

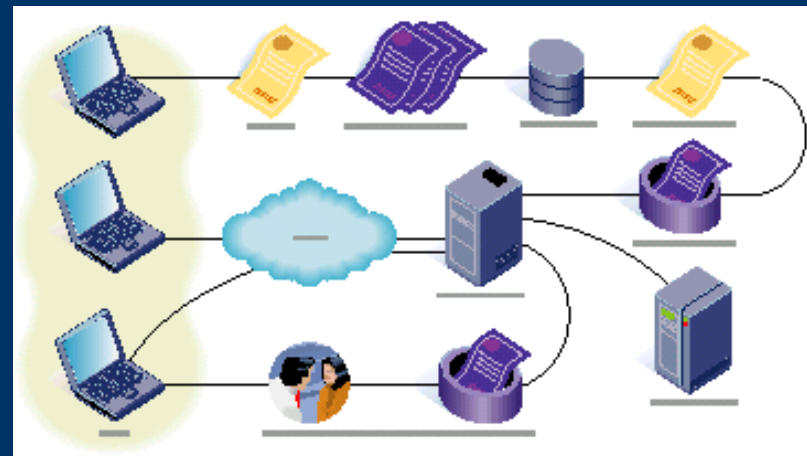


**ΚΡΥΠΤΟΓΡΑΦΙΑ
ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ
ΥΠΟΔΟΜΕΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ
SSL**

Αριστοτέλειο Πανεπιστήμιο, Γενικό Τμήμα

Περιεχόμενα

- ◆ Απαιτήσεις ασφάλειας πληροφορίας
- ◆ Κρυπτογραφία και Πιστοποίηση
- ◆ Υποδομές Δημόσιου Κλειδιού
- ◆ Πρωτόκολλο SSL



Εφαρμογές στο διαδίκτυο

Το διαδίκτυο αποτελεί ένα παγκόσμιο και χαμηλού κόστους μέσο για τη διακίνηση πληροφοριών και την παροχή υπηρεσιών.

Διαδεδομένη χρήση του Διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνία ευαίσθητων δεδομένων:

- τραπεζικές συναλλαγές
- ηλεκτρονικό εμπόριο
- ιατρική πληροφορία

Η ασφάλεια της πληροφορίας αποτελεί σημαντικό ζήτημα για την ηλεκτρονική κοινωνία

Ασφάλεια στο διαδίκτυο

Οι αδυναμίες που παρουσιάζει το διαδίκτυο στο θέμα της ασφάλειας των διακινούμενων πληροφοριών και της ασφαλούς πρόσβασης σε εφαρμογές, οφείλονται στον σχεδιασμό του πρωτοκόλλου TCP/IP.

Οι σχεδιαστές του IP δημιούργησαν ένα απλό και εύκολο στη χρήση πρωτόκολλο, με αποτέλεσμα να μην είναι ασφαλές.

Τα ασφαλή συστήματα πρέπει να βασίζονται:

- ♦ στην αυθεντικοποίηση των χρηστών και
- ♦ στην κρυπτογραφία

Το κλασικό IP δεν έχει τέτοιες ιδιότητες, γιατί αυτά τα συστήματα είναι πολύπλοκα στη χρήση και ακριβά υπολογιστικά.

Ασφάλεια στο διαδίκτυο

- Σχεδιάστηκε με γνώμονα τη βελτιστοποίηση του στις διασυνδέσεις των δικτύων και την κοινή εκμετάλλευσή τους και όχι στην παρεχόμενη ασφάλεια
- Ετερογένεια των δικτύων και το τεράστιο μέγεθός του
- Εύκολη χωρίς περιορισμούς πρόσβαση χρηστών
- Έλλειψη συνολική πολιτική ελέγχου προσπέλασης

Είδη Επιθέσεων στο Διαδίκτυο

- ◆ Υποκλοπή (Eavesdropping)

Η μεταφερόμενη πληροφορία παραμένει ακέραιη, όχι όμως η εμπιστευτικότητά της

Κρυπτογραφία

- ◆ Παραποίηση (Tampering)

Η πληροφορία που μεταφέρεται μπορεί να αλλαχθεί ή να αντικατασταθεί από κάποιον τρίτο

Ψηφιακές Υπογραφές

- ◆ Πλαστοπροσωπία (impersonation)

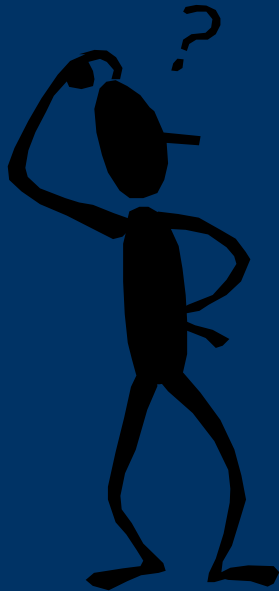
Η πληροφορία μεταφέρεται σε μη εξουσιοδοτημένο υπολογιστή που παριστάνει το νόμιμο παραλήπτη
Προσποίηση (spoofing)

Ψηφιακά Πιστοποιητικά

- ◆ Άρνηση παροχής υπηρεσιών

Ερώτηση

Πρέπει να χρησιμοποιείται το διαδίκτυο για τη διακίνηση ευαίσθητων πληροφοριών;



ΝΑΙ, αν ληφθούν κατάλληλα μέτρα ασφάλειας
(αυθεντικοποίηση, κρυπτογράφηση)

Απαιτήσεις ασφάλειας πληροφορίας

Προστασία της **ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ**

... ότι η πληροφορία θα διατηρηθεί ιδιωτική (data confidentiality)

Προστασία της **ΑΚΕΡΑΙΟΤΗΤΑ**

... ότι η πληροφορία δεν περιέχει λάθη (data integrity)

Προστασία της **ΔΙΑΘΕΣΙΜΟΤΗΤΑ**

... ότι η πληροφορία είναι συνεχώς διαθέσιμη

Απαιτήσεις ασφάλειας πληροφορίας

ΑΔΥΝΑΜΙΑ ΑΠΑΡΝΗΣΗ (non-repudiation)

... ότι ένας χρήστης δεν μπορεί να αρνηθεί τη συμμετοχή του σε μια συναλλαγή που έκανε

**Έλεγχος γνησιότητας της ταυτότητας
(identification and authentication)**

**Έλεγχος προσπέλασης και εξουσιοδοτήσεις
(access control and authorizations)**

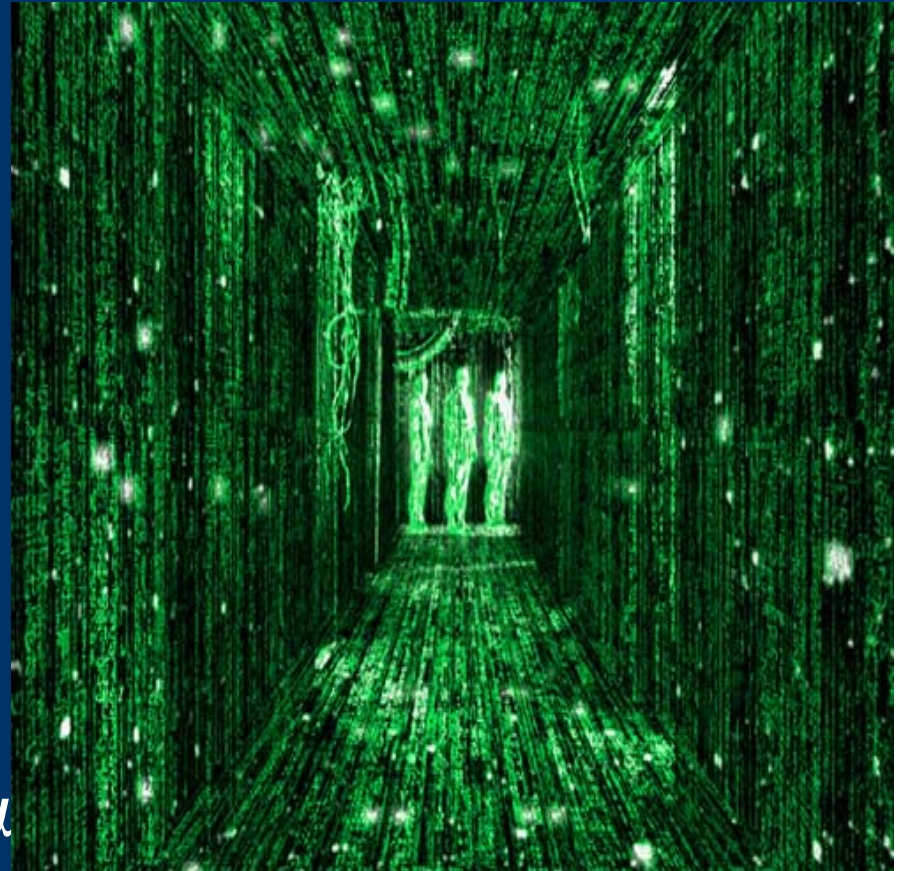
Μέθοδοι και τεχνικές προστασίας

- ⊗ Κρυπτογράφηση για αυθεντικοποίηση χρηστών
- ⊗ Κρυπτογραφημένη μεταφορά δεδομένων
- ⊗ Έλεγχος πρόσβασης
 - Συνθηματικά
 - Ψηφιακές υπογραφές
- ⊗ Ασφαλή δικτυακά πρωτόκολλα

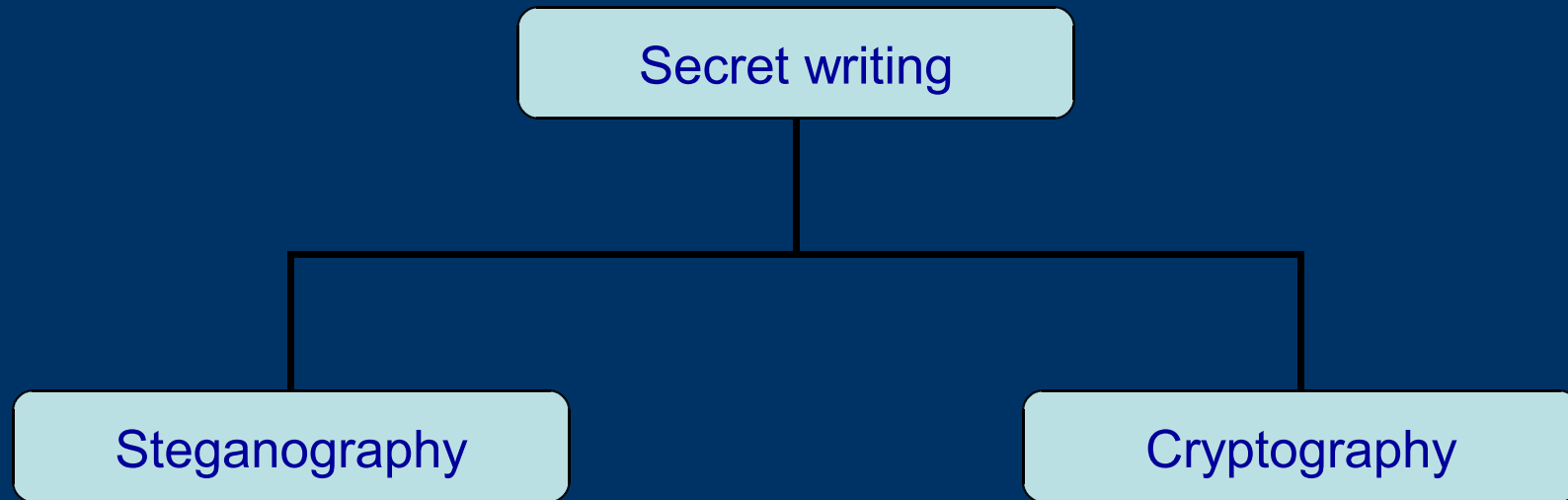


Χρήστες της Κρυπτογραφίας

- Κυβερνήσεις
- Στρατός
- Χρηματιστηριακή Οργανισμοί
- Μεγάλες Εταιρείες (Παραδοσιακό και Ηλεκτρονικό Εμπόριο)
- Νοσοκομειακά Ιδρύματα

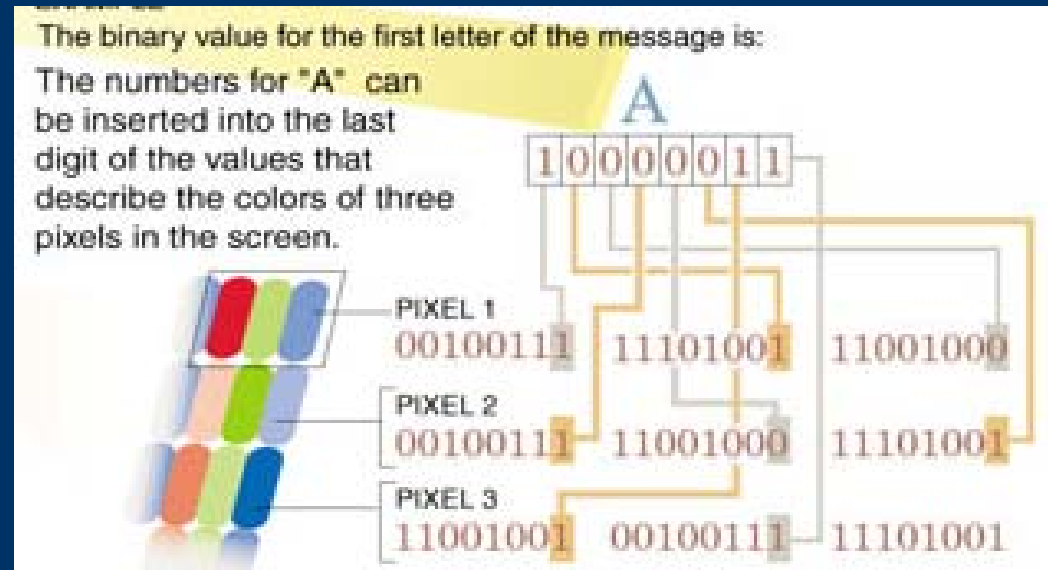


Secret Writing



Steganography

- Steganography – covered writing – is an art of hiding information
- Popular contemporary steganographic technologies hide information in images



New York Times, August 3rd, 2001

http://www.nytimes.com/images/2001/10/30/science/sci_STEGO_011030_00.jpg

Κρυπτογραφία

- Confidentiality (Εμπιστευτικότητα)
 - Steganography (Στεγανογραφία)
 - Απόκρυψη Μηνύματος (π.χ σε μια εικόνα)
 - Encryption (Κρυπτογράφηση) →
 - `encr_algorithm(μήνυμα, κλειδί)` ciphertext
- Authentication (Αυθεντικοποίηση)
 - Identification (Ταυτοποίηση)
 - Με ποιόν μιλάω?
 - Message Authentication (Αυθεντικοποίηση Μηνύματος)
 - Ποιός έφτιαξε το μήνυμα?
 - Digital Signature (Ψηφιακή Υπογραφή)
 - Απόδειξη σε τρίτη οντότητα περί του ποιός έφτιαξε το μήνυμα

Κρυπτογραφία

Εμπιστευτικότητα

«Μεταμφιέζει» ένα μήνυμα/αρχείο έτσι ώστε μόνο ο σωστός παραλήπτης να μπορεί να το διαβάσει.

Παρέχει προστασία με:

- Κρυπτογράφηση: μετατρέπει το αρχικό κείμενο (plaintext) σε κρυπτογραφημένο (ciphertext)
- Αποκρυπτογράφηση: μετατρέπει το κρυπτογραφημένο κείμενο (ciphertext) στην αρχική μορφή του (plaintext)

Κρυπτογραφικός αλγόριθμος (cipher): μαθηματική συνάρτηση που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση

Κλειδί (Key): ένας αριθμός που χρησιμοποιείται μαζί με τον αλγόριθμο.

Η Κρυπτογραφία δίνει λύση στα εξής προβλήματα :

- Ασφαλή επικοινωνία
 - Ταυτοποίηση και πιστοποίηση
 - Κοινοποίηση μυστικής πληροφορίας
 - Ηλεκτρονικό Εμπόριο
 - Ηλεκτρονικά πιστοποιητικά
 - Ασφαλή πρόσβαση σε υπολογιστικά συστήματα
-
-

Παλιότεροι Αλγόριθμοι

- Αλγόριθμος Αντικατάστασης (Καίσαρα, Vigenere)
- Αλγόριθμος Μετάθεσης (χρήση γεωμετρικών σχημάτων)

Caesar Cipher

- Substitution cipher
- Every character is replaced with the one three to right

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

S E C U R I T Y A N D P R I V A C Y

➔ V H F X U L W B D Q G S U L Y D F B



Ιστορία

2ος Παγκόσμιος
Πόλεμος

Αίνιγμα



ΣΤΙΣ ΜΈΡΕΣ ΜΑΣ...

- Είδη κρυπτογράφησης:
 - Συμμετρικού Κλειδιού ή Μυστικού Κλειδιού (Symmetric-Key)
 - Δημοσίου Κλειδιού (Public-Key)



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.

Είδη Κρυπτογραφίας

- ➔ Συμμετρική (Ιδιωτικού κλειδιού) - DES (Data Encryption Standard), Triple DES, RC2, Rivest, RC4, Rivest, RC5, Rivest, IDEA (International Data Encryption Algorithm), Lai, Massey
 - ➔ Μη Συμμετρική (Δημόσιου κλειδιού) - RSA Rivest, Shamir, Adleman, Diffie-Hellman
 - ➔ Περίληψεις μηνυμάτων (Hash Functions) - SHA & SHA-1 Secure Hash Algorithm, MD2, MD4, MD5, Rivest
-
-

Συμμετρικού Κλειδιού

- Κυριότερος Αλγόριθμος:
DES (Data Encryption Standard)

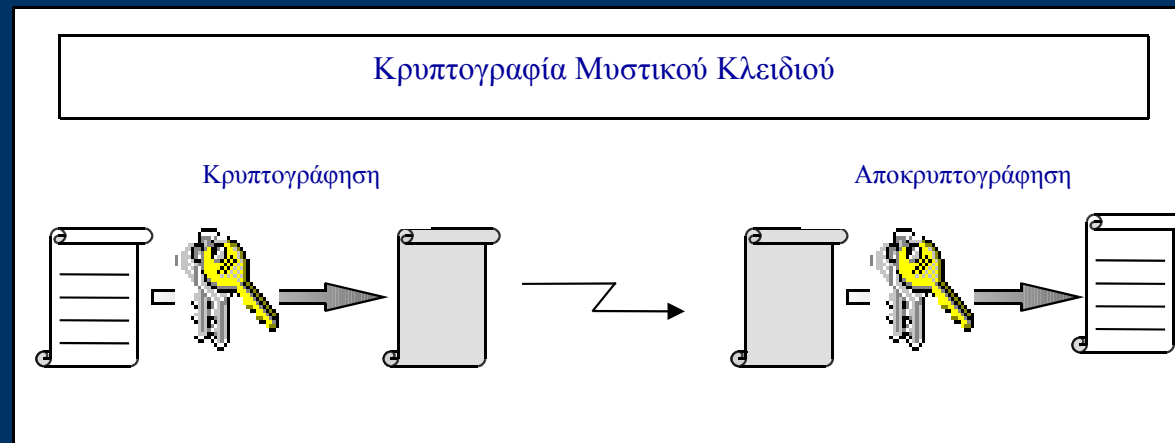
Πλεονέκτημα: Ταχύτητα

Μειονέκτημα: Κατανομή Κλειδιών

Συμμετρική Κρυπτογραφία

Κρυπτογραφία Μυστικού Κλειδιού ή Συμμετρική

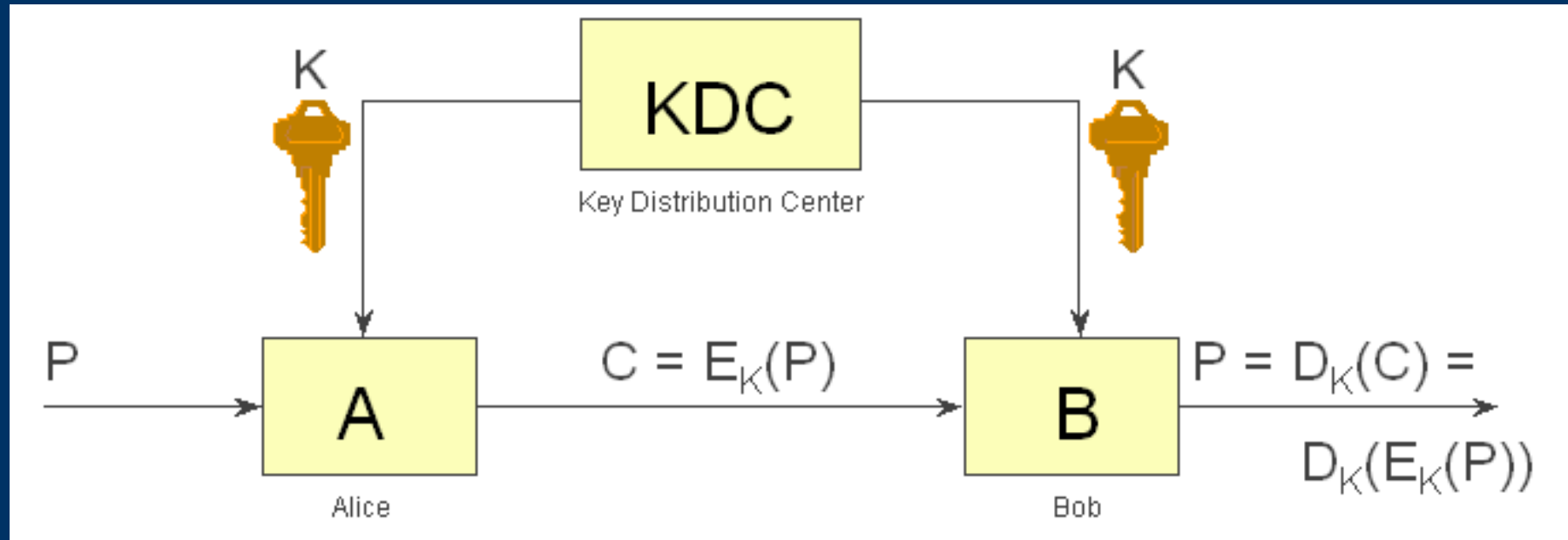
- το ίδιο κλειδί χρησιμοποιείται τόσο για τη κρυπτογράφηση όσο και για την αποκρυπτογράφηση του μηνύματος



Ζητήματα

- Ανταλλαγή μυστικού κλειδιού
- Αυθεντικοποίηση αποστολέα και παραλήπτη

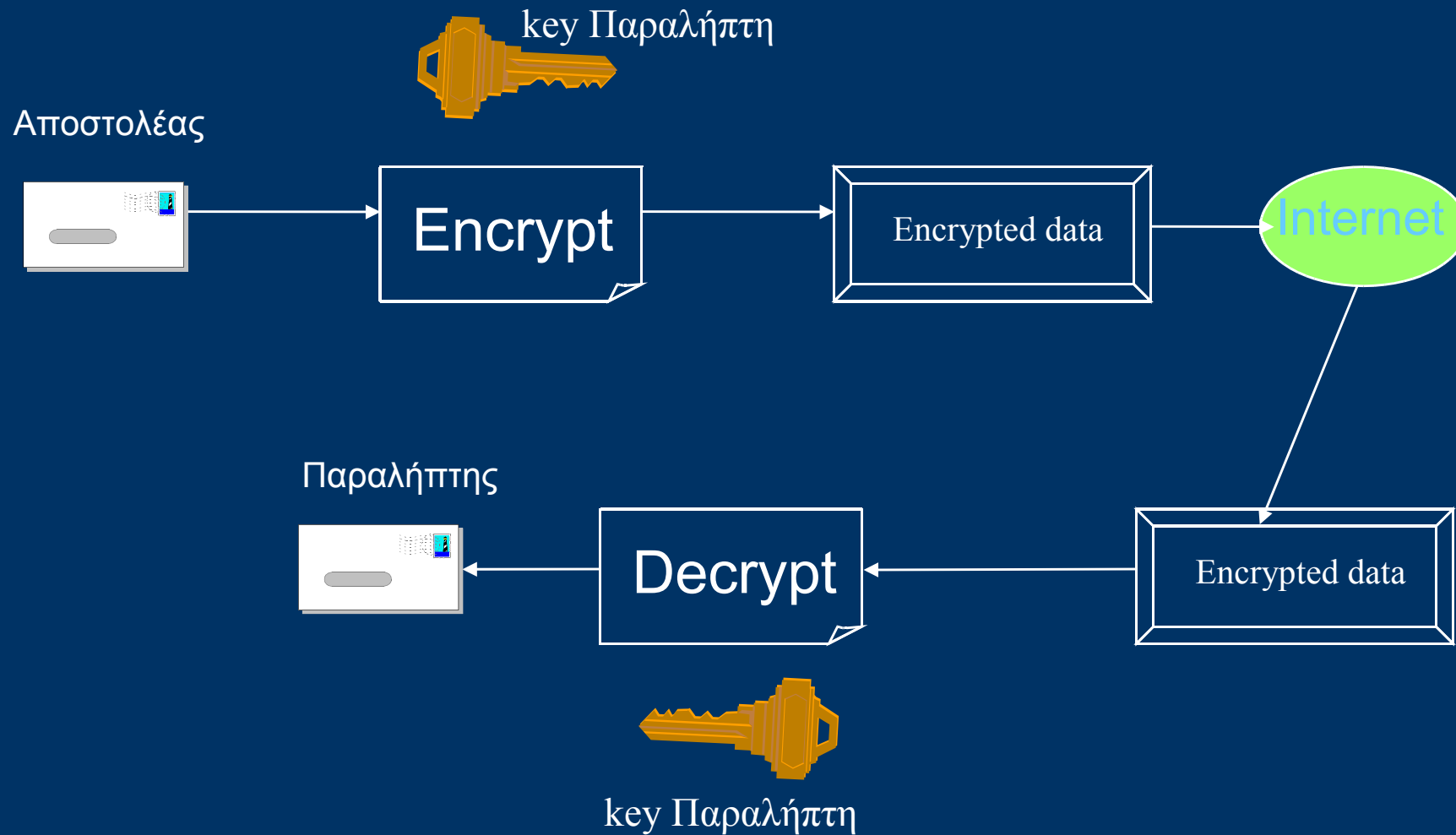
Συμμετρική Κρυπτογραφία



Γνωστοί Συμμετρικοί αλγόριθμοι:

- DES, Triple-DES
- Blowfish, SAFER, CAST
- RC2, RC4 (ARCFOUR), RC5, RC6

Συμμετρική Κρυπτογραφία

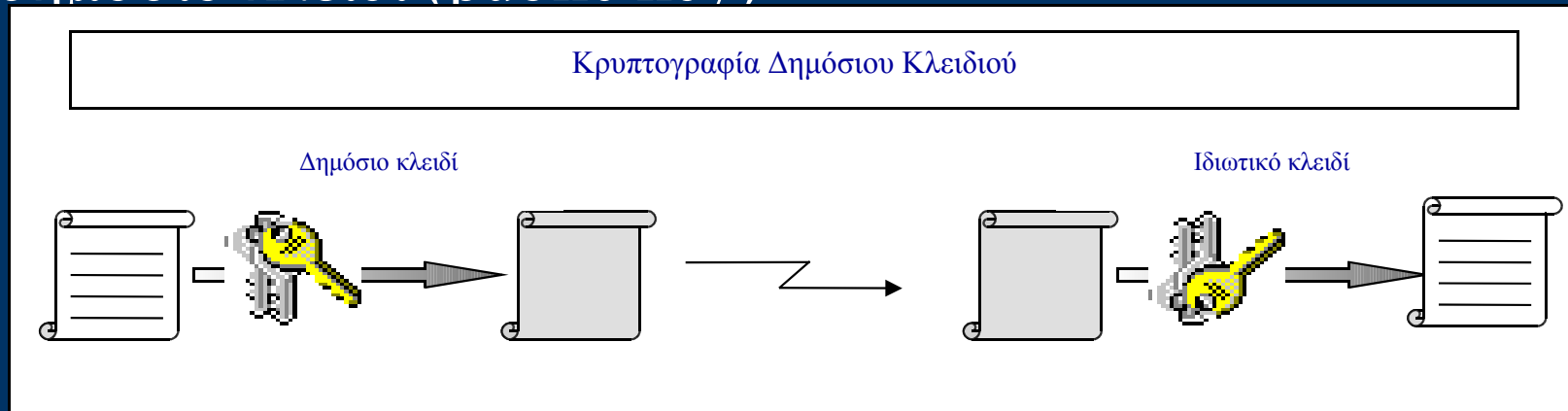


Ασύμμετρη Κρυπτογραφία

Κρυπτογραφία Δημόσιου Κλειδιού ή Ασύμμετρη

Αντικαθιστά το κοινό μυστικό κλειδί με ένα ζεύγος κλειδιών

- ιδιωτικό κλειδί (private key)
- δημόσιο κλειδί (public key)

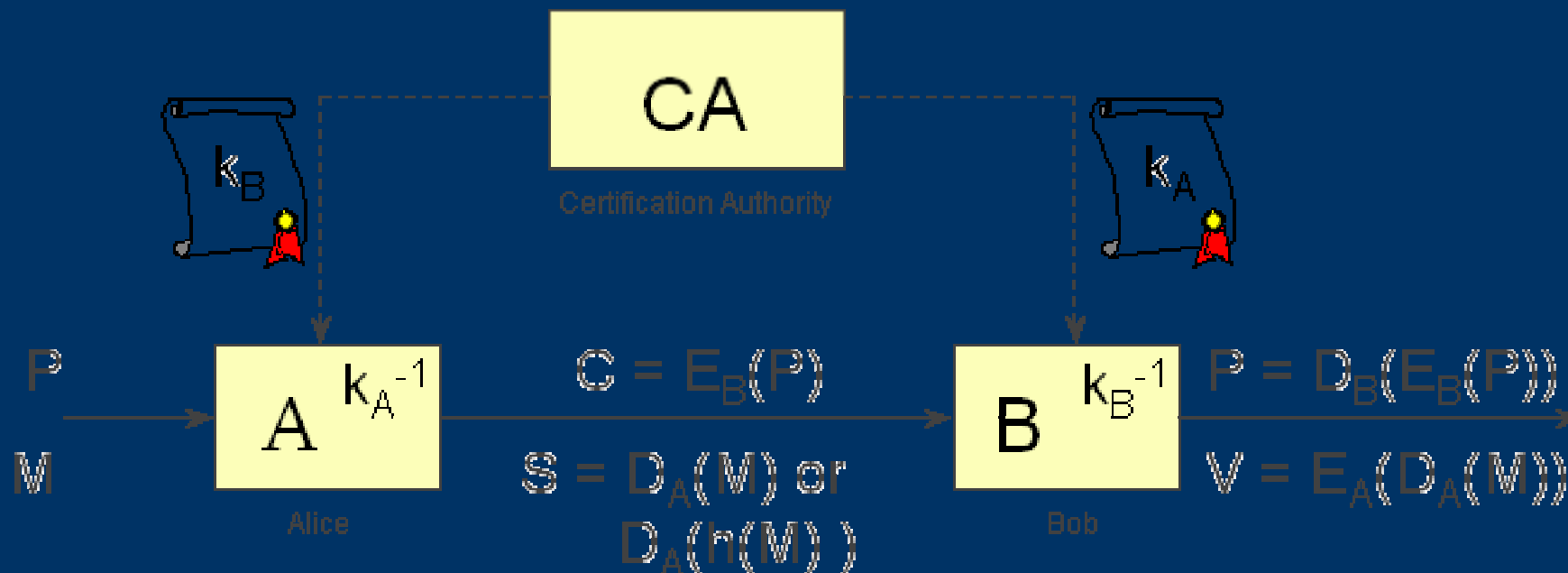


Είναι υπολογιστικά αδύνατο να υπολογιστεί το κλειδί της αποκρυπτογράφησης από τη γνώση του κλειδιού κρυπτογράφησης και του αλγορίθμου που χρησιμοποιήθηκε

Δημοσίου Κλειδιού

- Περιλαμβάνει τη χρήση δυο κλειδιών:
 - ενός δημοσίου κλειδιού (public key) και
 - ενός προσωπικού κλειδιού (private key).
 - Τα δεδομένα κρυπτογραφούνται με το δημόσιο κλειδί του παραλήπτη και αποστέλλονται.
 - Όταν παραληφθούν αποκρυπτογραφούνται με το προσωπικό κλειδί του παραλήπτη.
-
-

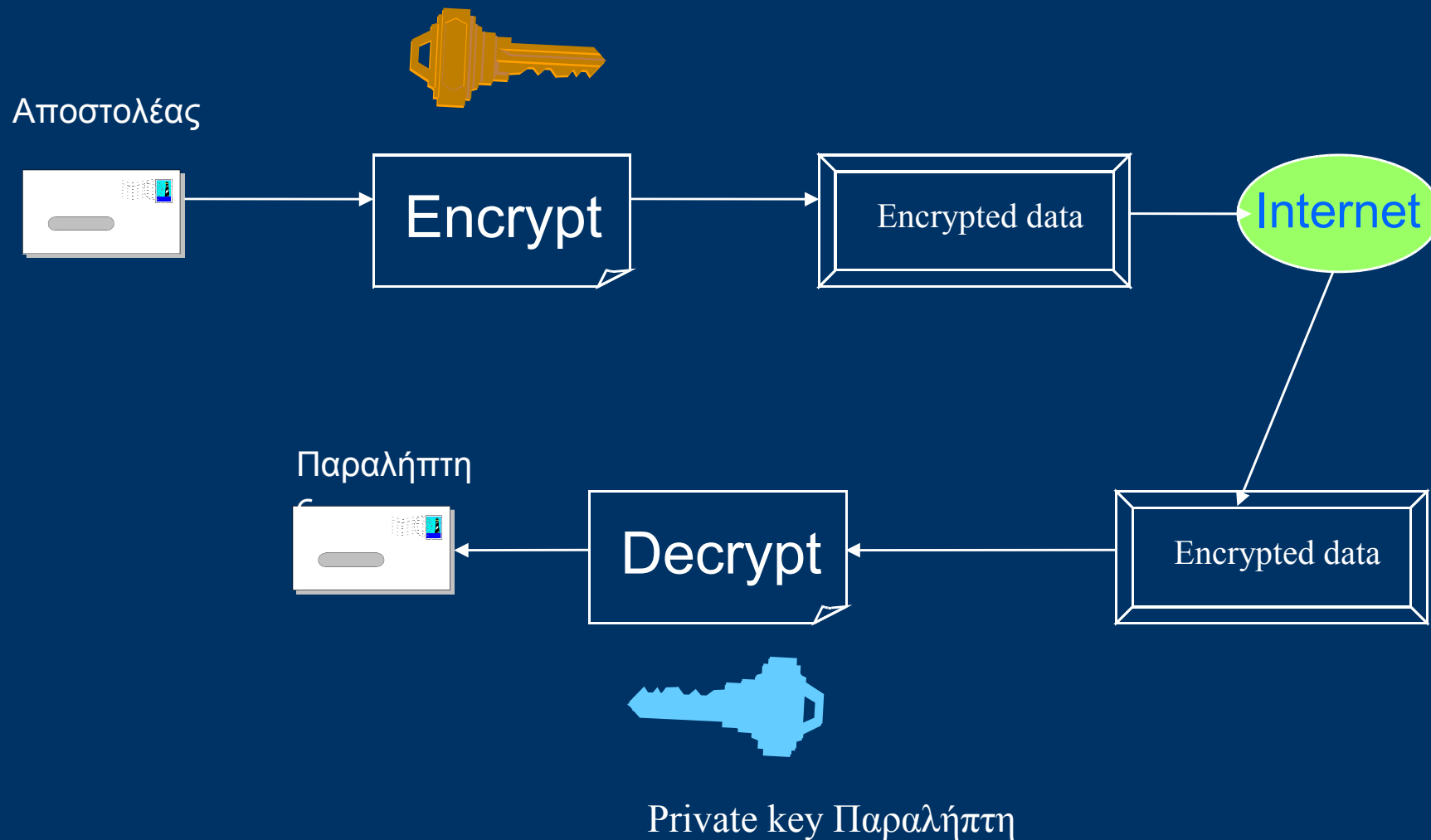
Κρυπτογραφία Δημόσιου Κλειδιού



Γνωστοί αλγόριθμοι Δημόσιου Κλειδιού

- RSA
- Diffie-Hellman Key Exchange
- ElGamal, Digital Signature Standard (DSS)

Ασύμμετρη Κρυπτογραφία



Δημοσίου Κλειδιού

- Κυριότερος Αλγόριθμος: RSA.

Πλεονέκτημα:

- το δημόσιο κλειδί διανέμεται ελεύθερα με αποτέλεσμα την εύκολη σύσταση ασφαλών καναλιών επικοινωνίας μεταξύ δυο απομακρυσμένων χρηστών.
 - Ψηφιακές Υπογραφές
-
-

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.

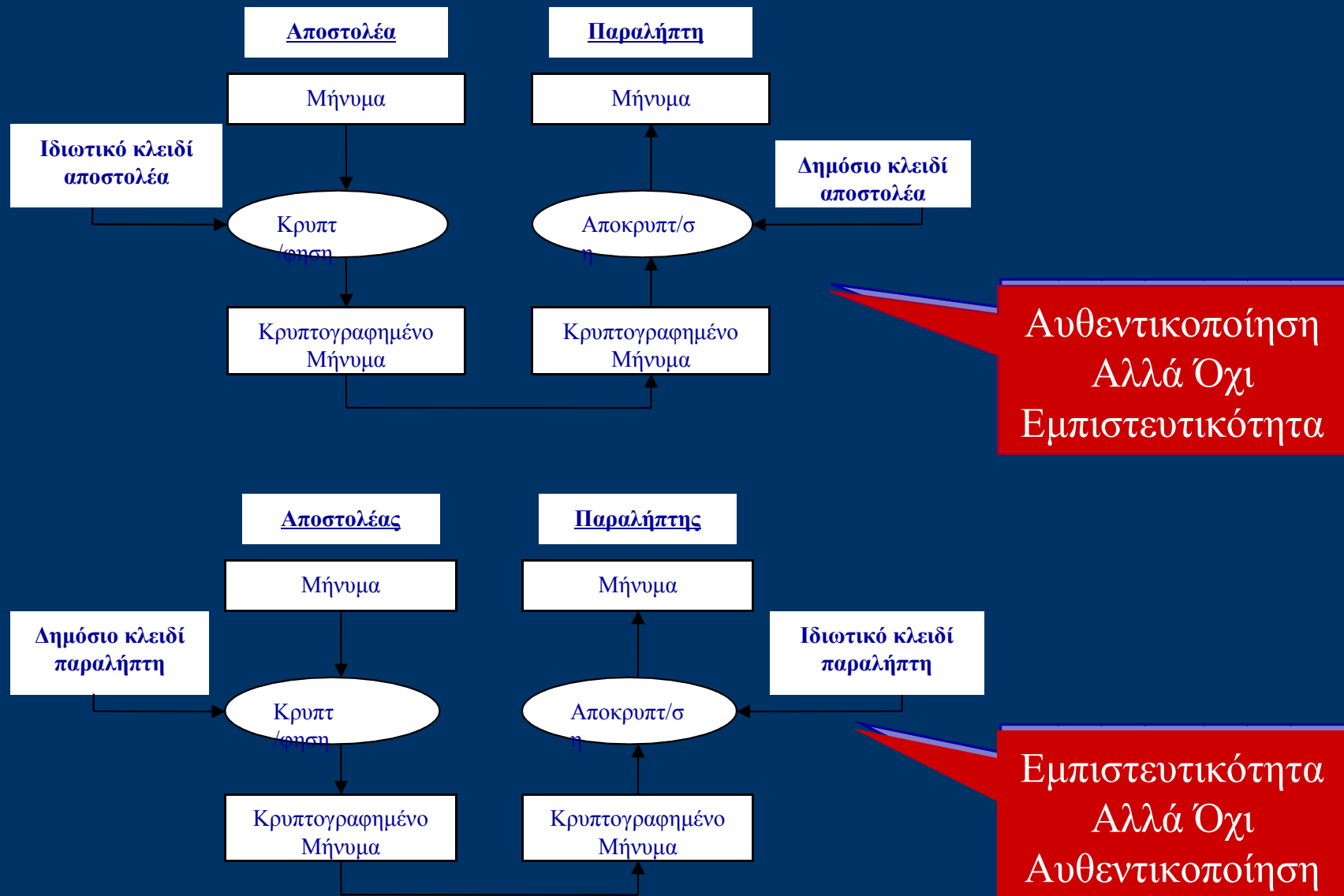
Πλεονεκτήματα της Κρυπτογραφίας Δημόσιου Κλειδιού

- 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’.

Διαφορετικές χρήσεις κλειδιών



Άλλοι Αλγόριθμοι

Μυστικού Κλειδιού

- **DES (Data Encryption Standard)** - IBM 1970, 56 bit key
- **Triple-DES** - 128 bit key
- **IDEA (International Data Encryption Algorithm)** - Swiss Federal Institute of Technology 1991, 128 bit key
- **RC2, RC4** - Ron Rivest. Υποστηρίζουν κλειδιά μεταβλητού μεγέθους
- **AES** - NIST 2001, 256 bit key. Θα αντικαταστήσουν τους DES

Δημόσιου κλειδιού

- **Diffie Hellman** - 1976
- **RSA** - Rivest, Shamir, Adleman 1977

Μέγεθος Κλειδιών

- Η ανθεκτικότητα της κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών που χρησιμοποιούνται παρά από τους αλγόριθμους.
- Το μέγεθος των κλειδιών μετριέται σε bits.
- Η ανθεκτικότητα της κρυπτογράφησης είναι ανάλογη του μεγέθους των κλειδιών.
 - Π.χ., η κρυπτογράφηση 128-bit RC4 είναι 3078 φορές ανθεκτικότερη από την 40-bit RC4.

Μέγεθος Κλειδιών

- Διαφορετικοί αλγόριθμοι απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.
- Π.χ. για το ίδιο περίπου επίπεδο ανθεκτικότητας χρειάζεται:
 - κλειδί μεγέθους τουλάχιστον 512 bits με κρυπτογράφηση RSA
 - κλειδί μεγέθους 64 bits με συμμετρικούς αλγορίθμους.

Εφαρμογές ασύμμετρης κρυπτογραφίας I

Διανομή συμμετρικού κλειδιού

- Ο αποστολέας κρυπτογραφεί το αρχικό κείμενο με το μυστικό κλειδί.
 - Κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη τα
 - μυστικό κλειδί
 - μήνυμα
- Ψηφιακός Φάκελος (Digital Envelope)
- Ο παραλήπτης με το ιδιωτικό του κλειδί, αποκτά το μυστικό κλειδί, το εφαρμόζει στο μήνυμα, ώστε να ανακτήσει το αρχικό κείμενο.

Εφαρμογές ασύμμετρης κρυπτογραφίας II

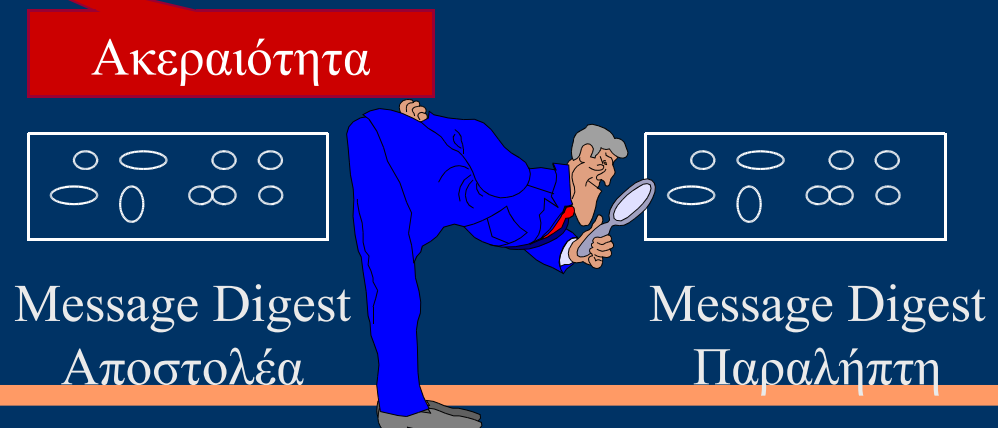
Ψηφιακές Υπογραφές (Digital Signatures)

Είναι μια τεχνική που χρησιμοποιεί το ιδιωτικό κλειδί μιας οντότητας για τη κρυπτογράφηση του **message digest** που υπολογίζεται από το μήνυμα.

Message Digest Algorithms - Αλγόριθμοι που εφαρμόζουν μια μονόδρομη συνάρτηση κατακερματισμού (Hash Function) στα δεδομένα εισόδου και παράγουν ένα σταθερό αριθμό από bits (message digest) μοναδικό για κάθε μήνυμα.

- ◆ MD2-4-5 128 bits
- ◆ SHA 160 bits

Στον παραλήπτη: Σύγκριση



Ψηφιακές υπογραφές - Ορισμός

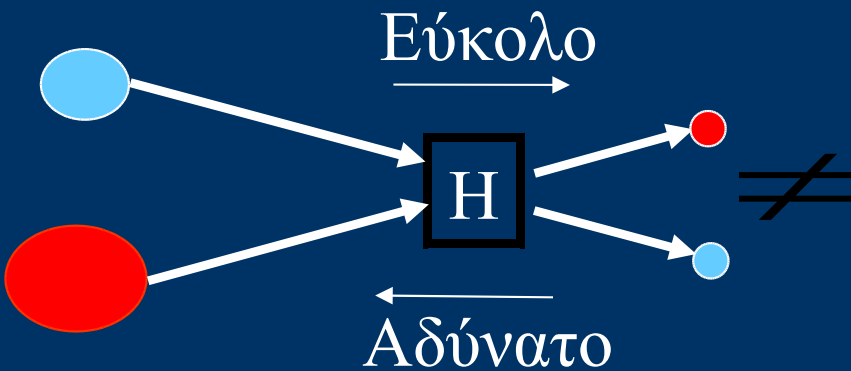
- Η Ψηφιακή Υπογραφή είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητας του.
 - Έχει τα εξής χαρακτηριστικά:
 - Είναι μονοσήμαντα συνδεδεμένα με τον υπογράφοντα
 - Παρέχει τη δυνατότητα αναγνώρισης του υπογράφοντα
 - Δημιουργείται με μέσα που βρίσκονται στον αποκλειστικό έλεγχο του υπογράφοντα
 - Είναι μονοσήμαντα συνδεδεμένα 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
-
-

Ψηφιακές Υπογραφές

Η υπογραφή σε ένα κείμενο είναι ένα στοιχείο το οποίο:

3. Επικυρώνει το κείμενο και επαληθεύει την προέλευση του.
 4. Χρησιμοποιείτε από τον παραλήπτη ως αποδεικτικό στοιχείο.
 5. Χρησιμοποιείτε από ένα τρίτο πρόσωπο με σκοπό την λύση παρεξηγήσεων.
-
-

Hash Συναρτήσεις



- Hash:
 - Μεταβλητό μέγεθος (Input),
 - Σταθερό μέγεθος (Output)
- One-way:
 - Εύκολο στον υπολογισμό
 - Δύσκολο στην αντιστροφή
- Collision-Resistant
 - Δεν γίνεται δύο διαφορετικά μηνύματα να έχουν ίδιο hash.

- Hash Συναρτήσεις (Υλοποίηση):
 - SHA-1, MD5, ...

Συναρτήσεις Σύνοψης (Hash functions)

- Δέχονται ως είσοδο μεταβλητό μέγεθος δεδομένων και επιστρέφουν μία σειρά bits σταθερού μήκους.
- Το αποτέλεσμα ονομάζεται 'Σύνοψη' ή 'Ίχνος' ή 'Αποτύπωμα' του 'Αρχικού κειμένου'
- Οι συναρτήσεις είναι μονόδρομες και συνεπώς η ανάκτηση του αρχικού κειμένου από τη σύνοψη είναι πρακτικά ανέφικτη.
- Η σύνοψη χαρακτηρίζει μοναδικά το αρχικό κείμενο, δηλαδή είναι πρακτικά ανέφικτο να βρεθούν δύο αρχικά κείμενα με την ίδια σύνοψη.
- Γνωστές συναρτήσεις: RIPEMD-160, MD2, MD5, SHA-1, BSAH, Square-Mod (σύνηθες μήκος σύνοψης: 128-160 bits)

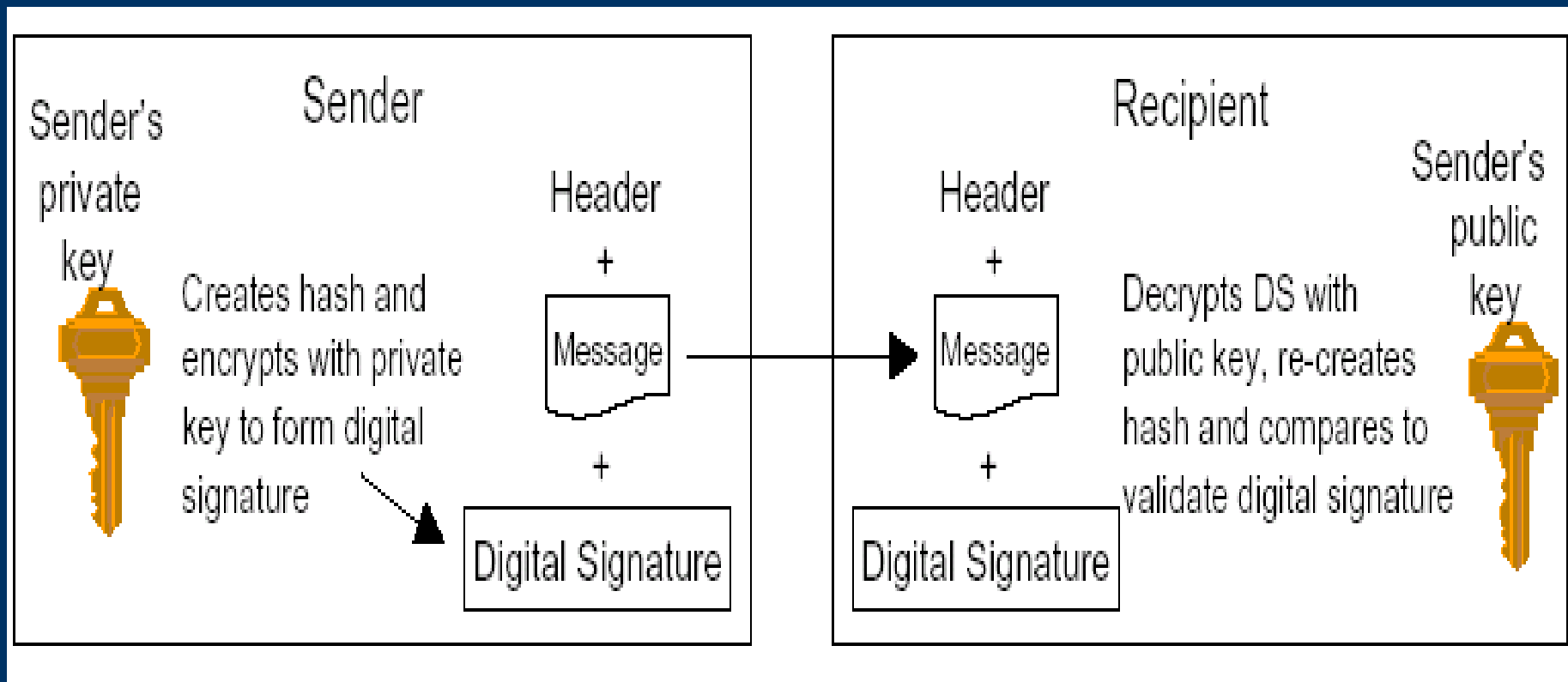
Message Digests

- Το message digest είναι ένα ψηφιακό αποτύπωμα ενός μεγαλύτερου μηνύματος
- ➔ Τα message digests χρησιμοποιούνται για να πιστοποιείται η ακεραιότητα ενός μηνύματος με τη χρήση ηλεκτρονικής υπογραφής.
Ουσιαστικά πρόκειται για μια hash function
- ➔ Μια τέτοια συνάρτηση H δεδομένου ενός μηνύματος x ανεξάρτητου μήκους επιστρέφει μια τιμή σταθερού μήκους η οποία είναι μοναδική. Δηλαδή για κάθε μήνυμα x δεν υπάρχει μήνυμα y , ώστε $H(x)=H(y)$

Ψηφιακές Υπογραφές

- ➔ Ένα μήνυμα υπογράφεται ως εξής:
 - ➔ Ο Αποστολέας περνά το μήνυμα από ένα Hash Function που δίνει αποτέλεσμα μια σειρά χαρακτήρων A (message digest), που είναι πάντα ίδιου μήκους ασχέτως με το μήκος του μηνύματος.
 - ➔ Η σειρά χαρακτήρων A κρυπτογραφείται με το ιδιωτικό κλειδί του Αποστολέα σε A' .
 - ➔ Το A' (η Ψηφιακή Υπογραφή) στέλνεται μαζί με το μήνυμα (χωρίς το σώμα του μηνύματος να είναι αναγκαστικά κρυπτογραφημένο).

Δημιουργία και Επαλήθευση Ψηφιακής Υπογραφής



Ψηφιακές Υπογραφές (συνεχ.)

- ➔ Ο Παραλήπτης παίρνει το μήνυμα μαζί με την Ψηφιακή υπογραφή A' .
 - ➔ Περνά το μήνυμα από την ίδια Hash Function με αποτέλεσμα μια σειρά χαρακτήρων B .
 - ➔ Με το δημόσιο του κλειδί αποκρυπτογραφεί την A' σε A .
 - ➔ Αν τα A και B είναι τα ίδια το μήνυμα δεν έχει αλλοιωθεί.
-
-

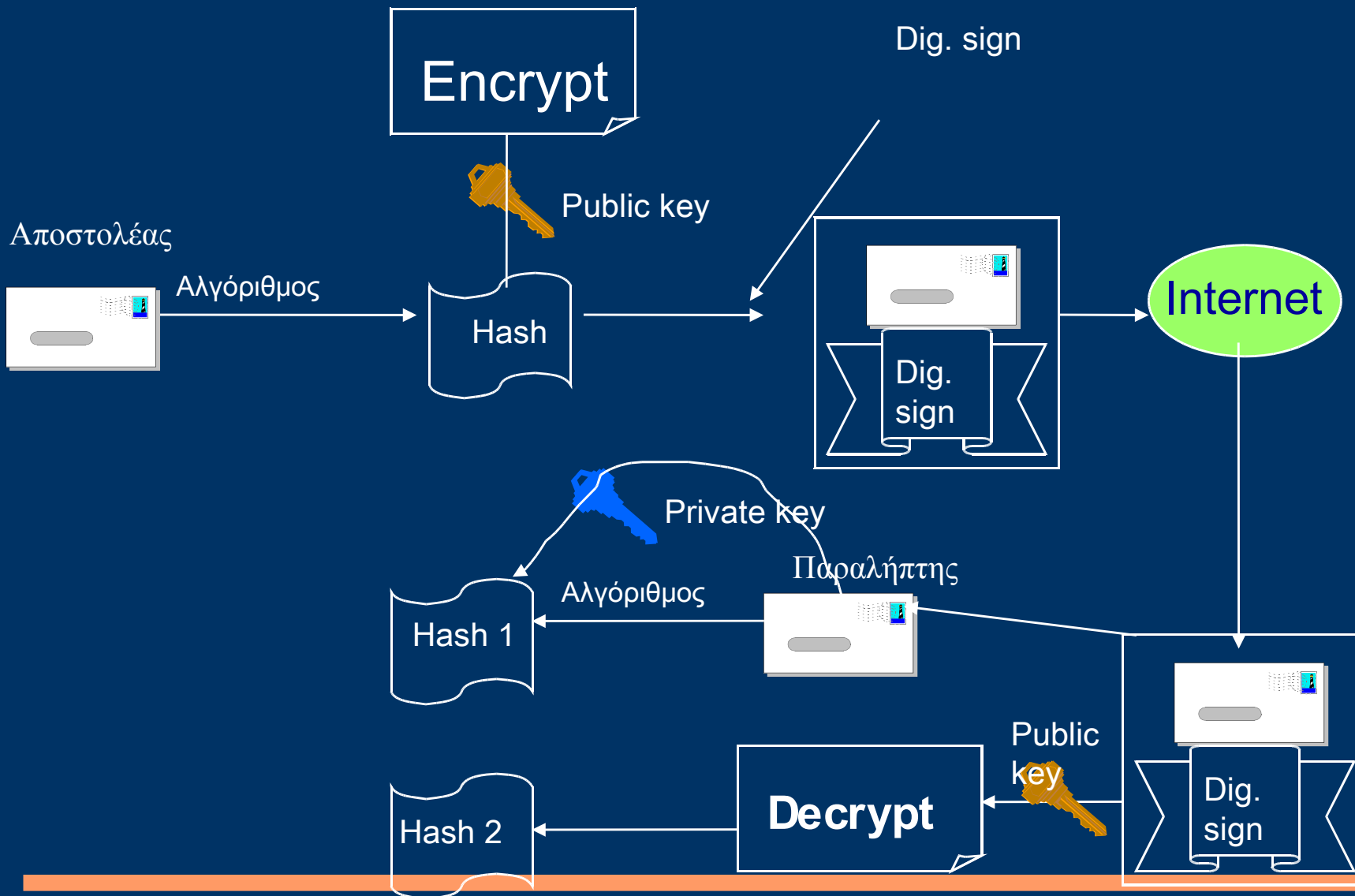
Ασφάλεια Ψηφιακής Υπογραφής

- Σε τι βασιζόμαστε για τη λειτουργία της ηλεκτρονικής υπογραφής;
 - Ασφαλής αλγόριθμος κρυπτογράφησης
 - Ισχυρές συναρτήσεις σύννοψης
 - Αντιστοίχιση 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 αντιστοίχιση κλειδιού - ταυτότητας
- Η κρυπτογραφία δημόσιου κλειδιού λύνει το πρόβλημα της Διανομής κλειδιών αλλά δημιουργεί το πρόβλημα της αντιστοίχισης κλειδιών.
- Διαφαίνεται ξανά η ανάγκη ύπαρξης μίας **‘Εμπιστης Τρίτης Οντότητας’**

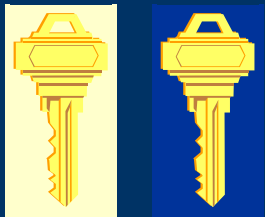
Νομικό πλαίσιο

- Διεθνής αναγνώριση των ψηφιακών υπογραφών ως ισότιμες με τις χειρόγραφες και σε μερικές περιπτώσεις ως ισχυρότερες
- Η Ευρωπαϊκή οδηγία EC/93/99 για τις ηλεκτρονικές υπογραφές έχει ήδη υιοθετηθεί από όλα τα κράτη μέλη.
- Στην Ελλάδα υιοθετήθηκε με το ΠΔ150/2001
- Η ΕΕΤΤ με την απόφαση 248/71 (ΦΕΚ 603/Β'/16-5-2002) ρυθμίζει την διαπίστευση των παρόχων υπηρεσιών πιστοποίησης και την έκδοση 'αναγνωρισμένων πιστοποιητικών'

Ψηφιακή Υπογραφή



Χρήση Ψηφιακής Υπογραφής

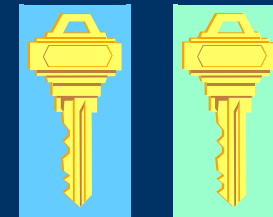


Public Key A
Private Key A

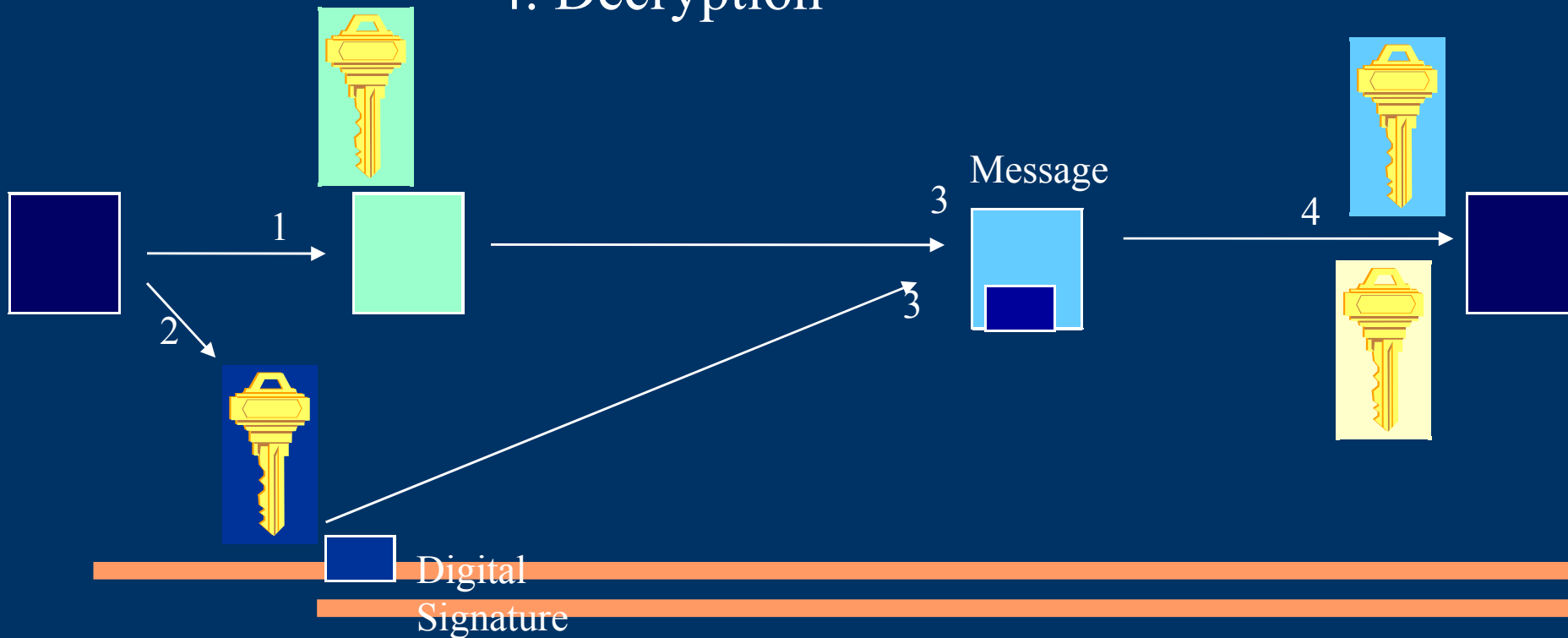
2. Signing

3. Transmission

4. Decryption



Private Key B
Public Key B



*Ένα ‘ηλεκτρονικώς υπογεγραμμένο έγγραφο’
επίσημα θα πρέπει να αποτελείται από τα εξής
στοιχεία:*

- Το κύριο έγγραφο, το οποίο μπορεί να είναι οποιασδήποτε γνωστής ηλεκτρονικής μορφής, π.χ. έγγραφο του Word, του Excel, μορφής ‘*.PDF’, ή ακόμη και μορφής εικόνας, όπως JPEG, TIFF, BMP κ.λ.π.
- Την συνημμένη -καθ’ αυτού- ηλεκτρονική υπογραφή, η οποία είναι στην πραγματικότητα μια κρυπτογράφηση, με το ιδιωτικό κλειδί του υπογράφοντα, μιας ‘σύνοψης’ του κύριου εγγράφου που παράγεται από ειδικό αλγόριθμο ‘κατακερματισμού’ (hashing),

Συνέχεια

- Πιθανώς, από τη χρονοσήμανση της υπογραφής, που αποδίδεται αξιόπιστα από τρίτο πάροχο υπηρεσιών χρονοσήμανσης ο οποίος κρυπτογραφεί με το ιδιωτικό του κλειδί τον συνδυασμό ‘ηλεκτρονική υπογραφή’ του εγγράφου και ‘ακριβή ώρα’ που παρέχει ο ίδιος,
- και τέλος, από το ‘πιστοποιητικό δημοσίου κλειδιού’ του υπογράφοντα, καθώς και από τα τυχόν άλλα πιστοποιητικά που παρέχονται, ανάλογα με τις απαιτήσεις της εφαρμογής

Εφαρμογές ασύμμετρης κρυπτογραφίας III

Ψηφιακά πιστοποιητικά (Digital Certificates)

- Ηλεκτρονικά έγγραφα που σχετίζονται με ένα δημόσιο κλειδί
- Είναι ο τρόπος που μεταδίδονται τα δημόσια κλειδιά

Αρχή Έκδοσης Πιστοποιητικών (Certification Authority)

- εκδίδει ψηφιακά πιστοποιητικά
- τα υπογράφει ψηφιακά

Αυθεντικότητα
πιστοποιητικού

View A Personal Certificate - Netscape

This Certificate belongs to: Koliarmou Despina dkolia@hotmail.com Digital ID Class 1 - Microsoft Persona Not Validated www.verisign.com/repository/RPA Incorp. by Ref., LIAB.LTD(c)98 VeriSign Trust Network VeriSign, Inc.	This Certificate was issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated www.verisign.com/repository/RPA Incorp. By Ref., LIAB.LTD(c)98 VeriSign Trust Network VeriSign, Inc.
--	---

Serial Number: 0A:37:D2:E4:76:66:89:3E:FB:F2:E5:9F:70:30:DC:1E
This Certificate is valid from Mon Oct 16, 2000 to Sat Dec 16, 2000
Certificate Fingerprint:
8F:18:EC:43:2F:95:0D:A7:BC:46:5B:87:20:BE:03:60

OK

```
-----BEGIN CERTIFICATE-----
MIICLCCAdYCEGAOO00decNoXZnrpu9y3eQwDQYJKoZIhvcNAQEEBQAwwgaxFjAU
BgNVBAoTDVZlcm1TaWduLCBjb2MxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20v
cmVwb3NpdG9yeS9UZXR0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYv
RAYDVQQLZm1GbnJlYmVyaVYVbnZ2Z2gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5v
IGFzc3VyYW5jZXMgKEMpVIMxOTk3MB4XDTAwMDYxMjAwMDAwMDAwMDAwMDAwMDYyNjJz
NTk1OVowgYgxCzAJBgNVBAYTAkdSMRiwEAYDVQQIEWlNQUitFRE9OSUEFTATBgNV
BACUFRIRVNTQUxPTkILSTEZMBcGA1UEChQQQVJlU1RPVEVVMRUIPVU5JVjEjEVBGMG
A1UECmQVJlU1RPVEVVMRUIPVU5JVjEjEVBGMGQwYDQVQDFBNPukNMU0VLDkdfTi5BVVRILkdS
MFwwDQYJKoZIhvcNAQEEBQAQSwAwSAJBALQAnKvawbmQ+Zr4idxRrUMoT+ONmy5y
Ndp5sUr/ZY3cLeLS1Z+ZR2H0uHz7MwFnC/WnPFwle001fiCKj227TMUCAwEAATAN
BgkqhkiG9w0BAQQFAANBALytpFFDgeWuGafeTXbysx15UkJ/eJPfojAX6OE81FN
Sdlq/VDFvIbgvqeVwDr7cICrHhB02gFR4WSdtyoO4Ic=
-----END CERTIFICATE-----
```

Σύγκριση Κρυπτογραφικών μεθόδων

- Μέθοδος Δημόσιου Κλειδιού
 - Μεγαλύτερη ευκολία στη χρήση.
 - Χρησιμοποίηση και στις ψηφιακές υπογραφές.
 - Γενικά αργή.
 - Αδύνατο σημείο η εμπιστοσύνη στα δημόσια κλειδιά
- Μέθοδος Ιδιωτικού Κλειδιού
 - Πολύ γρηγορότερη.
 - Οι χρήστες πρέπει να έχουν συγκεκριμένο πρωτόκολλο ανταλλαγής των κλειδιών.
- Η λύση: Συνδυασμός των δύο μεθόδων
 - Παράδειγμα: SSL

Ψηφιακά Πιστοποιητικά

Πρόβλημα Προσποίησης:

- Ποιος πιστοποιεί τα δημόσια κλειδιά;
- Ποιοι είναι οι πραγματικοί κάτοχοι των κλειδιών αυτών

Το παραπάνω πρόβλημα προσπαθεί να λυθεί με την χρήση ψηφιακών πιστοποιητικών.

Ψηφιακά Πιστοποιητικά

Έγγραφο με συγκεκριμένη μορφή. Τα περισσότερα ακολουθούν τη δομή X.509 v3 που είναι η πιο πρόσφατη έκδοση του πρότυπου X.509.

Περιλαμβάνει:

- όνομα και πληροφορίες αναγνώρισης του κατόχου του
- το δημόσιο κλειδί του
- το όνομα της εκδότριας αρχής του (Certification Authority)
- τη ψηφιακή της υπογραφή της ΑΠ (CA)
- ημερομηνία λήξης της ισχύος του
- ένα μοναδικό αριθμό (serial number)

Ψηφιακά πιστοποιητικά - Ορισμός

- Ψηφιακό Πιστοποιητικό είναι μία ψηφιακά υπογεγραμμένη δομή δεδομένων, η οποία αντιστοιχίζει μία ή περισσότερες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει.
- Το πιστοποιητικό είναι υπογεγραμμένο από μία Τρίτη Οντότητα, η οποία είναι Έμπιστη και Αναγνωρισμένη να δρα ως ‘Πάροχος Υπηρεσιών Πιστοποίησης - ΠΥΠ’ (Trusted Third Party –TTP & Certification Services Provider – CSP).
- 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)

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)

Περιεχόμενα ενός πιστοποιητικού

Ένα ψηφιακό πιστοποιητικό περιέχει τις παρακάτω βασικές ομάδες πεδίων:

- Αναγνωριστικά πιστοποιητικού: Τύπος - Πρότυπο, Έκδοση, Σειριακός αριθμός, Αλγόριθμος υπογραφής
- Περίοδος Ισχύος: Από – Έως
- Πληροφορίες Εκδότη: Διακριτικό όνομα, Σημείο πρόσβασης, Αναγνωριστικό κλειδιού
- Υποκείμενο: Πλήρες Διακριτικό Όνομα του κατόχου του πιστοποιητικού
- Δημόσιο κλειδί που αντιστοιχεί στο υποκείμενο
- Επεκτάσεις: Επιτρεπόμενες χρήσεις, Σημείο διανομής πληροφοριών κατάστασης, άλλα εξειδικευμένα ανά εφαρμογή πεδία
- Κρίσιμες επεκτάσεις: Όπως οι προηγούμενες, αλλά χαρακτηρισμένες ως ‘απαράβατες’.
- Υπογραφή Εκδότη σε όλη τη δομή
- Σύνοψη πιστοποιητικού ως κλειδί αναφοράς

Ψηφιακά Πιστοποιητικά

- ➔ Από τι αποτελείται ένα ψηφιακό πιστοποιητικό:
 - ➔ Πληροφοριακά στοιχεία για το χρήστη
 - ➔ Το δημόσιο κλειδί του χρήστη
 - ➔ Το όνομα μιας Αρχής Πιστοποίησης
 - ➔ Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης
-
-

Χρήση των Ψηφιακών Πιστοποιητικών

- 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).
 - Ανταλλάσσονται και χρησιμοποιούνται με συγκεκριμένο τρόπο που ορίζεται στο πρότυπο X.509.
-
-

Χρήση των Ψηφιακών Πιστοποιητικών

- Η Διαχείρισή τους γίνεται μέσω των Εξυπηρετητών Πιστοποιητικών (Certificate Servers).
 - Οι τελευταίοι πολλές φορές παίζουν και το ρόλο της Αρχής Πιστοποίησης.
 - Ανάλογα με την Αρχή Πιστοποίησης το πιστοποιητικό έχει και διαφορετικό εύρος αναγνώρισης. Συνήθως υπάρχει ιεραρχία πιστοποίησης που ορίζεται από το X.509
-
-

Δείγμα πιστοποιητικού X.509 v3 σε μορφή κειμένου

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Modulus:

00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:
55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:
61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:
45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:
a5:94:ac:8a:67

Exponent: 65537 (0x10001)

Key Usage: Digital Signature, Key Encipherment,
Client Authentication

Signature Algorithm: md5withRSAEncryption

7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:
a4:

54:39:80:7b:b9:d9:49:b3:b2:2a:fe:8a:52:f4:c2:89:0e:5c:

7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:01:bc:
40:

ee:bc:0e:fe:fc:f8:9b:9d:70:e3

Certificate:

Data:

Version: 3 (0x0)

Serial Number: 2003532 (0x0)

Signature Algorithm: md5withRSAEncryption

Issuer: C=GR, L=Athens, O=University of the
Aegean, OU=Certification Authority,
CN=ca.aegean.gr, Email=ca@aegean.gr

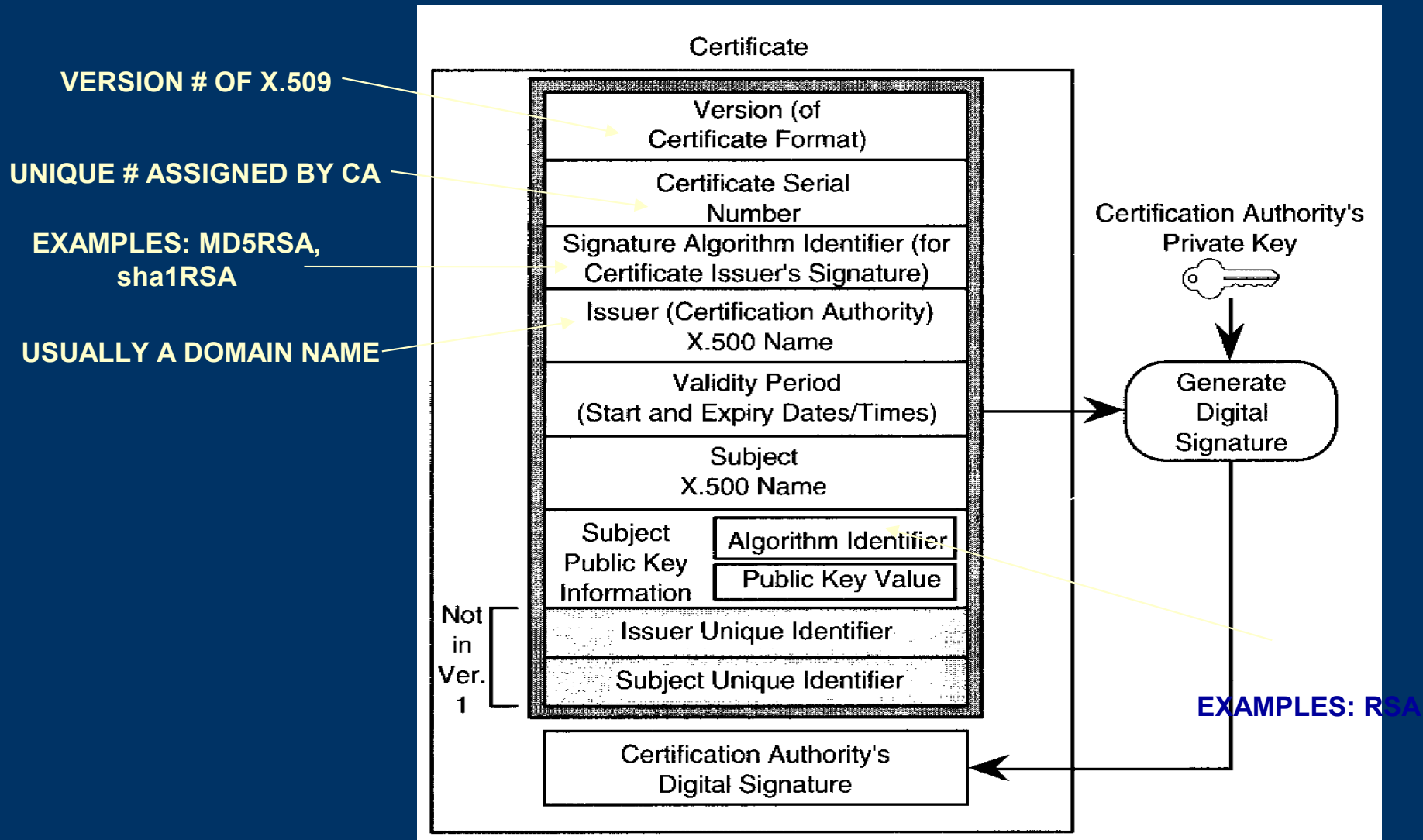
Validity

Not Before: Nov 14 17:15:25 2003 GMT

Not After : Dec 14 17:15:25 2003 GMT

Subject: C=GR, L=Hermoupolis, O= University
of the Aegean, OU=Syros,
CN=www.aegean.gr,
Email=webmaster@aegean.gr

Πιστοποιητικό X.509 Version 2 C



SOURCE: FORD & BAUM,
SECURE ELECTRONIC COMMERCE

Γενική Κατηγοριοποίηση

- Προσωπικό πιστοποιητικό ή Πιστοποιητικό Ταυτότητας (Personal or Identity certificate) : Το υποκείμενο είναι φυσικό πρόσωπο.
- Πιστοποιητικό Συσκευής ή Εξυπηρέτη (Server or Device certificate): Π.χ. Δρομολογητής ή Web server
- Πιστοποιητικό Ρόλου (Role-based certificate): Το υποκείμενο δεν είναι φυσικό πρόσωπο και ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αλλάξει.
- Πιστοποιητικό Οργανισμού (Organisational certificate): Π.χ. 'Microsoft Corp' για την υπογραφή λογισμικού
- Πιστοποιητικό Ιδιοτήτων (Attribute certificate): Χωρίς κλειδί. Αποδίδει ρόλους και δικαιώματα σε μια φυσική οντότητα
- Ομαδικό Πιστοποιητικό (Group certificate): Ταυτοποιεί μία ομάδα και επιβεβαιώνει τη συμμετοχή οντοτήτων σε αυτή.
- Πιστοποιητικό Αντιπροσώπου ή Προσωρινό (Proxy certificate): Παράγεται από το ίδιο το υποκείμενο, έχει διάρκεια ισχύος λίγων ωρών. Π.χ. Μηχανισμοί single-sign-on

Τύποι Ψηφιακών Πιστοποιητικών

- ◆ **Client SSL Certificates:** Για την αναγνώριση των χρηστών σε εξυπηρετητές μέσω SSL (client authentication)
- ◆ **Server SSL Certificates:** Για την αναγνώριση των εξυπηρετητών μέσω SSL (server authentication)
- ◆ **S/MIME Certificates:** Για κρυπτογράφηση και υπογραφή του ηλεκτρονικού ταχυδρομείου
- ◆ **Object-signing Certificates:** Για την αναγνώριση υπογεγραμμένου κώδικα Java, Javascript κ.α.
- ◆ **CA Certificates:** Για την αναγνώριση των CAs
 - ◆ **Root:** το υποκείμενο του πιστοποιητικού, υπογράφει ψηφιακά το πιστοποιητικό. Εκδίδει *Intermediate Certificates*.
 - ◆ **Intermediate:** μπορεί να εκδώσει όλα τα πιστοποιητικά, καθώς και *Intermediate*.

Κατηγοριοποίηση ανάλογα με τη θέση στην ιεραρχία

- Προσωπικό Πιστοποιητικό: Κατέχω το ιδιωτικό κλειδί
 - Πιστοποιητικό Τρίτου: Για χρήση στις συναλλαγές μαζί τους
 - Πιστοποιητικό Ριζικής Αρχής Πιστοποίησης: Του εκδότη που βρίσκεται υψηλότερα στην ιεραρχία. Αυτο-υπογραφόμενο
 - Πιστοποιητικό Ενδιάμεσης Αρχής Πιστοποίησης: Του εκδότη που βρίσκεται ιεραρχικά κάτω από άλλον, ο οποίος το υπογράφει
-
-

Αναγνωρισμένα Πιστοποιητικά (Qualified Certificates – QC)

- Μονοσήμαντος προσδιορισμός ταυτότητας του Παρόχου
 - Μονοσήμαντος προσδιορισμός ταυτότητας του Υποκειμένου
 - Προσδοκώμενη χρήση
 - Δεδομένα για την επαλήθευση της υπογραφής (Signature Verification Data) (π.χ. Δημόσιο κλειδί) που αντιστοιχούν στο υποκείμενο
 - Περίοδος Ισχύος
 - Κωδικός αναγνώρισης του πιστοποιητικού
 - Ηλεκτρονική Υπογραφή του Παρόχου
 - Τυχόν Περιορισμοί στη χρήση και Ευθύνες του Παρόχου
 - Επεκτάσεις κατά περίπτωση εφαρμογής
-
-

Τι απαιτείται από τον ΠΥΠ για την έκδοση αναγνωρισμένων πιστοποιητικών

- Επίδειξη της απαραίτητης αξιοπιστίας
 - Διασφάλιση των μηχανισμών έκδοσης, δημοσίευσης και ανάκλησης πιστοποιητικών
 - Αδιαμφισβήτητη επαλήθευση της ταυτότητας της πιστοποιούμενης οντότητας
 - Απασχόληση κατάλληλα εκπαιδευμένου προσωπικού
 - Χρήση αξιόπιστων Πληροφοριακών Συστημάτων
 - Προστασία των δεδομένων δημιουργίας υπογραφής του ΠΥΠ (signature creation data)
 - Τήρηση Ημερολογίου πράξεων (audit log)
 - Δημοσίευση Πολιτικών, Πρακτικών και Συνθηκών
 - Διασφάλιση ικανών οικονομικών, υλικών και ανθρώπινων πόρων
 - Φυσική ασφάλεια
-
-

Πιθανές πρόσθετες απαιτήσεις

- Εκτίμηση κινδύνων / Risk Analysis
 - Πιστοποίηση ποιότητας κατά ISO 9000
 - Προστασία Προσωπικών Δεδομένων
 - Ασφάλιση
 - Μακροχρόνια αποθήκευση δεδομένων για την επαλήθευση υπογραφών
-
-

Ανάκληση Πιστοποιητικών

- Λόγοι ανάκλησης
 - Απώλεια ιδιωτικού κλειδιού
 - Κλοπή ή διαρροή ιδιωτικού κλειδιού
 - Αλλαγή στοιχείων ή ρόλου
 - Παύση λειτουργίας ΠΥΠ
 - Δημοσίευση της Πληροφορίας Κατάστασης Πιστοποιητικών (Certificate Status Information – CSI)
 - Λίστα Ανάκλησης Πιστοποιητικών
 - Online Certification Status Protocol – OCSP (RFC-2560)
 - delta-CRL: Μόνο τα ανακληθέντα πιστοποιητικά που δεν υπήρχαν στην προηγούμενη delta-CRL
 - Πρόσβαση σε online βάσεις δεδομένων με http, ftp ή ldap URLs.
-
-

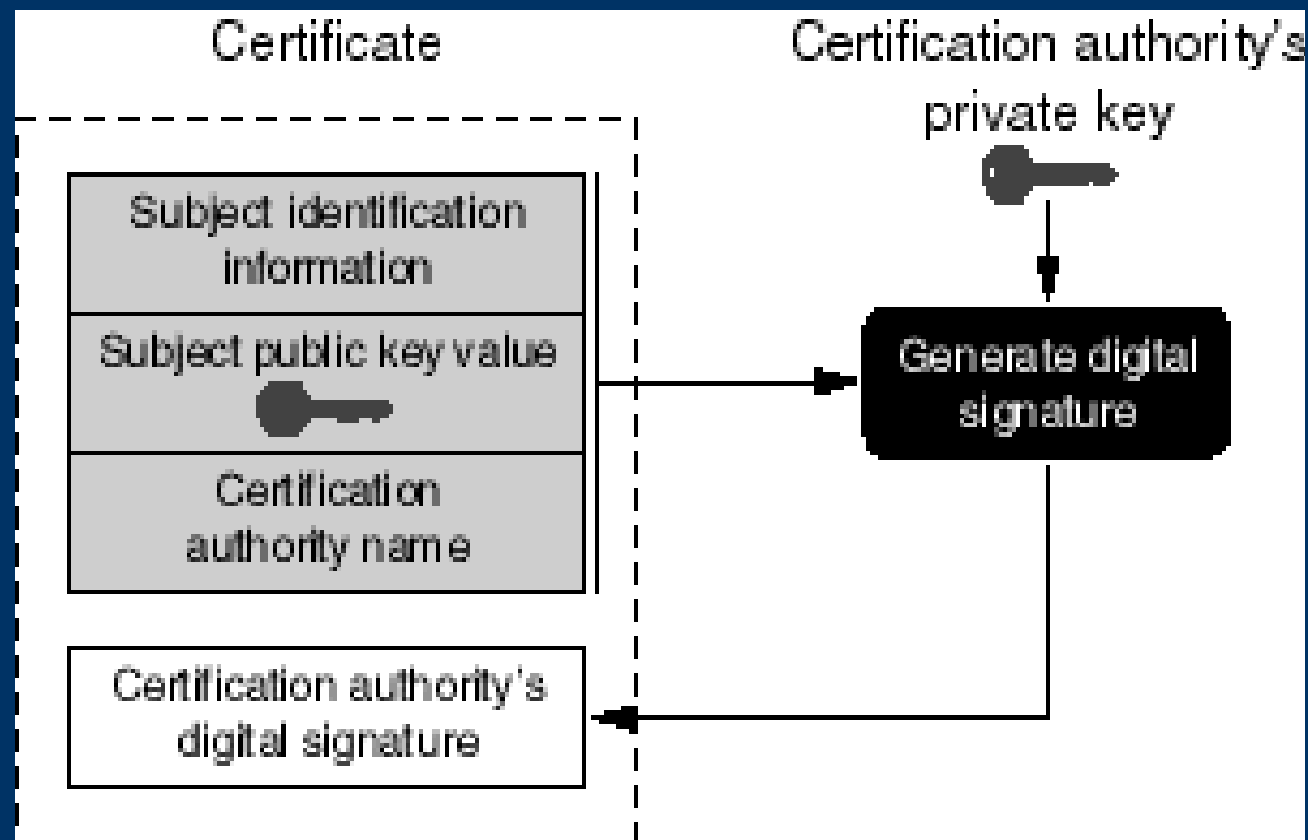
Κύκλος ζωής κλειδιών

- Όσο περισσότερο εκτίθεται ένα κλειδί, τόσο αυξάνουν οι πιθανότητες κρυπτανάλυσης.
 - Όσο περισσότερη πληροφορία κρυπτογραφείται με ένα κλειδί τόσο αυξάνονται οι πιθανότητες κρυπτανάλυσης.
 - Όσο μεγαλύτερο χρονικό διάστημα κατέχει κάποιος ένα κλειδί, τόσο αυξάνονται οι πιθανότητες κακού χειρισμού (π.χ. απώλεια, αποκάλυψη σε τρίτους, τροποποίηση).
 - Όσο μικρότερο είναι το μήκος ενός κλειδιού τόσο μικραίνει και ο κύκλος ζωής του.
 - Είναι απαραίτητο να υπάρχει ένας μηχανισμός ανανέωσης κλειδιών και κατά συνέπεια και των σχετικών πιστοποιητικών.
-
-

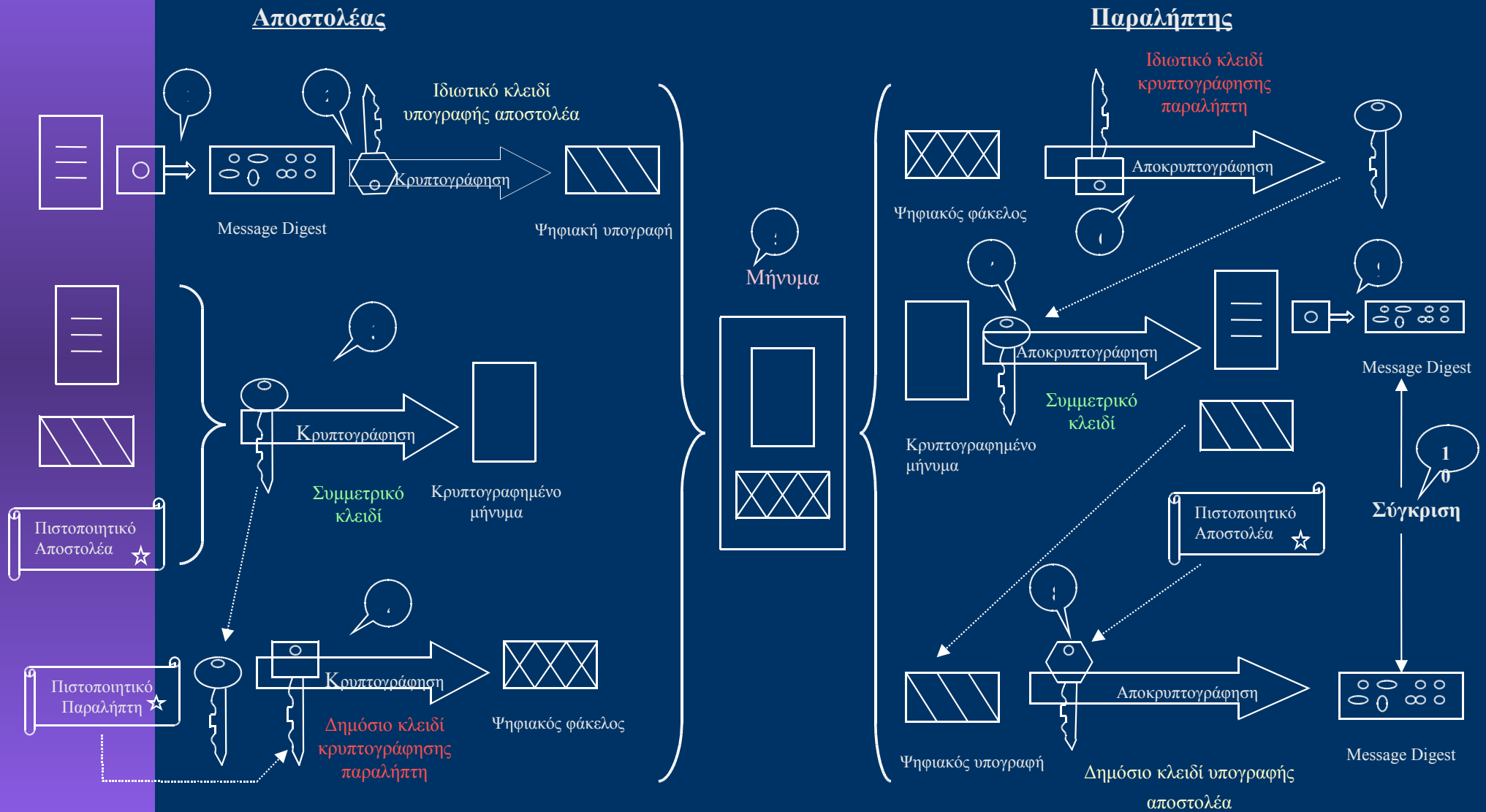
Πρότυπα

- Μορφοποίηση
 - X.509 (ITU)
 - SPKI – SDSI - PKIX (IETF)
 - PGP
 - PKCS#6 (RSA)
 - Αίτηση
 - PKCS#10 (RSA)
 - RFC-2511 (IETF)
 - Διανομή
 - PKCS#7 & PKCS#12 (RSA)
 - Πληροφορίες κατάστασης
 - RFC-2560: OCSP (IETF)
 - TR 102-030 (ETSI)
-
-

Ψηφιακά Πιστοποιητικά (2)



Διαδικασία κρυπτογράφησης



Υποδομές Δημόσιου Κλειδιού-ΥΔΚ

PKI

- PKI – Public Key Infrastructure
- Παρέχουν ένα τρόπο οργάνωσης της φυσικής υποδομής, των εφαρμογών, της διαχείρισης και των διαδικασιών που υποστηρίζουν την ασφάλεια των πληροφοριών
- Βασική τους μέριμνα είναι η διαχείριση των δημόσιων κλειδιών και πιστοποιητικών
- Διαφάνεια (transparency), δηλαδή οι χρήστες δεν χρειάζεται να καταλαβαίνουν τον τρόπο που γίνεται η διαχείριση των κλειδιών και των πιστοποιητικών ώστε να χρησιμοποιήσουν τις υπηρεσίες του PKI.

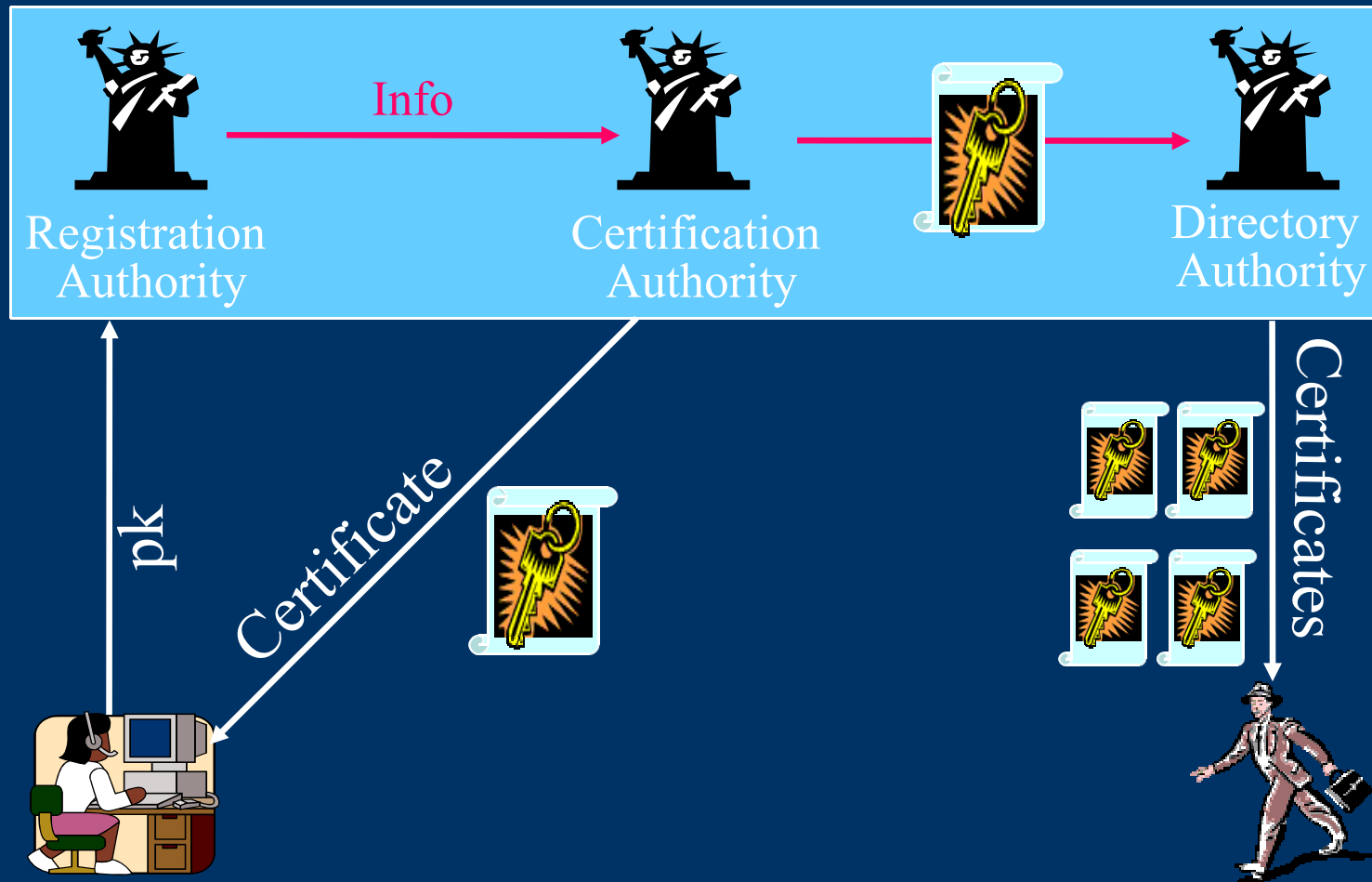
Τρίτη Οντότητα

- PKI (Υποδομή Δημοσίου Κλειδιού)
 - Registration, Certification, Directory Services
- Notary Services (Υπηρεσίες Έμπιστης Οντότητας)
 - Key Escrow / Key Recovery (Αποθήκευση κλειδιού)
 - Time stamping (Χρονολόγηση)
 - Trusted Intermediary (Ενδιάμεση Οντότητα - fair exchange)
 - Archiving (Αρχειοθέτηση Εγγράφων)
- Arbitration Services (Υπηρεσίες Επίλυσης Διαφορών)
 - Courts (Δικαστήριο)

PKI

- Οι οντότητες του PKI, όπως ορίζονται στο PKIX Working Group της IETF είναι :
 - Αρχή Πιστοποίησης (CA – Certification Authority)
 - Αρχή Εγγραφής (RA – Registration Authority)
 - Οι πελάτες (Clients)
 - Η αποθήκη πιστοποιητικών και λιστών ανάκλησης πιστοποιητικών (Repository/Certificate Revocation Lists).
-
-

Υποδομή Δημοσίου Κλειδιού



Τρίτη Οντότητα

Υπηρεσίες που προσφέρονται σε ένα σύστημα PKI

- **Καταγραφή δημοσίου κλειδιού (Key Registration):** έκδοση νέου πιστοποιητικού για ένα δημόσιο κλειδί.
 - **Ακύρωση Πιστοποιητικού (Certificate Revocation):** ακύρωση εκδοθέντος πιστοποιητικού.
 - **Επιλογή κλειδιού (Key Selection):** απόκτηση δημοσίου κλειδιού της άλλης οντότητας (χρήστης ή υπηρεσία).
 - **Εκτίμηση εμπιστοσύνης (Trust Evaluation):** αποφασίζεται εάν ένα πιστοποιητικό είναι έγκυρο και τι υπηρεσίες επιτρέπει.
-
-

Υπηρεσίες PKI (1/2)

① Δημιουργία Κλειδιού (*Generation*)

Δημιουργία του ζεύγους ιδιωτικού/δημόσιου κλειδιού

② Καταχώρηση Κλειδιού (*Registration*)

Κατοχύρωση της σχέσης μεταξύ του κλειδιού και της οντότητας που ανήκει (ψηφιακό πιστοποιητικό)

③ Διανομή Κλειδιού (*Distribution*)

Διανομή των κλειδιών στους χρήστες

Υπηρεσίες PKI (2/2)

④ *Επιβεβαίωση Κλειδιού (Verification)*

Επιβεβαίωση ότι δεν έχει ανακληθεί και είναι έγκυρο

⑤ *Ανάκληση Κλειδιού (Revocation)*

Όταν το κλειδί δεν είναι έγκυρο ή έχει κλαπεί.

Αποθηκεύονται σε λίστες ανάκλησης (CRLs)

⑥ *Επαναφορά Κλειδιού (Recovery)*

Αντίγραφα κλειδιών για την περίπτωση απώλειας ή αν ξεχάσει τον κωδικό πρόσβασης (password)

Σύγκριση τεχνολογιών ασφάλειας

	Αυθεντικοποίηση	Εμπιστευτικότητα	Μη απάρνηση	Ακεραιότητα
Anti-virus			✓	
Firewalls	✓	✓		
Έλεγχος πρόσβασης	✓	✓		
Κρυπτογραφία		✓		
PKI	✓	✓	✓	✓

Συστατικά μέρη των ΥΔΚ



Πολιτική ασφάλειας (Security Policy)

Αρχές για την ασφάλεια των πληροφοριών και τη χρήση της κρυπτογραφίας (CPS).



Αρχή Πιστοποίησης (Certification Authority)

Διαχείριση ψηφιακών πιστοποιητικών.



Αρχή Καταχώρησης (Registration Authority)

Διεπαφή μεταξύ του χρήστη και της CA.



Σύστημα διανομής πιστοποιητικών (Directory Services)

Αποθήκευση πιστοποιητικών που εκδίδει η CA.



Εφαρμογές

Συναλλαγές με πιστωτικές κάρτες, ηλεκτρονικό ταχυδρομείο, επικοινωνία πελάτη/εξυπηρετητή κ.α.

Πολιτική Ασφάλειας

Περιλαμβάνει οδηγίες για τη διαχείριση των κλειδιών και των σημαντικών πληροφοριών

Certificate Practice Statement -CPS

Περιλαμβάνει όλες τις λειτουργικές διαδικασίες για να εφαρμοστεί η πολιτική ασφάλειας στην πράξη. Δηλαδή:

- ✧ πως λειτουργούν οι αρχές πιστοποίησης
- ✧ πως δημιουργούνται και ανακαλούνται τα πιστοποιητικά
- ✧ πληροφορίες για δημιουργία, κατοχύρωση, επιβεβαίωση, αποθήκευση και διανομή των κλειδιών

Αρχή Καταχώρησης

Πιστοποίηση της ταυτότητας όσων ζητούν πιστοποιητικό

Η ποιότητα της διαδικασίας ταυτοποίησης καθορίζει και το επίπεδο εμπιστοσύνης που θα φαίνεται στο πιστοποιητικό

- *On line αίτηση*

Class 1

Ηλεκτρονική φόρμα. Η ταυτότητα καθορίζεται σε σχέση με τις πληροφορίες που παρέχει κάποιος αξιόπιστος οργανισμός π.χ. τράπεζα

- *Αποστελλόμενη αίτηση*

Class 2

Επιπλέον συνοδευτικό υλικό, όπως πιστοποιητικό γέννησης, δίπλωμα οδήγησης

- *Αίτηση μετά από προσωπική παρουσία*

Class 3

Αρχή Πιστοποίησης

Είναι τα πρόσωπα, οι διαδικασίες και τα εργαλεία για τη δημιουργία ψηφιακών πιστοποιητικών, που συνδέουν τα ονόματα των χρηστών με τα δημόσια κλειδιά τους.

- Δρουν ως φορείς εμπιστοσύνης του PKI. Όταν οι χρήστες εμπιστεύονται μια CA που εκδίδει και διαχειρίζεται πιστοποιητικά, εμπιστεύονται και τα πιστοποιητικά αυτά (Third Party Trust).
- Η ακεραιότητα ενός πιστοποιητικού μπορεί να καθοριστεί από την επιβεβαίωση της υπογραφής της CA και επομένως δεν χρειάζονται επιπλέον μηχανισμούς ασφάλειας. Το γεγονός αυτό σημαίνει ότι μπορούν να διανέμονται δημόσια (μέσα από συστήματα καταλόγου που επιτρέπουν την πρόσβαση σε όλους)

Σύστημα Διανομής Πιστοποιητικών

Οι ΥΔΚ αποθηκεύουν τα πιστοποιητικά που εκδίδουν σε αποθήκες πιστοποιητικών (**certificate repositories**), ώστε να μπορούν να ανακτούνται από τις εφαρμογές των χρηστών.

Τα τελευταία χρόνια, κυριαρχεί η άποψη ότι η καλύτερη τεχνολογία για τις αποθήκες πιστοποιητικών είναι να παρέχονται από συστήματα καταλόγου (Directory Systems) που είναι συμβατά με το πρωτόκολλο LDAP (Lightweight Directory Access Protocol)

Συστήματα καταλόγου

Εξυπηρετούν γιατί:

1 Παρέχουν διαφάνεια στους χρήστες, αφού οι εφαρμογές τους είναι υπεύθυνες για την ανάκτηση των πιστοποιητικών

2 Οι τεχνολογίες καταλόγου που υποστηρίζουν LDAP μπορούν:

- να υποστηρίξουν μεγάλο αριθμό εγγραφών
- να ανταποκριθούν αποτελεσματικά σε αιτήσεις αναζήτησης πιστοποιητικών, σύμφωνα με τις μεθόδους αναζήτησης που διαθέτουν
- να είναι κατανεμημένες

Βοηθητικές Υπηρεσίες - Επαναφορά κλειδιού (Key Recovery)

- Οι χρήστες ξεχνούν τους κωδικούς πρόσβασης στα κλειδιά κρυπτογράφησης.
- Απώλεια κλειδιών (π.χ. αν αποθηκεύονται σε μαγνητικές κάρτες που έχουν αλλοιωθεί)

Τα μόνα κλειδιά που χρειάζονται επαναφορά είναι τα κλειδιά κρυπτογράφησης.

Τα κλειδιά που χρησιμοποιούνται για ψηφιακές υπογραφές δεν πρέπει να επαναφέρονται γιατί τότε δεν ικανοποιείται μια βασική απαίτηση από ένα PKI

Non-repudiation

Ανάκληση κλειδιού (Revocation)

Ένα PKI πρέπει να παρέχει ένα σύστημα ανάκλησης των πιστοποιητικών, ώστε να μπορούν οι εφαρμογές να ελέγχουν την κατάσταση των πιστοποιητικών κάθε φορά πριν να τα χρησιμοποιήσουν.

Η CA πρέπει να δημοσιεύει τις πληροφορίες για την κατάσταση κάθε πιστοποιητικού του συστήματος σε τακτά χρονικά διαστήματα.

Για τη διανομή των πληροφοριών ανάκλησης, οι CAs δημιουργούν λίστες ανάκλησης (Certificate Revocation Lists - CRLs) και τις δημοσιεύουν μέσω του συστήματος καταλόγου.

Time - Stamping (Χρονολόγηση)

Πρόβλημα: Οι ψηφιακές υπογραφές πρέπει να έχουν μεγάλη διάρκεια ζωής, αλλά

- Τα κλειδιά μπορεί να χαθούν ή να κλαπούν
- Η αύξηση της ισχύος των υπολογιστών «εξασθενεί» ένα κλειδί δεδομένου μεγέθους
- Οι κρυπτογραφικοί αλγόριθμοι είναι «εν δυνάμει» ευάλωτοι !

Λύση:

- Επίσημη χρονολόγηση, από μια έμπιστη οντότητα (time stamping service), των ψηφιακών υπογραφών

Third-Party Trust

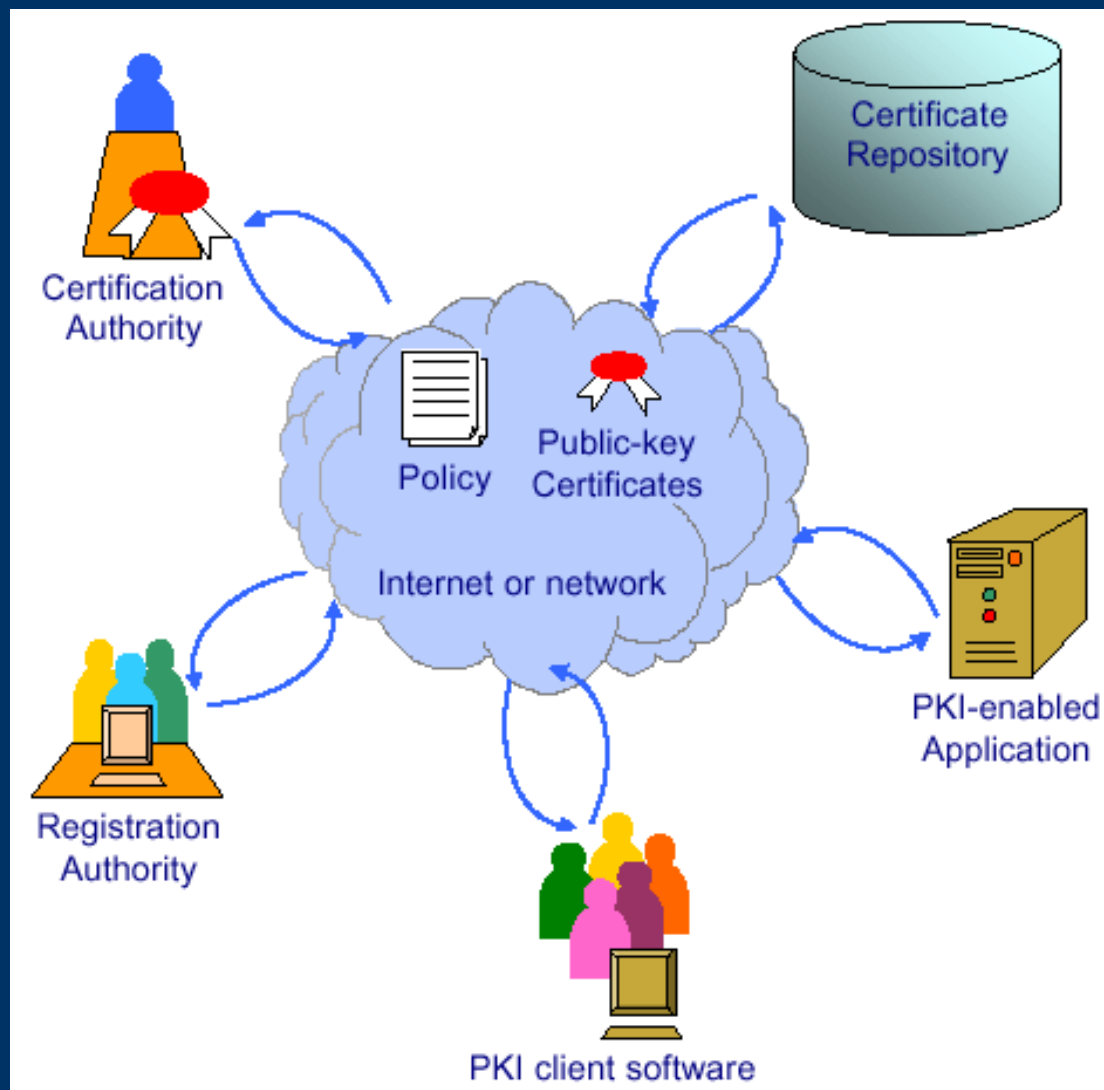
Αναφέρεται στην περίπτωση όπου δύο οντότητες εμπιστεύονται απόλυτα η μια την άλλη, χωρίς να έχουν προηγουμένη συναλλαγή μεταξύ τους.

Σε αυτή την περίπτωση, υπάρχει εμπιστοσύνη γιατί μοιράζονται μια σχέση με μια κοινή τρίτη πλευρά (CA), που εμπιστεύονται και οι δύο και πιστοποιεί την ταυτότητά τους.

Πιστοποίηση

- ◆ Μια CA δέχεται αιτήσεις από πολλές LRAs.
- ◆ Οι καταχωρημένες πληροφορίες μεταφέρονται στην CA με ασφαλή μηνύματα.
- ◆ Ο χρήστης κατοχυρώνει ένα δημόσιο κλειδί (όχι το ιδιωτικό)
- ◆ Η CA επιβεβαιώνει ότι το κλειδί δεν έχει καταχωρηθεί από άλλο χρήστη.
- ◆ Εκδίδει το πιστοποιητικό που έχει ορισμένο χρόνο ισχύος.
- ◆ Κάθε πιστοποιητικό έχει ένα μοναδικό αριθμό και μια κατάσταση.
- ◆ Οι χρήστες εξάγουν πληροφορίες για τα πιστοποιητικά από καταλόγους, με την βοήθεια πρακτόρων (agents). Οι κατάλογοι είναι απαραίτητοι γιατί η ύπαρξη ενός πιστοποιητικού δεν σημαίνει ότι είναι ακόμα έγκυρο.

Στοιχεία της Υποδομής Δημόσιου Κλειδιού

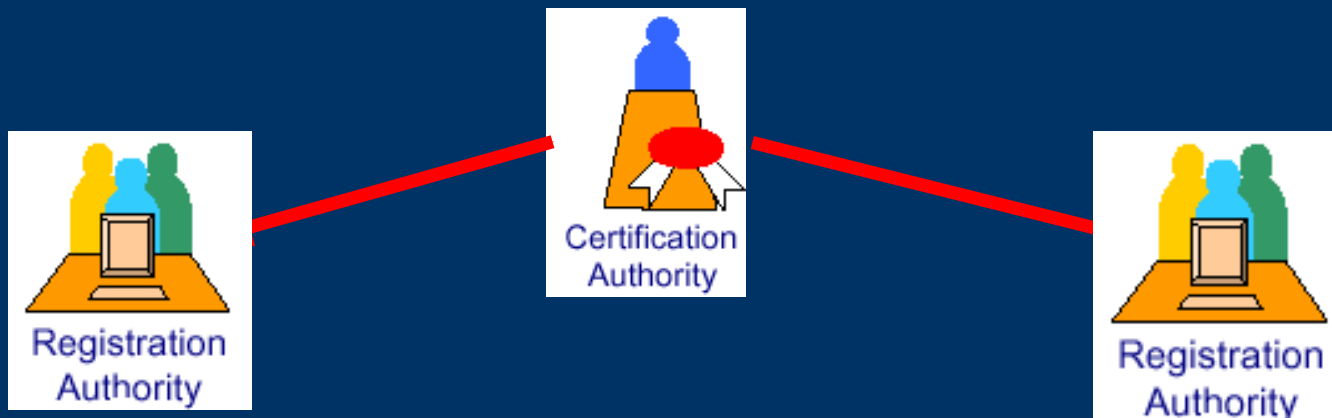


Η ΥΔΚ αποτελείται από

- Πιστοποιητικά (Certificates)
- Υποκείμενα ή Εγγραφόμενους (Subjects or Subscribers)
- Βασιζόμενες οντότητες (Relying Parties - RP)
- Αρχές Πιστοποίησης (Certification Authority - CA)
- Αρχές Καταχώρησης (Registration Authority - RA)
- Δηλώσεις Πρακτικών Πιστοποίησης (Certification Practice Statements - CPS)
- Πολιτικές Πιστοποιητικών (Certificate Policies - CP)
- Αποθηκευτικούς μηχανισμούς και Υπηρεσίες Καταλόγου (Repositories & Directories)
- Μηχανισμούς Διαλειτουργικότητας (Interoperability mechanisms)
- Δεδομένα Δημιουργίας Υπογραφής (Signature-creation data)
- Συσκευές Δημιουργίας Υπογραφής (Signature-creation device)
- Δεδομένα Επαλήθευσης Υπογραφής (Signature-verification data)

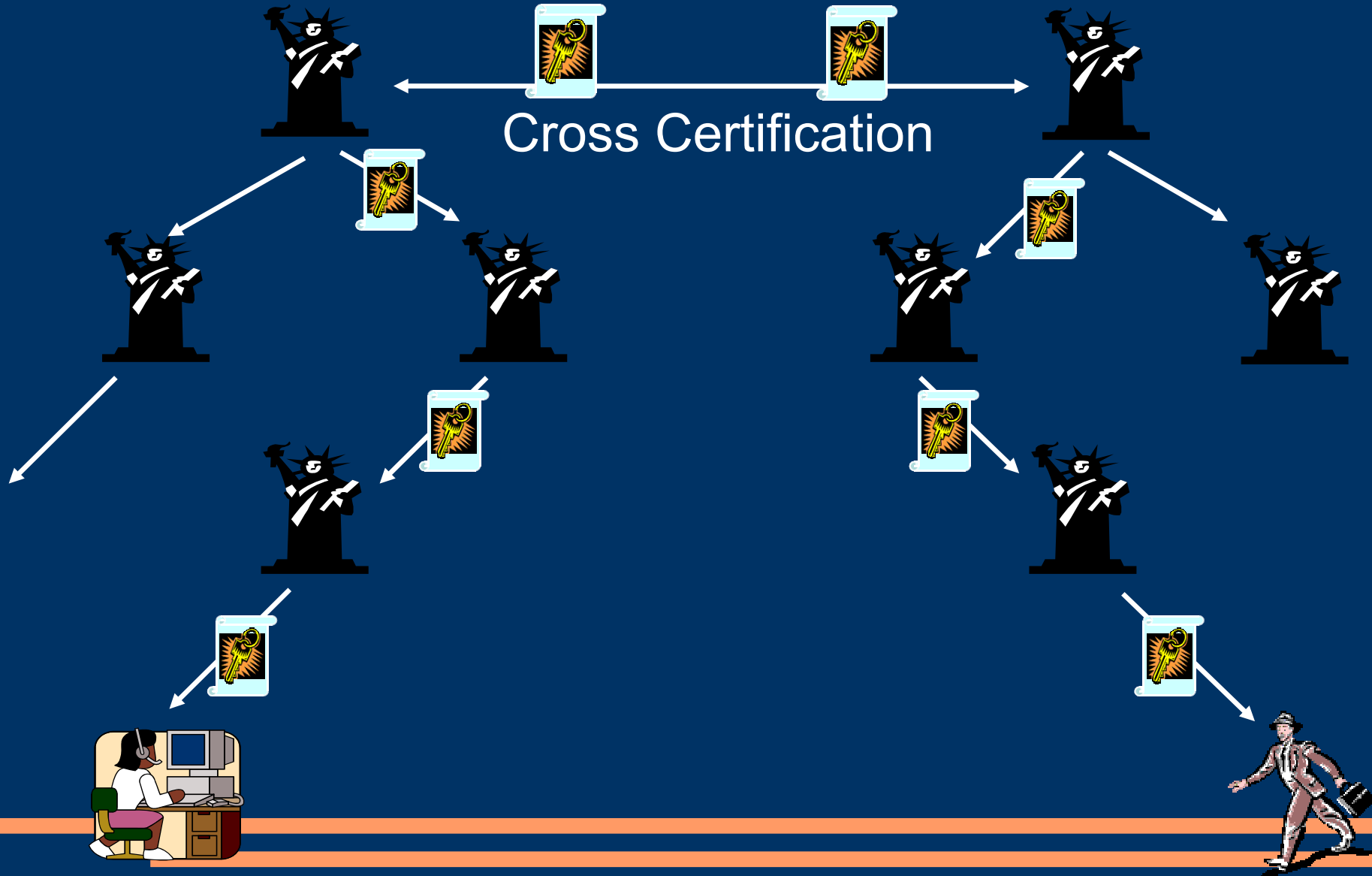
Ένας ΠΥΠ αποτελείται από

- Τουλάχιστο μία Αρχή Πιστοποίησης:
 - Άνθρωποι, Διαδικασίες και Εργαλεία για τη Δημιουργία, Διανομή και Διαχείριση των Ψηφιακών Πιστοποιητικών
- Τουλάχιστο μία Αρχή Καταχώρησης για κάθε ΑΠ:
 - Άνθρωποι, Διαδικασίες και Εργαλεία για την επαλήθευση της ταυτότητας των εγγραφόμενων οντοτήτων και την προώθηση της αίτησης στην ΑΠ

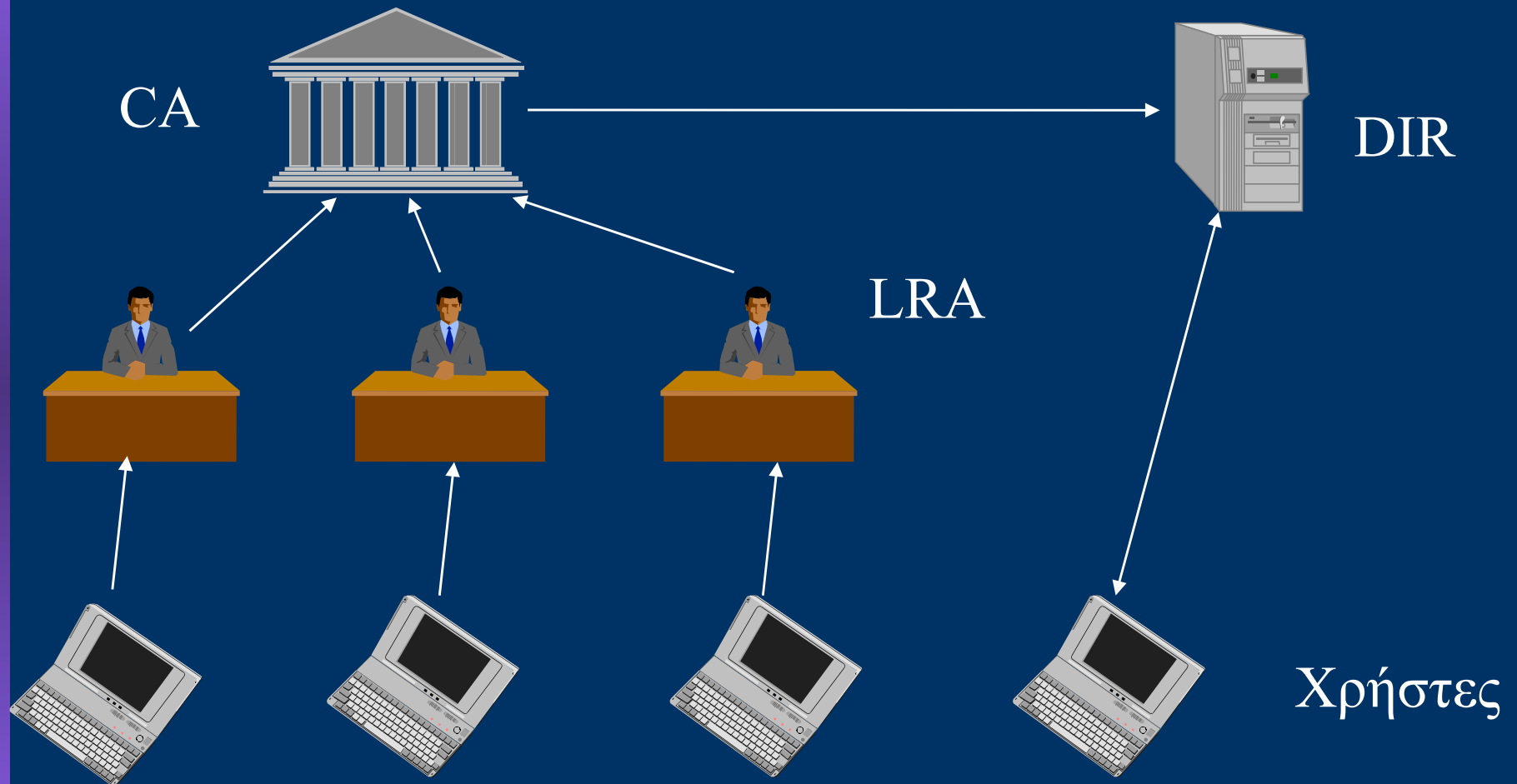


Ιεραρχία Πιστοποίησης

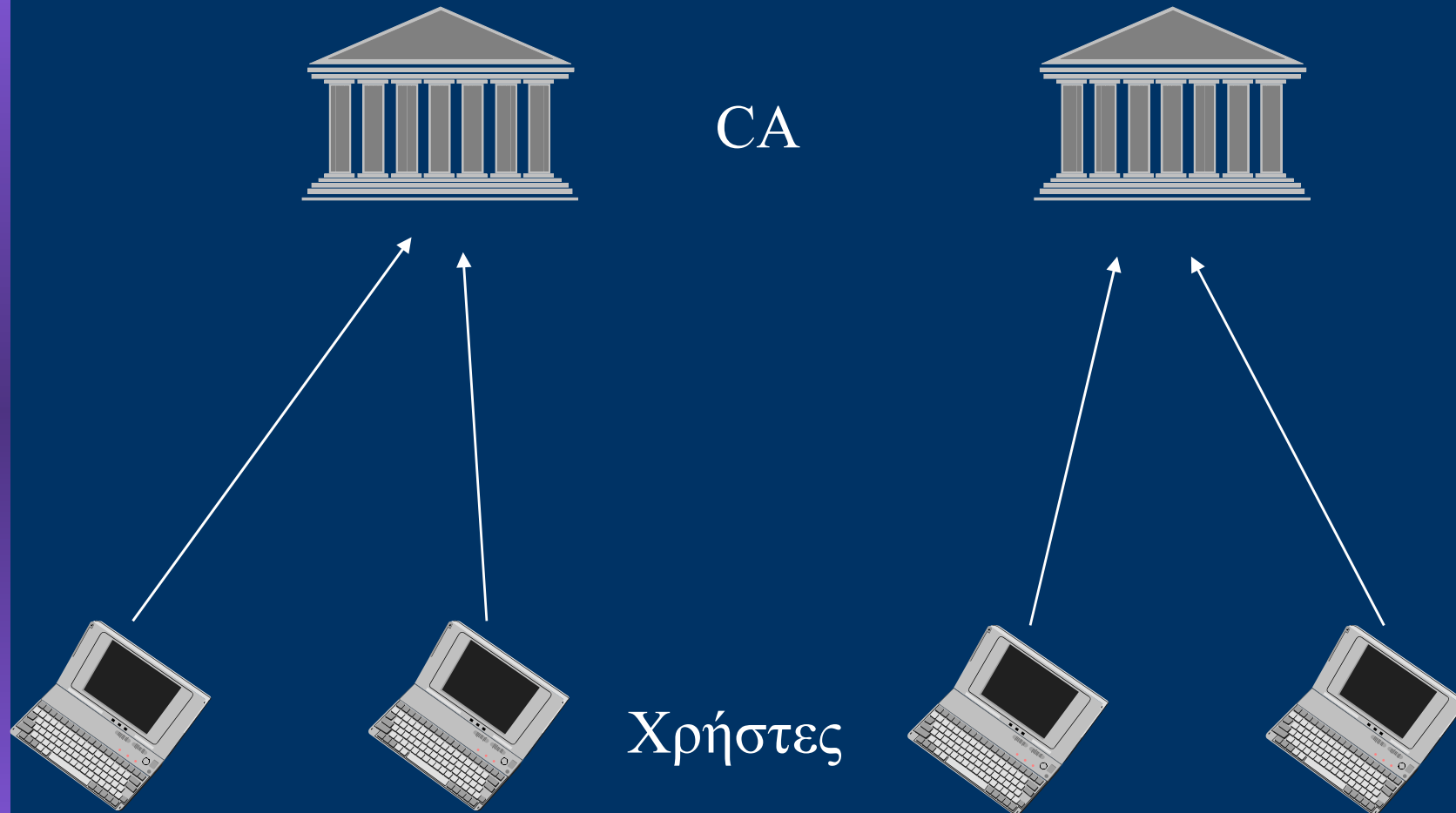
Τρίτη Οντότητα



Αρχιτεκτονική πιστοποίηση (1/4)



Αρχιτεκτονική πιστοποίηση (2/4)



Διαπιστοποίηση (Cross-Certification)

Η εμπιστοσύνη σε ένα πιστοποιητικό βασίζεται στην ψηφιακή υπογραφή της εκδότριας CA αλλά και στο πόσο έμπιστη είναι η ίδια η αρχή έκδοσης.

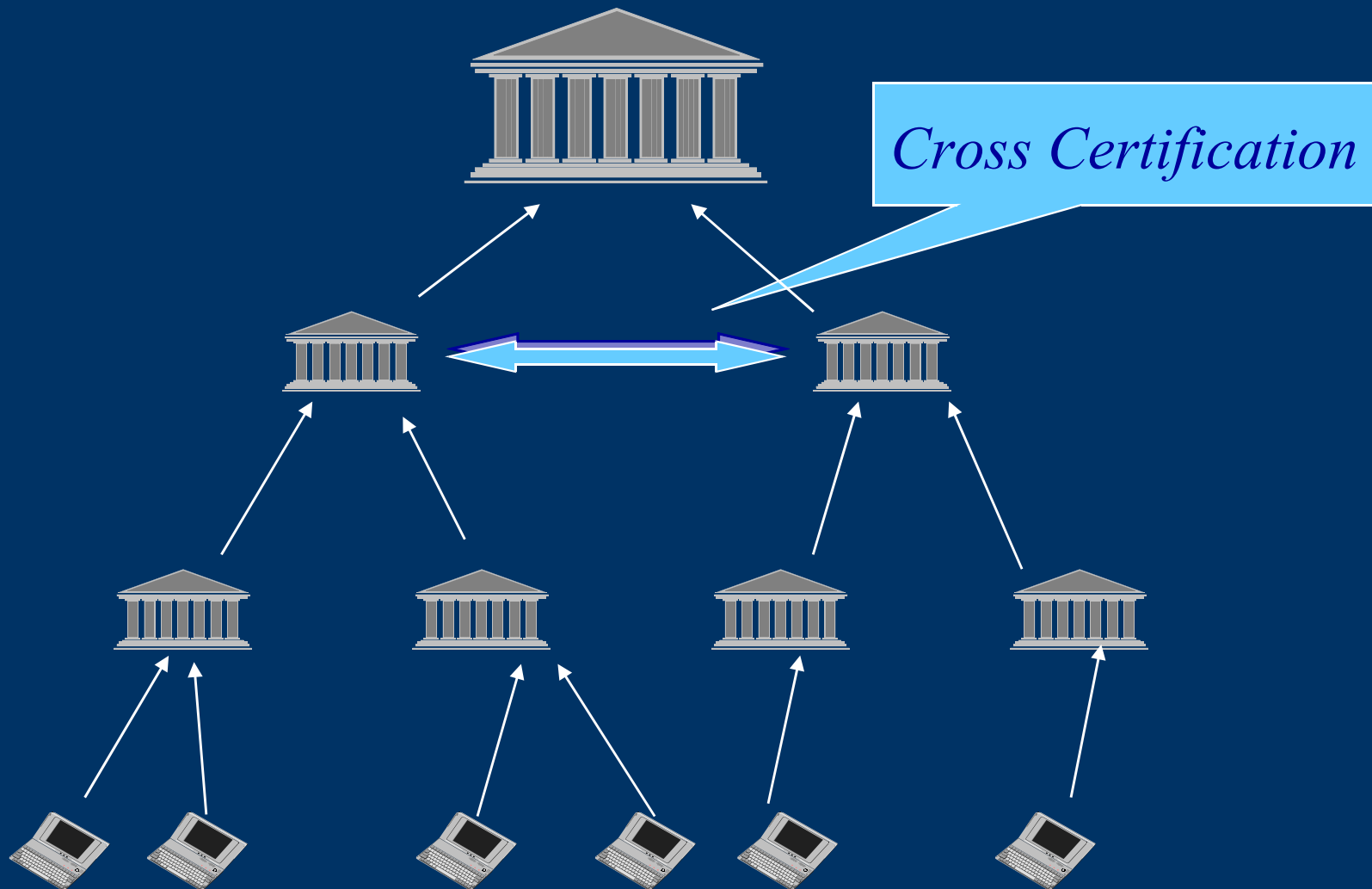
Διαπιστοποίηση είναι η διαδικασία ανταλλαγής πληροφοριών μεταξύ δύο CAs, ώστε να εμπιστεύεται η μια τα κλειδιά της άλλης.

Μπορεί να δημιουργήσει και να υπογράψει ένα πιστοποιητικό δημόσιου κλειδιού της άλλης

Αποτελεί μια εκτεταμένη μορφή third-party trust, όπου όλοι οι χρήστες που ανήκουν στην μία εμπιστεύονται όλους τους χρήστες που ανήκουν στην άλλη.

Κάθε μια από τις εμπλεκόμενες CAs πρέπει να εγκρίνει την πολιτική ασφάλειας που ακολουθεί η άλλη.

Αρχιτεκτονική πιστοποίηση (3/4)



Αρχιτεκτονική πιστοποίησης (4/4)

Για να υπάρχει εμπιστοσύνη μεταξύ δυο πελατών, πρέπει να μπορούν να αποκτήσουν και να επιβεβαιώσουν ο ένας το πιστοποιητικό του άλλου.

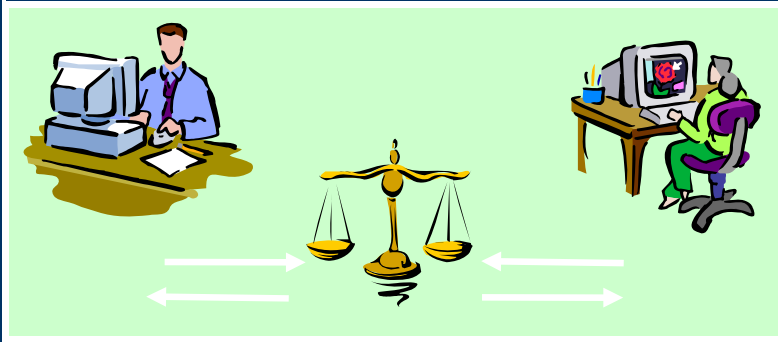
- 1 Λαμβάνει το δημόσιο κλειδί της CA που πιστοποιεί τον άλλο πελάτη
- 2 Αν πιστοποιούνται από διαφορετικές CAs, τότε πρέπει να πιστοποιηθούν με βάση την ιεραρχία, εκτός αν υπάρχει αμοιβαία πιστοποίηση
- 3 Κάθε πελάτης λαμβάνει το πιστοποιητικό του άλλου και ελέγχει την εγκυρότητα του με βάση το δημόσιο κλειδί της εκδότριας CA
- 4 Αν τα πιστοποιητικά είναι έγκυρα, τα δημόσια κλειδιά τους μπορούν να χρησιμοποιηθούν για ασφαλή μετάδοση πληροφοριών

Fairness & Trusted Intermediary: Υπηρεσίες Ενδιάμεσης Οντότητας

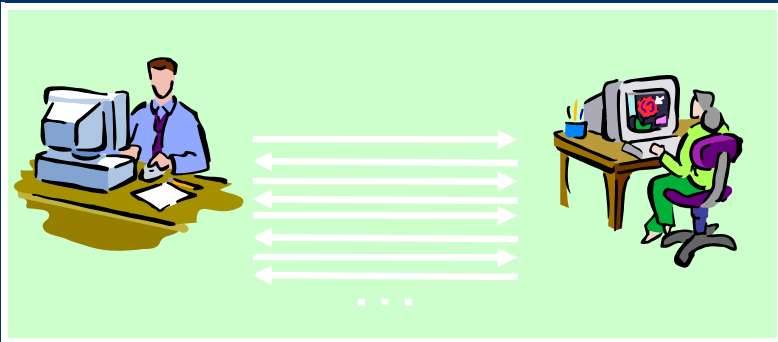
- Fairness (Αμεροληψία-Δικαιοσύνη-Τιμιότητα)
 - Non-repudiation (Καταλογισμός Ευθύνης)
 - Υποβολή / Παραλαβή / Απόδειξη
 - Πληρωμές
 - Απόδειξη, online αποστολή δεδομένων
 - Contract Signing (Υπογραφή Συμβολαίων)
- Στόχοι
 - Ελάχιστη ανάμειξη της Τρίτης Οντότητας
 - Όχι μεγάλο υπολογιστικό κόστος
 - Πρωτόκολλα ανεξάρτητα των αγαθών που ανταλλάσσονται

Fairness: Όλες οι Προσεγγίσεις

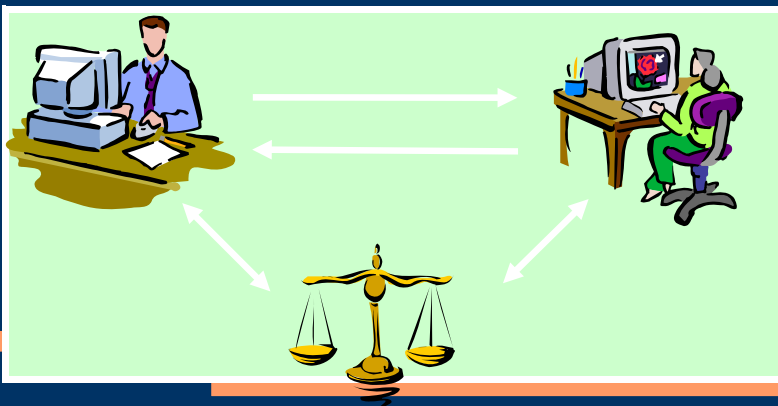
Τρίτη Οντότητα



- Ενδιάμεση Οντότητα
 - Απλό πρωτόκολλο
 - Χαμηλή απόδοση
 - Υπερβολική Εμπιστοσύνη



- Βαθμιαία ανταλλαγή μυστικών
 - ΔΕΝ υπάρχει τρίτη Οντότητα
 - Υψηλό υπολογιστικό κόστος
 - Υψηλή πιθανότητα λάθους

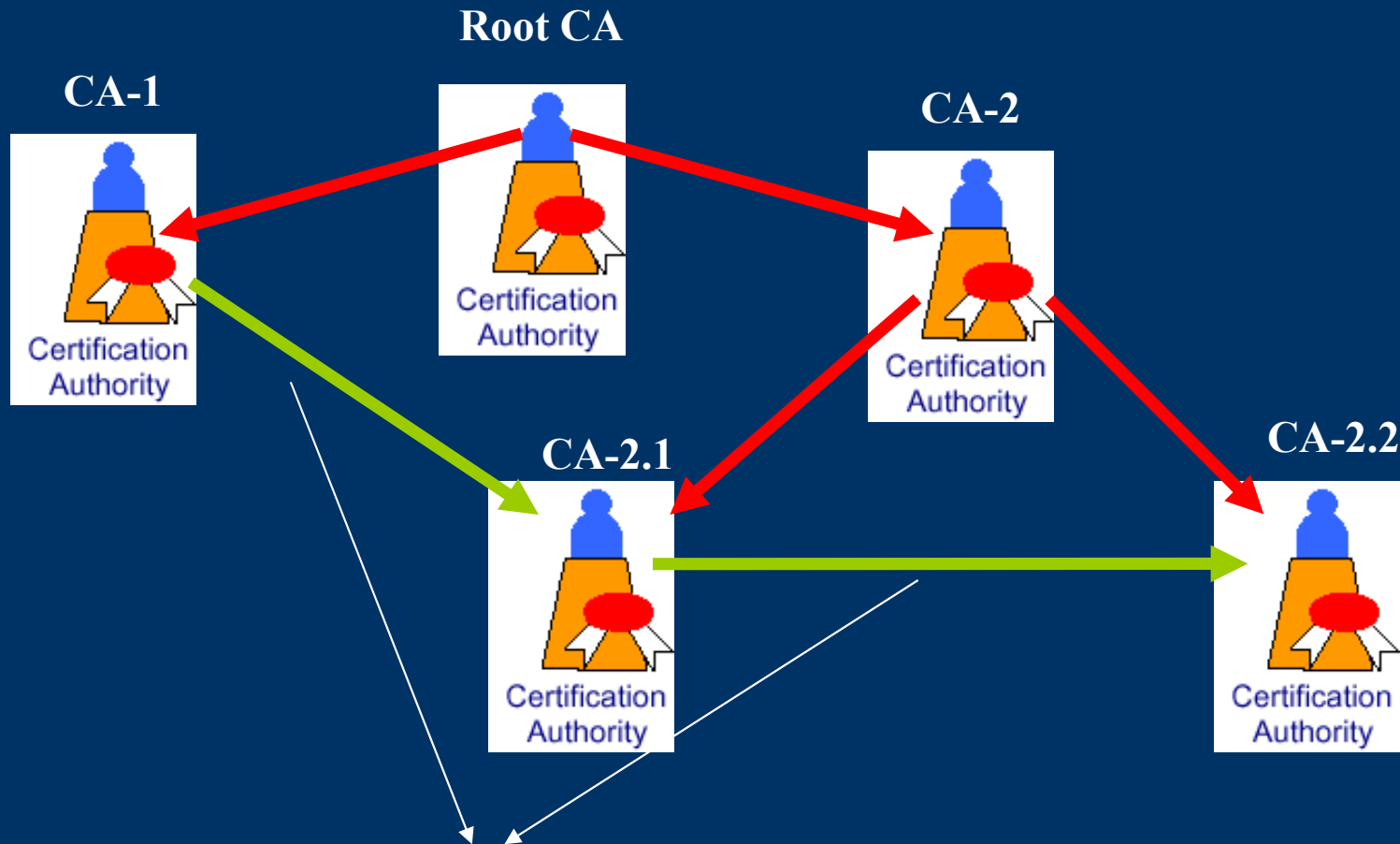


- Optimistic πρωτόκολλα
 - Απλό πρωτόκολλο
 - Η Τρίτη Οντότητα αναμειγνύεται ΜΟΝΟΝ στην περίπτωση απάτης ή λάθους

Οι ΑΠ συνδέονται μεταξύ τους σε Αρχιτεκτονικές Εμπιστοσύνης

- Ομοπάτρια (single parent)
 - Διμερής (web-of-trust)
 - Ιεραρχική (hierarchy)
 - Απόλυτα ιεραρχική
 - Ιεραρχία με χρήση αντίστροφων πιστοποιητικών
 - Μοντέλο προσανατολισμένου γράφου
 - Δια-πιστοποίηση (cross-certification)
 - Έμπιστου μεσολαβητή (Trusted broker ή Bridge CA)
 - Δάσος ή Μικτή (Forest ή Mixed)
-
-

Ιεραρχικό μοντέλο (1)

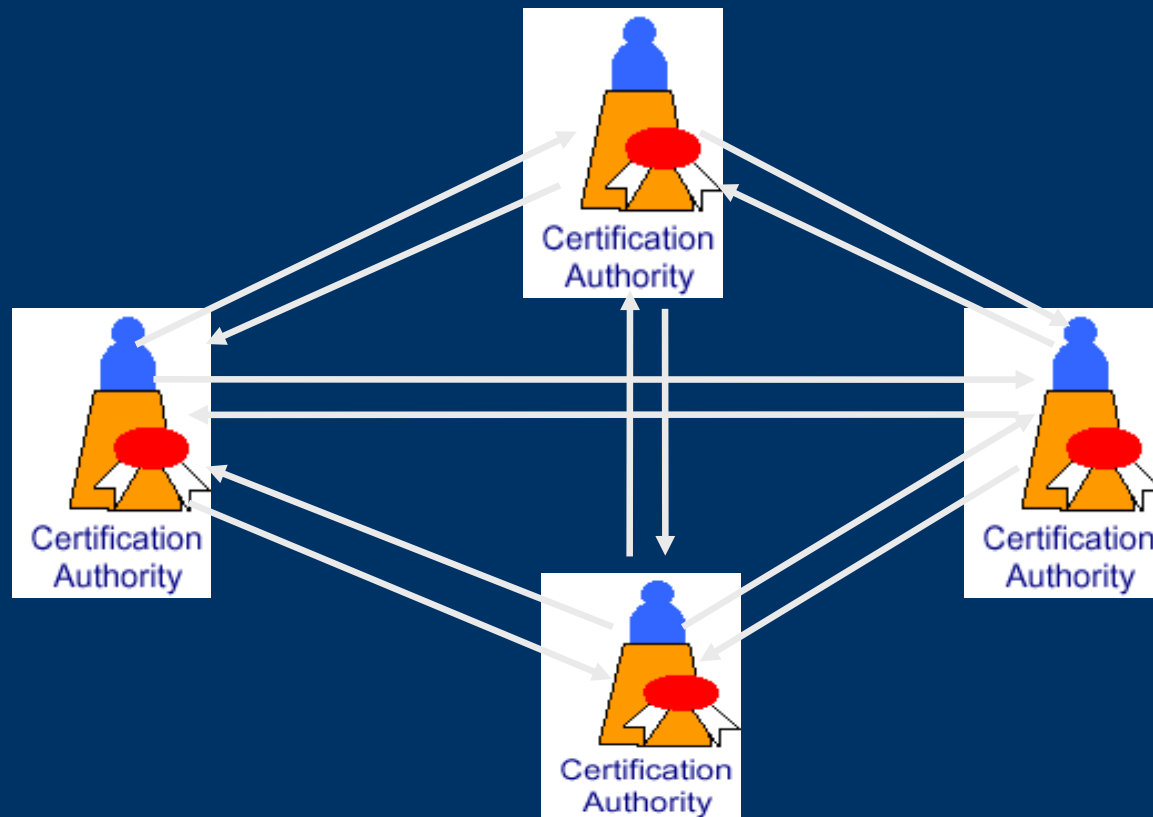


Σχέσεις μοντέλου προσανατολισμένου γράφου

Ιεραρχικό μοντέλο (2)

- Όλα τα πιστοποιητικά κάτω από ένα έμπιστο πιστοποιητικό, θεωρούνται έμπιστα
- Εμπιστοσύνη στο πιστοποιητικό ρίζας
 - Χρειάζεται ένα ‘αυτό-υπογραφόμενο’ (self-signed) πιστοποιητικό στην κορυφή της ιεραρχίας.
 - Δεν είναι ασφαλές, αλλά αποτελεί έναν πρακτικό μηχανισμό για τη διανομή του κλειδιού.
 - Μία ‘βασισόμενη οντότητα’ θα πρέπει να ελέγξει την προέλευση και την ακεραιότητα των αυτό-υπογραφόμενων πιστοποιητικών.
- Μη πρακτικό σχήμα σε παγκόσμια κλίμακα (π.χ. ασφάλεια ενός σημείου, εξουσία κλπ)

Δια-πιστοποίηση (*cross-certification*) (1)

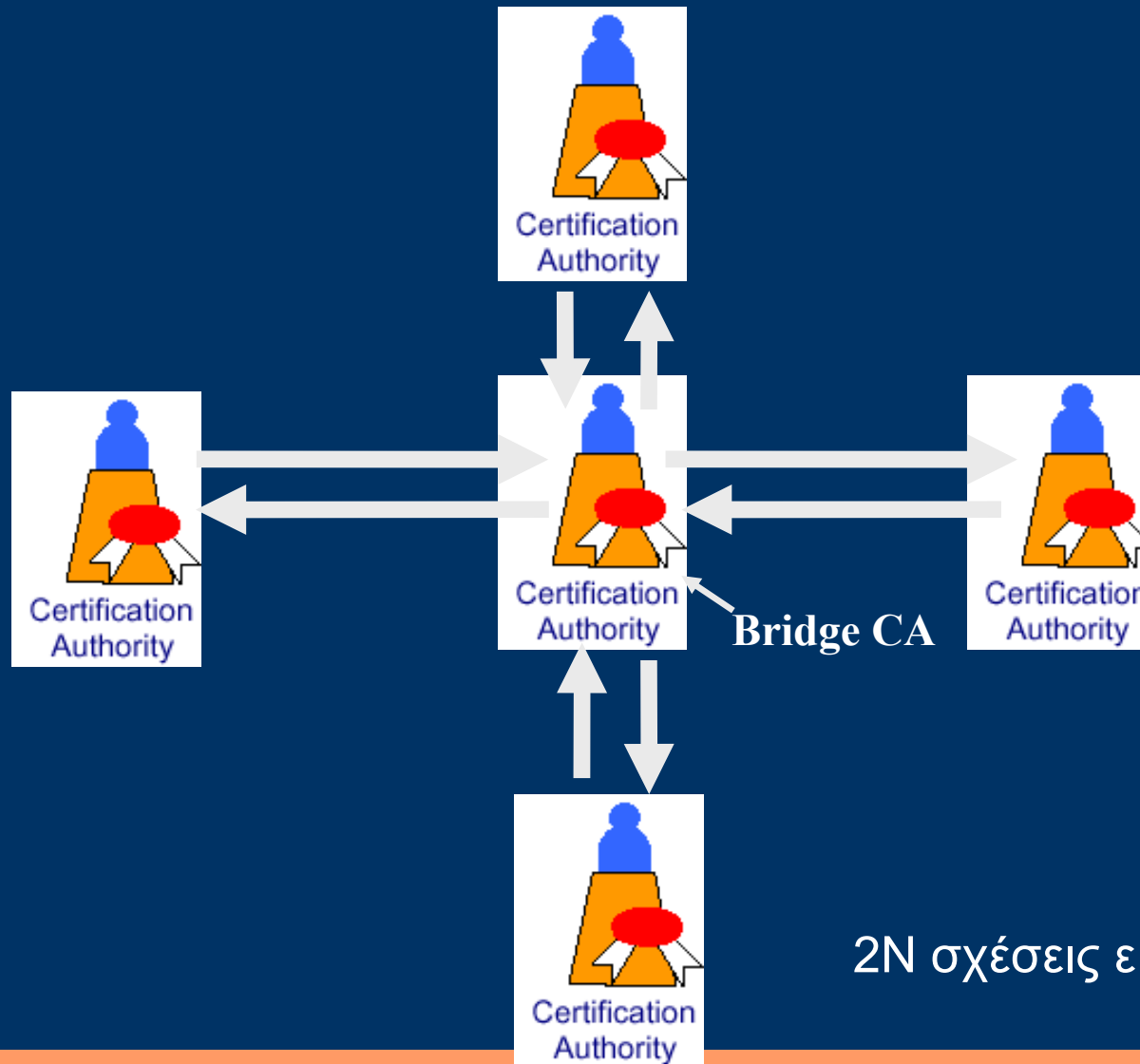


$N*(N-1)$ σχέσεις εμπιστοσύνης

Δια-πιστοποίηση (*cross-certification*) (2)

- Δεν είναι λογικό, όλος ο πλανήτης να εμπιστεύεται μια μοναδική ριζική αρχή πιστοποίησης
- Δύο ΑΠ δημιουργούν σχέση εμπιστοσύνης μεταξύ τους (αμφίδρομη ή μονόδρομη) υπογράφοντας η μία το πιστοποιητικό της άλλης
- Μια βασιζόμενη οντότητα Α που εμπιστεύεται τη μία ΑΠ, θα εμπιστεύεται και το πιστοποιητικό μιας οντότητας Β που εκδίδει η δεύτερη ΑΠ.
- Η ΑΠ1 ονομάζεται ‘σημείο εμπιστοσύνης’ (Trust anchor) για την οντότητα Α.
- Οτιδήποτε συνδέεται με αυτό το σημείο εμπιστοσύνης, μέσω μιας έμπιστης διαδρομής, είναι έμπιστο.

Έμπιστου Μεσολαβητή (Bridge CA) (1)

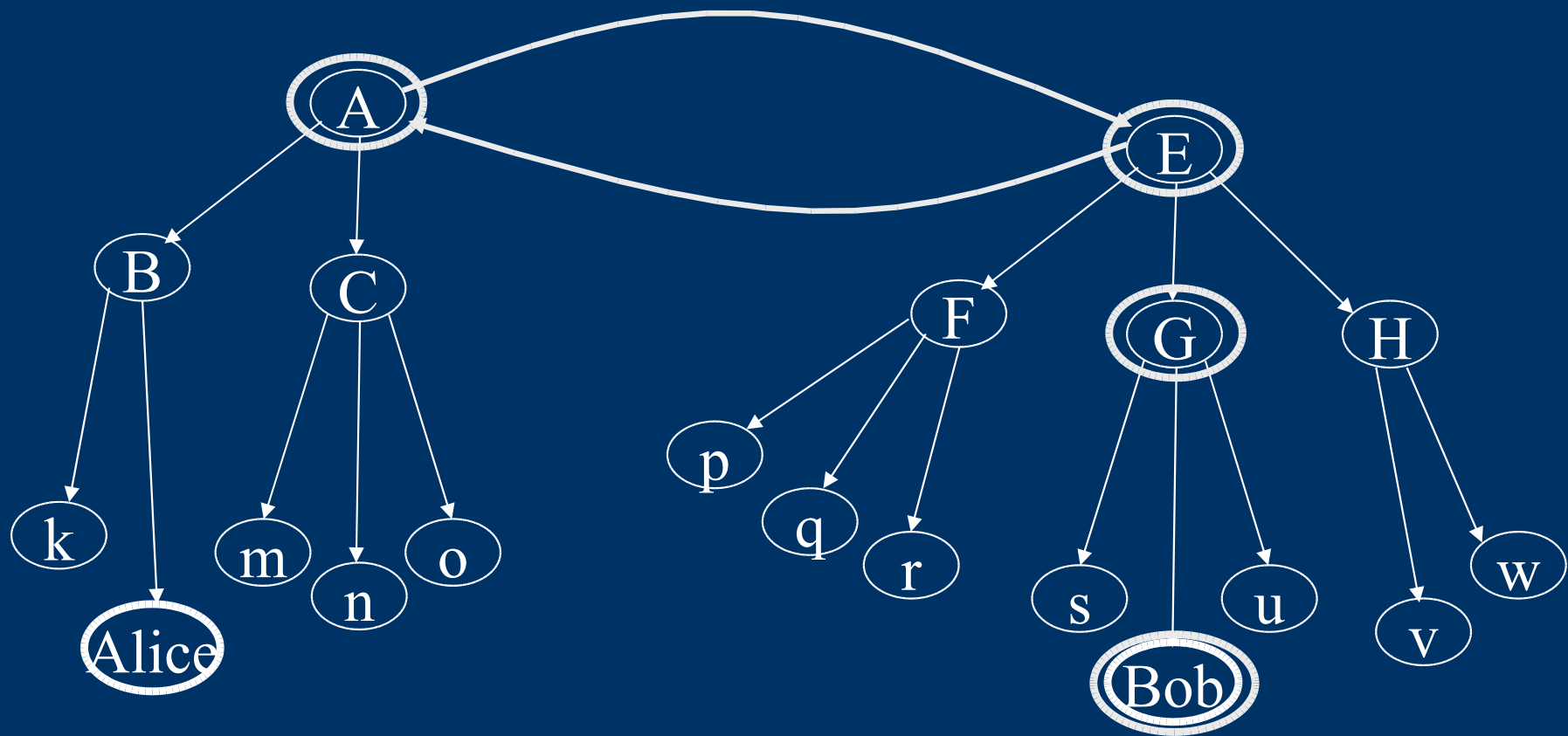


2N σχέσεις εμπιστοσύνης

Έμπιστου Μεσολαβητή (Bridge CA) (2)

- Όλες οι ΑΠ διαπιστοποιούνται με μία κεντρική ΑΠ (Bridge CA) σε σχήμα αστεριού.
 - Μία βασιζόμενη οντότητα που εμπιστεύεται τον έμπιστο μεσολαβητή (σημείο εμπιστοσύνης) εμπιστεύεται και όλες τις ΑΠ που αυτός υποδεικνύει.
 - Ο Έμπιστος Μεσολαβητής δεν είναι ΑΠ.
 - Σχήμα με λιγότερες πιστοποιήσεις
-
-

Μικτά σχήματα εμπιστοσύνης



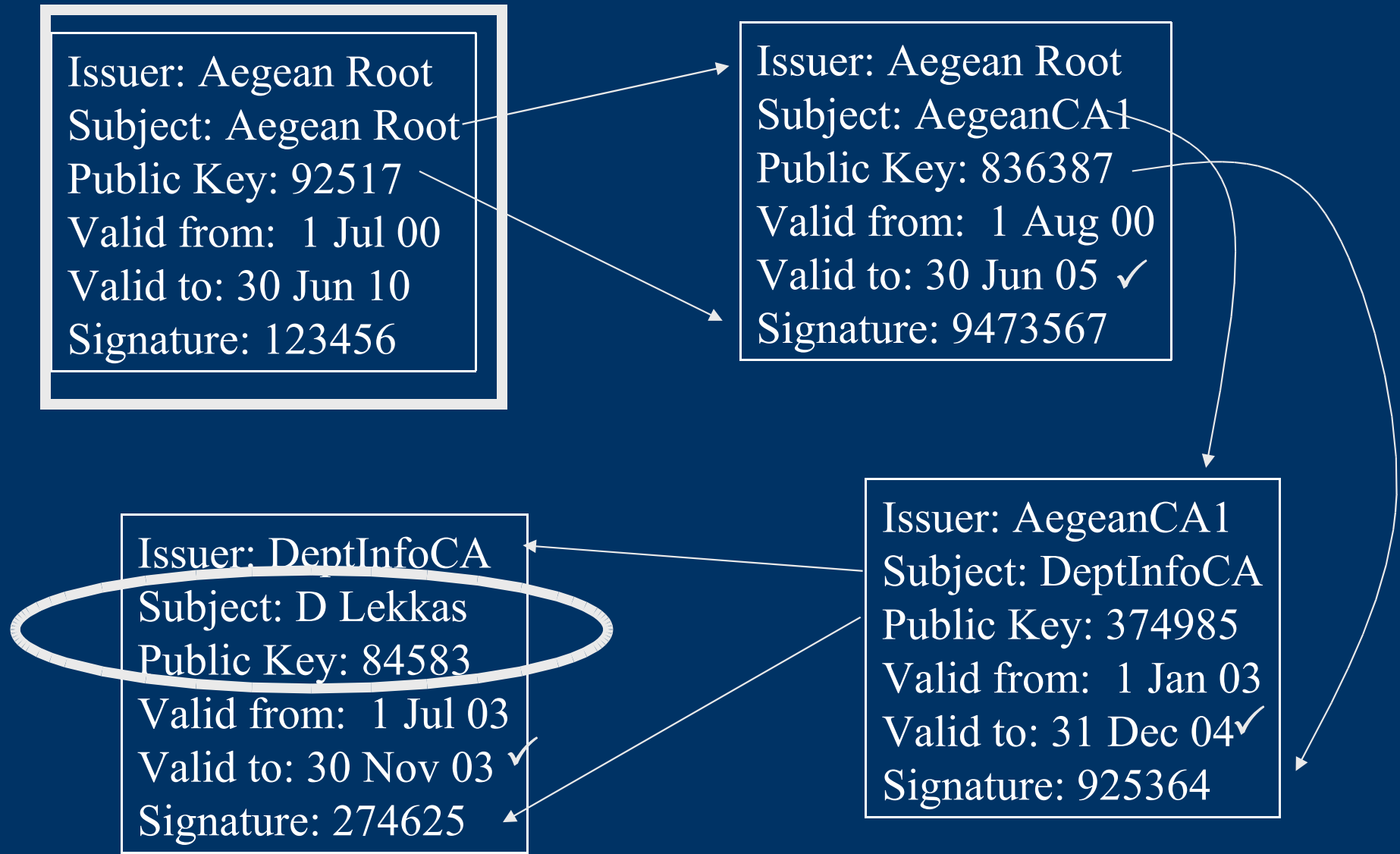
Διαδρομή πιστοποίησης

Issuer: Aegean Root
Subject: Aegean Root
Public Key: 92517
Valid from: 1 Jul 00
Valid to: 30 Jun 10
Signature: 123456

Issuer: Aegean Root
Subject: AegeanCA1
Public Key: 836387
Valid from: 1 Aug 00
Valid to: 30 Jun 05 ✓
Signature: 9473567

Issuer: DeptInfoCA
Subject: D Lekkas
Public Key: 84583
Valid from: 1 Jul 03
Valid to: 30 Nov 03 ✓
Signature: 274625

Issuer: AegeanCA1
Subject: DeptInfoCA
Public Key: 374985
Valid from: 1 Jan 03
Valid to: 31 Dec 04 ✓
Signature: 925364



Δημοσίευση Πληροφοριών

- Δημόσια προσβάσιμοι πόροι οι οποίοι περιέχουν τουλάχιστο:
 - Ψηφιακά Πιστοποιητικά εγγραφόμενων
 - Πληροφορίες κατάστασης πιστοποιητικών (CSI)
 - Δηλώσεις Πολιτικών και Πρακτικών
- Πρόσβαση μέσω διαδικτύου:
 - LDAP (προτιμώμενο για τα πιστοποιητικά)
 - HTTP (προτιμώμενο για τις πολιτικές)
 - FTP (εναλλακτικό)
- Ειδικές περιπτώσεις:
 - Διανομή κλειδιών
 - Διανομή Αυτο-υπογραφόμενων πιστοποιητικών

Κατανεμημένες υπηρεσίες προστιθέμενης αξίας

- Ο ΠΥΠ ως Αρχή Χρονοσήμανσης
 - Ο ΠΥΠ ως Κέντρο Διανομής Κλειδιών
 - Ο ΠΥΠ ως Αρχή Διαχείρισης Δικαιωμάτων
 - Ο ΠΥΠ ως Συμβολαιογραφική Αρχή
 - Ο ΠΥΠ ως Διαχειριστής αποδεικτικών στοιχείων
-
-

Αρχή Χρονοσήμανσης (TimeStamping Authority – TSA)

- Ασφαλής (υπογεγραμμένη) αντιστοίχιση του ίχνους ενός κειμένου με μία ένδειξη χρόνου
 - Λήψη αιτήσεων χρονοσήμανσης
 - Δεν γίνεται επεξεργασία ή αποθήκευση του αρχικού κειμένου, αλλά μόνο της σύνοψής του που του αντιστοιχεί μονοσήμαντα
 - Ανάκτηση χρόνου με ασφαλείς μηχανισμούς όπως NTP και GPS
 - Επαλήθευση της χρονοσφραγίδας από οποιονδήποτε διαθέτει το αρχικό κείμενο
-
-

Εφαρμογές που αξιοποιούν τις ΥΔΚ

Η αξία του PKI έχει άμεση σχέση με την ικανότητα των χρηστών να χρησιμοποιούν τις υπηρεσίες του. Πρέπει να παρέχει κατάλληλο λογισμικό στους πελάτες, που θα υποστηρίζει όλες τις υπηρεσίες που αναφέραμε.

Όλες οι εφαρμογές πρέπει να μπορούν:

- ♦ να χρησιμοποιούν πιστοποιητικά με διαφανή τρόπο και να ελέγχουν την εγκυρότητά τους
- ♦ να επικοινωνούν με ένα σύστημα που κρατά τα αντίγραφα των κλειδιών τους
- ♦ να δημιουργούν τα ζεύγη κλειδιών για τις ψηφιακές υπογραφές
- ♦ να έχουν πρόσβαση σε αποθήκες πιστοποιητικών, ώστε να ελαττωθεί το κόστος διανομής τους

Κέντρο Διανομής Κλειδιών (Key Distribution Center – KDC)

- Παραγωγή κλειδιών υπογραφής εγγραφόμενων:
 - Μόνο κάτω από συγκεκριμένες θεσμικές ή κανονιστικές προϋποθέσεις
 - Η παραγωγή κλειδιών υπογραφής παραμένει υπό τον απόλυτο έλεγχο του ιδιοκτήτη τους σύμφωνα με τη νομοθεσία
 - Είναι δυνατή μόνο με τη χρήση έξυπνων καρτών και την επίσημη δέσμευση του ΠΥΠ ότι δεν αποθηκεύονται κλειδιά
- Παραγωγή κλειδιών εμπιστευτικότητας:
 - Είναι δυνατή η ασφαλής αποθήκευσή τους από τον ΠΥΠ
 - Ανάκτηση κλειδιών (key recovery)
 - Παράδοση κλειδιών (key escrow)
- Ασφαλής διανομή κλειδιών ασφαλών συνόδων σε πολλαπλούς αποδέκτες

S/MIME

Πρωτόκολλο που σχεδιάστηκε για το διαδίκτυο.
Παρέχει ασφάλεια σε εφαρμογές αποθήκευσης και
προώθησης (store-and-forward), όπως το e-mail.

- ◆ Κρυπτογράφηση
- ◆ Ψηφιακή υπογραφή μηνύματος

More Information

- Για το ΥΔΚ:
<http://csrc.nist.gov/pki>
 - VeriSign
 - GlobalSign
 - BT
 - Thawte Certification
-
-

Ασφαλής επικοινωνία

Για να είναι ασφαλής η ανταλλαγή πληροφοριών μεταξύ των συναλλασσόμενων, πρέπει να είναι ασφαλής και η επικοινωνία.

- ◆ Ασφάλεια μηνύματος

Περιλαμβάνει αυθεντικοποίηση, ακεραιότητα μηνύματος, μη απάρνηση της πηγής (ψηφ. υπογραφές), εμπιστευτικότητα (κρυπτογραφία)

- ◆ Ασφάλεια μεταξύ πελάτη / εξυπηρετητή

Ασφάλεια πελάτη/εξυπηρετητή

Αφορά την ύπαρξη ενός πρωτοκόλλου δύο επιπέδων. Στο χαμηλότερο επίπεδο, πάνω από ένα αξιόπιστο πρωτόκολλο μεταφοράς, υπάρχει ένα Πρωτόκολλο Εγγραφής (Record Protocol) που ενθυλακώνει πρωτόκολλα υψηλότερου επιπέδου

Ένα τέτοιο πρωτόκολλο μπορεί να επιτρέπει στον πελάτη και τον εξυπηρετητή να διαπραγματεύονται τον κρυπτογραφικό αλγόριθμο και τα κλειδιά, πριν το πρωτόκολλο εφαρμογής μεταδώσει ή λάβει δεδομένα.

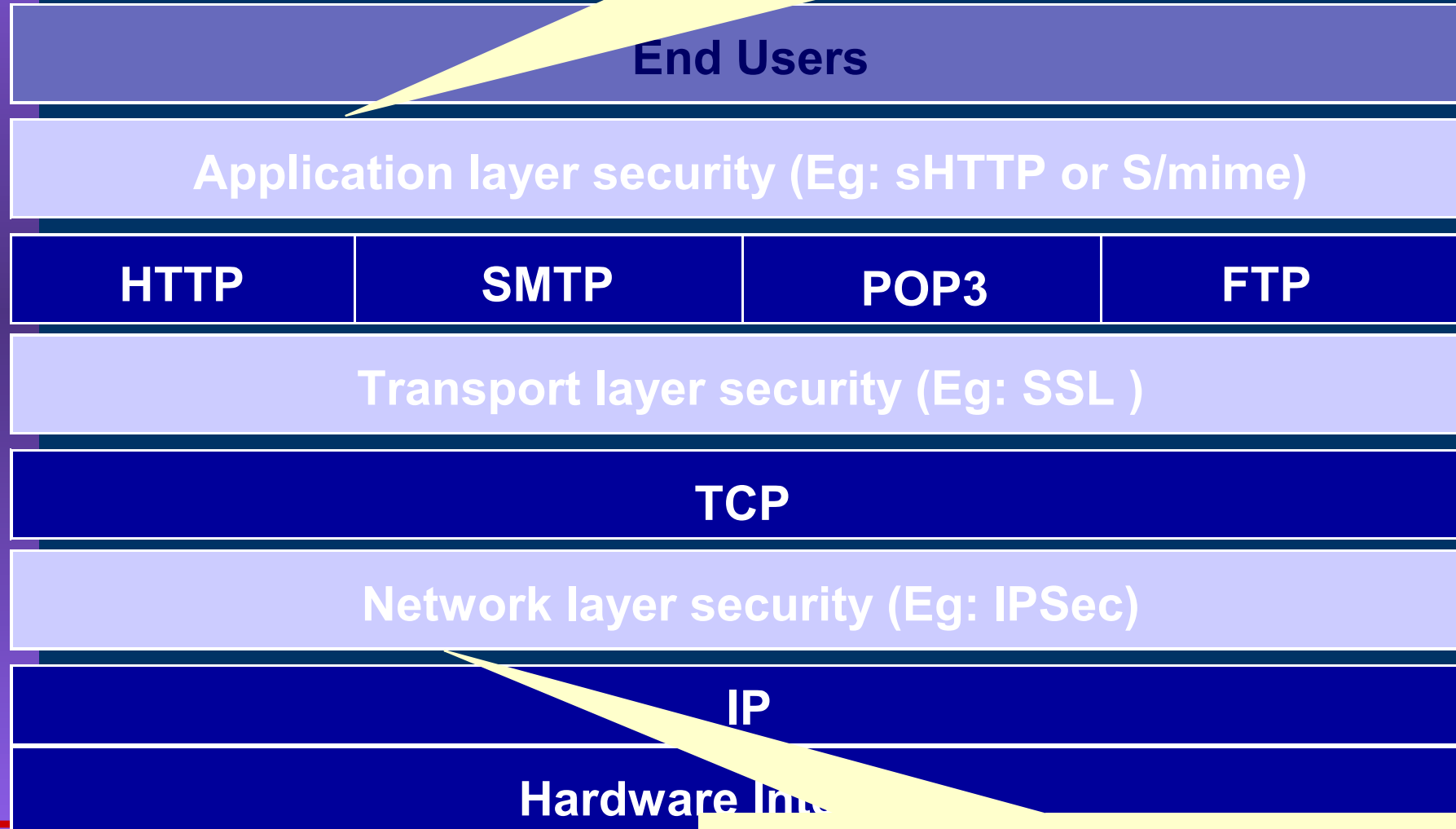
Ασφάλεια σύνδεσης

- ♦ Η κρυπτογραφία χρησιμοποιείται μετά από από την αρχική «χειραψία» (handshake) όπου ορίζεται ένα μυστικό κλειδί. Η συμμετρική κρυπτογραφία χρησιμοποιείται για την κρυπτογράφηση.
- ♦ Η αυθεντικοποίηση των οντοτήτων γίνεται με κρυπτογραφία δημόσιου κλειδιού



Προστασία σε επίπεδα

- κρυπτογράφηση μηνυμάτων, όπως e-mail
- απευθείας αυθεντικοποίηση των τελικών χρηστών



- κρυπτογράφηση IP πακέτων
- αυθεντικοποίηση συσκευών, όπως routers

Ασφάλεια επιπέδου μεταφοράς

- ◆ κρυπτογραφεί μηνύματα μεταξύ TCP/IP πελατών και εξυπηρετητών
- ◆ αυθεντικοποίηση TCP/IP πελατών και εξυπηρετητών

Για web εφαρμογές, η ασφάλεια στο επίπεδο μεταφοράς εφαρμόζεται από έναν παρουσιαστή ιστοσελίδων (browser).

Η ασφάλεια της εφαρμογής δεν εξαντλείται με την αυθεντικοποίηση. Χρειάζεται και έλεγχος πρόσβασης.

Secure Socket Layer (SSL)

Πρωτόκολλο ασφάλειας στο επίπεδο μεταφοράς για την επικοινωνία client/server (Netscape)

Υπηρεσίες:

- κρυπτογράφηση δεδομένων
- αυθεντικοποίηση εξυπηρετητή και πελάτη

SSL 2.0 - server authentication

SSL 3.0 - client/server authentication

- ◆ στον πελάτη, το SSL αποτελεί μέρος του λογισμικού του browser
- ◆ στον εξυπηρετητή, αποτελεί μέρος του λογισμικού του

Λειτουργία του SSL

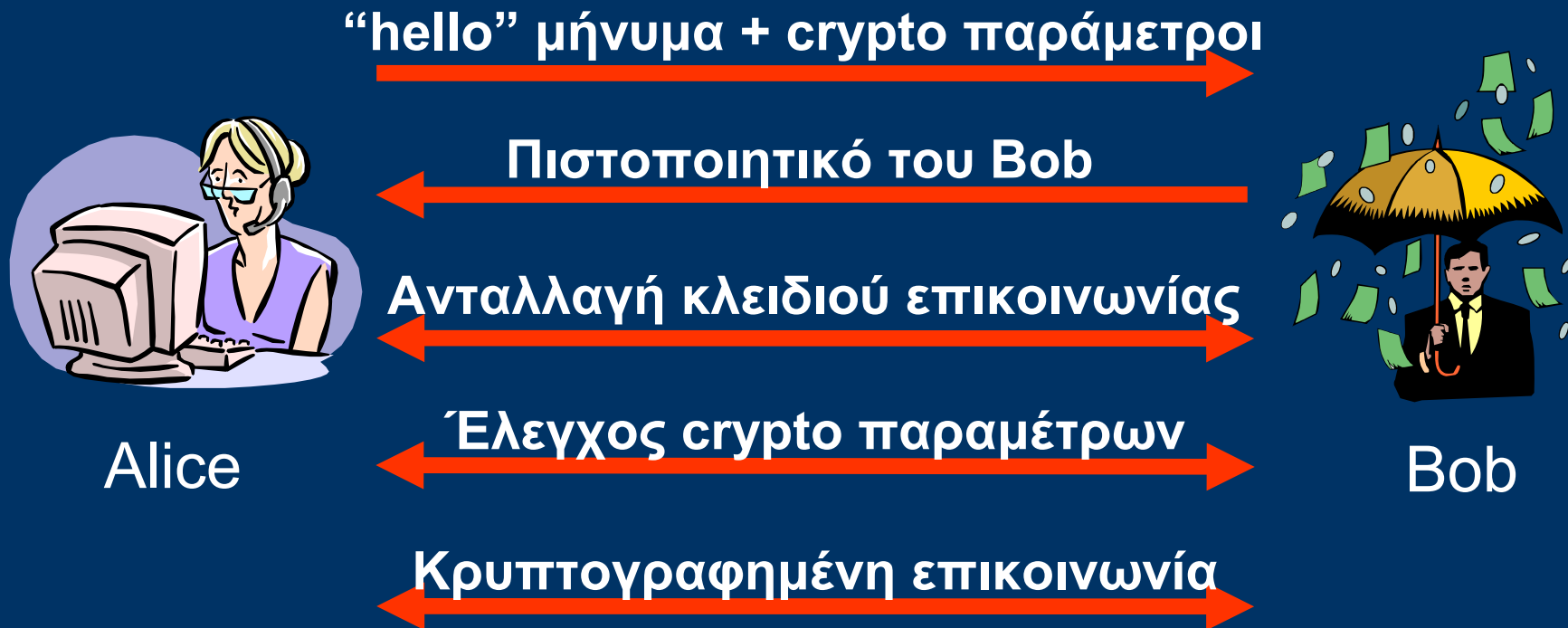
(Συνδυασμός Ασύμμετρης και Συμμετρικής Επικοινωνίας)

- Ο client κάνει μία κλήση στον server και εκείνος του στέλνει το δημόσιο κλειδί του (ή το ψηφιακό πιστοποιητικό κρυπτογραφημένο με το δημόσιο κλειδί του)
- Ο client δημιουργεί έναν τυχαίο αριθμό και τον κρυπτογραφεί με το δημόσιο κλειδί του server, δημιουργεί και ένα κλειδί 128 bits για την υπόλοιπη επικοινωνία τους
- Τον τυχαίο αριθμό και το κλειδί επικοινωνίας τα κρυπτογραφεί με το δημόσιο κλειδί του server και τα στέλνει στο server
- Ο server με το ιδιωτικό του κλειδί το αποκρυπτογραφεί και στη συνέχεια χρησιμοποιώντας το κλειδί των 128 bits συνεχίζει να επικοινωνεί με τον client με συμμετρική πλέον κρυπτογραφία

Πληρωμές με πιστωτική κάρτα: Secure Sockets Layer (SSL)

- Netscape 94
- Ενσωματωμένο στους web browsers

ΠΑΛΗΡΩΜΕΣ



Πληρωμές με πιστωτική κάρτα: Περιορισμοί στη Χρήση του SSL

ΠΛΗΡΩΜΕΣ

Η Alice πρέπει να ελέγξει την ορθότητα

“hello” μήνυμα + crypto parameters

Διάφοροι περιορισμοί μπορεί να υπονομεύουν την ασφάλεια

Πιστοποιητικό του Bob

Ανταλλαγή κλειδιού επικοινωνίας

Έλεγχος crypto παραμέτρων

Κρυπτογραφημένη επικοινωνία

Δεν υπάρχει καταλογισμός ευθύνης

Ο Bob γίνεται στόχος για Hackers



Alice



Bob

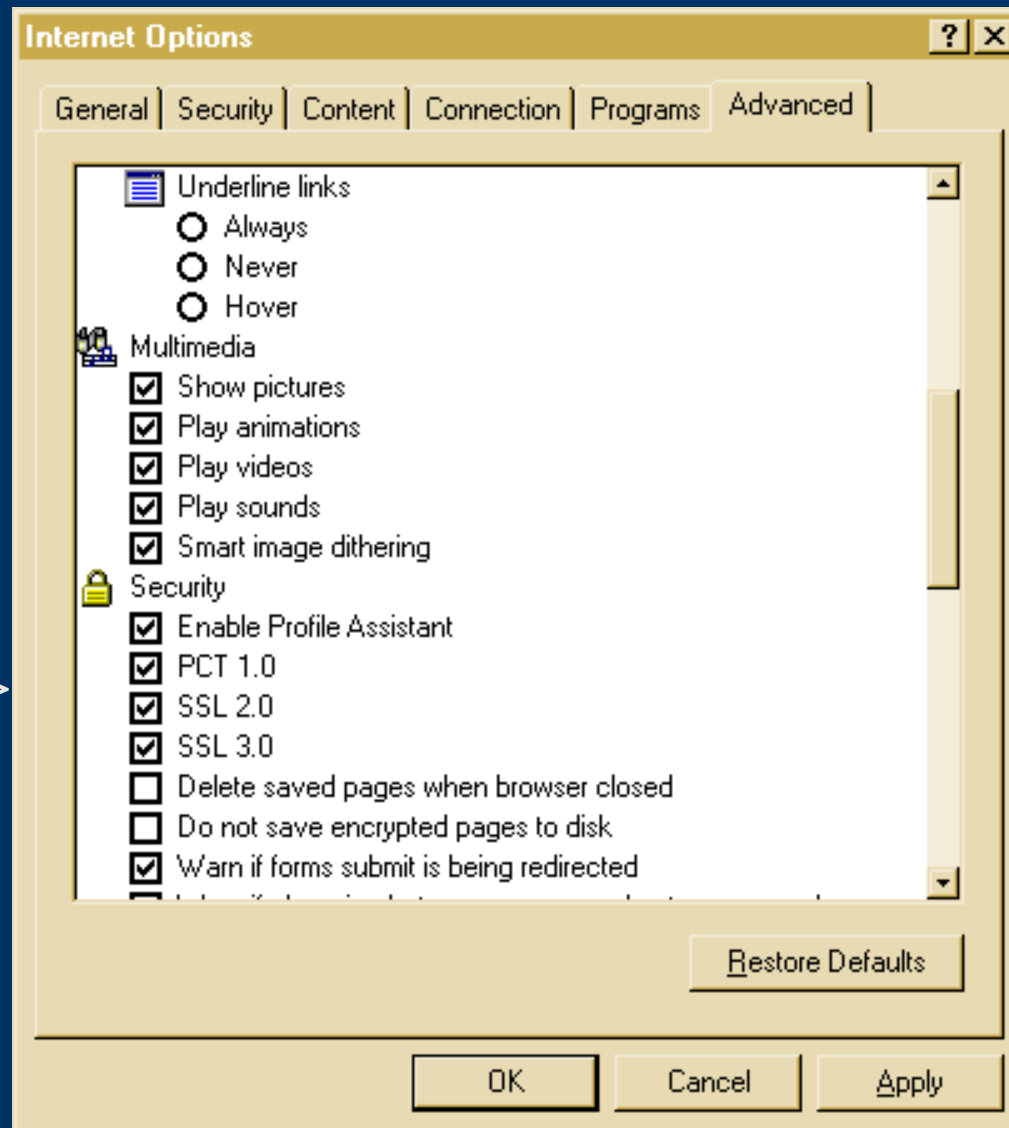
Ενεργοποίηση του SSL

Στο IE 4.0

Control Panel >

Internet Options >

Advanced



Υπηρεσίες διαπραγμάτευσης του SSL

- ◆ Φάση χειραψίας (Handshake)
 - Αυθεντικοποίηση πελάτη, εξυπηρετητή
 - Καθορισμός των αλγορίθμων κρυπτογράφησης, των συμμετρικών κλειδιών
- ◆ Φάση μεταφοράς δεδομένων
 - κρυπτογράφηση
 - έλεγχοι ακεραιότητας
- ◆ Όλες οι επικοινωνίες συμβαίνουν πάνω από ένα πρωτόκολλο εγγραφής (Record protocol)

Υπηρεσίες διαπραγμάτευσης SSL Handshake

1. Client Hello
 2. Server Hello
 3. Client Master Key
 4. Client Finished
 5. Server Verify
 6. Request Certificate
 7. Client Certificate
 8. Server Finished
- } προαιρετικά

SSL Handshake - 1. Client Hello

- ◆ η σύνοδος ξεκινά με αίτηση του πελάτη
 - ο browser κάνει μια HTTPs αίτηση
- ◆ Client Hello είναι μη κρυπτογραφημένο μήνυμα με
 - ✓ έκδοση του SSL
 - ✓ δυνατότητες κρυπτογράφησης του πελάτη (αλγόριθμοι, μήκη κλειδιών)
 - ✓ ταυτότητα της συνόδου (Session ID)
 - είναι δυνατό να χρησιμοποιηθεί μια προηγούμενη σύνοδος που είχε ανοίξει μεταξύ του πελάτη και του εξυπηρετητή
 - ✓ μια τυχαία δημιουργημένη ακολουθία χαρακτήρων (Client Challenge)

SSL Handshake - 2. Server Hello

- ◆ Εάν ο εξυπηρετητής ξεκινά μια νέα σύννοδο, τότε το Server Hello είναι ένα μη κρυπτογραφημένο μήνυμα με
 - ✓ δυνατότητες κρυπτογράφησης του εξυπηρετητή (αυτές που υποστηρίζει σε σχέση με τον πελάτη)
 - ✓ ταυτότητα σύνδεσης (Connection ID)
 - ✓ ψηφιακό πιστοποιητικό του εξυπηρετητή
- ◆ Εάν επαναχρησιμοποιείται μια προηγούμενη σύνδεση, τότε το μόνο που χρειάζεται είναι να δημιουργήσει μια νέα σύνδεση

SSL Handshake - 3. Client Master Key

Μετά από την εγκατάσταση μιας νέας συνόδου:

- ✓ Ο πελάτης εξετάζει την εγκυρότητα του πιστοποιητικού του εξυπηρετητή (verification), ελέγχει αν έχει ανακληθεί (revocation)
- ✓ Στέλνει τις τελικές παραμέτρους κρυπτογράφησης (μεταξύ αυτών που προτείνει ο εξυπηρετητής - ο οποίος μπορεί να επιβάλει τις παραμέτρους)
- ✓ Δημιουργεί το κλειδί της συνόδου (Session Key)
 - συμμετρικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων της εφαρμογής
 - το κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρετητή

SSL Handshake - 4. Client Finished

- ✓ Σηματοδοτεί την ετοιμότητα του πελάτη να στείλει και να λάβει δεδομένα
 - ✓ Η κρυπτογράφηση του Session ID με χρήση του συμμετρικού κλειδιού της συνόδου και αποστολή του στον εξυπηρετητή
-
- Διαφορετικό κλειδί (session key) σε κάθε σύνδεση (24 h)
 - Κρυπτογραφία δημόσιου κλειδιού για την ανταλλαγή του κλειδιού συνόδου και την αυθεντικοποίηση
 - Η κρυπτογράφηση της συνόδου χρησιμοποιεί συμμετρική κρυπτογραφία (ταχύτητα)

SSL Handshake - 5. Server Verify

- ✓ Ο εξυπηρετητής κρυπτογραφεί το client challenge με το κλειδί της συνόδου που δημιουργεί ο πελάτης

Αυθεντικοποίηση του εξυπηρετητή γιατί:

- ♦ απαιτείται ένα ιδιωτικό κλειδί που αντιστοιχεί στο πιστοποιητικό εξυπηρετητή για την αποκρυπτογράφηση του session key

SSL Handshake - 6. Request Certificate

Αίτηση του εξυπηρετητή για αυθεντικοποίηση του πελάτη

- Ρύθμιση του εξυπηρετητή, SSL 3.0

Στέλνει την αίτηση στα πλαίσια της κρυπτογραφημένης συνόδου που ξεκίνησε και:

- ✓ ζητά να χρησιμοποιήσει ο πελάτης το ιδιωτικό κλειδί του για να υπογράψει ψηφιακά τα:
 - κλειδί συνόδου
 - μια τυχαία ακολουθία χαρακτήρων (Certificate Challenge Data)
 - το πιστοποιητικό του εξυπηρετητή
- ✓ λίστα των αποδεκτών CA (μόνο για SSL 3.1)

SSL Handshake - 7. Client Certificate

Ο πελάτης στέλνει τα:

- ✓ ψηφιακό πιστοποιητικό του
- ✓ υπογράφει ψηφιακά τα δεδομένα που του ζήτησε ο εξυπηρετητής (Challenge data)

Αν το πιστοποιητικό του δεν έχει εκδοθεί από μια από τις αποδεκτές CAs, τότε η σύννοδος τερματίζεται.

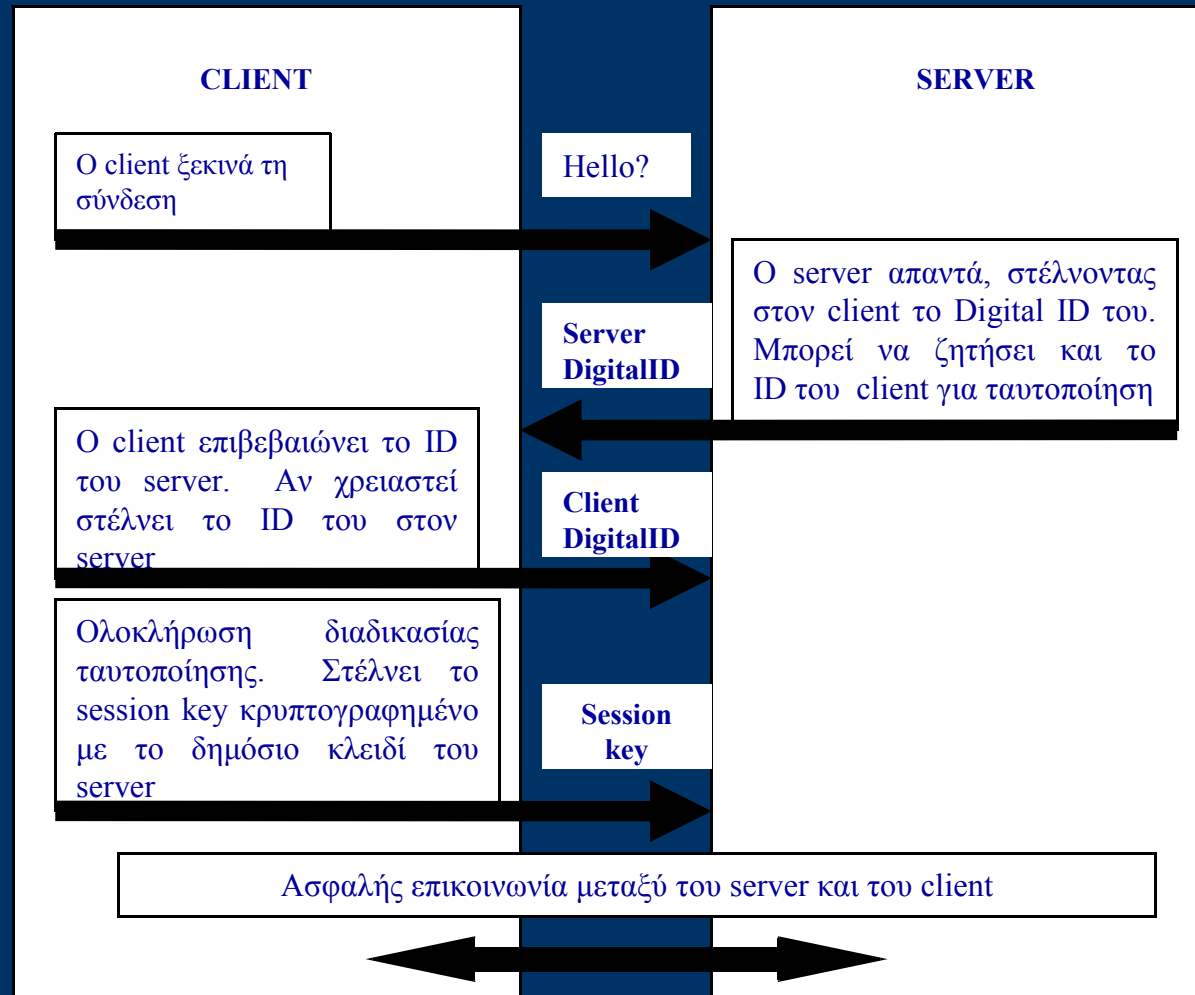
SSL Handshake - 8. Server Finished

Ο εξυπηρετητής στέλνει ένα κρυπτογραφημένο μήνυμα που περιέχει την ταυτότητα της συνόδου (Session ID). Το βήμα αυτό αποτελεί την εγκαθίδρυση από την αρχή της συνόδου που ήδη χρησιμοποιούσαν, χωρίς τα ενδιάμεσα βήματα αυθεντικοποίησης

Αυτό το μήνυμα σηματοδοτεί την ετοιμότητα του εξυπηρετητή να στείλει και να λάβει δεδομένα

Όλα τα δεδομένα του πρωτοκόλλου εφαρμογής κρυπτογραφούνται με το κλειδί συνόδου.

Πρωτόκολλο SSL



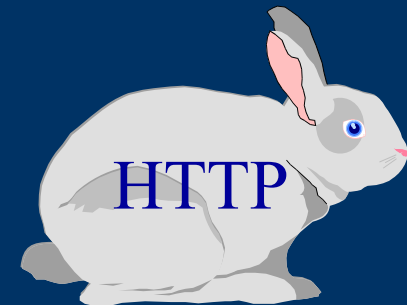
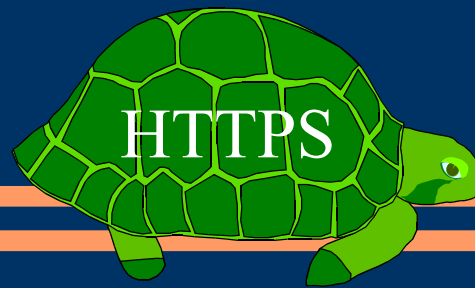
Όλες οι πληροφορίες (HTTP αιτήσεις, URLs, φόρμες) που ανταλλάσσονται είναι κρυπτογραφημένες

SSL Overhead

Αιτίες καθυστέρησης

- Η αρχική σύνδεση όπου κανονίζονται οι λεπτομέρειες σύνδεσης και ανταλλάσσονται οι πληροφορίες κρυπτογράφησης
- Η κρυπτογράφηση των δεδομένων σε κάθε υπολογιστή
- Τα κρυπτογραφημένα δεδομένα έχουν μεγαλύτερο όγκο

Εφαρμογή σε ιστοσελίδες και όχι σε ολόκληρο web site



Μερικές Υλοποιήσεις με SSL

- OpenSSL (<http://www.openssl.org/>)-- Provides Information about a free, open-source implementation of SSL.
 - Apache-SSL (<http://www.apache-ssl.org/>)-- Describes Apache-SSL, a secure Webserver, based on Apache and SSLesy/OpenSSL.
-
-

Μερικές Υλοποιήσεις με SSL

- SSLeay (<ftp://ftp.uni-mainz.de/pub/internet/security/ssl/SSL/>) -- a free implementation of Netscape's Secure Socket Layer
 - Planet SSL (<http://www.rsasecurity.com/standards/ssl/developers.html>)-- provides C-programs and Java-programs of SSL.
-
-

Απαιτήσεις για έλεγχο πρόσβασης

Η πρόσβαση σε ευαίσθητες πληροφορίες απαιτεί εκτός από την αυθεντικοποίηση (authentication) του χρήστη, να έχει και την εξουσιοδότηση να δράσει σε αυτή (authorization).

Προνόμια:

- ♦ σε κάθε χρήστη
- ♦ σε ομάδα χρηστών όπου κάθε χρήστης κληρονομεί τα προνόμια της ομάδας που ανήκει

Ο έλεγχος πρόσβασης (Access Control) επιβάλλει την εξουσιοδότηση, περιορίζοντας την πρόσβαση στην εφαρμογή σε χρήστες με τα κατάλληλα προνόμια.

Η φάση SSL Handshake αυθεντικοποιεί τους χρήστες, αλλά δεν εξετάζει την εξουσιοδότηση τους στην εφαρμογή.

Εξουσιοδότηση με Πιστοποιητικά

Η πρόσβαση στις πληροφορίες ενός εξυπηρετητή μπορεί να ελεγχθεί αντιστοιχίζοντας τα πιστοποιητικά των χρηστών σε λογαριασμούς χρηστών και αναθέτοντας δικαιώματα στους λογαριασμούς με τη βοήθεια μιας **Λίστας Ελέγχου Πρόσβασης (Access Control List - ACL)**

Λίστα Ελέγχου Πρόσβασης: είναι ένα σύνολο από κανόνες και ορίζει τις ομάδες και τους χρήστες που έχουν ή δεν έχουν πρόσβαση

(DAC - MAC - RBAC Policies)

Πιστοποιητικά vs συνθηματικά

- δεν στέλνονται συνθηματικά στο δίκτυο μεταξύ πελάτη και εξυπηρετητή
 - τα πιστοποιητικά είναι δημόσιες πληροφορίες και άρα οι χρήστες δεν ανταλλάσσουν ευαίσθητες πληροφορίες στο δίκτυο
- καλύτερη αυθεντικοποίηση των χρηστών σε σχέση με αυθεντικοποίηση από IP διευθύνσεις, e-mail
- απλούστερη διαχείριση - μπορεί να ρυθμιστεί ο εξυπηρετητής ώστε να επιτρέπει πρόσβαση σε χρήστες που παρουσιάζουν πιστοποιητικό από μια συγκεκριμένη CA (δεν χρειάζεται να διατηρούν λίστες ελέγχου πρόσβασης)

Συμπεράσματα

- *Οι κίνδυνοι για τους χρήστες, τα δεδομένα και τις συναλλαγές είναι υπαρκτοί.*

Οι Υποδομές Δημόσιου Κλειδιού μπορούν να αποτελέσουν τη βάση για την οικοδόμηση εμπιστοσύνης στο διαδίκτυο μεταξύ των συναλλασόμενων

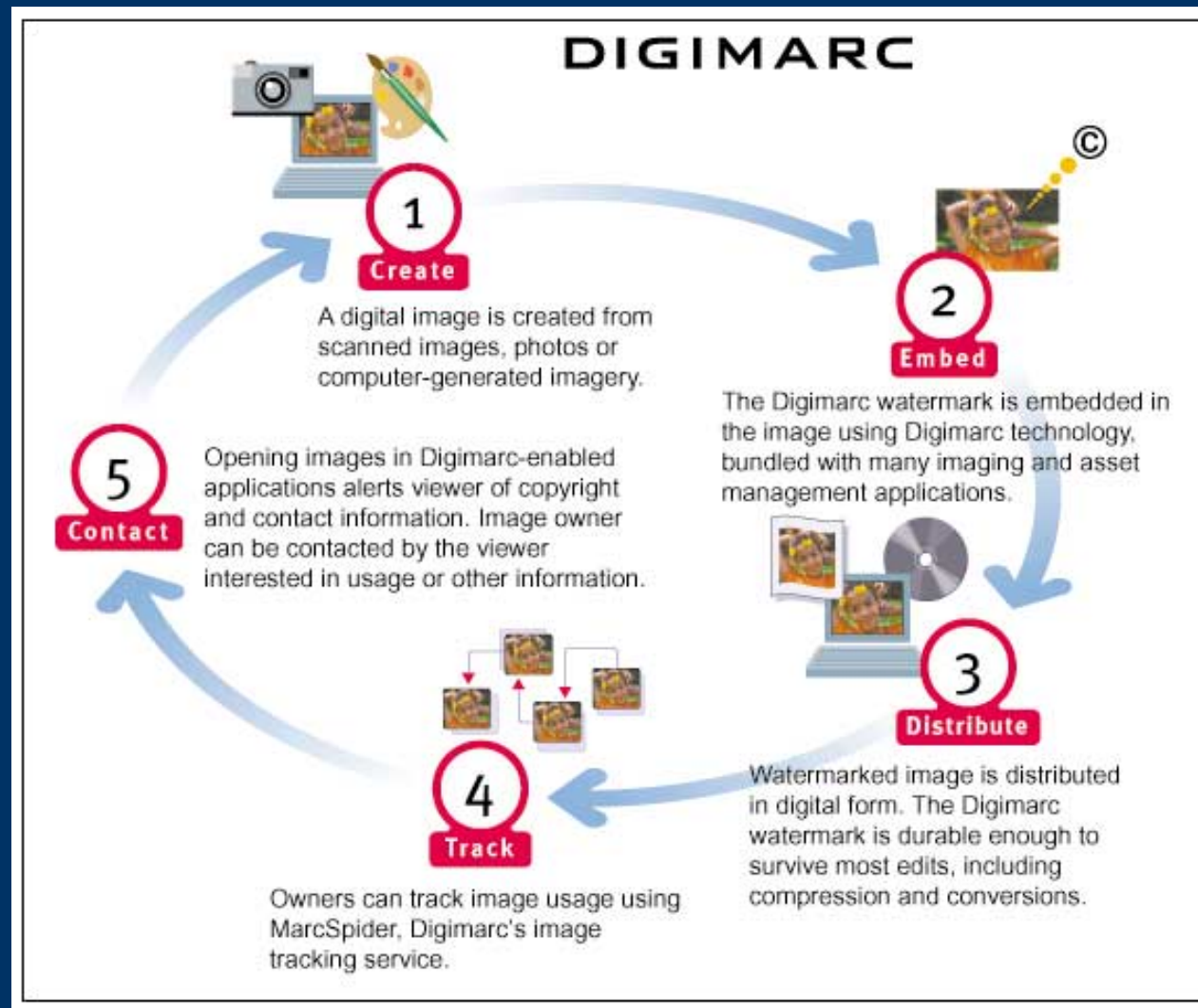
Πώς ορίζει ο καθένας την εμπιστοσύνη;

TRUST?
TRUST?



Your questions are welcome!

Digital Watermarks



Retrieving information from pictures



Image with other
hidden within



Recreated image

http://www.cl.cam.ac.uk/~fapp2/steganography/image_downgrading/

Έξυπνες κάρτες- Smart Cards



Τύποι καρτών

- Κάρτες μνήμης (memory cards): Μόνο αποθήκευση και ανάγνωση δεδομένων
- Κάρτες με μικροεπεξεργαστή (microprocessor intelligent cards): Ικανοποιητική υπολογιστική δυνατότητα με χαμηλό κόστος
- Υπερ-κάρτες (super smart cards): Με πληκτρολόγιο, οθόνη και φωτοβολταϊκή τροφοδοσία
- Ασύρματες κάρτες (Contactless cards): Αναγνώριση του κωδικού της κάρτας σε απόσταση <math>< 30\text{cm}</math> από τον αναγνώστη
- Υβριδικές κάρτες (Hybrid cards): Contactless + Microprocessor
 - Case study: Πανεπιστήμιο Αιγαίου

Χρήση στην ΥΔΚ

- Ειδικές κάρτες με ‘μικροεπεξεργαστή Δημόσιου Κλειδιού’ και μνήμη >32Kb
- Ιδανικές για την αποθήκευση ιδιωτικών κλειδιών:
 - Το ζεύγος κλειδιών μπορεί να παραχθεί ‘εντός’ της κάρτας
 - Η υπογραφή ή η αποκρυπτογράφηση μπορεί να γίνει ‘εντός’ της κάρτας
 - Το ιδιωτικό κλειδί δεν εξάγεται ποτέ από την κάρτα
 - Είναι εύκολα μεταφέρσιμες
 - Προστατεύουν τα δεδομένα με μηχανισμούς ασφάλειας και PIN
 - Μεγάλη αξιοπιστία και αντοχή

XML ενδεικτική δομή χρονοσφραγίδας

- <timestamp>
- <TSA_certificate>...binary data...</TSA_certificate>
- <message_hash>
- <algorithm_id>SHA-1</algorithm_id>
- <hash_value>AB00123F7B5D01</hash_value>
- </message_hash>
- <secure_time>
- <source>GPS</source>
- <time>1001531700</time>
- <format>seconds since 1-1-1900</format>
- <zone>GMT+2</zone>
- <accuracy>+/- 0.13 seconds</accuracy>
- </secure_time>
- <serial_no>000532</serial_no>
- <timestamp_sign>...binary data...</timestamp_sign>
- <sign_algorithm>MD5+RSA</sign_algorithm>
- </timestamp>