Kieren Ng

Homework 12

1. I think you have to check that the hash of the key is correct to authenticate the DNSKEY? Idk tho

2.

3. secure64.com. 5 IN DNSKEY 256 3 7 AwEAAabkKjyru8gmCZCjpFAQb/BNGFCSDCYb3crOZ1bKBTIQlVGZLW9t wH2LDZlUeujGPl8t5urWkGP1ofXmS1wtuGYbWsLlnv+quhSQ+QxTHmB3 WsLhx5x/++xHNkBHgSQJyUojflyLW0ONWDK+U53EM69Sna8o9EmthraF FCq3K1uV

secure64.com. 5 IN DNSKEY 256 3 7 AwEAAYCOmaToFmxz1vzKfqulHME53/onV7iMGXPVNkU/uxd4QPNT/Xe9 WLw25pp7M/67cr35CMRA9xiwG5OTV/86WFkOI3DGPAwjrBcIHMmy35UQ pDgw2ug6Ad1E8SX1qk0onAsAbpj7SoP6x4aJAzYJgzpGHLllAlvrBfky PGp2L+mp

secure64.com. 5 IN DNSKEY 257 3 7 AwEAAX2htcD8DvTuljGUCNvutZYG1eHHsQM22NB0D3UHYURy12EUriVl Hcj3beVyOo8vfIFNmqHxOrpPLdQSTYstfEy+tnCWBuvjzp/GXs4cyFXd s6VyCORv/GRi9/qWZxLEH+MFd61WVsoxDqcMPSCzG2O8CAmzJIX6bbky 5LTRTVj/

4.

5.

23.9

A public key infrastructure “is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption” (Wikipedia). It basically provides what is needed for entities to communicate safely.

23.4

Website: Canvas

Certificate issued by DigiCert SHA2 Secure Server CA, public key: 30 82 01 0a 02 82 01 01 00 aa 0c a2 92 82 e4 66 fc 5e 5a 5d d9 73 41 3e f3 b4 64 ef 83 b1 12 16 8a 45 77 a8 bb 1f f0 70 3d 6e ed 80 57 4d 2e ec d2 f9 f4 47 bc 32 b9 b9 1b a8 b4 23 9e 24 bd a6 81 b6 c3 aa a2 56 6b a4 1a b8 cb 9f 93 d2 b7 d4 d8 fd 2e 3f 25 84 96 4f 7f 50 e4 87 94 f0 57 45 1d 0f 67 35 5a 44 88 c4 78 bf 7f dd 68 0a 95 b5 1b 00 06 d4 82 3d 59 ce 4b ef 98 72 e2 ae 18 ef dd e5 60 47 55 24 d0 b6 96 5d 64 65 d0 f5 4e 07 b2 a3 ee 2c bc b1 8c 3e 6f ed 28 36 30 1c 0e 3f ef e0 57 99 21 ea 77 fc 09 a4 85 96 bb 9e bb 32 b8 09 b5 50 71 6a 38 c9 ee 68 d0 79 f8 a9 f0 ab 5d f9 0b 63 f5 37 d3 19 77 8f c3 72 70 3a c9 4d 21 c1 c7 19 b3 4a 9d 47 9d 0b e7 35 be d8 6e f9 ac ef 6a 27 8e 37 87 7d b2 a0 d6 5c b4 d7 93 ab d3 88 9d 59 1a 33 97 4b 39 eb 3c ad 62 62 ee 8a a6 ad b4 32 75 a4 83 d1 45 02 03 01 00 01

Valid from 4/12/2018 to 4/17/2020

Issued to canvas.colorado.edu

Signature is sha256RSA

b.

It’s a certificate, bc it is signed by a CA

c.

The certificate is valid because the certification path from Digicert-digicert sha2 secure server ca- canvas.colorado.edu are all valid and within their valid dates

d. Not that I see, but I’m not an expert on this

23.5

Issued by GlobalSign Root CA

Public key: 30 82 01 0a 02 82 01 01 00 c3 f0 65 88 df 1b dd c6 82 87 2f c9 0b ba 54 c6 63 3f 46 75 ac 4b 14 1f 98 72 8b 1c 10 ff 09 a9 52 6e 2f 65 df 65 84 3f 5f 81 b2 d8 f1 4f d7 f0 5a bb c9 af d0 31 dd 26 46 2a 99 9e d8 a9 a3 b6 b8 07 c4 c9 71 f7 95 84 ef d2 ea 1f 54 a0 e5 be e4 41 21 56 31 10 64 7d 1e 63 8e 9c 71 5c 3c a0 2e de 67 dc c8 9a 20 f0 75 c8 b0 b6 27 81 eb 97 0d ee 22 45 a5 c2 2f 34 27 ec e0 59 12 51 b3 1e 05 e5 38 20 d2 69 59 7a 59 17 be 1a 4b 39 08 12 79 33 9b 64 68 fe 58 81 dd 88 0c 6a ba 59 b4 af 24 4f 61 e0 ca fc 17 5a d2 3c 72 ab a7 4c b7 b9 ea 2d e3 f4 3f 99 a2 4d c8 1d 58 f8 7f 53 35 8e d7 22 88 b7 61 76 08 13 13 69 66 b0 57 59 13 31 0a 70 82 2b 93 d7 f6 e2 40 15 d0 1d 01 72 c7 13 58 6a 5a ec 19 89 16 3c e0 c8 8d 86 2a fa 37 f0 35 32 dd ec e5 fe 80 8e f7 05 67 b4 8b 42 75 35 02 03 01 00 01

Valid from 4/13/2011 to 4/13/2022

Issued to AlphaSSL CA-G2

Signature is sha1RSA

b.

It is a CA, because the trust store is a list of CAs

c.

Certificate is valid, I am within the valid dates

d. Not that I see