Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

Creación de un certificado autofirmado (sólo para proveer Confidencialidad)

1. Generar la clave privada (Private Key)del servidor, que será almacenada en el archivo server.key.openssl genrsa out server.key 4096

Se procede a crear la clave privada:

```
root@debian2:/home/victoriamedina# openssl genrsa -out server.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................
......++
.................................................++
e is 65537 (0x10001)
```

2. Generar la solicitud de firma de certificado Certificate Signing Request), que será almacenada en el archivo server.csr. Completar los campos solicitados según el formulario de solicitud.

Se genera la solicitud de firma del certificado:

```
root@debian2:/home/victoriamedina# openssl req -new -sha256 -key server.key -out
server.csr
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]:AR
State or Province Name (full name) [Some-State]:Buenos Aires
Locality Name (eg, city) []:Lujan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizacion Example
S.A
Organizational Unit Name (eg, section) []:Gerencia de Sistemas
Common Name (e.g. server FQDN or YOUR name) []:10.0.3.15
Email Address []:medina.vicc@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:makelove
An optional company name []:victoria S.A
```

3. Firmar la petición con la propia clave privada como sigue. En este caso se lo denomina “auto-firmar”, puesto que estamos firmando la clave pública con la misma clave privada que le corresponde. En los sitios web que operan con TLS, quien firma la petición es una tercera entidad en la que “todos” confían.

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
root@debian2:/home/victoriamedina# openssl x509 -req -days 365 -sha256 -in
server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
Getting Private key
```

4. Para visualizar el certificado digital:

```
root@debian2:/home/victoriamedina# openssl x509 -text -in server.crt
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            f9:c4:3c:38:e1:5c:d1:b9
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AR, ST=Buenos Aires, L=Lujan, O=Organizacion Example S.A,
OU=Gerencia de Sistemas, CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
        Validity
            Not Before: Nov 12 20:13:25 2016 GMT
            Not After : Nov 12 20:13:25 2017 GMT
        Subject: C=AR, ST=Buenos Aires, L=Lujan, O=Organizacion Example S.A,
OU=Gerencia de Sistemas, CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:e9:3f:bb:a1:c0:f1:42:b0:50:a7:8d:0d:a1:a8:
                    48:c6:28:09:47:ae:62:65:91:a0:21:7b:19:5e:0f:
                    3b:2a:ee:d6:77:3e:87:59:66:60:8c:a1:85:f5:3a:
                    a2:66:a1:16:fa:2c:42:a8:01:45:7a:46:be:8c:7c:
                    c3:c4:60:b8:ac:78:7c:a4:f7:45:6d:6e:d3:b4:ae:
                    dc:23:72:4f:13:ae:b1:1a:dd:be:c5:00:6c:dd:c7:
                    63:03:62:00:93:99:8a:00:63:e8:f5:54:7e:4f:be:
                    72:f4:18:ff:53:7a:4f:b9:40:e8:1f:97:40:f5:87:
                    e0:22:80:a0:05:6a:0a:7b:5f:83:b0:44:c6:9d:6e:
                    4e:e6:8c:44:d6:7b:8e:22:7e:f0:44:5d:b8:bd:0c:
                    5a:af:7d:4a:38:58:08:a8:cc:35:62:35:6b:55:95:
                    7d:e3:06:f2:6c:51:8f:82:c4:76:61:f1:8b:90:1a:
                    00:62:5d:80:81:6a:cc:33:d5:cb:7d:6e:ab:15:ad:
                    3f:a1:78:db:77:9f:f0:c5:b1:8d:b5:f5:cd:d9:79:
                    58:52:69:55:d0:4c:c0:41:f7:38:30:89:1c:90:33:
                    09:20:6d:cf:0e:a8:b3:a2:1d:7a:f9:a4:35:3e:e5:
                    6f:a6:31:70:c9:97:df:b1:f9:15:d3:82:be:c0:66:
                    e9:1c:0c:a2:87:36:e9:5d:35:6c:85:2f:0b:bb:c0:
                    a5:8f:e5:af:1a:00:10:4d:9f:0a:2c:78:68:41:f4:
                    2d:00:3c:f6:dc:ad:1d:c9:40:f5:ed:da:44:8d:e6:
                    48:15:30:e2:85:dc:53:68:b1:e1:f5:06:b3:2e:d0:
                    33:43:6a:6c:bb:65:03:5a:a3:4d:51:6e:55:a4:0d:
                    02:05:58:8f:2c:26:d9:bd:ea:77:3f:90:f0:80:7d:
                    88:c3:24:6c:ab:83:ed:a0:21:e6:fe:8c:55:1e:91:
                    05:e4:44:1c:e3:e8:96:ed:f9:0b:8f:17:7c:94:0e:
                    dc:40:96:49:79:e7:4f:47:b0:7c:cc:80:04:7b:34:
                    7a:f6:25:ea:f7:92:3b:ae:52:bc:51:1c:95:c6:40:
                    dc:68:91:08:3c:7c:72:72:90:09:ca:49:16:a1:ba:
```

Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
                    e9:86:6a:ff:05:88:68:fb:5c:14:37:ea:51:e9:05:
                    f0:94:9a:64:3e:ef:cd:6c:43:3d:24:96:27:0e:79:
                    d3:a7:5a:46:59:05:30:31:26:38:94:8b:67:b4:3a:
                    b6:09:4a:4a:eb:c1:ec:c0:70:78:70:47:58:81:0f:
                    6b:ad:68:17:83:81:3d:df:22:f8:f7:94:c3:12:71:
                    de:b9:2a:77:9b:1c:6c:09:b7:74:e6:41:e3:f0:36:
                    19:d5:3d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         55:97:56:85:2f:8e:6b:01:b7:2a:fb:ba:b7:99:93:7b:f2:6c:
         57:f9:22:1c:b9:c3:37:4d:a3:d1:34:45:0b:95:2a:e2:57:d9:
         a5:51:c8:17:60:1a:d2:26:08:34:a1:95:8e:0b:1b:4a:a6:c3:
         87:0c:79:d7:21:e4:53:0f:8b:f3:5d:88:4c:28:3a:20:6a:de:
         b8:26:34:fb:66:bb:ce:15:96:cd:99:ea:8a:56:45:e7:5b:5a:
         da:ca:f1:2f:52:2d:10:59:fb:2b:b4:bb:a2:37:c9:f3:b7:a5:
         d8:34:d8:6d:db:1c:4d:e6:a0:35:9a:1f:36:a4:b9:82:03:e0:
         37:cd:9f:d4:d8:c9:c5:99:d3:3a:be:49:dd:8f:bd:76:f8:4b:
         8a:cf:d7:db:1e:42:bf:50:81:ce:29:b7:8d:41:b1:b2:e1:ab:
         85:49:02:f0:29:de:4f:68:f4:16:51:99:25:12:ef:9e:a1:fa:
         1b:55:41:5b:b5:d1:57:2e:ae:64:1b:1f:70:a6:58:0b:54:d5:
         e0:93:c1:44:2b:04:94:4e:28:56:ac:07:dc:28:fb:d1:9b:a8:
         7e:20:57:02:36:7d:3d:01:67:b8:b3:d3:29:bb:65:14:64:81:
         18:0f:97:30:56:65:c6:18:5c:0f:48:31:ee:57:ce:29:3d:de:
         25:f6:49:8a:aa:f4:1b:3c:8c:2c:2b:08:a8:36:25:7e:9e:03:
         b3:9a:00:e9:33:b1:b2:d4:c2:98:88:01:b2:14:be:f5:91:45:
         49:a9:19:bc:8a:bc:c2:95:29:cc:9f:75:e5:92:28:d2:17:ae:
         47:20:3c:f8:b8:d4:14:7f:26:0d:55:7a:93:65:80:fc:2c:4f:
         fa:e2:2d:53:d8:55:29:5e:c9:51:41:10:d8:3a:e9:dd:f2:91:
         6a:a3:06:5f:02:dd:b5:e4:85:72:54:20:05:70:df:7d:b5:7f:
         4c:65:27:ec:b6:91:65:c2:5a:ba:94:8a:c0:4e:17:53:63:cb:
         e1:18:a9:49:1b:6c:b0:e7:b9:0e:42:4d:c2:54:a1:ef:14:61:
         da:69:ea:8c:ad:b3:57:5e:60:a8:8c:05:6c:c3:79:89:36:ca:
         f6:bb:07:0e:eb:6e:d2:96:54:33:fe:13:06:36:a7:6d:71:56:
         1a:01:5b:9b:55:2c:ac:58:e2:e6:11:1d:c9:a5:49:ad:a4:3a:
         c8:7d:d3:9d:a3:44:99:d8:a4:ed:dd:c7:d3:d9:ce:22:ad:12:
         ea:94:45:d7:4c:b4:65:78:d1:cc:93:87:42:55:d9:72:c2:59:
         32:f0:88:01:77:5b:7b:d1:76:d8:91:d8:46:a2:85:45:ec:b1:
         b4:dc:7d:23:26:60:4d:f9
-----BEGIN CERTIFICATE-----
MIIF3jCCA8YCCQD5xDw44VzRuTANBgkqhkiG9w0BAQsFADCBsDELMAkGA1UEBhMC
QVIxFTATBgNVBAgMDEJ1ZW5vcyBBaXJlczEOMAwGA1UEBwwFTHVqYW4xITAfBgNV
BAoMGE9yZ2FuaXphY2lvbiBFeGFtcGxlIFMuQTEdMBsGA1UECwwUR2VyZW5jaWEg
ZGUgU2lzdGVtYXMxEjAQBgNVBAMMCTEwLjAuMy4xNTEkMCIGCSqGSIb3DQEJARYV
bWVkaW5hLnZpY2NAZ21haWwuY29tMB4XDTE2MTExMjIwMTMyNVoXDTE3MTExMjIw
MTMyNVowgbAxCzAJBgNVBAYTAkFSMRUwEwYDVQQIDAxCdWVub3MgQWlyZXMxDjAM
BgNVBAcMBUx1amFuMSEwHwYDVQQKDBhPcmdhbml6YWNpb24gRXhhbXBsZSBTLkEx
HTAbBgNVBAsMFEdlcmVuY2lhIGRlIFNpc3RlbWFzMRIwEAYDVQQDDAkxMC4wLjMu
MTUxJDAiBgkqhkiG9w0BCQEWFW1lZGluYS52aWNjQGdtYWlsLmNvbTCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAOk/u6HA8UKwUKeNDaGoSMYoCUeuYmWR
oCF7GV4POyru1nc+hllmYIyhhfU6omahFvosQqgBRXpGvox8w8RguKx4fKT3RW1u
07Su3CNyTxOusRrdvsUAbN3HYwNiAJOZigBj6PVUfk++cvQY/1N6T7lA6B+XQPWH
4CKAoAVqCntfg7BExp1uTuaMRNZ7jiJ+8ERduL0MWq99SjhYCKjMNWI1a1WVfeMG
8mxRj4LEdmHxi5AaAGJdgIFqzDPVy31uqxWtP6F423ef8MWxjbX1zdl5WFJpVdBM
wEH3ODCJHJAzCSBtzw6os6IdevmkNT7lb6YxcMmX37H5FdOCvsBm6RwMooc26V01
bIUvC7vApY/lrxoAEE2fCix4aEH0LQA89tytHclA9e3aRI3mSBUw4oXcU2ix4fUG
sy7QM0NqbLtlA1qjTVFuVaQNAgVYjywm2b3qdz+Q8IB9iMMkbKuD7aAh5v6MVR6R
```

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
BeREHOPolu35C48XfJQO3ECWSXnnT0ewfMyABHs0evYl6veSO65SvFEclcZA3GiR
CDx8cnKQCcpJFqG66YZq/wWIaPtcFDfqUekF8JSaZD7vzWxDPSSWJw5506daRlkF
MDEmOJSLZ7Q6tglKSuvB7MBweHBHWIEPa61oF4OBPd8i+PeUwxJx3rkqd5scbAm3
dOZB4/A2GdU9AgMBAAEwDQYJKoZIhvcNAQELBQADggIBAFWXVoUvjmsBtyr7ureZ
k3vybFf5Ihy5wzdNo9E0RQuVKuJX2aVRyBdgGtImCDShlY4LG0qmw4cMedch5FMP
i/NdiEwoOiBq3rgmNPtmu84Vls2Z6opWRedbWtrK8S9SLRBZ+yu0u6I3yfO3pdg0
2G3bHE3moDWaHzakuYID4DfNn9TYycWZ0zq+Sd2PvXb4S4rP19seQr9Qgc4pt41B
sbLhq4VJAvAp3k9o9BZRmSUS756h+htVQVu10VcurmQbH3CmWAtU1eCTwUQrBJRO
KFasB9wo+9GbqH4gVwI2fT0BZ7iz0ym7ZRRkgRgPlzBWZcYYXA9IMe5Xzik93iX2
SYqq9Bs8jCwrCKg2JX6eA7OaAOkzsbLUwpiIAbIUvvWRRUmpGbyKvMKVKcyfdeWS
KNIXrkcgPPi41BR/Jg1VepNlgPwsT/riLVPYVSleyVFBENg66d3ykWqjBl8C3bXk
hXJUIAVw3321f0xlJ+y2kWXCWrqUisBOF1Njy+EYqUkbbLDnuQ5CTcJUoe8UYdpp
6oyts1deYKiMBWzDeYk2yva7Bw7rbtKWVDP+EwY2p21xVhoBW5tVLKxY4uYRHcml
Sa2kOsh9052jRJnYpO3dx9PZziKtEuqURddMtGV40cyTh0JV2XLCWTLwiAF3W3vR
dtiR2EaihUXssbTcfSMmYE35
-----END CERTIFICATE-----
```

Pasos a seguir para configurar e instalar los certificados en el servidor web

2. Activar los módulos rewrite y ssl, y el sitio default-ssl en Apache.

a2enmod rewrite
a2enmod ssl
a2ensite defaultssl

```
root@debian2:/home/victoriamedina# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  service apache2 restart

root@debian2:/home/victoriamedina# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart

root@debian2:/home/victoriamedina# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
```

3. Crear la ubicación /etc/apache2/certificados donde se almacenarán los certificados, copiarlos a la misma y asignar los permisos adecuados según la documentación disponible en /usr/share/doc/apache2.2-common/README.Debian.gz:

mkdir /etc/apache2/certificados
cd /etc/apache2/certificados
mv origen/server.crt .

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

mv origen/server.key .
chown root.root server.crt server.key
chmod 444 server.crt
chmod 400 server.key

Creamos el directorio:

```
root@debian2:/home/victoriamedina# mkdir /etc/apache2/certificados
```

Accedemos a el:

```
root@debian2:/home/victoriamedina# cd /etc/apache2/certificados
```

Movemos el archivo server.crt a la carperta donde nos posicionamos:

```
root@debian2:/etc/apache2/certificados# mv /home/victoriamedina/server.crt .
```

Verificamos que se haya movido correctamente:

```
root@debian2:/etc/apache2/certificados# ls
server.crt
```

Cambiamos los permisos:

```
root@debian2:/etc/apache2/certificados# chown root.root server.crt server.key
root@debian2:/etc/apache2/certificados# chmod 444 server.crt
root@debian2:/etc/apache2/certificados# chmod 400 server.key
```

4. Editar el archivo /etc/apache2/sites-available/default-ssl e incorporar las líneas SSLCertificateFile y SSLCertificateKeyFile según sigue:

SSLCertificateFile /etc/apache2/certificados/server.crt
SSLCertificateKeyFile /etc/apache2/certificados/server.key

```
SSLCertificateFile      /etc/apache2/certificados/server.crt
SSLCertificateKeyFile /etc/apache2/certificados/server.key
```

Utilización de OpenSSL para diagnóstico

1. Utilice el comando openssl para ver el certificado creado en su servidor web. ¿Qué información pudo recabar?

Se muestra el certificado con los datos que se cargaron en el mismo.

```
root@debian2:/etc/apache2/certificados# openssl s_client -connect 10.0.3.15:443
-showcerts
CONNECTED(00000003)
depth=0 C = AR, ST = Buenos Aires, L = Lujan, O = Organizacion Example S.A, OU =
Gerencia de Sistemas, CN = 10.0.3.15, emailAddress = medina.vicc@gmail.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AR, ST = Buenos Aires, L = Lujan, O = Organizacion Example S.A, OU =
Gerencia de Sistemas, CN = 10.0.3.15, emailAddress = medina.vicc@gmail.com
verify return:1
---
```

Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
Certificate chain
 0 s:/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
   i:/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
-----BEGIN CERTIFICATE-----
MIIF3jCCA8YCCQD5xDw44VzRuTANBgkqhkiG9w0BAQsFADCBsDELMAkGA1UEBhMC
QVIxFTATBgNVBAgMDEJ1ZW5vcyBBaXJlczEOMAwGA1UEBwwFTHVqYW4xITAfBgNV
BAoMGE9yZ2FuaXphY2lvbiBFeGFtcGxlIFMuQTEdMBsGA1UECwwUR2VyZW5jaWEg
ZGUgU2lzdGVtYXMxEjAQBgNVBAMMCTEwLjAuMy4xNTEkMCIGCSqGSIb3DQEJARYV
bWVkaW5hLnZpY2NAZ21haWwuY29tMB4XDTE2MTExMjIwMTMyNVoXDTE3MTExMjIw
MTMyNVowgbAxCzAJBgNVBAYTAkFSMRUwEwYDVQQIDAxCdWVub3MgQWlyZXMxDjAM
BgNVBAcMBUx1amFuMSEwHwYDVQQKDBhPcmdhbml6YWNpb24gRXhhbXBsZSBTLkEx
HTAbBgNVBAsMFEdlcmVuY2lhIGRlIFNpc3RlbWFzMRIwEAYDVQQDDAkxMC4wLjMu
MTUxJDAiBgkqhkiG9w0BCQEWFW1lZGluYS52aWNjQGdtYWlsLmNvbTCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAOk/u6HA8UKwUKeNDaGoSMYoCUeuYmWR
oCF7GV4POyru1nc+h1lmYIyhhfU6omahFvosQqgBRXpGvox8w8RguKx4fKT3RW1u
07Su3CNyTxOusRrdvsUAbN3HYwNiAJOZigBj6PVUfk++cvQY/1N6T7lA6B+XQPWH
4CKAoAVqCntfg7BExp1uTuaMRNZ7jiJ+8ERduL0MWq99SjhYCKjMNWI1a1WVfeMG
8mxRj4LEdmHxi5AaAGJdgIFqzDPVy31uqxWtP6F423ef8MWxjbX1zdl5WFJpVdBM
wEH3ODCJHJAzCSBtzw6os6IdevmkNT7lb6YxcMmX37H5FdOCvsBm6RwMooc26V01
bIUvC7vApY/lrxoAEE2fCix4aEH0LQA89tytHclA9e3aRI3mSBUw4oXcU2ix4fUG
sy7QM0NqbLtlA1qjTVFuVaQNAgVYjywm2b3qdz+Q8IB9iMMkbKuD7aAh5v6MVR6R
BeREHOPolu35C48XfJQO3ECWSXnnT0ewfMyABHs0evYl6veSO65SvFEclcZA3GiR
CDx8cnKQCcpJFqG66YZq/wWIaPtcFDfqUekF8JSaZD7vzWxDPSSWJw5506daRlkF
MDEmOJSLZ7Q6tglKSuvB7MBweHBHWIEPa61oF4OBPd8i+PeUwxJx3rkqd5scbAm3
dOZB4/A2GdU9AgMBAAEwDQYJKoZIhvcNAQELBQADggIBAFWXVoUvjmsBtyr7ureZ
k3vybFf5Ihy5wzdNo9E0RQuVKuJX2aVRyBdgGtImCDShlY4LG0qmw4cMedch5FMP
i/NdiEwoOiBq3rgmNPtmu84Vls2Z6opWRedbWtrK8S9SLRBZ+yu0u6I3yfO3pdg0
2G3bHE3moDWaHzakuYID4DfNn9TYycWZ0zq+Sd2PvXb4S4rP19seQr9Qgc4pt41B
sbLhq4VJAvAp3k9o9BZRmSUS756h+htVQVu10VcurmQbH3CmWAtU1eCTwUQrBJRO
KFasB9wo+9GbqH4gVwI2fT0BZ7iz0ym7ZRRkgRgPlzBWZcYYXA9IMe5Xzik93iX2
SYqq9Bs8jCwrCKg2JX6eA7OaAOkzsbLUwpiIAbIUvvWRRUmpGbyKvMKVKcyfdeWS
KNIXrkcgPPi41BR/Jg1VepNlgPwsT/riLVPYVSleyVFBENg66d3ykWqjBl8C3bXk
hXJUIAVw3321f0xlJ+y2kWXCWrqUisBOF1Njy+EYqUkbbLDnuQ5CTcJUoe8UYdpp
6oyts1deYKiMBWzDeYk2yva7Bw7rbtKWVDP+EwY2p21xVhoBW5tVLKxY4uYRHcml
Sa2kOsh9052jRJnYpO3dx9PZziKtEuqURddMtGV40cyTh0JV2XLCWTLwiAF3W3vR
dtiR2EaihUXssbTcfSMmYE35
-----END CERTIFICATE-----
---
Server certificate
subject=/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
issuer=/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
---
No client certificate CA names sent
---
SSL handshake has read 2453 bytes and written 415 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
```

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 7730F93195F1FA3930162A7668ABDEE6C6DD93A556A141125D7545BF23CD4A75
    Session-ID-ctx:
    Master-Key:
D54700382232D47C99E1E1772150043399316F968A2AB610F4FF964C484438962A6F30678B508762
15CBF811BC3CD303
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 67 70 51 86 66 c9 ed 7e-87 c2 0d 1f 5c de e6 3f   gpQ.f..~....\..?
    0010 - 76 21 27 4f fc be 2a be-a2 7c bf 0d 1f 2e 26 7d   v!'O..*..|....&}
    0020 - 70 60 66 2a 99 43 58 48-a8 05 b1 cf 43 4f 16 67   p`f*.CXH....CO.g
    0030 - 58 6a 84 23 71 ec d5 52-85 79 fc fa 6e 92 7d 94   Xj.#q..R.y..n.}.
    0040 - a7 14 1a a0 cd e7 dc d9-85 9e af 15 32 90 e4 20   ............2..
    0050 - 4e 20 33 64 26 1c c3 30-47 14 72 36 02 1d b4 62   N 3d&..0G.r6...b
    0060 - 5c 6b fa 8a 0d ed 38 a0-db 29 a0 dd 32 d7 bb 35   \k....8..)..2..5
    0070 - 3a a9 f6 c8 5b 9e 6e 9b-9f fe dc 48 67 03 19 89   :...[.n....Hg...
    0080 - 70 4a a4 79 38 34 27 3d-bb b8 b6 cd 88 d0 50 d0   pJ.y84'=......P.
    0090 - f2 70 ea 77 5d f8 d3 5e-68 b6 18 9d 2f 1a 48 54   .p.w]..^h.../.HT
    00a0 - b1 b5 c8 73 a1 44 2d fa-b0 08 f8 da 0e 11 fd 5d   ...s.D-........]
    00b0 - 39 49 a7 4a 26 04 71 85-2e e3 97 f6 bc d9 52 c1   9I.J&.q.......R.

    Start Time: 1478986404
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
```

2. Verifique el certificado copiándolo a un archivo de texto. ¿Qué información pudo obtener? ¿Qué diferencias observa en la salida de este comando respecto de la misma petición realizada contra un servidor de Google (p.ej: www.google.com.ar:443) ?

Un certificado de Google, contiene información de quien fue expedido y para quien, un periodo de validez, la huella digital que se uso para firmarlo

Creación y utilización de una Autoridad de Certificación (CA)

1. Editar en el archivo de configuración de OpenSSL, ubicado en /etc/ssl/openssl.cnf. Modificar la entrada correspondiente al directorio donde se almacenarán las claves y los certificados (Sección [CA_default]):
dir = /root/sslCA

```
root@debian2:/etc/apache2/certificados# nano /etc/ssl/openssl.cnf
```

2. Crear los directorios necesarios:
cd /root
mkdir sslCA
chmod 700 sslCA
cd /root/sslCA
mkdir certs private newcerts

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
root@debian2:/etc/apache2/certificados# cd /root
root@debian2:~# mkdir sslCA
root@debian2:~# chmod 700 sslCA
root@debian2:~# cd /root/sslCA
root@debian2:~/sslCA# mkdir certs private newcerts
```

3. Crear un archivo ca.srl, el cual será utilizado para nombrar los nuevos certificados y un archivo index.txt:

```
# echo 1000 > ca.srl
# touch index.txt
```

```
root@debian2:~/sslCA# echo 1000 > ca.srl
root@debian2:~/sslCA# touch index.txt
```

4. Creación del Certificado de Autoridad:

```
root@debian2:~/sslCA# openssl req -new -x509 -days 365 -extensions v3_ca -keyout
private/ca.key -out ca.crt -config /etc/ssl/openssl.cnf
Generating a 2048 bit RSA private key
....+++
.....................................+++
writing new private key to 'private/ca.key'
Enter PEM pass phrase:
Verifying - Enter 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]:AR
State or Province Name (full name) [Some-State]:Buenos Aires
Locality Name (eg, city) []:Lujan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizacion Example
S.A
Organizational Unit Name (eg, section) []:Gerencia Sistemas
Common Name (e.g. server FQDN or YOUR name) []:victoria
Email Address []:medina.vicc@gmail.com
```

5. Completar los datos solicitados. Verificar que el Certificado y la Clave fueron efectivamente creados:

```
# more /root/sslCA/ca.crt
# more /root/sslCA/private/ca.key
```

```
root@debian2:~/sslCA# more /root/sslCA/ca.crt
-----BEGIN CERTIFICATE-----
MIIELTCCAxWgAwIBAgIJAKLlAFTzWm/VMA0GCSqGSIb3DQEBCwUAMIGsMQswCQYD
VQQGEwJBUjEVMBMGA1UECAwMQnVlbm9zIEFpcmVzMQ4wDAYDVQQHDAVMdWphbjEh
MB8GA1UECgwYT3JnYW5pemFjaW9uIEV4YW1wbGUgUy5BMRowGAYDVQQLDBFHZXJl
bmNpYSBTaXN0ZW1hczERMA8GA1UEAwwIdmljdG9yaWExJDAiBgkqhkiG9w0BCQEW
```

Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

FW1lZGluYS52aWNjQGdtYWlsLmNvbTAeFw0xNjExMTIyMjA1NTRaFw0xNzExMTIy
MjA1NTRaMIGsMQswCQYDVQQGEwJBUjEVMBMGA1UECAwMQnVlbm9zIEFpcmVzMQ4w
DAYDVQQHDAVMdWphbjEhMB8GA1UECgwYT3JnYW5pemFjaW9uIEV4YW1wbGUgUy5B
MRowGAYDVQQLDBFHZXJlbmNpYSBTaXN0ZW1hczERMA8GA1UEAwwIdmljdG9yaWEx
JDAiBgkqhkiG9w0BCQEWFW1lZGluYS52aWNjQGdtYWlsLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMv5PIGuphG/FHg+qUnQnOoFl3E/abCSCFtf
u5Vf1DXIb4u7YEkUvN1dnovIehDYYqdjqVAFT/61hCmymdfCM0vzq8K7+oQXdlL0
qc7Rbl+jYl9+7QHa0EmyxSn2gcePUBBZuDEIVsvQ9cuWkXv2jacZ+7gfc/j+Thpk
q235V125TdW/HZP4fs1FRJQvomnVN6FkXf6xzarUIdAAi5l+l4yDvoHTVRFlinXp
mOq6/8hHR9u2bwtTD0Gg+mCpo2aDSnYXF8h/GknkLL0pIgNG6kq1tQ5c63SCVBKE
jmI3/5hkjrbg4eUERW40mrAChTn+T6oM2FuiI+9FW/vEmuFQSk8CAwEAAaNQME4w
HQYDVR0OBBYEFKXU7jJSYW+N8nw/YLnOxdQ85XwzMB8GA1UdIwQYMBaAFKXU7jJS
YW+N8nw/YLnOxdQ85XwzMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
AMMsJwsO3aYicLSHTxl/erbOoVBGvLv8Dbn3j064rRHCqciTdl0xi+nmLglgiGM6
U+v9tO14AnAx7za51i2fP0JqGBeJGOo38aMqzmS6PxjKUVDu53xqosJP436KgdYs
6VyDV+z0dc21M+gEPKUK8433ZZbuhqGYFVWDsbYBV+ErLKzltFmC4/TVs7ZPK9Ri
VHgC8L0/YxQVuo/aGXCq3iPlSc1TbyPKdWakDWPaATstFJOEad0qlrk5kuqYC7z4
B62gkAdZPv7u1TT0UQT6ezEVDFdN0aKnFmx4rMOWn+TlH4oLw4JC7P4ig1GweSq/
vFXZQiLohjjgtlLNNg5Lo0w=
-----END CERTIFICATE-----

root@debian2:~/sslCA# more /root/sslCA/private/ca.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIIUi+gdnZVEkCAggA
MBQGCCqGSIb3DQMHBAi7RhAPtJgyNwSCBMiiozs0kiRyQiRVffTmzYnmqAWkKybJ
6y6r8Ov9L8ZsvwJKRW2x9KdDPgURHXWiwizPMsapLp4567QxWAgKPn06qQ7D3uja
8QVPZGZSQ2YtitppWAdcYqf2a9izlzrm2LHG8J+c5Lx1i66NCbUbHpqaHmqtw7vN
YfuixPIah0ePRyoymv174smAZc/Ad1fRluKxeUl3xQvNCXPM092FDdKk640Gv8S4
QN6OYYbLKXdtG81w4w6Je0dE88xS1eh4opuiU8x6J6hOQTWTQH5go3UZgmOLAIUs
soee2NkzrcZDXL33b2dIaSGrLqobFdAU5NhHONOL7iJBR95mzD2dCBHiEkuURePP
+nsandnIX3d+kAYvD2FO0OnKNjZOdH6S+cjmAl8/RW3oE29TLnBJXgbh5ZTsLG6N
oHz4XjNzK5V8erWxLz+beepkmEIXQlI3WXpsCpZSR9uiBlxrNBucEkdSuM3j1r6M
vziaHnEkj0mqAwy2QM0AK2C3HQPdSTMp+fj/f7oOUbCROrWQODlzjhyblPSovqXJ
Y1MFzuyiVXZKUPGlTavw+IbpTdhL2y+f0r6+NsA69JaAVYVYHUaMGNuhqhypnMgN
BnDQuVukVYsMJ7VthjJwrOi0R3LpYvbhglmDQnr/To2DVXxErYAxBmwwrQAXyvXI
CkO4jzVekw86AtOA8IfTS8l00UeUhIOAsxl1IhluajZmnGJvDSmc0ukjyiCmTGOM
BpfKjubuzOiJS3/gddYvVC7+TXx7i7tkPhWRq5CcvFBocAxaH+OtAy9BB35sfqrO
J7dMWAqld8UaiID90SVv8+ex9qdoF/LncFB3P/wt7Bja/VQamJqMsh4MSW9Sy7La
eSzZjwnNjtLK/pZI49+sW3BzJtM7eeyERMrqjxpjE3XoJllMPevcq5XQTgcFKHXw
TylhTtUvSMR8qOgXnOTzB0PqqxyW7bBdAAqEvhbRSu1lYnRRa+Jt5gAR6XqP+0Gu
kI3foGKfJfKGr97pcYfj1J/+MUJsvYd3cbYzAwwA/PH8nJxL2c+m1oVTQ9Xr5xq8
B2D55Z6k00n+ozWd3xnaSRiMB4oityrIXRTVpq5KrOkSeJ2RdIaVTKG6dv+miTbY
kcMSiZ8V5ItRtPqQ9kIEpWWP96pf6Eo78cranw0EfAbX1tmQFaTAIROOF4b6vtUu
TbpC8aO+MTy2DkaQtc1vE/v9vHTuV9GFPF6XIh7LjXKoYwvQiKjvm192i3AWLORG
avS3FvOLXtQUlIMBw3/5wftDjZpZlQ7sjRTUpUxqSOCyoiZGpdEAaz3uBDDlgF39
uwTxTnQnViT85l23HpS/TCpjOroDfnlyH55+K2kOkpjcvIpqtp7xadp81a5IfTTw
kxjYlUMrnVDOT2eQ93EO72/q+7XcM7oUNG2aew9KFiCozfpp316CgOrscik3eFqC
cKJoCnh6mQb/x4hBykiLqIdbIrNKoWV3QB0zt7tHcO2wUEiT0lsJetFm98oY8fEz
a7/4UNDtDc1rmCEyyLMs3Q/ZP9M2gE78GWeoxBIJ4UU708hRr5ivTyDPE3J81BwA
lNrq9sXFBKj+B1L1MsvDEIse+aeateNCAI94LA4OQkVxg5d6YAdxFWZxwkZSB+88
MxY=
-----END ENCRYPTED PRIVATE KEY-----

6. Emplear la solicitud de firma de certificado creada anteriormente pero está vez firmarla empleando la CA recientemente definida, para ello:

Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

1. Crear el archivo config1.txtcon los siguientes datos:

```
basicConstraints = critical,CA:FALSE
extendedKeyUsage = serverAuth
```

2. Generar y firmar el certificado del servidor, que será almacenado en el archivo server-nuevo.crt

```
root@debian2:~/sslCA# openssl x509 -CA ca.crt -CAkey /root/sslCA/private/ca.key
-req -in /home/victoriamedina/server.csr -days 365 -extfile config1.txt -sha256
-CAserial ca.srl -out server-firmado.crt
Signature ok
subject=/C=AR/ST=Buenos Aires/L=Lujan/O=Organizacion Example S.A/OU=Gerencia de
Sistemas/CN=10.0.3.15/emailAddress=medina.vicc@gmail.com
Getting CA Private Key
Enter pass phrase for /root/sslCA/private/ca.key:
```

7. Pruebe ingresar mediante un navegador al Servidor Web en el cual fue instalado y configurado el certificado autofirmado. Luego, instale y configure el certificado generado en la consigna anterior y vuelva realizar la consulta. Finalmente agregue a su navegador la Autoridad de Certificación creada, y nuevamente ingrese al sitio desde el navegador. ¿Qué diferencias observa en cada caso? ¿A qué se debe?

Al ingresar al sitio sin la autoridad de certificación agregada al navegador, nos aparece el siguiente error:

Un error ocurrió durante una conexión a localhost porque usa un certificado de seguridad no válido.

El certificado no es confiable porque es auto firmado.
En cambio, al agregar al navegador la autoridad certificada este error ya no aparece, se accede directamente.

8. Realice una captura de petición de la página web principal del servidor mediante protocolo HTTP (puerto 80) y, luego, HTTPS (puerto 443).
    1. Analice la captura e identifique las distintas etapas del protocolo TLS

En la siguiente imagen se podrá observar el handshake entre el cliente y el servidor en las tramas #4 y #6

Para aportar un poco más de detalle, desde el lado del cliente podemos observar toda la información que es enviada para el comienzo de la negociación.

Trabajo Práctico #8

"OpenSSL - Certificados Digitales X.509"

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 160
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 156
      Version: TLS 1.2 (0x0303)
    ▸ Random
      Session ID Length: 0
      Cipher Suites Length: 22
    ▸ Cipher Suites (11 suites)
      Compression Methods Length: 1
    ▸ Compression Methods (1 method)
      Extensions Length: 93
    ▸ Extension: renegotiation_info
    ▸ Extension: elliptic_curves
    ▸ Extension: ec_point_formats
    ▸ Extension: SessionTicket TLS
    ▸ Extension: next_protocol_negotiation
    ▸ Extension: Application Layer Protocol Negotiation
    ▸ Extension: status_request
    ▸ Extension: signature_algorithms
```

Por el otro lado, desde el servidor, observamos la respuesta y su contenido:

```
▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 61
  ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 57
      Version: TLS 1.2 (0x0303)
    ▸ Random
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Method: null (0)
      Extensions Length: 17
    ▸ Extension: renegotiation_info
    ▸ Extension: ec_point_formats
    ▸ Extension: SessionTicket TLS
▸ TLSv1.2 Record Layer: Handshake Protocol: Certificate
▸ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
▸ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

El servidor envía un mensaje *ServerHelloDone*, lo que indica que terminó con la negociación del handshake.
En la trama #8 se detecta el comienzo del intercambio de claves.

2. Identifique las opciones intercambiadas respecto a Cipher Suite y Extensiones soportadas.

Trabajo Práctico #8

“OpenSSL - Certificados Digitales X.509”

Fecha de Entrega: 17/11/2016

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
Secure Sockets Layer
▾ TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 202
  ▾ Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 198
    ▸ TLS Session Ticket
▾ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
▾ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

3. Identifique la información del/los certificado/s provista y valídela contra lo generado en los pasos previos. Indique si el certificado es válido para el dominio/ip accedido y si aún es vigente.
4. Evalúe las diferencias entre las peticiones HTTP y HTTPS respecto a la confidencialidad del contenido