ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριακών Συστημάτων
«Υποδομή Δημόσιας Κλείδας»

Τμήμα Πληροφορικής

Καθ. Δ. Πολέμη – Καθ. Π.Κοτζανικολάου

3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

- **Εισαγωγή**
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- Οργανωτικές δομές
- Πρότυπα
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης
- Νομικό πλαίσιο

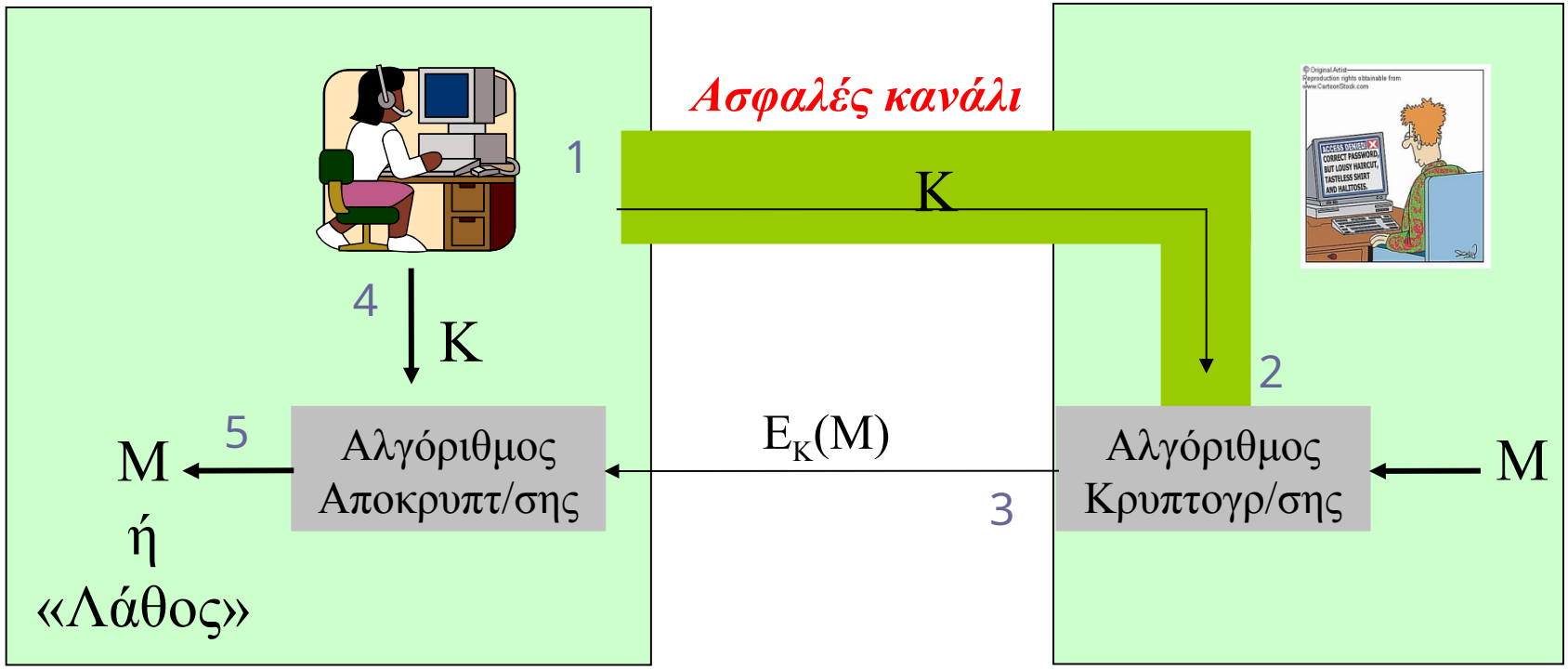
Εισαγωγή: Το Πρόβλημα Διαχείρισης Κλειδιών

- Η παροχή υπηρεσιών ασφάλειας είναι δυνατή με τη χρήση κρυπτογραφικών μηχανισμών.
  - Εμπιστευτικότητα μηνύματος:
    - Συμμετρική κρυπτογράφηση (AES, RC5, ChaCha20, …)
    - Ασύμμετρη κρυπτογράφηση (RSA, ElGamal, ECC, …)
  - Ακεραιότητα μηνύματος:
    - Συναρτήσεις κατακερματισμού (SHA2, SHA3,…)
    - Συναρτήσεις κατακερματισμού με κλειδί (HMAC)
    - Ψηφιακές υπογραφές (RSA, ElGamal, DSA, …)
  - Μη αποποίηση (non-repudiation):
    - Ψηφιακές υπογραφές (RSA, ElGamal, DSA, …)
- Η παροχή υπηρεσιών ασφάλειας προϋποθέτει τη ***διαχείριση των κρυπτογραφικών κλειδιών***

Διαχείριση Κλειδιών

- Η διαχείριση κρυπτογραφικών κλειδιών (key management) περιλαμβάνει:
  - Την ασφαλή δημιουργία των κλειδιών
  - Την πιστοποίηση των κλειδιών
  - Την αποθήκευση / αναζήτηση των κλειδιών
  - Την ανταλλαγή / διανομή των κλειδιών μεταξύ των χρηστών
  - Την ανανέωση των κλειδιών
  - Την ασφαλή καταστροφή παλαιών κλειδιών

Συμμετρική κρυπτογράφηση

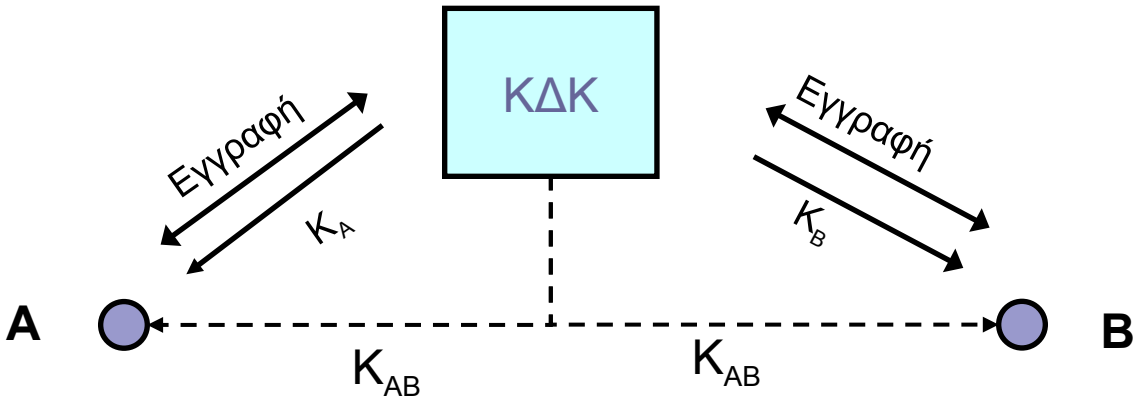


Προβλήματα διαχείρισης Συμμετρικών Κλειδιών

- **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**

Πιθανές λύσεις: Κέντρο Διανομής Κλειδων (ΚΔΚ) Key Distribution Center (KDC)

- Το ΚΔΚ είναι μία Έμπιστη Τρίτη Οντότητα (Trusted Third Party). Λειτουργεί ως κεντρικό σημείο εμπιστοσύνης.

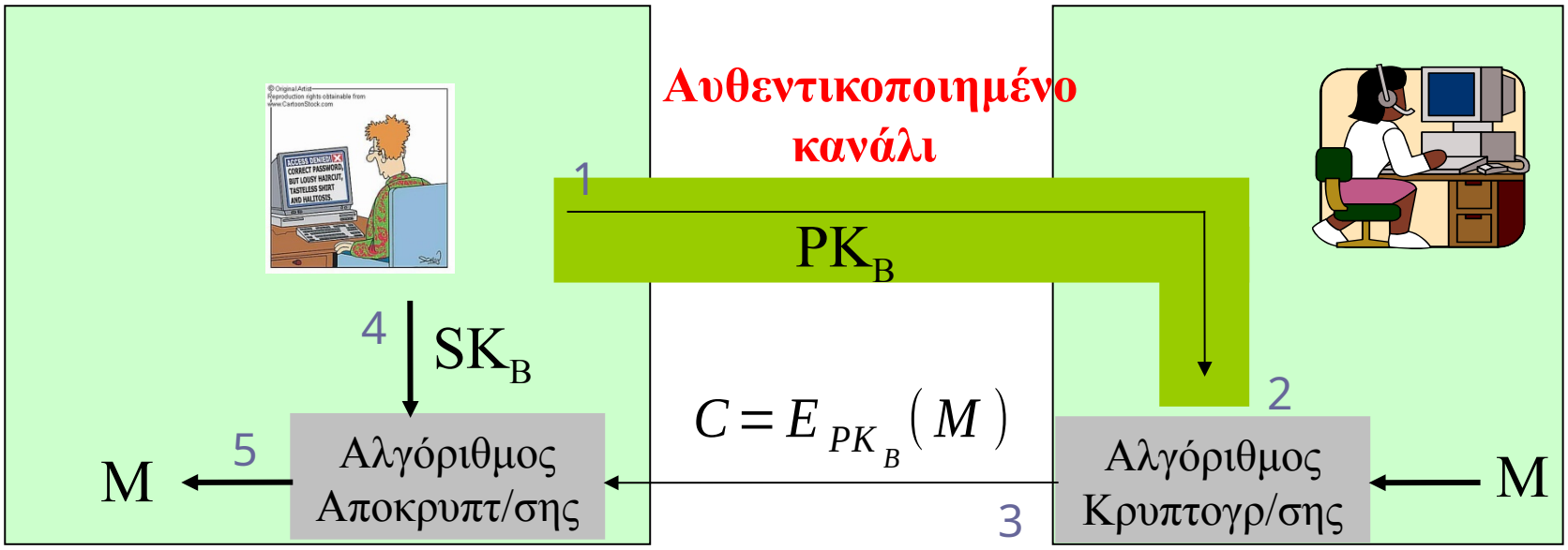


- Εάν ο χρήστης **A** θέλει να επικοινωνήσει με τον **B** επικοινωνεί με το ΚΔΚ, το οποίο δημιουργεί και στέλνει και στους δύο ένα κοινό κλειδί K_{AB}

Προβλήματα

- Επίπεδο εμπιστοσύνης
  - Το ΚΔΚ μπορεί να προσποιηθεί ότι είναι οποιοσδήποτε χρήστης
  - Εμπιστευόμαστε ότι δεν θα το κάνει!
- Μοναδικό σημείο αποτυχίας (single point of failure)
  - Εάν κάποιος επιτεθεί με επιτυχία στο ΚΔΚ τότε μπορεί να προσποιηθεί οποιονδήποτε χρήστη
- Απαιτεί συνεχή διαθεσιμότητα

Κρυπτογράφηση δημοσίου κλειδιού



Διαχείριση Δημόσιων Κλειδιών

- Κάθε χρήστης έχει μόνο ένα ζεύγος κλειδιών
  - Συνεπώς χρειάζονται **2 κλειδιά ανά χρήστη**
  - Συνολικά: **2× n** κλειδιά
- Ανταλλαγή κλειδιών
  - Δεν απαιτείται εμπιστευτικότητα κατά την ανταλλαγή κλειδιού
  - Απαιτείται όμως επαλήθευση της αυθεντικότητας αποστολέα & παραλήπτη
    - *Πως εξασφαλίζεται ότι ένα δημόσιο κλειδί ανήκει πραγματικά σε έναν χρήση;*

Πιθανή λύση: Χρήση Έμπιστης Οντότητας ως Αρχής Πιστοποίησης (Certificate Authority)

- Χρήση μίας *Έμπιστης Τρίτης Οντότητας* η οποία αυθεντικοποιεί τα δημόσια κλειδιά όλων των χρηστών.
- Αυτή η έμπιστη οντότητα ονομάζεται ***Αρχή Πιστοποίησης – ΑΠ (Certification Authority – CA)***
- Κάθε χρήστης αρκεί να γνωρίζει το δημόσιο κλειδί της ΕΟ $\mathbf{PK_{CA}}$ ώστε να επαληθεύσει το δημόσιο κλειδί οποιουδήποτε άλλου χρήστη της ΕΤΟ.
  - Ο χρήστης X στέλνει το δημόσιο κλειδί του $\mathbf{PK_X}$ στην ΑΠ (CA)
  - Η ΑΡ **υπογράφει ψηφιακά** ένα μήνυμα το οποίο περιλαμβάνει
    - Την ταυτότητα (ένα μοναδικό προσδιοριστικό) του χρήστη X: $\boldsymbol{ID_X}$
    - Το δημόσιο κλειδί του χρήστη X: $\boldsymbol{PK_X}$
    - Την ημερομηνία της υπογραφής $\boldsymbol{t_{create}}$ και της λήξης $\boldsymbol{t_{expire}}$
    - Όλα τα παραπάνω υπογράφονται με το μυστικό κλειδί $\boldsymbol{SK_{CA}}$ της ΑΠ

$$\boldsymbol{CERT_X = [\, ID_X \,|\, PK_X \,|\, t_{create} \,|\, t_{expire} \,|\, SIG_{SK^{CA}} (ID_X, PK_X, t_{create}, t_{expire}) \,]}$$

3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

- Εισαγωγή
- **Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ**
- Οργανωτικές δομές
- Πρότυπα
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης
- Νομικό πλαίσιο

Υποδομή Δημόσιου Κλειδιού– ΥΔΚ
Public Key Infrastructure - PKI

Μία Υποδομή Δημόσιου Κλειδιού (ΥΔΚ - PKI) είναι:

- Ένα σύνολο *ψηφιακών πιστοποιητικών, Αρχών Πιστοποίησης και άλλων υπηρεσιών*, οι οποίες *επιβεβαιώνουν και αυθεντικοποιούν τα δημόσια κλειδιά 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.

Υπηρεσίες ΥΔΚ

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

Υπηρεσία Εγγραφής (Registration Authority – RA)

- 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 Service)

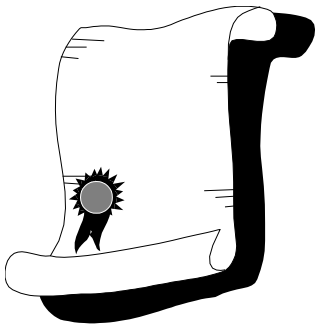
- Αναλαμβάνει την έκδοση και προσωποποίηση κάθε ζεύγους κλειδιών
  - Παρέχει στο χρήστη τη δυνατότητα **να δημιουργήσει ο ίδιος το ζεύγος κλειδιών του**
  - Τα ιδιωτικά κλειδιά πρέπει να διαφυλάσσονται σε ασφαλή μέσα, όπως **έξυπνες κάρτες**
- Επιτρέπει τη **διανομή / ανταλλαγή / αναζήτηση** των δημόσιων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

Υπηρεσία Πιστοποίησης

- **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



Πιστοποιητικό X.509

Certificate

thales.cs.unipi.gr | GEANT OV RSA CA 4 | USERTrust RSA Certification Authority

Subject Name

Country	GR
State/Province	Attikí
Organization	University of Piraeus
Common Name	thales.cs.unipi.gr

Issuer Name

Country	NL
Organization	GEANT Vereniging
Common Name	GEANT OV RSA CA 4

Validity

Not Before	Fri, 26 Apr 2024 00:00:00 GMT
Not After	Sat, 26 Apr 2025 23:59:59 GMT

Subject Alt Names

DNS Name	thales.cs.unipi.gr
DNS Name	www.thales.cs.unipi.gr

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	9E:48:56:2D:55:8E:71:DA:72:55:9A:1C:7D:5F:5D:EF:16:56:C0:D8:40:93:28:54:…

Miscellaneous

Serial Number	00:90:12:F5:63:B7:0C:90:DE:AD:AF:82:7C:41:37:B9:0D
Signature Algorithm	SHA-384 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	93:60:42:D3:BA:A0:6B:28:DC:E5:0D:19:BA:ED:5B:4E:49:AC:05:26:97:62:27:9…
SHA-1	CC:9E:23:23:B5:A2:56:D0:E2:D6:F6:A7:F0:53:37:6F:D9:72:95:C8

Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Key Encipherment

Extended Key Usages

Purposes	Server Authentication, Client Authentication

Βασικές Λειτουργίες Αρχής 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 .

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)
  - OCSP ανταποκριτές
  - Domain Name System (DNS)
  - Web εξυπηρετητές
  - File Transfer Protocol (FTP) - εξυπηρετητές

Υπηρεσία Ανάκλησης Πιστοποιητικών

- 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)

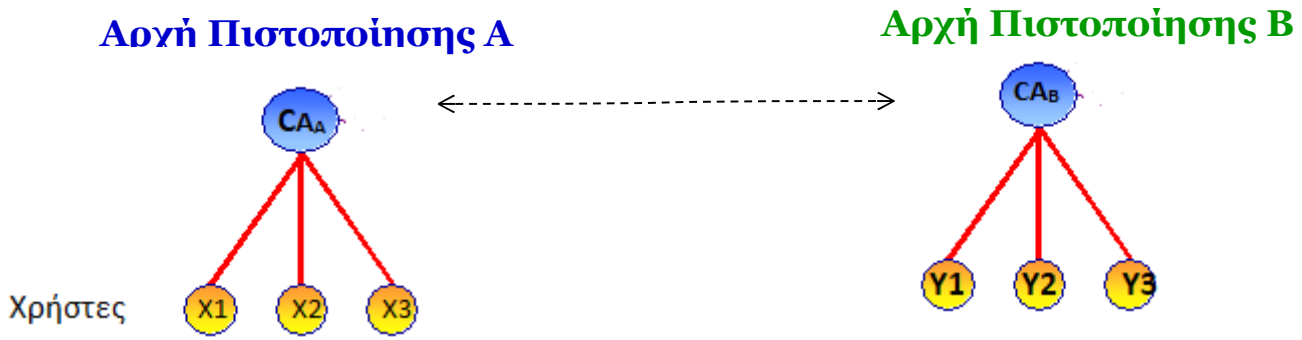
Υπηρεσία Χρονοσφράγισης

- 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

Διαπιστοποίηση:
Η κάθε Αρχή υπογράφει το πιστοποιητικό της άλλης Αρχής.

- 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.

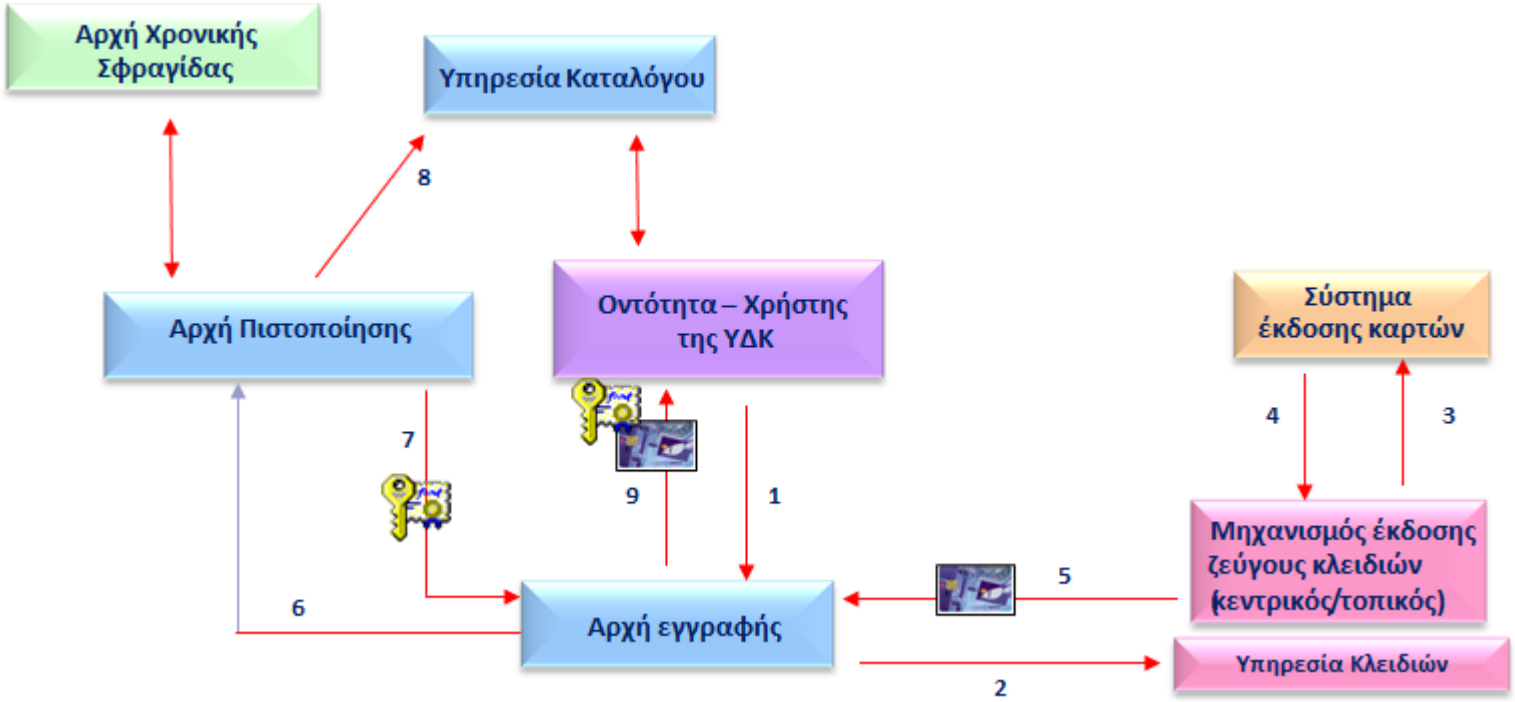


- Οι χρήστες που ανήκουν στην ΑΠ $\mathbf{CA_A}$ μπορούν να επικοινωνήσουν μεταξύ τους γιατί γνωρίζουν το κλειδί της ΑΠ Α.

Το ίδιο συμβαίνει με τους χρήστες της Αρχής Πιστοποίησης $\mathbf{CA_B}$.

Πως μπορούν να επικοινωνήσουν όλοι οι χρήστες και των δύο Αρχών Πιστοποίησης;

Γενικό Πλαίσιο ΥΔΚ



Γνωστοί Πάροχοι Υπηρεσιών Πιστοποίησης (Αρχές Πιστοποίησης)

- DigiCert
- COMODO
- GoDaddy
- Thawte
- GeoTrust
- RapidSSL
- Symantec

Στην Ελλάδα:

- Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)
- Υπηρεσία Ψηφιακών Πιστοποιητικών (PKI) – GRNET
- HARICA

3η θεματική ενότητα

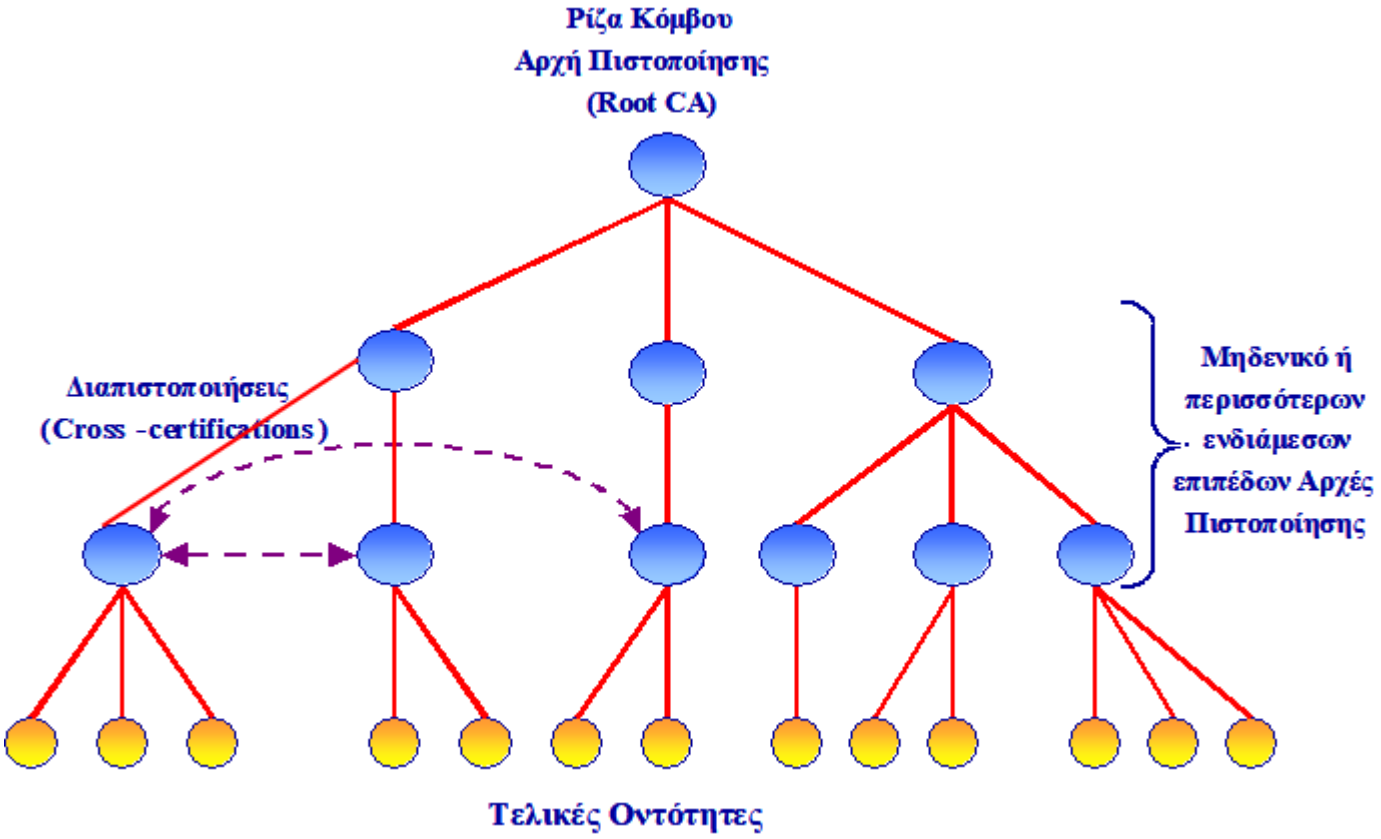
Υποδομή Δημόσιας Κλείδας

- Εισαγωγή
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- **Οργανωτικές δομές**
- Πρότυπα
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης
- Νομικό πλαίσιο

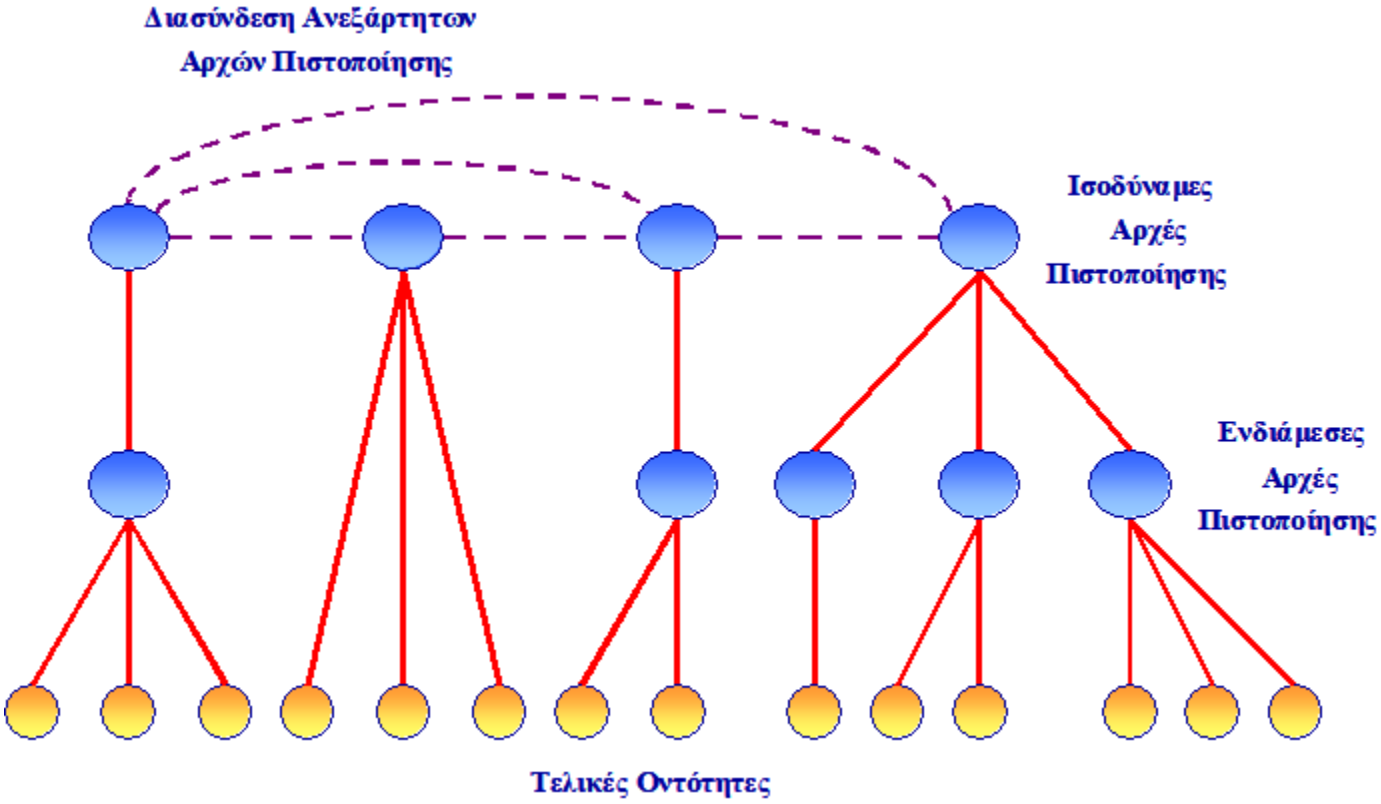
Οργανωτικές Δομές

- Βασικοί παράγοντες που επηρεάζουν τις αρχιτεκτονικές Υ.Δ.Κ.:
  - Τύποι εμπλεκόμενων οντοτήτων και ανάγκες πιστοποίησης.
  - Προφίλ πιστοποιητικών και ειδικές απαιτήσεις
  - Οντότητες που λειτουργούν ως Αρχές Πιστοποίησης και Εγγραφής.
  - Μέθοδος διάθεσης/δημοσίευσης πιστοποιητικών και δημόσιων κλειδιών
- Κάθε αρχιτεκτονική εκφράζει και ένα διαφορετικό *μοντέλο εμπιστοσύνης (trust model)*

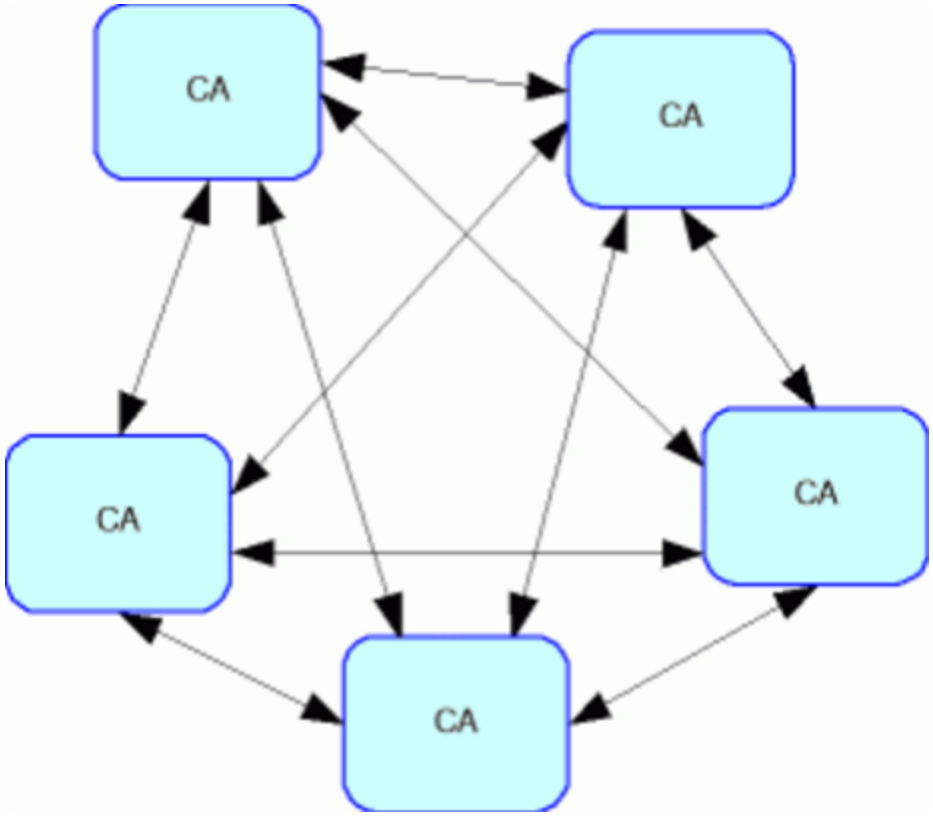
Ιεραρχικό μοντέλο (Hierarchical model)



Μερικώς κατανεμημένο μοντέλο: Πολλαπλές ιεραρχίες

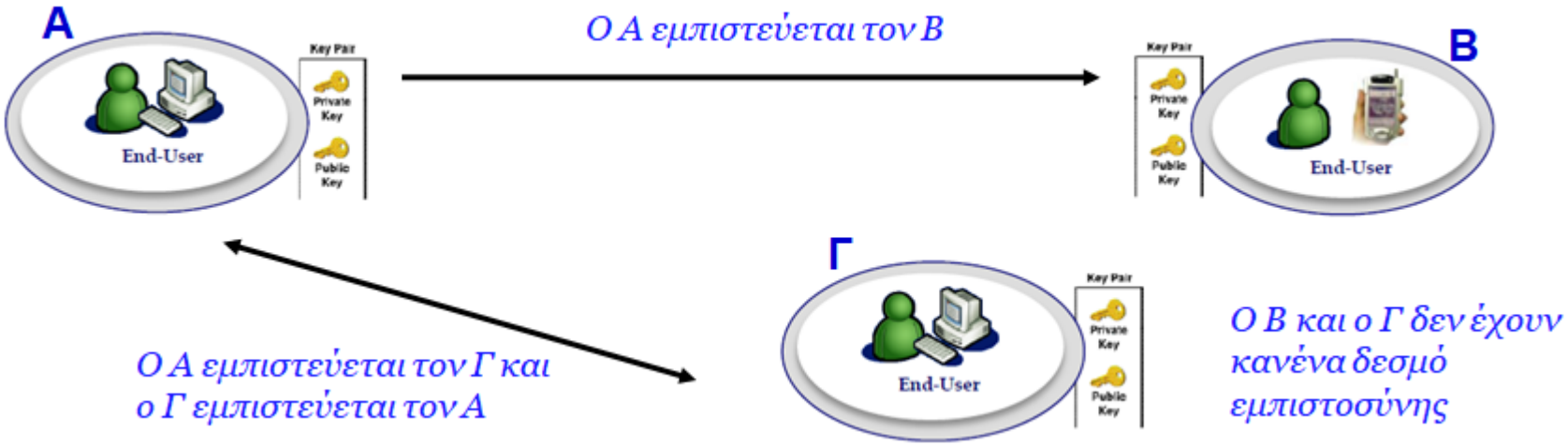


Πλήρως κατανεμημένο μοντέλο: Χωρίς ιεραρχία (Mesh model)



Παράδειγμα πλήρως κατανεμημένου μοντέλου: Το μοντέλο χρήστη

- Κάθε χρήστης είναι εξ ολοκλήρου υπεύθυνος να αποφασίσει ποια πιστοποιητικά εμπιστεύεται και ποία όχι.
- Εφαρμόζεται στο PGP.



3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

- Εισαγωγή
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- Οργανωτικές δομές
- **Πρότυπα**
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης
- Νομικό πλαίσιο

Πρότυπα ΥΔΚ 1ης γενιάς

- Πρότυπο ASN.1 για την προδιαγραφή της δομής των μηνυμάτων και των εγγράφων (Abstract Syntax Notation One)
  - Δημιουργία συγκεκριμένων πρωτοκόλλων επικοινωνίας (μηνυμάτων, σειρά που αυτά ανταλλάσσονται, κτλ)
  - Ευκολότερη περιγραφή των αντικειμένων (X.509 certificates)
  - Καμία δέσμευση σε γλώσσες προγραμματισμού
- Η ASN.1 διαθέτει απλούς τύπους δεδομένων και σημειογραφία που μπορεί να χρησιμοποιήσει οποιοσδήποτε προκειμένου να κατασκευάσει πιο πολύπλοκα σύνολα δομών δεδομένων.

Πρωτόκολλα ΥΔΚ 1ης γενιάς

- Προφίλ X.509 v3 Public Key Certificates
- Προφίλ X.509 v2 Certificate Revocation Lists – CRLs (RFC 2459)
- Πρωτόκολλα διαχείρισης Υ.Δ.Κ. (RFC 2510)
- Χρονοσφράγιση (RFC 3161)

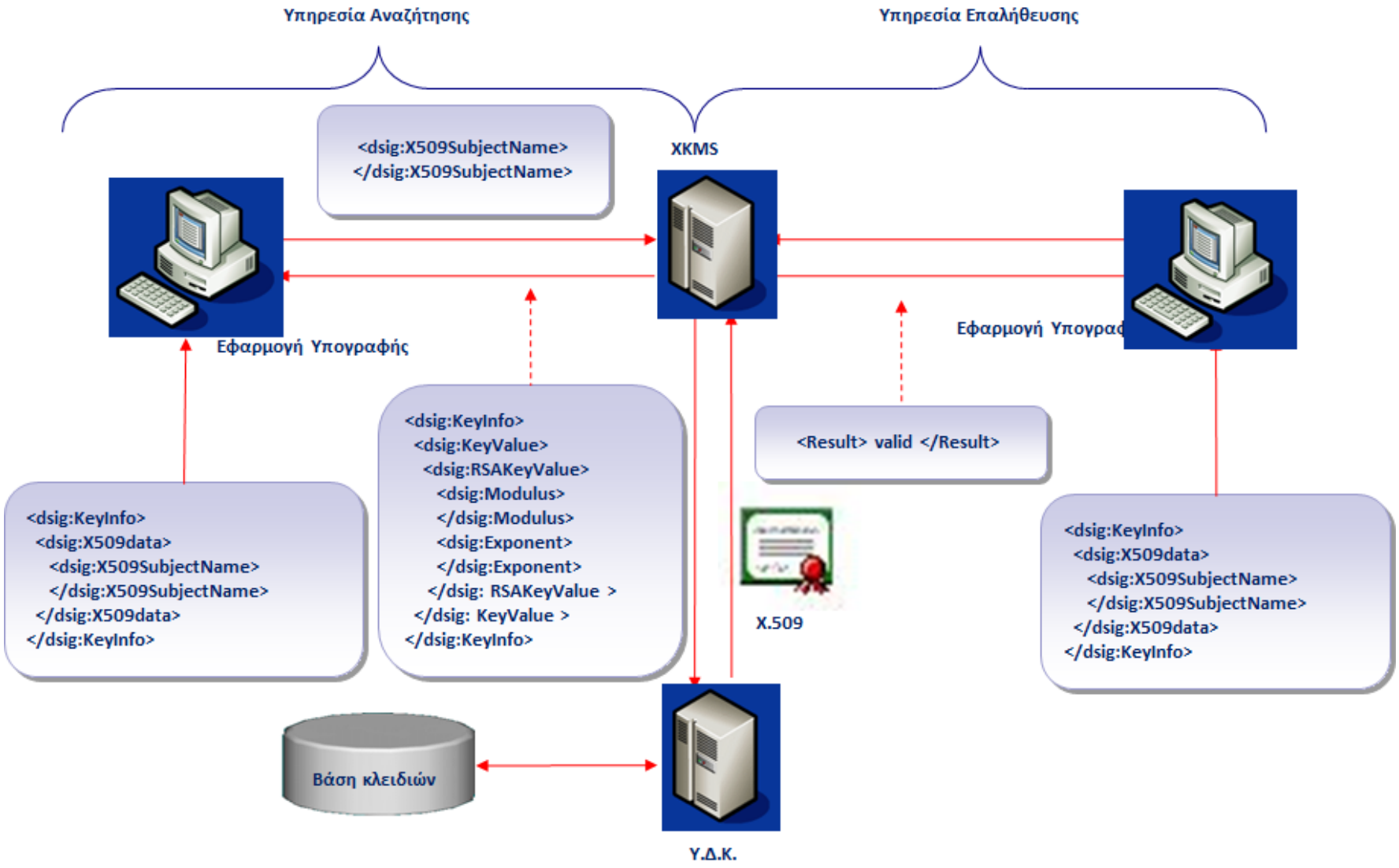
Διαδικασίες ΥΔΚ 1ης γενιάς

- Εγγραφή της οντότητας πριν εκδοθεί το πιστοποιητικό (*registration*)
- Διαδικασίες Αρχικοποίησης (δημιουργία του ζεύγους κλειδιών)
- Πιστοποίηση - Έκδοση του ψηφιακού πιστοποιητικού (*certification*)
- Ανάκτηση ζεύγους κλειδιών (*key recovery*)
- Ανανέωση ζεύγους κλειδιών (*key update*)
- Ανάκληση - όταν ένα εξουσιοδοτημένο πρόσωπο συμβουλεύει την CA να εισάγει ένα συγκεκριμένο πιστοποιητικό σε μια λίστα ανάκλησης (*key revocation*)
- Διαπιστοποίηση - δύο Αρχές Πιστοποίησης αλληλο-πιστοποιούνται (*cross-certificatation*).

ΥΔΚ 2ης γενιάς

- XML: Νέα μεταγλώσσα για τον ορισμό δομών δεδομένων
- X.509: Δυαδικά δεδομένα βασισμένα στην ASN.1 σε κωδικοποίηση CER ή DER
- Ανταλλαγή XML Μηνυμάτων διαμέσου Υπηρεσιών Ιστού (Web Services)
- Διαχείριση Κλειδιών με την χρήση της προτυποποίησης XML Key Management 2.0 – XKMS
  - Επιτρέπει την πρακτική εφαρμογή των ΥΔΚ στον παγκόσμιο ιστό και στις υπηρεσίες του
  - Δυνατότητα επικοινωνίας διαφορετικών εφαρμογών με τη χρήση μοναδικών ταυτοτήτων χρηστών σε εύρος εφαρμογών και συστημάτων
  - Βελτιώνει την εφαρμογή της ΥΔΚ αναθέτοντας τις λειτουργίες σε ένα εξυπηρετητή με πρωτόκολλα χαμηλού κόστους
  - Η ανταλλαγή κλειδιών και η διαχείριση πιστοποιητικών γίνεται σε επίπεδο εξυπηρετητή, αντί σε επίπεδο πελάτη
- Πλαίσιο ΑσφάλειαςW3C
  - Υπογραφή XML – XML Digital Signature
  - Κρυπτογράφηση XML – XML Encryption

XML Key Management System



3η θεματική ενότητα

2. Υποδομή Δημόσιας Κλείδας

- Εισαγωγή
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- Οργανωτικές δομές
- Πρότυπα
- **Πολιτική πιστοποίησης / Δήλωση πρακτικών πιστοποίησης**
- Νομικό πλαίσιο

Πολιτική Πιστοποίησης

- Πολιτική Πιστοποίησης
  - Ένα ***σύνολο κανόνων*** που καθορίζουν ***τις δυνατότητες χρήσης ενός πιστοποιητικού*** σε μια συγκεκριμένη κοινότητα ή/και ομάδα χρηστών με κοινές απαιτήσεις ασφαλείας.
  - Περιλαμβάνει τις απαιτήσεις ασφάλειας για τον ΠΥΠ.
- *Περιγράφει το προφίλ των πιστοποιητικών* της ΥΔΚ:
  - Θέματα αναγνώρισης
  - Θέματα εγγραφής χρηστών
  - Θέματα έκδοσης
  - Θέματα διανομής
  - Θέματα διάθεσης
  - Θέματα ανάκλησης

Πολιτική Πιστοποίησης
Επεκτάσεις Πιστοποιητικών (certificate extensions)

- Το πρότυπο The X.509 ορίζει πρότυπες επεκτάσεις (standard certificate extensions), με τις οποίες μπορούν να οριστούν οι επιτρεπτές χρήσεις των διαδρομών πιστοποίησης.
- Παραδείγματα πρότυπων επεκτάσεων είναι:
  1. Basic Constraints (Βασικοί περιορισμοί)
  2. Certificate policies (Πολιτικές Πιστοποίησης)
  3. Policy mappings (Αντιστοιχήσεις πολιτικών)
  4. Policy constraints (Περιορισμοί πολιτικών)
  5. Inhibit any policy
  6. Name constraints (Περιορισμοί ονομάτων)

Επέκταση Basic Constraints

- Η επέκταση Basic Constraints υποστηρίζει τη *διάκριση μεταξύ των πιστοποιητικών των Αρχών Πιστοποίησης (CA certificates) και των πιστοποιητικών των απλών χρηστών.*
- Δεν επιτρέπει τη χρήση ενός πιστοποιητικού χρήστη για την πιστοποίηση ενός άλλου πιστοποιητικού
- Σύνταξη basic constraints στη γλώσσα ASN.1:

```
BasicConstraintsSyntax ::= SEQUENCE {
    cA BOOLEAN DEFAULT FALSE,
    pathLenConstraint INTEGER (0..MAX) OPTIONAL }
```

- Πεδία:
  - `cA`: TRUE για πιστοποιητικά Αρχών Πιστοποίησης, FALSE για απλά πιστοποιητικά,
  - `pathLenConstraint`: Περιορίζε το μήκος της αλυσίδας πιστοποίησης (certificate chain).

Επέκταση Certificate Policies (1/2)

- Η επέκταση Certificate Policies εξασφαλίζει ότι τα πιστοποιητικά είναι έγκυρα μόνο για συγκεκριμένους σκοπούς που ορίζει ο εκδότης τους.
- Η πραγματική Πολιτική Πιστοποίησης είναι ένα κανονικό έγγραφο αναγνώσιμου κειμένου (plain-language document).
- Η Πολιτική Πιστοποίησης αναγνωρίζεται στην επέκταση με ένα μοναδικό **"object identifier"**.
  - Κάθε πιστοποιητικό μπορεί αν περιλαμβάνει κανένα, 1 ή περισσότερα `object identifier`.
  - Η ειδική τιμή "any policy" δεν θέτει κανένα περιορισμό στη χρήση του πιστοποιητικού.
  - Κατά την επαλήθευση του πιστοποιητικού, μόνο τα μονοπάτια πιστοποίησης που περιλαμβάνουν τα εγκεκριμένα object identifiers που περιλαμβάνεται στην πολιτική θα θεωρηθούν έγκυρα.
- Το πεδίο μοναδικό **"object qualifier"** παίρνει ως τιμή το url που περιέχει την αναγνώσιμη πολιτική πιστοποίησης.

Επέκταση Certificate Policies (2/2)

- Σύνταξη certificate policies στη γλώσσα ASN.1:

```
CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
policyIdentifier CertPolicyId,
policyQualifiers SEQUENCE SIZE (1..MAX) OF
PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
policyQualifierId CERT-POLICY-QUALIFIER.&id
({SupportedPolicyQualifiers}),
qualifier CERT-POLICY-QUALIFIER.&Qualifier
({SupportedPolicyQualifiers}{@policyQualifierId})
OPTIONAL }
```

Επέκταση Policy Mappings

- Η επέκταση Policy Mappings αντιστοιχεί όμοιες πολιτικές που έχουν εκδοθεί από διαφορετικές Αρχές Πιστοποίησης, ώστε να χρησιμοποιούνται σαν να είναι ίδιες.
- Σύνταξη policy mappings στη γλώσσα ASN.1:

```
PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy CertPolicyId,
    subjectDomainPolicy CertPolicyId }
```

Επέκταση Policy Constraints

- Η επέκταση Policy Constraints μπορεί να χρησιμοποιηθεί ώστε η Αρχή Πιστοποίησης να επιβάλλει:
  - την *απόρριψη πιστοποιητικών χωρίς πολιτική πιστοποίησης* (**requireExplicitPolicy**) ή
  - *για να περιορίσει τον επιτρεπτό αριθμό των Policy Mappings* (**inhibitPolicyMapping**)
- Σύνταξη policy mappings στη γλώσσα ASN.1:

```
PolicyConstraintsSyntax ::= SEQUENCE {
    requireExplicitPolicy [0] SkipCerts OPTIONAL,
    inhibitPolicyMapping [1] SkipCerts OPTIONAL }
SkipCerts ::= INTEGER (0..MAX)
```

Επέκταση Inhibit Any Policy

- Με την επέκταση Inhibit Any Policy, μία Αρχή Πιστοποίησης μπορεί να απαγορεύσει να γίνεται αποδεκτό πιστοποιητικό που έχει εκδοθεί από κατώτερη Αρχή Πιστοποίησης η οποία δεν έχει πολιτική πιστοποίησης.
- Σύνταξη Inhibit any policy στη γλώσσα ASN.1:

```
PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy CertPolicyId,
    subjectDomainPolicy CertPolicyId }
```

Επέκταση Name Constraints

- Η επέκταση Name Constraints βοηθά στη γρήγορη επαλήθευση ενός πιστοποιητικού, όταν η αναζήτηση γίνεται με βάση το όνομα.
- Σύνταξη Name Constraints στη γλώσσα ASN.1:

```
NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees [0] GeneralSubtrees OPTIONAL,
    excludedSubtrees [1] GeneralSubtrees OPTIONAL }
GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
GeneralSubtree ::= SEQUENCE {
    base GeneralName,
    minimum [0] BaseDistance DEFAULT 0,
    maximum [1] BaseDistance OPTIONAL }
BaseDistance ::= INTEGER (0..MAX)
```

Δήλωση Πρακτικών Πιστοποίησης Certificate Practice Statement (CPS)

- Περιγράφει τις πρακτικές που ακολουθεί η Α.Π. για τη διαχείριση των πιστοποιητικών.
- Λεπτομερές έγγραφο στο οποίο αναφέρονται:
  - Οι διαδικασίες λειτουργίας.
  - Τα συστήματα που παρέχουν υπηρεσίες ασφάλειας.
  - Οι ακολουθούμενες πρακτικές και οι ενέργειες διαχείρισης των πιστοποιητικών.
- Αποτελεί τμήμα του συμβολαίου του χρήστη με την Αρχή Πιστοποίησης.

Διαφορές Πολιτικής Πιστοποίησης και Δήλωσης Πρακτικών Πιστοποίησης

- Π.Π.
  - Προδιαγράφει τις δυνατότητες χρήσης των ψηφιακών πιστοποιητικών που εκδίδει η Α.Π. (πως μπορούν να χρησιμοποιηθούν τα πιστοποιητικά)
- Δ.Π.Π.
  - Τεχνικό έγγραφο τις διαδικασίες και τα μέτρα που λαμβάνει η Α.Π. για την καλή λειτουργία της

3η θεματική ενότητα

2. Υποδομή Δημόσιας Κλείδας

- Εισαγωγή
- Υπηρεσίες ΥΔΚ / Συναρτήσεις ΥΔΚ
- Οργανωτικές δομές
- Πρότυπα
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης
- **Νομικό πλαίσιο**

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 Πάροχοι Ασφαλών Εφαρμογών και Υπηρεσιών θα πρέπει να *ικανοποιούν απαιτήσεις συμβατότητας και διαλειτουργικότητας* χρησιμοποιώντας ευέλικτες και επεκτάσιμες τεχνολογίες.
- Διεύρυνση και πλήρη αξιοποίηση του η- επιχειρείν.

Γνωστοί Πάροχοι Υπηρεσιών Πιστοποίησης (Αρχές Πιστοποίησης)

- DigiCert
- COMODO
- GoDaddy
- Thawte
- GeoTrust
- RapidSSL
- Symantec

Στην Ελλάδα:

- Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)
- Υπηρεσία Ψηφιακών Πιστοποιητικών (PKI) – GRNET
- HARICA

Βιβλιογραφία

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC press, (5th ed) 2001.
2. C. Adams, S.Lloyd, “Understanding Public-Key Infrastructure” MacMillan Technical Publishing 1999
3. Δ. Πολέμη, Χ. Δημητριάδης, Σ. Παπαστεργίου, Α. Καλιαντζόγλου, Εργαστηριακά θέματα ασφάλειας, 2006.
4. Σ. Κάτσικας Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.
5. http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf