“IT WORKS FOR ME”

Ψηφιακή υπογραφή εγγράφων

Τμήμα Διοικητικής Υποστήριξης & Υποστήριξης Χρηστών

Στόχοι

Ολοκληρώνοντας αυτό το σεμινάριο θα γνωρίζετε:

1. Βασικές έννοιες για τα ψηφιακά πιστοποιητικά
2. Πώς ρυθμίζετε τον υπολογιστή σας για χρήση της ακαδημαϊκής κάρτας
3. Πώς μετατρέπετε ένα αρχείο Word σε pdf
4. Πώς υπογράφετε ψηφιακά ένα έγγραφο pdf
5. Πώς ελέγχετε την εγκυρότητα ενός ψηφιακά υπογεγραμμένου εγγράφου

Προεπισκόπηση παρουσίασης

- ✓ **Γενικά για τα ψηφιακά πιστοποιητικά**
- ✓ Απόκτηση ακαδημαϊκής ταυτότητας
- ✓ Ρύθμιση συσκευών για χρήση της ακαδημαϊκής ταυτότητας
- ✓ Ψηφιακή υπογραφή εγγράφου
- ✓ Επικύρωση υπογεγραμμένου εγγράφου

Νομοθεσία

Διεθνής αναγνώριση των ψηφιακών υπογραφών ως ισότιμες με τις χειρόγραφες και σε μερικές περιπτώσεις ως ισχυρότερες

- ✓ Η Ευρωπαϊκή οδηγία ΕC/93/99 έχει ήδη υιοθετηθεί από όλα τα κράτη μέλη
- ✓ Η ΕΕΤΤ με την απόφαση 248/71 (ΦΕΚ 603Β΄/16-5-2002) ρυθμίζει την διαπίστευση των παρόχων υπηρεσιών πιστοποίησης και την έκδοση ‘αναγνωρισμένων πιστοποιητικών’
- ✓ Αναγνώριση συναλλαγών με το δημόσιο με χρήση ΤΠΕ ΦΕΚ 138/16-06-2011
- ✓ Οδηγία για ηλεκτρονικές υπογραφές ΠΔ 25/ΦΕΚ 44/25-02-2014

Τι είναι το ψηφιακό πιστοποιητικό;

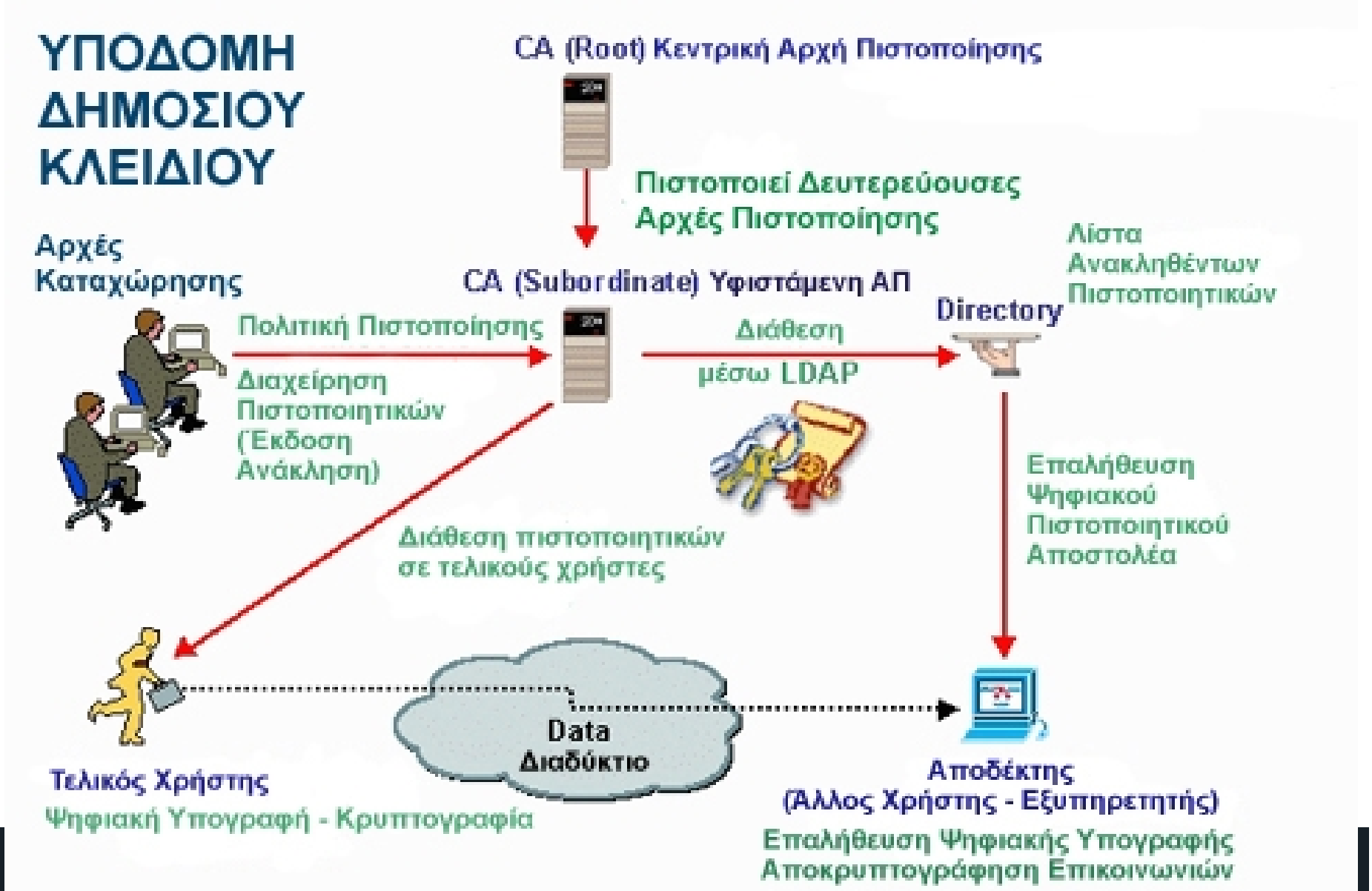
Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την αναγνώριση μίας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός κοκ).

Το ψηφιακό πιστοποιητικό ενός χρήστη είναι για τον ηλεκτρονικό κόσμο το **ανάλογο της αστυνομικής ταυτότητας.**

Για την έκδοση σε φυσικό πρόσωπο απαιτείται:

- ✓ Μια Αρχή Πιστοποίησης (εκδότης)
- ✓ Μια Αρχή Καταχώρησης
- ✓ Ταυτοποίηση δικαιούχου
- ✓ Ένα μέσο αποθήκευσης

Ποιος εκδίδει ψηφιακά πιστοποιητικά;



Τι πληροφορίες περιέχει;

Περιέχει:

- ✓ Αναγνωριστικά: Τύπος-πρότυπο, έκδοση, αλγόριθμος υπογραφής
- ✓ Πληροφορίες εκδότη
- ✓ Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού
- ✓ Το δημόσιο κλειδί του κατόχου του πιστοποιητικού
- ✓ Περίοδο ισχύος (από - έως)
- ✓ Επεκτάσεις και κρίσιμες επεκτάσεις
- ✓ Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε
- ✓ Σύνοψη πιστοποιητικού ως κλειδί αναφοράς

Hellenic Academic and Research Institutions Certification Authority

Αρχή Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων

Από τις **4/6/2015** η Κεντρική Αρχή Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (HARICA) έχει ενταχθεί στο Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής της Ε.Ε.Τ.Τ.

Η HARICA είναι μέλος του Mozilla Root CA program από το 2012, του Microsoft Root CA program από τον Ιούνιο του 2013 και του Apple Root CA program από το Σεπτέμβριο του 2013

Είδη-Χρήσεις ψηφιακών πιστοποιητικών χρηστών

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

Τι είναι η ψηφιακή υπογραφή;

Είναι ένας τρόπος **αυθεντικοποίησης** του υπογράφοντα με χρήση αλγορίθμων και μαθηματικών συναρτήσεων στον ψηφιακό κόσμο

Απαιτούνται 3 αλγόριθμοι:

1. Δημιουργίας του ζεύγους κλειδιών (ιδιωτικό και δημόσιο)
2. Προσθήκης ψηφιακής υπογραφής
3. Ελέγχου ψηφιακής υπογραφής

Τι είναι η ψηφιακή υπογραφή;

Η ψηφιακή υπογραφή που δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο (κάρτα ή ειδική συσκευή usb) είναι αυτή που σύμφωνα με το άρθρο 2 του ΠΔ 150/2001 ορίζεται ως «Προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή».

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

Γιατί προσθήκη χρονοσήμανσης;

Τι είναι η **Χρονοσήμανση**

Αλληλουχία χαρακτήρων ή στοιχεία που δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια και εκδίδεται από πάροχο υπηρεσιών χρονοσήμανσης.

Για τους φορείς του Δημόσιου Τομέα ο ακριβής χρόνος προσδιορίζεται με βάση την Εθνική ώρα Ελλάδας.

Προεπισκόπηση παρουσίασης

- ✓ Γενικά για τα ψηφιακά πιστοποιητικά
- ✓ **Απόκτηση ακαδημαϊκής ταυτότητας**
- ✓ Ρύθμιση συσκευών για χρήση της ακαδημαϊκής ταυτότητας
- ✓ Ψηφιακή υπογραφή εγγράφου
- ✓ Επικύρωση υπογεγραμμένου εγγράφου

Πώς θα αποκτήσω ακαδημαϊκή ταυτότητα;

Ηλεκτρονική Υπηρεσία Απόκτησης Ακαδημαϊκής Ταυτότητας (ΥΠΟΠΑΙΘ)
http://academicid.minedu.gov.gr/
(Γραφείο Αρωγής χρηστών υπηρεσίας)

Απαραίτητα για υποβολή:

- ✓ Φωτογραφία τύπου ταυτότητας ή διαβατηρίου (jpeg, 3MB, 240x240)

Παραλαβή από Διεύθυνση προσωπικού ΑΠΘ με:

- ✓ 12ψήφιο κωδικό αίτησης
- ✓ Αστυνομική ταυτότητα

Προεπισκόπηση παρουσίασης

- ✓ Γενικά για τα ψηφιακά πιστοποιητικά
- ✓ Απόκτηση ακαδημαϊκής ταυτότητας
- ✓ **Ρύθμιση συσκευών για χρήση της ακαδημαϊκής ταυτότητας**
- ✓ Ψηφιακή υπογραφή εγγράφου
- ✓ Επικύρωση υπογεγραμμένου εγγράφου

Οδηγίες

Ρύθμιση συσκευής
http://it.auth.gr/el/setupAcademicId

Έλεγχος πιστοποιητικού
http://it.auth.gr/el/checkAcademicId

Ρύθμιση για χρήση token
http://it.auth.gr/el/classwebSetup

Προεπισκόπηση παρουσίασης

- ✓ Γενικά για τα ψηφιακά πιστοποιητικά
- ✓ Απόκτηση ακαδημαϊκής ταυτότητας
- ✓ Ρύθμιση συσκευών για χρήση της ακαδημαϊκής ταυτότητας
- ✓ **Ψηφιακή υπογραφή εγγράφου**
- ✓ Επικύρωση υπογεγραμμένου εγγράφου

Ψηφιακή υπογραφή εγγράφου

Προϋποθέσε  

- ✓ Ακαδημαϊκή ταυτότητα ή άλλη ΑΔΔΥ
- ✓ Έκδοση πιστοποιητικού σε ΑΔΔΥ
- ✓ Adobe Reader
  - ρύθμιση διακομιστή χρονοσήμανσης

Σημαντικό

Ένα έγγραφο μπορεί να υπογραφεί διαδοχικά από περισσότερους τους ενός υπογράφοντα

http://it.auth.gr/el/signpdf

Διαμόρφωση εμφάνισης υπογραφής

- Εμφάνιση υπογραφής για τα μέλη του ΑΠΘ

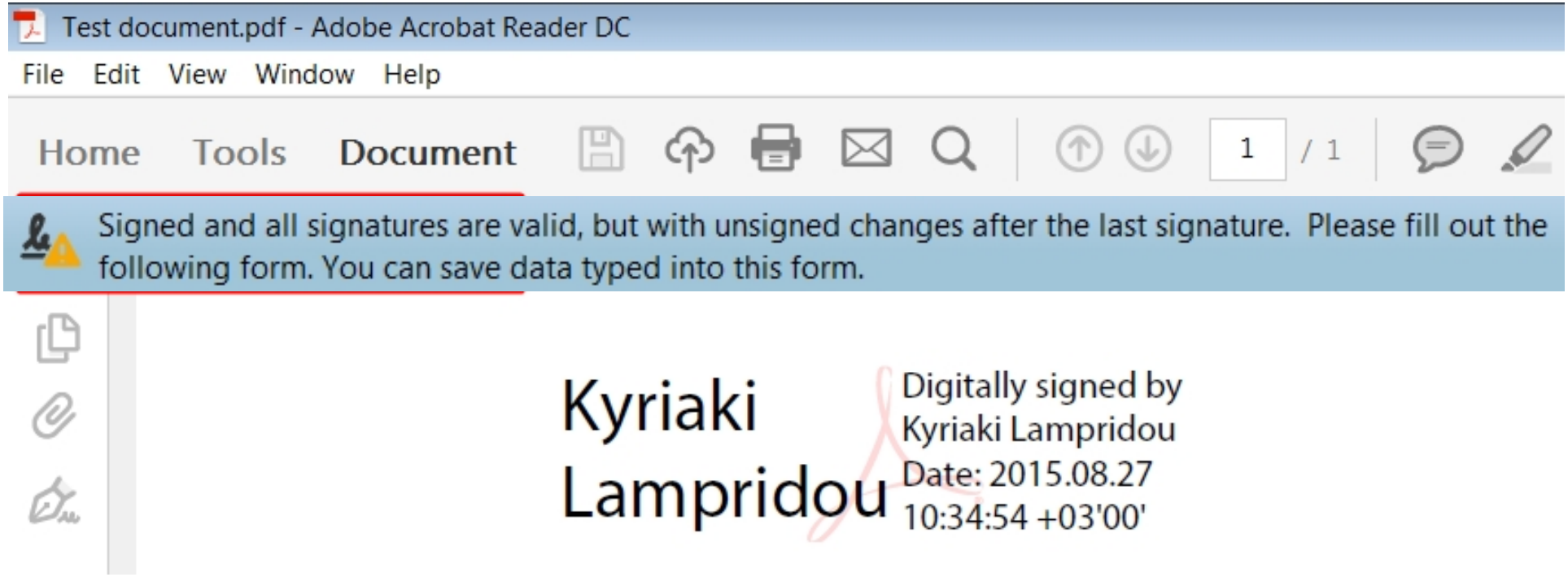
Kyriaki Lampridou
c=GR, o=Aristotle University of Thessaloniki, ou=IT Center,
ou=Class B - Private Key created and stored in software
CSP, cn=Kyriaki Lampridou, email=korina@it.auth.gr
2016.02.16 12:58:57 +02'00'

Οδηγίες διαμόρφωσης
https://it.auth.gr/el/logoAUThsign

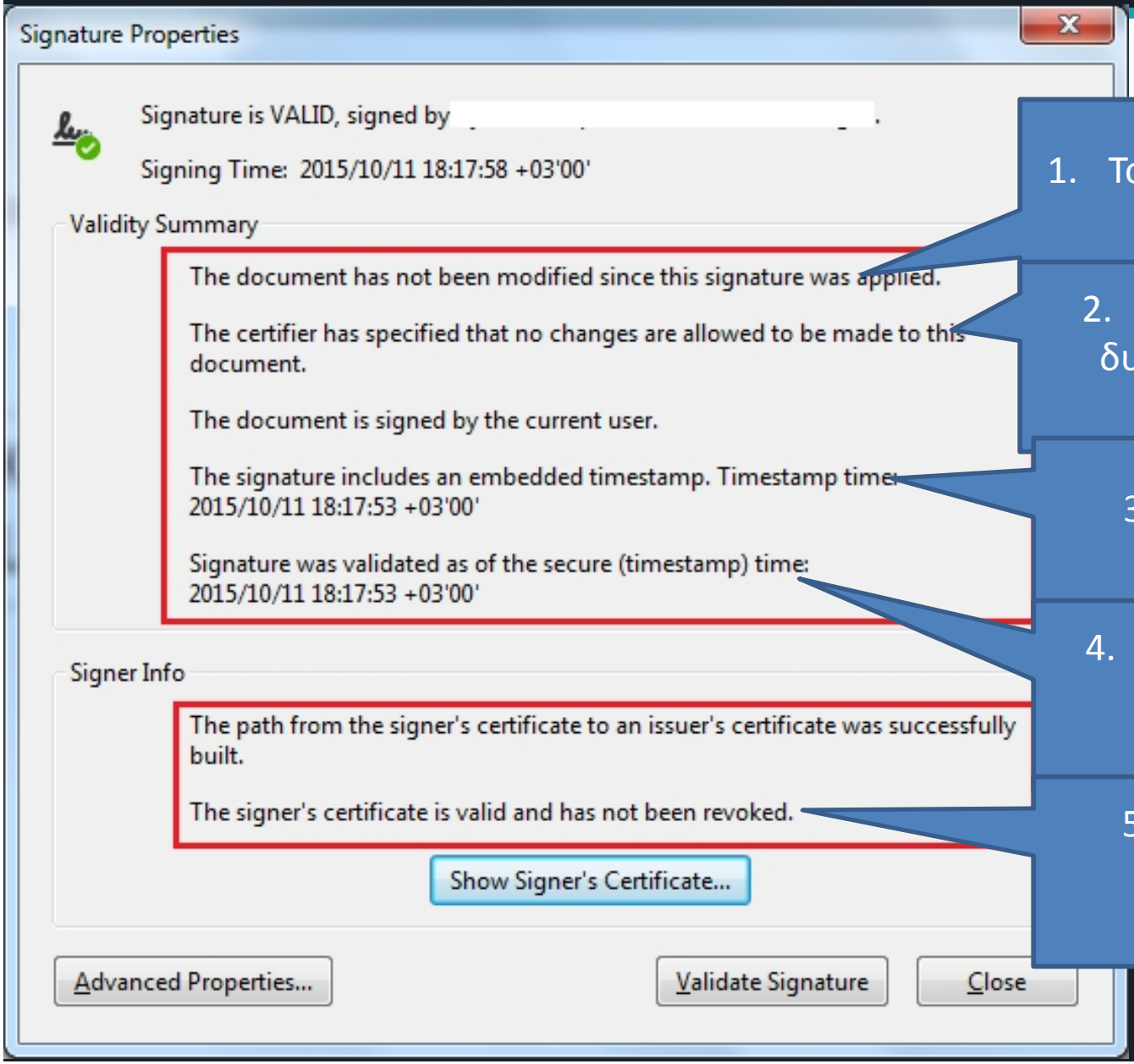
Προεπισκόπηση παρουσίασης

- ✓ Γενικά για τα ψηφιακά πιστοποιητικά
- ✓ Απόκτηση ακαδημαϊκής ταυτότητας
- ✓ Ρύθμιση συσκευών για χρήση της ακαδημαϊκής ταυτότητας
- ✓ Ψηφιακή υπογραφή εγγράφου
- ✓ **Επικύρωση υπογεγραμμένου εγγράφου**

Έλεγχος εγκυρότητας υπογεγραμμένου εγγράφου



Έλεγχος εγκυρότητας υπογεγραμμένου εγγράφου



1. Το έγγραφο δεν έχει αλλάξει μετά την υπογραφή
2. Αυτός που υπογράφει τι δυνατότητες για αλλαγές έχει δώσει στο έγγραφο
3. Πληροφορίες για την προσθήκη χρονοσήμανσης
4. Με ποιον τρόπο γίνεται η επικύρωση της χρονοσήμανσης
5. Το πιστοποιητικό του υπογράφοντα είναι έγκυρο και δεν έχει ανακληθεί

Χρήσεις

- ✓ Υποχρεωτική (από 1.7.2015) αποστολή εγγράφων για δημοσίευση στο **Φύλλο της Εφημερίδας της Κυβέρνησης** με χρήση τεχνολογιών πληροφορικής και επικοινωνιών και προηγμένης ηλεκτρονικής υπογραφής

- ✓ Η χρήση του συστήματος **ΕΣΗΔΗΣ από τους Οικονομικούς Φορείς (προμηθευτές δημοσίου)** πραγματοποιείται με τη χρήση προηγμένης ψηφιακής υπογραφής.

- ✓ Οι **αναθέτουσες αρχές** υποχρεούνται να χρησιμοποιούν αποκλειστικά το ΕΣΗΔΗΣ σε όλα τα στάδια της διαδικασίας ανάθεσης δημοσίων συμβάσεων, δηλαδή από την υποβολή αιτήματος μέχρι την υπογραφή και εκτέλεση των συμβάσεων αυτών, για τους διαγωνισμούς με προϋπολογισμό >60.000€

Ερωτήσεις – Συζήτηση

Σας ευχαριστούμε!