12/1/2021

Ψηφιακό πιστοποιητικό

Εργασία στο μάθημα της Ασφάλειας Πληροφοριακών Συστημάτων

Αλέξανδρος Πετρίδης

AEM: 9288 EMAIL: ALEPETPAN@ECE.AUTH.GR

Alexandros Petridis

Digitally signed by Alexandros Petridis
DN: 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=Petridis, givenName=Alexandros, serialNumber=8585743722, cn=Alexandros Petridis, email=alepetpan@ece.auth.gr
Date: 2021.01.12 01:17:42 +02'00'

Περιεχόμενα

Κατάλογος εικόνων

3.Εμφάνιση Περιεχομένου ψηφιακού πιστοποιητικού.

Για την εμφάνιση του περιεχομένου του πιστοποιητικού μου χρησιμοποίησα την παρακάτω εντολή του OpenSSL :

```
x509 -inform der -in alepetpan-cert.cer -text -out something.txt
```

Εικόνα 1. Εντολή OpenSSL

και έπειτα έκανα αντιγραφή όλες τις πληροφορίες που εκτυπώθηκαν στο something.txt επικόλληση παρακάτω:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

12:89:34:68:e2:1e:56:dc:19:6f:87:4f:d7:07:d3:23

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = GR, O = Greek Universities Network (GUnet), organizationIdentifier = VATGR-099028220, OU = Hellenic Academic and Research Institutions CA, CN = HARICA Institutional Client SubCA R1

Validity

Not Before: Jan 11 13:34:57 2021 GMT

Not After : Jan 11 13:34:56 2023 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 = Petridis, GN = Alexandros, serialNumber = 8585743722, CN = Alexandros Petridis, emailAddress = alepetpan@ece.auth.gr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:b3:fa:31:36:76:dc:0f:d0:88:bc:88:86:c5:4c:

3f:27:40:af:72:90:b6:17:44:fe:1d:45:5a:df:ae:

3a:3c:1c:51:1b:33:76:ff:23:fe:57:eb:94:79:62:

7e:da:ef:51:78:07:12:c5:c1:de:0e:f5:bb:87:d4:

41:b1:75:1d:7a:aa:c0:4a:2b:4b:d4:66:50:92:9e:

cb:76:d1:c6:c0:b0:e6:08:9e:8f:f4:45:10:bc:4d:

e0:0f:22:9e:01:80:39:6c:f7:ef:49:0a:3d:a8:59:

58:a9:48:89:2a:bc:4b:b3:e0:53:28:43:1e:2e:9e:

ef:c7:cf:3a:a3:50:81:84:e7:2c:f4:1c:2e:86:cc:

48:58:e5:18:ce:ba:70:25:48:a3:7d:8e:44:c2:b2:

14:c5:f9:f7:58:ff:1a:b5:27:fe:4b:3c:26:e3:4e:

c3:3a:4a:aa:b9:ef:d7:12:b6:ba:60:cf:de:b2:95:

fd:c3:52:99:57:8e:01:6b:d3:4e:a4:aa:e5:a2:77:

ca:c1:c4:e7:31:64:ac:e6:c3:02:e6:c9:5b:dd:51:

0b:74:a1:a2:44:59:ac:d0:84:74:af:14:9e:e8:5d:

dd:a4:68:f7:f6:f2:90:2b:bc:70:23:08:18:71:32:

c3:07:91:be:d0:9c:cb:85:f1:e4:01:c0:c2:f9:8f:

cb:27

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:CD:E9:4B:6B:5D:28:B3:7A:92:0D:8A:C4:5F:E4:4E:30:F5:AB:61:69

Authority Information Access:

CA Issuers - URI:http://repo.harica.gr/certs/HaricaInstitutionalClientSubCAR1.cer

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

X509v3 Subject Alternative Name:

email:alepetpan@ece.auth.gr, othername:<unsupported>

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

User Notice:

Explicit Text: This Qualified Certificate has been Issued by the QTSP "Greek Universities Network (GUnet)" with VAT number EL099028220

X509v3 Extended Key Usage:

TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5

qcStatements:

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

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.harica.gr/HaricaInstitutionalClientSubCAR1.crl

X509v3 Subject Key Identifier:

F4:66:13:A5:EA:D0:83:B3:B5:E4:25:34:BF:61:35:2C:B4:97:C2:74

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

Signature Algorithm: sha256WithRSAEncryption

46:41:ff:4a:18:f0:04:88:80:41:e9:6c:98:b5:9d:70:4b:39:
a4:0f:90:fc:aa:08:31:3e:02:67:06:9d:8c:45:79:fa:65:a3:
82:4a:fa:f9:0b:40:0a:ac:b8:46:3a:09:cf:ea:fb:e8:87:d9:
2e:63:d4:57:5a:e3:98:9b:6b:b0:0c:43:9f:6f:03:10:bf:f4:
76:e9:77:73:61:a3:b7:bc:4e:88:d2:ea:8a:6a:75:25:60:54:
c3:85:f0:12:d5:74:13:ba:4b:c3:21:34:54:d4:d3:75:e9:b2:
15:96:51:ba:1b:4f:fd:50:f5:99:f0:53:ae:08:80:db:57:45:
70:62:9f:10:ed:8d:5a:d9:31:b3:ef:cb:d6:af:8c:0a:14:b1:
e0:ef:8a:75:01:6d:94:38:a7:10:0c:3d:3c:53:50:19:1e:59:
2f:77:86:69:a4:69:f2:69:2c:44:9d:44:a0:02:d1:a7:38:7f:
3d:7d:b5:5e:60:ef:f6:c6:9a:2f:f0:1e:58:6e:e6:ed:40:bb:
1b:29:9f:ea:70:f0:3a:c5:b7:64:88:63:5f:b8:cf:62:f6:3a:
10:c1:3a:9a:fb:f7:42:1c:15:53:63:cc:1f:db:b1:81:4b:2d:
95:19:57:30:9a:3a:c3:3c:fb:f2:67:c0:ce:2b:5b:b2:1a:21:
64:8c:e1:a5:b6:27:aa:63:14:40:6d:f6:03:12:09:49:31:c1:
6f:34:e4:02:63:eb:0a:6c:a9:79:f1:32:47:ab:4a:91:b5:0e:
26:3d:5c:6a:e3:c4:8b:6d:01:fd:88:34:c7:7d:4b:c5:01:c2:
24:a2:29:ed:bb:a3:21:fc:93:ff:eb:7f:70:f2:5c:a7:88:94:
c0:ea:63:a0:aa:43:ec:e8:7f:14:10:ca:85:02:1f:c5:f7:49:
c2:a4:60:1a:d8:05:90:4b:0d:b9:dc:6c:99:2d:d5:d9:26:e3:
3e:ab:54:23:ee:49:fa:3f:b7:2c:b0:94:e7:37:4c:3b:b3:69:

3a:19:03:fc:3a:0a:1d:c4:54:d9:32:a0:f0:b9:d6:27:b9:80:

41:1e:01:17:a0:c1:22:08:da:a7:9e:b6:87:a6:04:9b:76:9c:

f1:5d:8f:7e:34:7d:05:ea:51:58:7a:99:54:89:f4:87:39:17:

ef:08:5e:06:7e:73:6a:31:de:64:dd:59:56:78:0d:5c:3d:80:

ce:6f:5c:c6:e8:97:9c:53:0f:a8:93:c4:93:77:1e:f3:93:72:

6c:44:c3:5c:17:e3:dd:4a:2f:6d:38:57:96:78:42:29:b9:5f:

34:a4:0f:dc:2b:29:43:1c:cd:34:c8:ee:5a:75:27:3a:4a:89:

24:62:2a:21:16:88:b6:0f

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

MIII7jCCBtagAwIBAgIQEok0aOIeVtwZb4dP1wfTIzANBgkqhkiG9w0BAQsFADCB

vDELMAkGA1UEBhMCR1IxKzApBgNVBAoMIkdyZWVrIFVuaXZlcnNpdGllcyBOZXR3

b3JrIChHVW5ldCkxGDAWBgNVBGEMD1ZBVEdSLTA5OTAyODIyMDE3MDUGA1UECwwu

SGVsbGVuaWMgQWNhZGVtaWMgYW5kIFJlc2VhcmNoIEluc3RpdHV0aW9ucyBDQTEt

MCsGA1UEAwwkSEFSSUNBIEluc3RpdHV0aW9uYWwgQ2xpZW50IFN1YkNBIFIxMB4X

DTIxMDExMTEzMzQ1N1oXDTIzMDExMTEzMzQ1NlowggFPMQswCQYDVQQGEwJHUjEV

MBMGA1UEBwwMVGhlc3NhbG9uaWtpMS0wKwYDVQQKDCRBcmlzdG90bGUgVW5pdmVy

c2l0eSBvZiBUaGVzc2Fsb25pa2kxNjA0BgNVBAsMLVNjaG9vbCBvZiBFbGVjdHJp

Y2FsIGFuZCBDb21wdXRlciBFbmdpbmVlcmluZzFBMD8GA1UECww4Q2xhc3MgQiAt

IFByaXZhdGUgS2V5IGNyZWF0ZWQgYW5kIHN0b3JlZCBpbiBzb2Z0d2FyZSBDU1Ax

ETAPBgNVBAQMCFBldHJpZGlzMRMwEQYDVQQqDApBbGV4YW5kcm9zMRMwEQYDVQQF

Ewo4NTg1NzQzNzIyMRwwGgYDVQQDDBNBbGV4YW5kcm9zIFBldHJpZGlzMSQwIgYJ

KoZIhvcNAQkBFhVhbGVwZXRwYW5AZWNlLmF1dGguZ3IwggEiMA0GCSqGSIb3DQEB

AQUAA4IBDwAwggEKAoIBAQCz+jE2dtwP0Ii8iIbFTD8nQK9ykLYXRP4dRVrfrjo8

HFEbM3b/I/5X65R5Yn7a71F4BxLFwd4O9buH1EGxdR16qsBKK0vUZlCSnst20cbA

sOYIno/0RRC8TeAPIp4BgDls9+9JCj2oWVipSIkqvEuz4FMoQx4unu/HzzqjUIGE

5yz0HC6GzEhY5RjOunAlSKN9jkTCshTF+fdY/xq1J/5LPCbjTsM6Sqq579cStrpg

z96ylf3DUplXjgFr006kquWid8rBxOcxZKzmwwLmyVvdUQt0oaJEWazQhHSvFJ7o

Xd2kaPf28pArvHAjCBhxMsMHkb7QnMuF8eQBwML5j8snAgMBAAGjggNUMIIDUDAf

BgNVHSMEGDAWgBTN6UtrXSizepINisRf5E4w9athaTB/BggrBgEFBQcBAQRzMHEw

TAYIKwYBBQUHMAKGQGh0dHA6Ly9yZXBvLmhhcmljYS5nci9jZXJ0cy9IYXJpY2FJ

bnN0aXR1dGlvbmFsQ2xpZW50U3ViQ0FSMS5jZXIwIQYIKwYBBQUHMAGGFWh0dHA6

Ly9vY3NwLmhhcmljYS5ncjBOBgNVHREERzBFgRVhbGVwZXRwYW5AZWNlLmF1dGgu

Z3KgLAYKKwYBBAGCNxQCA6AeDBxhbGVwZXRwYW5AcGNsYWJzLml0Yy5hdXRoLmdy

MIHkBgNVHSAEgdwwgdkwCQYHBACL7EABADCBywYMKwYBBAGBzxEBAQQBMIG6MDAG

CCsGAQUFBwIBFiRodHRwczovL3JlcG8uaGFyaWNhLmdyL2RvY3VtZW50cy9DUFMw

gYUGCCsGAQUFBwICMHkMd1RoaXMgUXVhbGlmaWVkIENlcnRpZmljYXRlIGhhcyBi

ZWVuIElzc3VlZCBieSB0aGUgUVRTUCAiR3JlZWsgVW5pdmVyc2l0aWVzIE5ldHdv

cmsgKEdVbmV0KSIgd2l0aCBWQVQgbnVtYmVyIEVMMDk5MDI4MjIwMDQGA1UdJQQt

MCsGCCsGAQUFBwMCBggrBgEFBQcDBAYKKwYBBAGCNwoDDAYJKoZIhvcvAQEFMIHD

BggrBgEFBQcBAwSBtjCBszAIBgYEAI5GAQEwEwYGBACORgEGMAkGBwQAjkYBBgEw

gZEGBgQAjkYBBTCBhjBBFjtodHRwczovL3JlcG8uaGFyaWNhLmdyL2RvY3VtZW50

cy9RdWFsaWZpZWROYXR1cmFsUERTLUVOLnBkZhMCZW4wQRY7aHR0cHM6Ly9yZXBv

LmhhcmljYS5nci9kb2N1bWVudHMvUXVhbGlmaWVkTmF0dXJhbFBEUy1FTC5wZGYT

AmVsMEoGA1UdHwRDMEEwP6A9oDuGOWh0dHA6Ly9jcmwuaGFyaWNhLmdyL0hhcmlj

YUluc3RpdHV0aW9uYWxDbGllbnRTdWJDQVIxLmNybDAdBgNVHQ4EFgQU9GYTperQ

g7O15CU0v2E1LLSXwnQwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBCwUAA4IC

AQBGQf9KGPAEiIBB6WyYtZ1wSzmkD5D8qggxPgJnBp2MRXn6ZaOCSvr5C0AKrLhG

OgnP6vvoh9kuY9RXWuOYm2uwDEOfbwMQv/R26XdzYaO3vE6I0uqKanUlYFTDhfAS

1XQTukvDITRU1NN16bIVllG6G0/9UPWZ8FOuCIDbV0VwYp8Q7Y1a2TGz78vWr4wK

FLHg74p1AW2UOKcQDD08U1AZHlkvd4ZppGnyaSxEnUSgAtGnOH89fbVeYO/2xpov

8B5YbubtQLsbKZ/qcPA6xbdkiGNfuM9i9joQwTqa+/dCHBVTY8wf27GBSy2VGVcw

mjrDPPvyZ8DOK1uyGiFkjOGltieqYxRAbfYDEglJMcFvNOQCY+sKbKl58TJHq0qR

tQ4mPVxq48SLbQH9iDTHfUvFAcIkointu6Mh/JP/639w8lyniJTA6mOgqkPs6H8U

EMqFAh/F90nCpGAa2AWQSw253GyZLdXZJuM+q1Qj7kn6P7cssJTnN0w7s2k6GQP8

OgodxFTZMqDwudYnuYBBHgEXoMEiCNqnnraHpgSbdpzxXY9+NH0F6lFYeplUifSH

ORfvCF4GfnNqMd5k3VlWeA1cPYDOb1zG6JecUw+ok8STdx7zk3JsRMNcF+PdSi9t

OFeWeEIpuV80pA/cKylDHM00yO5adSc6SokkYiohFoi2Dw==

-----END CERTIFICATE-----

3α. Ημερομηνία εναρξης και λήξης του πιστοποιητικού

Validity

Not Before: Jan 11 13:34:57 2021 GMT

Not After : Jan 11 13:34:56 2023 GMT

Η εγκυρότητα του πιστοποιητικού μου είναι από τις 11 Ιανουαρίου 2021 στις 13:34:57 Μέσος χρόνος Γκρίνουιτς μέχρι τις 11 Ιανουαρίου 2023 στις 13:34:56 Μέσος χρόνος Γκρίνουιτς.

3β. Το Subject και το Common Name του πιστοποιητικού

Το Subject του πιστοποιητικού είναι το παρακάτω:

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 = Petridis, GN = Alexandros, serialNumber = 8585743722, CN = Alexandros Petridis, emailAddress = alepetpan@ece.auth.gr

και το Common Name (CN) :

CN = Alexandros Petridis

3γ. Το όνομα του μη-συμμετρικού αλγορίθμου και το μέγεθος των κλειδιών σε bits.

Το όνομα του μη-συμμετρικού αλγορίθμου:

Public Key Algorithm: rsaEncryption

και το μέγεθος των κλειδιών σε bits:

RSA Public-Key: (2048 bit)

3δ. Το modulus n.

Το modulus n του πιστοποιητικού:

Modulus:

00:b3:fa:31:36:76:dc:0f:d0:88:bc:88:86:c5:4c:

3f:27:40:af:72:90:b6:17:44:fe:1d:45:5a:df:ae:

3a:3c:1c:51:1b:33:76:ff:23:fe:57:eb:94:79:62:

7e:da:ef:51:78:07:12:c5:c1:de:0e:f5:bb:87:d4:

41:b1:75:1d:7a:aa:c0:4a:2b:4b:d4:66:50:92:9e:

cb:76:d1:c6:c0:b0:e6:08:9e:8f:f4:45:10:bc:4d:

e0:0f:22:9e:01:80:39:6c:f7:ef:49:0a:3d:a8:59:

58:a9:48:89:2a:bc:4b:b3:e0:53:28:43:1e:2e:9e:

ef:c7:cf:3a:a3:50:81:84:e7:2c:f4:1c:2e:86:cc:

48:58:e5:18:ce:ba:70:25:48:a3:7d:8e:44:c2:b2:

14:c5:f9:f7:58:ff:1a:b5:27:fe:4b:3c:26:e3:4e:

c3:3a:4a:aa:b9:ef:d7:12:b6:ba:60:cf:de:b2:95:

fd:c3:52:99:57:8e:01:6b:d3:4e:a4:aa:e5:a2:77:

ca:c1:c4:e7:31:64:ac:e6:c3:02:e6:c9:5b:dd:51:

0b:74:a1:a2:44:59:ac:d0:84:74:af:14:9e:e8:5d:

dd:a4:68:f7:f6:f2:90:2b:bc:70:23:08:18:71:32:

c3:07:91:be:d0:9c:cb:85:f1:e4:01:c0:c2:f9:8f:

cb:27

3ε. Ο αριθμός του δημόσιου κλειδιού

Ο αριθμός e του δημόσιου κλειδιού (public exponent e):

Exponent: 65537 (0x10001)

3στ. Όνομα αλγορίθμου σύνοψης και μέγεθος του σε bits.

Το όνομα του αλγορίθμου σύνοψης είναι :

Signature Algorithm: sha256WithRSAEncryption

και το μέγεθός του το καταλαβαίνουμε από το όνομα του δηλαδή 256bits.

3ζ. Πολιτικές και διαδικασίες πιστοποίησης ΥΔΚ

Το url που περιγράφει τις πολιτικές και διαδικασίες πιστοποίησης της Υποδομής Δημόσιου Κλειδιού:

CA Issuers - URI:http://repo.harica.gr/certs/HaricaInstitutionalClientSubCAR1.cer

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

Το πρώτο είναι πιστοποιητικό και το δεύτερο γενικές πληροφορίες και έχουν περιεχόμενο αντίστοιχο με το προσωπικό μας πιστοποιητικό.

3η. Λίστα Ανάκλησης Πιστοποιητικών

Το url του CRL (Λίστα Ανάκλησης Πιστοποιητικών) που δημοσιοποιεί τα πιστοποιητικά που ανακαλούνται:

Full Name:

URI:http://crl.harica.gr/HaricaInstitutionalClientSubCAR1.crl

Στο παραπάνω αρχείο βλέπουμε γενικές πληροφορίες για τον εκδότη όπως είναι το όνομα, το διάστημα ισχύος, τις πληροφορίες για τον αλγόριθμο κρυπτογράφησης και κατακερματισμού καθώς και τη λίστα ανάκλησης πιστοποιητικών.

3θ. Χρήσεις ψηφιακού πιστοποιητικού

Οι χρήσεις του ψηφιακού πιστοποιητικού όπως βλέπουμε παρακάτω είναι για ψηφιακή υπογραφή και για κρυπτογράφηση σε αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου.

X509v3 Extended Key Usage:

TLS Web Client Authentication, E-mail Protection, 1.3.6.1.4.1.311.10.3.12, 1.2.840.113583.1.1.5

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

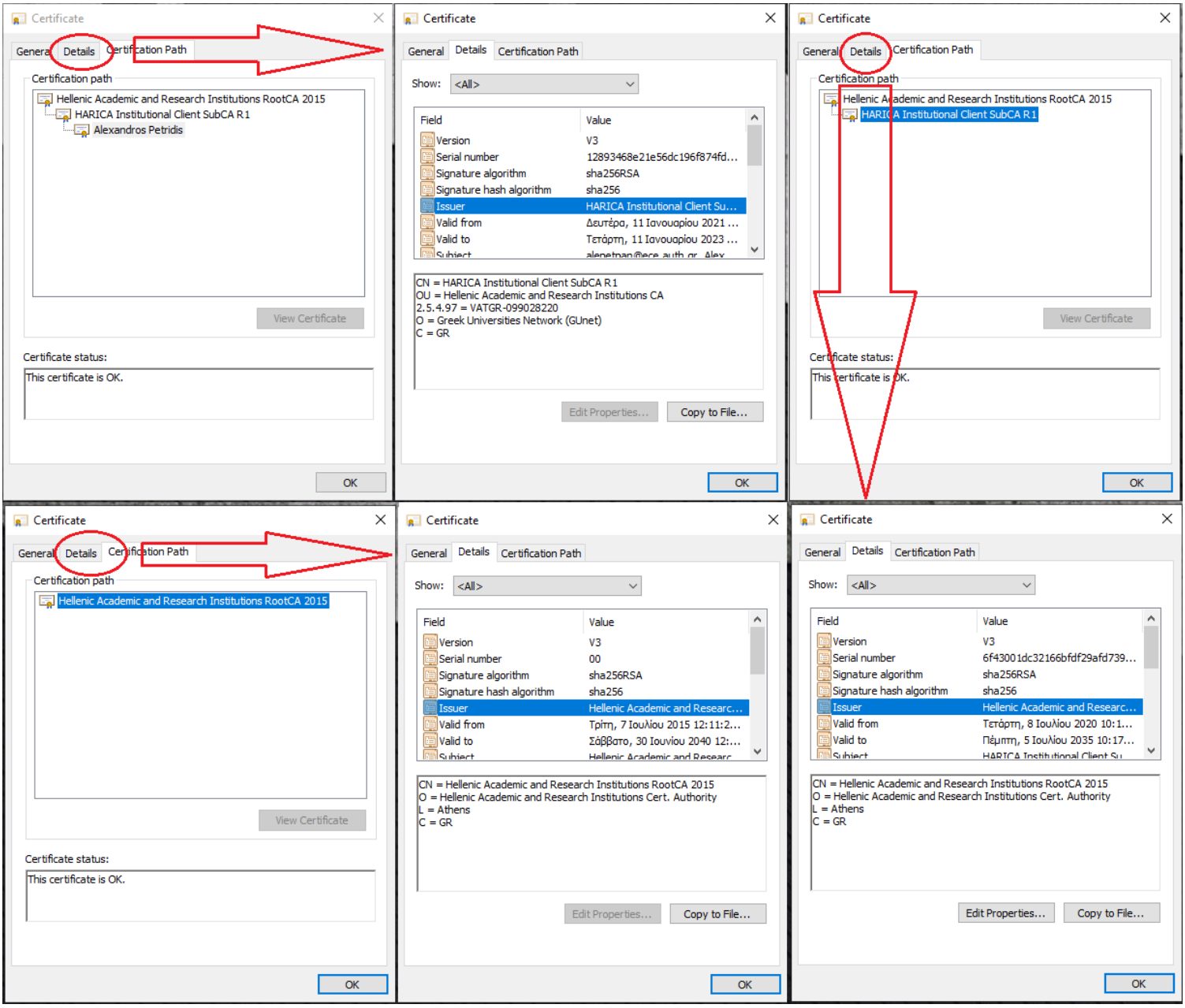
3ι. Αρχές Πιστοποίησης ιεραρχίας της ΥΔΚ

Οι αρχές πιστοποίησης από τις οποίες αποτελείται η ιεραρχία της Υποδομής Δημόσιου Κλειδιού που εξέδωσε το πιστοποιητικό μου με τα Common names τους είναι οι παρακάτω:

Hellenic Academic and Research Institutions RootCA 2015 με CN = Hellenic Academic and Research Institutions RootCA 2015

HARICA Institutional Client SubCA R1 με CN = Hellenic Academic and Research Institutions RootCA 2015

*Η απαντήθηκε με την βοήθεια του certmgr.msc ακολουθούν μερικά στιγμιότυπα οθόνης για μεγαλύτερη κατανόηση της προέλευσης της απάντησης.



Εικόνα 2. Στιγμιότυπα οθόνης του certmgr.msc

4. Θεωρητικές ερωτήσεις κατανόησης

4α. Διαδικασία μη-συμμετρικού αλγορίθμου

Ο μη-συμμετρικός αλγόριθμος χρησιμοποιήθηκε για την δημιουργία του δημόσιου και του ιδιωτικού κλειδιού. Στην περίπτωση του δικού μου πιστοποιητικού χρησιμοποιήθηκε ο μη-συμμετρικός αλγόριθμος RSA.

4β. Αλγόριθμος σύνοψης

Ο αλγόριθμος σύνοψης που παράγει μια σύνοψη του πιστοποιητικού είναι ο SHA256 με RSA κρυπτογράφηση. Η σύνοψη που παράγετε κρυπτογραφείται με το ιδιωτικό κλειδί του συγγραφέα του μηνύματος. Αυτή είναι η ψηφιακή υπογραφή του μηνύματος.

4γ. Κλειδί Υποδομής Δημόσιου Κλειδιού και λόγος ύπαρξης του

Το ιδιωτικό κλειδί της ΥΔΚ εμπλέκεται στο ψηφιακό πιστοποιητικό , για να διασφαλίζεται ο έλεγχος ταυτότητας κατά την αποκρυπτογράφηση με το δημόσιο κλειδί.

4δ. Κλειδί υπογραφής email

Το email υπογράφτηκε με το Ιδιωτικό κλειδί υπογραφής του αποστολέα που σε αυτήν την περίπτωση είμαι εγώ.

4ε. Κλειδί κρυπτογράφησης email

Για την κρυπτογράφηση του email απαιτείται το δημόσιο κλειδί του παραλήπτη, στην περίπτωσή μας του κ. Σιαχούδη