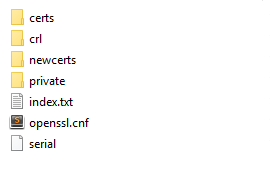
Seguridad y Protección de Sistemas Informáticos Práctica 4

Miguel Morales Castillo

1. Cread una autoridad certificadora. En este caso se premiará el uso de openssl ca frente a CA.pl, aunque este último comando es admisible.

Para crear la autoridad certificadora primero creamos la estructura de carpetas y archivos siguientes:



En cada carpeta se guarda lo que su propio nombre indica intuitivamente. Index.txt llevara un control de las firmas realizadas por la CA y en openssl.cnf se encuentra la configuración de la CA, que hemos modificado del archivo por defecto de OpenSSL para meter nuestros datos y ruta de la CA.

El certificado raíz de la CA se crea usando el siguiente comando:

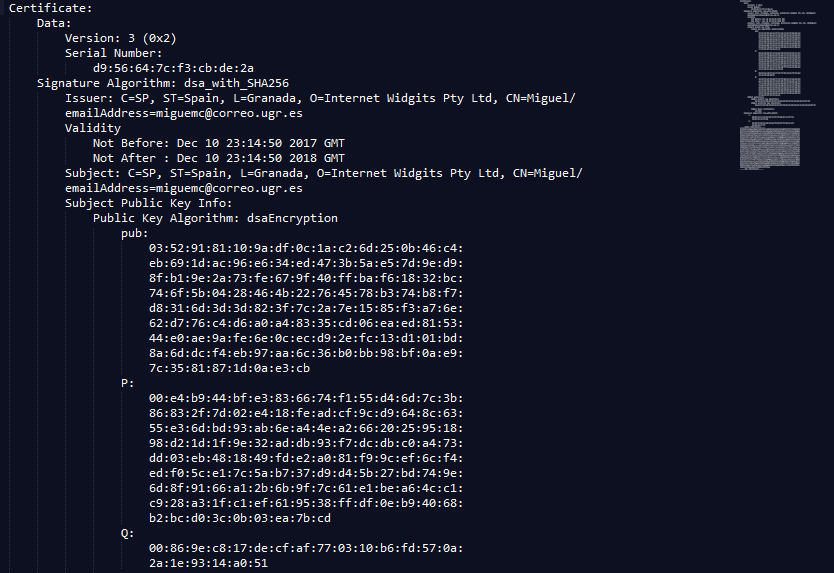
req -config openssl.cnf \

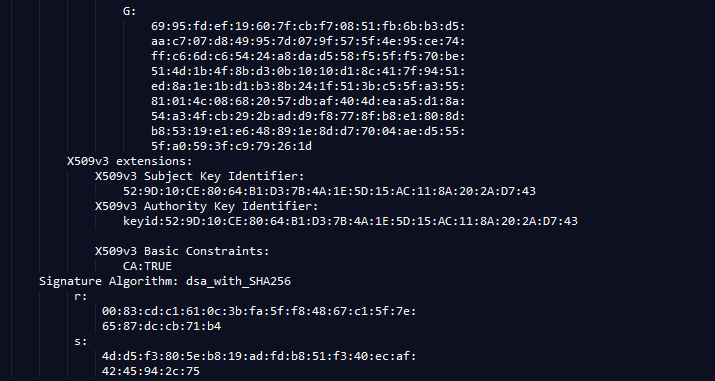
-key private/ca.key.pem \

-new -x509 -days 365 -sha256 -extensions v3\_ca \

-out certs/ca.cert.pem

Como key hemos usado una clave DSA de la práctica 3, la salida es la siguiente:



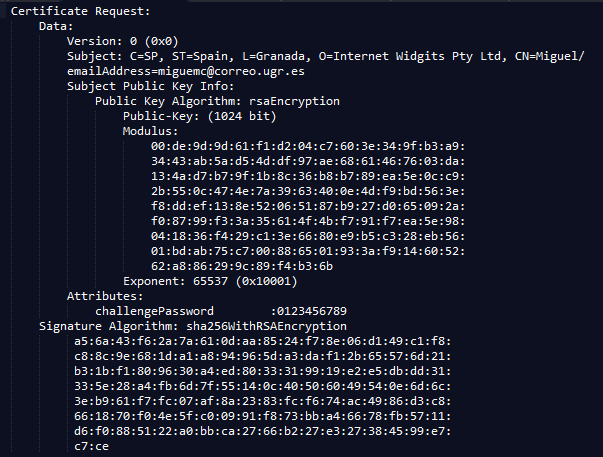


1. Cread una solicitud de certificado que incluya la generación de claves en la misma.

Para realizar esto, ejecutamos el siguiente comando:

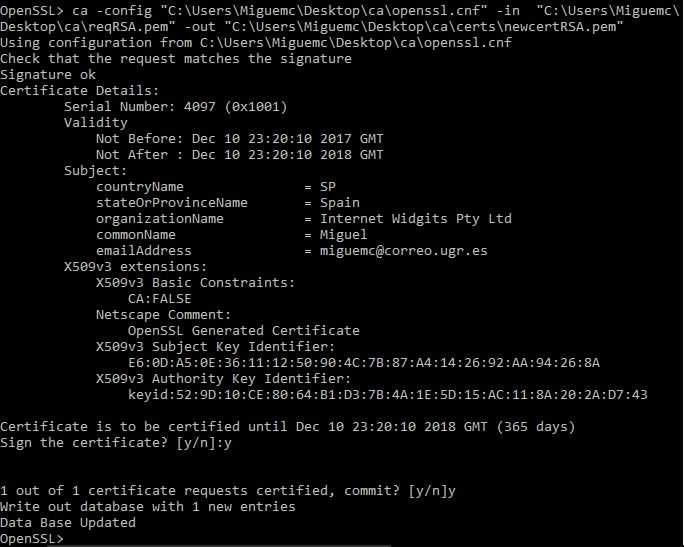
openssl req -newkey rsa:1024 -keyout key.pem -out reqRSA.pem

Tras rellenar las preguntas del DN, la salida es la siguiente:



1. Cread un certificado para la solicitud anterior empleando la CA creada en el primer punto

Para este apartado, lo que nos pide es que nuestra CA firme la solicitud, esto se hace de la siguiente forma:

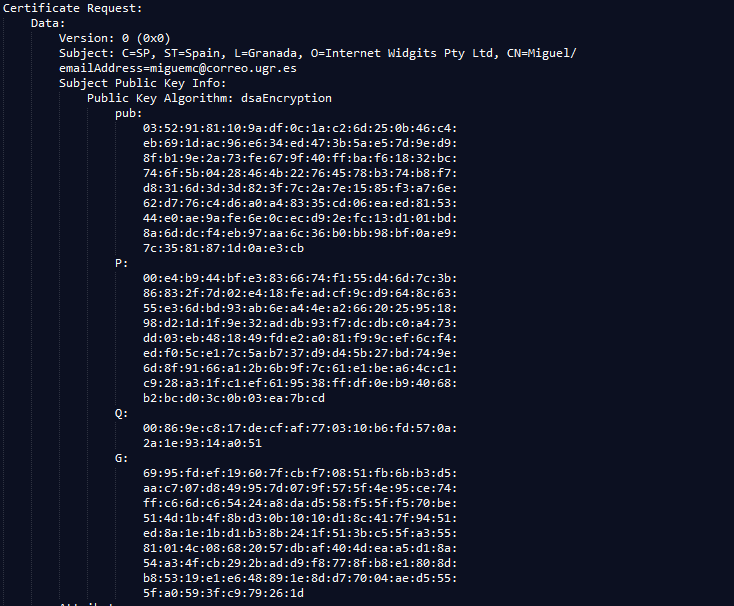


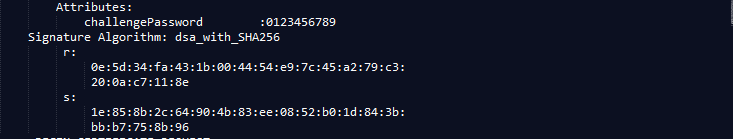
1. Cread una solicitud de certificado para cualquiera de las claves que habéis generado en las prácticas anteriores, excepto las RSA.

Repetimos el proceso del apartado 2 pero cambiando el flag correspondiente a la key. La key usada es miguelDSA.pem de la práctica 3, el comando quedaría así:

openssl req -config openssl.cnf –key miguelDSA.pem -text -new -out req.pem

La salida producida es la siguiente:





1. Cread un certificado para la solicitud anterior utilizando la CA creada.

Repetimos el proceso del apartado 3.

