Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πολυτεχνική Σχολή
Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Εργασία στην Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων

Απόκτηση προσωπικού ψηφιακού πιστοποιητικού - Εξέταση του περιεχομένου του - Χρήση του για την ψηφιακή υπογραφή - Κρυπτογράφηση αρχείων - email

---

Ioannis Manousaridis

Digitally signed by Ioannis Manousaridis
Date: 2019.12.31 11:47:34 +02'00'

Μανουσαρίδης Ιωάννης (8855)
imanousar@ece.auth.gr

Θεσσαλονίκη, Δεκέμβριος 2019

Περιεχόμενα

I. ΕΚΔΟΣΗ ΠΡΟΣΩΠΙΚΟΥ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ (ΨΠ)

α) Το ψηφιακό πιστοποιητικό που εξάχθηκε από το ΚΗΔ μπορεί να βρεθεί στον παρακάτω σύνδεσμο:

https://drive.google.com/open?id=1GjZlK-bJBN72RD5TBf71OjYQKxjmG0qq

II. ΕΞΕΤΑΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

β) Το περιεχόμενο και η δομή του πιστοποιητικού εμφανίστηκε σε αναγνώσιμη μορφή με χρήση της παρακάτω εντολής:

openssl x509 -in imanousar-cert.pem -text > imanousar_8855.txt

Στη συνέχεια φαίνεται το περιεχόμενο που αποκτήθηκε. Τα ερωτήματα αυτής της ενότητας απαντώνται στο πέρας του περιεχομένου.

1) Certificate:
2) Data:
3) Version: 3 (0x2)
4) Serial Number:
5) 6d:b3:31:95:54:e1:e9:79:31:1c:98:9f:ed:43:fb:5e
6) Signature Algorithm: sha256WithRSAEncryption
7) Issuer: C=GR, L=Thessaloniki, O=Aristotle University of Thessaloniki, **CN=Aristotle University of Thessaloniki Client RSA SubCA R2**
8) Validity
9) Not Before: Dec 28 17:36:16 2019 GMT
10) **Not After : Dec 27 17:36:16 2021 GMT**
    Subject: C=GR, L=Thessaloniki, O=Aristotle University of Thessaloniki, OU=School of Electrical and Computer Engineering, OU=Class B - Private Key created and stored in software CSP, SN=Manousaridis, GN=Ioannis/serialNumber=3685680232, **CN=Ioannis Manousaridis**/emailAddress=imanousar@ece.auth.gr
11) Subject Public Key Info:
12) **Public Key Algorithm: rsaEncryption**
    a) **Public-Key: (2048 bit)**
    b) **Modulus**:
    00:f2:9d:8e:d8:8f:08:f1:1f:dc:4e:f7:f1:77:ef:
    1c:11:96:14:49:3a:1b:e6:be:8d:b7:33:cf:7d:08:
    81:73:6b:18:b2:c5:6f:ef:87:44:59:57:84:0f:94:
    d9:cc:a6:59:b4:dc:9a:1b:81:22:7c:05:90:87:33:
    e1:11:52:4e:eb:f2:10:3b:ac:f5:c0:2e:51:1f:68:
    df:2d:8f:cc:09:9b:a7:0c:0f:44:54:d6:aa:39:ef:
    50:d9:6b:b5:57:0e:ea:95:8f:78:9e:90:07:8c:7a:

f9:84:22:3c:2c:9c:c8:3e:ad:5f:76:73:e7:bd:db:
17:f5:fc:f1:a5:27:93:58:9f:8b:08:bd:91:a0:a8:
0d:a8:b7:14:8e:ce:a5:46:b8:d2:2f:ef:44:ba:c8:
1b:51:be:01:11:d3:e7:36:32:d8:4a:e5:41:b1:0d:
52:d5:65:68:37:bd:63:52:42:0e:2f:1d:99:d8:f4:
64:f3:3a:8a:0c:1e:f5:67:d6:8f:bf:02:ee:f5:08:
da:86:e2:7c:a6:1c:87:84:11:08:d1:73:54:ae:61:
fe:1e:77:07:7d:8e:c4:a1:8a:11:1d:93:c8:3b:33:
5b:da:77:06:be:fc:88:23:53:6b:28:68:f3:fa:4d:
00:89:ae:ff:09:df:e2:43:25:6f:cf:69:79:2f:43:
b9:6d

c) **Exponent: 65537 (0x10001)**

13) X509v3 extensions:

14) X509v3 Authority Key Identifier:

a) keyid:62:35:7B:F4:B8:71:F4:BE:D8:80:14:6B:F5:E0:45:2C:D7:9B:7A:27

15) Authority Information Access:

a) CA Issuers - URI:http://repo.harica.gr/certs/HaricaAuthClientSubCAR2.crt

b) OCSP - URI:http://ocsp.harica.gr

16) X509v3 Subject Alternative Name:

a) email:imanousar@ece.auth.gr, othername:<unsupported>

17) **X509v3 Certificate Policies:**

Policy: 0.4.0.194112.1.0

Policy: 1.3.6.1.4.1.26513.1.1.4.1

CPS: https://repo.harica.gr/documents/CPS

18) X509v3 Extended Key Usage:

a) TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12

19) qcStatements:

20) 0..0.....F..0.....F..0.....F...0.....F..0..0A.;https://repo.harica.gr/documents/QualifiedNaturalPDS-EN.pdf..en0A.;https://repo.harica.gr/documents/QualifiedNaturalPDS-EL.pdf..el

21) X509v3 CRL Distribution Points:

Full Name:
URI:http://crl.harica.gr/HaricaAuthClientSubCAR2.crl

22) X509v3 Subject Key Identifier:

a) E1:51:71:C4:FE:F3:16:02:73:53:CB:68:28:FD:FF:2E:40:B7:76:5D

23) X509v3 Key Usage: critical

a) Digital Signature, Key Encipherment

24) Signature Algorithm: sha256WithRSAEncryption
01:39:3c:6b:0e:97:2e:dd:c9:26:f8:09:20:81:8f:9c:c1:6a:

c8:6e:0f:be:96:c5:9a:61:ca:1c:44:25:c3:b0:ef:e8:60:46:
b5:fa:6a:d0:a5:5a:c0:95:45:2c:6a:5d:fe:15:7c:f5:46:44:
83:50:f4:9e:50:45:c0:ca:3e:33:a5:fd:80:e0:ce:ed:cb:4a:
70:fa:b5:1e:8b:ab:e7:83:4e:00:e9:60:73:3d:ec:e9:5f:99:
49:96:cd:2f:f8:4d:59:98:70:34:73:bf:0f:4d:7e:df:e3:2b:
5d:8a:bb:0c:f5:a6:da:36:8b:a3:27:f6:42:e2:3c:1c:a7:15:
f7:c7:d2:77:70:3c:19:91:9f:77:4f:11:1f:89:4a:6f:36:bc:
82:9d:65:0f:15:be:ed:4f:eb:f9:b6:08:6b:87:d3:b5:8b:2e:
25:f3:23:71:97:59:b2:cf:f8:73:df:5b:92:af:2c:55:5a:37:
fe:2d:e5:8d:50:12:06:10:98:ef:d0:95:96:25:02:4b:8a:87:
75:63:2d:a8:e2:29:c2:1e:09:fc:31:4f:78:a8:39:f0:1f:3c:
6b:91:b8:d3:ce:a0:a1:9f:5e:df:37:25:f2:18:66:47:55:8b:
c6:69:30:02:ce:8e:98:6d:a8:c4:1a:96:13:f1:56:8d:e1:6f:
3a:02:1f:32:79:da:2a:77:13:b4:16:8d:85:b2:f8:bf:95:ea:
7f:4c:31:7c:95:2c:14:1c:52:c4:de:38:b1:21:e3:7f:c7:37:
07:67:e0:6a:8c:81:34:9d:4b:13:79:51:3c:c0:9e:7f:b5:6e:
4a:f8:3b:80:42:dd:98:ac:8f:3f:ea:7b:b4:a9:4d:25:76:76:
bf:41:dc:d8:c5:19:59:11:12:21:80:c0:5f:73:95:c4:b9:52:
3d:b3:af:e1:b9:ea:a3:87:2e:ea:cc:07:6e:b8:db:f7:85:25:
57:d7:86:33:a3:6d:88:bf:db:fa:4b:6e:25:75:5f:3f:40:f2:
fb:5c:96:58:7e:dd:bd:6b:2d:b5:d7:90:4d:34:3b:bb:a7:13:
da:bb:e6:64:b1:71:b7:73:b5:46:bc:19:80:28:40:c0:91:c8:
69:6d:6d:30:50:f7:46:14:cf:3f:b6:2c:85:7f:97:75:e6:0c:
a5:5c:cb:a9:4c:8b:12:f4:16:c6:c4:89:db:07:46:28:70:11:
19:b8:67:0d:81:89:42:6c:47:23:07:bd:fe:e5:57:57:33:45:
73:6a:a5:d9:a2:66:8d:50:35:e4:74:f7:9d:f5:c5:35:24:6b:
90:98:6b:32:6e:e3:3c:06:0b:3e:7c:f4:ad:36:5e:c5:25:87:
be:69:80:70:8c:9b:f1:22

Απαντήσεις Ερωτημάτων

1. Το Common Name (CN) του πιστοποιητικού σας και η ημερομηνία λήξης του.

Στη σειρά 10 με bold γράμματα φαίνεται το **CN=Ioannis Manousaridis** καθώς και η ημερομηνία λήξης του **"Not After : Dec 27 17:36:16 2021 GMT"**.

2. Τα Common-Names της ιεραρχίας της υποδομής δημοσίου κλειδιού (ΥΔΚ) που εξέδωσε το πιστοποιητικό σας.

Στη σειρά 7 με bold γράμματα φαίνεται το **CN=Aristotle University of Thessaloniki Client RSA SubCA R2**.

3. Το url που περιγράφει τις πολιτικές και διαδικασίες πιστοποίησης της ΥΔΚ.

Φαίνεται στη σειρά 17 με bold γράμματα

CPS: https://repo.harica.gr/documents/CPS

4. Εντοπίστε και επισημάνετε το URL του CRL που δημοσιοποιεί τα πιστοποιητικά που ανακαλούνται (CRL: λίστα ανάκλησης πιστοποιητικών).

Φαίνεται στη σειρά 21

URI:http://crl.harica.gr/HaricaAuthClientSubCAR2.crl (9)

5. Το όνομα του μη-συμμετρικού αλγόριθμου που χρησιμοποιήθηκε και το μέγεθος των κλειδιών σε bits.

Φαίνεται στη σειρά 12 με bold γράμματα:

Όνομα Αλγορίθμου: **Public Key Algorithm: rsaEncryption**

Μέγεθος κλειδιού: **Public-Key: (2048 bit)**

6. Το modulus n.

Φαίνεται στη σειρά 12b) με bold και italics γράμματα:

7. Το δημόσιο κλειδί σας e.

Φαίνεται στη σειρά 12c) με bold γράμματα: **Exponent: 65537 (0x10001)**

Πιστοποιητικό

-----BEGIN CERTIFICATE-----

MIIIIDCCBgigAwIBAgIQbbMxlVTh6XkxHJif7UP7XjANBgkqhkiG9w0BAQsFADCB

ljELMAkGA1UEBhMCR1IxFTATBgNVBAcMDFRoZXNzYWxvbmlraTEtMCsGA1UECgwk

QXJpc3RvdGxlIFVuaXZlcnNpdHkgb2YgVGhlc3NhbG9uaWtpMUEwPwYDVQQDDDhB

cmlzdG90bGUgVW5pdmVyc2l0eSBvZiBUaGVzc2Fsb25pa2kgQ2xpZW50IFJTQSBT

dWJDQSBSMjAeFw0xOTEyMjgxNzM2MTZaFw0yMTEyMjcxNzM2MTZaMIIBUTELMAkG

A1UEBhMCR1IxFTATBgNVBAcMDFRoZXNzYWxvbmlraTEtMCsGA1UECgwkQXJpc3Rv

dGxlIFVuaXZlcnNpdHkgb2YgVGhlc3NhbG9uaWtpMTYwNAYDVQQLDC1TY2hvb2wg

b2YgRWxlY3RyaWNhbCBhbmQgQ29tcHV0ZXIgRW5naW5lZXJpbmcxQTA/BgNVBAsM

OENsYXNzIEIgLSBQcml2YXRlIEtleSBjcmVhdGVkIGFuZCBzdG9yZWQgaW4gc29m

dHdhcmUgQ1NQMRUwEwYDVQQEDAxNYW5vdXNhcmlkaXMxEDAOBgNVBCoMB0lvY
W5u

aXMxEzARBgNVBAUTCjM2ODU2ODAyMzIxHTAbBgNVBAMMFElvYW5uaXMgTWFub3V
zYXJpZGlzMSQwIgYJKoZIhvcNAQkBFhVpbWFub3VzYXJAZWNlLmF1dGguZ3IwggEi

MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDynY7YjwjxH9xO9/F37xwRlhRJ

Ohvmvo23M899CIFzaxiyxW/vh0RZV4QPlNnMplm03JobgSJ8BZCHM+ERUk7r8hA7

rPXALlEfaN8tj8wJm6cMD0RU1qo571DZa7VXDuqVj3iekAeMevmEIjwsnMg+rV92

c+e92xf1/PGlJ5NYn4sIvZGgqA2otxSOzqVGuNIv70S6yBtRvgER0+c2MthK5UGx

DVLVZWg3vWNSQg4vHZnY9GTzOooMHvVn1o+/Au71CNqG4nymHIeEEQjRc1SuYf4e

dwd9jsShihEdk8g7M1vadwa+/IgjU2soaPP6TQCJrv8J3+JDJW/PaXkvQ7ltAgMB

AAGjggKqMIICpjAfBgNVHSMEGDAWgBRiNXv0uHH0vtiAFGv14EUs15t6JzB2Bggr

BgEFBQcBAQRqMGgwQwYIKwYBBQUHMAKGN2h0dHA6Ly9yZXBvLmhhcmljYS5nci9j

ZXJ0cy9IYXJpY2FBdXRoQ2xpZW50U3ViQ0FSMi5jcnQwIQYIKwYBBQUHMAGGFWh0

dHA6Ly9vY3NwLmhhcmljYS5ncjBOBgNVHREERzBFgRVpbWFub3VzYXJAZWNlLmF1

dGguZ3KgLAYKKwYBBAGCNxQCA6AeDBxpbWFub3VzYXJAcGNsYWJzLml0Yy5hdXRo

LmdyMFgGA1UdIARRME8wCQYHBACL7EABADBCBgwrBgEEAYHPEQEBBAEwMjAwBg

gr

BgEFBQcCARYkaHR0cHM6Ly9yZXBvLmhhcmljYS5nci9kb2N1bWVudHMvQ1BTMCkG

A1UdJQQiMCAGCCsGAQUFBwMCBggrBgEFBQcDBAYKKwYBBAGCNwoDDDCBwwYIKw

YB

BQUHAQMEgbYwgbMwCAYGBACORgEBMBMGBgQAjkYBBjAJBgcEAI5GAQYBMIGRBgYE

AI5GAQUwgYYwQRY7aHR0cHM6Ly9yZXBvLmhhcmljYS5nci9kb2N1bWVudHMvUXVh
bGlmaWVkTmF0dXJhbFBEUy1FTi5wZGYTAmVuMEEWO2h0dHBzOi8vcmVwby5oYXJp
Y2EuZ3IvZG9jdW1lbnRzL1F1YWxpZmllZE5hdHVyYWxQRFMtRUwucGRmEwJlbDBB
BgNVHR8EOjA4MDagNKAyhjBodHRwOi8vY3JsLmhhcmljYS5nci9IYXJpY2FBdXRo
Q2xpZW50U3ViQ0FSMi5jcmwwHQYDVR0OBBYEFOFRccT+8xYCc1PLaCj9/y5At3Zd
MA4GA1UdDwEB/wQEAwIFoDANBgkqhkiG9w0BAQsFAAOCAgEAATk8aw6XLt3JJvgJ
IIGPnMFqyG4PvpbFmmHKHEQlw7Dv6GBGtfpq0KVawJVFLGpd/hV89UZEg1D0nlBF
wMo+M6X9gODO7ctKcPq1Hour54NOAOlgcz3s6V+ZSZbNL/hNWZhwNHO/D01+3+Mr
XYq7DPWm2jaLoyf2QuI8HKcV98fSd3A8GZGfd08RH4lKbza8gp1lDxW+7U/r+bYI
a4fTtYsuJfMjcZdZss/4c99bkq8sVVo3/i3ljVASBhCY79CVliUCS4qHdWMtqOIp
wh4J/DFPeKg58B88a5G4086goZ9e3zcl8hhmR1WLxmkwAs6OmG2oxBqWE/FWjeFv
OgIfMnnaKncTtBaNhbL4v5Xqf0wxfJUsFBxSxN44sSHjf8c3B2fgaoyBNJ1LE3lR
PMCef7VuSvg7gELdmKyPP+p7tKlNJXZ2v0Hc2MUZWRESIYDAX3OVxLlSPbOv4bnq
o4cu6swHbrjb94UlV9eGM6NtiL/b+ktuJXVfP0Dy+1yWWH7dvWsttdeQTTQ7u6cT
2rvmZLFxt3O1RrwZgChAwJHIaW1tMFD3RhTPP7YshX+XdeYMpVzLqUyLEvQWxsSJ
2wdGKHARGbhnDYGJQmxHIwe9/uVXVzNFc2ql2aJmjVA15HT3nfXFNSRrkJhrMm7j
PAYLPnz0rTZexSWHvmmAcIyb8SI=
-----END CERTIFICATE-----