Σχεδίαση Εφαρμογών και Υπηρεσιών Διαδικτύου
11η Διάλεξη: Ασφάλεια στο Web

Δρ. Απόστολος Γκάμας

Λέκτορας (407/80)

gkamas@uop.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

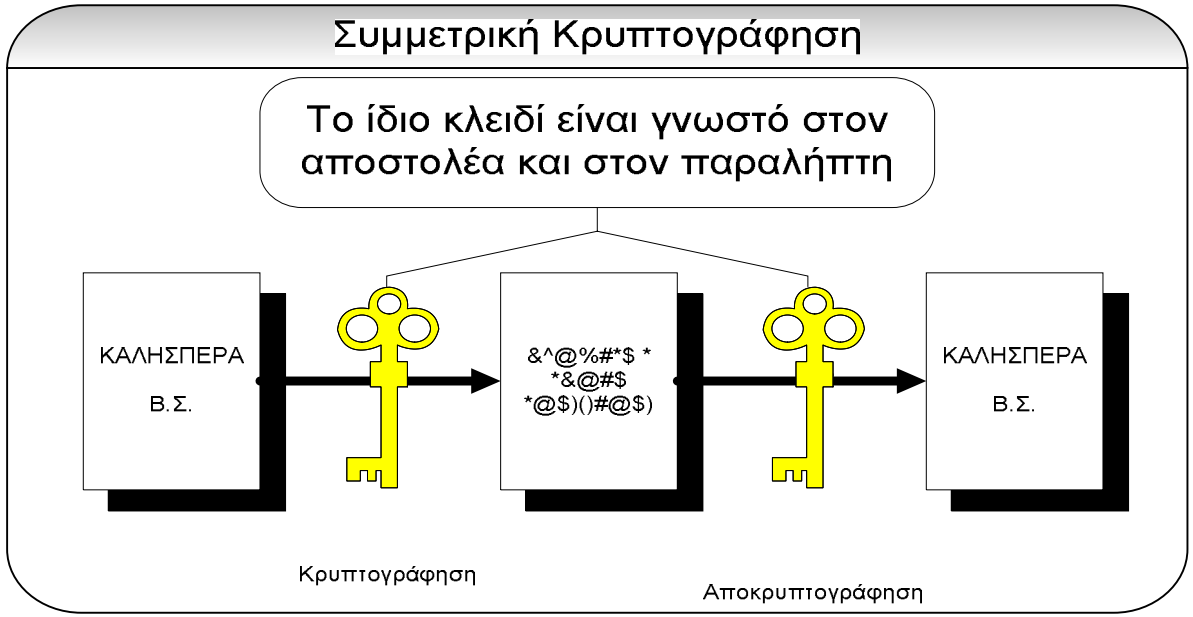
Εισαγωγικά

- Βασικές έννοιες κρυπτογράφησης
- Βασικά στοιχεία από πιστοποιητικά/ certificates
- Κρυπτογράφηση και πιστοποιητικά στα PKI

«Keep private key private!»

Ιδιωτικά Δεδομένα

- Συμμετρικοί αλγόριθμοι κρυπτογράφησης
- Συμμετρικός = ίδιο κλειδί για κρυπτογράφηση & αποκρυπτογράφηση



Συμμετρική Κρυπτογράφηση …

- Ανθεκτικότητα με βάση το είδος του αλγορίθμου και το μέγεθος του κλειδιού
- Χώρος κλειδιού = 2^x, όπου x το μέγεθος του κλειδιού - 40, 56, 128 bit
- Εξαντλητική αναζήτηση κλειδιού για μήνυμα 56-bit Data Encryption Standard
  - 0 έως 72.057.594.037.927.899 περιπτώσεις κλειδιών

Συμμετρική Κρυπτογράφηση

Μέγεθος Κλειδιού	Αριθμός Κλειδιών	Χρόνος για Έλεγχο Κλειδιών (στα 1,6 εκ. κλειδιά/δευτ.)	Χρόνος για Έλεγχο Κλειδιών (στα 1,6 δισεκ. κλειδιά/δευτ.)
40	1.099.511.627.776	8 ημέρες	109 δευτ.
56	72.057.594.037.927.899	1.427 χρόνια	83 ημέρες
64	18.446.744.073.709.600.000	365.338 χρόνια	58.5 χρόνια
128	3,40282E+28	6.7393E+24 χρόνια	1,07829E+21 χρόνια

Μέγεθος κλειδιών και χρόνοι υπολογισμού

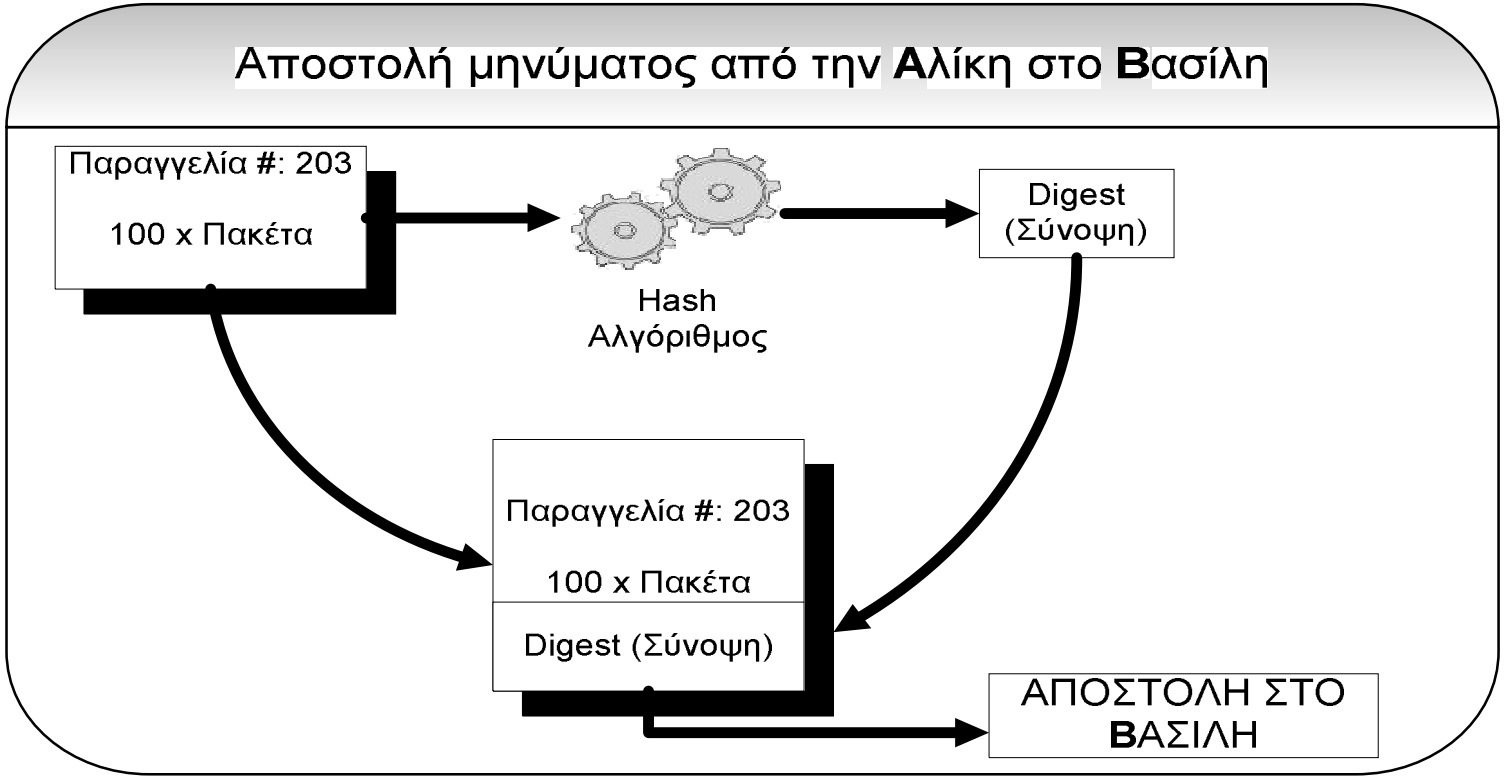
Συμμετρικοί Αλγόριθμοι

- Triple-DES (3DES), είναι ο DES χρησιμοποιημένος τρεις φορές με δύο κλειδιά που δημιουργούν ένα αποτελεσματικό χώρο κλειδιών 112bit ή ο DES με τρία κλειδιά για 168-bit χώρο κλειδιών
- RC2, RC4, RC5, που είναι αλγόριθμοι μεταβλητού κλειδιού από την RSA Data Security
- IDEA το 128-bit σύστημα του PGP
- Skipjack, ένας 80-bit αλγόριθμος των ΗΠΑ για ευαίσθητα αλλά όχι απόρρητα έγγραφα

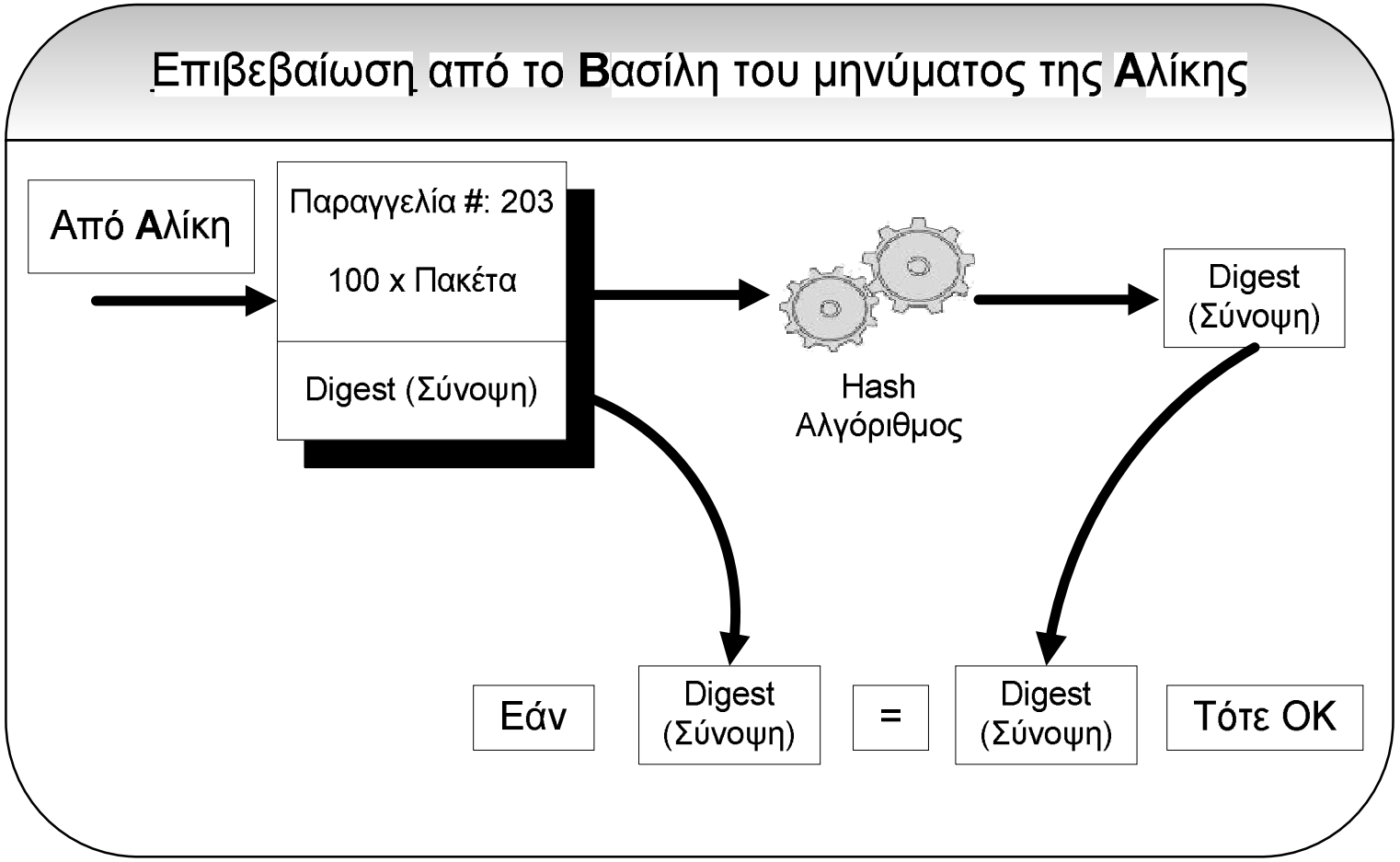
Πιστοποίηση ακεραιότητας δεδομένων…

- Hash συναρτήσεις ή Συναρτήσεις digest
- Digests (συνόψεις) μήκους 128-bit ή 160-bit
- Αντίστοιχο ανάλογο με το δακτυλικό αποτύπωμα - Παρόμοια με τα CRC

Πιστοποίηση ακεραιότητας δεδομένων…



Πιστοποίηση ακεραιότητας δεδομένων ...



Πιστοποίηση ακεραιότητας δεδομένων

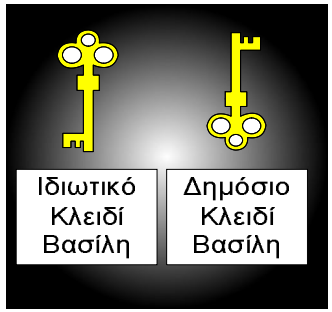
- Παραδείγματα συναρτήσεων Hash
- MD4 της RSA με 128-bit digest
- MD5 της RSA με 128-bit digest
- SHA-1, του NIST (αντίστοιχο του ΕΛΟΤ) που παράγει160-bit hash
- **Το hashing είναι γρήγορη διαδικασία ακόμη και με μεγάλες ποσότητες δεδομένων**

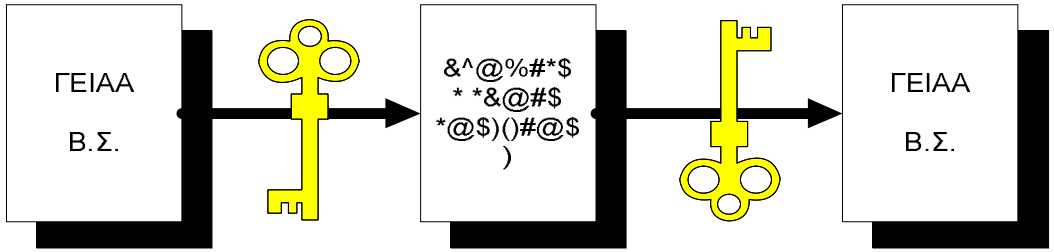
Επιβεβαιώνοντας την Αυθεντικότητα …

- Ασύμμετρα κλειδιά – Κρυπτογράφηση δημόσιου κλειδιού
- Ζεύγη κλειδιών - 1 ιδιωτικό & 1 δημόσιο κλειδί
- Μη αντιστρεπτοί αλγόριθμοι
- **Δεδομένα που κρυπτογραφούνται με το δημόσιο κλειδί αποκρυπτογραφούνται μόνο με το ιδιωτικό**
- **Δεδομένα κρυπτογραφημένα με το ιδιωτικό κλειδί αποκρυπτογραφούνται με το δημόσιο κλειδί μόνο**

Επιβεβαιώνοντας την Αυθεντικότητα …

Ο **Β**ασίλης στέλνει email στην **Α**λίκη,
ώστε αυτή να ξέρει ότι ήρθε από αυτόν και μόνο



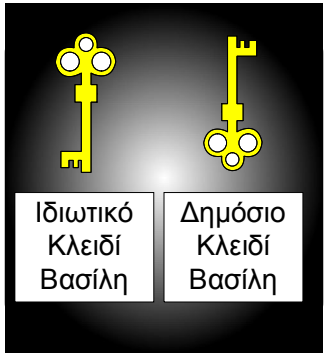


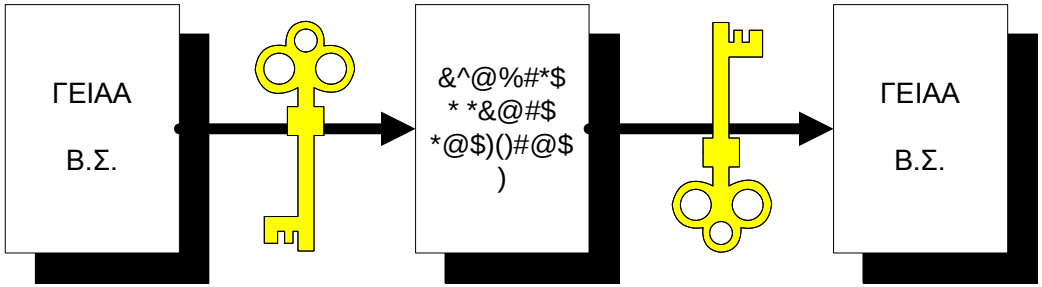
Ο **Β**ασίλης κρυπτογραφεί με το ιδιωτικό κλειδί του

Η **Α**λίκη αποκρυπτογραφεί με το δημόσιο κλειδί του **Β**ασίλη

Επιβεβαιώνοντας την Αυθεντικότητα …

Η **Α**λίκη στέλνει email στο **Β**ασίλη,
ώστε να μπορεί να αναγνωστεί από αυτόν και μόνο





Η **Α**λίκη κρυπτογραφεί με το δημόσιο κλειδί του **Β**ασίλη

Ο **Β**ασίλης αποκρυπτογραφεί με το ιδιωτικό κλειδί του

Επιβεβαιώνοντας την Αυθεντικότητα

- Το πιο δημοφιλές σύστημα κρυπτογράφησης δημοσίου κλειδιού είναι το
- **R**ivest
- **S**hamir
- **A**dleman
- **Η διαδικασία κρυπτογράφησης δημοσίου κλειδιού είναι εξαιρετικά αργή και μη πρακτική για μεγάλες ποσότητες δεδομένων**

Συμμετρική και Ασύμμετρη κρυπτογραφία

- Συμμετρική (Κλασική) Κρυπτογραφία
  - Το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση δεδομένων
  - Τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί
  - Η προστασία του κλειδιού αποτελεί κρίσιμο πρόβλημα
- Ασύμμετρη (Δημόσιου Κλειδιού) Κρυπτογραφία
  - Χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα ιδιωτικό (μυστικό) και ένα δημόσιο, τα οποία σχετίζονται μεταξύ τους με μονόδρομες συναρτήσεις (one-way functions)
  - Τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται αποκλειστικά με το άλλο
  - Μόνο μία φυσική οντότητα γνωρίζει το ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί είναι διαθέσιμο στο κοινό.

Υβριδική Κρυπτογραφία

- Η ασύμμετρη κρυπτογραφία είναι μη αποτελεσματική για την κρυπτογράφηση μεγάλου όγκου δεδομένων, αντίθετα από τη συμμετρική.
- Συνηθισμένη χρήση της ασύμμετρης κρυπτογραφίας είναι η αποστολή ενός συμμετρικού κρυπτογραφικού κλειδιού μέσω ενός ανασφαλούς καναλιού.
- 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.

Πλεονεκτήματα της Κρυπτογραφίας Δημόσιου Κλειδιού

- Τα δημόσια κλειδιά δεν χρήζουν προστασίας
- Τα ιδιωτικά κλειδιά δεν γνωρίζονται η διανέμονται σε τρίτους σε καμία περίπτωση
  - Για να σταλεί ένα εμπιστευτικό μήνυμα, χρησιμοποιείται το δημόσιο κλειδί του παραλήπτη. Μόνο το ιδιωτικό κλειδί που κατέχει ο παραλήπτης μπορεί να το αποκρυπτογραφήσει
  - Για να υπογραφεί ένα μήνυμα χρησιμοποιείται το ιδιωτικό κλειδί του αποστολέα. Οποιοσδήποτε τρίτος μπορεί να επαληθεύσει την υπογραφή με το δημόσιο κλειδί του αποστολέα
- Ελαχιστοποίηση της διαχείρισης κλειδιών – Δεν χρειάζεται κέντρο διανομής κλειδιών.
- Μεγάλος κύκλος ζωής των κλειδιών
- Δίνουν τη δυνατότητα επαλήθευσης της ακεραιότητας δεδομένων

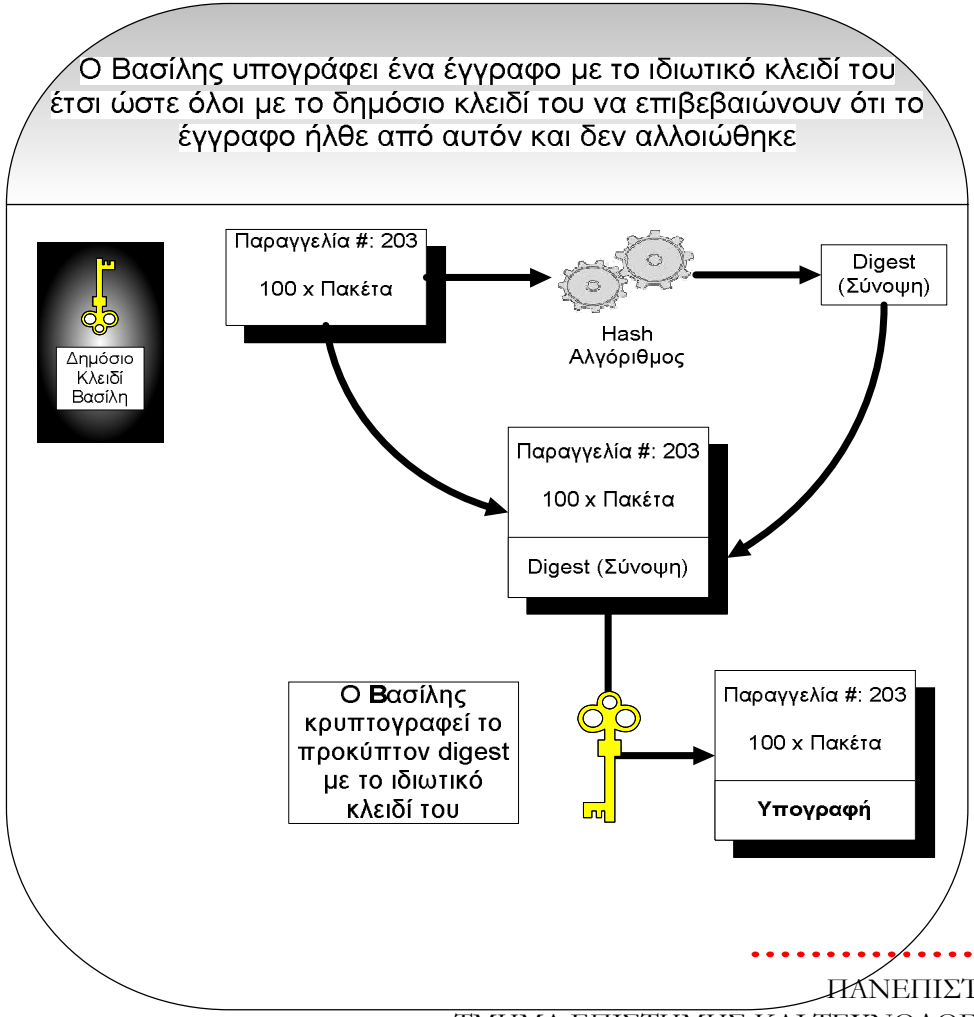
Προβλήματα της Κρυπτογραφίας Δημόσιου Κλειδιού

- Πως επαληθεύεται η ταυτότητα του κατόχου ενός ζεύγους κλειδιών;
- Πως διασφαλίζεται η ιδιωτικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία και τη χρήση τους;
- Πως διανέμονται στο κοινό τα δημόσια κλειδιά έτσι ώστε να διασφαλίζεται η σύνδεση τους με μία φυσική οντότητα;
- Πως τελειώνει ο κύκλος ζωής τους όταν αυτό κριθεί αναγκαίο;
- Διαφαίνεται η ανάγκη ύπαρξης μίας 'Εμπιστης Τρίτης Οντότητας' που διαχειρίζεται 'Ψηφιακά Πιστοποιητικά'.

Ψηφιακές υπογραφές …

- Η διαδικασία δημιουργίας ψηφιακής υπογραφής περιλαμβάνει δύο τεχνολογίες:
- Κρυπτογράφηση δημόσιου κλειδιού
- Hashing

Ψηφιακές υπογραφές …



Ψηφιακές υπογραφές …

- Ο Βασίλης κάνει **hash** στο έγγραφο του και κρυπτογραφεί την προκύπτουσα σύνοψη – **digest** με το ιδιωτικό κλειδί του. Η προκύπτουσα υπογραφή επισυνάπτεται μαζί και το δημόσιο κλειδί του.
- Η Αλίκη λαμβάνει το μήνυμα και κάνει **hash** στο έγγραφο και αποκρυπτογραφεί το μήνυμα με βάση το δημόσιο κλειδί του Βασίλη, εάν τα **digest** είναι ίδια τότε:

Ψηφιακές υπογραφές

- Το έγγραφο είναι άθικτο αφού τα hash ταιριάζουν
- Το μήνυμα πρέπει να ήρθε από το Βασίλη αφού μόνο το δικό της δημόσιο κλειδί μπορεί να αποκρυπτογραφήσει την υπογραφή. Άρα είχε πρόσβαση στο αντίστοιχο ιδιωτικό κλειδί

Ασφάλεια Ψηφιακής Υπογραφής

- Σε τι βασιζόμαστε για τη λειτουργία της ηλεκτρονικής υπογραφής;
  - Ασφαλής αλγόριθμος κρυπτογράφησης
  - Ισχυρές συναρτήσεις σύνοψης
  - Αντιστοίχηση των δημόσιων κλειδιών σε συγκεκριμένες οντότητες
- Προβλήματα;
  - Ο Βασίλης θέλει να πλαστογραφήσει την υπογραφή της Αλίκης
  - Μπορεί να υπογράψει μια επιταγή με το δικό του ιδιωτικό κλειδί και στη συνέχεια να παρουσιάσει το δημόσιο κλειδί του λέγοντας 'Αυτό είναι το κλειδί της Αλίκης'.
  - Εάν οι υπόλοιποι βασισθούν στα λεγόμενά του, η πλαστογράφηση θα είναι επιτυχημένη
  - Συνεπώς χρειάζεται να υπάρχει εμπιστοσύνη απέναντι στην αντιστοίχηση κλειδιού - ταυτότητας
- Η κρυπτογραφία δημόσιου κλειδιού λύνει το πρόβλημα της Διανομής κλειδιών αλλά δημιουργεί το πρόβλημα της αντιστοίχησης κλειδιών.
- Διαφαίνεται ξανά η ανάγκη ύπαρξης μίας 'Εμπιστης Τρίτης Οντότητας'

Ψηφιακά Πιστοποιητικά

- Βεβαιώνουν την ακεραιότητα του Δημόσιου κλειδιού.
- Βεβαιώνουν τη σύνδεση ενός δημόσιου κλειδιού με ένα άτομο ή οργανισμό μέσω της Έμπιστης Τρίτης Οντότητας (Trusted Third Party).
- Ανάλογα με την Αρχή Πιστοποίησης το πιστοποιητικό έχει και διαφορετικό εύρος αναγνώρισης. Συνήθως υπάρχει ιεραρχία πιστοποίησης που ορίζεται από το X.509.
- Από τι αποτελείται ένα ψηφιακό πιστοποιητικό:
  - Κάποια πληροφοριακά στοιχεία για το χρήστη του
  - Το δημόσιο κλειδί του χρήστη
  - Το όνομα μιας Αρχής Πιστοποίησης
  - Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης

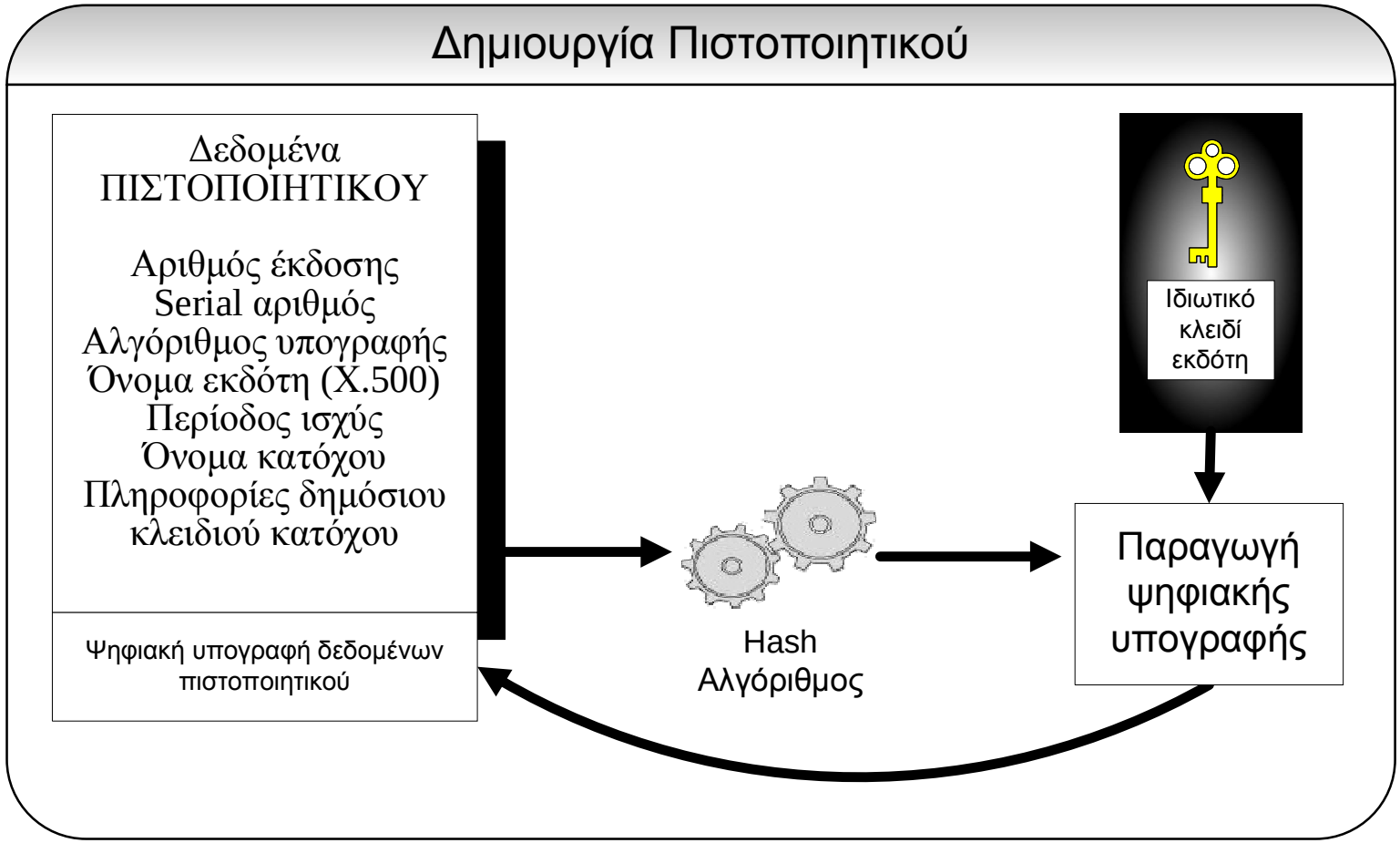
Πλεονεκτήματα Ψηφιακών Πιστοποιητικών

- Δημιουργούν σχέσεις Εμπιστοσύνης μεταξύ οντοτήτων που δεν γνωρίζονται, μέσω της Έμπιστης Τρίτης Οντότητας
- Μπορούν να χρησιμοποιούνται off-line
- Κλιμακώσιμο σχήμα
- Μπορούν να περιέχουν επιπλέον στοιχεία που επιβεβαιώνει ένας τρίτος εγγυητής, για χρήση σε διάφορες εφαρμογές (θυμηθείτε την αυθεντικοποίηση και το έλεγχο πρόσβασης)

Τι περιλαμβάνει το πιστοποιητικό (Certificate)…

- X.509 πιστοποιητικό σε τρεις εκδόσεις (3)
- Αριθμός έκδοσης
- Serial αριθμός
- Αλγόριθμος υπογραφής
- Όνομα εκδότη (X.500)
- Περίοδος ισχύς
- Όνομα κατόχου
- Πληροφορίες δημόσιου κλειδιού κατόχου
- Υπογραφή των δεδομένων του πιστοποιητικού
- Επεκτάσεις (εναλλακτικό όνομα, CRL ..)

Τι περιλαμβάνει το πιστοποιητικό…



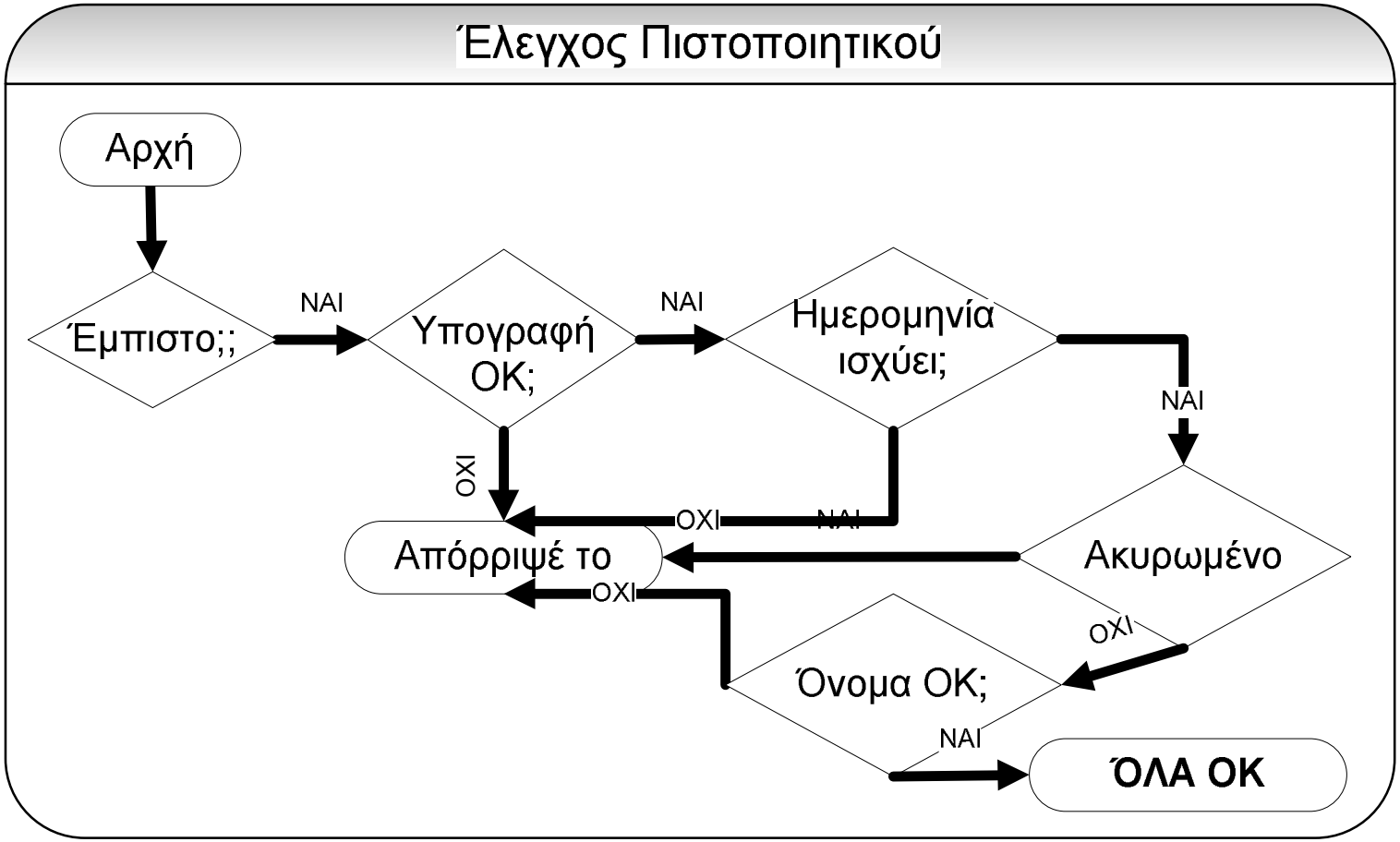
Τι περιλαμβάνει το πιστοποιητικό…

- Το πρότυπο πιστοποιητικό για το Internet δίνεται από το IETF PKIX working group στο:
- http://www.ietf.org/html.charters/pkix-charter.html
- Το πιο σημαντικό έγγραφο είναι το RFC 2459

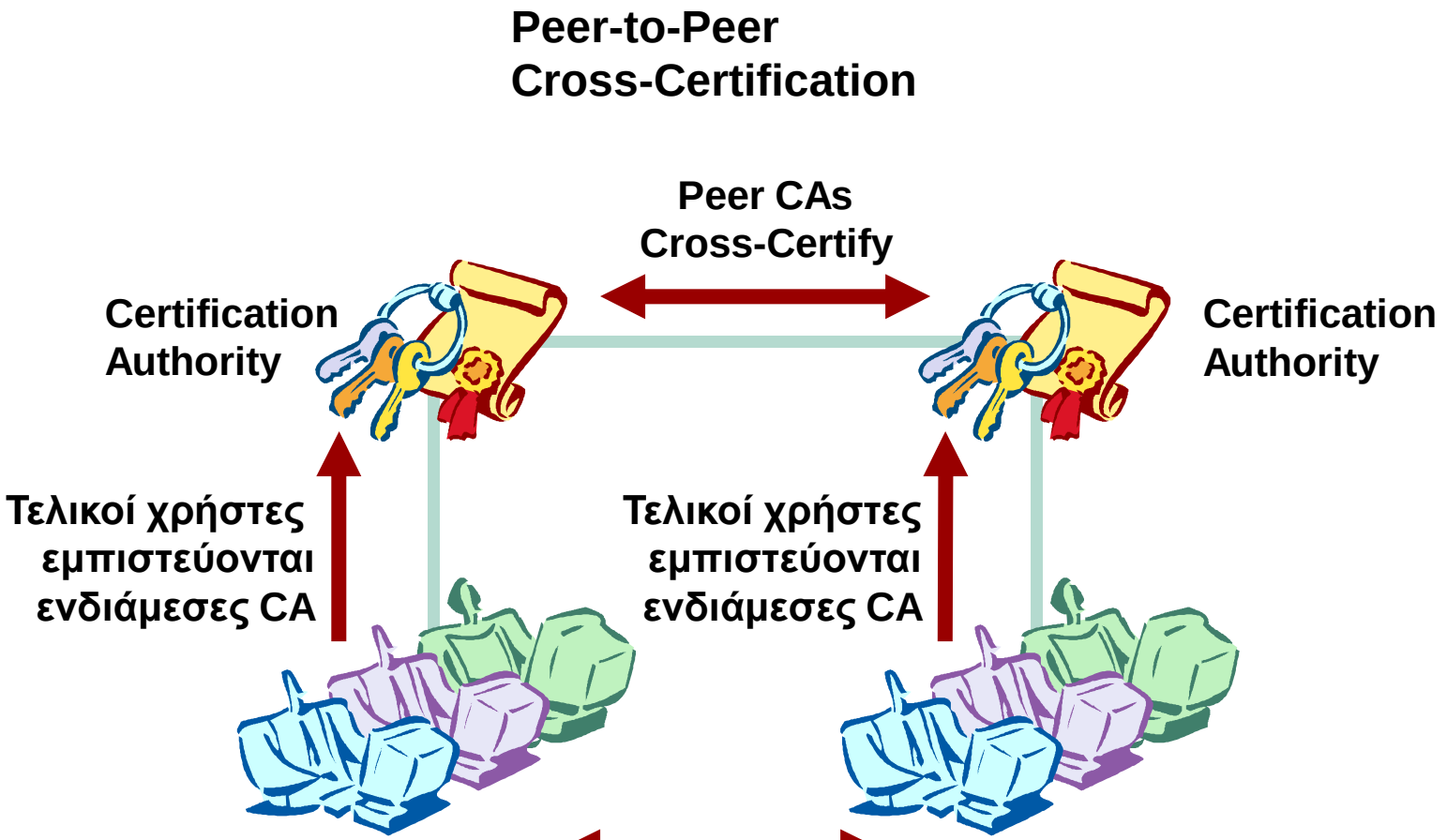
Η εμπιστοσύνη

- Certification Authority
- Principal (user, server, computer-client)
- Έλεγχος ταυτοπροσωπίας
- Δημιουργεί και υπογράφει ένα πιστοποιητικό με ιδιωτικό κλειδί
- Δίνει το πιστοποιητικό στο υποκείμενο
- Η CA ή το υποκείμενο δημοσιοποιεί το πιστοποιητικό του σε όλους τους ενδιαφερόμενους

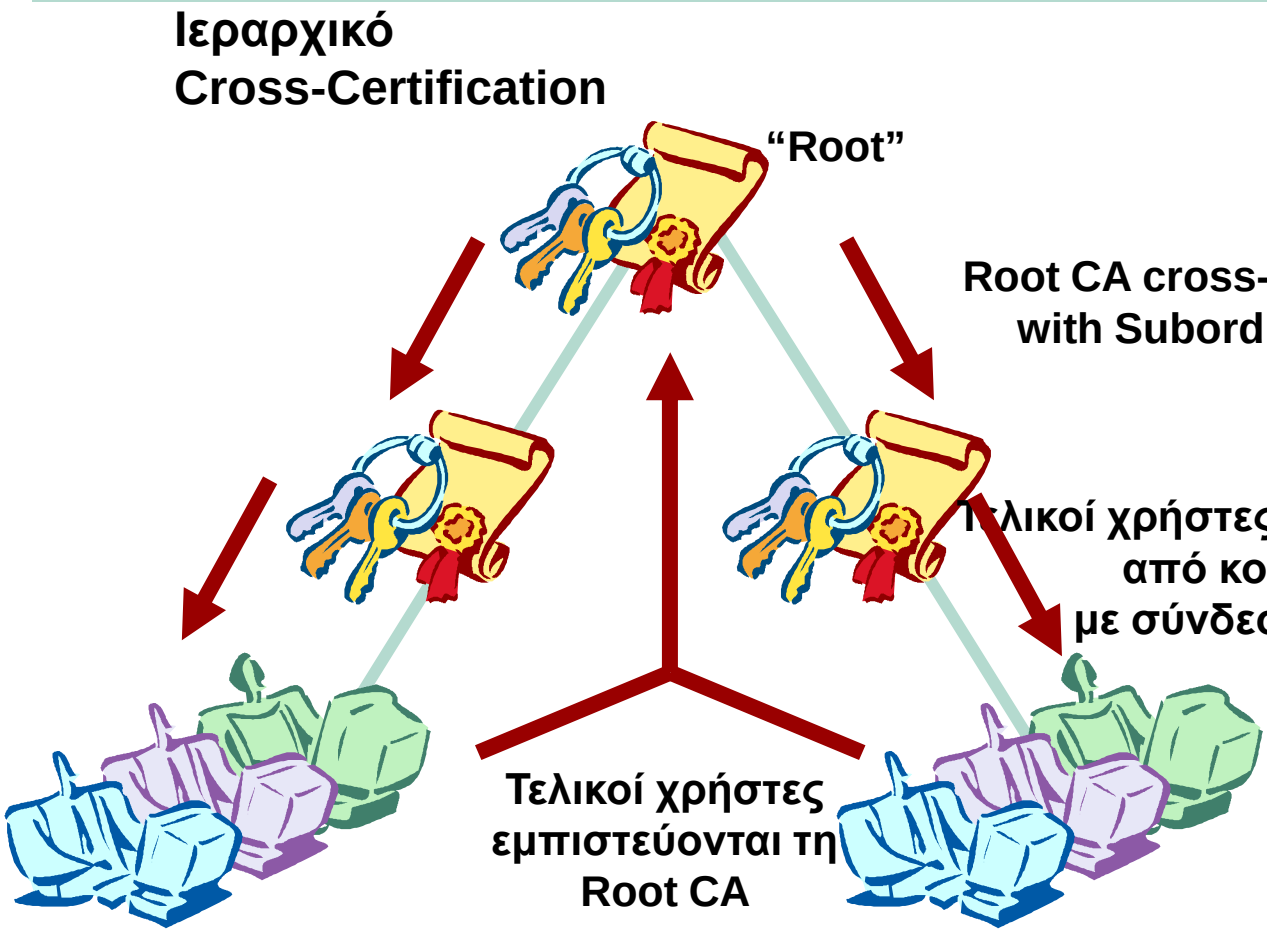
Ο έλεγχος


Έλεγχος Πιστοποιητικού
Αρχή
Έμπιστο;;
ΝΑΙ
Υπογραφή ΟΚ;
ΝΑΙ
Ημερομηνία ισχύει;
ΝΑΙ
ΟΧΙ
ΟΧΙ
ΝΑΙ
Απόρριψέ το
Ακυρωμένο
ΟΧΙ
ΟΧΙ
Όνομα ΟΚ;
ΝΑΙ
ΌΛΑ ΟΚ

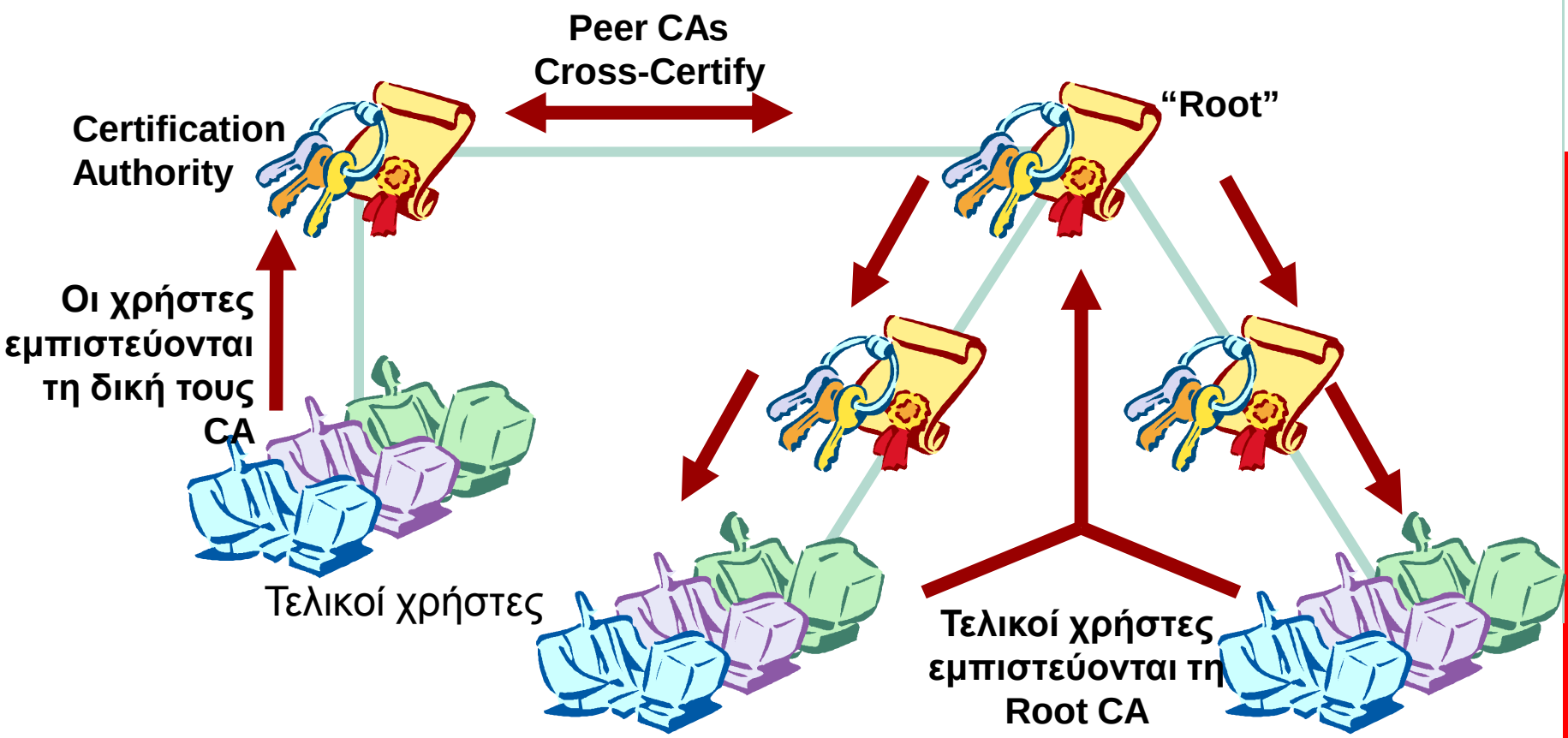
Δικτυακό PKI



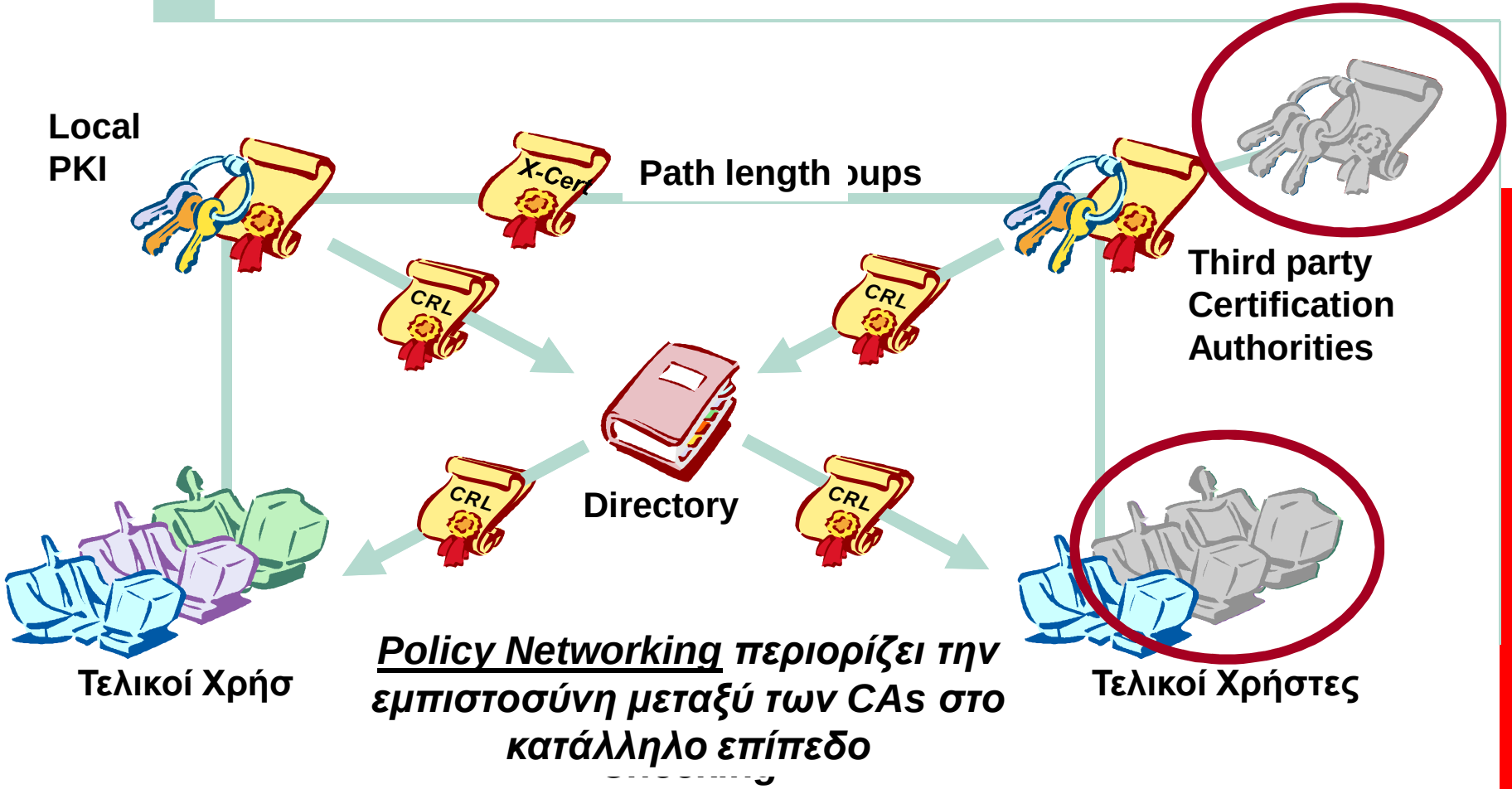
Δικτυακό PKI



Δικτυακό PKI



Δικτυακό PKI



Μύθοι

- Τα πιστοποιητικά ΔΕΝ κάνουν **encryption**
- Τα πιστοποιητικά ΔΕΝ είναι το τέλειο σύστημα αυθεντικοποίησης
- Η **CA** ΔΕΝ έχει το ιδιωτικό κλειδί
- Τα πιστοποιητικά ΔΕΝ κάνουν ότι και τα **web cookies**