Certificat digital

La publicació de ROCA: Vulnerable RSA generation (CVE-2017-15361) fa que es replantegi que es faci servir el DNIe per signar correus electrònics.

Per poder signar el correus amb el SHA512 de les pràctiques haurem de crear un parell clau púbica/clau privada i enviar la clau pública a una autoritat certificadora (AC) que crearà un certificat digital per aquesta clau pública. Aquest certificat digital conjuntament amb la clau privada corresponen permetrà la signatura de correus electrònics.

Per generar el parell clau púbica/clau privada podeu fer servir *openssl*[1] i el fitxer de comandes `new-user-cert.sh`. Si executeu[2]:

```
$ new-user-cert.sh direccion_email@est.fib.upc.edu
```

es generaran dos fitxers:

1. `nom.cognom@est.fib.upc.edu.req` amb la petició de certificat,
2. `nom.cognom@est.fib.upc.edu.private_key` amb la clau privada.

La petició de certificat, `nom.cognom@est.fib.upc.edu.req`, s'ha d'enviar a l'AC, en aquest cas s'ha de pujar al Racó.

Si tot és correcte, l'AC emetrà un certificat, `nom.cognom@est.fib.upc.edu.crt`, per la clau pública que trobareu també al Racó.

Per poder importar en el client de correu les claus s'ha de executar:

```
$ cat nom.cognom@est.fib.upc.edu.crt ...
            nom.cognom@est.fib.upc.edu.private_key > certificado+privkey.pem
$ openssl pkcs12 -export -in certificado+privkey.pem -out certificado+privkey.p12
```

La primera ordre guarda en el mateix fitxer la clau privada i el certificat, la segona canvia el format perquè pugui ser importat per diferents aplicacions.

Abans d'importar `certificado+privkey.p12` al gestor de correu és necessari llegir el certificat de l'AC `certificado_ca_curso_2017-2018.pem`.

---

[1] *openssl* està disponible en https://www.openssl.org. En la majoria de les distribucions linux s'instal.la per defecte; en la imatge linux de la FIB ho está.

[2] El fitxer `curva_a_usar_p521` conté la corba elíptica que es fa servir per crear el parell clau púbica/clau privada.