

NOVATRON®

Διαχείριση και Εγκατάσταση

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



NOVATRON®

Περιεχόμενα

Τεχνικά χαρακτηριστικά	3
Εισαγωγή	4
Κωδικοί PIN / PUK.....	4
Βήμα 1ο: Προμήθεια USB Token	4
Βήμα 2ο: Ηλεκτρονική αίτηση μέσω της Πύλης ΕΡΜΗΣ	4
Βήμα 3ο: Μετάβαση σε ΚΕΠ.....	9
Βήμα 4ο: Έλεγχος προδιαγραφών και προετοιμασία υπολογιστή.	11
Έλεγχος έκδοσης Internet Explorer.	11
Εγκατάσταση των ψηφιακών πιστοποιητικών των Αρχών Πιστοποίησης και Χρονοσήμανσης, παραμετροποίηση του Internet Explorer	15
Βήμα 5ο: Εγκατάσταση του Safenet Authentication Client (πρόγραμμα οδήγησης του USB Token).....	17
Βήμα 6ο: Έκδοση προσωπικών Ψηφιακών Πιστοποιητικών – Εγκατάσταση αυτών στο USB Token.	20
Ψηφιακή Υπογραφή με το πρόγραμμα JsignPdf.	25
Παράρτημα: Διαχείριση κωδικών και περιεχομένων της συσκευής.....	31
Πως αλλάζω τον κωδικό του Token (Token Password)?	31
Πως αλλάζω το κωδικό διαχειριστή του Token (Administrator Password)?.....	32
Πως ξεκλειδώνω τον κωδικό του Token με τη χρήση του κωδικού διαχειριστή (Unlock Token).....	33
Πως αλλάζω τον κωδικό ψηφιακής υπογραφής (Digital Signature PIN).....	35
Πως αλλάζω τον κωδικό διαχειριστή ψηφιακής υπογραφής (Digital Signature PUK).....	36
Πως ξεκλειδώνω τον κωδικό ψηφιακής υπογραφής (PIN) με τη χρήση του κωδικού διαχειριστή (PUK).....	38

ID Bridge K30.

Operating systems supported	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Plug and Play CCID (Chip Card Interface Device) USB 2.0 full speed (12 Mbps)
Human interface	<ul style="list-style-type: none"> LED one color (Blue), dual state (blinking: waiting card insertion; ON: card reading / writing)
Environmental	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> +/- 8kV direct air discharge +/- 4kV indirect contact discharge

ID Prime 840 smart card (eIDAS Compliant)

Product characteristics	
Memory	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> BaseCSP Minidriver v7 (IDGo 800 Minidriver) CSP and PKCS#11 (SafeNet Authentication Client)
Cryptographic algorithms	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> T=0, T=1, PPS, with baud up to 230 Kbps
Other features	<ul style="list-style-type: none"> Onboard PIN Policy Multi-PIN support
Chip characteristics	
Technology	<ul style="list-style-type: none"> Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	<ul style="list-style-type: none"> Minimum 500,000 write/erase cycles Data retention for minimum 25 years
Certification	<ul style="list-style-type: none"> CC EAL5+
Security	<ul style="list-style-type: none"> 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



Εθνική Πύλη ΕΡΜΗΣ
πάνω από 100 πιστοποιητικά
μέσω διαδικτύου

ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗ ΘΥΡΙΔΑ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ ΥΠΗΡΕΣΙΕΣ ΑΛΛΩΝ ΦΟΡΕΩΝ

Είστε εδώ: Αρχική σελίδα / Αρχική σελίδα

Η Πύλη «ΕΡΜΗΣ» αποτελεί την Κεντρική Διαδικτυακή Πύλη της δημόσιας διοίκησης, παρέχοντας στους πολίτες και τις επιχειρήσεις πληροφόρηση και ηλεκτρονικές υπηρεσίες.



Οι ηλεκτρονικές υπηρεσίες του ΕΡΜΗ χωρίζονται σε δύο κατηγορίες:



ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
Κατηγορία 01
>>>

Ηλεκτρονικές Υπηρεσίες - Όχι άμεση παραλαβή αποτελέσματος
Εδώ υποβάλλετε ηλεκτρονικές αιτήσεις για υπηρεσίες της δημόσιας διοίκησης, παραλαμβάνοντας το αποτέλεσμα (πιστοποιητικό, βεβαίωση, κλπ) είτε από την ηλεκτρονική σας θυρίδα είτε από το ΚΕΠ που δηλώνετε.

Επίκαιρες ανακοινώσεις

03/11/15

259η ηλεκτρονική έκδοση εβδομαδιαίας εφημερίδας "ΔΗΜΟΣΙΟΓΡΑΦΙΚΑ"

26/10/15

Στη συνέχεια επιλέγουμε το σύνδεσμο Είσοδος.

Είσοδος στο Σύστημα

Είσοδος με κωδικούς TAXISnet

Είσοδος με Κωδικούς ΕΡΜΗ

Είσοδος με Κωδικούς Εidas

Σύνδεση χρηστών στην πύλη ΕΡΜΗΣ μέσω της υπηρεσίας του Taxisnet.

Για να εισέλθετε στην πύλη ΕΡΜΗΣ απαιτείται πιστοποίηση. Η πιστοποίηση είναι απλή και συνίσταται σε δύο ενέργειες:

- 1 Επιλέγετε "Είσοδος".
- 2 Προωθείτε στην υπηρεσία πιστοποίησης της ΓΓΔΕ όπου εισάγετε τους προσωπικούς σας κωδικούς TAXISNET.

Είσοδος

Στη συνέχεια πληκτρολογούμε τους προσωπικούς κωδικούς TAXISnet και επιλέγουμε Είσοδος.

ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΗΜΟΣΙΩΝ ΕΣΟΔΩΝ 

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ 
Υπουργείο Οικονομικών

http://www.ermis.gov.gr ΟΝ ΛΙΝΕ υπηρεσίες

**ΚΑΛΩΣ ΗΛΘΑΤΕ ΣΤΗΝ ΣΕΛΙΔΑ ΕΙΣΟΔΟΥ ΤΩΝ ΥΠΗΡΕΣΙΩΝ WEB.
ΠΑΡΑΚΑΛΟΥΜΕ ΕΙΣΑΓΕΤΕ ΤΟΥΣ ΚΩΔΙΚΟΥΣ TAXISNET ΓΙΑ ΤΗΝ ΕΙΣΟΔΟ ΣΑΣ ΣΤΟ ΣΥΣΤΗΜΑ**

Username:

Password:

Επιλέγουμε Εξουσιοδότηση, όπως βλέπουμε την παρακάτω εικόνα.

ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΗΜΟΣΙΩΝ ΕΣΟΔΩΝ 

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ 
Υπουργείο Οικονομικών

http://www.ermis.gov.gr ΟΝ ΛΙΝΕ υπηρεσίες ΥΠΗΡΕΣΙΕΣ WEB

ΓΓΔΕ - ΚΑΛΩΣ ΗΛΘΑΤΕ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ WEB
Παρακαλούμε επιβεβαιώστε:

Εξουσιοδοτώ τον εξοπλιστή του συστήματος "Ερμής" να προσπελάσει στοιχεία μου (ΑΦΜ, Στοιχεία Ταυτότητας) που τηρούνται στη ΓΓΔΕ

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

Ermis. Εθνική Πύλη Δημόσιας Διοίκησης 
www.ermis.gov.gr **ΚΕΠ**

Πληκτρολογήστε το email σας

Email*

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.

Καλώς ήρθατε : ermis_

ΕΛ | EN | FR | DE

Λειτουργίες της πύλης

- Πίνακας Ελέγχου
- Προσωπική Σελίδα
- Ηλεκτρονική Θυρίδα
- Αποσύνδεση

Ermis.
www.ermis.gov.gr

Σχετικά με την πύλη

Εθνική Πύλη ΕΡΜΗΣ
πάνω από **100** πιστοποιητικά
μέσω **διαδικτύου**



ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗ ΘΥΡΙΔΑ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ ΥΠΗΡΕΣΙΕΣ ΑΛΛΩΝ ΦΟΡΕΩΝ

Επιλέγουμε το σύνδεσμο Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών.

NOVATRON®

Πίνακας ελέγχου χρήστη

Διαχείριση του προφίλ σας

Σελίδα όπου οι χρήστες μπορούν να τροποποιήσουν τα προσωπικά τους στοιχεία και τα στοιχεία επικοινωνίας.

Αλλαγή κωδικού πρόσβασης

Σελίδας αλλαγής κωδικού πρόσβασης

Διαχείριση προσωπικών ψηφιακών πιστοποιητικών

Εδώ μπορείτε να παρακολουθήσετε τον κύκλο ζωής των προσωπικών σας ψηφιακών πιστοποιητικών αυθεντικοποίησης/υπογραφής και κρυπτογραφησης.

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

Διαχείριση ψηφιακών πιστοποιητικών χρήστη

Ηλεκτρονική Υποβολή Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών

Στην Εθνική Πύλη Ερμής μπορείτε να εκδώσετε τα παρακάτω δύο πιστοποιητικά προσθέτοντας έτσι μεγαλύτερη ασφάλεια στις ηλεκτρονικές σας συναλλαγές με τη Δημόσια Διοίκηση.

Πιστοποιητικό αυθεντικοποίησης - ηλεκτρονικής υπογραφής

Το πιστοποιητικό αυτό μπορείτε να το χρησιμοποιήσετε για την είσοδό σας στην Εθνική Πύλη Ερμής αντί για το όνομα χρήστη και τον κωδικό πρόσβασης. Παράλληλα μπορείτε να υπογράψετε ψηφιακά τα δεδομένα που υποβάλετε κατά την εκτέλεση ηλεκτρονικών υπηρεσιών μέσω του Ερμή διασφαλίζοντας έτσι την ταυτότητα του υποβάλλοντος και την ακεραιότητα των δεδομένων.

Πιστοποιητικό κρυπτογράφησης

Το πιστοποιητικό αυτό μπορείτε να το χρησιμοποιείτε για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων στις ηλεκτρονικές σας συναλλαγές τόσο με τον Ερμή όσο και με άλλους πολίτες.

Αφού υποβάλετε το αίτημα με επιτυχία θα σας δωθούν οδηγίες για τα επόμενα βήματα που πρέπει να ακολουθήσετε μέχρι την τελική έκδοση των ψηφιακών πιστοποιητικών.

Παρακάτω επιλέξτε αν επιθυμείτε ή όχι την προσθήκη της ηλεκτρονικής σας διεύθυνσης στα ψηφιακά πιστοποιητικά που θα εκδώσετε. Σε περίπτωση που επιλέξετε να μην προστεθεί η ηλεκτρονική σας διεύθυνση δε θα έχετε τη δυνατότητα να χρησιμοποιείτε τα πιστοποιητικά σας για να υπογράψετε ψηφιακά ή να κρυπτογραφήτε μηνύματα ηλεκτρονικής αλληλογραφίας.

Δεν επιθυμώ την προσθήκη της ηλεκτρονικής μου διεύθυνσης στα ψηφιακά πιστοποιητικά

Υποβολή

Λαμβάνουμε το παρακάτω μήνυμα.

Διαχείριση ψηφιακών πιστοποιητικών χρήστη

Η ηλεκτρονική υποβολή αιτήματος έκδοσης ψηφιακών πιστοποιητικών ολοκληρώθηκε επιτυχώς.

Επόμενη ενέργεια:

Θα πρέπει να μεταβείτε σε οποιοδήποτε ΚΕΠ για την έγκριση του αιτήματος σας έχοντας μαζί σας τα απαραίτητα δικαιολογητικά. Η έγκριση του αιτήματος πραγματοποιείται στο ΚΕΠ άμεσα (κατά τη διάρκεια της επίσκεψής σας). Μετά την έγκριση μπορείτε να προχωρήσετε, χωρίς να αναμένετε κάποια ειδοποίηση, στην διαδικασία έκδοσης. Αναλυτικές πληροφορίες για τα παραπάνω αλλά και για όλα τα θέματα που αφορούν τις ψηφιακές υπογραφές μπορείτε να βρείτε στην ιστοσελίδα της Αρχής Πιστοποίησης [aped.gov.gr](http://www.aped.gov.gr)

Βήμα 3ο: Μετάβαση σε ΚΕΠ

Πηγαίνουμε σε οποιοδήποτε Κέντρο Εξυπηρέτησης Πολιτών για τη φυσική ταυτοποίησή μας, έχοντας μαζί μας την ταυτότητα (ή το διαβατήριό) 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_dilosoi.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:	<input type="text"/>	Επώνυμο:	<input type="text"/>
Όνομα και Επώνυμο Πατέρα:	<input type="text"/>		
Όνομα και Επώνυμο Μητέρας:	<input type="text"/>		
Ημερομηνία γέννησης (μορφής ηη/μμ/εεεε) ⁽¹⁾:	<input type="text"/>		
Αριθμός Δελτίου Ταυτότητας:	<input type="text"/>	Κινητό Τηλέφωνο (για λήψη sms) ⁽²⁾:	<input type="text"/>
Τόπος γέννησης:	<input type="text"/>		
Τόπος Κατοικίας (Δήμος/Κοινότητα):	<input type="text"/>		
Οδός:	<input type="text"/>	Αριθμός:	<input type="text"/> Τ.Κ.: <input type="text"/>
Αριθμός τηλεφώνου:	<input type="text"/>	Προσωπικό Ηλεκτρονικό Ταχυδρομείο (e-mail) ⁽³⁾:	<input type="text"/>
Όνομα χρήστη (username) στην πύλη ΕΡΜΗΣ:	<input type="text"/>		
Α.Μ.Κ.Α. ⁽⁴⁾:	<input type="text"/>	ΑΦΜ ⁽⁴⁾:	<input type="text"/> Άλλο: <input type="text"/>
Αριθμός σειριακού ΑΔΔΥ (έξυπνης κάρτας ή USB token) ⁽⁵⁾:	<input type="text"/>		

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

Φορέας:	<input type="text"/>		
Ταχυδρομική διεύθυνση Φορέα:	<input type="text"/>		
Τηλέφωνο :	<input type="text"/>	Αριθμός τηλεμοιτύπου (Fax) :	<input type="text"/>
Ηλεκτρονικό Ταχυδρομείο (e-mail) στον Φορέα:	<input type="text"/>		

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 ΑΔΔΥ, 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/ση Ηλεκτρ. Ταχυδρομείου (Email)
Έγγραφο ταυτοποίησης Χ: (Δελτίο Αστυνομικής / Στρατιωτικής Ταυτότητας)
Ιδιότητα Πολίτης
Σειριακός αριθμός συσκευής αποθήκευσης 2Α

Ο/Η ΔΗΛΩΝ/ΟΥΣΑ

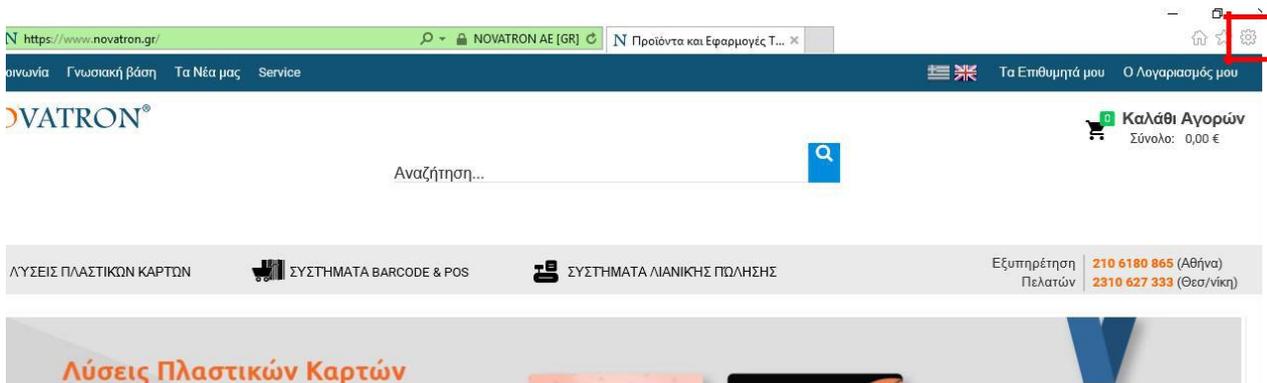
Ο/Η ΥΠΑΛΛΗΛΟΣ ΚΕΠ

Βήμα 4ο: Έλεγχος προδιαγραφών και προετοιμασία υπολογιστή.

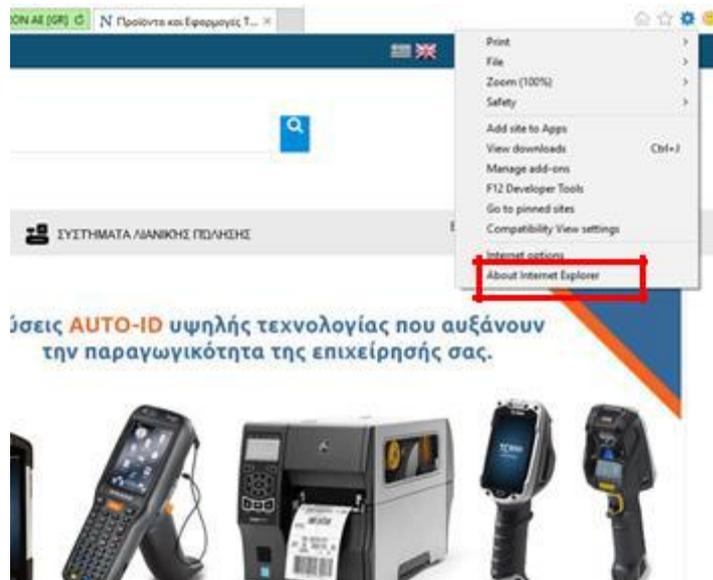
Βάσει των προδιαγραφών της κρατικής υπηρεσίας ανάπτυξης πληροφορικής για την ορθή εγκατάσταση των προσωπικών μας Ψηφιακών Πιστοποιητικών, είναι **υποχρεωτικό** να χρησιμοποιήσουμε υπολογιστή με **λειτουργικό σύστημα Windows 7 και Internet Explorer 8 ή 9 ή 10**. Η εγκατάσταση αυτή πραγματοποιείται μία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

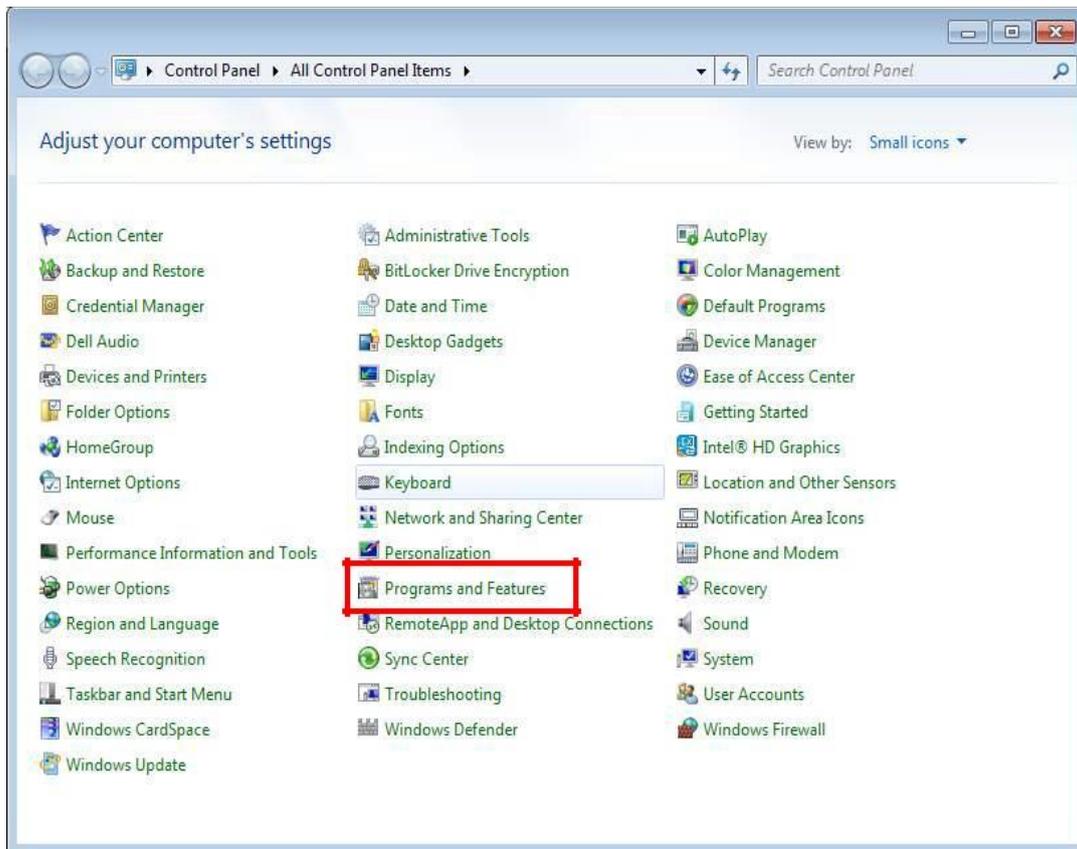


Λαμβάνουμε την πληροφορία για την έκδοση του προγράμματος.

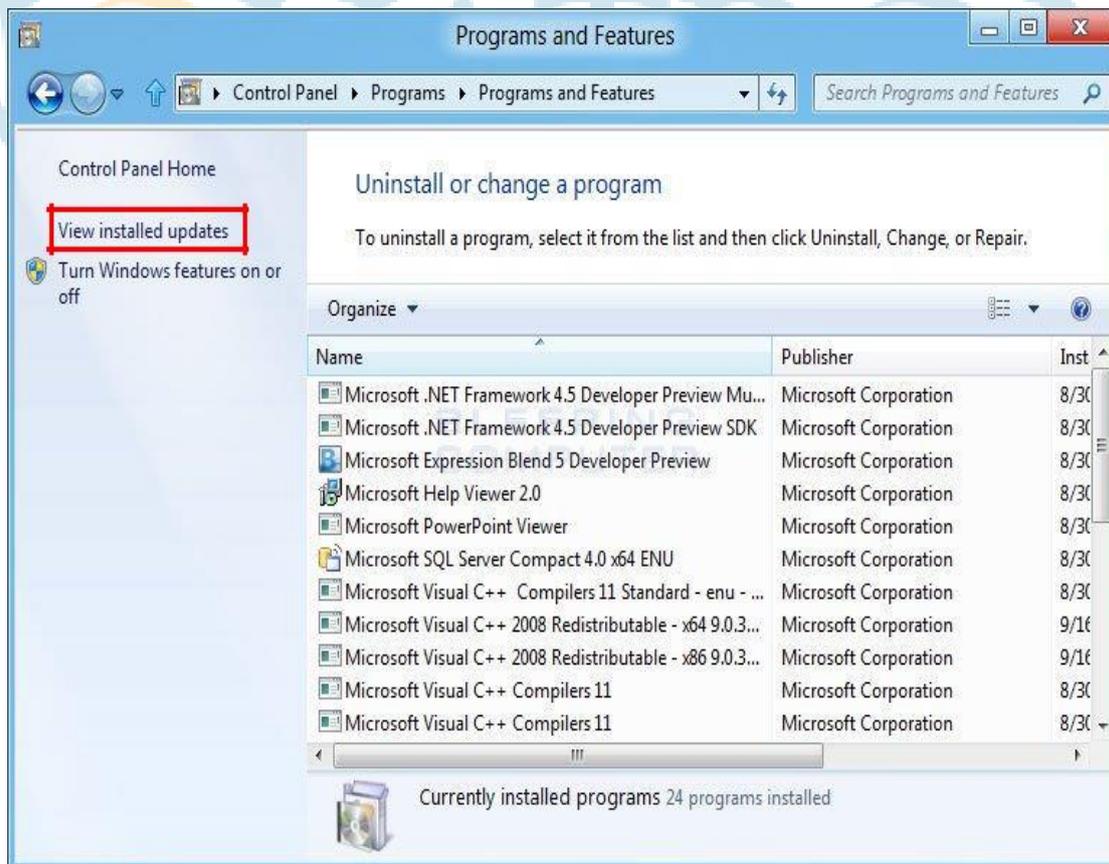


Αν στη προηγούμενη εικόνα λαμβάναμε τη πληροφορία ότι έχουμε έκδοση 8 ή 9 ή 10, παραλείπουμε τα παρακάτω και προχωράμε. Αν όμως έχουμε τον Internet Explorer 11 πρέπει να τον «υποβαθμίσουμε» με την παρακάτω διαδικασία.

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).



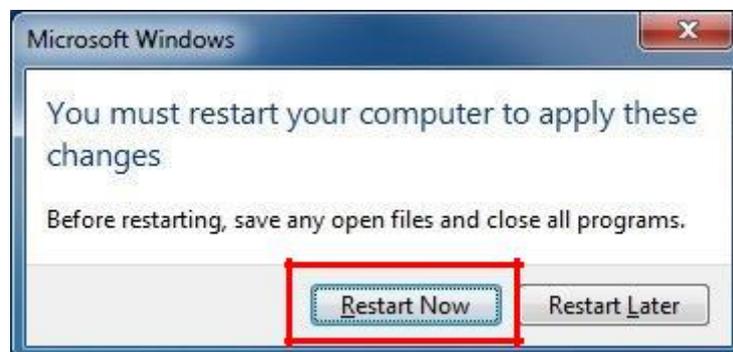
Και στη συνέχεια εντοπίζουμε και επιλέγουμε τον Internet Explorer 11 και πατάμε Κατάργηση Εγκατάστασης (Uninstall).



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 αποσεκάρουμε 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.

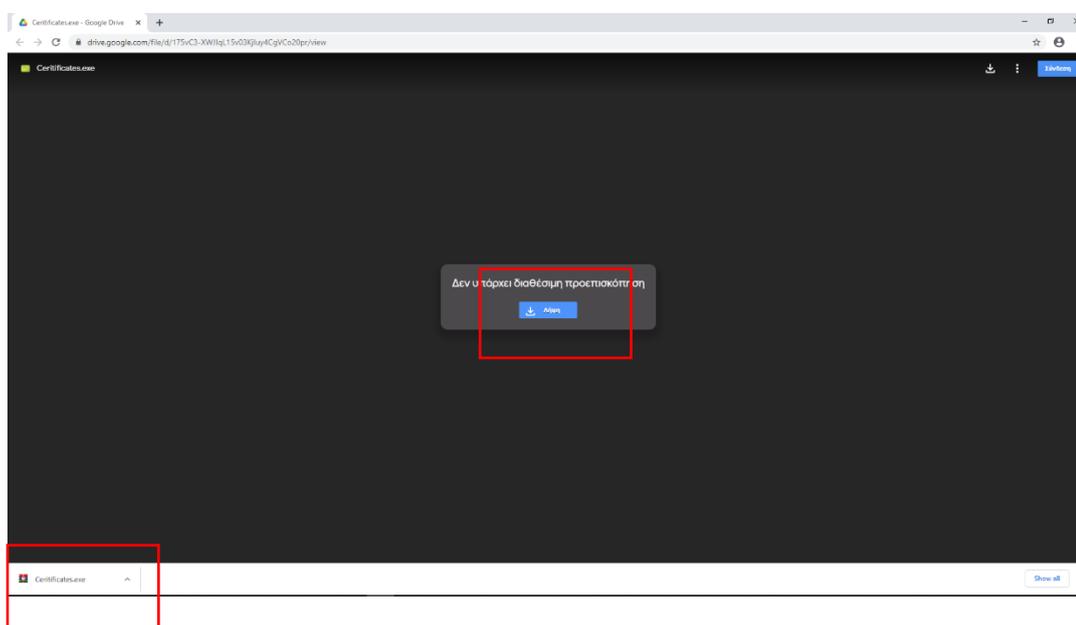
Εγκατάσταση των ψηφιακών πιστοποιητικών των Αρχών Πιστοποίησης και Χρονοσήμανσης, παραμετροποίηση του Internet Explorer

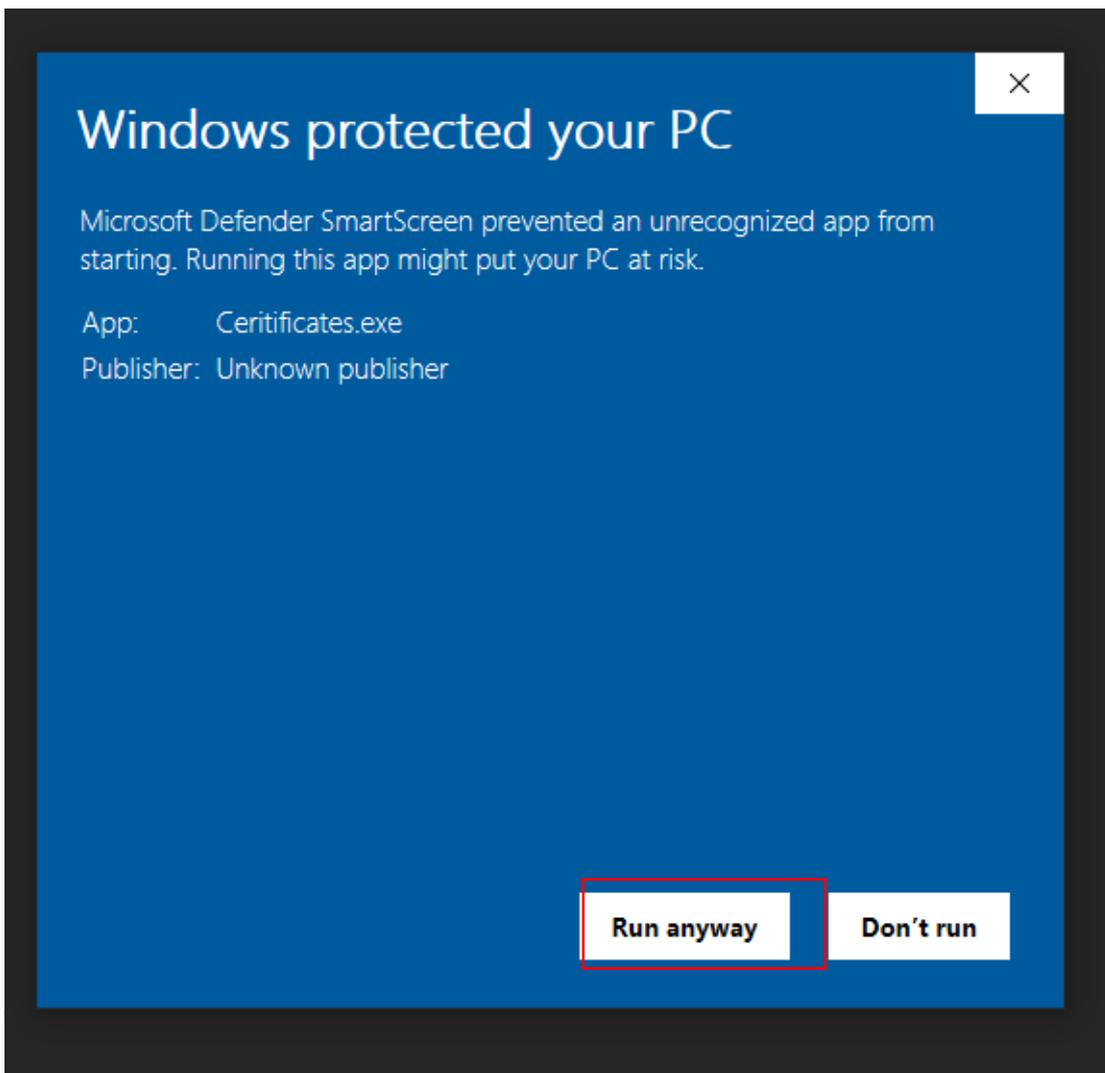
Αφού έχουμε προχωρήσει στην υποβάθμιση του Internet Explorer και έχουμε ελέγξει την έκδοση, κατεβάζουμε από τον παρακάτω σύνδεσμο το πρόγραμμα και το τρέχουμε, έχοντας αποσυνδεδεμένο το USB Token, έχοντας κλείσει και αποθηκεύσει τα προγράμματα και τα αρχεία στον υπολογιστή μας καθώς η εκτέλεση του προγράμματος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

[Win7-10 Certificates IE AdobeDC install Nov 2020.zip](#)

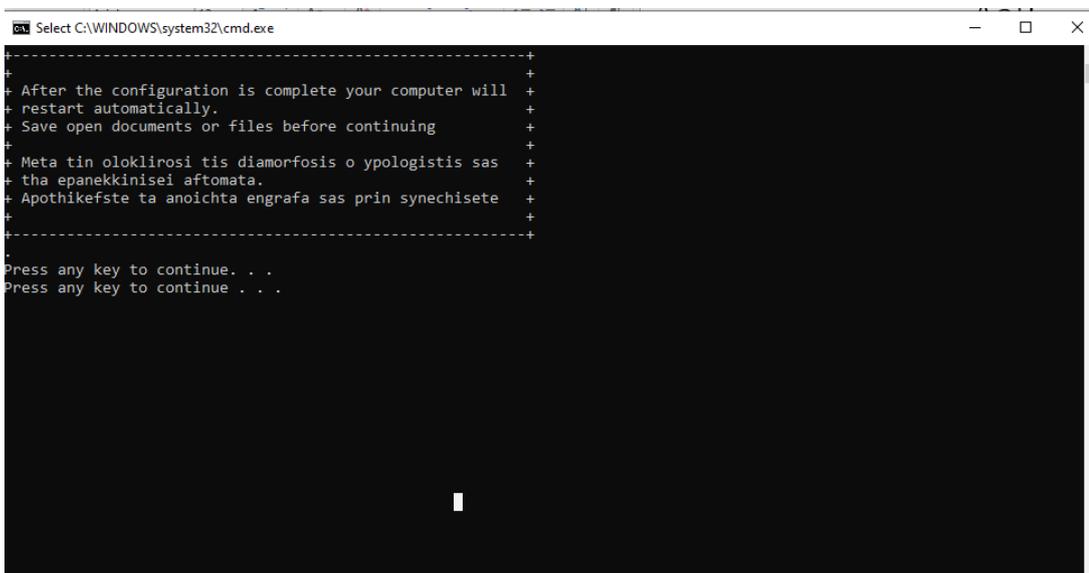
Κωδικός αποσυμπίεσης: 2020

Επιλέγουμε διαδοχικά:

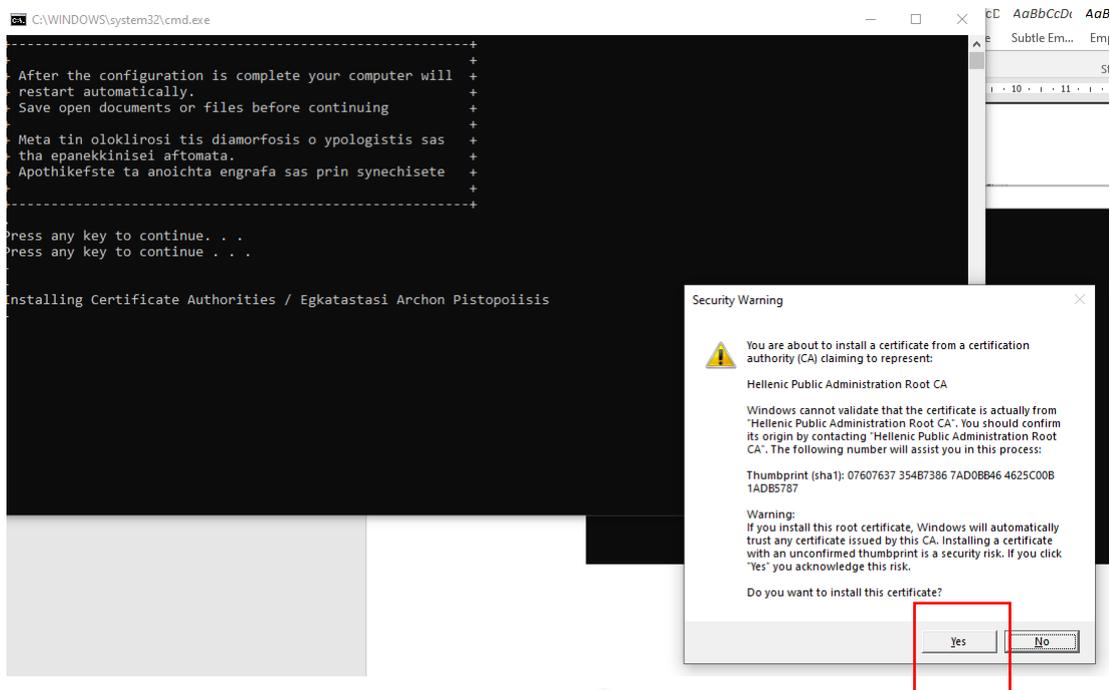




Πατάμε οποιοδήποτε πλήκτρο για να συνεχίσουμε πχ. Space



Επιλέγουμε Ναι σε όλα τα παράθυρα που θα εμφανιστούν



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

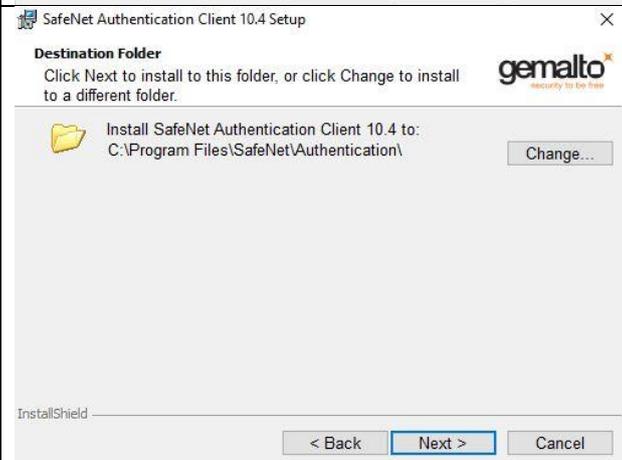
Βήμα 5ο: Εγκατάσταση του Safenet Authentication Client (πρόγραμμα οδήγησης του USB Token).

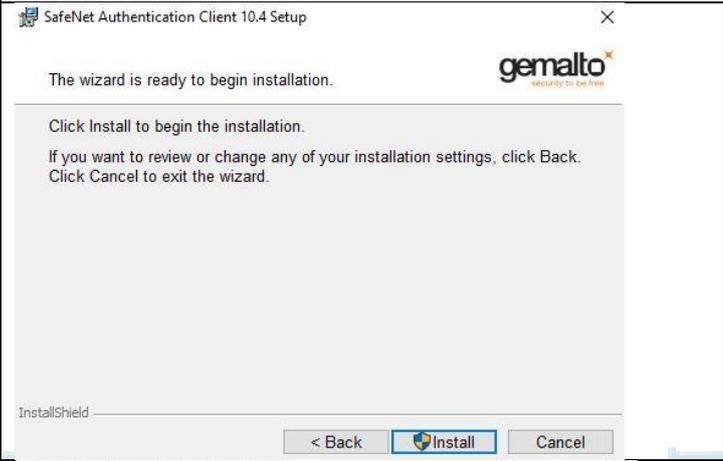
Οι οδηγοί (Driver & Middleware) είναι διαθέσιμοι στην ιστοσελίδα μας στην σελίδα του προϊόντος, στην καρτέλα σχετικά αρχεία ή στον παρακάτω σύνδεσμο:

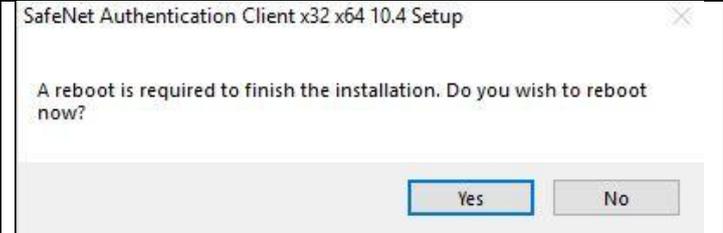
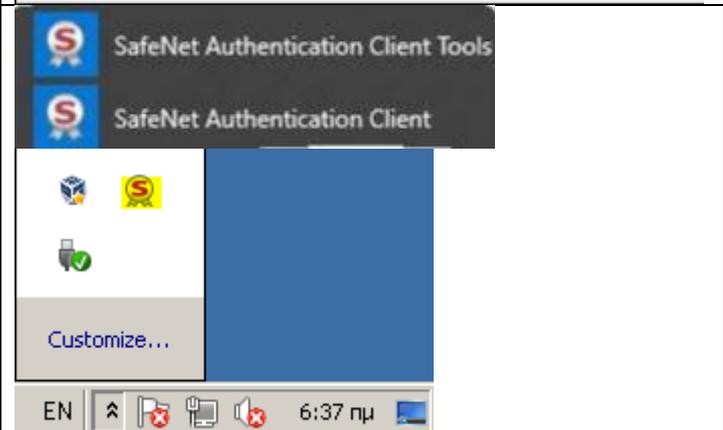
<https://drive.google.com/open?id=1mVR-QFRGSrqguhJfJ-ArJc7JrsyUMbKP>

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.
--	--

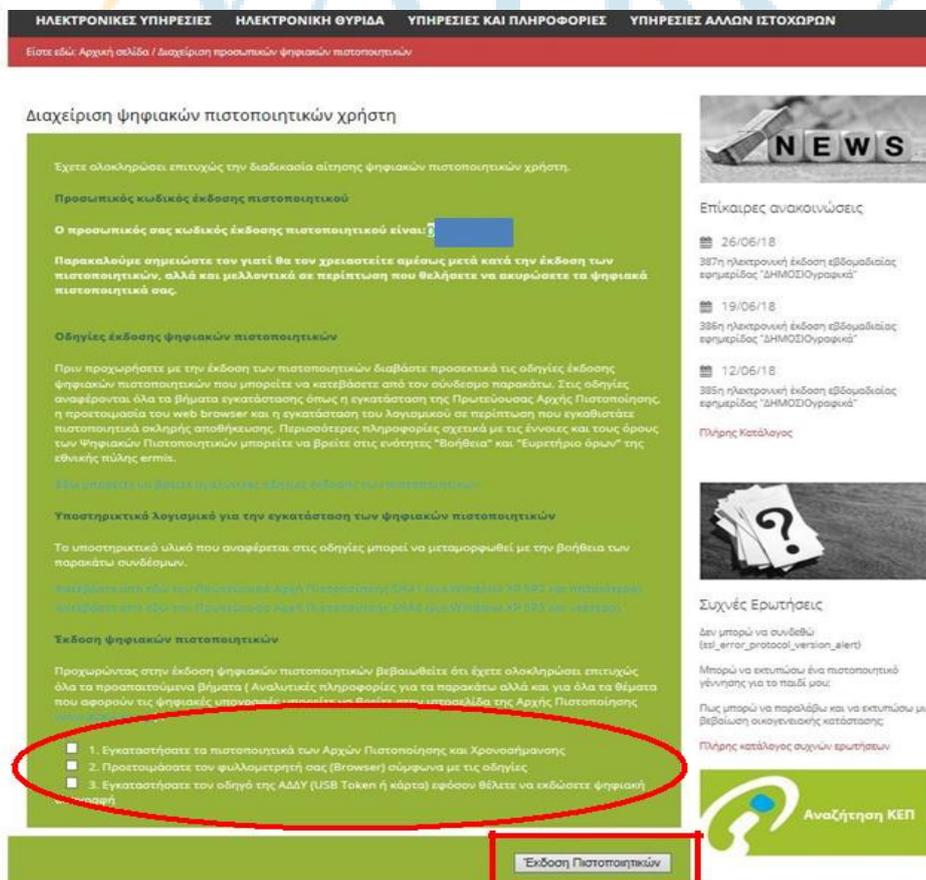
	<p>Στην επόμενη οθόνη επιλέγουμε Next.</p>
	<p>Επιλέγουμε τη γλώσσα εγκατάστασης και πατάμε το κουμπί Next.</p>
	<p>Αποδεχόμαστε τους όρους χρήσης και πατάμε το κουμπί Next.</p>
	<p>Επιλέγουμε τον προορισμό εγκατάστασης και πατάμε το κουμπί Next.</p>

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

	<p>Στο μήνυμα που ζητάει την επανεκκίνηση του υπολογιστή μας κάνουμε κλικ στο κουμπί Yes.</p>
	<p>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.</p>

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.



ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗ ΘΥΡΙΔΑ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΕΣ ΥΠΗΡΕΣΙΕΣ ΑΛΩΝ ΙΣΤΟΧΩΡΩΝ

Είστε εδώ: Αρχική σελίδα / Διαχείριση προσωπικών ψηφιακών πιστοποιητικών

Διαχείριση ψηφιακών πιστοποιητικών χρήστη

Έχετε ολοκληρώσει επιτυχώς την διαδικασία αίτησης ψηφιακών πιστοποιητικών χρήστη.

Προσωπικός κωδικός έκδοσης πιστοποιητικού

Ο προσωπικός σας κωδικός έκδοσης πιστοποιητικού είναι: [κωδικός]

Παρακαλούμε σημειώστε τον γιατί θα τον χρειαστείτε αμέσως μετά κατά την έκδοση των πιστοποιητικών, αλλά και μελλοντικά σε περίπτωση που θελήσετε να ακυρώσετε τα ψηφιακά πιστοποιητικά σας.

Οδηγίες έκδοσης ψηφιακών πιστοποιητικών

Πριν προχωρήσετε με την έκδοση των πιστοποιητικών διαβάστε προσεκτικά τις οδηγίες έκδοσης ψηφιακών πιστοποιητικών που μπορείτε να κατεβάσετε από τον σύνδεσμο παρακάτω. Στις οδηγίες αναφέρονται όλα τα βήματα εγκατάστασης όπως η εγκατάσταση της Πρωτεύουσας Αρχής Πιστοποίησης, η προετοιμασία του web browser και η εγκατάσταση του λογισμικού σε περίπτωση που εγκαθιστάτε πιστοποιητικά οκλήρης αποθήκευσης. Περισσότερες πληροφορίες σχετικά με τις έννοιες και τους όρους των Ψηφιακών Πιστοποιητικών μπορείτε να βρείτε στις ενότητες "Βοήθεια" και "Ευρετήριο όρων" της εθνικής πύλης ermis.

Εάν υπάρχει πρόβλημα εγκατάστασης ελάτε σε επικοινωνία με τον υπεύθυνο.

Υποστηρικτικό λογισμικό για την εγκατάσταση των ψηφιακών πιστοποιητικών

Το υποστηρικτικό υλικό που αναφέρεται στις οδηγίες μπορεί να μεταμορφωθεί με την βοήθεια των παρακάτω συνδέσμων.

Παράρτημα στο τέλος του Πρωτοκόλλου Καταχώρησης ΠΣΑ (προσβάσιμο από την ιστοσελίδα πιστοποίησης) που αφορά τον Πρωτόκολλο Καταχώρησης και Πιστοποίησης αλλά και τον ΠΣΑ (αν υπάρχει).

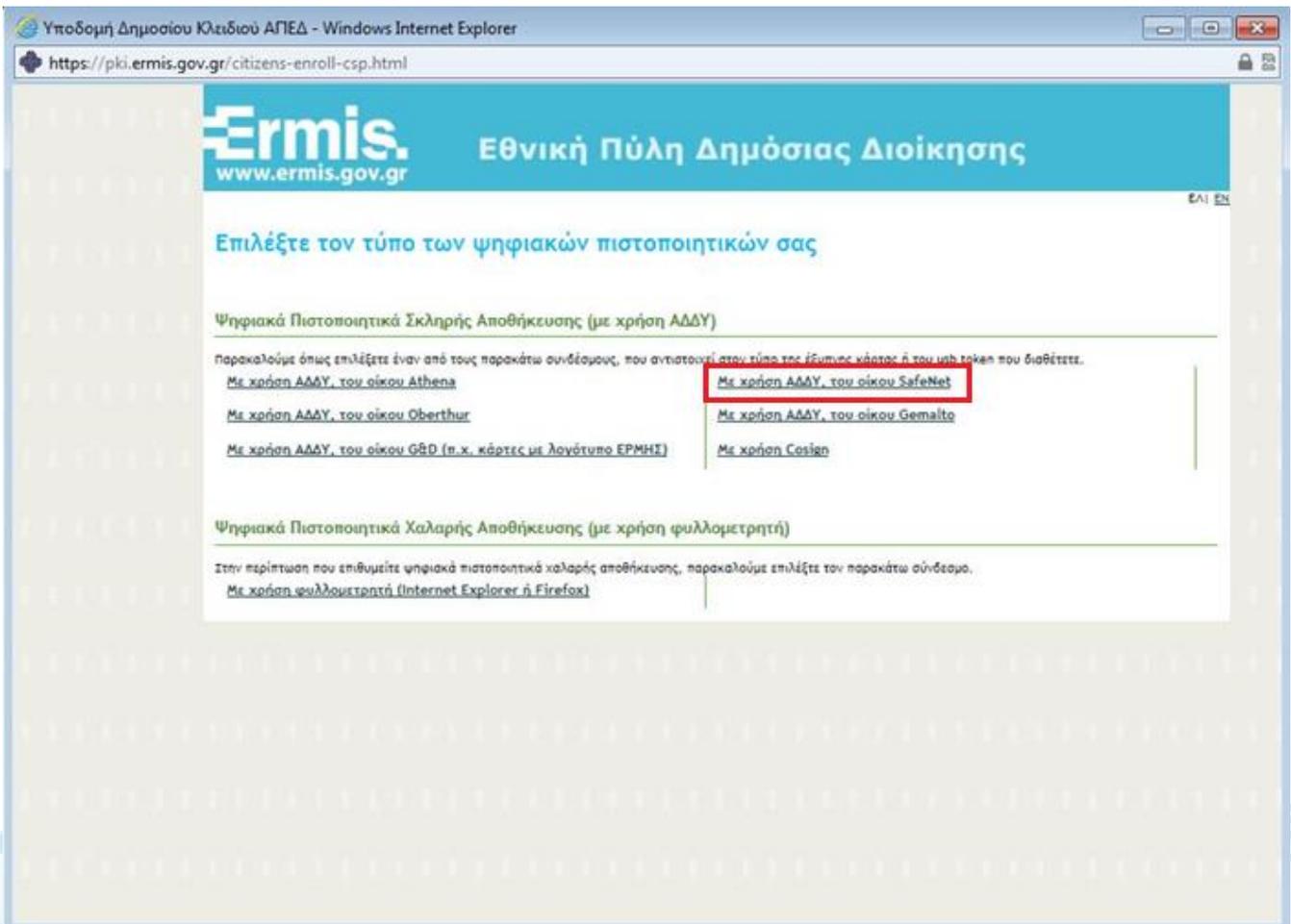
Έκδοση ψηφιακών πιστοποιητικών

Προχωρώντας στην έκδοση ψηφιακών πιστοποιητικών βεβαιωθείτε ότι έχετε ολοκληρώσει επιτυχώς όλα τα προαπαιτούμενα βήματα (Αναλυτικές πληροφορίες για τα παρακάτω αλλά και για όλα τα θέματα που αφορούν τις ψηφιακές υπογραφές μπορείτε να βρείτε στην ιστοσελίδα της Αρχής Πιστοποίησης).

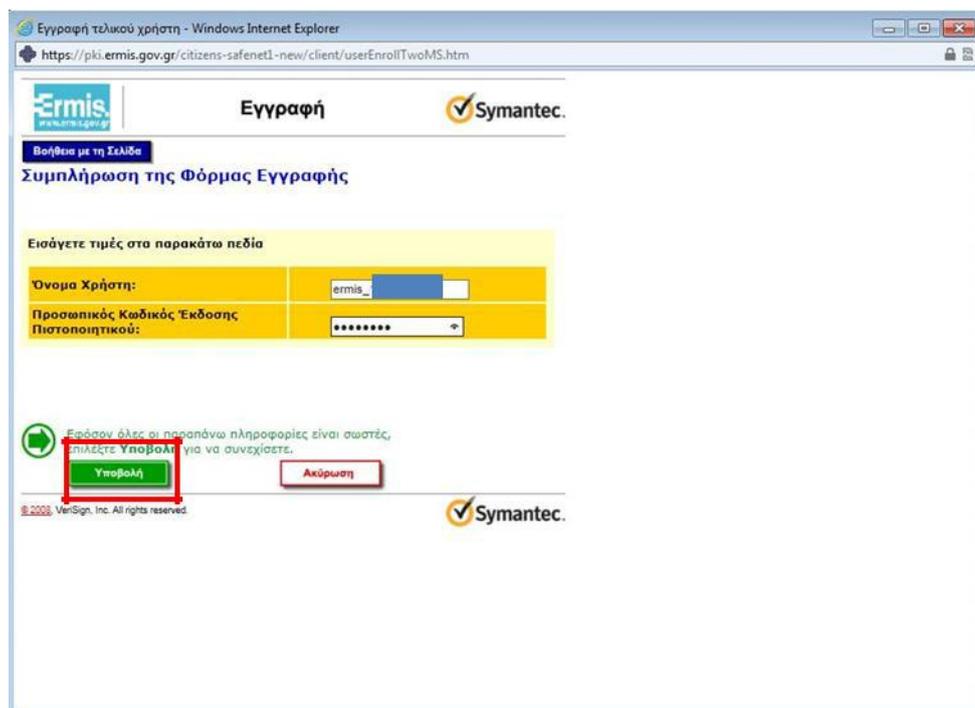
- 1. Εγκαταστήστε τα πιστοποιητικά των Αρχών Πιστοποίησης και Χρονοσήμανσης
- 2. Προετοιμάστε τον φυλλομετρητή σας (Browser) σύμφωνα με τις οδηγίες
- 3. Εγκαταστήστε τον οδηγό της ΑΔΔΥ (USB Token ή κάρτα) εφόσον θέλετε να εκδώσετε ψηφιακά πιστοποιητικά

Έκδοση Πιστοποιητικών

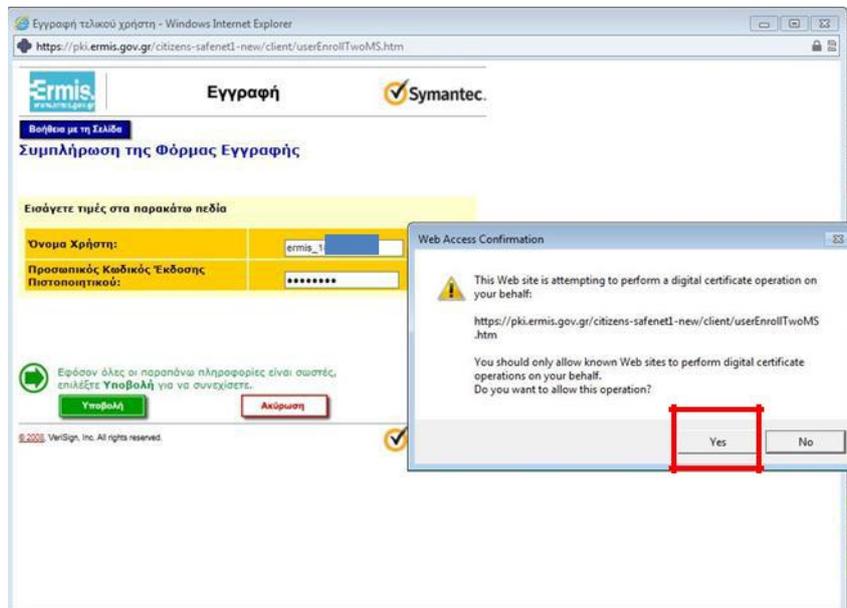
Ανοίγει η ακόλουθη καρτέλα όπου επιλέγουμε Με χρήση ΑΔΔΥ, του οίκου **Safenet** (Προσοχή, όχι Gemalto).



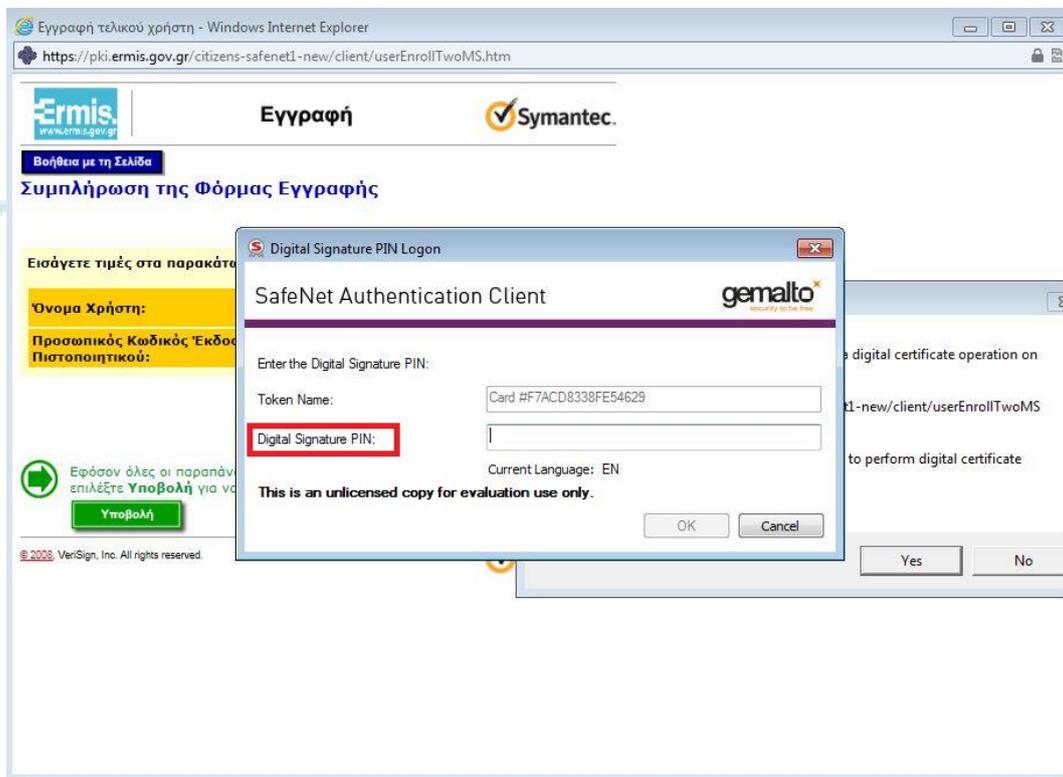
Τώρα εμφανίζεται σελίδα με δύο πεδία. Το πρώτο πεδίο θα πρέπει να συμπληρωθεί με το όνομα χρήστη που έχουμε στη Πύλη ΕΡΜΗΣ (ermis_), ενώ στο πεδίο Προσωπικός Κωδικός Έκδοσης Πιστοποιητικού πληκτρολογούμε τον οκταψήφιο κωδικό και στη συνέχεια πατάμε το κουμπί Υποβολή.



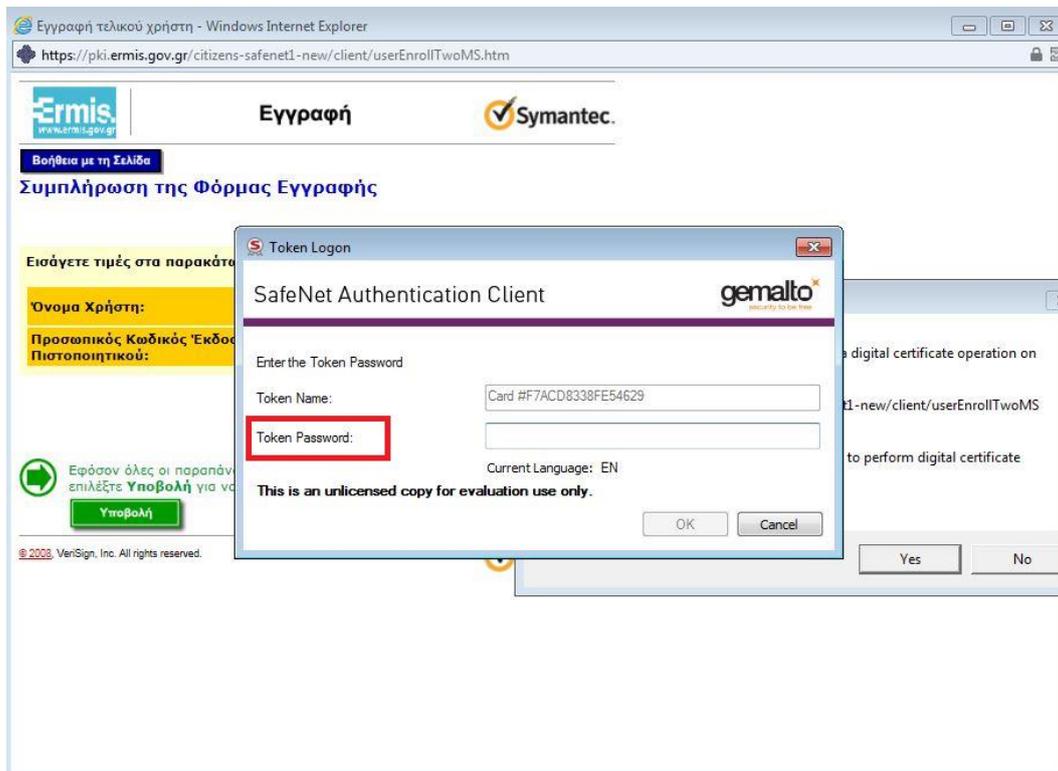
Στη συνέχεια πατάμε Yes στο μήνυμα της παρακάτω εικόνας, καθώς και σε όσα παρόμοια μηνύματα παρουσιαστούν.



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).

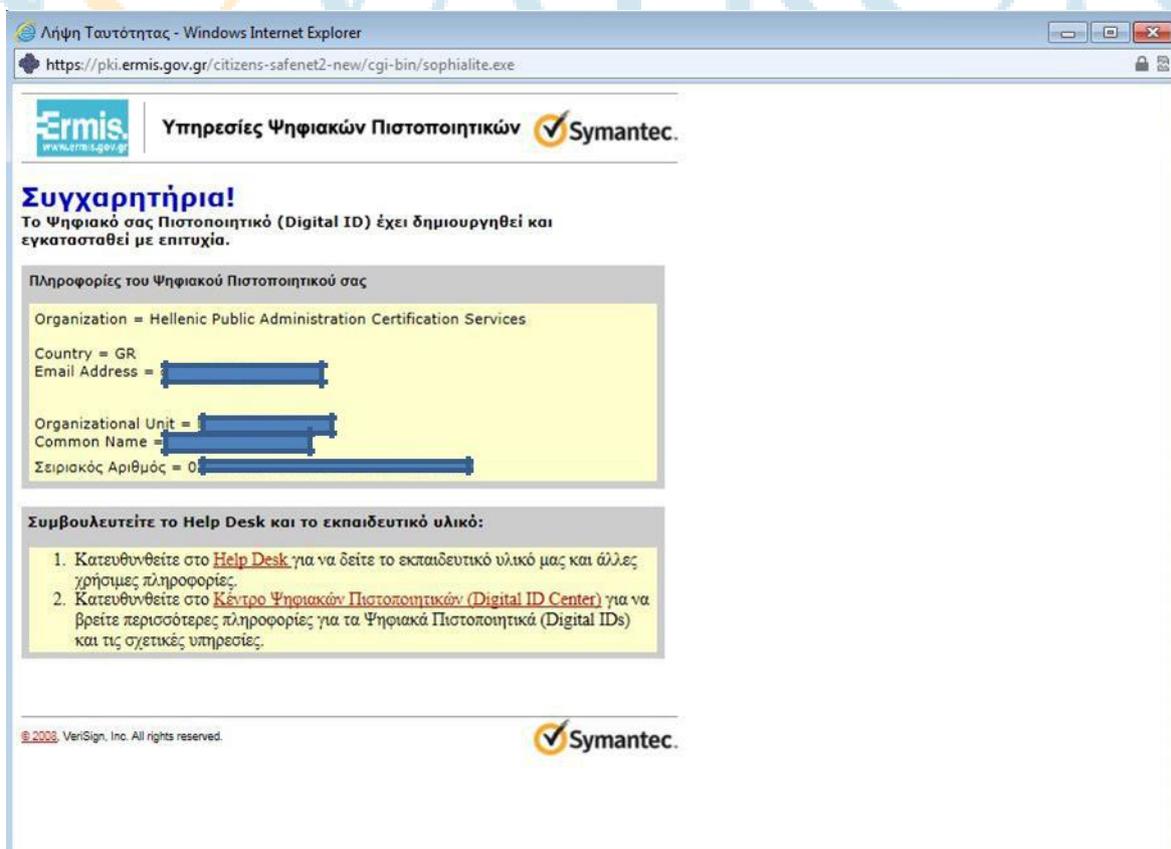


Επίσης αρκετές φορές μέσα στην διαδικασία εγκατάστασης θα μας ζητηθεί το Token Password το οποίο είναι τέσσερα (4) μηδενικά (0000)

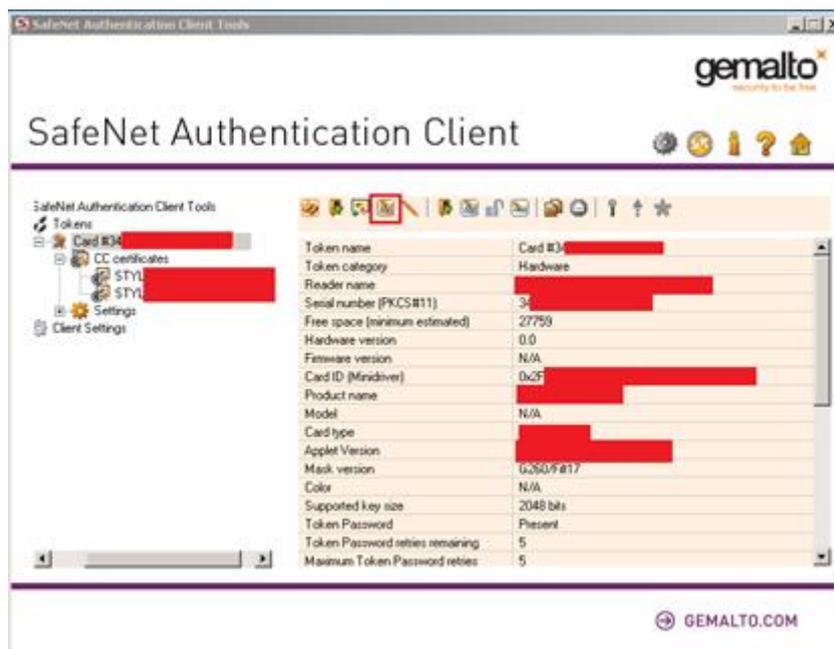


ΠΡΟΣΟΧΗ! Λόγω του ότι το Token Password και το Digital Signature PIN είναι διαφορετικά θα πρέπει να δώσουμε μεγάλη προσοχή στα μηνύματα που μας εμφανίζονται καθώς αν καταχωρήσουμε λάθος κωδικούς η διαδικασία θα αποτύχει.

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.

Διαχείριση ψηφιακών πιστοποιητικών χρήστη

Διαθέσιμα ψηφιακά πιστοποιητικά

Τύπος Πιστοποιητικού	Κατάσταση	Ημερομηνία λήξης
Αυθεντικοποίηση / Ψηφιακή υπογραφή (Πιστοποιητικό σκληρής αποθήκευσης)	Έγκυρο	25/01/2022
Ακύρωση	Προβολή	
Κρυπτογράφησης (Πιστοποιητικό σκληρής αποθήκευσης)	Έγκυρο	25/01/2022
Ακύρωση	Προβολή	

Οριστική ακύρωση πιστοποιητικών

Μπορείτε να ακυρώσετε απευθείας τα πιστοποιητικά σας πατώντας το κουμπί "Ακύρωση" παραπάνω και δίνοντας στη συνέχεια τον Προσωπικό Κωδικό Έκδοσης Πιστοποιητικών που σας είχε δοθεί κατά την έκδοση. Θα πρέπει να ακυρώσετε και τα δύο πιστοποιητικά για να έχετε τη δυνατότητα νέου αιτήματος για έκδοση.

Το USB Token φέρει τα ψηφιακά μας πιστοποιητικά, μπορούμε να υπογράψουμε 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:

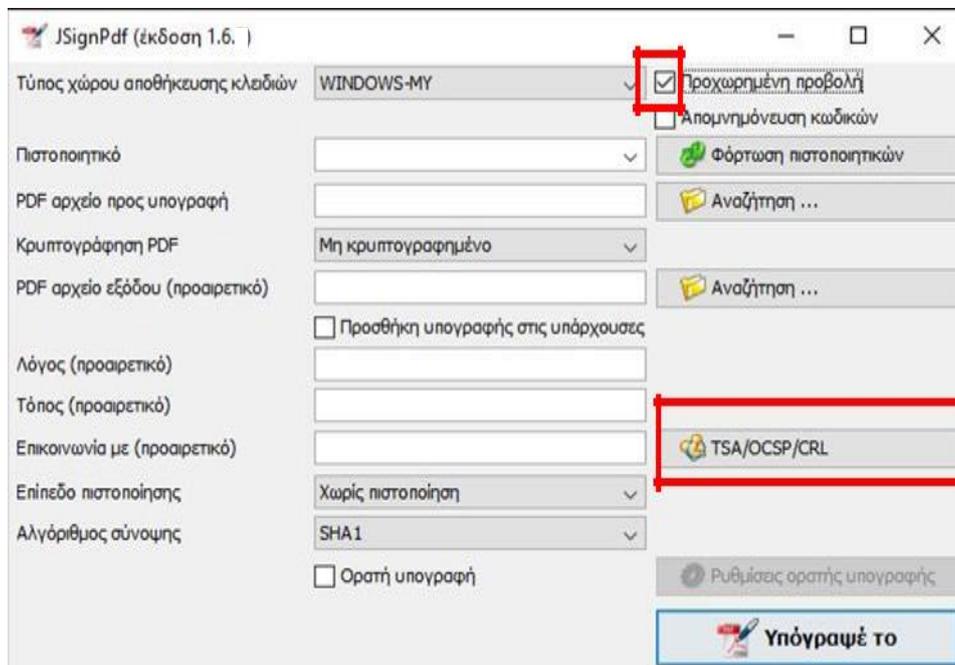
- Να υλοποιήσουμε το 4^ο βήμα του παρόντος οδηγού
- Να υλοποιήσουμε το 5^ο βήμα του παρόντος οδηγού
- Να εγκαταστήσουμε ένα πρόγραμμα το οποίο καθιστά δυνατή την υπογραφή Pdf αρχείων (θα το δούμε παρακάτω)

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/1G5uTu5ZA2jvaalHOBV1iSN4BvYcfl3WE/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. :

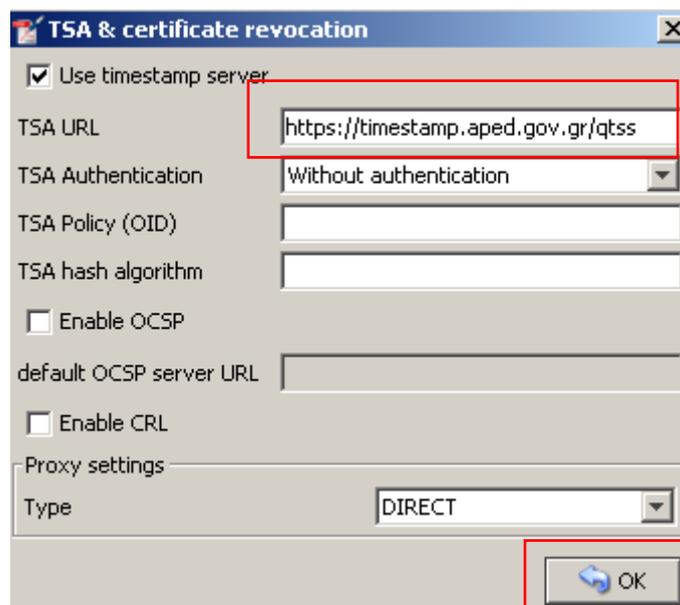


Επιλέγουμε Χρησιμοποίησε ασφαλή χρονοσήμανση.

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

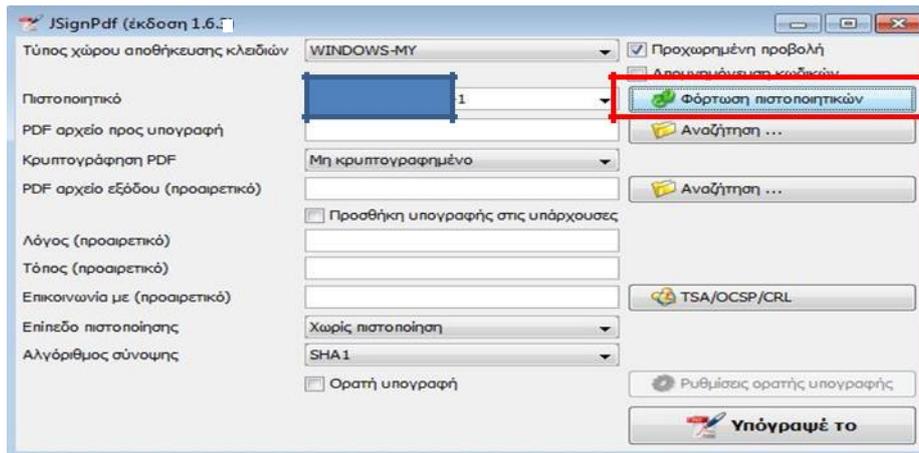
<https://timestamp.aped.gov.gr/qtss>

Κάνουμε κλικ στο κουμπί OK.

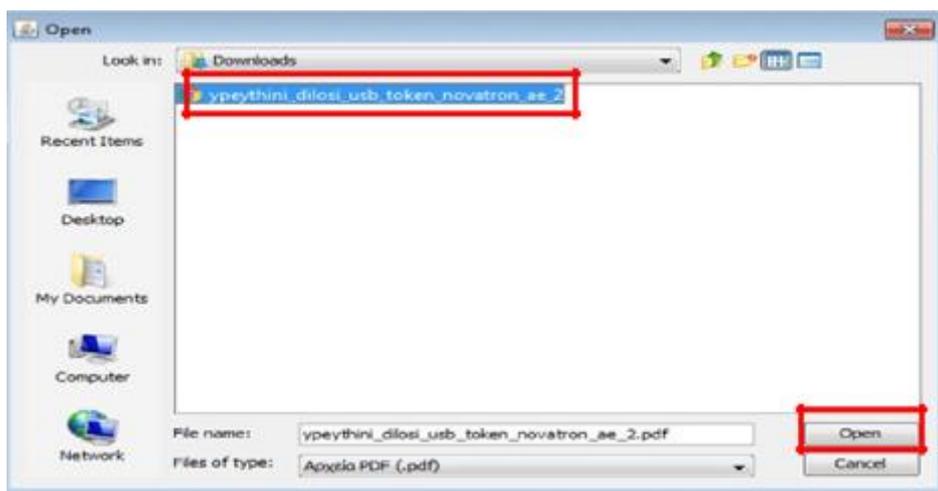
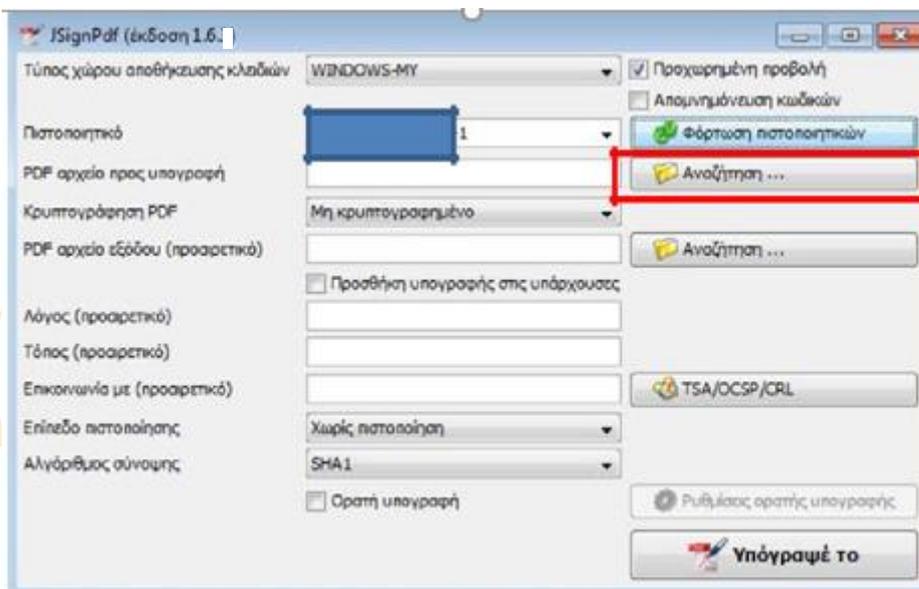


Η παραπάνω διαδικασία γίνεται μία φορά, το πρόγραμμα αποθηκεύει τις ρυθμίσεις.

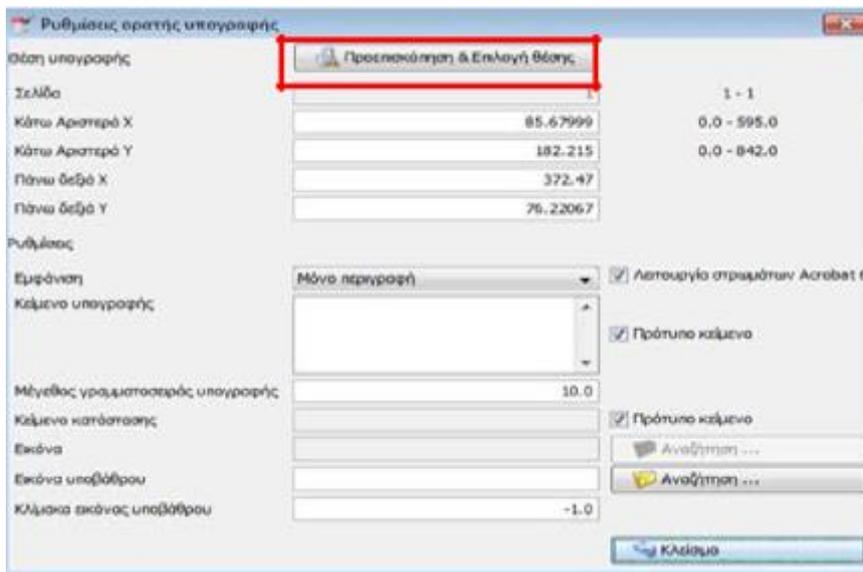
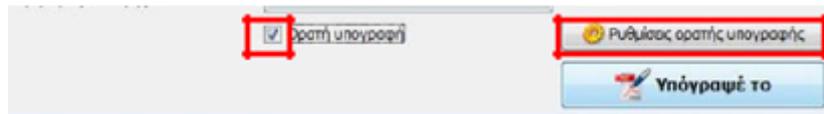
Έχουμε συνδεδεμένο στον υπολογιστή το USB Token μας. Έπειτα κάνουμε κλικ στο κουμπί Φόρτωση πιστοποιητικών και αριστερά φαίνεται το Ψηφιακό μας Πιστοποιητικό:



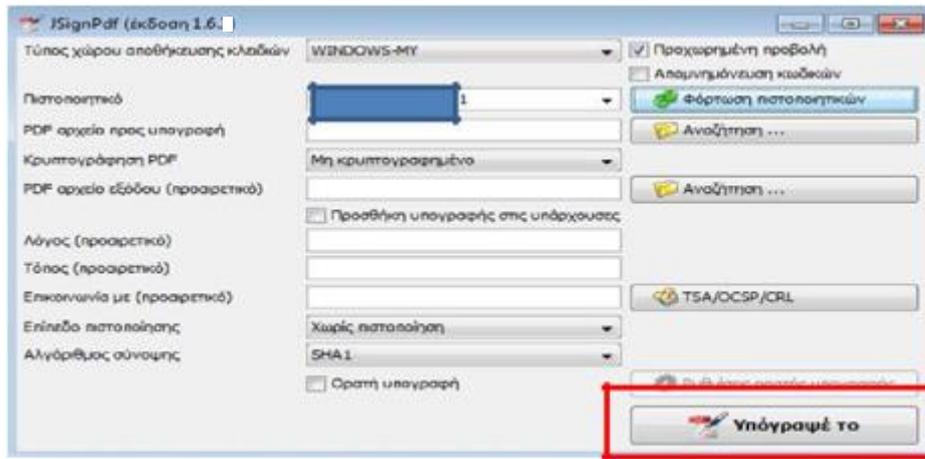
Κάνουμε κλικ στο πρώτο κουμπί Αναζήτηση για να επιλέξουμε το PDF αρχείο προς υπογραφή:



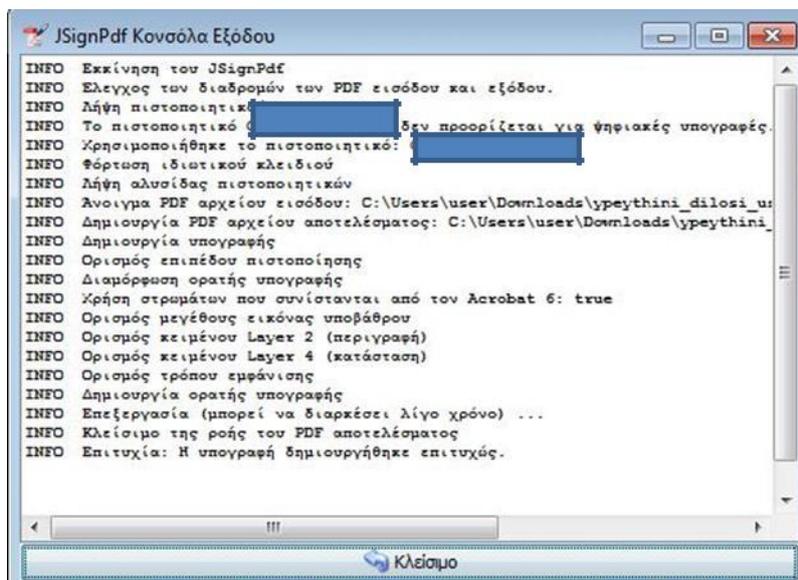
Για να προσθέσουμε Ορατή Υπογραφή, επιλέγουμε Ορατή υπογραφή, κάνουμε κλικ στο κουμπί Ρυθμίσεις ορατής υπογραφής, επιλέγουμε Προεπισκόπηση & Επιλογή θέσης όπου εμφανίζεται το έγγραφο στο οποίο (με το αριστερό κλικ από το ποντίκι μας) επιλέγουμε το ΠΟΥ θα τοποθετηθεί η υπογραφή μας και κάνουμε κλικ στο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



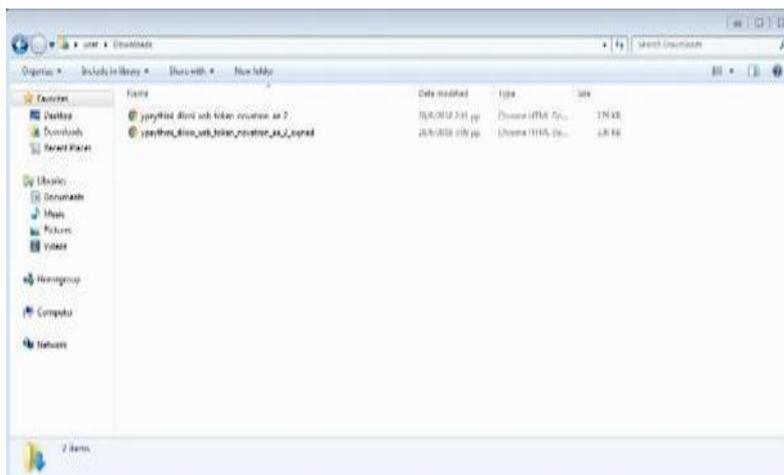
Κάνουμε κλικ στο κουμπί Υπέγραψε το και αυτόματα μας ζητάει το Digital Signature PIN που για το συγκεκριμένο Token είναι 6 φορές το 0 (000000), το εισάγουμε και πατάμε Ok.



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

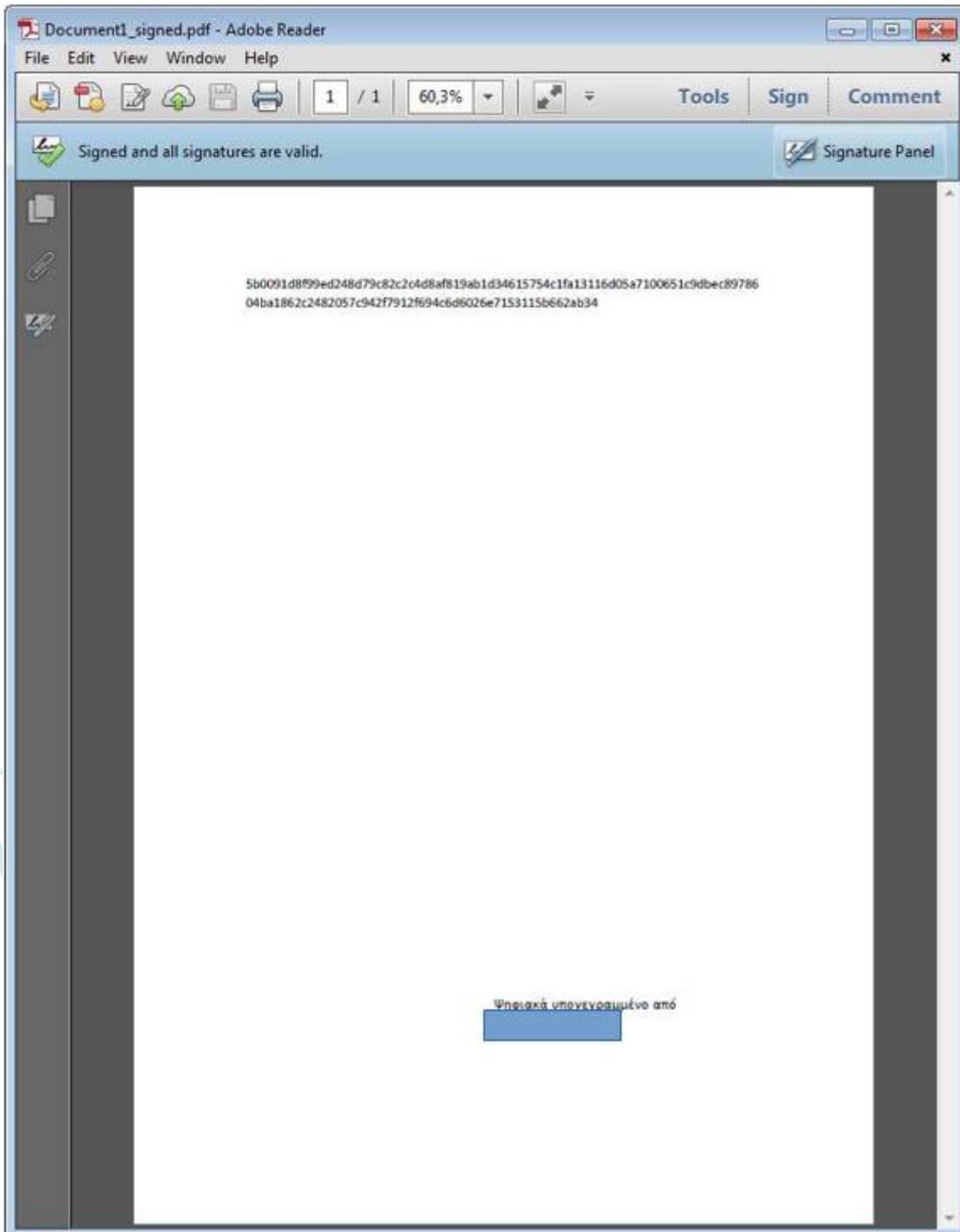


Δημιουργείται το Ψηφιακά Υπογεγραμμένο έγγραφο στον ίδιο φάκελο που βρισκόταν το αρχικό αλλά με την κατάληξη _signed.



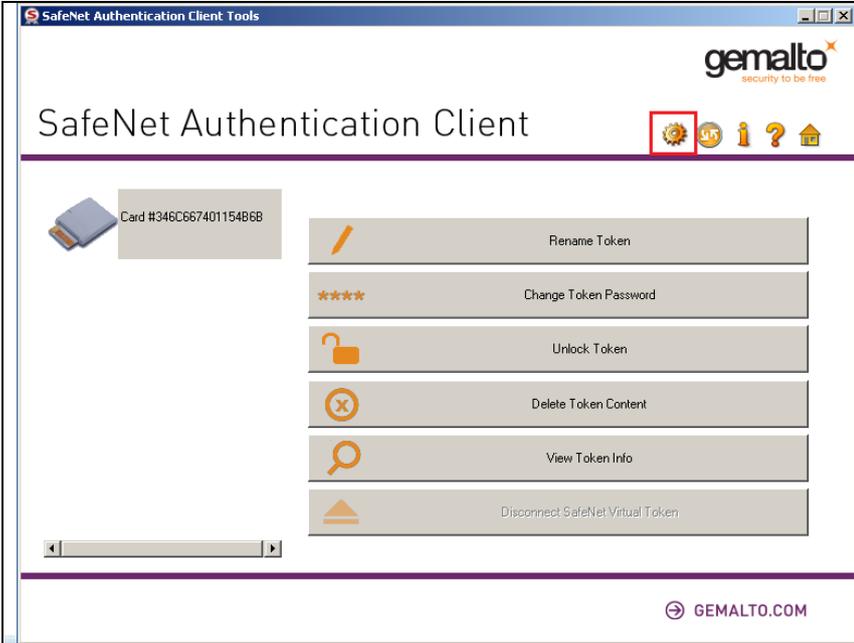
Έχουμε ολοκληρώσει επιτυχώς την Ψηφιακή Υπογραφή του εγγράφου μας. Βλέπουμε τη σήμανση Signed and all signatures are valid. Με τον τρόπο αυτό μπορούμε να βεβαιωθούμε ότι η υπογραφή είναι έγκυρη και δεν έχει γίνει επεξεργασία του εγγράφου μετά την υπογραφή (για να δούμε περισσότερες πληροφορίες κάνουμε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

NOVATRON®



Παράρτημα: Διαχείριση κωδικών και περιεχομένων της συσκευής

Πως αλλάζω τον κωδικό του Token (Token Password)?



SafeNet Authentication Client Tools

gemalto
security to be free

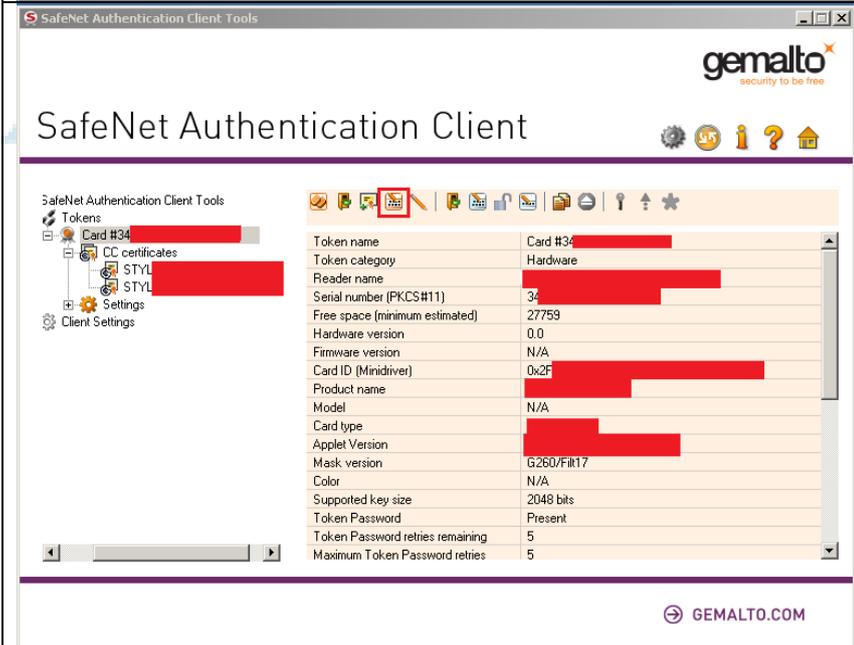
SafeNet Authentication Client

Card #346C667401154868

- Rename Token
- Change Token Password
- Unlock Token
- Delete Token Content
- View Token Info
- Disconnect SafeNet Virtual Token

GEMALTO.COM

Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.



SafeNet Authentication Client Tools

gemalto
security to be free

SafeNet Authentication Client

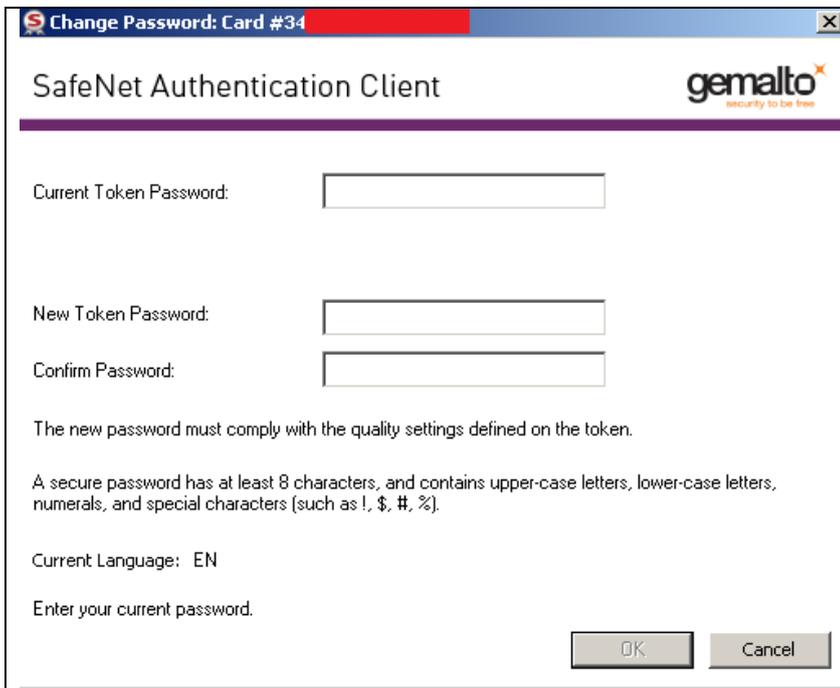
SafeNet Authentication Client Tools

- Tokens
 - Card #34
 - CC certificates
 - STYL
 - STYL
 - Settings
 - Client Settings

Token name	Card #34
Token category	Hardware
Reader name	
Serial number (FKCS#11)	34
Free space (minimum estimated)	27759
Hardware version	0.0
Firmware version	N/A
Card ID (Minidriver)	0x2F
Product name	
Model	N/A
Card type	
Applet Version	
Mask version	G260/Filt17
Color	N/A
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	5
Maximum Token Password retries	5

GEMALTO.COM

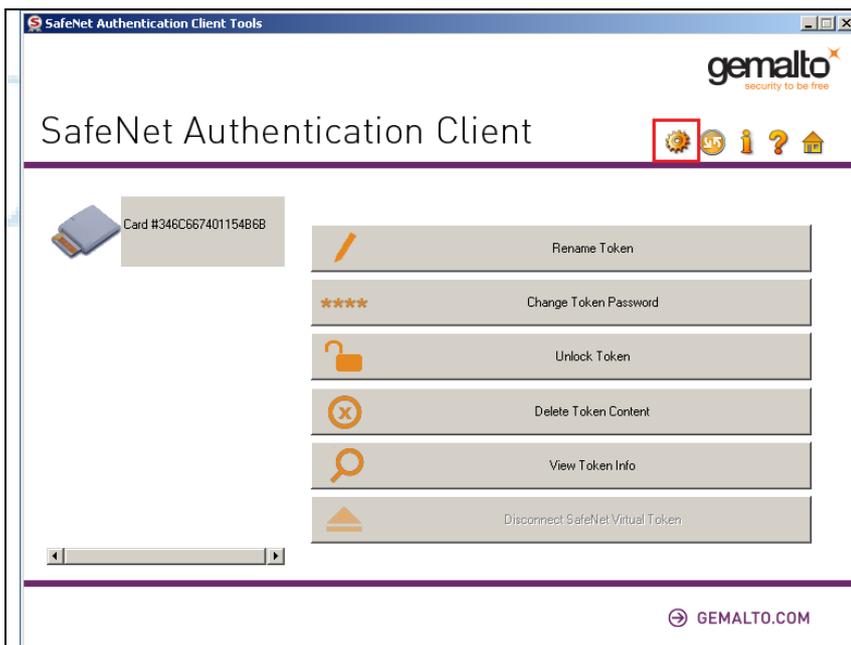
Επιλέγουμε το τέταρτο εικονίδιο από τα αριστερά.



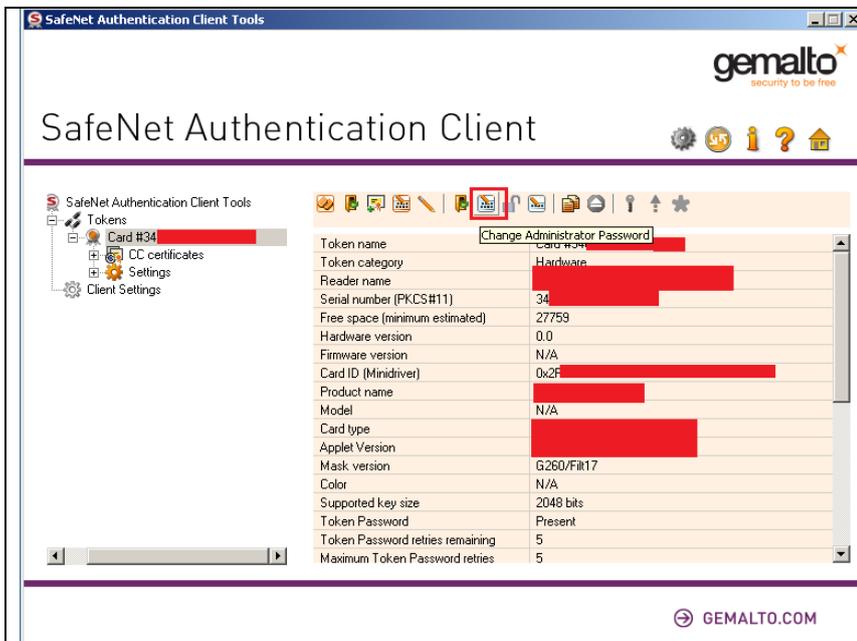
Current Token Password: Εδώ καταχωρούμε τον τρέχον κωδικό του Token .
New Token Password: Εδώ καταχωρούμε το νέο κωδικό που επιθυμούμε.
Confirm Password: Εδώ επιβεβαιώνουμε το νέο κωδικό που επιθυμούμε.

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 γράναζι.



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.

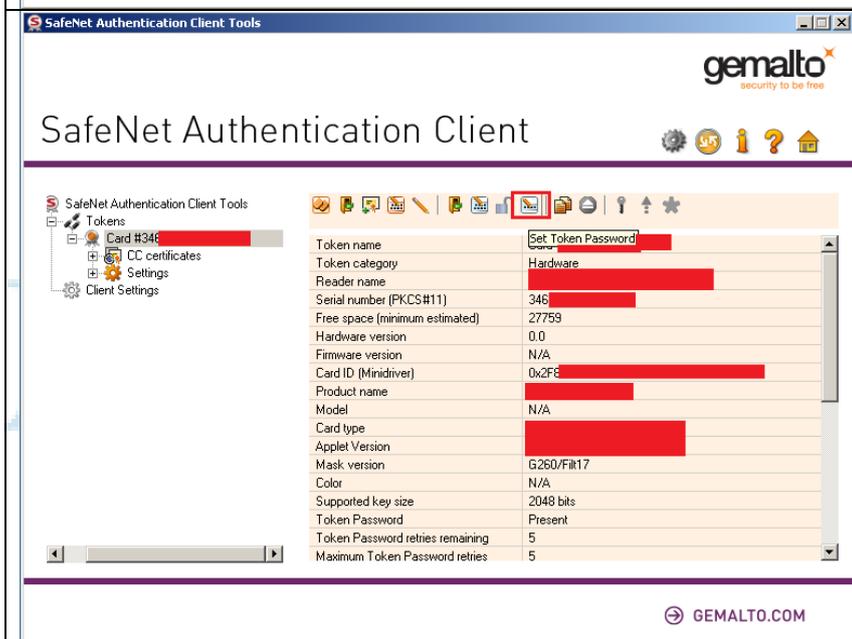
Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

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.



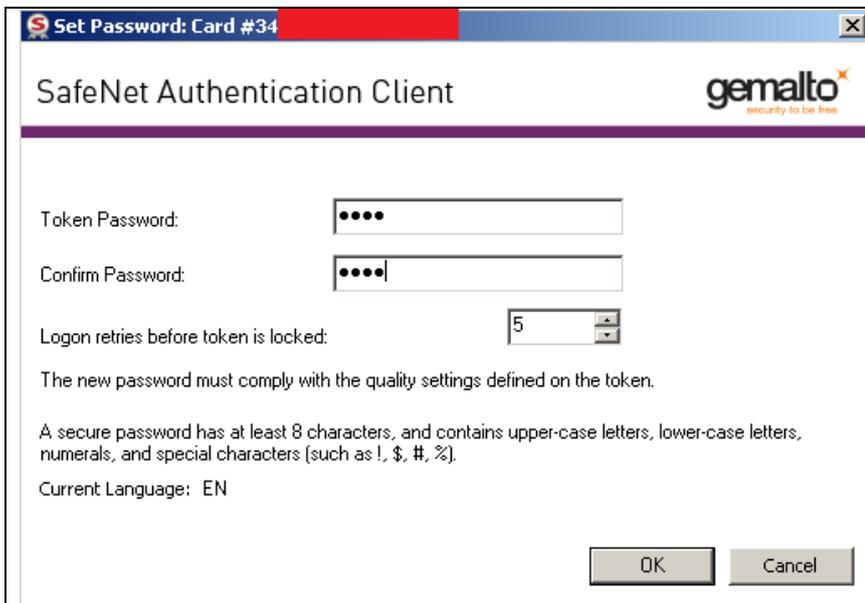
Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάτζι.



Επιλέγουμε το ένατο εικονίδιο από τα αριστερά.



Καταχωρούμε τον κωδικό διαχειριστή (από προεπιλογή σαράντα οκτώ μηδενικά) και κάνουμε κλικ στο κουμπί OK.



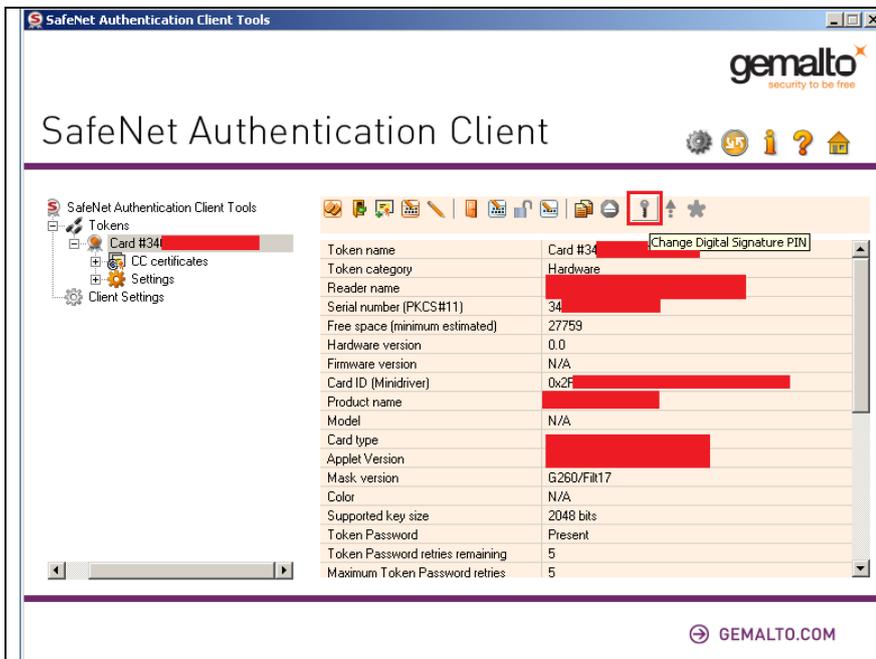
Στην επόμενη οθόνη καταχωρούμε το νέο κωδικό Token που επιθυμούμε (πεδίο Token Password) και τον επιβεβαιώνουμε (πεδίο Confirm Password).

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

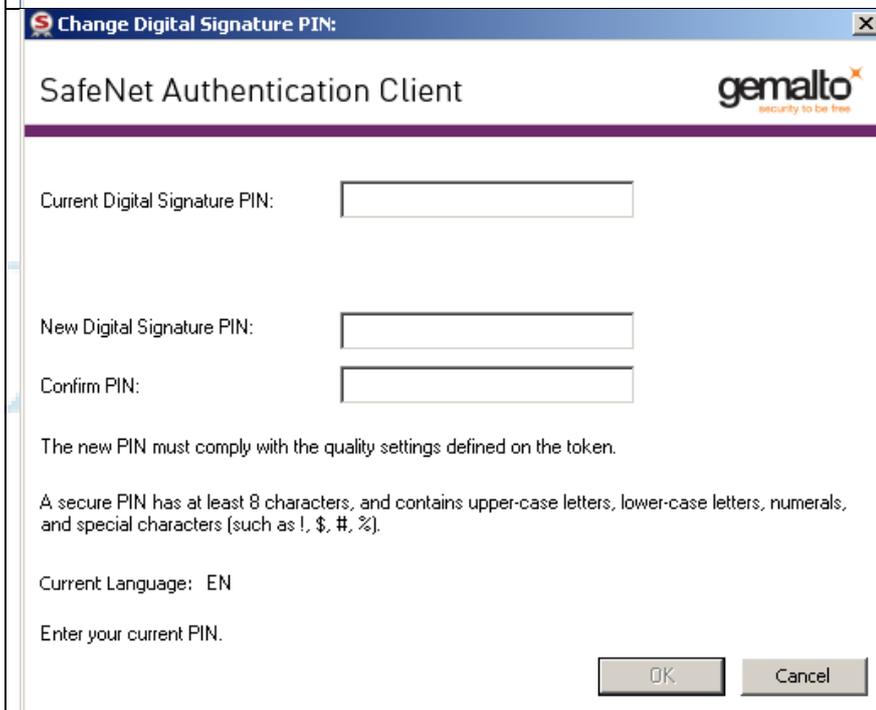
Πως αλλάζω τον κωδικό ψηφιακής υπογραφής (Digital Signature PIN).



Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.



Επιλέγουμε το δωδέκατο εικονίδιο από τα αριστερά.



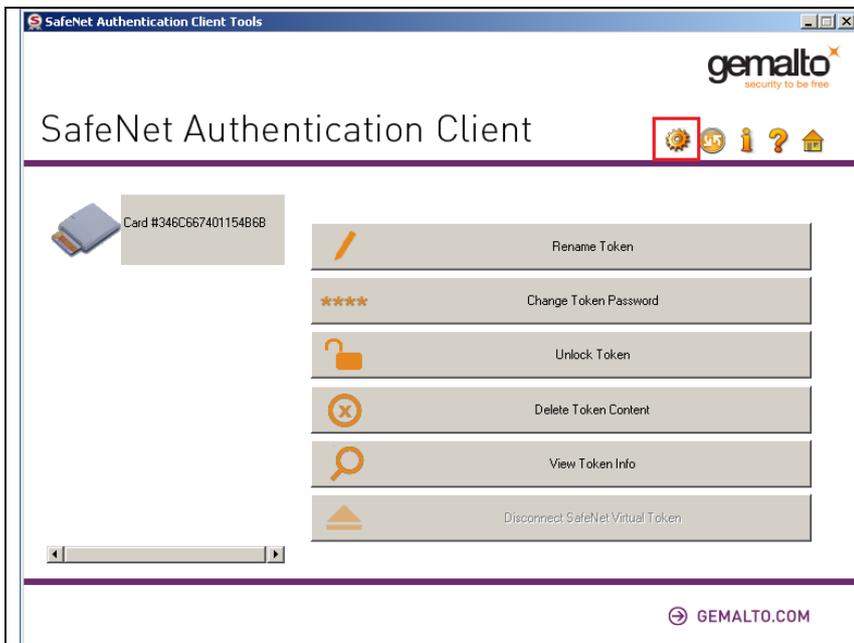
Current Digital Signature PIN: Εδώ καταχωρούμε τον τρέχον κωδικό ψηφιακής υπογραφής (από προεπιλογή έξι μηδενικά 000000).

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

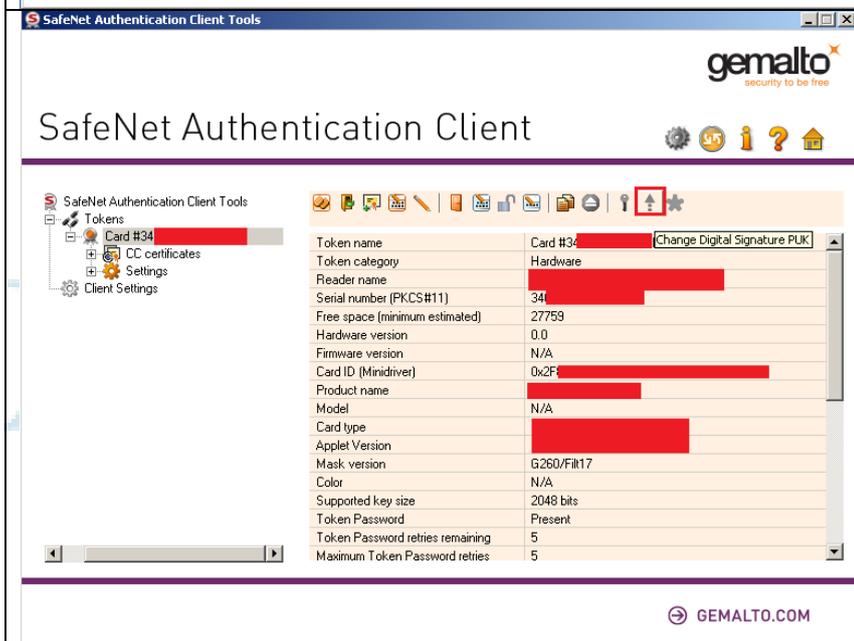
Confirm PIN: Εδώ επιβεβαιώνουμε το νέο κωδικό ψηφιακής υπογραφής.

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.

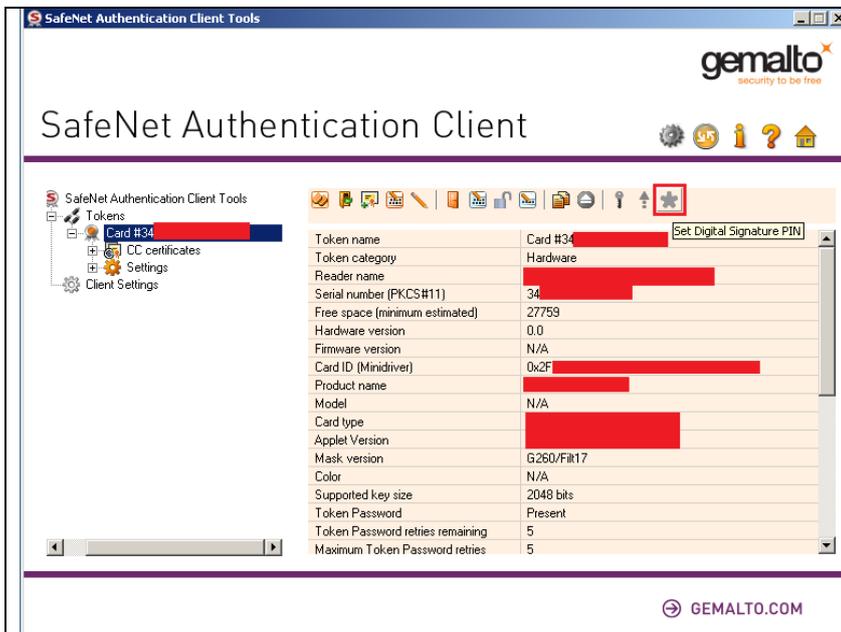
Confirm PUK: Εδώ επιβεβαιώνουμε το νέο κωδικό διαχειριστή ψηφιακής υπογραφής.

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

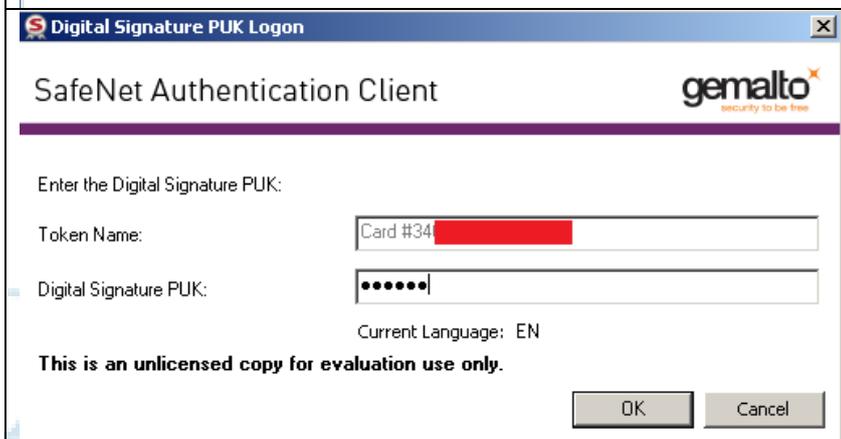
Πως ξεκλειδώνω τον κωδικό ψηφιακής υπογραφής (PIN) με τη χρήση του κωδικού διαχειριστή (PUK).

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.

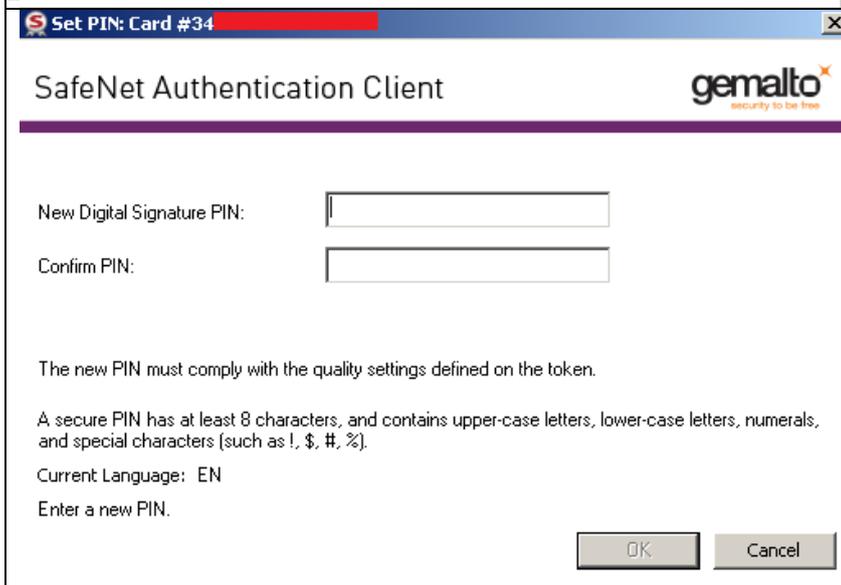
Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάτζι.



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.