Apéndice

A continuación se presentarán algunas definiciones utilizadas en este documento:

- **Llaves pública/privada:** La encriptación usando el par llave pública/privada asegura que la información encriptada con una llave solo puede ser desencriptada por su par. El par de llaves está basado en un número primo y su longitud en términos de bits asegura que sea difícil de desencriptar en ausencia del par de llaves. La base es mantener una llave guardada (la llave privada) y distribuir la otra (llave pública) a todo el mundo. Cualquier persona puede enviar mensajes encriptados con la llave pública pero solo el poseedor de la llave privada los puede desencriptar. Asimismo lo encriptado por la llave privada, sólo puede ser desencriptado por la llave pública, pero en este caso el mensaje no es seguro, solamente fue firmado.

- **Certificado Digital:** Para asegurar que se establece comunicación con el destino correcto, existen entidades que se han dedicado a asegurar que alguien es realmente quien dice ser, esta entidad tiene nuestra confianza de manera implícita pues tiene su certificado digital almacenado en el navegador web, este certificado es conocido como certificado raíz (root Certificate). Un certificado contiene información acerca de su poseedor, como su dirección electrónica, su nombre, uso del certificado, período de validez, la dirección web en caso de las páginas o una dirección de correo dependiendo del uso, y el ID de la entidad que certifica esta información. También contiene la llave pública y finalmente un hash para asegurar que el certificado no ha sido alterado. Normalmente el navegador web carga el certificado raíz de todas las Autoridades Certificadoras (CA), las cuales mantienen una lista de todos los certificados firmados, así mismo de los certificados revocados. Un certificado es inseguro mientras no se firme, y un certificado firmado no puede ser modificado, uno puede firmar su propio certificado, pero solo las CA poseen certificados raíz auto firmados. A continuación se adjunta un ejemplo de certificado digital:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=FJ, ST=Fiji, L=Suva, O=SOPAC, OU=ICT, CN=SOPAC Root
CA/Email=administrator@sopac.org
        Validity
            Not Before: Nov 20 05:47:44 2001 GMT
            Not After : Nov 20 05:47:44 2002 GMT
        Subject: C=FJ, ST=Fiji, L=Suva, O=SOPAC, OU=ICT,
CN=www.sopac.org/Email=administrator@sopac.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:54:2c:ab:88:74:aa:6b:35:a5:a9:c1:d0:5a:
                    9b:fb:6b:b5:71:bc:ef:d3:ab:15:cc:5b:75:73:36:
                    b8:01:d1:59:3f:c1:88:c0:33:91:04:f1:bf:1a:b4:
```

```
                    7a:c8:39:c2:89:1f:87:0f:91:19:81:09:46:0c:86:
                    08:d8:75:c4:6f:5a:98:4a:f9:f8:f7:38:24:fc:bd:
                    94:24:37:ab:f1:1c:d8:91:ee:fb:1b:9f:88:ba:25:
                    da:f6:21:7f:04:32:35:17:3d:36:1c:fb:b7:32:9e:
                    42:af:77:b6:25:1c:59:69:af:be:00:a1:f8:b0:1a:
                    6c:14:e2:ae:62:e7:6b:30:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

FE:04:46:ED:A0:15:BE:C1:4B:59:03:F8:2D:0D:ED:2A:E0:ED:F9:2F
            X509v3 Authority Key Identifier:

keyid:E6:12:7C:3D:A1:02:E5:BA:1F:DA:9E:37:BE:E3:45:3E:9B:AE:E5:A6
                DirName:/C=FJ/ST=Fiji/L=Suva/O=SOPAC/OU=ICT/CN=SOPAC
Root CA/Email=administrator@sopac.org
                serial:00
    Signature Algorithm: md5WithRSAEncryption
        34:8d:fb:65:0b:85:5b:e2:44:09:f0:55:31:3b:29:2b:f4:fd:
        aa:5f:db:b8:11:1a:c6:ab:33:67:59:c1:04:de:34:df:08:57:
        2e:c6:60:dc:f7:d4:e2:f1:73:97:57:23:50:02:63:fc:78:96:
        34:b3:ca:c4:1b:c5:4c:c8:16:69:bb:9c:4a:7e:00:19:48:62:
        e2:51:ab:3a:fa:fd:88:cd:e0:9d:ef:67:50:da:fe:4b:13:c5:
        0c:8c:fc:ad:6e:b5:ee:40:e3:fd:34:10:9f:ad:34:bd:db:06:
        ed:09:3d:f2:a6:81:22:63:16:dc:ae:33:0c:70:fd:0a:6c:af:
        bc:5a
-----BEGIN CERTIFICATE-----
MIIDoTCCAwqgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBiTELMAkGA1UEBhMCRkox
DTALBgNVBAgTBEZpamkxDTALBgNVBAcTBFN1dmExDjAMBgNVBAoTBVNPUEFDMQww
CgYDVQQLEwNJQ1QxFjAUBgNVBAMTDVNPUEFDIFJvb3QgQ0ExJjAkBgkqhkiG9w0B
CQEWF2FkbWluaXN0cmF0b3JAc29wYWMub3JnMB4XDTAxMTEyMDA1NDc0NFoXDTAy
MTEyMDA1NDc0NFowgYkxCzAJBgNVBAYTAkZKMQ0wCwYDVQQIEwRGaWppMQ0wCwYD
VQQHEwRTdXZhMQ4wDAYDVQQKEwVTT1BBQzEMMAoGA1UECxMDSUNUMRYwFAYDVQQD
Ew13d3cuc29wYWMub3JnMSYwJAYJKoZIhvcNAQkBFhdhZG1pbmlzdHJhdG9yQHNv
cGFjLm9yZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAulQsq4h0qms1panB
0Fqb+2u1cbzv06sVzFt1cza4AdFZP8GIwDORBPG/GrR6yDnCiR+HD5EZgQlGDIYI
2HXEb1qYSvn49zgk/L2UJDer8RzYke77G5+IuiXa9iF/BDI1Fz02HPu3Mp5Cr3e2
JRxZaa++AKH4sBpsFOKuYudrMOkCAwEAAaOCARUwggERMAkGA1UdEwQCMAAwLAYJ
YIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBT+BEbtoBW+wUtZA/gtDe0q4O35LzCBtgYDVR0jBIGuMIGrgBTmEnw9oQLl
uh/anje+40U+m67lpqGBj6SBjDCBiTELMAkGA1UEBhMCRkoxDTALBgNVBAgTBEZp
amkxDTALBgNVBAcTBFN1dmExDjAMBgNVBAoTBVNPUEFDMQwwCgYDVQQLEwNJQ1Qx
FjAUBgNVBAMTDVNPUEFDIFJvb3QgQ0ExJjAkBgkqhkiG9w0BCQEWF2FkbWluaXN0
cmF0b3JAc29wYWMub3JnggEAMA0GCSqGSIb3DQEBBAUAA4GBADSN+2ULhVviRAnw
VTE7KSv0/apf27gRGsarM2dZwQTeNN8IVy7GYNz31OLxc5dXI1ACY/x4ljSzysQb
xUzIFmm7nEp+ABlIYuJRqzr6/YjN4J3vZ1Da/ksTxQyM/K1ute5A4/00EJ+tNL3b
Bu0JPfKmgSJjFtyuMwxw/Qpsr7xa
-----END CERTIFICATE-----
```

- **Llave simétrica:** Si bien la encriptación usando el par llave pública privada es muy buena, usualmente no resulta práctica, no permite usar la misma llave para la encriptación y desencriptación. Un algoritmo que usa la misma llave para encriptar y desencriptar debe utilizar una llave simétrica, estos algoritmos son mucho más veloces que los algoritmos asimétricos, sin embargo una llave simétrica es potencialmente muy insegura pues si un intruso obtiene la llave simétrica, se acaban la seguridad y la encriptación, es necesario transmitir la llave simétrica de una forma segura como por ejemplo transmitirla encriptada con un algoritmo asimétrico.

- **Algoritmos de Encriptación:** Por lo general, salvo en Estados Unidos, los algoritmos no pueden ser patentados, OpenSSL fue desarrollado en un país donde los algoritmos no pueden ser patentados, y donde la tecnología de encriptación no está reservada a las agencias del estado. OpenSSL puede ser compilado con o sin ciertos, de manera que pueda ser usado en la mayoría de los países donde las restricciones se aplican.

- **Hash:** Un hash es un número dado por una función hash aplicada a un mensaje. Esta es una función en un solo sentido, lo que significa que es imposible obtener el mensaje original conociendo el hash. El hash cambiará drásticamente incluso para la menor modificación en el mensaje, por otro lado resulta extremadamente difícil modificar un mensaje y mantener su hash original. Las funciones hash son utilizadas en sistemas de password, para certificar que una aplicación es original, y en general, para asegurar que cualquier mensaje no ha sido modificado.

Proceso de Firmado: Firmar un mensaje no significa nada más que asumir la autenticidad de un mensaje, éste puede ser un mensaje de texto o el certificado de alguien más. Para firmar un mensaje se crea su hash y luego se encripta el hash con la llave privada y se agrega el hash encriptado al certificado firmado. La ventaja de firmar un mensaje, es que se transmite la llave pública a todos los receptores. Normalmente existen 2 formas de firmar un mensaje, la antes descrita y codificando el mensaje en conjunto con la firma, la última forma es mas simple pues cualquier programa puede desencriptarlo y leer la llave pública contenida en él, además con este método modificar el mensaje y hacerlo legible, pues va encriptado completamente, a diferencia del primero