Curs 2021-2022

Pràctica 2. Gestió de certificats

1 Informació important

Sessions dedicades a la pràctica:
24 i 31 de març, i 7 d'abril

Data de validació:
28 d'abril

Data de lliurament:
1 de maig (fins les 23:59)

Objectes d'avaluació per aquesta pràctica:

1. **Informe** en PDF que reculli les respostes a totes les preguntes o qüestions formulades a l'enunciat. L'informe ha de seguir les següents consideracions:
   (a) El nom del fitxer ha de ser *GIS_{A,B,C,D,E}{1..12}_P2.pdf*.
   (b) En la capçalera cal indicar, clarament, el codi grup (i.e. GIS_{A,B,C,D,E}{1..12}), els noms dels integrants del grup i el NIU corresponent.
   (c) L'**extensió màxima** de l'informe és de **10 pàgines**. Sobrepassar aquesta extensió pot comportar penalitzacions en la nota de la pràctica.

L'arxiu s'ha de lliurar per l'Aula Moodle a través d'una tramesa que s'obrirà a tal efecte. Només cal realitzar un lliurament per equip de treball, especificant el nom dels integrants de l'equip en els comentaris de la tramesa.

Consideracions addicionals:

- No només s'avaluarà el contingut tècnic de l'informe sinó que també s'avaluarà la redacció i estil del document.
- Qualsevol intent de copia serà penalitzat amb una qualificació de **0 punts** per tots els grups implicats.
- En cap cas s'acceptaran entregues fora dels terminis establerts.

2 Introducció

En aquesta pràctica veurem com gestionar els certificats digitals. Concretament, veurem el procés de generació de les claus, creació de nous certificats, revocació de certificats existents i l'ús de certificats per a configurar un servidor segur HTTPS.

2.1 OpenSSL

Per a realitzar aquesta activitat només caldrà tenir instal·lat el programari `OpenSSL`[1]. OpenSSL es pot instal·lar en qualsevol sistema operatiu basat en Linux, Mac OS i Windows. La majoria de sistemes Linux el porten instal·lat per defecte i, en cas contrari, es pot instal·lar fàcilment a través de les eines típiques de gestió de paquets (p.ex. `apt-get`).

Per tenir un cert ordre en la gestió de certificats, es recomana seguir la següent estructura de directoris i fitxers:

- certs: directori on es guardaran els certificats
- csr: directori on es tindran les sol·licituds de certificats.
- private: directori per emmagatzemar els fitxers de les claus.
- crl: directori per contenir els certificats revocats.
- newcerts: directori on es tindran els nous certificats signats.
- index.txt: fitxer amb l'índex de certificats signats.
- serial.txt: fitxer que conté el numero de serie de certificats firmats.
- crlnumber.txt: fitxer que conté el numero de serie de certificats revocats.
- openssl.cnf: fitxer que conté les opcions de configuració per defecte.

Creeu l'estructura anterior dins d'un directori específic per a la pràctica en qüestió.

Els fitxers *serial.txt* i *crlnumber.txt* han de contenir el valor "01", i el fitxer *index.txt* ha d'estar buit.

Adjunt a aquest enunciat trobareu un fitxer *openssl.cnf*, copieu-lo en el vostre directori base.

Les instruccions per realitzar els passos anteriors són:

```
mkdir certs crl crlnumber csr newcerts private
touch index.txt
echo "01"> serial.txt
echo "01"> crlnumber.txt
```

2.2 Fitxers de la pràctica

Els fitxers que composen l'enunciat d'aquesta pràctica són:

- Enunciat en format PDF.
- Fitxer de configuració de OpenSSL ("openssl.conf")
- Fitxer amb el certificat de la CA ("ca.crt") per validar els testX.crt
- Quatre fitxers amb certificats ("test1,2,3,4.crt")

[1] https://www.openssl.org/

3 Creació i gestió de certificats

3.1 Creació de la CA

Exercici 1.- Generar les claus (0.5p)

Per generar les claus primer generarem una llavor aleatòria de 512 bits amb la comanda `rand`, guardant-la en el fitxer *randFile*.

A continuació, cal generar una clau privada de 2048 bits i desar-la en un fitxer de claus, que tindrà el nom de *ca.key*. El generarem amb la comanda `genrsa` i usant el fitxer *randFile*.

Aquest dos fitxers han d'estar guardats dins del directori *private*.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu emprat per generar la llavor aleatòria i les claus, indicant el significat de cadascun dels paràmetres que heu fet servir.
b. Verifiqueu que la clau generada és correcta emprant l'eina OpenSSL.
c. Visualitzeu el fitxer de claus que heu generat emprant l'eina OpenSSL i comenteu la informació que es mostra de la clau.

Exercici 2.- Crear un certificat auto-signat (0.5p)

Ara hem de crear un certificat auto-signat de validesa 60 dies, amb el nom *ca.crt* usant la comanda `req` i la clau creada anteriorment.

Nota: En el fitxer *openssl.cnf* del vostre directori heu d'adequar els paràmetres:

- dir
- certificate
- crl
- privatekey

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per generar el certificat, indicant el significat de cadascun dels paràmetres que heu emprat.
b. Visualitzeu el certificat que heu generat i comenteu la informació que us mostra l'eina OpenSSL.

3.2 Creació dels certificats

Exercici 3.- Crear sol·licituds de certificats (1p)

Els fitxers CSR (*Certificate Signing Request*), són sol·licituds de persones o institucions, que un cop firmats per una CA seran certificats que ja podran ser utilitzats.

Creeu un parell de sol·licituds de certificat amb els noms *client1.csr* i *client2.csr* usant la comanda `req` i les claus *client1.key* i *client2.key*, que haureu de crear prèviament amb un tamany de 1024 bits.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per generar les claus i les peticions de certificat, indicant el significat de cadascun dels paràmetres que heu emprat.
b. On s'haurien de guardar aquest fitxers per mantenir un cert ordre?
c. Quina funció *hash* utilitza sinó li especifiquem cap?
d. Verifiqueu que la sol·licitud generada és correcta emprant l'eina OpenSSL.

Exercici 4.- Signar els certificats (1p)

Un cop la CA rep un CSR d'un client, es pot procedir a firmar-lo.

Firmeu els CSRs que heu creat amb el nom *client1.crt* i *client2.crt*, utilitzant la comanda `ca`. El certificat del "client1" cal que tingui una validesa de 1 any, mentre que en el cas del "client2" limitarem la seva validesa a 30 dies.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per signar les peticions de certificat, indicant el significat de cadascun dels paràmetres que heu emprat.
b. Quins fitxers s'han creat un cop signats els certificats?

Exercici 5.- Verificar els certificats (1p)

En aquest exercici comprovarem la validesa d'un conjunt de certificats que no hem creat nosaltres.

Per aquesta tasca, farem servir el certificat de la CA ("ca.crt") i els quatre certificats ("test1,2,3,4.crt") inclosos en l'enunciat d'aquesta activitat.

Activitat

Responeu a les següent qüestions:

a. Comproveu la validesa dels certificats *testX.crt* adjunts a aquest enunciat. En cas de no ser vàlids expliqueu què els hi passa.

3.3 Procés de revocació de certificats

Exercici 6.- Revocar certificats (1p)

Pot ser que algun dels certificats signats ja no es consideri fiable; ja sigui perquè es creu que li han robat la clau, s'ha fet un canvi de nom,... Això donarà pas a que la CA revoqui un certificat.

Revoqueu el certificat *client2.crt* que heu signat. Per això s'ha d'usar la comanda `ca`.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per revocar el certificat, indicant el significat de cadascun dels paràmetres que heu emprat.
b. S'ha modificat algun dels fitxers que mantenen les llistes dels certificats? En cas afirmatiu, comenteu quin fitxer ha estat i les modificacions introduïdes pel procés de revocació.

Exercici 7.- Llista de certificats revocats (1p)

Per tal que els usuaris sàpiguen quin certificats han estat revocats hem de crear una llista de certificats revocats CRL.

Creeu la llista en el fitxer *list.crl*.

Revocar un certificat no és una feina molt complicada, la part laboriosa és difondre la llista de certificat revocats pels diferents usuaris que hagin utilitzat el certificat revocat.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per generar la llista de revocació dels certificat, indicant el significat de cadascun dels paràmetres que heu emprat.
b. Comproveu la llista de revocació i mostreu els resultats, tot comentant la informació que ens proporciona OpenSSL.

3.4 Exportació de certificats i claus associades

Exercici 8.- Exportar i importació de certificats i claus associades (1p)

Abans de poder incloure en un navegador un certificat i la seva clau privada associada s'ha d'exportar tota la informació en un sol fitxer en format PKCS12 amb la comanda `pkcs12`.

Creeu el fitxer *client1.p12* amb el certificat digital i la clau privada associada. Aquest fitxer ha de contenir també el certificat de la CA signant.

Activitat

Responeu a les següent qüestions:

a. Indiqueu les comandes que heu fet servir per exportar certificat i la corresponent clau privada, indicant el significat de cadascun dels paràmetres que heu emprat.
b. Comproveu el contingut del fitxer PKCS12 i mostreu els resultats, tot comentant la informació que ens proporciona OpenSSL.

Importeu a un navegador o a un sistema operatiu qualsevol el fitxer PKCS12 amb el certificat i la seva clau privada associada.

Activitat

Responeu a les següent qüestions:

a. Indiqueu els passos que heu fet per a importar el fitxer p12.

b. Mostreu una captura de pantalla amb la informació que us mostra del certificat, explicant els principals camps i la informació que contenen.

4 Aplicacions pràctiques amb certificats digitals

En aquesta segona part de la pràctica, veurem aplicacions pràctiques dels certificats digitals basats en clau asimètrica.

A diferència de la primera part d'aquesta pràctica, la segona part no és guiada; sinó que en aquest cas esperem que poseu en pràctica els coneixements adquirits en la primera part de forma autònoma.

4.1 Creació i configuració d'un certificat HTTPS

En aquesta segona part, crearem unes claus i un certificat mitjançant l'eina OpenSSL i configurarem el servidor web Apache per a poder oferir servei HTTPS.

Exercici 9.- Crear i instal·lar el certificat (2p)

En primer lloc, cal que creeu una autoritat de certificació (CA) amb el nom "CA-UAB", localitat "Barcelona" i país "Espanya". Utilitzarem aquest certificat per a crear un segon certificat vàlid per a un servidor web. Cal indicar el nom del grup "gis_{A,B,C,D,E}_{1, . . . , 12}" en el certificat del servidor web.

Una vegada creat el certificat, caldrà instal·lar-lo en el servidor web Apache. En aquest cas hi ha dues opcions per accedir al servidor web:

- Sistema Linux de l'estudiant: Tots els estudiants que tingueu un sistema Linux, podeu utilitzar-lo per aquesta part de la pràctica. Qualsevol sistema Linux sol incorporar el servidor Apache, o en cas contrari, permet descarregar-lo i instal·lar-lo de forma senzilla.
- Màquina virtual: Es poden trobar multitud de imatges de màquines virtuals per la xarxa, de tal forma que només cal descarregar una de les imatges i executar-la en la plataforma de virtualització. Per exemple, podem utilitzar el software Virtual Box[2] (gratuït) i descarregar alguna de les diferents imatges que podem trobar en la següent URL: http://virtualboxes.org/images/

Notes:

- Un servidor web, per defecte, escolta pel port 80/TCP utilitzant el protocol HTTP.
- Quan es configura per funcionar emprant SSL, el protocol s'anomena HTTPS i el port per defecte que se sol utilitzar és el 443/TCP.
- El fitxer de configuració del servidor web Apache s'anomena *httpd.conf* i es pot trobar en diferents ubicacions segons la distribució i versió del sistema Linux. Per exemple, */etc/httpd/conf/httpd.conf* en sistemes Red Hat o */etc/apache2/apache2.conf* en sistemes Ubuntu. En qualsevol dels casos, trobareu molta informació a la xarxa sobre on localitzar els fitxers de configuració i quins paràmetres cal modificar per a la seva correcta configuració.

[2] https://www.virtualbox.org/

Activitat

Responeu a les següent qüestions:

a. Indiqueu els passos que heu dut a terme per crear el certificat de la CA i el certificat del servidor web.
b. Indiqueu els passos que heu seguit per a configurar el certificat en el servidor web Apache.
c. Mostreu una captura de pantalla que mostri que el servidor web Apache està responen en el port 443 (HTTPS).
d. Mostreu una captura de pantalla del navegador web on es vegi el detall del certificat. Mostra algun avís o error el navegador web? En cas afirmatiu, indiqueu l'error, la causa i una possible solució al problema.

4.2 Disseny d'un sistema de llicències de software

En aquesta segona part, dissenyarem i construirem un sistema de validació de llicències de software basat en claus públiques i privades, emprant l'eina OpenSSL.

Exercici 10.- Disseny del sistema de llicències de software (1p)

Una empresa que es dedica a la creació de software vol crear un sistema de llicències per a validar el seu programari. Aquest programari s'executa en un servidor i permet que múltiples clients es connectin a ell per treballar de forma concurrent.

Els clients poden adquirir llicències per un determinat nombre de connexions concurrents i per a una determinada durada.

Per tant, cada "certificat" ha d'incloure, com a mínim, la següent informació:

- Un identificador únic del servidor del client (per evitar que una mateixa llicència es pugui copiar en diferents servidors).
- Un nombre enter que indica el nombre màxim de connexions que pot permetre el servidor.
- Una data inicial i una data final, que determinen el període en el qual la llicència és vàlida.

Aquesta informació es pot emmagatzemar de diferents maneres, per exemple en un fitxer de text pla, un document estructurat o semi-estructurat (tipus XML o JSON).

Activitat

Responeu a les següent qüestions:

a. Dissenyeu un sistema que permeti validar les llicències de programari segons els paràmetres descrits anteriorment. Expliqueu-ne el funcionament, indicant clarament quins ítems són necessaris per cada entitat ()claus, certificats, etc).
b. Indiqueu els passos que seguiria l'empresa per a generar una llicència de software per a un client concret, suposant 10 connexions simultànies i un període de validesa fins al 31 de desembre de l'any en curs.
c. Indiqueu els passos que seguiria l'aplicació per validar la llicència de software.
d. Finalment, caldria que us plantegéssiu possibles atacs que es poden fer contra el vostre sistema de llicències de programari, i indicar per cada cas, com es comporta el sistema. Per exemple, us heu de plantejar coses som "seria possible que un client fraudulent utilitzés la llicència d'un client legítim?" o "seria possible que un client fraudulent generés els seus propis certificats i enganyés al programari?".

Notes:

- En aquest exercici **no cal implementar el sistema**, només es demana pensar i dissenyar un possible sistema de validació de llicències de programari emprant certificats digitals.

5 Annex 1: Comandes de OpenSSL

Es pot obtenir una completa ajuda de OpenSSL a través de la comanda *man openssl* del sistema Linux.

```
asn1parse Parse an ASN.1 sequence.
ca        Certificate Authority (CA) Management.
ciphers   Cipher Suite Description Determination.
cms       CMS (Cryptographic Message Syntax) utility
crl       Certificate Revocation List (CRL) Management.
crl2pkcs7 CRL to PKCS#7 Conversion.
dgst      Message Digest Calculation.
dh        Diffie-Hellman Parameter Management.  Obsoleted by dhparam.
dsa       DSA Data Management.
dsaparam  DSA Parameter Generation and Management. Superseded by genpkey and pkeyparam
ec        EC (Elliptic curve) key processing
ecparam   EC parameter manipulation and generation
enc       Encoding with Ciphers.
engine    Engine (loadble module) information and manipulation.
errstr    Error Number to Error String Conversion.
gendh     Generation of Diffie-Hellman Parameters.  Obsoleted by dhparam.
gendsa    Generation of DSA Private Key from Parameters. Superseded by genpkey and pkey
genpkey   Generation of Private Key or Parameters.
genrsa    Generation of RSA Private Key. Superceded by genpkey.
nseq      Create or examine a netscape certificate sequence
ocsp      Online Certificate Status Protocol utility.
passwd    Generation of hashed passwords.
pkcs12    PKCS#12 Data Management.
pkcs7     PKCS#7 Data Management.
pkey      Public and private key management.
pkeyparam Public key algorithm parameter management.
pkeyutl   Public key algorithm cryptographic operation utility.
rand      Generate pseudo-random bytes.
req       PKCS#10 X.509 Certificate Signing Request (CSR) Management.
rsa       RSA key management.
rsautl    RSA utility for signing, verification, encryption, and decryption. Superseded by  pkeyutl
s_time    SSL Connection Timer.
sess_id   SSL Session Data Management.
smime     S/MIME mail processing.
speed     Algorithm Speed Measurement.
spkac     SPKAC printing and generating utility
ts        Time Stamping Authority tool (client/server)
verify    X.509 Certificate Verification.
version   OpenSSL Version Information.
x509      X.509 Certificate Data Management.
```