

## ECC y certificados digitales – Ex 2

### a) Període de validesa i clau pública

```
(venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ openssl s_client -connect www.fib.upc.edu:443 -servername www.fib.upc.edu -showcerts </dev/null 2>/dev/null \
| awk '/BEGIN CERTIFICATE/{i++} {print > ("cert-" i ".pem")}' \
ls -l cert-*.*.pem
-rw-rw-r-- 1 sara sara 2814 dic 15 21:36 cert-1.pem
-rw-rw-r-- 1 sara sara 2530 dic 15 21:36 cert-2.pem
-rw-rw-r-- 1 sara sara 4511 dic 15 21:36 cert-3.pem
-rw-rw-r-- 1 sara sara 288 dic 15 21:36 cert-.pem
```

El període de validesa del certificat és:

- notBefore: Nov 21 09:18:51 2025 GMT
- notAfter: Nov 21 09:18:51 2026 GMT

```
(venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ openssl x509 -in cert-1.pem -noout -dates
notBefore=Nov 21 09:18:51 2025 GMT
notAfter=Nov 21 09:18:51 2026 GMT
```

La clau pública del certificat del servidor és RSA de 3072 bits, amb exponent públic i mòdul visibles al certificat.

```
notAfter=Nov 21 09:18:51 2026 GMT
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ openssl x509 -in cert-1.pem -noout -text > cert1.txt
grep -n "Public Key Algorithm" -A20 cert1.txt
13:          Public Key Algorithm: rsaEncryption
14:          Public-Key: (3072 bit)
15:            Modulus:
16:              00:d8:70:8c:71:ea:35:e3:4a:b2:15:f3:f8:76:68:
17:              4f:58:8e:62:79:07:80:48:5a:af:06:d3:aa:bf:2e:
18:              c8:ca:2c:b7:27:f1:16:ae:e4:7a:59:a4:b3:90:34:
19:              e7:2f:4d:ee:71:bb:28:c5:bb:d2:a4:35:5d:f7:09:
20:              28:ac:ba:78:3e:3c:aa:62:e9:68:bd:b8:05:e2:4b:
21:              3f:e3:1a:f9:13:60:62:c8:bb:ec:56:54:44:e7:b4:
22:              cf:54:32:cb:47:62:c5:31:13:5a:5c:ac:24:05:3e:
23:              d7:06:20:8c:ae:9a:ea:8b:0a:09:f3:2f:62:f7:ba:
24:              8b:ef:ca:00:f4:1a:ab:68:aa:e1:39:2c:27:2e:8c:
25:              a2:09:06:ce:a4:d0:2f:f7:a5:d3:d8:8b:f2:36:0c:
26:              3e:6d:37:cf:dc:59:e4:2b:ec:35:a2:b3:dd:17:54:
27:              9f:41:dc:10:2b:b6:51:81:72:83:58:40:b1:01:9a:
28:              00:c0:8c:4e:70:da:cc:bc:86:51:2a:0a:21:4a:a1:
29:              46:6d:44:ca:99:41:56:c4:5e:cf:ff:ac:3c:4b:69:
30:              d4:1e:7b:fb:62:c0:87:0d:24:88:5b:5e:ab:7e:8a:
31:              47:2f:3e:38:3b:69:30:55:fa:20:29:14:01:cc:d6:
32:              6b:a0:5d:1e:75:62:32:8f:57:cf:50:cf:de:3d:99:
33:              79:92:cc:f9:33:d0:3c:f7:ea:e2:71:fd:13:7c:58:
```

## b) Signed Certificate Timestamps

Per a cada SCT s'ha obtingut el LogID, la versió i el timestamp.

```
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ grep -n "Signed Certificate Timestamp" -A8 cert1.txt
65:          Signed Certificate Timestamp:
66:            Version : v1 (0x0)
67:            Log ID  : 94:4E:43:87:FA:EC:C1:EF:81:F3:19:24:26:A8:18:65:
68:                           01:C7:D3:5F:38:02:01:3F:72:67:7D:55:37:2E:19:D8
69:            Timestamp : Nov 21 09:28:57.277 2025 GMT
70:            Extensions: none
71:            Signature : ecdsa-with-SHA256
72:                           30:44:02:20:3C:99:EE:C5:27:D8:B4:96:06:01:56:E9:
73:                           FD:00:EC:C9:46:2E:9D:01:71:A2:CF:21:11:EA:00:5D:
74:
75:          Signed Certificate Timestamp:
76:            Version : v1 (0x0)
77:            Log ID  : D8:09:55:3B:94:4F:7A:FF:C8:16:19:6F:94:4F:85:AB:
78:                           B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14
79:            Timestamp : Nov 21 09:28:57.228 2025 GMT
80:            Extensions: none
81:            Signature : ecdsa-with-SHA256
82:                           30:45:02:21:00:98:29:C1:0B:F7:F7:5D:0F:0B:9F:7C:
83:                           FE:70:38:65:35:97:BA:31:44:95:64:B4:D5:33:7D:9E:
84:
85:          Signed Certificate Timestamp:
86:            Version : v1 (0x0)
87:            Log ID  : AC:AB:30:70:6C:EB:EC:84:31:F4:13:D2:F4:91:5F:11:
88:                           1E:42:24:43:B1:F2:A6:8C:4F:3C:2B:3B:A7:1E:02:C3
89:            Timestamp : Nov 21 09:28:57.281 2025 GMT
90:            Extensions: none
91:            Signature : ecdsa-with-SHA256
92:                           30:46:02:21:00:91:24:62:BB:90:01:CB:9E:13:97:E5:
93:                           43:EB:B9:8B:E6:F4:F9:35:37:6D:51:7D:EF:83:F5:A0:
```

## c) DNS

A l'extensió SAN del certificat s'indica que el certificat és vàlid per [www.fib.upc.edu](http://www.fib.upc.edu) i fib.upc.edu.

```
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ grep -n "Subject Alternative Name" -A3 cert1.txt
49:          X509v3 Subject Alternative Name:
50:            DNS:www.fib.upc.edu, DNS:www.fib.upc.es
51:          X509v3 Certificate Policies:
52:            Policy: 2.23.140.1.2.1
```

## d) CRL

La CRL té 13.562 certificats revocats i 468 certificats han estat revocats per Key Compromise.

```
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ grep -n "CRL Distribution Points" -A10 cert1.txt
57:          X509v3 CRL Distribution Points:
58:            Full Name:
59:              URI:http://crl.harica.gr/HARICA-GEANT-TLS-R1.crl
60:          X509v3 Subject Key Identifier:
61:            D3:69:36:3C:77:A6:FA:21:ED:F8:9C:5D:46:59:7A:9E:71:25:57:4D
62:          X509v3 Key Usage: critical
63:            Digital Signature, Key Encipherment
64:          CT Precertificate SCTs:
65:            Signed Certificate Timestamp:
66:              Version : v1 (0x0)
67:              Log ID   : 94:4E:43:87:FA:EC:C1:EF:81:F3:19:24:26:A8:18:65:
```

```
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ grep -c "Serial Number" crl.txt
13562
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ grep -c "Key Compromise" crl.txt
468
```

### e) OCSP (Online Certificate Status Protocol)

Del certificat del servidor obtenim la URL del servei OCSP: <http://ocsp-tls.harica.gr>.

L'estatus és GOOD i és vàlid fins a Dec 18 11:18:18 2025 GMT, tal i com indica el camp NextUpdate.

```
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ openssl x509 -in cert-1.pem -noout -ocsp_uri http://ocsp-tls.harica.gr
● (venv) sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ OCSP_URL=$(openssl x509 -in cert-1.pem -noout -ocsp_uri)
openssl ocsp -issuer cert-2.pem -cert cert-1.pem -url "$OCSP_URL" -resp_text -noverify
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: 8601723F8CA970E231065316CE015F5B79C83C3B
    Produced At: Dec 15 11:18:19 2025 GMT
    Responses:
        Certificate ID:
            Hash Algorithm: sha1
            Issuer Name Hash: 2892028EABFCA4FFDDA1B5EC1474688142C20012
            Issuer Key Hash: 8601723F8CA970E231065316CE015F5B79C83C3B
            Serial Number: 540CB6B83DBB8CEDE1BA201E50FC74BF
        Cert Status: good
        This Update: Dec 15 11:18:19 2025 GMT
        Next Update: Dec 18 11:18:18 2025 GMT

        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            29:fd:c1:bd:58:a1:8:14:bc:54:55:22:d6:62:cc:94:82:ce:
            b7:72:99:6c:58:bf:41:ce:42:9b:d1:62:7d:9d:5a:a8:d8:fd:
            91:50:e7:dc:0f:82:6a:6e:65:32:81:a5:f5:5d:30:54:da:7f:
            0f:47:d9:86:e4:8b:91:07:63:62:a6:c4:96:26:9a:4a:6d:7f:
            a8:ee:46:18:8c:1b:8b:42:bf:a7:a1:b7:a7:9d:34:78:55:be:
            65:af:c3:e1:d8:53:7d:6e:f4:c0:3d:48:7d:12:e7:59:d6:7b:
            f7:4e:c1:cf:bb:fc:60:67:a5:2a:6b:99:ac:ea:30:40:d1:23:
            93:c1:5b:ad:47:1a:53:0c:70:0d:ea:7e:4b:d6:ee:28:e3:77:
            d9:19:f3:54:41:77:c4:43:f5:d7:12:92:eb:e4:47:b0:ef:78:
            62:93:19:0a:5d:45:1a:e8:33:76:5c:a2:e5:1b:91:8e:fb:ca:
            70:6b:79:6c:8d:0a:df:39:37:07:37:09:d4:1b:6a:2c:d2:b1:
            e1:cb:36:b6:49:51:1e:04:f1:1c:78:29:8e:31:80:35:2a:05:
            e1:lc:54:2f:86:7f:35:79:0f:b3:72:16:13:72:d0:59:a2:3f:
            37:b2:7e:c4:2c:47:ca:79:00:b8:34:7d:28:e3:2b:4e:50:16:
            67:b6:26:17:46:8b:1f:47:33:d3:8f:0b:39:5a:9b:00:53:dc:
            51:4c:23:4b:60:35:5e:0e:7f:78:4b:06:69:06:f9:84:07:7b:
            3a:f8:9e:11:47:b9:14:fc:7d:3f:69:60:70:a4:72:f9:bb:8c:
            15:b6:4d:b6:45:3d:db:4c:cd:fb:64:69:a7:e7:20:ef:3a:66:
            56:09:fb:b5:a9:44:e9:f3:c5:b6:d1:27:f1:0e:e3:06:0c:45:
            d2:15:a3:02:02:be:51:3e:fb:30:06:4f:0e:8b:05:fd:68:ba:
            68:e0:84:c2:3e:54:62:b2:4a:84:e9:8e:13:78:a8:1e:e0:17:
            42:2c:f0:01:0b:fd
cert-1.pem: good
    This Update: Dec 15 11:18:19 2025 GMT
    Next Update: Dec 18 11:18:18 2025 GMT
```

```
● sara@sara-Vostro-3580:~/Documentos/crypto/ECC$ cat > check_ocsp.sh << 'EOF'
#!/usr/bin/env bash
set -euo pipefail

openssl s_client -connect www.fib.upc.edu:443 -servername www.fib.upc.edu -showcerts </dev/null 2>/dev/null \
| awk '/BEGIN CERTIFICATE/{i++} {print > ("cert-" i ".pem")}'
OCSP_URL=$(openssl x509 -in cert-1.pem -noout -ocsp_uri)
echo "OCSP URL: $OCSP_URL"

openssl ocsp -issuer cert-2.pem -cert cert-1.pem -url "$OCSP_URL" -respout ocsp.der
openssl ocsp -respin ocsp.der -issuer cert-2.pem -cert cert-1.pem -resp_text -text
EOF

chmod +x check_ocsp.sh
```

```
● sara@sara-Vostro-3580:~/Documentos/crypto/ECCS ./check_ocsp.sh
OCSP URL: http://ocsp-tls.harica.gr
WARNING: no nonce in response
Response verify OK
cert-1.pem: good
    This Update: Dec 15 11:18:19 2025 GMT
    Next Update: Dec 18 11:18:18 2025 GMT
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
            Hash Algorithm: sha1
            Issuer Name Hash: 2892028EABFCA4FFDDA1B5EC1474688142C20012
            Issuer Key Hash: 8601723F8CA970E231065316CE015F5B79C83C3B
            Serial Number: 540CB6B83DBB8CEDE1BA201E50FC74BF
        Request Extensions:
            OCSP Nonce:
                04109C8D2AB34F5FEC9CBB01F5791B4F0C4F
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: 8601723F8CA970E231065316CE015F5B79C83C3B
    Produced At: Dec 15 11:18:19 2025 GMT
    Responses:
        Certificate ID:
            Hash Algorithm: sha1
            Issuer Name Hash: 2892028EABFCA4FFDDA1B5EC1474688142C20012
            Issuer Key Hash: 8601723F8CA970E231065316CE015F5B79C83C3B
            Serial Number: 540CB6B83DBB8CEDE1BA201E50FC74BF
        Cert Status: good
        This Update: Dec 15 11:18:19 2025 GMT
        Next Update: Dec 18 11:18:18 2025 GMT

    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        29:fd:c1:bd:58:a1:a8:14:bc:54:55:22:d6:62:cc:94:82:ce:
        b7:72:99:6c:58:bf:41:ce:42:9b:d1:62:7d:9d:5a:a8:d8:fd:
        91:50:e7:dc:0f:82:6a:6e:65:32:81:a5:f5:5d:30:54:da:7f:
        0f:47:d9:86:e4:8b:91:07:63:62:a6:c4:96:26:9a:4a:6d:7f:
        a8:ee:46:18:8c:1b:8b:42:bf:a7:a1:b7:7a:9d:34:78:55:be:
        65:af:c3:el:d8:53:7d:6e:f4:c0:3d:48:7d:12:e7:59:d6:7b:
        f7:4e:c1:cf:bb:fc:60:67:a5:2a:6b:99:ac:ea:30:40:d1:23:
        93:c1:5b:ad:47:1a:53:0c:70:8d:ea:7e:4b:d6:ee:28:e3:77:
        d9:19:f3:54:41:77:c4:43:f5:d7:12:92:eb:e4:47:b0:ef:78:
        62:93:19:8a:5d:45:1a:e8:33:76:5c:a2:e5:1b:91:8e:fb:ca:
        70:6b:79:6c:8d:0a:df:39:37:07:37:09:d4:1b:6a:2c:d2:b1:
        e1:cb:36:b6:49:51:1e:04:f1:1c:78:29:8e:31:80:35:2a:05:
        e1:1c:54:2f:86:7f:35:79:0f:b3:72:16:13:72:d0:59:a2:3f:
        37:b2:7e:c4:2c:47:ca:79:00:b8:34:7d:28:e3:2b:4e:50:16:
        67:b6:26:17:46:8b:1f:47:33:d3:8f:0b:39:5a:9b:00:53:dc:
        51:4c:23:4b:60:35:5e:0e:7f:78:4b:06:69:06:f9:84:07:7b:
        3a:f8:9e:11:47:b9:14:fc:7d:3f:69:60:70:a4:72:f9:bb:8c:
        15:b6:4d:b6:45:3d:db:4c:cd:fb:64:69:a7:e7:20:ef:3a:66:
        56:09:fb:b5:a9:44:e9:f3:c5:b6:d1:27:f1:0e:e3:06:0c:45:
        d2:15:a3:02:02:be:51:3e:fb:30:06:4f:0e:8b:05:fd:68:ba:
        68:e0:84:c2:3e:54:62:b2:4a:84:e9:8e:13:78:a8:1e:e0:17:
        42:2c:f0:01:0b:fd
    WARNING: no nonce in response
    Response verify OK
    cert-1.pem: good
        This Update: Dec 15 11:18:19 2025 GMT
        Next Update: Dec 18 11:18:18 2025 GMT
```