ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΒΙΟΜΗΧΑΝΙΑΣ

GRNET
ΕΔΕΤ

ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΠΟΚΕΝΤΡΩΣΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
"ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ"

ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ
ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ
ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ

ebusiness forum

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ 'Ε2':
«Ηλεκτρονικές Υπογραφές & Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης»
(Τεχνική & Νομική Ανάλυση)

Μέρος Β:

Τεχνική Ανάλυση των η-Υπογραφών & των η-Πιστοποιητικών

Παρουσίαση
Νίκος Κυρλόγλου
(ΣΥΝΤΟΝΙΣΤΗΣ ΤΗΣ Ο.Ε. 'Ε2')
Ειδικός Επιστήμονας Πληροφορικής
Εμπορικό & Βιομηχανικό Επιμελητήριο Αθηνών
nikoky@acci.gr

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- **Γιατί;**
  - Διεθνής αγορά χωρίς γεωγραφικούς ή χρονικούς περιορισμούς
  - Δυνατότητα ανταγωνισμού στο αυτό επίπεδο με πολυεθνικές εταιρείες
  - Συμμετοχή σε δραστηριότητες ανάλογα με τις ανάγκες
  - Οικονομικά και χρονικά οφέλη για επιχειρήσεις

ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (2)

- **Γιατί όχι;*** (κατά σειρά προτεραιότητας)
  - Προβλήματα ασφάλειας στις συναλλαγές (77%)
  - Προϊόντα/Υπηρεσίες όχι κατάλληλες για πώληση μέσω διαδικτύου (71%)
  - Πελάτες ή επιχειρήσεις ανέτοιμοι για διαδικτυακές πωλήσεις (65%)
  - Κίνδυνος από ελαττωματικά ή κακής ποιότητας προϊόντα (65%)
  - Έλλειψη εξοικείωσης με τεχνολογία/εφαρμογές (61%)
  - Αβεβαιότητα για το νομικό πλαίσιο (56%)
  - κλπ...

* Ερωτηματολόγιο έργου La Mer μεταξύ ΜΜΕ (09/2003)

ΤΙ ΣΗΜΑΙΝΕΙ «ΑΣΦΑΛΕΙΑ»;

- **Πιστοποίηση Ταυτότητας**
  - Μόνο οι νόμιμοι χρήστες μπορούν να προσπελάσουν το σύστημα και τις υπηρεσίες
- **Εμπιστευτικότητα και Ιδιωτικότητα**
  - Προσωπικά ή ευαίσθητα δεδομένα προστατεύονται
- **Ακεραιότητα**
  - Τα δεδομένα ή το σύστημα δεν έχουν αλλοιωθεί
- **Διαθεσιμότητα**
  - Το σύστημα πρέπει να είναι διαθέσιμο στους νόμιμους χρήστες διαρκώς

ΤΙ ΣΗΜΑΙΝΕΙ «ΑΣΦΑΛΕΙΑ»; (2)

- **ΕΜΠΙΣΤΟΣΥΝΗ**
  - Ο αποδέκτης των δεδομένων δεν θα τα χειρισθεί με μη αναμενόμενο τρόπο
- **ΣΙΓΟΥΡΙΑ**
  - Ο συναλλασσόμενος πρέπει να είναι εξίσου σίγουρος στο διαδικτυακό εμπόριο όπως και στο καθημερινό

ΥΠΕΝΘΥΜΙΣΗ!

- Οι συναλλαγές B2B αποτελούν το 80% του η-εμπορίου και αυξάνονται
- Οι συναλλαγές B2C όμως ελκύουν το 80% των Μέσων Μαζικής Ενημέρωσης και του πολιτικού ενδιαφέροντος

ΜΕΘΟΔΟΙ «ΑΣΦΑΛΕΙΑΣ»

- Ανοικτά/Κλειστά δίκτυα
- User Id (κωδικός πρόσβασης)/Password (συνθηματικό)
- Συμμετρική κρυπτογράφηση
  - **Διακίνηση «κλειδιού»**
- Ασύμμετρη κρυπτογράφηση
  - **Δύο κλειδιά (δημόσιο – ιδιωτικό)**
  - **Ό,τι κρυπτογραφεί το ένα αποκρυπτογραφείται από το άλλο**
  - **Από το ένα κλειδί δεν μπορεί να παραχθεί το άλλο**

ΠΡΟΗΓΜΕΝΗ (ΨΗΦΙΑΚΗ) ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ

ΠΑΡΟΧΟΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

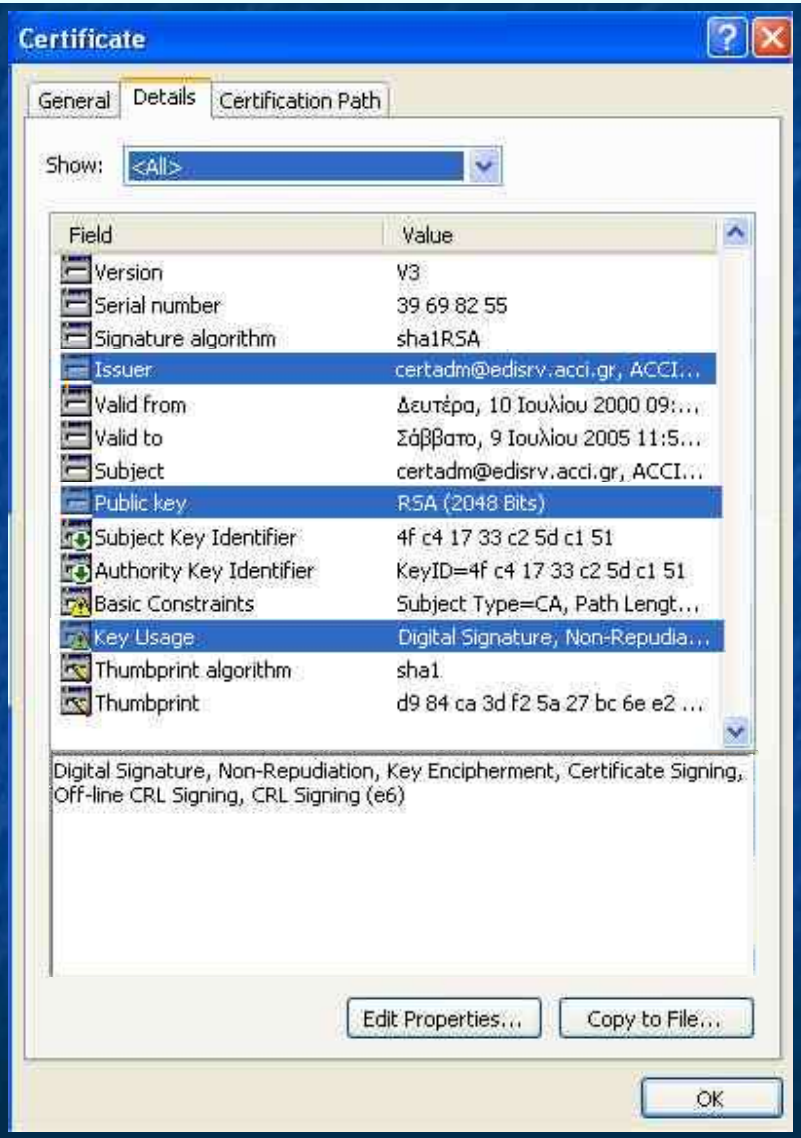
Ένας ουδέτερος οργανισμός, ο οποίος εμπνέει επιχειρηματική εμπιστοσύνη σε μια ηλεκτρονική συναλλαγή με εμπορικά και τεχνικά χαρακτηριστικά ασφάλειας, πιστοποιώντας την κατοχή συγκεκριμένων ζευγών ασύμμετρων κρυπτογραφικών κλειδιών από τους συναλλασσόμενους.

Με την χρήση **πιστοποιημένων κρυπτογραφικών κλειδιών** επιτυγχάνουμε:

- την επιβεβαίωση του αποστολέα του μηνύματος,
- την επιβεβαίωση της ακεραιότητας του μηνύματος καθ' οδόν
- και, εάν το επιθυμούμε, την κρυπτογράφηση του μηνύματος

ΠΙΣΤΟΠΟΙΗΤΙΚΟ X.509

- Τύπος (Εκδοχή)
- Σειριακός Αριθμός Πιστοποιητικού
- Χρησιμοποιούμενος Αλγόριθμος
- Εκδότης (Πιστοποιητικού)
- Έγκυρο από (ημ/νία) έως (ημ/νία)
- Θέμα (Υποκείμενο-Υπογράφων)
- Δημόσιο κλειδί
- Περιορισμοί χρήσης
- Όρια Συναλλαγών
- Αλγόριθμος αποτύπωσης
- … άλλες πληροφορίες



= Σημαντικά πεδία = Προαιρετικά πεδία = Τυπικά (απαραίτητα) πεδία

ΣΤΟΙΧΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΣ ΥΠΟΓΕΓΡΑΜΜΕΝΟΥ ΕΓΓΡΑΦΟΥ

Προς το Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών

ΑΙΤΗΣΗ

Του: ……

……
……
……
……
……
……
……
……
……
……

----------BEGIN SIGNATURE------
IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthb
a4BlrcnjaqbcKgNv+4537y8RCd+RHm75yYh5xxA1ojELwN
hhb7cltrp2V7LlOnAelws4S87UX80ctBcN6AACf11qymC2h
+Rb2j5SU+rmXWru+=QMx
----------END SIGNATURE------

----------BEGIN T-S SIGNATURE------
IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4Blrc
njaqbcKgNv+4537y8RCd+RHm75yYh5xxA1ojELwNhhb7cltrp2V
7LlOnAelws4S87UX80ctBh+Rb2j5SU+rmXWru+=QMx
----------END T-S SIGNATURE------

ΚΥΡΙΟ ΕΓΓΡΑΦΟ

Οποιασδήποτε ηλεκτρονικής μορφής
(π.χ.: *.doc, *.pdf, *.xls, κ.λ.π.)

ΥΠΟΓΡΑΦΗ

Κρυπτογράφηση 'σύνοψης' του Εγγράφου
-με το Ιδιωτικό κλειδί του υπογράφοντα

ΧΡΟΝΟΣΗΜΑΝΣΗ

Κρυπτογράφηση συγκεκριμένης ηλεκτρονικής υπογραφής MAZI με αξιόπιστη Χρονοσήμανση,
-με το Ιδιωτικό κλειδί του Παρόχου Υπηρεσιών Χρονοσήμανσης

ΠΙΣΤΟΠΟΙΗΤΙΚΑ

• 'Δημοσίου Κλειδιού' του Υπογράφοντα
ΚΑΙ ΠΙΘΑΝΩΣ:
• 'Δημοσίου Κλειδιού' του Π.Υ.Χρονοσήμανσης,
• 'Δημοσίου Κλειδιού' των Π.Υ.Πιστοποίησης,
• 'Ιδιοτήτων' του Υπογράφοντα, κ.ά.

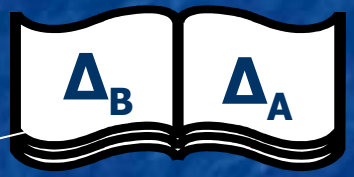
ΛΕΙΤΟΥΡΓΙΕΣ–ΥΠΗΡΕΣΙΕΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

- Α) ΥΠΟΧΡΕΩΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
  - Θεμελιώδης Εκδότης Πιστοποιητικού (Root CA)
  - Εκδότης Πιστοποιητικών (CA - Certification Authority)
  - Υπηρεσία Εγγραφής (RA - Registration Authority)
  - Υπηρεσία Δημοσίευσης και Διανομής (Dissemination Service)
  - Υπηρεσία Διαχείρισης Ανάκλησης (Revocation Management & Status Service)

ΛΕΙΤΟΥΡΓΙΕΣ–ΥΠΗΡΕΣΙΕΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

- Β) ΠΡΟΑΙΡΕΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ
  - Υπηρεσία Χρονοσήμανσης (Time Stamping Authority)
  - Υπηρεσία Προμήθειας Συσκευών (Device Provision Service)
  - Υπηρεσία Αποθήκευσης Εγγράφων (Notary Service)

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΗΝΥΜΑΤΟΣ/ΕΓΓΡΑΦΟΥ



Δημόσιος κατάλογος

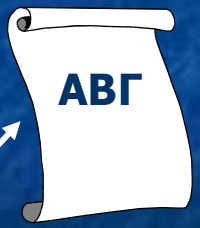
Δ_B

Η οντότητα Α χρησιμοποιεί το δημόσιο κλειδί της Β (Δ_B) για να κρυπτογραφήσει το αποστελλόμενο μήνυμα. Μόνο η οντότητα Β μπορεί πλέον να το αποκρυπτογραφήσει καθόσον μόνο αυτή γνωρίζει το ιδιωτικό της κλειδί I_B, το οποίο και μόνο αποκρυπτογραφεί ότι κρυπτογραφείται με το δημόσιο κλειδί Δ_B

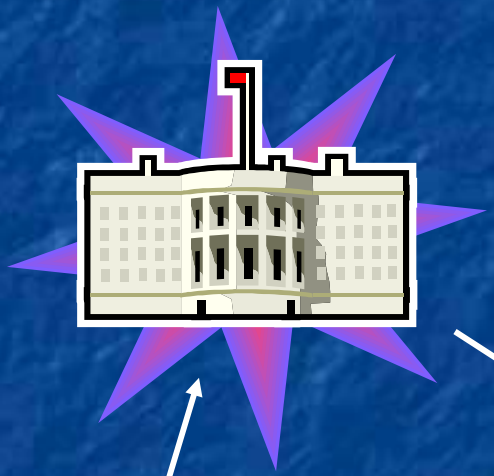
I_B

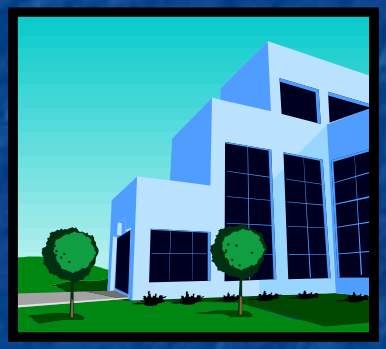
Δ_B

I_B



ΧΡΟΝΟΣΗΜΑΝΣΗ ΜΗΝΥΜΑΤΟΣ/ΕΓΓΡΑΦΟΥ





Δ_A

ΧΨΩ

I_A

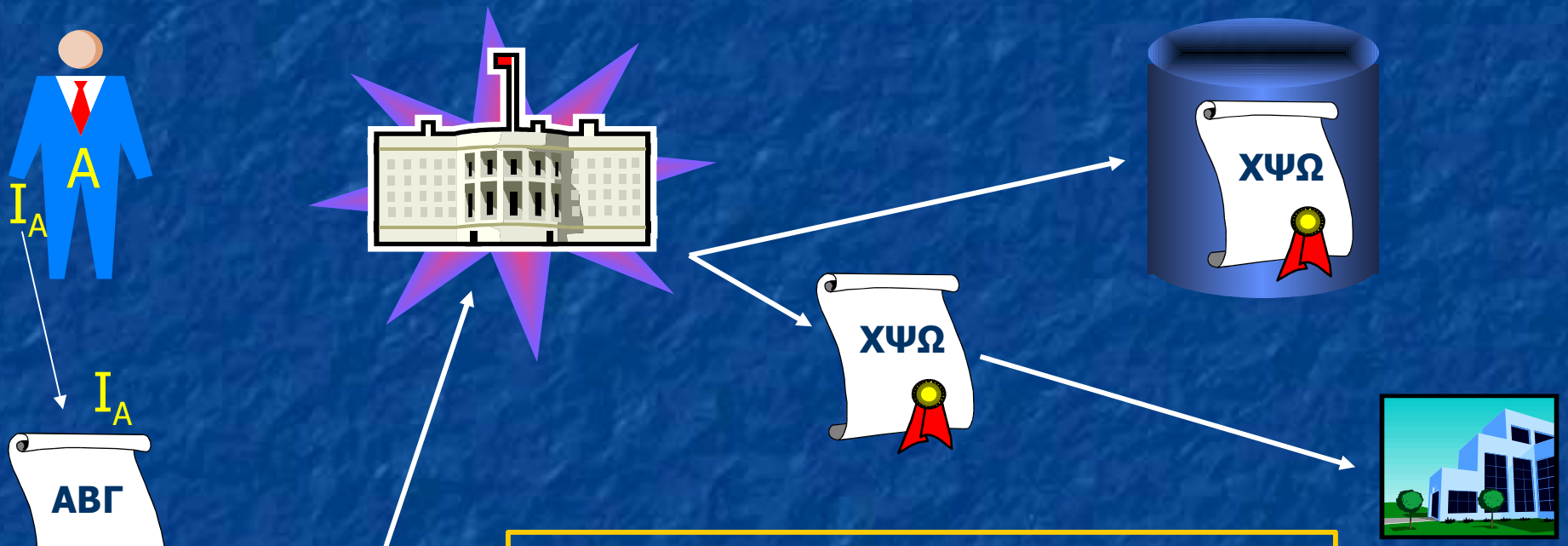
ΑΒΓ

ΧΨΩ

ΑΒΓ

Η Έμπιστη Τρίτη Οντότης 'σφραγίζει' την 'σύνοψη' (digest) του έγγραφου με την ημερομηνία και ώρα παραλαβής και στέλνει το σχετικό πιστοποιητικό

ΑΠΟΘΗΚΕΥΣΗ ΜΗΝΥΜΑΤΟΣ/ΕΓΓΡΑΦΟΥ



Η Έμπιστη Τρίτη Οντότης αποθηκεύει το αποσταλέν έγγραφο ώστε να είναι διαθέσιμο στο μέλλον για ελέγχους (π.χ. δικαστικούς, φορολογικούς, διοικητικούς κλπ.)

ΑΠΟΘΗΚΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ/ΠΡΟΜΗΘΕΙΑ ΣΥΣΚΕΥΩΝ

----------BEGIN SIGNATURE------

IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNE
sbthba4BlrcnjaqbcKgNv+4537y8RCd+RHm75yYh5
xxA1ojELwNhhb7cltrp2V7LlOnAelws4S87UX80ctBc
N6AACf11qymC2h+Rb2j5SU+rmXWru+=QMx
n----------END SIGNATURE------

ΕΛΕΓΧΟΣ ΕΓΚΥΡΟΤΗΤΑΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

- **Αξιοπιστία Εκδότη Πιστοποιητικού (ΠΥΠ)**
  - Προεγκατεστημένο αξιόπιστο πιστοποιητικό ρίζας (Root CA) του ΠΥΠ
  - Άντληση από αξιόπιστη υπογεγραμμένη λίστα Trusted List
  - Άντληση από μη αξιόπιστη πηγή και έλεγχος (γνωστού) αποτυπώματος
- **Έλεγχος ισχύος του Πιστοποιητικού**
  - Έλεγχος ημερομηνίας έναρξης-λήξης ισχύος
  - Έλεγχος ανάκλησης μέσω Certificate Revocation Lists (CRLs), ή
  - Έλεγχος ανάκλησης μέσω Online Certificate Status Protocol (OCSP)
- **Πρόσθετα στοιχεία ελέγχου**
  - (π.χ. Χρονοσήμανση υπογεγραμμένου εγγράφου, επιτρεπόμενες χρήσεις πιστοποιητικού, επιτρεπόμενα όρια στην αξία των συναλλαγών πιστοποίηση απαραίτητων ιδιοτήτων του υπογράφοντα, κ.λ.π.)