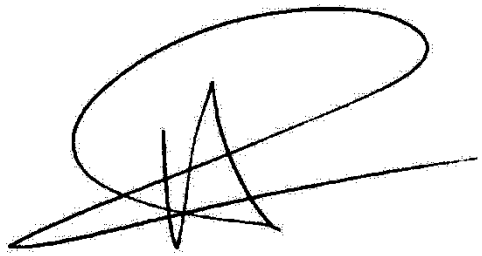
ΗΜΕΡΙΔΑ PAPERLESS ΔΙΑΔΙΚΑΣΙΩΝ Α΄Β/ΘΜΙΑΣ ΕΚΠΑΙΔΕΥΣΗΣ ΡΕΘΥΜΝΗΣ

Ψηφιακές Υπογραφές

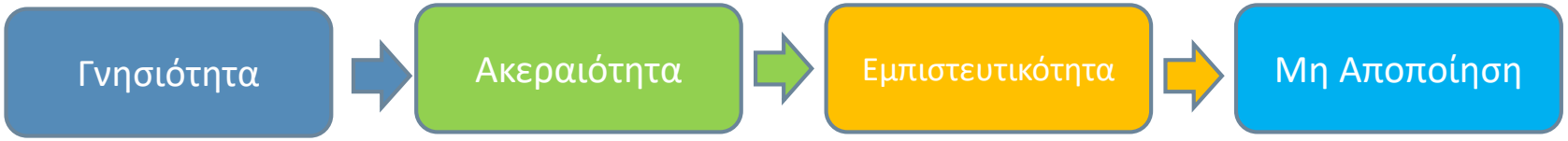
Ηλεκτρονική Υπογραφή

- Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε
- Τα ηλεκτρονικά έγγραφα τείνουν να αντικαταστήσουν τα «παραδοσιακά» χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται ηλεκτρονική.



Ηλεκτρονική Υπογραφή

- Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε
- Τα ηλεκτρονικά έγγραφα τείνουν να αντικαταστήσουν τα «παραδοσιακά» χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται ηλεκτρονική.



Ηλεκτρονική Υπογραφή

- Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε
- Τα ηλεκτρονικά έγγραφα τείνουν να αντικαταστήσουν τα «παραδοσιακά» χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται ηλεκτρονική.
- Ως ηλεκτρονική υπογραφή, λοιπόν, νοείται κάθε «κλειδωμένη» σύντμηση ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του
- Έχει επιβεβαιωτική λειτουργία (ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις) και εμπιστευτική λειτουργία (μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα)

Ορισμοί (ΠΔ 150/2001)

- **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
- **Προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή**
  - Συνδέεται μονοσήμαντα με τον υπογράφοντα
  - Είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
  - Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο
  - Συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλαγή
- **Πιστοποιητικό**
  - Ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του

Ορισμοί (ΠΔ 150/2001)

- **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
- **ΑΔΔΥ (Ασφαλή Διάταξη Δημιουργίας Υπογραφής)**
  - Διάταξη δημιουργίας υπογραφής σύμφωνα με συγκεκριμένες προδιαγραφές
- **Υπηρεσία Χρονοσήμανσης**
  - Η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε ψηφιακή μορφή, έτσι να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μια συγκεκριμένη χρονική στιγμή

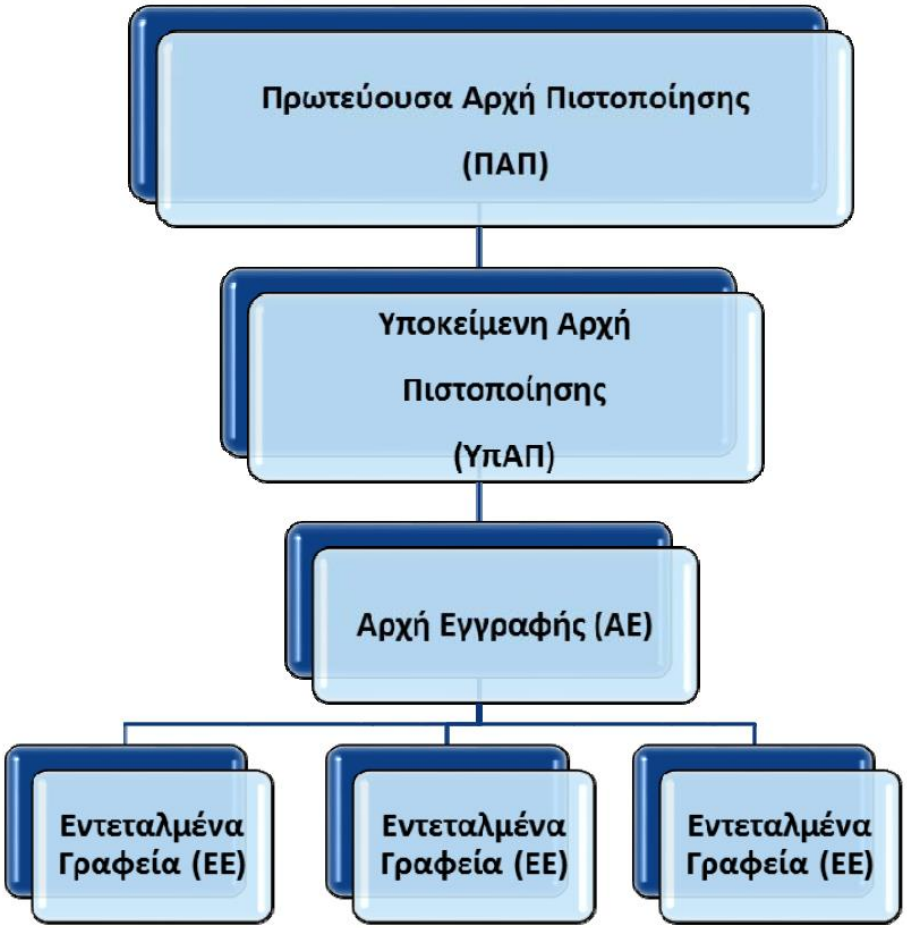
Αρχή Πιστοποίησης Ελληνικού Δημοσίου

- **Αρχή Πιστοποίησης**

  Ως Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (Hellenic Public Administration Root Certification Authority - HPARCA) και Πρωτεύουσα Αρχή Πιστοποίησης, ορίστηκε η Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) (Ν. 3536/2007 - ΦΕΚ 42/Α/23-2-2007)

- **Αρμοδιότητες**
  - Οι όροι για την έκδοση, τον έλεγχο, την ανάκληση και εν γένει τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών που εκδίδονται από την ΑΠΕΔ και τις Υποκείμενες σε αυτήν Αρχές (φορείς του δημόσιου τομέα),
  - οι πολιτικές πιστοποίησης,
  - Το προφίλ και η εμβέλεια των πιστοποιητικών που εκδίδονται,
  - Οι μηχανισμοί ασφάλειας για την προστασία του απορρήτου και των προσωπικών δεδομένων
  - Οι υποχρεώσεις των φορέων παροχής υπηρεσιών πιστοποίησης προς τους τελικούς χρήστες.

Αρχή Πιστοποίησης Ελληνικού Δημοσίου



Αρχή Πιστοποίησης στην Ελλάδα

- HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY
  https://pki.ermis.gov.gr/repository_en.html
- ADACOM ADVANCED INTERNET APPLICATIONS S.A.
  http://www.adacom.com/repository
- HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE S.A
  http://www.helex.gr/en/web/guest/digital-certificates
- BYTE Computer S.A.
  http://www.byte.gr/pki/repository/
- GREEK ACADEMIC NETWORK
  https://repo.harica.gr/

Αντίστοιχες αρχές υπάρχουν σε όλες τις χώρες της ΕΕ.
http://tlbrowser.tsl.website/tools/

Ψηφιακές υπογραφές

- Η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και **δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής (ΑΔΔΥ) επέχει θέση ιδιόχειρης υπογραφής** τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο (ΠΔ 150/2001).
- Η ισχύς της ψηφιακής υπογραφής ή το παραδεκτό της ως αποδεικτικό στοιχείο αποκλείεται μόνο αν δεν συντρέχουν οι προϋποθέσεις της προηγούμενης παραγράφου (ΠΔ 150/2001).

Ψηφιακές Υπογραφές

- Η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι **διαφορετική για κάθε μήνυμα.**
- Η ψηφιακή υπογραφή είναι **ένας τρόπος αυθεντικοποίησης** του αποστολέα του μηνύματος.
- Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Ψηφιακές Υπογραφές

Ψηφιακά Πιστοποιητικά – Ασύμμετρη Κρυπτογράφηση

1. Κάθε χρήστης διαθέτει **δύο κλειδιά κρυπτογράφησης**
   - Ιδιωτικό κλειδί (private key)
   - Δημόσιο κλειδί (public key)
2. Το ιδιωτικό κλειδί κρατιέται **κρυφό από κάθε χρήστη.**
3. Το δημόσιο κλειδί μπορεί να το βρει και να το χρησιμοποιήσει ο **οποιοσδήποτε τρίτος συμμετέχων.**

Ψηφιακές Υπογραφές

Ψηφιακά πιστοποιητικά – Συσχέτιση δημοσίου & ιδιωτικού κλειδιού

- «Ένα μήνυμα το οποίο κρυπτογραφείται με το ιδιωτικό κλειδί κάποιου χρήστη, αποκρυπτογραφείται με το δημόσιο κλειδί του ίδιου χρήστη»

Και αντίστροφα:

- «Ένα μήνυμα το οποίο κρυπτογραφείται με το δημόσιο κλειδί κάποιου χρήστη, αποκρυπτογραφείται με το ιδιωτικό κλειδί του ίδιου χρήστη»

Ψηφιακές Υπογραφές

Ψηφιακά πιστοποιητικά - Συνάρτηση κατακερματισμού

- Η συνάρτηση - αλγόριθμος κατακερματισμού (one way hash function) δημιουργεί **τη σύνοψη ενός μηνύματος** (message digest)
- •Ανεξάρτητα από το μέγεθος του μηνύματος, **παράγεται μία συγκεκριμένου μήκους σειρά ψηφίων**
- •Η διαφοροποίηση του μηνύματος προκαλεί **διαφοροποίηση της σύνοψης**
- •Είναι πρακτικά αδύνατο να βρεθεί μήνυμα το οποίο να παράγει την ίδια σύνοψη με ένα άλλο μήνυμα

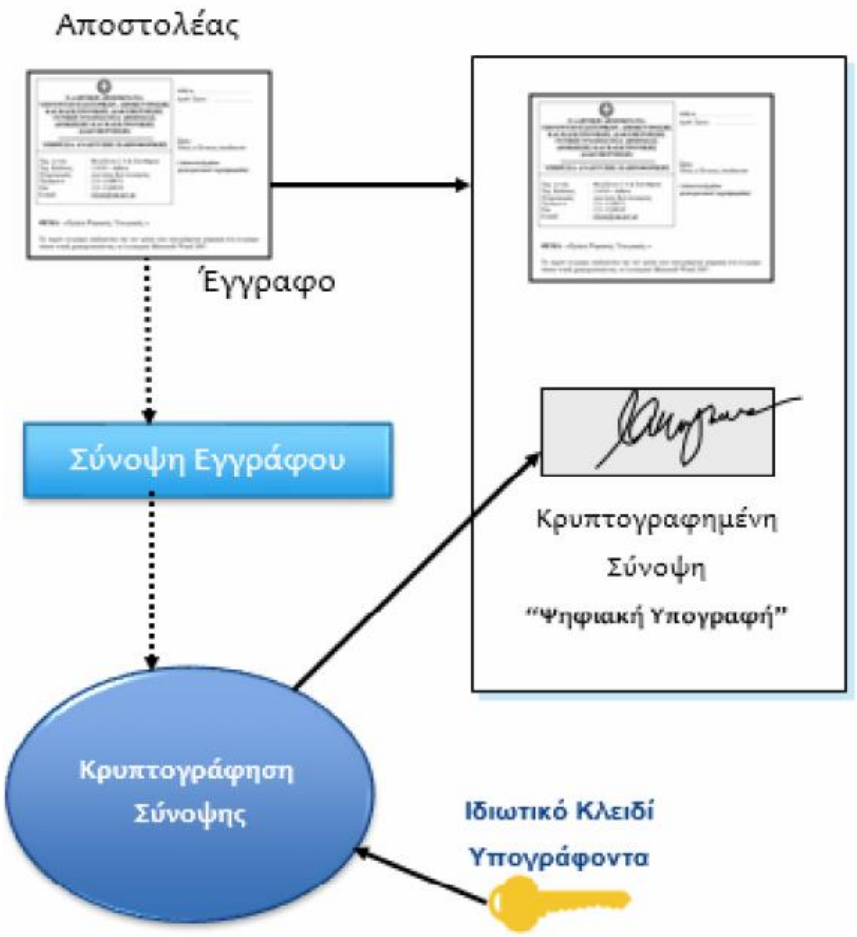
Ψηφιακές Υπογραφές

Ψηφιακά πιστοποιητικά - Δημιουργία ηλεκτρονικής υπογραφής

- Ο υπογράφων χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει
- •Με το ιδιωτικό του κλειδί, ο υπογράφων κρυπτογραφεί τη σύνοψη του μηνύματος
- •Η κρυπτογραφημένη σύνοψη είναι η ηλεκτρονική υπογραφή
- •Η ηλεκτρονική υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους
- •Η κρυπτογραφημένη σύνοψη (ηλεκτρονική υπογραφή) προσαρτάται στο αρχικό κείμενο

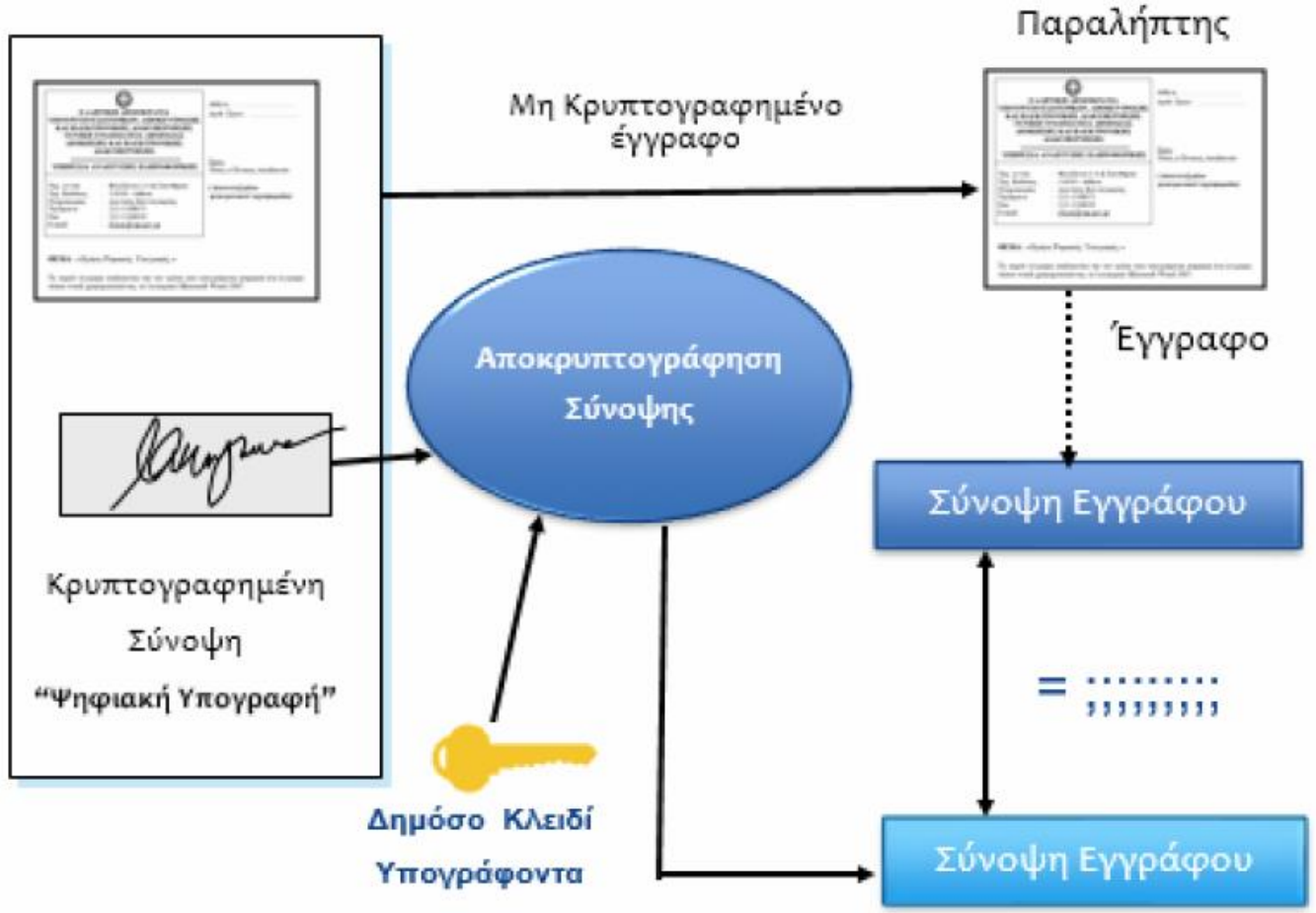
Ψηφιακές Υπογραφές

Ψηφιακά πιστοποιητικά – Δημιουργία Ηλεκτρονικής Υπογραφής



Ψηφιακές Υπογραφές

Ψηφιακά πιστοποιητικά – Επαλήθευση Ηλεκτρονικής Υπογραφής



Ψηφιακές Υπογραφές

Ψηφιακά Πιστοποιητικά – Πυλώνες Εμπιστοσύνης

- **Εμπιστευτικότητα (Confidentiality):** Μόνο εξουσιοδοτημένοι χρήστες θα μπορούν να έχουν πρόσβαση σε αυτές τις πληροφορίες. Η εμπιστευτικότητα επιτυγχάνεται με τη χρήση μεθόδων της κρυπτογραφίας.
- **Αυθεντικότητα (Authentication)**: Το σύστημα εξασφαλίζει ότι οι εμπλεκόμενοι σε μια συναλλαγή είναι αυτοί που δηλώνουν ότι είναι. Η απόδειξη γνησιότητας της υπογραφής επιτυγχάνεται με τα ψηφιακά πιστοποιητικά.
- **Ακεραιότητα (Integrity):** Μηνύματα που παραμένουν «ακέραια», δηλαδή, δεν πρέπει να τροποποιούνται ή να αλλοιώνονται. Η ανίχνευση τυχόν αλλοιώσεων επιτυγχάνεται με τους αλγόριθμους σύνοψης.
- **Μη αποκήρυξη (Non – Repudiation):** Ο αποστολέας δεν μπορεί να απαρνηθεί το μήνυμα και τις πιθανές συνέπειες ή υποχρεώσεις που συνδέονται με αυτό.

Ψηφιακές Υπογραφές

Ψηφιακά Πιστοποιητικά – Πυλώνες Εμπιστοσύνης

Παροχή υπηρεσίας ασφάλειας		Μέσο υλοποίησης της υπηρεσίας		Αποτέλεσμα
Προσδιορισμός και επικύρωση (**Identification & Authentication**)		Ψηφιακή Υπογραφή		Πιστοποίηση ταυτότητας υπογράφοντα
Εμπιστευτικότητα (**Confidentiality**)		Κρυπτογράφηση		Μόνο οι κάτοχοι κλειδιών έχουν πρόσβαση στην πληροφορία
Ακεραιότητα (**Integrity**)		Ψηφιακή Υπογραφή		Το μήνυμα δεν έχει αλλοιωθεί
Μη αποποίηση ευθύνης (**Non repudiation**)		Ψηφιακή Υπογραφή		Ο υπογράφων δεν μπορεί να αρνηθεί ότι υπέγραψε

Ψηφιακές Υπογραφές

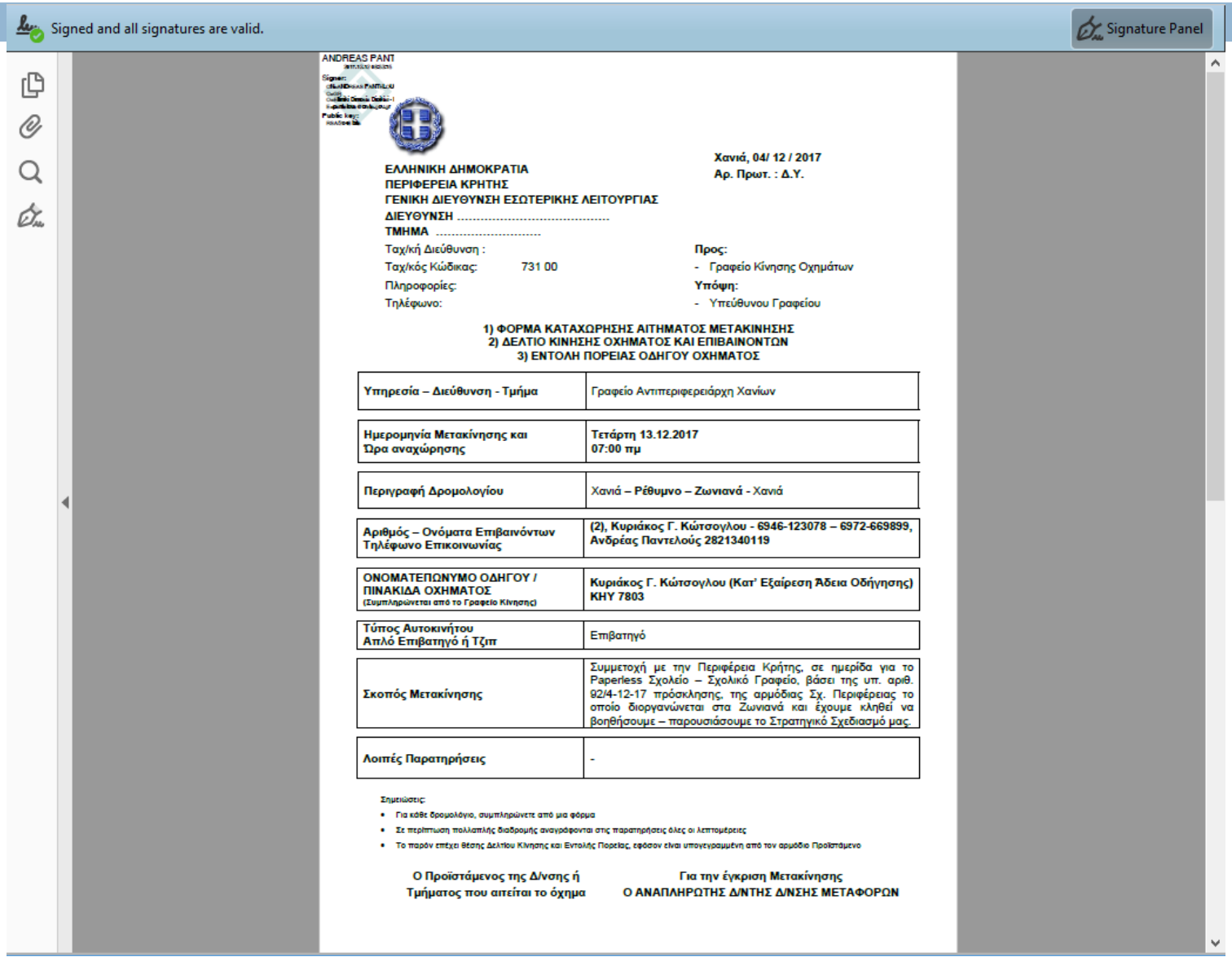
Class A (σκληρής αποθήκευσης)

- Πιστοποιητικά που έχουν εκδοθεί και εγκαθίστανται μόνο σε ασφαλή διάταξη (ΑΔΔΥ) όπως είναι η κρυπτοσυσκευή (usb token) ή η ακαδημαϊκή ταυτότητα
- εκδίδονται μόνο παρουσία κατάλληλου εξουσιοδοτημένου προσωπικού
- δεν μπορούν να αντιγραφούν

Class B (χαλαρής αποθήκευσης):

- Πιστοποιητικά που αποθηκεύονται σε αρχείο υπολογιστή
- Εκδίδονται με ενέργειες του χρήστη μέσω ιστοχώρου
- Μπορούν να υπάρχουν πολλαπλά αντίγραφα

Ψηφιακές Υπογραφές



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑ ΚΡΗΤΗΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΣΩΤΕΡΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ
ΔΙΕΥΘΥΝΣΗ .....
ΤΜΗΜΑ .....
Ταχ/κή Διεύθυνση :
Ταχ/κός Κώδικας: 731 00
Πληροφορίες:
Τηλέφωνο:

Χανιά, 04/ 12 / 2017
Αρ. Πρωτ. : Δ.Υ.

Προς:
- Γραφείο Κίνησης Οχημάτων

Υπόψη:
- Υπεύθυνου Γραφείου

1) ΦΟΡΜΑ ΚΑΤΑΧΩΡΗΣΗΣ ΑΙΤΗΜΑΤΟΣ ΜΕΤΑΚΙΝΗΣΗΣ
2) ΔΕΛΤΙΟ ΚΙΝΗΣΗΣ ΟΧΗΜΑΤΟΣ ΚΑΙ ΕΠΙΒΑΙΝΟΝΤΩΝ
3) ΕΝΤΟΛΗ ΠΟΡΕΙΑΣ ΟΔΗΓΟΥ ΟΧΗΜΑΤΟΣ

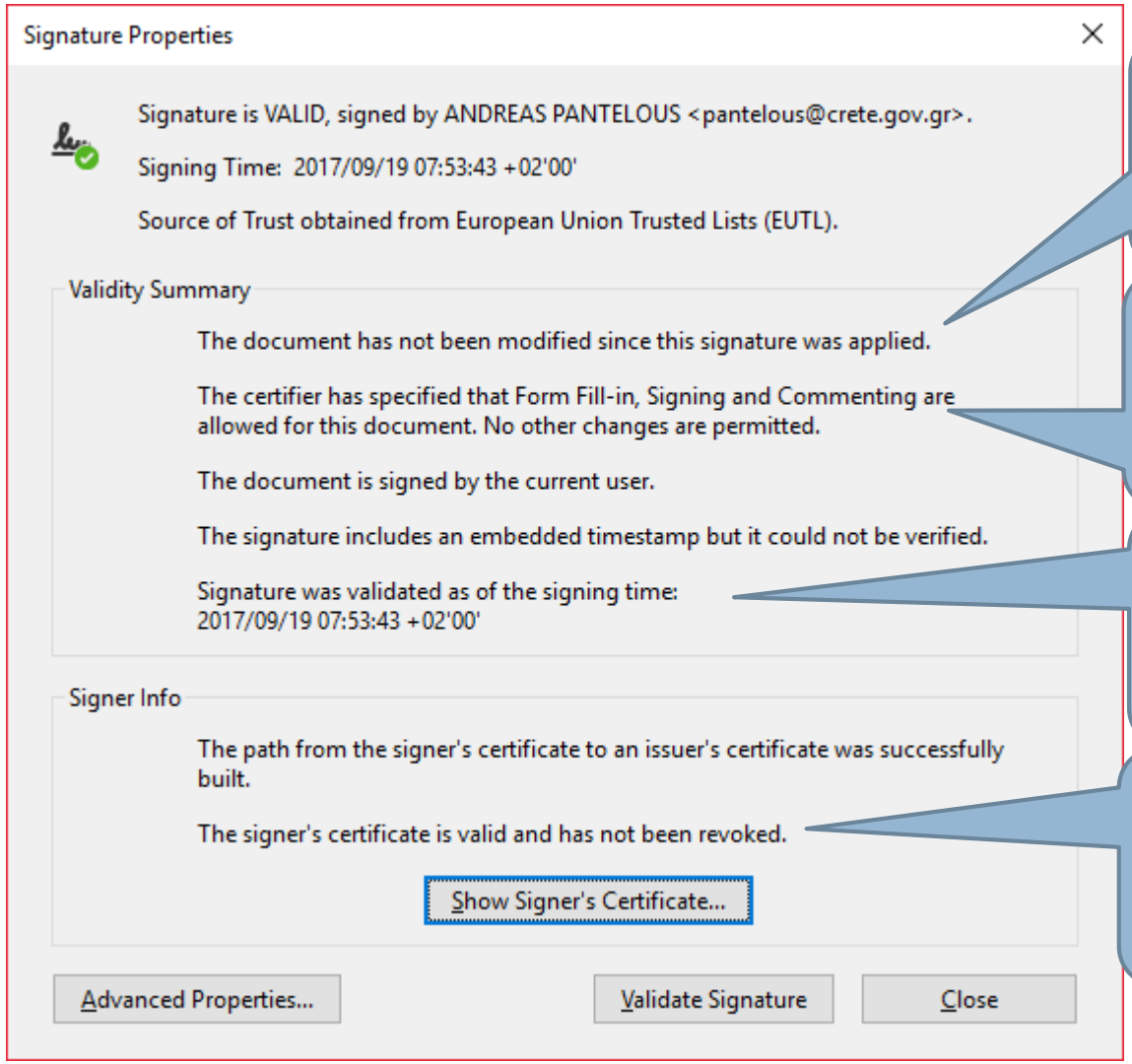
Υπηρεσία – Διεύθυνση - Τμήμα	Γραφείο Αντιπεριφερειάρχη Χανίων
Ημερομηνία Μετακίνησης και Ώρα αναχώρησης	**Τετάρτη 13.12.2017 07:00 πμ**
Περιγραφή Δρομολογίου	Χανιά – **Ρέθυμνο – Ζωνιανά** - Χανιά
Αριθμός – Ονόματα Επιβαινόντων Τηλέφωνο Επικοινωνίας	**(2), Κυριάκος Γ. Κώτσογλου - 6946-123078 – 6972-669899, Ανδρέας Παντελούς 2821340119**
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΟΔΗΓΟΥ / ΠΙΝΑΚΙΔΑ ΟΧΗΜΑΤΟΣ (Συμπληρώνεται από το Γραφείο Κίνησης)	**Κυριάκος Γ. Κώτσογλου (Κατ' Εξαίρεση Άδεια Οδήγησης) ΚΗΥ 7803**
Τύπος Αυτοκινήτου Απλό Επιβατηγό ή Τζιπ	Επιβατηγό
Σκοπός Μετακίνησης	Συμμετοχή με την Περιφέρεια Κρήτης, σε ημερίδα για το Paperless Σχολείο – Σχολικό Γραφείο, βάσει της υπ. αριθ. 92/4-12-17 πρόσκλησης, της αρμόδιας Σχ. Περιφέρειας το οποίο διοργανώνεται στα Ζωνιανά και έχουμε κληθεί να βοηθήσουμε – παρουσιάσουμε το Στρατηγικό Σχεδιασμό μας.
Λοιπές Παρατηρήσεις	-

Σημειώσεις:
- Για κάθε δρομολόγιο, συμπληρώνετε από μια φόρμα
- Σε περίπτωση πολλαπλής διαδρομής αναγράφονται στις παρατηρήσεις όλες οι λεπτομέρειες
- Το παρόν επέχει θέση Δελτίου Κίνησης και Εντολής Πορείας, εφόσον είναι υπογεγραμμένη από τον αρμόδιο Προϊστάμενο

Ο Προϊστάμενος της Δ/νσης ή Τμήματος που αιτείται το όχημα

Για την έγκριση Μετακίνησης
Ο ΑΝΑΠΛΗΡΩΤΗΣ Δ/ΝΤΗΣ Δ/ΝΣΗΣ ΜΕΤΑΦΟΡΩΝ

Ψηφιακές Υπογραφές

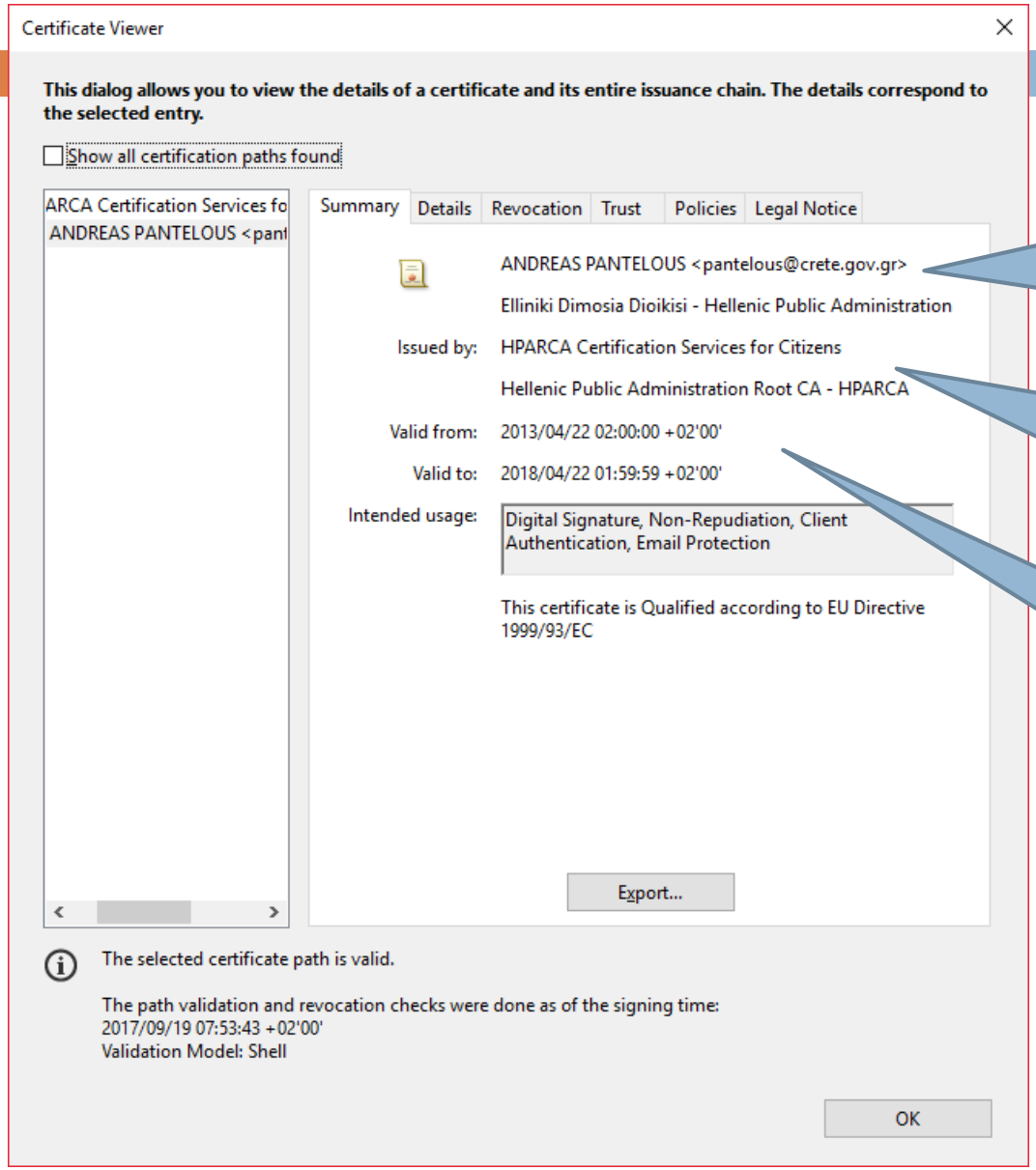


1. Το έγγραφο δεν έχει αλλάξει μετά την υπογραφή

2. Αναφέρεται τι δυνατότητες για αλλαγές έχει δώσει ο υπογράφων

3. Χρονοσήμανση

4. Το πιστοποιητικό του υπογράφοντα είναι έγκυρο.



Το όνομα του υπογράφοντα.

Η Αρχή Πιστοποίησης

Η διάρκεια ισχύς του πιστοποιητικού

Διάφορες Διαδικασίες Ψηφιακών Υπογραφών

- Διαδικασία Απόκτησης Ψηφιακών Υπογραφών
  - http://www.aped.gov.gr/more/obtainsignature.html
- Διαδικασία Ανάκλησης Ψηφιακών Πιστοποιητικών
  - http://www.aped.gov.gr/more/obtainsignature.html
- Διαδικασία Ανανέωσης Ψηφιακών Πιστοποιητικών
  - http://www.aped.gov.gr/procedures/16-how-to/12-renew-cert.html