Digital signatures in practice in Greece: Capabilities and limitations

Dimitrios Lekkas, Dimitris Gritzalis

September 2014

Σύνδεσμος Επιχειρήσεων Διεθνούς Διαμεταφοράς
& Επιχειρήσεων Logistics Ελλάδος
Αθήνα, 24 Σεπτέμβρη 2014

Ψηφιακές Υπογραφές στην πράξη: Δυνατότητες και περιορισμοί

Δημήτρης Λέκκας (dlek@aegean.gr)
Επίκουρος Καθηγητής Πανεπιστημίου Αιγαίου

Δημήτρης Γκρίτζαλης (dgrit@aueb.gr)
Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών

Η υπογραφή στον Ψηφιακό κόσμο

- Η **ηλεκτρονική υπογραφή** είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητάς του.

- Η αυθεντικότητα ενός ηλεκτρονικού κειμένου περιλαμβάνει τις έννοιες της **ακεραιότητας** και της **ταυτοποίησης της προέλευσης**.

Ευρωπαϊκή Νομοθεσία (1)

«Ψηφιακή Υπογραφή» ή
«Προηγμένη Ηλεκτρονική Υπογραφή»

- Μονοσήμαντα συνδεδεμένη με τον υπογράφοντα
- Παρέχει τη δυνατότητα ταυτοποίησης του υπογράφοντα
- Δημιουργείται με μέσα που βρίσκονται στον αποκλειστικό έλεγχο του υπογράφοντα
- Μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο, με τρόπο ώστε να διασφαλίζεται η ακεραιότητά του
- Δεν μπορεί να δημιουργηθεί από άλλη οντότητα και δεν μπορεί να μεταφερθεί σε άλλο κείμενο
- Ο υπογράφων δεν μπορεί να αρνηθεί ότι δημιούργησε μια υπογραφή

Ευρωπαϊκή Νομοθεσία (2)

- Δεδομένα δημιουργίας υπογραφής:

  Μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται για τη δημιουργία ηλεκτρονικής υπογραφής

- Δεδομένα επαλήθευσης υπογραφής:

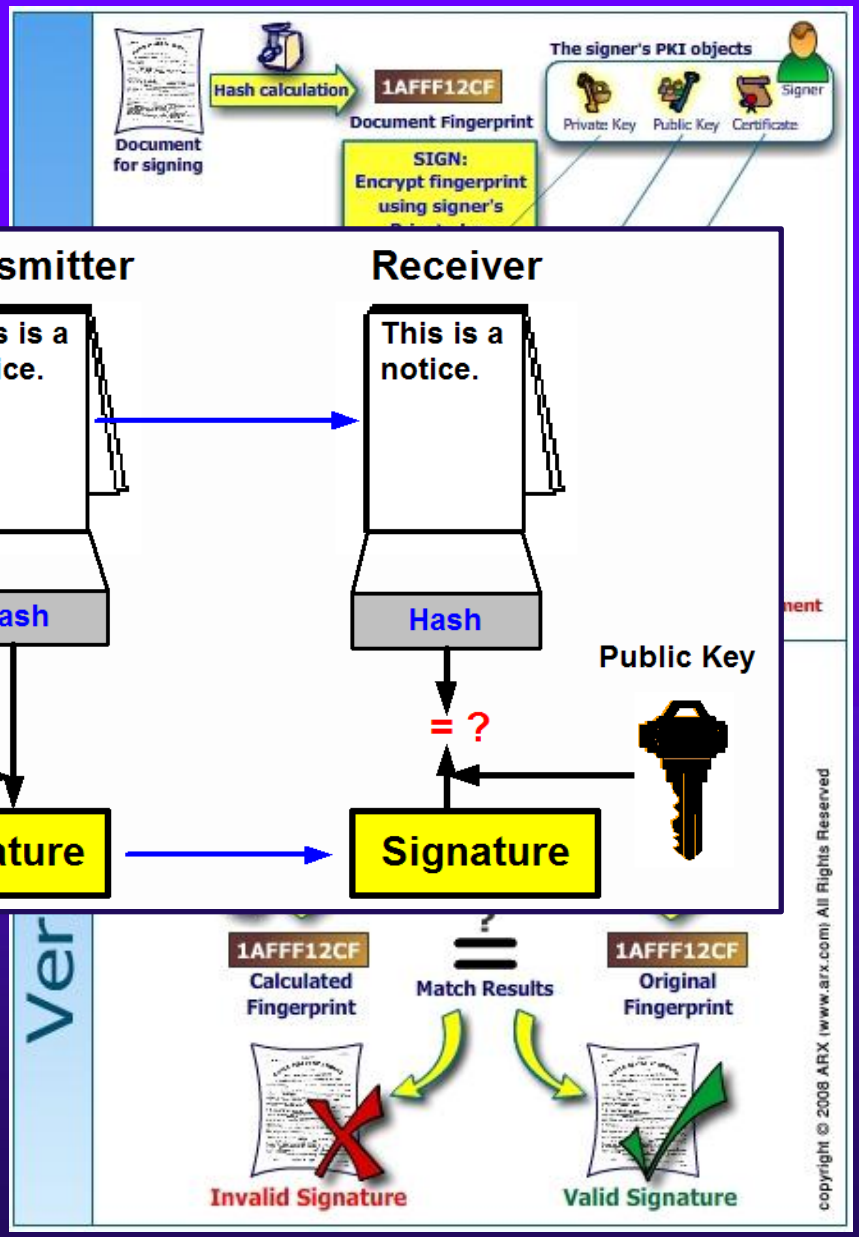
  Δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, που χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής

Στην πράξη: Κρυπτογραφία

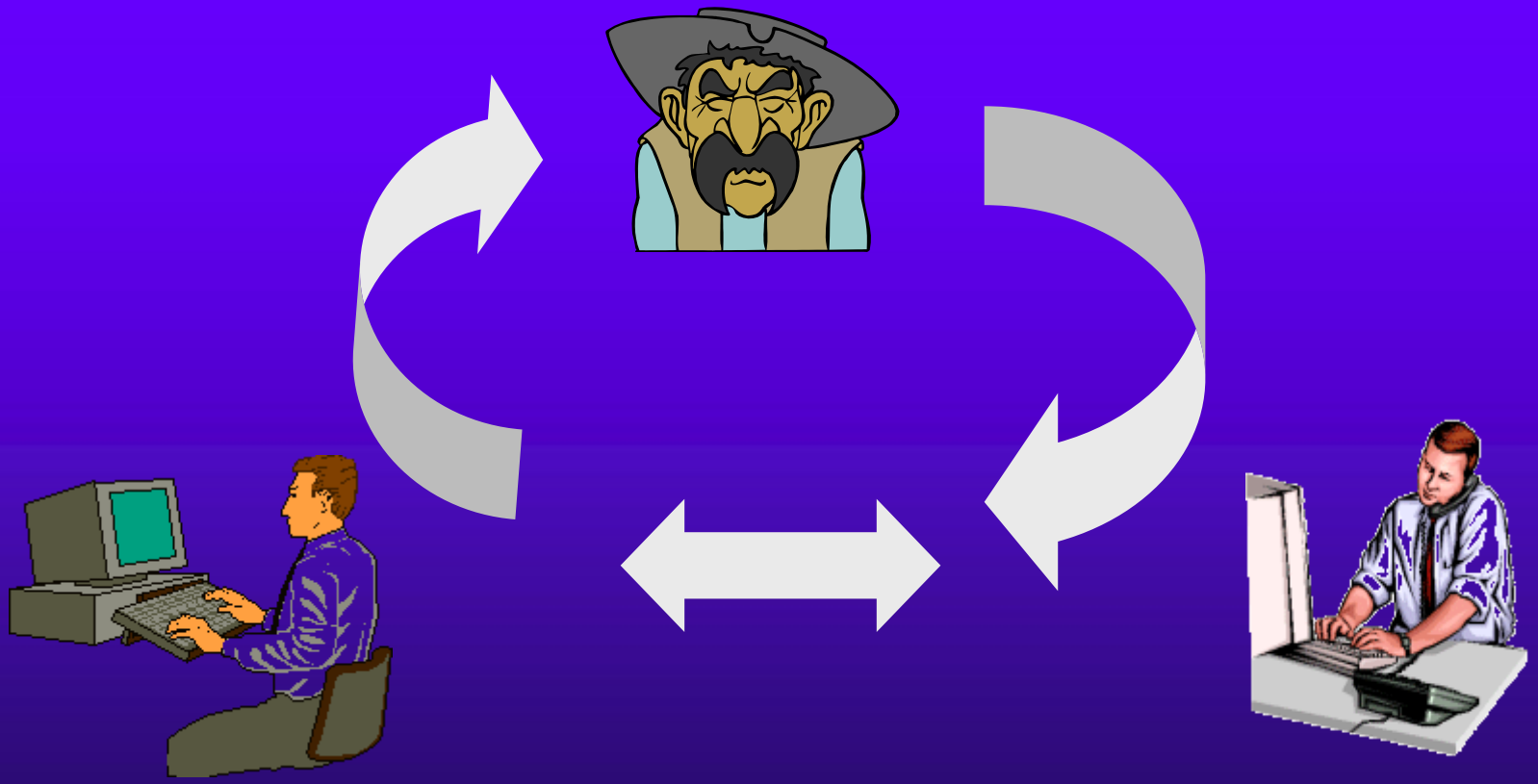
- Δημιουργία ζεύγους κλειδιών
- Ασφαλής αποθήκευση ιδιωτικού κλειδιού (δεδομένα δημιουργίας υπογραφής)
- Διανομή και δημοσίευση δημόσιου κλειδιού (δεδομένα επαλήθευσης υπογραφής)

Μηχανισμός Ψηφιακών Υπογραφών

- Ο αποστολέας υπογράφει (κρυπτογραφεί) το μήνυμα με το του κλειδί
- Ο παραλήπτης αποκρυπτογρα υπογραφή με κλειδί του απο
- Επιβεβαιώνει, μήνυμα υπογρ τον μοναδικό κάτοχο του αντίστοιχου ιδιωτικού κλειδιού



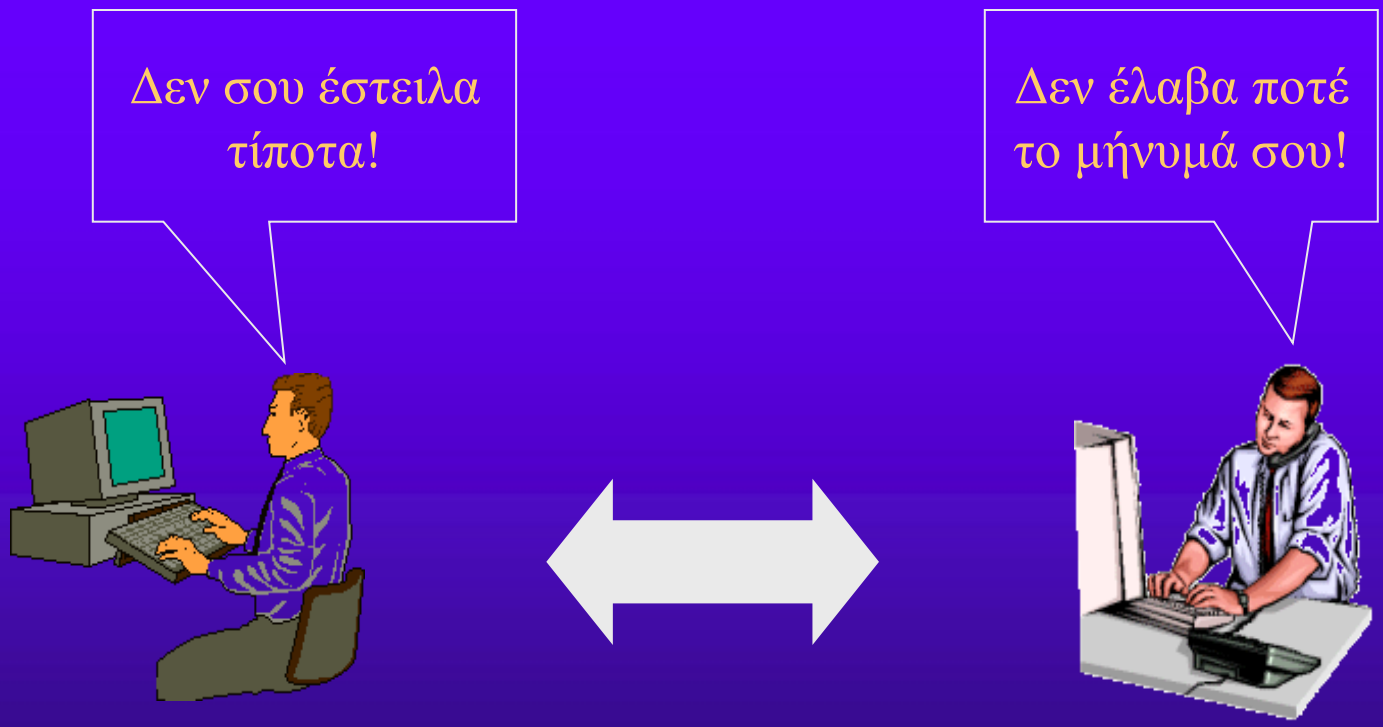
Ψηφιακή Υπογραφή: Μέσο προστασίας από τις απειλές (1/4)



Παρεχόμενη υπηρεσία:

Ακεραιότητα

Ψηφιακή Υπογραφή: Μέσο προστασίας από τις απειλές (2/4)



Παρεχόμενη υπηρεσία:

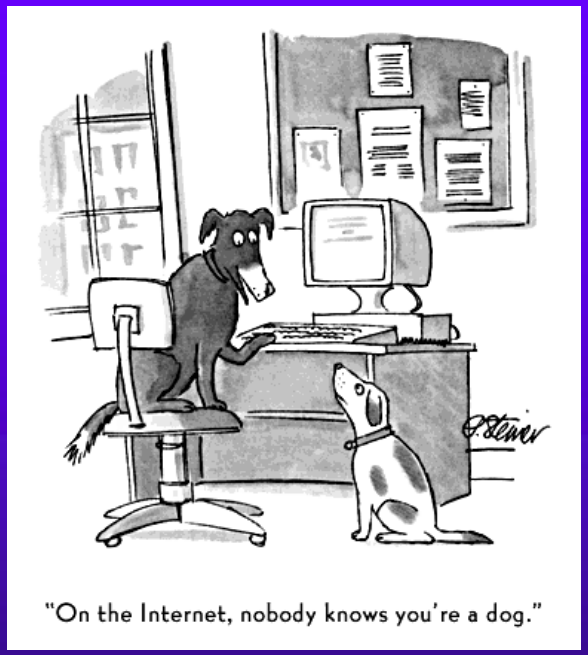
Μη αποποίηση αποστολής ή λήψης

Ψηφιακή Υπογραφή: Μέσο προστασίας από τις απειλές (3/4)

Παρεχόμενη υπηρεσία:

Ασφαλής χρονοσήμανση

Ψηφιακή Υπογραφή: Μέσο προστασίας από τις απειλές (4/4)



Παρεχόμενη υπηρεσία:

Ταυτοποίηση εμπλεκομένων

Ψηφιακή vs. Ιδιόχειρη υπογραφή

Ιδιόχειρη υπογραφή	Ψηφιακή υπογραφή
Ενσωματωμένη στο μήνυμα με φυσικό τρόπο	Εξωτερικό ή συνημμένο «αντικείμενο» το οποίο συνδέεται με το μήνυμα
Για όλα τα έγγραφα χρησιμοποιείται η ίδια υπογραφή	Διαφορετικές υπογραφές για διαφορετικά έγγραφα
Περιορισμένη δυσκολία πλαστογράφησης	Πολύ μεγάλη δυσκολία πλαστογράφησης
Πιστοποιεί την ταυτότητα του υπογράφοντος	Πιστοποιεί την ακεραιότητα του περιεχομένου της πληροφορίας και την ταυτότητα του υπογράφοντος
Άμεσα ορατή και οπτικά αναγνωρίσιμη	Μη άμεσα αναγνώσιμα δεδομένα
Ο «μηχανισμός» δημιουργίας της παραμένει ο ίδιος και δεν μπορεί να αποσυρθεί	Ο μηχανισμός δημιουργίας της μπορεί να ανακληθεί και να υποκατασταθεί από κάποιον εντελώς διαφορετικό

Κρυπτογραφία Δημόσιου Κλειδιού: Ισχυρά σημεία

- Τα δημόσια κλειδιά **δεν** χρήζουν προστασίας
- Τα ιδιωτικά κλειδιά **δεν** χρειάζεται να διανεμηθούν/γνωστοποιηθούν σε τρίτους
- Η διαχείριση κλειδιών **ελαχιστοποιείται** (παράγονται από τους ίδιους τους χρήστες)
- Ο κύκλος ζωής των κλειδιών είναι **μεγάλος**
- Υπάρχει δυνατότητα **επαλήθευσης** της ακεραιότητας των δεδομένων

Κρυπτογραφία Δημόσιου Κλειδιού: Αδυναμίες και ελλείψεις

- Πώς επαληθεύεται η ταυτότητα του κατόχου ενός ζεύγους κλειδιών;
- Πώς διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία και τη χρήση τους;
- Πώς διανέμονται στο κοινό τα δημόσια κλειδιά έτσι ώστε να συνδέονται μόνο με μία φυσική οντότητα;
- Πώς ολοκληρώνεται ο κύκλος ζωής τους, όταν αυτό κριθεί αναγκαίο;

Υπάρχει ανάγκη δημιουργίας Έμπιστης Τρίτης Οντότητας που διαχειρίζεται τον κύκλο ζωής των κλειδιών και την αντιστοίχησή τους με φυσικές οντότητες

Ελληνική Νομοθεσία (Π.Δ. 150/2001)

- Ψηφιακό Πιστοποιητικό:

  Ηλεκτρονική βεβαίωση που συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του

- Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ):
  Φυσικό ή νομικό πρόσωπο ή άλλος φορέας που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές

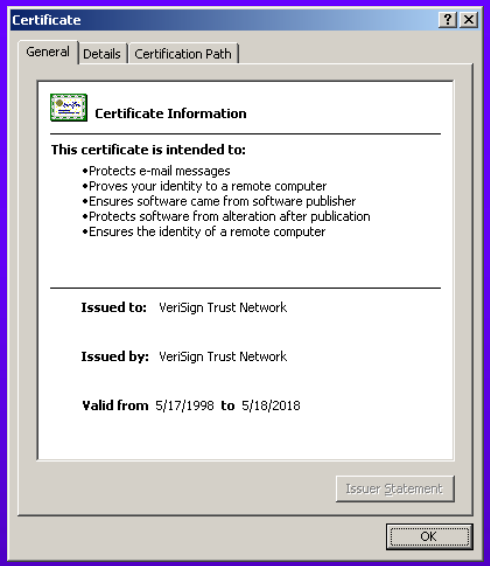
Ψηφιακό Πιστοποιητικό

1. Στοιχεία Υποκειμένου
2. Στοιχεία Εκδότη
3. Διάρκεια ισχύος
4. Δημόσιο Κλειδί Υποκειμένου
5. (Άλλα μετα-δεδομένα)

Ψηφιακή Υπογραφή Εκδότη

Γιατί Ψηφιακά Πιστοποιητικά;

- Δημιουργούν **σχέσεις εμπιστοσύνης** μεταξύ οντοτήτων που δεν γνωρίζονται
- Μπορούν να χρησιμοποιούνται **off-line**
- Αποτελούν **κλιμακώσιμο** σχήμα
- Μπορούν να περιέχουν **επιπλέον στοιχεία**, που επιβεβαιώνει τρίτος εγγυητής, για χρήση σε διάφορες εφαρμογές (πχ. χρονοσήμανση, δικαιώματα πρόσβασης σε πόρους κλπ.)



Αναγνωρισμένα Πιστοποιητικά

- Μονοσήμαντος προσδιορισμός ταυτότητας Παρόχου
- Μονοσήμαντος προσδιορισμός ταυτότητας Υποκειμένου
- Προσδοκώμενη χρήση
- Δεδομένα επαλήθευσης της υπογραφής (πχ. Δημόσιο κλειδί) που αντιστοιχούν στο υποκείμενο
- Περίοδος ισχύος
- Κωδικός αναγνώρισης Πιστοποιητικού
- Ηλεκτρονική υπογραφή Παρόχου
- Περιορισμοί στη χρήση και ευθύνες Παρόχου
- Επεκτάσεις κατά περίπτωση εφαρμογής

Απαιτήσεις έκδοσης αναγνωρισμένων πιστοποιητικών

- Επίδειξη απαραίτητης **αξιοπιστίας**
- Διασφάλιση **μηχανισμών** έκδοσης, δημοσίευσης και ανάκλησης πιστοποιητικών
- **Αδιαμφισβήτητη επαλήθευση** ταυτότητας πιστοποιούμενης οντότητας
- Απασχόληση κατάλληλα **εκπαιδευμένου προσωπικού**
- Χρήση **αξιόπιστων** Πληροφοριακών Συστημάτων
- **Προστασία δεδομένων** δημιουργίας υπογραφής του ΠΥΠ
- Τήρηση **ημερολογίου πράξεων**
- Δημοσίευση **Πολιτικών, Πρακτικών και Συνθηκών**
- Διασφάλιση επαρκών οικονομικών, υλικών και ανθρώπινων **πόρων**
- **Φυσική ασφάλεια**

Προστασία Κλειδιού Δημιουργίας Ψηφιακής Υπογραφής: Έξυπνες κάρτες

- Απαιτείται **ειδικό υλικό** και διεπαφές
- Εξαιρετικά **δύσκολη αντιγραφή**
- **Προστασία** ανάγνωσης/τροποποίησης περιεχομένου
- Μεγάλη **αξιοπιστία** και μηχανική αντοχή
- Εύκολα **μεταφέρσιμη**
- Εκτέλεση λειτουργιών **μέσα** στην κάρτα

Ελληνική Νομοθεσία (Π.Δ. 150/2001)

- Ασφαλής Διάταξη Δημιουργίας Υπογραφής: Διατεταγμένο υλικό ή λογισμικό για δημιουργία ηλεκτρονικής υπογραφής
- Πληροί συγκεκριμένους όρους:
  - Μοναδικότητα δεδομένων δημιουργίας υπογραφής
  - Διασφάλιση απορρήτου
  - Προστασία κατά της χρήσης από τρίτους

Ψηφιακές Υπογραφές: Νομικό πλαίσιο

- **Διεθνής αναγνώριση** των ψηφιακών υπογραφών: Ισότιμες με τις χειρόγραφες (ενίοτε ισχυρότερες)
- **Ευρωπαϊκή Οδηγία EC/93/99** (ηλεκτρονικές υπογραφές): Έχει υιοθετηθεί από όλα τα κράτη-μέλη (στην Ελλάδα υιοθετήθηκε με το Π.Δ. 150/2001)
- **ΕΕΤΤ** απόφαση 248/71 (ΦΕΚ 603/Β'/16-5-2002): Ρυθμίζει τη διαπίστευση των ΠΥΠ και την έκδοση αναγνωρισμένων πιστοποιητικών
- **Π.Δ. 342/2002**: Προσδιορίζει όρους διακίνησης ψηφιακά υπογεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου στις επικοινωνίες του δημόσιου τομέα

Ψηφιακή Υπογραφή και η-Τιμολόγιο

1. **Διασφάλιση της ταυτότητας** του εκδότη του παραστατικού
2. **Ακεραιότητα περιεχομένου** και εξασφάλιση ότι το ηλεκτρονικό παραστατικό **δεν έχει αλλοιωθεί**
3. **Αδυναμία άρνησης** (μη αποποίηση) της έκδοσης του παραστατικού
4. Το περιεχόμενο του παραστατικού μπορεί να **αναγνωσθεί απο άνθρωπο**

Αντί συμπερασμάτων

Η ψηφιακή υπογραφή παρέχει σημαντικές **νέες δυνατότητες**

Η χρήση της ψηφιακής υπογραφής **δεν είναι πολύπλοκη**

Η χρήση της ψηφιακής υπογραφής **δεν απαιτεί ειδικές γνώσεις**

Η αξιοποίηση της ψηφιακής υπογραφής **δεν απαιτεί υψηλές επενδύσεις**

Το υπάρχον θεσμικό πλαίσιο είναι **σαφές και επαρκές**

Η αξιοποίση της ψηφιακής υπογραφής χρειάζεται **μεθοδικό-τητα και συστηματικότητα**

References

1. Buchmann J., Karatsiolis E., Wiesmaier A., *Introduction to Public Key Infrastructure: Concepts, Standards, and Deployment Considerations*, Springer, 2013.
2. Katz J., *Digital Signatures*, Springer, 2010.
3. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security*, pp. 93-103, Springer (LNCS 6983), 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructures*, Vol. 9, No. 1-2, pp. 93-110, 2013.
5. Lekkas D., Gritzalis D., Cumulative Notarization for Long-term Preservation of Digital Signatures, *Computers & Security*, Vol. 23, no. 5, pp. 413-424, 2004.
6. Lekkas D., Gritzalis D., "Long-term verifiability of healthcare records authenticity", *International Journal of Medical Informatics*, Vol. 76, Issue 5-6, pp. 442-448, 2006.
7. Lekkas D., Gritzalis D., "e-Passports as a means towards a globally interoperable Public Key Infrastructure", *Journal of Computer Security*, Vol. 18, No. 3, pp. 379-396, 2010.
8. Lekkas D., Gritzalis D., "e-Passports as a means towards the first world-wide Public Key Infrastructure", in *Proc. of the 4th European PKI Workshop*, pp. 34-48, Springer (LNCS 4582), Spain, 2007.
9. Mylonas A., Meletiadis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security*, Vol. 38, pp. 51-75, 2013.
10. Theoharidou M., Mylonas A., Gritzalis D., "A risk assessment method for smartphones", in *Proc. of the 27th IFIP International Information Security and Privacy Conference*, pp. 428-440, Springer (AICT 267), Greece, 2012.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, 2009.