ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΠΟΛΙΤΕΣ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ ΥΠΟΔΟΜΗ PKI ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Επιμέλεια Διαφανειών:

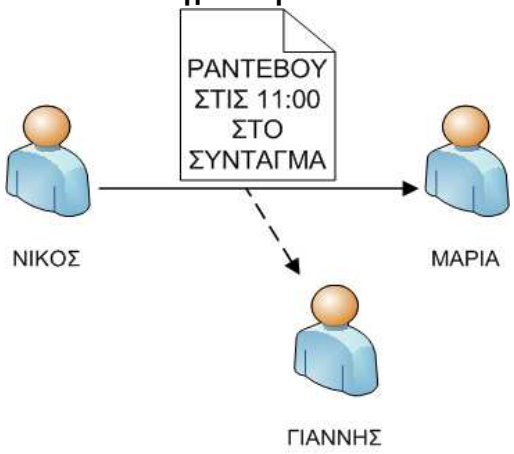
Φ. ΚΑΚΛΑΜΑΝΗΣ – Γ. ΚΑΤΣΙΚΟΓΙΑΝΝΗΣ – Δ. ΚΟΝΤΟΓΙΩΡΓΗΣ – Α. ΠΑΠΑΔΑΚΗΣ – Κ. ΡΑΝΤΟΣ – Ν. ΣΑΡΙΔΑΚΗΣ – Α. ΣΤΑΣΗΣ

Τι είναι ασφάλεια

- Ασφάλεια ενός πληροφοριακού συστήματος είναι η προστασία των υπολογιστικών πόρων και δεδομένων από μη εξουσιοδοτημένη ή κακή χρήση τους.
- Στόχος είναι η προστασία όλων των περιουσιακών στοιχείων:
  - Υλικό
  - Λογισμικό
  - Δεδομένα
- Βασικές αρχές: το τρίπτυχο
  - Εμπιστευτικότητα (**C**onfidentiality)
  - Ακεραιότητα (**I**ntegrity)
  - Διαθεσιμότητα (**A**vailability)

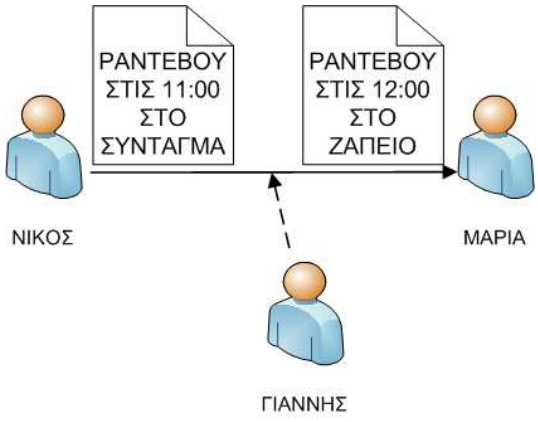
Εμπιστευτικότητα

- Προφυλάσσει από μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.
  - Συνήθως είναι συνώνυμη με την ασφάλεια.
  - Επιτυγχάνεται με:
    - τη κρυπτογράφηση των δεδομένων η οποία καθιστά τα δεδομένα μη αναγνώσιμα



Ακεραιότητα

- Προφυλάσσει από μη εξουσιοδοτημένη τροποποίηση των δεδομένων.
  - Τροποποίηση περιλαμβάνει:
    - Εγγραφή/Δημιουργία νέων δεδομένων.
    - Εισαγωγή νέων δεδομένων στα υπάρχοντα.
    - Διαγραφή μέρους ή όλων των δεδομένων.
  - Επιτυγχάνεται με:
    - ψηφιακές υπογραφές



Διαθεσιμότητα

- Εξασφαλίζει ότι οι πόροι ενός συστήματος είναι πάντα διαθέσιμοι, σε εύλογο χρονικό διάστημα, σε όλους τους εξουσιοδοτημένους χρήστες και μόνο σε αυτούς.

Άλλες αρχές

Ταυτοποίηση (Identification)	Η διαδικασία με την οποία μία οντότητα (π.χ. άνθρωπος, υπολογιστής, διαδικασία, πιστωτική κάρτα) αναγνωρίζει μία άλλη οντότητα.
Αυθεντικο-ποίηση ή Πιστοποίηση ταυτότητας (Authentication)	Η διαδικασία με την οποία μια οντότητα διαβεβαιώνεται για την ταυτότητα μιας άλλης οντότητας.

Άλλες αρχές

Εξουσιοδότηση (Authorization)	Η παροχή σε ένα υποκείμενο του δικαιώματος πρόσβασης σε ένα αντικείμενο. Η παροχή αυτή γίνεται τυπικά μετά την απαραίτητη ταυτοποίηση και αυθεντικοποίηση του υποκειμένου.
Απονομή ευθυνών (Accountability)	Υποδεικνύει ότι μία οντότητα πρέπει να είναι αναγνωρίσιμη και υπεύθυνη των πράξεων της.
Μη αποποίηση (Non-repudiation)	Η διαθεσιμότητα αδιάψευστων αποδείξεων που μπορούν να χρησιμοποιηθούν σε μία διαφωνία. Δύο κατηγορίες: ▫ Μη αποποίηση αποστολής: να μη μπορεί ο αποστολέας ενός μηνύματος να αρνηθεί την αποστολή του. ▫ Μη αποποίηση παραλαβής: να μη μπορεί ο παραλήπτης ενός μηνύματος να αρνηθεί τη λήψη του.

Προστασία από ποιούς;

- Οι περισσότερες επιθέσεις προέρχονται από μέσα παρά από έξω.
- Hackers-Εισβολείς: Επιτίθενται είτε από χόμπι είτε για οικονομικά οφέλη.
  - Τράπεζες
  - Κυβερνητικά συστήματα
  - Τηλεπικοινωνιακούς φορείς
  - Επιχειρήσεις
- Ατυχήματα – Ακούσιες βλάβες

Που εφαρμόζεται;

- Που εφαρμόζεται η ασφάλεια;
  - **Ασφάλεια επικοινωνιών**: Η προστασία των πληροφοριών κατά την επικοινωνία ενός συστήματος με ένα άλλο.
  - **Ασφάλεια υπολογιστών**: Η προστασία των πληροφοριών μέσα σε ένα υπολογιστικό σύστημα (λειτουργικό σύστημα, βάσεις δεδομένων)
  - **Φυσική ασφάλεια**.
  - **Ασφάλεια προσωπικού**.

Αυθεντικοποίηση

Αυθεντικοποίηση

- **Αυθεντικοποίηση:** Η διαδικασία σύμφωνα με την οποία μια οντότητα Α βεβαιώνεται για την ταυτότητα μιας άλλης οντότητας Β ή για την πηγή των δεδομένων.

Αυθεντικοποίηση οντότητας

- Η αυθεντικοποίηση οντότητας γίνεται σύμφωνα με
  - κάτι που **ξέρει**
    - Password
    - PIN
  - κάτι που **έχει**
    - Security token (password generator)
    - Έξυπνη κάρτα (smart card), magnetic stripe card
    - Για να κάνουμε την αυθεντικοποίηση πιο ασφαλή συνήθως τις χρησιμοποιούμε σε συνδυασμό με κάποια μέθοδο τύπου “κάτι που ξέρει”
  - κάτι που **είναι**
    - Βιομετρικές μέθοδοι

Αυθεντικοποίηση μηνύματος

- Η επαλήθευση της πηγής των δεδομένων είναι εφικτή με τη χρήση ψηφιακών υπογραφών

Passwords

- Πρόκειται για μια ακολουθία x χαρακτήρων γνώση της οποίας αποδέχεται ένα σύστημα ως διαβεβαίωση της ταυτότητας μιας οντότητας.
- Απειλές από τις οποίες πρέπει να προστατευτούμε όταν χρησιμοποιούμε passwords:
  - Αποκάλυψη του κωδικού πρόσβασης.
  - Παρακολούθηση της γραμμής μεταβίβασης του κωδικού πρόσβασης.
  - Εύρεση του κωδικού πρόσβασης χρησιμοποιώντας τεχνικές τύπου dictionary attacks.
- Απαραίτητη η χρήση δύσκολων κωδικών (χρήση αλφαριθμητικών χαρακτήρων σε συνδυασμό με μη αλφαριθμητικούς χαρακτήρες)

Passwords

- Τρόποι μείωσης του κινδύνου εύρεσης ενός password:
  - Εκπαίδευση σε χρήστες και διαχειριστές
  - Περιορισμός των μη έγκυρων προσπαθειών αυθεντικοποίησης σε πολύ μικρό αριθμό
  - Χρήση μηχανισμών που αποτρέπουν τους χρήστες να επιλέξουν passwords που είναι πολύ μικρά, εύκολα, σχετίζονται με τα χαρακτηριστικά του χρήστη.
  - Συχνή αλλαγή των passwords.
  - Αποφυγή των default passwords.

Κακόβουλο λογισμικό

Τρόποι αντιμετώπισης ιών

Κακόβουλο λογισμικό

- **Ιός**: είναι ένα κομμάτι κώδικα το οποίο αναπαράγεται από μόνο του (self-replicating) και το οποίο είναι προσκολλημένο σε άλλο κώδικα.
- **Ο όρος ιός προκύπτει από το γεγονός ότι το μολυσμένο πρόγραμμα μπορεί να αλλάξει ώστε να συμπεριλάβει ένα αντίγραφο του ιού και να αρχίσει να συμπεριφέρεται το ίδιο ως ιός μολύνοντας άλλα προγράμματα.**

Κακόβουλο λογισμικό

- **Δούρειος Ίππος (Trojan Horse)**: πρόκειται για ένα πρόγραμμα με κρυμμένες παρενέργειες οι οποίες δεν αναφέρονται στις λειτουργίες του προγράμματος. Αυτές οι παρενέργειες δεν αποτελούν μέρος των φυσιολογικών λειτουργιών του προγράμματος. Έχουν απλά σκοπό να βλάψουν το σύστημα.

Κακόβουλο λογισμικό

- **Spyware**: πρόκειται για ένα πρόγραμμα το οποίο εγκαθίσταται κρυφά και έχει ως κύριο σκοπό την υποκλοπή προσωπικών δεδομένων.

Τρόποι αντιμετώπισης ιών

- Η αντιμετώπιση των ιών απαιτεί την ύπαρξη ελέγχων για την ακεραιότητα των προγραμμάτων και των αρχείων. Η στρατηγική αντιμετώπισης ιών είναι η ακόλουθη:
  - **Πρόληψη**: σταματάει κάποιο ιό από το να μολύνει το σύστημα.
  - **Ανίχνευση**: ανιχνεύει κάποιον ιό που έχει μολύνει το σύστημα (απαιτείται τακτική ενημέρωση του λογισμικού αντιμετώπισης ιών).
  - **Αντιμετώπιση**: αποκατάσταση του συστήματος σε μια καθαρή κατάσταση (απαιτείται ύπαρξη σχεδίων αντιμετώπισης και αποκατάστασης του συστήματος).
- Ένα βασικό στοιχείο για την αντιμετώπιση των ιών εκτός από την ύπαρξη διαχειριστικών ελέγχων είναι και η **εκπαίδευση των χρηστών**.

Προσωπικά δεδομένα

Συλλογή προσωπικών δεδομένων

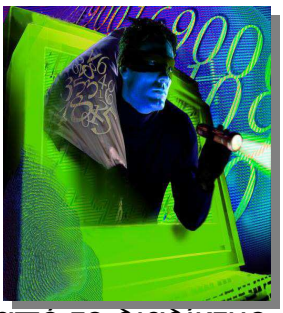
- Προστατεύονται από νομοθετικό πλαίσιο
  - Ν2472/97 (υποχρέωση προστασίας της εμπιστευτικότητας)
  - Ν3471/06 (προστασία προσωπικών δεδομένων και ιδιωτικής ζωής στο πεδίο των ηλεκτρονικών επικοινωνιών)
- Μπορεί να γίνει με θεμιτά ή αθέμιτα μέσα
  - Έντυπα που συμπληρώνει ο χρήστης
  - Cookies
  - Spyware
  - Social engineering
  - Phishing

Μέσα συλλογής προσωπικών δεδομένων

- Φωνή (ηχητικά κύματα)
- Εικόνα (κάμερες)
- Φως (οπτικές ίνες)
- Ηλεκτρικό ρεύμα (τηλέφωνο, fax)
- Ηλεκτρομαγνητικά κύματα (όλες οι μορφές ραδιοκυμάτων)

Υποκλοπή δεδομένων από τον προσωπικό υπολογιστή

- Κάθε προσωπικός υπολογιστής περιέχει έναν αρκετά «ελκυστικό» αριθμό προσωπικών δεδομένων
  - Email address book
  - Προσωπικά αρχεία
  - Διευθύνσεις ιστοσελίδων που επισκεπτόμαστε
  - Αριθμούς πιστωτικών καρτών που χρησιμοποιήσαμε για αγορές από το διαδίκτυο
  - Κωδικούς πρόσβασης



Cookies

- Πρόκειται για αρχεία που αποθηκεύονται στο σκληρό δίσκο και περιέχουν πληροφορίες αναφορικά με την επίσκεψη μας σε κάποια ιστοσελίδα
- Μπορεί να περιέχουν και προσωπικά στοιχεία (κωδικούς, αριθμούς πιστωτικών καρτών)
- Αποθηκεύονται στον κατάλογο C:\Documents and Settings\“username”\Local Settings\Temporary Internet Files υπό τη μορφή .txt αρχείων
- Τρόποι προστασίας
  - Να μην επιτρέπονται τα cookies
  - Διαγραφή ανά τακτά χρονικά διαστήματα

Social Engineering

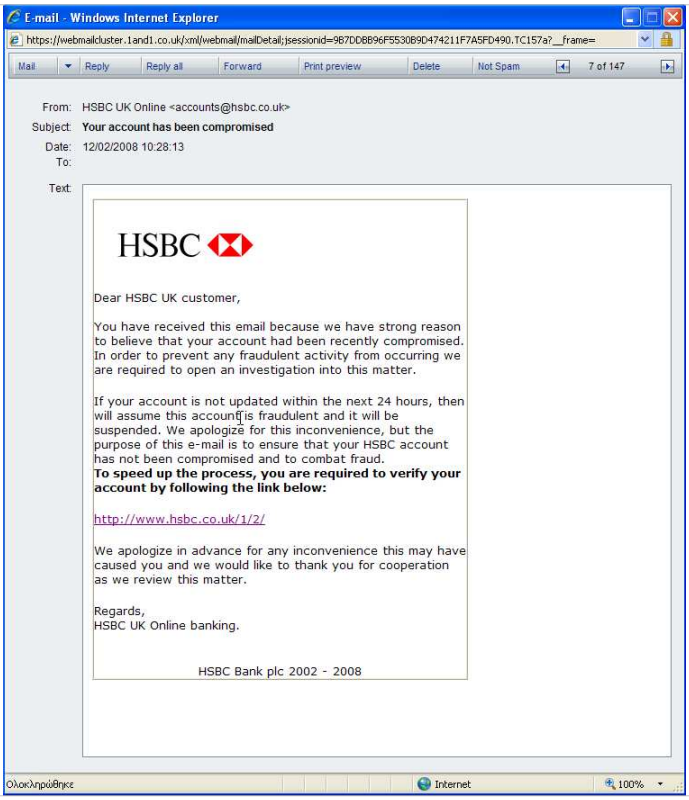
- Πρόκειται για την προσπάθεια υποκλοπής προσωπικών στοιχείων από τον ίδιο το χρήστη
- Ο επιτιθέμενος χρησιμοποιεί τις επικοινωνιακές του ικανότητες προκειμένου να εκμαιεύσει προσωπικά στοιχεία από τον ίδιο το χρήστη
- Τρόποι προστασίας
  - Ο χρήστης πρέπει να είναι
    - Υποψιασμένος
    - Επιφυλακτικός
    - Εγρήγορση

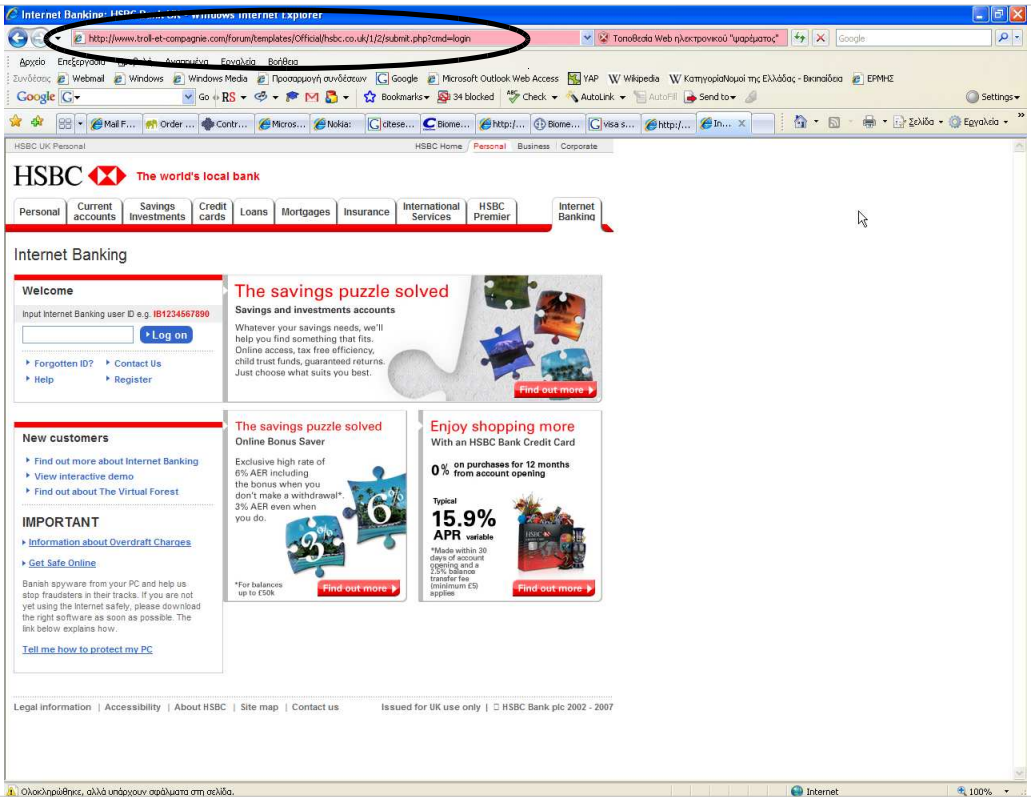
Phishing

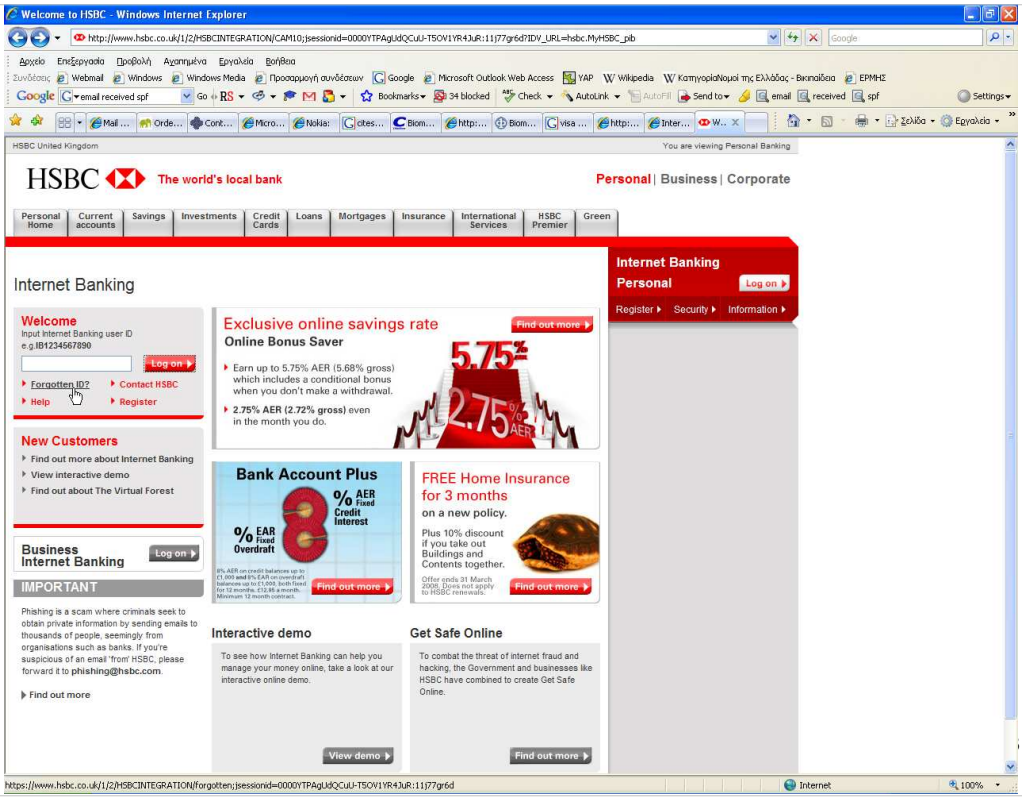
- Μια αρκετά διαδεδομένη τεχνική υποκλοπής πληροφοριών μέσω ανακατευθύνσεων ιστοσελίδων
- Τυπικά
  - Ο χρήστης δέχεται ένα email το οποίο δείχνει να προέρχεται από κάποιον έμπιστο οργανισμό (π.χ. τράπεζα) και παρακινεί το χρήστη να ακολουθήσει κάποιο σύνδεσμο προκειμένου να εισάγει κάποια προσωπικά στοιχεία (η διαδικασία παρουσιάζεται απαραίτητη και επείγουσα)

Phishing

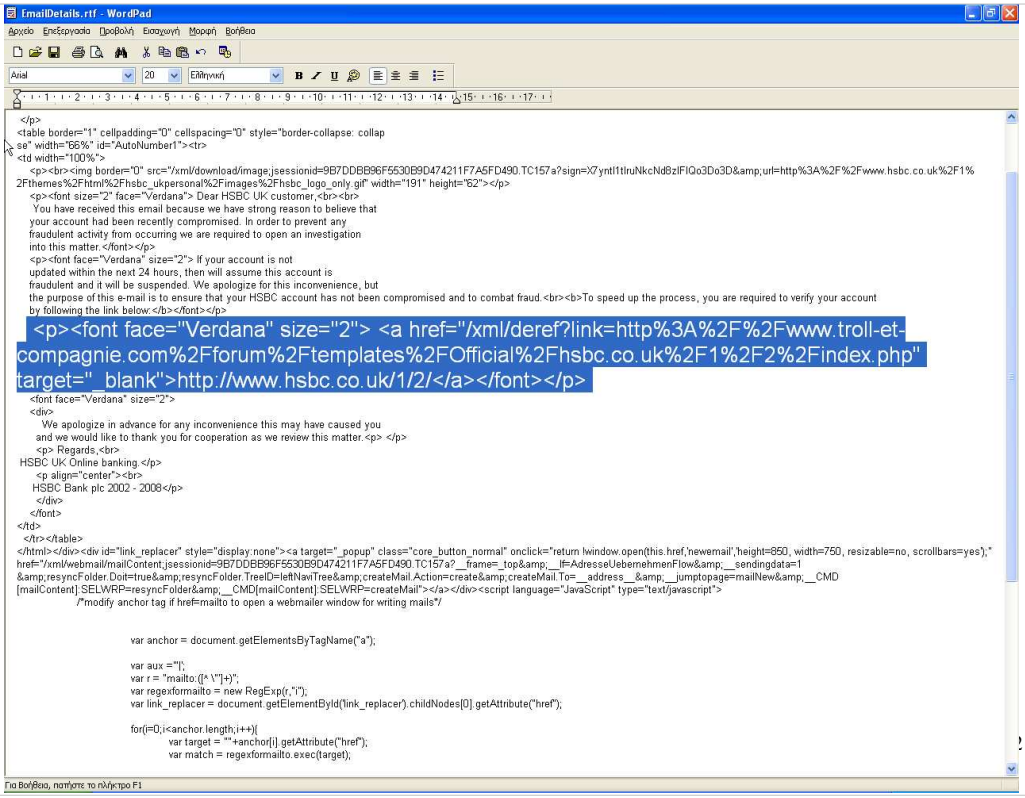
- Τυπικά
  - Ο χρήστης ακολουθώντας το σύνδεσμο οδηγείται σε μια ιστοσελίδα η οποία είναι παρόμοια με αυτή της τράπεζας όμως πρόκειται για σελίδα του επιτιθέμενου
  - Ο χρήστης εισάγει τα προσωπικά στοιχεία (π.χ. κωδικό πρόσβασης, αριθμούς λογαριασμών) τα οποία είναι πλέον στη διάθεση του επιτιθέμενου
  - Η διαδικασία υποκλοπής ολοκληρώνεται με τον χρήστη ανυποψίαστο


E-mail - Windows Internet Explorer
https://webmailcluster.1and1.co.uk/xml/webmail/mailDetail;jsessionid=987DDBB96F5530B9D474211F7A5FD490.TC157a?__frame=
Mail
Reply
Reply all
Forward
Print preview
Delete
Not Spam
7 of 147
From: HSBC UK Online <accounts@hsbc.co.uk>
Subject: Your account has been compromised
Date: 12/02/2008 10:28:13
To:
Text:
HSBC
Dear HSBC UK customer,
You have received this email because we have strong reason to believe that your account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.
If your account is not updated within the next 24 hours, then will assume this account is fraudulent and it will be suspended. We apologize for this inconvenience, but the purpose of this e-mail is to ensure that your HSBC account has not been compromised and to combat fraud.
To speed up the process, you are required to verify your account by following the link below:
http://www.hsbc.co.uk/1/2/
We apologize in advance for any inconvenience this may have caused you and we would like to thank you for cooperation as we review this matter.
Regards,
HSBC UK Online banking.
HSBC Bank plc 2002 - 2008
Internet
100%


http://www.troll-et-compagnie.com/forum/templates/Official/hsbc.co.uk/1/2/submit.php?cmd=login
HSBC
The world's local bank
Personal
Current accounts
Savings Investments
Credit cards
Loans
Mortgages
Insurance
International Services
HSBC Premier
Internet Banking
Internet Banking
Welcome
Log on
Forgotten ID?
Contact Us
Help
Register
The savings puzzle solved
Savings and investments accounts
Find out more
New customers
Find out more about Internet Banking
View interactive demo
Find out about The Virtual Forest
IMPORTANT
Information about Overdraft Charges
Get Safe Online
Tell me how to protect my PC
The savings puzzle solved
Online Bonus Saver
Find out more
Enjoy shopping more
With an HSBC Bank Credit Card
0% on purchases for 12 months from account opening
Typical
15.9% APR variable
Find out more
Legal information | Accessibility | About HSBC | Site map | Contact us
Issued for UK use only | HSBC Bank plc 2002 - 2007


Welcome to HSBC - Windows Internet Explorer
HSBC
The world's local bank
Personal | Business | Corporate
Internet Banking
Welcome
Log on
Forgotten ID?
Contact HSBC
Help
Register
New Customers
Find out more about Internet Banking
View interactive demo
Find out about The Virtual Forest
Business Internet Banking
Log on
IMPORTANT
Phishing is a scam where criminals seek to obtain private information by sending emails to thousands of people, seemingly from organisations such as banks. If you're suspicious of an email 'from' HSBC, please forward it to phishing@hsbc.com.
Find out more
Exclusive online savings rate
Online Bonus Saver
Earn up to 5.75% AER (5.68% gross) which includes a conditional bonus when you don't make a withdrawal.
2.75% AER (2.72% gross) even in the month you do.
Find out more
Bank Account Plus
Find out more
FREE Home Insurance for 3 months
on a new policy.
Plus 10% discount if you take out Buildings and Contents together.
Find out more
Interactive demo
To see how Internet Banking can help you manage your money online, take a look at our interactive online demo.
View demo
Get Safe Online
To combat the threat of internet fraud and hacking, the Government and businesses like HSBC have combined to create Get Safe Online.
Find out more
Internet Banking
Personal
Log on
Register
Security
Information

1


EmailDetails.rtf - WordPad

<table border="1" cellpadding="0" cellspacing="0" style="border-collapse: collap
se" width="66%" id="AutoNumber1"><tr>
<td width="100%">

<img border="0" src="/xml/download/image;jsessionid=9B7DDBB96F5530B9D474211F7A5FD490.TC157a?sign=X7yntI1tIruNkcNdBzIFlQo3Do3D&url=http%3A%2F%2Fwww.hsbc.co.uk%2F1%
2Fthemes%2Fhtml%2Fhsbc_ukpersonal%2Fimages%2Fhsbc_logo_only.gif" width="191" height="62">
 Dear HSBC UK customer,

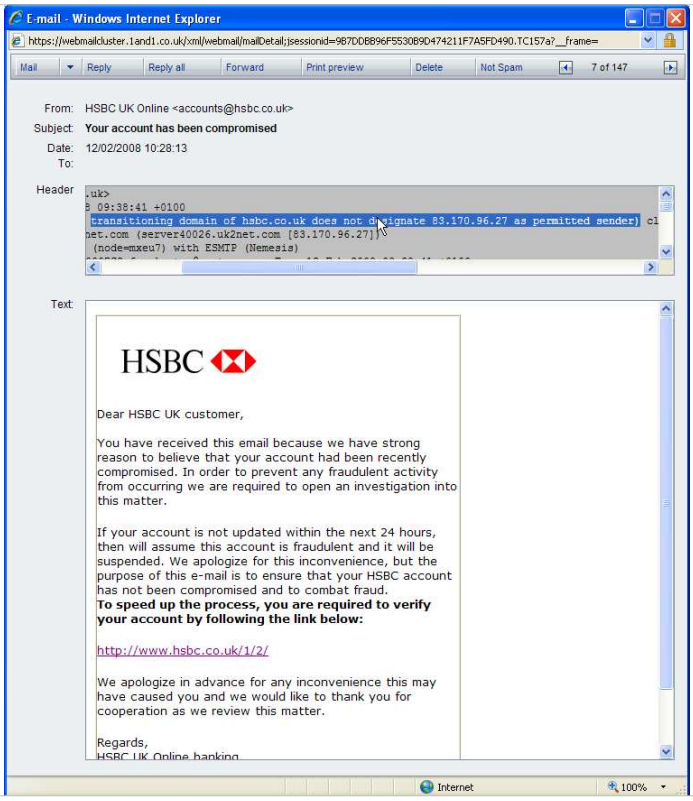
You have received this email because we have strong reason to believe that
your account had been recently compromised. In order to prevent any
fraudulent activity from occurring we are required to open an investigation
into this matter.
 If your account is not
updated within the next 24 hours, then will assume this account is
fraudulent and it will be suspended. We apologize for this inconvenience, but
the purpose of this e-mail is to ensure that your HSBC account has not been compromised and to combat fraud.
To speed up the process, you are required to verify your account
by following the link below:
 http://www.hsbc.co.uk/1/2/

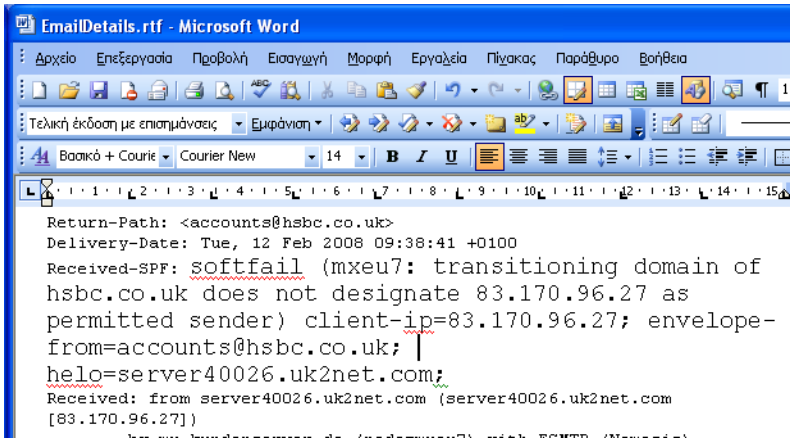
We apologize in advance for any inconvenience this may have caused you
and we would like to thank you for cooperation as we review this matter.
 Regards,
HSBC UK Online banking.

HSBC Bank plc 2002 - 2008

</td>
</tr></table>
</html> <a target="_popup" class="core_button_normal" onclick="return !window.open(this.href,'newemail','height=850, width=750, resizable=no, scrollbars=yes');" href="/xml/webmail/mailContent;jsessionid=9B7DDBB96F5530B9D474211F7A5FD490.TC157a?__frame=_top&__lf=AdresseUebernehmenFlow&__sendingdata=1
&resyncFolder.Doit=true&resyncFolder.TreeID=leftNaviTree&createMail.Action=create&createMail.To=__address__&__jumptopage=mailNew&__CMD
[mailContent].SELWRP=resyncFolder&__CMD[mailContent].SELWRP=createMail"> <script language="JavaScript" type="text/javascript">
/*modify anchor tag if href=mailto to open a webmailer window for writing mails*/
var anchor = document.getElementsByTagName("a");
var aux ="|";
var r = "mailto:([^ \"]+)";
var regexformailto = new RegExp(r,"i");
var link_replacer = document.getElementById('link_replacer').childNodes[0].getAttribute("href");
for(i=0;i<anchor.length;i++){
var target = ""+anchor[i].getAttribute("href");
var match = regexformailto.exec(target);
Για Βοήθεια, πατήστε το πλήκτρο F1

2


E-mail - Windows Internet Explorer
https://webmailcluster.1and1.co.uk/xml/webmail/mailDetail;jsessionid=987DDB896F553089D474211F7A5FD490.TC157a?__frame=
Mail
Reply
Reply all
Forward
Print preview
Delete
Not Spam
7 of 147
From: HSBC UK Online <accounts@hsbc.co.uk>
Subject: Your account has been compromised
Date: 12/02/2008 10:28:13
To:
Header
.uk>
09:38:41 +0100
transitioning domain of hsbc.co.uk does not designate 83.170.96.27 as permitted sender) cl
net.com (server40026.uk2net.com [83.170.96.27])
(node=mxeu7) with ESMTP (Nemesis)
Text:
HSBC
Dear HSBC UK customer,
You have received this email because we have strong reason to believe that your account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.
If your account is not updated within the next 24 hours, then will assume this account is fraudulent and it will be suspended. We apologize for this inconvenience, but the purpose of this e-mail is to ensure that your HSBC account has not been compromised and to combat fraud.
To speed up the process, you are required to verify your account by following the link below:
http://www.hsbc.co.uk/1/2/
We apologize in advance for any inconvenience this may have caused you and we would like to thank you for cooperation as we review this matter.
Regards,
HSBC UK Online banking
Internet
100%


EmailDetails.rtf - Microsoft Word
Αρχείο Επεξεργασία Προβολή Εισαγωγή Μορφή Εργαλεία Πίνακας Παράθυρο Βοήθεια
Τελική έκδοση με επισημάνσεις
Εμφάνιση
Βασικό + Courie
Courier New
14
Return-Path: <accounts@hsbc.co.uk>
Delivery-Date: Tue, 12 Feb 2008 09:38:41 +0100
Received-SPF: softfail (mxeu7: transitioning domain of hsbc.co.uk does not designate 83.170.96.27 as permitted sender) client-ip=83.170.96.27; envelope-from=accounts@hsbc.co.uk;
helo=server40026.uk2net.com;
Received: from server40026.uk2net.com (server40026.uk2net.com [83.170.96.27])

Πολιτική Ασφαλείας

Πολιτικές Ασφαλείας

- Τι είναι;
- Τι θα πρέπει να περιλαμβάνει;
- Ποιοι παράγοντες συμβάλλουν στην αποτελεσματική εφαρμογή μιας Πολιτικής Ασφάλειας;

Γιατί χρειαζόμαστε ΠΑ;

- Γιατί χρειαζόμαστε ένα συστηματικό και ολοκληρωμένο πλαίσιο που θα καθοδηγήσει την υλοποίηση των μέτρων Ασφάλειας
  - Γιατί έτσι θεμελιώνεται η σημασία της ασφάλειας του ΠΣ για όλα τα μέλη του οργανισμού
  - Γιατί συμβάλλει στη δημιουργία κουλτούρας ασφάλειας
  - Γιατί σε ορισμένες περιπτώσεις αποτελεί νομική υποχρέωση
  - Γιατί αποτελεί παράγοντα εμπιστοσύνης στις σχέσεις του οργανισμού με συνεργαζόμενους φορείς και πελάτες

Τι περιέχει η ΠΑ;

- Σκοπό και στόχοι ασφάλειας
- Οδηγίες
- Διαδικασίες
- Κανόνες
- Ρόλοι και υπευθυνότητες

Θέματα ΠΑ

- Ποια είναι τα αγαθά του ΠΣ που χρειάζονται προστασία;
- Ποιοι είναι οι υπεύθυνοι για την προστασία των αγαθών αυτών και ποιες είναι οι αρμοδιότητές τους;
- Ποιο είναι το εύρος και ποια τα όρια εφαρμογής της;
- Πώς θα γίνεται ο έλεγχος της εφαρμογής της;
- Ποια είναι τα χρονικά πλαίσια που ισχύει η Πολιτική;

Περιεχόμενο ΠΑ

- Ζητήματα Προσωπικού
- Φυσική Ασφάλεια
- Έλεγχος Πρόσβασης στο ΠΣ
- Διαχείριση Υλικού και Λογισμικού
- Νομικές υποχρεώσεις
- Διαχείριση της Πολιτικής Ασφάλειας
- Οργανωτική Δομή
- Σχέδιο Συνέχισης Λειτουργίας

Χαρακτηριστικά ΠΑ

- Σαφήνεια και ευκολία κατανόησης
- Τεχνολογική ανεξαρτησία
- Καταλληλότητα
- Εφαρμοσιμότητα

Διαμόρφωση ΠΑ

- «Υποχρεωτική» εφαρμογή
  - Επιτρεπτές ενέργειες θεωρούνται μόνο εκείνες που προβλέπονται και προδιαγράφονται στην Πολιτική Ασφάλειας
- «Διακριτικός» έλεγχος
  - Όλες οι ενέργειες που δεν περιλαμβάνονται στις απαγορευμένες θεωρούνται επιτρεπτές και σύμφωνες με την πολιτική
- «Κατά περίπτωση» εφαρμογή
  - Οι οδηγίες ασφάλειας της Πολιτικής θεωρούνται υποχρεωτικές, υπάρχει όμως η δυνατότητα να παρακαμφθούν κατά περίπτωση

Αναθεώρηση ΠΑ

- Σε τακτικά χρονικά διαστήματα (Τακτικές αναθεωρήσεις)
- Έπειτα από σημαντικά περιστατικά παραβίασης της ασφάλειας, ουσιώδεις αλλαγές στο υλικό ή το λογισμικό, επέκταση ή διασύνδεση του ΠΣ με άλλα συστήματα (Έκτακτες αναθεωρήσεις)

Κρυπτογραφία

Κρυπτογραφία

- Κρυπτογραφία = κρυφή γραφή
- Η επιστήμη η οποία έχει ως αντικείμενο την εξεύρεση μεθόδων που μπορούν να χρησιμοποιηθούν στην ασφάλεια πληροφοριών
- Η διακίνηση (προσωπικών) πληροφοριών μέσω δημοσίων δικτύων επιβάλλει την εκτεταμένη χρήση της

Κρυπτογραφία – Ιστορική αναδρομή

- Το πρώτο κρυπτογραφημένο μήνυμα χρονολογείται από το 1500π.χ. στη Βαβυλωνία
- Οι αρχαίοι Αιγύπτιοι διακοσμούσαν με ιερογλυφικά στους τάφους τους για να περιγράψουν τη ζωή του αποθανόντος.
- Ο Ηρόδοτος κάνει αναφορές για κρυπτογραφημένα μηνύματα που μετέφεραν οι αγγελιοφόροι.
- Το 400π.Χ. οι Σπαρτιάτες χρησιμοποιούσαν ένα σύστημα κρυπτογράφησης μηνυμάτων για να μεταφέρουν με ασφάλεια μηνύματα στους στρατιώτες τους.

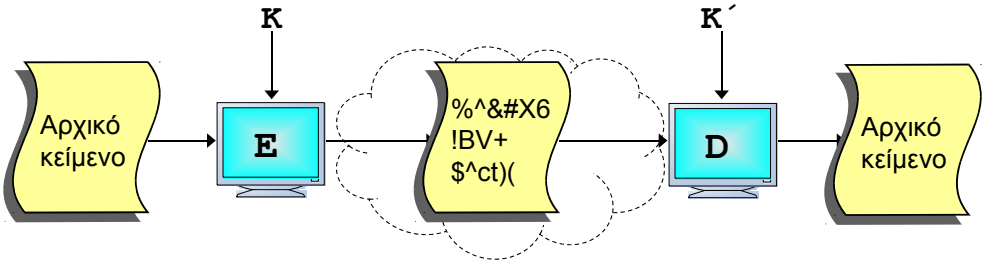
Κρυπτογραφία – Ιστορική αναδρομή

- Ο Ιούλιος Καίσαρας χρησιμοποιούσε έναν αλγόριθμο (γνωστό ως Αλγόριθμος του Καίσαρα) για την αποστολή μηνυμάτων στους στρατιώτες του
- Η πιο εκτενής αναφορά έγινε κατά τον Β' Παγκόσμιο Πόλεμο λόγω της μηχανής Enigma που χρησιμοποιούσαν οι Γερμανοί

Κρυπτογραφία – Βασικοί ορισμοί

- **Κρυπτογράφηση (encryption)** –
  Η μετατροπή μιας ακολουθίας δεδομένων (ή ενός κειμένου) σε μη αναγνώσιμη η επεξεργάσιμη μορφή
- **Αποκρυπτογράφηση (decryption)** – Η μετατροπή ενός κρυπτογραφημένου κειμένου σε αναγνώσιμη ή επεξεργάσιμη μορφή
- **Αλγόριθμος κρυπτογράφησης/αποκρυπτογράφησης** – Η μαθηματική μέθοδος με την οποία γίνεται ο μετασχηματισμός των δεδομένων
- **Κρυπτογράφημα ή κρυπτομήνυμα (ciphertext) –**
  Το κρυπτογραφημένο κείμενο

Κρυπτογραφία – Βασικό μοντέλο



Ε : Αλγόριθμος κρυπτογράφησης – γνωστός στους ενδιαφερόμενους
D : Αλγόριθμος αποκρυπτογράφησης – γνωστός στους ενδιαφερόμενους

Κ : Κλειδί κρυπτογράφησης
Κ΄ : Κλειδί αποκρυπτογράφησης

Κρυπτομήνυμα (ciphertext) $c = E_K(m)$
Αρχικό μήνυμα (plaintext) $m = D_{K'}(m)$

$\Big\}\ m = D_{K'}(E_K(m))$

Η ΑΣΦΑΛΕΙΑ ΒΑΣΙΖΕΤΑΙ ΣΤΗ ΜΥΣΤΙΚΟΤΗΤΑ ΤΟΥ ΚΛΕΙΔΙΟΥ Κ΄

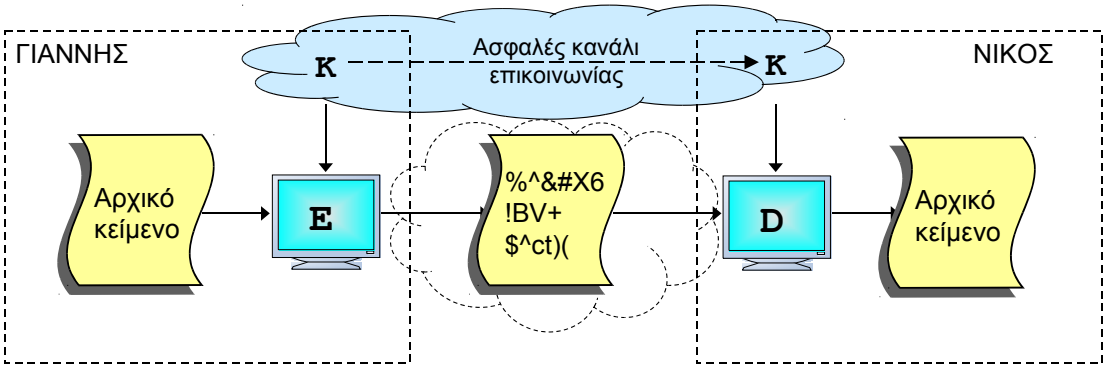
Κρυπτογραφία – Ο ρόλος των κλειδιών

- Ο κάθε αλγόριθμος έχει τις δικές του απαιτήσεις αναφορικά με το μέγεθος των κλειδιών
- Όσο μεγαλύτερο το κλειδί τόσο μεγαλύτερη ασφάλεια μας παρέχει
- Η ασφάλεια ενός κρυπτογραφημένου μηνύματος δε βασίζεται στη μυστικότητα του αλγορίθμου αλλά στην προστασία των κλειδιών

Κρυπτογραφία – Κατηγορίες Αλγορίθμων

- **Συμμετρική κρυπτογραφία** – η κρυπτογραφία όπου γνωρίζοντας το κλειδί της κρυπτογράφησης K είναι εύκολο να δημιουργήσουμε το κλειδί της αποκρυπτογράφησης K' (στην πράξη K = K΄)
- **Ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού** – η κρυπτογραφία όπου γνωρίζοντας το κλειδί της κρυπτογράφησης είναι υπολογιστικά αδύνατο να δημιουργήσουμε το κλειδί της αποκρυπτογράφησης

Συμμετρική Κρυπτογραφία – Παράδειγμα



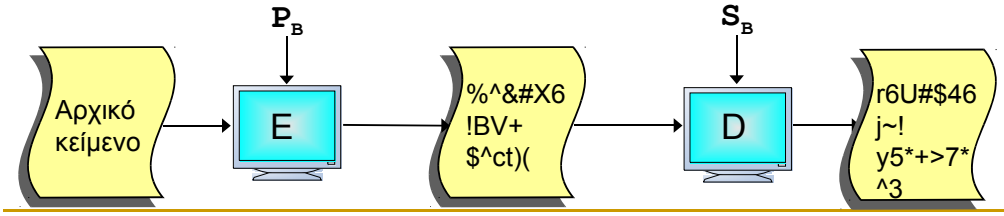
Ερώτηση: Με ποιο τρόπο μπορεί ο Γιάννης να δώσει στον Νίκο το κλειδί **Κ**;

Κρυπτογραφία Δημοσίου Κλειδιού

- Κάθε χρήστης έχει ένα ζεύγος κλειδιών
  - Ιδιωτικό: Γνωστό μόνο στο χρήστη
  - Δημόσιο: Γνωστό σε όλους
- Τα δύο κλειδιά σχετίζονται με κάποιο μαθηματικό τρόπο και σχηματίζουν ένα διατεταγμένο ζεύγος κλειδιών
- Το δημόσιο κλειδί γνωστοποιείται στους ενδιαφερόμενους μέσω δημόσιων βάσεων δεδομένων ή δημόσιων καταλόγων

Κρυπτογραφία Δημοσίου Κλειδιού

- Τυπικές χρήσεις:
  - Ψηφιακές υπογραφές
  - Κρυπτογράφηση
    - Ο αποστολέας **A** κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη **B**, $\mathbf{P_B}$.
    - Ο παραλήπτης αποκρυπτογραφεί με το ιδιωτικό του κλειδί $\mathbf{S_B}$ (μόνο ο **B** μπορεί να αποκρυπτογραφήσει το μήνυμα)



Κρυπτογραφία Δημοσίου Κλειδιού

- Κρυπτογράφηση
  - Δεν ενδείκνυται για την κρυπτογράφηση μεγάλου όγκου δεδομένων (κυρίως λόγω ταχύτητας)
  - Χρησιμοποιείται κυρίως για την μετάδοση (κρυπτογράφηση) συμμετρικών κλειδιών κρυπτογράφησης

Ψηφιακές Υπογραφές

Ψηφιακές Υπογραφές – ΠΔ 150/2001

- **Ηλεκτρονική υπογραφή**: Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.
- **Ψηφιακή υπογραφή (ή προηγμένη ηλεκτρονική υπογραφή)**: Ηλεκτρονική υπογραφή που πληροί τους εξής όρους :
  - συνδέεται μονοσήμαντα με τον υπογράφοντα
  - είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
  - δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και
  - συνδέεται με τα δεδομένα στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων

Ψηφιακές Υπογραφές

*Η **ψηφιακή υπογραφή** που βασίζεται σε **αναγνωρισμένο πιστοποιητικό** και δημιουργείται από **ασφαλή διάταξη δημιουργίας υπογραφής** επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο*
(Π.Δ. 150/2001)

Χρήση Ψηφιακών Υπογραφών Π.Δ. 342/2002

Άρθρο 1
Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο με υποχρεωτική ψηφιακή υπογραφή

1. Αποφάσεις, πιστοποιητικά και βεβαιώσεις, διακινούνται με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α, ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, εφόσον φέρουν ψηφιακή υπογραφή.

2. Γνωμοδοτήσεις, αντίγραφα πρακτικών, εισηγήσεις και εκθέσεις, διακινούνται με ηλεκτρονικό ταχυδρομείο από υπηρεσίες του δημοσίου, Ν.Π.Δ.Δ. και Ο.Τ.Α, προς φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου, εφόσον φέρουν ψηφιακή υπογραφή.

Χρήση Ψηφιακών Υπογραφών Π.Δ. 342/2002

Άρθρο 2
Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο χωρίς ψηφιακή υπογραφή

Η διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο χωρίς ψηφιακή υπογραφή, επιτρέπεται και έχει ισχύ μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α. ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή εννόμων αποτελεσμάτων ή με την άσκηση δικαιώματος, ιδίως όταν έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, οδηγίες, μελέτες, στατιστικά στοιχεία, αιτήσεις παροχής πληροφοριών και σχετικές απαντήσεις.

Χρήση Ψηφιακών Υπογραφών Π.Δ. 342/2002

Άρθρο 2
Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο χωρίς ψηφιακή υπογραφή

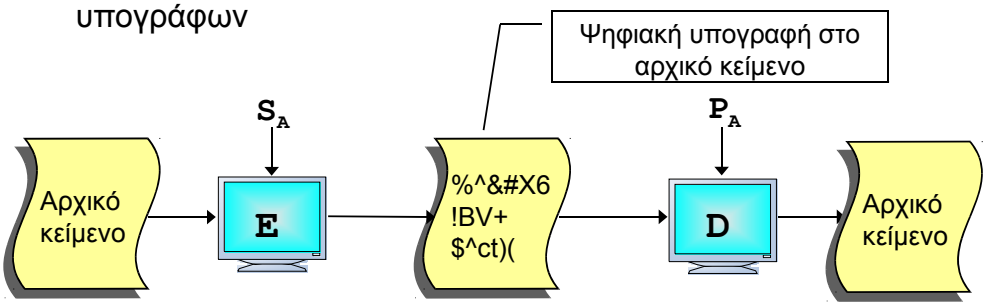
Η διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο χωρίς ψηφιακή υπογραφή, επιτρέπεται και έχει ισχύ μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α. ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή εννόμων αποτελεσμάτων ή με την άσκηση δικαιώματος, ιδίως όταν έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, οδηγίες, μελέτες, στατιστικά στοιχεία, αιτήσεις παροχής πληροφοριών και σχετικές απαντήσεις.

Ψηφιακές Υπογραφές – Ιδιότητες

- Οι ψηφιακές υπογραφές παρέχουν
  - **Αυθεντικοποίηση** – ο παραλήπτης μπορεί να επιβεβαιωθεί για την ταυτότητα του αποστολέα του μηνύματος
  - **Ακεραιότητα** – ο παραλήπτης μπορεί να είναι σίγουρος ότι το μήνυμα δεν έχει αλλοιωθεί από μη εξουσιοδοτημένα άτομα
  - **Μη αποποίηση αποστολέα** (κάτω από ορισμένες προϋποθέσεις) – ο αποστολέας του μηνύματος (και υπογράφων) δε μπορεί να αρνηθεί την αποστολή του μηνύματος

Ψηφιακές Υπογραφές και Κρυπτογραφία Δημοσίου Κλειδιού

- Σε αντίθεση με την κρυπτογραφία δημοσίου κλειδιού
  - Υπογραφή: κρυπτογράφηση με το ιδιωτικό κλειδί του υπογράφων (έστω **A**)
  - Επαλήθευση: αποκρυπτογράφηση με το δημόσιο κλειδί του υπογράφων



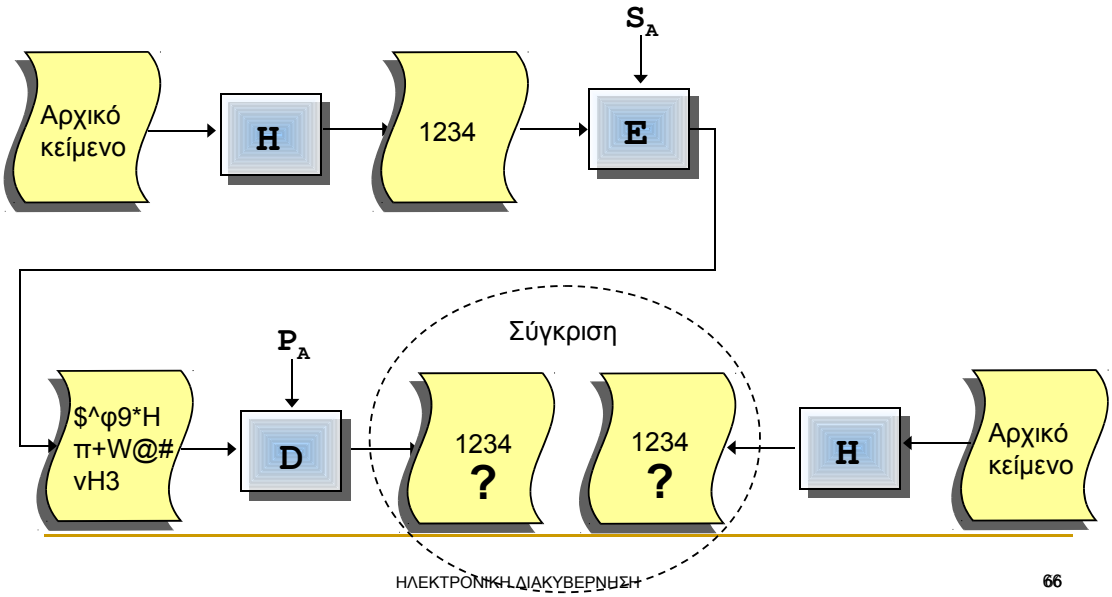
Ψηφιακές Υπογραφές και Συναρτήσεις Σύνοψης

- Οι ψηφιακές υπογραφές στην πράξη απαιτούν τη χρήση συναρτήσεων σύνοψης
- **Συνάρτηση Σύνοψης ή Κατακερματισμού (Hash Function):** είναι μια συνάρτηση η οποία παίρνει ως είσοδο ένα μήνυμα αυθαίρετου μεγέθους και δίνει ως έξοδο ένα μήνυμα συγκεκριμένου μεγέθους

Ψηφιακές Υπογραφές και Συναρτήσεις Σύνοψης

- Δε χρησιμοποιούν κάποιο κλειδί κρυπτογράφησης
- Το κατακερματισμένο μήνυμα χρησιμοποιείται ως είσοδος στον αλγόριθμο κρυπτογράφησης για τη δημιουργία της υπογραφής
- Παράδειγμα:
  - Συνάρτηση: Η σύνοψη αποτελείται από το Τρίτο Γράμμα της Δεύτερης Λέξης, το Πρώτο Γράμμα της Τρίτης, το Τέταρτο Γράμμα της Πέμπτης και το Πρώτο Γράμμα της Έκτης
  - Κείμενο: ΤΟ ΣΕΜΙΝΑΡΙΟ ΑΦΟΡΑ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ
  - Σύνοψη: ΜΑΚΔ

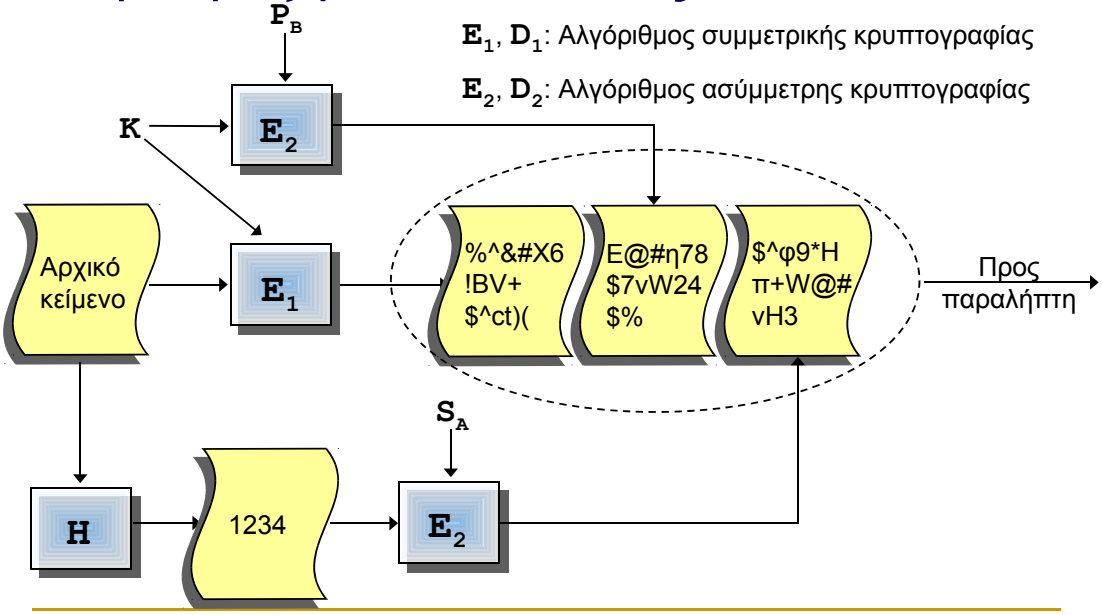
Ψηφιακές Υπογραφές και Συναρτήσεις Σύνοψης



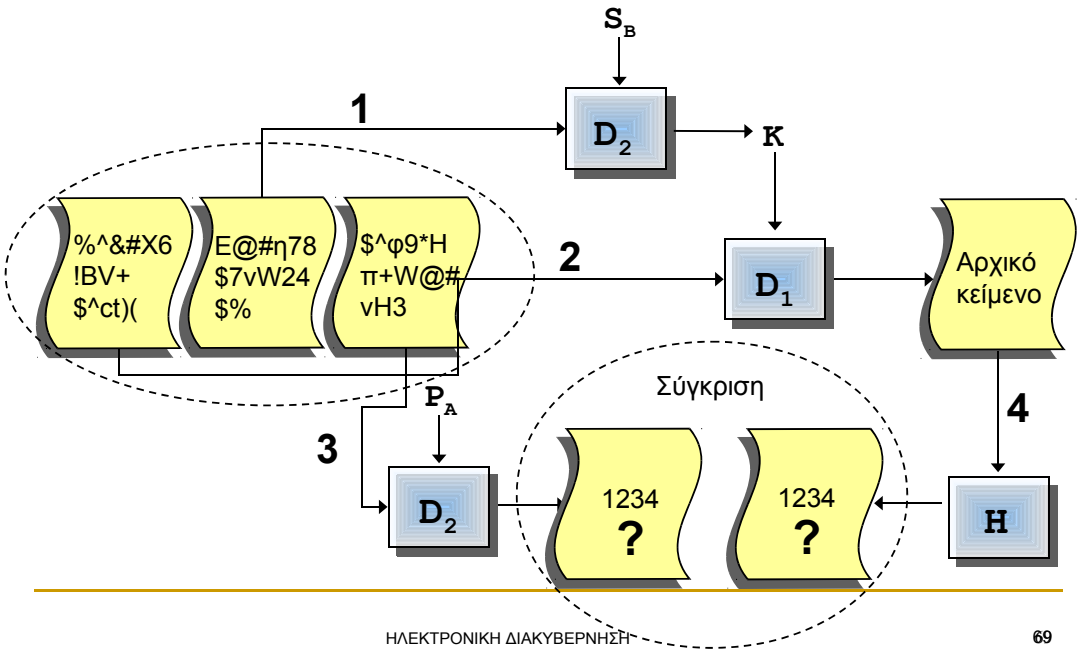
Στην πράξη

- Πως μπορούμε να παρέχουμε εμπιστευτικότητα, ακεραιότητα, και αυθεντικοποίηση σε ένα μήνυμα;
  - Εμπιστευτικότητα: Λόγω ταχύτητας αλγορίθμων επιλέγουμε τη χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας
  - Για τη μεταφορά του κλειδιού επιλέγουμε τη χρήση κρυπτογραφίας δημοσίου κλειδιού (κρυπτογραφούμε με το δημόσιο κλειδί του παραλήπτη)
  - Αυθεντικοποίηση και ακεραιότητα: Κάνουμε χρήση ψηφιακών υπογραφών (κρυπτογραφούμε με το ιδιωτικό μας κλειδί)

Στην πράξη – Αποστολέας Α



Στην πράξη – Παραλήπτης Β



Στην πράξη

- Πως είναι σίγουρος ο αποστολέας Α ότι το δημόσιο κλειδί που χρησιμοποιεί για την κρυπτογράφηση του συμμετρικού κλειδιού είναι του παραλήπτη Β;
- Πως είναι σίγουρος ο παραλήπτης Β ότι το δημόσιο κλειδί που χρησιμοποιεί ο για την επαλήθευση της υπογραφής είναι του αποστολέα Α;

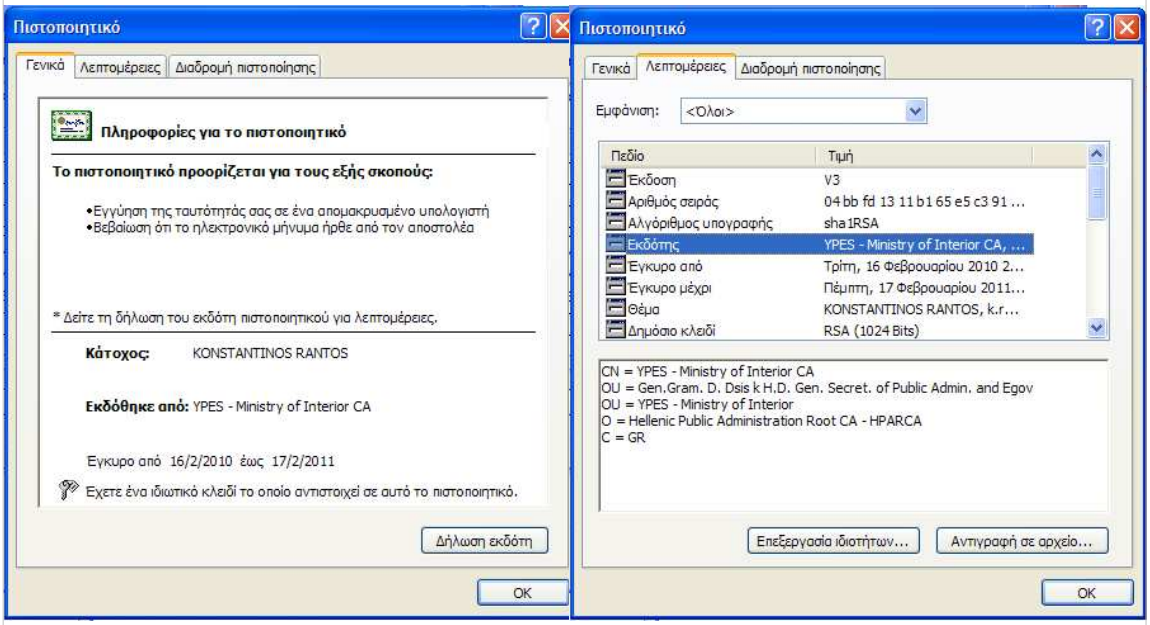
Ψηφιακά πιστοποιητικά
Υποδομές δημοσίου κλειδιού

Ψηφιακά πιστοποιητικά

- Είναι ο μηχανισμός που χρησιμοποιείται για να σχετίσει κάποιες πληροφορίες που αφορούν μια οντότητα με την ταυτότητα αυτής της οντότητας. Αποτελείται από ένα **τμήμα δεδομένων** και από ένα **τμήμα υπογραφής**.
  - Το τμήμα δεδομένων αποτελείται από το όνομα της οντότητας, το δημόσιο κλειδί της, καθώς και άλλες πληροφορίες που αφορούν αυτήν την οντότητα.
  - Το τμήμα υπογραφής αποτελείται από την ψηφιακή υπογραφή μιας έμπιστης τρίτης οντότητας στο τμήμα δεδομένων.
- Λύνουν το πρόβλημα της μετάδοσης ενός αυθεντικοποιημένου αντιγράφου του δημοσίου κλειδιού

Ψηφιακά πιστοποιητικά

- Άλλες πληροφορίες που μπορεί να υπάρχουν στο τμήμα δεδομένων ενός πιστοποιητικού:
  - Μια περίοδος ισχύος του δημοσίου κλειδιού (ημερομηνία έναρξης και ημερομηνία λήξης)
  - Έναν σειριακό αριθμό ο οποίος αναγνωρίζει μοναδικά το πιστοποιητικό.
  - Πρόσθετες πληροφορίες για την οντότητα (π.χ. διεύθυνση)
  - Πρόσθετες πληροφορίες για το κλειδί (π.χ. αλγόριθμος με τον οποίο χρησιμοποιείται και για ποιούς σκοπούς)
  - Πληροφορίες σχετικά με την υπογραφή στο πιστοποιητικό (αλγόριθμος, το όνομα της αρχής πιστοποίησης)



Ψηφιακά πιστοποιητικά

- Για να επαληθεύσει η οντότητα Α την αυθεντικότητα κάποιων πληροφοριών που αφορούν την οντότητα Β (και πιό συγκεκριμένα αυτών των πληροφοριών που περιλαμβάνονται σε ένα πιστοποιητικό) η Α πρέπει να κάνει τα εξής (θεωρούμε ότι η Α έχει ένα αυθεντικοποιημένο αντίγραφο του δημοσίου κλειδιού της έμπιστης τρίτης οντότητας TTP):
  - Να πάρει ένα αντίγραφο του πιστοποιητικού της Β
  - Χρησιμοποιώντας το δημόσιο κλειδί της TTP που υπέγραψε το πιστοποιητικό να επαληθεύσει την υπογραφή στο πιστοποιητικό.
  - Εάν η υπογραφή επαληθευτεί σωστά τότε η Α μπορεί να δεχτεί ότι τα στοιχεία που αφορούν τον Β και περιλαμβάνονται στο πιστοποιητικό ως έγκυρα.

Υποδομή Δημοσίου Κλειδιού

- Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και λειτουργία κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε πιστοποιητικό

Υποδομή Δημοσίου Κλειδιού

- Μια υποδομή δημοσίου κλειδιού απαρτίζεται από:
  - Αρχές πιστοποίησης
  - Αρχές εγγραφής
  - Πιστοποιητικά
  - Τελικούς Χρήστες
  - Τρίτους Συμμετέχοντες
  - Πολιτικές Πιστοποίησης
  - Αποθήκη πιστοποιητικών (repository)
  - Κλειδιά
  - Μηχανισμό ανάκλησης κλειδιών

Υποδομή Δημοσίου Κλειδιού – Αρχή Εγγραφής

- Ο φορέας ή υπηρεσία που έχει εγκριθεί από μια Αρχή Πιστοποίησης και υποβοηθά τους ενδιαφερόμενους κατά την υποβολή αίτησης έκδοσης πιστοποιητικού, εγκρίνει ή απορρίπτει τις αιτήσεις αυτές, καθώς επίσης αιτείται στην Αρχή Πιστοποίησης την έκδοση, ανάκληση, ανανέωση ή ανάκτηση Πιστοποιητικών.
- Οι λόγοι χρήσης μιας αρχής εγγραφής είναι:
  - Να μειωθεί το φόρτο εργασίας της αρχής πιστοποίησης
  - Να μπορεί να καλυφθεί μια μεγαλύτερη γεωγραφική έκταση

Υποδομή Δημοσίου Κλειδιού – Αρχή Εγγραφής

- Η **Αρχή Εγγραφής (Registration Authority)** είναι υπεύθυνη για:
  - τη συλλογή των στοιχείων μιας οντότητας που αιτείται ένα πιστοποιητικό
  - την επαλήθευση της εγκυρότητας των.
  - την παράδοση ενός πιστοποιητικού.
  - τη διαχείριση αιτημάτων του κατόχου αναφορικά με τη διαχείριση των πιστοποιητικών
- Η ΑΕ **δε** μπορεί να εκδώσει πιστοποιητικά.

Υποδομή Δημοσίου Κλειδιού – Αρχή Πιστοποίησης

- Πρόκειται για το Φορέα (έμπιστη τρίτη οντότητα) που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται, να ανακαλεί και να ανανεώνει πιστοποιητικά
- Όταν μια οντότητα αιτείται ενός πιστοποιητικού η αρχή πιστοποίησης συγκεντρώνει τα στοιχεία από την αρχή εγγραφής, δημιουργεί το πιστοποιητικό, το υπογράφει, το διανέμει στην οντότητα που το αιτήθηκε, προαιρετικά το δημοσιεύει, και είναι υπεύθυνη για τη διαχείριση του καθ' όλη τη διάρκεια της ζωής του.

Υποδομή Δημοσίου Κλειδιού

- **Τελικός Χρήστης:** Το υποκείμενο για το οποίο έχει εκδοθεί ένα πιστοποιητικό ύστερα από αίτηση του. Ο Τελικός Χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο πιστοποιητικό.
- **Τρίτος Συμμετέχων:** Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος στις πληροφορίες οι οποίες περιέχονται σε ένα ψηφιακό πιστοποιητικό.
- **Πολιτική Πιστοποίησης:** Πρόκειται για ένα σύνολο κανόνων αναφορικά με τη χρήση ενός πιστοποιητικού μέσα σε μια κοινωνία ή σύνολο εφαρμογών

Υποδομή Δημοσίου Κλειδιού – Μηχανισμός Ανάκλησης Πιστοποιητικών

- Κάθε πιστοποιητικό έχει τυπικά μια ημερομηνία λήξης. Υπάρχουν όμως περιπτώσεις που αυτό το πιστοποιητικό πρέπει να πάψει να είναι έγκυρο πριν την ημερομηνία λήξης του. Τέτοιοι λόγοι περιλαμβάνουν:
  - Αποκάλυψη του αντίστοιχου ιδιωτικού κλειδιού ή υποψία αποκάλυψης.
  - Αλλαγή των στοιχείων της οντότητας για την οποία εκδόθηκε το πιστοποιητικό
  - Αλλαγή της ιδιότητας της οντότητας (προαγωγή, μετάθεση, απόσπαση, κ.λ.π.)

Υποδομή Δημοσίου Κλειδιού – Μηχανισμός Ανάκλησης Πιστοποιητικών

- Σε μια τέτοια περίπτωση γίνεται χρήση ενός μηχανισμού ανάκλησης πιστοποιητικών, δηλ. ενός μηχανισμού που θα δίνει σε μια οντότητα τη δυνατότητα ελέγχου ισχύος ενός πιστοποιητικού. Ένας τέτοιος μηχανισμός είναι ο **κατάλογος ανακληθέντων πιστοποιητικών** (certificate revocation list).
- Ο ΚΑΠ είναι μια υπογεγραμμένη, από την αρχή πιστοποίησης, λίστα με όλα τα πιστοποιητικά που έχουν ανακληθεί. Αποτελεί υποχρέωση της αρχής πιστοποίησης να διατηρεί και να ανανεώνει αυτή τη λίστα ανά τακτά χρονικά διαστήματα.

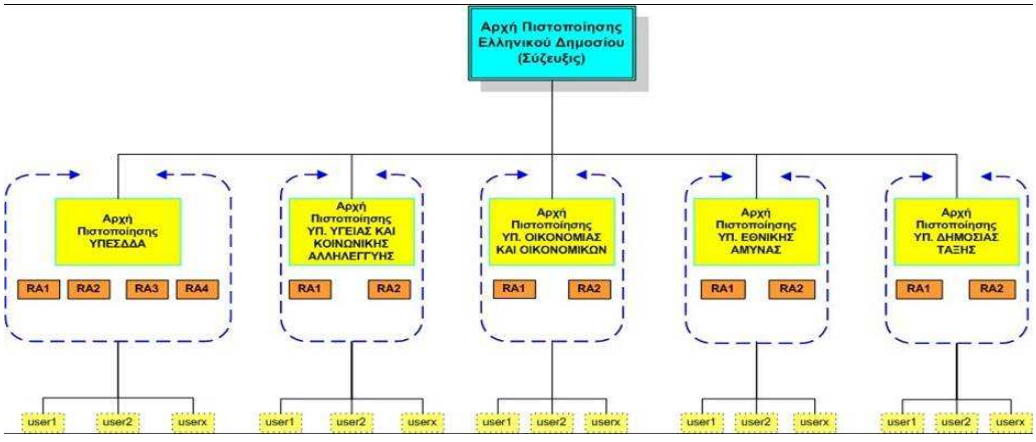
Υποδομή Δημοσίου Κλειδιού

- **Κατάλογος πιστοποιητικών (certificate directory):** Πρόκειται για μια βάση δεδομένων στην οποία οι χρήστες έχουν πρόσβαση ανάγνωσης για να μπορούν να παίρνουν κάποιο πιστοποιητικό. Υπεύθυνη για την διαχείριση όλης της βάσης (εγγραφή νέου πιστοποιητικού, διαγραφή πιστοποιητικών που έχουν λήξει κ.λ.π.) είναι η Αρχή Πιστοποίησης.

Υποδομή Δημοσίου Κλειδιού –
Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

- Ορίστηκε στα πλαίσια του έργου «Εθνικό Δίκτυο Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ» με την ΚΥΑ των Υπουργών
  - Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης
  - Μεταφορών και Επικοινωνιών

Υποδομή Δημοσίου Κλειδιού –
Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)



Υποδομή Δημοσίου Κλειδιού –
Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

- Το ρόλο της Πρωτεύουσας Αρχής Πιστοποίησης τον έχει αναλάβει η Υπηρεσία Ανάπτυξης Πληροφορικής του ΥΠΕΣΔΔΑ
- Προς το παρόν μόνο η Υποκείμενη Αρχή Πιστοποίησης του ΥΠΕΣΔΔΑ είναι σε λειτουργία
  - Σύμφωνα με το ν. 3536/2007 παρέχει υπηρεσίες πιστοποίησης και σε υπαλλήλους άλλων φορέων οι οποίοι δεν έχουν ή δε λειτουργεί ακόμη δική τους Υποκείμενη Αρχή Πιστοποίησης

Υποδομή Δημοσίου Κλειδιού –
Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

- Ο Κανονισμός Πιστοποίησης (ΚΥΑ 2512/2006) ορίζει δύο πολιτικές πιστοποίησης
  - ΠΠ1: Τα πιστοποιητικά χρησιμοποιούνται για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων ή εγγράφων. Βάσει του ΠΔ 150/2001 απαιτείται χρήση «ασφαλών διατάξεων δημιουργίας υπογραφών» (έξυπνες κάρτες)
  - ΠΠ2: Τα πιστοποιητικά χρησιμοποιούνται για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων

Υποδομή Δημοσίου Κλειδιού –
Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

- Η ύπαρξη δύο πολιτικών έχει ως συνέπεια κάθε Τελικός Χρήστης να έχει δύο πιστοποιητικά (και κατ' επέκταση, δύο ζεύγη κλειδιών)
  - Ένα για ψηφιακές υπογραφές (ΠΠ1)
  - Ένα για κρυπτογράφηση (ΠΠ2)
- Ενδεικτικές χρήσεις των πιστοποιητικών
  - Ασφαλής επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου / ανταλλαγής μηνυμάτων (υπογραφή και κρυπτογράφηση)
  - Υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων (π.χ. αρχεία Adobe Acrobat, αρχεία Word)
  - Ασφαλής προσδιορισμός ηλεκτρονικής ταυτότητας
  - Έλεγχος πρόσβασης σε κατάλληλες εφαρμογές.

SSL

Secure Sockets Layer (SSL)

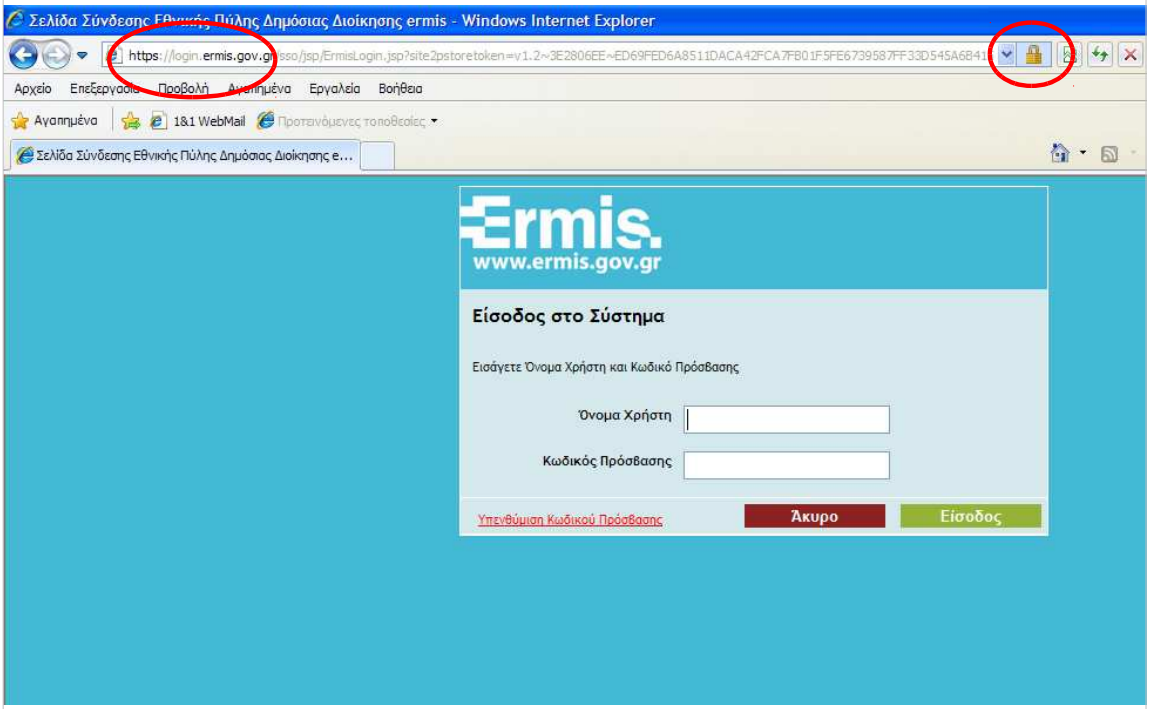
- Πρόκειται για ένα πρωτόκολλο το οποίο παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ ενός πελάτη και ενός διακομιστή για την ανταλλαγή πληροφοριών μέσω Internet.
- Χρησιμοποιεί **κρυπτογραφία δημοσίου κλειδιού** και παρέχει
  - Εμπιστευτικότητα
  - Ακεραιότητα
  - Αυθεντικοποίηση διακομιστή, και
  - Προαιρετικά, αυθεντικοποίηση πελάτη.

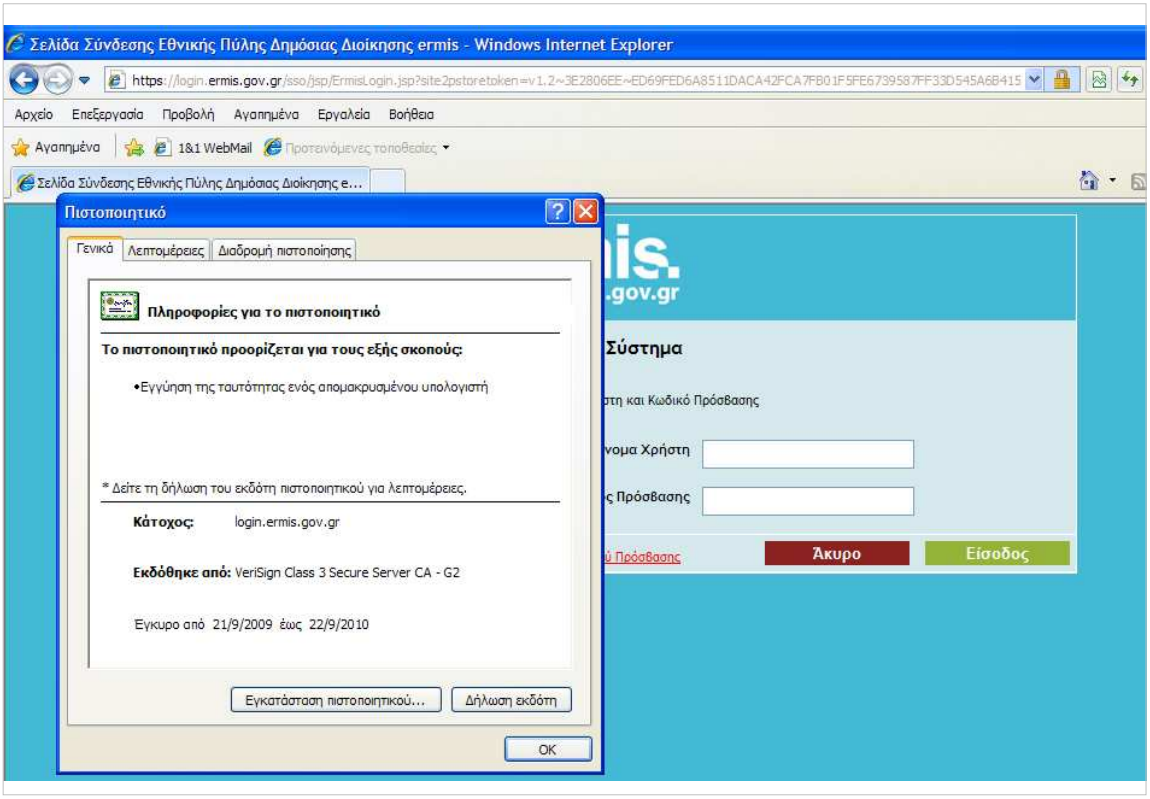
Secure Sockets Layer (SSL)

- Μια ιστοσελίδα μπορεί να έχει δημόσια και προστατευμένα τμήματα. Όταν κάποιος χρήστης/πελάτης επισκέπτεται μια τέτοια ιστοσελίδα και θέλει να έχει πρόσβαση στα προστατευμένα/ασφαλή τμήματα της ιστοσελίδας ο διακομιστής θα ξεκινήσει τη διαδικασία χρήσης του SSL για να προστατεύσει αυτά τα τμήματα της προστατευμένης ιστοσελίδας.

Secure Sockets Layer (SSL)

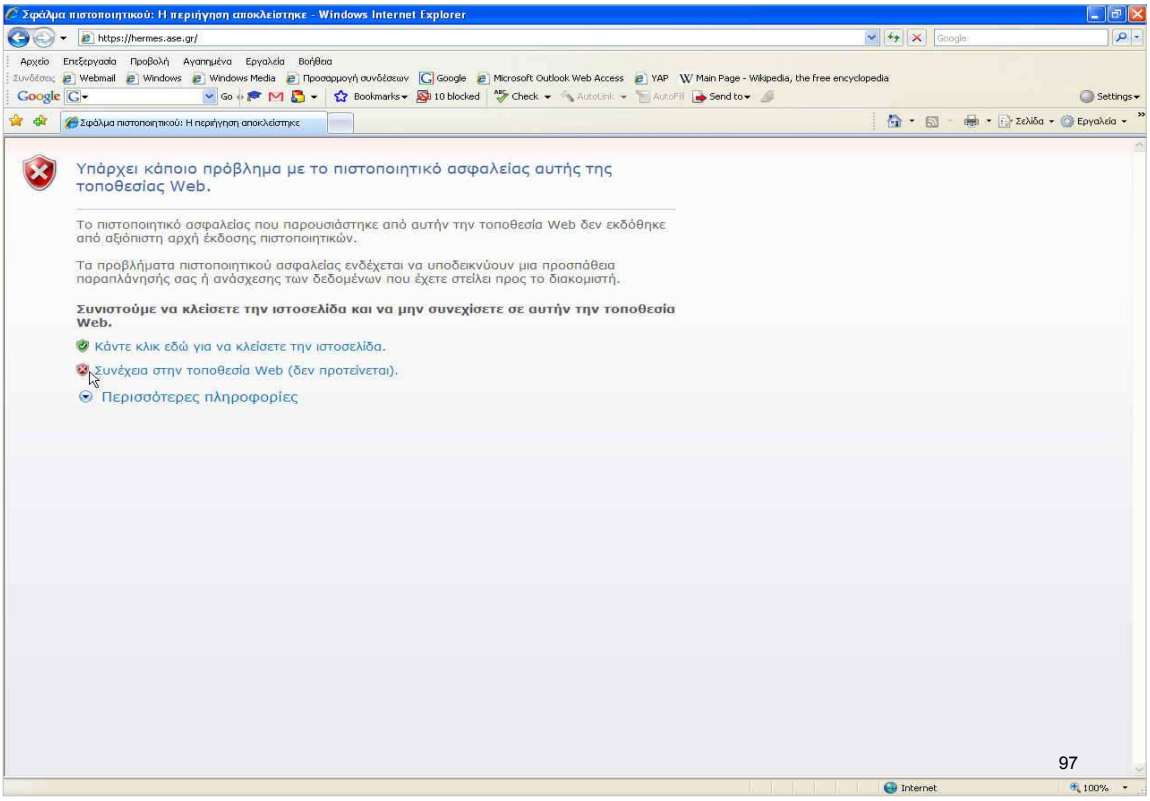
- Ο χρήστης μπορεί να επαληθεύσει μια προστατευμένη (με χρήση του SSL) επικοινωνία
  - εξετάζοντας το URL το οποίο θα πρέπει να ξεκινά με την ακολουθία https:// αντί του http://
  - από την ύπαρξη κλειδαριάς ή ενός κλειδιού στον browser τα οποία υποδηλώνουν την προστασία των δεδομένων.
  - εξετάζοντας το πιστοποιητικό του εξυπηρετητή

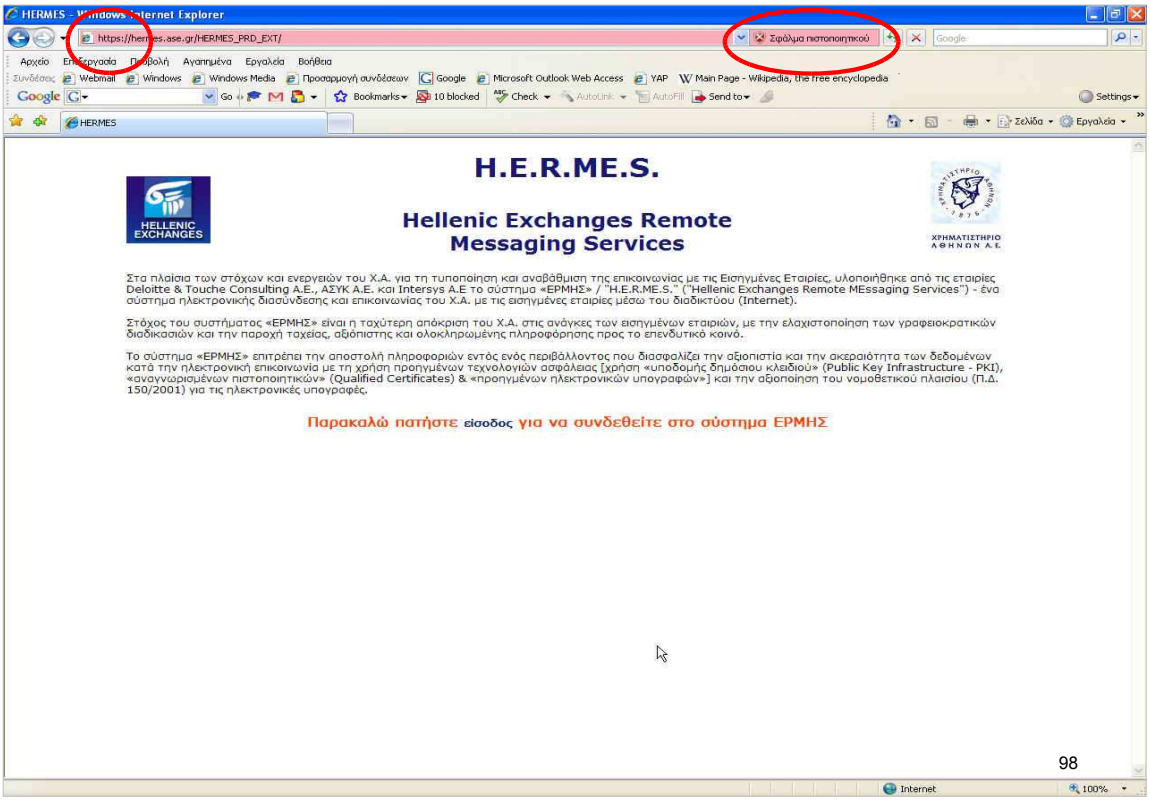


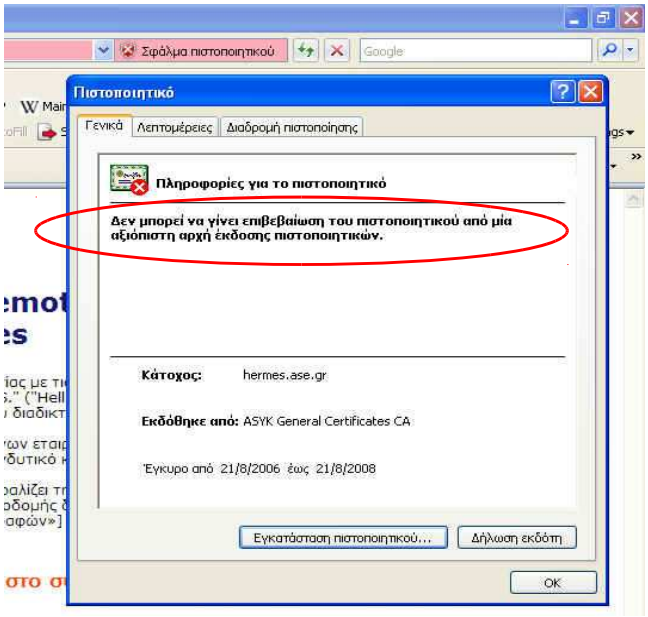


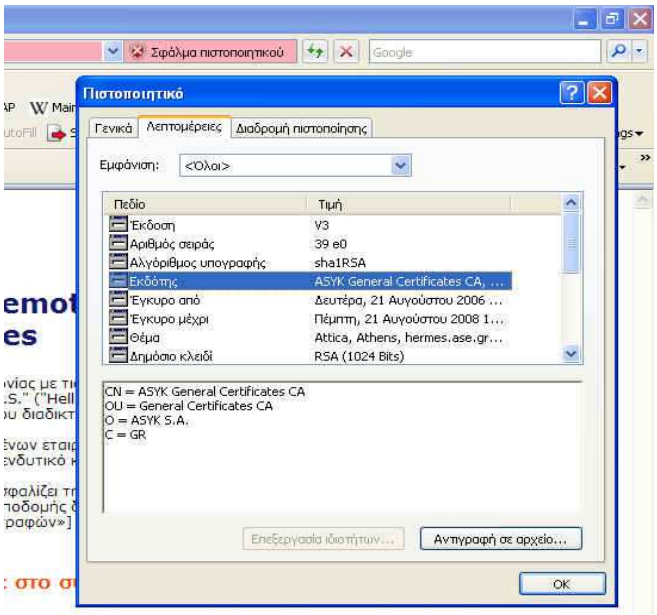
Προβλήματα που μπορεί να παρουσιαστούν

- Το όνομα του διακομιστή να είναι διαφορετικό από αυτό του υποκειμένου του πιστοποιητικού
- Να έχει λήξει το πιστοποιητικό
- Το πιστοποιητικό να έχει εκδοθεί από κάποια Αρχή Πιστοποίησης της οποίας το κλειδί δεν υπάρχει προεγκατεστημένο στον browser


Σφάλμα πιστοποιητικού: Η περιήγηση αποκλείστηκε - Windows Internet Explorer
https://hermes.ase.gr/
Υπάρχει κάποιο πρόβλημα με το πιστοποιητικό ασφαλείας αυτής της τοποθεσίας Web.
Το πιστοποιητικό ασφαλείας που παρουσιάστηκε από αυτήν την τοποθεσία Web δεν εκδόθηκε από αξιόπιστη αρχή έκδοσης πιστοποιητικών.
Τα προβλήματα πιστοποιητικού ασφαλείας ενδέχεται να υποδεικνύουν μια προσπάθεια παραπλάνησής σας ή ανάσχεσης των δεδομένων που έχετε στείλει προς το διακομιστή.
Συνιστούμε να κλείσετε την ιστοσελίδα και να μην συνεχίσετε σε αυτήν την τοποθεσία Web.
Κάντε κλικ εδώ για να κλείσετε την ιστοσελίδα.
Συνέχεια στην τοποθεσία Web (δεν προτείνεται).
Περισσότερες πληροφορίες
97


https://hermes.ase.gr/HERMES_PRD_EXT/
Σφάλμα πιστοποιητικού
H.E.R.M.E.S.
Hellenic Exchanges Remote Messaging Services
Στα πλαίσια των στόχων και ενεργειών του Χ.Α. για τη τυποποίηση και αναβάθμιση της επικοινωνίας με τις Εισηγμένες Εταιρίες, υλοποιήθηκε από τις εταιρίες Deloitte & Touche Consulting A.E., ΑΣΥΚ Α.Ε. και Intersys A.E το σύστημα «ΕΡΜΗΣ» / "H.E.R.ME.S." ("Hellenic Exchanges Remote MEssaging Services") - ένα σύστημα ηλεκτρονικής διασύνδεσης και επικοινωνίας του Χ.Α. με τις εισηγμένες εταιρίες μέσω του διαδικτύου (Internet).
Στόχος του συστήματος «ΕΡΜΗΣ» είναι η ταχύτερη απόκριση του Χ.Α. στις ανάγκες των εισηγμένων εταιριών, με την ελαχιστοποίηση των γραφειοκρατικών διαδικασιών και την παροχή ταχείας, αξιόπιστης και ολοκληρωμένης πληροφόρησης προς το επενδυτικό κοινό.
Το σύστημα «ΕΡΜΗΣ» επιτρέπει την αποστολή πληροφοριών εντός ενός περιβάλλοντος που διασφαλίζει την αξιοπιστία και την ακεραιότητα των δεδομένων κατά την ηλεκτρονική επικοινωνία με τη χρήση προηγμένων τεχνολογιών ασφάλειας [χρήση «υποδομής δημόσιου κλειδιού» (Public Key Infrastructure - PKI), «αναγνωρισμένων πιστοποιητικών» (Qualified Certificates) & «προηγμένων ηλεκτρονικών υπογραφών»] και την αξιοποίηση του νομοθετικού πλαισίου (Π.Δ. 150/2001) για τις ηλεκτρονικές υπογραφές.
Παρακαλώ πατήστε είσοδος για να συνδεθείτε στο σύστημα ΕΡΜΗΣ
98


Σφάλμα πιστοποιητικού
Google
Πιστοποιητικό
Γενικά
Λεπτομέρειες
Διαδρομή πιστοποίησης
Πληροφορίες για το πιστοποιητικό
Δεν μπορεί να γίνει επιβεβαίωση του πιστοποιητικού από μία αξιόπιστη αρχή έκδοσης πιστοποιητικών.
Κάτοχος: hermes.ase.gr
Εκδόθηκε από: ASYK General Certificates CA
Έγκυρο από 21/8/2006 έως 21/8/2008
Εγκατάσταση πιστοποιητικού...
Δήλωση εκδότη
OK


Σφάλμα πιστοποιητικού
Google
Πιστοποιητικό
Γενικά
Λεπτομέρειες
Διαδρομή πιστοποίησης
Εμφάνιση: <Όλοι>
Πεδίο
Τιμή
Έκδοση V3
Αριθμός σειράς 39 e0
Αλγόριθμος υπογραφής sha1RSA
Εκδότης ASYK General Certificates CA, ...
Έγκυρο από Δευτέρα, 21 Αυγούστου 2006 ...
Έγκυρο μέχρι Πέμπτη, 21 Αυγούστου 2008 1...
Θέμα Attica, Athens, hermes.ase.gr...
Δημόσιο κλειδί RSA (1024 Bits)
CN = ASYK General Certificates CA
OU = General Certificates CA
O = ASYK S.A.
C = GR
Επεξεργασία ιδιοτήτων...
Αντιγραφή σε αρχείο...
OK

ΚΩΝΣΤΑΝΤΙΝΟΣ ΡΑΝΤΟΣ
ΜΗΧΑΝΙΚΟΣ Η/Υ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ (MSc, PhD)
ΥΠΕΣΑΗΔ
2131313923
k.rantos@ypes.gov.gr