ACEPTA

Empresas
a velocidad
digital

Consulta a servicio OCSP

Consulta en línea de estado de Certificados

Marzo 2014

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y Seguridad	Gerencia Certificación y seguridad Oficial de seguridad	Gerencia PSC

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
procedimiento.consulta.ocsp	1.0	Creación de documento	Marzo 2014

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Media **NIVEL DE CONFIDENCIALIDAD: Público**
NOTA DE CONFIDENCIALIDAD: El documento está orientado para clientes de Acepta y publico receptor de objetos firmados con certificados emitidos por Acepta.

CONTROL DE DIFUSIÓN

AUTOR/ES: Certificación y seguridad
DISTRIBUCIÓN: • Personal de Acepta • Clientes de Certificados digitales • Publico receptor de documentos firmados con certificados de Acepta.

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	
https://www.openssl.org/	
RFC 2560 y RFC 6277	

ÍNDICE

1.- INTRODUCCIÓN

A continuación se describe el proceso para realizar consultas sobre un certificado de Firma Electrónica Avanzada, emitido por Acepta, contra el servicio de consulta en línea de certificados (OCSP) provisto por nuestra empresa. Para este fin se utiliza la herramienta multiplataforma OPENSSL, la cual es una aplicación masiva para revisión.

La estructura de comunicación con el servicio OCSP está basada y descrita en el RFC 2560 "*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*", actualizada según RFC 6277 "*Online Certificate Status Protocol Algorithm Agility*".

En el presente documento se describirá además las referencias necesarias para obtener la herramienta, y los mínimos elementos para utilizarlas.

2.- REQUERIMIENTOS

A continuación se describe los elementos sugeridos para realizar la consulta contra el servicio OCSP de acepta.

2.1.- Sistema Operativo

Para realizar la consulta, se consideran las siguientes plataformas:

- Windows
- Linux
- MacOS

2.2.- Aplicación

Se utilizará la aplicación OPENSSL, popular programa de consola para el uso de diferentes funciones criptográficas, la cual está disponible para diferentes plataformas. En los sistemas MacOS como en la mayoría de las distribuciones Linux está aplicación está pre-instalado.

Para instalación de la aplicación en Windows dirigirse al “Anexo 1: Instalación de OPENSSL en Windows” en el presente documento.

En el caso de no contar con la aplicación, ya sea instalada por defecto o para Windows como se describe en el anterior manual, el sitio oficial del comando OPENSSL describe la compilación y los pasos necesarios para realizar una instalación adhoc con el sistema que utilice. Para esto acceder a

- http://wiki.openssl.org/index.php/Compilation_and_Installation

2.3.- Acceso a Consola

Se requerirá acceso a la consola del sistema operativo. En Windows ir a inicio y ejecutar el comando “cmd” abrirá la consola tipo DOS lo que permitirá ir a la ruta donde se alojarán los certificados a consultar.

En el caso de Linux y MacOS, el formato de consola es similar, la aplicación para acceder a esta tiene diversas alternativas. En MacOS está por defecto el comando “terminal” o bien abriendo "Finder" situado en el Dock del SO, luego selecciona "Aplicaciones > Utilidades" y finalmente ejecutar el icono "Terminal". En Linux es posible encontrar “gnome-terminal” dependiendo siempre de la distribución y del gestor de ventanas que se utilice.

3.- ELEMENTOS PARA CONSULTA

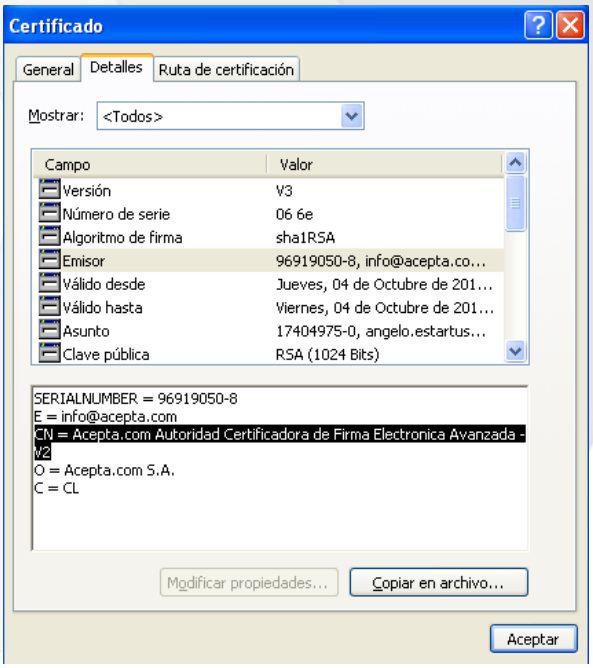
Para realizar la consulta se contará con los siguientes elementos en alguna ruta seleccionada por el usuario.

3.1.- Jerarquías de Certificado

Para la consulta se utilizará la jerarquía del certificado de Firma Electrónica Avanzada:

- Certificado intermedio de la autoridad que emitió el certificado
- Certificado raíz de la autoridad que emitió el certificado

Dependiendo de la jerarquía que firmó el certificado a consultar estos certificados se podrán obtener directamente desde el certificado (si se dispone de él), o bien desde una descarga directa desde servidores de Acepta. De no conocer la jerarquía del certificado, se podrá identificar a partir del certificado que se quiere consultar, en el campo "emisor", parámetro CN (CommonName). A continuación un ejemplo del campo señalado, destacado en fondo negro:



Este campo emisor también puede ser obtenido a través del comando openssl, como se muestra a continuación:

- openssl x509 -in [ARCHIVO_DER] -issuer –noout

La salida del comando será similar al siguiente ejemplo:

“issuer= /C=CL/O=Acepta.com S.A./CN=Acepta.com Autoridad Certificadora de Firma Electronica Avanzada - G3/emailAddress=info@acepta.com/serialNumber=96919050-8”

Donde el CN corresponde a “CN=Acepta.com Autoridad Certificadora de Firma Electronica Avanzada - G3/”

Las jerarquías podrán ser obtenidas desde los siguientes URL:

Para un certificado generado con la instalación V2:

- https://www.acepta.com/autoservicio2/CertificadoRaizV2New.crt
- https://www.acepta.com/autoservicio2/IntermedioFAV2New.crt

Para un certificado generado con la instalación G3:

- https://acg3.acepta.com/descargas/acepta.com.g3.raiz.crt
- https://acg3.acepta.com/descargas/acepta.com.g3.FirmaElectronicaAvanzada.crt

Estas jerarquías deben ser alojadas en una ruta seleccionada por el usuario, la cual permita acceder a través de la consola.

3.2.- Certificado o Serial

Se utilizará la exportación del certificado FEA (Firma Electrónica Avanzada) o bien el serial del mismo, si no se dispone de esta llave.

El certificado FEA deberá estar en formato DER (x509 en base64), y NO como PEM (x509 binario), obtenido exportando desde el FEA en un dispositivo criptográfico o bien desde un documento firmado. El archivo deberá ser alojado en la misma ruta donde se alojarán los certificados de las jerarquías asociadas.

En caso de disponer sólo de un archivo de certificado x509 binario, se podrá convertir utilizando el siguiente comando desde la consola del sistema.

- Acceder a la ruta del certificado
- openSSL x509 -inform PEM -outform DER -in [ARCHIVO_PEM] –out [ARCHIVO_DER]

Donde ARCHIVO_PEM corresponde al certificado que se dispone en format x509 binario, y ARCHIVO_DER el archivo que se utilizará a futuro en formato x509 en base64, con un nombre descriptivo a elección del usuario (ej. Certificado.der)

Para el Serial o número identificador del certificado, podrá ser obtenido desde el Certificado Original o desde un documento firmado con este, extrayendo el certificado. Este dato podrá ser obtenido utilizando el comando openssl, con la siguiente instrucción desde la consola:

- Acceder a la ruta del certificado
- openssl x509 -in [ARCHIVO_DER] –serial -noout

Con esto se obtendrá un valor como el que sigue: ej. “serial=01”, este valor se encuentra en hexadecimal.

3.3.- URL de consulta OCSP

Las direcciones de los servicios a utilizar dependerá de la jerarquía con la que se emitió el certificado.

Para certificados “Acepta.com Autoridad Certificadora de Firma Electronica Avanzada - V2”: http://ocsp.acepta.com/FirmaAvanzadaV2

Para certificado “Acepta.com Autoridad Certificadora de Firma Electronica Avanzada - G3”: https://acg3.acepta.com/acg3/ocsp/FirmaAvanzada-G3

Este proceso es totalmente confiable utilizando las URL descritas anteriormente.

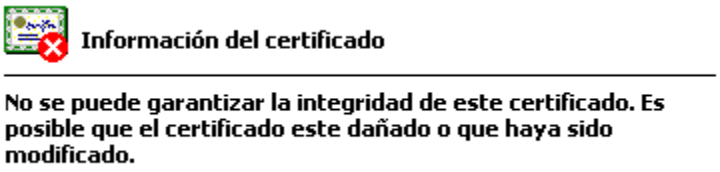
Alternativamente se puede obtener la URL del servicio OCSP asociado, directamente desde el certificado. Para obtener estas URL para Windows, es consultar en forma grafica el certificado si se cuenta con este, con doble click se abrirá la información del certificado, se podrá ir a la segunda pestaña y en el listado seleccionar el campo “Acceso a información de la entidad emisora”, se mostrará la url del campo OCSP.

Alternativa para Linux y MacOS, se podrá ejecutar una consulta con OPENSSL desde la consola, con lo siguiente:

- Acceder a la ruta del certificado
- openssl x509 -in [ARCHIVO_DER] –ocsp_uri –noout

Con esto se obtendrá la URL a utilizar para acceder al servicio OCSP.

Al leer directamente del certificado la URL para acceder al servicio OCSP, cumpliendo con las confianzas en la autoridad que genera las jerarquías de la AC de Acepta, se mostrará el certificado como correcto y de una entidad confiable. El certificado será reconocido si se tienen las raíces de Acepta instaladas, por ejemplo en un navegador, se evidenciará el correcto emisor del certificado. Al consultar el certificado en Windows por ejemplo, si no existen las confianzas en el emisor, será por no tener instaladas las raíces y se mostrará un indicador como el siguiente:



Si es el caso, el usuario debe descargar las jerarquías descritas en el punto 3.1 e instalarlas o leerlas desde la aplicación que se utilice para su validación. De continuar el mensaje se recomienda utilizar las URL antes descritas.

4.- EJECUCIÓN DE COMANDOS

Para realizar la consulta se deberá tener presente todo lo señalado en los puntos 2 y 3, para reproducir lo que se sugiere a continuación.

4.1.- Consulta OCSP

Al usar un comando para todas las plataformas indicadas en el punto 2, se podrá repetir o bien utilizar un comando común. OPENSSL será ejecutado desde la consola disponible, donde deberá acceder a la ruta donde se encuentran el certificado y las jerarquías correspondientes.

4.1.1.- Para consultar por Serial de certificado

Para consultar por serial, se debe realizar lo siguiente

- openssl ocsp -text -issuer [INTERMEDIA_FEA] -nonce -CAfile [RAIZ_FEA] -url [URL_OCSP] -serial [SERIAL_CERTIFICADO_FEA]

Donde:

- INTERMEDIA_FEA, corresponde al certificado intermedio de la jerarquía FEA de Acepta, obtenido según se indica en el punto 3.1.
- RAIZ_FEA, corresponde al certificado raíz de la jerarquía FEA de Acepta, obtenido según se indica en el punto 3.1.
- URL_OCSP, corresponde a la URL del servicio OCSP que ofrece Acepta, obtenido según se indica en 3.3.
- SERIAL_CERTIFICADO_FEA, corresponde al serial del certificado a consultar.

4.1.2.- Para consultar con el archivo de certificado

Para consultar por serial, se debe realizar lo siguiente

- openssl ocsp -text -issuer [INTERMEDIA_FEA] -nonce -CAfile [RAIZ_FEA] -url [URL_OCSP] –cert [CERTIFICADO_FEA_DER]

Donde:

- INTERMEDIA_FEA, corresponde al certificado intermedio de la jerarquía FEA de Acepta, obtenido según se indica en el punto 3.1.
- RAIZ_FEA, corresponde al certificado raíz de la jerarquía FEA de Acepta, obtenido según se indica en el punto 3.1.
- URL_OCSP, corresponde a la URL del servicio OCSP que ofrece Acepta, obtenido según se indica en 3.3.

- CERTIFICADO_FEA_DER, corresponde al archivo de certificado a consultar, el cual está en formato x509 en base64.

4.2.- Estructura de la respuesta esperada

Al realizar una consulta contra el servicio OCSP, técnicamente se espera una estructura con 3 secciones, las que entrega información técnica del la consulta y del estado del certificado registrado en la Autoridad Certificador de Acepta.

- OCSP Request Data: Estructura de consulta
- OCSP Response Data: Estructura de Respuesta
- Certificate: correspondiente a la información del certificado del servicio OCSP (en este caso el mismo intermedio de FEA)

El detalle de la estructura y el contenido que se espera del Request y del Response se entrega a continuación:

4.2.1.- Request

- Versión del protocolo
- Lista de Identificación de certificados
    - ID certificado
        - Algoritmo Hash
        - Nombre emisor del Hash
        - Clave emisor hash
        - Número de serie
    - Extensión
- Extensiones opcionales que pueden ser procesadas por el servicio OCSP

4.2.2.- Response

- Status de Response
- Tipo de Response
- Versión de la respuesta
- Identificador de quien responde
- Fecha de response
- Respuesta para certificado consultado del request
    - Identificador del certificado
        - Algoritmo
        - Nombre de emisor en HASH
        - Llave del emisor en HASH
        - Serie del certificado
    - Estado del certificado

  - Fecha de actualización
  - Extensiones opcionales
- Extensiones opcionales
- Algoritmo de firma
- Firma calculada con Hash de la respuesta

5.- ANEXO 1: INSTALACIÓN DE OPENSSL EN WINDOWS

5.1.- Descargas

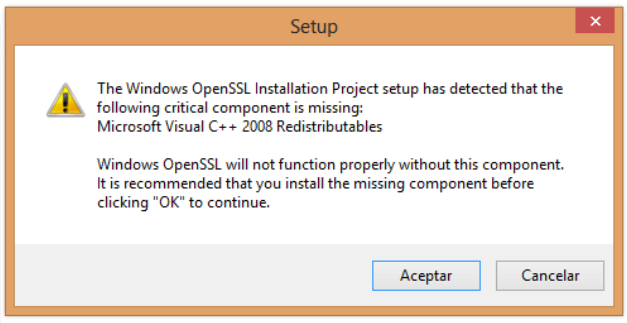
Para realizar la instalación de descargarán los binarios instalables para la arquitectura del SO Windows instalado

- Versión para x32
  - http://slproweb.com/download/Win32OpenSSL_Light-1_0_1i.exe
- Versión para x64
  - http://slproweb.com/download/Win64OpenSSL_Light-1_0_1i.exe

5.2.- Instalación

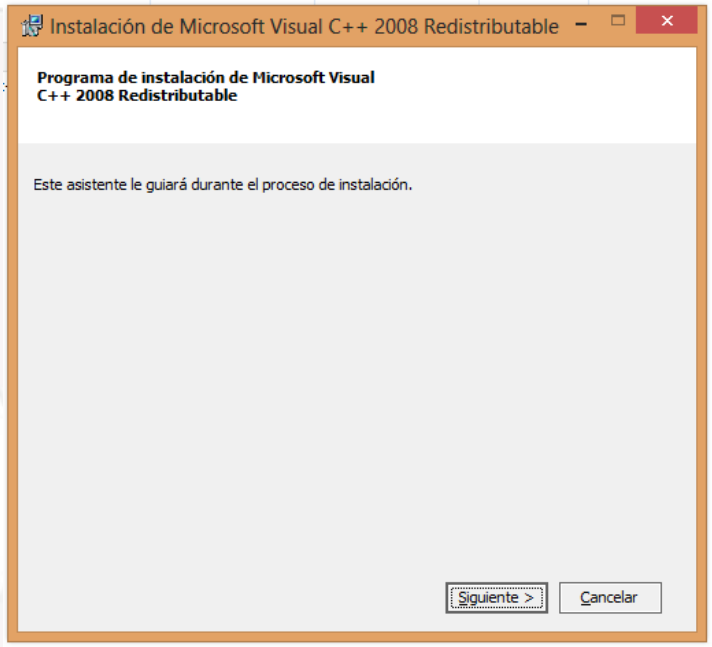
Realizar el siguiente procedimiento:

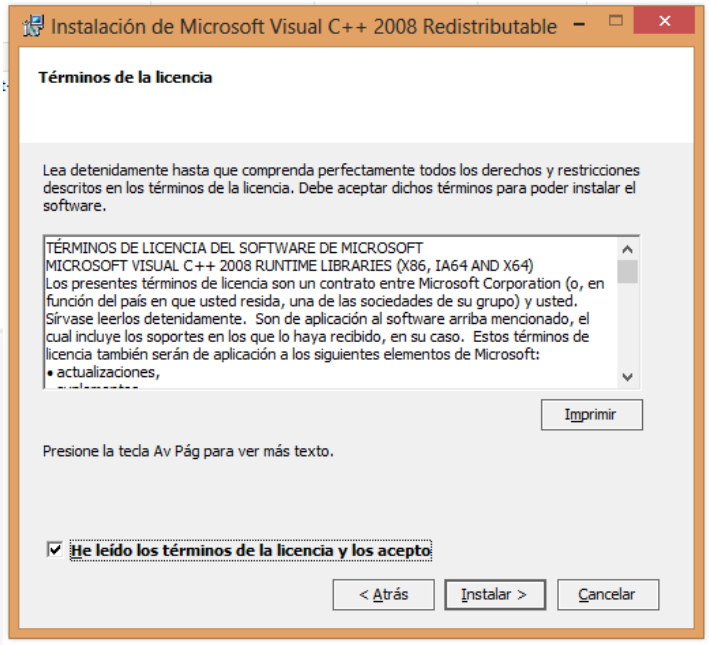
- ir a la carpeta donde se realizó la descarga
- ejecutar el archivo:
  - si es para x64 -> Win64OpenSSL_Light-1_0_1i.exe
  - si es para x32 -> Win32OpenSSL_Light-1_0_1i.exe
- Si en tu instalación aparece el error

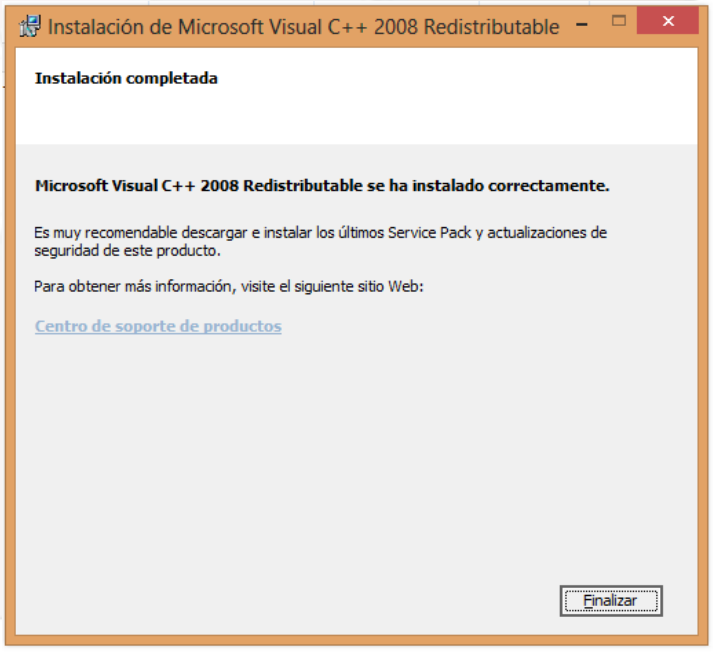


  - dar click en cancelar al mensaje
  - Descargar lo siguiente:
    - para x32
      - http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF
    - para x64
      - http://www.microsoft.com/downloads/details.aspx?familyid=bd2a6171-e2d6-4230-b809-9a8d7548c1b6

- Ir a carpeta de descarga y ejecutar el archivo según corresponda:
  - para x32
    - vcredist_x32.exe
  - para x64
    - vcredist_x64.exe
- Ver imágenes de instalación de Microsoft Visual C++ 2008 Redistributable

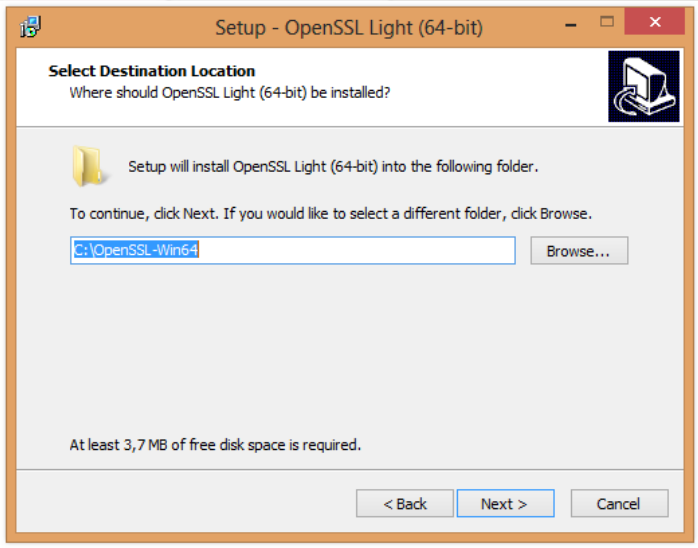


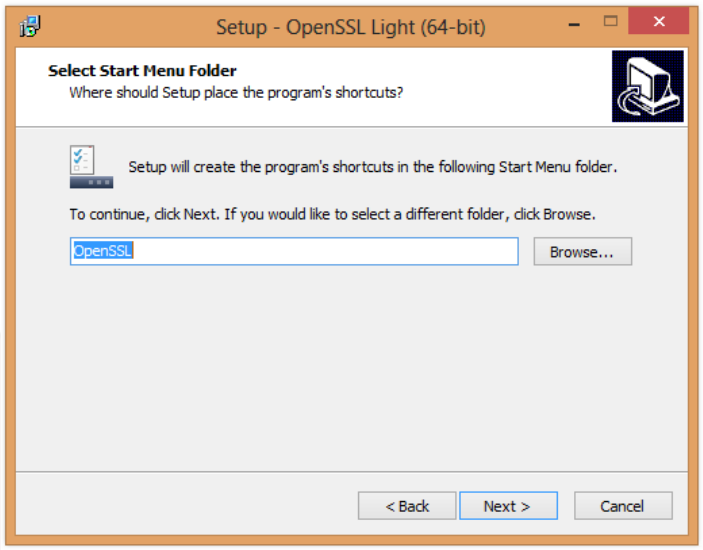


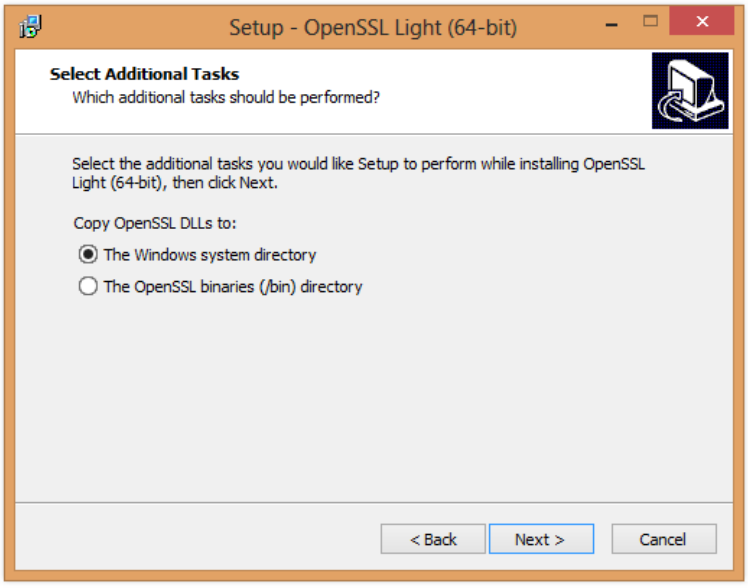


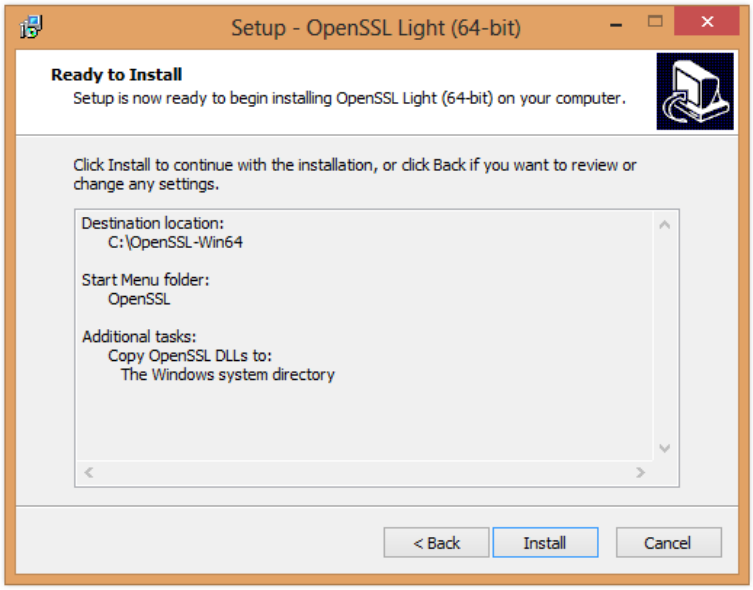
  - Reiniciar equipo
- Si no aparece este error o ya instalaste lo que faltaba continua con el proceso normal, según muestran las imágenes siguientes:

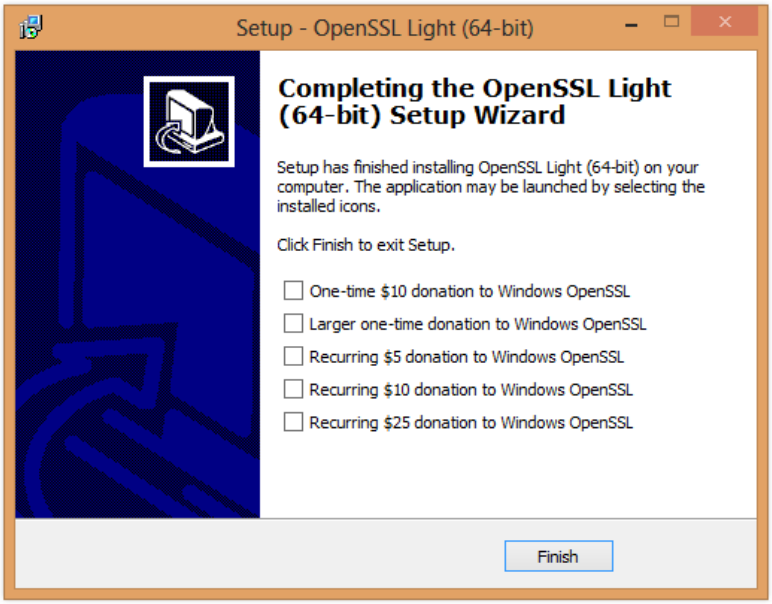

Setup - OpenSSL Light (64-bit)
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
DONATIONS NEEDED! If you are a business you should be contributing regular donations. If you are a generous individual, consider regular donations. Most people simply take and run - leaving me to foot the bill. That's not nice. Some businesses even drop their customers onto me to provide direct support to the customer (ahem, PayPal). That's just evil. Even if you can't afford a small, one time donation of $10, at least drop a line saying how much you appreciate the effort put into this project (and, optionally, what you use OpenSSL for). Lots of complaints and few compliments is discouraging.
LEGAL NOTICE: This product includes software developed by the OpenSSL
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel


Setup - OpenSSL Light (64-bit)
Select Destination Location
Where should OpenSSL Light (64-bit) be installed?
Setup will install OpenSSL Light (64-bit) into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\OpenSSL-Win64
Browse...
At least 3,7 MB of free disk space is required.
< Back
Next >
Cancel


Setup - OpenSSL Light (64-bit)
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
OpenSSL
Browse...
< Back
Next >
Cancel


Setup - OpenSSL Light (64-bit)
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing OpenSSL Light (64-bit), then click Next.
Copy OpenSSL DLLs to:
The Windows system directory
The OpenSSL binaries (/bin) directory
< Back
Next >
Cancel





*NOTA: El mensaje de error continuará apareciendo pero el software faltante ya estará operativo, solo dar click a "Aceptar"

5.3.- Configuración

Cuando finalice la instalación se debe abrir una línea de comandos o consola como administrador

- Inicio > Todas las aplicaciones > click derecho sobre simbolo de sistema > Ejecutar como administrador

- Ejecuta:
  set OPENSSL_CONF=c:\[UBICACION DEL DIRECTORIO DE OPENSSL]\bin\openssl.cfg

Luego ubicarse en la carpeta en que se encuentra el ejecutable de OpenSSL:

- cd c:\<ubicacion de Openssl>\bin

*NOTA:si ejecutaste el paso a paso de esta guía la [UBICACION DEL DIRECTORIO DE OPENSSL] sería:

- c:\OpenSSL *si es de x32
- c:\OpenSSL-Win64 *si es de x64

Con esto queda la instalación terminada.