

# Διαχείριση ταυτότητας & Ψηφιακή υπογραφή

Εφαρμογή στο Ηλεκτρονικό πρωτόκολλο

27/10/2011

Σχεδίαση και Ανάπτυξη για το ΕΚΕΦΕ - Δ.  
Χαράλαμπος Κουτσούρης, MSc. CISA, CISSP  
Κέντρο Δικτύου - Ινστιτούτο Πληροφορικής & Τηλ.  
[noc@ariadne-t.gr](mailto:noc@ariadne-t.gr), 2106503125

# Αντζέντα – Διαχείριση ταυτότητας & Ψηφιακή υπογραφή

- ▶ Σημασία για τους χρήστες
- ▶ Κεντρική διαχείριση ταυτότητας στο Δημόκριτο
- ▶ Ψηφιακά πιστοποιητικά / υπογραφή – Τεχνολογία
  - Παραδείγματα χρήσης
- ▶ Έκδοση και χρήση προσωπικού πιστοποιητικού
- ▶ ΑΔΕΙΑ ΧΡΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΥΠΟΧΡΕΩΣΕΙΣ
- ▶ Προστασία πιστοποιητικού και υπογραφής
- ▶ Πιστοποιητικά ηλεκτρονικών υπηρεσιών (Web services)
- ▶ Σύνοψη

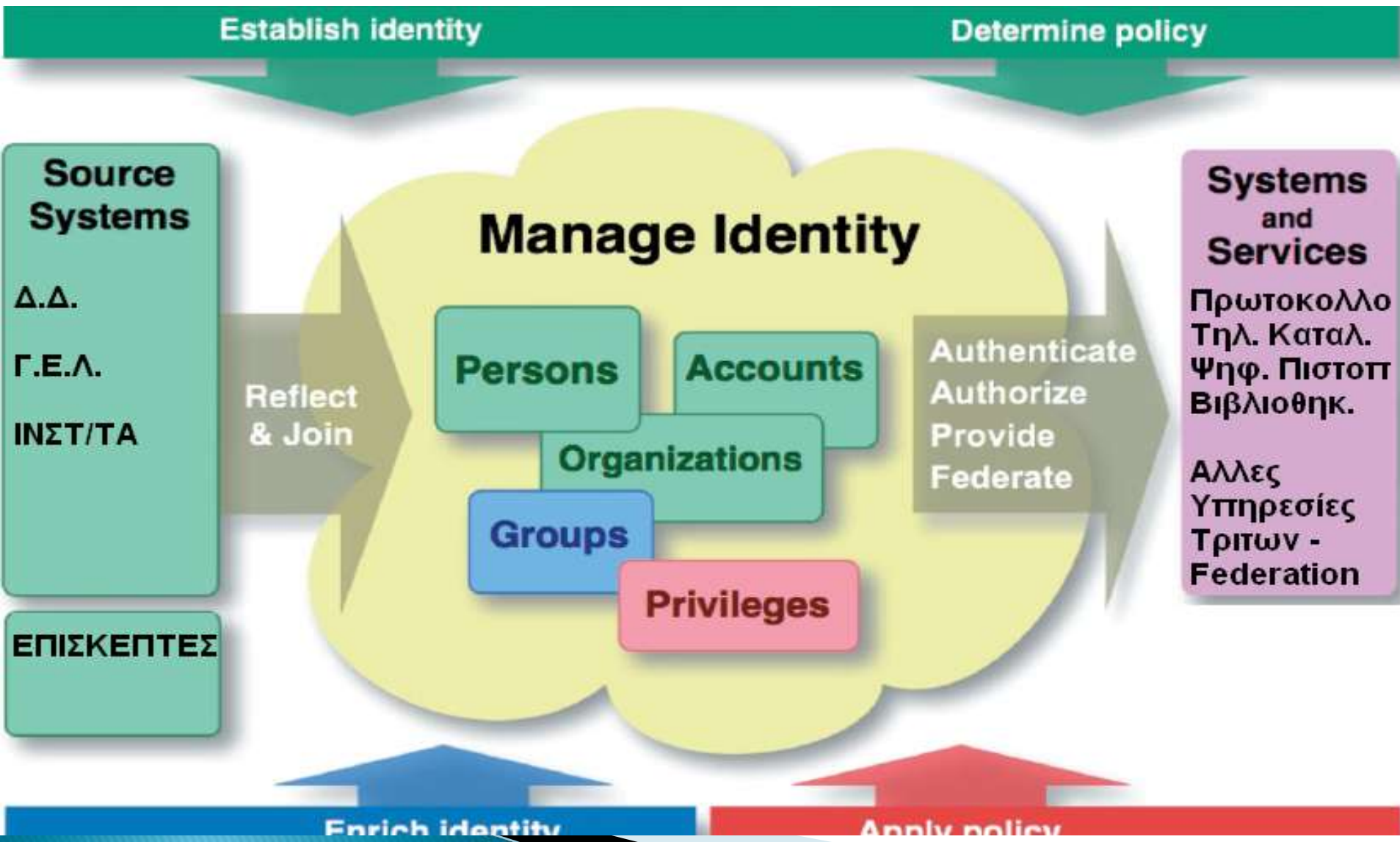
# Τι σημαίνει για τους χρήστες

- ▶ Απλοποίηση πρόσβασης σε όλες τις εφαρμογές
  - Προς ένα μοναδικό username και password
    - Το email σας και το password του.
  - Ξεκινάμε με χρήση στο ηλεκτρονικό πρωτόκολλο.
- ▶ Ψηφιακή υπογραφή εγγράφων
  - Κατάργηση χειρόγραφων αιτήσεων.
    - Τέλος στις διαδρομές προς τη γραμματεία για υπογραφή
  - Επιβεβαίωση αυθεντικότητας υπογραφής με μια ματιά.
  - Δυνατή η επικοινωνία μέσω υπογεγραμμένου email
    - χρήσιμο για Ερευνητές και σύντομα απαίτηση σε όλο το Δημόσιο τομέα.

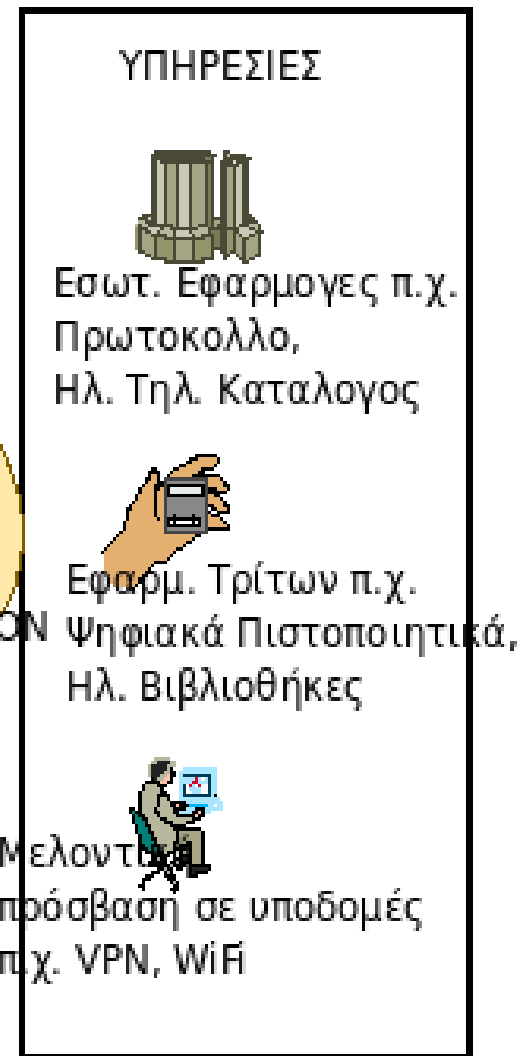
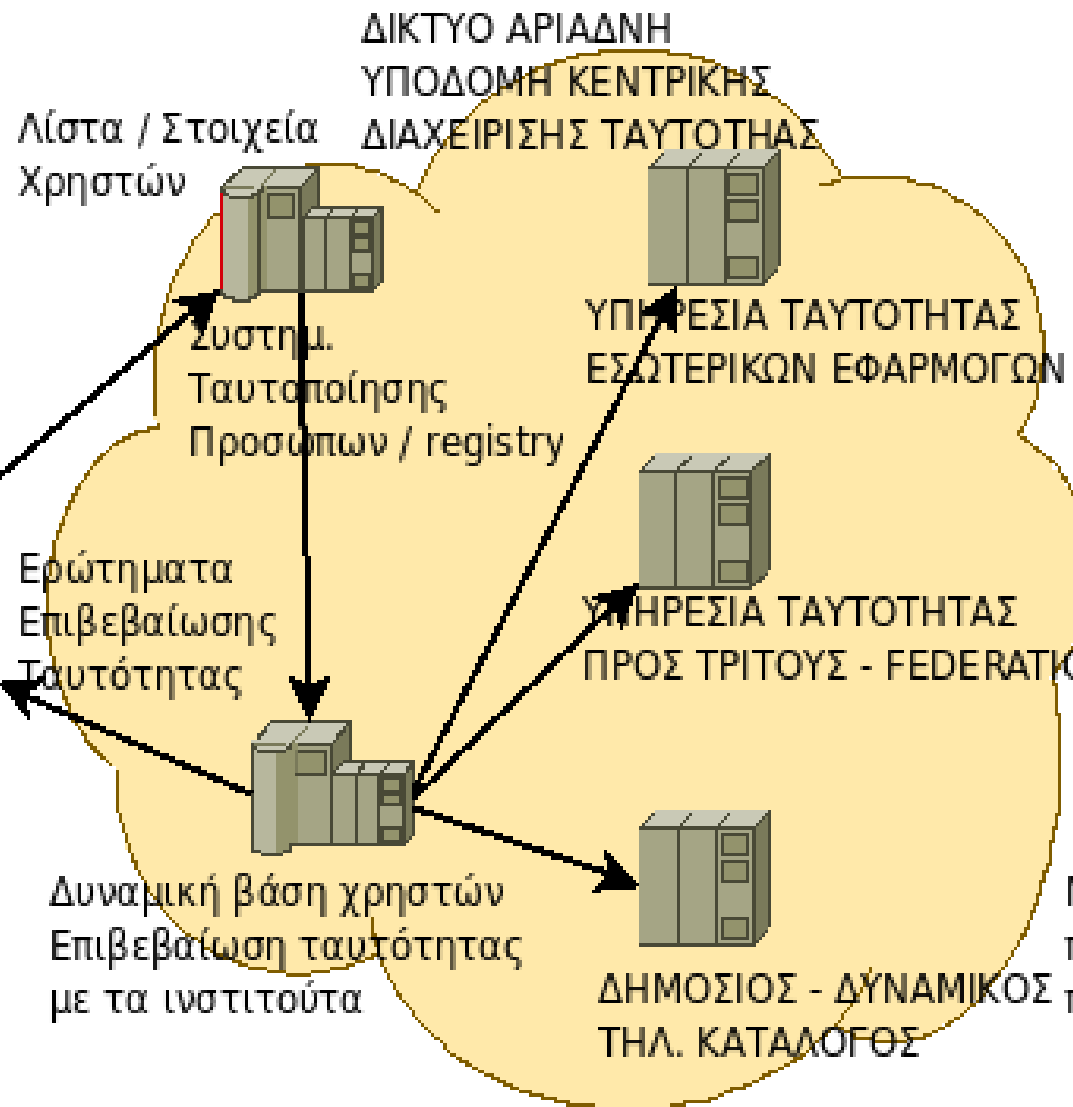
# Κεντρική υποδομή διαχείρισης ταυτότητας στο Δημόκριτο



# Κεντρική διαχείριση ταυτότητας στο Δημόκριτο



# Αρχιτεκτονική κεντρικής υποδομής διαχείρισης ταυτότητας



# Ηλεκτρονικό Πρωτόκολλο και Κεντρικές υπηρεσίες

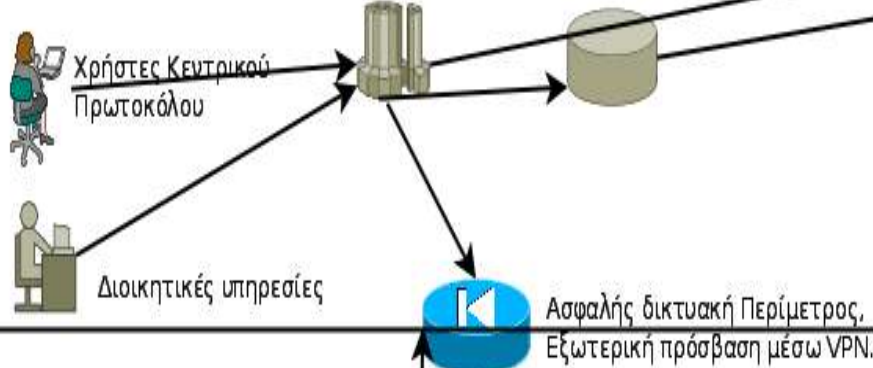
## Σύστημα Ηλεκτρονικού πρωτοκόλλου / Διακίνησης εγγράφων και υλοποίησης ροών εργασίας

Server 1:

- 1) Σύστημα διαχείρισης Εγγράφων και ροών εργασίας
- 2) Εφαρμογή υλοποίησης επιχειρησιακής λογικής, μέσω web java Application Server

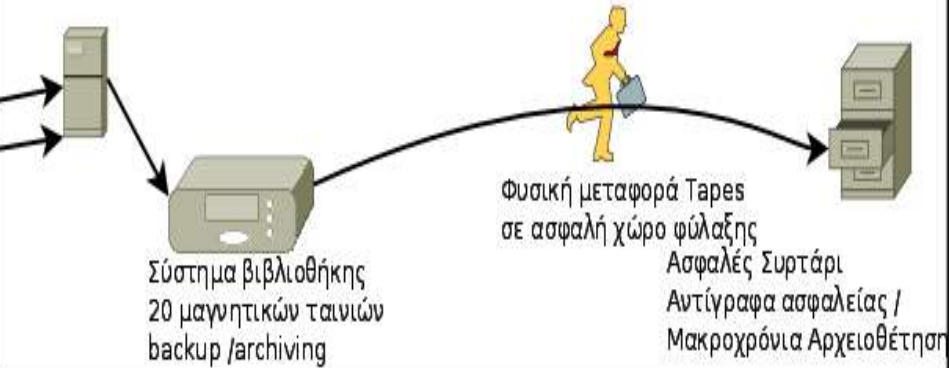
Server 2:

- Βάση Δεδομένων για στοιχεία Document Management και Εφαρμογή πρωτοκόλλησης



## Σύστημα τήρησης αντιγράφων ασφαλείας/ μακρόχρονης αποθήκευσης ηλεκτρονικών εγγράφων και αρχείων

Server 3: Λήψη αντιγράφων ασφαλείας, Backup Server (Καλύπτει τα συστήματα Πρωτόκολλο / ΓΕΛ / ΔΔ)



## Σημαντικές υποδομές για την υλοποίηση,

Κάποιες ήδη σε πιλοτική λειτουργία (χρειάζονται αναβάθμιση)



Ασφαλής ώρα αναφοράς, κατάσταση: Πιλότος



Κεντρική πιστοποίηση ταυτότητας, Κατάσταση: πιλοτική λειτουργία



Διαχείριση ταυτότητας χρηστών, κατάσταση: Σχεδιασμός



Ψηφιακή ταυτότητα δημοσίου Πάροχος δικτυακή πύλη δημοσίου Ερμής




Ψηφιακή ταυτότητα πάροχος Comodo (Μέσω ΕΔΕΤ)



Κεντρικός κατάλογος χρηστών / υπηρεσιών (Addressbook) Κατάσταση: Πιλ. λειτουργία



**Τεχνολογία Ψηφιακών  
πιστοποιητικών  
και ψηφιακής υπογραφής**





# Κρυπτογραφία δημοσίου κλειδιού

## ΑΣΣΥΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ



ΖΕΥΓΟΣ ΚΛΕΙΔΙΩΝ

ΟΤΙ ΚΡΥΠΤΟΓΡΑΦΕΙΤΑΙ  
ΜΕ ΤΟ ΕΝΑ ΚΛΕΙΔΙ



ΔΗΜΟΣΙΟ

ΑΠΟΚΡΥΠΤΟΓΡΑΦΕΙΤΑΙ  
ΜΕ ΤΟ ΑΛΛΟ



ΑΠΟΚΡΥΠΤΟΓΡΑΦΕΙΤΑΙ  
ΜΕ ΤΟ ΑΛΛΟ

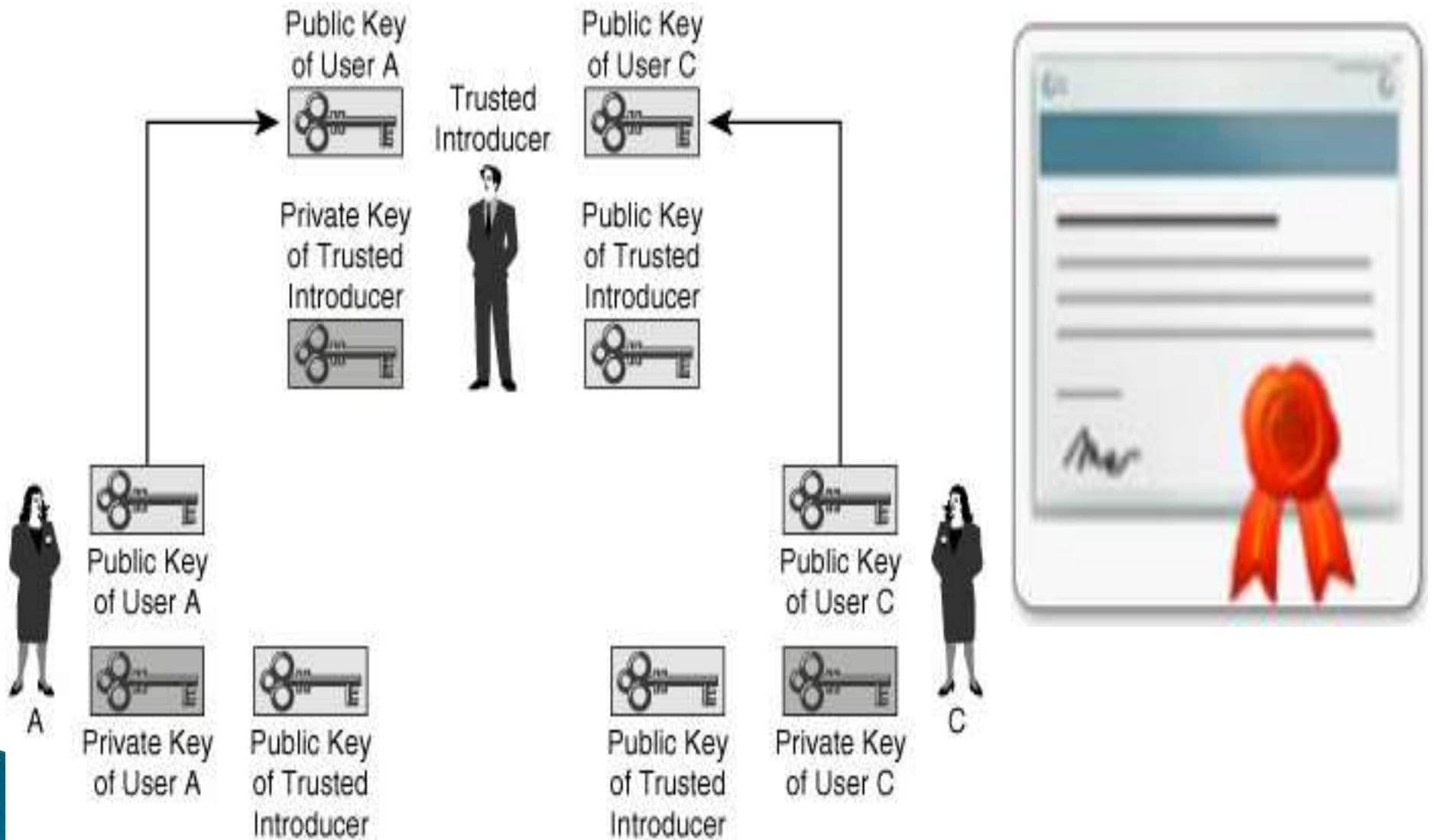


ΙΔΙΩΤΙΚΟ

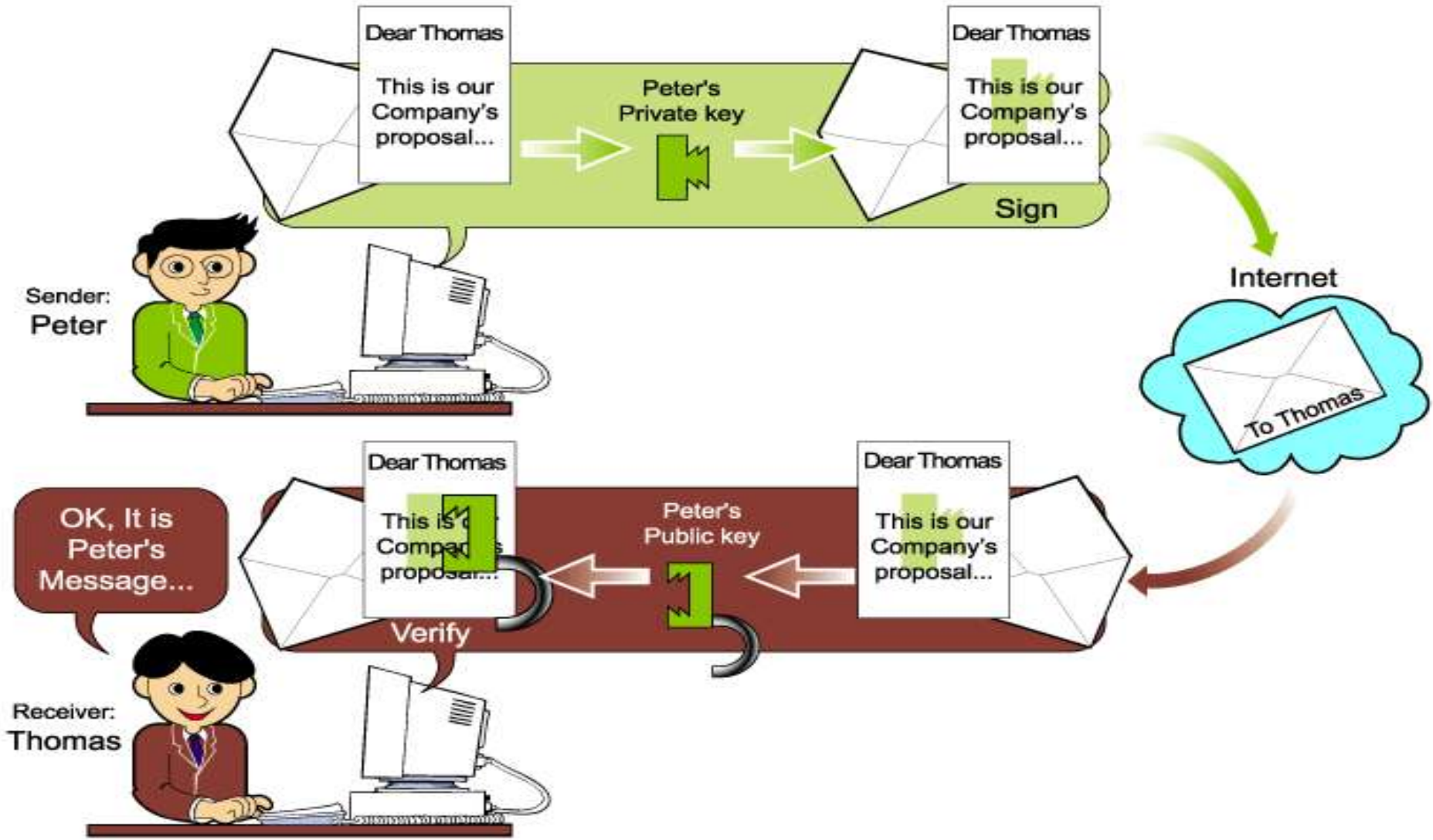
ΟΤΙ ΚΡΥΠΤΟΓΡΑΦΕΙΤΑΙ  
ΜΕ ΤΟ ΕΝΑ ΚΛΕΙΔΙ



# Τρίτη έμπιστη οντότητα / CA



# Υπογραφή email / Εγγράφου



# Υπογεγραμμένο email

Inbox - harisk@iit.demokritos.gr    Re: First personal digital certifica... x

from ΑΕΟΝΤΙΑΔΗΣ ΑΕΟΝΤΙΟΣ★

subject **Re: First personal digital certificate issued**

to Χάρης Κουτσούρης★

19/9/2011 12:52 μμ

reply forward archive junk delete

other actions ▾

test  
\*\*\*\*\*  
Dr. Leonidios Leonidiadis

Certificate Viewer: "ΙΙΙΙΙΙΙΙΙΙ>ΙΙΙΙΙΙΙΙΙΙΙΙ ΙΙΙΙΙΙΙΙΙΙ>ΙΙΙΙΙΙ"

General Details

**This certificate has been verified**

Email Signer Certificate

Email Recipient Certificate

**Certificate Hierarchy**

- [-] AddTrust External CA Root
  - [-] UTN-USERFirst-Client Authentication and Email
    - [-] TERENA Personal CA
      - ΑΕΟΝΤΙΑΔΗΣ ΑΕΟΝΤΙΟΣ

**Issued To**

Common Name (CN)	ΑΕΟΝΤΙΑΔΗΣ ΑΕΟΝΤΙΟΣ
Organization (O)	Demokritos National Center for Scientific Research
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:F1:8E:C4:B1:2C:A8:6D:9E:00:CE:39:C4:88:74:44:C4

**Issued By**

Common Name (CN)	TERENA Personal CA
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>

**Validity**

Issued On	19/9/2011
Expires On	19/9/2014

Message Security

**Message Is Signed**

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: ΑΕΟΝΤΙΑΔΗΣ ΑΕΟΝΤΙΟΣ  
Email address: leondi@rrp.demokritos.gr  
Certificate issued by: TERENA Personal CA

View Signature Certificate

**Message Not Encrypted**

This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

OK

# Παράδειγμα χρήσης(1)

EGEL140-2\_v2-sign-koutsouris-fontaras\_2.pdf - Adobe Reader

Αρχείο Επεξεργασία Προβολή Παράθυρο Βοήθεια



Εργαλεία

Σχόλιο

Κοι



Υπάρχουν προβλήματα σε μία τουλάχιστον υπογραφή. Συμπληρώστε την παρακάτω φόρμα. Μπορείτε να αποθηκεύσετε τα δεδομένα που πληκτρολογούνται στη φόρμα αυτή.



Πίνακας υπογραφών



Επισήμανση υπαρχό

Ινστιτούτο - Διεύθυνση ΙΠΤ

Αρ. Πρωτοκόλλου 345/23

Ημερομηνία 21 Σεπ 2011

Αριθμός Έργου 345

## ΕΙΔΟΣ ΑΜΟΙΒΗΣ

Σύμβαση με αριθμό

Επιμίσθιο (%)

Αμοιβή Τρίτων

Προκαταβολή Μετακίνησης

Εξόφληση Μετακίνησης

Πρόσθετη Αμοιβή (Μόνιμοι/ΙΔΑΧ)

Αμοιβή υποτρόφου

Αποζημίωση

Πρόσθετη απασχόληση  
σε ώρες

Άλλη

(οτιδήποτε σχετικά με το τμήμα Αμοιβές - Μετακινήσεις)

# Παράδειγμα χρήσης(2)

EGEL140-2\_v2-sign-koutsouris-fontaras\_2.pdf - Adobe Reader

Αρχείο Επεξεργασία Προβολή Παράθυρο Βοήθεια

1 / 1 105% Εργαλεία Σχόλιο Κοινή χρήση

Υπάρχουν προβλήματα σε μία τουλάχιστον υπογραφή. Συμπληρώστε την παρακάτω φόρμα. Μπορείτε να αποθηκεύσετε τα δεδομένα που πληκτρολογούνται στη φόρμα αυτή.

Πίνακας υπογραφών

Επισήμανση υπαρχόντων πεδίων

Ποσό σε ΕΥΡΩ	500
Ποσό σε συνάλλαγμα	
Δικαιούχος:	

Παρατηρήσεις	Παρατηρήσεις Να εκδοθεί άμεσα!
--------------	-----------------------------------

Η ανωτέρω δαπάνη είναι επιλέξιμη δαπάνη του Έργου και απαραίτητη για την υλοποίησή του.

Ο ΕΠΙΣΤΗΜΟΝΙΚΟΣ  
ΥΠΕΥΘΥΝΟΣ

Ο ΔΙΕΥΘΥΝΤΗΣ ΙΝΣΤΙΤΟΥΤΟΥ / ΔΙΕΥΘΥΝΣΗΣ  
(μόνο στις περιπτώσεις εφάπαξ αμοιβών)

ΚΟΥΤΣΟΥΡΗΣ  
ΧΑΡΑΛΑΜΠΟΣ

Υπογραφή από: ΚΟΥΤΣΟΥΡΗΣ ΧΑΡΑΛΑΜΠΟΣ  
DN: cn=χ, o=Εθνικό Κέντρο για Σχετική  
Κινητική, ou=ΕΠΙΣΤΗΜΟΝΙΚΟΣ ΧΑΡΑΛΑΜΠΟΣ,  
1.2.840.1.12541.1.1.2=charalambos.koutsouris.gr  
Ημερομηνία: 2011.09.21 10:09:58 +03'00'

Nasos Fontaras

Digitally signed by Nasos Fontaras  
DN: cn=Nasos Fontaras, o=NCSR, ou=GEI,  
email=fontas@gei.demokritos.gr, c=GR  
Date: 2011.09.21 10:09:58 +03'00'

ονοματεπώνυμο & υπογραφή

ονοματεπώνυμο & υπογραφή

# Παράδειγμα χρήσης(3)

## Ο ΕΠΙΣΤΗΜΟΝΙΚΟΣ ΥΠΕΥΘΥΝΟΣ

ΚΟΥΤΣΟΥΡΗΣ  
ΧΑΡΑΛΑΜΠΟΣ

Υπογράφηκε από: ΚΟΥΤΣΟΥΡΗΣ ΧΑΡΑΛΑΜΠΟΣ  
DN: c=GR, o=Demokritos National Center for Scientific  
Research, cn=ΚΟΥΤΣΟΥΡΗΣ ΧΑΡΑΛΑΜΠΟΣ,  
1.2.840.113549.1.9.2=harisk@demokritos.gr  
Ημερομηνία: 2011.09.21 10:04:13 +03'00'

# Έλεγχος εγκυρότητας πιστοποιητικών / υπογραφών

- ▶ Αυτόματος έλεγχος από τις εφαρμογές
  - Εκδότης έμπιστη Τρίτη οντότητα;
  - Εντός περιόδου ισχύος;
  - Σε λίστα γνωστών πλαστών πιστοποιητικών;
  - Ο εκδότης το έχει ανακαλέσει; (CRL, OCSP)
- ▶ Ο χρήστης
  - Αναζητάει την ετυμηγορία της εφαρμογής. Εικονίδια και μηνύματα. **Δεν αποδέχεται λάθος πιστοποιητικά!**
  - Αν η ταυτότητα του υπογράφοντος είναι σωστή:
    - Έχει το άτομο δικαίωμα / ρόλο να υπογράψει π.χ.
      - σαν διευθυντής;
      - Επιστημονικός υπεύθυνος ;
      - Να κάνει αίτηση για τρίτο άτομο;



# Πως αποκτάτε πιστοποιητικό – HTTPS://pki.demokritos.gr



**ΔΗΜΟΚΡΙΤΟΣ**  
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΕΡΕΥΝΑΣ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

**ΕΚΕΦΕ-Δημόκριτος**  
Υπηρεσία Ψηφιακών Πιστοποιητικών

Διαχειριστές | Ανάκληση Πιστοποιητικών | Αποσύνδεση

Επίπεδο Προβολής: **Απλός Χρήστης** | Διαχειριστής

Είστε συνδεδεμένος στην υπηρεσία

Παρακαλούμε μη χρησιμοποιείτε την υπηρεσία έκδοσης προσωπικών πιστοποιητικών απο κοινόχρηστους υπολογιστές. Το προσωπικό πιστοποιητικό που θα εκδώσετε θα αποθηκευτεί σ'αυτόν τον υπολογιστή

## Προσωπικές Πληροφορίες

Οι παρακάτω πληροφορίες έχουν σταλθεί απο την υπηρεσία ταυτοποίησης του οικείου φορέα σας (Demokritos National Center for Scientific Research)

<b>Όνοματεπώνυμο:</b>	ΚΟΥΤΣΟΥΡΗΣ ΧΑΡΑΛΑΜΠΟΣ
<b>Διευθύνσεις e-mail:</b>	✉ harisk@iit.demokritos.gr
<b>Τίτλοι δικαιωμάτων:</b>	user, admin
<b>Μοναδικό αναγνωριστικό:</b>	harisk@demokritos.gr
<b>Οικείος φορέας:</b>	Demokritos National Center for Scientific Research
<b>Χώρα:</b>	GR
<b>Όνομα χώρου:</b>	demokritos.gr
<b>Διακεκριμένο όνομα:</b>	/C=GR/O=Demokritos National Center for Scientific Research/CN=ΚΟΥΤΣΟΥΡΗΣ ΧΑΡΑΛΑΜΠΟΣ/unstructuredName=harisk@demokritos.gr

# ΑΔΕΙΑ ΧΡΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΥΠΟΧΡΕΩΣΕΙΣ (1 / 2)

- ▶ Έγκριση πιστοποιητικού μόνο από φυσική επιβεβαίωση ταυτότητας
- ▶ Ο οργανισμός ΥΠΟΧΡΕΟΥΤΑΙ να πάρει μέτρα για την σωστή χρήση των πιστοποιητικών / κλειδιών
- ▶ ΌΧΙ χρήση για πληρωμές / πιστωτικές κάρτες / οικονομικές συναλλαγές
- ▶ ΌΧΙ χρήση για παράνομες δραστηριότητες, συμμόρφωση με το εθνικό δίκαιο
- ▶ ΌΧΙ σε συστήματα FAIL SAFE, π.χ. Αντιδραστήρας

# ΑΔΕΙΑ ΧΡΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΥΠΟΧΡΕΩΣΕΙΣ (2 / 2)

- ▶ Τα πρόσωπα ΣΥΜΦΩΝΟΥΝ να προστατεύουν το ιδιωτικό κλειδί τους από μη εξουσιοδοτημένη χρήση.
- ▶ ΣΥΜΦΩΝΟΥΝ να ανακαλούν πιστοποιητικά που έχει θιγεί η γνησιότητα / ακρίβεια στοιχείων και η μυστικότητα του ιδιωτικού κλειδιού.
- ▶ ΌΧΙ χρήση άκυρων / ληγμένων κλειδιών
- ▶ ΑΠΟΔΟΧΗ υπογραφών ΜΟΝΟ μετά από έλεγχο εγκυρότητας υπογραφής

# Επισκόπηση διαδικασίας(1)

- ▶ Αίτηση στο [rki.demokritos.gr](http://rki.demokritos.gr) και επιτόπου παραλαβή.
  - Κατά την παραλαβή επιλέξτε προστασία με password
- ▶ Εξαγωγή από το certificate store του browser και αποθήκευση στον σκληρό δίσκο – πάντα προστατευμένο με password.
  - Αντιγραφή σε 1 τουλάχιστον CD.
  - Προσοχή μην ξεχάσετε το password, σημειώστε και αποθηκεύστε ξεχωριστά από το CD.
  - Επιπλέον – Συζητήστε με τον Δ.Υ. την δυνατότητα κεντρικού backup.
    - Το password είναι πάντα δική σας ευθύνη!

# Επισκόπηση διαδικασίας(2)

- ▶ Εισαγωγή του πιστοποιητικού και του κλειδιού στις εφαρμογές που χρησιμοποιείτε.
  - Windows certificate store
  - Thunderbird
  - Firefox
  - Internet explorer
  - Adobe Acrobat Reader
- ▶ Στείλτε ένα υπογεγραμμένο email στην διεύθυνση: [cert-dir@ariadne-t.gr](mailto:cert-dir@ariadne-t.gr)
  - Απαιτείται για την αυτόματη προσθήκη του πιστοποιητικού σας στον κεντρικό κατάλογο του κέντρου.
- ▶ Συνδεθείτε στο ηλ.πρωτόκολλο (Απαραίτητο) (<https://protocol.demokritos.gr>)

# Προστασία της υπογραφής(1)

- ▶ Προστατέψτε την ψηφιακή όπως και την φυσική υπογραφή σας.
  - Μην την αποθηκεύετε χωρίς password
  - Χρησιμοποιείτε μόνο «ασφαλής» υπολογιστές
  - Κρατήστε backup σε ασφαλές μέρος
  - Χρησιμοποιείτε «ισχυρά» password:
    - Όχι password που χρησιμοποιείται και αλλού (π.χ. Email)
    - Προτείνεται η χρήση password manager (keepass, passwordsafe)
      - Παρέχουν και μέτρηση ποιότητας του password σας.
    - Ελάχιστο μήκος 8-12 χαρακτήρες, τυχαία αλφαριθμητική ακολουθία,
    - καλύτερα ακόμη είναι μια μεγάλη φράση.

# Προστασία της υπογραφής(2)

- ▶ Προστατέψτε την ψηφιακή όπως και την φυσική υπογραφή σας.
  - Ρυθμίστε το σύστημα σας να ζητάει password κάθε φορά που υπογράφετε!
  - Εάν υποψιάζεστε ότι σας έκλεψαν το πιστοποιητικό:
    - Ανακαλέστε το και εκδώστε καινούργιο
    - Ενημερώστε τον Δικτυακό σας Υπεύθυνο και το κέντρο δικτύου.
  - Αποφύγετε υπερβολική χρήση του πιστοποιητικού:
    - Μην στέλνετε υπογεγραμμένα email όταν δεν χρειάζεται.
  - **Συμβουλευτείτε τον Δικτυακό Υπεύθυνο σας.**
    - Θα ενημερωθεί σύντομα από το κέντρο δικτύου.
    - Οποιαδήποτε έλλειψη εντοπιστεί να ενημερωθεί το κέντρο δικτύου

# Πιστοποιητικά υπηρεσιών/web (1)

- ▶ Αντίστοιχα με τα πρόσωπα, πιστοποιητικά (SSL) χρησιμοποιούμε και στις υπηρεσίες
- ▶ Στον Δημόκριτο πλέον έχουμε επιβεβαιωμένα και έγκυρα πιστοποιητικά – ΔΩΡΕΑΝ
  - Πολλά πιστοποιητικά δεν επιβεβαιώνονται από έμπιστη Τρίτη οντότητα (πάροχος πιστοποίησης)
- ▶ Ο χρήστης μπορεί / ΠΡΕΠΕΙ να ελέγχει την εγκυρότητα μέσω του Web browser.
  - **ΟΠΩΣΔΗΠΟΤΕ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΠΡΩΤΟΚΟΛΛΟ!!!**



# Πιστοποιητικά υπηρεσιών/web (2)

## Έγκυρο πιστοποιητικό

ΕΚΕΦΕ-Δημόκριτος -- Υπηρεσία Ψηφιακών Πιστοποιητικών - Mozilla Firefox

File Edit View History Bookmarks Tools Help

demokritos.gr https://pki.demokritos.gr/ digital signi

Εκκινώντας Hellenic Seaways f# File se

Shibboleth Identity Provider -... Πά

grnet Υπη

You are connected to **demokritos.gr** which is run by (unknown) Verified by: TERENA

Your connection to this web site is encrypted to prevent eavesdropping.

More Information...

Μέσα από την παρούσα εφαρμογή, μπορείτε να αιτηθείτε την έκδοση Ψηφιακών Πιστοποιητικών X.509 για Εξυπηρετητές που βρίσκονται κάτω από τα domains **ariadne-t.gr, demokritos.gr, nh.gr, epmhs.gr, honeynet.org.gr**

Έκδοση νέου Προσωπικού Ψηφιακού Πιστοποιητικού

Έκδοση νέου Ψηφιακού Πιστοποιητικού για Εξυπηρετητή

Done FoxyProxy: Default

# Πιστοποιητικά υπηρεσιών/web (3)

## Έγκυρο πιστοποιητικό

Page Info - https://pki.demokritos.gr/

General Media Permissions Security

Web Site Identity

Web site: **pki.demokritos.gr**

Owner: **This web site does not supply ownership information.**

Verified by: **TERENA**

Certificate Viewer: "pki.demokritos.gr"

General Details

**This certificate has been verified for the following uses:**

SSL Server Certificate

**Issued To**

Common Name (CN)	pki.demokritos.gr
Organization (O)	Demokritos National Center for Scientific Research
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	72:EE:CC:9E:1E:53:20:F3:55:1D:94:B3:2E:3E:B3:9

**Issued By**

Common Name (CN)	TERENA SSL CA
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>

**Validity**


Issued On	26/8/2011
Expires On	26/8/2014

**Fingerprints**

SHA1 Fingerprint	6F:24:E9:4B:AA:E2:45:5F:E2:12:5E:FF:99:AD:6A:D4:6C:8C:6E:23
MD5 Fingerprint	DC:FD:DA:A0:C5:F0:B2:28:68:75:9C:12:62:F3:16:4D

Πιστοποιητικό

Γενικά Λεπτομέρειες Διαδρομή πιστοποίησης

 **Πληροφορίες για το πιστοποιητικό**

**Το πιστοποιητικό προορίζεται για τους εξής σκοπούς:**

- Εγγύηση της ταυτότητας ενός απομακρυσμένου υπολογιστή

**Κάτοχος:** pki.demokritos.gr

**Εκδόθηκε από:** TERENA SSL CA

Έγκυρο από 26/8/2011 έως 26/8/2014

Εγκατάσταση πιστοποιητικού... Δήλωση

Πιστοποιητικό

Γενικά Λεπτομέρειες Διαδρομή πιστοποίησης

Διαδρομή πιστοποίησης

- USERTrust
- TERENA SSL CA
- pki.demokritos.gr

**Κατάσταση πιστοποιητικού:**

Αυτό το πιστοποιητικό είναι έγκυρο.

# Πιστοποιητικά υπηρεσιών/web (4)

## ΑΚΥΡΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ – Firefox



### This Connection is Untrusted

You have asked Firefox to connect securely to **protocol.demokritos.gr**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ Technical Details
- ▶ I Understand the Risks

# Πιστοποιητικά υπηρεσιών/web (5) ΑΚΥΡΟ ΠΙΣΤ. – Internet Explorer

The screenshot shows the Internet Explorer browser window with the address bar displaying <https://protocol.demokritos.gr/>. A red oval highlights the address bar and the security warning icon. The security warning dialog box is open, titled "Πιστοποιητικό", and contains the following text:

**Πληροφορίες για το πιστοποιητικό**

Αυτό το πιστοποιητικό ρίζας της αρχής έκδοσης πιστοποιητικών δεν είναι αξιόπιστο. Για να είναι αξιόπιστο, εγκαταστήστε το στο χώρο αποθήκευσης των αξιόπιστων πιστοποιητικών ρίζας της Αρχής έκδοσης πιστοποιητικών.

**Κάτοχος:** Dimokritos

**Εκδόθηκε από:** Dimokritos

Έγκυρο από 6/10/2011 έως 4/1/2012

Buttons: Εγκατάσταση πιστοποιητικού..., Δήλωση εκδότη, OK

Background text: ΜΟΔUS SOFTWARE, Πάπυρος Millenium III... R.6.1.5580, Κωδικό

Bottom status bar: Ολοκληρώθηκε

# Σύνοψη & άλλα αναγκαία (1)

- ▶ Η κεντρική υποδομή ταυτότητας μπορεί:
  - Να απλοποιήσει την καθημερινή χρήση των εφαρμογών
  - Να επιταχύνει την εισαγωγή νέων υπηρεσιών
    - Το Ηλεκτρονικό πρωτόκολλο η πρώτη αξιοποίηση
    - Ακολουθεί κεντρικός τηλεφωνικός κατάλογος
- ▶ Η ψηφιακή ταυτότητα μπορεί να:
  - Επιταχύνει / απλοποιήσει την γραφειοκρατία μας
  - Να καταργήσει τις στοίβες από φυσικά έντυπα
  - Παρέχει μεγαλύτερη εξασφάλιση γνήσιου υπογραφής, εάν την προσέχουμε όπως την φυσική.

# Σύνοψη & άλλα αναγκαία (2)

- ▶ Η υπηρεσία διαχείρισης ταυτότητας είναι ακόμη έργο σε εξέλιξη από πιλοτική δράση του Κέντρου Δικτύου (Αριάδνη) από το 2010.
- ▶ Η υπηρεσία προσωπικών πιστοποιητικών ενώ παρέχεται δωρεάν:
  - Έχει μισθωθεί από το παν-Ευρωπαϊκό ακαδημαϊκό δίκτυο TERENA με σύμβαση στον αναγνωρισμένο πάροχο COMODO.
  - Παρέχεται μέσω του Εθνικού δικτύου Έρευνας και Τεχνολογίας (ΕΔΕΤ).

# Σύνοψη & άλλα αναγκαία (3)

1. Διατηρείστε τον ηλεκτρονικό υπολογιστή σας έναν ΕΜΠΙΣΤΟ συνεργάτη / εργαλείο.
2. Προστατέψτε τα ιδιωτικά κλειδιά και την ψηφιακή υπογραφή σας, τηρείτε αντίγραφα ασφαλείας.
3. Ελέγξτε ψηφιακές υπογραφές για εγκυρότητα αλλά και εξουσιοδότηση υπογράφωντος.
4. Ελέγχετε τα πιστοποιητικά των WEB υπηρεσιών, πριν από κάθε χρήση.
5. Χρησιμοποιείτε ΔΥΝΑΤΑ passwords, ένα πρόγραμμα διαχείρισης passwords, δίνει πρακτική και εύκολη λύση.
6. Συνεργαστείτε με τον ΔΥ της υπηρεσίας σας.

# Ερωτήσεις;

Χαράλαμπος Κουτσούρης, MSc. CISA, CISSP  
Κέντρο Δικτύου - Ινστιτούτο Πληροφορικής & Τηλ.

[harisk@iit.demokritos.gr](mailto:harisk@iit.demokritos.gr),

[noc@ariadne-t.gr](mailto:noc@ariadne-t.gr),

2106503125