Υποδομές Δημόσιας Κλείδας

Τεχνολογιες Διαχειρισης Ασφαλειας (ΤεΔΑ) - ΠΜΣ Προηγμενα Συστηματα Πληροφορικης

δρ. Καραντζιας Θανος

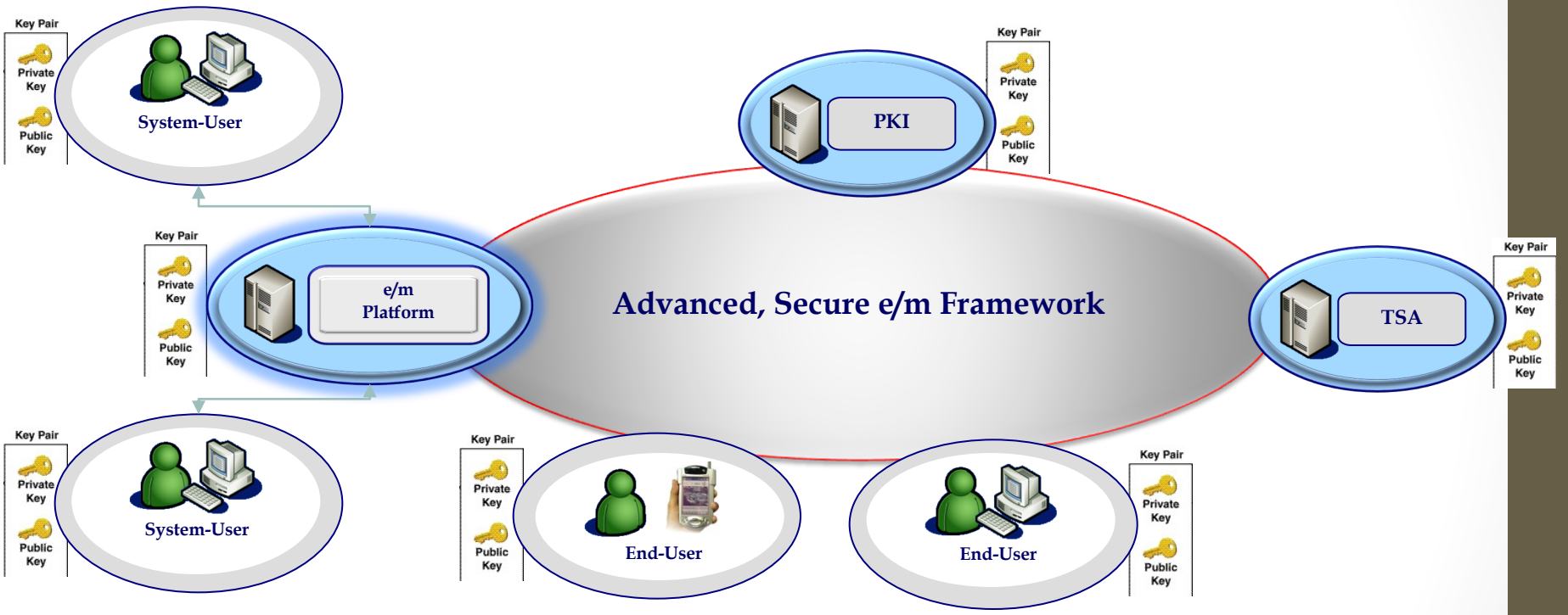
Περιεχόμενα

- Υ.Δ.Κ. & Πάροχοι Υπηρεσιών Πιστοποίησης
- Υπηρεσίες Πιστοποίησης
- Γενικό Πλαίσιο Παρόχων Υπηρεσιών Πιστοποίησης
- Μοντέλα Εμπιστοσύνης & Αρχιτεκτονικές Υ.Δ.Κ.
- Νομικό Πλαίσιο
- Γνωστοί Πάροχοι Υπηρεσιών Πιστοποίησης

Υ.Δ.Κ. & Πάροχος Υπηρεσιών Πιστοποίησης

- «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 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».

Προηγμένα-Ασφαλή η/α-Πλαίσια



Υπηρεσίες Πιστοποίησης

- **Εγγραφή**:
  - 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 Κλειδιών**: Η υπηρεσία που αναλαμβάνει:
  - Την έκδοση/ προσωποποίηση ζεύγους κλειδιών
  - Την διανομή/αποθήκευση/ανάκτηση κλειδιών: τα ιδιωτικά κλειδιά πρέπει να διαφυλάσσονται σε ασφαλή μέσα, όπως έξυπνες κάρτες

Υπηρεσίες Πιστοποίησης

Πιστοποίηση:

- Έκδοση πιστοποιητικών για το δημόσιο κλειδί των εγγεγραμμένων χρηστών και η διασφάλιση της ακεραιότητας για την κατάσταση των πιστοποιητικών αυτών μέσω αποτελεσματικής διαχείρισής τους.
- Η εκτέλεση της υπηρεσίας πιστοποίησης γίνεται από ειδική αρχή της ΥΔΚ που καλείται ***Αρχή Πιστοποίησης***

Αρχή Πιστοποίησης

Βασικές Λειτουργίες Αρχής Πιστοποίησης

- Έκδοση/Ανανέωση πιστοποιητικών βάσει συγκεκριμένων προτύπων.
- Διανομή πιστοποιητικών στους χρήστες.
- Αποθήκευση πιστοποιητικών στο Κατάλογο για κοινή χρήση.
- Ανάκληση πιστοποιητικών με έκδοση *Λίστας ανάκλησης πιστοποιητικών*, η οποία περιέχει όλα τα πιστοποιητικά που δεν ισχύουν ή που έχουν λήξει .

Υπηρεσίες Πιστοποίησης

- **Υπηρεσία Καταλόγου**: Η υπηρεσία αυτή μέσω κατάλληλου *Εξυπηρετητή Καταλόγου (Directory Server)* χρησιμοποιείται για 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

Λίστες Ανάκλησης Πιστοποιητικών

- **Certificate Revocation Lists (CRLs)**
- Οι CRLs είναι υπογεγραμμένες δομές δεδομένων που περιέχουν μια λίστα από ανακαλούμενα πιστοποιητικά.
- Η αξιοπιστία των CRL έγκειται στο ότι είναι ψηφιακά υπογεγραμμένες (συνήθως από τον εκδότη των πιστοποιητικών)

Υπηρεσίες Πιστοποίησης

Υπηρεσία Χρονοσφράγισης:

- Η υπηρεσία που σχετίζεται με την επικόλληση ημερομηνίας και ώρας σε δεδομένα, με σκοπό την απόδειξη ότι τα τελευταία 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.

Αρχιτεκτονική Υ.Δ.Κ.

Βασικοί παράγοντες που επηρεάζουν τις αρχιτεκτονικές Υ.Δ.Κ.:

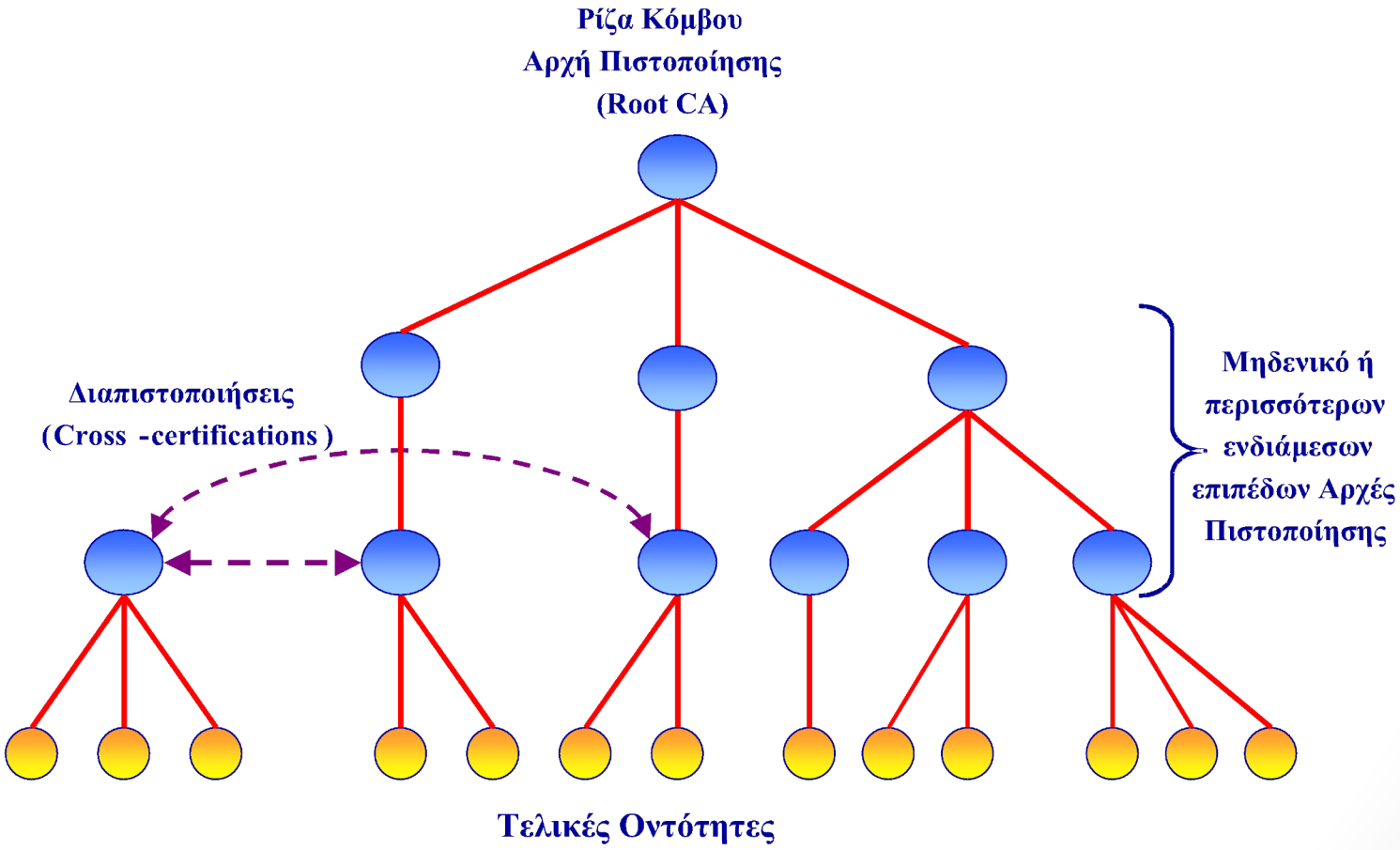
- Τύποι εμπλεκόμενων οντοτήτων και ανάγκες πιστοποίησης.
- Προφίλ πιστοποιητικών και ειδικές απαιτήσεις
- Οντότητες που λειτουργούν ως Αρχές Πιστοποίησης και Εγγραφής.
- Μέθοδος διάθεσης/δημοσίευσης πιστοποιητικών και δημόσιων κλειδιών

Πολιτική Πιστοποιητικού

- «*ένα σύνολο κανόνων που καθορίζουν τη δυνατότητα εφαρμογής ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα ή/και ομάδα χρηστών με κοινές απαιτήσεις ασφαλείας*»
- *Περιλαμβάνει το προφίλ των πιστοποιητικών* της ΥΔΚ:
  - Θέματα αναγνώρισης
  - Θέματα εγγραφής χρηστών
  - Θέματα έκδοσης
  - Θέματα διανομής
  - Θέματα διάθεσης
  - Θέματα ανάκλησης

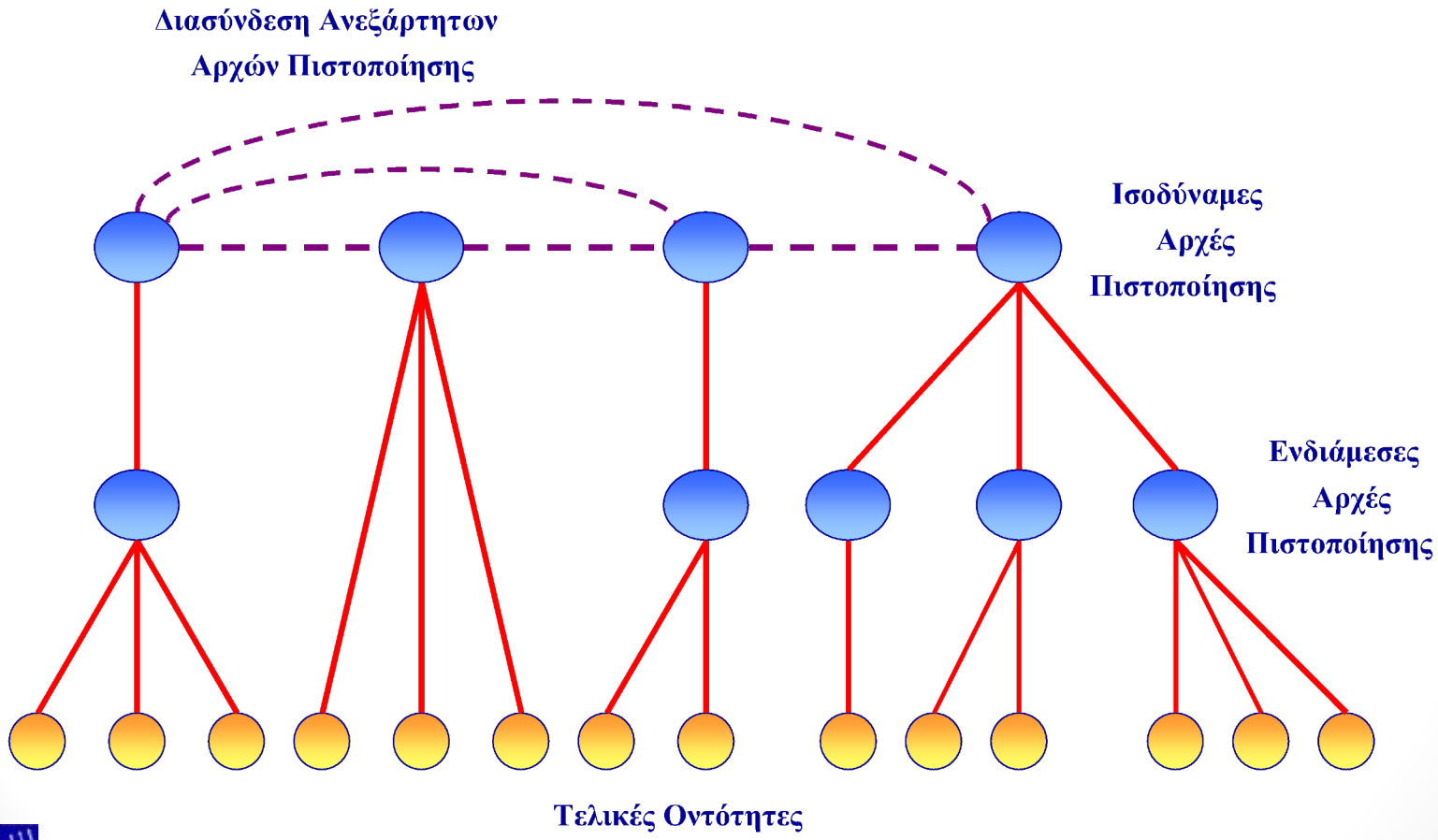
Μοντέλα Εμπιστοσύνης

Ιεραρχικό Μοντέλο



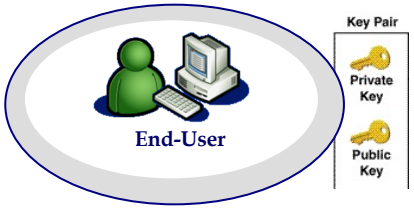
Μοντέλα Εμπιστοσύνης

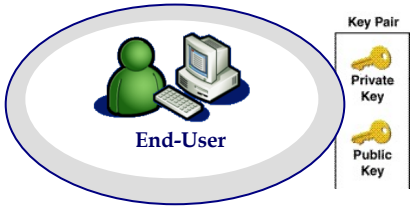
Κατανεμημένο Μοντέλο



Μοντέλα Εμπιστοσύνης

Μοντέλο Χρήστη: Καθένας από τους χρήστες είναι απευθείας και ολοκληρωτικά υπεύθυνος στο να αποφασίσει ποια πιστοποιητικά μπορεί να εμπιστευτεί και ποια όχι.





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).
  - Αναμένεται τεχνική επεξεργασία του Διατάγματος για λειτουργία διαπιστευμένων Αρχών Πιστοποίησης.
- Το ΠΔ 150/2001 θα πλαισιωθεί με τεχνικές προδιαγραφές βασισμένες στις τεχνολογίες ΥΔΚ
- Η ΕΕΤΤ θα είναι ο υπεύθυνος εποπτικός, ελεγκτικός οργανισμός ο οποίος θα παρέχει εθελοντική διαπίστευση στους ΠΥΠ.
- Οι ΠΥΠ θα πρέπει να είναι νομικά και επιχειρησιακά συμβατοί με το ΠΔ.
- 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 Π.Υ.Π.

Στην Ευρώπη:

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

Στην Ελλάδα:

- EETT
- ACCI& National Bank of Greece @Alpha Credit Bank
- Telecom Italia & Forthnet
- National Committee of Greek Telecoms & Post Offices
- Data Media & Eurobank

Βιβλιογραφία

C. Adams, S.Lloyd, “*Understanding Public-Key Infrastructure*” MacMillan Technical Publishing 1999

Ευχαριστώ
για την προσοχή σας!!

Επικοινωνία: karant@unipi.gr

Ενημέρωση: http://athina.cs.unipi.gr/site-ergastirio/asfaleia/index.html