UAM Universidad Autónoma de Madrid

Servicios de sellado de tiempo

En este ejercicio vamos a realizar el sellado de tiempo de un fichero utilizando algunos de los servicios gratuitos que pueden encontrarse en Internet. Para ello:

a) Selecciona algún fichero cuya existencia quieras certificar para siempre. Por ejemplo, alguna foto o documento PDF.
b) Visita la página de FreeTSA y echa un ojo a las distintas certificaciones. ¿Qué tipos de hash utilizan?
c) Generemos manualmente la petición de certificación (Timestamp Query, TSQ):

```
# openssl ts -query -data [fichero] -cert -no_nonce -sha512 -out
tsa_request.tsq
```

d) Enviamos ahora la petición a la TSA, y recibimos la respuesta:

```
# curl -H "Content-Type: application/timestamp-query"
--data-binary '@tsa_request.tsq' https://freetsa.org/tsr >
tsa_response.tsr
```

e) Verifica ahora el sellado en la opción 'Online Signature', o manualmente:

```
# openssl ts -reply -in tsa_response.tsr -text
```

f) Finalmente podríamos verificar la existencia del documento incluso si la TSA ha desaparecido o está temporalmente caída. Para ello necesitaremos el certificado con el que firmaba las respuestas:

```
# wget https://www.freetsa.org/files/tsa.crt -O freetsa.crt
# openssl ts -verify -queryfile [fichero] -in tsa_response.tsr
-CAfile freetsa.crt -untrusted freetsa.crt
```

Homework

g) Conéctate ahora a TrueTimeStamp y realiza el mismo proceso de creación y verificación de un fichero