

Οδηγός Διαχείρισης και Εγκατάστασης
Ψηφιακού Πιστοποιητικού και Ηλεκτρονικής Υπογραφής
με τη χρήση του **Oberthur-Idemia v8.1 Cosmo** USB Token
στο νέο περιβάλλον της ΑΠΕΔ



Περιεχόμενα

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
-Χρήση Ψηφιακής Υπογραφή με το πρόγραμμα JsignPdf	15
-Διαχείριση κωδικών (PIN & PUK) και περιεχομένων της συσκευής.....	21
-Αλλαγή Password (PIN)	21
-Ξεμπλοκάρισμα Password (PIN).....	23
-Διαγραφή Token (Αρχικοποίηση)	24
-Περιεχόμενα Token	26
-Πιθανά Προβλήματα κατά τη διαδικασία έκδοσης Νέου Πιστοποιητικού	26

Τεχνικά Χαρακτηριστικά

Main Features:

- CCID Standard compliant
- Short Circuit Protection
- Led Status Indicator
- Over 500,000 card Insertions

Certifications and Compliance:

CE, FCC, VCCI, RoHS, REACH, EMV Level1, Microsoft WHQL

Standards:

USB 2.0, CCID, PS/SC, CT-API, PPS, CEI/EN62368 (Ex. CEI/EN 60950), PKCS#11 v2.11, Microsoft CAPI, TokenD, X.509 v3, IPsec

Configurations:

Configuration 1 _ Common Criteria Light
ST Security chip (EAL 4+)
RSA: up to 2048bit, Memory: up to 128kb

Configuration 2_Common Criteria (IAS-ECC)
IDEMIA Security chip (EAL 4+)
RSA: up to 4096bit, Memory: up to 128kb

Configuration 3_Common Criteria Enhanced {IAS-ECC}
IDEMIA Security chip {EAL 4+}
RSA: up to 4096 bit, Memory: up to 144kb

Configuration 4_ FIPS Light [PIV]
IDEMIA Security chip (FIPS 140-2 level 3)
RSA: up to 2048 bit, Memory: up to 64kb

Configuration 5_FIPS Enhanced {IAS-ECC}
NXP Security chip (FIPS 140-2 level 3):
RSA: up to 4096 bit, Memory: up to 144kb

Technical Features:

Interface USB 2.0 (Type A)
Dimensions 50mm x 20mm x 8mm
Weight 8g
Color White
Power Supply USB: 5V DC /50mA
Operating Temperature: 0°C-85°C
Status Led: Green
Symmetric enc. AES: 128-192-256bit
DES/3DES
Hashing: SHA: 1,224,256,384,512bit
Operating Systems:
Win 8, Win 8.1, Win 10,
Windows Server 2008(+)
Mac OS 10, 12(+)
Ubuntu 18.04
RedHat E.7.0 (+)
Centos 7.0(+)
Fedora 28(+)
Debian 8.0(+)

- 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 **Oberthur- Idemia v8.1** λειτουργεί σε όλα τα λειτουργικά συστήματα **Windows (7,8,8.1,10,11)** καθώς και **Mac OS 10,11** σύμφωνα με τις ανακοινώσεις της αναβαθμισμένης ΑΠΕΔ.

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:

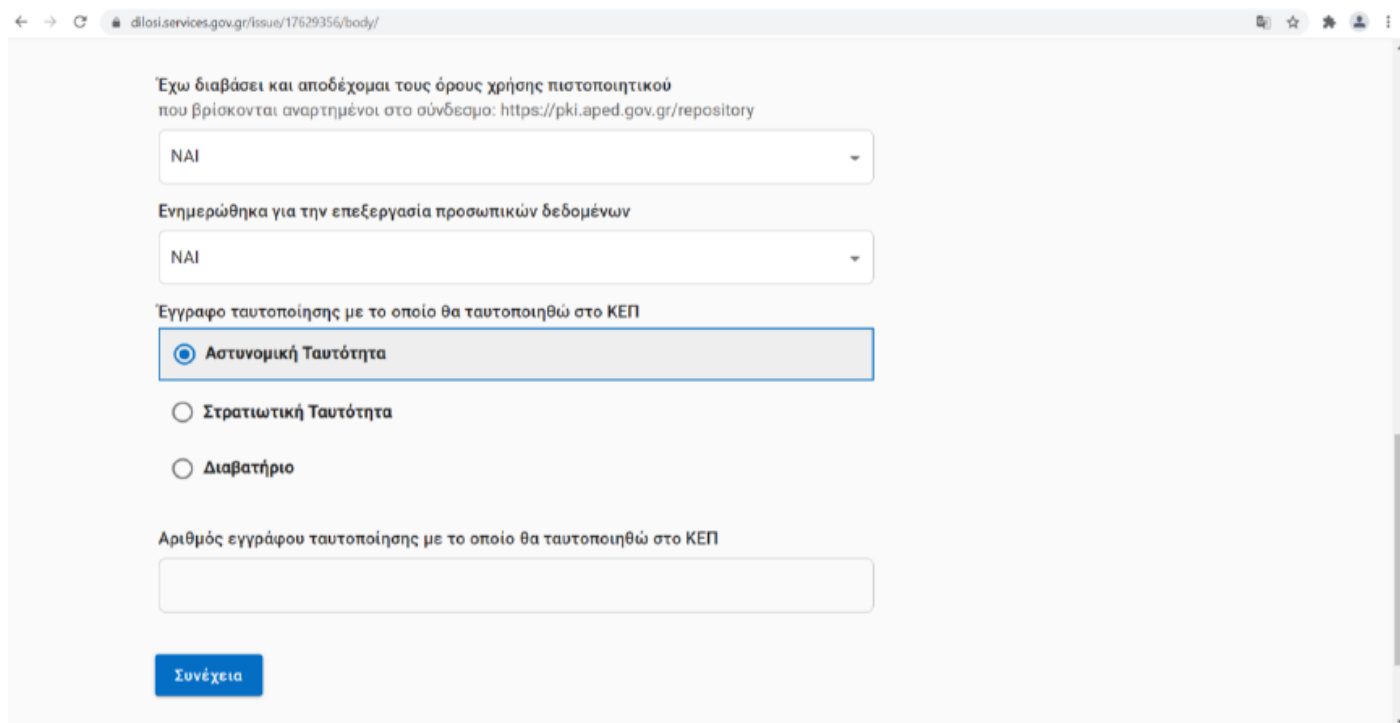
1. με τους προσωπικούς κωδικούς στο Taxisnet.

- 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 <https://dilos.services.gov.gr/issue/17629356/body/>. The form contains the following elements:

- A heading: "Έχω διαβάσει και αποδέχομαι τους όρους χρήσης πιστοποιητικού που βρίσκονται αναρτημένοι στο σύνδεσμο: <https://pki.aped.gov.gr/repository>"
- A dropdown menu with the value "ΝΑΙ".
- A heading: "Ενημερώθηκα για την επεξεργασία προσωπικών δεδομένων"
- A dropdown menu with the value "ΝΑΙ".
- A heading: "Έγγραφο ταυτοποίησης με το οποίο θα ταυτοποιηθώ στο ΚΕΠ"
- Three radio button options:
 - Αστυνομική Ταυτότητα
 - Στρατιωτική Ταυτότητα
 - Διαβατήριο
- A heading: "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 ...

Καλωσήλθατε στην εφαρμογή διαχείρισης πιστοποιητικών της ΑΠΕΔ

Παρακαλώ επιλέξτε τον τρόπο εισόδου στην εφαρμογή

Αυθεντικοποίηση με κωδικούς TAXISNET

Έχετε την δυνατότητα να εισέλθετε στην εφαρμογή διαχείρισης ψηφιακών πιστοποιητικών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου με την βοήθεια των διαπιστευτηρίων σύνδεσης του συστήματος TAXISNET της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (ΑΑΔΕ).

[ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΜΕΣΩ 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 Πως 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 ονοματεπωνύμου 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. Σε περίπτωση που οι οδηγοί της ΕΔΔΥ έχουν εγκατασταθεί στο παρελθόν και είναι λειτουργικοί, δεν απαιτείται να γίνει εκ νέου η εγκατάσταση. Παρακάτω αναφέρονται οι οδηγοί που απαιτούνται για την έκδοση του πιστοποιητικού. Για την εγκατάσταση των οδηγών στους υπολογιστές που επιθυμείτε να υπογράψετε ,ακολουθείτε τους συνδέσμους παρακάτω:

TokenME EVO/ Oberthur/ IDEMIA – Cosmo v8.1 – ΟΔΗΓΟΣ (DRIVER)

[Windows 7, 8.1, 10 – AWP v5.2.0](#)

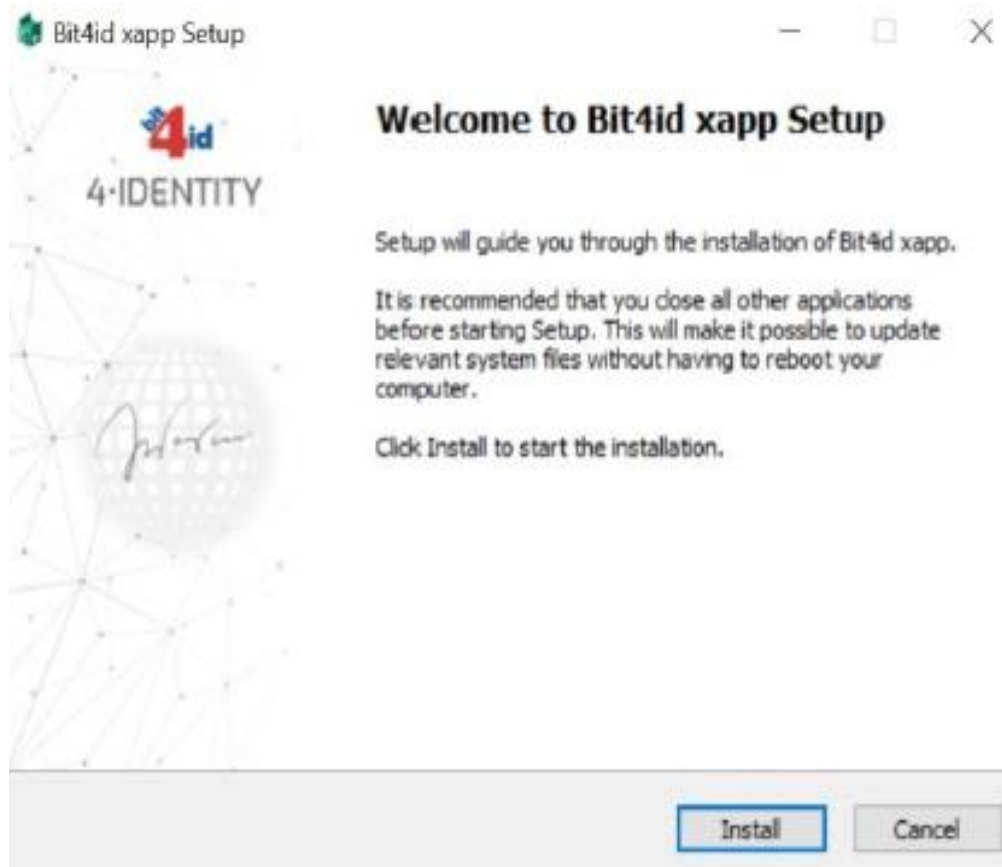
[Windows 10, 11 – AWP 5.3.4](#)

[MacOS 11, 12 – AWP 5.3.4](#)

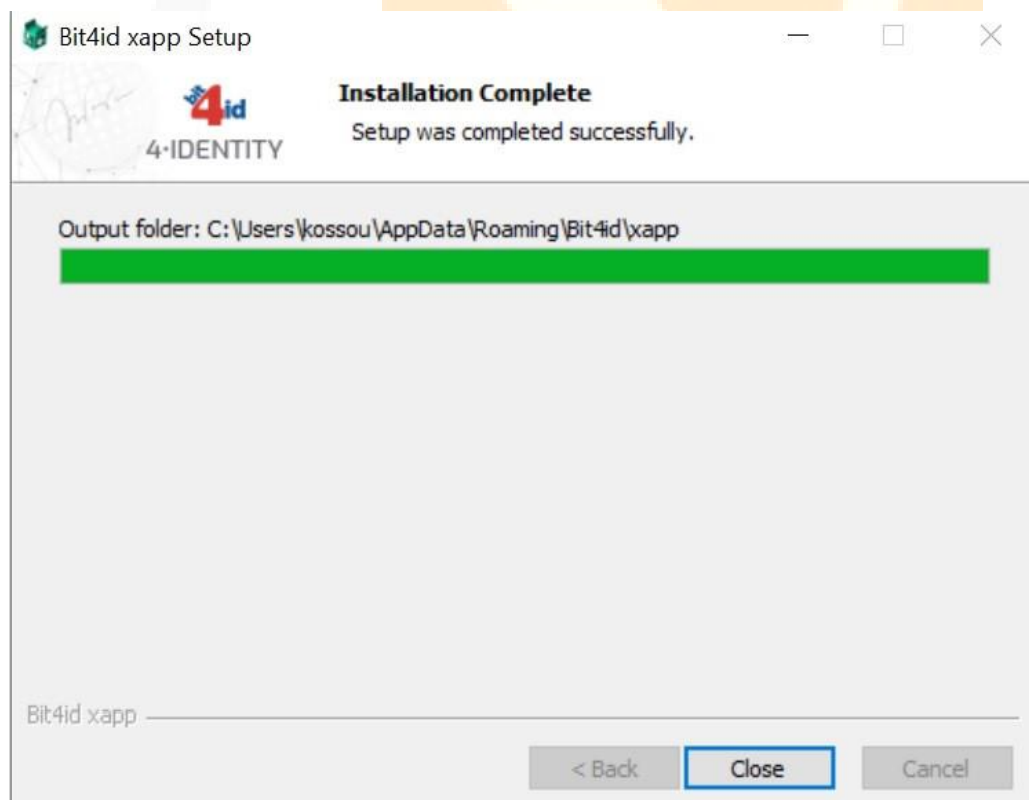
2. Για την έκδοση μόνο του ψηφιακού πιστοποιητικού θα πρέπει να εγκατασταθεί μία κατάλληλη εφαρμογή (BIT4ID middleware) από τον παρακάτω σύνδεσμο:

[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.

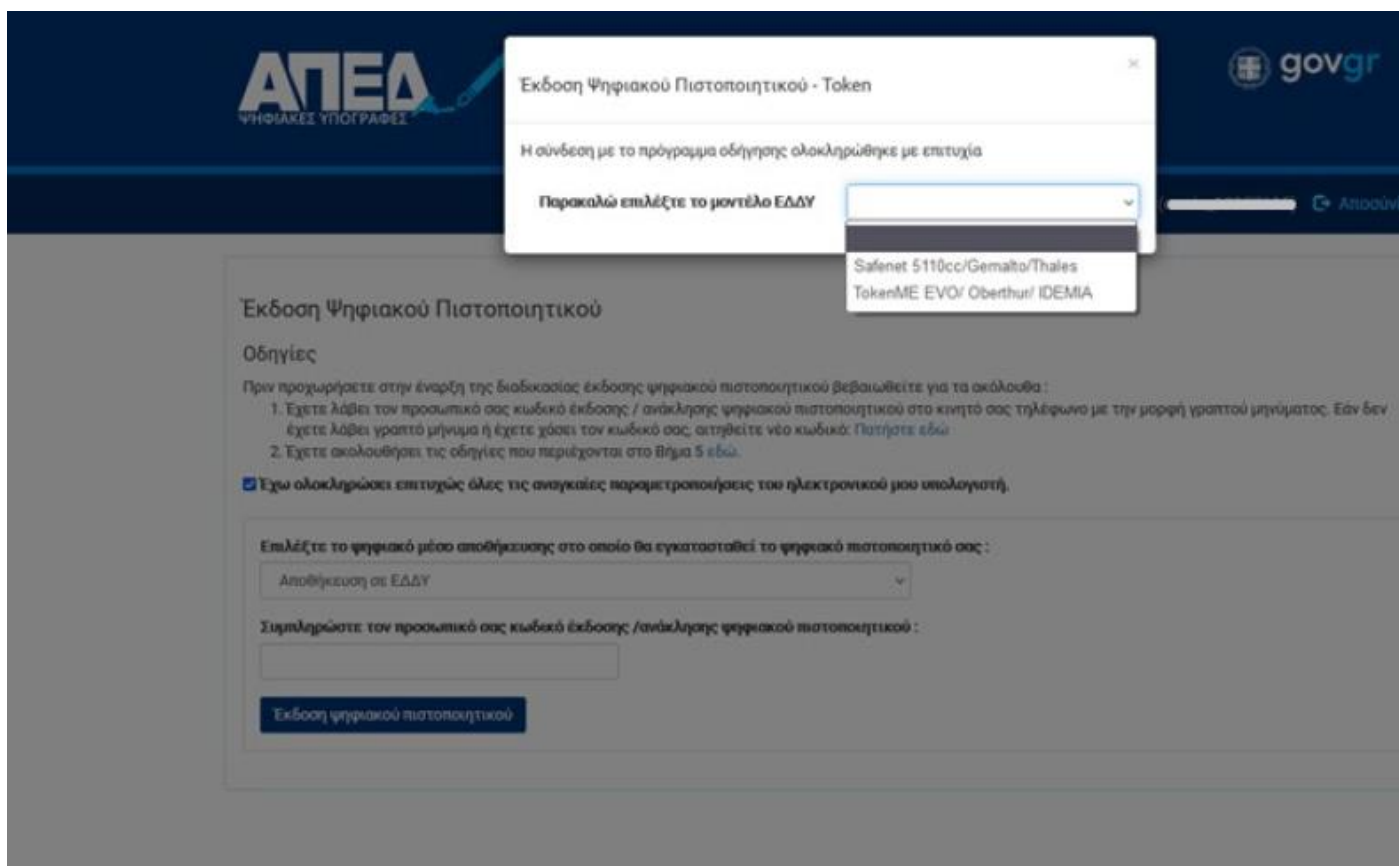
Επιλέξτε το ψηφιακό μέσο αποθήκευσης στο οποίο θα εγκατασταθεί το ψηφιακό πιστοποιητικό σας :

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».



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 **“TokenME Evo Oberthur/Idemia”**


Αφού έχει εκκινήσει το middleware και η ΕΔΔΥ έχει αναγνωριστεί, τότε θα ζητηθεί το PIN προκειμένου να υπάρξει πρόσβαση στην ΕΔΔΥ για να μπορέσουν να εγκατασταθούν τα ψηφιακά πιστοποιητικά.

Το **αρχικό PIN** της συσκευής είναι : **9999** , το οποίο μπορεί να τροποποιηθεί μέσα από το διαχειριστικό λογισμικό του usb token σε παρακάτω βήματα.

Αφού πληκτρολογήσει το PIN σωστά, ξεκινάει η διαδικασία της έκδοσης του πιστοποιητικού , η οποία διαρκεί μερικά δευτερόλεπτα.

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

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 Oberthur USB Token περιέχει τα ψηφιακά σας πιστοποιητικά και έτσι μπορείτε να υπογράφετε τα έγγραφά σας στον υπολογιστή σας.

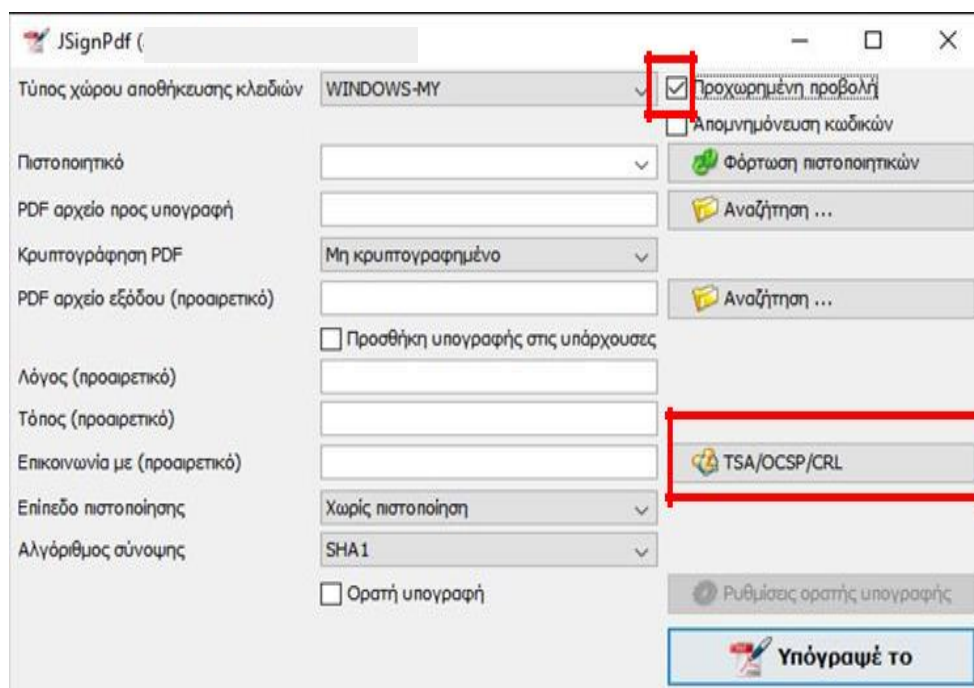
ΣΗΜΑΝΤΙΚΟ: Μετά την ολοκλήρωση έκδοσης του ψηφιακού πιστοποιητικού, ενδεχομένως να χρειαστεί να αφαιρέσετε και να τοποθετήσετε εκ νέου την συσκευή ΕΔΔΥ στον υπολογιστή σας, ώστε να αναγνωριστεί το νέο πιστοποιητικό.

-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

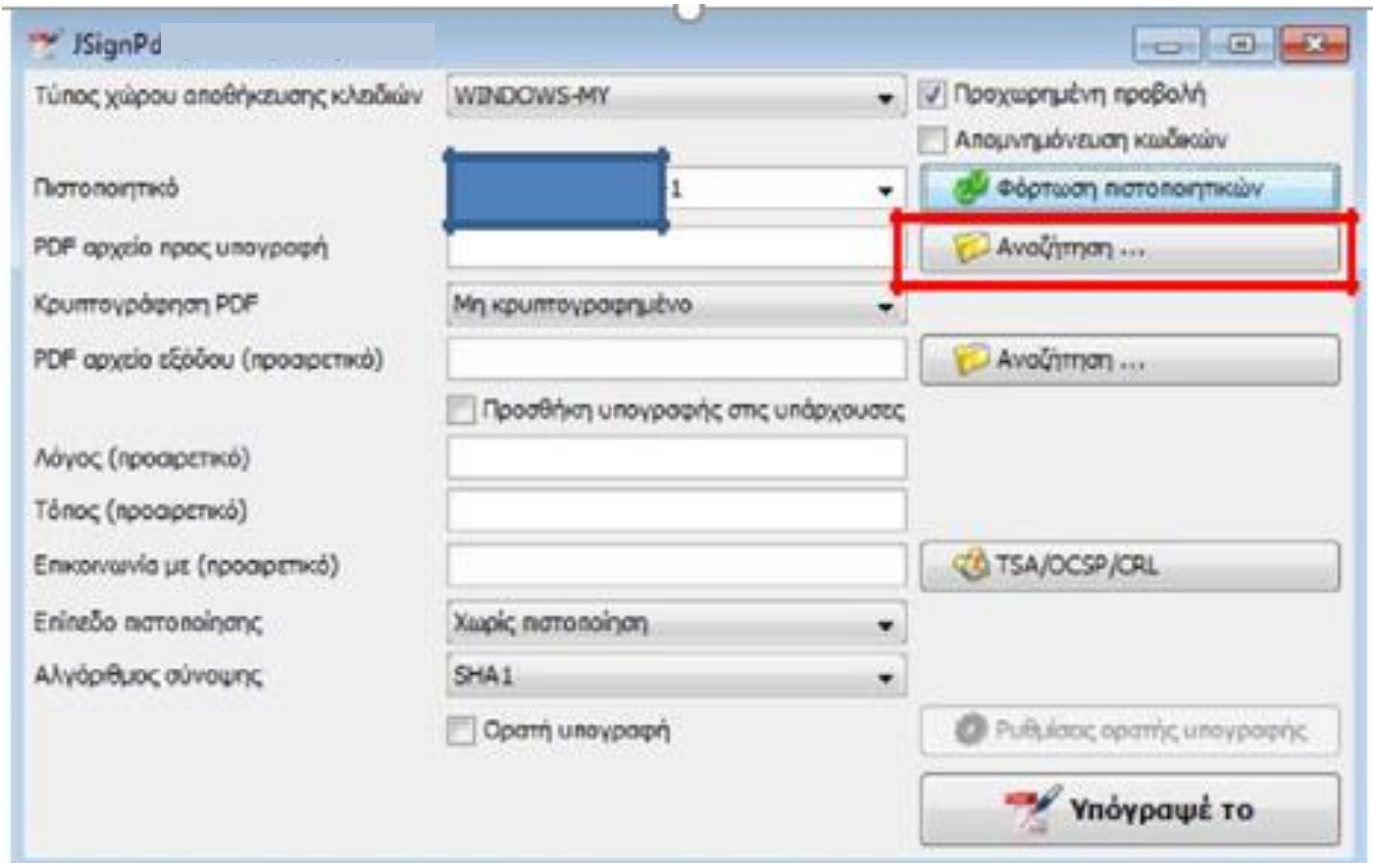
Type:

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).

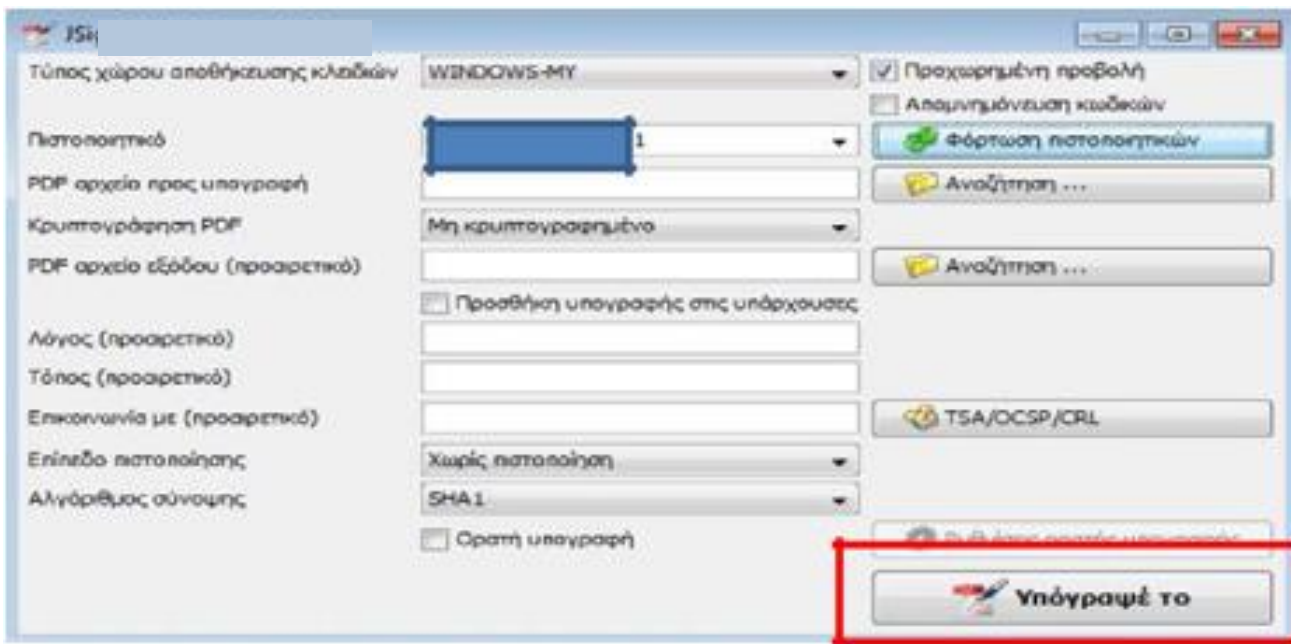
Κάνετε κλικ στο πρώτο κουμπί Αναζήτηση για να επιλέξετε το PDF αρχείο προς υπογραφή:



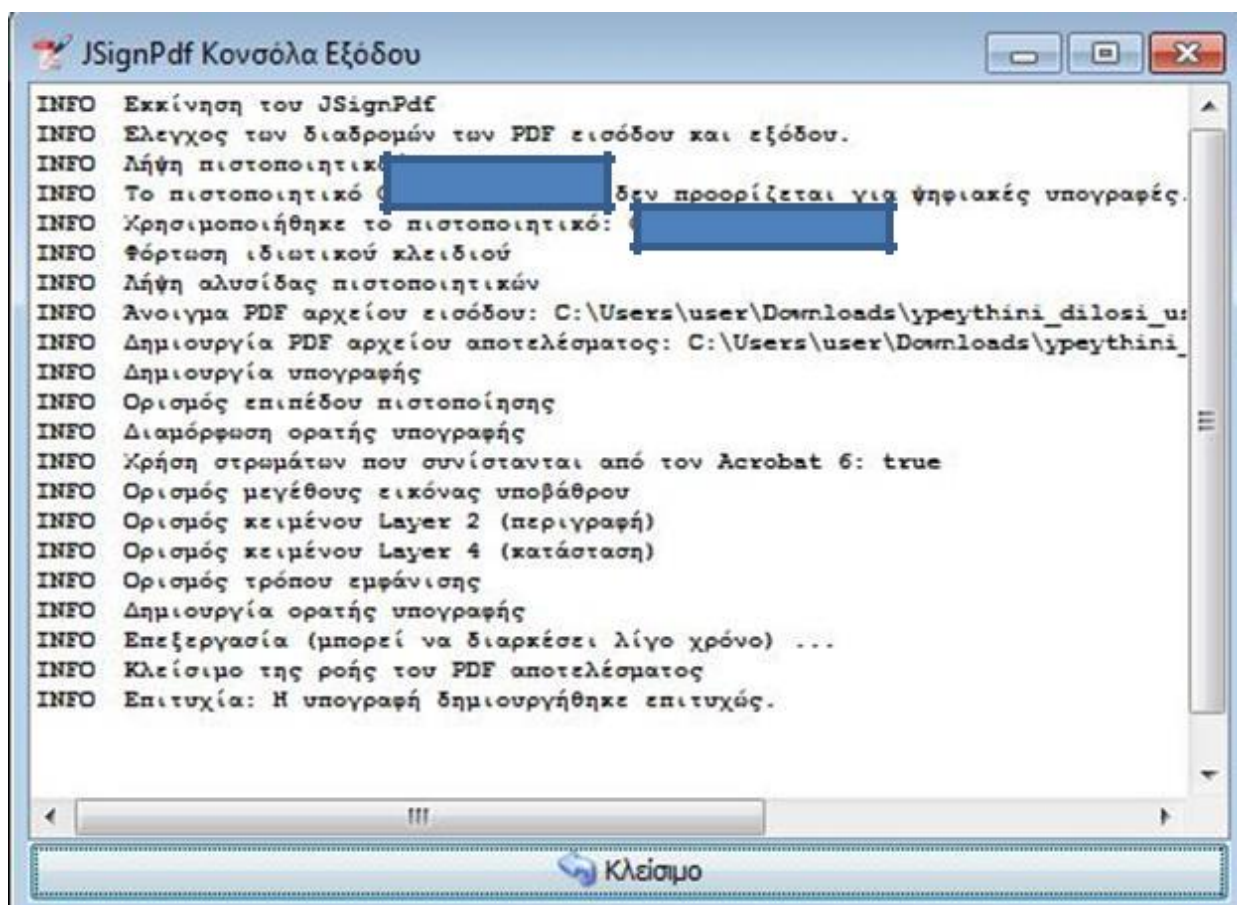
Για να προσθέσετε Ορατή Υπογραφή, επιλέγετε Ορατή υπογραφή, κάνετε κλικ στο κουμπί Ρυθμίσεις ορατής υπογραφής, επιλέγετε Προεπισκόπηση & Επιλογή θέσης όπου εμφανίζεται το έγγραφο στο οποίο (με το αριστερό κλικ από το ποντίκι σας) επιλέγετε το που θα τοποθετηθεί η υπογραφή σας και κάνετε κλικ στο κουμπί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



Κάνετε κλικ στο κουμπί **Υπόγραψε το** και αυτόματα σας ζητάει το PIN που για το συγκεκριμένο Token είναι 4 φορές το 9 (9999), το εισάγετε και πατάτε Ok.

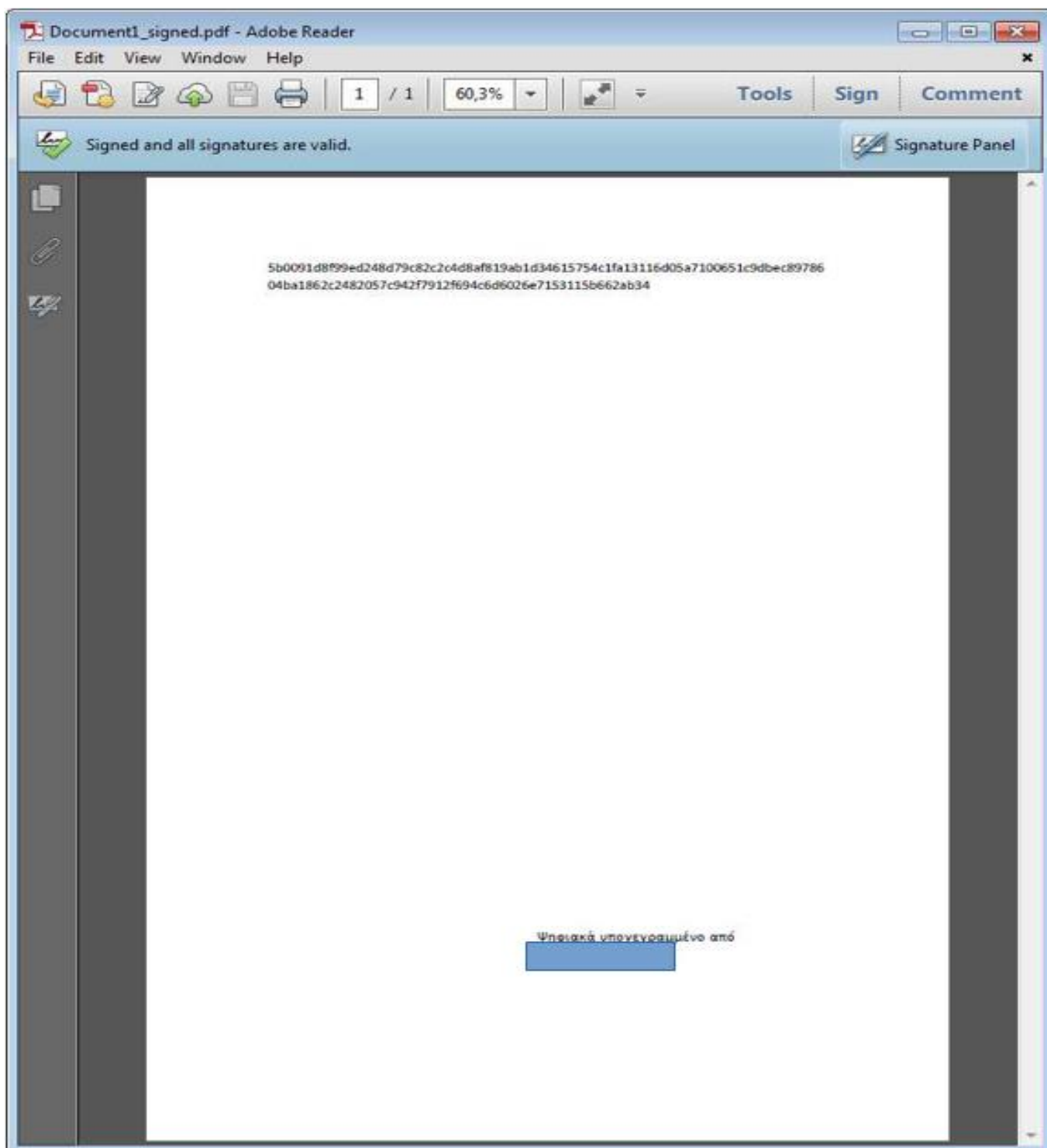


Στην συνέχεια σας δείχνει την πορεία της διαδικασίας βγάζοντας μας το αποτέλεσμα...



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

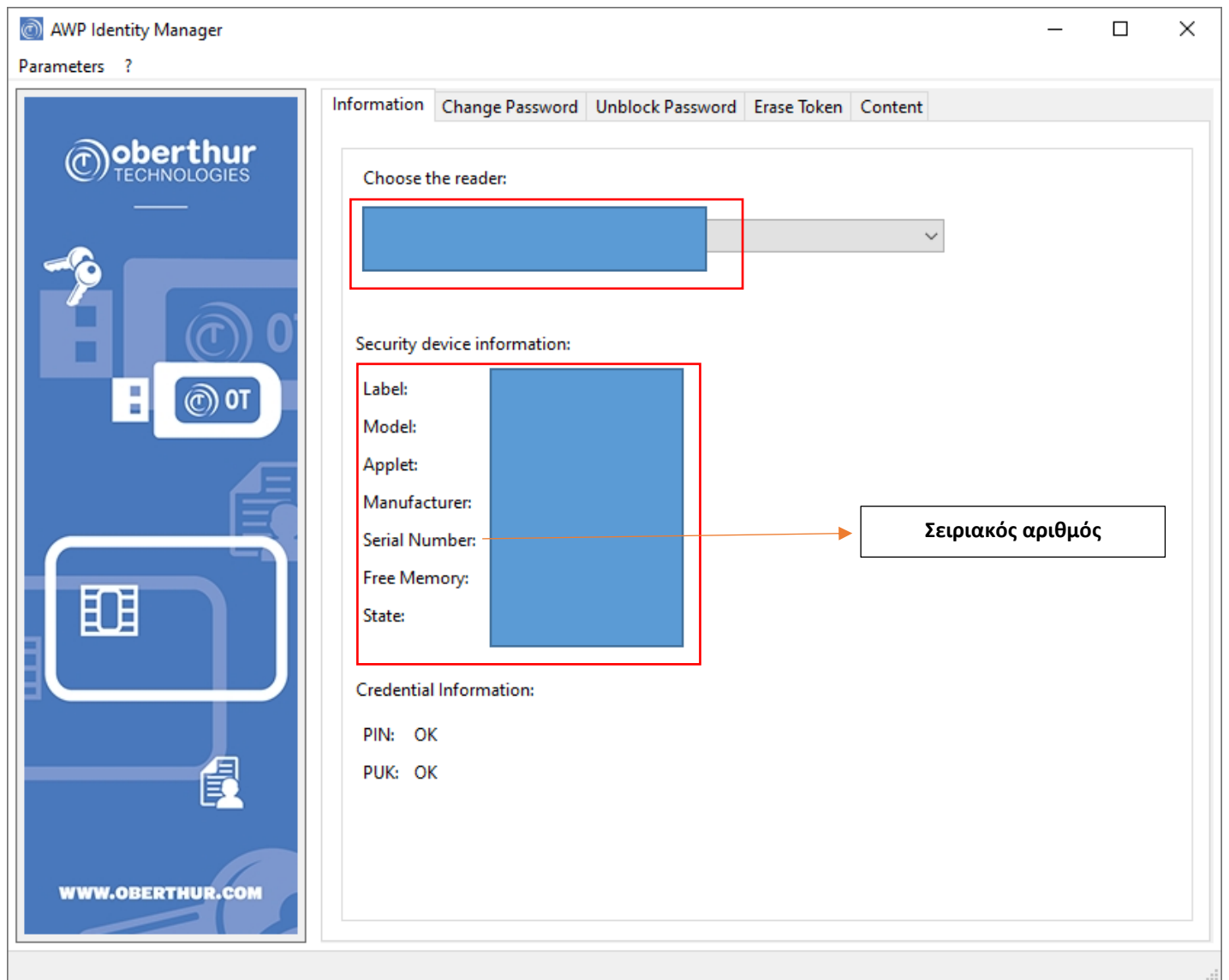
Έχετε ολοκληρώσει επιτυχώς την Ψηφιακή Υπογραφή του εγγράφου σας. Βλέπετε τη σήμανση Signed and all signatures are valid ([με τη χρήση του Adobe Acrobat Reader DC](#)). Με τον τρόπο αυτό μπορείτε να βεβαιωθείτε ότι η υπογραφή είναι έγκυρη και δεν έχει γίνει επεξεργασία του εγγράφου μετά την υπογραφή.



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

Πληροφορίες:

Συνδέετε το USB Token, εμφανίζονται πληροφορίες για αυτό:



The screenshot shows the 'AWP Identity Manager' application window. The left sidebar features the Oberthur Technologies logo and icons for a key, a USB token, a SIM card, and a user profile, with the website 'WWW.OBERTHUR.COM' at the bottom. The main window has a tabbed interface with 'Information' selected. Under 'Choose the reader:', a dropdown menu is highlighted with a red box. Below that, the 'Security device information:' section is also highlighted with a red box. It lists fields: Label, Model, Applet, Manufacturer, Serial Number, Free Memory, and State. The 'Serial Number' field is pointed to by an orange arrow that leads to a box containing the text 'Σειριακός αριθμός'. At the bottom, the 'Credential Information:' section shows 'PIN: OK' and 'PUK: OK'.

-Αλλαγή Password (PIN)

Στην καρτέλα Change Password μπορείτε να αλλάξετε τα προεπιλεγμένα PIN (User Password) και PUK (Admin Password) της συσκευής (το PIN και το PUK πρέπει να αποτελείται από τουλάχιστον 4 ψηφία).

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

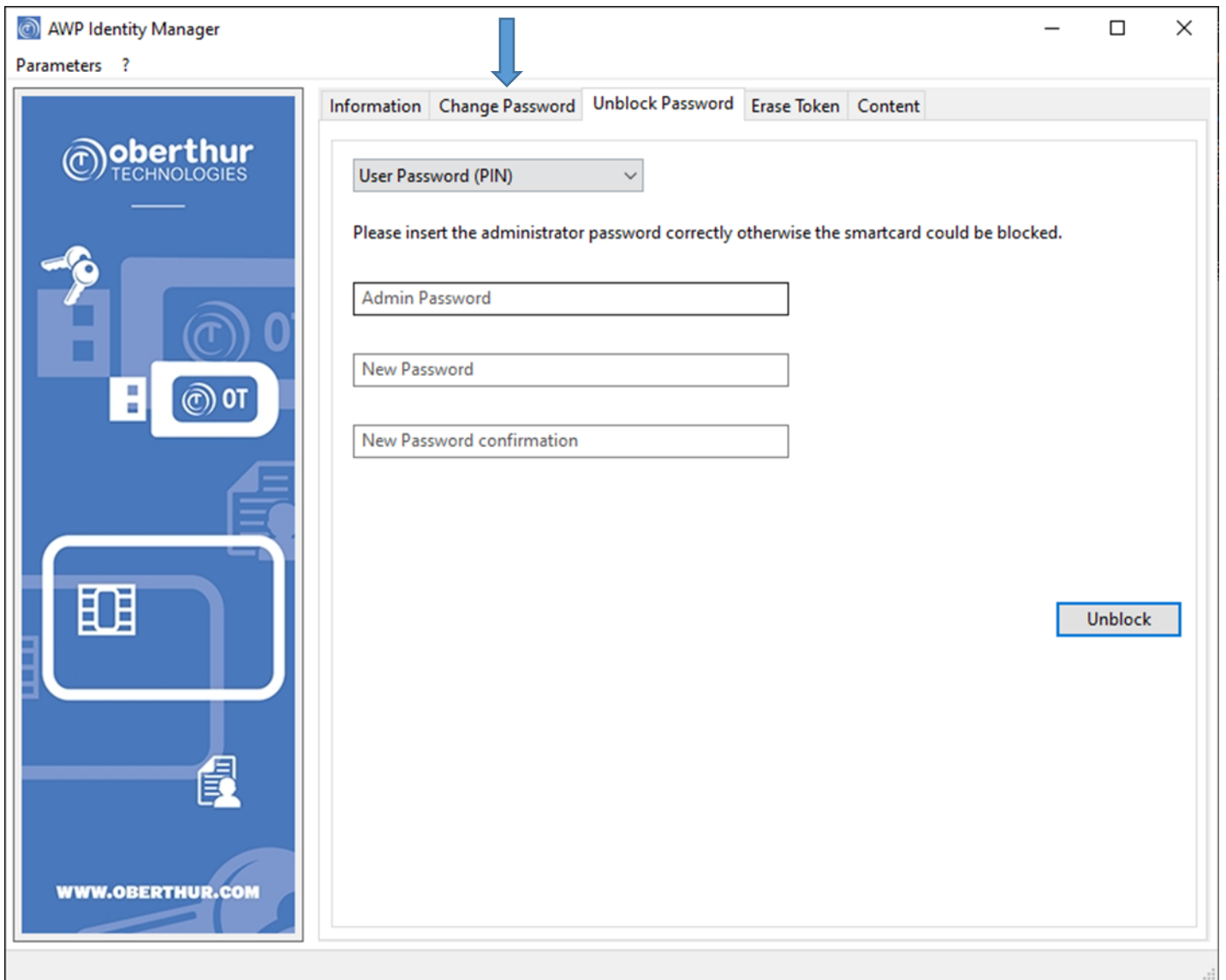
Επιλέγοντας από την κορυφή πιο συνθηματικό επιθυμείτε να αλλάξετε (User Password ή Admin Password) συμπληρώνετε ανάλογα τα παρακάτω πεδία.

User Password: Το τρέχον συνθηματικό της συσκευής.

New User Password: Το νέο συνθηματικό που επιθυμείτε.

New User Password Confirmation: Επιβεβαίωση του νέου συνθηματικού.

Με το κουμπί Change: Επιβεβαιώνετε τις αλλαγές.



-Ξεμπλοκάρισμα Password (PIN)

Στην καρτέλα Unblock Password μπορείτε να ξεκλειδώσετε το USB Token, εάν έχετε εισάγει το PIN τρεις φορές λάθος:

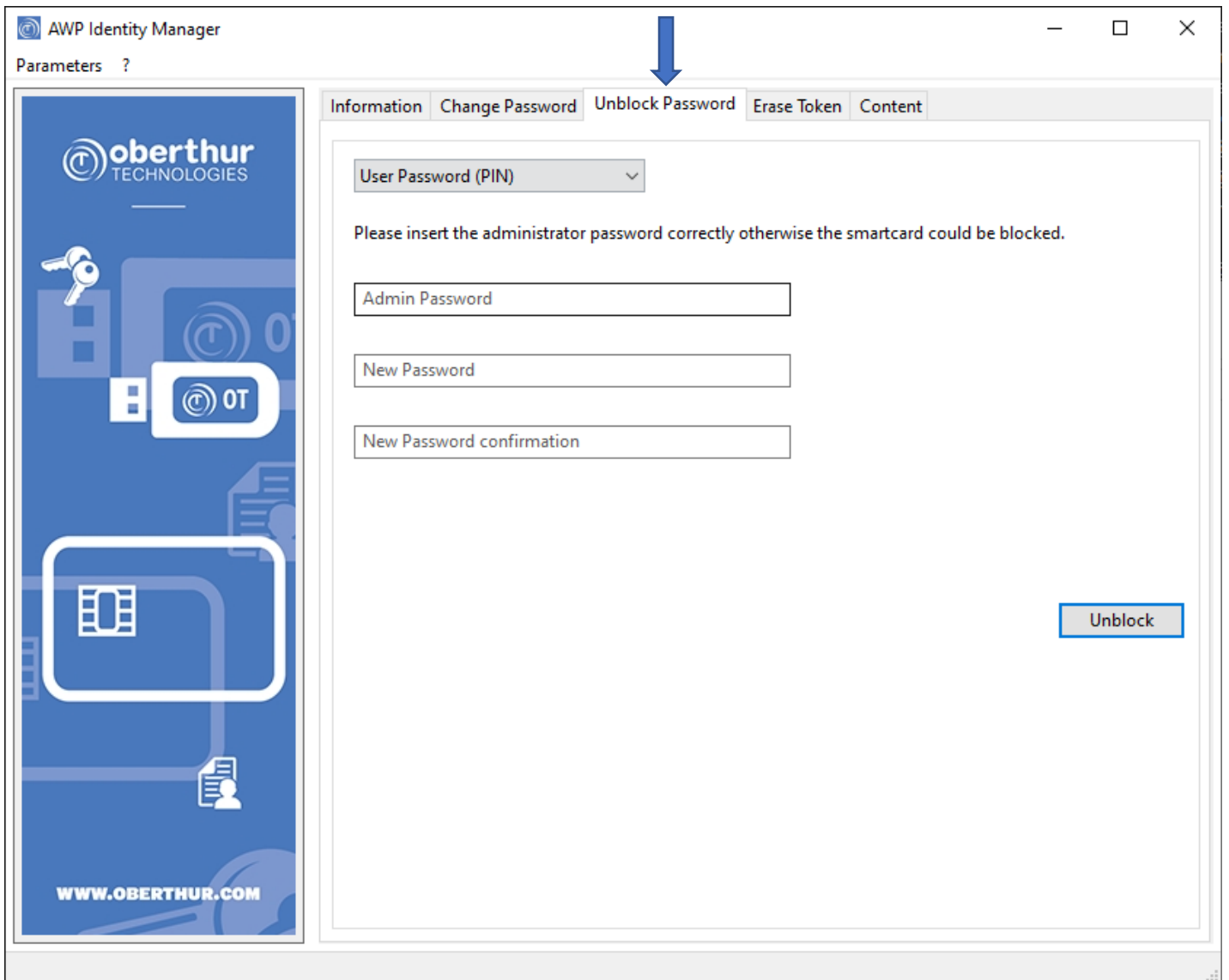
ΠΡΟΣΟΧΗ: Σε περίπτωση τριών λανθασμένων καταχωρήσεων του PUK το USB Token κλειδώνει οριστικά και δεν είναι δυνατή η επαναφορά του, όπως αναφέρθηκε και παραπάνω.

Admin Password: Συμπληρώνετε το PUK της συσκευής.

New Password: Το νέο συνθηματικό που επιθυμείτε.

New Password Confirmation: Επιβεβαίωση του νέου συνθηματικού.

Με το κουμπί Unblock: Επιβεβαιώνετε τις αλλαγές.



-Διαγραφή Token (Αρχικοποίηση)

Στην καρτέλα Erase Token μπορείτε να διαγράψετε το περιεχόμενο του USB Token χρησιμοποιώντας το PUK, ρυθμίζοντας νέο PIN:

ΠΡΟΣΟΧΗ: Σε περίπτωση τριών λανθασμένων καταχωρήσεων του PUK το USB Token κλειδώνει οριστικά και δεν είναι δυνατή η επαναφορά του.

Admin Password: Συμπληρώνετε το PUK της συσκευής.

Token Label: Συμπληρώνετε το νέο «όνομα» της συσκευής.

New Password: Το νέο συνθηματικό που επιθυμείτε.

New Password Confirmation: Επιβεβαίωση του νέου συνθηματικού.

Με το κουμπί Erase:Επιβεβαιώνετε τις αλλαγές.

AWP Identity Manager

Parameters ?

Information Change Password Unblock Password **Erase Token** Content

Please insert the administrator password correctly otherwise the smartcard could be blocked.

Admin Password

New smartcard information

Token Label

New Password

New Password confirmation

Erase

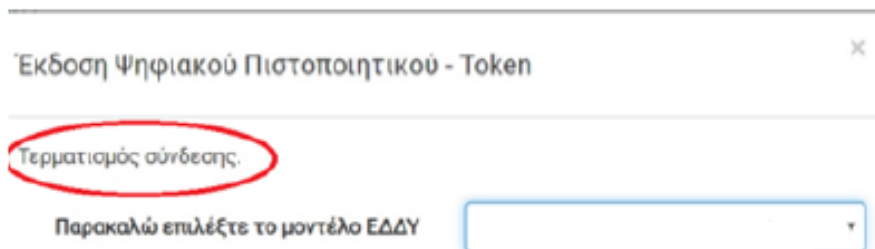
www.oberthur.com

-Περιεχόμενα Token

Στην καρτέλα Content μπορείτε να δείτε το εγκατεστημένο πιστοποιητικό στο USB Token σας πατώντας πάνω σε αυτό διπλό αριστερό κλικ, βλέπετε επιπλέον πληροφορίες όπως: Ονοματεπώνυμο Χρήστη, Ημερομηνία Λήξης, Αρχή Έκδοσης Πιστοποιητικού.....)

-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 charp 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:

Εκδοση Ψηφιακού Πιστοποιητικού - Token

Παραταμίως εύνδεσης.
Πατήστε εδώ για να κατεβάσετε το πρόγραμμα οδήγησης ή πατήστε εδώ για να ξαναδοκιμάσετε.

Εκδοση Ψηφιακού Πιστοποιητικού

Οδηγίες

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

1. Έχετε λάβει τον προσωπικό σας κωδικό ένδεσης / ανάλογης ψηφιακού πιστοποιητικού στο κινητό σας τηλέφωνο με την μαρφή γραπτού μηνύματος. Εάν δεν έχετε λάβει γραπτό μήνυμα ή έχετε χυθεί τον κωδικό σας, αιτηθείτε νέο κωδικό. Πατήστε [εδώ](#).
2. Έχετε ακολουθήσει τις οδηγίες που περιέχονται στο θέμα 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

Πληκτρολογήστε τον προσωπικό σας κωδικό ένδεσης / ανάλογης ψηφιακού πιστοποιητικού:

Έκδοση ψηφιακού πιστοποιητικού

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, αρχικοποίηση του usb token και επανεκκίνηση του υπολογιστή σας πριν κάνετε νέα προσπάθεια έκδοσης.