

Οδηγός Διαχείρισης και Εγκατάστασης
Ψηφιακού Πιστοποιητικού και Ηλεκτρονικής Υπογραφής
με τη χρήση του **Thales – Gemalto Prime MD940 USB Token**



THALES

gemalto
security to be free

Τεχνικά Χαρακτηριστικά.....	3
Εισαγωγή	4
Βήμα 1ο: Προμήθεια ΕΔΔΥ	4
Βήμα 2ο: Υπεύθυνη Δήλωση στην Πύλη gov.gr.....	4
Βήμα 3ο: Ηλεκτρονική αίτηση μέσω της εφαρμογής της ΑΠΕΔ	5
Βήμα 4ο: Μετάβαση σε ΚΕΠ.....	9
Βήμα 5ο: Εγκατάσταση Απαραίτητων Προγραμμάτων	10
Βήμα 6ο: Έκδοση Ψηφιακού Πιστοποιητικού	12
-Κωδικοί Που Θα Χρειαστούν Κατά Την Έκδοση του Ψηφιακού Πιστοποιητικού.....	13
-Χρήση Ψηφιακής Υπογραφή με το πρόγραμμα JsignPdf	15
-Διαχείριση κωδικών (PIN & PUK) και περιεχομένων της συσκευής.....	21
-Αλλαγή Password (PIN) & (PUK).....	22
-Διαγραφή Token (Αρχικοποίηση)	23
-Αρχικοί Προκαθορισμένοι Κωδικοί Συσκευής.....	24
-Πιθανά Προβλήματα κατά τη διαδικασία έκδοσης Νέου Πιστοποιητικού	25

Memory

- SafeNet IDPrime 940 is based on a 400KB Flash memory chip. SafeNet IDPrime 940B is based on a 500KB Flash memory chip. Both cards come as standard with 20 key containers. The memory available for certificates and other applets and data in this standard configuration is at least 73 KB.

Standards

- BaseCSP minidriver (SafeNet minidriver)
- Global Platform 2.2.1
- Java Card 3.0.4
- ISO 7816

Operating systems

- Windows, MAC, Linux

Cryptographic algorithms

- 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

Communication protocols

- T=0, T=1, PPS, with baud rate up to 446 Kbps at 3.57 MZ (TA1=97h)

Other features

- Onboard PIN Policy
- Multi-PIN support
- SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.

Technology

- Embedded crypto engine for symmetric and asymmetric cryptography

Lifetime

- Minimum 500,000 write/erase cycles
- Data retention for minimum 25 years

Certification

- CC EAL6+
- SafeNet IDPrime smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.
- SafeNet IDPrime 940 and SafeNet IDPrime 940B are 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, is eIDAS qualified for both eSignature and eSeal.

Εισαγωγή

Σε αυτόν τον οδηγό χρήσης περιγράφονται αναλυτικά όλες οι διαδικασίες που θα πρέπει να ακολουθηθούν προκειμένου ένας χρήστης να αποκτήσει ψηφιακό πιστοποιητικό από τη Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), για τη χρήση της ψηφιακής του υπογραφής.

Βήμα 1ο: Προμήθεια ΕΔΔΥ

Για αρχή, ο χρήστης θα πρέπει να προμηθευτεί κάποια Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ), η οποία είναι συμβατή με την ΑΠΕΔ και να εγκαταστήσει το διαχειριστικό της λογισμικό στο τερματικό που θα γίνει η έκδοση.

Η **ΕΔΔΥ** είναι μία ειδική συσκευή (έξυπνη κάρτα), σε μορφή USB token, που χρησιμοποιείται μόνο για τη δημιουργία ψηφιακής υπογραφής.

Οι συσκευές ΕΔΔΥ (USB token) της παλιάς ΑΠΕΔ **ΔΕΝ είναι συμβατές με την υποδομή της νέας ΑΠΕΔ.**

Το **Thales – Gemalto Prime MD940** λειτουργεί σε όλα τα λειτουργικά συστήματα **Windows (8,8.1,10,11)** καθώς και **Mac OS 10,11** σύμφωνα με τις ανακοινώσεις της αναβαθμισμένης ΑΠΕΔ.

Μπορείτε να το προμηθευτείτε μέσω της ιστοσελίδας μας , www.novatron.gr ή επικοινωνώντας με το τμήμα πωλήσεων της εταιρείας στο τηλέφωνο 210 6180 865.

Βήμα 2ο: Υπεύθυνη Δήλωση στην Πύλη gov.gr

Ο ενδιαφερόμενος χρήστης θα πρέπει να μεταβεί στο gov.gr στην αίτηση – υπεύθυνη δήλωση (Υ/Δ) για έκδοση Ψ/Π.

Ο χρήστης επιλέγει το τυποποιημένο κείμενο της Υ/Δ και ταυτοποιείται στο σύστημα με έναν από τους παρακάτω τρόπους:

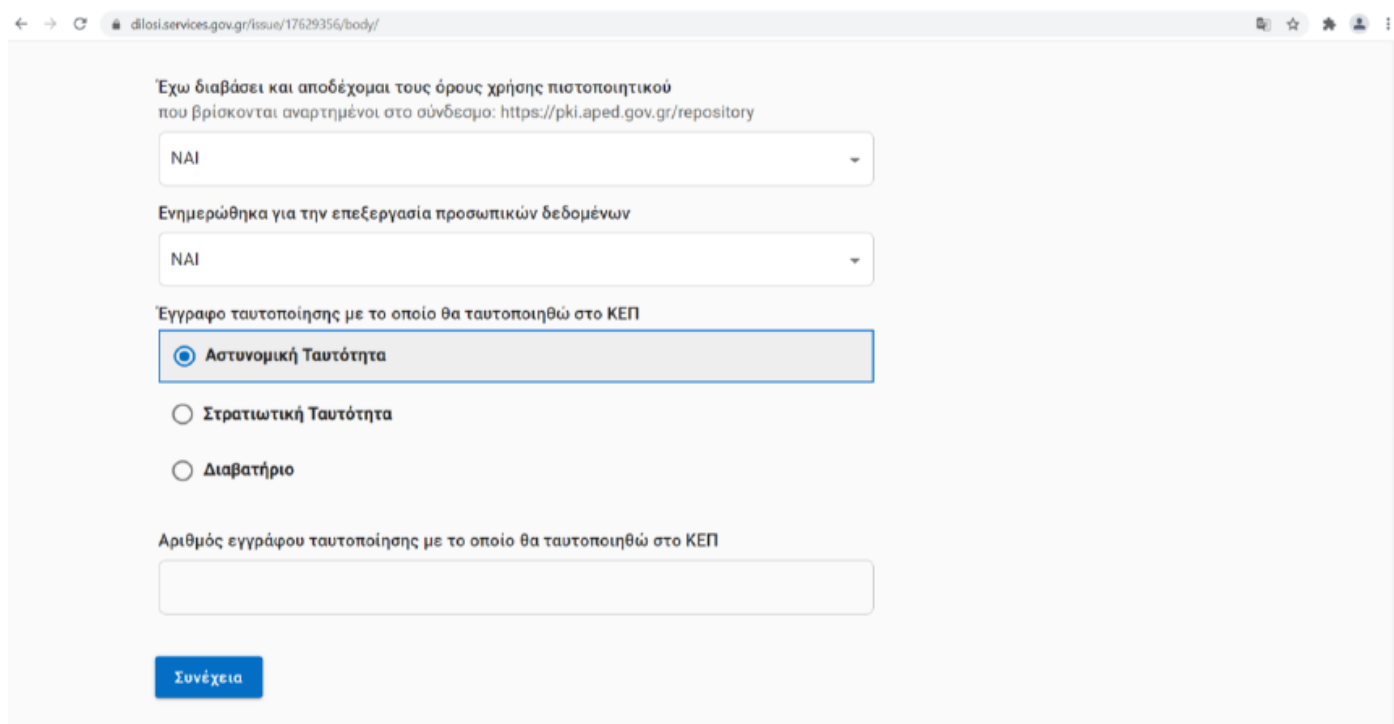
1. με τους προσωπικούς κωδικούς στο Taxisnet.

- Κατά την πρώτη είσοδο σε υπηρεσίες gov.gr μόνο, ο χρήστης θα χρησιμοποιήσει τους προσωπικούς κωδικούς Web banking σε **Εθνική Τράπεζα της Ελλάδος, Τράπεζα Πειραιώς, Alpha Bank, Eurobank, Παγκρήτια Τράπεζα, Τράπεζα Ηπείρου, Συνεταιριστική Τράπεζα Καρδίτσας ή Τράπεζα Κεντρικής Μακεδονίας** για την επιβεβαίωση του αριθμού του κινητού τηλεφώνου. Σε κάθε επόμενη είσοδο σε υπηρεσία του gov.gr απαιτούνται μόνο οι κωδικοί Taxisnet.

- Εναλλακτικά, πριν την πρώτη είσοδο, θα πρέπει να έχει εγγραφεί στο [Εθνικό Μητρώο Επικοινωνίας \(ΕΜΕπ\)](#) ώστε να επιβεβαιωθεί ο αριθμός κινητού τηλεφώνου. Σε κάθε επόμενη είσοδο σε υπηρεσία του gov.gr απαιτούνται μόνο οι κωδικοί Taxisnet.

2. με τους προσωπικούς κωδικούς Web banking σε μία από τις παραπάνω τράπεζες

Στη συνέχεια, ο χρήστης λαμβάνει κωδικούς επιβεβαίωσης με SMS στο κινητό και προχωράει στη δημιουργία της Υ/Δ.



The screenshot shows a web browser window with the URL dilos.services.gov.gr/issue/17629356/body/. The page contains the following elements:

- A text block: "Έχω διαβάσει και αποδέχομαι τους όρους χρήσης πιστοποιητικού που βρίσκονται αναρτημένοι στο σύνδεσμο: <https://pki.aped.gov.gr/repository>"
- A dropdown menu with "NAI" selected.
- A text block: "Ενημερώθηκα για την επεξεργασία προσωπικών δεδομένων"
- A dropdown menu with "NAI" selected.
- A text block: "Έγγραφο ταυτοποίησης με το οποίο θα ταυτοποιηθώ στο ΚΕΠ"
- Three radio button options: "Αστυνομική Ταυτότητα" (selected), "Στρατιωτική Ταυτότητα", and "Διαβατήριο".
- A text block: "Αριθμός εγγράφου ταυτοποίησης με το οποίο θα ταυτοποιηθώ στο ΚΕΠ"
- An empty text input field.
- A blue button labeled "Συνέχεια".

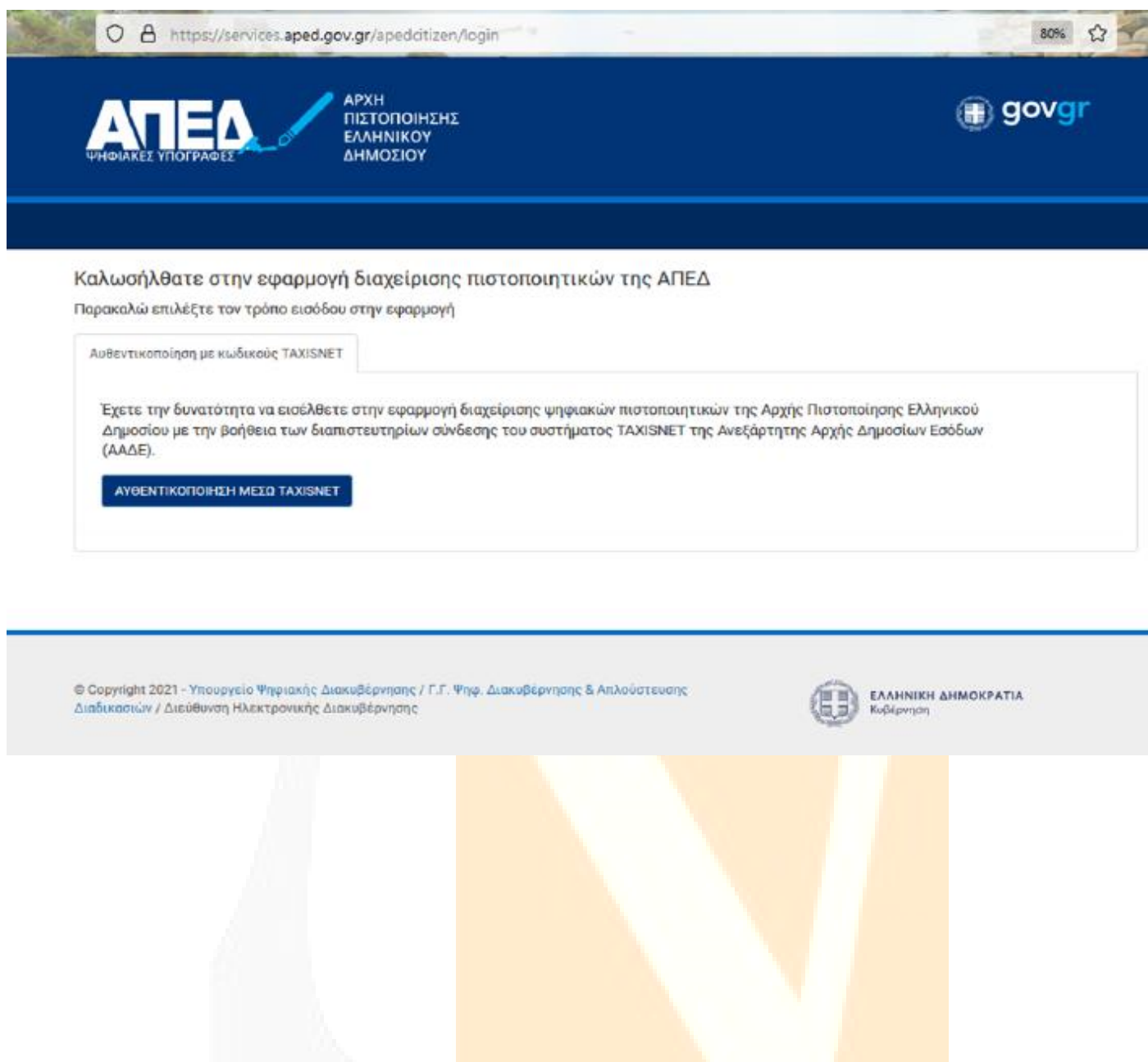
Η Υ/Δ που δημιουργείται έχει ένα μοναδικό **κωδικάριθμο**, τον οποίο κρατάτε για να χρησιμοποιήσετε στο επόμενο βήμα.

[Βήμα 3ο: Ηλεκτρονική αίτηση μέσω της εφαρμογής της ΑΠΕΔ](#)

Το πρώτο βήμα για την απόκτηση ψηφιακού πιστοποιητικού είναι η υποβολή ηλεκτρονικού αιτήματος. Ο χρήστης μεταβαίνει στο

<https://services.aped.gov.gr/apedcitizen/login>

Μπορεί να εισέλθει μέσω κωδικών taxisnet ...



Στη συνέχεια θα πατήσει το κουμπί «Υποβολή Αίτησης»

Διαδικασία έκδοσης Ψηφιακής Υπογραφής

- Βήμα 1: Προμήθεια ΕΔΔΥ
- Βήμα 2: Υπεύθυνη Δήλωση στην Πύλη gov.gr
- Βήμα 3: Ηλεκτρονική αίτηση μέσω της εφαρμογής της ΑΠΕΔ
- Βήμα 4: Μετάβαση σε Εντεταλμένο Γραφείο
- Βήμα 5: Εγκατάσταση απαραίτητων προγραμμάτων
- Βήμα 6: Έκδοση ψηφιακού πιστοποιητικού

Δείτε αναλυτικές οδηγίες στο [Πώς θα αποκτήσω ψηφιακή υπογραφή](#)

Για να εκκινήσετε την διαδικασία έκδοσης ψηφιακών πιστοποιητικών, πρέπει να υποβάλλετε ηλεκτρονική αίτηση.

[Υποβολή Αίτησης](#)



Οπότε θα εμφανιστεί η ηλεκτρονική αίτηση η οποία αποτελείται από δύο μέρη:

Α) Το πρώτο μέρος αφορά στοιχεία τα οποία λαμβάνονται αυτόματα από το λογαριασμό στη πύλη ΕΡΜΗΣ και αυτά δεν μπορούν να τροποποιηθούν.

Β) Το δεύτερο αφορά στοιχεία που θα πρέπει να συμπληρώσει ο πολίτης και σχετίζονται με το email, τη διεύθυνση κατοικίας του αιτούντος και τον **κωδικάριθμο** από την αίτηση-Υ/Δ του gov.gr. Αυτά θα πρέπει υποχρεωτικά να συμπληρωθούν πριν αποσταλεί η αίτηση .

Κωδικός: VGq8vp2iJuXaFpirB-οθ_Q

Επιβεβαιώνεται το γνήσιο. Υπουργείο
Ψηφιακής Διακυβέρνησης / Verified by the Ministry
of Digital Governance, Hellenic Republic
20220205131103+02'00'



Αίτηση - Υπεύθυνη Δήλωση: Έκδοση εγκεκριμένου πιστοποιητικού Ηλεκτρονικής Υπογραφής

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 ⁽¹⁾ :	Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)						
Όνομα:				Επώνυμο:			
Όνομα και Επώνυμο Πατέρα:							
Όνομα και Επώνυμο Μητέρας:							
Ημερομηνία γέννησης:							
Τόπος Γέννησης:							
Αριθμός Δελτίου Ταυτότητας:				Τηλ:			
Τόπος Κατοικίας:			Οδός:			Αριθ:	ΤΚ:

Ο χρήστης, αφού συμπληρώσει όλα τα απαραίτητα πεδία της αίτησης και είναι βέβαιος για την ορθότητα τους, πατάει το κουμπί «Υποβολή Αίτησης»

Βήμα 4ο: Μετάβαση σε ΚΕΠ

Στη συνέχεια ο χρήστης μεταβαίνει στο ΚΕΠ, έχοντας μαζί του το ταυτοποιητικό έγγραφο που έχει δηλώσει στην ηλεκτρονική αίτηση στο gov.gr, προκειμένου να γίνει η φυσική ταυτοποίηση από τον υπάλληλο.



Πορεία Αιτήματος Έκδοσης Ψηφιακού Πιστοποιητικού



Έχετε υποβάλει επιτυχώς την ηλεκτρονική αίτηση έκδοσης ψηφιακού πιστοποιητικού. Πρέπει να μεταβείτε σε οποιοδήποτε Κέντρο Εξυπηρέτησης Πολιτών (ΚΕΠ) ώστε να ολοκληρώσετε την διαδικασία φυσικής ταυτοποίησης. Μην ξεχάσετε να φέρετε μαζί σας το έγγραφο πιστοποίησης ταυτότητας που έχετε δηλώσει στην υπεύθυνη δήλωση που υποβάλλατε στο gov.gr. Σε περίπτωση που επιθυμείτε να ακυρώσετε το αίτημα έκδοσης του ψηφιακού πιστοποιητικού πατήστε [εδώ](#).

- Ο υπάλληλος ταυτοποιεί τον χρήστη και επιβεβαιώνει την ορθότητα των στοιχείων της Υ/Δ του gov.gr. Ελέγχει την ταύτιση των στοιχείων ανάμεσα στην Υ/Δ και την αίτηση της ΑΠΕΔ. Αν δεν υπάρχει ταύτιση θα ακυρώνεται το αίτημα.
- Ο υπάλληλος διορθώνει, αν απαιτείται, τα πεδία που μπορεί να επεξεργαστεί [ονοματεπώνυμο (λατινικά), διεύθυνση, email]. Η λατινική γραφή του ονοματεπώνυμου θα είναι ίδια με αυτή που αναφέρεται στο ταυτοποιητικό έγγραφο.
- Το αναγνωριστικό του ταυτοποιητικού εγγράφου (ταυτότητα ή διαβατήριο) εισάγεται αυτόματα από την αίτηση gov.gr. Το ταυτοποιητικό έγγραφο πρέπει να είναι το ίδιο με αυτό που έχει εισάγει στην αίτηση gov.gr ο συνδρομητής και είναι είτε ταυτότητα (αστυνομική ή στρατιωτική), είτε διαβατήριο.
- Ο υπάλληλος του ΕΓ ολοκληρώνει την ταυτοποίηση και καταχώρηση του αιτήματος («Ολοκλήρωση ενεργειών»). Αυτόματα αποστέλλεται sms στο κινητό του συνδρομητή που ενημερώνει ότι ολοκληρώθηκε επιτυχώς η φυσική ταυτοποίηση.
- Στο portal, στην οθόνη διαχείρισης ΨΠ του συνδρομητή, θα αναγράφεται ότι έχει γίνει η ταυτοποίηση από Εντεταλμένο Γραφείο καθώς και ο μοναδικός αναγνωριστικός αριθμός.

- Η αίτηση προωθείται αυτόματα στην Αρχή Εγγραφής όπου ολοκληρώνεται η έγκριση της αίτησης του ενδιαφερόμενου μέσα σε διάστημα έως 30 ημερών

ΠΡΟΣΟΧΗ : Σε αυτό το σημείο, ο συνδρομητής θα πρέπει να περιμένει να λάβει ένα 2ο αυτοματοποιημένο SMS , στο οποίο θα του αναγράφεται ο κωδικός έκδοσης - ανάκλησης ψηφιακού πιστοποιητικού.

Βήμα 5ο: Εγκατάσταση Απαραίτητων Προγραμμάτων

1. Θα πρέπει να γίνει εγκατάσταση των οδηγών (drivers) της ΕΔΔΥ που έχει προμηθευτεί ο τελικός χρήστης.

Ιδιαίτερη προσοχή θα πρέπει να δοθεί:

- στην έκδοση του λειτουργικού συστήματος του τελικού χρήστη και
- τον τύπο ΕΔΔΥ που έχει προμηθευτεί

Τα βήματα που απαιτούνται συνοδεύουν υποχρεωτικά την ΕΔΔΥ (USB token) κατά την αγορά της.

Η διαδικασία θα πρέπει να γίνει μία φορά. Παρακάτω αναφέρονται οι οδηγοί που απαιτούνται για την έκδοση του πιστοποιητικού. Για την εγκατάσταση των οδηγών στους υπολογιστές που επιθυμείτε να υπογράφετε ,ακολουθείτε τους συνδέσμους παρακάτω:

Thales/Gemalto Prime MD940 – ΟΔΗΓΟΣ (DRIVER)

Windows 10,11 (Θα εγκαταστήσετε και τους δύο drivers παρακάτω)

[SafeNet Minidriver 10.8 R6\(Post GA\)](#)

[SafeNet Authentication Client \(SAC\) 10.8 R6\(Post GA\)](#)

[MacOS 11 – SAC 10.2](#)

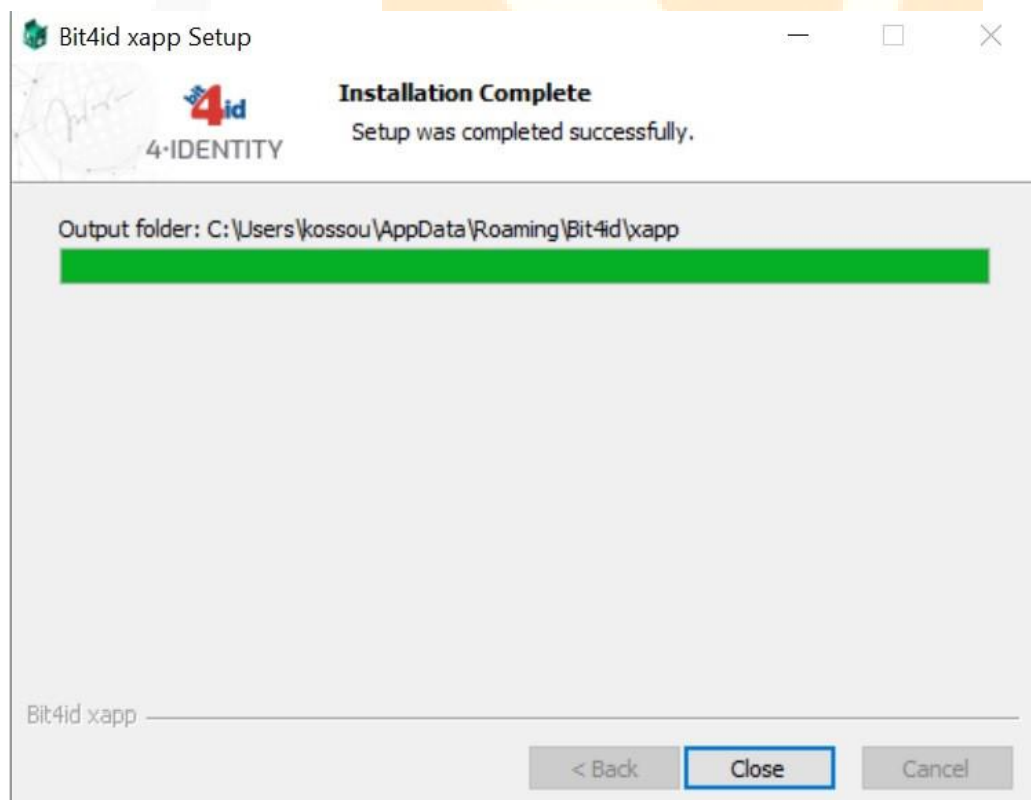
2. Για την έκδοση μόνο του ψηφιακού πιστοποιητικού θα πρέπει να εγκατασταθεί μία κατάλληλη εφαρμογή (BIT4ID middleware) από τον παρακάτω σύνδεσμο:

[BIT4ID για Windows 10, 11](#)

[BIT4ID για MacOS 11, 12](#)



Ο χρήστης θα πρέπει να πατήσει το κουμπί «install» και όταν εμφανιστεί το μήνυμα «**Setup was completed successfully**», τότε θα πατήσει το κουμπί «Close»



Βήμα 6ο: Έκδοση Ψηφιακού Πιστοποιητικού

Όταν ολοκληρωθεί η έγκριση της αίτησης (μέσα σε διάστημα έως 30 ημερών), ο ενδιαφερόμενος λαμβάνει SMS που περιέχει τον **οκταψήφιο κωδικό έκδοσης/ ανάκλησης** (απαιτείται για την έκδοση ψηφιακού πιστοποιητικού).

Ο ενδιαφερόμενος συνδέεται στην **εφαρμογή της ΑΠΕΔ**. Τσεκάρει τη επιλογή «έχω ολοκληρώσει επιτυχώς όλες τις αναγκαίες παραμετροποιήσεις του ηλεκτρονικού μου υπολογιστή» και επιλέγει «Αποθήκευση σε ΕΔΔΥ».



Έκδοση Ψηφιακού Πιστοποιητικού

Οδηγίες

Πριν προχωρήσετε στην έναρξη της διαδικασίας έκδοσης ψηφιακού πιστοποιητικού βεβαιωθείτε για τα ακόλουθα :

1. Έχετε λάβει τον προσωπικό σας κωδικό έκδοσης / ανάκλησης ψηφιακού πιστοποιητικού στο κινητό σας τηλέφωνο με την μορφή γραπτού μηνύματος. Εάν δεν έχετε λάβει γραπτό μήνυμα ή έχετε χάσει τον κωδικό σας, αιτηθείτε νέο κωδικό: [Πατήστε εδώ](#)
2. Έχετε ακολουθήσει τις οδηγίες που περιέχονται στο Βήμα 5 [εδώ](#).

☒ Έχω ολοκληρώσει επιτυχώς όλες τις αναγκαίες παραμετροποιήσεις του ηλεκτρονικού μου υπολογιστή.

Επιλέξτε το ψηφιακό μέσο αποθήκευσης στο οποίο θα εγκατασταθεί το ψηφιακό πιστοποιητικό σας :

Αποθήκευση σε ΕΔΔΥ

Συμπληρώστε τον προσωπικό σας κωδικό έκδοσης / ανάκλησης ψηφιακού πιστοποιητικού :

Έκδοση ψηφιακού πιστοποιητικού

Μετά, συνδέει την ΕΔΔΥ(usb token) στον υπολογιστή, συμπληρώνει τον οκταψήφιο κωδικό έκδοσης και πατάει το κουμπί «Έκδοση ψηφιακού πιστοποιητικού».

ΑΠΕΔ
ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

govgr

Έκδοση Ψηφιακού Πιστοποιητικού - Token

Η σύνδεση με το πρόγραμμα οδήγησης ολοκληρώθηκε με επιτυχία

Παρακαλώ επιλέξτε το μοντέλο ΕΔΔΥ

Safenet 5110cc/Gemalto/Thales
TokenME EVO/ Oberthur/ IDEMIA

Έκδοση Ψηφιακού Πιστοποιητικού

Οδηγίες

Πριν προχωρήσετε στην έναρξη της διαδικασίας έκδοσης ψηφιακού πιστοποιητικού βεβαιωθείτε για τα ακόλουθα :

1. Έχετε λάβει τον προσωπικό σας κωδικό έκδοσης / ανάκλησης ψηφιακού πιστοποιητικού στο κινητό σας τηλέφωνο με την μορφή γραπτού μηνύματος. Εάν δεν έχετε λάβει γραπτό μήνυμα ή έχετε χύσει τον κωδικό σας, αιτηθείτε νέο κωδικό: [Πατήστε εδώ](#)
2. Έχετε ακολουθήσει τις οδηγίες που περιέχονται στο Βήμα 5 [εδώ](#).

☒ Έχω ολοκληρώσει επιτυχώς όλες τις αναγκαίες παραμετροποιήσεις του ηλεκτρονικού μου υπολογιστή.

Επιλέξτε το ψηφιακό μέσο αποθήκευσης στο οποίο θα εγκατασταθεί το ψηφιακό πιστοποιητικό σας :

Αποθήκευση σε ΕΔΔΥ

Συμπληρώστε τον προσωπικό σας κωδικό έκδοσης / ανάκλησης ψηφιακού πιστοποιητικού :

Έκδοση ψηφιακού πιστοποιητικού

Στη συνέχεια γίνεται εκκίνηση του middleware(το οποίο έχει εγκατασταθεί νωρίτερα, στα προηγούμενα βήματα) και εμφανίζεται ένα μενού που περιέχει τις συμβατές, με την ΑΠΕΔ, ΕΔΔΥ.

Εδώ ο χρήστης επιλέγει “SafeNet 5110cc/Gemalto/Thales”

Αφού έχει εκκινήσει το middleware και η ΕΔΔΥ έχει αναγνωριστεί, τότε θα ζητηθεί το **Token Password(ΕΔΔΥ PIN)** και το **Digital Signature PIN** προκειμένου να υπάρξει πρόσβαση στην ΕΔΔΥ για να μπορέσουν να εγκατασταθούν τα ψηφιακά πιστοποιητικά.

Το **Token Password(ΕΔΔΥ PIN)** είναι : **0000** και το **Digital Signature PIN** της συσκευής είναι : **000000**, τα οποία μπορούν να τροποποιηθούν μέσα από το διαχειριστικό λογισμικό του usb token σε παρακάτω βήματα.

Αφού πληκτρολογήσει το **Token Password(ΕΔΔΥ PIN)** σωστά, ξεκινάει η διαδικασία της έκδοσης του πιστοποιητικού, στη συνέχεια θα ζητηθεί να πληκτρολογήσει το **Digital Signature PIN**.

Στο τέλος της διαδικασίας, εμφανίζεται το ψηφιακό πιστοποιητικό στο λογαριασμό του χρήστη.

-Κωδικοί Που Θα Χρειαστούν Κατά Την Έκδοση του Ψηφιακού Πιστοποιητικού

Token Password (PIN ΕΔΔΥ): 0000

Digital Signature PIN: 000000

Τα ψηφιακά πιστοποιητικά μου

Τύπος Ψηφιακού Πιστοποιητικού	Κατάσταση	Έναρξη Ισχύος	Λήξη Ισχύος	Προβολή	Ανάκληση
Ψηφιακής Υπογραφής	Έγκυρο				



Σε περίπτωση που επιθυμείτε να προχωρήσετε σε ανάκληση του ψηφιακού πιστοποιητικού σας, θα πρέπει να πατήσετε το κουμπί Ανάκληση και να συμπληρώσετε τον προσωπικό σας κωδικό έκδοσης / ανάκλησης του ψηφιακού πιστοποιητικού τον οποίο λάβατε μέσω γραπτού μηνύματος (SMS) από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) κατά την έγκριση του αιτήματος έκδοσης του ψηφιακού πιστοποιητικού σας. Εναλλακτικά, μπορείτε να υποβάλλετε αίτημα ανάκλησης του ψηφιακού πιστοποιητικού στην πύλη gov.gr και ακολούθως να συμπληρώσετε τον κωδικό αριθμό της αίτησης αυτής αφού πρώτα πατήσετε το κουμπί Ανάκληση.

Εάν ο ενδιαφερόμενος δεν ολοκληρώσει την έκδοση του πιστοποιητικού μέσα σε 45 ημέρες από την ταυτοποίηση στο ΚΕΠ, τότε η αίτησή του ακυρώνεται αυτόματα.

Σημείωση: Η ΑΠΕΔ δεν παρέχει πλέον ψηφιακό πιστοποιητικό κρυπτογράφησης. Το ψηφιακό πιστοποιητικό που έχει ο πολίτης, μπορεί να χρησιμοποιηθεί μόνο για την υπογραφή εγγράφων.

Το Thales/Gemalto USB Token περιέχει τα ψηφιακά σας πιστοποιητικά και έτσι μπορείτε να υπογράφετε τα έγγραφά σας στον υπολογιστή σας.

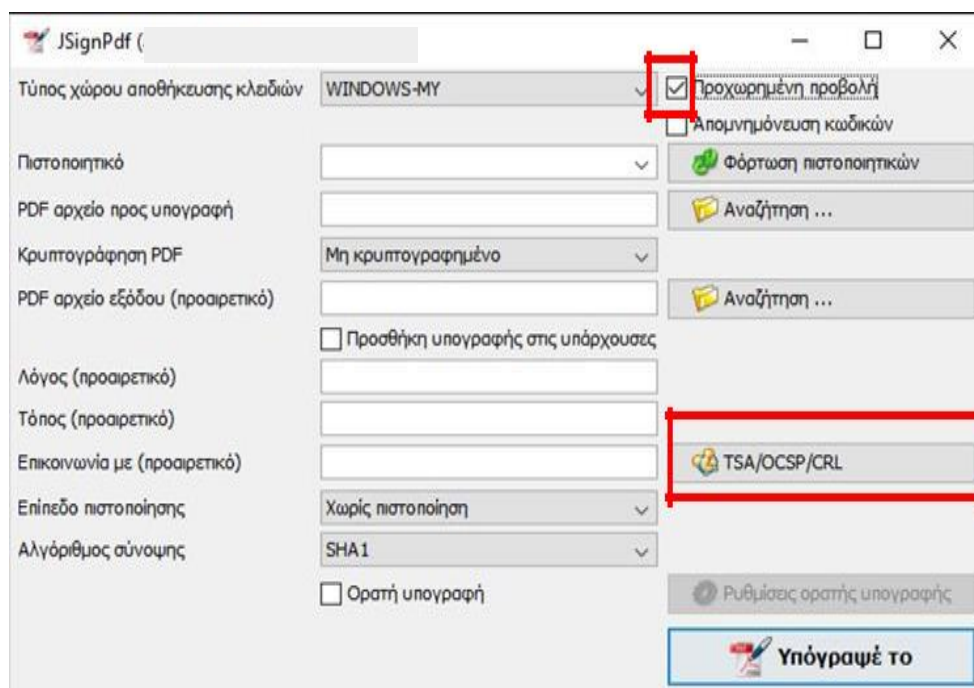
ΣΗΜΑΝΤΙΚΟ: Μετά την ολοκλήρωση έκδοσης του ψηφιακού πιστοποιητικού, ενδεχομένως να χρειαστεί να αφαιρέσετε και να τοποθετήσετε εκ νέου την συσκευή ΕΔΔΥ στον υπολογιστή σας, ώστε να αναγνωριστεί το νέο πιστοποιητικό.

-Χρήση Ψηφιακής Υπογραφή με το πρόγραμμα JsignPdf

Το πρόγραμμα JsignPdf είναι ένα ελεύθερο στο διαδίκτυο πρόγραμμα, μπορείτε να το κατεβάσετε και από εδώ:

JSignPdf

Κατεβάζετε, εκτελείτε και εγκαθιστάτε το πρόγραμμα, μόλις εμφανιστεί η αρχική σελίδα επιλέγετε Προχωρημένη Προβολή και στη συνέχεια κάνετε κλικ στο κουμπί TSA/OCSP/CRL. :

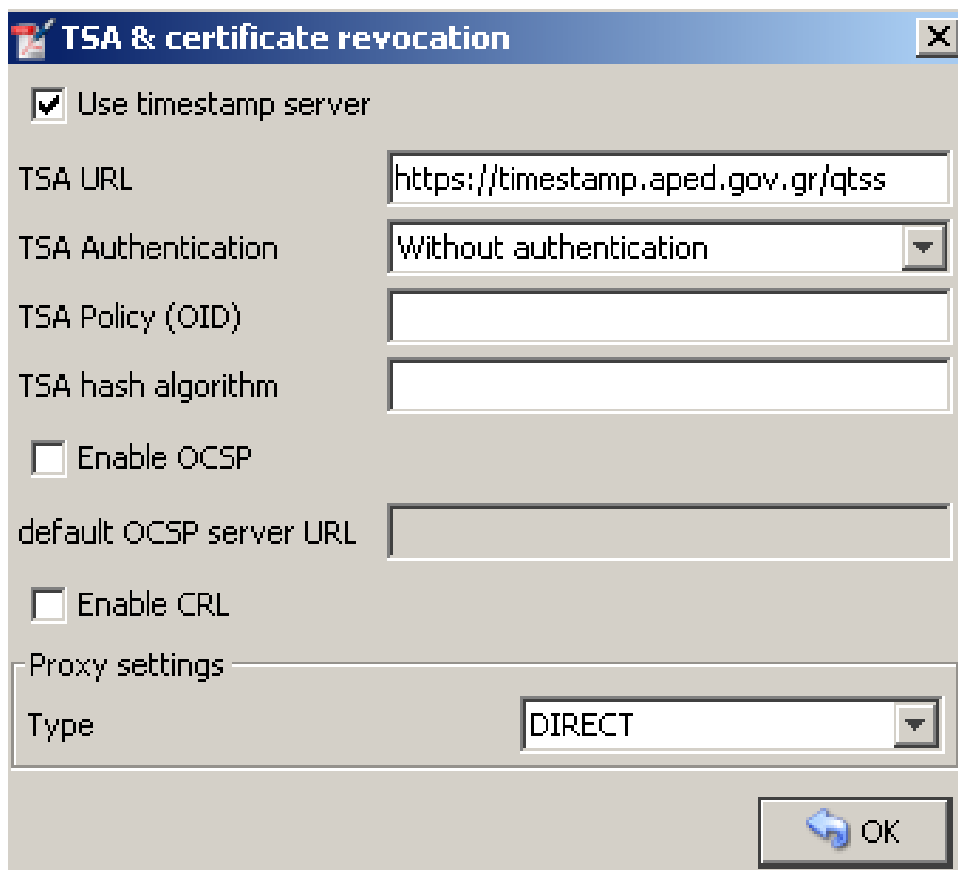


Επιλέγετε... Χρησιμοποίησε ασφαλή χρονοσήμανση.

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

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

Κάνετε κλικ στο κουμπί OK.



TSA & certificate revocation

☒ Use timestamp server

TSA URL:

TSA Authentication:

TSA Policy (OID):

TSA hash algorithm:


☐ Enable OCSP

default OCSP server URL:

☐ Enable CRL

Proxy settings

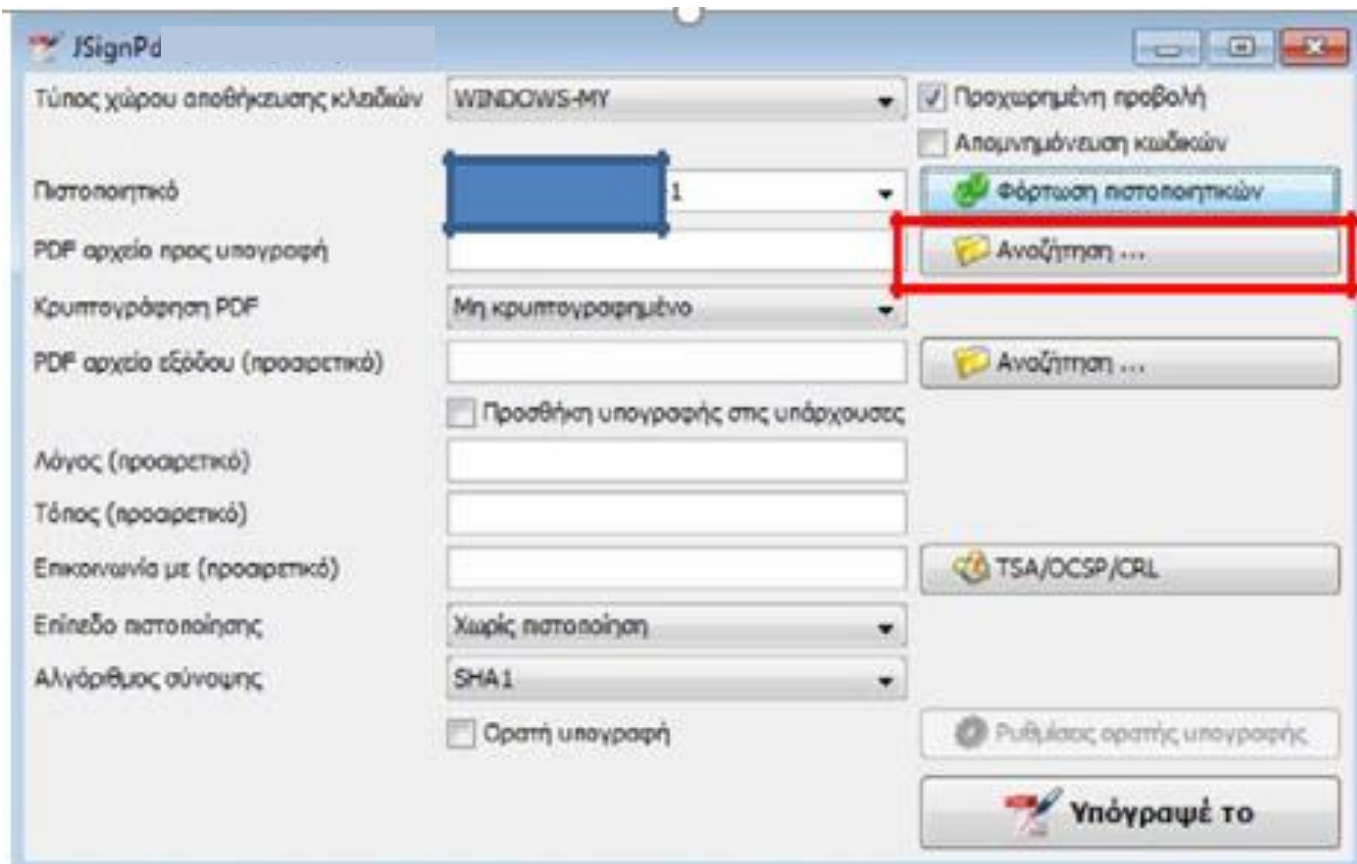
Type:

 OK

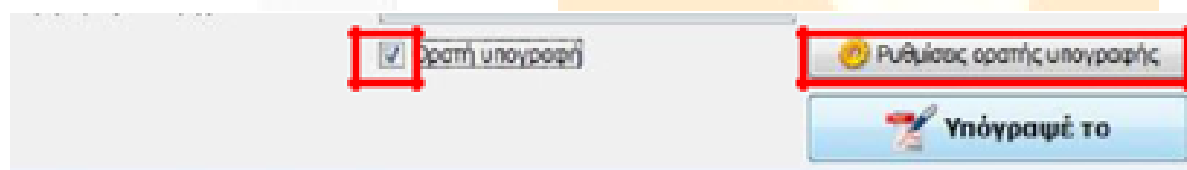
Η παραπάνω διαδικασία γίνεται μία φορά, το πρόγραμμα αποθηκεύει τις ρυθμίσεις.

Έχετε συνδεδεμένο στον υπολογιστή σας το USB Token σας. Έπειτα κάνετε κλικ στο κουμπί Φόρτωση πιστοποιητικών και αριστερά φαίνεται το Ψηφιακό σας Πιστοποιητικό (Με αναφορά στο Ονοματεπώνυμο του Χρήστη).

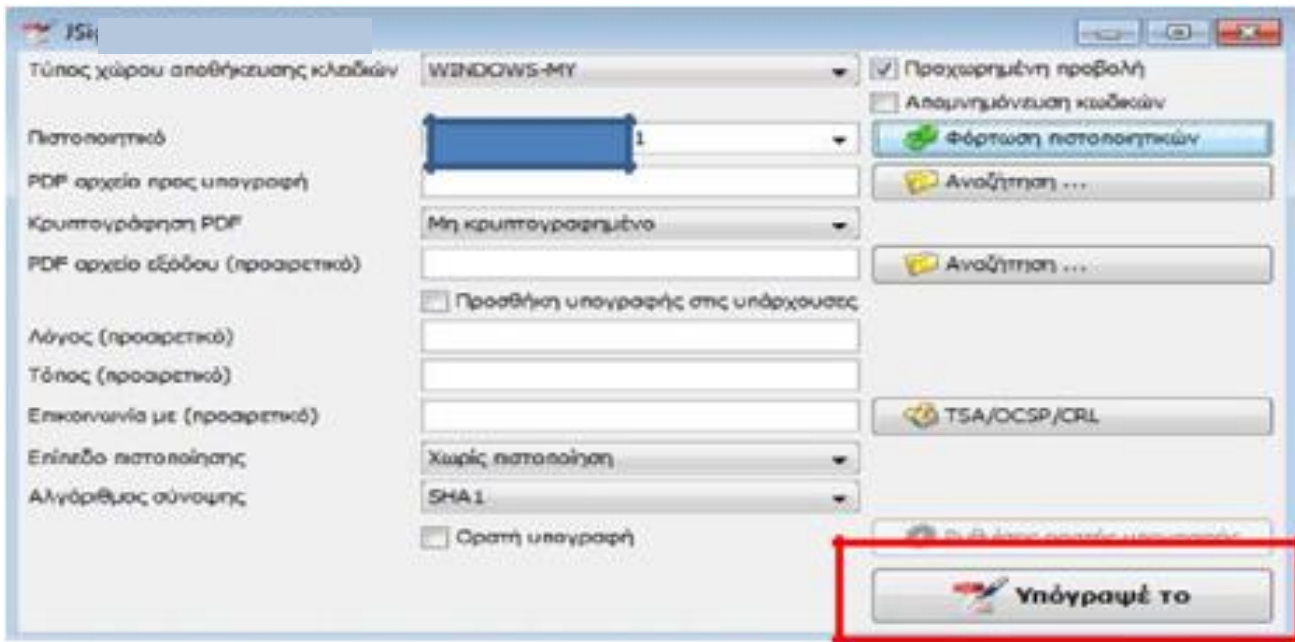
Κάνετε κλικ στο πρώτο κουμπί Αναζήτηση για να επιλέξετε το PDF αρχείο προς υπογραφή:



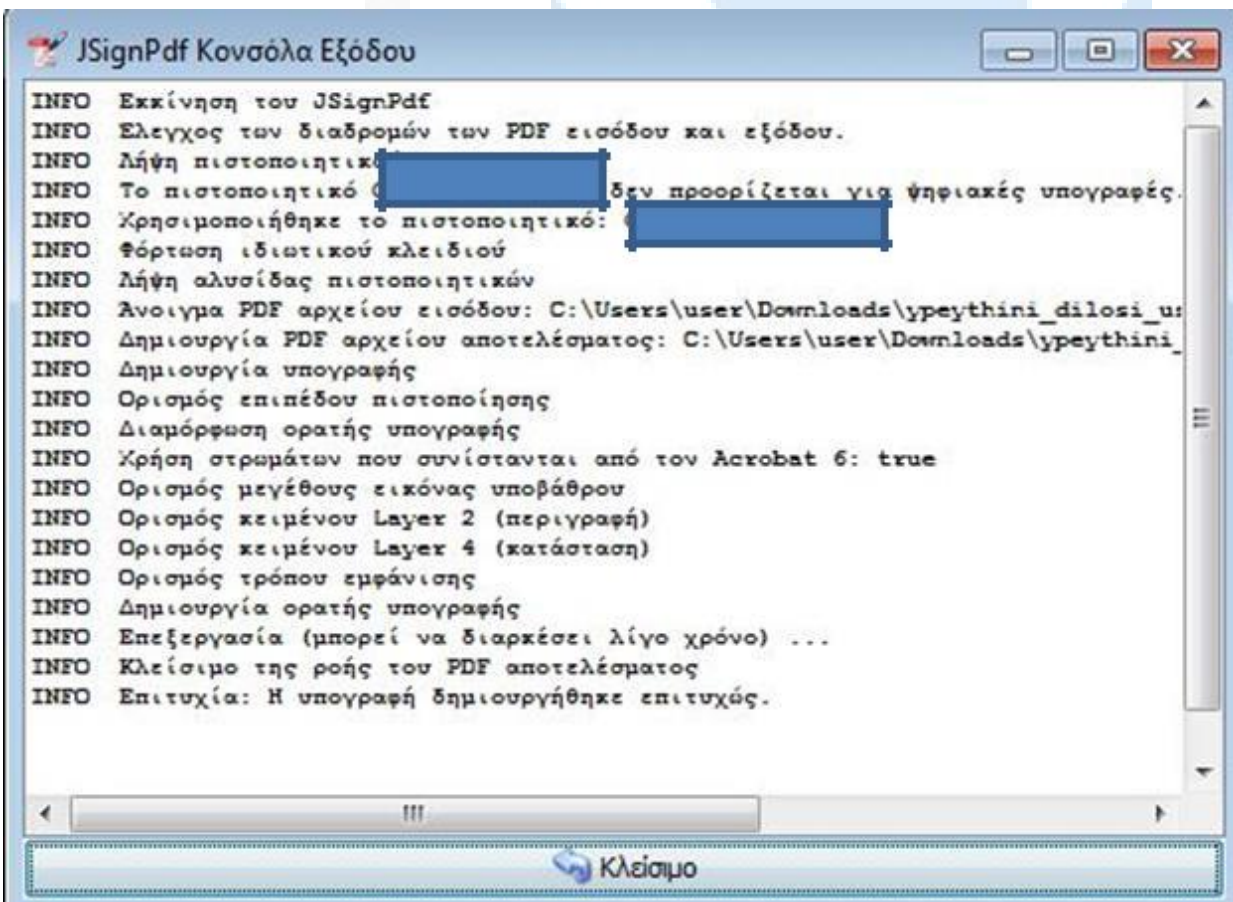
Για να προσθέσετε Ορατή Υπογραφή, επιλέγετε Ορατή υπογραφή, κάνετε κλικ στο κουμπί Ρυθμίσεις ορατής υπογραφής, επιλέγετε Προεπισκόπηση & Επιλογή θέσης όπου εμφανίζεται το έγγραφο στο οποίο (με το αριστερό κλικ από το ποντίκι σας) επιλέγετε το που θα τοποθετηθεί η υπογραφή σας και κάνετε κλικ στο κουμπί Κλείσιμο (2 φορές):



Κάνετε κλικ στο κουμπί **Υπογράψτε το** και αυτόματα σας ζητάει το PIN που για το συγκεκριμένο Token είναι 6 φορές το 0 (000000), το εισάγετε και πατάτε Ok.

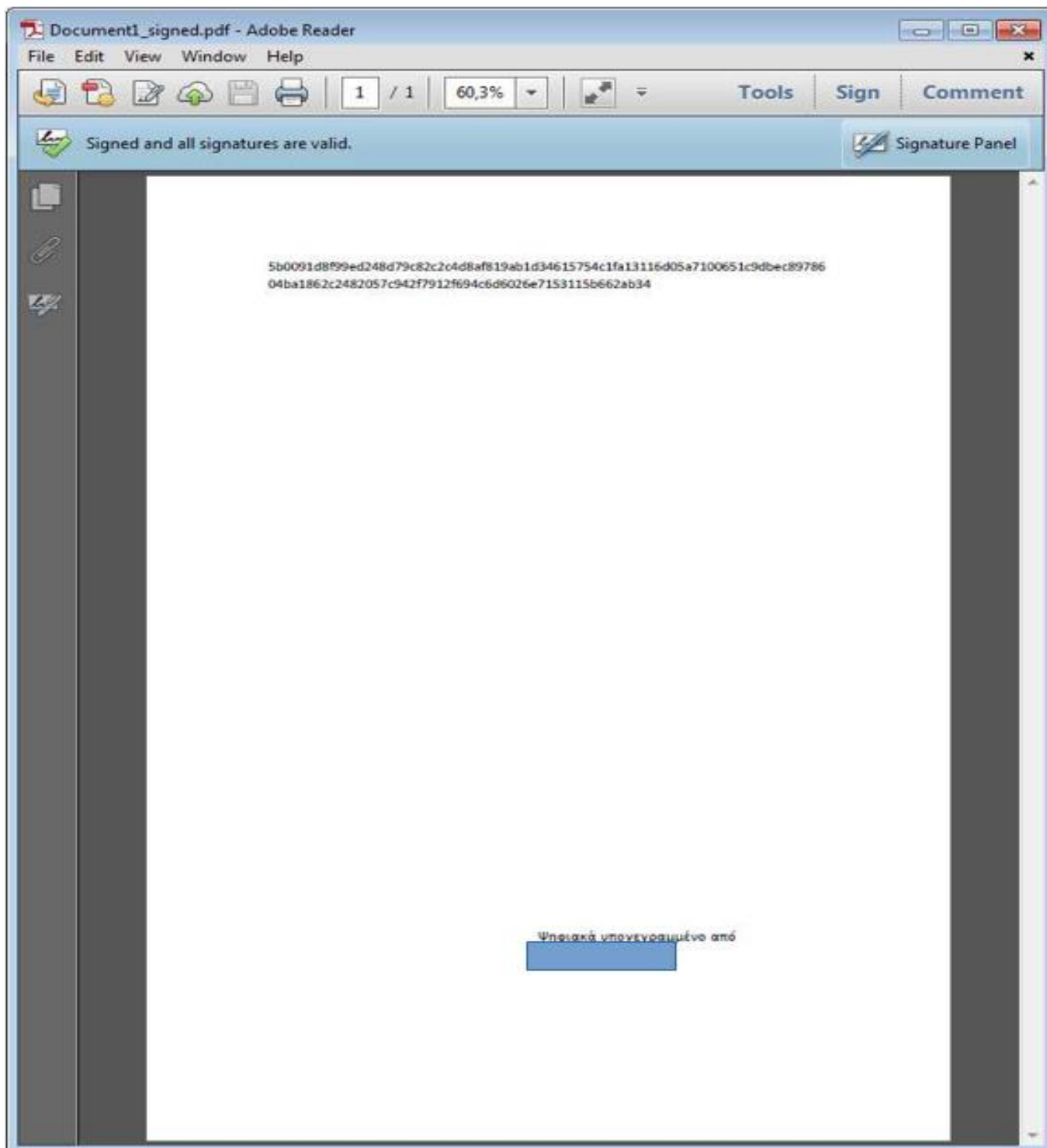


Στην συνέχεια σας δείχνει την πορεία της διαδικασίας βγάζοντας μας το αποτέλεσμα...



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

Έχετε ολοκληρώσει επιτυχώς την Ψηφιακή Υπογραφή του εγγράφου σας. Βλέπετε τη σήμανση Signed and all signatures are valid ([με τη χρήση του Adobe Acrobat Reader DC](#)). Με τον τρόπο αυτό μπορείτε να βεβαιωθείτε ότι η υπογραφή είναι έγκυρη και δεν έχει γίνει επεξεργασία του εγγράφου μετά την υπογραφή.



-Διαχείριση κωδικών (PIN & PUK) και περιεχομένων της συσκευής

Πληροφορίες:

Συνδέετε το USB Token, εμφανίζονται πληροφορίες για αυτό:

The screenshot displays the 'SafeNet Authentication Client Tools' application window. The title bar includes the application name and standard window controls. The 'THALES' logo is prominently displayed in the top right. Below the logo, the text 'SafeNet Authentication Client' is shown, accompanied by several icons representing different functions. On the left side, a tree view shows the 'Tokens' section expanded, with 'Card #ADB972B72F8E94C2' selected. Below this, 'Settings' and 'Client Settings' are visible. The main area of the window contains a table of token details. The table has two columns: a label column and a value column. The data is as follows:

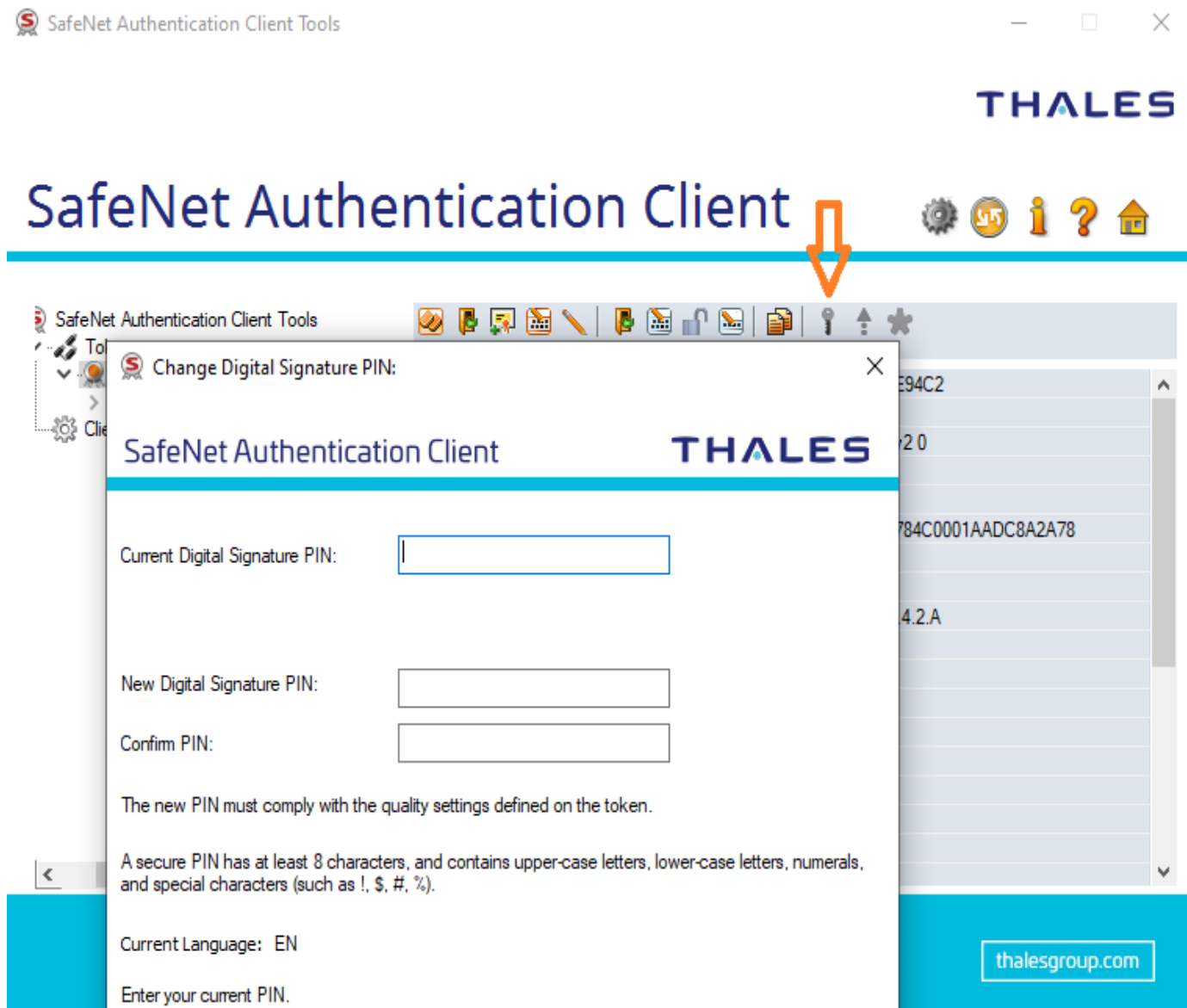
Token name	Card #ADB972B72F8E94C2
Token category	Hardware
Reader name	bit4id TokenME EVO v2 0
Serial number (PKCS#11)	
Free space (minimum estimated)	74752
Card ID (GUID)	
Product name	IDPrime 940
Card type	IDPrime
Applet Version	IDPrime Java Applet 4.4.2.A
Mask version	G286
Token Password	Present
Token Password retries remaining	5
Maximum Token Password retries	5
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	5
Maximum administrator Password retries	5
FIPS	N/A

At the bottom right of the application window, there is a button labeled 'thalesgroup.com'.

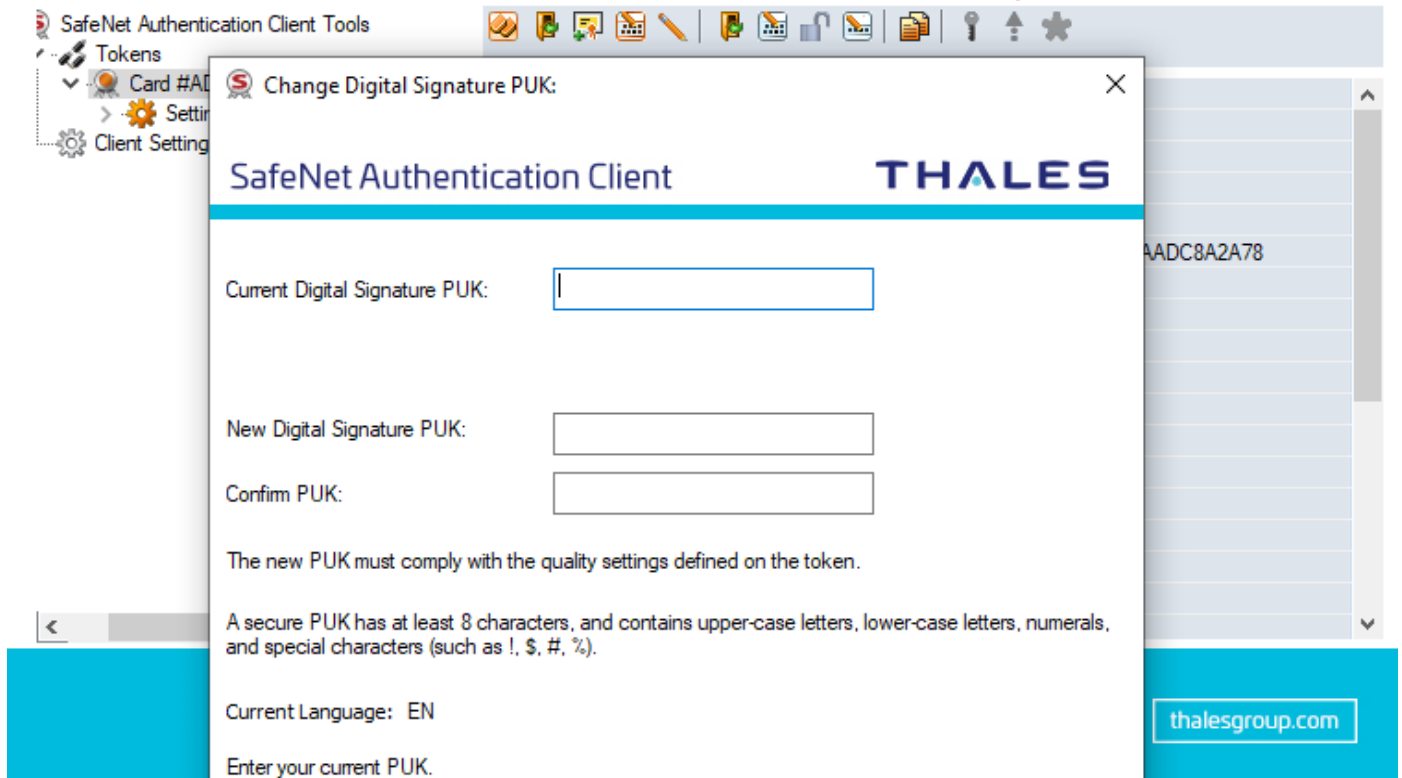
-Αλλαγή Password (PIN) & (PUK)

Στην καρτέλα Change Digital Signature PIN & PUK μπορείτε να αλλάξετε τα προεπιλεγμένα PIN και PUK της συσκευής. (Ο ελάχιστος απαιτούμενος αριθμός ψηφίων είναι 6)

ΠΡΟΣΟΧΗ: Το αρχικό PIN(Digital Signature PIN) του USB Token είναι 000000 και το αρχικό PUK(Digital Signature PUK) είναι 000000.



SafeNet Authentication Client



-Διαγραφή Token (Αρχειοποίηση)

Στην καρτέλα Initialize Token μπορείτε να διαγράψετε το περιεχόμενο του USB Token και να διαμορφώσετε εκ νέου όλους τους κωδικούς της συσκευής σας ανάλογα με τις προτιμήσεις σας.

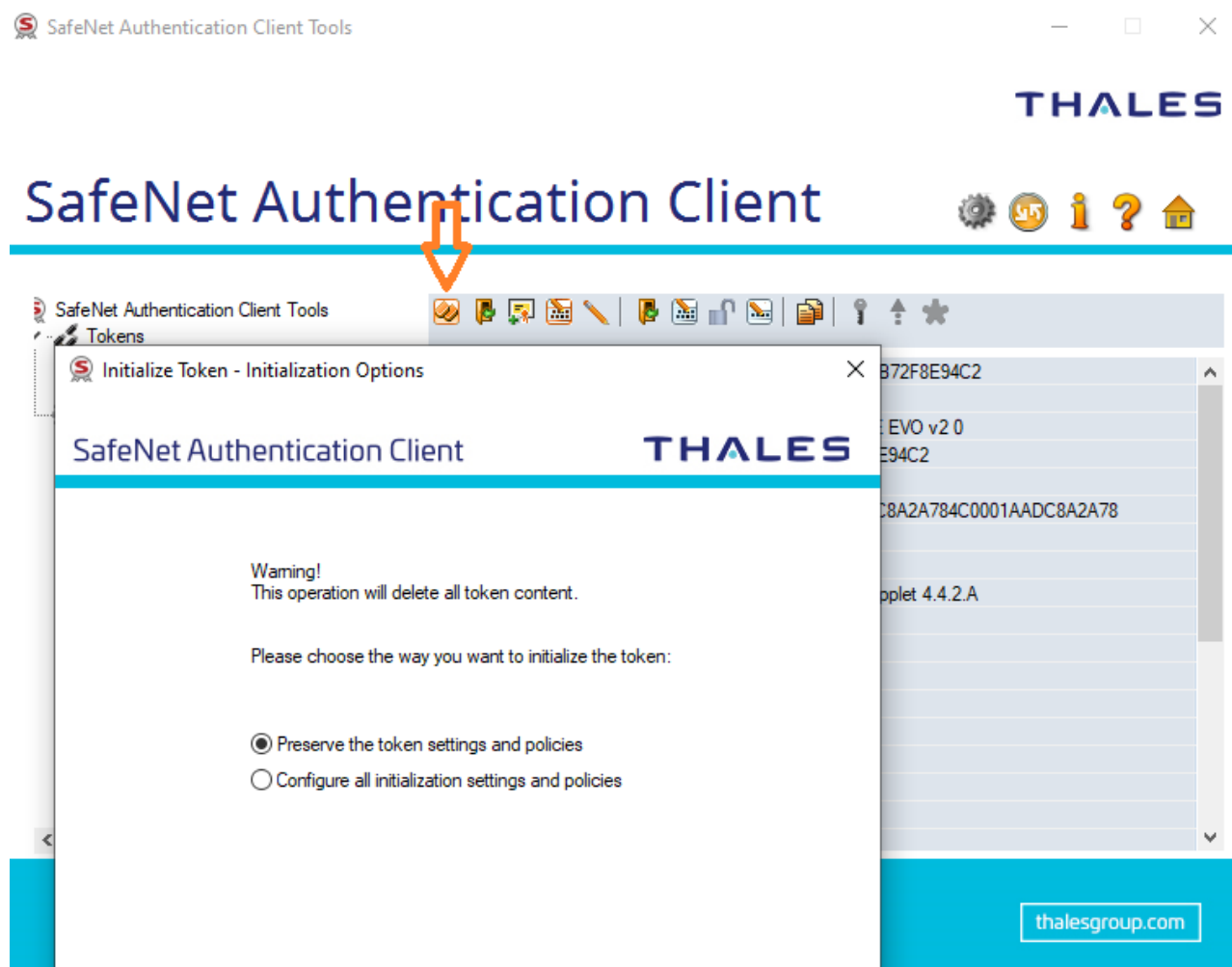
-Αρχικοί Προκαθορισμένοι Κωδικοί Συσκευής

Token Password (PIN ΕΔΔΥ): 0000

Digital Signature PIN: 000000

Digital Signature PUK: 000000

Administrator Password: 00 (48 digits)



THALES



Initialize Token - Administrator Logon



SafeNet Authentication Client

THALES

☐ Use Initialization key to initialize the Token

Enter the current Administrator Password to initialize the Token

☒ Use factory default administrator password

Administrator Password:

.....

Enter the current Digital Signature PUK to initialize the Token

☒ Use factory default digital signature PUK

Digital Signature PUK:

.....

Current Language: EN

The default administrator password and digital signature PUK is a known value of 0's set on the standard profile.
For the non-default value, please enter it manually.

< Προηγούμενο

Επόμενο >

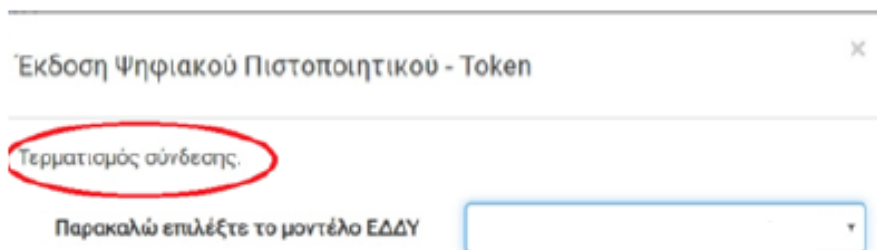
Τέλος

Άκυρο

[thalesgroup.com](https://www.thalesgroup.com)

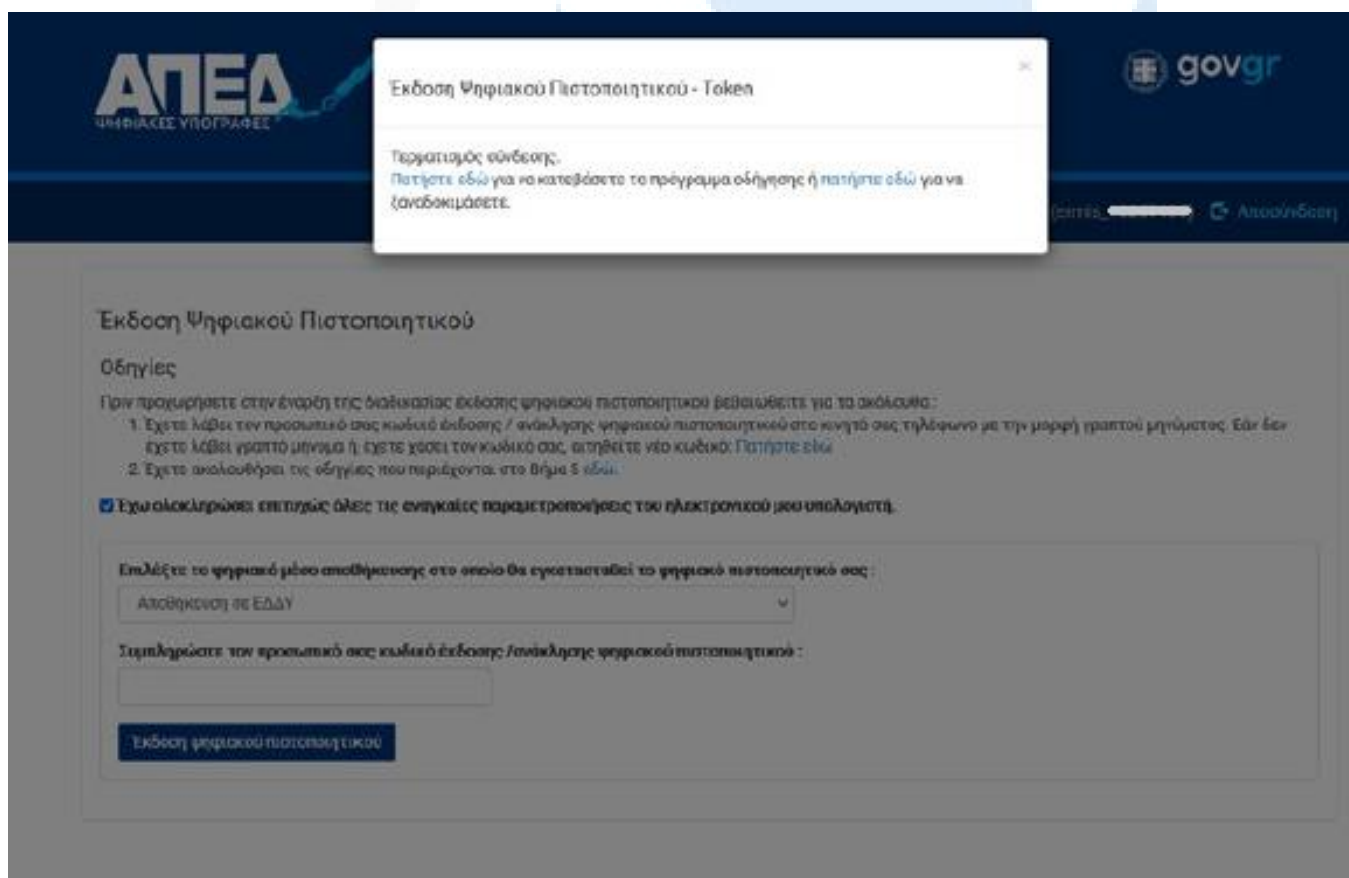
-Πιθανά Προβλήματα κατά τη διαδικασία έκδοσης Νέου Πιστοποιητικού

Το πιο πιθανό πρόβλημα είναι να εμφανιστεί ένα μήνυμα της παρακάτω μορφής:



Δηλαδή, ενώ θα έχει επιλεγεί το σωστό μοντέλο ΕΔΔΥ, δεν δίνεται η δυνατότητα συμπλήρωσης του PIN καθώς επίσης θα εμφανίζεται το μήνυμα «Τερματισμός σύνδεσης». Αυτό συμβαίνει διότι ο browser δεν κατάφερε να εκκινήσει το xapp middleware, με αποτέλεσμα να μην υπάρχει επικοινωνία με την ΕΔΔΥ, ενώ ο χρήστης το έχει εγκαταστήσει κανονικά βάσει των προαναφερόμενων οδηγιών.

Σε αυτή τη περίπτωση ο χρήστης δεν κλείνει το παράθυρο και περιμένει έως ότου αλλάξει το μήνυμα που εμφανίζεται, γύρω στο 1 λεπτό, και εμφανιστεί το ακόλουθο:



Τότε ο χρήστης επιλέγει το σύνδεσμο που αναφέρει «πατήστε εδώ για να ξαναδοκιμάσετε». Με αυτό τον τρόπο γίνεται επανεκκίνηση του xapp.

Επαναλαμβάνετε λοιπόν εκ νέου τη διαδικασία , ελέγχοντας ότι έχετε επιλέξει την σωστή ΕΔΔΥ συσκευή από τη λίστα.

Αν το πρόβλημα παραμένει, προτείνεται επανεγκατάσταση του middleware, δοκιμή με άλλο browser και αρχικοποίηση του usb token πριν κάνετε νέα προσπάθεια έκδοσης.

