

Έκδοση και εγκατάσταση ψηφιακού πιστοποιητικού - Harica

Έκδοση ψηφιακού πιστοποιητικού

Οι ακόλουθες οδηγίες αφορούν την έκδοση ψηφιακού πιστοποιητικού τύπου Β (χωρίς χρήση εξωτερικής αποθηκευτικής συσκευής e-token ή ακαδημαϊκής ταυτότητας) της **Αρχής Πιστοποίησης Ελληνικών Ακαδημαϊκών & Ερευνητικών Ιδρυμάτων**. (HARICA, <https://www.harica.gr/>). Σε περίπτωση που επιθυμείτε να εκδώσετε πιστοποιητικό σε εξωτερική μονάδα αποθήκευσης ή σε ακαδημαϊκή ταυτότητα, παρακαλώ απευθυνθείτε στο τμήμα IT, καθώς θα απαιτηθεί η παρέμβαση του αρμόδιου validator.

Η διαδικασία που περιγράφεται στο παρόν κείμενο αφορά την έκδοση και εγκατάσταση ψηφιακού πιστοποιητικού με την χρήση των περιηγητών **Google Chrome** και **Mozilla Firefox**.

Στον περιηγητή (browser) που χρησιμοποιείτε, πληκτρολογήστε την διεύθυνση: **<https://ca.ihu.edu.gr>** . Από το μενού αριστερά, επιλέξτε **Certificate Issuance – User (Έκδοση πιστοποιητικού – χρήση)**.

HARICA
Hellenic Academic & Research Institutions Certification Authority

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 the National Technology Network (GRNET) which is the Greek National Research and Educational Network (NREN) the VNOCC project (funded by GRNET through the Operational Program "Information Society"). HARICA is supported by the Greek Universities Network (GUNET). This service is available for the members of the Hellenic Academic and Research Institutions.

The HARICA PKI Goals

The main goal of HARICA is the deployment of an infrastructure for secure communication between the members of the collaborating Academic and Research Institutions.

The HARICA PKI :

- Implements a Public Key Hierarchy having root authority the HARICA Root Certification Authority, which collaborates with the other parties' Certification Authorities in Greece and abroad aiming at widening the network of trust.
- Issues -on behalf of its members- digital certificates for network servers, in order to secure the data exchanged with the network users.
- Issues -on behalf of its members- digital certificates for network users, which can be used to prove the identity of the users while using network services and to secure email communication.

Policies and Procedures

The HARICA PKI issues certificates to entities according to certain procedures included in the "Certificate Practice Statement" and must also comply with the "Certification Policies" of each Certification Authority.

Independent audit report

HARICA PKI has been audited by an independent auditor and was found to be fully compliant with the requirements of ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421 and CA/Browser Forum Baseline Requirements.

You may download the ETSI EN 319 411-1 411-2, 421, CA/Browser Forum BR 1.4.5 latest audit report (year 2017). These reports are also available at the QMSCERT Website. Here is a link to the latest audit report:

- ETSI EN 319 411-1, 411-2, 421, CA/Browser Forum BR 1.4.5

Trust

Relevant Links

- Digital Signatures at the Hellenic Telecommunications & Post Commission
- European Committee for Academic Middleware
- European Middleware Coordination and Collaboration
- Public Key Infrastructure at AUTH

Στην επόμενη σελίδα, εισάγετε το όνομά σας (**Given name**), επίθετο (**Surname**) (θα πρέπει να υποβληθούν όπως ακριβώς αναγράφονται σε ταυτότητα ή διαβατήριό με λατινικούς χαρακτήρες) και την διεύθυνση αλληλογραφίας σας στο Διεθνές Πανεπιστήμιο Ελλάδος (με την κατάληξη @ihu.gr). Μην τσεκάρετε το **Verification with eiDAS credentials** και πατήστε **Next**.



Hellenic Academic & Research Institutions Certification Authority





International Hellenic University

- Certification Authority >
- Certificate Issuance >
- Certificate Revocation >
- Certificate Search
- Statistics

Relevant Links

- 

Digital Signatures at the Hellenic Telecommunications & Post Commission
- 

European Committee for Academic Middleware
- 

European Middleware Coordination and Collaboration
- 

International Hellenic University

Application for a User Certificate

Please enter your e-mail address and your full name. Then press the "NEXT" key in order to initiate the user certificate request process.

You may skip the Given Name and Surname fields if your institution supports Single sign-on (SSO) or LDAP login or if you select the verification with eIDAS option.

Given name:

Surname:

E-mail Address:

Verification with eIDAS credentials:

Next

The eIDAS integration was funded by the Connecting Europe Facility (CEF)



Θα λάβετε την ακόλουθη ειδοποίηση για να ελέγξετε την ηλεκτρονική σας αλληλογραφία.



Hellenic Academic & Research Institutions Certification Authority





International Hellenic University

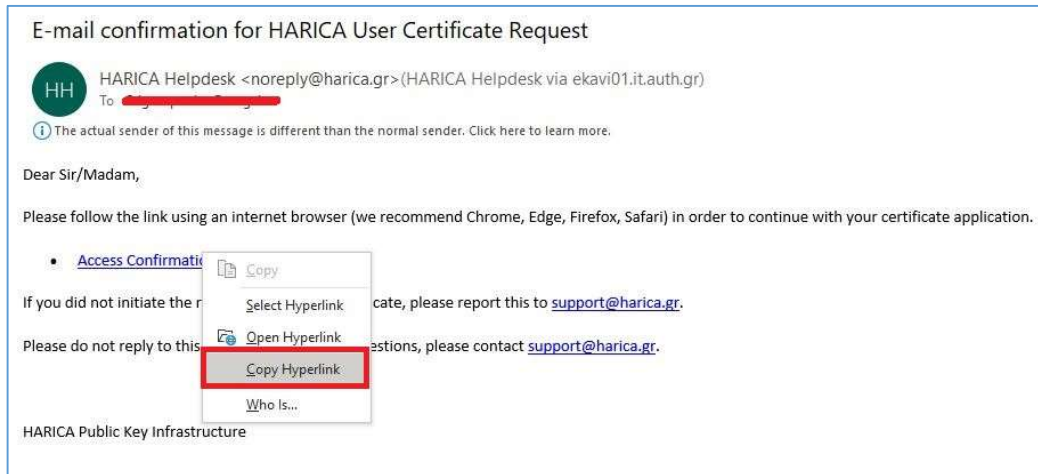
- Certification Authority >
- Certificate Issuance >
- Certificate Revocation >
- Certificate Search
- Statistics

Application for a User Certificate

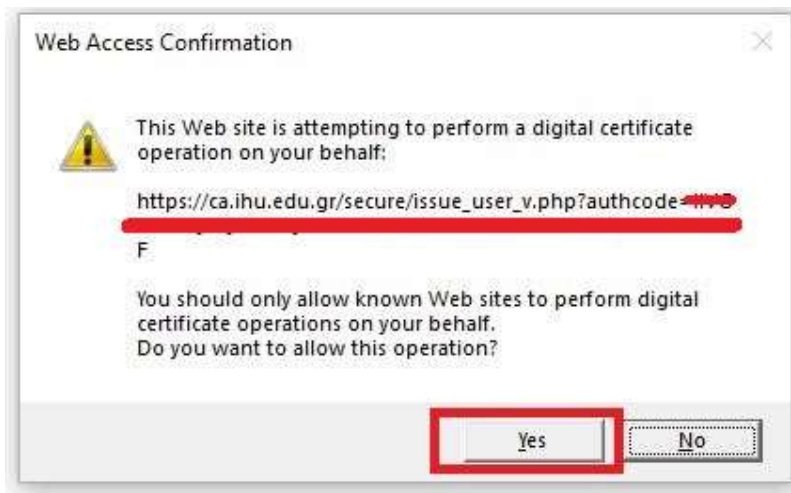
In order to proceed with the request for a digital certificate, please check your e-mail with your provider **International Hellenic University** for a confirmation message from HARICA and follow the instructions therein.

In case you have not received any email or encountered an error, please contact support at [harica.gr](mailto:support@harica.gr).

Στο ηλεκτρονικό μήνυμα που λάβατε στην διεύθυνση που δηλώσατε κατά το πρώτο βήμα, κάνετε δεξί κλικ στον σύνδεσμο **Access Confirmation Link**. Στην συνέχεια κάνετε **Αντιγραφή διεύθυνσης συνδέσμου (Copy the Hyperlink)** και επικόλλησή του σε μία νέα καρτέλα ή παράθυρο του περιηγητή σας.



Πατήστε **yes** στο αναδυόμενο παράθυρο.



Στο επόμενο παράθυρο κάντε κλικ στο **Browse** για να ανεβάσετε ένα ψηφιακό αντίγραφο της αστυνομικής σας ταυτότητας ή διαβατηρίου (μπορείτε να ανεβάσετε και δύο αρχεία, ένα για κάθε όψη). Στην συνέχεια εισάγετε ένα password της επιλογής σας για να προστατέψετε το προσωπικό σας κλειδί (θα το χρησιμοποιήσετε και στην συνέχεια). Κάνετε κλικ στο **Save private key**.

Solemn Statement of Identification

I solemnly state by submitting this request for a digital certificate that my full name is [REDACTED], the email address [REDACTED] belongs to me and the information which is part of my certificate Email=[REDACTED]@ihu.edu.gr, serialNumber=[REDACTED], CN=[REDACTED], GivenName=[REDACTED], Surname=[REDACTED], O=International Hellenic University, L=Thessaloniki, C=GR is true and valid.

You are required to upload a file that contains an official photo ID for Identity validation (Passport/ID). Scanned documents must clearly display the full name (in Latin) and picture of the Applicant with resolution at least 400x400 and must not exceed 2MB in size. IDs that do not display the full name in Latin will not be accepted and the request will be denied.

Disclaimer: The ID upload is **mandatory** in order to request a certificate.

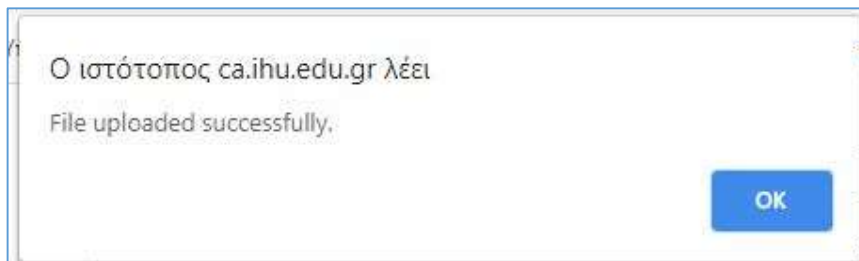
Identity upload

Private key protection

You have just created a new private key on your device. Please insert a password to protect it. Please note that the password is required to obtain and use the certificate and should therefore be secured and not forgotten.

Please repeat the password

Εάν δεν υπάρχει κάποιο πρόβλημα με την ανάρτηση των αρχείων αντιγράφων της αστυνομικής ταυτότητας ή του διαβατηρίου θα πρέπει να εμφανιστεί το ακόλουθο παράθυρο.



Στο επόμενο παράθυρο, αφήστε τσεκαρισμένο το **S/MIME + eSignature** (μη πατήσετε ξανά στο **Browse**) και κάνετε κλικ στο **Request (Αποδοχή)**

Solemn Statement of Identification

I solemnly state by submitting this request for a digital certificate that my full name is [redacted], the email address [redacted] belongs to me and the information which is part of my certificate Email=[redacted], serialNumber=[redacted], CN=[redacted], GivenName=[redacted], Surname=[redacted], O=International Hellenic University, L=Thessaloniki, C=GR is true and valid.

You are required to upload a file that contains an official photo ID for Identity validation (Passport/ID). Scanned documents must clearly display the full name (in Latin) and picture of the Applicant with resolution at least 400x400 and must not exceed 2MB in size. IDs that do not display the full name in Latin will not be accepted and the request will be denied.

Disclaimer: The ID upload is **mandatory** in order to request a certificate.

Identity upload:

Certificate usage:

S/MIME

S/MIME + eSignature

I agree with the [Terms of Use](#), sign the statements and the Certificate.

Όπως περιγράφεται και την εικόνα που ακολουθεί, αφού υποβάλλετε την αίτησή σας, θα πρέπει να περιμένεται ώστε ένας εκ των αρμοδίων validator του ιδρύματος να επιβεβαιώσει την ταυτότητά σας και να εγκρίνει την αίτηση του πιστοποιητικού.

Application for a User Certificate

Application Acceptance Status

Your application for a digital certificate associated with the e-mail address [redacted] and distinguished name Email=[redacted], serialNumber=[redacted], CN=[redacted], OU=Class B - Private Key created and stored in software CSP, GivenName=[redacted], Surname=[redacted], O=International Hellenic University, L=Thessaloniki, C=GR, has been successfully submitted.

After approval of your request you will receive an e-mail from HARICA with further instructions on how to obtain your digital certificate. If you do not receive such an e-mail in 5 working days please contact support at harica.gr.

Μόλις ο validator εγκρίνει το πιστοποιητικό, θα λάβετε ένα email για την παραλαβή του πιστοποιητικού σας. Κάνετε δεξί κλικ στο **Παραλαβή του πιστοποιητικού μου (Get my certificate)** και στην συνέχεια **Αντιγραφή συνδέσμου (Copy hyperlink)**. Επικολλήστε τον σύνδεσμο σε μία νέα καρτέλα ή παράθυρο του περιηγητή σας.

Your HARICA Digital Certificate request has been approved

HP HARICA PKI Administrator <noreply@harica.gr>
To [redacted]

Δευ 27/04/2020 11:09 πμ

Αγαπητέ Κύριε/Κυρία,

Το πιστοποιητικό σας για την οντότητα με διακεκριμένο όνομα [redacted], serialNumber=[redacted], CN=[redacted], OU=Class B - Private Key created and stored in software CSP, GivenName=[redacted], Surname=[redacted], O=International Hellenic University, L=Thessaloniki, C=GR έχει εκδοθεί από τον διαχειριστή της Αρχής Πιστοποίησης.

Ακολουθήστε τον παρακάτω σύνδεσμο χρησιμοποιώντας τον πλοηγό και τον υπολογιστή με τον οποίο υποβάλατε την αίτηση για να παραλάβετε το πιστοποιητικό σας:

- [Παραλαβή του πιστοποιητικού μου](#)

Στην περίπτωση που δεν παραλάβετε το πιστοποιητικό σας εντός 30 ημερών, αυτό θα ανακληθεί αυτόματα.

Παρακαλώ μην απαντήσετε σε αυτό ο e-mail. Για οτιδήποτε περαιτέρω παρακαλώ επικοινωνήστε με το support@harica.gr

Υποδομή Δημοσίου Κλειδιού HARICA

Dear Sir/Madam,

Your certificate for the entity with distinguished name Email=[redacted], serialNumber=[redacted], CN=[redacted], OU=Class B - Private Key created and stored in software CSP, GivenName=[redacted], Surname=[redacted], O=International Hellenic University, L=Thessaloniki, C=GR has been issued by the Certificate Authority administrator.

Click the following link using the same Internet browser and computer from which you submitted the request in order to retrieve the certificate:

- [Get my certificate](#)

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

Please do not reply to this email. If you have any questions please contact support@harica.gr

HARICA Public Key

(Note: In the original image, a context menu is open over the 'Copy Hyperlink' link, with 'Copy Hyperlink' selected.)

Στο επόμενο παράθυρο, πατήστε στο **I accept and want to retrieve my certificate**

HARICA + IHU
Hellenic Academic & Research Institutions Certification Authority

GU net

International Hellenic University

Certification Authority
Certificate Issuance
Certificate Revocation
Certificate Search
Statistics

Relevant Links

- Digital Signatures at the Hellenic Telecommunications & Post Commission
- European Committee for Academic Middleware
- European Middleware Coordination and Collaboration
- International Hellenic University

Certificate Acceptance and Retrieval

I, [redacted] applied for a HARICA digital certificate with the following Distinguished Name Email=[redacted], serialNumber=[redacted], CN=[redacted], OU=Class B - Private Key created and stored in software CSP, GivenName=[redacted], Surname=[redacted], O=International Hellenic University, L=Thessaloniki, C=GR which has been issued from 27-04-2020 until 27-04-2022.

I state that I accept the certificate and request to retrieve it according to the Terms of Use and the Certification Practices of HARICA.

- I accept and want to retrieve my certificate
- I changed my mind and want to revoke my certificate

Ξεκλειδώστε το προσωπικό σας κλειδί, εισάγοντας το password που δημιουργήσατε νωρίτερα.

Private key protection

Please insert your private key's password to unlock it

..... |

The revocation code for this certificate is [REDACTED]. 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.

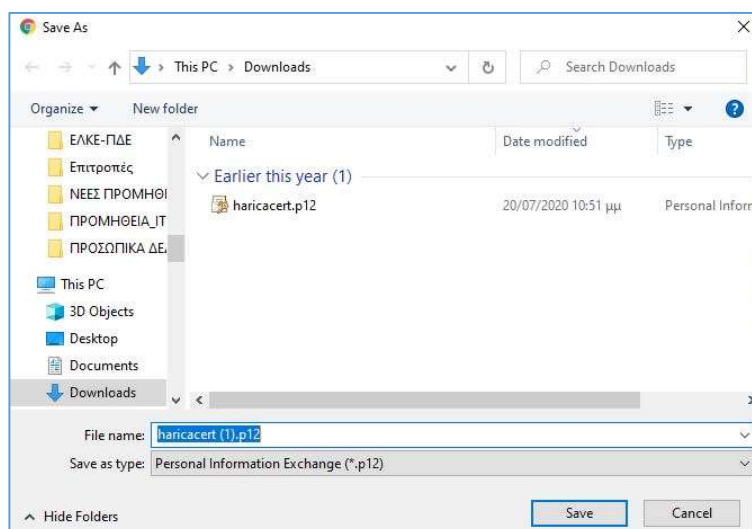
Κάνετε κλικ στο **Download certificate & private key**

Certificate Acceptance

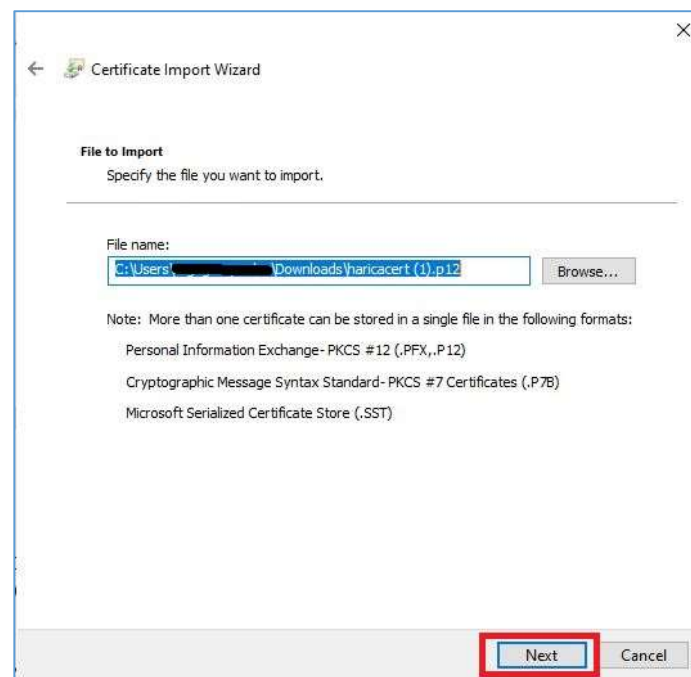
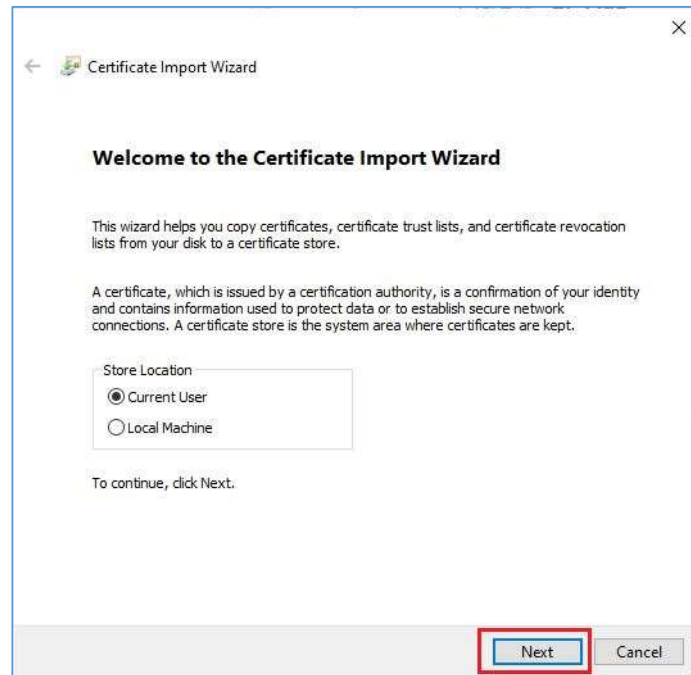
Acceptance of certificate with distinguished name Email=[REDACTED], serialNumber=[REDACTED], CN=[REDACTED], OU=Class B - Private Key created and stored in software CSP, GivenName=[REDACTED], Surname=[REDACTED], O=International Hellenic University, L=Thessaloniki, C=GR which has been issued from 11-10-2020 until 11-10-2022.

The revocation code for this certificate is [REDACTED]. 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.

Σώστε το αρχείο του πιστοποιητικού σας (*.p12) στον υπολογιστή σας.



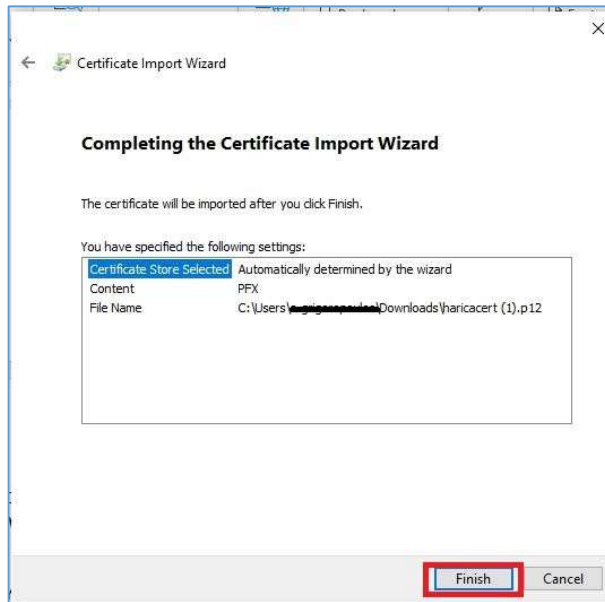
Κάνετε διπλο κλικ στο αρχείο πιστοποιητικού που κατεβάσατε για να ξεκινήσετε τον οδηγό εγκατάστασης του πιστοποιητικού. Πατήστε **Next** σε κάθε στάδιο του οδηγού.



Εισάγετε ξανά το ίδιο password με το οποίο ξεκλειδώσατε το προσωπικό σας κλειδί.

The screenshot shows the 'Certificate Import Wizard' window at the 'Private key protection' step. The text reads: 'Private key protection. To maintain security, the private key was protected with a password. Type the password for the private key.' There is a 'Password:' label above a text input field containing ten dots. A red rectangle highlights this input field. Below the field is a checkbox labeled 'Display Password'. Underneath is the 'Import options' section with four checkboxes: 'Enable strong private key protection...', 'Mark this key as exportable...', 'Protect private key using virtualized-based security(Non-exportable)', and 'Include all extended properties.' The 'Include all extended properties.' checkbox is checked. At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.

The screenshot shows the 'Certificate Import Wizard' window at the 'Certificate Store' step. The text reads: 'Certificate Store. Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store:'. Below the second option is a text input field labeled 'Certificate store:' and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons, with the 'Next' button highlighted by a red rectangle.



Αμέσως μετά θα πρέπει να λάβετε ένα μήνυμα ότι το πιστοποιητικό σας εγκαταστάθηκε επιτυχώς.

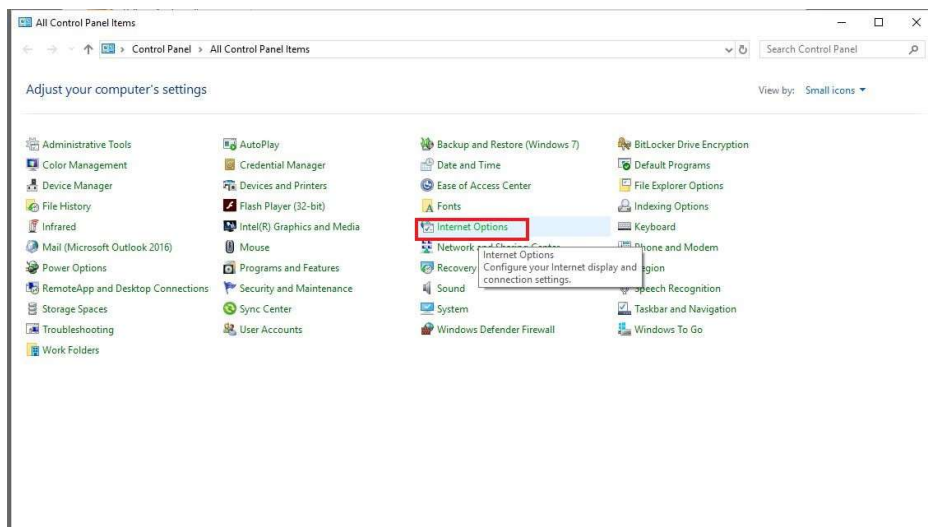


Θα λάβετε επίσης ένα email με τίτλο **Certificate retrieval**, το οποίο θα σας ενημερώνει για την διάρκεια ισχύος του ψηφιακού πιστοποιητικού που μόλις εκδόθηκε (δύο έτη) αλλά και για τον κωδικό ανάκλησης (revocation code). Κρατήστε τον κωδικό ανάκλησης σε ασφαλές σημείο, ώστε να είναι δυνατή η ανάκληση του πιστοποιητικού, σε περίπτωση που κάτι τέτοιο απαιτηθεί.

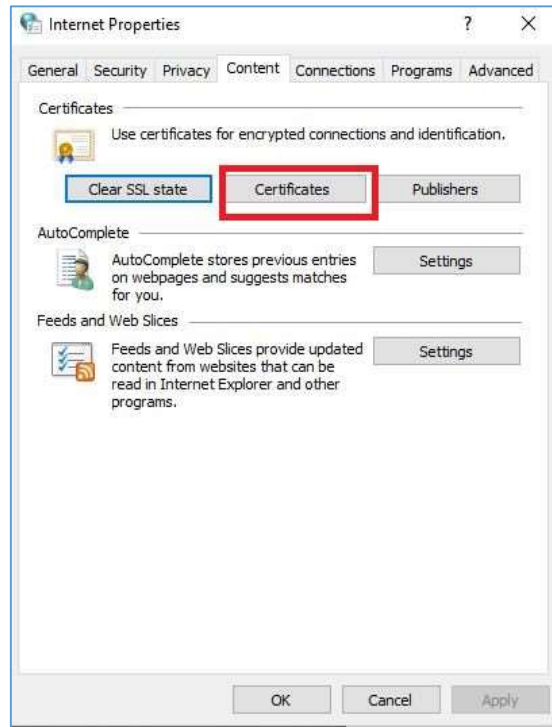
Επιβεβαίωση εγκατάστασης

Ως μία επιπλέον προαιρετική διαδικασία επιβεβαίωσης της εγκατάστασης του ψηφιακού πιστοποιητικού, πηγαίνετε στον **Πίνακα Ελέγχου (Control Panel)**.

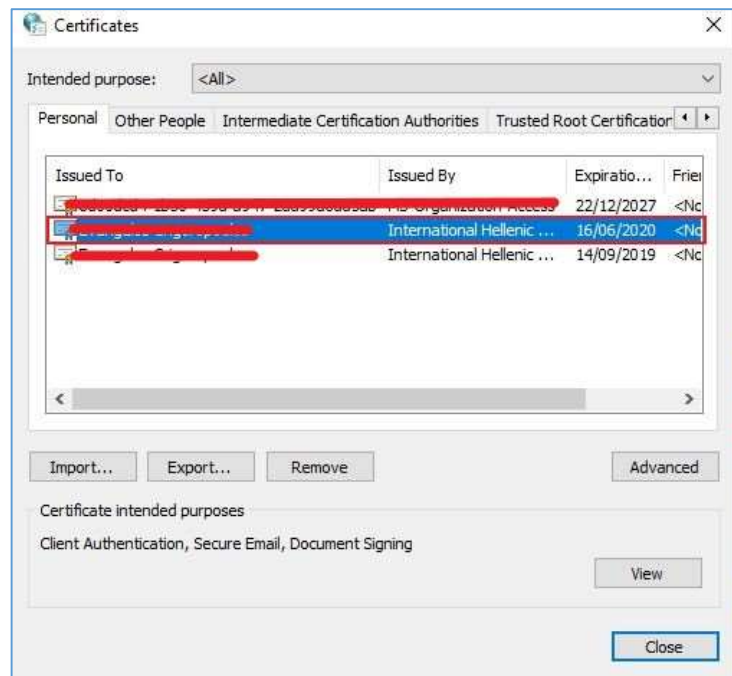
Από τα αντικείμενα του Πίνακα Ελέγχου, επιλέξτε **Επιλογές Internet (Internet Options)**.



Επιλέξτε την καρτέλα **Περιεχόμενο (Content)** και κάνετε κλικ στο **Πιστοποιητικά (Certificates)**.



Στο παράθυρο **Certificates**, θα εντοπίσετε το πιστοποιητικό που μόλις εκδόθηκε, την ενδιάμεση αρχή έκδοσης (International Hellenic University) και την ημερομηνία λήξης του.



Σημαντικό: Δεν μπορείτε να επαναλάβετε την παραπάνω διαδικασία για την εγκατάσταση του ψηφιακού πιστοποιητικού τύπου Β και σε άλλη συσκευή

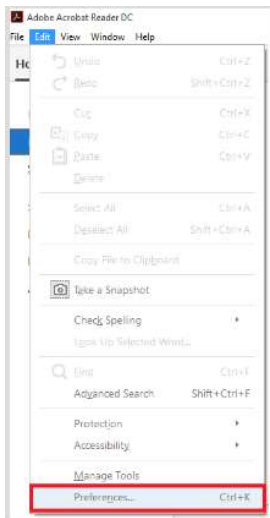
(PC/laptop). Στην περίπτωση αυτή, θα πρέπει να κάνετε εξαγωγή του πιστοποιητικού σε ένα απλό flash drive - πατώντας στο κουμπί **Export** της παραπάνω εικόνας. Με την αντίστροφη διαδικασία – κάνοντας **Import** - εισάγετε το πιστοποιητικό στην δεύτερη συσκευή.

Προσθήκη ψηφιακής υπογραφής σε έγγραφα PDF

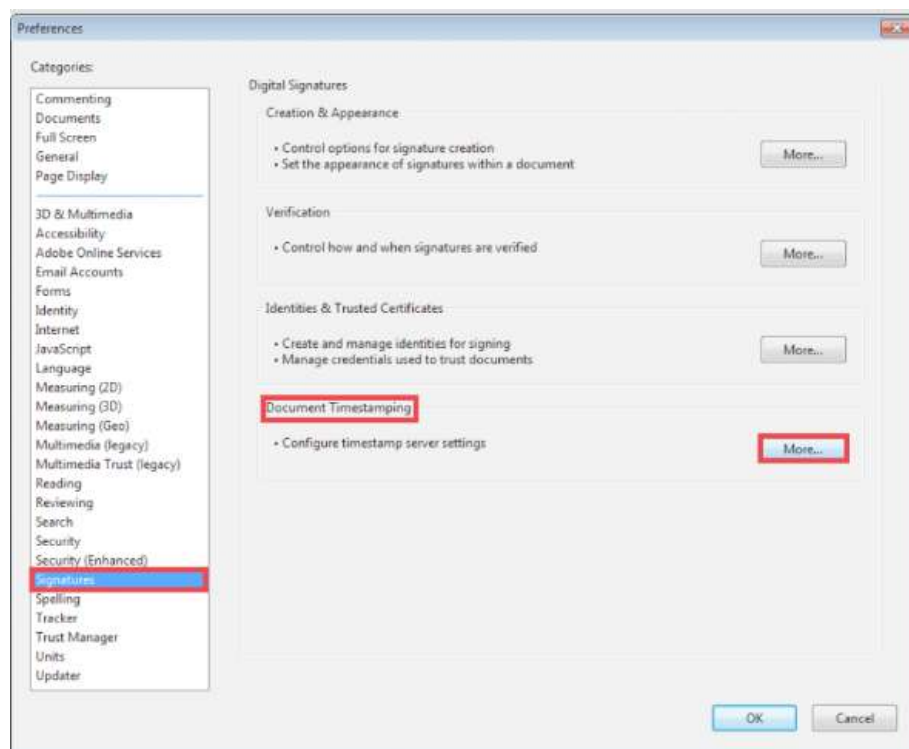
Κατεβάστε και εγκαταστήστε την εφαρμογή **Adobe Reader DC**:
<https://get.adobe.com/reader/>

Προσθήκη διακομιστή χρονοσήμανσης

Ανοίξετε τον Adobe Reader DC και επιλέξτε **Edit - Preferences**



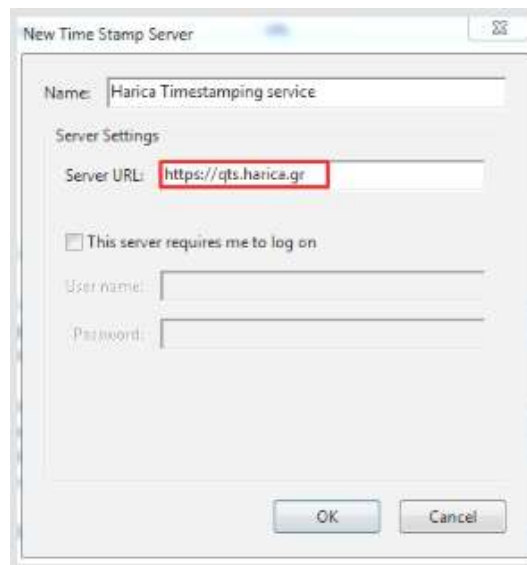
Επιλέξτε **Signatures – Document Timestamping - More**



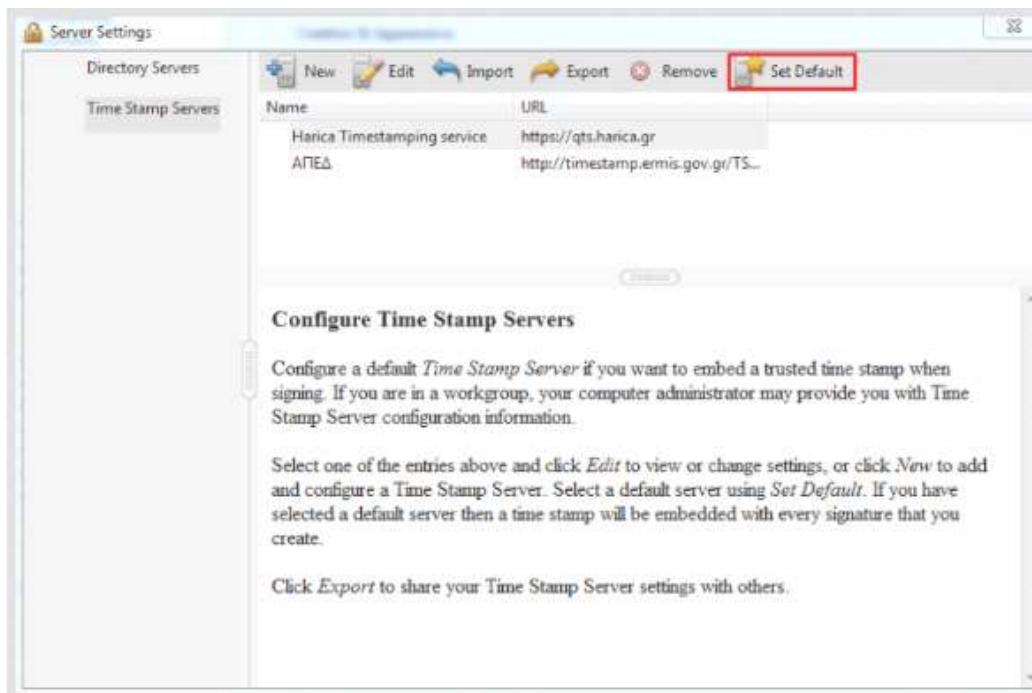
Στο αναδυόμενο παράθυρο, επιλέξτε **New**.

- Name: **Harica Timestamping Service**
- Server URL: <https://qts.harica.gr>

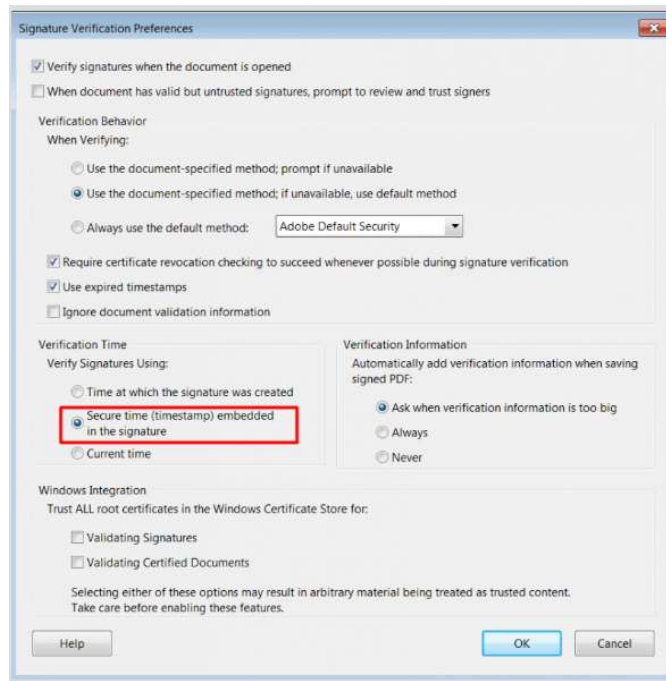
Πατήστε **OK**.



Κάντε κλικ στο **Harica Timestamping service** and πατήστε **set as default**, σε περίπτωση που υπάρχει και άλλος διακομιστής χρονοσήμανσης. Στην συνέχεια κλείστε το παράθυρο.



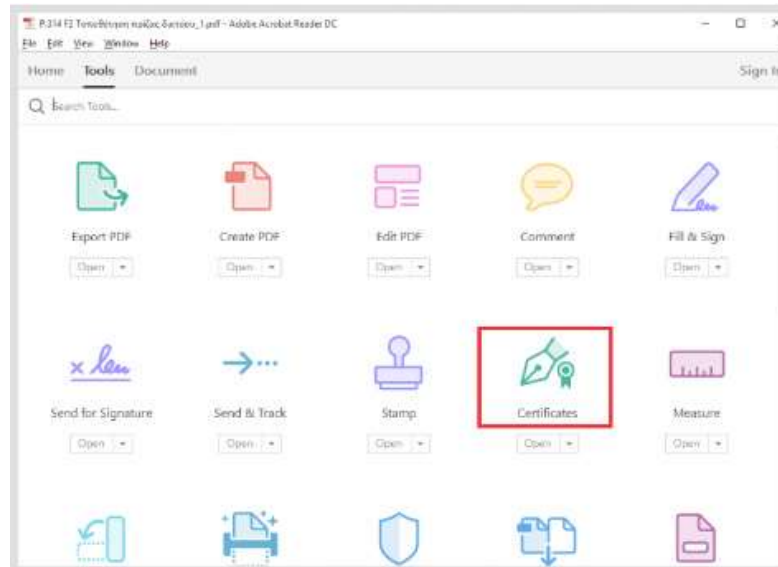
Επιλέξτε **Preferences – Signatures - Verification – More**. Στο πεδίο **verification time**, πατήστε στο **Secure time (timestamp) embedded in the signature**. Κλείστε το παράθυρο πατώντας **OK**.



Η παραπάνω διαδικασία ορισμού διακομιστή χρονοσήμανσης γίνεται μία φορά στην αρχή.

Ψηφιακή υπογραφή εγγράφου

Για να υπογράψετε ψηφιακά το έγγραφο, επιλέξτε **Tools - Certificates**



Επιλέξτε **Digitally Sign**. Καθορίστε με drag and drop του κέρσορα του ποντικιού σας την περιοχή του εγγράφου στην οποία θα υπογράψετε ψηφιακά.

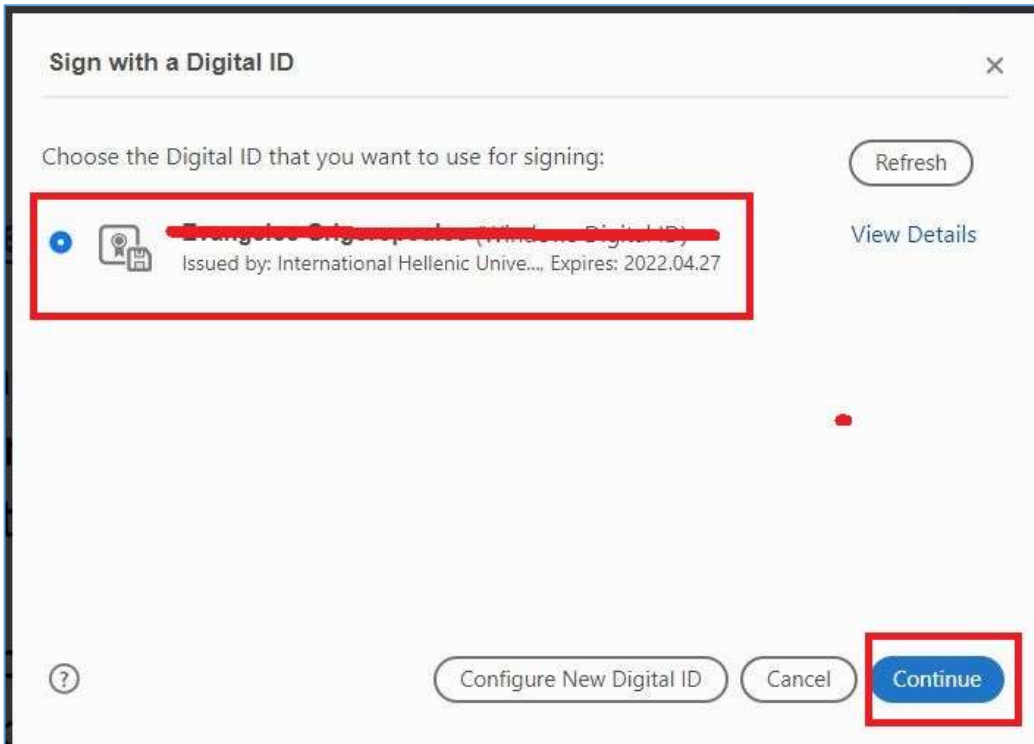
A screenshot showing the 'Digitally Sign' toolbar at the top of a document window. The 'Digitally Sign' button is highlighted with a red box. Below the toolbar, the document content is visible, featuring a heading and two paragraphs of text.

Harica digital certificate issuance/renewal

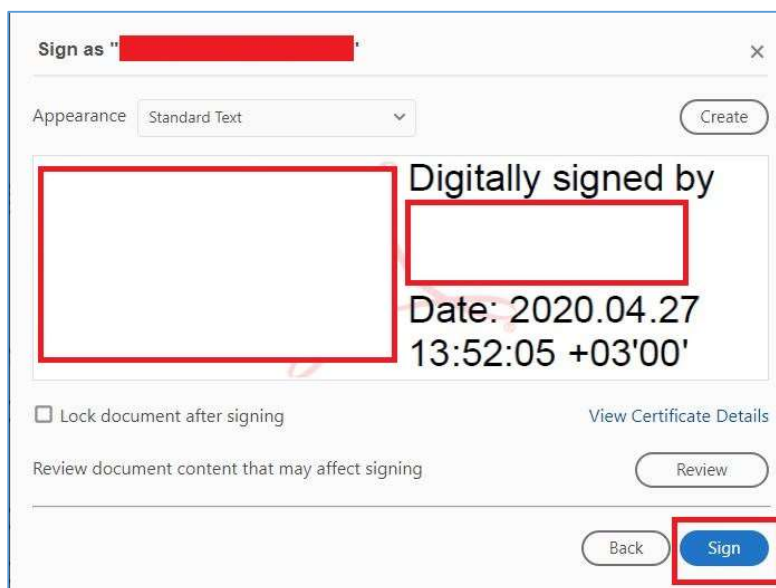
The following instructions should be followed for the issuance of a Class B digital user certificate by the Hellenic Academic & Research Institutions Certification Authority (HARICA, <https://www.harica.gr/>).

The procedure presented here is applied to certificate issuance by use of the Internet Explorer browser. Other browsers (Firefox, Safari) can be used as well, **but we strongly recommend that you use Internet Explorer.**

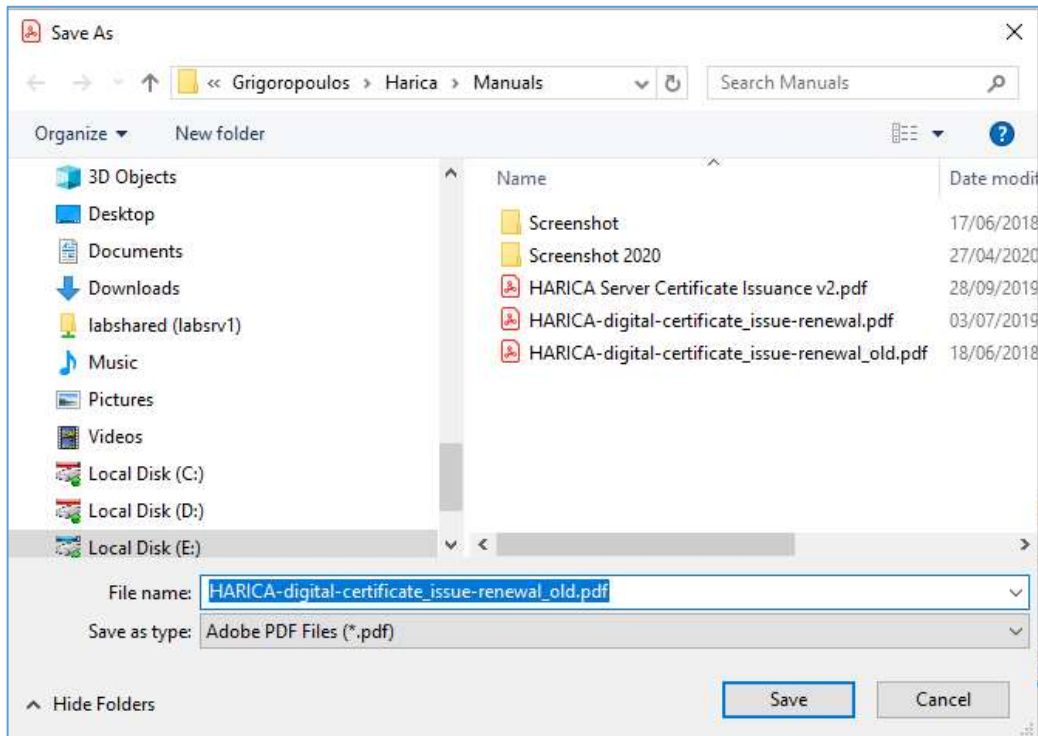
Επιλέξτε το σωστό πιστοποιητικό (σε περίπτωση που υπάρχουν περισσότερα του ενός στην συσκευή σας) και πατήστε **Continue**



Στο επόμενο παράθυρο, αφού επιβεβαιώσετε ότι το πιστοποιητικό είναι ορθό, πατήστε **Sign**.



Αποθηκεύστε το ψηφιακά υπογεγραμμένο έγγραφο. Κατά την πρώτη προσπάθεια μετά την εγκατάσταση του πιστοποιητικού, θα σας ζητηθεί να επιτρέψετε την σύνδεση στον διακομιστή χρονοσήμανσης. Πατήστε **Allow**.



Για να ολοκληρωθεί η αποθήκευση του ψηφιακά υπογεγραμμένου εγγράφου, επιβεβαιώστε το πιστοποιητικό πατώντας OK στο επόμενο παράθυρο.

