Η Αρχή Πιστοποίησης των Ελληνικών Ακαδημαϊκών Ιδρυμάτων (HARICA)

Δρ. Σπύρος Μπόλης

Η GUnet

- **Αστική, μη κερδοσκοπική Εταιρεία**
- **Μέλη όλα τα Ακαδημαϊκά Ιδρύματα**
- **Σκοποί :**
  - Συντονισμός, ανάπτυξη, διάχυση και προαγωγή προηγμένων δικτυακών υπηρεσιών και εφαρμογών.
  - Παροχή υπηρεσιών στα μέλη της και σε οποιοδήποτε τρίτο.
  - Συμμετοχή σε αναπτυξιακά, εκπαιδευτικά και ερευνητικά προγράμματα.
  - Ανάπτυξη συνεργασιών με αντίστοιχα ακαδημαϊκά, ερευνητικά και εκπαιδευτικά δίκτυα άλλων χωρών.

Υποδομή Δημοσίου Κλειδιού

Η **Υποδομή Δημόσιου Κλειδιού (Public-Key Infrastructure (PKI))** είναι ένα σύστημα για τη:

- δημιουργία
- αποθήκευση και
- διανομή

Ψηφιακών Πιστοποιητικών

Κατηγορίες Ψηφιακών Πιστοποιητικών

- **Προσωπικά Ψηφιακά Πιστοποιητικά**
- **Ψηφιακά Πιστοποιητικά Εξυπηρετητών**
- **Ψηφιακά Πιστοποιητικά Ειδικών Χρήσεων**

Προσωπικά Ψηφιακά Πιστοποιητικά - Ι

Ασφαλές Ηλεκτρονικό Ταχυδρομείο (μέσω Mozilla Thunderbird, Microsoft Outlook, Apple mailApp, εφαρμογές κινητών τηλεφώνων)

- Επιβεβαίωση Ταυτότητας (Authentication)
- Ακεραιότητα (Integrity)
- Μη Απόρριψη Υποχρέωσης (Non-repudiation)
- Εμπιστευτικότητα (Confidentiality)

Προσωπικά Ψηφιακά Πιστοποιητικά - ΙΙ

Υπογραφή Ψηφιακών Κειμένων (Μορφές PDF, MS Word, κ.α.)

- Επιβεβαίωση Ταυτότητας (Authentication)
- Ακεραιότητα (Integrity)
- Μη Απόρριψη Υποχρέωσης (Non-repudiation)

Ψηφιακά Πιστοποιητικά Εξυπηρετητών

Πλοήγηση σε ασφαλείς ιστοχώρους (SSL) με τη χρήση σύγχρονων φυλλομετρητών (Firefox, Internet Explorer, Chrome, πλοηγοί κινητών τηλεφώνων)

- Επιβεβαίωση Ταυτότητας Διακομιστή (Authentication)
- Ακεραιότητα (Integrity)
- Εμπιστευτικότητα (Confidentiality)

Ψηφιακά Πιστοποιητικά Ειδικών Χρήσεων

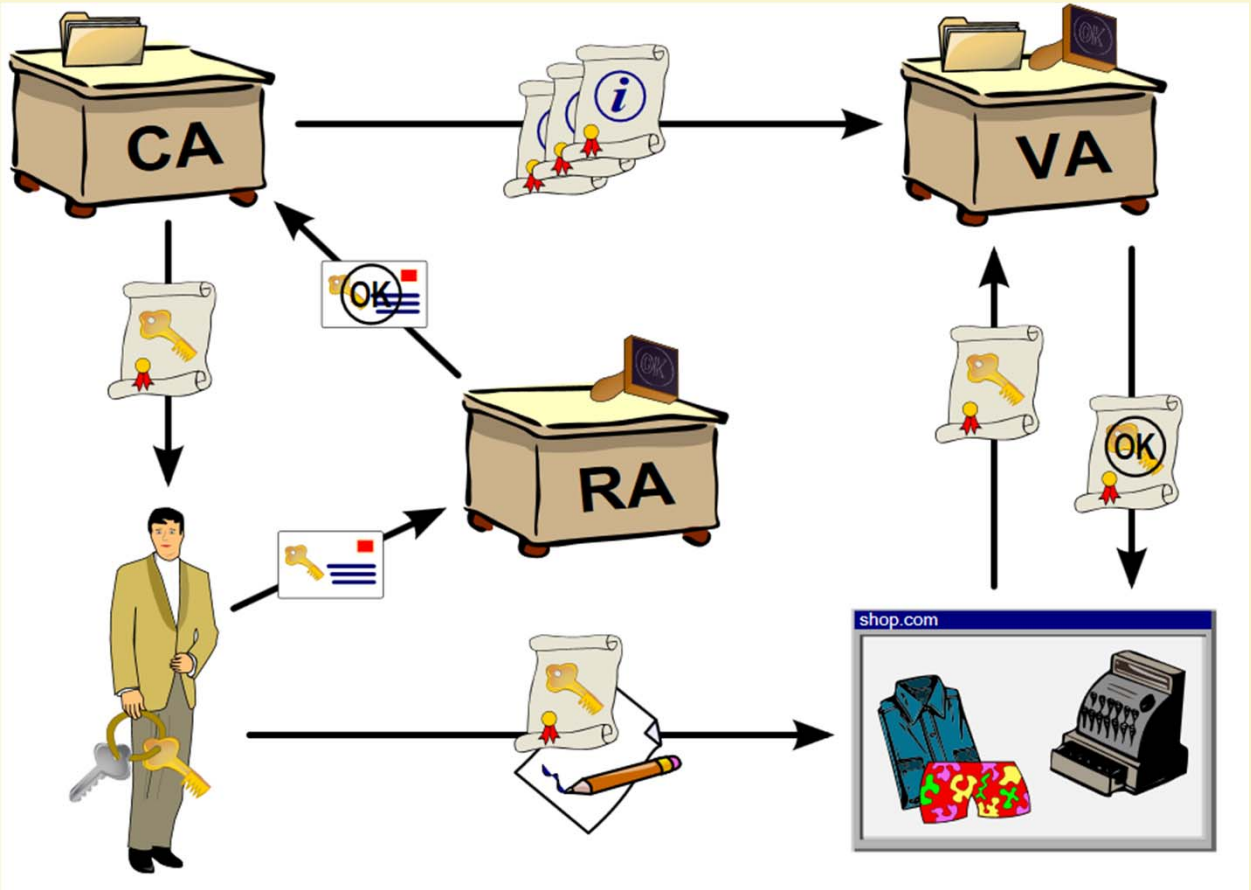
Πιστοποιητικά που επιτρέπουν άλλες χρήσεις ή περιέχουν επεκτάσεις χαρακτηριστικών (extended attributes)

- Υπογραφή κώδικα λογισμικού

Υποδομή Δημοσίου Κλειδιού - Ι

- Αρχή Πιστοποίησης (CA) η οποία εκδίδει και πιστοποιεί τα Ψηφιακά Πιστοποιητικά
- Αρχή Καταχώρησης (RA) η οποία πιστοποιεί την ταυτότητα των χρηστών
- Κεντρικός Κατάλογος που αποθηκεύει τα πιστοποιητικά

Υποδομή Δημοσίου Κλειδιού - II

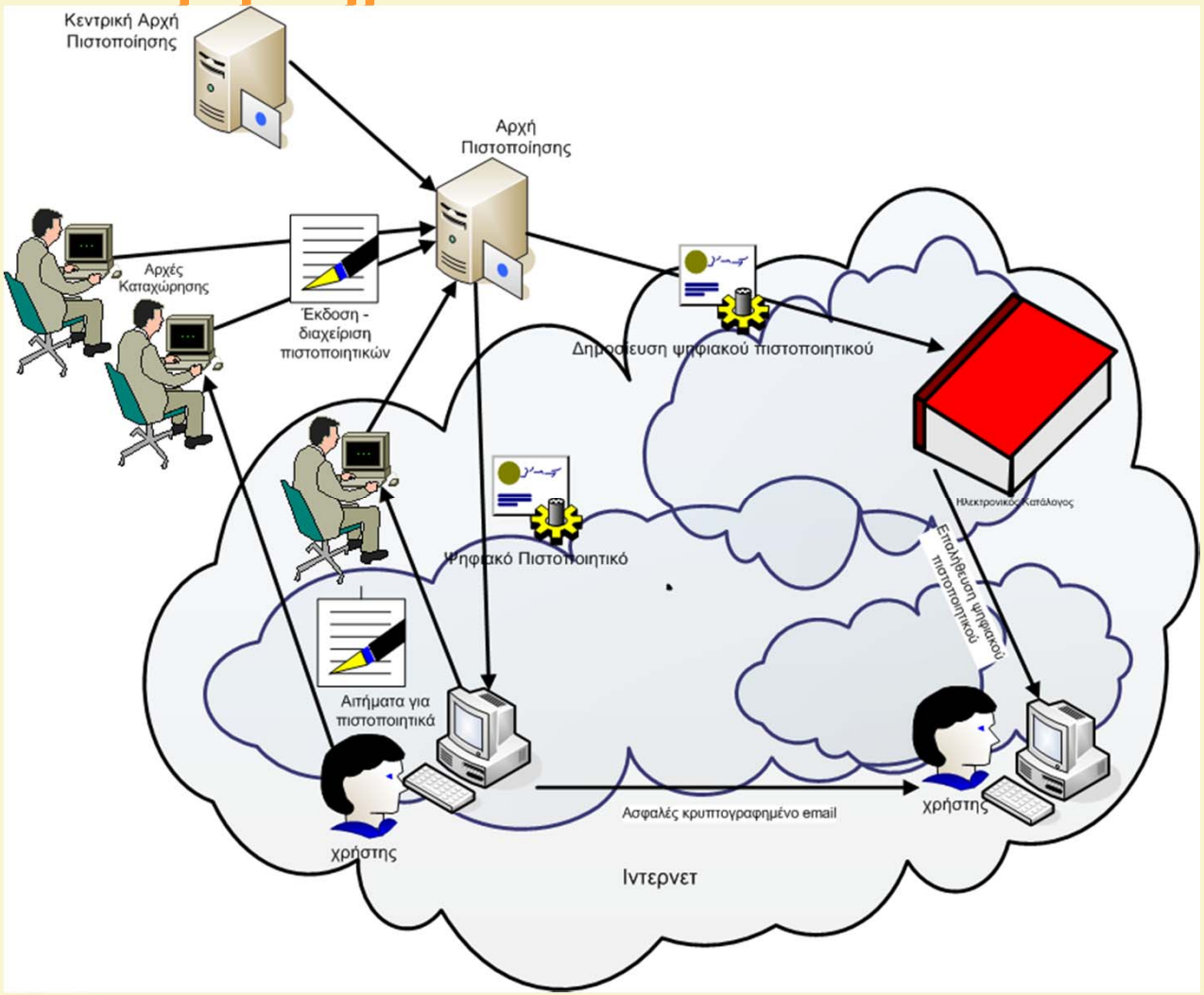


Υποδομή Δημοσίου Κλειδιού HARICA - I

Ιεραρχική Υποδομή

- Κορυφαία Αρχή Πιστοποίησης (HARICA)
- Αρχή Πιστοποίησης Ιδρύματος
- Αρχή Καταχώρησης Ιδρύματος (LDAP)
- Κεντρικός Κατάλογος

Υποδομή Δημοσίου Κλειδιού HARICA - II



Μνημόνιο Συνεργασίας

Στα πλαίσια της HARICA έχουν υπογράψει οι ακόλουθοι 24 φορείς:

- Ακαδημαϊκό Διαδίκτυο GUNET
- Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
- Γεωπονικό Πανεπιστήμιο Αθηνών
- Δημοκρίτειο Πανεπιστήμιο Θράκης
- Εθνικό Δίκτυο Έρευνας και Τεχνολογίας
- Εθνικό Κέντρο Έρευνας και Τεχνολογικής Ανάπτυξης
- Εθνικό Κέντρο Τεκμηρίωσης
- Εθνικό Μετσόβιο Πολυτεχνείο
- Ιόνιο Πανεπιστήμιο
- Πανεπιστήμιο Αιγαίου
- Πανεπιστήμιο Θεσσαλίας
- Πανεπιστήμιο Ιωαννίνων
- Πανεπιστήμιο Κρήτης
- Πανεπιστήμιο Πειραιά
- Πανεπιστήμιο Στερεάς Ελλάδας
- Πολυτεχνείο Κρήτης
- ΤΕΙ Αθήνας
- ΤΕΙ Ηπείρου
- ΤΕΙ Καλαμάτας
- ΤΕΙ Κρήτης
- ΤΕΙ Λαμίας
- ΤΕΙ Λάρισας
- ΤΕΙ Μεσολογγίου
- ΤΕΙ Σερρών

Υπηρεσίες

- Πιστοποιεί τις Αρχές Πιστοποίησης των Ιδρυμάτων
- Εκδίδει -για λογαριασμό των μελών του- ψηφιακά πιστοποιητικά για τους εξυπηρετητές του δικτύου.
- Εκδίδει -για λογαριασμό των μελών του- ψηφιακά πιστοποιητικά για τους χρήστες του δικτύου.

Αρχές Πιστοποίησης

Έχει εκδοθεί πιστοποιητικό Αρχής Πιστοποίησης για τα εξής 13 ιδρύματα:

- Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
- Εθνικό Κέντρο Τεκμηρίωσης
- Πανεπιστήμιο Θεσσαλίας
- Πανεπιστήμιο Κρήτης
- Πανεπιστήμιο Πειραιά
- Πανεπιστήμιο Στερεάς Ελλάδας
- ΤΕΙ Ηπείρου
- ΤΕΙ Καλαμάτας
- ΤΕΙ Κρήτης
- ΤΕΙ Λαμίας
- ΤΕΙ Λάρισας
- ΤΕΙ Μεσολογγίου
- ΤΕΙ Σερρών

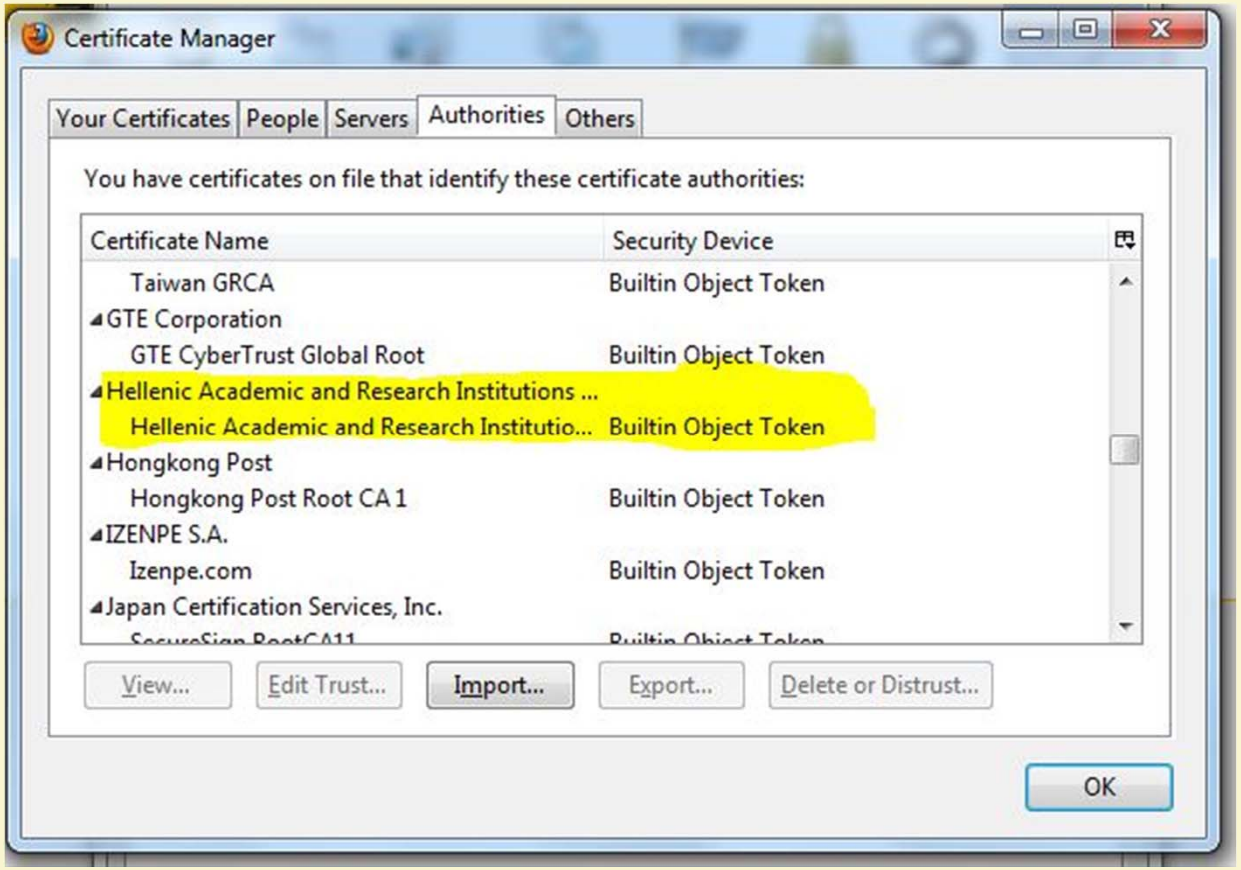
Τεχνολογικά Χαρακτηριστικά

- Η Υποδομή Δημοσίου Κλειδιού HARICA συμμορφώνεται πλήρως με τις απαιτήσεις του προτύπου ETSI TS 101 456 («Policy requirements for certification authorities issuing qualified certificates»)
- Είναι η πρώτη ΥΔΚ που στο πιστοποιητικό κορυφαίας Αρχής Πιστοποίησης χρησιμοποιεί προηγμένα χαρακτηριστικά ασφάλειας (Name Constraints σύμφωνα με το RFC 5280)

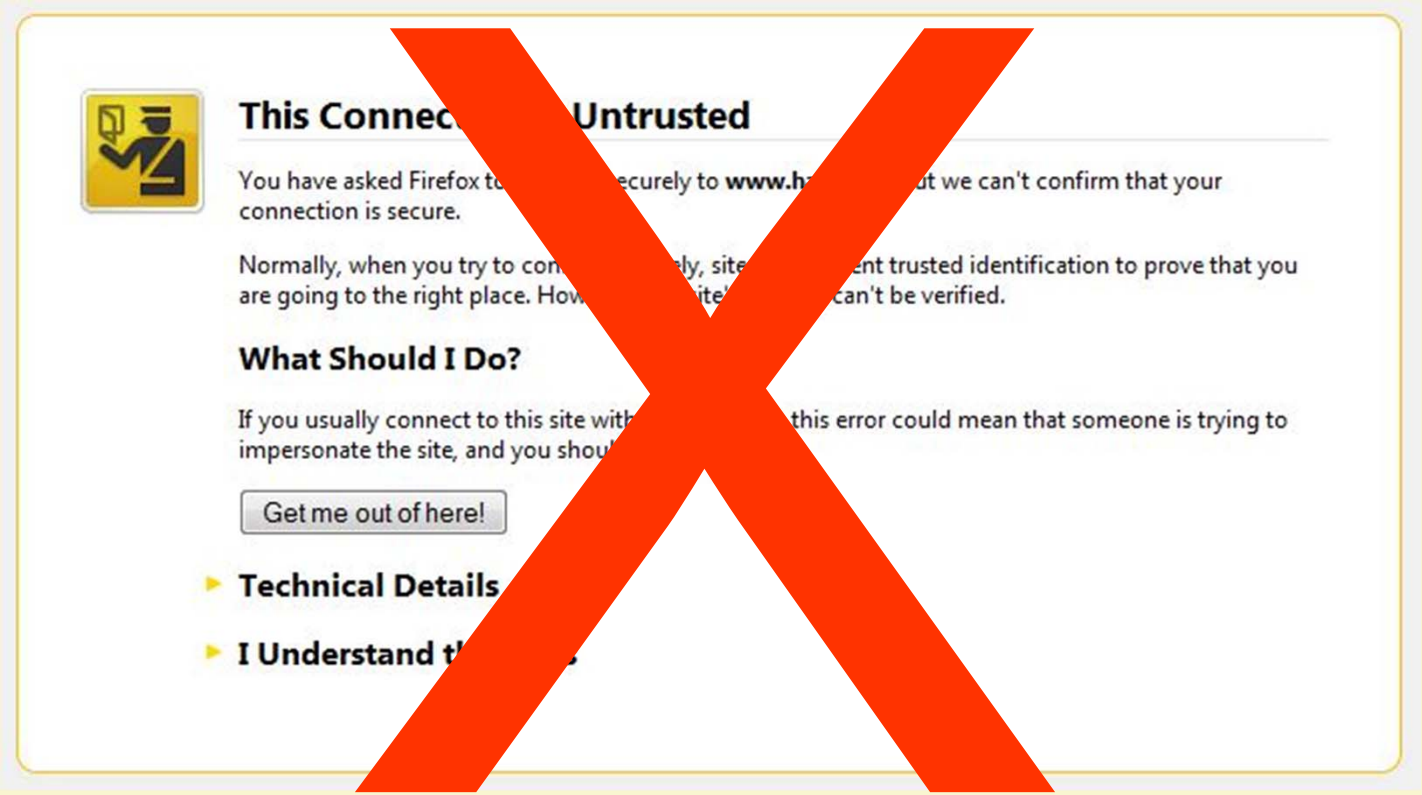
Πιστοποιητικό Κορυφαίας Αρχής Πιστοποίησης - Ι

- **Το πιστοποιητικό της HARICA βρίσκεται ήδη προεγκατεστημένο στο αποθετήριο NSS (έκδοση 3.13.2 ή νεότερη) το οποίο χρησιμοποιείται από τα ακόλουθα προγράμματα:**
  - Mozilla Firefox
  - Mozilla Thunderbird
  - Libre Office
  - Πλειοψηφία Linux Distributions
  - Server προϊόντα από Sun Java Enterprise System

Πιστοποιητικό Κορυφαίας Αρχής Πιστοποίησης - ΙΙ



Πιστοποιητικό Κορυφαίας Αρχής Πιστοποίησης - III



Πιστοποιητικό Κορυφαίας Αρχής Πιστοποίησης - IV

- **Έχουν γίνει αιτήσεις για ένταξη στο αποθετήριο των Microsoft και Apple**
  - Η διαδικασία ένταξης στο αποθετήριο της Microsoft βρίσκεται σε προχωρημένο στάδιο με προοπτική ένταξης τον Ιούνιο 2012
  - Η διαδικασία ένταξης στο αποθετήριο της Apple έχει ξεκινήσει αλλά βρίσκεται σε πρώιμο στάδιο

Εκδοθέντα Πιστοποιητικά

- **Συνολικά όλα τα ιδρύματα από τον Ιούλιο του 2006 ως τώρα έχουν εκδώσει:**
  - 19.041 πιστοποιητικά χρηστών
  - 734 πιστοποιητικά διακομιστών
- **Η HARICA έχει ανακαλέσει**
  - 9.734 πιστοποιητικά χρηστών
  - 171 πιστοποιητικά διακομιστών

Ευχαριστώ για την προσοχή σας

Ερωτήσεις;

http://www.harica.gr
Mail: ca@harica.gr