ΑΠΕΔ
ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

ΑΡΧΗ
ΠΙΣΤΟΠΟΙΗΣΗΣ
ΕΛΛΗΝΙΚΟΥ
ΔΗΜΟΣΙΟΥ

ΟΔΗΓΙΕΣ ΓΙΑ ΤΗΝ ΑΝΑΓΝΩΡΙΣΗ ΨΗΦΙΑΚΑ ΥΠΟΓΕΓΡΑΜΜΕΝΩΝ ΕΓΓΡΑΦΩΝ ΜΕ ΑΝΑΓΝΩΡΙΣΜΕΝΑ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΣΚΛΗΡΗΣ ΑΠΟΘΗΚΕΥΣΗΣ ΤΗΣ ΑΠΕΔ ΚΑΙ ΑΣΦΑΛΟΥΣ ΧΡΟΝΟΣΗΜΑΝΣΗΣ ΑΠΟ ΤΗΝ ΠΥΛΗ «ΕΡΜΗΣ»

Έκδοση 1.1

Αύγουστος 2017

Πίνακας Περιεχομένων

1. Εισαγωγή

Στο παρόν εγχειρίδιο παρουσιάζονται τα σημαντικά στοιχεία ενός ψηφιακά υπογεγραμμένου εγγράφου καθώς και οδηγίες προκειμένου ο παραλήπτης / κάτοχος του να μπορεί να επιβεβαιώσει την εγκυρότητα τους, εφόσον χρησιμοποιούνται ψηφιακά πιστοποιητικά που έχει εκδώσει η Αρχή Πιστοποίησης του Ελληνικού Δημόσιου (ΑΠΕΔ) μέσω της Υποδομής Δημοσιου Κλειδιού (αγγλικά Public Key Infrastructure- PKI) της Εθνικής Πύλης της Δημόσιας Διοίκησης «ΕΡΜΗΣ».

Τα ψηφιακά πιστοποιητικά αφορούν τόσο την ψηφική υπογραφή του εγγράφου όσο και την ασφαλή χρονοσήμανση του. Οι οδηγίες αφορούν έγγραφα σε μορφοποίηση PDF.

2. Θεσμικό Πλαίσιο

Σύμφωνα με το άρθρο 2 του Προεδρικού Διατάγματος 150/2001 (**ΦΕΚ 125 Α/25-6-2001**) με το οποίο ενσωματώθηκε η Οδηγία 99/93/ΕΚ για τις ψηφιακές υπογραφές στην ελληνική έννομη τάξη ορίζονται τα ακόλουθα:

1. «***ηλεκτρονική υπογραφή***»: δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.
2. «***προηγμένη ηλεκτρονική υπογραφή***» ή «ψηφιακή υπογραφή»: ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:
   α) συνδέεται μονοσήμαντα με τον υπογράφοντα,
   β) είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος,
   γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και
   δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.
3. «***υπογράφων***»: φυσικό ή νομικό πρόσωπο, που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε στο δικό του όνομα είτε στο όνομα άλλου φυσικού ή νομικού προσώπου ή φορέα.
4. «***δεδομένα δημιουργίας υπογραφής***»: μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής.
5. «***διάταξη δημιουργίας υπογραφής***»: διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής.
6. «***ασφαλής διάταξη δημιουργίας υπογραφής***» διάταξη δημιουργίας υπογραφής, που πληροί τους όρους του Παραρτήματος ΙΙΙ του Π.Δ.150/2001.
7. «***δεδομένα επαλήθευσης υπογραφής***»: δεδομένα, όπως κώδικες, ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής.
8. «***διάταξη επαλήθευσης υπογραφής***»: διατεταγμένο υλικό ή λογισμικό, που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής.
9. «***πιστοποιητικό***»: ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.
10. «***αναγνωρισμένο πιστοποιητικό***»: πιστοποιητικό που πληροί τους όρους του Παραρτήματος Ι και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος πληροί τους οριζόμενους στο Παράρτημα ΙΙ όρους.
11. «***πάροχος υπηρεσιών πιστοποίησης***»: φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.
12. «***προϊόν ηλεκτρονικής υπογραφής***»: υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την προσφορά υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.

Σχετικά με τα ψηφιακά δημόσια έγγραφα επιπλέον ισχύει και η Υπουργική Απόφαση «Ηλεκτρονικό Αρχείο και Ψηφιοποίηση Εγγράφων» **ΦΕΚ 44Α/25-02-2014**, όπου ορίζεται ότι θα πρέπει να φέρουν ασφαλή χρονοσήμανση.

Αρμόδια για την παροχή πληροφορίων σχετικά με τα θέματα παροχής υπηρεσιών εμπιστοσύνης (ψηφιακή υπογραφή, χρονοσημανση) για τη χώρα μας είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) (**http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/**).

3. Προηγμένη Ηλεκτρονική Υπογραφή (Ψηφιακή Υπογραφή)

Η προηγμένη ηλεκτρονική υπογραφή (ψηφιακή υπογραφή) βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται με τη χρήση Ασφαλούς Διάταξης Δημιουργίας Υπογραφής (ΑΔΔΥ). Ως ΑΔΔΥ ορίζεται η μικροσυσκευή (Usb Token / Smart Card + Card Reader) που πληροί συγκεκριμένες προδιαγραφές και στην οποία εισάγονται τα ψηφιακά πιστοποιητικά σκληρής αποθήκευσης με ασφαλή τρόπο (Περισσότερες πληροφορίες διατίθενται και στο σχετικό εγχειρίδιο που διατίθεται στα εργαλεία του διαδικτυακού τόπου της ΑΠΕΔ.

Η προηγμένη ηλεκτρονική υπογραφή είναι η μόνη ηλεκτρονική υπογραφή που υπέχει θέσης ιδιόχειρης τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο. Σημαντική σημείωση: οι όροι προηγμένη ηλεκτρονική υπογραφή και ψηφιακή υπογραφή είναι ισοδύναμοι και χρησιμοποιούνται εναλλακτικά, συμφωνα και με το αρ. 2 του ΠΔ 150/2001.

Σύμφωνα με τον Κανονισμό Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημόσιου (ΑΠΕΔ) (**ΦΕΚ 799 Β/09-06-2010** που τροποποιήθηκε με την ΚΥΑ με ΑΠ ΥΑΠ /Φ.60/3431/27-12-2013) - **ΦΕΚ 3320 Β/27-12-2013** και πιο συγκεκριμένα την ενότητα 1.2.1 που αφορά τις Πολιτικές Πιστοποιητικών, η προηγμένη ηλεκτρονική υπογραφή (ψηφιακή υπογραφή) ηλεκτρονικών μηνυμάτων, εγγράφων και η αυθεντικοποίηση του χρήστη προϋποθέτει την έκδοση πιστοποιητικών βάσει της Πολιτικής Πιστοποίησης 1 (ΠΠ 1). Στην παράγραφο 1.2.1 αναφέρεται ότι η ΠΠ1 «Η ΠΠ 1 αντιστοιχεί στην δημόσια πολιτική πιστοποιητικών "QCP +SSCD" όπως περιγράφεται στο πρότυπο ETSI 101 456του European Telecommunications Standards Institute».

Ως εκ τούτου, τα ψηφιακά πιστοποιητικά που εκδίδονται από την ΑΠΕΔ βάσει της ΠΠ 1 μπορούν να υποστηρίξουν προηγμένη ηλεκτρονική υπογραφή σύμφωνα με τις διατάξεις της παρ. 1 του άρθρου 3 του Π.Δ. 150/2001.

Με βάση τις διατάξεις του Π.Δ. 150/2001 και του Κανονισμού Πιστοποίησης της ΑΠΕΔ όπως ισχύει, όταν ο χρήστης θέλει να υπογράφει ψηφιακά έγγραφα, ψηφιακά μηνύματα και η ψηφιακή υπογραφή του να έχει αντίστοιχη ισχύ με την ιδιόχειρη θα πρέπει να χρησιμοποιεί ψηφιακά πιστοποιητικά σκληρής αποθήκευσης, τα οποία να καλύπτουν τις απαιτήσεις (OID) της ΠΠ1 (βλέπε σχετικά τον Κανονισμό Πιστοποίησης).

Ο έλεγχος για το αν ένα έγγραφο φέρει προηγμένη ηλεκτρονική υπογραφή γίνεται προκειμένου να ελεγχθεί αν το ψηφιακό πιστοποιητικό της αυθεντικοποίησης φέρει την τιμή αντικειμένου 1.2.300.0.110001.1.7.1.1.1 που αντιστοιχεί στην ΠΠ1.

4. Ασφαλής Χρονοσήμανση

Ένα ψηφιακό δημόσιο έγγραφο πρέπει να φέρει ασφαλή χρονοσήμανση από αναγνωρισμένο πάροχο υπηρεσιών ασφαλούς χρονοσήμανσης σχετικά με την ώρα υπογραφής του και όχι την ώρα από το ρολόι του υπολογιστή του υπογράφοντος.

Η ασφαλής χρονοσήμανση πέρα από την υποχρέωση του δημόσιου τομέα σύμφωνα με τη σχετική ΥΑ, είναι δυνατό να χρησιμοποιηθεί ή να απαιτηθεί για την απόδειξη του ακριβούς χρόνου ψηφιακής υπογραφής ενός ψηφιακού εγγράφου.

5. Βήματα για τον εντοπισμό της ΠΠ της ψηφιακής υπογραφής και της πηγής ασφαλούς χρονοσήμανσης

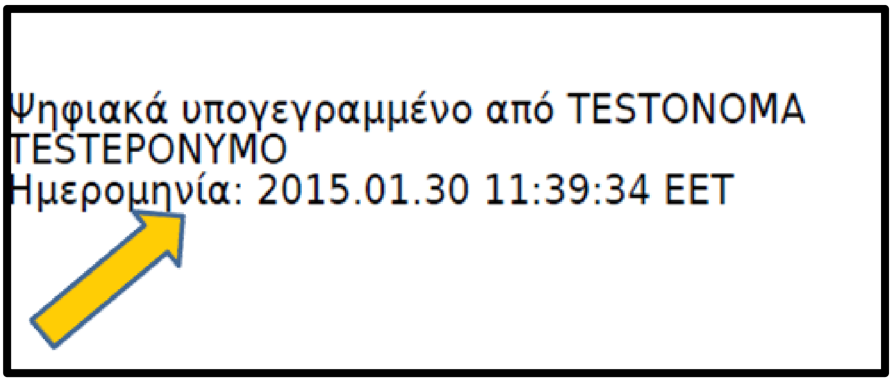
Τα βήματα για την πραγματοποίηση των παραπάνω ελέγχων είναι τα ακόλουθα:

➢ **<u>Βήμα προαπαιτούμενο</u>**

Ο χρήστης έχει εγκαταστήσει στον υπολογιστή που χρησιμοποιεί για τον έλεγχο της ψηφιακής υπογραφής τα ψηφιακά πιστοποιητικά της ΑΠΕΔ, της Υποκείμενης Αρχής Πιστοποίησης και της Αρχής Χρονοσήμανσης
Σε περίπτωση που η Ψηφιακή Υπογραφή βασίζεται σε ψηφιακά πιστοποιητικά διαφορετικού παρόχου θα πρέπει να διασταυρωθεί με την ΕΕΤΤ αν είναι πιστοποιημένος παρόχος υπηρεσιών εμπιστοσύνης και να εγκατασταθούν τα σχετικά ΨΠ στον υπολογιστή που γίνεται ο έλεγχος των ψηφιακών υπογραφών.
Οι πιστοποιημένοι πάροχοι υπηρεσιών εμπιστοσύνης στην Ελλάδα περιλαμβάνονται στον σχετικό κατάλογο της ΕΕΤΤ. Η ΕΕΤΤ είναι αρμόδια για την παροχή πληροφορίων σχετικά με τους πιστοποιημένους πάροχους υπηρεσιών εμπιστοσύνης στην Ευρωπαϊκή Ένωση
(http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/).

➢ **<u>ΒΗΜΑ 1ο</u>**

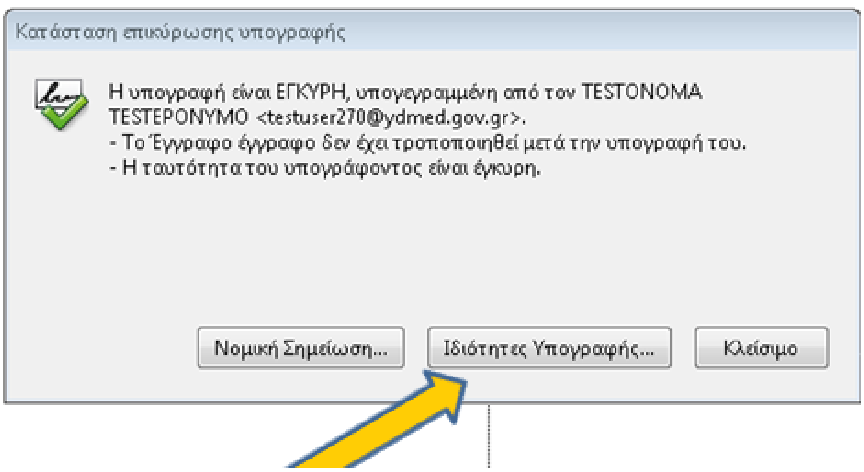
Ο χρήστης ανοίγει το υπογεγραμμένο έγγραφο PDF και κάνει κλικ πάνω στην ορατή υπογραφή όπως υποδεικνύεται στην παρακάτω Εικόνα 1.



Εικόνα 1

➢ **<u>ΒΗΜΑ 2ο</u>**

Στη συνέχεια ο χρήστης βλέπει το παράθυρο «κατάσταση επικύρωσης υπογραφής» όπου επιλέγει «ιδιότητες υπογραφής» όπως φαίνεται στην παρακάτω Εικόνα 2



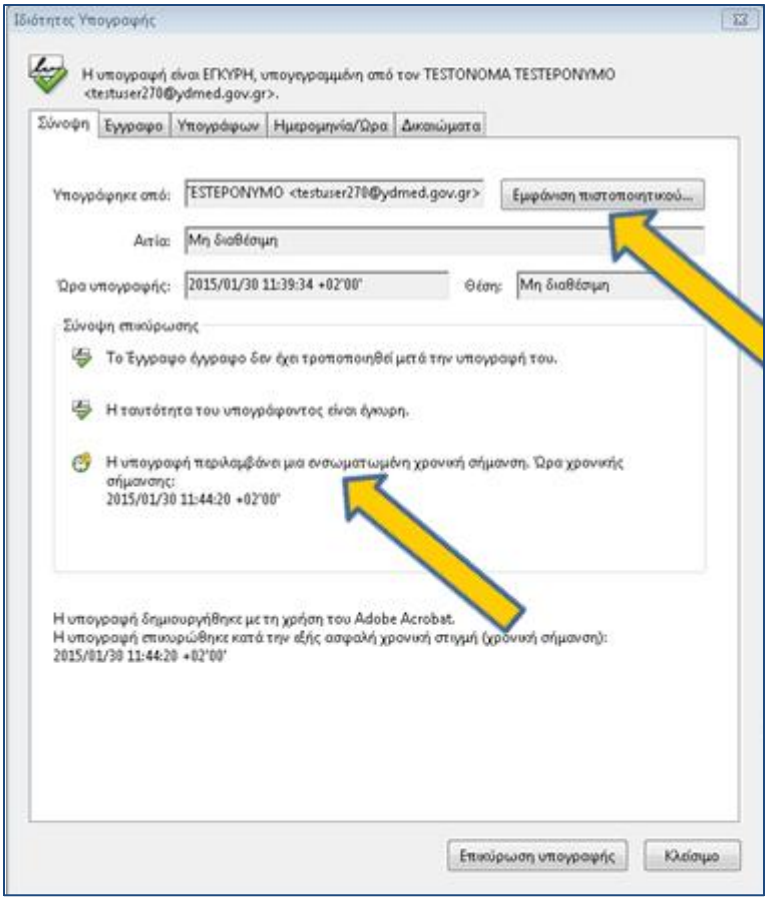
Εικόνα 2

➢ **<u>ΒΗΜΑ 3ο</u>**

Ο Χρήστης βρίσκεται στο περιβάλλον διερεύνησης για τις «Ιδιότητες Υπογραφής» όπου πραγματοποιεί τις ακόλουθες ενέργειες:

A. Ελέγχει αν το έγγραφο φέρει ενσωματωμένη χρονική σήμανση από αναγνωρισμένο πάροχο υπηρεσιών ασφαλούς χρονοσήμανσης όπως πρέπει και όχι την ώρα από το ρολόι του υπογράφοντος (κάτω βέλος στην παρακάτω Εικόνα 3)

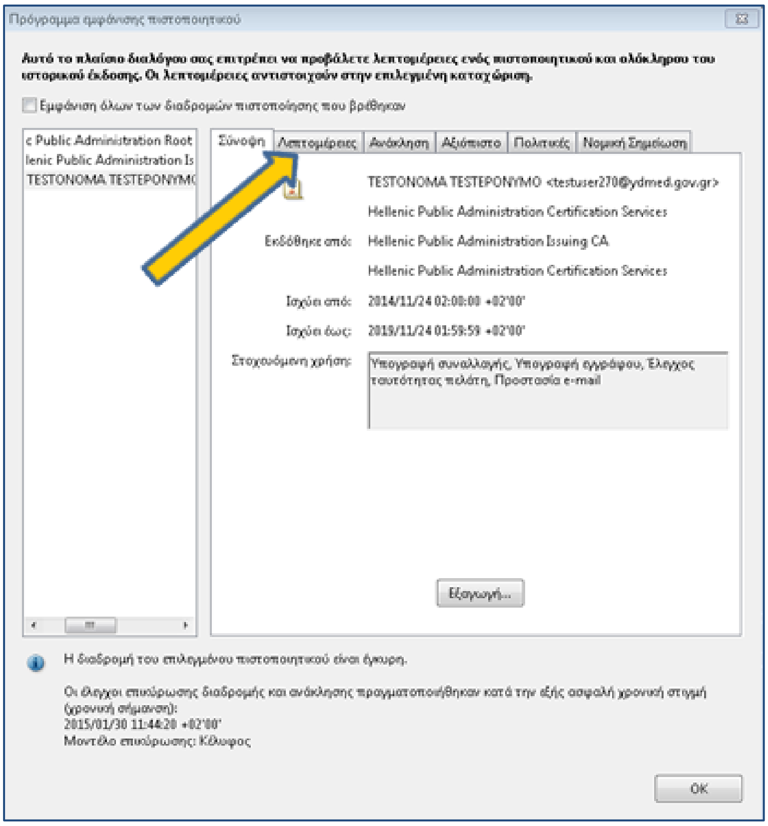
B. Επιλέγει «εμφάνιση πιστοποιητικού» (πάνω βέλος στην παρακάτω Εικόνα 3)



Εικόνα 3

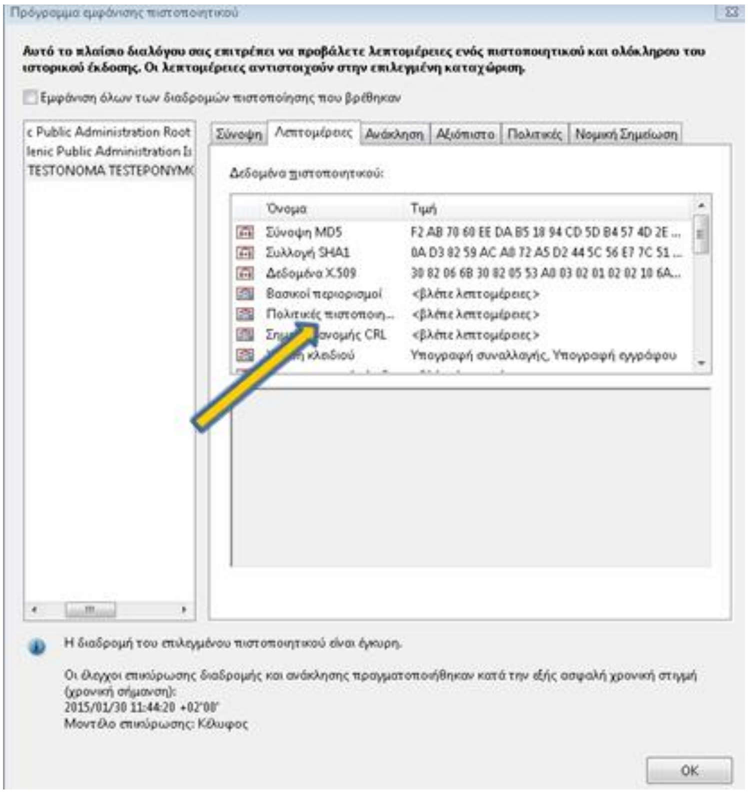
➢ **<u>ΒΗΜΑ 4ο</u>**

Ο Χρήστης βρίσκεται στο «πρόγραμμα εμφάνισης πιστοποιητικού» όπου επιλέγει «Λεπτομέρειες» (Εικόνα 4).



Εικόνα 4

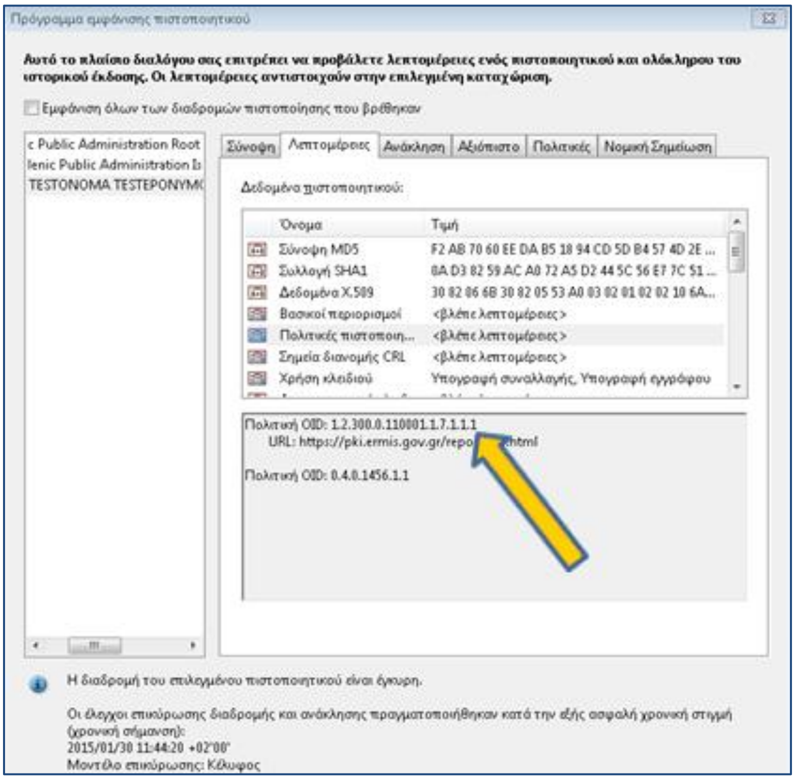
- **<u>ΒΗΜΑ 5ο</u>**



Εικόνα 5

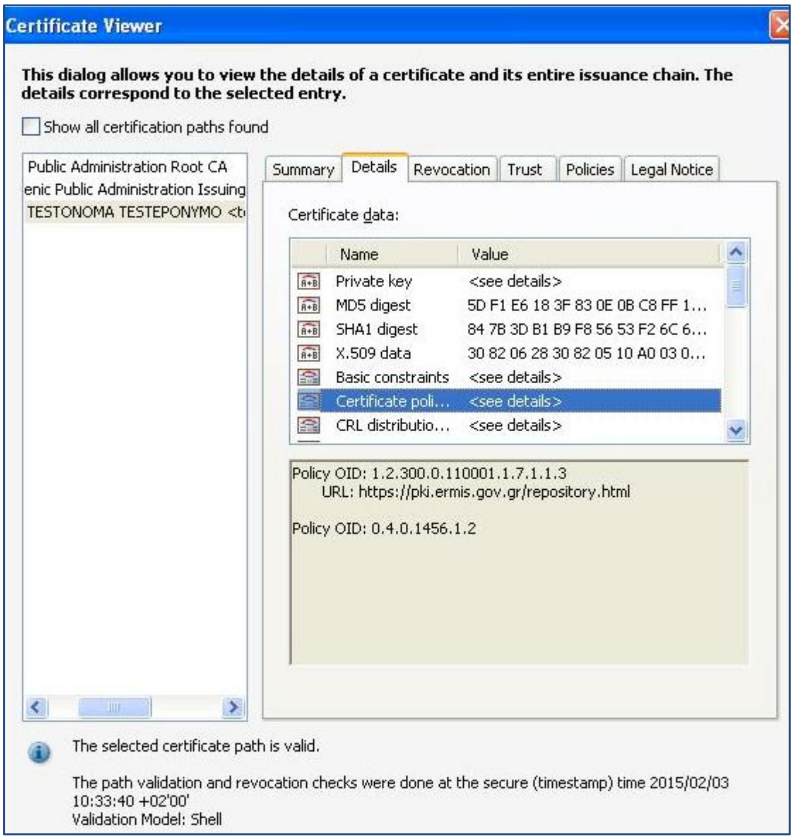
Όταν ο χρήστης επιλέξει «Λεπτομέρειες» μέσα από το «Πρόγραμμα εμφάνισης πιστοποιητικού» θα ανοίξει ένας κατάλογος με πληροφορίες όπου πρέπει να αναζητήσει τις «Πολιτικές πιστοποιητικών» (Εικόνα 5)

- **<u>ΒΗΜΑ 6ο</u>**



*Εικόνα 6 - Ψηφιακό Πιστοποιητικό **<u>Σκληρής</u>** Αποθήκευσης*

Όταν ο χρήστης επιλέξει «Πολιτικές πιστοποιητικών» / Certificate policies έχει τη δυνατότητα να ελέγξει αν το ψηφιακό πιστοποιητικό είναι σκληρής αποθήκευσης σύμφωνα με την ΠΠ1 όπου σύμφωνα με τον κανονισμό πιστοποίησης παράγραφο 1.2.5 η τιμή του Προσδιοριστή Αντικειμένου (αγγλικά Object Identifier- OID) για την Πολιτική Πιστοποίησης 1 είναι **1.2.300.0.110001.1.7.1.1.1**). Αντίστοιχα το αμέσως παρακάτω εμφανίζεται ο Προσδιοριστής Αντικειμένου κατά ETSI TS 101 456 παράγραφος 5.2, a) QCP public + SSCD. O ένας από τους δύο αυτούς ελέγχους αρκεί.
Η Εικόνα 6 υποδεικνύει πως ο χρήστης επιβεβαιώνει ότι πρόκειται για ψηφιακό πιστοποιητικό σκληρής αποθήκευσης.



*Εικόνα 7 - Ψηφιακό Πιστοποιητικό **Χαλαρής** Αποθήκευσης*

Στην Εικόνα 7 φαίνεται αντίστοιχα ψηφιακό πιστοποιητικό χαλαρής αποθήκευσης, αντιστοιχεί στον Προσδιοριστή Αντικειμένου για ΠΠ3 του κανονισμού πιστοποίησης της ΑΠΕΔ και Προσδιοριστής Αντικειμένου κατά ETSI TS 101 456 παράγραφος 5.2, b) QCP public.

Σε περίπτωση που ένα έγγραφο δεν έχει ορατή υπογραφή ο χρήστης επιλέγει «πάνελ υπογραφών» (βρίσκεται δεξιά στο πάνω μέρος του ψηφιακά υπογεγραμμένου εγγράφου, κάνει κλικ στον σύνδεσμο που εμφανίζεται αριστερά (π.χ. Αναθ. 1 Υπογράφηκε από ΤΕΣΤΟΝΟΜΑ ΤΕΣΤΕΠΩΝΥΜΟ <testuser270@ydmed.gov.gr>).

Στην καρτέλα που ανοίγει, ο χρήστης πραγματοποιεί τις ακόλουθες ενέργειες:

A. Ελέγχει αν το έγγραφο φέρει ενσωματωμένη χρονική σήμανση από αναγνωρισμένο πάροχο υπηρεσιών ασφαλούς χρονοσήμανσης όπως πρέπει και όχι την ώρα από το ρολόι του υπογράφοντος.
B. Επιλέγει «στοιχεία πιστοποιητικού», στη συνέχεια «Λεπτομέρειες» και ακολουθεί τα αντίστοιχα βήματα που περιγράφηκαν παραπάνω στην περίπτωση που το έγγραφο φέρει ορατή υπογραφή προκειμένου να ελέγξει με τον ίδιο τρόπο αν το έγγραφο φέρει προηγμένη ηλεκτρονική υπογραφή με τη χρήση ΑΔΔΥ και ψηφιακών πιστοποιητικών σκληρής αποθήκευσης από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου.