Πανεπιστήμιο Πειραιώς - Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση της ηλεκτρονικής υπογραφής**
Ονοματεπώνυμο Φοιτητή	**Γεώργιος Νικλητσιώτης**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΠΛ/ 07022**
Επιβλέπουσα	**Σινανιώτη Αριστέα, Καθηγήτρια Εμπορικού Δικαίου**

Ημερομηνία Παράδοσης **21 Νοεμβρίου 2011**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
ΑΡΙΣΤΕΑ ΣΙΝΑΝΙΩΤΗ Τακτική Καθηγήτρια	ΧΡΗΣΤΟΣ ΔΟΥΛΗΓΕΡΗΣ Καθηγητής	ΔΕΣΠΟΙΝΑ ΠΟΛΕΜΗ Επίκ. Καθηγήτρια

Περίληψη

Τα τελευταία χρόνια παρατηρούμε μεγάλη και ραγδαία εξέλιξη στους τομείς της τεχνολογίας και ειδικότερα στους τομείς της τεχνολογίας που σχετίζονται με τους ηλεκτρονικούς υπολογιστές. Στο δεύτερο κεφάλαιο θα δούμε ότι, τα «ηλεκτρονικά δεδομένα», οι «ηλεκτρονικές συναλλαγές» και τα «ηλεκτρονικά έγγραφα» έχουν αντικαταστήσει τα αντίστοιχα συμβατικά. Τα πρώτα δημιουργούνται, υφίστανται επεξεργασία, επαληθεύονται και αρχειοθετούνται με ηλεκτρονικά μέσα, δηλαδή χωρίς να υπάρχει η ανάγκη για ενσωμάτωσή τους σε υλικό φορέα, όπως είναι για παράδειγμα το χαρτί. Στο πλαίσιο αυτό βλέπουμε ότι υπάρχει μεγάλη ανάπτυξη στο ηλεκτρονικό εμπόριο και στις ηλεκτρονικές συναλλαγές. Το σημαντικότερο ζήτημα που προκύπτει στο ηλεκτρονικό εμπόριο (e-commerce) αλλά και γενικότερα στις ηλεκτρονικές επικοινωνίες είναι αυτό της ασφάλειας των συναλλαγών.

Στο τρίτο κεφάλαιο θα δούμε ότι, ο κάθε χρήστης που συναλλάσσεται ηλεκτρονικά μέσω του Διαδικτύου απαιτεί τα δεδομένα 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). Είναι επίσης, απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

Προκείμενου να καλυφθούν όλες αυτές οι απαιτήσεις γίνεται χρήση της ηλεκτρονικής υπογραφής. Η χρήση των (προηγμένων) «ηλεκτρονικών υπογραφών» και τα «ηλεκτρονικά πιστοποιητικά ταυτοποίησης» είναι εκείνα που εξασφαλίζουν την «αυθεντικότητα» και την «ακεραιότητα» των ηλεκτρονικών δεδομένων, την «ταυτοποίηση» των συναλλασσόμενων και κάτω από προϋποθέσεις, τη «νομική δέσμευση» του υπογράφοντα ή αλλιώς την «μη αποποίηση» της συναλλαγής, μπορούν επίσης να προσφέρουν αξιόπιστη λύση και στο ζήτημα της «εμπιστευτικότητας» των δεδομένων κατά την διακίνηση τους.

Στο τέταρτο κεφάλαιο θα δούμε ότι, για τις ηλεκτρονικές υπογραφές υπάρχει φυσικά και ένα αυστηρό νομοθετικό πλαίσιο σε ευρωπαϊκό και εθνικό επίπεδο, μέσα στο οποίο ορίζονται, οι προϋποθέσεις και οι τρόποι λειτουργίας και δημιουργίας των ηλεκτρονικών υπογραφών καθώς και η νομική τους ισχύ.

Στο πέμπτο κεφάλαιο θα παρουσιάσουμε το σύστημα υλοποίησης ψηφιακής υπογραφής PGP (Pretty Good Privacy), το οποίο είναι ένα από τα πιο διαδεδομένα προγράμματα υλοποίησης ψηφιακών υπογραφών. Τέλος, στο όγδοο κεφάλαιο θα υλοποιήσουμε μια ιστοσελίδα στην οποία θα εφαρμόσουμε ψηφιακή υπογραφή και ψηφιακό πιστοποιητικό.

Abstract

In recent years we observe large and rapid changes in technology and especially in technology related to computers. In the second chapter we see that, the "electronic data", the "electronic transactions" and "electronic documents" have replaced their conventional counterparts. The first generated, processed, verified and archived electronically, ie without the need for incorporation into a medium such as paper. In this context we see that there is strong growth in electronic commerce and electronic transactions. The most important question that arises in electronic commerce (e-commerce) and more generally to electronic communications is that the security of transactions.

In the third chapter we will see tha, each user is doing business electronically over the Internet requires the data sent can not be disclosed or made available to unauthorized people about it (confidentiality). The data should not be altered during transmission. The recipient should take them exactly as the sender sent them and be sure that the data received is what the sender sent (integrity). It is also necessary that the recipient can be sure of the identity of the sender (authenticity). Finally, participating in an electronic transaction should not be possible for parties to refuse subsequent participation in the transaction (no disclaimer).

To meet all these requirements is the use of electronic signatures. The use of (advanced) "electronic signature" and "electronic identification certificates" are those that ensure the "authenticity" and "integrity" of electronic data, "Identification" of transacting and under conditions, "legally binding" the undersigned or otherwise 'non-waiver "of the transaction may also provide a reliable solution to the issue of" confidentiality "of data in their movement.

In the fourth chapter we see that, for electronic signatures is of course a strict legislative framework at European and national level, in which defined the conditions and methods of operation and creation of electronic signatures and their legal effect.

In the fifth chapter will introduce the system for delivering digital signature PGP (Pretty Good Privacy), which is one of the most popular programs for implementing digital signatures. Finally, the eighth chapter will create a website which will apply digital signature and digital certificate.

Ευχαριστίες

Ευχαριστώ θερμά την καθηγήτρια μου, κυρία Σινανιώτη, για την πολύτιμη βοήθεια της και την συνεχή καθοδήγηση της σχετικά με την ορθή ανάπτυξη της παρούσας μεταπτυχιακής διατριβής και την σωστή διεκπεραίωση της. Επιπροσθέτως ευχαριστώ όλους τους καθηγητές του μεταπτυχιακού προγράμματος για το σύνολο των γνώσεων που μου προσέφεραν στον τομέα της Πληροφορικής και ιδιαιτέρως τους καθηγητές κύριο Δουληγέρη και κυρία Πολέμη. Τέλος, θα ήθελα να ευχαριστήσω ιδιαίτερα την οικογένεια μου για την συνεχή και πολύτιμη στήριξη και συμπαράσταση της καθ' όλη την διάρκεια της συγγραφής και ολοκλήρωσης της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Περιεχόμενα εικόνων

1. Εισαγωγη

Παρατηρούμε ότι καθ' όλη τη διάρκεια των τελευταίων ετών, υπάρχει πολύ μεγάλη και ραγδαία εξέλιξη σε όλους τους τομείς της τεχνολογίας. Επίσης, υπάρχει μια διαρκείς και αδήριτη ανάγκη για σταδιακή αντικατάσταση όλων των παραδοσιακών μέσων για την καταγραφή και απόδειξη μιας «συμβατικής συναλλαγής» (όπως είναι ενυπόγραφα ιδιωτικά έγγραφα, φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι, θεωρημένα τιμολόγια, κ.λ.π.), η αντικατάστασή τους γίνεται με τα αντίστοιχα «ηλεκτρονικά δεδομένα», τα οποία δημιουργούνται, υφίστανται επεξεργασία, επαληθεύονται και αρχειοθετούνται με ηλεκτρονικά μέσα, δηλαδή χωρίς να υπάρχει η ανάγκη για ενσωμάτωσή τους σε υλικό φορέα, όπως είναι για παράδειγμα το χαρτί. Τα πιο πάνω έχουν οδηγήσει στην ανάπτυξη συγκεκριμένων τεχνολογιών καθώς και μεθόδων, όπως οι «Υποδομές Δημοσίων Κλειδιών» – PKI, η «Pretty Good Privacy»–PGP, οι βιομετρικές μεθόδους, καθώς και πολλές άλλες μέθοδοι.

Επίσης, υπάρχει μια τεχνολογική επανάσταση στους τομείς της αναζήτησης, αποθήκευσης, ανάκτησης και μετάδοσης των κάθε είδους πληροφοριών, η οποία φέρνει την παγκόσμια κοινότητα μπροστά σε τεράστιες οικονομικές, κοινωνικές, νομικές και πολιτιστικές προκλήσεις. Στο πλαίσιο αυτό βλέπουμε ότι υπάρχει μεγάλη ανάπτυξη στο ηλεκτρονικό εμπόριο και στις ηλεκτρονικές συναλλαγές. Ένα από τα σημαντικότερα ζητήματα που προκύπτουν στο ηλεκτρονικό εμπόριο (e-commerce) αλλά και γενικότερα στις ηλεκτρονικές επικοινωνίες είναι αυτό της ασφάλειας των συναλλαγών.

Στην περίπτωση που η επικοινωνία δύο μερών γίνεται μέσω ενός κλειστού δικτύου, όπως είναι ένα τοπικό δίκτυο υπολογιστών (LAN), το πρόβλημα της ασφάλειας των συναλλαγών είναι σαφώς μειωμένο καθώς ο φορέας που λειτουργεί και ελέγχει το δίκτυο μπορεί σχετικά εύκολα να εντοπίσει τις τυχόν παρεμβολές ή και υποκλοπές στις επικοινωνίες του δικτύου.

Στην περίπτωση, όμως, που έχουμε επικοινωνία δύο μερών μέσω ενός ανοικτού, δημόσιου δικτύου, τότε δεν υπάρχει κανείς που να μπορεί να είναι σε θέση ώστε γνωρίζει αν το δίκτυο παρακολουθείται και σε ποιο σημείο του και κανείς δεν μπορεί να εγγυηθεί ότι τα μηνύματα θα φθάσουν ακέραια στον προορισμό τους. Οι τεχνικώς ασφαλείς αλλά και νομικώς αναγνωρισμένες ηλεκτρονικές συναλλαγές μέσω των «ανοικτών δικτύων» (όπως το διαδίκτυο, κ.λ.π.), αποτελούν τη βασική προϋπόθεση για την περαιτέρω ανάπτυξη του «ηλεκτρονικού επιχειρείν» και τη παροχή προηγμένων ηλεκτρονικών υπηρεσιών στην «Κοινωνία της Πληροφορίας».

Βλέπουμε λοιπόν ότι, 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). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

Μερικά από τα μεγαλύτερα προβλήματα στην ηλεκτρονική επικοινωνία δύο μερών μέσω ενός ανοικτού, ανασφαλούς δικτύου, όπως είναι το Internet, είναι τα εξής :

- Η επικοινωνία των δύο μερών μπορεί απλά να παρακολουθείται από τρίτους.
- Το περιεχόμενο των μηνυμάτων που ανταλλάσσονται όχι μόνο μπορεί να παρακολουθείται από τρίτους αλλά και να αλλοιωθεί σκόπιμα απ' αυτούς.
- Να μην είναι δυνατόν να εξακριβωθεί η ταυτότητα των επικοινωνούντων μερών.
- Πλαστοπροσωπία με τη χρήση πλαστής ηλεκτρονικής διεύθυνσης.

Γίνεται λοιπόν φανερό ότι 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.

Σε αυτό το σημείο θα πρέπει να 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.

Με την συνδυασμένη χρήση κρυπτογραφικών εργαλείων (αλγόριθμοι), κατάλληλα διαμορφωμένου λογισμικού (software), ειδικού υλισμικού και υποδομών (hardware) και συγκεκριμένων διαδικασιών (procedures), είναι δυνατόν σήμερα να προσφερθούν λύσεις που ικανοποιούν τις απαιτήσεις και τις λειτουργίες των συμβατικών συναλλαγών. Τέτοιες είναι οι (προηγμένες) «ηλεκτρονικές υπογραφές» και τα «ηλεκτρονικά πιστοποιητικά ταυτοποίησης» τα οποία εξασφαλίζουν την «αυθεντικότητα» (authentication) και την «ακεραιότητα» (integrity) των σχετικών δεδομένων, την «ταυτοποίηση» (identification) των συναλλασσόμενων και κάτω από προϋποθέσεις, τη «νομική δέσμευση» του υπογράφοντα ή αλλιώς την «μη αποποίηση» (non repudiation) της συναλλαγής. ενώ, παράλληλα, μπορούν να προσφέρουν αξιόπιστη λύση και στο ζήτημα της «εμπιστευτικότητας» (confidentiality) των δεδομένων κατά την διακίνηση ή/και την αρχειοθέτησή τους.

Από τα πιο πάνω, γίνεται αντιληπτό ότι όλοι οι χρήστες οι οποίοι συναλλάσσονται ηλεκτρονικά απαιτούν να υπάρχει πάντα σε αυτές τις συναλλαγές:

- **Εμπιστευτικότητα (Confidentiality):** 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. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. .
- **Ακεραιότητα (Integrity):** 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.
- **Μη Άρνηση Αποδοχής – Αυθεντικότητα (Non-Repudiation):** Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.
- **Πιστοποίηση - Μη αποποίηση ευθύνης (Authentication):** Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου με το οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Οι παραπάνω ιδιότητες, (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση ευθύνης) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή. 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 αρχικά, όπως ακριβώς το δημιούργησε και το απέστειλε σε αυτόν ο αποστολέας του.

Γίνεται αντιληπτό ότι όλα όσα αναφέρθηκαν θα ήταν κενά περιεχομένου και άνευ ουσίας αν δεν οργανώνονταν και δεν καλύπτονταν από ένα ολοκληρωμένο νομικό πλαίσιο, το οποίο υπάρχει σε ευρωπαϊκό αλλά και σε εθνικό επίπεδο και τα βασικά σημεία του θα παρουσιαστούν στην συνέχεια της παρούσας μεταπτυχιακής διατριβής. Στο σημείο αυτό αρκεί να αναφέρουμε ότι υπάρχουν σχετικές νομοθετικές ρυθμίσεις προσφέρουν στις ηλεκτρονικές συναλλαγές το κύρος, την ασφάλεια, την αναγνωρισιμότητα και την εμπιστοσύνη που διαθέτουν οι συμβατικές μέθοδοι.

2. Το Ηλεκτρονικο Έγγραφο

2.1 Εισαγωγή

Το πιο βασικό στοιχείο σχεδόν όλων των συναλλαγών στο Internet είναι το ηλεκτρονικό έγγραφο. Η νομική φύση του ηλεκτρονικού εγγράφου είναι εντελώς διαφορετική από αυτή των έγγραφων του άρθρου 160 ΑΚ και αυτό γιατί το ηλεκτρονικό έγγραφο στερείται κατά πρώτον ιδιόχειρης υπογραφής και δεύτερον στερείται της σταθερότητας κατά την ενσωμάτωσή του σε υλικό, το οποίο να παρουσιάζει διάρκεια ζωής.

Εάν κάνουμε αναφορά για το ηλεκτρονικό έγγραφο θα λέγαμε ότι πρόκειται για το σύνολο των δεδομένων, τα οποία έχουν εγγραφεί στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή και μπορούν να αποτυπωθούν κατά τρόπο αναγνώσιμο στην οθόνη του υπολογιστή, ενδεχομένως δε και να εκτυπωθούν σε υλικό φορέα με τη μορφή κειμένου ή εικόνων[1].

Το ηλεκτρονικό έγγραφο (electronic document) δεν είναι άμεσα αναγνώσιμο και αυτό γιατί αποτελείται από μαγνητικές εγγραφές, με αποτέλεσμα να καθίσταται αναγνώσιμο υπό μορφή κειμένου μόνο διαμέσου της οθόνης ενός τερματικού/υπολογιστή με τη μεσολάβηση πάντα, της κατάλληλης τεχνικής διαδικασίας, δηλαδή της μετατροπής των αρχειοθετημένων μαγνητικών εγγράφων σε εικόνα, γράμματα και λέξεις. Η χρήση του ηλεκτρονικού εγγράφου θεωρείται αυτονόητη σε συμβάσεις που καταρτίζονται ηλεκτρονικά, στο ηλεκτρονικό εμπόριο και σε ηλεκτρονικές βάσεις δεδομένων, όπως πελατολόγια ή αρχεία ασθενών νοσοκομείων. Το ηλεκτρονικό έγγραφο κυριαρχεί φυσικά και στο χώρο του Διαδικτύου, όπου ως ηλεκτρονικά έγγραφα θεωρούνται οι κάθε είδους εγγραφές στην οθόνη του υπολογιστή, όπως οι ηλεκτρονικές επιστολές (email), οι ιστοσελίδες (sites), τα αρχεία που διακινούνται μέσω Internet καθώς επίσης και οι τηλεδιασκέψεις που είναι αποτυπωμένες σε μαγνητικά μέσα (δισκέτες ή βιντεοκασέτες), οι τηλεφωνικές επαφές, οι ραδιοφωνικές εκπομπές και οι συζητήσεις που πραγματοποιούνται μέσω Internet το επονομαζόμενο Chat και γενικά κάθε είδους σταθερά ενσωματωμένες σε υλικό φορέα εγγραφές δεδομένων, που διακινούνται μέσω του διαδικτύου[2].

Με βάση τα πιο πάνω θα μπορούσε το ηλεκτρονικό έγγραφο να οριστεί ως κάθε έγγραφο που έχει το χαρακτηριστικό ότι δημιουργείται στο πλαίσιο και με τη βοήθεια της ηλεκτρονικής τεχνολογίας. Από τον ορισμό αυτόν αντιλαμβάνεται κανείς ότι πρέπει να θεωρούνται ηλεκτρονικά έγγραφα τόσο εκείνα που έχουν εξαρχής ηλεκτρονική υπόσταση, δηλαδή είναι άυλα, όσο και αυτά που έχουν μεν υλική υπόσταση αλλά το περιεχόμενό τους αποτυπώνεται και με τη βοήθεια της ηλεκτρονικής τεχνολογίας. Δεδομένου ότι είναι νομικά αδιάφορος ο τρόπος δημιουργίας του λοιπού περιεχομένου του εγγράφου εκτός από την υπογραφή του, είναι φανερό ότι η ειδοποιός διαφορά του ηλεκτρονικού εγγράφου από το παραδοσιακού τύπου έγγραφο έγκειται κατά βάση στο μέσον δημιουργίας της υπογραφής του, δηλαδή στο μέσον με το οποίο βεβαιώνεται η αυθεντικότητα του εγγράφου[3].

Στο σημείο αυτό κρίνεται σκόπιμο να αναφέρουμε ότι, όλα τα έγγραφα τα οποία αποθηκεύονται στη μνήμη ενός υπολογιστή ή ενός μαγνητικού μέσου καθώς επίσης, και όλα τα έγγραφα που διακινούνται ηλεκτρονικά, δηλαδή τα ηλεκτρονικά έγγραφα στο σύνολό τους, παρουσιάζουν μειονεκτήματα. Τα μειονεκτήματα των ηλεκτρονικών εγγράφων είναι το γεγονός ότι στερούνται της σταθερότητας κατά την ενσωμάτωσή τους και μπορεί να υποστούν μετατροπές, αλλοιώσεις ή διαγραφές που είναι αδύνατον να εντοπιστούν. Επίσης, δεν διαθέτουν ιδιόχειρη υπογραφή που είναι απαραίτητη στα έγγραφα όπου ο τύπος είναι συστατικός. Επιπλέον, πολύ σημαντικό μειονέκτημα είναι το γεγονός ότι κατά την διακίνηση αυτών των εγγράφων, μέσω ανοικτών δικτύων, υπάρχει πάντα σε μεγάλο βαθμό ο κίνδυνος να υποκλαπούν αυτά από τρίτους και να αλλοιωθεί ή να τροποποιηθεί το περιεχόμενό τους, με αποτέλεσμα να χάσουν την αξιοπιστία τους και την αυθεντικότητά τους.

[1] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ.49.
[2] Ιωάννης Κ. Καράκωστας, «Δίκαιο στο Internet, Νομικά Ζητήματα του Διαδικτύου», Αθήνα 2003, σελ. 183.
[3] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 10.

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 μέσω ανοιχτών δικτύων.

Προκειμένου να εξασφαλιστεί η γνησιότητα όλων των ηλεκτρονικών εγγράφων που διακινούνται ηλεκτρονικά χρησιμοποιείται ειδικότερα, η τεχνολογία της ηλεκτρονικής υπογραφής. Σήμερα, υπάρχουν δύο κύριοι τύποι συστημάτων κρυπτογραφίας που χρησιμοποιούνται με στόχο και σκοπό την παραγωγή της ηλεκτρονικής υπογραφής. Αυτά είναι, το συμμετρικό σύστημα κρυπτογράφησης και το ασύμμετρο σύστημα κρυπτογράφησης. Τα δυο πιο πάνω συστήματα κρυπτογραφίας θα παρουσιαστούν αναλυτικά στην συνέχεια της παρούσας μεταπτυχιακής διατριβής.

Παρά το νομοθετικό κενό που παρουσιάζεται στην ισχύουσα ελληνική νομοθεσία σε ότι αφορά τον σαφή ορισμό του τι είναι ηλεκτρονικό έγγραφο, θα μπορούσαμε να πούμε ότι στο άρθρο 2 παράγραφος 1 του π.κ. 150/2001 προκύπτει έμμεσα ο ορισμός του ηλεκτρονικού εγγράφου. Σύμφωνα λοιπόν με το άρθρο 2 παράγραφος 1, ως ηλεκτρονική υπογραφή ορίζονται τα «δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας»[4].

Από τον ορισμό αυτό προκύπτει ότι η ηλεκτρονική υπογραφή πρέπει να συνάπτεται σε δεδομένα με ηλεκτρονική μορφή, τα οποία και θα αποτελούν το λοιπό περιεχόμενο του ηλεκτρονικού εγγράφου. Βλέπουμε ότι η διάταξη πολύ σωστά δεν κάνει καμία διάκριση για το αν τα δεδομένα πρέπει να είναι καταχωρημένα σε κάποιο μαγνητικό μέσο όπως είναι ο σκληρός δίσκος, η δισκέτα, το zip, το chip ή το cd. Τέλος, η πιο πάνω διάταξη δεν απαιτεί να έχει εκτυπωθεί το περιεχόμενο του ηλεκτρονικού εγγράφου ή να έχει προβληθεί στην οθόνη τερματικού ή του υπολογιστή. Γίνεται λοιπόν αντιληπτό ότι, ως ηλεκτρονικό έγγραφο θα μπορούσε να νοηθεί κάθε υλικός φορέας καταχωρημένων ηλεκτρονικών δεδομένων.

Ηλεκτρονικό έγγραφο μπορούμε να πούμε ότι είναι ένα σύνολο δεδομένων, τα οποία έχουν εγγραφεί σε κάποιο μαγνητικό δίσκο ή άλλο μαγνητικό μέσο ενός ηλεκτρονικού υπολογιστή και στα οποία αφού πρώτα γίνει κάποια μορφή επεξεργασίας, μπορούν να αποτυπωθούν με βάση κάποιων εντολών του προγράμματος με τρόπο τέτοιο ώστε να είναι αναγνώσιμο στην οθόνη του μηχανήματος ή σε εκτυπωτή.

2.2 Γνήσια και μη γνήσια ηλεκτρονικά έγγραφα

Το ηλεκτρονικό έγγραφο όπως γίνεται φανερό δεν παρέχει τα εχέγγυα της γνησιότητας και της αυθεντικότητας που παρέχει ένα «συμβατικό έγγραφο». Αυτό συμβαίνει γιατί στερείται ιδιόχειρης υπογραφής και υλικής ενσωμάτωσης σε υλικό φορέα που παρουσιάζει διάρκεια ζωής[5]. Μπορούμε να πούμε ότι όλα τα ηλεκτρονικά έγγραφα χωρίζονται σε δύο μεγάλες κατηγορίες, αυτές οι κατηγορίες είναι: α) τα γνήσια ηλεκτρονικά έγγραφα και β) τα μη γνήσια ηλεκτρονικά έγγραφα.

Γνήσια θεωρούνται τα ηλεκτρονικά έγγραφα που έχουν αποκλειστικά ηλεκτρονική υπόσταση, δηλαδή καταχωρίσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό. Αντίθετα, τα μη γνήσια ηλεκτρονικά έγγραφα είναι έγγραφα με υλική μορφή, των οποίων το περιεχόμενο αλλά και η υπογραφή είναι ηλεκτρονικά αποτυπωμένα, μη γνήσια ηλεκτρονικά έγγραφα είναι η τηλεομοιοτυπία (fax) και το τηλέτυπο (telex)[6].

Η τηλεομοιοτυπία δηλαδή η διαδικασία παραγωγής του τηλεομοιότυπου, ορίζεται ως η «πιστή αναπαραγωγή από απόσταση κειμένων, σχεδίων και κάθε μορφής εντύπων με τη

[4] Άρθρο 2 αριθ. 1 του π.δ. 150/2001 περί προσαρμογής στην οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.
[5] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 76.
[6] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.12.

βοήθεια τερματικών διατάξεων», ενώ ως τηλεομοιότυπο ορίζεται «το λαμβανόμενο στο σταθμό λήψεως αντίτυπο». Το τηλεομοιότυπο μπορεί να συνιστά είτε αναπαραγωγή ενός προτύπου εγγράφου που εισάγεται στον τερματικό σταθμό αποστολής, είτε πρώτη εκτύπωση σε χαρτί ενός ηλεκτρονικού αρχείου που είναι αποθηκευμένο στο σκληρό δίσκο υπολογιστή, ο οποίος συνδέεται ηλεκτρονικά με τον τερματικό σταθμό αποστολής με ένα modem[7].

Για την αντιμετώπιση των κινδύνων κακόβουλης αλλοίωσης του κειμένου ή υποκλοπής των δεδομένων που περιέχει ένα ηλεκτρονικό έγγραφο, εφαρμόζονται διάφορες μέθοδοι κρυπτογράφησης, με τις οποίες επιτυγχάνεται η ασφαλής διαβίβαση των δεδομένων μέσω των δικτύων επικοινωνίας. Τις μορφές κρυπτογράφησης θα τις παρουσιάσουμε αναλυτικά στην συνέχεια της μεταπτυχιακής διατριβής σε επόμενο κεφάλαιο, εδώ απλά θα πρέπει να αναφέρουμε ότι στη μέθοδο κρυπτογράφησης και μάλιστα στη λεγόμενη ασύμμετρη κρυπτογράφηση, θεμελιώνεται και η τεχνική της ηλεκτρονικής υπογραφής, της οποίας η σημασία είναι μεγάλη, καθώς παρέχει τα εχέγγυα της αυθεντικότητας και της μη αλλοίωσης του κρυπτογραφημένου κειμένου[8].

2.3 Ασφάλεια των συναλλαγών στο ηλεκτρονικό εμπόριο

Όπως αναφέρθηκε και στην αρχή αυτής της μεταπτυχιακής διατριβής, υπάρχει τα τελευταία χρόνια, μεγάλη και ραγδαία εξέλιξη σε όλους τους τομείς της τεχνολογίας και στο μέλλον θα γίνει ακόμα μεγαλύτερη. Στο πλαίσιο αυτό, βλέπουμε ότι υπάρχει μεγάλη ανάπτυξη στο ηλεκτρονικό εμπόριο και στις ηλεκτρονικές συναλλαγές. Αυτή η διόγκωση του ηλεκτρονικού εμπορίου και των ηλεκτρονικών συναλλαγών φέρνει στο προσκήνιο την μεγάλη και επιτακτική ανάγκη για διασφάλιση όλων των ηλεκτρονικών συναλλαγών από εξωτερικούς κινδύνους.

Ως εξωτερικοί κίνδυνοι μπορούν να οριστούν οι όλες κακόβουλες άμεσες επιθέσεις στις ηλεκτρονικές συναλλαγές που πραγματοποιούνται μεταξύ ενός παρόχου υπηρεσιών και ενός καταναλωτή από κάποια άτομα τα οποία επιθυμούν να αλλοιώσουν την συναλλαγή ή έχουν ως στόχο τους την υπεξαίρεση στοιχείων ώστε να τα χρησιμοποιήσουν για ιδιοτελείς σκοπούς, ως τέτοια άτομα μπορεί να είναι οι λεγόμενοι hackers ή crackers. Εκτός από τις άμεσες επιθέσεις έχουμε και τις έμμεσες επιθέσεις με την χρήση ιών που καταργούν την αυθεντικότητα και την εγκυρότητα της ηλεκτρονικής συναλλαγής και οι χρήση τους αποσκοπεί στο να αλλοιώσει ή να καταστρέψει την συναλλαγή ή τα δεδομένα αυτής.

Όταν μιλάμε για ασφάλεια των συναλλαγών στο ηλεκτρονικό εμπόριο, μιλάμε για μεθόδους προστασίας των ηλεκτρονικών δεδομένων, είτε αποθηκευμένων είτε διαβιβαζομένων ηλεκτρονικά και τα οποία ο κάτοχος τους επιθυμεί να παραμείνουν κρυφά σε περίπτωση κλοπής ή απώλειας τους και να μεταβιβαστούν στον πραγματικό τους παραλήπτη χωρίς να έχουν υποστεί κανενός είδους αλλοίωσης ή καταστροφής. Οι μέθοδοι που χρησιμοποιούνται για την προστασία των ηλεκτρονικών δεδομένων, μπορεί να έχουν διάφορες μορφές, κάποιες από αυτές τις μορφές είναι η ηλεκτρονική υπογραφή, τα λεγόμενα firewalls, τα ειδικά συστήματα τηλεπικοινωνιών μεγάλης ασφάλειας, όπως τέτοια είναι τα πρωτόκολλα επικοινωνίας OPS, SAL[9].

Τα ανοικτά δίκτυα ηλεκτρονικής επικοινωνίας, όπως είναι το Internet, είναι τα δίκτυα εκείνα στα οποία μπορεί να συμμετέχει απεριόριστος και απροσδιόριστος αριθμός ατόμων, στην πραγματικότητα όπως είναι γνωστό συμμετοχή σε αυτά τα δίκτυα μπορεί να έχει ο κάθε ένας απλά θα πρέπει να πληρείται η προϋπόθεση ότι διαθέτει τα απαραίτητα τεχνικά μέσα. Αυτά τα μέσα δεν είναι τίποτα περισσότερο από έναν ηλεκτρονικό υπολογιστή, ένα modem, ένα κατάλληλο πρόγραμμα πλοήγησης και ένα κατάλληλο τηλεπικοινωνιακό δίκτυο. Σε όλα τα ανοικτά δίκτυα, γίνεται αντιληπτό ότι υπάρχει μεγάλη και επιτακτική ανάγκη για μεγάλη ασφάλεια και εμπιστευτικότητα και αυτό γιατί όλοι όσοι συμμετέχουν στα ανοικτά δίκτυα δεν γνωρίζονται μεταξύ τους, με αποτέλεσμα να μην είναι δυνατόν να υπάρξει εμπιστοσύνη εκ των προτέρων, ούτε φυσικά και ασφάλεια και εμπιστευτικότητα κατά τις ηλεκτρονικές συναλλαγές.

[7] Καραδημητρίου, ο.π., σελ. 13.
[8] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 49 – 50.
[9] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.10.

Σε αντίθεση με τα ανοικτά δίκτυα που είδαμε, έχουμε τα κλειστά δίκτυα. Στα κλειστά δίκτυα υπάρχει σαφώς μεγαλύτερη ασφάλεια και εμπιστοσύνη των ηλεκτρονικών συναλλαγών μεταξύ των ατόμων που βρίσκονται στα δίκτυα αυτά. Αυτό μπορεί και συμβαίνει γιατί σε κάθε κλειστό δίκτυο έχει την δυνατότητα και την πρόσβαση να συμμετέχει μόνο ένας κλειστός και αυστηρά συγκεκριμένος αριθμός ατόμων, ο οποίος είναι εκ των προτέρων καθορισμένος.

Γίνεται φανερό από τα πιο πάνω ότι, ο όγκος των ηλεκτρονικών συναλλαγών στα ανοικτά δίκτυα είναι πολύ πιο μεγάλος σε σύγκριση με τον αντίστοιχο αριθμό στα κλειστά δίκτυα. Αυτό έχει ως άμεση συνέπεια να είναι πολύ μεγαλύτερα και τα προβλήματα ασφάλειας στα ανοικτά δίκτυα, καθώς ο αντισυμβαλλόμενος σε ένα ανοικτό δίκτυο δεν είναι γνωστός εκ των προτέρων και αυτό έχει ως άμεση συνέπεια να μην μπορεί να είναι κανένας βέβαιος και σίγουρος για την πραγματική του ταυτότητα, για τις προθέσεις του, για τους σκοπούς του και τα κίνητρα του.

Τα συνηθέστερα προβλήματα ασφάλειας που παρουσιάζονται κατά καιρούς στις συναλλαγές στο ηλεκτρονικό εμπόριο είναι[10]:

1) **Παρακολούθηση των γραμμών επικοινωνίας.** Η παρακολούθηση και η υποκλοπή δεδομένων που αποστέλλονται μέσω του τηλεφωνικού δικτύου από Η/Υ σε Η/Υ είναι εύκολη, αν η τηλεφωνική γραμμή του χρήστη συνδεθεί με Η/Υ που έχει το κατάλληλο λογισμικό πρόγραμμα παρακολούθησης.

2) **Η κλοπή κλειδιών πρόσβασης ή συνθηματικών.** Εφόσον είναι εύκολη η παρακολούθηση γραμμών επικοινωνίας, είναι επίσης εύκολο να καταγραφούν και να υποκλαπούν ηλεκτρονικά κλειδιά ή συνθηματικά που χρησιμοποιούνται για πρόσβαση σε εμπιστευτικά στοιχεία ή αριθμοί πιστωτικών καρτών ή άλλα ευαίσθητα δεδομένα. Υπάρχουν για το σκοπό αυτό ειδικά ηλεκτρονικά προγράμματα, οι «ανιχνευτές κωδικών», οι οποίοι ανιχνεύουν και απομνημονεύουν το όνομα και τον προσωπικό κωδικό χρηστών Η/Υ τη στιγμή που αυτοί μπαίνουν στο πρόγραμμα του Η/Υ.

3) **Η υποκλοπή και τροποποίηση της μεταδιδόμενης πληροφορίας.** Πρόκειται για ενέργεια που μπορεί να επιφέρει στους παθόντες σοβαρή οικονομική ζημία και να προκαλέσει ανωμαλία στην ομαλή διεξαγωγή των συναλλαγών. Αν για παράδειγμα, ο υποκλοπέας διακόψει την επικοινωνία μεταξύ ενός εμπόρου και του προμηθευτή του σχετικά με την παραγγελία συγκεκριμένης ποσότητας εμπορευμάτων, τροποποιήσει τη μεταδιδόμενη πληροφορία και την επαναδρομολογήσει προς τον ανυποψίαστο προμηθευτή, τότε ο τελευταίος χωρίς να έχει αντιληφθεί ότι τροποποιήθηκε η πληροφορία, θα αποστείλει λανθασμένη ποσότητα εμπορευμάτων, προκαλώντας έτσι οικονομική ζημία τόσο στον ίδιο όσο και στο έμπορο.

4) **Η «μεταμφίεση» μέσω πλαστής ηλεκτρονικής διεύθυνσης.** Αποτελεί σύνηθες φαινόμενο για τους χρήστες του Διαδικτύου να πέφτουν θύματα παραπλάνησης κατά τις ηλεκτρονικές συναλλαγές τους από άτομα που χρησιμοποιούν πλαστή ηλεκτρονική διεύθυνση και ταυτότητα. Το αποτέλεσμα αυτής της ηλεκτρονικής «μεταμφίεσης» είναι να αποκτά ο δράστης πρόσβαση σε ηλεκτρονικά συστήματα ξεγελώντας τους μηχανισμούς ασφάλειας των συστημάτων αυτών.

2.4 Ιδιότητες μιας Ασφαλούς Ηλεκτρονικής Επικοινωνίας

Στις μέρες ήδη υπάρχει πολύ μεγάλη ανάπτυξη της τεχνολογίας και των ηλεκτρονικών επικοινωνιών και ηλεκτρονικών συναλλαγών. Βλέπουμε επίσης ότι, αυτή η ανάπτυξη είναι συνεχής και δημιουργείται έτσι η ανάγκη για επίλυση των προβλημάτων που παρουσιάστηκαν πιο πάνω, καθώς η επίτευξη της ασφάλειας στις ηλεκτρονικές συναλλαγές είναι επιτακτική όχι μόνο από τους παρόχους, όπως είναι εταιρίες, οργανισμοί, επιχειρήσεις αλλά η ανάγκη για ασφάλεια είναι επιτακτική κυρίως από τους καταναλωτές, οι οποίοι προκειμένου να κάνουν χρήση των ηλεκτρονικών συναλλαγών απαιτούν μεγάλο επίπεδο ασφάλειας και εμπιστευτικότητας. Αυτό γίνεται ακόμα πιο αντιληπτό αν σκεφτούμε ότι μπορεί σε μια μόνο ηλεκτρονική συναλλαγή να διακυβεύονται πολύ μεγάλα χρηματικά ποσά ή και απόρρητα

[10] Καραδημητρίου, ο.π., σελ. 22-23.

έγγραφα, τα οποία οι συμβαλλόμενοι όχι μόνο επιθυμούν αλλά απαιτούν και θεωρούν δεδομένο ότι θα πρέπει να πληρούνται η ασφάλεια, η εμπιστευτικότητα, η αυθεντικότητα και η γνησιότητα σε όλα τα στάδια των συναλλαγών μέσα από την καθιέρωση ενός προηγμένου συστήματος επικοινωνίας μεταξύ των συναλλασσομένων.

Η Ευρωπαϊκή Επιτροπή , με στόχο και γνώμονα την προώθηση του ηλεκτρονικού εμπορίου, αναφέρει: «Για να αναπτυχθεί το ηλεκτρονικό εμπόριο, τόσο οι καταναλωτές όσο και οι προμηθευτές πρέπει να είναι βέβαιοι ότι η συναλλαγή τους δεν θα διακοπεί ή αλλοιωθεί, ότι ο αγοραστής και ο πωλητής είναι αυτοί που ισχυρίζονται ότι είναι και ότι οι συναλλακτικοί μηχανισμοί είναι διαθέσιμοι, νόμιμοι και ασφαλείς. Το χτίσιμο αυτής της εμπιστοσύνης και της πίστης αποτελεί απαραίτητη προϋπόθεση για να προσελκύσουμε προμηθευτές και καταναλωτές στο ηλεκτρονικό εμπόριο»[11].

Προκειμένου η τεχνολογία της επικοινωνίας να ανταποκριθεί επαρκώς στις σημερινές συναλλακτικές ανάγκες, γίνεται αποδεκτό ότι πρέπει να παρέχει στους συναλλασσόμενους τις παρακάτω τέσσερις ιδιότητες[12]:

1. **Να πιστοποιεί την αυθεντικότητα της ταυτότητας του κάθε συναλλασσομένου.** Το γεγονός ότι η ηλεκτρονική συναλλαγή διενεργείται μεταξύ ατόμων αγνώστων μεταξύ τους καθιστά επιτακτική την διαπίστωση της του αντισυμβαλλομένου.
2. **Να διαφυλάσσει την ακεραιότητα, δηλαδή το αναλλοίωτο του περιεχομένου του μηνύματος.** Ο παραλήπτης πρέπει να λαμβάνει το μήνυμα όπως ακριβώς το έστειλε ο αποστολέας και πρέπει να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει. Η ανάγκη της ακεραιότητας πηγάζει από το γεγονός ότι ένα ηλεκτρονικό έγγραφο αλλοιώνεται πολύ εύκολα με τρόπο που δεν εντοπίζεται, ώστε κάθε αντίγραφο ηλεκτρονικού εγγράφου αποτελεί τέλεια αναπαραγωγή του προτύπου.
3. **Να εξασφαλίζει την εμπιστευτικότητα**. Δηλαδή αφενός την προστασία του αποστελλόμενου μηνύματος από την πρόσβαση σε αυτό μη εξουσιοδοτημένων προσώπων και αφετέρου σε περίπτωση που επιτυγχάνεται παράνομη πρόσβαση στο μήνυμα, την αδυναμία του εισβολέα να το διαβάσει (π.χ. μέσω κρυπτογράφησης μηνύματος).
4. **Να εξασφαλίζει τη μη αποποίηση ευθύνης.** Δηλαδή την ανυπαρξία δυνατότητας των εμπλεκομένων σε μια ηλεκτρονική συναλλαγή μερών να αρνηθούν εκ των υστέρων τη συμμετοχή του στη συναλλαγή αυτή. Ο αποστολέας δεδομένων δεν πρέπει να έχει τη δυνατότητα να αρνηθεί ότι δημιούργησε και απέστειλε το ηλεκτρονικό μήνυμα. Υπάρχουν διάφορα είδη μη αποποίησης ενός ηλεκτρονικού εγγράφου ή ηλεκτρονικού μηνύματος γενικότερα, όπως είναι η μη αποποίηση της δημιουργίας της προέλευσης, της λήψης ή της αποδοχής του εγγράφου.

Αυτές είναι οι τέσσερις ιδιότητες, οι οποίες εξασφαλίζονται με τον καλύτερο δυνατό τρόπο με τη χρήση της προηγμένης ηλεκτρονικής υπογραφής.

[11] Commission of the European Communities «A European initiative in Electronic Commerce» COM (97) 157 final, 16/4/1997.
[12] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 25.

3. Ηλεκτρονικη Υπογραφη

3.1 Ορισμός Ηλεκτρονικής Υπογραφής

Εάν επιχειρούσαμε να δώσουμε έναν γενικό ορισμό για την υπογραφή, θα μπορούσαμε να πούμε ότι ως υπογραφή ορίζεται η χειρόγραφη αποτύπωση από ένα φυσικό πρόσωπο του ονοματεπωνύμου του. Αυτή η χειρόγραφη αποτύπωση θεωρείται παραδοσιακά ότι δηλώνει τη βούληση του υπογράφοντος και την πρόθεση του να δεσμευτεί από το περιεχόμενο του εγγράφου που υπογράφει. Επίσης, πιστοποιεί την προέλευση του από αυτόν και αποτελεί ένα ιδιαίτερης σημασίας αποδεικτικό μέσο σε περίπτωση δικαστικής διένεξης. Η ιδιόχειρη υπογραφή εξασφαλίζει την εξατομίκευση του συντάκτη του εγγράφου, αφού σε κάθε πρόσωπο αντιστοιχεί ένας μοναδικός και προσωπικός γραφικός χαρακτήρας. Με τον τρόπο αυτόν, καθίσταται δύσκολη η απομίμηση της υπογραφής από τρίτα πρόσωπα και διευκολύνεται ο έλεγχος ης γνησιότητας της με βάση ατομικά δείγματα υπογραφής. Στην ευρύτερη έννοια της υπογραφής εμπίπτουν και η σφραγίδα ή η υπογραφές που δημιουργούνται με μηχανικά μέσα και παρέχουν διαφορετικές διαβαθμίσεις ασφάλειας.

Η διαρκείς ανάπτυξη των ηλεκτρονικών συναλλαγών και η μεγάλη αύξηση από όλο και περισσότερα άτομα και εταιρείες που χρησιμοποιούν ψηφιακά έγγραφα αντί για έντυπα έγγραφα για τη διεξαγωγή των καθημερινών τους συναλλαγών έκανε εμφανή την ανάγκη χρήσης μιας υπογραφής ανάλογης με την ιδιόχειρη, η οποία θα μπορούσε να χρησιμοποιηθεί σε ηλεκτρονικό περιβάλλον, δηλαδή στο Διαδίκτυο ή σε συναλλαγές με ηλεκτρονικά μηχανήματα όπως για παράδειγμα ΑΤΜ. Επίσης, με τη μείωση της εξάρτησης από τα έντυπα έγγραφα και την ολοένα και αυξανόμενη χρήση των ψηφιακών εγγράφων, γίνεται επιτακτική η ανάγκη για ασφάλεια και εμπιστευτικότητα. Οι ηλεκτρονικές υπογραφές υποστηρίζουν αυτήν την αλλαγή και καλύπτουν με τον καλύτερο δυνατό τρόπο τις ανάγκες που έχουν εμφανιστεί, παρέχοντας διασφαλίσεις σχετικά με την εγκυρότητα και την αυθεντικότητα ενός ψηφιακού εγγράφου. Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που αυτό έφερε καθώς, τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα παραδοσιακά χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται εικονική – ηλεκτρονική καθώς θα πρέπει να συνοδεύει το εκάστοτε ηλεκτρονικό έγγραφο ή την εκάστοτε ηλεκτρονική συναλλαγή.

Με τον όρο «ψηφιακή υπογραφή» ή «ηλεκτρονική υπογραφή» εννοούμε «μια συμβολοσειρά από δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας»[13]. Με βάση αυτόν τον ορισμό προκύπτει ότι η ηλεκτρονική υπογραφή μπορεί να είναι ένα οποιοδήποτε ηλεκτρονικό ανάλογο μιας ιδιόγραφης υπογραφής ή αλλιώς ένα οποιοδήποτε ψηφιακό προσδιοριστικό που επικυρώνει μια ηλεκτρονική συναλλαγή.

Από τα πιο πάνω γίνεται αντιληπτό ότι υπάρχουν πολλοί τρόποι, περισσότερο ή λιγότερο ασφαλείς, για να υπογράψει κανείς ηλεκτρονικά και με αυτό τον τρόπο είτε να δείξει την πρόθεσή του να δεσμευτεί από την υπογραφή του και από το περιεχόμενο του εγγράφου, είτε να επιβεβαιώσει την ταυτότητά του. Παραδείγματα επισφαλών ηλεκτρονικών υπογραφών, δηλαδή που δεν πληρούν τις τέσσερις ιδιότητες μιας ασφαλούς ηλεκτρονικής επικοινωνίας είναι[14]:

1. Η απλή ηλεκτρονική αναφορά του ονόματος του συγγραφέα στο τέλος ενός ηλεκτρονικού εγγράφου.
2. Η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση που έχει οριστεί και χρησιμοποιείται από τον ίδιο τον αποστολέα ενός e-mail.
3. Μια ψηφιακή εικόνα χειρόγραφης υπογραφής που προσαρτάται στο τέλος ενός ηλεκτρονικού αρχείου.

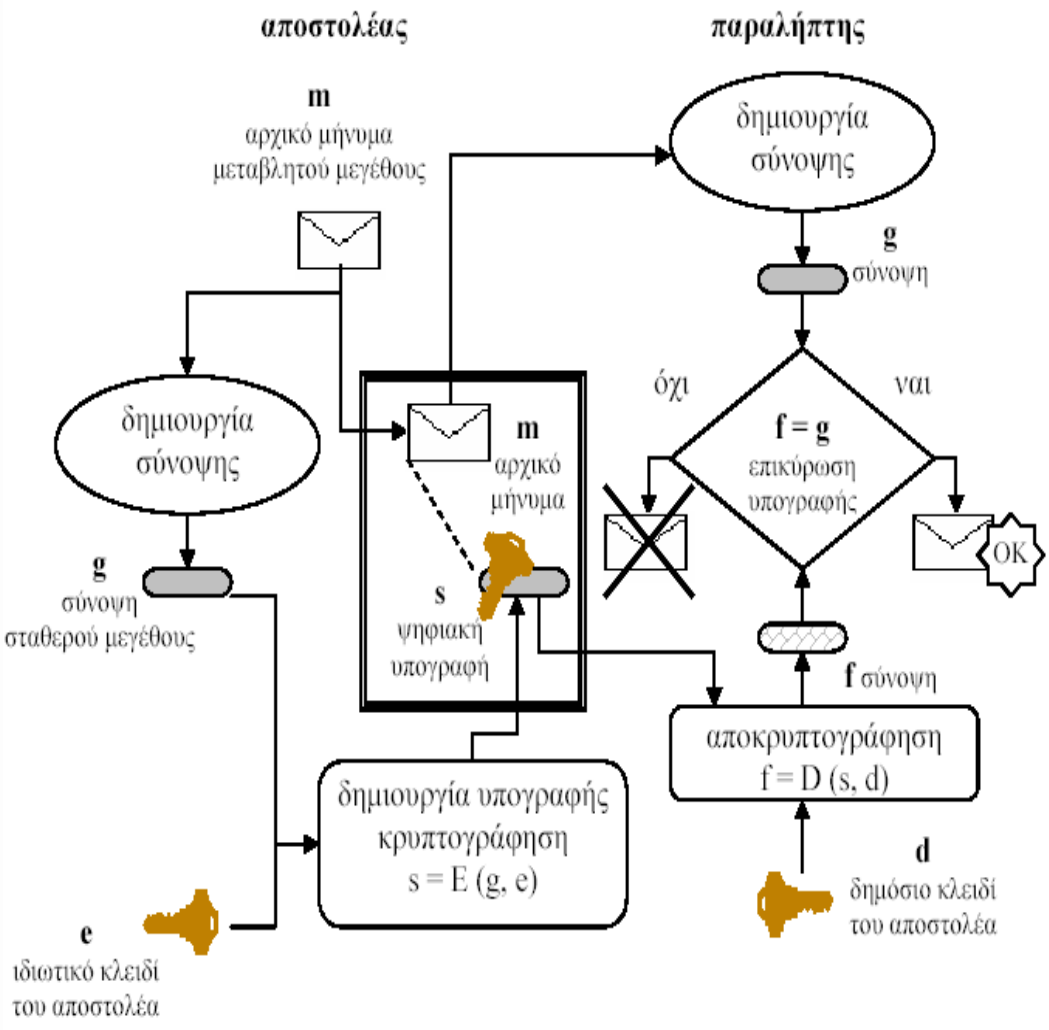
[13] Άρθρο 2 παράγραφος 1 π.δ. 150/2001
[14] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 29-31.

4. Η επιλογή με το ποντίκι του Η/Υ του εικονιδίου «ναι», ως πράξη αποδοχής, σε μια ιστοσελίδα κατά την κατάρτιση ηλεκτρονικής σύμβασης μεταξύ καταναλωτή και προμηθευτή.
5. Ένα σήμα που ο αποστολέας το χρησιμοποιεί για να αυτοσυστήνεται, όπως ένας ήχος ή μια εικόνα.

Παραδείγματα αρκετά ασφαλών ηλεκτρονικών υπογραφών, οι οποίες πληρούν μερικές ή όλες τις ιδιότητες μιας ασφαλούς ηλεκτρονικής επικοινωνίας είναι:

1. Η υπογραφή που βασίζεται στην εκ των προτέρων γνώση κάποιου κωδικού, όπως μια λέξη-κλειδί ή ένας μυστικός αριθμός PIN.
2. Η υπογραφή που βασίζεται στη συμμετρική ή ασύμμετρη κρυπτογραφία.
3. Η υπογραφή που στηρίζεται σε βιομετρικό σύστημα πιστοποίησης της ταυτότητας.

Αυτά τα τρία είδη υπογραφής θα παρουσιαστούν και στην συνέχεια της παρούσας μεταπτυχιακής διατριβής.



Εικόνα 1. Ψηφιακή Υπογραφή

Όπως γίνεται αντιληπτό από τα πιο πάνω, οι ηλεκτρονικές υπογραφές αποτελούν το ηλεκτρονικό ισοδύναμο των χειρόγραφων υπογραφών. Σύμφωνα με το άρθρο 3 του προεδρικού διατάγματος 150/2001 η ψηφιακή υπογραφή εξομοιώνεται με την ιδιόχειρη. Η ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

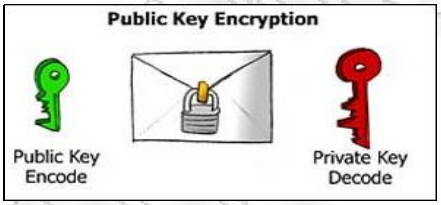
Στο Ελληνικό Δίκαιο υπάρχει μια πρόβλεψη ειδική, με την οποία έχουμε την εισαγωγή του όρου «ψηφιακή υπογραφή» αντί του όρου «ηλεκτρονική υπογραφή». Επίσης, δίνεται ο ορισμός της ψηφιακής υπογραφής ως εξής: «Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή[15]:

α) συνδέεται μονοσήμαντα με τον υπογράφοντα,

β) ταυτοποιεί τον υπογράφοντα, δηλαδή να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος

γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό έλεγχό του και

δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων».



Εικόνα 2. Κρυπτογράφηση ιδιωτικό – δημόσιο κλειδί

Σύμφωνα με τα όσα πιο πάνω αναφέρθηκαν, μπορούμε να πούμε ότι, η ηλεκτρονική υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει, είναι το σύνολο των ηλεκτρονικών δεδομένων, τα οποία συνοδεύουν ένα ηλεκτρονικό έγγραφο ή μια ηλεκτρονική συναλλαγή και ουσιαστικά επιτελούν αυτό ακριβώς που επιτελεί και η παραδοσιακή υπογραφή στα παραδοσιακά έγγραφα.

Η ηλεκτρονική υπογραφή αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί ή αλλοιωθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι, δηλαδή η ηλεκτρονική υπογραφή διασφαλίζει και υποδηλώνει την γνησιότητα του ηλεκτρονικού εγγράφου. Ουσιαστικά λοιπόν, η ηλεκτρονική υπογραφή είναι μονοσήμαντη και εξατομικεύει απόλυτα τον υπογράφοντα.

Θα λέγαμε πιο αναλυτικά ότι, ως ηλεκτρονική υπογραφή, δεν νοείται απλά η ηλεκτρονική αποτύπωση της ιδιόχειρης υπογραφής αλλά στην ουσία πρόκειται για «μια κλειδωμένη σύντμηση ηλεκτρονικού κειμένου», η οποία θα μπορούσε να χαρακτηριστεί και ως «δακτυλικό αποτύπωμα» αυτού[16]. Η ηλεκτρονική υπογραφή παρέχει σε ένα ηλεκτρονικό έγγραφο την εγγύηση της αυθεντικότητας, της εμπιστευτικότητας, της γνησιότητας και της μη αλλοίωσής του.

[15] Σύμφωνα με τον Ν. 2672/1999
[16] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 109.

Έχει επιβεβαιωτική λειτουργία, δηλαδή ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις και εμπιστευτική λειτουργία, δηλαδή μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα. Τέλος, οι ηλεκτρονικές υπογραφές συνδέονται με τα υπογεγραμμένα δεδομένα με τέτοιο τρόπο ώστε οποιαδήποτε επέμβαση να μπορεί να γίνει αντιληπτή, αλλά και να μπορεί επίσης να αναγνωριστεί ο αποστολέας πέρα από κάθε αμφιβολία.

3.2 Ηλεκτρονική Υπογραφή – Ιδιόχειρη υπογραφή

Η ηλεκτρονική υπογραφή μπορούμε να πούμε ότι υπηρετεί τους ίδιους σκοπούς ύπαρξης με αυτούς της ιδιόχειρης υπογραφής. Όπως αναφέρθηκε πιο πάνω, 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. Οι βασικές από τις διαφορές των δύο υπογραφών παρουσιάζονται στον πιο κάτω πίνακα.

Ιδιόχειρη υπογραφή	Ηλεκτρονική υπογραφή
Είναι ενσωματωμένη στο μήνυμα	Αποτελεί εξωτερικό «αντικείμενο», το οποίο συνδέεται με το μήνυμα
Για όλους τους σκοπούς χρησιμοποιείται η ίδια υπογραφή	Έχουμε διαφορετικές υπογραφές για διαφορετικούς σκοπούς
Υπάρχει η δυνατότητα πλαστογράφησης	Είναι σχεδόν αδύνατη η «πλαστογράφησή» της
Πιστοποιεί την ταυτότητα του υπογράφοντος	Πιστοποιεί τη γνησιότητα του περιεχομένου της πληροφορίας και την ταυτότητα του υπογράφοντος
Είναι απευθείας ορατή	Απαιτείται ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια για να είναι ορατή
Ο «μηχανισμός» δημιουργίας της παραμένει ο ίδιος και δεν μπορεί να αποσυρθεί	Ο μηχανισμός δημιουργίας, επαλήθευσής 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. Από τα πιο πάνω γίνεται άμεσα αντιληπτό ότι υπάρχουν ουσιαστικές διαφορές μεταξύ των δύο ειδών υπογραφών. 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.

Συνοψίζοντας τα πιο πάνω θα λέγαμε ότι η χειρόγραφη υπογραφή αποτελεί μέρος του φυσικού εγγράφου που υπογράφεται. Ωστόσο η ηλεκτρονική υπογραφή δεν προσαρτάται

φυσικά στο μήνυμα που υπογράφεται, άρα ο αλγόριθμός που χρησιμοποιείται πρέπει κάπως να «δένει» την υπογραφή με το μήνυμα. Δευτερευόντως, προκύπτει το ζήτημα της επαλήθευσης. Η χειρόγραφη υπογραφή επαληθεύεται από την σύγκρισή της με άλλες, αυθεντικές υπογραφές. Για παράδειγμα, όταν κάποιος υπογράφει αγορά πιστωτικής κάρτας, ο πωλητής υποτίθεται ότι συγκρίνει την υπογραφή στο απόκομμα πώλησης με το πίσω μέρος της πιστωτικής κάρτας για να επαληθεύσει την υπογραφή. Φυσικά, αυτή δεν είναι και πολύ ασφαλής μέθοδος καθώς εύκολα πλαστογραφεί κανείς την υπογραφή κάποιου. Από την άλλη πλευρά, οι ψηφιακές υπογραφές μπορούν να επαληθευτούν χρησιμοποιώντας έναν δημόσιο γνωστό αλγόριθμο επαλήθευσης, Έτσι, μπορεί οποιοσδήποτε να επαληθεύσει μια ψηφιακή υπογραφή. Η χρήση ενός ασφαλούς σχήματος υπογραφής προλαμβάνει τη δυνατότητα πλαστογραφήσεων.

Τέλος, μια άλλη σημαντική διαφορά μεταξύ των χειρόγραφων και των ηλεκτρονικών υπογραφών είναι ότι ένα αντίγραφο του υπογεγραμμένου ψηφιακού μηνύματος είναι ταυτόσημο με το πρωτότυπο. Από την άλλη πλευρά, ένα αντίγραφο υπογεγραμμένου εγγράφου μπορούμε συνήθως να το ξεχωρίσουμε από ένα πρωτότυπο. Αυτό το χαρακτηριστικό σημαίνει ότι πρέπει να προσέξουμε ώστε να προληφθεί η νέα χρήση ενός υπογεγραμμένου ψηφιακού μηνύματος. Για παράδειγμα, εάν το μέλος Α υπογράφει εάν ψηφιακό μήνυμα εξουσιοδοτώντας το μέλος Β για ανάληψη 100€ από τον τραπεζικό του λογαριασμό, θέλει απλώς να κρατήσει τον Β ικανό να το κάνει μια φορά. Έτσι, το ίδιο το μήνυμα θα πρέπει να περιλαμβάνει πληροφορίες όπως η ημερομηνία που προλαμβάνουν τη δεύτερη χρήση.

3.3 Ηλεκτρονική Υπογραφή που Βασίζεται στην εκ των Προτέρων Γνώση του Κώδικα

Αυτό το είδος της ηλεκτρονικής υπογραφής έχει γίνει ευρύτερα γνωστό κυρίως από τη χρήση PIN στις τραπεζικές συναλλαγές και στις τραπεζικές κάρτες που χρησιμεύουν για την ανάληψη ή κατάθεση χρηματικών ποσών στα μηχανήματα αυτόματης ανάληψης ΑΤΜ. Αποτελεί μια πολύ απλή μορφή ηλεκτρονικής υπογραφής, γιατί στερείται μοναδικότητας και προσωπικού χαρακτήρα, ενώ ταυτόχρονα απαιτεί από τα μέρη να έχουν μια προϋπάρχουσα μεταξύ τους σχέση.

Συνέπεια αυτού του γεγονότος είναι ο κωδικός να μπορεί να κλαπεί ή να υποστεί τέλεια αντιγραφή και να χρησιμοποιηθεί από άλλον χρήστη μη δικαιούχο, χωρίς τη δυνατότητα διάγνωσης από το ίδιο το μηχάνημα όπου χρησιμοποιείται ο κωδικός, παρά μόνο από τον πραγματικό κάτοχο του γνήσιου κώδικα, όταν για παράδειγμα ελέγχει το υπόλοιπο του τραπεζικού του λογαριασμού ή της πιστωτικής του κάρτας[17].

3.4 Ηλεκτρονική Υπογραφή που Βασίζεται στην Κρυπτογραφία

3.4.1 Εισαγωγικά για την Κρυπτογραφία

Η ανάγκη για την διαφύλαξη των μυστικών μέσω της κρυπτογραφίας βλέπουμε ότι είναι αισθητή ήδη από τα αρχαία χρόνια. Πιο συγκεκριμένα, ήδη από το 1500 π.χ στη πόλη της Βαβυλώνας έχουμε το πρώτο κρυπτογραφημένο κείμενο. Χρόνια αργότερα στην αρχαία Ελλάδα έχουμε στην αρχαία Σπάρτη, τους Σπαρτιάτες να κάνουν χρήση κρυπτογράφησης και στην Ρωμαϊκή εποχή γνωρίζουμε ότι ο Ιούλιος Καίσαρας έκανε χρήση κρυπτογράφησης με την μέθοδο της αντικατάστασης και της μετάθεσης των γραμμάτων των λέξεων. Στην πιο σύγχρονη εποχή βλέπουμε ότι κατά τον Β' Παγκόσμιο Πόλεμο οι Γερμανοί χρησιμοποιούν ευρέως τον κρυπτογραφικό κώδικα Enigma για στρατιωτικούς σκοπούς.

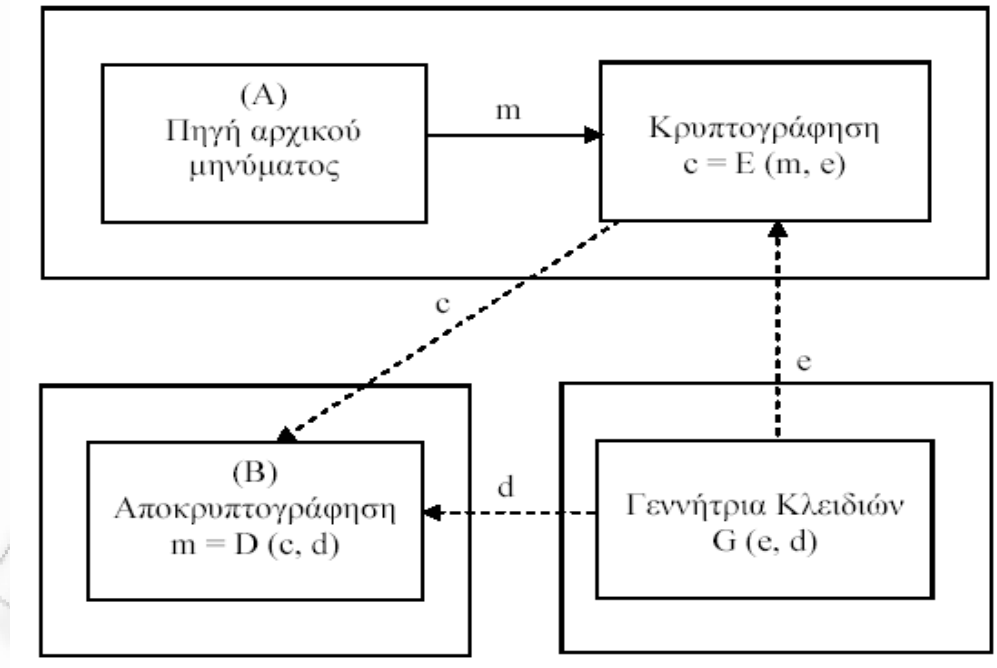
Στις μέρες μας η κρυπτογραφία έχει αναπτυχθεί πάρα πολύ και αποτελεί σημαντικό μέσο για την ανάπτυξη και την ασφάλεια του ηλεκτρονικού περιβάλλοντος. Στην εποχή μας που όλο ένα και περισσότερες ηλεκτρονικές συναλλαγές πραγματοποιούνται, υπάρχει η ανάγκη και η ζήτηση από τον επιχειρηματικό κόσμο αλλά και από απλούς καταναλωτές για όλο και πιο

[17] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.31-32.

ισχυρή κρυπτογραφία, προκειμένου να προστατεύεται το απόρρητο των επικοινωνιών. Με την συνεχή ανάπτυξη των μαθηματικών τα τελευταία χρόνια, η κρυπτογραφία έχει σήμερα την έννοια του μετασχηματισμού ηλεκτρονικών δεδομένων με τη χρήση αλγορίθμων, έτσι ώστε να μπορούν αυτοί να αναγνωστούν μόνο με την βοήθεια ενός κλειδιού αποκρυπτογράφησης.

Όταν λοιπόν, αναφερόμαστε στην «κρυπτογραφία» αναφερόμαστε γενικά σε μια μέθοδο κωδικοποίησης του περιεχομένου του ηλεκτρονικού μηνύματος που διαβιβάζεται με ηλεκτρονικά μέσα, σύμφωνα με προκαθορισμένο μυστικό κώδικα. Πιο αναλυτικά θα μπορούσαμε να πούμε ότι με τον όρο «κρυπτογραφία» εννοείται η μετατροπή των δεδομένων ενός ηλεκτρονικού υπολογιστή με τη χρησιμοποίηση αλγορίθμων κατά τέτοιο τρόπο, ώστε τα δεδομένα να μπορούν να αναγνωσθούν μόνο με τη χρήση ανάλογων κλειδιών αποκρυπτογράφησης. Η κρυπτογραφία αποτελεί εφαρμογή της επιστήμης των μαθηματικών. Με τη χρήση αυτής της μεθόδου το περιεχόμενο ενός μηνύματος μπορεί να γίνει γνωστό μόνο σε όσους διαθέτουν το ανάλογο «κλειδί» με αυτόν τον τρόπο εξασφαλίζεται το απόρρητο στις ηλεκτρονικές επικοινωνίες[18].

Στην πιο κάτω εικόνα, αποτυπώνεται η γενική μορφή ενός σύγχρονου κρυπτογραφικού συστήματος. Υποθέτουμε ότι ένας χρήστης Α και ένας χρήστης Β θέλουν να έχουν μια ασφαλή επικοινωνία. Αρχικά, πρέπει να διαλέξουν ή να ανταλλάξουν ένα ζεύγος κλειδιών (e,d). Στη συνέχεια, όταν ο Α (αποστολέας) θελήσει να στείλει μυστικά δεδομένα m στον Β (παραλήπτη), εφαρμόζεται μια μαθηματική συνάρτηση Ε, η οποία χρησιμοποιεί ως παράμετρο το κλειδί e, με σκοπό τον υπολογισμό του κρυπτογραφήματος c = E (m, e). Το κρυπτογράφημα c αποστέλλεται στον Β. Μόλις αυτός το λάβει, εφαρμόζεται μια αντίστροφη μαθηματική συνάρτηση D, η οποία χρησιμοποιεί το άλλο κλειδί d, με σκοπό τον υπολογισμό του m = D (c, d). Οπότε ανακτώνται τα αρχικά δεδομένα m.



Εικόνα 3. Γενική Μορφή Κρυπτογραφικού Συστήματος

Οι βασικές τεχνολογικές εφαρμογές της κρυπτογραφίας είναι σήμερα η κρυπτοθέτηση (encryption) και η ηλεκτρονική υπογραφή (electronic signature). Επίσης, η κρυπτογράφηση σε

[18] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 108.

επίπεδο φωτονίων και η στεγανογραφία αποτελούν σημαντικά πεδία έρευνας για την κρυπτογράφηση στο μέλλον.

Η ουσιαστική διαφορά της κρυπτοθέτησης σε σχέση με την ηλεκτρονική υπογραφή είναι ότι στην πρώτη τα δεδομένα που διαβάζονται από τον συναλλασσόμενο προς ένα φορές υπηρεσιών ηλεκτρονικού εμπορίου ή τηλεπικοινωνιών, κρυπτογραφούνται αλλά δεν υπογράφονται ηλεκτρονικά. Κατά συνέπεια, αν και διασφαλίζεται το απόρρητο της επικοινωνίας δεν είναι δυνατόν να διαπιστωθεί η ταυτότητα του αποστολέα των ηλεκτρονικών δεδομένων. Η κρυπτοθέτηση χρησιμοποιείται ευρέως και πολλές φορές σε συνδυασμό με συστήματα ηλεκτρονικής υπογραφής, συνήθως από σταθμούς συνδρομητικής τηλεόρασης, από τράπεζες κατά την εκτέλεση on-line τραπεζικών συναλλαγών. Τα πιο γνωστά συστήματα κρυπτοθέτησης που σήμερα χρησιμοποιούνται είναι το SSL και το SET[19].

Η ανάγκη λοιπόν, για εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την κρυπτογραφία. Κατά την κρυπτογραφία ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, προκειμένου με αυτό τον τρόπο να μετατρέψει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο δηλαδή σε κρυπτογραφημένο κείμενο.

Ο παραλήπτης, έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί, αφού κάθε φορά την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης την γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης. Εάν για οποιονδήποτε λόγο κάποιος τρίτος εκτός του αποστολέα και του παραλήπτη γνωρίζει ή μάθει την αποκρυπτογράφηση του κειμένου τότε η εμπιστευτικότητα, η αυθεντικότητα και η ακεραιότητα του κειμένου παύουν να υφίστανται.

Οι διάφορες μέθοδοι κρυπτογράφησης βασίζονται στη χρήση ενός «κλειδιού», ενός μαθηματικού δηλαδή κώδικα - αλγόριθμου, ο οποίος διασφαλίζει το μη «αναγνώσιμο» από τρίτους, και χρησιμοποιείται στην κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε αλγόριθμος παίρνει την ονομασία του από τον αριθμό που μεταλλάσσεται και πρέπει να βρεθεί με μια σειρά μαθηματικών πράξεων. Τα κυριότερα συστήματα κρυπτογραφίας είναι εκείνο της συμμετρικής κρυπτογραφίας και εκείνο της ασυμετρικής ή ασύμμετρης κρυπτογραφίας. Το σύστημα της συμμετρικής κρυπτογραφίας βασίζεται στην ύπαρξη ενός αλγοριθμικού κλειδιού, με βάση το οποίο το μεταδιδόμενο μήνυμα κρυπτογραφείται και αποκρυπτογραφείται, όπως είναι για παράδειγμα το Data Encryption System. Αντίθετα, το σύστημα της ασύμμετρης κρυπτογραφίας βασίζεται στην ύπαρξη δύο κλειδιών, ενός ιδιωτικού, το οποίο είναι το κλειδί της κρυπτογράφησης και ενός δημόσιου που είναι το κλειδί της αποκρυπτογράφησης, τα δύο αυτά κλειδιά λειτουργούν πάντοτε σας ζεύγος, σε αυτό το σύστημα έχουμε το παράδειγμα του συστήματος RSA[20]. Ανάλυση των δυο αυτών συστημάτων θα πραγματοποιηθεί στην συνέχεια αυτής της μεταπτυχιακής διατριβής.

Με βάση όλα τα παραπάνω γίνεται κατανοητό ότι με τη χρήση της τεχνολογίας της κρυπτογραφίας, δημιουργούνται οι ψηφιακές υπογραφές. Μπορούμε να πούμε ότι η Κρυπτογραφία είναι η επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων, είναι αυτή που καθιστά τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι και στερεί την πρόσβαση στα δεδομένα αυτά σε τρίτους, εξασφαλίζεται με τον τρόπο αυτό το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Αυτό είναι και η απαίτηση όλων όσων μετέχουν σε όλες τις ηλεκτρονικές συναλλαγές και διαδικασίες, δηλαδή να μπορούν να είναι βέβαιοι ότι η πληροφορία που αποστέλλουν θα φράσει και θα αναγνωστεί μόνο στον παραλήπτη στον οποίο έχει σταλεί και δεν θα έχει πρόσβαση σε αυτήν κανένας άλλος.

Σε αυτό το σημείο κρίνεται σκόπιμο να γίνει μια αναφορά και μικρή παρουσίαση σχετικά με τον τρόπο που λειτουργεί η κρυπτογραφία και τις διαδικασίες που ακολουθούνται σε αυτήν.

[19] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.34-35.
[20] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 84.

3.4.2 Βασικές έννοιες κρυπτογραφίας

- Αρχικό κείμενο (plaintext): Αποτελεί το αρχικό μήνυμα (ονομάζεται απλό μήνυμα) ή τα αρχικά δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Η δημιουργία του κρυπτογραφήματος με τη χρήση αλγόριθμου πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.
- Μυστικό κλειδί (secret key): Αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (ciphertext): Είναι το μετασχηματισμένο μήνυμα που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης, δηλαδή από την κρυπτογράφηση του απλού κειμένου. Το κρυπτογράφημα αυτό εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Πρόκειται για έναν αλγόριθμο που πραγματοποιεί την αντίστροφη διαδικασία, δηλαδή λαμβάνει το κρυπτογράφημα και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο. Με άλλα λόγια είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου.

Εικόνα 4. Κρυπτογράφηση και αποκρυπτογράφηση ψηφιακής υπογραφής

3.4.3 Μορφες Κρυπτογραφιας

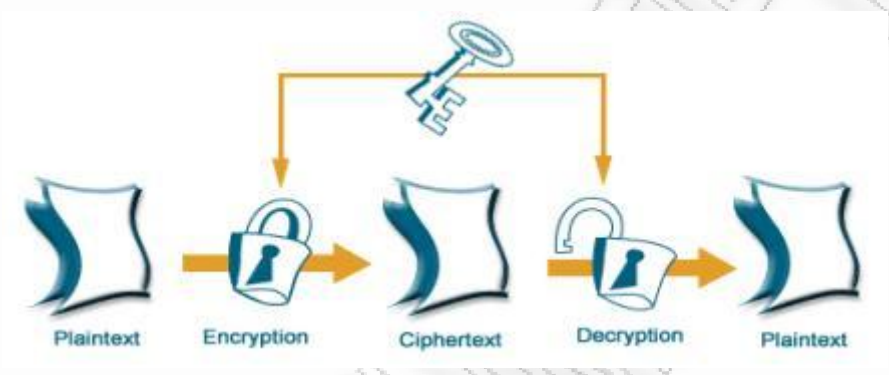
Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρούν την πληροφορία ασφαλή και χρησιμοποιούνται και στην κρυπτογράφηση αλλά και στην αποκρυπτογράφηση. Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης όταν λάβει τα δεδομένα αποκρυπτογραφεί το κείμενο και το μετατρέπει στην μορφή που είχε πριν.

Η κρυπτογράφηση λοιπόν, ενός μηνύματος όπως και η αποκρυπτογράφησή του, απαιτεί την χρήση ενός κλειδιού. Με σημείο αναφοράς το κλειδί διακρίνονται δυο μεγάλες κατηγορίες κρυπτογραφίας:

α) η συμμετρική (symmetric) ή κρυπτογραφία ιδιωτικού κλειδιού (private key cryptography). Τα συμμετρικά συστήματα κρυπτογραφίας, είναι αυτά που χρησιμοποιούν συμμετρικούς αλγόριθμους, όπως είναι για παράδειγμα 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.

Το σύστημα αυτό είναι απλούστερο και ως εκ τούτου φθηνότερο, όμως δεν μπορεί να ανταποκριθεί στις σύγχρονες ανάγκες ασφαλούς διακίνησης ηλεκτρονικών δεδομένων και ηλεκτρονικών εγγράφων μέσα στα πλαίσια του διαδικτύου. Αυτό συμβαίνει γιατί η λειτουργία του προϋποθέτει ότι μαζί με το μεταδιδόμενο κάθε φορά μήνυμα θα πρέπει να αποστέλλεται και το αντίστοιχο κλειδί, έτσι ώστε να καθίσταται δυνατή η αποκρυπτογράφησή του. Η αποστολή ωστόσο του τελευταίου καθιστά ευάλωτη την εν λόγω διαδικασία καθώς, ελλοχεύει ο κίνδυνος της υποκλοπής του. Επίσης, η χρήση του οδηγεί σε μη πρακτικά αποτελέσματα καθώς, συνεπάγεται την παραγωγή διαφορετικών κλειδιών για κάθε συναλλαγή ξεχωριστά, καθιστώντας με αυτόν τον τρόπο δυσχερή την διαχείρισή τους. Για τους λόγους αυτούς προτιμάται συνηθέστερα η χρήση του στα κλειστά δίκτυα[21].



Εικόνα 5. Ένα κλειδί για κρυπτογράφηση και αποκρυπτογράφηση - Συμμετρική Κρυπτογραφία

β) η ασύμμετρη (asymmetric) ή κρυπτογραφία δημόσιου κλειδιού (public key cryptography) ή υποδομή δημόσιου κλειδιού (public key infrastructure). Τα συστήματα που χρησιμοποιούν ασύμμετρους αλγόριθμους 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).

[21] Θεόδωρος Σιδηρόπουλος, ο.π., σελ. 84.

Εικόνα 6. Ιδιωτικό και δημόσιο κλειδί

Το σύστημα της ασύμμετρης κρυπτογραφίας αναγνωρίζεται διεθνώς ως το πλέον ασφαλές και πρακτικό σύστημα διασφάλισης της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των ηλεκτρονικών εγγράφων. Αυτό συμβαίνει γιατί εκτός από την κρυπτογραφία των κειμένων, μπορεί να χρησιμοποιηθεί και για την πιστοποίηση της ταυτότητας του εκδότη τους και της ακεραιότητας του περιεχόμενου του. Έτσι εάν ο αποστολέας κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη, αποστέλλοντας όμως ταυτόχρονα ως συνημμένο περίληψη (σύντμηση) του ίδιου εγγράφου κωδικοποιημένου με το δικό του ιδιωτικό κλειδί πετυχαίνει δυο πράγματα. Πρώτον, εξασφαλίζει ότι το μήνυμα του θα φθάσει στον προορισμό του χωρίς τον κίνδυνο της υποκλοπής του από κάποιον τρίτο καθώς, η αποκρυπτογράφηση του είναι δυνατή μόνο βάσει του ιδιωτικού κλειδιού του παραλήπτη. Δεύτερον, πιστοποιεί ότι ο ίδιος είναι ο εκδότης του εγγράφου, καθώς η συντετμημένη μορφή του εγγράφου, που κωδικοποίησε με το ιδιωτικό κλειδί, μπορεί να διαβαστεί από οποιονδήποτε τρίτο δια της εφαρμογής του δημόσιου κλειδιού. Προκειμένου μάλιστα να εξασφαλιστεί ότι το εκάστοτε ιδιωτικό κλειδί χρησιμοποιείται από το πραγματικό δικαιούχο του, μπορούν να υιοθετηθούν και πρόσθετα μέτρα ασφάλειας, που αφορούν κυρίως στην χρήση τεχνικών μεθόδων αναγνώρισης της ταυτότητας του μέσω μυστικών κωδικών αριθμών (PIN) ή βιομετρικών συσκευών αναγνώρισης των δακτυλικών αποτυπωμάτων ή της ίριδας των ματιών του[22].

Η ασύμμετρη κρυπτογραφία είναι πιο πρόσφορη για την αποστολή εκτενών μηνυμάτων είναι η διαδικασία 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 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.

[22] Θεόδωρος Σιδηρόπουλος, ο.π., σελ. 84-85.

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.

Πιο αναλυτική παρουσίαση των δύο κατηγοριών κρυπτογραφίας γίνεται στην συνέχεια.

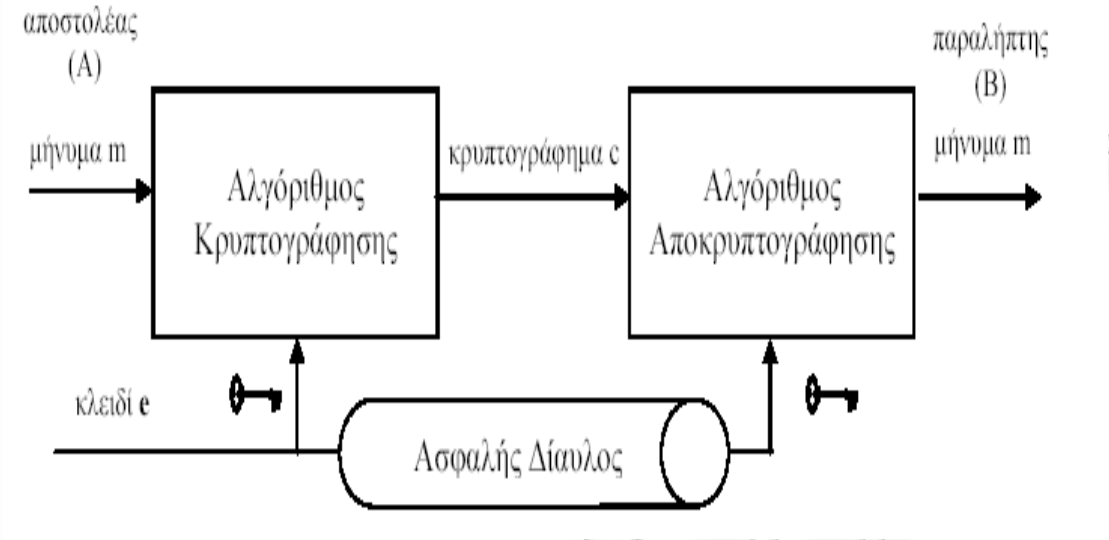
Α) Συμμετρικη Κρυπτογραφια

Αρχικά και έως και το 1976, υπήρχε μόνο η συμμετρική κρυπτογραφία. Στην συμμετρική κρυπτογραφία οι δύο χρήστες που επιθυμούν να ανταλλάξουν ένα κρυπτογραφημένο μήνυμα, πρέπει να διαθέτουν και οι δύο εκ των προτέρων το ίδιο μοναδικό κλειδί κρυπτογράφησης και αποκρυπτογράφησης [23] . Το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα (symmetric cryptosystem). Επομένως, και τα δυο συμβαλλόμενα μέρη θα πρέπει να διαθέτουν το ένα και μοναδικό κλειδί για να είναι δυνατή η ανταλλαγή μηνυμάτων[24].

Το σύστημα της συμμετρικής κρυπτογραφίας, χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε για τη μεταφορά τραπεζικών δεδομένων. Στο σύστημα αυτό το κλειδί ήταν γνωστό μόνο στους συναλλασσόμενους, οι οποίοι είναι λίγοι στον αριθμό και γνωστοί μεταξύ τους συνεπώς υπάρχει εκ των προτέρων οι εμπιστοσύνη μεταξύ τους..

Η μόνη δυνατότητα που υπάρχει στη συμμετρική κρυπτογραφία να γνωρίζει ο παραλήπτης του κρυπτογραφημένου μηνύματος το ένα και μοναδικό κλειδί είναι να σταλεί το κλειδί χωριστά και εκ των προτέρων στον παραλήπτη του μηνύματος και αυτό γιατί εάν σταλεί μαζί με το μήνυμα υπάρχει μεγάλος κίνδυνος κλοπής του. Ακόμα και εκ των προτέρων αποστολή του κλειδιού στον παραλήπτη του μηνύματος είναι πολύ επισφαλής και πρέπει να πραγματοποιείται μόνο από κάποιον που εμπιστεύεται απόλυτα και γνωρίζει προσωπικά τον παραλήπτη. Από την άλλη η συμμετρική κρυπτογραφία δεν επιτρέπει στον παραλήπτη του μηνύματος να διαπιστώσει εάν το μήνυμα στάλθηκε πραγματικά από τον επιθυμητό αποστολέα ή από κάποιον άλλο απατεώνα που χρησιμοποιεί παράνομα την ηλεκτρονική ταυτότητα ενός άλλο προσώπου[25].

[23] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.36.
[24] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 108-109.
[25] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.36.



Εικόνα 7. Συμμετρική Κρυπτογραφία

Τα βασικά χαρακτηριστικά της συμμετρικής κρυπτογραφίας είναι τα εξής:

- Χρησιμοποιείται το ίδιο μοναδικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των μηνυμάτων.
- Το κλειδί πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη, δηλαδή να είναι μόνο γνωστό στον αποστολέα και στον παραλήπτη των μηνυμάτων, 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 στο Διαδίκτυο.
- Η συμμετρική κρυπτογραφία έχει ως μοναδικό σκοπό της τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών και είναι κατάλληλη για μετατροπές μεγάλου όγκου δεδομένων επειδή οι υπολογισμοί που απαιτεί εκτελούνται πολύ γρήγορα.
- 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, το οποίο αποτελεί το πιο διαδεδομένο σύστημα υποστήριξης της ασφαλούς μεταφοράς κλειδιών μέσω δημόσιων δικτύων.

Γίνεται άμεσα αντιληπτό από τα πιο πάνω, ότι η συμμετρική κρυπτογραφία είναι αποτελεσματική μόνο στις περιπτώσεις που τα συναλλασσόμενα μέρη είναι λίγα στον αριθμό και υπάρχει εκ των προτέρων αμοιβαία εμπιστοσύνη μεταξύ τους, ενώ αντίθετα είναι εντελώς ακατάλληλη σε μεγάλα τηλεπικοινωνιακά δίκτυα όπως το Διαδίκτυο, όπου οι χρήστες είναι γεωμετρικά απομακρυσμένοι και άγνωστοι μεταξύ τους. Απόρροια αυτού είναι η μέθοδος αυτή να παρουσιάσει πολλά μειονεκτήματα στην εφαρμογή της σε ανοιχτά δίκτυα με πολλούς

χρήστες όπου οι απαιτήσεις είναι μεγαλύτερες και αυξάνονται συνεχώς, γιατί δεν μπορεί να ανταποκριθεί στις ποικίλες ανάγκες τους, διότι ενέχει κινδύνους για την ασφάλεια και την προστασία των συναλλασσόμενων μερών[26]. Επίσης, η συμμετρική κρυπτογραφία προσφέρει πολύ γρήγορους σε εκτέλεση αλγορίθμους. Έτσι είναι σε θέση να εγγυηθεί την εμπιστευτικότητα των επικοινωνιών, χωρίς να επιβαρύνει τη διαθεσιμότητα των συστημάτων.

Θα μπορούσαμε να πούμε ότι τα βασικά μειονεκτήματα της συμμετρικής κρυπτογραφίας που καθιστούν ακατάλληλη την χρήση της στο Διαδίκτυο είναι τα εξής: **α)** Το βασικό πρόβλημα είναι αυτό της διανομής και της διαχείρισης γενικότερα των απαιτούμενων κλειδιών (key distribution - management). Σε μια επικοινωνία δυο μερών τα συναλλασσόμενα μέρη πρέπει, πριν αρχίσουν τις διαδικασίες αποστολής και λήψης μηνυμάτων, να χρησιμοποιήσουν ένα ασφαλές κανάλι για τον προσδιορισμό του κλειδιού που θα χρησιμοποιήσουν. Στα μεγάλα δίκτυα, ο αριθμός των διακινούμενων κλειδιών αυξάνεται γεωμετρικά λόγω του πλήθους των χρηστών (σε δίκτυο t πλήθους χρηστών, t(t-1) / 2 ζεύγη χρηστών σχηματίζονται), αλλά και επειδή τα κλειδιά πρέπει να αλλάζουν συχνά προκειμένου να διατηρηθεί ένα υψηλό επίπεδο ασφάλειας. Πολλές φορές η διάρκεια ισχύος των κλειδιών περιορίζεται στο διάστημα μιας συνεδρίας επικοινωνίας (communication session). Τα συστήματα ασφαλούς ανταλλαγής κλειδιών, όπως το προαναφερθέν Kerberos, δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλης κλίμακας χρηστών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως είναι η αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή διανομέα - εξυπηρετητή. **β)** Η αναγκαιότητα που υπάρχει για γνώση από τα συμβαλλόμενα μέρη του κλειδιού κρυπτογράφησης και αποκρυπτογράφησης πριν από την συναλλαγή, οδηγεί σε χρονική καθυστέρηση που ακυρώνει εκ των πραγμάτων ένα από τα μεγαλύτερα πλεονεκτήματα που έχουν οι ηλεκτρονικές συναλλαγές, δηλαδή την ταχύτητα διεξαγωγής τους. **γ)** Εκτός από την εμπιστευτικότητα των μηνυμάτων, υπάρχουν και άλλες απαιτήσεις ασφάλειας (ακεραιότητα, αυθεντικότητα, μη - αποποίηση ευθύνης) στα ανοικτά και μεγάλης κλίμακας δίκτυα, όπως το Διαδίκτυο, για τις οποίες η συμμετρική κρυπτογραφία δεν προσφέρει λύσεις. **δ)** Η κάθε δημόσια υπηρεσία, οργανισμός, εταιρία ή συναλλασσόμενος ιδιώτης θα πρέπει να κατέχει και από ένα διαφορετικό κλειδί κρυπτογράφησης και αποκρυπτογράφησης για κάθε δημόσια υπηρεσία, οργανισμό, εταιρία ή ιδιώτη με τον οποίο θα συναλλασσόταν. Κάτι τέτοιο είναι εξαιρετικά δαπανηρό και ανεφάρμοστο. **ε)** Τέλος, δεν παρέχει δυνατότητα χρήσης ψηφιακής υπογραφής . Στα ζητήματα αυτά, η σχετικά πρόσφατη ανεπτυγμένη κρυπτογραφία δημόσιου κλειδιού προσφέρει ικανοποιητικές διεξόδους.

Στο σημείο κρίνεται σκόπιμο να αναφέρουμε επιγραμματικά τους αλγόριθμους της συμμετρικής κρυπτογραφίας Οι αλγόριθμοι αυτοί είναι:

- **DES (Data Encryption Standard):** Αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1, που επίσης περιγράφει τον Data Encryption Algorithm (DEA). Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το National Institute of Standards and Technology (NIST). Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος. Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.
- **Triple-DES:** Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου.
- **DESX:** Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης.

[26] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ.109.

- **AES (Advanced Encryption Standard):** Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES.
- **DSS (Digital Signature Algorithm):** Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή.
- **RC2, RC4, RC5**
- **IDEA (International Data Encryption Algorithm):** Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να εύκολα εφαρμόσιμος τόσο hardware σε όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.
- **Blowfish:** είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

Β) Ασυμμετρη Κρυπτογραφια

Το 1976 παρουσιάζεται για πρώτη φορά η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού. Η ουσιαστική διαφορά της ασύμμετρης κρυπτογραφίας από την συμμετρική είναι ότι στην ασύμμετρη δεν είναι απαραίτητη η εκ των προτέρων διανομή του κλειδιού και αυτό γιατί κάθε συναλλασσόμενος έχει πλέον το δικό του ζεύγος κλειδιών, δηλαδή το ιδιωτικό κλειδί (private key) κα, το οποίο είναι μυστικό και το γνωρίζει μόνο ο ιδιοκτήτης του και το δημόσιο κλειδί (public key) το οποίο είναι ελεύθερα προσβάσιμο σε όλους όσους συναλλάσσονται με τον ιδιοκτήτη του ιδιωτικού κλειδιού[27].

Η τεχνολογία της «ασύμμετρης κρυπτογράφησης», βάσει συγκεκριμένων «μαθηματικών αλγορίθμων» (π.χ. RSA, DSA, κ.ά.), παράγει τυχαία ζεύγη κρυπτογραφικών «κλειδιών» (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από δύο σημαντικές ιδιότητες:

1) το καθένα ιδιωτικό κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το αντίστοιχο δημόσιο (συμπληρωματικό του) κλειδί και αντίστροφα, και
2) δεν είναι δυνατόν (με τις παρούσες δυνατότητες της τεχνολογίας) να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο, δηλαδή το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

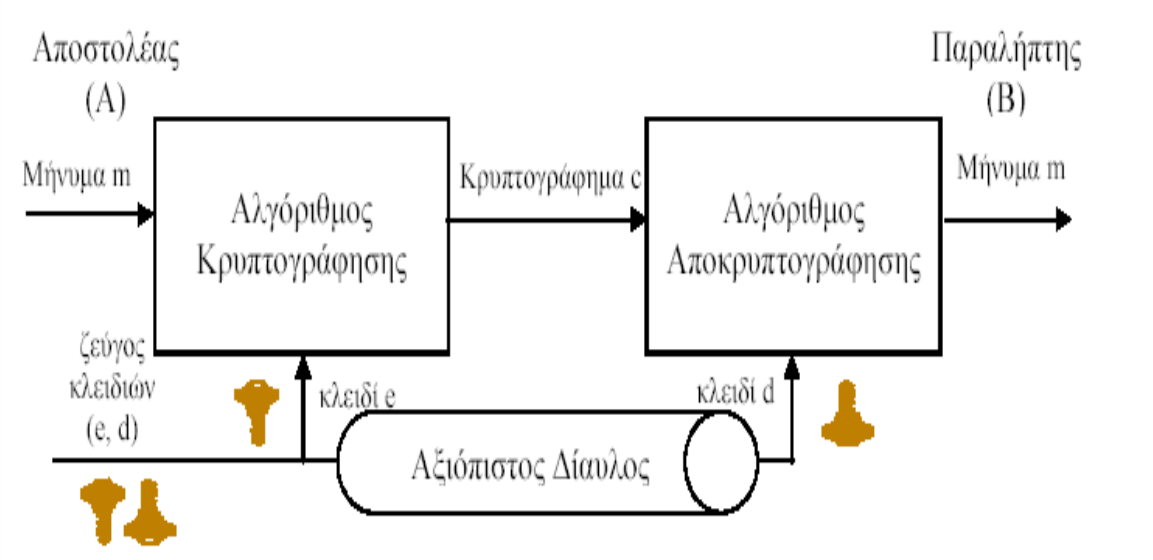
Τα συστήματα δημοσίου κλειδιού ή ασύμμετρης κρυπτογραφίας χρησιμοποιούν δύο ξεχωριστά αλλά συμπληρωματικά κλειδιά για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Το ένα από αυτά διατηρείται απόρρητο και καλείται ιδιωτικό (private) κλειδί, ενώ το άλλο γίνεται γνωστό στο κάθε ενδιαφερόμενο και καλείται δημόσιο (public). Παρόλο που τα δύο κλειδιά έχουν μια σύνθετη μαθηματική σχέση μεταξύ τους, η γνώση του δημόσιου κλειδιού δεν καθιστά εφικτό τον υπολογισμό του μυστικού ιδιωτικού κλειδιού. Η προστασία της εμπιστευτικότητας των μηνυμάτων επιτυγχάνεται ως εξής : Το αρχικό μήνυμα

[27] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.37-38.

κρυπτογραφείται από τον αποστολέα με το δημόσιο κλειδί του παραλήπτη και μόνο ο κάτοχος του ιδιωτικού κλειδιού, δηλαδή ο ίδιος ο παραλήπτης, μπορεί να το αποκρυπτογραφήσει.

Με τη χρήση της τεχνολογίας της ασύμμετρης κρυπτογραφίας, διατηρώντας μυστικό το ένα κλειδί ως «ιδιωτικό» («δεδομένα δημιουργίας υπογραφής») και διανέμοντας ελεύθερα το άλλο κλειδί ως «δημόσιο» («δεδομένα επαλήθευσης υπογραφής»), εξασφαλίζουμε ότι όλοι όσοι γνωρίζουν το «δημόσιο κλειδί» μπορούν να «επαληθεύσουν» μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου «ιδιωτικού κλειδιού». Η βασική θεωρητική ιδέα πίσω από την ασύμμετρη κρυπτογραφία είναι η έννοια των «μονόδρομων συναρτήσεων με καταπακτή» (trapdoor one-way functions). Οι συναρτήσεις αυτές είναι ειδικές περιπτώσεις των μονόδρομων συναρτήσεων που ήδη αναφέρθηκαν. Η επιπλέον ιδιότητα που τις κάνει διακριτές, είναι ότι όταν χρησιμοποιηθεί μια επιπλέον πληροφορία (η αποκαλούμενη καταπακτή), γίνεται εφικτός ο υπολογισμός της αντιστρόφου της.

Ο κάθε αλγόριθμος δημοσίου κλειδιού έχει τις δικές του ιδιαιτερότητες, όλοι όμως χρησιμοποιούν ζεύγος κλειδιών και βασίζονται στο ότι όποιο από τα κλειδιά δημοσιευθεί, δεν διακυβεύει τη μυστικότητα του άλλου κλειδιού. Οι χρήστες λοιπόν του Διαδικτύου μπορούν ελεύθερα να συμπεριλαμβάνουν στις ιστοσελίδες τους ή σε ειδικούς καταλόγους - ευρετήρια (directories), τα δημόσια κλειδιά τους, οπότε και παύει να υφίσταται το βασικό πρόβλημα διαχείρισης των κλειδιών της κρυπτογραφίας μυστικού κλειδιού. Τα δημόσια κλειδιά δεν χρειάζονται για τη διανομή τους έναν ασφαλή δίαυλο. Δεν τίθεται ζήτημα εμπιστευτικότητας στα κανάλια διανομής των δημόσιων κλειδιών, αφού αυτά είναι προσπελάσιμα και ανοικτά προς όλους τους ενδιαφερόμενους. Όμως, χρειάζονται για την διανομή τους έναν αξιόπιστο δίαυλο, δηλαδή ένα μέσο που θα υποστηρίζει την ακεραιότητά τους. Οι μικρότερες απαιτήσεις ασφάλειας για τη διανομή των κλειδιών της, κάνουν τη κρυπτογραφία δημόσιου κλειδιού ιδανική για ένα εκ φύσεως δημόσιο δίκτυο, το Διαδίκτυο, στο οποίο πολλές φορές χρειάζεται να αποκαθίσταται η εμπιστοσύνη ανάμεσα σε δυο απομακρυσμένους χρήστες χωρίς αυτοί να συναντηθούν ή χωρίς να μεσολαβήσει κάποιο έμπιστο τρίτο μέρος.



Εικόνα 8. Ασύμμετρη Κρυπτογραφία

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 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.

Με βάση την ελληνική νομοθεσία, ορίζετε ότι τα ιδιωτικά κλειδιά είναι: «δεδομένα δημιουργίας υπογραφής, τα οποία είναι μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον γράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής»[28]. Σε ότι αφορά τα δημόσια κλειδιά ορίζετε ότι είναι: «δεδομένα επαλήθευσης υπογραφής, τα οποία είναι δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής»[29]. Καθένα από τα δυο αυτά κλειδιά είναι ένας αλγόριθμος, δηλαδή ένας αριθμός που προκύπτει μετά από μια σειρά μαθηματικών πράξεων, ο αριθμός αυτός όσο πιο μεγάλος είναι δηλαδή όσο πιο πολλά ψηφία έχει τόσο πιο ισχυρή είναι η κρυπτογράφηση που παρέχει[30].

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά. Τα δύο κλειδιά λειτουργούν πάντα ως ζεύγος, ότι κρυπτογραφεί το ένα αποκρυπτογραφείται μόνο από το άλλο και αντιστρόφως. Το δημόσιο κλειδί δημοσιοποιείται, ενώ αντίθετα το ιδιωτικό κλειδί είναι μυστικό και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Το ιδιωτικό κλειδί (private key) λοιπόν, που χρησιμοποιείται για την κρυπτογράφηση του ηλεκτρονικού μηνύματος και είναι απόρρητο, το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο μήνυμα. Γίνεται αντιληπτό ότι με την χρήση των δύο κλειδιών παύει να υφίσταται η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί.

Στην συνέχεια προκειμένου να γίνει η αποκρυπτογράφηση του μηνύματος, δεν μπορεί να γίνει από το ιδιωτικό κλειδί αλλά, από το αντίστοιχο δημόσιο κλειδί. Το δημόσιο κλειδί (public key) από την άλλη, αντιστοιχεί πάντα στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο, γνωστοποιεί σε κάθε συναλλασσόμενο του, για να μπορεί να

[28] Άρθρο 2 αριθ. 4 του π.δ. 150/2001
[29] Άρθρο 2 αριθ. 7 του π.δ. 150/2001
[30] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.38.

αποκρυπτογραφεί/διαβάζει τα μηνύματα του πρώτου. Μόνο με το δημόσιο κλειδί μπορεί λοιπόν ο παραλήπτης να διαβάσει τις πληροφορίες. Αντίστροφα, εάν ένα ηλεκτρονικό μήνυμα κρυπτογραφηθεί με το δημόσιο κλειδί, τότε μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστοσύνη και η επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. 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.

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. 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 αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Εδώ θα πρέπει να πούμε ότι είναι πρακτικά αδύνατο από το ένα κλειδί να παραχθεί το άλλο. Αυτή η αλληλεξάρτηση των κλειδιών στηρίζεται στις μαθηματικές ιδιότητες των πρώτων αριθμών, δηλαδή αυτών που μόνο όταν διαιρούνται με τον εαυτό τους και με τον αριθμό ένα, δίνουν πηλίκο έναν ακέραιο αριθμό. Όταν οι πρώτοι αριθμοί πολλαπλασιάζονται μεταξύ τους δημιουργούν έναν τρίτο αριθμό, ο οποίος μόνο όταν διαιρείται με τους αρχικούς πρώτους αριθμούς και με τον αριθμό ένα, δίνει πηλίκο ακέραιο αριθμό. Η μαθηματική δυσκολία της εύρεσης των δυο αρχικών πρώτων αριθμών, όταν μόνο το γινόμενο αυτών των αριθμών είναι γνωστό, είναι η μαθηματική βάση της σύγχρονης ασύμμετρης κρυπτογραφίας[31].

Μπορούμε να πούμε ότι το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένη με το αντίστοιχο δημόσιο κλειδί. Ο τρίτος αριθμός που προκύπτει από τον πολλαπλασιασμό είναι το δημόσιο κλειδί, ενώ οι δυο αριθμοί που πολλαπλασιάζονται μεταξύ τους και δημιουργούν τον τρίτο αριθμό είναι το ιδιωτικό κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο σύστημα κρυπτογραφίας ανακτώντας το ιδιωτικό κλειδί από το δημόσιο. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Το σύστημα που αναφέραμε με το δημόσιο και το ιδιωτικό κλειδί προσφέρει όλες τις απαραίτητες ιδιότητες μιας ασφαλούς ηλεκτρονικής συναλλαγής, δηλαδή προσφέρει την αυθεντικότητα, την ακεραιότητα, την εμπιστευτικότητα και τη μη αποποίηση ευθύνης.

Η ασύμμετρη κρυπτογράφηση παρέχει πολύ μεγαλύτερη ασφάλεια από ότι η συμμετρική και αυτό γιατί δεν υπάρχει η δυνατότητα παραγωγής του κλειδιού της αποκρυπτογράφησης γνωρίζοντας μόνο το κλειδί κρυπτογράφησης. Γίνεται λοιπόν αντιληπτό ότι αυτό το σύστημα κρυπτογράφησης παρέχει μεγάλη εμπιστευτικότητα και αυξημένη ασφάλεια στις ηλεκτρονικές συναλλαγές[32]. Το πλεονέκτημα της ασύμμετρης κρυπτογραφίας έναντι της συμμετρικής φαίνεται 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. Συνεπώς, η ασύμμετρη κρυπτογραφία είναι καταλληλότερη σε ένα «ανοικτό» συναλλακτικό περιβάλλον με πολλούς και άγνωστους μεταξύ τους συναλλασσομένους. Αντίθετα η συμμετρική κρυπτογραφία είναι κατάλληλη όταν οι συναλλασσόμενοι γνωρίζονται προσωπικά και υπάρχει μεταξύ τους εμπιστοσύνη.

Άλλο ένα ακόμα πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι μπορεί να παρέχει ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο

[31] Καραδημητρίου, ο.π., σελ.39-40.
[32] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ.109.

αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Έκτος όμως από τα πιο πάνω πλεονεκτήματα η ασύμμετρη κρυπτογραφία έχει και μειονέκτημα. Ένα από τα βασικά μειονεκτήματα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα και αυτό γιατί οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής *(non-repudiation)*. Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς *(Certificate Authority)* ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη. Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στην περίπτωση που η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Πάρα πολλές είναι οι εφαρμογές και οι μηχανισμοί ασφαλείας στο Διαδίκτυο που κάνουν ευρεία χρήση της ασύμμετρης κρυπτογραφίας, μερικές από αυτές παρουσιάζονται πιο κάτω:

- Υποδομές Πιστοποίησης, οι οποίες διαχειρίζονται ψηφιακά πιστοποιητικά έμπιστων τρίτων φορέων, με σκοπό την αναγνώριση και πιστοποίηση της ταυτότητας των χρηστών (πιστοποιητικά ταυτότητας), αλλά και τον έλεγχο των εξουσιοδοτήσεών τους (πιστοποιητικά χαρακτηριστικών).
- Ασφαλής παρουσίαση ιστοσελίδων αλλά και δικτυακών αγορών, βάσει του πρωτοκόλλου SSL (Secure Sockets Layer) της Netscape αλλά και του πρωτοκόλλου TLS (Transport Layer Security) της IETF (Internet Engineering Task Force).
- Ασφαλείς συναλλαγές μέσω πιστωτικών καρτών, βάσει του πρωτοκόλλου SET (Secure Electronic Transactions) των VISA και Mastercard.
- Ασφαλής ηλεκτρονική αλληλογραφία, βάσει του πρωτοκόλλου S/MIME (Secure/multipurpose Internet mail extensions) της ΙΕΤΦ.

Στο σημείο κρίνεται σκόπιμο να αναφέρουμε τον πιο βασικό αλγόριθμο της ασύμμετρης κρυπτογραφίας. Ο αλγόριθμος αυτός είναι ο RSA. Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς *p,q* και υπολογίζουμε το γινόμενο τους *n = pq*. Το *n* καλείται *modulus*. Διαλέγουμε έναν αριθμό *e* μικρότερο του *n* και τέτοιο, ώστε *e* και *(p-1)(q-1)* να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό *d*, ώστε *(ed-1)* να διαιρείται από το *(p-1)(q-1)*. Τα ζευγάρια *(n,e)* και *(n,d)* καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα. Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα *d* από την δημόσια κλείδα *e*. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού *n*, δηλαδή των αριθμών *p* και *q*. Ο *n* είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς των κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

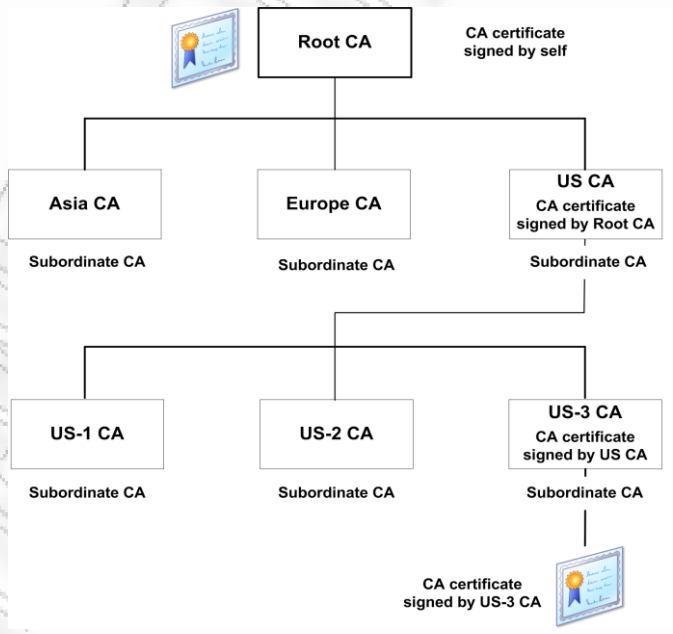
Ενδεικτικά παρουσιάζουμε ένα παράδειγμα κρυπτογράφησης με το RSA. Έστω ο χρήστης Α που θέλει να στείλει κρυπτογραφημένο στον χρήστη Β ένα έγγραφο. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = me \bmod n$, όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = cd \bmod n$, όπου (n,d) η ιδιωτική κλείδα του Β. Η μαθηματική σχέση που το e και το d εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το d, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

3.5 Η Τριμερής Ασύμμετρη Κρυπτογραφία

3.5.1 Ηλεκτρονική υπογραφή και Ηλεκτρονικά Πιστοποιητικά

Κατά την πολιτική ασφάλειας ενός συστήματος ηλεκτρονικών συναλλαγών είναι απαραίτητη η εξακρίβωση της ταυτότητας του χρήστη. Τα ηλεκτρονικά πιστοποιητικά είναι αυτή την περίοδο το ωριμότερο εργαλείο ταυτοποίησης των χρηστών ενός συστήματος ηλεκτρονικών συναλλαγών μέσω διαδικτύου[33]. Εάν θα θέλαμε να ορίσουμε το ηλεκτρονικό πιστοποιητικό, μπορούμε να πούμε ότι ηλεκτρονικό πιστοποιητικό είναι ένα ηλεκτρονικό αντικείμενο που συσχετίζει ένα δημόσιο κλειδί και επιπλέον και το αντίστοιχο ιδιωτικό κλειδί του, με ορισμένες άλλες πληροφορίες, συνήθως οι πληροφορίες αυτές είναι πληροφορίες ταυτότητας του κατόχου του (όπως όνομα, επάγγελμα) ή περιγραφές αδειών και το δημόσιο κλειδί του.

Η διαδικασία έκδοσης ενός ηλεκτρονικού πιστοποιητικού πρέπει να επικυρώνεται από μια εκδίδουσα αρχή πιστοποίησης, ένα ηλεκτρονική πιστοποιητικό λοιπόν, υπογράφεται από κάποια αρχή πιστοποίησης (Certification Authority - CA), η οποία βεβαιώνει την σύνδεση μεταξύ της ταυτότητας ή της άδειας και του ιδιοκτήτη του ιδιωτικού κλειδιού. Στην πιο κάτω εικόνα παρουσιάζονται σχηματικά οι αρχές πιστοποίησης που υπάρχουν σε παγκόσμιο επίπεδο.



Εικόνα 9. Ιεραρχία και δομή των πιστοποιητικών

[33] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, ο.π.., σελ.149.

Το ηλεκτρονικό πιστοποιητικό εκδίδεται από έναν Πάροχο Υπηρεσιών Πιστοποίησης (αρχή ψηφιακής πιστοποίησης) που εγγυάται για τα στοιχεία του κατόχου του, ακριβώς όπως η αρμόδια κρατική αρχή εγγυάται για την έκδοση του διαβατηρίου. Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο Πάροχος δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου. Έτσι έχει υποβάλλει τις εξής τεχνικές προδιαγραφές: Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα και αποτελεί μια ψηφιακή «ετικέτα» η οποία επισυνάπτεται στα προς υπογραφή δεδομένα. Σκοπός 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[34].

Πολύ σημαντικό πλεονέκτημα των ηλεκτρονικών πιστοποιητικών είναι το γεγονός ότι υπάρχει η πιθανότητα να ελεγχθούν χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης. Αυτό ουσιαστικά σημαίνει ότι είναι πολύ πιθανόν να εισαχθεί ένας νέος χρήστης στο σύστημα, χωρίς το ίδιο το σύστημα να ξέρει κάτι για αυτό. Ένα μέρος βέβαια αυτού του πολύ σημαντικού πλεονεκτήματος αναιρείται, από την ανάγκη σε αρκετές περιπτώσεις να γίνει έλεγχος της κατάστασης του ηλεκτρονικού πιστοποιητικού κάθε φορά που γίνεται χρήση αυτού.

Η χρήση των ηλεκτρονικών πιστοποιητικών σήμερα γίνεται κυρίως 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. Επίσης, ελέγχει ότι πρόκειται για συναλλαγή της με την ίδια την οντότητα και όχι κάποιον τρίτο. Σε αυτούς τους ελέγχους είναι πιθανόν να έχουμε σημαντικές συνέπειες από τυχόν σφάλματα.

Χρήση των ηλεκτρονικών πιστοποιητικών έχουμε και στα γνωστά «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. 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 ηλεκτρονικού πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών από έναν ΠΥΠ, περιορίζεται σε συγκεκριμένες επιτρεπόμενες χρήσεις, οι οποίες προσδιορίζονται και από το σχετικό πεδίο «Χρήση Κλειδιού» («Key Usage») των πιστοποιητικών X.509[35] το οποίο δέχεται συγκεκριμένες προκαθορισμένες τιμές. Έχει

[34] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/FAQS/Digital Signatures/ (ημερομηνία επίσκεψης 20/05/2011)

[35] Το X.509 είναι το πιο διαδεδομένο διεθνώς πρότυπο το οποίο σχεδιάστηκε για τη σύνταξη ενός ψηφιακού πιστοποιητικού και να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP). Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol). Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO και το ότι αποτελεί Σύσταση τη Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών. Η έκδοση ενός πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών, περιορίζεται σε συγκεκριμένες επιτρεπόμενες χρήσεις, οι οποίες προσδιορίζονται και από το σχετικό πεδίο subject unique identifier 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

επικρατήσει, 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 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, 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 στο πιστοποιητικό τους[36].

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 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 ΠΥΠ και η οποία συμπεριλαμβάνει όλους τους ειδικότερους όρους έκδοσης και χρήσης που καθορίζει ο ΠΥΠ 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 ομώνυμο πεδίο των πιστοποιητικών X.509, ενημερώνοντας τόσο το υποκείμενο πιστοποίησης, όσο και κάθε τρίτο αποδέκτη των πιστοποιητικών του για την εφαρμοζόμενη «Πολιτική Πιστοποιητικού»[37].

Ένας φορέας πιστοποίησης θα πρέπει να είναι σε θέση να διασφαλίζει ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε ένα συγκεκριμένο άτομο, οργανισμό ή οντότητα και πουθενά αλλού. Η διαδικασία αυτή της αντιστοίχισης και δέσμευσης ενός δημόσιου κλειδιού σε μια οντότητα, καλείται πιστοποίηση (certification). Κατ' αναλογία, καλούνται πιστοποιητικά δημόσιου κλειδιού (public key certificates) ή απλά πιστοποιητικά, τα ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση μιας οντότητας και τη συσχέτισή της με ένα δημόσιου κλειδί. Μια Υποδομή Δημόσιου Κλειδιού, στην απλούστερή της μορφή, είναι ένα τέτοιο σύστημα δημοσιοποίησης δημόσιων κλειδιών, το οποίο ως βασική του λειτουργία έχει τη πιστοποίηση όσων επικοινωνούν μέσω Διαδικτύου. 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 online επικοινωνίας, μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου από το υποκείμενο του πιστοποιητικού. Επίσης, πέρα από τα πιστοποιητικά για φυσικά πρόσωπα, μια άλλη κατηγορία πιστοποιητικών είναι εκείνη που εκδίδεται με «υποκείμενο» τηλεπικοινωνιακά ή πληροφοριακά συστήματα και συσκευές. Χαρακτηριστική εφαρμογή αυτής της κατηγορίας πιστοποιητικών είναι η «πιστοποίηση προέλευσης ιστοσελίδων», όπου πιστοποιείται η νομική εξυπηρέτηση μιας διαδικτυακής διεύθυνσης από έναν συγκεκριμένο διακομιστή δικτύου (web server)[38].

χρησιμοποιεί αποκλειστικά για τη δημιουργία αναγνωρισμένων υπογραφών με έννομες συνέπειες σε ηλεκτρονικά έγγραφα (με την ένδειξη μη αποκήρυξη – 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 – 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-Key/Data Encipherment), αν και συνίσταται η χρήση τρίτου ξεχωριστού ζεύγους κλειδιών και αντίστοιχου πιστοποιητικού για τις εφαρμογές κρυπτογράφησης.

[36] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 7 - 8, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[37] ο.π.

[38] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008 σελ. 56.

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 «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 «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: α) σε «υπογραφές ταυτοποίησης» των συσκευών αυτών (π.χ. server authentication) και β) 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», που χρησιμοποιούνται για την επίτευξη ασφαλούς και εμπιστευτικής επικοινωνίας τύπου SSL ή TSL[39].

Μια διαφορετική κατηγορία ηλεκτρονικών πιστοποιητικών, αποτελούν τα «πιστοποιητικά χρονοσήμανσης» (time stamping certificates). Η χρονοσήμανση (time stamping) των ηλεκτρονικών μηνυμάτων είναι η υπηρεσία με την οποία ο ΠΥΠ θέτει στο έγγραφο ηλεκτρονική σφραγίδα η οποία είναι αδύνατο να αλλοιωθεί και φανερώνει με ακρίβεια την ημερομηνία και την ώρα αποστολής και λήψης ενός ηλεκτρονικά υπογεγραμμένου έγγραφο στο πλαίσιο μιας συναλλαγής. Η χρήση των ηλεκτρονικών υπογραφών και η ασφάλεια που αυτές παρέχουν στις συναλλαγές έχει ως βάση της το γεγονός ότι ο υπογράφον δεν έχει την δυνατότητα να αποποιηθεί την ευθύνη του και να αρνηθεί εκ των υστέρων ότι υπέγραψε[40]. Τα πιστοποιητικά χρονοσήμανσης, εκδίδονται adhoc σε συγκεκριμένα ηλεκτρονικά έγγραφα, μετά από αίτημα του υπογράφοντα ή/και του αποδέκτη τους. Στα περιεχόμενά τους, εκτός των στοιχείων του εκδότη τους, 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[41].

Στην συνέχεια του κεφαλαίου αυτού θα μιλήσουμε πιο αναλυτικά για τους Παρόχους Υπηρεσιών Πιστοποίησης (ΠΥΠ) και την νομική τους ευθύνη και την πιστοποίηση των ψηφιακών υπογραφών.

[39] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 8, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[40] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.46.

[41] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 9, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

3.5.2 Πάροχος Υπηρεσιών Πιστοποίησης και Νομική Ευθύνη

Όπως έχουμε αναφέρει έως τώρα και πιο πάνω, με την λήψη ενός ηλεκτρονικού μηνύματος το οποίο φέρει ηλεκτρονική υπογραφή, ο παραλήπτης έχει την δυνατότητα, επαληθεύοντας την ηλεκτρονική υπογραφή να βεβαιώνεται ότι το ηλεκτρονικό μήνυμα είναι ακέραιο και αμετάβλητο. Στο σημείο αυτό όμως υπάρχει και ένας περιορισμός, δηλαδή ο παραλήπτης, πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι και όχι κάποιος κακόβουλος τρίτος. 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. Όπως γίνεται αντιληπτό 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. Υπάρχει με άλλα λόγια η απαίτηση για την ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι ο «οργανισμός» που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του, όπως και πιο πάνω αναφέραμε. 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[42].

Γίνεται αντιληπτό ότι με την ύπαρξη της τεχνολογίας της ασύμμετρης κρυπτογραφίας, ο κίνδυνος πλαστογράφησης εκ μέρους του αποστολέα ή του παραλήπτη ενός ηλεκτρονικού μηνύματος δεν εξαλείφεται πλήρως. Η χρήση της ασύμμετρης κρυπτογραφίας οδηγεί στην ανάγκη ύπαρξης ενός μηχανισμού, ο οποίο θα εγγυάται και θα πιστοποιεί ανά πάσα στιγμή στο συναλλασσόμενο ότι το δημόσιο κλειδί που χρησιμοποιεί για να αποκρυπτογραφήσει ένα ηλεκτρονικό υπογεγραμμένο αρχείο ανήκει πραγματικά στον αντισυμβαλλόμενο του και επομένως ότι η ηλεκτρονική υπογραφή που χρησιμοποιεί ο αντισυμβαλλόμενος ανήκει πράγματι σε αυτόν. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από έναν έμπιστο τρίτο, τον οποίο τα συναλλασσόμενα μέρη γνωρίζουν εκ των προτέρων. Ο τρίτος αυτό ονομάζεται «Πάροχος Υπηρεσιών Πιστοποιητικών» (ΠΥΠ). Ο ΠΥΠ είναι «φυσικό ή νομικό πρόσωπο ή άλλος φορέας που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές»[43]. Η έκδοση πιστοποιητικών γνησιότητας, με τα οποία πιστοποιείται η μοναδική σχέση μεταξύ του δημόσιου κλειδιού και του νόμιμου ιδιοκτήτη του, είναι ιδιαίτερα σημαντική λειτουργία του ΠΥΠ, χωρίς αυτή την λειτουργία, ο οποιοσδήποτε θα ήταν σε θέση να δημιουργήσει ένα ζευγάρι δημόσιου – ιδιωτικού κλειδιού στο όνομα κάποιου άλλου προσώπου και με τον τρόπο αυτό να εξαπατήσει όλους όσους θα συναλλάσσονται μαζί του μέσω του Διαδικτύου[44].

Μια Υποδομή Δημοσίου Κλειδιού περιλαμβάνει έναν ή περισσότερους Παρόχους Υπηρεσιών Πιστοποίησης (ΠΥΠ). Οι Πάροχοι Υπηρεσιών Πιστοποίησης (Certification Service Providers - CSP) παλαιότερα αποκαλούνταν Έμπιστες Τρίτες Οντότητες (Trusted Third Parties – TTP), αλλά σήμερα αναφέρονται ως ΠΥΠ αφού εκδίδουν, υπογράφουν, δημοσιεύουν και υποστηρίζουν τυποποιημένες ηλεκτρονικές βεβαιώσεις (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών τους. Οι ΠΥΠ παρέχουν τεχνική αλλά και νομική υποστήριξη για θέματα που σχετίζονται με την παραγωγή και διανομή των απαιτούμενων διακριτικών διασφάλισης και επαλήθευσης μιας ηλεκτρονικής δοσοληψίας. Το βασικό έργο των ΠΥΠ είναι η άρτια οργάνωση των μηχανισμών διαχείρισης πιστοποιητικών. Οι ΠΥΠ είναι οντότητες-φορείς που πρωταρχικό σκοπό έχουν να πιστοποιούν τεχνικά και νομικά την αντιστοίχηση της ταυτότητας μιας οντότητας με ένα δημόσιο κλειδί το οποίο περιέχεται σε ένα πιστοποιητικό. Ουσιαστικά οι ΠΥΠ δραστηριοποιούνται για την παραγωγή, αποθήκευση, αποστολή και ανάκληση πιστοποιητικών για την υποβοήθηση στην επίτευξη ασφαλών ηλεκτρονικών επικοινωνιών. Ουσιαστικά μια Αρχή Πιστοποίησης λειτουργεί στα πλαίσια ενός ΠΥΠ.

---

[42] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/ IntroEsign (ημερομηνία επίσκεψης 20/05/2011)

[43] Σύμφωνα με το άρθρο 2 αριθ. 11 του π.δ. 150/2001

[44] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.43-44.

Οι βασικές υπηρεσίες που προσφέρει υποχρεωτικά ένας Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ), μπορούν να διακριθούν σε οργανωμένες ξεχωριστές λειτουργικές οντότητες και συγκεκριμένα είναι οι εξής[45]:

- **Υπηρεσία Εγγραφής-Καταχώρησης** (Registration Authority – RA), η οποία ελέγχει τη ταυτότητα των υποκειμένων και συλλέγει τα σχετικά αποδεικτικά στοιχεία - πιθανώς συνεπικουρούμενη από εξουσιοδοτημένες Τοπικές Υπηρεσίες Υποβολής (Local Registration Authorities – LRA) - πριν να δώσει την έγκρισή της για την έκδοση των σχετικών πιστοποιητικών. Η Αρχή Έγγραφής, ουσιαστικά παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ ενός χρήστη και του ΠΥΠ. Είναι το τμήμα του οργανισμού που είναι υπεύθυνο για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ταυτότητας ή του ρόλου ενός χρήστη ή μιας οντότητας όπως μιας εφαρμογής ή ενός εξυπηρετητή. Η RA προωθεί προς τη CA τις έγκυρες υποβληθείσες προς αυτήν αιτήσεις για τη δημιουργία των αντίστοιχων πιστοποιητικών.
- **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. Η Αρχή Πιστοποίησης αποτελεί ένα έμπιστο τμήμα του οργανισμού ΠΥΠ και η λειτουργία της είναι η έκδοση και υπογραφή των τελικών πιστοποιητικών των υποκειμένων. Η ακεραιότητα λειτουργίας του ΠΥΠ συγκεντρώνεται στην Αρχή Πιστοποίησης. Πιο αναλυτικά θα μπορούσαμε να πούμε ότι, μία αρχή πιστοποίησης (certification authority ή CA) είναι υπεύθυνη για την υπογραφή πιστοποιητικών. Προκειμένου 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 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.
- **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 για την κατάλληλη (ψηφιακή) υπογραφή των σχετικών εκδιδόμενων Λιστών Ανακληθέντων Πιστοποιητικών (Certificate Revocation Lists ή CRL),
- **Υπηρεσία Δημοσίευσης** (Dissemination & Revocation Status Service), η οποία αναλαμβάνει την δημοσίευση των κειμένων τεκμηρίωσης των υπηρεσιών του CSP, δηλαδή του Παρόχου Υπηρεσιών Τυποποίησης (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 (δηλαδή 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 (ΠΥΠ) μπορεί επίσης να παρέχει (προαιρετικά) και τις εξής υπηρεσίες[46]:

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

[45] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 11, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[46] ο.π.

- **Υπηρεσίες Χρονοσήμανσης ηλεκτρονικών εγγράφων** (Time-Stamping Authority – TSA),
- **Υπηρεσίες Έκδοσης Πιστοποιητικών Ιδιοτήτων** (Attribute Authority), Υπηρεσίες Ασφαλούς Αρχειοθέτησης εγγράφων (καλούμενες συχνά και ως Notary Services) κ.τ.λ.

Στο περιεχόμενο ενός πιστοποιητικού περιλαμβάνονται:

α) ένας μμοναδικός αριθμός (serial number),

β) η ψηφιακή υπογραφή της ΑΠ και ο αλγόριθμος (signature algorithm) που χρησιμοποιήθηκε,

γ) το όνομα της ΑΠ, δηλαδή της εκδότριας αρχής (issuer) του πιστοποιητικού,

δ) οι ημερομηνίες έκδοσής του (valid from) και λήξης της ισχύος του (valid to),

ε) το όνομα και πληροφορίες αναγνώρισης του υποκειμένου του πιστοποιητικού (subject),

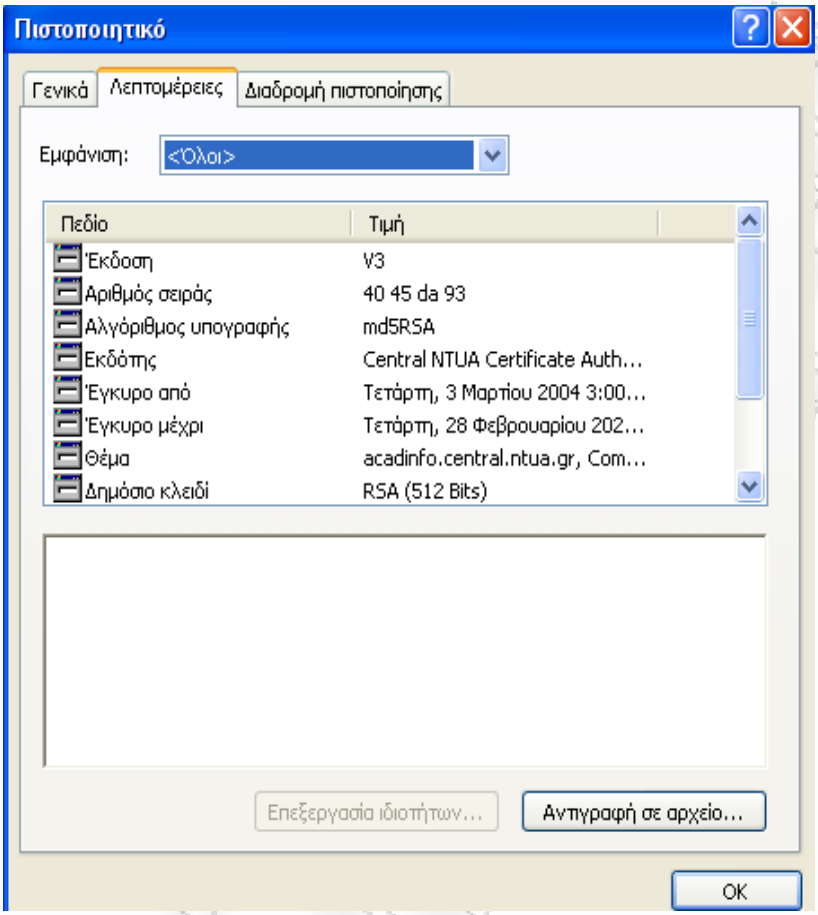
στ) το δημόσιο κλειδί του υποκειμένου, δηλαδή του κατόχου του πιστοποιητικού (public key). Το περιεχόμενο ενός πιστοποιητικού παρουσιάζεται και στην πιο κάτω εικόνα.

Ο ΠΥΠ, επιπλέον, πιστοποιεί προς οποιοδήποτε τρίτο - αποδέκτη μιας ψηφιακής υπογραφής:

- την καταγραφή (registration) της πραγματικής ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο χρησιμοποιούμενο δημόσιο κλειδί, και
- τη σύνδεση του σχετικού ιδιωτικού κλειδιού με τον κάτοχο του πιστοποιητικού (proof of possession).

Η παραπάνω πιστοποίηση, προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής, γίνεται με την έκδοση «ψηφιακών πιστοποιητικών» τα οποία υπογράφονται ηλεκτρονικά από τον ΠΥΠ και τα οποία περιέχουν τα στοιχεία ταυτοποίησης του κατόχου του ιδιωτικού κλειδιού, καθώς και το σχετικό δημόσιο κλειδί του.

Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, δημοσιεύει και υποστηρίζει «τυποποιημένες ηλεκτρονικές βεβαιώσεις» (πιστοποιητικά) για τους συνδρομητές του, δηλαδή τα υποκείμενα πιστοποίησης, ονομάζεται «**Υποδομή Δημοσίων Κλειδιού»** (Public Key Infrastructure – 'PKI').



Εικόνα 10. Ψηφιακό Πιστοποιητικό Ταυτότητας

Κύριος τύπος λοιπόν, των ψηφιακών πιστοποιητικών είναι τα πιστοποιητικά δημοσίου κλειδιού (public key certificate). Το πιστοποιητικό αναφέρει το δημόσιο κλειδί και 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. Ουσιαστικά ένας χρήστης δείχνει εμπιστοσύνη στον ΠΥΠ και κατ' επέκταση δείχνει εμπιστοσύνη και στο πιστοποιητικό που ο ίδιος ΠΥΠ έχει εκδώσει.

Εικόνα 11. Παράδειγμα προβολής πιστοποιητικού

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.

Είναι επιτρεπτό για έναν ΠΥΠ να εκχωρήσει σε τρίτους (outsourcing) τη διεκπεραίωση μέρους ή ακόμη και του συνόλου των παραπάνω παρεχόμενων υπηρεσιών του. Εφόσον όμως ο ΠΥΠ 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.

Οι ιδιωτικές αρχές πιστοποίησης, δηλαδή αυτές που λειτουργούν μόνο στα πλαίσια εντός ενός οργανισμού, ασχολούνται συχνότερα με πιστοποιητικά πελατών. Ένας από τους ελέγχους που οφείλει και θα πρέπει 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.

Η ταυτοποίηση αυτού που υπογραφεί ηλεκτρονικά ένα αρχείο με το πρόσωπο στο οποίο ανήκει το δημόσιο κλειδί αποκρυπτογράφησης του αρχείου επιτυγχάνεται χάρη στο δημόσιο κλειδί του ΠΥΠ, ο οποίο έχει στο μεταξύ υπογράψει και επικυρώσει με το ιδιωτικό κλειδί τα δημόσια κλειδιά των πελατών του, ιδιοκτητών ηλεκτρονικής υπογραφής. Το δημόσιο κλειδί του ΠΥΠ είναι ελεύθερα προσβάσιμο στο Διαδίκτυο. Επίσης, ο ΠΥΠ τηρεί μια βάση δεδομένων προσβάσιμη σε όλους η οποία περιέχει τα δημόσια κλειδιά όλων των πελατών της που είναι κάτοχοι ηλεκτρονικής υπογραφής[47].

Αν η ίδια η αρχή πιστοποίησης παράγει ένα ζεύγος κλειδιών και το αποδώσει στον αιτούντα, μπορεί να διασφαλιστεί ότι εκείνη ακριβώς την στιγμή μόνο ο αιτών έχει στην κατοχή του το ιδιωτικό κλειδί και ότι κανένας άλλος, εκτός από την αρχή πιστοποίησης, δεν έχει

[47] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 44.

πρόσβαση στο ιδιωτικό κλειδί. 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.

Η ευθύνη του ΠΥΠ στηρίζεται αφενός στις γενικές διατάξεις περί συμβατικής και αδικοπρακτικής ευθύνης και αφετέρου στην ειδικότερη ρύθμιση του άρθρου 6 π.δ. 150/2001. Γενικότερα γίνεται δεκτό ότι η παροχή υπηρεσιών πιστοποίησης προϋποθέτει την υπογραφή σύμβασης μεταξύ συνδρομητή (φυσικού ή νομικού προσώπου με δικαιοπρακτική ικανότητα) και ΠΥΠ, αντικείμενο της οποίας αποτελεί η έναντι αμοιβής δημιουργία ηλεκτρονικής υπογραφής, η έκδοση σχετικού πιστοποιητικού και η χορήγηση των δεδομένων επαλήθευσης δημόσιου κλειδιού κάθε φορά που ζητούνται από τους αντισυμβαλλόμενους του συνδρομητή, υπό την προϋπόθεση βέβαια ότι προ της συνάψεως της σύμβασης τηρούνται οι ειδικοί όροι ενημέρωσης, που θέτει το άρθρο 8 Απόφασης Ε.Ε.Τ.Τ 248/71. Ως εκ τούτου η αθέτηση ή πλημμελής εκπλήρωση οιασδήποτε των ως άνω υποχρεώσεων επιφέρει καταρχήν συμβατική ευθύνη του ΠΥΠ έναντι του συνδρομητή με βάση τις γενικές διατάξεις περί πώλησης. Επιπλέον η ύπαρξη ελαττώματος κατά την κατασκευή της υπογραφής επισύρει την ειδική αδικοπρακτική ευθύνη του παραγωγού ελαττωματικού προϊόντος του άρθρου 6 ν. 2251/1994[48].

Από τα πιο πάνω γίνεται αντιληπτό ότι ο κάθε ΠΥΠ, με την έκδοση οποιουδήποτε είδους πιστοποιητικού, αναλαμβάνει ευθύνες τόσο έναντι του «συνδρομητή» του, ο οποίος είτε ταυτίζεται, είτε σχετίζεται με το «υποκείμενο» του εκδιδόμενου πιστοποιητικού, όσο και έναντι κάθε τρίτου προσώπου που 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 του ΠΥΠ, «σύμβαση αποδέκτη»[49].

Από την άλλη μεριά η ευθύνη του ΠΥΠ έναντι του τρίτου αντισυμβαλλόμενου του συνδρομητή είναι κατά βάση αδικοπρακτική. Ως εκ τούτου στηρίζεται στις γενικές διατάξεις περί αδικοπραξίας (άρθρα 914επ ΑΚ). Κατ' εξαίρεση το άρθρο 6 π.δ. 150/2001 προβλέπει ειδική βάση αδικοπρακτικής ευθύνης για όσους φορείς εκδίδουν αναγνωρισμένα πιστοποιητικά. Η διαφορά του έγκειται στο ότι ενώ οι πρώτες (ΑΚ) ιδρύουν υποκειμενική ευθύνη, η δεύτερη προβλέπει νόθο αντικειμενική (υποκειμενική ευθύνη με αντιστροφή του βάρους απόδειξης) (άρθρο 6 παρ. 1 και 3 π.δ. 150/2001), περιορίζοντας όμως ταυτόχρονα το πεδίο εφαρμογής της στις περιπτώσεις εκείνες, κατά τις οποίες η ζημιά οφείλεται σε ελαττώματα του εκδοθέντος πιστοποιητικού, ιδίως όσο αφορά:

α) την ακρίβεια όλων των στοιχείων που αναφέρονται στο αναγνωρισμένο πιστοποιητικό κατά την στιγμή της έκδοσης του[50], καθώς και την πληρότητά του,

β) τη διαβεβαίωση ότι ο υπογράφων που ταχτοποιείται στο «αναγνωρισμένο πιστοποιητικό» είναι κάτοχος των δεδομένων δημιουργίας υπογραφής (ιδιωτικό κλειδί), που

[48] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο του Διαδικτύου», 2003, σελ. 88-89.

[49] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 10, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

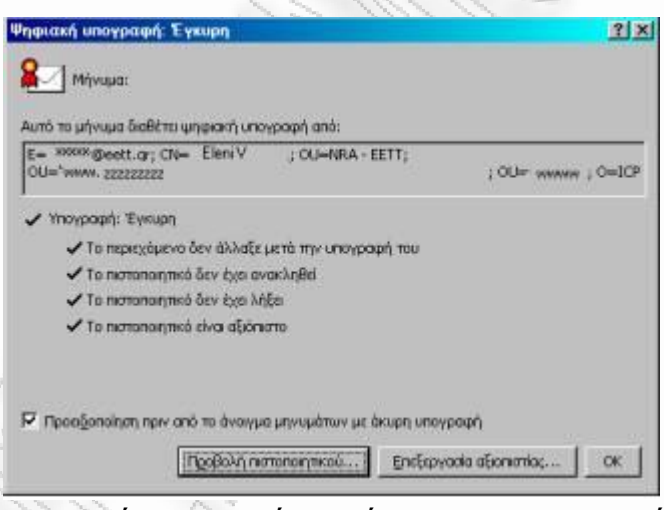
[50] Αν αργότερα αυτά τροποποιηθούν και ο ΠΥΠ δεν λάβει γνώση για αυτό, τότε δεν ευθύνεται αυτός, αλλά το «υποκείμενο» της πιστοποίησης, δηλαδή ο κάτοχος των δεδομένων δημιουργίας υπογραφής, που οφείλει να ενημερώσει τον ΠΥΠ για την συγκεκριμένη αλλαγή, ώστε να «ανακληθεί» το σχετικό πιστοποιητικό.

αντιστοιχούν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό δεδομένα επαλήθευσης της υπογραφής (δημόσιο κλειδί) και

γ) τη διαβεβαίωση ότι τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά. Το ίδιο συμβαίνει και στην περίπτωση που ο φορέας πιστοποίησης παραλείψει να καταγράψει την ανάκληση του υπό κρίση πιστοποιητικού (άρθρο 6 παρ. 2 π.δ. 150/2001). Κατά συνέπεια σε κάθε άλλη περίπτωση ζημίας (π.χ. λόγω παραβίασης των όρων του ν. 2472/1997, προσβολής της φήμης ή της προσωπικότητας του ζημιωθέντος κλπ.) το βάρος απόδειξης θα έχει ο επικαλούμενος τη ζημία (άρθρο 338 ΚΠολΔ)[51].

Η Οδηγία προβλέπει ακόμη και το δικαίωμα του ΠΥΠ «αναγνωρισμένων πιστοποιητικών» να περιορίζει «συμβατικά» την παραπάνω ευθύνη του από την χρήση των πιστοποιητικών που εκδίδει, με την αναγραφή «ορίων στις οικονομικές συναλλαγές»[52] για τις οποίες αυτά επιτρέπεται να χρησιμοποιηθούν, ή / και με κάθε άλλο «περιορισμό στην χρήση» των πιστοποιητικών που ρητώς καθορίζει ο ΠΥΠ. Επίσης, ο ΠΥΠ απαλλάσσεται από κάθε ευθύνη του αν αποδείξει ότι δεν έπραξε «αμελώς».

Εδώ θα πρέπει να αναφέρουμε ότι, 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. Εάν διαπιστωθεί ότι ένα πιστοποιητικό για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον ΠΥΠ ως προς τα στοιχεία της ταυτότητάς του κ.λπ), τότε ο ΠΥΠ είναι υποχρεωμένος να προβεί στην ανάκλησή του, όπως φυσικά ρυθμίζεται από τη ισχύουσα νομοθεσία.



Εικόνα 12. Ένδειξη ψηφιακής υπογραφής σε μήνυμα με πιστοποιητικό

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

[51] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο του Διαδικτύου», 2003, σελ. 89.
[52] Σύμφωνα με το πρότυπο TS 101 862: «Qualified Certificate Profile» του ευρωπαϊκού οργανισμού ETSI, καθώς και το ομώνυμο RFC 3039 του διεθνούς οργανισμού IETF σχετικά με τον τρόπο αναγραφής στα αναγνωρισμένα πιστοποιητικά των διαφόρων «δηλώσεων» («qcStatements») που προβλέπονται από την Οδηγία.

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.

Η ΕΕΤΤ μπορεί μεν να απονέμει δικαιώματα και να επιβάλει υποχρεώσεις στους παρόχους υπηρεσιών πιστοποίησης, δεν μπορεί όμως να περιορίσει τον αριθμό των παρόχων, που επιθυμούν τη διαπίστευση του (άρθρο 4 παράγραφος 5 π.δ. 150/2001)[53].

Η ευθύνη του ΠΥΠ 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 ΠΥΠ μπορεί να απαλλαχθεί εντελώς από την ευθύνη εκ του νόμου εάν αποδείξει ότι η σχετική πράξη ή παράλειψη του δεν προήλθε από αμέλεια[54].

Εάν θα θέλαμε να δούμε τις υποχρεώσεις των ΠΥΠ συνοπτικά θα μπορούσαμε να πούμε ότι είναι οι πιο κάτω:

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

Σε αυτό το σημείο κρίνεται αναγκαίο να αναφέρουμε ότι, η φερεγγυότητα ενός ΠΥΠ εξασφαλίζεται με δυο μεθόδους. Η πρώτη μέθοδος βασίζεται στην θέσπιση μιας «Κορυφαίας Αρχής Πιστοποίησης» και βασίζεται στην πιστοποίηση της φερεγγυότητας ενός ΠΥΠ, από υψηλότερο ιεραρχικά ανώτερου επιπέδου ΠΥΠ, ο οποίος μπορεί με την σειρά του να ελέγχεται από έναν ανώτερου επιπέδου ΠΥΠ. Ο ενδιαφερόμενος μπορεί να ζητήσει πιστοποίηση ηλεκτρονικής υπογραφής από έναν ΠΥΠ και εάν δεν τον εμπιστεύεται ο ενδιαφερόμενος μπορεί να ζητήσει από έναν πιο αξιόπιστο ΠΥΠ να του πιστοποιήσει την ηλεκτρονική υπογραφή. Αυτή η μέθοδος έχει κάποια μειονεκτήματα όπως, πολύ πιθανό ένας ΠΥΠ να μην καλύπτεται πλήρως από μια «αλυσίδα εμπιστοσύνης», γεγονός που καθιστά αναξιόπιστο τον συγκεκριμένο ΠΥΠ. Επίσης, όσο πιο μεγάλη είναι η «αλυσίδα εμπιστοσύνης» που δημιουργείται μεταξύ πολλών ΠΥΠ, τόσο πιο ευάλωτη καθίσταται. Προκειμένου να αποφευχθούν τα πιο πάνω προβλήματα, ακολουθείται συχνά μια δεύτερη μέθοδος, αυτής της «λίστας». Εδώ αναλαμβάνει ενεργό ρόλο κρατική πιστοποίηση, η οποία ελέγχει όσους ΠΥΠ επιθυμούν να λάβουν κρατική πιστοποίηση

[53] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 53.

[54] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 11, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

και δημιουργεί έτσι μια λίστα ελεγμένων και αξιόπιστων ΠΥΠ, τους οποίους προτείνει στον συναλλακτικό κοινό[55].

Θα πρέπει επίσης να σημειωθεί ότι η ευθύνη του ΠΥΠ σχετικά με την ακρίβεια και την εγκυρότητα των χορηγούμενων αναγνωρισμένων πιστοποιητικών περιορίζεται χρονικά κατά τη στιγμή της έκδοσης του. Ως εκ τούτου δεν ευθύνεται για οποιοδήποτε επιγενόμενο ελάττωμα, το οποίο καθιστά το χορηγούμενο πιστοποιητικό ανασφαλές λόγω ενδεχόμενων τεχνολογικών εξελίξεων, που δεν μπορούν να προβλεφτούν κατά το χρόνο έκδοσής του. Παρομοίως η ευθύνη του αίρεται στην περίπτωση, που το υπό κρίση πιστοποιητικό χρησιμοποιήθηκε καθ' υπέρβαση των περιορισμών, που τέθηκαν κατά την έκδοσή του σχετικά με το εύρος της χρήσης του ή το ύψος των συναλλαγών (άρθρο 6 παρ.5 π.δ. 150/2001). Πέρα πάντως της ευθύνης του ΠΥΠ η δημιουργία ελαττωματικής ηλεκτρονικής υπογραφής επιφέρει ανάλογες συνέπειες και στις σχέσεις του συνδρομητή με τον αντισυμβαλλόμενο του, όταν συνεπάγεται ανωμαλία στη μεταξύ τους συμβατική σχέση. Εν προκειμένω ο ΠΥΠ επέχει τη θέση βοηθού εκπληρώσεως και ως εκ τούτου η από μέρους του παράνομη συμπεριφορά γεννά συμβατική ευθύνη του συνδρομητή - οφειλέτη - έναντι του τρίτου - δανειστή - βάσει της διάταξης του άρθρου 334 ΑΚ[56].

Θα πρέπει να διευκρινίσουμε ότι οι ΠΥΠ ηλεκτρονικών υπογραφών και «συναφών υπηρεσιών» δεν υπόκειται σε καθεστώς αδειοδότησης και άρα μπορεί οποιοσδήποτε (φυσικό ή νομικό πρόσωπο) να λειτουργήσει ως ΠΥΠ και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός ΠΥΠ προς την εποπτεύουσα αρχή (ΕΕΤΤ) είναι η «Δήλωση Έναρξης Λειτουργίας» και η εγγραφή του στο σχετικό «Μητρώο ΠΥΠ», καθώς και η αποστολή «Ετήσιων Εκθέσεων» σχετικά με την λειτουργία τους. Για να μπορέσει να εκδώσει ένας ΠΥΠ «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 ΠΥΠ 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 ΠΥΠ αποκτά «δικαίωμα επίκλησης» της συγκεκριμένης διαπίστευσής του προς κάθε τρίτο, υποβάλλεται όμως σε περαιτέρω υποχρεώσεις και ελέγχους που συνήθως επιβάλλει ο σχετικός φορέας[57].

Στο σημείο αυτό θα πρέπει να αναφέρουμε δυο πολύ σημαντικές υπηρεσίες που παρέχουν οι ΠΥΠ, αυτές είναι η χρονοσήμανση και η αποθήκευση. Η χρονοσήμανση (time stamping) των ηλεκτρονικών μηνυμάτων είναι η υπηρεσία με την οποία ο ΠΥΠ θέτει στο έγγραφο ηλεκτρονική σφραγίδα η οποία είναι αδύνατο να αλλοιωθεί και φανερώνει με ακρίβεια την ημερομηνία και την ώρα αποστολής και λήψης ενός ηλεκτρονικά υπογεγραμμένου έγγραφο στο πλαίσιο μιας συναλλαγής. Η χρήση των ηλεκτρονικών υπογραφών και η ασφάλεια που αυτές παρέχουν στις συναλλαγές έχει ως βάση της το γεγονός ότι ο υπογράφον δεν έχει την δυνατότητα να αποποιηθεί την ευθύνη του και να αρνηθεί εκ των υστέρων ότι υπέγραψε[58].

Στην αποθήκευση των ηλεκτρονικών μηνυμάτων ο ΠΥΠ λειτούργει ως ένας ηλεκτρονικός συμβολαιογράφος. Κάθε είδους ηλεκτρονικά έγγραφα που ο συναλλασσόμενος θεωρεί πολύτιμα ή δεν επιθυμεί να αμφισβητηθούν από κανέναν, μπορούν να κατατεθούν στον ΠΥΠ, έτσι ώστε εάν προκύψει οποιαδήποτε στιγμή πρόβλημα ή δικαστική διαμάχη να είναι δυνατή ανά πάσα στιγμή η παρουσίαση του πρωτοτύπου αποθηκευμένου μηνύματος. Το ηλεκτρονικό έγγραφο φυλάσσεται πάντα στη μορφή που το απέστειλε ο συναλλασσόμενος, δηλαδή απλώς

[55] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 45-47.
[56] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο του Διαδικτύου», 2003, σελ. 89.
[57] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 10, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)
[58] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 47-49.

υπογεγραμμένο ή και κρυπτογραφημένο και για όσο διάστημα επιθυμούν τα συμβαλλόμενα μέρη. Το αποθηκευμένο κείμενο μπορεί να είναι και χαρτοσημασμένο[59].

Τέλος, η Ευρωπαϊκή 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 απαιτήσεις ασφάλειας και αξιοπιστίας της Οδηγίας (βάσει σχετικών γενικώς αναγνωρισμένων προτύπων) από σχετικούς αρμόδιους φορείς[60].

3.5.3 Οργανισμοί Τυποποίησης και Πιστοποίησης της Ηλεκτρονικής Υπογραφής στην Ευρωπαϊκή Ένωση

Ένας πολύ σημαντικός παράγοντας για την εξέλιξη της τεχνολογίας των ηλεκτρονικών υπογραφών είναι η ύπαρξη πρότυπων που έχουν εκδοθεί από Ευρωπαϊκούς και από διεθνείς οργανισμούς τυποποίησης. Όπως έχει ήδη αναφερθεί, η οδηγία 1999/93 παρέχει τη δυνατότητα στην Ευρωπαϊκή Επιτροπή να καθορίζει και να δημοσιεύει αριθμούς αναφοράς «γενικώς αναγνωρισμένων προτύπων» για προϊόντα ηλεκτρονικής υπογραφής[61]. Στην χώρα μας έχουμε την ενσωμάτωση των περιεχόμενων της οδηγίας στο π.δ. 150/2001.

Σήμερα 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. Με εντολή της Ευρωπαϊκής Επιτροπής προς την Ευρωπαϊκή Επιτροπή Τυποποίησης (CEN), συγκροτήθηκε η Ευρωπαϊκή Πρωτοβουλία τυποποίησης της Ηλεκτρονικής υπογραφής (EESSI), η οποία αποτελούνται από μέλη των οργανισμών CEN/ISSS και ETSI και η οποία εκπόνησε πρότυπα για προϊόντα και υπηρεσίες ηλεκτρονικής υπογραφής.

Η Ευρωπαϊκή Επιτροπή επίσης, δημοσίευσε Απόφαση [62] βασισμένη στο άρθρο 3 παράγραφος 5 της οδηγίας, η οποία συμπεριέλαβε αναφορές σε πρότυπα CEN (CWA) για τις προϋποθέσεις και τις απαιτήσεις που αναφέρονται στη δημιουργία αναγνωρισμένων ηλεκτρονικών υπογραφών[63]. Πέρα από αυτά Σύμφωνα με το άρθρο 3 παράγραφος 5, είναι δυνατόν να εκπονηθούν και άλλα πρότυπα και να γίνουν αποδεκτά από την Επιτροπή για την κάλυψη των απαιτήσεων της οδηγίας, εφόσον μπορούν να θεωρηθούν ως «γενικά αναγνωρισμένα πρότυπα». Οι απαιτήσεις των παραρτημάτων είναι επίσης δυνατόν να καλυφθούν εν γένει από άλλα πρότυπα εκτός των αναφερόμενων στην Επίσημη Εφημερίδα.

---

[59] Καραδημητρίου, ο.π., σελ. 47-49.

[60] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 4, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[61] Το άρθρο 3 παράγραφος 5 της οδηγίας παρέχει στην Επιτροπή τη δυνατότητα να καθορίζει και να δημοσιεύει αριθμούς αναφοράς «γενικώς αναγνωρισμένων προτύπων», για προϊόντα ηλεκτρονικής υπογραφής. Κατά συνέπεια, εφόσον ένα προϊόν ηλεκτρονικής υπογραφής ανταποκρίνεται στα εν λόγω πρότυπα, τεκμαίρεται η συμμόρφωσή του με τις απαιτήσεις του παραρτήματος ΙΙ στοιχείο στ) και του παραρτήματος ΙΙΙ. (πηγή http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006 DC0120:EL:NOT, Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Έκθεση αναφορικά με τη λειτουργία της οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές , ημερομηνία επίσκεψης 31/07/2011).

[62] 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.

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

Είναι σημαντικό για την αγορά, κατά τις μελλοντικές εργασίες τυποποίησης να λαμβάνονται υπόψη οι νέες τεχνολογικές εξελίξεις, δεδομένου ότι οι χρήστες θα μεταφέρουν μελλοντικά το κλειδί ηλεκτρονικής υπογραφής τους από συσκευή σε συσκευή, σε ένα ευρύτερα συνδεδεμένο περιβάλλον[64].

Ο τομέας των επικοινωνιών και της πληροφορικής είναι ένας τομέας ταχύτατα αναπτυσσόμενος και διαρκώς μεταβαλλόμενος, σε αυτόν τον 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:

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

Τέλος, θα πρέπει να αναφέρουμε στο σημείο αυτό το Ινστιτούτο Ευρωπαϊκών Τηλεπικοινωνιακών Προτύπων (European Telecommunications Institute – ETSI), το οποίο είναι ένα ακόμα από τα ευρωπαϊκά σώματα τυποποίησης και το οποίο παράγει ένα μεγάλο εύρος προτύπων και άλλης τεχνικής βιβλιογραφίας. Αποτελεί με τον τρόπο αυτό σημαντικό μέρος της Ευρωπαϊκής συμβολής στην παγκόσμια τυποποίηση στις τηλεπικοινωνίες και στα συναφή πεδία της εκπομπής (broadcasting) και της τεχνολογίας των πληροφοριών. Το Ινστιτούτο Ευρωπαϊκών Τηλεπικοινωνιακών Προτύπων, 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:

- Τη χρήση των πιστοποιητικών του κοινού κλειδιού X.509 ως εγκεκριμένων
- Την ασφάλεια και την πολιτική πιστοποίησης των CSP που δίνουν αναγνωρισμένα πιστοποιητικά
- Τη σύνταξη των ηλεκτρονικών υπογραφών και τα μορφότυπα κωδικοποίησης καθώς και άλλες τεχνικές πλευρές της σχετικής πολιτικής
- Το πρωτόκολλο για τη διαλειτουργικότητα με την υπηρεσία χρονοσήμανσης
- Την ασφάλεια και την πολιτική πιστοποίησης των CSP που δίνουν μη αναγνωρισμένα πιστοποιητικά
- Την ασφάλεια και την πολιτική των απαιτήσεων για τους CSP που εκδίδουν χρονοσήμαντρα

[64] Διαθέσιμο στην ιστοσελίδα http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0120:EL:NOT, Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Έκθεση αναφορικά με τη λειτουργία της οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές**,** **(**ημερομηνία επίσκεψης 31/07/2011).

- Τη σύνταξη των ηλεκτρονικών υπογραφών και τα μορφότυπα κωδικοποίησης σε XML
- Τις πολιτικές υπογραφών για εκτεταμένα μοντέλα εργασιών
- Την εναρμονισμένη παροχή πληροφοριών για την κατάσταση των CSP

3.6 Δημιουργία Ψηφιακής υπογραφής

3.6.1 Εισαγωγή

Η ψηφιακή υπογραφή βασίζεται στην τριμερή ασύμμετρη κρυπτογραφία και φέρει όλα τα πλεονεκτήματα αυτής της τεχνολογίας, για τον λόγο αυτό θεωρείται η πιο άρτια και ασφαλής τεχνολογικά μέθοδος διαπίστωσης της ταυτότητας του ηλεκτρονικά συναλλασσόμενου και διαφύλαξης της ακεραιότητας του αποστελλόμενου αρχείου[65]. Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: α) τη δημιουργία της υπογραφής και β) την επαλήθευσή της[66]. Ο αποστολέας πραγματοποιεί την μέθοδο της δημιουργίας ψηφιακής υπογραφής ενός ηλεκτρονικού κειμένου, ενώ ο παραλήπτης πραγματοποιεί τη μέθοδο επαλήθευσης της ψηφιακής υπογραφής, δηλαδή επαληθεύει το αν η ψηφιακή υπογραφή παράχθηκε από αυτόν που πραγματικά αντιπροσωπεύει. Η ψηφιακή υπογραφή δημιουργείται από ένα ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί χρησιμοποιείται για να επαληθευθεί ότι η υπογραφή δημιουργήθηκε χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί. Στην συνέχεια θα παρουσιάσουμε αυτές τις δυο διαδικασίες αναλυτικά.

3.6.2 Μέθοδοι δημιουργίας ψηφιακής υπογραφής

Η πιο συνηθισμένη και εύχρηστη μέθοδος δημιουργίας μιας ψηφιακής υπογραφής είναι η μέθοδος της δημιουργίας του «δακτυλικού αποτυπώματος», δηλαδή της σύντμησης του αρχείου που πρόκειται να κρυπτογραφηθεί. Κατά την μέθοδο αυτή ο αποστολέας του ηλεκτρονικού αρχείου, κειμένου ή άλλου, το «σφραγίζει» δηλαδή παράγει μια σύντμηση (message digest) του μεταβιβαζόμενου κειμένου με τη βοήθεια ενός αλγόριθμου (hashing algorithm), ο οποίος δεν έχει καμία σχέση με κανέναν άλλο αλγόριθμο. Από τα πιο πάνω γίνεται αντιληπτό ότι σε αυτή την διαδικασία δημιουργίας ψηφιακής υπογραφής, δεν κρυπτογραφούνται τα προς υπογραφή δεδομένα, αλλά μία μικρή μαθηματική «σύνοψή» τους.

Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μια συγκεκριμένου μήκους σειρά αριθμητικών ψηφίων, αναλόγως του πόσο ισχυρή κρυπτογραφία χρησιμοποιούμε. Ο αλγόριθμος αυτός παράγει πάντα το ίδιο συντετμημένο κείμενο (hash reslt) για το ίδιο αρχικό κείμενο, ενώ αντίστροφη διαδικασία είναι αδύνατη. Είναι επίσης, πρακτικά αδύνατο να βρούμε δύο διαφορετικά κείμενα από τα οποία να παράγεται η ίδια συνάρτηση, επειδή ο αλγόριθμος που χρησιμοποιείται είναι εξαιρετικά ευαίσθητος σε μεταβολές που γίνονται στο αρχικό μήνυμα[67].

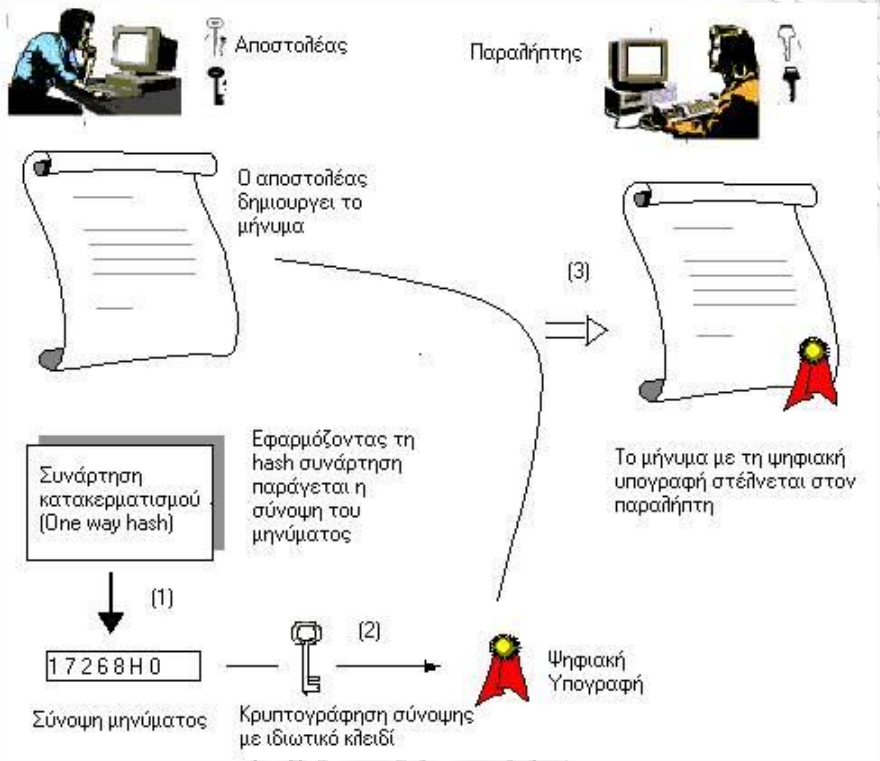
Το συντετμημένο κείμενο που προκύπτει από την πιο πάνω διαδικασία, κρυπτογραφείται με την χρήση του απόρρητου ιδιωτικού κλειδιού, το οποίο έχει στην κατοχή του ο αποστολέας, ο οποίος είναι και εκείνος που υπογράφει το κείμενο. Αυτό το κείμενο, που έχει πλέον κρυπτογραφηθεί και είναι συντετμημένο αποτελεί, μαζί με μια σειρά επιπρόσθετες πληροφορίες, όπως είναι η ταυτότητα του υπογράφοντα και η ημερομηνία υπογραφής, την ψηφιακή υπογραφή. Η ψηφιακή υπογραφή προσαρτάται στο πρωτότυπο ηλεκτρονικό μήνυμα που είναι μη κρυπτογραφημένο. Τελικά και τα δύο μαζί ως ένα ενιαίο μήνυμα αποστέλλονται μέσω του Διαδικτύου στον παραλήπτη.

[65] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.50.

[66] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_ Communications/DigitalSignatures/ IntroEsign.html (ημερομηνία επίσκεψης 20/05/2011)

[67] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.50-51.

Στην εικόνα που παρουσιάζεται πιο κάτω, φαίνεται αναλυτικά η διαδικασία δημιουργίας της ψηφιακής υπογραφής και τα βήματα που ακολουθούνται για αυτήν.

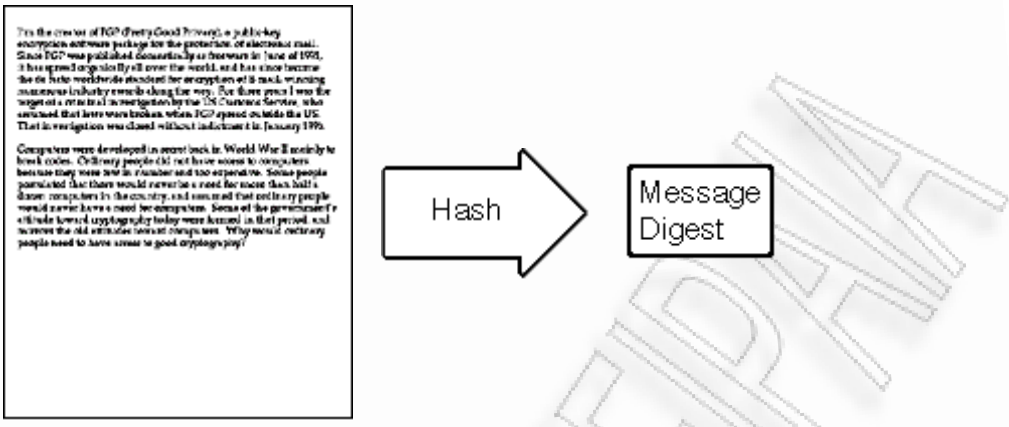


Εικόνα 13. Μέθοδος δημιουργίας ψηφιακής υπογραφής Message Digest

Τα βήματα για την δημιουργία ψηφιακής υπογραφής με την χρήση της μεθόδου massage digest, παρουσιάζονται πιο κάτω και είναι τα έξης[68]:

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.

[68] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html (ημερομηνία επίσκεψης 20/05/2011)

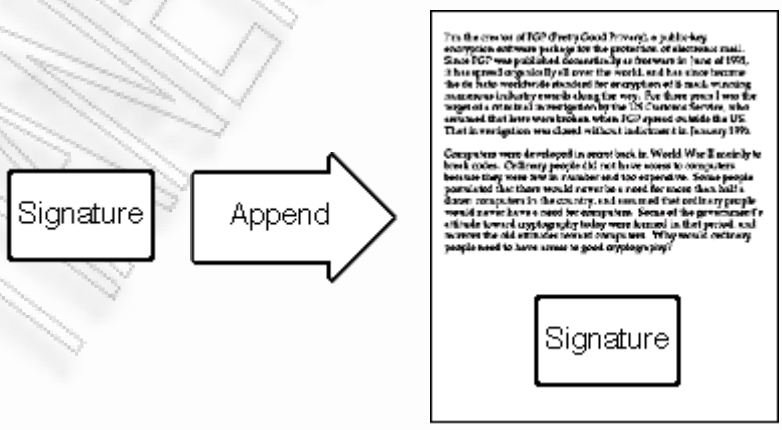


Εικόνα 14. Βήμα πρώτο – Αλγόριθμος κατακερματισμού και σύνοψη μηνύματος

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.

Εικόνα 15. Βήμα δεύτερο – Κρυπτογράφηση με ιδιωτικό κλειδί

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.



Εικόνα 16. Βήμα τρίτο – Προσάρτηση ψηφιακής υπογραφής και αποστολή μηνύματος

Στην διαδικασία της δημιουργίας και της επαλήθευσης της ψηφιακής 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. 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 ψηφιακή υπογραφή είναι στην ουσία η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα, σύνοψη και είναι διαφορετική για κάθε μήνυμα. Από τα πιο πάνω γίνεται αντιληπτό ότι, η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή.

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 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.

Μια άλλη μέθοδος δημιουργίας ψηφιακής υπογραφής είναι αυτή του «ψηφιακού φακέλου» (digital envelope), Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με την δημόσια κλείδα της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Η μέθοδος του ψηφιακού φακέλου συνδυάζει τα συστήματα συμμετρικών και ασύμμετρων αλγορίθμων και επιτυγχάνει με τον τρόπο αυτό να μειώνει το χρόνο κρυπτογράφησης του μηνύματος, καθώς οι συμμετρικοί αλγόριθμοι κρυπτογραφούν ένα αρχείο πολύ πιο γρήγορα από τους συμμετρικούς. Η μέθοδος αυτή διεθνώς αναφέρεται ως «υβριδικό σύστημα κρυπτογραφίας» (hybrid crypto system), το μήνυμα κρυπτογραφείται συμμετρικά από τον αποστολέα με τη χρήση ενός σύντομου αλλά ασφαλούς κλειδιού μήκους 128 bits, το ποίο καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και ονομάζεται «κλειδί συνεδρίας». Στην συνέχεια και για περισσότερη ασφάλεια, το κλειδί αυτό κρυπτογραφείται με ασύμμετρη κρυπτογραφία, δηλαδή με το δημόσιο κλειδί του παραλήπτη. Έτσι, ο παραλήπτης του εγγράφου θα πρέπει πρώτα να χρησιμοποιήσει το ιδιωτικό του κλειδί για να βρει το «κλειδί συνεδρίας» του αποστολέα και μέσω αυτού του κλειδιού και το αρχικό μήνυμα[69]. Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι η μέθοδος ασύμμετρης κρυπτογραφίας RSA με τη μέθοδο συμμετρικής κρυπτογραφίας DES.

Υπάρχουν τέλος, περιπτώσεις κατά τις οποίες ο αποστολέας του ηλεκτρονικού μηνύματος, με σκοπό και στόχο να επιτύχει ακόμα μεγαλύτερη εμπιστευτικότητα διπλοκρυπτογραφεί το ηλεκτρονικό μήνυμα. Αυτό το κάνει τόσο με το δικό του ιδιωτικό κλειδί, όσο και με το αντίστοιχο δημόσιο κλειδί του παραλήπτη. Με τον τρόπο αυτό ο αποστολέας και ο παραλήπτης είναι βέβαιοι για την ταυτότητα του αντισυμβαλλόμενου τους και αυξάνεται με τον τρόπο αυτό η εμπιστοσύνη μεταξύ τους.

[69] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.52.

Στο σημείο αυτό κρίνεται σκόπιμο να παρουσιάσουμε τις συστάσεις για την διασφάλιση της αξιοπιστίας της δημιουργίας υπογραφής σύμφωνα με το π.δ. 150/2001[70], αναφέρει τα εξής:

1. 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 μια 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.

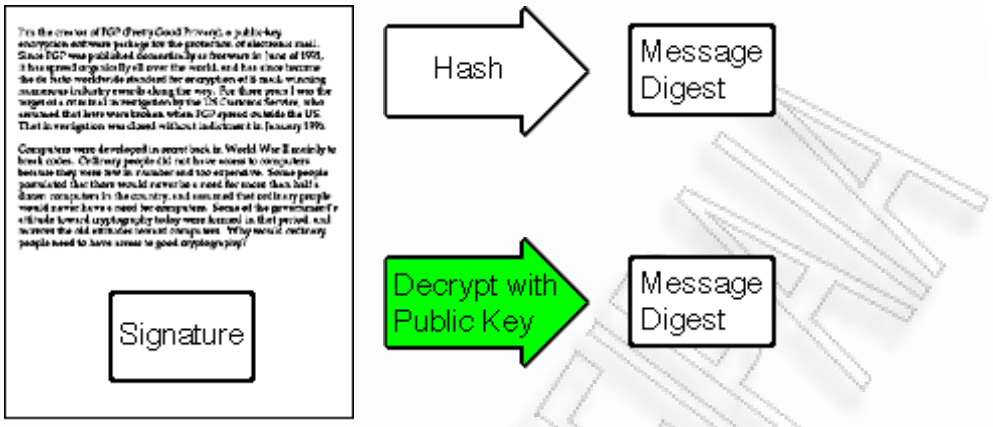
2. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν μεταβάλλουν τα προς υπογραφή δεδομένα ούτε εμποδίζουν την υποβολή των δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

3.6.3 Διαδικασία Επαλήθευση Ψηφιακής Υπογραφής

Η διαδικασία επαλήθευσης της ψηφιακής υπογραφής εκτυλίσσεται στον παραλήπτη του κρυπτογραφημένου αρχείου. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή, δηλαδή την κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύντμηση του μηνύματος και την αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα. Το δημόσιο κλειδί του αποστολέα είτε αποστέλλεται στο λήπτη μαζί με το κρυπτογραφημένο κείμενο είτε γνωστοποιείται μέσω δημοσίευσης σε ειδικό δημόσιο κατάλογο που τηρεί ο ΠΥΠ. Με την αποκρυπτογράφηση αυτή ο παραλήπτης επαληθεύει την ταυτότητα του αποστολέα[71].

Κατά την διαδικασία της επαλήθευσης της ψηφιακής υπογραφής, εφαρμόζει ο παραλήπτης στο κείμενο που έλαβε από τον αποστολέα, το «δακτυλικό αποτύπωμα» του κειμένου που έλαβε, εφαρμόζοντας στο πρωτότυπο μήνυμα τον ίδιο αλγόριθμο κατακερματισμού (hashing algorithm) που χρησιμοποιήθηκε κατά την υπογραφή του από τον αποστολέα και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Ο αλγόριθμος παράγει εκ νέου μια σύντμηση του μεταβιβαζόμενου ηλεκτρονικού κειμένου, η οποία συγκρίνεται από τον παραλήπτη με τη σύντμηση που παρέλαβε (επαλήθευση ψηφιακής υπογραφής). Αν οι δυο συντμήσεις είναι ίδιες, τότε η υπογραφή επαληθεύεται και επιβεβαιώνεται και επίσης πιστοποιείται ότι το απεσταλμένο μήνυμα δεν αλλοιώθηκε ώσπου να φτάσει στον παραλήπτη. Αν το μήνυμα έχει αλλοιωθεί ή μεταβληθεί, η σύνοψη που παράγει ο παραλήπτης κατά την διαδικασία της επαλήθευσης, είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί και συνεπώς το ηλεκτρονικό μήνυμα έχει υποστεί κάποια αλλοίωση ή μεταβολή.

[70] Π.Δ. 150/2001 Παράρτημα ΙΙΙ, Διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής.
[71] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.53.



Εικόνα 17. Μέθοδος επαλήθευσης ψηφιακής υπογραφής

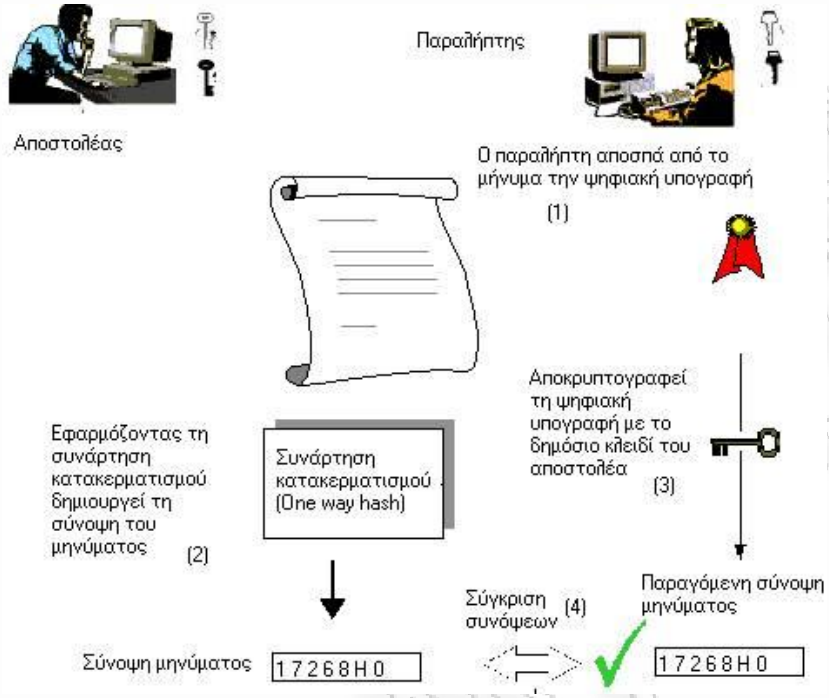
Τα βήματα για την επαλήθευση ψηφιακής υπογραφής παρουσιάζονται πιο κάτω και είναι τα έξης[72]:

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. 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.

Στο σημείο αυτό θα πρέπει να προσθέσουμε ότι σύμφωνα με το π.δ. 150/2001, κατά την διαδικασία επαλήθευσης της ψηφιακής υπογραφής θα πρέπει να διασφαλίζεται με εύλογη βεβαιότητα ότι[73]:

- Τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα.
- Η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο
- Ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται
- Η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία
- Το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο.
- Η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς και
- Μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.

[72] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html (ημερομηνία επίσκεψης 20/05/2011).
[73] π.δ. 150/2001 Παράρτημα IV, Συστάσεις για την ασφαλή επαλήθευση της υπογραφής.



Εικόνα 18. Διαδικασία επαλήθευσης ψηφιακής υπογραφής με χρήση ιδιωτικού και δημόσιου κλειδιού.

3.6.4 Εξοπλισμός Δημιουργίας και Επαλήθευσης Ηλεκτρονικής Υπογραφής[74]

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 υλισμικού (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.

Για την δημιουργία αναγνωρισμένης ψηφιακής υπογραφής, η νομοθεσία απαιτεί την χρήση ασφαλούς διάταξης δημιουργίας υπογραφής (Secure Signature Creation Devices – SSCD). Ως τέτοια προσδιορίζεται[75] 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' ουσία, 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

[74] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 9 - 10, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011).
[75] Σύμφωνα με το Παράρτημα ΙΙΙ της Οδηγίας 1999/93 και το ΠΔ 150/2001.

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 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.

3.6.5 Διαδικασία Έκδοσης Πιστοποιητικού Γνησιότητας Ψηφιακής Υπογραφής

Ο ιδιοκτήτης ψηφιακής υπογραφής αλλά και κάθε τρίτος συναλλασσόμενος με αυτόν, μπορεί ανά πάσα στιγμή να προμηθευτεί από τον αρμόδιο ΠΥΠ πιστοποιητικό γνησιότητας της υπογραφής. Για να γίνει αυτό θα πρέπει καταρχήν ο ενδιαφερόμενος χρήστης να παραγάγει, με την βοήθεια κατάλληλου λογισμικού που έχει προμηθευτεί από τον ΠΥΠ, το ζεύγος ιδιωτικού και δημόσιου κλειδιού που αποτελεί την ψηφιακή υπογραφή. Αφού αποθηκεύσει το ιδιωτικό του κλειδί είτε στο σκληρό δίσκο του Η/Υ του είτε σε κινητό μαγνητικό μέσο προστατευμένο από μυστικό κώδικα, ο χρήστης αποστέλλει το δημόσιο κλειδί του στον ΠΥΠ αιτούμενος την πιστοποίηση του. Ο αρμόδιος χρήστης του ΠΥΠ διαπιστώνει την ύπαρξη της αίτησης και επικοινωνεί με τον ενδιαφερόμενο για να του ζητήσει να εμφανιστεί στην «Αρχή Εγγραφής», δηλαδή στο περιφερικό όργανο έλεγχου, το οποίο διαπιστώνει την ακριβή ταυτότητα του ενδιαφερόμενου. Ως περιφερικό όργανο ελέγχου μπορεί να λειτουργήσει οποιοσδήποτε φορέας, όπως ένα γραφείο Επιμελητηρίου, υπό τον έλεγχο πάντα του ΠΥΠ[76].

Μέτα τον έλεγχο, ο αρμόδιος υπάλληλος του ΠΥΠ προχωρεί στην έκδοση του ψηφιακού πιστοποιητικού, το οποίο περιέχει συνήθως το όνομα του ιδιοκτήτη της ψηφιακής υπογραφής, το δημόσιο κλειδί του, την ηλεκτρονική του διεύθυνση, την διεύθυνση νόμιμης κατοικίας του, την διάρκεια ισχύος του πιστοποιητικού[77], τυχόν περιορισμούς για την χρήση του, τυχόν όρια για το ύψος των συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί το σχετικό πιστοποιητικό καθώς και τα στοιχεία της Αρχής που το εξέδωσε. Το πιστοποιητικό με όλες τις πληροφορίες υπογράφεται ηλεκτρονικά, δηλαδή κρυπτογραφείται, με το ιδιωτικό κλειδί του ΠΥΠ και

[76] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.54.

[77] Τα πιστοποιητικά έχουν ημερομηνία λήξης, συνήθως 6 μήνες έως ένα χρόνο από την ημερομηνία έκδοσης τους. Μετά την λήξη τους δημοσιεύονται σε δημόσιο κατάλογο ληγμένων πιστοποιητικών, ώστε ο κάθε ενδιαφερόμενος να είναι σε θέση να πληροφορείται το περιεχόμενο του καταλόγου.

αποστέλλεται στον ενδιαφερόμενο. Όταν το πιστοποιητικό έχει ζητηθεί από τον ιδιοκτήτη της υπογραφής, τότε αυτός μπορεί να το αποθηκεύσει στον σκληρό δίσκο του Η/Υ του και να το χρησιμοποιήσει σε κάθε ηλεκτρονική συναλλαγή του προς επιβεβαίωση της ταυτότητας του ως υπογράφοντος. Η επιβεβαίωση αυτή επιτυγχάνεται με την αποκρυπτογράφηση της ηλεκτρονικής υπογραφής του ΠΥΠ χρησιμοποιώντας το δημόσιο κλειδί του ΠΥΠ, το οποίο είναι διαθέσιμο στο Διαδίκτυο[78].

Εκτός όμως από τις ευθύνες του ΠΥΠ, ευθύνη για την γνησιότητα και την σωστή λειτουργία και χρήση των πιστοποιητικών έχουν τόσο ο αποστολέας όσο και ο αποδέκτης των ηλεκτρονικών υπογραφών. Δηλαδή, τόσο ο αποστολέας όσο και ο αποδέκτης μιας ψηφιακής υπογραφής, πρέπει να κατανοούν τον τρόπο χρήσης και λειτουργίας των ψηφιακών υπογραφών που χρησιμοποιούν. Επίσης, πρέπει 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 «υπογράφων» (δηλ. ο αποστολέας), που είναι ο 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[79]:

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

Η ισχύς ενός πιστοποιητικού μπορεί να ανακληθεί οριστικά ή να ανασταλεί οποιαδήποτε στιγμή, ύστερα από αίτημα του υπογράφοντος, ο οποίο είναι ο νόμιμος χρήστης του πιστοποιητικού είτε με σχετική απόφαση του ΠΥΠ[80]. Αυτά τα πιστοποιητικά αναγράφονται σε μια λίστα ανακληθέντων πιστοποιητικών, η οποία εποπτεύεται από τον ΠΥΠ. Ένα πιστοποιητικό είναι έγκυρο μόνο όταν δεν έχει λήξει ή δεν έχει ανακληθεί[81].

Ο «αποδέκτης» μιας ψηφιακής υπογραφής, πριν βασισθεί στα περιεχόμενα του σχετικού πιστοποιητικού (ώστε να διαμορφώσει συγκεκριμένη πεποίθηση για ένα γεγονός ή να προβεί σε

[78] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ.55.

[79] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 12, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[80] Αιτίες ανάκλησης ή αναστολής της ισχύος ενός πιστοποιητικού μπορεί να είναι η καταστροφή του φυσικού μέσου αποθήκευσης της ηλεκτρονικής υπογραφής, η κλοπή της ηλεκτρονικής υπογραφής ή η λάθος αναγραφή στοιχείων στο πιστοποιητικό.

[81] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 55 - 56.

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 επαληθεύει την υπογραφή)[82]:

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 [83], τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή, έστω, να επιτρέπεται από την εφαρμοζόμενη Πολιτική Υπογραφής.

Από τη στιγμή που τα συμβαλλόμενα μέρη συμφωνούν σχετικά με την έκδοση πιστοποιητικού γνησιότητας ηλεκτρονικής υπογραφής από τον αρμόδιο για αυτό ΠΥΠ, η περιεχόμενη στο πιστοποιητικό βεβαίωση της γνησιότητας της υπογραφής είναι δεσμευτική για τα μέρη. Η γνησιότητα της ηλεκτρονικής υπογραφής λοιπόν, τεκμαίρεται δυνάμει της προϋπάρχουσας συμφωνίας μεταξύ των μερών, όχι όμως αμάχητη, αφού κάτι τέτοιο θα αντέβαινε στο δικαίωμα του κάθε μέρους να προστατευθεί δικαστικά. Ο δικαστής είναι αυτός που τελικά κρίνει αν ο ΠΥΠ είναι αρμόδιος και αξιόπιστος να εκδώσει πιστοποιητικό γνησιότητας[84].

3.6.6 Εφαρμογές της Ψηφιακής υπογραφής

Σήμερα η ψηφιακή υπογραφή έχει εφαρμογή σε πάρα πολλούς, εάν όχι σε όλους, τους τομείς που αφορούν τις ηλεκτρονικές συναλλαγές. Η εφαρμογή της ψηφιακής υπογραφής υπάρχει ακόμα και στην καθημερινότητα του κάθε απλού χρήστη ηλεκτρονικών υπηρεσιών πολλές φορές αυτό είναι εν αγνοία του. Έτσι για παράδειγμα μπορεί ένας χρήστης να πραγματοποιεί τις

[82] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 12, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[83] 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.

[84] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 56 - 57.

απλές καθημερινές του ηλεκτρονικές συναλλαγές κάνοντας χρήση της ψηφιακής υπογραφής χωρίς να το γνωρίζει.

Σε διεθνές επίπεδο, η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφάλειας σε συναλλαγές διαφόρων τύπων όπως[85]:

- 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 EuroPay, 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.

Στα πλαίσια της Ευρωπαϊκής Ένωσης, εκτός από ένα μεγάλο πλήθος άτυπων εφαρμογών ηλεκτρονικής υπογραφής σε τομείς όπως οι τηλεπικοινωνίες, οι τραπεζικές εφαρμογές, το εμπόριο κλπ, έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία τυπικές εφαρμογές των ηλεκτρονικών υπογραφών. Τέτοιες εφαρμογές ηλεκτρονικών υπογραφών παρουσιάζονται στην συνέχεια.

Ένας πολύ σημαντικός τομέας εφαρμογής των ηλεκτρονικών υπογραφών είναι τα ηλεκτρονικά τιμολόγια. Η χρησιμοποίηση ηλεκτρονικής υπογραφής ή του τυποποιημένου συστήματος EDI (Electronic Data Interchange) κατά την έκδοση «ηλεκτρονικών τιμολογίων» (e-invoicing) υποχρεώνει τις αρχές των κρατών μελών να δεχθούν τα εκδιδόμενα ηλεκτρονικά τιμολόγια, ενώ, παράλληλα, διευκολύνει την αρχειοθέτηση και την άμεση ανταλλαγή τους[86].

Οι ηλεκτρονικές ταυτότητες και τα διαβατήρια που αναφέραμε πιο πριν, αποτελούν μία περίπτωση ευρείας εφαρμογής των ηλεκτρονικών υπογραφών, ήδη έχουν θεσμοθετηθεί ή βρίσκονται σε λειτουργία σε αρκετά ευρωπαϊκά κράτη, όπως π.χ. Βέλγιο, Φινλανδία, Ιταλία, Εσθονία, κ.ά. Η κυρίαρχη τάση σ' αυτές είναι η χρήση δύο (ή και τριών) ζευγών κλειδιών και σχετικών πιστοποιητικών, (ένα για «ταυτοποίηση» και ένα για «αναγνωρισμένες ηλεκτρονικές υπογραφές» και πιθανώς και ένα τρίτο για την κρυπτογράφηση δεδομένων). Τα στοιχεία αυτά δημιουργούνται ή τοποθετούνται σε ένα μικροεπεξεργαστή που βρίσκεται σε έναν ασφαλή φορέα όπως για παράδειγμα μία έξυπνη κάρτα. Στην κάρτα αυτή αναγράφονται επίσης και τα στοιχεία του κατόχου και περιλαμβάνεται και η φωτογραφία του, ώστε να διευκολύνεται ο οπτικός έλεγχος. Η ταυτότητα αυτή χρησιμοποιείται όπως κάθε άλλη ταυτότητα από τα κράτη - μέλη. Παραδείγματα αποτελούν η FINeID της Φινλανδίας, η eID στο Βέλγιο, Σουηδία κλπ. Σχετική με τις ηλεκτρονικές ταυτότητες και τα διαβατήρια είναι η σχεδιαζόμενη ηλεκτρονική

[85] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 13, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)
[86] Σύμφωνα με την Ευρωπαϊκή Οδηγία 115 της 20ης Δεκεμβρίου 2001.

«Ευρωπαϊκή Κάρτα Υγείας» με την οποία ο κάτοχός της θα ταυτοποιείται και θα μπορεί να έχει πρόσβαση στα διαφορετικά συστήματα υγειονομικής περίθαλψης όλων των κρατών - μελών[87].

Πολύ σημαντικός επίσης, τομέας εφαρμογής των ηλεκτρονικών υπογραφών είναι και 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.).

Η εφαρμογή των ηλεκτρονικών υπογραφών υπάρχει ακόμα και μέσω των δικτύων κινητής τηλεφωνίας. Η συσκευή του κινητού τηλεφώνου που έχουμε και χρησιμοποιούμε όλοι μας είναι στην ουσία ένας «αναγνώστης έξυπνων καρτών», δηλαδή SIM κάρτες, θα μπορούσε να αποτελέσει μια διέξοδο στο ζήτημα της εξάπλωσης της χρήσης αναγνωστών έξυπνων καρτών. Τα πρότυπα για ασφαλείς αναγνώστες «smart – card» (CEN/ISSS FINREAD) προβλέπουν την ύπαρξη ξεχωριστού πληκτρολογίου (numeric pad) και οθόνης για τους αναγνώστες καρτών, και τα κινητά τηλέφωνα μπορούν να αποτελέσουν έτσι ένα μέσο για την εξάπλωση της χρήσης ηλεκτρονικών υπογραφών.

Στα κράτη - μέλη της Ευρωπαϊκής Ένωσης αναπτύσσονται σε εθνικό επίπεδο αρκετές άλλες εφαρμογές που σχετίζονται με τις ηλεκτρονικές υπογραφές. Κάποιες από τις εφαρμογές σε επίπεδο κρατών - μελών παρουσιάζονται στην συνέχεια[88].

Στην Ιταλία, έχοντας ξεκινήσει την θεσμοθέτηση της χρήσης των ηλεκτρονικών υπογραφών ειδικά για την Δημόσια Διοίκηση από το 1997 υπό την εποπτεία τότε της AIPA (Autorita per l' Informatica nella Publica Amministrazione) και πρόσφατα του CNIPA (www.cnpa.it - 'Centro Nationale per l' Informatica nella Publica Amministrazione) έχουν καταφέρει να έχουν ευρύτατη χρήση και αποδοχή (υπογεγραμμένων) ηλεκτρονικών εγγράφων στις δημόσιες υπηρεσίες τους. Σ' αυτό βοήθησε ο καθορισμός συγκεκριμένου τύπου ηλεκτρονικών υπογραφών που χρησιμοποιούνται αποκλειστικά για την υπογραφή ηλεκτρονικών έγγραφων («Firme Sicure») και η θέσπιση αυστηρών κανόνων για την διαλειτουργικότητα των σχετικών πιστοποιητικών που εκδίδουν οι «εγγεγραμμένοι ΠΥΠ» στο μητρώο του CNIPA , γεγονός που οδήγησε και στην ανάπτυξη εφαρμογών λογισμικού για την δημιουργία και επαλήθευση ηλεκτρονικών υπογραφών το οποίο λειτουργεί με τα πιστοποιητικά όλων των ΠΥΠ της Ιταλίας, βάσει των κοινών προδιαγραφών.

Στην Γερμανία, όπου υπήρχε «αυστηρή» νομοθεσία για την αποδοχή των ηλεκτρονικών υπογραφών από το 1997, προσφέρεται και χρησιμοποιείται από την δημόσια διοίκηση ένας ακόμη πιο «βελτιωμένος» σε σχέση με τις «αναγνωρισμένες ηλεκτρονικές υπογραφές» του άρθρου 5§1 της Οδηγίας 99/93/ΕΚ, τύπος ηλεκτρονικών υπογραφών (οι αποκαλούμενες «enhanced signatures») οι οποίες παρέχονται μόνο από τους «εθελοντικά διαπιστευμένους ΠΥΠ» («accredited CAs») και προβλέπουν την υποχρεωτική χρήση «χρονοσήμανσης» (timestamping) στα υπογεγραμμένα ηλεκτρονικά έγγραφα, ώστε αυτά να μπορούν να εξετασθούν για την εγκυρότητά τους και μετά από την λήξη του πιστοποιητικού που υποστήριξε την ηλεκτρονική υπογραφή τους. Μάλιστα, η αρμόδια εθνική αρχή «Regulierungsbehφrde fór Telekommunikation und Post» (RegTP) έχει προχωρήσει στην «διαπίστωση» και στην δημοσίευση της συμμόρφωσης συγκεκριμένων «προϊόντων ηλεκτρονικών υπογραφών» (συσκευές / φορείς ιδιωτικών κλειδιών, αυτόνομα ή πρόσθετα προγράμματα (plug-ins) δημιουργίας και επαλήθευσης ηλεκτρονικών υπογραφών, βιβλιοθήκες σχετικών «ρουτινών», αναγνώστες καρτών, κ.λ.π.) με αυστηρές προδιαγραφές.

Στην Εσθονία, σε συνδυασμό με την «ηλεκτρονική ταυτότητα» που εκδίδεται υποχρεωτικά προς όλους τους πολίτες της και η οποία ενσωματώνει πιστοποιητικά ηλεκτρονικής υπογραφής, έχουν προχωρήσει στο σχεδιασμό ενός ολοκληρωμένου συστήματος ηλεκτρονικής ταυτοποίησης και υπογραφής εγγράφων (επονομαζόμενο «DigiDoc»), τόσο για

[87] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 33 - 34, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Paradoteo_E2-Teliko.doc (ημερομηνία επίσκεψης: 15/05/2011)

[88] Ο.π, σελ. 34 – 35.

χρήση του μεταξύ των υπαλλήλων της Δημόσιας Διοίκησης, όσο και μεταξύ αυτών και των πολιτών. Χαρακτηριστικά της εφαρμογής τους είναι η δυνατότητα ταυτόχρονης ενσωμάτωσης πληροφοριών επαλήθευσης των πιστοποιητικών και χρονοσήμανσης της υπογραφής στο υπογεγραμμένο έγγραφο, (όπως στις «enchanced signatures» της Γερμανίας), καθώς και η απόδοση μιας σταθερής, αλλά «εικονικής» διεύθυνσης ηλεκτρονικού ταχυδρομείου, για κάθε πολίτη και δημόσιο υπάλληλο. Με την χρήση αυτής της «εικονικής» διεύθυνσης, μπορούν να στέλνουν και να λαμβάνουν υπογεγραμμένα και κρυπτογραφημένα μηνύματα από την εκάστοτε πραγματική διεύθυνση ηλεκτρονικού ταχυδρομείου τους την οποία διασύνδεουν με αυτή.

Στη Γαλλία, αναφέρθηκε ότι έχει ολοκληρωθεί εφαρμογή με την οποία οι δικηγόροι μπορούν ήδη να καταθέτουν ηλεκτρονικά κάποιους τύπους δικογράφων προς την υπηρεσίες συγκεκριμένων δικαστηρίων, με την χρήση της ηλεκτρονικής υπογραφής τους.

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 Αξιών Αθηνών (ΧΑΑ) 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[89]:

- «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.

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[90].

[89] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 13 - 14, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[90] Ο.π., σελ. 14.

3.6.7 Άλλες Μέθοδοι Προστασίας

Βλέπουμε ότι η ραγδαία εξάπλωση και η ευρύτατη διείσδυση του Διαδικτύου σε όλους τους τομείς της κοινωνικής δραστηριότητας έχει ως αποτέλεσμα την ανάπτυξη πολλών μηχανισμών, οι οποίοι έχουν ως στόχο και σκοπό τους να διαφυλάξουν την ασφάλεια και την εμπιστευτικότητα των ηλεκτρονικών συναλλαγών και την κατοχύρωση των πνευματικών δικαιωμάτων σε όλα τα διακινούμενα ψηφιακά αντικείμενα. Προς την κατεύθυνση αυτή, εκτός από τις ψηφιακές υπογραφές και την κρυπτογραφία, έχουμε και άλλες μεθόδους προστασίας των ηλεκτρονικών εγγράφων και συναλλαγών, τέτοιες μέθοδοι είναι εκείνη της στενογραφίας και της υδατογράφησης. Κρίθηκε λοιπόν απαραίτητη, για την αποφυγή συγχύσεων η συνοπτική παράθεση των τεχνικών αυτών, και η αποσαφήνιση πιθανών μεταξύ τους διαφορών.

Η στενογραφία επιτρέπει θα μπορούσαμε να πούμε, την κρυφή επικοινωνία. Αυτό το πετυχαίνει συνήθως κρύβοντας τις πληροφορίες σε άλλα δεδομένα υπεράνω υποψίας. Η στενογραφία 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 σε έναν μη εξουσιοδοτημένο να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει ή ακόμα και να αλλοιώσει την πληροφορία, ο στόχος της στενογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη «αθώα» ή ουδέτερη πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια σε κάποιον μη εξουσιοδοτημένο να ανιχνεύσει την ύπαρξή της.

Μπορούμε να πούμε ότι η στενογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντας την μέσα σε κάποιο «στεγανό». Η κρυπτογραφία αντίθετα, 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) τέλος, 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 έως αδύνατο να καταστραφεί το ένθετο υδατογράφημα, οπότε με τον τρόπο αυτό παρέχεται ασφάλεια με την μέθοδο της υδατογράφησης.

3.6.8 Περιορισμοί στη διακίνηση Κρυπτογραφικού Υλικού

Οι περιορισμοί που υπάρχουν στην διεθνή διακίνηση ισχυρών κρυπτογραφικών συστημάτων είναι ένα ζήτημα που σχετίζεται άμεσα με τη χρήση της κρυπτογραφίας. Οι περιορισμοί αυτοί θα μπορούσαμε να πούμε ότι αποτελούν τροχοπέδη στην απρόσκοπτη διακίνηση και χρήση δυνατής κρυπτογραφίας στις ηλεκτρονικές συναλλαγές. Η δικαιολογία που χρησιμοποιείται διεθνώς για την ύπαρξη αυτών των περιορισμών είναι το επιχείρημα ότι η κρυπτογραφία μπορεί να χρησιμοποιηθεί για την κατασκευή ισχυρών οπλικών συστημάτων και έτσι θεωρείται πιθανό εργαλείο εγκληματιών και τρομοκρατών σε εθνικό και διεθνή επίπεδο.

Οι περιορισμοί στη διακίνηση κρυπτογραφικής τεχνολογίας έχουν θεσπιστεί διεθνώς στο πλαίσιο του συμφώνου Wassenaar για τους ελέγχους σε εξαγωγές συμβατικών όπλων, αγαθών και τεχνολογιών διπλής χρήσης, δηλαδή τόσο για πολιτικούς σκοπούς, όπως οι συνήθεις ηλεκτρονικές συναλλαγές, όσο και για στρατιωτικούς όπως η κατασκευή όπλων. Σε αυτό το σύμφωνο μπορούν να μετέχουν όσες χώρες το επιθυμούν. Η Ευρωπαϊκή Ένωση στο πλαίσιο του ανώτερου συμφώνου υιοθέτησε και αυτή αυστηρούς ελέγχους στην εξαγωγή κρυπτογραφικού υλικού, θεσπίζοντας για πρώτη φορά σχετικό Κανονισμό το 1994. Κατά τη διάρκεια των επόμενων ετών εφάρμοσε πιο χαλαρή και αυτόνομη ευρωπαϊκή πολιτική σε ζητήματα κρυπτογραφίας. Η Ευρωπαϊκή Επιτροπή δημοσίευσε τον Οκτώβριο του 1997 ανοικτή επιστολή προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο Υπουργών, η οποία μεταξύ άλλων

καλούσε τα κράτη-μέλη να υποστηρίξουν τη χαλάρωση των περιορισμών της συμφωνίας Wassenaar και να μην υιοθετήσουν κανέναν νέο περιορισμό[91].

Είναι κάτι περισσότερο από προφανές ότι η οποιαδήποτε παρεμπόδιση της διακίνησης της κρυπτογραφίας, με οποιονδήποτε τρόπο ή μορφή πραγματοποιείται, συνεπάγεται αναπόφευκτα την παρεμπόδιση της δημιουργίας ενός ασφαλούς περιβάλλοντος μέσα στο οποίο ο κάθε χρήστης θα μπορεί να πραγματοποιεί τις ηλεκτρονικές του συναλλαγές με εμπιστευτικότητα και ασφάλεια, καταλήγοντας με αυτόν τον τρόπο σε ουσιαστική αδυναμία μιας αποτελεσματικής προστασίας του συναλλασσόμενου – χρήστη στις ηλεκτρονικές του συναλλαγές.

3.7 Ηλεκτρονική Υπογραφή - Βιομετρική Υπογραφή

3.7.1 Εισαγωγή

Η Βιομετρία είναι ο επιστημονικός κλάδος που χρησιμοποιεί ένα μοναδικό και μετρήσιμο βιολογικό χαρακτηριστικό ή μια συνήθεια ενός ατόμου προκειμένου να ελέγξει ή να πιστοποιήσει την ταυτότητα του, ενώ Βιομετρική αποτελεί τον επιστημονικό κλάδο ο οποίος ασχολείται με την μέτρηση των φυσικών χαρακτηριστικών ενός ατόμου και αναλύει στατιστικά τα βιολογικά χαρακτηριστικά του ατόμου. Η βιομετρική τεχνολογία έχει ως κύριος στόχο της την ανάπτυξη μεθόδων και συνθημάτων τα οποία να πιστοποιούν την ταυτότητα των προσώπων, μέσα από τις μεθόδους αυτές θα πραγματοποιείται αυτόματος έλεγχος της ταυτότητας, δηλαδή την αναγνώριση ενός ανθρώπινου χαρακτηριστικού μέσα σε ελάχιστα δευτερόλεπτα. Τα πιο σημαντικά φυσικά - βιομετρικά χαρακτηριστικά του ανθρώπινου σώματος που επιδέχονται έλεγχο και μετρώνται με βιομετρικές τεχνικές είναι η ίριδα (αναγνώριση της ίριδας), ο αμφιβληστροειδής στο μάτι, το πρόσωπο (γεωμετρία του προσώπου), το δάκτυλο (δακτυλικά αποτυπώματα) και το χέρι (γεωμετρία του χεριού). Ενώ συνήθη μετρήσιμα βιομετρικά χαρακτηριστικά συμπεριφοράς που μετρώνται με συμπεριφορικές βιομετρικές συμπεριφορές, είναι η φωνή (επιβεβαίωση φωνής), ο ρυθμός δυναμικής πληκτρολόγησης και η επιβεβαίωση χειρόγραφης υπογραφής.

Βιομετρικά στοιχεία είναι ένας γενικός όρος που χρησιμοποιείται εναλλακτικά για να περιγράψει ένα χαρακτηριστικό ή μια διαδικασία. Ως χαρακτηριστικό εννοούμε ότι ένα βιομετρικό στοιχείο είναι μετρήσιμο βιολογικά (ανατομικά και φυσιολογικά) και τα συμπεριφορικά χαρακτηριστικά του μπορούν να χρησιμοποιηθούν για την αυτόματη αναγνώριση. Ως διαδικασία εννοούμε ένα βιομετρικό στοιχείο ως μια αυτοματοποιημένη μέθοδο της αναγνώρισης ενός ατόμου, βάση των μετρήσιμων βιολογικών (ανατομικών και φυσιολογικών) και συμπεριφορικών χαρακτηριστικών του.

Στη βιομηχανία των συστημάτων ασφάλειας η βιομετρική υπογραφή ενός προσώπου θεωρείται ότι παρέχει το υψηλότερο επίπεδο ασφάλειας στις ηλεκτρονικές συναλλαγές. Αυτά πάντα σε σχέση με τη γενικά αποδεκτή διαβάθμιση ασφάλειας των μεθόδων πιστοποίησης της ταυτότητας ενός προσώπου[92]:

- Πρώτο επίπεδο (χαμηλή ασφάλεια) : η ταυτότητα του συναλλασσομένου πιστοποιείται με κάτι το οποίο έχει, όπως μια ταυτότητα με φωτογραφία.
- Δεύτερο επίπεδο (μέση ασφάλεια) : η ταυτότητα του συναλλασσομένου πιστοποιείται με κάτι το οποίο γνωρίζει, όπως μια λέξι-κλειδί ή το PIN.
- Τρίτο επίπεδο (υψηλή ασφάλεια) : η ταυτότητα του συναλλασσομένου πιστοποιείται χάρη σε ένα χαρακτηριστικό του σώματός του, όπως το δακτυλικό αποτύπωμα ή χάρη στον ιδιαίτερο τρόπο με τον οποίο εκτελεί μια συγκεκριμένη ενέργεια, όπως ο ρυθμός πληκτρολόγησης.

[91] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 57 - 60.
[92] Καραδημητρίου, ο.π, σελ. 64 - 65.

Ένα πολύ σημαντικό πλεονέκτημα των βιομετρικών χαρακτηριστικών είναι ότι ένας προσωπικός αριθμός αναγνώρισης PIN ή ένα ιδιωτικό κλειδί κρυπτογραφίας προσφέρουν περιορισμένη ασφάλεια και δεν είναι αξιόπιστα καθώς, μπορεί να ξεχαστούν, να χαθούν ή να κλαπούν, τα βιομετρικά χαρακτηριστικά δεν μπορεί να ξεχαστούν, να χαθούν ή να κλαπούν καθώς είναι φυσικά χαρακτηριστικά ενός ατόμου και έχουν την ιδιότητα να είναι μοναδικά. Επίσης, είναι πολύ σημαντικό να αναφέρουμε ότι ο τεχνολογικός συνδυασμός μιας βιομετρικής ηλεκτρονικής υπογραφής με έναν προσωπικό αριθμό αναγνώρισης PIN ή με μια ηλεκτρονική υπογραφή, η οποία βασίζεται στην ασύμμετρη τριμερή κρυπτογραφία, θα μπορούσε να προσφέρει στον υπογράφοντα τη μέγιστη δυνατή ασφάλεια και εμπιστευτικότητα κατά τις ηλεκτρονικές του συναλλαγές και κατά τη διακίνηση ηλεκτρονικών εγγραφών στο Διαδίκτυο.

Όλα τα βιομετρικά συστήματα λειτουργούν περίπου με τον ίδιο τρόπο, είναι ουσιαστικά συστήματα αναγνώρισης προτύπων που λειτουργούν με την απόκτηση των βιομετρικών δεδομένων από ένα άτομο και την σύγκριση των δεδομένων αυτών με το υπάρχον πρότυπο στην βάση δεδομένων. Για να πραγματοποιηθεί η πιο πάνω διαδικασία, το σύστημα καταγράφει ένα δείγμα βιομετρικού χαρακτηριστικού, η διαδικασία αυτή ονομάζεται «διαδικασία εκμάθησης», κατά την διάρκεια αυτής της διαδικασίας ορισμένα συστήματα μπορεί να χρειαστούν πολλαπλά δείγματα για να καταγράψουν πλήρως το χαρακτηριστικό. Το Βιομετρικό σύστημα μπορεί να λειτουργεί είτε για να επιβεβαιώσει την ταυτότητα του ατόμου είτε για να εξακριβώσει των ταυτότητα του ατόμου.

Στην συνέχεια της διαδικασίας, εξάγονται τα μοναδικά γνωρίσματα του βιομετρικού χαρακτηριστικού και μετατρέπονται από το σύστημα σε μαθηματικό κώδικα, ο οποίος αποθηκεύεται στο βιομετρικό πρότυπο του συγκεκριμένου ατόμου. Το πρότυπο αυτό μπορεί να βρίσκεται αποθηκευμένο στο ίδιο το βιομετρικό σύστημα ή σε οποιαδήποτε μορφή μνήμης π.χ. σε «έξυπνη» κάρτα. Κατά την λειτουργία της επιβεβαίωσης της ταυτότητας του χρήστη, το σύστημα επικυρώνει την ταυτότητα ενός ατόμου από την σύγκριση των βιομετρικών δεδομένων, με το δικό της βιομετρικό πρότυπο το οποίο είναι αποθηκευμένο στην βάση δεδομένων του συστήματος.

Στην λειτουργία εξακρίβωσης ταυτότητας χρήστη το σύστημα αναγνωρίζει ένα άτομο αναζητώντας τα πρότυπα όλων των χρηστών στην βάση δεδομένων για μια αντιστοίχηση. Ως εκ τούτου το σύστημα διεξάγει μια σύγκριση σε ένα προς όλους, για την εξακρίβωση της ταυτότητας ενός ατόμου ή αποτυγχάνει εάν το πρότυπο δεν είναι εγγεγραμμένο στην βάση του συστήματος. Η εξακρίβωση ταυτότητας χρήστη είναι ένα κρίσιμο συστατικό σε εφαρμογές που χρησιμοποιούν αρνητική αναγνώριση, όπου αποτρέπει ένα μόνο πρόσωπο από την χρήση πολλαπλών ταυτοτήτων. Επίσης χρησιμοποιεί την θετική αναγνώριση για λόγους ευκολίας (ο χρήστης δεν υποχρεούται να υποβάλει αίτηση για ταυτότητα). Οι παραδοσιακές μέθοδοι προσωπικής αναγνώρισης όπως είναι οι κωδικοί πρόσβασης, τα PINs, και τα keys tokens μπορούν να λειτουργήσουν για την θετική αναγνώριση, ενώ η αρνητική αναγνώριση μπορεί να επιτευχθεί μόνο μέσα από την χρήση βιομετρικών στοιχείων.

Το βιομετρικό σύστημα μπορεί να χρειάζεται και μια σκανδάλη ή ένα τρόπο σύνδεσης του ατόμου με το βιομετρικό πρότυπο, όπως πληκτρολόγηση ενός PIN. Ο έλεγχος της ταυτότητας του χρήστη από το βιομετρικό σύστημα πραγματοποιείται με σύγκριση του δείγματος του χρήστη με το πρότυπο. Αν το πρότυπο και το νέο δείγμα ταιριάξουν, τότε αναγνωρίζεται η ταυτότητα του χρήστη. Μπορούμε να πούμε λοιπόν, ότι η διαδικασία λειτουργίας των βιομετρικών συστημάτων ηλεκτρονικής υπογραφής περιλαμβάνει τέσσερα στάδια[93]:

1. Καταγραφή δείγματος κατά τη διάρκεια της εκμάθησης.
2. Εξαγωγή μοναδικών γνωρισμάτων και δημιουργία προτύπου.
3. Σύγκριση του προτύπου με το νέο δείγμα.
4. Αποδοχή ή μη αποδοχή του νέου δείγματος.

Είναι πολύ πιθανό τα φυσικά - βιομετρικά χαρακτηριστικά ενός ατόμου και η συμπεριφορά του να αλλάξουν με το πέρασμα του χρόνου, υπάρχει λοιπόν η ανάγκη ένα βιομετρικό σύστημα προκείμενου να είναι αξιόπιστο και ευέλικτο να έχει την δυνατότητα να

[93] Καραδημητρίου, ο.π., σελ. 66.

αποδέχεται αυτές τις όποιες αλλαγές προκύπτουν. Υπάρχουν κάποια προκαθορισμένα όρια στην απόκλιση του δείγματος ενός βιομετρικού χαρακτηριστικού από το αρχικό πρότυπο, αυτά τα όρια δεν πρέπει σε καμία περίπτωση να ξεπεραστούν προκειμένου να γίνει αποδεκτή η μέτρηση. Εάν το δείγμα που εξετάζεται την εκάστοτε φορά και το αρχικό πρότυπο είναι αρκούντος παραπλήσιας, τότε και μόνο τότε το βιομετρικό σύστημα θα συμπεράνει ότι αυτά πράγματι ταιριάζουν και τελικά θα αναγνωρίσει την ταυτότητα του προς εξέταση ατόμου, σε διαφορετική περίπτωση το αποτέλεσμα θα είναι αρνητικό.

Τα χαρακτηριστικά που χρησιμοποιούνται σήμερα για βιομετρικούς σκοπούς ή είναι ακόμα στο στάδιο της έρευνας περιλαμβάνουν την μυρωδιά του σώματος, το DNA, το σχήμα του αυτιού, το θερμικό διάγραμμα του προσώπου, τη δύναμη με την οποία κάποιος γράφοντας πιέζει το στυλό στο χαρτί, την ταχύτητα της πληκτρολόγησης, το αποτύπωμα της παλάμης, το σχέδιο του αμφιβληστροειδούς χιτώνα του ματιού, το σχέδιο της ίριδας ή των φλεβών και τον τόνο της φωνής[94].

3.7.2 Συνηθέστεροι τρόποι Βιομετρικής Υπογραφής και Εφαρμογές τους[95]

Ένας αριθμός βιομετρικών χαρακτηριστικών υπάρχει και χρησιμοποιείται σε διάφορες εφαρμογές. Κάθε βιομετρικό στοιχείο έχει δυνατά και αδύνατα σημεία, και η επιλογή εξαρτάται από την εφαρμογή κάθε φορά. Δεν υπάρχει κάποιο βιομετρικό στοιχείο, που αναμένεται να ανταποκριθεί αποτελεσματικά στις απαιτήσεις του συνόλου των αιτήσεων, με άλλα λόγια δεν είναι βιομετρικά ιδανικό.

1. Δακτυλικό αποτύπωμα

Η αναγνώριση δακτυλικών αποτυπωμάτων είναι ένα από τα πιο γνωστά και διάσημα βιομετρικά στοιχεία. Λόγω της μοναδικότητας και της αντοχής τους με την πάροδο του χρόνου, τα δακτυλικά αποτυπώματα χρησιμοποιούνται για αναγνώριση για πάνω από έναν αιώνα. Μέσο της δυνατότητας αξιοποίησης υπολογιστικών και τεχνολογικών μεθόδων, η αναγνώριση δακτυλικών αποτυπωμάτων έχει αυτοματοποιηθεί. Η μέθοδος της σάρωσης του δακτυλικού αποτυπώματος έχει διαδοθεί τόσο πολύ, ώστε φαίνεται πως θα είναι μια από τις βιομετρικές τεχνολογίες που θα χρησιμοποιηθούν ευρύτατα στο μέλλον για να υπογράφουν ηλεκτρονικά οι συναλλασσόμενοι. Συσκευές σάρωσης αποτυπωμάτων έχουν εγκατασταθεί ήδη σε κρατικές υπηρεσίες, ιδιωτικές εγκαταστάσεις, μηχανήματα ανάληψης χρημάτων από τράπεζες ακόμα και σε Η/Υ. Ο συναλλασσόμενος έχει την δυνατότητα τη στιγμή που με ένα απλό κλικ του ποντικιού του να αγοράζει αγαθά και υπηρεσίες από ηλεκτρονικό κατάστημα, ταυτόχρονα να υπογράφει ηλεκτρονικά με το δακτυλικό του αποτύπωμα, εξασφαλίζοντας έτσι την μεγαλύτερη δυνατή ασφάλεια της συναλλαγής και ταυτόχρονα πιστοποιεί άμεσα την ταυτότητά του.

Τα πλεονεκτήματα της χρήσης του δακτυλικού αποτυπώματος είναι κυρίως η ευκολία του και η αξιοπιστία του. Απαιτείτε ελάχιστος χρόνος και κόπος για να αποθηκευτεί ένα αποτύπωμα. Επίσης, η πιστοποίηση της γνησιότητας του αποτυπώματος είναι γρήγορη και αξιόπιστη. Σημαντικά όμως είναι και τα μειονέκτημα της διαδικασίας αυτής, το πιο σημαντικό μειονέκτημα είναι η δυνατότητα αντιγραφής του ίχνους του δακτυλικού αποτυπώματος που μένει πάνω στο γυαλί του σαρωτή. Επίσης, ένα άλλο μειονέκτημα είναι να μην λειτουργήσει σωστά, όταν οι άκρες των δακτύλων του χρήστη είναι βρώμικες ή ο χρήστης πιέζει το δάκτυλο του στο γυαλί του σαρωτή με πολύ δύναμη. Τέλος, ο νόμιμος χρήστης του συστήματος μπορεί να αναγκαστεί από άλλο πρόσωπο να πιέσει το δακτυλικό του αποτύπωμα πάνω στον σαρωτή.

2. Γεωμετρία χεριού

Τα συστήματα γεωμετρίας χειρός βασίζονται σε μια σειρά από μετρήσεις που λαμβάνονται από το ανθρώπινο χέρι ,από το σχήμα, το μέγεθος της παλάμης καθώς και από τα μήκη και πλάτη των δακτύλων. Η μέθοδος αυτή αναπτύχθηκε κυρίως για να ξεπεραστεί η ανεπάρκεια που παρουσιάζει η μέθοδος του δακτυλικού αποτυπώματος. Μια συσκευή σάρωσης του αποτυπώματος της παλάμης πρέπει να εξετάζει τόσο την επάνω όψη όσο και τις πλαϊνές όψεις

[94] Καραδημητρίου, ο.π., σελ. 66.
[95] Καραδημητρίου, ο.π., σελ. 67 - 75.

του χεριού, χρησιμοποιώντας ενσωματωμένη βιντεοκάμερα. Συσκευές ανίχνευσης γεωμετρίας του χεριού βρίσκονται σε κοινοβούλια, αεροδρόμια, νοσοκομεία. Τα πλεονέκτημα της μεθόδου αυτής είναι ίδια με τα πλεονέκτημα της μεθόδου του δακτυλικού αποτυπώματος. Σημαντικό μειονέκτημα είναι ότι οι σαρωτές παλάμης απαιτούν περισσότερο χώρα προκειμένου να τοποθετηθούν και για τον λόγο αυτό δεν είναι τόσο διαδεδομένη η χρήση τους.

3. Σχέδιο ίριδας

Το πλεονέκτημα ενός σαρωτή της ίριδας του ματιού είναι ότι δεν απαιτεί από τον χρήστη να εστιάσει το βλέμμα του σε συγκεκριμένο σημείο, επειδή τα σημάδια της ίριδας είναι απλωμένα στην επιφάνεια του ματιού. Επίσης, η σάρωση της ίριδας μπορεί να γίνει και από απόσταση μερικών μέτρων, η μέθοδος αυτή λειτουργεί και σε χρήστες μειωμένης όρασης και η μόνο προϋπόθεση είναι η ίριδα τουλάχιστον του ενός ματιού να είναι άθικτη.

Η τεχνολογία της σάρωσης της ίριδας έχει και μειονεκτήματα. Ένα πολύ σημαντικό μειονέκτημα είναι το αυξημένο κόστος του σαρωτή. Επίσης, υπάρχει ο κίνδυνος εξαπάτησης του σαρωτή με την παρουσίαση μιας άριστης ποιότητας φωτογραφίας της ίριδας του ματιού ενός προσώπου, αντί της παρουσίασης του ίδιου του προσώπου.

4. Σχέδιο αμφιβληστροειδούς

Ο τρόπος με τον οποίο λειτουργεί η σάρωση του αμφιβληστροειδούς χιτώνα του ματιού γίνεται με μια χαμηλής ισχύος υπέρυθρη δέσμη φωτός μέσω της κόρης του ματιού, στο πλέγμα των αιμοφόρων αγγείων στο πίσω μέρα του ματιού. Οι πιο πολλές χρήσεις αυτής της βιομετρικής ηλεκτρονικής υπογραφής συναντώνται σε σημεία έλεγχου πρόσβασης σε εγκαταστάσεις υψίστης ασφάλειας, γιατί εξασφαλίζουν πολύ χαμηλά ποσοστά λανθασμένης απόρριψης και σχεδόν μηδενικό ποσοστό λανθασμένης αποδοχής. Ωστόσο η τεχνολογική αυτή εφαρμογή επηρεάζεται από παθήσεις όπως καταρράκτης ή γλαύκωμα και αυτό γιατί η σάρωση του αμφιβληστροειδούς απαιτεί καθαρή εικόνα του πίσω μέρους του ματιού.

5. Δείγμα φωνής

Η μέθοδος αυτή εφαρμόζεται με την προφορά μιας συγκεκριμένης φράσης από το χρήστη σε μικροφωνική ή τηλεφωνική βιομετρική συσκευή, η οποία καταγράφει χαρακτηριστικά της φωνής διαφορετικά από αυτά στα οποία εστιάζεται η ανθρώπινη ακοή, οπότε είναι δύσκολο να εξαπατηθεί η βιομετρική συσκευή από μια μίμηση της φωνής του νόμιμου χρήστη. Μπορούμε να πούμε όμως ότι το δείγμα φωνής δεν θεωρείται τόσο αξιόπιστο όσο άλλες βιομετρικές τεχνικές. Αφενός γιατί δεν λειτουργεί σωστά όταν υπάρχουν εξωτερικοί θόρυβοι κατά την προφορά της φράσης-κλειδί από το χρήστη και αφετέρου γιατί ένας χρήστης ηλικιωμένος ή κρυολογημένος ή βραχνιασμένος συχνά αντιμετωπίζει πρόβλημα αφού η χροιά της φωνής του έχει υποστεί μεταβολές. Επίσης, είναι πολύ εύκολο κάποιος να εξαπατήσει την συσκευή αναγνώρισης φωνής, εάν μαγνητοφωνήσει την φράση-κλειδί που προφέρει ο χρήσης. Για τους πιο πάνω λόγους η μέθοδος αυτή χρησιμοποιείται κυρίως σε εγκαταστάσεις μεσαίου επιπέδου ασφάλειας και όχι υψηλού.

6. Χαρακτηριστικά προσώπου

Η βιομετρική ηλεκτρονική υπογραφή μέσω των χαρακτηριστικών του προσώπου πλησιάζει πολύ στο φυσικό τρόπο με τον οποίο οι άνθρωποι αναγνωρίζουν ο ένας τον άλλο, γεγονός που βοηθά στο να θεωρείται γενικά η μέθοδος αυτή ότι δεν προσβάλλει την προσωπικότητα του χρήστη. Η τεχνική αυτή ευνοείται από την ανάπτυξη κλειστών κυκλωμάτων παρακολούθησης και από την ανάπτυξη των τεχνολογιών βίντεο και είναι πολύ αποτελεσματική σε περιπτώσεις σάρωσης αιθουσών αεροδρομίου για πιθανούς τρομοκράτες.

Το σημαντικότερο μειονέκτημα της τεχνικής αυτής είναι ότι το ανθρώπινο πρόσωπο αλλάζει λόγω ηλικίας ή και με τεχνητούς τρόπους, με αποτέλεσμα να κάνει τους ερευνητές αυτής της μεθόδου να επικεντρώνονται στη μέτρηση της ακριβούς θέσης πάνω το πρόσωπο σταθερών χαρακτηριστικών όπως είναι τα μάτια, η μύτη, το στόμα και τα αυτιά.

7. Ρυθμός πληκτρολόγησης

Η τεχνική αυτή ελέγχει τον ρυθμό με τον οποίο ο χρήστης πληκτρολογεί κάτι σε τερματικό Η/Υ παρακολουθώντας το πληκτρολόγιο ανά χιλιοστό του δευτερολέπτου. Το πλεονέκτημα αυτής

της βιομετρικής υπογραφής είναι ότι η διαδικασία αναγνώρισης του χρήστη δεν διαφοροποιείται από την καθημερινή ρουτίνα όταν ο χρήστης βρίσκεται σε περιβάλλον όπου υπάρχουν Η/Υ. Ωστόσο, η εφαρμογή της μεθόδου αυτής έχει αποτύχει πρώτον γιατί έχει πολύ μεγάλο κόστος αλλά και γιατί δεν είναι εύκολο ο χρήστης της μεθόδου αυτής να διατηρεί δια βίου στις συναλλαγές του τον ίδιο ρυθμό πληκτρολόγησης.

8. Ηλεκτρονική καταγραφή της χειρόγραφης υπογραφής

Η ηλεκτρονική καταγραφή της χειρόγραφης υπογραφής είναι αρκετά συνηθισμένη ως υποκατάστατο της παραδοσιακής υπογραφής. Οι συσκευές ηλεκτρονικής καταγραφής της υπογραφής χρησιμοποιούν ηλεκτρονικά στυλό, επιφάνειες ευαίσθητες σε πίεση ή συνδυασμό των δυο, είναι οικονομικές αλλά έχουν και μικρή διάρκεια ζωής. Πολλές τράπεζες αποφεύγουν να χρησιμοποιούν αυτή την μέθοδο για τη διακρίβωση της γνησιότητας της υπογραφής σε πιστωτικές κάρτες και επιταγές, επειδή η υπογραφή πλαστογραφείται σχετικά εύκολα. Αυτό αποτελεί εμπόδιο για τη χρήση της συγκεκριμένης μεθόδου σε συναλλαγές οπού απαιτείται υψηλή ασφάλεια, αντίθετα η μέθοδος είναι συνηθισμένη σε απλές συναλλαγές όπως η παράδοση αλληλογραφίας από εταιρίες courier.

3.8 Ηλεκτρονική Υπογραφή και «Έξυπνες» Κάρτες

Προκείμενου ο υπογραφών ηλεκτρονικά να επωφελείται από όλες τις προαναφερθείσες τεχνολογικές εφαρμογές της ηλεκτρονικής υπογραφής χρειάζεται να την έχει αποθηκευμένη σε ένα μέσο εύχρηστο, ελαφρύ και οικονομικό ως προς την κατασκευή του, το οποίο θα μπορεί να το έχει συνέχεια μαζί του προκειμένου να πραγματοποιεί τις ηλεκτρονικές συναλλαγές του. Αυτό το μέσω αποθήκευσης της ηλεκτρονικής υπογραφής το οποίο φαίνεται να είναι το πλέον κατάλληλο είναι οι «έξυπνες» κάρτες (smart cards)[96]. Με την «έξυπνη κάρτα» ουσιαστικά, η ηλεκτρονικά αποθηκευμένη στην κάρτα αξία αγοράζεται από τον χρήστη και μειώνεται μετά από κάθε χρήση της κάρτα, για την πραγματοποίηση πληρωμών. Πέρα από την έξυπνη κάρτα «μέσο αποθήκευσης» μπορεί να είναι και η μνήμη ενός ηλεκτρονικού υπολογιστή. Πρόκειται για μορφές του λεγομένου «ηλεκτρονικού χρήματος» σε αυτήν την κατηγορία υπάγονται και οι προπληρωμένες κάρτες πολλαπλών χρήσεων (e-purse – ηλεκτρονικό πορτοφόλι) και τα προπληρωμένα προϊόντα λογισμικού, εγκατεστημένα στη μνήμη ηλεκτρονικού υπολογιστή συνδεδεμένου με το διαδίκτυο (digital cash – ψηφιακά μετρητά)[97].

Οι «έξυπνες» κάρτες είναι μικροσκοπικοί Η/Υ που έχουν το μέγεθος και το σχήμα μιας πιστωτικής κάρτας, επάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο ηλεκτρονικό κύκλωμα (chip) που περιέχει αποθηκευμένη την ηλεκτρονική υπογραφή. Ο χρήστης της κάρτας διαθέτει και έναν προσωπικό κωδικό αριθμό για μεγαλύτερη ασφάλεια[98]. Ο συνδυασμό κωδικών πρόσβασης και έξυπνης κάρτας κερδίζει έδαφος, καθώς οι περισσότεροι κατασκευαστές περιφερειακών (πληκτρολόγιων κλπ.) ενσωματώνουν αναγνώστες στα προϊόντα τους. Το ίδιο συμβαίνει και με τις συσκευές αναγνώρισης αποτυπωμάτων, καθώς όσο ασφαλής και αν είναι η smart card σε σχέση με το ψηφιακό πιστοποιητικό εγκυμονεί τον κίνδυνο απώλειας ή κλοπής κάτι που δεν συμβαίνει με τα ανθρώπινα αποτυπώματα ή την ίριδα του ματιού[99].

Κύρια γνωρίσματα των «έξυπνων» καρτών είναι η ικανότητα να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ασφαλή τρόπο. Σημαντικά πλεονεκτήματα τους είναι ότι δεν απομαγνητίζονται με την πάροδο του χρόνου παρέχοντας έτσι αυξημένη προστασία στα δεδομένα που περιέχουν, δεν αντιγράφονται, έχουν φορητότητα, είναι εύχρηστες και οικονομικές στην κατασκευή και το πλέον σημαντικό πλεονέκτημά τους είναι η ικανότητά τους να αποθηκεύουν το ιδιωτικό κλειδί της ψηφιακής υπογραφής του χρήστη της κάρτας, έτσι ώστε να διασφαλίζονται τα μοναδικά πλεονεκτήματα που προσφέρει η χρήση του ιδιωτικού κλειδιού

[96] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 76.
[97] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 150.
[98] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 76.
[99] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 151.

και άρα της ασύμμετρης κρυπτογραφίας στις ηλεκτρονικές συναλλαγές (αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα και μη απόκριση ευθύνης)[100].

Οι «έξυπνες» κάρτες μπορούν να κατηγοριοποιηθούν με κριτήριο την επεξεργαστική δυνατότητα και με κριτήριο την δυνατότητα εισόδου – εξόδου. Σύμφωνα λοιπόν με αυτά τα δυο κριτήρια κατηγοριοποίησης έχουμε τα εξής:

1. Επεξεργαστική δυνατότητα της κάρτας:

   α) Κάρτες μνήμης ή αποθήκευσης πληροφοριών (memory card, stored value card)

   β) «Έξυπνες» κάρτες ή κάρτες με μικροεπεξεργαστή (smart cards, microprocessor cards)

   γ) «Έξυπνες» κάρτες πολλαπλών εφαρμογών (multi-application smart cards)

2. Δυνατότητα εισόδου – εξόδου της κάρτας:

   α) «Έξυπνες» κάρτες που λειτουργούν με φυσική επαφή (Contact cards)

   β) Ασύρματες «έξυπνες» κάρτες (Contactless cards)

   γ) Υβριδικές κάρτες ή κάρτες που συνδυάζουν τις δυο παραπάνω μεθόδους επικοινωνίας (Hybrid or Combination cards)

Όπως αναφέραμε και πιο πριν, οι «έξυπνες κάρτες» έχουν την ιδιότητα και την δυνατότητα να αποθηκεύουν με μεγάλη ασφάλεια πολλά προσωπικά στοιχεία του ιδιοκτήτη τους, τέτοια προσωπικά στοιχεία είναι η ηλεκτρονική υπογραφή και το ιδιωτικό κλειδί της ψηφιακής υπογραφής του κατόχου τους. Εάν θα θέλαμε να παρουσιάσουμε τις βασικές περιπτώσεις στις οποίες διευκολύνουν οι «έξυπνες κάρτες» στις ηλεκτρονικές συναλλαγές, θα λέγαμε ότι αυτές οι περιπτώσεις είναι:

α) Η χρήση της «έξυπνης» κάρτας ως ηλεκτρονικό πορτοφόλι.

β) Η χρήση της «έξυπνης» κάρτας ως κάρτας εξυπηρέτησης και διατήρησης πελατών (loyalty card).

γ) Η χρήση της «έξυπνης» κάρτας ως κάρτας ελέγχου πρόσβασης.

δ) Η χρήση της «έξυπνης» κάρτας σε τραπεζικές συναλλαγές.

[100] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 77.

4. Νομικο Πλαισιο – Ηλεκτρονικες Υπογραφες

4.1 Εισαγωγή

Τα νομικά προβλήματα που δημιουργούνται από την πραγματοποίηση συναλλαγών μέσω του διαδικτύου, δεδομένου και του γεγονότος ότι πρόκειται κατά κανόνα για διασυνοριακές συναλλαγές, είναι πολλά, αφού το δίκαιο είναι δυνατόν να συμβαδίσει με τους ταχύτερους ρυθμούς ανάπτυξης της τεχνολογίας. Τα προβλήματα επιτείνονται από το γεγονός ότι λόγω της φύσης του διαδικτύου, αφενός εμπλέκονται περισσότερες εθνικές έννομες τάξεις και αφετέρου περισσότεροι, σχεδόν όλοι οι κλάδοι δικαίου[101].

Από όλα τα παραπάνω που αναφέραμε γίνεται φανερό ότι υπάρχει η απαίτηση για ένα σύγχρονο, καινοτόμο και ομοιόμορφο σε παγκόσμιο επίπεδο, νομοθετικό πλαίσιο σχετικό με την ηλεκτρονική υπογραφή, έτσι ώστε ο συναλλασσόμενος να έχει τη δυνατότητα να πραγματοποιεί όλες τις ηλεκτρονικές του συναλλαγές χωρίς κινδύνους, απρόσκοπτα και με πολύ μεγάλο επίπεδο ασφάλειας. Προκειμένου να μην δημιουργηθούν προβλήματα και ασάφειες στις νομοθετικές προσεγγίσεις της ηλεκτρονικής υπογραφής, θα πρέπει οι νομοθετικές αυτές προσεγγίσεις να λαμβάνουν υπόψη τους το στοιχείο της οικουμενικότητας του Διαδικτύου, μέσα στο οποίο δεν υπάρχουν φυσικά σύνορα και μέσα στο οποίο πραγματοποιούν ηλεκτρονικές συναλλαγές καθημερινά συναλλασσόμενοι από διαφορετικές χώρες.

Η θεσμική αναγνώριση των ηλεκτρονικών υπογραφών πρωτοεμφανίστηκε παγκοσμίως σε νομοθέτημα της Πολιτείας Utah των ΗΠΑ το 1995, και έκτοτε άρχισαν να εκδίδονται ανάλογοι νόμοι και σε άλλες Πολιτείες των ΗΠΑ αλλά και σε πολλά άλλα κράτη του κόσμου, όπως η Μαλαισία και η Σιγκαπούρη[102].

Στον Ευρωπαϊκό χώρο ο πρώτος σχετικός νόμος περί θεσμοθέτησης της χρήσης ψηφιακών υπογραφών και όχι γενικά περί ηλεκτρονικής υπογραφής ψηφίστηκε στην Ιταλία το 1997 και παρείχε πλήρη νομική αναγνώριση σε ηλεκτρονικές πράξεις, δεδομένα και έγγραφα, ιδιωτικά και δημόσια καθώς και αρχειοθέτηση, διαβίβαση και αναπαραγωγή τους με ηλεκτρονικά μέσα και μάλιστα όχι μόνο στις συναλλακτικές σχέσεις μεταξύ ιδιωτών αλλά και στις σχέσεις πολιτών – δημόσιας διοίκησης. Ο νόμος προέβλεπε ακόμα την έκδοση πιστοποιητικών προς επιβεβαίωση της ταυτότητας των ηλεκτρονικά συμβαλλόμενων[103].

Στην Γερμανία επίσης, υπήρξε μια αξιόλογη νομοθετικά προσπάθεια με νόμο που ψηφίστηκε το 1997 σχετικά με τις υπηρεσίες στους τομείς της πληροφορικής και των τηλεπικοινωνιών που περιείχε πληθώρα διατάξεων για την ψηφιακή υπογραφή, χωρίς όμως να την εξομοιώνει με την ιδιόχειρη υπογραφή του αστικού δικαίου. Επίσης, προέβλεπε την υιοθέτηση της τεχνολογίας της ασύμμετρης κρυπτογραφίας, με χρήση ατομικού μυστικού κλειδιού από τους συναλλασσόμενους, το οποίο θα κρυπτογραφούσε το μήνυμα μετατρέποντας το σε αλγόριθμο, ενώ ο παραλήπτης του μηνύματος θα το αποκρυπτογραφούσε με το δημόσιο κλειδί. Τέλος, προβλεπόταν η δημιουργία μιας ανεξάρτητης διοικητικής αρχής για τις τηλεπικοινωνίες, η οποία θα χορηγούσε υπό αυστηρές προϋποθέσεις άδεις σε φυσικά ή νομικά πρόσωπα, ώστε να έχουν το νομικό δικαίωμα να παρέχουν υπηρεσίες πιστοποίησης ηλεκτρονικής υπογραφής[104].

Στην χώρα μας έχουμε επίσης ένα πολύ σημαντικό άρθρο το 1998, πιο συγκεκριμένα στην Ελλάδα με το άρθρο 14 του νόμου 2672/1998 με τίτλο «Διακίνηση εγγράφων με ηλεκτρονικά μέσα» έχουμε τις πρώτες βάσεις για την χρήση ηλεκτρονικών υπογραφών στην ελληνική Δημόσια Διοίκηση. Πιο αναλυτικά θα παρουσιάσουμε το συγκεκριμένο άρθρο στην συνέχεια αυτό του κεφαλαίου.

---

[101] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 15.

[102] «Η Ευρωπαϊκή Νομοθεσία για τις ηλεκτρονικές υπογραφές (Ανάλυση και σχολιασμός)», Χρήστος Ευαγ. Σιουλης σελ. 2, άρθρο στα πλαίσια των ομάδων Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)» και Δ1 «Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα» (ημερομηνία επίσκεψης: 15/05/2011).

[103] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 89 - 90.

[104] Καραδημητρίου, ο.π., σελ. 90.

Γίνεται αντιληπτό από τα πιο πάνω ότι όλες οι προσπάθειες που έκαναν τα κράτη της Ευρωπαϊκής Ένωσης ή άλλα κράτη σε παγκόσμιο επίπεδο ήταν μεμονωμένες. Αποτέλεσμα αυτού ήταν να μην υπάρχει κοινός συντονισμός και κοινό πεδίο νομοθετικής θέσπισης των ηλεκτρονικών υπογραφών. Το μεγάλο πρόβλημα που υπήρχε ήταν η νομοθετική ανομοιομορφία στους νόμους που είχαν θέσπιση μεμονωμένα τα κράτη για την ηλεκτρονική υπογραφή. Αποτέλεσμα αυτής της νομοθετικής διαφοροποίησης των κρατών-μελών της Ευρωπαϊκής Ένωσης, είναι η διαφορετική νομική ισχύς της ηλεκτρονικής υπογραφής καθώς και οι διαφορετικές απαιτήσεις σε σχέση με τον τύπο του ηλεκτρονικού υπογεγραμμένου εγγράφου.

Η εμφανέστατη ανάγκη για τον προσδιορισμό «κοινών κανόνων», τόσο από τεχνολογική όσο και από νομική άποψη, ώστε να επιτευχθεί σταδιακά μια «διαλειτουργικότητα» στην δημιουργία, στην χρήση αλλά και στην αναγνώριση των ηλεκτρονικών υπογραφών σε κοινοτικό επίπεδο, οδήγησε την Ευρωπαϊκή Επιτροπή να προτείνει την συγκεκριμένη Οδηγία «σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές», η οποία εγκρίθηκε και ψηφίσθηκε τελικά από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις 13 Δεκεμβρίου του 1999 (Επίσημη Εφημερίδα Ε.Ε. αριθ. L 013 της 19/01/2000 σ. 0012 – 0020)[105]. Πιο συγκεκριμένα, τα πιο πάνω προβλήματα και με στόχο την ανάπτυξη των ηλεκτρονικών συναλλαγών το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο Υπουργών αρμόδιων για θέματα τηλεπικοινωνιών υιοθέτησαν στις 13 Δεκεμβρίου 1999 την οδηγία 1999/93/ΕΚ, σε στόχο και σκοπό να δημιουργήσουν ένα σαφές κοινοτικό νομικό πλαίσιο σχετικά με τις ηλεκτρονικές υπογραφές, το οποίο θα ενισχύσει την εμπιστοσύνη στις νέες τεχνολογίες και θα συμβάλει στη γενική αποδοχή τους. Η Ελλάδα ενσωμάτωσε στο εθνικό της δίκαιο την οδηγία 1999/93 με το π.δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές»[106].

Στην Οδηγία 1999/98/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, που ψηφίστηκε για να δώσει στα κράτη μέλη τη δυνατότητα να εναρμονίσουν τα δίκαια τους όσον αφορά στην ηλεκτρονική υπογραφή, αναφέρεται ότι στόχος της είναι η διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών και η συμβολή στην αναγνώριση της νομικής ισχύος τους. Θεσπίζεται έτσι νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για ορισμένες υπηρεσίες πιστοποίησης, που προσφέρονται στο κοινό, ώστε να επιτευχθεί η εξασφάλιση της ομαλής λειτουργίας της εσωτερικής αγοράς[107].

4.2 Νομοθετικές προσεγγίσεις της τεχνολογίας των ηλεκτρονικών υπογραφών

Στις μέρες μας οι τρόποι νομοθετικής προσέγγισης της τεχνολογίας των ηλεκτρονικών υπογραφών χωρίζονται διεθνώς σε δυο μεγάλες κατηγορίες, αυτές είναι:

1. Η τεχνολογικά ουδέτερη προσέγγιση (technology - neutral) και
2. Η τεχνολογικά εξειδικευμένη προσέγγιση (technology - specific)

Η τεχνολογικά ουδέτερη νομοθεσία περί ηλεκτρονικών υπογραφών πρέπει να έχει διατύπωση προσανατολισμένη τεχνολογικά προς το μέλλον, να προνοεί για τη χρήση ηλεκτρονικών υπογραφών με διαφορετικά μεταξύ τους τεχνικά χαρακτηριστικά, ακόμα και με χαρακτηριστικά που δεν έχουν ως σήμερα εφευρεθεί. Αν και σε μια τέτοια νομοθεσία είναι πολύ δύσκολο να προβλεφτούν οι συγκεκριμένες νομικές συνέπειες της χρήσης των νέων ηλεκτρονικών υπογραφών, υπάρχει το θετικό στοιχείο της εύκολης προσαρμογής της νομοθεσίας στις προκλήσεις των καιρών και στις νέες τεχνολογίες. Επίσης, αν χρειαστεί στο μέλλον να τροποποιηθεί η νομοθεσία περί ηλεκτρονικών υπογραφών, η τροποποίηση μιας τεχνολογικά ουδέτερης νομοθεσίας είναι σαφώς ευκολότερη από αυτήν της εξειδικευμένης

[105] «Η Ευρωπαϊκή Νομοθεσία για τις ηλεκτρονικές υπογραφές (Ανάλυση και σχολιασμός)», Χρήστος Ευαγ. Σιουλης σελ. 2, άρθρο στα πλαίσια των ομάδων Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)» και Δ1 «Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα» (ημερομηνία επίσκεψης: 15/05/2011).

[106] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 91 - 92.

[107] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 51.

νομοθεσίας, η οποία θα έχει ήδη δημιουργήσει ισχυρό προηγούμενο στη νομολογία και στις συναλλαγές[108].

Η τεχνολογικά εξειδικευμένη νομοθεσία για τις ηλεκτρονικές υπογραφές, είναι η νομοθεσία που είναι στενά και λεπτομερειακά προσκολλημένη στις τεχνικές ορολογίες του σήμερα, επικεντρώνεται στην τεχνολογία που υπάρχει προς το παρόν διαθέσιμη στην αγορά. Με αυτόν τον τρόπο, δίνεται έμφαση στην ασφάλεια, στη βεβαιότητα και στην αξιοπιστία των ήδη γνωστών και δοκιμασμένων στο εμπόριο τεχνολογιών, θωρακίζοντας με νομική ισχύ μόνο αυτές, με το σκεπτικό ότι δεν είναι δυνατόν να αναγνωρίσει νομικά άγνωστης τεχνολογίας ηλεκτρονικές υπογραφές, που δεν έχουν δοκιμαστεί στην πράξη και δεν έχουν γίνει αποδεκτές ακόμη στην αγορά. Η τεχνολογικά εξειδικευμένη νομοθεσία των ηλεκτρονικών υπογραφών έχει το θετικό στοιχείο ότι απαλλάσσει τον δικαστή από την υποχρέωση να κρίνει τις σχετικές υποθέσεις κατά περίπτωση ανάλογα δηλαδή με το ποια τεχνολογία ηλεκτρονικής υπογραφής χρησιμοποιούν οι αντίδικοι κάτι που εάν γινόταν θα απαιτούσε από τους δικαστικούς λειτουργούς πολύ καλές γνώσεις τεχνικές. Όμως η εξειδικευμένη τεχνολογικά νομοθεσία χρειάζεται συνεχή τροποποίηση και προσαρμογή στα νέα τεχνολογικά δεδομένα[109].

4.3 Νομικές Προσεγγίσεις αναγνώρισης ηλεκτρονικών υπογραφών

Η «νομική αναγνώριση» των ηλεκτρονικών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της δεκαετίας του 1990, με την θέσπιση σχετικών νόμων σε διάφορα κράτη. Το ζήτημα της έκτασης που θα έχει η νομική αναγνώριση των ηλεκτρονικών υπογραφών είναι πολύ σημαντικό και έχει απασχολήσει αρκετά τα τελευταία χρόνια. Το ζήτημα αυτό αφορά στο εάν έπρεπε ή όχι να αναγνωριστούν ως νομικά ισότιμες με τις ιδιόχειρες όλες οι ηλεκτρονικές υπογραφές, ανεξαρτήτως των τεχνολογικών προτύπων στα οποία βασίζονται. Σε διεθνές επίπεδο, μπορούμε να διακρίνουμε δύο διαφορετικές νομικές προσεγγίσεις: α) η «μινιμαλιστική» και β) η «μαξιμαλιστική».

Η μινιμαλιστική προσέγγιση (minimalist approach)[110], όπου «κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή» [111]. Παρέχεται λοιπόν, πλήρης και χωρίς όρους νομική αναγνώριση σε όλες τις ηλεκτρονικές υπογραφές, ανεξάρτητα από τις τεχνολογικές τους προδιαγραφές. Η ανεπιφύλακτη νομική εξίσωση όλων των ηλεκτρονικών υπογραφών με τις ιδιόχειρες, λόγω της τεχνολογικής ουδετερότητας που επιτυγχάνει, υποστηρίζεται ότι ενθαρρύνει τους καταναλωτές να διενεργήσουν ηλεκτρονικές συναλλαγές, αφού γνωρίζουν εκ των προτέρων ότι όποιων τεχνικών προδιαγραφών ηλεκτρονική υπογραφή χρησιμοποιήσουν, αυτή παράγει πλήρη έννομα αποτελέσματα, όπως ακριβώς και η ιδιόχειρη υπογραφή. Επίσης, η μινιμαλιστική νομοθετική προσέγγιση δεν περιέχει πολλές δύσκολες τεχνικές έννοιες, επομένως είναι πολύ απλή και εύκολα αντιληπτή για το νομικό κόσμο που θα κληθεί να την εφαρμόσει και να την ερμηνεύσει. Η προσέγγιση αυτή ευνοεί και την ανάπτυξη νέων τεχνολογιών ηλεκτρονικής υπογραφής, για το λόγο ότι δεν προκρίνει κάποια συγκεκριμένη υπάρχουσα τεχνολογία, για τον λόγο αυτό ενισχύει την ομοιόμορφη σε διεθνές επίπεδο νομοθετική αντιμετώπιση της ηλεκτρονικής υπογραφής, παρακάμπτοντας εμπόδια που θα δημιουργούσε η πρόκριση κάποιας συγκεκριμένης τεχνολογίας από χώρα σε χώρα[112].

Στην μινιμαλιστική προσέγγιση υπάρχουν και σημαντικά μειονεκτήματα. Ένα σημαντικό μειονέκτημα είναι ότι δεν υπάρχει ορισμός συγκεκριμένου είδους ηλεκτρονικής υπογραφής, η οποία δεσμεύει τον υπογράφοντα όπως η χειρόγραφη υπογραφή, καθιστά κάθε μέθοδο

[108] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 97.
[109] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 97 - 98.
[110] Η μινιμαλιστική προσέγγιση έχει υιοθετηθεί από κράτη όπως οι Η.Π.Α., ο Καναδάς, η Μεγάλη Βρετανία, η Αυστραλία.
[111] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 3, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)
[112] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 102 - 103.

ηλεκτρονικής υπογραφής, από την πιο απλή μέχρι την πιο περίπλοκη, το ίδιο δεσμευτική. Αυτή η εξίσωση του επιπέδου των ηλεκτρονικών υπογραφών μπορεί να αποβεί σε βάρος του υπογράφοντα συναλλασσόμενου, γιατί ίσως βρεθεί δεσμευμένος χωρίς να έχει τέτοια πρόθεση ακόμα και από ένα λανθασμένο κλικ του Η/Υ του. Σημαντικό μειονέκτημα επίσης είναι το γεγονός ότι, επειδή δεν ορίζει υψηλά τεχνικά στάνταρ για τις ηλεκτρονικές υπογραφές, είναι πιθανό κάποιες από αυτές να είναι τεχνολογικά επισφαλείς, δημιουργώντας έτσι τον κίνδυνο εξαπάτησης καταναλωτών από επιτήδειους που εμπορεύονται ελαττωματικής τεχνολογίας ηλεκτρονικές υπογραφές[113].

Η μαξιμαλιστική ή αναλυτική προσέγγιση (maximalistic or prescrip approach)[114], είναι νομικά πιο περίπλοκη σύμφωνα με την προσέγγιση αυτή, «μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται άμεσα ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές»[115]. Γίνεται αντιληπτό ότι η συγκεκριμένη προσέγγιση προσδίδει έννομα αποτελέσματα μόνο σε ορισμένα είδη ηλεκτρονικών υπογραφών, ανάλογα με το εάν αυτές συμμορφώνονται ή όχι με συγκριμένα τεχνικά πρότυπα. Εάν και φαίνεται η προσέγγιση αυτή να αποτελεί εμπόδιο στην ελεύθερη ανάπτυξη της αγοράς των ηλεκτρονικών υπογραφών, λόγω του γεγονότος ότι απαιτεί την ύπαρξη κάποιων συγκεκριμένων τεχνολογικών προδιαγραφών για την εξίσωση ηλεκτρονικής και χειρόγραφης υπογραφής, υπάρχει το πολύ θετικό στοιχείο ότι η προσέγγιση αυτή προστατεύει τον καταναλωτή από αναξιόπιστες τεχνολογικές εφαρμογές της ηλεκτρονικής υπογραφής που διατίθενται στην αγορά[116].

4.4 Διεθνή και Ευρωπαϊκό Νομικό Πλαίσιο

Το θεσμικό πλαίσιο και η «νομική αναγνώριση» των ηλεκτρονικών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη όπως αναφέραμε και πιο πάνω. Στο Ευρωπαϊκό δίκαιο και κατά συνέπεια και στο Ελληνικό ακολουθείται μια μικτή, υβριδική όπως ονομάζεται, προσέγγιση στο θέμα της νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, δηλαδή την προσέγγιση των «δυο επιπέδων» (two-tier approach or hybrid model), η οποία συνδυάζει και τις δυο παραπάνω κατευθύνσεις[117].

Η αρχή της «τεχνολογικής ουδετερότητας» (και η εξ αυτής υποχρέωση για αποδοχή όλων των αξιόπιστων μεθόδων ηλεκτρονικών υπογραφών της αγοράς) από την μία πλευρά, και η ανάγκη για διασφάλιση ενός «υψηλού επιπέδου αξιοπιστίας» (το οποίο ήδη απαιτούσαν ή/και παρείχαν μερικές υφιστάμενες νομοθεσίες και σχετικές εφαρμογές κάποιων κρατών - μελών) από την άλλη, οδήγησαν τον κοινοτικό νομοθέτη στην σύνταξη μιας Οδηγίας με «υβριδική» προσέγγιση («two-tier» approach), η οποία αφ' ενός με την πρώτη παράγραφο του άρθρου της 5, ορίζει έναν αυστηρά προδιαγεγραμμένο τύπο («prescriptive» approach) ηλεκτρονικών υπογραφών, στον οποίο αποδίδει exl ege ισοδυναμία με την «ιδιόγραφη συμβατική υπογραφή», και, αφ' ετέρου, στη δεύτερη παράγραφο του ίδιου άρθρου, εναποθέτει στους εθνικούς δικαστές την αναγνώριση ως αποδεικτικών στοιχείων σε νομικές διαδικασίες, κάθε άλλου τύπου ηλεκτρονικών υπογραφών ο οποίος παρέχει -κατά την γνώμη τους- «αποδεκτά» επίπεδα αξιοπιστίας ή/και «εύλογη» πεποίθηση για την πραγματοποίηση μιας συγκεκριμένης ηλεκτρονικής συναλλαγής, σύμφωνα πάντα με την αρχή της «ελεύθερης εκτίμησης των

[113] Καραδημητρίου, ο.π., σελ. 103 - 104.
[114] Η μαξιμαλιστική ή αναλυτική προσέγγιση έχει υιοθετηθεί και έχει διαμορφώσει την εθνική νομοθεσία πολλών χωρών της ηπειρωτικής Ευρώπης, όπως η Γερμανία, Ιταλία, Εσθονία και Γαλλία.
[115] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 3, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)
[116] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 104 - 105.
[117] Σύμφωνα 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).

αποδείξεων» από τα δικαστήρια («minimalistic» approach)[118]. Πιο αναλυτικά παρουσιάζονται στην συνέχεια τα δύο επίπεδα νομικής αναγνώρισης της ηλεκτρονικής υπογραφής.

Στο πρώτο επίπεδο της νομικής αναγνώρισης η νομοθεσία ακολουθεί την μαξιμαλιστική προσέγγιση και αποδίδει μόνο στις προηγμένες ηλεκτρονικές υπογραφές, που πληρούν συγκεκριμένες τεχνικές προϋποθέσεις, πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές. Με τον τρόπο αυτό επιτυγχάνεται κατά το δυνατόν μεγαλύτερη προστασία του αδαούς περί την τεχνολογία της ηλεκτρονικής υπογραφής καταναλωτή καθώς γίνεται φιλτράρισμα των διαφόρων τεχνολογιών ηλεκτρονικής υπογραφής και πρόκριση εκείνων των τεχνολογιών που εξασφαλίζουν ένα υψηλότερο ποιοτικά αποτέλεσμα[119]. Πιο συγκεκριμένα θα λέγαμε ότι, η Οδηγία (άρθρο 5 αριθ. 1) διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών, αποκαλούμενες στη πράξη στην πλειοψηφία των ευρωπαϊκών κρατών ως «αναγνωρισμένες ηλεκτρονικές υπογραφές», στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις «ιδιόχειρες υπογραφές», όπως οι τελευταίες ορίζονται και ό, τι και αν αποδεικνύουν σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους. Σε αυτήν την κατηγορία ανήκουν όλες οι «προηγμένες ηλεκτρονικές υπογραφές» που, επιπλέον, βασίζονται σε «αναγνωρισμένο πιστοποιητικό» και δημιουργούνται από «ασφαλή διάταξη δημιουργίας υπογραφής» [120].

Στο δεύτερο και πιο γενικό επίπεδο νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, επιδιώκεται να γίνει ενθάρρυνση της ελεύθερης ανάπτυξης της αγοράς των ηλεκτρονικών υπογραφών και να αφεθεί ανεπηρέαστη η ομαλή λειτουργία της. Έτσι ακολουθείται η μινιμαλιστική προσέγγιση, δηλαδή αναγνωρίζει νομικά όλες τις ηλεκτρονικές υπογραφές σε τεχνολογικά ουδέτερη βάση και παρέχει σε όλες ανεξαρτήτως στοιχειώδη νομική ισχύ. Τέτοιου είδους ηλεκτρονικές υπογραφές μπορούν να ικανοποιήσουν τις απαιτήσεις της ηλεκτρονικής γραφής, αλλά δεν εξισώνονται με τις ιδιόχειρες υπογραφές, γιατί δεν είναι τεχνολογικά ικανές να συνδεθούν μονοσήμαντα με τον υπογράφοντα, ούτε να τον ταχτοποιήσουν, άρα υπάρχει έλλειμμα ασφάλειας [121]. Πιο συγκεκριμένα, η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως «ηλεκτρονικές υπογραφές», που μπορούν να χρησιμοποιηθούν ως «αποδεικτικά στοιχεία» σε νομικές διαδικασίες (άρθρο 5 αριθ. 2 της Οδηγίας, αρχή της μη διακρίσεως), 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» (άρθρο 2 αριθ. 1 της Οδηγίας). Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο «απλές» (π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής σε ένα e-mail ή του αριθμού του τηλεφώνου αποστολής σε ένα SMS μήνυμα, κλπ), ως την πιο «σύνθετες» (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κλπ), ανεξάρτητα, δηλαδή, από τον βαθμό τεχνικής ασφάλειας που παρέχουν[122].

Η επιλογή της υβριδικής προσέγγισης για την αναγνώριση των ηλεκτρονικών υπογραφών είναι πολύ επιτυχημένη γιατί δίνει μεγάλο βάρος στην προστασία των καταναλωτών από ελαπτωματικές τεχνολογίες ηλεκτρονικής υπογραφής, αποφεύγοντας να αφήσει την αγορά εντελώς ελεύθερη και ανεξέλεγκτη στο συγκεκριμένο θέμα. Αυτό γίνεται ακόμα πιο σημαντικό

[118] «Η Ευρωπαϊκή Νομοθεσία για τις ηλεκτρονικές υπογραφές (Ανάλυση και σχολιασμός)», Χρήστος Ευαγ. Σιουλης σελ. 2, άρθρο στα πλαίσια των ομάδων Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)» και Δ1 «Θεσμικό πλαίσιο και ηλεκτρονικό επιχειρείν στην Ελλάδα» (ημερομηνία επίσκεψης: 15/05/2011).

[119] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 105.

[120] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 4, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[121] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 105.

[122] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 4, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

εάν σκεφτούμε ότι υπάρχει η όλο και μεγαλύτερη τάση για πλήρη απελευθέρωση του εμπορίου και του αμείλικτου οικονομικού ανταγωνισμού σε παγκόσμιο επίπεδο[123].

Επίσης, η επιλογή της Ευρωπαϊκής Επιτροπής και του Συμβουλίου Υπουργών να υιοθετήσουν νομοθετική διατύπωση τεχνολογικά ουδέτερη και ευέλικτη, είναι η πλέον ενδεδειγμένη, εάν σκεφτεί κανείς την αλματώδη ανάπτυξη και τεχνολογική πρόοδο που αναμένεται να γνωρίσουν οι ηλεκτρονικές υπογραφές τα επόμενα χρόνια. «Η ταχεία τεχνολογική ανάπτυξη και ο παγκόσμιος χαρακτήρας του Διαδικτύου επιβάλλουν προσέγγιση που θα είναι ανοικτή σε διάφορες τεχνολογίες και υπηρεσίες ηλεκτρονικής αναγνώρισης της γνησιότητας δεδομένων»[124]. Σε αντίθετη περίπτωση η επιλογή μιας τεχνολογικά εξειδικευμένης νομοθεσίας, θα σήμαινε αυτόματα την διαρκή ανάγκη τροποποίησης της οδηγίας 1999/93, προκειμένου να μπορέσει να ακολουθήσει τις τεχνολογικές εξελίξεις και να μπορεί να διασφαλίσει κάθε στιγμή την αναγνώριση των ηλεκτρονικών υπογραφών, αυτό θα ήταν πολύ δύσκολο έως αδύνατο να γίνει γιατί θα έπρεπε να λαμβάνει χώρα σε μια ένωση τόσο πολλών κρατών, που διαρκώς αυξάνονται.

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 (άρθρο 2 αριθ. 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[125].

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[126].

Τέλος, 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. Επίσης, 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.

---

[123] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 105 - 106.

[124] Σύμφωνα με την αιτιολογική σκέψη 8 του προοιμίου της οδηγίας 1999/93.

[125] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 4, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)

[126] Ο.π.

Στο σημείο αυτό κρίνουμε σκόπιμο να αναφέρουμε ότι, 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:

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

4.4.1 Ασάφειες θεσμικού πλαισίου

Η ανάγκη για διατήρηση ουδετερότητας προς την υπάρχουσα αγορά και τις σχετικές τεχνολογίες, σε συνδυασμό με την αποφυγή της επέμβασης σε ήδη υφιστάμενες σχετικές εφαρμογές και εθνικές επιλογές των κρατών-μελών, αλλά και το γεγονός ότι η Οδηγία δεν στόχευε στην ρύθμιση θεμάτων «που αφορούν την σύναψη και την ισχύ των συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου»[127], είχε ως αποτέλεσμα την ύπαρξη πολλών ασαφειών και παραλείψεων στο υφιστάμενο ευρωπαϊκό θεσμικό πλαίσιο, γεγονός που οδηγεί σε αντιμετώπιση αρκετών προβλημάτων κατά την ερμηνεία του και την προσπάθεια εφαρμογής του. Συγκεκριμένα, η Οδηγία[128]:

- Δεν αποσαφηνίζει εάν οι «αναγνωρισμένες ηλεκτρονικές υπογραφές» (του άρθρου 5 παράγραφος 1) μπορούν να χρησιμοποιηθούν εξίσου για «απλή γνησιότητα δεδομένων» και για την απλή «επίδειξη ταυτότητας» (ηλεκτρονικές ταυτότητες) του υπογράφοντα.
- Δεν αναφέρεται καθόλου στα στοιχεία που απαιτούνται για την «διαχρονική ισχύ» των ηλεκτρονικών υπογραφών (Χρονοσήμανση, Αρχειοθέτηση), ούτε αναφέρεται διεξοδικότερα στην παροχή των σχετικών υπηρεσιών από τους ΠΥΠ.
- Δεν αποσαφηνίζει τον ρόλο των προβλεπόμενων «Εθελοντικών Διαπιστεύσεων» των ΠΥΠ (εάν θα είναι σε εθνικό ή σε πανευρωπαϊκό/κλαδικό επίπεδο)
- Κάνει μόνο «απλές συστάσεις» για την ασφαλή επαλήθευση των υπογραφών (Παράρτημα IV)

Τα ζητήματα αυτά αποτελούν ακόμη αντικείμενο συζητήσεων και αντιπαραθέσεων στα πλαίσια των σχετικών διεργασιών προτυποποίησης, με περιορισμένα έως τώρα αποτελέσματα.

4.5 Νομικό Πλαίσιο στην Ελλάδα

4.5.1 Εισαγωγή

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. Σύμφωνα με το άρθρο 14 παρ. 2 του ν. 2672/1998 με τον όρο «ψηφιακή υπογραφή» νοείται η ψηφιακής μορφής υπογραφή σε δεδομένα ή συνημμένη 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 συνδέεται μονοσήμαντα με τον υπογράφοντα, ταυτοποιεί τον υπογράφοντα, δημιουργείται με μέσα που ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και συνδέεται με τα δεδομένα, στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε

[127] Άρθρο 2 εδ. β' της Οδηγίας 1999/93/ΕΚ

[128] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 46, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Paradoteo_E2-Teliko.pdf (ημερομηνία επίσκεψης: 15/05/2011).

επακόλουθη αλλοίωση των εν λόγω δεδομένων. Ο ορισμός αυτός λήφθηκε από την τότε πρόταση Οδηγίας COM (1999) 195 τελικό[129].

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 άρθρου 14, 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.

Παρέχεται επίσης, 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. Πιο συγκεκριμένα, αναφέρονται τα εξής:

Με προεδρικό διάταγμα, που εκδίδεται με πρόταση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Οικονομικών, Ανάπτυξης και Μεταφορών και Επικοινωνιών, καθορίζονται οι προϋποθέσεις και η διαδικασία έκδοσης, διακίνησης, διαχείρισης και διασφάλισης της ψηφιακής υπογραφής, οι προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, οι τεχνικοί κανόνες για την κατάρτιση, την αποστολή, τη διατήρηση, την αντιγραφή και την αναπαραγωγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εγγύηση ακεραιότητας, διάθεσης και διατήρησης των πληροφοριών που περιέχονται στο μήνυμα καθώς και κάθε άλλη αναγκαία λεπτομέρεια. Με το ίδιο προεδρικό διάταγμα μπορεί να καθορίζονται και οι κατηγόριες μηνυμάτων τα οποία έχουν ισχύ και χωρίς να φέρουν ψηφιακή υπογραφή[130].

Η ψηφιακή υπογραφή επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής, και την κείμενη νομοθεσία. Το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή σύμφωνα με το προεδρικό διάταγμα της παραγράφου 19 έχει τη αποδεικτική ισχύ εγγράφου κατά τους ορισμούς του Κώδικα Πολιτικής Δικονομίας και κάθε άλλης σχετικής διάταξης[131].

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. Ακόμα, προβλέπεται ότι το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή έχει την αποδεικτική ισχύ έγγραφου κατά τον ΚΠολΔ[132].

Όπως γίνεται φανερό από τα πιο πάνω στον νόμο υπήρξε ο ορισμός του ηλεκτρονικού ταχυδρομείου καθώς επίσης και ο ορισμός της ψηφιακής υπογραφής. Σύμφωνα λοιπόν, 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:

- Συνδέεται μονοσήμαντα με τον υπογράφοντα.
- Ταυτοποιεί τον υπογράφοντα

[129] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 110.
[130] Σύμφωνα με το άρθρο 14 του Ν.2672/98 παράγραφος 19.
[131] Σύμφωνα με το άρθρο 14 του Ν.2672/98 παράγραφος 22.
[132] Σύμφωνα με το άρθρο 14 του Ν.2672/98 παράγραφος 22.

- Δημιουργεί με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχο του και
- 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. που θα εξασφαλίζουν την ταυτοπροσωπία αλλά και τη μοναδικότητα του φορέα της ηλεκτρονικής υπογραφής. Ο κάθε χρήστης θα μπορεί να εφοδιασθεί με τη δική του «ηλεκτρονική υπογραφή», μέσω διαπιστευμένων προς τον σκοπό αυτό εταιρειών, σε μορφή λογισμικού, καθώς και μ' έναν μυστικό κωδικό αριθμό (PIN) για να είναι δυνατή η πρόσβαση στην ηλεκτρονική υπογραφή. Το λογισμικό αυτό θα μπορεί να εγκατασταθεί στον προσωπικό υπολογιστή του χρήστη ώστε να βάζει την ψηφιακή υπογραφή του όταν χρειασθεί ή θα μπορεί να το έχει μαζί του αποθηκευμένο σε μια μνήμη USB flash ώστε να μπορεί να το χρησιμοποιεί και από άλλους υπολογιστές.

Οι διατάξεις του πδ 150/2001 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 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.

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. 342/2002 (ΦΕΚ Α' 284/22.11.2002), στο πλαίσιο του άρθρου 14 παρ. 19 και 20 ν. 2672/1998 και το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων μηνυμάτων του ηλεκτρονικού ταχυδρομείου στις επικοινωνίες του δημόσιου τομέα. Πιο αναλυτικά το πδ 342/2002 επικεντρώνεται στην «Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ δημόσιων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών προσώπων». Σύμφωνα με το άρθρο 3 του πδ 342/2002 για την εφαρμογή του παρόντος προεδρικού διατάγματος ισχύουν οι ορισμοί του άρθρου 2 του πδ 150/2001, για δε τις έννομες συνέπειες τα οριζόμενα στο άρθρο 3 του ίδιου πδ. Κατά το άρθρο 4 του πδ 342/2002, οι διατάξεις του πδ 150/2001 για την πρόσβαση στην αγορά, τις αρχές της εσωτερικής αγοράς, τους παρόχους πιστοποίησης, την ευθύνη τους, την προστασία δεδομένων, τους όρους που ισχύουν για αναγνωρισμένα πιστοποιητικά, τη διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής ισχύουν ανάλογα και

κατά τη διακίνηση μηνυμάτων με ηλεκτρονικό ταχυδρομείο, κατά τις διατάξεις του άρθρου 1 του πδ 342/2002[133].

Το ρυθμιστικό πεδίο του πδ 342/2002 προσδιορίζεται από τα άρθρα 1 και 2: αποφάσεις, πιστοποιητικά και βεβαιώσεις διακινούνται με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των ΠΝΔΔ και των ΟΤΑ ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, εφόσον φέρουν ψηφιακή υπογραφή (άρθρο 1 παρ. 1 πδ 342/2002). Γνωμοδοτήσεις, αντίγραφα πρακτικών, εισηγήσεις και εκθέσεις διακινούνται με ηλεκτρονικό ταχυδρομείο από υπηρεσίες του δημοσίου, ΝΠΔΔ και ΟΤΑ, προς φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου εφόσον φέρουν ψηφιακή υπογραφή (άρθρο 1 παρ. 2 πδ 342/2002). Πέρα όμως από τη ρύθμιση του άρθρου 1 είναι δυνατή κατά το άρθρο 2 του πδ 342/2002 και η διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο, χωρίς ψηφιακή υπογραφή. Η κατ' αυτόν τον τρόπο διακίνηση επιτρέπεται και έχει νομική ισχύ μεταξύ των υπηρεσιών του δημοσίου, των ΝΠΔΔ και των ΟΤΑ ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή έννομων αποτελεσμάτων ή με την άσκηση δικαιώματος, ιδίως όταν έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, οδηγίες, μελέτες, στατιστικά στοιχεία, αιτήσεις παροχής πληροφοριών αι σχετικές απαντήσεις[134].

Αξίζει σε αυτό το σημείο να αναφέρουμε 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 ΕΕΤΤ και κυρώθηκε με την Υ.Α 2512οικ/18-10-2006.

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. Έτσι για την παροχή υπηρεσιών πιστοποίησης δεν απαιτείται η χορήγηση κρατικής άδειας στους ΠΥΠ (άρθρο 4 παράγραφος 4 π.δ. 150/2001), υιοθετείται ένα σύστημα εθελοντικής διαπίστευσης τους (άρθρο 4 παράγραφος 5), που παρέχεται από την ΕΕΤΤ (βλ. το ν. 3431/2006) ή από ορισμένους άλλους δημόσιους ή ιδιωτικούς φορείς, που ορίζονται από την τελευταία. Οι προϋποθέσεις για την εθελοντική διαπίστευση πρέπει να είναι αντικειμενικές, διαφανείς και ανάλογες με τον επιδιωκόμενο σκοπό, δεν πρέπει δε να οδηγούν σε διακρίσεις[135].

4.5.2 Το προεδρικό διάταγμα 150/2001 σκοπός και εφαρμογή

Σύμφωνα με το άρθρο 1 παράγραφος 1 του π.δ. 150/2001, σκοπός του είναι η προσαρμογή και η συμμόρφωση της ελληνικής νομοθεσίας προς τις διατάξεις της κοινοτικής οδηγίας 1999/93, η οποία με την σειρά της είναι σκοπό «να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να

[133] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 113.
[134] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης , ο.π., σελ. 114
[135] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 53.

συμβάλει στη νομική αναγνώριση τους»[136]. Με το π.δ. 150/2001, αναγνωρίζονται οι τεχνολογίες ηλεκτρονικής υπογραφής καθορίζονται οι έννομες συνέπειες τους και ρυθμίζεται η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών[137].

Το π.δ. 150/2001 στο άρθρο 1 παράγραφος 2 οριοθετεί το πεδίο εφαρμογής του, ορίζοντας ότι «οι διατάξεις του παρόντος Διατάγματος δεν θίγουν διατάξεις που, αναφορικά με τη σύναψη και ισχύ συμβάσεων ή εν γένει τη σύσταση νομικών υποχρεώσεων, 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 ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα». Η Διάταξη αυτή ουσιαστικά επαναλαμβάνει την κατευθυντήρια γραμμή του άρθρου 1 αριθ. 2 της οδηγίας 1999/93, η οποία «δεν καλύπτει πτυχές που αφορούν τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου και δεν θίγει κανόνες και περιορισμούς σχετικά με τη χρήση εγγράφων οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο». Η οδηγία δεν αποσκοπεί σε εναρμόνιση των εθνικών κανόνων που αφορούν το ενοχικό δίκαιο των κρατών-μελών σχετικά με την κατάρτιση και την εκτέλεση συμβάσεων ή σε άλλες διατυπώσεις μη συμβατικής φύσης σχετικά με τις υπογραφές[138].

Μπορούμε να πούμε ότι η ρύθμιση του π.δ. 150/2001 σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές δεν θεωρείται ότι επηρεάζει τις διατάξεις του ΑΚ ή άλλων νόμων, που επιβάλλουν την τήρηση έγγραφου τύπου για την έγκυρη κατάρτιση ορισμένων δικαιοπραξιών. Μετά την ψήφισή του, η εκάστοτε νομοθετική πρόβλεψη ότι για το κύρος μιας δικαιοπραξίας είναι απαραίτητη η ύπαρξη ιδιωτικού εγγράφου, δεν έρχεται σε αντίθεση με το άρθρο 9 παράγραφος 1 της οδηγίας για το ηλεκτρονικό εμπόριο, που απαγορεύει στα κράτη μέλη να περιλαμβάνουν στη νομοθεσίας τους ρυθμίσεις, που παρακωλύουν την κατάρτιση ηλεκτρονικών συμβάσεων[139].

Σύμφωνα με το άρθρο 2 αριθ. 1 του π.δ. 150/2001 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». 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)[140].

Σύμφωνα με την εισηγητική έκθεση του Σχεδίου Νόμου για τις ηλεκτρονικές υπογραφές, ηλεκτρονική υπογραφή μπορεί να είναι ακόμη και ένα ψευδώνυμο πληκτρολογημένο και ενσωματωμένο στο ηλεκτρονικό κείμενο. Θα λέγαμε ότι έτσι υιοθετείτε μια τεχνολογικά ουδέτερη προσέγγιση κατά τον ορισμό της ηλεκτρονικής υπογραφής, στοχεύοντας στο να περιληφθούν στο πεδίο εφαρμογής του νόμου τόσο οι τεχνολογικά απλές, όσο και οι πιο προηγμένες ηλεκτρονικές υπογραφές, ακόμα και αυτές που δεν έχουν εφευρεθεί. Δεδομένα σε ηλεκτρονική μορφή θα μπορούσαν να είναι ακόμα και ένας ηλεκτρονικός ήχος ή ένα ηλεκτρονικό σύμβολο, εφόσον ο ηλεκτρονικά συμβαλλόμενος το χρησιμοποιεί ως υπογραφή του[141].

Η επιλογή της Ευρωπαϊκής Επιτροπής και του Συμβουλίου Υπουργών να υιοθετήσουν νομοθετική διατύπωση τεχνολογικά ουδέτερη και ευέλικτη είναι η πλέον ενδεδειγμένη, με δεδομένο την αλματώδη ανάπτυξη και τεχνολογική πρόοδο που αναμένεται να γνωρίσουν οι ηλεκτρονικές υπογραφές τα επόμενα χρόνια.

Επίσης, το π.δ. 150 /2001 ρυθμίζει την παροχή υπηρεσιών πιστοποίησης. Αυτές, όπως έχουμε αναφέρει και πιο πάνω, παρέχονται από τους ΠΥΠ, οι οποίοι μπορεί να είναι φορείς,

[136] Άρθρο 1 παράγραφος 1 εδ. 1της οδηγίας 1999/93.
[137] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 159.
[138] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 93.
[139] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 54.
[140] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 159.
[141] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 98 - 99.

φυσικά ή νομικά πρόσωπα, με αρμοδιότητα να εκδίδουν πιστοποιητικά ή να παρέχουν άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές. Τα πιστοποιητικά 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 ΠΥΠ 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»[142]. Υπάρχουν επίσης και 3 Κανονισμοί σχετικά με την «Εθελοντική Διαπίστευση» των ΠΥΠ, την «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[143].

Σύμφωνα με το παράρτημα ΙΙ του π.δ. 150/2001, μεταξύ άλλων, οι ΠΥΠ 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 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 πάροχος δεν ευθύνεται, αν αποδείξει ότι δεν τον βαρύνει πταίσμα (άρθρο 6 παρ. 3 π.δ. 150/2001)[144].

Τέλος, η συλλογή προσωπικών δεδομένων κατά την έκδοση πιστοποιητικού πρέπει να περιορίζεται στο απολύτως απαραίτητο μέτρο. Συγκεκριμένα, ορίζεται ότι οι ΠΥΠ 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 π.δ. 150/2001).

4.5.3 Ορισμός προηγμένης ηλεκτρονικής υπογραφής στο Π.Δ. 150/2001

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 παράγραφος 1, μόνο η «προηγμένη ηλεκτρονική υπογραφή» που βασίζεται σε «αναγνωρισμένο πιστοποιητικό» που εκδίδεται από Πάροχο Υπηρεσιών Πιστοποίησης, ο οποίο πληροί τις προϋποθέσεις του Παραρτήματος ΙΙΙ του π.δ. 150/2001 και δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφής» επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο[145]. Όταν πληρούνται οι προϋποθέσεις αυτές, η ηλεκτρονική υπογραφή αποκτά τις ιδιότητες που χαρακτηρίζουν την ιδιόχειρη υπογραφή και τα ηλεκτρονικά έγγραφα που είναι υπογεγραμμένα με τέτοιο τρόπο εξομοιώνονται πλήρως με τα ιδιωτικά έγγραφα και αποκτούν την ίδια αποδεικτική δύναμη με αυτά.

Το αναγνωρισμένο πιστοποιητικό στο οποίο αναφέρεται η παραπάνω διάταξη, είναι μια ηλεκτρονική βεβαίωση και συνδέει «δεδομένα επαλήθευσης υπογραφής», πρέπει δε να εκδοθεί από τρίτο ανεξάρτητο πρόσωπο, τον Πάροχο Υπηρεσιών Πιστοποίησης (ΠΥΠ). Με το αναγνωρισμένο πιστοποιητικό, που εκδίδεται από τον Πάροχο Υπηρεσιών Πιστοποίησης επιβεβαιώνεται, αφενός μεν η ταυτότητα των προσώπων που χρησιμοποιούν τα κλειδιά, αφετέρου δε, η μοναδικότητα των εκ λόγω κλειδιών[146].

---

[142] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 87 - 88.

[143] Πρόκειται για την απόφαση υπ' αριθμόν 295/63 με τίτλο « Κανονισμός ορισμού φορέων για την διαπίστωση συμμόρφωσης ΑΔΔΥ και ΑΚΜ και προς τα κριτήρια της εθελοντικής διαπίστευσης», την απόφαση 295/64 σχετικά με τον «Έλεγχο συμμόρφωσης ΑΔΔΥ και ΑΚΜ» και την απόφαση 295/63 η οποία αποτελεί τον «Κανονισμό για την εθελοντική διαπίστευση των ΠΥΠ».

[144] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 88 – 90.

[145] Θεόδωρος Σιδηρόπουλος, ο.π., σελ. 159.

[146] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 52.

Το άρθρο 2 παράγραφος 2 του π.δ. 150/2001, το οποίο ορίζει την προηγμένη ηλεκτρονική υπογραφή αποκλίνοντας σημαντικά από τον ορισμό της οδηγίας 1999/93. Σύμφωνα με τη διάταξη αυτή «προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή» ορίζεται η ηλεκτρονική υπογραφή, που πληροί τους εξής όρους[147] [148]:

1. **Συνδέεται μονοσήμαντα με τον υπογράφοντα.** Ο όρος «μονοσήμαντα» έχει την έννοια ότι η κατοχή του ιδιωτικού κλειδιού της ηλεκτρονικής υπογραφής ανήκει σε ένα συγκεκριμένο πρόσωπο.
2. **Είναι ικανή να ταυτοποιήσει (να καθορίσει ειδικά και αποκλειστικά) τον υπογράφοντα.** Ταυτοποίηση είναι η δυνατότητα να διαπιστώνεται ότι το ηλεκτρονικό μήνυμα που φέρει την προηγμένη ηλεκτρονική υπογραφή προήλθε πραγματικά από το φερόμενο ως αποστολέα του. Θα πρέπει λοιπόν, να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος.
3. **Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο**. Ο υπογράφω πρέπει να ελέγχει απόλυτα το ιδιωτικό κλειδί με το οποίο δημιουργεί την υπογραφή του και να αποκλείει τυχόν παρέμβαση από τρίτα πρόσωπα. Για το σκοπό αυτόν, συνήθως το ιδιωτικό κλειδί αποθηκεύεται σε μια «έξυπνη κάρτα»
4. **Συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο , ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.** Είναι απαραίτητο η προηγμένη ηλεκτρονική υπογραφή να μπορεί να αποκαλύπτει τυχόν αλλοιώσεις που επήλθαν στο αρχικό απεσταλμένο ηλεκτρονικό κείμενο. Τη δυνατότητα αυτή την παρέχει η ψηφιακή υπογραφή που δημιουργείται με τη μέθοδο του «δακτυλικού αποτυπώματος».

Η προηγμένη ηλεκτρονική υπογραφή εξασφαλίζει την ακεραιότητα των δεδομένων και την ταυτοποίηση του υπογράφοντος. Επίσης, σε μια ηλεκτρονική συναλλαγή, εξασφαλίζει την αυθεντικότητα του μηνύματος και τη μη αποποίηση της ευθύνης των εμπλεκόμενων μερών, τα οποία δεν μπορούν εκ των υστέρων να αρνηθούν τη συμμετοχή τους στη ηλεκτρονική συναλλαγή.

Η οδηγία 1999/93 στο άρθρο 2 αριθ. 2, παρά το γεγονός ότι αναφέρει τους ίδιους ακριβώς τέσσερις όρους που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή, δεν χρησιμοποιεί την ορολογία «ψηφιακή υπογραφή» διαζευκτικά με την ορολογία «προηγμένη ηλεκτρονική υπογραφή». Αυτό σημαίνει ότι στο προεδρικό διάταγμα περιορίζει την έννοια της προηγμένης ηλεκτρονικής υπογραφής και την ταυτίζει με την ψηφιακή υπογραφή, θεωρώντας έτσι λανθασμένα ότι μόνο η ψηφιακή υπογραφή που βασίζεται στην ασύμμετρη κρυπτογραφία πληροί τα τέσσερα κριτήρια της προηγμένης ηλεκτρονικής υπογραφής. Αντίθετα η οδηγία 1999/93 καλύπτει κάθε προηγμένη ηλεκτρονική υπογραφή που πληροί τα τέσσερα κρίσιμα κριτήρια, έστω και εάν αυτή δεν βασίζεται στην ασύμμετρη κρυπτογραφία. Έχει πολύ μεγάλη πρακτική σημασία το ζήτημα αυτό, λόγω των διαφορετικών έννομων συνεπειών που αναγνωρίζονται από το π.δ. 150/2001 για το κάθε είδος ηλεκτρονικής υπογραφής[149].

Τέλος, Σύμφωνα με τον ορισμό που δίνεται στο άρθρο 2 παράγραφος 12, «προϊόν ηλεκτρονικής υπογραφής» θεωρείται κάθε υλικό ή λογισμικό ή συναφή στοιχεία, τα οποία προορίζονται:

- Είτε για χρήση από τον ΠΥΠ σχετικά με την παροχή των σχετικών υπηρεσιών του (π.χ. κρυπτογραφικές μονάδες για την δημιουργία κρυπτογραφικών κλειδιών).
- Είτε για τη φιλοξενία και ενεργοποίηση των ιδιωτικών κλειδιών και τη δημιουργία της ηλεκτρονικής υπογραφής («διατάξεις δημιουργίας υπογραφής»).

[147] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 99 - 100.
[148] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 159 – 161.
[149] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 100 – 101.

- Είτε, τέλος, για την αυτόματη επαλήθευση μιας ηλεκτρονικής υπογραφής («διατάξεις επαλήθευσης υπογραφής»).

Μετά τη νομοθετική αναγνώριση του κύρους της ηλεκτρονικής υπογραφής είναι δυνατόν πλέον τα ηλεκτρονικά έγγραφα να υποκαταστήσουν τον έγγραφο τύπο, επιτελώντας τις λειτουργίες του. Πρόκειται συγκεκριμένα, πρώτον, για την αποδεικτική λειτουργία του εγγράφου, καθώς μετά τη χορήγηση του πιστοποιητικού τεκμαίρεται ότι η δήλωση βούλησης προέρχεται από τον υπογράφοντα. Πρόκειται, δεύτερον, για τη λειτουργία προσδιορισμού της ταυτότητας του εκδότη, καθώς το κλειδί κρυπτογράφησης παρέχεται από τον ΠΥΠ σε συγκεκριμένο πρόσωπο με το οποίο συνδέεται. Πρόκειται, τρίτον, για τη λειτουργία επιβεβαίωσης του αναλλοίωτου του εγγράφου και τέταρτον, για την εγγυητική λειτουργία, καθώς το πρόσωπο που στέλνει το υπογεγραμμένο με ηλεκτρονική υπογραφή έγγραφο εγγυάται για τη γνησιότητα και την ακρίβεια του περιεχομένου του. Συνέπεια της παραπάνω ρύθμισης είναι ότι το ηλεκτρονικό έγγραφο με την ηλεκτρονική υπογραφή επέχει θέση ιδιωτικού εγγράφου με την έννοια της ΑΚ 160. Αυτό σημαίνει ότι, όπου ο νόμος ή η συμφωνία των μερών επιβάλλουν τον έγγραφο τύπο, η προϋπόθεση αυτή πληρούται και με την ύπαρξη ηλεκτρονικού εγγράφου με προηγμένη ηλεκτρονική υπογραφή, αφού, όπως συνάγεται από το άρθρο 3 παράγραφος 1 του π.δ. 150/2001, το εν λόγω ηλεκτρονικό έγγραφο θεωρείται ιδιωτικό έγγραφο[150].

4.5.4 Η νομική αναγνώριση της προηγμένης ηλεκτρονικής υπογραφής

Στο π.δ. 150/2001 στο άρθρο 3 αριθ. 1 (αντίστοιχο άρθρο 5 αριθ. 1 της οδηγίας 1999/93) ορίζει και ενισχύει με ειδικά νομικά προνόμια μόνο την προηγμένη ηλεκτρονική υπογραφή. Ως προηγμένες ηλεκτρονικές υπογραφές[151], προσδιορίζονται οι ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις: 1) συνδέονται μονοσήμαντα με τον υπογράφοντα, 2) είναι ικανές να ταυτοποιήσουν τον υπογράφοντα, 3) δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και 4) συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση στα εν λόγω δεδομένα (άρθρο 2 αριθ. 2)[152].

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[153]. Πιο συγκεκριμένα, η προηγμένη ηλεκτρονική υπογραφή επέχει θέση ιδιόχειρης υπογραφής, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, μόνο όμως όταν πληροί δυο συγκεκριμένες τεχνικές προϋποθέσεις, αυτές είναι:

α) να βασίζεται σε «αναγνωρισμένο πιστοποιητικό» και

β) να δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφής».

Ως προς την πρώτη προϋπόθεση που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή το «αναγνωρισμένο πιστοποιητικό», ορίζεται από την οδηγία 1999/93 και απο το άρθρο 2 αριθ. 9 του π.δ. 150/2001 και το «πιστοποιητικό» είναι μια ηλεκτρονική βεβαίωση, η οποία εκδίδεται και χορηγείται από τον ΠΥΠ και συνδέει μονοσήμαντα τα «δεδομένα επαλήθευσης υπογραφής» με ένα άτομο επιβεβαιώνοντας την ταυτότητά του, ενώ σύμφωνα με το άρθρο 2 αριθ. 10, «αναγνωρισμένο πιστοποιητικό» είναι ένα πιστοποιητικό που πληροί τους όρους του Παραρτήματος I και εκδίδεται από ΠΥΠ, ο οποίο πληροί του όρους του Παραρτήματος II του π.δ. 150/2001[154].

---

[150] Ελίζα Αλεξανδρίδου, «Το δίκαιο του ηλεκτρονικού εμπορίου», Αθήνα – Θεσσαλονίκη 2010, σελ. 53 – 54.
[151] Σύμφωνα με το εθνικό μας δίκαιο – Π.Δ. 150/2001 - αποκαλούνται και ψηφιακές υπογραφές και σύμφωνα με την Οδηγία 1999/93.
[152] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 95 - 96.
[153] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 4, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Dekalogos_el.pdf (ημερομηνία επίσκεψης: 15/05/2011)
[154] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 106.

Στο σημεία αυτό θα πρέπει να αναφέρουμε ότι, τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν[155] [156]:

- Ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό.
- Τα στοιχεία αναγνώρισης του ΠΥΠ και το κράτος, στο ποιο είναι εγκατεστημένος.
- Το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο.
- Πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό.
- Δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος.
- Ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού.
- Τον κώδικα ταυτοποίησης του πιστοποιητικού.
- Την προηγμένη ηλεκτρονική υπογραφή του ΠΥΠ που το εκδίδει.
- Τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού.
- Τυχόν όριο στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

Επίσης, οι ΠΥΠ που εκδίδουν αναγνωρισμένα πιστοποιητικά πρέπει[157] [158]:

- Να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης, σύμφωνα με τα εκάστοτε ισχύοντα κριτήρια.
- Να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης.
- Να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς.
- Να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευσή της ταυτότητας και ενδεχομένως τυχόν ειδικών χαρακτηριστικών του ατόμου, στο όνομα του όποιου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό.
- Να απασχολούν προσωπικό που διαθέτει την κατάρτιση, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, τεχνογνωσία και εμπειρία στις ηλεκτρονικές υπογραφές και εξοικείωση με τις κατάλληλες διαδικασίες ασφάλειας και να χρησιμοποιούν κατάλληλες διοικητικές και διαχειριστικές διαδικασίες, οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα.
- Να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται έναντι τροποποίησης και να διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά.
- Να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και σε περίπτωση που οι ΠΥΠ παράγει δεδομένα δημιουργίας υπογραφής να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων..
- Να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία 1999/93, ιδίως για την ανάληψη της ευθύνης ζημιών.
- Να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες.

[155] Σύμφωνα με το Παράρτημα I του Π.Δ. 150/2001.
[156] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 96 - 97.
[157] Σύμφωνα με το Παράρτημα II, του Π.Δ. 150/2001
[158] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 97 – 98.

- Να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο ΠΥΠ παρέσχε υπηρεσίες διαχείρισης κλειδιών.
- Πριν συνάψουν συμβατική σχέση με πρόσωπο, που ζητάει πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, συμπεριλαμβανομένων ενδεχόμενων περιορισμών της χρήσης του πιστοποιητικού.
- Να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή έτσι ώστε: 1) μόνο αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις, 2) να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών, 3) να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνο στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου και 4) οι τυχόν αλλαγές που θέτουν σε κίνδυνο τις εν λόγω απαιτήσεις ασφάλειας να γίνονται εμφανώς αντιληπτές από τον χρήστη.

Ως προς τη δεύτερη προϋπόθεση που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή, δηλαδή να δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφή», το άρθρο 2 αριθ. 5 του π.δ. ορίζει ότι «διάταξη δημιουργίας υπογραφής» είναι το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού ή των «δεδομένων δημιουργίας της υπογραφής», δηλαδή των δεδομένων, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής και το οποίο διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής, ενώ σύμφωνα με το άρθρο 2 αριθ. 6, «ασφαλής διάταξη δημιουργίας υπογραφής» είναι η διάταξη δημιουργίας υπογραφής που πληροί τους όρους του Παραρτήματος ΙΙΙ του π.δ. 105/2001[159].

Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον ότι[160]:

α) Τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσία, μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο. Αυτό 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 ΠΥΠ, οι οποίες μεταφέρουν άμεσα τα ιδιωτικά κλειδιά που δημιουργούνται σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφά τους[161].

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. Γίνεται φανερό ότι με την διασφάλιση αυτή, απαγορεύεται η διατήρηση με οποιονδήποτε τρόπο αντιγράφου του ιδιωτικού κλειδιού και επιβάλλεται η χρήση της τεχνολογίας ασύμμετρης κρυπτογραφίας.

γ) Τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.

Επίσης, στο παράρτημα ΙΙΙ 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.

Το άρθρο 3 αριθ. 1 του π.δ. 150/2001 υποχρεώνει τον δικαστή να εφαρμόσει αναλογικά τις επί της ιδιόχειρης υπογραφής ήδη υφιστάμενες διατάξεις εσωτερικού δικαίου και να αποδώσει στην προηγμένη ηλεκτρονική υπογραφή, που βασίζεται σε αναγνωρισμένο

[159] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 108 - 109.
[160] Σύμφωνα με το Παράρτημα ΙΙΙ, του Π.Δ. 150/2001.
[161] Ομάδα Εργασίας Ε2 του ebusinessforum, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 23, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/Paradoteo_E2-Teliko.pdf (ημερομηνία επίσκεψης: 15/05/2011)

πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, την ίδια αποδεικτική δύναμη με την ιδιόχειρη υπογραφή, αποφεύγοντας οποιαδήποτε δυσμενή διάκριση σε βάρος της και αφήνοντας εν ανάγκη ανεφάρμοστη εσωτερική διάταξη, η οποία θα εισήγε ή θα μπορούσε να οδηγήσει σε τέτοιου είδους διακριτική μεταχείριση. Με αντίστοιχο τρόπο τα ηλεκτρονικά έγγραφα, που φέρουν προηγμένη ηλεκτρονική υπογραφή η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται βάσει ασφαλούς διάταξης δημιουργίας υπογραφής, εξομοιώνονται με τα παραδοσιακά υπογεγραμμένα ιδιωτικά έγγραφα[162].

Από την άλλη μεριά η απόδοση πλήρους νομικής ισχύος στην προηγμένη ηλεκτρονική υπογραφή δεν σημαίνει ότι κάθε άλλη μη προηγμένη στερείται παντελώς αποδεικτικής δύναμης. Αντίθετα ορίζεται ότι η ισχύς της ηλεκτρονικής υπογραφής, καθώς και το παραδεκτό της ως αποδεικτικού στοιχείου, δεν αποκλείεται από το λόγο μόνο ότι δεν συντρέχουν οι ως άνω προϋποθέσεις (άρθρο 3 παρ. 2 π.δ. 150/2001)[163].

Με τα πιο πάνω γίνεται φανερό το γεγονός ότι αναγνωρίζεται η προηγμένη ηλεκτρονική υπογραφή πως παρέχει υψηλό επίπεδο ασφάλειας και μπορεί να αντικαταστήσει την ιδιόχειρη υπογραφή επιτελώντας άριστα τις λειτουργίες της[164]:

α) **Την αποδεικτική λειτουργία.** Στο βαθμό που με τη βοήθεια του αναγνωρισμένου πιστοποιητικού τεκμαίρεται ότι η δήλωση βουλήσεως προέρχεται από τον υπογράφοντα.

β) **Τη λειτουργία προσδιορισμού της ταυτότητας του εκδότη.** Αφού το κλειδί κρυπτογράφησης της προηγμένης ηλεκτρονικής υπογραφής παρέχεται από τον ΠΥΠ σε συγκεκριμένο πρόσωπο με το οποίο συνδέεται.

γ) **Τη λειτουργία επιβεβαίωσης του αναλλοίωτου του εγγράφου.** Εφόσον με τη διαδικασία επαλήθευσης της προηγμένης ηλεκτρονικής υπογραφής διαπιστώνεται αν έχει αλλοιωθεί ή όχι το περιεχόμενο του ηλεκτρονικού εγγράφου.

δ) **Την εγγυητική λειτουργία.** Διότι αυτός που αποστέλλει ένα έγγραφο υπογεγραμμένο με την προηγμένη ηλεκτρονική του υπογραφή εγγυάται ουσιαστικά, για τη γνησιότητα και την ακρίβεια του περιεχομένου του εγγράφου.

Από τα πιο πάνω γίνεται αντιληπτό ότι είναι δυνατόν ένα ηλεκτρονικό έγγραφο, το οποίο φέρει προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται βάσει ασφαλούς διάταξης δημιουργίας υπογραφής, να χρησιμοποιηθεί για τη σύναψη δικαιοπραξιών που σύμφωνα με τον Αστικό Κώδικα, πρέπει να περιβληθούν τον έγγραφο τύπο προκειμένου να είναι έγκυρες. Εξάλλου το άρθρο 14 του νόμου 2672/1998, το οποίο αφορά στη διακίνηση εγγράφων με ηλεκτρονικά μέσα, ορίζει στην παράγραφο 22 ότι το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή έχει την αποδεικτική ισχύ εγγράφου που φέρει ιδιόχειρη υπογραφή.

4.5.5 Η νομική αναγνώριση όλων των ηλεκτρονικών υπογραφών

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. Όπως ήδη έχουμε αναφέρει πιο πάνω, το άρθρο 3 παράγραφος 1 του πδ ορίζει ότι «η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή μέθοδο δημιουργίας υπογραφής, επέχει θέση ιδιόχειρης υπογραφής τόσο κατά το ουσιαστικό όσο και στο δικονομικό δίκαιο, επιτρέπονται με τη διατύπωση αυτή την

[162] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 110.
[163] Θεόδωρος Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003, σελ. 86.
[164] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 110 - 111.

ευθεία εφαρμογή των διατάξεων ΑΚ 160 και ΚΠολΔ 443, οι οποίες ορίζουν το ιδιωτικό έγγραφο ως συστατικό τύπο και ως μέσο απόδειξης[165].

Σύμφωνα με το άρθρο 3 παράγραφος 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 έχουν νομική ισχύει αλλά δεν αναγνωρίζονται ως ισότιμες με τις ιδιόχειρες υπογραφές. 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[166].

Με το άρθρο 3 παράγραφος 2 του πδ ορίζεται ότι «η ισχύς της ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο το λόγο ότι δεν συντρέχουν οι προϋποθέσεις που πιο πάνω αναφέρθηκαν». Η διάταξη ετέθη προς αποφυγή επιχειρήματος εξ αντιδιαστολής από την έλλειψη των προϋποθέσεων της παραγράφου 1[167].

Επίσης, σύμφωνα πάντα με το άρθρο 3 παράγραφος 2 του π.δ. 150/2001, η ισχύς μιας ηλεκτρονικής υπογραφής ή το αποδεικτικό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο του, λόγο ότι η ηλεκτρονική υπογραφή: α) δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εκδίδεται από ΠΥΠ ή β) δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής[168].

Από τα πιο πάνω γίνεται αντιληπτό ότι μια απλή ηλεκτρονική υπογραφή δεν απαιτείται να πληροί συγκεκριμένες τεχνικές προϋποθέσεις προκειμένου να αναγνωριστεί νομικά, αλλά είναι δυνατό να στηρίζεται και σε τεχνολογία «χαμηλού» επίπεδο. Επίσης, δεν αποδίδεται συγκεκριμένη αποδεικτική αξία στην απλή ηλεκτρονική υπογραφή, αλλά απλώς προσδιορίζεται ότι για τους λόγους που αναφέρει περιοριστικά η διάταξη δεν μπορεί να απορρίπτεται η νομική ισχύς ή το παραδεκτό του προσκομιζόμενου και βασιζόμενου σε ηλεκτρονική υπογραφή αποδεικτικού μέσου[169].

Από πλευράς ουσιαστικού δικαίου εφόσον συντρέχουν οι προϋποθέσεις της παραγράφου 2 δεν εφαρμόζεται η ΑΚ 160. Η χρήση της απλής ηλεκτρονικής υπογραφής σε ηλεκτρονικά έγγραφα για τα οποία απαιτείται η τήρηση του συστατικού τύπου του ιδιωτικού εγγράφου, θα ισοδυναμεί με έλλειψη κύρους του ιδιωτικού εγγράφου και άρα η δικαιοπραξία θα κρίνεται άκυρη[170]. Όμως σύμφωνα με την αρχή του άτυπου των δικαιοπραξιών του άρθρου 158 ΑΚ, για τις περιπτώσεις που δεν απαιτείται ρητώς ως συστατικός τύπος το ιδιωτικό έγγραφο, ακόμη και η υπογραφή που δεν πληροί τις προϋποθέσεις της παραγράφου 1 του άρθρου 3 θα αρκεί για το έγκυρο των δικαιοπραξιών[171]. Βλέπουμε λοιπόν ότι, 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.

Στο δικονομικό δίκαιο, η απλή ηλεκτρονική υπογραφή δεν οδηγεί υποχρεωτικά στο αποδεικτικό της αποδεικτικής αξίας των δεδομένων με τα οποία συνδέεται. Κατά το άρθρο 444 παράγραφος 3 ΚΠολΔ, κάθε ηλεκτρονικό έγγραφο, δηλαδή και αυτό που δεν φέρει προηγμένη ηλεκτρονική υπογραφή, θεωρείται μηχανική απεικόνιση και συνεπώς βάσει του άρθρου 448 παράγραφος 2 ΚΠολΔ, αποτελεί πλήρη απόδειξη για τα γεγονότα ή πράγματα που

[165] Ιωάννης Κ. Καράκωστας, «Δίκαιο στο Internet, Νομικά Ζητήματα του Διαδικτύου», Αθήνα 2003, σελ. 205.
[166] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 114.
[167] Ιωάννης Κ. Καράκωστας, «Δίκαιο στο Internet, Νομικά Ζητήματα του Διαδικτύου», Αθήνα 2003, σελ. 205.
[168] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 114.
[169] Καραδημητρίου, ο.π., σελ. 114
[170] Σύμφωνα με τις ΑΚ 160 παράγραφος 1 και 159 παράγραφος 1.
[171] Ιωάννης Κ. Καράκωστας, «Δίκαιο στο Internet, Νομικά Ζητήματα του Διαδικτύου», Αθήνα 2003, σελ. 205.

αναγράφει[172]. Ασφαλώς, όμως, δεν δύναται να εξομοιωθεί με την ιδιόχειρη υπογραφή, αφού κάτι τέτοιο θα αντέβαινε στο νόμο και πιο συγκεκριμένα, στο άρθρο 3 παράγραφος 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, η 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 παράγραφος 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.

Συμπερασματικά, η διαφορά ανάμεσα στην απλή και στην προηγμένη ηλεκτρονική υπογραφή, η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, συνίσταται στο ότι η απλή ηλεκτρονική υπογραφή μπορεί να χρησιμοποιηθεί σε όσα έγγραφα δεν απαιτείται, κατά το κοινό δίκαιο, η τήρηση τύπου, ενώ η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής μπορεί να λειτουργεί ως υποκατάστατο της ιδιόχειρης υπογραφής και να χρησιμοποιείται, μεταξύ άλλων, εκεί όπου απαιτείται η τήρηση έγγραφου τύπου. Ενώ η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής μπορεί να λειτουργήσει ως υποκατάστατο της ιδιόχειρης υπογραφής και να χρησιμοποιηθεί μεταξύ άλλων εκεί όπου απαιτείται η τήρηση έγγραφου τύπου. Στις περιπτώσεις αυτές, μια προηγμένη ηλεκτρονική υπογραφή θα μπορεί να προσβληθεί ως πλαστή[173].

4.5.6 Κατηγορίες νομικά αναγνωρισμένων ηλεκτρονικών υπογραφών

Εάν θα θέλαμε να κατηγοριοποιήσουμε τα είδη των ηλεκτρονικών υπογραφών που τυγχάνουν νομικής αναγνώρισης από το π.δ. 150/2001 και από την ευρωπαϊκή οδηγία 1999/93, θα λέγαμε ότι υπάρχουν 4 μεγάλες κατηγορίες, αυτές οι κατηγορίες είναι οι ακόλουθες[174]:

1) Για τις απλές ηλεκτρονικές υπογραφές, στις οποίες περιλαμβάνονται, όπως έχει ήδη αναφερθεί, κάθε μορφής ηλεκτρονικά δεδομένα, τα οποία σχετίζονται με άλλα ηλεκτρονικά δεδομένα, ώστε να χρησιμεύσουν ως μέθοδος απόδειξης της γνησιότητας των δεδομένων αυτών.
2) Για τις προηγμένες ηλεκτρονικές υπογραφές, οι οποίες παρέχουν τεχνολογικά τις εξής ιδιότητες: α) συνδέονται μονοσήμαντα με τον υπογράφοντα, β) είναι ικανές να ταχτοποιούν τον υπογράφοντα, γ) δημιουργούνται με μέσα τα οποία να μπορεί ο υπογράφων να διατηρεί υπό τον αποκλειστικό του έλεγχο και δ) συνδέονται με τέτοιο τρόπο με τα δεδομένα στα οποία αναφέρονται, ώστε να είναι δυνατός ο εντοπισμός κάθε επακόλουθης αλλοίωσης τους. Η μόνη τεχνολογία που παρέχει σήμερα τις συγκεκριμένες δυνατότητες, είναι η τεχνολογία της ψηφιακής υπογραφής, δηλαδή της ασύμμετρης κρυπτογράφησης με ιδιωτικό και δημόσιο κλειδί.
3) Για τις προηγμένες ηλεκτρονικές υπογραφές που είναι αναγνωρισμένες ως ισότητες με τις ιδιόχειρες, οι οποίες διαφοροποιούνται από τις προηγμένες ηλεκτρονικές υπογραφές κατά το γεγονός ότι απαιτούνται ως πρόσθετοι όροι για τη δημιουργία του: α) η υποστήριξή τους από αναγνωρισμένο πιστοποιητικό και β) η χρήση ασφαλούς διάταξης δημιουργίας υπογραφής.

[172] Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008, σελ. 115.
[173] Καραδημητρίου, ο.π., σελ. 116.
[174] Καραδημητρίου, ο.π., σελ. 116 - 118.

4) Υπάρχει και μια ενδιάμεση κατηγορία, η οποία δεν μνημονεύεται ρητά σε κανένα σημείο του κειμένου του π.δ. 150/2001, αλλά αναφέρεται στην αιτιολογική σκέψη 20 του προοιμίου της οδηγίας 1999/93. Πρόκειται για τις «προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό» (αλλά που δεν παράγονται με «ασφαλή διάταξη δημιουργίας υπογραφής», όπως απαιτείται για τις ηλεκτρονικές υπογραφές που είναι ισότιμες με τις ιδιόχειρες), για τις οποίες αναφέρεται χαρακτηριστικά ότι «στοχεύουν σε υψηλότερο επίπεδο ασφάλειας». Η ξεχωριστή αυτή κατηγορία είναι ουσιαστικής σημασίας, γιατί αποτελεί το πλησιέστερο, σε επίπεδο ασφάλειας και αξιοπιστίας, υποκατάστατο της ισότιμης με την ιδιόχειρη ηλεκτρονικής υπογραφής, το οποίο έχουν τη δυνατότητα στην πράξη να παρέχουν στο καταναλωτικό κοινό οι ΠΥΠ. Και αυτό γιατί οι κατασκευαστές ολοκληρωμένων ασφαλών συστημάτων ηλεκτρονικής υπογραφής, τα οποία βάσει του Παραρτήματος ΙΙΙ του π.δ. 150/2001 θεωρούνται συνολικά ως «ασφαλής διάταξη δημιουργίας υπογραφής», δεν είναι ακόμα σε θέση, είτε λόγω του αυξημένου κόστους κατασκευής, είτε λόγω της υψηλής τεχνογνωσίας που απαιτείται, να παρέχουν σε ικανοποιητικό βαθμό τους ΠΥΠ την απαραίτητη τεχνολογία που θα πιστοποιεί ότι μια συγκεκριμένη ηλεκτρονική υπογραφή δημιουργείται με τη χρήση «ασφαλούς διάταξης δημιουργίας υπογραφής».

Τα πολλά και διαφορετικά είδη ηλεκτρονικών υπογραφών, που αναφέραμε πιο πάνω και που θεσμοθετούνται από το π.δ. 150/2001 και την ευρωπαϊκή οδηγία 1999/93, έχουν αντιμετωπιστεί με μια κριτική ματιά από πολλούς, αυτή η κριτική που έχει ασκηθεί αφορά στην σκοπιμότητα και στην αναγκαιότητα της ύπαρξης ενός τέτοιου πολύπλοκου συστήματος. Οι υποστηρικτές της προσέγγισης των δυο επιπέδων κατά τη νομική αναγνώριση των ηλεκτρονικών υπογραφών έχουν δυο πολύ σημαντικά επιχειρήματα, προκειμένου να υποστηρίξουν την εκτεταμένη και αυστηρή κατηγοριοποίησης των ηλεκτρονικών υπογραφών. Αυτά τα επιχειρήματα είναι[175]:

α) ότι μόνο με αυστηρή προδιαγραφή και προτυποποίηση των διαφορετικών ειδών ηλεκτρονικών πιστοποιητικών υπογραφής είναι δυνατόν να επιτευχτεί η διασυνοριακή αξιοπιστία αυτών των προϊόντων και

β) ότι μόνο με συγκριμένο και προδιαγεγραμμένο διαχωρισμό στα χρησιμοποιούμενα είδη ηλεκτρονικών πιστοποιητικών και υπογραφών μπορεί να προστατευθεί ουσιαστικά ο χρήστης-υπογράφων, γιατί έτσι διευκολύνεται ο αποτελεσματικός μηχανικός έλεγχος της υπογραφής και του συνακόλουθου πιστοποιητικού, ώστε πριν ο υπογράφων εναποθέσει την ηλεκτρονική του υπογραφή, να γνωρίζει επακριβώς ποια η ιδιαίτερη νομική σημασία της.

Θα μπορούσαμε να πούμε ότι τα πιο πάνω επιχειρήματα είναι σωστά, όπως σωστή είναι και η υιοθέτηση του συνδυασμού της μινιμαλιστικής και της μαξιμαλιστικής προσέγγισης του θέματος από την πλευρά της Ευρωπαϊκής Ένωσης. Φαίνεται όμως ότι η θεσμοθέτηση τεσσάρων διαφορετικών ειδών ηλεκτρονικής υπογραφής είναι δυνατό να αποτελέσει στην πράξη μια αρκετά περίπλοκη υπόθεση τόσο για τους ΠΥΠ όσο και για τους καταναλωτές. Ο ΠΥΠ είναι αναγκασμένος να ανταποκρίνεται επιτυχώς ανά πάσα στιγμή στην ταυτόχρονη ζήτηση διαφορετικών ειδών ηλεκτρονικής υπογραφής, αυτό ενέχει τον κίνδυνο να αδυνατεί να προσφέρει ποιοτικές υπηρεσίες, υποπίπτοντας σε τεχνικά σφάλματα. Επίσης, οι ΠΥΠ πρέπει να δαπανούν μεγάλα ποσά προκειμένου να διαθέτουν ηλεκτρονικές υπογραφές διαφορετικής τεχνολογίας. Ο καταναλωτής από την πλευρά του είναι αντιμέτωπος με την δυσκολία να επιλέξει μέσα από πολλά τεχνικά χαρακτηριστικά και διαφορετικές έννομες συνέπειες την ηλεκτρονική υπογραφή που ταιριάζει στη χρήση που τον ενδιαφέρει, Επίσης, το υψηλό κόστος των διαφόρων ειδών ηλεκτρονικής υπογραφής φτάνει και στον καταναλωτή. Δυσκολίες είναι πολύ πιθανό να αντιμετωπίσει και ο νομικός κόσμος προκειμένου να κατανοήσουν πλήρως τις διαφορετικές έννομες συνέπειες.

[175] Καραδημητρίου, ο.π., σελ. 119.

4.6 Προτάσεις για την αντιμετώπιση των νομοθετικών προβλημάτων και παραλείψεων

Στις διατάξεις των νομοθετημάτων π.δ. 150/2001 και 1999/93/ΕΚ έχει ασκηθεί από πολλούς κριτική σχετικά με τις παραλείψεις και τις ασάφειες που εμφανίζουν και παράλληλα έχουν προταθεί λύσεις που έχουν ως στόχο τους την αντιμετώπισή τους[176].

4.6.1 Π.Δ. 150/2001

Το άρθρο 1 παράγραφος 2 του π.δ. 150/2001, ορίζει ότι «οι διατάξεις του παρόντος διατάγματος δεν θίγουν διατάξεις που, αναφορικά με την σύνοψη και την ισχύ συμβάσεων ή εν γένει την σύσταση νομικών υποχρεώσεων, επιβάλλουν την 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 ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα». Ωστόσο, αν λάβει κανείς υπόψη τη βούληση και τον σκοπό του κοινοτικού νομοθέτη, όπως αναφέρονται στο προοίμιο της Οδηγίας 1999/93, να προάγει δηλαδή τη χρήση των ηλεκτρονικών υπογραφών, η ανωτέρω διατύπωση θα έπρεπε να είναι πιο συγκεκριμένη. Θα ήταν χρήσιμο δηλαδή, να προβλέπεται συμπληρωματικά πως σε περίπτωση που κάποιος κανόνας του ελληνικού δικαίου προάγει την χρήση των ηλεκτρονικών υπογραφών, τότε αυτός ο κανόνας θα έπρεπε να εφαρμόζεται. Αντίθετα, αν κάποιος κανόνας του εσωτερικού δικαίου εμποδίζει ή αποτρέπει την χρήση των ηλεκτρονικών υπογραφών, τότε αυτός ο κανόνας ενδεχομένως θα έπρεπε να παραμεριστεί. Μια συμπλήρωση και διευκρίνιση του παραπάνω άρθρου θα ήταν ίσως αναγκαία, ώστε ο δικαστής να μην αποφασίζει με αποκλειστικό κριτήριο το γράμμα του νόμου (δηλαδή το άρθρο 1 παράγραφος 2) ποιος κανόνας δικαίου πρέπει να εφαρμοστεί, αλλά να είναι ελεύθερος να κρίνει κατά περίπτωση με κριτήρια τελεολογικά, δηλαδή τον σκοπό διάδοσης των ηλεκτρονικών υπογραφών.

Επίσης, εντοπίζεται και η διαφοροποίηση του Έλληνα νομοθέτη σε σχέση με το κείμενο της Οδηγίας 1999/93, όσο αφορά στον ορισμό της προηγμένης ηλεκτρονικής υπογραφής. Το άρθρο 2 παράγραφος 2 του π.δ. 150/2001 χρησιμοποιεί την ορολογία «ψηφιακή υπογραφή» διαζευκτικά με την ορολογία «προηγμένη ηλεκτρονική υπογραφή». Στο σημείο αυτό ο Έλληνας νομοθέτης περιορίζει χωρίς προφανή λόγο την έννοια της προηγμένης ηλεκτρονικής υπογραφής ταυτίζοντας την με την ψηφιακή, θεωρώντας έτσι λανθασμένα ότι μόνο η ψηφιακή υπογραφή, η οποία βασίζεται στην ασύμμετρη κρυπτογραφία πληροί τα τέσσερα κριτήρια της προηγμένης ηλεκτρονικής υπογραφής[177]. Αντίθετα με τα πιο πάνω, η Οδηγία 1999/93, παρά το γεγονός ότι έχει υποστηριχθεί πως αναφέρεται κατά βάση στις ψηφιακές υπογραφές, καλύπτει με τη διατύπωση της κάθε προηγμένη ηλεκτρονική υπογραφή που πληροί τα τέσσερα κριτήρια, έστω και εάν αυτή δεν στηρίζεται στην ασύμμετρη κρυπτογραφία.

Το άρθρο 3 παράγραφος 2 του π.δ. 150/2001 είναι άλλο ένα σημείο άξιο προσοχής, ο νομοθέτης εδώ παρέχει νομική ισχύ σε όλες τις απλές ηλεκτρονικές υπογραφές. Η παρέκκλιση του π.δ. από την Οδηγία έγκειται στο ότι αυτό κάνει λόγο για την χρήση της ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου χωρίς κανένα περεταίρω προσδιορισμό, υπονοώντας μάλλον την χρήση μόνο στο πεδίο του δικονομικού δικαίου, ενώ θα έπρεπε από την διατύπωση να συνάγεται εμφανώς ότι η ηλεκτρονική υπογραφή συνιστά αποδεκτό αποδεικτικό στοιχείο σε όλες τις νομικές διαδικασίες, δηλαδή όχι μόνο ενώπιον των δικαστηρίων, αλλά και ενώπιων πάσης φύσεως διαιτητικών, διοικητικών και πειθαρχικών οργάνων.

Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθούμε στην αναξιοποίητη δυνατότητα προβλέψεις πρόσθετων απαιτήσεων για την χρήση ηλεκτρονικών υπογραφών στον δημόσιο

[176] Η κριτική που παρουσιάζεται στις επόμενες παραγράφους αφορά στις ασάφειες και τις παραλείψεις των διατάξεων σύμφωνα με τον Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», 2008 σελ. 155 - 177.

[177] Τα κριτήρια αυτά, όπως παρουσιάστηκαν και πιο πάνω στην παρούσα εργασία είναι: 1) Να συνδέεται μονοσήμαντα με τον υπογράφοντα, 2) να είναι ικανή να ταυτοποιήσει τον υπογράφοντα, 3) να δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρεί υπό τον αποκλειστικό του έλεγχο και 4) να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο τέτοιο ώστε να μπορεί να εντοπισθεί οποιαδήποτε επακολουθεί αλλοίωση των εν λόγω δεδομένων.

τομέα, κάτι που δόθηκε σαν δυνατότητα από το άρθρο 3 παράγραφος 7 της οδηγίας 1999/93 και ο Έλληνας νομοθέτης δεν αξιοποίησε παρόλο που στην χώρα μας πολλές δημόσιες υπηρεσίες διαχειρίζονται ευαίσθητα προσωπικά δεδομένα πολιτών και ο δημόσιος τομέας είναι πολύ ευρύς και διαδραματίζει πολύ σημαντικό ρόλο στις συναλλαγές.

Από την πλευρά του Έλληνα νομοθέτη, θα ήταν πολύ αξιόλογες πρωτοβουλίες προς την κατεύθυνση να ενθαρρύνει την χρήση των ηλεκτρονικών υπογραφών, η μέριμνα για την σύνταξη κωδίκων δεοντολογίας μεταξύ καταναλωτών και επαγγελματικών οργανισμών, αλλά και η σύνταξη πολιτικών ηλεκτρονικής υπογραφής, δηλαδή κειμένων με σκοπό την διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών και των πιστοποιητικών τους σε εφαρμογές ομοειδών συναλλακτικών κύκλων, όπως ο δημόσιος τομέας και οι τράπεζες.

4.6.2 Οδηγία 1999/93/ΕΚ

Το πρώτο σημείο αρνητικής κριτικής αναφορικά με την Οδηγία 1999/93/ΕΚ είναι το πρόβλημα της εκτεταμένης κατηγοριοποίησης και της περίπλοκης τεχνικής ορολογίας των ηλεκτρονικών υπογραφών, καθώς πρόκειται για ένα μάλλον περίπλοκο σύστημα, το οποίο δεν παρέχει ευελιξία στην αγορά λόγω της δυσκολίας να παρασχεθούν προϊόντα και υπηρεσίες που να ικανοποιούν τις αυστηρές τεχνικές απαιτήσεις της Οδηγίας. Όσο αφορά την σύνθετη τεχνική ορολογία, αυτή έχει ήδη δημιουργήσει ερμηνευτικά προβλήματα σε δικηγόρους, δικαστές, ΠΥΠ και καταναλωτές.

Επίσης, πέρα από τα τέσσερα κριτήρια τα οποία ο κοινοτικός νομοθέτης έθεσε (άρθρο 2 παράγραφος 2 της Οδηγίας 1999/93) ως απαραίτητα για την στοιχειοθέτηση προηγμένης ηλεκτρονικής υπογραφής, απαραίτητη για την ασφάλεια των συναλλαγών κρίνεται επιπλέον και η χρονοσήμανση της υπογραφής, ώστε να εξασφαλίζεται η έλλειψη δυνατότητας από τα συμβαλλόμενα μέρη της αποποίησης της ευθύνης τους (non repudiation).

Απαραίτητη κρίνεται και η επιβολή υποχρεωτικού προληπτικού ελέγχου στους ΠΥΠ πέρα από τους ήδη θεσπισμένους προαιρετικό προληπτικό έλεγχο (εθελοντική διαπίστευση) και υποχρεωτικό κατασταλτικό έλεγχο από την ΕΕΤΤ. Επίσης, απαραίτητη κρίνεται η αποσαφήνιση του νομικού πλαισίου σχετικά με την εθελοντική διαπίστευση (άρθρο 3 παράγραφος 2 της Οδηγίας 1999/93). Συγκεκριμένα, η Οδηγία αναφέρει ότι οι προϋποθέσεις που συνδέονται με τον εν λόγω μηχανισμό πρέπει να είναι «αντικειμενικές, διαφανείς, ανάλογες και να μην οδηγούν σε διακρίσεις», αλλά δεν γίνεται καμία ειδική αναφορά στο περιεχόμενο και στην ουσία των περιορισμών αυτών. Η ομοιομορφία ως προς τις εθνικές νομοθεσίες στο συγκεκριμένο ζήτημα θα μπορούσε να διασφαλιστεί μόνο μέσα από σαφείς οδηγίες του κοινοτικού νομοθέτη.

Πολύ μεγάλη σημασία πρέπει να δοθεί και στην θέσπιση υποχρεωτικής ασφάλισης αστικής ευθύνης από τον ΠΥΠ, κάτι το οποίο δεν προβλέφθηκε από τον κοινοτικό νομοθέτη. Πολύ δικαιολογημένα θα υποστήριζε κανείς ότι η υποχρεωτική σύναψη σύμβασης ασφάλισης που να καλύπτει τους κινδύνους από την έκδοση αναγνωρισμένων πιστοποιητικών είναι επιβεβλημένη, λόγω των τεράστιων οικονομικών συμφερόντων που μπορεί να διακυβεύονται κατά την διακίνηση εγγράφων μέσω ηλεκτρονικών δικτύων. Μάλιστα, η σύναψη σύμβασης ασφάλισης ίσως επιβάλλεται και από την πιθανή πληθώρα δικών που αναμένεται να προκαλέσει η αντιστροφή του βάρους της απόδειξης στις περιπτώσεις του άρθρου 6 της Οδηγίας. Πιο συγκεκριμένα, στο άρθρο 6 παράγραφος 1 και 2 της Οδηγίας ο νομοθέτης επέλεξε να θεσπίσει την περιορισμένη εφαρμογή της δικονομικής αντιστροφής του βάρους της απόδειξης, δηλαδή μόνο για τις περιπτώσεις που περιγράφονται στο συγκεκριμένο άρθρο. Ωστόσο, με την πάροδο του χρόνου, όταν η λειτουργία της αγοράς και οι ηλεκτρονικές συναλλαγές των καταναλωτών και των σχέσεως τους με τους ΠΥΠ είναι πιο ώριμες, θα καταδειχθεί το κατά πόσο απαιτείται ή όχι να έχει ο ΠΥΠ το βάρος της απόδειξης μόνο για τις περιπτώσεις που περιγράφονται στις παραγράφους 1 και 2 του άρθρου 6.

Τέλος, ένα σημείο που ίσως θα πρέπει να τροποποιηθεί στο άρθρο 6 της Οδηγίας είναι η ανυπαρξία οποιασδήποτε αναφοράς σε υποχρεώσεις από την πλευρά του κατόχου της ηλεκτρονικής υπογραφής, του κατόχου του σχετικού πιστοποιητικού και του καλόπιστου τρίτου. Φυσικά, το βάρος της απόδειξης που έχει ο ΠΥΠ στις περιπτώσεις της παραγράφου 1 και 2 του άρθρου 6 ενθαρρύνει τους καταναλωτές να εμπιστευτούν τις ηλεκτρονικές υπογραφές και να συμμετέχουν στην Κοινωνία της Πληροφορικής. Όμως, ίσως το βάρος αυτό να είναι

δυσανάλογο για τον ΠΥΠ, λόγω της ευκολίας με την οποία οποιοσδήποτε, καλόπιστος ή κακόπιστος κάτοχος ηλεκτρονικής υπογραφής ή αναγνωρισμένου πιστοποιητικού ή ένας τρίτος που βασίζεται σε αυτό μπορεί να κατηγορήσει τον ΠΥΠ για πταίσμα. Η δυσκολία του ΠΥΠ να αποδείξει δικαστικά ότι δεν ευθύνεται θα μπορούσε να οδηγήσει σε ατέρμονους και δαπανηρούς δικαστικούς αγώνες, άρα μια πιο επιεικής για τον ΠΥΠ νομοθετική πρόβλεψη θα έπρεπε να θεσπιστεί στις περιπτώσεις των παραγράφων 1 και 2 του άρθρου 6[178].

4.7. Νομοθετικά κείμενα και Αποφάσεις

Κρίνεται σκόπιμο στο σημείο αυτό να παρουσιάσουμε συγκεντρωτικά την νομολογία και τις αποφάσεις που ισχύουν στην Ελλάδα και αφορούν στο θέμα των ηλεκτρονικών υπογραφών. Πέρα από το Π.Δ. 150/2001 στο οποίο έχουμε αναφερθεί εκτενέστατα στην παρούσα μεταπτυχιακή διατριβή και αφορά στην Προσαρμογή της χώρας μας στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, έχουμε και τα πιο κάτω νομοθετικά κείμενα και αποφάσεις:

Ν.2672/1998 Άρθρο 14: «Διακίνηση εγγράφων με ηλεκτρονικά μέσα».

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. Σύμφωνα με το άρθρο 14 παρ. 2 του ν. 2672/1998 με τον όρο «ψηφιακή υπογραφή» νοείται η ψηφιακής μορφής υπογραφή σε δεδομένα ή συννημένη 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 συνδέεται μονοσήμαντα με τον υπογράφοντα, ταυτοποιεί τον υπογράφοντα, δημιουργείται με μέσα που ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και συνδέεται με τα δεδομένα, στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

Επίσης, ο νόμος 2672/1998 ρυθμίζει την χρήση της ηλεκτρονικής υπογραφής στον δημόσιο τομέα. Ορίζεται η 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 παράγραφο 19 του νόμου 2672/1998, καθορίζονται οι προϋποθέσεις και η διαδικασία έκδοσης, διακίνησης, διαχείρισης και διασφάλισης της ψηφιακής υπογραφής, οι προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, οι τεχνικοί κανόνες για την κατάρτιση, την αποστολή, τη διατήρηση, την αντιγραφή και την αναπαραγωγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εγγύηση ακεραιότητας, διάθεσης και διατήρησης των πληροφοριών που περιέχονται στο μήνυμα καθώς και κάθε άλλη αναγκαία λεπτομέρεια. Επίσης, σύμφωνα με την παράγραφο 20 του νόμου, Η ψηφιακή υπογραφή επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής. Τέλος, η νομική ισχύ των μηνυμάτων ηλεκτρονικής αλληλογραφίας που φέρει ψηφιακή υπογραφή, ορίζεται ότι η τελευταία επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής, κατά την κείμενη νομοθεσία.

Συνοψίζοντας θα λέγαμε ότι με τον νόμο 2672/1998, υπήρξε ο ορισμός του ηλεκτρονικού ταχυδρομείου ως το σύστημα αποστολής και λήψης μηνυμάτων μέσω δικτύου από και προς την ηλεκτρονική διεύθυνση των χρηστών καθώς επίσης και ο ορισμός της ψηφιακής υπογραφής, ως 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 α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, δ) δημιουργεί με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχο του και ε) συνδέεται με τα δεδομένα στα οποία αναφέρατε κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

[178] Ένα παράδειγμα θα μπορούσε να είναι η ειδική νομική υποχρέωση των προσώπων που βασίζονται στο αναγνωρισμένο πιστοποιητικό να ενημερώσουν χωρίς υπαίτια καθυστέρηση τον ΠΥΠ, όταν ανακαλύπτουν ότι μια ηλεκτρονική υπογραφή έχει κλαπεί ή πλαστογραφηθεί ή ότι ένα πιστοποιητικό έχει αλλοιωθεί.

Π.Δ. 342/2002: «Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων».

Τον Οκτώβριο του 2002, εκδόθηκε το Π.Δ. 342/2002 (ΦΕΚ Α' 284/22.11.2002), στο πλαίσιο του άρθρου 14 παρ. 19 και 20 ν. 2672/1998 και το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων μηνυμάτων του ηλεκτρονικού ταχυδρομείου στις επικοινωνίες του δημόσιου τομέα. Πιο αναλυτικά το πδ 342/2002 επικεντρώνεται στην «Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ δημόσιων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών προσώπων». Σύμφωνα με το άρθρο 3 του πδ 342/2002 για την εφαρμογή του παρόντος προεδρικού διατάγματος ισχύουν οι ορισμοί του άρθρου 2 του πδ 150/2001, για δε τις έννομες συνέπειες τα οριζόμενα στο άρθρο 3 του ίδιου πδ. Κατά το άρθρο 4 του πδ 342/2002, οι διατάξεις του πδ 150/2001 για την πρόσβαση στην αγορά, τις αρχές της εσωτερικής αγοράς, τους παρόχους πιστοποίησης, την ευθύνη τους, την προστασία δεδομένων, τους όρους που ισχύουν για αναγνωρισμένα πιστοποιητικά, τη διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής ισχύουν ανάλογα και κατά τη διακίνηση μηνυμάτων με ηλεκτρονικό ταχυδρομείο, κατά τις διατάξεις του άρθρου 1 του πδ 342/2002[179].

Το ρυθμιστικό πεδίο του πδ 342/2002 προσδιορίζεται από τα άρθρα 1 και 2: αποφάσεις, πιστοποιητικά και βεβαιώσεις διακινούνται με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των ΠΝΔΔ και των ΟΤΑ ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, εφόσον φέρουν ψηφιακή υπογραφή (άρθρο 1 παρ. 1 πδ 342/2002). Γνωμοδοτήσεις, αντίγραφα πρακτικών, εισηγήσεις και εκθέσεις διακινούνται με ηλεκτρονικό ταχυδρομείο από υπηρεσίες του δημοσίου, ΝΠΔΔ και ΟΤΑ, προς φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου εφόσον φέρουν ψηφιακή υπογραφή (άρθρο 1 παρ. 2 πδ 342/2002). Πέρα όμως από τη ρύθμιση του άρθρου 1 είναι δυνατή κατά το άρθρο 2 του πδ 342/2002 και η διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο, χωρίς ψηφιακή υπογραφή. Η κατ' αυτόν τον τρόπο διακίνηση επιτρέπεται και έχει νομική ισχύ μεταξύ των υπηρεσιών του δημοσίου, των ΝΠΔΔ και των ΟΤΑ ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή έννομων αποτελεσμάτων ή με την άσκηση δικαιώματος, ιδίως όταν έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, οδηγίες, μελέτες, στατιστικά στοιχεία, αιτήσεις παροχής πληροφοριών αι σχετικές απαντήσεις[180].

Π.Δ. 39.2001: «Καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της Κοινωνίας των Πληροφοριών». Επίσης σε αυτό το προεδρικό διάταγμα ορίζεται και το ηλεκτρονικό εμπόριο. Σύμφωνα με το π.δ. 39.2001, ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων. Το ηλεκτρονικό εμπόριο αποτελεί έκφανση των λεγόμενων υπηρεσιών εξ αποστάσεως.

Απόφαση 248/71: «Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής»

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχή Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β΄/16-5-2002) ρυθμίζει ζητήματα για την έκδοση αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης καθώς και την διαπίστευσή τους. Πιο αναλυτικά, στο άρθρο 3 αναφέρεται ότι η παροχή υπηρεσιών πιστοποίησης οποιασδήποτε μορφής είναι ελεύθερη και δεν υπόκειται σε προηγούμενη άδεια ή έγκριση και στο άρθρο 9 αναφέρεται ότι η ΕΕΤΤ ασκεί την εποπτεία και τον έλεγχο όλων των εγκατεστημένων στην Ελλάδα Παροχών Υπηρεσιών Πιστοποίησης.

[179] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», 2005, σελ. 113.
[180] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης , ο.π., σελ. 114

Απόφαση 295/63: «Κανονισμός ορισμού φορέων για την διαπίστωση συμμόρφωσης ΑΔΔΥ και ΑΚΜ και προς τα κριτήρια της εθελοντικής διαπίστευσης»[181]

Με την Απόφαση 295/63/10-10-2003 Απόφαση της ΕΕΤΤ προσδιορίζεται η διαδικασία ορισμού Φορέων για τη διαπίστωση συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα κριτήρια Εθελοντικής Διαπίστευσης. Στο Παράρτημα 1 της Απόφασης αναφέρονται τα κριτήρια ορισμού Φορέα.

Η διαδικασία συνοπτικά έχει ως ακολούθως:

- Ο αιτών τον ορισμό του ως Φορέας για Εθελοντική Διαπίστευση καταθέτει αίτηση στην ΕΕΤΤ με την οποία αιτείται τον ορισμό του, υποβάλλοντας προς τούτο όλα τα απαιτούμενα δικαιολογητικά που αναφέρονται στο Παράρτημα Ι του Κανονισμού 295/63 (ΦΕΚ 1730/Β/24-11-03).
- Επιτροπή Ελέγχου οριζόμενη από την ΕΕΤΤ διενεργεί έλεγχο στον τόπο εγκατάστασης και λειτουργίας του αιτούντος τον ορισμό του.
- Η Επιτροπή Ελέγχου συντάσσει Έκθεση Αξιολόγησης του αιτούντος και την υποβάλλει στην ΕΕΤΤ η οποία με αιτιολογημένη απόφασή της αποφασίζει για τον Ορισμό του αιτούντος.

Η ΕΕΤΤ τηρεί Μητρώο των Φορέων για Εθελοντική Διαπίστευση, οι οποίοι ορίσθηκαν ως αρμόδιοι να διενεργούν τους Ελέγχους Συμμόρφωσης σύμφωνα με τις διατάξεις του Κανονισμού 295/63/10-10-2003. Στο εκάστοτε Μητρώο αναγράφονται τα στοιχεία του Φορέα Ελέγχου (επωνυμία, διακριτικός τίτλος, έδρα, ΑΦΜ, νόμιμοι εκπρόσωποι) η περιγραφή του αντικειμένου και της χρονολογίας του ορισμού του. Στο ίδιο Μητρώο αναγράφεται κάθε τροποποίηση του ορισμού, καθώς και οποιαδήποτε αναστολή ή ανάκλησή του. Το Μητρώο Φορέων για Εθελοντική Διαπίστευση είναι στην ιστοσελίδα του ΕΕΤΤ.

Η ΕΕΤΤ εποπτεύει τους Φορείς για Εθελοντική Διαπίστευση με σκοπό να διασφαλισθεί η εφαρμογή του σχετικού ρυθμιστικού πλαισίου σχετικά με τις Ηλεκτρονικές Υπογραφές, διενεργώντας ελέγχους που πραγματοποιούνται αυτεπαγγέλτως ή κατόπιν καταγγελίας.

Προς το παρόν δεν έχει οριστεί Φορέας για τη διαπίστωση συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα κριτήρια Εθελοντικής Διαπίστευσης.

Απόφαση 295/65: «Κανονισμός για την εθελοντική διαπίστευση των ΠΥΠ»[182]

Με την Απόφαση της ΕΕΤΤ 295/65 «Κανονισμός για την Εθελοντική Διαπίστευση των παρόχων υπηρεσιών πιστοποίησης» (ΦΕΚ 1730/Β/24-11-03) προσδιορίζονται τα κριτήρια και η διαδικασία εθελοντικής διαπίστευσης.

Παρακάτω συνοπτικά παρέχονται πληροφορίες σχετικά με το εθνικό σχήμα Εθελοντικής Διαπίστευσης των παρόχων υπηρεσιών πιστοποίησης ηλ. υπογραφής. Τα κριτήρια για την Εθελοντική Διαπίστευσης του παρόχου είναι τα ακόλουθα :

- Ο ΠΥΠ αποδεικνύει τη συμμόρφωσή του με τις απαιτήσεις του ΠΔ 150/2001 και της Απόφασης της ΕΕΤΤ 248/71/2002 και με κάθε άλλη ρύθμιση που αφορά στην έκδοση Αναγνωρισμένων Πιστοποιητικών.
- Οι δικαιούχοι, στους οποίους έχει χορηγηθεί πιστοποιητικό συμμόρφωσης Ασφαλών Κρυπτογραφικών Μονάδων ή Ασφαλών Διατάξεων Δημιουργίας Υπογραφής, σύμφωνα με τις διατάξεις της Απόφασης ΑΠ 295/64/2003 της ΕΕΤΤ «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων», οφείλουν να μεριμνούν για την εκπλήρωση των απαιτήσεων περιβάλλοντος χώρου ώστε να διασφαλίζονται οι ακόλουθες λειτουργίες: α) παραγωγή των Δεδομένων Δημιουργίας Υπογραφής που χρησιμοποιούν για την

[181] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/InfoConfxrmityAssess.html (ημερομηνία επίσκεψης: 30/09/2011)

[182] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/InfoNVAS.html (ημερομηνία επίσκεψης: 30/09/2011)

υπογραφή των Αναγνωρισμένων Πιστοποιητικών των δικαιούχων και για την υπογραφή της πληροφορίας σχετικά με την κατάσταση των Πιστοποιητικών, β) παραγωγή των Δεδομένων Δημιουργίας Υπογραφής των δικαιούχων Αναγνωρισμένων Πιστοποιητικών, γ) υπογραφή των Αναγνωρισμένων Πιστοποιητικών των δικαιούχων, δ) υπογραφή της πληροφορίας σχετικά με την κατάσταση των Πιστοποιητικών.

- Η ασφάλεια των παρεχόμενων υπηρεσιών του ΠΥΠ πρέπει να έχει διαπιστωθεί από Φορέα για Εθελοντική Διαπίστευση σύμφωνα με τη διαδικασία που ορίζεται στο άρθρο 5 του Κανονισμού για την Εθελοντική Διαπίστευση (ΑΠ. ΕΕΤΤ 295/65).
- Ο ΠΥΠ που δηλώνει προς τους δικαιούχους Αναγνωρισμένων Πιστοποιητικών, στην ΕΕΤΤ ή σε τρίτους ότι τα Δεδομένα Δημιουργίας Υπογραφής των δικαιούχων Αναγνωρισμένων Πιστοποιητικών παράγονται ή αποθηκεύονται σε ή εφαρμόζονται με Ασφαλή Διάταξη Δημιουργίας Υπογραφής, οφείλει να είναι σε θέση να τεκμηριώνει, πώς διασφαλίζει το γεγονός αυτό.

Η διαδικασία για την εθελοντική διαπίστευση ενός παρόχου ξεκινά κατόπιν αιτήσεως του ενδιαφερόμενου ΠΥΠ σε Φορέα για Εθελοντική Διαπίστευση. Ο Φορέας για Εθελοντική Διαπίστευση ελέγχει την ασφάλεια των παρεχόμενων υπηρεσιών του ΠΥΠ όσον αφορά την καταλληλότητα των μέτρων ασφάλειας και της υλοποίησης αυτών στην πράξη. Ο ΠΥΠ υποβάλει στον Φορέα για Εθελοντική Διαπίστευση τα ακόλουθα έγγραφα:

α) Πιστοποιητικά συμμόρφωσης που χορηγήθηκαν από Φορέα για Προϊόντα, τα οποία πρέπει να αντιστοιχούν στα προϊόντα που χρησιμοποιεί ο ΠΥΠ Ο Φορέας για Εθελοντική Διαπίστευση ελέγχει ιδίως την ισχύ των ως άνω Πιστοποιητικών και εάν οι απαιτήσεις περιβάλλοντος χώρου που αναφέρονται σε αυτά υλοποιούνται αποτελεσματικά από τον ΠΥΠ.

β) Έκθεση μέτρων ασφαλείας που περιλαμβάνει τουλάχιστον :

- περιγραφή των εγκαταστάσεων και όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων ασφάλειας και της καταλληλότητάς τους,
- τον κατάλογο των προϊόντων που χρησιμοποιούνται για τη δημιουργία Προηγμένων Ηλεκτρονικών Υπογραφών,
- τα προβλεπόμενα μέτρα ασφάλειας προκειμένου να διατηρηθούν σε αδιάλειπτη λειτουργία οι παρεχόμενες υπηρεσίες, ιδίως σε καταστάσεις έκτακτης ανάγκης,
- τα μέτρα προστασίας αρχείων και δεδομένων,
- περιγραφή των διαδικασιών εξασφάλισης της αξιοπιστίας του απασχολούμενου προσωπικού,
- τα κείμενα τα οποία περιγράφουν την Πολιτική Πιστοποίησης και τη Δήλωση Πρακτικής του ΠΥΠ.

Ο Φορέας για Εθελοντική Διαπίστευση ελέγχει, διεξάγοντας προς τούτο αυτοψία, την υλοποίηση στην πράξη των περιγραφόμενων στην Έκθεση μέτρων ασφάλειας. Στην περίπτωση διαπίστωσης συμμόρφωσης του ΠΥΠ, ο Φορέας για Εθελοντική Διαπίστευση χορηγεί Πιστοποιητικό Συμμόρφωσης. Η αξιολόγηση του Εθελοντικά Διαπιστευμένου ΠΥΠ για τη διαπίστωση της συμμόρφωσής του επαναλαμβάνεται κάθε τρία (3) έτη.

Η Διαδικασία Εθελοντικής Διαπίστευσης των ΠΥΠ περιγράφεται στο άρθρο 6 του Κανονισμού για την Εθελοντική Διαπίστευση των Παρόχων Υπηρεσιών Πιστοποίησης (ΑΠ. ΕΕΤΤ 295/65). Ο αιτών την Εθελοντική του Διαπίστευση θα πρέπει να καταθέσει έγγραφη αίτηση στην ΕΕΤΤ προσκομίζοντας το σύνολο των εγγράφων που αναφέρονται στο άρθρο 6 παρ. 2 της Απόφασης 295/65. Στα εν λόγω έγγραφα περιλαμβάνεται, μεταξύ άλλων, και το Πιστοποιητικού Συμμόρφωσης που εξέδωσε ο Φορέας για Εθελοντική Διαπίστευση. Η ΕΕΤΤ, λαμβάνοντας υπόψη τα ανωτέρω, εκδίδει αιτιολογημένη απόφασή της για την Εθελοντική Διαπίστευση του αιτούντα.

Η ΕΕΤΤ εποπτεύει τους διαπιστευμένους Παρόχους Υπηρεσιών Πιστοποίησης. Προς το σκοπό αυτό, η ΕΕΤΤ ή τα οριζόμενα από την ΕΕΤΤ πρόσωπα έχουν το δικαίωμα αυτεπαγγέλτως ή κατόπιν καταγγελίας να ζητούν στοιχεία και να προβαίνουν σε επιθεωρήσεις

στους χώρους εγκατάστασης και λειτουργίας των διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης.

Προς το παρόν δεν έχουν οριστεί Φορείς για τη διαπίστωση συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα κριτήρια Εθελοντικής Διαπίστευσης.

Απόφαση 295/64 : «Κανονισμός για τον έλεγχο συμμόρφωσης ΑΔΔΥ και ΑΚΜ»[183]

Με την υπ. αρ. 295/63 Απόφαση της ΕΕΤΤ «Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων και φορέων για τη διαπίστωση διαμόρφωσης των παρόχων υπηρεσιών πιστοποίησης προς τα κριτήρια Εθελοντικής Διαπίστευσης» (ΦΕΚ 1730/Β/24-11-03) η ΕΕΤΤ προσδιόρισε τη διαδικασία ορισμού των Εντεταλμένων Φορέων που θα διαπιστώνουν τη συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής (smartcards κ.λπ) και ασφαλών κρυπτογραφικών μονάδων προς το Παράρτημα ΙΙΙ και ΙΙ στ του Π.Δ. 150/2001, αντίστοιχα.

Ενδιαφερόμενοι Φορείς που πληρούν τα κριτήρια ορισμού για τη διεξαγωγή των εν λόγω ελέγχων συμμόρφωσης μπορούν να αιτηθούν τον ορισμό τους στην ΕΕΤΤ υποβάλλοντας την αντίστοιχη αίτηση και τα απαιτούμενα δικαιολογητικά.

Οι φορείς που ορίζονται από την ΕΕΤΤ για τον έλεγχο συμμόρφωσης των προϊόντων εγγράφονται στο Μητρώο της ΕΕΤΤ «Μητρώο Εντεταλμένων φορέων για τον έλεγχο των προϊόντων ηλεκτρονικής υπογραφής».

Με την υπ. αρ. 295/64 Απόφαση της ΕΕΤΤ «Κανονισμός για τον έλεγχο συμμόρφωσης ασφαλών διατάξεων δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων» (ΦΕΚ 1730/Β/24-11-03) η ΕΕΤΤ προσδιόρισε τα κριτήρια και τη διαδικασία ελέγχου συμμόρφωσης των ασφαλών Διατάξεων Δημιουργίας Υπογραφής και των Ασφαλών Κρυπτογραφικών Μονάδων προς τα παραρτήματα ΙΙΙ και ΙΙ στ) του Π.Δ. 150/2001, αντίστοιχα.

Κατασκευαστές ή εξουσιοδοτημένοι αντιπρόσωποι μπορούν να απευθύνονται σε Εντεταλμένους Φορείς για τα προϊόντα για να διαπιστώσουν τη συμμόρφωση των προϊόντων τους ως προς τα παραρτήματα ΙΙΙ και ΙΙ του Π.Δ. 150/2001.

Στην περίπτωση συμμόρφωσης ο Εντεταλμένος Φορέας εκδίδει πιστοποιητικό συμμόρφωσης. Τα προϊόντα για τα οποία έχει χορηγηθεί πιστοποιητικό συμμόρφωσης εγγράφονται στο Μητρώο της ΕΕΤΤ «Μητρώο προϊόντων ηλεκτρονικής υπογραφής».

Προς το παρόν δεν έχουν οριστεί Φορείς για τον έλεγχο συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής.

Στο σημείο αυτό θα πρέπει να αναφέρουμε, έστω και επιγραμματικά, τον «Κανονισμός Επικοινωνίας Δημόσιων Υπηρεσιών» (ΚΕΔΥ) και την Εγκύκλιο ΔΙΑΔΠ/Α1/2523/4-2-1999 περί διακίνησης εγγράφων με ηλεκτρονικά μέσα, του Υπουργείου Δημόσιας Διοίκησης και Αποκέντρωσης Διεύθυνση Απλούστευσης Διαδικασιών και Παραγωγικότητας – Διευκρινήσεις. Θέμα αυτής της Εγκυκλίου είναι η διακίνηση εγγράφων μεταξύ Δημοσίου Ν.Π.Δ.Δ. και Ο.Τ.Α. και ιδιωτών με ηλεκτρονικά μέσα (τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο). Διευκρινήσεις στις διατάξεις του άρθρου 14 του Ν. 2672/1998 (ΦΕΚ 290/Α').

Εκτός από το νομικό πλαίσιο που ισχύει στην Ελλάδα θα πρέπει να κάνουμε και μια σύντομη αναφορά στο Ευρωπαϊκό πλαίσιο. Η Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, έχει παρουσιαστεί αναλυτικά στην παρούσα μεταπτυχιακή διατριβή, έχουμε επίσης σε ευρωπαϊκό επίπεδο α) την **Απόφαση 6 Νοεμβρίου 2000** της Επιτροπής Ηλεκτρονικής υπογραφής (άρθρο 9 Οδηγίας 99/93/ΕΕ) για τα ελάχιστα κριτήρια που θα πρέπει να πληρούν οι αρμόδιοι φορείς για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής, β) την **Οδηγία 98/34/ΕΚ** για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών καθώς και την τροποποίησή της από την

[183] Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/entetalm_foreis_HY.html (ημερομηνία επίσκεψης: 30/09/2011)

Οδηγία 98/48/ΕΚ) και γ) την **Απόφαση της Επιτροπής της 14ης Ιουλίου 2003** σχετικά με τη δημοσίευση αριθμών αναφοράς γενικά αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής, σύμφωνα με την Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

5. Το σύστημα υλοποίησης Ψηφιακής Υπογραφής PGP (Pretty Good Privacy)

5.1 Εισαγωγή

Κρίνουμε σκόπιμο να παρουσιάσουμε σε αυτό το σημείο, το πρόγραμμα PGP (Pretty Good Privacy), το οποίο είναι ένα από τα πιο διαδεδομένα προγράμματα υλοποίησης ψηφιακών υπογραφών. Το σύστημα PGP σχεδιάστηκε και δημιουργήθηκε από τον καθηγητή του MIT Philip Zimmermann το 1991, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες. Επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο[184] και την πιστοποίηση της ταυτότητας[185] σε συνδυασμό με την ευκολία λειτουργίας, δηλαδή η διασφάλιση του απόρρητου και η πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι συνεπώς, αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το σύστημα PGP κάνει χρήση της κρυπτογραφίας «δημοσίου κλειδιού» (public key).

Το PGP θα μπορούσαμε να πούμε ότι είναι μια εναλλακτική μέθοδος πιστοποίησης των δημοσίων κλειδιών ενός χρήστη, η οποία βασίζεται στα «αυτό - υπογραφόμενα πιστοποιητικά» που εκδίδονται από το ίδιο τον τελικό χρήστη (κάτοχο του συγκεκριμένου ζεύγους κρυπτογραφικών κλειδιών), ο οποίος λειτουργεί παράλληλα και ως «αποδέκτης». Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους «εξυπηρετητές κλειδιών» (key servers), απ' όπου λαμβάνονται, αξιολογούνται και πιθανώς υπογράφονται και από άλλους χρήστες, οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο - κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Το PGP λοιπόν, θα λέγαμε ότι είναι ένα σύστημα αλληλοπιστοποιησης το οποίο βασίζεται στην δημιουργία ενός αποκεντρωμένου «δικτύου εμπιστοσύνης» (web of trust) που αναπτύσσεται με την μεταβίβαση της εμπιστοσύνης μεταξύ των χρηστών της.

Το PGP κάνει χρήση της ασύμμετρης κρυπτογράφησης με δημόσιο κλειδί και ιδιωτικό κλειδί. Χρησιμοποιείται συχνότερα για την κρυπτογράφηση και την υπογραφή ηλεκτρονικών αντικειμένων και γίνεται ευρεία χρήση αυτό του συστήματος στην αποστολή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνήθως μεταξύ ιδιωτών και οργανισμών αλλά, χρησιμοποιείται επίσης και ως τμήμα μιας ασφαλούς υποδομής ηλεκτρονικού εμπορίου, για παράδειγμα για την κρυπτογράφηση παραγγελιών από τον εξυπηρετητή διαδικτύου στο τμήμα που θα τις εκτελέσει.

Στην παρακάτω εικόνα φαίνεται ένα κωδικοποιημένο μήνυμα με την χρήση του συστήματος PGP, για να μπορέσουμε να δούμε ποιο είναι το μήνυμα και να μπορέσουμε να το αποστείλουμε σαν συνημμένο αρχείο μέσω ηλεκτρονικού ταχυδρομείου, μπορούμε να το κάνουμε με την χρήση ενός κειμενογράφου και το κείμενο έχει περίπου την μορφή που παρουσιάζεται στην εικόνα. Αυτό το κείμενο αποτελεί το δημόσιο κλειδί μας και μπορούμε εάν θέλουμε να το αποθηκεύσουμε ως αρχείο στον υπολογιστή μας και το επισυνάψουμε και να το αποστείλουμε μέσω ηλεκτρονικού ταχυδρομείου, σε όσα άτομα θέλουμε να επικοινωνήσουν μαζί μας κρυπτογραφημένα.

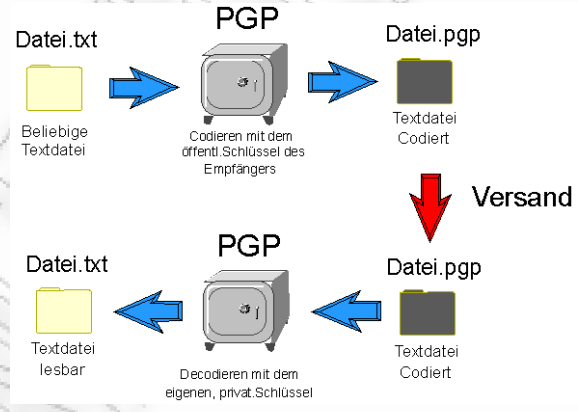
[184] Η διασφάλιση του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το αναγνώσει.

[185] Η πιστοποίηση της ταυτότητας σημαίνει ότι τα μηνύματα που φαίνεται πως έχουν αποσταλεί από κάποιο συγκεκριμένο αποστολέα, μπορούν να έχουν αποσταλεί μόνο από αυτόν και δεν υπάρχει πιθανότητα να έχει παρέμβει στα μηνύματα αυτά κάποιος τρίτος.

```
-----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
FO7v9BdvuIvK7vcWAKC7g1yH52+cVTqlNAs90J7USepJHA==
=H66o
-----END PGP PUBLIC KEY BLOCK-----
```

Εικόνα 19. Κωδικοποιημένα Μηνύματα

Το PGP κρυπτογραφεί τα μηνύματα με IDEA, διανέμει τα κλειδιά κρυπτογραφώντας τα με RSA και δημιουργεί ψηφιακές υπογραφές στα μηνύματα με MDS και RSA. Για την κυριότητα των κλειδιών το PGP δεν επαφίεται σε κάποια κεντρική αρχή αλλά, σε ένα δίκτυο εμπιστοσύνης, δηλαδή κάθε κλειδί υπογράφεται από τα άλλα κλειδιά και τελικά η εμπιστοσύνη του χρήστη σε κάποιο κλειδί εξαρτάται από την μπιστοσύνη του ίδιου στα κλειδιά που υπέγραψαν το συγκεκριμένο κλειδί. Το PGP έχει τυποποιηθεί ως OpenPGP.



Εικόνα 20. Διαδικασία λειτουργία της εφαρμογής PGP Pretty Good Privacy

Το PGP λοιπόν, σύμφωνα με τα όσα αναφέραμε πιο πάνω θα μπορούσαμε να πούμε ότι, συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον, εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

5.2 Η Λειτουργία του PGP

Για να μπορέσουμε να κατανοήσουμε καλύτερα τη λειτουργία του συστήματος PGP, θα πρέπει να αναφέρουμε πρώτα κάποια πράγματα για τα συμβατικά κρυπτοσυστήματα και τα κρυπτοσυστήματα δημόσιων κλειδιών. Ας υποθέσουμε λοιπόν, ότι κάποιος επιθυμεί να αποστείλει ένα ηλεκτρονικό μήνυμα και δεν επιθυμεί να το αναγνώσει κανένας άλλος παρά μόνο ο παραλήπτης στον οποίο προορίζεται το μήνυμα. Ο αποστολέας έχει την δυνατότητα να το κρυπτογραφήσει το ηλεκτρονικό μήνυμα με τη χρήση ενός κλειδιού, το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη, αυτή είναι η μέθοδος βάσει της οποίας λειτουργεί η συμβατική κρυπτογραφία ενός κλειδιού.

Σε όλα τα συμβατικά κρυπτοσυστήματα, όπως είναι για παράδειγμα το DES, κάνουν χρήση ενός μόνο κλειδιού το οποίο χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης του μηνύματος από τον αποστολέα και κατά την διαδικασία της αποκρυπτογράφηση του από τον παραλήπτη. Αυτό ουσιαστικά σημαίνει ότι το ένα και μοναδικό κλειδί θα πρέπει να μεταδοθεί αρχικά μέσα από ένα ασφαλές κανάλι έτσι ώστε και τα δυο μέρη να το γνωρίζουν προτού αρχίσει η αποστολή κρυπτογραφημένων ηλεκτρονικών μηνυμάτων μέσω ασφαλών καναλιών. Αυτό το σύστημα συμμετρικής κρυπτογραφίας ενέχει πολλούς κινδύνους όπως έχουν αναφερθεί και πιο πάνω στην παρούσα μεταπτυχιακή διατριβή.

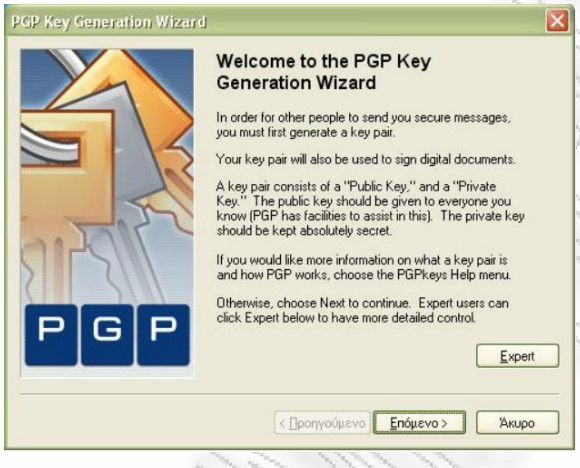
Σε αντίθεση με την συμμετρική κρυπτογραφία, όλα τα κρυπτοσυστήματα ασύμμετρης κρυπτογραφίας κάνουν χρήση δημοσίων κλειδιών, ο κάθε χρήστης έχει δυο συμπληρωματικά κλειδιά. Το ένα κλειδί δίδεται δημόσια (public key) και το άλλο κλειδί είναι μυστικό (secret key ή private key). Όπως αναφέραμε και πιο πάνω στο κεφάλαιο της ασύμμετρης κρυπτογραφίας η γνώση του δημοσίου κλειδιού δεν βοηθάει στην εξαγωγή του αντίστοιχου μυστικού κλειδιού. Το δημόσιο κλειδί μπορεί να διατεθεί σε ένα ανοικτό δίκτυο επικοινωνιών. Αυτό παρέχει διασφάλιση του απόρρητου χωρίς την ανάγκη ύπαρξης ασφαλών καναλιών, όπως απαιτεί η συμβατική - συμμετρική κρυπτογραφία. Στην ασύμμετρη κρυπτογραφία κάθε χρήστης μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός ηλεκτρονικού μηνύματος για να κρυπτογραφήσει ένα ηλεκτρονικό μήνυμα και να το αποστείλει προς αυτό το άτομο ενώ αντίθετα ο παραλήπτης μπορεί να χρησιμοποιήσει το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το ηλεκτρονικό μήνυμα. Μόνο ο παραλήπτη μπορεί να το αποκρυπτογραφήσει διότι κανένας άλλος δεν έχει πρόσβαση στο μυστικό κλειδί.

Το μυστικό - ιδιωτικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του ηλεκτρονικού μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του ηλεκτρονικού μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. Αυτό αποδεικνύει ότι ο αποστολέας ήταν ο πραγματικός δημιουργός του μηνύματος και ότι το μήνυμα δεν αλλοιώθηκε από κάποιον άλλον διότι μόνο ο αποστολέας έχει στην κατοχή του το μυστικό κλειδί που έφτιαξε την υπογραφή. Η πλαστογράφηση ενός υπογεγραμμένου μηνύματος δεν είναι εφικτή και ο αποστολέας δεν μπορεί μετά να απαρνηθεί την υπογραφή του.

Αυτές οι δυο διαδικασίες μπορούν να συνδυαστούν για την παροχή τόσο διασφάλισης του απόρρητου όσο και πιστοποίησης της ταυτότητας αφού μπορεί κάποιος πρώτα να υπογράψει ένα μήνυμα με το μυστικό κλειδί του και μετά να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αντιστρέφει αυτά τα βήματα αποκρυπτογραφώντας πρώτα το μήνυμα με το μυστικό κλειδί του και κατόπιν ελέγχοντας την ψηφιακή υπογραφή που περιέχεται σε αυτό με το δημόσιο κλειδί του αποστολέα. Αυτές οι διαδικασίες γίνονται αυτόματα από το λογισμικό του παραλήπτη.

Επειδή ο αλγόριθμος της ασύμμετρης κρυπτογραφία δημοσίων κλειδιών είναι πολύ πιο αργός από την συμμετρική κρυπτογραφία ενός κλειδιού η κρυπτογράφηση επιτυγχάνεται καλύτερα με τη χρήση ενός υψηλής ποιότητας γρήγορου αλγόριθμου συμβατικής κρυπτογραφίας ενός κλειδιού για την κρυπτογράφηση του μηνύματος. Το αρχικό μη κρυπτογραφημένο μήνυμα καλείται «απλό κείμενο». Σε μια διαδικασία αόρατη στο χρήστη ένα προσωρινό τυχαίο κλειδί, το οποίο έχει δημιουργηθεί μόνο για τη συγκεκριμένη φορά, χρησιμοποιείται για να κρυπτογραφηθεί συμβατικά το αρχείο «απλό κείμενο». Μετά το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για να κρυπτογραφηθεί αυτό το προσωρινό κλειδί. Αυτό

το συμβατικά δημιουργημένο κλειδί μιας φοράς (session key) το οποίο έχει κρυπτογραφηθεί και με τη διαδικασία του δημόσιου κλειδιού αποστέλλεται μαζί με το κρυπτογραφημένο κείμενο (κρυπτοκείμενο) στον παραλήπτη. Ο παραλήπτης χρησιμοποιεί το δικό του μυστικό κλειδί για να ανακτήσει το session key και μετά χρησιμοποιεί αυτό κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο. Στην πιο κάτω εικόνα φαίνεται το αρχικό παράθυρο στην εφαρμογή PGP για την δημιουργία ιδιωτικού και δημόσιου κλειδιού.



Εικόνα 21. Έναρξη οδηγού κατασκευής κλειδιών

Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη), μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε και τέλος το ίδιο το υλικό του κλειδιού. Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια αρχεία κλειδιών περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά αρχεία κλειδιών περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα «key id» (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Όταν αυτή η ταυτότητα παρουσιάζεται μόνο τα 32 λιγότερο σημαντικά bits δίνονται για επιπλέον ελαχιστοποίηση του όγκου της ταυτότητας. Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολλή δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Είναι κάτι ανάλογο με το «check sum» ή CRC κώδικα ελέγχου στο ότι αντιπροσωπεύουν συμπαγώς το μήνυμα και χρησιμοποιούνται για την ανίχνευση αλλαγών σε αυτό. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή

τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο αρχείο δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο αρχείο μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι αρχείων κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε αρχεία κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος αρχείων. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του αρχείο κλειδιών.

Το σύστημα PGP δίνει την δυνατότητα στον χρήστη που το χρησιμοποιεί, να βλέπει πληροφορίες όπως την Key ID του κλειδιού, το μέγεθός του, τις ημερομηνίες δημιουργίας και τερματισμού ύπαρξής του, την εικόνα, αν έχουμε εισάγει πιο πριν. Επίσης, ο χρήστης μπορεί να δει το Fingerprint «Δακτυλικό αποτύπωμα» και έχει την δυνατότητα να ορίσει το πεδίο εμπιστευτικότητας του κλειδιού, μέσα σε μία κλίμακα Untrusted-Trusted. Κάθε κλειδί στην ουσία αποτελείται από ένα signing key και ένα encryption subkey. Έχουμε την δυνατότητα να δημιουργήσουμε πολλά encryption subkeys, τα οποία μπορούμε να τα 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.

5.3 Προστασία Δημοσίων Κλειδιών

Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών, διότι το επιδιωκόμενο είναι η όσο το δυνατόν ευρύτερη διάδοσή τους. Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν. Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών.

Ο μόνος τρόπος να αποτραπούν τέτοιες καταστάσεις είναι η αποφυγή της υποκλοπής και του μπερδέματος των δημοσίων κλειδιών. Μία διέξοδος σε αυτό το πρόβλημα είναι η χρήση κάποιου «τρίτου» κοινά αποδεκτού ο οποίος έχει στη κατοχή του ένα καλό αντίγραφο του δημόσιου κλειδιού. Με την διαδικασία αυτή, θα παράγεται ένα υπογεγραμμένο πιστοποιητικό δημόσιου κλειδιού που θα αποδείκνυε την ακεραιότητα του δημόσιου κλειδιού. Το υπογεγραμμένο δημόσιου κλειδί μπορεί να σταλεί από τον «τρίτο» στο BBS και από εκεί να το πάρει αργότερα όποιος το χρειαστεί. Αυτός το μόνο που θα χρειαστεί να κάνει, για να σιγουρευτεί για την ακεραιότητα του δημόσιου κλειδιού, είναι να την ελέγξει μέσω του δημόσιου κλειδιού του «τρίτου. Κανένας δεν μπορεί να ξεγελάσει πλέον όποιον έχει το υπογεγραμμένο από τον «τρίτο» δημόσιο κλειδί ενός παραλήπτη, διότι κανείς δεν μπορεί να πλαστογραφήσει την υπογραφή του «τρίτου».

Κάποιο άτομο που τυγχάνει ευρείας εμπιστοσύνης θα μπορούσε να εξειδικευτεί στην παροχή αυτής της υπηρεσίας, δηλαδή της παροχής υπογραφών σε πιστοποιητικά δημοσίων κλειδιών άλλων χρηστών. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος «key server» ή κάποια υπηρεσία πιστοποίησης. Κάθε πιστοποιητικό δημόσιου κλειδιού που φέρει την υπογραφή αυτού του key server θα μπορεί να θεωρείται γνήσιο και έτσι άξιο της εμπιστοσύνης κάποιου. Το μόνο που χρειάζεται να κάνουν όσοι χρήστες θα ήθελαν να συμμετέχουν σε αυτή τη διαδικασία είναι να αποκτήσουν ένα καλό αντίγραφο του δημοσίου κλειδιού του key server έτσι ώστε να είναι σε θέση να επιβεβαιώσουν την υπογραφή αυτού. Κάποιος κεντρικός key

server ή μια υπηρεσία πιστοποίησης, θα ήταν κατάλληλη για κάποια μεγάλη και απρόσωπη επιχείρηση ή κυβερνητική υπηρεσία.

Η αποκεντρωμένη έκδοση του σχήματος αυτού είναι εκείνη που επιτρέπει σε όλους τους χρήστες να δρουν σαν μεσάζοντες, ο ένας για τον άλλο, κάτι που έχει καλύτερα αποτελέσματα από έναν και μοναδικό key server. Το PGP τείνει προς αυτή τη κατεύθυνση διότι αντανακλά καλύτερα το φυσικό τρόπο με τον οποίο αλληλεπιδρούν μεταξύ τους οι άνθρωποι στις σχέσεις τους και ταυτόχρονα επιτρέπει σε αυτούς να διαλέξουν ποιόν εμπιστεύονται για τη διαχείριση των κλειδιών τους.

Αυτή ολόκληρη η διαδικασία της προστασίας των δημοσίων κλειδιών είναι το μοναδικό δύσκολο πρόβλημα στις πρακτικές εφαρμογές της κρυπτογράφησης δημοσίων κλειδιών. Θα μπορούσαμε να πούμε ότι είναι η Αχίλλειος φτέρνα της κρυπτογράφησης δημοσίων κλειδιών και έχει καταβληθεί μεγάλη προσπάθεια για τη λύση αυτού του προβλήματος. Η χρήση ενός δημόσιου κλειδιού δεν θα πρέπει να ξεκινάει εάν δεν είμαστε σίγουροι ότι πρόκειται για ένα καλό δημόσιο κλειδί το οποίο ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει. Μπορούμε να είμαστε σίγουροι για την προέλευση του κλειδιού εάν έχουμε κάποιο πιστοποιητικό από τον ιδιοκτήτη του ή κάποιον άλλο που εμπιστευόμαστε, από τον οποίο όμως έχουμε ήδη ένα εγγυημένο δημόσιο κλειδί. Επιπλέον το user id θα πρέπει να έχει ολόκληρο το όνομα του ιδιοκτήτη και όχι απλά το μικρό του ή κάποιο άλλο ψευδώνυμο.

Δεν έχει σημασία πόσο σίγουροι μπορεί να αισθανόμαστε για κάποιο δημόσιο κλειδί που κατεβάσαμε από κάποιον ηλεκτρονικό πίνακα ανακοινωθέντων, ποτέ δεν θα πρέπει να εμπιστευόμαστε οτιδήποτε δεν έχει την υπογραφή κάποιου που εμπιστευόμαστε. Ένα δημόσιο κλειδί που απλά κατεβάσαμε δίχως να το ελέγξουμε είναι πιθανόν να έχει αλλοιωθεί από κάποιον τρίτο, ακόμα και από το διαχειριστή του ηλεκτρονικού πίνακα. Εάν ποτέ μας ζητηθεί να υπογράψουμε το δημόσιο κλειδί κάποιου άλλου θα πρέπει να σιγουρευτούμε ότι αυτό πραγματικά του ανήκει. Αυτό πρέπει να γίνει διότι η υπογραφή μας στο δημόσιο κλειδί εγγυάται την αυθεντικότητά του. Εάν έχουμε κάνει λάθος, τότε όσοι μας εμπιστεύονται θα εμπιστευτούν και το κλειδί με αβέβαια αποτελέσματα. Ο κανόνας λέει ότι υπογράφουμε δημόσια κλειδιά για τα οποία έχουμε ιδία γνώση της αυθεντικότητάς τους. Για να αποκτήσουμε αυτή τη γνώση μπορούμε για παράδειγμα να μιλήσουμε στον ιδιοκτήτη του κλειδιού στο τηλέφωνο και να επιβεβαιώσουμε τα στοιχεία που έχουμε στα χέρια μας. Με το να βάλουμε την υπογραφή μας σε ένα δημόσιο κλειδί για το οποίο ήμαστε σίγουροι δεν χάνουμε την αξιοπιστία μας ακόμα και αν αυτό ανήκει σε κάποιον ψυχοπαθή. Αυτό συμβαίνει διότι με την υπογραφή μας δεν λέμε τίποτα παραπάνω από το ότι αυτό το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει, το ότι κάποιος μπορεί να εμπιστευθεί το κλειδί δεν έχει καμία σχέση με το αν μπορεί να εμπιστευθεί ή όχι τον ιδιοκτήτη του.

Θα πρέπει οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτό από διαφόρους μεσάζοντες με την ελπίδα ότι οι περισσότεροι χρήστες εμπιστεύονται κάποιον από αυτούς. Μπορεί λοιπόν, κάποιος χρήστης να ανακοινώσει το δημόσιο κλειδί του μαζί με τη συλλογή των πιστοποιητικών που διαθέτει για αυτό. Όταν υπογράφουμε το δημόσιο κλειδί κάποιου πρέπει να του το επιστρέφουμε μαζί με την υπογραφή μας ώστε να την προσθέσουνε στη συλλογή πιστοποιητικών για το δημόσιο κλειδί τους.

Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας. Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.

Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το αρχείο με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο αρχείο μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των αρχείων δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για τη πιστοποίηση ή μη όλων των άλλων κλειδιών του αρχείου είναι σημαντική για την ασφάλεια όλου

του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.

Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα αρχεία και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοιώσει σε άλλα κλειδιά.

Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το αρχείο με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο αρχείο, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

Τέλος, εάν επιθυμούμε μπορούμε να κάνουμε αναζήτηση δημόσιου κλειδιού χρήστη μέσω Server μέσω της εφαρμογής PGP, όπως φαίνεται και στην πιο κάτω εικόνα.

Εικόνα 22. Διαδικασία αναζήτησης και εύρεσης δημόσιου κλειδιού

5.4 Διαδικασία Αναγνώρισης Έγκυρων Κλειδιών

Το PGP παρακολουθεί ποια από τα κλειδιά που υπάρχουν στο αρχείο δημοσίων κλειδιών είναι πιστοποιημένα και ποια όχι με υπογραφές χρηστών που εμπιστευόμαστε. Το μόνο που πρέπει να κάνουμε είναι να «πούμε» στο PGP ποιους χρήστες εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας κλειδί. Το PGP αναλαμβάνει από εκεί να κινήσει αυτόματα διαδικασίες ελέγχου της εγκυρότητας κλειδιών που είναι υπογεγραμμένα από τους μεσάζοντες που εμείς ορίσαμε. Υπάρχει βέβαια πάντα η δυνατότητα να υπογράψουμε κλειδιά και εμείς οι ίδιοι.

Υπάρχουν δύο διαφορετικά κριτήρια βάση των οποίων το PGP κρίνει τη χρησιμότητα των κλειδιών και τα οποία δεν πρέπει να συγχέουμε:

1. Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει; (έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;).
2. Ανήκει σε κάποιον που μπορούμε να εμπιστευθούμε για την πιστοποίηση άλλων κλειδιών;

Το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση. Η απάντηση στη δεύτερη πρέπει να δοθεί αποκλειστικά από το χρήστη. Όταν ο χρήστης δώσει την απάντηση στην δεύτερη ερώτηση τότε το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση

για άλλα κλειδιά τα οποία υπογράφονται από αυτόν που έχουμε ορίσει σαν έμπιστο. Κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχουμε ορίσει ως έμπιστο θεωρούνται έγκυρα από το PGP. Τα κλειδιά που ανήκουν σε έμπιστους μεσάζοντες πρέπει να πιστοποιηθούν από είτε από εμάς τους ίδιους είτε από κάποιον άλλο που έχουμε ορίσει ως έμπιστο.

Το PGP δίνει επιπλέον τη δυνατότητα ορισμού διαφορετικών επιπέδων εμπιστοσύνης για διαφορετικούς μεσάζοντες. Το ότι εμπιστευόμαστε κάποιον να δράσει ως μεσάζοντας δεν σημαίνει μόνο ότι τον εμπιστευόμαστε αλλά επιπλέον ότι τον θεωρούμε αρκετά ικανό να διαχειριστεί κλειδιά επιλέγοντας ποια από αυτά πρέπει και ποια όχι να υπογράψει. Μπορεί να ορίσουμε έναν χρήστη - μεσάζοντα στο PGP σαν άγνωστο, μη έμπιστο, μερικώς έμπιστο και εντελώς έμπιστο για να πιστοποιεί δημόσια κλειδιά. Αυτή η πληροφορία, που αφορά το βαθμό εμπιστοσύνης κάποιου μεσάζοντα, περιέχεται στο αρχείο των κλειδιών μαζί με το αντίστοιχο κλειδί (του μεσάζοντα) και δεν αντιγράφεται σε καμία περίπτωση κατά την αντιγραφή κάποιου κλειδιού του αρχείου διότι θεωρείται εμπιστευτική πληροφορία μια και αντικατοπτρίζει την άποψη του κατόχου του για τους μεσάζοντες - απόλυτα προσωπικό στοιχείο.

Όταν το PGP ελέγχει την εγκυρότητα ενός κλειδιού αυτό που κάνει είναι να ελέγχει τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησής του. Κατόπιν υπολογίζει ένα μέσο επίπεδο εμπιστοσύνης - για παράδειγμα δύο μερικώς έμπιστες υπογραφές ισοδυναμούν με μία πλήρως έμπιστη. Το σκεπτικό λειτουργίας του PGP προσαρμόζεται στις απαιτήσεις του χρήστη και ρυθμίζεται αναλόγως (για παράδειγμα μπορούμε να ρυθμίσουμε το PGP να θεωρεί ένα κλειδί έγκυρο μόνο εάν αυτό φέρει δύο πλήρως έμπιστες υπογραφές ή τρεις μερικώς έμπιστες).

Το δικό μας κλειδί θεωρείται έγκυρο από το PGP αξιωματικά και για αυτό το λόγο δεν χρειάζεται την πιστοποίηση από κανέναν. Το PGP γνωρίζει ποια δημόσια κλειδιά είναι δικά μας κοιτάζοντας να βρει τα αντίστοιχα μυστικά κλειδιά στο αρχείο τους. Το PGP θεωρεί επιπλέον ότι εμπιστευόμαστε τους εαυτούς μας για να πιστοποιούν άλλα κλειδιά.

Όσο θα περνάει ο καιρός θα λαμβάνουμε όλο και περισσότερα κλειδιά από χρήστες που ίσως να θέλουμε να ορίσουμε ως μεσάζοντες. Κάθε ένας από αυτούς θα έχει τους δικούς του μεσάζοντες των οποίων τα πιστοποιητικά - υπογραφές θα μοιράζει μαζί με το κλειδί του με την ελπίδα ότι όποιος τα λάβει να εμπιστεύεται κάποιο από όλα. Έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο εμπιστοσύνης για όλα τα δημόσια κλειδιά.

Αυτή η μοναδική προσέγγιση έρχεται σε αντίθεση με τα κατεστημένα κυβερνητικά σχήματα διαχείρισης κλειδιών, όπως το PEM (Internet Privacy Enhanced Mail), τα οποία βασίζονται σε συστήματα κεντρικού ελέγχου και υποχρεωτικής εμπιστοσύνης σε αυτά. Τα σχήματα αυτά απαρτίζονται από ιεραρχικές οντότητες που υπαγορεύουν ποιόν πρέπει να εμπιστευόμαστε. Αυτό είναι φανερό ότι έρχεται σε πλήρη αντίθεση με τη σχεδιαστική αρχή του PGP η οποία επιτρέπει στον καθένα και ανεξάρτητα από οποιονδήποτε και οτιδήποτε άλλο να καθορίσει ο ίδιος την πολιτική που θέλει να ακολουθήσει στη διαχείριση των κλαδιών του. Έτσι το PGP βάζει το χρήστη και όχι το σύστημα στην κορυφή της προσωπική του πυραμίδα πιστοποίησης.

5.5 Προστασία του Μυστικού Κλειδιού

Η προστασία του μυστικού κλειδιού και της φράσης-κλειδί του, είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια, τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας, τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το «όνομά» μας. Θα μπορούσε, για παράδειγμα, να υπογράψει ένα σύνολο από δημόσια κλειδιά δημιουργώντας έτσι πρόβλημα σε πολλούς χρήστες ειδικά εάν η υπογραφή μας τυγχάνει ευρείας εμπιστοσύνης και αποδοχής. Φυσικά, κίνδυνο διατρέχουμε και από το γεγονός της έκθεσης όλων των μηνυμάτων μας στα μάτια αυτού που έχει το προσωπικό μας κλειδί.

Η προστασία του μυστικού κλειδιού πρέπει να αρχίζει με τη φυσική του διασφάλιση. Μπορούμε να το κρατάμε σε κάποιο PC στο σπίτι ή κάποιο υπολογιστή notebook μια και αυτά τα έχουμε υπό την επίβλεψή μας συνεχώς. Εάν ποτέ υπάρξει ανάγκη χρησιμοποίησης

υπολογιστή στο γραφείο ή οπουδήποτε αλλού τότε θα πρέπει να μεταφέρουμε το μυστικό κλειδί μας σε αυτόν μέσο κάποιας δισκέτας ενδεχομένως και για όσο χρειάζεται ενώ όταν τελειώσουμε τη δουλεία μας δεν πρέπει να αφήσουμε πίσω οτιδήποτε μπορεί να οδηγήσει στην αποκάλυψη του. Δεν είναι επίσης σωστό να αφήνουμε το μυστικό κλειδί μας σε κάποιο απομακρυσμένο μηχάνημα (ένας Unix dial-in server) διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες μέσω modem να υποκλέψει τη μυστική φράση (pass phrase) και να αποκτήσει το μυστικό από το απομακρυσμένο σύστημα. Συμπερασματικά λέμε ότι θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο.

Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί. Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας. Η αποθήκευση τόσο του μυστικού κλειδιού όσο και της μυστικής φράσης στον ίδιο υπολογιστή είναι το ίδιο επικίνδυνη με την φύλαξη του PIN ενός τραπεζικού ATM λογαριασμού στο ίδιο πορτοφόλι με την κάρτα ATM. Ένα πράγμα είναι σίγουρο - δεν θέλουμε σε καμία περίπτωση αυτός που θα έχει στα χέρια του τον σκληρό δίσκο με το μυστικό μας κλειδί να έχει στη διάθεσή του και τη μυστική φράση. Το ιδανικό θα ήταν να απομνημονεύαμε τη μυστική φράση και να μην την φυλάγαμε σε κανένα άλλο μηχάνημα εκτός του εγκεφάλου μας. Εάν, ωστόσο, νιώθουμε ότι πρέπει να τη γράψουμε κάπου θα πρέπει να την ασφαλίσουμε καλλίτερα ίσως και από το ίδιο το μυστικό μας κλειδί.

Κάτι άλλο επίσης σημαντικό, που πρέπει να κάνουμε, είναι να παίρνουμε backup του μυστικού αρχείου μας διότι μόνο εμείς έχουμε το μοναδικό αντίγραφο αυτού και πιθανή απώλειά του θα ισοδυναμούσε με αχρήστευση όλων των δημοσίων κλειδιών που διανείμαμε στον κόσμο.

Το αποκεντρωτικό σχήμα φιλοσοφίας αλλά και λειτουργίας που έχει επιλέξει να χρησιμοποιήσει το PGP εκτός από τα πλεονεκτήματα στη διαχείριση των κλειδιών έχει και τα μειονεκτήματα του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα «πιστοποιητικό απολεσθέντος κλειδιού» (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Μπορούμε να χρησιμοποιήσουμε το PGP στη δημιουργία αυτού του πιστοποιητικού και κατόπιν να το στείλουμε σε όλους τους φίλους και συνεργάτες μας σε όλο τον κόσμο. Η έκδοση του PGP που τρέχει σε αυτούς θα αναλάβει να εγκαταστήσει το πιστοποιητικό του απολεσθέντος κλειδιού στα δημόσια αρχεία τους και από εκείνη τη στιγμή θα αποτρέπεται αυτόματα η επαναχρησιμοποίησή τους. Μπορούμε κατόπιν να δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

5.6 Νομική δεσμευτικότητα των PGP υπογραφών

Ένα πολύ σημαντικό ζήτημα είναι η νομική δέσμευση αυτού που υπογράφει με PGP υπογραφή ένα λογισμικό πακέτο κατά την διανομή του. Ποια είναι η ευθύνη του υπογράφοντος σε περίπτωση που το λογισμικό περιέχει ένα σφάλμα, έναν ιό ή οτιδήποτε μπορεί να βλάψει τον χρήστη που θα προμηθευτεί το λογισμικό.

Η υπογραφή έχει την έννοια που της προσδίδει το περιεχόμενο του αντικειμένου που υπογράφεται. Αν ο υπογράφων δεν είναι βέβαιος για αυτό το περιεχόμενο, πρέπει να το διευκρινίσει, για παράδειγμα, εισάγοντας ένα σχόλιο σχετικά με το ότι η υπογραφή του αποσκοπεί στην ταυτοποίηση αυθεντικότητας της πηγής του κώδικα και δεν περιέχει εγγυήσεις ως προς το περιεχόμενο του κώδικα. Εδώ θα πρέπει να πούμε ότι είναι αδύνατη η απευθείας ανάγνωση του αντικειμένου που υπογράφεται ηλεκτρονικά, αφού μπορεί να πρόκειται για ένα έγγραφο κειμενογράφου ή ένα οποιοδήποτε φύλλο εργασίας. Ακόμη και το «απλό κείμενο» δεν μπορεί να αναγνωστεί χωρίς την βοήθεια ενός text editor, παρόλο που σε αυτήν τουλάχιστον την περίπτωση δεν υπάρχει ο κίνδυνος εκπλήξεων, όπως για παράδειγμα η διατήρηση από έναν κειμενογράφο μιας παλαιότερης έκδοσης του κειμένου χωρίς αυτό να το παρουσιάζει στον δημιουργό του.

Το πιο πάνω γεγονός βρίσκεται σε αντίθεση με το έντυπα έγγραφα, στα οποία είναι πάντα ευδιάκριτο το περιεχόμενο του κειμένου που υπογράφεται. Ο σχεδιασμός πολλών

σύγχρονων συστημάτων αγνοεί αυτό το πρόβλημα. Μια πολύ πιθανή επίθεση σε έναν ανυποψίαστο χρήστη είναι η μετατροπή του λογισμικού που παρουσιάζει το έγγραφο στον χρήστη και τελικά το γεγονός της υπογραφής του ηλεκτρονικού εγγράφου από τον χρήστη με την πεποίθηση ότι υπογράφει κάτι διαφορετικό από αυτό που πραγματικά υπογράφει. Ακόμα και η έξυπνη κάρτα δεν μπορεί να αντιμετωπίσει αυτό το πρόβλημα. Η ευρεία χρήση των επισφαλών λειτουργικών συστημάτων και λογισμικού φαίνεται να προκαλεί προβλήματα σε αυτόν τον τομέα όσο διευρύνεται η χρήση των ηλεκτρονικών υπογραφών.

Οι κανόνες που ισχύουν για τις ηλεκτρονικές υπογραφές είναι ακριβώς οι ίδιοι με τους κανόνες που ισχύουν στις ιδιόχειρες υπογραφές. Η PGP υπογραφή κάποιου, όπως και η ιδιόχειρη υπογραφή του είναι έγκυρη εάν όντως αυτός έχει υπογράψει.

Συμπερασματικά, μπορούμε να πούμε ότι η μέθοδος PGP και όλες οι παραλλαγές της (GPG, OpenPGP κ.λ.π.) δημιουργούν μεν «ψηφιακές υπογραφές», δηλαδή υπογραφές που ικανοποιούν τους όρους της νομοθεσίας για «προηγμένες ηλεκτρονικές υπογραφές» όμως, δεν μπορούν να παράξουν «αναγνωρισμένες ηλεκτρονικές υπογραφές», εφόσον δεν υποστηρίζονται από ένα «αναγνωρισμένο πιστοποιητικό». Επειδή κανένας από τους πιστοποιούντες δεν αναλαμβάνει ιδιαίτερη ευθύνη και υποχρεώσεις έναντι των τρίτων, η μέθοδος αυτή δεν μπορεί προϋποθέσεις ασφάλειας για διενέργεια «σημαντικών ηλεκτρονικών συναλλαγών» μεταξύ αγνώστων, εφόσον δεν εξασφαλίζει «επαρκείς αποδείξεις» και δεν παρέχει εγγυήσεις ως προς την πραγματική ταυτότητα των συναλλασσομένων.

5.7 Κρυπτογράφηση και Αποκρυπτογράφηση με PGP

Πριν ολοκληρώσουμε την αναφορά που κάναμε στο σύστημα PGP, κρίνουμε σκόπιμο να δούμε στην πράξη την διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης με την χρήση του PGP.

Για να κρυπτογραφήσουμε με το PGP, ένα απλό κείμενο που γράφουμε στο MS-Word και να το στείλουμε ως συνημμένο αρχείο σε κάποιον παραλήπτη αλληλογραφίας, 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 του PGP, την κλειδαριά και στην συνέχεια επιλέγουμε Encrypt. Η διαδικασία κρυπτογράφησης του μηνύματος έχει ολοκληρωθεί και μπορούμε να αποθηκεύσουμε το αρχείο και να το επισυνάψουμε σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου. Στην πιο κάτω εικόνα φαίνεται η επιλογή του κλειδιού προς κρυπτογράφηση.

Εικόνα 23. Επιλογή κλειδιού προς κρυπτογράφηση

Εάν έχουμε τώρα, 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 ηλεκτρονικό μήνυμα, μπορούμε να το αποκρυπτογραφήσουμε έχοντας ως τρέχον το παράθυρο με το κρυπτογραφημένο κείμενο και επιλέγοντας από τη γραμμή εργασιών όπως και κατά την κρυπτογράφηση την κλειδαριά αλλά στην συνέχεια επιλέγουμε Decrypt & Verify. Εν συνεχεία μα ζητάτε να πληκτρολογήσουμε τον κωδικό που είχαμε αρχικά χρησιμοποιήσει για τη δημιουργία των προσωπικών μας κλειδιών. Εάν δώσουμε τον σωστό κωδικό, μας εμφανίζεται το κείμενό μας αποκρυπτογραφημένο σε ένα νέο παράθυρο.

Εικόνα 24. Αποκρυπτογραφημένο μήνυμα

6. Αντι Επιλογου

Προκειμένου οι ηλεκτρονικές υπογραφές να αποκτήσουν ακόμα μεγαλύτερο κύρος και να είναι ακόμα πιο ισχυρός ο ρόλος τους για την παροχή εμπιστευτικότητας, αυθεντικότητας και ακεραιότητας όλων των ηλεκτρονικών εγγράφω και των ηλεκτρονικών συναλλαγών, είναι επιβεβλημένες ορισμένες ενέργειες από όλες τις εμπλεκόμενες πλευρές.

Σε ότι αφορά τις ενέργειες από την πλευρά της Ελλάδας και της Ελληνικής Πολιτείας θα πρέπει σε πρώτο επίπεδο να έχουμε την σύνταξη μιας ενιαίας «Πολιτικής Ηλεκτρονικής Υπογραφής» του Δημοσίου για όλες τις υπηρεσίες e-government που αναπτύσσει. Αυτό θα έχει ως άμεσο αποτέλεσμα την ύπαρξη μιας ενιαίας στάσης όλων των δημόσιων υπηρεσιών, οργανισμών και φορέων στα θέματα της ηλεκτρονικής υπογραφής και της πιστοποιημένης αυθεντικότητας όλων των δημόσιων ηλεκτρονικών συναλλαγών. Η ενιαία «Πολιτική Ηλεκτρονική Υπογραφή» θα πρέπει να πραγματοποιηθεί παράλληλα με την σύσταση ενός κεντρικού συμβουλευτικού οργάνου το οποίο θα έχει ως βασικούς και μείζονος σημασίας στόχους α) την υποστήριξη των παραπάνω υπηρεσιών και β) την ανταλλαγή τεχνογνωσίας με την σχετική αγορά. Από την άλλη πλευρά, εκείνη δηλαδή της πιστοποίησης θα πρέπει να πραγματοποιηθεί η άμεση ολοκλήρωση και λειτουργία των θεσμών πιστοποίησης («Διαπίστωσης» & «Εθελοντικής Διαπίστευσης») των σχετικών προϊόντων και υπηρεσιών που θα συμβάλουν στην ανάπτυξη της εμπιστοσύνης των χρηστών. Φυσικά όλα τα πιο πάνω θα είναι κενά ουσίας και περιεχόμενου εάν δεν συνοδευτούν από την πλευρά της πολιτείας με ενημέρωση των πολιτών, έτσι θα πρέπει να εκπονηθεί ολοκληρωμένη εκστρατεία ενημέρωσης του πολίτη για την σωστή χρήση των τεχνολογιών ηλεκτρονικής υπογραφής, με σκοπό και στόχο ο πολίτης ο οποίος είναι ο ουσιαστικός και τελικός χρήστης.

Σε ότι αφορά του ΠΥΠ θα πρέπει να ακολουθηθεί μια αυστηρή συμμόρφωση με τα εκδιδόμενα σχετικά ευρωπαϊκά πρότυπα για την διασφάλιση ενός ελάχιστου επιπέδου διαλειτουργικότητας τόσο σε εθνικό, όσο και σε ενδοκοινοτικό επίπεδο. Επίσης, πολύ σημαντικό κομμάτι θεωρείται εκείνο που αφορά την ανάπτυξη περαιτέρω συνεργασίας μεταξύ των ΠΥΠ με στόχο την προώθηση της τυποποίησης και της συμβατότητας των πολιτικών έκδοσης πιστοποιητικών και γενικότερα των υπηρεσιών τους, στο βαθμό που αυτό θα συμβάλλει στην μεγαλύτερη αποδοχή τους από τους χρήστες και την σχετική αγορά. Τέλος, σε ότι αφορά τους ΠΥΠ είναι πολύ σημαντική η σύσταση ενός κοινού συστήματος «κλάσεων» για τα εκδιδόμενα πιστοποιητικά, όπου θα προσδιορίζονται κοινά επίπεδα στα όρια των επιτρεπόμενων συναλλαγών και στην ανάληψη αντίστοιχης ευθύνης εκ μέρους τους, λαμβάνοντας υπ' όψιν τις ανάγκες της εγχώριας αγοράς, σε αυτό το σημείο θα πρέπει να υπάρχει η ουσιαστική διαβούλευση με Τράπεζες, Δημόσιο και όλους τους υπόλοιπους φορείς οι οποίοι θα είναι οι κύριοι αποδέκτες των πιστοποιητικών που θα εκδίδονται από τους ΠΥΠ.

Σε ότι αφορά τους παρόχους άλλων υπηρεσιών που χρησιμοποιούν ηλεκτρονικές υπογραφές θα πρέπει σε πρώτο επίπεδο να υπάρχει η σύνταξη ή η υιοθέτηση κοινών «Πολιτικών Ηλεκτρονικής Υπογραφής» με άλλους παρόχους συναφών υπηρεσιών, όπως είναι τράπεζες, τηλεπικοινωνιακοί φορείς, πάροχοι υπηρεσιών περιεχομένου, γεγονός που θα συμβάλει στην μεγιστοποίηση του αριθμού χρηστών, στους κατόχους κρυπτογραφικών κλειδιών με τυποποιημένες προδιαγραφές, στους οποίους θα απευθύνουν τις υπηρεσίες τους. Θα πρέπει να υπάρχει επίσης και η συμβολή των παρόχων αυτών, στην ανάπτυξη κλίματος εμπιστοσύνης των χρηστών, με την αυστηρή τήρηση όλων των προβλεπόμενων πολιτικών ασφάλειας και την υποστήριξη των κατάλληλων τεχνολογιών και μεθόδων που διασφαλίζουν την εμπιστευτικότητα των προσωπικών δεδομένων των χρηστών-πελατών τους.

Όλα τα πιο πάνω θα πρέπει να συνοδεύονται και από κάποιες ουσιαστικές ενέργειες που θα πρέπει να κάνει ο τελικός χρήσης με στόχο να είναι ενεργός σε ότι αφορά τα θέματα των ηλεκτρονικών υπογραφών και των πιστοποιητικών. Ο τελικός χρήστης θα πρέπει να ενημερώνεται διεξοδικά για όλους τους όρους χρήσης των κρυπτογραφικών κλειδιών, των πιστοποιητικών και των συναφών υπηρεσιών του ΠΥΠ κατά την αίτησή του για την έκδοση πιστοποιητικού ηλεκτρονικής υπογραφής. Πέρα από αυτό θα πρέπει επίσης, να τηρεί με αυστηρότητα και μεγάλη επιμέλεια την μυστικότητα και την αποκλειστική χρήση των σχετικών ιδιωτικών κλειδιών του και να μην υπάρχει σε καμία περίπτωση η έκθεση των κλειδιών υπογραφής του σε τρίτους. Ο τελικός χρήστης έχει την δυνατότητα και θα πρέπει πάντα να ζητά από τον ΠΥΠ την ανάκληση ή την αναστολή του σχετικού πιστοποιητικού του εάν βεβαιωθεί ή

έχει την υποψία για οποιαδήποτε έκθεση των ιδιωτικών κλειδιών του σε τρίτους, καθώς και στην περίπτωση που απολέσει τον φορέα ή/και τον έλεγχο των ιδιωτικών κλειδιών του. Τέλος, πολύ σημαντικό κρίνεται, από την πλευρά του τελικού χρήστη, ότι είναι να χρησιμοποιεί τα συγκεκριμένα κρυπτογραφικά κλειδιά του μόνο στις επιτρεπόμενες, από το σχετικό πιστοποιητικό του, χρήσεις και να μην υπερβαίνει σε αξία συναλλαγών τα τυχόν «όρια» που προβλέπονται από την Σύμβαση και την Πολιτική του πιστοποιητικού του.

Στις μέρες μας οι ηλεκτρονικές συναλλαγές πραγματοποιούνται από όλους τους ανθρώπους είτε άμεσα είτε έμμεσα, είτε το γνωρίζουν είτε το κάνουν δυνητικά. Στο μέλλον προβλέπεται ότι θα υπάρξει ακόμα μεγαλύτερη χρήση των ηλεκτρονικών συναλλαγών από περισσότερους χρήστες και σε περισσότερους τομείς. Προϋπόθεση για την σωστή και εύρυθμη χρήση και λειτουργιά των ηλεκτρονικών συναλλαγών είναι η ανάπτυξη και δημιουργία ηλεκτρονικών υπογραφών και πιστοποιητικών τα οποία θα πληρούν τις απαιτήσεις των Ευρωπαϊκών Οδηγιών και των Ελληνικών Νόμων που τις ενσωματώνουν, θα πληρούν όμως και τις ανάγκες των χρηστών. Αυτό μπορούμε να το πετύχουμε μόνο εάν υπάρχει άμεση συνεργασία της Πολιτείας και των ΠΥΠ και υπάρχει η συνειδητοποιημένη αντιμετώπιση του θέματος από τους τελικούς χρήστες, αυτή η συνειδητοποίηση μπορεί να υπάρξει μόνο μέσα από την ουσιαστική γνώση των δικαιωμάτων και των υποχρεώσεων που έχει ο κάθε χρήστης και ο κάθε ΠΥΠ. Μέσα από αυτό το πρίσμα μπορεί να υπάρξει ουσιαστική εμπιστοσύνη και ανάπτυξη για τις πιστοποιήσεις των ηλεκτρονικών υπογραφών που θα έχουν ως απώτερο σκοπό την ακεραιότητα, την εμπιστευτικότητα και την αυθεντικότητα των ηλεκτρονικών εγγράφων και ηλεκτρονικών συναλλαγών.

7. ΣΥΝΟΨΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ

Από την παρούσα μεταπτυχιακή διατριβή, έγινε φανερό ότι οι ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά ταυτοποίησης, παρά την πολυπλοκότητα που τα χαρακτηρίζει,, αποτελούν σήμερα την μόνη αξιόπιστη λύση για την ταυτόχρονη πιστοποίηση της προέλευσης και τη διασφάλιση της ακεραιότητας, την εμπιστευτικότητας και της αυθεντικότητας των διακινούμενων ηλεκτρονικών δεδομένων σε «ανοικτά δίκτυα».

Πολύ σημαντικά στοιχεία κρίνουμε ότι είναι η μελέτη και η πιστή τήρηση των σχετικών ευρωπαϊκών νομικοτεχνικών προτύπων αποτελεί μια βασική μέθοδος για την τεκμηριωμένη συμμόρφωση των υπηρεσιών και των προϊόντων με τις απαιτήσεις της Οδηγίας 1999/93, ιδίως για την έκδοση και χρήση «αναγνωρισμένων πιστοποιητικών», αλλά και για την επίτευξη ευρύτερης διαλειτουργικότητας από τις σχετικές εφαρμογές.

Η τυποποίηση και η διαλειτουργικότητα των παρεχόμενων υπηρεσιών πιστοποίησης και των προϊόντων ηλεκτρονικής υπογραφής αποτελούν βασική προϋπόθεση για την περαιτέρω διάδοση και ενσωμάτωσή τους σε εφαρμογές «ηλεκτρονικού επιχειρείν». 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.

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 δυσλειτουργικών υπηρεσιών πιστοποίησης ψηφιακής υπογραφής, εξακολουθεί να εμφανίζει ακόμα αρκετές δυσχέρειες. Το γεγονός αυτό οφείλεται σε κάποιους ανασταλτικούς παράγοντες μεταξύ των οποίων περιλαμβάνονται:

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

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.

Υπάρχουν αρκετά παραδείγματα στον Ευρωπαϊκό χώρο που έχουν δείξει ότι 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 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. Γίνεται αντιληπτό λοιπόν, ότι θα πρέπει να δοθεί μεγαλύτερη βαρύτητα στην υιοθέτηση ανοικτών προτύπων.

Σημαντικό σημείο είναι και η σύνταξη σαφών κανόνων και προδιαγραφών Πολιτική Υπογραφής (Signature Policies), οι οποίοι 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), για τη χρήση και αποδοχή ηλεκτρονικών υπογραφών και πιστοποιητικών σε συγκεκριμένους τύπους συναλλαγών, θεωρείται απαραίτητη σε καθεστώς «ελεύθερης παροχής» των σχετικών υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής. Επίσης, θεωρείται ότι μπορεί να συμβάλλει στην αποσαφήνιση των απαραίτητων προδιαγραφών για τις παρεχόμενες υπηρεσίες πιστοποίησης ψηφιακών υπογραφών και στην περαιτέρω διαλειτουργικότητά τους.

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.

Ο Δημόσιος Τομέας, αναγνωρίζεται ως ο βασικότερος παράγοντας για την προώθηση της χρήσης ηλεκτρονικών υπογραφών στην Ελλάδα, λόγω των πολυάριθμων σχετικών έργων

ηλεκτρονικής διακυβέρνησης (e-government) που σχεδιάζει και την δημιουργία της απαραίτητης «κρίσιμης μάζας» πιστοποιημένων χρηστών, η οποία θα συμβάλει στην περαιτέρω ανάπτυξη σχετικών υπηρεσιών.

Σημαντικό σημείο θεωρείται και η έμφαση που θα πρέπει να δοθεί στο να ενισχυθεί η εμπιστοσύνη των χρηστών στις μεθόδους ηλεκτρονικής υπογραφής και να διασφαλιστεί τεχνολογικά η προστασία των προσωπικών δεδομένων τους (τα οποία θα διακινούνται σε ηλεκτρονική μορφή), από την μη εξουσιοδοτημένη πρόσβαση και συλλογή, προφανώς με την αποδοχή και χρήση –όπου αυτό είναι εφικτό- 'ψευδώνυμων πιστοποιητικών', καθώς και την παράλληλη υποστήριξη των εφαρμογών κρυπτογράφησης δεδομένων.

8. Υλοποιηση - Εφαρμογη

8.1. Εισαγωγή

Στα πλαίσια της μεταπτυχιακής διατριβής και θέλοντας να δείξουμε την χρησιμότητα των ηλεκτρονικών υπογραφών, προχωρήσαμε στην δημιουργία και υλοποίηση μιας ιστοσελίδας με την χρήση των HTML και JavaScript. Η ιστοσελίδα περιλαμβάνει αρκετές επιμέρους σελίδες και στην συνέχεια θα παρουσιάσουμε κάποιες από αυτές.

Η ιστοσελίδα αφορά έναν τουριστικό οδηγό για την Κρήτη, στον οποίο εκτός από τις σελίδες που μπορεί ο χρήστης να προηγηθεί και να δει την ιστορία της Κρήτης, αξιοθέατα, παραλίες κ.α, έχει επίσης, την δυνατότητα να κάνει και Online κράτηση, αυτό σημαίνει ότι ο χρήστης από την στιγμή που θα δώσει προσωπικά του στοιχεία αυτά να είναι διασφαλισμένα και ότι δεν πρόκειται να χρησιμοποιηθούν από κάποιον κακόβουλο τρίτο, σε αυτό ακριβώς το σημείο είναι που απαιτείται η ενσωμάτωση της ηλεκτρονικής υπογραφής ώστε να επιτυγχάνεται αυτή η απαίτηση.

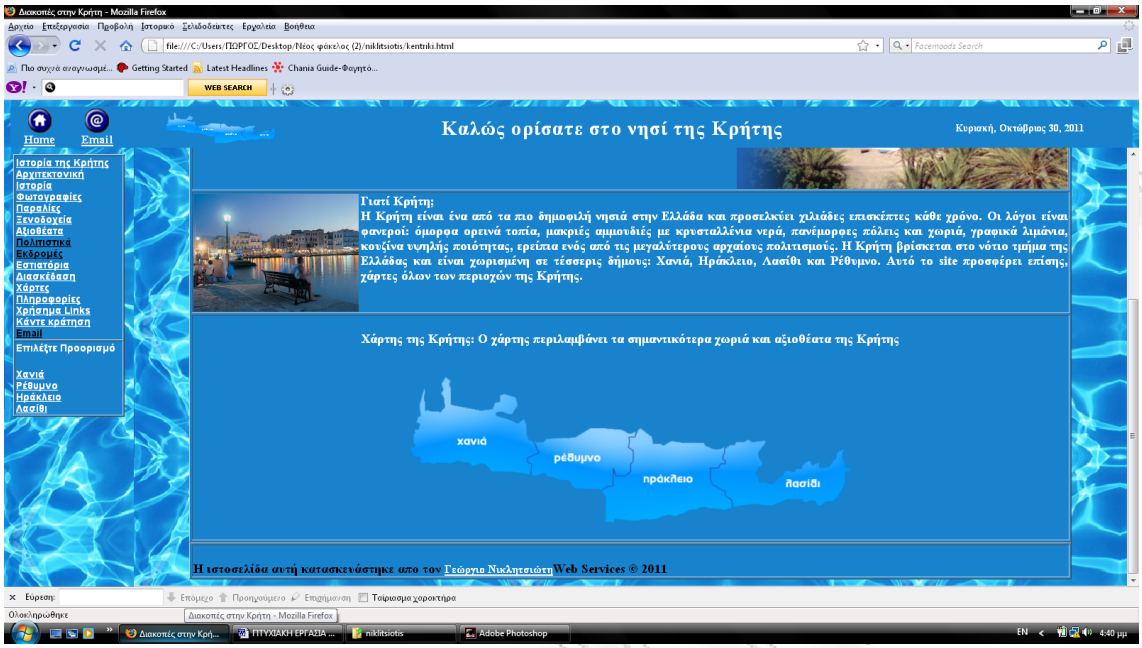
Στην συνέχεια παρουσιάζεται η υλοποίηση της ιστοσελίδας και αμέσως μετά παρουσιάζεται η διαδικασία για την δημιουργία και ενσωμάτωση ηλεκτρονικής υπογραφής στην ιστοσελίδα.

8.2. Υλοποίηση ιστοσελίδας

Σε αυτήν την ενότητα παρουσιάζεται ο κώδικας HTML, των κυριότερων σελίδων της ιστοσελίδας που έχουμε υλοποιήσει.

Η κεντρική σελίδα της ιστοσελίδας μας, παρουσιάζεται στην εικόνα 25 και τον κώδικα HTML τον παραθέτουμε πιο κάτω. Η κεντρική σελίδα αποτελείται από τρεις σελίδες τον κώδικα και την μορφή των οποίων θα δούμε στην συνέχεια.

```
<html>

<head>

<title>Διακοπές στην Κρήτη</title>

<META http-equiv=content-type content="text/html; charset=iso-8859-7">

</head>

<frameset frameBorder=0 frameSpacing=0 rows="60,*">

<frame name="top" src="top.html" scrolling=no>

<frameset frameBorder=0 frameSpacing=0 cols="165,*">

<frame name="left" src="left.html" scrolling="no">

<frame name="center" src="index.html">

</frameset>

</frameset>

<noframes><body>KPHTH</body></noframes>

</html>
```



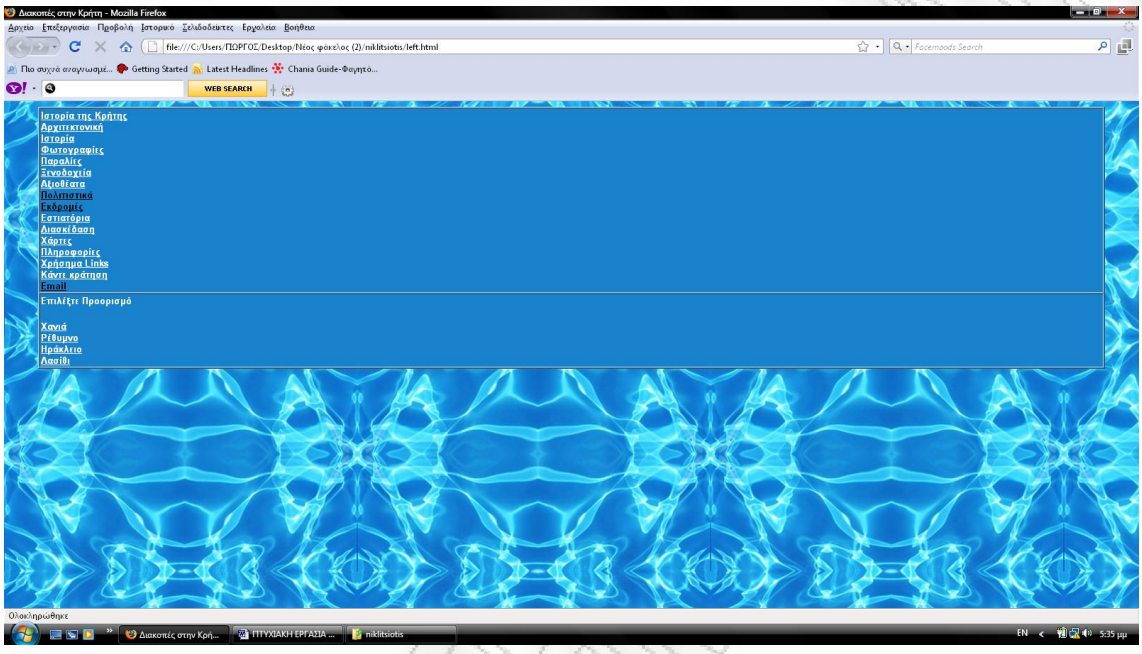
Εικόνα 25. Κεντρική σελίδα

Η αριστερή πλευρά της κεντρικής σελίδας της ιστοσελίδας μας, παρουσιάζεται στην εικόνα 26 και τον κώδικα HTML τον παραθέτουμε πιο κάτω.

```
<html>

<head>

<title>Διακοπές στην Κρήτη</title>

<link rel="stylesheet" type="text/css" href="KRHTH.css">

</head>

<body class="background"">

<table align="center" cellspacing="1" cellpadding="1"
bgcolor="#1982CD" width="95%" align="center" border="1">

<tr>

<th align="left" width="16%">

<font size="2" face="arial" color="FFFFFF">

<a class="link" href="istoria.html" target="center">Ιστορία της
Κρήτης</a><br>

<a class="link" href="arxitektoniki.html"
target="center">Αρχιτεκτονική</a><br>
```

```
<a class="link" href="chaniaistoria.html"
target="center">Ιστορία</a><br>

<a class="link" href="chaniaphotos.html"
target="center">Φωτογραφίες</a><br>

<a class="link" href="chaniaparalies.html"
target="center">Παραλίες</a><br>

<a class="link" href="chaniahotel.html"
target="center">Ξενοδοχεία</a><br>

<a class="link" href="chaniadiaksiotheata.html"
target="center">Αξιοθέατα</a><br>

<a class="link" href="chaniapolitistika.html"
target="center">Πολιτιστικά</a><br>

<a class="link" href="chaniaekdromes.html"
target="center">Εκδρομές</a><br>

<a class="link" href="chaniaestiatoria.html"
target="center">Εστιατόρια</a><br>

<a class="link" href="chaniadiaskedasi.html"
target="center">Διασκέδαση</a><br>

<a class="link" href="chaniamap.html" target="center">Χάρτες</a><br>

<a class="link" href="chaniainfo.html"
target="center">Πληροφορίες</a><br>

<a class="link" href="chanialinks.html" target="center">Χρήσημα
Links</a><br>

<a class="link" href="kratisi.html" target="center">Κάντε
κράτηση</a><br>

<a class="link" href="mailto:gniklitsiotis@yahoo.gr?subject=Κράτηση
Ξεδοδοχείου">Email</a>

</font>

</th>

<tr>

<th align="left" width="15%">
<div class="word3">Επιλέξτε Προορισμό</div><br>

<a class="link" href="chania.html" target="center"> Χανιά</a><br>

<a class="link" href="rethimno.html" target="center">Ρέθυμνο</a><br>

<a class="link"href="iraklio.html" target="center">Ηράκλειο</a><br>

<a class="link" href="lasithi.html" target="center">Λασίθι</a>

</th>
```

```
</table>

</body>

</html>
```

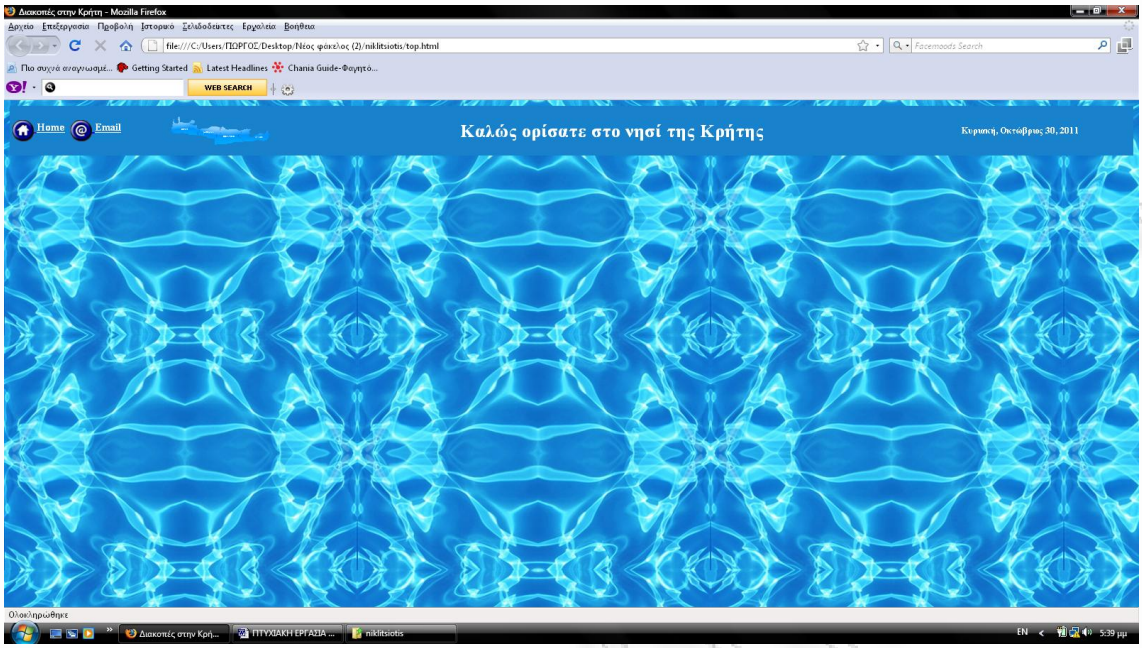


Εικόνα 26. Αριστερή σελίδα

Η πάνω πλευρά της κεντρικής σελίδας της ιστοσελίδας μας, παρουσιάζεται στην εικόνα 27 και τον κώδικα HTML τον παραθέτουμε πιο κάτω.

```
<html>

<head>

<title>Διακοπές στην Κρήτη</title>

<link rel="stylesheet" type="text/css" href="KRHTH.css">

</head>

<body class="background">

<table bgcolor="#1982CD" align="center" border="0" height="10%"
width="100%">

<tr>
<th align="center" width="5%">
<a href="index.html" target="center"><img
src="photos/buttons/home.gif" height="30" width="30" align="middle"
border="0">
<a class="links" href="index.html" target="center">Home</a>
</th>
```

```
<th align="center" width="5%">
<a href="mailto:gniklitsiotis@yahoo.gr?subject=Κράτηση Ξεδοδοχείου"
target="center"><img src="photos/buttons/email.gif" height="30"
width="30" align="middle" border="0">
<a class="links" href="mailto:gniklitsiotis@yahoo.gr?subject=Κράτηση
Ξεδοδοχείου">Email</a>
</th>

<th align="center" width="17%">
<img src="photos/kriti/kriti.png" height="40" width="140" align="top">
</th>

<th valign="center" align="center">
<div class="title1">Καλώς ορίσατε στο νησί της Κρήτης</div>
</th>

<th align="left" width="20%">

<div class="word4">

<script language="JavaScript">

var now = new Date();
var days = new
Array('Κυριακή','Δευτέρα','Τρίτη','Τετάρτη','Πέμπτη','Παρασκευή','Σάββ
ατο');
var months = new
Array('Ιανουάριος','Φεβρουάριος','Μάρτιος','Απρίλιος','Μάιος','Ιούνιος
','Ιούλιος','Αύγουστος','Σεμπτέμβριος','Οκτώβριος','Νοέμβριος','Δεκέμβ
ριος');
var date = ((now.getDate()<10) ? "0" : "")+ now.getDate();
function fourdigits(number)
{return (number < 1000) ? number + 1900 : number;}
today =  days[now.getDay()] + ", " +
months[now.getMonth()] + " " +
date + ", " +
(fourdigits(now.getYear())) ;
document.write(today);

</script>

</div>

</th>

</tr>

</table>

</body>

</html>
```



Εικόνα 27. Πάνω σελίδα

Η κεντρική σελίδα της κεντρικής σελίδας της ιστοσελίδας μας, παρουσιάζεται στην εικόνα 28 και τον κώδικα HTML τον παραθέτουμε πιο κάτω.

```
<html>

<head>

<title>Διακοπές στην Κρήτη</title>

<link rel="stylesheet" type="text/css" href="KRHTH.css">
</head>

<body class="background">

<table bgcolor="#1982CD" width="90%" align="center" border="1">

<tr>
<th>
<div class="word2">
<pre>
"Η αίσθηση του μυστηρίου της Κρήτης είναι εξαιρετικά βαθιά.
Όποιος βάζει το πόδι του σε αυτό το νησί αισθάνεται μια μυστήρια
δύναμη
να διακλαδίζεται θερμά και ευεργετικά στις φλέβες του,
αισθάνεται την ψυχή του να αρχίζει να τρανεύει"
Νίκος Καζαντζάκης (Αναφορά στον Γκρέκο)
</pre>
</div>
</th>
</tr>

<tr>
<th align="justify">
```

```
<img src="photos/kriti/crete1.jpg" height="195" width="420"
align="right" alt="ΚΡΗΤΗ">

<div class="word">
Το νησί της Κρήτης είναι το μεγαλύτερο νησί της Ελλάδας. Έχει ποικίλα
και απίστευτα όμορφα τοπία που αποτελούνται από βουνά, εντυπωσιακές
χαράδρες, σπηλιές, αρχαιολογικές ανασκαφές, Μινωικά Παλάτια,
Βυζαντινές εκκλησίες και ειδυλλιακές παραλίες με λεπτή χρυσή άμμο η
πολύχρωμα χαλίκια και κρυσταλλένια νερά. Όλοι αυτοί οι θησαυροί
αποτελούν τον λόγο για τον οποίο η Κρήτη έχει γίνει ένας τόσο
δημοφιλής προορισμός και γοητεύει οποίον την επισκεφτεί.
Αυτό το site, προσφέρει πολλές πληροφορίες: αρχιτεκτονική, χάρτες,
ιστορία, φωτογραφίες, παραλίες μουσεία και πολλά άλλα!!!
</div>

</th>

</tr>


<tr>
<th align="justify">
<img src="photos/chania/chania.jpg" height="150" width="210"
align="left" alt="Χανία">
<div class="word">
Γιατί Κρήτη;<br>
Η Κρήτη είναι ένα από τα πιο δημοφιλή νησιά στην Ελλάδα και προσελκύει
χιλιάδες επισκέπτες κάθε χρόνο.
Οι λόγοι είναι φανεροί: όμορφα ορεινά τοπία, μακριές αμμουδιές με
κρυσταλλένια νερά, πανέμορφες πόλεις και χωριά, γραφικά λιμάνια,
κουζίνα υψηλής ποιότητας, ερείπια ενός από τις μεγαλύτερους αρχαίους
πολιτισμούς.
Η Κρήτη βρίσκεται στο νότιο τμήμα της Ελλάδας και είναι χωρισμένη σε
τέσσερις δήμους: Χανιά, Ηράκλειο, Λασίθι και Ρέθυμνο. Αυτό το site
προσφέρει επίσης, χάρτες όλων των περιοχών της Κρήτης.
</div>

</th>

</tr>

<tr>

<th>
<div class="word1"><br>
Χάρτης της Κρήτης: Ο χάρτης περιλαμβάνει τα σημαντικότερα χωριά και
αξιοθέατα της Κρήτης
</div><br><br>

<img src="photos/kriti/kriti.png " height="187" width="560"
align="down" usemap="#kriti" alt="Χάρτης Κρήτης" border="0">

<map name="kriti">

<area shape="poly"
coords="10, 117, 0, 87, 12, 17, 24, 14, 23, 40, 35, 44, 41, 36, 34, 13,
43, 3, 52, 0, 57, 14, 55, 31, 90, 40, 102, 34, 111, 30, 126, 20, 140,
34, 135, 51, 149, 57, 158, 75, 159, 85, 163, 99, 149, 107, 154, 114,
155, 130, 92, 121, 67, 115"
```

```
href="chania.html">

<area shape="poly"
coords="161, 82, 179, 75, 208, 77, 227, 65, 273, 67, 288, 70, 278, 77,
278, 87, 285, 95, 282, 110, 282, 120, 264, 127, 259, 118, 257, 138,
242, 145, 208, 145, 198, 134, 182, 134, 172, 129, 157, 128, 153, 109,
165, 99"
href="rethimno.html">

<area shape="poly"
coords="286, 76, 295, 63, 314, 82, 323, 86, 332, 80, 371, 82, 384, 89,
403, 87, 400, 101, 403, 109, 394, 116, 383, 117, 387, 137, 402, 142,
403, 151, 411, 157, 413, 168, 402, 170, 384, 168, 369, 168, 338, 177,
328, 177, 308, 183, 298, 179, 290, 184, 268, 180, 263, 186, 251, 183,
252, 156, 248, 145, 260, 138, 261, 118, 266, 125, 284, 120, 287, 96,
281, 87, 281, 76"
href="iraklio.html">

<area shape="poly"
coords="399, 90, 418, 83, 450, 80, 441, 95, 446, 109, 439, 123, 443,
133, 458, 135, 475, 119, 488, 119, 505, 108, 512, 112, 515, 107, 520,
116, 539, 105, 538, 97, 554, 90, 550, 101, 555, 115, 560, 117, 554,
121, 552, 138, 538, 159, 527, 159, 520, 165, 513, 158, 501, 161, 495,
156, 481, 155, 458, 164, 438, 163, 408, 168, 410, 159, 400, 152, 400,
145, 384, 137, 379, 121, 392, 118, 401, 112, 398, 102"
href="lasithi.html">

</map>

</th>

</tr>

</table>

<table bgcolor="#1982CD" width="90%" align="center" border="1">

<tr>

<th align="left"><br>

<span class="creation">Η ιστοσελίδα αυτή κατασκευάστηκε απο τον <a
class="links1" href="STOIXEIA.html">Γεώργιο Νικλητσιώτη</a>Web
Services © 2011</span>

</th>

</tr>

</table>

</body>

</html>
```

Εικόνα 28. Βασική σελίδα

Στην συνέχεια παραθέτουμε τον κώδικα HTML, μιας σελίδας της ιστοσελίδας μας, όπως αυτή φαίνεται όταν ο τελικός χρήσης πραγματοποιεί πλοήγηση σε αυτήν. Η σελίδας φαίνεται και στην εικόνα 29 που παραθέτουμε.

```
<html>

<head>

<title>Διακοπές στην Κρήτη</title>

<link rel="stylesheet" type="text/css" href="KRHTH.css">

</head>

<body class="background">

<caption>
<div class="title"><b><a name="chania">XANIA</a></b></div>
</caption>

<table bgcolor="#1982CD" width="90%" align="center" border="1">

<tr>

<th align="left" width="16%">

<a class="links" href="chaniaistoria.html" target="center">Ιστορία</a>

<a class="links" href="chaniaphotos.html"
target="center">Φωτογραφίες</a>

<a class="links" href="chaniaparalies.html"
target="center">Παραλίες</a>
```

```
<a class="links"  href="chaniahotel.html"
target="center">Ξενοδοχεία</a>

<a class="links" href="chaniadiaksiotheata.html"
target="center">Αξιοθέατα</a>

<a class="links" href="chaniapolitistika.html"
target="center">Πολιτιστικά</a>

<a class="links" href="chaniaekdromes.html"
target="center">Εκδρομές</a>

<a class="links" href="chaniaestiatoria.html"
target="center">Εστιατόρια</a>

<a class="links" href="chaniadiaskedasi.html"
target="center">Διασκέδαση</a>

<a class="links" href="chaniamap.html" target="center">Χάρτες</a>

<a class="links" href="chaniainfo.html"
target="center">Πληροφορίες</a>

<a class="links" href="kratisi.html" target="center">Κάντε κράτηση</a>

<a class="links" href="chanialinks.html" target="center">Χρήσημα
Links</a>

</th>

</table>

<table bgcolor="#1982CD" width="90%" align="center" border="1">

<tr>
<th align="center">
<div class="title2">Η πόλη που ποτέ δεν κοιμάται</div>
</th>
</tr>

<tr>
<th align="justify">
<img src="photos/chania/chania0.jpg" height="195" width="420"
align="right" alt="Τα πανέμοπρφα Χανία">
<div class="word">
Ολοι οι τουρίστες που τη επισκέπτονται, σπαταλάνε το χρόνο τους στην
περαντζάδα, προσπαθόντας να δουν όσα περισσότερα μπορούν. Μια πόλη για
όλα τα γούστα, ακόμα και για τα ποιό προχωρημένα. Αν ανηφορίσετε προς
το Ακρωτήρι, στο δρόμο που οδηγεί στους τάφους των βενιζέλων και
κοιτάξετε πίσω σας, θα συμφωνήσετε μ'αυτούς που αβίαστα ονόμασαν τα
Χανιά την οραιότερη
Ελληνική πόλη. Δαντελωτές παραλίες, βράχοι που ξεψυχούν στη φιλόξενη
θάλασσα. Η Χαλέπα, το όμορφο Βενετσιάνικο λιμάνι, το φρούριο Φίρκα, το
Καστέλι, σχηματίζουν εικόνες που μαρτυρούν ότι κάπου εδώ χτυπά μια
καρδιά 3.000 χρόνων που σας προκαλεί να την ανακαλύψετε. Τα Χανιά δεν
είναι μια απλή πόλη. Είναι ο ζωντανός μάρτυρας της συναρπαστικής
ιστορίας της Μεγαλονήσου μας.
Τα Χανιά πήραν το όνομα τους από το προελληνικό τοπωνύμιο Αλχανιά, που
οι Αραβες, μπερδεμένοι από το αρχαίο "αλ" που είναι ίδιο με το άρθρο
```

τους, μετέτρεψαν σε Al Hanim. Το ξαναπήραμε εμείς, το μεταφράσαμε πιστά και προέκυψε η ονομασία Χανιά.Αλλη εκδοχή είναι από το ψάρι χάνος, πληθυντικός Χανιά, ή από το παλίο όνομα του νησιού Χθόνα.
Οι Κρητικοί υποστηρίζουν ότι η πόλη τους είναι η πιο ερωτική στη χώρα και ότι οι ίδιοι είναι οι καλύτεροι εραστές. Ακόμα υπερηφανεύονται για την Δημοτική τους Αγορά,την οποία εγκαινίασε ο Ελευθέριος Βενιζέλος, στις 4 Δεκεμβρίου 1913, στα πλαίσια των εκδηλώσεων για το εορτασμό της ένωσης της Κρήτης με την Ελλάδα. Θα βρείτε πολλά καταστήματα με ντόπια προιόντα, αλλά και αρκετά ρακάδικα. Αν δεν δοκιμάσετε την μπουγάτσα του Ιορδάνη θα έχετε διαπράξει ένα τεράσιο λάθος. Με δύο παραρτήματα, ένα στο λιμάνι και ένα στην πόλη. Χρησιμοποιεί αγνά υλικά, την top μυζήθρα και τα μυστικά της κατασκευής κουβαλημένα από την Μικρασία, διατηρόντας την καλή παράδωση. Στην τοποθεσία Βρύσες, στο δρόμο από τα Χανιά προς το Ρέθυμνο, θα συναντήσετε το καλύτερο γιαούρτι με μέλι. Τα μαγαζάκια είναι αρκετά, το γιαούρτι όμως είναι ένα και μοναδικό. Και κάτι ακόμα. Coca Cola βρίσκεις και στην Αθήνα. Γκαζόζα "Γεράνι" με άρωμα βανίλιας μόνο στην Κρήτη.
Παρ'όλα αυτά για οποιοδήποτε πρόβλημα σας παρουσιαστεί σχετικά με την διαμονή σας, απευθυνθείτε στην Τουριστική Αστυνομία και ει δυνατόν ζητήστε την συνδρομή της κας Νταμαδάκη Κατερίνας.

</th>
</tr>

<tr>
<th align="justify">

Μουσεία:
Ιστορικό Αρχείο της Κρήτης: εκεί μπορείτε να δείτε όλα τα αρχεία των επαναστάσεων του 19ου αιώνα, το αρχείο Κρητικού Τύπου από το 1831, την εξειδικευμένη βιβλιοθήκη με τα 500.000 έγγραφα, το αρχείο με τις 3.000 φωτογραφίες, καθώς και το ιστορικό λαογραφικό τμήμα.
Αρχαιολογικό Μουσείο των Χανίων: Θα δείτε σημαντικά ευρήματα από την ύστερη Νεολιθική εποχή, την Μινωική και τους ιστορικούς χρόνους.
Ναυτικό Μουσείο: μπορείτε να δείτε ναυτικούς Χάρτες, ομειώματα πλοίων, γκραβούρες, και τμήμα από την τροπίλη που βύθισε την "Ελλη".
Λαογραφικό Μουσείο: Θα δείτε ενδυμασίες, φινετσάτες δαντέλες, και εικόνες από την ζωή του 19ου αιώνα.

</th>
</tr>

<tr>
<th align="justify">

Παραλίες:
Κάποιες από τις ωραιότερες παραλίες της Κρήτης αλλά και ολόκληρης της Μεσογείου βρίσκονται εδώ.Ξεκινόντας από τα Χανιά με κατεύθυνση το Καστέλι η πρώτη παραλία είναι η Αγ.Μαρίνα. Τεράστια με πολλές ξαπλώστρες και ομπρέλες, καθώς και μαγαζία για να φάτε και να ξεδιψάσετε. Λίγο παραπάνω ο Πλατανιάς. Φτυστή η Αγ.Μαρίνα, με όμορφη αμμουδιά και σε μικρή απόσταση από το χωριό και δεκάδες εστιατόρια που προσφέρουν από καλαμαράκια μέχρι και κρέας. Στη συνέχεια το Μάλεμε και το Κολυμβάρι, και ο κόλπος του Κισσάμου, όπου τελίώνει και η εθνική οδός. Ομορφες, καθαρές και με κόσμο, ξενοδοχειακές μονάδες, αλλα και οικογενιακές παραλίες. Μην παραλείψετε να πα΄τε στο Ελαφονήσι. Παρότι νησί, είναι φανταστικό. Μοιάζει με πισίνα, έχει ζεστά νερά, δεν έχει όμως κοντινές ταβέρνες. Αλλες περιοχές είναι η Σκάλα και η Παχιά Αμμός,

οι δύο μεγαλύτερες αμμουδερές παραλίες, με ήρεμη κατάσταση. Τέλος οι παραλίες των Σφακίων. Η ποιό γνωστή το Φραγκοκάστελλο με ρηχά νερά και το ενετικό κάστρο να στέκεται έρημο και απειλητικό στη μέση της παραλίας. Βεβαια μην ξεχάσετε και το φαράγγι της Σαμαρίας. Για δυνατούς περπατητές.

</th>
</tr>

<tr>
<th align="justify">

Φαράγγι:
Το φαραγγι της Σαμαριάς είναι το ποιό γνωστό από τα πολλά που υπάρχουν στην Κρήτη, έχει μήκος 16χιλ., ανακηρύχθηκε Εθνικός Δριμός το 1962 και στα δάση του βρίσκουν καταφύγιο πολλά είδη άγριων πουλιών, άγρια θηλαστικά, μεταξύ των οποίων το πολυδιαφημισμένο κρι-κρι και το κρητικό κουνάβι γνωστό ως ζουρίδα. Κάθε χρόνο περίπου 300.000 επισκέπτονται το φαράγγι. Η διαδρομή στο φαράγγι είναι δύσκολη, ειδικά γι΄αυτούς που καπνίζουν. Σας περιμένουν πόλλες εκπλήξεις, μην βάλετε ψηλοτάκουνα, προτιμήστε αθλητικά παπούτσια και πάρτε μαζί σας φωτογραφική μηχανή. Η είσοδος κοστίζει 1.000 δρχ. και απαγορεύεται η διανυκτέρευση, το άναμμα φωτιάς, το κυνήγι, το κάπνισμα, το ραδιόφωνο, το ψάρεμα, το κολύμπι και τα οινοπνευματώδη ποτά. Θα φτάσετε εκεί αφού πάρετε λεωφορείοαπό τα Χανιά, θα κατεβελιτε στο Ξυλόκαστρο, θα κατεβείτε το φαράγγι, θα σβήσετε τα πόδια της στα νερά της Αγίας Ρούμελης, θα σηνεχίσετε με το καραβάκι για την Χώρα των Σφακίων και τέλος, αργά πια, θα επιβιβαστείτε στο λεοφορείο πίσω για τα Χανιά.

</th>
</tr>

<tr>
<th align="justify">

Για τον Νομό Χανίων
Τουριστική Αστυνομία: 73333
Λιμεναρχείο Χανίων: 45037
Λιμεναρχείο Σούδας: 89240
Ε.Ο.Τ.: 92943

</th>
</tr>

</table>

<table bgcolor="#1982CD" width="90%" align="center" border="1">
<tr>
<th align="center">
BACK
TOP
</th></tr>
</table>

</body>

</html>

Εικόνα 29. Κεντρική σελίδα Χανιά

Τέλος, παραθέτουμε τον κώδικα HTML, της σελίδας που αφορά την κράτηση ξενοδοχείου που έχει την δυνατότητα να κάνει ο τελικός χρήσης που πραγματοποιεί πλοήγηση σε αυτήν. Η σελίδας φαίνεται και στην εικόνα 30 που παραθέτουμε.

```
<html>

<head>

\title|Online kr;athsh jenodoxe;ioy!!!\/title|

<link rel="stylesheet" type="text/css" href="KRHTH.css">

</head>

<body class="background">

<caption>
<div class="title1"><b><a name="chania">Online Κράτηση
Ξενοδοχείου</a></b></div>
</caption>

<table bgcolor="#0099FF" width="80%" align="center" border="1">

<form name="form">

<tr>
<th colspan="2" height="40" align="center">
<div class="title1">ΣΤΟΙΧΕΙΑ ΠΕΛΑΤΗ</div></th></tr>
<tr>

<th align="left">
<span class="word">ONOMA:</span><br>
<input type="text name" name="fname" size="30" maxlength="30">
```

```
</th>

<th align="left">
<span class="word">ΕΠΩΝΥΜΟ:</span><br>
<input type="text name" name="lname" size="40" maxlength="40">
</th></tr>

<tr>
<th align="left">
<span class="word">ΟΝΟΜΑ ΠΑΤΡΟΣ:</span><br>
<input type="text name" name="patros" size="30" maxlength="30">
</th>
<th align="left">
<span class="word">ΕΠΩΝΥΜΟ:</span><br>
<input type="text name" name="lname" size="40" maxlength="40">
</th></tr>

<tr>
<th align="left">
<span class="word">ΔΙΕΥΘΥΝΣΗ:</span><br>
<input type="text name" name="fname" size="30" maxlength="30">
</th>
<th align="left">
<span class="word">ΑΡΙΘΜΟΣ:</span><br>
<input type="text name" name="lname" size="4" maxlength="4">
</th></tr>

<tr>
<th align="left">
<span class="word">ΠΟΛΗ:</span><br>
<input type="text name" name="arithmos" size="50" maxlength="50">
</th>
<th align="left">
<span class="word">Τ.Κ.:</span><br>
<input type="text name" name="tk" size="5" maxlength="5">
</th></tr>

<tr>
<th align="left">
<span class="word">ΑΡ. ΣΤΑΘΕΡΟΥ:</span><br>
<input type="text name" name="tilefono" size="25" maxlength="15">
</th>
<th align="left">
<span class="word">ΑΡ. ΚΙΝΗΤΟΥ:</span><br>
<input type="text name" name="kinito" size="25" maxlength="15">
</th></tr>

<tr>
<th align="left">
<span class="word">E-MAIL:</span><br>
<input type="text name" name="mail" size="50" maxlength="70">
</th>
<th></th>
</tr>

<tr>
<th  colspan="2" height="40" align="center"><br><br>
<div class="title1">ΣΤΟΙΧΕΙΑ ΚΡΑΤΗΣΗΣ</div>
</th></tr>
```

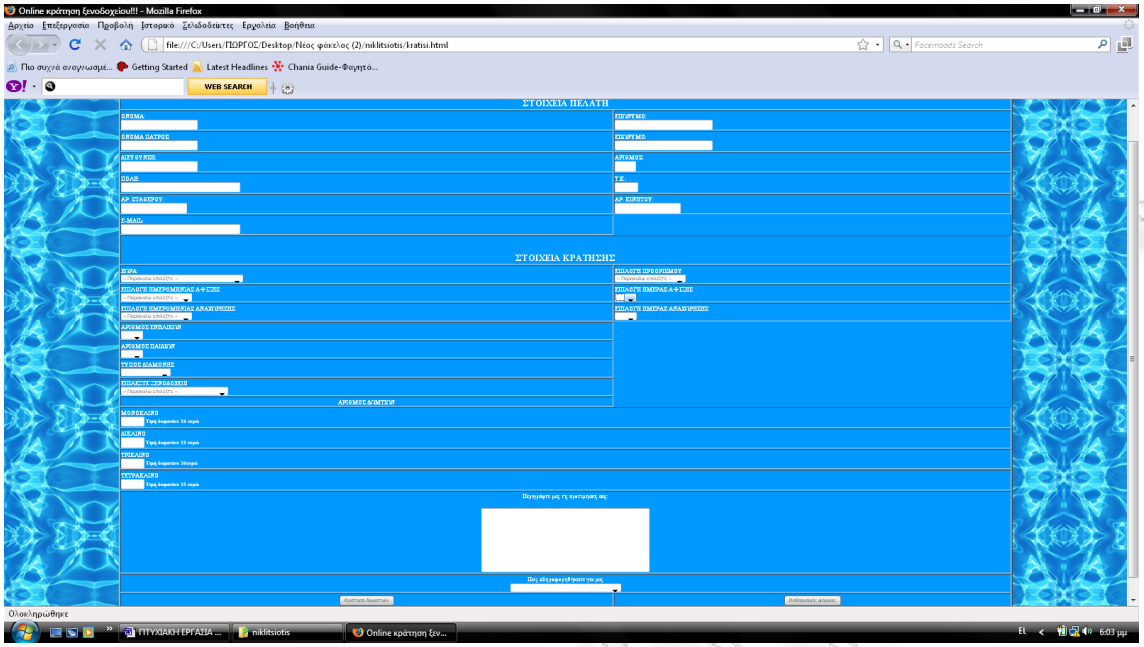
```
<tr>
<td>
<span class="word" for="enq_nationality">ΧΩΡΑ:</span><br>
<select id="enq_nationality" name="enq[nationality]"
class="selectbox">
<option>-- Παρακαλώ επιλέξτε --</option>
<option value="AF">Afghanistan</option>
. . .
. . .
. . .
<option value="ZW">Zimbabwe</option>

</select>
</td>

<td>
<span class="word">ΕΠΙΛΟΓΗ ΠΡΟΟΡΙΣΜΟΥ</span><br>
<select name="proorismos">
<option selected="xania">ΧΑΝΙΑ</option>
<option selected="rethimno">ΡΕΘΥΜΝΟ</option>
<option selected="irakleio">ΗΡΑΚΛΕΙΟ</option>
<option selected="lasithi">ΛΑΣΙΘΙ</option>
<option selected="keno">-- Παρακαλώ επιλέξτε --</option>
</select>
</td>
</tr>

<tr><td>
<span class="word">ΕΠΙΛΟΓΗ ΗΜΕΡΟΜΗΝΙΑΣ ΑΦΙΞΗΣ</span><br>
<select name="minas">
<option selected="ianouarios">ΙΑΝΟΥΑΡΙΟΣ</option>
<option selected="febrouarios">ΦΕΒΡΟΥΑΡΙΟΣ</option>
<option selected="martios">ΜΑΡΤΙΟΣ</option>
<option selected="aprilios">ΑΠΡΙΛΙΟΣ</option>
<option selected="maios">ΜΑΙΟΣ</option>
<option selected="iounios">ΙΟΥΝΙΟΣ</option>
<option selected="ioulios">ΙΟΥΛΙΟΣ</option>
<option selected="augoustos">ΑΥΓΟΥΣΤΟΣ</option>
<option selected="septembrios">ΣΕΠΤΕΜΒΡΙΟΣ</option>
<option selected="oktobrios">ΟΚΤΩΒΡΙΟΣ</option>
<option selected="noembrios">ΝΟΕΜΒΡΙΟΣ</option>
<option selected="dekembrios">ΔΕΚΕΜΒΡΙΟΣ</option>
<option selected="keno">-- Παρακαλώ επιλέξτε --</option>
</select>
</td>

<td>
<span class="word">ΕΠΙΛΟΓΗ ΗΜΕΡΑΣ ΑΦΙΞΗΣ</span><br>
<select name="mera">
<option selected="01">01</option>
<option selected="02">02</option>
<option selected="03">03</option>
<option selected="04">04</option>
<option selected="05">05</option>
<option selected="06">06</option>
<option selected="07">07</option>
<option selected="08">08</option>
<option selected="09">09</option>
<option selected="10">10</option>
```

```
<option selected="11">11</option>
<option selected="12">12</option>
<option selected="13">13</option>
<option selected="14">14</option>
<option selected="15">15</option>
<option selected="16">16</option>
<option selected="17">17</option>
<option selected="18">18</option>
<option selected="19">19</option>
<option selected="20">20</option>
<option selected="21">21</option>
<option selected="22">22</option>
<option selected="23">23</option>
<option selected="24">24</option>
<option selected="25">25</option>
<option selected="26">26</option>
<option selected="27">27</option>
<option selected="28">28</option>
<option selected="29">29</option>
<option selected="30">30</option>
<option selected="31">31</option>
<option selected="keno"></option>
</select>
</td></tr>

<tr><td>
<span class="word">ΕΠΙΛΟΓΗ ΗΜΕΡΟΜΗΝΙΑΣ ΑΝΑΧΩΡΗΣΗΣ</span><br>
<select name="minas1">
<option selected="ianouarios">ΙΑΝΟΥΑΡΙΟΣ</option>
<option selected="febrouarios">ΦΕΒΡΟΥΑΡΙΟΣ</option>
<option selected="martios">ΜΑΡΤΙΟΣ</option>
<option selected="aprilios">ΑΠΡΙΛΙΟΣ</option>
<option selected="maios">ΜΑΙΟΣ</option>
<option selected="iounios">ΙΟΥΝΙΟΣ</option>
<option selected="ioulios">ΙΟΥΛΙΟΣ</option>
<option selected="augoustos">ΑΥΓΟΥΣΤΟΣ</option>
<option selected="septembrios">ΣΕΠΤΕΜΒΡΙΟΣ</option>
<option selected="oktobrios">ΟΚΤΩΒΡΙΟΣ</option>
<option selected="noembrios">ΝΟΕΜΒΡΙΟΣ</option>
<option selected="dekembrios">ΔΕΚΕΜΒΡΙΟΣ</option>
<option selected="keno">-- Παρακαλώ επιλέξτε --</option>
</select>
</td>

<td>
<span class="word">ΕΠΙΛΟΓΗ ΗΜΕΡΑΣ ΑΝΑΧΩΡΗΣΗΣ</span><br>
<select name="mera1">
<option selected="01">01</option>
<option selected="02">02</option>
<option selected="03">03</option>
<option selected="04">04</option>
<option selected="05">05</option>
<option selected="06">06</option>
<option selected="07">07</option>
<option selected="08">08</option>
<option selected="09">09</option>
<option selected="10">10</option>
<option selected="11">11</option>
<option selected="12">12</option>
```

```
<option selected="13">13</option>
<option selected="14">14</option>
<option selected="15">15</option>
<option selected="16">16</option>
<option selected="17">17</option>
<option selected="18">18</option>
<option selected="19">19</option>
<option selected="20">20</option>
<option selected="21">21</option>
<option selected="22">22</option>
<option selected="23">23</option>
<option selected="24">24</option>
<option selected="25">25</option>
<option selected="26">26</option>
<option selected="27">27</option>
<option selected="28">28</option>
<option selected="29">29</option>
<option selected="30">30</option>
<option selected="31">31</option>
<option selected="keno"></option>
</select>
</td></tr>

<tr><td>
<span class="word">ΑΡΙΘΜΟΣ ΕΝΗΛΙΚΩΝ</span><br>
<select name="arithmosenilikon">
<option selected="01">01</option>
<option selected="02">02</option>
<option selected="03">03</option>
<option selected="04">04</option>
<option selected="05">05</option>
<option selected="06">06</option>
<option selected="07">07</option>
<option selected="08">08</option>
<option selected="09">09</option>
<option selected="10">10</option>
<option selected="keno"></option>
</select>
</td></tr>

<tr><td>
<span class="word">ΑΡΙΘΜΟΣ ΠΑΙΔΙΩΝ</span><br>
<select name="arithmospaidion">
<option selected="01">01</option>
<option selected="02">02</option>
<option selected="03">03</option>
<option selected="04">04</option>
<option selected="05">05</option>
<option selected="06">06</option>
<option selected="07">07</option>
<option selected="08">08</option>
<option selected="09">09</option>
<option selected="10">10</option>
<option selected="keno"></option>
</select>
</td></tr>


<tr><td>
```

```
<span class="word">ΤΥΠΟΣ ΔΙΑΜΟΝΗΣ</span><br>
<select name="tipos">
<option selected="ksenodoxeio">ΞΕΝΟΔΟΧΕΙΟ</option>
<option selected="pansion">ΠΑΝΣΙΟΝ</option>
<option selected="diamerisma">ΔΙΑΜΕΡΙΣΜΑ</option>
<option selected="  "> </option>
<option selected="  "> </option>
<option selected="  "> </option>
<option selected="keno"></option>
</select>
</td></tr>

<tr><td>
<span class="word">ΕΠΙΛΕΞΤΕ ΞΕΝΟΔΟΧΕΙΟ</span><br>
<select name="perioxi">
<option selected="hotel">Perle Resort Hotel & Health Spa
Marine</option>
<option selected="hotel">Renieris Hotel</option>
. . .
. . .
. . .
<option selected="hotel">Paradisio</option>
<option selected="keno">-- Παρακαλώ επιλέξτε --</option>
</select>
</td></tr>

<tr>
<th>
<span class="word">ΑΡΙΘΜΟΣ ΔΩΜΤΙΩΝ</span><br>
</th>
</tr>

<tr><td colspan="2">
<span class="word">ΜΟΝΟΚΛΙΝΟ</span><br>
<input type="text" name="monoklino" size="5" maxlength="3" value="">
<span class="word1">Τιμή δωματίου 20 ευρώ</b></span>
</td></tr>

<tr><td colspan="2">
<span class="word">ΔΙΚΛΙΝΟ</span><br>
<input type="text" name="diklino" size="5" maxlength="3" value="">
<span class="word1">Τιμή δωματίου 25 ευρώ</span>
</td></tr>

<tr><td colspan="2">
<span class="word">ΤΡΙΚΛΙΝΟ</span><br>
<input type="text" name="triklino" size="5" maxlength="3" value="">
<span class="word1">Τιμή δωματίου 30ευρώ</span>
</td></tr>

<tr><td colspan="2">
<span class="word">ΤΕΤΡΑΚΛΙΝΟ</span><br>
<input type="text" name="tetraklino" size="5" maxlength="3" value="">
<span class="word1">Τιμή δωματίου 35 ευρώ</span>
</td></tr>


<tr>
<th colspan="2" height="40" align="center">
```

```
<span class="word">
<label for="f-message">Περιγράψτε μας τις προτιμήσεις
σας:</label><br><br>
<textarea id="f-message" name="enq[message]" rows="5" cols="50"
style="width: 475px; height: 180px;"></textarea>
</span>
</th>
</tr>

<tr>
<th colspan="2" height="40" align="center">
<span class="word">
<label for="f-findout">Πώς πληροφορηθήκατε για μας</label><br>
<select id="f-findout" name="enq[findout]" class="selectbox">
<option></option>
<option>Μέσω μηχανής αναζήτησης (π.χ. Google)</option>
<option>Έχω ταξιδεύσει με σας ξανά</option>
<option>Κάποιος μας σύστησε σε σας</option>
<option>Διάβασα για σας κάπου</option>
<option>Άλλο</option>
<option>-- Παρακαλώ επιλέξτε --</option>
</select>
</span>
</th>
</tr>

<tr>
<th>
<input type="button" name="kratisi" value="Κράτηση δωματιών"
onClick="alert(form.monoklino.value * 20 + form.diklino.value * 25 +
form.triklino.value * 30 + form.tetraklino.value * 35)">
</th>

<th>
<input type="reset" value="Καθαρισμός φόρμας"/>
</th>
</tr>
</form>
<br><br>
</td>
</tr>

</table>

<table  bgcolor="#0099FF" width="80%" align="center" border="1">

<tr>
<th align="center">
<a class="back" href="index.html"><b>BACK</b></a>
<a class="back" href="#chania"><b>TOP</b></a>
</th></tr>

</table>

</doby>

</html>
```



Εικόνα 30. Σελίδα κράτησης

8.3. Ενσωμάτωση ηλεκτρονικής υπογραφής και ηλεκτρονικού πιστοποιητικού

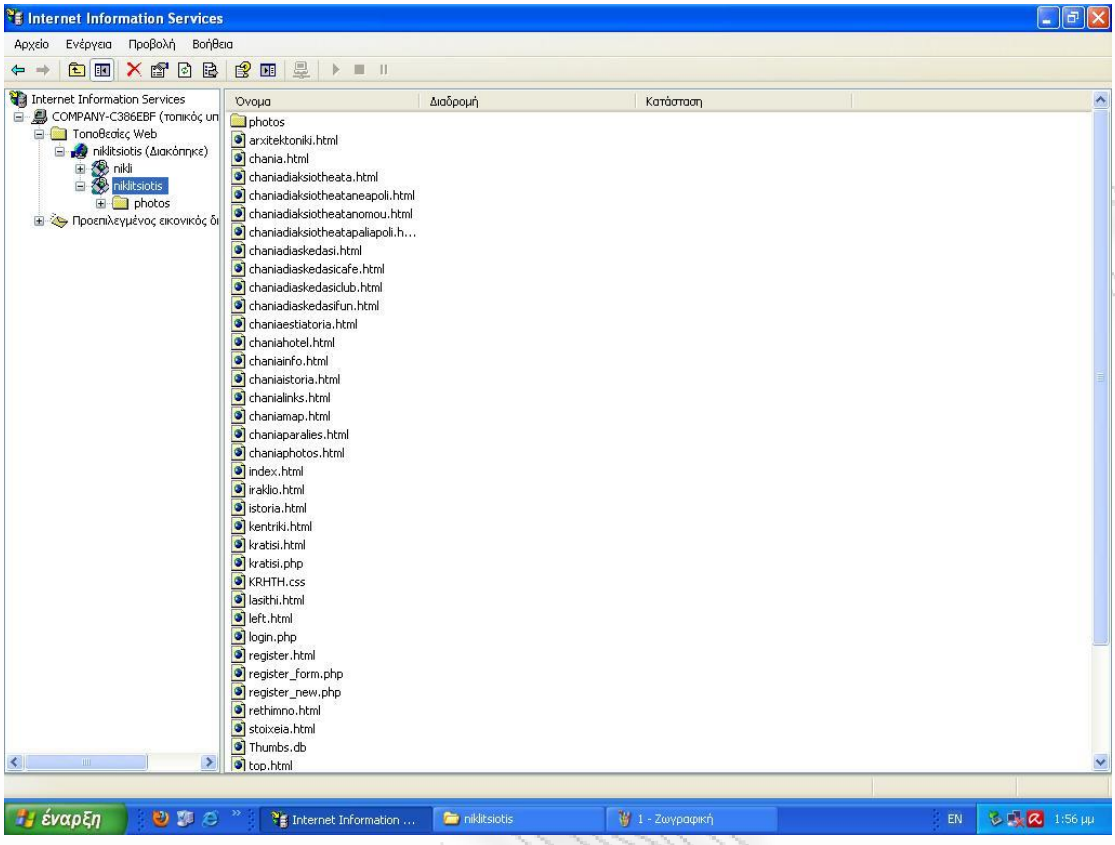
Τον τρόπο με τον οποίο συνδυάζεται τελικά η υλοποίηση μιας ιστοσελίδας με τις ηλεκτρονικές υπογραφές, τον βλέπουμε εάν σκεφτούμε, πώς μπορεί να γνωρίζει ένας τυχαίος απλός χρήστης ότι αυτή η ιστοσελίδα υπάρχει και είναι ασφαλής για την κράτηση ώστε να δώσει τα στοιχεία του άφοβα και με ποιον τρόπο κάποιος μπορεί να του διασφαλίσει ότι τα προσωπικά του δεδομένα κάποιος κακόβουλος τρίτος δεν θα του τα κλέψει.

Η ηλεκτρονική υπογραφή στην συγκεκριμένη υλοποίηση έρχεται να λύσει αυτά τα προβλήματα και να παρέχει ασφάλεια και εμπιστευτικότητας στον χρήστη, ώστε να του διασφαλίσει το ασφαλές και την αυθεντικότητας τις ηλεκτρονικής συναλλαγής .

Πριν πραγματοποιήσουμε οποιαδήποτε άλλη ενέργεια θα πρέπει να κάνουμε έλεγχο προκειμένου να επιβεβαιώσουμε ότι οι επιλογές του Internet Information Services είναι ενεργοποιημένες. Προκειμένου να πραγματοποιήσουμε τον έλεγχο αυτό πάμε στον Πίνακα Ελέγχου και στην Προσθαφαίρεση προγραμμάτων επιλέγουμε αριστερά Ενεργοποίηση ή Απενεργοποίηση των δυνατοτήτων των Windows στο παράθυρο που ανοίξει βλέπουμε εάν είναι επιλεγμένο το Internet Information Services, εάν είναι κλείνουμε το παράθυρο, εάν δεν είναι το επιλέγουμε και πατάμε ενεργοποίηση ώστε να ενεργοποιηθούν οι Internet Information Services.

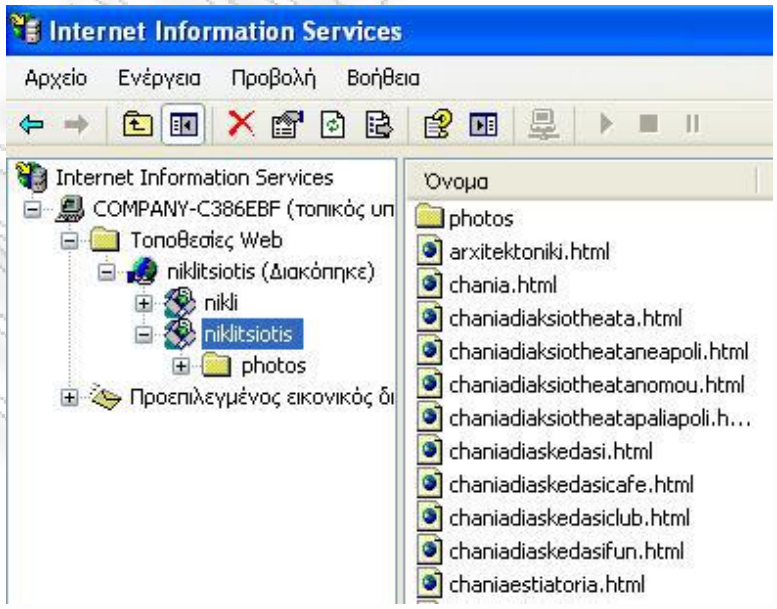
Μετά την πραγματοποίηση του πιο πάνω βήματος, θα πρέπει να ενσωματώσουμε την ηλεκτρονική υπογραφή και το ηλεκτρονικό πιστοποιητικό στην ιστοσελίδα μας. Προκειμένου να το πετύχουμε αυτό κάνουμε χρήση του SSL Diagnostics Version 1.1, το οποίο παρέχεται δωρεάν από την Microsoft για εκπαιδευτικούς κυρίους σκοπούς.

Ενώ έχουμε τρέξει το πρόγραμμα SSL Diagnostics επιλέγουμε το Open Internet Information Services και στο νέο παράθυρο που εμφανίζεται, στην αριστερή πλευρά της οθόνης δημιουργούμε στο σημείο Τοποθεσίες web την δική μας web τοποθεσία όπως φαίνεται στην εικόνα 31.



Εικόνα 31. Κεντρική οθόνη Internet Information Services

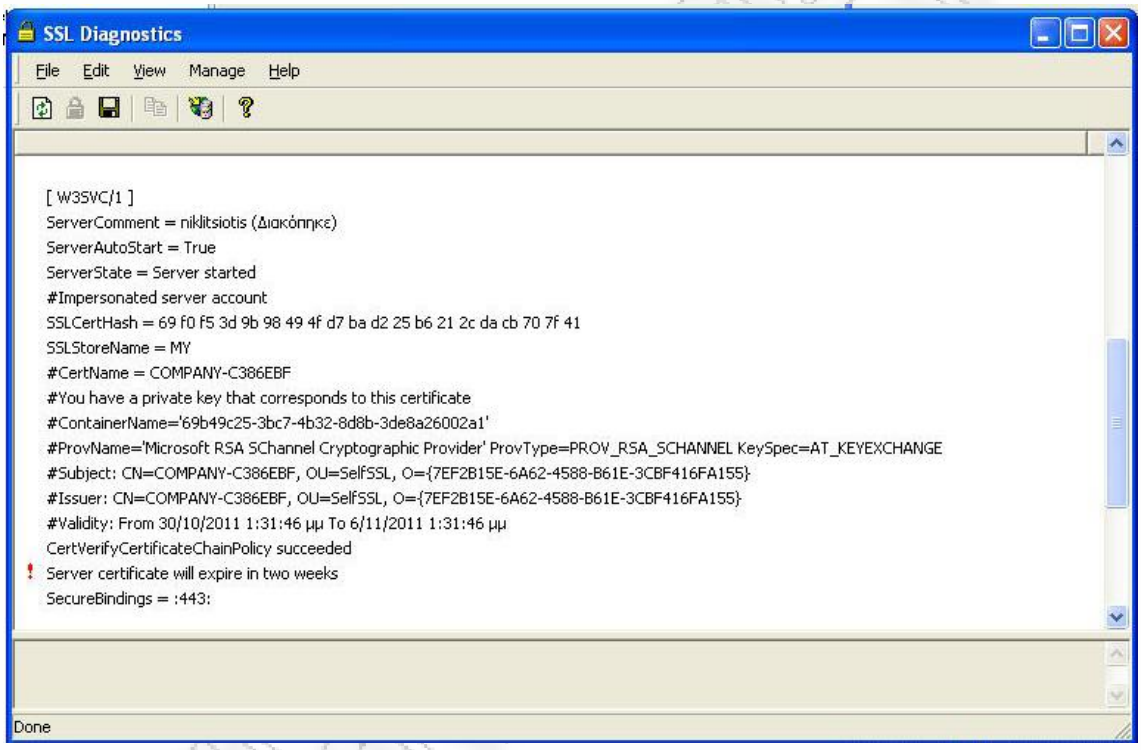
Στην εικόνα 32, παρουσιάζεται η τοποθεσίας web που έχουμε δημιουργήσει στο Internet Information Services, για την ιστοσελίδα που έχουμε υλοποιήσει. Αριστερά φαίνεται η τοποθεσία που την έχουμε ονομάσει niklitsiotis και δεξιά φαίνονται όλες οι σελίδες που αποτελούν το σύνολο της τοποθεσίας web.



Εικόνα 32. Δημιουργία τοποθεσίας web

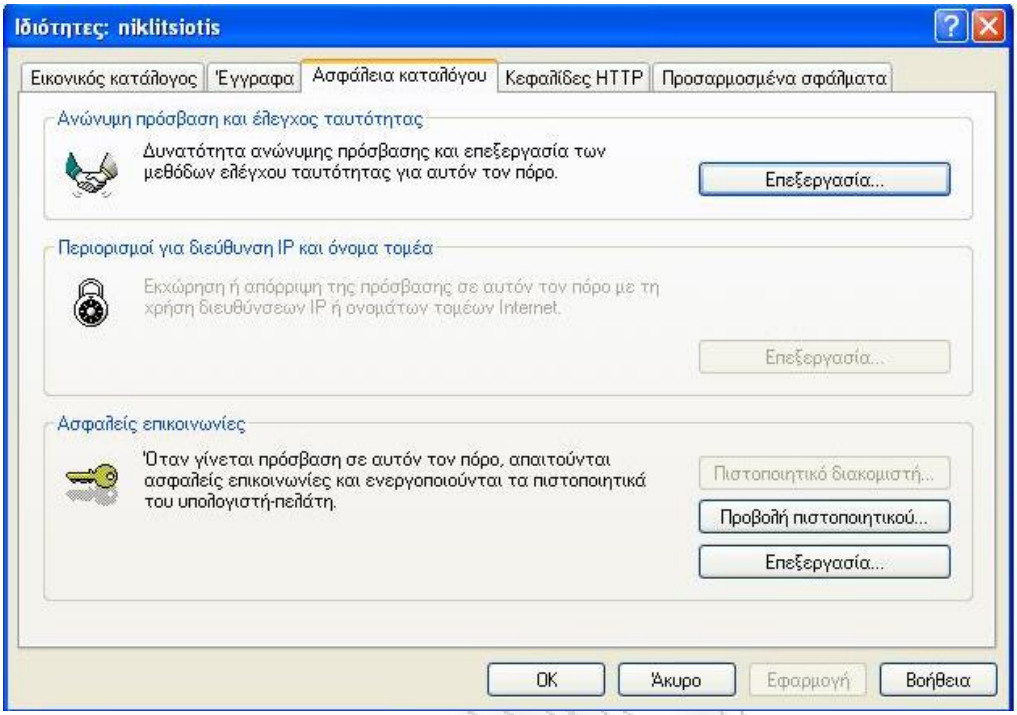
Μέχρι το σημείο αυτό έχουμε υλοποιήσει την ιστοσελίδα μας και την έχουμε ορίσει ως τοποθεσία web στην εφαρμογή SSL Diagnostics. Στην συνέχεια επιλέγουμε το Έναρξη στοιχείου από το μενού του στο Internet Information Services, ώστε να ορίσουμε ότι η τοποθεσία web με όνομα niklitsiotis επιθυμούμε να εκτελείται και είναι εκείνη στην οποία θα εφαρμόσουμε το ηλεκτρονικό κλειδί και το ηλεκτρονικό πιστοποιητικό. Όταν κάνουμε αυτή την επιλογή πάμε στην κεντρική οθόνη του SSL Diagnostics και κάνουμε κλικ στην επιλογή Refresh.

Στην εικόνα 33, παρουσιάζεται η ηλεκτρονική υπογραφή που έχει δημιουργηθεί και έχει ενσωματωθεί στην ιστοσελίδα μας. Στην ηλεκτρονική υπογραφή βλέπουμε ότι μας ενημερώνει ότι έχουμε ένα ιδιωτικό κλειδί για αυτό το πιστοποιητικό και ότι αυτό έχει εφαρμοστεί στο niklitsiotis που είναι η ιστοσελίδα μας ενημερώνει επίσης, για την εγκυρότητα του κλειδιού και του πιστοποιητικού έχει διάρκεια από τις 30/10/2011 1:31:46 μμ μέχρι τις 06/11/2011 1:31:46 μμ.



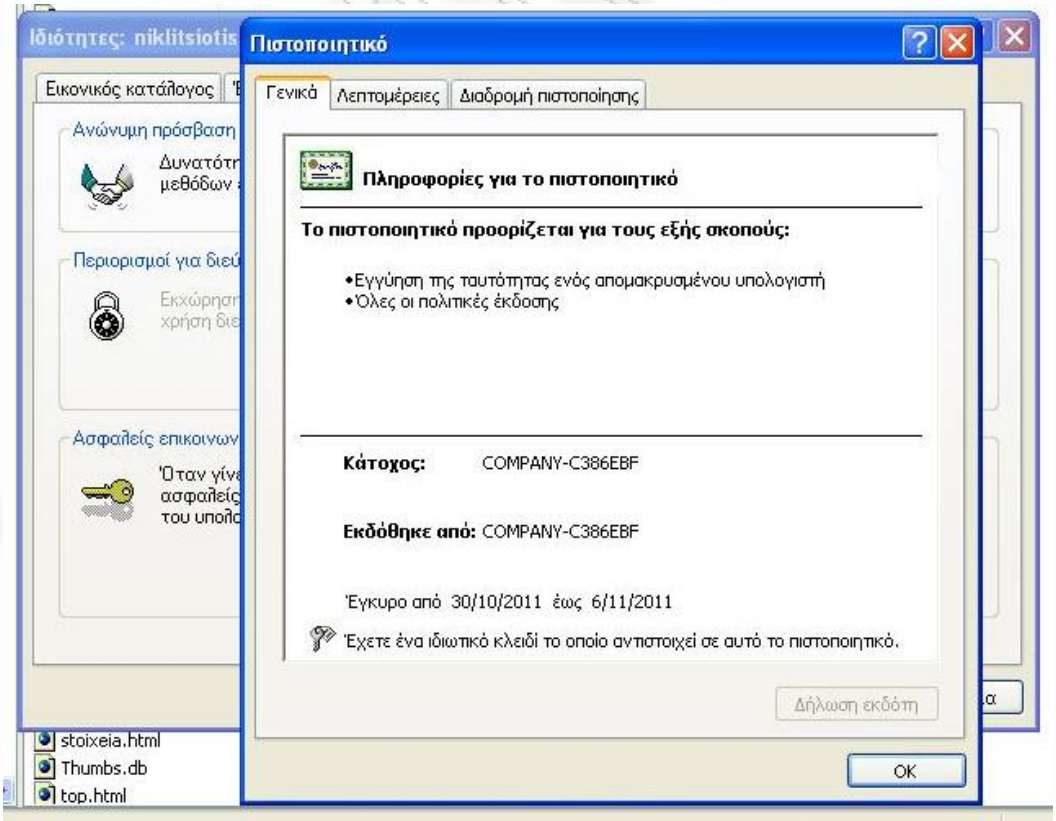
Εικόνα 33. Ηλεκτρονική υπογραφή

Εάν τώρα θέλουμε να διαπιστώσουμε και να δούμε το ηλεκτρονικό πιστοποιητικό που έχουμε δημιουργήσει για την τοποθεσία niklitsiotis, μπορούμε να κάνουμε δεξί κλικ στο πεδίο niklitsiotis και να επιλέξουμε ιδιότητες από το νέο παράθυρο που θα εμφανιστεί επιλέγουμε ασφάλεια καταλόγου και μετά επιλέγουμε Προβολή Πιστοποιητικού. Η ενέργεια αυτό παρουσιάζεται και στην εικόνα 34.



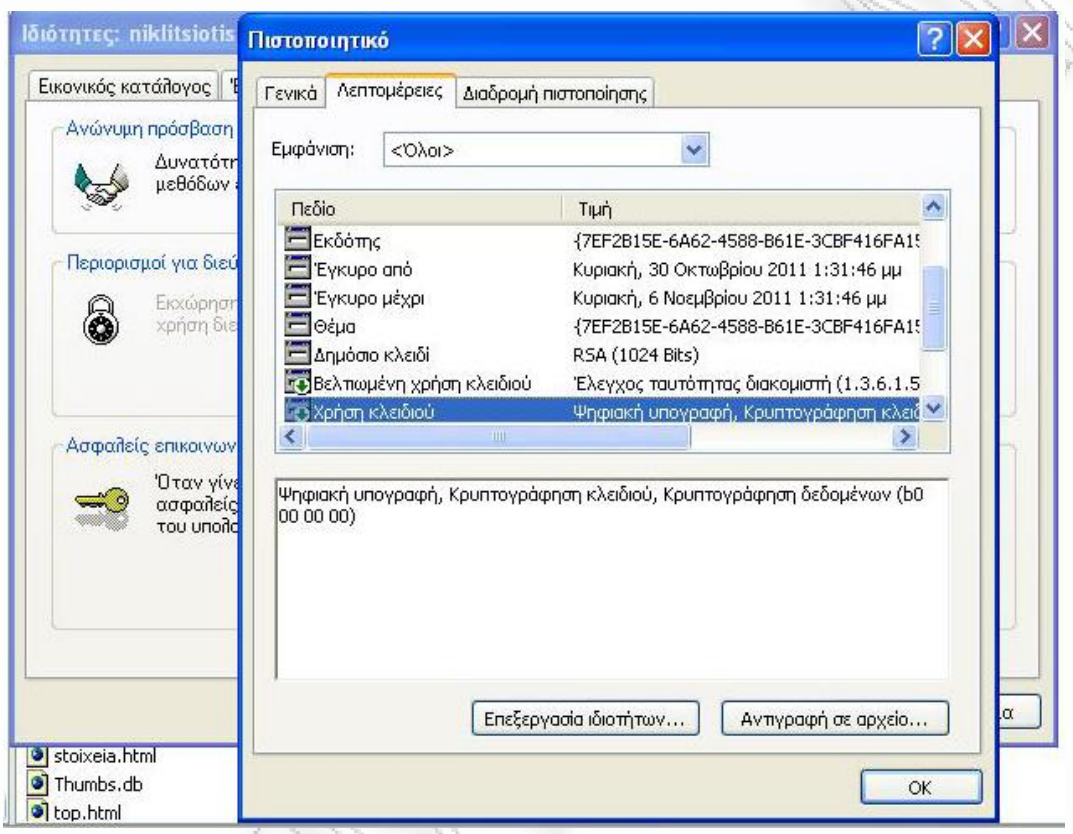
Εικόνα 34. Προβολή ηλεκτρονικού πιστοποιητικού

Στην εικόνα 35, παρουσιάζεται το ηλεκτρονικό πιστοποιητικό. Στην καρτέλα γενικά βλέπουμε την εγκυρότητα του και το ποιος είναι ο κάτοχος του πιστοποιητικού.



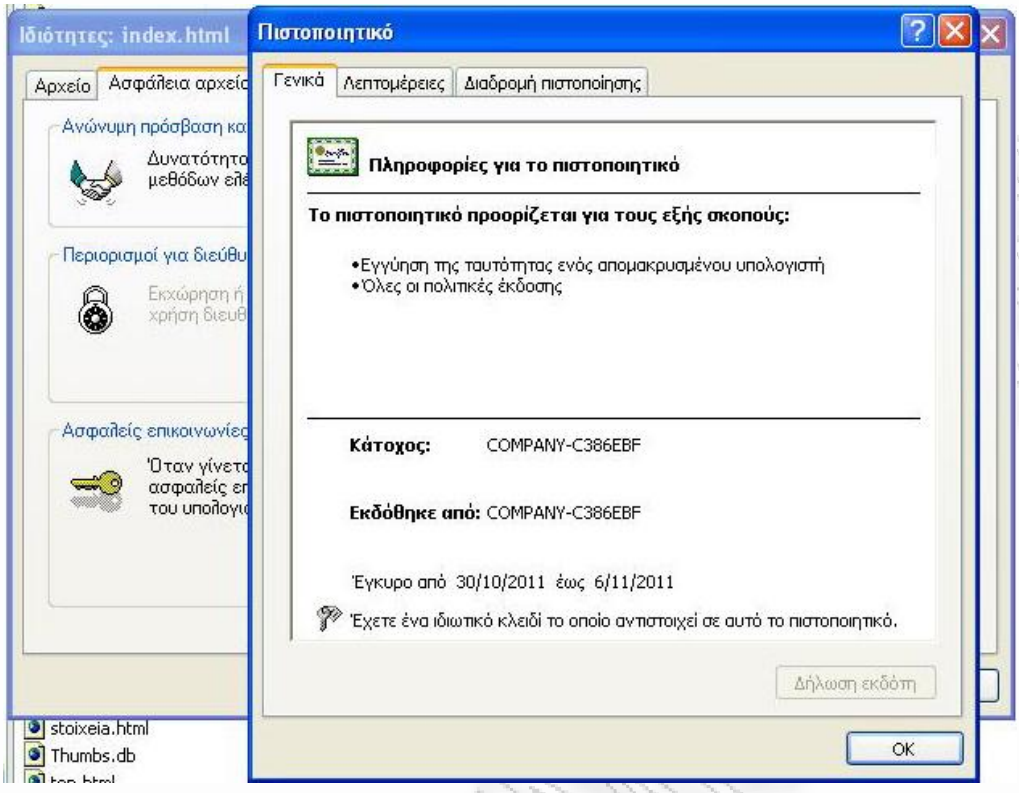
Εικόνα 35. Ηλεκτρονικό Πιστοποιητικό

Στην καρτέλα Λεπτομέρειες παρουσιάζονται όλες οι λεπτομέρειες που αφορούν τα ηλεκτρονικό πιστοποιητικό μας, ο εκδότης, από ποια έως ποιά ημερομηνία είναι έγκυρο, το Δημόσιο κλειδί του πιστοποιητικού καθώς επίσης και η χρήση του κλειδιού. Η καρτέλα των λεπτομερειών του ηλεκτρονικού πιστοποιητικού παρουσιάζονται στην εικόνα 36.



Εικόνα 36. Λεπτομέρειες ηλεκτρονικού πιστοποιητικού

Προκειμένου να διαπιστώσουμε ότι η ηλεκτρονική υπογραφή και το ηλεκτρονικό πιστοποιητικό έχουν εφαρμοστεί σε όλες τις σελίδες της ιστοσελίδας μας, μπορούμε να κάνουμε δεξί κλικ σε μια από τις σελίδες μας και να επιλέξουμε να δούμε τις ιδιότητες της. Στο παράθυρο με τις ιδιότητες της σελίδας μας επιλέγουμε ασφάλεια αρχείου και μας εμφανίζεται ένα νέο παράθυρο στο οποίο προβάλλεται το ηλεκτρονικό πιστοποιητικό. Το αποτέλεσμα αυτής της διαδικασίας παρουσιάζεται στην συνέχεια στην εικόνα 37.



Εικόνα 37. Ηλεκτρονικό πιστοποιητικό σε ιστοσελίδα

ΠΑΡΑΡΤΗΜΑ

ΠΑΡΑΡΤΗΜΑ Α

Κατάλογος Νομοθετικών-Κανονιστικών κειμένων

Α. ΔΙΕΘΝΗ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

- UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES, **«Νόμος-Πρότυπο για τις ηλεκτρονικές υπογραφές**» 5 Ιουλίου 2001
- United Kingdom, Statutory Instrument 2002 No. 318, «**The Electronic Signatures Regulations 2002»**
- USA, **«The Electronic Signatures in Global and National Commerce Act»**

Β. ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ

- **Οδηγία 1999/93/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές
- **Απόφαση 6 Νοεμβρίου 2000** της Επιτροπής Ηλεκτρονικής υπογραφής (άρθρο 9 Οδηγίας 99/93/ΕΕ) για τα ελάχιστα κριτήρια που θα πρέπει να πληρούν οι αρμόδιοι φορείς για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής.
- **Οδηγία 98/34/ΕΚ** για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών καθώς και η τροποποίησή της από την Οδηγία 98/48/ΕΚ)
- **Απόφαση της Επιτροπής της 14ης Ιουλίου 2003** σχετικά με τη δημοσίευση αριθμών αναφοράς γενικά αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής, σύμφωνα με την Οδηγία 1999/93/ΕΚ .

Γ. ΕΘΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

- ***Π.Δ. 150/2001:*** Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- ***Π.Δ.*** **39.2001:** Καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της Κοινωνίας των Πληροφοριών
- **Ν.2672/1998 'Αρθρο 14:** Διακίνηση εγγράφων με ηλεκτρονικά μέσα
- **Π.Δ. 342/2002:** Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.
- **Απόφαση 248/71**: «Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκ. υπογραφής»
- **Απόφαση 295/63**: « Κανονισμός ορισμού φορέων για την διαπίστωση συμμόρφωσης ΑΔΔΥ και ΑΚΜ και προς τα κριτήρια της εθελοντικής διαπίστευσης»
- **Απόφαση 295/64** : «Κανονισμός για τον έλεγχο συμμόρφωσης ΑΔΔΥ και ΑΚΜ»
- **Απόφαση 295/63:** «Κανονισμός για την εθελοντική διαπίστευση των ΠΥΠ»
- **«Κανονισμός Επικοινωνίας Δημόσιων Υπηρεσιών»** (ΚΕΔΥ)
- **Εγκύκλιος *ΔΙΑΔΠ/Α1/2523*** του Υπουργείου Δημόσιας Διοίκησης και Αποκέντρωσης Δ/νση Απλούστευσης Διαδικασιών και Παραγωγικότητας-Διευκρινήσεις στις διατάξεις του άρθρου 14 του Ν. 2672/1998

ΠΑΡΑΡΤΗΜΑ Β

Κατάλογος Ευρωπαϊκών Προτύπων/Τεχνικών προδιαγραφών[186]

A. Electronic Telecommunication Standardization Institute / Electronic Signatures Initiative (ETSI/ESI):

- **ETSI TS 101 862 v.1.2** (Mars 2002) - Qualified Certificate Profile
- **ETSI TS 102 023 v.1.2.1** (January 2003) - Policy requirements for timestamping authorities
- **ETSI TS 102 042** (April 2002) - Policy requirements for certification authorities issuing public key certificates
- **ETSI TS 101 456 v 1.2.1** (April 2002) - Policy requirements for certification authorities issuing qualified certificates
- **ETSI TS 101 733 v 1.4.0** (September 2002) - Electronic Signature Formats
- **ETSI TS 101 861 v 1.2.1** (March 2002) - Time stamping profile
- **ETSI TS 101 903 v. 1.1.1** (February 2002) - XML Advanced Electronic Signatures (XAdES)
- **ETSI SR 002 176** (March 2003) - Algorithms and Parameters for Secure Electronic Signatures
- **ETSI TR 102 045** (March 2003) - Signature policy for extended business model
- **ETSI TR 102 153** (February 2003) - Pre study on Certificate Profiles
- **ETSI TR 102 023** (January 2003) - Policy requirements for time-stamping authorities
- **ETSI TR 102 044** (December 2002) - Identification of requirements for attribute certification
- **ETSI TR 102 038** (April 2002) - XML format for signature policies
- **ETSI TR 102 040** (March 2002) - International Harmonization of Policy Requirements for CAs issuing Certificates
- **ETSI TR 102 041** (February 2002) - Signature Policies Report
- **ETSI TS 102 231** (October 2003) - Harmonized TSP status information
- **ETSI TS 102 280** (March 2004) – X.509 v3 Certificate Profile for Certificates Issued to Natural Persons
- **Frequently Asked Questions** (March 2002)

B. 'European Committee For Standardisation/ Information Society Standardization System (CEN/ISSS):

- **CWA 14365** Guide on the use of Electronic Signatures
- **CWA 14355** Guidelines for the implementation of Secure Signature-Creation Devices
- **CWA 14172-1** EESSI Conformity Assessment Guidance - Part:1: General

[186] Ο κατάλογος είναι ενδεικτικός και περιλαμβάνει μερικές μόνο από τις εκδόσεις προτύπων από τους Ευρωπαϊκούς Οργανισμούς Προτυποποίησης. Για την πλήρη και ενημερωμένη λίστα προτύπων ανατρέξτε στις σχετικές ηλεκτρονικές τοποθεσίες μέσω της εισαγωγικής ιστοσελίδας του EESSI, http://www.ict.etsi.org/EESSI_home.htm (ημερομηνία επίσκεψης 11/06/2011).

- **CWA14172-2** EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes
- **CWA 14172-3** EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
- **CWA 14172-4** EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification
- **CWA 14172-5** EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices
- **CWA 14171** Procedures for Electronic Signature Verification
- **CWA 14170** Security Requirements for Signature Creation Systems
- **CWA 14169** Secure Signature-Creation Devices, version 'EAL 4+'
- **CWA 14167-1** Revised Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- **CWA14167-2** Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

Γ. Κοινές Προδιαγραφές του eEurope Smart Card Charter (OSCIE v. 2):

- **Vol. 3:** Global interoperability Framework for identification, authentification and electronic signature (IAS) with smart cards
- **Vol. 4:** Public Electronic Identity, Electronic Signature and PKI

Βιβλιογραφια

Ελληνική

[1] Αλεξανδρίδου Ελίζα, «Το δίκαιο του ηλεκτρονικού εμπορίου», εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2010.

[2] Ιγγλεζάκης Δ. Ιωάννης, «Πληροφορική και Δημόσιο Δίκαιο, Έμπειρα συστήματα ασαφούς λογικής και η εφαρμογή της στις αόριστες έννοιες», εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2000.

[3] Ιγγλεζάκης Δ. Ιωάννης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2006.

[4] Καραδημητρίου Κοσμάς, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», Εκδοτικός Οίκος: ΣΑΚΚΟΥΛΑΣ ΕΚΔΟΣΕΙΣ Α.Ε., Αθήνα – Θεσσαλονίκη, 2008.

[5] Καράκωστας Κ. Ιωάννης, «Δίκαιο και Internet Νομικά Ζητήματα του Διαδικτύου», Εκδότης Π.Ν. Σάκκουλας, Αθήνα, 2003.

[6] Σιδηρόπουλος Θεόδωρος, «Το δίκαιο του Διαδικτύου», εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2003.

[7] Σιδηρόπουλος Θεόδωρος, « Εισαγωγή στο Δίκαιου του ηλεκτρονικού εμπορίου», εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2000.

[8] Σινανιώτη - Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, «Ηλεκτρονική τραπεζική», Εκδότης: Σάκκουλας Αντ. Ν., Αθήνα, 2005.

[9] Παπακωνσταντίνου Ευάγγελος, «Νομικά θέματα πληροφορικής, Προστασία Δεδομένων προσωπικού χαρακτήρα, έννομη προστασία λογισμικού, ηλεκτρονικό εμπόριο», Εκδόσεις Σάκκουλα, Αθήνα, 2006.

[10] Παπανικολάου Π., «Η έννοια του καταναλωτή σήμερα – Ιδίως στις καταρτιζόμενες με ΓΟΣ πιστωτικές συμβάσεις», ΔΕΕ 2010.

Αγγλική

[1] Reed C., «What is a Signature?», JILT 2000 (3), The Journal of Information, Law and Technology, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.

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

Διαδίκτυο

[1] **http://www.eett.gr/**, δικτυακός τόπος της «Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων» (ΕΕΤΤ). Σε αυτόν τον δικτυακό τόπο υπάρχουν θεματικές ενότητες για τις ηλεκτρονικές υπογραφές, τους Παρόχους Υπηρεσιών Πιστοποίησης και αποφάσεις που αποτελούν το εθνικό ρυθμιστικό πλαίσιο της Ελλάδας.

[2] **http://www.ebusinessforum.gr/**, Δικτυακός τόπος Πανεπιστημίου Κρήτης. Συγκεκριμένα στην ιστοσελίδα της Ομάδας Εργασίας «Ε2», υπάρχουν σχετικές πηγές, κείμενα και μελέτες, για το θέμα της ηλεκτρονικής υπογραφής και τους Παρόχους Υπηρεσιών Πιστοποίησης.

[3] **http://www.esee.gr/UploadFiles/Documents/ProedrikaDiatagmata/PD150-01**, 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.

[4] **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006,** DC0120:EL:NOT, Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο - Έκθεση αναφορικά με τη λειτουργία της οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

[5] **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».

[6] **http://www.ict.etsi.org/EESSI_home.htm**, κεντρική σελίδα του «European Electronic Signature Standardization Initiative» (EESSI) που έχει την ευθύνη του σχεδιασμού και του συντονισμού των ευρωπαϊκών προτύπων στη βάση της Οδηγίας 99/93/ΕΚ. Στην ιστοσελίδα υπάρχουν συγκεντρωμένες πληροφορίες σχετικά με την διαδικασία προτυποποίησης των ηλεκτρονικών υπογραφών, καθώς και συνδέσεις προς τις λίστες με όλα τα πρότυπα που έχουν συνταχθεί και δημοσιεύονται από τους ευρωπαϊκούς οργανισμούς προτυποποίησης «Electronic Telecommunication Standardization Institute» (ETSI) και «European Committee for Standardization/Information Society Standardisation System» (CEN/ISSS).

[7] **http://www.acci.gr/ecomm/legal/index.htm**, Στην ιστοσελίδα υπάρχει το ισχύον εθνικό, κοινοτικό και διεθνές δίκαιο, καθώς και η υπάρχουσα σχετική νομολογία για τις ηλεκτρονικές υπογραφές. Υπάρχει σχετική θεματική ενότητα για τις ηλεκτρονικές υπογραφές στην «Τράπεζα Νομικών Πληροφοριών Ηλεκτρονικού Εμπόριο»', την οποία συντηρεί και δημοσιεύει δωρεάν το «Εμπορικό & Βιομηχανικό Επιμελητήριο Αθηνών» (ΕΒΕΑ).

[8] **http://www.go-online.gr/**, επίσημος κόμβος της «Εκπαιδευτικής Στήριξης του Δικτυωθείτε».

[9] **http://en.wikipedia.org/wiki/Digital_signature**, Wikipedia, The Free Encyclopedia, Digital Signature.