ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριακών Συστημάτων

«Υποδομή Δημόσιας Κλείδας»

Τμήμα Πληροφορικής

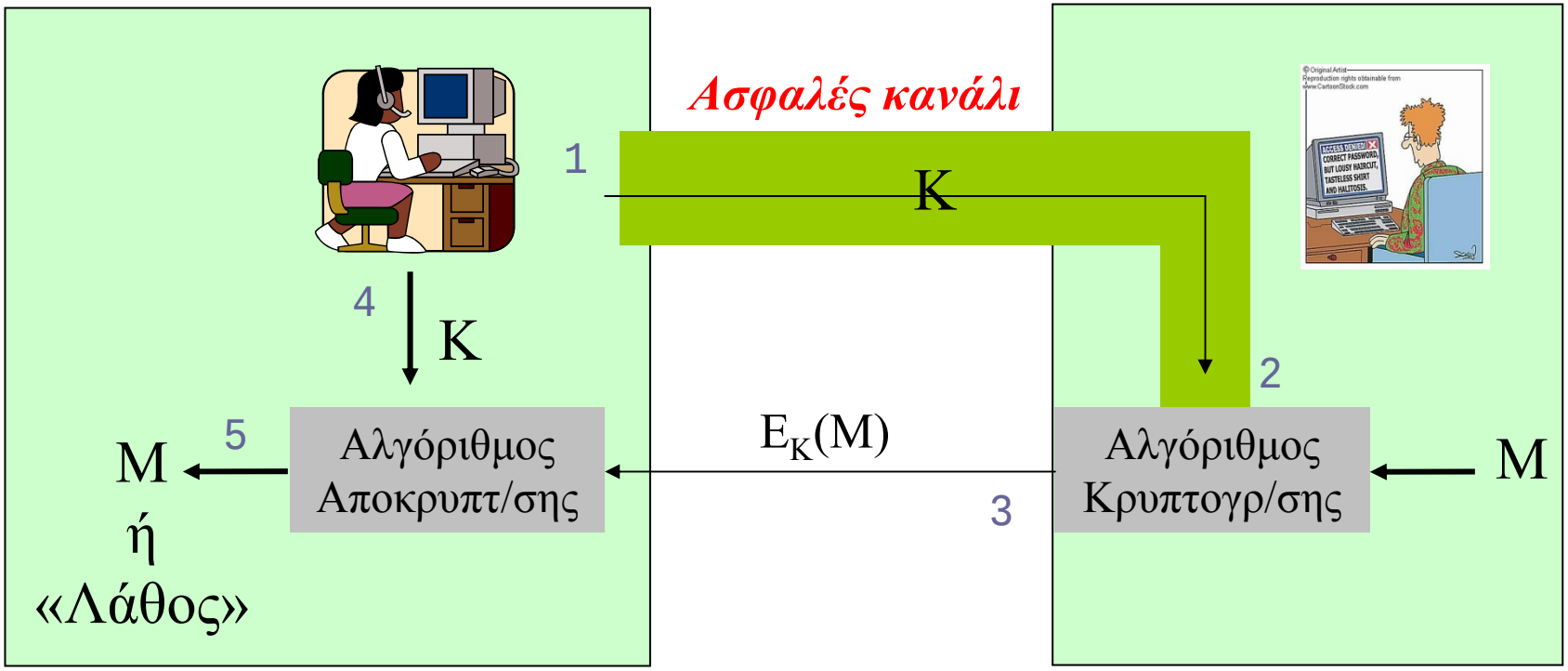
Επ. Καθ. Δ. Πολέμη
Λέκτορας Π.Κοτζανικολάου
dpolemi@unipi.gr, pkotzani@unipi.gr

3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

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

Συμμετρική κρυπτογράφηση

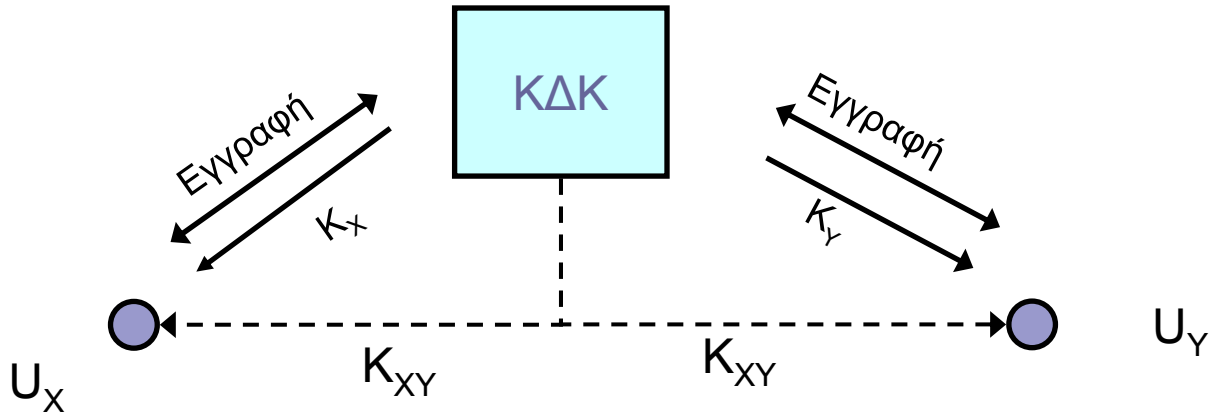


Το Πρόβλημα Διαχείρισης Συμμετρικών Κλειδιών

- 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 Κλείδων
Key Distribution Center (KDC)

- Έμπιστη Τρίτη Οντότητα (Trusted Third Party). Λειτουργεί ως κεντρικό σημείο.

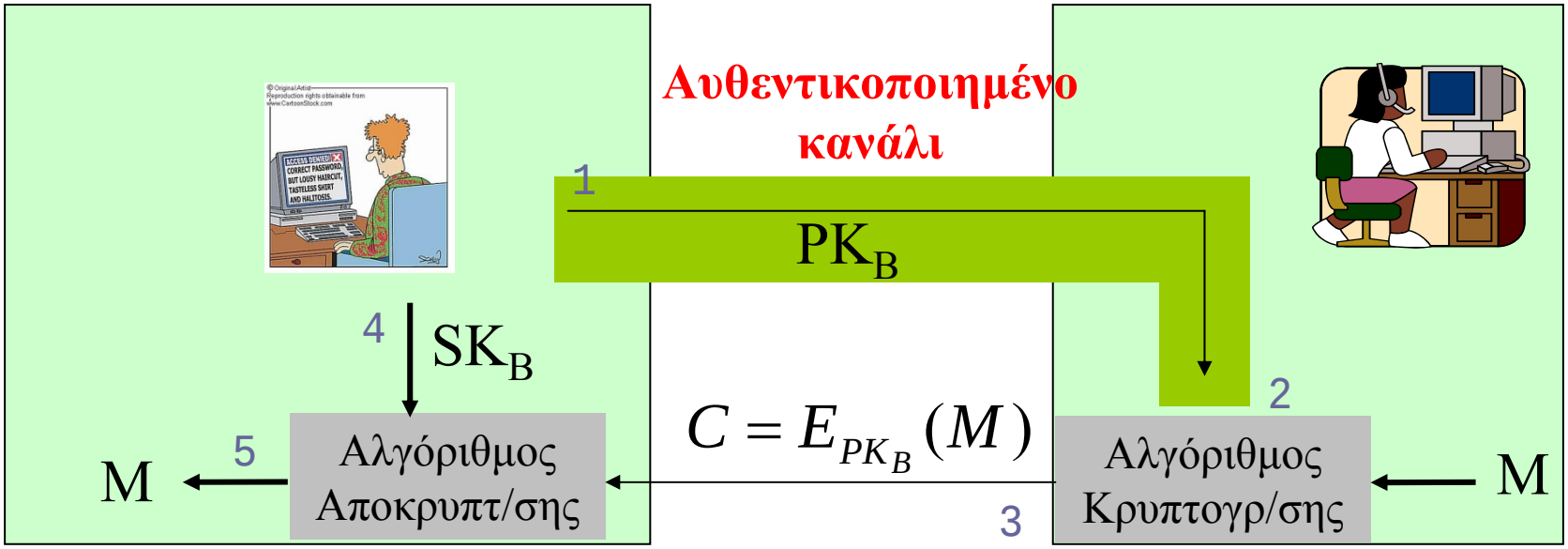


- Εάν ο **X** θέλει να επικοινωνήσει με τον **Y** επικοινωνεί με το ΚΔΚ, το οποίο δημιουργεί και στέλνει και στους δύο ένα κοινό κλειδί K_{XY}

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: **2n** κλειδιά
- Ανταλλαγή κλειδιών
  - Δεν απαιτείται εμπιστευτικότητα κατά την ανταλλαγή κλειδιού
  - Απαιτείται όμως αυθεντικότητα αποστολέα – παραλήπτη

Πιθανή λύση: Έμπιστη Οντότητα και Ψηφιακά Πιστοποιητικά

- Χρήση μίας *Έμπιστης Τρίτης Οντότητας - ΕΤΟ (Trusted Third Party – TTP)* η οποία αυθεντικοποιεί τα δημόσια κλειδιά όλων των χρηστών
  - Όλοι οι χρήστες γνωρίζουν μόνο το δημόσιο κλειδί της ΕΟ: PK_{TTP}
  - Κάθε χρήστης Χ στέλνει το δημόσιο κλειδί του PK_X στην ΕΤΟ
- Η ΕΤΟ **υπογράφει ψηφιακά** ένα μήνυμα το οποίο περιλαμβάνει
  - Την ταυτότητα (ένα μοναδικό προσδιοριστικό) του χρήστη Χ: ID_X
  - Το δημόσιο κλειδί του χρήστη Χ: PK_X
  - Την ημερομηνία της υπογραφής t_o και της λήξης t_1

Όλα τα παραπάνω υπογράφονται με το μυστικό κλειδί SK_{TTP} της ΕΤΟ

$$CERT_X = [ID_X, PK_X, t_o, t_1, \text{SIG}_{SK_{TTP}}(ID_X, PK_X, t_o, t_1)]$$

3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

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

Υποδομή Δημόσιας Κλείδας – ΥΔΚ
Public Key Infrastructure - PKI

Μία ΥΔΚ είναι:

- Ένα σύνολο *ψηφιακών πιστοποιητικών των Αρχών Πιστοποίησης και άλλων υπηρεσιών*, οι οποίες *επιβεβαιώνουν και αυθεντικοποιούν κάθε εμπλεκόμενο μέρος* σε μία δικτυακή συναλλαγή»
- *Υπόβαθρο ανάπτυξης κρυπτοσυστημάτων δημόσιου κλειδιού* για τη παροχή λειτουργιών 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*
- *Υπηρεσία Πιστοποίησης (Certification)*
- *Υπηρεσία Ανάκλησης (Revocation)*
- *Υπηρεσία Χρονοσφράγισης (Time-stamping)*
- *Υπηρεσία Διαπιστοποίησης*

Υπηρεσία Εγγραφής

- 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

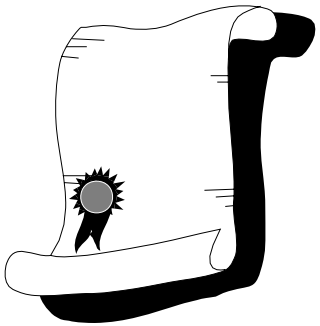
- Αναλαμβάνει την έκδοση και προσωποποίηση ζεύγους κλειδιών
- Διανομή κλειδιών
- Αποθήκευση κλειδιών
- (Πιθανώς) Ανάκτηση κλειδιών σε περίπτωση απώλειας
- Τα ιδιωτικά κλειδιά πρέπει να διαφυλάσσονται σε ασφαλή μέσα, όπως έξυπνες κάρτες

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:
Data:
Version: 3 (0x2)
Serial Number: 2 (0x0)
Signature Algorithm: sha1withRSAEncryption
Issuer: C=GR, SP=ATTIKH, L=Piraeus, O=UNIPI,
OU=Security Dept., CN=DemoCA,
Validity
Not Before: Sep 14 17:15:25 2010 GMT
Not After : Dec 14 17:15:25 2010 GMT
Issuer: C=GR, SP=ATTIKH, , L=Piraeus, O=UNIPI,
OU=Security Dept., CN=Panagiotis K,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Modulus:
00:9a: …… :8a:67
Exponent: 65537 (0x10001)
Signature Algorithm: sha1withRSAEncryption
0e:28:…...70:e3

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
  - Δεν ισχύουν πλέον για λόγους ασφάλειας ή για άλλες αιτίες
- Η αξιοπιστία των CRL έγκειται στο ότι είναι ψηφιακά υπογεγραμμένες (συνήθως από τον εκδότη των πιστοποιητικών)

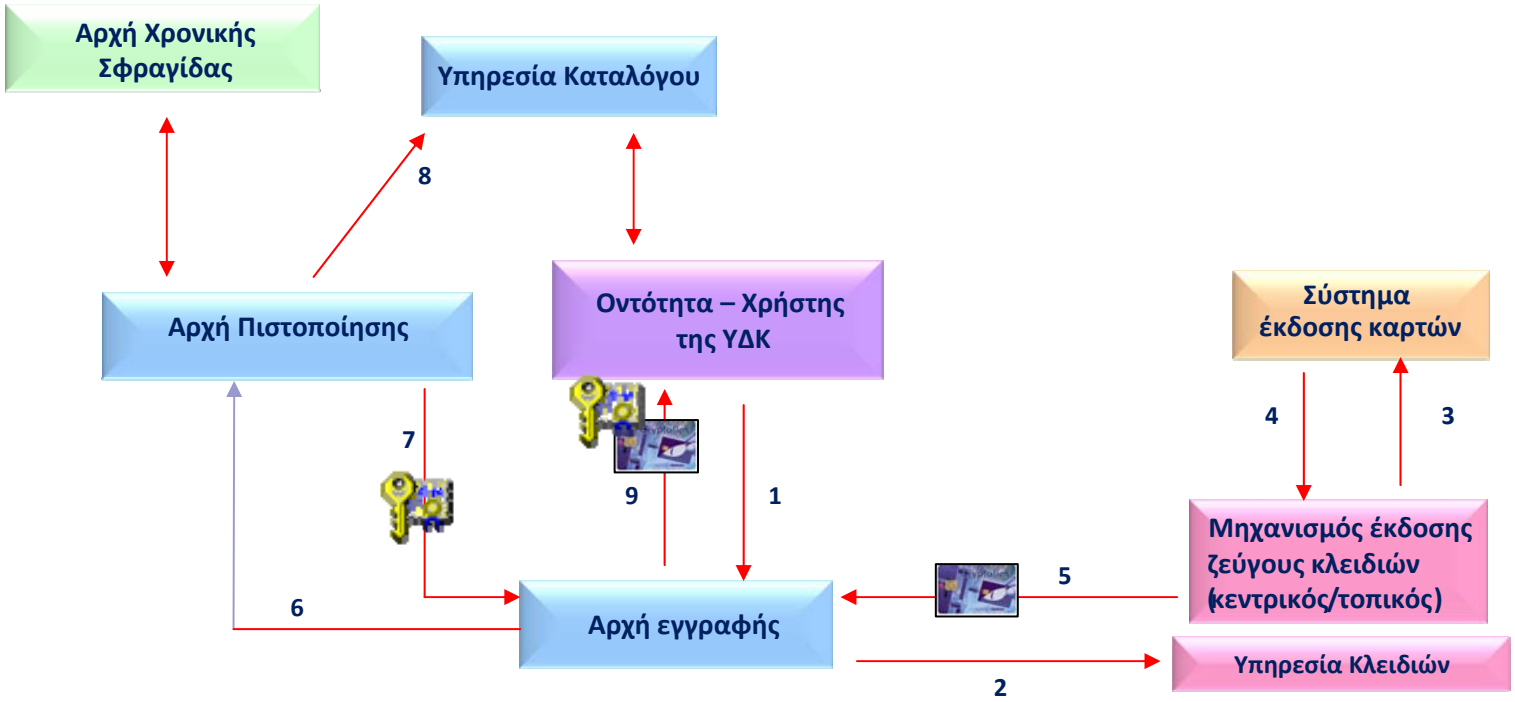
Υπηρεσία Χρονοσφράγισης

- 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*.

Υπηρεσία Διαπιστοποίησης

- Ως «δια-πιστοποιητικό» 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.

Γενικό Πλαίσιο ΥΔΚ



Γνωστοί Πάροχοι Υπηρεσιών Πιστοποίησης (Αρχές Πιστοποίησης)

Στην Ευρώπη:

- France Telecom & Gemplus
- BT & Verisign
- Racal Telecom
- AT&T, Deutsche Telecom, Telecom Italia
- Vodafone

Στην Ελλάδα:

- ΕΕΤΤ
- ACCI& National Bank of Greece & Alpha Credit Bank
- Telecom Italia & Forthnet
- Data Media & Eurobank

3η θεματική ενότητα

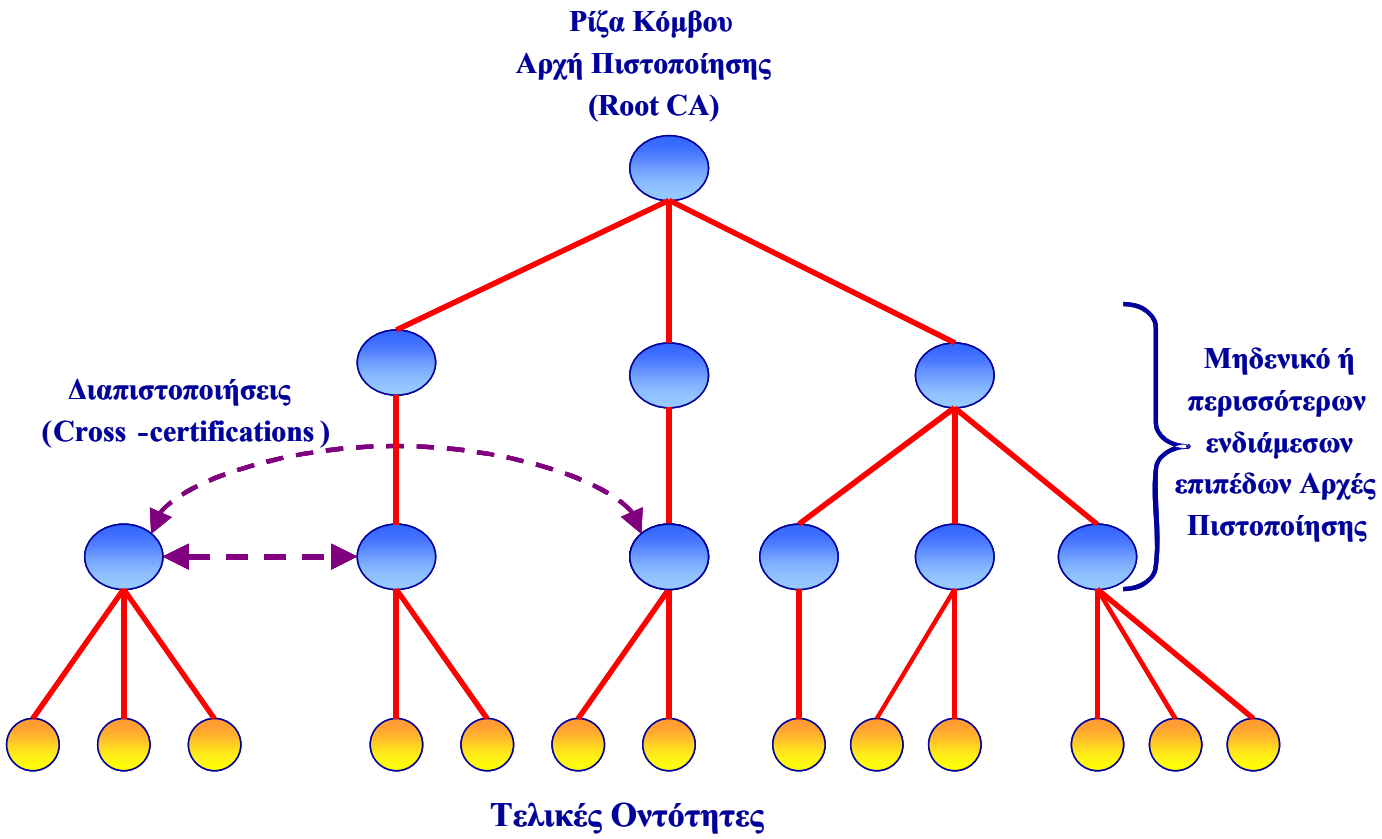
Υποδομή Δημόσιας Κλείδας

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

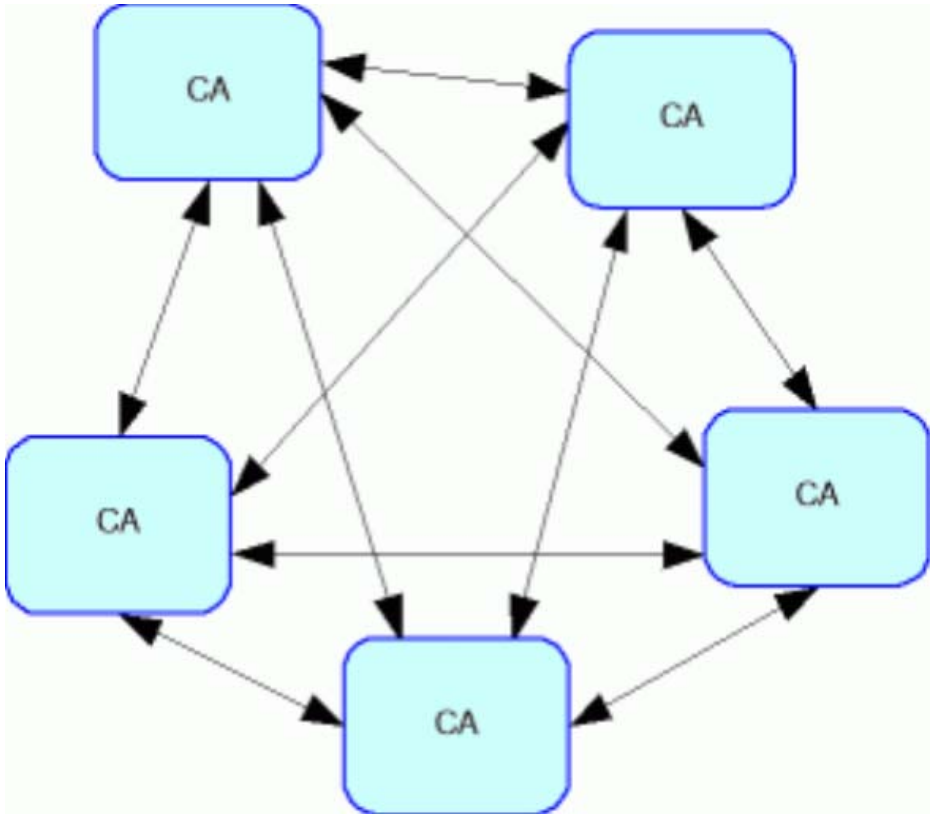
Οργανωτικές Δομές

- 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)*

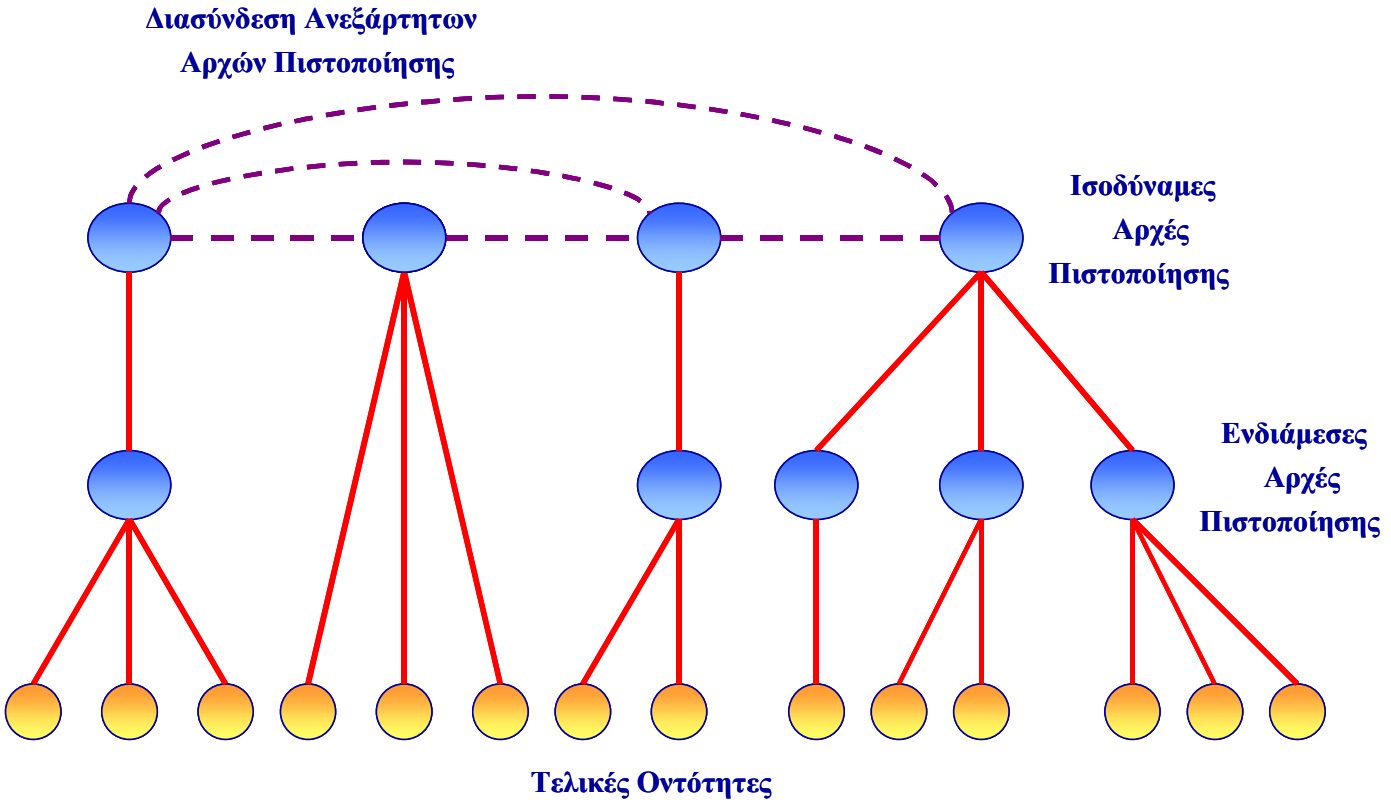
Ιεραρχικό μοντέλο (Hierarchical model)



Πλήρως κατανεμημένο μοντέλο (Mesh model)



Υβριδικό ή μερικώς κατανεμημένο μοντέλο



3η θεματική ενότητα

Υποδομή Δημόσιας Κλείδας

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

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)

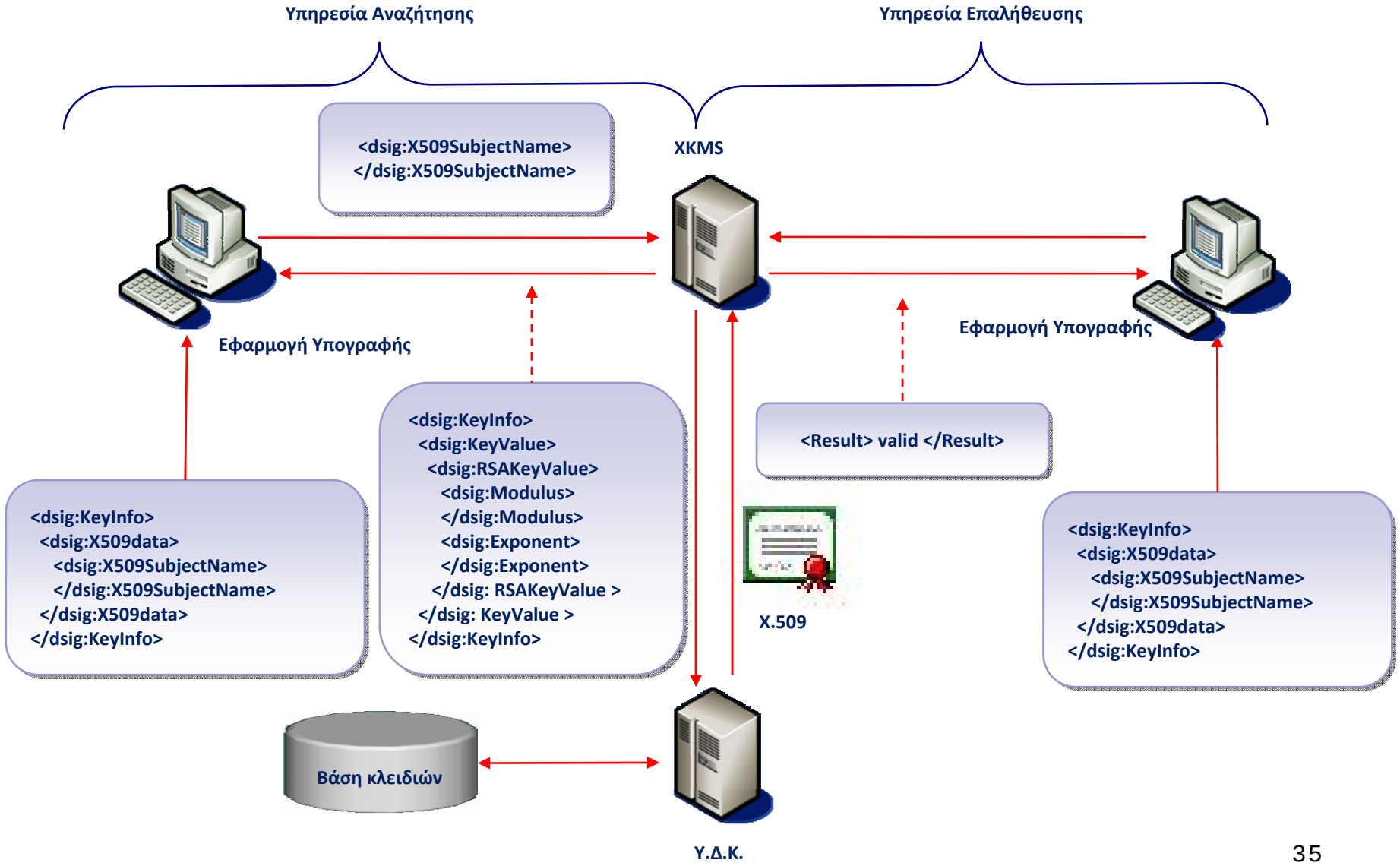
Διαδικασίες ΥΔΚ 1ης γενιάς

- 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 (overhead)
  - Η ανταλλαγής 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
- **Νομικό πλαίσιο**
- Πολιτική ασφάλειας / Δήλωση πρακτικών πιστοποίησης

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.

Εγγεγραμμένες Α.Π. στο μητρώο της ΕΕΤΤ

http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/EsignProviders.html

Ημερ. Καταχώρησης	Ονοματε-πώνυμο/ επωνυμία	Διεύθυνση /έδρα	Τηλέφωνο	Fax	Email	Ιστοσελίδα	Παρεχόμενες Υπηρεσίες	Παροχή αναγνωρισμένων πιστοποιητικών κατά δήλωση του παρόχου
10-9-2002	ΤΡΑΠΕΖΑ EFG EUROBANK ERGASIAS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ	ΟΘΩΝΟΣ 8, ΑΘΗΝΑ	210 3337000	210 3233866	info@ eurobank.gr	eurobank.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ
1-10-2002	ΑΝΤΑΚΟΜ-ΠΡΟΗΓΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ ΔΙΑΔΙΚΤΥΟΥ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ	ΚΡΕΟΝΤΟΣ 25, Τ.Κ. 10442 ΑΘΗΝΑ	210 5193740	210 5193555	info@ adacom.com	adacom.com	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΝΑΙ
29-1-2003	ΕΜΠΟΡΙΚΟ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ(ΕΒΕΑ)	ΑΚΑΔΗ-ΜΙΑΣ 7, Τ.Κ. 106 71 ΑΘΗΝΑ	210 3382203	210 3619421	info@ acci.gr	acci.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ
18-3-2005	EDPS ΕΠΕΞΕΡΓΑΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΤΗΛΕΜΑΤΙΚΗΣ ΑΕ	Λ. ΒΟΥΛΙΑ ΓΜΕΝΗΣ & ΔΙΓΕΝΗ 43, Τ.Κ. 166 73 ΒΟΥΛΑ	210 8993660	210 8993662	info@ edps.gr	edps.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ
17-3-2006	ΧΡΗΜΑΤΙ-ΣΤΗΡΙΟ ΑΘΗΝΩΝ ΑΕ	ΛΕΩΦΟ-ΡΟΣ ΑΘΗΝΩΝ 110, 104 42, ΑΘΗΝΑ	210 3366300	210 3366301	PKICA-Services@ helex.gr	ase.gr/ repository	Παροχή πιστοποιητικών / Ενημέρωση εισηγμένων στο Χρηματιστήριο Αθηνών	ΝΑΙ
20-6-2007	Αρχή Πιστοποίησης Ελληνικού Δημοσίου	ΒΑΣ. ΣΟΦΙΑΣ 15, ΑΘΗΝΑ 10674	213 1313000	210 3646670		ypesdda. gov.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΝΑΙ
21-11-07	ΓΕΝΙΚΗ ΤΡΑΠΕΖΑ Τ ΗΣ ΕΛΛΑΔΟΣ Α.Ε.	Μεσογείων 109-111, Αμπελό-κηποι, 11510	210 6975000	210 6975539	info@ geniki.gr	geniki.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ
15-4-2009	ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ	Πάροδος Αριστοτέλους 18, Περίβολα Πάτρα 26335	2610 367380	2610 367376	support@ eap.gr	eap.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ
18-1-2010	ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΑΕ	Ηλιουπόλεως 2-4, ΥΜΗΤΤΟΣ, 172 37	213 1300700	213 1300801	info@ktpae.gr	www.ktpae.gr	Παροχή πιστοποιητικών και συναφών υπηρεσιών	ΟΧΙ

3η θεματική ενότητα

2. Υποδομή Δημόσιας Κλείδας

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

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

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

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.