHDARNZWxiMRIwEAYDVQQKDAlJbnRDZXJ0QTEx

EjAQBgNVBAMMCUludENlcnRBMTAeFw0yNDA4MTQwMTExNTBaFw0yNTA4MTQwMTEx

NTBaMIGNMQswCQYDVQQGEwJBVTERMA8GA1UECAwIVmljdG9yaWExEjAQBgNVBAcM

CU1lbGJvdXJuZTEMMAoGA1UECgwDU1VUMREwDwYDVQQLDAhUTkUyMDAzNDESMBAG

A1UEAwwJSW50Q2VydEEyMSIwIAYJKoZIhvcNAQkBFhNwYnJhbmNoQHN3aW4uZWR1

LmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxi3akIhXaMTil2qh

WvRWy4Dfj6ueoACo7+GZH2e6zCDcl0LikCXlLTv33POjABesL+ONJEANjBzLcVLg JLU8jliPJCnUe82YCMZvwXce7iBiTQx4oh6Amn+moXMU1SOOMEeHOJVaqlFhMJOo yxwTjUtM8dfqUavqxREkxpVTBQpfT5YyniXfRtFm3zDXTslKH+YQzRQxvDMlt3N7 9E5d5vbnbum/nEE4gHTt8slzv0LN/ba87S5+TG0wqXOUJrWDweiqqOgN5mfr7Kgg

DajDsaXXNd9M18VG807PePUCNu3Qqbb2NZC9Gi9/N1lYoKGkJUVXtOafQOKKSfBH

/JoBAQIDAQABo34wfDBfBgNVHSMEWDBWoVGkTzBNMQswCQYDVQQGEwJBVTEMMAoG

A1UECAwDVmljMRIwEAYDVQQHDAlNZWxib3VybmUxDTALBgNVBAoMBFJvb3QxDTAL BgNVBAMMBFJvb3SCAQowDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCBPAwDQYJKoZI hvcNAQELBQADggEBAC1cLJBYIMUodFWJNW/1GbijTMyaXL0wiuBUVA67hx8HlJ/h

J7b3itCxyjJItcr+1+/6HzlBjFH/mYUgfTXVSxPzmGK6AorZD1bj52NipdbnZIQd

3EicFMeJrGF09FLRrzznooivabefLl356ggnN6YDsjAQLUv44fG9TvZ/iPPIhIZG

RW2myoRtr7J9nwTXbRoVfrxfx47dCGfrTPrDReuBM6CU3VuynJRkF5lz/FP07deI /hqmE81wMhSZfJ3FJNqUKUDHwQaTfgTvmy9SJhWCj2Pn8S2iqBCGqv7ML0eRR3Fw

txI6el6JakbfZ+RPfaRwe5OzJsg1EMWUxGA/ICk=

-----END CERTIFICATE-----

PRIVATE – look at the subject and issuer Organization – this show Swinburne (Root) and IntCertA1

Certificate 4

-----BEGIN CERTIFICATE-----

MIIDTDCCAjQCARQwDQYJKoZIhvcNAQELBQAwQzELMAkGA1UEBhMCQVUxDDAKBgNV

BAgMA1ZpYzESMBAGA1UECgwJSW50Q2VydEEyMRIwEAYDVQQDDAlJbnRDZXJ0QTIw

HhcNMjQwODE0MDA0NzQ0WhcNMjUwODE0MDA0NzQ0WjCBlDELMAkGA1UEBhMCQVUx

ETAPBgNVBAgMCFZpY3RvcmlhMRIwEAYDVQQHDAlNZWxib3VybmUxEjAQBgNVBAoM CVN3aW5idXJuZTERMA8GA1UECwwIVE5FMzAwMjQxEzARBgNVBAMMCkZpbmFsQ2Vy dEExIjAgBgkqhkiG9w0BCQEWE3BicmFuY2hAc3dpbi5lZHUuYXUwggEiMA0GCSqG SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9R8XiYsHlVfwZomBVVQwsleUYtUTn34ij 7IFpIeZmqea6mSztv8lPQCDCsEUIFhtGZ03c80df2dysM2Z1ZgSYPJUI8qIUwgZf xg25ls8tasdJOusMQ8inWAc6aKKlIYafeqtlTJYsjDzvuGLZd0Ha1A0UJXoK+D9C N2kGKNSKkzomoFAWmdus2/CPcNi7vW3A9Wmq1hEn+oOYyDRb0OzFwrDdJYZjZoJ2 KJMU3anf/h2TK2CVPE+4Hi3YA8ZQPxgbaGiznXJX5vxehUNHys19rSbG/PDDbAJx w3SnNo/joVCtsVPHpQrI07J3W1U3GfkDwdd8WVCryU5vqnHBKXjHAgMBAAEwDQYJ KoZIhvcNAQELBQADggEBAI+rosEZlLgOtewW/poYNfZPz/83XBCupLmSccwebz9P Kw2va+seyxZkBVj1V0klIHC5kGxP8GPSLtd7Wzjuz6BI4S/AXVuuBSBnBSEE4Py8 onCNCKhtCqZFrBuZ4tuqGRBhz8j8bggqIQP1fASClG5nLFVlV6GRxqLouRfAG2aB bW9ysY9MfWvmdu55dyDsu9YmMUOhs7CaAqlt3FrrZXD5HdWC6Irx+odTIR5EG3bA

1oHyS7Fjuw3a+P4LttIbfx+E4rF1cyu+O7Z1zDdfLFil7eU0d66B+4YyykWNIGTQ

BtO+JLktL6HrQvKxp+ZzRe9QqV/oOVwUOCjL6bbitaI=

-----END CERTIFICATE-----

2