NOVATRON®
61A, Apostolopoulou Str. - Halandri, Athens
www.novatron.gr

Oberthur ID-One Cosmo Token οδηγός χρήσης (v3.0).

Περιεχόμενα

Τεχνικές προδιαγραφές.

Host interface	
Connection	USB 2.0 Low Speed (Plug & Play)
USB Hub Compatible	Yes
Power supply	USB bus powered
Contact Interface	
Protocols	T=1, T=0 (driver)
Status indicator	Two status LED (Blue)
Contactless Interface	
Embedded connection	Etched copper antenna
Protocols	T=CL, MIFARE Classic™ 1K emulation
Transmission speed	up to 424 kbps
Chip features overview	
Oberthur Reference	ID-One Cosmo v7.0.1
Memory	80 Kbytes
Java Card (2.2.2)	2 RMI, logic channel, Garbage collector, Sun 2.2.2
Cryptographic algorithms	AES-128/192/256bits, DES, 3DES, RSA
Hashing algorithm	SHA1, SHA-2, SHA-224, SHA-256, SHA384, SHA512
RSA key length	From 512 up to 2048 bits
Elliptic Curve Diffie-Helman	160/192/224/256/384/521 bits
Algorithm Elliptic Curve DSA GFP	160/192/224/256/384/521 bits
True Random Number Generator	Yes, compliant to FIPS 140-2
APDU	Extended length APDU
Secure Messaging	Yes
Compliance	
Card Standards	ISO 7816, ISO 14443 Type A, MIFARE Classic™ (1 Kb)
OS Standards	Javacard 2.2.2, Global Platform 2.1.1
Chip Security Certifications	Fips 140-2 level 3, EAL4+ SSCD
Software drivers	PC/SC, Microsoft WHQL
Environmental certifications	RoHS, FCC Class B part 15, CE
Other	
Housing color	Black
Label on recto side (visible when token inserted)	White, plasticized, with an Oberthur Technologies color logo
Label on verso side	White, printed in black with a unique serial number
Customization options	Color logo. Labels placement. Fixed text above serial number
Hardware specifications	
Color	Black
Reliability	100 000 Read / Write Operations
Dimensions	60 x 22 x 8 mm
Weight	5 g
Operating Temperature	-10°C ~ 55°C
Storage Temperature	-25°C ~ 85°C
Relative Humidity	5% ~ 90%
Durability	5000 insertion cycles
Mean Time Between Failure	5000 Hours

Εισαγωγή.

Ο συγκεκριμένος οδηγός περιγράφει τη συνολική διαδικασία της Ψηφιακής Υπογραφής. Το πρώτο που χρειάζεται να κάνει ο ενδιαφερόμενος είναι να προμηθευτεί το USB Token. Έπειτα πρέπει να υποβάλλει ηλεκτρονικό αίτημα μέσω της Πύλης του ΕΡΜΗ, να μεταβεί σε ΚΕΠ ώστε να γίνει η ταυτοπροσωπία και να αιτηθεί την έκδοση των προσωπικών του Ψηφιακών Πιστοποιητικών. Ακολουθεί η εγκατάσταση των απαραίτητων πιστοποιητικών στον υπολογιστή του, η παραμετροποίηση του Internet Explorer και η εγκατάσταση του προγράμματος οδήγησης του USB Token, ώστε να προχωρήσει στην εγκατάσταση των προσωπικών του Ψηφιακών Πιστοποιητικών σε αυτό. Πλέον, με τη χρήση κατάλληλου λογισμικού, θα μπορεί να υπογράψει ψηφιακά και να αποστείλει ή να ανεβάσει τα έγγραφά του όπου απαιτεί η εργασία του, για κάθε νόμιμη χρήση.

Κωδικοί PIN / PUK.

Οι παρακάτω κωδικοί είναι οι προεπιλεγμένοι από το εργοστάσιο και συνιστάται να αλλάζονται από τον κάτοχο του Token.

Token PIN (User Password): Τέσσερις φορές το εννέα 9999 (μετά από 3 ανεπιτυχείς προσπάθειες κλειδώνει).

Token PUK (SO Password): 1234 (μετά από 3 ανεπιτυχείς προσπάθειες κλειδώνει).

ΠΡΟΣΟΧΗ: Σε περίπτωση που κλειδώσει και το PIN και το PUK της συσκευής, αυτή δεν μπορεί να χρησιμοποιηθεί πλέον.

Βήμα 1ο: Προμήθεια USB Token

Το Usb Token που θα προμηθευτούμε είναι το Oberthur ID-One Cosmo Token. είναι μία Πιστοποιημένη Ασφαλής Διάταξη Δημιουργίας Ψηφιακής Υπογραφής (ΑΔΔΥ). Εξωτερικά μοιάζει με μνήμη USB Flash. Σ' αυτή τη συσκευή αποθηκεύονται τα ψηφιακά πιστοποιητικά μας.

Oberthur ID-One Cosmo Token: Ασφαλής Διάταξη Δημιουργίας Ψηφιακής Υπογραφής (ΑΔΔΥ) ή αλλιώς USB Token

Το Oberthur ID-One Cosmo Token λειτουργεί σε όλα τα λειτουργικά συστήματα αλλά για την εισαγωγή των πιστοποιητικών από την πύλη του **ΕΡΜΗ** χρειάζεται **απαραίτητα** λειτουργικό σύστημα **Windows 7 με Internet Explorer 8, 9 ή 10**.

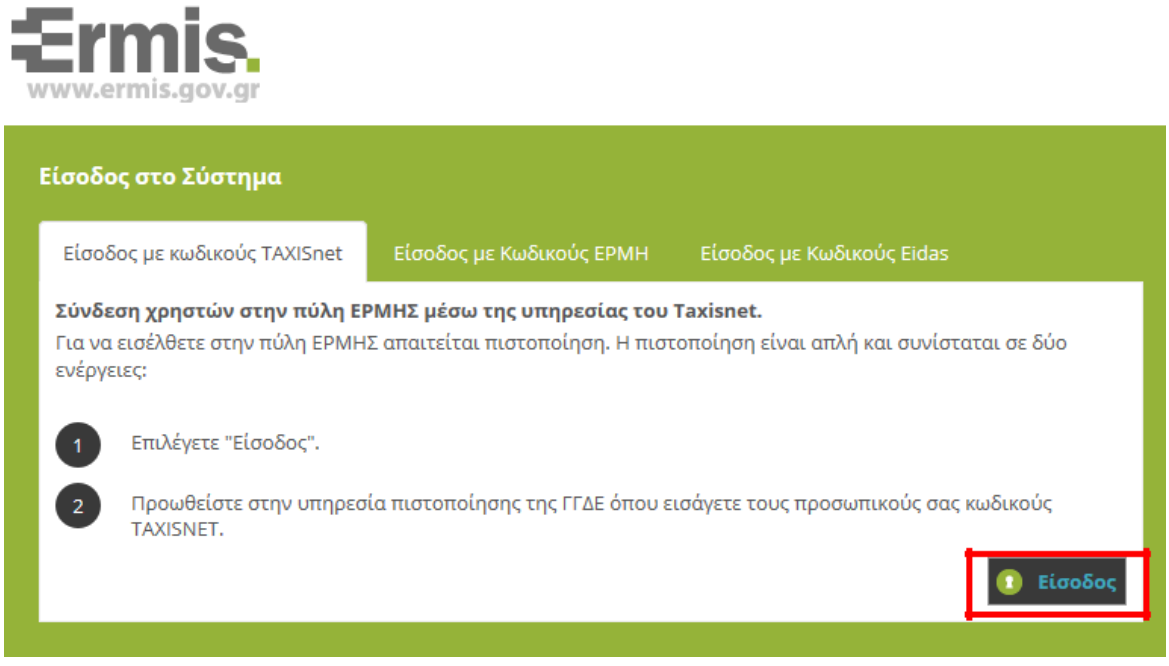
Μπορούμε να το προμηθευτούμε μέσω της ιστοσελίδας www.novatron.gr , επικοινωνώντας με το τμήμα πωλήσεων της εταιρείας στο τηλέφωνο 210 6180 865 ή με φυσική παρουσία στην έδρα της στο Χαλάνδρι, Ι. Αποστολοπούλου 61Α, Τ.Κ.: 15231, Χαλάνδρι.

Βήμα 2ο: Ηλεκτρονική αίτηση μέσω της Πύλης ΕΡΜΗΣ

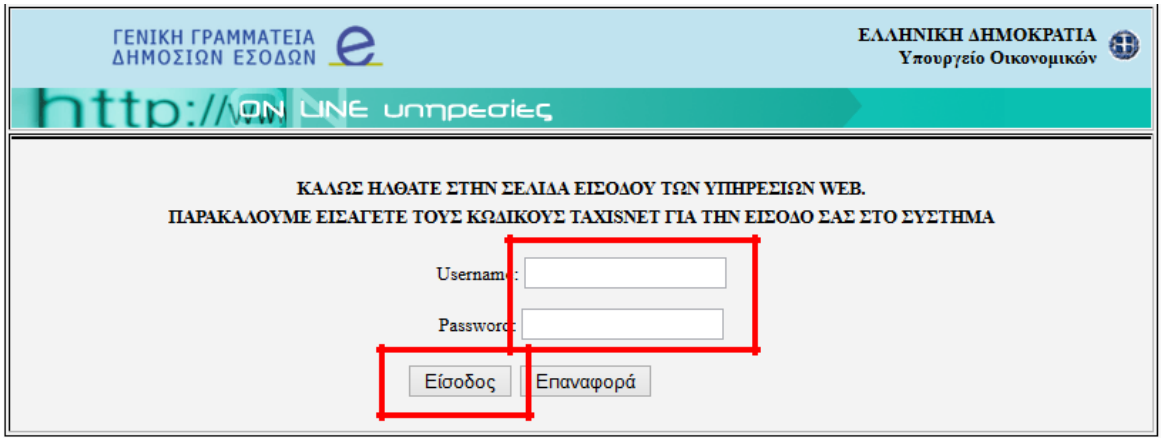
Πληκτρολογούμε τη διεύθυνση www.ermis.gov.gr , κατευθυνόμαστε στη σελίδα όπως αυτή φαίνεται στην παρακάτω εικόνα και επιλέγουμε Σύνδεση.

Δεν μπορούμε να αποκτήσουμε πρόσβαση στην πύλη του ΕΡΜΗ με τη χρήση Windows XP καθώς τα Windows XP δεν υποστηρίζουν τη χρήση TLS 1.2.

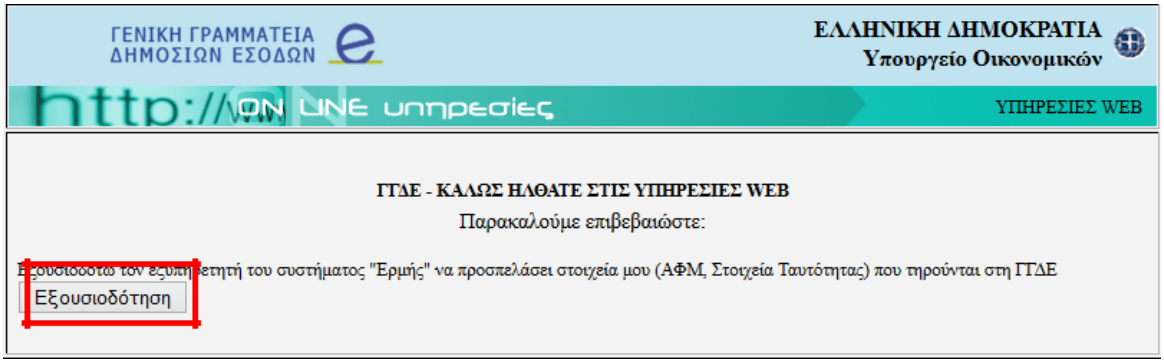
Στη συνέχεια επιλέγουμε το σύνδεσμο Είσοδος.



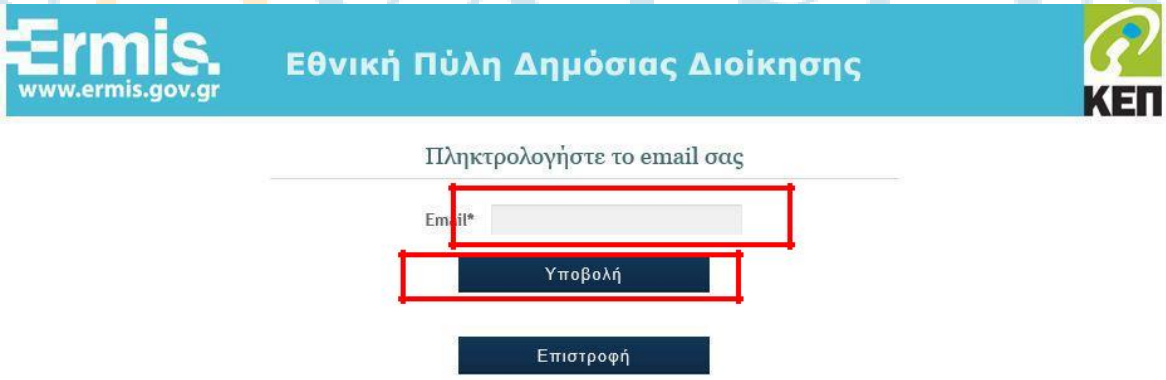
Στη συνέχεια πληκτρολογούμε τους προσωπικούς κωδικούς TAXISnet και επιλέγουμε Είσοδος.



Επιλέγουμε Εξουσιοδότηση, όπως βλέπουμε την παρακάτω εικόνα.

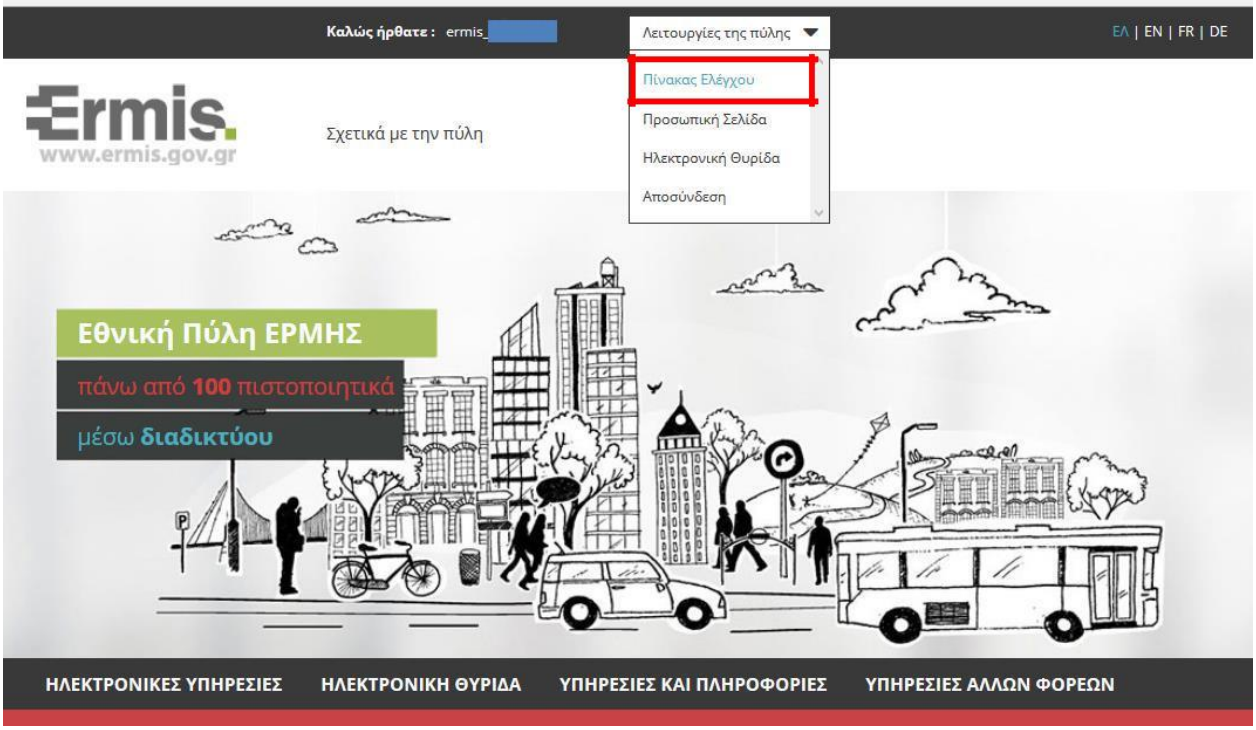


Στην περίπτωση που μπαίνουμε στην Πύλη ΕΡΜΗΣ για πρώτη φορά θα πρέπει να συμπληρώσουμε το προσωπικό/εταιρικό email και να επιλέξουμε Υποβολή.

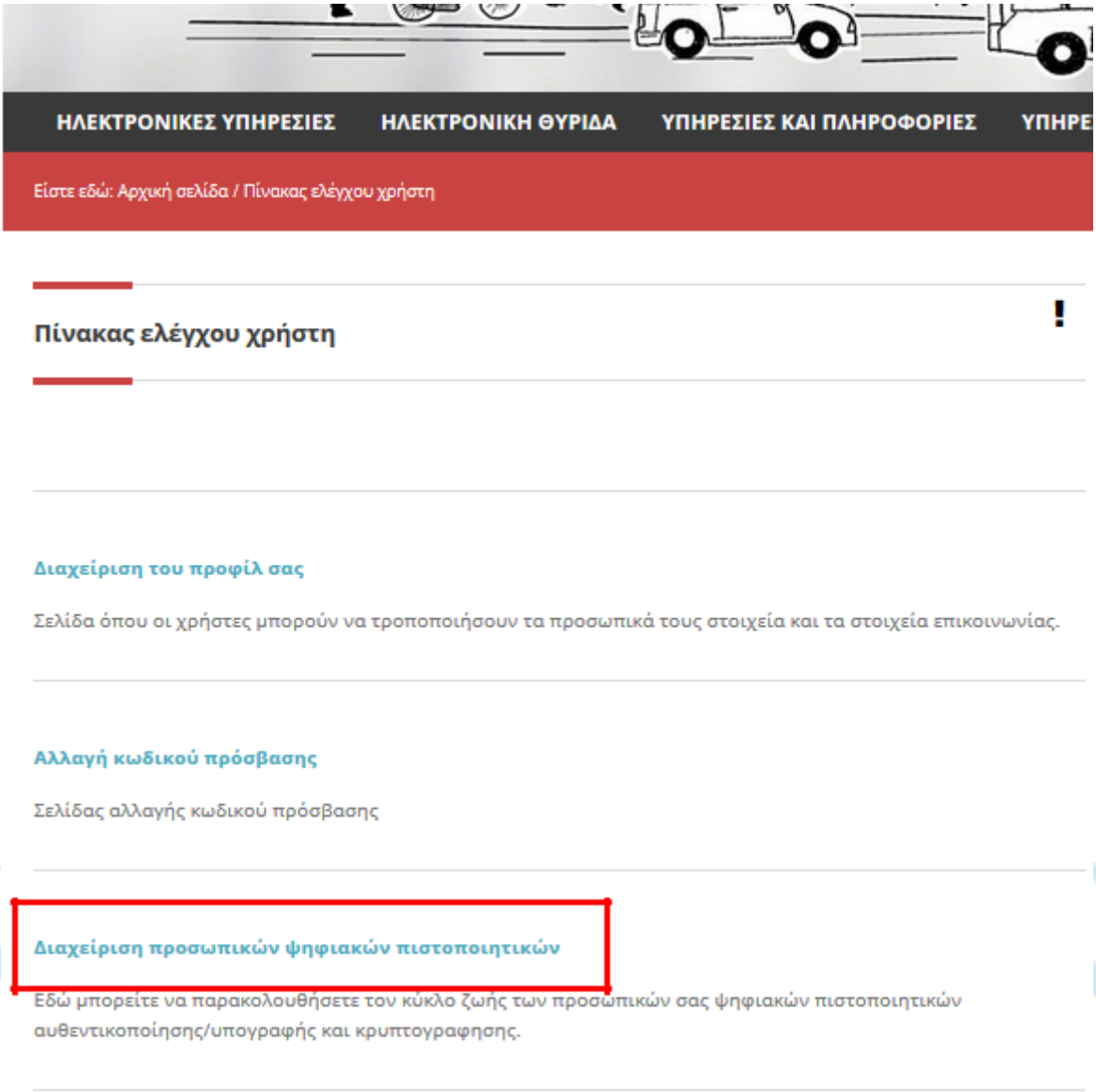


Βρισκόμαστε πλέον στην κεντρική σελίδα της Πύλης ΕΡΜΗΣ.

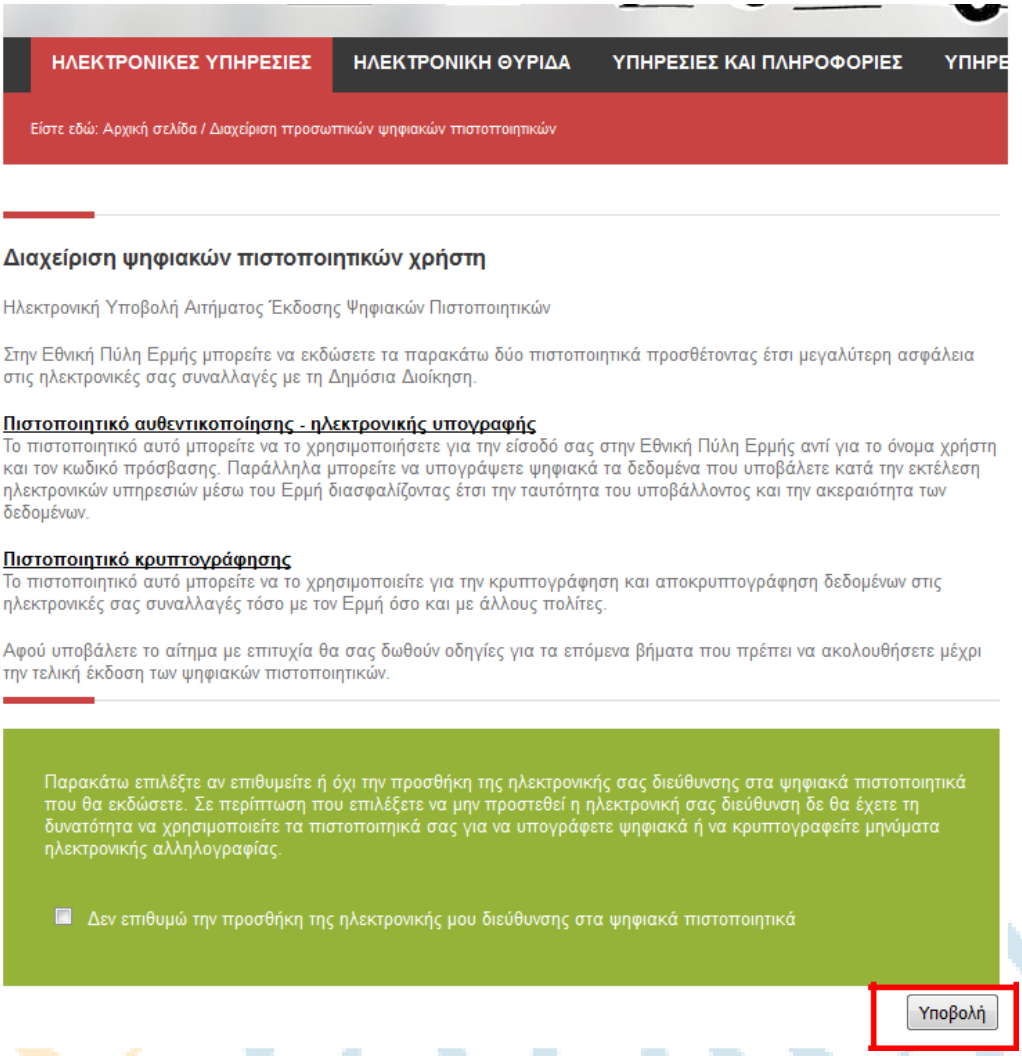
Για να υποβάλουμε αίτημα έκδοσης Ψηφιακού Πιστοποιητικού. Επιλέγουμε το σύνδεσμο Πίνακας Ελέγχου, όπως φαίνεται στην παρακάτω εικόνα.



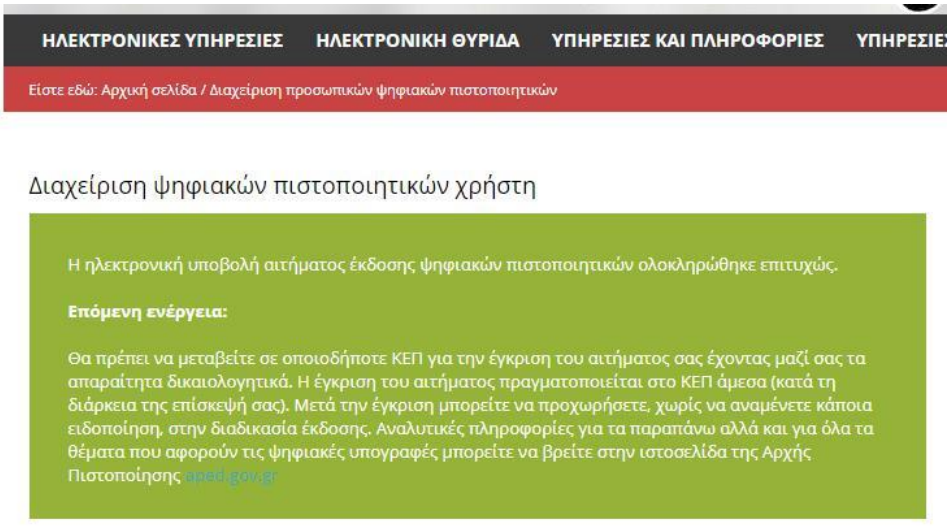
Επιλέγουμε το σύνδεσμο Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών.



Εμφανίζεται η δυνατότητα ηλεκτρονικής υποβολής αιτήματος έκδοσης ψηφιακού πιστοποιητικού, επιλέγουμε Υποβολή.



Λαμβάνουμε το παρακάτω μήνυμα.



Βήμα 3ο: Μετάβαση σε ΚΕΠ

Πηγαίνουμε σε οποιοδήποτε Κέντρο Εξυπηρέτησης Πολιτών για τη φυσική ταυτοποίησή μας, έχοντας μαζί μας την ταυτότητα (ή το διαβατήριο) και φωτοτυπία αυτής, όπως επίσης συμπληρωμένη και υπογεγραμμένη την Αίτηση - Υπεύθυνη Δήλωση για την έκδοση των πιστοποιητικών την οποία μπορούμε να την κατεβάσουμε από εδώ.

http://www.aped.gov.gr/images/steps1-6/pki_citizen_yp_dilosi.pdf

Αρ. Πρωτ.: _____

(συμπληρώνεται από την Αρχή Εγγραφής)

ΑΙΤΗΣΗ - ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

ΕΚΔΟΣΗΣ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

ΕΚΤΥΠΩΣΗ

ΑΠΟΘΗΚΕΥΣΗ

Η ακρίβεια των στοιχείων που υποβάλλονται με αυτή τη δήλωση μπορεί να ελεγχθεί με βάση το αρχείο άλλων υπηρεσιών (άρθρο 8 παρ. 4 Ν. 1599/1986)

ΠΡΟΣ:	**Αρχή Πιστοποίησης Ελληνικού Δημοσίου** - Υπηρεσία Ανάπτυξης Πληροφορικής		
Ο – Η Όνομα:		**Επώνυμο:**	
Όνομα και Επώνυμο Πατέρα:			
Όνομα και Επώνυμο Μητέρας:			
Ημερομηνία γέννησης (μορφής ηη/μμ/εεεε) [1]:			
Αριθμός Δελτίου Ταυτότητας:		**Κινητό Τηλέφωνο (για λήψη sms) [2]:**	
Τόπος γέννησης:			
Τόπος Κατοικίας (Δήμος/Κοινότητα):			
Οδός:		**Αριθμός:**	**Τ.Κ:**
Αριθμός τηλεφώνου:		**Προσωπικό Ηλεκτρονικό Ταχυδρομείο (e-mail) [3]:**	
Όνομα χρήστη (username) στην πύλη ΕΡΜΗΣ:			
Α.Μ.Κ.Α. [4]		**ΑΦΜ [4]:**	**Άλλο:**
Αριθμός σειριακού ΑΔΔΥ (έξυπνης κάρτας ή USB token) [5]:			

Στην περίπτωση Δημοσίου Υπαλλήλου ή Φορέα (μέλους ή εκπροσώπου) συμπληρώνονται και τα στοιχεία:

Φορέας:			
Ταχυδρομική διεύθυνση Φορέα:			
Τηλέφωνο :		**Αριθμός τηλεομοιοτύπου (Fax) :**	
Ηλεκτρονικό Ταχυδρομείο (e-mail) στον Φορέα:			

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις[6], που προβλέπονται από τις διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

Επιθυμώ την έκδοση πιστοποιητικών αυθεντικοποίησης / υπογραφής και κρυπτογράφησης[7]. Επιπλέον, επισυνάπτω φωτοαντίγραφο του Δελτίου της Αστυνομικής Ταυτότητας / Διαβατηρίου μου.

(1) Αναγράφεται με την μορφή ηη/μμ/εεεε , παράδειγμα 01/01/2000.
(2) Για την λήψη SMS μηνυμάτων.
(3) Για τον δημόσιο υπάλληλο ή Φορέα (μέλους ή εκπροσώπου) δεν είναι υποχρεωτικό.
(4) Προαιρετικά, σε περίπτωση που επιθυμείτε την έκδοση τομεακών πιστοποιητικών στο μέλλον.
(5) Βάσει του ΠΔ 150/2001, θέση ιδιόχειρης υπογραφής επέχει αναγνωρισμένο πιστοποιητικό που δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.
(6) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.".
(7) Ο αιτών/αιτούσα έχει λάβει γνώση των όρων χρήσης των πιστοποιητικών (Κανονισμός Πιστοποίησης ΑΠΕΔ) και τους αποδέχεται πλήρως.

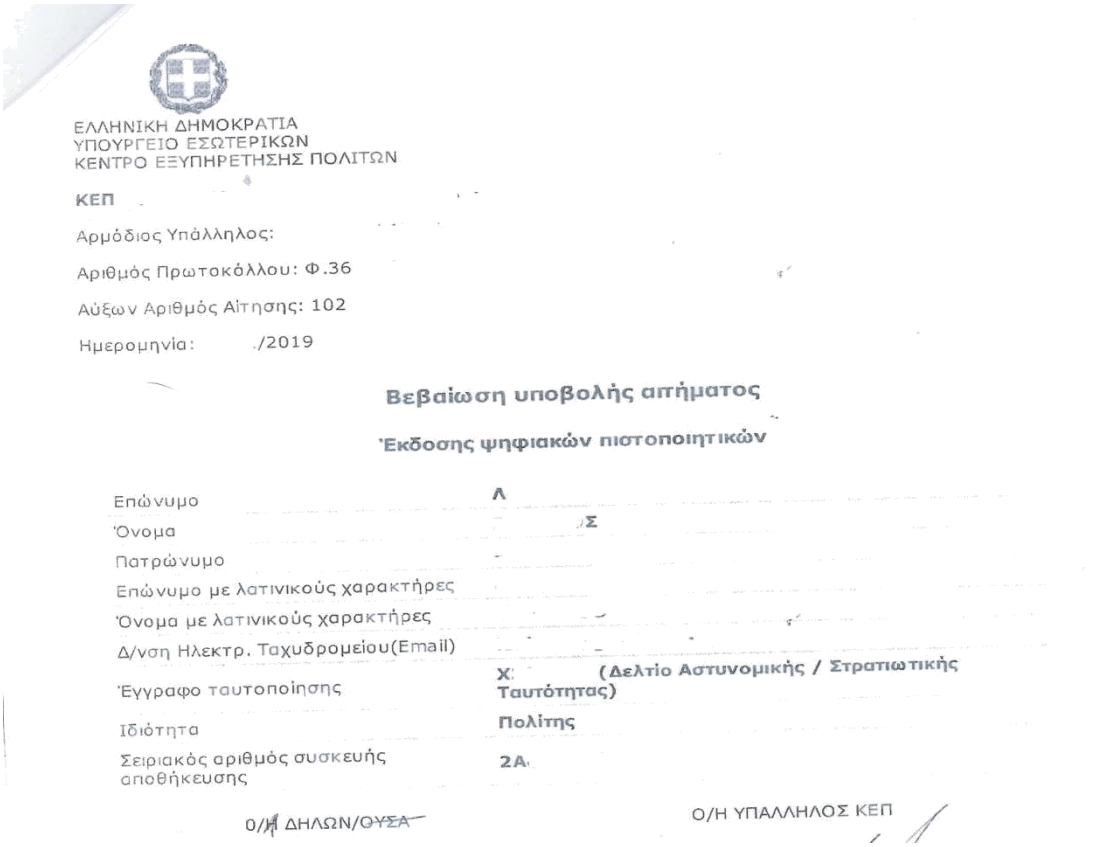
Ημερομηνία: ..../...../201....

Ο / Η Δηλ...

(Υπογραφή)

Ο Αριθμός σειριακού ΑΔΔΥ είναι διακριτός στην μία πλευρά του Oberthur Usb Token.

Από το ΚΕΠ παραλαμβάνουμε την βεβαίωση υποβολής αιτήματος για την έκδοση ψηφιακών πιστοποιητικών, η οποία έχει την παρακάτω μορφή.



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΚΕΝΤΡΟ ΕΞΥΠΗΡΕΤΗΣΗΣ ΠΟΛΙΤΩΝ

ΚΕΠ

Αρμόδιος Υπάλληλος:

Αριθμός Πρωτοκόλλου: Φ.36

Αύξων Αριθμός Αίτησης: 102

Ημερομηνία: /2019

Βεβαίωση υποβολής αιτήματος

Έκδοσης ψηφιακών πιστοποιητικών

Επώνυμο	Λ
Όνομα	Σ
Πατρώνυμο	
Επώνυμο με λατινικούς χαρακτήρες	
Όνομα με λατινικούς χαρακτήρες	
Δ/νση Ηλεκτρ. Ταχυδρομείου(Email)	
Έγγραφο ταυτοποίησης	Χ (Δελτίο Αστυνομικής / Στρατιωτικής Ταυτότητας)
Ιδιότητα	Πολίτης
Σειριακός αριθμός συσκευής αποθήκευσης	2A

Ο/Η ΔΗΛΩΝ/ΟΥΣΑ

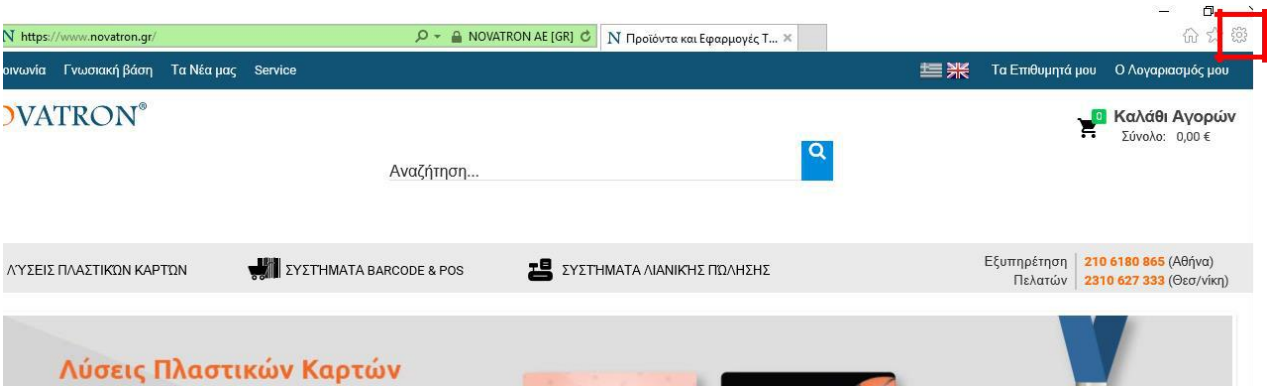
Ο/Η ΥΠΑΛΛΗΛΟΣ ΚΕΠ

Βήμα 4ο: Έλεγχος προδιαγραφών και προετοιμασία υπολογιστή.

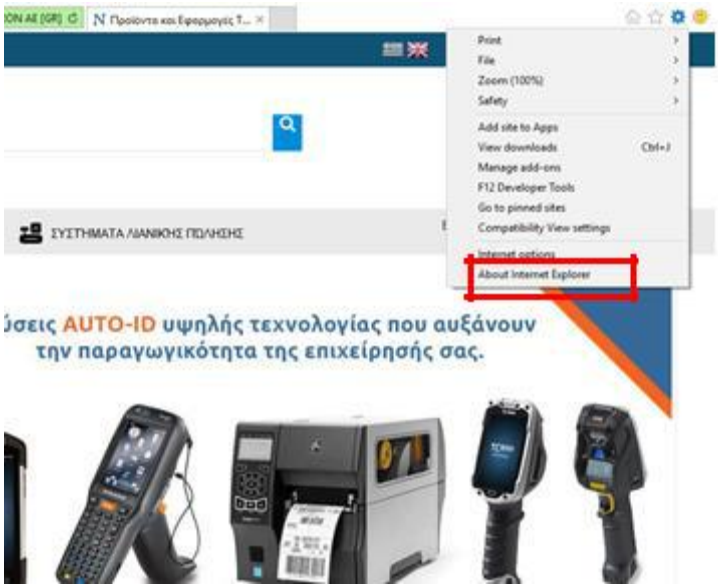
Βάσει των προδιαγραφών της κρατικής υπηρεσίας ανάπτυξης πληροφορικής για την ορθή εγκατάσταση των προσωπικών μας Ψηφιακών Πιστοποιητικών, είναι **υποχρεωτικό** να χρησιμοποιήσουμε υπολογιστή με **λειτουργικό σύστημα Windows 7 και Internet Explorer 8 ή 9 ή 10**. Η εγκατάσταση αυτή πραγματοποιείται μία φορά, έπειτα μπορούμε να χρησιμοποιήσουμε το Usb Token σε υπολογιστές με «σύγχρονα» λειτουργικά συστήματα πχ Windows 10.

Έλεγχος έκδοσης Internet Explorer.

Ανοίγουμε τον Internet Explorer και επιλέγουμε Εργαλεία (Tools).



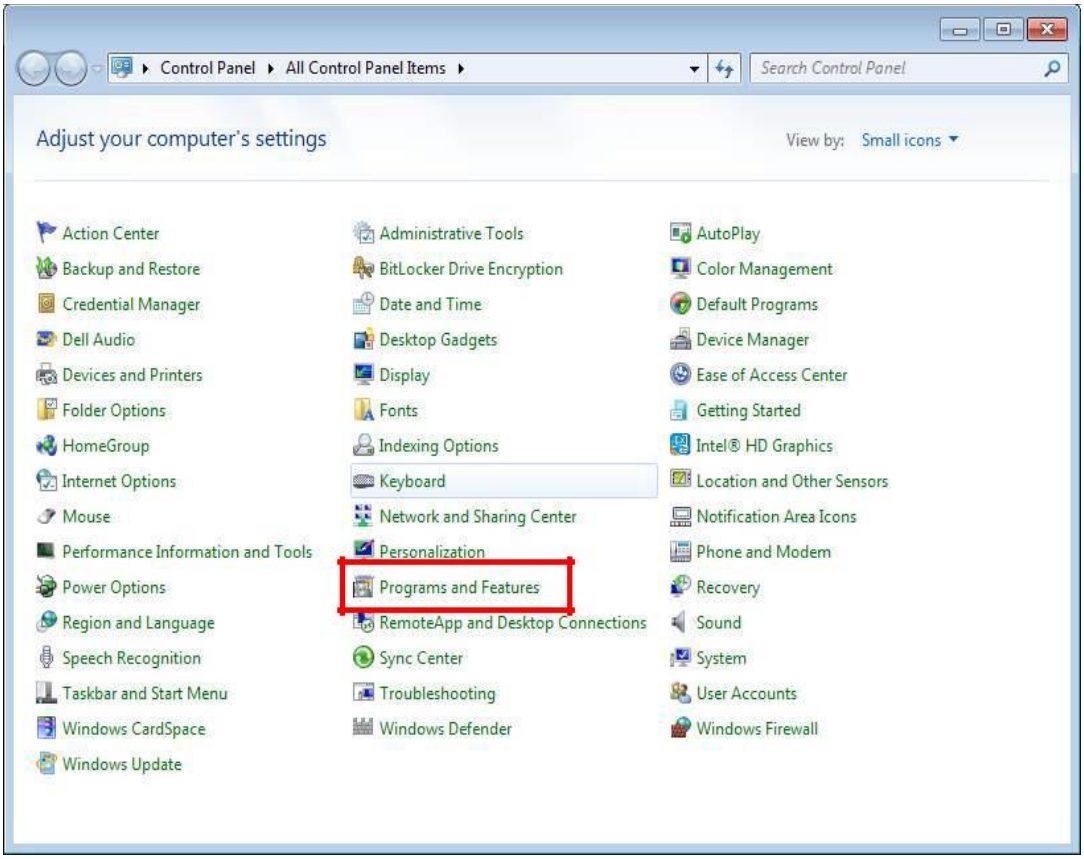
Επιλέγουμε About Internet Explorer (Πληροφορίες για τον Internet Explorer).



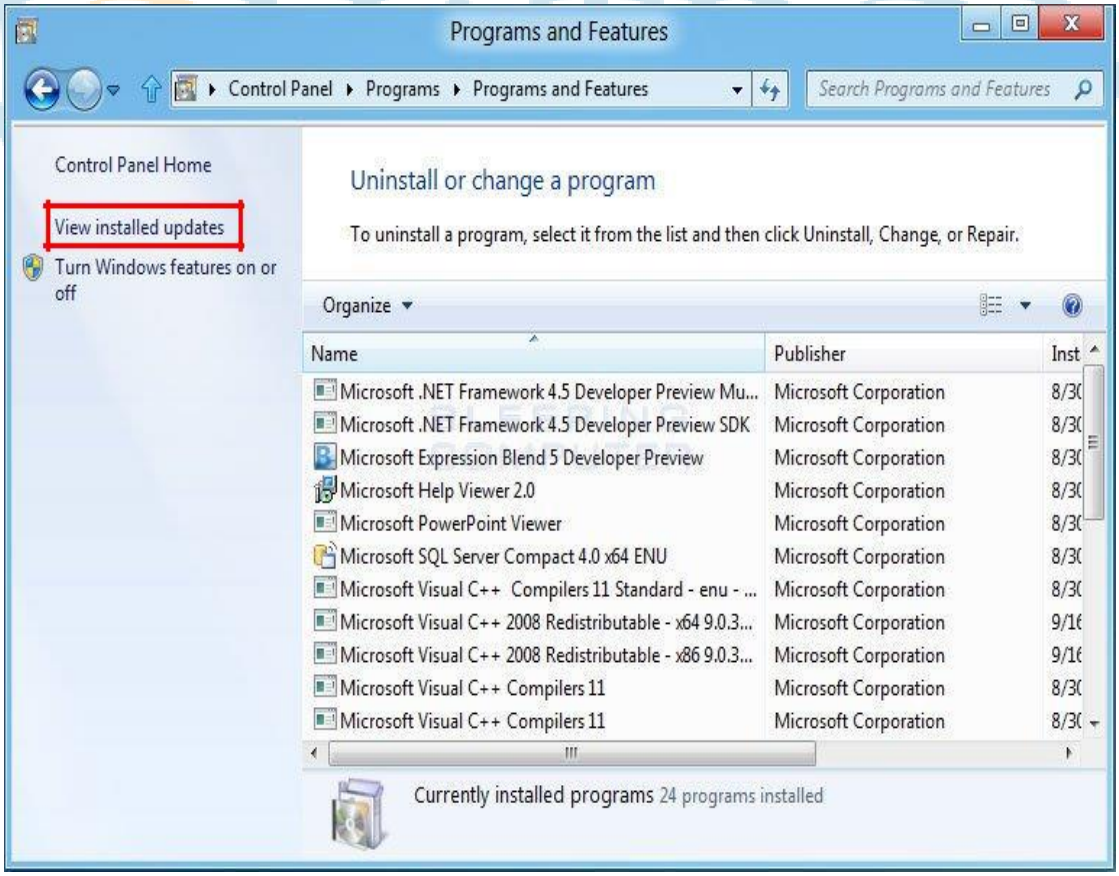
Λαμβάνουμε την πληροφορία για την έκδοση του προγράμματος.

Αν στη προηγούμενη εικόνα λαμβάναμε τη πληροφορία ότι έχουμε έκδοση 8 ή 9 ή 10, παραλείπουμε τα παρακάτω και προχωράμε. Αν όμως έχουμε τον Internet Explorer 11 πρέπει να τον «υποβαθμίσουμε» με την παρακάτω διαδικασία.

Επιλέγουμε Έναρξη και στη συνέχεια Πίνακας Ελέγχου (Control Panel). Στη συνέχεια επιλέγουμε Προγράμματα και Δυνατότητες (Programs and Features).

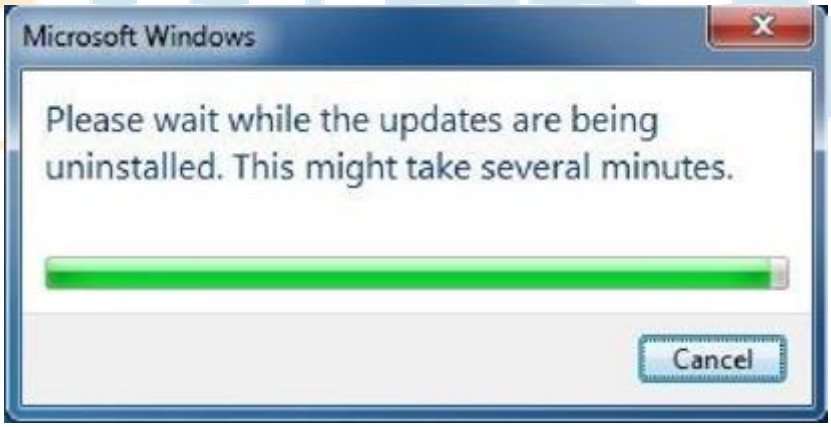


Επιλέγουμε Προβολή εγκατεστημένων ενημερώσεων (View installed updates).

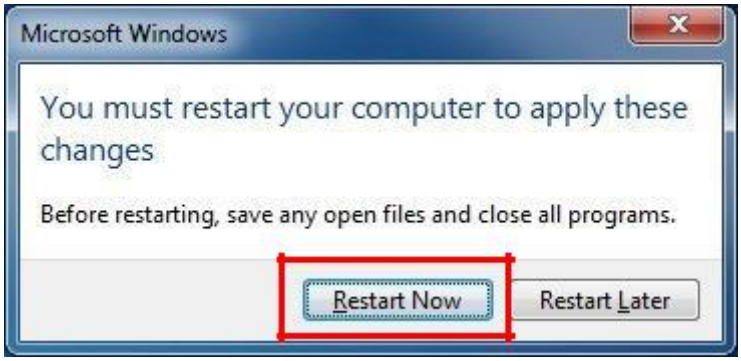


Και στη συνέχεια εντοπίζουμε και επιλέγουμε τον Internet Explorer 11 και πατάμε Κατάργηση Εγκατάστασης (Uninstall).

Επιλέγουμε Ναι.



Επιλέγουμε Επανεκκίνηση Τώρα (Restart Now).



Ο υπολογιστής μας θα κάνει επανεκκίνηση, ελέγχουμε εκ νέου την έκδοση του Internet Explorer και θα πρέπει πλέον να είναι 8 ή 9 ή 10 (πρέπει να αποτσεκάρουμε το checkbox Install new versions automatically μέχρι να ολοκληρωθούν τα βήματα της εγκατάστασης).

Για τις παρακάτω διαδικασίες θα χρειαστεί να έχουμε δικαιώματα διαχειριστή (Administrator) στον υπολογιστή μας.

Εγκατάσταση των ψηφιακών πιστοποιητικών των Αρχών Πιστοποίησης και Χρονοσήμανσης.

Από την σελίδα https://pki.ermis.gov.gr/repository.html , θα πρέπει να εγκατασταθούν **όλα** τα ψηφιακά πιστοποιητικά σε μορφή **DER** ώστε να αναγνωρίζονται όλες οι ψηφιακές υπογραφές από την αρχή λειτουργίας της ΑΠΕΔ.

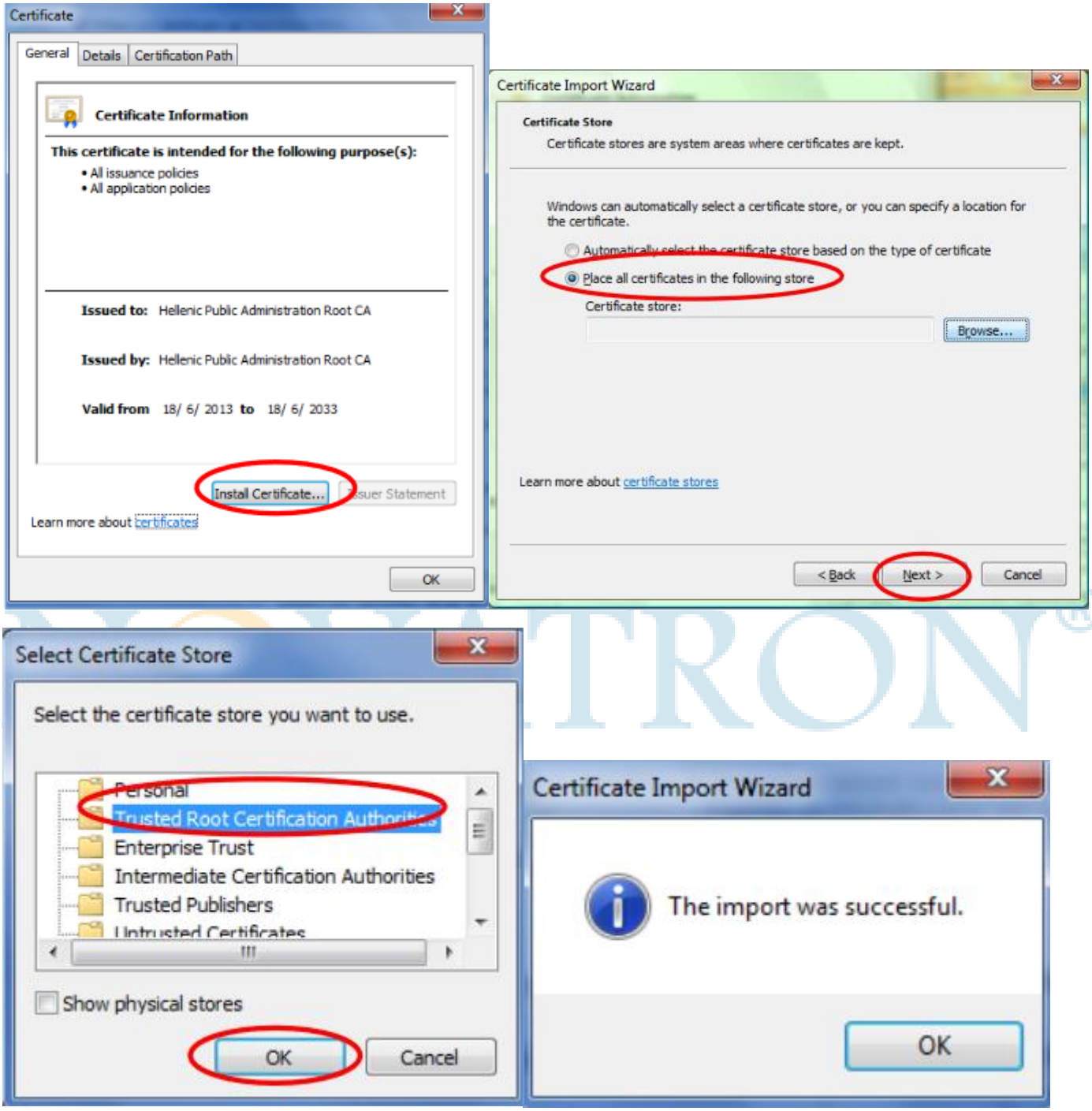
Για τα ψηφιακά πιστοποιητικά της Πρωτεύουσας Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) και της παλιάς Αρχής Χρονοσήμανσης εγκαθιστούμε τα παρακάτω πιστοποιητικά.

1.1 Πρωτεύουσας Αρχής Πιστοποίησης σε μορφή DER, Base64 Thumbprint Algorithm: SHA1 Thumbprint: 07 60 76 37 35 4b 73 86 7a d0 bb 46 46 25 c0 0b 1a db 57 87 Subject key identifier: 59 0b 18 a2 09 1e 21 dc 61 65 d3 a4 be 05 e5 4c e6 41 88 1d	**1.1 Πρωτεύουσας Αρχής Πιστοποίησης σε μορφή DER**
3.1 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA1) σε μορφή DER, Base64 Thumbprint Algorithm: SHA1 Thumbprint: 31 53 41 d3 d0 05 d3 41 37 a7 42 eb 83 d3 02 5e 58 e8 33 b6 Subject key identifier: 32 49 40 49 88 16 1d 6a ab c4 24 29 c8 27 c4 49 fb 4f 61 0b	**3.1 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA1) σε μορφή DER**
3.3 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA2) σε μορφή DER, Base64 Thumbprint Algorithm: SHA256 Thumbprint: d1 40 88 fa 00 2c 8b 13 00 15 86 19 96 6a 10 38 91 3a a8 f2 Subject key identifier: 32 49 40 49 88 16 1d 6a ab c4 24 29 c8 27 c4 49 fb 4f 61 0b	**3.3 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA2) σε μορφή DER**
5.5 Αρχής Χρονοσήμανσης Α σε μορφή DER, Base64 Πριν από 1/8/2013 Thumbprint Algorithm: SHA1 Thumbprint: 67 88 a7 7c 0e c4 6c 4e 39 3e 39 bb 05 4b c0 90 f2 8c bd b1	**5.5 Αρχής Χρονοσήμανσης Α σε μορφή DER**
5.6 Αρχής Χρονοσήμανσης Β σε μορφή DER, Base64 Πριν από 1/8/2013 Thumbprint Algorithm: SHA1 Thumbprint: e4 85 d3 b4 ff 99 13 4a f0 3a f5 18 44 22 18 81 ba 59 a4 9b	**5.6 Αρχής Χρονοσήμανσης Β σε μορφή DER**

Τα πέντε πιστοποιητικά τα εγκαθιστούμε ένα προς ένα όπως παραθέτουμε στις επόμενες εικόνες.

Επιλέγω "Place all certificates in the Following store / Τοποθέτηση όλων των πιστοποιητικών στον παρακάτω χώρο αποθήκευσης ".

Χειροκίνητα επιλέγω το "Trusted Root Certification Authorities/ Αξιόπιστες Κεντρικές Αρχές έκδοσης Πιστοποιητικών".

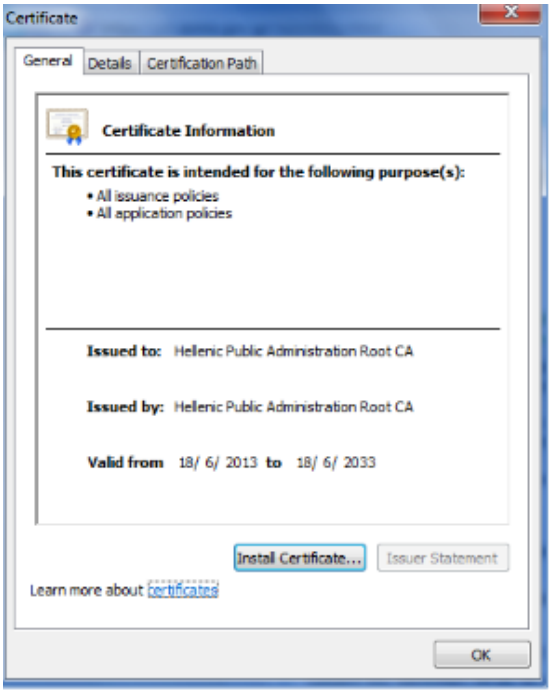


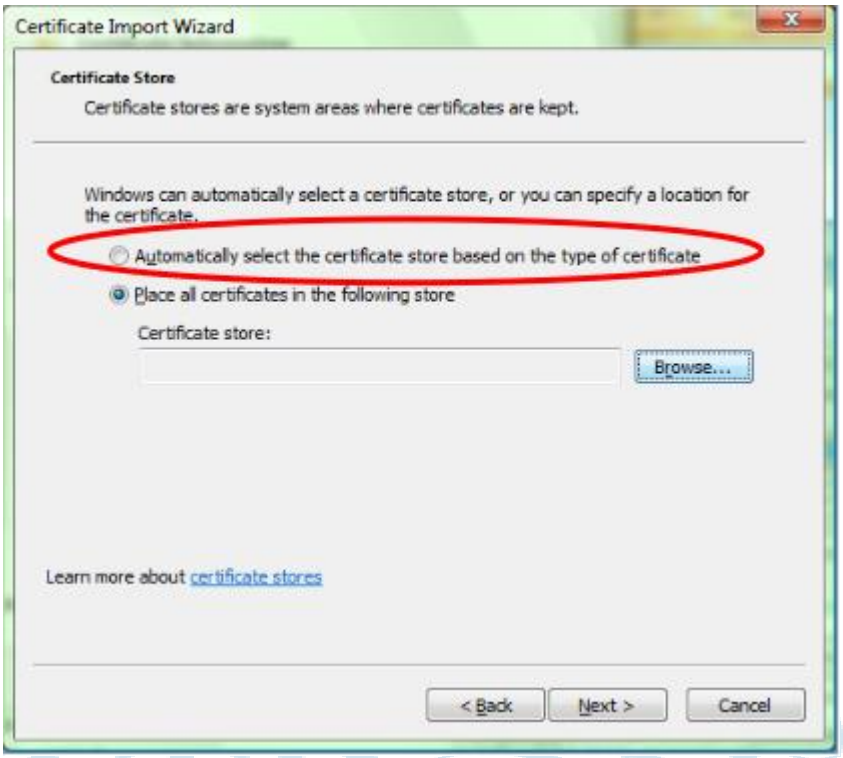
Για τα ψηφιακά πιστοποιητικά της Υποκείμενη Αρχής Πιστοποίησης (ΥΑΠ) και της νέας Αρχής Χρονοσήμανσης, εγκαθιστούμε τα παρακάτω πιστοποιητικά.

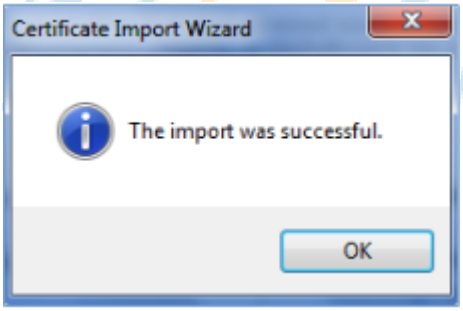
1.2 Υποκείμενης Αρχής Πιστοποίησης σε μορφή DER, Base64 Thumbprint Algorithm: SHA1 Thumbprint: 95 f2 1d c3 fe a2 d3 7c 4b 60 e9 44 6d ce 15 4e 70 86 15 05 Subject key identifier: b3 32 42 e6 3f d7 d5 2b d7 78 b9 bd 0a a4 bc b9 e8 d8 f9 41	**1.2 Υποκείμενης Αρχής Πιστοποίησης**

2.1 Υποκείμενης Αρχής Πιστοποίησης σε μορφή DER Thumbprint Algorithm: SHA1 Thumbprint: 4f 87 4b ed 10 c0 bb 80 41 5e 65 9e 6f 59 ab 75 63 b9 7d f8 Subject key identifier: 84 cb ee 22 80 9e 2d 48 37 53 1b 12 07 73 1e 6f 33 72 3b cd	**2.1 Υποκείμενης Αρχής Πιστοποίησης**
3.2 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA1) σε μορφή DER, Base64 Thumbprint Algorithm: SHA1 Thumbprint: 3a 6b 78 cf e7 d4 54 63 10 87 8f 76 1d 2a 68 52 2b f5 14 bf Subject key identifier: f9 b2 e0 b7 23 5a 09 30 2d 2e 79 de ee f5 ea e3 fd ca 13 c4	**3.2 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA1)**
3.4 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA2) σε μορφή DER, Base64 Thumbprint Algorithm: SHA256 Thumbprint: 50 1d 8a 09 f1 4d c5 ee 40 e1 b8 23 4c 1c 06 fd bf e7 c0 fb Subject key identifier: f9 b2 e0 b7 23 5a 09 30 2d 2e 79 de ee f5 ea e3 fd ca 13 c4	**3.4 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA2)**
4.1 Υποκείμενης Αρχής Πιστοποίησης για φορείς του δημοσίου τομέα (SHA1) σε μορφή DER, Base64 Thumbprint Algorithm: SHA1 Thumbprint: 01 e0 87 17 08 00 d3 ac 4a a9 91 9d 42 34 d4 c4 d4 51 fb 44 Subject key identifier: 96 19 0f 3b 06 67 13 09 fc a1 d5 15 91 fc a9 01 b5 e6 6b 3a	**4.1 Υποκείμενης Αρχής Πιστοποίησης για φορείς του δημοσίου τομέα (SHA1)**
4.2 Υποκείμενης Αρχής Πιστοποίησης για φορείς του δημοσίου τομέα (SHA2) σε μορφή DER, Base64 Thumbprint Algorithm: SHA256 Thumbprint: c4 ff 18 ff b6 bc 6f 3e d3 e4 5d 3e 30 2b 12 64 03 43 d4 c6 Subject key identifier: 96 19 0f 3b 06 67 13 09 fc a1 d5 15 91 fc a9 01 b5 e6 6b 3a	**4.2 Υποκείμενης Αρχής Πιστοποίησης για φορείς του δημοσίου τομέα (SHA2)**
5.1 Αρχής Χρονοσήμανσης #1 σε μορφή DER, Base64 Από 1/8/2013 έως 16/10/2017 Thumbprint Algorithm: SHA1 Thumbprint: d8 ba 52 c8 e4 9b 22 7f 03 79 0b 55 ec 80 e5 d4 93 b0 bb 0a	**5.1 Αρχής Χρονοσήμανσης #1**
5.2 Αρχής Χρονοσήμανσης #1 σε μορφή DER, Base64 Από 16/10/2017 και έπειτα Thumbprint Algorithm: SHA1 Thumbprint: 93 5f a6 62 a0 0a 89 65 ec a9 82 55 3e 31 8f e0 ee 0e 01 dd	**5.2 Αρχής Χρονοσήμανσης #1 (Νέο)**
5.3 Αρχής Χρονοσήμανσης #2 σε μορφή DER, Base64 Από 1/8/2013 και έπειτα Thumbprint Algorithm: SHA1 Thumbprint: c6 47 20 f3 d5 4b 5b 31 5b 56 49 c6 03 13 d6 0f 95 f3 36 42	**5.3 Αρχής Χρονοσήμανσης #2**
5.4 Αρχής Χρονοσήμανσης #3 σε μορφή DER, Base64 Από 1/8/2013 και έπειτα Thumbprint Algorithm: SHA1 Thumbprint: 55 2d c0 17 78 9d 13 6d 20 ec 79 19 11 18 91 54 a6 5f 1d b5	**5.4 Αρχής Χρονοσήμανσης #3**
5.7 Πιστοποιητικό Υποκείμενης Αρχής Χρονοσήμανσης σε μορφή DER Μετά από 1/8/2013 Thumbprint Algorithm: SHA1 Thumbprint: 59 f0 15 10 cf 95 41 7d dd 2e ee 9e c1 9a 89 c2 27 1a f6 ca Subject key identifier:56 e0 ae b4 aa 0e 82 f3 8b 33 83 de 3f 4e c8 e6 a1 38 75 04	**5.7 Πιστοποιητικό Υποκείμενης Αρχής Χρονοσήμανσης**

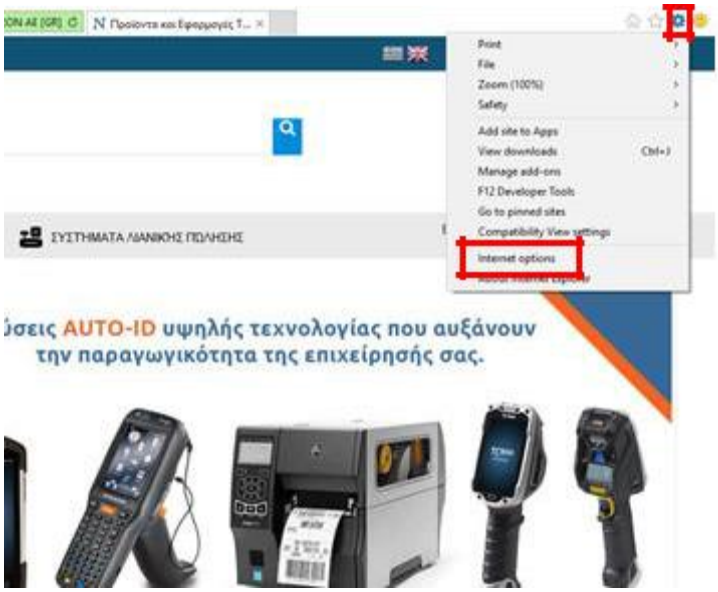
Τα έντεκα πιστοποιητικά τα εγκαθιστούμε ένα προς ένα, στην διαδρομή που επιλέγει το εργαλείο «automatically select the certificate store based on the type of certificate» όπως παραθέτουμε στις επόμενες εικόνες.



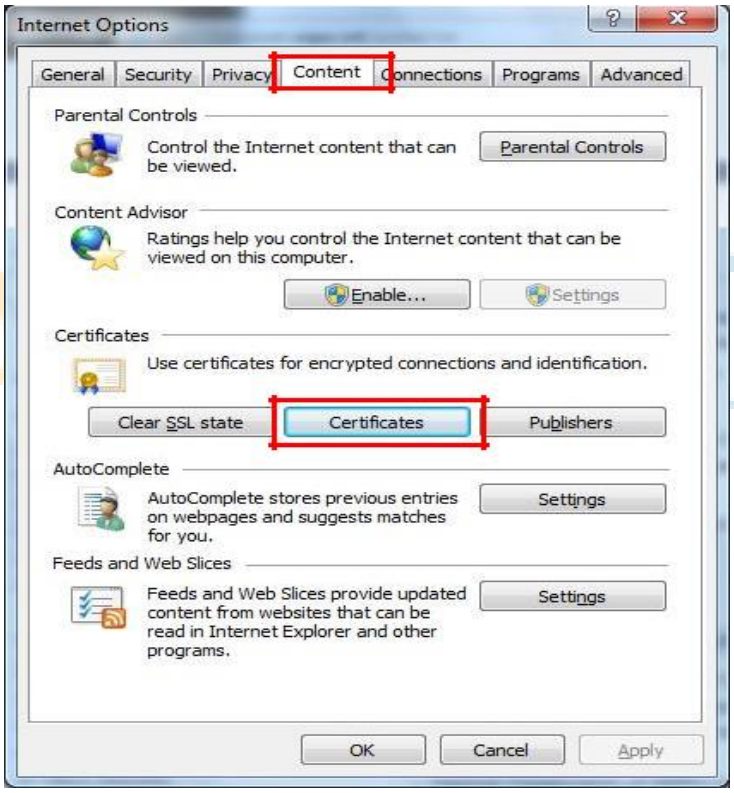




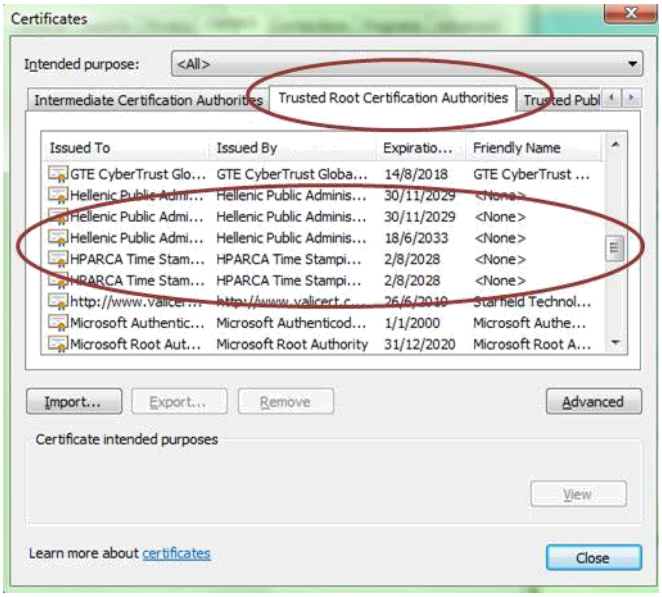
Ελέγχουμε την ορθή εγκατάσταση των Ψηφιακών Πιστοποιητικών ανοίγοντας τον Internet Explorer, επιλέγουμε Εργαλεία (Tools) και στη συνέχεια Internet Options (Επιλογές Internet).



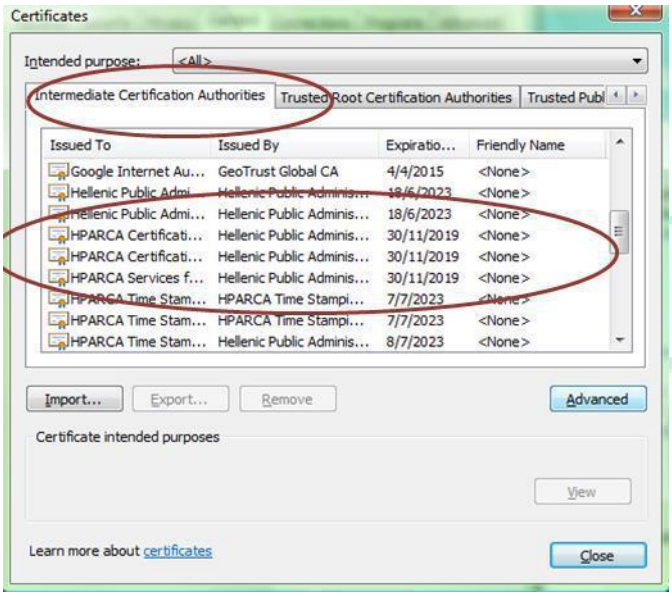
Επιλέγουμε Content (Περιεχόμενο) και Certificates (Πιστοποιητικά).



Στο Trusted Root Certification Authorities (Αξιόπιστες Κεντρικές Αρχές έκδοσης Πιστοποιητικών), πρέπει να υπάρχουν πέντε πιστοποιητικά (3 Hellenic Public Administration, 2 HPARCA).

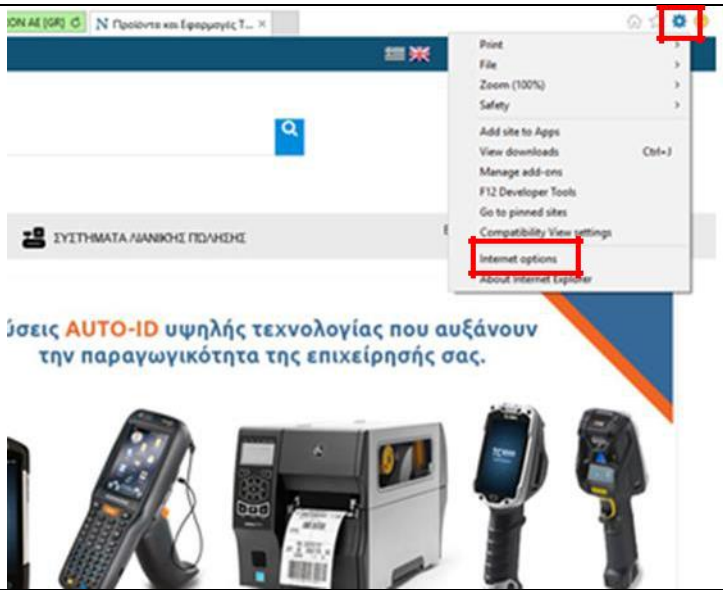


Στο Intermediate Certification Authorities (Ενδιάμεσες Αρχές Έκδοσης Πιστοποιητικών), πρέπει να υπάρχουν έντεκα πιστοποιητικά (2 Hellenic Public Administration, 9 HPARCA).



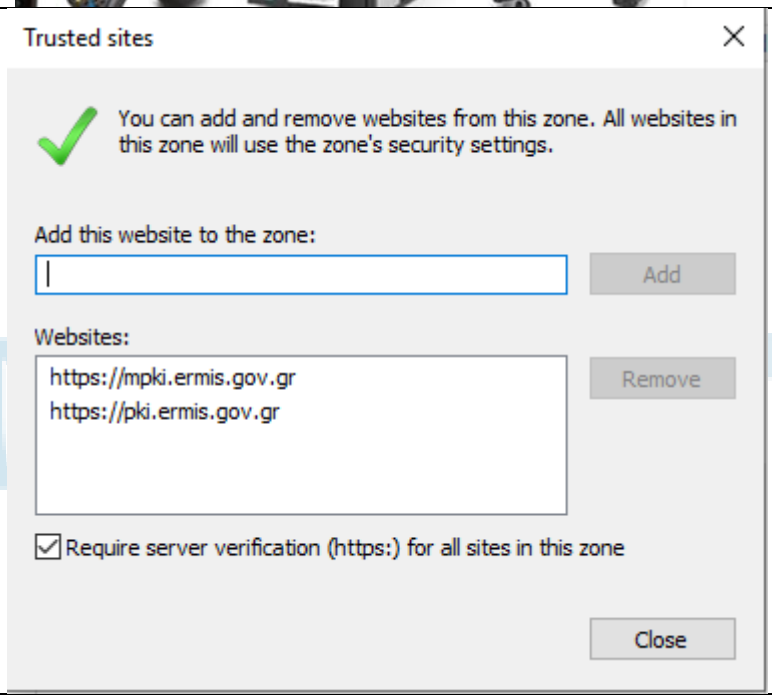
Παραμετροποίηση Internet Explorer

Οι παρακάτω ρυθμίσεις πρέπει να γίνουν αποκλειστικά στον υπολογιστή με τον οποίο θα εγκαταστήσουμε τα προσωπικά μας Ψηφιακά Πιστοποιητικά.

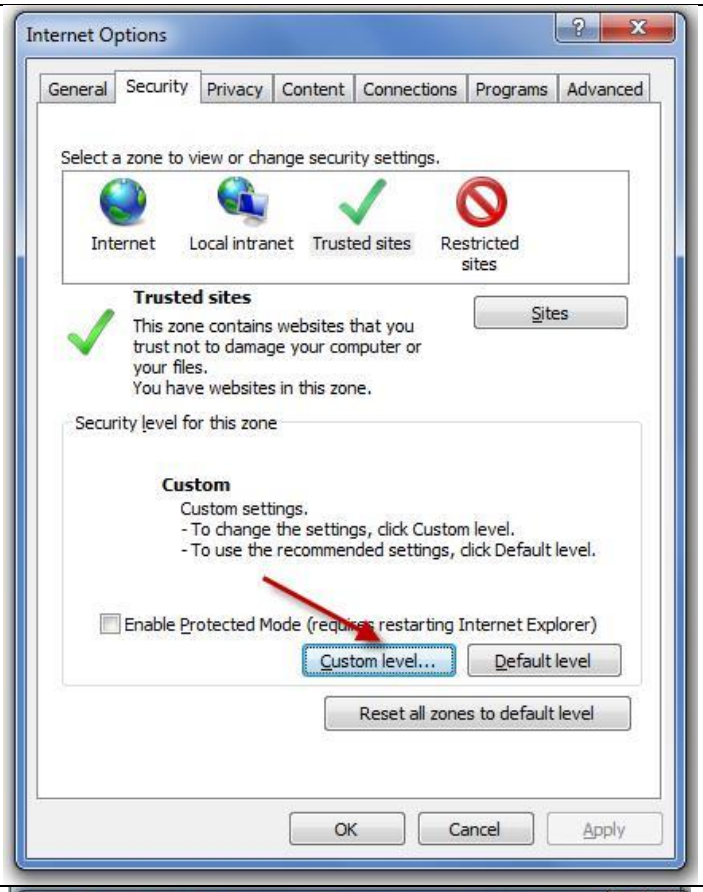


Ανοίγουμε τον Internet Explorer, επιλέγουμε Εργαλεία (Tools) και έπειτα Επιλογές Internet (Internet Options).

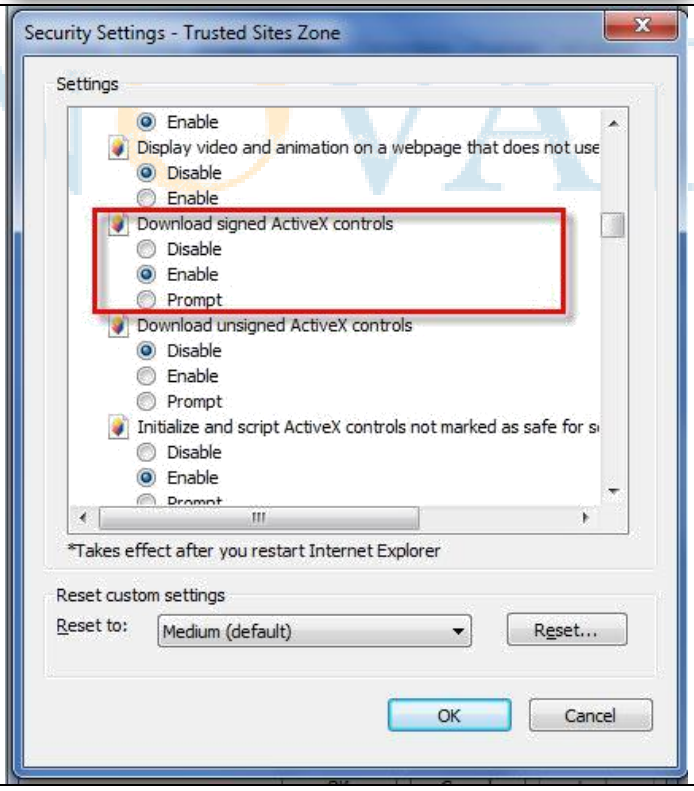
Επιλέγουμε την καρτέλα Ασφάλεια (Security). Από την καρτέλα Ασφάλεια, επιλέγουμε Αξιόπιστες τοποθεσίες (trusted sites) και έπειτα Τοποθεσίες (sites).



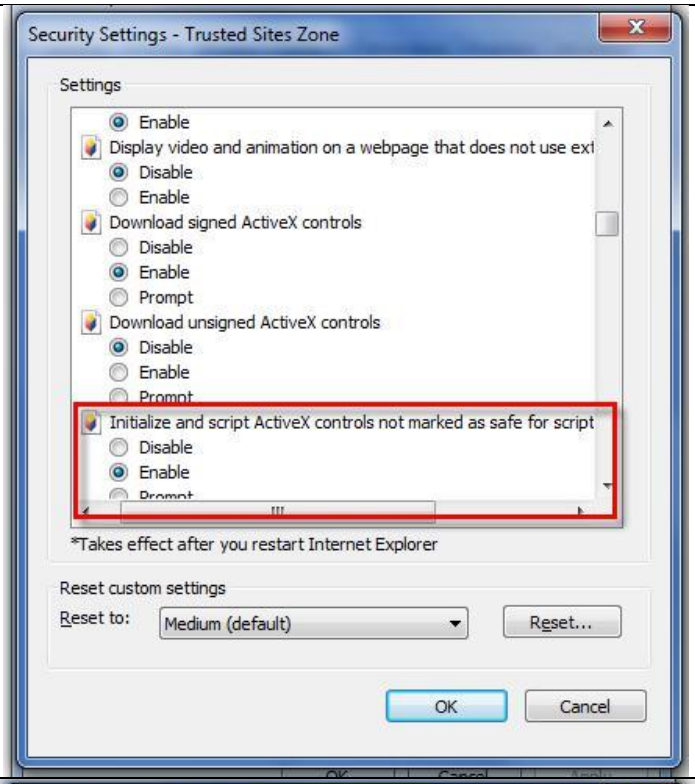
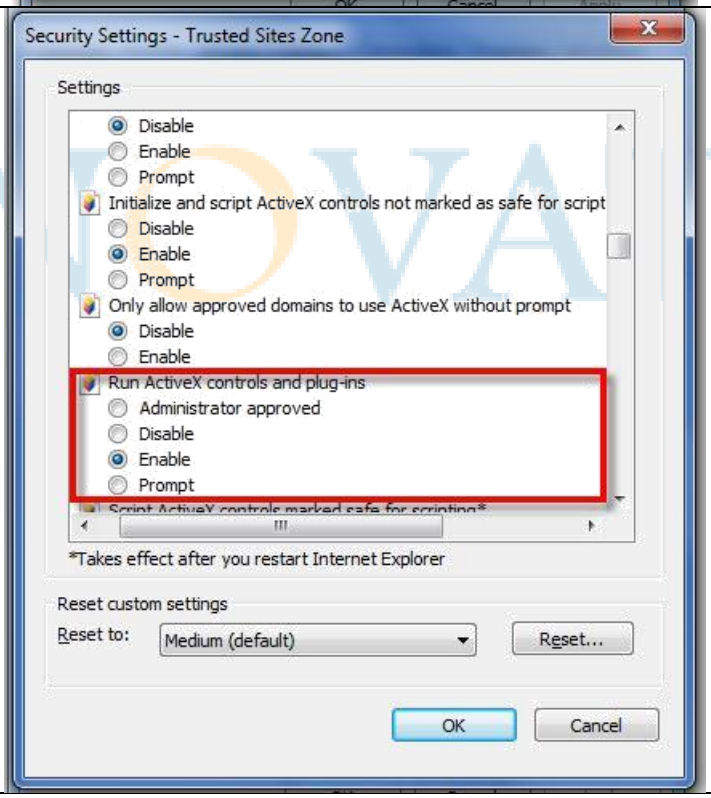
Προσθέτουμε μια, μια τις δύο παρακάτω τοποθεσίες στη λίστα αξιόπιστων τοποθεσιών, πληκτρολογώντας τες στο πλαίσιο και επιλέγοντας Προσθήκη.
https://mpki.ermis.gov.gr
https://pki.ermis.gov.gr

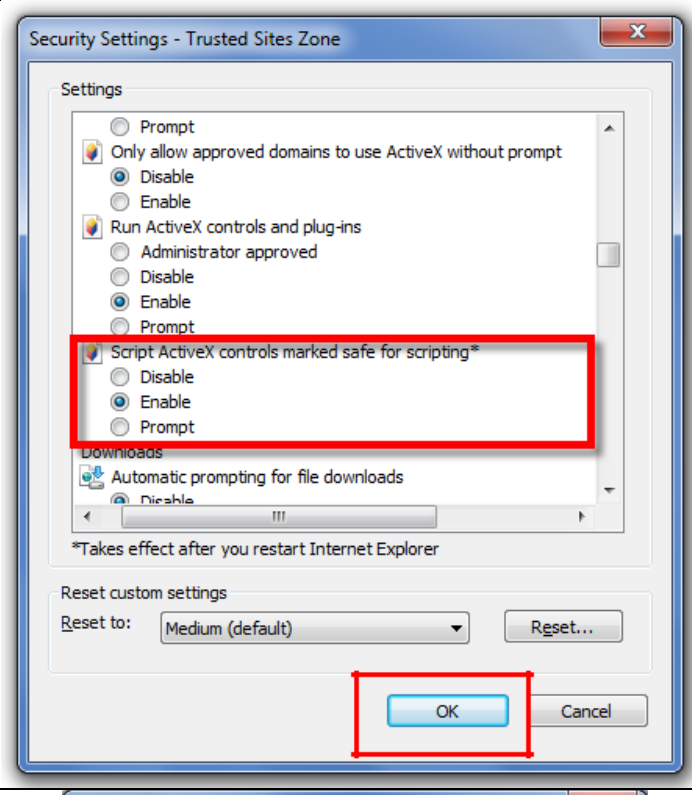
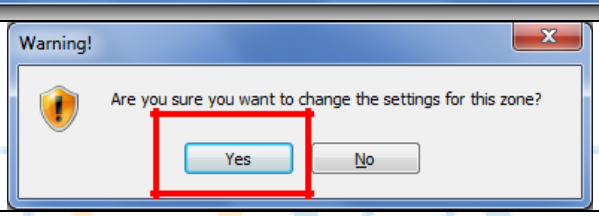


Παραμένουμε στην καρτέλα Ασφάλεια (Security) και έχοντας επιλέξει τις Αξιόπιστες Τοποθεσίες επιλέγετε Προσαρμοσμένο Επίπεδο (Custom Level) και ενεργοποιούμε τα παρακάτω.



Λήψη στοιχείων ελέγχου ActiveX με υπογραφή – Ενεργοποίηση (Download signed ActiveX controls -Enable).

	Προετοιμασία και εκτέλεση στοιχείων ελέγχου ActiveX που δεν χαρακτηρίζονται ως ασφαλή – Ενεργοποίηση (Initialize and script ActiveX controls not marked as safe for scripting – Enable).
	Εκτέλεση στοιχείων ελέγχου ActiveX και προσθηκών – Ενεργοποίηση (Run ActiveX controls and Plugins - Enable).

	Στοιχεία ελέγχου ActiveX που χαρακτηρίζονται ως ασφαλή για εκτέλεση – Ενεργοποίηση (Script ActiveX controls marked safe for scripting* = Enable).
	Αφού ολοκληρώσουμε τις παραπάνω αλλαγές επιλέγουμε OK και εμφανίζεται η εικόνα όπου επιλέγουμε ΝΑΙ για επιβεβαίωση των αλλαγών.

Κλείνουμε όλα τα ανοιχτά παράθυρα του Internet Explorer.

Βήμα 5ο: Εγκατάσταση του AWP Manager (πρόγραμμα οδήγησης του Oberthur Usb Token).

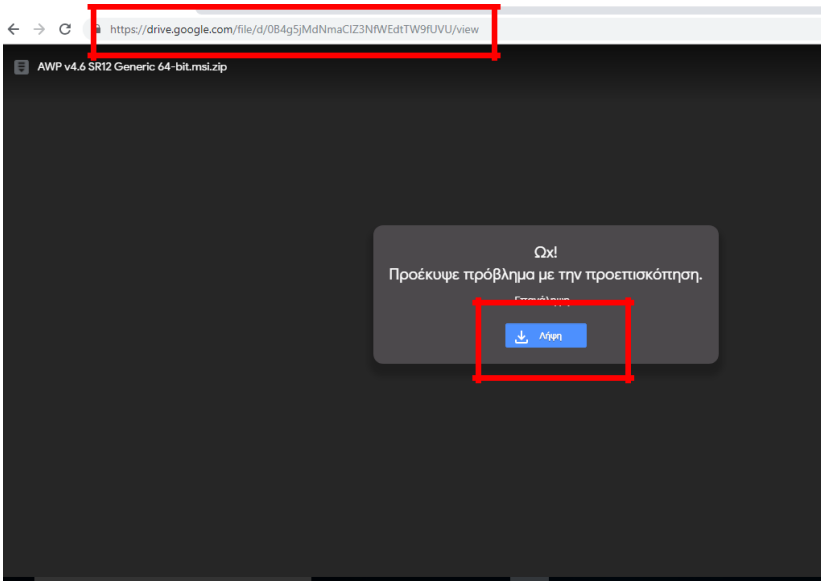
Για Windows 7, 8, 10 (32bit) κατεβάζουμε το AWP Manager από εδώ:

https://drive.google.com/open?id=0B4g5jMdNmaCITlJud2MxRzNtbUU

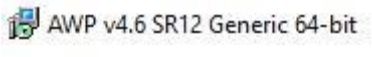
Για Windows 7, 8, 10 (64bit) κατεβάζουμε το AWP Manager από εδώ:

https://drive.google.com/open?id=0B4g5jMdNmaCIZ3NfWEdtTW9fUVU

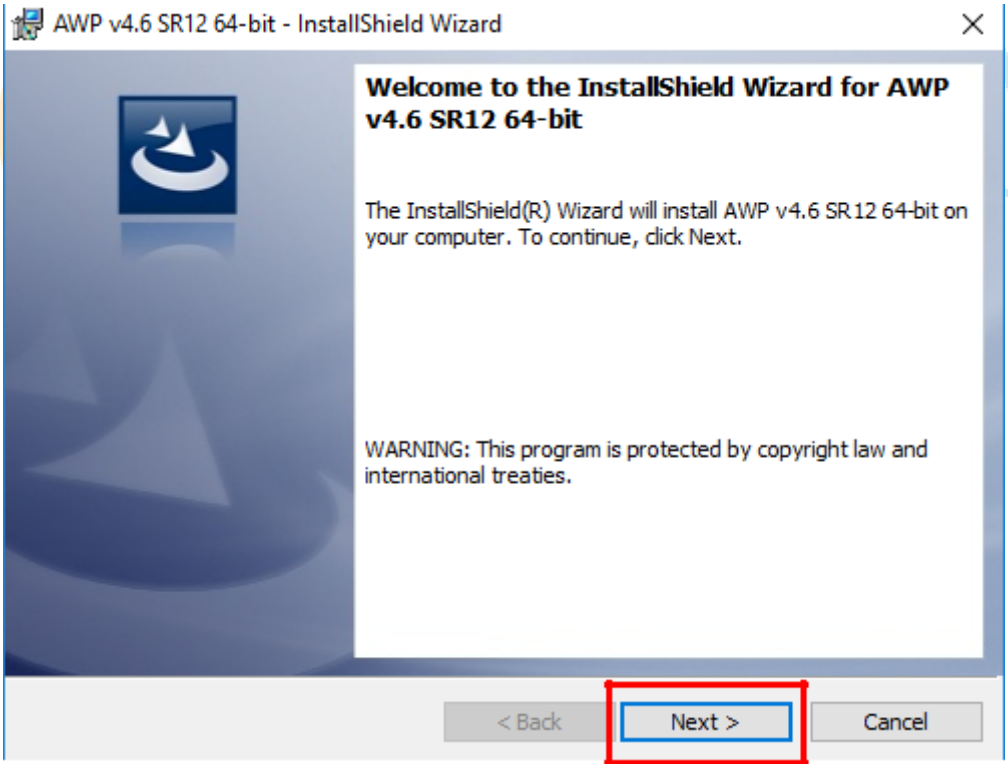
Επιλέγουμε Λήψη (Download).



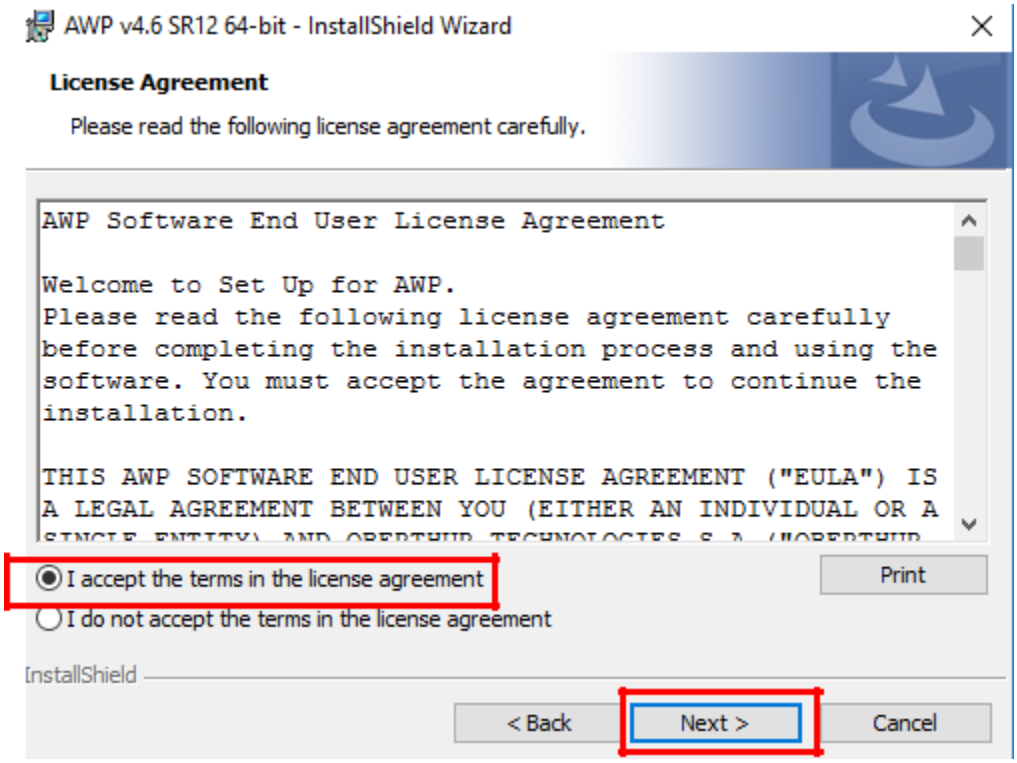
Κατεβαίνει το zip αρχείο (θα βρίσκεται στα Downloads του υπολογιστή μας), το ανοίγουμε και το τρέχουμε (για την εγκατάσταση σε περιβάλλον Windows θα πρέπει να έχουμε όλες τις εφαρμογές κλειστές καθώς στο τέλος της εγκατάστασης θα γίνει επανεκκίνηση του υπολογιστή).

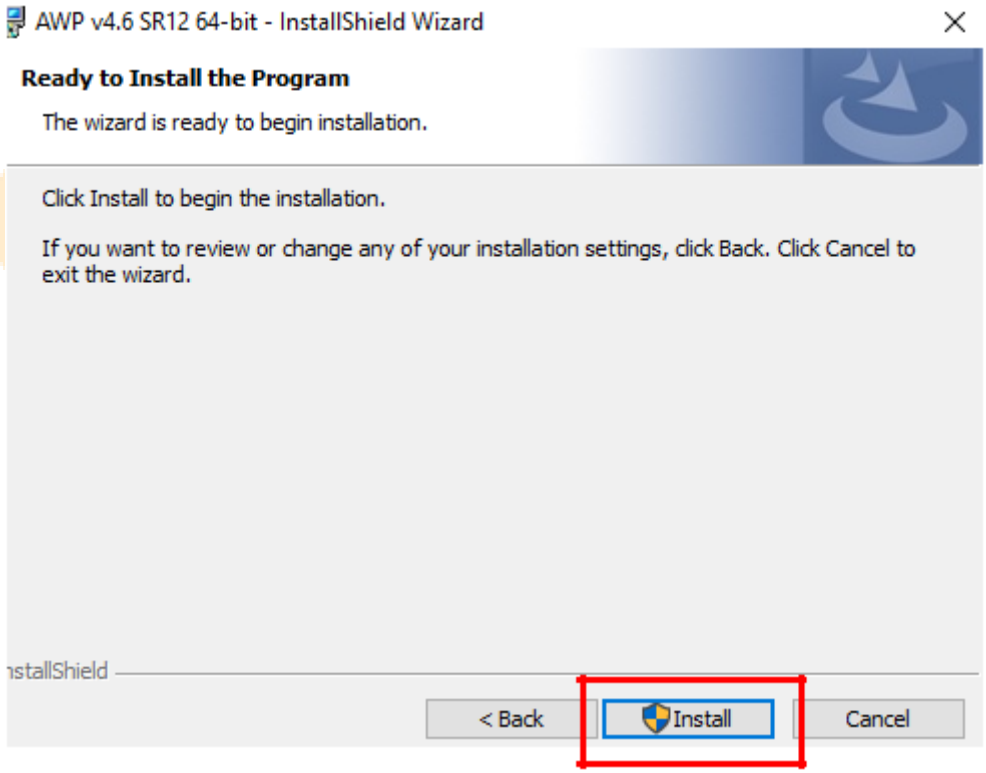


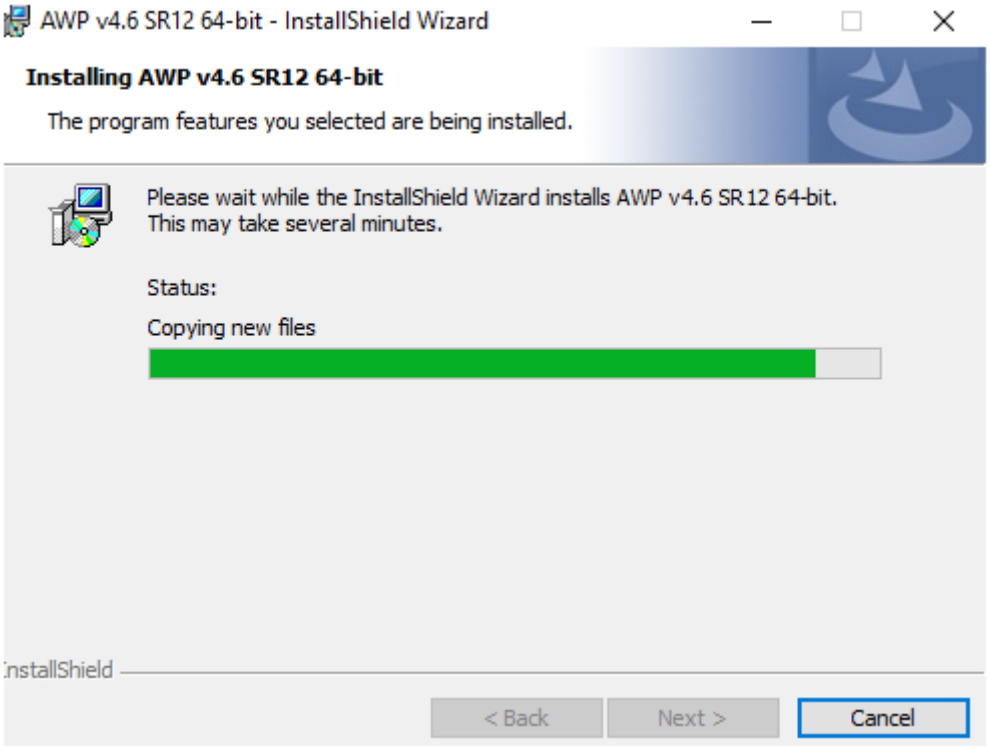
Επιλέγουμε Next.

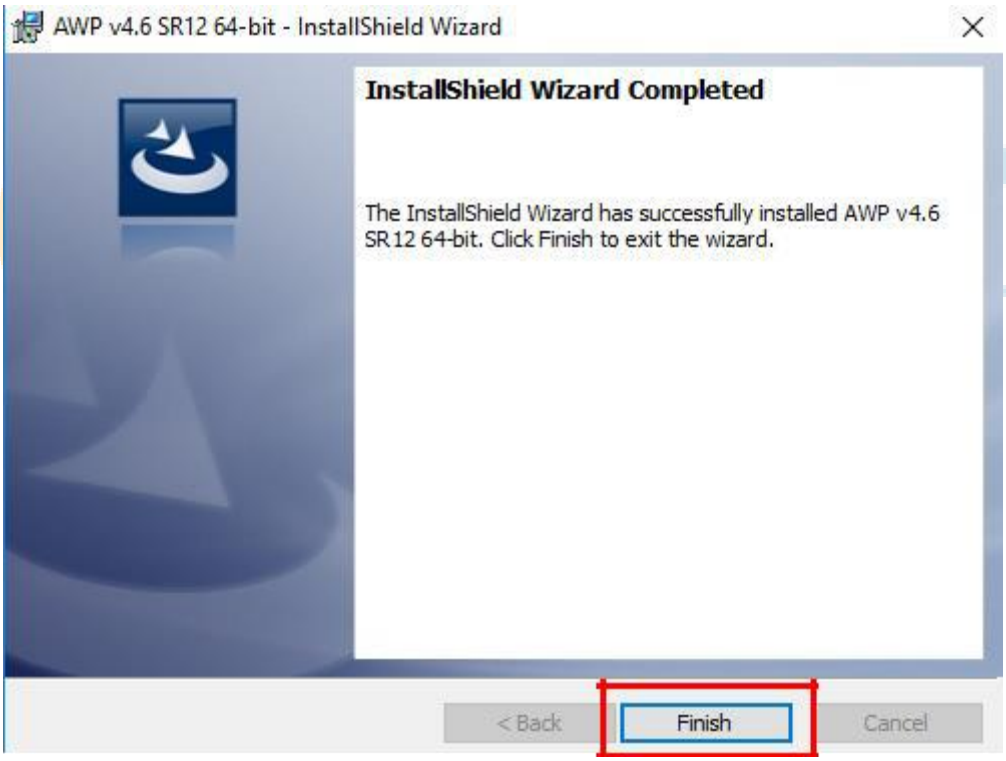


Κάνουμε με τη σειρά τις επιλογές που φαίνονται στις φωτογραφίες.

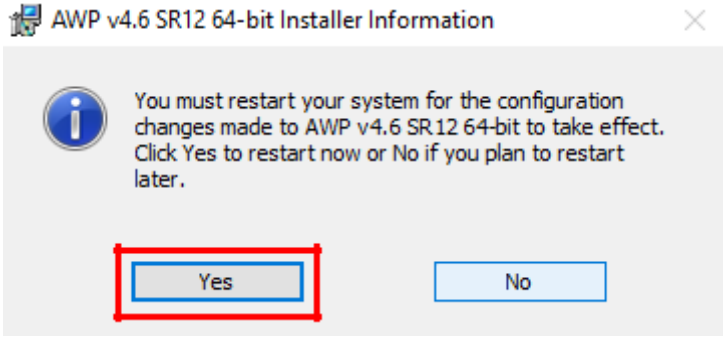

AWP v4.6 SR12 64-bit - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AWP Software End User License Agreement
Welcome to Set Up for AWP.
Please read the following license agreement carefully before completing the installation process and using the software. You must accept the agreement to continue the installation.
THIS AWP SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel


AWP v4.6 SR12 64-bit - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel





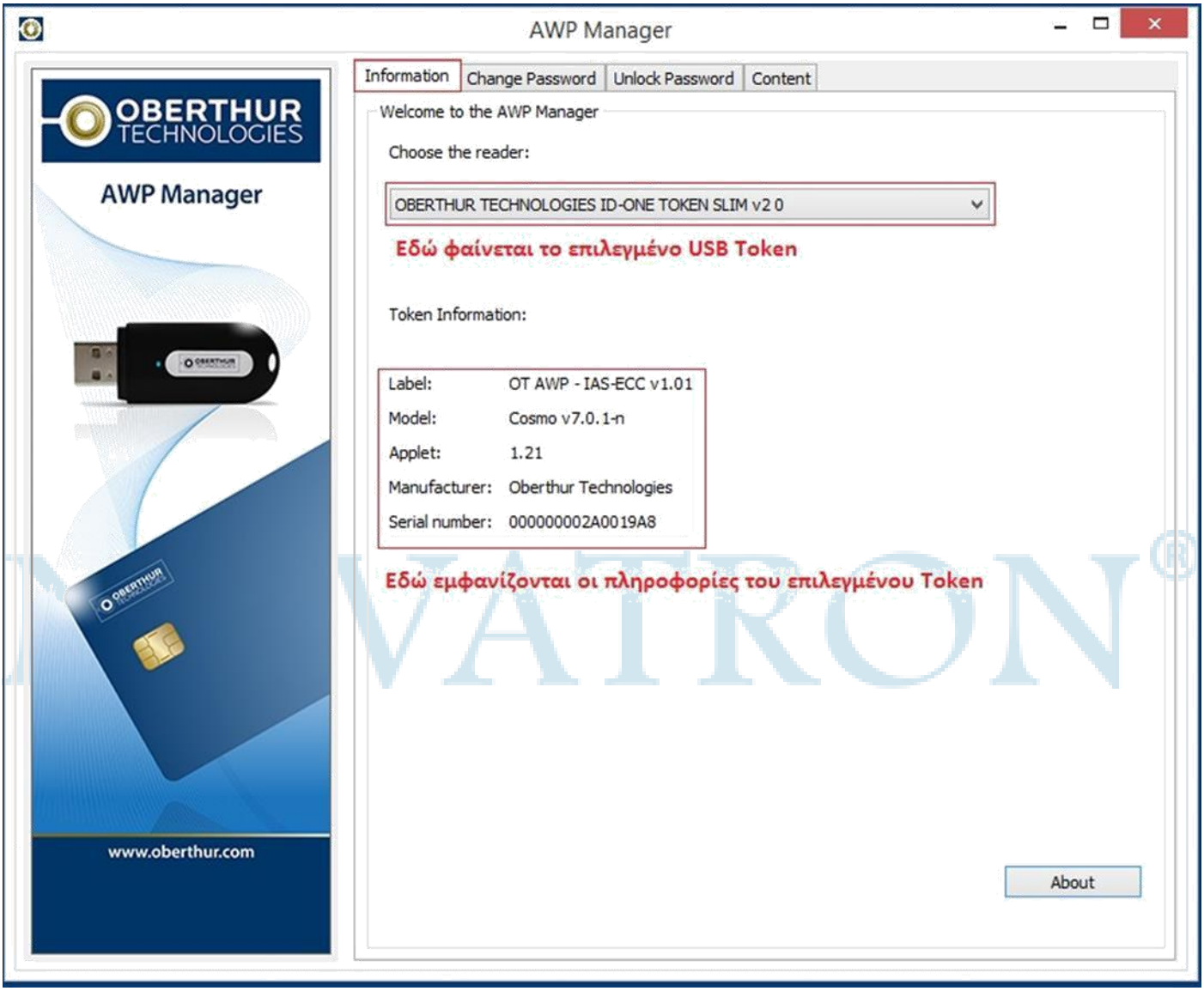
Ολοκληρώνουμε την εγκατάσταση με επανεκκίνηση του υπολογιστή πατώντας Yes.



Μετά την επανεκκίνηση μπορούμε να ελέγξουμε την ορθή εγκατάσταση επιλέγοντας διαδοχικά: Έναρξη (Start) → Όλα τα προγράμματα (All Programs) → AWP → AWP Manager.

Η εφαρμογή AWP Manager είναι ένα βοηθητικό εργαλείο για την διαχείριση του USB Token όσον αφορά τους κωδικούς πρόσβασης και τα εγκατεστημένα πιστοποιητικά.

Από την καρτέλα Information μπορούμε να δούμε χρήσιμες πληροφορίες για το USB Token όπως το μοντέλο και το σειριακό αριθμό.



Από την καρτέλα Change Password μπορούμε να αλλάξουμε τα προεπιλεγμένα PIN (User Password) και PUK (SO Password) της συσκευής (το PIN και το PUK πρέπει να αποτελείται από 4 ψηφία).

Επιλέγοντας από την κορυφή πιο συνθηματικό επιθυμούμε να αλλάξουμε (User Password ή SO Password) συμπληρώνουμε ανάλογα τα παρακάτω πεδία.

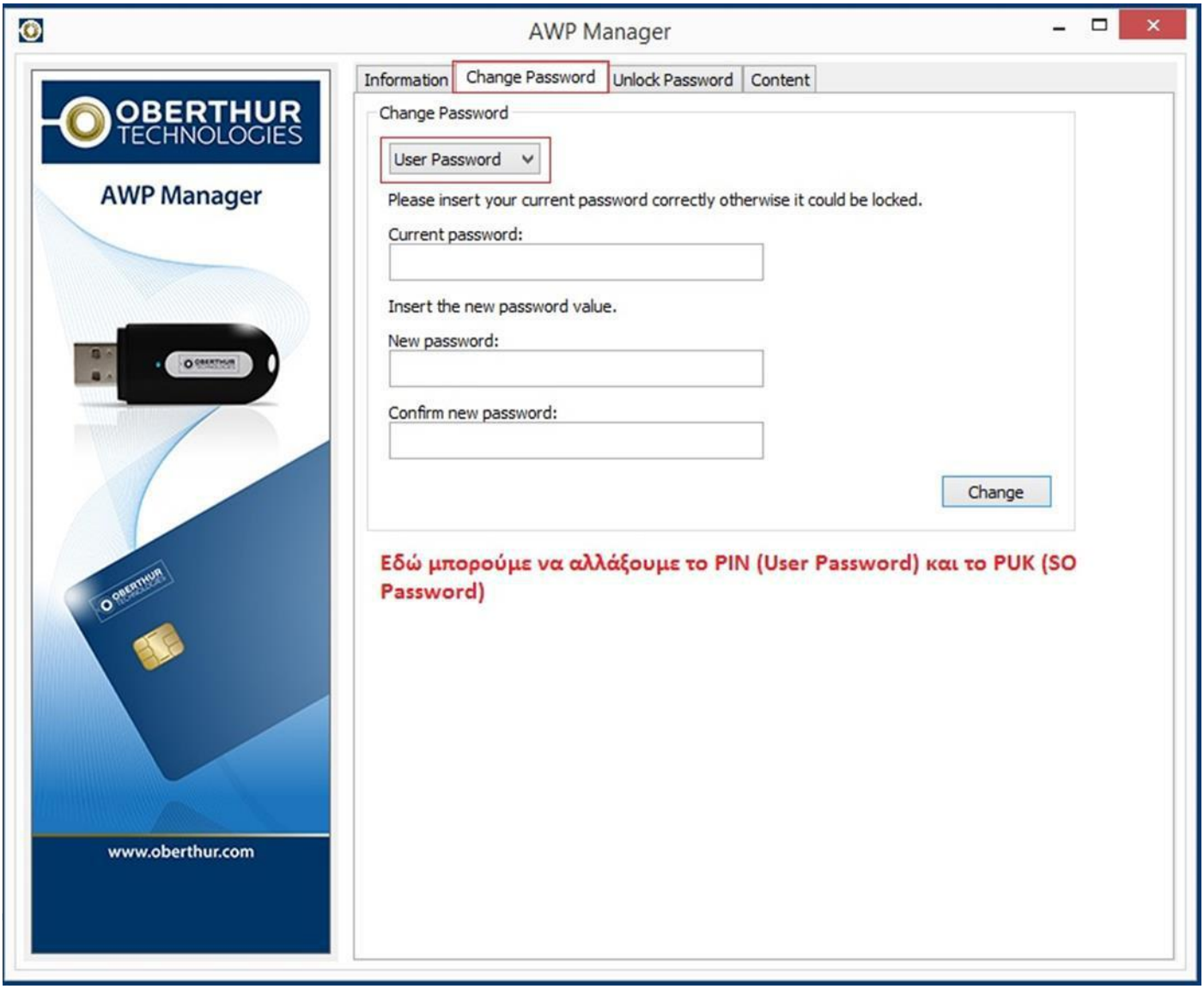
Current Password: Το τρέχον συνθηματικό της συσκευής.

New Password: Το νέο συνθηματικό που επιθυμούμε.

Confirm new password: Επιβεβαίωση του νέου συνθηματικού.

Με το κουμπί Change επιβεβαιώνουμε τις αλλαγές.

ΠΡΟΣΟΧΗ: Το αρχικό PIN του USB Token είναι 9999 και το αρχικό PUK είναι 1234. Σε περίπτωση τριών λάθος καταχωρήσεων του PIN το USB Token κλειδώνει και πρέπει να ξεκλειδωθεί το PIN με τη χρήση του PUK. Σε περίπτωση τριών λάθος καταχωρήσεων του PUK η συσκευή κλειδώνει οριστικά και δεν είναι δυνατή η επαναφορά της.



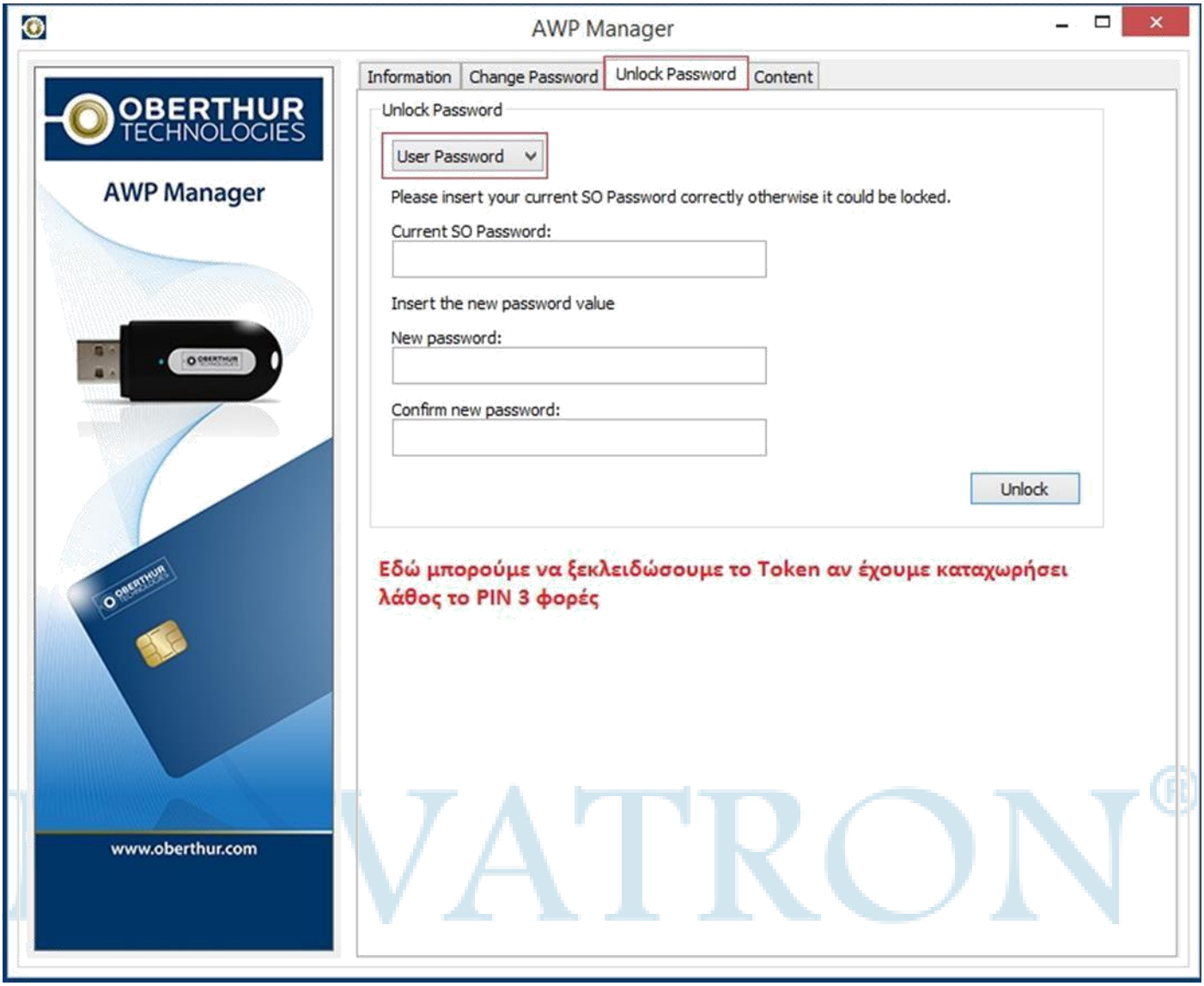
Από την καρτέλα Unlock Password μπορούμε να ξεκλειδώσουμε το συνθηματικό της συσκευής σε περίπτωση που το έχουμε χρησιμοποιήσει λάθος τρεις φορές συμπληρώνοντας τα ακόλουθα πεδία.

Current SO Password: Συμπληρώνουμε το PUK (SO Password) της συσκευής.

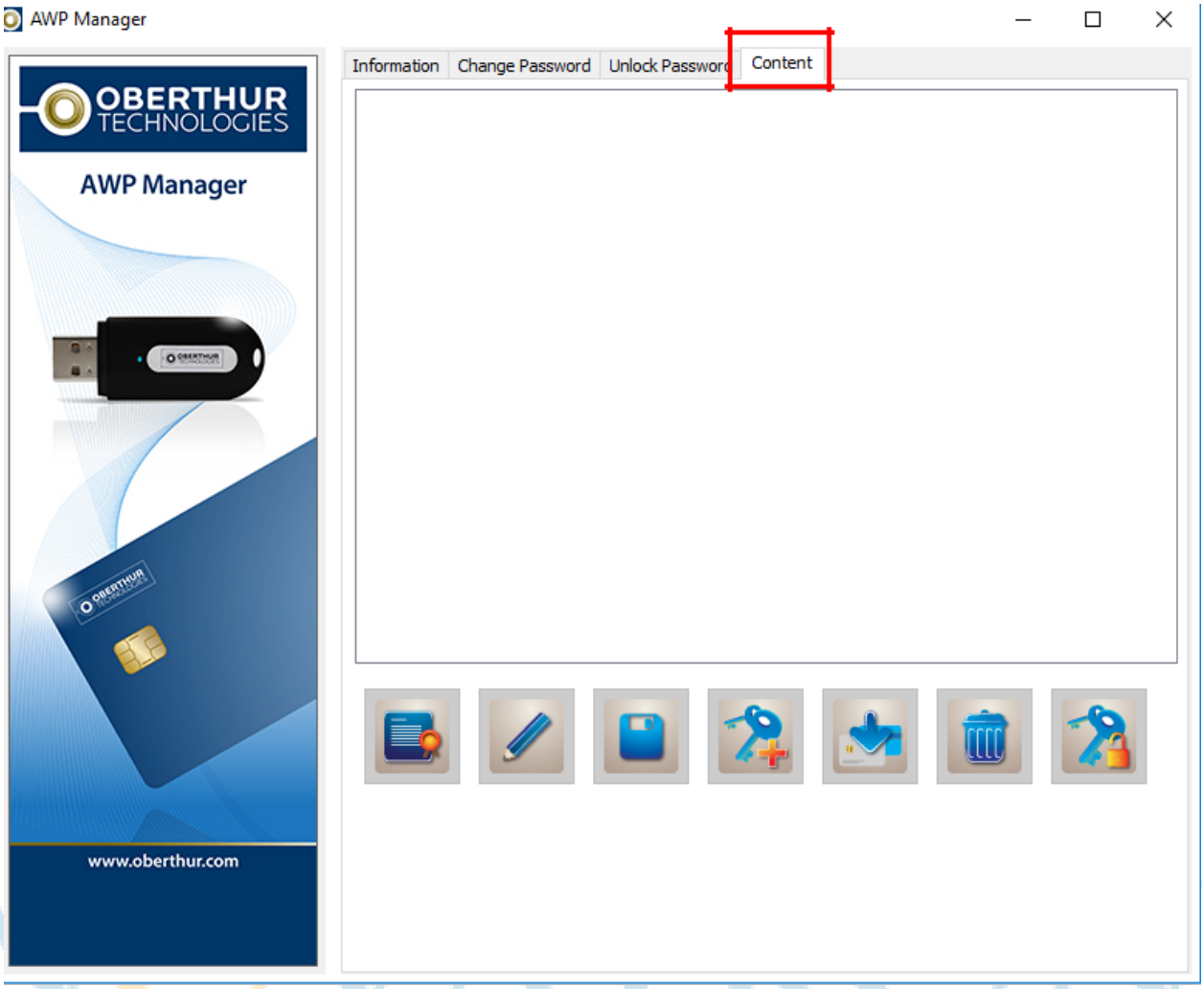
New Password: Το νέο συνθηματικό που επιθυμούμε.

Confirm new password: Επιβεβαίωση του νέου συνθηματικού.

Με το κουμπί Unlock επιβεβαιώνουμε τις αλλαγές.



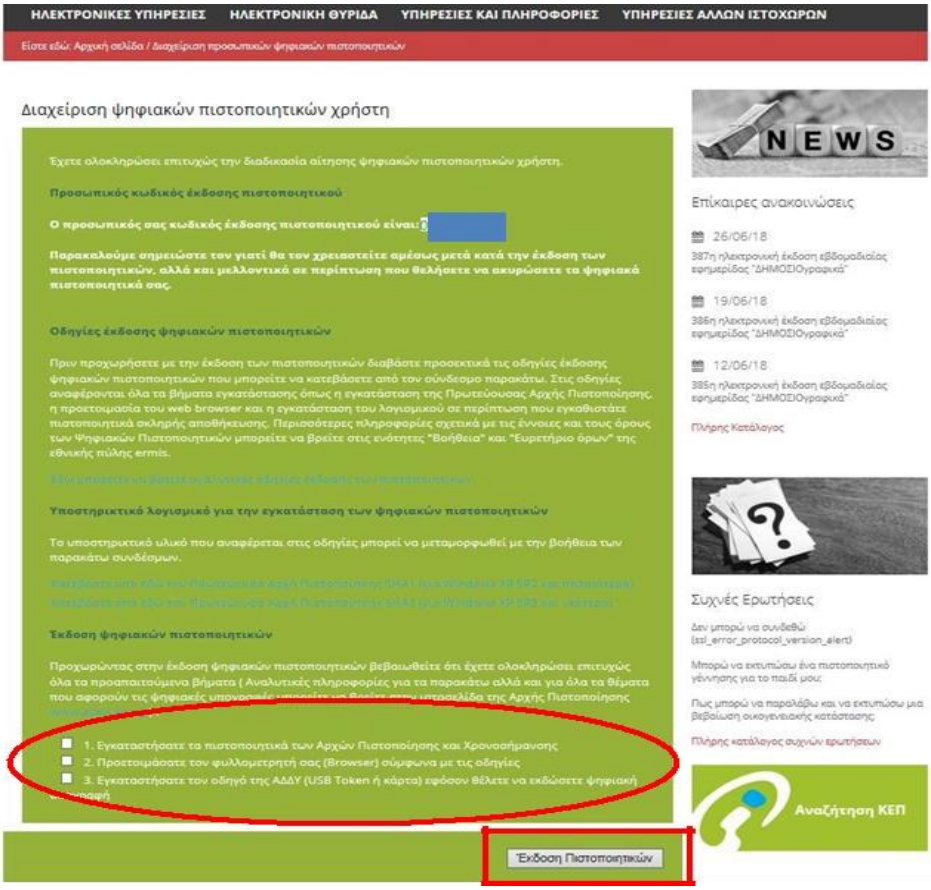
Από αυτήν την καρτέλα μπορούμε να δούμε τα εγκατεστημένα πιστοποιητικά στο USB Token (για να ολοκληρωθεί η διαδικασία χωρίς προβλήματα πρέπει το Token να είναι άδειο).



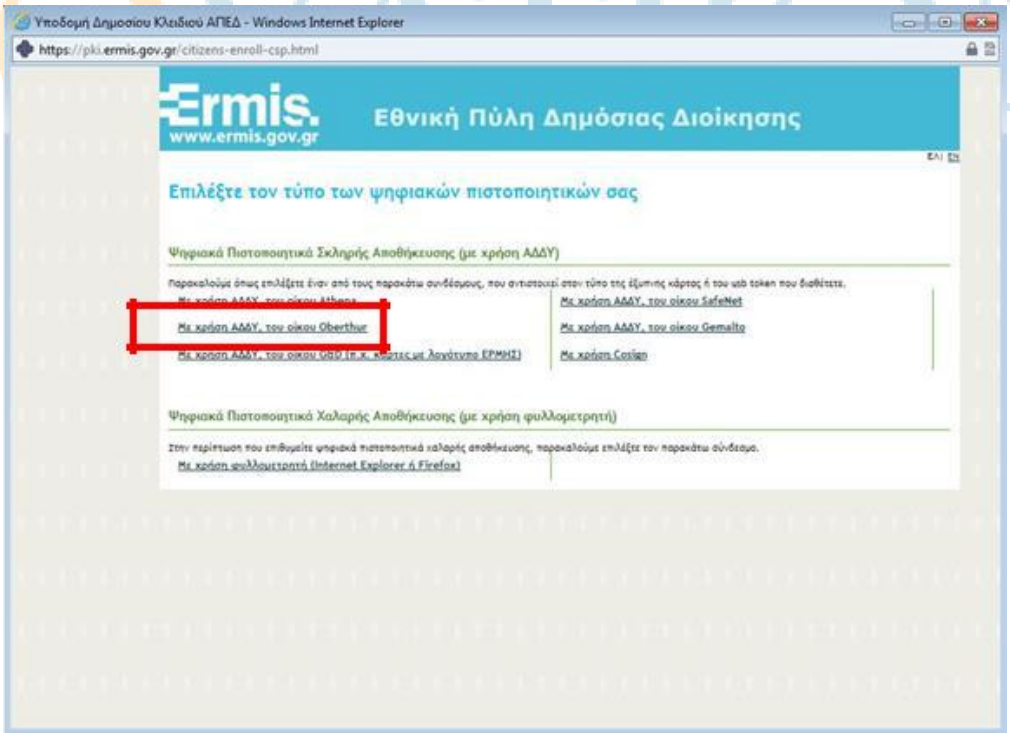
Πλέον είμαστε έτοιμοι να εγκαταστήσουμε τα πιστοποιητικά μας στο USB Token.

Βήμα 6ο: Έκδοση προσωπικών Ψηφιακών Πιστοποιητικών – Εγκατάσταση αυτών στο Oberthur USB Token.

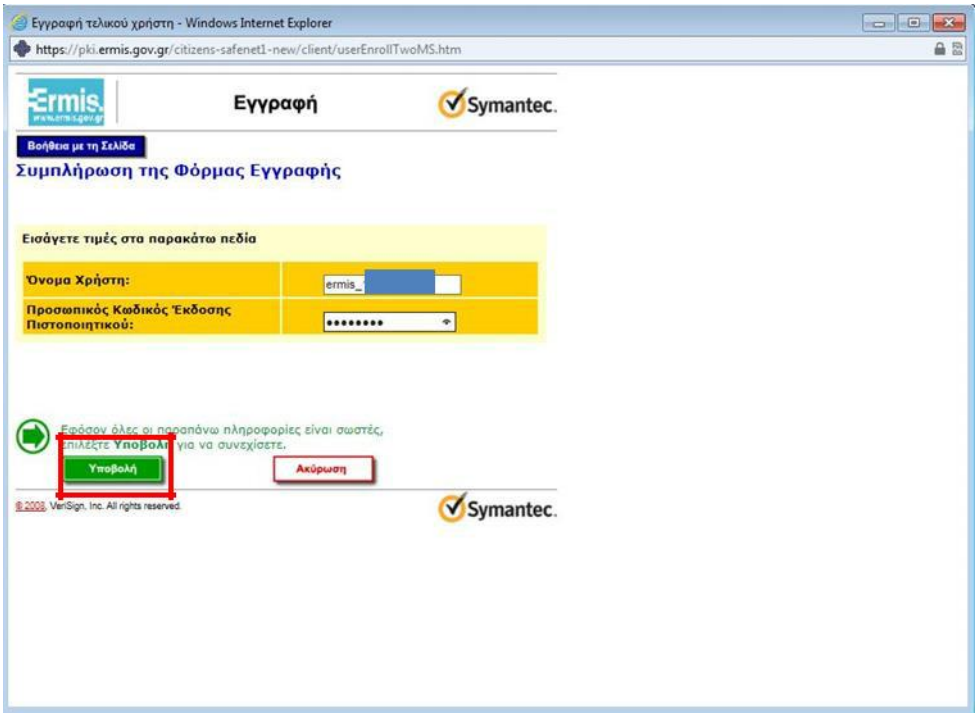
Μπαίνουμε με τους κωδικούς Taxisnet στην Πύλη ΕΡΜΗΣ (βλ. Βήμα 1ο) και επιλέγουμε το σύνδεσμο Πίνακας Ελέγχου και στη συνέχεια το σύνδεσμο Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών (βλ. Βήμα 1ο), πλέον έχουμε την παρακάτω εικόνα, όπου καταγράφουμε τον οκταψήφιο κωδικό έκδοσης και τσεκάρουμε τις τρεις επιλογές που υπάρχουν στο τέλος της ιστοσελίδας πριν από το κουμπί Έκδοση Πιστοποιητικών, έπειτα επιλέγουμε Έκδοση Πιστοποιητικών.



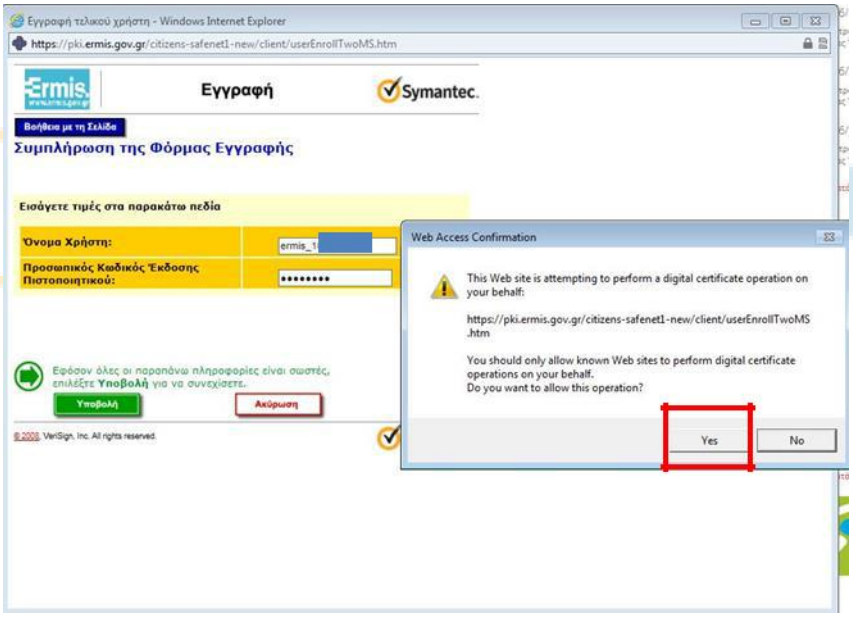
Ανοίγει η ακόλουθη καρτέλα όπου επιλέγουμε Με χρήση ΑΔΔΥ, του οίκου Oberthur.



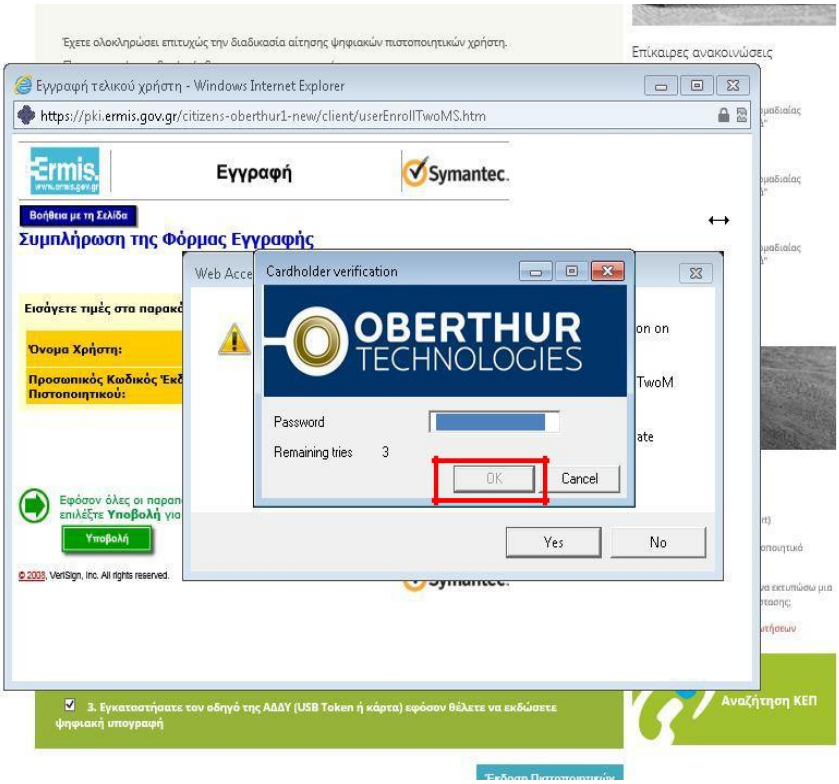
Τώρα εμφανίζεται σελίδα με δύο πεδία. Το πρώτο πεδίο θα πρέπει να συμπληρωθεί με το όνομα χρήστη που έχουμε στη Πύλη ΕΡΜΗΣ (ermis_ …….), ενώ στο πεδίο Προσωπικός Κωδικός Έκδοσης Πιστοποιητικού πληκτρολογούμε τον οκταψήφιο κωδικό και στη συνέχεια πατάμε το κουμπί Υποβολή.



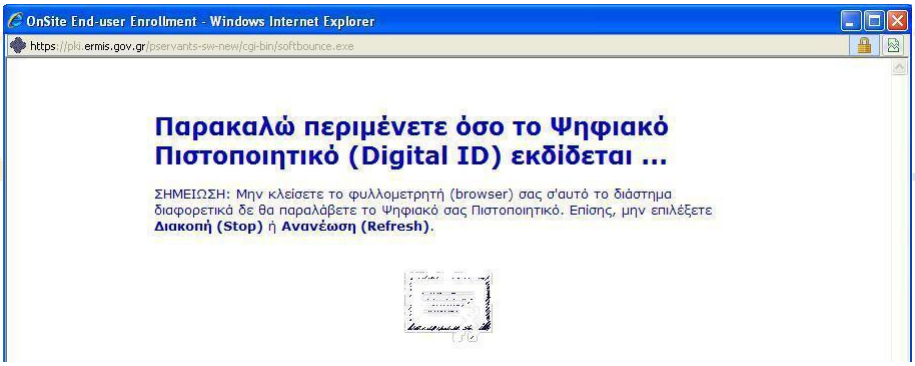
Στη συνέχεια πατάμε Yes στο μήνυμα της παρακάτω εικόνας, καθώς και σε όσα παρόμοια μηνύματα παρουσιαστούν.



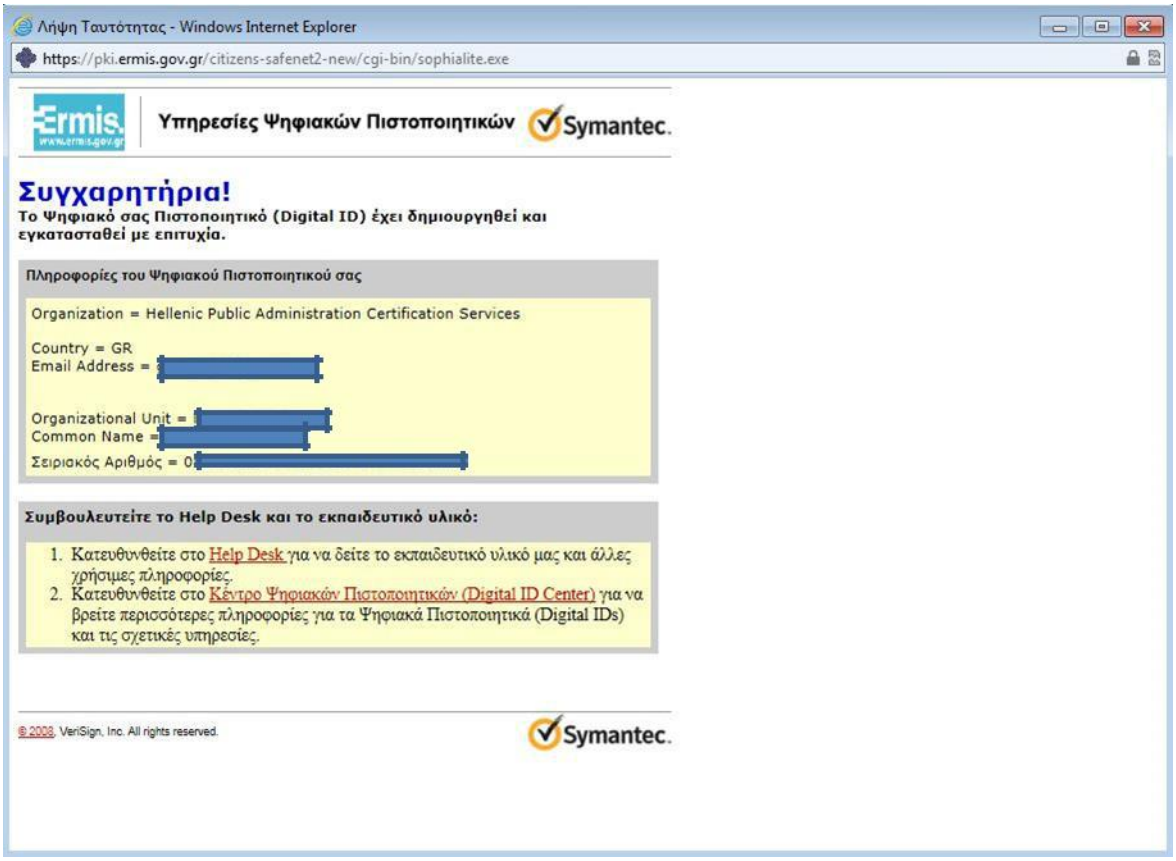
Έπειτα εισάγουμε το Pin του Oberthur USB Token στο οποίο θα αποθηκευτούν τα ψηφιακά πιστοποιητικά και πατάμε Ok.



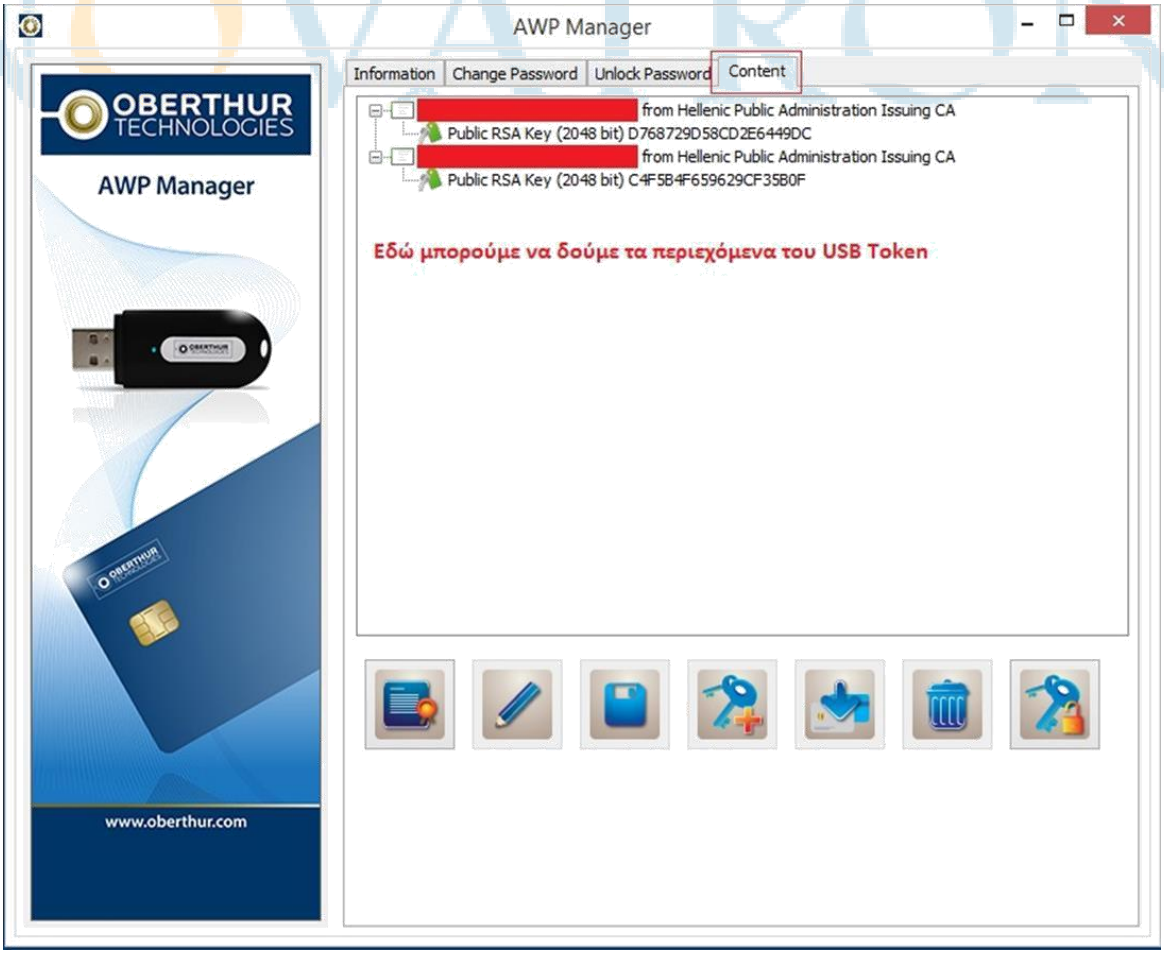
Περιμένουμε όσο χρειαστεί και σε περίπτωση που βγάλει οποιοδήποτε μήνυμα που ζητά την άδειά μας για πρόσβαση πατάμε Yes, εισάγουμε το Pin και Ok.



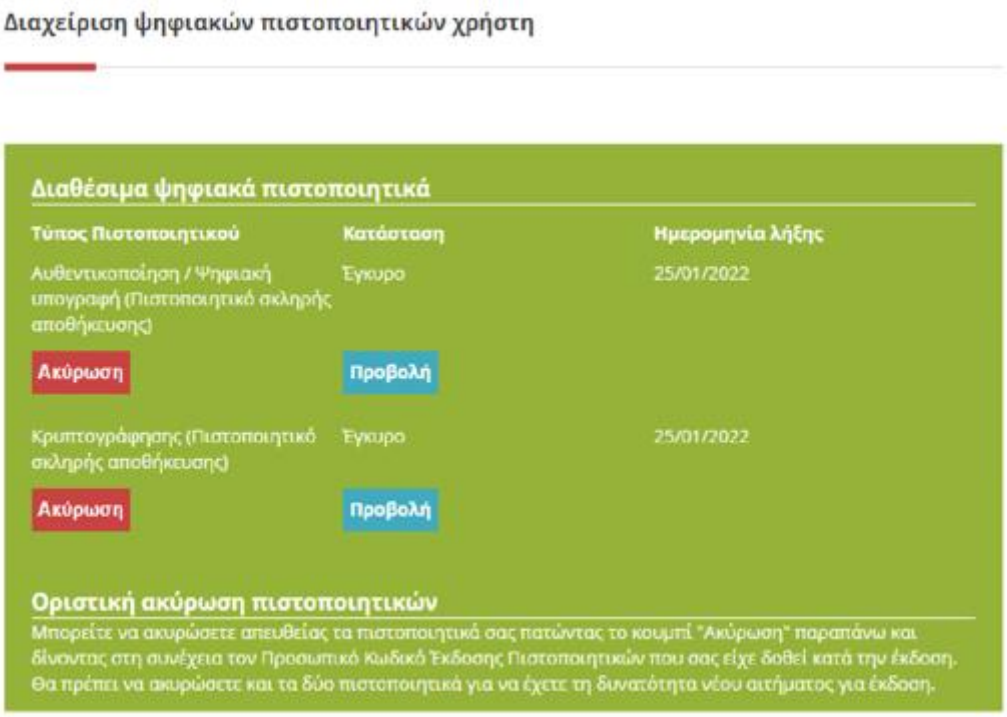
Όταν η διαδικασία ολοκληρωθεί θα παρουσιαστεί η ακόλουθη εικόνα, η οποία περιέχει και τα στοιχεία του κατόχου του πιστοποιητικού.



Τέλος, ανοίγουμε το AWP Manager και στο πεδίο Content, μπορούμε να δούμε τα αποθηκευμένα προσωπικά Ψηφιακά Πιστοποιητικά.



Πλέον στην Πύλη ΕΡΜΗΣ, στον Πίνακα Ελέγχου και στη συνέχεια στη Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών, έχουμε την εξής εικόνα.



Το Oberthur USB Token φέρει τα ψηφιακά μας πιστοποιητικά, μπορούμε να υπογράφουμε τα έγγραφά μας στον υπολογιστή με τα Windows 7 στον οποίο ολοκληρώσαμε την εγκατάσταση αλλά και σε υπολογιστές με νεότερα λειτουργικά συστήματα (πχ Windows 10).

Στο σύνολο των υπολογιστών που θα χρησιμοποιούμε το Token μας πρέπει:

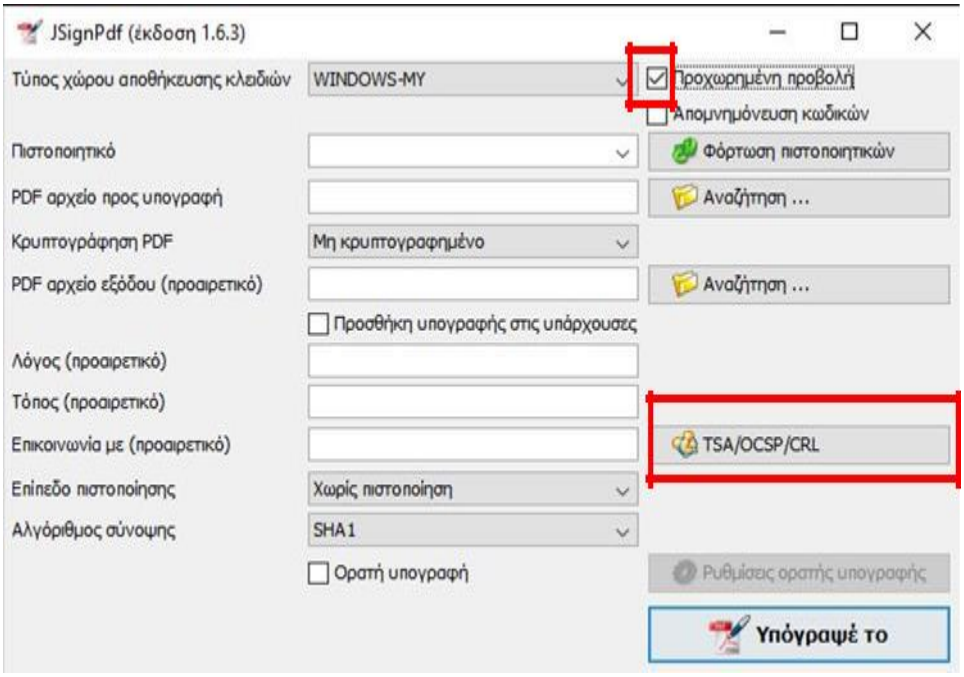
- Να εγκαταστήσουμε τα 16 πιστοποιητικά των Αρχών Πιστοποίησης και Χρονοσήμανσης (βλ. Βήμα 4ο)
- Να εγκαταστήσουμε το AWP Manager
- Να εγκαταστήσουμε ένα πρόγραμμα το οποίο καθιστά δυνατή την υπογραφή Pdf αρχείων (θα το δούμε παρακάτω)

Ψηφιακή Υπογραφή με το πρόγραμμα JsignPdf.

Το πρόγραμμα JsignPdf είναι ένα ελεύθερο στο διαδίκτυο πρόγραμμα, μπορούμε να το κατεβάσουμε και από εδώ:

https://sourceforge.net/projects/jsignpdf/

Κατεβάζουμε, τρέχουμε, εγκαθιστούμε και ανοίγουμε το πρόγραμμα, μόλις εμφανιστεί η αρχική σελίδα επιλέγουμε Προχωρημένη Προβολή και στη συνέχεια κάνουμε κλικ στο κουμπί TSA/OCSP/CRL. :



Επιλέγουμε Χρησιμοποίησε ασφαλή χρονοσήμανση.

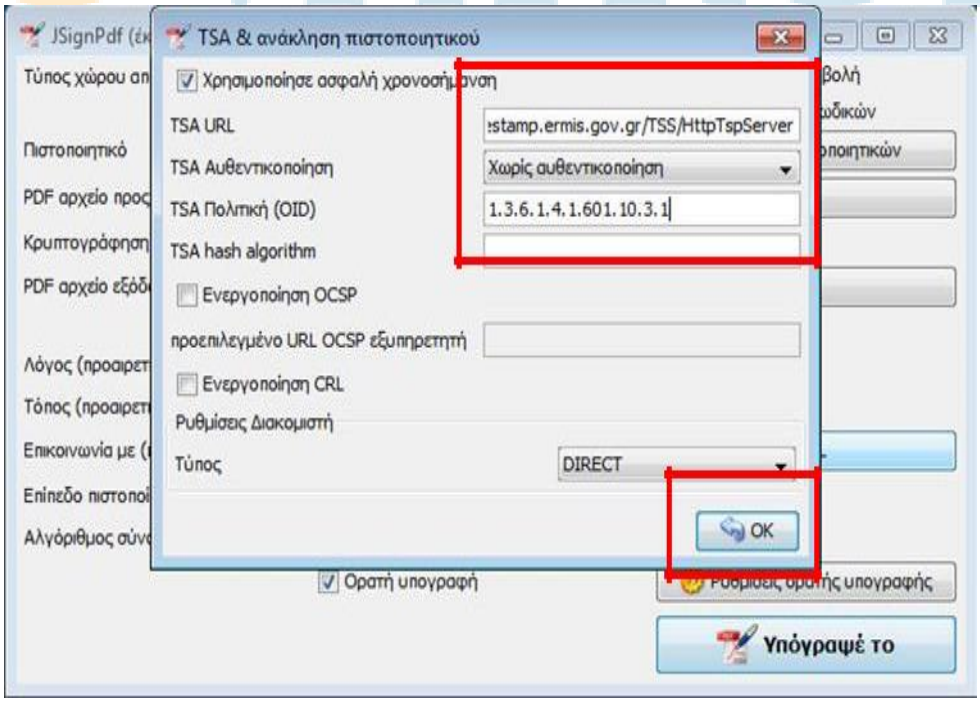
Για να χρησιμοποιήσουμε την ασφαλή χρονοσήμανση της Εθνικής Πύλης ΕΡΜΗΣ, στο πεδίο TSA/URL πληκτρολογούμε τη διεύθυνση του αξιόπιστου Εξυπηρετητή:

http://timestamp.ermis.gov.gr/TSS/HttpTspServer

Επίσης απαιτείται στο πεδίο TSA Πολιτική (OID) να πληκτρολογήσουμε το:

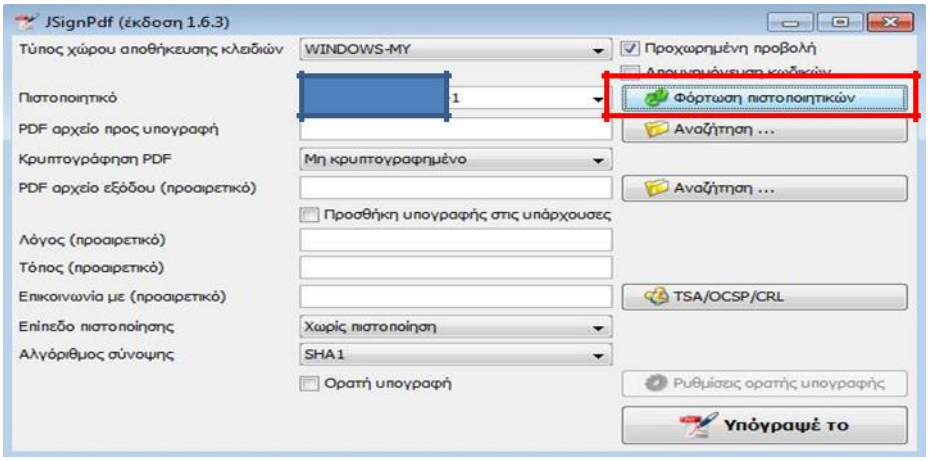
1.3.6.1.4.1.601.10.3.1

Κάνουμε κλικ στο κουμπί OK.

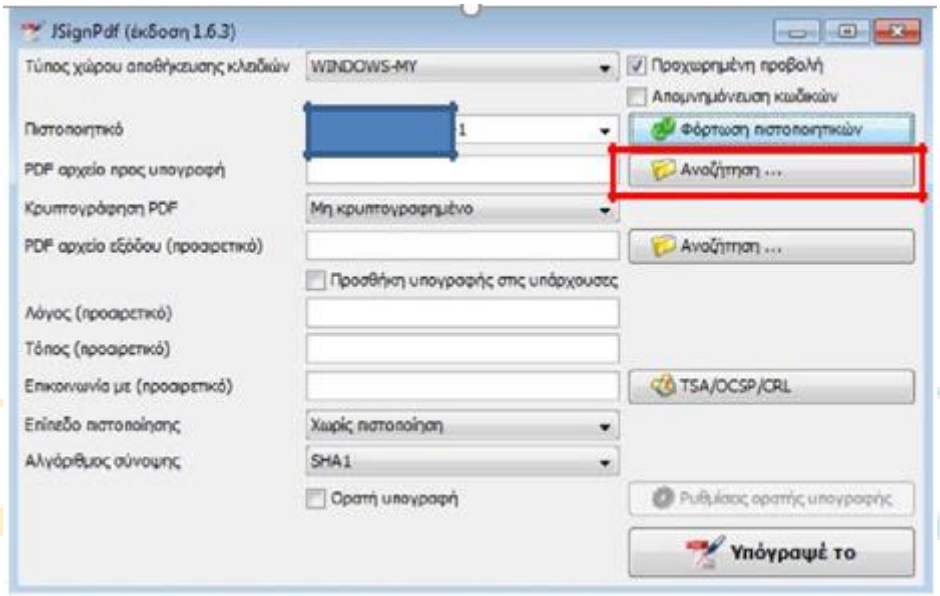


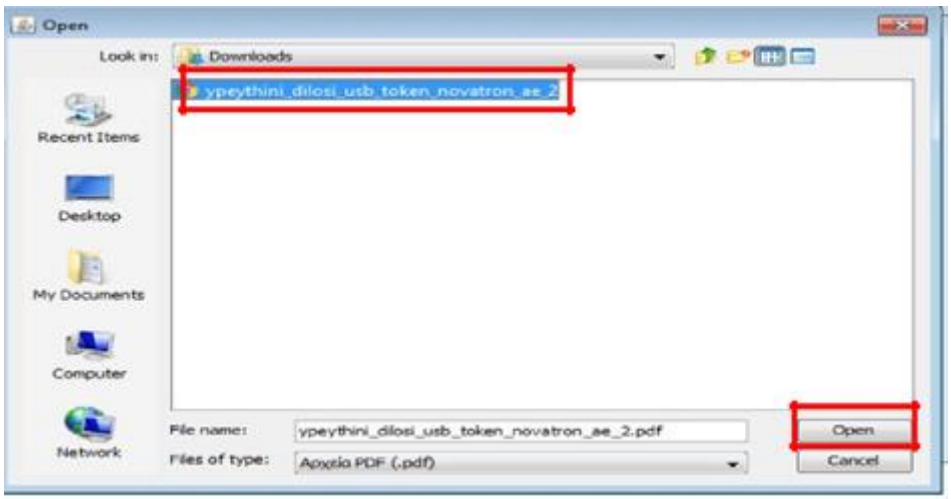
Η παραπάνω διαδικασία γίνεται μία φορά, το πρόγραμμα αποθηκεύει τις ρυθμίσεις.

Έχουμε συνδεδεμένο στον υπολογιστή το USB Token μας. Έπειτα κάνουμε κλικ στο κουμπί Φόρτωση πιστοποιητικών και αριστερά φαίνεται το Ψηφιακό μας Πιστοποιητικό:

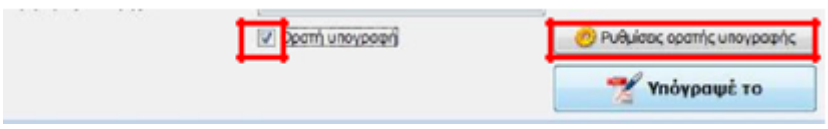


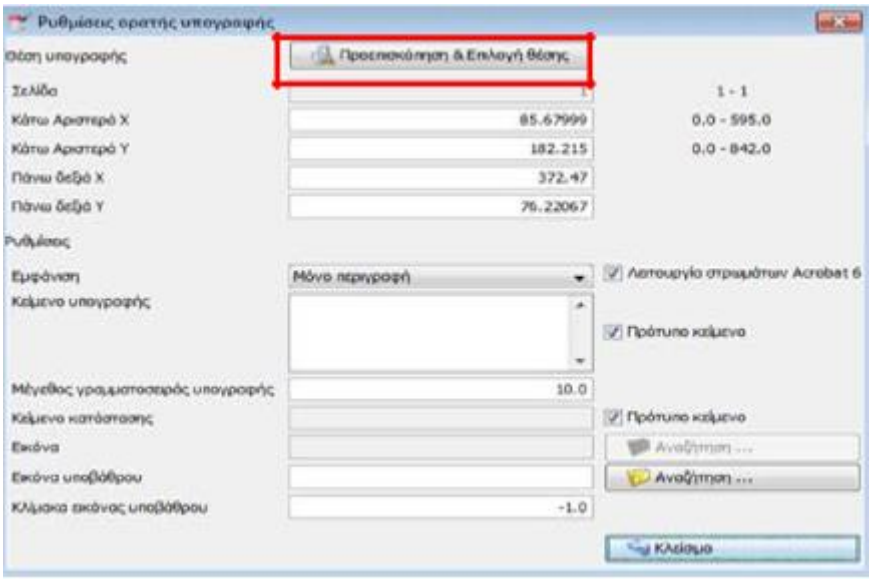
Κάνουμε κλικ στο πρώτο κουμπί Αναζήτηση για να επιλέξουμε το PDF αρχείο προς υπογραφή:



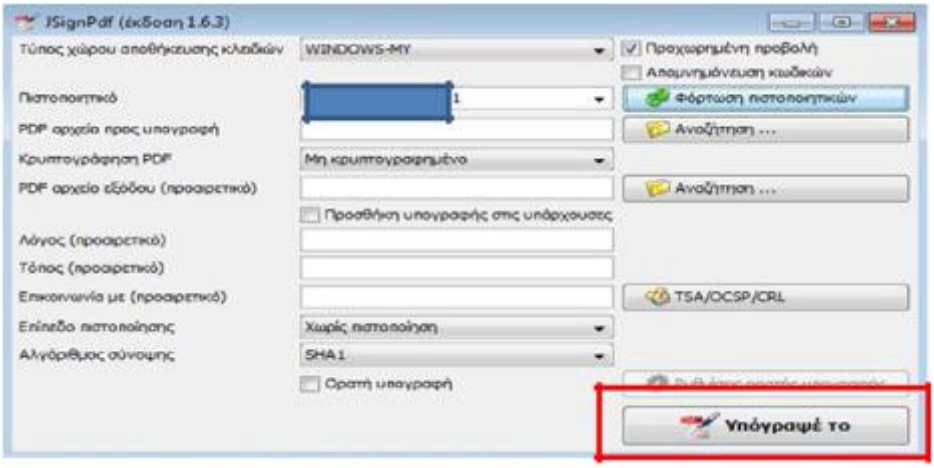


Για να προσθέσουμε Ορατή Υπογραφή, επιλέγουμε Ορατή υπογραφή, κάνουμε κλικ στο κουμπί Ρυθμίσεις ορατής υπογραφής, επιλέγουμε Προεπισκόπηση & Επιλογή θέσης όπου εμφανίζετε το έγγραφο στο οποίο (με το αριστερό κλικ από το ποντίκι μας) επιλέγουμε το ΠΟΥ θα τοποθετηθεί η υπογραφή μας και κάνουμε κλικ στο κουμπί Κλείσιμο (2 φορές):

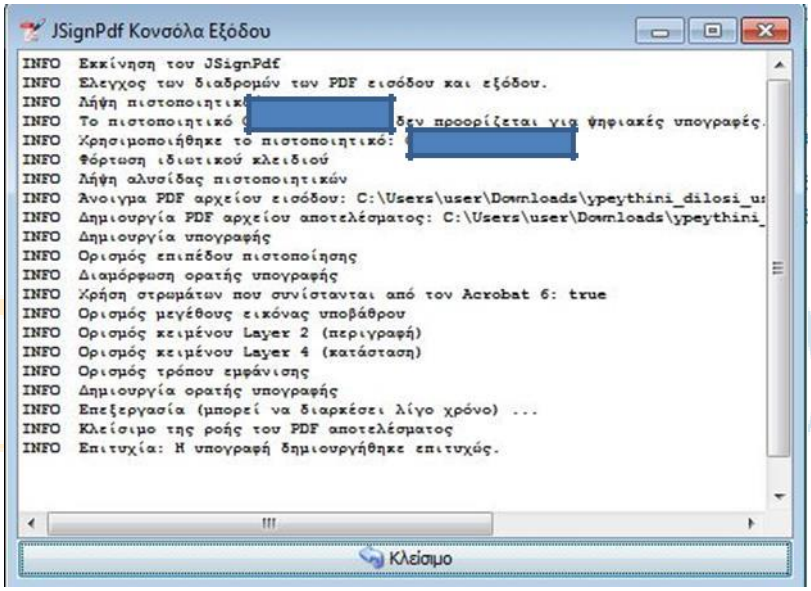




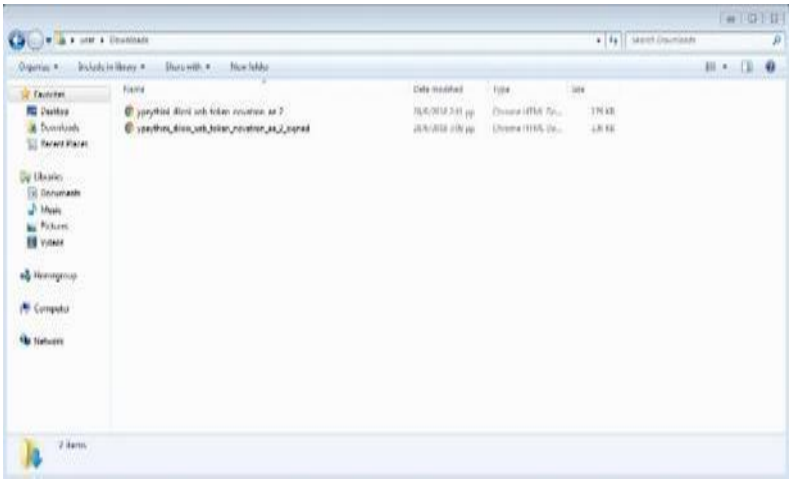
Κάνουμε κλικ στο κουμπί Υπέγραψε το και αυτόματα μας ζητάει το PIN που για το συγκεκριμένο Token είναι 4 φορές το 9 (9999), το εισάγουμε και πατάμε Ok.



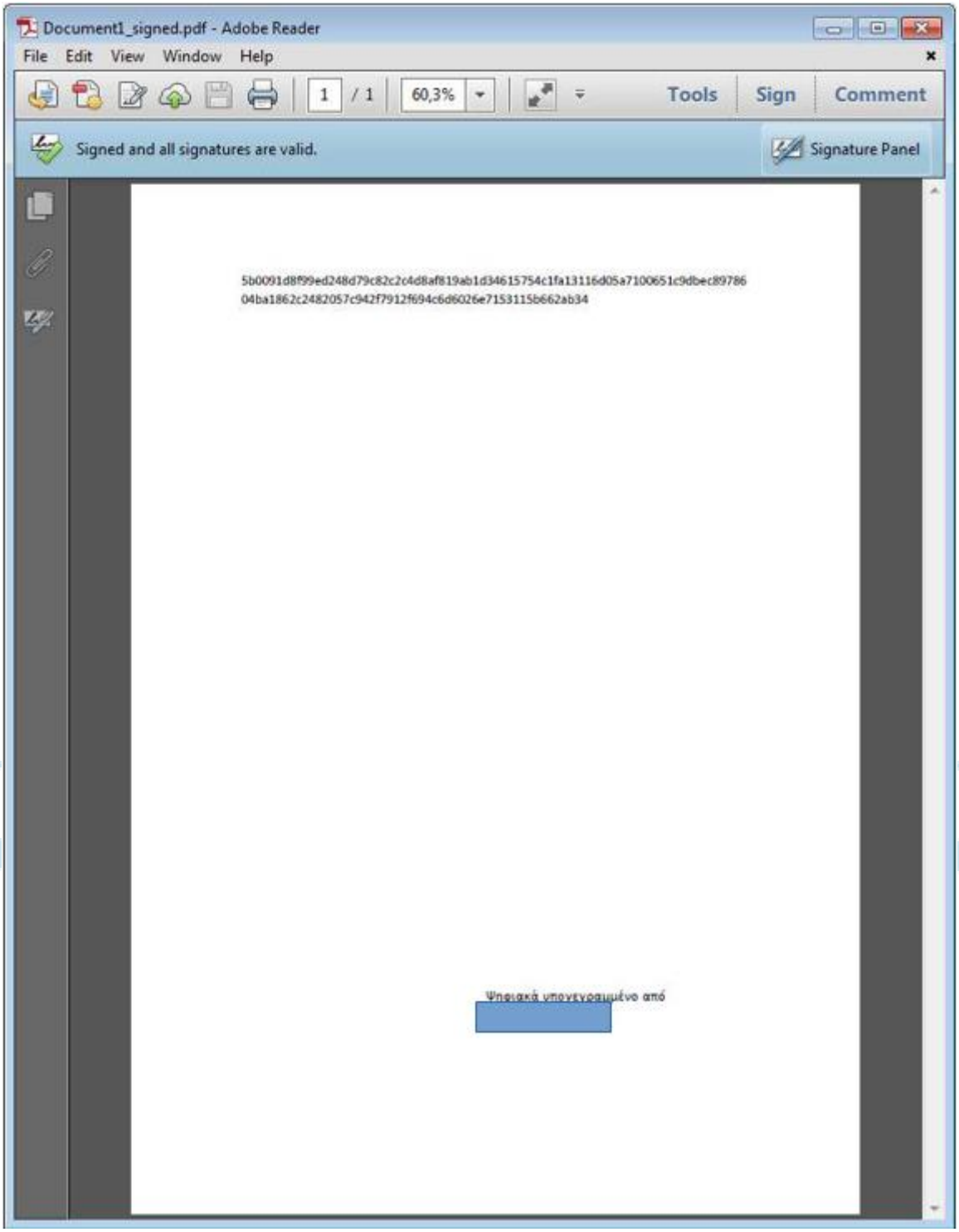
Στην συνέχεια μας δείχνει την πορεία της διαδικασίας βγάζοντας μας το αποτέλεσμα:



Δημιουργείται το Ψηφιακά Υπογεγραμμένο έγγραφο στον ίδιο φάκελο που βρισκόταν το αρχικό αλλά με την κατάληξη _signed.



Έχουμε ολοκληρώσει επιτυχώς την Ψηφιακή Υπογραφή του εγγράφου μας. Βλέπουμε τη σήμανση Signed and all signatures are valid. Με τον τρόπο αυτό μπορούμε να βεβαιωθούμε ότι η υπογραφή είναι έγκυρη και δεν έχει γίνει επεξεργασία του εγγράφου μετά την υπογραφή (για να δούμε περισσότερες πληροφορίες κάνουμε κλικ πάνω στην υπογραφή, επιλέγουμε Signature properties, ελέγχουμε όλες τις πληροφορίες που εμφανίζονται ώστε να είναι έγκυρες και να έχει γίνει η επικύρωσή τους).



Διαδικασία Ψηφιακής Υπογραφής .dxf αρχείων.

Στον συγκεκριμένο οδηγό θα μελετήσουμε τη διαδικασία Ψηφιακής Υπογραφής .dxf αρχείων. Έχοντας εξοικειωθεί με την υπογραφή των Pdf αρχείων μας με τη χρήση εξειδικευμένων προγραμμάτων όπως το JsignPdf, τίθεται το ερώτημα: Με ποιον τρόπο υπογράφουμε σχέδια και διαγράμματα;

Προκειμένου να γίνεται αποδεκτό ένα Τοπογραφικό Διάγραμμα πρέπει αυτό να είναι ψηφιακά υπογεγραμμένο. Για κάθε αρχείο (dxf στην περίπτωση που εξετάζουμε) υπάρχει ένας μοναδικός κωδικός που σχετίζεται με το αρχείο αυτό και μπορεί να ανακτηθεί σε κάθε περίπτωση. Ο κωδικός αυτός είναι το αναφερόμενο ως hash code του αρχείου (με την χρήση του αλγορίθμου SHA512).

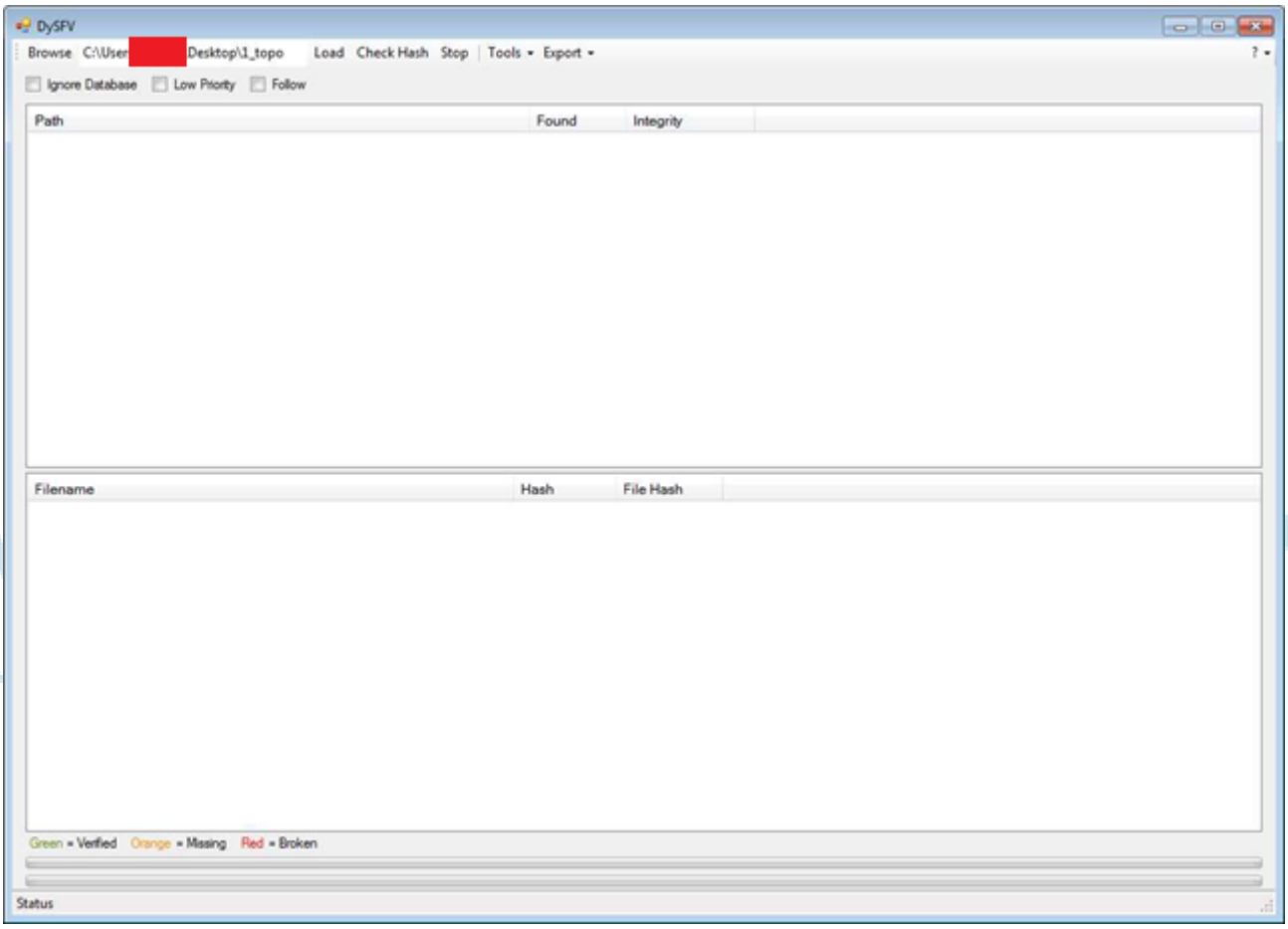
Συνεπώς πρέπει να βρούμε το hash code του αρχείου μας και να το επικολλήσουμε σε ένα αρχείο Word. Στη συνέχεια μετατρέπουμε το Word σε Pdf, υπογράφουμε ψηφιακά το Pdf. Ομαδοποιούμε το dxf και το Pdf σε ένα zip αρχείο. Αυτό το αρχείο υποβάλλουμε.

Αναλυτικά:

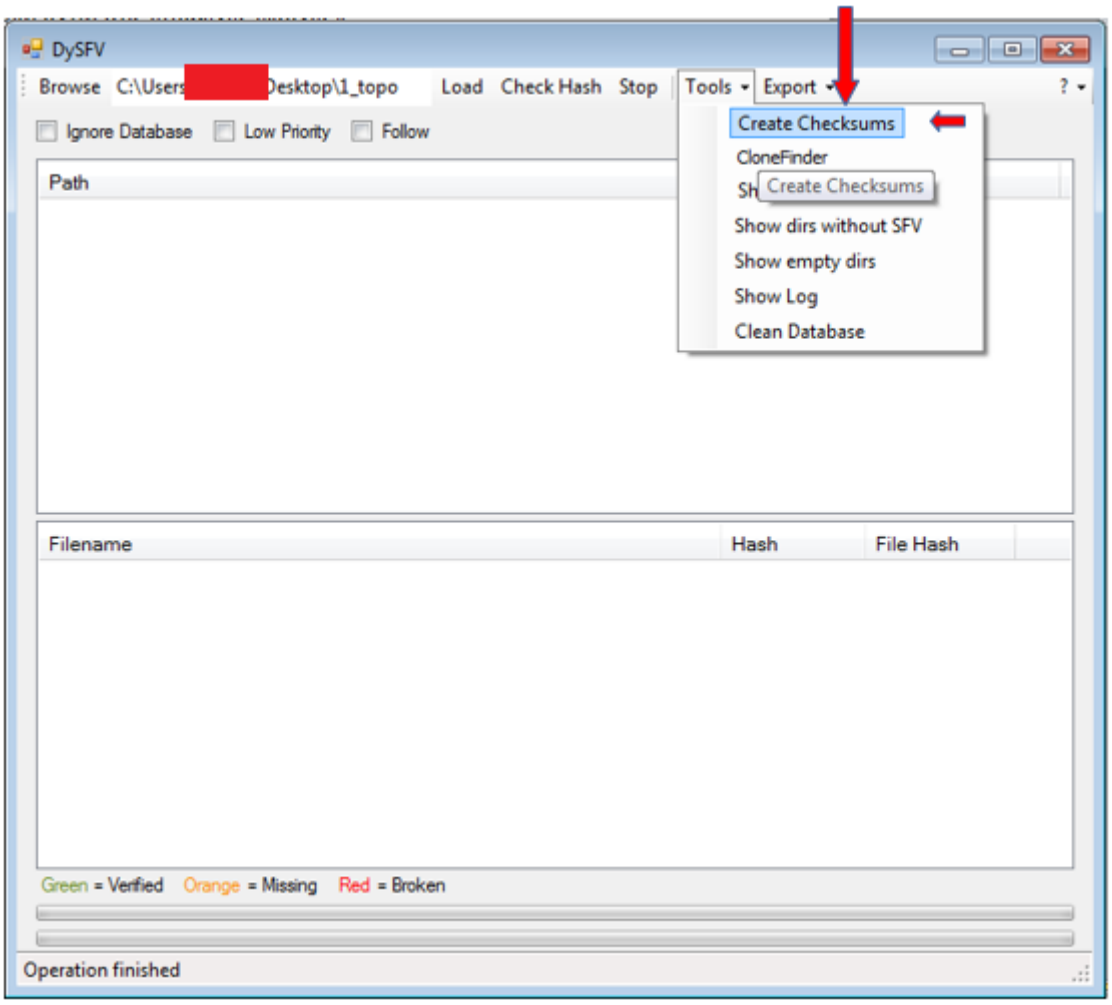
Για την εύρεση του hash code ενός αρχείου είναι δυνατόν να χρησιμοποιηθεί ελεύθερο λογισμικό, το DYSfv, μπορούμε να το κατεβάσουμε από εδώ:

https://sourceforge.net/projects/dysfv/

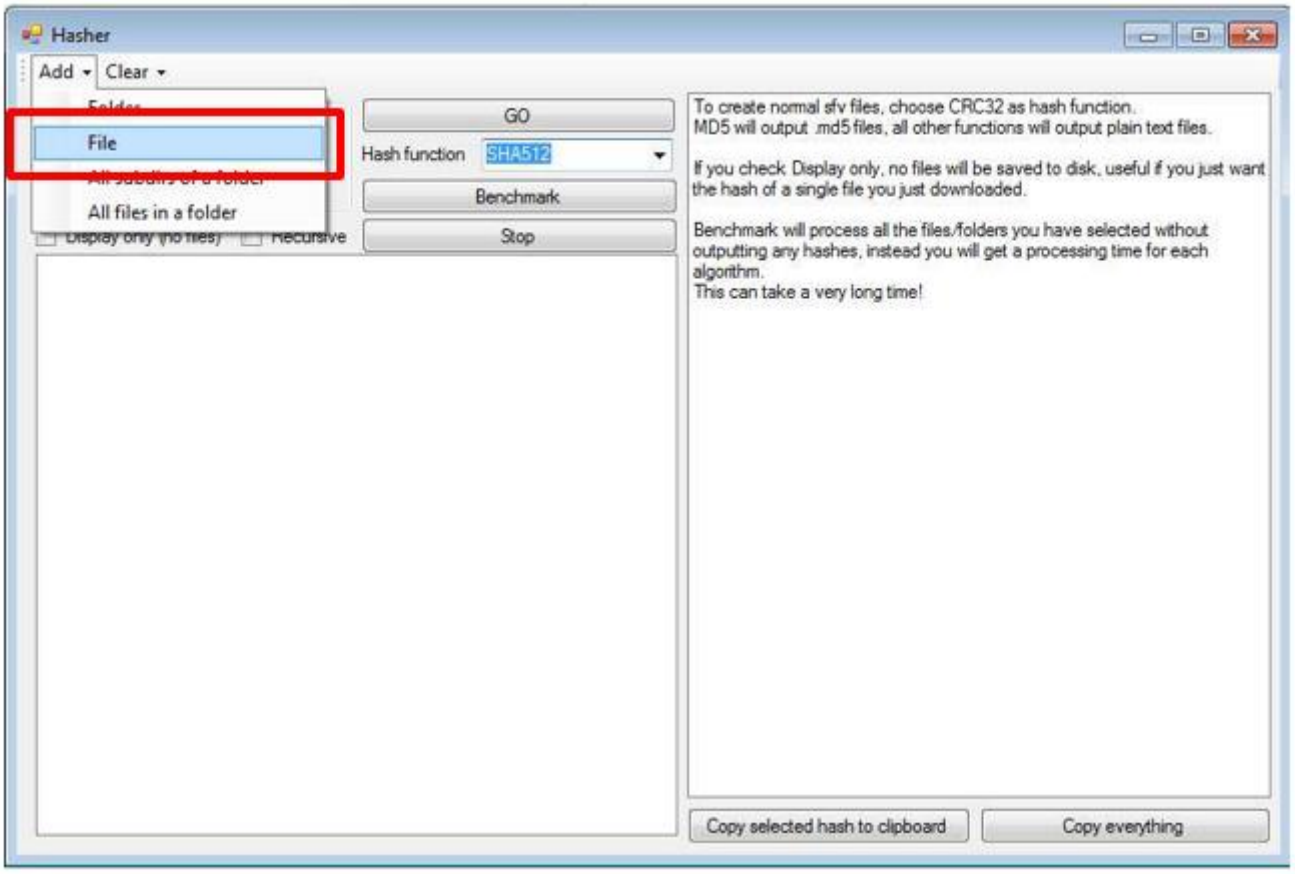
Εγκαθιστούμε, τρέχουμε το πρόγραμμα:



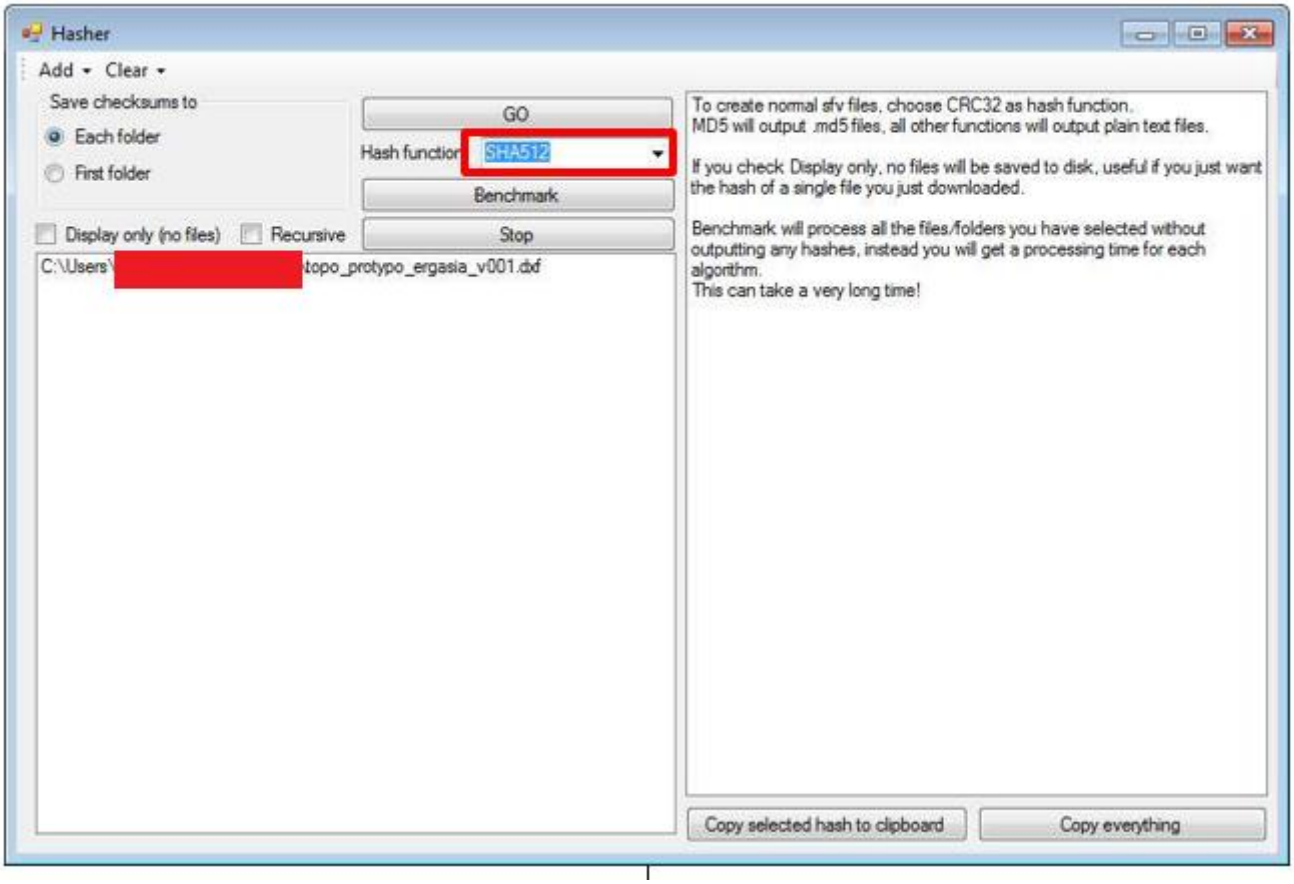
Επιλέγουμε Tools και στη συνέχεια Create Checksums:



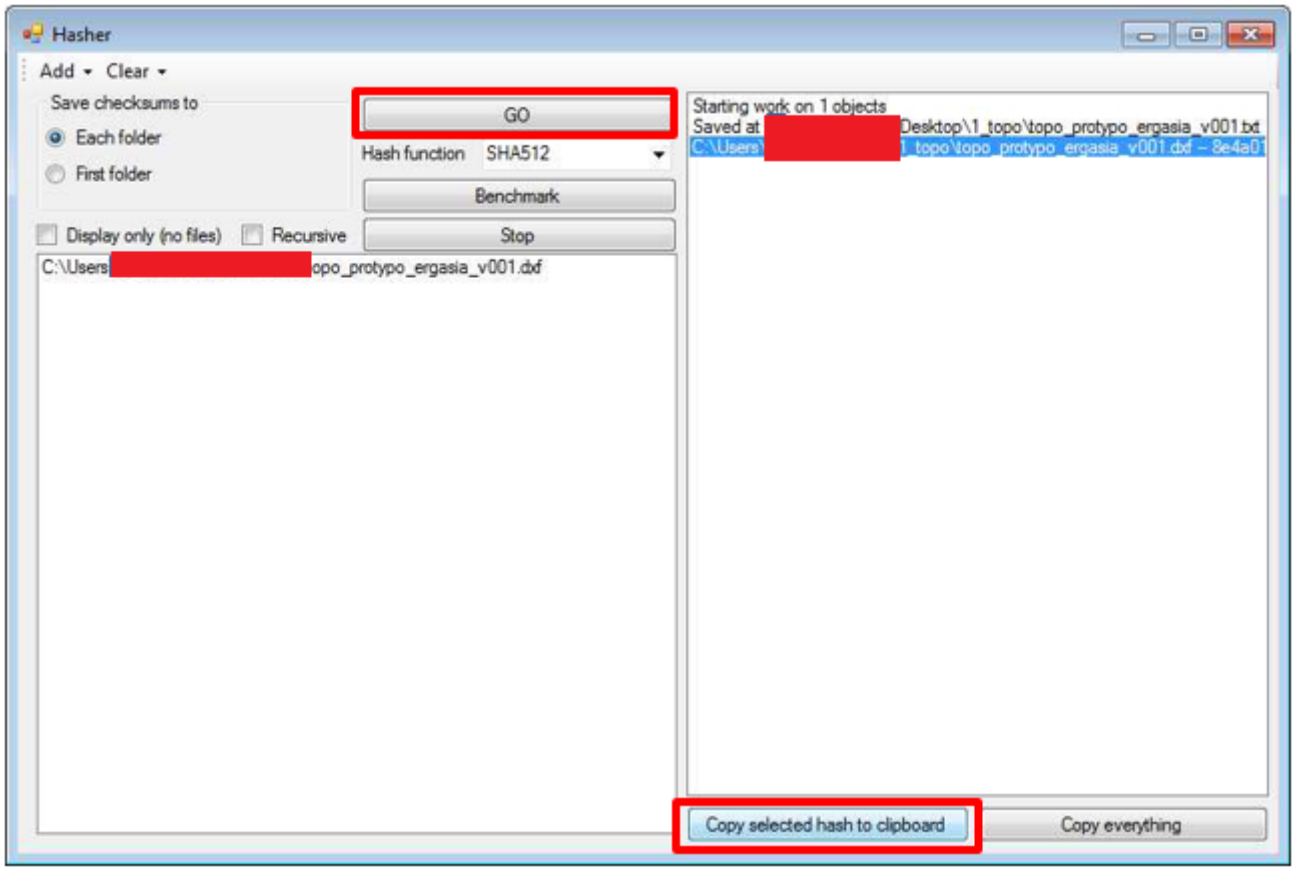
Επιλέγουμε από τον υπολογιστή μας το αρχείο dxf που μας ενδιαφέρει:



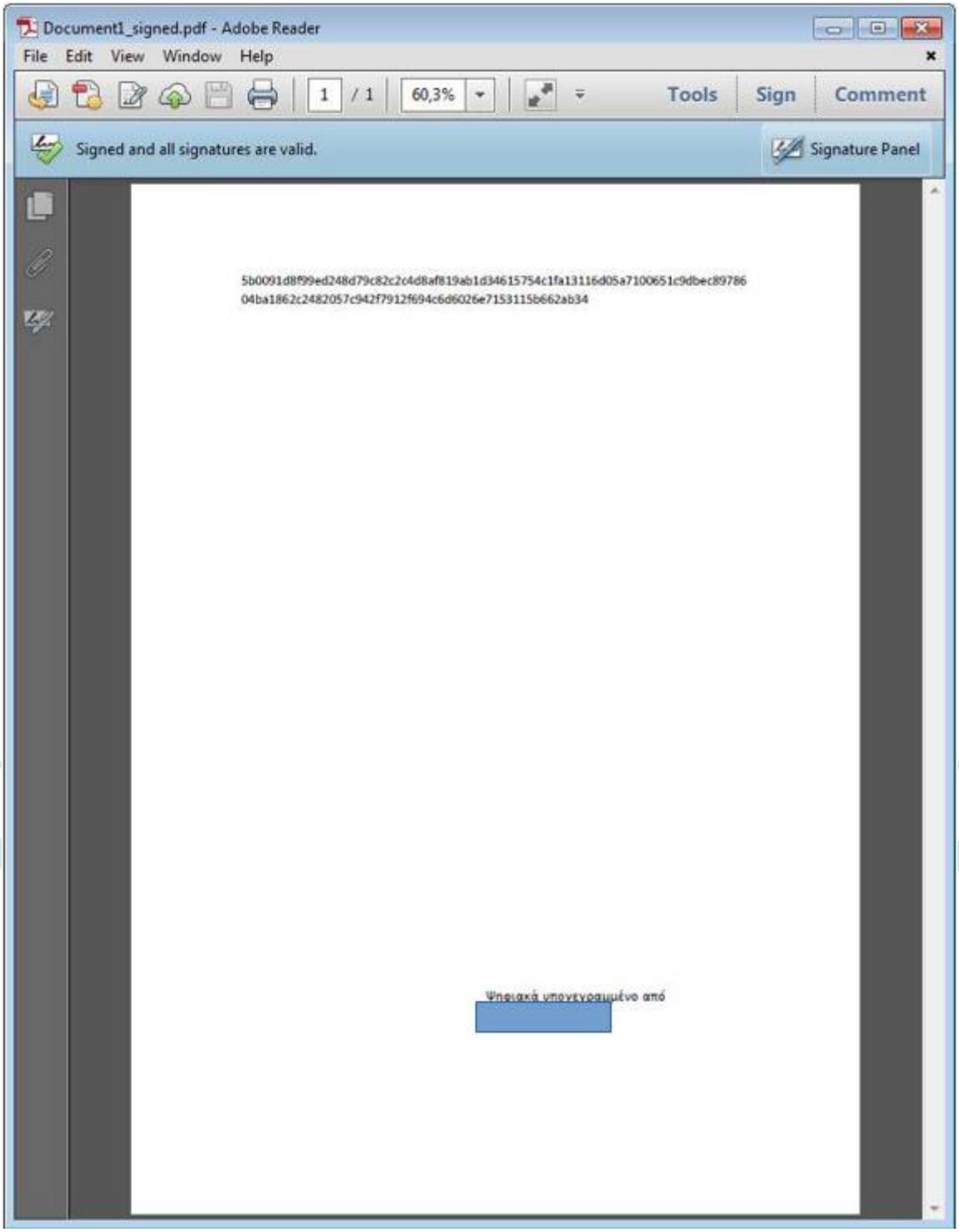
Επιλέγουμε τον αλγόριθμο SHA512:



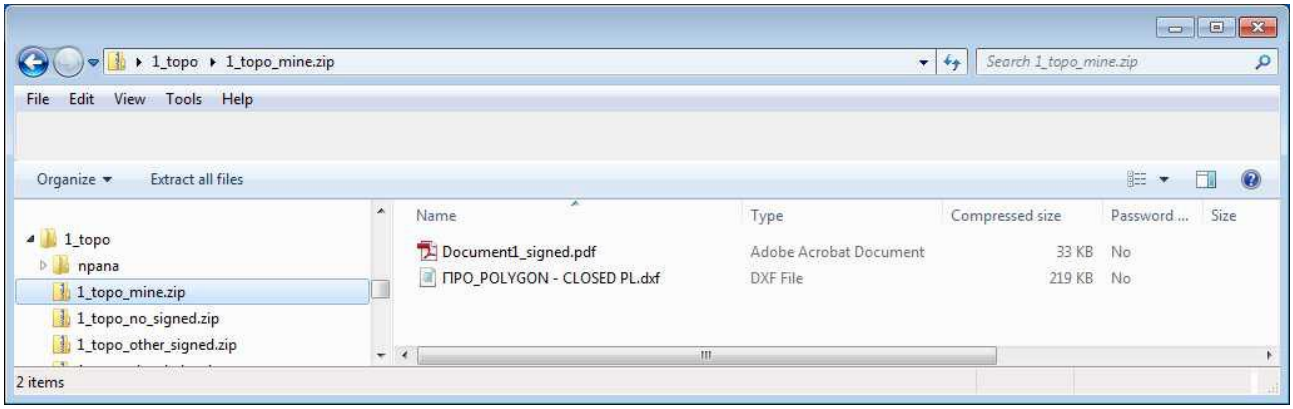
Επιλέγουμε Go και Copy selected hash to Clipboard:



Το hash code του αρχείου είναι διαθέσιμο για επικόλληση σε Word που θα μετατραπεί σε Pdf. Υπογράφουμε ψηφιακά το Pdf:



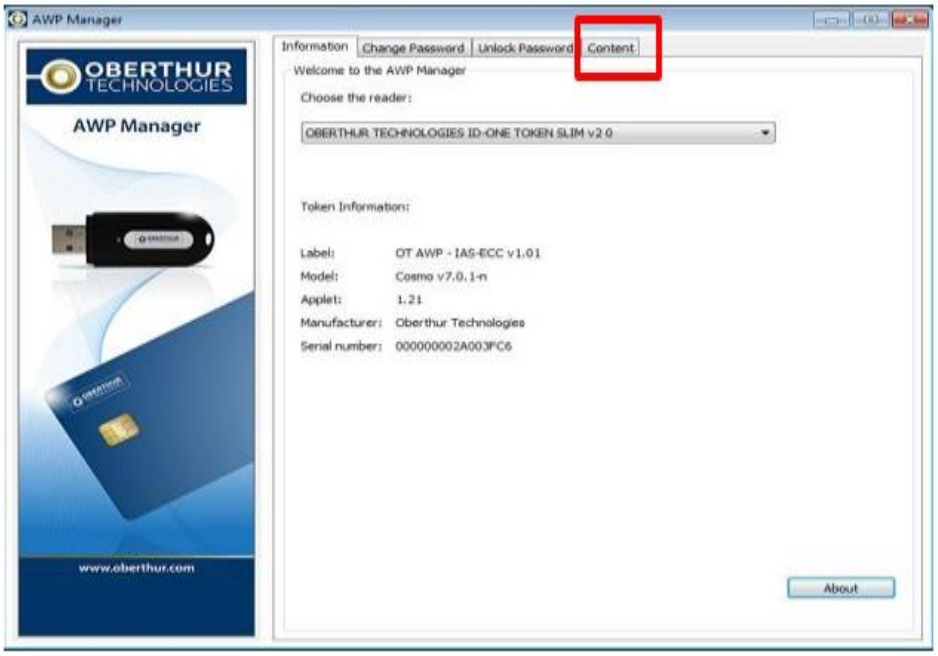
Τέλος, ομαδοποιούμε σε ένα zip αρχείο το dxf και το ψηφιακά υπογεγραμμένο pdf. Υποβάλλουμε το zip αρχείο:



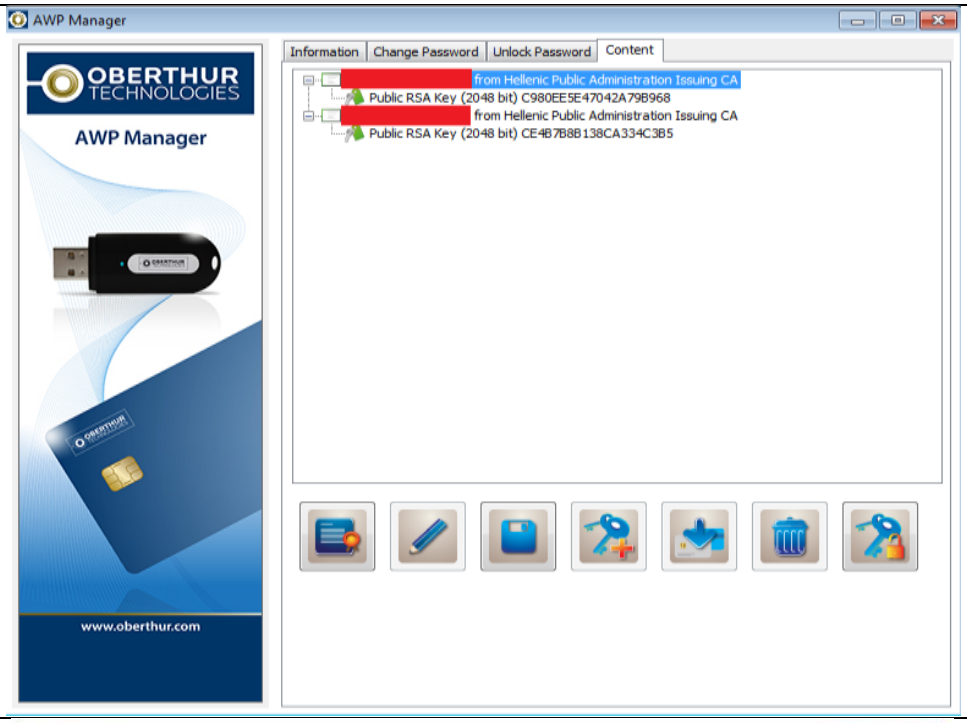
Διαδικασία υποβολής Ψηφιακού Πιστοποιητικού στο ΤΕΕ

Στον συγκεκριμένο οδηγό θα μελετήσουμε τη διαδικασία υποβολής του προσωπικού μας Ψηφιακού πιστοποιητικού στο ΤΕΕ, προκειμένου να γίνονται αποδεκτά τα Τοπογραφικά μας Διαγράμματα από τον υποδοχέα του Ελληνικού Κτηματολογίου. Η διαδικασία γίνεται μία φορά, επαναλαμβάνεται μόνο εάν ανακαλέσουμε ή λήξει το Ψηφιακό μας Πιστοποιητικό και εκδώσουμε νέο.

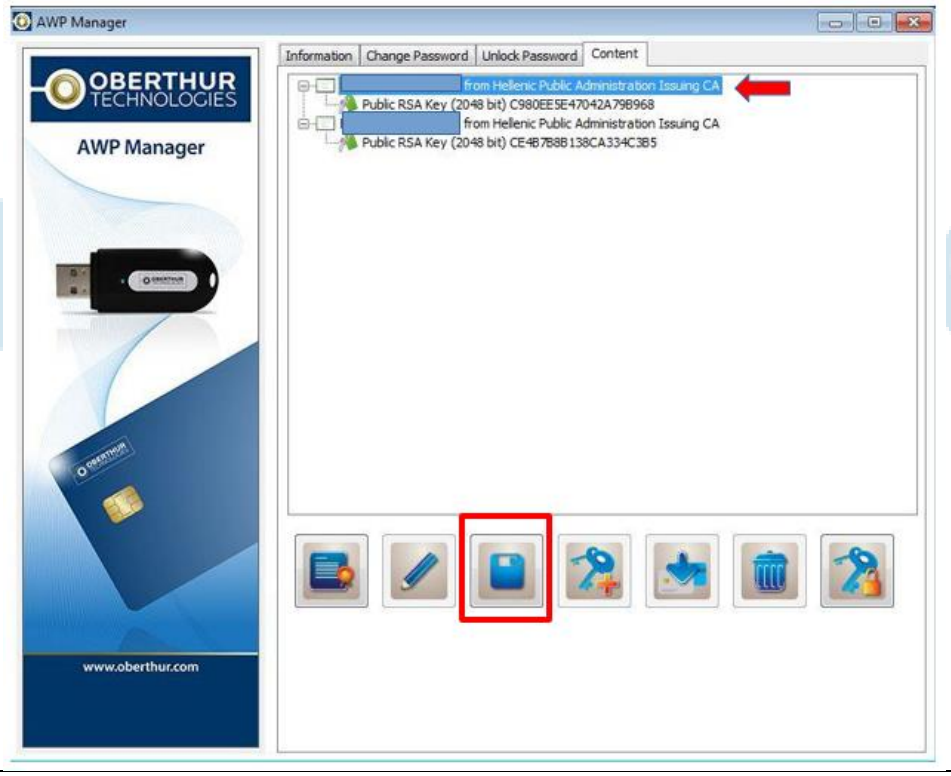
Βήμα 1ο: Εξαγωγή Ψηφιακού Πιστοποιητικού από το USB Token και αποθήκευση στον υπολογιστή μας.



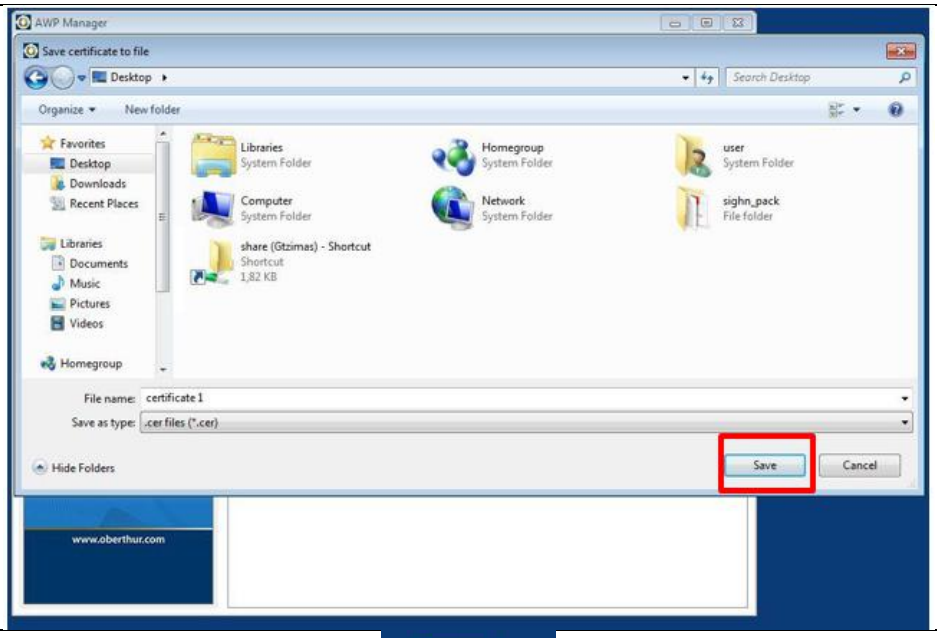
Ανοίγουμε το πρόγραμμα διαχείρισης AWP Manager και επιλέγουμε την καρτέλα Content:



Στην οθόνη αυτή φαίνονται τα δύο αρχεία του Πιστοποιητικού μας.



Κάνουμε κλικ στο πρώτο αρχείο και στη συνέχεια στη δισκέτα.

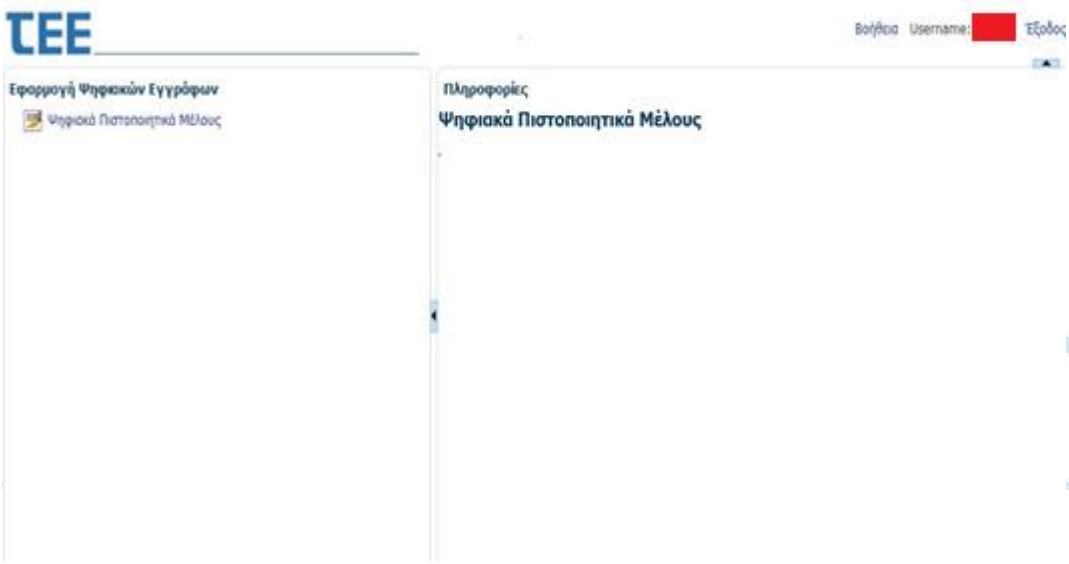
	Ανοίγει το παράθυρο όπου γράφουμε το όνομα του αρχείου και ορίζουμε την ονομασία του και το πού θα αποθηκευτεί πατώντας Save.
	Έχουμε αποθηκεύσει το πρώτο αρχείο (.cer) του Ψηφιακού μας Πιστοποιητικού στην επιφάνεια εργασίας του υπολογιστή μας.
	Την ίδια διαδικασία ακολουθούμε και για το δεύτερο αρχείο (.cer) του Ψηφιακού μας Πιστοποιητικού.
	

Βήμα 2ο: Είσοδος στο ΤΕΕ.

Η υποβολή του Ψηφιακού Πιστοποιητικού γίνεται με την χρήση των ίδιων κωδικών που έχει ο Μηχανικός στο ΤΕΕ για όλες τις παρεχόμενες ηλεκτρονικές υπηρεσίες μέσα από την παρακάτω ιστοσελίδα:

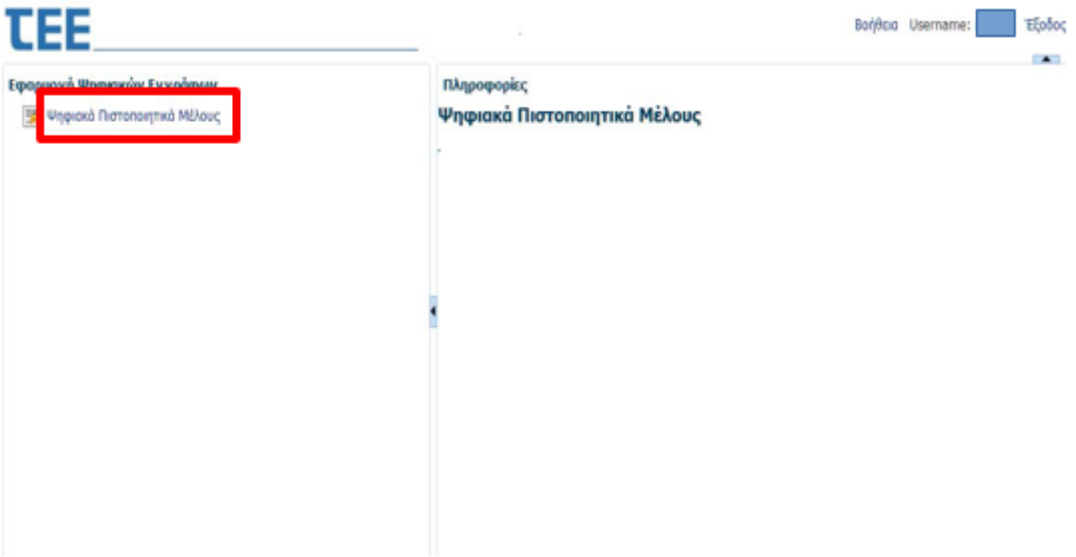
https://apps.tee.gr/eteedoc/faces/appMainCert

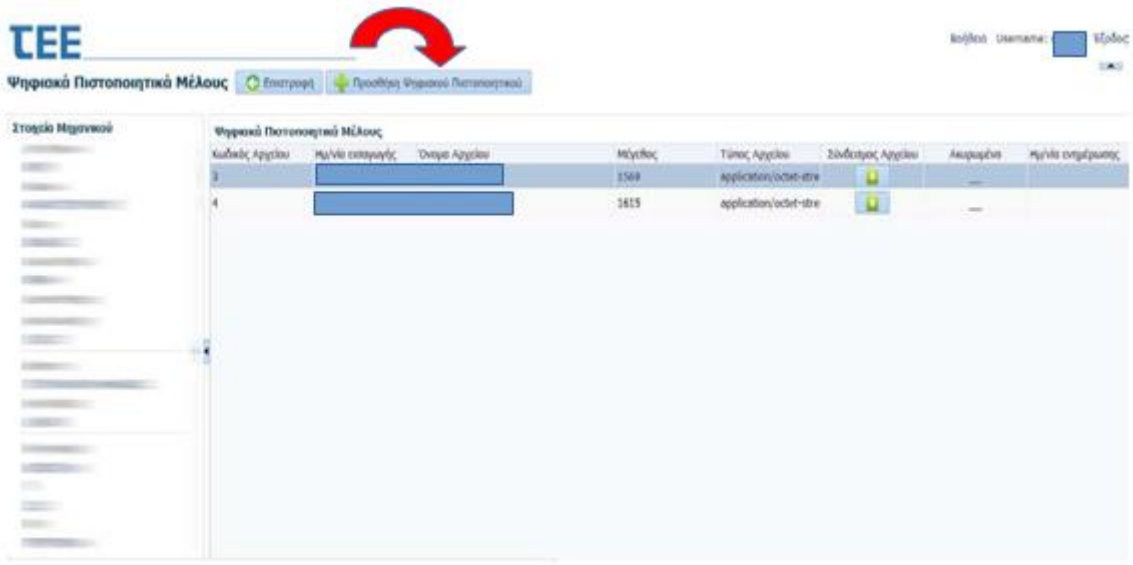
Μετά την επιτυχημένη εισαγωγή των κωδικών πρόσβασης γίνεται είσοδος στην εφαρμογή:



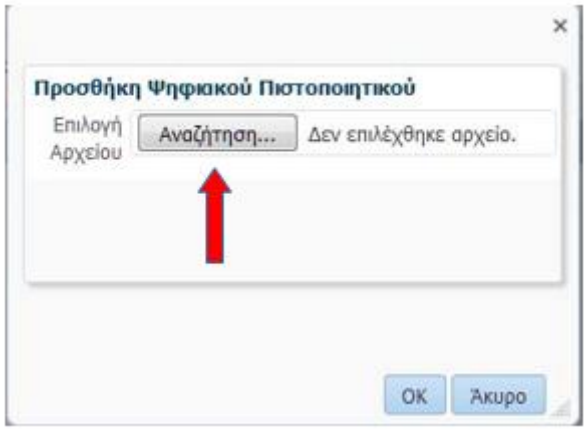
Βήμα 3ο: Εισαγωγή Ψηφιακού Πιστοποιητικού.

Με την επιλογή Ψηφιακά Πιστοποιητικά Μέλους γίνεται η εισαγωγή στην ατομική σελίδα διαχείρισης των ψηφιακών πιστοποιητικών:





Με την επιλογή Προσθήκη Ψηφιακού Πιστοποιητικού γίνεται η εισαγωγή ενός νέου πιστοποιητικού (για την τήρηση ιστορικού δεν επιτρέπεται η διαγραφή πιστοποιητικού):



Πατάμε Αναζήτηση και επιλέγουμε ένα, ένα τα αρχεία του Ψηφιακού Πιστοποιητικού από την επιφάνεια εργασίας:

Μετά την επιλογή των αρχείων (της μορφής *.cer) αυτά εισάγονται στο ΤΕΕ. Έχουμε ολοκληρώσει επιτυχώς τη διαδικασία υποβολής του Ψηφιακού μας Πιστοποιητικού.