ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

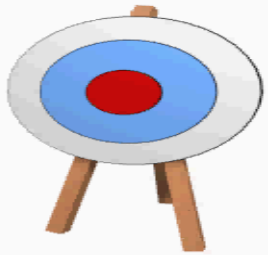
ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ
Τομέας Νέων Τεχνολογιών

«ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΠΟΛΙΤΕΣ»

ΑΣΦΑΛΕΙΑ – ΚΡΥΠΤΟΓΡΑΦΗΣΗ – ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Εισηγητής: Καπλάνογλου Λάζαρος

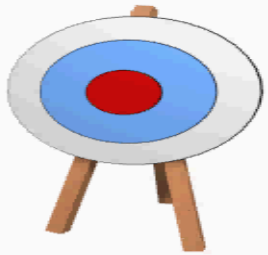
ΣΤΟΧΟΙ ΤΗΣ ΕΝΟΤΗΤΑΣ (1/2)



Με την ολοκλήρωση της ενότητας οι επιμορφούμενοι θα είναι σε θέση να:

- Διακρίνουν τις βασικές απειλές που αντιμετωπίζουν τα δίκτυα των υπολογιστών και αφορούν στην ακεραιότητα της πληροφορίας και τις ηλεκτρονικές συναλλαγές.
- Αναλύουν τα είδη των κινδύνων και τους τρόπους αντιμετώπισης τους
- Προσδιορίζουν τις αρχές της κρυπτογραφίας και τις εφαρμογές της στην επίτευξη ασφαλών επικοινωνιών.

ΣΤΟΧΟΙ ΤΗΣ ΕΝΟΤΗΤΑΣ (2/2)

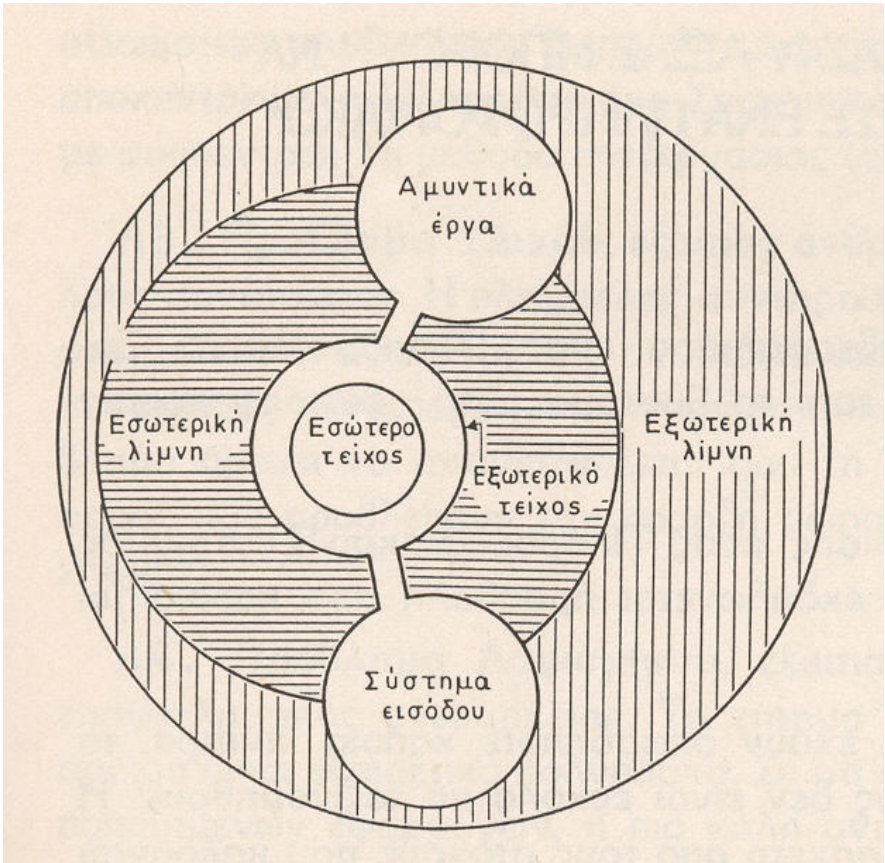


Με την ολοκλήρωση της ενότητας οι επιμορφούμενοι θα είναι σε θέση να:

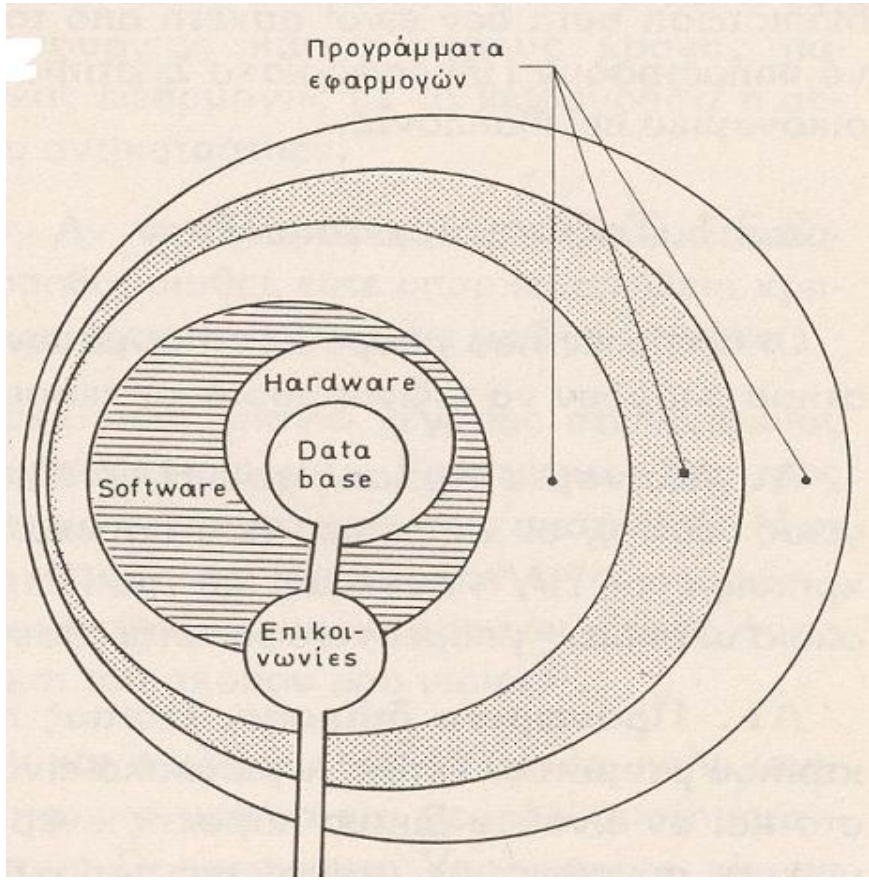
- Περιγράφουν τη διαδικασία απόκτησης ψηφιακών πιστοποιητικών και ψηφιακών υπογραφών.
- Αναλύουν τα οφέλη από τη χρήση των ψηφιακών υπογραφών.
- Χρησιμοποιούν ψηφιακές υπογραφές στη δημιουργία ψηφιακών εγγράφων και αποστολή ηλεκτρονικής αλληλογραφίας.

ΜΕΣΑΙΩΝΙΚΟ ΚΑΣΤΡΟ vs ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ

Μεσαιωνικό Κάστρο

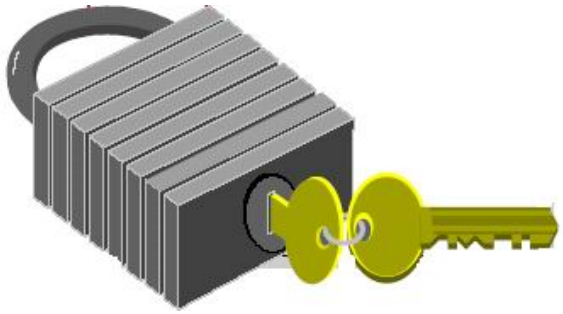


Πληροφοριακό Σύστημα



ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η προστασία πόρων (δεδομένων και προγραμμάτων) από συμπτωματική ή κακόβουλη τροποποίηση, καταστροφή ή διαρροή.



ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

- ***Εμπιστευτικότητα (confidentiality):***

  Οι πληροφορίες είναι προσπελάσιμες μόνο από εξουσιοδοτημένους χρήστες

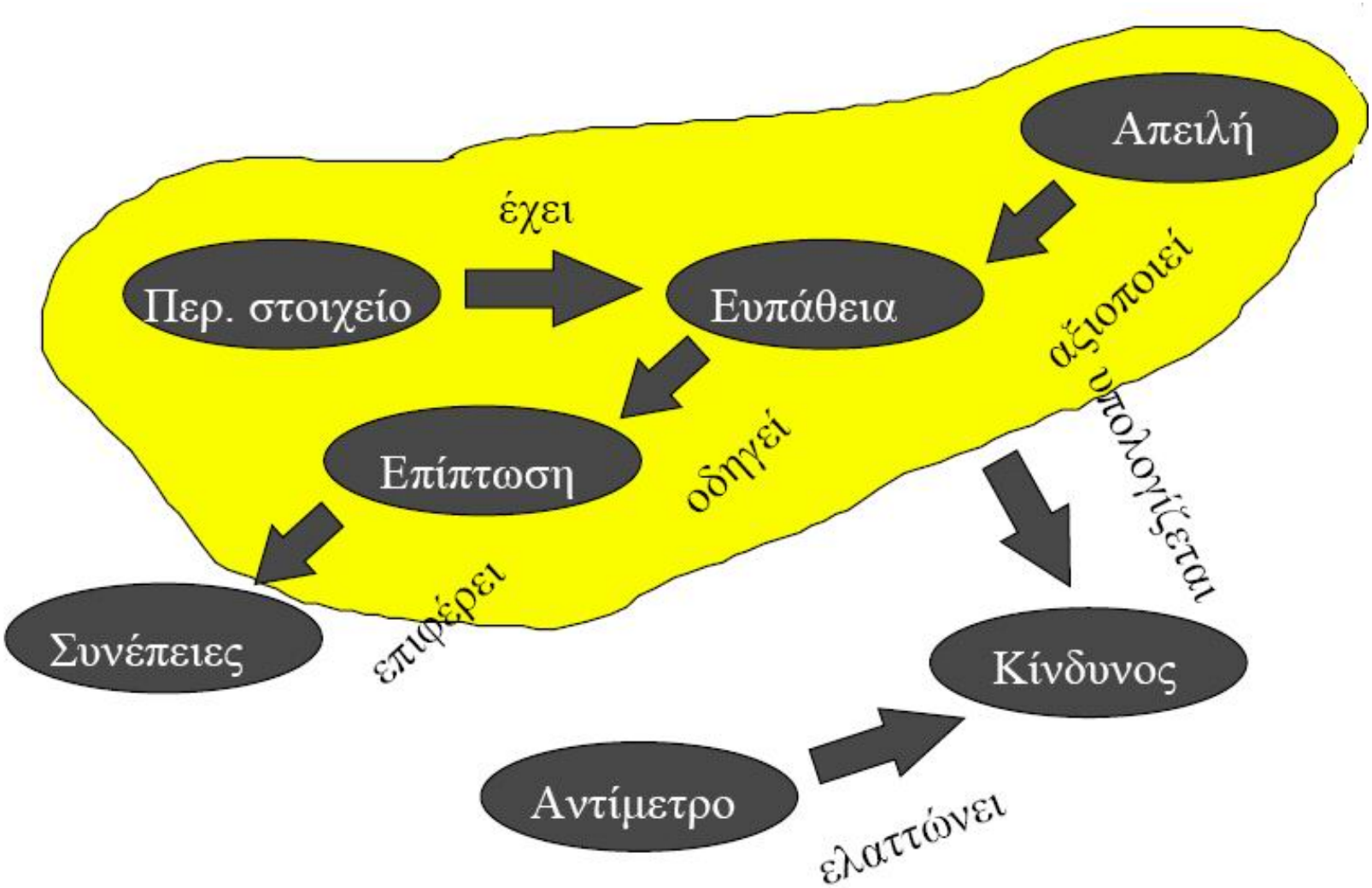
- ***Ακεραιότητα (integrity):***

  Τα δεδομένα και τα προγράμματα τροποποιούνται και καταστρέφονται μόνο με καλά καθορισμένους τρόπους και με κατάλληλη εξουσιοδότηση

- ***Διαθεσιμότητα (availability):***

  Οι εξουσιοδοτημένοι χρήστες θα μπορούν να χρησιμοποιήσουν δεδομένα, προγράμματα και υπηρεσίες όταν το επιθυμήσουν

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (1)

- **Ιοί**

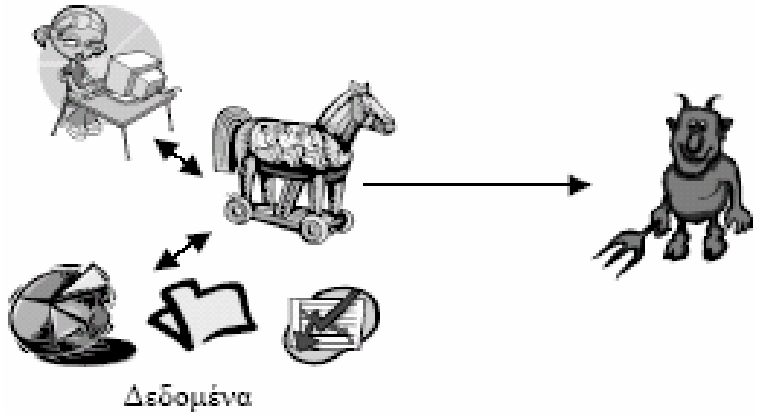
  Προγράμματα που «μολύνουν» άλλα προγράμματα, ενσωματώνοντας σ' αυτά – πιθανώς εξελιγμένα - αντίγραφα του εαυτού τους

  - ✓ Βλάβες: διαγραφή/αλλοίωση αρχείων, υποβάθμιση απόδοσης, κατανάλωση χώρου, ενόχληση
  - ✓ Βασικοί τρόποι διάδοσης: τομείς εκκίνησης, εκτέλεση μολυσμένου προγράμματος, εκτέλεση δικτυακής εφαρμογής, άνοιγμα «παραλλαγμένου» συνημμένου αρχείου, χρήση διαμοιρασμένου πόρου κλπ

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (2)

- **Δούρειοι Ίπποι**

  Πρόγραμμα ή μέρος κώδικα υπολογιστή κρυμμένο σε άλλο πρόγραμμα το οποίο εκτελεί μία παράνομη ενέργεια.



- ✓ Προγράμματα υποκλοπής διευθύνσεων, συνθηματικών, στοιχείων του υπολογιστή
- ✓ Κάθε πρόγραμμα είναι τόσο «ύποπτο» όσο ο συγγραφέας του ή το δίκτυο διανομής του

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (3)

- **Αντιποίηση ή μεταμφίεση (spoofing)**

  Ο χρήστης πιστεύει ότι αλληλεπιδρά με το επιθυμητό σύστημα, εφαρμογή ή δικτυακό τόπο ενώ στην πραγματικότητα συνδέεται σε κάποιο άλλο

  - ✓ Υποκλοπείς συνθηματικών, στοιχείων πιστωτικών καρτών κλπ
  - ✓ Παραφθαρμένα ονόματα δικτυακών τόπων

    https://www.amason.com
  - ✓ Πλαστές δικτυακές διευθύνσεις

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (4)

- **Cookies**
  - Τα COOKIES περιέχουν πληροφορίες σχετικά με το WEB SITE που επισκεφθήκαμε και βρίσκονται στο σκληρό μας δίσκο του PC μας σαν .TXT FILES
  - Αποσκοπούν στην αναγνώρισή μας από τα ίδια Web sites την επόμενη φορά που θα βρεθούμε στις ιστοσελίδες τους.
  - Θέματα περί προσωπικών δεδομένων και του προσωπικού απορρήτου

    Μη αποδοχή εγκατάστασης

    Διαγραφή

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (5)

- **Spam mail**
  - Απρόκλητη, εμπορική και μαζική αποστολή μεγάλου αριθμού μηνυμάτων, τα οποία απευθύνονται σ' ένα σύνολο χρηστών του Internet, χωρίς αυτοί να έχουν ζητήσει ή να επιθυμούν
  - Προσβολή ακόμη και κατά την απλή πρόσβαση σε ιστοσελίδες (π.χ. Active-X)

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (6)

- **Παρεμπόδιση παροχής υπηρεσιών**

  Υποβάθμιση απόδοσης ή ολική αποτροπή της πρόσβασης των εξουσιοδοτημένων χρηστών

Π.χ. Ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου μπορεί να καταστεί «άχρηστος» αν του ανατεθεί να διακινήσει 5000 μηνύματα των 200 Mbytes έκαστο, καθώς σίγουρα θα εξαντληθεί ο αποθηκευτικός του χώρος. ή

Εάν ένας εξυπηρέτητης WWW θα είναι επίσης «άχρηστος» αν «βομβαρδισθεί» με δυσανάλογο προς τις προδιαγραφές του αριθμό αιτήσεων.

Η παρεμπόδιση παροχής υπηρεσιών αποσκοπεί στη στέρηση από τους νόμιμους χρήστες της δυνατότητάς τους να εξυπηρετηθούν από το υπολογιστικό σύστημα.

ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ (7)

- **Μη ηθελημένη καταστροφή**

  Εξουσιοδοτημένοι χρήστες πραγματοποιούν ατυχείς ενέργειες

  ✓ π.χ. να διαγράψει ένα (χρήσιμο) αρχείο ή να σβήσει ένα σύνολο εγγραφών από μια βάση δεδομένων.

  ✓ Ως ενέργειες που υποβαθμίζουν την αξία του συστήματος τα περιστατικά αυτά πρέπει να καλύπτονται από τους μηχανισμούς ασφάλειας.

  ✓ Μολονότι προφανώς δεν είναι δυνατόν να στερήσουμε από τους χρήστες τα βασικά τους προνόμια για να αποτραπούν οι ατυχείς ενέργειες, θα πρέπει στο σχέδιο ασφάλειας να μεριμνούμε για μεθόδους αντιμετώπισης των περιστατικών αυτών

ΑΝΤΙΜΕΤΡΑ

- Εφαρμογή Σχεδίου Ασφαλείας
- Χρήση Firewall
- Intrusion Detection systems
- Ενημέρωση νέων εκδόσεων του λογισμικού συστήματος (λειτουργικό, βάση δεδομένων)
- Antivirus λογισμικό
- Honey - Pots

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ - ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

- **Νόμος 2472/97**:Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα (ΦΕΚ50, Τεύχος Α', 10-4-1997)

- **Νόμος 2774/99**:Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα (ΦΕΚ 287, Τεύχος Α', 22-12-1999)

ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- **Δεδομένα προσωπικού χαρακτήρα**

  Κάθε πληροφορία που αναφέρεται στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.

Η **επεξεργασία** τους επιτρέπεται υπό προϋποθέσεις

ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- **Ευαίσθητα Δεδομένα**

- ✓ Φυλετική ή εθνική προέλευση
- ✓ Πολιτικά φρονήματα
- ✓ Θρησκευτικές πεποιθήσεις
- ✓ Φιλοσοφικές πεποιθήσεις
- ✓ Κοινωνική πρόνοια
- ✓ Ερωτική ζωή
- ✓ Ποινικές διώξεις ή καταδίκες
- ✓ Συμμετοχή σε ένωση σωματείο
- ✓ Υγεία

Η **επεξεργασία** τους, <u>γενικά, απαγορεύεται</u>

ΑΝΑΓΝΩΡΙΣΗ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

- Το νομικό πλαίσιο και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.
  - ✓ Διαφύλαξη προσωπικών δεδομένων
  - ✓ Διαφύλαξη δεδομένων του οργανισμού
  - ✓ Δικαιώματα πνευματικής ιδιοκτησίας
- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός

ΑΠΟΤΙΜΗΣΗ ΚΙΝΔΥΝΩΝ (Risk Assessment)

Η αποτίμηση κινδύνων είναι μια συστηματική εξέταση των ακόλουθων παραγόντων:

- ✓ Της ζημιάς που θα υποστεί ο οργανισμός στην περίπτωση που εμφανιστεί ένας κίνδυνος ασφάλειας,

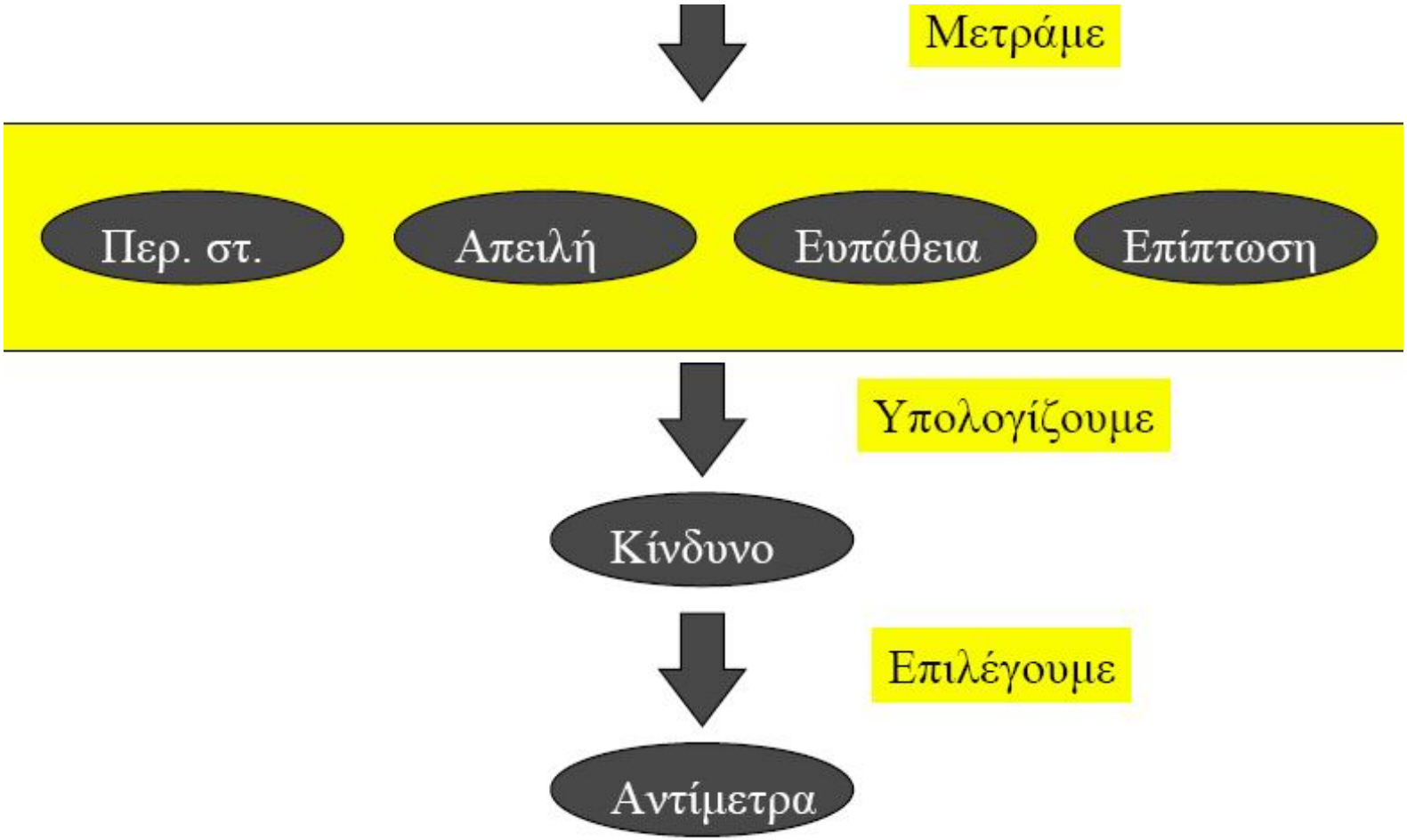
- ✓ Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφάλειας

ΑΣΦΑΛΕΙΑ ή ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ

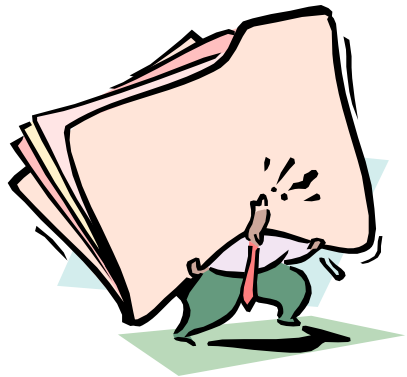
Υπάρχει 100% ασφαλές σύστημα;

- Η εφαρμογή μέσων προστασίας έχει κόστος
- Τα αγαθά έχουν αξία
- Το κόστος προστασίας οφείλει να είναι ανάλογο της προστατευόμενης αξίας
- Το κόστος παραβίασης πρέπει να είναι υψηλότερο του οφέλους του εισβολέα από την παραβίαση

ΑΣΦΑΛΕΙΑ ή ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ



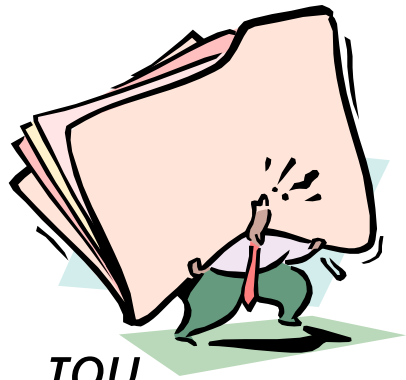
ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ (1)



- Το σχέδιο ασφάλειας (security plan) είναι το έγγραφο, στο οποίο περιγράφονται οι απαιτήσεις ασφάλειας ενός οργανισμού ή μιας επιχείρησης, οι απαραίτητες ενέργειες για την υλοποίησή τους, καθώς και τα αναγκαία διοικητικά και οργανωτικά μέτρα

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ (2)

- Οι βασικοί άξονες του Σχεδίου Ασφάλειας



- ✓ *Οργάνωση και διαχείριση της ασφάλειας του πληροφοριακού συστήματος*
- ✓ *Ασφάλεια ανάπτυξης και συντήρησης του πληροφοριακού συστήματος*
- ✓ *Φυσική ασφάλεια*
- ✓ *Ασφάλεια δεδομένων*
- ✓ *Ασφάλεια της υπολογιστικής και τηλεπικοινωνιακής υποδομής*
- ✓ *Ανάκαμψη από καταστροφές*

ΒΑΣΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ (1/2)

Οι δύο βασικοί μηχανισμοί προστασίας είναι:

- ΔΙΑΚΡΙΒΩΣΗ ΤΑΥΤΟΤΗΤΑΣ, προκειμένου να εξασφαλίζεται ότι ο χρήστης που παρουσιάζεται με κάποια ταυτότητα όντως είναι αυτός. Ζητείται κάτι που ο χρήστης
  - Γνωρίζει (ένα μυστικό, ένα συνθηματικό, ένας προσωπικός αριθμός αναγνώρισης ή ένα κρυπτογραφικό κλειδί)
  - Κατέχει (έξυπνη κάρτα, μία κάρτα αυτόματων ταμειακών συναλλαγών κλπ.)
  - Είναι δηλ. βιομετρικό χαρακτηριστικό (δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.)

ΜΗΧΑΝΙΣΜΟΙ ΠΡΟΣΤΑΣΙΑΣ (2/2)

- ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ που χρησιμοποιείται για να επιτρέψει σε ένα χρήστη (διακριβωμένο πια) να προσπελάσει μόνο τα αντικείμενα και τις υπηρεσίες για τα οποία είναι εξουσιοδοτημένος. (Διαχείριση δικαιοδοσιών πρόσβασης)

ΒΑΣΙΚΟΙ ΠΑΡΑΓΟΝΤΕΣ ΕΠΙΤΥΧΙΑΣ (1)

- ✓ Πολιτική ασφάλειας που αντικατοπτρίζει τους στόχους του οργανισμού.
- ✓ Διαδικασίες ασφάλειας συμβατές με την κουλτούρα του οργανισμού
- ✓ Ενεργή υποστήριξη από τη διοίκηση του οργανισμού.
- ✓ Κατανόηση των απαιτήσεων & της αποτίμησης κινδύνων ασφαλείας

ΒΑΣΙΚΟΙ ΠΑΡΑΓΟΝΤΕΣ ΕΠΙΤΥΧΙΑΣ (2)

- ✓ Κατανόηση από όλο το προσωπικό του οργανισμού της αναγκαιότητας (δημιουργία κουλτούρας ασφάλειας)
- ✓ Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό.
- ✓ Εκπαίδευση και επιμόρφωση του προσωπικού.
- ✓ Κατανοητό και ισορροπημένο σύστημα μέτρησης της απόδοσης του συστήματος ασφάλειας

ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

- Η έκρηξη των τεχνολογιών Internet έχει οδηγήσει στα **εξωστρεφή πληροφοριακά** συστήματα και στις **ηλεκτρονικές συναλλαγές**

- **Ζητούμενο**: η **ασφάλεια στην επικοινωνία** μεταξύ υπολογιστικών συστημάτων που χρησιμοποιούνται ως μέσο συλλογικής εργασίας που μπορεί:
  - να ανήκουν σε διαφορετικούς οργανισμούς,
  - να αφορούν μεγάλο αριθμό ατόμων με ενδεχομένως συγκρουόμενες επιδιώξεις και συμφέροντα, και που πιθανώς
  - δεν γνωρίζονται μεταξύ τους πριν την εγκαθίδρυση της επικοινωνιακής οδού

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

- Για να επιτευχθούν **ασφαλείς ηλεκτρονικές συναλλαγές**, θα πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις:
  - **Εμπιστευτικότητα (Confidentiality)**
  - **Ακεραιότητα (Integrity)**
  - **Διαθεσιμότητα (Availability)**
  - **Αυθεντικότητα ή Πιστοποίηση (Authentication)**
  - **Μη αποποίηση της ευθύνης (Non Reputation)**

ΑΥΘΕΝΤΙΚΟΤΗΤΑ

- Ο αποδέκτης είναι σίγουρος για τον αποστολέα (είναι ο αναγραφόμενος και όχι κάποιος που τον υποδύεται ηλεκτρονικά)

- Αυθεντικοποίηση – Πιστοποίηση

  Η διαδικασία με την οποία καθορίζεται εάν κάποιος (ή κάτι) είναι στην πραγματικότητα αυτός (ή αυτό) που ισχυρίζεται ότι είναι.

ΜΗ ΑΠΟΠΟΙΗΣΗ ή ΜΗ ΑΠΑΡΝΗΣΗ

- Ο αποστολέας να μην μπορεί να αρνηθεί ότι απέστειλε το συγκεκριμένο μήνυμα ή πραγματοποίησε στην συναλλαγή και τις όποιες συνέπειες προκύπτουν. (πχ τραπεζικές, χρηματιστηριακές εντολές κλπ)

ΚΡΥΠΤΟΓΡΑΦΙΑ: Ιστορική Αναδρομή

- Η προέλευσή της επινοήθηκε κυρίως από βασιλείς αλλά και στρατηγούς για τη μεταφορά σχεδίων σε **εμπόλεμες καταστάσεις.**
- Ένα χαρακτηριστικό παράδειγμα για την κρυπτογράφηση πληροφοριών είναι **ο αλγόριθμος του Καίσαρα**. Ο αλγόριθμος βασιζόταν στην **αντικατάσταση** κάθε **γράμματος** του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Η **επιλογή** του γράμματος γινόταν με κάποιον κρυπτογραφικό αλγόριθμο συγκεκριμένα με **ολίσθηση** των **γραμμάτων δεξιά**.
- Εκτενή χρήση της κρυπτογράφησης κατά τον Β' Παγκόσμιο Πόλεμο από μηχανικές και ηλεκτρομηχανικές κατασκευές.

ΚΡΥΠΤΟΓΡΑΦΙΑ: Βασικοί ορισμοί (1)

Η **Επιστήμη** (και η Τέχνη) η οποία έχει ως αντικείμενο την εξεύρεση μεθόδων για το μετασχηματισμό των κειμένων έτσι ώστε να είναι αναγνώσιμα μόνο από εξουσιοδοτημένα άτομα.

ΚΡΥΠΤΟΓΡΑΦΙΑ: Βασικοί ορισμοί (2)

- **Κρυπτογράφηση:**

  Η διαδικασία με την οποία ένα αρχικό κείμενο (plaintext):

  - μετασχηματίζεται σε μία ακατανόητη μορφή (κρυπτογραφημένο κείμενο - cipher text) για οποιοδήποτε τρίτο,
  - σύμφωνα με ορισμένο αλγόριθμο και κρυπτογραφικά κλειδιά,
  - είναι αναγνώσιμο μόνο από εκείνους που γνωρίζουν τον αλγόριθμο και τα αντίστοιχα κλειδιά

ΚΡΥΠΤΟΓΡΑΦΙΑ: Βασικοί ορισμοί (3)

- **Αλγόριθμοι κρυπτογραφίας**
  Οι μέθοδοι και οι τεχνικές (πχ μία μαθηματική συνάρτηση) με τις οποίες πραγματοποιείται ο μετασχηματισμός των κειμένων

- **Κλειδί (ή κρυπτογραφικό κλειδί)**
  Ένα σύνολο χαρακτήρων (μυστική πληροφορία) που ενεργοποιεί τον αλγόριθμο κρυπτογράφησης ή αποκρυπτογράφησης

ΚΡΥΠΤΟΓΡΑΦΙΑ: Βασικοί ορισμοί (4)

- **Κρυπτογράφημα (κρυπτοκείμενο):**

  Το κρυπτογραφημένο κείμενο

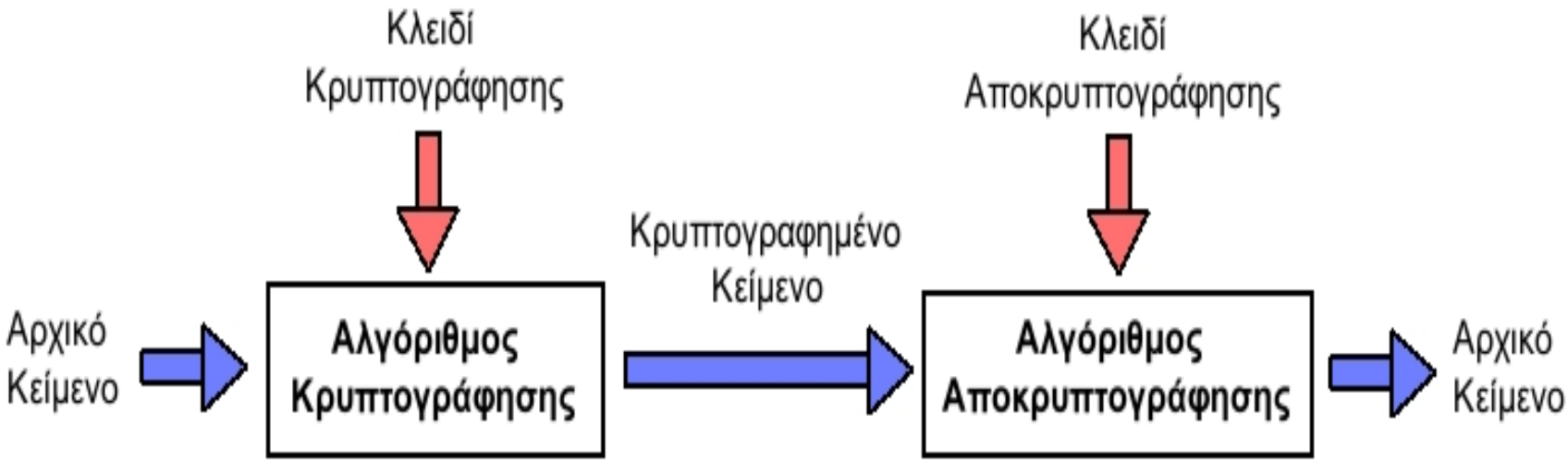
- **Αποκρυπτογράφηση:**

  Η διαδικασία με την οποία το κρυπτογραφημένο κείμενο αποκτά την αρχική κατανοητή μορφή του

- **Κρυπτανάλυση:**

  "Σπάσιμο" της κρυπτογράφησης με τον προσδιορισμό του κλειδιού κρυπτογράφησης (εξέταση των δυνατών συνδυασμών)

ΔΙΑΔΙΚΑΣΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ & ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ (1)



ΔΙΑΔΙΚΑΣΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ & ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ (2)

- Συνήθως ο **αλγόριθμος κρυπτογράφησης** είναι **γνωστός**

- Η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος βασίζεται στη **μυστικότητα** του **κλειδιού κρυπτογράφησης**.

ΔΙΑΔΙΚΑΣΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ & ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ (3)

- Το **μέγεθος** του κλειδιού κρυπτογράφησης μετριέται σε αριθμό **bits**.
- Όσο μεγαλύτερο είναι το κλειδί τόσο μεγαλύτερος είναι ο αριθμός των προς εξέταση δυνατών κλειδιών
  - **Μικρό** μέγεθος κλειδιού → **Ασθενής** Κρυπτογράφηση
  - **Μεγάλο** μέγεθος κλειδιού → **Ισχυρή** Κρυπτογράφηση

Πχ

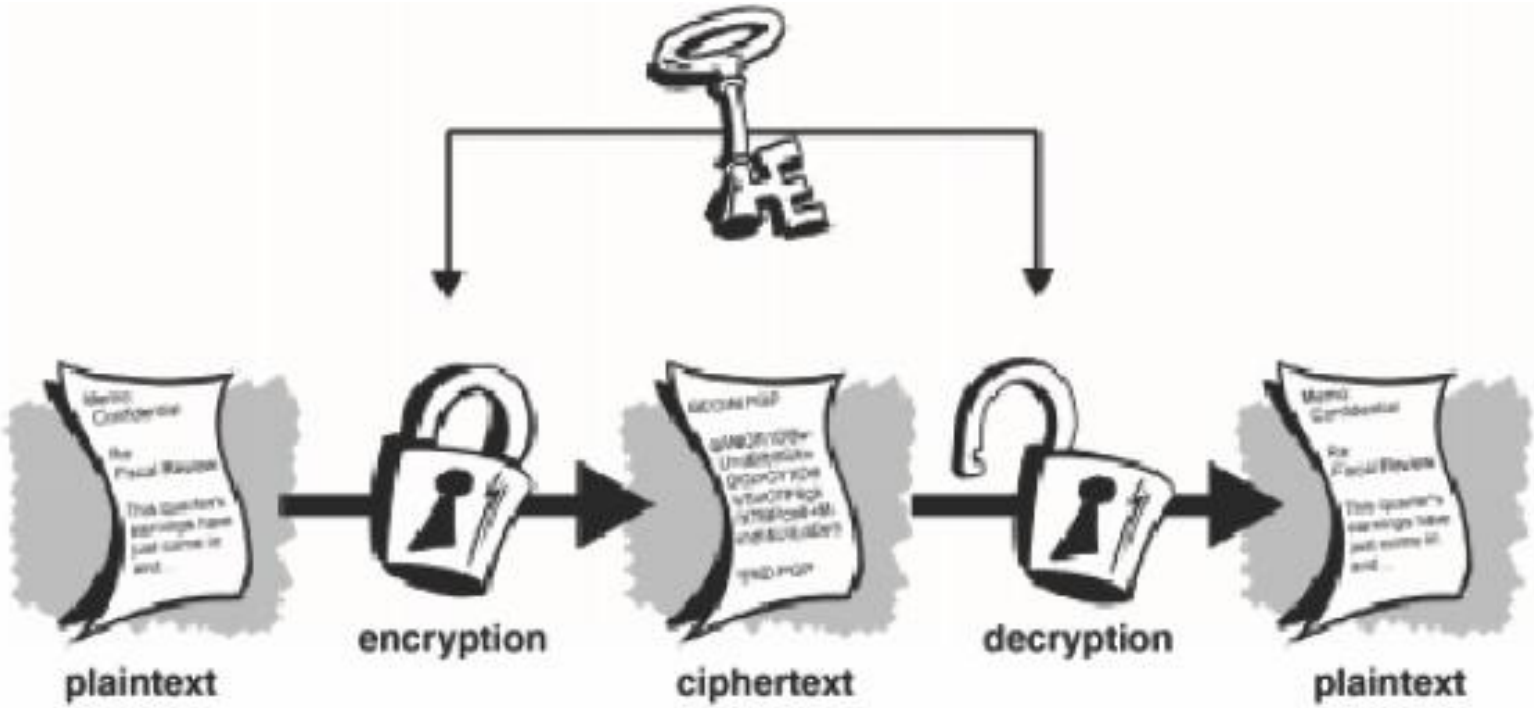
Μέγεθος Κλειδιού (bits)	**Δυνατοί Συνδυασμοί Κλειδιών**	
56	2^{56} =	7,206 **X** 10^{16}
64	2^{64} =	1,845 **X** 10^{19}
128	2^{128} =	3,403 **X** 10^{38}

ΚΑΤΗΓΟΡΙΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

- **Συμμετρική Κρυπτογραφία (Κλασσική ή Κρυφού Κλειδιού)**
  Χρησιμοποιεί το **ΙΔΙΟ** κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση (κρυφό κλειδί)

- **Ασύμμετρη Κρυπτογραφία (Δημοσίου Κλειδιού)**
  Χρησιμοποιεί **ΔΙΑΦΟΡΕΤΙΚΑ** κλειδιά για την κρυπτογράφηση και για την αποκρυπτογράφηση

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (1)



ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (3)

- Χρησιμοποιείται **το ίδιο κλειδί** τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση αλλά με αντίστροφο τρόπο.

  Αλγόριθμοι - Μέθοδοι:
  - Αντικατάστασης
  - Μετάθεσης
  - Μεικτή
- Δεν παρέχεται η δυνατότητα Αυθεντικοποίησης & Μη αποποίησης (γνωρίζουν τουλάχιστον 2 το κλειδί)
- Απαιτείται ασφαλής τρόπος μετάδοσης των κλειδιών
- Συχνά χρησιμοποιείται με κλειδιά μόνο μίας χρήσης (session keys): δημιουργούνται στιγμιαία από τον αποστολέα κατά την στιγμή έναρξης μίας συνόδου με τον αποδέκτη και αποστέλλονται κρυπτογραφημένα με την μέθοδο Ασύμμετρης Κρυπτογράφησης.

ΜΕΘΟΔΟΙ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ (1)

- **Αλγόριθμος του Καίσαρα (ή Ολίσθησης)**: Κάθε σύμβολο του αλφαβήτου αντικαθίσταται από σύμβολο που ευρίσκεται Κ θέσεις μετά.

Κλειδί: αριθμός θέσεων (Κ) ολίσθησης του αλφάβητου δεξιά

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ

Πχ Αν Κ=6 τότε “ΑΡΧΗ” -> “ΗΨΔΝ”

ΜΕΘΟΔΟΙ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ (2)

- Κάθε σύμβολο του αρχικού μηνύματος αντικαθίσταται από ένα ή περισσότερα άλλα σύμβολα, σύμφωνα με κάποιον αλγόριθμο - κλειδί (1-1 αντιστοίχιση).

  Τα σύμβολα μπορεί να ανήκουν στο ίδιο αλφάβητο ή σε διαφορετικό

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
1	Α	Β	2	Γ	Δ	3	Ε	Ζ	4	Η	Θ	5	Ι	Κ	6	Λ	Μ	7	Ν	Ξ	8	Ο	Π

Πχ Κλειδί: αριθμός θέσεων (Κ) ολίσθησης της δεύτερης γραμμής δεξιά

Αν Κ=2 τότε “ΤΕΛΟΣ” -> “ΛΒΖ56”

ΜΕΘΟΔΟΙ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ (3)

- **Αλγόριθμος του Πίνακα**: Κάθε σύμβολο του ελληνικού αλφαβήτου αντικαθίσταται από το δύο τα αντίστοιχα σύμβολα γραμμής & στήλης

	Κ	**Ο**	**Ζ**	**Α**	**Ν**	**Η**
Α	Α	Β	Γ	Δ	Ε	Ζ
Ω	Η	Θ	Ι	Κ	Λ	Μ
Ο	Ν	Ξ	Ο	Π	Ρ	Σ
Σ	Τ	Υ	Φ	Χ	Ψ	Ω

Πχ “ΠΡΟΓΡΑΜΜΑ” -> “ΟΑΟΝΟΖΑΖΟΝΑΚΩΗΩΗΑΚ”

ΜΕΘΟΔΟΙ ΜΕΤΑΘΕΣΗΣ

- **Αναδιάταξη της σειράς των συμβόλων του μηνύματος, σύμφωνα με κάποιον αλγόριθμο και ένα κλειδί (πχ μία ή περισσότερες μεταθέσεις)**

Πχ το μήνυμα αναδιατάσσεται σε ένα Πίνακα (NXM) κατά γραμμές και στην συνέχεια κατά στήλες

Αρχικό μήνυμα: "ΘΑ ΠΕΡΑΣΩ ΝΑ ΣΕ ΠΑΡΩ ΑΠΟ ΤΟ ΣΠΤΙ ΤΟΥΣ"

	M=10									
N=3	Θ	Α	Π	Ε	Ρ	Α	Σ	Ω	Ν	Α
	Σ	Ε	Π	Α	Ρ	Ω	Α	Π	Ο	Τ
	Ο	Σ	Π	Ι	Τ	Ι	Τ	Ο	Υ	Σ

Κρυπτομήνυμα: "ΘΣΟΑΕΣΠΠΠΕΑΙΡΡΤΑΩΙΣΑΤΩΠΟΝΟΥΑΤΣ"

ΜΕΙΚΤΕΣ ΜΕΘΟΔΟΙ (1)

- Περιλαμβάνουν **σειρά αντικαταστάσεων & μεταθέσεων** των συμβόλων του αρχικού μηνύματος με αντίστοιχα κλειδιά
- Ο πιο διαδεδομένος αλγόριθμος συμμετρικής κρυπτογραφίας είναι ο **DES** (Data Encryption Standard) IBM – USA Government,1977. Κλειδί 64 bits
- **Βασικά Βήματα** (για κάθε block 64 bit ==> block 64 bit)
  - ✓ Αρχική μετάθεση (σταθερή)
  - ✓ Διαίρεση σε δύο τμήματα 32 bit
  - ✓ Κάθε ένα από αυτά τροποποιείται (αντικατάσταση) 16 φορές, με βάση μία συνάρτηση F και το Κλειδί
  - ✓ Τελική μετάθεση (αντίστροφη της αρχικής)

ΜΕΙΚΤΕΣ ΜΕΘΟΔΟΙ (2)

- **3DES**: Ο παραπάνω αλγόριθμος εκτελείται 3 φορές μ 3 διαφορετικά κλειδιά (A,B,C). ==> αύξηση ισχύος κρυπτογράφησης ==> δυσκολότερη η αποκρυπτογράφηση
- **AES**(Advanced Encryption Standard): Ισχυρότερος αλγόριθμος με χρήση κλειδιού 128, 192, 256 bits.
- **RC2, RC4, RC5, RC6** : Αλγόριθμοι με χρήση μεταβλητού μήκους κλειδιού.

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ - ΠΛΕΟΝΕΚΤΗΜΑΤΑ

- Ταχεία κρυπτογράφηση/αποκρυπτογράφηση με χαμηλές απαιτήσεις υπολογισμών κ υπολογιστικής ισχύος.
- Εύκολη και απλή υλοποίηση
- Δύσκολη κρυπτανάλυση (εύρεση του κλειδιού)

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ – ΜΕΙΟΝΕΚΤΗΜΑΤΑ (1)

- **Δύσκολη διαχείριση κλειδιών** (key management) για μεγάλο αριθμό επικοινωνούντων, απαιτείται τεράστια προσπάθεια για την δημιουργία, αλλαγή & οργάνωση κλειδιών.

  Κ επικοινωνούντες → **Κ(Κ-1)/2** κλειδιά

  2 επικοινωνούντες → 2(2-1)/2=1 κλειδιά

  3 επικοινωνούντες → 3(3-1)/2=3 κλειδιά

  ….

  10 επικοινωνούντες → 10(10-1)/2= 45 κλειδιά

- Ανάγκη για **ασφαλή φύλαξη και διανομή** του κλειδιού

  Το κλειδί αυτό πρέπει να γνωρίζουν ο αποστολέας και ο αποδέκτης και να τηρείται μυστικό από οποιοδήποτε άλλο τρίτο

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ – ΜΕΙΟΝΕΚΤΗΜΑΤΑ (2)

- **Προκύπτει όμως το εξής πρόβλημα**: *Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πώς γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα;*

- Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα.

- Οι **κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού** λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κ.ο.κ.).

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ - ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (1)

Κάθε χρήστης χρησιμοποιεί ένα ζευγάρι κλειδιών:

- **ΔΗΜΟΣΙΟ ΚΛΕΙΔΙ (PUBLIC KEY) - ΔΚ**

  Γνωστοποιείται στο κοινό μέσω δημόσιων καταλόγων ή δημόσιας βάσης δεδομένων

- **ΙΔΙΩΤΙΚΟ ΚΛΕΙΔΙ (PRIVATE KEY) - ΙΚ**

  Κρατείται απόρρητο. Το γνωρίζει μόνο ο ιδιοκτήτης του

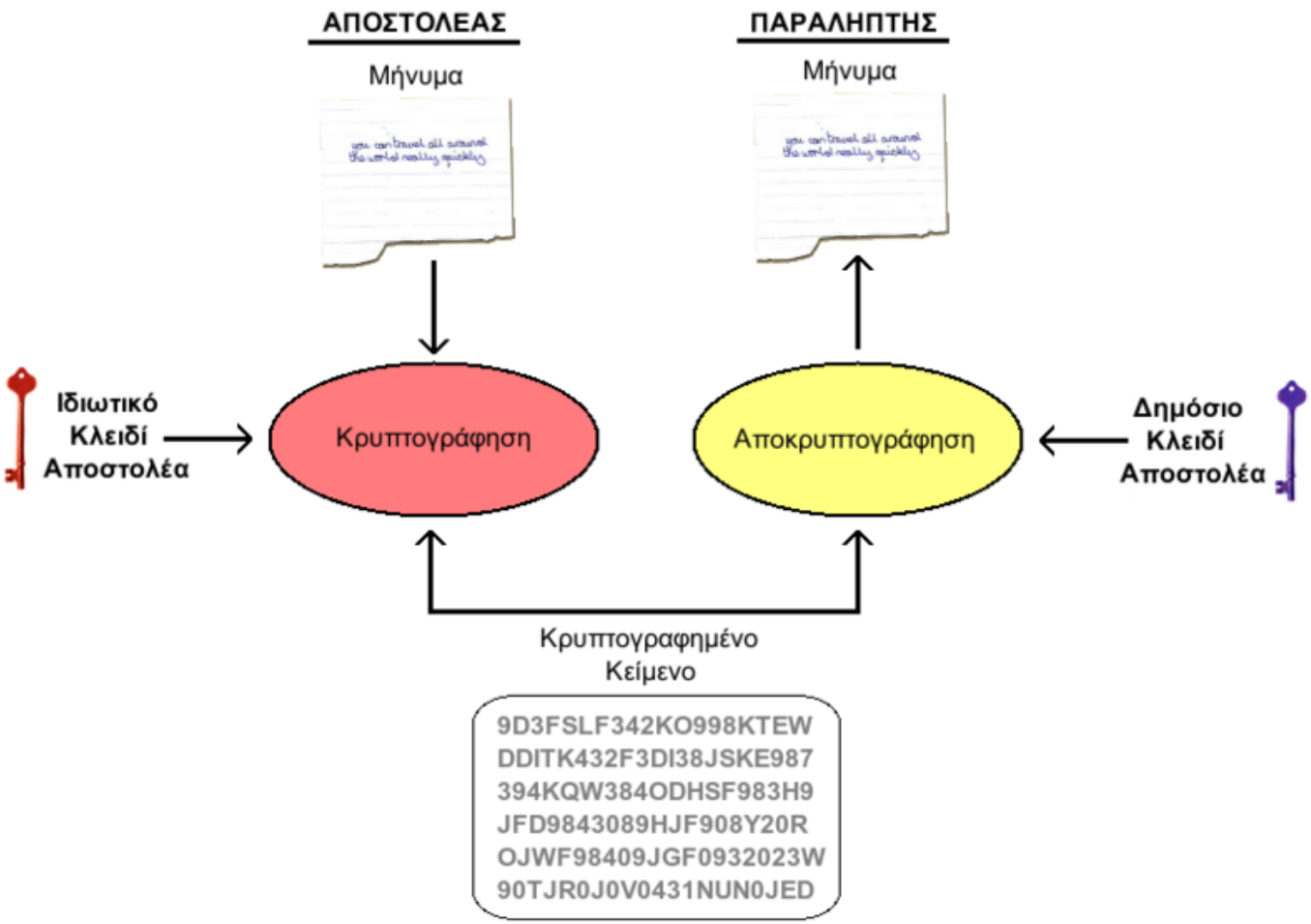
ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ - ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ()

- Μηνύματα που κρυπτογραφούνται με **το ένα κλειδί** αποκρυπτογραφούνται **μόνο από το άλλο κλειδί**
- Για κάθε Ιδιωτικό Κλειδί αντιστοιχεί μόνο ένα Δημόσιο Κλειδί.
- Ο υπολογισμός του Ιδιωτικό Κλειδί ενός χρήστη από το Δημόσιο Κλειδί του είναι πρακτικά ανέφικτος.

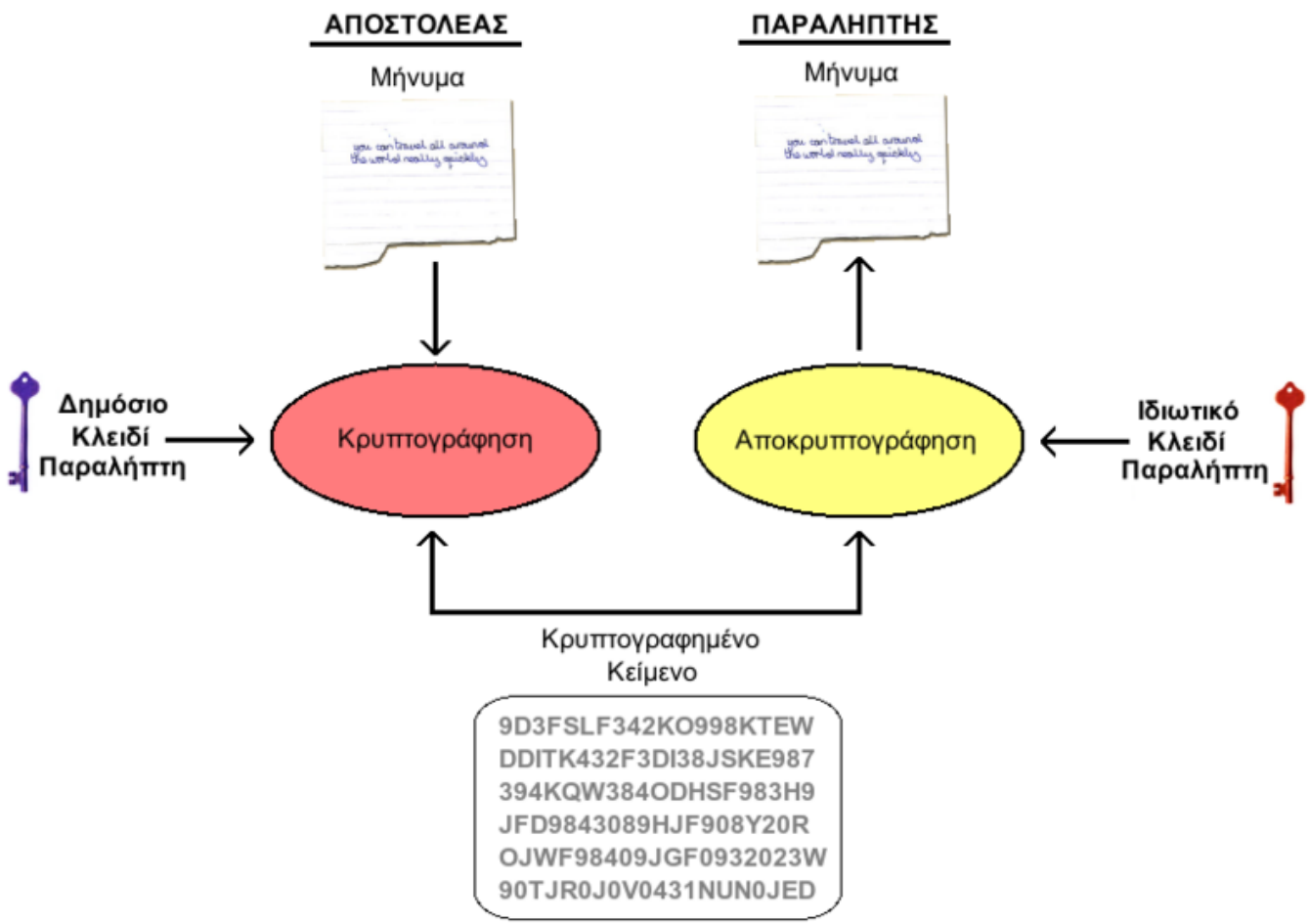
ΧΡΗΣΗ

1. Επιβεβαίωση ταυτότητας (**αυθεντικότητα**) του αποστολέα
2. Ανταλλαγή **εμπιστευτικών** μηνυμάτων

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ:
Επιβεβαίωση ταυτότητας αποστολέα



ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ:
Εμπιστευτικά μηνύματα



ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ - ΑΛΓΟΡΙΘΜΟΙ

- RSA (Rivest, Shamir, Adelman): Ο κυριότερος αλγόριθμος ΑΚ που χρησιμοποιείται σήμερα.
- Diffie-Hellman Key Exchange
- ElGamal,
- Digital Signature Standard (DSS)

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ:
Επιβεβαίωση ταυτότητας αποστολέα & Εμπιστευτικότητα

- Εάν θέλουμε να έχουμε **εμπιστευτικότητα** & **αυθεντικότητα** αποστολέα: ο αποστολέας κρυπτογραφεί το μήνυμα με το ΙΚ του και κατόπιν ξανακρυπτογραφεί με το ΔΚ του αποδέκτη
- Η συγκεκριμένη **πρακτική** απαιτεί **πολλούς υπολογισμούς** -> διαρκεί **μεγάλο χρονικό διάστημα**

ΥΒΡΙΔΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (1)

- Η ασύμμετρη κρυπτογραφία είναι μη αποτελεσματική για την κρυπτογράφηση μεγάλου όγκου δεδομένων, αντίθετα από τη συμμετρική.
- Εναλλακτικά χρησιμοποιείται συνδυασμός συμμετρικής (DES) και ασύμμετρης κρυπτογράφησης (RSA): λιγότεροι υπολογισμοί και μικρότερο χρονικό διάστημα.
- Συνηθισμένη χρήση της ασύμμετρης κρυπτογραφίας είναι η αποστολή ενός συμμετρικού κρυπτογραφικού κλειδιού μέσω ενός ανασφαλούς καναλιού.

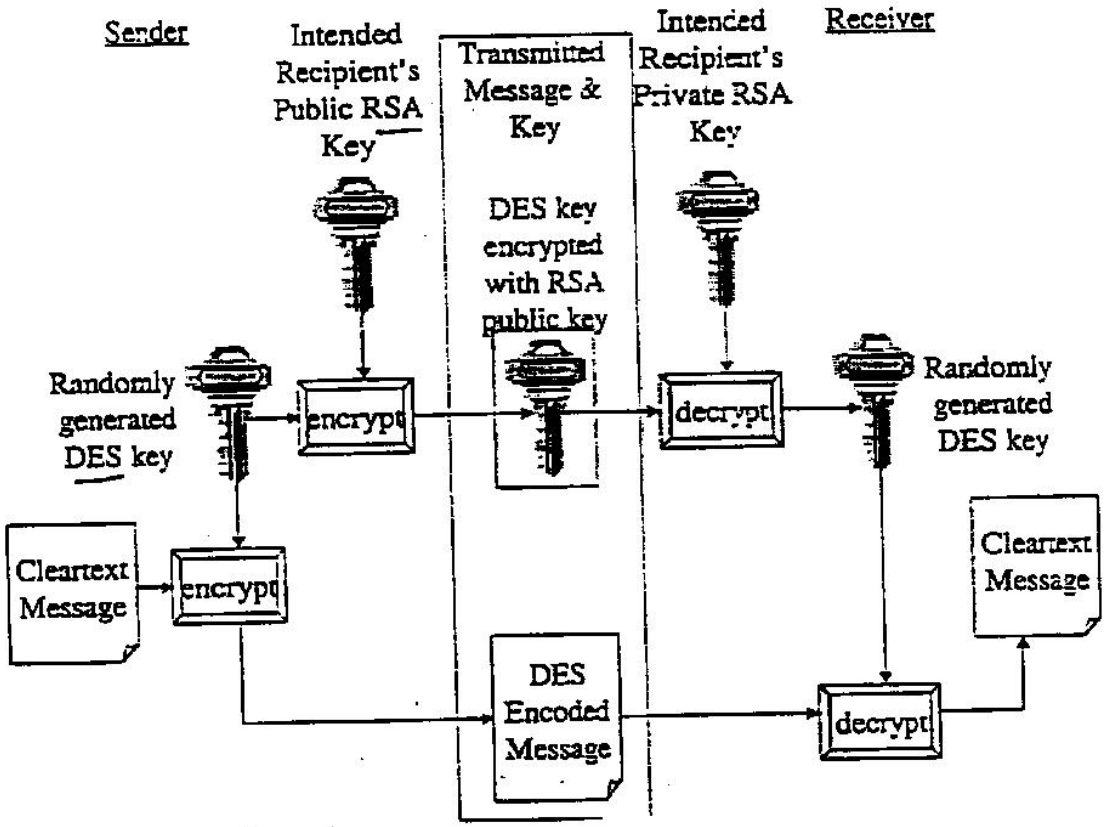
ΥΒΡΙΔΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (2)

- Ένα ‘Κέντρο Διανομής Κλειδιών’ διανέμει με ασφάλεια στα συναλλασσόμενα μέρη ένα συμμετρικό κλειδί, κρυπτογραφημένο με τα δημόσια κλειδιά των εμπλεκομένων.
- Οι συναλλασσόμενοι αποκρυπτογραφούν το κλειδί και ξεκινούν εμπιστευτικές συνόδους μεταξύ τους, χρησιμοποιώντας συμμετρικούς αλγόριθμους
- Ο συνδυασμός των δύο τεχνολογιών ονομάζεται Υβριδική Κρυπτογραφία. Π.χ. πρωτόκολλο SSL.

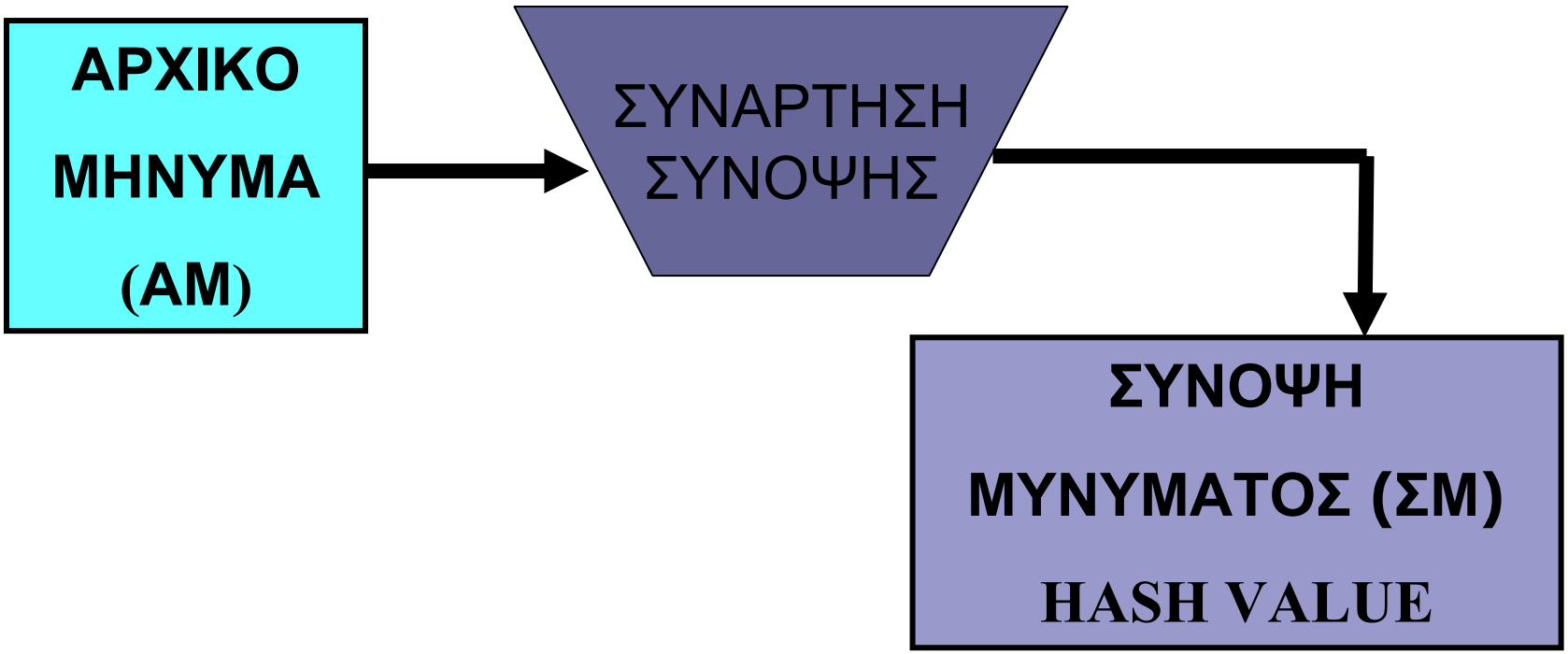
ΥΒΡΙΔΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (3)

Εξασφάλιση Εμπιστευτικότητας με DES & RSA

(δεν εξασφαλίζει Αυθεντικότητα Αποστολέα)



ΣΥΝΑΡΤΗΣΗ ΣΥΝΟΨΗΣ: HASH FUNCTION



ΣΥΝΑΡΤΗΣΗ ΣΥΝΟΨΗΣ: ΠΑΡΑΔΕΙΓΜΑ

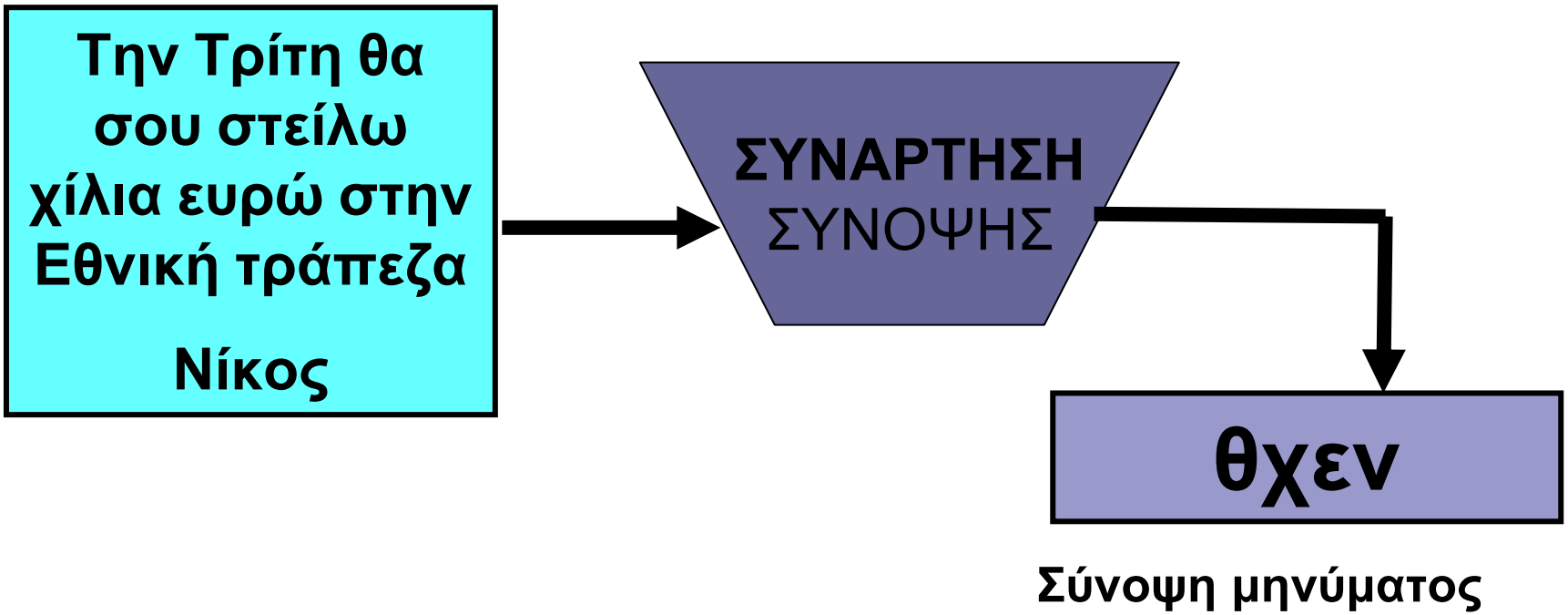
- **ΜΗΝΥΜΑ**

  "*Την Τρίτη θα σου στείλω χίλια ευρώ στην Εθνική τράπεζα. Νίκος*"

- **ΣΥΝΑΡΤΗΣΗ ΣΥΝΟΨΗΣ**

  Διάβασε το πρώτο γράμμα της τρίτης, της έκτης, της έβδομης και της τελευταίας λέξης και γράψε το αποτέλεσμα

ΣΥΝΑΡΤΗΣΗ ΣΥΝΟΨΗΣ: ΠΑΡΑΔΕΙΓΜΑ (2)



ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ

- **ΠΔ 150 25-6- 2001**
- **Ηλεκτρονική υπογραφή:** δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμοποιούνται ως απόδειξη γνησιότητας

ΠΡΟΗΓΜΕΝΗ ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ (ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ)

Πληροί τους εξής όρους:

- Συνδέεται μονοσήμαντα με τον υπογράφοντα
- Είναι ικανή να προσδιορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
- Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό έλεγχο
- Συνδέεται με τα δεδομένα, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ στην πράξη (1)

- Το κρυπτογραφημένο **σύνολο των χαρακτήρων της σύνοψης** με το **ιδιωτικό κλειδί** του υπογράφοντος αποτελεί την **ηλεκτρονική (ψηφιακή) του υπογραφή**

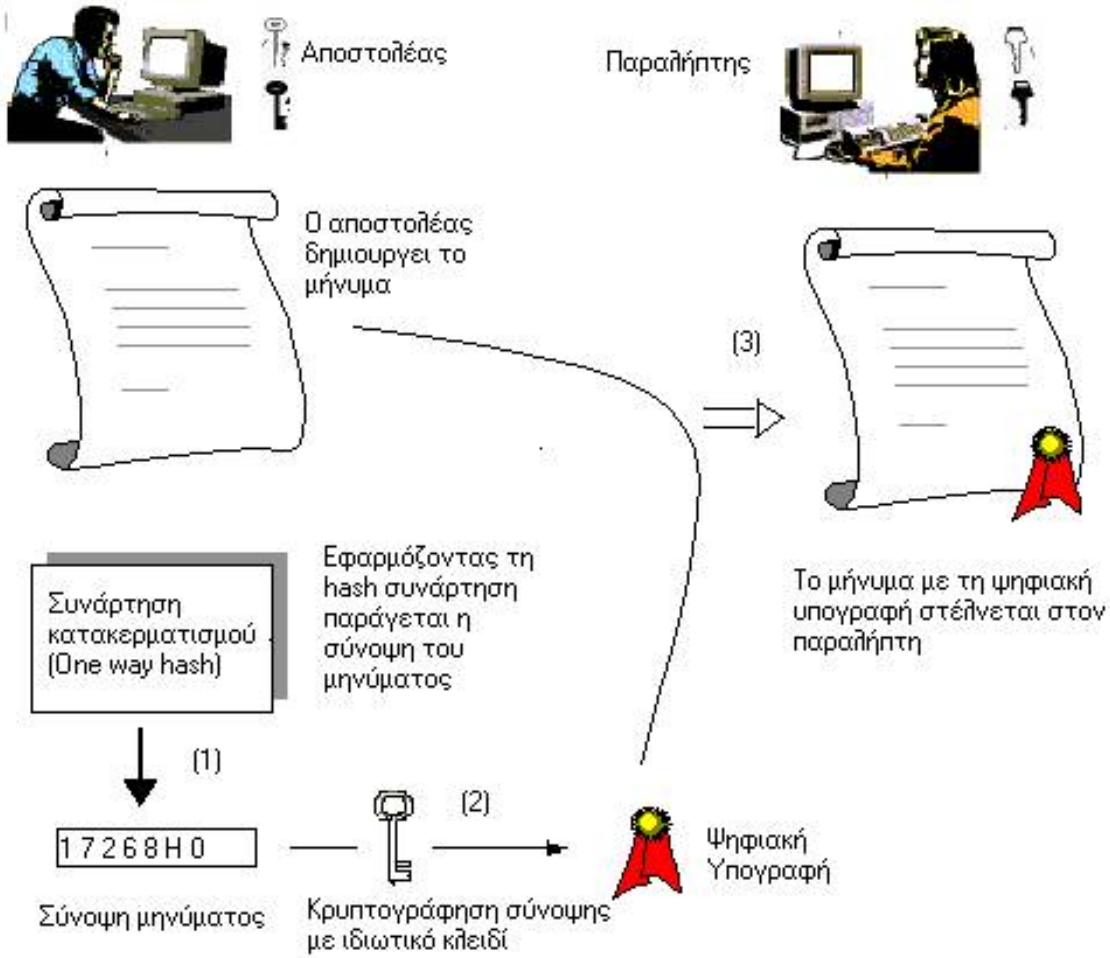
- Συνεπώς η Ψηφιακή Υπογραφή αφορά ένα **συγκεκριμένο μήνυμα ενός συγκεκριμένου χρήστη** (ζεύγος μήνυμα-χρήστης) και όχι μόνον έναν συγκεκριμένο χρήστη άτομο όπως η φυσική υπογραφή

- Με την κρυπτογράφηση της Σύνοψης του μηνύματος με το ΙΚ του αποστολέα δεν μπορούν να αμφισβητηθούν ούτε το Περιεχόμενο ούτε ο Αποστολέας

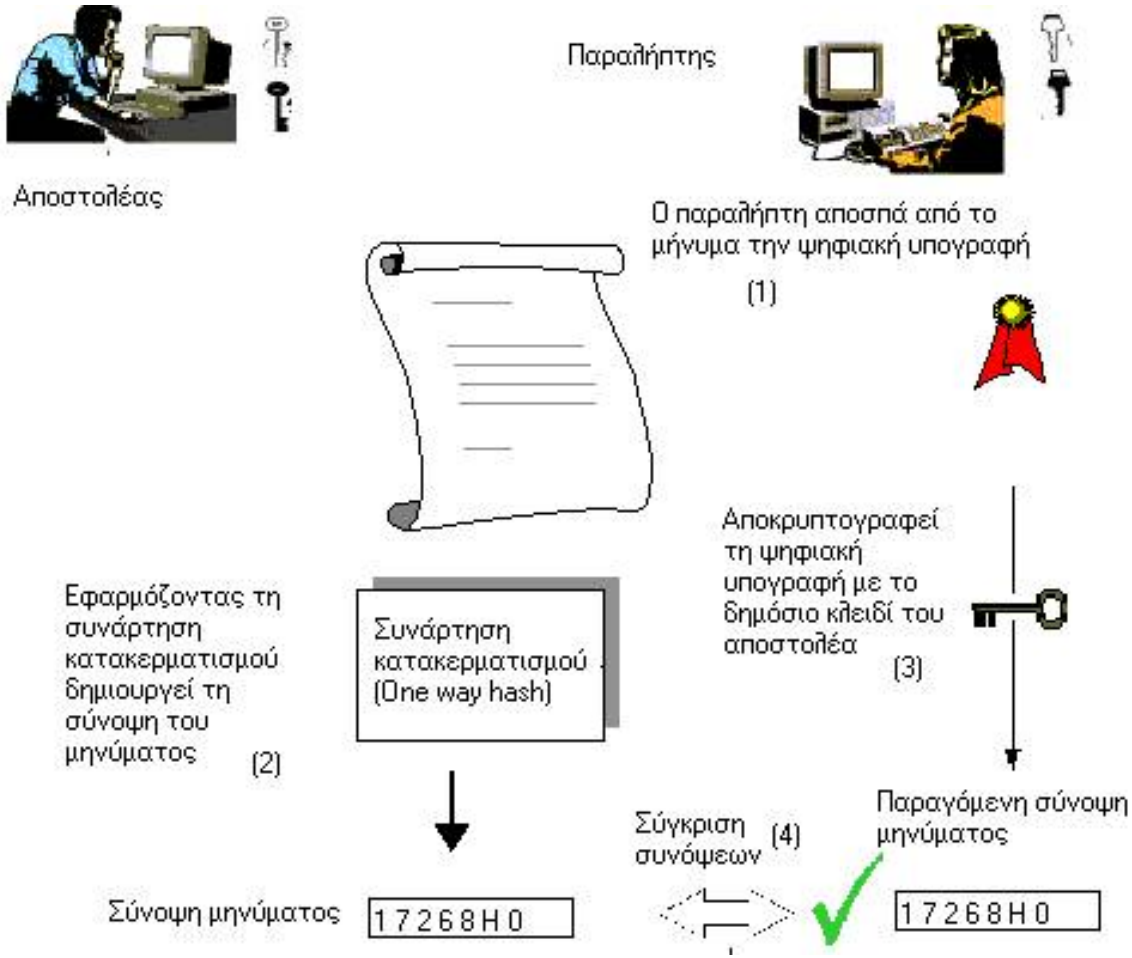
ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ στην πράξη (2)

- Η ψηφιακή υπογραφή είναι νομικά δεσμευτική όσο και η φυσική (ΠΔ 150/2001)
- Οι κυριότεροι αλγόριθμοι σύνοψης είναι: MD2, MD4, MD5 (παράγουν συνόψεις 128 bit)
- Για να εξασφαλιστεί (εάν είναι αναγκαία) και η Εμπιστευτικότητα γίνεται χρήσης συμμετρικής κρυπτογράφησης (DES αλγόριθμος)

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ: Υπογραφή του μηνύματος



ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ: Παραλαβή του υπογεγραμμένου μηνύματος



ΥΠΟΔΟΜΗ ΣΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKI: Public key Infrastructure)

- ΤΟ PKI είναι ένα **ολοκληρωμένο σύστημα** από:
  - πολιτικές,
  - διαδικασίες και
  - τεχνολογίες

το οποίο παρέχει στους χρήστες του Διαδικτύου τη δυνατότητα να ανταλλάσσουν πληροφορίες με **μυστικότητα** και **ασφάλεια**

ΠΟΙΕΣ ΛΥΣΕΙΣ ΥΠΑΡΧΟΥΝ;

- Εμπιστευτικότητα: Κρυπτογραφία (Συμμετρική και Ασύμμετρη)
- Ακεραιότητα: Ψηφιακές Υπογραφές, Συναρτήσεις σύνοψης
- Αυθεντικότητα, Μη αποκήρυξη : Μέθοδοι αυθεντικοποίησης, Ψηφιακά πιστοποιητικά, υπογραφές, έξυπνες κάρτες

ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ:CA-CERTIFICATION AUTHORITY (1)

- Απαιτείται η ύπαρξη ενός μηχανισμού, μιας **Έμπιστης Τρίτης Οντότητας,** που να πιστοποιεί την ταυτότητα του κατόχου ενός κλειδιού

- Ο **Πάροχος Υπηρεσιών Πιστοποίησης** (ΠΥΠ) είναι ένας Οργανισμός (φυσικό ή νομικό πρόσωπο) ο οποίος εκδίδει και δημοσιεύει πιστοποιητικά τα οποία συνδέουν το δημόσιο κλειδί του χρήστη με τα στοιχεία ταυτότητας του

ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ:CA-CERTIFICATION AUTHORITY (2)

- Βασικές λειτουργίες του Π.Υ.Π.
  - Ταυτοποίηση οντοτήτων
  - Παροχή λογισμικού δημιουργίας ΙΚ και ΔΚ σε κάθε οντότητα
  - Αποθήκευση ΔΚ (αφού το δημιουργήσει ο χρήστης)
  - Έκδοση ΨΠ
  - Λίστες ανακληθέντων ΨΠ και ΔΚ

ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ (1)

- Το ψηφιακό πιστοποιητικό είναι ένα **«επίσημο έγγραφο»**, συνήθως σε ηλεκτρονική μορφή, το οποίο συνδέει τα στοιχεία του κατόχου με τα στοιχεία της ηλεκτρονικής του υπογραφής

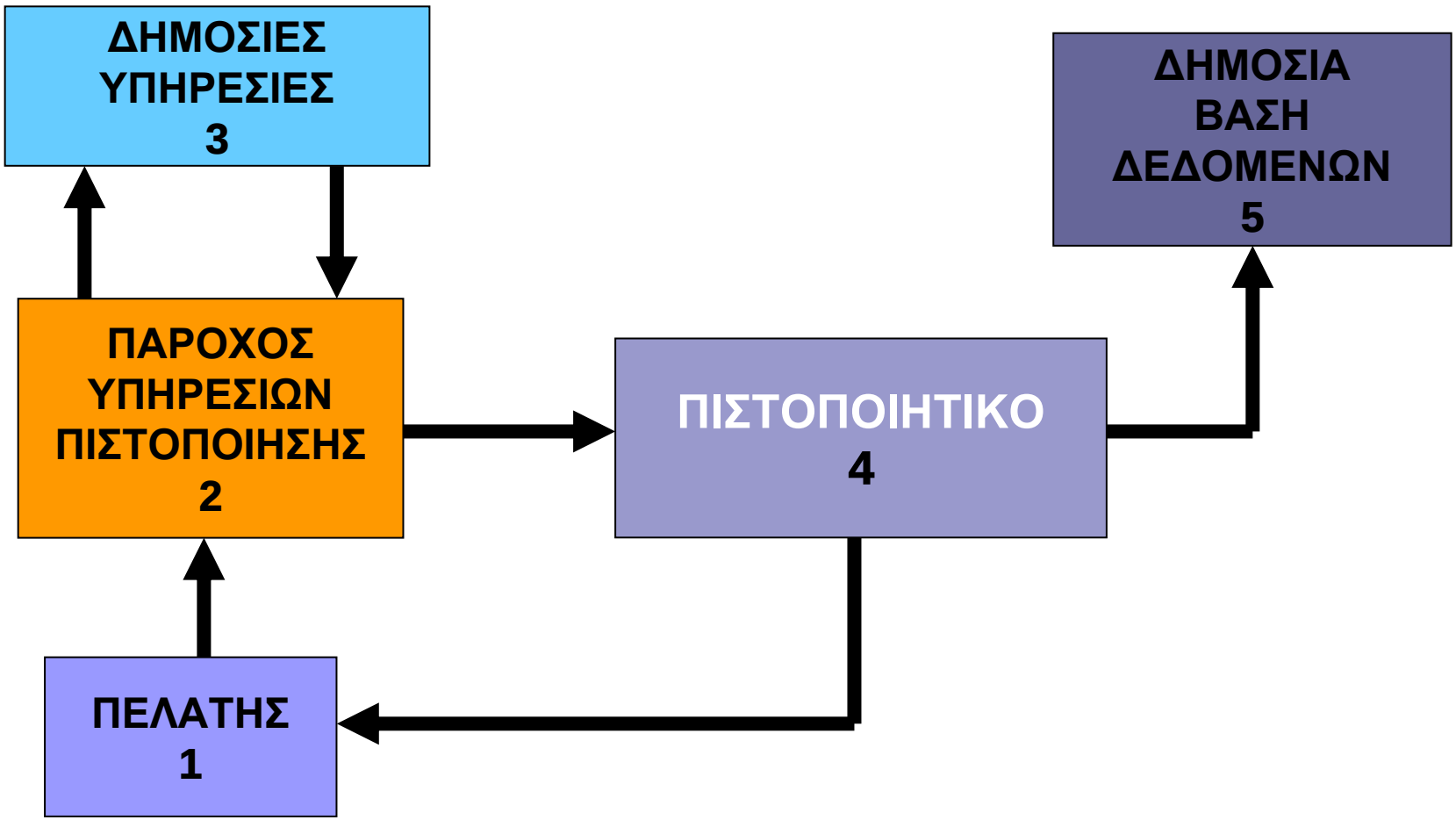
- Το ψηφιακό πιστοποιητικό περιέχει:
  - Το δημόσιο κλειδί
  - Τα στοιχεία ταυτότητας του κατόχου του κλειδιού
  - Την ψηφιακή υπογραφή του ΠΥΠ που πιστοποιεί όλα τα παραπάνω

- **Διασφαλίζει με τεχνικά (αλλά και νομικά) μέσα** ότι ένα δημόσιο κλειδί ανήκει σε μία (και μόνο μία) συγκεκριμένη οντότητα (και συνεπώς ότι η οντότητα αυτή είναι ο νόμιμος κάτοχος του αντίστοιχου ιδιωτικού κλειδιού)

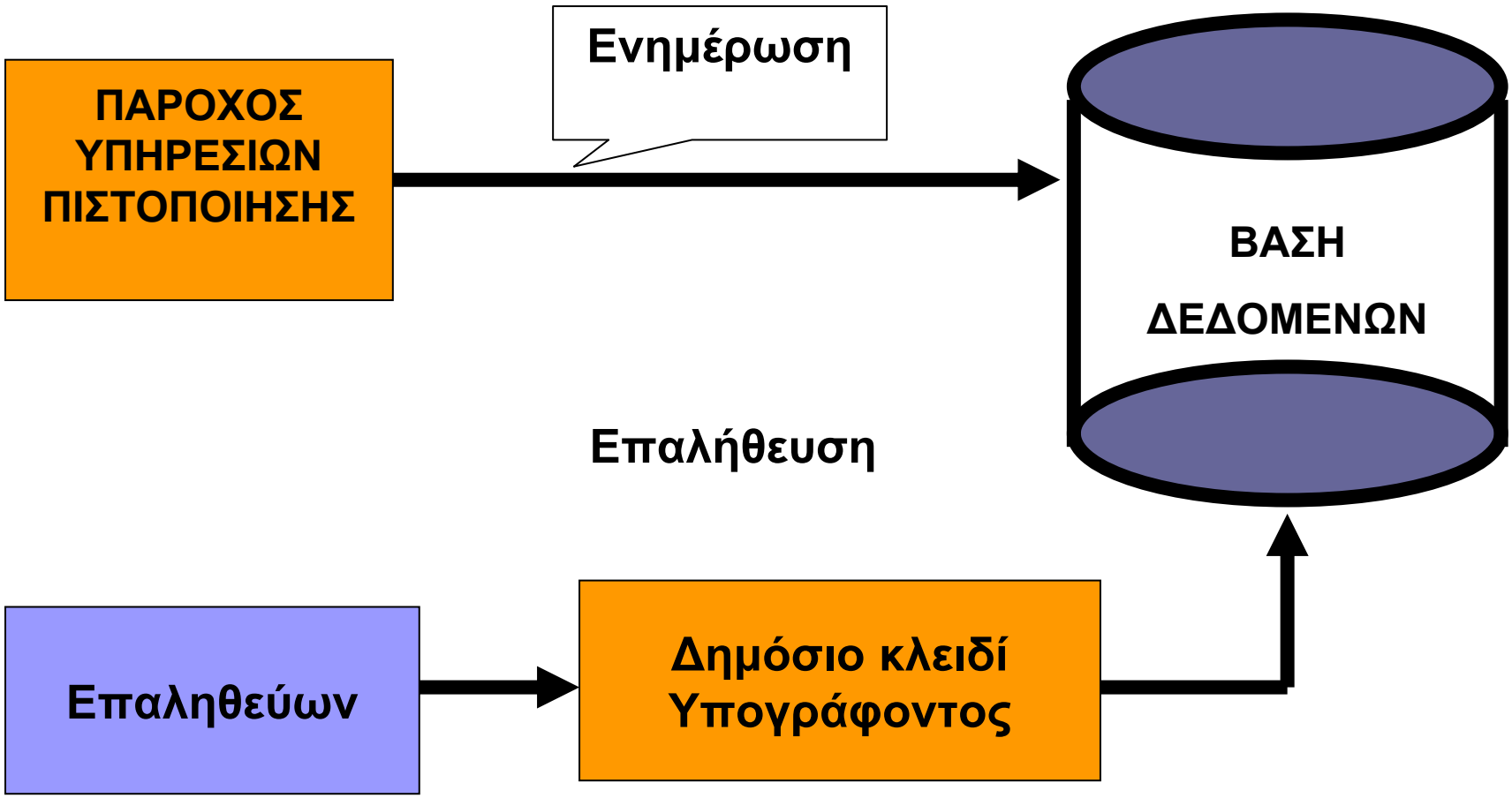
ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ (2)

Σειριακός αριθμός πιστοποιητικού	**A0345BF303203833000012BBB0**
Ονομασία Παρόχου	**3000D092A864F7D00111DD87**
Αλγόριθμος υπογραφής του Παρόχου	**30160503560426563F06C45662**
Ονοματεπώνυμο κατόχου	**30C060365C04B154466AC3597**
Δημόσιο κλειδί κατόχου	**300906036504663D1C0983E566**
Ατομικός αριθμός κατόχου	**3015060AD45929569BC452009**
Περιορισμοί χρήσεως	**30080B003551DA2C45D39DAE**
Σημείο ανάκλησης	**301F0603551DBF3A3781D4409**
Χρόνος ισχύος	**301905004986FD308487520AD**
Ψηφιακή υπογραφή Παρόχου	**30D0609F0D05687AEC452001**

ΔΙΑΔΙΚΑΣΙΑ ΠΙΣΤΟΠΟΙΗΣΗΣ



ΔΙΑΔΙΚΑΣΙΑ ΕΠΑΛΗΘΕΥΣΗΣ ΥΠΟΓΡΑΦΗΣ



ΑΝΑΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

- Λίστα Ανάκλησης Πιστοποιητικών
- Λόγοι ανάκλησης:
  - Απώλεια ιδιωτικού κλειδιού
  - Κλοπή ή διαρροή ιδιωτικού κλειδιού
  - Αλλαγή στοιχείων ή ρόλου
  - Παύση λειτουργίας ΠΥΠ

ΚΥΚΟΣ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Ο κύκλος ζωής ενός πιστοποιητικού αποτελείται από τα παρακάτω στάδια:

- **Έκδοση (Issue):** Αφορά την απόκτηση του ψηφιακού πιστοποιητικού από τον χρήστη ύστερα από αίτημα υποβολής
- **Ανανέωση (Renewal):** Αφορά το δικαίωμα που έχει κάθε χρήστης κάτοχος ήδη ενός πιστοποιητικού για ανανέωση της ισχύος του πιστοποιητικού.
- **Ανάκληση (Revoke):** Η απαραίτητη και άμεσα πραγματοποιήσιμη διαδικασία για την κατάργηση του πιστοποιητικού σε περίπτωση που υπάρχει κίνδυνος αποκάλυψης των δεδομένων του υπάρχοντος πιστοποιητικού μας από κάποιον τρίτο.
- **Ανάκτηση (Recovery):** Η διαδικασία κατά την οποία ο χρήστης απαιτεί ανάκτηση του ανακληθέντος πιστοποιητικού του.

ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

- Ο βασικός μηχανισμός αυθεντικοποίησης στο μέλλον;;;
- Απαιτούν εισαγωγή PIN – Συνεπώς είναι μέσο αυθεντικοποίησης δύο παραγόντων:
  - Κάτι που γνωρίζω και
  - Κάτι που κατέχω
- Απαιτεί ειδικό υλικό
  - Αναγνώστης έξυπνης κάρτας
  - Διεπαφή PC card (PCMCIA)
  - Διεπαφή USB/ RS232 / parallel
- Εξαιρετικά δύσκολη αντιγραφή
- Προστασία ανάγνωσης/τροποποίησης περιεχομένου
- Μεγάλη αξιοπιστία και μηχανική αντοχή
- Εύκολα μεταφέρσιμη

ΔΙΑΔΙΚΑΣΙΑ – ΔΟΜΗ ΡΚΙ ΣΥΖΕΥΞΙΣ (1)

- Πάροχος Υπηρεσιών Πιστοποίησης για τους Φορείς μέλη του "ΣΥΖΕΥΞΙΣ", σύμφωνα με το **Προεδρικό Διάταγμα 150/2001**

- Υλοποίηση Δομής πιστοποίησης (**άρθρο 20, Ν3448/2006 και άρθρο 25, Ν3536/2007**) Αρχής Πιστοποίησης (Certification Authority) και εγγραφής (Registration Authority)

- Έκδοση Ψηφιακών Πιστοποιητικών για εξουσιοδοτημένους χρήστες με βάση τον κανονισμό της **ΑΠΕΔ ΦΕΚ 1654/Β-10-11-2006** ενσωμάτωση της πληροφορίας σχετικά με το χρήστη και τον Φορέα στον οποίο ανήκει.

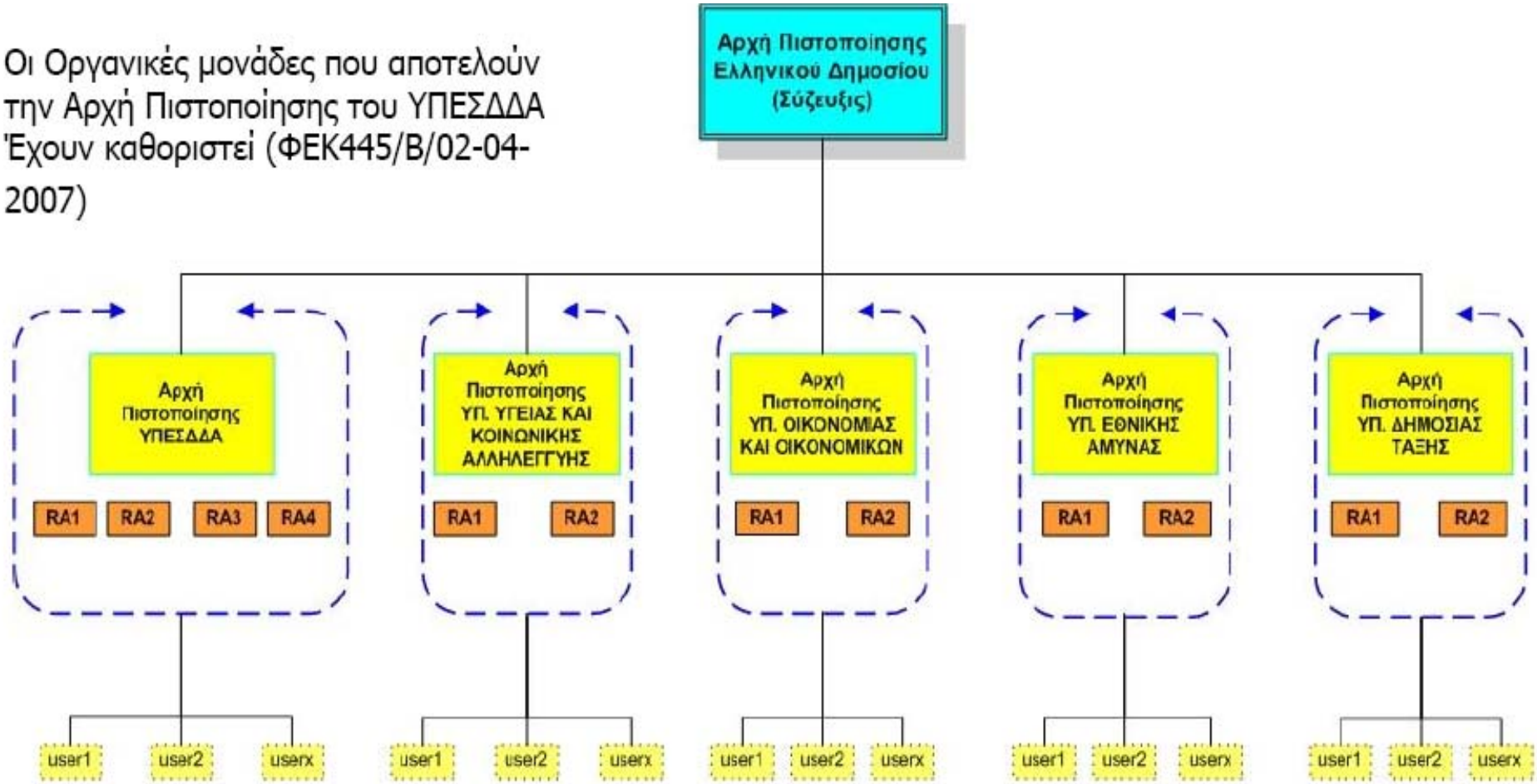
- Η χρήση των ψηφιακών πιστοποιητικών θα πρέπει να γίνεται μέσω Έξυπνων Καρτών (smart cards) ή άλλης ασφαλούς διάταξης δημιουργίας υπογραφής.

ΔΙΑΔΙΚΑΣΙΑ – ΔΟΜΗ PKI ΣΥΖΕΥΞΙΣ (2)

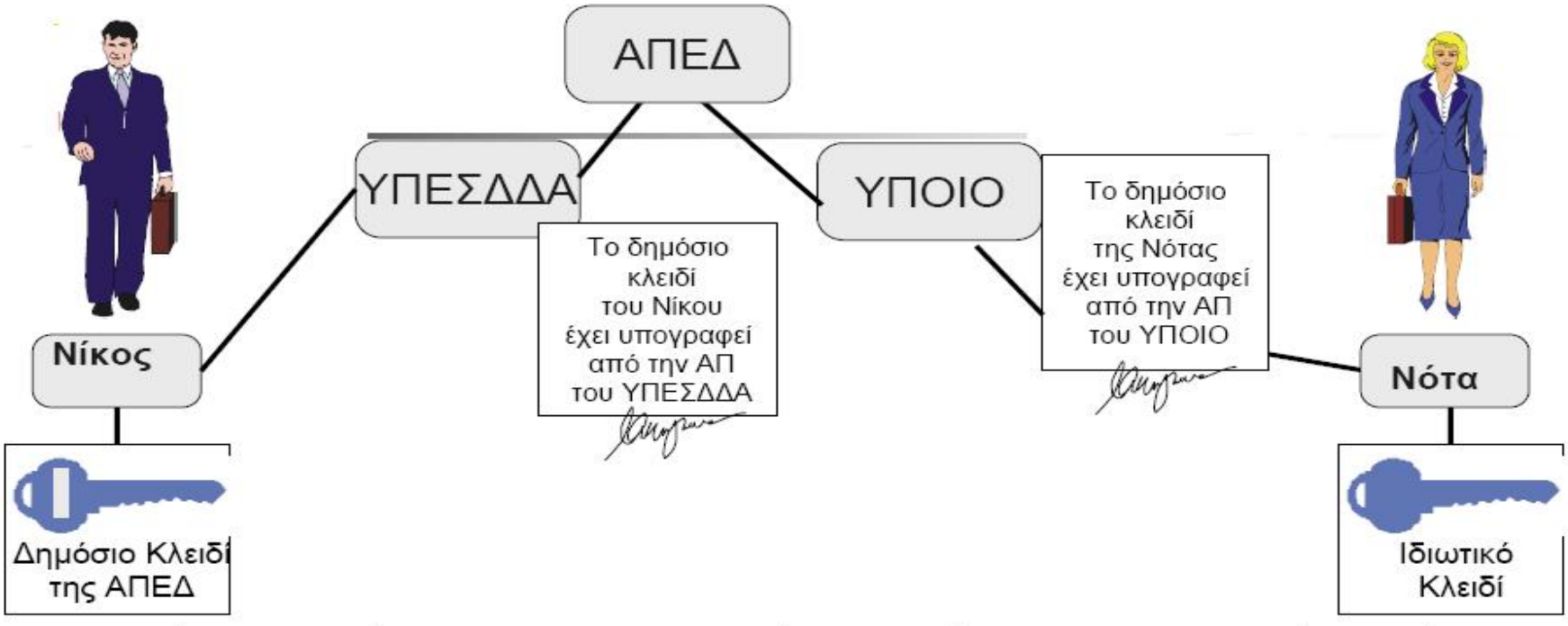
- Ο Φορέας ορίζει τους υπαλλήλους που θα πάρουν ψηφιακό πιστοποιητικό.
- **Εντεταλμένο γραφείο:** αναλαμβάνει τη διεκπεραίωση των αιτημάτων για έκδοση πιστοποιητικών.
- **Αρχές Εγγραφής (Registration Authorities)** ελέγχει τα αιτήματα και εκκινεί τη διαδικασία για την έκδοση του Ψηφιακού Πιστοποιητικού
- **Αρχές Πιστοποίησης (Certification Authorities):** Εκδίδουν δύο (2) ψηφιακών πιστοποιητικά για κάθε χρήστη, τα οποία αποθηκεύονται σε Έξυπνη Κάρτα (smart card).
  - Ψηφιακό πιστοποιητικό για κρυπτογράφηση σύμφωνα με το Προεδρικό διάταγμα 150/2001 και τον κανονισμό (ΦΕΚ 1654/Β 10-11-2006).
  - Ψηφιακό πιστοποιητικό για ψηφιακή υπογραφή – αναγνωρισμένο πιστοποιητικό σύμφωνα με το Προεδρικό διάταγμα 150/2001και τον κανονισμό (ΦΕΚ 1654/Β 10-11-2006).

ΔΟΜΗ ΑΡΧΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΥΠΗΡΕΣΙΑΣ PKI

Οι Οργανικές μονάδες που αποτελούν την Αρχή Πιστοποίησης του ΥΠΕΣΔΔΑ Έχουν καθοριστεί (ΦΕΚ445/Β/02-04-2007)



Η ΑΛΥΣΙΔΑ ΕΜΠΙΣΤΟΣΥΝΗΣ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ



- Η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) εγγυάται μέσω της υπογραφής και των Πιστοποιητικών ΑΠ τόσο του ΥΠΕΣΔΔΑ όσο και του ΥΠΟΙΟ.
- Οπότε υπάρχει αλυσίδα εμπιστοσύνης μεταξύ των τελικών χρηστών των δύο Υπουργείων.

ΔΙΑΔΙΚΑΣΙΑ ΧΡΗΣΗΣ

- Το πιστοποιητικό ψηφιακής υπογραφής και τα κλειδιά είναι στον έλεγχο του χρήστη και αποθηκεύονται στην έξυπνη κάρτα ή σε άλλο ισοδύναμο μέσο.

- Τα δημόσια κλειδιά του χρήστη θα είναι αποθηκευμένα από την Αρχή Πιστοποίησης στο site του Σύζευξις.

- Κάθε χρήστης του δικτύου "ΣΥΖΕΥΞΙΣ" ή πολίτης θα έχει πρόσβαση σε μια πιστοποιημένη σελίδα για να ρωτά αν κάποιο πιστοποιητικό είναι γνήσιο και έγκυρο.

ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ

- Ψηφιακές υπογραφές
  - Επίδειξη λειτουργίας (σε έγγραφο και ηλεκτρονικό ταχυδρομείο)
- Εκτέλεση υπηρεσίας 3ου επιπέδου ηλεκτρονικοποίησης
  - Επιλογή ΚΕΠ διεκπεραίωσης και παραλαβής
- Εκτέλεση υπηρεσίας 4ου επιπέδου ηλεκτρονικοποίησης
  - Πιστοποίηση ταυτότητας χρήστη
  - Επισκόπηση βημάτων διαλειτουργικότητας
    - «Διαλειτουργικότητα και XML στην πράξη»
  - Έλεγχος αποτελέσματος