Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

Πιστοποίηση X.509

Το πρόβλημα...

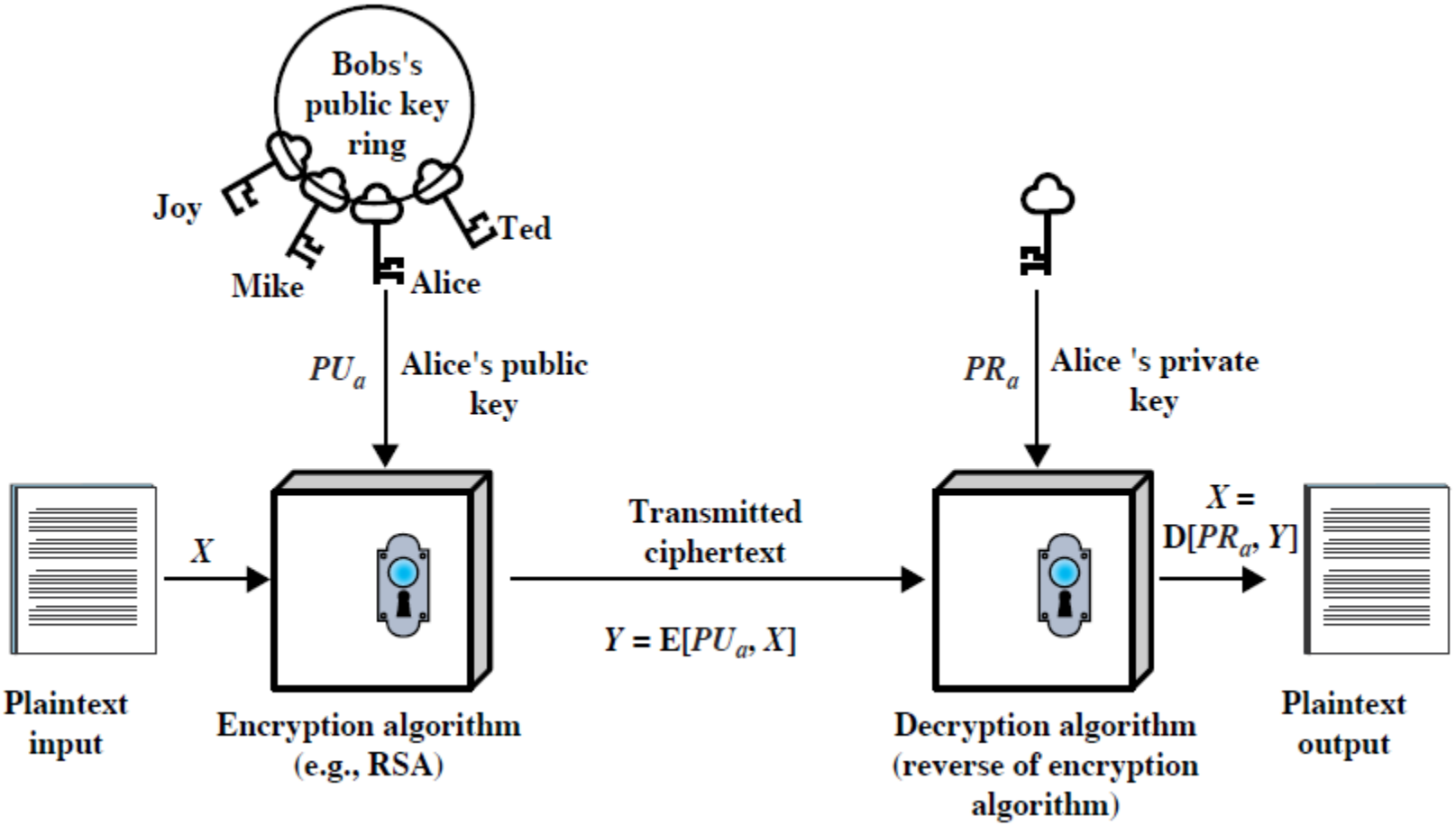
- Κατά τα γνωστά, η Alice και ο Bob θέλουν να επικοινωνήσουν...

- Αλλά υπάρχουν θέματα αναφορικά με:
  - την ταυτότητα του άλλου
  - τη μυστικότητα της επικοινωνίας
  - την ακεραιότητα των πληροφοριών
  - τη μη αποποίηση ευθύνης
- Τα θέματα λύνονται εν μέρει με τη χρήση κρυπτογραφικών μηχανισμών
  - Κρυπτογραφία Δημοσίου Κλειδιού
  - Ψηφιακές υπογραφές

Επανάληψη: Κρυπτογραφία δημοσίου κλειδιού

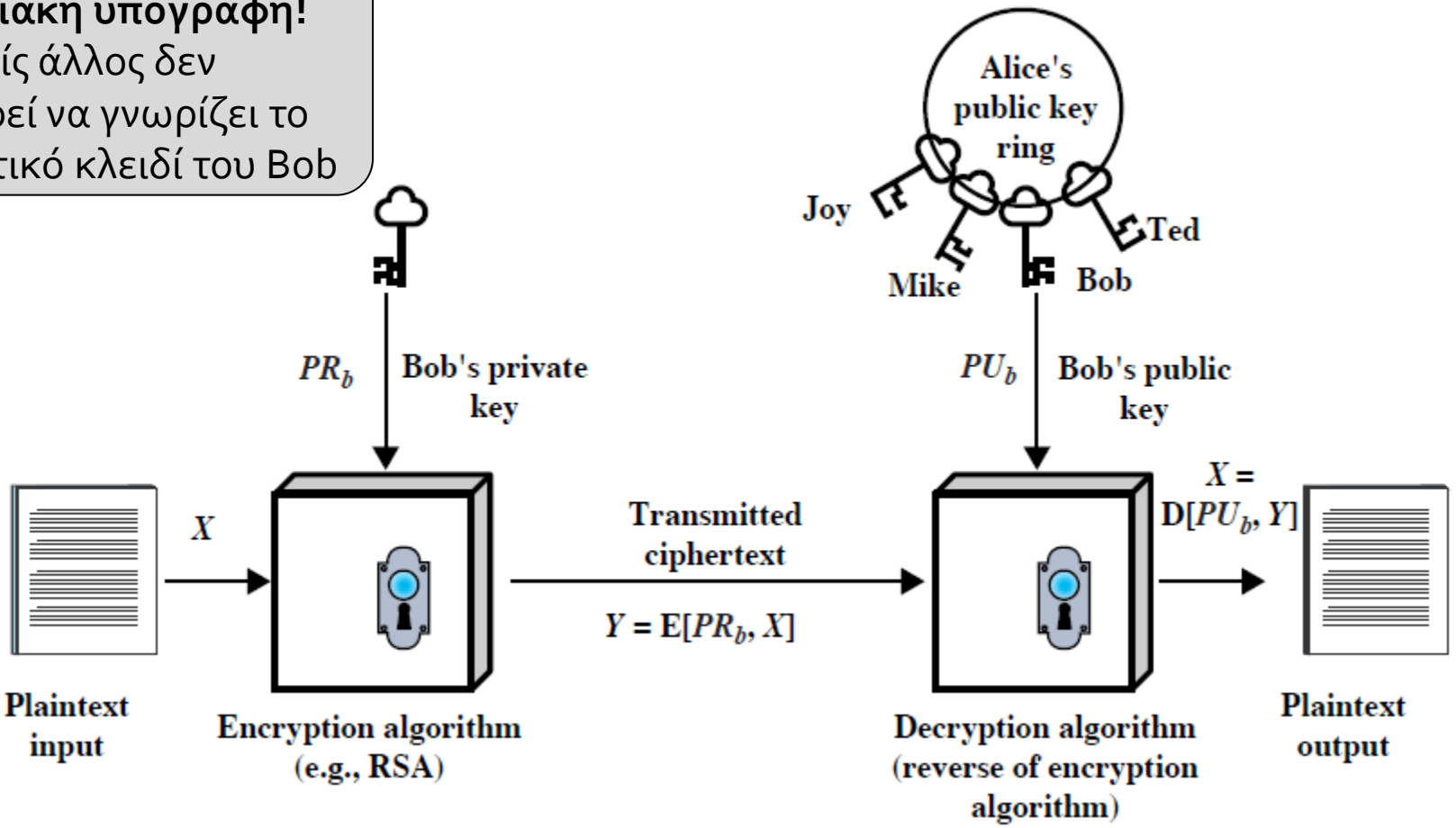
- Diffie & Hellman, 1976
- Ασύμμετρη κρυπτογραφία, με χρήση ζεύγους κλειδιών:
  - Ιδιωτικό κλειδί (private key), το οποίο παραμένει μυστικό
  - Δημόσιο κλειδί (public key), το οποίο καθίσταται γνωστό
- Βασίζεται σε μαθηματικές συναρτήσεις
- Βασική λογική: ό,τι κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται με το άλλο κλειδί
- Σημαντικές εφαρμογές:
  - Κρυπτογράφηση & αποκρυπτογράφηση
  - Διανομή κλειδιών
  - Ψηφιακές υπογραφές
- Αντιπροσωπευτικοί αλγόριθμοι:
  - Diffie-Hellman
  - Rivest-Shamir-Adleman (RSA)
  - Κρυπτογραφία ελλειπτικής καμπύλης (elliptic-curve cryptography)

Επανάληψη: Κρυπτογράφηση με ΚΔΚ



Επανάληψη: Πιστοποίηση αυθεντικότητας με ΚΔΚ

Ψηφιακή υπογραφή!
Κανείς άλλος δεν μπορεί να γνωρίζει το ιδιωτικό κλειδί του Bob



Επανάληψη: Πιστοποιητικά δημοσίου κλειδιού

- Θέμα: εφόσον το δημόσιο κλειδί είναι δημόσιο, ο καθένας μπορεί να δημοσιεύσει ένα κλειδί προσποιούμενος ότι είναι κάποιος άλλος
- π.χ.: κάποια ιστοσελίδα υποκρίνεται ότι είναι το amazon.com, δημοσιεύοντας και κάποιο αντίστοιχο δημόσιο κλειδί
- Λύση: πιστοποιητικά δημοσίου κλειδιού (Public Key Certificates), τα οποία πιστοποιούν με κρυπτογραφικό τρόπο την πατρότητα ενός δημοσίου κλειδιού
- Τα πιστοποιητικά δημοσίου κλειδιού εκδίδονται (και υπογράφονται) από "έμπιστες οντότητες"
  - Κυβερνητικούς οργανισμούς (π.χ., ΣΥΖΕΥΞΙΣ)
  - Φορείς κοινής αποδοχής (π.χ., VeriSign)

X.509

- X.500: σειρά προτύπων της ITU που αφορούν τη δημιουργία και διαχείριση υπηρεσιών καταλόγου (directory services)
- Κατάλογος: μητρώο πληροφοριών για οντότητες ενός συστήματος

  "*The Directory is a collection of open systems which cooperate to hold a logical database of information about a set of objects in the real world.*"

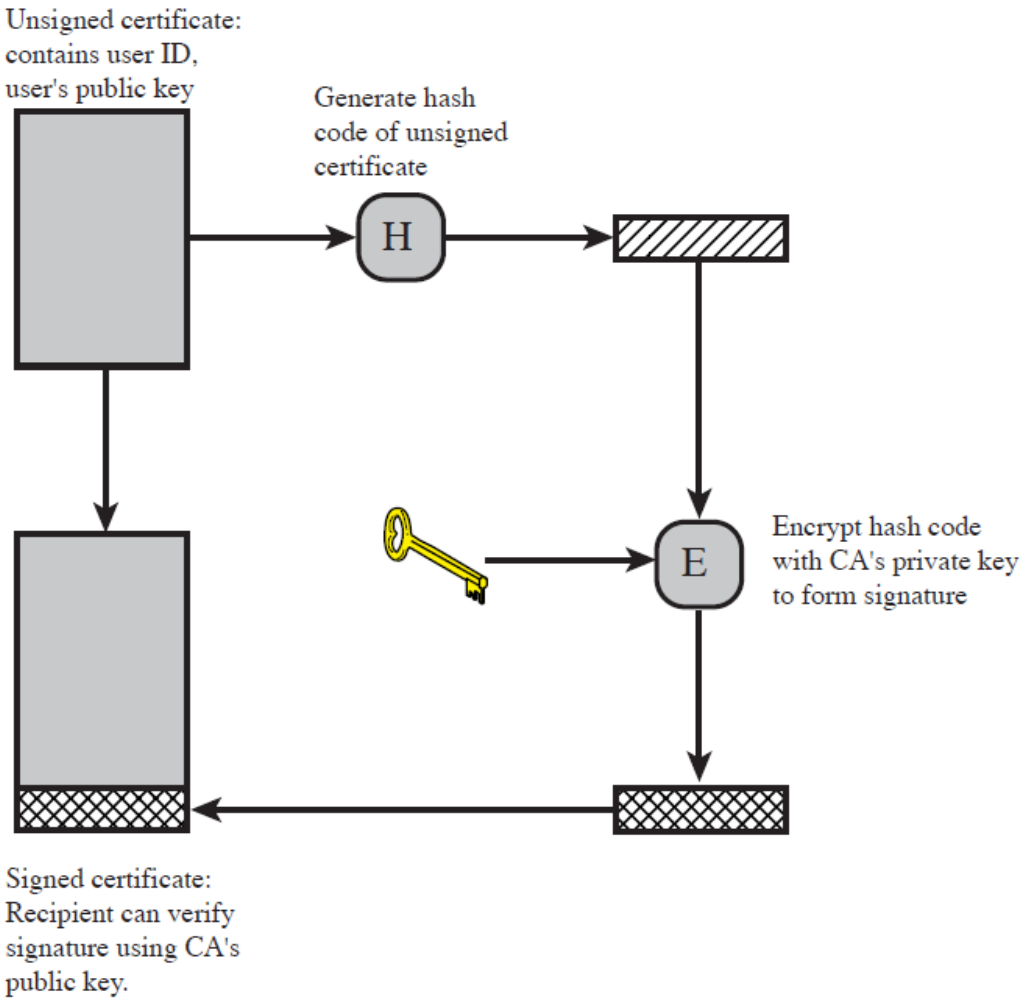
  (The Directory: Overview of concepts, models and services, ITU-T Recommendation X.500)

  - π.χ., οι χρήστες του pelopas.uop.gr είναι οργανωμένοι σε έναν τέτοιο κατάλογο
- X.509: σύσταση της ITU, μέρος του X.500, που αναφέρεται στα ψηφιακά πιστοποιητικά
- Χρησιμοποιείται από πληθώρα εφαρμογών και υπηρεσιών: SSL/TLS, IPSec, S/MIME, κλπ.

Ψηφιακά πιστοποιητικά X.509

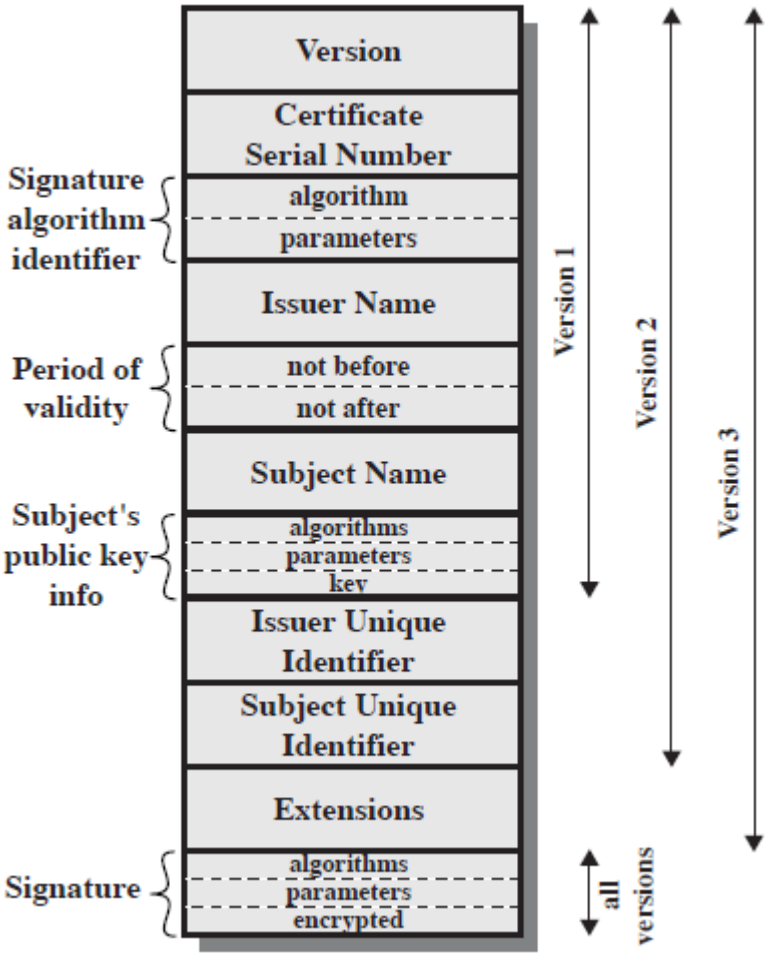
- Πιστοποιητικά Δημοσίου Κλειδιού (Public Key Certificates)
  - Εμπεριέχει το δημόσιο κλειδί κάποιας οντότητας
  - Είναι υπογεγραμμένο από κάποια τρίτη "έμπιστη" οντότητα, την Αρχή Πιστοποίησης (Certification Authority – CA)
  - Οι αποδέκτες του πιστοποιητικού μπορούν να είναι βέβαιοι αναφορικά με την προέλευση του πιστοποιητικού (και του δημοσίου κλειδιού που αυτό περιέχει…)
  - Δεν υπαγορεύεται συγκεκριμένος αλγόριθμος κρυπτογράφησης, αλλά προτείνεται ο RSA
- Πιστοποιητικά Γνωρισμάτων (Attribute Certificates)
  - Γενίκευση των ΠΔΚ
  - Πιστοποιούν περισσότερα γνωρίσματα για κάποια οντότητα πέρα από το δημόσιο κλειδί

Χρήση πιστοποιητικού δημοσίου κλειδιού

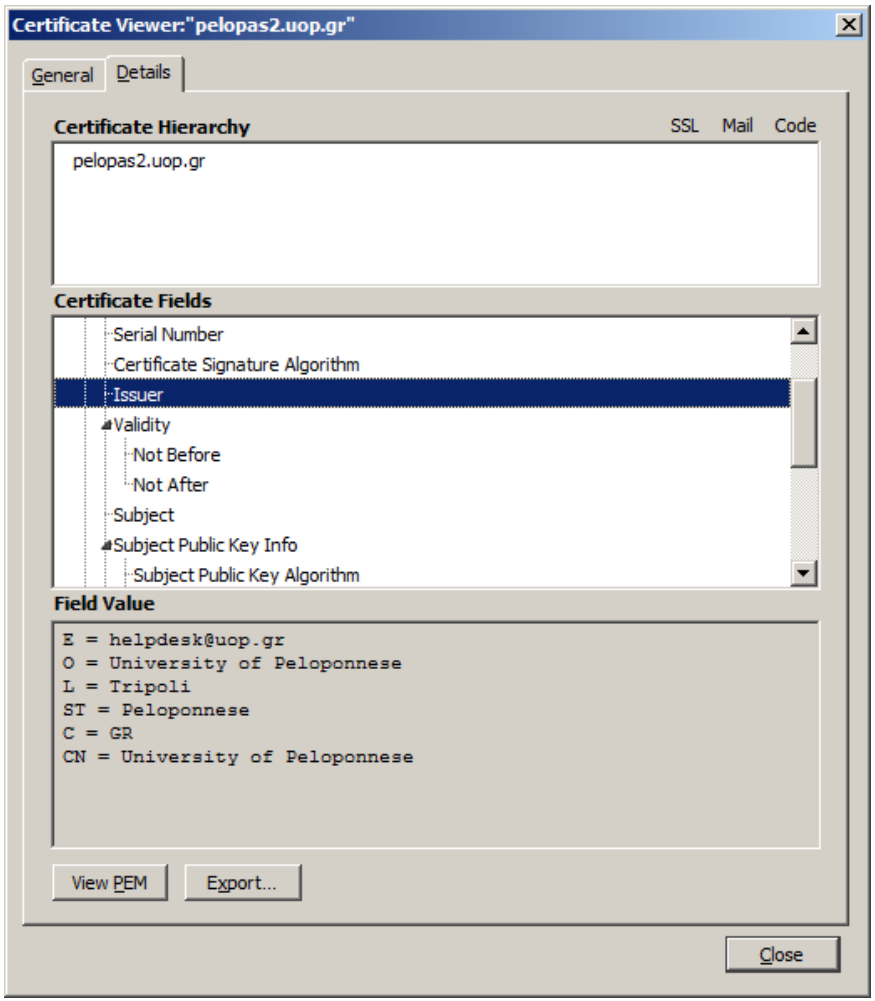


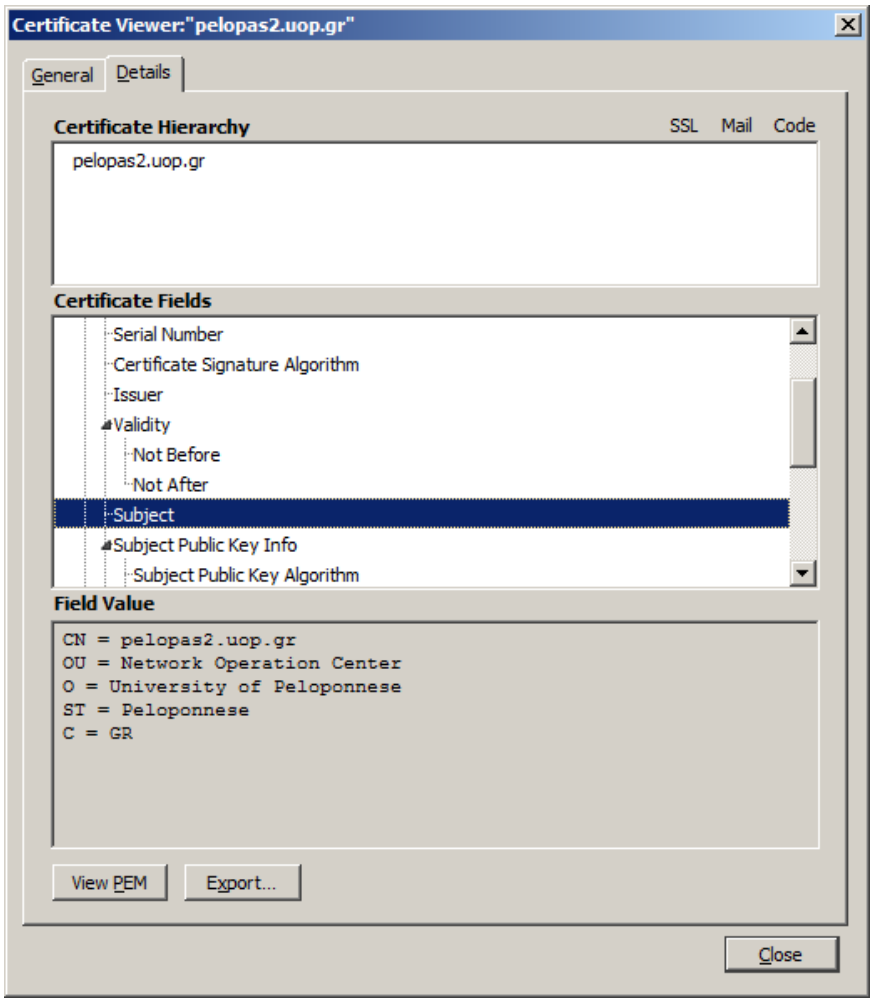
Μορφή πιστοποιητικών X.509

- Πεδία:
  - Έκδοση
  - Σειριακός αριθμός
  - Αλγόριθμός υπογραφής (+ παράμετροι)
  - Εκδότης πιστοποιητικού
  - Περίοδος ισχύος
  - Υποκείμενο πιστοποιητικού
  - Πληροφορίες για το δημόσιο κλειδί του υποκειμένου
  - Μοναδικός προσδιοριστής εκδότη
  - Μοναδικός προσδιοριστής υποκειμένου
  - Επεκτάσεις
  - Υπογραφή



Παράδειγμα πιστοποιητικού X.509





Παράδειγμα πιστοποιητικού X.509

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d0:ff:23:a9:ef:bc:56:cb
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=GR, ST=Attica, L=Athens, O=NTUA, OU=ICBNET, CN=peace.icbnet.ece.ntua.gr
        Validity
            Not Before: Jun 15 07:00:17 2007 GMT
            Not After : Jun 12 07:00:17 2017 GMT
        Subject: C=GR, ST=Attica, L=Athens, O=NTUA, OU=ICBNET, CN=peace.icbnet.ece.ntua.gr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:9b:d9:5d:51:1a:2a:4b:e5:b0:4e:09:16:e7:11:
                    c2:e3:75:61:8f:66:c5:53:92:96:20:96:cf:b3:25:
                    37:ae:cc:88:5e:74:c0:11:50:38:b0:26:f2:f6:68:
                    79:36:e0:a1:95:95:33:6f:e0:6a:ae:57:cf:e4:5c:
                    9d:0f:42:03:47:62:ad:cd:55:60:3d:83:fc:33:2f:
                    e1:4e:7f:fc:cb:0d:d4:21:77:d1:44:f5:bc:3d:44:
                    1e:b2:49:58:f0:10:87:23:dd:f9:c9:65:ea:0a:dd:
                    48:b2:f3:8f:97:6d:cd:0c:30:41:7d:7b:c7:88:75:
                    4b:9d:a1:00:41:95:d4:f4:b7
```

Παράδειγμα πιστοποιητικού X.509

```
X509v3 extensions:
        X509v3 Subject Key Identifier:
            E8:50:82:5A:F1:C7:4F:84:CD:5D:8E:22:59:57:87:AD:D6:42:BB:4E
        X509v3 Authority Key Identifier:
            keyid:E8:50:82:5A:F1:C7:4F:84:CD:5D:8E:22:59:57:87:AD:D6:42:BB:4E
            DirName:/C=GR/ST=Attica/L=Athens/O=NTUA/OU=ICBNET/CN=peace.icbnet.ece.ntua.gr
            serial:D0:FF:23:A9:EF:BC:56:CB
        X509v3 Basic Constraints:
            CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
          94:40:27:c1:14:18:db:28:25:c0:27:55:d6:33:d5:5b:9e:26:
          51:c2:3b:9b:01:7c:f2:8f:f5:fb:36:5e:a2:0c:fd:e1:22:63:
          4f:5b:d3:85:9f:99:ab:08:67:7d:69:bf:d4:c7:b3:f5:fc:2f:
          fd:2d:b0:c1:1e:37:2c:2e:84:e9:39:9f:54:e5:18:fb:bd:c8:
          db:7a:97:87:17:db:ec:49:a6:41:9c:4f:9e:fc:60:8c:9b:57:
          e2:7e:3c:d7:09:1e:04:85:28:60:a2:5f:44:fe:5a:7f:50:d8:
          2d:e7:5a:58:db:29:62:d0:ba:b6:99:62:a9:1a:bd:7e:48:e2:
          38:74
```

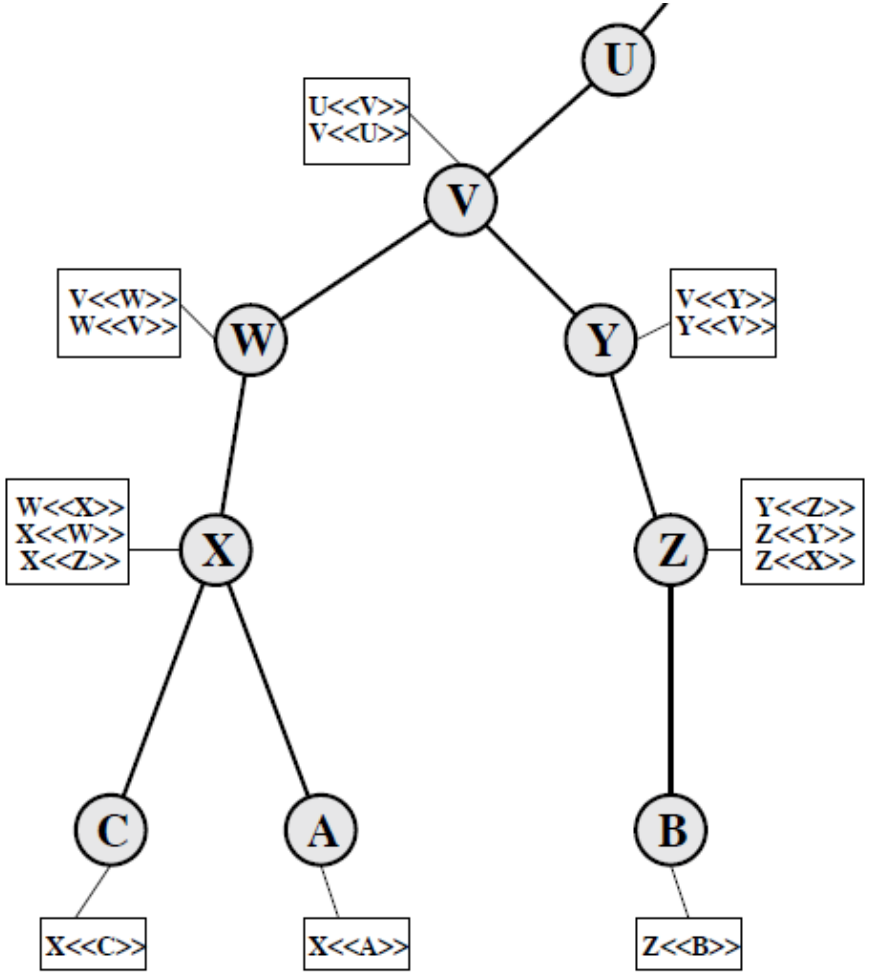
Γενικός ορισμός X.509 πιστοποιητικού

- CA <<A>> = CA {V, SN, AI, CA, T_A, A, Ap}
  όπου:
  - CA <<A>>: πιστοποιητικό για την οντότητα A, που έχει εκδοθεί από την Αρχή Πιστοποίησης CA
  - V: Έκδοση
  - SN: Σειριακός αριθμός
  - AI: Αναγνωριστικό αλγορίθμου
  - CA: Πληροφορίες για την Αρχή Πιστοποίησης
  - T_A: Χρόνος εγκυρότητας
  - A: Πληροφορίες για την υποκείμενη οντότητα
  - Ap: Δημόσιο κλειδί οντότητας A

Πιστοποίηση X.509

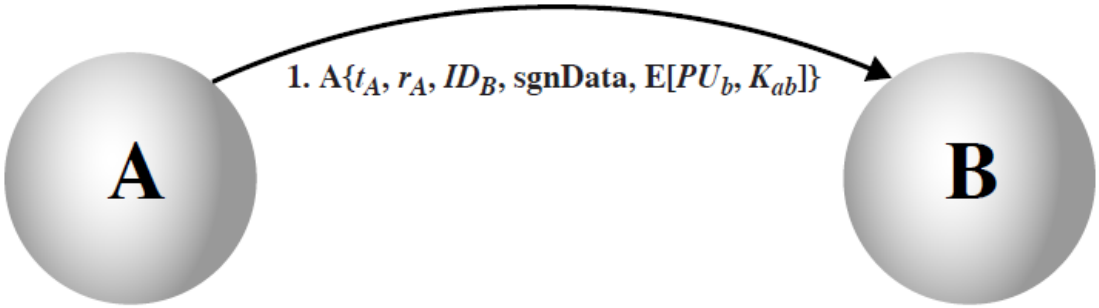
- Οποιαδήποτε οντότητα έχει πρόσβαση στο δημόσιο κλειδί της CA, μπορεί να επαληθεύσει το δημόσιο κλειδί της οντότητας που πιστοποιήθηκε
- Εφόσον δύο οντότητες A και B πιστοποιούνται από την ίδια Αρχή Πιστοποίησης, η επαλήθευση είναι εύκολη: και οι δύο οντότητες εμπιστεύονται την ίδια Αρχή και γνωρίζουν το δημόσιο κλειδί της
- Εφόσον δύο οντότητες A και B πιστοποιούνται από διαφορετικές Αρχές, CA_A και CA_B:
  - Χρησιμοποιείται "αλυσίδα πιστοποίησης" προκειμένου η οντότητα A (ή B) να επαληθεύσει το δημόσιο κλειδί της B (ή A), δηλαδή:
  - → CA_A <<CA_B>> CA_B <<B>>
  - → CA_B <<CA_A>> CA_A <<A>>
- Αναλόγως, η αλυσίδα μπορεί να περιλαμβάνει αυθαίρετα μεγάλο αριθμό από Αρχές Πιστοποίησης, δηλαδή:
  - CA_1 <<CA_2>> CA_2 <<CA_3>> CA_3 <<CA_4>> … Ca_{v-1} <<CA_v>> CA_v <<N>>
- Δυνατότητα ιεραρχικής οργάνωσης!

Ιεραρχία X.509



Αυθεντικοποίηση X.509

Ενός σταδίου

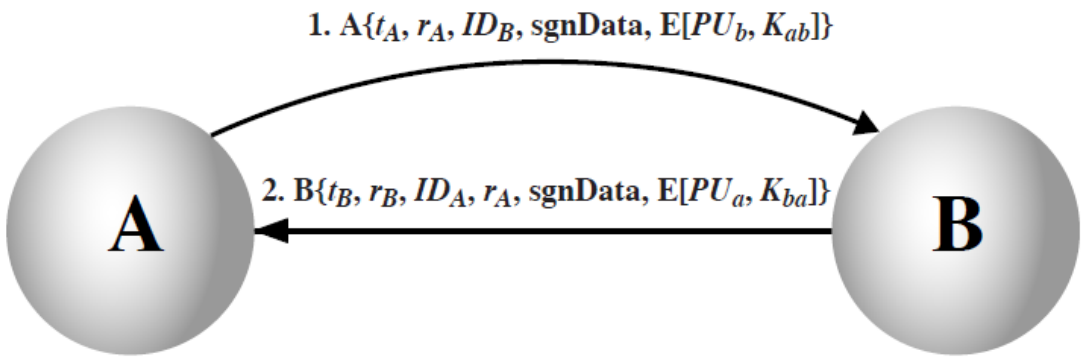


- Πιστοποιούνται:
  - Η ταυτότητα του A
  - Η δημιουργία του μηνύματος από τον A
  - Ότι το μήνυμα προορίζεται για το B
  - Η ακεραιότητα του μηνύματος
- Μήνυμα υπογεγραμμένο με το ιδιωτικό κλειδί του A

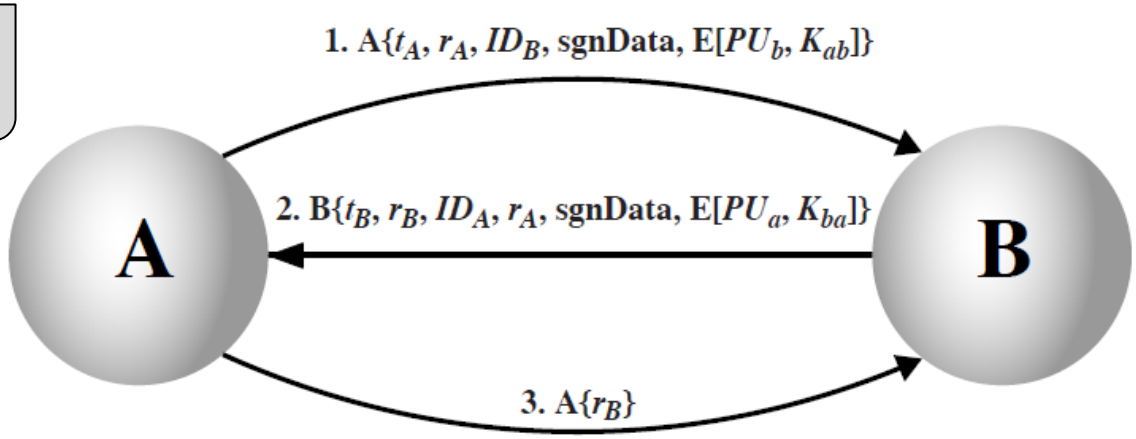
- Το μήνυμα περιλαμβάνει:
  - t_A: χρονοσφραγίδα
  - r_A: προσδιοριστικό χρήσης
  - ID_B: ταυτότητα B
  - sgnData: δεδομένα
  - E[PU_b, K_{ab}]: κλειδί εργασίας κρυπτογραφημένο με το δημόσιο κλειδί του B

Αυθεντικοποίηση X.509

Δύο σταδίων

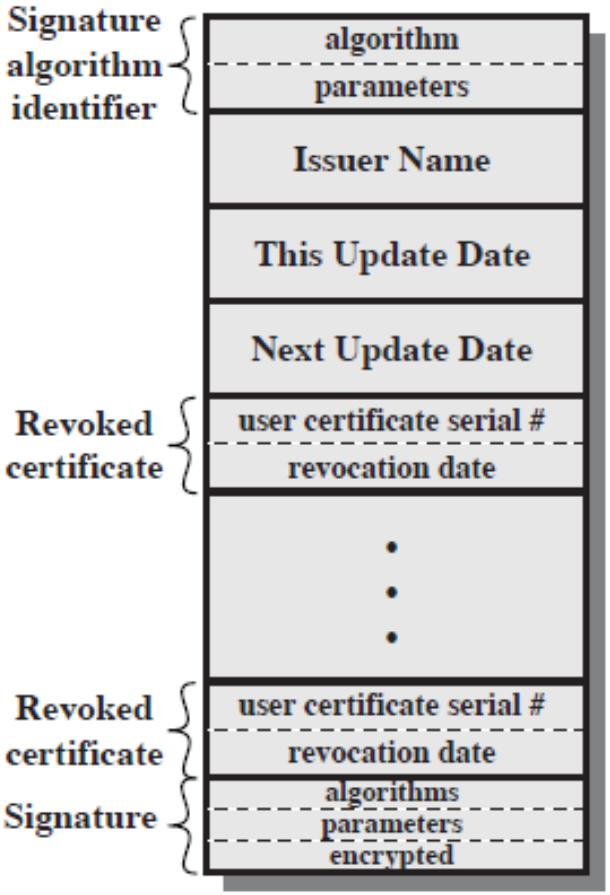


Τριών σταδίων



Ανάκληση πιστοποιητικών

- Γιατί?
  - Υπάρχει υποψία "διαρροής" κάποιου ιδιωτικού κλειδιού
  - Η Αρχή Πιστοποίησης παύει να πιστοποιεί την έως τώρα πιστοποιούμενη οντότητα
  - Υπάρχει υποψία "έκθεσης" του πιστοποιητικού της Αρχής
- Πώς?
  - Λίστα Ανάκλησης Πιστοποιητικών (Certificate Revocation List – CRL)
  - "Μαύρη λίστα" πιστοποιητικών
  - Διάφοροι τρόποι υλοποίησης



Παράδειγμα Πιστοποιητικού Γνωρισμάτων

```
Serial Number: 1274464610307
Signature: SHA256WithRSAEncryption
Issuer: C=PPC
    Holder: C=PPC,1266856347057
Validity:
Not Before: Fri May 21 20:56:50 EEST 2010
Not After: Sat May 21 20:56:50 EEST 2011
Number of Attributes: 11
Attributes: 0:1: NetworkSectionAdministrator
Attributes: 1:1: Monday,Tuesday,Wednesday,Thursday,Friday
Attributes: 2:1: 00:00-07:59,00:00-07:59,00:00-07:59,00:00-07:59,00:00-07:59
Attributes: 3:1: Roger Rabbit
Attributes: 4:1: roger@nettare.it
Attributes: 5:1: Italy
Attributes: 6:1: Pisa
Attributes: 7:1: 12345
Attributes: 8:1: via Giuntini, 63 interno A5 - 56023 - Navacchio
Attributes: 9:1: 34785697
Attributes: 10:1: 10.11.12.1
```

Υποδομή Δημοσίου Κλειδιού

Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI):

το σύνολο υλικού, λογισμικού, ανθρώπων, πολιτικών και διαδικασιών που απαιτούνται για τη δημιουργία, διαχείριση, αποθήκευση, διανομή και ανάκληση ψηφιακών πιστοποιητικών που βασίζονται σε κρυπτογραφία δημοσίου κλειδιού