# Cryptography and Network Security Chapter 14

Fifth Edition

by William Stallings

# Chapter 14 – Key Management and Distribution

*No Singhalese, whether man or woman, would venture out of the house without a bunch of keys in his hand, for without such a talisman he would fear that some devil might take advantage of his weak state to slip into his body.*

***—The Golden Bough, Sir James George Frazer***

# Διαχειριση και διανομη κλειδιου (Key Management and Distribution)

- Τα συμμετρικα συστηματα κρυπτογραφησης απαιτουν και τα δυο μέρη να μοιραζονται ένα κοινο κλειδι.

- Τα σχηματα δημοσιου κλειδιου απαιτουν και τα δυο μερη να αποκτησουν δημοσια κλειδια

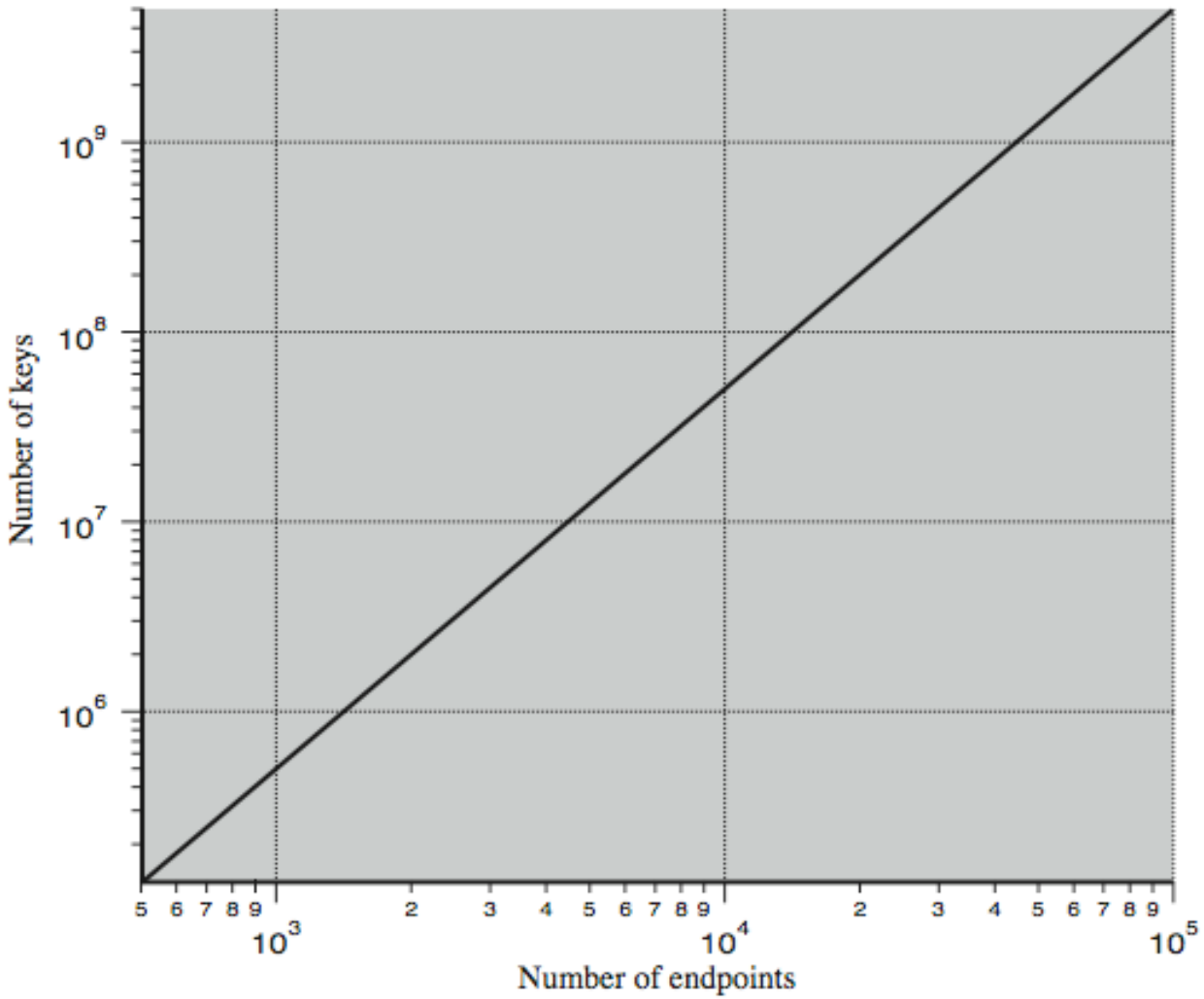
# Διανομη Κλειδιου (Key Distribution)

- Τα συμμετρικα σχηματα απαιτουν και τα δυο μερη να μοιραζονται ένα κοινο μυστικο κλειδι
- Το θεμα είναι πως θα διανεμηθει με ασφαλεια το κλειδι αυτό
- Ενώ θα πρεπει το κλειδι αυτό να προστατευτει απο τριτους που πιθανο να θελουν να το υποκλεψουν
- Συχνες αλλαγες κλειδιου είναι επιθυμητες
- Συχνα η αποτυχια του συστηματος ασφαλειας οφειλεται σε σπασιμο του συστηματος διανομης κλειδιου

# Διανομη Κλειδιου

- Τα μερη Α και Β εχουν τις εξης επιλογες για τη διανομη κλειδιου:
  1. Ο Α μπορει να επιλεξει το κλειδι και να το παραδωσει φυσικα (π.χ. σε ένα φλασακι) στον Β.
  2. Μια τριτη οντοτητα να επιλεξει και να διανειμει το κλειδι από τον Α στον Β.
  3. Αν οι  Α και Β εχουν επικοινωνησει προηγουμενως, μπορουν να χρησιμοποιησουν το προηγουμενο κλειδι για να κρυπτογραφησουν ενα νέο κλειδι.
  4. Αν οι Α και Β εχουν ασφαλεις επικοινωνιες με ένα τριτο μερος C, ο C μπορει να αναμεταδωσει το κλειδι αναμεσα στον Α και στον Β

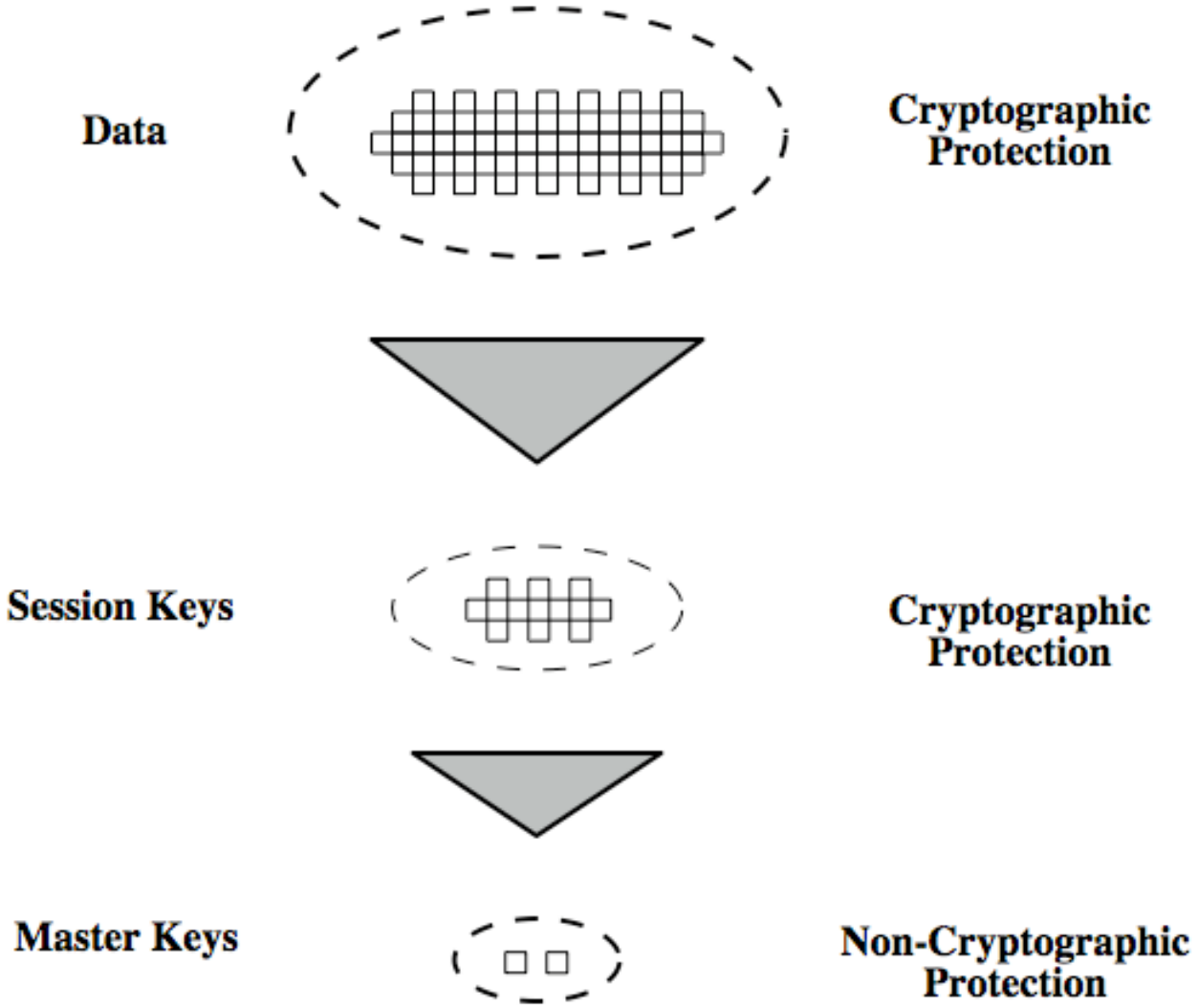
# Key Distribution Task



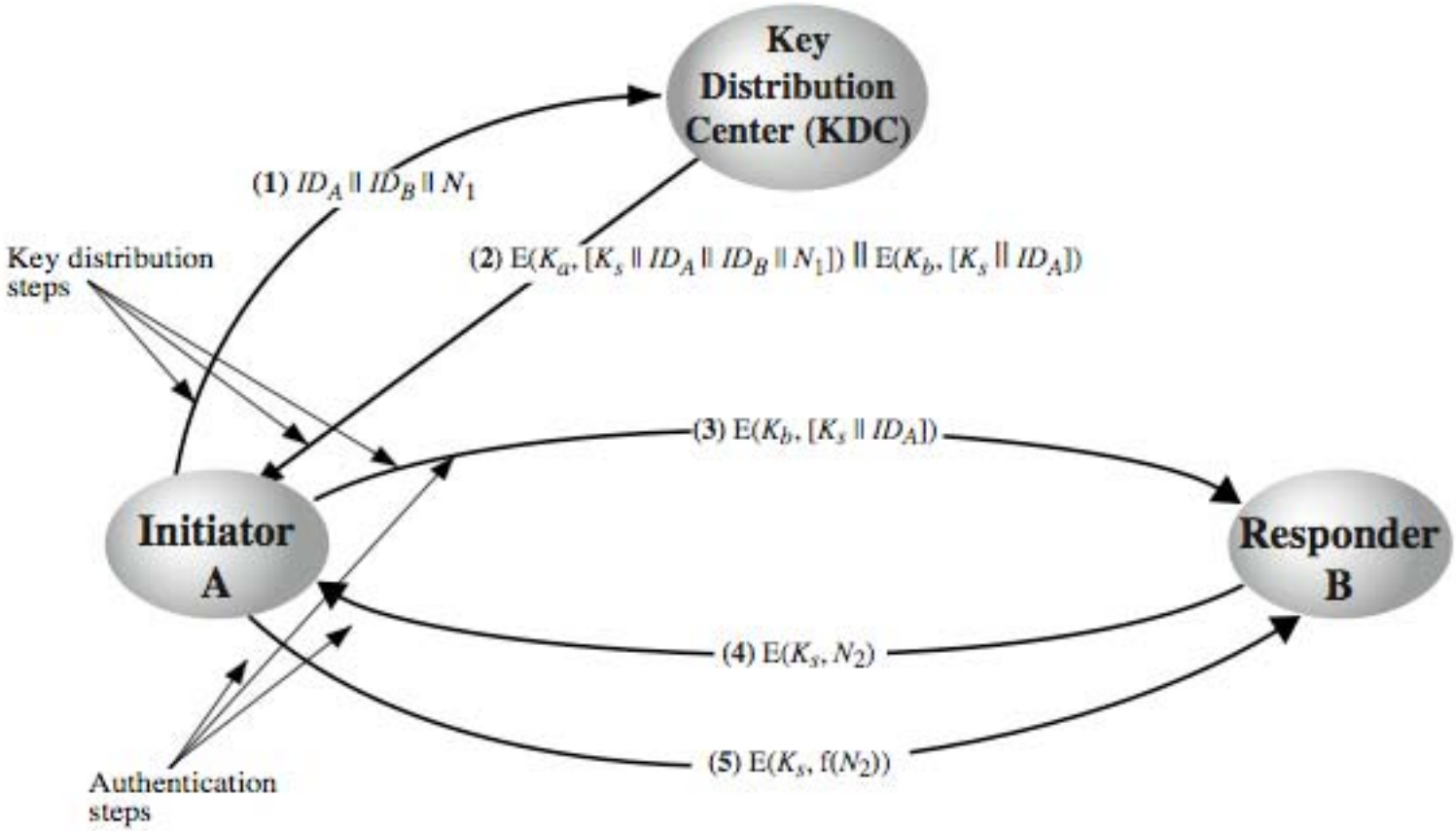
# Ιεραρχια Κλειδιων

- Τυπικα εχουμε μια ιεραρχια κλειδιων
- Κλειδι συνοδου (session key)
  - Είναι προσωρινο
  - Χρησιμοποιειται για κρυπτογραφηση των δεδομενων που μεταδιδονται μεταξυ των χρηστων
  - Χρησιμοποιειται μονο για μια λογικη συνοδο (session) και στη συνεχεια καταργειται
- Γενικο Κλειδι (master key)
  - Χρησιμοποιειται για να κρυπτογραφει τα κλειδια συνοδου
  - Το μοιραζεται ο χρηστης και το κεντρο διανομης κλειδιου (key distribution center)

# Ιεραρχια Κλειδιων



# Σεναριο Διανομης Κλειδιου με χρήση Κεντρου Διανομης Κλειδιου (KDC)



# Θεματα διανομης Κλειδιου

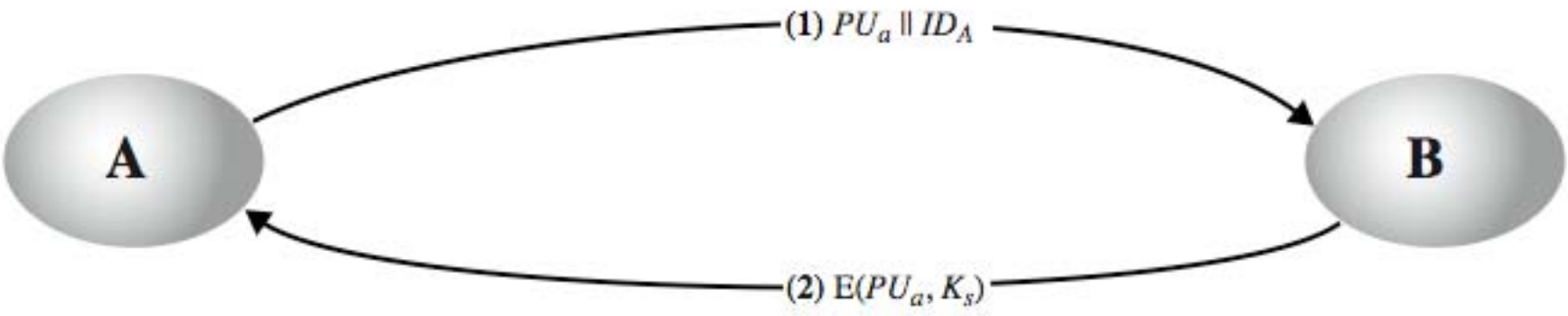
- Για μεγαλυτερα δικτυα απαιτουνται Ιεραρχιες απο ΚΔΔ (KDC), αλλα πρεπει να εμπιστευονται το ένα το άλλο.
- Ο χρονος ζωης των Κλειδιων συνοδου πρεπει να είναι περιορισμενος για μεγαλυτερη ασφαλεια
- Μπορει το συστημα  να κανει αυτοματη διανομη κλειδιου για λογαριασμο των χρηστων, αλλα θα πρεπει οι χρηστες να εμπιστευονται το συστημα
- Μπορει επισης να γινει αποκεντροποιημενη διανομη κλειδιου

# Διανομη Συμμετρικου Κλειδιου με χρηση Δημοσιου Κλειδιου

- Τα συστηματα δημοσιου κλειδιου δεν είναι αποδοτικα
  - Γι'αυτό σχεδον ποτε δεν χρησιμοποιουνται αμεσα για κρυπτογαφηση των δεδομενων
  - Συνηθως χρησιμοποιουνται για να κρυπτογραφουν τα κλειδια συμμετρικων αλγοριθμων κατά τη διανομη κλειδιου.

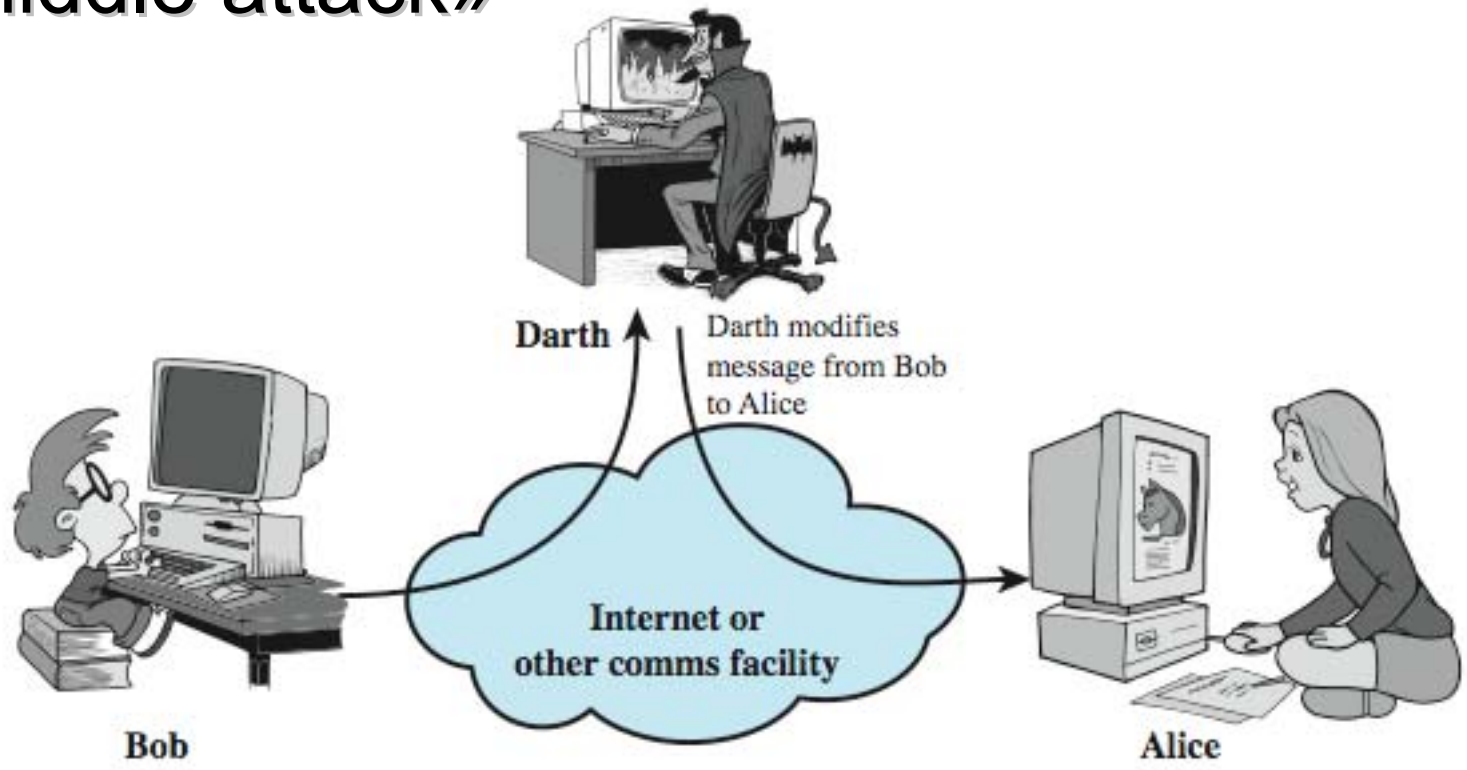
# Απλη διανομη Μυστικου Κλειδιου (Simple Secret Key Distribution)

- Ο Merkle προτεινε αυτό το πολύ απλο σχημα
  - Επιτρεπει ασφαλεις επικοινωνιες
  - Δεν προυποθετει την υπαρξη κλειδιων από πριν

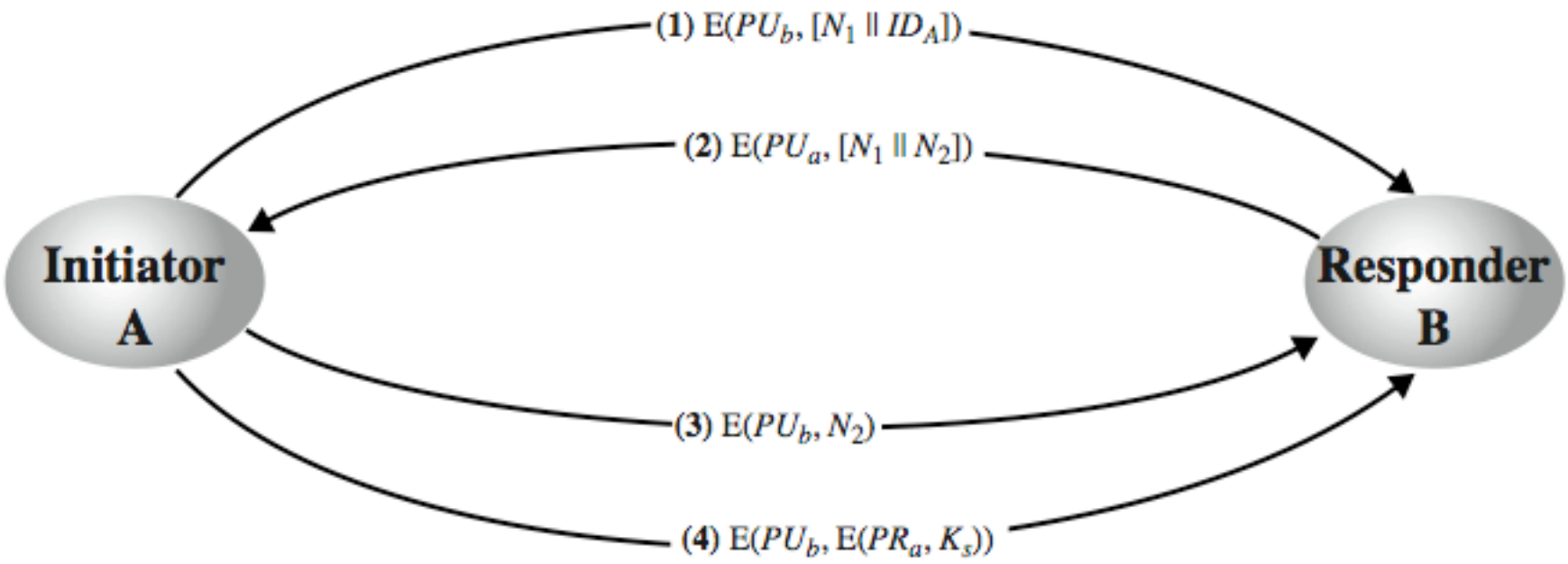


# Man-in-the-Middle Attack

- Αυτό το πολύ απλο σχημα ειναι ευαλωτο στην ενεργητικη επιθεση «man-in-the-middle attack»



# Διανομη Μυστικου Κλειδιου με Εμπιστευτικοτητα και Πιστοποιηση Αυθεντικοτητας



# Υβριδικη Διανομη Κλειδιου (Hybrid Key Distribution)

- Χρησιμοποιουν ενα KDC ιδιωτικου κλειδιου
- Το KDC μοιραζεται ένα μυστικο Γενικο Κλειδι (master key) με κάθε χρηστη
- Διανεμει το κλειδι συνοδου χρησιμοποιωντας το Γενικο Κλειδι
- Χρησιμοποιειται **κρυπτογραφια δημοσιου κλειδιου** για τη **διανομη** των **Γενικων Κλειδιων**
  - Είναι ιδιαιτερα χρησιμο για ευρεως κατανεμημενους χρηστες που δεν μπορουν να μοιραστουν με φυσικο τροπο ένα συμμετρικο κλειδι με το KDC
- Λογικη
  - αποδοση
  - προς τα πισω συμβατοτητα

# Διανομη Δημοσιων Κλειδιων (Distribution of Public Keys)

- Μπορει να υποτεθει η χρηση ενός από τα παρακατω:
  - Δημοσια ανακοινωση (public announcement)
  - Δημοσια διαθεσιμος καταλογος (publicly available directory)
  - Αρχη δημοσιου κλειδιου (public-key authority)
  - Πιστοποιητικα Δημοσιου Κλειδιου (public-key certificates)

# Δημοσια Ανακοινωση (Public Announcement)

- Οι χρηστες διανεμουν τα δημοσια κλειδια στους αποδεκτες ή τα εκπεμπουν
  - προσθετουν τα κλειδια PGP σε μηνυματα email ή τα στελνουν σε news groups ή σε email lists
- Κυριο μειονεκτημα η πλαστογραφια
  - Ο καθενας μπορει να δημιουργησει ένα κλειδι, να το εκπεμψει και να ισχυριστει οτι είναι καποιος άλλος
  - Μεχρι να ανακαλυφθει η πλαστογραφια μπορει να προσποιειται ότι είναι καποιος αλλος

# Δημοσια Διαθεσιμος Καταλογος (Publicly Available Directory)

- Μπορουμε να εχουμε μεγαλυτερη ασφαλεια εγγραφοντας τα κλειδια σε έναν καταλογο
- Ο καταλογος μπορει να είναι αξιοπιστος εφοσον πληρει τις εξης ιδιοτητες:
  - Περιέχει εγγραφες της μορφης {ονομα, δημοσιο κλειδι}
  - Οι συμμετεχοντες γραφουν με ασφαλεια στον καταλογο
  - Οι συμμετεχοντες μπορουν να αντικαταστησουν το κλειδι τους οποιαδηποτε στιγμη
  - Ο καταλογος δημοσιευεται περιοδικα
  - Ο καταλογος μπορει να προσπελαστει ηλεκτρονικα
- Ο κινδυνος της πλαστογραφιας παραμενει

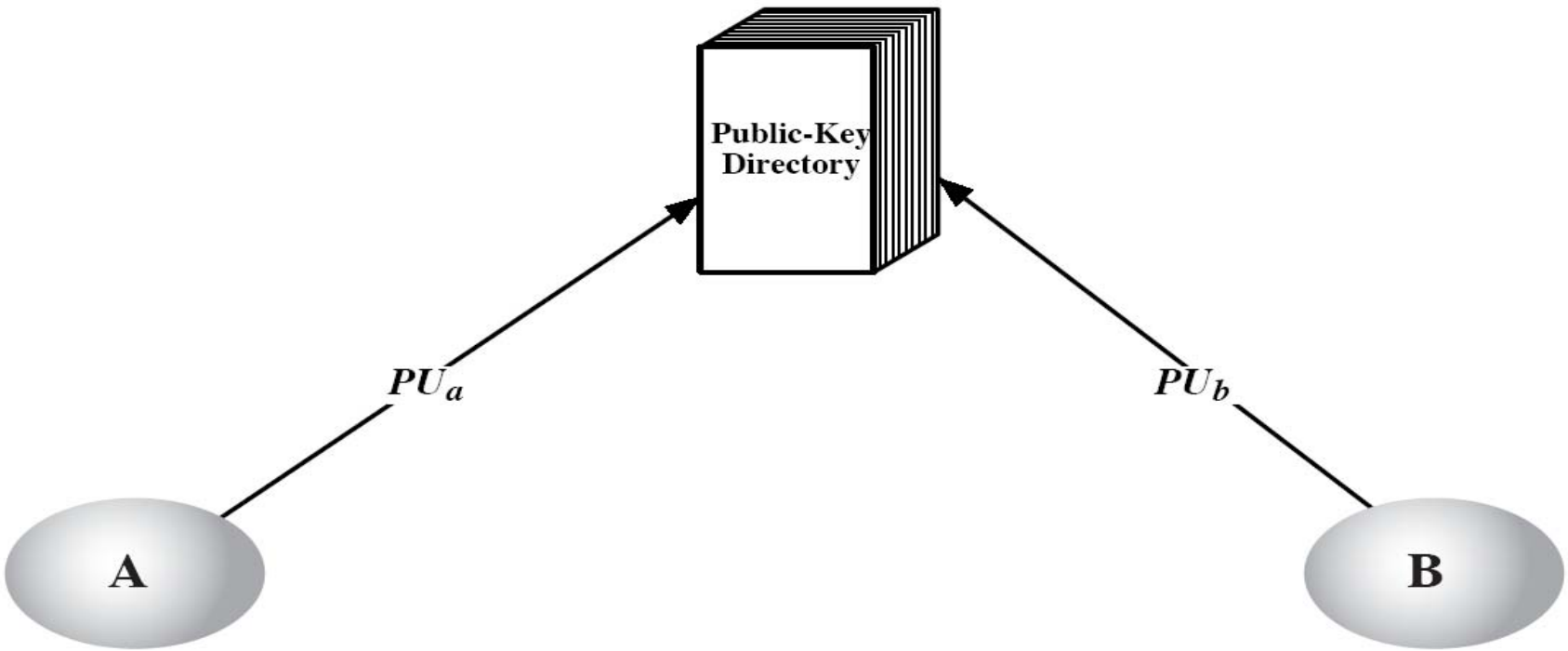
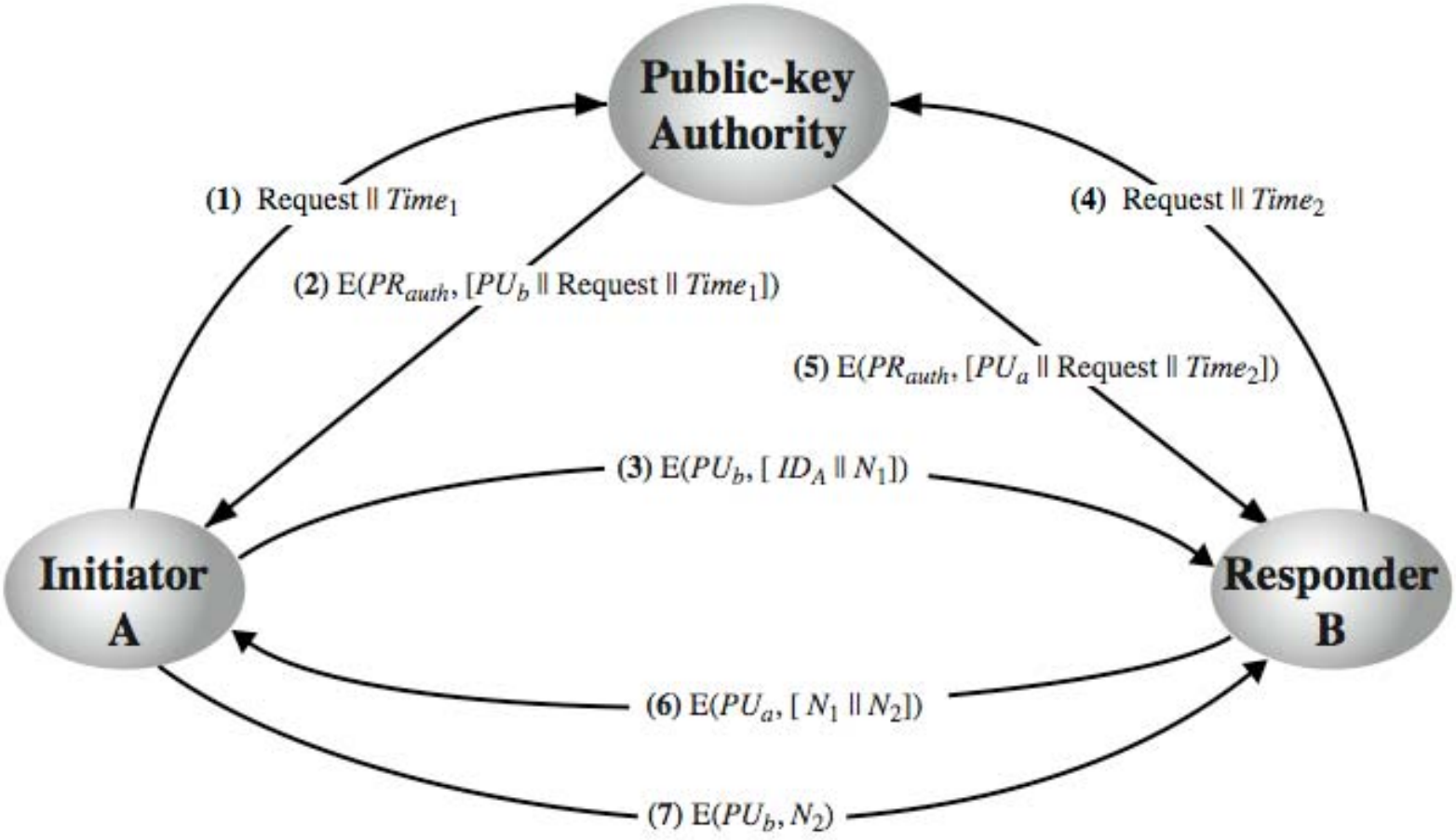



**Figure 14.10 Public Key Publication**

# Αρχη Δημοσιου Κλειδιου

- Βελτιωνει την ασφαλεια κανοντας πιο αυστηρο τον ελεγχο στη διανομη των δημοσιων κλειδιων
- Εχει ιδιοτητες του καταλογου
- Απαιτει από τους χρήστες να γνωριζουν το δημοσιο κλειδι του καταλογου
- Τοτε οι χρηστες επικοινωνουν με τον καταλογο και λαμβανουν γνωση οποιουδηποτε δημοσιου κλειδιου θελουν με ασφαλεια
  - Απαιτειται προσβαση σε **πραγματικο χρονο** στον καταλογο όταν χρειαζονται τα κλειδια

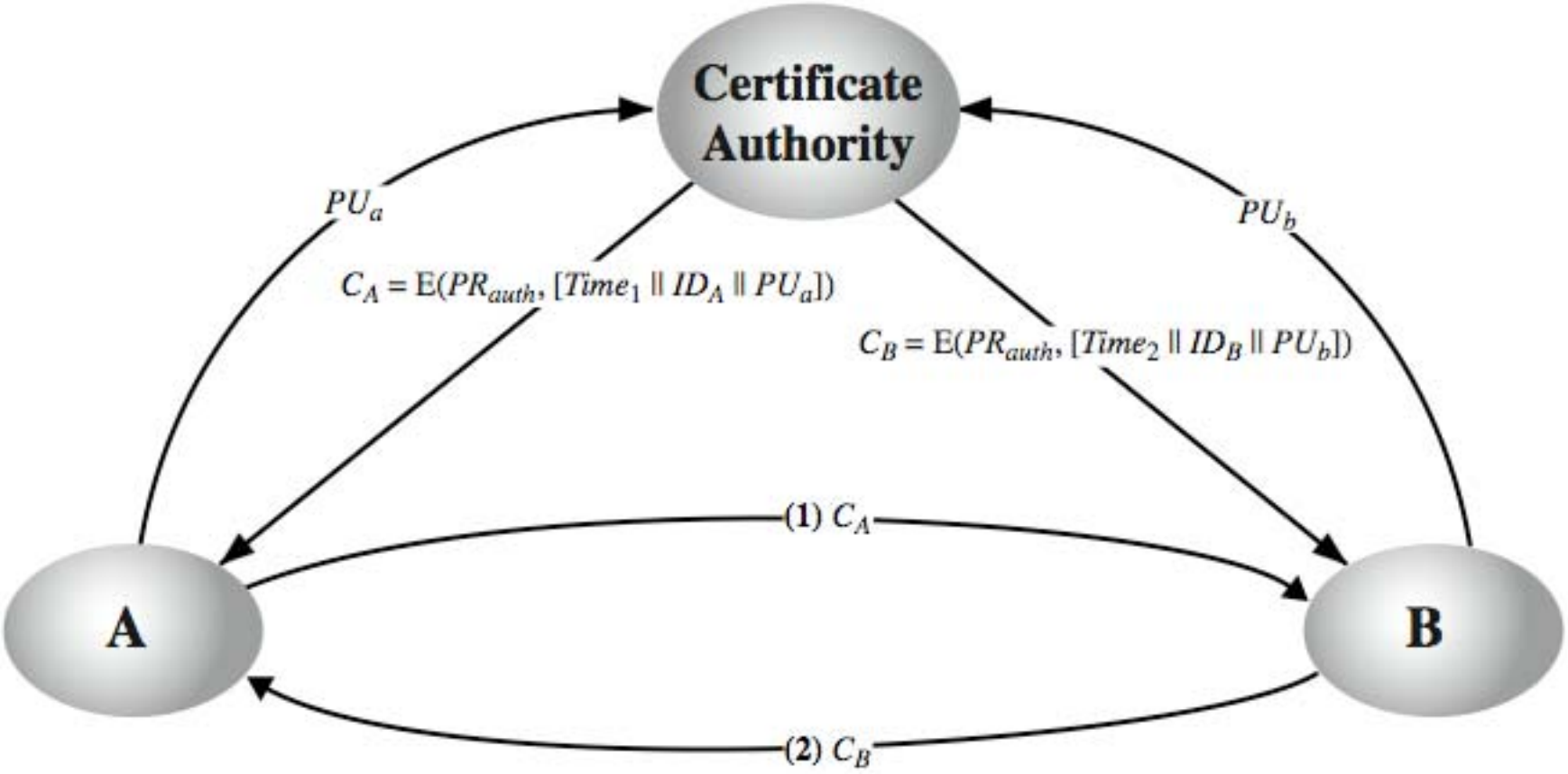
# Αρχη Δημοσιου Κλειδιου



# Πιστοποιητικα Δημοσιου Κλειδιου (Public-Key Certificates)

- Τα πιστοποιητικα επιτρεπουν την ανταλλαγη κλειδιου **χωρις real-time προσβαση στην Αρχή Δημοσιου Κλειδιου**
- Ένα πιστοποιητικο συνδεει την οντοτητα με το δημοσιο κλειδι
  - Συνηθως το δημοσιο κλειδι συνοδευεται και από άλλη πληροφορια όπως η περιοδος εγκυροτητας, τα δικαιωματα χρησης, κλπ.
- Ολο το περιεχομενο υπογραφεται από την εμπιστη αρχη Δημοσιου Κλειδιου ή Αρχη Πιστοποίητικών ή Αρχη Πιστοποιησης, (Certification Authority, CA)
- Το πιστοποιητικο μπορει να επιβεβαιωθει από οποιονδήποτε γνωριζει το δημοσιο κλειδι της CA

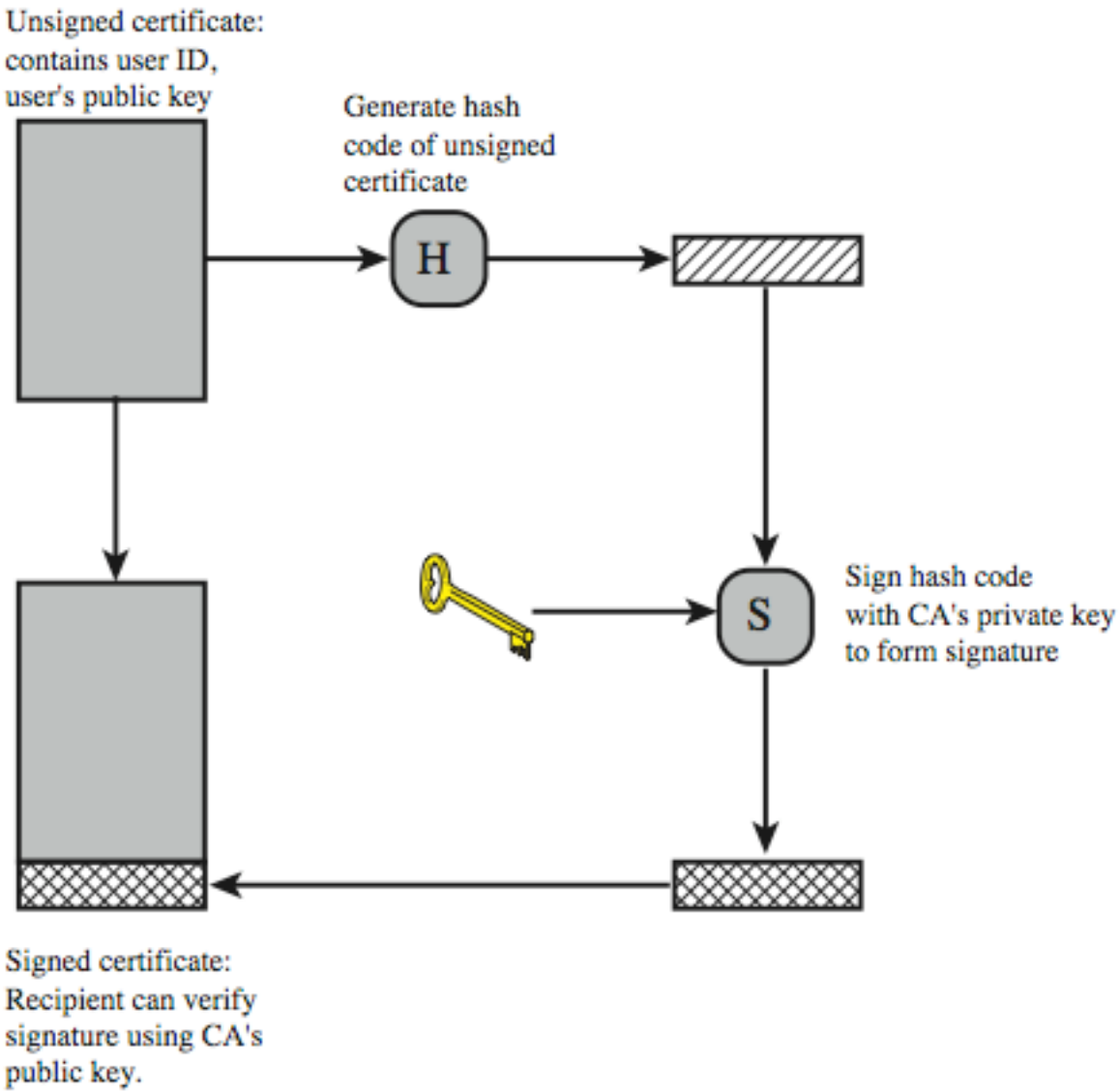
# Public-Key Certificates



# Υπηρεσια Πιστοποιησης Αυθεντικοτητας X.509 (X.509 Authentication Service)

- Είναι μερος του προτυπου υπηρεσίας καταλογου (directory service) CCITT X.500
  - Κατανεμημενοι servers διατηρουν μια βαση δεδομενων πληφορορίες χρήστη
- Ορίζει το πλαισιο για υπηρεσιες πιστοποίησης αυθεντικότητας
  - Ο καταλογος μπορει να αποθηκευει πιστοποιητικα δημοσιου κλειδιου
  - Με το δημοσιο κλειδι του χρήστη υπογεγραμμένο από την αρχη πιστοποιησης (CA)
- Επίσης, ορίζει πρωτόκολλα πιστοποίησης αυθεντικότητας (authentication protocols).
- Χρησιμοποιεί κρυπτογραφια δημοσιου κλειδιου και ψηφιακες υπογραφες
  - στο προτυπο δεν περιλαμβανεται ο κρυπτογραφικος αλγοριθμος, αλλα συνιστάται η χρήση του RSA
- Τα πιστοποιητικα X.509 χρησιμοποιούνται ευρύτατα
  - Υπαρχουν τρεις versions

# X.509 Certificate Use

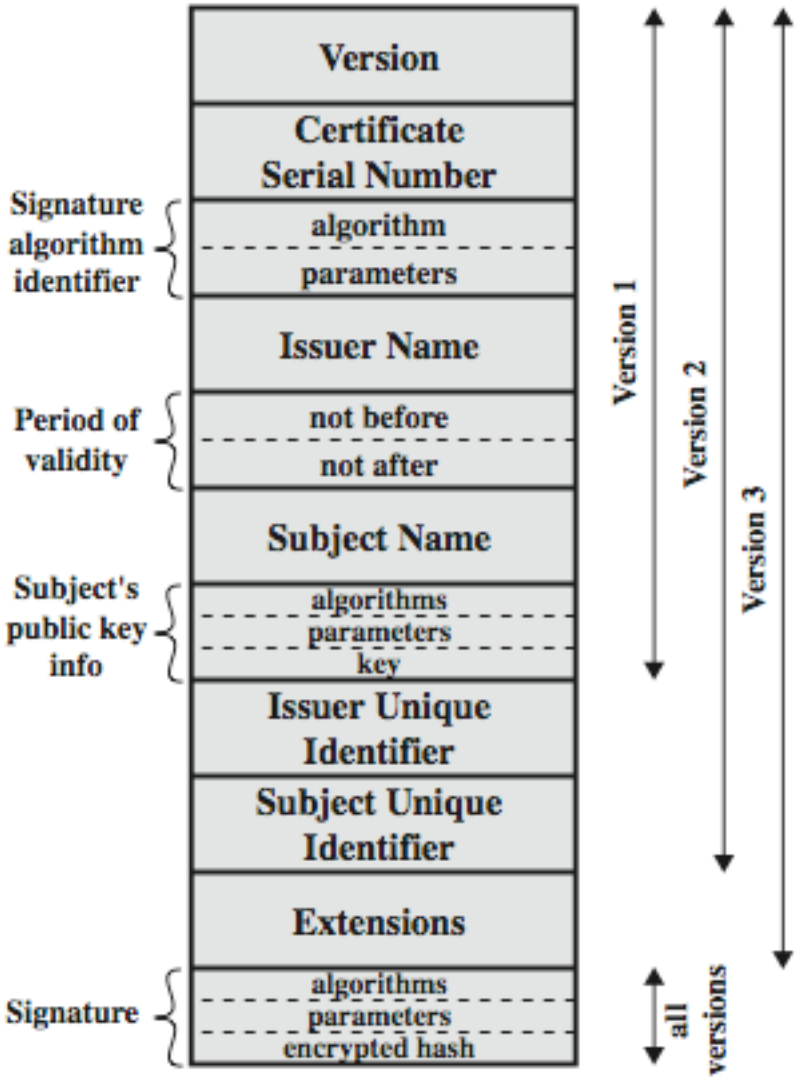


# Πιστοποιητικα X.509 (X.509 Certificates)

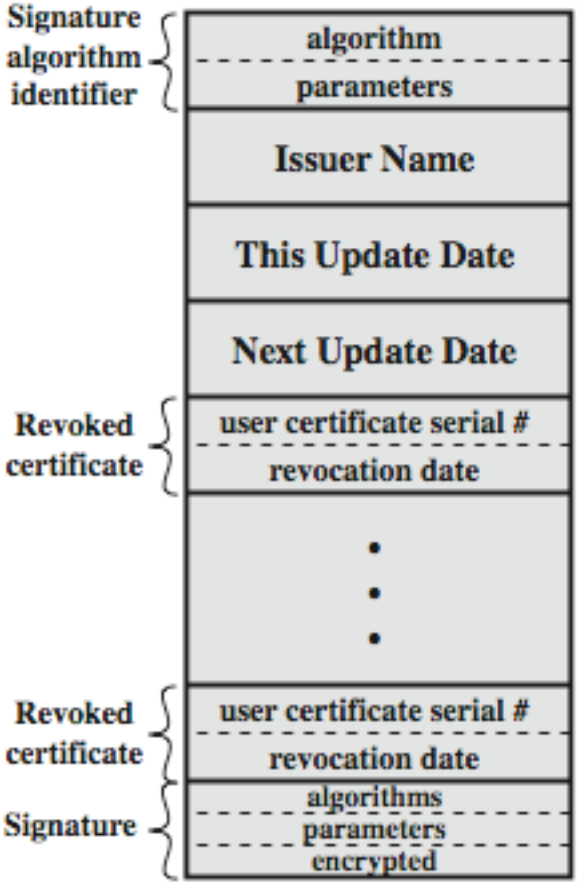
- Εκδίδονται από μια Αρχή Πιστοποίησης (CA), και περιέχουν:
  - version V (1, 2, or 3)
  - serial number SN (unique within CA) identifying certificate
  - signature algorithm identifier AI
  - issuer X.500 name CA)
  - period of validity TA (from - to dates)
  - subject X.500 name A (name of owner)
  - subject public-key info Ap (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)

- Ο συμβολισμός: CA<<A>> συμβολίζει πιστοποιητικο για τον Α υπογεγραμμενο από την Αρχη Πιστοποιησης CA

# X.509 Certificates




(a) X.509 Certificate




(b) Certificate Revocation List

# Απόκτηση Πιστοποιητικου

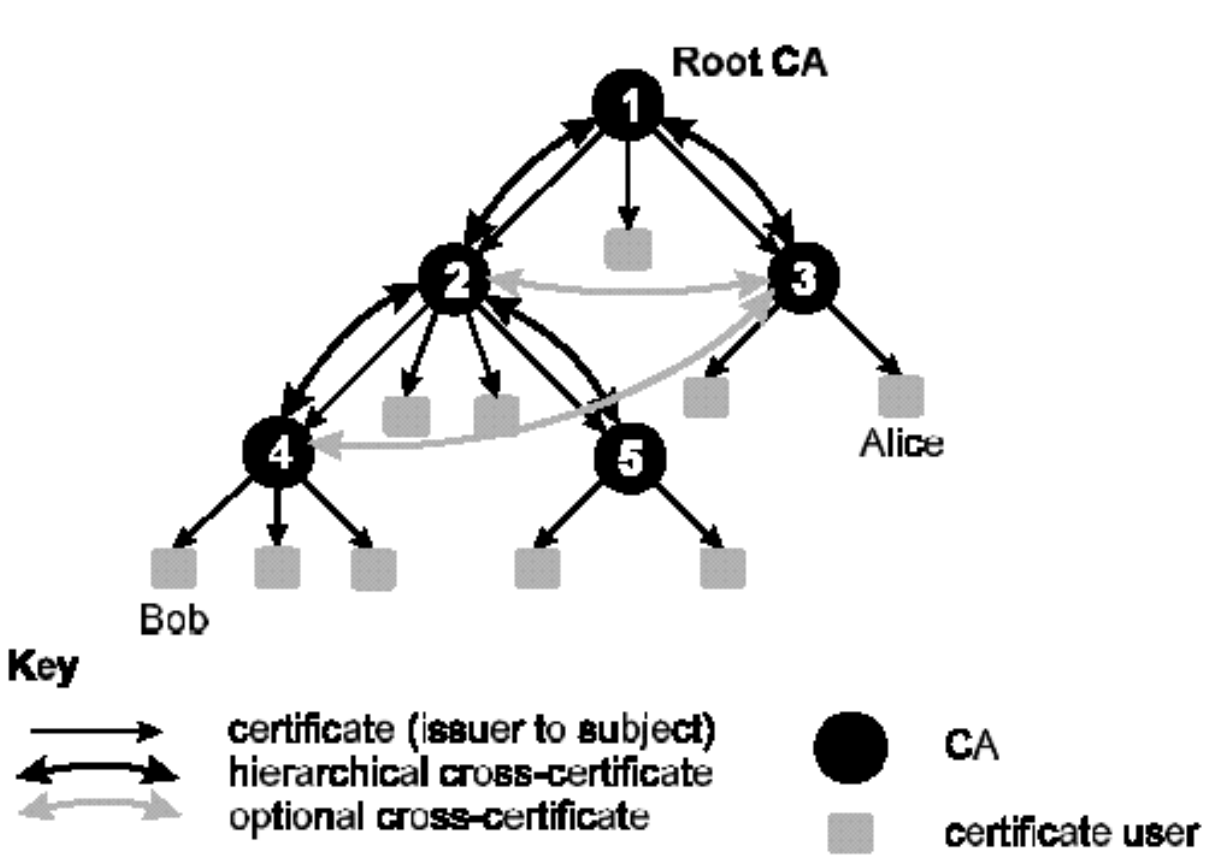
- Κάθε χρηστης με προσβαση στην Αρχη Πιστοποιησης (CA) μπορει να παρει πιστοποιητικο από αυτην
- Μονο η CA μπορει να τροποποιησει ένα πιστοποιητικο
- Επειδη δεν μπορει να πλαστογραφηθουν, τα πιστοποιητικα τοποθετουνται σε ένα δημοσιο καταλογο (public directory)

# Ιεραρχια Αρχων Πιστοποιησης (CA Hierarchy)

- Αν και οι δυο χρηστες εχουν μια κοινη Αρχη Πιστοποιησης (CA) τότε υποτιθεται ότι γνωριζουν το δημοσιο κλειδι της
- Αλλιως, οι CAs πρεπει να σχηματιζουν μια ιεραρχια
- Χρησιμοποιουνται τα πιστοποιητικα που δυνδεουν τα μελη της ιεραρχιας για να επικυρωσουμε (επιβεβαιωσουμε) τις άλλες CAs
  - Κάθε CA εχει πιστοποιητικα για clients (forward) και parent (reverse)
- Κάθε client εμπιστευεται της πιστοποιητικα των parents
- Επιτρεπεται η επιβεβαιωση οποιουδηποτε πιστοποιητικου από μια CA από χρηστες ολων των αλλων CAs στην ιεραρχια

# Η Ιεραρχια των CAs

Forward Certificates: Πιστοποιητικα της Χ που εχουν εκδοθει απο αλλες CA
Reverse Certificates:Πιστοποιητικα που εχει εκδοσει η Χ για αλλες CA



# Ανακληση Πιστοποιητικου (Certificate Revocation)

- Τα πιστοποιητικα εχουν μια περιοδο ισχυος (period of validity)
- Μπορει να χρειαστει να ανακληθουν πριν τη ληξη τους, π.χ.:
  1. Όταν γνωστοποιηθει το ιδιωτικο κλειδι του χρήστη
  2. Όταν ο χρηστης δεν υπαγεται πια σε αυτη τη CA
  3. Όταν γνωστοποιηθει το ιδιωτικο κλειδι της CA
- Η CAs διατηρουν μια λιστα των ανακληθεντων πιστοποιητικων (Certificate Revocation List, CRL)
- Οι χρηστες πρεπει να ελεγχουν τα πιστοποιητικα μηπως ανηκουν στη CRL

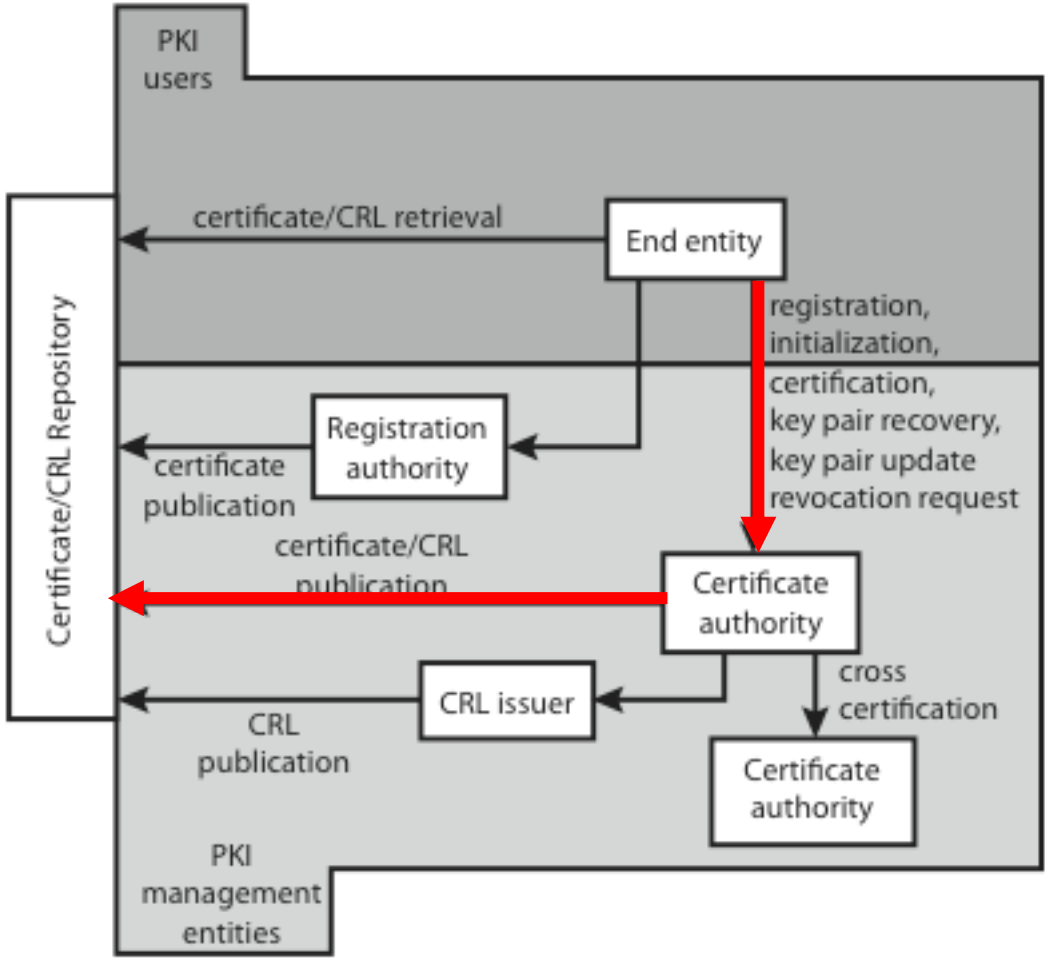
# X.509 Version 3

- Είναι γενικα αποδεκτο ότι χρειαζεται προσθετη πληροφορια για ένα πιστοποιητικο
  - email/URL, λεπτομερειες της πολιτικής, περιορισμοι χρησης
- Αντι να κατονομαστουν ρητα νεα πεδια, οριστηκε μια γενικη μεθοδος επεκτασης
- Η επεκταση αποτελειται απο:
  - Προσδιοριστικο επεκτασης (extension identifier)
  - Δεικτης κρισιμοτητας (criticality indicator)
  - Τιμη επεκτασης (extension value)

# Επεκτασεις Πιστοποιητικων (Certificate Extensions)

- Πληροφοριες κλειδιων και πολιτικης
  - Μεταφερουν πληροφοριες σχετικα με το αντικειμενο και τα κλειδια του εκδοτη καθως και ενδειξεις που αφορουν την πολιτικη πιστοποιησης
- Χαρακτηριστικα του υποκειμενου του πιστοποιητικου και του εκδοτη του
  - Υποστηριζουν εναλλακτικα ονοματα σε εναλλακτικα format για το υποκειμενο η/και τον εκδοτη του πιστοποιητικου
- Περιορισμους του μονοπατιου του πιστοποιητικου (certificate path constraints)
  - Επιτρεπει περιορισμους στη χρηση πιστοποιητικων από αλλες CA.

# Υποδομη Δημοσιου Κλειδιου (Public Key Infrastructure)



# Διαχειριση Υποδομης Δημοσιου Κλειδιου (PKIX Management)

- Λειτουργιες:
  - Εγγραφη (registration)
  - Αρχικοποιηση (initialization)
  - Πιστοποιηση (certification)
  - Ανακτηση ζευγους κλειδιων (key pair recovery)
  - Επικαιροποιηση ζευγους κλειδιων (key pair update)
  - Αιτηση ανακλησης (revocation request)
  - Δια-Πιστοποιηση μεταξυ CAs (cross certification)
- Πρωτοκολλα: CMP (Certificate Management Protocol), CMC (Cryptographic Message Syntax)

# Συνοψη

- Μελετησαμε:
  - Διανομη συμμετρικου κλειδιου με συμμετρικη κρυπτογραφια
  - Διανομη συμμετρικου κλειδιου με κρυπτογραφια δημοσιου κλειδιου
  - Διανομη δημοσιων κλειδιων
    - Ακακοινωση, καταλογος, αρχη πιστοποιησης (CA).
  - Πιστοποιηση Αυθεντικοτητας και Πιστοποιητικα X.509
  - Υποδομη Δημοσιου Κλειδιου (Public key infrastructure, PKIX)