NOVATRON®

Διαχείριση και Εγκατάσταση
Ψηφιακής Υπογραφής και Ψηφιακών Πιστοποιητικών
με τη χρήση του Gemalto Id Prime 840 USB Token

Περιεχόμενα

Τεχνικά χαρακτηριστικά.

ID Bridge K30.

Operating systems supported	• Windows 7, Windows 8, Windows 10 (32, 64 bit versions) • Win CE 4.1, 4.2, 5.0, 6.0 • Linux Kernel 2.6 and higher • Mac OS X Panther, Tiger, Leopard 32 editions
APIs	Microsoft PC/SC environment with associated drivers
Host interface	• Plug and Play • CCID (Chip Card Interface Device) • USB 2.0 full speed (12 Mbps)
Human interface	• LED one color (Blue), dual state (blinking: waiting card insertion; ON: card reading / writing)
Environmental	• CE, FCC part 15 Class B • EN 60950 / UL 950 / CSA 950 • Operating: +0°C / +70°C • Storage: -20°C / +85°C • ROHS compliant , WEEE marking
Electrostatic Discharge	• +/- 8kV direct air discharge • +/- 4kV indirect contact discharge

ID Prime 840 smart card (eIDAS Compliant)

Product characteristics	
Memory	• 80KB total, including 50KB available for data, certificates and additional applets. IDPrime MD memory allows the storage of up to 15 RSA or Elliptic curve key containers (depending on the card profile)
Standards	• BaseCSP Minidriver v7 (IDGo 800 Minidriver) • CSP and PKCS#11 (SafeNet Authentication Client)
Cryptographic algorithms	• Hash: SHA-1, SHA-256, SHA-384, SHA-512. • RSA: up to RSA 2048 bits (and optionally up to 4096 bits) • RSA OAEP & RSA PSS • Elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH • On-card asymmetric key pair generation (RSA up to RSA2048 & Elliptic curves) • Symmetric: 3DES (ECB, CBC), AES – For secure messaging and Microsoft Challenge/Response only
Communication protocols	• T=0, T=1, PPS, with baud up to 230 Kbps
Other features	• Onboard PIN Policy • Multi-PIN support
Chip characteristics	
Technology	• Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	• Minimum 500,000 write/erase cycles • Data retention for minimum 25 years
Certification	• CC EAL5+
Security	• The IDPrime MD smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The IDPrime MD 840 is both CC EAL5+ / PP Java Card certified for the java platform and CC EAL5+ / • PP QSCD certified for the combination of java platform plus PKI applet

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 Password: 0000 (μετά από 5 ανεπιτυχείς προσπάθειες κλειδώνει).

Admin Password: Σαράντα οκτώ μηδενικά 000000000000000000000000000000000000000000000000 (μετά από 3 ανεπιτυχείς προσπάθειες κλειδώνει).

Digital Signature PIN: Έξι μηδενικά 000000 (μετά από 3 ανεπιτυχείς προσπάθειες κλειδώνει).

Digital Signature PUK: Έξι μηδενικά 000000 (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 Gemalto Id Prime 840. Αποτελεί μία Πιστοποιημένη Ασφαλής Διάταξη Δημιουργίας Ψηφιακής Υπογραφής (θα μετονομαστούν σε Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής - ΕΔΔΥ). Εξωτερικά μοιάζει με μνήμη USB Flash. Σ' αυτή τη συσκευή αποθηκεύονται τα ψηφιακά πιστοποιητικά μας.

Το Gemalto Id Prime 840 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**.

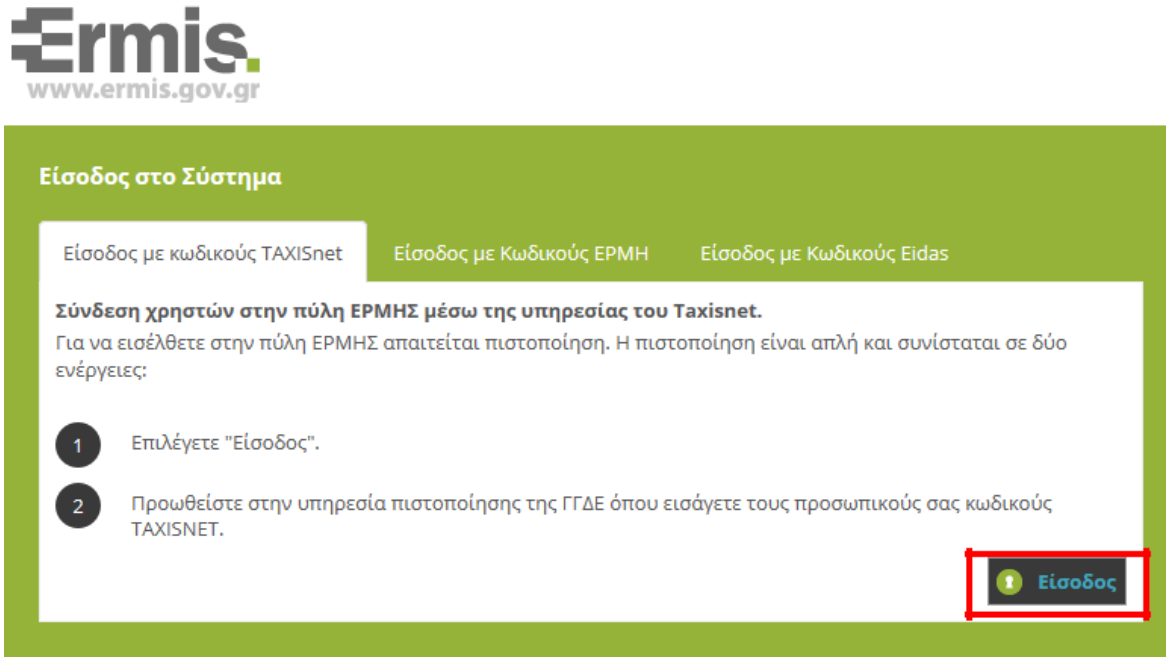
Μπορούμε να το προμηθευτούμε μέσω της ιστοσελίδας www.novatron.gr ή επικοινωνώντας με το τμήμα πωλήσεων της εταιρείας στο τηλέφωνο 210 6180 865.

Βήμα 2ο: Ηλεκτρονική αίτηση μέσω της Πύλης ΕΡΜΗΣ

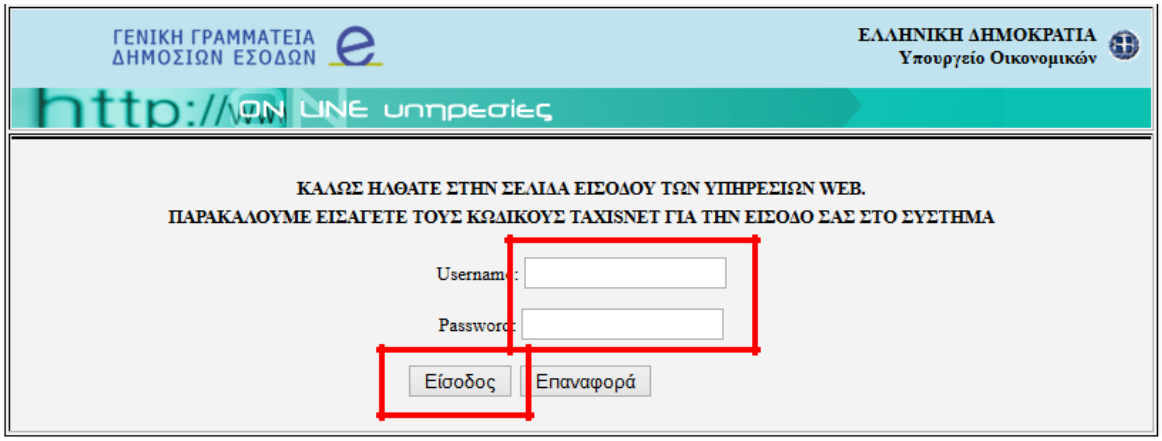
Πληκτρολογούμε τη διεύθυνση www.ermis.gov.gr , κατευθυνόμαστε στη σελίδα όπως αυτή φαίνεται στην παρακάτω εικόνα και επιλέγουμε Σύνδεση.

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.

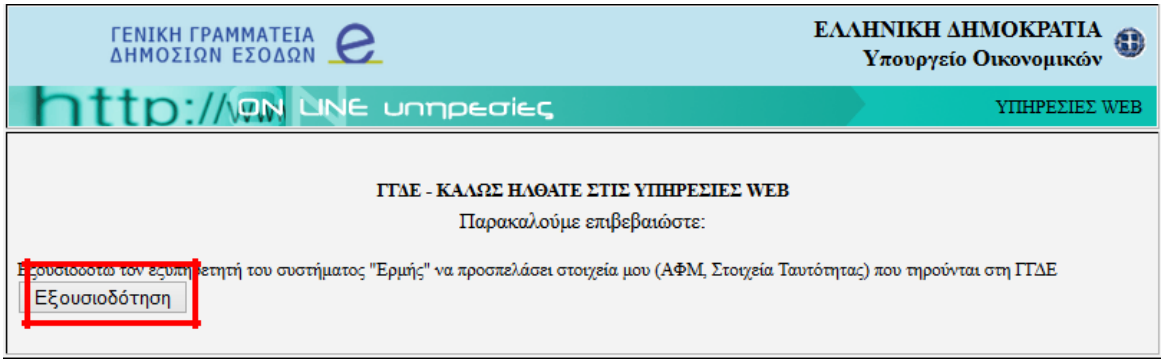
Στη συνέχεια επιλέγουμε το σύνδεσμο Είσοδος.



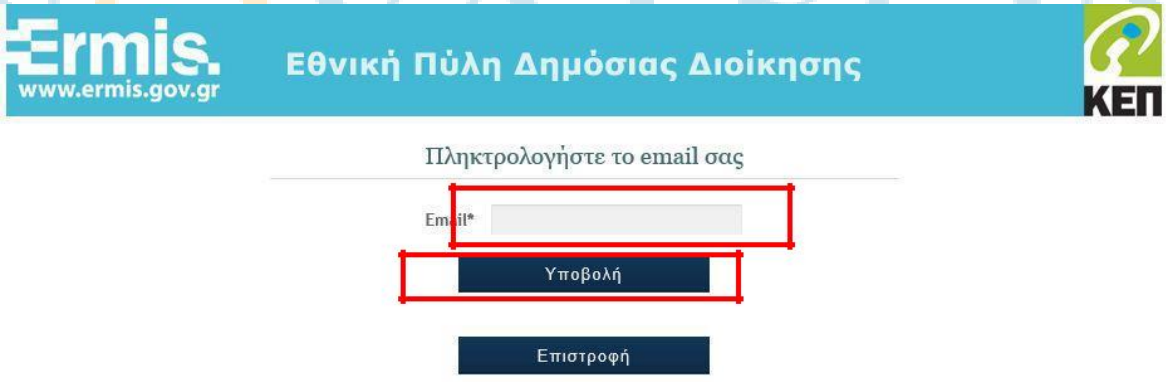
Στη συνέχεια πληκτρολογούμε τους προσωπικούς κωδικούς TAXISnet και επιλέγουμε Είσοδος.



Επιλέγουμε Εξουσιοδότηση, όπως βλέπουμε την παρακάτω εικόνα.

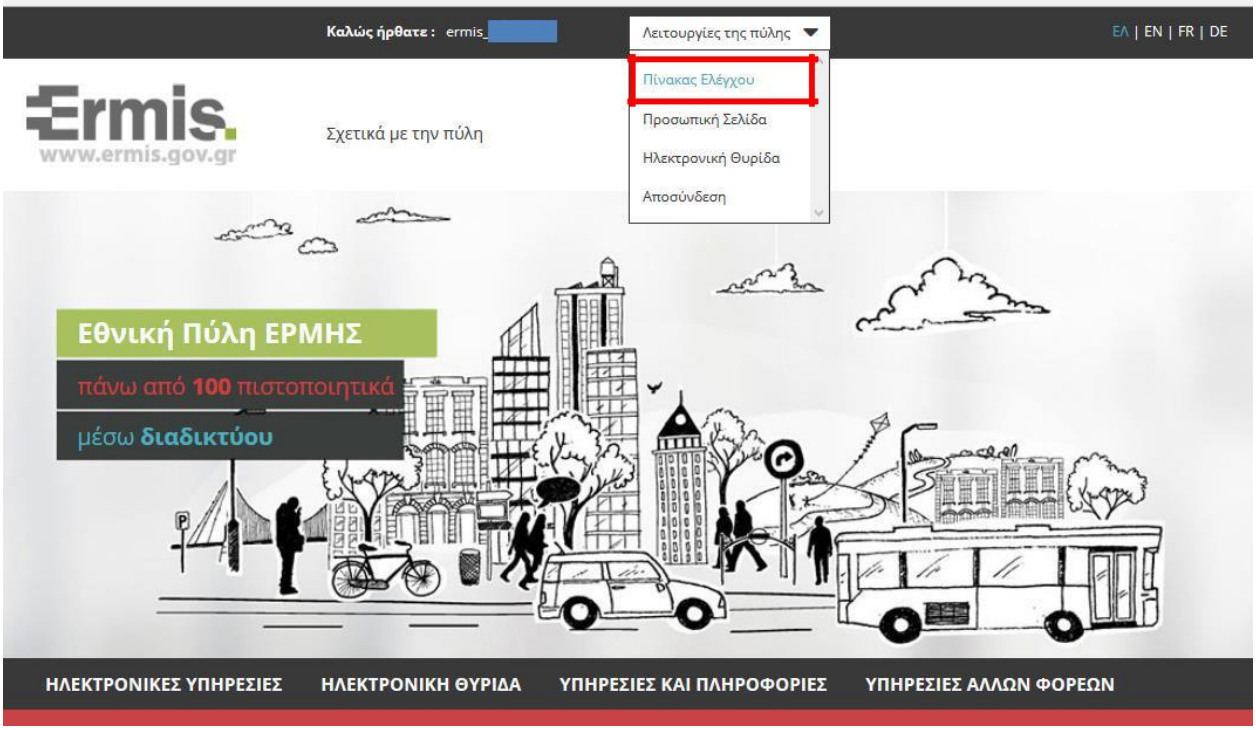


Στην περίπτωση που μπαίνουμε στην Πύλη ΕΡΜΗΣ για πρώτη φορά θα πρέπει να συμπληρώσουμε το προσωπικό/εταιρικό email και να επιλέξουμε Υποβολή.

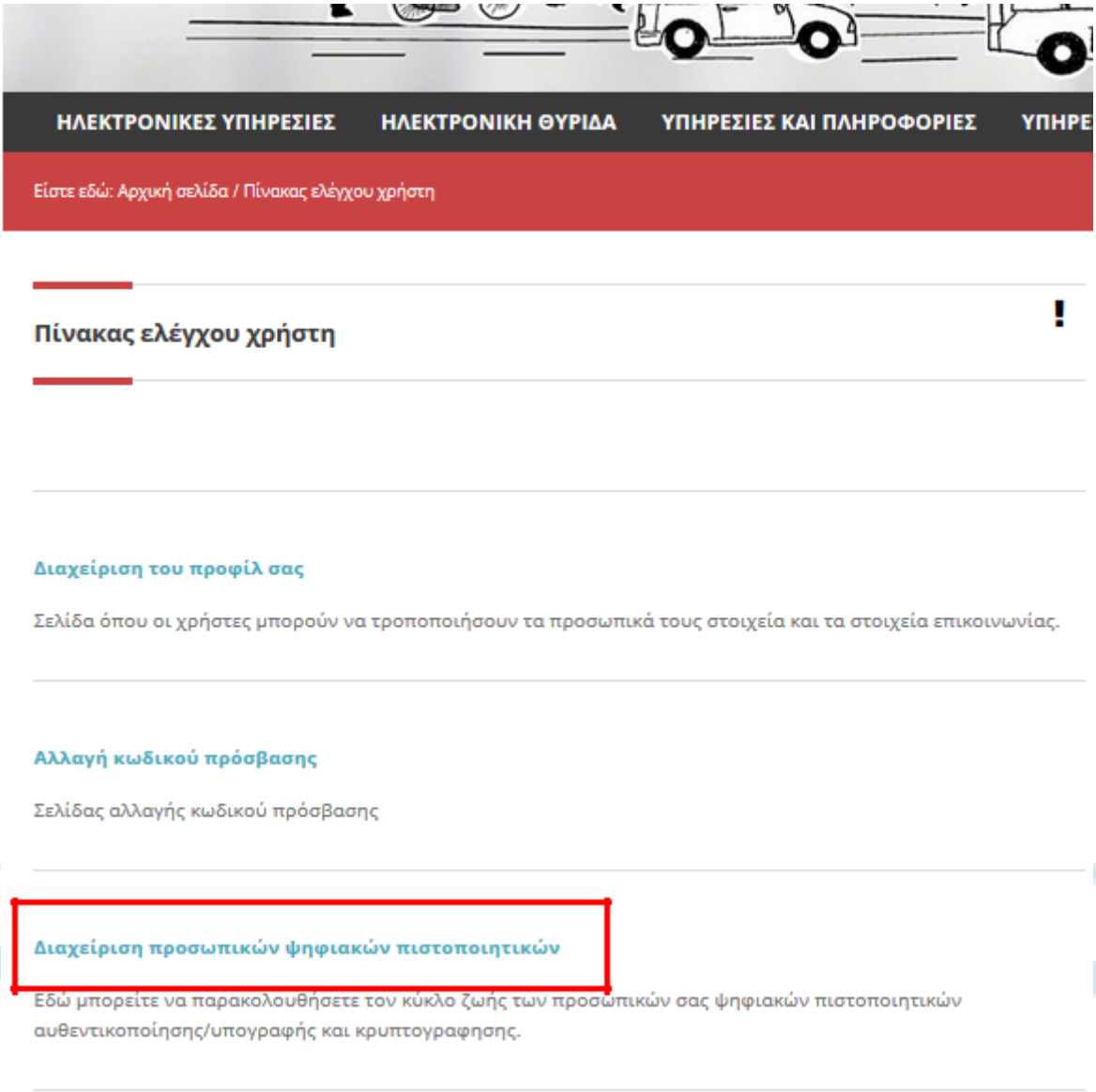


Βρισκόμαστε πλέον στην κεντρική σελίδα της Πύλης ΕΡΜΗΣ.

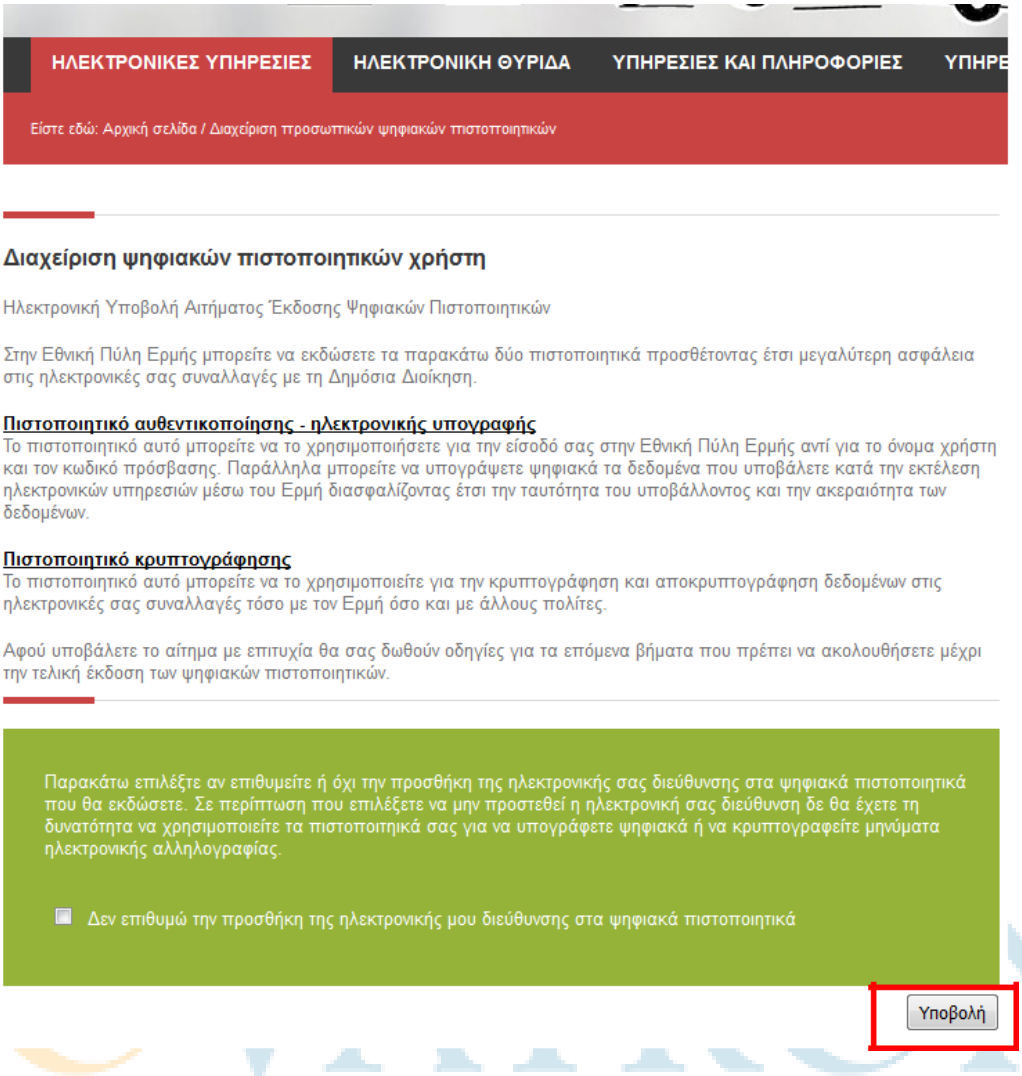
Για να υποβάλουμε αίτημα έκδοσης Ψηφιακού Πιστοποιητικού. Επιλέγουμε το σύνδεσμο Πίνακας Ελέγχου, όπως φαίνεται στην παρακάτω εικόνα.



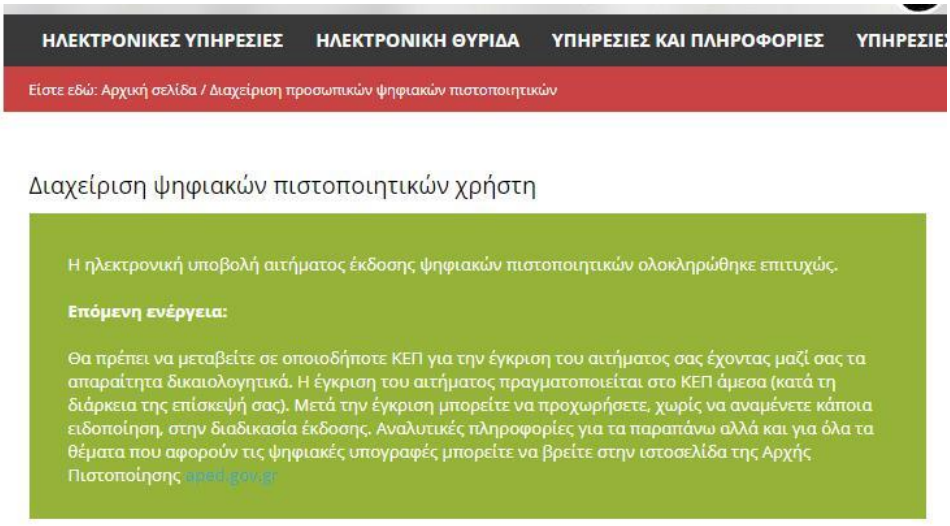
Επιλέγουμε το σύνδεσμο Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών.



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



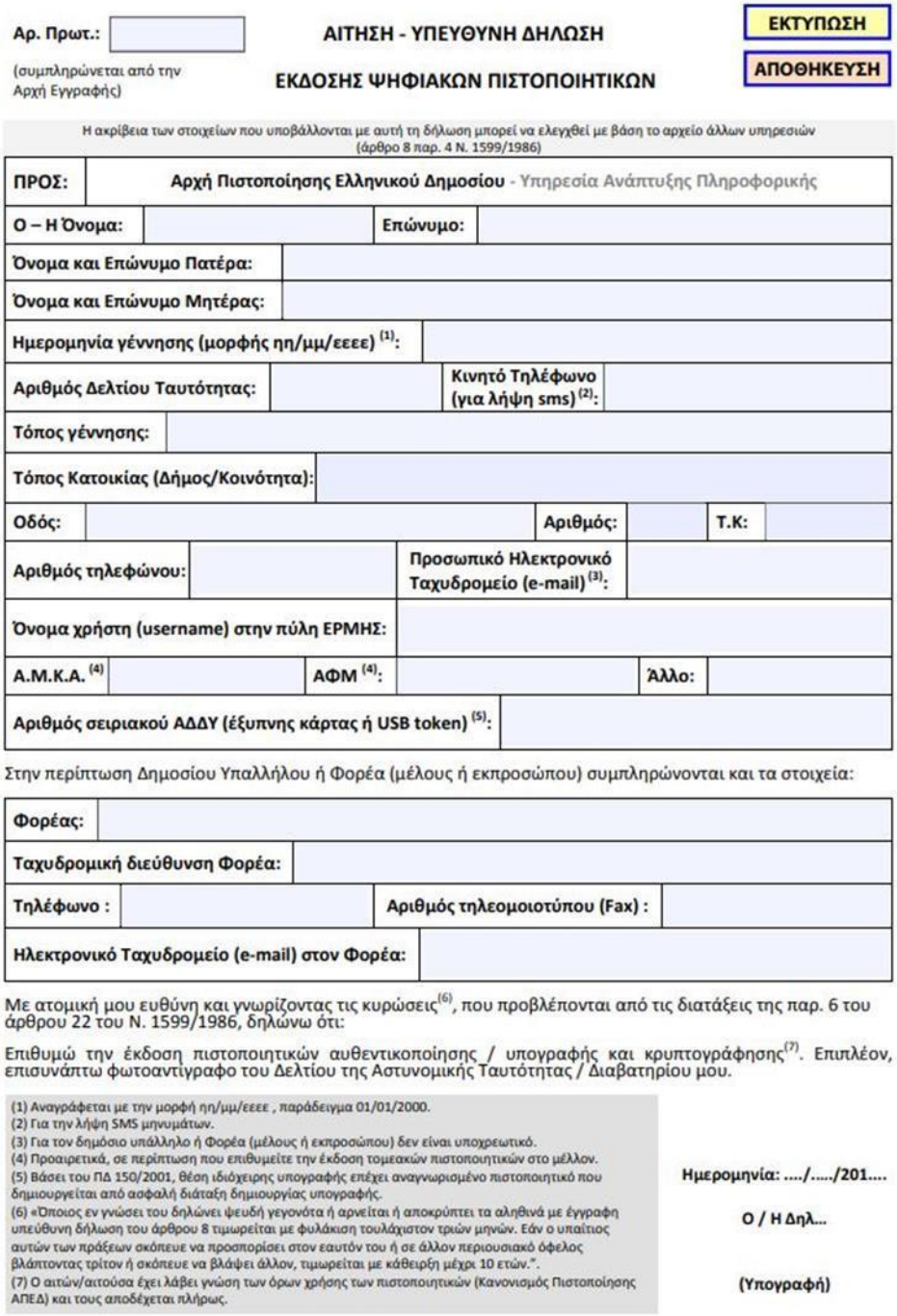
Λαμβάνουμε το παρακάτω μήνυμα.



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.

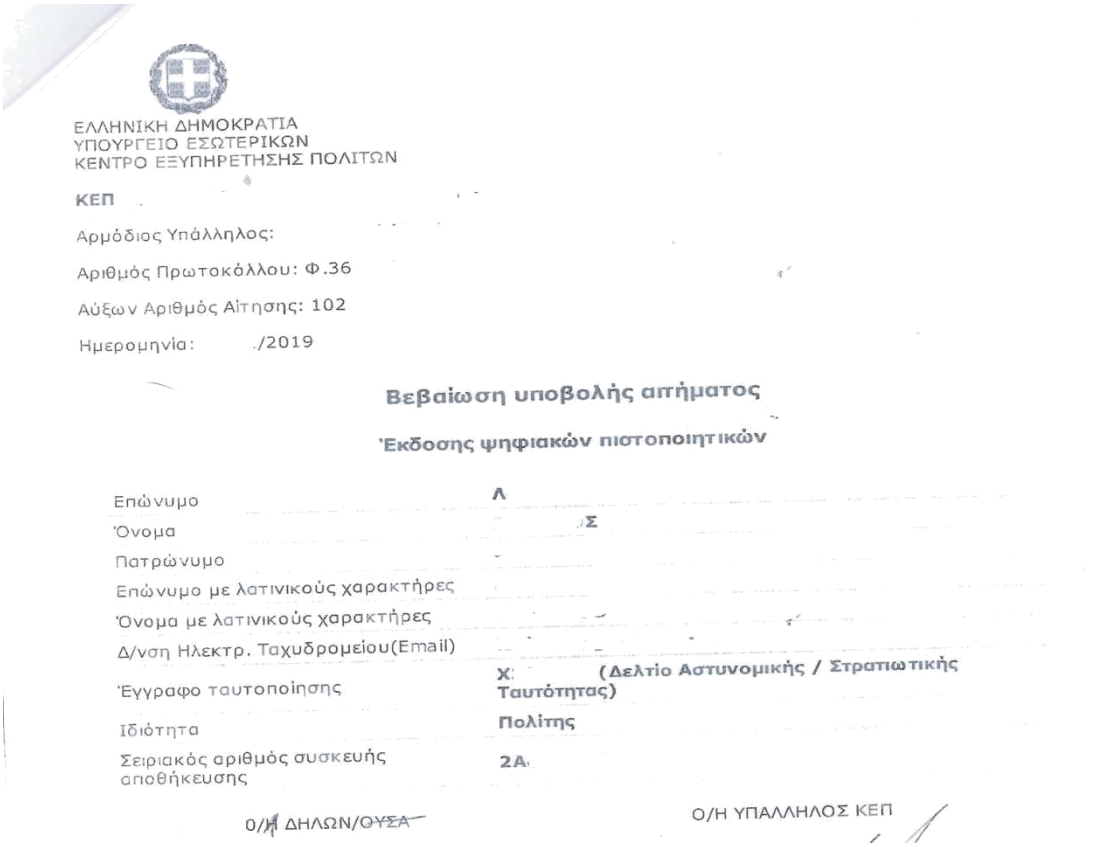
Ημερομηνία: ..../...../201....

Ο / Η Δηλ...

(Υπογραφή)

*****Το 99% των αιτούντων δεν συμπληρώνει αριθμό σειριακού ΑΑΔΥ, αν σας τον ζητήσουν στο ΚΕΠ τον βρίσκετε στην ετικέτα της συσκευασίας**

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

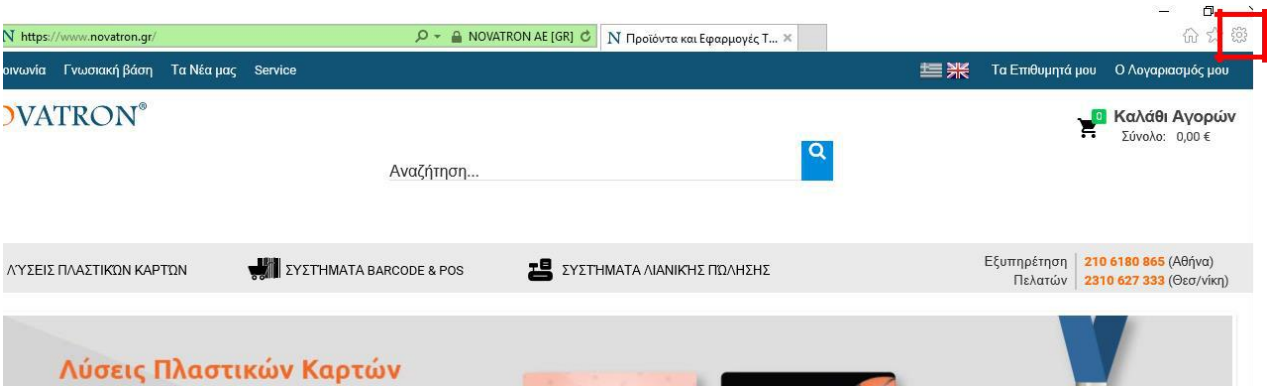
Ο/Η ΥΠΑΛΛΗΛΟΣ ΚΕΠ

Βήμα 4ο: Έλεγχος προδιαγραφών και προετοιμασία υπολογιστή.

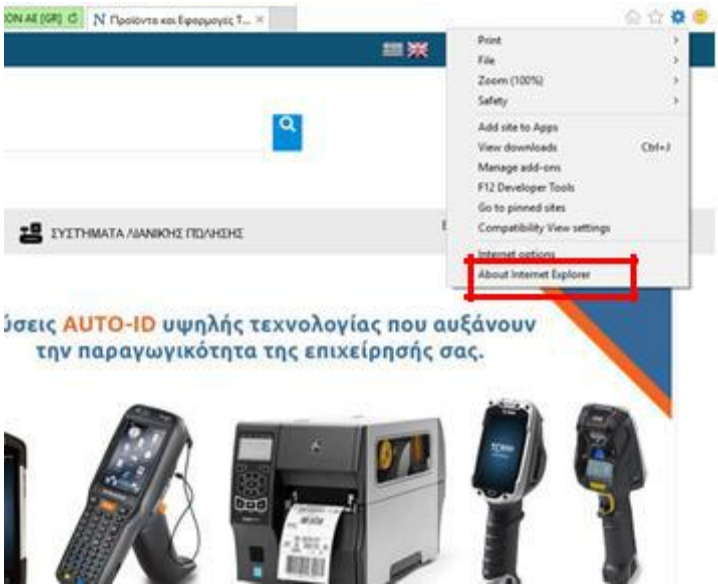
Βάσει των προδιαγραφών της κρατικής υπηρεσίας ανάπτυξης πληροφορικής για την ορθή εγκατάσταση των προσωπικών μας Ψηφιακών Πιστοποιητικών, είναι **υποχρεωτικό** να χρησιμοποιήσουμε υπολογιστή με **λειτουργικό σύστημα Windows 7 και Internet Explorer 8 ή 9 ή 10**. Η εγκατάσταση αυτή πραγματοποιείται μία 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).



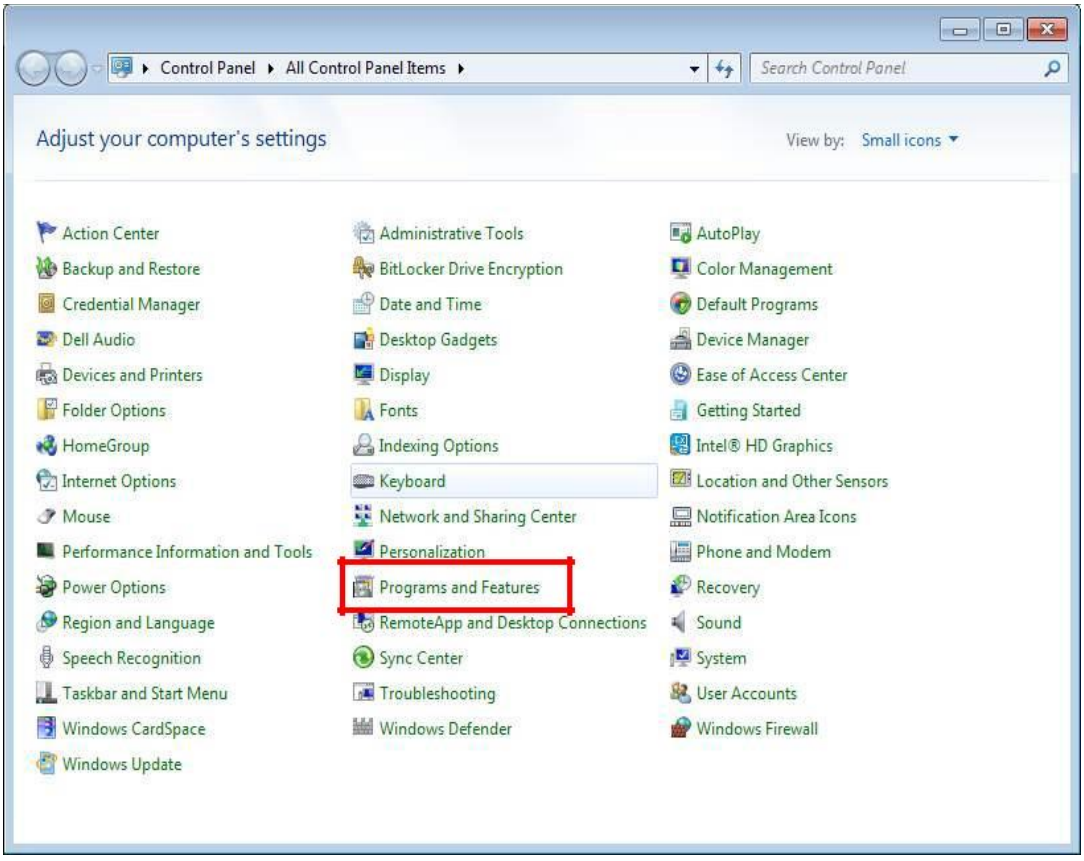
Επιλέγουμε About Internet Explorer (Πληροφορίες για τον Internet Explorer).



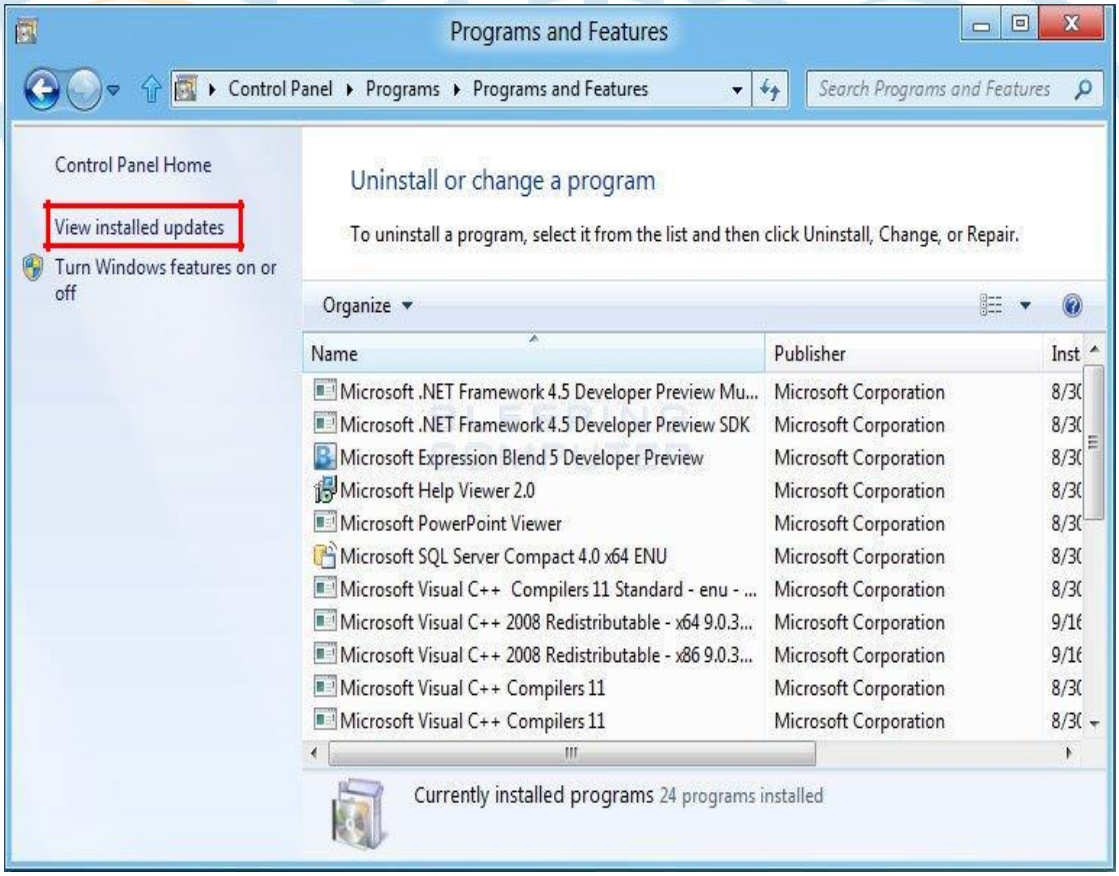
Λαμβάνουμε την πληροφορία για την έκδοση του προγράμματος.

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).

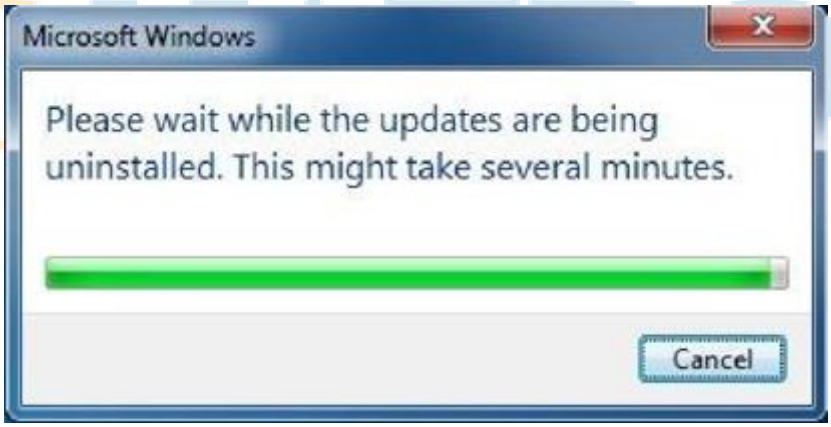


Επιλέγουμε Προβολή εγκατεστημένων ενημερώσεων (View installed updates).

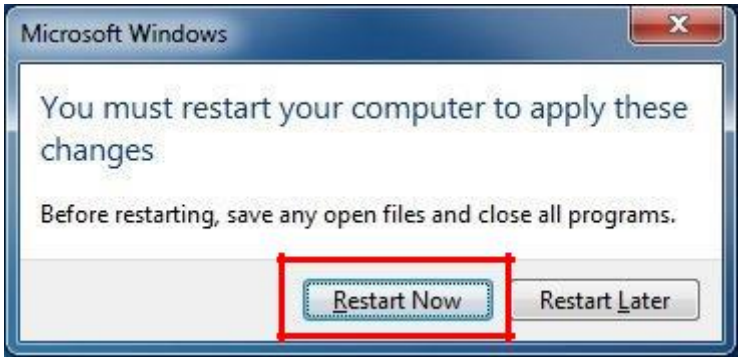


Και στη συνέχεια εντοπίζουμε και επιλέγουμε τον Internet Explorer 11 και πατάμε Κατάργηση Εγκατάστασης (Uninstall).

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.

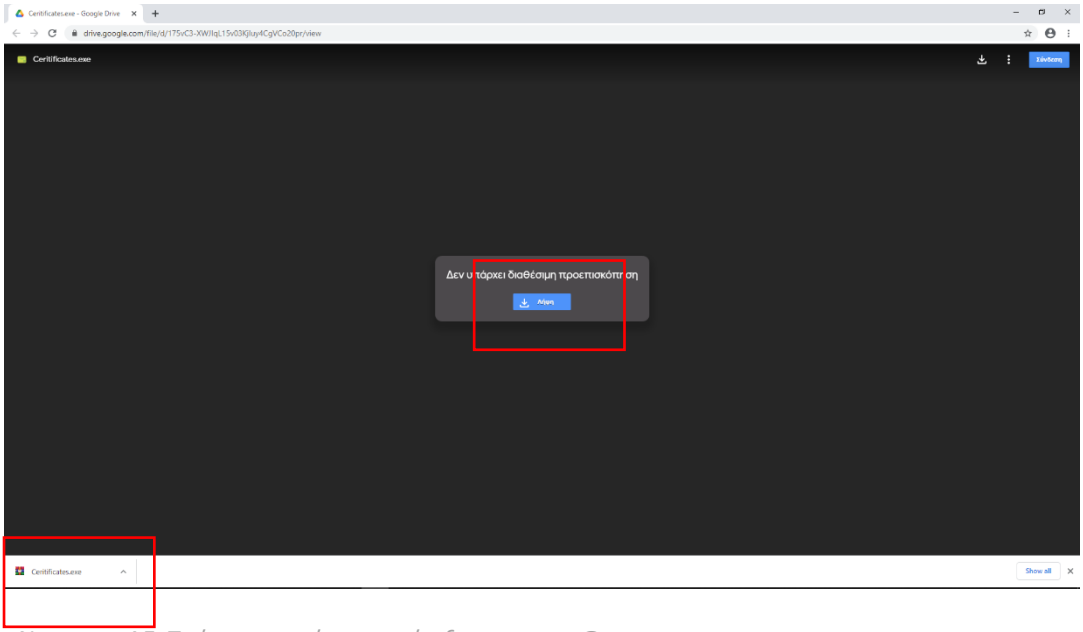
Εγκατάσταση των ψηφιακών πιστοποιητικών των Αρχών Πιστοποίησης και Χρονοσήμανσης, παραμετροποίηση του Internet Explorer

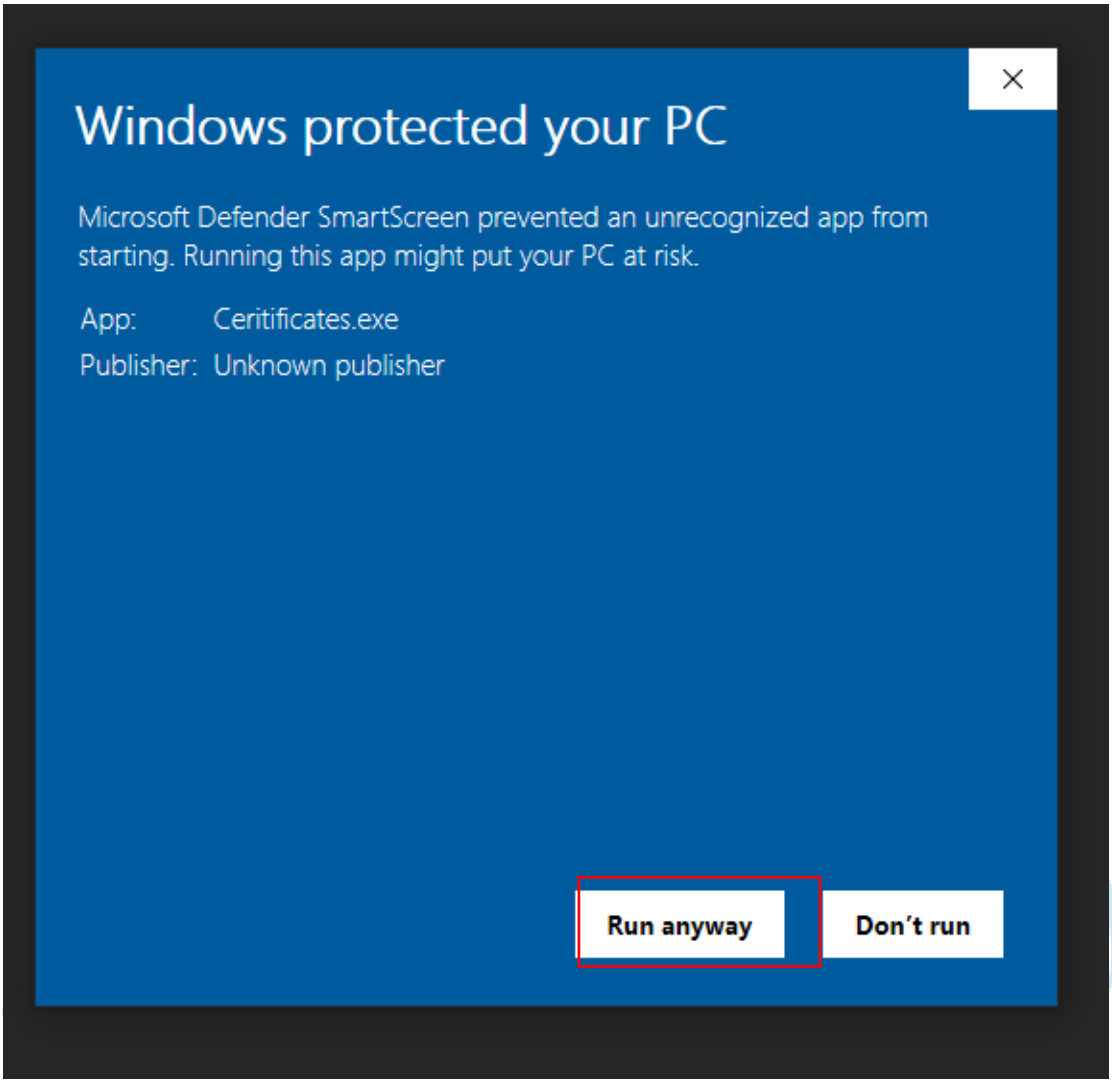
Αφού έχουμε προχωρήσει στην υποβάθμιση του Internet Explorer και έχουμε ελέγξει την έκδοση, κατεβάζουμε από τον παρακάτω σύνδεσμο το πρόγραμμα και το τρέχουμε, έχοντας αποσυνδεδεμένο το USB Token, έχοντας κλείσει και αποθηκεύσει τα προγράμματα και τα αρχεία στον υπολογιστή μας καθώς η εκτέλεση του προγράμματος θα οδηγήσει σε υποχρεωτική επανεκκίνηση τον υπολογιστή μας:

Win7-10_Certificates_IE_AdobeDC_install_Nov_2020.zip

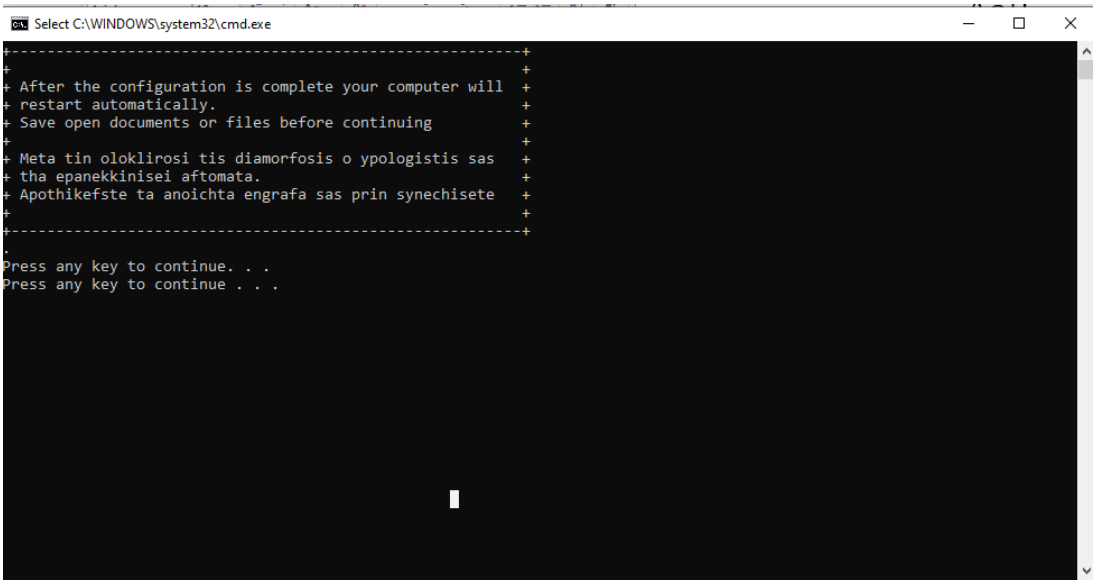
Κωδικός αποσυμπίεσης: 2020

Επιλέγουμε διαδοχικά:

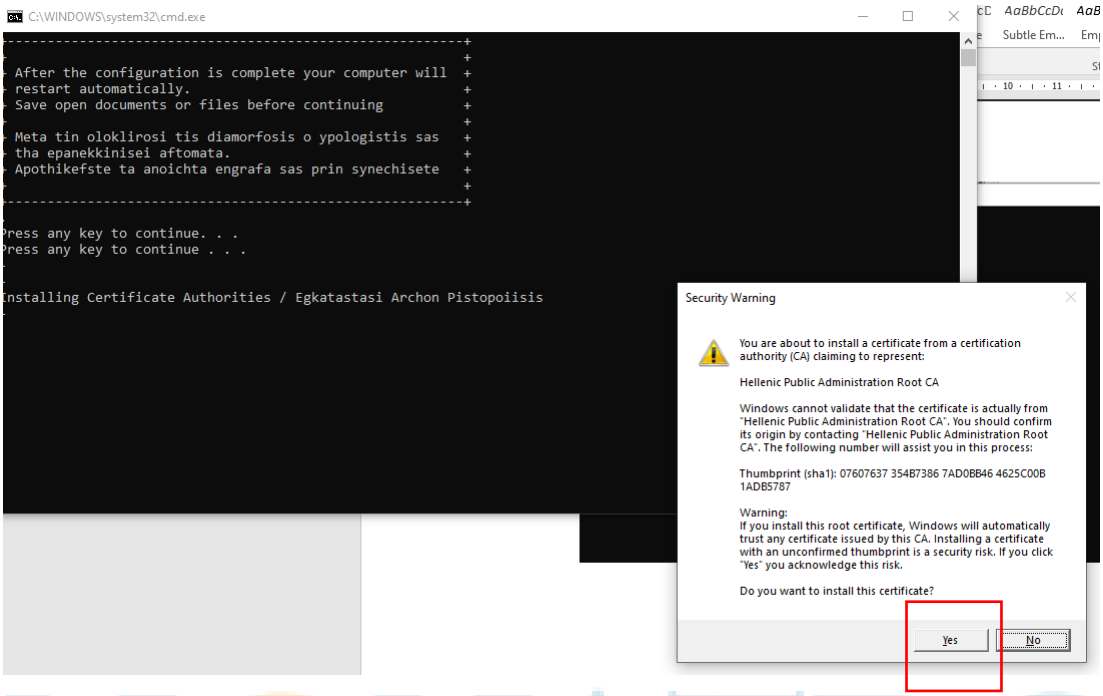




Πατάμε οποιοδήποτε πλήκτρο για να συνεχίσουμε πχ. Space



Επιλέγουμε Ναι σε όλα τα παράθυρα που θα εμφανιστούν



Ο υπολογιστής μας κάνει επανεκκίνηση, μόλις ανοίξει προχωράμε στο επόμενο βήμα.

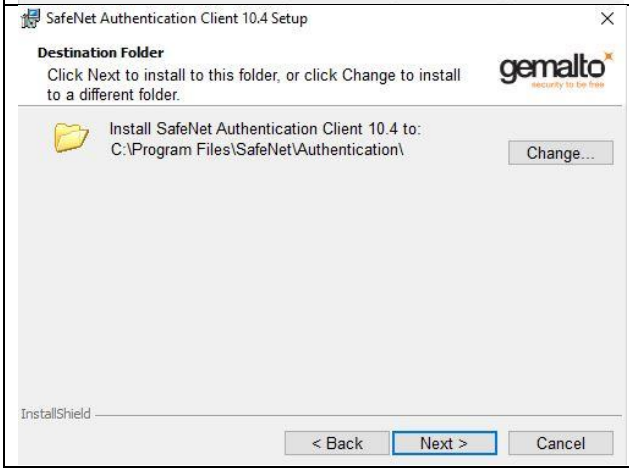
Βήμα 5ο: Εγκατάσταση του Safenet Authentication Client (πρόγραμμα οδήγησης του USB Token).

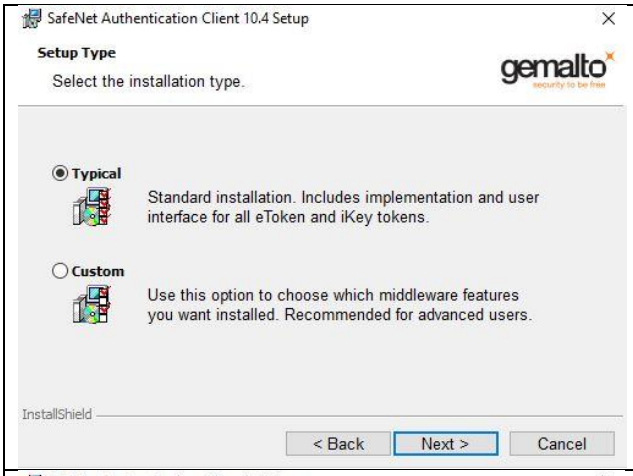
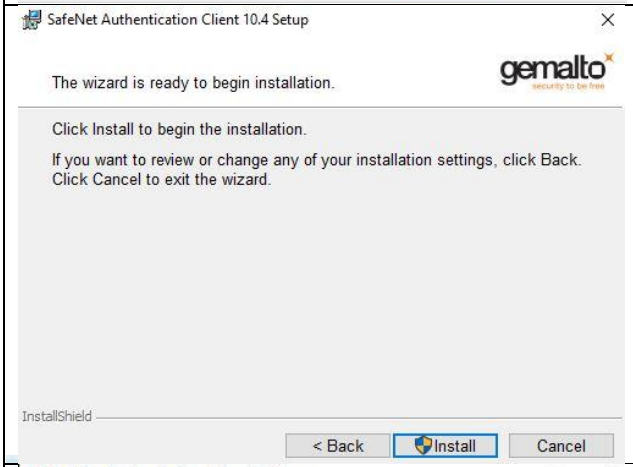
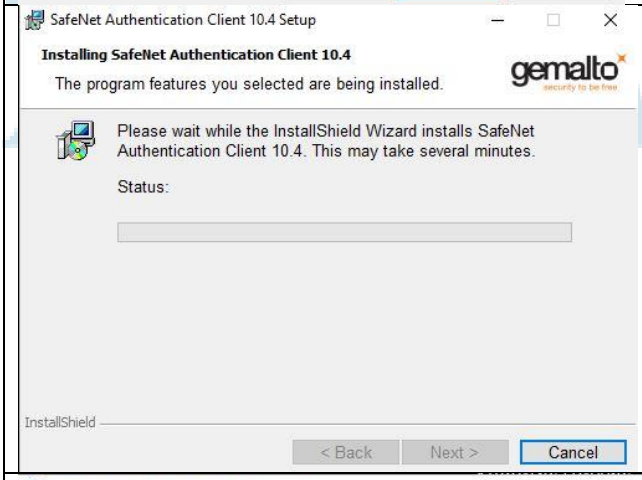
Οι οδηγοί (Driver & Middleware) είναι διαθέσιμοι στην ιστοσελίδα μας στην σελίδα του προϊόντος, στην καρτέλα σχετικά αρχεία ή στον παρακάτω σύνδεσμο:

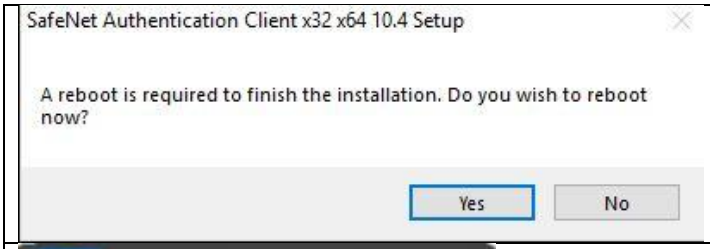
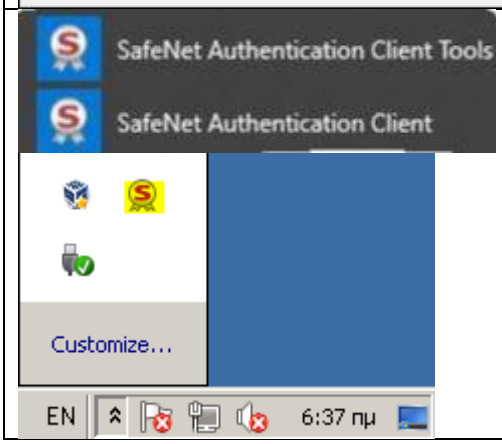
https://drive.google.com/open?id=1mVR-QFRGSrqguhJfJ-ArJc7JrsyUMbKP

Αφού κατεβάσουμε το αρχείο μπορούμε να το εκτελέσουμε φροντίζοντας να έχουμε πλήρη δικαιώματα (δικαιώματα διαχειριστή) στον υπολογιστή μας.

SafeNetAuthenticationClient-x32-x64-10.4	Κάνουμε διπλό κλικ στο εκτελέσιμο αρχείο που κατεβάσαμε.

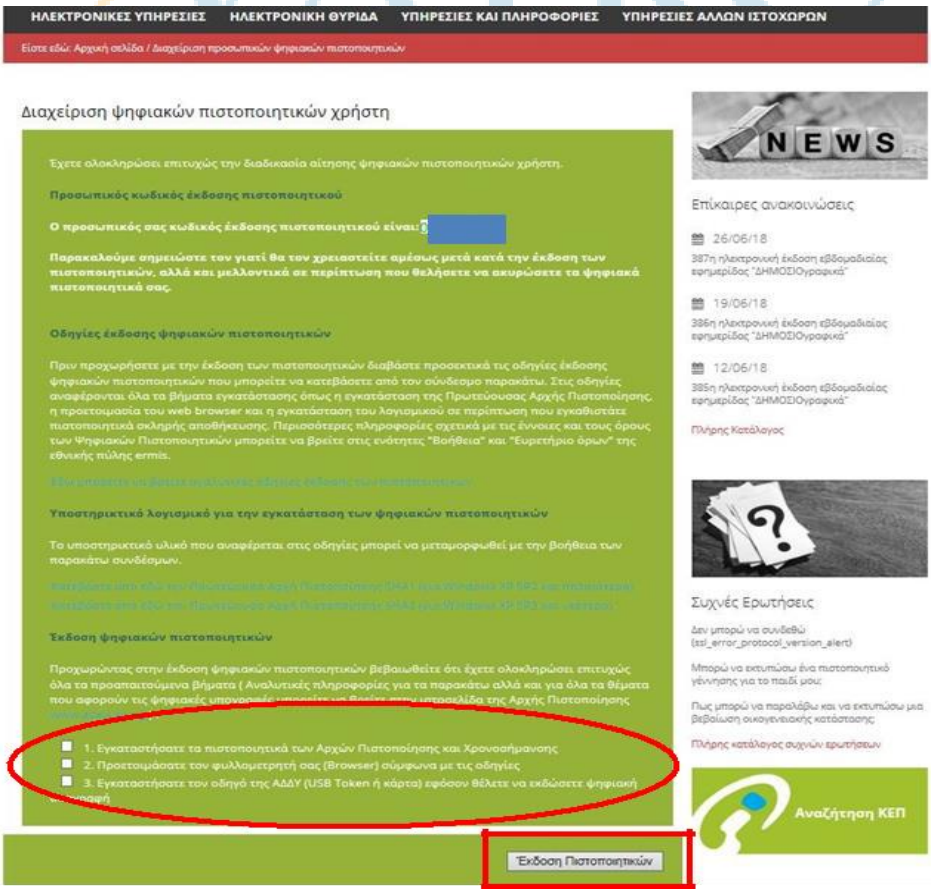
	Στην επόμενη οθόνη επιλέγουμε Next.
	Επιλέγουμε τη γλώσσα εγκατάστασης και πατάμε το κουμπί Next.
	Αποδεχόμαστε τους όρους χρήσης και πατάμε το κουμπί Next.
	Επιλέγουμε τον προορισμό εγκατάστασης και πατάμε το κουμπί Next.

	Επιλέγουμε τυπική εγκατάσταση και πατάμε το κουμπί Next.
	Στην επόμενη οθόνη κάνουμε κλικ στο κουμπί Install.
	Περιμένουμε να ολοκληρωθεί η εγκατάσταση.
	Μόλις ολοκληρωθεί η εγκατάσταση κάνουμε κλικ στο κουμπί Finish.

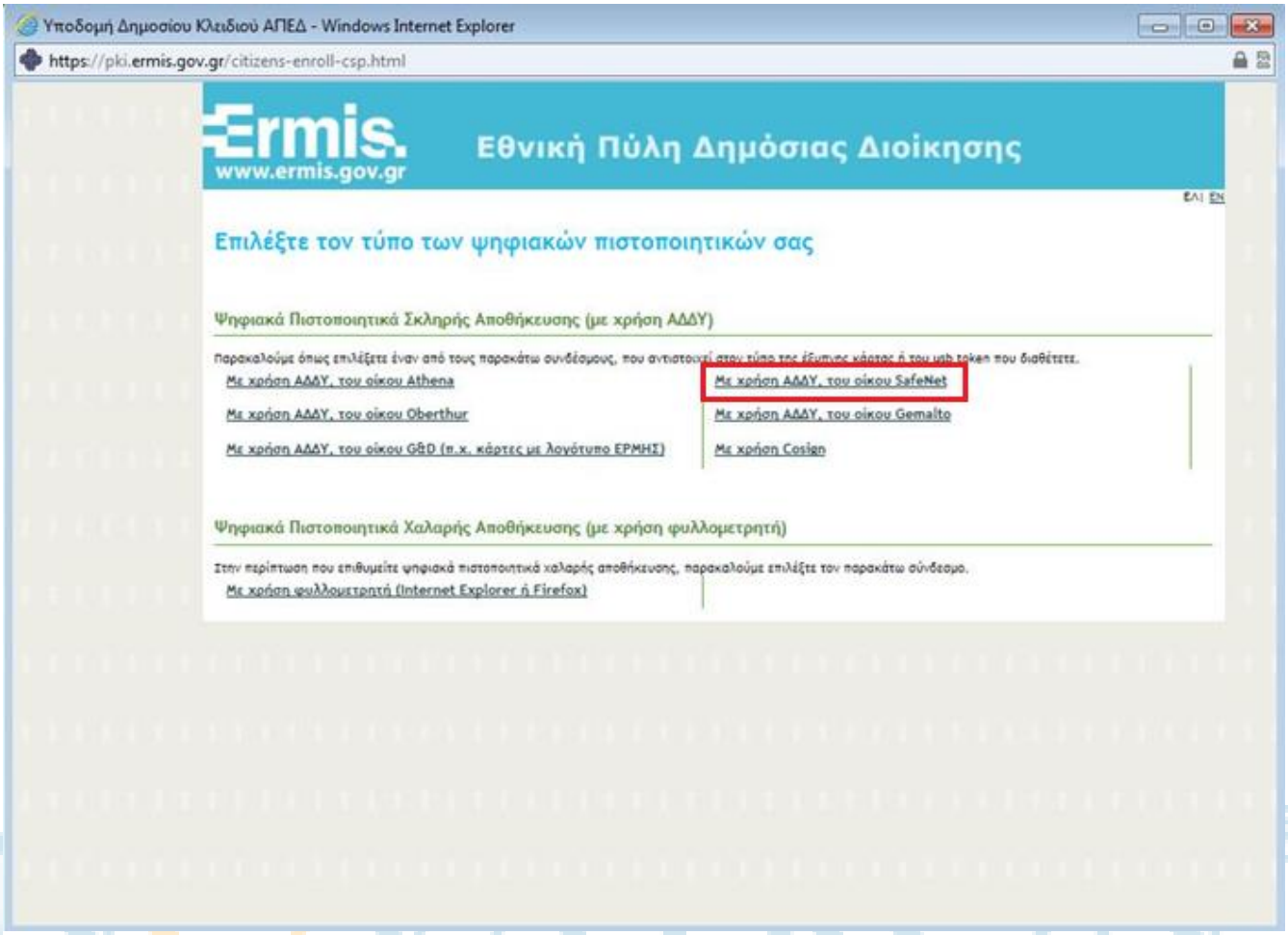
	Στο μήνυμα που ζητάει την επανεκκίνηση του υπολογιστή μας κάνουμε κλικ στο κουμπί Yes.
	Αφού ολοκληρωθεί η επανεκκίνηση συνδέουμε το Token σε μια από τις θύρες USB και θα εγκατασταθεί αυτόματα. Στο μενού έναρξη του υπολογιστή μας καθώς και στο System Tray θα εμφανιστεί το ανάλογο εικονίδιο του Safenet Authentication Client με το οποίο μπορούμε να διαχειριστούμε το Token μας.

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

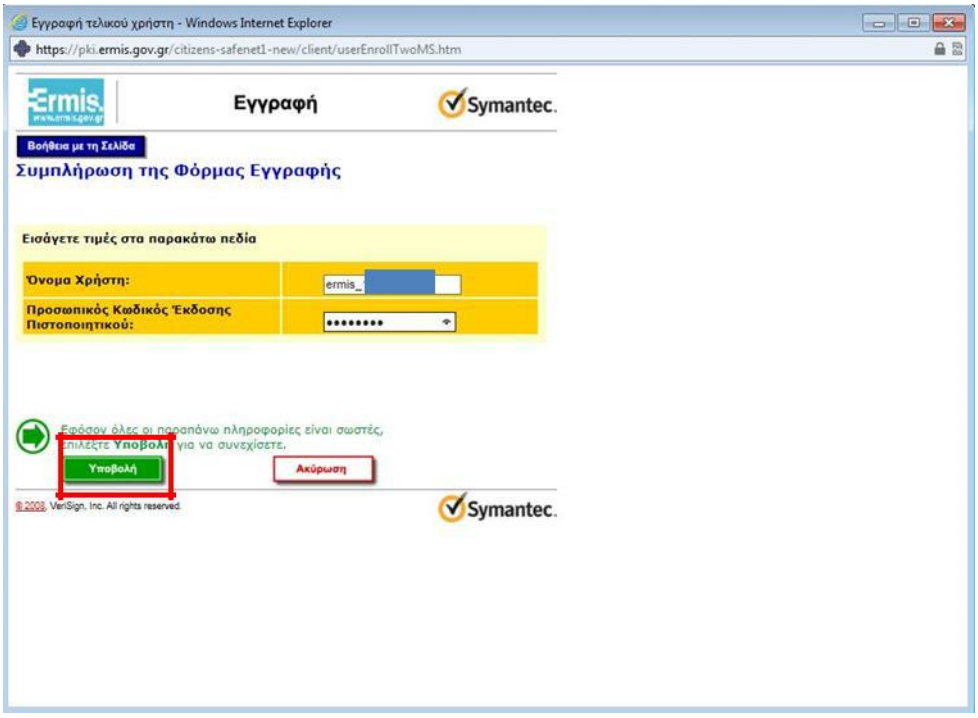
Συνδέουμε το USB Token στον υπολογιστή μας. Μπαίνουμε με τους κωδικούς Taxisnet στην Πύλη ΕΡΜΗΣ (βλ. Βήμα 1ο) και επιλέγουμε το σύνδεσμο Πίνακας Ελέγχου και στη συνέχεια το σύνδεσμο Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών (βλ. Βήμα 1ο), πλέον έχουμε την παρακάτω εικόνα, όπου καταγράφουμε τον οκταψήφιο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



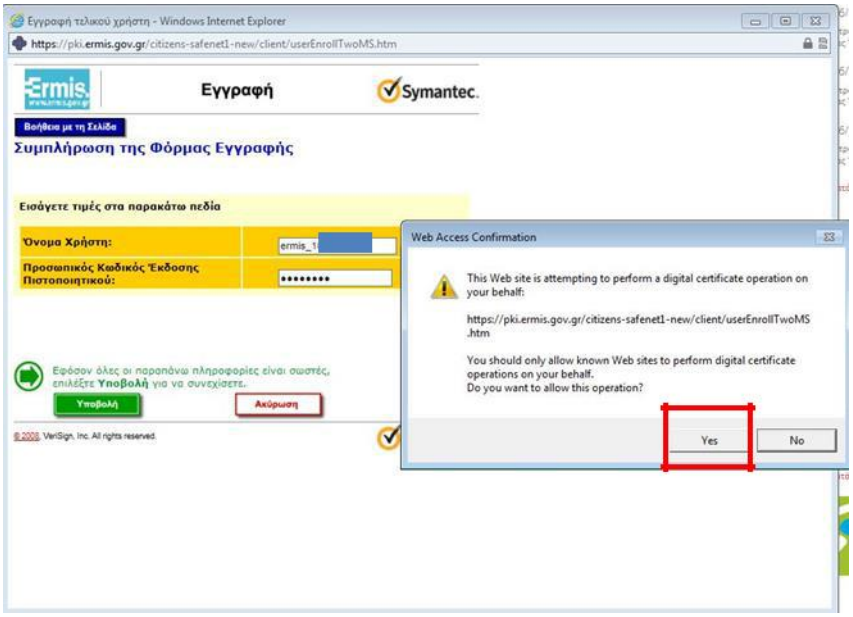
Ανοίγει η ακόλουθη καρτέλα όπου επιλέγουμε Με χρήση ΑΑΔΥ, του οίκου **Safenet** (Προσοχή, όχι Gemalto).



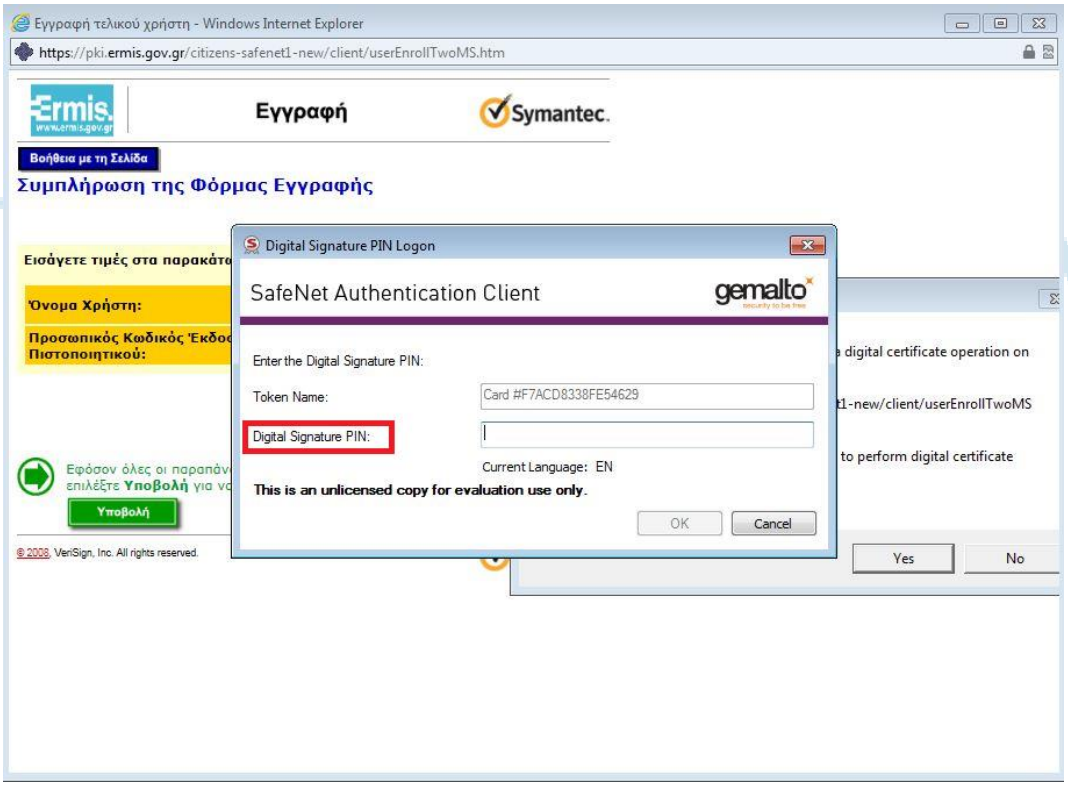
Τώρα εμφανίζεται σελίδα με δύο πεδία. Το πρώτο πεδίο θα πρέπει να συμπληρωθεί με το όνομα χρήστη που έχουμε στη Πύλη ΕΡΜΗΣ (ermis_ …….), ενώ στο πεδίο Προσωπικός Κωδικός Έκδοσης Πιστοποιητικού πληκτρολογούμε τον οκταψήφιο κωδικό και στη συνέχεια πατάμε το κουμπί Υποβολή.



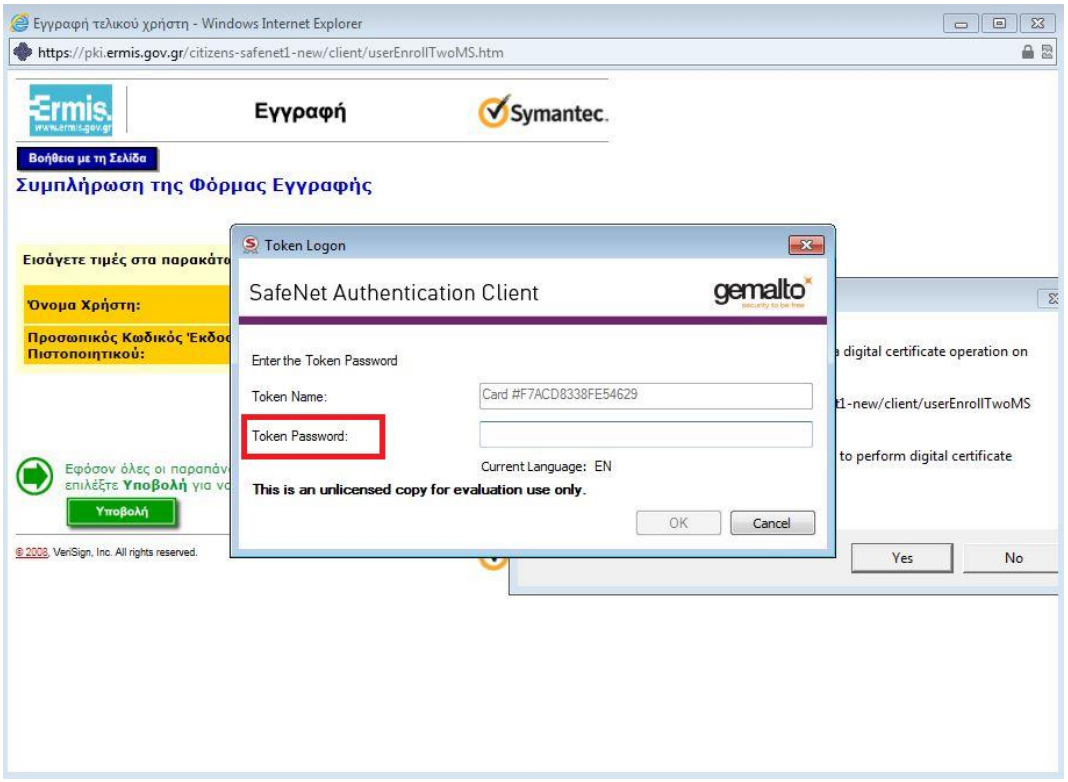
Στη συνέχεια πατάμε Yes στο μήνυμα της παρακάτω εικόνας, καθώς και σε όσα παρόμοια μηνύματα παρουσιαστούν.



Αρκετές φορές μέσα στην διαδικασία εγκατάστασης των πιστοποιητικών μας από την πύλη του ΕΡΜΗ θα μας ζητηθεί το Digital Signature PIN του Token το οποίο είναι έξι (6) μηδενικά από προεπιλογή (000000).

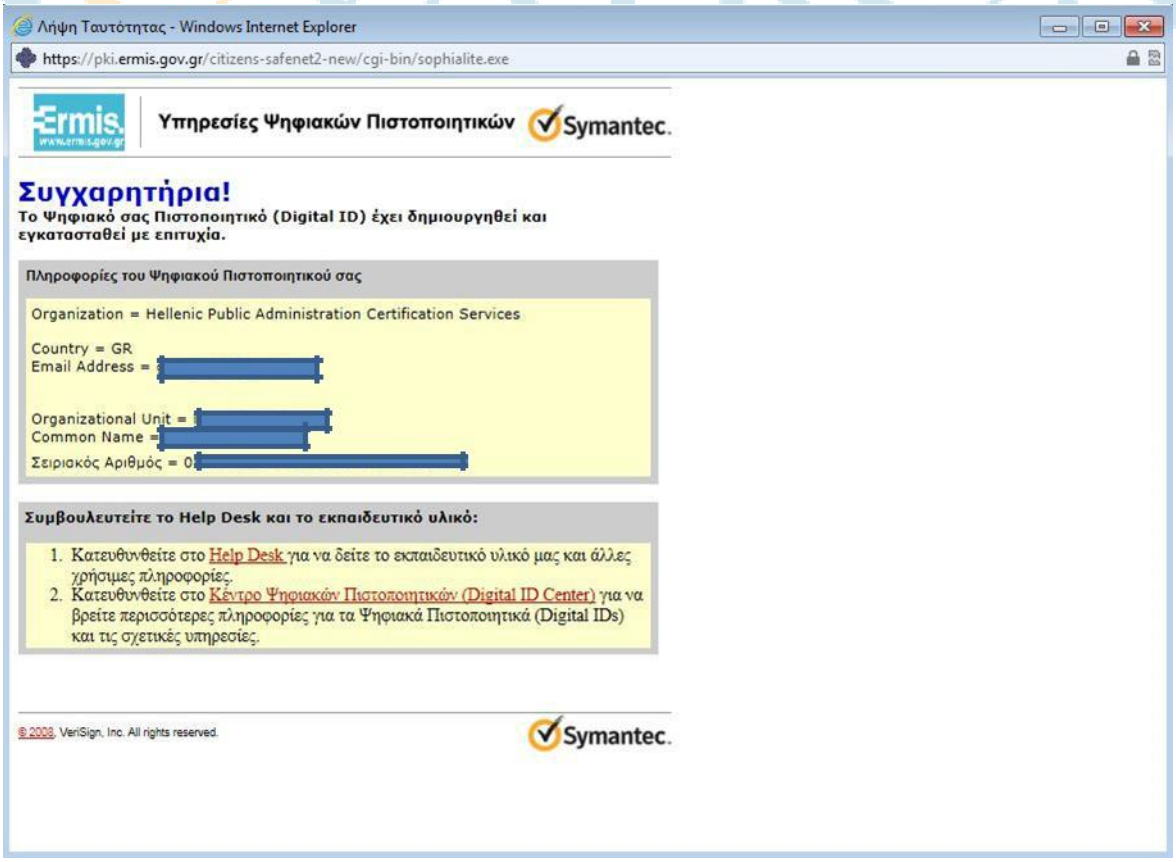


Επίσης αρκετές φορές μέσα στην διαδικασία εγκατάστασης θα μας ζητηθεί το Token Password το οποίο είναι τέσσερα (4) μηδενικά (0000)

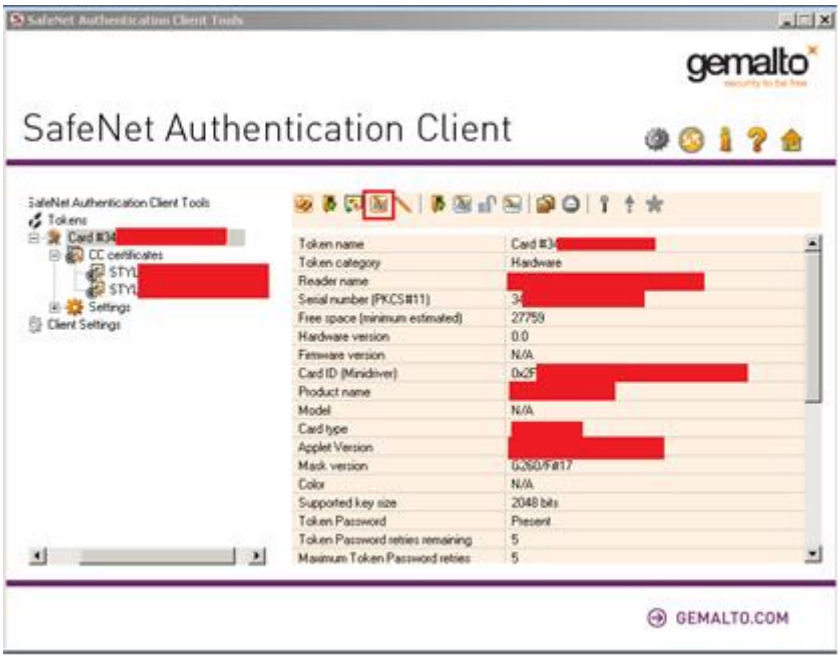


ΠΡΟΣΟΧΗ! Λόγω του ότι το Token Password και το Digital Signature PIN είναι διαφορετικά θα πρέπει να δώσουμε μεγάλη προσοχή στα μηνύματα που μας εμφανίζονται καθώς αν καταχωρήσουμε λάθος κωδικούς η διαδικασία θα αποτύχει.

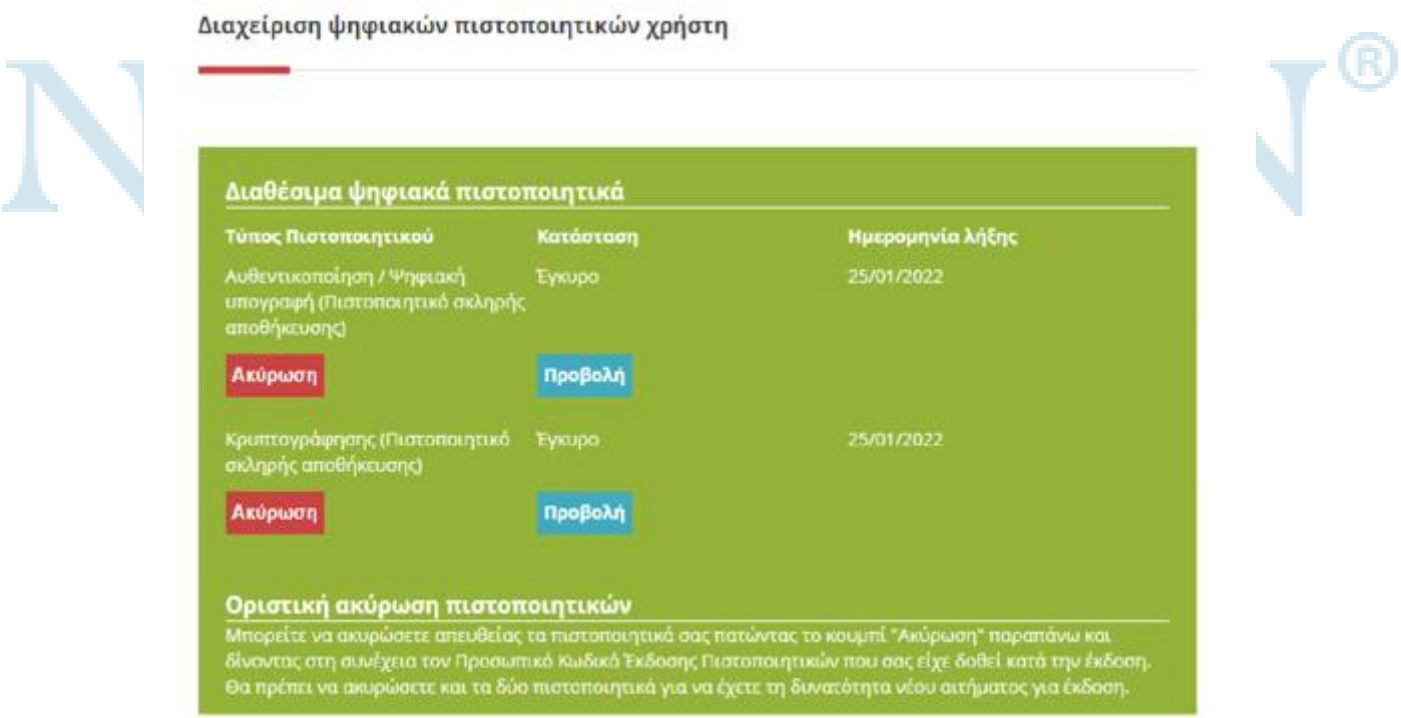
Όταν η διαδικασία ολοκληρωθεί θα παρουσιαστεί η ακόλουθη εικόνα, η οποία περιέχει και τα στοιχεία του κατόχου του πιστοποιητικού.



Τέλος, ανοίγουμε το Safenet Authentication Client και στο πεδίο Advanced View, 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 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:

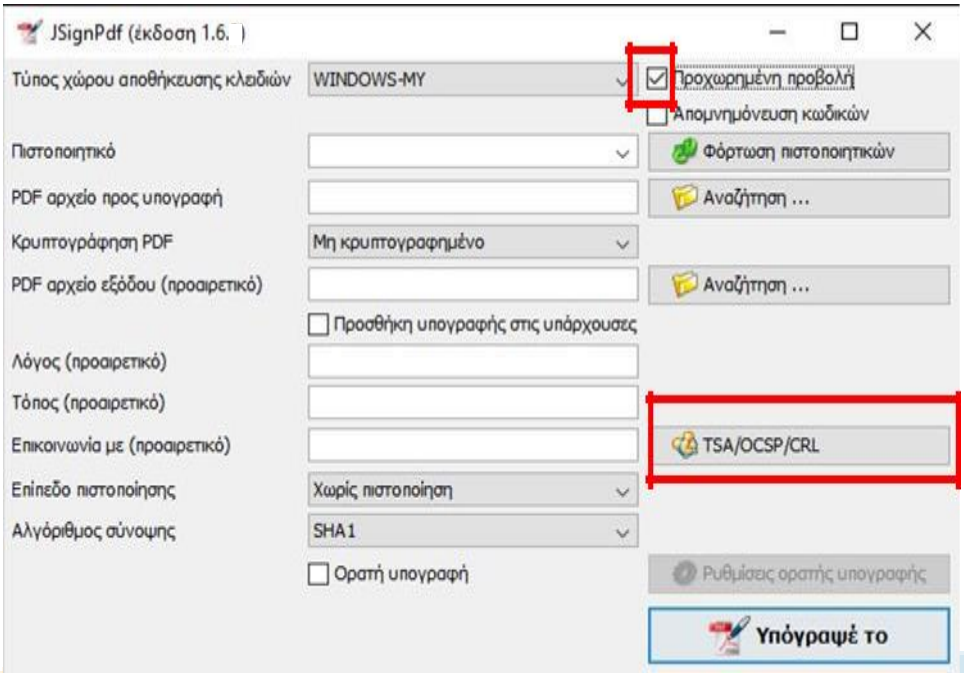
- Να υλοποιήσουμε το 4ο βήμα του παρόντος οδηγού
- Να υλοποιήσουμε το 5ο βήμα του παρόντος οδηγού
- Να εγκαταστήσουμε ένα πρόγραμμα το οποίο καθιστά δυνατή την υπογραφή Pdf αρχείων (θα το δούμε παρακάτω)

Ψηφιακή Υπογραφή με το πρόγραμμα JsignPdf.

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

https://drive.google.com/file/d/1G5uTu5ZA2jvaaIHOBV1iSN4BvYcfL3WE/view?usp=sharing

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. :

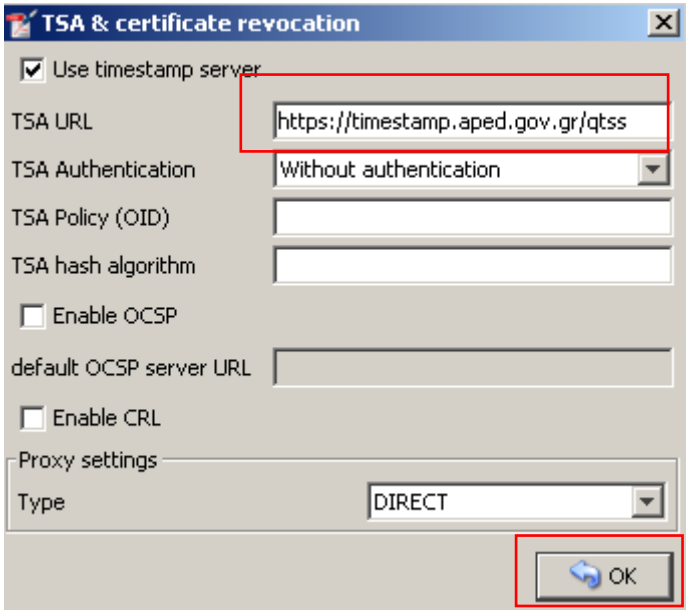


Επιλέγουμε Χρησιμοποίησε ασφαλή χρονοσήμανση.

Για να χρησιμοποιήσουμε την ασφαλή χρονοσήμανση της ΑΠΕΔ, στο πεδίο TSA URL κάνουμε αντιγραφή (Control+C) και επικόλληση (Control+V) τον παρακάτω σύνδεσμο:

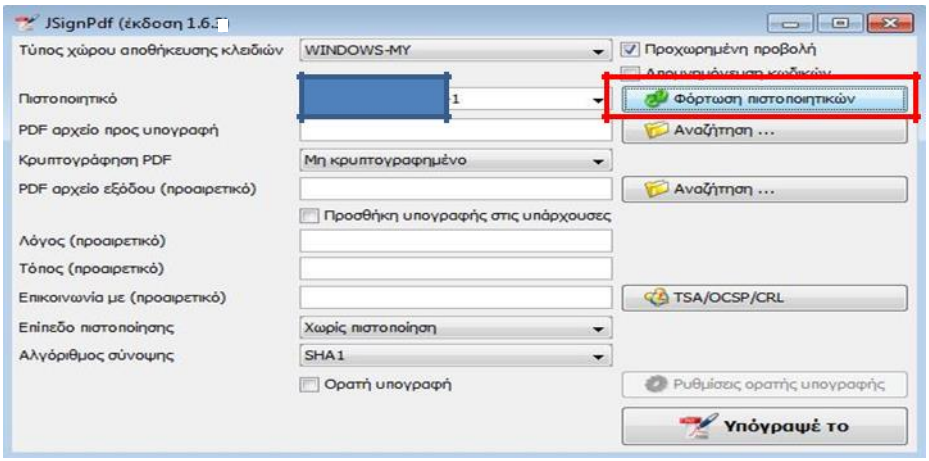
https://timestamp.aped.gov.gr/qtss

Κάνουμε κλικ στο κουμπί OK.

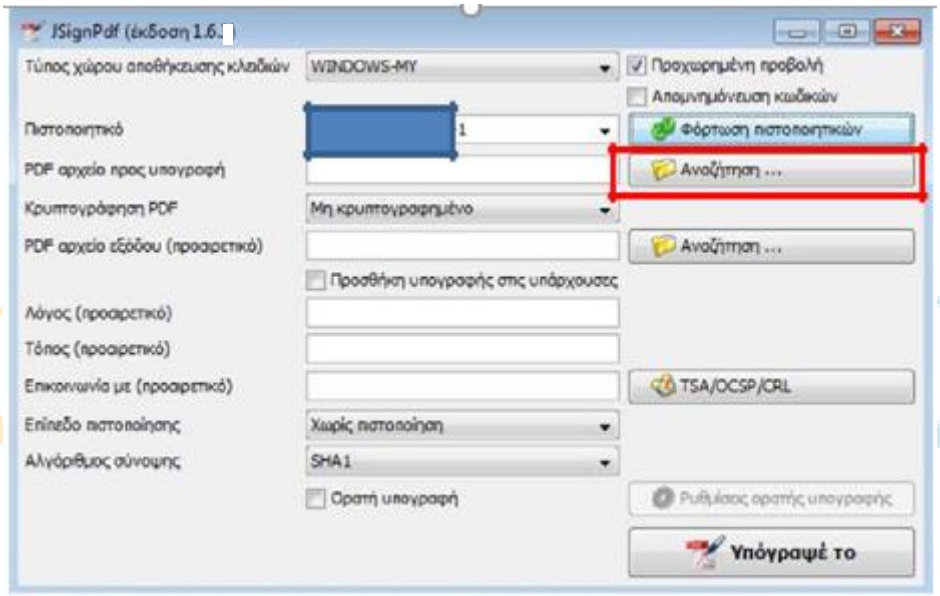


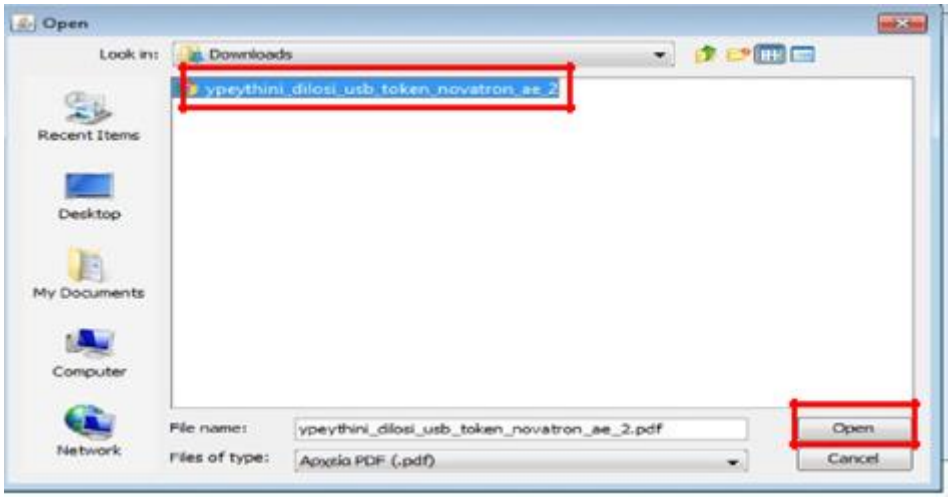
Η παραπάνω διαδικασία γίνεται μία φορά, το πρόγραμμα αποθηκεύει τις ρυθμίσεις.

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

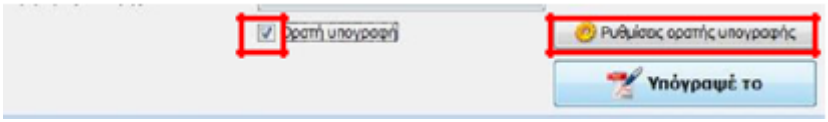


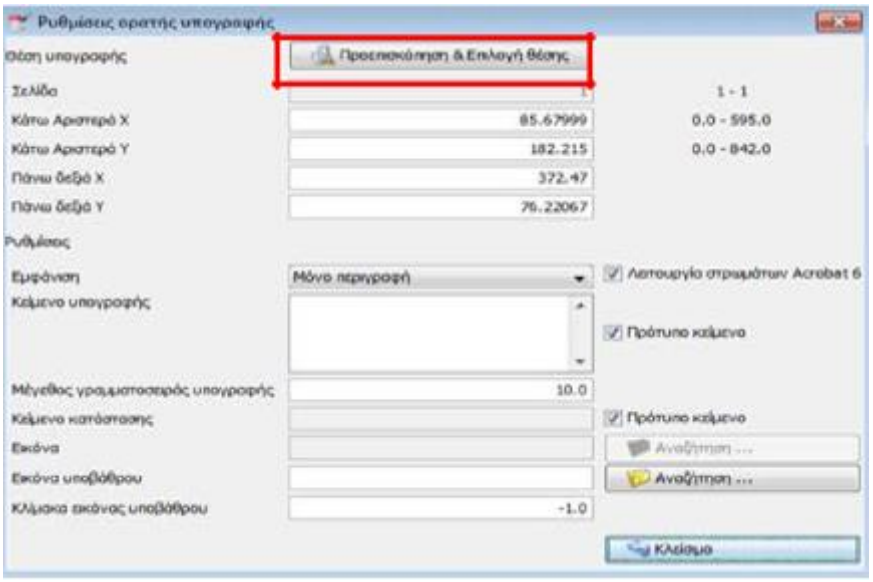
Κάνουμε κλικ στο πρώτο κουμπί Αναζήτηση για να επιλέξουμε το PDF αρχείο προς υπογραφή:



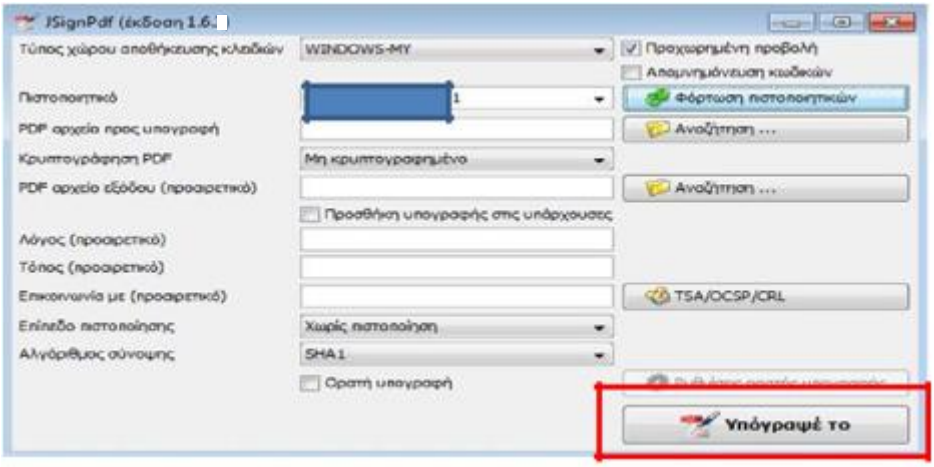


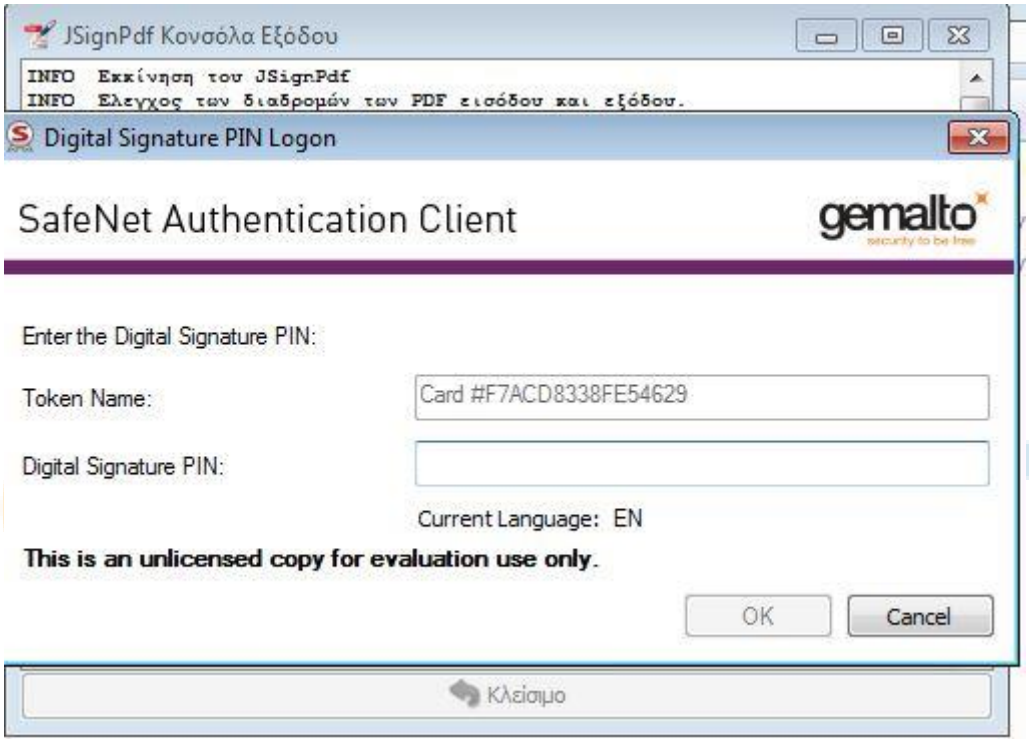
Για να προσθέσουμε Ορατή Υπογραφή, επιλέγουμε Ορατή υπογραφή, κάνουμε κλικ στο κουμπί Ρυθμίσεις ορατής υπογραφής, επιλέγουμε Προεπισκόπηση & Επιλογή θέσης όπου εμφανίζετε το έγγραφο στο οποίο (με το αριστερό κλικ από το ποντίκι μας) επιλέγουμε το ΠΟΥ θα τοποθετηθεί η υπογραφή μας και κάνουμε κλικ στο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



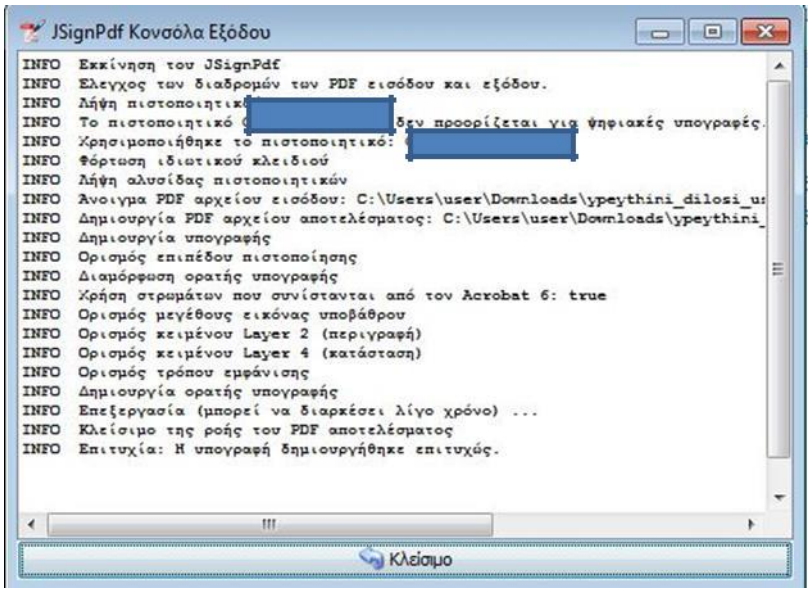


Κάνουμε κλικ στο κουμπί Υπέγραψε το και αυτόματα μας ζητάει το Digital Signature PIN που για το συγκεκριμένο Token είναι 6 φορές το 0 (000000), το εισάγουμε και πατάμε Ok.

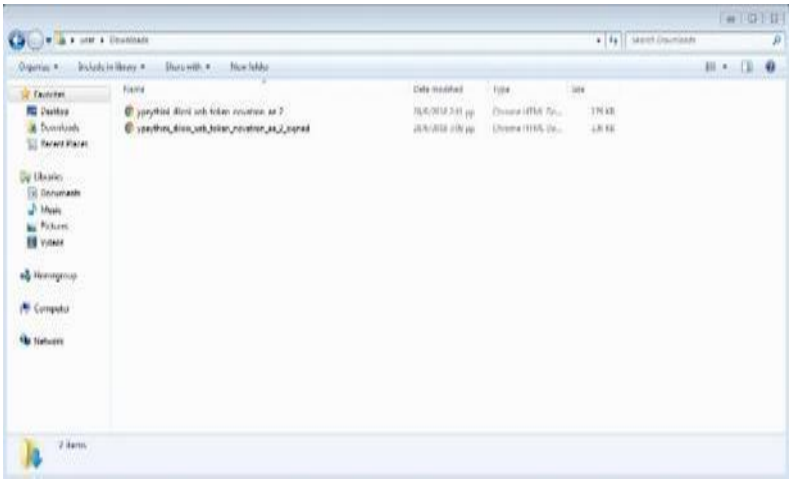




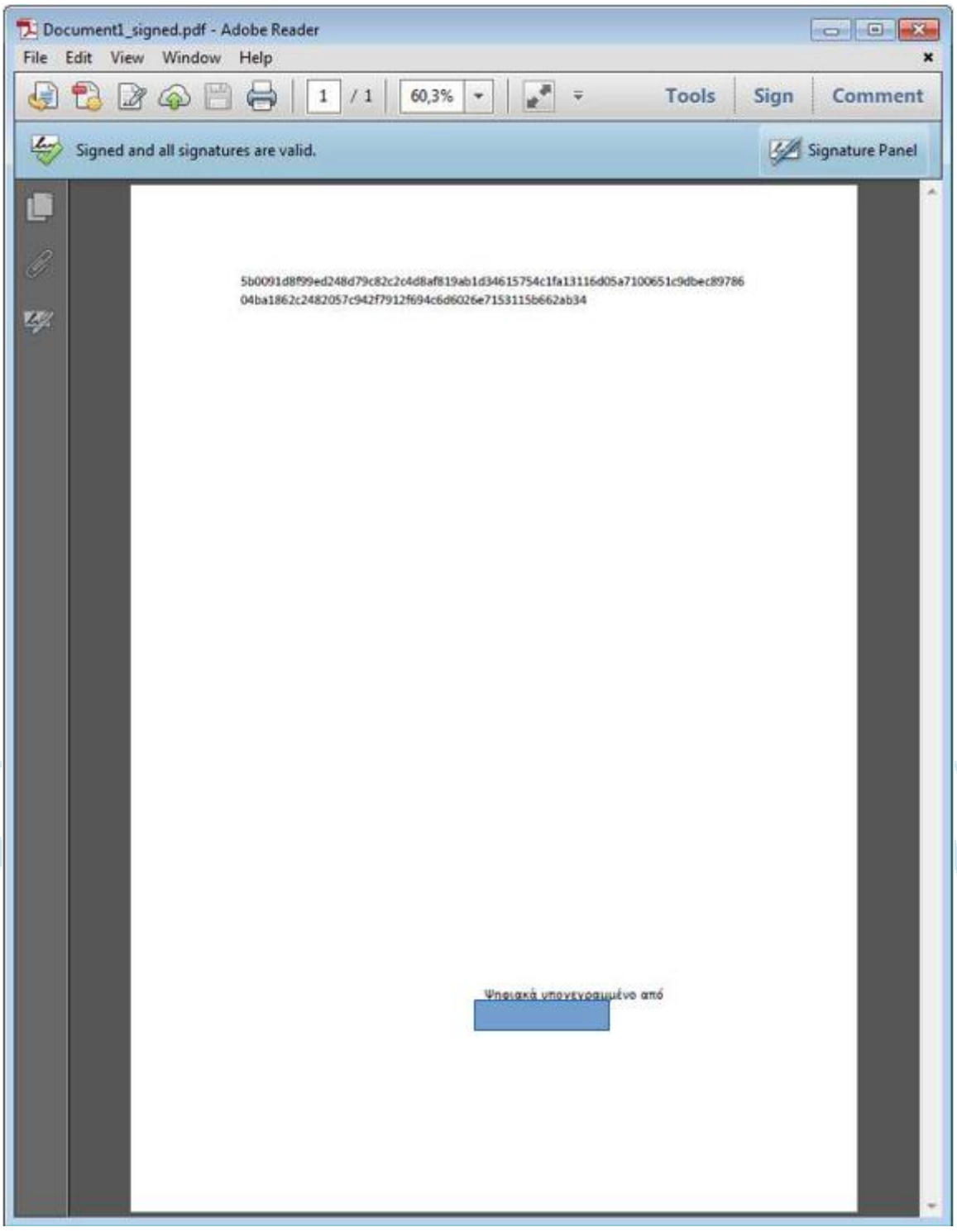
Στην συνέχεια μας δείχνει την πορεία της διαδικασίας βγάζοντας μας το αποτέλεσμα:



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

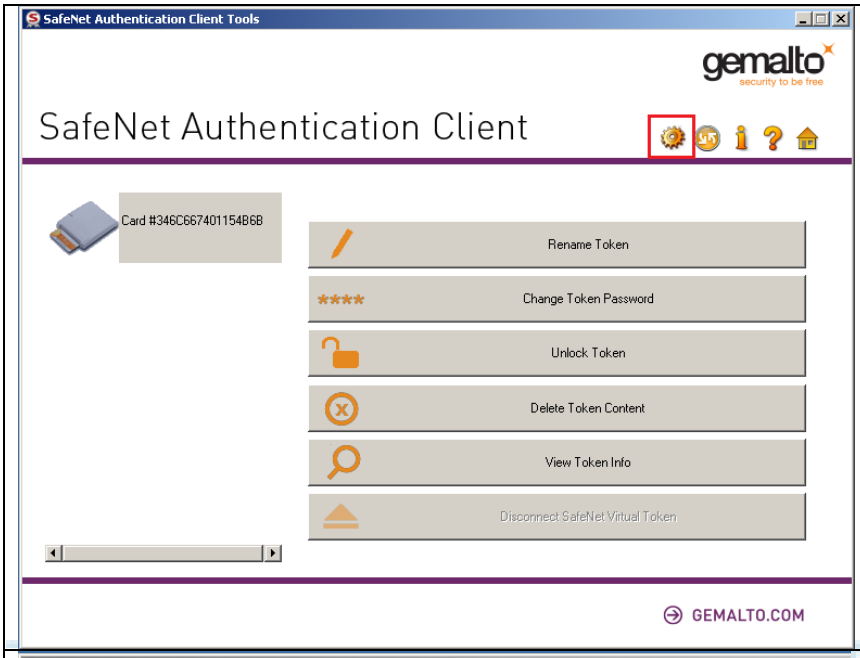
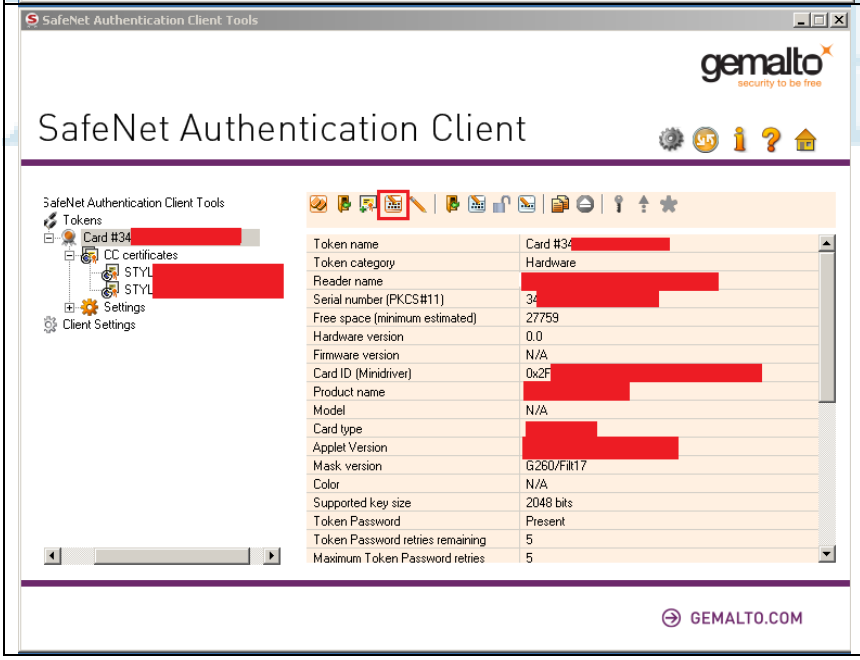


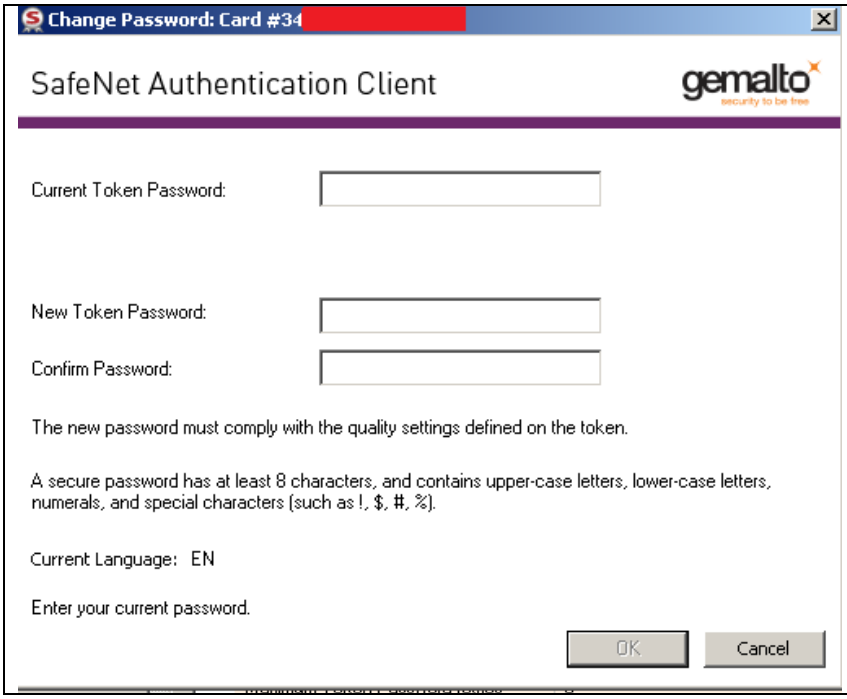
Έχουμε ολοκληρώσει επιτυχώς την Ψηφιακή Υπογραφή του εγγράφου μας. Βλέπουμε τη σήμανση Signed and all signatures are valid. Με τον τρόπο αυτό μπορούμε να βεβαιωθούμε ότι η υπογραφή είναι έγκυρη και δεν έχει γίνει επεξεργασία του εγγράφου μετά την υπογραφή (για να δούμε περισσότερες πληροφορίες κάνουμε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


Document1_signed.pdf - Adobe Reader
File Edit View Window Help
1 / 1
60,3%
Tools
Sign
Comment
Signed and all signatures are valid.
Signature Panel
5b0091d8f99ed248d79c82c2c4d8af819ab1d34615754c1fa13116d05a7100651c9dbec89786
04ba1862c2482057c942f7912f694c6d6026e7153115b662ab34
Ψηφιακά υπογεγραμμένο από

Παράρτημα: Διαχείριση κωδικών και περιεχομένων της συσκευής

Πως αλλάζω τον κωδικό του Token (Token Password)?

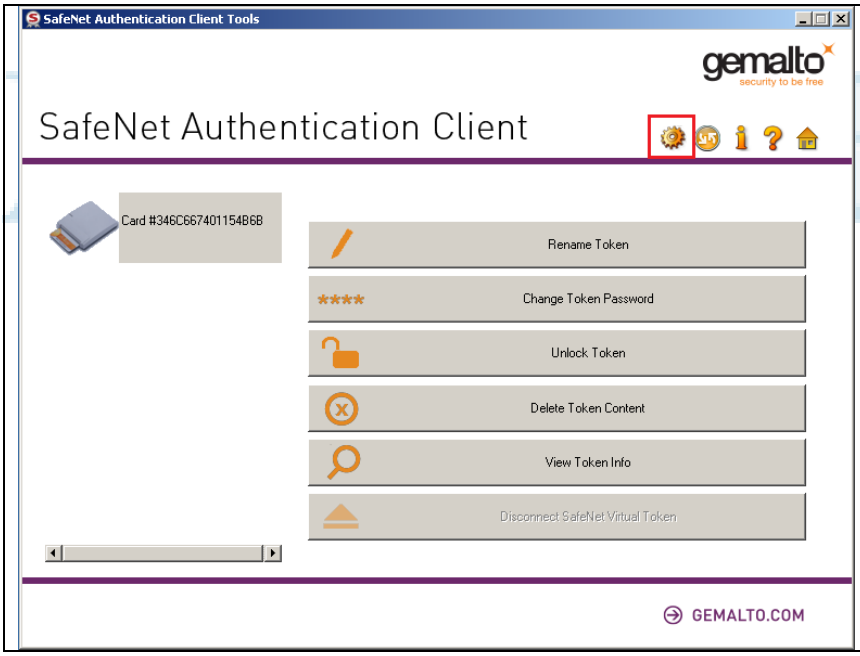
	Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.
	Επιλέγουμε το τέταρτο εικονίδιο από τα αριστερά.



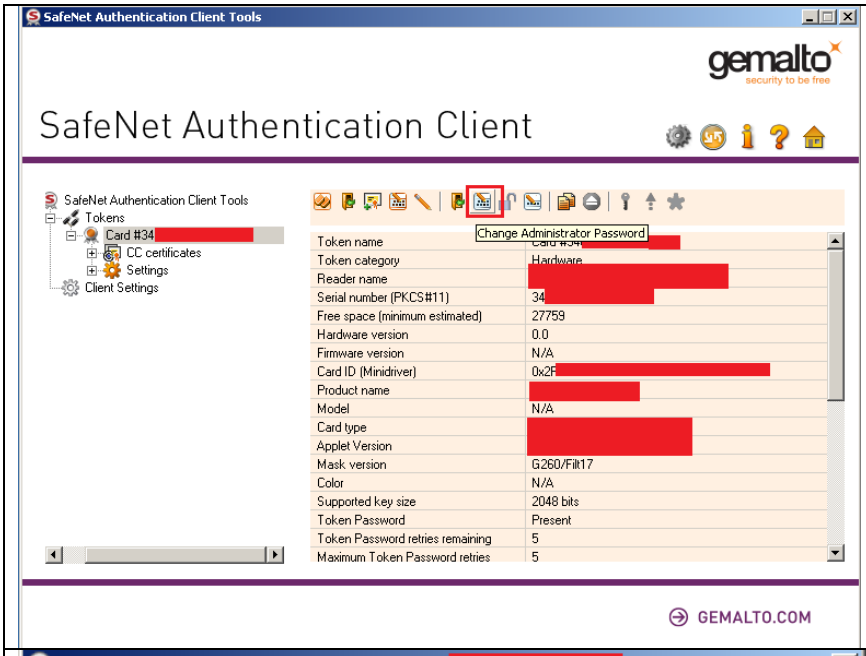
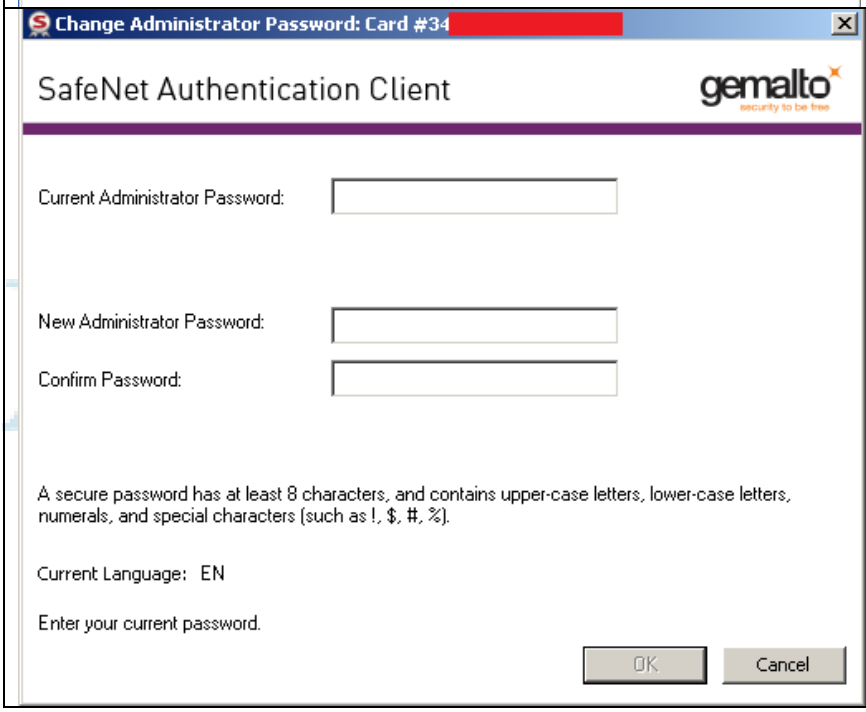
Current Token Password: Εδώ καταχωρούμε τον τρέχον κωδικό του Token .
New Token Password: Εδώ καταχωρούμε το νέο κωδικό που επιθυμούμε.
Confirm Password: Εδώ επιβεβαιώνουμε το νέο κωδικό που επιθυμούμε.

Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

Πως αλλάζω το κωδικό διαχειριστή του Token (Administrator Password)?

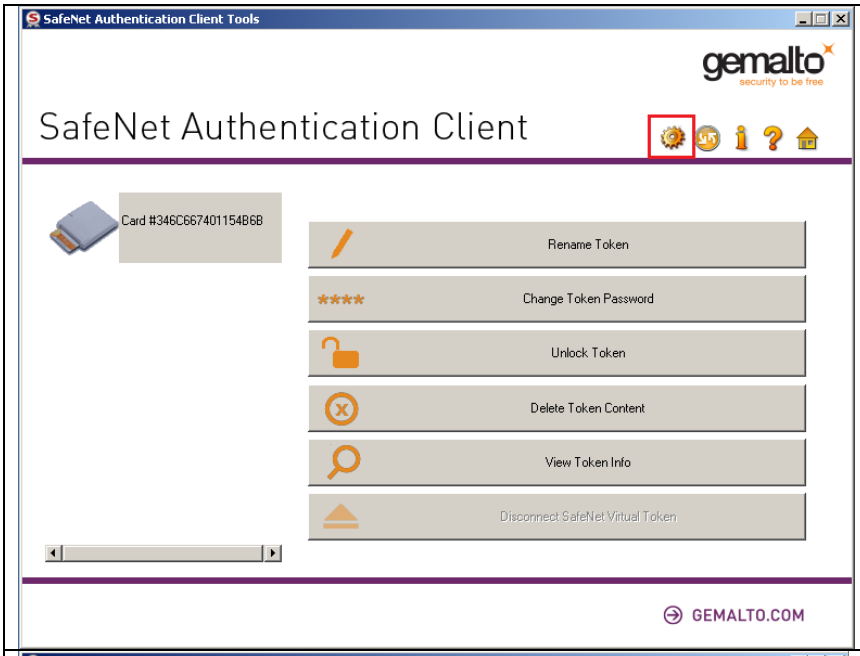
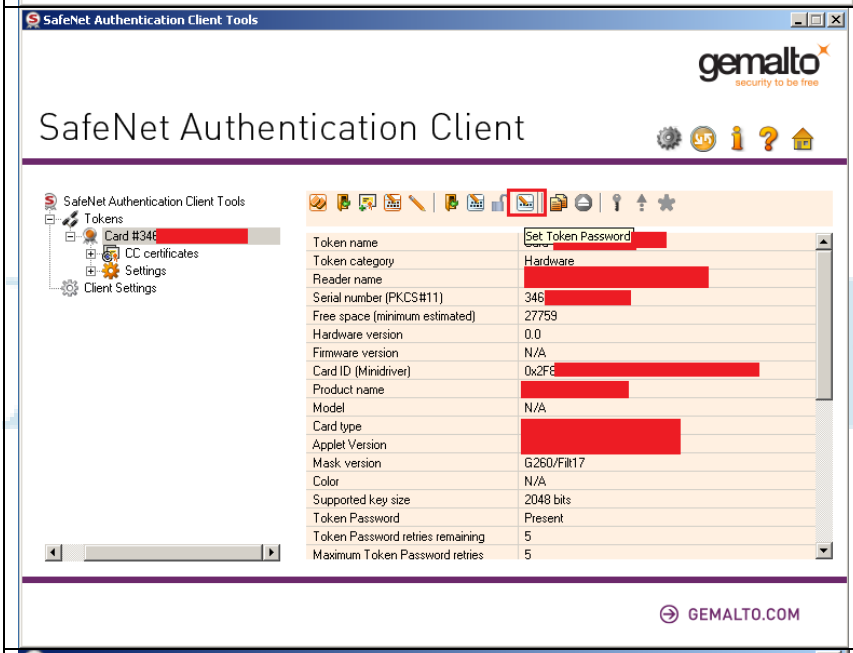
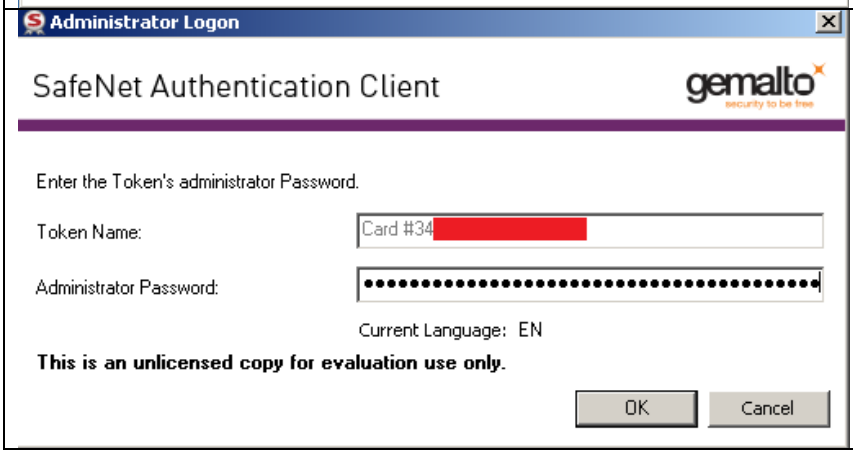


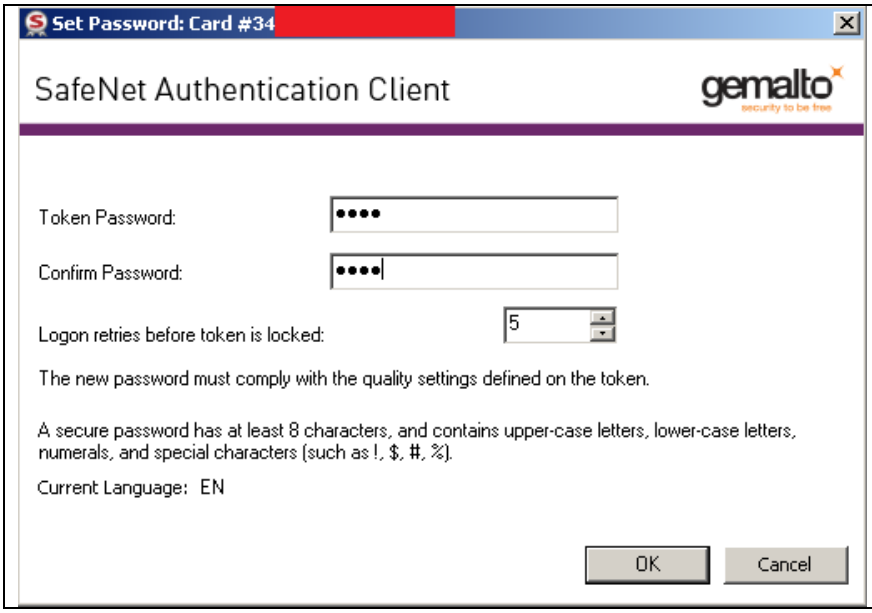
Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.

	Επιλέγουμε το έβδομο εικονίδιο από τα αριστερά.
	**Current Administrator Password:** Εδώ καταχωρούμε τον τρέχον κωδικό διαχειριστή (από προεπιλογή σαράντα οκτώ μηδενικά). **New Administrator Password:** Εδώ καταχωρούμε το νέο κωδικό διαχειριστή που επιθυμούμε. **Confirm Password:** Εδώ επιβεβαιώνουμε το νέο κωδικό διαχειριστή που επιθυμούμε. Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

Πως ξεκλειδώνω τον κωδικό του Token με τη χρήση του κωδικού διαχειριστή (Unlock Token).

Σε περίπτωση που κλειδώσει ο κωδικός χρήστη του Token μπορούμε να τον ξεκλειδώσουμε με τη χρήση του κωδικού διαχειριστή ακολουθώντας τα παρακάτω βήματα.

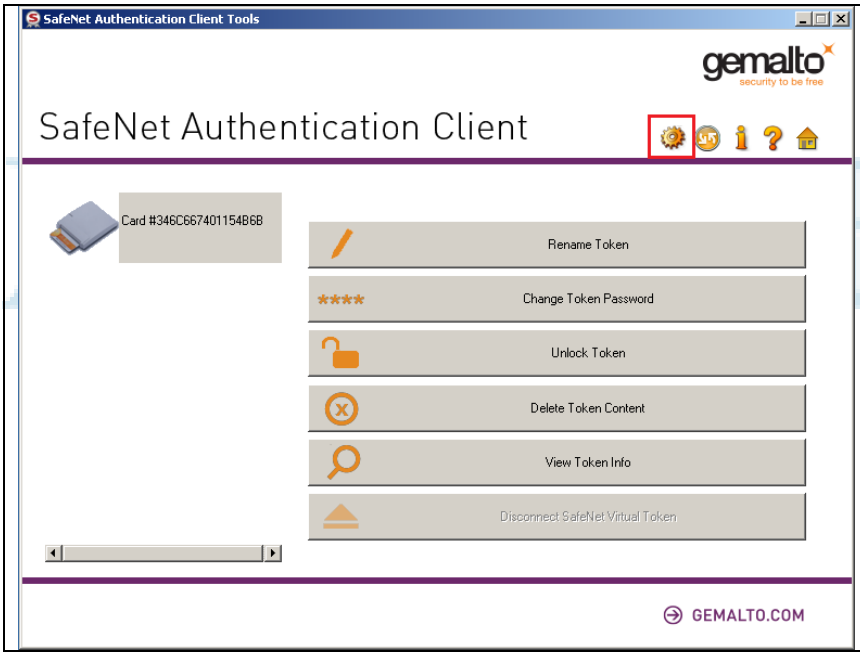
	Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.
	Επιλέγουμε το ένατο εικονίδιο από τα αριστερά.
	Καταχωρούμε τον κωδικό διαχειριστή (από προεπιλογή σαράντα οκτώ μηδενικά) και κάνουμε κλικ στο κουμπί OK.



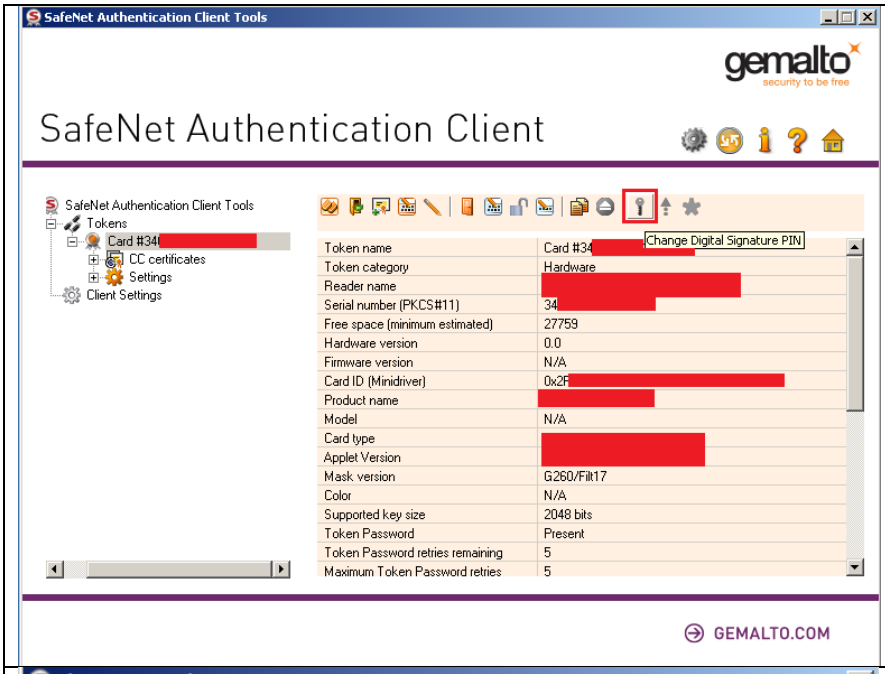
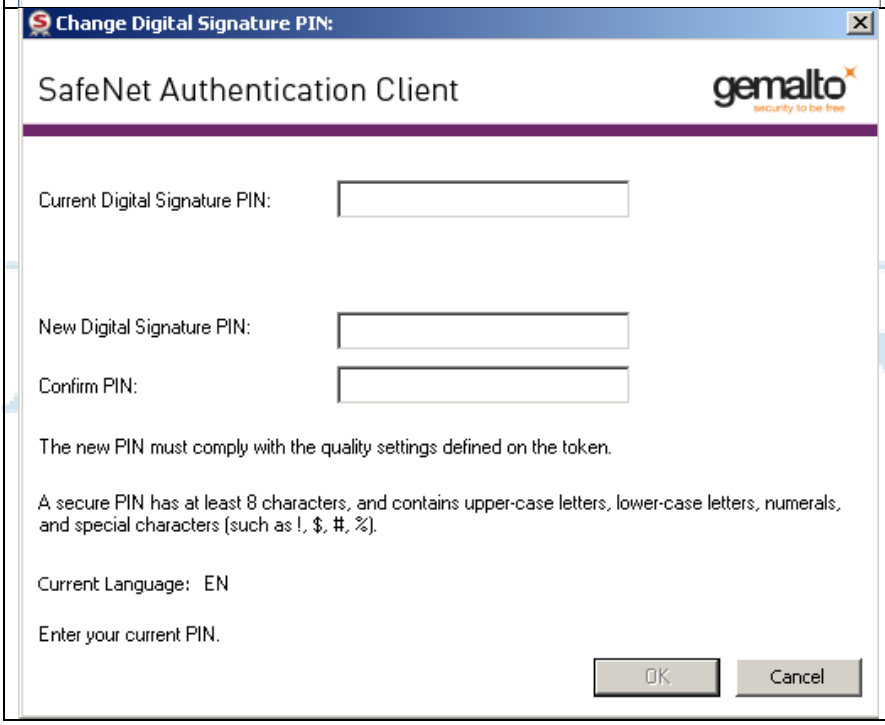
Στην επόμενη οθόνη καταχωρούμε το νέο κωδικό Token που επιθυμούμε (πεδίο Token Password) και τον επιβεβαιώνουμε (πεδίο Confirm Password).

Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

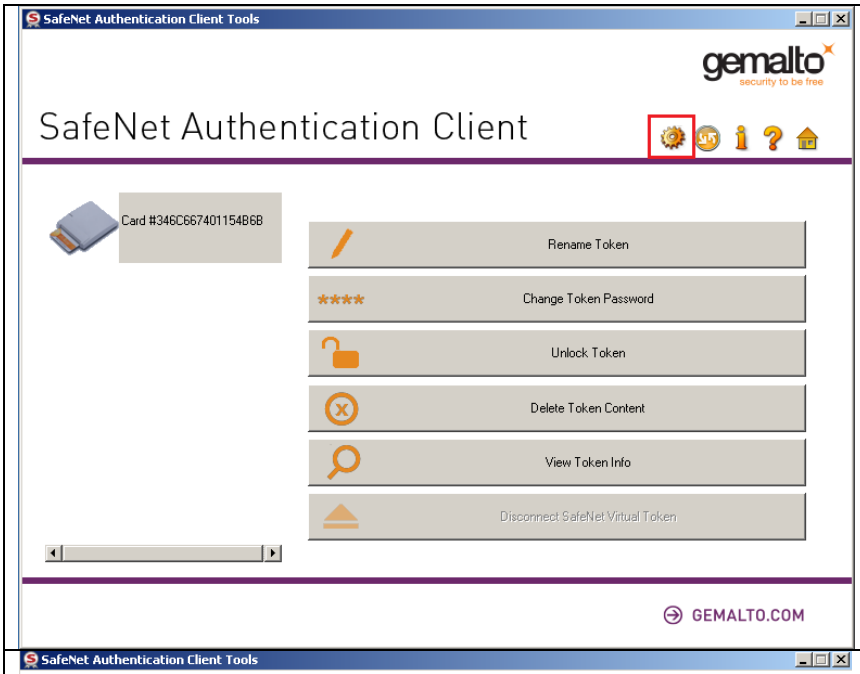
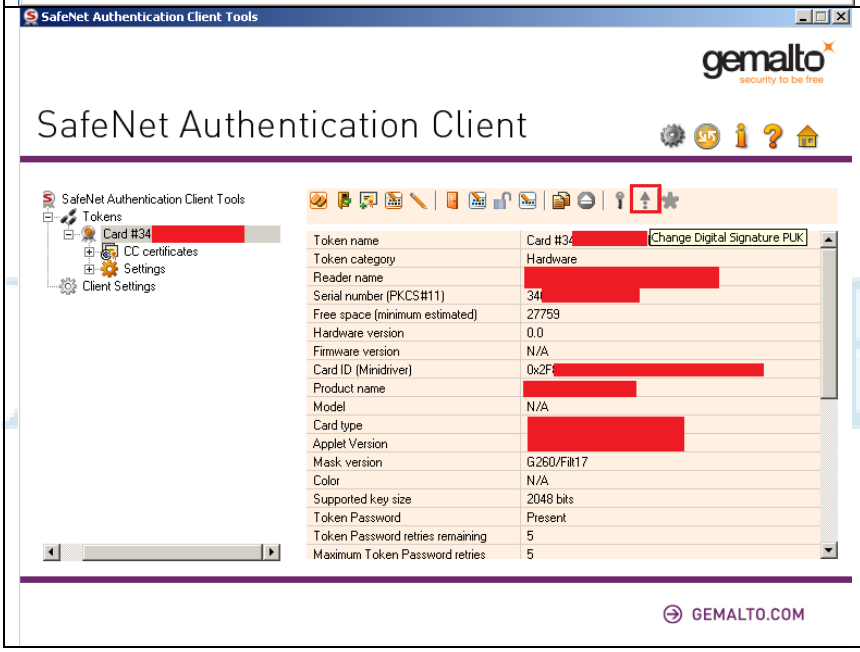
Πως αλλάζω τον κωδικό ψηφιακής υπογραφής (Digital Signature PIN).

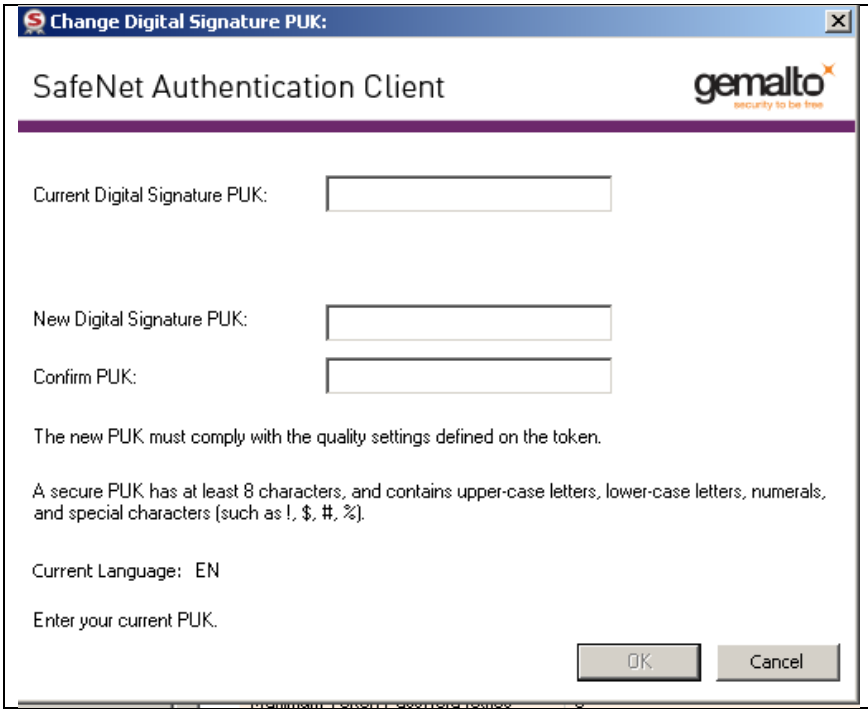


Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.

	Επιλέγουμε το δωδέκατο εικονίδιο από τα αριστερά.
	**Current Digital Signature PIN:** Εδώ καταχωρούμε τον τρέχον κωδικό ψηφιακής υπογραφής (από προεπιλογή έξι μηδενικά 000000). **New Digital Signature PIN:** Εδώ καταχωρούμε το νέο κωδικό ψηφιακής υπογραφής. **Confirm PIN:** Εδώ επιβεβαιώνουμε το νέο κωδικό ψηφιακής υπογραφής. Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

Πως αλλάζω τον κωδικό διαχειριστή ψηφιακής υπογραφής (Digital Signature PUK).

	Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.
	Επιλέγουμε το δέκατο τρίτο εικονίδιο από τα αριστερά.

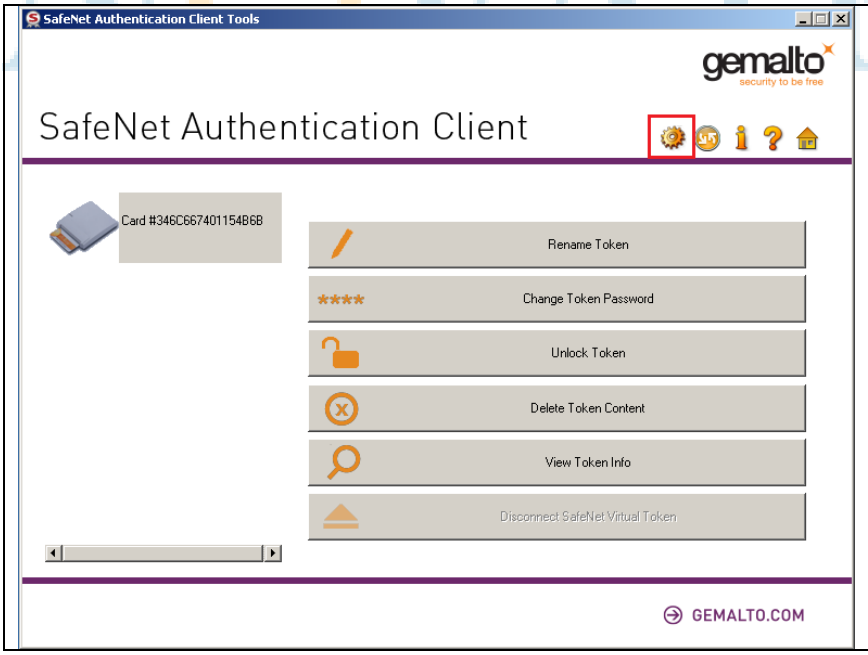


Current Digital Signature PUK: Εδώ καταχωρούμε τον τρέχον κωδικό διαχειριστή ψηφιακής υπογραφής (από προεπιλογή έξι μηδενικά 000000).
New Digital Signature PUK: Εδώ καταχωρούμε το νέο κωδικό διαχειριστή ψηφιακής υπογραφής.
Confirm PUK: Εδώ επιβεβαιώνουμε το νέο κωδικό διαχειριστή ψηφιακής υπογραφής.

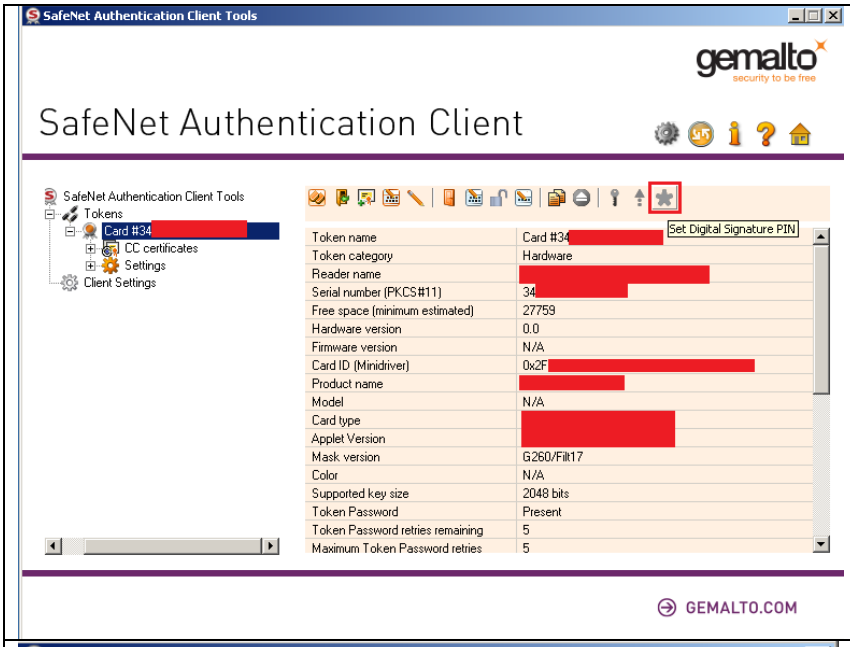
Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

Πως ξεκλειδώνω τον κωδικό ψηφιακής υπογραφής (PIN) με τη χρήση του κωδικού διαχειριστή (PUK).

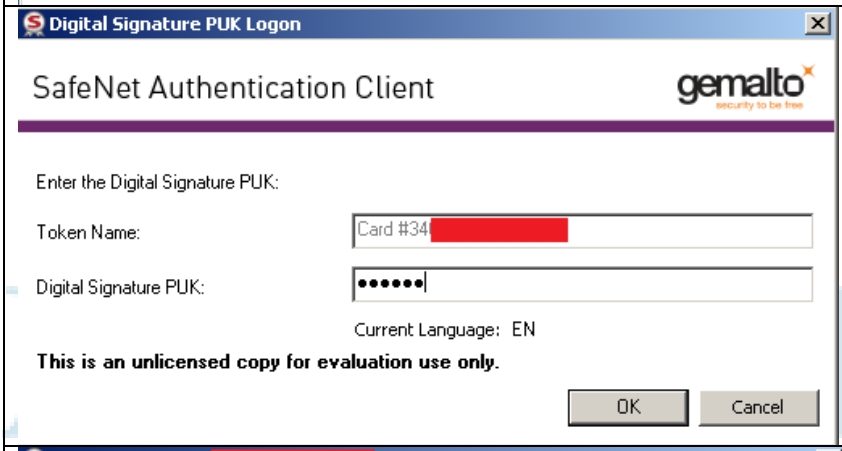
Σε περίπτωση που κλειδώσει ο κωδικός χρήστη ψηφιακής υπογραφής (PIN) μπορούμε να τον ξεκλειδώσουμε με τη χρήση του κωδικού διαχειριστή ψηφιακής υπογραφής (PUK) ακολουθώντας τα παρακάτω βήματα.



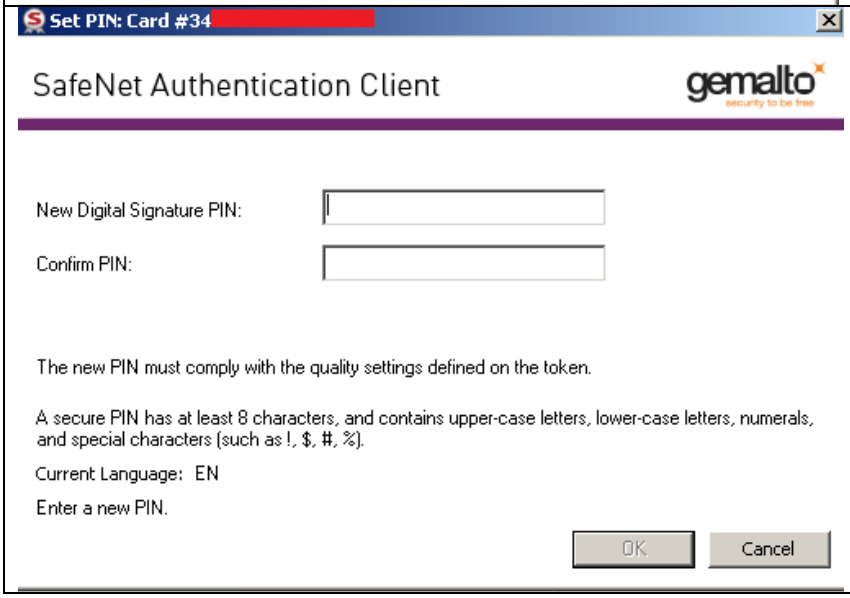
Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.



Επιλέγουμε το τελευταίο εικονίδιο από τα αριστερά.



Καταχωρούμε τον κωδικό διαχειριστή ψηφιακής υπογραφής (από προεπιλογή έξι μηδενικά 000000) και κάνουμε κλικ στο κουμπί OK.



New Digital Signature PIN: Εδώ καταχωρούμε το νέο κωδικό ψηφιακής υπογραφής.
Confirm PIN: Εδώ επιβεβαιώνουμε το νέο κωδικό ψηφιακής υπογραφής.

Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.