ΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΠΡΟΓΡΑΜΜΑΤΟΣ ΕΚΠΑΙΔΕΥΣΗΣ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

ΕΜΜΑΝΟΥΗΛ ΚΥΡ. ΜΙΡΤΖΑΝΗΣ

Μαθηματικός – Msc Πληροφορικής
Καθηγητής Πληροφορικής

Online Παρουσίαση για τους καθηγητές ΜΕ

www.it-seminars.com

ΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΠΡΟΓΡΑΜΜΑΤΟΣ ΕΚΠΑΙΔΕΥΣΗΣ ΓΙΑ ΤΗΝ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

ΕΚΠΑΙΔΕΥΤΙΚΟΙ ΣΤΟΧΟΙ ΠΡΟΓΡΑΜΜΑΤΟΣ

- ΥΠΟΒΟΛΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΣΕ Η-ΕΓΓΡΑΦΟ ΚΑΙ Η-ΜΗΝΥΜΑ
- ΕΛΕΓΧΟΣ ΝΟΜΙΜΟΤΗΤΑΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΣΕ ΕΙΣΕΡΧΟΜΕΝΑ
- ΣΥΝΕΙΔΗΣΗ ΓΕΝΙΚΟΥ ΠΛΑΙΣΙΟΥ (ΝΟΜΙΚΟΥ-ΘΕΣΜΙΚΟΥ-ΤΕΧΝΟΛΟΓΙΚΟΥ)
- ΣΥΝΕΙΔΗΣΗ ΣΥΝΑΦΩΝ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Εισαγωγή – Τεχνολογικό Πλαίσιο

- Κρυπτογραφία – κρυπταλγόριθμος **ασύμμετρου κλειδιού RSA** - Αλγόριθμος δημιουργίας **ψηφιακής σύνοψης** του η-κειμένου **και** αλγόριθμος **κρυπτογράφησής** της με το **Ιδιωτικό κλειδί** (ψηφιακή υπογραφή). Υπάρχουν 2 κλειδιά: **Ιδιωτικό κλειδί και Δημόσιο κλειδί**
  (**R**on Rivest, Adi **S**hamir Len **A**dleman – 1977 - Public Key Infrastructure)

- Η προηγμένη ηλεκτρονική υπογραφή **δεν έχει εικόνα** , είναι μία μη ορατή σε εμάς **αλγοριθμική ψηφιακή σύνοψη του ηλεκτρονικού κειμένου** που υπογράφουμε, η οποία **κρυπτογραφείται** (αυτή είναι η υπογραφή) και συνδέεται με το η-έγγραφο (ή η-μήνυμα) και με το πιστοποιητικό μας (ψηφιακή ταυτότητα) με “άρρηκτο” και μονοσήμαντο τρόπο.
  Η προηγμένη ηλεκτρονική υπογραφή μας **δεν είναι ποτέ η ίδια**, εκτός αν αφορά το ίδιο η-έγγραφο.

Εισαγωγή – Ασφάλεια Ι

Το ψηφιακά υπογεγραμμένο η-έγγραφο αποστέλλεται στον παραλήπτη μαζί με το ψηφιακό του πιστοποιητικό (ψηφιακή ταυτότητα του υπογράφοντος) και όλες τις απαραίτητες πληροφορίες για τον αναγκαίο έλεγχο!

▪

Το ίδιο ισχύει για **ΚΑΘΕ** ψηφιακή υπογραφή, αν το **ΙΔΙΟ** η-έγγραφο έχει υπογραφεί από περισσότερους!

Εισαγωγή – Ασφάλεια II

- Αποδεικνύεται η **αυθεντικότητα** (**ταυτότητα** του υπογράφοντος) ενός ψηφιακού εγγράφου ή ηλεκτρονικού μηνύματος (email) (Πώς ;;;)
- Ελέγχεται η **ακεραιότητα** του η-εγγράφου ή του η-μηνύματος (email) **από ενδεχόμενη προσπάθεια παραποίησης** (Πώς ;;;)
- Δίνει την δυνατότητα **κρυπτογράφησης** σε η-έγγραφα και η-μηνύματα, το περιεχόμενο των οποίων δεν πρέπει να είναι προσβάσιμο από τρίτους παρά μόνο από τον αρμόδιο παραλήπτη (**εμπιστευτικότητα**) (Πώς ;;;)

Εισαγωγή – Ασφάλεια II

(συνέχεια)

- Ο χρόνος υποβολής της προηγμένης ηλεκτρονικής υπογραφής μπορεί να είναι **ασφαλής (αντικειμενικός)**, δηλαδή από πιστοποιημένο Ηλεκτρονικό Υπολογιστή - Διακομιστή του Παρόχου Υπηρεσιών Πιστοποίησης **και όχι από εκείνον του υπογράφοντος ! (χρονοσήμανση ή χρονοσφραγίδα)**.

Εισαγωγή – Ασφάλεια III

Attacks (Book Understanding Cryptography p. 194)

"There have been numerous attacks proposed against RSA since it was invented in 1977. None of the attacks are serious, and moreover, they typically exploit weaknesses in the way RSA is implemented or used rather than the RSA algorithm itself."

Εισαγωγή – Νομικό Πλαίσιο

- **Ευρωπαϊκή Οδηγία 99/93/ΕΚ,**
  σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές
- **ΠΔ 150/2001, άρθρο 3 παράγραφος 1**
  (προηγμένη ηλεκτρονική υπογραφή + αναγνωρισμένο πιστοποιητικό + ΑΔΔΥ –> Νομική Ισχύ Ιδιόχειρης Υπογραφής - Ιδιότητα ΜΗ ΑΠΟΠΟΙΗΣΗΣ)

- **ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ 910/2014 ΕΚ,** κατάργηση της οδηγίας 1999/93/ΕΚ
- **Νόμος 4440/2016 άρθρο 24** (αντικαθιστά το άρθρο 12 του ν. 3979/2011)
  (εγκεκριμένη ηλεκτρονική υπογραφή + εγκεκριμένη χρονοσφραγίδα - χρονοσήμανση)

ΑΝΑΓΚΑΙΟΤΗΤΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

Πότε είναι αναγκαία η υποβολή ψηφιακής υπογραφής σε ηλεκτρονικά έγγραφα και μηνύματα;

SMART CARD–USB TOKEN (ΑΔΔΥ)

- Τί είναι το Usb Token;
- Πώς εγκαθίστανται τα ψηφιακά πιστοποιητικά (ψηφιακές ταυτότητες) σε αυτό;

- Τι περιέχει ;
- Πώς διαχειριζόμαστε το περιεχόμενο του και τι μπορούμε να δούμε;

- Τι γίνεται αν το χάσουμε ή αν κλαπεί;

ΔΟΜΗ ΑΝΑΓΝΩΡΙΣΜΕΝΟΥ (ΕΓΚΕΚΡΙΜΕΝΟΥ) ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ (ΨΗΦΙΑΚΗΣ ΤΑΥΤΟΤΗΤΑΣ)

- Τι περιέχει το πιστοποιητικό;
- Μπορεί το πρόγραμμα που εμφανίζει το η-έγγραφο ή το e-mail να το διαβάσει;
- Είναι αναγκαίο να γνωρίζουμε την ανάγνωσή του και γιατί;

ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

- Πάροχοι Υπηρεσιών Πιστοποίησης (ΠΥΠ)
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)
  (ΠΔ 150/2001, Νόμος 3431/2006)
- Ευρωπαϊκή ένωση (ΕΕ)

ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (ΑΠΕΔ) – ΠΥΛΗ ΕΡΜΗΣ

- Διαδικασία έκδοσης Πιστοποιητικών
  ΠΥΛΗ ΕΡΜΗΣ – ΚΕΠ (γιατί;) (αίτηση)

- ERMIS REPOSITORY (γιατί;)
  (Κανονισμός – Πιστοποιητικά ΑΠΕΔ -
  Αναζήτηση Πιστοποιητικών Χρηστών ΑΠΕΔ)

- ΠΥΛΗ ΕΡΜΗΣ (Έκδοση Ψηφιακών Πιστοποιητικών -
  Ανάκληση - Ανανέωση)

ΥΠΟΒΟΛΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

- Σε ψηφιακό έγγραφο PDF (doc;)
- Σε εξερχόμενο e-mail (γιατί;)
- Κρυπτογράφηση εξερχόμενου e-mail (πότε; πώς;)

ΕΛΕΓΧΟΣ ΥΠΑΡΞΗΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ - ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

- Σε εισερχόμενο ψηφιακό έγγραφο PDF (γιατί; πώς;)
- Σε εισερχόμενο e-mail (γιατί; πώς;)
- Κρυπτογράφησης σε εισερχόμενο PDF, e-mail (με ποιές προυποθέσεις ανοίγει;)

ΕΛΕΓΧΟΣ ΝΟΜΙΜΟΤΗΤΑΣ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

- Σε εισερχόμενο ψηφιακό έγγραφο PDF (γιατί; πώς;)
- Αντιπαράδειγμα ελέγχου ψηφιακής υπογραφής PDF νόμου 3979/2011 **(ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ)**
- Σε εισερχόμενο e-mail (γιατί; πώς;)

ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΓΙΑ

ΤΗ ΠΡΟΣΟΧΗ ΣΑΣ

Μιρτζάνης Κυρ. Εμμανουήλ