ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2015-2016

Μαρκάκης Ευάγγελος
markakis@aueb.gr

Ντούσκας Θεόδωρος
tntouskas@aueb.gr

Υπηρεσίες Ασφάλειας με χρήση Κρυπτογραφίας

- **Δασφάλιση Εμπιστευτικότητας (Confidentiality) Μηνύματος**
  - Συμμετρική Κρυπτογράφηση (AES, DES RC4 ..)
  - Ασύμετρη Κρυπτογράφηση (RSA, ElGamal…)
- **Διασφάλιση Ακεραιότητας (Integrity) Μηνύματος**
  - Συναρτήσεις κατακερματισμού (MD5, SHA-1, SHA-2)
  - Συναρτήσεις κατακερματισμού με κλειδί
  - Ψηφιακές Υπογραφές
- **Διασφάλιση Μη Αποποίησης (non-repudiation)**
  - Ψηφιακές Υπογραφές

  - **Προϋπόθεση η διαχείριση των κρυπτογραφικών κλειδιών**

Key Management Definition

- Διαχείριση Κλειδιών (Key Management): είναι ένα σύνολο από κανόνες, τεχνικές και διαδικασίες για την υποστήριξη της δημιουργίας και συντήρησης της επικοινωνίας κλειδιών μεταξύ authorized parties
- Οι τεχνικές αυτές πρέπει να είναι σε θέση να υποστηριζουν:
  - ✓ Την εγκαθίδρυση ενός συστήματος σε ένα συγκεκριμένο domain
  - ✓ Την δημιουργία, διανομή και εγκατάσταση των κρυπτογραφικών κλειδιών
  - ✓ Την διαχείριση της λειτουργίας -χρήσης των κλειδιών
  - ✓ Ανανέωση, ανάκληση και καταστροφή των κλειδιών
  - ✓ Αποθήκευση, backup/recovery και αρχειοθέτηση των κλειδιών

Διαχείριση Κρυπτογραφικών Κλειδιών

- Ασφαλής Δημιουργία κλειδιών
- Πιστοποίηση κλειδιών
- Αποθήκευση κλειδιών
- Αναζήτηση κλειδιών
- Ανταλλαγή – Διανομή κλειδιών μεταξύ των οντοτήτων
- Ανανέωση κλειδιών
- Καταστροφή κλειδιών
- Αρχειοθέτηση κλειδιών

Key management Objectives, Threats and Policy

- Οι στόχοι της διαχείρισης κλειδιών είναι να συντηρήσουν όλες τις προηγούμενες υπηρεσίες ώστε να προστατευτούν από:
  - ✓ Απώλεια εμπιστευτικότητας των μυστικών κλειδιών
  - ✓ Απώλεια της αυθεντικότητας των δημόσιων κλειδιών
  - ✓ Μη εξουσιοδοτημένη χρήση των δημόσιων κλειδιών

Πολιτική Διαχείρισης Κλειδιών

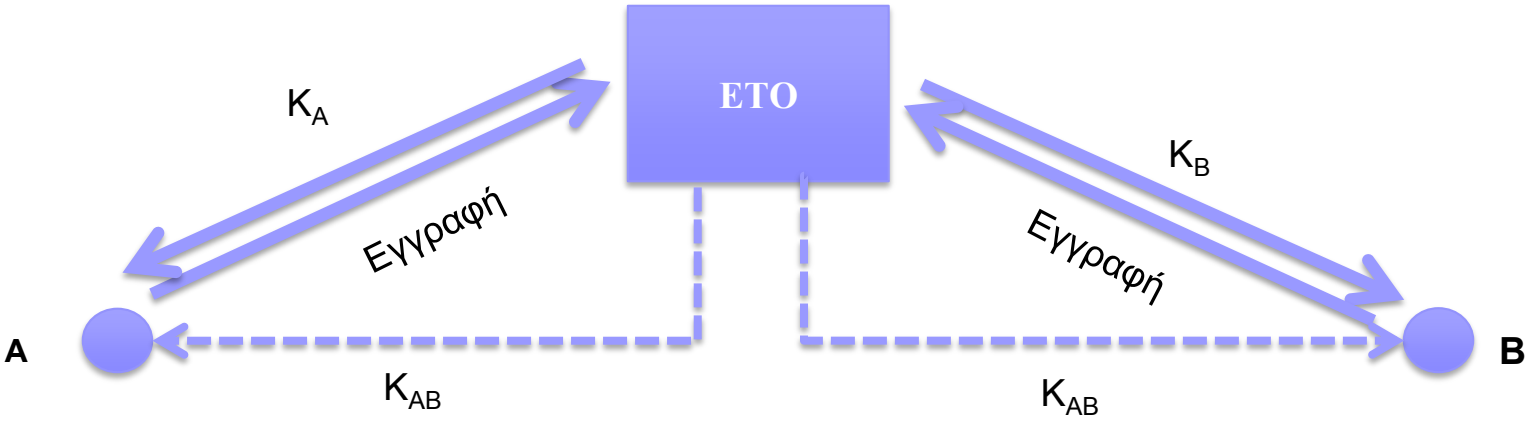
- Θα πρέπει να υπάρχει συγκεκριμένη πολίτική και διαδικασίες οι οποίες θα περιλαμβάνουν:
  - ✓ Συγκεκριμένους κανόνες
  - ✓ Συγκεκριμένα βήματα
  - ✓ Ρόλους και αρμοδιότητες
  - ✓ Records
- Είναι πλέον συγκεκριμένη απαίτηση του ISO 27001:2013
  - ✓ A.10.1.1 Policy on the use of cryptographic controls: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
  - ✓ A.10.1.2 Key management: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

Προβλήματα διαχείρισης συμμετρικών κλειδιών

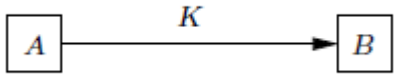
- **Ανταλλαγή κλειδιών**
  - ✓ Η ανταλλαγή απαιτεί ένα ασφαλές κανάλι
    - Εμπιστευτικότητα, ακεραιότητα επικοινωνίας
    - Αυθεντικότητα αποστολέα – παραλήπτη
- **Αριθμός κλειδιών:** Έστω ένα σύστημα με **n** χρήστες
  - ✓ Κάθε ζεύγος χρηστών μοιράζεται **ένα** διαφορετικό κλειδί
  - ✓ Συνεπώς χρειάζονται **(n-1)** κλειδιά ανά χρήστη,
  - ✓ Συνολικά: **n × (n-1)/2** κλειδιά
- **Ανανέωση κλειδιών**

Πιθανή λύση

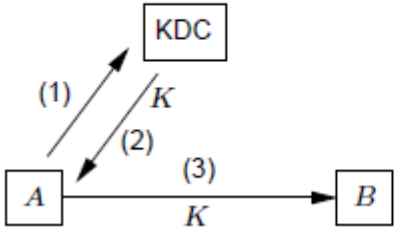
- Ύπαρξη ενός Κέντρου Διανομής Κλειδιών (Key Distribution Center - KDC) η οποία λειτουργεί ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ)
- Αν ο **Α** θέλει να επικοινωνήσει με τον **Β** τότε πρέπει να επικοινωνήσει μέσω του ΚΔΚ. Η ΕΤΟ δημιουργεί και στέλνει και στους δύο χρήστες το κοινό κλειδί

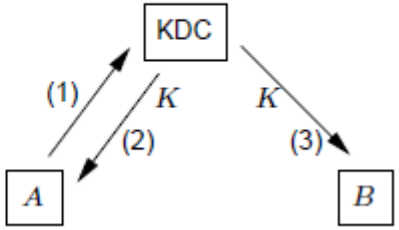


- Point-to-point key distribution: άμεση επικοινωνία

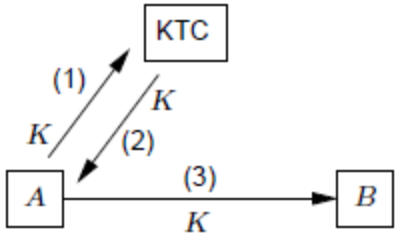


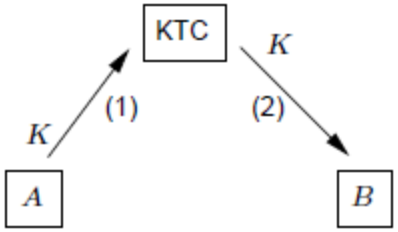
- *kev distribution centers* (KDCs)





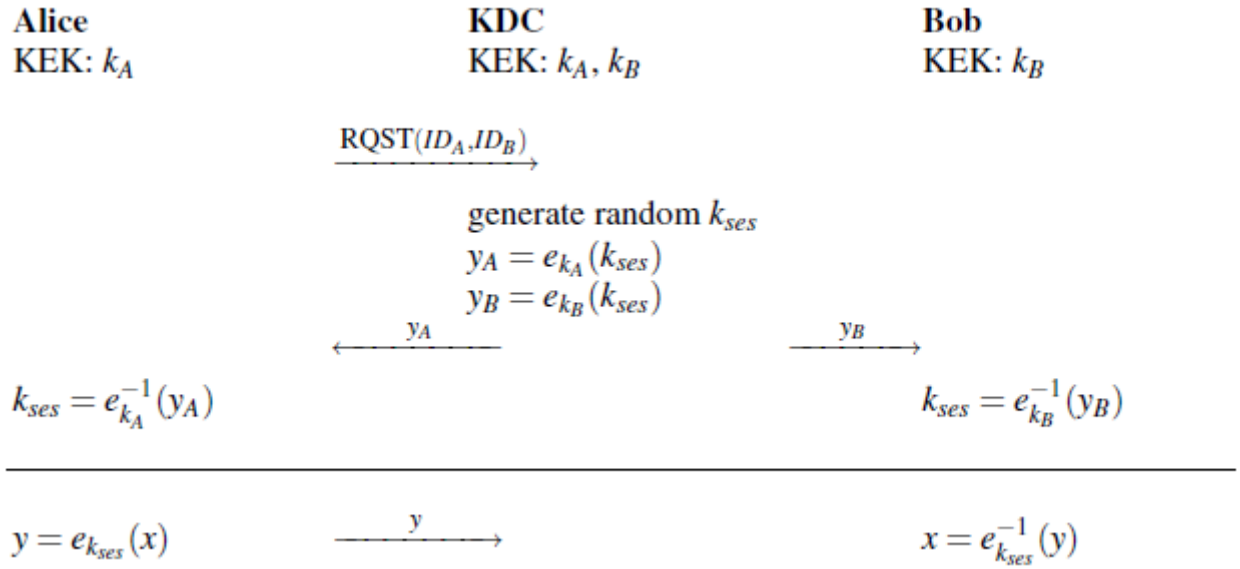
- Key translation center (KTC)





Βασικός τρόπος λειτουργίας KDC

- Κάθε χρήστης U πρέπει να μοιραστεί ένα Key Encryption Key (KEK) Ku με το KDC
- Το K_A, K_B είναι long term keys, ενώ το K_{ses} θα πρέπει να αλλάζει συνεχώς



Προβλήματα ETO στην συμμετρική κρυπτογράφηση

- Συνεχής διαθεσιμότητα ETO
- Single point of failure: Αν κάποιος επιτεθεί στην ETO τότε μπορεί να προσποιηθεί οποιονδήποτε χρήστη
- Η ETO μπορεί να προσποιηθεί ότι είναι οποιασδήποτε χρήστης

- **Replay Attack:** δεν γνωρίζει κανένας από τους χρήστες αν το συγκεκριμένο encrypted session είναι καινούριο.
- **Key Confirmation Attack:** δεν είναι εύκολο να διασφαλιστεί η αυθεντικότητα του Session

Προβλήματα Διαχείρισης Δημόσιων Κλειδιών

- Κάθε χρήστης έχει μόνο **ενα ζεύγος** κλειδιών
  - ✓ Χρειάζονται **2** κλειδιά ανά χρήστη (ένα δημόσιο και ένα ιδωτικό)
  - ✓ Για **n** χρήστες χρειαζόμαστε **2n** κλειδιά
- Ανταλλαγή κλειδιών
  - ✓ Δεν χρειάζεται εμπιστευτικότητα κατά την μεταφορά των κλειδιών, καθώς η όλη διαδικασία της κρυπτογράφησης γίνεται με την χρήση του Δημόσιου Κλειδιού του παραλήπτη – τοοποίο είναι γνωστό!
  - ✓ Απατείται επαλήθευση της αυθεντικότητας του αποστολέα και του παραλήπτη. Οτι το συγκεκριμένο δημόσιο κλειδί ανήκει όντως στην συγκεκριμένη οντότητα

Απαιτήσεις

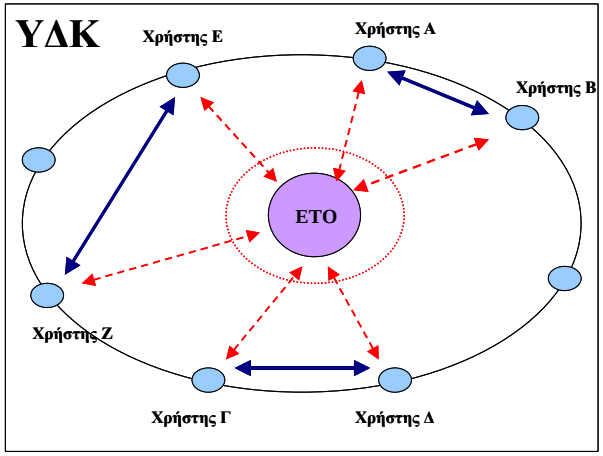
- Για την απρόσκοπτη λειτουργία των κρυπτοσυστημάτων δημόσιου κλειδιού απαιτείται για κάθε ζεύγος ιδιωτικού – δημόσιου κλειδιού:
  - ✓ Ασφαλής δημιουργία και διαφύλαξη του ιδιωτικού κλειδιού, έτσι ώστε να μην έχει πρόσβαση σε αυτό κανείς άλλος εκτός του κατόχου του. Κάτι τέτοιο μπορεί να επιτευχθεί με την αποθήκευση του ιδιωτικού κλειδιού σε ασφαλή «ιδιωτικά» μέσα (π.χ. έξυπνες κάρτες).
  - ✓ Πιστοποίηση του τρόπου δημιουργίας και εγκυρότητας του δημόσιου κλειδιού, έτσι ώστε να εξασφαλίζεται πως το τελευταίο ταυτίζεται πραγματικά με το κάτοχο του (προς αποφυγή πλαστοπροσωπίας).

Πιθανή Λύση

- Χρήση μίας **Έμπιστης Τρίτης Οντότητας - ΕΤΟ** (Trusted Third Party – TTP) η οποία αυθεντικοποιεί τα δημόσια κλειδιά όλων των χρηστών
- Κάθε χρήστης αρκεί να γνωρίζει το δημόσιο κλειδί της ΕΟ PKTTP ώστε να επαληθεύσει το δημόσιο κλειδί οποιουδήποτε άλλου χρήστη της ΕΤΟ.
  - ✓ Ο χρήστης Χ στέλνει το δημόσιο κλειδί του στην ΕΤΟ
  - ✓ Η ΕΤΟ υπογράφει ψηφιακά ένα μήνυμα το οποίο περιλαμβάνει
    - Την ταυτότητα (ένα μοναδικό προσδιοριστικό) του χρήστη Χ
    - Το δημόσιο κλειδί του χρήστη Χ
    - Την ημερομηνία της υπογραφής και της λήξης
    - Όλα τα παραπάνω υπογράφονται με το ιδωτικό κλειδί της ΕΤΟ

Έμπιστη Τρίτη Οντότητα (ΕΤΟ)

Ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ) ορίζεται «*μια αρχή ασφαλείας ή ο αντιπρόσωπος της, η οποία θεωρείται έμπιστη από τους χρήστες με σκοπό τη παροχή δράσεων σχετικών με ασφάλεια, όπως π.χ. την υποστήριξη της χρήσης ψηφιακών υπογραφών και την εμπιστευτικότητα των υπηρεσιών*».



Χρόνος λειτουργίας Έμπιστων Τρίτων Οντοτήτων

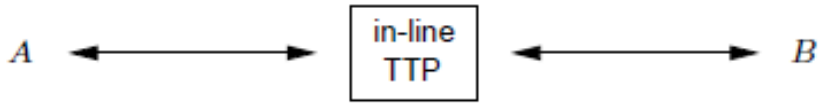
- Ως «χρόνος λειτουργίας» μίας ΕΤΟ εννοείται η *χρονική στιγμή* κατά την οποία απαιτείται η παρέμβαση - λειτουργία της τελευταίας στις ηλεκτρονικές συναλλαγές των χρηστών.
  - ✓ *Λειτουργία πριν τις συναλλαγές*: η ΕΤΟ δημιουργεί ή/και αποδίδει ιδιότητες και μέσα στους χρήστες που είναι απαραίτητες προϋποθέσεις για τη πραγματοποίηση των συναλλαγών (όπως π.χ. η έκδοση κλειδιών και πιστοποιητικών).
  - ✓ *Λειτουργία κατά τη διάρκεια των συναλλαγών*: η ΕΤΟ παρεμβαίνει στις συναλλαγές (μετά από κλήση των χρηστών ή αυτόματα) με σκοπό την πιστοποίηση και εξακρίβωση στοιχείων των τελευταίων.
  - ✓ *Λειτουργία μετά τη συναλλαγή*: η ΕΤΟ καλείται να επιλύσει τυχόν διαφωνίες και προβλήματα που προέκυψαν λόγω αποτυχίας ολοκλήρωσης μιας συναλλαγής.

Θέσεις λειτουργίας Έμπιστων Τρίτων Οντοτήτων

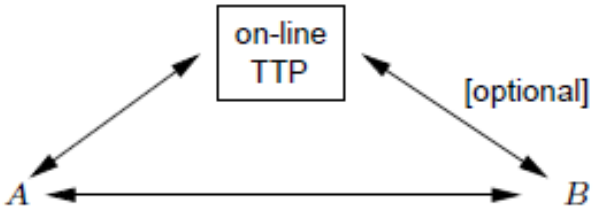
- Ως «θέση λειτουργίας» μίας ΕΤΟ εννοείται *ο τρόπος* με τον οποίο παρεμβάλλεται η ΕΤΟ κατά τις ηλεκτρονικές συναλλαγές των χρηστών
- Οι τρόποι είναι οι ακόλουθοι:
  - ✓ *«Άμεσες» υπηρεσίες ΕΤΟ*: η ΕΤΟ παρεμβάλλεται άμεσα στη διαδρομή επικοινωνίας των συναλλασσόμενων μερών, ή αλλιώς αποτελεί υποχρεωτικό μέρος αυτής της επικοινωνίας.
  - ✓ *«Έμμεσες» υπηρεσίες ΕΤΟ*: η ΕΤΟ παρεμβάλλεται έμμεσα στη διαδρομή επικοινωνίας μετά από σχετική απαίτηση/κλήση ενός των δύο συναλλασσόμενων μερών.
  - ✓ *«Εκτός γραμμής» υπηρεσίες ΕΤΟ*: η ΕΤΟ δε παρεμβαίνει στις συναλλαγές και απλά παρέχει τα απαραίτητα μέσα για την ομαλή διεκπεραίωση τους.

Θέσεις λειτουργίας Έμπιστων Τρίτων Οντοτήτων

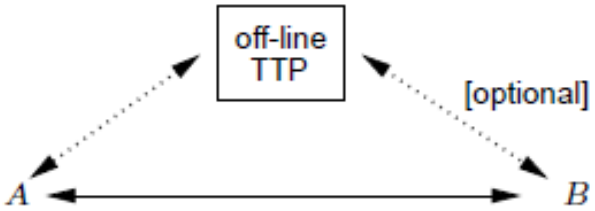
in-line



on-line



off-line



Υποδομή Δημόσιας Κλείδας

Μία **Υποδομή Δημόσιας Κλείδας (Public Key Infrastructure - PKI)** είναι:

- *«ένα σύστημα ψηφιακών πιστοποιητικών, Αρχών Πιστοποίησης και άλλων αρχών εγγραφής που επιβεβαιώνουν και αυθεντικοποιούν την ισχύ του κάθε εμπλεκόμενου μέρους σε μία δικτυακή συναλλαγή».*
- Υπόβαθρο ανάπτυξης κρυπτοσυστημάτων δημόσιου κλειδιού για τη παροχή μηχανισμών ασφαλείας (κρυπτογράφηση - ψηφιακή υπογραφή).
- Μια αρχή ασφαλείας (ή ο αντιπρόσωπος της) η οποία θεωρείται έμπιστη από τους χρήστες με σκοπό τη παροχή δράσεων σχετικών με ασφάλεια, όπως π.χ. την υποστήριξη της χρήσης ψηφιακών υπογραφών και την εμπιστευτικότητα των υπηρεσιών

- Για τη λειτουργία του συστήματος μιας ΥΔΚ είναι απαραίτητη η εμπλοκή μίας τουλάχιστον κοινά αποδεκτής οντότητας που θα αποτελεί το *κεντρικό σημείο εμπιστοσύνης* σε όλη την ΥΔΚ. Η οντότητα αυτή, που καλείται **Έμπιστη Τρίτη Οντότητα** (ΕΤΟ), είναι ουσιαστικά ο φορέας που εμπιστεύονται όλοι οι χρήστες κατά την είσοδο τους στην ΥΔΚ.

Υπηρεσίες Υποδομής Δημόσιας Κλείδας (ΥΔΚ)

- Υπηρεσία Εγγραφής (Registration)
- Υπηρεσία Διαχείρισης Κλειδιών (Key Management)
- Υπηρεσία Πιστοποίησης (Certification)
- Υπηρεσία Ανάκλησης (Revocation)
- Υπηρεσία Χρονοσφραγίδας (Time - stamping)
- Υπηρεσία Διαπιστοποίησης (Cross- certification)

Υπηρεσία Εγγραφής (Registration)

- Λαμβάνει χώρα κατά την είσοδο ενός καινούργιου χρήστη στην Υποδομή Δημόσιου Κλειδιού.
- Αναγνώριση και αυθεντικοποίηση του νέου χρήστη, έτσι ώστε να πραγματοποιηθεί η αξιόπιστη σύνδεση του με το δημόσιο κλειδί του.
- Εκτελείται από ειδική αρχή της ΥΔΚ που καλείται Αρχή Εγγραφής (Registration Authority - RA)

Υπηρεσία Διαχείρισης Κλειδιών (Key Management)

- Αναλαμβάνει την έκδοση και προσωποποίηση κάθε ζεύγους κλειδιών
  - ✓ Παρέχει στο χρήστη τη δυνατότητα να δημιουργήσει ο ίδιος το ζεύγος κλειδιών του
  - ✓ Τα ιδιωτικά κλειδιά πρέπει να διαφυλάσσονται σε ασφαλή μέσα, όπως έξυπνες κάρτες
- Επιτρέπει τη διανομή / ανταλλαγή / αναζήτηση των δημόσιων κλειδιών
- (Πιθανώς) διασφαλίζει την ανάκτηση των ιδιωτικών κλειδιών σε περίπτωση απώλειας

Υπηρεσία Πιστοποίησης (Certification)

- **Έκδοση ψηφιακού πιστοποιητικού** για το δημόσιο κλειδί κάθε χρήστη
- Διασφάλιση της ακεραιότητας για την κατάσταση των πιστοποιητικών αυτών μέσω αποτελεσματικής διαχείρισης
- Η εκτέλεση της υπηρεσίας πιστοποίησης γίνεται από ειδική αρχή της ΥΔΚ που καλείται Αρχή Πιστοποίησης (Certification Authority – CA)

Ψηφιακό Πιστοποιητικό (Digital Certificate)

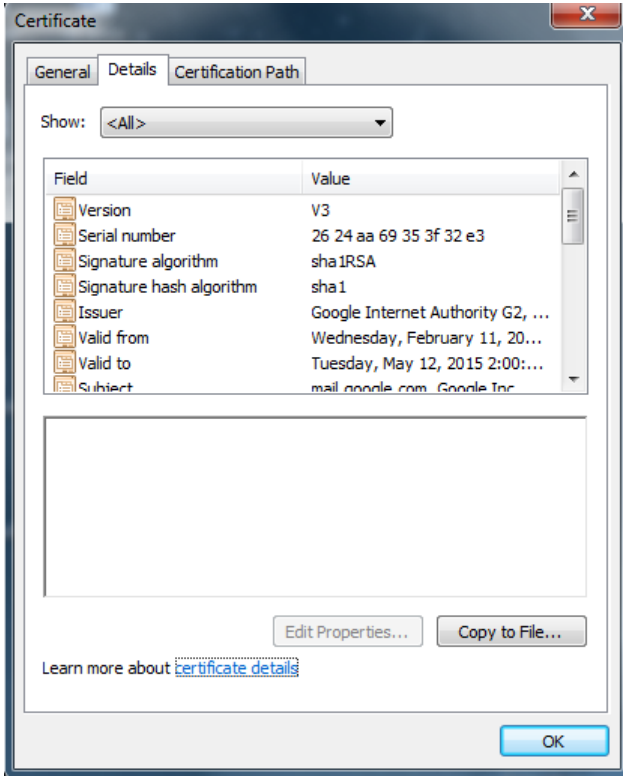
- Ψηφιακά υπογεγραμμένο αρχείο το οποίο περιλαμβάνει το δημόσιο κλειδί, την ταυτότητα και λοιπά στοιχεία ενός χρήστη και που διασφαλίζει τη σύνδεση μεταξύ του χρήστη και του δημόσιου κλειδιού του
- Είδη Πιστοποιητικών:
  - ✓ X.509 Public Key Certificates
  - ✓ Identity Certificates
  - ✓ S/MIME Certificates
  - ✓ Object Signing Certificates
  - ✓ SSL Certificates
  - ✓ Simple Public Key Infrastructure (SPKI) Certificates

Σκοπός Πιστοποιητικού

- Πιστοποιεί το δημόσιο κλειδί μιας οντότητας
- Κάθε χρήστης με πρόσβαση στο δημόσιο κλειδί της CA μπορεί να ανακτήσει το δημόσιο κλειδί του χρήστη με τον οποίο συναλλάσεται:
- Να κρυπτογραφήσει
- Να αυθεντικοποιηθεί
- Καμία οντότητα εκτός της CA δεν μπορεί να τροποποιήσει ένα πιστοποιητικό

Βασικά μέρη ενός πιστοποιητικού

- **Version**. The X.509 version number.
- **Serial number**. The unique serial number that the issuing certification authority (CA) assigns to the certificate. The serial number is unique for all certificates issued by a given CA.
- **Signature algorithm**. The hash algorithm that the CA uses to digitally sign the certificate.
- **Issuer**. Information regarding the CA that issued the certificate.
- **Valid from**. The beginning date for the period in which the certificate is valid.
- **Valid to**. The final date for the period in which the certificate is valid.
- **Subject**. The name of the individual, computer, device, or CA to whom the certificate is issued. If the issuing CA exists on a domain member server in your enterprise, this will be a distinguished name within the enterprise. Otherwise, this may be a full name and e-mail name or other personal identifier.
- **Public key**. The public key type and length associated with the certificate.
- **Thumbprint algorithm**. The hash algorithm that generates a digest of data (or thumbprint) for digital signatures.
- **Thumbprint**. The digest (or thumbprint) of the certificate data.
- **Friendly name**. (Optional) A display name to use instead of the name in the Subject field.
- **Enhanced key usage**. (Optional) The purposes for which this certificate can be used.



Αρχή Πιστοποίησης

- Έκδοση και ανανέωση πιστοποιητικών βάσει συγκεκριμένων προτύπων.
- Διανομή πιστοποιητικών στους χρήστες.
- Αποθήκευση πιστοποιητικών σε Υπηρεσία Καταλόγου (Directory Server) για κοινή χρήση.
- Ανάκληση πιστοποιητικών με έκδοση Λίστας ανάκλησης πιστοποιητικών (Certificate Revocation List – CRL), η οποία περιέχει όλα τα πιστοποιητικά που δεν ισχύουν ή που έχουν λήξει .

Αρχή Πιστοποίησης – Υπηρεσία Καταλόγου

- Υποστηρίζει μέσω κατάλληλου Εξυπηρετητή Καταλόγου (Directory Server) την αποθήκευση και διάθεση των εκδοθέντων πιστοποιητικών και δημόσιων κλειδιών
- Παραδείγματα Εξυπηρετητών Καταλόγων:
  - ✓ LDAP εξυπηρετητές
  - ✓ X.500 Directory System Agents (DSAs)
  - ✓ Domain Name System (DNS)
  - ✓ Web εξυπηρετητές
  - ✓ File Transfer Protocol (FTP) - εξυπηρετητές

Υπηρεσία Ανάκλησης (Revocation)

- Λίστα Ανάκλησης Πιστοποιητικών – Certificate Revocation Lists (CRLs)
- Οι CRLs είναι υπογεγραμμένες δομές δεδομένων που περιέχουν μια λίστα από πιστοποιητικά που έχουν ανακληθεί. Δηλαδή πιστοποιητικά που δεν είναι πλέον έγκυρα για λόγους ασφάλειας ή για άλλες αιτίες
- Η αξιοπιστία των CRL έγκειται στο ότι είναι ψηφιακά υπογεγραμμένες (συνήθως από τον εκδότη των πιστοποιητικών)

Υπηρεσία Ανάκλησης (Revocation)

- Λήξη πιστοποιητικού
- Τροποποίηση πιστοποιητικού (π.χ. αλλαγή ονόματος κλπ)
- Υποκλοπή πιστοποιητικού (είτε του χρήστη είτε της CA)

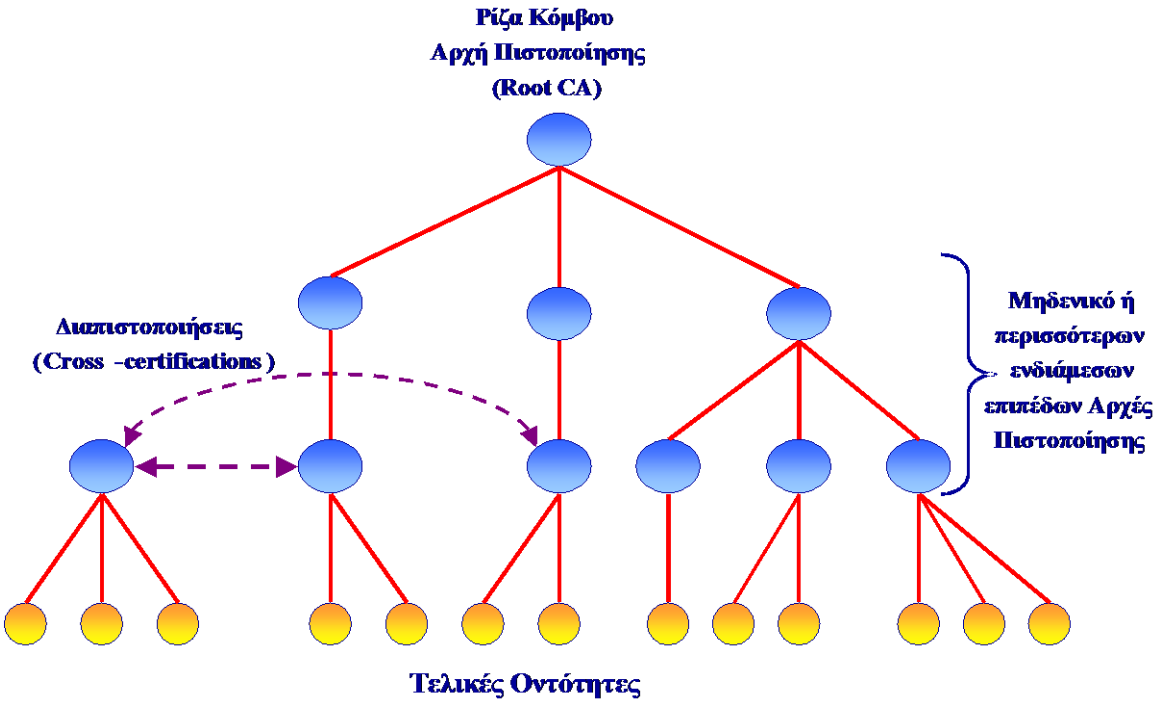
Υπηρεσία Χρονοσφράγισης (Time – stamping)

- Η υπηρεσία αυτή σχετίζεται με την “επικόλληση” ημερομηνίας και ώρας στα πιστοποιητικά.
- Αποδεικνύει ότι τα δημιουργήθηκαν ή απεστάλησαν σε μία συγκεκριμένη χρονική στιγμή.
- Η υπηρεσία εκτελείται από ειδική Αρχή Χρονικής Σφραγίδας (Time-Stamping service)

Υπηρεσία Διαπιστοποίησης (Cross- certification)

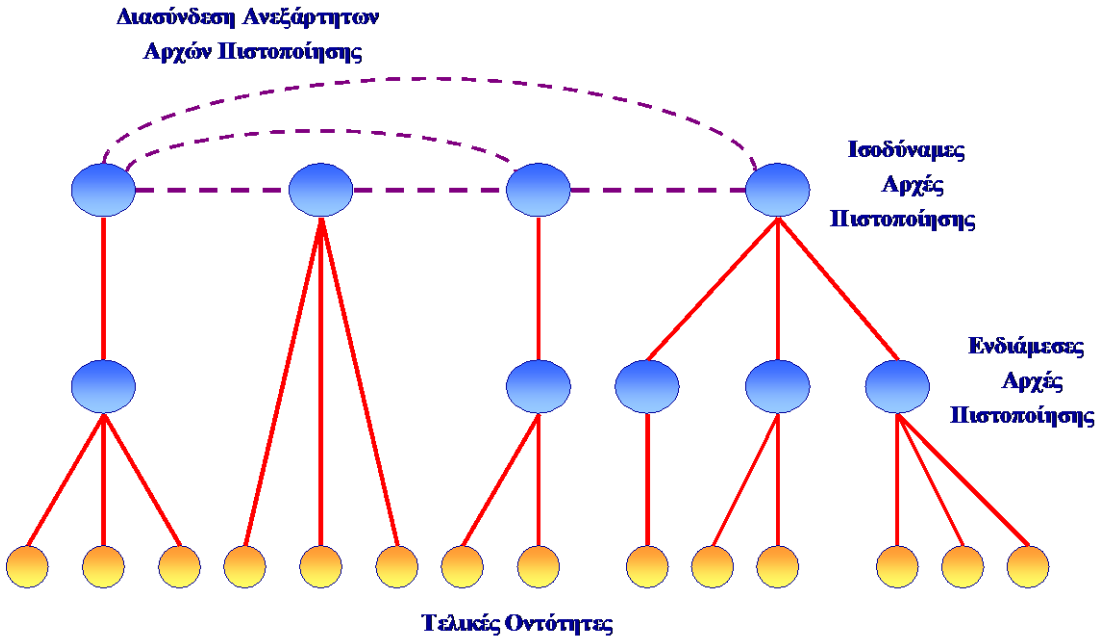
- Ως «δια-πιστοποιητικό» (cross-certificate) εννοείται το πιστοποιητικό που εκδίδεται από μία Αρχή Πιστοποίησης Α σε μία άλλη Αρχή Πιστοποίησης Β και εκφράζει την εμπιστοσύνη της **Α** ως προς τη **Β**.
- Η κάθε Αρχή Πιστοποίησης υπογάφει το πιστοποιητικό της άλλης Αρχής Πιστοποίησης
- Οι χρηστες που ανήκουν στην Αρχή Πιστοποίησης **Α** μπορούν να επικοινωνήσουν μεταξύ τους για γνωρίζουν το κλειδί της αρχής πιστοποίησης **Α**
- Οι χρηστες που ανήκουν στην Αρχή Πιστοποίησης **Β** μπορούν να επικοινωνήσουν μεταξύ τους για γνωρίζουν το κλειδί της αρχής πιστοποίησης **Β**

Αυστηρά Ιεραρχικό Μοντέλο Εμπιστοσύνης



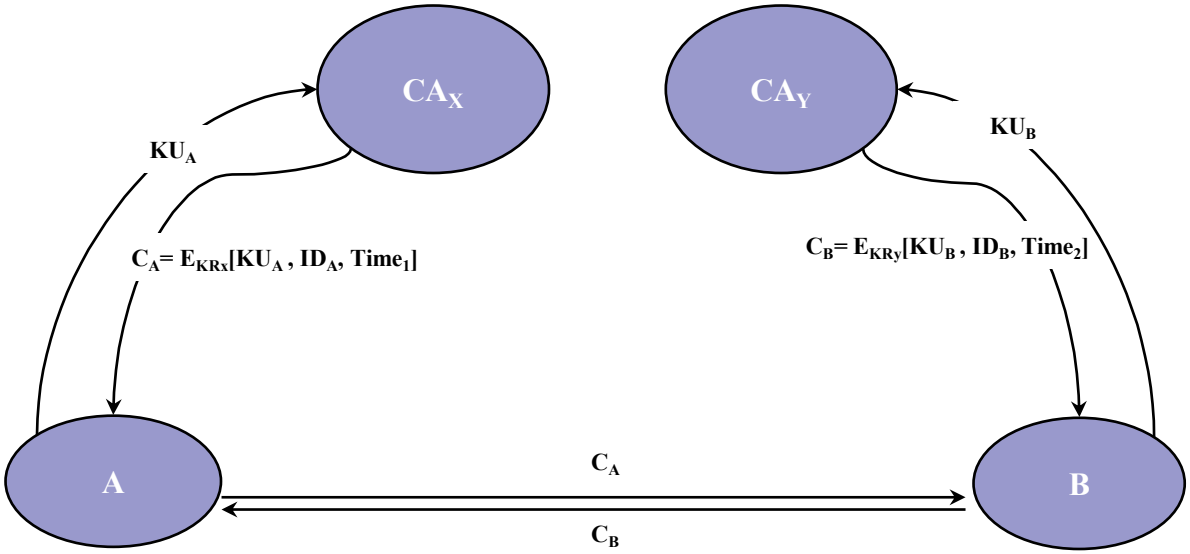
Πηγή: Δ. Πολέμη, Χ., Α. Καλιαντζόγλου, «Πρακτικά Θέματα Ασφάλειας Πληροφοριακών Συστημάτων Και Εφαρμογών», 2008

Κατανεμημένο Μοντέλο Εμπιστοσύνης



Πηγή: Δ. Πολέμη, Χ., Α. Καλιαντζόγλου, «Πρακτικά Θέματα Ασφάλειας Πληροφοριακών Συστημάτων Και Εφαρμογών», 2008

Διαπιστοποίηση



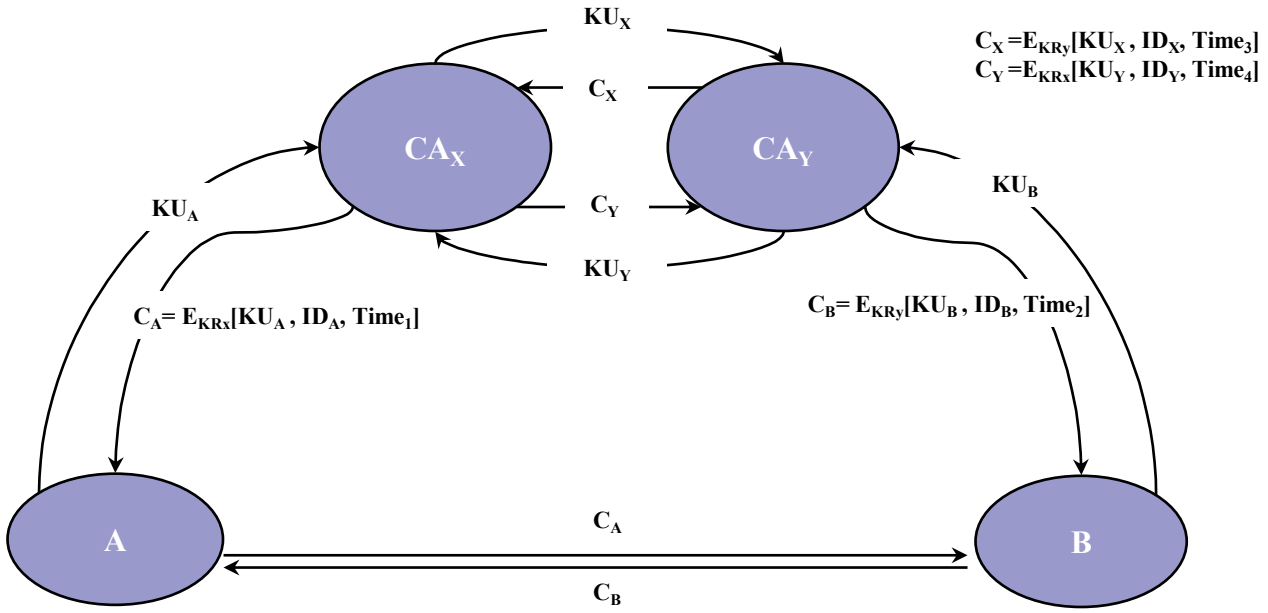
Α ανάκτησε certificate από CA X.

Β ανάκτησε certificate από CA Y.

Αν ο Α «δεν γνωρίζει» το public key της Y, του είναι άχρηστο το certificate του Β.

Αν ο Β «δεν γνωρίζει» το public key της X, του είναι άχρηστο το certificate του Α.

Διαπιστοποίηση



Δια-πιστοποίηση CAs

Οι CAs ανταλλάσσουν τα public keys τους

Κάθε CA πιστοποιεί το public key της άλλης CA

Ο Α γνωρίζει το public key του X

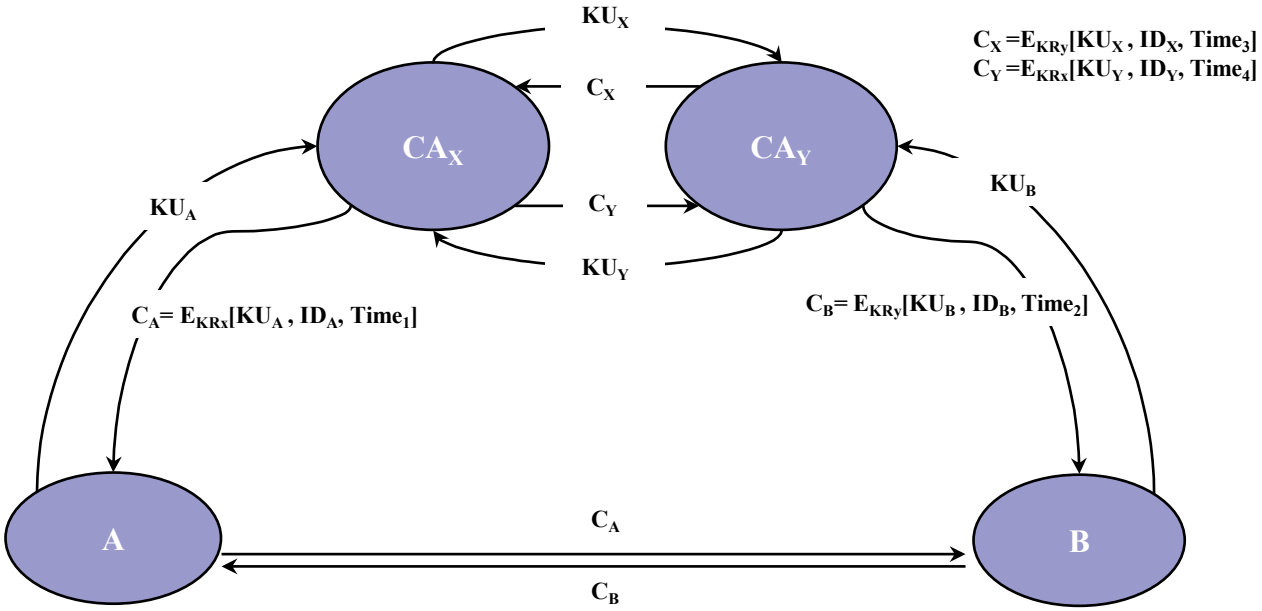
Ο Α μπορεί να ανακτήσει το certificate του Y (C_Y) signed by X

Ο Α μπορεί να ανακτήσει το δημόσιο κλειδί του Y που περιέχεται στο πιστοποιητικό C_Y

Ο Α διαθέτει το πιστοποιητικό του Β (C_B, issued by Y)

Άρα μπορεί να ανακτήσει το δημόσιο κλειδί του Β.

Διαπιστοποίηση



Σενάριο: Ο Α πρέπει να κρυπτογραφήσει μήνυμα Μ προς Β .....

$D_{KUx}[C_Y] \rightarrow D_{KUx}[E_{KRx}[[KU_Y, ID_Y, Time_4]] \rightarrow \mathbf{KU_Y}, ID_Y, Time_4$

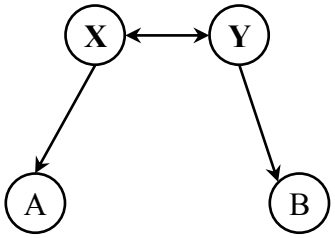
$D_{KUy}[C_B] \rightarrow D_{KUy}[E_{KRy}[[KU_B, ID_B, Time_2]] \rightarrow \mathbf{KU_B}, ID_B, Time_2$

$C = M^{KU_B} \bmod n$

Διαπιστοποίηση

- Στην περίπτωση ανάμειξης πολλαπλών CAs η οντότητα που θέλει να επικυρώσει την εγκυρότητα μιας ψηφιακής υπογραφής επιθυμεί την απόκτηση ενός αυθεντικοποιημένου δημοσίου κλειδιού επικυρωμένου μέσω ενός πιστοποιητικού υπογεγραμμένου από μία CA διαφορετική από αυτή που έχει αρχικά συμβληθεί
- Έτσι μια αλυσίδα από πιστοποιητικά (certificate chain) θα πρέπει να παρασχεθεί στην οντότητα που επιθυμεί επικύρωση δημόσιου κλειδιού.
- Η αλυσίδα αντιστοιχεί σε ένα μονοπάτι εμπιστοσύνης που ξεκινά από την CA με την οποία η οντότητα έχει αρχικά συμβληθεί και καταλήγει στο δημόσιο κλειδί του οποίου η εγκυρότητα πρέπει να επικυρωθεί
- Στόχος: ανεύρεση ενός κατευθυντικού μονοπατιού που ξεκινά από τον κόμβο που αντιστοιχεί στην CA την οποία η οντότητα εμπιστεύεται a priori και καταλήγει στην CA που έχει υπογράψει το πιστοποιητικό που περιλαμβάνει το δημόσιο κλειδί του οποίου η εγκυρότητα επιζητάτε να επικυρωθεί

Διμερής Διαπιστοποίηση



X<<A>>: το πιστοποιητικό του Α που εκδίδεται από τη CA X

Y<<B>>: το πιστοποιητικό του Β που εκδίδεται από τη CA Y

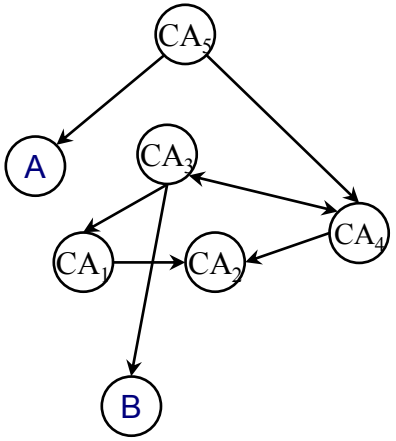
Ο χρήστης Α (ή Β) μπορεί να χρησιμοποιήσει μία αλυσίδα δια-πιστοποίησης για να ανακτήσει το δημόσιο κλειδί του Β (ή Α).

Σημειογραφικά:

- ✓ Α δημόσιο κλειδί του Β X<<Y>>Y<<B>>
- ✓ Β δημόσιο κλειδί του Α Y<<X>>X<<A>>

Αλυσίδα πιστοποίησης

Κατανεμημένη - Διαπιστοποίηση



Οντότητα Α, κάτοχος πιστοποιητικού με KU_A (έχει εκδοθεί από CA_5)

Οντότητα Β, κάτοχος πιστοποιητικού με KU_B (έχει εκδοθεί από CA_3)

Η Β στέλνει στην Α ένα ψηφιακά υπογεγραμμένο μήνυμα !!!

Η Α επιθυμεί να αποκτήσει εμπιστοσύνη στο δημόσιο κλειδί KU_B της οντότητας Β

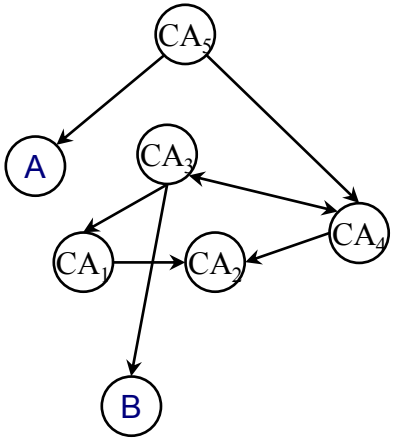
Το κατευθυνόμενο μονοπάτι $\{CA_5, CA_4, CA_3\}$ υπάρχει

Η αλυσίδα $CA_5<<CA_4>>CA_4<<CA_3>>$ και η εμπιστοσύνη στην CA_5 αρκεί για την Α:

- Η Α χρησιμοποιεί το KU_5 και εξάγει επικυρωμένο αντίγραφο του KU_4 από $CA_5<<CA_4>>$
- Η Α χρησιμοποιεί το KU_4 και εξάγει επικυρωμένο αντίγραφο του KU_3 από $CA_4<<CA_3>>$
- Η Α χρησιμοποιεί το KU_3 για να επικυρώσει την αυθεντικότητα του πιστοποιητικού που περιέχει το KU_B

* Αναφέρεται και mesh-organized. Στο «*Ασφάλεια Δικτύων Υπολογιστών», Σ. Γκρίτζαλης, Σ. Κάτσικας, Δ. Γκρίτζαλης,* αναφέρεται ως μοντέλο εμπιστοσύνης προσανατολισμένου γράφου. Το παράδειγμα είναι από το σύγγραμμα, κεφ. 3.8.2

Κατανεμημένη - Διαπιστοποίηση



(–) Δυσκολία στην ανεύρεση αλυσίδων για large scale δίκτυα εμπιστοσύνης

(–) Προβλήματα τύπου ΠΠΠ

(–) Εναλλακτικά το σχήμα όλοι με όλους (Full Mesh topology) πλεονάζει σε δια-πιστοποιήσεις

Fully distributed → PGP: Web of Trust

Η εμπιστοσύνη κτίζεται εξ-αρχής

Καμία public key authority, ή Root CA

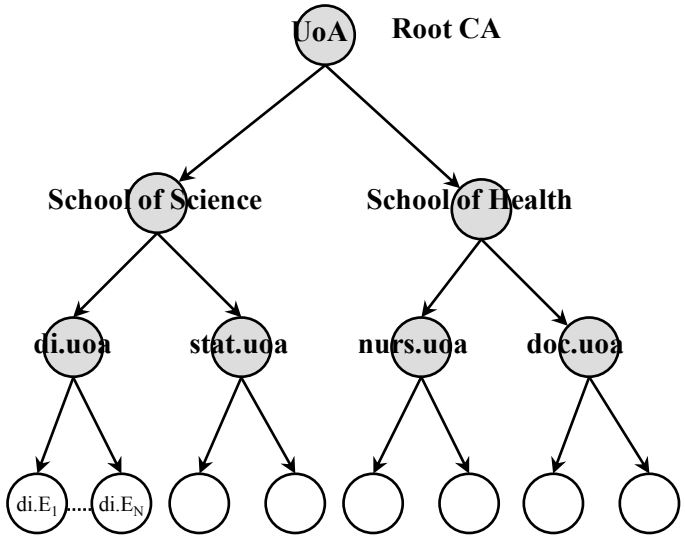
Κάθε οντότητα είναι μία CA

n-1 certificates ανά οντότητα

n*(n-1) / 2 certificates στο σύνολο

κάθε οντότητα «αυτο-υπογράφει»το certificate της

Ιεραρχική - Διαπιστοποίηση



Η Root CA (UoA) υπογράφει το πιστοποιητικό της CA School of Science

Η CA School of Science υπογράφει το πιστοποιητικό της CA di.uoa

Η CA di.uoa υπογράφει το πιστοποιητικό της οντότητας $di.E_1$.

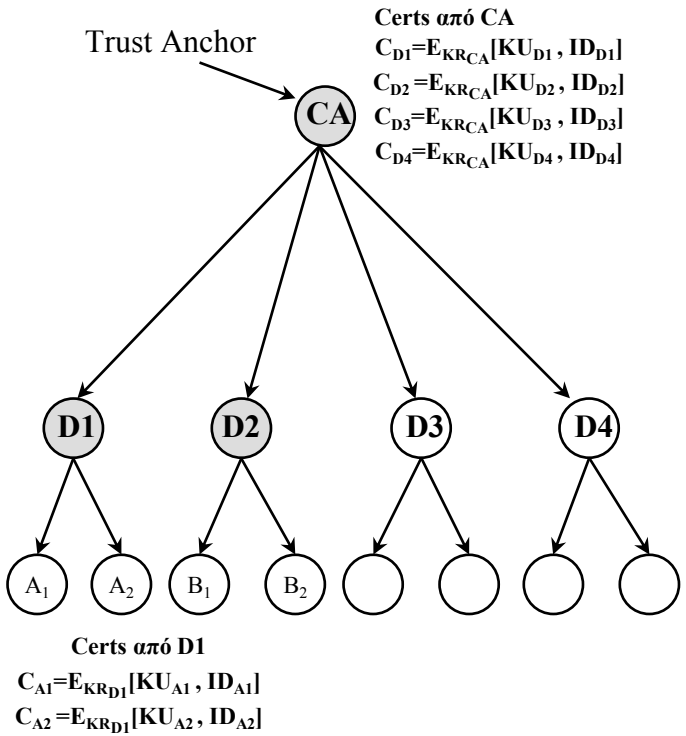
Ωστόσο, η οντότητα $di.E_1$ χρησιμοποιεί το δημόσιο κλειδί της Root CA (UoA) για να επιζητήσει την εγκυρότητα δημοσίου κλειδιού άλλης Ei στην ιεραρχία

Η root CA αυτο-υπογράφει το πιστοποιητικό της (self-signed)

(–) Η αξιοπιστία εξαρτάται από το ιδιωτικό κλειδί της Root CA

(–) Μακροσκελείς αλυσίδες πιστοποίησης σε μεγάλες ιεραρχίες`

Ιεραρχική - Διαπιστοποίηση



Πώς η root CA λειτουργεί ως trust anchor

$A_2 \rightarrow A_1$ υπογεγραμμένο μήνυμα M:

$A_2 \rightarrow A_1$: $E_{KR_{A2}}[M \,||\, ID_{A2}] \,||\, ID_{A2} \,||\, D_1$

A_1 αναζητά δημόσιο κλειδί A_2

A_1 ανασύρει πιστοποιητικό C_{A2}

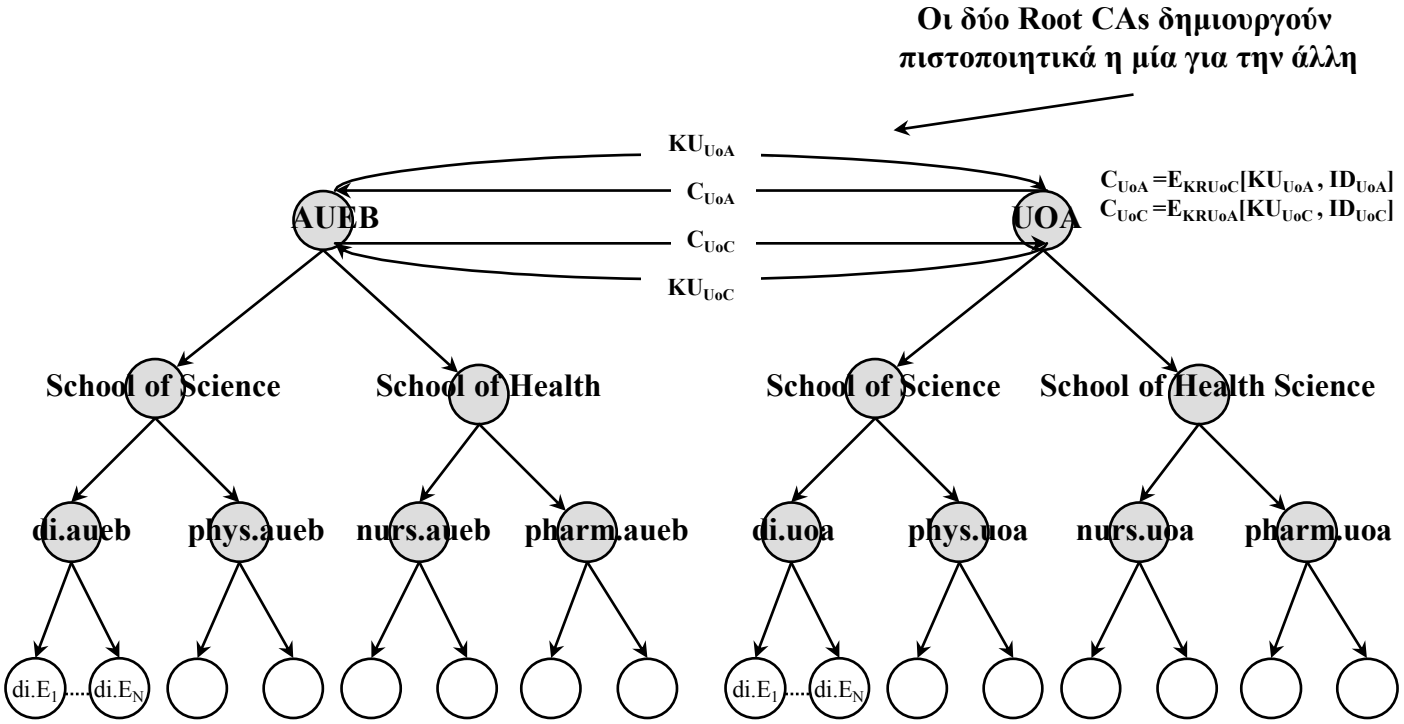
Το C_{A2} υπογεγραμμένο από ιδιωτικό κλειδί D_1

A_1 αναζητά δημόσιο κλειδί D_1

A_1 ανασύρει πιστοποιητικό C_{D1}

Το C_{D1} υπογεγραμμένο από ιδιωτικό κλειδί root CA την οποία όλοι εμπιστεύονται

Δένδρα πολλαπλών ριζών



Οι χρήστες που ανήκουν στην ιεραρχία με Root CA το UoA αποκτούν εμπιστοσύνη στα πιστοποιητικά της ιεραρχίας με Root CA το AUEB, και τανάπαλιν.

Νομικό πλαίσιο

- Οδηγία 1999/93/ΕC για Ηλεκτρονικές Υπογραφές:
  - ✓ Επικεντρώνεται στη χρήση δομών ΥΔΚ για τη παροχή υπηρεσιών ηλεκτρονικής υπογραφής.
- Προεδρικό Διάταγμα 150/2001 (υλοποίηση της Ευρωπαϊκής Οδηγίας).
  - ✓ Ορίζει τις απαιτήσεις ασφάλειας για τη δημιουργία προηγμένης ηλεκτρονικής υπογραφής
  - ✓ Απαιτεί τη δημιουργία της υπογραφή μέσα από ασφαλή κρυπτογραφική διάταξη
  - ✓ Προβλέπει την εθελοντική διαπίστευση των Αρχών Πιστοποίησης (Παρόχων Υπηρεσιών Πιστοποίησης)
- Το ΠΔ 150/2001 πλαισιώνεται με τεχνικές προδιαγραφές βασισμένες στις τεχνολογίες ΥΔΚ

Εποπτεία Αρχών Πιστοποίησης

- Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι ο υπεύθυνος εποπτικός, ελεγκτικός οργανισμός ο οποίος θα παρέχει εθελοντική διαπίστευση στις Αρχές Πιστοποίησης (Παρόχους Υπηρεσιών Πιστοποίησης – Π.Υ.Π.)
- Οι Α.Π.θα πρέπει να είναι νομικά και επιχειρησιακά συμβατές με το ΠΔ 150/2001
- Οι ΠάροχοιΑσφαλώνΕφαρμογώνκαιΥπηρεσιώνθαπρέπεινα ικανοποιούν απαιτήσεις συμβατότητας και διαλειτουργικότητας χρησιμοποιώντας ευέλικτες και επεκτάσιμες τεχνολογίες.
- Διεύρυνση και πλήρη αξιοποίηση του η- επιχειρείν.

Εγκαθίδρυση Κλειδιών με Diffie-Hellman

Δυνάμεις σε υπόλοιπα

- Ακολουθίες δυνάμεων a modulo n, όπου a ϵ $\mathbf{Z}^*n$
- Δηλαδή a^0, a^1, a^2, …. modulo n. Η 0th τιμή της ακολουθίας είναι $a^0 \bmod n = 1$, και η ith τιμή είναι $a^i \bmod n$.
- Δυνάμεις 3 modulo 7
  - ✓ i 0 1 2 3 4 5 6 7 8 9 10 11
  - ✓ $3^i \bmod 7$ 1 3 2 6 4 5 1 3 2 6 4 5
- Δυνάμεις 2 modulo 7
  - ✓ i 0 1 2 3 4 5 6 7 8 9 10 11
  - ✓ $2^i \bmod 7$ 1 2 4 1 2 4 1 2 4 1 2 4
- π.χ. $\langle 2^* \rangle = \{1, 2, 4\}$ στο $\mathbf{Z}^*_7$, και $\mathrm{ord}_7(2) = 3$.

Δυνάμεις σε υπόλοιπα

- Έστω ‹a*› υποομάδα του $\mathbf{Z}^*_n$ που γεννά ο a από επαναλαμβανόμενο πολλαπλασιασμό και $ord_n(a)$ ("order of a, modulo n") να ορίζει την τάξη του a στο $\mathbf{Z}^*_n$.
- Αν ordn(g)=|$\mathbf{Z}^*n$|, τότε κάθε στοιχείο του $\mathbf{Z}^*_n$ είναι δύναμη του g, modulo n, οπότε g είναι πρωτεύων ρίζα ή γεννήτορας του $\mathbf{Z}^*_n$.
- Π.χ. 3 είναι πρωτογενής ρίζας modulo 7, αλλά όχι ο 2
- Αν το $\mathbf{Z}^*_n$ έχει ρίζα τότε η ομάδα αναφέρεται ως κυκλική

Πρόβλημα διακριτού λογαρίθμου

- Αν θέλουμε να υπολογίζουμε την k^{th} δύναμη στοιχείου συνόλου (discrete exponentiation):
  - ✓ Ακέραια ύψωση σε δύναμη k
  - ✓ Εύρεση υπολοίπου κατά με n
  - ✓ Π.χ. στο Z^*_{17}: $3^4 = 81$, με διαίρεση με το 17, έχουμε υπόλοιπο 13, άρα $3^4 \equiv 13 \bmod 17$
- **Discrete logarithm**: είναι το αντίστροφο πρόβλημα:
  - ✓ Δεδομένου ότι $3^k \equiv 13 \pmod{17}$, ποιο είναι το k?
  - ✓ Συνήθως βρίσκουμε το μικρότερο, άρα $k = 4$.
  - ✓ Όμως υπάρχουν άπειροι k

Διανομή Κλειδιών Diffie Hellman

- Για το σύνολο $Z^*_p=\{1, \ldots, p-1\}$
- Έστω πρώτος αριθμός p
- Ως πρωτογενής ρίζα (ή γεννήτορας) g του πρώτου p ορίζεται ο αριθμός του οποίου οι δυνάμεις του modulo(p) παράγουν όλους τους ακεραίους από 1 έως p-1
- Δυνάμεις 3 modulo 7
  - ✓ i 0 1 2 3 4 5 6 7 8 9 10 11
  - ✓ $3^i \bmod 7$ 1 3 2 6 4 5 1 3 2 6 4 5
- Άρα g=3 πρωτογενής ρίζα του p=7 με τάξη 6
- Για οποιοδήποτε ακέραιο a ϵ $\mathbf{Z}^*_p$ και για μια πρωτογενή ρίζα g ενός πρώτου p μπορεί να βρεθεί z ώστε $g^z=a \bmod p$
- Ο z καλείται διακριτός λογάριθμος ή δείκτης του a για βάση g και modp και συμβολίζεται ως $z=\text{ind}_{g,p}(a)$

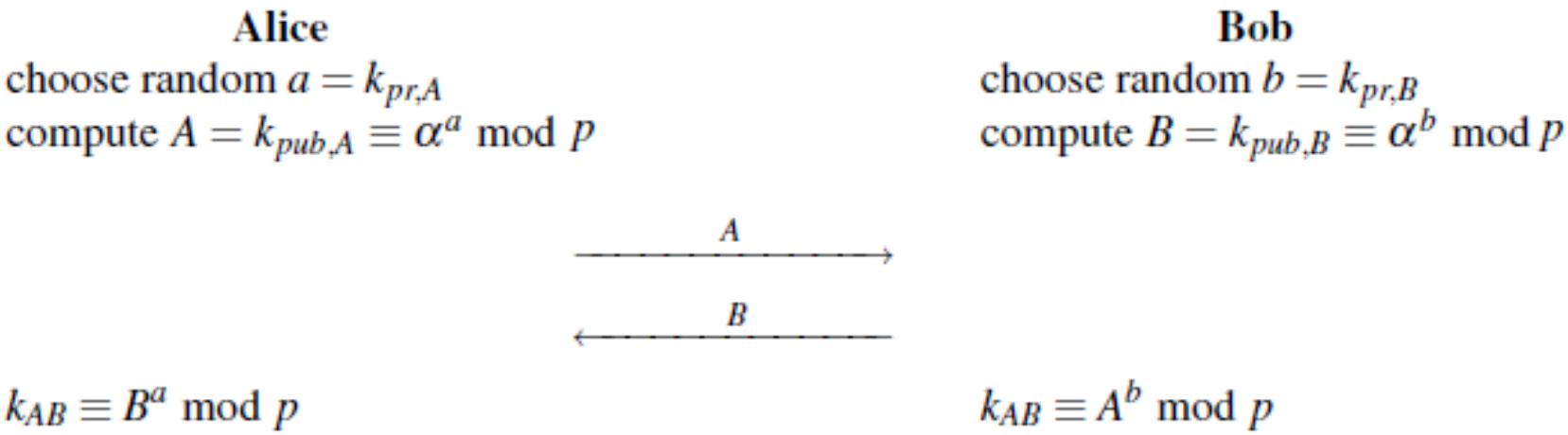
Διανομή Κλειδιών Diffie Hellman

- *DLP: Discrete Logarithm Problem*:
  - ✓ Δεδομένου ενός πρώτου p, μιας γεννήτριας g του Z*p, και ενός στοιχείου β ϵ Z^*_p, βρες τον ακέραιο x, $0 \leq x \leq p-2$, ώστε $g^x = \beta \bmod p$
    - Δεδομένου του x είναι υπολογιστικά εφικτό να βρεθεί το g^x
- DHP: *Diffie-Hellman problem*
  - ✓ Δεδομένου ενός πρώτου p, μιας γεννήτριας g του Z^*_p, και των στοιχείων $g^\alpha \bmod p$, $g^\beta \bmod p$, βρες το $g^{\alpha\beta} \bmod p$

Διανομή Κλειδιών Diffie Hellman

- Ο Α και Β στέλνουν από ένα μήνυμα σε ένα ανασφαλές κανάλι
- Αποτέλεσμα: Κοινό μυστικό κλειδί Κ και στα δύο μέρη
  - ✓ Βήμα 1. Επιλέγεται και δημοσιοποιείται πρώτος αριθμός p και μια πρωτογενής ρίζα g του p
  - ✓ Βήμα 2. Δημιουργία τυχαίων αριθμών
    - Ο Α επιλέγει έναν τυχαίο ακέραιο $a=K_A$, $K_A<p$ και υπολογίζει το $A=Kpub=g^{KA} mod p$
    - Ο Β επιλέγει έναν τυχαίο ακέραιο $b=K_B$, $K_B<p$ και υπολογίζει το $B=Kpub=g^{KB} mod p$
  - ✓ Βήμα 3.
    - Κάθε πλευρά αποστέλλει στην άλλη τις τιμές Α και Β
    - Κάθε πλευρά κρατά μυστικές τις τιμές K_A και K_B
  - ✓ Βήμα 4. Παραγωγή κλειδιού
    - Α: $kAB \equiv B^a \bmod p$
    - B: $kAB \equiv A^b \bmod p$

Διανομή Κλειδιών Diffie Hellman



- Και οι δύο μεριές υπολογίζουν το ίδιο αποτέλεσμα K_{AB}
- Κάποιος κακόβουλος δράστης ξέρει g,p,A,B και πρέπει να υπολογίσει τον διακριτό αλγόριθμο για να μπορέσει να βρει το κλειδί
- Αν επιτεθεί στον B πρέπει να υπολογίσει το $b=ind_{g,p}(B)$
- Για μεγάλους πρώτους θεωρείται ανέφικτο

Παράδειγμα

- Υποθέτουμε ότι ο πρώτος είναι το p=71
- Η πρωτογενής ρίζα είναι a=7
- Ο **Α και ο Β** επιλέγουν τα ιδωτικά κλειδιά $K_A=5$ και $K_B=12$
- Τα αντίστοιχα δημόσια κλειδιά είναι
  - ✓ **Α**: $A = 7^5 \bmod 71 = 51 \bmod 71$
  - ✓ **Β**: $B = 7^{12} \bmod 71 = 4 \bmod 71$
- Ανταλλάζουν τα δημόσια κλειδιά K_A και K_B ώστε να υπολογίζουν το κοινό τους κλειδί K_{AB}
  - Α: $kAB \equiv B^a \bmod p = (4 \bmod 71)^5 \bmod 71 = 4^5 \bmod 71 = 30 \bmod 71$
  - *Β:* $kAB \equiv A^b \bmod p = (51 \bmod 71)^{12} \bmod 71 = 51^{12} \bmod 71 = 30 \bmod 71$

Συμπερασματικά

- Ο Α και ο Β συμφωνούν σε μια πεπερασμένη κυκλική ομάδα G και σε έναν γεννήτορα g του G
- Ο Α επιλέγει έναν τυχαίο φυσικό αριθμό a και στέλνει το g^a στον Β
- Ο Β επιλέγει έναν τυχαίο φυσικό αριθμό b και στέλνει το g^b στον Α
- Ο Α υπολογίζει το $K_{AB}=(g^b)^a$
- Ο Α υπολογίζει το $K_{AB}=(g^a)^b$
- Και οι υπολογίζουν το ίδιο κλειδί καθώς η πολλαπλασιαστική ομάδα G είναι μεταβατική ως προς τον πολλαπλασιασμο οπότε $(g^a)^b=(g^b)^a$

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2015-2016

Μαρκάκης Ευάγγελος
markakis@aueb.gr

Ντούσκας Θεόδωρος
tntouskas@aueb.gr