Laboratorio 3
Criptografía y Seguridad Informática

Jorge Rodríguez Fraile, 100405951

OpenSSL

1. Parte Linux/Windows

Cuestiones:

a) ¿Para qué se usa el fichero “serial”?

Almacena el numero de serie de los certificados que va generando.

b) ¿Para qué se usa el fichero “index.txt”?

Almacena los certificados, uno por línea, a modo de base de datos.

c) ¿Podría AC2 crear su certificado utilizando el paso 2 de este guión?

Podría autoformarse, pero no debería ya que solo lo debe hacer la autoridad raíz porque nadie superior le puede firmar, sin embargo, a AC2 le puede certificar y debe AC1.

d) Si su grupo de prácticas se convirtiera en una Autoridad de Certificación de verdad, explique razonadamente (i.e. ventajas, inconvenientes, otras alternativas razonables, etc.) qué valor le pondría a cada uno de los siguientes parámetros de su política de certificación: default_days, default_crl_days, countryName.

Default_days: Un valor muy largo es peligroso (compromiso de la clave)

pero uno muy corto es impráctico (caduca muy rápido)

Default_crl_days: Lo más corto posible

countryName: si ponemos un match, evitamos que nos hagan solicitudes

válidas de otros países (lógico para la FNMT, por ejemplo) La Autoridad Pública de Certificación CERES de la FNMT-RCM

13. Acceda a su página web http://www.cert.fnmt.es/home.

14. Consulte el manual de solicitud de certificado de persona física, accesible en esta

dirección web: http://www.cert.fnmt.es/documents/10445900/10528353/solicitud_certificado_persona_fisica.pdf

15. Consulte el documento de “Declaración General de Prácticas de Certificación” https://www.sede.fnmt.gob.es/documents/10445900/10536309/dgpc.pdf

Cuestiones

e) ¿Qué es CERES, qué tipo de certificados ofrece y cuáles son los servicios que oferta?

Es una iniciativa puesta en marcha por la Administración, liderada por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), que consiste en establecer una Entidad Pública de Certificación que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

Tipos de certificado: Persona física, Certificado de Representante, Administración Publica y Certificado de componente.

Servicios: La FNMT-RCM a través del departamento CERES ofrece una serie de servicios a ciudadanos, empresas y administraciones públicas que permiten la implementación de los sistemas que permiten la realización de transacciones telemáticas.
A continuación se expone la relación de servicios esenciales de certificación:

Emisión, renovación y revocación de certificados de usuario, de representación para administradores únicos y solidarios, de persona jurídica y de entidad sin personalidad jurídica de la FNMT-RCM. Certificados de empleado público.

1. Revocación on-line y a través de call center.
2. Servicio de call center. Existe un servicio de atención telefónica al usuario, en las cuatro lenguas oficiales del Estado.
3. Verificación del estado del certificado propio en el web.
4. Registro de usuarios:
    - Aplicación de registro web.
    - Registro a través de las oficinas habilitadas por Organismos de la Administración.
    - Registro a través de personal de la FNMT-RCM a petición de la empresa solicitante de los servicios de certificación, en los centros u oficinas que se determinarán a tal fin.
5. Servicio de verificación de la validez de los certificados electrónicos
    - OCSP.
    - URL/HTTP (excepto AC FNMT Usuarios).
    - Servicio de directorio LDAP.
    - Consulta de CRLs.
    - Servicio de réplica del directorio.
6. Servicio de sellado de tiempo cualificado.
7. Certificados de servidor SSL (estándar, wildcard y multidominio), sello de entidad, sede electrónica, sello electrónico.
8. Registro de eventos significativos relacionados con su propia actividad y la de los usuarios del sistema.
9. Publicación de políticas y normas técnicas, así como información administrativa relacionada con los servicios ofrecidos.

f) ¿Cuándo se inicia el procedimiento para solicitar un certificado de clave pública de persona física, dónde se generan las claves pública y privada?

En el ordenador del usuario, en caso de disponer de HW criptográfico adecuado, en éste, si no es el caso, en el navegado

g) ¿Puede el usuario elegir el tamaño de las claves que se acreditarán en dicho certificado?

Si.

h) ¿Para qué sirve la dirección de correo solicitada durante el proceso de generación de la solicitud de dicho certificado?

Para recibir el código identificativo de la solicitud de certificado.

i) ¿Qué es necesario presentar en la oficina de registro y con qué propósito una vez se ha solicitado el certificado de clave pública de persona física a través de Internet?
Tras haber obtenido el código de solicitud, deberá personarse en una oficina de registro para acreditar su identidad. Ha de ser el propio solicitante, futuro suscriptor y
titular del certificado quien deberá acudir personalmente a una oficina de registro a acreditar su identidad. En el caso de que no pudiera hacerlo por cualquier circunstancia, podrá ir una tercera persona en su nombre, pero previa legitimación de la firma ante notario.
Documentación necesaria para una persona física, deberá presentar:
- DNI o tarjeta de residencia (NIE) para los ciudadanos extracomunitarios.
- Los ciudadanos comunitarios que no tengan la tarjeta de residencia,
presentaran el "Certificado de Registro de Ciudadanos de la Unión y su Pasaporte".”

j) ¿Qué condiciones se le exigen al usuario para poder descargar correctamente el certificado de clave pública de persona física?

Para descargar el certificado debe usar el mismo ordenador, el mismo navegador y el mismo usuario con el que realizó la Solicitud. Si usted ha extraviado su código de solicitud, deberá solicitar un nuevo código y hacer el proceso de acreditación de nuevo.

k) ¿Se realiza una copia de seguridad de las claves privadas (“Datos de creación de firma”) de la Autoridad de Certificación de la FNMT-RCM?

116. Cuando los Datos de creación de Firma se encuentran fuera del dispositivo criptográfico, se encuentran asimismo protegidos por los mecanismos criptográficos necesarios para procurar su Confidencialidad ante ataques basados en criptoanálisis.

117. Las operaciones de copia, salvaguarda o recuperación de los Datos de creación de Firma se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

118. Se mantiene una copia de los ficheros y componentes necesarios para la restauración del entorno de seguridad del dispositivo criptográfico, para el caso de que haya que hacer uso de ellos, en sobres de seguridad debidamente custodiados dentro de un armario ignífugo, que solo pueden ser obtenidos por personal autorizado

l) ¿Cómo se distribuye la clave pública de las AC a las partes que confían y que tamaño tienen las claves y que algoritmos utilizan?

m) Los pasos que tiene que seguir un ciudadano para obtener un certificado de clave pública emitido por la Fábrica Nacional de Moneda y Timbre vienen resumidos en la siguiente tabla. Rellene la tabla, que sirve para relacionar cada

uno de esos pasos con los realizados en esta práctica: para cada paso de ese proceso, indique en qué punto de esta práctica se ha realizado.

Paso	**Descripción**	**Punto de este guión en que se ha realizado**
1	Crear un par de claves (pública y privada) y envío de la solicitud de certificado	2, 4 7
2	Personarse en una oficina de registro	No se hace
3	Generación del certificado de clave pública de acuerdo a las políticas	8 y 9
4	Descargarse el certificado	10