

Public Key Infrastructure Lab Report

Hayden Eubanks

School of Business, Liberty University

CSIS 463-B01

Dr. De Queiroz

October 7, 2023

Public Key Infrastructure Lab Report

Introduction:

One of the most important technologies employed in network communications today is the public key infrastructure (PKI) as the PKI forms the foundations for secure communication and allows for the verification of communicating parties through trusted intermediaries (Höglund et al., 2020). Being able to verify communications is a core requirement in many business domains and the use of the PKI has enabled online operations in sectors such as banking, e-commerce, government communications, and the Internet of Things (IoT) that would otherwise not be secure (NCSC, n.d.). Further, PKI technologies allow verification even when parties have never physically met additionally highlighting their value in the sphere of networking (Basta, 2018). However, proper security practices must be implemented within PKI applications to ensure that security is upheld, and that verification is accurately performed (SSH, 2023b). The lack of security best practices within a PKI could leave a system vulnerable to man-in-the-middle attacks and in doing so allow malicious actors to intercept communications or impersonate the identity of a legitimate source. The ability for a malicious actor to masquerade as a legitimate source highlights an extreme point of concern within PKI security and with this, the critical importance for a security professional to understand PKI systems and implement resilient solutions can be seen. By studying the components of the public key infrastructure and how they can be exploited, a security professional can be best empowered to implement security solutions that protect network communications and the identities of communicating parties.

The PKI is a collection of cryptographic technologies implemented together to provide secure network communications through which the verification of communicating entities can be performed (ENISA, 2023). As the name implies, the PKI is built upon applications of public-key

cryptography and as such, the components of a PKI can be summarized as keys, certificates, certificate authorities, and standards (SSH, 2023a). This process can be seen to first utilize a public-key encryption algorithm such as RSA to generate a public and private key for a user (Basta, 2018). Once these keys are created, a certificate authority (CA) can then validate the identity of that user, giving that user a certificate as a statement that they have been verified by the CA (ENISA, 2023). This certificate is crafted using the keys generated for that user allowing the identity document to be cryptographically sealed providing non-repudiation for the user based on the CA's verification (Basta, 2018). The certificate created through this process can then be requested by additional parties to verify the user and ensure that communications are from the intended source. The level of trust given to cryptographic applications such as nonrepudiation through a PKI then highlights the importance of ensuring these processes cannot be broken. Further, secure practices in PKI formation can allow for increased security and resilience within the sphere of networking, and with this, the operation of many organizations on the internet making the securing of the PKI an essential aspect of organizational security (Geeks for Geeks, 2022).

However, vulnerabilities exist within poor PKI implementations, and as such a security professional must be aware of attack vectors such as man-in-the-middle attacks threatening the effectiveness of these solutions as well as how they can be combatted through the application of best practices. The user identification provided through the PKI is a valuable target for malicious actors in faking their identity, and as such criminals have tried to exploit the PKI to gain an advantage in their illicit activities (SSH, 2023b). Often, malicious actors attempt to accomplish this through man-in-the-middle attacks, where they attempt to intercept the initial communication between an entity and the server in which a secret key is transferred (Basta,

2018). In this way, the attacker places themselves in the middle of the communication, and in doing so is able to gain access to this initial private-key transfer and afterward will be able to decrypt communications between the server and that entity (SSH, 2023b). In addition to this, malicious actors can attempt to exploit PKI weakness to impersonate trusted sites or entities, highlighting another area of security concern. If a CA is compromised, a malicious actor may be able to generate their own certificates allowing themselves to masquerade as trusted sources unbeknownst to their victims (SSH, 2023b). Further, malicious actors could attempt to re-route users from legitimate sites to malicious sites that appear similar in nature to steal their data. Fortunately, each of these vulnerabilities could be mitigated through strong PKI applications, and as such it is essential for a security professional to understand how these attacks are performed and defended against highlighting the objective of this exploratory lab.

Throughout this lab, an exploration of the public-key infrastructure as well as the threats facing it were performed giving the user a better understanding of best practices within PKI applications. This was accomplished by first exploring CAs and the methods by which certificates are generated for the CA itself as well as entities requesting certificates. This includes an examination of the importance of the root CA certificate and the security implications associated with the loss of that document's confidentiality (ENISA, 2023). The compromising of the CA root certificate could allow for the arbitrary creation of certificates and as such a malicious actor with access to the root certificate could create certificates for themselves to masquerade as other legitimate entities (SSH, 2023b). After this, an examination was performed for certificates within the context of a web browser and the protocols used to access the web page. This step highlights the importance of using secure networking protocols such as HTTPS over HTTP as well as the extra security provided by a browser regarding untrusted certificate

authorities (Basta, 2018). Finally, the lab simulated man-in-the-middle attacks that a malicious actor may attempt to give an understanding of the attack surface facing the PKI. This included the simulation of attack scenarios such as the redirecting of a user to a malicious website by modifying their routing tables or attacking the DNS process (SSH, 2023b). Further, this included the examination of the extreme vulnerability posing the PKI when a malicious actor has gained access to a CA's private key as they are then able to impersonate any website. Great care should be taken by a security professional when implementing a PKI and the exploration of attack vectors through labs such as this can greatly assist a security professional in hardening their systems to be resilient to attack.

Lab Procedure:

The first task in this lab directed the user to create their own certificate authority which would be then used to issue certificates to other entities. This is the core functionality around which the PKI is constructed providing users with clear insight into the process of certificate generation. Before the CA could be fully configured, the user first had to modify the configuration file of OpenSSL ([Screenshot 1](#)) to allow for the creation of certificates with the same subject. Traditionally it may not be desirable for a CA to enable this configuration feature, but within this lab sites with the same subject are used for ease of demonstration pointing to the need for the configuration change within the lab context. After this, an empty index file was created ([Screenshot 2](#)) as well as a serial file containing the integer 1000 ([Screenshot 3](#)) which will further be used in the CA configuration. OpenSSL could then be used to create the root certificate for the CA using RSA to generate the self-signed certificate ([Screenshot 4](#)). This process will prompt the CA to create a password that is used in the encryption of this certificate which can be entered by the user and after this is complete, OpenSSL can further be used to view the contents of this certificate ([Screenshot 5](#) – [Screenshot 6](#)). Further, the file containing the keys used in encryption can be inspected ([Screenshot 7](#) – [Screenshot 11](#)) and upon viewing these files, the certificate can be verified as a self-signed CA certificate as the issuer and subject fields are identical. With this, the file containing the keys can be inspected to identify the values for the core variables used in RSA encryption. The public exponent e can be identified as private exponent, the private exponent d is labeled as public exponent, the modulus n is labeled as modulus, and the numbers p & q can be identified as prime 1 and prime 2 respectively.

Identifying these elements can then allow for an inspection of the RSA encryption process which allows certificate verification to be performed.

The next lab task then involved creating a certificate request to the web server so that the CA would generate a certificate for that source. In order to generate the certificate signing request (CSR) the X509 option must be removed from the OpenSSL command and doing so will direct the CA to generate a certificate for this source ([Screenshot 12](#)). This will generate a server certificate request ([Screenshot 13](#) – [Screenshot 14](#)) and key file ([Screenshot 15](#) – [Screenshot 17](#)), and examining both of these files will give all of the information needed to perform certificate verification with this source. Aliases can then be created to re-route alternative names to the same server location ([Screenshot 18](#)) and a new certificate request created that includes the alternative alias names in the request ([Screenshot 19](#)).

After this certificate request has been generated, the request can then be passed to the CA who will generate the certificate fulfilling that request. This can be accomplished through an OpenSSL command to turn the CSR into an X509 certificate utilizing the root CA's keys to generate this certificate ([Screenshot 20](#)). For the purposes of this lab, the configuration file for OpenSSL was then modified to allow commands to be performed that within the context of an operating server could pose security concerns but are modified to simplify processes for the purpose of learning in this lab ([Screenshot 21](#)). With these configurations changed, the decoded content of the certificate could then be viewed revealing the certificate details including the alternative names for the server ([Screenshot 22](#) – [Screenshot 23](#)). With this accomplished, the certificate for the server has been successfully generated and is able for use in the verification of the server.

The fourth lab task then takes a look at certificates within the context of web interactions and how public key encryption is utilized to increase network security. To accomplish this, the web server first needed to be launched and the password entered to successfully access the server ([Screenshot 24](#)). With the server up, the configuration file for the bank 32 website could be modified to use port 443 by default and include elements such as the root directory and the aliases for the server ([Screenshot 26](#)). Additionally, a similar file could be created for the “website” that will be used as the user-created website for which a certificate will also be generated ([Screenshot 25](#)). With the pre-certified bank 32 website, it can be seen that access to the server is granted as the certificate for that site can be verified ([Screenshot 27](#)). However, before a certificate is generated for the user's website, attempting to connect will result in a verification error ([Screenshot 28](#)). In order to correct this, the CA used in verifying this file must be added to the Firefox browser so that certificates from the user-generated CA can be accepted for verification ([Screenshot 29](#) – [Screenshot 31](#)). Adding the CA to the browser for verification then allows the site to be accessed as verification can be performed ([Screenshot 32](#)).

With an understanding of CA's and certificates within the context of the web performed, an exploration of threats facing this process such as man-in-the-middle attacks can be examined. One of the most common attack vectors for malicious actors in this process involves the re-routing of HTTPS requests so that the user is unknowingly redirected to a malicious source. This can be done by modifying the user's list of IP host resolutions so that a request for one source will redirect to the malicious source ([Screenshot 33](#) – [Screenshot 34](#)). However, as the certificate for the malicious site will not match the requested domain, the browser will fail to verify the source and as such will not allow access to the site using the HTTPS protocol ([Screenshot 35](#)). This highlights the advantage of the HTTPS protocol in providing security from man-in-the-

middle attacks as the PKI can be used to verify that the source is illegitimate and can therefore alert users to the suspicious activity (SSH, 2023b).

For the final lab task, the user was then asked to operate under the assumption that the root CA had been compromised giving the malicious actor the ability to generate arbitrary certificates (SSH, 2023b). If the private key for a CA is compromised, the malicious actor is then able to use the encryption process to generate a verifiable certificate for any source. This means that an attacker could then generate a certificate to verify their illegitimate site giving validity that could be used to deceive users. To demonstrate this, the example from the previous task was used, but this time a certificate was generated for the malicious site the user was redirected to ([Screenshot 36](#)). Similar to the previous example, the user's routing was re-directed to the malicious site ([Screenshot 37](#)), and from this it could then be seen that attempting to access the original site would reroute to the malicious site. However, as the certificate had been generated by the CA, access to the malicious site was then given ([Screenshot 38](#)) highlighting the extreme security concern associated with the compromising of a CA's private key. With this in mind, security professionals must protect the private keys of CAs, potentially going as far as keeping CAs offline to better protect their resources (Basta, 2018). The PKI is a powerful tool in modern encryption, but with this powerful tool comes the responsibility associated with secure implementation. Through practicing strong security best practices in the implementation of a PKI, a security professional can ensure strong web security and best protect system resources and users.

References

- Basta, A. (2018). *Oriyano, cryptography: Infosec pro guide*. McGraw-Hill Education.
<https://bookshelf.vitalsource.com/reader/books/9781307297003/pageid/14>
- ENISA. (2023). *Public key infrastructure (PKI)*. European Union Agency for Cybersecurity.
<https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki>
- Geeks for Geeks. (June 9, 2022). *Public key infrastructure*. Geeks for Geeks.
<https://www.geeksforgeeks.org/public-key-infrastructure/>
- Höglund, J., Lindemer, S., Furuheid, M., & Raza, S. (2020). PKI4IoT: Towards public key infrastructure for the internet of things. *Computers & Security*, 89, 101658. <https://doi.org/10.1016/j.cose.2019.101658>
- NCSC. (n.d.). *Design and build a privately hosted public key infrastructure*. National Cyber Security Centre. <https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/introduction-to-public-key-infrastructure>
- SSH. (2023a). *What is PKI (public key infrastructure)*. SSH. <https://www.ssh.com/academy/pki>
- SSH. (2023b). *Man-in-the-middle attack in SSH- How does it work?*. SSH.
<https://www.ssh.com/academy/attack/man-in-the-middle>

Screenshots: Task 1

Screenshot1: ([Return to text](#))

```

GNU nano 6.2 openssl.cnf
# openssl may not work correctly which could lead to significant system
# problems including inability to remotely access the system.
[default_section]
# activate = 1

#####
[ ca ]
default_ca = CA_default          # The default ca section
#####
[ CA_default ]

dir               = ./demoCA      # Where everything is kept
certs             = $dir/certs    # Where the issued certs are kept
crl_dir           = $dir/crl      # Where the issued crl are kept
database          = $dir/index.txt # database index file.
unique_subject    = no            # Set to 'no' to allow creation of
                                   # several certs with same subject.
new_certs_dir     = $dir/newcerts # default place for new certs.

certificate       = $dir/cacert.pem # The CA certificate
serial            = $dir/serial     # The current serial number
crlnumber         = $dir/crlnumber  # The current crl number
                                   # must be commented out to leave a V1 CRL
crl               = $dir/crl.pem    # The current CRL
private_key       = $dir/private/cakey.pem # The private key

x509_extensions  = usr_cert        # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt          = ca_default     # Subject Name options
cert_opt          = ca_default     # Certificate field options

# Extension copying option: use with caution.
# copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions  = crl_ext

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^G Location  ^U Undo     ^M Set Mark  ^I To Bracket
^X Exit      ^R Read File ^L Replace   ^P Paste     ^_ Justify  ^J Go To Line ^B Redo     ^C Copy      ^Q Where Was
  
```

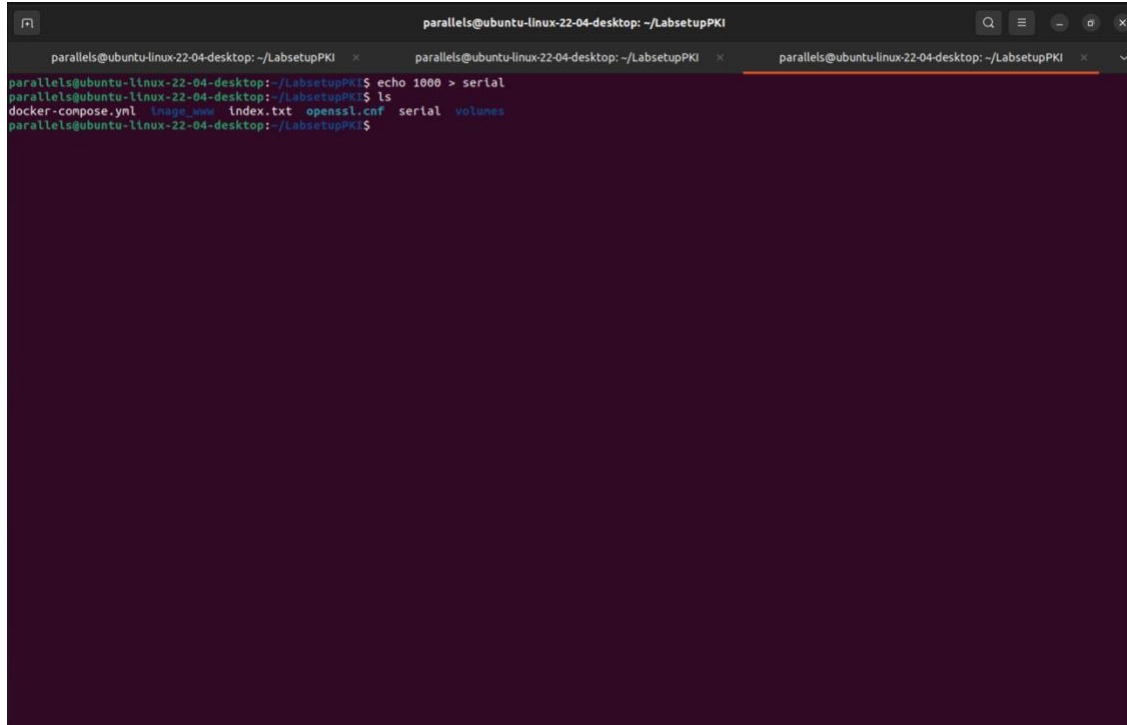
Screenshot2: ([Return to text](#))

```

GNU nano 6.2 index.txt

```

Screenshot3: ([Return to text](#))

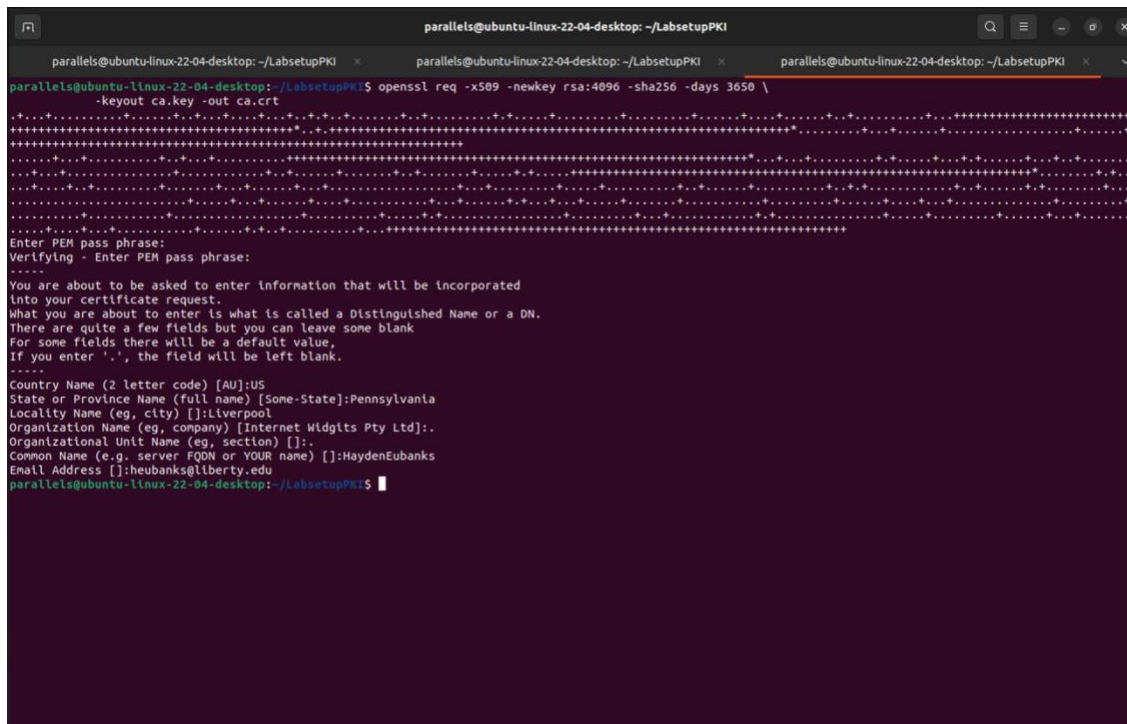


```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ echo 1000 > serial
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ ls
docker-compose.yml  image_www  index.txt  openssl.cnf  serial  volumes
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```

Screenshot4: ([Return to text](#))



```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
-keyout ca.key -out ca.crt
.....
Enter PEM pass phrase:
Verify PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Pennsylvania
Locality Name (eg, city) []:Liverpool
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:HaydenEubanks
Email Address []:heubanks@liberty.edu
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```

Screenshot5: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    10:ef:aa:d2:72:ee:49:b5:c8:70:a6:fe:2f:59:1c:5e:c9:6a:1f:20
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = US, ST = Pennsylvania, L = Liverpool, CN = HaydenEubanks, emailAddress = heubanks@liberty.edu
  Validity
    Not Before: Oct  5 12:40:39 2023 GMT
    Not After : Oct  2 12:40:39 2033 GMT
  Subject: C = US, ST = Pennsylvania, L = Liverpool, CN = HaydenEubanks, emailAddress = heubanks@liberty.edu
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (4096 bit)
    Modulus:
      00:b7:ef:11:a4:89:ba:df:75:76:b9:a2:f2:7a:79:
      57:83:45:2e:5e:8e:10:e3:92:6e:2c:dc:0e:bd:fd:
      27:f4:e7:12:70:89:b8:61:ef:16:ee:c3:ac:7f:20:
      01:36:89:6c:ee:c8:94:36:99:c7:64:e8:44:4f:38:
      a3:0f:a9:d7:c3:5d:cc:0a:42:24:9c:17:4c:ff:9e:
      52:11:b0:09:12:86:e0:87:a9:c9:00:64:02:36:2e:
      cf:8f:de:25:1c:cc:e5:a8:e0:4b:fe:5d:10:c2:71:
      86:41:a6:6c:6a:98:df:3d:cb:68:10:ee:a1:7b:39:
      29:97:1e:04:81:54:65:1b:31:e8:0e:bb:f5:db:21:
      68:c3:d3:0a:5e:39:86:72:c5:8c:bc:81:b2:44:7f:
      92:3e:d5:07:a7:83:90:e7:ee:0a:a3:a1:fc:7e:0d:
      60:0b:15:26:86:d6:ae:bd:14:84:42:c7:2e:fe:e1:
      d3:7d:7e:22:eb:08:13:f9:fb:00:5c:ac:5a:04:3e:
      ec:fd:a0:b7:03:b8:87:a9:77:9a:e5:1a:3d:6b:bd:
      d3:00:ba:04:49:e3:ae:e4:a2:77:ee:bb:0a:4b:ac:
      a1:8c:74:26:ab:9d:f5:02:00:fe:7a:fa:28:05:fb:
      f1:33:e5:79:e0:c2:42:7a:ce:dd:f0:fb:71:cf:7a:
      04:1a:ad:50:35:c6:7d:5d:d7:2d:e0:2f:0a:06:6d:
      60:44:94:28:05:b5:5b:df:58:6e:10:26:90:b6:7e:
      00:45:fa:88:2c:49:ab:5b:cf:7c:ad:5e:a3:08:bb:
      38:51:ea:38:e4:38:c4:5c:87:72:26:b5:0e:98:77:
      af:01:15:c8:d1:0c:99:3f:66:8c:94:21:79:9f:1f:
      af:b2:50:de:cc:55:a5:ed:75:76:31:4f:6a:78:cd:
      c5:10:3e:a4:68:40:0b:21:82:e9:3e:5f:30:1c:85:
      d1:5c:56:f8:ad:a2:24:18:03:61:a6:90:72:37:2f:
      fe:10:70:9e:36:63:f0:fa:93:aa:d0:1f:70:f0:86:
      5f:d9:0e:73:73:bf:00:5e:32:8f:18:00:c3:f3:6e:
      01:aa:e1:4f:22:a2:33:26:fb:dc:d6:bb:12:08:fd:
      ba:19:94:40:87:43:e2:4b:b9:cc:96:11:76:8a:b2:
      70:e0:f1:c0:3f:31:86:e5:bd:ce:1b:41:13:7f:09:

```

Screenshot6: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
70:e0:f1:c0:3f:31:86:e5:bd:ce:1b:41:13:7f:09:
ed:f0:1c:0a:fd:26:65:06:e5:dc:84:1d:57:34:73:
01:64:d3:1f:1d:20:c2:55:84:78:3d:e5:30:96:82:
a4:50:06:23:50:72:fa:85:99:43:89:7f:10:01:72:
af:bf:61:7d:55:6a:d0:5f:e0:44:f3:82:62:f7:9e:
86:11:59
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    04:7E:85:D3:53:30:22:3B:8C:B7:0B:8D:BF:FC:31:7F:4C:3A:78:26
  X509v3 Authority Key Identifier:
    04:7E:85:D3:53:30:22:3B:8C:B7:0B:8D:BF:FC:31:7F:4C:3A:78:26
  X509v3 Basic Constraints: critical
    CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
  4c:bf:33:20:68:19:49:5a:a4:17:bc:04:52:00:99:50:ab:9d:
  0f:3b:f5:51:76:93:fb:90:e8:02:82:90:81:53:fe:42:8b:b3:
  bf:ad:c0:62:22:89:bc:39:b9:35:89:63:73:92:49:8a:c4:b0:
  85:4f:97:4c:2d:0f:05:93:8d:a0:70:6d:5b:e4:21:aa:f5:ba:
  44:ca:fb:bc:b9:9d:7a:6d:94:75:b5:06:25:71:bd:15:05:b2:
  35:5a:a1:0e:3d:76:2f:8d:0b:8c:7b:91:89:a9:a3:61:14:b5:
  13:e7:a5:8f:6b:cd:11:7e:0f:54:40:29:1f:27:0f:98:37:d1:
  db:9b:3c:81:65:a3:55:9b:79:fe:4c:be:69:0d:b5:bb:90:b9:
  12:c5:e3:45:e4:74:e5:25:b5:f1:83:72:c5:07:4f:ca:03:52:
  8d:a7:dc:e2:cd:3f:62:e0:04:05:fd:e5:31:6c:06:ff:46:25:
  bf:27:af:5e:10:75:21:02:90:fe:26:f0:3d:67:85:97:21:f3:
  2a:8c:8f:e8:c9:8d:db:a7:40:ec:b4:39:7f:ad:f4:00:02:24:
  a4:97:49:b3:37:5e:12:23:f3:59:30:2c:f9:e8:22:7f:11:58:
  f3:7a:d5:34:1d:58:aa:02:29:0b:d0:76:fe:08:23:7a:c2:16:
  8e:54:b5:24:66:7a:3c:33:15:0e:93:81:a0:a6:cb:f0:76:75:
  1f:65:bf:9d:91:b4:39:92:74:28:c4:4b:2c:df:9f:2b:9a:69:
  95:8c:30:0d:d7:85:7a:a7:65:64:a2:44:0b:9b:1d:6b:24:32:
  28:c9:c1:a8:04:b8:9f:03:92:3c:d9:34:67:97:c0:12:09:
  79:85:9d:54:e7:18:2b:a9:cd:5e:3c:92:5f:c6:cb:60:e4:e4:
  58:41:ef:c5:26:0f:09:b7:0a:4c:50:1b:40:9e:25:3f:51:71:
  e4:ad:fb:33:93:7c:bd:93:a9:04:32:2a:63:47:35:42:28:64:
  a4:39:3e:1b:b5:c0:80:77:87:75:d6:e9:da:6b:cd:ab:ed:13:
  ef:bd:ec:6b:1b:0a:93:72:1f:d8:e5:b3:30:2f:1f:6f:58:2e:
  a2:25:5b:1b:0d:80:d8:f4:ec:0f:0e:75:01:fb:d2:3d:02:
  00:dc:1b:68:57:ad:33:7b:d2:26:f0:3b:d9:b6:a9:d4:2e:3e:
  50:1d:36:43:4a:3a:c0:c1:de:5c:e4:d6:3f:df:d0:e1:bb:4a:
  64:42:f2:95:ad:c9:91:c4:86:35:ce:cb:82:8b:09:64:e2:8e:
  5d:5b:17:0d:dd:74:04:38:c9:fc:ff:f7:45:b0:f4:f6:de:3f:
  19:d3:38:70:33:3c:3d:64
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```


Screenshot7: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop:~/LabsetupPKI$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
Private-Key: (4096 bit, 2 primes)
modulus:
00:b7:ef:11:a4:89:ba:df:75:76:b9:a2:f2:7a:79:
57:83:45:2e:e5:8e:10:e3:92:6e:2c:dc:0e:bd:fd:
27:f4:e7:12:70:89:b8:61:ef:16:ee:c3:ac:7f:20:
01:36:89:6c:ee:c8:94:36:99:c7:04:e8:44:4f:38:
a3:0f:a9:d7:c3:5d:cc:6a:42:24:9c:17:4c:ff:9e:
52:11:b0:89:12:86:e0:87:a9:c9:80:64:02:36:2e:
cf:8f:6e:25:1c:cc:e5:a8:e0:4b:f6:5d:10:c2:71:
86:41:a6:6c:6a:98:df:3d:cb:68:10:ee:a1:7b:39:
29:97:1e:04:81:54:65:1b:31:e8:0e:bb:fb:5d:21:
68:c3:d3:0a:5e:39:86:72:c5:8c:bc:81:b2:44:7f:
92:3e:d5:07:a7:83:90:e7:ee:0a:a3:a1:fc:7e:0d:
60:0b:15:26:86:d6:ae:bd:14:04:42:c7:2e:fe:e1:
d3:7d:7e:22:eb:08:13:f9:b7:00:5c:ac:5a:04:3e:
ec:fd:a0:b7:03:b8:87:a9:77:9a:e5:1a:3d:6b:bd:
d3:00:ba:94:49:e3:ae:e4:a2:77:ee:bb:0a:4b:ac:
a1:8c:74:26:ab:9d:f5:02:00:fe:78:fa:28:05:f8:
f1:33:e5:79:e0:c2:42:7a:ce:dd:f0:fb:71:cf:7a:
04:1a:ad:50:35:c6:7d:d5:d7:2d:e6:2f:0a:06:6d:
60:44:94:28:05:b5:5b:df:58:6e:10:26:90:b6:7e:
00:45:fa:88:2c:49:ab:5b:cf:7c:ad:5e:a3:08:bb:
38:51:ea:38:e4:38:c4:5c:87:72:26:b5:0e:98:77:
af:01:15:c8:d1:0c:99:3f:66:0c:94:21:79:9f:1f:
af:b2:56:de:cc:55:a5:ed:75:76:31:4f:6a:70:cd:
c5:10:3e:a4:68:40:9b:21:82:a9:3e:5f:30:1c:85:
d1:5c:56:f8:ad:a2:24:18:03:61:a6:90:72:37:2f:
fe:10:70:9e:36:63:f0:fa:93:aa:d0:1f:70:f0:86:
5f:d9:0e:73:73:bf:00:5e:32:8f:18:00:c3:f3:6e:
01:aa:e1:4f:22:a2:33:26:fb:dc:d6:bb:12:08:fd:
ba:19:94:40:87:43:e2:4b:b9:cc:96:11:76:8a:b2:
70:e6:f1:c0:3f:31:86:e5:bd:ce:1b:41:13:7f:09:
ed:f0:1c:0a:fd:26:65:06:e5:dc:84:1d:57:34:73:
01:64:d3:1f:21:20:c2:55:84:78:3d:e5:30:96:82:
a4:50:66:23:56:72:fa:85:99:43:09:7f:10:61:72:
af:b7:61:7d:55:6a:d0:5f:e8:44:f3:82:62:f7:9e:
86:11:59
publicExponent: 65537 (0x10001)
privateExponent:
07:4d:ef:90:cd:d5:ed:a2:1d:f0:07:16:33:52:2e:
8d:24:62:15:84:6f:ec:03:b0:8b:a8:45:0f:1b:36:
bb:21:72:90:64:cd:bd:58:ef:fb:9d:2a:74:65:76:
5a:de:b8:04:5f:13:99:bc:08:68:bb:d7:1b:a0:cb:
8b:77:92:1d:9c:73:dd:db:eb:d5:88:90:da:9d:64:
53:b6:c3:a0:c8:51:b2:1d:86:66:aa:82:12:7a:07:
2c:e2:62:47:ab:a4:ea:b1:16:9f:2e:e8:b7:9a:17:
cb:73:63:1e:94:19:d8:7b:c3:93:19:90:f0:e2:6f:
22:04:d3:87:b9:cc:e6:98:b3:a7:23:24:83:3a:67:
4d:50:8c:1a:bc:14:d8:09:bb:3a:30:b9:de:41:c5:
32:68:d6:1c:1b:4b:d5:c4:14:a8:d5:29:e0:6d:22:
4d:6a:5e:7c:70:19:e2:21:26:93:fa:d2:45:55:bd:
47:08:0b:7d:53:35:ac:e1:a0:8c:ed:9c:c9:0a:a1:
31:7c:d0:b3:cd:a8:18:8d:2b:09:f2:d1:f2:4d:88:
6b:c0:dd:1a:f6:97:67:55:c2:e6:c8:87:83:04:14:
e9:cd:a2:8c:01:f2:bd:0c:c2:4e:56:5b:e0:c9:d7:
35:59:05:77:2d:23:c3:fa:03:63:1a:af:35:3e:ba:
9b:2d:be:8e:bb:c3:de:dc:b5:56:bf:f2:90:57:4b:
9e:3a:e9:99:e2:1a:54:9b:60:5f:5b:23:c8:2d:99:
cf:1c:45:fa:10:34:37:1b:8d:e0:2b:d3:4b:8e:e5:
6f:50:19:a1:86:77:21:51:82:1c:56:85:87:52:4b:
54:23:2f:5f:dc:68:fd:cd:f1:c2:82:26:ec:0a:45:
31:22:e5:29:3b:dd:d1:f9:4c:66:91:41:c6:92:81:
a8:51:84:a3:fb:d0:53:1e:a5:2c:9f:7d:cd:5d:fa:
15:de:52:dd:41:ba:67:e1:dc:a9:c2:31:b7:1b:7c:
ae:23:a3:25:91:be:7c:14:4b:db:48:13:59:56:ee:
e2:fb:17:51:83:db:5b:64:82:bf:88:04:35:ca:f8:
ec:2d:63:92:96:45:c5:78:9a:22:90:e5:21:e8:c4:
b5:d1:fe:89:7c:f4:3d:62:10:97:ee:5a:b0:70:ea:
72:04:24:ad:81:d7:7c:a4:bb:c9:4a:be:d6:15:b3:
37:9d:d6:cc:da:bd:ac:c0:91:e4:7b:ef:9d:62:58:
c9:c3:5c:0b:11:9e:6a:60:4b:f3:31:9d:a8:19:b0:
99:28:33:84:a2:81:81:9b:29:25:45:16:af:3f:c5:
19:78:46:5b:df:20:c1:47:bf:01:f6:85:40:e5:5d:
1d:51
prime1:
00:c0:44:8f:88:4b:3b:65:7f:6e:d0:0b:96:7a:82:
da:5a:6f:b6:de:8e:c3:a4:69:c7:a7:9b:50:fc:
0d:f5:0d:1e:a7:5d:3e:f9:32:03:80:28:34:da:1b:
b9:0b:a1:32:c0:34:dc:57:95:ed:0b:e4:53:c8:66:
17:6e:67:11:13:53:ea:4b:b8:06:af:4f:9b:fe:e4:
af:26:56:64:b5:89:42:96:22:08:12:5c:fe:9d:b7:
9a:a9:82:5d:e5:9e:ef:43:c7:59:d2:0f:1e:bl:17:
d8:8f:13:e6:d6:ff:f3:2c:b4:9d:19:4d:80:84:cf:

```

Screenshot8: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
publicExponent: 65537 (0x10001)
privateExponent:
07:4d:ef:90:cd:d5:ed:a2:1d:f0:07:16:33:52:2e:
8d:24:62:15:84:6f:ec:03:b0:8b:a8:45:0f:1b:36:
bb:21:72:90:64:cd:bd:58:ef:fb:9d:2a:74:65:76:
5a:de:b8:04:5f:13:99:bc:08:68:bb:d7:1b:a0:cb:
8b:77:92:1d:9c:73:dd:db:eb:d5:88:90:da:9d:64:
53:b6:c3:a0:c8:51:b2:1d:86:66:aa:82:12:7a:07:
2c:e2:62:47:ab:a4:ea:b1:16:9f:2e:e8:b7:9a:17:
cb:73:63:1e:94:19:d8:7b:c3:93:19:90:f0:e2:6f:
22:04:d3:87:b9:cc:e6:98:b3:a7:23:24:83:3a:67:
4d:50:8c:1a:bc:14:d8:09:bb:3a:30:b9:de:41:c5:
32:68:d6:1c:1b:4b:d5:c4:14:a8:d5:29:e0:6d:22:
4d:6a:5e:7c:70:19:e2:21:26:93:fa:d2:45:55:bd:
47:08:0b:7d:53:35:ac:e1:a0:8c:ed:9c:c9:0a:a1:
31:7c:d0:b3:cd:a8:18:8d:2b:09:f2:d1:f2:4d:88:
6b:c0:dd:1a:f6:97:67:55:c2:e6:c8:87:83:04:14:
e9:cd:a2:8c:01:f2:bd:0c:c2:4e:56:5b:e0:c9:d7:
35:59:05:77:2d:23:c3:fa:03:63:1a:af:35:3e:ba:
9b:2d:be:8e:bb:c3:de:dc:b5:56:bf:f2:90:57:4b:
9e:3a:e9:99:e2:1a:54:9b:60:5f:5b:23:c8:2d:99:
cf:1c:45:fa:10:34:37:1b:8d:e0:2b:d3:4b:8e:e5:
6f:50:19:a1:86:77:21:51:82:1c:56:85:87:52:4b:
54:23:2f:5f:dc:68:fd:cd:f1:c2:82:26:ec:0a:45:
31:22:e5:29:3b:dd:d1:f9:4c:66:91:41:c6:92:81:
a8:51:84:a3:fb:d0:53:1e:a5:2c:9f:7d:cd:5d:fa:
15:de:52:dd:41:ba:67:e1:dc:a9:c2:31:b7:1b:7c:
ae:23:a3:25:91:be:7c:14:4b:db:48:13:59:56:ee:
e2:fb:17:51:83:db:5b:64:82:bf:88:04:35:ca:f8:
ec:2d:63:92:96:45:c5:78:9a:22:90:e5:21:e8:c4:
b5:d1:fe:89:7c:f4:3d:62:10:97:ee:5a:b0:70:ea:
72:04:24:ad:81:d7:7c:a4:bb:c9:4a:be:d6:15:b3:
37:9d:d6:cc:da:bd:ac:c0:91:e4:7b:ef:9d:62:58:
c9:c3:5c:0b:11:9e:6a:60:4b:f3:31:9d:a8:19:b0:
99:28:33:84:a2:81:81:9b:29:25:45:16:af:3f:c5:
19:78:46:5b:df:20:c1:47:bf:01:f6:85:40:e5:5d:
1d:51
prime1:
00:c0:44:8f:88:4b:3b:65:7f:6e:d0:0b:96:7a:82:
da:5a:6f:b6:de:8e:c3:a4:69:c7:a7:9b:50:fc:
0d:f5:0d:1e:a7:5d:3e:f9:32:03:80:28:34:da:1b:
b9:0b:a1:32:c0:34:dc:57:95:ed:0b:e4:53:c8:66:
17:6e:67:11:13:53:ea:4b:b8:06:af:4f:9b:fe:e4:
af:26:56:64:b5:89:42:96:22:08:12:5c:fe:9d:b7:
9a:a9:82:5d:e5:9e:ef:43:c7:59:d2:0f:1e:bl:17:
d8:8f:13:e6:d6:ff:f3:2c:b4:9d:19:4d:80:84:cf:

```

Screenshot9: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
19:78:46:5b:df:20:c1:47:bf:01:f6:85:40:e5:5d:
1d:51
prime1:
00:c0:44:8f:88:4b:3b:65:7f:6e:d0:0b:96:7a:82:
d0:5a:0f:b6:de:8e:c3:a4:69:c7:a7:9b:50:fc:
0d:f5:0d:1e:a7:5d:3e:f9:32:03:80:20:34:da:1b:
b9:0b:a1:32:c0:34:dc:57:95:ed:0b:e4:53:c8:66:
17:6e:67:11:13:53:ea:4b:b8:d0:af:4f:3b:fe:e4:
af:26:56:64:b5:89:42:96:22:98:12:5c:fe:9d:b7:
9a:a9:82:5d:e5:9e:ef:43:c7:59:d2:0f:1e:b1:17:
d8:8f:13:e6:d6:ff:f3:2c:b4:9d:19:4d:80:84:cf:
0d:07:4f:ee:b6:ff:18:f3:98:d9:60:dc:f7:68:0e:
63:cd:82:27:6c:14:40:0b:e2:73:0a:06:5d:72:24:
15:a6:3a:89:51:bb:d0:04:f3:19:28:c9:d9:0d:85:
66:2c:8c:f4:07:88:c3:1a:bb:2c:e8:67:ec:f3:82:
8a:92:b6:3d:ab:ad:81:6e:b8:8c:c8:52:da:53:c9:
40:ea:bd:5a:9a:c7:30:c5:41:46:5b:4b:3c:24:8c:
cc:af:e3:a9:5b:76:91:65:ba:7f:42:7f:01:c6:ca:
89:ca:6e:72:6b:b7:e0:09:12:5c:e5:c0:3b:81:d6:
ac:9c:c9:66:7e:bd:1d:df:26:61:13:c9:4e:7e:0d:
db:49
prime2:
00:f4:e7:4e:85:73:6c:7d:25:41:4e:1e:56:fa:81:
19:77:91:cb:6e:81:01:20:02:18:aa:78:b2:2f:89:
cc:6d:fb:62:02:d1:fc:59:dd:75:95:01:ab:4c:63:
82:0e:ee:49:f2:90:48:c8:79:ea:3e:b0:56:d3:4b:
93:40:e9:6c:7c:41:31:42:11:3b:bd:4b:ec:10:f8:
83:a1:3a:08:c6:e5:f4:f6:df:3f:c7:cc:c8:b6:ee:
c0:22:da:36:14:f6:57:93:ba:4f:fe:e7:89:0d:38:
51:a3:28:35:4e:83:36:61:d7:7b:10:2f:71:37:a4:
26:7b:af:06:04:70:7c:97:88:00:cf:04:29:e0:db:
3f:54:2a:e4:1d:d1:be:94:a1:28:0d:fd:e5:8a:7b:
5d:a6:0b:12:ee:0b:4a:17:6c:72:87:c0:4b:6a:0b:
e5:db:6a:00:7e:11:f7:72:14:f6:ea:f4:40:2b:1d:
ba:9b:18:40:f0:a2:5f:35:94:12:8b:61:29:a4:fc:
7c:09:e7:b3:49:99:ae:6a:05:03:20:5a:a7:1f:ee:
53:b6:44:e7:fc:a0:52:3b:8d:c0:2d:24:22:1e:b8:
da:11:18:d4:a1:df:34:2c:0c:00:07:b1:39:1d:16:
c5:a3:e1:07:bf:64:de:e9:35:9e:0c:5d:3f:f7:50:
f5:91
exponent1:
00:ad:ba:c5:bf:2f:cb:81:d0:fd:fe:3b:1a:43:a5:
0d:4c:7e:79:4c:ec:cf:57:36:c5:d3:76:1d:5f:b6:
01:9e:95:b6:47:20:78:90:8f:02:9e:0b:b6:31:06:
af:d4:14:5a:59:56:ea:6a:b1:ec:39:bc:9d:00:0d:
4f:ca:d0:92:9b:56:4d:f5:12:15:da:de:cb:a5:6c:
59:df:58:5d:33:b3:cd:58:ff:f5:4d:52:7e:37:60:
f9:fd:84:f0:f7:54:ff:79:cd:1e:1a:32:d3:56:cd:
e7:3e:91:8b:1a:66:b8:02:83:49:18:dd:f0:ed:10:
72:03:53:74:ae:1a:e4:8e:e8:64:33:a4:36:61:ed:
ee:bc:79:88:c9:9e:1a:a9:22:7b:34:69:bf:f2:2d:
2c:ea:cd:12:5e:79:0b:bf:46:59:ab:38:31:fb:50:be:
63:2e:8a:46:ce:b0:03:2b:9a:49:df:ce:58:4b:48:
7f:92:45:dd:bf:cc:cd:91:90:6c:95:6e:58:1d:31:
52:d9:49:34:1f:7b:31:54:6b:c0:79:29:28:35:16:
8c:b5:ba:0f:03:b8:45:75:18:69:79:5a:6d:ee:84:
80:b1:4b:cf:54:0a:18:03:da:75:da:9c:32:a9:05:
a3:7f:20:74:de:bc:5f:cb:8d:50:56:a2:a5:ac:3d:
35:11
exponent2:
00:bc:a5:17:f4:ef:ee:17:90:04:f7:d9:a3:02:1f:
43:b0:b8:db:4c:e9:8e:26:4b:b7:18:49:14:68:4d:
ea:ec:a5:00:e0:4f:43:e5:2d:13:0f:8d:d3:97:69:
e7:1a:fd:2e:74:eb:f3:44:89:b4:88:49:68:f8:25:
74:ee:41:5f:d1:6e:9e:34:d7:f5:7e:60:e7:1c:43:
71:91:55:94:c1:31:0d:3a:c4:c8:f0:96:3b:dd:b8:
f7:97:61:22:db:90:58:55:70:e4:81:e3:74:2f:15:
bc:bc:c3:12:1c:c2:31:b7:b8:36:11:47:9a:1c:54:
13:58:9e:7f:32:18:3b:c0:b5:80:79:f6:29:14:0d:
8e:80:94:f1:56:8e:e4:10:b4:fa:97:9c:85:9d:ee:
5d:48:fd:9d:7d:43:b0:f4:ce:12:82:c7:99:fc:a5:
d4:ee:e8:7e:2c:9e:46:4e:d8:1b:42:ec:96:29:20:
23:47:a8:ad:0d:2e:e5:cb:ed:9d:43:43:ba:c2:5d:
c2:66:16:d6:21:d1:81:0a:25:26:3d:5b:d6:f4:54:
e5:e6:b6:b9:43:fd:72:9a:71:22:4a:b3:54:9c:f9:
a2:f0:1c:82:5d:96:03:28:12:ae:4b:3e:96:51:f3:
e2:95:d3:97:16:34:eb:08:14:c7:03:9b:28:d4:a6:
c6:21
coefficient:
3b:63:67:76:40:3e:6b:c2:f7:7e:b1:5a:fc:12:e7:
14:2d:d3:60:1d:54:ba:83:8b:e1:04:0f:5e:bb:fc:
87:ee:ff:c6:8b:9e:ce:fe:dd:9a:ef:61:53:68:19:
5a:a5:35:fa:cc:ca:63:56:83:5e:28:11:44:29:83:
e1:f7:14:15:be:1a:b9:2b:81:61:18:66:89:76:91:
cd:a0:a9:02:17:dc:f6:fe:98:a5:1c:f7:77:94:ba:
ce:40:a1:27:c5:03:fc:bc:f6:31:10:16:7b:ab:63:

```

Screenshot10: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
exponent1:
00:ad:ba:c5:bf:2f:cb:81:d0:fd:fe:3b:1a:43:a5:
0d:4c:7e:79:4c:ec:cf:57:36:c5:d3:76:1d:5f:b6:
01:9e:95:b6:47:20:78:90:8f:02:9e:0b:b6:31:06:
af:d4:14:5a:59:56:ea:6a:b1:ec:39:bc:9d:00:0d:
4f:ca:d0:92:9b:56:4d:f5:12:15:da:de:cb:a5:6c:
59:df:58:5d:33:b3:cd:58:ff:f5:4d:52:7e:37:60:
f9:fd:84:f0:f7:54:ff:79:cd:1e:1a:32:d3:56:cd:
e7:3e:91:8b:1a:66:b8:02:83:49:18:dd:f0:ed:10:
72:03:53:74:ae:1a:e4:8e:e8:64:33:a4:36:61:ed:
ee:bc:79:88:c9:9e:1a:a9:22:7b:34:69:bf:f2:2d:
2c:ea:cd:12:5e:79:0b:bf:46:59:ab:38:31:fb:50:be:
63:2e:8a:46:ce:b0:03:2b:9a:49:df:ce:58:4b:48:
7f:92:45:dd:bf:cc:cd:91:90:6c:95:6e:58:1d:31:
52:d9:49:34:1f:7b:31:54:6b:c0:79:29:28:35:16:
8c:b5:ba:0f:03:b8:45:75:18:69:79:5a:6d:ee:84:
80:b1:4b:cf:54:0a:18:03:da:75:da:9c:32:a9:05:
a3:7f:20:74:de:bc:5f:cb:8d:50:56:a2:a5:ac:3d:
35:11
exponent2:
00:bc:a5:17:f4:ef:ee:17:90:04:f7:d9:a3:02:1f:
43:b0:b8:db:4c:e9:8e:26:4b:b7:18:49:14:68:4d:
ea:ec:a5:00:e0:4f:43:e5:2d:13:0f:8d:d3:97:69:
e7:1a:fd:2e:74:eb:f3:44:89:b4:88:49:68:f8:25:
74:ee:41:5f:d1:6e:9e:34:d7:f5:7e:60:e7:1c:43:
71:91:55:94:c1:31:0d:3a:c4:c8:f0:96:3b:dd:b8:
f7:97:61:22:db:90:58:55:70:e4:81:e3:74:2f:15:
bc:bc:c3:12:1c:c2:31:b7:b8:36:11:47:9a:1c:54:
13:58:9e:7f:32:18:3b:c0:b5:80:79:f6:29:14:0d:
8e:80:94:f1:56:8e:e4:10:b4:fa:97:9c:85:9d:ee:
5d:48:fd:9d:7d:43:b0:f4:ce:12:82:c7:99:fc:a5:
d4:ee:e8:7e:2c:9e:46:4e:d8:1b:42:ec:96:29:20:
23:47:a8:ad:0d:2e:e5:cb:ed:9d:43:43:ba:c2:5d:
c2:66:16:d6:21:d1:81:0a:25:26:3d:5b:d6:f4:54:
e5:e6:b6:b9:43:fd:72:9a:71:22:4a:b3:54:9c:f9:
a2:f0:1c:82:5d:96:03:28:12:ae:4b:3e:96:51:f3:
e2:95:d3:97:16:34:eb:08:14:c7:03:9b:28:d4:a6:
c6:21
coefficient:
3b:63:67:76:40:3e:6b:c2:f7:7e:b1:5a:fc:12:e7:
14:2d:d3:60:1d:54:ba:83:8b:e1:04:0f:5e:bb:fc:
87:ee:ff:c6:8b:9e:ce:fe:dd:9a:ef:61:53:68:19:
5a:a5:35:fa:cc:ca:63:56:83:5e:28:11:44:29:83:
e1:f7:14:15:be:1a:b9:2b:81:61:18:66:89:76:91:
cd:a0:a9:02:17:dc:f6:fe:98:a5:1c:f7:77:94:ba:
ce:40:a1:27:c5:03:fc:bc:f6:31:10:16:7b:ab:63:

```

Screenshot 11: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
63:2e:8a:46:ce:b0:03:2b:9a:49:df:ce:58:4b:48:
7f:92:45:dd:bf:cc:cd:91:90:6c:95:6e:58:1d:31:
52:d9:49:34:1f:7b:31:54:0b:c0:f9:29:28:35:16:
8c:b5:ba:0f:03:b0:45:75:10:69:79:5a:6d:ee:04:
80:b1:4b:cf:54:0a:18:03:da:75:da:9c:32:a9:05:
a3:7f:20:74:de:bc:5f:cb:8d:50:56:a2:a5:ac:3d:
35:11
exponent2:
00:bc:a5:17:f4:ef:ee:17:90:04:f7:d9:a3:02:1f:
43:b0:b8:db:4c:e9:8e:26:4b:b7:18:49:14:68:4d:
ea:ec:a5:00:e0:4f:43:e5:2d:13:0f:0d:d3:97:69:
e7:1a:fd:2e:74:eb:f3:44:89:b4:08:49:68:f8:25:
74:ee:41:5f:d1:6e:9e:34:d7:f5:7e:66:e7:1c:43:
71:91:55:94:c1:31:0d:3a:c4:c8:f0:96:3b:dd:b8:
f7:97:61:22:db:90:58:55:70:e4:81:e3:74:2f:15:
bc:bc:c3:12:1c:c2:31:b7:b0:36:11:47:9a:1c:54:
13:58:9e:7f:32:18:3b:c0:b5:80:79:f6:29:14:0d:
8e:80:94:f1:56:8e:e4:10:b4:fa:97:9c:85:9d:e0:
5d:48:fd:9d:7d:43:b0:f4:ce:12:02:c7:99:fc:05:
d4:ee:e0:7e:2c:9e:46:4e:d0:1b:42:ec:96:29:20:
23:47:a8:ad:0d:2e:e5:cb:ed:9d:43:43:ba:c2:5d:
c2:06:16:d6:21:d1:81:6a:25:26:3d:5b:d0:f4:54:
e5:ee:b6:b9:43:fd:72:9a:71:22:4a:b3:54:9c:f9:
a2:f0:1c:02:5d:96:03:28:12:ae:4b:3e:96:51:f3:
e2:95:d3:97:16:34:eb:08:14:c7:03:9b:28:d4:a6:
c6:21
coefficent:
3b:03:d7:76:40:3e:6b:c2:f7:7e:b1:5a:fc:12:e7:
14:2d:d3:60:1d:54:ba:83:0b:e1:04:0f:5e:bb:fc:
87:ee:ff:c6:8b:9e:ce:f0:dd:9a:ef:01:53:08:19:
5a:a5:35:fa:cc:ca:03:56:03:5e:28:11:44:29:83:
e1:f7:14:15:be:1a:b9:2b:01:01:18:66:89:76:91:
cd:a0:a9:02:17:dc:f6:fe:98:a5:1c:7f:77:94:ba:
ce:40:a1:27:c5:03:fc:bc:f0:31:10:16:7b:ab:63:
f2:c2:af:aa:43:06:8a:14:33:48:55:5e:7e:33:e7:
0c:4f:5a:73:d1:1b:74:f3:ac:bf:e9:c2:97:6b:e2:
0a:f2:bc:9f:9b:13:99:9a:df:cf:05:93:f1:c5:1a:
b0:0c:cc:da:d6:d4:b0:9c:8e:94:c8:5b:25:40:df:
2b:d6:73:7b:80:1a:94:b7:19:1f:b1:fa:b0:68:7c:
90:44:e1:f9:79:16:8e:19:54:fb:07:c9:a5:98:18:
fe:b7:60:1a:25:52:42:c5:63:e1:f2:94:8d:c4:d6:
6c:17:a5:c6:d9:75:56:9f:f1:0d:32:cc:d7:2f:66:
1c:86:38:09:8a:00:e4:03:da:4b:a2:68:08:4b:01:
12:21:b2:1a:21:d7:2e:75:d7:b4:d1:2b:7b:28:28:
c0
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```


Screenshots: Task 2

Screenshot12: ([Return to text](#))

```
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl req -newkey rsa:2048 -sha256 \
    -keyout server.key -out server.csr \
-subj "/CN=www.eubanks2023.com/O=Bank32 Inc./C=US" \
-passout pass:19June2022
```

A large amount of asterisks (*) representing progress or output.

```
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$
```

Screenshot13: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
++++
-----
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl req -in server.csr -text -noout
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: CN = www.eubanks2023.com, O = Bank32 Inc., C = US
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:ad:bc:b1:a7:83:4d:31:db:f2:f8:36:b8:f1:cd:
        1e:11:f7:55:54:ff:f0:60:cf:f8:13:6c:ea:3a:92:
        51:d1:6b:49:06:34:b3:60:bb:e4:62:4f:12:cf:0c:
        37:12:07:2f:2e:a8:81:01:ab:52:c1:90:fc:01:d2:
        f4:6f:6b:e9:ae:13:49:06:6c:04:d2:05:a3:4d:43:
        4e:7c:f3:c2:b5:6d:92:dc:f7:fb:0e:db:34:cc:a4:
        08:26:32:16:91:47:12:d8:3f:e9:12:7d:6e:8a:8a:
        bd:1a:1e:e5:33:d3:39:54:12:79:66:0f:0b:67:13:
        a8:54:56:f0:85:70:e0:30:29:ea:a4:72:6b:13:ac:
        ec:07:17:53:ab:11:fb:50:e9:3e:09:0c:52:90:50:
        7a:b8:a3:98:e0:ca:de:92:b1:eb:fe:0e:b6:26:c0:
        fe:67:c8:5b:92:ef:eb:26:3d:8f:40:7f:45:2e:5:
        3f:34:10:ee:71:12:fd:23:49:6e:7c:30:09:cc:53:
        de:61:be:e7:cf:4f:20:51:46:a9:01:b4:85:86:f4:
        41:47:9e:db:cf:c4:41:dc:da:99:80:17:53:be:b0:
        2a:1e:0f:d3:63:cf:e8:b4:4b:7e:88:1f:ee:95:9e:
        55:95:80:db:63:52:14:13:80:9c:c4:95:a8:03:9b:
        48:d3
      Exponent: 65537 (0x10001)
  Attributes:
    (none)
  Requested Extensions:
  Signature Algorithm: sha256withRSAEncryption
  Signature Value:
    03:1d:b8:e3:58:c1:e5:55:8e:d9:f1:3b:67:b8:00:17:a5:11:
    fc:8f:e4:63:et:53:91:7c:0b:42:0f:9c:44:de:78:b6:22:75:
    1a:cf:a3:60:50:27:25:65:09:0c:9a:3b:11:ea:67:e5:30:97:
    72:7e:99:51:22:32:d4:07:3e:a3:a4:82:cd:ed:42:08:86:c6:
    66:ef:f5:cc:3f:dc:2b:af:ea:20:92:c7:f4:1d:fa:f4:5d:06:
    cc:07:a3:4e:7e:67:9f:7e:ae:28:ed:1b:10:ac:f1:13:3c:21:
    c4:7f:7d:31:51:ae:28:ab:25:79:c4:aa:84:38:e8:71:53:42:
    30:07:13:ca:59:a4:9f:ba:d6:69:b3:e5:5b:86:40:67:2b:a1:
    0b:de:4b:2d:ba:34:fb:c4:b4:71:42:b7:2f:c9:4d:3b:7e:ed:
    7f:91:1c:34:45:1f:17:cb:98:b8:3b:f2:2b:4a:40:63:25:0e:
    59:27:02:34:8a:cf:3d:a9:43:db:66:f8:1b:95:d0:73:5e:cc:

```

Screenshot14: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
Version: 1 (0x0)
Subject: CN = www.eubanks2023.com, O = Bank32 Inc., C = US
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
  Modulus:
    00:ad:bc:b1:a7:83:4d:31:db:f2:f8:36:b8:f1:cd:
    1e:11:f7:55:54:ff:f0:60:cf:f8:13:6c:ea:3a:92:
    51:d1:6b:49:06:34:b3:60:bb:e4:62:4f:12:cf:0c:
    37:12:07:2f:2e:a8:81:01:ab:52:c1:90:fc:01:d2:
    f4:6f:6b:e9:ae:13:49:06:6c:04:d2:05:a3:4d:43:
    4e:7c:f3:c2:b5:6d:92:dc:fb:7f:8e:db:34:cc:a4:
    08:26:32:16:91:47:12:d8:3f:e9:12:7d:6e:8a:a8:
    bd:1a:1e:e5:33:df:39:54:12:79:66:8f:0b:67:13:
    a8:54:56:f0:85:70:e0:30:29:ea:a4:72:6b:13:ac:
    ec:07:17:53:ab:11:fb:50:e9:3e:09:0c:52:90:50:
    7a:b8:a3:98:e6:ca:de:92:b1:eb:fe:0e:b6:26:c0:
    f8:f7:c8:5b:92:ef:eb:26:3d:8f:49:a7:f5:2e:65:
    3f:34:10:ee:71:12:fd:23:49:6e:7c:30:09:cc:53:
    de:61:be:e7:cf:4f:20:51:46:a9:01:ba:85:86:f4:
    41:47:9e:db:cf:c4:41:dc:da:99:80:17:53:be:b0:
    2a:1e:0f:d3:63:cf:e8:b4:4b:7e:88:1f:ee:95:9e:
    55:95:80:db:63:52:14:13:80:9c:c4:95:a8:03:9b:
    48:d3
  Exponent: 65537 (0x10001)
Attributes:
  (none)
Requested Extensions:
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
  63:1d:b8:e3:58:c1:e5:55:0e:d9:f1:3b:67:b8:80:17:a5:11:
  fc:8f:e4:63:e1:53:91:7c:0b:42:0f:9c:44:de:78:86:22:75:
  1a:cf:a3:08:50:27:25:65:09:0c:38:3b:11:e4:67:e5:38:97:
  72:7e:99:51:22:32:4d:07:3e:a3:a4:82:dc:ed:42:e8:86:c6:
  66:ef:f5:cc:3f:dc:2b:af:ea:20:92:c7:f4:1d:fa:f4:5d:06:
  cc:07:a3:4e:7e:07:9f:7e:ae:28:ed:1b:10:ac:f1:13:3c:21:
  c4:7f:7d:31:51:ae:28:ab:25:79:c4:aa:84:38:e8:71:53:42:
  30:07:13:ca:59:a4:9f:ba:d6:69:b3:e5:b5:86:40:67:2b:a1:
  0b:d4:4b:2d:ba:34:fb:c4:b4:71:42:b7:2f:c9:42:b3:7e:ed:
  f7:91:1c:34:45:1f:17:cb:98:b8:3b:f2:2b:4a:48:63:25:0e:
  50:27:02:34:8a:cf:3d:a9:43:db:66:f8:1b:95:d9:73:5e:cc:
  b8:6c:8d:ab:cd:f4:66:1c:19:37:36:0f:5b:a8:e2:0d:e4:1c:
  26:1f:ef:78:c4:95:73:4f:18:d8:94:f8:db:c1:9a:fa:7a:ad:
  a2:ed:16:c3:f4:b2:22:12:a5:aa:8d:d5:c5:1e:e9:f3:1c:ca:
  aa:e5:09:a9
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```

Screenshot15: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
26:1f:ef:78:c4:95:73:4f:18:d8:94:f8:6b:c1:9a:fa:7a:ad:
a2:ed:16:c3:f4:b2:22:12:a5:aa:8d:d5:c5:1e:e9:f3:1c:ca:
aa:e5:09:a9
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
Private-Key: (2048 bit, 2 primes)
modulus:
  00:ad:bc:b1:a7:83:4d:31:db:f2:f8:36:b8:f1:cd:
  1e:11:f7:55:54:ff:f0:60:cf:f8:13:6c:ea:3a:92:
  51:d1:6b:49:06:34:b3:60:bb:e4:62:4f:12:cf:0c:
  37:12:07:2f:2e:a8:81:01:ab:52:c1:90:fc:01:d2:
  f4:6f:6b:e9:ae:13:49:06:6c:04:d2:05:a3:4d:43:
  4e:7c:f3:c2:b5:6d:92:dc:fb:7f:8e:db:34:cc:a4:
  08:26:32:16:91:47:12:d8:3f:e9:12:7d:6e:8a:a8:
  bd:1a:1e:e5:33:df:39:54:12:79:66:8f:0b:67:13:
  a8:54:56:f0:85:70:e0:30:29:ea:a4:72:6b:13:ac:
  ec:07:17:53:ab:11:fb:50:e9:3e:09:0c:52:90:50:
  7a:b8:a3:98:e6:ca:de:92:b1:eb:fe:0e:b6:26:c0:
  f8:f7:c8:5b:92:ef:eb:26:3d:8f:49:a7:f5:2e:65:
  3f:34:10:ee:71:12:fd:23:49:6e:7c:30:09:cc:53:
  de:61:be:e7:cf:4f:20:51:46:a9:01:ba:85:86:f4:
  41:47:9e:db:cf:c4:41:dc:da:99:80:17:53:be:b0:
  2a:1e:0f:d3:63:cf:e8:b4:4b:7e:88:1f:ee:95:9e:
  55:95:80:db:63:52:14:13:80:9c:c4:95:a8:03:9b:
  48:d3
publicExponent: 65537 (0x10001)
privateExponent:
  07:44:f1:7b:91:c2:2b:a9:61:e6:37:df:66:db:46:
  e5:b8:ae:e5:bf:49:43:0f:33:10:16:37:c6:de:a0:
  5a:40:6a:b0:11:25:c4:ef:03:8d:99:08:65:f5:d1:
  fc:e1:ed:31:73:34:22:ce:d9:7d:28:ce:02:81:a4:
  cf:6a:64:fb:c7:a2:03:86:d9:03:c1:ea:fd:48:7f:
  98:30:bb:99:89:3d:6c:d6:ef:a7:cd:40:16:a6:32:
  15:9c:21:09:07:40:70:20:ed:d2:b2:66:cc:52:8d:
  20:4e:a6:94:f2:a8:90:b4:f5:03:c5:07:7f:7f:75:
  f9:3e:cb:81:74:f3:bf:f3:21:d2:08:bd:f3:06:0e:
  b7:cd:35:31:22:05:c9:4d:75:1f:60:bf:8f:76:1b:
  8c:5a:69:49:38:29:03:7d:9f:8c:78:52:d1:b6:75:
  d2:50:0d:ef:a6:39:e0:07:b5:ae:85:f0:9e:f5:9e:
  1c:91:9c:7b:78:32:f2:86:79:88:7e:30:f0:d8:54:
  a5:cc:6e:c4:ef:8c:39:30:6c:20:52:86:12:00:23:
  30:df:53:85:52:00:59:e8:f2:47:74:74:2b:7a:bb:
  a0:f5:34:d2:3f:b8:be:5e:83:b8:7f:d5:0e:07:bf:
  42:c5:06:f0:88:11:38:81:17:cf:a5:51:0d:2f:62:
  01
prime1:

```

Screenshot16: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI

prime1:
00:bc:0c:44:8f:87:a1:ae:18:af:a9:59:94:bd:60:
a6:11:fc:94:88:00:1e:cd:80:81:b3:24:6d:9a:50:
70:24:8c:75:8f:c6:84:cc:0c:22:48:99:00:42:51:
be:08:b2:27:c4:23:00:3a:02:2f:0b:a6:5d:4b:d8:
97:44:48:28:1a:e4:bb:fa:f5:5b:6a:dd:98:c2:7a:
76:79:ff:46:27:83:36:48:c3:04:ef:12:5a:31:fa:
2f:0a:0d:1c:34:91:fa:bc:28:7b:62:fd:c0:15:47:
7d:43:02:0a:a3:f7:38:60:61:6a:41:3e:56:17:d4:
ab:ad:d2:11:c2:c7:e2:19:01

prime2:
00:ec:84:93:32:19:2d:34:0b:9d:ae:5e:c1:ae:50:
fa:76:0f:7a:16:17:43:4f:40:cc:04:33:45:b3:c9:
5c:12:4d:32:a1:58:09:c1:de:c2:7b:52:66:50:7b:
7f:d5:6e:9b:57:2a:6d:80:fb:0a:c7:7f:90:40:66:
20:e1:a1:0b:ca:7d:2d:63:d4:3c:35:32:f5:86:34:
6d:de:71:8c:9d:b1:fd:08:5b:48:ae:08:8a:ab:31:
f6:bf:e3:b5:25:ad:71:da:a3:1e:48:2b:7a:be:49:
73:bc:18:44:d9:ea:06:81:cb:08:2e:86:b6:56:d6:
24:ef:de:65:04:96:5b:ad:d3

exponent1:
3d:03:7d:fb:53:f6:91:96:50:e8:91:b8:40:f9:ea:
e8:4b:1b:a6:44:e3:b9:a9:c8:0b:67:96:08:4b:51:
17:8a:bb:5a:3a:ff:3b:75:74:6a:39:ba:6b:ca:3a:
17:5a:16:ac:fd:17:cd:ea:0f:7f:a8:2a:fd:40:f9:
53:9e:55:e4:e3:f2:5a:2a:e1:ce:7a:b7:e5:e1:f6:
2e:ff:34:b3:fd:4e:cf:ac:f7:1c:da:c7:89:0f:b3:
d3:7f:0d:77:c1:25:a9:87:39:01:95:73:8d:73:f4:
a0:99:38:fa:9a:6c:20:59:7b:30:50:19:7f:01:f1:
f2:24:06:bf:3c:3b:90:01

exponent2:
00:bc:db:0d:1c:3f:04:4c:ce:e8:29:ce:20:fb:6e:
55:69:5e:7b:62:f7:db:4e:5a:af:b9:2f:43:5a:eb:
91:a6:9e:cb:33:cf:cc:48:7e:de:6e:02:01:b2:22:
00:7f:96:22:b8:38:fb:8d:61:f0:7f:67:77:12:66:
89:d1:55:4b:a0:5f:42:76:a1:cf:e9:0d:94:9c:fa:
4d:80:84:f2:e1:79:b6:bb:1e:85:72:e7:29:19:22:
af:90:c4:a5:3d:c3:c3:cc:ca:5f:c8:5c:a2:e6:ce:
7b:1d:a0:33:d1:69:e7:0f:25:20:7a:78:24:f0:5e:
9e:84:5c:a6:1b:16:71:28:b3

coefficient:
54:ea:ea:b0:3b:2a:65:d4:d5:2f:ff:e9:01:00:86:
5f:94:68:27:75:b0:7d:7c:fb:5a:4f:1f:02:ad:36:
7e:1e:1d:ea:81:20:4d:8f:9f:4d:c6:68:a5:73:82:
18:ba:bf:9e:3a:e9:3e:c3:5c:fb:23:59:56:d6:4b:
f1:ed:c1:90:ce:db:da:05:15:cf:0d:10:9b:4b:c5:
e5:7c:fd:c3:4a:dc:d6:1d:75:e4:d3:b6:01:4c:71:
12:aa:82:7b:2e:eb:ab:08:33:fe:73:b0:fa:70:64:
4b:bf:41:09:67:0d:de:41:15:0b:fe:fe:es:58:07:
9f:cb:56:36:b6:08:fb:ec

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```

Screenshot17: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI

97:44:48:28:1a:e4:bb:fa:f5:5b:6a:dd:98:c2:7a:
76:79:ff:46:27:83:36:48:c3:04:ef:12:5a:31:fa:
2f:0a:0d:1c:34:91:fa:bc:28:7b:62:fd:c0:15:47:
7d:43:02:0a:a3:f7:38:60:61:6a:41:3e:56:17:d4:
ab:ad:d2:11:c2:c7:e2:19:01

prime2:
00:ec:84:93:32:19:2d:34:0b:9d:ae:5e:c1:ae:50:
fa:76:0f:7a:16:17:43:4f:40:cc:04:33:45:b3:c9:
5c:12:4d:32:a1:58:09:c1:de:c2:7b:52:66:50:7b:
7f:d5:6e:9b:57:2a:6d:80:fb:0a:c7:7f:90:40:66:
20:e1:a1:0b:ca:7d:2d:63:d4:3c:35:32:f5:86:34:
6d:de:71:8c:9d:b1:fd:08:5b:48:ae:08:8a:ab:31:
f6:bf:e3:b5:25:ad:71:da:a3:1e:48:2b:7a:be:49:
73:bc:18:44:d9:ea:06:81:cb:08:2e:86:b6:56:d6:
24:ef:de:65:04:96:5b:ad:d3

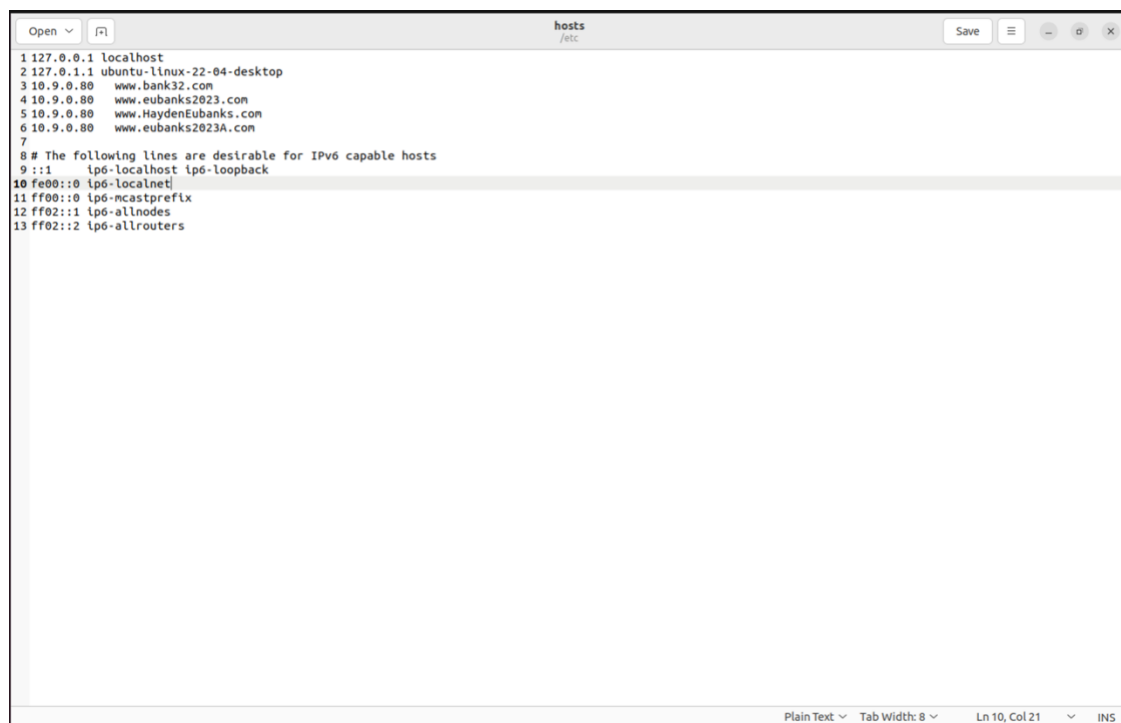
exponent1:
3d:03:7d:fb:53:f6:91:96:50:e8:91:b8:40:f9:ea:
e8:4b:1b:a6:44:e3:b9:a9:c8:0b:67:96:08:4b:51:
17:8a:bb:5a:3a:ff:3b:75:74:6a:39:ba:6b:ca:3a:
17:5a:16:ac:fd:17:cd:ea:0f:7f:a8:2a:fd:40:f9:
53:9e:55:e4:e3:f2:5a:2a:e1:ce:7a:b7:e5:e1:f6:
2e:ff:34:b3:fd:4e:cf:ac:f7:1c:da:c7:89:0f:b3:
d3:7f:0d:77:c1:25:a9:87:39:01:95:73:8d:73:f4:
a0:99:38:fa:9a:6c:20:59:7b:30:50:19:7f:01:f1:
f2:24:06:bf:3c:3b:90:01

exponent2:
00:bc:db:0d:1c:3f:04:4c:ce:e8:29:ce:20:fb:6e:
55:69:5e:7b:62:f7:db:4e:5a:af:b9:2f:43:5a:eb:
91:a6:9e:cb:33:cf:cc:48:7e:de:6e:02:01:b2:22:
00:7f:96:22:b8:38:fb:8d:61:f0:7f:67:77:12:66:
89:d1:55:4b:a0:5f:42:76:a1:cf:e9:0d:94:9c:fa:
4d:80:84:f2:e1:79:b6:bb:1e:85:72:e7:29:19:22:
af:90:c4:a5:3d:c3:c3:cc:ca:5f:c8:5c:a2:e6:ce:
7b:1d:a0:33:d1:69:e7:0f:25:20:7a:78:24:f0:5e:
9e:84:5c:a6:1b:16:71:28:b3

coefficient:
54:ea:ea:b0:3b:2a:65:d4:d5:2f:ff:e9:01:00:86:
5f:94:68:27:75:b0:7d:7c:fb:5a:4f:1f:02:ad:36:
7e:1e:1d:ea:81:20:4d:8f:9f:4d:c6:68:a5:73:82:
18:ba:bf:9e:3a:e9:3e:c3:5c:fb:23:59:56:d6:4b:
f1:ed:c1:90:ce:db:da:05:15:cf:0d:10:9b:4b:c5:
e5:7c:fd:c3:4a:dc:d6:1d:75:e4:d3:b6:01:4c:71:
12:aa:82:7b:2e:eb:ab:08:33:fe:73:b0:fa:70:64:
4b:bf:41:09:67:0d:de:41:15:0b:fe:fe:es:58:07:
9f:cb:56:36:b6:08:fb:ec

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

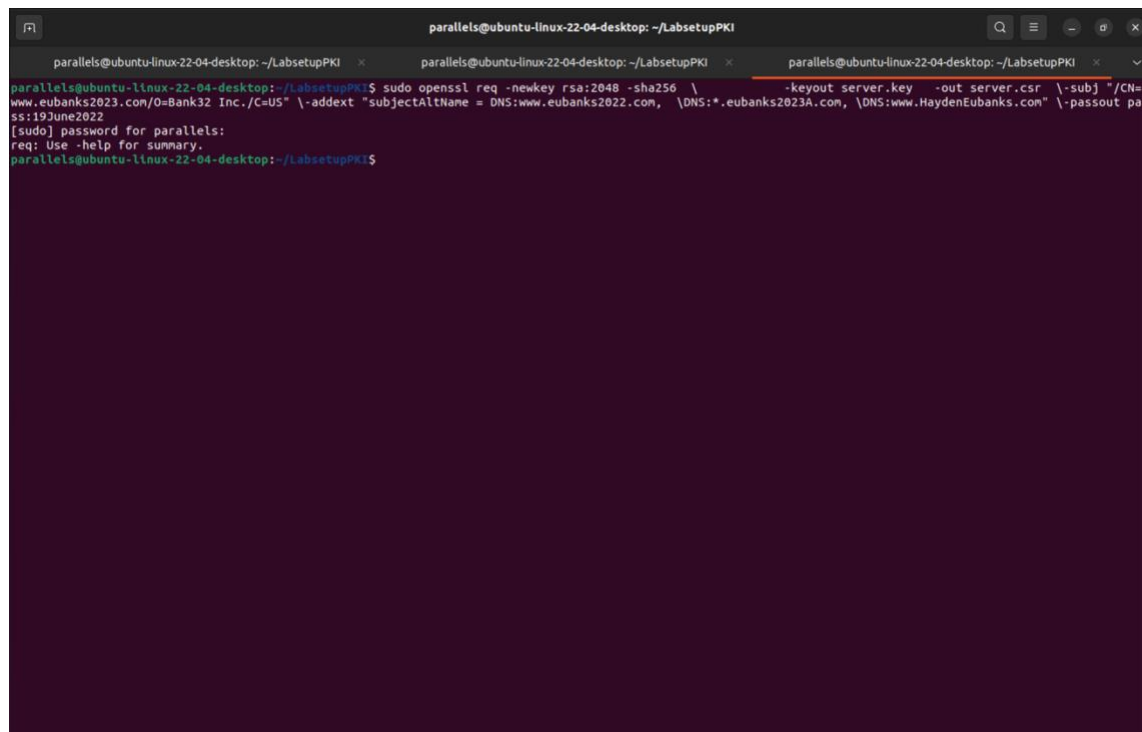
```

Screenshot18: ([Return to text](#))

A screenshot of a text editor window titled 'hosts /etc'. The window contains the following text:

```
1 127.0.0.1 localhost
2 127.0.1.1 ubuntu-linux-22-04-desktop
3 10.9.0.80 www.bank32.com
4 10.9.0.80 www.eubanks2023.com
5 10.9.0.80 www.HaydenEubanks.com
6 10.9.0.80 www.eubanks2023A.com
7
8 # The following lines are desirable for IPv6 capable hosts
9 ::1   tp6-localhost tp6-loopback
10 fe00::0 tp6-localnet
11 ff00::0 tp6-ncastprefix
12 ff02::1 tp6-allnodes
13 ff02::2 tp6-allrouters
```

The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 10, Col 21', and 'INS'.

Screenshot19: ([Return to text](#))

A screenshot of a terminal window titled 'parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI'. The terminal shows the following commands and output:

```
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ sudo openssl req -newkey rsa:2048 -sha256 \
    -keyout server.key -out server.csr \-subj "/CN=
www.eubanks2023.com/O=Bank32 Inc./C=US" \-addext "subjectAltName = DNS:www.eubanks2022.com, \DNS:*.eubanks2023A.com, \DNS:www.HaydenEubanks.com" \-passout pa
ss:19June2022
[sudo] password for parallels:
req: Use -help for summary.
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$
```


Screenshots: Task 3

Screenshot20: ([Return to text](#))

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl ca -config myCA_openssl.cnf -policy policy_anything \
    -md sha256 -days 3650 \
    -in server.csr -out server.crt -batch \
    -cert cacert -keyfile ca.key
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: Oct  5 13:32:12 2023 GMT
    Not After : Oct  2 13:32:12 2033 GMT
  Subject:
    countryName       = US
    organizationName  = Bank32 Inc.
    commonName        = www.eubanks2023.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      30:FA:7D:6D:46:6F:F3:83:4E:69:E4:18:F8:46:47:2D:59:38:42:72
    X509v3 Authority Key Identifier:
      04:7E:85:D3:53:30:22:38:8C:B7:0B:8D:BF:FC:31:7F:4C:3A:78:26
Certificate is to be certified until Oct  2 13:32:12 2033 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

```

Screenshot21: ([Return to text](#))

```

GNU nano 6.2 myCA_openssl.cnf
crl_dir      = $dir/crl           # Where the issued crl are kept
database     = $dir/index.txt     # database index file.
unique_subject = no              # Set to 'no' to allow creation of
                                # several certs with same subject.
new_certs_dir = $dir/newcerts     # default place for new certs.

certificate  = $dir/cacert.pem    # The CA certificate
serial       = $dir/serial        # The current serial number
crlnumber    = $dir/crlnumber     # the current crl number
                                # must be commented out to leave a V1 CRL
crl          = $dir/crl.pem       # The current CRL
private_key  = $dir/private/cakey.pem # The private key

X509_extensions = usr_cert       # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt     = ca_default        # Subject Name options
cert_opt     = ca_default        # Certificate field options

# Extension copying option: use with caution.
copy_extensions = copy

# Extensions to add to a CRL. Note: Netscape communicator chokes on V2 CRLs
# so this is commented out by default to leave a V1 CRL.
# crlnumber must also be commented out to leave a V1 CRL.
# crl_extensions = crl_ext

default_days = 365                # how long to certify for
default_crl_days = 30            # how long before next CRL
default_md   = default           # use public key default MD
preserve     = no                # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-))
policy      = policy_match

# For the CA policy
[ policy_match ]
countryName = match
stateOrProvinceName = match

```

Wrote 397 lines

Help Write Out Where Is Cut Execute Location U Undo M-A Set Mark M-] To Bracket
Exit Read File Replace Paste Justify / Go To Line E Redo M-G Copy M-; Where Was

Screenshot22: [\(Return to text\)](#)

```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ openssl x509 -in server.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = US, ST = Pennsylvania, L = Liverpool, CN = HaydenEubanks, emailAddress = heubanks@liberty.edu
    Validity
      Not Before: Oct  5 13:32:12 2023 GMT
      Not After : Oct  2 13:32:12 2033 GMT
    Subject: C = US, O = Bank32 Inc., CN = www.eubanks2023.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:ad:bc:b1:a7:83:4d:31:db:f2:f8:36:b8:f1:cd:
        1e:11:f7:55:54:ff:f0:00:cf:f8:13:6c:ea:3a:92:
        51:d1:0b:49:06:34:b3:60:bb:e4:62:4f:12:cf:0e:
        37:12:07:2f:2e:a8:01:01:ab:52:c1:9a:fc:01:d2:
        f4:0f:6b:e9:ae:13:49:06:6c:04:d2:05:a3:4d:43:
        4e:7c:f3:c2:b5:6d:92:dc:fb:7f:8e:db:34:cc:a4:
        08:26:32:16:91:47:12:d8:3f:e9:12:7d:6e:8a:a8:
        bd:1a:1e:e5:33:df:39:54:12:79:66:8f:0b:67:13:
        a8:54:56:f0:85:70:e0:30:29:ea:a4:72:6b:13:ac:
        ec:07:17:53:ab:11:fb:50:e9:3e:09:0c:52:90:50:
        7a:b8:a3:98:e6:ca:de:92:b1:eb:fe:0e:b6:26:c0:
        f8:f7:c8:5b:92:ef:eb:26:3d:8f:49:a7:f5:2e:65:
        3f:34:10:ee:71:12:fd:23:49:de:7c:30:09:cc:53:
        de:61:be:e7:cf:4f:20:51:46:a9:01:ba:85:80:f4:
        41:47:9e:db:cf:c4:41:dc:da:99:80:17:53:be:b0:
        2a:1e:0f:d3:63:cf:e8:b4:4b:7e:88:1f:ee:95:9e:
        55:95:80:db:63:52:14:13:80:9c:c4:95:a8:03:9b:
        48:d3
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        30:FA:7D:6D:46:6F:F3:83:4E:69:E4:18:F8:46:47:2D:59:38:42:72
      X509v3 Authority Key Identifier:
        04:7E:85:D3:53:30:22:3B:8C:87:0B:8D:BF:FC:31:7F:4C:3A:78:26
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
      53:39:b0:44:5b:b1:2b:76:ae:c1:6d:2a:58:34:5a:26:9c:10:
      bc:35:a0:74:4c:3d:79:6c:09:4c:5e:9f:12:f8:0d:76:f9:d4:
      f0:84:89:46:89:f0:cd:ce:5f:6c:b7:95:98:6a:ea:d8:1e:1b:

```

Screenshot23: [\(Return to text\)](#)

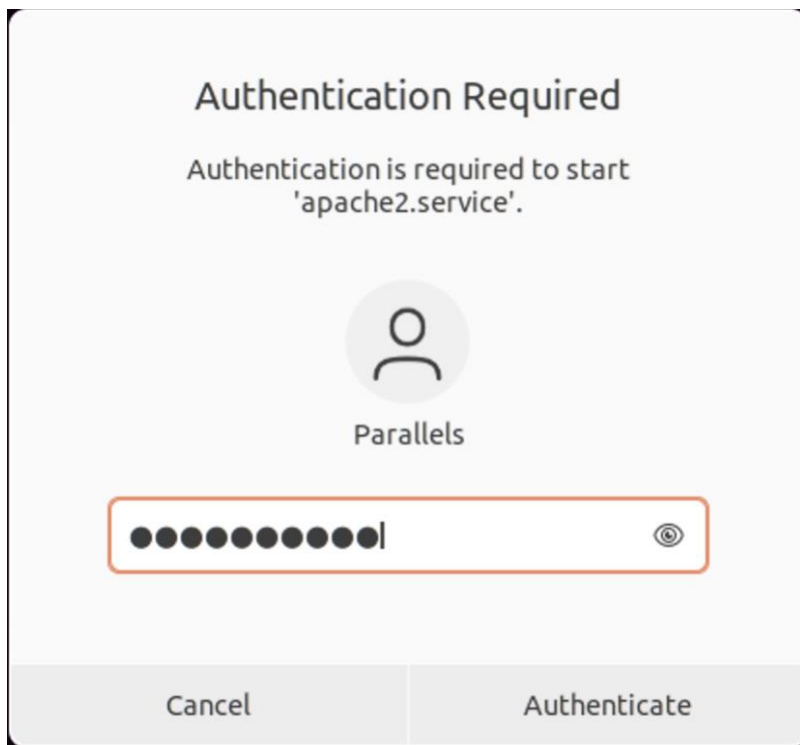
```

parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$ 
3f:34:10:ee:71:12:fd:23:49:de:7c:30:09:cc:53:
de:61:be:e7:cf:4f:20:51:46:a9:01:ba:85:80:f4:
41:47:9e:db:cf:c4:41:dc:da:99:80:17:53:be:b0:
2a:1e:0f:d3:63:cf:e8:b4:4b:7e:88:1f:ee:95:9e:
55:95:80:db:63:52:14:13:80:9c:c4:95:a8:03:9b:
48:d3
  Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      30:FA:7D:6D:46:6F:F3:83:4E:69:E4:18:F8:46:47:2D:59:38:42:72
    X509v3 Authority Key Identifier:
      04:7E:85:D3:53:30:22:3B:8C:87:0B:8D:BF:FC:31:7F:4C:3A:78:26
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    53:39:b0:44:5b:b1:2b:76:ae:c1:6d:2a:58:34:5a:26:9c:10:
    bc:35:a0:74:4c:3d:79:6c:09:4c:5e:9f:12:f8:0d:76:f9:d4:
    f0:84:89:46:89:f0:cd:ce:5f:6c:b7:95:98:6a:ea:d8:1e:1b:
    be:51:40:da:29:9c:7d:b3:a9:16:2c:18:34:c3:e9:c4:42:b2:
    b7:4c:d5:ae:e5:30:72:44:d1:aa:5c:0c:b5:37:f1:98:e7:01:
    99:e3:39:20:97:e0:17:d6:79:96:dc:1b:86:64:3c:53:68:33:
    be:6e:6d:32:ed:ad:c6:e0:fd:c8:1c:2f:d0:7b:f1:07:74:7c:
    4b:b5:80:c5:c0:0a:c0:f9:98:06:81:2d:44:23:f5:b8:75:99:
    b0:27:97:30:c3:76:d0:34:64:d0:0f:af:e5:8e:4c:d9:a9:7f:
    2a:bc:fc:e5:d0:4b:af:e1:90:b8:43:b1:2e:0c:d4:1f:00:3e:
    89:48:ce:dd:cc:e6:26:a1:d9:21:d4:ab:55:98:b5:13:66:4b:
    73:79:47:90:04:43:aa:9a:b3:fa:66:e8:e8:11:b9:07:3e:3b:
    91:6d:fe:45:b1:af:88:ee:56:c4:33:cb:d0:4e:60:b0:b8:73:
    fb:58:44:36:80:0d:b3:59:04:42:55:8c:0a:12:5e:2e:e2:46:
    a2:57:ad:fa:85:64:30:17:e0:2a:2e:46:1a:cc:9a:57:81:7c:
    f0:67:04:51:c6:be:5f:7e:46:c1:2d:ce:73:5d:f0:9a:75:1c:
    52:f2:69:91:bf:46:e0:13:2b:63:f2:7a:24:46:c0:34:4d:81:
    02:9a:81:73:0c:da:d0:40:30:49:f1:95:15:81:6c:23:b1:59:
    2d:db:d7:0d:8c:b9:22:2a:f8:77:09:95:b6:bd:ad:f0:4e:7e:
    ce:cc:8f:ef:14:5a:fc:a4:ce:27:de:cc:51:49:7b:bd:d3:77:
    dd:a3:9a:55:b6:e9:56:92:1c:6e:ac:ae:bf:4f:df:37:26:73:
    7a:0e:b7:20:b2:67:e4:79:96:5e:c2:a8:3f:14:da:14:79:c1:
    ac:4c:77:27:6d:92:64:a0:71:14:d1:3a:c9:7b:cb:12:7a:53:
    27:2f:9a:18:c1:4e:48:09:3e:7b:ed:f2:2d:e8:a9:2c:6e:65:
    87:21:f2:d3:dc:cb:f0:cb:5e:a5:35:f8:ed:b3:73:2f:89:7b:
    2b:86:5b:4a:63:19:38:bf:02:bd:e8:f0:a2:8d:f4:4e:f0:b3:
    1b:0d:18:b6:b3:9e:fc:e3:4f:b1:19:4a:42:2b:14:23:3e:36:
    7e:6b:cc:06:70:1f:76:84:63:68:61:ac:89:0b:80:99:88:fd:
    35:0b:7e:95:26:85:e5:a1
parallels@ubuntu-linux-22-04-desktop: ~/LabsetupPKI$

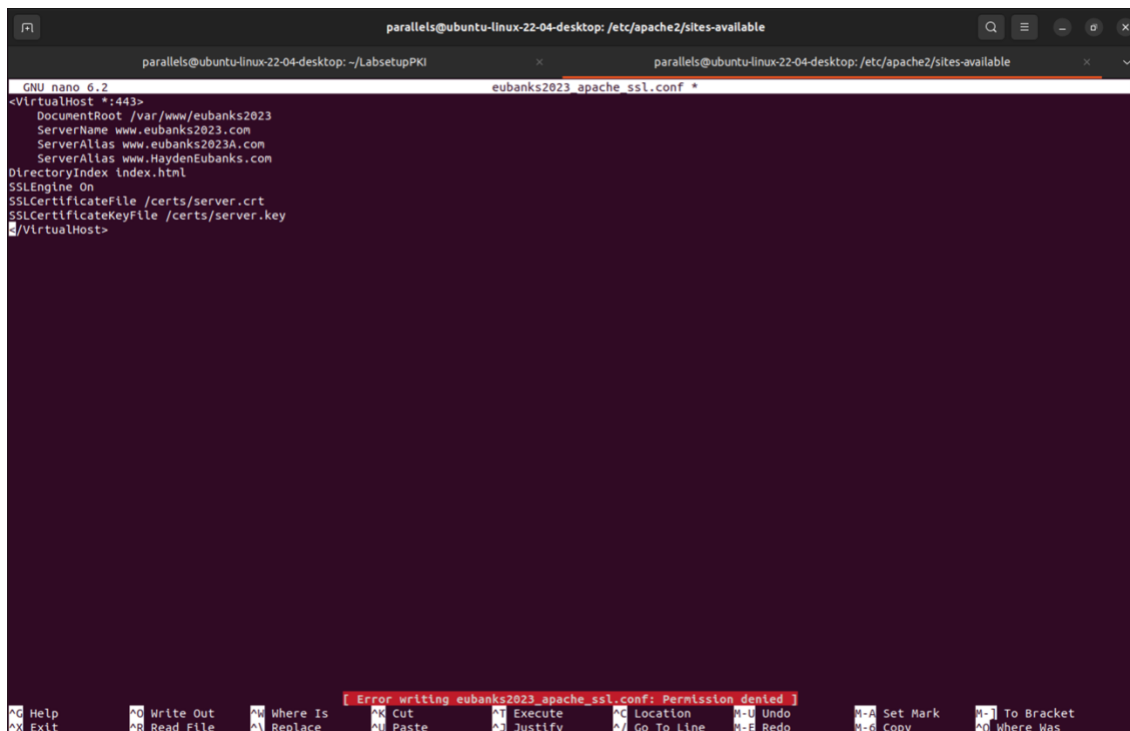
```

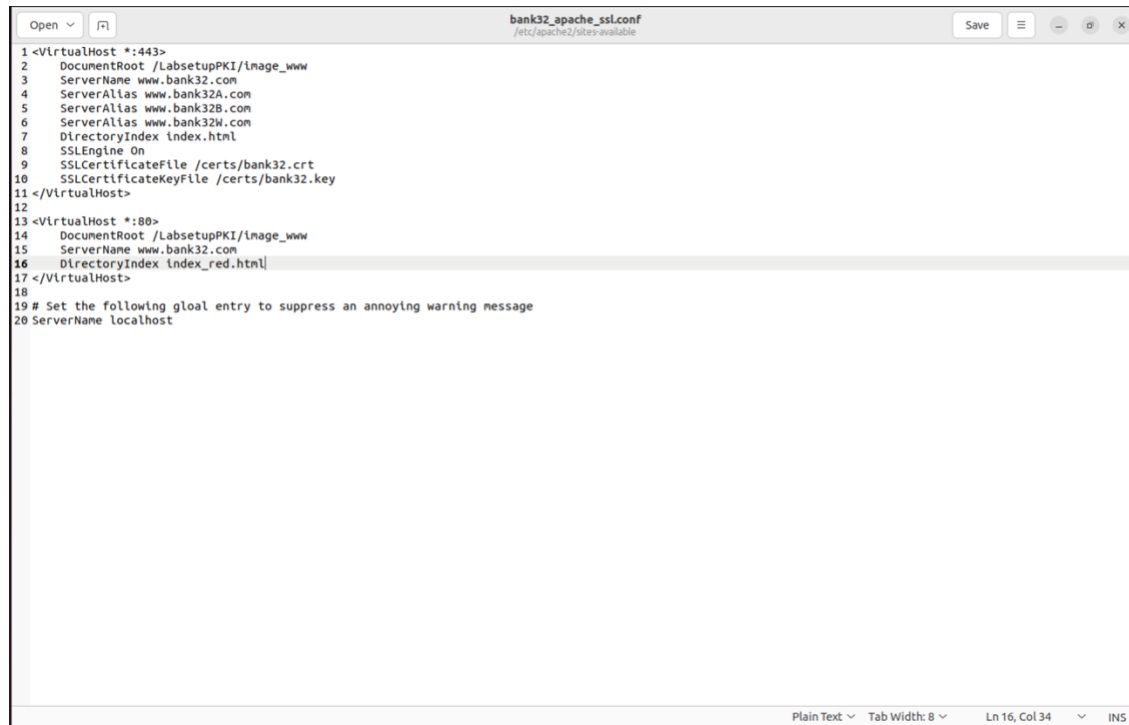
Screenshots: Task 4

Screenshot24: ([Return to text](#))

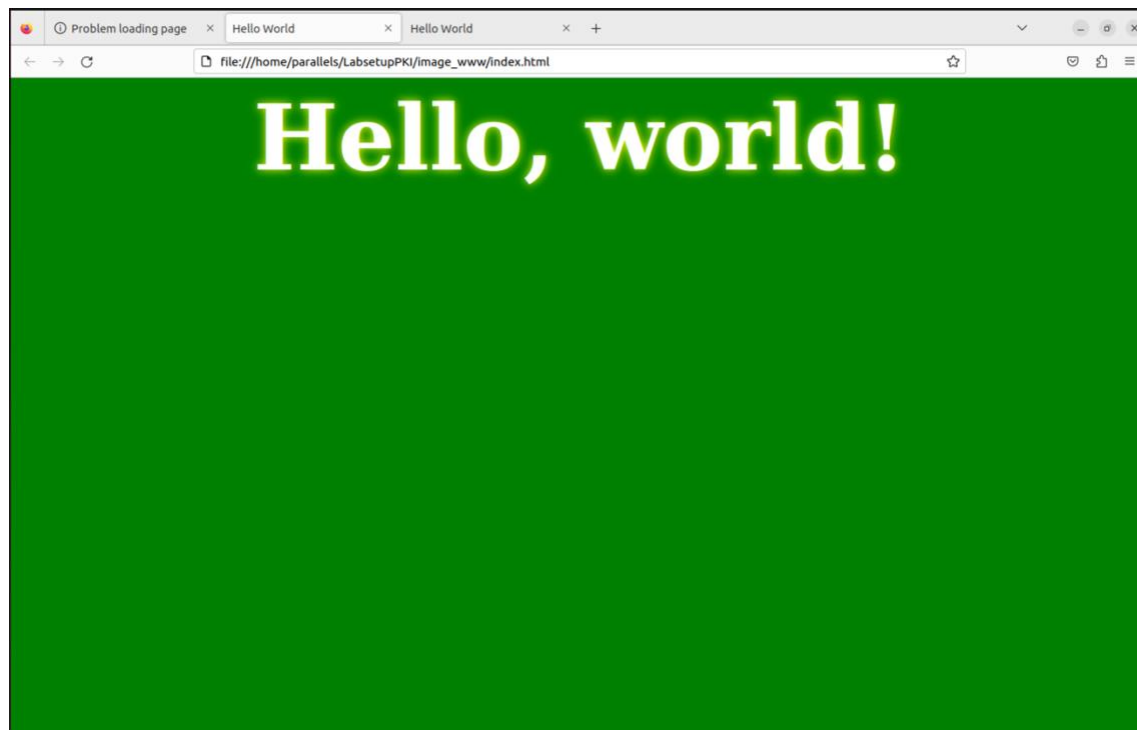


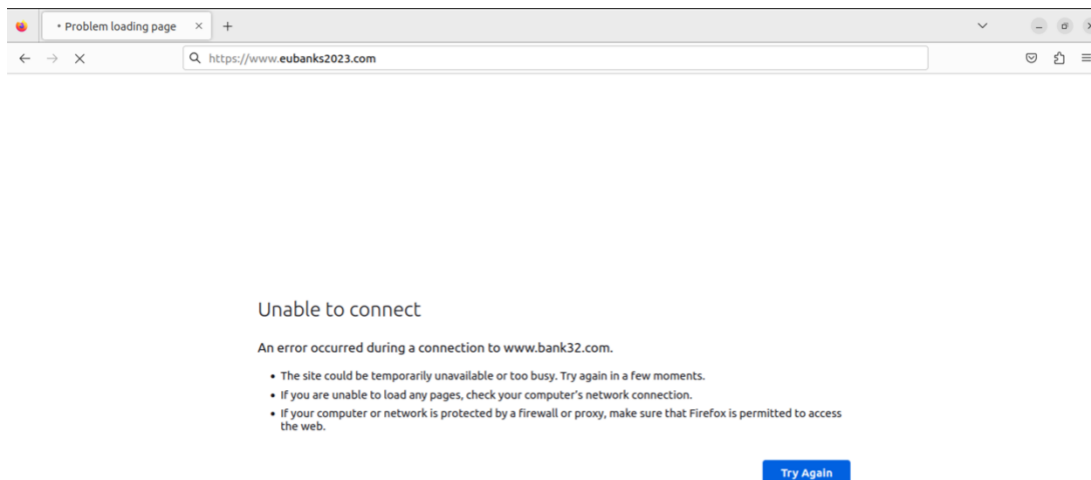
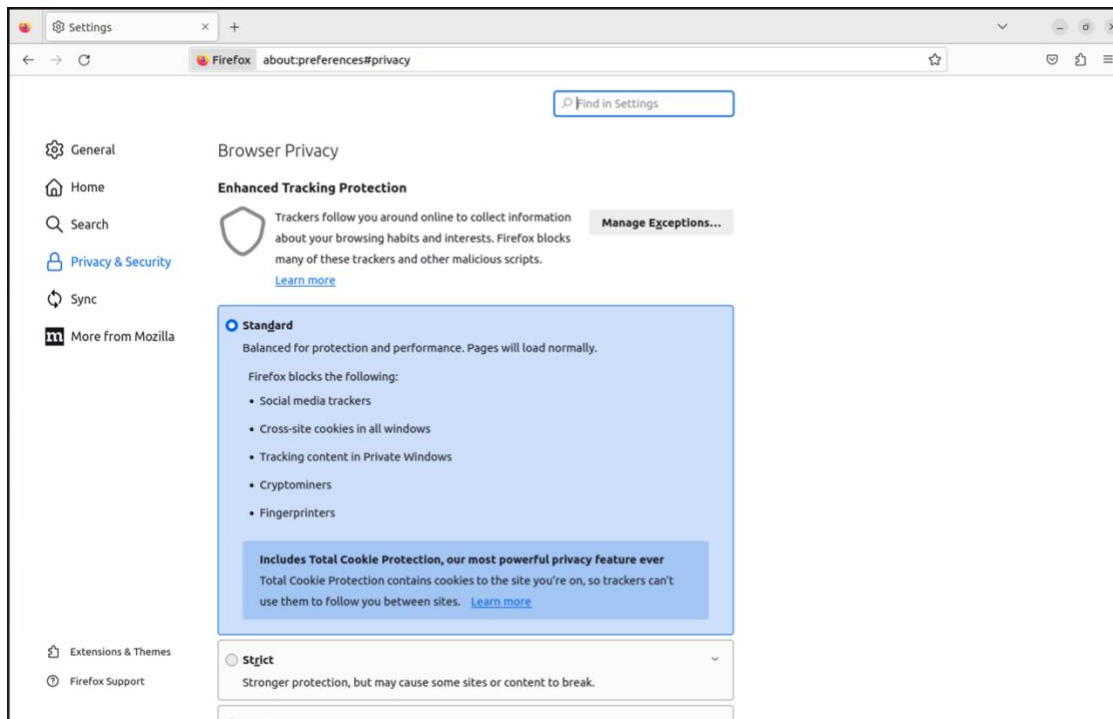
Screenshot25: ([Return to text](#))



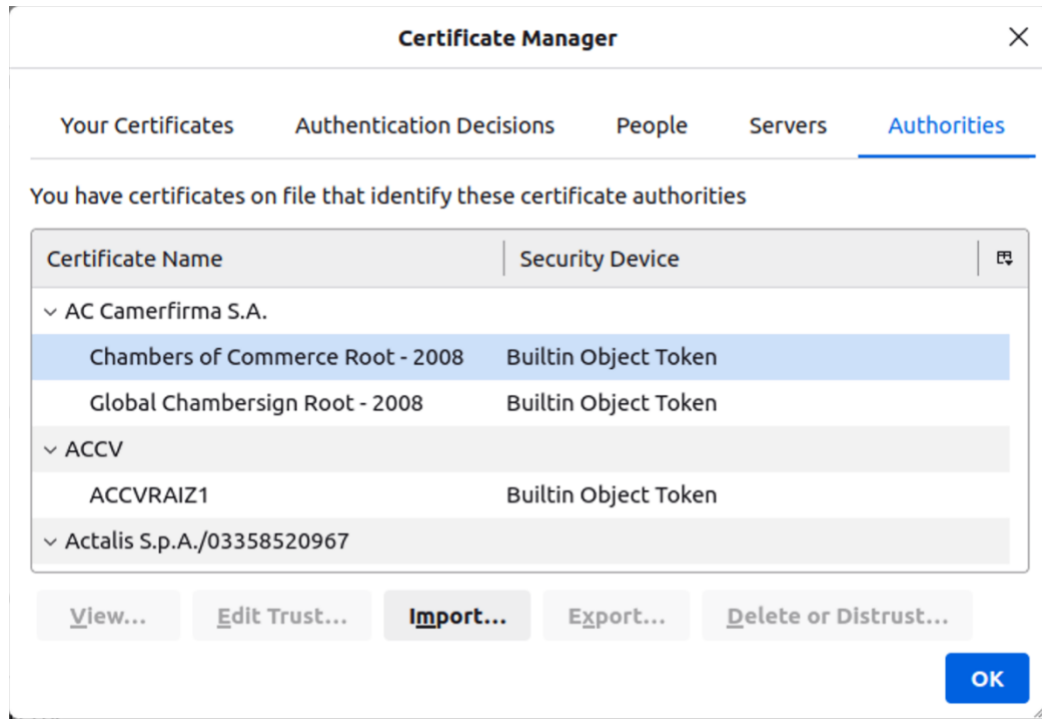
Screenshot26: ([Return to text](#))

```
1 <VirtualHost *:443>
2     DocumentRoot /LabsetupPKI/image_www
3     ServerName www.bank32.com
4     ServerAlias www.bank32A.com
5     ServerAlias www.bank32B.com
6     ServerAlias www.bank32M.com
7     DirectoryIndex index.html
8     SSLEngine On
9     SSLCertificateFile /certs/bank32.crt
10    SSLCertificateKeyFile /certs/bank32.key
11 </VirtualHost>
12
13 <VirtualHost *:80>
14     DocumentRoot /LabsetupPKI/image_www
15     ServerName www.bank32.com
16     DirectoryIndex index_red.html
17 </VirtualHost>
18
19 # Set the following gloal entry to suppress an annoying warning message
20 ServerName localhost
```

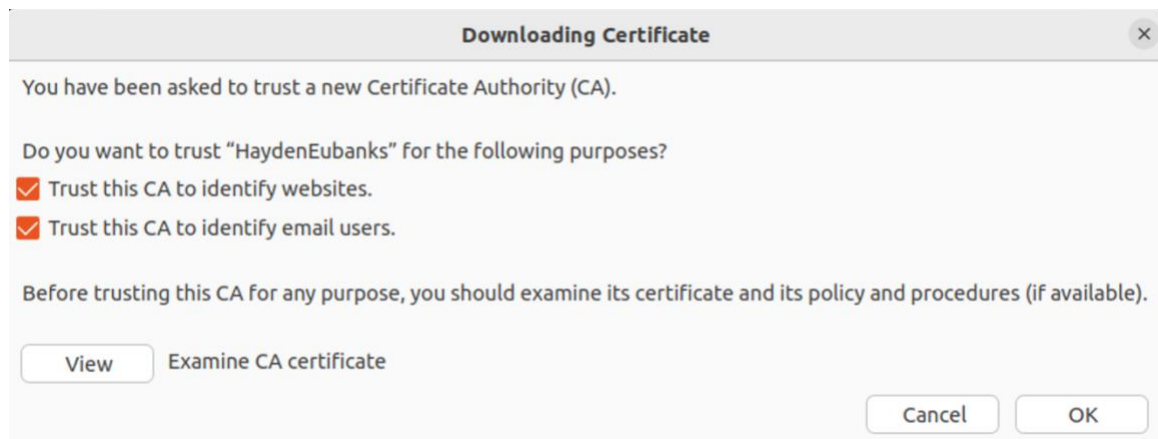
Screenshot27: ([Return to text](#))

Screenshot28: ([Return to text](#))Screenshot29: ([Return to text](#))

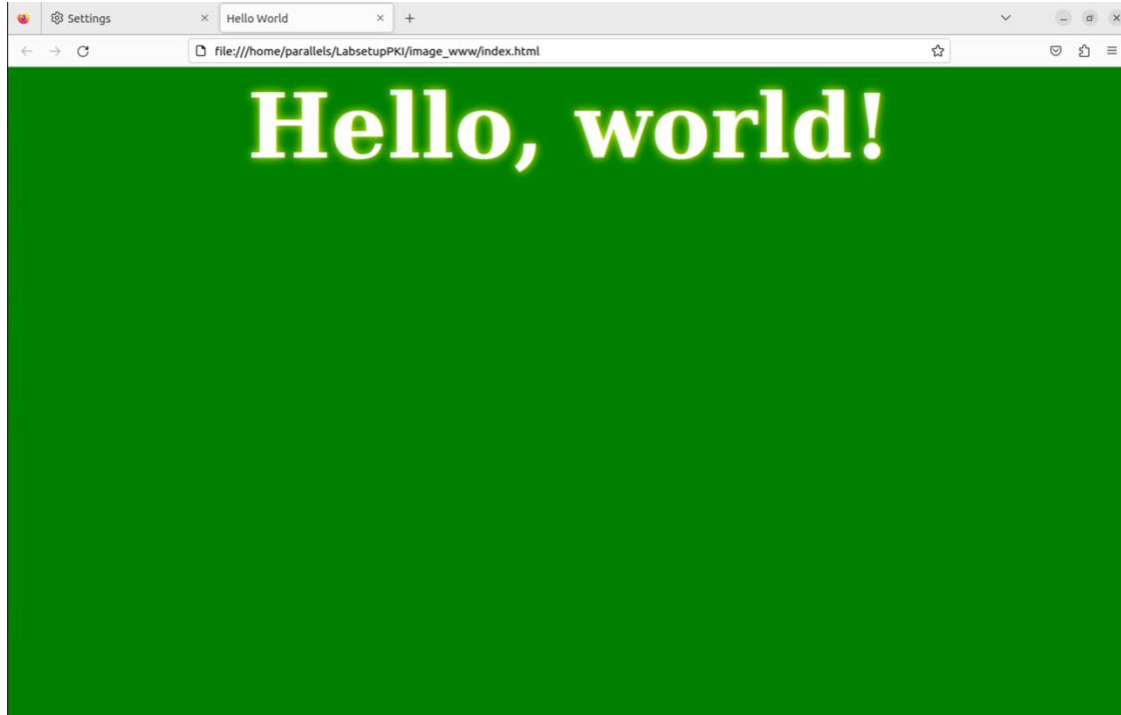
Screenshot30: ([Return to text](#))



Screenshot31: ([Return to text](#))




Screenshot32: ([Return to text](#))



Screenshots: Task 5

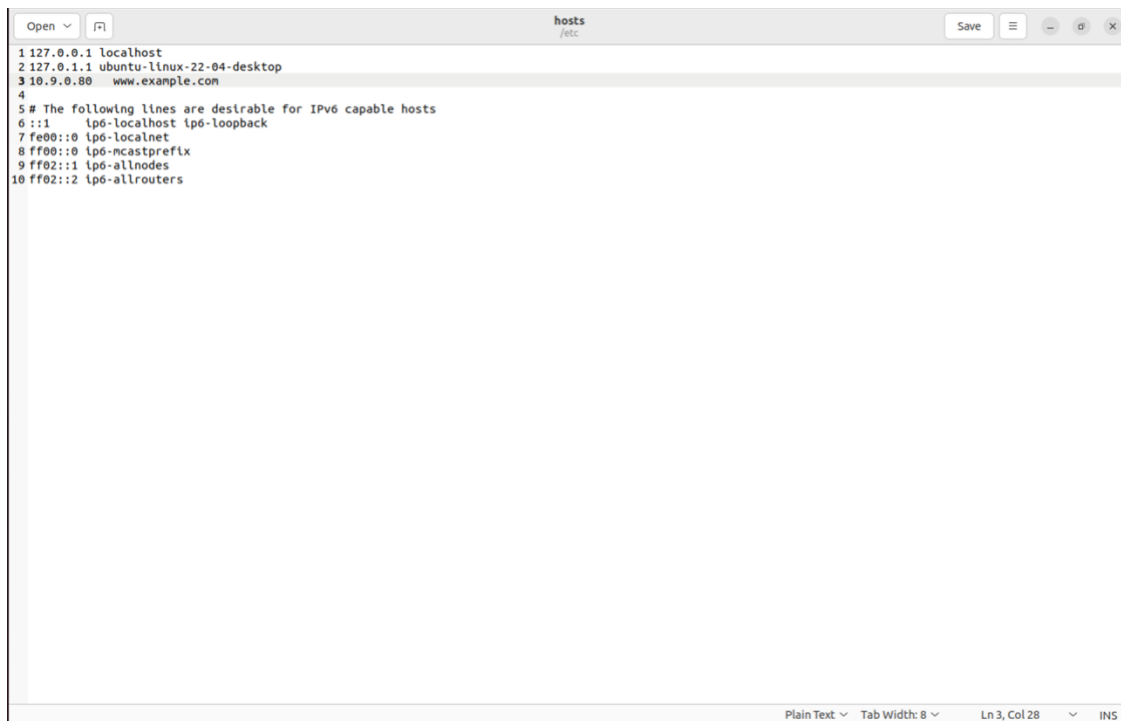
Screenshot33: ([Return to text](#))



```
1 <VirtualHost *:443>
2     DocumentRoot /LabsetupPKI/image_www/index.html
3     ServerName www.example.com
4     ServerAlias www.exampleA.com
5     ServerAlias www.exampleB.com
6     DirectoryIndex index.html
7     SSLEngine On
8     SSLCertificateFile /LabsetupPKI/image_www/certs/bank32.crt
9     SSLCertificateKeyFile /LabsetupPKI/image_www/certs/bank32.key
10 </VirtualHost>
11
12 <VirtualHost *:80>
13     DocumentRoot /LabsetupPKI/image_www
14     ServerName www.bank32.com
15     DirectoryIndex index_red.html
16 </VirtualHost>
17
18 # Set the following gloal entry to suppress an annoying warning message
19 ServerName localhost
```

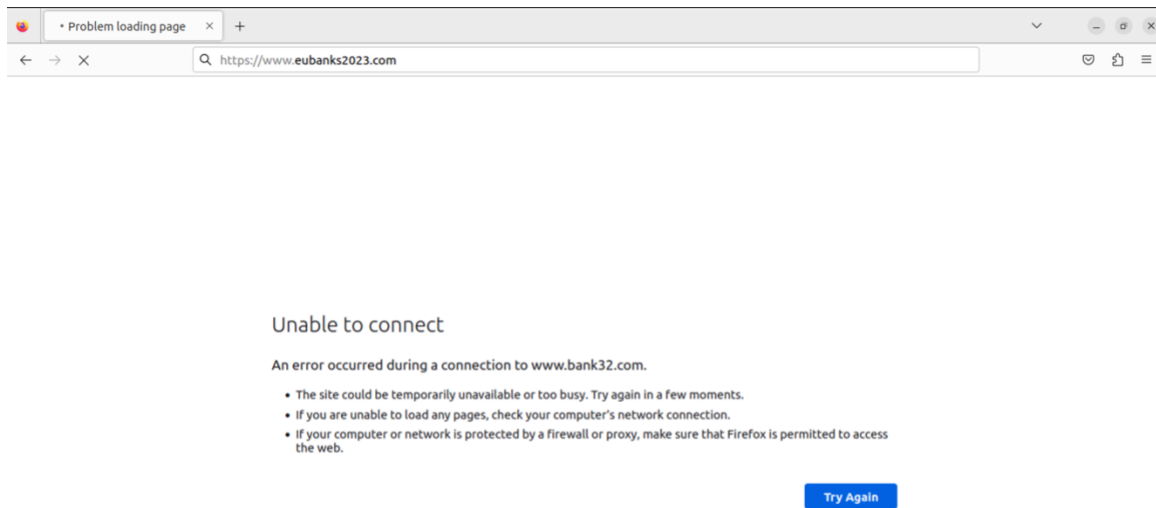
Plain Text ▾ Tab Width: 8 ▾ Ln 5, Col 33 ▾ INS

Screenshot34: ([Return to text](#))



```
1 127.0.0.1 localhost
2 127.0.1.1 ubuntu-linux-22-04-desktop
3 10.9.0.80 www.example.com
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1   ip6-localhost ip6-loopback
7 fe00::0 ip6-localnet
8 ff00::0 ip6-mcastprefix
9 ff02::1 ip6-allnodes
10 ff02::2 ip6-allrouters
```

Plain Text ▾ Tab Width: 8 ▾ Ln 3, Col 28 ▾ INS

Screenshot35: [\(Return to text\)](#)

Screenshot37: ([Return to text](#))

```
bank32_apache_ssl.conf
/etc/apache2/sites-enabled

1 <VirtualHost *:443>
2     DocumentRoot /LabsetupPKI/image_www/index.html
3     ServerName www.google.com
4     DirectoryIndex index.html
5     SSLEngine On
6     SSLCertificateFile /LabsetupPKI/image_www/certs/server.crt
7     SSLCertificateKeyFile /LabsetupPKI/image_www/certs/server.key
8 </VirtualHost>
9
10 <VirtualHost *:80>
11     DocumentRoot /LabsetupPKI/image_www
12     ServerName www.google.com
13     DirectoryIndex index_red.html
14 </VirtualHost>
15
16 # Set the following gloal entry to suppress an annoying warning message
17 ServerName localhost
```

Screenshot38: ([Return to text](#))

