ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΓΙΑ ΑΣΦΑΛΕΙΣ ΣΥΝΑΛΛΑΓΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

ΣΠΟΥΔΑΣΤΡΙΑ:

ΑΡΓΥΡΟΥΛΑΣ ΤΣΙΝΤΖΟΥΡΑ Α.Μ: 631

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ:

ΣΩΤΗΡΙΑ ΑΝΤΩΝΟΠΟΥΛΟΥ

ΠΑΤΡΑ 2013

PDF created with pdfFactory Pro trial version www.pdffactory.com

Περιεχόμενα

PDF created with pdfFactory Pro trial version www.pdffactory.com

PDF created with pdfFactory Pro trial version www.pdffactory.com

PDF created with pdfFactory Pro trial version www.pdffactory.com

Περίληψη

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (εμπιστευτικότητα). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία.

Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής. Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί (public key) του αποστολέα.

Το Π.Δ. 150/2000 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εισαγωγή

Η ανάπτυξη του Διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας στις διαδικασίες και στις συναλλαγές, η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσομένων.

Θα πρέπει επισημάνουμε πως με το όρο ηλεκτρονικές συναλλαγές δεν εννοούμε μόνο τις οικονομικές συναλλαγές αλλά κάθε ανταλλαγή δεδομένων που γίνεται στο διαδίκτυο. Τα δεδομένα αυτά απαγορεύεται να αλλοιωθούν κατά την μετάδοση τους και ο παραλήπτης θα πρέπει να τα λαμβάνει χωρίς την παραμικρή τους αλλοίωση. Ο παραλήπτης θα πρέπει επίσης να είναι σίγουρος για την ταυτότητα του αποστολέα. Σε μια συναλλαγή οποιοσδήποτε συμμετέχει δεν θα πρέπει να μπορεί να αρνηθεί την συμμετοχή του στην συναλλαγή εκ των υστέρων.

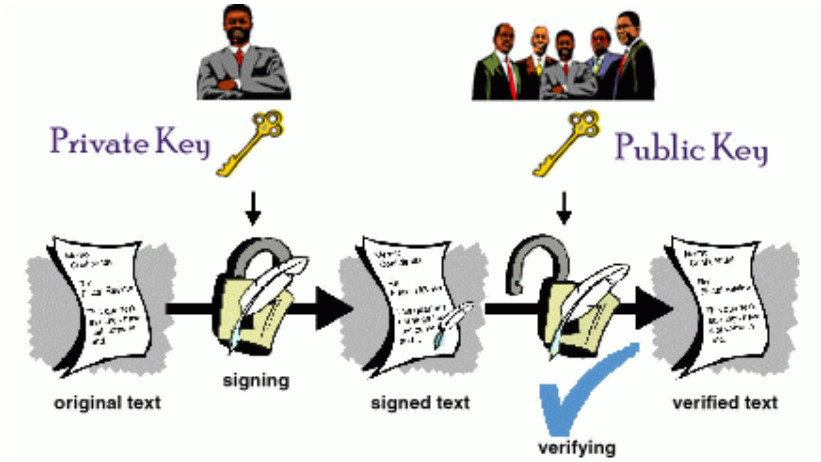
Γίνεται λοιπόν αντιληπτό ότι όλοι οι χρήστες οι οποίοι συναλλάσσονται ηλεκτρονικά απαιτούν να υπάρχει πάντα σε αυτές τις συναλλαγές:

- **Εμπιστευτικότητα:** Προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Έτσι ώστε να είναι σίγουρος ο αποστολές και ο παραλήπτης ότι κανένας μη εξουσιοδοτημένος χρήστης δεν είχε πρόσβαση στα δεδομένα.
- **Ακεραιότητα:** Προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Έτσι ώστε να υπάρχουν εγγυήσεις για το ότι τα δεδομένα που φτάνουν από τον αποστολέα στον παραλήπτη φτάνουν αναλλοίωτα και με ακεραιότητα.
- **Αυθεντικότητα:** Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα
- **Μη αποποίηση ευθύνης:** Επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών.

Η ανάγκη για αξιοπιστία, εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα ικανοποιείται με την κρυπτογραφία. Στην συνέχεια της παρουσίασης αυτής θα μιλήσουμε αναλυτικότερα για την κρυπτογραφία, εδώ απλώς θα πρέπει να αναφέρουμε ότι στην κρυπτογραφία ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο. Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρούν την πληροφορία ασφαλή και χρησιμοποιούνται και στην κρυπτογράφηση αλλά και στην αποκρυπτογράφηση. Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης όταν λάβει τα δεδομένα αποκρυπτογραφεί το κείμενο και το μετατρέπει στην μορφή που είχε πριν.

Φυσικά όλα όσα αναφέρθηκαν έως τώρα θα ήταν κενά περιεχομένου και άνευ ουσίας αν δεν οργανώνονταν και δεν καλύπτονταν από ένα ολοκληρωμένο νομικό πλαίσιο, το οποίο θα παρουσιαστεί αναλυτικά στην συνέχεια.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 1.Δημιουργία Ψηφιακής Υπογραφής

PDF created with pdfFactory Pro trial version www.pdffactory.com

1. Ψηφιακή Υπογραφή

[14]Η πιο σημαντική εφαρμογή της κρυπτογραφίας με δημόσιο-κλειδί [14] είναι η Ψηφιακή Υπογραφή. Η Ψηφιακή Υπογραφή παρέχει επίπεδα προστασίας που είναι δύσκολο να επιτευχθούν με οποιοδήποτε άλλο τρόπο. Ξεκινάμε αυτό το κεφάλαιο κάνοντας μια γενική αναφορά στις Ψηφιακές Υπογραφές. Στη συνέχεια αναφερόμαστε στα Πρωτόκολλα Αυθεντικοποίησης (authentication protocols), πολλά από τα οποία εξαρτώνται από τη χρήση της Ψηφιακής Υπογραφής. Τελειώνοντας, αναφερόμαστε στα Ψηφιακά Πρότυπα Υπογραφών (DSS).

Η Αυθεντικοποίηση μηνυμάτων προστατεύει δύο χρήστες που ανταλλάσουν μηνύματα από κάποιον αντίπαλο. Δεν παρέχει προστασία όμως του ενός χρήστη από τον άλλο. Είναι δυνατόν να υπάρξουν αρκετές διαφωνίες μεταξύ τους. Για παράδειγμα, έστω ότι ο Πέτρος στέλνει ένα μήνυμα στον Θωμά. Κάποιες από τις διαφωνίες που μπορεί να προκύψουν είναι οι εξής:

1. Ο Θωμάς μπορεί να ανασκευάσει ένα μήνυμα και να ισχυριστεί ότι το έστειλε ο Πέτρος. Το μόνο που έχει να κάνει ο Θωμάς είναι να ανασκευάσει ένα μήνυμα και να επισυνάψει ένα κωδικό αυθεντικοποίησης, χρησιμοποιώντας το κλειδί που μοιράζονται με το Πέτρο.

2. Ο Πέτρος μπορεί να αρνηθεί ότι έστειλε το μήνυμα. Επειδή όμως είναι πιθανό ο Θωμάς να ανασκευάσει ένα μήνυμα, δεν υπάρχει τρόπος να αποδειχθεί ότι τελικά ο Πέτρος δεν έστειλε το μήνυμα.

[2]Και τα δύο σενάρια δημιουργούν ανησυχίες ως προς τη νομιμότητά τους. Ένα παράδειγμα του πρώτου σεναρίου: κατά την πραγματοποίηση μιας ηλεκτρονικής συναλλαγής κεφαλαίου, ο παραλήπτης αυξάνει το ποσό του μεταφερόμενου κεφαλαίου και ισχυρίζεται ότι το ποσό αυτό εστάλη από τον αποστολέα. Ένα παράδειγμα για το δεύτερο σενάριο: ένα ηλεκτρονικό μήνυμα που περιέχει οδηγίες σε ένα χρηματιστή για την πραγματοποίηση μιας συναλλαγής η οποία αποδεικνύεται ζημιογόνα. Ο αποστολέας μπορεί να ισχυριστεί ότι δεν έστειλε ποτέ αυτό το μήνυμα.

Σε περιπτώσεις που δεν υπάρχει απόλυτη εμπιστοσύνη μεταξύ αποστολέα και παραλήπτη, χρειάζεται κάτι περισσότερο από την αυθεντικοποίηση των μηνυμάτων. Η πιο ενδεδειγμένη λύση σε αυτό το πρόβλημα φαίνεται να είναι η Ψηφιακή Υπογραφή. Η Ψηφιακή Υπογραφή θεωρείται αντίστοιχη της ιδιόχειρης και πρέπει να έχει τις ακόλουθες ιδιότητες:

1. Να μπορεί να επιβεβαιώνει τον συγγραφέα, την ημερομηνία και την ώρα της υπογραφής.

2. Να μπορεί να πιστοποιεί την αυθεντικότητα του περιεχομένου του μηνύματος τη στιγμή που υπογράφθηκε.

3. Η υπογραφή πρέπει να επιβεβαιώνεται και από τρίτους, έτσι ώστε να μπορούν να λυθούν διαφωνίες.

Επιπλέον, η συνάρτηση της Ψηφιακής Υπογραφής εμπεριέχει τη συνάρτηση Αυθεντικοποίησης.

Με βάση τις παραπάνω ιδιότητες, μπορούμε να μορφοποιήσουμε τις απαιτήσεις της Ψηφιακής Υπογραφής ως εξής:

4. Η υπογραφή πρέπει να είναι μια αλληλουχία bit που να είναι διαφορετική για κάθε μήνυμα που υπογράφεται.

PDF created with pdfFactory Pro trial version www.pdffactory.com

5. Η υπογραφή πρέπει να χρησιμοποιεί μερικές μοναδικές πληροφορίες για τον αποστολέα, ώστε να αποτρέπεται η πλαστογραφία και η άρνηση αποστολής ενός μηνύματος.

6. Πρέπει να είναι σχετικά εύκολο να παραχθεί η Ψηφιακή Υπογραφή.

7. Πρέπει να είναι σχετικά εύκολο να αναγνωρίζεται και να επιβεβαιώνεται μια Ψηφιακή Υπογραφή.

8. Πρέπει να είναι υπολογιστικά αδύνατο να πλαστογραφήσεις μια Ψηφιακή Υπογραφή, είτε κατασκευάζοντας ένα νέο μήνυμα για μια ήδη υπάρχουσα Ψηφιακή Υπογραφή, είτε κατασκευάζοντας μια ψευδή Ψηφιακή Υπογραφή από κάποιο μήνυμα.

9. Πρέπει να είναι πρακτικά εύκολο να αποθηκεύεις αντίγραφο της Ψηφιακής Υπογραφής στη μνήμη.

Έχουν προταθεί διάφορες προσεγγίσεις για το θέμα της συνάρτησης της Ψηφιακής Υπογραφής. Οι προσεγγίσεις αυτές χωρίζονται σε 2 κατηγορίες: την Άμεση και την Παραμετρική.

[14]Η Άμεση Ψηφιακή Υπογραφή εμπλέκει μόνο αυτούς που επικοινωνούν (αποστολέα, παραλήπτη). Υποτίθεται ότι ο παραλήπτης γνωρίζει το δημόσιο κλειδί του αποστολέα. Μια Ψηφιακή Υπογραφή μπορεί να παραχθεί κρυπτογραφώντας όλο το μήνυμα από το κλειδί του αποστολέα ή κρυπτογραφώντας ένα μέρος του μηνύματος με Hash code (Κώδικα Μετασχηματισμού), χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα.

Άμεση Ψηφιακή Υπογραφή

Η Εμπιστευτικότητα μπορεί να παρασχεθεί με περαιτέρω κρυπτογράφηση όλου του μηνύματος μαζί με την υπογραφή, είτε με το δημόσιο κλειδί του παραλήπτη (κρυπτογράφηση δημόσιου κλειδιού), είτε με ένα κοινό μεταξύ τους δημόσιο κλειδί (συμβατική κρυπτογράφηση). Να σημειωθεί ότι είναι σημαντικό πρώτα να εκτελεστεί η συνάρτηση για την Ψηφιακή Υπογραφή και μετά η συνάρτηση για την Εμπιστευτικότητα. Σε περίπτωση διαφωνίας, ένας τρίτος πρέπει να δει το μήνυμα και την υπογραφή. Αν η υπογραφή έχει μαθηματικό συσχετισμό με το μήνυμα, τότε πρέπει να δοθεί το κλειδί κρυπτογράφησης στον παρατηρητή για να διαβάσει το μήνυμα. Αν όμως η υπογραφή είναι «εσωτερική διαδικασία», τότε ο παραλήπτης μπορεί να αποθηκεύσει το κείμενο του μηνύματος και την υπογραφή για μελλοντική επίλυση διαφωνιών.

Όλες οι περιπτώσεις Άμεσης Ψηφιακής Υπογραφής μέχρι τώρα έχουν μια αδυναμία: όλες εξαρτώνται από το επίπεδο ασφάλειας αποστολής του ιδιωτικού κλειδιού του αποστολέα. Αν ο αποστολέας κάποια στιγμή αποφασίσει να αρνηθεί ότι έστειλε κάποιο μήνυμα, τότε μπορεί να ισχυρισθεί ότι το ιδιωτικό του κλειδί εκλάπη ή χάθηκε και πως κάποιος άλλος οικειοποιήθηκε την υπογραφή του. Ο έλεγχος από το διαχειριστή του συστήματος που αφορά την ασφάλεια των ιδιωτικών κλειδιών μπορεί να αντικρούσει ή να αμφισβητήσει αυτόν τον ισχυρισμό, αλλά παρόλα αυτά ο κίνδυνος να συμβεί αυτό θα συνεχίσει να υπάρχει ως ένα βαθμό. Ένα παράδειγμα είναι να απαιτείται κάθε υπογεγραμμένο μήνυμα να φέρει χρονοσήμανση (ημερομηνία και ώρα) και να απαιτείται άμεση αναφορά των εμπλεκόμενων κλειδιών στον κεντρικό διαχειριστή του συστήματος.

PDF created with pdfFactory Pro trial version www.pdffactory.com

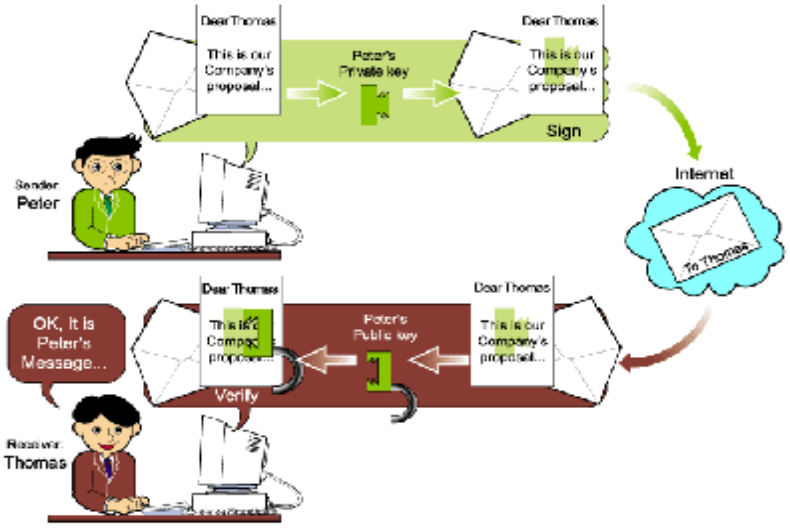
Μια άλλη απειλή είναι το ότι κάποια ιδιωτικά κλειδιά μπορεί πραγματικά να κλαπούν από τον Χ τον χρόνο Τ. Ο αντίπαλος μπορεί να στείλει ένα μήνυμα με την υπογραφή του Χ και να βάλει χρονοσήμανση προγενέστερη ή ίδια με τον Τ.

Ελεγχόμενη Ψηφιακή Υπογραφή

[14]Τα προβλήματα [14] που παρουσιάζονται στην Άμεση Ψηφιακή Υπογραφή μπορούν να ξεπεραστούν χρησιμοποιώντας έναν επόπτη.

Όπως και στις περιπτώσεις της Άμεσης Ψηφιακής Υπογραφής, υπάρχουν αρκετές περιπτώσεις υπογραφής με επόπτη. Σε γενικές γραμμές, όλοι λειτουργούν ως εξής: κάθε υπογεγραμμένο μήνυμα από τον αποστολέα Χ στον παραλήπτη Υ πηγαίνει πρώτα στον Α, ο οποίος υποβάλλει το μήνυμα και την υπογραφή σε κάποιες δοκιμές για να ελέγξει την προέλευση και το περιεχόμενο. Τότε στο μήνυμα μπαίνει χρονοσήμανση και εν συνεχεία στέλνεται στον Υ με σήμανση ότι έχει πιστοποιηθεί, σύμφωνα με τις απαιτήσεις του παρόχου. Η ύπαρξη του Α λύνει το πρόβλημα που εμφανίζεται στις περιπτώσεις της Άμεσης Ψηφιακής Υπογραφής, δηλαδή ότι το μήνυμα μπορεί και να μην ανήκει στον Χ.

Ο επόπτης παίζει ένα κρίσιμο ρόλο σε αυτές τις περιπτώσεις και όλα τα μέλη πρέπει να εμπιστεύονται το μηχανισμό ελέγχου του επόπτη. Η χρήση ενός έμπιστου συστήματος μπορεί να ικανοποιήσει τις παραπάνω απαιτήσεις.



Εικόνα 2. Διαδικασία Αποστολής Ψηφιακού Υπογεγραμμένου Έγγραφου μεταξύ χρηστών

PDF created with pdfFactory Pro trial version www.pdffactory.com

1.1 Ψηφιακή υπογραφή – Ιδιόχειρη υπογραφή

Με το άρθρο 3 του προεδρικού διατάγματος 150/2001 η ψηφιακή υπογραφή εξομοιώνεται με την ιδιόχειρη. Πέρα όμως από αυτήν την εξομοίωση υπάρχουν κάποιες ουσιαστικές διαφορές μεταξύ της ψηφιακής και της ιδιόχειρης υπογραφής, κάποιες από τις διαφορές των δύο υπογραφών είναι οι εξής:

1. Η ιδιόχειρη υπογραφή είναι ενσωματωμένη στο μήνυμα, αντίθετα η ψηφιακή υπογραφή αποτελεί εξωτερικό «αντικείμενο» το οποίο συνδέεται με το μήνυμα.

2. Για όλους τους σκοπούς χρησιμοποιείται η ίδια υπογραφή σε ότι αφορά την ιδιόχειρη υπογραφή. Στην ψηφιακή υπογραφή έχουμε την χρήση διαφορετικών υπογραφών για διαφορετικούς σκοπούς.

3. Στην ιδιόχειρη υπογραφή υπάρχει δυνατότητα πλαστογράφησης. Στην ψηφιακή υπογραφή είναι σχεδόν αδύνατη η πλαστογράφησή της.

4. Η ιδιόχειρη υπογραφή πιστοποιεί την ταυτότητα του υπογράφοντος. Η ψηφιακή υπογραφή πιστοποιεί την γνησιότητα του περιεχομένου της πληροφορίας και την ταυτότητα του υπογράφοντος.

5. Η ιδιόχειρη υπογραφή είναι απευθείας ορατή, αντίθετα για την ψηφιακή υπογραφή απαιτείται ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια για να είναι ορατή.

6. Στην ιδιόχειρη υπογραφή ο «μηχανισμός» δημιουργίας της παραμένει ο ίδιος και δεν μπορεί να αποσυρθεί. Στην ψηφιακή υπογραφή ο μηχανισμός δημιουργίας της μπορεί να καταστραφεί ή να αποσυρθεί και να υποκατασταθεί από κάποιον εντελώς διαφορετικό.

Σε αντιδιαστολή λοιπόν, με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ηλεκτρονικής υπογραφής διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα αφού προκύπτει με βάση και αυτά. Η ψηφιακή υπογραφή σε ένα ηλεκτρονικό κείμενο δεν είναι παρά μια σειρά από bits, προσαρτημένη σε αυτό, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση του υπογράφοντος και την επαλήθευση της ακεραιότητας του μηνύματος.

PDF created with pdfFactory Pro trial version www.pdffactory.com

2. Το Νομικό Πλαίσιο

2.1 Διεθνή και Ευρωπαϊκό Νομικό Πλαίσιο

[8]Η νομική αναγνώριση των ηλεκτρονικών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη. Σε διεθνές επίπεδο, η Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) συνέταξε το 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, ρυθμίζοντας με αυτόν τον νόμο ζητήματα όπως:

1. η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης,
2. η νομική ισχύς της ηλεκτρονικής υπογραφής,
3. η αποδεικτική δύναμη των ηλεκτρονικών κειμένων,
4. ο τόπος, χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος.

Σε διεθνές επίπεδο, μπορούμε να διακρίνουμε δύο διαφορετικές νομικές προσεγγίσεις:

1. Τη μινιμαλιστική προσέγγιση (minimalist approach), όπου «κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή», και

2. Την αναλυτική προσέγγιση (prescriptive approach), σύμφωνα με την οποία «μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας.

Η Ευρωπαϊκή Ένωση, με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές (EEL 13/19.1.2000) ακολούθησε μία μικτή προσέγγιση δύο επιπέδων (two-tier approach), η οποία συνδυάζει και τις δύο παραπάνω κατευθύνσεις.

Η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως ηλεκτρονικές υπογραφές - οι οποίες μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες (ά. 5§2 της Οδηγίας) - όλα τα «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (ά. 2§1 της Οδηγίας).

[8]Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο απλές (π.χ. απλή αναγραφή του ονόματος του συντάξαντος στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής στο ηλεκτρονικό ταχυδρομείο ή του αριθμού του τηλεφώνου αποστολής σε ένα μήνυμα από κινητό τηλέφωνο κ.τ.λ.), ως τις πιο σύνθετες (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων κ.τ.λ.), ανεξάρτητα δηλαδή από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

Από την κανονιστική πλευρά, η Οδηγία διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών - αποκαλούμενες συχνά ως αναγνωρισμένες ψηφιακές υπογραφές - στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές, σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους. Σε αυτήν την κατηγορία ανήκουν όλες οι προηγμένες ψηφιακές

PDF created with pdfFactory Pro trial version www.pdffactory.com

υπογραφές που, επιπλέον, βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής (ά. 5§1).

Η Ευρωπαϊκή Ένωση, αναγνωρίζοντας την ανάγκη νομικής ρύθμισης των ηλεκτρονικών εμπορικών συναλλαγών, εξέδωσε Οδηγία για το ηλεκτρονικό εμπόριο. Πιο συγκεκριμένα, το Ευρωπαϊκό Κοινοβούλιο προέβη το 1999 στην έκδοση της υπ' αριθμ. 2000/31/ΕΚ Οδηγίας, η οποία τέθηκε σε ισχύ στις 17/07/2000. Με την Οδηγία αυτή καθιερώθηκε η αρχή της ελευθερίας σύναψης ηλεκτρονικών συμβάσεων, η αρχή της χώρας προέλευσης, που σήμαινε ότι το Δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το Δίκαιο της χώρας μόνιμης εγκατάστασης του φορέα παροχής υπηρεσιών, και ο εξωδικαστικός διακανονισμός των διαφορών που θα προκύψουν.

Το Ευρωκοινοβούλιο, προκειμένου να διασφαλίσει τη γνησιότητα της ηλεκτρονικής υπογραφής, προέβλεψε την έκδοση αναγνωρισμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, μιας ηλεκτρονικής βεβαίωσης, η οποία συνδέει δεδομένα επαλήθευσης της υπογραφής με ένα φυσικό πρόσωπο, επιβεβαιώνοντας έτσι την ταυτότητά του.

[7]Ως προηγμένες ηλεκτρονικές υπογραφές (οι οποίες όπως θα αναφέρουμε και πιο κάτω, στο εθνικό μας δίκαιο – Π.Δ. 150/2001 - αποκαλούνται και ψηφιακές υπογραφές), η Οδηγία προσδιορίζει τις ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις: συνδέονται μονοσήμαντα με τον υπογράφοντα, είναι ικανές να ταυτοποιήσουν τον υπογράφοντα, δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση στα εν λόγω δεδομένα (ά. 2§2). Οι συγκεκριμένες απαιτήσεις μπορούν να ικανοποιηθούν σήμερα μόνο με την χρήση της τεχνολογίας της ασύμμετρης κρυπτογραφίας η οποία κάνει χρήση ιδιωτικών (δεδομένα δημιουργίας υπογραφής) και δημοσίων (δεδομένα επαλήθευσης υπογραφής) κρυπτογραφικών κλειδιών που χρησιμοποιούνται συμπληρωματικά το ένα προς το άλλο για την παραγωγή και την επαλήθευση της ηλεκτρονικής υπογραφής.

Ως αναγνωρισμένο πιστοποιητικό ορίζεται από την Οδηγία η ηλεκτρονική βεβαίωση που εκδίδεται από κάποιον Πάροχο Υπηρεσιών Πιστοποίησης (Certification Service Providers – CSP) και η οποία συνδέει μονοσήμαντα τα δεδομένα επαλήθευσης μιας υπογραφής (ή δημόσιο κλειδί) με ένα συγκεκριμένο φυσικό πρόσωπο, τηρώντας κάποιους βασικούς όρους.

Τέλος, ως Ασφαλής Διάταξη Δημιουργίας Υπογραφής (Secure Signature Creation Device – SSCD) ορίζεται το διατεταγμένο υλικό ή και λογισμικό που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού (ή των δεδομένων δημιουργίας υπογραφής) από τον υπογράφοντα και το οποίο διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής βάσει συγκεκριμένων απαιτήσεων που αναγράφονται στην Οδηγία.

[8]Η Οδηγία προβλέπει την ελεύθερη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, απαγορεύοντας οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης (ΠΥΠ, αγγλικός όρος CSP) προσδιορίζοντας, όμως τις προϋποθέσεις λειτουργίας και την ευθύνη των ΠΥΠ που εκδίδουν αναγνωρισμένα πιστοποιητικά προς το κοινό. Παράλληλα προβλέπει την δυνατότητα Εθελοντικής Διαπίστευσης των ΠΥΠ, καθώς και διαδικασία Διαπίστωσης της συμμόρφωσης των προϊόντων ηλεκτρονικών υπογραφών με τις

PDF created with pdfFactory Pro trial version www.pdffactory.com

απαιτήσεις ασφάλειας και αξιοπιστίας της Οδηγίας (βάσει σχετικών γενικώς αναγνωρισμένων προτύπων) από σχετικούς αρμόδιους φορείς.

PDF created with pdfFactory Pro trial version www.pdffactory.com

2.2 Νομικό Πλαίσιο στην Ελλάδα

[6]Στην Ελλάδα η πρώτη νομοθετική πρόβλεψη για την ψηφιακή υπογραφή, (οι οποίες ταυτίζονται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές της Οδηγίας), γίνεται ήδη το 1998 από το άρθρο 14 του Ν. 2672/98, όπου παρέχεται μία αρχική, αλλά περιορισμένη αναγνώρισή των ψηφιακών υπογραφών, σε διαδικασίες του δημόσιου τομέα. Πιο συγκεκριμένα στο άρθρο του Ν. 2672/98, υπήρξε ο ορισμός του ηλεκτρονικού ταχυδρομείου καθώς επίσης και ο ορισμός της ψηφιακής υπογραφής. Σύμφωνα με το άρθρο 14 του νόμου 2672/98 ορίζονται:

Α) Ως ηλεκτρονικό ταχυδρομείο, το σύστημα αποστολής και λήψης μηνυμάτων μέσω δικτύου από και προς την ηλεκτρονική διεύθυνση των χρηστών

Β) Ως ψηφιακή υπογραφή, η ψηφιακής μορφή υπογραφή σε δεδομένα ή λογικά συσχετιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη αποδοχής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή:

1. Συνδέεται μονοσήμαντα με τον υπογράφοντα.
2. Ταυτοποιεί τον υπογράφοντα
3. Δημιουργεί με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχο του και
4. Συνδέεται με τα δεδομένα στα οποία αναφέρατε κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

Ακολούθησε το Π.Δ. 150/2001 (ΦΕΚ Ά/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία και καθόρισε την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για την λειτουργία μηχανισμών εθελοντικής διαπίστευσης των ΠΥΠ και διαπίστωσης της συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής. Επίσης, όπως αναφέρθηκε και πιο πάνω με το Π.Δ 150/2001 η ψηφιακή υπογραφή εξομοιώνεται με την ιδιόχειρη κάτω από αυστηρές προϋποθέσεις.

[4]Οι διατάξεις του Προεδρικού Διατάγματος 150 του 2001 δεν θίγουν διατάξεις που επιβάλλουν τη χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα. Επίσης, το διάταγμα περιέχει ορισμούς των εννοιών ψηφιακή υπογραφή, προηγμένη ψηφιακή, υπογράφων, δεδομένα δημιουργίας υπογραφής, διάταξη δημιουργίας υπογραφής και άλλων. Ορίζει τις έννομες συνέπειες των ψηφιακών υπογραφών δηλαδή ότι η ψηφιακή υπογραφή επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο. Στο διάταγμα αναφέρεται ποια νομοθεσία δεσμεύει τα φυσικά ή νομικά πρόσωπα που εκδίδουν πιστοποιητικά ψηφιακών υπογραφών στην Ελλάδα και στο εξωτερικό αλλά και τις ευθύνες με τις οποίες βαρύνονται οι πάροχοι υπηρεσιών πιστοποίησης (ΠΥΠ). Περιέχει διατάξεις για την προστασία των προσωπικών δεδομένων στην διαδικασία έκδοσης πιστοποιητικών.

Το άρθρο 3 του Π.Δ. αναγνωρίζει ότι «η προηγμένη ψηφιακή υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο

PDF created with pdfFactory Pro trial version www.pdffactory.com

και στο δικονομικό δίκαιο». Το άρθρο 7 αναφέρεται στους παροχείς υπηρεσιών πιστοποίησης οι οποίοι υπόκεινται στις διατάξεις του ν. 2472/1997 και του ν. 2774/1999 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

[7]Η ψηφιακή υπογραφή αποτελεί την «ψηφιοποίηση» της κανονικής υπογραφής και την επικόλλησή της σε ένα έγγραφο. Με αυτόν τον τρόπο δεν πιστοποιείται μόνο η ταυτότητα του χρήστη αλλά και η εγκυρότητα του εγγράφου, καθώς η οποιαδήποτε εκ των υστέρων αλλοίωσή του είναι δυνατόν να εντοπιστεί.

Τον Οκτώβριο του 2002, εκδόθηκε το Π.Δ. 342/02 το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων μηνυμάτων του ηλεκτρονικού ταχυδρομείου στις επικοινωνίες του δημόσιου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής, καθώς και τρεις Κανονισμούς σχετικά με την εθελοντική διαπίστευση των ΠΥΠ, τη διαπίστωση (της συμμόρφωσης με τις απαιτήσεις της Οδηγίας) βασικών προϊόντων ηλεκτρονικής υπογραφής, και τον ορισμό των Φορέων που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ.

2.3 Νομοθετικές απαιτήσεις για τον εξοπλισμό δημιουργίας και επαλήθευσης υπογραφών

[3]Για την δημιουργία μιας ψηφιακής υπογραφής πάνω σε συγκεκριμένα ηλεκτρονικά δεδομένα, θα πρέπει κάποιος, -εκτός από τα απαραίτητα κρυπτογραφικά κλειδιά και το αντίστοιχο έγκυρο πιστοποιητικό, να διαθέτει και μια ολοκληρωμένη "διάταξη δημιουργίας υπογραφής" η οποία να απαρτίζεται από κατάλληλη σύνθεση υλικού (hardware) και λογισμικού (software). Στην διάταξη αυτή περιλαμβάνονται ο "φορέας" των κρυπτογραφικών κλειδιών (π.χ. σκληρός δίσκος υπολογιστή, έξυπνη κάρτα, USB token, κ.λπ.), ο τυχόν απαραίτητος "αναγνώστης του φορέα" αυτού (π.χ. αναγνώστης έξυπνης κάρτας, θύρα USB, κ.λπ.), το "τερματικό επικοινωνίας" του χρήστη (π.χ. PC, pda, smart phone, κ.λπ.), τα "λειτουργικά συστήματα" και οι "οδηγοί" (drivers) των συσκευών αυτών, καθώς και το "λογισμικό επικοινωνίας" (interface) του χρήστη που χρησιμοποιείται για τη δημιουργία της ηλεκτρονικής υπογραφής.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 3. Νομοθετικές διατάξεις και πρωτόκολλα ασφάλειας κατά την δημιουργία μιας Ψηφιακής Υπογραφής

[4]Ιδίως για την δημιουργία "αναγνωρισμένης" ηλεκτρονικής υπογραφής, η νομοθεσία απαιτεί την χρήση "ασφαλούς διάταξης δημιουργίας υπογραφής"(α.δ.δ.υ.). Ως τέτοια προσδιορίζεται (Παράρτημα ΙΙΙ Οδηγίας και π.δ. 150/2001) η "διάταξη" η οποία, -μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, διασφαλίζει τουλάχιστον ότι τα "δεδομένα δημιουργίας υπογραφής" (ιδιωτικά κλειδιά) που χρησιμοποιούνται για την παραγωγή υπογραφών:

1) "απαντούν, κατ' ουσίαν, μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο" -το οποίο σημαίνει ότι τα σχετικά κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με τους κατάλληλους αλγόριθμους δημιουργίας τυχαίων κωδικών, είτε απευθείας μέσα σε συσκευή του χρήστη, είτε από κατάλληλες κρυπτογραφικές μονάδες του Παρόχου Υπηρεσιών Πιστοποίησης οι οποίες μεταφέρουν άμεσα τα δημιουργηθέντα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται, χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφά τους.
2) "δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας" όρος που, εκτός από την απαγόρευση της διατήρησης με οποιονδήποτε τρόπο αντιγράφου του ιδιωτικού κλειδιού, στην ουσία του επιβάλλει την χρήση της τεχνολογίας ασύμμετρης κρυπτογραφίας.
3) "μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους" που σημαίνει ότι τα ιδιωτικά κλειδιά δεν πρέπει να μπορούν να εξαχθούν ή/και να αντιγραφούν από τον φορέα τους, ούτε να ενεργοποιηθούν χωρίς την προηγούμενη χρήση μιας επιπλέον "μεθόδου επιβεβαίωσης της ταυτότητας" του χρήστη (π.χ. χρήση μυστικού κωδικού αναγνώρισης (PIN) ή/και ανάγνωση βιομετρικών δεδομένων του δικαιούχου).

Παράλληλα, η νομοθεσία ορίζει ότι οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν πρέπει να μεταβάλλουν τα προς υπογραφή δεδομένα, ούτε να εμποδίζουν την εμφάνιση των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής (επιβάλλεται δηλαδή η αρχή "What You See Is What You Sign" ή "WYSIWYS").

PDF created with pdfFactory Pro trial version www.pdffactory.com

[11]Η έως σήμερα προτυποποίηση για την εξειδίκευση των απαιτήσεων για ασφαλείς διατάξεις δημιουργίας υπογραφής έχει δώσει ιδιαίτερη έμφαση στην ασφάλεια των "συσκευών δημιουργίας κρυπτογραφικών κλειδιών" (key generation systems) καθώς και των "τελικών φορέων" τους, που συνήθως είναι μια "έξυπνη κάρτα" (smart card) ή άλλη αντίστοιχη συσκευή (π.χ. USB Token).

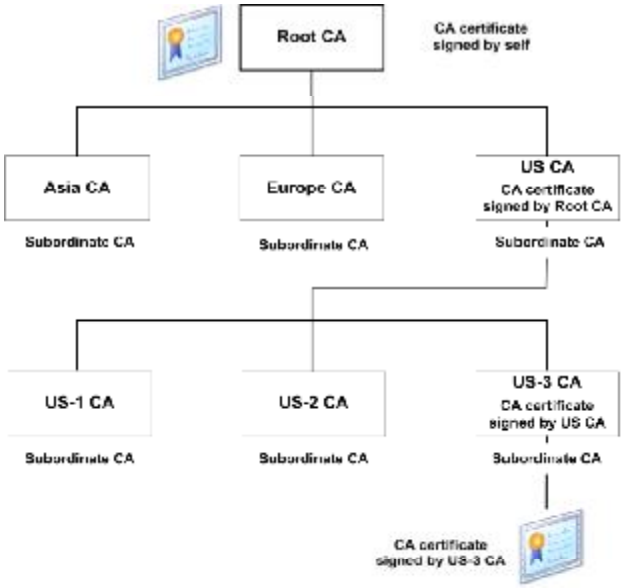
Αντίστοιχα, για την επαλήθευση (verification) των ψηφιακών υπογραφών και τον έλεγχο της εγκυρότητας (validation) των σχετικών πιστοποιητικών, απαιτείται μια ανάλογη διάταξη, η οποία, εκτός του τερματικού επικοινωνίας του χρήστη και του κατάλληλου λογισμικού, θα πρέπει, επιπλέον, να διαθέτει και την δυνατότητα πρόσβασης είτε με "on line" σύνδεση, είτε και με συχνές "off-line" ενημερώσεις σε επικαιροποιημένες πληροφορίες εγκυρότητας ή/και ανάκλησης πιστοποιητικών τις οποίες δημοσιεύει ο εκάστοτε εκδότης (ΠΥΠ) τους. Για τις "διατάξεις επαλήθευσης υπογραφής" η Οδηγία 99/93/ΕΚ "συστήνει" (ά.3§6) προς τα κράτη-μέλη την συνεργασία τους για την ανάπτυξη συστημάτων τα οποία θα πρέπει να διασφαλίζουν τόσο την αξιοπιστία τους, όσο και την ορθή πληροφόρηση του επαληθεύοντα ως προς τα στοιχεία και τα αποτελέσματα της επαλήθευσης.

PDF created with pdfFactory Pro trial version www.pdffactory.com

3. Ψηφιακά πιστοποιητικά, αρχές πιστοποίησης και αρχές εγγραφής

3.1 Πιστοποιητικό

[1]Το πιστοποιητικό είναι ένα ηλεκτρονικό αντικείμενο που συσχετίζει ένα δημόσιο κλειδί (και επιπλέον και το αντίστοιχο ιδιωτικό του) με ορισμένες άλλες πληροφορίες, συνήθως πληροφορίες ταυτότητας ή περιγραφές αδειών. Ένα πιστοποιητικό υπογράφεται, βάση μίας υποδομής, από κάποια αρχή πιστοποίησης (Certification Authority- CA), η οποία βεβαιώνει με κάποιο τρόπο, τουλάχιστον θεωρητικά, την σύνδεση μεταξύ της ταυτότητας ή της άδειας και του ιδιοκτήτη του ιδιωτικού κλειδιού. Στον νομικό κόσμο, ένα πιστοποιητικό μπορεί να είναι ένα έγγραφο και όχι ηλεκτρονικό αντικείμενο, το οποίο δεν συσχετίζεται με κανέναν τρόπο με κλειδιά.



Εικόνα 4. Ιεραρχία και δομή των πιστοποιητικών

Το πλεονέκτημα των πιστοποιητικών είναι ότι είναι πιθανόν να ελεγχθούν χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης. Αυτό σημαίνει ότι είναι πιθανόν να εισαχθεί ένας καινούριος χρήστης στο σύστημα χωρίς το ίδιο το σύστημα να ξέρει κάτι για αυτό. Δυστυχώς, μέρος αυτού του πλεονεκτήματος αναιρείται από την ανάγκη σε πολλές περιπτώσεις να ελεγχθεί η κατάσταση του πιστοποιητικού κάθε φορά που αυτό χρησιμοποιείται.

Η πιο συνήθης χρήση των πιστοποιητικών σήμερα είναι με HTTPS για την επαλήθευση της ταυτότητας των ασφαλών εξυπηρετητών διαδικτύου. Σε αυτή την περίπτωση, η ταυτότητα που συνδέεται με το δημόσιο κλειδί είναι το domain name του εξυπηρετητή διαδικτύου. Πριν η αρχή πιστοποίησης εκδώσει ένα πιστοποιητικό που συνδέει το domain name με ένα δημόσιο κλειδί, ελέγχει ότι το domain ανήκει στο πρόσωπο ή την οντότητα, συνήθως εταιρία, που έχει αιτηθεί του πιστοποιητικού.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Ελέγχει επίσης ότι πρόκειται για συναλλαγή της με την ίδια την οντότητα και όχι κάποιον τρίτο. Σφάλματα σε αυτούς τους ελέγχους είναι πιθανόν να έχουν σημαντικές συνέπειες. Για παράδειγμα, τον Ιανουάριο του 2001, η VeriSign εξέδωσε εσφαλμένα για λογαριασμό ενός μη εξουσιοδοτημένου τρίτου ένα πιστοποιητικό υπογραφής κωδικού συνδεμένο με την ταυτότητα της Microsoft, το οποίο θα μπορούσε να χρησιμοποιηθεί για την εισαγωγή αυθαίρετου κώδικα σε μηχανές ανυποψίαστων χρηστών.

Μία άλλη, λιγότερο συνήθης αλλά εξίσου δημοφιλής χρήση των πιστοποιητικών είναι τα γνωστά ως «πιστοποιητικά πελατών». Τα πιστοποιητικά αυτά εκδίδονται για λογαριασμό ιδιωτών ως μία απόδειξη της ταυτότητας που είναι ανεξάρτητη από οποιονδήποτε συγκεκριμένο εξυπηρετητή ή σύστημα και εκπληρώνουν τους σκοπούς ενός ηλεκτρονικού πιστοποιητικού. Προσφιλές παράδειγμα αποτελεί η ηλεκτρονική υποβολή της φορολογικής δήλωσης σε ορισμένα κράτη για την οποία πρέπει να έχει εκδοθεί ηλεκτρονικό πιστοποιητικό από αναγνωρισμένη αρχή πιστοποίησης.

Η έκδοση ενός πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών από έναν Πάροχο Υπηρεσιών Πιστοποίησης, περιορίζεται σε συγκεκριμένες επιτρεπόμενες χρήσεις, οι οποίες προσδιορίζονται και από το σχετικό πεδίο "Χρήση Κλειδιού" ("Key Usage") των πιστοποιητικών X.509 το οποίο δέχεται συγκεκριμένες προκαθορισμένες τιμές. Έχει επικρατήσει, -τουλάχιστον στις περισσότερες σχετικές εφαρμογές στην Ευρώπη, να εκδίδεται σε ένα υποκείμενο ένα ξεχωριστό "αναγνωρισμένο" πιστοποιητικό για το ζεύγος κρυπτογραφικών κλειδιών που θα χρησιμοποιεί αποκλειστικά για δημιουργία "αναγνωρισμένων υπογραφών" με έννομες συνέπειες σε ηλεκτρονικά έγγραφα (με την τιμή-ένδειξη "Μη Απάρνηση" ή αλλιώς "Non Repudiation") και ένα δεύτερο πιστοποιητικό (για άλλο ζεύγος κλειδιών) το οποίο θα χρησιμοποιείται για "υπογραφές αυθεντικότητας δεδομένων" ή/και για "υπογραφές ταυτοποίησης" (με την ένδειξη "Ψηφιακή Υπογραφή" ή "Digital Signature"). Στο δεύτερο αυτό πιστοποιητικό μπορούν να παρασχεθούν και δυνατότητες χρήσης των κλειδιών για απλή "κρυπτογράφηση δεδομένων (με την πρόσθετη ένδειξη "Κρυπτογράφηση Κλειδιών/Δεδομένων" ή "Key/Data Encipherment"), αν και συνιστάται η χρήση τρίτου ξεχωριστού ζεύγους κλειδιών και αντίστοιχου πιστοποιητικού για τις εφαρμογές κρυπτογράφησης.

Ακολούθως, τα κλειδιά που χρησιμοποιούν οι ίδιοι οι Εκδότες για την ψηφιακή υπογραφή των πιστοποιητικών των υποκειμένων (τελικών οντοτήτων) και των "Λιστών Ανακληθέντων Πιστοποιητικών" (CRLs) που εκδίδουν, περιορίζονται αποκλειστικά σ' αυτήν την χρήση τους με την αναγραφή των αντίστοιχων ενδείξεων ("KeyCertSign" ή/και "CRLSign") στο πιστοποιητικό τους.

[2]Άλλοι περιορισμοί στην χρήση των πιστοποιητικών δημοσίων κλειδιών μπορούν να αναφέρονται στα όρια ως προς την αξία των συναλλαγών στις οποίες αυτά επιτρέπεται να χρησιμοποιηθούν. Οι περιορισμοί αυτοί πρέπει -τουλάχιστον για τα "αναγνωρισμένα πιστοποιητικά"- να αναγράφονται σε κατάλληλα πεδία μέσα στο ίδιο πιστοποιητικό ή/και να αναφέρονται εμφανώς μέσα στο κείμενο της σχετικής "Πολιτικής Πιστοποιητικού" (Certificate Policy) που δημοσιεύει ο Πάροχος Υπηρεσιών Πιστοποίησης και η οποία συμπεριλαμβάνει όλους τους ειδικότερους όρους έκδοσης και χρήσης που καθορίζει ο Πάροχος Υπηρεσιών Πιστοποίησης για το συγκεκριμένο είδος πιστοποιητικών. Το κείμενο μιας "Πολιτικής Πιστοποιητικού" προσδιορίζεται ("ταυτοποιείται") με τη χρήση ενός μοναδικού "κωδικού αριθμού ταυτοποίησης' ("Object Identification number" ή "OID") ο οποίος αναγράφεται στο

PDF created with pdfFactory Pro trial version www.pdffactory.com

ομώνυμο πεδίο των πιστοποιητικών X.509, ενημερώνοντας τόσο το υποκείμενο πιστοποίησης ("συνδρομητή" του ΠΥΠ), όσο και κάθε τρίτο-αποδέκτη των πιστοποιητικών του για την εφαρμοζόμενη "Πολιτική Πιστοποιητικού".

Τα "πιστοποιητικά δημοσίου κλειδιού" μπορούν επίσης να διακριθούν σε "επώνυμα" και σε "ψευδώνυμα" πιστοποιητικά, ανάλογα με τη δημοσιοποίηση του πραγματικού ονόματος του υποκειμένου στο οποίο αναφέρονται. Είναι ακόμη δυνατόν να εκδοθούν και "ανώνυμα" πιστοποιητικά, στα οποία συνήθως πιστοποιείται -μέσω απομακρυσμένης επικοινωνίας- μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου (e-mail address) από το υποκείμενο.

Εικόνα 5. Προειδοποίηση Ασφαλείας - ταυτοποίηση πιστοποιητικού μέσω της εταιρίας Microsoft

Εκτός από την πιστοποίηση της ταυτότητας του υποκειμένου τους, τα πιστοποιητικά δημοσίου κλειδιού μπορούν να περιλαμβάνουν και αναφορά σε συγκεκριμένες (πιστοποιημένες ή μη) ιδιότητες του υποκειμένου (π.χ. επάγγελμα κλπ), αλλά στη περίπτωση αυτή, η χρήση των συγκεκριμένων κλειδιών για την δημιουργία μιας ηλεκτρονικής υπογραφής θα πρέπει να συσχετίζεται με την αναφερόμενη ιδιότητα του υποκειμένου. Μια άλλη λύση που παρέχει επιλεκτική επίκληση μιας (τυχόν απαιτούμενης) "ιδιότητας" του υποκειμένου κατά την δημιουργία συγκεκριμένων ηλεκτρονικών υπογραφών, είναι η χρήση ειδικών πρόσθετων "πιστοποιητικών ιδιοτήτων" (attribute certificates) τα οποία εκδίδονται από μια "Αρχή Πιστοποίησης Ιδιοτήτων" (Attribute Authority – "AA") και χρησιμοποιούνται συμπληρωματικά μαζί με τα (βασικά) "πιστοποιητικά δημοσίου κλειδιού". Εκτός από τα πιστοποιητικά που εκδίδονται σε φυσικά πρόσωπα, μια άλλη κατηγορία πιστοποιητικών δημοσίων κλειδιών αποτελεί αυτή που εκδίδεται με υποκείμενο τηλεπικοινωνιακά ή πληροφορικά συστήματα και συσκευές (web servers, routers, client devices, κ.λ.π.). Η χρήση των κρυπτογραφικών κλειδιών που σχετίζονται με τα συγκεκριμένα πιστοποιητικά, γίνεται συνήθως με αυτόματο τρόπο και περιορίζεται κυρίως:

1) σε "υπογραφές ταυτοποίησης" των συσκευών αυτών (π.χ. server authentication) και

PDF created with pdfFactory Pro trial version www.pdffactory.com

2) σε "κρυπτογράφηση άλλων συμμετρικών κλειδιών" που χρησιμοποιούνται για την περαιτέρω κρυπτογράφηση των διακινούμενων δεδομένων. Χαρακτηριστική εφαρμογή είναι η "πιστοποίηση προέλευσης ιστοσελίδων" όπου, στην πράξη, πιστοποιείται η νόμιμη εξυπηρέτηση μιας "διεύθυνσης διαδικτύου" (URL) από έναν συγκεκριμένο υπολογιστή/εξυπηρετητή διαδικτύου (web server) -στον οποίον έχουν εγκατασταθεί τα σχετικά κρυπτογραφικά κλειδιά- επιτρέποντας παράλληλα την κρυπτογράφηση και ανταλλαγή άλλων "παροδικών συμμετρικών κρυπτογραφικών κλειδιών" (session keys) που χρησιμοποιούνται για την επίτευξη ασφαλούς (εμπιστευτικής) επικοινωνίας τύπου SSL ή TSL.

Τέλος, μια διαφορετική κατηγορία ηλεκτρονικών πιστοποιητικών, αποτελούν τα "πιστοποιητικά χρονοσήμανσης" (time stamping certificates) τα οποία, εκδίδονται ad hoc σε συγκεκριμένα ηλεκτρονικά έγγραφα, μετά από αίτημα του υπογράφοντα ή/και του αποδέκτη τους. Στα περιεχόμενά τους, εκτός των στοιχείων του εκδότη τους (και πιθανώς και του αιτούντα), περιλαμβάνουν την σύνοψη (αποτύπωμα) του συγκεκριμένου εγγράφου στο οποίο αναφέρονται και την ακριβή χρονική στιγμή έκδοσής τους (η οποία βασίζεται σε αξιόπιστη πηγή χρονολόγησης που διαθέτει ο εκδότης τους). Η χρήση των πιστοποιητικών χρονοσήμανσης εξασφαλίζει αποδείξεις για την ύπαρξη μιας ηλεκτρονικής υπογραφής σε ένα συγκεκριμένο ηλεκτρονικό έγγραφο σε μια συγκεκριμένη χρονική στιγμή, αποκλείοντας έτσι την δυνατότητα μελλοντικής "αποποίησης" ή "αμφισβήτησης" της υπογραφής από τον υπογράφοντα, με τον ισχυρισμό ότι αυτή δημιουργήθηκε μετά την λήξη ή την ανάκληση (π.χ. λόγω έκθεσης του σχετικού κρυπτογραφικού κλειδιού σε τρίτους) του συγκεκριμένου πιστοποιητικού δημοσίου κλειδιού, και, άρα σε χρόνο που το πιστοποιητικό αυτό δεν βρισκόταν σε ισχύ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

3.2 Προτυποποίηση

[5]Το X.509 [33] είναι ένα ITU πρότυπο για τα ψηφιακά πιστοποιητικά, αρχικά σχεδιασμένο για την διασφάλιση των ταχυδρομικών καταλόγων, το οποίο έχει υιοθετηθεί για χρήση με SSL.

Σύμφωνα με το X.509 ένα δημόσιο κλειδί συσχετίζεται με ένα Διακεκριμένο Όνομα (Distinguished Name ή DN), το οποίο είναι μία τεράστια μάζα δεδομένων που προσδιορίζει την ταυτότητα του ιδιοκτήτη του πιστοποιητικού με έναν ιεραρχικό τρόπο. Το παραπάνω, συμβαδίζει με το μοντέλο του X.500, ένα πρότυπο ταχυδρομικού καταλόγου που απέτυχε στο να κερδίσει ευρεία αποδοχή, αλλά στην πραγματικότητα δεν λειτουργεί αποτελεσματικά στις συναλλαγές.

3.3 Αρχή πιστοποίησης – CA ή Πάροχος Υπηρεσιών Πιστοποίησης και Νομική ευθύνη του

Μία αρχή πιστοποίησης (certification authority ή CA) είναι υπεύθυνη για την υπογραφή πιστοποιητικών. Για να παρέχεται οποιαδήποτε αξιοπιστία σε αυτήν την υπογραφή από πλευράς της αρχής πιστοποίησης, θα πρέπει αυτή να ασκεί κάποιο είδος ελέγχου στο πιστοποιητικό πριν το υπογράψει. Γενικά, οι δημόσιες αρχές πιστοποίησης διενεργούν πράγματι αυτόν τον έλεγχο ή τον αναθέτουν στις αρμόδιες Αρχές Εγγραφής τους, ωστόσο προσπαθούν να αποποιηθούν όλων των ευθυνών τους στην περίπτωση που ο απαραίτητος έλεγχος δεν διενεργηθεί αποτελεσματικά.

[14]Οι ιδιωτικές αρχές πιστοποίησης, δηλαδή αυτές που λειτουργούν μόνο στα πλαίσια εντός ενός οργανισμού, ασχολούνται συχνότερα με πιστοποιητικά πελατών. Ας σημειωθεί ότι ένας από τους ελέγχους που οφείλει να διενεργήσει μία αρχή πιστοποίησης είναι ο έλεγχος του εάν ο αιτών έχει την κατοχή του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού. Αυτό πρέπει να επιτυγχάνεται μέσω μίας υπογραφής με αίτημα του πιστοποιητικού και όχι μέσω της παραγωγής του ιδιωτικού κλειδιού από την ίδια την αρχή πιστοποίησης για λογαριασμό του αιτούντα.

Αν η ίδια η αρχή πιστοποίησης παράγει ένα ζεύγος κλειδιών και το αποδώσει στον αιτούντα, μπορεί να διασφαλιστεί ότι εκείνη ακριβώς την στιγμή ο αιτών έχει στην κατοχή του το ιδιωτικό κλειδί και ότι κανένας άλλος, εκτός από την αρχή πιστοποίησης, δεν έχει πρόσβαση σε αυτό. Αυτό εξυπηρετεί την αρχή πιστοποίησης αφού έτσι μπορεί να πιστοποιήσει ότι ο αιτών είναι το μόνο πρόσωπο με το κλειδί στην κατοχή του. Ωστόσο, αυτό δεν εξυπηρετεί τον αιτούντα, ο οποίος θα πρέπει να θεωρεί το γεγονός της πρόσβασης της αρχής πιστοποίησης στο κλειδί ως σημαντική αδυναμία της ασφάλειας. Από την άλλη μεριά, αν ο αιτών επιμείνει στην δημιουργία του ιδιωτικού κλειδιού από τον ίδιο και στην απόδοση μόνο του δημοσίου κλειδιού του στην αρχή πιστοποίησης, η αρχή πιστοποίησης δεν είναι σε θέση να γνωρίζει με βεβαιότητα ότι ο αιτών είναι το μοναδικό πρόσωπο με πρόσβαση στο ιδιωτικό κλειδί. Ωστόσο, η αρχή πιστοποίησης δεν θα μπορούσε να το γνωρίζει αυτό με βεβαιότητα μετά από την απόδοση του κλειδιού στον αιτούντα, ακόμη και στην περίπτωση που αυτή δημιουργούσε το ζεύγος κλειδιών, οπότε το κέρδος ασφάλειας σε αυτήν την περίπτωση είναι ελάχιστο.

[8]Η Παροχή Υπηρεσιών Πιστοποίησης ηλεκτρονικών υπογραφών (και "συναφών υπηρεσιών") δεν υπόκειται σε καθεστώς αδειοδότησης και άρα μπορεί οποιοσδήποτε (φυσικό ή νομικό πρόσωπο) να λειτουργήσει ως Πάροχος Υπηρεσιών

PDF created with pdfFactory Pro trial version www.pdffactory.com

Πιστοποίησης και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός Παρόχου Υπηρεσιών Πιστοποίησης προς την εποπτεύουσα αρχή (ΕΕΤΤ) είναι η "Δήλωση Έναρξης Λειτουργίας" και η εγγραφή του στο σχετικό "Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης", καθώς και η αποστολή "Ετήσιων Εκθέσεων" σχετικά με την λειτουργία τους.

Για να εκδώσει ένας Πάροχος Υπηρεσιών Πιστοποίησης "αναγνωρισμένα πιστοποιητικά προς το κοινό", θα πρέπει ("κατά δήλωσή του", η οποία ελέγχεται από την εποπτεύουσα ΕΕΤΤ) να ικανοποιεί τις απαιτήσεις ασφάλειας, αξιοπιστίας και παροχής ολοκληρωμένων υπηρεσιών που επιβάλλονται στους όρους του Παραρτήματος ΙΙ της σχετικής ευρωπαϊκής Οδηγίας 99/93/ΕΚ (και του ΠΔ 150/2001), πολλοί από τους οποίους εξειδικεύονται από τη σχετική ευρωπαϊκή προτυποποίηση (π.χ. στα πρότυπα CEN CWA 14167-1 και ETSI TS 101456 & TS 101862). Ένας Πάροχος Υπηρεσιών Πιστοποίησης που εκδίδει "αναγνωρισμένα πιστοποιητικά" έχει, επίσης, τη δυνατότητα να "διαπιστευτεί εθελοντικά" (σε κάποιον σχετικό εθνικό ή κλαδικό "φορέα διαπίστευσης"), ως προς το επίπεδο των παρεχόμενων υπηρεσιών του και την συμμόρφωσή του σε καθιερωμένα "πρότυπα" (standards). Με την "Εθελοντική Διαπίστευση" ο Πάροχος Υπηρεσιών Πιστοποίησης αποκτά "δικαίωμα επίκλησης" της συγκεκριμένης διαπίστευσής του προς κάθε τρίτο, υποβάλλεται όμως σε περαιτέρω υποχρεώσεις και ελέγχους που συνήθως επιβάλλει ο σχετικός φορέας.

Κάθε Πάροχος Υπηρεσιών Πιστοποίησης, με την έκδοση οποιουδήποτε είδους πιστοποιητικού, αναλαμβάνει ευθύνες τόσο έναντι του "συνδρομητή" του (ο οποίος είτε ταυτίζεται, είτε σχετίζεται με το "υποκείμενο" (ή "θέμα") του εκδιδόμενου πιστοποιητικού), όσο και έναντι κάθε τρίτου προσώπου που "ευλόγως" βασίζεται στο πιστοποιητικό του. Οι ευθύνες αυτές κρίνονται, καταρχήν, κατά τις «γενικές διατάξεις περί ευθύνης» και τις «διατάξεις περί προστασίας των καταναλωτών», ενώ προσδιορίζονται ειδικότερα στους συμβατικούς όρους που συμφωνούνται με το υποκείμενο (συνδρομητή) της πιστοποίησης ("συνδρομητική σύμβαση"), καθώς και στους όρους τους οποίους οφείλει να αποδεχθεί οποιοσδήποτε τρίτος, πριν να αποφασίσει να βασισθεί στα περιεχόμενα των πιστοποιητικών και των συναφών υπηρεσιών (π.χ. "Υπηρεσίες Καταλόγου") του Παρόχου Υπηρεσιών Πιστοποίησης ("σύμβαση αποδέκτη").

[13]Στην περίπτωση, όμως, που ο Πάροχος Υπηρεσιών Πιστοποίησης εκδίδει «αναγνωρισμένα πιστοποιητικά προς το κοινό», η ευθύνη του έναντι κάθε τρίτου-αποδέκτη των εκδιδόμενων πιστοποιητικών του προκύπτει απ' ευθείας από τον νόμο (ά. 6 Οδηγίας) και αφορά την "ακρίβεια και την πληρότητα των πληροφοριών" που αναγράφονται σε αυτά, καθώς και την "διαβεβαίωση της κατοχής των σχετικών κλειδιών" από τα πιστοποιούμενα υποκείμενα. Το ίδιο συμβαίνει και ως προς την παράλειψή του Παρόχου Υπηρεσιών Πιστοποίησης να καταγράψει και να δημοσιοποιήσει την τυχόν "ανάκληση" ενός "αναγνωρισμένου πιστοποιητικού", καθώς και ως προς την μη σωστή λειτουργία των σχετικών κρυπτογραφικών κλειδιών του υποκειμένου (στην περίπτωση που αυτά τα δημιούργησε και τα παρέδωσε στο υποκείμενο ο ίδιος ο Πάροχος Υπηρεσιών Πιστοποίησης).

Η ευθύνη του Παρόχου Υπηρεσιών Πιστοποίησης έναντι των "τρίτων" μπορεί να περιοριστεί σε συγκεκριμένα όρια και για συγκεκριμένες χρήσεις του πιστοποιητικού, εφόσον όμως οι περιορισμοί αυτοί προσδιορίζονται ρητά στην "Πολιτική Πιστοποιητικού" (Certificate Policy) που διέπει το συγκεκριμένο πιστοποιητικό και είναι εμφανείς και αναγνωρίσιμοι σε κάθε αποδέκτη του. Ο

PDF created with pdfFactory Pro trial version www.pdffactory.com

Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να απαλλαχθεί εντελώς από την ευθύνη εκ του νόμου εάν αποδείξει ότι η σχετική πράξη ή παράλειψη του δεν προήλθε από αμέλεια.

[8]Οι βασικές υπηρεσίες που προσφέρει υποχρεωτικά ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορούν να διακριθούν σε οργανωμένες ξεχωριστές λειτουργικές οντότητες, και συγκεκριμένα σε:

- Υπηρεσία Εγγραφής/Καταχώρησης (Registration Authority – RA), η οποία αναλύεται παρακάτω,
- Υπηρεσία Έκδοσης Πιστοποιητικών (Certification Authority –CA), που εκδίδει (σύμφωνα με τις αιτήσεις της "Υπηρεσίας Εγγραφής") και υπογράφει τα τελικά πιστοποιητικά των υποκειμένων, και η οποία πιθανότατα χρησιμοποιεί περισσότερους από ένα λειτουργικούς ή ουσιαστικούς "Υπο-Εκδότες"(Sub-CAs) -με διαφορετικά πιστοποιημένα (από τον "Root CA" ή άλλον ενδιάμεσο "Sub-CA") κλειδιά- για την υπογραφή των πιστοποιητικών των συνδρομητών.
- Υπηρεσία Διαχείρισης Αιτημάτων Ανάκλησης (Revocation Management Service), η οποία υποδέχεται, ελέγχει (σε συνεργασία με την "Υπηρεσία Εγγραφής") και διεκπεραιώνει τα αιτήματα -σε 24ωρη βάση, 7 ημέρες την εβδομάδα- για ανάκληση, παύση ή επανεργοποίηση των πιστοποιητικών, συνεργαζόμενη με την "Υπηρεσία Έκδοσης Πιστοποιητικών" για την κατάλληλη (ψηφιακή) υπογραφή των σχετικών εκδιδόμενων "Λιστών Ανακληθέντων Πιστοποιητικών" (Certificate Revocation Lists ή "CRLs").
- Υπηρεσία Δημοσίευσης (Dissemination και Revocation Status Service), η οποία αναλαμβάνει την δημοσίευση των κειμένων τεκμηρίωσης των υπηρεσιών του Παρόχου Υπηρεσιών Πιστοποίησης (πιθανότατα με την χρήση μιας ηλεκτρονικής τοποθεσίας – "Repository"), την δημοσίευση των Καταλόγων και των Λιστών Ανακληθέντων Πιστοποιητικών, καθώς και σχετικές ενημερώσεις ή κοινοποιήσεις προς τους συνδρομητές του Παρόχου Υπηρεσιών Πιστοποίησης.

Εκτός από τις παραπάνω υποχρεωτικές υπηρεσίες, -οι οποίες προβλέπονται έμμεσα από την Οδηγία αλλά και από σχετικά νομικοτεχνικά πρότυπα- ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί επίσης να παρέχει (προαιρετικά) και "Υπηρεσίες Προμήθειας-Προετοιμασίας Φορέα" (π.χ. έξυπνη κάρτα ή USB token) για τους Συνδρομητές (Subject Device Provision Service), "Υπηρεσίες Χρονοσήμανσης" ηλεκτρονικών εγγράφων (Time-Stamping Authority ή TSA), "Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων" (Attribute Authority), "Υπηρεσίες Ασφαλούς Αρχειοθέτησης" εγγράφων (καλούμενες και Notary Services), κλπ.

Είναι επιτρεπτό για έναν Πάροχο Υπηρεσιών Πιστοποίησης να εκχωρήσει σε τρίτους (outsourcing) τη διεκπεραίωση μέρους ή ακόμη και του συνόλου των παραπάνω παρεχόμενων υπηρεσιών του. Εφόσον όμως ο Πάροχος εξακολουθεί να αναγράφεται στα εκδιδόμενα πιστοποιητικά ως "Εκδότης", τότε διατηρεί ακέραια την ευθύνη του έναντι των τρίτων για οποιοδήποτε πράξη ή παράλειψη που αναφέρεται στην Οδηγία (ή στο ΠΔ 150/2001) και προξενεί ζημία σε συνδρομητές ή τρίτους. Σύμφωνα με πληροφορίες που παρέχονται από το ICRI (Inter disciplinary centre for Law and Information Technology) ηγέτης στον χώρο την παροχής πιστοποιητικών στην ελληνική αγορά φαίνεται να είναι η εταιρία VeriSign, η οποία δραστηριοποιείται μέσω της ελληνικής εταιρείας Adacom

PDF created with pdfFactory Pro trial version www.pdffactory.com

.

PDF created with pdfFactory Pro trial version www.pdffactory.com

4. Εφαρμογές της Ψηφιακής Υπογραφής

[2]Σήμερα η ψηφιακή υπογραφή έχει εφαρμογή σε πολλούς ένα όχι σε όλους τους τομείς που αφορούν ηλεκτρονικές συναλλαγές. Η εφαρμογή της ψηφιακής υπογραφής υπάρχει ακόμα και στην καθημερινότητα του κάθε χρήστη ηλεκτρονικών υπηρεσιών πολλές φορές αυτό είναι εν αγνοία του. Σε διεθνές επίπεδο, η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφάλειας σε συναλλαγές διαφόρων τύπων όπως:

- Τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange -EDI),
- Ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη από EDI,
- Ηλεκτρονικές δημόσιες προμήθειες,
- Ηλεκτρονική ψηφοφορία,
- Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες Euro Pay, MasterCard & VISA μέσω του κοινού πρωτοκόλλου τους EMV),
- Ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες (γενικής ή ειδικής χρήσης – π.χ. ναυτικές διεθνείς ταυτότητες) που συνήθως φέρουν ενσωματωμένα και κάποια βιομετρικά στοιχεία (φωτογραφία, δακτυλικά αποτυπώματα κ.τ.λ.) του κατόχου τους,
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου (S/MIME),
- Συστήματα υπογραφής αυθεντικότητας διακινούμενου λογισμικού (π.χ. Microsoft Authenticode),
- Κλειστές υποδομές PKI για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. NATO),
- Πιστοποίηση της ταυτότητας εξυπηρετητών Διαδικτύου (web servers), κ.ά..

Στην Ευρωπαϊκή Ένωση, εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κλπ, έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία τυπικές εφαρμογές των ηλεκτρονικών υπογραφών, οι προϋποθέσεις των οποίων πηγάζουν από το νόμο. Ένας άλλος τομέας εφαρμογής ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Ένωση είναι:

- Τα ηλεκτρονικά τιμολόγια, τα οποία σύμφωνα και με την Ευρωπαϊκή Οδηγία 01/115/ΕΚ, εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.
- Οι ηλεκτρονικές δημόσιες προμήθειες στο πλαίσιο των σχετικών σχεδίων Οδηγιών της Ευρωπαϊκής Ένωσης. Επίσης, θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως η Υπηρεσία Επίσημων Δημοσιεύσεων, σχεδιάζουν την χρήση των ηλεκτρονικών υπογραφών για τα έγγραφα που εκδίδουν σε ηλεκτρονική μορφή (π.χ. την Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, τη δημοσίευση προκηρύξεων, κ.λπ.).

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 6. Διαδικασία εισαγωγής Ψηφιακής Υπογραφής

Σε ότι αφορά την Ελλάδα, μια από τις πρώτες εφαρμογές νομικά έγκυρης ψηφιακής υπογραφής επίσημων εγγράφων, η οποία λειτουργεί ήδη από το 2002, είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αθηνών (ΧΑ) με τις εισηγμένες σ' αυτό εταιρίες. Το σύστημα αυτό ονομάζεται «ΕΡΜΗΣ» (ή 'H.E.R.M.E.S.' -Hellenic Exchanges Remote MEssaging Services) και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων (εκπροσώπων των εισηγημένων), στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών, ένα για την ταυτοποίησή τους στο σύστημα και ένα για την αναγνωρισμένη ηλεκτρονική υπογραφή τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους, εναποθετημένα σε μια προσωποποιημένη έξυπνη κάρτα. Το σύστημα «ΕΡΜΗΣ» επιτρέπει την αποστολή πληροφοριών μέσω ενός περιβάλλοντος που διασφαλίζει την αξιοπιστία και την ακεραιότητα των δεδομένων κατά την ηλεκτρονική επικοινωνία με τη χρήση προηγμένων τεχνολογιών ασφάλειας και την αξιοποίηση του υφιστάμενου νομοθετικού πλαισίου (Π.Δ. 150/2001) για τις «ψηφιακές υπογραφές» (Digital Signatures). Μεταξύ των χρησιμοποιούμενων τεχνολογιών περιλαμβάνονται:

- «υποδομή δημόσιου κλειδιού» (Public Key Infrastructure - PKI),
- «αναγνωρισμένα πιστοποιητικά» (Qualified Certificates), και
- «προηγμένες ψηφιακές υπογραφές» με τη χρήση «έξυπνων καρτών»(Smart Cards), τύπου SmartAccess Card, ως μέρος ασφαλούς διάταξης δημιουργίας υπογραφής.

PDF created with pdfFactory Pro trial version www.pdffactory.com

[13]Παράλληλα, η υποστήριξη και η χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσότερων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια του προγράμματος για την Κοινωνία της Πληροφορίας και των σχετικών Επιχειρησιακών Προγραμμάτων των φορέων του ευρύτερου Δημόσιου Τομέα. Χαρακτηριστικά παραδείγματα αποτελούν τα έργα ψηφιοποίησης του Ποινικού Μητρώου του Υπουργείου Δικαιοσύνης, οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση Εμπορικών νημάτων καθώς και το σύστημα ηλεκτρονικών Δημόσιων Προκηρύξεων & Προμηθειών στο Υπουργείο Ανάπτυξης (Γ.Γ. Εμπορίου), τα σχέδια για ψηφιακές υπογραφές των ηλεκτρονικών Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ) του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ (e-ΚΕΠ) κ.ά. Σημαντικότατη εξέλιξη προς την γενικευμένη χρήση ψηφιακών υπογραφών στην Ελληνική Δημόσια Διοίκηση θα αποτελέσει ιδίως η υλοποίηση και η ολοκλήρωση του "Υποέργου 9" του - ήδη σε εξέλιξη - συνολικού έργου Σύζευξις, όπου προβλέπεται η χρήση Υποδομής Δημοσίου Κλειδιού (PKI) και η πιστοποίηση ψηφιακών υπογραφών για έναν μεγάλο αριθμό δημοσίων υπαλλήλων, οι οποίοι θα μπορούν να εκδίδουν, να υπογράφουν και να διακινούν επίσημα ηλεκτρονικά δημόσια έγγραφα.

PDF created with pdfFactory Pro trial version www.pdffactory.com

5. Κρυπτογραφία (Encryption)

[14]Το Διαδίκτυο ήδη χρησιμοποιείται από εκατομμύρια χρήστες, και επεκτείνεται με εκθετικούς ρυθμούς αύξησης. Μπορεί να θεωρηθεί όπως χώρος επικοινωνίας, εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη. Η νέα αυτή ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου όπως προσωπικής ζωής των μελών όπως, το οποίο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα.

Σε **νομικό και κοινωνικό επίπεδο**, τίθεται ζήτημα προστασίας του απορρήτου όπως ηλεκτρονικής αλληλογραφίας (e-mail), των συναλλαγών (αριθμός πιστωτικής κάρτας, τραπεζικό απόρρητο), του ιατρικού απορρήτου και γενικότερα το ζήτημα όπως προστασίας προσωπικών στοιχείων και δεδομένων του κάθε χρήστη του Διαδικτύου, που με διάφορους τρόπους μπορούν να συλλεχθούν από τρίτους και να χρησιμοποιηθούν για οποιονδήποτε σκοπό χωρίς τη συγκατάθεση του.

Σε **ακαδημαϊκό επίπεδο**, τίθεται θέμα προστασίας αποτελεσμάτων ακαδημαϊκής έρευνας, ευαίσθητων προσωπικών δεδομένων (βαθμολογία φοιτητών), ακαδημαϊκών μελετών και γενικότερα προστασίας των πνευματικών δικαιωμάτων (copyright) των μελών όπως ακαδημαϊκής κοινότητας.

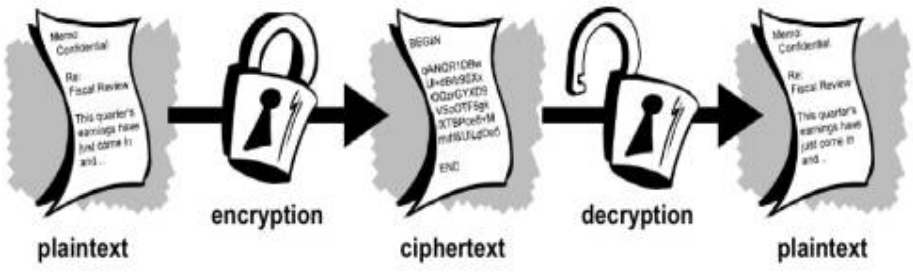
Σε **οικονομικό επίπεδο**, η ασφάλεια και προστασία των εμπορικών πλέον δεδομένων, όπως η εξασφάλιση όπως εγκυρότητας των συναλλαγών μέσω όπως αποδοχής όπως ηλεκτρονικής υπογραφής και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα, που αποτελούν το υπόβαθρο όπως ψηφιακής παγκόσμιας αγοράς.

Η κρυπτογραφία εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών και είναι η τεχνολογική πλευρά όπως λύσης στα προαναφερθέντα ζητήματα ασφαλείας.

5.1 Βασικές έννοιες κρυπτογραφίας

[8]Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο όπως ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.

Το αρχικό μήνυμα ονομάζεται **απλό κείμενο** (plaintext) και είναι αυτό που θέλουμε να προστατεύσουμε, ενώ το *ακατάληπτο* μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται **κρυπτογράφημα** (ciphertext) (Σχήμα 1).



PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 7. Κρυπτογράφηση απλού κειμένου

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκρυπτογράφηση κρυπτογραφημένων πληροφοριών χωρίς την χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης (από-κρυπτογράφησης) είναι μια **μαθηματική συνάρτηση** που χρησιμοποιείται για την κρυπτογράφηση (αποκρυπτογράφηση) των πληροφοριών.

- **Κρυπτογράφηση** $F_e(t,K_e) = c$ όπου Fe ο αλγόριθμος κρυπτογράφησης και t τα δεδομένα σε ελεύθερη μορφή όπως, ενώ Ke το κλειδί κρυπτογράφησης ενώ c είναι το «κρυπτογράφημα»
- **Αποκρυπτογράφηση** $F_d(c,K_d) = t$ όπου F_d ο αλγόριθμος από-κρυπτογράφησης, c το «κρυπτογράφημα» και t τα δεδομένα, ενώ Ke το κλειδί κρυπτογράφησης

Το ίδιο αρχικό κείμενο κρυπτογραφείτε σε διαφορετικά *κρυπτογραφήματα* όταν χρησιμοποιούνται διαφορετικά κλειδιά. Δηλαδή $F_e(t,K_e) = c$ ενώ αν χρησιμοποιήσουμε άλλο K_e (έστω K_e') τότε $F_e(t,K_e') = c'$ με $c \neq c'$

Ο αλγόριθμος F_e (για την κρυπτογράφηση) και F_d πρέπει θεωρούνται γνωστοί (δεν είναι κρυφή) ενώ η μόνη μυστική πληροφορία είναι το κλειδί K. Η ασφάλεια των κρυπτογραφικών αλγορίθμων και των πληροφοριών που προστατεύουν στηρίζονται μόνο στο κλειδί που χρησιμοποιείτε.

Όσο καλός και να είναι όπως αλγόριθμος κρυπτογράφησης θα πρέπει ταυτόχρονα να έχει *ικανό-αρκετό* «μέγεθος κλειδιού» (ή πλήθος *δυνατών* κλειδιών). Σε τελική ανάλυση κανείς δεν μπορεί να αποτρέψει κάποιον επιτιθέμενο να προσπαθήσει να *μαντέψει* το κλειδί (να δοκιμάζει διάφορα κλειδιά μέχρι να βρει το σωστό). Η επίθεση που δοκιμάζει όλα τα δυνατά κλειδιά ονομάζεται "*εξαντλητική επίθεση*" (brute force). Για να είναι ασφαλής όπως αλγόριθμος θα πρέπει αυτή η διαδικασία να είναι «πρακτικά» μη εφικτή. Αν όπως επιτιθέμενος δοκιμάζει 100 κλειδιά το δευτερόλεπτο και εμείς πρέπει να κρατήσουμε μυστική την πληροφορία για 1 ώρα θα πρέπει να έχουμε περισσότερα από 360.000 δυνατά κλειδιά (για την ακρίβεια θα πρέπει να έχουμε τουλάχιστον τα διπλάσια 720.000 ώστε η πιθανότητα να το βρει σε μία ώρα να είναι μικρότερη από ½). Οι σημερινοί αλγόριθμοι υποστιρίζουν συνήθως εξαιρετικά μεγάλο πλίθος πιθανών κλειδιών. Όπως σύγχρονος συμμετρικός αλγόριθμος υποστηρίζει 2^{128} δυνατά κλειδιά ή 3,402823669209384634633746074317 7e+38 δυνατά κλειδιά (possible keys). Ως εκ τούτου η πιθανότητα να το μαντέψει κάποιος τρίτος είναι σχεδόν μηδενική (πρακτικά 0). Το να προσπαθήσει να δοκιμάσει όλα τα πιθανά κλειδιά είναι διαδικασία που απαιτεί χρόνο ίσο με πολλά γαλαξιακά έτη (δισεκατομμύρια χρόνια).

Παράδειγμα: Κρυπτογραφικός Αλγόριθμος του Καίσαρα

Λέγεται ότι ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με όπως επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε

PDF created with pdfFactory Pro trial version www.pdffactory.com

γράμματος του αλφαβήτου με κάποιο άλλο, όχι όπως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου όπως τα δεξιά Κάθε γράμμα αντικαθιστάται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση όπως μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε φυσικά το κλειδί να ήταν 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Ο πίνακας αντιστοίχησης των γραμμάτων φαίνεται παρακάτω:

Το γράμμα	a	b	c	d	e	f	g	h	i	j	k	v	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη **secret**, θα προκύψει το κρυπτογράφημα **wigvix**. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου όπως τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3.

Η σύγχρονη κρυπτογραφία είναι πολύ πιο πολύπλοκη. Ένα κρυπτογραφημένο κείμενο αν αποδοθεί με χαρακτήρες μπορεί να δείχνει κάπως έτσι

Αρχικό κείμενο

"This information need to remain secret. Never reviiel it to third parties. All data are considered national secrets and should be treated with extreme causion…"

Η κρυπτογραφημένη πληροφορία για το ίδιο κείμενο μπορεί να δείχνει κάπως έτσι

hIwDY32hYGCE8MkBA/wOu7d45aUxF4Q0RKJprD3v5Z9K1YcRJ2fve87lMl Dlx4OjeW4GddBfLbJE7Vupp13N19GL8e/AqbyyjHH4aS0YoTk10QQ9nnRvjY 8nZL3MPXSZg9VGQxFeGqzykzmykU6A26MSMexR4ApeeON6xzZWfo+

Όπως βλέπουμε το να υποκλέψει κανείς κρυπτογραφημένη πληροφορία δεν τον βοηθά όταν δεν ξέρει το κλειδί γιατί δεν μπορεί να συμπεράνει οτιδήποτε για το αρχικό κείμενο. Η πληροφορία για αυτόν είναι απλά θόρυβος (ή «σκουπίδια»)

5.2 Διαδικασίες Κρυπτογράφησης – Αποκρυπτογράφησης

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρούν την πληροφορία ασφαλή και χρησιμοποιούνται και στην κρυπτογράφηση αλλά και στην αποκρυπτογράφηση.

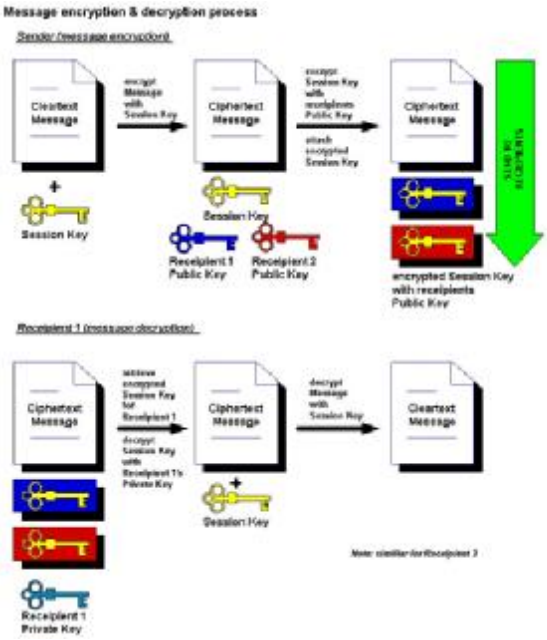
PDF created with pdfFactory Pro trial version www.pdffactory.com

Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης όταν λάβει τα δεδομένα αποκρυπτογραφεί το κείμενο και το μετατρέπει στην μορφή που είχε πριν.

[11]Αρχικά στην δεκαετία το ‘80, το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα (symmetric cryptosystem). Το σύστημα αυτό χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε για τη μεταφορά τραπεζικών δεδομένων. Στο σύστημα αυτό το κλειδί ήταν γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή όμως παρουσίασε πολλά μειονεκτήματα στην εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες όπου οι απαιτήσεις είναι μεγαλύτερες και αυξάνονται συνεχώς. Τα βασικά χαρακτηριστικά της συμμετρικής κρυπτογραφίας είναι τα εξής:

- Χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση.
- Το κλειδί πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη, διαφορετικά δεν διασφαλίζεται η ακεραιότητα του μηνύματος
- Προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική
- Στη συμμετρική κρυπτογραφία αποκαλούμενη και ως κρυπτογράφηση μυστικού κλειδιού (secret-key), ο αποστολέας και ο παραλήπτης του μηνύματος χρησιμοποιούν το ίδιο κοινό κλειδί. Δηλαδή, ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί.
- Στην κρυπτογραφία αυτού του τύπου, θα πρέπει όλα τα κλειδιά που χρησιμοποιούνται να παραμένουν κρυφά, κάτι που είναι εξαιρετικά δύσκολο Internet.
- Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος DES (Data Encryption Standard), που υιοθετήθηκε από την Αμερικάνικη και το σύστημα Kerberos του γνωστού Πανεπιστημίου MIT.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 7. Διαδικασία κρυπτογράφηση - αποκρυπτογράφησης μηνύματος

Αργότερα η εξέλιξη οδήγησε στη χρησιμοποίηση δύο κλειδιών, ενός ιδιωτικού και ενός δημόσιου, το σύστημα αυτό ονομάστηκε ασύμμετρο κρυπτογραφικό σύστημα - asymmetric or public key cryptosystem. Τα βασικά χαρακτηριστικά της συμμετρικής κρυπτογραφίας είναι τα εξής:

- Χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί.
- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο. Ακόμα κι αν γνωρίζει κάποιος το ένα κλειδί, είναι πρακτικά αδύνατον να υπολογίσει το άλλο.
- Ο αποστολέας ενός μηνύματος κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη.
- Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.
- Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της.
- Η τεχνολογία της ασύμμετρης κρυπτογραφίας, χρησιμοποιείται για τη δημιουργία ψηφιακών υπογραφών.
- Παράγονται, βάσει συγκεκριμένων μαθηματικών αλγορίθμων τυχαία ζεύγη κρυπτογραφικών κλειδιών.
- Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ψηφιακής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της, ο παραλήπτης χρησιμοποιεί

PDF created with pdfFactory Pro trial version www.pdffactory.com

το δημόσιο κλειδί του αποστολέα. Το δημόσιο κλειδί δημοσιεύεται στον κόσμο ενώ το ιδιωτικό κλειδί φυλάσσεται μυστικό.

- Στη διαδικασία της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής υπεισέρχεται και η έννοια της μονόδρομης συνάρτησης κερματισμού (ή κατατεμαχισμού - one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από κάθε μήνυμα - ανεξαρτήτως μεγέθους - παράγεται μια «σύνοψη», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) αποτελεί ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει.

Το ιδιωτικό κλειδί (private key) λοιπόν, χρησιμοποιείται για το σφράγισμα του ηλεκτρονικού μηνύματος και είναι απόρρητο, το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο,

Το δημόσιο κλειδί (public key) από την άλλη, αντιστοιχεί στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο, γνωστοποιεί σε κάθε συναλλασσόμενο του για να μπορεί να αποκρυπτογραφεί/διαβάζει τα μηνύματα του πρώτου. Μόνο με το δημόσιο κλειδί μπορεί λοιπόν ο παραλήπτης να διαβάσει τις πληροφορίες.

Συνεπώς, το πρώτο κλειδί το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο, ενώ το δεύτερο το γνωστοποιεί σε κάθε συναλλασσόμενο του για να μπορεί να αποκρυπτογραφεί/διαβάζει τα μηνύματα του πρώτου.

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας έναντι της συμμετρικής φαίνονται από την διανομή του δημόσιου κλειδιού. Οποιοσδήποτε μπορεί να πάρει το δημόσιο κλειδί ενός χρήστη και να το χρησιμοποιήσει για να του στείλει ένα κρυπτογραφημένο μήνυμα. Δεν υπάρχει όμως ο κίνδυνος να το διαβάσει κάποιος άλλος αφού ξεκλειδώνει μόνο με το αντίστοιχο ιδιωτικό (μυστικό) κλειδί.

Συνοπτικά μπορούμε να πούμε ότι η μέθοδος που χρησιμοποιείται για να «καλυφθεί» το απλό κείμενο ονομάζεται κρυπτογράφηση (encryption). Η επιστήμη αυτή βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι και με τον τρόπο αυτό εξασφαλίζεται έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου.

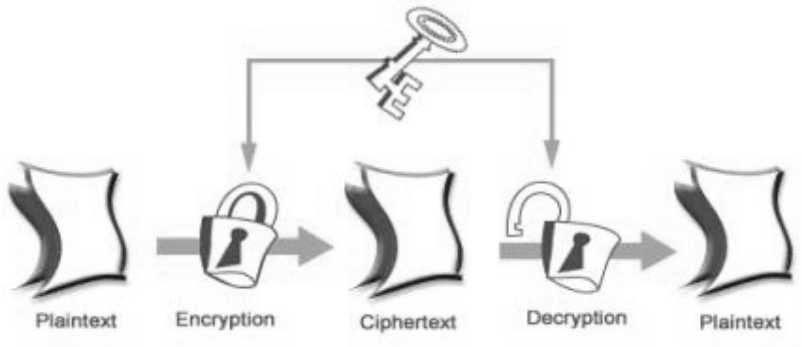
5.3 Συμμετρική και ασύμμετρη κρυπτογραφία

5.3.1 Συμμετρική κρυπτογραφία

Στη συμμετρική κρυπτογραφία, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση (Σχήμα 2). Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική

PDF created with pdfFactory Pro trial version www.pdffactory.com

συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



Εικόνα 9. Συμμετρική Κρυπτογραφία

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο ιστορικά γνωστό το Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών. Ο DES έχει μόνο 56bit κλειδί το οποίο σήμερα θεωρείτε μικρό. Μικρό μήκος κλειδιού θα πει πώς τα δυνατά κλειδιά που είναι 2^{56} δεν είναι αρκετά για να εμποδίσουν επιθέσεις όπου δοκιμάζονται όλα τα δυνατά κλειδιά μέχρι να βρεθεί το σωστό (brute force). Σήμερα μπορούμε με ειδική συσκευή υλικού να βρούμε το κλειδί (όποιο και αν είναι αυτό) σε οποιοδήποτε κρυπτογραφημένο κείμενο με DES σε μία (1) περίπου ώρα.

Για τον λόγο αυτό δεν χρησιμοποιείτε ο ίδιος ο DES. Στην θέση του χρησιμοποιούνται ο **3DES** (112bit) και ο αντικαταστάτης του DES ή πιο πρόσφατα ο **AES** (advanced encryption standard) με 128 και 256bit μέγιστο μέγεθος κλειδιού. Ο **AES** εκτός από την ασφάλεια έχει επιλεχθεί ώστε να είναι και αποδοτικός. Έτσι ο **AES** αν και 128bit είναι περίπου το ίδιο γρήγορος με το απλό DES (56bit) (και 3 φορές πιο γρήγορος από τον 3DES) σε μηχανήματα με ίδια υπολογιστική ισχύ. Κλειδιά μεγαλύτερα των 64bit θεωρούνται άσπαστα σε επιθέσεις brute force (2^{64} δυνατά κλειδιά). Κλειδιά 128bit και πάνω θεωρούνται άσπαστα και σήμερα και στο μέλλον όσο και να αυξηθεί (σε λογικά επίπεδα) η γραμμική επεξεργαστική ισχύς των υπολογιστών.

5.3.1.1 Αλγόριθμοι ροής και αλγόριθμοι ομάδας δεδομένων

Η συμμετρική κρυπτογραφία έχει κυρίως δύο τύπους αλγορίθμων τους αλγόριθμους ροής (**stream ciphers**) και τους αλγόριθμους ομάδας δεδομένων (**block ciphers**). Οι πρώτοι επεξεργάζονται την πληροφορία ένα ένα bit ενώ οι δεύτεροι σε ομάδες από bits (blocks). Οι *block ciphers* σήμερα θεωρούνται εν γένει πιο ασφαλείς από τους *stream ciphers* μιας που εκτός από το να αλλάζουν το κάθε ένα Bit με κάτι άλλο (confusion) επιπλέον μεταθέτουν τα bit μεταξύ τους (confusion). Έχουν ωστόσο κάποια μειονεκτήματα έναντι των stream ciphers όπως ότι

α) είναι εν γένει πιο αργοί (συγκρινόμενοι στο ίδιο υλικό)

β) απαιτούν ακριβότερα κυκλώματα για υλοποίηση σε επίπεδο hardware

PDF created with pdfFactory Pro trial version www.pdffactory.com

γ) έχουν το παράγοντα «μετάδοσης λάθους» (**error propagation**). Αν χαθεί ένα bit στην μετάδοση του κρυπτογραφήματος επηρεάζονται περισσότερα bit στην αποκρυπτογράφηση με αποτέλεσμα να μην είναι το ίδιο χρήσιμοι σε περιβάλλοντα όπως μετάδοση φωνής πχ μέσω RF όπου η συνεχής απώλεια κάποιων bit είναι δεδομένη.

δ) Δεν είναι «σύγχρονοι» πάντα (εισάγουν καθυστέρηση) με αποτέλεσμα να μην είναι το ίδιο χρήσιμοι σε περιβάλλοντα όπως μετάδοση φωνής.

Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT. Τα σχήματα αυτά παρουσιάζουν το μειονέκτημα ότι δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή

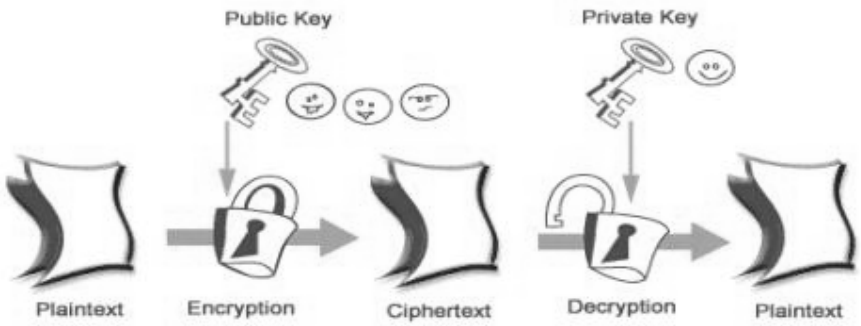
Ωστόσο σήμερα όπως εξηγούμε παρακάτω συνήθως χρησιμοποιούνται τεχνικές *ασύμμετρης κρυπτογράφησης* για ανταλλαγή κλειδιών που λύνουν το παραπάνω πρόβλημα.

5.3.2 Ασύμμετρη Κρυπτογραφία

Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα (Σχήμα 3). Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες.

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό και αποδοτικό τρόπο.



Εικόνα 10. Ασύμμετρη κρυπτογραφία

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους **Diffie και Hellman**, ενώ το 1977 οι Rivest, Shamir και Adleman βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων δημιούργησαν το κρυπτοσύστημα **RSA**, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου

PDF created with pdfFactory Pro trial version www.pdffactory.com

κλειδιού. Τέλος πρόσφατα έχουν αναπτυχθεί και άλλες μέθοδοι όπως της **ελλειπτικής καμπύλης** (elliptic curve) που όμως είναι λιγότερο δημοφιλείς.

Για να αποκατασταθεί επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Τα ζεύγη κλειδιών που χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία δεν είναι αντίστοιχα της συμμετρικής. Εδώ τα συνήθεις μεγέθη είναι 1024 και 2048bits (έναντι 128 και 256bit). Ο λόγος έχει να κάνει με τους αλγορίθμους και τα μαθηματικά προβλήματα που χρησιμοποιούν και στηρίζουν σε αυτά την ασφάλεια τους. Εδώ συνήθως η καλύτερη επίθεση δεν είναι να βρεις το κλειδί με brute-force αλλά να επιλύσεις ένα μαθηματικό πρόβλημα (παραγοντοποιήση μεγάλων πρώτων αριθμών).

Η ασύμμετρη κρυπτογραφία αν και θεωρητικά πιο πρακτική έχει το μειονέκτημα ότι οι αλγόριθμοι της είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης (>10 φορές).

Για τον λόγο αυτό δεν χρησιμοποιούμε ασύμμετρη κρυπτογραφία για την κρυπτογράφηση του κυρίου όγκου πληροφοριών που θέλουμε να ανταλλάξουμε. Την χρησιμοποιείτε σε συνδυασμό με την συμμετρική. Έτσι το κυρίως μήνυμα (που έχει και τον πιο πολύ όγκο) κρυπτογραφείτε με συμμετρικούς αλγορίθμους (**AES, 3DES, IDEA**) ενώ τα κλειδιά που χρησιμοποιήθηκαν (πολύ μικρά σε όγκο) ανταλλάσσονται κρυπτογραφημένα με μεθόδους ασύμμετρης κρυπτογραφίας.

Windows 2000 και XP και κρυπτογράφηση αρχείων

Τα Windows 2000 (XP) και νεώτερα υποστηρίζουν ευγενώς κρυπτογραφία αρχείων (EFS) που συνδυάζει ασύμμετρη και συμμετρική κρυπτογραφία. Η υλοποίηση είναι πολύ απλή και διάφανη στο χρήστη. Μπορεί οποιοσδήποτε χρήστης να κρυπτογραφήσει ένα οποιοδήποτε αρχείο με ένα απλό δεξί κλικ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 11.

Τα δεδομένα κρυπτογραφούνται με ένα τυχαίο κλειδί (μοναδικό για κάθε αρχείο) που δημιουργείται κατά την πρώτη κρυπτογράφηση από το σύστημα (Data encryption key) και με τους αλγόριθμους DES, 3DES, AES (αναλόγως έκδοση). Το τυχαίο κλειδί στην συνέχεια κρυπτογραφείται με το δημόσιο κλειδί (key encryption key) του χρήστη που κρυπτογραφεί το αρχείο αλλά και προαιρετικά και με των πρακτόρων ανάκτησης (recovery agents) που τις πιο πολλές φορές είναι εξορισμού ο administrator.

Προσοχή: Τα αρχεία που είναι κρυπτογραφημένα με EFS ΔΕΝ ανακτώνται από recvery εργαλεία (linux boot CDs, WinPE κτλ) ή τρίτους χρήστες που απλά έχουν read access στο folder. Αν χαθεί ο κωδικός του χρήστη που χρησιμοποιείτε για να έχει πρόσβαση στο μυστικό του κλειδί τα δεδομένα που κρυπτογραφήθηκαν χάνονται οριστικά (εκτός αν υπάρχει *πράκτωρ ανάκτησης* στο ίδιο σύστημα. Λήψη αντιγράφων των κλειδιών ή των ίδιων αρχείων σε κανονική μορφή πρέπει να λαμβάνονται σύμφωνα με την πολιτική ασφαλείας.

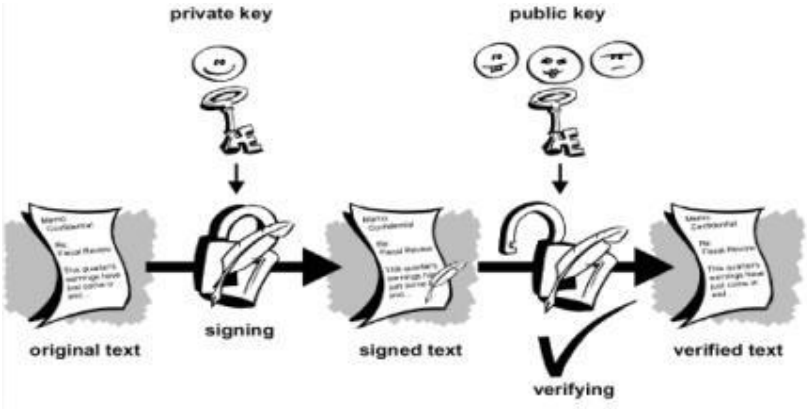
5.4 Ψηφιακές Υπογραφές

[13]Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής ψηφιακής υπογραφής (digital signature). Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι.

Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί. Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να επιβεβαιώσει ότι το μήνυμα υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί. Εφόσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, μόνο αυτός θα μπορούσε να το χρησιμοποιήσει, για

PDF created with pdfFactory Pro trial version www.pdffactory.com

να υπογράψει κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό.



Εικόνα 12. Ψηφιακές Υπογραφές

Πιο αναλυτικά, πρώτο βήμα για την δημιουργία της ψηφιακής υπογραφής είναι η παραγωγή μιας σύνοψης μηνύματος (message digest). Για το σκοπό αυτό, το λογισμικό που παράγει τις υπογραφές χρησιμοποιεί μία συνάρτηση κατακερματισμού (hash function). Η συνάρτηση αυτή αντιστοιχεί σε κάθε μήνυμα μία μοναδική ακολουθία χαρακτήρων, που ονομάζεται σύνοψη του μηνύματος και έχει σταθερό μήκος, ανεξάρτητα από το μήκος του μηνύματος. Η σύνοψη, κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα, αποτελεί την υπογραφή, η οποία επισυνάπτεται στο μήνυμα.

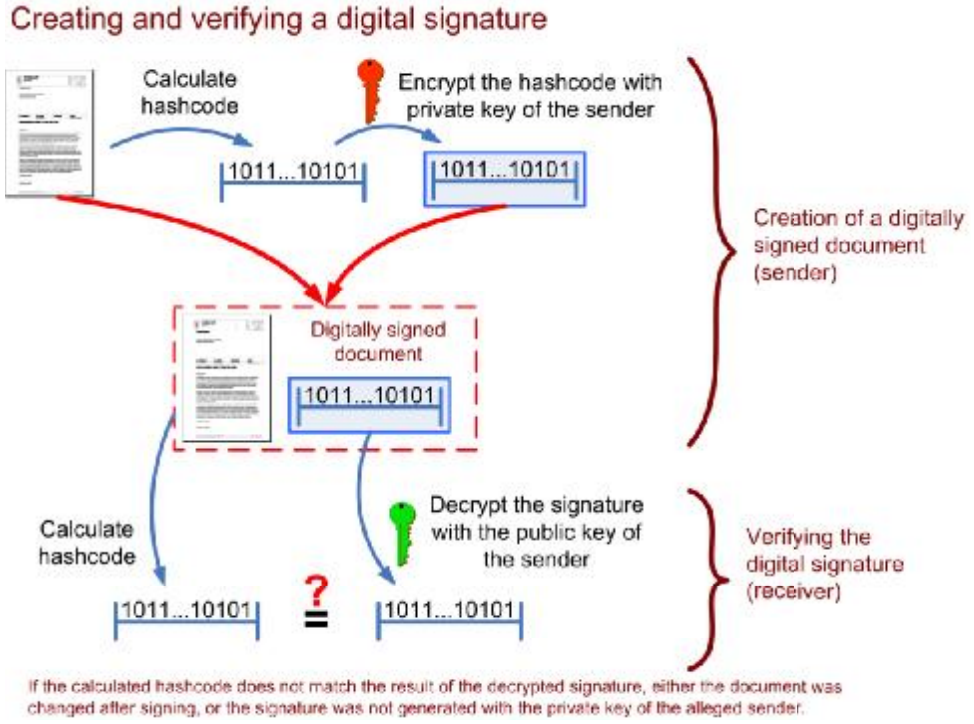
Ο παραλήπτης λαμβάνει τόσο το μήνυμα όσο και την υπογραφή. Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την υπογραφή, οπότε προκύπτει η σύνοψη του μηνύματος, όπως αυτή είχε παραχθεί πριν την αποστολή του μηνύματος. Εφόσον η υπογραφή έχει παραχθεί με το ιδιωτικό κλειδί του αποστολέα, μόνο το δημόσιο κλειδί του μπορεί να την αποκρυπτογραφήσει και να δώσει τη σύνοψη του μηνύματος. Η συνάρτηση κατακερματισμού χρησιμοποιείται για να παραχθεί μία σύνοψη του μηνύματος, όπως αυτό έχει φτάσει στα χέρια του παραλήπτη. Εφόσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά την αποστολή του, η σύνοψη του μηνύματος θα είναι ίδια με αυτήν που είχε προκύψει κατά την υπογραφή του από τον αποστολέα. Με τον τρόπο αυτό, ο παραλήπτης βεβαιώνει την αυθεντικότητα του μηνύματος.

PDF created with pdfFactory Pro trial version www.pdffactory.com

6. Δημιουργία Ψηφιακής Υπογραφής

[14]Πριν αναφέρουμε τα βήματα για την δημιουργία ψηφιακής υπογραφής θα πρέπει να επισημάνουμε το γεγονός ότι στην διαδικασία αυτή δεν κρυπτογραφούνται τα προς υπογραφή δεδομένα, αλλά μία μικρή μαθηματική «σύνοψή» τους (message digest).

Στην διαδικασία της δημιουργίας και της επαλήθευσης της ηλεκτρονικής υπογραφής λοιπόν, εμπλέκεται η έννοια της συνάρτησης one way hash- ή συνάρτησης κατακερματισμού. Πρόκειται για μηχανισμούς που στην είσοδο τους δέχονται ένα οποιοδήποτε μήνυμα, μεγάλο ή μικρό, ενώ στην έξοδο δίνουν ένα μεγάλο αλφαριθμητικό σταθερού μήκους. Η σύνοψη του μηνύματος (message digest) είναι μια ψηφιακή αναπαράσταση του μηνύματος. Είναι μοναδική για το μήνυμα και το αντιπροσωπεύει, αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του.. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Τέλος, η σύνοψη των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται στα αρχικά δεδομένα, αποτελώντας την ψηφιακή υπογραφή.



Εικόνα 13.Δημιουργία και επικύρωση Ψηφιακής Υπογραφής

Το ενδιαφέρον με τις συναρτήσεις hash είναι ότι έχουν εξαιρετικά μεγάλη ευαισθησία στο περιεχόμενο του μηνύματος εισόδου. Αν αυτό μεταβληθεί στο παραμικρό τότε το αλφαριθμητικό εξόδου διαφέρει σημαντικά από το προηγούμενο. Είναι υπολογιστικά αδύνατον κάποιος να καταφέρει να εξάγει το αρχικό μήνυμα. Η ηλεκτρονική υπογραφή είναι στην ουσία η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα, σύνοψη και είναι διαφορετική για κάθε μήνυμα.

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί

PDF created with pdfFactory Pro trial version www.pdffactory.com

στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί, την ταυτότητα του αποστολέα. Αυτός είναι και ο τρόπος αυθεντικοποίησης της ταυτότητας του αποστολέα μηνύματος. Μια ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχο του.

6.1 Βήματα

[1]Τα βήματα για την δημιουργία ψηφιακής υπογραφής παρουσιάζονται πιο κάτω και είναι τα έξης:

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (oneway hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειράς ψηφίων.

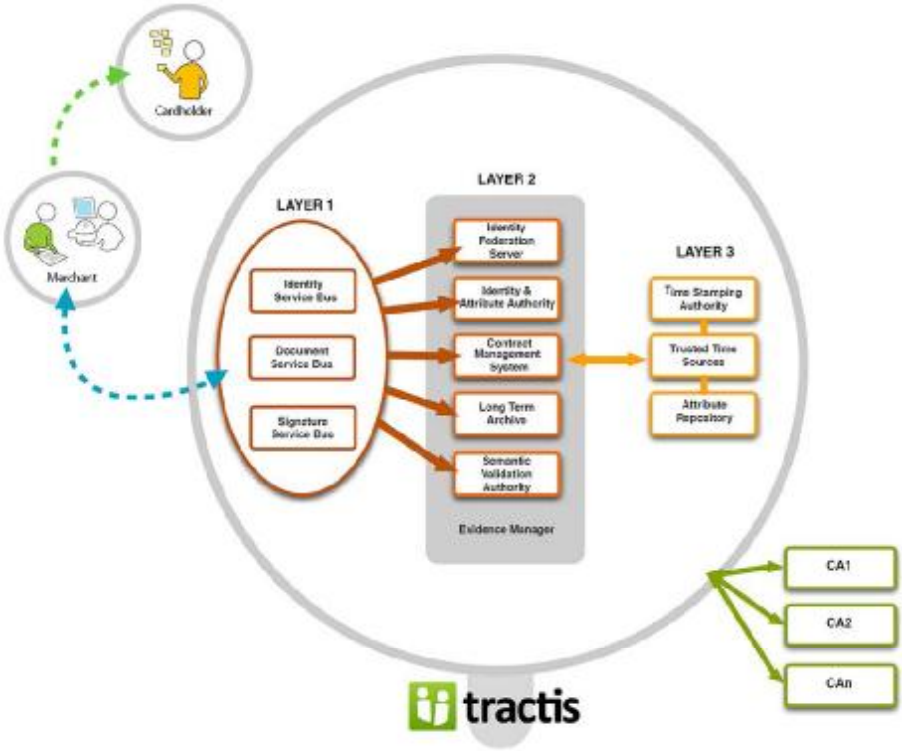
2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη που έχει δημιουργηθεί. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου. Ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη)

PDF created with pdfFactory Pro trial version www.pdffactory.com

6.2 Επαλήθευση Ψηφιακής Υπογραφής

Κατά την διαδικασία της επαλήθευσης της ψηφιακής υπογραφής, εφαρμόζεται στο κανονικό κείμενο ο ίδιος αλγόριθμος κατακερματισμού που χρησιμοποιήθηκε κατά την υπογραφή του και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Στην συνέχεια, αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα η κρυπτογραφημένη σύνοψη του μηνύματος.



Εικόνα 14. Επίπεδα επαλήθευσης Ψηφιακής Υπογραφής

Η νέα σύνοψη που παράγεται, συγκρίνεται με την αντίστοιχη σύνοψη που προέρχεται από την αποκρυπτογράφηση της ψηφιακής υπογραφής. Εάν ταυτίζονται οι δύο συνόψεις, τότε η υπογραφή επαληθεύεται και επιβεβαιώνεται αφενός μεν ότι τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού, αφετέρου δε ότι τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.

6.3 Βήματα

[14]Τα βήματα για την επαλήθευση ψηφιακής υπογραφής παρουσιάζονται πιο κάτω και είναι τα έξης:

Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

1. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

PDF created with pdfFactory Pro trial version www.pdffactory.com

2. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

3. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο (αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί)

Τόσο ο αποστολέας όσο και ο αποδέκτης μιας ψηφιακής υπογραφής, πρέπει, κατ' αρχήν, να κατανοούν τον τρόπο χρήσης και λειτουργίας των ηλεκτρονικών υπογραφών που χρησιμοποιούν. Πρέπει, επίσης, να λάβουν γνώση όλων των σχετικών όρων στα κείμενα που τους παρέχει ο ΠΥΠ (π.χ. Σύμβαση Συνδρομητή με τον ΠΥΠ, Πολιτική Πιστοποιητικού κ.λπ.) διότι εκεί αναγράφονται όλοι οι όροι χρήσης και οι περιορισμοί του πιστοποιητικού που υποστηρίζει την συγκεκριμένη ψηφιακή υπογραφή.

Ειδικότερα ο αποστολέας που είναι και αυτός που υπογράφει (κάτοχος των κρυπτογραφικών κλειδιών και υποκείμενο του σχετικού πιστοποιητικού τους) θα πρέπει να συμμορφώνεται πλήρως με τους όρους της συνδρομητικής σύμβασης που σύναψε με τον ΠΥΠ για την απόκτηση του σχετικού πιστοποιητικού του, διότι, σε αντίθετη περίπτωση, είναι πιθανόν να επωμισθεί ο ίδιος την ευθύνη για την οποιαδήποτε τυχόν πλημμέλεια των συναλλαγών που θα πραγματοποιηθούν με την χρήση της σχετικής ηλεκτρονικής υπογραφής του. Οι βασικότερες υποχρεώσεις του υπογράφοντα οι οποίες περιλαμβάνονται, συνήθως, σε όλες τις τυποποιημένες σχετικές συνδρομητικές συμβάσεις που συντάσσουν οι ΠΥΠ, είναι οι εξής:

1. Να δηλώνει πραγματικά και ενημερωμένα στοιχεία της ταυτότητάς του κατά την αίτησή του για την έκδοση του σχετικού πιστοποιητικού ηλεκτρονικής υπογραφής του στην Υπηρεσία Εγγραφής του ΠΥΠ και να ελέγχει την ορθή μεταφορά τους στο πιστοποιητικό, πριν το χρησιμοποιήσει.

2. Να τηρεί με επιμέλεια την μυστικότητα και την αποκλειστική χρήση των σχετικών ιδιωτικών κλειδιών του (μη έκθεση σε τρίτους),

3. Να ζητά από τον ΠΥΠ την ανάκληση (ή την αναστολή) του σχετικού πιστοποιητικού του εάν βεβαιωθεί για (ή υποψιασθεί) οποιαδήποτε έκθεση των ιδιωτικών κλειδιών του σε τρίτους, καθώς και στην περίπτωση που απολέσει τον φορέα ή και τον έλεγχο των ιδιωτικών κλειδιών του.

4. Να χρησιμοποιεί τα συγκεκριμένα κρυπτογραφικά κλειδιά του μόνο στις επιτρεπόμενες για το σχετικό πιστοποιητικό τους χρήσεις και να μην υπερβαίνει στις σχετικές συναλλαγές του τα τυχόν όρια που προβλέπονται από την σύμβαση και την εφαρμοζόμενη πολιτική του συγκεκριμένου πιστοποιητικού.

Ο αποδέκτης μιας ψηφιακής υπογραφής πριν βασισθεί στα περιεχόμενα του σχετικού πιστοποιητικού (ώστε να διαμορφώσει συγκεκριμένη πεποίθηση για ένα γεγονός ή να προβεί σε μια σε μια σχετική πράξη), θα πρέπει να ελέγξει και να αποδεχτεί τους όρους χρήσης του πιστοποιητικού, οι οποίοι, συνήθως, αναφέρονται συνοπτικά σε μια τυποποιημένη και δημοσιευμένη από τον ΠΥΠ Σύμβαση Αποδέκτη (Relying Party Agreement) ή και ενσωματώνονται (μαζί με άλλους όρους) στην προσδιοριζόμενη Πολιτική Πιστοποιητικού (Certificate Policy). Για να στηριχθεί στην ηλεκτρονική υπογραφή κάποιου τρίτου, ένας αποδέκτης της θα πρέπει, πρώτα, να εξασφαλίσει ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα (που

PDF created with pdfFactory Pro trial version www.pdffactory.com

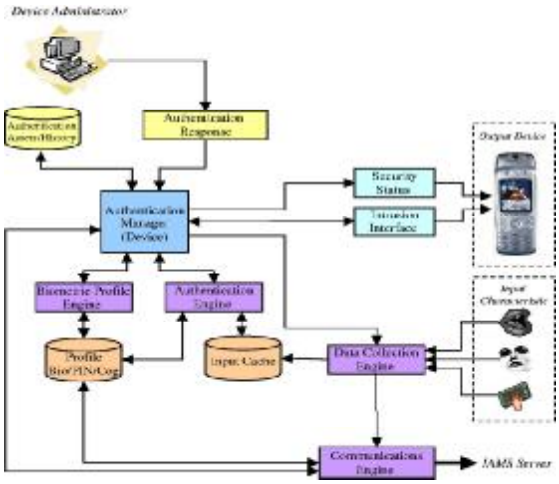
επαληθεύει την υπογραφή): α) είναι αυθεντικό, με την έννοια ότι υπάρχει τουλάχιστον μία αλληλουχία πιστοποιητικών (με όλους τους μεσολαβούντες υπό-εκδότες) η οποία να καταλήγει σε μια αξιόπιστη γι' αυτόν ρίζα εμπιστοσύνης'(συνήθως το αυτό-υπογραφόμενο πιστοποιητικό Root CA ενός γνωστού ΠΥΠ), β) είναι έγκυρο, δηλαδή ότι δεν έχει λήξει ή ανακληθεί η ισχύς του. Αυτό σημαίνει ότι ο αποδέκτης θα πρέπει να ελέγξει, όχι μόνο την διάρκεια ισχύος (ημερομηνία λήξης) που αναγράφεται μέσα στο ίδιο το εξεταζόμενο πιστοποιητικό, αλλά και τις σχετικές Λίστες Ανακληθέντων Πιστοποιητικών που δημοσιεύει ο ίδιος ο εκδότης του. Ο έλεγχος αυτός μπορεί να γίνει είτε μέσω ειδικών αυτοματοποιημένων εφαρμογών που εμπιστεύεται ο χρήστης, είτε μέσω σχετικής Απ' ευθείας Υπηρεσίας Ενημέρωσης Ανάκλησης Πιστοποιητικών (Online Certificate Status Protocoll - OCSP) που πιθανώς να παρέχει ο ΠΥΠ ή τρίτος, γ) είναι κατάλληλο για την συναλλαγή ή την χρήση στην οποία ο αποδέκτης του πρόκειται να προβεί. Για να θεωρηθεί κατάλληλο ένα πιστοποιητικό θα πρέπει η προτιθέμενη χρήση του να μην απαγορεύεται από την σχετική Πολιτική Πιστοποιητικού. Επίσης, εάν από τον τύπο της επιχειρούμενης συναλλαγής έχει καθοριστεί ή και πρέπει να ακολουθηθεί μια συγκεκριμένη Πολιτική (ηλεκτρονικής) Υπογραφής, τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή, έστω, να επιτρέπεται από την εφαρμοζόμενη Πολιτική Υπογραφής.

Η Πολιτική Υπογραφής (Signature Policy) είναι ένα συγκεκριμένο κείμενο, το οποίο αναφέρει διεξοδικά όλους τους απαραίτητους όρους για την έγκυρη εναπόθεση ή και επαλήθευση μιας ηλεκτρονικής υπογραφής, οι οποίοι εφαρμόζονται σε έναν καθορισμένο κύκλο συναλλαγών. Η Πολιτική Υπογραφής επιλέγεται με συμφωνία των μερών ή, συνηθέστερα, επιβάλλεται από την πλευρά του αποδέκτη των υπογραφών ως γενικός όρος συναλλαγών. Αποτελώντας, μάλιστα, και αντικείμενο πρόσφατης προτυποποίησης από τους αρμόδιους ευρωπαϊκούς οργανισμούς προτυποποίησης, η Πολιτική Υπογραφής μπορεί να προσδιορίζει, εκτός από τα αποδεκτά είδη /πολιτικές πιστοποιητικών, τις τυχόν απαραίτητες ιδιότητες του υπογράφοντα, την πιθανή υποχρέωση για εναπόθεση αξιόπιστης χρονοσήμανσης στην δημιουργηθείσα υπογραφή, την ανάγκη για επανέλεγχο της ανάκλησης του πιστοποιητικού πριν την οριστική αποδοχή της υπογραφής, κάποιες συγκεκριμένες ρίζες εμπιστοσύνης που απαιτείται να χρησιμοποιηθούν για την επαλήθευση των πιστοποιητικών.

6.4 Εξοπλισμός Δημιουργίας και Επαλήθευσης

Σε ότι αφορά τη δημιουργία της ψηφιακής υπογραφής πάνω σε συγκεκριμένα ηλεκτρονικά δεδομένα, θα πρέπει κάποιος - εκτός από τα απαραίτητα κρυπτογραφικά κλειδιά και το αντίστοιχο έγκυρο πιστοποιητικό - να διαθέτει και μια ολοκληρωμένη διάταξη δημιουργίας υπογραφής η οποία να απαρτίζεται από κατάλληλη σύνθεση λογισμικού (hardware) και λογισμικού (software). Στην διάταξη αυτή περιλαμβάνονται ο φορέας των κρυπτογραφικών κλειδιών (π.χ. σκληρός δίσκος υπολογιστή, έξυπνη κάρτα, USB token), ο τυχόν απαραίτητος αναγνώστης του φορέα αυτού (π.χ. αναγνώστης έξυπνης κάρτας, θύρα USB, κ.λπ.), το τερματικό επικοινωνίας του χρήστη (π.χ. PC, pda, smart phone), τα λειτουργικά συστήματα και οι οδηγοί (drivers) των συσκευών αυτών, καθώς και το λογισμικό επικοινωνίας (interface) του χρήστη που χρησιμοποιείται για τη δημιουργία της ηλεκτρονικής υπογραφής.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 85. Ασφαλές διάταξη δημιουργίας υπογραφής (Secure Signature Creation Devices – SSCD).

Για την δημιουργία αναγνωρισμένης ψηφιακής υπογραφής, η νομοθεσία απαιτεί την χρήση ασφαλούς διάταξης δημιουργίας υπογραφής (Secure Signature Creation Devices – SSCD). Ως τέτοια προσδιορίζεται (Παράρτημα ΙΙΙ Οδηγίας και ΠΔ 150/2001) η διάταξη η οποία - μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων - διασφαλίζει τουλάχιστον ότι τα δεδομένα δημιουργίας υπογραφής (ιδιωτικά κλειδιά) που χρησιμοποιούνται για την παραγωγή υπογραφών:

α) απαντούν, κατ' ουσίαν, μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο - το οποίο σημαίνει ότι τα σχετικά κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με τους κατάλληλους αλγόριθμους δημιουργίας τυχαίων κωδικών, είτε απευθείας μέσα σε συσκευή του χρήστη, είτε από κατάλληλες κρυπτογραφικές μονάδες του CSP οι οποίες μεταφέρουν άμεσα τα δημιουργηθέντα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται, χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφά τους ,

β) δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας - όρος που, εκτός από την απαγόρευση της διατήρησης με οποιονδήποτε τρόπο αντιγράφου του ιδιωτικού κλειδιού, στην ουσία του επιβάλλει την χρήση της τεχνολογίας ασύμμετρης κρυπτογραφίας ,

γ)μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους - που σημαίνει ότι τα ιδιωτικά κλειδιά δεν πρέπει να μπορούν να εξαχθούν ή και να αντιγραφούν από τον φορέα τους, ούτε να ενεργοποιηθούν χωρίς την προηγούμενη χρήση μιας επιπλέον μεθόδου επιβεβαίωσης της ταυτότητας του χρήστη (π.χ. χρήση μυστικού κωδικού αναγνώρισης (PIN) ή και ανάγνωση βιομετρικών δεδομένων του δικαιούχου).

Παράλληλα, η νομοθεσία ορίζει ότι οι SSCD δεν πρέπει να μεταβάλλουν τα προς υπογραφή δεδομένα, ούτε να εμποδίζουν την εμφάνιση των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής (επιβάλλεται δηλαδή η αρχή "What You See Is What You Sign" – WYSIWYS). Η έως σήμερα προτυποποίηση για την εξειδίκευση των απαιτήσεων για ασφαλείς διατάξεις δημιουργίας υπογραφής έχει δώσει ιδιαίτερη έμφαση στην ασφάλεια των συσκευών δημιουργίας

PDF created with pdfFactory Pro trial version www.pdffactory.com

κρυπτογραφικών κλειδιών (key generation systems) καθώς και των τελικών φορέων τους που συνήθως είναι μια έξυπνη κάρτα (smart card) ή άλλη αντίστοιχη συσκευή (USB Token). Αντίστοιχα, για την επαλήθευση (verification) των ψηφιακών υπογραφών και τον έλεγχο της εγκυρότητας (validation) των σχετικών πιστοποιητικών, απαιτείται μια ανάλογη διάταξη, η οποία, εκτός του τερματικού επικοινωνίας του χρήστη και του κατάλληλου λογισμικού, θα πρέπει, επιπλέον, να διαθέτει και την δυνατότητα πρόσβασης - είτε με σύνδεση εντός δικτύου (on-line), είτε και με συχνές ενημερώσεις εκτός δικτύου (off-line) - σε επικαιροποιημένες πληροφορίες εγκυρότητας και ανάκλησης πιστοποιητικών τις οποίες δημοσιεύει ο εκάστοτε εκδότης (CSP) τους. Για τις διατάξεις επαλήθευσης υπογραφής η Οδηγία 99/93/ΕΚ συστήνει (ά.3§6) προς τα κράτη μέλη την συνεργασία τους για την ανάπτυξη συστημάτων τα οποία θα πρέπει να διασφαλίζουν τόσο την αξιοπιστία τους, όσο και την ορθή πληροφόρηση του επαληθεύοντα ως προς τα στοιχεία και τα αποτελέσματα της επαλήθευσης.

6.5 Πιστοποίηση της Ψηφιακής Υπογραφής

Στην Ευρώπη υπάρχουν κάποια αναγνωρισμένα σώματα τυποποίησης, μέσα στους σκοπούς που έχουν και τις διαδικασίες που πιστοποιούν έχουν και ως στόχο τους να τυποποιήσουν και θέματα που αφορούν την ψηφιακή υπογραφή. Η Ευρωπαϊκή Επιτροπή Τυποποίησης (European Committee for Standardisation – CEN) είναι ένα από τα αναγνωρισμένα ευρωπαϊκά σώματα τυποποίησης και καλύπτει το θέμα αυτό σε πεδία όχι ηλεκτροτεχνικά ή επικοινωνιακά.

Στον ταχύτατα μεταβαλλόμενο τομέα των Πληροφοριακών και Επικοινωνιακών Τεχνολογιών (Information and Communications Technologies – ICT), η CEN έχει δημιουργήσει το ISSS. Επιπροσθέτως στις παραδοσιακές τεχνικές επιτροπές της, το ISSS χρησιμοποιεί ανοιχτά εργαστήρια τα οποία δημιουργεί όπου υπάρχει κάποια αναγνωρισμένη ανάγκη και τα οποία είναι προσβάσιμα σε όλους τους ενδιαφερόμενους φορείς. Τα παραδοτέα τους εκδίδονται από τη CEN ως συμφωνίες των εργασιών (CEN Workshop Agreements – CWAs).

Οι εργασίες της CEN είναι υπεύθυνες για τον τομέα του προγράμματος EESSI που αφορά στα ποιοτικά και λειτουργικά πρότυπα για τη δημιουργία και επαλήθευση των ψηφιακών υπογραφών, καθώς και για τους CSP. Οι εργασίες κάτω από την EESSI περιλαμβάνουν τα εξής:

1. Τις απαιτήσεις ασφάλειας για αξιόπιστα συστήματα και προϊόντα
2. Τις απαιτήσεις ασφαλείας για τα συστήματα δημιουργίας των υπογραφών
3. Το περιβάλλον δημιουργίας των υπογραφών
4. Το περιβάλλον και τις διαδικασίες επαλήθευσης
5. Τον καθορισμό των προϊόντων και υπηρεσιών που συμμορφώνονται με τις απαιτήσεις του νέου συστήματος.

Το Ινστιτούτο Ευρωπαϊκών Τηλεπικοινωνιακών Προτύπων (European Telecommunications Institute – ETSI) είναι ένα ακόμα από τα ευρωπαϊκά σώματα τυποποίησης και παράγει ένα μεγάλο εύρος προτύπων και άλλης τεχνικής βιβλιογραφίας. Αποτελεί έτσι την Ευρωπαϊκή συμβολή στην παγκόσμια τυποποίηση στις τηλεπικοινωνίες και στα συναφή πεδία της εκπομπής (broadcasting) και της

PDF created with pdfFactory Pro trial version www.pdffactory.com

τεχνολογίας των πληροφοριών. Είναι ένας μη κερδοσκοπικός οργανισμός που εδρεύει στη Γαλλία και ενώνει σχεδόν 800 μέλη από 60 περίπου χώρες εντός και εκτός της Ευρώπης ενώ επιπλέον εκπροσωπεί κατασκευαστές, χειριστές δικτύων, διοικήσεις, παροχείς υπηρεσιών, ερευνητικούς οργανισμούς και χρήστες.

Εντός του ETSI, η Τεχνική Επιτροπή των Ηλεκτρονικών Υπογραφών και Υποδομών (Technical Committee for Electronic Signatures and Infrastructures – TCESI), έχει ως αντικείμενο τις σχετικές με την ψηφιακή υπογραφή διεργασίες. Οι ευθύνες του κάτω από την EESSI περιλαμβάνουν:

1. Τη χρήση των πιστοποιητικών του κοινού κλειδιού X.509 ως εγκεκριμένων

2. Την ασφάλεια και την πολιτική πιστοποίησης των CSP που δίνουν αναγνωρισμένα πιστοποιητικά

3. Τη σύνταξη των ηλεκτρονικών υπογραφών και τα μορφότυπα κωδικοποίησης καθώς και άλλες τεχνικές πλευρές της σχετικής πολιτικής

4. Το πρωτόκολλο για τη διαλειτουργικότητά με την υπηρεσία χρονοσήμανσης

5. Την ασφάλεια και την πολιτική πιστοποίησης των CSP που δίνουν μη αναγνωρισμένα πιστοποιητικά

6. Την ασφάλεια και την πολιτική των απαιτήσεων για τους CSP που εκδίδουν χρονοσήμαντρα

7. Τη σύνταξη των ηλεκτρονικών υπογραφών και τα μορφότυπα κωδικοποίησης σε XML

8. Τις πολιτικές υπογραφών για εκτεταμένα μοντέλα εργασιών

9. Την εναρμονισμένη παροχή πληροφοριών για την κατάσταση των CSP

Με την λήψη ενός μηνύματος με ψηφιακή υπογραφή, ο παραλήπτης επαληθεύοντας την ψηφιακή υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης, όμως, πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε.

Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί.

Η Πάροδος Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι ο «οργανισμός» που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο ΠΥΠ πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Κύριος τύπος ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificate). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και

PDF created with pdfFactory Pro trial version www.pdffactory.com

επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι εν ολίγοις ένα διαβατήριο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του ΠΥΠ, ο οποίος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου.

Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο ΠΥΠ δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου. Όπως αναφέρθηκε και πιο πάνω λοιπόν, οι ΠΥΠ εκδίδουν τα πιστοποιητικά με στόχο τη συσχέτιση του δημόσιου κλειδιού με τον δικαιούχο του, προβαίνοντας παράλληλα και στην οργάνωση μιας αξιόπιστης «Υποδομής Δημόσιου Κλειδιού», (PKI Public Key Infrastructure) για την έκδοση, διάθεση και διαχείριση των σχετικών πιστοποιητικών.

Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα. Αποτελεί μια ψηφιακή «ετικέτα» η οποία επισυνάπτεται στα προς υπογραφή δεδομένα.

Η χρησιμοποίησή της ψηφιακής υπογραφής (έτσι όπως αυτή ρητά περιγράφεται στο Π.Δ.150/2001) μέσω του δημόσιου κλειδιού σε συνδυασμό με το παρεχόμενο πιστοποιητικό, θα αποτελεί την τεχνολογικά και νομικά προκρινόμενη λύση για την εξασφάλιση της αποδειξιμότητας της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας μιας υπογραφής. Αρμόδια αρχή για την πιστοποίηση είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ). Η οποία διαπιστώνει αν οι εταιρείες που παρέχουν υπηρεσίες πιστοποίησης, αλλά και βεβαιώσεις για την ασφάλεια της ψηφιακής υπογραφής, λειτουργούν με τέτοια υποδομή και κανόνες ώστε να είναι σε θέση να παρέχουν υπηρεσίες πιστοποίησης της ψηφιακής υπογραφής. Σε μια τέτοια περίπτωση η ΕΕΤΤ μπορεί να τους παρέχει τη δυνατότητα να αναθέτουν και σε τρίτους το έργο αυτό.

Βασικοί στόχοι είναι:

α) η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει,

β) η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και

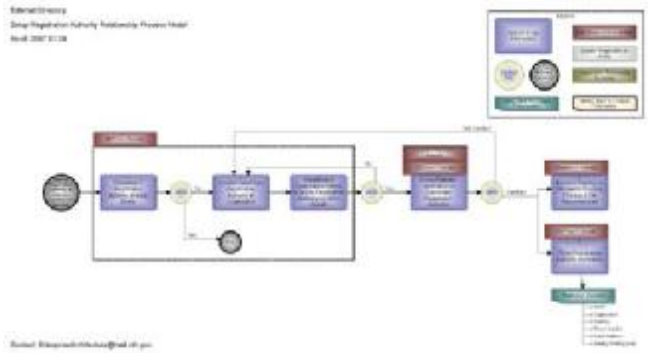
γ) η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί την συμβολή του στην εν λόγω συναλλαγή.

Σε αντιδιαστολή με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ηλεκτρονικής υπογραφής διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα αφού προκύπτει με βάση και αυτά. Συνοπτικά θα μπορούσαμε να παρουσιάσουμε τις υπηρεσίες των Παροχών Πιστοποίησης (ΠΥΠ) ως εξής:

1. **Υπηρεσία Εγγραφής-Καταχώρησης** (Registration Authority – RA), η οποία ελέγχει τη ταυτότητα των υποκειμένων και συλλέγει τα σχετικά αποδεικτικά στοιχεία - πιθανώς συνεπικουρούμενη από εξουσιοδοτημένες

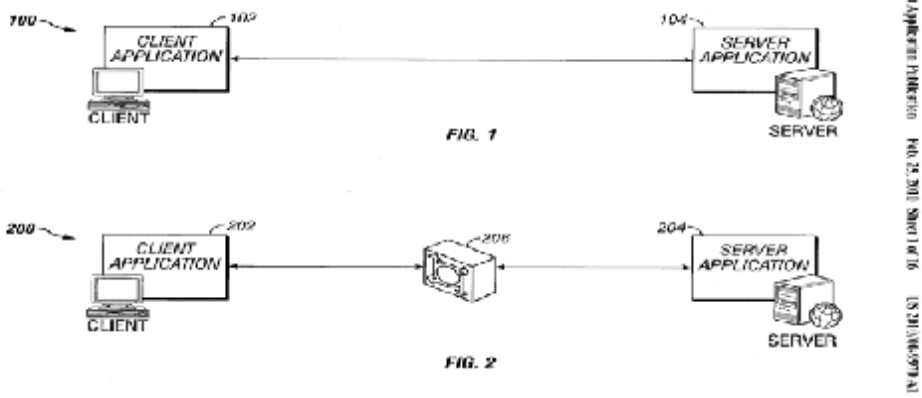
PDF created with pdfFactory Pro trial version www.pdffactory.com

Τοπικές Υπηρεσίες Υποβολής (Local Registration Authorities – LRA) - πριν να δώσει την έγκρισή της για την έκδοση των σχετικών πιστοποιητικών,



Εικόνα 16.Υπηρεσία Εγγραφής-Καταχώρησης (Registration Authority – RA)

2. **Υπηρεσία Έκδοσης Πιστοποιητικών** (Certification Authority – CA), που εκδίδει (σύμφωνα με τις αιτήσεις της Υπηρεσίας Εγγραφής) και υπογράφει τα τελικά πιστοποιητικά των υποκειμένων και η οποία πιθανότατα χρησιμοποιεί περισσότερους από ένα λειτουργικούς ή ουσιαστικούς υποεκδότες (Sub-CAs) - με διαφορετικά πιστοποιημένα (από τον Root CA ή άλλον ενδιάμεσο Sub-CA) κλειδιά - για την υπογραφή των πιστοποιητικών των συνδρομητών,



Εικόνα 17.Υπηρεσία Έκδοσης Πιστοποιητικών (Certification Authority – CA)

3. **Υπηρεσία Διαχείρισης Αιτημάτων Ανάκλησης** (Revocation Management Service), η οποία υποδέχεται, ελέγχει (σε συνεργασία με την Υπηρεσία Εγγραφής) και διεκπεραιώνει τα αιτήματα - σε 24ωρη βάση, 7 ημέρες την εβδομάδα - για ανάκληση, παύση ή επανενεργοποίηση των πιστοποιητικών, συνεργαζόμενη με την Υπηρεσία Έκδοσης Πιστοποιητικών

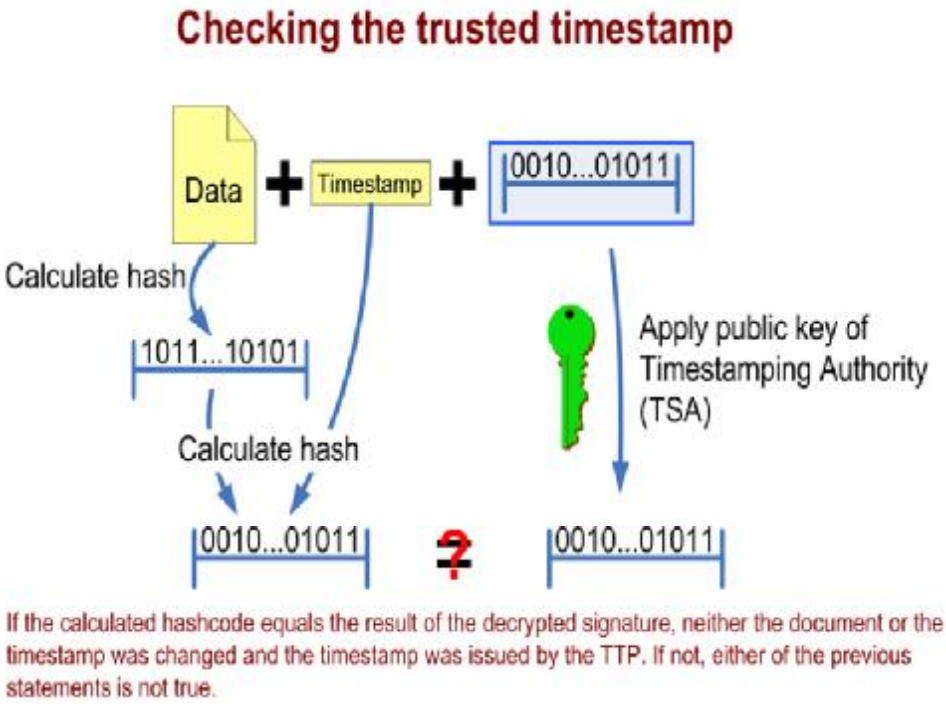
PDF created with pdfFactory Pro trial version www.pdffactory.com

για την κατάλληλη (ψηφιακή) υπογραφή των σχετικών εκδιδόμενων Λιστών Ανακληθέντων Πιστοποιητικών (Certificate Revocation Lists ή CRL),

4. Υπηρεσία Δημοσίευσης (Dissemination & Revocation Status Service), η οποία αναλαμβάνει την δημοσίευση των κειμένων τεκμηρίωσης των υπηρεσιών του CSP (πιθανότατα με την χρήση μιας ηλεκτρονικής τοποθεσίας – Repository), την δημοσίευση των Καταλόγων και των Λιστών Ανακληθέντων Πιστοποιητικών, καθώς και σχετικές ενημερώσεις ή κοινοποιήσεις προς τους συνδρομητές του CSP.

5. Υπηρεσίες Προμήθειας-Προετοιμασίας Φορέα (π.χ. έξυπνη κάρτα ή USB token) για τους συνδρομητές (Subject Device Provision Service),

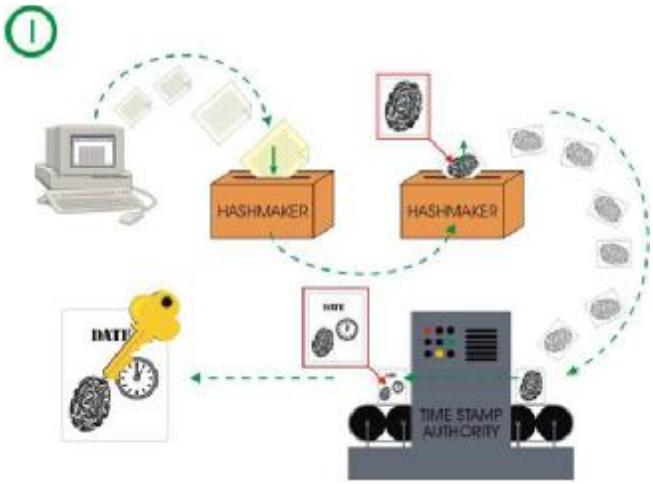
6. Υπηρεσίες Χρονοσήμανσης ηλεκτρονικών εγγράφων (Time-Stamping Authority – TSA),



Εικόνα 189. Υπηρεσίες Χρονοσήμανσης ηλεκτρονικών εγγράφων (Time-Stamping Authority – TSA)

7. Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων (Attribute Authority), Υπηρεσίες Ασφαλούς Αρχειοθέτησης εγγράφων (καλούμενες συχνά και ως Notary Services) κ.τ.λ..

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 19. Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων (Attribute Authority), Υπηρεσίες Ασφαλούς Αρχειοθέτησης εγγράφων

Συνοπτικά θα μπορούσαμε να παρουσιάσουμε τις υποχρεώσεις των Παροχών Πιστοποίησης (ΠΥΠ):

1. Αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης,
2. Ασφάλεια και άμεσες υπηρεσίες καταλόγου και ανάκλησης,
3. Επαλήθευση ταυτότητας του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό
4. Λήψη μέτρων έναντι της πλαστογράφησης πιστοποιητικών
5. Καταγραφή των πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό για χρονικό διάστημα τριάντα ετών,
6. Να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου που παρέχουν υπηρεσίες διαχείρισης κλειδιών
7. Ενημέρωση σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού

Να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών

6.6 Ψηφιακές Υπογραφές – Υδατογραφήματα (watermarks)

[10]Η ραγδαία εξάπλωση και ευρύτατη διείσδυση του Διαδικτύου (Internet) σε ποικίλους χώρους της κοινωνικής δραστηριότητας είχε σαν αποτέλεσμα την ανάπτυξη συνόλου μηχανισμών προστασίας για τη διαφύλαξη της ασφάλειας των συναλλαγών, της κατοχύρωσης των πνευματικών δικαιωμάτων στα διακινούμενα ψηφιακά αντικείμενα. Εκτός από τις ψηφιακές υπογραφές και την κρυπτογραφία έννοιες όπως η στεγανογραφία, η υδατογράφηση αναφέρονται στη βιβλιογραφία ως μέθοδοι προστασίας των πνευματικών δικαιωμάτων στον ψηφιακό κόσμο. Κρίθηκε λοιπόν απαραίτητη, για την αποφυγή συγχύσεων η συνοπτική παράθεση των τεχνικών αυτών, και η αποσαφήνιση πιθανών μεταξύ τους διαφορών.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Η στεγανογραφία επιτρέπει την κρυφή επικοινωνία, συνήθως κρύβοντας τις πληροφορίες σε άλλα δεδομένα υπεράνω υποψίας. Βασίζεται στην υπόθεση ότι η ύπαρξη κρυφής επικοινωνίας είναι άγνωστη σε τρίτους και χρησιμοποιείται κυρίως στην κρυφή σημείο-προς-σημείο επικοινωνία ανάμεσα σε έμπιστα μέρη. Ως εκ τούτου, οι κρυφές πληροφορίες δε μπορούν να ανακτηθούν μετά από παραποίηση των δεδομένων.

Σε αντίθεση με την κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει την πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Συμπερασματικά, θα μπορούσαμε να αναφέρουμε ότι η στεγανογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντάς την μέσα σε κάποιο "στεγανό". Η κρυπτογραφία εξασφαλίζει ότι η πληροφορία που θα διαβαστεί από μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη και ακατανόητη ή παραπλανητική. Η κρυπτογραφία επίσης, προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο.

Η υδατογράφηση (watermarking) έχει την ιδιότητα προστασίας του περιεχομένου και μετά την αποκρυπτογράφηση του, τοποθετώντας την πληροφορία μέσα στο περιεχόμενο, απ᾽ όπου δεν αφαιρείται ποτέ κατά την κανονική χρήση. Ακόμα κι αν η ύπαρξη κρυφών πληροφοριών είναι γνωστή, είναι δύσκολο -ιδανικά αδύνατο- να καταστραφεί το ένθετο υδατογράφημα.

PDF created with pdfFactory Pro trial version www.pdffactory.com

7. Ηλεκτρονικά Έγγραφα και Ηλεκτρονικές Υπογραφές

[8]Τα έγγραφα που αποθηκεύονται στη μνήμη η/υ και διακινούνται ηλεκτρονικά, δηλ. τα ηλεκτρονικά έγγραφα , παρουσιάζουν μια σειρά από μειονεκτήματα όπως ότι στερούνται της σταθερότητας κατά την ενσωμάτωσή τους και μπορεί να υποστούν μετατροπές, αλλοιώσεις ή διαγραφές που είναι αδύνατον να εντοπιστούν, αλλά και δεν διαθέτουν την ιδιόχειρη υπογραφή που είναι απαραίτητη στα έγγραφα όπου ο τύπος είναι συστατικός. Επιπλέον, όταν διακινούνται μέσω ανοικτών δικτύων υπάρχει ο κίνδυνος να υποκλαπούν αυτά από τρίτους και να αλλοιωθεί ή τροποποιηθεί το περιεχόμενό τους.

Ειδικά δε όσον αφορά τα έγγραφα που διακινούνται ηλεκτρονικά, παρατηρείται ότι είναι δυσχερής η ακριβής εξακρίβωση της ταυτότητας του αποστολέα (συντάκτη) των εγγράφων, όπως και της αυθεντικότητας και της μη αλλοίωσης τους. Για την πλήρη αξιοποίηση των δυνατοτήτων που προσφέρει η σύγχρονη τεχνολογία απαιτείται, συνεπώς , η ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών και προς τούτο χρησιμοποιούνται μέθοδοι κρυπτογράφησης που εξασφαλίζουν την ασφαλή μεταφορά δεδομένων η/υ μέσω ανοιχτών δικτύων.

Για την εξασφάλιση της γνησιότητας των εγγράφων που διακινούνται ηλεκτρονικά χρησιμοποιείται ειδικότερα, η τεχνολογία της ηλεκτρονικής υπογραφής. Δύο είναι δε οι κυριότεροι τύποι συστημάτων κρυπτογράφησης που χρησιμοποιούνται για την παραγωγή της ηλεκτρονικής υπογραφής, το συμμετρικό κρυπτογραφικό σύστημα και το ασύμμετρο κρυπτογραφικό σύστημα. Τα συμμετρικά συστήματα, τα συστήματα δηλ. που χρησιμοποιούν συμμετρικούς αλγόριθμους, όπως είναι λ.χ. τα συστήματα δηλ. που χρησιμοποιούν συμμετρικούς αλγόριθμους, όπως είναι λ.χ. το σύστημα DES(Data Encryption Standard), έχουν ένα κοινό κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση το οποίο είναι γνωστό στον αποστολέα και στον παραλήπτη του μηνύματος μόνο και πρέπει να παραμένει μυστικό. Η τεχνολογία αυτή είναι κατάλληλη επομένως μόνο για κλειστές ομάδες χρηστών και όχι για συναλλαγές, στις οποίες μετέχει ένας μεγάλος αριθμός συναλλασσομένων.

Τα συστήματα που χρησιμοποιούν ασύμμετρους αλγόριθμους- ή συστήματα δημοσίου κλειδιού(διαδικασία RSA)- για την θέση της ηλεκτρονικής υπογραφής εφαρμόζουν ένα συνδυασμό δημόσιου και μυστικού κλειδιού. Ο αποστολέας ενός μηνύματος χρησιμοποιεί το μυστικό, ιδιωτικό κλειδί(private key) για την κρυπτογράφησή του. Ο συνδυασμός αυτός του μηνύματος με το μυστικό κλειδί αποτελεί την ηλεκτρονική ή ψηφιακή υπογραφή του αποστολέα. Ο αποδέκτης του μηνύματος αποκρυπτογραφεί στη συνέχεια το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί (public key) η κλειδί αποκρυπτογράφησης. Η διαδικασία αυτή είναι πιο πρόσφορη για ανοιχτά δίκτυα, όπως είναι το Internet αλλά δεν είναι κατάλληλη για την μεταβίβαση εκτενών μηνυμάτων λόγω του ότι είναι χρονοβόρα (τα συστήματα DES χρησιμοποιούν κλειδιά με μήκος 56 bit, ενώ τα συστήματα RES χρησιμοποιούν κλειδιά με μήκος 1024 bits).

[14]Πιο πρόσφορη για την αποστολή εκτενών μηνυμάτων είναι η διαδικασία (επίσης δημοσίου κλειδιού η ασύμμετρη), κατά την οποία δημιουργείται το «δακτυλικό αποτύπωμα» του εγγράφου, δηλ εξάγεται το άθροισμα των bits (data digest), από τα οποία αποτελείται το κείμενο με μια διαδικασία hashing και στην

PDF created with pdfFactory Pro trial version www.pdffactory.com

συνέχεια κρυπτογραφείται με την μέθοδο RSA. Ο αποστολέας κρυπτογραφεί έτσι, την περίληψη αυτή του εγγράφου , μαζί με άλλα πρόσθετα δεδομένα, όπως είναι π.χ. ο τόπος και η ημερομηνία της υπογραφής , χρησιμοποιώντας το ιδιωτικό (μυστικό) κλειδί. Ο αποδέκτης χρησιμοποιεί το δημόσιο κλειδί για την αποκρυπτογράφηση του δακτυλικού αποτυπώματος , το οποίο και εξάγει με τη βοήθεια κατάλληλου λογισμικού, ώστε να διαπιστώσει εάν το περιεχόμενο του έχει παραμείνει αναλλοίωτο (επαλήθευση υπογραφής).

Επίσης, πρέπει να αναφερθεί και το σύστημα του «ψηφιακού φάκελου» (digital envelope), το οποίο συνδυάζει τα συστήματα συμμετρικών και ασύμμετρων αλγόριθμων. Κατά τη μέθοδο αυτή, το έγγραφο κρυπτογραφείται από τον αποστολέα, με ένα συμμετρικό αλγόριθμο και με τη χρήση ενός σύντομου, αλλά ασφαλούς κλειδιού, 128 bits, το οποίο καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και για αυτό ονομάζεται κλειδί συνεδρίας (session key). Το κλειδί αυτό για την ασφάλεια κρυπτογραφείται με ένα ασύμμετρο αλγόριθμο. Έτσι, ο παραλήπτης του εγγράφου θα πρέπει να πρώτα να αποκρυπτογραφήσει το κλειδί με το δημόσιο και στη συνέχεια και το μήνυμα.

7.1 Ρυθμίσεις του π.δ. 150/2001

[6]Με το π.δ. 150/2001, το οποίο εκδόθηκε σε συμμόρφωση προς την κοινοτική οδηγία 1999/93, αναγνωρίζονται οι τεχνολογίες ηλεκτρονικής υπογραφής καθορίζονται οι έννομες συνέπειες τους και ρυθμίζεται η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών[1] .Ως ηλεκτρονική υπογραφή νοούνται τα «δεδομένα σε ηλεκτρονική μορφή , τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτό και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (άρθρο 2 αριθ. 1 π.δ 150/2001). Από τον ορισμό αυτό γίνεται σαφές ότι στην έννοια της ηλεκτρονικής υπογραφής εμπίπτουν οι τεχνικές κρυπτογράφησης, με τις οποίες κρυπτογραφείται όλο ή τμήμα του ηλεκτρονικού εγγράφου. Για το σκοπό αυτό χρησιμοποιείται μια διάταξη δημιουργίας υπογραφής (άρθρο 2 αριθ 5), δηλ κατάλληλο λογισμικό , και κλειδιά κρυπτογράφησης που ορίζονται ως δεδομένα επαλήθευσης υπογραφής (άρθρο 2 αριθ 7).

Η προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή , σύμφωνα με την ορολογία του π.δ. 150/2001, εξομοιώνεται με την ιδιόχειρη υπογραφή. Ειδικότερα, σύμφωνα με το άρθρο 3 , § 1 , η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο και στο δικονομικό δίκαιο.

Ως «προηγμένη ηλεκτρονική υπογραφή» ορίζεται η ηλεκτρονική υπογραφή, που πληροί τους εξής όρους :

- Συνδέεται μονοσήμαντα με τον υπογράφοντα

[1] Βλ. Iglezakis, Regulation of Electronic Signatures, σε: Cyber law in Hellas, σελ. 175 επ. Ε. Τρουλινού, Το Προεδρικό Διάταγμα 150/2001. Μια χαμένη ευκαιρία για ρύθμιση των ηλεκτρονικών υπογραφών από τον Έλληνα νομοθέτη;, ΔΕΕ 2001, σελ 1234 επ. Ι. Λιναρίτη, Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 της ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο με το ΠΔ 150/2001, ΔΕΕ 2002, σελ. 257 επ. Δ. Ζέκου, Ιδιόχειρες ηλεκτρονικές υπογραφές και ηλεκτρονικές συμβάσεις, ΔΕΕ 2004, σελ.627 επ. Καραδημητρίου, Ηλεκτρονικές Υπογραφές : Προβλήματα και σκέψεις με αφορμή το π.δ 150/2001 ,Αρμ 2002, σελ 1535 επ. Σ. Βασιλοπούλου, Ηλεκτρονική Υπογραφή, σε : Β. Δούβλη/Α.Μπώλου , Δίκαιο προστασίας καταναλωτών , 2008 , σελ 720 επ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

- 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 εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων (άρθρο 2 αριθ 2).

[15]Επιπρόσθετα, πρέπει η προηγμένη ηλεκτρονική υπογραφή να βασίζεται σε αναγνωρισμένο πιστοποιητικό και να δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής. Οι όροι αυτοί εξειδικεύονται στα παραρτήματα που συνοδεύουν το προεδρικό διάταγμα.

Ειδικότερα, σύμφωνα με το Παράρτημα 1 του π.δ. 150/2001, τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν : α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, β) τα στοιχεία αναγνώρισης του παροχέα υπηρεσιών πιστοποίησης και το κράτος , στο οποίο είναι εγκατεστημένος , γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με ον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος , στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού, η) την προηγμένη ηλεκτρονική υπογραφή του παροχέα των υπηρεσιών πιστοποίησης που το εκδίδει , θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και ι) τυχόν όρια των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

Περαιτέρω, σύμφωνα με το Παράρτημα ΙΙΙ του π.δ. 105/2001, οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον ότι: α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσία, μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο, β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας, γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους. Ακόμα, προβλέπεται ότι οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν μεταβάλλουν τα προς υπογραφή δεδομένα ούτε εμποδίζουν την υποβολή των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

Από τα παραπάνω γίνεται σαφές ότι μόνο τεχνολογίες ηλεκτρονικής υπογραφής που βασίζονται στο ασύμμετρο σύστημα κρυπτογράφησης πληρούν τις προϋποθέσεις για να θεωρηθούν ως προηγμένες υπογραφές, ενώ σαφώς δεν τις πληρούν τα συμμετρικά συστήματα που χρησιμοποιούν ένα μόνο κλειδί, το οποίο δεν μπορεί να παραμείνει μυστικό. Η εξομοίωση της προηγμένης ηλεκτρονικής με την ιδιόχειρη υπογραφή σημαίνει ότι όπου προβλέπεται έγγραφος τύπος από το νόμο ή από τη συμφωνία των μερών, το ηλεκτρονικό έγγραφο με την ηλεκτρονική υπογραφή επέχει θέση ιδιωτικού εγγράφου με την έννοια του άρθρο 443 ΚΠολΔ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Παραπέρα, σύμφωνα με το άρθρο 3 § 2 π.δ. 150/2001, σε περίπτωση όπου η ηλεκτρονική υπογραφή δεν είναι προηγμένη ή δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, η ισχύς της ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο τον λόγο αυτό. Η διάταξη αυτή έχει ερμηνευτικό χαρακτήρα και δεν καθορίζει τις έννομες συνέπειες της απλής ηλεκτρονικής υπογραφής, με συνέπεια να εξακολουθεί να παραμένει ζητούμενο η εξακρίβωση της νομικής ισχύος της απλής ηλεκτρονικής υπογραφής.

Κατά την άποψής μας, η «απλή» ηλεκτρονική υπογραφή μπορεί να παρέχει τα εχέγγυα για την εγκυρότητα των συμβάσεων, για τις οποίες δεν προβλέπεται έγγραφος τύπος, αφού κανόνας είναι το άτυπο των δικαιοπραξιών, σύμφωνα με την ΑΚ 158. Επιπλέον, το έγγραφο που φέρει απλή ηλεκτρονική υπογραφή μπορεί να χρησιμοποιηθεί ως αποδεικτικό έγγραφο κατά το άρθρο 444 αριθ. 3 ΚΠολΔ, καθ' σον εμπίπτει ευχερώς στην έννοια της μηχανικής απεικόνισης. Ασφαλώς, όμως, δεν δύναται να εξομοιωθεί με την ιδιόχειρη υπογραφή, αφού άτι τέτοιο θα αντέβαινε στο νόμο και πιο συγκεκριμένα, στο άρθρο 3 § 1 του π.δ. 150/2001, και συνεπώς, δεν δύναται να χρησιμοποιηθεί ως υποκατάστατο της ηλεκτρονικής υπογραφής σε δικαιοπραξίες όπου ο έγγραφος τύπος είναι συστατικός.

Όσον αφορά τα ηλεκτρονικά έγγραφα που δεν φέρουν κανενός είδος ηλεκτρονική υπογραφή, α απόδειξη της γνησιότητας τους καθίσταται δυνατή, καταρχήν με την βοήθεια των διδαγμάτων των κοινής πείρας κατά την εφαρμογή της μεθόδου της έμμεσης δια τεκμηρίων απόδειξης (άρθρο 36 § 3 ΚΠολΔ), χωρίς να αποκλείεται και η θεώρηση τους ως μηχανικών απεικονίσεων κατ' άρθρο 444 αριθ. 3 ΚΠολΔ.

Στην Ελληνική νομολογία αναγνωρίζεται η αποδεικτική αξία των ηλεκτρονικών εγγράφων που περιέχονται σε μηνύματα ηλεκτρονικής αλληλογραφίας και δεν φέρουν ηλεκτρονική υπογραφή, τα οποία εντάσσονται στην παραπάνω κατηγορία ηλεκτρονικών εγγράφων. Πιο συγκεκριμένα, έγινε δεκτό ότι η εκτύπωση των ηλεκτρονικών εγγράφων και των ηλεκτρονικών επιστολών (e-mails) μπορεί να θεωρηθεί ως μηχανική απεικόνιση, η οποία εμπίπτει στην έννοια του ιδιωτικού εγγράφου με αποδεικτική δύναμη.

Το π.δ. 150 /2001 ρυθμίζει, περαιτέρω, την παροχή υπηρεσιών πιστοποίησης. Αυτές παρέχονται από «παροχείς υπηρεσιών πιστοποίησης» οι οποίοι μπορεί να είναι φορείς, φυσικά ή νομικά πρόσωπα, με αρμοδιότητα να εκδίδουν πιστοποιητικά ή να παρέχουν άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές. Τα παροχείς που εκδίδουν οι παροχείς υπηρεσιών πιστοποίησης είναι ηλεκτρονικές βεβαιώσεις που συνδέουν δεδομένα επαλήθευσης απογραφής με ένα άτομο και επιβεβαιώνουν έτσι την ταυτότητα του (άρθρο 2 αριθ 9). Οι παροχείς υπηρεσιών πιστοποίησης τελούν υπό την εποπτεία της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και πρέπει να συμμορφώνονται με τους όρους που προβλέπονται στην υπ' αριθ 248/71. Απόφαση της ΕΕΤΤ («Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής»).

Σύμφωνα με το παράρτημα ΙΙ του π.δ. 150/2001, μεταξύ άλλων, οι παροχείς υπηρεσιών πιστοποίησης πρέπει να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης , σύμφωνα με τα εκάστοτε ισχύοντα κριτήρια, να καταγράφουν τις αναγκαίες πληροφορίες, ώστε να ελέγχουν τη γνησιότητα των πιστοποιητικών και το χρόνο έκδοσης ή ανάκλησης τους και να προβαίνουν σε επαλήθευση της ταυτότητας του κατόχου του πιστοποιητικού. Οι παροχείς που

PDF created with pdfFactory Pro trial version www.pdffactory.com

εκδίδουν αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυώνται για την ακρίβεια ενός τέτοιου πιστοποιητικού, ευθύνονται έναντι τρίτου για τη ζημία που προκλήθηκε σε βάρος του κα ι η ευθύνη αυτή καθορίζεται στο νόμο ως νόθος αντικειμενική, καθ' όσον προβλέπεται ότι ο παροχέας δεν ευθύνεται, αν αποδείξει ότι δεν τον βαρύνει πταίσμα (άρθρο 6 § 3 π.δ. 150/2001).

Η συλλογή προσωπικών δεδομένων κατά την έκδοση πιστοποιητικού πρέπει να περιορίζεται στο απολύτως απαραίτητο μέτρο. Συγκεκριμένα, ορίζεται ότι παροχείς υπηρεσιών πιστοποίησης συγκεντρώνουν προσωπικά δεδομένα μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή ρητή συγκατάθεση του και μόνο εφόσον είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού, ενώ η συλλογή ή επεξεργασία δεδομένων για άλλους σκοπούς απαγορεύεται , χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου.(άρθρο 7).

7.2 Η Ηλεκτρονική Υπογραφή στο Δημόσιο Δίκαιο

[13]Η χρήση της ηλεκτρονικής υπογραφής στον δημόσιο τομέα ρυθμίζεται από τον νόμο 2672/1998 και το άρθρο 14 , που αφορά τη διακίνηση εγγράφων μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α. ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων, νομικών προσώπων ιδιωτικού δικαίου και ενώσεων προσώπων, με τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο. Στην ίδια διάταξη δίδεται ο ορισμός της ψηφιακής υπογραφής, ο οποίος αντιστοιχεί στον ορισμό της προηγούμενης ηλεκτρονικής υπογραφής της οδηγίας 1999/93/ΕΚ.

Σύμφωνα με την παρ. 1 του παραπάνω άρθρου, ορίζεται ότι επιτρέπεται η διακίνηση εγγράφων μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των οργανισμών τοπικής αυτοδιοίκησης ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων με τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο.

Παραπέρα, παρέχεται εξουσιοδότηση στη Διοίκηση για τον καθορισμό των προϋποθέσεων και της διαδικασία έκδοσης, διακίνησης και διασφάλισης της ψηφιακής υπογραφής, οι προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, καθώς και οι τεχνικοί κανόνες για την παραγωγή της ηλεκτρονικής υπογραφής, όπως και η επέκταση της διακίνησης των μηνυμάτων ηλεκτρονικού ταχυδρομείου σε κατηγορίες εγγράφων που θα καθορισθούν (§ 19,20).

Όσον αφορά τη νομική ισχύ των μηνυμάτων ηλεκτρονικής αλληλογραφίας που φέρει ψηφιακή υπογραφή, ορίζεται ότι η τελευταία επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής, κατά την κείμενη νομοθεσία (§ 22). Ακόμα , προβλέπεται ότι το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή έχει την αποδεικτική ισχύ έγγραφου κατά τον ΚΠολΔ.

Με βάση την προβλεπόμενη εξουσιοδότηση εκδόθηκε το π.δ. 342/2002, το οποίο βασίζεται στο π.δ. 150.2001 όσον αφορά τους ορισμούς , τη λειτουργία και τις έννομες συνέπειες της ψηφιακής υπογραφής. Στην παρ. 1 του π.δ. 342/2002 ορίζεται ότι, αποφάσεις , πιστοποιητικά και βεβαιώσεις, διακινούνται με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ και των Ο.Τ.Α., μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, εφόσον φέρουν ψηφιακή υπογραφή. Περαιτέρω, στην παρ. 2 ορίζεται ότι η διακίνηση των 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., μεταξύ αυτών

PDF created with pdfFactory Pro trial version www.pdffactory.com

και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή έννομων αποτελεσμάτων ή με την άσκηση δικαιώματος.

Αξίζει να αναφερθεί ότι η τεχνολογία της υποδομής δημοσίου κλειδιού προωθείται στα πλαίσια του έργου «Εθνικού δικτύου δημόσιας διοίκησης – σύζευξις». Η εν λόγω υποδομή έχει στόχο να παρέχει τη δυνατότητα στα στελέχη του Δημοσίου να υπογράφουν ψηφιακά ηλεκτρονικά έγγραφα που αποστέλλουν ηλεκτρονικά και τις συναλλαγές που καταρτίζουν, χρησιμοποιώντας έξυπνες κάρτες που εμπεριέχουν δύο ψηφιακά πιστοποιητικά. Από αυτά το ένα χρησιμοποιείται για να υπογράψει ηλεκτρονικά τα έγγραφα και το δεύτερο είναι ένα ψηφιακό πιστοποιητικό. Αντίστοιχη υποδομή θα αναπτυχθεί στο πλαίσιο του έργου «Εθνική Κεντρική Διαδικτυακή Πύλη – Ερμής », η οποία θα αξιοποιηθεί τις ηλεκτρονικές συναλλαγές των πολιτών και επιχειρήσεων με τις δημόσιες υπηρεσίες.

Για την υποστήριξη της υποδομής δημοσίου κλειδιού διαμορφώθηκε το κατάλληλο οργανωτικό και θεσμικό πλαίσιο. Ειδικότερα, θεσμοθετήθηκε η αρχή πιστοποίησης του Ελληνικού Δημοσίου ως πρωτεύουσα αρχή πιστοποίησης (Root CA),σύμφωνα με το άρθρο 20 ν. 3448/2007, όπως τροποποιήθηκε από το άρθρο 25 ν. 3536/2007 , και ως τέτοια ορίσθηκε η Υπηρεσία Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης & Ηλεκτρονικής Διακυβέρνησης του Υπουργείου Εσωτερικών , Δημόσιας Διοίκησης και Αποκέντρωσης. Ο Κανονισμός Πιστοποίησης της παραπάνω αρχής εγκρίθηκε από την Ε.Ε.Τ.Τ. και κυρώθηκε με την Υ.Α 2512οικ/18-10-2006.

7.3 Τυποποίηση των προϊόντων ηλεκτρονικών υπογραφών

[14]Σημαντικός παράγοντας για την εξέλιξη της τεχνολογίας των ηλεκτρονικών υπογραφών αποτελεί η ύπαρξη πρότυπων που έχουν εκδοθεί από Ευρωπαϊκούς η διεθνούς οργανισμούς τυποποίησης. Η οδηγία 1999/93 παρέχει τη δυνατότητα στην Ευρωπαϊκή Επιτροπή να καθορίζει και να δημοσιεύει αριθμούς αναφοράς «γενικώς αναγνωρισμένων προτύπων» για προϊόντα ηλεκτρονικής υπογραφής . Η ανταπόκριση ενός τέτοιου προϊόντος με τα εν λόγω πρότυπα έχει ως συνέπεια να τεκμαίρεται η συμμόρφωση του με τις απαιτήσεις του παραρτήματος || στοιχ. Στ' και του παραρτήματος ||| της οδηγίας, τα οποία ενσωματώνονται στο π.δ. 150/2001.

Μετά από εντολή της Επιτροπής προς τον Ευρωπαϊκό οργανισμό τυποποίησης (CEN) συγκροτήθηκε η Ευρωπαϊκή Πρωτοβουλία τυποποίησης της Ηλεκτρονικής υπογραφής (EESI) , η οποία αποτελούνται από μέλη των οργανισμών CEN και ETSI και η οποία εκπόνησε πρότυπα για προϊόντα και υπηρεσίες ηλεκτρονικής υπογραφής.

Συνακόλουθα, η Επιτροπή εξέδωσε της Απόφαση της 14ης Ιουλίου 2003, σχετικά με την δημοσίευση αριθμών αναφοράς γενικά αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής, σύμφωνα με την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1]. Η απόφαση αυτή αναφέρεται σε προϊόντα CEN (CWA) για τις προϋποθέσεις για τη δημιουργία αναγνωρισμένων ηλεκτρονικών υπογραφών[2]. Πέρα από αυτά, βεβαίως, μπορεί να καταρτισθούν και

[2] Η απόφαση περιλαμβάνει τα εξής πρότυπα : α)CWA 14167-1 (Μάρτιος 2003): security requirements for trustworthy systems managing certificates for electronic signatures , part 1 – system Security Requirements , β))CWA 14167-2 (Μάρτιος 2002) : security requirements for trustworthy systems managing certificates for electronic signatoures , part 2 –

PDF created with pdfFactory Pro trial version www.pdffactory.com

άλλα πρότυπα , τα οποία θα λαμβάνουν υπόψη τις τεχνολογικές εξελίξεις. Η συμμόρφωση με τις προϋποθέσεις που θέτει η οδηγία και το π.δ. 150/2001 μπορούν βεβαίως να πληρωθούν και με άλλα πρότυπα πέρα από τα εναρμονισμένα πρότυπα, τα οποία δημοσιεύονται στην Επίσημη Εφημερίδα της ΕΕ.

Cryptographic module for CSP signing operations και γ) CWA 14169 (Μάρτιος 2002): secure signature – creation devices

PDF created with pdfFactory Pro trial version www.pdffactory.com

8. Public Key Infrastructure (PKI)

[2]Το Internet σήμερα, αποτελεί ένα ιδιαίτερα ισχυρό επιχειρηματικό εργαλείο, το οποίο αποφέρει πολύτιμα οφέλη για τις επιχειρήσεις, όπως η παρουσίαση επιχειρηματικών δραστηριοτήτων, η εδραίωση νέων δεσμών με τους πελάτες σε μία παγκόσμια αγορά, η αύξηση της παραγωγικότητας και η μείωση του λειτουργικού κόστους. Όμως, σε ένα τέτοιο ανταγωνιστικό και "μη ασφαλές" περιβάλλον, οι διακινούμενες πληροφορίες χρήζουν προστασίας, γιατί είναι άρρηκτα συνδεδεμένες με την ανάπτυξη μίας εταιρίας.

Η επιχειρηματική δραστηριότητα και η ιδιωτική επικοινωνία μέσα από δίκτυα υπολογιστών, μπορεί να διασφαλιστεί με το ηλεκτρονικό ισοδύναμο της υπογραφής ενός γράμματος και της σφράγισής του σε ένα φάκελο. Η πράξη της υπογραφής είναι απόδειξη αυθεντικότητας και μη αποποίησης ευθυνών, ενώ η πράξη της σφράγισης του φακέλου εγγυάται την εμπιστευτικότητα και την ακεραιότητα.

Το Public Key Infrastructure (PKI) είναι ένας αναδυόμενος χώρος της ασφάλειας πληροφορικής. Βασίζεται στην χρήση του ψηφιακού πιστοποιητικού που έχει έννοια «ψηφιακού διαβατηρίου», για την παροχή υπηρεσιών ασφαλείας. Βασικός σκοπός του είναι να προσφέρει σε έναν οργανισμό, ένα πλαίσιο ηλεκτρονικής διαχείρισης που θα αντιμετωπίζει τις σημερινές λειτουργικές και νομικές ανάγκες, αλλά και τις απαιτήσεις σε ασφάλεια και εμπιστευτικότητα κατά τη μετάδοση και αποθήκευση δεδομένων.

8.1 Τεχνικές Κρυπτογράφησης

Χρησιμοποιώντας την τεχνική της συμμετρικής κρυπτογραφίας, ένα μήνυμα κρυπτογραφείται και αποκρυπτογραφείται με τη χρήση ενός μυστικού κλειδιού, παρέχοντας εμπιστευτικότητα στην επικοινωνία μεταξύ των κατόχων του κλειδιού αυτού. Πέρα από τα προβλήματα σχετικά με την ασφαλή διαχείριση και διανομή του μυστικού κλειδιού στα εμπλεκόμενα μέρη, ο σημαντικότερος περιορισμός αυτού του τύπου της κρυπτογράφησης ο οποίος τον καθιστά ανεπαρκή, είναι η έλλειψη απόδειξης για τη μη αποποίηση ευθυνών. Τις αδυναμίες αυτές, έρχεται να καλύψει η κρυπτογραφία δημοσίου κλειδιού με την ύπαρξη ενός ζεύγους κλειδιών, ενός δημόσιου και ενός ιδιωτικού, μαθηματικά συνδεδεμένων μεταξύ τους.

8.2 Ψηφιακή Υπογραφή

Στον ηλεκτρονικό κόσμο, η πιο σημαντική εφαρμογή της κρυπτογραφίας δημοσίου κλειδιού είναι η ψηφιακή υπογραφή, που αποτελεί και το υποκατάστατο της χειρόγραφης υπογραφής. Με τη βοήθεια του μυστικού κλειδιού, μία μόνο οντότητα μπορεί να "υπογράψει" ορισμένα δεδομένα, όπως για παράδειγμα ένα κείμενο, ενώ με το αντίστοιχο δημόσιο κλειδί δίνεται η δυνατότητα σε όλους να επιβεβαιώσουν την υπογραφή.

8.3 Ψηφιακό Πιστοποιητικό

Η γνησιότητα της υπογραφής, εξασφαλίζεται από το ότι μία μόνο οντότητα (φυσικό πρόσωπο, εταιρία, υπολογιστικό σύστημα) είναι ο πραγματικός κάτοχος ενός δημοσίου κλειδιού. Για το λόγο αυτό, κρίνεται αναγκαία η ύπαρξη μίας Τρίτης Έμπιστης Οντότητας που θα εγγυάται για την αυθεντικότητα ενός συγκεκριμένου

PDF created with pdfFactory Pro trial version www.pdffactory.com

δημόσιου κλειδιού. Την απαίτηση αυτή, έρχεται να καλύψει η ύπαρξη μίας ψηφιακής ταυτότητας, γνωστής και ως "ψηφιακό πιστοποιητικό», που δρα ως «ψηφιακό διαβατήριο».

Το πιστοποιητικό αυτό δεν είναι τίποτα περισσότερο από μία λίστα δεδομένων που περιλαμβάνει το όνομα της οντότητας στην οποία ανήκει, το δημόσιο κλειδί της και το όνομα της τρίτης έμπιστης οντότητας που εκδίδει το πιστοποιητικό. Η τρίτη έμπιστη οντότητα υπογράφει το πιστοποιητικό αυτό και έτσι κανείς δεν μπορεί να αμφισβητήσει την γνησιότητά του.

8.4 Αρχιτεκτονική PKI

[13]Η έκδοση ενός ψηφιακού πιστοποιητικού δεν είναι αρκετή, εάν απαιτείται η πλήρης αναπαραγωγή του παραδοσιακού τρόπου επιχειρηματικής δραστηριότητας στον ηλεκτρονικό κόσμο. Επιπρόσθετα, χρειάζονται:

- Πολιτικές ασφάλειας για να καθορίσουν τους κανόνες κάτω από τους οποίους τα συστήματα κρυπτογραφίας θα λειτουργούν.
- Προϊόντα για τη δημιουργία, την αποθήκευση και τη διαχείριση των κλειδιών.
- Διαδικασίες που θα υπαγορεύουν τον τρόπο με τον οποίο δημιουργούνται, διανέμονται και χρησιμοποιούνται τα κλειδιά και τα πιστοποιητικά.

Με άλλα λόγια, είναι επιβεβλημένη η ανάπτυξη μίας υποδομής δημοσίου κλειδιού γνωστής και ως Public Key Infrastructure (PKI). Μέσα από αυτό το πλαίσιο, επιτυγχάνονται οι τέσσερις βασικές υπηρεσίες ασφάλειας για τις επιχειρηματικές συναλλαγές:

- Εμπιστευτικότητα: για τη διατήρηση της μυστικότητας των πληροφοριών.
- Ακεραιότητα: για την αποτροπή της αλλοίωσης της πληροφορίας.
- Αυθεντικοποίηση: για την επικύρωση την ταυτότητας ενός χρήστη ή μίας εφαρμογής.
- Μη αποποίηση ευθυνών: για τη διασφάλιση ότι οι ψηφιακές συναλλαγές δεν θα μπορούν να αμφισβητηθούν.

Εκτός από το ψηφιακό πιστοποιητικό, θεμελιώδες συστατικό της αρχιτεκτονικής του PKI, ένας αριθμός εμπλεκομένων μερών συνιστούν το PKI. Πρωταρχική οντότητα είναι η Αρχή Πιστοποίησης (Certification Authority ή CA) που προσφέρει μία σειρά υπηρεσιών για τη διαχείριση κλειδιών, τη μη αποποίηση ευθυνών, τη χρονική σφράγιση αλλά και τη διαχείριση των ψηφιακών πιστοποιητικών με την έκδοση, την ανανέωση, τη διανομή και την ανάκληση τους. Η επικύρωση της ταυτότητας των τελικών χρηστών ή άλλων CA πραγματοποιείται, είτε από την ίδια CA, είτε σε συνεργασία με την Αρχή Εγγραφής (Registration Authority ή RA).

Ένας δημόσια προσπελάσιμος χώρος, γνωστός ως Repository μίας CA κρατάει ενημερωμένες πληροφορίες για πιστοποιητικά που έχουν εκδοθεί, ή/και που έχουν ανακληθεί από την συγκεκριμένη CA. Ωστόσο, όλες αυτές οι υποστηριζόμενες

PDF created with pdfFactory Pro trial version www.pdffactory.com

τεχνολογίες χρήζουν ενός πλαισίου πολιτικών ασφάλειας, που θα καθορίσουν το βαθμό εμπιστοσύνης σε ένα πιστοποιητικό. Η Πολιτική Πιστοποιητικού (Certificate Policy ή CP) είναι ένα δημόσια διαθέσιμο έγγραφο και προσδιορίζει τη χρήση του ψηφιακού πιστοποιητικού. Συμπληρωματικά, η Δήλωση Εφαρμογής Πιστοποιητικού (Certificate Statement Policy ή CPS) είναι ένα εσωτερικό έγγραφο που περιγράφει τον τρόπο υλοποίησης της Πολιτικής Πιστοποιητικού σε ένα συγκεκριμένο οργανισμό.

8.5 Εφαρμογές του PKI

Μέσα στο ανοιχτό περιβάλλον του Internet, η λειτουργία του PKI ως μία υπηρεσία υψηλής διαθεσιμότητας και ασφάλειας αποτελεί μία από τις μεγαλύτερες προκλήσεις. Από την πλευρά των πελατών, των επιχειρηματικών συνεργατών ή και των εσωτερικών χρηστών, ένα επιτυχημένο PKI κρίνεται από την ευκολία απόκτησης και χρήσης ενός πιστοποιητικού. Ταυτόχρονα, από την πλευρά της επιχείρησης, η λειτουργία του PKI ταυτίζεται με την ανάπτυξη μίας αξιόπιστης online υπηρεσίας για τους τελικούς χρήστες.

Με την υιοθέτηση του PKI, μία σειρά υπηρεσιών για έναν οργανισμό απλουστεύονται με ταυτόχρονη αύξηση του επιπέδου ασφάλειας. Ενδεικτικά, μπορούμε να αναφέρουμε:

1. Αυθεντικοποίηση χρηστών από το WEB και δημιουργία ιδιωτικών καναλιών επικοινωνίας
2. Υπογεγραμμένα και κρυπτογραφημένα μηνύματα π.χ. ασφαλές e-mail
3. Υπογεγραμμένες συναλλαγές και υπογραφή εντύπων
4. Δημιουργία Virtual Private Networks
5. Αυθεντικοποίηση για απομακρυσμένη πρόσβαση
6. Single Sign On (SSO) σε εταιρικές εφαρμογές

8.6 Προσεγγίσεις υλοποίησης PKI

Τα πλεονεκτήματα που προσφέρει το PKI δεν μπορούν να αγνοηθούν από εκείνες τις επιχειρήσεις, τους οργανισμούς και τους φορείς που θέλουν να έχουν μερίδιο στην ανερχόμενη ψηφιακή αγορά. Δύο προσεγγίσεις αποτελούν τις βασικές επιχειρηματικές λύσεις PKI:

Αγορά αυτόνομου λογισμικού PKI. Με αυτή την προσέγγιση, μία εταιρεία γίνεται Αρχή Πιστοποίησης., Τα πιστοποιητικά που εκδίδει, έχουν περιορισμένη ισχύ μόνο στον ίδιο τον οργανισμό και ίσως σε συνεργάτες με τους οποίους έχει συνάψει λεπτομερείς ιδιωτικές συμφωνίες, για χρήση των συγκεκριμένων πιστοποιητικών. Ταυτόχρονα, η επιχείρηση είναι αποκλειστικά υπεύθυνη για τη διαχείριση όλης της τεχνολογικής υποδομής, όπως λογισμικό, δίκτυα και βάσεις δεδομένων, την παροχή ασφάλειας, υψηλής διαθεσιμότητας, νομικής και οικονομικής ευθύνης.

Αγορά μίας ολοκληρωμένης πλατφόρμας υπηρεσίας PKI. Η λύση αυτή προσφέρει την υπάρχουσα υποδομή και τις υπηρεσίες μίας εφαρμογής PKI, με υψηλή ασφάλεια και διαθεσιμότητα. Επιπρόσθετα, συνδυάζει τον επιχειρηματικό έλεγχο και τη λειτουργία του απαραίτητου λογισμικού και υλικού, με την από κοινού

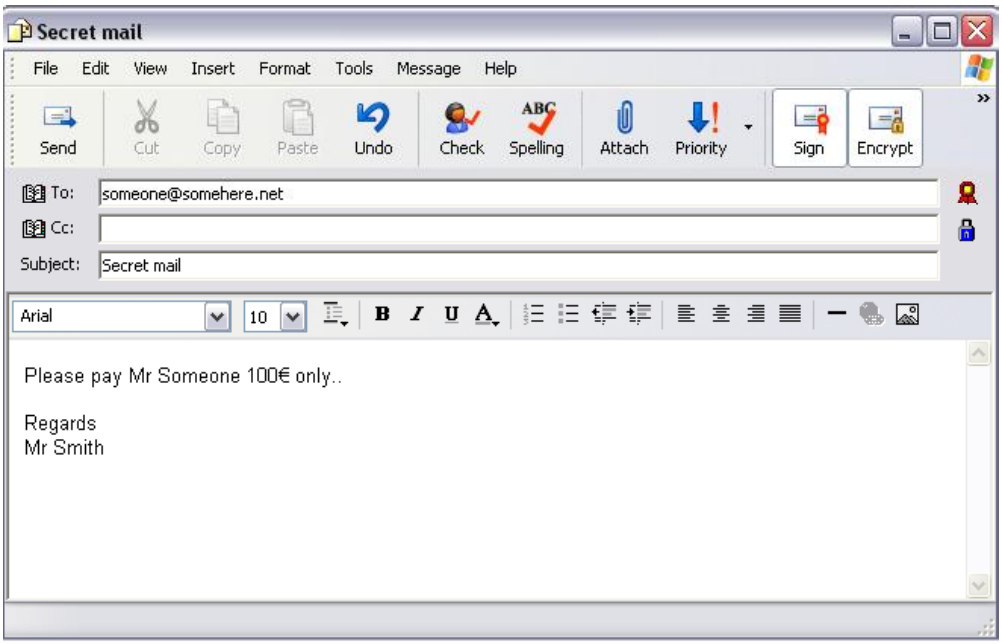
PDF created with pdfFactory Pro trial version www.pdffactory.com

υπαιτιότητα και τις ανεξάρτητες, αλλά ελεγχόμενες επιχειρηματικές διαδικασίες για το PKI. Τέλος, μέσα στο περιβάλλον της ευρωπαϊκής ένωσης, η παροχή υπηρεσίας PKI συμμορφωμένης με την Κοινοτική Οδηγία 1999/93/EC για το πλαίσιο των ψηφιακών υπογραφών, δίνει ένα συγκριτικό πλεονέκτημα.

Συνοψίζοντας, μπορούμε να παρατηρήσουμε ότι το βασικό μειονέκτημα της πρώτης προσέγγισης είναι η ανάγκη για ανάληψη όλης της επένδυσης και του ρίσκου από την ίδια την επιχείρηση. Αντίθετα, η υιοθέτηση της υπηρεσίας PKI, εγγυάται συνεχή προσφορά υπηρεσιών (24 ώρες X 7 ημέρες) με μείωση του κόστους και του ρίσκου της επένδυσης, προσφέροντας άμεση υποστήριξη ποικίλων ηλεκτρονικών εφαρμογών.

Windows και Outlook Express

Το Outlook Express είναι ίσος το πιο διαδεδομένο πρόγραμμα αλληλογραφίας (mail Client). Νεότερες εκδώσεις υποστηρίζουν εγγενώς λειτουργίες ψηφιακής υπογραφής και κρυπτογράφησης με βάση το πρωτόκολλο SMIME



Εικόνα 20.

Με την πίεση απλά δύο πλήκτρων υπογράφουμε και κρυπτογραφούμε το email πριν το στείλουμε. Το λογισμικό Outlook (email client) θα φροντίσει να βρει το δημόσιο κλειδί του παραλήπτη ώστε να κρυπτογραφήσει το περιεχόμενο l ώστε να μπορεί να το ανοίξει μόνο αυτός.

Για να λειτουργήσει σωστά θα πρέπει τόσο ο αποστολέας όσο και ο παραλήπτης να έχουν σύνδεση με κάποιου είδους κατάλογο (LDAP) και PKI (πχ Microsoft CA και AD).

PDF created with pdfFactory Pro trial version www.pdffactory.com

9. Αλγόριθμοι Ψηφιακών Υπογραφών

Η ψηφιακή υπογραφή είναι μια βασική κρυπτογραφική έννοια, τεχνολογικά ισοδύναμη με την χειρόγραφη υπογραφή. Σε πολλές Εφαρμογές, οι ψηφιακές υπογραφές χρησιμοποιούνται ως δομικά συστατικά για μεγαλύτερα κρυπτογραφικά πρωτόκολλα και συστήματα.

Σε ένα σχήμα υπογραφής, κάθε μέρος έχει ένα μοναδικό κλειδί υπογραφής sk που μοναδικά υπογράφει το μήνυμα . Κάθε μεριά δημοσιεύει το αντίστοιχο δημόσιο κλειδί επαλήθευσης pk. Μόνο κάποιος με την γνώση του sk μπορεί να υπογράψει ένα μήνυμα, αλλά όλες οι μεριές έχουν πρόσβαση στο pk και μπορούν να επαληθέψουν μιαν υπογραφή. Τέτοια σχήματα είναι χρήσιμα γιατί αποφεύγουν πως κάποιος μέσω του κλειδιού επαλήθευσης να μπορεί να υπολογίσει το κλειδί υπογραφής με μη αμελητέα πιθανότητα. Επιπλέον είναι ανέφικτο για κάποιον αντίπαλο να παράγει ένα έγκυρο ζευγάρι μήνυμα-υπογραφή ως προς κάποιο κλειδί επαλήθευσης.

Ένα σχήμα ψηφιακής υπογραφής (digital signature scheme) είναι μια τριάδα αλγορίθμων τέτοια ώστε :

1. Ο αλγόριθμος παραγωγής κλειδιού Gen: Πάρε ως είσοδο μια παράμετρο ασφαλείας 1λ και επέστρεψε το ζευγάρι (pk, sk). Θα ονομάζουμε το κλειδί pk ως δημόσιο ή επαλήθευσης και το κλειδί sk ως κρυφό ή υπογραφής

2. Ο αλγόριθμος υπογραφής Sign: Πάρε ως είσοδο την κρυπτογραφική παράμετρο 1λ, το κλειδί υπογραφής sk και ένα μήνυμα M και παρήγαγε την ψηφιακή υπογραφή σ του M.

3. Ο αλγόριθμος επαλήθευσης Verify: Πάρε ως είσοδο το κλειδί επαλήθευσης vk, μια ψηφιακή υπογραφή σ και ένα μήνυμα m. Επέστρεψε True= 1 ή False=0 δείχνοντας αν η υπογραφή είναι έγκυρη ή όχι.

Ο κύριος στόχος των ψηφιακών υπογραφών είναι μη δυνατότητα πλαστογράφησης (unforgeability), ή διαφορετικά πως ένας PPT αντίπαλος δεν μπορεί να κατασκευάσει ένα έγκυρο ζευγάρι μηνύματος-υπογραφής. Η δυνατότερη επίθεση ενάντια σε ψηφιακές υπογραφές ονομάζετε επίθεση επιλεγμένης μεθόδου (chosen method attack). Σε μια τέτοια επίθεση, ο αντίπαλος έχει απεριόριστη πρόσβαση σε ένα μαντείο υπογραφών που υπογράφει μηνύματα που διαλέγει ο αντίπαλος.

Ένα σχήμα ψηφιακών υπογραφών (Gen, Sign, Verify) χαρακτηρίζεται από μη δυνατότητα πλαστογράφησης ενάντια σε επιθέσεις επιλεγμένου μηνύματος (unforgeability against chosen message attacks) (UF-CMA) αν για κάθε PPT αντίπαλο A που χρησιμοποιεί το μαντείο υπογραφών Sign(sk, ·) ℓ φορές, η πιθανότητα να παράξει ο A ℓ+1 διαφορετικά έγκυρα ζευγάρια μηνύματος υπογραφής είναι αμελητέα.

Όταν τα μηνύματα είναι διακριτά, θα λέμε πως υπάρχει ισχυρή μη δυνατότητα πλαστογράφησης (strong unforgeability). Όταν τα ζευγάρια μηνύματος-υπογραφής είναι διακριτά, θα λέμε πως υπάρχει απλή μη δυνατότητα πλαστογράφησης (regular unforgeability).

PDF created with pdfFactory Pro trial version www.pdffactory.com

9.1 Η Συνάρτηση RSA: Η ΄Υψωση στην e-οστή δύναμη στο Z_n

Το κρυπτοσύστημα RSA αναπτύχθηκε το 1977 στο MIT από τους Ron Rivest, Adi Shamer, and Leonard Adleman. Ήταν το πρώτο σχήμα κρυπτογράφησης δημοσίου κλειδιού που μπορούσε να κρυπτογραφήσει και να υπογράψει μηνύματα. Όπως και με το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman, το σύστημα έδινε τη δυνατότητα σε δύο μεριές να επικοινωνήσουν σε ένα δημόσιο κανάλι.

Υποθέστε πως η Αλίκη αποφασίζει να στείλει στον αγαπητό της φίλο Βασίλη ένα μήνυμα. Για να εξασφαλιστεί μια ιδιωτική συνομιλία σε ένα μη ασφαλές κανάλι, ο Βασίλης διαλέγει και δημοσιεύει τους ακεραίους n και e. Η Αλίκη γράφει το μήνυμα x και υπολογίζει το

$$\mathbf{E(x) = x^{\,e} \bmod n,}$$

που είναι γνωστό ως η ύψωση στην e-οστη δύναμη (e-th Power map του x. Τότε στέλνει το y = E(x) στον Βασίλη, ο οποίος για να δει το μήνυμα, πρέπει να υπολογίσει την e-οστη ρίζα του y. Πιστεύεται πως αυτό είναι δύσκολο, όπως συζητήθηκε και στην ενότητα ??. Αν ο Βασίλης διαλέξει τα n και e με ανάλογα, υπάρχει και μια εναλλακτική μέθοδος. Βλέπουμε πως ο Βασίλης μπορεί να εφαρμόσει την ύψωση στην d-οστη δύναμη του y για να πάρει το x,

$$D(y) = y^d = x^{ed} \equiv x^{1+\varphi(n)k} \equiv x \bmod n$$

όπου το k ∈ Zn και η συνάρτηση Euler φ(n) ορίζεται ως εξής:

Για κάθε n ∈ N, η συνάρτηση Euler (Euler function) φ(n) υπολογίζει τον αριθμό των ακεραίων στο Zn που είναι σχετικά πρώτοι με το n:

$$\varphi(n) = \#\ \{\ k \in Zn : \gcd(k, n) = 1\}\ .$$

Αντίστοιχα, το φ(n) είναι ο αριθμός των αντιστρέψιμος στοιχείων στο Zn:

$$\varphi(n) = \#\ \{\ k \in Zn : k\ell = 1 \text{ for some } \ell \in Zn\}\ .$$

Για να υπολογίσουμε την συνάρτηση Euler μελετάμε τις εξής περιπτώσεις:

$$\varphi(n) = \begin{cases} p^e - p^{e-1}, n = p^e \\ \prod_{i=1}^{j} \varphi(p_i^{ei}), n = p_1^{e1} \ldots p_j^{ej} \end{cases}$$

Αν n = pe, είναι εύκολο να μετρήσουμε τους αριθμούς υπόλοιπο n τους οποίους το p δεν διαιρεί. Μπορούμε να επεκτείνουμε το φ σε ένα σύνθετο ακέραιο $n = p_1^{e1} \ldots\ldots p_j^{ej}$ χρησιμοποιώντας το γεγονός ότι το φ είναι πολλαπλασιαστικό σε σχετικά πρώτους ακέραιους: $\varphi(mn) = \varphi(m)\varphi(n)$ όταν gcd(m, n) = 1. Αυτό μπορεί να δειχθεί αποδεικνύοντας ότι :

$$\mathbf{Z}^{*}_{mn} \cong \mathbf{Z}^{*}_{m} x\ \mathbf{Z}^{*}_{n}$$

PDF created with pdfFactory Pro trial version www.pdffactory.com

9.2 Το Πρότυπο Ψηφιακής Υπογραφής

Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard, DSS), δημοσιεύτηκε από το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) το οποίο καθορίζει ένα σύστημα ψηφιακών υπογραφών, για γενική χρήση. Το DSS περιγράφει έναν αλγόριθμο ψηφιακής υπογραφής, τον DSA (Digital Signature Algorithm), οποίος βασίζεται σε ασύμμετρη κρυπτογραφία. Σε αντίθεση με τα συστήματα ψηφιακών υπογραφών που περιγράψαμε, ο DSA αναφέρεται αποκλειστικά σε σύστημα ψηφιακών υπογραφών και δεν μπορεί να χρησιμοποιηθεί ως κρυπτοσύστημα. Επίσης, το DSS προβλέπει τη χρήση της SHA-1 (Κεφάλαιο 4) ως κρυπτογραφική μονόδρομη hash, η οποία συμμετέχει στη δημιουργία της ψηφιακής υπογραφής.

Ο DSA είναι μια τροποποίηση του συστήματος ψηφιακής υπογραφής ElGamal. Επομένως, η ασφάλειά του βασίζεται στο πρόβλημα του υπολογισμού του διακριτού λογάριθμου. Όπως όλα τα συστήματα ψηφιακών υπογραφών που εξετάσαμε παραπάνω, έτσι και ο DSA αποτελείται από τον καθορισμό των ασύμμετρων παραμέτρων (των κλειδιών), το πρωτόκολλο ψηφιακής υπογραφής και το πρωτόκολλο επαλήθευσης της υπογραφής.

Κατά τη δημιουργία των κλειδιών, το κάθε μέλος θα πρέπει να εκτελέσει τα ακόλουθα βήματα. Αρχικά, επιλέγεται ένας πρώτος αριθμός q τέτοιος ώστε $2^{159} < q < 2^{160}$. Από τα όρια αυτά φαίνεται ότι το μέγεθος του αριθμού q θα είναι ίσο με 160 bits. Στη συνέχεια επιλέγεται πρώτος αριθμός p τέτοιος ώστε $2t-1 < p < 2t$, με $512 \leq t \leq 1024$, και ο t να είναι ακέραιο πολλαπλάσιο του 64. Επίσης ο q θα πρέπει να διαιρεί τον (p–1).

Με βάση τους πρώτους αριθμούς p και q, επιλέγεται γεννήτορας a μιας κυκλικής υποομάδας τάξης q της ομάδας Z^*_p. Αυτό επιτυγχάνεται επιλέγοντας $g \in Z^*_p$ τέτοιο ώστε:

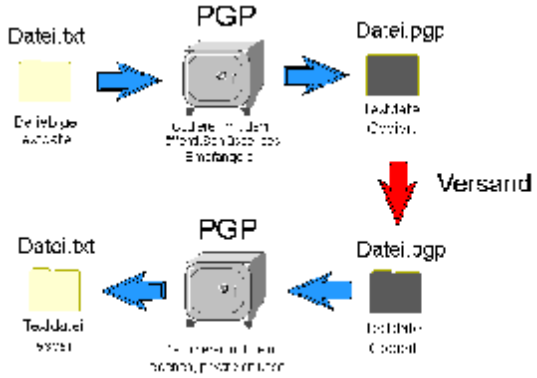
$$g^{(p-1)/q} \bmod p > 1$$

PDF created with pdfFactory Pro trial version www.pdffactory.com

10. Προγράμματα υλοποίησης ψηφιακής υπογαφής

10.1 Το Πρόγραμμα PGP (Pretty Good Privacy)

[13]Το πρόγραμμα PGP (Pretty Good Privacy), που αποτελεί δημιούργημα του καθηγητή του MIT Philip Zimmermann το έτος 1991, είναι από τα πιο γνωστά προγράμματα κρυπτογράφησης ηλεκτρονικού ταχυδρομείου και αρχείων και οι αλγόριθμοι που χρησιμοποιεί είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του (source code) είναι διαθέσιμος (ανοικτός) στους χρήστες, ενώ το πρόγραμμα χρησιμοποιείται εδώ και πολύ καιρό και θεωρείται σε μεγάλο βαθμό αξιόπιστο. Χρησιμοποιεί την ασύμμετρη μέθοδο κρυπτογράφησης με δημόσιο και ιδιωτικό κλειδί.

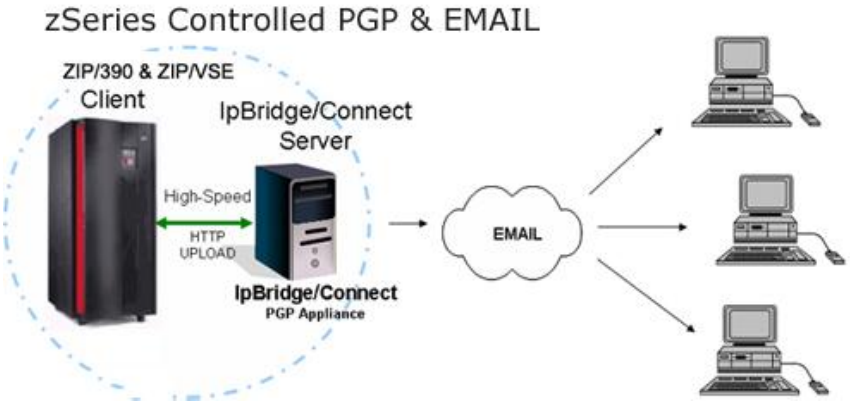


Εικόνα 21. Διαδικασία λειτουργία της εφαρμογής PGP Pretty

Αν και το πρόγραμμα είναι σε μεγάλο βαθμό αξιόπιστο για απλές εφαρμογές ταυτοποίησης χρηστών, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου (e-commerce) καθώς και γι' όσες εφαρμογές απαιτούν ισχυρή ταυτοποίηση. Ο δημιουργός του διώχθηκε ποινικά από τις αρχές των ΗΠΑ, καθώς με τη δωρεάν διανομή του προγράμματός του παραβίασε την ισχύουσα τότε νομοθεσία περί απαγόρευσης εξαγωγής προγραμμάτων κρυπτογράφησης, τα οποία αντιμετωπίζονταν ως στρατιωτικό υλικό. Ο νομός τελικά τροποποιήθηκε το 2000 μετά από πίεση της βιομηχανίας πληροφορικής.

Οι αρχές χρησιμοποίησαν ως βασικό επιχείρημά τους το ότι η τεχνική αυτή της κρυπτογράφησης θα μπορούσε να μετατραπεί σε πανίσχυρο όπλο στα χέρια τρομοκρατών, για να μπορούν, για παράδειγμα, να ανταλλάσσουν μεταξύ τους e-mails με άγνωστο και επικίνδυνο περιεχόμενο. Ο κ. Philip Zimmermann ισχυρίζεται ότι είναι καλύτερο για την κοινωνία μας να διαθέτει ένα χρήσιμο εργαλείο προστασίας της ιδιωτικότητας και ότι εκτός από το κυνήγι των τρομοκρατών, οι αρχές έχουν την υποχρέωση να προστατεύουν τις επικοινωνίες και τις συναλλαγές των απλών πολιτών.

PDF created with pdfFactory Pro trial version www.pdffactory.com



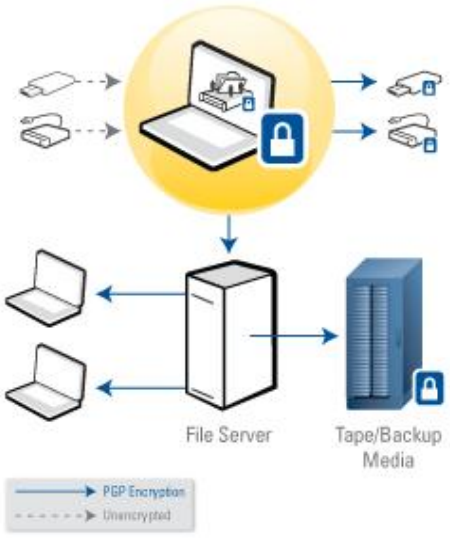
Εικόνα 22. Απαιτούμενες περιφερειακές συσκευές για την λειτουργία της εφαρμογής PGP.

Το PGP, πιο συγκεκριμένα το PGPi, στη διεθνή έκδοσή του, μπορούμε να κατεβάσουμε και να χρησιμοποιήσουμε δωρεάν από την επίσημη ιστοσελίδα http://www.pgpi.ogr. Η εμπορική έκδοση του προγράμματος PGP αναπτύσσεται στις ΗΠΑ από την γνωστή εταιρεία Network Associates (βλ. McAfee) και εξαιτίας των αυστηρών τοπικών νόμων περί απαγόρευσης εξαγωγής κρυπτογραφικού υλικού, απαγορεύεται η χρήση του εκτός ΗΠΑ. Περισσότερες πληροφορίες υπάρχουν στην ιστοσελίδα http://www.pgp.com.

Το PGP, πιο συγκεκριμένα το PGPi, στη διεθνή έκδοσή του, μπορούμε να κατεβάσουμε και να χρησιμοποιήσουμε δωρεάν από την επίσημη ιστοσελίδα http://www.pgpi.ogr. Η εμπορική έκδοση του προγράμματος PGP αναπτύσσεται στις ΗΠΑ από την γνωστή εταιρεία Network Associates (βλ. McAfee) και εξαιτίας των αυστηρών τοπικών νόμων περί απαγόρευσης εξαγωγής κρυπτογραφικού υλικού, απαγορεύεται η χρήση του εκτός ΗΠΑ. Περισσότερες πληροφορίες υπάρχουν στην ιστοσελίδα http://www.pgp.com.

Κατά την εγκατάσταση του προγράμματος στον υπολογιστή μας, θα πρέπει να ακολουθήσουμε κάποια βήματα για τη δημιουργία ενός νέου ζεύγους κλειδιών. Μπορούμε να επιλέξουμε ένα επίπεδο ασφάλειας για τα κλειδιά μας από 1.024, 1.536, 2.048, 3.072 ή 4.096 bits. Όσο περισσότερα bits επιλέξουμε, τόσο πιο ασφαλή θα είναι τα κλειδιά που θα δημιουργήσουμε, αλλά θα αργήσει πολύ η δημιουργία τους και θα είναι πολύ αργά και στη χρήση τους. Οι τιμές από 1.024 έως 2.048 bits είναι υπεραρκετές για τις περισσότερες εφαρμογές. Εκεί που θα πρέπει να δώσουμε πολύ προσοχή είναι στην επιλογή της συνθηματικής φράσης (passphrase), για να μπορούμε να κρυπτογραφούμε τα μηνύματά μας με το ιδιωτικό κλειδί. Για να κρυπτογραφήσουμε ένα μήνυμα ή ένα αρχείο, το αντιγράφουμε πρώτα στο Πρόχειρο (Clipboard), κάνουμε μετά δεξί κλικ πάνω στο εικονίδιο με το λουκέτο που έχει δημιουργήσει το PGP στη γραμμή εργασιών και επιλέγουμε *Clipboard* και *Encrypt* από το πτυσσόμενο μενού.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 23. Χρήση των συστημάτων File Server & \ Backup Server στην κρυπτογράφηση

Θα πρέπει στο σημείο αυτό να δηλώσουμε τον ή τους παραλήπτες του μηνύματος και αν θέλουμε να το κρυπτογραφήσουμε για δική μας χρήση, θα πρέπει να δηλώσουμε ως παραλήπτη τον εαυτό μας. Μόλις κάνουμε κλικ στο OK, το κρυπτογραφημένο μήνυμα θα είναι διαθέσιμο από το Πρόχειρο του υπολογιστή μας, απ' όπου θα μπορούμε να το πάρουμε με απλή επικόλληση. Το κρυπτογραφημένο αυτό μήνυμα θα μπορεί τώρα να αποκρυπτογραφηθεί μόνο από το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε. Αυτό σημαίνει ότι δεν θα μπορούμε να το διαβάσουμε ούτε εμείς που το δημιουργήσαμε, στην περίπτωση που το κρυπτογραφήσαμε με το δημόσιο κλειδί ενός άλλου χρήστη.

Αν κάνουμε δεξί κλικ πάνω στο εικονίδιο με το λουκέτο που έχει δημιουργήσει το PGP στη γραμμή εργασιών και επιλέξουμε PGPkeys από το πτυσσόμενο μενού, θα μπορούμε να δούμε όλα τα δημόσια κλειδιά των άλλων χρηστών που έχουμε αποθηκεύσει στον υπολογιστή μας. Ένα δημόσιο κλειδί μπορούμε να το λάβουμε με e-mail ή με μια δισκέτα ως ένα απλό αρχείο κειμένου .txt ή και να το κατεβάσουμε (download) από το Internet.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης υπάρχουν και εκδόσεις open source/free software (λογισμικό ανοιχτού/ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnupgp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις

PDF created with pdfFactory Pro trial version www.pdffactory.com

αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του.

Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντάς το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς:

- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής ταυτοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για όσες απαιτούν ισχυρή ταυτοποίηση. Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό βαθμού εμπιστοσύνης.

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

Για να υπογράψουμε ψηφιακά ένα μήνυμα, να το κρυπτογραφήσουμε δηλαδή με το ιδιωτικό μας κλειδί, πρώτα το αποθηκεύουμε στο Πρόχειρο και μετά κάνουμε δεξί κλικ πάνω στο εικονίδιο με το λουκέτο που έχει δημιουργήσει το PGP στη

PDF created with pdfFactory Pro trial version www.pdffactory.com

γραμμή εργασιών και επιλέγουμε Clipboard και Sign από το πτυσσόμενο μενού. Το μήνυμα θα μπορεί να αποκρυπτογραφηθεί με το αντίστοιχο δικό μας δημόσιο κλειδί, αλλά θα είναι ψηφιακά υπογεγραμμένο και ακέραιο, δηλαδή οι παραλήπτες θα είναι σίγουροι για την αυθεντικότητά του. Αν επιλέξουμε Clipboard και Encrypt & Sign από το πτυσσόμενο μενού, τότε το μήνυμα θα κρυπτογραφηθεί με το δικό μας ιδιωτικό κλειδί καθώς και με το δημόσιο κλειδί όποιου ή όποιων παραληπτών επιλέξουμε. Τέλος, για την αποκρυπτογράφηση ενός μηνύματος, το οποίο έχει κρυπτογραφηθεί από κάποιον άλλον με το δικό μας δημόσιο κλειδί και το οποίο λαμβάνουμε ως παραλήπτες, πρώτα το αποθηκεύουμε στο Πρόχειρο και μετά κάνουμε δεξί κλικ πάνω στο εικονίδιο με το λουκέτο που έχει δημιουργήσει το PGP στη γραμμή εργασιών και επιλέγουμε Clipboard και Decrypt & Verify από το πτυσσόμενο μενού.

10.1.1 Το PGP στην πράξη

[13]Το PGP ανήκει σε εκείνα τα εκτελέσιμα αρχεία (*.exe) τα οποία εκκινούνται μαζί με την εκκίνηση του Λειτουργικού σας Συστήματος, εν προκειμένω τα MS Windows. Στη γραμμή εργασιών (task bar), στα δεξιά της οθόνης και δίπλα στο ρολόι, υπάρχει ένα εικονίδιο με μία κλειδαριά. Κάνοντας κλικ πάνω στην κλειδαριά σας εμφανίζεται το μενού του προγράμματος PGP, όπως φαίνεται στη παρακάτω εικόνα.

Εικόνα 24. Ξεκινώντας το PGP

Το μενού του PGP:

- PGP keys: δημιουργία προσωπικών κλειδιών, εύρεση και διαχείριση δημόσιων κλειδιών άλλων ατόμων.
- PGP mail: κρυπτογράφηση email για αποστολή, αποκρυπτογράφηση email που παραλήφθηκαν.
- PGP disk: κρυπτογράφηση μέρους του σκληρού δίσκου ώστε να είναι πλήρως προστατευμένος ακόμη και αν κλαπεί.

PDF created with pdfFactory Pro trial version www.pdffactory.com

10.1.2 Κατασκευή ζεύγους προσωπικών κλειδιών (ιδιωτικό και δημόσιο)

Αφού επιλέξουμε από το PGP μενού την επιλογή PGP keys, μας ανοίγει το αντίστοιχο παράθυρο. Από το βασικό μενού επιλέγουμε Keys→New key και μας εμφανίζεται σε νέο παράθυρο ο οδηγός δημιουργίας των προσωπικών μας κλειδιών.

Εικόνα 25 .Κατασκευή ζεύγους προσωπικών κλειδιών

Εικόνα 26. Έναρξη οδηγού κατασκευής κλειδιών

Στο PGP Generation Wizard (οδηγό) αρχικά πατάμε Επόμενο. Στο επόμενο βήμα μας ζητείτε να γράψουμε το όνομά μας και τη διεύθυνση του ηλεκτρονικού μας ταχυδρομείου e-mail και πατάμε πάλι Επόμενο. Στο τρίτο βήμα καλούμαστε να δώσουμε έναν κωδικό βάση του οποίου θα δημιουργηθούν ταυτόχρονα το ιδιωτικό και το δημόσιο κλειδί μας. Ο κωδικός αυτός θα πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες (γράμματα ή αριθμούς). Το δεύτερο πεδίο είναι απλά για να επιβεβαιώσουμε τον κωδικό που δώσαμε πιο πάνω. ΠΡΟΣΟΧΗ!. Τον κωδικό αυτόν θα πρέπει να τον θυμάστε διότι θα σας ξαναζητηθεί όπως θα δούμε στη

PDF created with pdfFactory Pro trial version www.pdffactory.com

συνέχεια. Αμέσως μετά πατάμε Επόμενο ώστε να δημιουργηθεί το ζευγάρι κλειδιών μας, ξανά **Επόμενο** και **Τέλος.** Το ζευγάρι των προσωπικών μας κλειδιών έχει πλέον δημιουργηθεί και μπορούμε να το δούμε μέσα στο κεντρικό παράθυρο του PGPkeys.

10.1.3 Δουλεύοντας με το προσωπικό μας κλειδί

Αφού δημιουργήσουμε όπως είπαμε πιο πάνω το προσωπικό μας κλειδί, επιλέγοντάς το από το παράθυρο του PGPkeys με δεξί κλικ μας εμφανίζει ένα ολόκληρο μενού, όπου μας δίνεται η δυνατότητα να κάνουμε διάφορες παραμετροποιήσεις. Καθορισμός σαν προεπιλεγμένου κλειδιού Επιλέγουμε το κλειδί με δεξί κλικ→Set as Default.

Προσθήκη νέου ονόματος και e-mail στο κλειδί

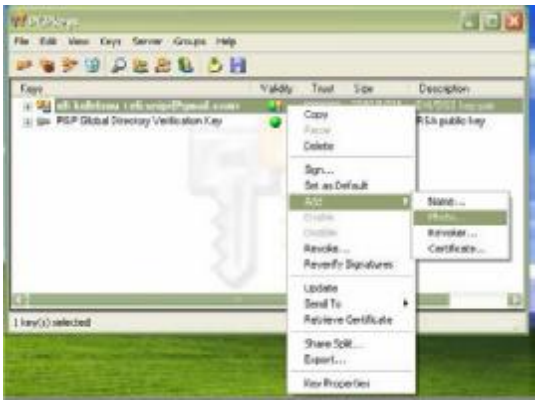
Επιλέγουμε το κλειδί με δεξί κλικ → Add → Name… →. Δίνουμε τα καινούρια στοιχεία → OK → .Μας ζητάει τον αρχικό κωδικό που είχαμε δώσει κατά τη δημιουργία του κλειδιού, ως επαλήθευση OK

Προσθήκη εικόνας/φωτογραφίας στο προσωπικό μας κλειδί

Επιλέγουμε το κλειδί με δεξί κλικ → Add → Photo → Select file →Επιλογή εικόνας/φωτογραφίας από το αρχείο του υπολογιστή

Διαγραφή κλειδιού

Επιλέγουμε το κλειδί με δεξί κλικ → Delete



Εικόνα 27. Διαχείριση κλειδιών

Αλλαγή Ιδιοτήτων

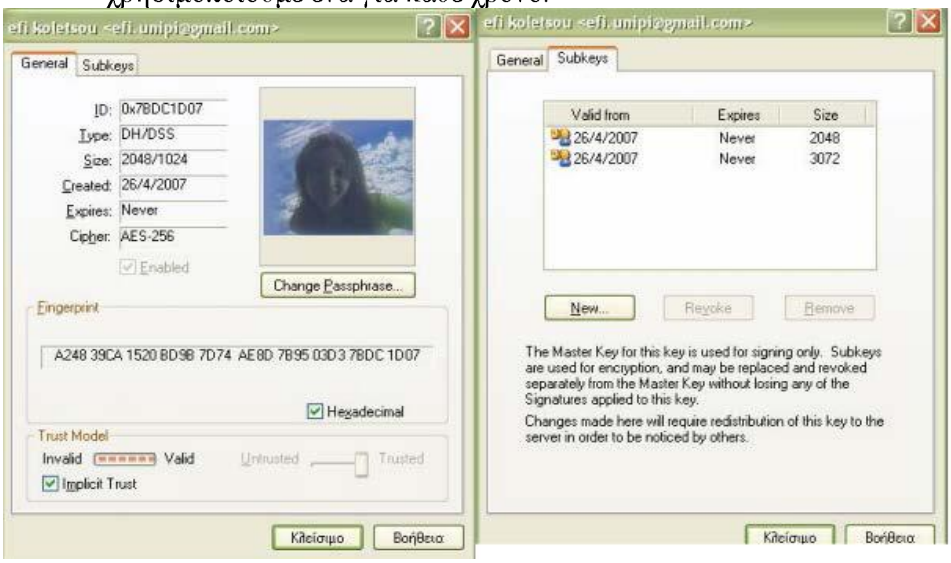
Επιλέγουμε Έπειτα στο κλειδί με δεξί κλικ → Key Properties

- ✓ Καρτέλα General: Στο πρώτο πεδίο βλέπουμε πληροφορίες όπως την Key ID του κλειδιού, το μέγεθός του, ημερομηνίες δημιουργίας και τερματισμού ύπαρξής του, την εικόνα –αν έχουμε εισάγει πιο πριν. Στο δεύτερο πεδίο της καρτέλας δίνεται το Fingerprint1 (‘Δακτυλικό αποτύπωμα’). Για να το δω επιλέγω το πλαίσιο ‘Hexadecimal’. Το τρίτο και

PDF created with pdfFactory Pro trial version www.pdffactory.com

τελευταίο πεδίο της καρτέλας δίνει τη δυνατότητα να ορίσουμε το πεδίο εμπιστευτικότητας του κλειδιού, μέσα σε μία κλίμακα Untrusted-Trusted.

✓ Καρτέλα Subkeys: Κάθε κλειδί στην ουσία αποτελείται από ένα signing key και ένα encryption subkey. Μπορούμε να δημιουργήσουμε πολλά encryption subkeys τα οποία χρησιμοποιήσουμε σε διαφορετικές χρονικές στιγμές, π.χ. αν δημιουργήσουμε ένα δημόσιο κλειδί για 3 χρόνια , μπορούμε να δημιουργήσουμε τρία subkeys και μπορούμε να χρησιμοποιούμε ένα για κάθε χρόνο.



Εικόνα 28. Ιδιότητες ψηφιακής υπογραφής

Split keys

Από το βασικό μενού του PGPkeys επιλέγουμε Keys → Share Split…

Εικόνα 29. Διαδικασία πρόσβασης στο private key σε περισσότερα από 1 άτομα

PDF created with pdfFactory Pro trial version www.pdffactory.com

Χρησιμοποιείται από εταιρίες όπου πολλά άτομα έχουν πρόσβαση ένα private key. Κάθε private key σπάει σε κομμάτια μεταξύ διαφορετικών χρηστών με τρόπο ώστε περισσότερα από δύο άτομα να παρουσιάσουν ένα κομμάτι του κλειδιού με σκοπό να μπορούν να το επαναφέρουν σε χρησιμότητα.

10.1.4 Δημιουργία ομάδων

Από το βασικό μενού του PGPkeys επιλέγουμε Groups → New Group…

Εικόνα 30. Δημιουργία ομάδων

Για αποστολή κρυπτογραφημένου mail σε μια ομάδα χρηστών, δημιουργούμε μία distribution list με το όνομα αυτής και στη συνέχεια βάζουμε τους χρήστες που θέλουμε. Π.χ. η λίστα all@hotmail.com περιλαμβάνει τους χρήστες kwstas@hotmail.com και efi@hotmail.com.

10.1.4.1 Αποστολή του προσωπικού δημόσιου κλειδιού σε παραλήπτη ηλεκτρονικής αλληλογραφίας

Επιλέγουμε το προσωπικό κλειδί που έχουμε ήδη φτιάξει και φαίνεται στο παράθυρο PGPkeys. Με δεξί κλικ πάνω στο κλειδί και την επιλογή **Copy** έχουμε αντιγράψει το δημόσιο κλειδί μας στο keyboard.

Για να το δούμε ποιο είναι και να μπορέσουμε να το αποστείλουμε σαν συνημμένο αρχείο μέσω ηλεκτρονικού ταχυδρομείου, ανοίγουμε ένα οποιοδήποτε πρόγραμμα το οποίο μπορεί να διαβάσει απλό κείμενο (π.χ. MS Word), και κάνουμε **Paste**. Το κείμενο έχει περίπου την εξής μορφή:

PDF created with pdfFactory Pro trial version www.pdffactory.com

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

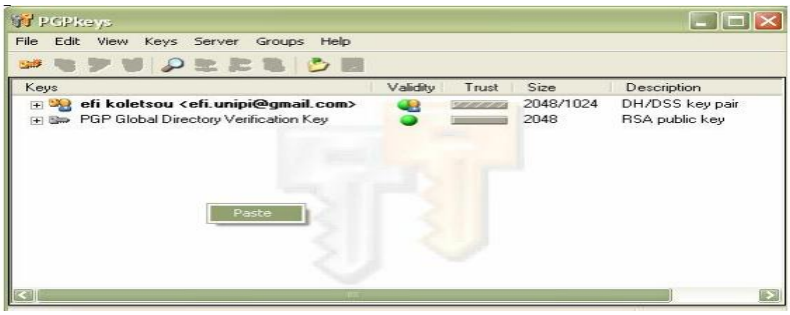
mQGiBEYwZqkRBADwrhmEFdf05Amw6ybe+4NFHBJjlN8Gx3aFozUsl3sKFxsYPBTe
7/ipzeQmY/lajVeUb9O6TrO0nN+dq8yJwNgkUsEepS7wxi5LER6A5pL2Tf1yelN2
YHD/tW/H8mZF0Wa9k1jYaQJUhl6d2npUHF3P6o4PFHdt48u6D1Dz8pdqTwCg/9Bl
FyRe0qdAbCX6ukaKzdifrqUEAJEFgWF/nbAN3HGqoDCHzFUlUnlSsCD3GAIR7lh1
RM1QByHDT91vlpVqYSUFeziX8As/2so6zXn798vReen6ldYXy3DKSSFZ7m9Duja9
EJUvgcakfHt+teo+7k6CWZRdymQQgFf6bq26Ef9H6RkCiPcyWrQ8zPEpejMxgeJ4
[.....πολύ μεγαλύτερο σε έκταση.....]
iKyGBE+Hu/yIydanxbvDpu/vXKh7FZpF4X4SqsA14+WgO4c3zykijIuJ/VBepuL6
DKxMnxz8ZSIXwyg8mJbtli/QQf9wgHdmP+Jb6LxIOG9oWIE44clBfvL4MQCMbzzw
s8G6iQBMBBgRAgAMBQJGMHzABRsMAAAAAAoJEHuVA9N73B0HoTYAniK9XeF3
LoTU
FO7v9BdvulvK7vcWAKC7g1yH52+cVTqlNAs90J7USepJHA==
=H66o
-----END PGP PUBLIC KEY BLOCK-----

Εικόνα 31. Κωδικοποιημένα Μηνύματα

Αποθηκεύουμε το αρχείο στον υπολογιστή μας και το επισυνάπτουμε μέσω ηλεκτρονικού ταχυδρομείου, όπου και το στέλνουμε σε όσα άτομα θέλουμε να επικοινωνήσουν μαζί μας κρυπτογραφημένα.

10.1.4.2 Αποθήκευση δημόσιου κλειδιού μέσα στα PGP keys που έχει παραληφθεί ως συνημμένο αρχείο μέσω e-mail

Ανοίγουμε το συνημμένο αρχείο (π.χ. MS Word), επιλέγουμε και αντιγράφουμε (Copy) όλο το περιεχόμενο στο keyboard, και ανοίγουμε το παράθυρο του PGPkeys. Σε ένα ελεύθερο χώρο μέσα στο παράθυρο κάνουμε δεξί κλικ και Paste.



Εικόνα 32.Αποθήκευση δημόσιου κλειδιού μέσα στα PGPkeys

Στο καινούριο παράθυρο που εμφανίζεται, επιλέγω Import και έτσι έχουμε εισάγει το δημόσιο κλειδί κάποιου άλλου χρήστη, που μας έχει αποσταλεί, μέσα στη λίστα των κλειδιών του PGP.

PDF created with pdfFactory Pro trial version www.pdffactory.com

10.1.5 Αποστολή του προσωπικού δημόσιου κλειδιού σε ένα Server

Από το βασικό μενού του PGPkeys επιλέγουμε Server → Send to… → ...

- ✓ Domain Server
- ✓ Mail Recipient
- ✓ Idap://keyserver.pgp.com (επίσημος Server της PGP.com)
- ✓ Idap://europe.keys.pgp.com:11370(επίσημος Server της PGP.com για την Ευρώπη)

Όταν η αίτησή σας αποσταλεί και γίνει αποδεχτή, θα λάβετε ένα e-mail στο ηλεκτρονικό σας ταχυδρομείο, όπου θα ζητήστε να επιβεβαιώσετε την εγκυρότητα του κλειδιού με το να επισκεφτείτε κάποιο site που θα σας υποδεικνύουν, ώστε να ολοκληρωθεί το αίτημά σας.

Εικόνα 33.Αποστολή του προσωπικού δημόσιου κλειδιού σε ένα Server

10.1.5.1 Αναζήτηση δημόσιου κλειδιού χρήστη μέσω Server

Από το βασικό μενού του PGPkeys επιλέγουμε Server → Search…

Εικόνα 34.Αναζήτηση δημόσιου κλειδιού χρήστη μέσω Server

Αφού επιλέξουμε την αναζήτηση μας εμφανίζεται το παρακάτω παράθυρο, απ' όπου επιλέγουμε τον Server όπου είναι υποθηκευμένο το κλειδί (π.χ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

ldap://keyserver.pgp.com) και δίνουμε κάποια στοιχεία που θα βοηθήσουν στην αναζήτηση (π.χ. το User ID να περιέχει/contains το όνομα “efi koletsou”) → Search.

Εικόνα 35. Διαδικασία εύρεσης κλειδιού

10.1.6 Κρυπτογράφηση και Αποκρυπτογράφηση με το PGP

10.1.6.1 Κρυπτογράφηση απλού κειμένου

Έστω ότι θέλουμε να κρυπτογραφήσουμε ένα απλό κείμενο που γράφουμε στο MS-Word και να το στείλουμε ως συνημμένο αρχείο σε κάποιον παραλήπτη αλληλογραφίας. Για να κάνουμε κάτι τέτοιο, θα πρέπει πρώτα απ’ όλα να γνωρίζουμε το δημόσιο κλειδί του παραλήπτη, το οποίο και να βρίσκεται μέσα στη λίστα του PGPkeys, ώστε να κρυπτογραφήσουμε με αυτό το κείμενο και μόνο ο παραλήπτης να μπορέσει να το αποκρυπτογραφήσει και να το διαβάσει. Έχοντας ως τρέχον το παράθυρο με το κείμενο που θέλουμε να κρυπτογραφήσουμε, επιλέγουμε από τη γραμμή εργασιών (task bar), στα δεξιά της οθόνης και δίπλα στο ρολόι, την κλειδαριά , κάνοντας ένα κλικ πάνω της. Από το μενού που μας εμφανίζει επιλέγουμε Current Window → Encrypt. Εν συνεχεία εμφανίζεται το ακόλουθο παράθυρο:

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 36. Κρυπτογράφηση

Εικόνα 37. Επιλογή κλειδιού προς κρυπτογράφηση

απλού κειμένου (βήμα 1)

Με τη μέθοδο drag & drop, επιλέγουμε τον/τους παραλήπτες του μηνύματος (recipients), ώστε το μήνυμα να κρυπτογραφηθεί με χρήση των δημόσιων κλειδιών τους → OK. Η διαδικασία κρυπτογράφησης του μηνύματος έχει ολοκληρωθεί. Αρκεί τώρα να αποθηκεύσουμε το αρχείο και να το επισυνάψουμε σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου.

10.1.6.2 Αποκρυπτογράφηση απλού κειμένου

Έστω ότι έχουμε λάβει ένα επισυναπτόμενο κρυπτογραφημένο μήνυμα από κάποιον αποστολέα, ο οποίος γνώριζε εκ των προτέρων το δημόσιο κλειδί μας και μας έχει κρυπτογραφήσει με αυτό το μήνυμα. Έχοντας ως τρέχον το παράθυρο με το κρυπτογραφημένο κείμενο, επιλέγουμε από τη γραμμή εργασιών (task bar), στα δεξιά της οθόνης και δίπλα στο ρολόι, την κλειδαριά, κάνοντας ένα κλικ πάνω της. Από το μενού που μας εμφανίζει επιλέγουμε Current Window → Decrypt & Verify.

Εν συνεχεία εμφανίζεται το ακόλουθο παράθυρο:

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 38.Αποκρυπτογράφηση απλού κειμένου

Όπου πρέπει να πληκτρολογήσουμε τον κωδικό που είχαμε αρχικά χρησιμοποιήσει για τη δημιουργία των προσωπικών μας κλειδιών. Δίνοντας, λοιπόν, τον σωστό κωδικό, μας εμφανίζεται το κείμενό μας αποκρυπτογραφημένο σε ένα νέο παράθυρο.

Εικόνα 39. Αποκρυπτογραφημένο μήνυμα

10.2 Το Πρόγραμμα WinPT (Windows Privacy Tools)

Το WinPT (Windows Privacy Tools) είναι ένα πρόγραμμα ελεύθερου λογισμικού για την κρυπτογράφηση μηνυμάτων και τη δημιουργία ψηφιακών υπογραφών. Με την εγκατάστασή του θα μας ζητήσει να δημιουργήσουμε ένα ζεύγος κλειδιών ή να εισάγουμε ένα ήδη υπάρχον. Για να κρυπτογραφήσουμε, αποκρυπτογραφήσουμε ή και να υπογράψουμε κάποιο αρχείο, πρέπει να κάνουμε δεξί κλικ πάνω του και να επιλέξουμε την αντίστοιχη λειτουργία από το μενού WinPT. Για να αποθηκεύσουμε το δημόσιο κλειδί σ' ένα ξεχωριστό αρχείο, ανοίγουμε τον Key Manager, κάνουμε δεξί κλικ στο ζεύγος κλειδιών που θέλουμε και επιλέγουμε Cope Key to Clipboard. Μπορούμε μετά να το επικολλήσουμε στο

PDF created with pdfFactory Pro trial version www.pdffactory.com

Σημειωματάριο (Notepad) των Windows και να το αποθηκεύσουμε ως ένα απλό αρχείο κειμένου.

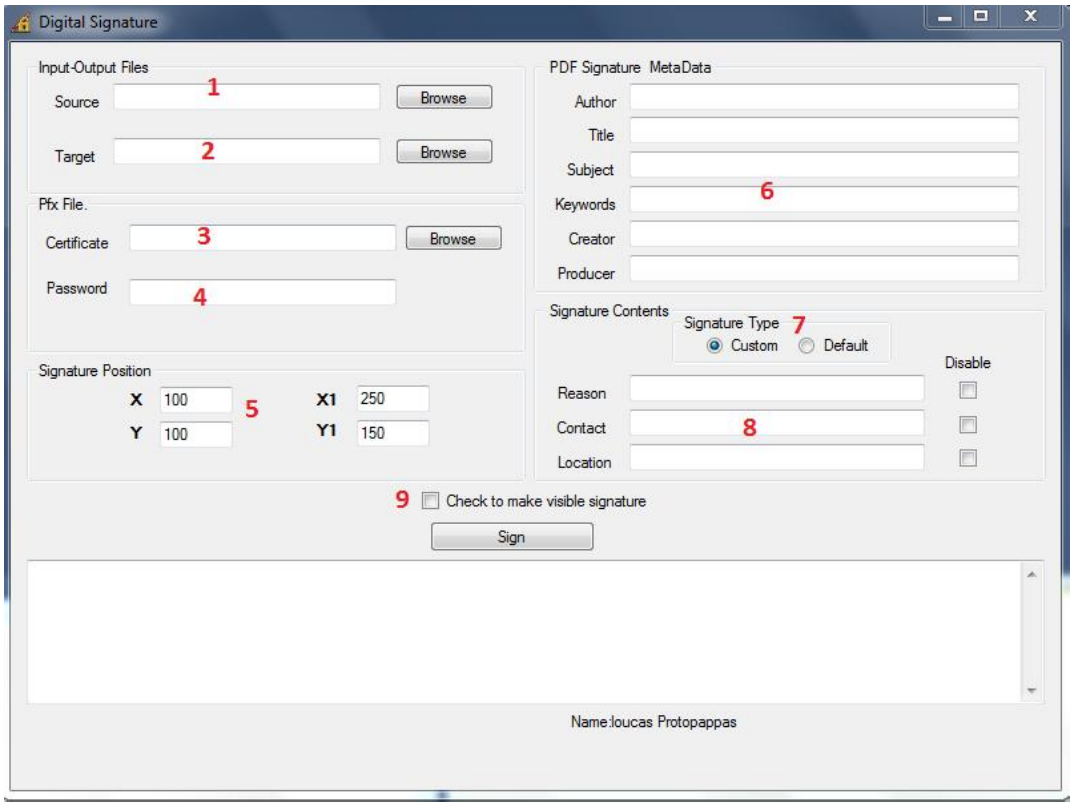
10.3 Το Πρόγραμμα Steganos Security Suite

Το Steganos Security Suite είναι ένα σύνολο προγραμμάτων που βασίζονται σε τεχνικές συμμετρικής κρυπτογράφησης αλλά δεν είναι δωρεάν. Από τα χαρακτηριστικά του, τα βασικότερα είναι η δυνατότητα δημιουργίας έως και τεσσάρων εικονικών κρυπτογραφημένων δίσκων όπου η πρόσβαση σ' αυτούς απαιτεί ειδικό κωδικό ασφαλείας, η δημιουργία ενός κρυπτογραφημένου CDs με δεδομένα της επιλογής μας και η δυνατότητα μεταμφίεσης των κρυπτογραφημένων δεδομένων σε αρχεία ήχου ή εικόνας, μια διαδικασία που αποκαλείται στεγανογραφία.

PDF created with pdfFactory Pro trial version www.pdffactory.com

11. Εφαρμογή Προσθήκης Ψηφιακής Υπογραφής

Σε εφαρμογή όλων όσων αναπτύχθηκαν στο θεωρητικό κομμάτι της διπλωματικής εργασίας έγινε η υλοποίηση της παρακάτω εφαρμογής. Η παρακάτω εφαρμογή, όπου και παραθέτονται απεικονίσεις λειτουργίας και ενδιάμεσων σταδίων εκτέλεσης της, δέχεται ως είσοδο ένα αρχείο εμπλουτισμένης μορφής κειμένου τύπου .pdf και το υπογράφει ψηφιακά.



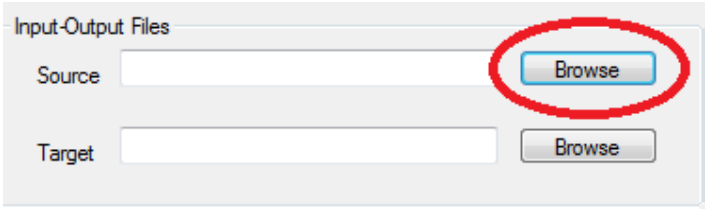
Εικόνα 40. Εικόνα Εισαγωγής στη εφαρμογή Digital Signature

11.1 Επεξήγηση Εφαρμογής

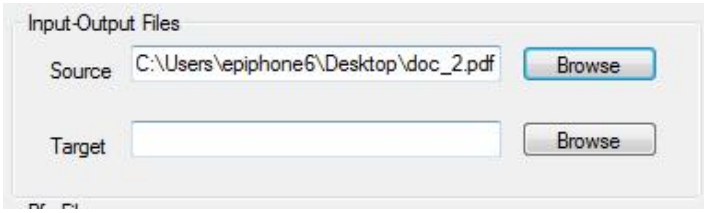
Πεδίο 1

Στο πεδίο 1 ο χρήστης καλείται να εισάγει ένα αρχείο εμπλουτισμένου κειμένου (pdf) με αποκλειστική κατάληξη του αρχείου .pdf. Ο χρήστης επιλέγοντας το button→Browse μπορεί να επιλέξει το αρχείο pdf κάνοντας αναζήτηση στα περιεχόμενα του υπολογιστή του.

PDF created with pdfFactory Pro trial version www.pdffactory.com



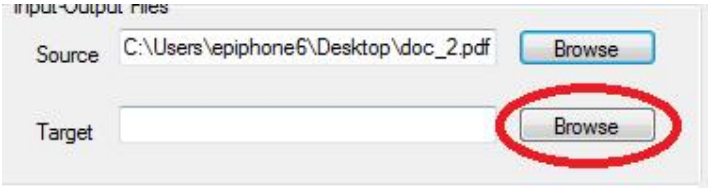
Εικόνα 41. Επιλογή του Button Browse(Αναζήτηση)



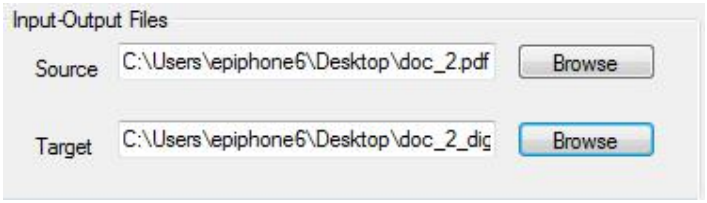
Εικόνα 42. Αποδοχή Επιλεχθέντος Αρχείου

Πεδίο 2

Στο πεδίο 1 ο χρήστης καλείται να ορίσει τον φάκελο στο οποίο επιθυμεί να αποθηκεύσει το ψηφιακά υπογεγραμμένο αρχείο.



Εικόνα 43. Επιλογή του Button Browse (Αναζήτηση)

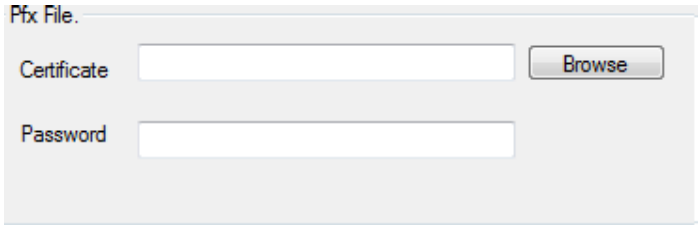


Εικόνα 44.Αποδοχή Επιλεχθέντος Σημείου Αποθήκευσης

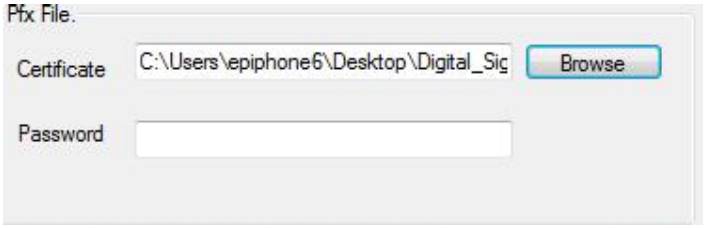
Πεδίο 3

PDF created with pdfFactory Pro trial version www.pdffactory.com

Στο πεδίο 1 ο χρήστης καλείται να εισάγει το πιστοποιητικό με το οποίο θα υπογραφεί ψηφιακά το αρχείο. Σημειώνεται ότι το πιστοποιητικό πρέπει να είναι με κατάληξη .pfx.



Εικόνα 45.Επιλογή πιστοποιητικού



Εικόνα 46. Αποδοχή Επιλεχθέντος Πιστοποιητικού.

Πεδίο 4

Στο πεδίο 1 ο χρήστης καλείται να εισάγει το password του εισαχθέν πιστοποιητικού.

Εικόνα 47. Εισαγωγή Κωδικού

Στο σημείο αυτό θα γίνει μια αναλυτική παρουσίαση των πιστοποιητικών για να γίνει αντιληπτό η χρησιμότητα και η λειτουργία των.

PDF created with pdfFactory Pro trial version www.pdffactory.com

12. Πιστοποιητικά

Το Κέντρο Λειτουργίας Δικτύου ΑΠΘ (για συντομία ΚΛΔ) παρέχει την υπηρεσία έκδοσης και υποστήριξης ψηφιακών πιστοποιητικών σε όλους τους κατόχους Λογαριασμού Χρήστη στο ΚΛΔ, οι οποίοι πληρούν τις προϋποθέσεις των κειμένων πολιτικής και διαδικασιών http://www.pki.auth.gr/documents/CPS.php Η ανάγκη προστασίας δεδομένων καθώς και η ασφαλής ηλεκτρονική επικοινωνία που επιτάσσουν οι αυξανόμενες ηλεκτρονικές συναλλαγές στο διαδίκτυο, οδήγησαν στην δημιουργία υποδομής και χρήση των ψηφιακών πιστοποιητικών. Πρόκειται για μια ραγδαία εξελισσόμενη τεχνολογική περιοχή που επηρεάζει άμεσα τους χρήστες του διαδικτύου.

12.1 Τι είναι και πού χρησιμοποιούνται τα ψηφιακά πιστοποιητικά;

Το προσωπικό ψηφιακό πιστοποιητικό πιστοποιεί την ταυτότητα του κατόχου του σε τρίτους και παρέχει στους τελευταίους τα μέσα ελέγχου της εγκυρότητας αυτής της ταυτότητας. Η έκδοσή του βασίζεται στις αρχές της επιστήμης της Κρυπτογραφίας.

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται από τους τελικούς χρήστες κατά κύριο λόγο στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου. Το κοινό ηλεκτρονικό ταχυδρομείο δεν εξασφαλίζει την ταυτότητα του αποστολέα ούτε την ακεραιότητα του περιεχομένου του μηνύματος, σε αντίθεση με το ασφαλές ηλεκτρονικό. Το τελευταίο, βασίζεται στο πρωτόκολλο S/MIME (Secure Multipurpose Internet Mail Extensions), που υποστηρίζεται από τις τελευταίες εκδόσεις λογισμικού διαχείρισης ηλεκτρονικού ταχυδρομείου (πχ Outlook Express, Mozilla Thunderbird).

Ειδικά, το ασφαλές ηλεκτρονικό ταχυδρομείο (Secure Email) παρέχει τις εξής εγγυήσεις:

Απόδειξη ταυτότητας (Authentication)

Οι παραλήπτες ενός μηνύματος που έχει υπογραφεί ψηφιακά, μπορούν να ελέγξουν την εγκυρότητα της ταυτότητας του αποστολέα .

Ακεραιότητα (Integrity)

Οι παραλήπτες ενός μηνύματος που έχει υπογραφεί ψηφιακά, μπορούν να είναι βέβαιοι για το αμετάβλητο του περιεχομένου του μηνύματος που έχει σταλεί.

- **Εμπιστευτικότητα (Confidentiality)**

Οι παραλήπτες ενός μηνύματος που έχει υπογραφεί ψηφιακά και έχει κρυπτογραφηθεί, μπορούν να είναι βέβαιοι ότι κανείς τρίτος δεν είχε τη δυνατότητα να διαβάσει το περιεχόμενο του μηνύματος.

- **Μη απόρριψη υποχρέωσης (Non repudiation)**

Οι αποστολείς ενός μηνύματος που έχει υπογραφεί ψηφιακά δεν μπορούν να απαρνηθούν την αποστολή του μηνύματος.

Μια άλλη δικτυακή υπηρεσία που σχετίζεται με την χρήση ψηφιακών πιστοποιητικών είναι η πλοήγηση σε ασφαλείς δικτυακούς τόπους/ιστοσελίδες. Η προσπέλαση των δικτυακών τόπων που χαρακτηρίζονται ασφαλείς, χρησιμοποιούν

PDF created with pdfFactory Pro trial version www.pdffactory.com

ψηφιακά πιστοποιητικά εξυπηρετητών (με ενεργοποίηση πρωτοκόλλου SSL) και με τεχνολογίες κρυπτογράφησης εξασφαλίζουν το απόρρητο της επικοινωνίας. Το αποτέλεσμα είναι τα στοιχεία που ο χρήστης πληκτρολογεί και "στέλνει" προς τον ιστοχώρο να μην μπορούν να διαβαστούν από τρίτους.

Επιπλέον, υπάρχουν εξυπηρετητές ιστοσελίδων (Web Servers) που απαιτούν "ισχυρή" απόδειξη της ταυτότητας του χρήστη για να παρέχουν δικτυακές υπηρεσίες. Όλοι οι σύγχρονοι πλοηγοί (πχ Internet Explorer, Mozilla, Safari), παρέχουν τη δυνατότητα πιστοποίησης ταυτότητας με την χρήση ψηφιακών πιστοποιητικών (Web Authentication). Τέλος, "ισχυρή" απόδειξη ταυτότητας απαιτεί και η υπηρεσία "εικονικού" δικτύου (VPN) που παρέχει το ΚΛΔ.

12.2 Κανονισμοί χρήσης & Οδηγίες

Το ψηφιακό πιστοποιητικό ενός χρήστη είναι για τον ηλεκτρονικό κόσμο το ανάλογο της αστυνομικής ταυτότητας, γι' αυτό και η χρήση του επιβάλλεται να είναι αυστηρά προσωπική. Τονίζεται ότι το Κέντρο Λειτουργίας και Διαχείρισης Δικτύου δε φέρει καμία ευθύνη για τυχόν απώλεια ή λανθασμένη χρήση του ψηφιακού πιστοποιητικού.

Για να αποκτήσετε το προσωπικό σας ψηφιακό πιστοποιητικό θα πρέπει:

- Να εμπιστευτείτε την Κεντρική Αρχή Πιστοποίησης του ΑΠΘ ως βασική αρχή έκδοσης πιστοποιητικών. Η διαδικασία που πρέπει να ακολουθήσετε περιγράφεται λεπτομερώς στις ιστοσελίδες της υπηρεσίας Υποδομής Δημοσίου Κλειδιού του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης.

- Να έχετε εγκατεστημένο τον πλοηγό IE (έκδοση 6+ ή μεγαλύτερη) ή Mozilla (έκδοση 1.6 ή μεγαλύτερη) ή FireFox (έκδοση 1 ή μεγαλύτερη) ή Safari για υπολογιστή MAC.

- Να αιτηθείτε την έκδοση προσωπικού ψηφιακού πιστοποιητικού από τον υπολογιστή σας με την χρήση του πλοηγού που χρησιμοποιείτε για ηλεκτρονικό ταχυδρομείο από τη σελίδα https://www.pki.auth.gr/secure/issue_user.php.el. Θα σας ζητηθεί η ηλεκτρονική σας διεύθυνση και ο κωδικός πρόσβασης που έχετε αποκτήσει από το ΚΛΔ.

ΠΡΟΣΟΧΗ: Αν επιθυμείτε να αποκτήσετε προσωπικό ψηφιακό πιστοποιητικό για να χρησιμοποιήσετε την υπηρεσία εικονικού ιδιωτικού δικτύου (Virtual Private Network - VPN) του ΚΛΔ, συνιστάται να χρησιμοποιήσετε internet explorer για την υποβολή της αίτησης έκδοσης και για την παραλαβή του πιστοποιητικού σας.

12.3 Η Αρχή Πιστοποίησης του ΑΠΘ

Οι χρήστες που ανταλλάσουν μεταξύ τους μηνύματα ασφαλούς ταχυδρομείου ή συνδέονται σε ασφαλείς δικτυακούς τόπους (sites), πρέπει να εμπιστεύονται μια κοινή Αρχή, υπεύθυνη για την αξιοπιστία έκδοσης των Πιστοποιητικών. Λόγω της έλλειψης ενός παγκόσμια αποδεκτού μη εμπορικού φορέα Πιστοποίησης, το ΑΠΘ υλοποίησε Αρχή Πιστοποίησης ειδικά για την Ακαδημαϊκή Κοινότητα. Οι χρήστες του δικτύου μπορούν να απολαμβάνουν όλες τις υπηρεσίες που σχετίζονται με Ψηφιακά Πιστοποιητικά αρκεί στον υπολογιστή που χρησιμοποιούν να έχουν ρυθμίσει την αποδοχή της Αρχής Πιστοποίησης του ΑΠΘ.

PDF created with pdfFactory Pro trial version www.pdffactory.com

12.4 Σημαντικές πληροφορίες για την Αίτηση Ψηφιακού Πιστοποιητικού

Η αίτηση πρέπει να γίνεται χρησιμοποιώντας προσωπικούς υπολογιστές και όχι υπολογιστές νησίδων ή δημοσίας χρήσης. Κατά τη διαδικασία της αίτησης, ο πλοηγός (browser) του συγκεκριμένου υπολογιστή που βρίσκεστε, δημιουργεί ένα ζεύγος κλειδιών (το δημόσιο και το ιδιωτικό) που βασίζονται στην κρυπτογράφηση Δημοσίου Κλειδιού. Το **ιδιωτικό κλειδί αποθηκεύεται στον πλοηγό με τον οποίο γίνεται η αίτηση** και το δημόσιο κλειδί αποστέλλεται στο σύστημα Διαχείρισης Πιστοποιητικών προκειμένου να πιστοποιηθεί από την κατάλληλη Αρχή Πιστοποίησης του ΑΠΘ, ώστε να παραχθεί το τελικό Ψηφιακό Πιστοποιητικό σας. Στη συνέχεια θα λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που θα σας ειδοποιεί να το παραλάβετε το Ψηφιακό Πιστοποιητικό σας. Τότε **θα πρέπει πραγματοποιήσετε την παραλαβή από τον ίδιο υπολογιστή και πλοηγό (browser) που πραγματοποιήσατε την αίτηση**, διότι θα πρέπει να παρουσιάσετε στο σύστημα Διαχείρισης Πιστοποιητικών το ιδιωτικό κλειδί που αντιστοιχεί στο Πιστοποιητικό που πρόκειται να παραλάβετε.

Το μυστικό κλειδί θα βρίσκεται πάντα αποθηκευμένο στον πλοηγό του υπολογιστή της αρχικής αίτησης. Συνεπώς, θα μπορείτε να παραλάβετε όσες φορές θέλετε το πιστοποιητικό σας, αρκεί να βρίσκεστε στον ίδιο υπολογιστή/πλοηγό που κάνατε την αρχική αίτηση.

Για τη διαδικασία απόκτησης-χρήσης-ακύρωσης των ψηφιακών πιστοποιητικών, μπορείτε να επισκεφθείτε τις σελίδες οδηγών που έχει ετοιμάσει το ΚΛΔ.

Προκειμένου να στείλετε ένα κρυπτογραφημένο μήνυμα σε ένα χρήστη, είναι απαραίτητο να έχετε πρόσβαση στο ψηφιακό του Πιστοποιητικό. Αυτό μπορείτε να το αναζητήσετε μέσω της υπηρεσίας καταλόγου του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης.

12.5 Συχνές Ερωτήσεις & Απαντήσεις

Τα ψηφιακά πιστοποιητικά είναι αποδεικτικά ταυτότητας σε ηλεκτρονικές συναλλαγές. Ο κάτοχός τους μπορεί να τα χρησιμοποιήσει για να αποδείξει την ταυτότητά του, όπως αυτή αναγράφεται στο πιστοποιητικό, το οποίο είναι υπογεγραμμένο από κάποια Αρχή κοινής εμπιστοσύνης. Η λειτουργία τους είναι αντίστοιχη των αστυνομικών ταυτοτήτων και η έκδοση τους γίνεται από Αρχές που εμπιστεύονται οι ίδιοι οι χρήστες μεταξύ τους. Για την Ακαδημαϊκή και Ερευνητική κοινότητα χρηστών, δημιουργήθηκε μια Αρχή Πιστοποίησης που παρέχει ψηφιακά πιστοποιητικά κοινής αποδοχής από τους χρήστες της.

Σε τι μου χρησιμεύει η απόκτηση προσωπικού ψηφιακού πιστοποιητικού;

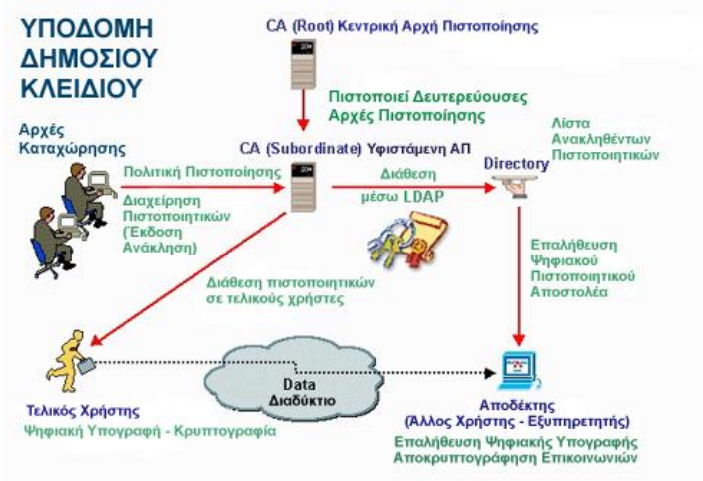
Τα προσωπικά ψηφιακά πιστοποιητικά χρησιμοποιούνται κυρίως για την απόδειξη της ταυτότητάς του κατόχου, αλλά και για την κρυπτογράφηση ευαίσθητου περιεχομένου σε ηλεκτρονικές πράξεις. Το κοινό ηλεκτρονικό ταχυδρομείο δεν εξασφαλίζει ούτε την ταυτότητα του αποστολέα ούτε την ακεραιότητα του περιεχομένου. Η υπογραφή ενός e-mail μέσω του προσωπικού πιστοποιητικού μου, αποδεικνύει στον παραλήπτη ότι το έστειλα πράγματι εγώ, καθώς και ότι το περιεχόμενό του δεν έχει αλλοιωθεί από κάποιον τρίτο, από την αποστολή μέχρι την παραλαβή του. Μια ακόμη χρήση του πιστοποιητικού μου είναι η δυνατότητα να μου

PDF created with pdfFactory Pro trial version www.pdffactory.com

αποσταλούν κρυπτογραφημένα μηνύματα που μόνο εγώ μπορώ να διαβάσω. Ένα ψηφιακό πιστοποιητικό ανήκει στην Υποδομή Δημόσιου Κλειδιού (ΥΔΚ), δηλαδή σε ένα σύστημα έκδοσης, χρησιμοποίησης και ακύρωσης ψηφιακών πιστοποιητικών τόσο για χρήστες όσο και για εξυπηρετητές δικτύου.

Τι είναι η Υποδομή Δημόσιου Κλειδιού;

Η Υποδομή Δημόσιου Κλειδιού είναι ένας συνδυασμός από λογισμικό, τεχνολογίες κρυπτογράφησης, διεργασίες και υπηρεσίες που καταστούν δυνατή την σύνθεση μιας υποδομής για ασφαλείς διαδικτυακές επικοινωνίες. Η δυνατότητα μίας τέτοιας υποδομής να μπορεί να προσφέρει εμπιστευτικές επικοινωνίες είναι βασισμένη στην ανταλλαγή ψηφιακών πιστοποιητικών μεταξύ εξουσιοδοτημένων χρηστών και διαπιστευμένων δικτυακών πόρων.



Εικόνα 48. Υποδομή Δημοσίου Κλειδιού

Τα ψηφιακά πιστοποιητικά βασίζονται στις έννοιες ενός προσωπικού και ενός δημόσιου κλειδιού. Το δημόσιο κλειδί ενός χρήστη είναι διαθέσιμο στον οποιονδήποτε άλλο χρήστη στην αποκρυπτογραφημένη (απλή) μορφή του. Χρησιμοποιείται από οποιονδήποτε θελήσει να σας στείλει κάποιο υπογεγραμμένο ή κρυπτογραφημένο μήνυμα. Αντιθέτως το ιδιωτικό κλειδί σας είναι μυστικό από οποιονδήποτε άλλο και συνήθως προστατεύεται από κάποιον προσωπικό κωδικό πρόσβασης. Είναι ακατόρθωτο να μπορέσει να παραχθεί το ιδιωτικό κλειδί σας από το κοινώς διαδεδομένο δημόσιο.

Τι περιέχει και τι μορφή έχει το ψηφιακό πιστοποιητικό μου;

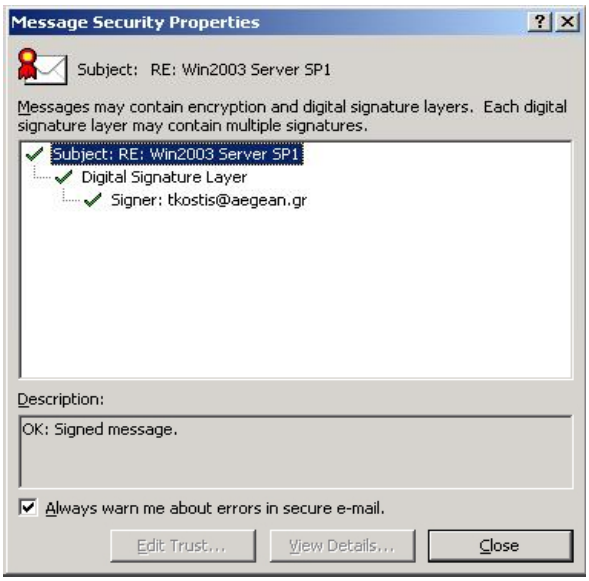
Το προσωπικό ψηφιακό πιστοποιητικό περιέχει τα στοιχεία μου και το δημόσιο κλειδί μου (μια κωδικωσειρά δημοσίως γνωστή) υπογεγραμμένα από την Αρχή Πιστοποίησης που το εκδίδει. Σε αυτή την περίπτωση είναι η Κεντρική Αρχή Πιστοποίησης από την Υποδομή Δημοσίου Κλειδιού ΑΠΘ. Για να εκδοθεί το πιστοποιητικό απαιτείται η ταυτοποίηση των στοιχείων με τον αιτούμενο χρήστη,

PDF created with pdfFactory Pro trial version www.pdffactory.com

που γίνεται μέσω των κατάλληλων ιστοσελίδων, εφόσον ήδη έχει λογαριασμό χρήστη σε φορέα συνεργαζόμενο με την Υποδομή Δημοσίου Κλειδιού ΑΠΘ.

Πώς χρησιμοποιώ το ψηφιακό πιστοποιητικό μου;

Το προσωπικό ψηφιακό πιστοποιητικό εγκαθίσταται στον πλοηγό (browser) και στο πρόγραμμα διαχείρισης ηλεκτρονικού ταχυδρομείου μου, μετά την απόκτησή του από την κατάλληλη ιστοσελίδα. Τα προγράμματα αυτά το χρησιμοποιούν αυτόματα, όταν ζητήσω να υπογράψω κάποιο e-mail π.χ. Οι ρυθμίσεις γίνονται συνήθως κατά την εγκατάσταση του πιστοποιητικού και σαν προεπιλογή χρησιμοποιείται από τα προγράμματα η υπογραφή των ηλεκτρονικών μηνυμάτων κατά την αποστολή τους. Ακολουθεί ένα παράδειγμα ενός μηνύματος ηλεκτρονικού ταχυδρομείου που έχει υπογραφεί από ένα ψηφιακό πιστοποιητικό.



Εικόνα 49.Ρυθμίσεις Ασφαλείας Μηνύματος

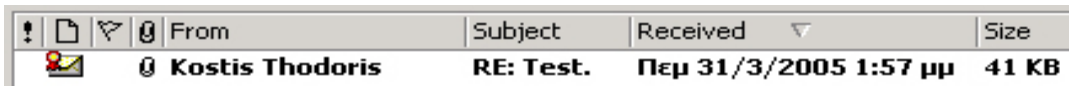
Γιατί πρέπει να αποδεχθώ την Αρχή Πιστοποίησης από την Υποδομή Δημοσίου Κλειδιού ΑΠΘ;

Η ταυτότητα του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι δυνατό να επιβεβαιωθεί και να την αποδεχτεί το πρόγραμμά μου ως παραλήπτη, μόνο αν έχω ήδη αποδεχθεί την Αρχή Πιστοποίησης που έχει εκδώσει το πιστοποιητικό του αποστολέα. Καθώς δεν υπάρχουν μη εμπορικές Αρχές Πιστοποίησης με διεθνή εμβέλεια, ομάδες χρηστών που συνεργάζονται πρέπει να αποδέχονται μια Αρχή κοινής εμπιστοσύνης. Για το λόγο αυτό, όσοι επιθυμούν να δέχονται μηνύματα υπογεγραμμένα από χρήστες που συμμετέχουν στην Υποδομή Δημοσίου Κλειδιού ΑΠΘ, θα πρέπει να αποδεχθούν την Αρχή Πιστοποίησης. Ταυτόχρονα, μπορούν να προτρέπουν και συνεργάτες τους να κάνουν το ίδιο, αν θέλουν να δέχονται μηνύματα τους.

Πώς καταλαβαίνω ότι ένα e-mail που έλαβα είναι υπογεγραμμένο; Τι μου εξασφαλίζει αυτό;

PDF created with pdfFactory Pro trial version www.pdffactory.com

Όλα τα προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου μπορούν να αναγνωρίσουν και να επαληθεύσουν ψηφιακά πιστοποιητικά. Όταν ανιχνεύσουν ένα υπογεγραμμένο μήνυμα εμφανίζουν ένα εικονίδιο που ενημερώνει για την ύπαρξη υπογραφής.

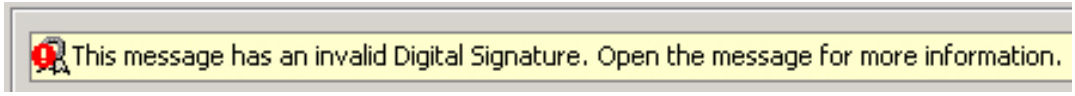


Εικόνα 50. Λήψη ψηφιακού υπογεγραμμένου ηλεκτρονικού μηνύματος

Επίσης θα πρέπει να εμφανίζεται η ένδειξη ότι το μήνυμα είναι "υπογεγραμμένο" (signed).

Εικόνα 51. Στοιχεία του Ατόμου που υλοποίησε την Ψηφιακή Υπογραφή

Τότε και μόνο τότε εξασφαλίζεται η πιστοποίηση της ταυτότητας του αποστολέα, η ακεραιότητα του περιεχομένου του μηνύματος καθώς και το ότι ο αποστολέας δεν μπορεί να αποποιηθεί την αποστολή. Επιπλέον, αν η ένδειξη είναι "κρυπτογραφημένο" (encrypted), ο αποστολέας θέλει να εξασφαλίσει ότι μόνο εγώ μπορώ να διαβάσω τα περιεχόμενα του μηνύματος, και έχει χρησιμοποιήσει κρυπτογράφηση με το δικό μου δημόσιο κλειδί. Αν το μήνυμα είναι υπογεγραμμένο, αλλά δεν μπορεί να επαληθευτεί το πιστοποιητικό του αποστολέα, εμφανίζεται σχετική ειδοποίηση (invalid signature).



Εικόνα 52. Υπόδειξη για μη έγκυρη Ψηφιακή Υπογραφή

Πιθανοί λόγοι μπορεί να είναι ότι ο χρήστης δεν έχει αποδεχτεί την Αρχή Πιστοποίησης από την Υποδομή Δημοσίου Κλειδιού ΑΠΘ, ή ότι το πιστοποιητικό του έχει λήξει ή έχει ανακληθεί.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Πώς στέλνω ένα υπογεγραμμένο και κρυπτογραφημένο e-mail;

Το πρόγραμμα διαχείρισης ηλεκτρονικού ταχυδρομείου μου δίνει τη δυνατότητα να υπογράψω και να κρυπτογραφήσω e-mails, αφού εισάγω στο πρόγραμμα το πιστοποιητικό μου. Ενεργοποιώντας την επιλογή υπογραφής των μηνυμάτων θα μπορώ να στέλνω κάθε μήνυμα υπογεγραμμένο. Για να κρυπτογραφήσω ένα e-mail θα πρέπει να έχω το πιστοποιητικό του παραλήπτη αποθηκευμένο στον υπολογιστή μου για να χρησιμοποιήσω το δημόσιο κλειδί του κατά την αποστολή. Η εύρεση και αποθήκευση των πιστοποιητικών άλλων χρηστών μπορεί να γίνει μέσα από την υπηρεσία εύρεσης πιστοποιητικών από την Υποδομή Δημοσίου Κλειδιού ΑΠΘ.

Πώς καταλαβαίνω ότι ένα web site έχει ψηφιακό πιστοποιητικό; Τι μου εξασφαλίζει αυτό;

Κάθε φορά που συνδέομαι σε ένα site που έχει ψηφιακό πιστοποιητικό ο πλοηγός (browser) χρησιμοποιεί διαφορετικό πρωτόκολλο επικοινωνίας εμφανίζεται https αντί για http στη διεύθυνση του site). Επίσης, βλέπω ότι υπάρχει ένα εικονίδιο κλειδωμένης κλειδαριάς στο περιβάλλον του πλοηγού. Η παρουσία ψηφιακού πιστοποιητικού του site μου εξασφαλίζει την πιστοποίηση της ταυτότητας του υπολογιστή που φιλοξενεί το site καθώς και την κρυπτογραφημένη επικοινωνία μεταξύ του υπολογιστή μου και του απομακρυσμένου site που επισκέπτομαι.

Πώς χρησιμοποιώ το προσωπικό ψηφιακό πιστοποιητικό μου για είσοδο σε ένα web site;

Ορισμένα web sites δίνουν τη δυνατότητα εισόδου σε περιορισμένους χρήστες παίρνοντας αυξημένα μέτρα ασφαλείας, δηλαδή απαιτούν όχι απλώς την εισαγωγή κάποιου κωδικού χρήστη, αλλά την επίδειξη κάποιου προσωπικού πιστοποιητικού από τον πλοηγό του χρήστη, ελέγχοντας όχι μόνο την ταυτότητά του, αλλά και την Αρχή που το εξέδωσε. Σε αυτές τις σπάνιες περιπτώσεις, ο χρήστης ενημερώνεται από τον πλοηγό του, ώστε να υποδείξει το προσωπικό πιστοποιητικό που θέλει να χρησιμοποιηθεί για την είσοδο του, και αν περάσει τον έλεγχο του web site, του επιτρέπεται η πρόσβαση. Αυτή η διαδικασία είναι ασφαλέστερη από την χρήση κάποιου κωδικού, αλλά και απλούστερη για τον χρήστη.

Πώς προστατεύω το ψηφιακό πιστοποιητικό μου;

Το προσωπικό ψηφιακό πιστοποιητικό μου αποθηκεύεται στο πρόγραμμα διαχείρισης του ηλεκτρονικού ταχυδρομείου και του πλοηγού στον υπολογιστή μου, κατά την ολοκλήρωση της διαδικασίας της αίτησής μου για απόκτηση του. Όταν ο υπολογιστής που χρησιμοποιώ χρησιμοποιείται αποκλειστικά από μένα, δεν υπάρχει άμεσα ο κίνδυνος να βρεθεί σε χέρια τρίτων και κάποιος να το χρησιμοποιήσει παράνομα υποδυόμενος εμένα. Όταν όμως ο υπολογιστής είναι κοινόχρηστος, πρέπει να πάρω ειδικά μέτρα. Δηλαδή, κατά την αποθήκευση του πιστοποιητικού στο πρόγραμμα του πλοηγού να χρησιμοποιήσω έναν κρυφό κωδικό χρήσης, για να εξασφαλίσω ότι το πιστοποιητικό θα χρησιμοποιείται αποκλειστικά από μένα.

Πώς μεταφέρω το ψηφιακό πιστοποιητικό μου σε άλλο υπολογιστή;

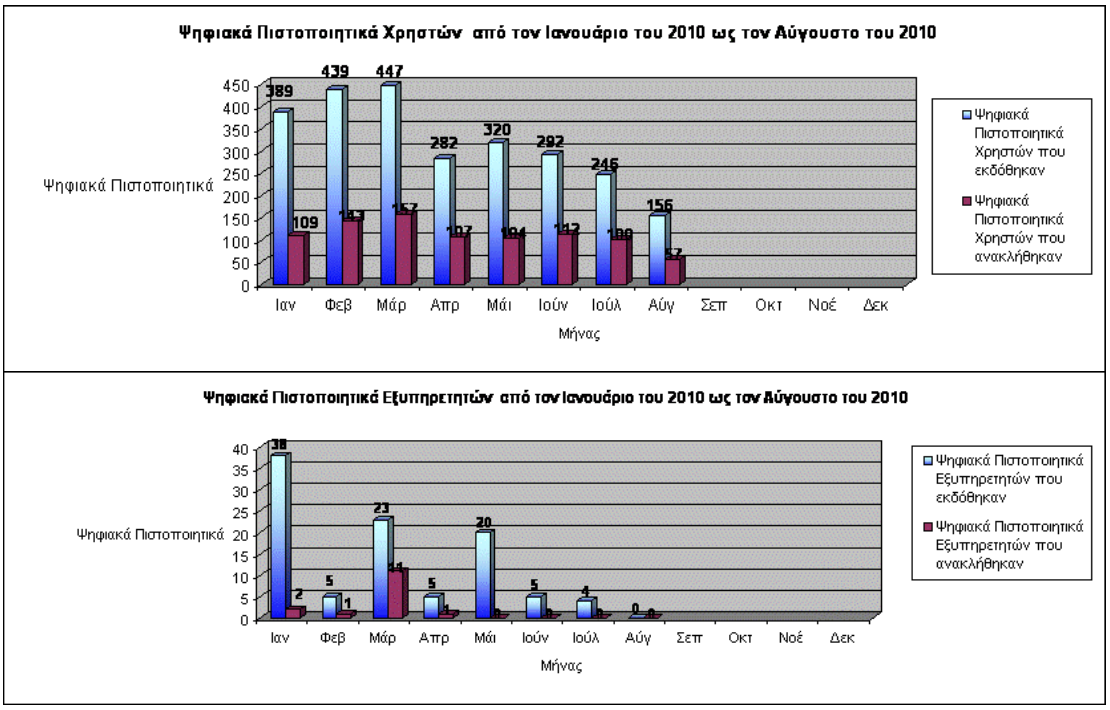
Τα προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου και οι πλοηγοί (browsers) στον υπολογιστή όπου έχω εγκαταστήσει το ψηφιακό πιστοποιητικό μου, έχουν τη δυνατότητα εξαγωγής (export) του σε ένα αρχείο. Η μεταφορά του αρχείου αυτού μπορεί να γίνει με οποιονδήποτε ασφαλή τρόπο (δισκέτα, CD-RW), και η

PDF created with pdfFactory Pro trial version www.pdffactory.com

εγκατάσταση του σε άλλο υπολογιστή μου με την διαδικασία εισαγωγής (import) στον πλοηγό (browser). Είναι όμως εξαιρετικά κρίσιμο να φροντίσω για την καταστροφή των αντιγράφων, ώστε να μην γίνουν ποτέ διαθέσιμα σε τρίτους, ιδίως αν το αρχείο μου αυτό δεν προστατεύεται με κωδικό χρήσης.

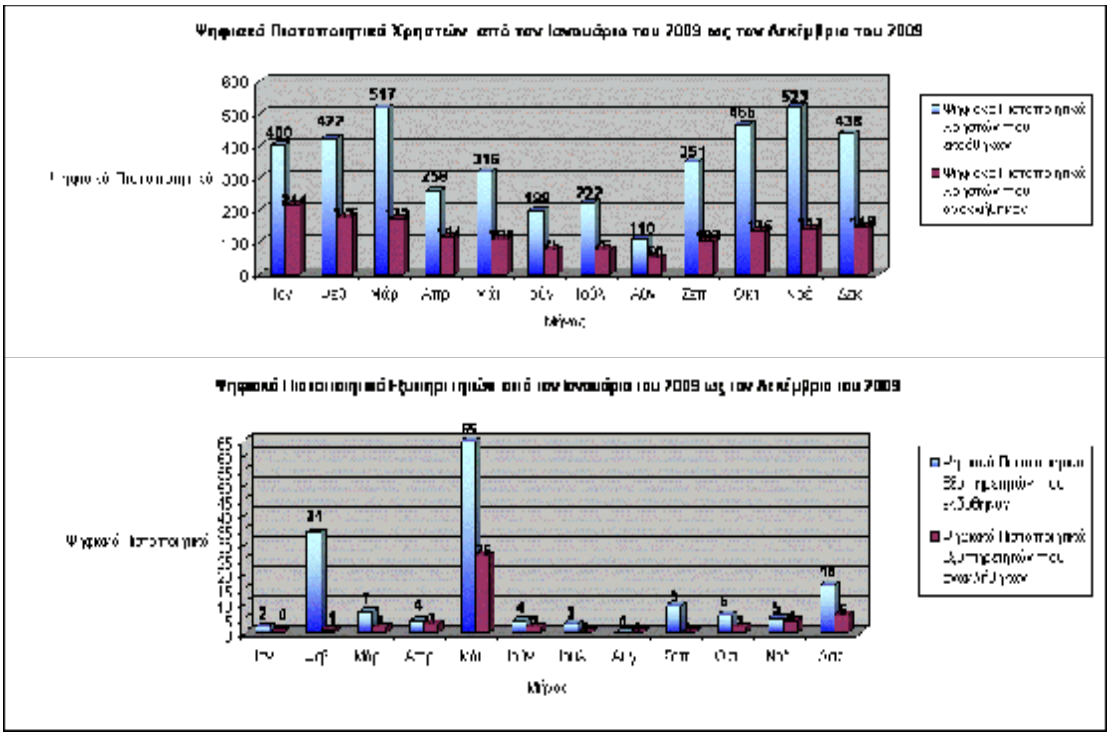
12.6 Στατιστικά υπηρεσίας Υποδομής Δημοσίου Κλειδιού

Στη σελίδα αυτή παρουσιάζονται τα στατιστικά της υπηρεσίας Υποδομής Δημοσίου Κλειδιού(Public Key Infrastructure) που διαχειρίζεται το Κέντρο Λειτουργίας Δικτύου ΑΠΘ. Παρακάτω φαίνονται τα αιτήματα που εξυπηρετήθηκαν και αφορούσαν σε έκδοση και σε ανάκληση ψηφιακών πιστοποιητικών χρηστών καθώς και εξυπηρετητών **για το έτος 2010*:**



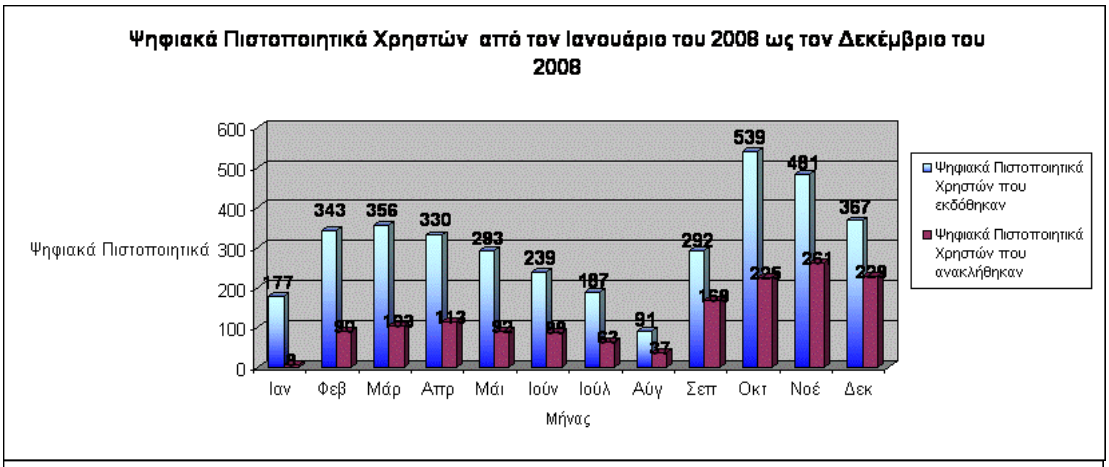
Παρακάτω φαίνονται τα αιτήματα που εξυπηρετήθηκαν και αφορούσαν σε έκδοση και σε ανάκληση ψηφιακών πιστοποιητικών χρηστών καθώς και εξυπηρετητών **για το έτος 2009:**

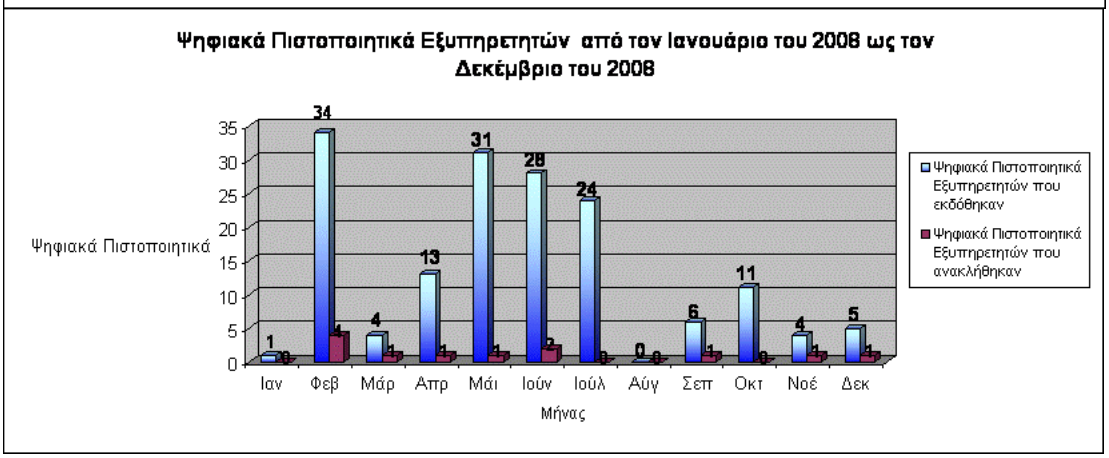
PDF created with pdfFactory Pro trial version www.pdffactory.com



Παρακάτω φαίνονται τα αιτήματα που εξυπηρετήθηκαν και αφορούσαν σε έκδοση και σε ανάκληση ψηφιακών πιστοποιητικών χρηστών καθώς και εξυπηρετητών **για το έτος 2008:**

PDF created with pdfFactory Pro trial version www.pdffactory.com





PDF created with pdfFactory Pro trial version www.pdffactory.com

12.7 Ψηφιακό Πιστοποιητικό Ασφαλείας (SSL 128 bit)

12.7.1 Πως λειτουργεί το SSL;

Εικόνα 53. Λειτουργία SSL ψηφιακού Πιστοποιητικού

- ✓ Με το SSL, ο υπολογιστής του χρήστη, μέσω του οποίου πρόκειται να πραγματοποιηθεί κρυπτογραφημένη SSL επικοινωνία, στέλνει το αίτημα του στο server, ο οποίος κάνει χρήση ψηφιακού πιστοποιητικού ασφαλείας και φιλοξενεί το web site με το οποίο πρόκειται να πραγματοποιηθεί η ηλεκτρονική συναλλαγή.
- ✓ Ο Server στέλνει: α) το πιστοποιητικό ασφαλείας στον υπολογιστή του χρήστη και του επιβεβαιώνει πως έχει επισκεφτεί την σωστή σελίδα και β) το δημόσιο κλειδί του (κωδικός).
- ✓ Ο υπολογιστής του χρήστη, χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει απόρρητες πληροφορίες (πχ. τον αριθμό της πιστωτικής του κάρτας).
- ✓ Στη συνέχεια οι πληροφορίες αυτές αποστέλλονται στον server που χρησιμοποιεί το ιδιωτικό του κλειδί για να τις αποκρυπτογραφήσει.

12.7.2 Με τα Ψηφιακά Πιστοποιητικά Ασφαλείας έχετε την δυνατότητα:

1. Να βελτιώσετε την παρουσία του web site σας.
2. Να προσφέρετε την πιο αξιόπιστη λύση για την πιστοποίηση του web site σας.

PDF created with pdfFactory Pro trial version www.pdffactory.com

3. Να επιδείξετε την ηλεκτρονική σας ταυτότητά του web site σας - όπως αυτή αναγράφεται στο πιστοποιητικό, το οποίο είναι υπογεγραμμένο από έμπιστη Αρχή Πιστοποίησης.

4. Να βελτιώσετε τα επίπεδα ασφάλειας στο web site σας.

5. Να αυξήσετε την εμπιστοσύνη των επισκεπτών σας, για να πραγματοποιήσουν ηλεκτρονικές συναλλαγές και κάθε είδους ηλεκτρονική επικοινωνία μέσα από τον δικτυακό σας τόπο.

12.7.3 Αποκτήστε τώρα Ψηφιακό Πιστοποιητικό Ασφαλείας για να εξασφαλίσετε στους επισκέπτες του web site σας κρυπτογραφημένη SSL 128 bit.

- Για τις συναλλαγές μέσω του Ηλεκτρονικού σας Καταστήματος (E-Shop), όπου απαιτείται η χρήση πιστωτικής κάρτας.
- Για φόρμες επικοινωνίας, όπου απαιτείται ο επισκέπτης να εισάγει ευαίσθητα προσωπικά δεδομένα όπως διεύθυνση, ημερομηνία γέννησης, αριθμό ταυτότητας ή διαβατηρίου.
- Για τους εταιρικούς σας συνεργάτες, που έχουν πρόσβαση σε κεντρική εμπορική εφαρμογή για να πραγματοποιήσουν ηλεκτρονικές συναλλαγές όπως πχ. παραγγελίες και τιμολόγηση.

12.8 Εγχειρίδιο Χρήσης και Διαχείρισης Ψηφιακών Πιστοποιητικών.

12.8.1 Λήψη αντιγράφου ασφαλείας (export) ψηφιακών πιστοποιητικών

Η λήψη αντιγράφου ασφαλείας των ψηφιακών πιστοποιητικών σας που έχετε εγκαταστήσει στον browser του υπολογιστή σας, σας παρέχει την δυνατότητα:

Να εγκαταστήσετε τα ψηφιακά πιστοποιητικά σας σε διαφορετικό υπολογιστή από αυτόν που χρησιμοποιήσατε για την έκδοσή τους (για παράδειγμα, εάν χρησιμοποιείτε δύο υπολογιστές και θέλετε να μπορείτε να χρησιμοποιείτε και από τους δύο τα πιστοποιητικά).

Να κρατήσετε το αντίγραφο ασφαλείας σε ασφαλές σημείο, ώστε να μπορέσετε να επαναφέρετε τα ψηφιακά σας πιστοποιητικά σε περίπτωση που αυτά διαγραφούν από τον browser του υπολογιστή ή εάν αλλάξετε υπολογιστή.

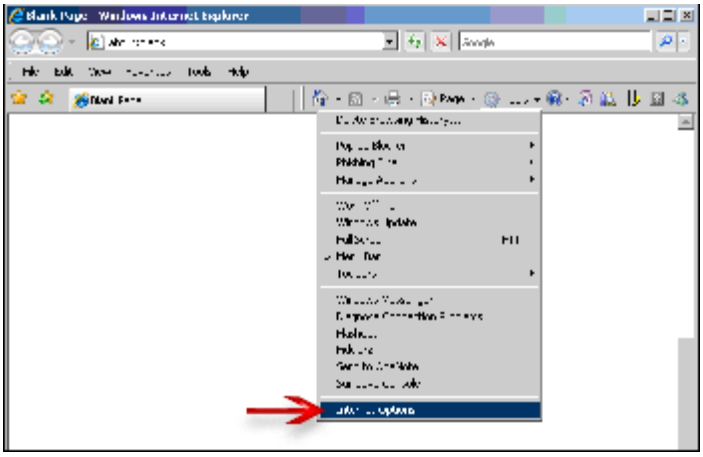
Η διαδικασία λήψης αντιγράφου ασφαλείας διαφέρει, ανάλογα με τον browser στον οποίο είναι εγκατεστημένα τα πιστοποιητικά. Για να εκτελέσετε την διαδικασία, ακολουθήστε τις αντίστοιχες οδηγίες που παρουσιάζονται στις παρακάτω σελίδες.

Σημείωση: Η λήψη αντιγράφου ασφαλείας είναι δυνατή μόνο αν έχετε παραλάβει πιστοποιητικά χαλαρής αποθήκευσης. Τα πιστοποιητικά σκληρής αποθήκευσης δεν είναι δυνατό να αναπαραχθούν (μαζί με το ιδιωτικό κλειδί).

12.8.2 Με χρήση Internet Explorer

Στην μπάρα εργαλείων του Internet Explorer, επιλέγετε «εργαλεία» (tools) και «Επιλογές Internet» (Internet Options), όπως φαίνεται στην εικόνα 50.

PDF created with pdfFactory Pro trial version www.pdffactory.com



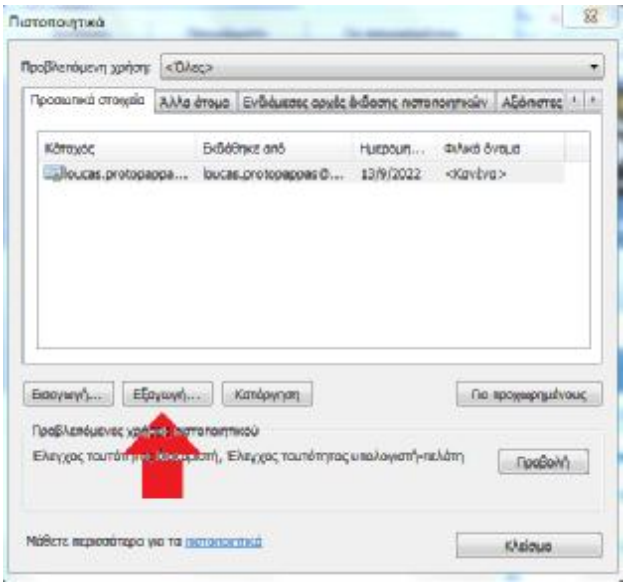
Εικόνα 54. Internet Explorer -- Internet Options

Στο παράθυρο που εμφανίζεται, επιλέξτε την καρτέλα «Περιεχόμενο» (Content). Στην καρτέλα αυτή, επιλέξτε «Πιστοποιητικά» (Certificates).

Εικόνα 55.Internet Explorer -- Internet Option – Content

Στο παράθυρο εμφανίζονται τα ψηφιακά πιστοποιητικά που σας ανήκουν και είναι αποθηκευμένα στον υπολογιστή (εικόνα 3). Επιλέξτε το ψηφιακό πιστοποιητικό που επιθυμείτε να εξάγετε και κάντε κλικ στο «Εξαγωγή» (export), για να εκκινήσετε την διαδικασία εξαγωγής.

PDF created with pdfFactory Pro trial version www.pdffactory.com



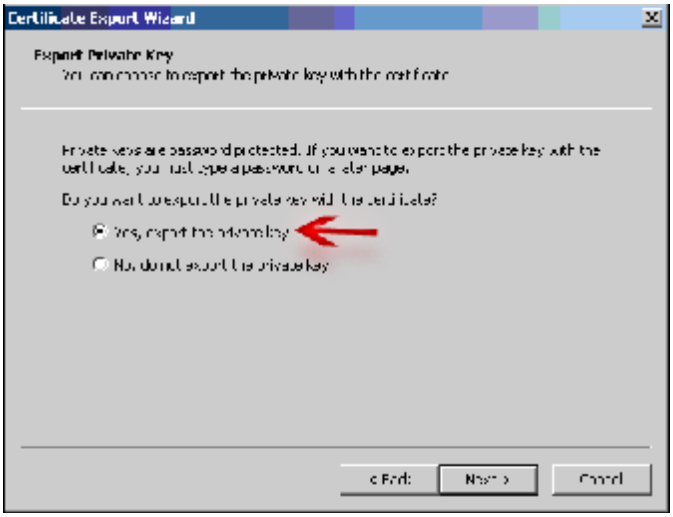
Εικόνα 56. Internet Explorer -- Internet Option – Content -- Export

Στο παράθυρο «Οδηγός εξαγωγής ψηφιακού πιστοποιητικού» που εμφανίζεται, επιλέξτε «Επόμενο» (Next).

Εικόνα 57.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού

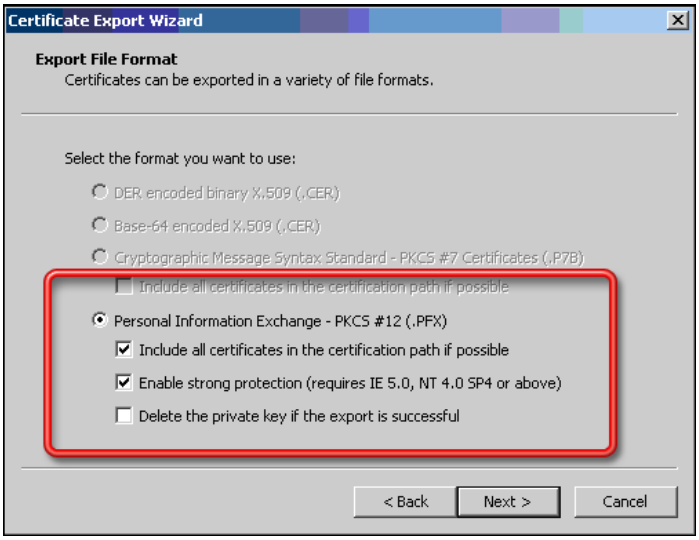
Στο παράθυρο που εμφανίζεται, μην τροποποιήσετε τις προεπιλεγμένες επιλογές, και κάντε κλικ στο «Επόμενο» (Next).

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 58.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού (Βήμα 2)

Στο επόμενο παράθυρο, ενεργοποιήστε τις διαθέσιμες επιλογές ακριβώς όπως φαίνονται στην παρακάτω εικόνα.

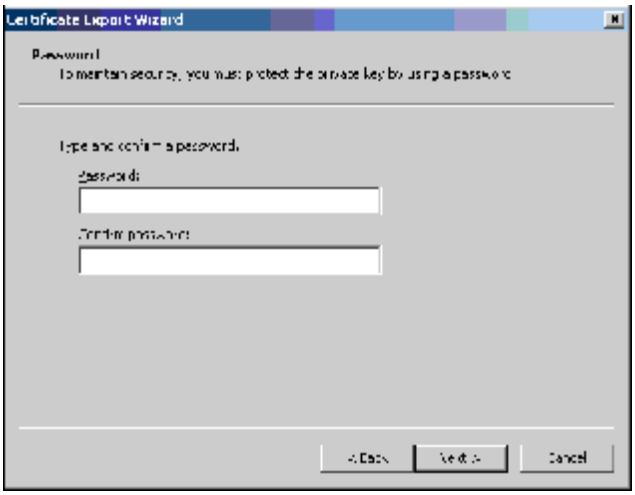


Εικόνα 59.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού (Επιλογές Κωδικοποίησης Πιστοποιητικού)

Στο επόμενο παράθυρο, καλείστε να ορίσετε έναν κωδικό ασφαλείας ο οποίος θα σας ζητηθεί όταν θελήσετε να χρησιμοποιήσετε το αντίγραφο ασφαλείας που δημιουργείτε.

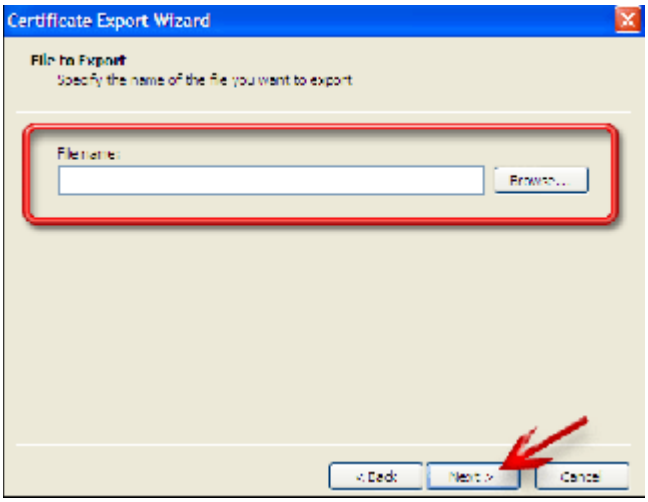
PDF created with pdfFactory Pro trial version www.pdffactory.com

Προσοχή: Σημειώστε σε ασφαλές σημείο τον κωδικό που έχετε ορίσει. Δεν υπάρχει δυνατότητα ανάκτησής του σε περίπτωση απώλειας.



Εικόνα 60.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού (Εισαγωγή Password)

Στο παράθυρο που εμφανίζεται, πληκτρολογήστε στο πεδίο το επιθυμητό όνομα του αρχείου στο οποίο θα αποθηκευθεί το ψηφιακό πιστοποιητικό και επιλέξτε «Επόμενο» για να συνεχίσετε.

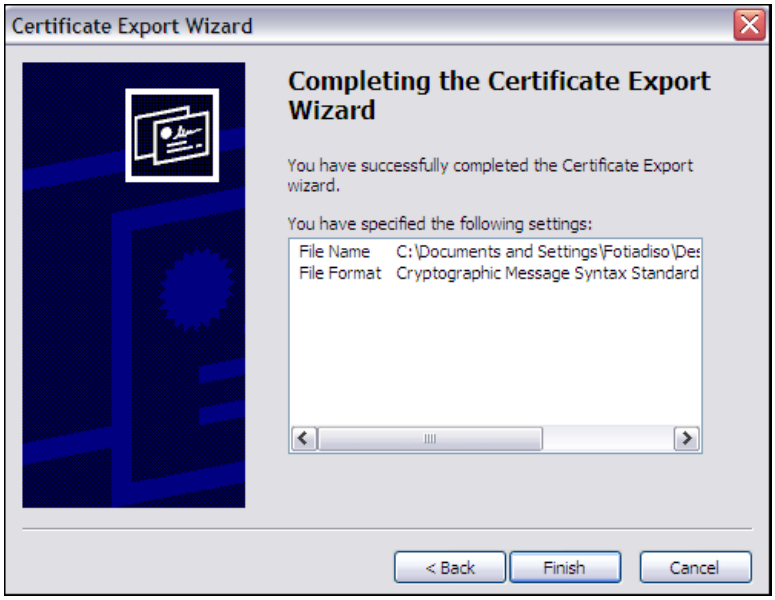


Εικόνα 61.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού (Επιλογή Αρχείου)

PDF created with pdfFactory Pro trial version www.pdffactory.com

Η διαδικασία λήψης αντιγράφου ασφαλείας έχει ολοκληρωθεί με επιτυχία. Στο παράθυρο που εμφανίζεται, επιλέξτε «Ολοκλήρωση» (Finish). Το ψηφιακό πιστοποιητικό έχουν πλέον αποθηκευθεί στο αρχείο που δημιουργήσατε.

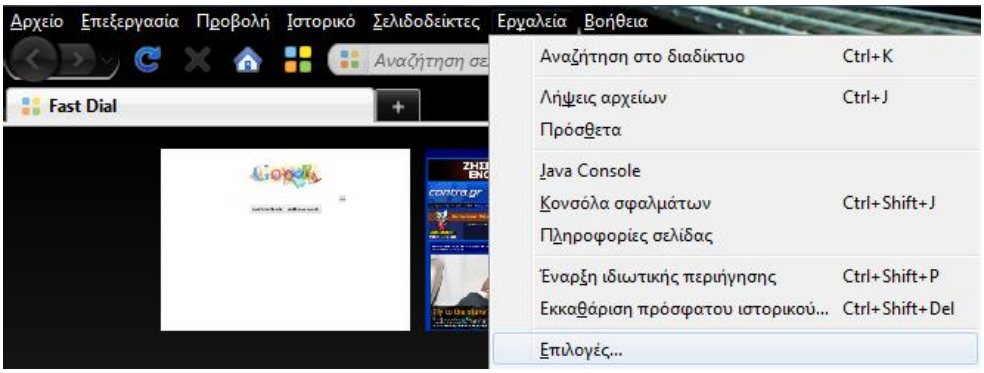
Προσοχή: Μην στείλετε σε καμία περίπτωση το αρχείο που περιέχει το ψηφιακό πιστοποιητικό σε τρίτα πρόσωπα. Προορίζεται αποκλειστικά για δική σας χρήση.



Εικόνα 62.Οδηγός εξαγωγής ψηφιακού πιστοποιητικού (Ολοκλήρωση)

12.8.3 Με χρήση Mozilla Firefox

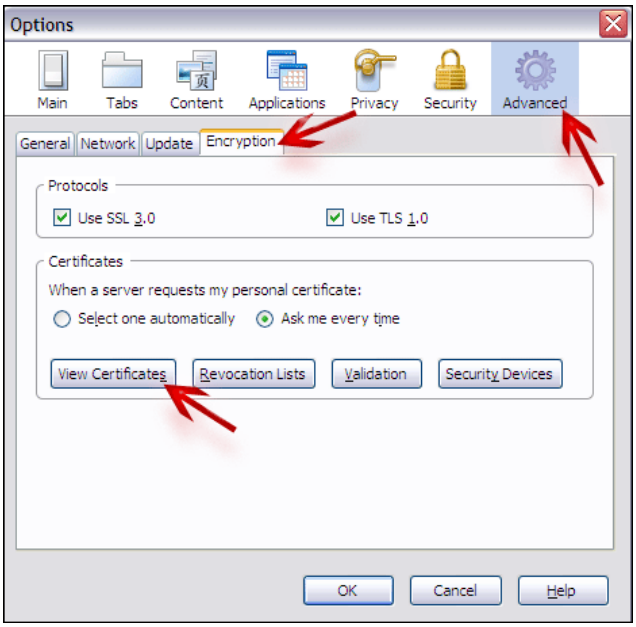
Στην μπάρα εργαλείων του Firefox, επιλέγετε «εργαλεία» (tools) και «Επιλογές» (Options), όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 63.Mozilla Firefox - Εργαλεία – Επιλογές

PDF created with pdfFactory Pro trial version www.pdffactory.com

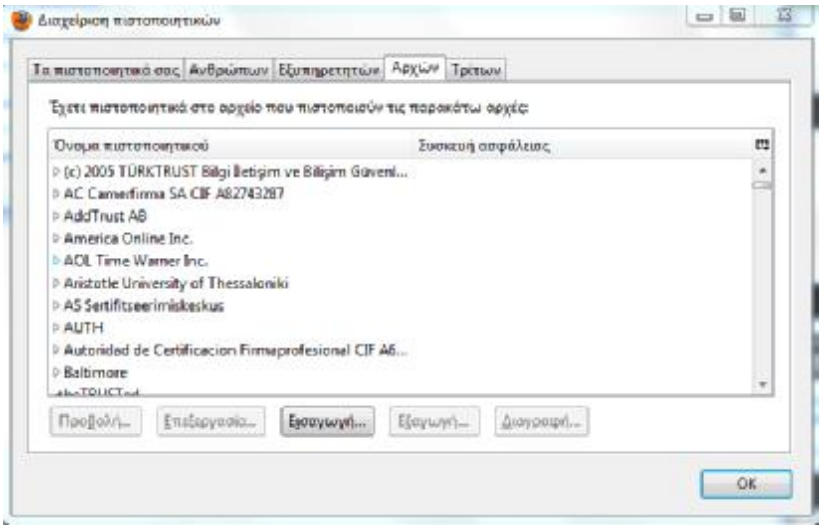
Επιλέγετε το εικονίδιο «Για προχωρημένους» (Advanced) και ακολούθως την καρτέλα «Κρυπτογράφηση» (Encryption). Κάντε κλικ στο «Προβολή Πιστοποιητικών» (View Certificates).



Εικόνα 64. Mozilla Firefox- Κρυπτογράφηση- Προβολή Πιστοποιητικών

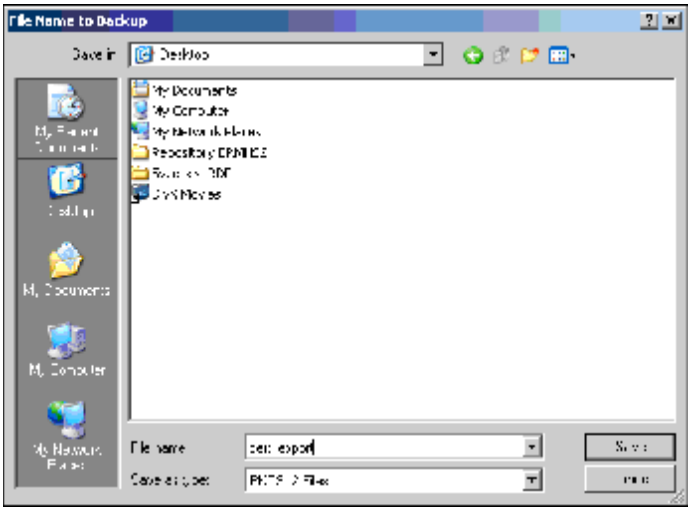
Στο παράθυρο εμφανίζονται τα ψηφιακά πιστοποιητικά που σας ανήκουν και είναι αποθηκευμένα στον υπολογιστή. Επιλέξτε το πιστοποιητικό που επιθυμείτε να εξάγετε και κάντε κλικ στο «Εξαγωγή»(Backup), για να εκκινήσετε την διαδικασία εξαγωγής. Εναλλακτικά, επιλέξτε «Εξαγωγή όλων» (backup all) για να εξάγετε όλα τα ψηφιακά πιστοποιητικά σας.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 65.Mozilla Firefox- Εξαγωγή

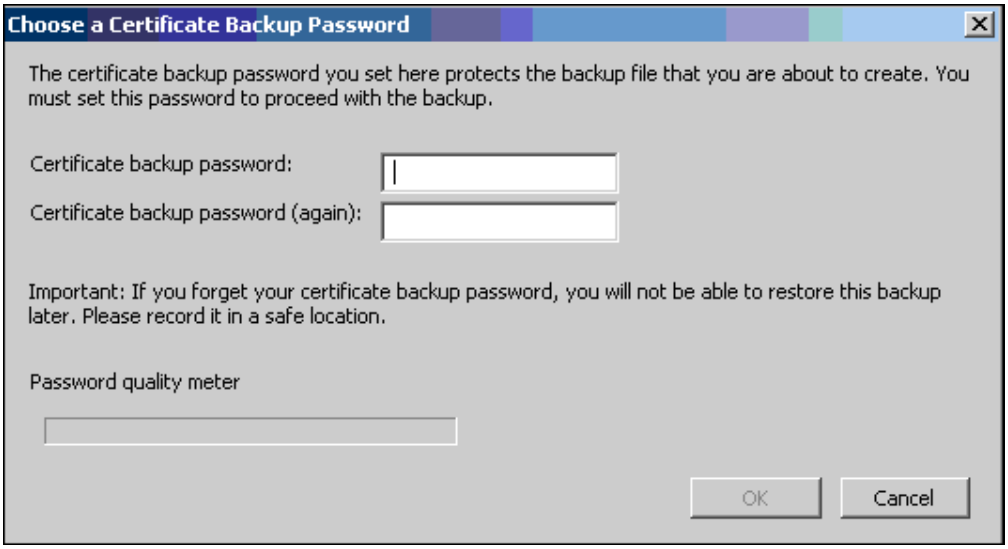
Ακολούθως, στο επόμενο παράθυρο καλείστε να επιλέξετε το όνομα και την διαδρομή του αρχείου στο οποίο θα αποθηκευθούν τα ψηφιακά πιστοποιητικά.



Εικόνα 66.Mozilla Firefox - Αποθήκευση Πιστοποιητικού

Στο παράθυρο που εμφανίζεται, πρέπει υποχρεωτικά να πληκτρολογήσετε έναν επιθυμητό κωδικό ασφαλείας, ο οποίος είναι απαραίτητος για μελλοντική χρήση του αντιγράφου ασφαλείας των ψηφιακών πιστοποιητικών. Αφού ορίσετε τον κωδικό, επιλέξτε «OK» για να συνεχίσετε.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 67.Εισαγωγή κωδικού Ασφαλείας

Η εξαγωγή των ψηφιακών πιστοποιητικών σας σε αντίγραφο ασφαλείας έχει πλέον ολοκληρωθεί. Το παραγόμενο αρχείο εμφανίζεται στον φάκελο που το αποθηκεύσατε και με την ονομασία που επιλέξατε.

12.9 Μεταφορά Ψηφιακών Πιστοποιητικών σε νέο browser.

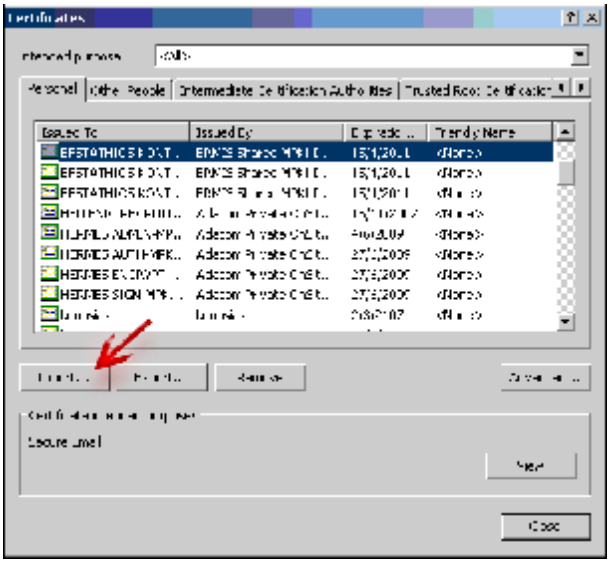
Για να μπορέσετε να χρησιμοποιήσετε τα Ψηφιακά Πιστοποιητικά σας σε διαφορετικό υπολογιστή από αυτόν που χρησιμοποιήσατε για την έκδοσή τους (ή και στον ίδιο, εάν τα έχετε διαγράψει κατά λάθος), θα πρέπει εκτός από την διαδικασία λήψης αντιγράφων ασφαλείας, να εγκαταστήσετε στον browser του νέου υπολογιστή, το ψηφιακό πιστοποιητικό της Πρωτεύουσας Αρχής Πιστοποίησης (Root CA) σύμφωνα με τις οδηγίες έκδοσης ψηφιακών πιστοποιητικών και το κεφάλαιο «Οδηγίες εγκατάστασης της Πρωτεύουσας Αρχής Πιστοποίησης»

12.9.1 Με χρήση Internet Explorer

Για την διαδικασία εισαγωγής ψηφιακού πιστοποιητικού στον Internet Explorer, μεταβείτε στην οθόνη προβολής των αποθηκευμένων ψηφιακών πιστοποιητικών, όπως περιγράφεται στο κεφάλαιο Α, και ακολουθήστε τα παρακάτω βήματα:

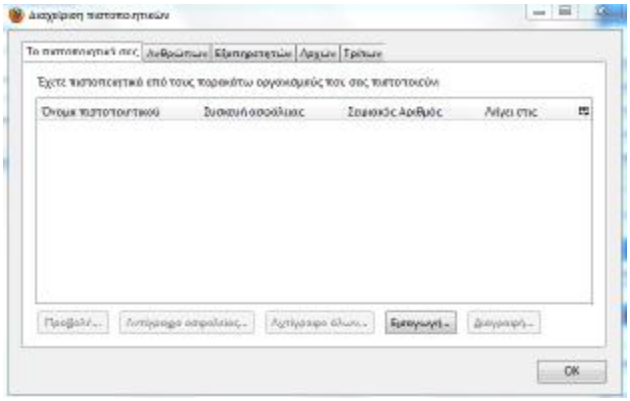
Στο παράθυρο «Πιστοποιητικά» επιλέξτε «Εισαγωγή» (Import).

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 68.Internet Explorer - Πιστοποιητικά – Εισαγωγή

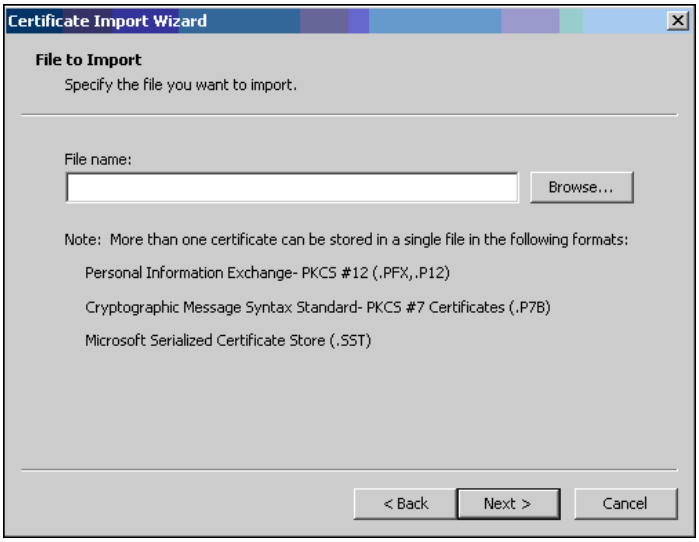
Στο παράθυρο «Οδηγός εισαγωγής πιστοποιητικού» (Certificate Import Wizard), επιλέξτε «Επόμενο».



Εικόνα 69.Οδηγός εισαγωγής πιστοποιητικού

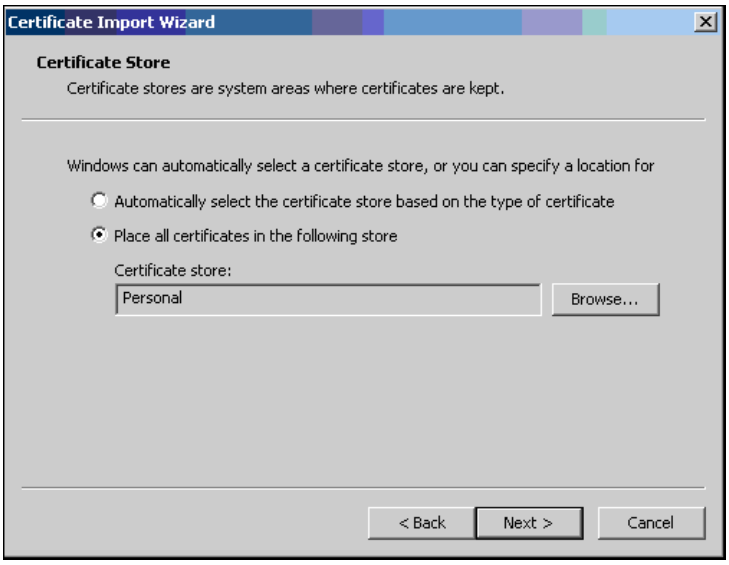
Στο επόμενο παράθυρο, καλείστε να αναζητήσετε το αρχείο που έχετε εξάγει και περιέχει το ψηφιακό πιστοποιητικό και επιλέξτε «Επόμενο» (Next).

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 70.Οδηγός εισαγωγής πιστοποιητικού (Βήμα 2)

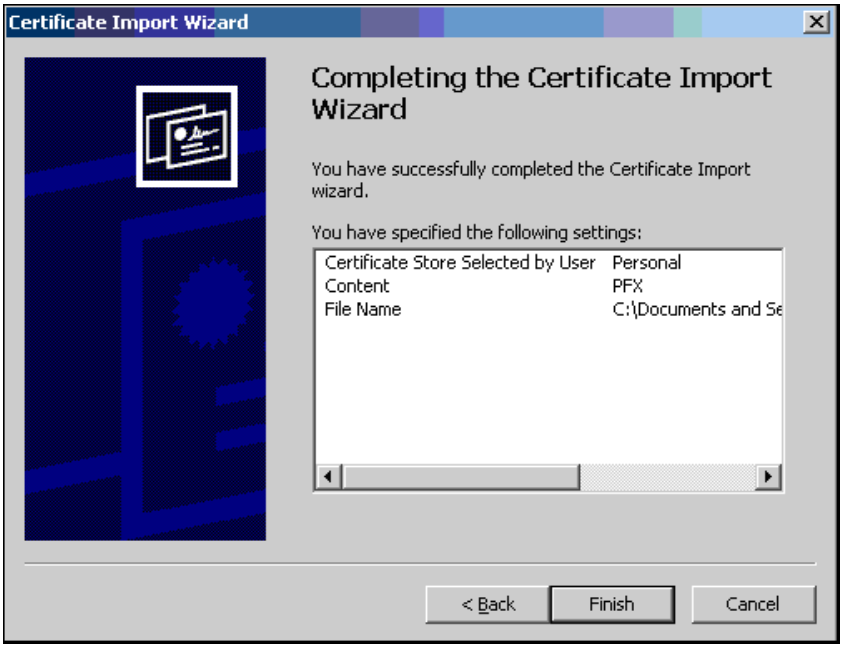
Στην συνέχεια, βεβαιωθείτε πως οι εικονιζόμενες επιλογές είναι ενεργοποιημένες και εισάγετε τον κωδικό πρόσβασης που ορίσατε κατά την εξαγωγή του πιστοποιητικού.



Εικόνα 71.Οδηγός εισαγωγής πιστοποιητικού (Βήμα 3)

Τέλος, επιλέξτε «Ολοκλήρωση» (Finish). Η εισαγωγή του ψηφιακού πιστοποιητικού στον Internet Explorer έχει ολοκληρωθεί με επιτυχία.

PDF created with pdfFactory Pro trial version www.pdffactory.com



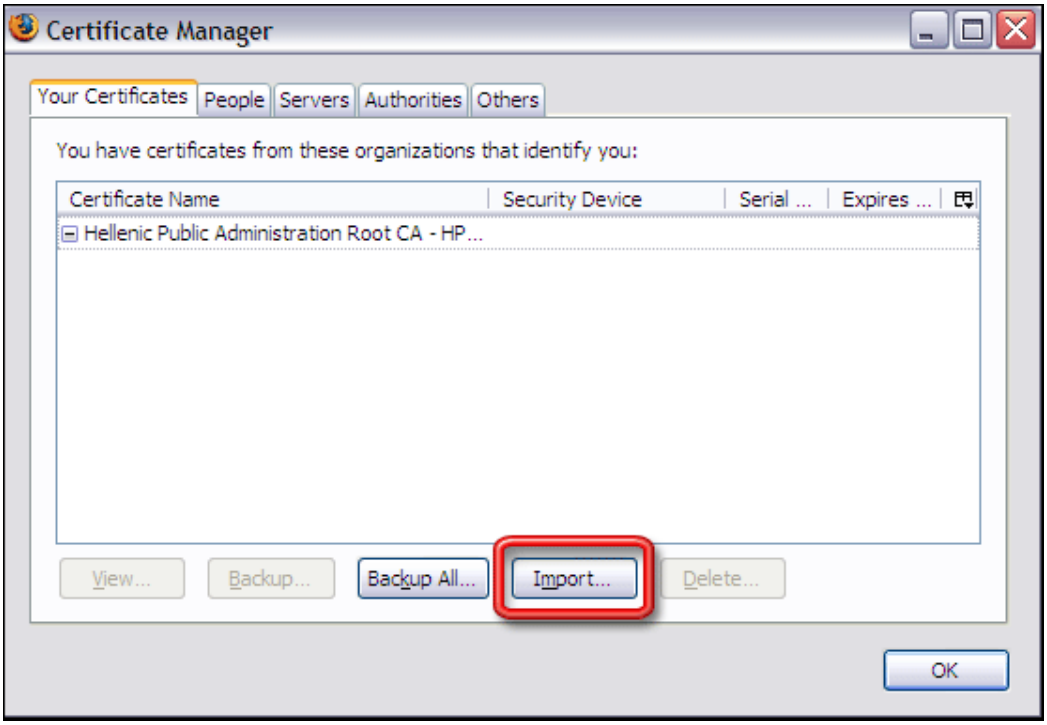
Εικόνα 72.Οδηγός εισαγωγής πιστοποιητικού (Βήμα 4)

12.9.2 Με χρήση Mozilla Firefox

Για την διαδικασία εισαγωγής ψηφιακού πιστοποιητικού στον Firefox, μεταβείτε στην οθόνη προβολής των αποθηκευμένων ψηφιακών πιστοποιητικών, όπως περιγράφεται στο κεφάλαιο Α, και ακολουθήστε τα παρακάτω βήματα:

Στο παράθυρο εμφανίζονται τα ψηφιακά πιστοποιητικά που σας ανήκουν και είναι αποθηκευμένα στον υπολογιστή. Εάν δε διαθέτετε άλλα ψηφιακά πιστοποιητικά, το παράθυρο θα είναι κενό. Επιλέξτε «Εισαγωγή» (Import).

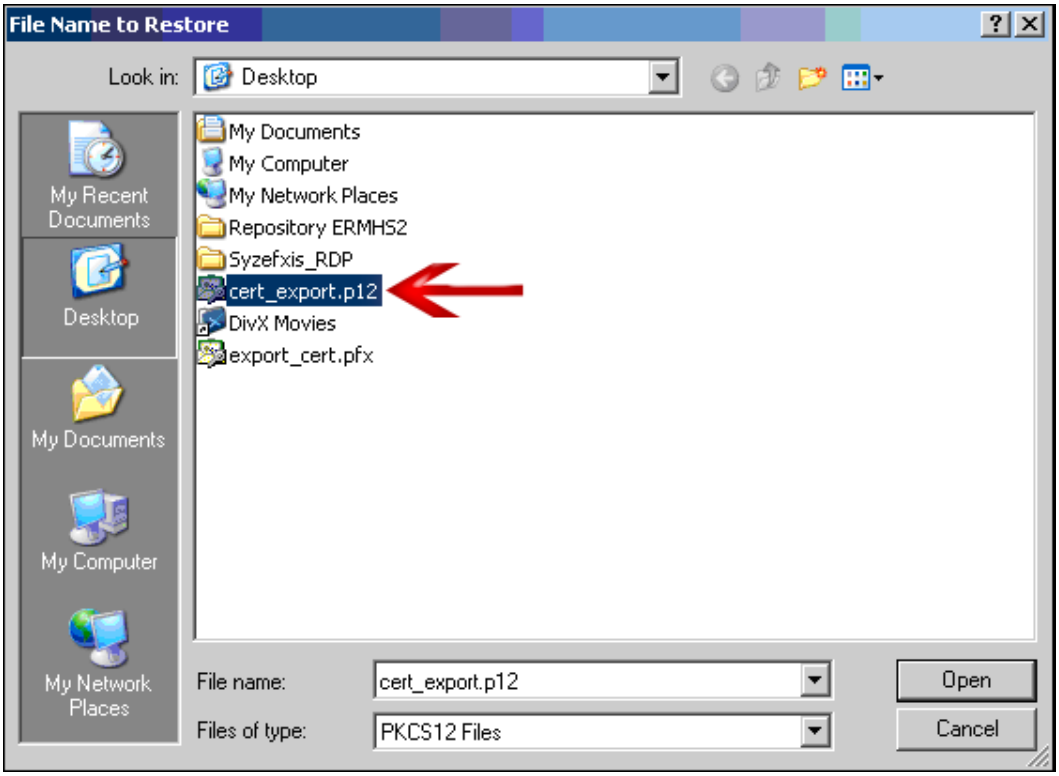
PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 73.Mozilla Firefox- Επιλογές - Εισαγωγή

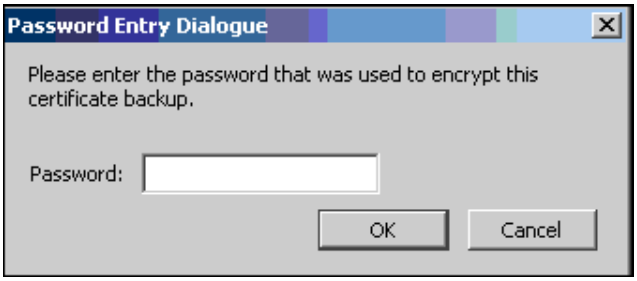
Ακολούθως, στο επόμενο παράθυρο καλείστε να αναζητήσετε το αρχείο που περιέχει τα ψηφιακά πιστοποιητικά που θέλετε να εισάγετε.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 74. Επιλογή Αποθηκευμένου Πιστοποιητικού

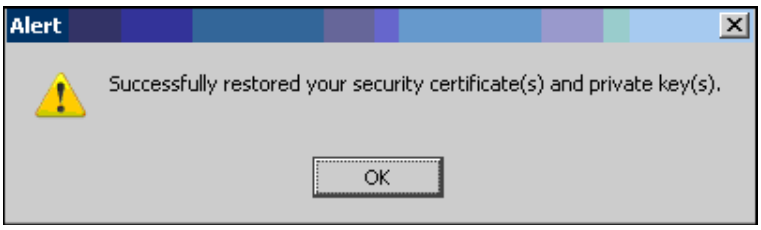
Στο παράθυρο που εμφανίζεται, πληκτρολογήστε τον κωδικό ασφαλείας που ορίσατε κατά την διαδικασία εξαγωγής των πιστοποιητικών.



Εικόνα 75. Εισαγωγή Pass του Πιστοποιητικού

Η διαδικασία έχει ολοκληρωθεί με επιτυχία και τα ψηφιακά πιστοποιητικά σας έχουν εγκατασταθεί στον Firefox του υπολογιστή. Επιπλέον, εμφανίζεται σχετικό ενημερωτικό μήνυμα.

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 76.Μήνυμα επιτυχούς Αποθήκευσης

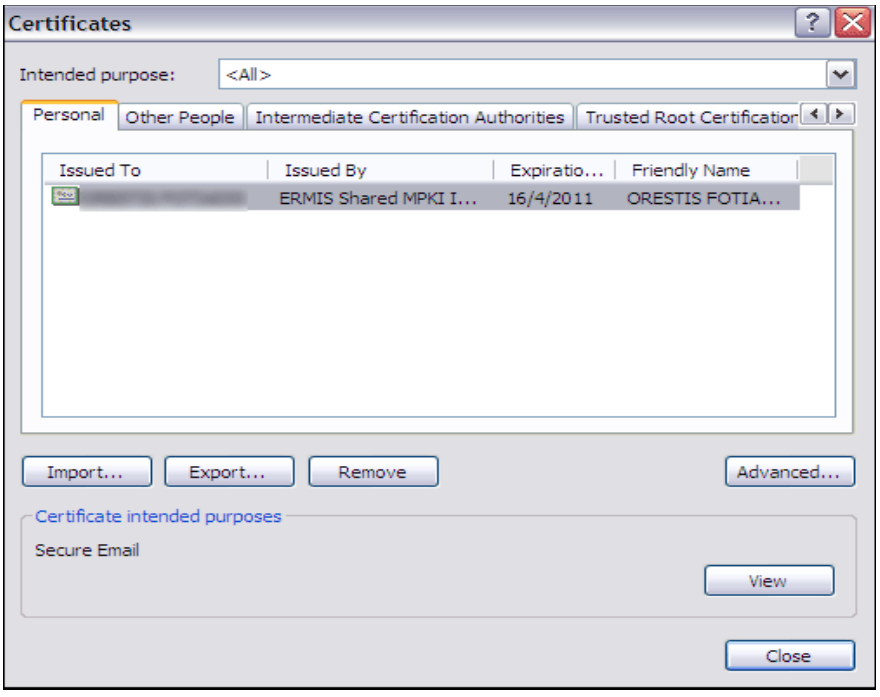
12.10 Διαγραφή Ψηφιακών Πιστοποιητικών

Εάν για οποιοδήποτε λόγο ακυρώσετε τα ψηφιακά πιστοποιητικά σας (π.χ. λόγω απώλειας τους), θα πρέπει να ακολουθήσετε και την παρακάτω διαδικασία για να διαγράψετε τα αρχεία που έχουν παραμείνει στον browser που εγκαταστήσατε.

Τα άκυρα πλέον ψηφιακά πιστοποιητικά θα πρέπει να διαγραφούν από όλους τους browsers στους οποίους είχαν εγκατασταθεί.

12.10.1 Με χρήση Internet Explorer

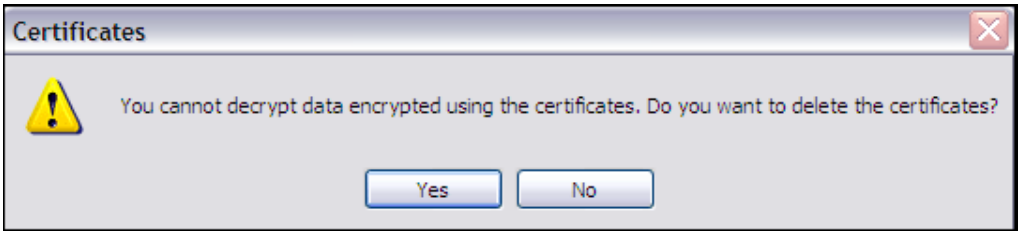
Από την οθόνη προβολής των ψηφιακών πιστοποιητικών, επιλέξτε τα πιστοποιητικά που επιθυμείτε να διαγράψετε, και κάντε κλικ στο «Αφαίρεση» (Remove).



Εικόνα 77. Internet Explorer - Επιλογές -Διαγραφή Πιστοποιητικού

PDF created with pdfFactory Pro trial version www.pdffactory.com

Στο προειδοποιητικό μήνυμα που εμφανίζεται, επιλέξτε «Ναι».

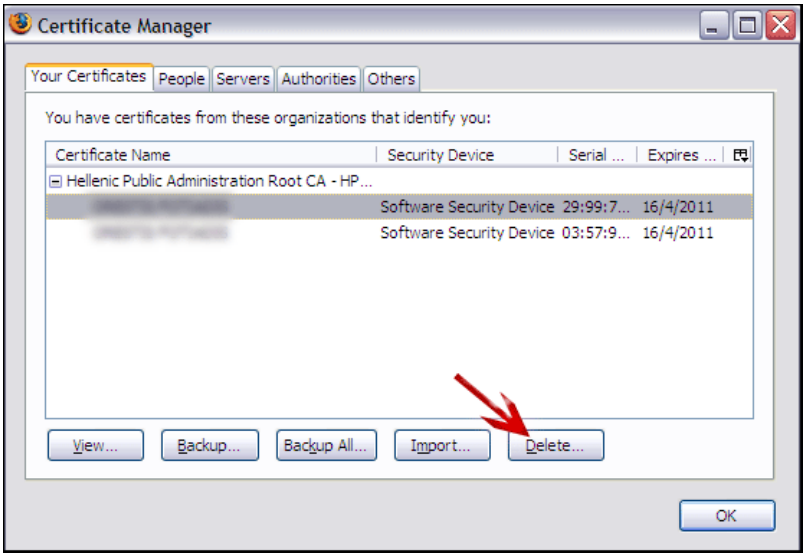


Εικόνα 78. Επιβεβαίωση Διαγραφής

Το ψηφιακό πιστοποιητικό έχει πλέον διαγραφεί.

12.10.2 Με χρήση Mozilla Firefox

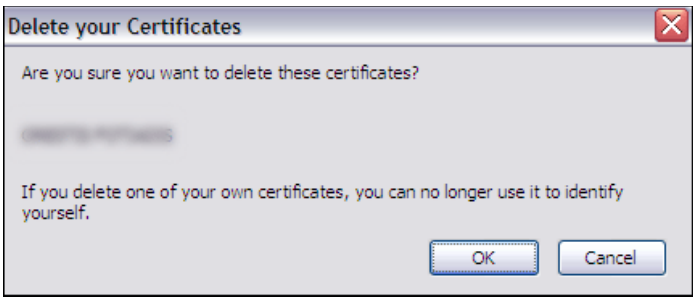
Από την οθόνη προβολής των ψηφιακών πιστοποιητικών, επιλέξτε τα πιστοποιητικά που επιθυμείτε να διαγράψετε, και κάντε κλικ στο «Διαγραφή» (Delete).



Εικόνα 79. Mozilla Firefox- Επιλογές -Διαγραφή Πιστοποιητικού

Στο προειδοποιητικό μήνυμα που εμφανίζεται, επιλέξτε «OK».

PDF created with pdfFactory Pro trial version www.pdffactory.com



Εικόνα 80.Επιβεβαίωση Διαγραφής

Το ψηφιακό πιστοποιητικό έχει πλέον διαγραφεί.

PDF created with pdfFactory Pro trial version www.pdffactory.com

13. Ισχυρή Αυθεντικοποίηση-Πιστοποιήση

13.1 Εισαγωγή – Τι είναι αυθεντικοποίηση

Ως κυριότερο μέσο για την εισαγωγή σε ένα σύστημα είναι η χρήση κωδικών (password) και ονομάτων χρηστών (usernames). Η διαδικασία όπου το σύστημα εξακριβώνει για τον πιο χρήστη έχει απέναντι του ονομάζεται αυθεντικοποίηση (κάποιοι χρησιμοποιούν το όρο πιστοποίηση). Με βάση την διαδικασία της αυθεντικοποίησης το σύστημα μπορεί να δώσει την σωστή εξουσιοδότηση (authorization) σε κάποιο χρηστή (πχ πρόσβαση σε συγκεκριμένα αρχεία που δεν πρέπει να βλέπουν άλλοι κτλ). Με βάση την αυθεντικοποίησης ένα σύστημα κρατάει ημερολόγιο (logs) για το τι πράξη εκτέλεσε ο κάθε χρήστης. Η λειτουργία αυτή λέγετε καταλογισμός (accountability). Με βάση το accountability μπορούμε να πετύχουμε πολλά πράγματα όπως να χρεώσουμε λογαριασμό ανάλογα με την χρήση ή και σε περίπτωση κάποιου συμβάντος μπορεί να βρεθεί αυτός που το προκάλεσε.

13.2 Στατικοί Κωδικοί (ασθενής αυθεντικοποίηση)

Οι κωδικοί (κλειδάριθμοι, λέξεις κλειδιά) αποτελούν το κύριο μέσο αυθεντικοποίησης των χρηστών στα πληροφοριακά συστήματα. Όταν το «πιστήριο» που πρέπει να παρέχει κάποιος είναι μόνο ενα τότε αυτό ονομάζεται αυθεντικοποίηση ενός παράγοντα.

1. Οι «κωδικοί» (passwords) είναι αυθεντικοποίηση ενός παράγοντα. Στην περίπτωση μας (κωδικοί) ο παράγοντας είναι «το κάτι που ξέρουμε»). Δυστυχώς το κάτι που ξέρω είναι κάτι «που μπορεί να μαντέψει ο άλλος» και άρα να νικήσει το σύστημα.
2. Ο χρηστές έχοντας έλλειψη εκπαίδευσης και μην γνωρίζοντας πολλά για ασφάλεια σπάνια επιλέγουν καλούς κωδικούς.
3. Οι χρήστες δεν γνωρίζουν ότι οι κωδικοί δεν πρέπει να
4. Να είναι κενοί (να μην υπάρχει κωδικός)
5. Να είναι το ίδιο όπως και το Login username ή να περιέχει μέρος του ή να προέρχεται από αυτό (password και Login πρέπει να είναι ανεξάρτητα μεταξύ τους)
6. Να είναι μια εύκολα μαντέψημη πληροφορία (όπως ημερομηνία ή χρονολογία γέννησης, όνομα συγγενή, συζύγου, κατοικίδιου κτλ). Ούτε συνδυασμός αυτών (πχ kostas1967)
7. Να μην είναι τετριμμένοι (1234, 4444, abc, qwerty, aaaa κτλ) ή συνδυασμοί τετριμμένων κωδικών (abc123)
8. Να είναι μικροί σε πλήθος χαρακτήρων (qk1, 234a κτλ). Για το απαραίτητο μήκος βλέπε παρακάτω
9. Να μην είναι εύκολα προβλέψιμοι. Πχ κάποιος να χρησιμοποιεί ως κωδικό το όνομά του ακολουθούμενο από τον τρέχον μήνα (kostasjuly) ή το όνομά του ακολουθούμενο από το όνομα του συστήματος (kostasmail, mariawebserver)

PDF created with pdfFactory Pro trial version www.pdffactory.com

10. Να μην είναι απλές λέξεις που συναντιόνται σε λεξικό. Σε αυτή την περίπτωση αυτοματοποιημένα προγράμματα μπορούν να τους βρουν σε ελάχιστα δευτερόλεπτα

Αν ο κωδικός είναι κάτι από τα παραπάνω τότε λέμε ότι είναι «ασθενής» (μη ισχυρός) και σπάει εύκολα.

Εικόνα 81. Ο χρήστης πληκτρολογεί όνομα και κωδικό (ασθενής αυθεντικοποίηση - πιστοποίηση)

Ένας κακός (μη ισχυρός) κωδικός μπορεί να είναι η αιτία για την έκθεση του πληροφοριακού συστήματος σε τρίτους. Δυστυχώς οι χρηστές δεν επιλέγουν καλούς κωδικούς με αποτέλεσμα να μην υπάρχει ουσιαστική ασφάλεια.

Για να επιλέγουν οι χρήστες έναν ισχυρό-καλό κωδικό αυτός θα πρέπει

1. Να είναι αρκούντως μεγάλος (>10 χαρακτήρες)

2. Να περιέχει εκτός από γράμματα, αριθμούς ή/και σύμβολα (πχ p4pak11!)

3. Αν πρέπει να χρησιμοποιηθεί λέξη (για να είναι ευκολο-μνημόνευτος ένας κωδικός) τότε συνίσταται η λέξη να γράφετε ανορθόγραφα και με κάποια από τα γράμματα διπλές φορές (πχ indeerneet12 αντί Internet). Να μην χρησιμοποιούνται λέξεις ή ονόματα αγγλικά αλλά ελληνικά γραμμένα με λατινικούς χαρακτήρες και αντικατάσταση κάποιον από αυτά με αριθμούς που ομοιάζουν με γράμματα (0 αντί ο, 4 αντί Α, 3 αντί ε) (πχ η λέξη χελιδόνι θα γράφονταν x3lidd0ni ενώ η λέξη αυτοκίνητο θα μπορούσε να γραφτεί aftookin1to)

4. Εναλλακτικά αντί λέξεων κωδικών προτείνεται να χρησιμοποιούνται φράσεις κωδικοί (passphrases). Μια πρόταση (στίχος, παροιμία έκφραση που αποτελείτε από πολλές λέξεις) μπορεί να χρησιμοποιηθεί ως ασφαλέστερος τρόπος αυθεντικοποίησης. Επειδή τα κενά (spaces) σε κάποια συστήματα προκαλούν προβλήματα αντικαθίστανται με άλλους χαρακτήρες (πχ -,_) ή παραλείπονται. Η διαφορά από τους πολύπλοκους κωδικούς είναι ότι ο χρήστης μπορεί να τον θυμάται πιο εύκολα.

Τέτοιες προτάσεις είναι

1. “osa-denftane-i-ialepou”

PDF created with pdfFactory Pro trial version www.pdffactory.com

2. “tokalotopalikari”
3. “tospitimoueinaiaspro”
4. “eimai_78_kila_mono”
5. “sousami-anoi3e”

Τέλος οι κωδικοί πρέπει να αλλάζουν τακτικά ώστε να μην υπάρχουν προβλήματα με διαρροές αλλά και σε ειδικές επιθέσεις που απαιτούν χρόνο για να βρεθεί ένας κωδικός.

Ωστόσο δεν είναι εύκολο για τους ανθρώπους να επιλέγουν ισχυρούς κωδικούς μιας και συνήθως τους ξεχνάνε, ή τους πληκτρολογούν λάθος με αποτέλεσμα να κλειδώνονται διαρκώς και να απασχολούν τα τμήματα υποστηρίξεως (support) υπάρχει η απαίτηση καλύτερου τρόπου αυθεντικοποίησης (ασφαλέστερου και πρακτικού)

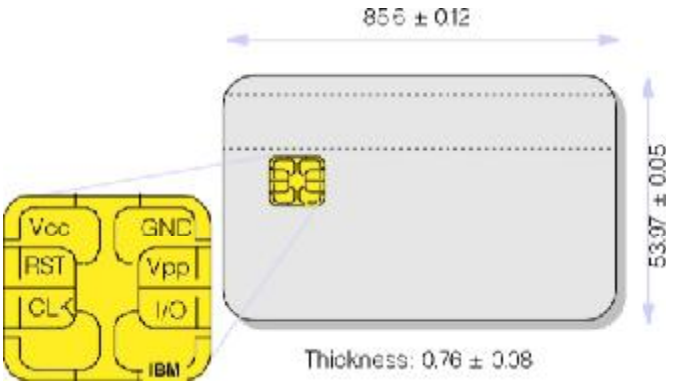
13.3 Αυθεντικοποίηση δύο παραγόντων (Ισχυρή αυθεντικοποίηση)

Σε αυτή την κατηγορία ο χρήστης για να εισαχθεί σε ένα σύστημα απαιτητέ να το αποδείξει με δύο τρόπους. Ο πιο συνηθισμένος τρόπος είναι αυτός με κάποια έξυπνη (γνωστό ώς token) κάρτα και ένα PIN (μοιάζει αλλά δεν είναι ίδιος με την χρήση των ATM και των cash cards). Στην περίπτωση αυτή για να πιστοποιηθεί ο χρήστης απαιτούνται δύο παράγοντες

1. Να κατέχει την κάρτα – token (1ος παράγοντας)
2. Να γνωρίζει το PIN (2ος παράγοντας)

Και ένα από τα δύο να πέσει στην κατοχή κάποιου τρίτου αυτός δεν μπορεί να παραβιάσει το σύστημα.

Η μέθοδος αυτή ονομάζεται αυθεντικοποίηση δύο παραγόντων και αποτελεί μέθοδο ισχυρή αυθεντικοποίησης (strong authentication)



Εικόνα 82. Έξυπνες κάρτες (συνήθης μορφή ισχυρής αυθεντικοποίησης)

PDF created with pdfFactory Pro trial version www.pdffactory.com

Εικόνα 83. Έξυπνες κάρτες σε μορφή USB (token)

Εναλλακτικά αντί για PIN υπάρχουν και περιπτώσει που ο δεύτερος παράγοντας είναι κάποιο βιομετρικό (πχ κάρτα και δακτυλικό αποτύπωμα).

Υπάρχουν πολλές μορφές διαφορετικών παραγόντων, όπως οι κωδικοί μίας χρήσης. Οι κωδικοί μίας χρήσεως παράγονται από ειδικές συσκευές ασφαλείας (tokens) οι οποίες δίνονται στους χρήστες. Οι χρηστές χρησιμοποιούν το τρέχοντα κωδικό (1ος παράγοντας) αλλά και ένα προσωπικό PIN (2ος παράγοντας). Ο σωστός συνδυασμός κωδικού και PIN πιστοποιεί την αυθεντικότητα τους.

Εικόνα 84. Tokens παραγωγής κωδικών μίας χρήσης. Ο κωδικώς που ισχύει κάθε φωρά αλλάζει κάθε λίγα δευτερόλεπτα

Τυπικές συσκευές παραγωγής κωδικών που δίνεται μία σε κάθε χρήστη. Ο κωδικός που παρουσιάζεται αλλάζει κάθε 60’’. Ο χρήστης πρέπει αντί για στατικό κωδικό να πληκτρολογήσει το PIN του ακολουθούμενο από τον κωδικό που βλέπει στην οθόνη την τρέχουσα στιγμή.

PDF created with pdfFactory Pro trial version www.pdffactory.com

14. Επίλογος

Η δυνατότητα ενός υποκειμένου - που αποκαλείται και τελική οντότητα - να μπορεί να χρησιμοποιήσει τα ίδια μέσα (π.χ. κρυπτογραφικά κλειδιά, ασφαλείς φορείς, πιστοποιητικά, λογισμικό επικοινωνίας κ.τ.λ.), για την δημιουργία των δικών του ψηφιακών υπογραφών και την επαλήθευση των ψηφιακών υπογραφών τρίτων, σε περισσότερους από έναν συναλλακτικούς κύκλους, δηλαδή η διαλειτουργικότητα όλων των σχετικών εφαρμογών, αποτελεί ένα σημαντικό ζητούμενο, αφού θα μειώσει το συνολικό κόστος εξοπλισμού, θα απλοποιήσει τις λειτουργίες του χρήστη, θα περιορίσει τις πολλαπλές διαδικασίες ταυτοποίησης των υποκειμένων, θα συμβάλει στην δημιουργία της κρίσιμης μάζας των χρηστών με δυνατότητα ψηφιακής υπογραφής, που - με την σειρά της - θα οδηγήσει στην ανάπτυξη και παροχή περισσότερων σχετικών υπηρεσιών προς τους χρήστες.

Παράλληλα, όμως, η διαλειτουργικότητα και η χρήση της ίδιας ατομικής ψηφιακής υπογραφής σε πολλούς συναλλακτικούς κύκλους, θέτει έντονα ζητήματα προστασίας των προσωπικών δεδομένων των χρηστών από πιθανές ανεπίτρεπτες διασταυρώσεις των συναλλαγών τους και την δημιουργία, έτσι, αρχείων με ολοκληρωμένα ατομικά περιγράμματα (profiles) των χρηστών.

Η τεχνική πολυπλοκότητα, οι παραλλαγές των εφαρμογών προηγμένων ψηφιακών υπογραφών και τα διαφορετικά επίπεδα νομικής αναγνώρισής τους, αναδεικνύουν ιδιαίτερες δυσκολίες ως προς την επίτευξη πλήρους διαλειτουργικότητας μεταξύ των υφιστάμενων εφαρμογών ψηφιακής υπογραφής σε διεθνές και ευρωπαϊκό επίπεδο. Έχει παρατηρηθεί σχετικά ότι η διαλειτουργικότητα επιτυγχάνεται ευκολότερα σε κλειστές ή κεντρικά ελεγχόμενες εφαρμογές οι οποίες επιβάλλουν οι ίδιες συγκεκριμένες αναλυτικές προδιαγραφές (π.χ. τα πρότυπα EMV για τις πιστωτικές κάρτες, συντονισμένες εφαρμογές ηλεκτρονικής διακυβέρνησης ενός κράτους κ.τ.λ.).

Στα πλαίσια της Ευρωπαϊκής Ένωσης, παρά τα τέσσερα και πλέον χρόνια από την έκδοση της σχετικής Ευρωπαϊκής Οδηγίας που είχε ως στόχο την εναρμόνιση του σχετικού θεσμικού πλαισίου μεταξύ των κρατών μελών, η παροχή πανευρωπαϊκώς αναγνωρισμένων και διαλειτουργικών υπηρεσιών πιστοποίησης ψηφιακής υπογραφής, εξακολουθεί να εμφανίζει ακόμα αρκετές δυσχέρειες. Το γεγονός αυτό οφείλεται σε κάποιους ανασταλτικούς παράγοντες μεταξύ των οποίων περιλαμβάνονται:

1. Ορισμένες ασάφειες του ευρωπαϊκού κανονιστικού πλαισίου, το οποίο προσπαθώντας να εξισορροπήσει μεταξύ τεχνολογικής ουδετερότητας και ασφάλειας δικαίου, καταλήγει σε ορισμένες αοριστίες,

2. Η ανάπτυξη αυτόνομων εθνικών κανονιστικών πλαισίων σε ορισμένα κράτη μέλη πριν από την έκδοση της Οδηγίας, και η διαφορετική ερμηνευτική προσέγγιση της Οδηγίας από αυτά τα κράτη μέλη, ώστε να διατηρηθεί απαράλλακτη η υφιστάμενη υποδομή τους,

3. Οι αργοί ρυθμοί ανάπτυξης της προβλεπόμενης σχετικής προτυποποίησης από τους ευρωπαϊκούς οργανισμούς, δεδομένου ότι επιχειρείται η όσο το δυνατόν μεγαλύτερη συμβατότητα με τις υφιστάμενες (διαφορετικές) υποδομές και τα εφαρμοζόμενα συστήματα στα διάφορα κράτη μέλη.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Μάλιστα, με εξαίρεση ορισμένα κράτη μέλη που είχαν προβεί εγκαίρως σε αναλυτικές ρυθμίσεις για την παροχή υπηρεσιών πιστοποίησης ψηφιακής υπογραφής, σοβαρά ζητήματα διαλειτουργικότητας υπάρχουν ακόμη και ανάμεσα στις σχετικές υπηρεσίες που παρέχονται από τους CSP που λειτουργούν στο ίδιο κράτος, όπως παρατηρήθηκε - στο πλαίσιο της λειτουργίας της ΟΕ "E2" του eBusinessForum - ότι συμβαίνει και στην Ελλάδα.

Τα σημαντικότερα προβλήματα διαλειτουργικότητας μεταξύ των υπηρεσιών πιστοποίησης ψηφιακών υπογραφών που παρατηρούνται, αναφέρονται κυρίως στην περιγραφή των στοιχείων του υποκειμένου των πιστοποιητικών (naming policy / conventions), στον τρόπο προσδιορισμού των επιτρεπόμενων χρήσεων των σχετικών κρυπτογραφικών κλειδιών και στα μέσα που χρησιμοποιούνται για την ενημέρωση των κατόχων και των αποδεκτών των ηλεκτρονικών πιστοποιητικών ως προς τους λοιπούς όρους έκδοσης και χρήσης που θέτονται από την εφαρμοζόμενη Πολιτική των εκδιδόμενων πιστοποιητικών. Επίσης σημαντικά ζητήματα υφίστανται και με άλλα σχετιζόμενα θέματα, όπως η χρονοσήμανση των υπογραφών, η πιστοποίηση των ιδιοτήτων των υποκειμένων, οι υπηρεσίες ενημέρωσης για την ανάκληση των πιστοποιητικών, η αλληλοδιαπίστευση των ΠΥΠ κ.ά.. Όλα αυτά έχουν ως πρόσθετο αρνητικό αποτέλεσμα την έλλειψη κοινώς αποδεκτών εφαρμογών λογισμικού για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, οι οποίες να εφαρμόζουν και να ερμηνεύουν σωστά όλες τις παραπάνω παραμέτρους, ανεξάρτητα από τον εκδότη, το υποκείμενο, ή και τον αποδέκτη των σχετικών πιστοποιητικών.

Η υφιστάμενη έλλειψη διαλειτουργικότητας στις εφαρμογές ψηφιακών υπογραφών, το μεγάλο κόστος δημιουργίας και διατήρησης μιας ασφαλούς Υποδομής Δημοσίου Κλειδιού και ο μεγάλος επιχειρηματικός κίνδυνος της ανάπτυξης μιας τέτοιας υποδομής την στιγμή που δεν έχουν προσδιοριστεί σαφώς οι τελικές προδιαγραφές που θα επικρατήσουν (και οι οποίες θα εξασφαλίζουν την διαλειτουργικότητα των παρεχόμενων υπηρεσιών και άρα την δημιουργία της απαραίτητης κρίσιμης μάζας στη σχετική αγορά, οδηγούν σε συγκράτηση και περιορισμό των σχετικών επενδύσεων και των πρωτοβουλιών για την ανάπτυξη συναφών εφαρμογών. Παράλληλα διατηρείται ένα κλίμα σύγχυσης και πλημμελούς - ή ακόμη και αντιφατικής - ενημέρωσης των δυνητικών χρηστών των εφαρμογών ηλεκτρονικής υπογραφής, το οποίο δυσχεραίνει την ανάπτυξη της απαραίτητης σχετικής εμπιστοσύνης.

Από την άλλη πλευρά, σημαντική ενίσχυση της εμπιστοσύνης του κοινού στις σχετικές υπηρεσίες θα προσφέρει η λειτουργία του προβλεπόμενου μηχανισμού για την Διαπίστωση (επίσημη πιστοποίηση) της συμμόρφωσης των προϊόντων ψηφιακής υπογραφής με τις απαιτήσεις της νομοθεσίας, καθώς και η εφαρμογή στην πράξη του θεσμού της Εθελοντικής Διαπίστευσης των CSP.

Παράλληλα, η σύνταξη Πολιτικών (Ψηφιακής) Υπογραφής (Signature Policies) που θα προσδιορίζουν ακριβείς όρους για την δημιουργία έγκυρων ψηφιακών υπογραφών σε εφαρμογές μεγάλων ομοειδών συναλλακτικών κύκλων, όπως είναι ο Δημόσιος Τομέας (e-government) και οι Τράπεζες (e-Banking), θεωρείται ότι μπορεί να συμβάλλει στην αποσαφήνιση των απαραίτητων προδιαγραφών για τις παρεχόμενες υπηρεσίες πιστοποίησης ψηφιακών υπογραφών και στην περαιτέρω διαλειτουργικότητά τους.

Τέλος, η υιοθέτηση ανοικτών προτύπων (όπως π.χ. τα "OpenXades" & "Digi-Doc" που έχουν υιοθετηθεί σε Φινλανδία και Εσθονία)και η χρήση της γλώσσας XML στην ανάπτυξη των σχετικών εφαρμογών ηλεκτρονικών υπογραφών (σύμφωνα

PDF created with pdfFactory Pro trial version www.pdffactory.com

και με τα σχετικά ευρωπαϊκά πρότυπα που έχουν εκδοθεί στα πλαίσια της πρωτοβουλίας "European Electronic Signature Standardization Initiative" ή "EESSI"), μπορούν να παράσχουν πιο αναλυτικές και τυποποιημένες πληροφορίες στην λειτουργία των εφαρμογών αυτών και να συμβάλλουν στην επίτευξη μεγαλύτερης διαλειτουργικότητας και αναγνώρισης των σχετικών συναλλαγών σε πανευρωπαϊκό και διεθνές επίπεδο.

PDF created with pdfFactory Pro trial version www.pdffactory.com

15. Συμπεράσματα

Η ευρύτατη διείσδυση της τεχνολογίας σε όλους τους τομείς του κοινωνικού γίγνεσθαι, κάνει επιτακτική περισσότερο από ποτέ την ανάπτυξη μηχανισμών και μεθόδων προστασίας για την ασφαλή διακίνηση των ψηφιακών «αντικειμένων». Η ανάγκη προστασίας του απαραβίαστου του απορρήτου, στο σύγχρονο ψηφιακό περιβάλλον προκύπτει περισσότερο καθοριστική από ποτέ. Ειδικότερα, καθώς το Διαδίκτυο αποτελεί σήμερα το σημαντικότερο εκφραστικό μέσο της ελευθερίας στην επικοινωνία των ανθρώπων, θα πρέπει να αναπτυχθούν μηχανισμοί προστασίας και ασφάλειας, από εκείνους που επιβουλεύονται την ελευθερία αυτή.

Η δημιουργία των ψηφιακών υπογραφών, βασιζόμενη στη τεχνολογία της κρυπτογραφίας, αποτελεί μια διαδεδομένη μέθοδο, προστασίας και ασφαλείας στη διακίνηση των ηλεκτρονικών εγγράφων. Συμπερασματικά, κρίνεται σκόπιμο να αναφερθεί ότι η ψηφιακή υπογραφή, παρέχει εγγύηση της αυθεντικότητας, της ακεραιότητας, της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Ωστόσο, όπως προαναφέρθηκε, η ψηφιακή υπογραφή προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο. Κατά συνέπεια, προκύπτει πως η ιδανικότερη λύση για την ασφαλή διακίνηση αλλά και χρήση των ψηφιακών αντικειμένων είναι ο συνδυασμός των αναπτυγμένων μεθόδων προστασίας. Η προσθήκη δηλαδή ψηφιακής υπογραφής και υδατογραφήματος στα διακινούμενα ηλεκτρονικά έγγραφα, αποτελούν ενδεδειγμένο τρόπο, για την προστασία του εγγράφου τόσο κατά την μεταφορά του, όσο και κατά τη χρήση του.

PDF created with pdfFactory Pro trial version www.pdffactory.com

16. Βιβλιογραφία

[1]. Reed C, 'What is a Signature?', 2000 (3) The Journal of Information, Law and Technology (JILT) http://elj.warwick.ac.uk

[2]. Rivest, R., Shamir, A., and Adleman, L., (1978) 'A Method for Obtaining Digital Signatures and Public Key Cryptosystems'; Communications of the ACM, 21(2):120-126, February.

[3]. http://www.go-online.gr/, Επίσημος κόμβος της «Εκπαιδευτικής Στήριξης του Δικτυωθείτε», «Η ηλεκτρονική υπογραφή (e-signature) στις online συναλλαγές».

[4]. http://www.eett.gr/opencms/opencms/EETT/FAQS/DigitalSignatures/ ,

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, «Ηλεκτρονική Υπογραφή».

[5]. «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», Συγγραφέας: Καραδημητρίου Κοσμάς, Εκδοτικός Οίκος: ΣΑΚΚΟΥΛΑΣ ΕΚΔΟΣΕΙΣ Α.Ε. http://www.ebooks.gr/book/117546

[6]. http://www.ekt.gr/content/img/product/14911/pd150_2001.pdf ,

Φύλλο Εφημερίδας Της Κυβερνήσεως, Προεδρικό διάταγμα υπ' αριθμ. 150,«Προσαρμογή στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.»

[7]
http://news.kathimerini.gr/4dcgi/_w_articles_economyepix_8673_28/06/2003_68010, Εφημερίδα «Καθημερινή», άρθρο για την ηλεκτρονική υπογραφή

[8]. Cypher Research Laboratories, A brief history of cryptography

http://www.cypher.com.au/crypto_history.htm

[9]. Wikipedia, The Free Encyclopedia, Digital Signature,

http://en.wikipedia.org/wiki/Digital_signature

[10]. Η-επιχειρείν, Ψηφιακή υδατογράφηση,

http://www.go-online.gr/ebusiness/specials/article.html?article_id=618 ,

2006

[11]. Εθνική Συνομοσπονδία Ελληνικού Εμπορίου, Προεδρικό Διάταγμα υπ' αριθ. 150, Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές

http://www.esee.gr/el/Emporio/DedomenaProsopikouXaraktira/Proedriko-

Diatagma-150.shtml

[12]. Η-επιχειρείν, Η υποδομή δημοσίου κλειδιού και η κρυπτογράφηση στην πράξη,

PDF created with pdfFactory Pro trial version www.pdffactory.com

http://www.go-online.gr/ebusiness/specials/article.html?article_id=714

[13]. Α.Σουρής, Δ.Πατσός, Ν.Γρηγοριάδης (2004) « Ασφάλεια της πληροφορίας στους υπολογιστές, στο internet, στην καθημερινή μας ζωή...» ΕΚΔΟΣΕΙΣ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ

[14]. William Stallings, 2006, "Cryptography and Network Security, 4rd Edition", Publisher: Dorling Kindersley, 299-315.

[15]. Iglezakis Regulation of Electronic Signatures

PDF created with pdfFactory Pro trial version www.pdffactory.com