Sean Blanchard

5/6/2021

L10 Networking

qanda

1. What is the OPENSSLDIR?

It is a variable, stores the path to where the ssl certificates are on the system.

1. What files are contained in this path?

Openssl valid certificates

1. Where are most of the files actually located? (use ls -l)

/usr/lib/ssl

qanda

1. Submit your CSR to canvas in the human readable format **AND** in the csr format. Make sure the field for **Common Name** is YOUR name.

Top of Form

Bottom of Form

Top of Form

Bottom of Form

|  |  |
| --- | --- |
|  | Certificate Request: |
|  | Data: |
|  | Version: 1 (0x0) |
|  | Subject: C = US, ST = California, L = Ventura, O = comp429, CN = seanblanch |
|  | Subject Public Key Info: |
|  | Public Key Algorithm: rsaEncryption |
|  | RSA Public-Key: (2048 bit) |
|  | Modulus: |
|  | 00:d9:4a:04:99:2f:67:8c:cf:c6:19:2d:33:b0:72: |
|  | 2c:c2:f5:e9:1f:0a:71:14:31:a1:ba:b5:9c:f8:ac: |
|  | 0a:68:f9:44:a3:50:c0:00:c8:9d:44:c0:7c:83:af: |
|  | 5a:89:6b:ea:f9:c2:e4:ef:7a:31:23:e1:d7:a6:f9: |
|  | 9e:ea:e8:8a:84:5a:8c:b1:4b:e4:96:05:5b:77:1a: |
|  | 3f:f0:b3:21:51:39:06:20:cd:51:08:19:11:ec:6c: |
|  | 96:71:7a:86:1b:d7:e8:ff:9f:d9:56:c0:af:42:f5: |
|  | aa:d2:4a:9c:f0:8d:e9:7b:a6:e2:e7:c9:bc:56:7b: |
|  | 7d:78:84:d4:23:48:53:30:98:5f:59:47:67:d0:ff: |
|  | 8b:57:21:b2:10:d3:9a:ce:b8:20:8f:1b:00:89:36: |
|  | 08:0a:34:d8:b9:03:c7:b7:fe:45:e6:52:fa:c6:48: |
|  | 91:7f:e4:24:6e:94:13:4d:cf:d9:25:c1:88:77:e6: |
|  | 6e:7d:76:23:3f:69:89:41:dd:0f:8d:9d:f8:81:07: |
|  | 76:d9:ab:f4:77:72:89:27:62:3d:51:b4:a2:22:bf: |
|  | 2c:a4:a2:5d:ae:d8:c5:7f:06:d2:7e:ee:01:83:67: |
|  | 91:83:20:51:53:18:d2:f4:ae:13:0e:b2:4f:09:40: |
|  | 54:46:e6:05:ee:ac:8d:c2:35:36:69:87:2b:09:56: |
|  | d1:d5 |
|  | Exponent: 65537 (0x10001) |
|  | Attributes: |
|  | a0:00 |
|  | Signature Algorithm: sha256WithRSAEncryption |
|  | 1f:6f:8c:c0:9d:bc:df:d0:8c:c7:da:10:0a:37:9c:67:32:b8: |
|  | 5b:0a:60:8b:09:bd:1c:c3:df:b2:6e:2e:b6:01:4d:5b:10:1d: |
|  | c0:68:33:c2:7f:65:7c:85:4a:97:ee:24:92:ab:aa:d3:09:3b: |
|  | 2b:89:07:5d:8f:15:7d:d1:5d:ed:fb:3b:b8:a5:82:0a:0b:9a: |
|  | fe:19:7d:99:78:35:6a:b9:ee:07:52:53:50:49:a3:9c:de:f7: |
|  | 9b:97:9d:f0:15:0d:a1:91:a2:77:27:29:16:f0:c3:1b:c1:cb: |
|  | 44:df:ba:b3:b8:86:cb:bb:43:07:89:17:cf:c3:a0:4a:fc:c7: |
|  | 54:e4:75:10:07:6f:41:db:57:1a:f7:09:c7:a4:b3:a4:f1:6f: |
|  | 05:ec:84:e9:5f:c0:e9:45:8c:c3:76:64:31:7e:7a:0b:0a:ab: |
|  | 3d:bd:2a:de:0e:7b:4a:a0:05:cd:72:6b:33:16:98:5b:3e:51: |
|  | 9a:49:32:b0:26:db:cc:c2:06:ca:72:82:9e:7d:5d:e4:b0:62: |
|  | c4:30:78:f7:87:56:7a:5a:0d:58:23:f6:28:40:fa:76:c9:f7: |
|  | e1:cc:6b:32:4e:c5:b9:01:9c:e8:ce:b1:85:d3:81:a5:98:6c: |
|  | ef:54:d0:b3:c5:03:20:af:40:6b:ee:09:e2:93:a9:61:7f:d6: |
|  | c6:4c:de:15 |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

|  |  |
| --- | --- |
|  | -----BEGIN CERTIFICATE REQUEST----- |
|  | MIICoDCCAYgCAQAwWzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx |
|  | EDAOBgNVBAcMB1ZlbnR1cmExEDAOBgNVBAoMB2NvbXA0MjkxEzARBgNVBAMMCnNl |
|  | YW5ibGFuY2gwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZSgSZL2eM |
|  | z8YZLTOwcizC9ekfCnEUMaG6tZz4rApo+USjUMAAyJ1EwHyDr1qJa+r5wuTvejEj |
|  | 4dem+Z7q6IqEWoyxS+SWBVt3Gj/wsyFROQYgzVEIGRHsbJZxeoYb1+j/n9lWwK9C |
|  | 9arSSpzwjel7puLnybxWe314hNQjSFMwmF9ZR2fQ/4tXIbIQ05rOuCCPGwCJNggK |
|  | NNi5A8e3/kXmUvrGSJF/5CRulBNNz9klwYh35m59diM/aYlB3Q+NnfiBB3bZq/R3 |
|  | coknYj1RtKIivyykol2u2MV/BtJ+7gGDZ5GDIFFTGNL0rhMOsk8JQFRG5gXurI3C |
|  | NTZphysJVtHVAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAH2+MwJ2839CMx9oQ |
|  | CjecZzK4Wwpgiwm9HMPfsm4utgFNWxAdwGgzwn9lfIVKl+4kkquq0wk7K4kHXY8V |
|  | fdFd7fs7uKWCCgua/hl9mXg1arnuB1JTUEmjnN73m5ed8BUNoZGidycpFvDDG8HL |
|  | RN+6s7iGy7tDB4kXz8OgSvzHVOR1EAdvQdtXGvcJx6SzpPFvBeyE6V/A6UWMw3Zk |
|  | MX56CwqrPb0q3g57SqAFzXJrMxaYWz5RmkkysCbbzMIGynKCnn1d5LBixDB494dW |
|  | eloNWCP2KED6dsn34cxrMk7FuQGc6M6xhdOBpZhs71TQs8UDIK9Aa+4J4pOpYX/W |
|  | xkzeFQ== |
|  | -----END CERTIFICATE REQUEST----- |

1. Encrypt a text file that has your name in it with the public key above.
   * Use openssl rsautl --help to see the rsautl command options
   * The options you will need to provide are an infile, outfile, keyfile, public key flag, and encrypt flag.
   * Submit your encrypted file.
2. Submit the encryption command you used as well.
3. Verify that this file was signed by me: [http://429.scrivnor.cikeys.com/signed (Links to an external site.)](http://429.scrivnor.cikeys.com/signed)
   * I "signed" this file with my private key. Since only I can do that, you should be able to view the file in plaintext using my public key.
   * Submit the command used and contents of the file.
4. Why can we not truly verify that the file was signed by me?