



BANBAJIO

MULTIPAGOS

**DEPÓSITOS ELECTRÓNICOS
A TRAVÉS DE SU COMPUTADORA**

► GENERACIÓN DE LLAVES ASIMÉTRICAS

Objetivos:

- Contar con una guía que facilite la generación de llaves asimétricas, para el adecuado despliegue del producto de Multipagos.

Dirigido a:

- Áreas de seguridad lógica (informática), áreas de arquitectura y desarrollo de software que participan en el desarrollo de Multipagos por parte del cliente.



► GENERACIÓN DE LLAVES ASIMÉTRICAS

WINDOWS



LINUX



► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)

1. Abrir la carpeta “OpenSSL for Windows”.



OpenSSL for Windows

2. Dentro de la carpeta “OpenSSL for Windows”, se encuentran las versiones OpenSSL para Windows a 32 bits y 64 bits. Descomprimir el que corresponda a la arquitectura de su Sistema Operativo en la carpeta que considere conveniente.



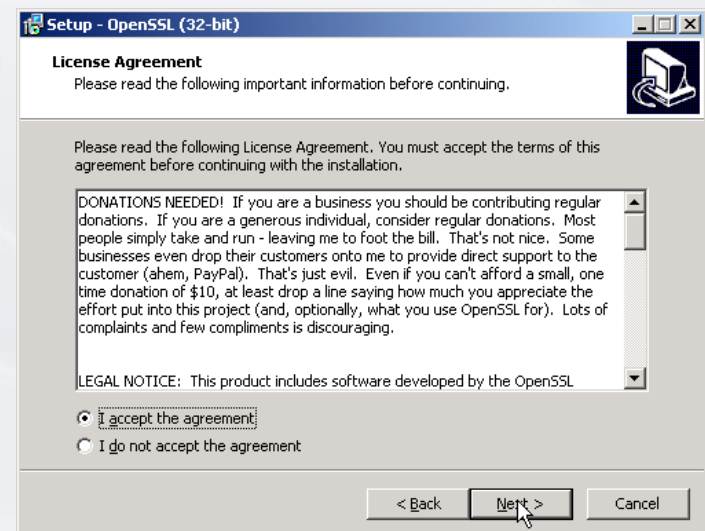
► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)

3. Una vez que se descomprimió el “OpenSSL” para la versión de Windows con la que se cuente, se procederá a ejecutar el archivo ejecutable (*.exe) como lo muestran las siguientes pantallas:

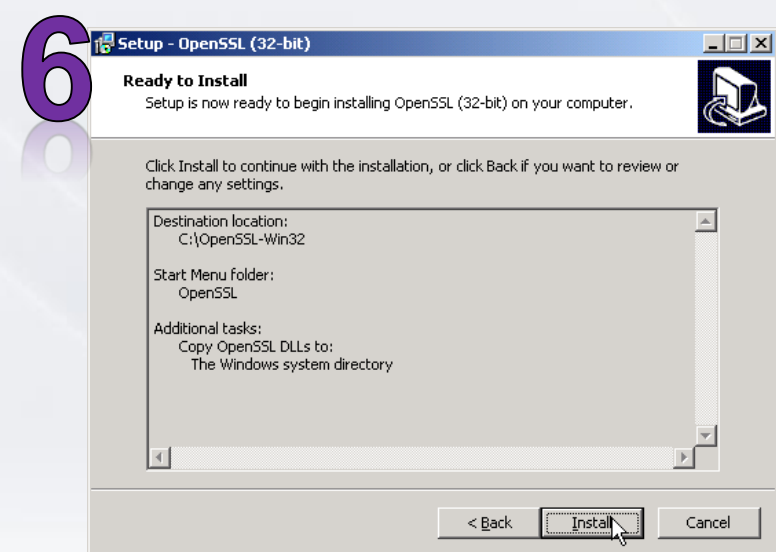
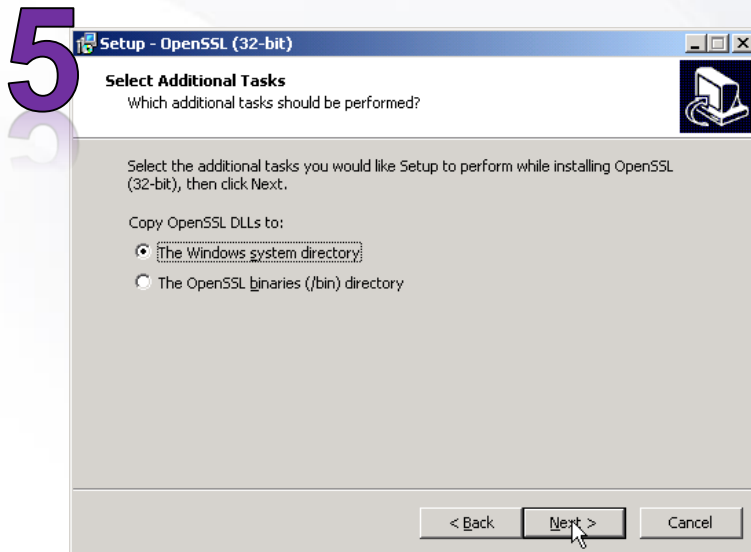
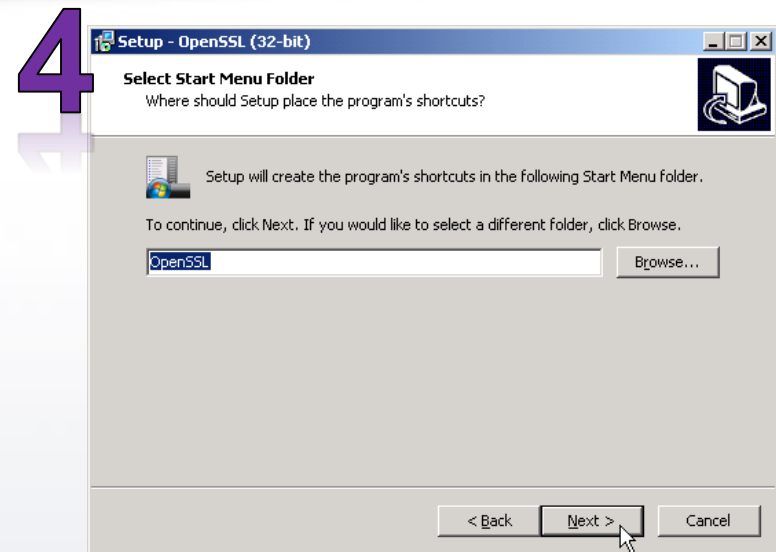
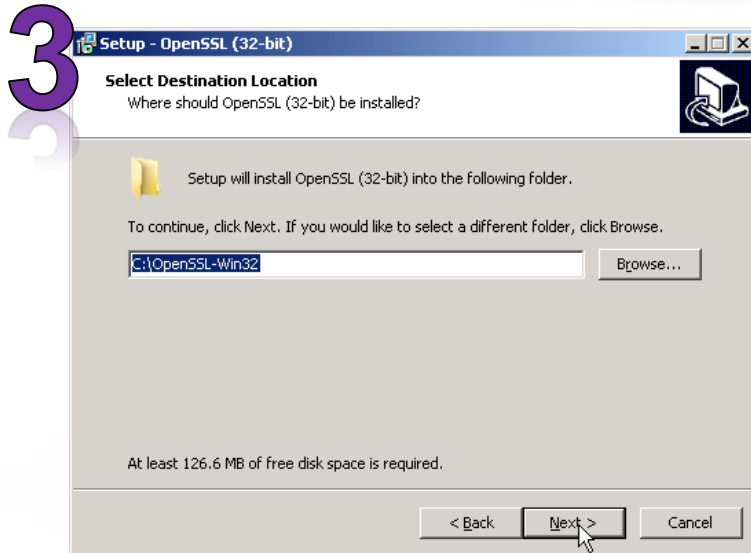
1



2



► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)



► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)

4. Una vez habiendo instalado correctamente el OpenSSL, se debe abrir una ventana del símbolo del sistema e ingresar a la carpeta “bin” en la que se tenga instalado el OpenSSL:

EJEMPLO

```
cd C:\OpenSSL-Win32\bin
```

- Se establecen las variables de entorno, según la arquitectura de Windows por medio de los siguientes comandos:

```
set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg  
set RANDFILE=C:\OpenSSL-Win32\bin\rnd
```

- Se genera la llave privada por medio del siguiente comando:

```
openssl genrsa -out Private_key.pem 1024
```

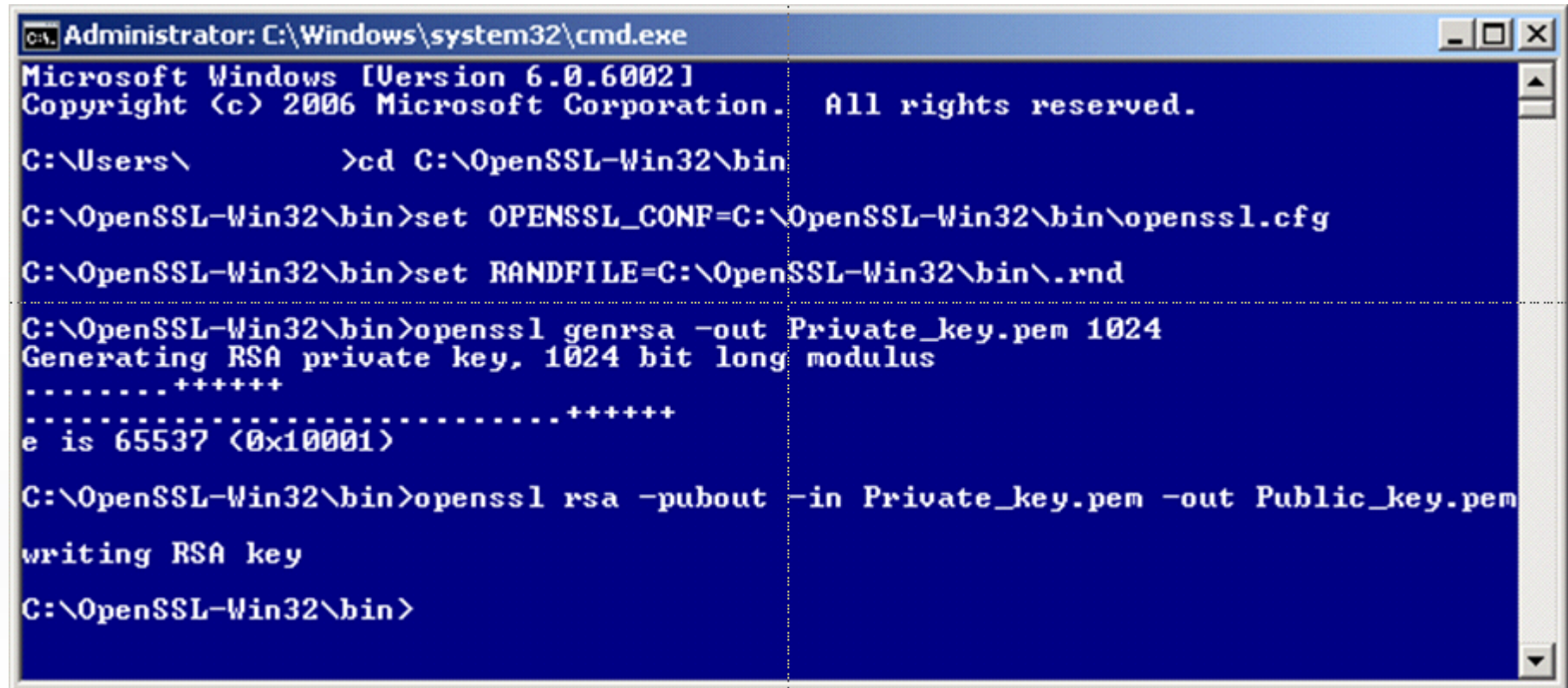
- Con la llave privada, se genera la llave pública por medio del siguiente comando :

```
openssl rsa -pubout -in Private_key.pem -out Public_key.pem
```



► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)

La siguiente imagen muestra el proceso completo:



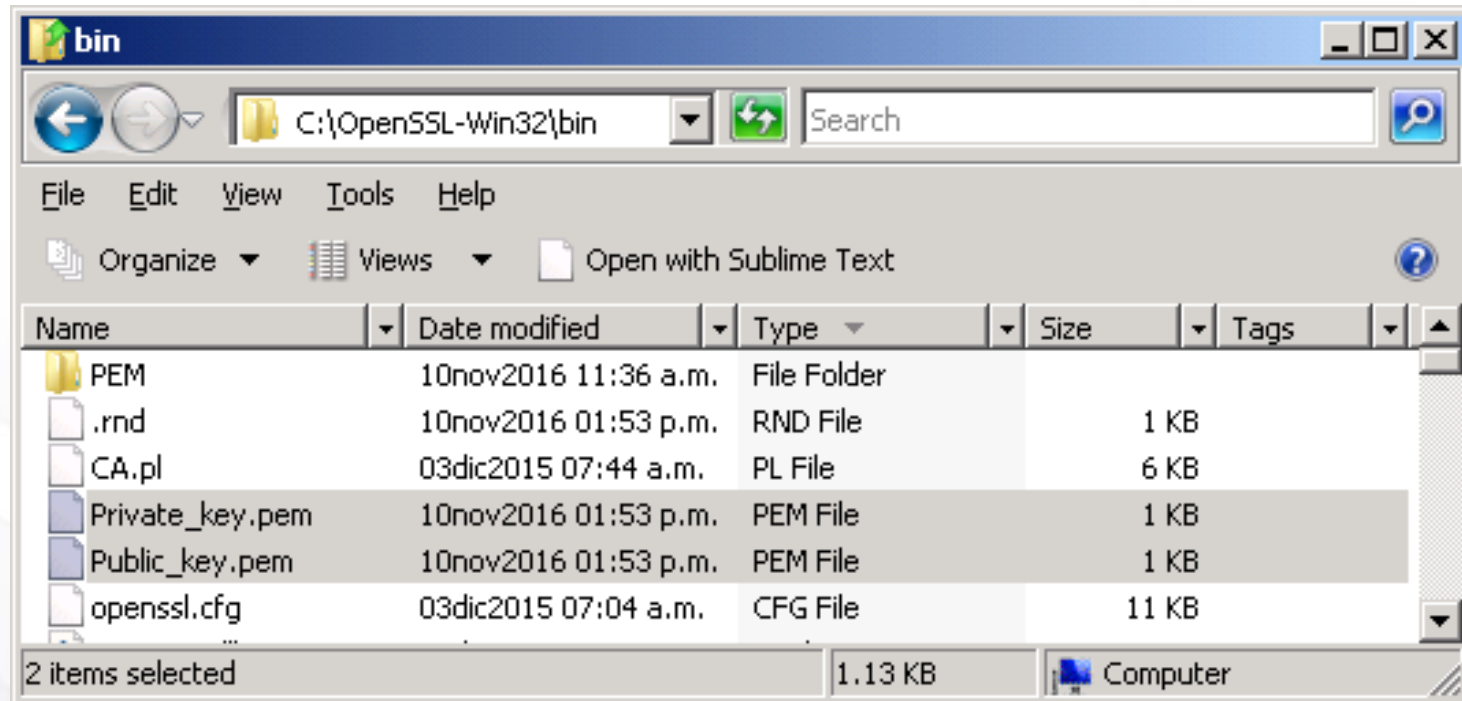
```
C:\>Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\>>cd C:\OpenSSL-Win32\bin
C:\OpenSSL-Win32\bin>set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
C:\OpenSSL-Win32\bin>set RANDFILE=C:\OpenSSL-Win32\bin\.rnd
C:\OpenSSL-Win32\bin>openssl genrsa -out Private_key.pem 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
C:\OpenSSL-Win32\bin>openssl rsa -pubout -in Private_key.pem -out Public_key.pem
writing RSA key
C:\OpenSSL-Win32\bin>
```



► GENERACIÓN DE LLAVES ASIMÉTRICAS (WINDOWS)

5. En la carpeta “bin” se encontrarán las dos llaves creadas (Privada y Pública) :



La llave Pública se deberá de proporcionar a BanBajío para el intercambio de información.

Con esto se finaliza el proceso de generación de Llaves Asimétricas para Windows.



► GENERACIÓN DE LLAVES ASIMÉTRICAS (LINUX)

1. Se descarga e instala desde <https://www.openssl.org/source/> la última versión disponible de OpenSSL.

KBytes	Date	File
5058	2016-Nov-10 14:15:12	openssl-1.1.0c.tar.gz (SHA256) (PGP sign) (SHA1)
5183	2016-Sep-26 10:04:14	openssl-1.0.2j.tar.gz (SHA256) (PGP sign) (SHA1)
4460	2016-Sep-22 10:35:26	openssl-1.0.1u.tar.gz (SHA256) (PGP sign) (SHA1)
1440	2016-Aug-17 01:04:54	openssl-fips-2.0.13.tar.gz (SHA256) (PGP sign) (SHA1)
1420	2016-Aug-17 01:04:54	openssl-fips-ecp-2.0.13.tar.gz (SHA256) (PGP sign) (SHA1)

2. Una vez instalado, se ejecutan los siguientes comandos:

- Se genera la llave privada por medio del siguiente comando :

```
openssl genrsa -out Private_key.pem 1024
```

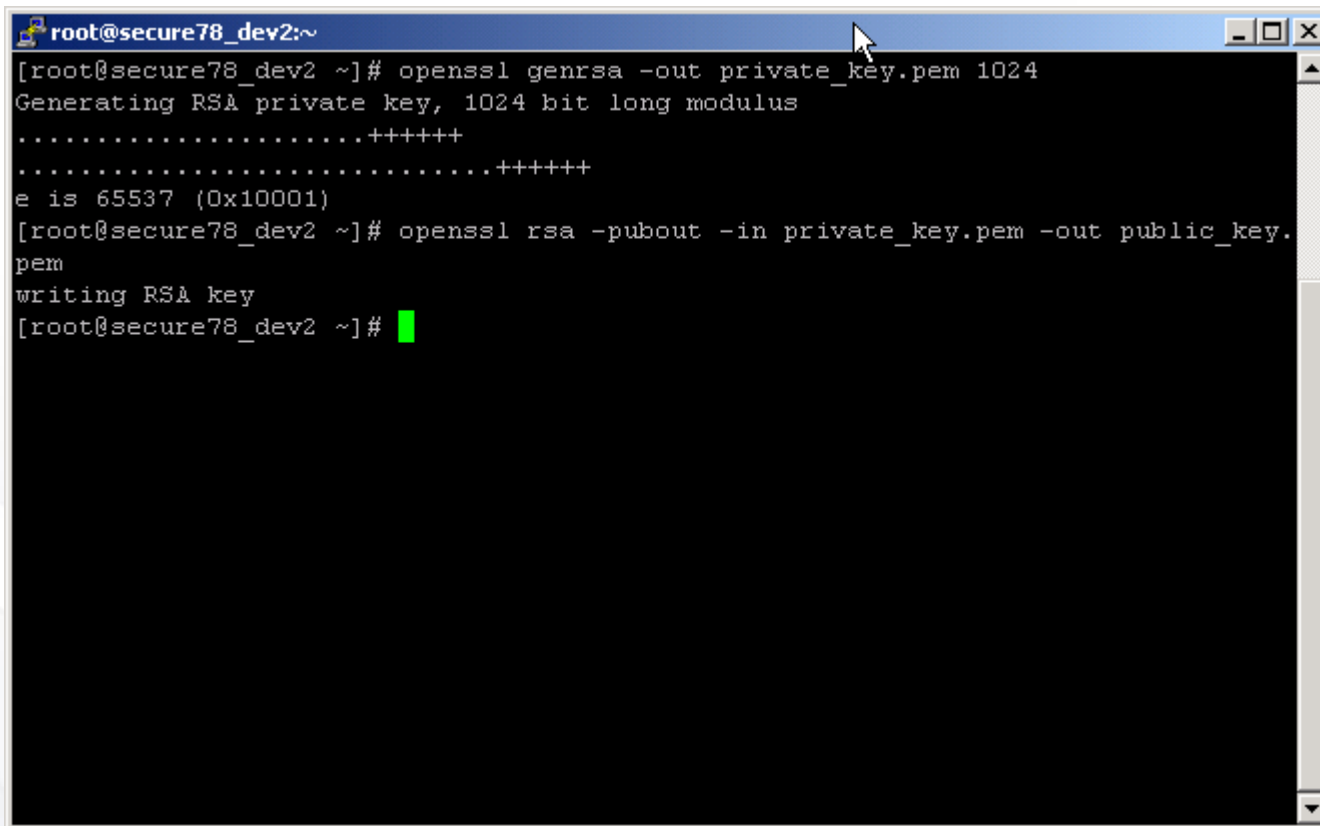
-Con la llave privada, se genera la llave pública por medio del siguiente comando :

```
openssl rsa -pubout -in Private_key.pem -out Public_key.pem
```



► GENERACIÓN DE LLAVES ASIMÉTRICAS (LINUX)

3. En la siguiente imagen se muestra su ejecución:



```
root@secure78_dev2:~  
[root@secure78_dev2 ~]# openssl genrsa -out private_key.pem 1024  
Generating RSA private key, 1024 bit long modulus  
.....++++++  
.....++++++  
e is 65537 (0x10001)  
[root@secure78_dev2 ~]# openssl rsa -pubout -in private_key.pem -out public_key.  
pem  
writing RSA key  
[root@secure78_dev2 ~]#
```

4. La llave pública se deberá de proporcionar a BanBajío para el intercambio de información.

Con esto se finaliza el proceso de generación de Llaves Asimétricas para Linux.



Para mayor información:

Consulte

www.bb.com.mx

Llámenos

En León, Guanajuato

7 10 46 40

Desde el Resto del País

01 800 47 10 400

Lada Sin Costo

