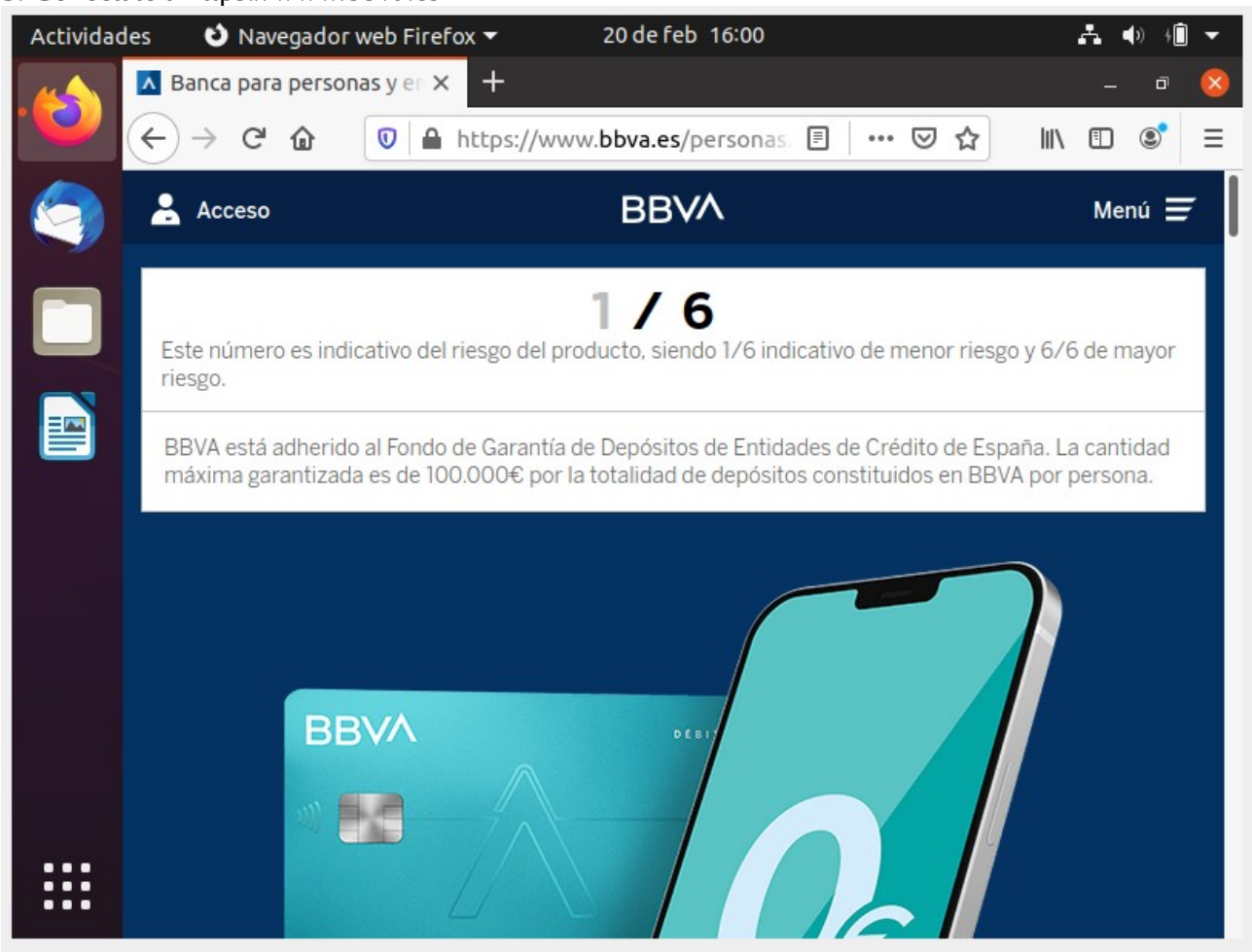
Certificado digital verificado

1. Inicia sesión en máquina cliente (Escritorio)

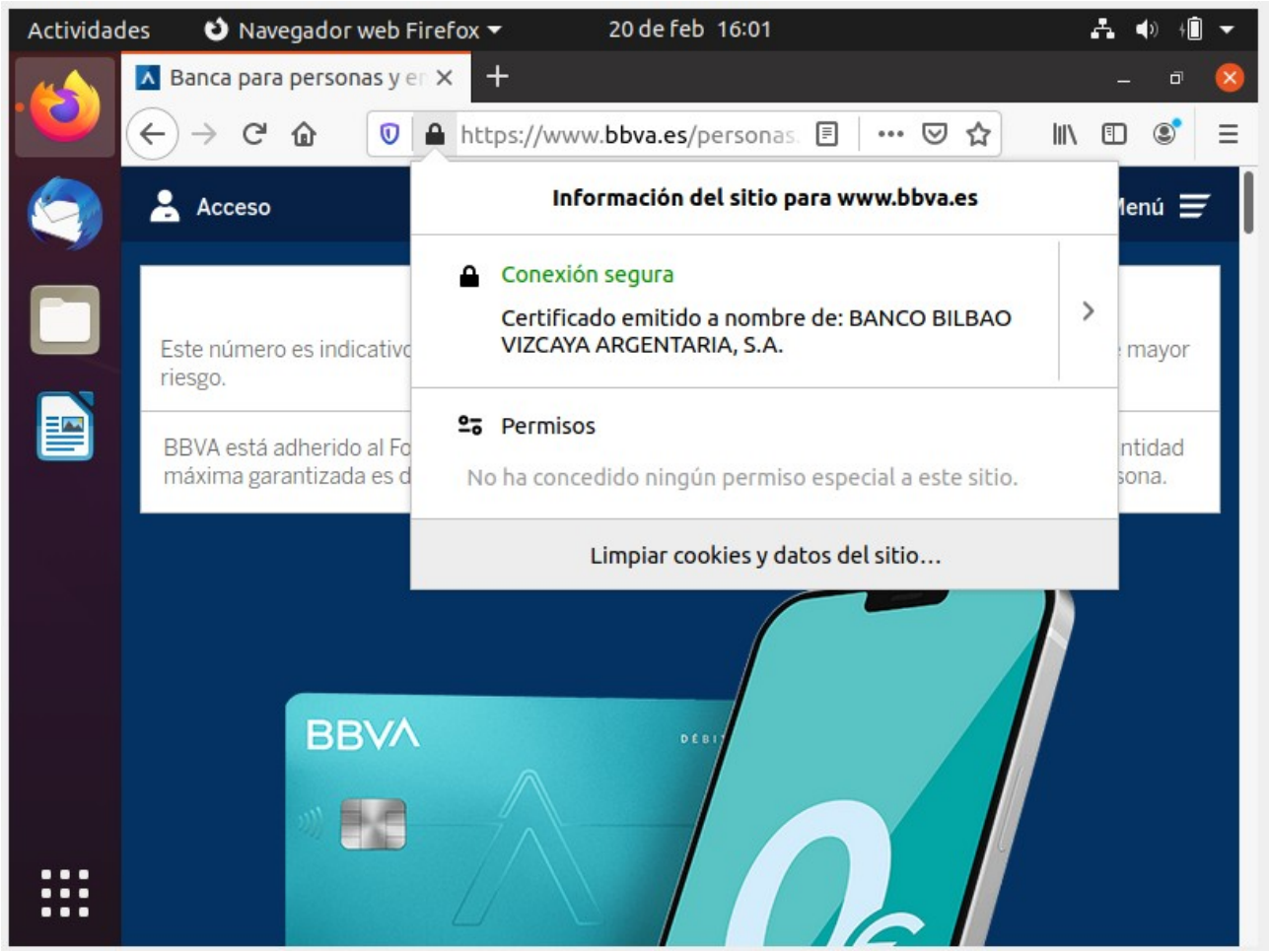
2. Inicia tu navegador.

3. Conéctate a https://www.bbva.es



4. Observa la URL que el protocolo usado es https.

5. Pincha en el candado



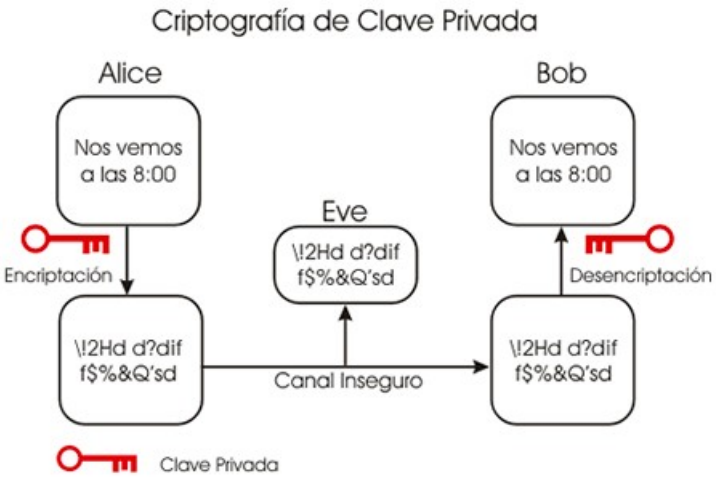
6. Pincha sobre Más información para consultar el certificado digital que ha enviado el servidor web y responde a las siguientes preguntas:

a. ¿Qué es una clave simétrica y una clave asimétrica?

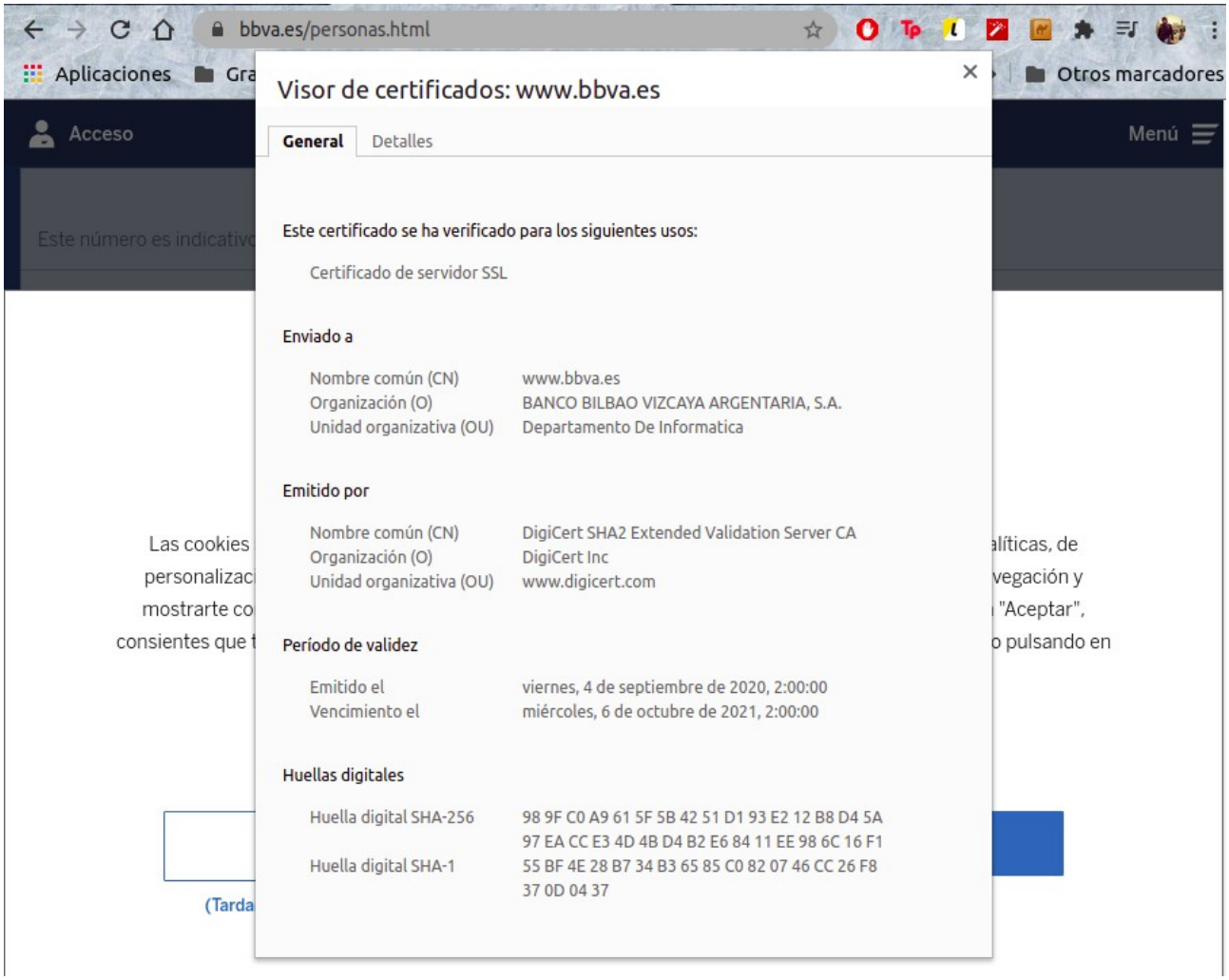
-Simétrica: Se utilizan en la misma llave para las funciones de encriptación y desencriptación.
-Asimétrica:Se emplean una clave para encriptar los datos y otra distinta para desencriptarlos.

b. ¿Qué algoritmo de clave simétrica se ha utilizado para cifrar la información que viaja por la red?
-Las claves suelen ir cifradas en una longitud de mas de 64 bits.

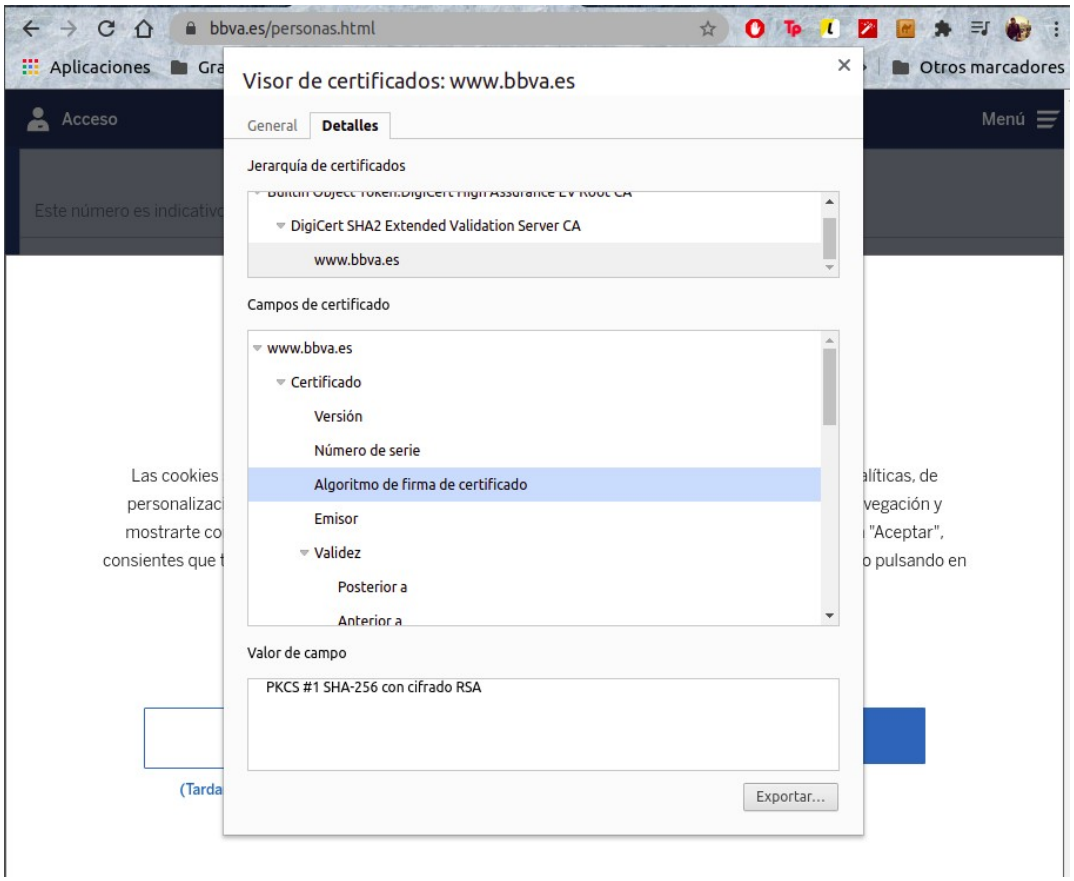
¿Cuál es la longitud de la clave utilizada? (Captura de pantalla)



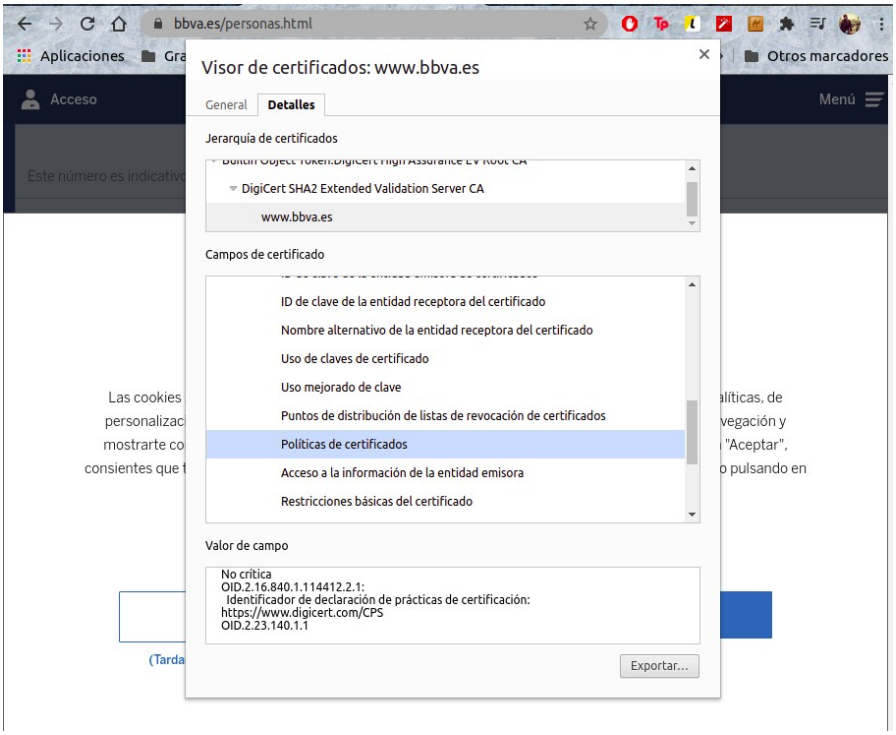
c. ¿Cuál es el período de validez del certificado? (Captura de pantalla)



d. ¿Qué algoritmo de clave asimétrica ha utilizado la autoridad de certificación para firmar el certificado? (Captura de pantalla)



e. Busca el certificado de la autoridad certificadora que ha firmado el certificado. (Captura de pantalla)



Certificado digital no verificado

1. Inicia tu navegador.

2. Conéctate a una url http://www.rmc.es u otra.

3. Observa que la página no es segura. ¿Por qué?

- Porque no tiene los certificados de seguridad , ni de codificación de claves incluida en su pagina. La privacidad del usuario puede estar en peligro.

Servidor virtual HTTPS por defecto en Linux

1. Iniciar sesión el Servidor Linux.

2. Habilita el servidor virtual por defecto de Apache.

```
enrique@enrique:~$ sudo a2ensite 000-default.conf
[sudo] password for enrique:
Site 000-default already enabled
enrique@enrique:~$
```

sudo a2ensite 000-default

3. Verifica que dentro del directorio /etc/apache2/sites-enabled se ha creado el enlace 000-default.conf.

```
enrique@enrique:~$ cd /etc/apache2/sites-enabled/
enrique@enrique:/etc/apache2/sites-enabled$ ls
000-default.conf
enrique@enrique:/etc/apache2/sites-enabled$
```

4. Reinicia el servidor para que los cambios tengan efecto.

```
enrique@enrique:/etc/apache2/sites-enabled$ sudo service apache2 restart
enrique@enrique:/etc/apache2/sites-enabled$
```

5. Habilita el módulo modssl que permita usar https

sudo a2enmod ssl

```
enrique@enrique:~$ sudo 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 certifica
tes.
To activate the new configuration, you need to run:
  systemctl restart apache2
enrique@enrique:~$
```

6. Reinicia el servidor para que los cambios tengan efecto.

```
enrique@enrique:~$ sudo systemctl restart apache2
enrique@enrique:~$
```

7. Consulta el fichero /etc/apache2/ports.conf y observa que si habilita el módulo ssl el servidor escuchará el puerto 443.

```
enrique@enrique:~$ cd /etc/apache2/
enrique@enrique:/etc/apache2$ ll
total 96
drwxr-xr-x  8 root root  4096 Feb 18 14:47 ./
drwxr-xr-x 98 root root  4096 Feb 20 15:13 ../
-rw-r--r--  1 root root  7224 Aug 12  2020 apache2.conf
-rw-r--r--  1 root root    96 Feb 11 14:39 claves_basic
-rw-r--r--  1 root root   110 Feb 11 15:34 claves_digest
drwxr-xr-x  2 root root  4096 Jan 18 11:56 conf-available/
drwxr-xr-x  2 root root  4096 Jan 18 11:56 conf-enabled/
-rw-r--r--  1 root root  1782 Apr 13  2020 envvars
-rw-r--r--  1 root root 31063 Apr 13  2020 magic
drwxr-xr-x  2 root root 12288 Feb 18 15:19 mods-available/
drwxr-xr-x  2 root root  4096 Feb 20 16:03 mods-enabled/
-rw-r--r--  1 root root   320 Apr 13  2020 ports.conf
drwxr-xr-x  2 root root  4096 Feb 15 20:03 sites-available/
drwxr-xr-x  2 root root  4096 Feb 15 20:00 sites-enabled/
enrique@enrique:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
enrique@enrique:/etc/apache2$ _
```

8. Verifica que el servidor escucha los puertos 80/TCP y 443/TCP.

netstat –ltn

```
enrique@enrique:/etc/apache2$ netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.200:53        0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.240:53        0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 fe80::a00:27ff:fe98::53 :::*                    LISTEN
tcp6       0      0 fe80::a00:27ff:fe19::53 :::*                    LISTEN
tcp6       0      0 ::1:53                  :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
enrique@enrique:/etc/apache2$ _
```

9. Accede al directorio /etc/apache2/sites-available y observa que existe un fichero denominado default-ssl.conf que contiene la configuración por defecto de un servidor HTTPS.

```
enrique@enrique:/etc/apache2$ cd sites-available/
enrique@enrique:/etc/apache2/sites-available$ ll
total 20
drwxr-xr-x 2 root root 4096 Feb 15 20:03 ./
drwxr-xr-x 8 root root 4096 Feb 18 14:47 ../
-rw-r--r-- 1 root root    0 Feb  4 16:44 .000-default.conf.swp
-rw-r--r-- 1 root root 2953 Feb 15 19:52 000-default.conf
-rw-r--r-- 1 root root 6338 Apr 13  2020 default-ssl.conf
enrique@enrique:/etc/apache2/sites-available$
```

10. Habilita el servidor virtual ssl defecto (default-ssl.conf) de Apache.

sudo a2ensite default-ssl

```
enrique@enrique:/etc/apache2/sites-available$ sudo a2ensite default-ssl
[sudo] password for enrique:
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
enrique@enrique:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ===
enrique@enrique:/etc/apache2/sites-available$ _
```

11. Reinicia el servidor para que los cambios tengan efecto.

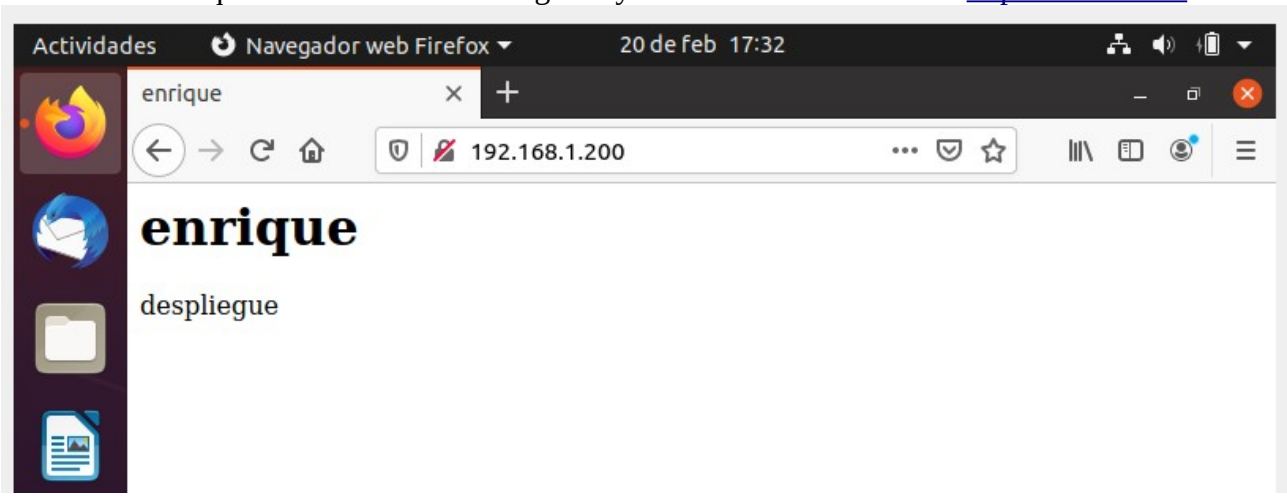
```
enrique@enrique:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ===
enrique@enrique:/etc/apache2/sites-available$
```

12. Consulta el fichero /etc/apache2/sites-available/default-ssl.conf y observa su configuración. Fíjate en las directivas que habilitan SSL y que definen la ruta del certificado digital que usará el servidor.

```
  GNU nano 4.8                          default-ssl.conf
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example the
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on
```

El servidor utiliza por defecto un certificado digital auto firmado que se ha creado al instalar Apache. Un certificado auto firmado no está firmado por una autoridad de certificación (tercera parte de confianza) y, por tanto, no existen mecanismos automáticos que garanticen su autenticidad.

13. Desde la máquina cliente abre el navegador y establece una conexión a http://IP-servidor.



14. Desde la máquina cliente abre el navegador y establece una conexión a https://IP-servidor.

¿Por qué aparece el candado amarillo?

Porque nuestro servidor no tiene ningún tipo de certificado que nos permita establecer una conexión segura con el usuario. Ni que el usuario pueda hacer una transferencia de datos con nuestro servidor, que sus datos correrían peligros de ser filtrados.