Διαχείριση και διανομή κλειδιών

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα

- Διανομή συμμετρικών κλειδιών
- Διανομή δημοσίων κλειδιών
- Ψηφιακά πιστοποιητικά X.509
- Υποδομές δημοσίου κλειδιού

Διανομή συμμετρικών κλειδιών

ΜΕ ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Διανομή κλειδιών: ανάγκη

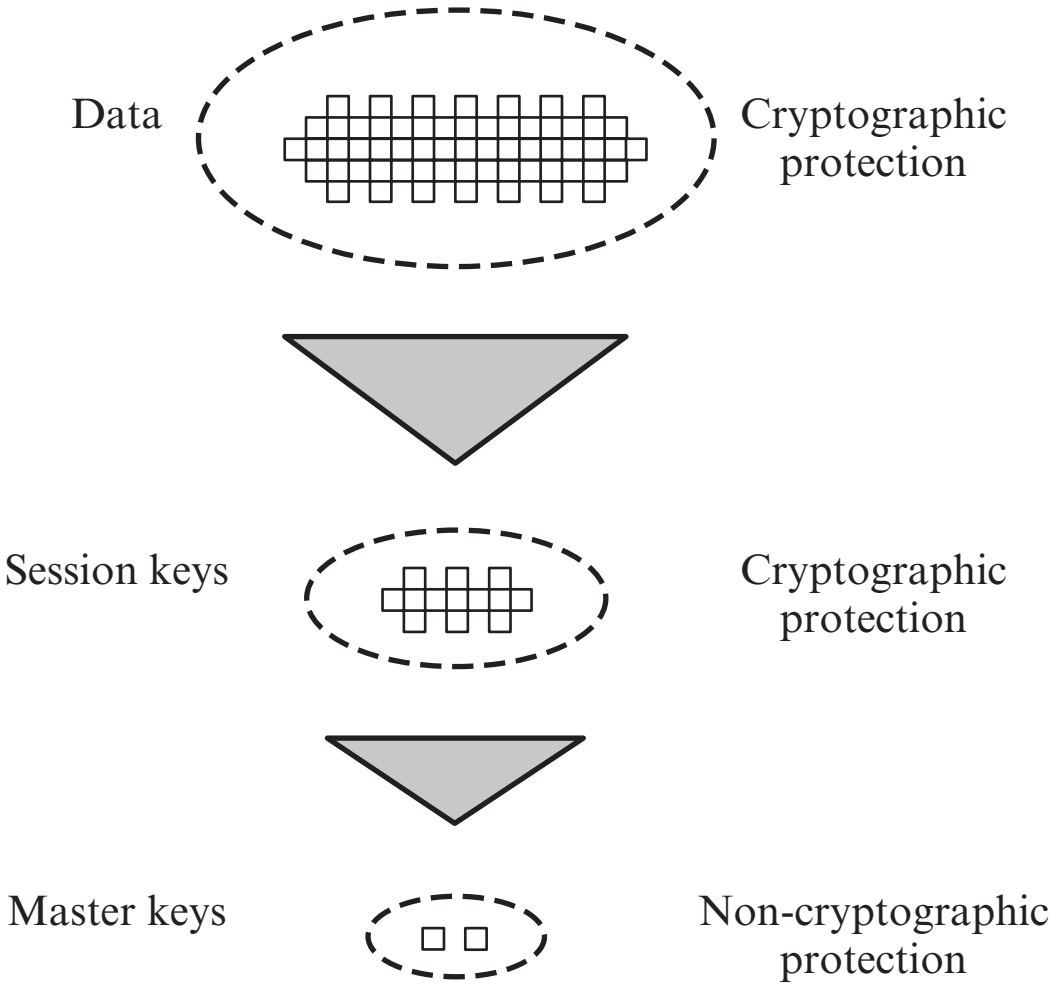
- For symmetric encryption to work, the two parties to an exchange must share the same key
  - that key must be protected from access by others
- Frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key
- Key distribution technique
  - The means of delivering a key to two parties that wish to exchange data, without allowing others to see the key

Διανομή κλειδιών: επιλογές

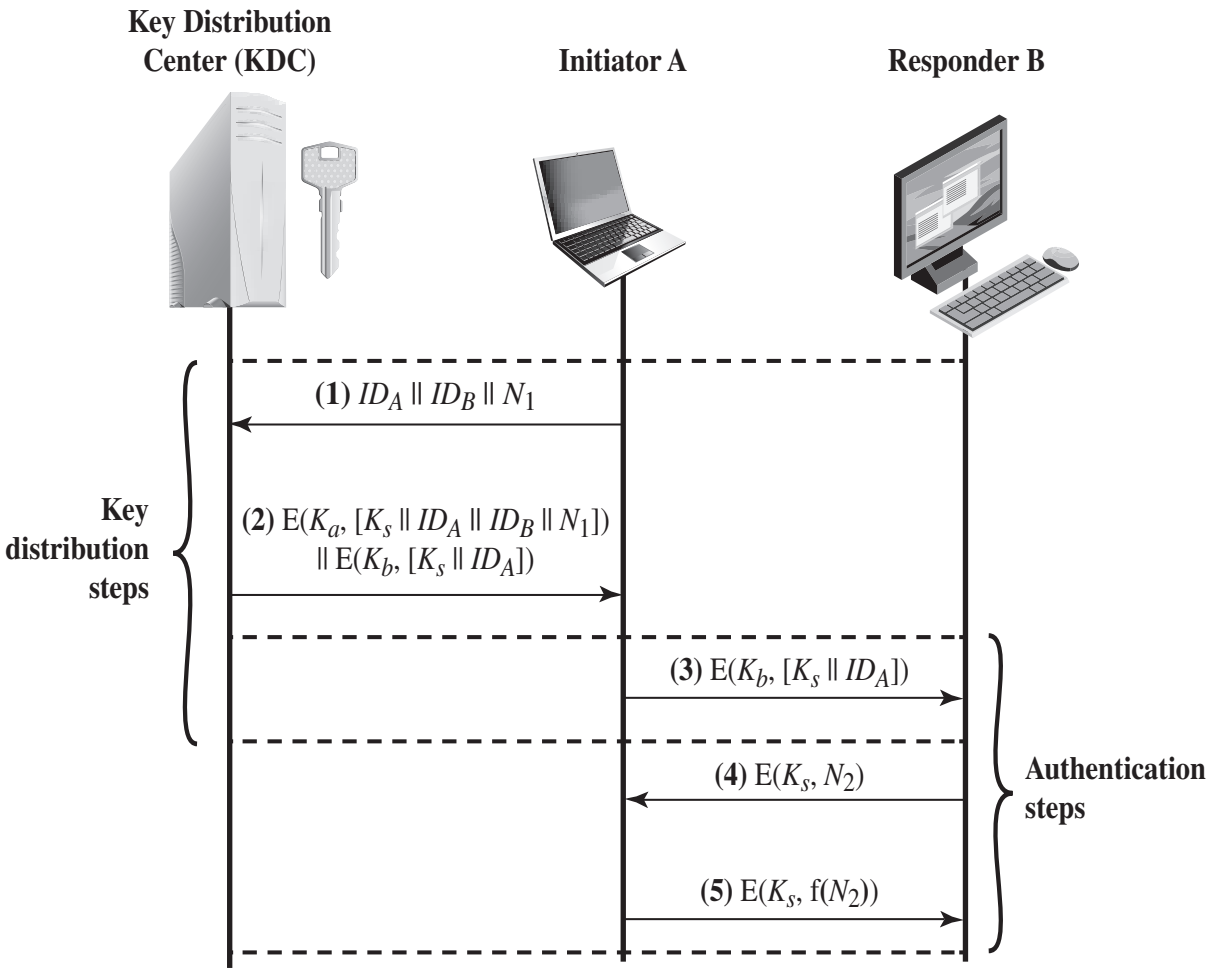
- For two parties A and B, there are the following options:

1. A key can be selected by A and physically delivered to B
2. A third party can select the key and physically deliver it to A and B
3. If A, B have previously/recently used a key, a party could transmit a new key to the other using the old key to encrypt the new one
4. If A, B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B

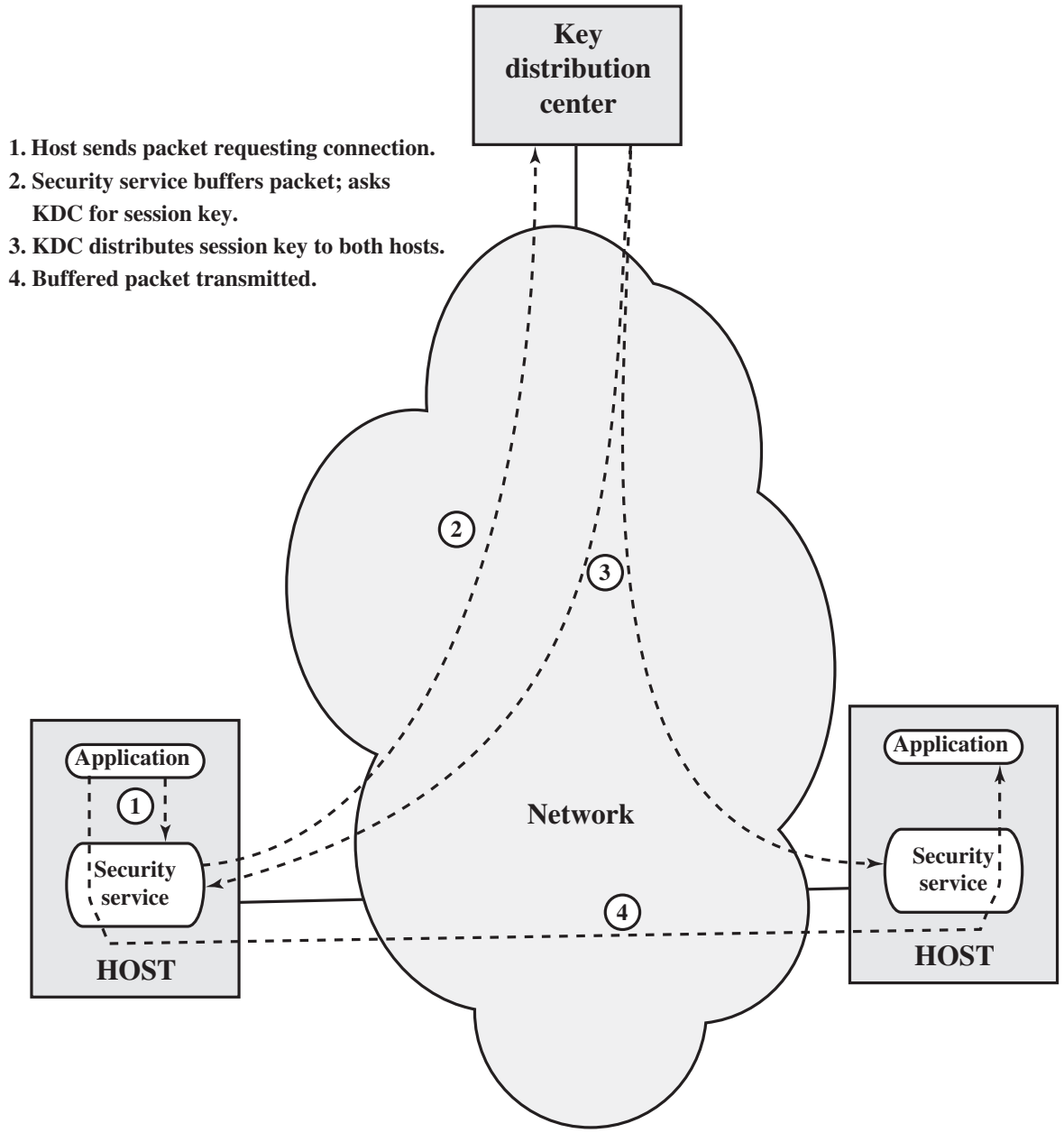
Διανομή κλειδιών: ιεραρχία



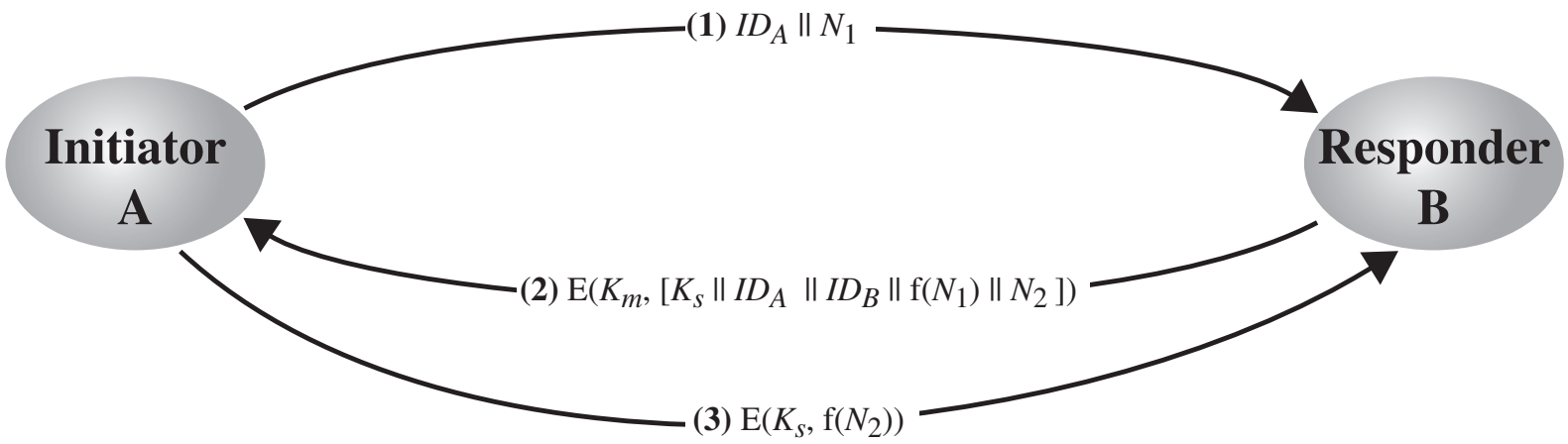
Διανομή κλειδιών: χρήση KDC



Διανομή κλειδιών: ανά υπηρεσία



Διανομή κλειδιών: κατανεμημένο

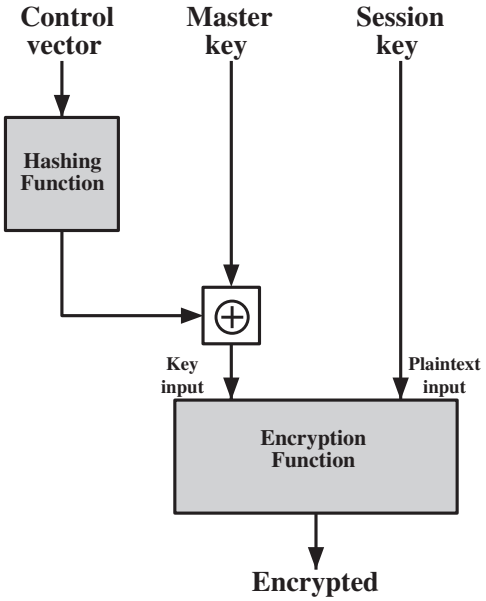


Διανομή κλειδιών: με έλεγχο

- We may define different types of session keys on the basis of their use
  - Data-encrypting key, for general communication across a network
  - PIN-encrypting key, for personal identification numbers (PINs) used in electronic funds transfer and point-of-sale applications
  - File-encrypting key, for encrypting files stored in publicly accessible locations
- Π.χ. τα bit ισοτιμίας σε κλειδί για τον αλγόριθμο DES θα μπορούσαν να χρησιμοποιηθούν για το σκοπό αυτό

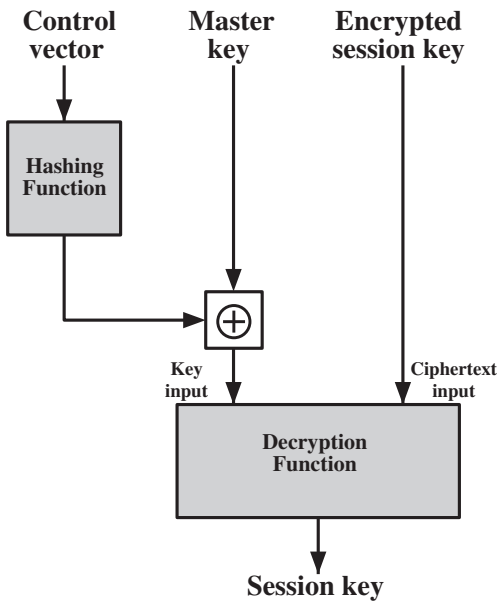
Διανομή κλειδιών: με έλεγχο

- (α) Κρυπτογράφηση



- Key input $K_c = K_m \oplus h(CV)$
- Ciphertext $C = Enc(K_c, K_s)$

- (β) Αποκρυπτογράφηση



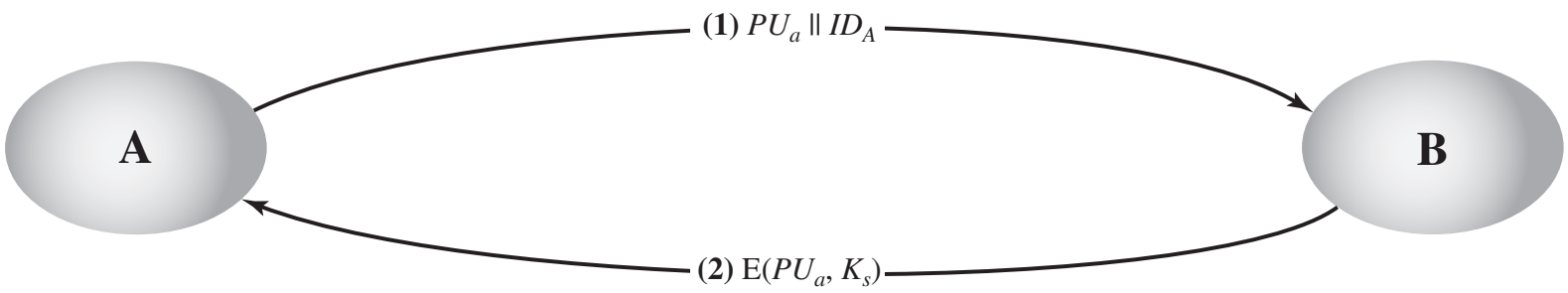
- Key input $K_c = K_m \oplus h(CV)$
- Plaintext $K_s = Dec(K_c, C)$

Διανομή συμμετρικών κλειδιών

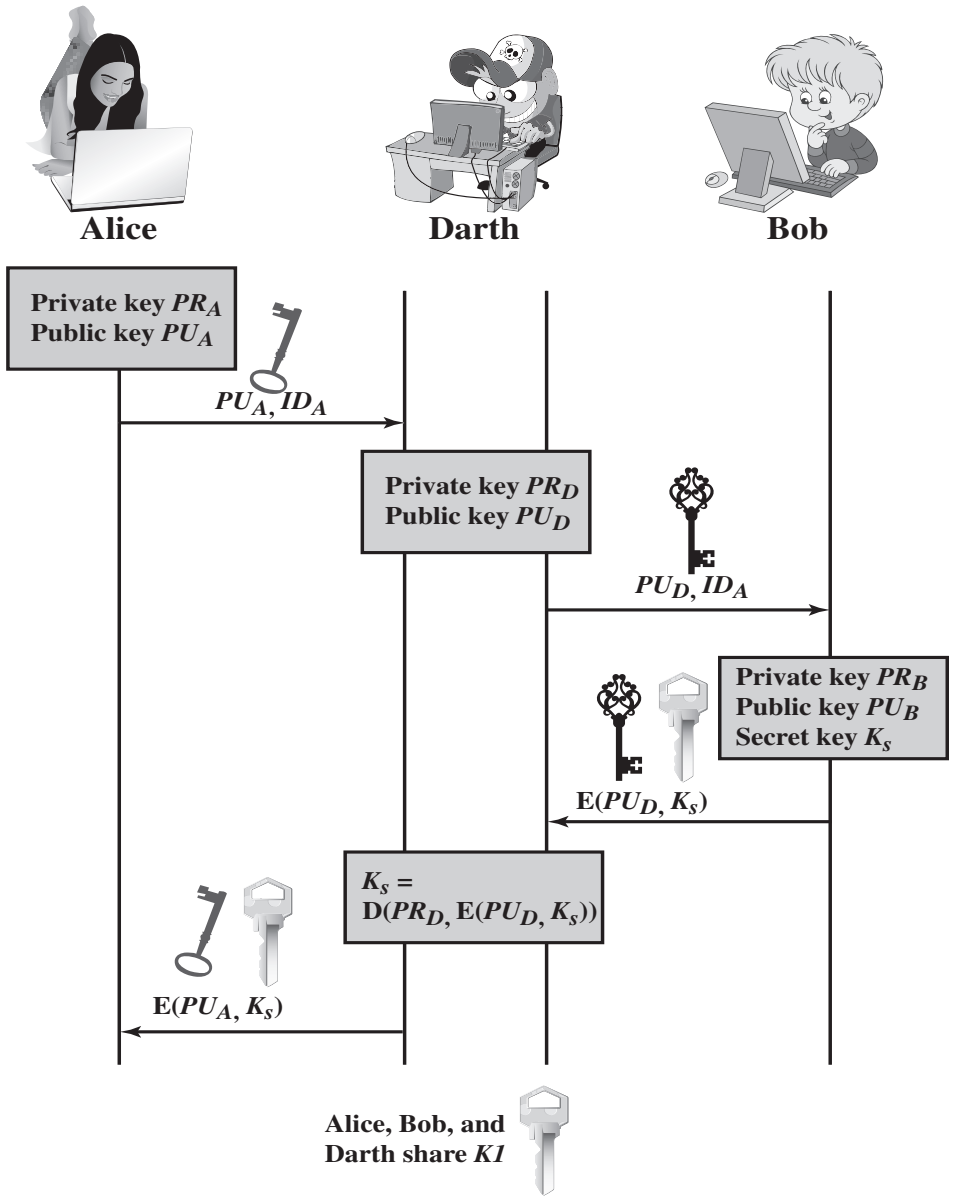
ΜΕ ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Διανομή κλειδιών: με χρήση PKC

- Απλός τρόπος συμφωνίας κλειδιού

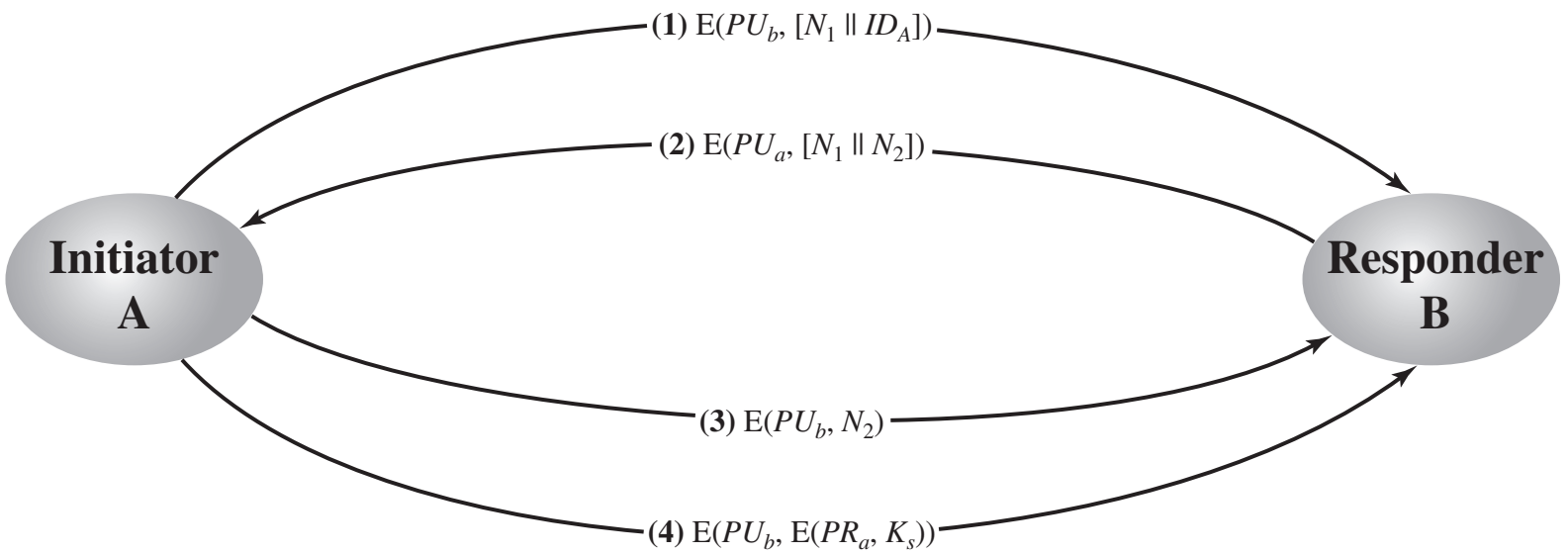


Διανομή κλειδιών: MiTM



Διανομή κλειδιών: χρήση PKC

- Εάν οι χρήστες έχουν ήδη ανταλλάξει δημόσια κλειδιά



Διανομή δημοσίων κλειδιών

Διανομή κλειδιών

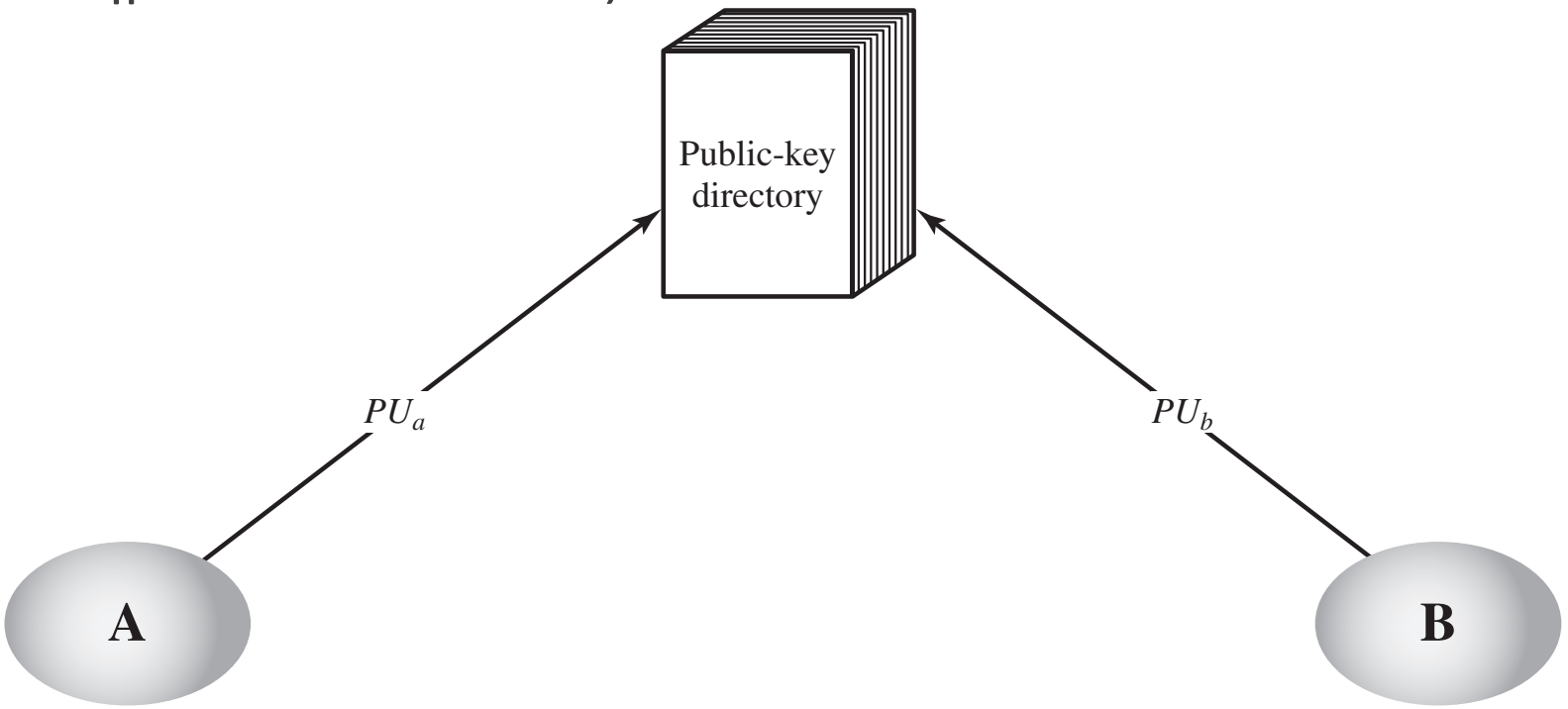
- Προσωπική διανομή κλειδιών
- Χρήση ενός δημόσιου καταλόγου
- Έμπιστες αρχές διανομής δημοσίων κλειδιών
- Πιστοποιητικά δημοσίων κλειδιών

Διανομή κλειδιών: προσωπική

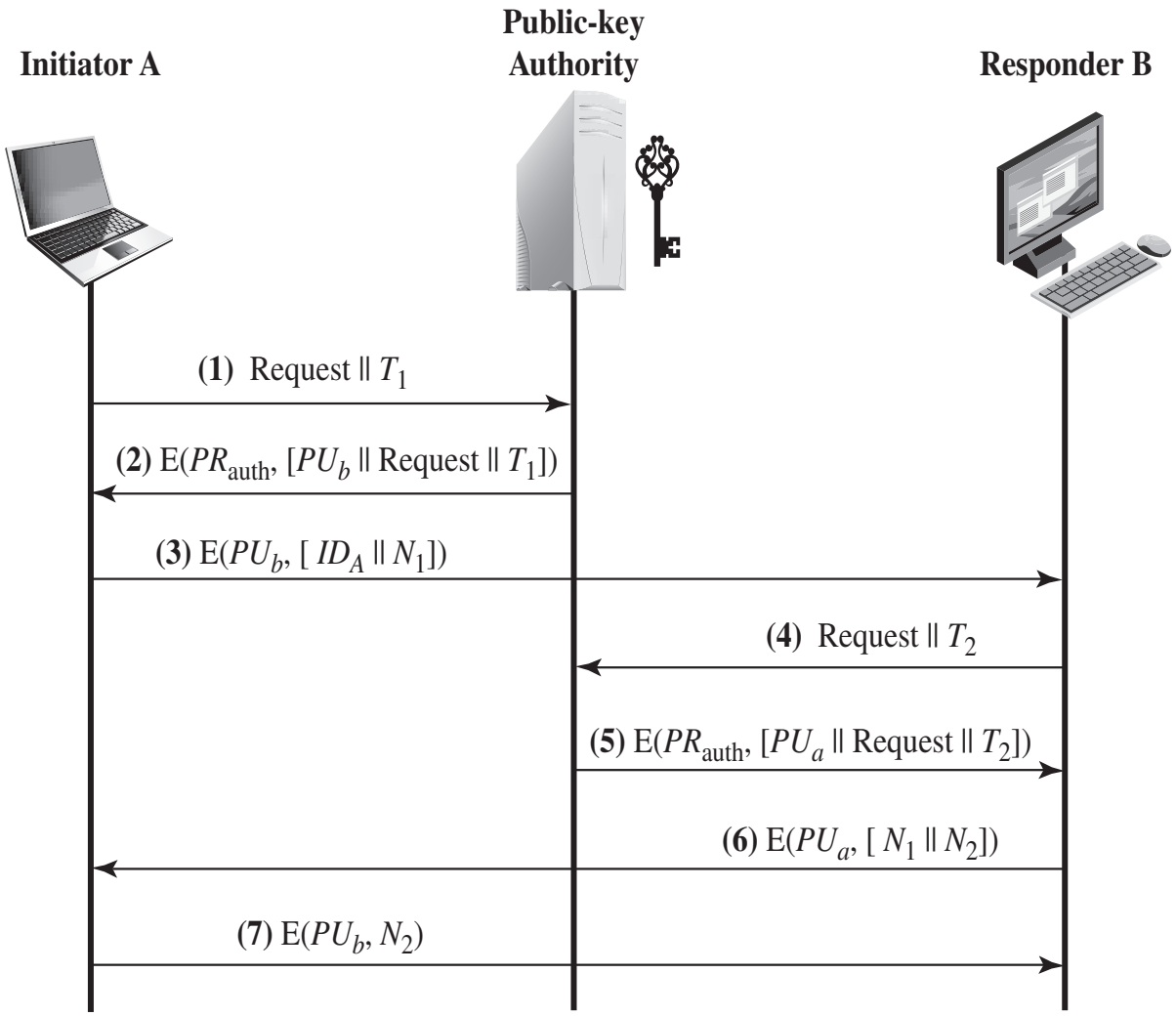
- Παραδείγματα χρήσης από PGP

Διανομή κλειδιών: κατάλογος

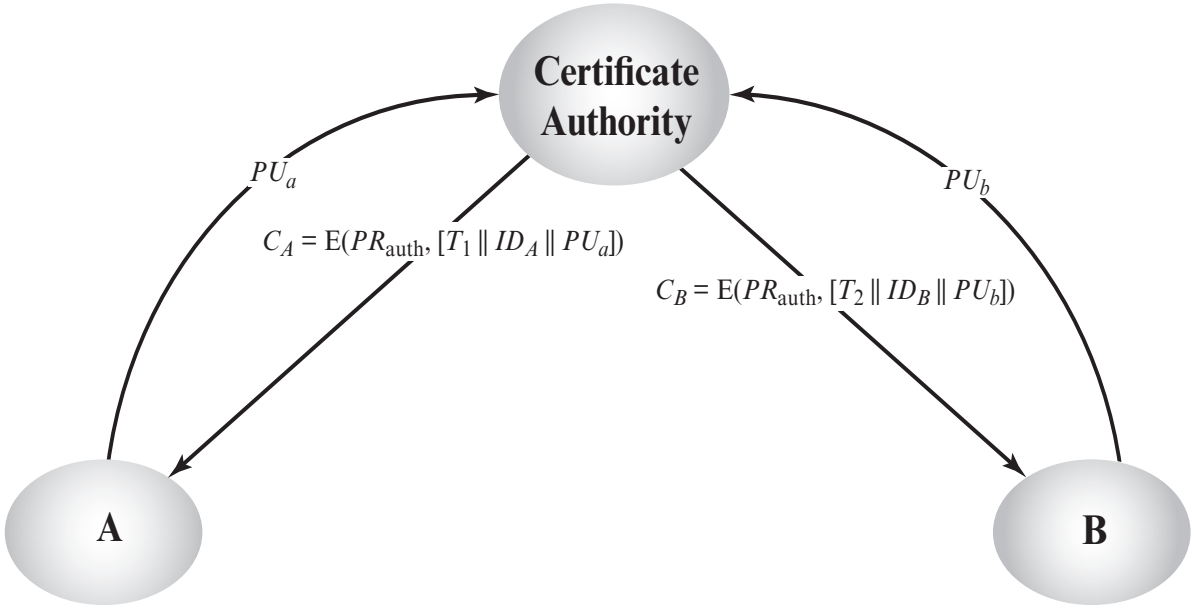
- Πρέπει να υπάρχει ασφαλής αντιστοίχιση χρηστών με τα δημόσια κλειδιά τους



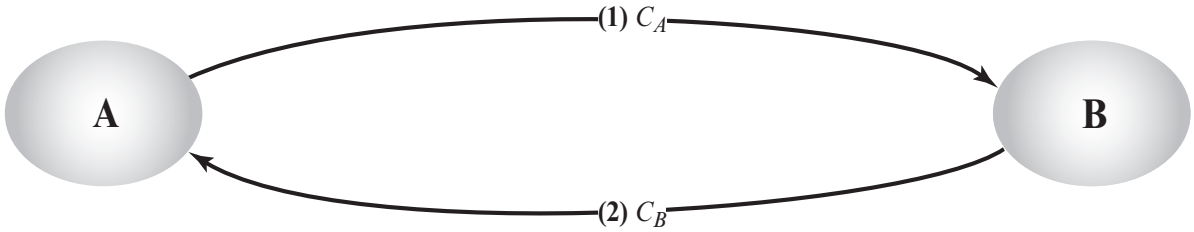
Διανομή κλειδιών: έμπιστες αρχές



Διανομή κλειδιών: πιστοποιητικά



(a) Obtaining certificates from CA

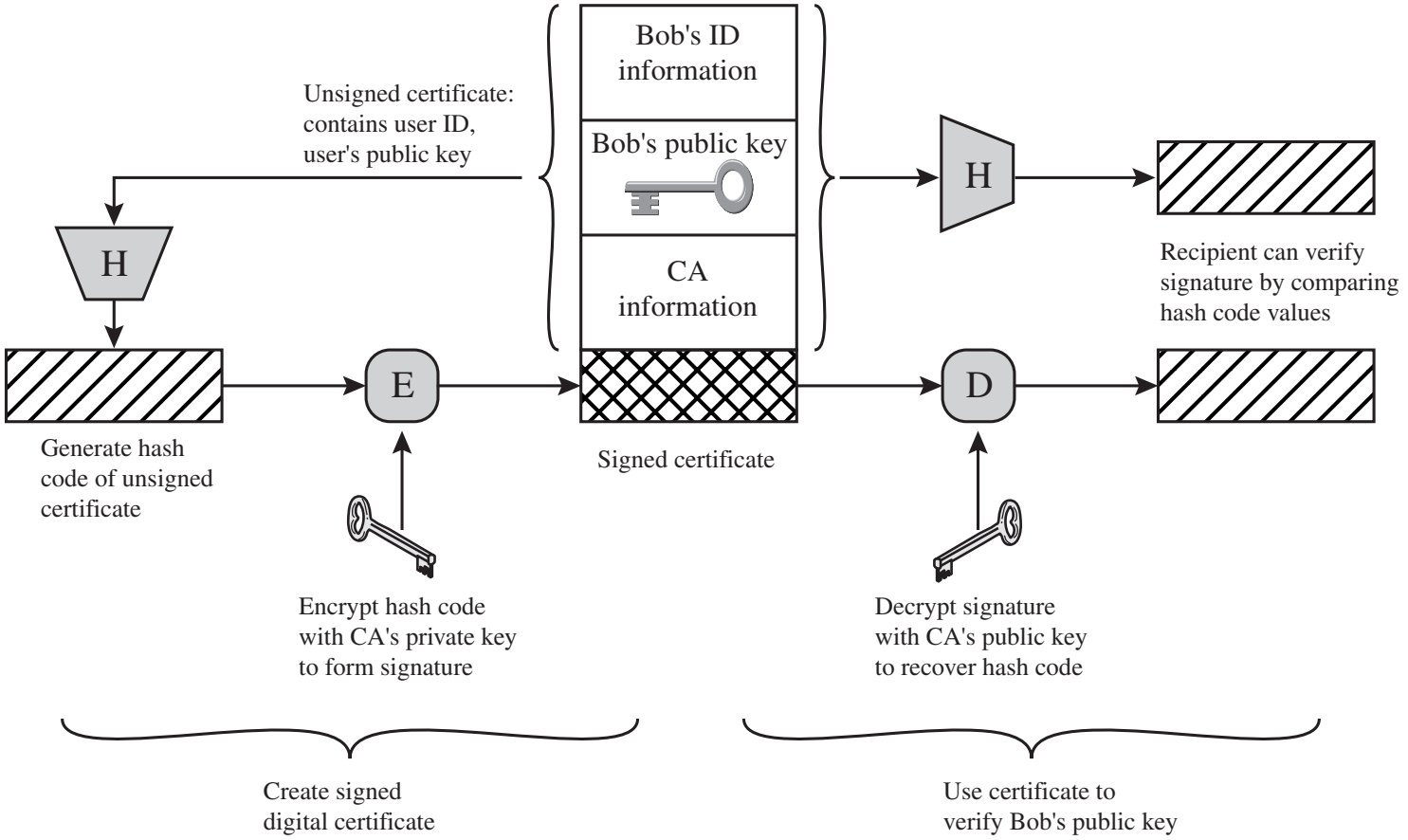


(b) Exchanging certificates

Ψηφ. πιστοποιητικά

- Πρότυπα ψηφιακών πιστοποιητικών
  - X.509 (v1, v2, και v3)
  - PKCS #6
- Πιο διαδεδομένο: X.509 v3
  - V1: 1988 (προτάθηκε από ISO και ITU)
  - Υιοθετήθηκε από Visa και MasterCard
  - Χρήση στο SET (Secure Electronic Transactions)

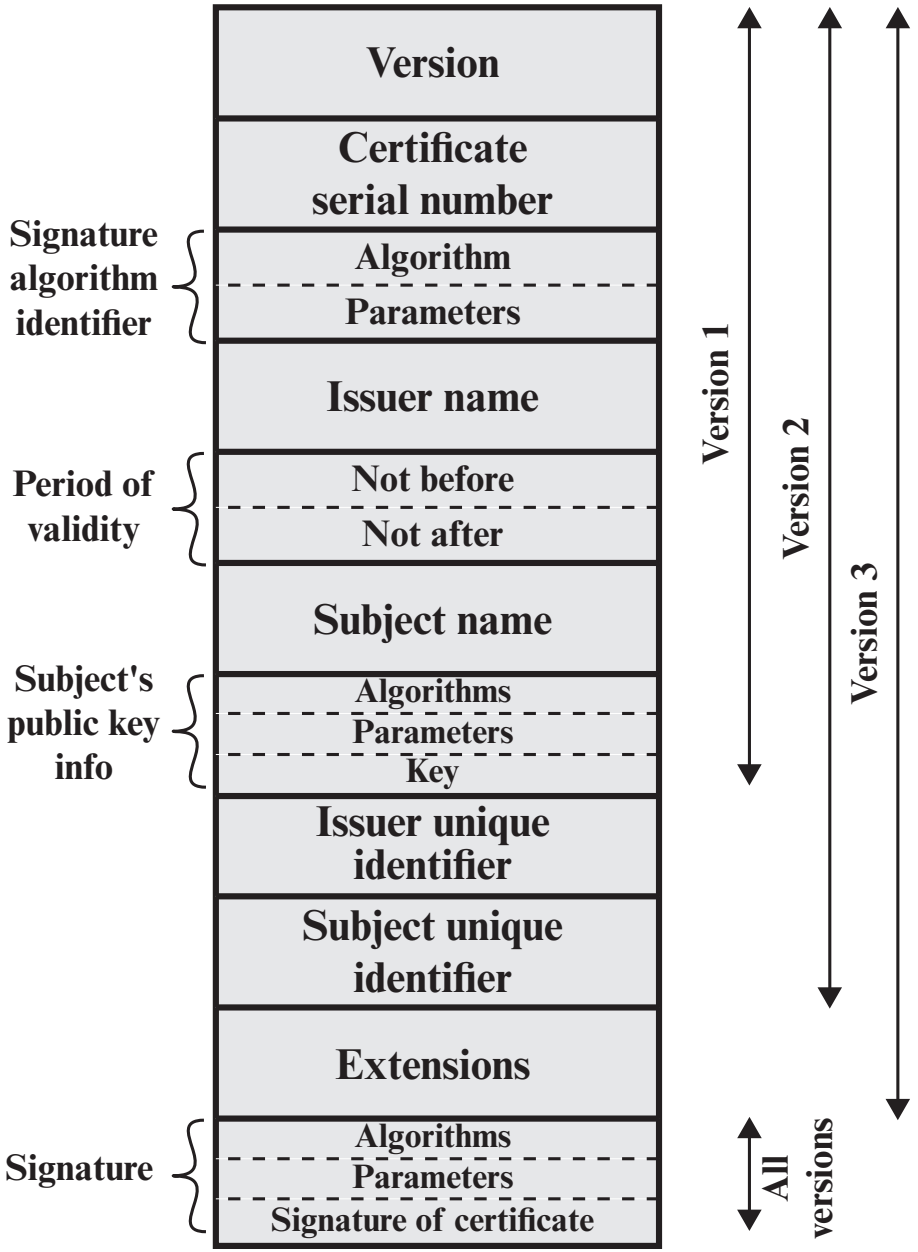
Ψηφ. πιστοποιητικά: χρήση



Ψηφ. πιστοποιητικά: X.509

- Στοιχεία πιστοποιητικού
  - Σειριακός αριθμός
  - Περίοδος ισχύος
- Στοιχεία αρχής/δικαιούχου
  - Όνομα καταλόγου X.500
- Στοιχεία κλειδιού
  - Αλγ. δημοσίου κλειδιού
  - Τιμή δημοσίου κλειδιού
- Στοιχεία επαλήθευσης
  - Ψηφιακή υπογραφή

Ψηφ. πιστοποιητικά: X.509



Ψηφ. πιστοποιητικά: X.509

X.509 v3 includes a number of optional extensions

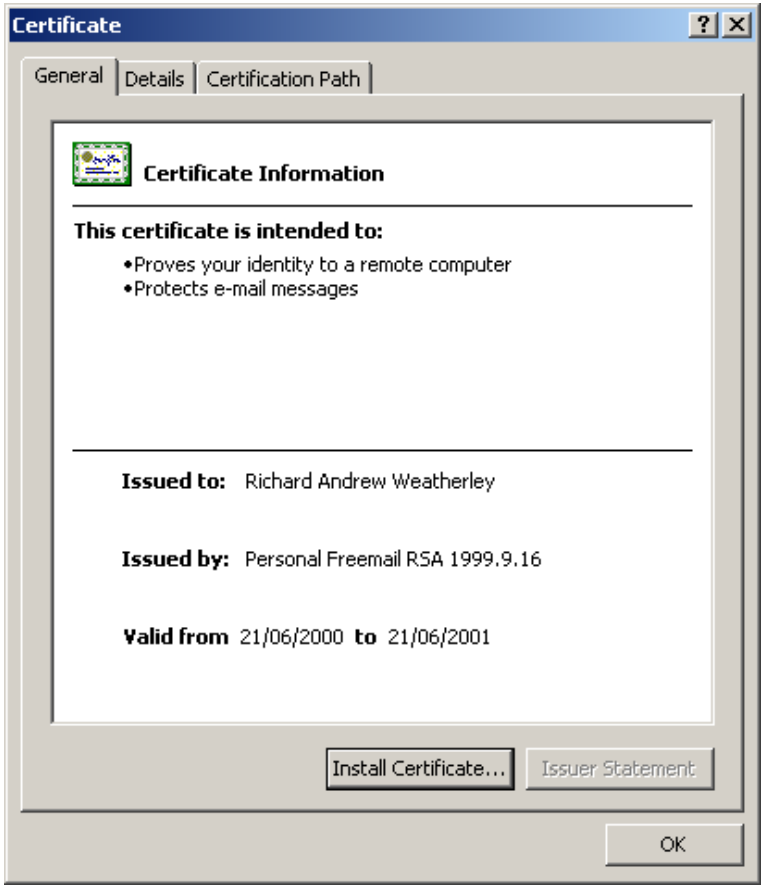
Extensions consist of:

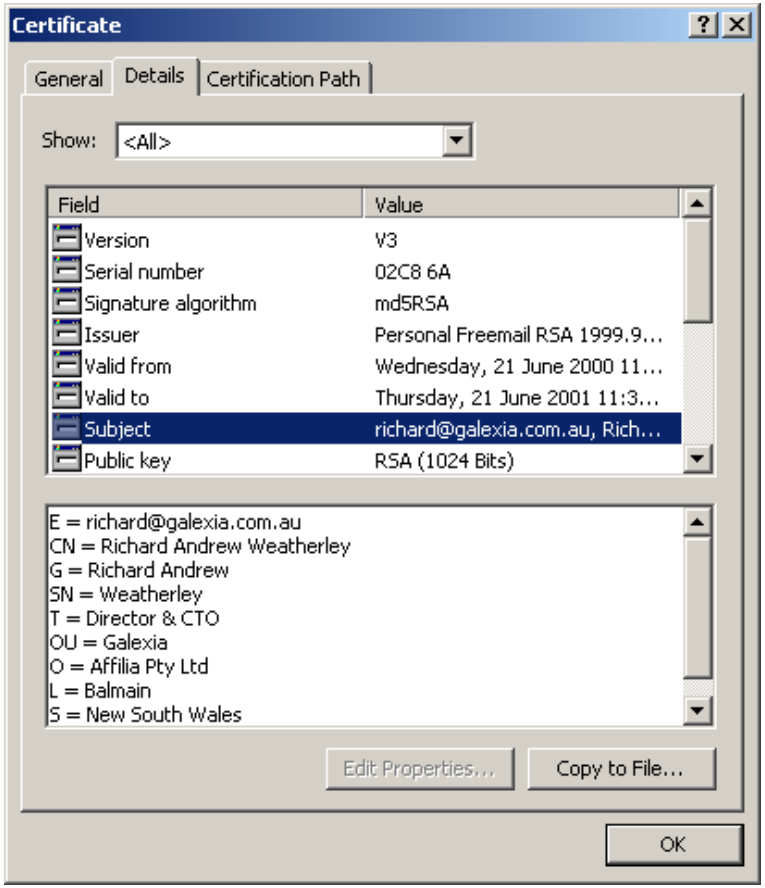
- an extension identifier
- a criticality indicator
- an extension value

Extension categories:

- key and policy information
- certification path constraints
- subject & issuer attributes

Ψηφ. πιστοποιητικά: X.509





Ψηφ. πιστοποιητικά: X.509

- Το πρότυπο χρησιμοποιεί την εξής σημειογραφία

$$CA\ll A\gg = CA\{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$$

όπου $Y\ll X\gg$ το πιστοποιητικό του X από τον Y και

$Y\{I\}$ = the signing of I by Y

V = version of the certificate

SN = serial number of the certificate

AI = identifier of the algorithm used to sign the certificate

CA = name of certificate authority

Ψηφ. πιστοποιητικά: X.509

- Το πρότυπο χρησιμοποιεί την εξής σημειογραφία

$$CA\ll A\gg = CA\{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$$

όπου $Y\ll X\gg$ το πιστοποιητικό του X από τον Y και

UCA = optional unique identifier of the CA

A = name of user A

UA = optional unique identifier of the user A

Ap = public key of user A

T^A = period of validity of the certificate

Ψηφ. πιστοποιητικά: PKCS #6

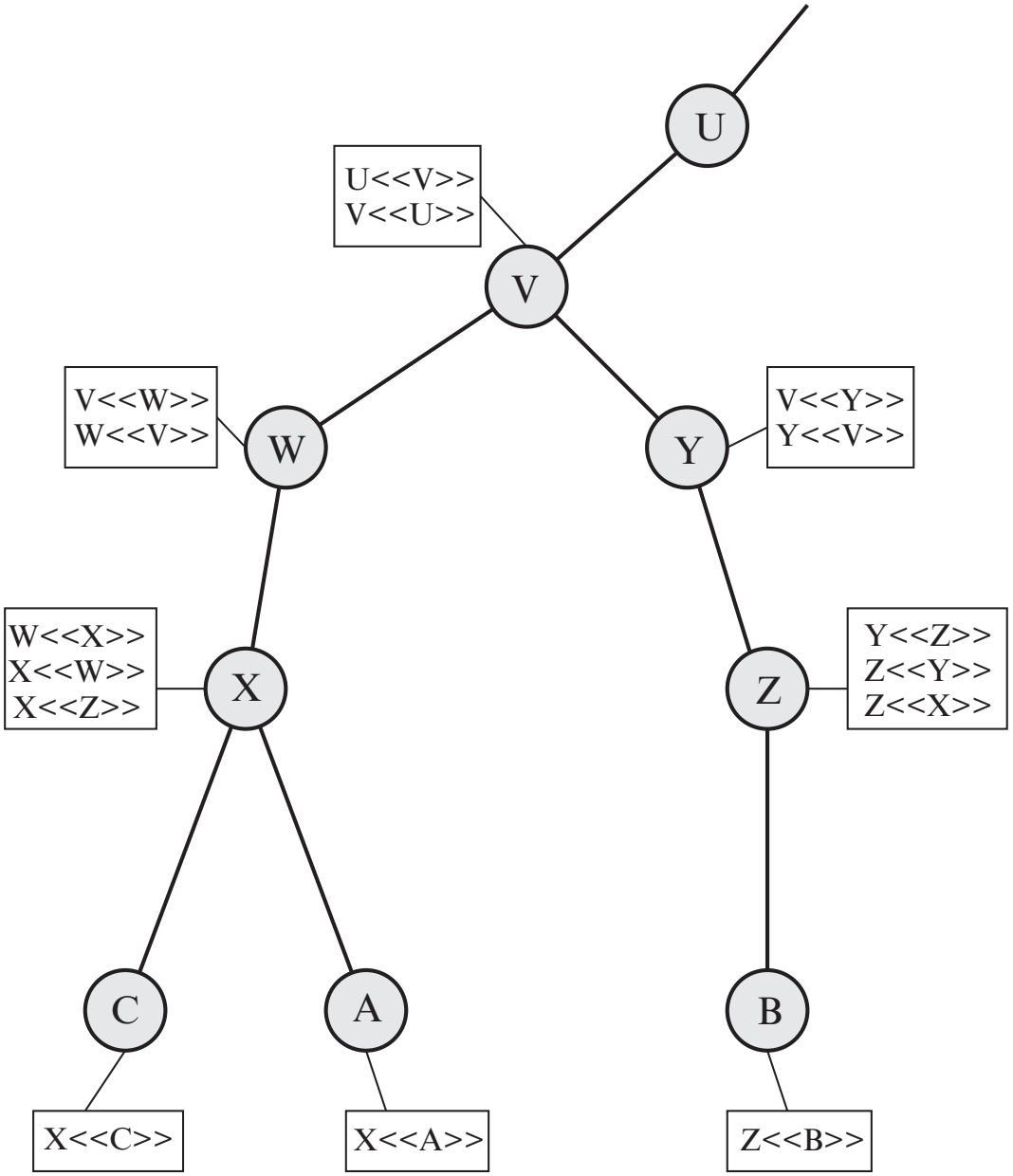
- Το πρότυπο ορίστηκε από την RSA Data Security Inc.
  - http://www.rsasecurity.com/
- Περιλαμβάνονται τα ακόλουθα στοιχεία:
  - Αριθμός έκδοσης
  - Πιστοποιητικό τύπου X.509
  - Λίστα επιλεγμένων χαρακτηριστικών
  - Αλγόριθμος ψηφιακής υπογραφής
  - Ψηφιακή υπογραφή αρχής έκδοσης

Ψηφ. πιστοποιητικά: PKCS #6

- Επιλεγμένα χαρακτηριστικά (PKCS #9)

businessCategory	commonName	countryName
description	destinationIndicator	x121Address
iSDNAddress	localityName	member
objectClass	organizationName	title
postalAddress	postalCode	postOfficeBox
presentationAddress	registeredAddress	streetAddress
roleOccupant	serialNumber	stateOrProvinceName
telephoneNumber	surname	preferredDeliveryMethod

Ιεραρχία πιστοποιητικών X.509



Μονοπάτια πιστοποίησης

ΕΠΑΛΗΘΕΥΣΗ

- Η επαλήθευση ενός πιστο-ποιητικού απαιτεί ένα ολοκληρωμένο μονοπάτι
- Παράδειγμα σχήματος

  Z≪Y≫ Y≪V≫ V≪W≫ W≪X≫ X≪A≫

ΜΟΝΤΕΛΑ ΕΜΠΙΣΤΟΣΥΝΗΣ

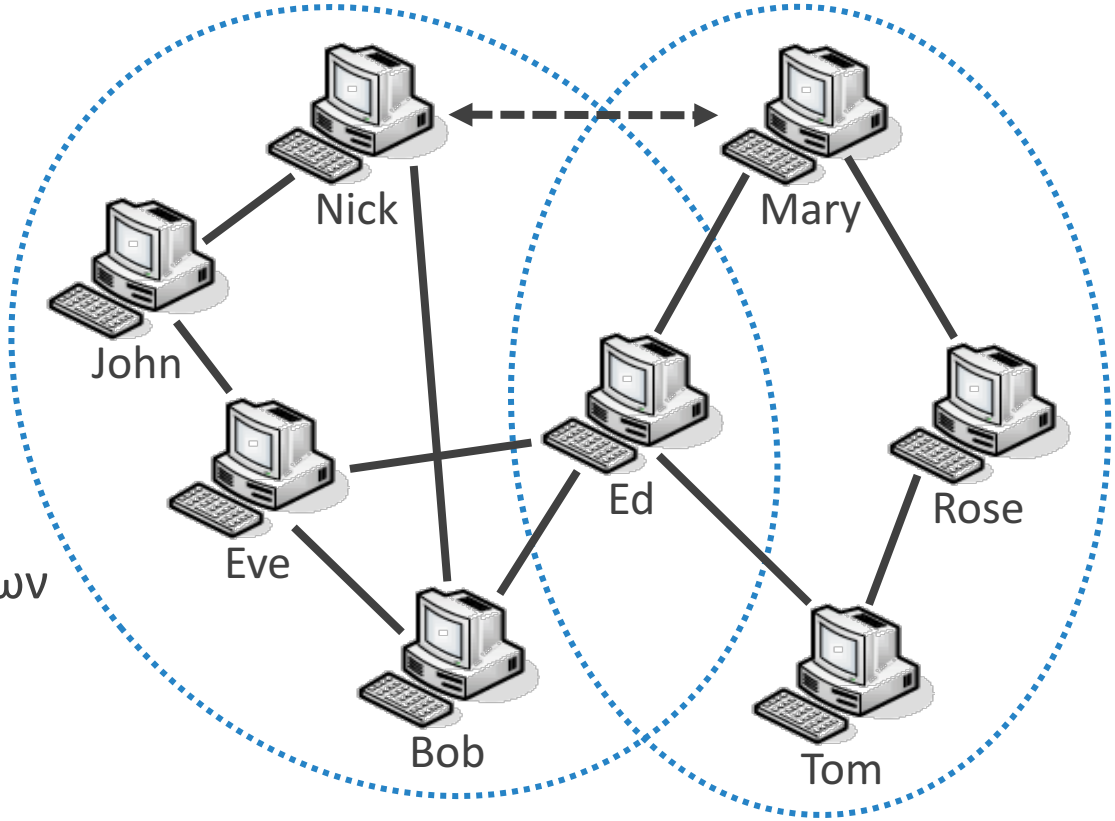
- Ένα σύνολο μονοπατιών πιστοποίησης ονομάζεται μοντέλο εμπιστοσύνης
- Κύριοι αντιπρόσωποι
  - ιεραρχικό μοντέλο
  - σύνθετο ιεραρχικό μοντέλο
  - web of trust

Μονοπάτια πιστοποίησης

- Η επίτευξη σχέσεων εμπιστοσύνης μεταξύ των δύο βασικών αρχών πιστοποίησης μπορεί να επιτευχθεί
  - Μέσω διασταυρωμένων πιστοποιητικών
  - Προσοχή: διαπίστευση και από τις δύο πλευρές
- Η ασφάλεια του όλου συστήματος βασίζεται στο ιδιωτικό κλειδί της βασικής αρχής πιστοποίησης
  - Κίνδυνοι από πιθανή αποκάλυψη
- Μεγάλα μήκη αλυσίδων επαλήθευσης ακόμα και για χρήστες που ανήκουν στην ίδια ιεραρχία

Μονοπάτια πιστοποίησης

- Web of trust
  - Χρησιμοποιήθηκε πρώτη φορά από το PGP
  - Προβλήματα επεκτασιμότητας
  - Θεωρία προσανα-τολισμένων γράφων

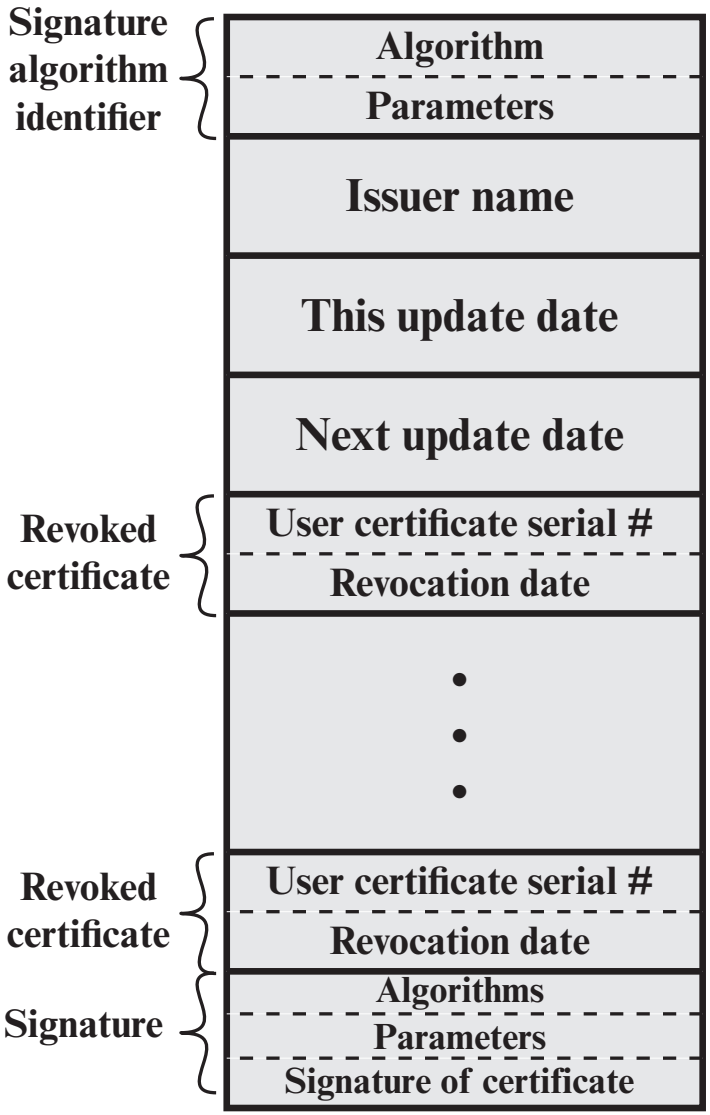


Ανάκληση πιστοποιητικών

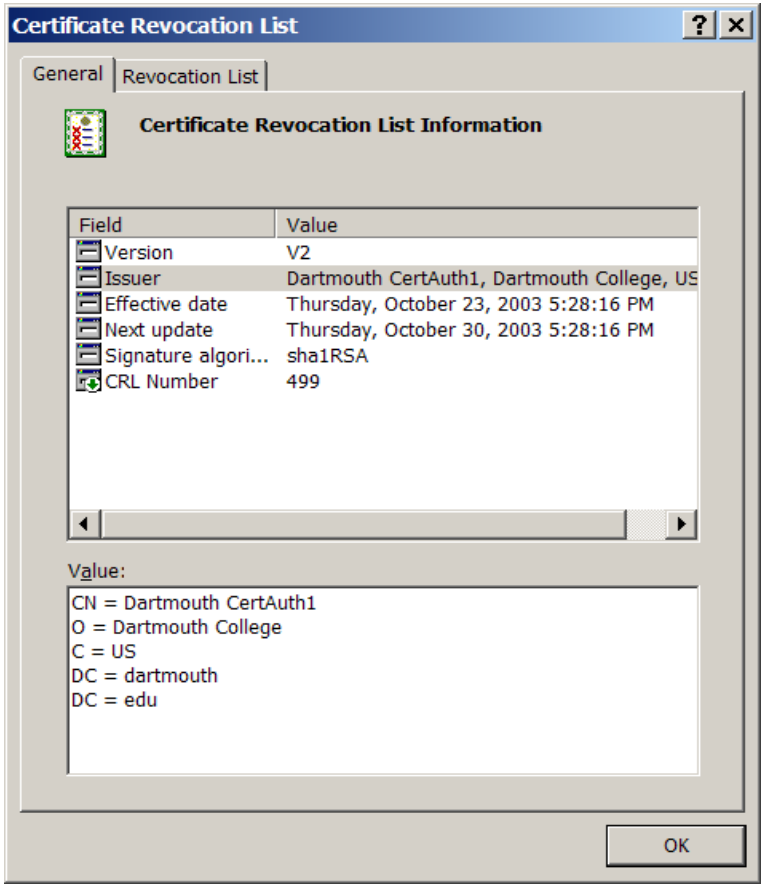
- Cert. revocation list (CRL)
  - Κλασικό μοντέλο
  - Σημεία διανομής CRLs (CDP)
  - Freshest CRLs (FCRL)
- Online cert. status protocol (OCSP)
  - Προτάθηκε από την IETF - αναπτύχθηκε από τη VeriSign
  - Επαλήθευση πραγματικού χρόνου
  - OCSP responders - παρέχουν πληροφορίες στους clients

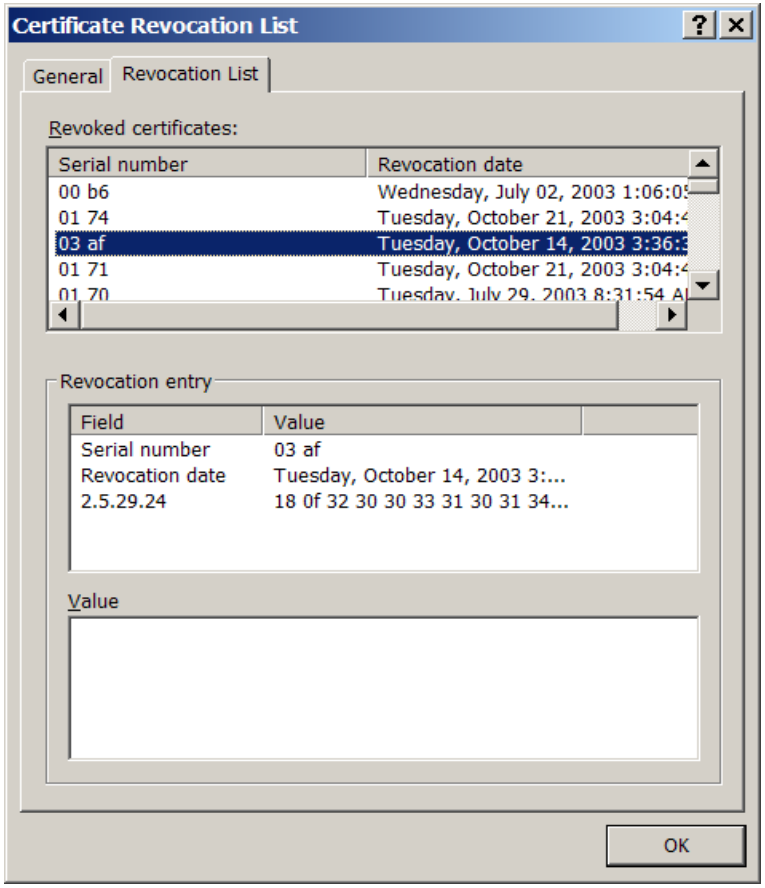
Ανάκληση πιστοποιητικών: CRL

- Επεκτάσεις
  - *Σε κάθε αντικείμενο της λίστας*
  - *Συνολικά στη λίστα*



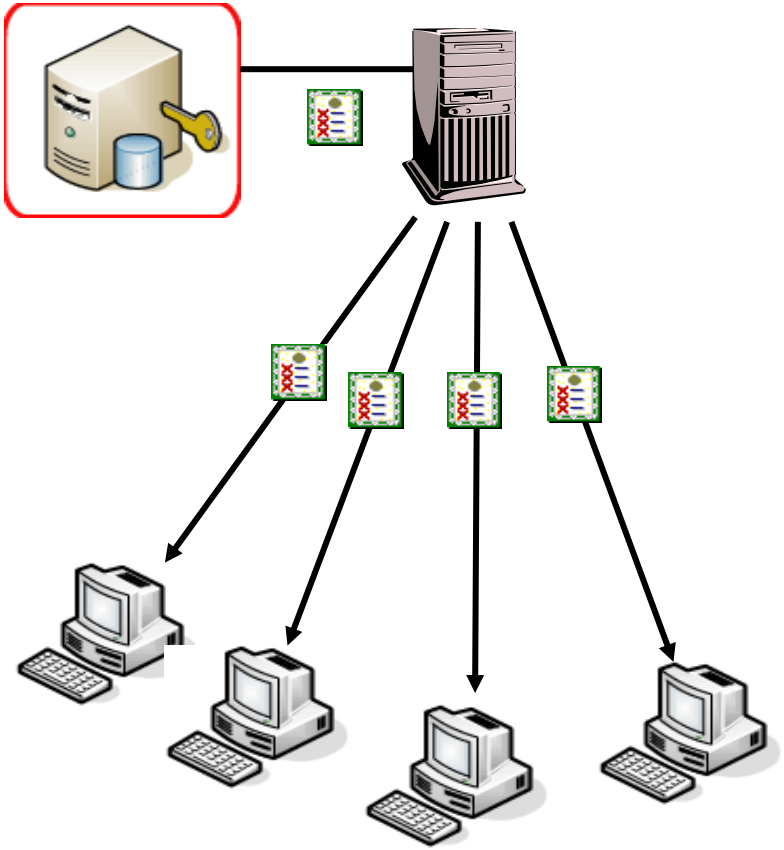
Ανάκληση πιστοποιητικών: CRL





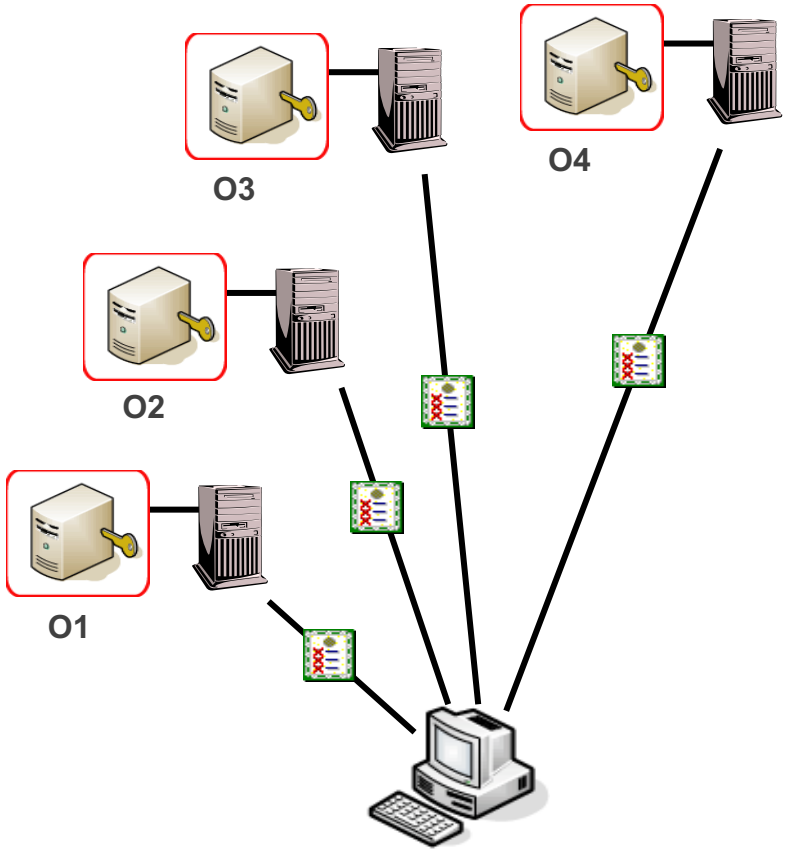
Ανάκληση πιστοποιητικών: CRL

- Θέματα επεκτασιμότητας
  - ανάλογη του πλήθος των συνδρομητών
  - ανάλογη της πιθανότητας ανάκλησης
  - ανάλογη του χρόνου ζωής πιστοποιητικών



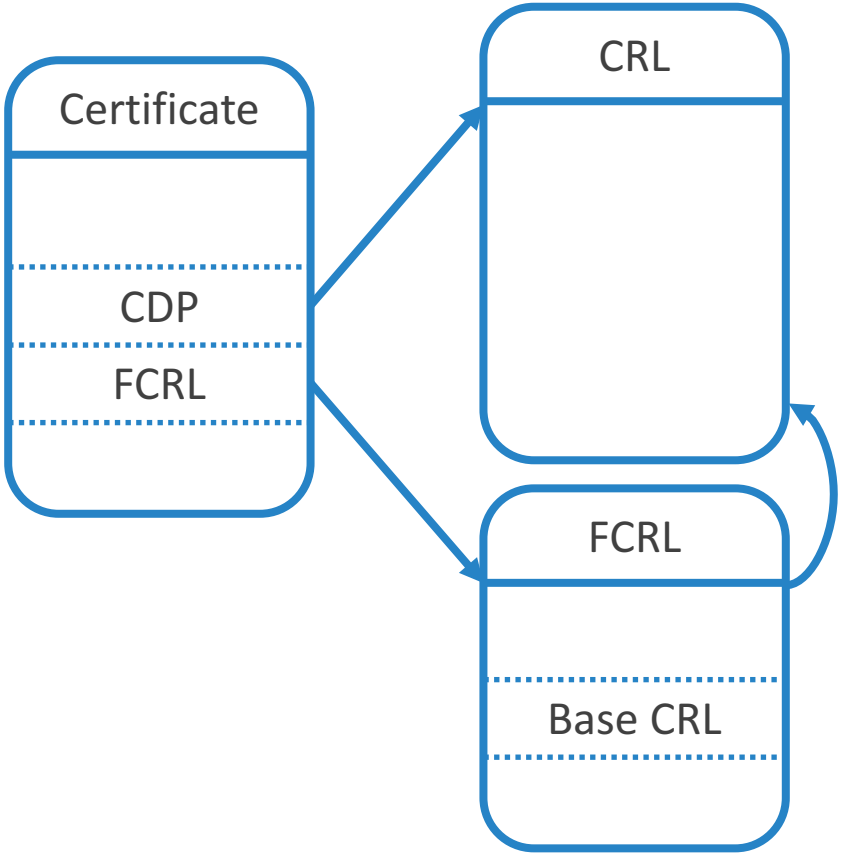
Ανάκληση πιστοποιητικών: CRL

- Θέματα αποδοτικότητας
  - ανάγκη συχνής ανανέωσης της λίστας
  - ανάγκη λήψης για κάθε εφαρμογή
  - ανάγκη λήψης από πολλές αρχές πιστοποίησης



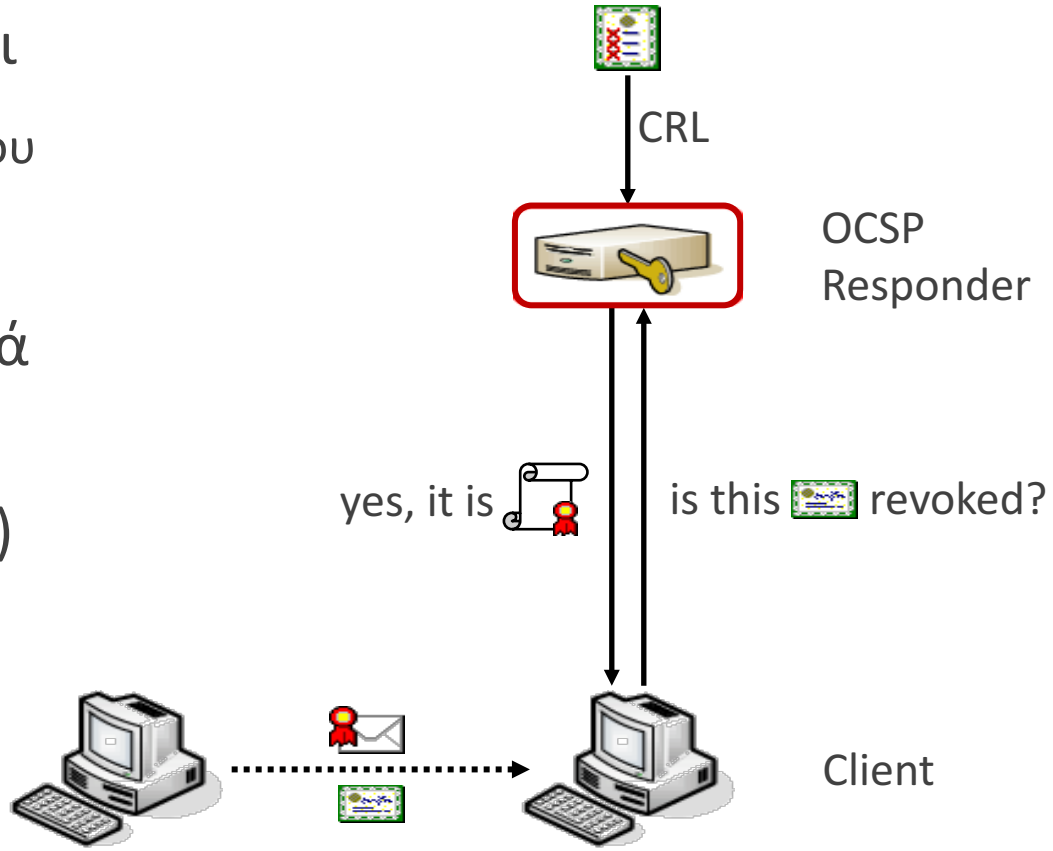
Ανάκληση πιστοποιητικών: CRL

- Κατάχρηση διαθέσιμου εύρους ζώνης δικτύου
  - ανάλογη του τετραγώνου του πλήθους χρηστών
- Λύση προβλήματος(;)
  - Σημεία διανομής CRLs (CDP)
    - κατάτμηση σε μικρότερα τμήματα
  - Freshest CRLs (FCRL)
    - μόνο πρόσφατα πιστοποιητικά
    - Συχνότερες εκδόσεις της λίστας



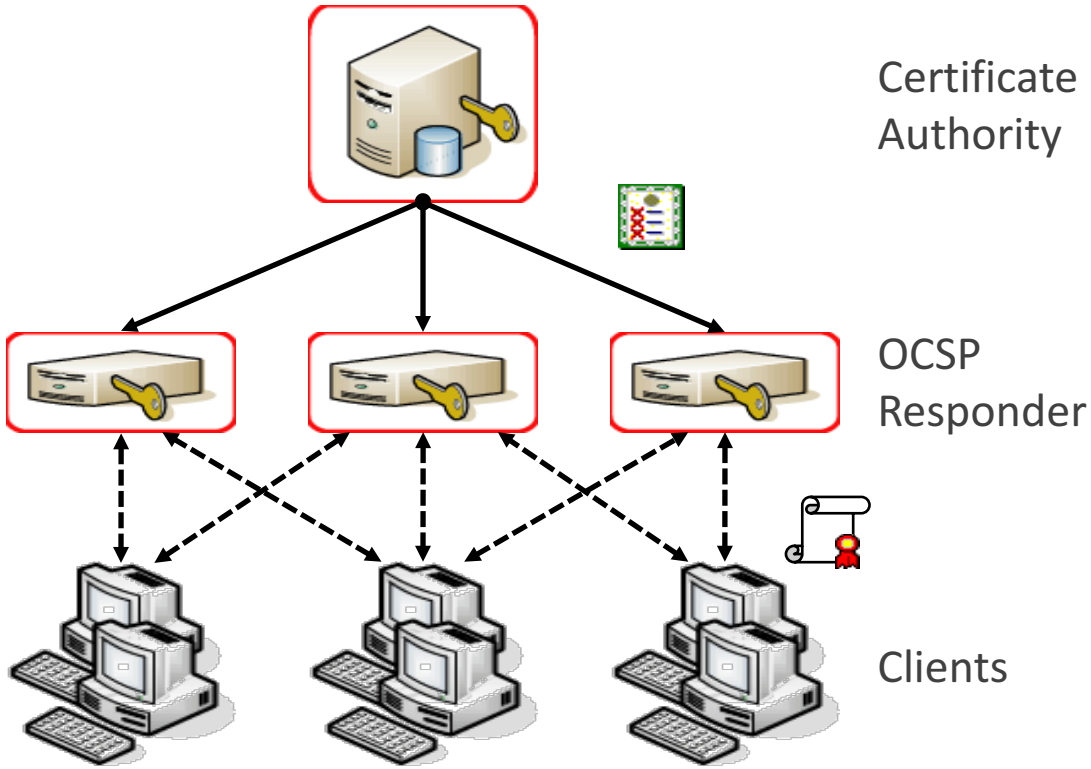
Ανάκληση πιστοποιητικών: OCSP

- Η αίτηση OCSP έχει
  - Έκδοση πρωτοκόλλου
  - S/N πιστοποιητικού
- Απάντηση ψηφιακά υπογεγραμμένη
- Κατάσταση (status)
  - good
  - revoked
  - unknown

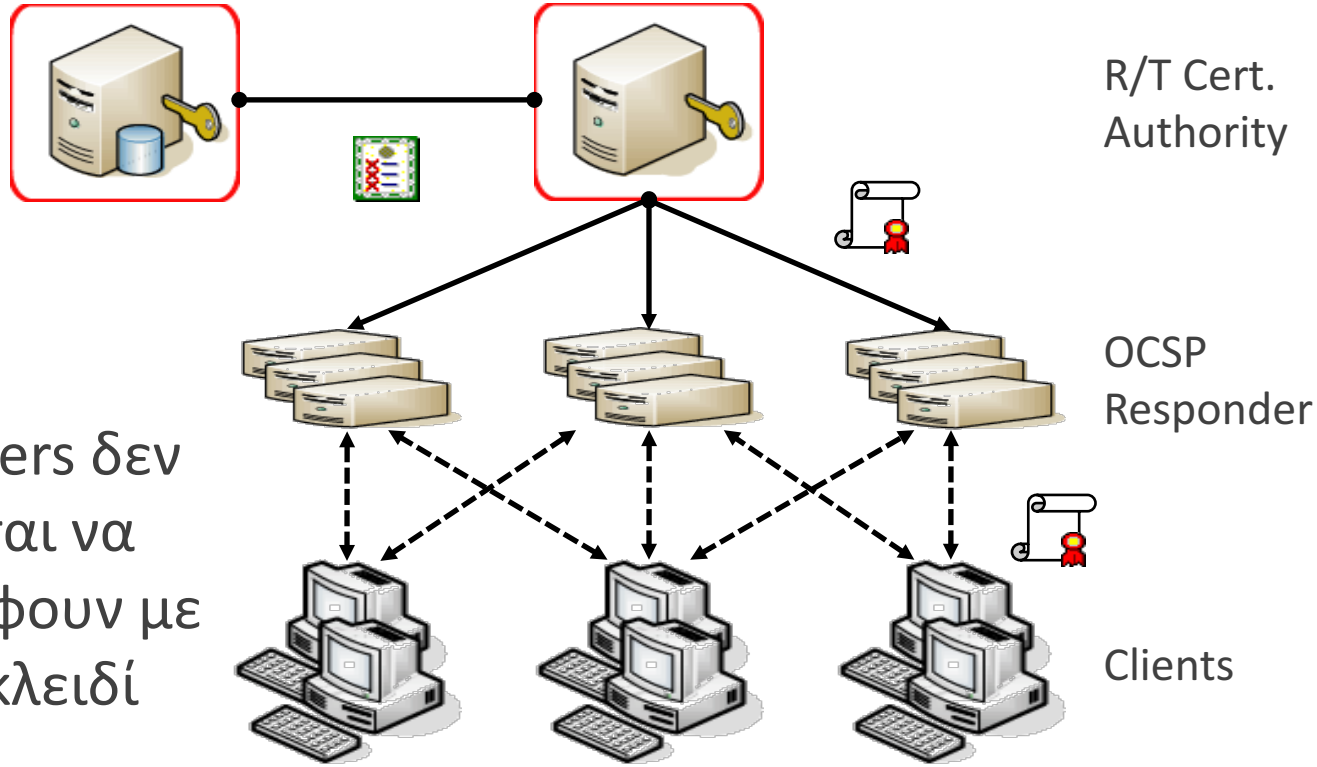


Ανάκληση πιστοποιητικών: OCSP

- Ανάγκη για ασφάλεια σε υποδομές
- Οι OCSP responders θα πρέπει να υπογράφουν με το ίδιο κλειδί

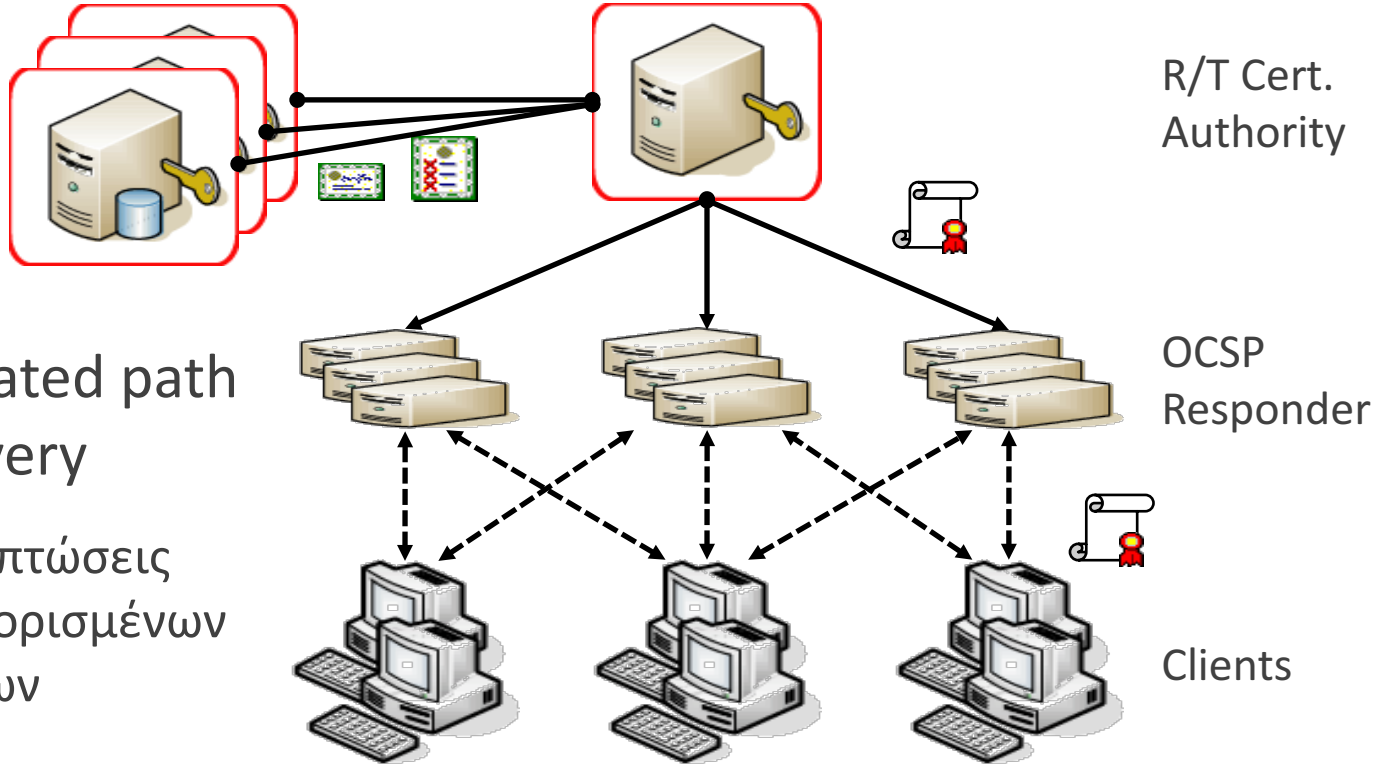


Ανάκληση πιστοποιητικών: OCSP



- Οι OCSP responders δεν χρειάζεται να υπογράφουν με κάποιο κλειδί

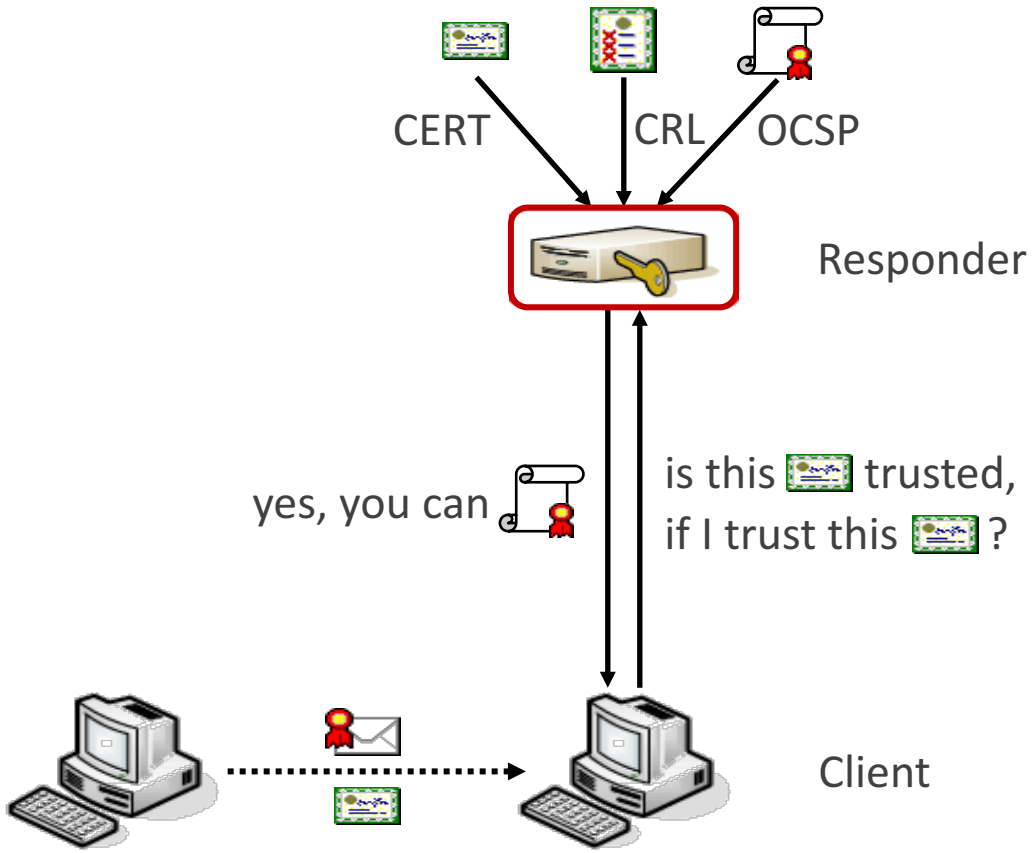
Ανάκληση πιστοποιητικών: DPD



- Delegated path discovery
  - Περιπτώσεις περιορισμένων πόρων

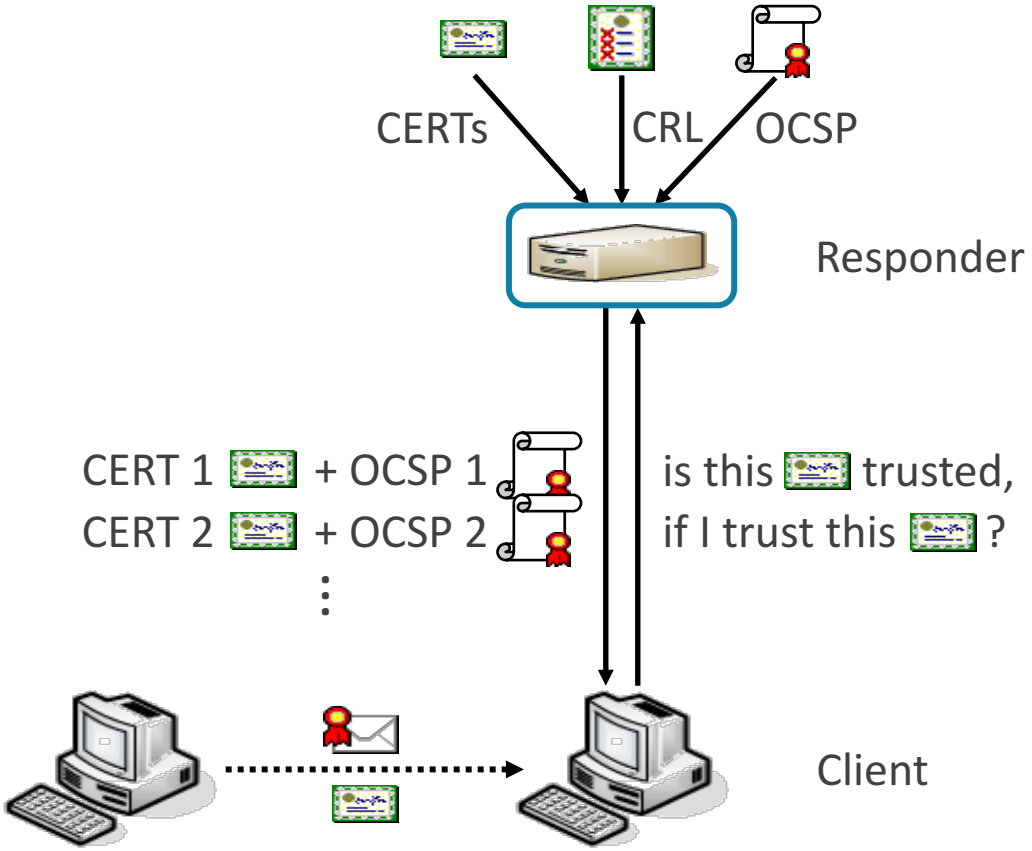
Ανάκληση πιστοποιητικών: DPV

- Delegated path validation
  - Περιπτώσεις περιορισμένων πόρων
- Εκδοχή 1η
  - Η απάντηση είναι ψηφιακά υπογεγραμμένη



Ανάκληση πιστοποιητικών: DPV

- Delegated path validation
  - Περιπτώσεις περιορισμένων πόρων
- Εκδοχή 2η
  - Μειωμένη ανάγκη για ασφάλεια
  - Επιστρέφει ότι ανακτήθηκε



Υποδομές δημοσίου κλειδιού

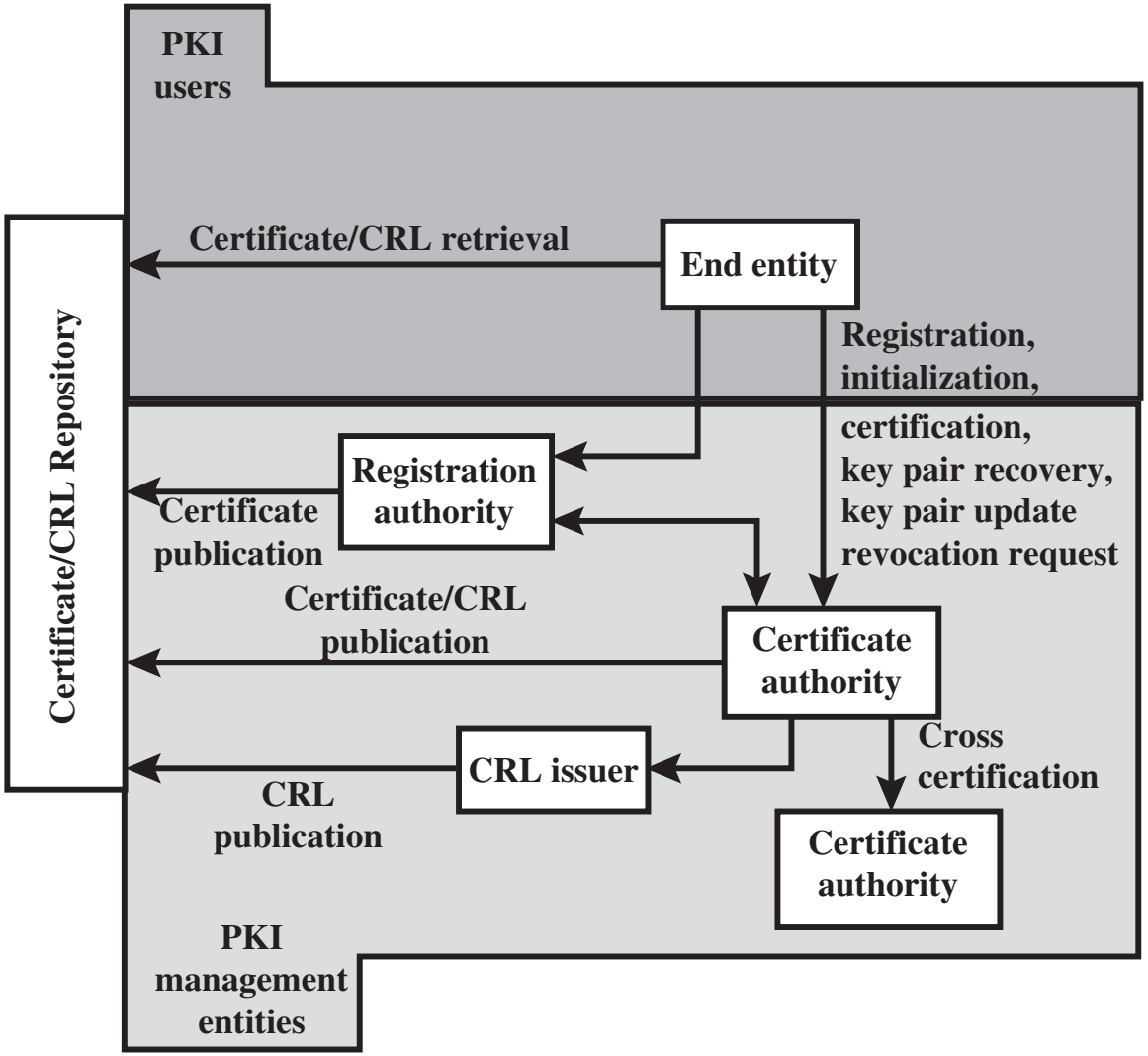
Υποδομές δημοσίου κλειδιού

- Ορισμός
  - Η ΥΔΚ είναι οι δομές αρχών πιστοποίησης οι οποίες επιτρέπουν την αξιοποίηση των δυνατοτήτων της κρυπτογραφίας δημοσίου κλειδιού
- Απαιτήσεις σχεδιασμού
  - μεγάλος βαθμός επεκτασιμότητας
  - δια–λειτουργικότητα ανεξάρτητων υποδομών
  - υποστήριξη πολλαπλών πολιτικών/εφαρμογών
  - απλουστευμένη διαχείριση κινδύνων

Υποδομές δημοσίου κλειδιού

- Βασικές απαιτήσεις χρηστών
  - Πρόληψη, προστασία, αποφυγή σφαλμάτων
  - Ανίχνευση και διόρθωση σφαλμάτων
  - Πρόληψη, προστασία, αποφυγή αμφισβητήσεων
  - Απόδοση αποζημιώσεων
  - Μηχανισμός διασφάλισης επιδόσεων
  - Παρακολούθηση χρηστών και υπηρεσιών

Υποδομές δημοσίου κλειδιού: PKIX



PKIX: διαχείριση πιστοποιητικών

- Δημιουργία πιστοποιητικού
  - Μετά από από αίτηση της RA
- Αποθήκευση και ανάκτηση πιστοποιητικού
  - Διατήρηση αντιγράφου
  - Διανομή πιστοποιητικού
- Ανάκληση πιστοποιητικού
  - Λήξη περιόδου ισχύος
  - Διακύβευση ιδιωτικού κλειδιού

PKIX: διαχείριση πιστοποιητικών

- Δήλωση πρακτικών πιστοποίησης
  - Η εξακρίβωση της εγκυρότητας των στοιχείων που αναγράφονται στο πιστοποιητικό γίνεται από την “αρχή εγγραφής” (πιστοποιητικά κλάσης A, B, και C)
  - Όλες οι λειτουργίες γίνονται βάση της “δήλωσης πρακτικών πιστοποίησης” που διατηρεί στην κατοχή της ο πάροχος υπηρεσιών πιστοποίησης
  - Η “δήλωση πρακτικών πιστοποίησης” συντάσσεται από την “αρχή δημιουργίας πολιτικών” και εγκρίνεται από την “αρχή έγκρισης πολιτικών”

PKIX: διαχείριση πιστοποιητικών

- Have several well-known CA's
  - Verisign one of most widely used
- Verisign issues several types of Digital IDs
  - Increasing levels of checks & hence trust

Class	Identity checks	Usage
1	name/email check	web browsing/email
2	+ enroll/address check	email, subs, software validate
3	+ ID documents	e-banking/service access

Κλάσεις πιστοποιητικών VeriSign

IA = Issuing Authority

CA = Certification Authority

PCA = VeriSign public primary certification authority

PIN = Personal Identification Number

LRAA = Local Registration Authority Administrator

	Class 1	Class 2	Class 3
Summary of Confirmation of Identity	Automated unambiguous name and e-mail address search.	Same as Class 1, plus automated enrollment information check and automated address check.	Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check for individuals; business records (or filings) for organizations.
IA Private Key Protection	PCA: trustworthy hardware; CA: trust-worthy software or trustworthy hardware.	PCA and CA: trustworthy hardware.	PCA and CA: trustworthy hardware.
Certificate Applicant and Subscriber Private Key Protection	Encryption software (PIN protected) recommended but not required.	Encryption software (PIN protected) required.	Encryption software (PIN protected) required; hardware token recommended but not required.
Applications Implemented or Contemplated by Users	Web-browsing and certain e-mail usage.	Individual and intra- and inter-company e-mail, online subscriptions, password replacement, and software validation.	E-banking, corp. database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation; authentication of LRAAs; and strong encryption for certain servers.

PKIX: διαχείριση πιστοποιητικών

- IETF PKIX
  - Part I: Certificate and CRL Profiles
  - Part III: Cert. Mgmt. Protocols
  - Part IV: Certificate Policy and Certification Practices
- Υπάρχουν όμως κι άλλα πρωτόκολλα, π.χ.
  - ANSI X9.55 και X9.57
  - PKCS #10 cert. request
  - S/MIME cert. request
  - Cisco certificate mgmt.

PKIX: διαχείριση πιστοποιητικών

- Ενδεικτικό λογισμικό για την υλοποίηση ΥΔΚ
  - OpenSSL (https://www.openssl.org/)
  - TinyCA (https://tinyca.alioth.debian.org/)
  - OpenCA PKI (https://www.openca.org/)
  - EJBCA (https://www.ejbca.org/)
  - gnoMint CA (http://gnomint.sourceforge.net/)
  - Universal SSL (https://blog.cloudflare.com/)
  - Dogtag (http://pki.fedoraproject.org/)

PKIX: διαχείριση κλειδιών

- Δημιουργία ζεύγους κλειδιών
- Αντιστοίχιση ζεύγους κλειδιών και οντότητας
- Αποθήκευση κλειδιού
- Διανομή κλειδιών
- Ανάκτηση ζεύγους κλειδιών
- Ενημέρωση κλειδιού

PKIX: διαχείριση κλειδιών

- Μηχανισμοί εφεδρείας (back–up)
- Μηχανισμοί ανάκτησης κλειδιών (key recovery)
  - ενθυλάκωσης κλειδιών (key encapsulation)
  - αναπαραγωγής κλειδιών (key derivation)
  - εγγύησης κλειδιών (key escrow)

PKIX: διαχείριση κλειδιών

- Για να ικανοποιούνται τα αιτήματα επιβολής του νόμου πρέπει:
  - Διεθνής η υιοθέτηση των συστημάτων ανάνηψης κλειδιών
  - Πρόσβαση κυβερνητικών υπηρεσιών χωρίς τη συγκατάθεση και τη γνώση του κατόχου του κλειδιού
  - Πρόσβαση στη μη–κρυπτογραφημένη πληροφορία, επί 24ώρη βάση, κάτω από οποιαδήποτε συνθήκη
  - Πρόσβαση τόσο σε κρυπτογραφημένες επικοινωνίες όσο και σε αποθηκευμένες (κρυπτογραφημένες) πληροφορίες

PKIX: διαχείριση κλειδιών

- Τα συστήματα ανάκτησης δεδομένων/κλειδιών είναι:
  - Λιγότερο ασφαλή
  - Πιο δύσκολα στη χρήση
  - Πιο δαπανηρά
- Άλλα προβλήματα:
  - Έλλειψη κυριαρχίας στον τρόπο αποκρυπτογράφησης των δεδομένων
  - Καταπάτηση των θεμελιωδών αρχών της ελευθερίας και της ιδιωτικότητας

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017.
- H. Bidgoli
  Handbook of Information Security
  Vol. 1, John Wiley & Sons, 2006
- S. Choudhury, K. Bhatnagar, and W. Haque
  Public Key Infrastructure: Implementation and Design
  M&T Pubs, 2002.