Practica 4

December 20, 2022

1 Connexió a la pagina de la FIB

1.1 Periode de validesa

Ens hem connectat a la pàgina web de la fib i hem investigat quina ha sigut la clau pública utilitzada i quina és la seva data d'expiració.

Hem obtingut una clau de 1233 dígits (en base 10) i que es valida des del dia 28/03/2022 fins al 29/03/2022.

1.2 Política de certificats

Hem accedit a la política de certificats del servidor i hem trobat que tenen vigents dues versions del protocol:

- 1.3.2

  - En aquesta versió donem suport al sistema de xifratge RSA i exigim claus de 2048 bits fins al 2030 i de 3072 a partir de llavors.

  - També done suport al sistema ECDSA de corbes el·líptiques amb una clau de 256 bits

- 5.3.4

  - En aquesta versió també donem suport als dos sistemes vist anteriorment. Per RSA, exigim una clau de 2048 bits i que sigui mòdul 8 en el nombre de bits.

  - Per ECDSA demanem claus que estiguin a les corbes P-256 o P384.

1.3 Certificats Rebutjats

En la connexió que hem realitzat podem trobar un total de 13874 certificats revocats

1.4 Estat del certificat

Hem realitzat una petició a l'OCSP per verificat l'estat del certificat, i quina és la seva data d'expiració si és que era vàlid.

Tal com esperàvem, hem obtingut que el certificat és vàlid, i la seva data d'expiració és el 26 de desembre a les 08:34 del 2022.