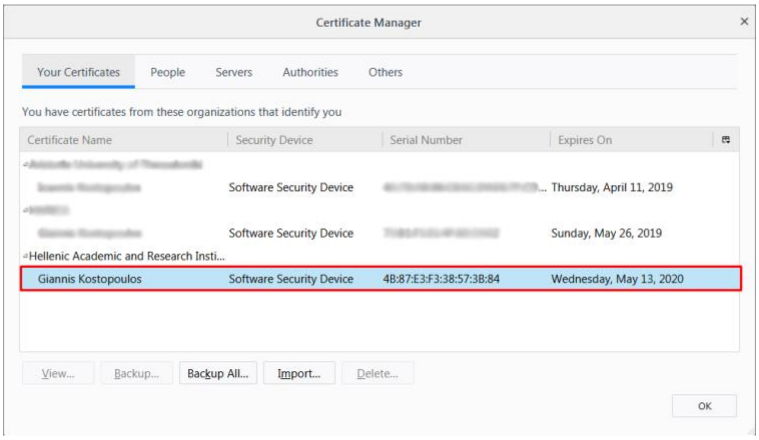
# HARICA Server Certificate Issuance

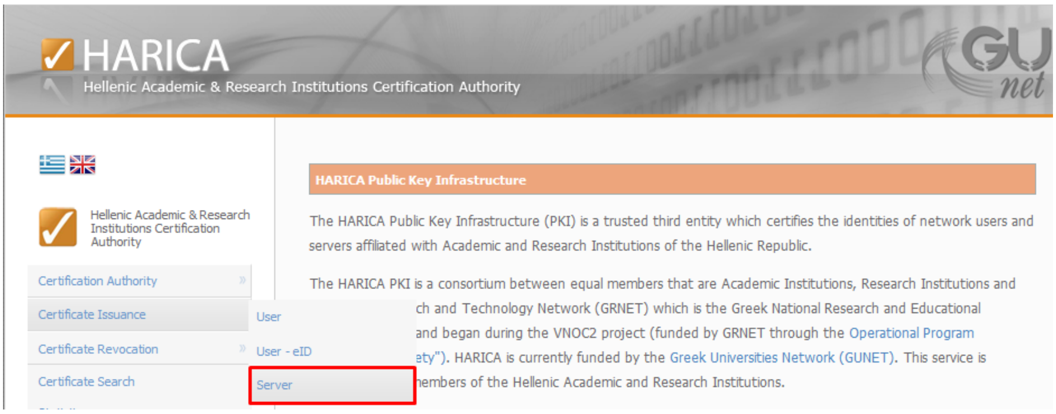
➔ To issue a server Certificate you must have your personal user HARICA Certificate in your browser's certificate store.



You have certificates from these organizations that identify you

| Certificate Name | Security Device | Serial Number | Expires On |
|---|---|---|---|
| [redacted] | | | |
| [redacted] | Software Security Device | [redacted] | Thursday, April 11, 2019 |
| [redacted] | | | |
| [redacted] | Software Security Device | [redacted] | Sunday, May 26, 2019 |
| Hellenic Academic and Research Insti... | | | |
| Giannis Kostopoulos | Software Security Device | 4B:87:E3:F3:38:57:3B:84 | Wednesday, May 13, 2020 |

1. Visit https://app.harica.gr/ and choose **Certificate Issuance -> Server**



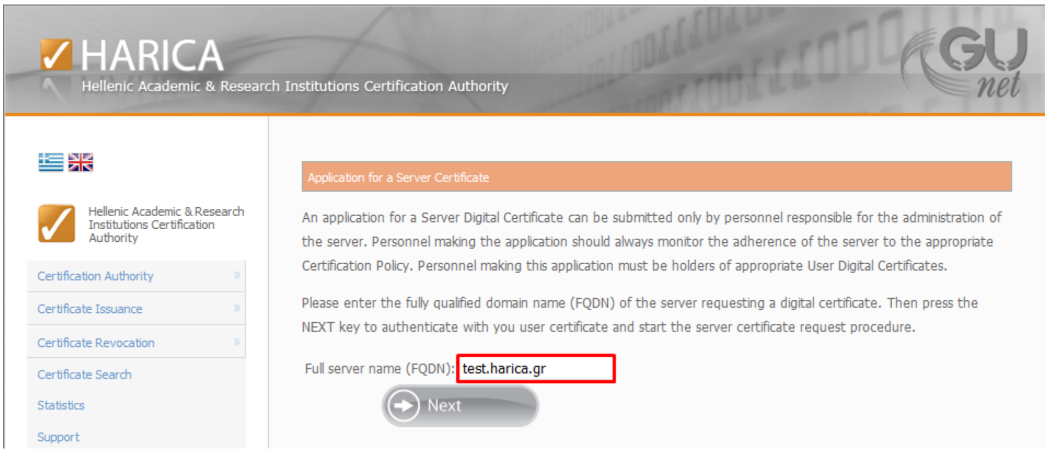
HARICA
Hellenic Academic & Research Institutions Certification Authority
Hellenic Academic & Research Institutions Certification Authority
Certification Authority
Certificate Issuance
Certificate Revocation
Certificate Search
User
User - eID
Server

HARICA Public Key Infrastructure

The HARICA Public Key Infrastructure (PKI) is a trusted third entity which certifies the identities of network users and servers affiliated with Academic and Research Institutions of the Hellenic Republic.

The HARICA PKI is a consortium between equal members that are Academic Institutions, Research Institutions and ...ch and Technology Network (GRNET) which is the Greek National Research and Educational ...and began during the VNOC2 project (funded by GRNET through the Operational Program ...ety"). HARICA is currently funded by the Greek Universities Network (GUNET). This service is ...hembers of the Hellenic Academic and Research Institutions.

2. Enter the server name (Fully Qualified Domain Name – FQDN) you want to issue a Certificate for. In this example, the server name is **test.harica.gr**. Press **Next**



HARICA
Hellenic Academic & Research Institutions Certification Authority
Hellenic Academic & Research Institutions Certification Authority
Certification Authority
Certificate Issuance
Certificate Revocation
Certificate Search
Statistics
Support
Next

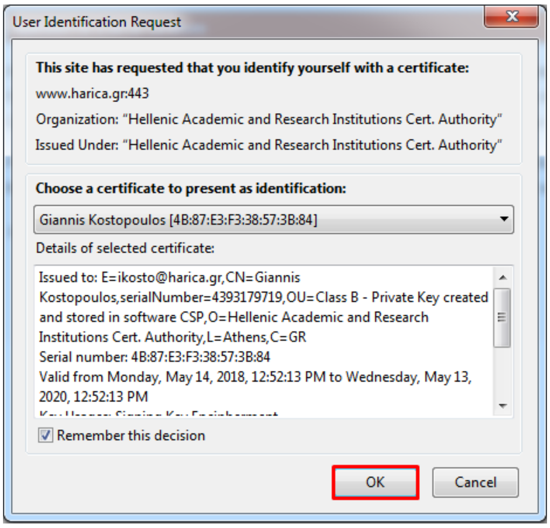
Application for a Server Certificate

An application for a Server Digital Certificate can be submitted only by personnel responsible for the administration of the server. Personnel making the application should always monitor the adherence of the server to the appropriate Certification Policy. Personnel making this application must be holders of appropriate User Digital Certificates.

Please enter the fully qualified domain name (FQDN) of the server requesting a digital certificate. Then press the NEXT key to authenticate with you user certificate and start the server certificate request procedure.

Full server name (FQDN): test.harica.gr

3. Choose your personal HARICA Certificate to authenticate and press **OK**.



**This site has requested that you identify yourself with a certificate:**

www.harica.gr:443

Organization: "Hellenic Academic and Research Institutions Cert. Authority"

Issued Under: "Hellenic Academic and Research Institutions Cert. Authority"

**Choose a certificate to present as identification:**

Giannis Kostopoulos [4B:87:E3:F3:38:57:3B:84]

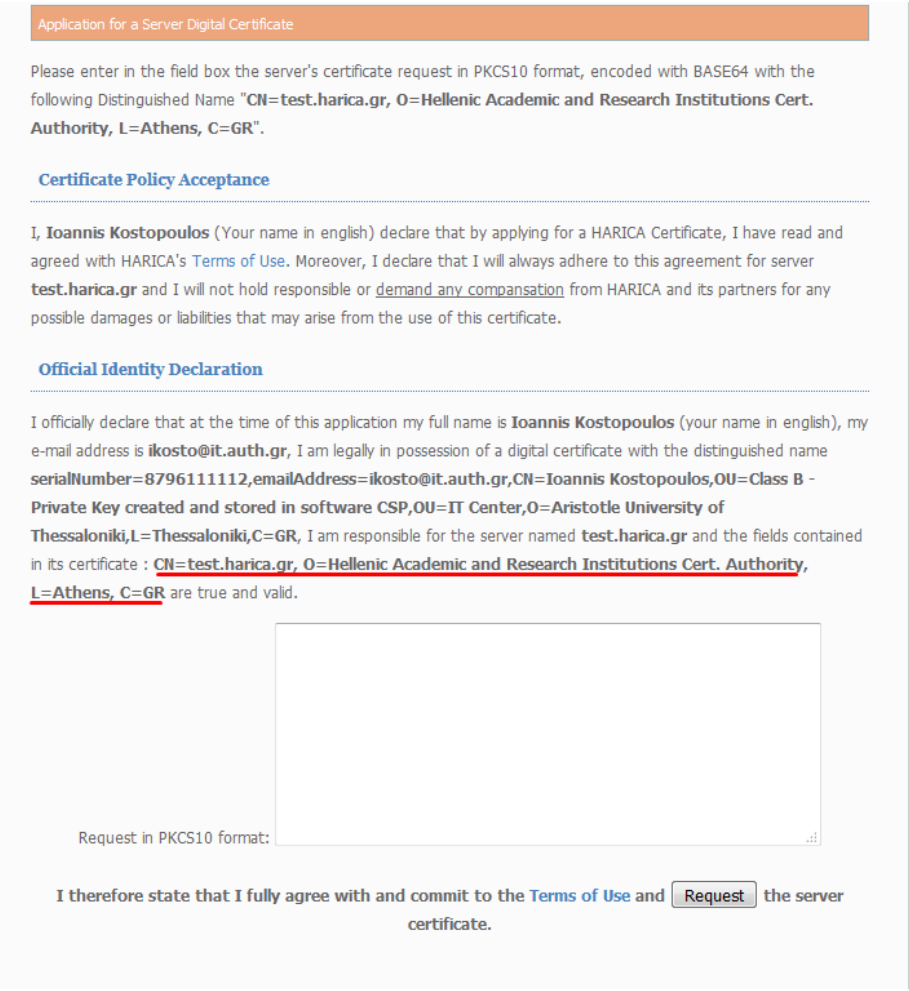
Details of selected certificate:

Issued to: E=ikosto@harica.gr,CN=Giannis Kostopoulos,serialNumber=4393179719,OU=Class B - Private Key created and stored in software CSP,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR
Serial number: 4B:87:E3:F3:38:57:3B:84
Valid from Monday, May 14, 2018, 12:52:13 PM to Wednesday, May 13, 2020, 12:52:13 PM

☑ Remember this decision

4. Once authenticated, read the page information and make sure you COPY the **Distinguished Name** as demonstrated below

**"CN=FQDN, O=Organization, L=Locality, C=Country"**



Please enter in the field box the server's certificate request in PKCS10 format, encoded with BASE64 with the following Distinguished Name "**CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR**".

**Certificate Policy Acceptance**

I, **Ioannis Kostopoulos** (Your name in english) declare that by applying for a HARICA Certificate, I have read and agreed with HARICA's Terms of Use. Moreover, I declare that I will always adhere to this agreement for server **test.harica.gr** and I will not hold responsible or demand any compansation from HARICA and its partners for any possible damages or liabilities that may arise from the use of this certificate.

**Official Identity Declaration**

I officially declare that at the time of this application my full name is **Ioannis Kostopoulos** (your name in english), my e-mail address is **ikosto@it.auth.gr**, I am legally in possession of a digital certificate with the distinguished name **serialNumber=8796111112,emailAddress=ikosto@it.auth.gr,CN=Ioannis Kostopoulos,OU=Class B - Private Key created and stored in software CSP,OU=IT Center,O=Aristotle University of Thessaloniki,L=Thessaloniki,C=GR**, I am responsible for the server named **test.harica.gr** and the fields contained in its certificate : **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** are true and valid.

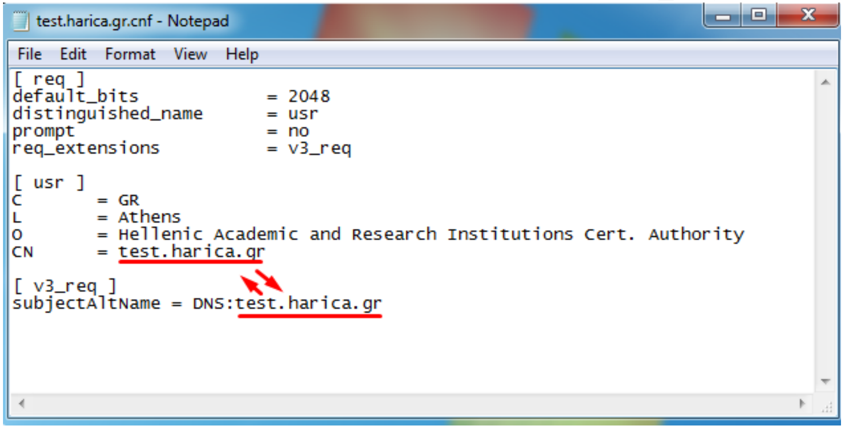
Request in PKCS10 format:

**I therefore state that I fully agree with and commit to the Terms of Use and** Request **the server certificate.**

5. Use the OPENSSL free software to create the Certificate Signing Request. Create a new text document with .cnf extension and paste the following using the Distinguished Name details from the previous step :

```
[ req ]
default_bits = 2048
distinguished_name = usr
prompt = no
req_extensions = v3_req

[usr ]
C = Country
L = Locality
O = Organization
CN = FQDN

[ v3_req ]
subjectAltName = DNS:FQDN
```

➔ You must have the same server name in the [usr] and [v3_req] fields



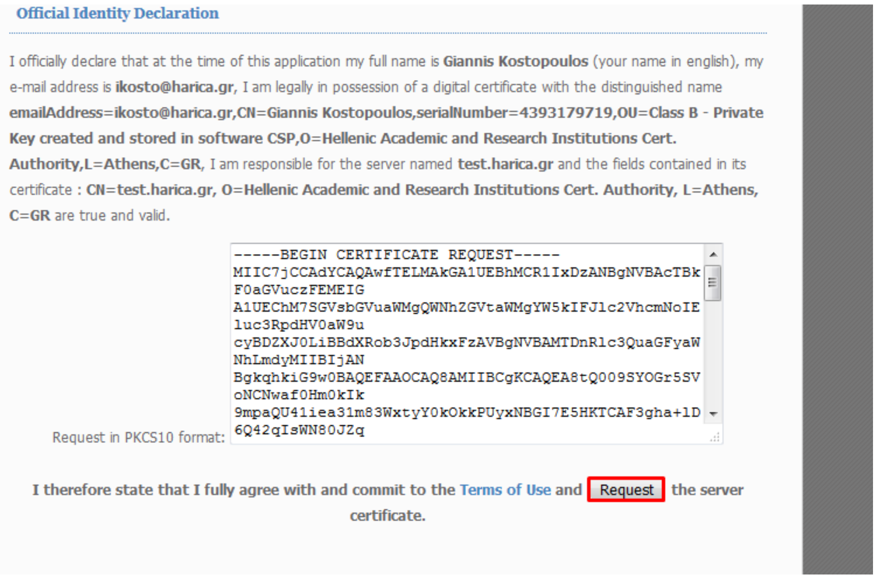
```
[ req ]
default_bits              = 2048
distinguished_name        = usr
prompt                    = no
req_extensions            = v3_req

[ usr ]
C        = GR
L        = Athens
O        = Hellenic Academic and Research Institutions Cert. Authority
CN       = test.harica.gr

[ v3_req ]
subjectAltName = DNS:test.harica.gr
```

6. Using openssl, run the following command to generate the server.key /server.req :

```
openssl req -new -keyout server.key -config server.cnf -out server.req -nodes
```

**IMPORTANT NOTICE**: The file named server.key contains the **UNENCRYPTED PRIVATE KEY** associated with the Certificate that will be issued so it must be properly protected with appropriate permissions.

7. Open server.req with any text editor (like Notepad) and paste the contents in the previous web form, in the “PKCS10 format” field. Press **Request**.



**Official Identity Declaration**

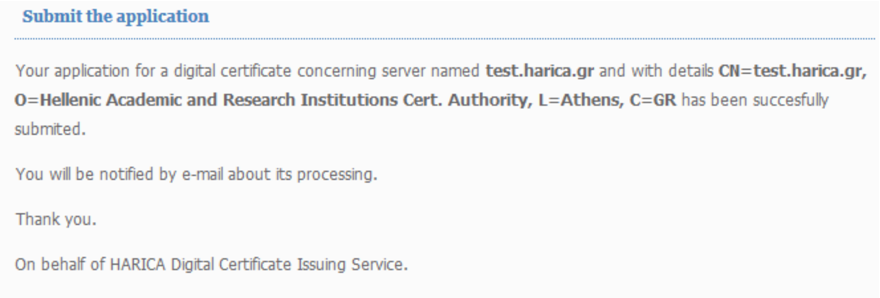
I officially declare that at the time of this application my full name is **Giannis Kostopoulos** (your name in english), my e-mail address is **ikosto@harica.gr**, I am legally in possession of a digital certificate with the distinguished name **emailAddress=ikosto@harica.gr,CN=Giannis Kostopoulos,serialNumber=4393179719,OU=Class B - Private Key created and stored in software CSP,O=Hellenic Academic and Research Institutions Cert. Authority,L=Athens,C=GR**, I am responsible for the server named **test.harica.gr** and the fields contained in its certificate : **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** are true and valid.

Request in PKCS10 format:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwfTELMAkGA1UEBhMCR1IxDzANBgNVBAcTBk
F0aGVuczFEMEIG
A1UEChM7SGVsbGVuaWMgQWNhZGVtaWMgYW5kIFJlc2VhcmNoIE
luc3RpdHV0aW9u
cyBDZXJ0LiBBdXRob3JpdHkxFzAVBgNVBAMTDnRlc3QuaGFyaW
NhLmdyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8tQ009SYOGr5SV
oNCNwaf0Hm0kIk
9mpaQU41iea31m83WxtyY0kOkkPUyxNBGI7E5HKTCAF3gha+1D
6Q42qIsWN80JZq
```

**I therefore state that I fully agree with and commit to the Terms of Use and** Request **the server certificate.**

8. Once the Certificate application is submitted successfully, you will have to wait for a validator of your Organization to check and approve your request.



**Submit the application**

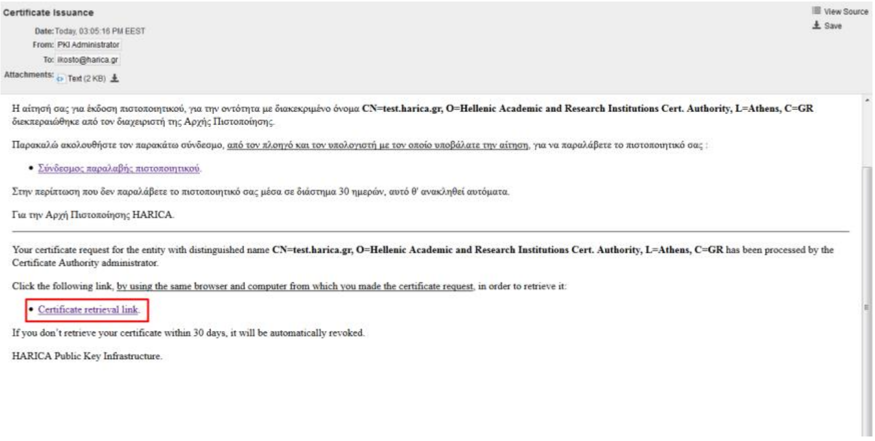
Your application for a digital certificate concerning server named **test.harica.gr** and with details **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** has been succesfully submited.

You will be notified by e-mail about its processing.

Thank you.

On behalf of HARICA Digital Certificate Issuing Service.

9. After the approval of your request you will receive an email to proceed with the Certificate acceptance. Press **Certificate retrieval link**.



**Certificate Issuance**

Date: Today, 03:05:16 PM EEST
From: PKI Administrator
To: ikosto@harica.gr
Attachments: Text (2 KB)

Η αίτησή σας για έκδοση πιστοποιητικού, για την οντότητα με διακεκριμένο όνομα **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** διεκπεραιώθηκε από τον διαχειριστή της Αρχής Πιστοποίησης.

Παρακαλώ ακολουθήστε τον παρακάτω σύνδεσμο, από τον πλοηγό και τον υπολογιστή με τον οποίο υποβάλατε την αίτηση, για να παραλάβετε το πιστοποιητικό σας :

- Σύνδεσμος παραλαβής πιστοποιητικού.

Στην περίπτωση που δεν παραλάβετε το πιστοποιητικό σας μέσα σε διάστημα 30 ημερών, αυτό θ' ανακληθεί αυτόματα.

Για την Αρχή Πιστοποίησης HARICA.

Your certificate request for the entity with distinguished name **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** has been processed by the Certificate Authority administrator.

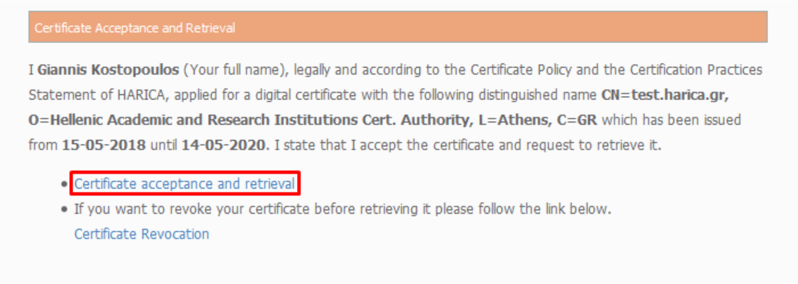
Click the following link, by using the same browser and computer from which you made the certificate request, in order to retrieve it:

- Certificate retrieval link.

If you don't retrieve your certificate within 30 days, it will be automatically revoked.

HARICA Public Key Infrastructure.

10. If all expected information is accurate, press **Certificate acceptance and retrieval**.

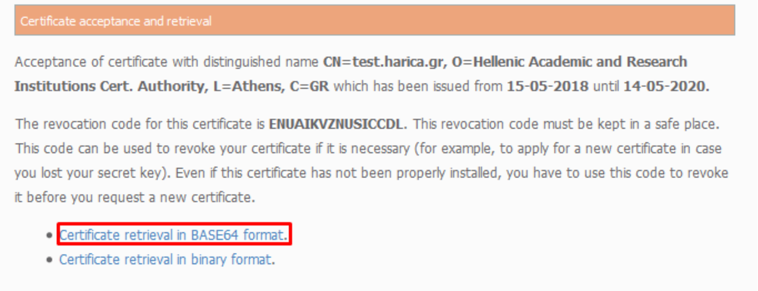


Certificate Acceptance and Retrieval

I **Giannis Kostopoulos** (Your full name), legally and according to the Certificate Policy and the Certification Practices Statement of HARICA, applied for a digital certificate with the following distinguished name **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** which has been issued from **15-05-2018** until **14-05-2020**. I state that I accept the certificate and request to retrieve it.

- Certificate acceptance and retrieval
- If you want to revoke your certificate before retrieving it please follow the link below.
  Certificate Revocation

11. Press **Certificate retrieval in BASE64 format** and save your Certificate in PEM (base64) format.



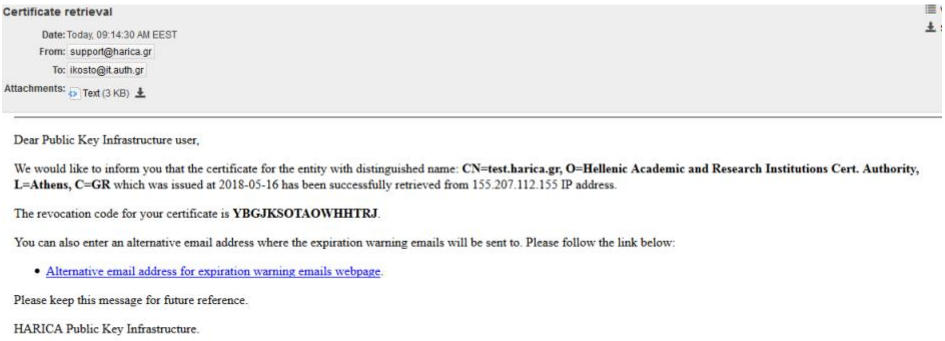
Certificate acceptance and retrieval

Acceptance of certificate with distinguished name **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** which has been issued from **15-05-2018** until **14-05-2020.**

The revocation code for this certificate is **ENUAIKVZNUSICCDL**. This revocation code must be kept in a safe place. This code can be used to revoke your certificate if it is necessary (for example, to apply for a new certificate in case you lost your secret key). Even if this certificate has not been properly installed, you have to use this code to revoke it before you request a new certificate.

- Certificate retrieval in BASE64 format.
- Certificate retrieval in binary format.

12. After you retrieve your Certificate you will receive a confirmation mail. Please save the mail since it contains critical information like the revocation code of the Certificate.



**Certificate retrieval**

Date: Today, 09:14:30 AM EEST
From: support@harica.gr
To: ikosto@it.auth.gr
Attachments: Text (3 KB)

Dear Public Key Infrastructure user,

We would like to inform you that the certificate for the entity with distinguished name: **CN=test.harica.gr, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR** which was issued at 2018-05-16 has been successfully retrieved from 155.207.112.155 IP address.

The revocation code for your certificate is **YBGJKSOTAOWHHTRJ**.

You can also enter an alternative email address where the expiration warning emails will be sent to. Please follow the link below:

- Alternative email address for expiration warning emails webpage.

Please keep this message for future reference.

HARICA Public Key Infrastructure.