NOVATRON®

Τμήμα Τεχνικής Υποστήριξης

Safenet 5110cc

Οδηγός χρήσης

Περιεχόμενα.

Τεχνικές προδιαγραφές.

Feature	Details
Supported operating systems	Windows Server 2008/R2, Windows Server 2012 and 2012 R2, Windows 7, Mac OS, Linux, Windows 8, Windows 10
API & Standards Support	PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver, CNG
Memory Size	80K
Dimensions	5110–16.4mm*8.5mm*40.2mm
ISO specification support	Support for ISO 7816-1 to 4 specifications
Operating temperature	0º C to 70º C (32º F to 158º F)
Storage temperature	-40º C to 85º C (-40º F to 185º F)
Humidity rating	0-100% without condensation
Water resistance certification	IP X7 – IEC 60529
USB connector	USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Casing	Hard molded plastic, tamper evident
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000

	SafeNet eToken 5110 FIPS	SafeNet eToken 5110 CC	SafeNet eToken 5110
On-board security algorithms	• Symmetric: AES, 3DES (Triple DES) 128/192/256 bit • Hash: SHA-256 • RSA: 2048-bit • Elliptic curves: P-256, P-384, ECDH	• Hash: SHA-1, SHA-256, SHA-384, SHA-512 • RSA: up to RSA 4096 bits • RSA OAEP & RSA PSS • P-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA, ECDH are available via a custom configuration • On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits) • Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	• Symmetric: 3DES (Triple DES), AES 128/192/256 bit • Hash: SHA1, SHA256 • RSA 1024-bit / 2048-bit • Elliptic curves: P-256, P-384, ECDH
Security certifications	FIPS 140-2 level 3	CC EAL5+	FIPS 140-2 level 3(SC chip and OS)
Smart Card Platform	Gemalto IDCore 30 (rev B) and eToken applet	IDPrime MD 940	Gemalto IDCore 30 and eToken applet

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): 1234567890 (μετά από 5 ανεπιτυχείς προσπάθειες κλειδώνει).

Token PUK (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.

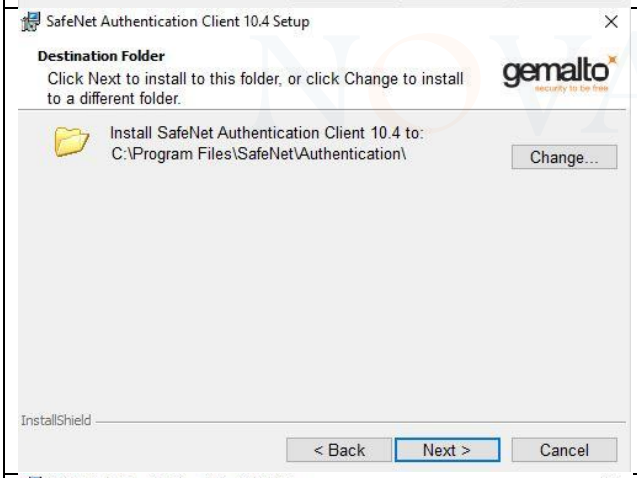
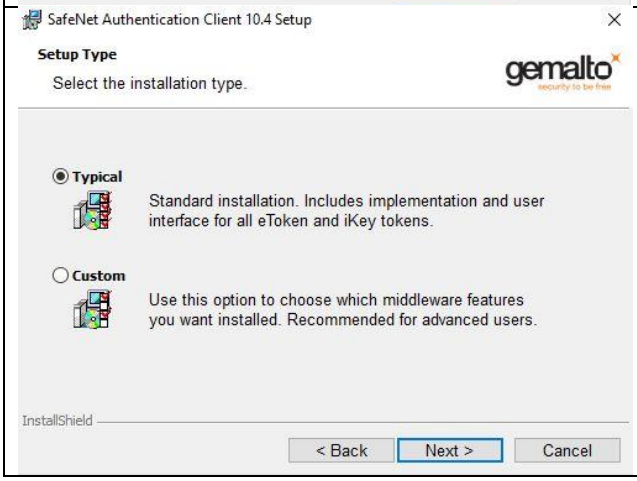
Εγκατάσταση Driver / Middleware.

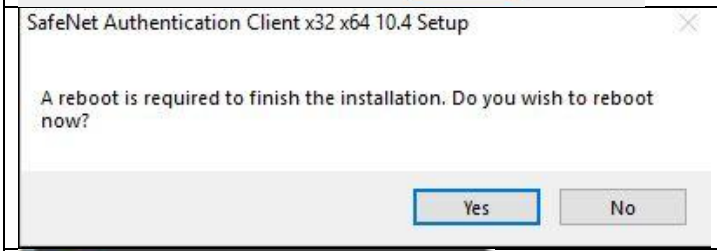
Οι οδηγοί (Driver & Middleware) είναι διαθέσιμοι στην ιστοσελίδα μας στην σελίδα του προϊόντος, στην καρτέλα σχετικά αρχεία ή στον παρακάτω σύνδεσμο:

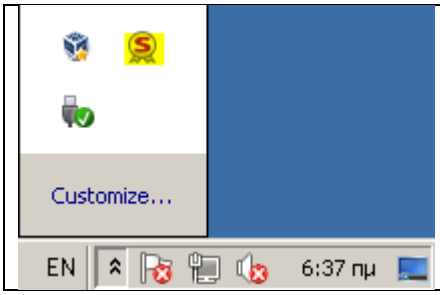
https://drive.google.com/open?id=1mVR-QFRGSrqguhJfJ-ArJc7JrsyUMbKP

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

	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. **Θα σας ζητηθεί να αλλάξετε το PIN του token, πληκτρολογήστε στο πεδίο default**

	**token PIN “1234567890” και στη συνέχεια πληκτρολογήστε το PIN που επιθυμείτε (το οποίο θα γνωρίζετε μόνο εσείς)**

Οδηγίες για την απόκτηση ψηφιακής υπογραφής.

Όλα τα απαραίτητα βήματα για την απόκτηση ψηφιακής υπογραφής είναι διαθέσιμα στην ιστοσελίδα της ΑΠΕΔ (www.aped.gov.gr).

ΠΡΟΣΟΧΗ! Για την επικοινωνία με την ηλεκτρονική πύλη του ΕΡΜΗ και την απόκτηση των προσωπικών μας ψηφιακών πιστοποιητικών απαιτείται λειτουργικό σύστημα Windows 7 και Internet Explorer 8 έως 10 όπως αναφέρεται και στην ιστοσελίδα της ΑΠΕΔ.

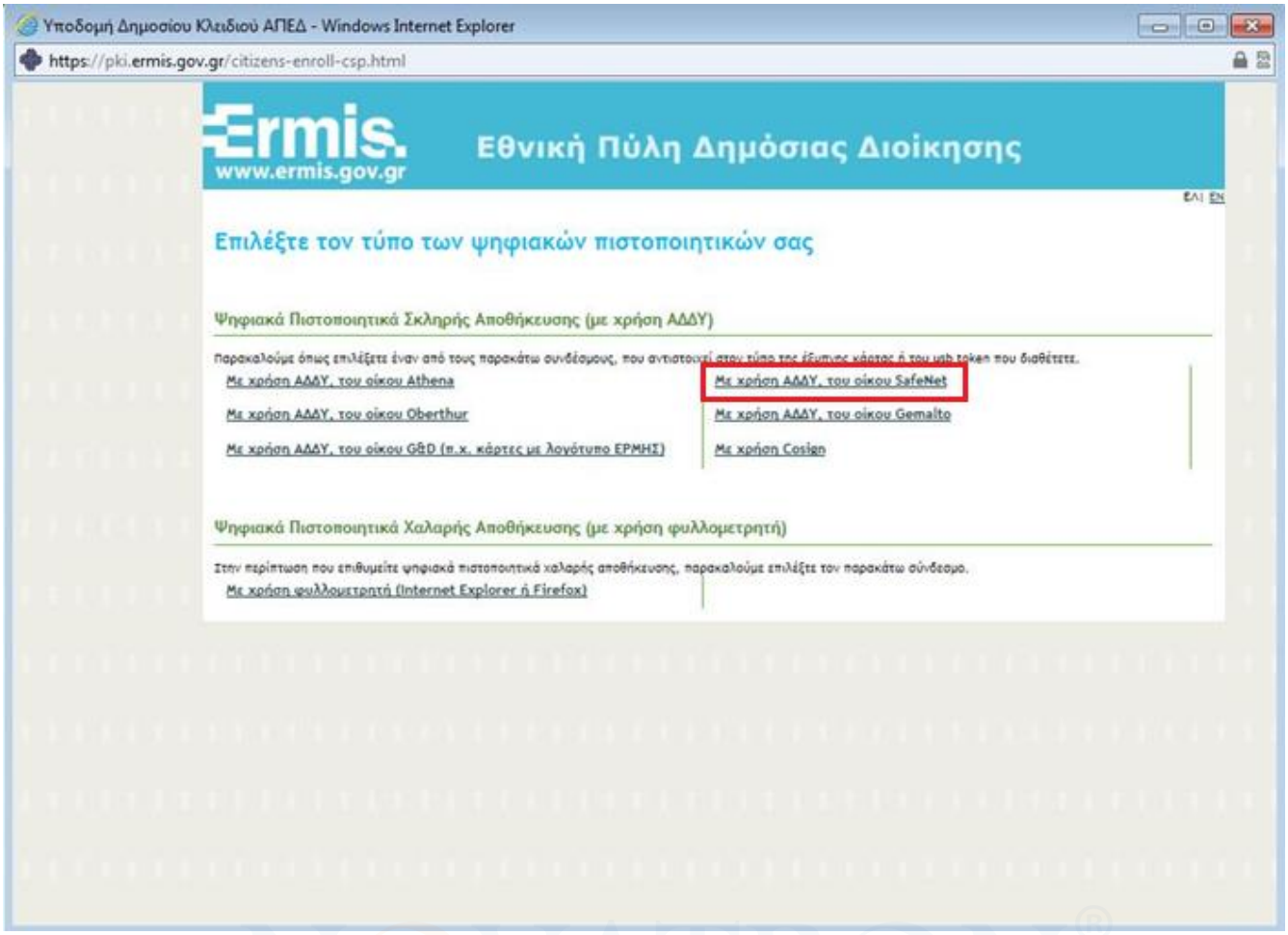
Εφ’ όσον ολοκληρωθεί η εγκατάσταση των πιστοποιητικών στο Token αυτό μπορεί να λειτουργήσει σε οποιοδήποτε λειτουργικό σύστημα (Windows 7, 8, 10).

ΣΗΜΕΙΩΣΗ: Το τεχνικό μας τμήμα υποστηρίζει μόνο λειτουργικά συστήματα Windows.

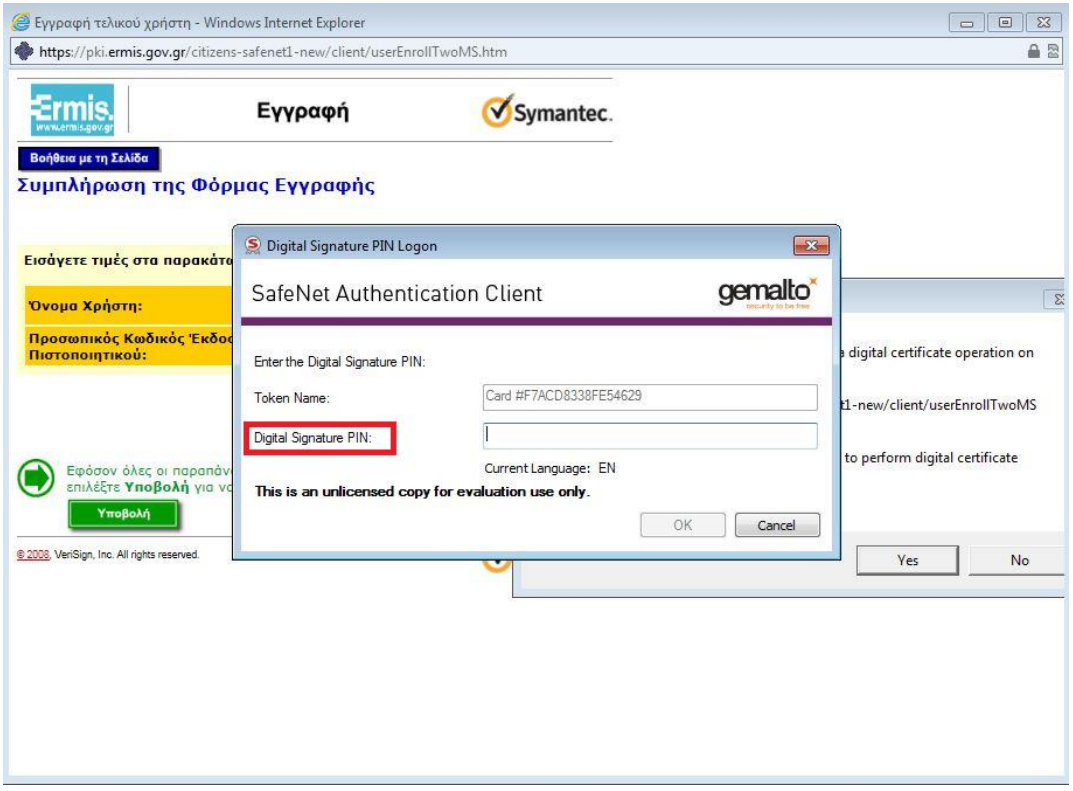
Τα συνοπτικά βήματα είναι τα εξής:

1. Προμήθεια του Token (ΑΔΔΥ) (http://www.aped.gov.gr/more/obtainsignature/4-step1.html).
2. Ηλεκτρονική αίτηση μέσω της πύλης ΕΡΜΗΣ (http://www.aped.gov.gr/more/obtainsignature/5-step2.html).
3. Μετάβαση σε ΚΕΠ (http://www.aped.gov.gr/more/obtainsignature/6-step3.html).
4. Προετοιμασία υπολογιστή (http://www.aped.gov.gr/more/obtainsignature/7-step4.html).
5. Εγκατάσταση απαραίτητων προγραμμάτων (Αναλύεται στην ενότητα Εγκατάσταση Driver / Middleware του παρόντος οδηγού χρήσης).
6. Έκδοση ψηφιακού πιστοποιητικού.

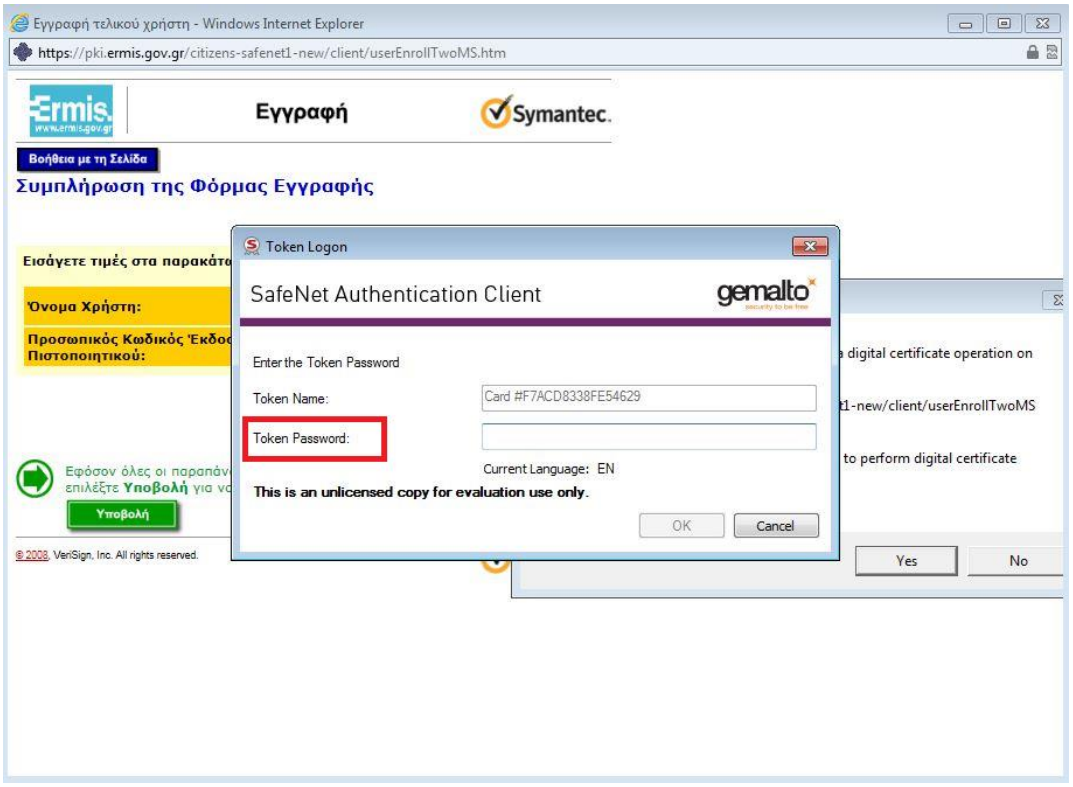
Σημαντικό!!! Στην πύλη του ΕΡΜΗ **θα πρέπει να επιλέξουμε τον οίκο Safenet κατά την έκδοση των πιστοποιητικών μας.**



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 θα έχουμε ορίσει μετά τη σύνδεση του Token στον υπολογιστή.



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.

Οδηγίες χρήσης της ψηφιακής υπογραφής.

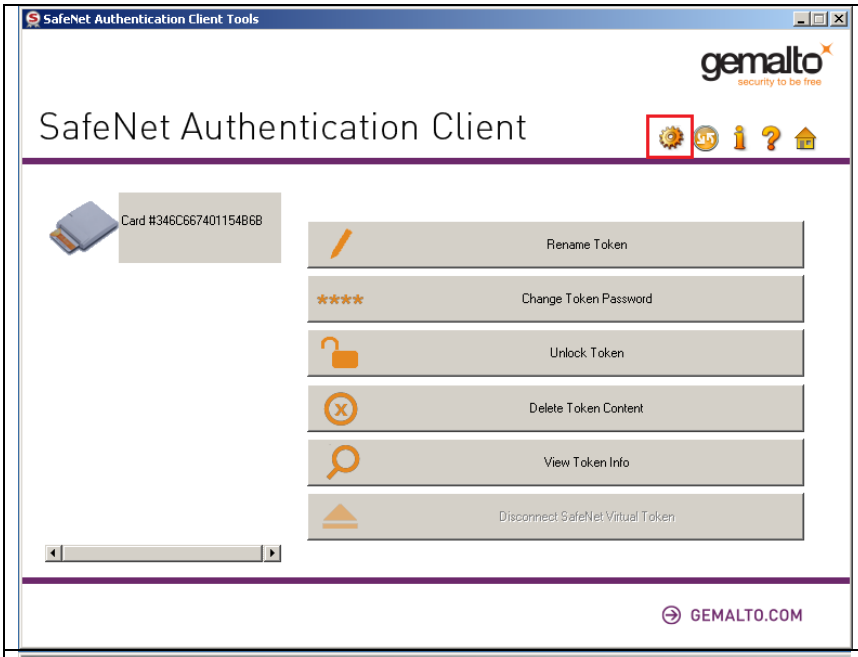
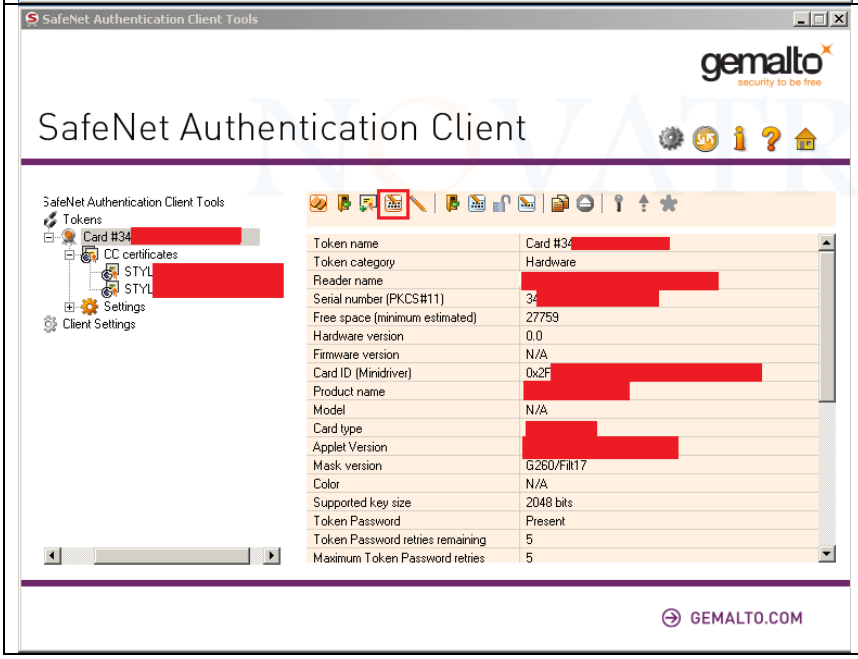
Όλες οι απαραίτητες οδηγίες για την χρήση της ψηφιακής υπογραφής είναι διαθέσιμες στην ιστοσελίδα της Υπηρεσίας Ανάπτυξης Πληροφορικής (www.yap.gov.gr)

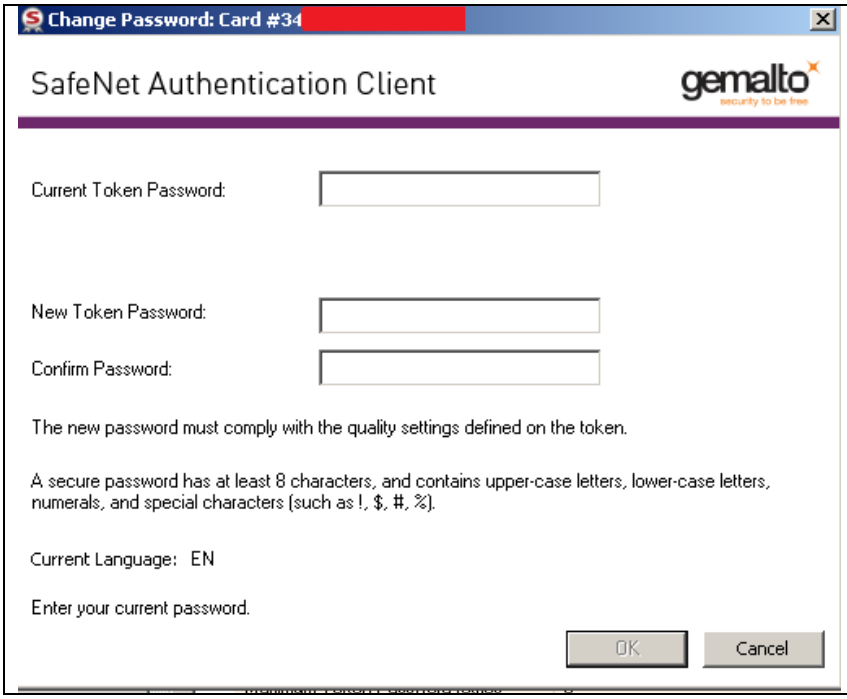
http://www.yap.gov.gr/index.php/aped/aped-odigies-xrisis-pistopoihtikon-menu.html

Η εταιρεία μας υποστηρίζει την υπογραφή εγγράφων PDF με τη χρήση του εργαλείου JSign PDF σε λειτουργικά συστήματα Windows.

Συχνές ερωτήσεις.

Πως αλλάζω τον κωδικό του Token (Token Password)?

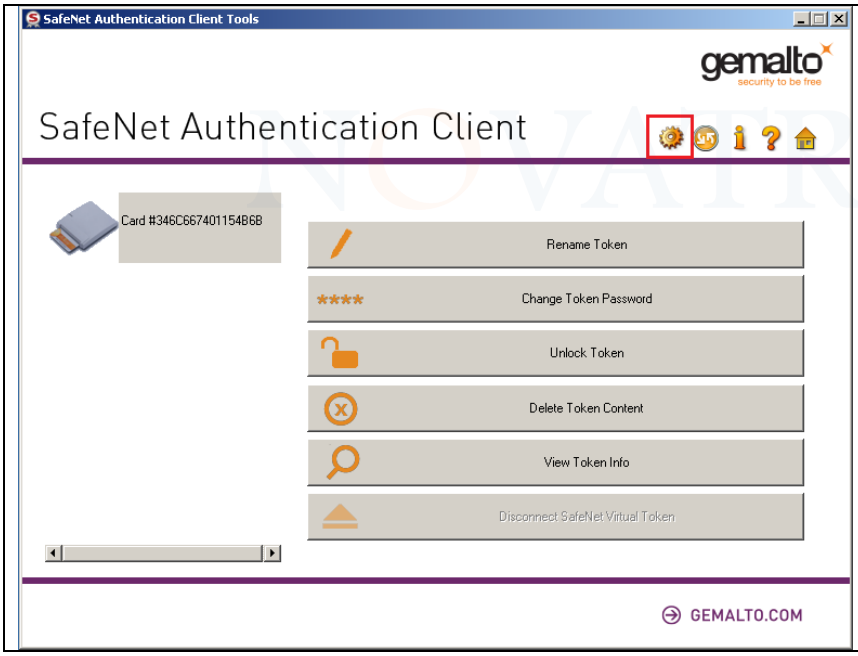
	Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.
	Επιλέγουμε το τέταρτο εικονίδιο από τα αριστερά.



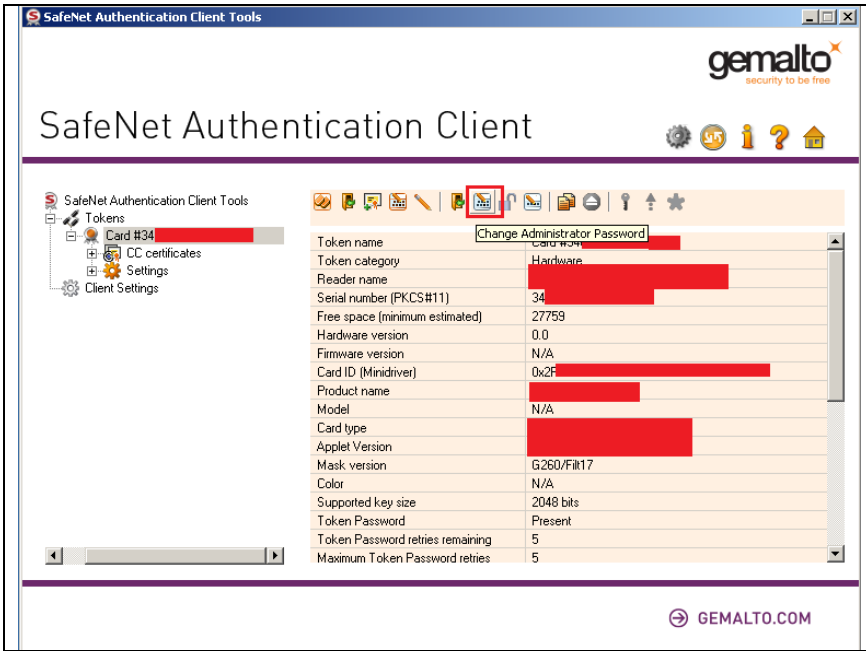
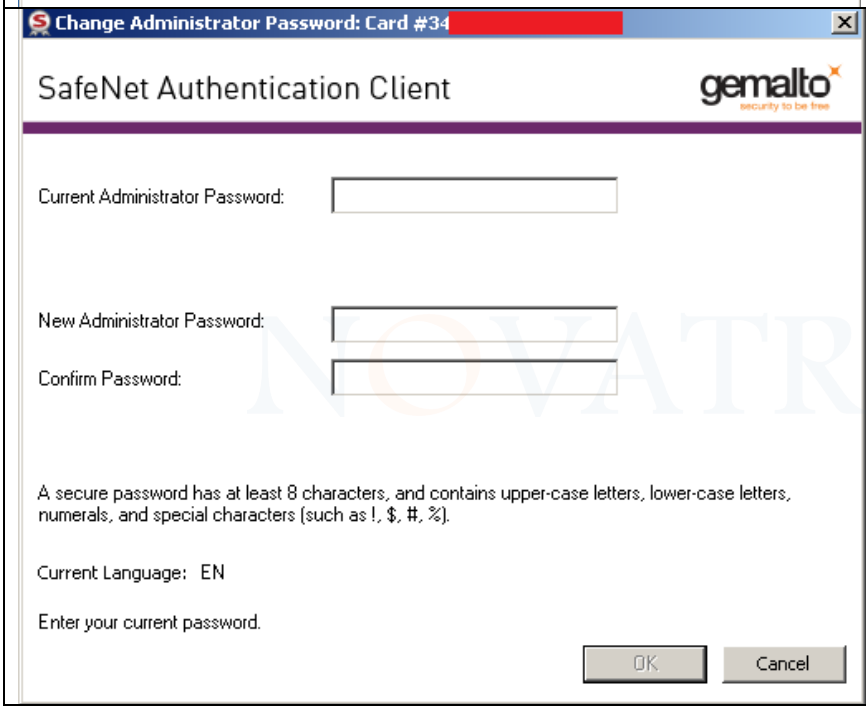
Current Token Password: Εδώ καταχωρούμε τον τρέχον κωδικό του Token .
New Token Password: Εδώ καταχωρούμε το νέο κωδικό που επιθυμούμε.
Confirm Password: Εδώ επιβεβαιώνουμε το νέο κωδικό που επιθυμούμε.

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

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

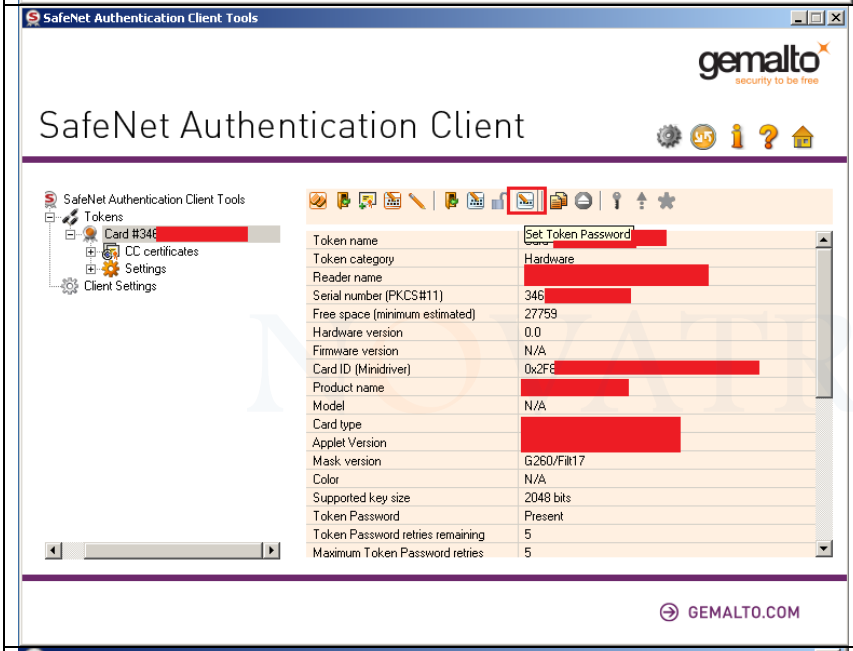
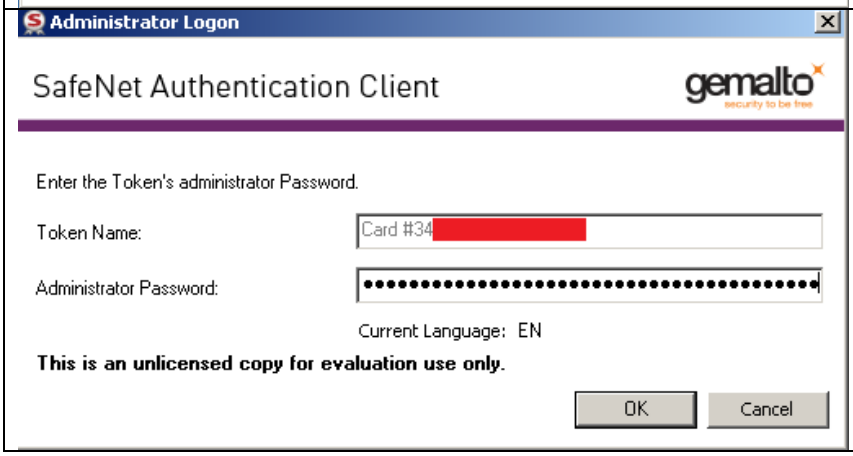


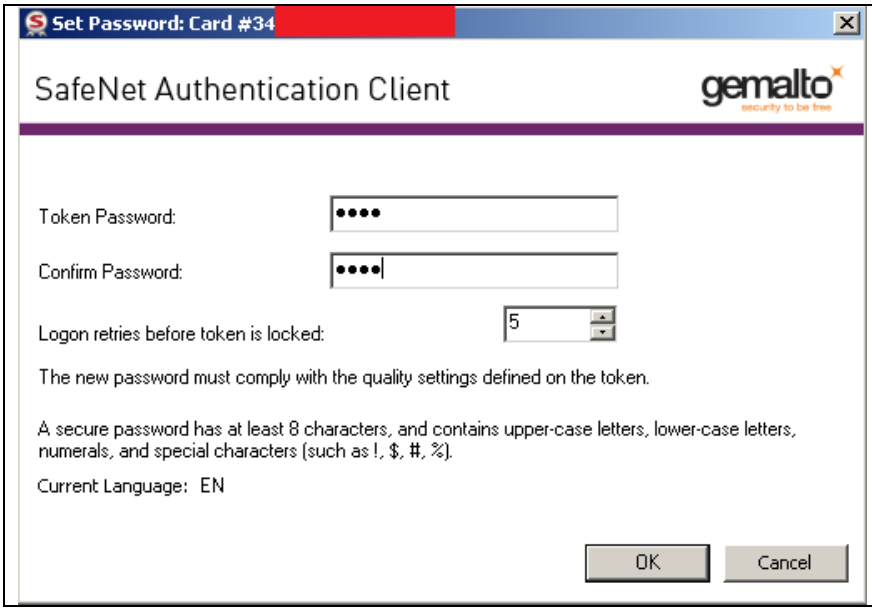
Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.

	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.

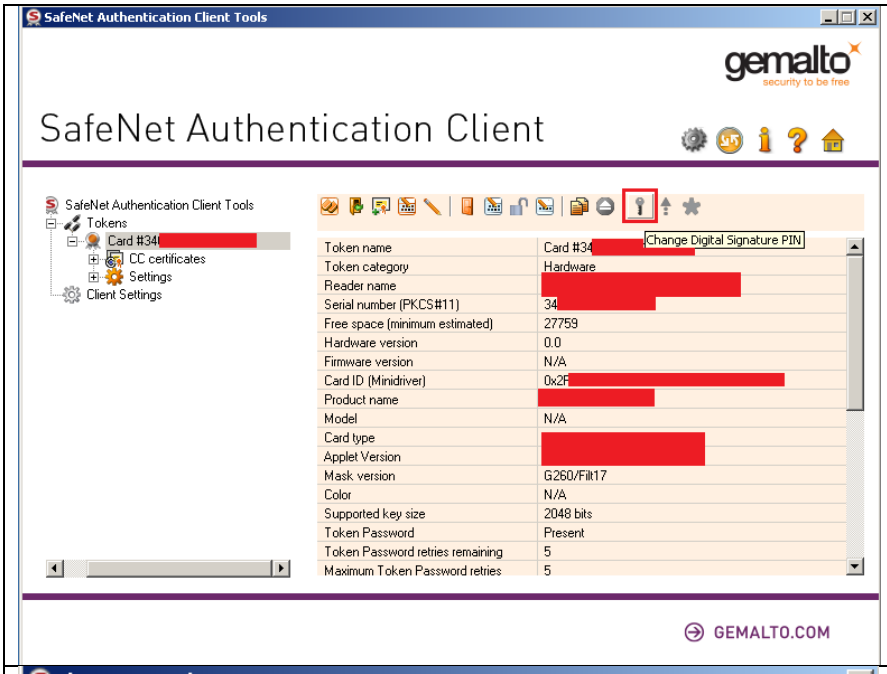
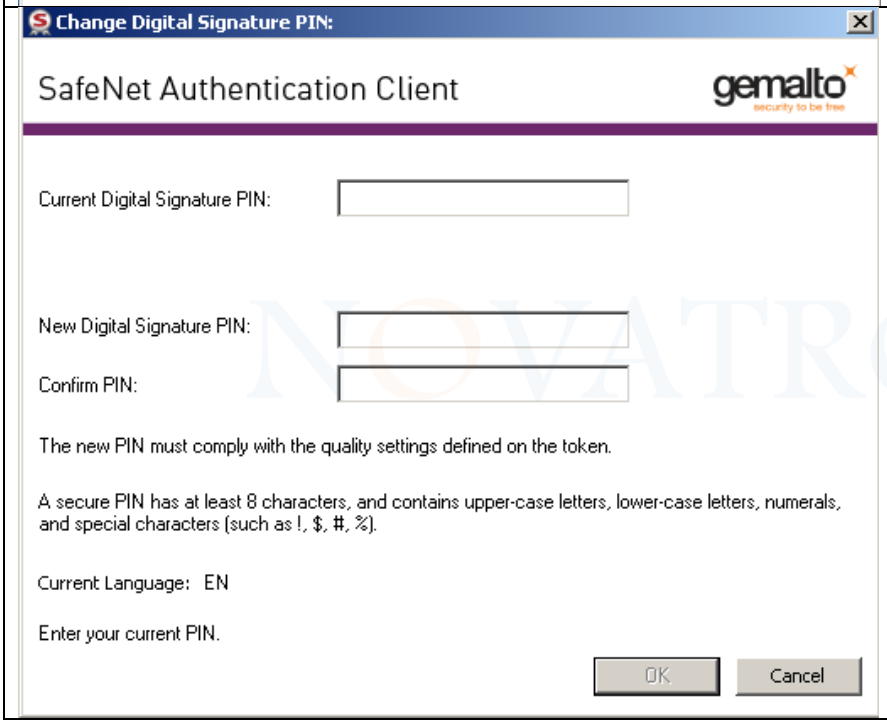


Στην επόμενη οθόνη καταχωρούμε το νέο κωδικό Token που επιθυμούμε (πεδίο Token Password) και τον επιβεβαιώνουμε (πεδίο Confirm Password).

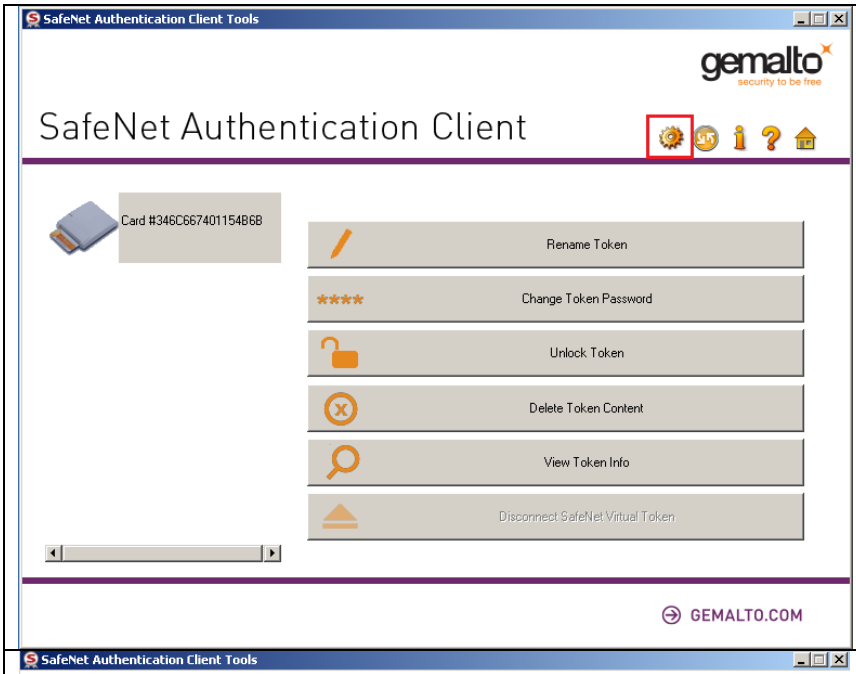
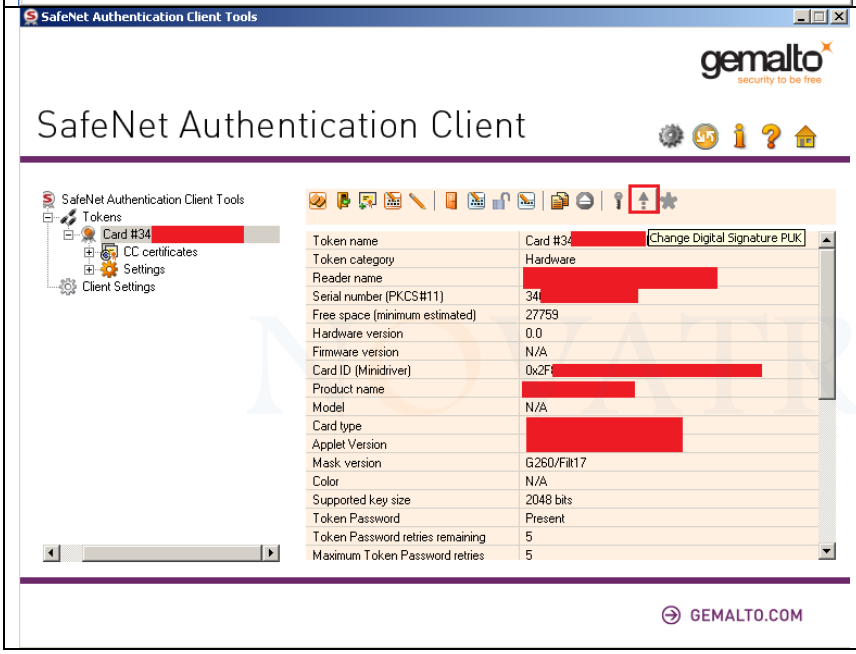
Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

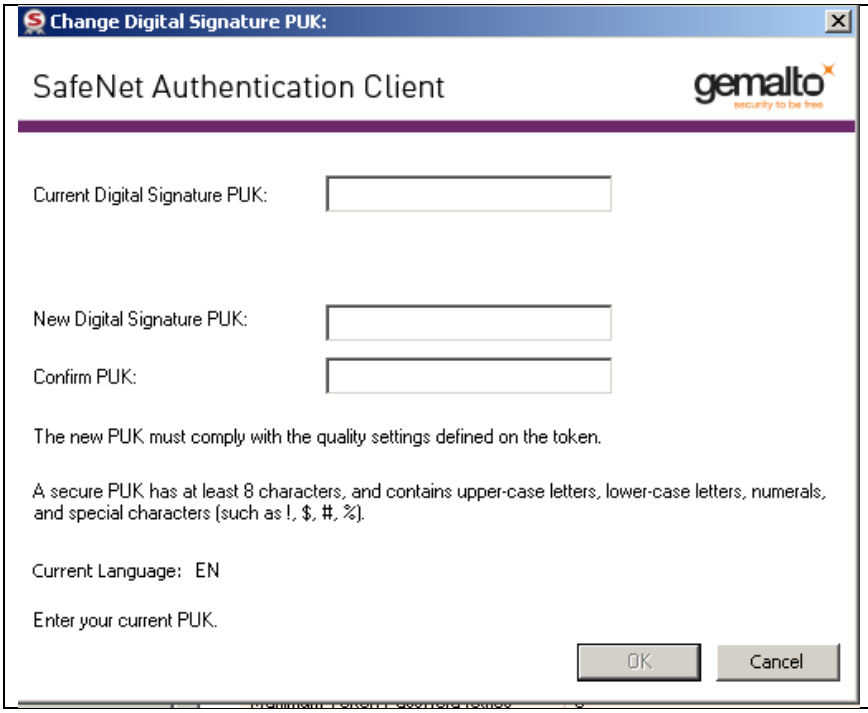
Πως αλλάζω τον κωδικό ψηφιακής υπογραφής (Digital Signature PIN).

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.

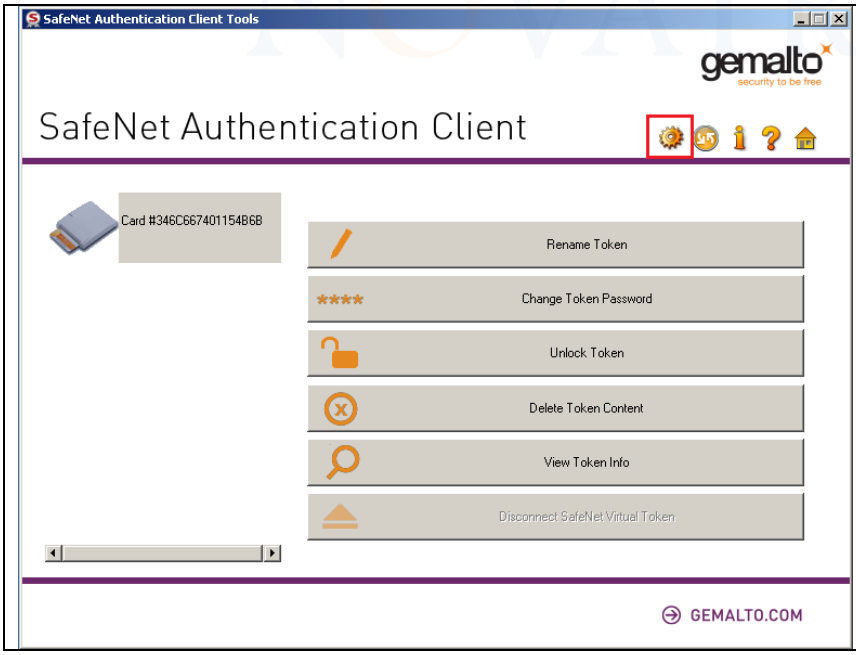


Current Digital Signature PUK: Εδώ καταχωρούμε τον τρέχον κωδικό διαχειριστή ψηφιακής υπογραφής (από προεπιλογή έξι μηδενικά 000000).
New Digital Signature PUK: Εδώ καταχωρούμε το νέο κωδικό διαχειριστή ψηφιακής υπογραφής.
Confirm PUK: Εδώ επιβεβαιώνουμε το νέο κωδικό διαχειριστή ψηφιακής υπογραφής.

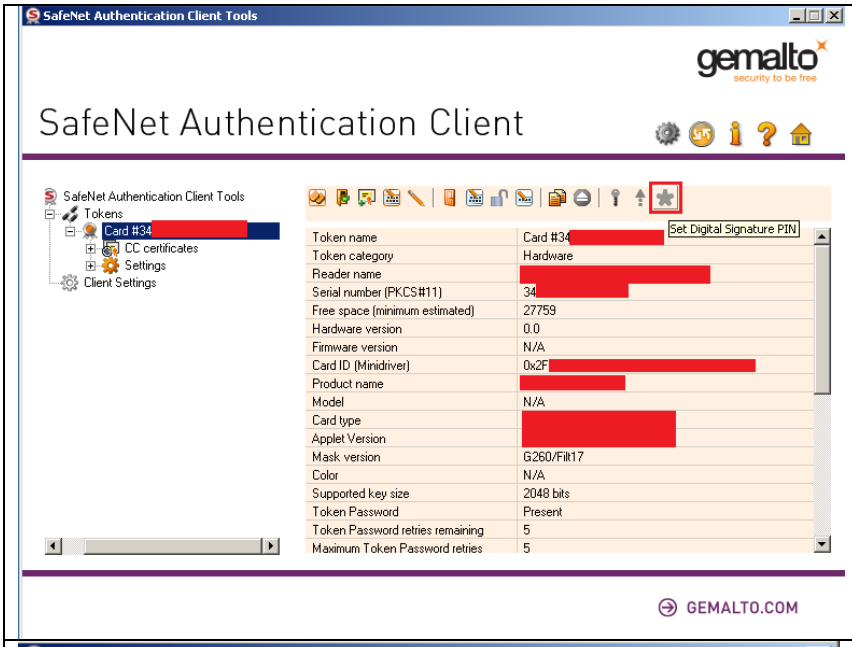
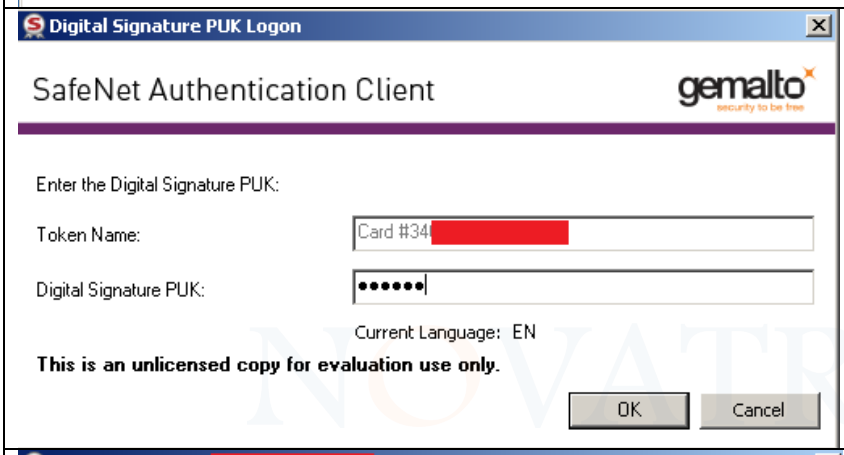
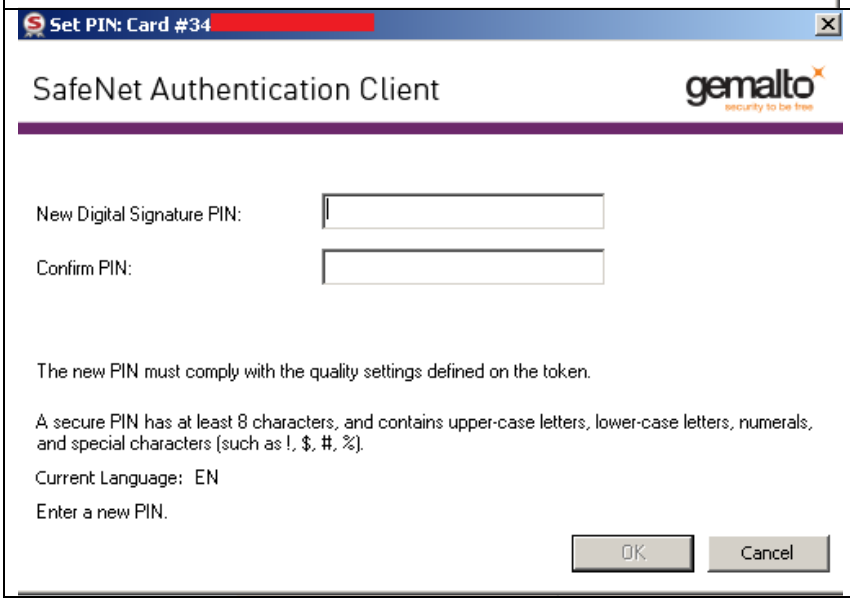
Αφού συμπληρωθούν όλα τα παραπάνω πεδία κάνουμε κλικ στο κουμπί OK.

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

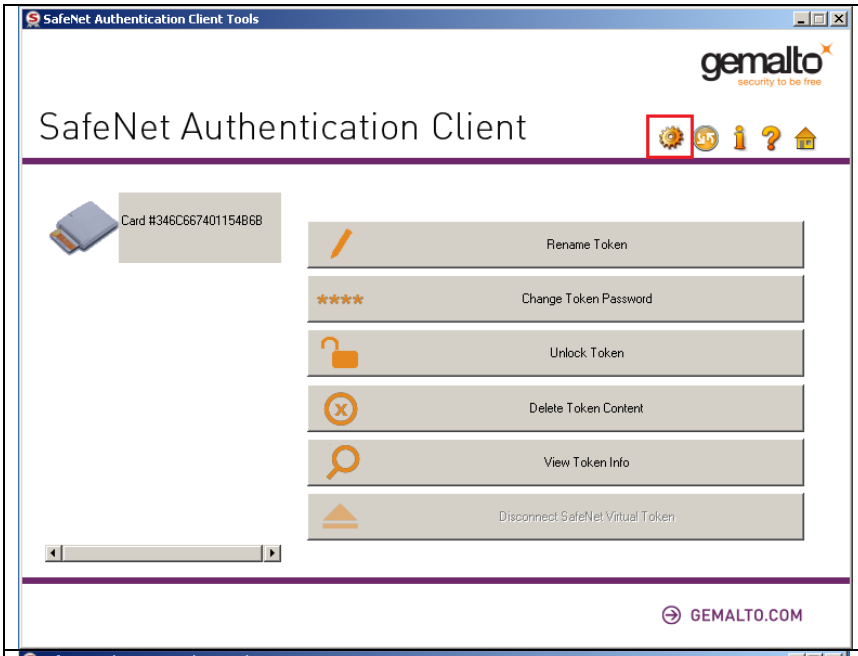
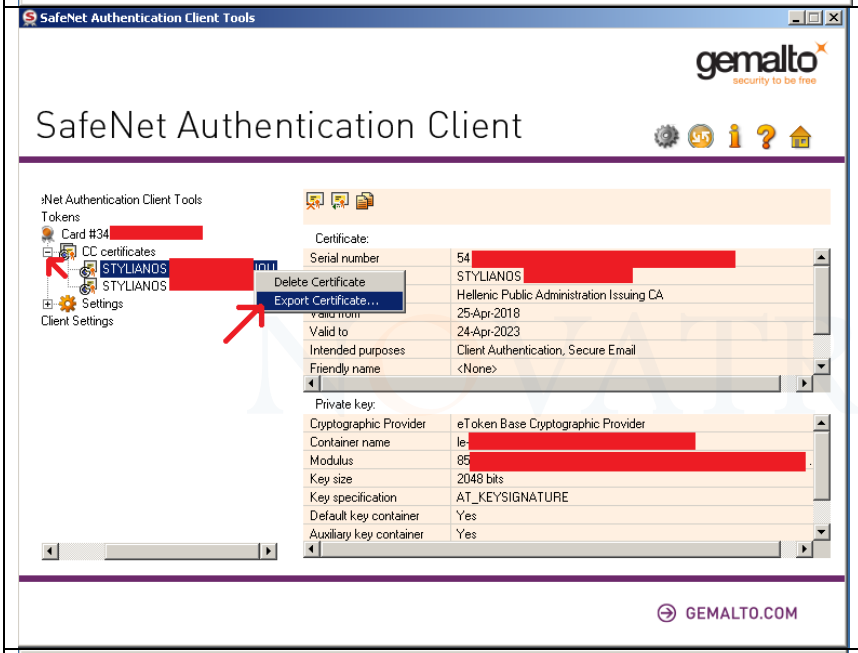
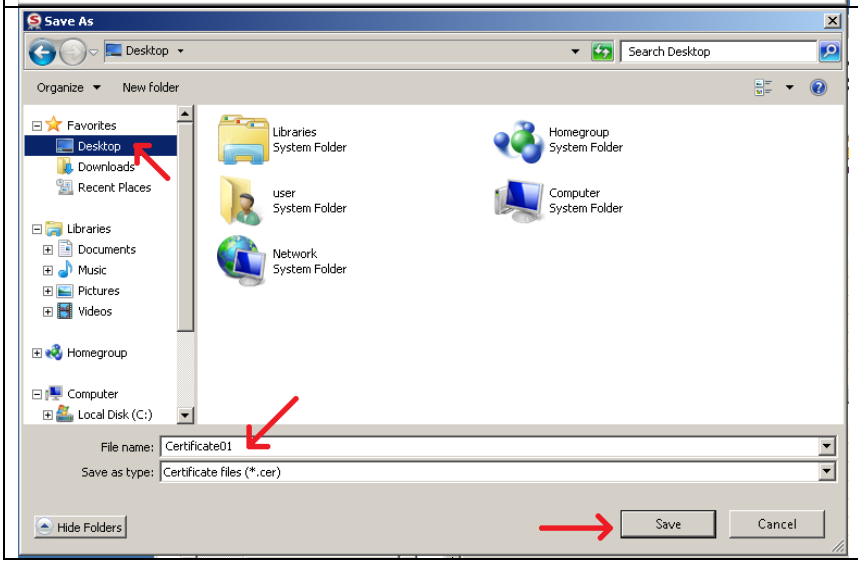
Σε περίπτωση που κλειδώσει ο κωδικός χρήστη ψηφιακής υπογραφής (PIN) μπορούμε να τον ξεκλειδώσουμε με τη χρήση του κωδικού διαχειριστή ψηφιακής υπογραφής (PUK) ακολουθώντας τα παρακάτω βήματα.

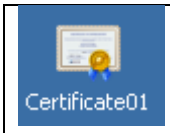


Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.

	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.

Πως μπορώ να εξάγω τα προσωπικά ψηφιακά πιστοποιητικά.

	Από την εφαρμογή Safenet Authentication Client επιλέγουμε το γρανάζι.
	Κάνουμε δεξί κλικ στο πιστοποιητικό που επιθυμούμε να εξάγουμε και επιλέγουμε Export Certificate.
	Δίνουμε ένα μοναδικό όνομα στο αρχείο εξαγωγής, επιλέγουμε το φάκελο αποθήκευσης και κάνουμε κλικ στο κουμπί Save.

	Αυτή η διαδικασία θα δημιουργήσει ένα αρχείο cer στο φάκελο που επιλέξαμε για την αποθήκευση. Ακολουθούμε την ίδια διαδικασία για την εξαγωγή και του δεύτερου πιστοποιητικού.

Χρήσιμοι σύνδεσμοι.

Αρχή Πιστοποίησης του Ελληνικού Δημοσίου	www.aped.gov.gr
Υπηρεσία Ανάπτυξης Πληροφορικής	www.yap.gov.gr