CS – 2024

Lab 3: Certificats

1 Introducció

En aquesta pràctica treballarem el concepte de certificat digital i veurem les conseqüències de l'ús de funcions hash insegures en l'ús de certificats. A més, explorarem l'ús de certificats digitals en esquemes d'autenticació.

1.1 Informació important

Per a aquesta pràctica cal lliurar dos fitxers: un informe i un fitxer comprimit en zip amb el codi que hagueu fet servir.

L'informe ha de seguir les següents consideracions:

- L'**informe** ha d'estar en format PDF i ha de recollir les respostes a totes les preguntes o qüestions formulades a l'enunciat.
- En la capçalera cal indicar, clarament, els noms dels integrants del grup i els NIUs corresponents.
- Per cada activitat de la pràctica, cal incloure: una petita descripció de la solució plantejada i el resultat de l'activitat. Per a les activitats en què cal enviar correus, proporcioneu tant el correu enviat com la resposta rebuda pel servidor.

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 grup de treball.

2 Activitats

2.1 Part 1: Obtenció d'un certificat legítim

1. El sistema d'autenticació del professorat i l'alumnat de la UAB està basat en certificats. Els professors i els alumnes disposen d'uns certificats que tenen els següents camps:
   - **Identitat** (*subject name*): el correu institucional de la persona (per exemple, `John.Doe@uab.cat`).
   - **Professió:** cadena de caràcters (format lliure).
   - **Clau pública:** clau pública RSA.

   Creeu un parell de claus RSA (pub1, priv1) en format OpenSSH.

   Creeu-vos un certificat fent servir un editor de text convencional amb l'estructura prèviament descrita i les vostres dades. El certificat ocuparà una única línia i els camps se separaran pel símbol %.

2. Per fer aquests certificats més segurs, a la UAB han creat una **autoritat de certificació** amb identitat CA-UAB i la següent clau pública RSA:

   ```
   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAlw0VcSQVWZhgYMvGqLjueutYCIX2YxWrtH1YO3JdD
   VEObclxIbKfX1YfXJ6N4QVYMUAxb+/0TXTrDSF13YE2kA2SqJ6si1LrrCPm4dbYgsrOLCvKfuYwti
   ICsFdjwpgixQ/kJQMAInNil/psK7MxvSS7Dfv8T88+49yYujMIrj6VN9O5Huc5baCPZRC8x6q/OGc
   55RlO/8O=
   ```

   Aquesta Autoritat de Certificació completa els certificats anteriorment descrits amb els següents camps:

- **Identitat de la persona signant** (*issuer name*): CA-UAB, en el nostre cas.
- **Clau pública de la identitat signant:** clau pública anteriorment descrita.
- **Data d'expiració:** 3 anys a partir del moment la signatura en format dd/MM/YYYY HH:MM:SS.
- **Signatura:** signatura fent servir l'expressió $Ek_{priv}(h(m))$, on $h(x)$ correspon al SHA256 de m podat (els 16 primers bits es mantenen i la resta es fixen a 0), *priv* la clau privada del signant i m el missatge (certificat complet, sense signatura, amb tots els camps anteriors separats per % en una única línia). *Ek* fa servir l'esquema de pàdding PKCS #1 v1.5 i la signatura es codifica en base 64.

Un exemple de certificat complet seria (una única línia):

```
marta.garcia@uab.cat%Estudiant%ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAlw1l/iuC4c9
NEloKbyG2A8NexmqfAr/y38H2tWoWMaS42Hzonlx6UaCVK7lNm6xpMVsMKrPO5Yhv/45dJH4a8Dt+9
GYmi0vJRlvgZp7v70usYV5j11Dht06XwReXgZ/Cor78sH5XLikb7P+vN43xbGZCb7ZmZKP3GzMzNip
Ly8dlHFfnEPrHmr8bS5hKAdp3eRUkatCSwWc=%CA-UAB%ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA
AAAlw0VcSQVWZhgYMvGqLjueutYCIX2YxWrtH1YO3JdDVEObclxIbKfX1YfXJ6N4QVYMUAxb+/0TXT
rDSF13YE2kA2SqJ6si1LrrCPm4dbYgsrOLCvKfuYwtiICsFdjwpgixQ/kJQMAInNil/psK7MxvSS7D
fv8T88+49yYujMIrj6VN9O5Huc5baCPZRC8x6q/OGc55RlO/8O=%24/10/2026 19:49:54%AtaT75
/SIO0k9/kohe0rYoGUcHRBW7JVywNHhsg4AvAqhGv3JDhHUXnP8CXB8u0HG+UtfVpHF57jVDl8pGYh
9tYAHvH/7N/rBHqzv5FH0l0oybB5BBOoZWQCwAwGDCTL2mUx8Vmx8gI3Y9lpqAknwcNxhgmoA5tw3/
h5i8HDgU6am8y40+ke0oC0lGjvMVgIPvbAc6TIog==
```

El procediment per demanar la signatura d'un certificat és enviar un correu, des del correu institucional de la UAB a l'adreça de la CA-UAB (`ca-uab-sign@eines.uab.es`). **El tema del correu (*subject*) ha d'incloure la cadena de caràcters** `CA-SIGN`, indicant a la CA que esteu sol·licitant un nou certificat. El cos del missatge ha de ser text pla i ha d'incloure el certificat parcial (identitat del subjecte, professió i clau pública) tal com l'heu creat a l'exercici anterior (en una sola línia, amb els camps separats per %).

La CA-UAB comprovarà que la identitat del treballador/estudiant relacionat amb l'adreça d'origen del correu electrònic coincideix amb el camp Identitat del certificat. Si és així, el signarà, i l'enviarà al seu propietari.

Demaneu a la CA-UAB que us signi el vostre certificat amb identitat el vostre correu institucional.

2.2 Part 2: Tripijocs amb un certificat il·legítim

L'assignatura Criptografia i Seguretat cada vegada és més difícil d'aprovar. Una manera que han trobat unes alumnes de l'assignatura és aconseguir un certificat del professorat de l'assignatura que estigui signat amb la CA de la UAB. Els estudiants han pogut fer servir aquest certificat per enviar un correu electrònic autenticat a `canvi-de-notes-uab@eines.uab.es` i canviar la seva nota.

3. Aconseguiu un certificat signat per la CA-UAB que tingui com a identitat (*subject name*) el correu d'un membre del professorat de l'assignatura (`carlos.borrego@uab.cat` o `cristina.perez@uab.cat`).

   Recordeu que la CA-UAB només signa els certificats en què la identitat del subjecte coincideix amb l'origen del correu, de manera que no podeu demanar aquest certificat a la CA-UAB.

4. Feu servir el certificat obtingut a l'exercici anterior per canviar la vostra nota de l'assignatura. Per fer-ho, envieu un correu a l'adreça `canvi-de-notes-uab@eines.uab.es`. **El tema del correu (*subject*) ha d'incloure la cadena de caràcters** `GRADE-CHANGE`, indicant que esteu sol·licitant un canvi de notes. El cos del missatge ha de ser text pla i ha de tenir 3 línies:

   - Una línia delimitada per coixinets (`#`) indicant la nova nota. Per exemple, `#CHANGE GRADE TO 10#`.
   - Una línia amb el certificat complet (en el mateix format que el retorna la CA-UAB, és a dir, amb els camps separats per %).

- Una línia delimitada per dòlars ($) amb la signatura del missatge de canvi de notes. La signatura farà servir la mateixa expressió que la signatura del certificat: $Ek_{priv}(h(m))$, on $h(x)$ correspon al SHA256 de m podat (els 16 primers bits es mantenen i la resta es fixen a 0), $priv$ la clau privada del signant i m el missatge (que en aquest cas, correspondrà al missatge delimitat per coixinets de la primera línia del correu). Ek fa servir l'esquema de pàdding PKCS #1 v1.5 i la signatura es codifica en base 64. A l'Apèndix A hi trobareu una descripció més detallada de la funció hash i la codificació de la signatura utilitzades, així com un conjunt de vectors de test que us permetran comprovar la vostra implementació.

L'aplicació de canvi de notes validarà que el certificat sigui vàlid, estigui emés per la CA-UAB i que correspongui a una identitat autoritzada per al canvi de notes. També validarà que la signatura del missatge de canvi de notes sigui vàlida (amb la clau pública inclosa al certificat).

Si totes les validacions són correctes, l'aplicació canviarà la nota i respondrà amb un missatge confirmant el canvi.

Pista: Amb l'enunciat de la pràctica us proporcionem el fitxer `sign_message.py` que conté el codi necessari per signar un missatge amb RSA amb les consideracions esmentades a l'enunciat pel que fa al pàdding, la codificació i la variació de la funció hash. Per a executar-lo, cal instal·lar la llibreria `pycryptodome` (us proporcionem també un fitxer de `requirements.txt` amb aquesta dependència).

2.3 Part 3: Dels certificats a la PKI

5. Els certificats X.509 són un estàndard que es fa servir en la majoria de protocols que requereixen certificats digitals. Investigueu quins són els **camps bàsics** que conté un certificat X.509 i indiqueu quins canvis caldria fer als certificats d'aquesta pràctica per tal d'adaptar-los a l'estàndard.

A Vectors de test

A.1 SHA256 podat

La funció hash que es fa servir en aquesta pràctica és una versió *podada* de la funció hash SHA256, que anomenarem SHA256P. La poda consisteix a mantenir únicament els primers 16 bits de la funció hash i deixar la resta de bits a 0.

A continuació es proveeix un vector de test per a la funció SHA256P tal com l'acabem de definir.

```
m:        HELLO WORLD!
SHA256:   bf96648169ba89c284b3e94108074c7d5e5806c7b9498031aceded5ca139ed69
SHA256P:  bf960000000000000000000000000000000000000000000000000000000000000000
```

A.2 RSA amb PKCS #1 v1.5

Les signatures digitals d'aquesta pràctica són signatures RSA seguint l'estàndard PKCS#1 v1.5 per al pàdding i codificades en base 64.

A continuació es proveeix un vector de test per a la funció de signatura tal com l'acabem de definir.

```
m:        HELLO WORLD!
SHA256P:  bf960000000000000000000000000000000000000000000000000000000000000000
PK:       ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAlwy2lKVn+vu7GFPG+um/XSJBrAn77IJkrRSt9Hz
          dMF2FWrVSHLMDZhU5kEHGwVNxhw7ARM4vDBsaBtYnMaFBCiSa+ChFMSNCRrvpPeCoJBc+3YhlKm
          9BbUc1XPy7x9Fh3chK5wIkv3q7OwBXSfnUMv1rItcaoLA/2YOdI53LgxpP5y7jZpR5S+RE1as/v
          YyFL+9HqbIZ7G8=
SIG:      BWtroi+ooBIXxLCztI4CeQNfK7H37mq1uhzcqfjB2bKEO37kmFjHAezJr5Hourc4pLaoEjAgbDw
          OVYr9PTj5jwr8ZlzqydwqbrK2HUPMiLJHvObsPCdlg1jdoCDhaehVO1dvJdO+8udpDIv6QrVWom
          YHhH9+OC9sEuNcPdASBKG7OI3PMaf1MSKHwoTbHG3GS3Pe+YHMQg==
```