Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**«ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ»**
Ονοματεπώνυμο Φοιτήτριας	**ΦΩΤΕΙΝΗ ΓΡΥΛΛΑΚΗ**
Πατρώνυμο	**ΕΜΜΑΝΟΥΗΛ**
Αριθμός Μητρώου	**ΜΠΠΛ/ 07026**
Επιβλέπουσα	**ΑΡΙΣΤΕΑ ΣΙΝΑΝΙΩΤΗ, ΚΑΘΗΓΗΤΡΙΑ**

ΑΠΡΙΛΙΟΣ 2011

Τριμελής Εξεταστική Επιτροπή

Σινανιώτη Αριστέα Καθηγήτρια	Ασημακόπουλος Νικήτας Καθηγητής	Δουληγέρης Χρήστος Καθηγητής

Ευχαριστίες

Έχοντας φτάσει πλέον στην ολοκλήρωση της μεταπτυχιακής μου διατριβής, αισθάνομαι υποχρεωμένη να εκφράσω τις ευχαριστίες μου σε εκείνους τους ανθρώπους που μου πρόσφεραν τη βοήθειά τους καθ' όλη τη διάρκεια διεκπεραίωσης της παρούσας εργασίας.

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου κ^{α} Αριστέα Σινανιώτη, που μου έδωσε την ευκαιρία να ασχοληθώ με ένα θέμα ιδιαιτέρου ενδιαφέροντος, όπως επίσης και για τη μέριμνα και την καθοδήγησή της.

Επίσης θα ήθελα να ευχαριστήσω τον καθηγητή κ^{ο} Χρήστο Δουληγέρη για τη βοήθεια και τις συμβουλές του για την υλοποίηση του πρακτικού μέρους της εργασίας μου και τον καθηγητή κ^{ο} Νικήτα Ασημακόπουλο για τα εποικοδομητικά και χρήσιμα σχόλιά του και οι δύο μέλη της τριμελούς εξεταστικής επιτροπής μου.

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον κ^{ο} Αντώνη Στασή, προϊστάμενος του Υπουργείου Εσωτερικών, Αποκέντρωσης & Ηλεκτρονικής Διακυβέρνησης, για την άμεση ανταπόκρισή του για την έκδοση των ψηφιακών μου πιστοποιητικών και στον κ^{ο} Γιώργο Κατσικογιάννη, υποψήφιο διδάκτορα και στέλεχος του Υπουργείου Εσωτερικών, Αποκέντρωσης & Ηλεκτρονικής Διακυβέρνησης, για τη βοήθεια, το ενδιαφέρον και το χρόνο που μου διέθεσε για την υλοποίηση του πρακτικού μέρους της εργασίας μου.

Ευχαριστίες θα ήθελα επίσης να απευθύνω στην κ^{α} Ματθούλα Τριανταφύλλου, και στον κ^{ο} Μανόλη Γιαμπουρά, προϊστάμενοι του Υπουργείου Οικονομίας, Ανταγωνιστικότητας και Ναυτιλίας για τις χρήσιμες υποδείξεις τους σχετικά με τη μεταπτυχιακή μου διατριβή καθώς και στους φίλους μου Κωνσταντίνο Μακαρούνη, Σωτήρη Αθανασίου, Καλή Νικολάου και Ευαγγελία Τερζάκου.

Τέλος ένα μεγάλο ευχαριστώ στους γονείς μου που χωρίς την ηθική και οικονομική στήριξή τους δε θα είχα τη δυνατότητα να πραγματοποιήσω τις μεταπτυχιακές μου σπουδές.

Περίληψη

Η εξάπλωση του διαδικτύου, το ηλεκτρονικό εμπόριο, οι ηλεκτρονικές συναλλαγές και η μετάδοση εμπιστευτικών δεδομένων μέσω ανοιχτών δικτύων αποτελούν όψεις της σύγχρονης κοινωνίας της πληροφορίας. Το διαδίκτυο δημιουργεί νέες ευκαιρίες και δυνατότητες κρίσιμης σημασίας για την ανάπτυξη της ανταγωνιστικότητας των οικονομιών.

Η ανάπτυξη των ηλεκτρονικών συναλλαγών επιβάλλει την ύπαρξη μηχανισμών προστασίας του απαραβίαστου του προσωπικού απορρήτου των συναλλασσόμενων χρηστών. Επιβάλλει μηχανισμούς ασφάλειας στις συναλλαγές και στις ανταλλαγές δεδομένων, ασφάλειας η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, δηλαδή την ταυτότητα των συναλλασσόμενων.

Από το 1996 έχει ξεκινήσει η δημιουργία ενός διεθνούς νομικού πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών. Το 1999 η Οδηγία 1999/93/ΕΚ σχετικά με ένα κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, έθεσε τις βάσεις του ρυθμιστικού πλαισίου των ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Ένωση. Στη συνέχεια το Προεδρικό Διάταγμα 150/2001, προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, θέτει το κανονιστικό πλαίσιο και εναρμονίζει το ελληνικό με το ευρωπαϊκό δίκαιο στο ζήτημα των ηλεκτρονικών υπογραφών.

Ο σκοπός αυτής της εργασίας είναι να παρουσιάσει την έννοια της ηλεκτρονικής (ψηφιακής) υπογραφής, το μηχανισμό εφαρμογής της, τα σχετικά με αυτή ψηφιακά πιστοποιητικά καθώς επίσης και το σχετικό θεσμικό πλαίσιο που διέπει αυτήν. Τέλος, θα παρουσιαστεί μια μελέτη περίπτωσης αναφορικά με την έκδοση ψηφιακών πιστοποιητικών και τη χρήση αυτών.

Λέξεις κλειδιά

Κρυπτογραφία, ηλεκτρονικές υπογραφές, ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά (πιστοποιητικά δημοσίου κλειδιού), Πάροχος Υπηρεσιών Πιστοποίησης, Οδηγία 1999/93/ΕΚ, π.δ.150/2001, Απόφαση 248/71/2002, π.δ. 342/2002.

Abstract

The internet expansion, the electronic commerce, the electronic transactions and the transmission of confidential data via open networks are aspects of the current information society. Internet creates new opportunities and possibilities critical for the improvement of the competitiveness of the economy.

The development of electronic transactions requires protection mechanisms of the inviolable personal secrecy of dealing users. Mechanisms of safety in the transactions and in the exchanges of data are necessary to be put in place. The safety in the transactions depends to a great extent from the signature, that is to say the identity dealing users.

Since 1996, the creation of international legal frame for the use of electronic signatures has been started. In 1999 the Directive 1999/93/EK with regard to a Community frame for the electronic signatures, placed the bases of regulating frame of electronic signatures in the European Union. Afterwards Presidential Decree 150/2001, adaptation in the Directive of 99/93/[EK] European Parliament and Council with regard to the Community frame for electronic signatures, places the lawful frame and harmonises Greek with the European right in the question of electronic signatures.

The aim of this dissertation is to present the significance of the electronic (digital) signature, the mechanism of its application, the relative digital certificates as well as the relative institutional frame. Finally, a case study is presented concerning the publication and the use of digital certificates.

Πίνακας περιεχομένων

Σελ.

Κεφάλαιο 4

Κεφάλαιο 5

Κεφάλαιο 6

Κεφάλαιο 7

Κατάλογος σχημάτων

Σελ.

Κατάλογος πινάκων

Σελ.

Κατάλογος εικόνων

Σελ.

Μέρος Α΄

Κεφάλαιο 1

1.1 Εισαγωγή

Η μετάδοση πληροφοριών χωρίς να γίνεται αντιληπτή από κάποιον ανεπιθύμητο, η εξασφάλιση της δυνατότητας να μην μπορεί να ερμηνευθεί το μήνυμα στην περίπτωση που η μετάδοση γίνει αντιληπτή από κάποιον ξένο, καθώς και η απόδειξη της κυριότητος ενός μηνύματος απασχόλησαν και εξακολουθούν να απασχολούν τον άνθρωπο. Φυσικά, τα προβλήματα αυτά θα εξακολουθούν να υπάρχουν όσο θα υπάρχουν άνθρωποι που θα προσπαθούν να προστατέψουν τα δικαιώματά τους και κάποιοι που θα προσπαθούν να τα παραβιάσουν.

Στη σημερινή εποχή, η διαμάχη αυτή διεξάγεται στο χώρο των ψηφιακών δεδομένων. Σύγχρονες υπολογιστικές μηχανές, με υψηλές δυνατότητες επεξεργασίας πληροφοριών, χρησιμοποιούνται τόσο για να εξασφαλίζουν τη νομιμότητα όσο και για να την παρακάμπτουν. Η ανάγκη για σταδιακή αντικατάσταση των παραδοσιακών μέσων για την καταγραφή και απόδειξη μιας συμβατικής συναλλαγής όπως είναι τα ενυπόγραφα ιδιωτικά έγγραφα με αντίστοιχα ηλεκτρονικά δεδομένα που θα δημιουργούνται, θα επεξεργάζονται, θα επαληθεύονται και θα αρχειοθετούνται με ηλεκτρονικά μέσα, χωρίς δηλαδή την ανάγκη ενσωμάτωσής τους σε υλικό φορέα όπως το χαρτί, έχει οδηγήσει στην ανάπτυξη συγκεκριμένων τεχνολογιών και μεθόδων. Σχετικές νομοθετικές ρυθμίσεις προσφέρουν στις ηλεκτρονικές συναλλαγές το κύρος, την ασφάλεια και την εμπιστοσύνη που διαθέτουν οι συμβατικές μέθοδοι.

Λόγοι οι οποίοι καθιστούν την ασφάλεια στην ηλεκτρονική επικοινωνία επιτακτική είναι η ευκολία που παρέχεται μέσω ενός ανοικτού δικτύου, όπως είναι το Internet, στην παρακολούθηση της επικοινωνίας από τρίτους, στην αλλοίωση του περιεχομένου του μεταφερομένου μηνύματος και στην αδυναμία να εξακριβωθεί η ταυτότητα των συναλλασσόμενων.

Προκειμένου να αντιμετωπιστούν τα διάφορα προβλήματα που προκαλεί η έλλειψη ειδικής νομοθετικής ρύθμισης στα διάφορα κράτη-μέλη της ΕΕ αλλά και για τη βελτίωση των διαφόρων συναλλαγών μέσω των ηλεκτρονικών μέσων και την ανταπόκριση τους στις σύγχρονες απαιτήσεις, η ΕΕ εξέδωσε την Οδηγία 1999/93/ΕΚ η οποία αναφέρεται στις ηλεκτρονικές υπογραφές. Η οδηγία αυτή ενσωματώθηκε στο ελληνικό δίκαιο με το προεδρικό διάταγμα 150/2001.

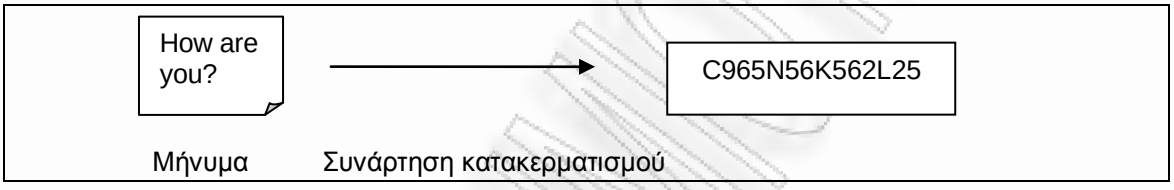
Στην παρούσα εργασία γίνεται περιγραφή της λειτουργίας της ψηφιακής υπογραφής και παρουσιάζεται το νομοθετικό πλαίσιο που ισχύει γι' αυτήν. Αρχικά στο πρώτο κεφάλαιο παρουσιάζεται η βασική ορολογία της εργασίας αυτής. Στο δεύτερο κεφάλαιο γίνεται μια σύντομη ιστορική αναδρομή της κρυπτογραφίας, αναπτύσσεται η έννοια και η λειτουργία της και αναλύονται τα είδη αυτής. Σύντομη επισκόπηση της ηλεκτρονικής υπογραφής από τεχνική και νομική σκοπιά γίνεται στο τρίτο κεφάλαιο. Στο τέταρτο κεφάλαιο αναλύεται η έννοια της ψηφιακής υπογραφής, περιγράφεται η δημιουργία και η λειτουργία αυτής και γίνεται σύγκριση με την παραδοσιακή ιδιόχειρη υπογραφή. Ακολουθεί το πέμπτο κεφάλαιο στο οποίο εξετάζεται ο ρόλος των παρόχων υπηρεσιών πιστοποίησης και τα εκδιδόμενα από αυτούς ψηφιακά πιστοποιητικά. Το θεσμικό πλαίσιο που διέπει την ηλεκτρονική υπογραφή και περιλαμβάνει την Οδηγία 1999/93/ΕΚ, το π.δ. 150/2001, την Απόφαση 248/71/2002 και το π.δ. 342/2002 αναλύονται στο έκτο κεφάλαιο. Το επόμενο έβδομο κεφάλαιο είναι αφιερωμένο στη χρήση των ηλεκτρονικών υπογραφών σε ευρωπαϊκό επίπεδο και ειδικότερα στην Ελλάδα. Τέλος στο όγδοο κεφάλαιο περιγράφουμε πρακτικά όλη τη διαδικασία έκδοσης ψηφιακών πιστοποιητικών από την εθνική πύλη δημόσιας διοίκησης ermis του Υπουργείου Εσωτερικών και τη χρήση αυτών. Ακολουθούν τα συμπεράσματα στο ένατο κεφάλαιο στα οποία συνοψίζονται οι τελικές παρατηρήσεις.

1.2 Βασική ορολογία

Με τον όρο **ηλεκτρονικό αντικείμενο** νοείται ένα έγγραφο, ένα πρόγραμμα ή οποιοδήποτε άλλο αντικείμενο ηλεκτρονικής μορφής. Η έννοια του ηλεκτρονικού αντικειμένου περιλαμβάνει την δυνατότητά του να αποθηκευτεί σε έναν υπολογιστή και να μεταφερθεί από έναν υπολογιστή σε έναν άλλο.[10]

Σύμφωνα με την απόφαση υπ' αρ. 1327/2001 του Μονομελούς Πρωτοδικείου Αθηνών, **ηλεκτρονικό έγγραφο** είναι το σύνολο των έγγραφων δεδομένων στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή. Τα δεδομένα αυτά λογίζονται ως έγγραφα με βάση το Νόμο όταν αφού γίνουν αντικείμενο επεξεργασίας από την κεντρική μονάδα επεξεργασίας, αποτυπώνονται με βάση τις εντολές του software κατά τρόπο που να μπορεί να τα διαβάσει ο άνθρωπος. Εναλλακτικά χρησιμοποιούνται οι όροι αρχείο ή συλλογή από bytes. Σε περίπτωση αντιγραφής ενός ηλεκτρονικού αντικειμένου, το αντίγραφο που προκύπτει αποτελείται από ταυτόσημη ακολουθία bits και η ηλεκτρονική υπογραφή που θα παραχθεί από το κάθε αντίγραφο θα είναι ίδια με αυτήν του πρωτοτύπου.[10]

Η **συνάρτηση κατακερματισμού** (ή συνάρτηση κατατεμαχισμού) είναι μια μαθηματική συνάρτηση που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων δίνει έξοδο μια καθορισμένου μεγέθους στοιχειοσειρά (string), συνήθως έναν ακέραιο αριθμό, πολύ μικρότερη από την είσοδο, σχήμα 1.1. [11]



Σχήμα 1.1: Συνάρτηση κατακερματισμού

Η συνάρτηση κατακερματισμού είναι ένας αλγόριθμος ο οποίος υπολογίζει μία τιμή βασισμένη σε ένα ηλεκτρονικό αντικείμενο (όπως ένα μήνυμα ή ένα αρχείο, συνήθως πολύ μεγάλο), χαρτογραφώντας το ηλεκτρονικό αντικείμενο σε ένα μικρότερο ηλεκτρονικό αντικείμενο [3]. Το ηλεκτρονικό αντικείμενο που εξάγεται από τον αλγόριθμο κατακερματισμού ονομάζεται σύνοψη του αρχικού μηνύματος. Οποιαδήποτε αλλαγή του ηλεκτρονικού αντικειμένου που εισάγεται στον αλγόριθμο οδηγεί σε διαφορετική σύνοψη. Η σύνοψη του μηνύματος δεν μπορεί να πλαστογραφηθεί, υπό την έννοια ότι δεδομένου κάποιου συγκεκριμένου μηνύματος εισόδου είναι υπολογιστικά αδύνατο να παραχθεί από την αρχή ένα άλλο μήνυμα που να έχει την ίδια ακριβώς σύνοψη με το πρώτο. Υπάρχει όμως μια μικρή πιθανότητα σε περίπτωση που η σύνοψη είναι πολύ μικρή κάποιος δοκιμάζοντας διαδοχικές ασήμαντες αλλαγές, όπως τα διαστήματα μεταξύ των λέξεων ή η αντικατάσταση μιας λέξης ή φράσης, να πετύχει την εξαγωγή της επιθυμητής σύνοψης. Επομένως μεγάλη σημασία έχει το μήκος της σύνοψης.

Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.[12]

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση** (decryption).[12]

Κρυπτογραφικός αλγόριθμος (cipher) είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος.[12]

Αρχικό κείμενο ή απλό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.[12]

Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο ή κρυπτογράφημα (ciphertext) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.[12]

Κρυπτανάλυση (cryptanalysis) είναι η επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής, χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης. Δηλαδή χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.[12]

Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union- ITU) είναι η ειδικευμένη οργάνωση του ΟΗΕ μέσα στην οποία οι κυβερνήσεις και ο ιδιωτικός τομέας συντονίζουν την ίδρυση και λειτουργία δικτύων και υπηρεσιών τηλεπικοινωνιών. Η ITU είναι υπεύθυνη για τη ρύθμιση, την τυποποίηση, το συντονισμό και την ανάπτυξη των διεθνών τηλεπικοινωνιών καθώς και για την εναρμόνιση των εθνικών πολιτικών.[17]

Ηλεκτρονική υπογραφή είναι μια ηλεκτρονική σύντμηση που προκύπτει από το ηλεκτρονικό έγγραφο το οποίο συνοδεύει και από απόρρητα δηλωτικά στοιχεία του υπογράφοντα.

Ψηφιακή υπογραφή είναι η κρυπτογραφημένη σύνοψη του ηλεκτρονικού κειμένου με τη μέθοδο της ασύμμετρης κρυπτογράφησης, μια μέθοδος τεκμηρίωσης της γνησιότητας των ηλεκτρονικών δεδομένων.

Ψηφιακό πιστοποιητικό είναι μια βεβαίωση σε ηλεκτρονική μορφή που περιλαμβάνει το δημόσιο κλειδί του υπογράφοντα, το οποίο χρησιμοποιείται για την επαλήθευση της υπογραφής του και στοιχεία που επιβεβαιώνουν την ταυτότητά του.

Πάροχος Υπηρεσιών Πιστοποίησης ή Αρχή Πιστοποίησης είναι ένας ουδέτερος οργανισμός που αρμοδιότητά του είναι η έκδοση ψηφιακού πιστοποιητικού και η παρακολούθηση του για όλο τον κύκλο της ζωής του.

Κεφάλαιο 2

2.1 Κρυπτογραφία

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, (που μελετάει την τέχνη του μυστικού γραψίματος δηλαδή το να διατηρείς την πληροφορία μυστική), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της κρυπτογραφίας είναι να παρέχει μηχανισμούς για δύο ή περισσότερα άτομα ώστε να μπορούν να επικοινωνούν μεταξύ τους χωρίς κάποιος ξένος να μπορεί να αλλάξει ή να διαβάσει την πληροφορία αυτή.

2.1.1 Ιστορική αναδρομή της κρυπτογραφίας

Η εξέλιξη της κρυπτογραφίας, ιστορικά χωρίζεται σε τρεις περιόδους:

- Η πρώτη περίοδος ξεκινά περίπου το 1900 π.Χ. μέχρι τις αρχές του 20^{ου} αιώνα.
- Η δεύτερη περίοδος ξεκινά στις αρχές του 20^{ου} αιώνα και φτάνει μέχρι το 1950 μ.Χ., ενώ
- Η τρίτη περίοδος ξεκινά το 1950 μ.Χ., και συνεχίζεται μέχρι τις μέρες μας.

Θα παρατηρήσουμε ότι το κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης είναι ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή. Αντίθετα, στις νεότερες μορφές η κρυπτογραφία έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών και υπολογιστική πολυπλοκότητα.[2]

2.1.1.1 Πρώτη περίοδος κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές οι μέθοδοι δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευρηματικότητα των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (σύμφωνα με τον αμερικάνο ιστορικό της κρυπτογραφίας David Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας η οποία περιλαμβάνει τους αριθμούς από το 1 έως και το 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5^{ο} π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Η «Σπαρτιατική Σκυτάλη» (Εικόνες 2.1), ήταν μια ξύλινη ράβδος συγκεκριμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, και έτσι όταν ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατανόητο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης. Ο παραλήπτης χρησιμοποιούσε μια ράβδο από την ίδια διάμετρο κατά την οποία αναδίπλωνε το χαρτί για να διαβάσει το μήνυμα.

Εικόνες 2.1 :Σπαρτιατική Σκυτάλη

Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δε θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 5, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Παράδειγμα έχοντας ως κλειδί το 3, ο πίνακας 2.1 αντιστοίχισης των γραμμάτων είναι ο εξής:

Το γράμμα	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Θα αντικατασταθεί από το γράμμα	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Πίνακας 2.1: Αντιστοίχιση γραμμάτων

Έτσι για παράδειγμα, η λέξη HELP, θα γίνει το κρυπτογράφημα KHOS. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, δηλαδή να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να γνωρίζει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να ξέρει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Δηλαδή πρέπει να γνωρίζει το κλειδί, που στο συγκεκριμένο παράδειγμα είναι ο αριθμός 3.

Σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Ο Wheatstone, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές.

Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό

ερμηνείας τους, με τίτλο «Oedipus Aegyptiacus». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρη εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια στα ιερογλυφικά, μια στα ελληνικά και μια στην ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους.

Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ..Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής:

3000 -1600 π.Χ.: Εικονογραφική (Ιερογλυφική) γραφή

1850 -1450 π.Χ.: Γραμμική γραφή Α

1450 -1200 π.Χ.: Γραμμική Γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού (Εικόνα 2.2), που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή. Ο δίσκος είναι φτιαγμένος από πηλό. Η μέση διάμετρός του είναι 16 εκατοστά και το μέσο πάχος του 2.1 εκατοστά. Στις δύο όψεις του βρίσκονται 45 διαφορετικά σύμβολα, πολλά από τα οποία αναπαριστούν εύκολα αναγνωρίσιμα αντικείμενα, όπως ανθρώπινες μορφές, ψάρια, πουλιά, έντομα, φυτά κ.α. Συνολικά υπάρχουν 241 σύμβολα, 122 στην 1η πλευρά και 119 στη 2η, τοποθετημένα σπειροειδώς. Τα σύμβολα είναι χωρισμένα σε ομάδες με τη χρήση μικρών γραμμών που κατευθύνονται προς το κέντρο του δίσκου.

Ο δίσκος έχει κεντρίσει τη φαντασία πολλών αρχαιολόγων, επαγγελματιών και μη, και έχουν γίνει αρκετές προσπάθειες αποκρυπτογράφησής του. Έχουν προταθεί πάρα πολλές ερμηνείες του κειμένου του, όπως ότι πρόκειται για προσευχή, για τη διήγηση μίας ιστορίας, για ένα γεωμετρικό θεώρημα, για ημερολόγιο κ.α. Παρόλα αυτά η επιστημονική κοινότητα δεν έχει αποδεχθεί καμία από τις προτεινόμενες αποκρυπτογραφήσεις και ο δίσκος παραμένει ένα άλυτο μυστήριο.

Εικόνα 2.2 : Ο Δίσκος της Φαιστού

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς , ένας μεγάλος Άγγλος αρχαιολόγος, που ανάσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και στη Φαιστό της Κρήτης, αλλά ορισμένα πρόσφατα ευρήματα δείχνουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού όπως στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Έβανς έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα.

Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες.

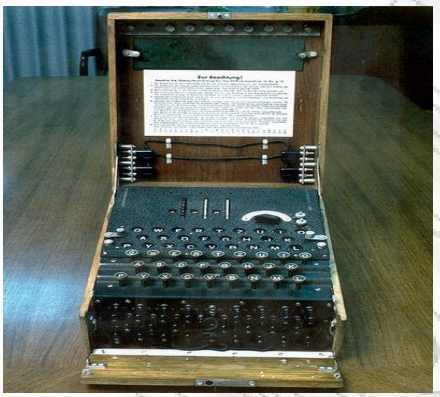
Συστηματικά με την γραφή αυτή ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».[2]

2.1.1.2 Δεύτερη περίοδος κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950μ.Χ. Επομένως, καλύπτει τους δύο παγκόσμιους πολέμους, όπου λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3.000 χρόνια.

Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται κρυπτομηχανές. Η κρυπτανάλυση τους απαιτούσε μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που είχαν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου, η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.

Η πιο γνωστή κρυπτογραφική μηχανή εκείνης της περιόδου είναι το Enigma (Εικόνα 2.3). Η φήμη της πηγάζει κυρίως από τον ρόλο που διαδραμάτισε η αποκρυπτογράφησή της στην τελική έκβαση του δευτέρου παγκοσμίου πολέμου. Το σύστημα αυτό χρησιμοποιήθηκε εκτεταμένα από τους Γερμανούς, σε διάφορες παραλλαγές του.



Εικόνα 2.3 : Η μηχανή Αίνιγμα

Το όνομα Enigma οι δημιουργοί της το δανείστηκαν από την ελληνική λέξη αίνιγμα και με αυτό ήθελαν να δώσουν έμφαση στην περίπλοκη δομή της, καθώς και στην απόλυτη ασφάλεια των μηνυμάτων που αυτή κρυπτογραφούσε.

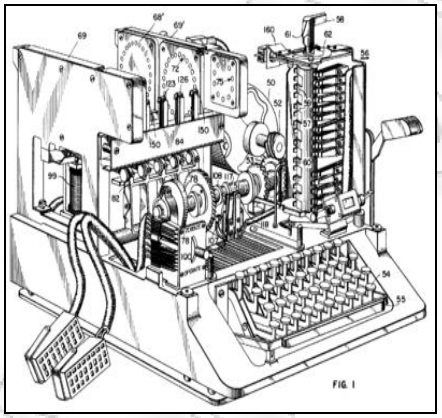
Το 1932, ο Marian Rejewski στην Πολωνία, ήταν αυτός που τελικά παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά. Ήταν η μεγαλύτερη ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και στους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του, όπως ο Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας αποκρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια ενός υπολογιστή που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάστηκε Colossus και δυστυχώς καταστράφηκε με το τέλος του Πολέμου. Μετά από το 1940, οι κρυπτογράφοι του αμερικανικού ναυτικού σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, το Purple και χρησιμοποίησε παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αναφέρθηκε ως "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη ως «Red». Μια ομάδα του αμερικανικού στρατού, η SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης, το "Purple" πριν καν ακόμα

αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης και ειδικότερα της μηχανής Purple, αποκαλώντας το ως ‘‘Μαγεία’’.

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό Sigaba (Εικόνα 2.4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια με το πνεύμα του Enigma, με σημαντικές όμως βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα δηλαδή ένα ποίημα του Πολ Βερλέν, για το οποίο χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελλε την απόβαση. Όμως η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.[2]



Εικόνα 2.4: Κρυπτό-μηχανή SIGABA

2.1.1.3 Τρίτη περίοδος κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το 1949 δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (Communication Theory of Secrecy Systems) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (Mathematical Theory of Communication), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Το 1977, μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο

υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακό τυποποιημένο πρότυπο επεξεργασίας πληροφοριών.

Ο αλγόριθμος DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή Triple-DES χρησιμοποιούνται ακόμα και σήμερα ενσωματωμένοι σε πολλά εθνικά και οργανωτικά πρότυπα. Παρόλα αυτά, το βασικό μέγεθος των 56 bits έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις. Π.χ. μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες. Κατά συνέπεια, όλα τα μηνύματα που έχουν αποσταλεί με τη χρήση απλής κρυπτογράφησης με τον DES, διατρέχουν σοβαρό κίνδυνο αποκρυπτογράφησης.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια της κρυπτογραφίας δημοσίου κλειδιού και παρείχε μια νέα και έξυπνη μέθοδο για ανταλλαγή κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του ‘80 το RSA παρέμεινε ακόμα ασφαλές. Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.[2]

2.2 Η έννοια της κρυπτογραφίας και της κρυπτογράφησης

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Η κρυπτογράφηση αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet καθώς η μετάδοση εμπιστευτικών δεδομένων μέσω του διαδικτύου έχει γίνει κοινός τόπος σήμερα και θα πρέπει να βρεθούν μηχανισμοί προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των χρηστών του Internet. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν τη χρήση κάποιας μυστικής πληροφορίας που το ονομάζουμε κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται είναι διαφορετικά.

Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από τη διασφάλιση του απόρρητου (privacy), η πιστοποίηση ταυτότητας (authentication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά, για παράδειγμα όταν υπογράφουμε ένα έγγραφο και δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που οι αποφάσεις και οι συναλλαγές γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουροι για το ποιος το έχει γράψει.

Η Κρυπτογράφηση είναι μια επιστήμη που στηρίζεται στα μαθηματικά για την κωδικοποίηση (encoding) και αποκωδικοποίηση (decoding) των δεδομένων που διακινούνται μέσω του Διαδικτύου. Με τη σωστή χρήση των μεθόδων κρυπτογράφησης, τα ευαίσθητα προσωπικά δεδομένα των χρηστών είναι προσβάσιμα μόνο απ' όσους διαθέτουν την κατάλληλη εξουσιοδότηση. Με τις τεχνολογίες της κρυπτογράφησης μπορούμε να εξασφαλίσουμε ότι ένα μήνυμα θα μπορεί να διαβαστεί μόνο από τον παραλήπτη του μηνύματος αφού στα ενδιάμεσα στάδια απ' όπου περνάει το μήνυμα εμφανίζεται με ακατανόητους χαρακτήρες και είναι μη αναγνωρίσιμο.

Τα βασικά προβλήματα που έχουν σχέση με το απόρρητο των πληροφοριών που διακινούνται στο Internet είναι τα εξής :

- Η εξασφάλιση ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι, που είναι γνωστό με τον όρο πιστοποίηση (authentication).
- Η εξασφάλιση ότι το μήνυμα ή το κείμενο που λάβαμε είναι το σωστό και ότι δεν έχει τροποποιηθεί από κάποιον τρίτο κατά την πορεία του από τον αποστολέα ως τον παραλήπτη, που είναι γνωστό με τον όρο ακεραιότητα (integrity).
- Η εξασφάλιση ότι μόνο εμείς μπορούμε να διαβάσουμε ένα μήνυμα που απευθύνεται μόνο σ' εμάς, που είναι γνωστό με τον όρο εμπιστευτικότητα (confidentiality).
- Η εξασφάλιση ότι τα μέρη που εμπλέκονται σε μια ηλεκτρονική επικοινωνία δε θα μπορούν να αρνηθούν εκ των υστέρων τη συμμετοχή τους σ' αυτήν, που είναι γνωστό με τον όρο μη αποποίηση ευθύνης (non-repudiation).

Το αρχικό μήνυμα αποκαλείται απλό κείμενο (plaintext), ενώ το ακατανόητο μήνυμα που προκύπτει από την κρυπτογράφηση (μετατροπή) του απλού κειμένου αποκαλείται κρυπτογράφημα (ciphertext). Κρυπτογράφηση (encryption) αποκαλείται η μετατροπή ενός απλού και κατανοητού κειμένου (plaintext) σε μια μη κατανοητή μορφή (κρυπτογράφημα, ciphertext) με την εφαρμογή ενός κατάλληλου αλγορίθμου, ενώ αποκρυπτογράφηση (decryption) αποκαλείται η ανάκτηση του αρχικού απλού κειμένου από το κρυπτογράφημα αφού εφαρμοσθεί ο αντίστροφος αλγόριθμος. Οι αλγόριθμοι κρυπτογράφησης λειτουργούν σε συνδυασμό μ' ένα κλειδί ή κλείδα (key), για να μπορέσει να γίνει η κρυπτογράφηση του απλού κειμένου. Αν για το ίδιο απλό κείμενο χρησιμοποιήσουμε διαφορετικά κλειδιά, θα δημιουργηθούν και διαφορετικά κρυπτογραφήματα.[2]

2.3 Λειτουργίες της κρυπτογραφίας

Η κρυπτογραφία ορίζεται στο Handbook of Applied Cryptography (εγχειρίδιο εφαρμοσμένης κρυπτογραφίας) ως η μελέτη των μαθηματικών τεχνικών που σχετίζονται με τομείς της ασφάλειας πληροφοριών όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η ταυτοποίηση αυθεντικότητας οντότητας και η ταυτοποίηση αυθεντικότητας της πηγής των δεδομένων.

Οι τέσσερις βασικές λειτουργίες της Κρυπτογραφίας είναι:

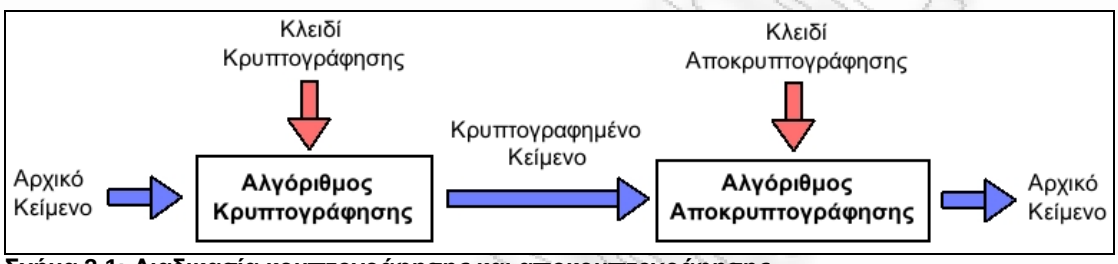
- Η εμπιστευτικότητα (Confidentiality) αφορά την απόκρυψη του περιεχομένου μιας μεταβίβασης από οποιονδήποτε, πλην των εξουσιοδοτημένων, να έχουν πρόσβαση σε αυτήν. Δηλαδή η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη, ενώ είναι ακατανόητη σε κάποιον τρίτο. Υπάρχουν πολλές προσεγγίσεις για την επίτευξη της εμπιστευτικότητας που κυμαίνονται από φυσική προστασία μέχρι μαθηματικούς αλγορίθμους που καθιστούν τα δεδομένα μη αναγνώσιμα.
- Η ακεραιότητα (Integrity) των δεδομένων αφορά την προστασία από μη εξουσιοδοτημένη αλλαγή των δεδομένων που μεταβιβάζονται. Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης. Λέγοντας αλλαγή των δεδομένων εννοούμε προσθήκη, διαγραφή, ή αντικατάσταση δεδομένων.
- Η μη απάρνηση (Non-Repudiation) αφορά την αδυναμία μίας οντότητας να αρνηθεί ότι προέβη σε ενέργειες στις οποίες πράγματι προέβη στο παρελθόν. Δηλαδή ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την

αυθεντικότητα της μετάδοσης ή της δημιουργίας της. Για παράδειγμα, αν μία οντότητα εξουσιοδοτήσει μία άλλη οντότητα για την αγορά ενός περιουσιακού στοιχείου για λογαριασμό της πρώτης, η δεύτερη οντότητα θα πρέπει να μπορεί να εξασφαλίσει ότι η πρώτη δε θα αμφισβητήσει την εξουσιοδότηση που της παρείχε σε προγενέστερο χρόνο.

- Η ταυτοποίηση αυθεντικότητας (Authentication) μπορεί να αφορά την ταυτοποίηση του αποστολέα, του παραλήπτη ή και των ίδιων των δεδομένων που μεταβιβάζονται. Συγκεκριμένα, η ταυτοποίηση αυθεντικότητας σχετίζεται συχνότερα με τη δυνατότητα του παραλήπτη να επιβεβαιώνει ότι το μήνυμα προέρχεται πράγματι από τον συγκεκριμένο αποστολέα και δεν έχει τροποποιηθεί από τρίτο μη εξουσιοδοτημένο πρόσωπο καθοδόν.[9]

2.4 Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα 2.1:



Σχήμα 2.1: Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης

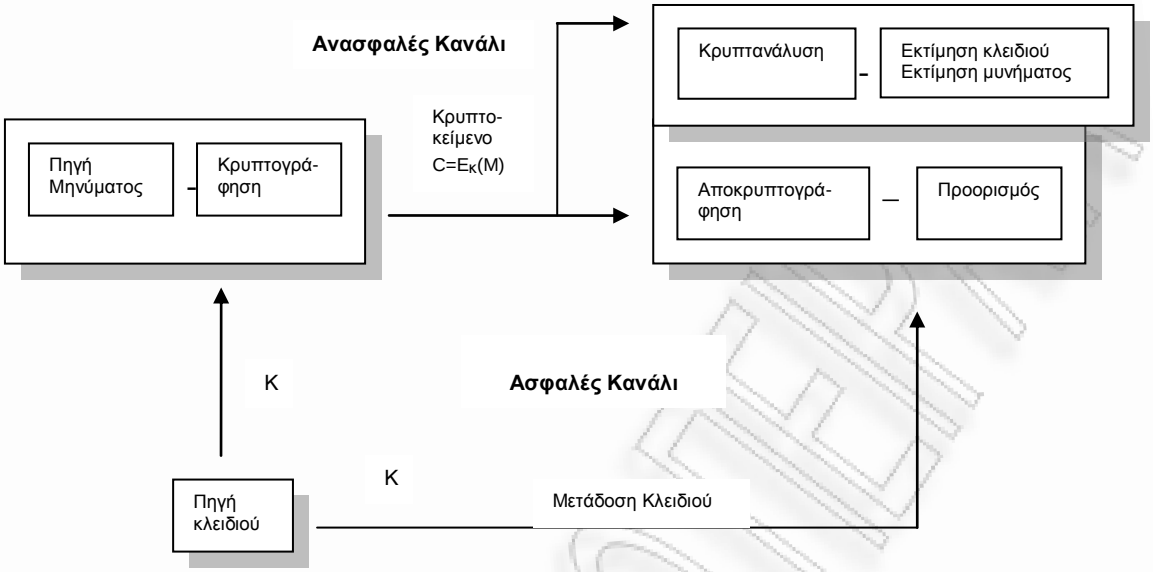
Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από διαφόρους εισβολείς.

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω π.χ. τον Νίκο και τη Μαρία, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο μη εξουσιοδοτημένο, να μην μπορεί να παρεμβάλει στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα δηλαδή ένα σύνολο διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης, αποτελείται από μία πεντάδα (P,C,k,E,D) όπου:

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από το χώρο P και το χώρο k και παράγει μία ακολουθία που ανήκει στο χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, το χώρο C και το χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P.



Σχήμα 2.2: Μοντέλο Τυπικού Κρυπτοσυστήματος

Το Σύστημα του σχήματος 2.2 λειτουργεί με τον ακόλουθο τρόπο:

1) Ο αποστολέας επιλέγει ένα κλειδί μήκους n από το χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2) Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3) Ο αποστολέας δημιουργεί ένα μήνυμα από το χώρο μηνυμάτων.
4) Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (ένα γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5) Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δυο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δεν μπορεί να αναδημιουργήσει το μήνυμα.[2]

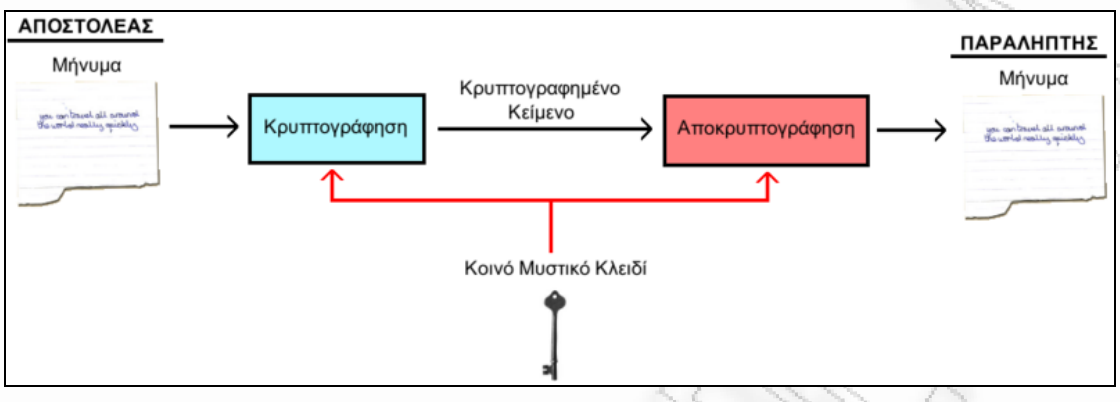
2.5 Είδη Κρυπτογραφίας

2.5.1 Συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού (Symmetric Cryptography or Secret-Key Cryptography)

Στην κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography), χρησιμοποιείται ένα μοναδικό και κοινό κλειδί τόσο κατά τη διαδικασία της κρυπτογράφησης όσο και κατά τη διαδικασία της αποκρυπτογράφησης των δεδομένων (Σχήμα 5). Επομένως και τα δυο συμβαλλόμενα μέρη θα πρέπει να διαθέτουν το ένα και μοναδικό κλειδί για να είναι δυνατή η ανταλλαγή μηνυμάτων και άρα απαιτείται ένα ασφαλές μέσο για τη μετάδοσή του.{[8],σελ.108-109}

Η διανομή κλειδιών μπορεί να επιτευχθεί με διάφορους τρόπους ανάμεσα σε δυο συμβαλλόμενα μέρη Α και Β, π.χ. ένα κλειδί θα μπορούσε να επιλεγεί από τον Α και να παραδοθεί με φυσικό τρόπο στον Β. Επίσης εάν ο Α και Β έχουν χρησιμοποιήσει πρόσφατα κάποιο κλειδί που παραμένει μυστικό, θα μπορούσε ο ένας να διαβιβάσει στον άλλον το νέο κλειδί κρυπτογραφώντας το με το παλαιό κλειδί.

Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης ενός κειμένου με συμμετρική κρυπτογραφία φαίνεται στο παρακάτω σχήμα 2.3:



Σχήμα 2.3: Συμμετρική Κρυπτογραφία

Ο πιο γνωστός αλγόριθμος που ανήκει στην κατηγορία αυτή είναι ο Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Το πρόβλημα που παρουσιάζει όμως αυτή η τεχνική είναι η διανομή των κλειδιών, η εξασφάλιση δηλαδή ότι τα κλειδιά που αποστέλλονται στους παραλήπτες δε θα πέσουν σε λάθος χέρια. Γι' αυτό το λόγο τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοιο σύστημα είναι το σύστημα Kerberos του MIT (Massachusetts Institute of Technology).[Αναλυτικά για το σύστημα Kerberos βλέπε Παράρτημα 1]

Το σύστημα της συμμετρικής κρυπτογράφησης είναι ιδιαίτερα αποτελεσματικό όταν μετέχουν στην επικοινωνία λίγα πρόσωπα τα οποία είναι γνωστά και έχουν εμπιστοσύνη μεταξύ τους. Όποιος θέλει να στείλει μήνυμα με αυτή τη μέθοδο πρέπει να γνωρίζει ότι η κρυπτογραφική κλείδα που θα χρησιμοποιήσει θα πρέπει να γίνει γνωστή και στον αποδέκτη του μηνύματος. Όσο ο αριθμός των χρηστών μεγαλώνει, τόσο μεγαλώνουν και τα προβλήματα της δημιουργίας, της διανομής, της ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών. Άρα τα συστήματα αυτά δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών.[4], [39, σελ.14], [41, σελ.41]

2.5.2 Ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού (Asymmetric Cryptography or Public Key Cryptography)

Η κρυπτογράφηση δημοσίου κλειδιού επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Diffie και Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δε μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Ο κάθε χρήστης, το ιδιωτικό του κλειδί δε θα πρέπει ποτέ να το μεταδίδει στο δίκτυο, αλλά να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Υπάρχουν και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν χρησιμοποιηθεί το δημόσιο κλειδί για την κρυπτογράφηση ενός μηνύματος, μόνο το αντίστοιχο

ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει και αντιστρόφως. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Όπως ήδη έχουμε αναφέρει, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Το πρόβλημα όμως που προκύπτει είναι ότι εάν το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε ο αποστολέας δεν μπορεί να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα. Το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δε γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα.

Η κρυπτογραφία δημόσιου κλειδιού αξιοποιείται για αυθεντικότητα μηνυμάτων και διανομή μυστικών κλειδιών.[13], [39, σελ.14]

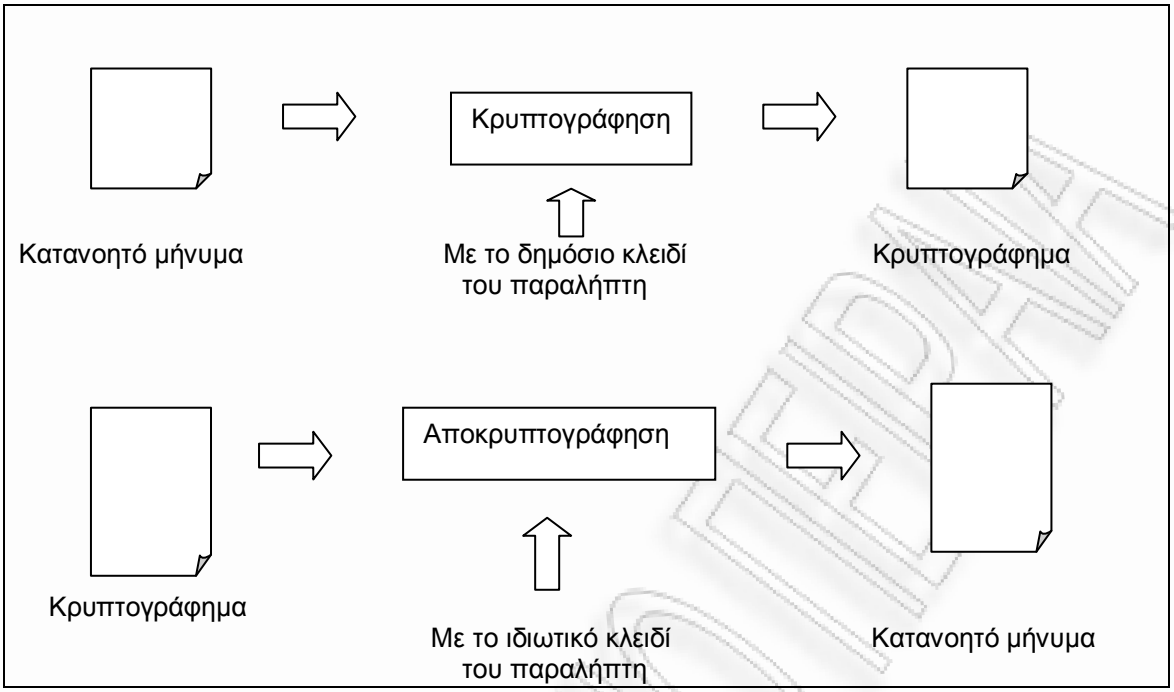
2.5.2.1 Τρόπος λειτουργίας της ασύμμετρης κρυπτογραφίας

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού που χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στην συνέχεια για να παραχθεί ο τυχαίος αριθμός συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από την συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

Στην ασύμμετρη κρυπτογράφηση, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα που θέλει να στείλει με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα αυτό με το ιδιωτικό του κλειδί. Δηλαδή, ένα μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό, καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα.

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

Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης φαίνεται στην παρακάτω σχήμα 2.4.



Σχήμα 2.4: Διαδικασία ασύμμετρης κρυπτογράφησης και αποκρυπτογράφησης

Συνοψίζοντας μπορούμε να πούμε ότι τα βασικά χαρακτηριστικά του δημόσιου και του ιδιωτικού κλειδιού είναι:

- Κάθε κλειδί, ιδιωτικό και δημόσιο, είναι ένα δυαδικό αλφαριθμητικό.
- Τα δημόσια και ιδιωτικά κλειδιά παράγονται ταυτόχρονα από ειδικό πρόγραμμα λογισμικού.
- Τα κλειδιά δεν είναι ταυτόσημα, αλλά σχετίζονται μοναδικά έτσι ώστε να είναι δυνατή η χρήση τους για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Η διαδικασία μέσω της οποίας παράγεται το ζεύγος των κλειδιών εξασφαλίζει ότι κάθε κλειδί σχετίζεται μοναδικά με το ταίρι του και κανένα κλειδί δεν μπορεί να παραχθεί από το άλλο.
- Τα κλειδιά, δημόσια και ιδιωτικά, που ανήκουν σε ένα ζεύγος είναι συμπληρωματικά, δηλαδή οι πληροφορίες που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το άλλο και αντίστροφα.
- Κάθε οντότητα που συμμετέχει σε ένα σύστημα επικοινωνίας δημοσίου κλειδιού έχει το δικό της ζεύγος δημόσιου και ιδιωτικού κλειδιού.
- Το ιδιωτικό κλειδί πρέπει να προστατεύεται από τον ιδιοκτήτη του για να παραμείνει κρυφό και χρησιμοποιείται για την ψηφιακή υπογραφή μηνυμάτων.
- Το δημόσιο κλειδί διανέμεται ελεύθερα και είναι προσβάσιμο σε όποιον το θελήσει. Χρησιμοποιείται για την πιστοποίηση των ψηφιακών υπογραφών, για την κρυπτογράφηση μηνυμάτων και αποθηκεύεται μέσα σε ψηφιακά πιστοποιητικά που παρέχουν την ακεραιότητα και την αυθεντικότητα του ιδιοκτήτη του κλειδιού.

Το 1977 οι Rivest, Shamir και Adleman βασιζόμενοι στις αρχές της θεωρίας αριθμών, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού. Είναι ο ευρύτερα χρησιμοποιούμενος αλγόριθμος ασύμμετρης κρυπτογράφησης. Χρησιμεύει και για την κρυπτογράφηση δημοσίας κλείδας αλλά και για τη δημιουργία ψηφιακής υπογραφής. Το σύστημα αυτό χρησιμοποιεί μεγάλου μεγέθους κλείδες (από 512 έως 1024 bit) οι οποίες προκύπτουν ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς p, q και υπολογίζουμε το γινόμενο τους n = pq. Το n καλείται modulus. Διαλέγουμε ένα 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.[13]

2.6 Περιγραφή της διαδικασίας κωδικοποίησης με τη μέθοδο RSA με μορφή παραδείγματος

Ο Bob θέλει να στείλει ένα μήνυμα στην Alice που να μπορεί να διαβαστεί μόνο από αυτήν. Δηλαδή ο Bob θέλει να στείλει ένα κωδικοποιημένο μήνυμα που μόνο η Alice θα έχει τη δυνατότητα να το αποκωδικοποιήσει .

Για να επιτευχθεί αυτός ο σκοπός, σύμφωνα με το μηχανισμό κωδικοποίησης και αποκωδικοποίησης RSA, η παραλήπτης Alice και ο αποστολέας Bob πρέπει να ακολουθήσουν την επόμενη διαδικασία:

1. Η Alice διαλέγει δύο πολύ μεγάλους πρώτους αριθμούς p και q τους οποίους δεν πρέπει να γνωρίζει κανένας άλλος. Οι αριθμοί αυτοί είναι το ιδιωτικό κλειδί (private key) της Alice. Εδώ για απλοποίηση των υπολογισμών επιλέγουμε τους πρώτους p=17 και q=11.
2. Η Alice πολλαπλασιάζει τους δυο πρώτους αριθμούς p και q και παίρνει τον αριθμό N=p*q. Εδώ N=17*11 $\rightarrow$ N= 187.
3. Η Alice κατόπιν επιλέγει ένα άλλο ακέραιο e τέτοιο ώστε μκδ [e, (p-1)*(q-1)]=1. Εδώ (p-1)*(q-1)= 16*10=160 και ένας τέτοιος αριθμός είναι ο e=7 ,προφανώς ο e=7 δεν είναι ο μοναδικός ακέραιος που είναι πρώτος ως προς τον 160.
4. Η Alice δημοσιοποιεί αυτούς τους δυο αριθμούς e και N που είναι το δημόσιο κλειδί (public key) της. Ο αριθμός e μπορεί να είναι μέρος του δημόσιου κλειδιού και κάποιου άλλου, αλλά το N πρέπει να ανήκει μόνο στην Alice. Εδώ (e, N)=(7, 187).

Τώρα ο Bob για να στείλει ένα κωδικοποιημένο μήνυμα στην Alice πρέπει να κάνει τα επόμενα βήματα:

5. Ο Bob προκειμένου να κωδικοποιήσει το μήνυμά του το μετατρέπει σε ένα αριθμό, έστω M, του δεκαδικού συστήματος.

   Π.χ. αν το μήνυμα του Bob είναι το γράμμα X τότε πρώτα μετατρέπει το X σε αριθμό του δυαδικού συστήματος. Σύμφωνα με το σύστημα ASCII (American Standard Code for Information Interchange), το X παρίσταται με τον αριθμό 01011000 του δυαδικού.

   Στο δεκαδικό σύστημα ο αριθμός αυτός είναι:

   $0*2^0+0*2^1+0*2^2+1*2^3+1*2^4+0*2^5+1*2^6+0*2^7=8+16+64=88$

   Άρα M= 88

   Δηλαδή το μήνυμα X του Bob προς την Alice είναι ο αριθμός M=88 του δεκαδικού συστήματος.
6. Ο Bob γνωρίζει το δημόσιο κλειδί της Alice και προκειμένου να κωδικοποιήσει το μήνυμα M χρησιμοποιεί τον τύπο : $C \equiv M^e (\text{mod} N)$

   Εδώ $C \equiv 88^7 (\text{mod} 187)$

   Και επειδή $88^7 = 88^{4+2+1}$ είναι:

   $88^7 (\text{mod} 187) = [88^4 (\text{mod} 187) * 88^2 (\text{mod} 187) * 88^1 (\text{mod} 187)] (\text{mod} 187)$

   $= (132*77*88)(\text{mod} 187)$

   $= 894.432(\text{mod} 187)$

   $=11(\text{mod} 187)$

   Άρα το M= 88 σε κωδικοποιημένη μορφή είναι το C=11
7. Η Alice λαμβάνει το κρυπτογραφημένο μήνυμα C=11 και χρησιμοποιεί το ιδιωτικό της κλειδί (p,q) και προσδιορίζει τον αριθμό d από την εξίσωση

   $e*d \equiv 1(\text{mod} (p-1)*(q-1))$

   Εδώ $7* d \equiv 1(\text{mod} 160)$

   Δηλαδή $7* d \equiv 160*\kappa+1$

   αν για κ=1, d= 161/7= 23

8. Η Alice τώρα προχωρεί στην αποκρυπτογράφηση του μηνύματος με βοήθεια της σχέσης $M= C^d(modN)$

Εδώ $M= 11^{23} (mod187)$

Τώρα, $11^{23}(mod187)=$

$= [11^1(mod187)*11^2(mod187)*11^4(mod187)*11^{16}(mod187)] (mod187)$

$= (11*121*55*154) (mod187)$

$= 88$

Άρα στο ASCII το 88 αντιστοιχεί στο X

Το όλο εγχείρημα στηρίζεται σε κάποιες συναρτήσεις που είναι γνωστές σαν μονόδρομες συναρτήσεις. Μια τέτοια συνάρτηση είναι και η $C≡M^e(modN)$.

Είναι πολύ δύσκολο, από τη συνάρτηση αυτή, κάποιος που γνωρίζει ότι C= 11 να βρει το M που είναι 88.[18]

2.7 Παράδειγμα συμμετρικής και ασύμμετρης κρυπτογραφίας

Θα παρουσιάσουμε ένα αναλογικό παράδειγμα από την καθημερινή ζωή για να καταλάβουμε τη διαφορά ανάμεσα στη συμμετρική και στην ασύμμετρη κρυπτογράφηση.

Έστω η Alice και ο Bob, θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας το δημόσιο ταχυδρομείο. Η Alice θέλει να στείλει ένα κρυφό μήνυμα στον Bob και περιμένει μια κρυφή απάντηση από αυτόν.

Σύμφωνα με την κρυπτογράφηση συμμετρικού κλειδιού η Alice θα βάλει το μήνυμά της μέσα σε ένα κουτί με λουκέτο για το οποίο έχει το κλειδί και στέλνει το κλειδωμένο κουτί με το δημόσιο ταχυδρομείο στον Bob. Ο Bob έχει ένα ίδιο κλειδί (το οποίο έχει πάρει από την Alice στο παρελθόν, σε διαπροσωπική συνάντηση που είχαν) και μόλις λαμβάνει το κουτί ανοίγει το λουκέτο και διαβάζει το μήνυμα. Ο Bob βάζει το μήνυμά του μέσα στο κουτί, το κλειδώνει και το στέλνει με τη σειρά του με το δημόσιο ταχυδρομείο στην Alice.

Το πρόβλημα εδώ είναι ότι το κλειδί για το λουκέτο είναι κοινό και για την Alice και για τον Bob και για να δώσει αντίγραφο του κλειδιού ο ένας με τον άλλον θα πρέπει να συναντηθούν γιατί δεν είναι ασφαλές να το στείλουν με το δημόσιο ταχυδρομείο, αφού θα μπορούσε τότε κάποιος υπάλληλος του ταχυδρομείου να υποκλέψει το κλειδί και να δημιουργήσει ένα αντίγραφο ώστε στο μέλλον να υποκλέπτει ή και να παραποιεί τα μηνύματα που ανταλλάσσονται στο κουτί.

Η κρίσιμη διαφορά στο κλειδί ασύμμετρης κρυπτογράφησης είναι ότι η Alice και ο Bob ποτέ δε χρειάζεται να στείλουν αντίγραφο του κλειδιού ο ένας στον άλλον. Έτσι αποφεύγεται το ενδεχόμενο να υποκλέψει κάποιος υπάλληλος του ταχυδρομείου το κλειδί αφού σε αυτή την περίπτωση η Alice και ο Bob δε χρειάζεται να εμπιστευτούν το δημόσιο ταχυδρομείο. Επίσης ο Bob επιτρέπει σε όποιον επιθυμεί να αντιγράψει το κλειδί του άρα και τα μηνύματα της Alice προς τον Bob θα είναι εκτεθειμένα σε κίνδυνο υποκλοπής. Όμως όλα τα μηνύματα της Alice προς άλλους θα είναι μυστικά, αφού οι υπόλοιποι θα παρέχουν διαφορετικά λουκέτα για να κλειδώσει η Alice το μήνυμα στο κουτί πριν το στείλει σε αυτούς.[13]

Στην πράξη της ασύμμετρης κρυπτογραφίας, ο Bob και η Alice έχουν ξεχωριστές κλειδαριές. Πρώτα η Alice βάζει το μυστικό μήνυμα στο κουτί, το κλειδώνει με το λουκέτο που μόνο αυτή έχε κλειδί και στη συνέχεια στέλνει το κουτί στον Bob με απλό δημόσιο ταχυδρομείο. Όταν ο Bob λαμβάνει το κουτί, προσθέτει το δικό του λουκέτο στο κουτί και το στέλνει πίσω στην Alice. Η Alice λαμβάνει το κουτί με δύο λουκέτα, αφαιρεί το δικό της λουκέτο και το στέλνει πίσω στον Bob. Όταν ο Bob λαμβάνει το κουτί έχει πάνω μόνο το δικό του λουκέτο, το οποίο μπορεί να ξεκλειδώσει και να δει το μήνυμα της Alice. Σε αυτό το παράδειγμα η διαδικασία της αποκρυπτογραφίας είναι ίδια με τη διαδικασία της κρυπτογραφίας.

2.8 Πλεονεκτήματα και μειονεκτήματα συμμετρικής και ασύμμετρης κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας είναι να πραγματοποιηθεί η ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε αν γνωρίζει για τη συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Στη συνέχεια, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για τη μετάδοση του κλειδιού (π.χ. μέσω τηλεφωνου), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Σε αυτό το πρόβλημα η ασύμμετρη κρυπτογραφία δίνει λύση αφού σε καμία περίπτωση οι εν λόγω ευαίσθητες πληροφορίες δε μεταφέρονται μέσω δικτύου.

Ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν 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 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.

Ένα όμως μειονέκτημα που έχει η ασύμμετρη κρυπτογραφία είναι σχετικά με την ταχύτητά της. Οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης. Κατά κανόνα, η διαδικασία κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Επίσης, μεγάλο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Αρχές Πιστοποίησης) ώστε να διασφαλίζεται η κατοχή τους από νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με τη 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 περιβάλλοντα 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, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι.

Οι ψηφιακοί φάκελοι (Digital Envelopes) αποτελούν ένα συνδυασμό της συμμετρικής και ασύμμετρης κρυπτογράφησης προκειμένου να επιτευχθεί η ασφαλής μετάδοση της πληροφορίας που προσφέρει η ασύμμετρη κρυπτογράφηση και η ταχύτητα που προσφέρει η συμμετρική κρυπτογράφηση. Έτσι σε έναν ψηφιακό φάκελο, το κείμενο ή το μήνυμα κρυπτογραφείται συμμετρικά με μια μυστική κλείδα και η κλείδα αυτή κρυπτογραφείται με το δημόσιο κλειδί του αποδέκτη του μηνύματος. Συνεπώς μόνο ο αποδέκτης που γνωρίζει την ιδιωτική του κλείδα μπορεί να αποκρυπτογραφήσει τη μυστική κλείδα και εν συνεχεία χρησιμοποιώντας την, μπορεί να αναγνώσει το κείμενο που έχει κρυπτογραφηθεί συμμετρικά. Προκειμένου να επιτευχθεί αυτή η ανταλλαγή μυστικής κλείδας υπάρχουν συγκεκριμένα πρωτόκολλα, με ευρύτερα γνωστό και χρησιμοποιούμενο το Diffie Hellman Key Exchange.

2.9 Εφαρμογές της κρυπτογραφίας

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου (privacy) μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στη δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση.

Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου ότι οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφικής διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη.

Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά λοιπόν αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

Η βασικότερη εφαρμογή της κρυπτογραφίας όμως υπηρετεί τη διακρίβωση της γνησιότητας των ηλεκτρονικών εγγράφων αποτελεί δηλαδή μορφή ηλεκτρονικής υπογραφής.

Κεφάλαιο 3

3.1 Η ηλεκτρονική υπογραφή

3.1.1 Εισαγωγικές παρατηρήσεις

Η ανασφάλεια που νιώθει ο συναλλασσόμενος για τις ηλεκτρονικές συναλλαγές είναι ένας από τους σημαντικότερους παράγοντες που εμποδίζουν την ανάπτυξη τους. Τα ανοιχτά δίκτυα, όπως το διαδίκτυο, δηλαδή τα δίκτυα ηλεκτρονικής επικοινωνίας στα οποία μπορεί να συμμετέχει ο οποιοσδήποτε διαθέτει τα απαραίτητα τεχνικά μέσα, είναι ιδιαίτερα επιρρεπή στην υποκλοπή και στην τροποποίηση του περιεχομένου της πληροφορίας την οποία μεταφέρουν. Οι κίνδυνοι αυτοί αυξάνονται με γεωμετρική πρόοδο καθώς αυξάνονται οι χρήστες των ανοικτών δικτύων.

Η εξασφάλιση της ακεραιότητας, δηλαδή το αναλλοίωτο των εγγράφων και η εξακρίβωση της αυθεντικότητας των δεδομένων, δηλαδή της ταυτότητας του αποστολέα είναι αρκετά δύσκολο να επιτευχθεί στο βαθμό που είναι από τεχνικής πλευράς πολύ απλό για έναν ειδικό να έχει πρόσβαση στα δεδομένα που διαβιβάζονται αλλά και να παρεμβαίνει σε αυτά. Επίσης τίποτα δεν μπορεί να διαβεβαιώσει την εμπιστευτικότητα, δηλαδή ότι το μήνυμα θα διαβαστεί μόνο από τον παραλήπτη για τον οποίο προορίζεται.[35,σελ.151]

Όμως το πιο σημαντικό είναι το ζήτημα της αβεβαιότητας σχετικά με τη νομική αξία των ηλεκτρονικών εγγράφων που δεν μπορούν φυσικά να φέρουν τη χειρόγραφη υπογραφή του εκδότη τους. Το δίκαιό μας απαιτεί την ιδιόχειρη υπογραφή για τον έγγραφο τύπο επειδή αυτή μπορεί να λειτουργήσει ως ένδειξη της προέλευσης του εγγράφου αλλά και ως πιστοποίηση της αυθεντικότητάς του. [35, σελ.153]

Μια από τις μεθόδους που χρησιμοποιούνται για την ασφαλή διακίνηση των πληροφοριών στο σύγχρονο περιβάλλον, είναι η κρυπτογραφία. Η κρυπτογραφία αποτέλεσε πανάρχαια μέθοδο εξασφάλισης της εμπιστευτικότητας των συναλλαγών. Εξακολουθεί έως και σήμερα να συμβάλλει στον παραπάνω στόχο καθώς η ίδια αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet. Έτσι, με τη συνδυασμένη χρήση κρυπτογραφικών εργαλείων (αλγόριθμοι), κατάλληλα διαμορφωμένου λογισμικού, υποδομών και συγκεκριμένων διαδικασιών, 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 και την ακεραιότητα των σχετικών δεδομένων, την ταυτοποίηση των συναλλασσόμενων και τη νομική δέσμευση του υπογράφοντα ή αλλιώς τη μη αποποίηση της συναλλαγής. Ενώ παράλληλα, μπορούν να προσφέρουν αξιόπιστη λύση και στο ζήτημα της εμπιστευτικότητας των δεδομένων κατά την διακίνηση και την αρχειοθέτησή τους.[1]

3.2 Μέθοδοι ασφάλειας ηλεκτρονικών συναλλαγών

Στις καθημερινές συμβατικές συναλλαγές έχουν καθιερωθεί είτε εθιμικά είτε νομοθετικά η χρήση διαφόρων μεθόδων για την εξακρίβωση της ταυτότητας των συναλλασσόμενων και την συγκέντρωση και διατήρηση αποδείξεων για την πραγματοποίηση μιας συναλλαγής, που βασίζονται κυρίως σε πρωτότυπα ενυπόγραφα έγγραφα που αρχειοθετούνται και επιδεικνύονται όποτε χρειάζεται.

Αντιθέτως, στις ηλεκτρονικές συναλλαγές τα χρησιμοποιούμενα ψηφιακά δεδομένα, λόγω της μη ενσωμάτωσής τους σε ένα μοναδικό υλικό φορέα, είναι δύσκολο να προστατευθούν από αλλοίωση ή και αντιγραφή, ενώ και η απόδειξη της προέλευσής τους καθίσταται επίσης ιδιαίτερα προβληματική.

Σήμερα οι βασικές μέθοδοι ηλεκτρονικής ταυτοποίησης των συναλλασσόμενων (π.χ. κωδικός χρήστη, κωδικός πρόσβασης) και διαφύλαξης της ακεραιότητας των δεδομένων (π.χ. συμμετρική κρυπτογράφηση), λειτουργούν με τη χρήση κοινών κλειδιών ή κωδικών από τους συναλλασσόμενους, με συνέπεια να μην μπορούν να υποστηρίξουν εφαρμογές που απαιτούν

ασφαλή, αξιόπιστη και εγγυημένη πιστοποίηση της ταυτότητας (ταυτοποίηση) των χρηστών και των κλειδιών αυτών έναντι κάθε τρίτου, ούτε και να εξασφαλίσουν την πιστοποίηση της προέλευσης (αυθεντικότητα), την ακεραιότητα και την εμπιστευτικότητα των διακινούμενων ή και αρχειοθετούμενων ηλεκτρονικών δεδομένων. Σχετική με την παραπάνω ανεπάρκεια των χρησιμοποιούμενων μεθόδων, αποτελεί και η διαπίστωση μεγάλης έρευνας που πραγματοποιήθηκε στα πλαίσια του έργου 'La Mer' (9/2003) με την συμπλήρωση σχετικού ερωτηματολογίου από πολλές συμμετέχουσες ΜΜΕ, σύμφωνα με την οποία, η έλλειψη ασφάλειας στις ηλεκτρονικές συναλλαγές αποτελεί τον πρώτο αρνητικό λόγο με ποσοστό 77% που δικαιολογούν οι επιχειρήσεις την απροθυμία τους να ενασχοληθούν με το ηλεκτρονικό εμπόριο.

Έτσι τα έντυπα μέσα που χρησιμοποιούνται για την καταγραφή και την απόδειξη μιας συναλλαγής (π.χ. ενυπόγραφα ιδιωτικά έγγραφα, επικυρωμένα φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι κ.λ.π.) εξακολουθούν να αποτελούν σήμερα τα κύρια αποδεικτικά στοιχεία μιας συναλλαγής.

Η πλήρης αντικατάστασή τους με αντίστοιχα ψηφιακά δεδομένα τα οποία επιτρέπουν ολοκληρωμένες ηλεκτρονικές συναλλαγές ιδίως σε περιπτώσεις σημαντικών συναλλαγών, προϋποθέτει τη χρήση ασφαλών και τεχνικώς αξιόπιστων μεθόδων πιστοποίησης της προέλευσης και της ακεραιότητας των δεδομένων και κυρίως την παροχή αποδείξεων για τη μη αποκήρυξη της συναλλαγής κάτι που με τις υπάρχουσες σήμερα τεχνολογικές δυνατότητες, μπορεί να παράσχει άμεσα μόνο η χρήση προηγμένων ηλεκτρονικών υπογραφών και σχετικών ηλεκτρονικών πιστοποιητικών ταυτοποίησης.[1]

3.3 Η παραδοσιακή έννοια της υπογραφής

Υπογραφή είναι η χειρόγραφη αποτύπωση του ονοματεπωνύμου ενός φυσικού προσώπου, με την οποία αυτό εκφράζει τη βούλησή του να δεσμευθεί από ένα γραπτό κείμενο. Η παραδοσιακή αυτή μορφή της υπογραφής καθιερώθηκε για πρώτη φορά από το γαλλικό σύστημα δικαίου στα μέσα του 16ου αιώνα επιτελώντας τρεις βασικές λειτουργίες. Πρώτον δηλώνει την έγκυρη βούληση του υπογράφοντος, δεύτερον πιστοποιεί την προέλευσή του από αυτόν και τρίτον αποτελεί αποδεικτικό μέσο σε περίπτωση δικαστικής διένεξης.

Επίσης, η υπογραφή μπορεί να επιτελεί μια ποικιλία από λειτουργίες εξαρτώμενες από τη φύση του εγγράφου που έχει υπογραφεί. Για παράδειγμα μια υπογραφή μπορεί να βεβαιώνει την πρόθεση του προσώπου να δεσμευθεί από το περιεχόμενο του υπογεγραμμένου συμβολαίου, την πρόθεση του προσώπου να πιστοποιήσει τη σύνταξη του εγγράφου από τον ίδιο, την πρόθεση του προσώπου να συσχετιστεί με το περιεχόμενο ενός εγγράφου συντεταγμένου από τρίτο πρόσωπο, ή και το γεγονός ότι ένα πρόσωπο βρισκόταν σε συγκεκριμένη χρονική στιγμή σε ορισμένο τόπο.

Η ιδιόχειρη υπογραφή, δηλαδή η γραφή του ονόματος και του επωνύμου του εκδότη με το ίδιο του το χέρι, εξασφαλίζει την εξατομίκευση του συντάκτη του εγγράφου, αφού σε κάθε πρόσωπο αντιστοιχεί ένας μοναδικός και προσωπικός γραφικός χαρακτήρας. Με τον τρόπο αυτό καθίσταται δύσκολη η απομίμηση της υπογραφής από τρίτα πρόσωπα και διευκολύνεται ο έλεγχος της γνησιότητας της με βάση ατομικά δείγματα υπογραφής. Ωστόσο και στην περίπτωση της ιδιόχειρης υπογραφής δεν υπάρχει απόλυτη ασφάλεια, αφού μια υπογραφή μπορεί να πλαστογραφηθεί, να μεταφερθεί από ένα έγγραφο σε ένα άλλο, ενώ δυνατή είναι και η τροποποίηση ενός εγγράφου μετά την υπογραφή του.

Στην ευρύτερη έννοια της υπογραφής εμπίπτουν και άλλα είδη που θεωρούνται εξίσου επαρκή να εκπληρώσουν τις απαιτήσεις της κλασικής υπογραφής, όπως η σφραγίδα ή ακόμη και η με μηχανικά μέσα υπογραφή. Τέλος σε ορισμένες περιπτώσεις απαιτείται ένας συνδυασμός της ιδιόχειρης υπογραφής με πρόσθετες διαδικασίες ασφάλειας, όπως επιβεβαίωση της από μάρτυρες.[27]

3.4 Η έννοια της ηλεκτρονικής υπογραφής

Η νομιμοποίηση ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα παραδοσιακά χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται ηλεκτρονική.

Όταν ακούει κανείς τον όρο υπογραφή, αντιλαμβάνεται μια ιδιόχειρη γραφή με την οποία επιβεβαιώνει τη βούληση, τη συμφωνία ή την εγγύηση του ο υπογράφων. Η ηλεκτρονική υπογραφή όμως, δεν έχει σχεδόν καμία σχέση με την ιδιόχειρη υπογραφή, παρά μόνο στο γεγονός ότι και με την ηλεκτρονική υπογραφή, βεβαιώνεται η ταυτότητα και η βούληση αυτού που υπογράφει.[6]

Με τον όρο ηλεκτρονική υπογραφή δεν εννοούμε την αποτύπωση της ιδιόχειρης υπογραφής με ηλεκτρονικά μέσα π.χ. μέσω ενός σαρωτή εγγράφου, ούτε τη μεταβίβαση της με ηλεκτρονικά μέσα. Ουσιαστικά, πρόκειται για μια ηλεκτρονική σύντμηση που προκύπτει από το ηλεκτρονικό έγγραφο το οποίο συνοδεύει και από απόρρητα δηλωτικά στοιχεία του υπογράφοντα η οποία θα μπορούσε να χαρακτηριστεί και ως δακτυλικό αποτύπωμα του εγγράφου αυτού.[8,σελ.109], [35,σελ.155]

Στο άρθρο 2 της Οδηγίας 99/93/ΕΚ αλλά και του Π.Δ. 150/2001 ορίζεται ότι ως ‘’ηλεκτρονική υπογραφή’’ νοούνται 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.[26]

Σκοπός της ηλεκτρονικής υπογραφής είναι αφενός η διασφάλιση της γνησιότητας και της ακρίβειας του περιεχομένου του ηλεκτρονικού εγγράφου (ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις) και αφετέρου της εξατομίκευσης του εκδότη του εγγράφου αυτού.[6]

Τα είδη των ηλεκτρονικών υπογραφών αναφέρονται στα νομοθετήματα. Όπως αναφέρεται στο Π.Δ. 150/2001, γίνεται λόγος για δύο ηλεκτρονικές υπογραφές: την απλή ηλεκτρονική υπογραφή και την προηγμένη ηλεκτρονική υπογραφή δηλαδή τη ψηφιακή υπογραφή, την οποία και θα αναλύσουμε παρακάτω στο κεφάλαιο 4. Οι μεταξύ τους διαφοροποιήσεις περιγράφονται με σαφήνεια στο Π.Δ., τις οποίες και θα δούμε εκτενέστερα στη συνέχεια της εργασίας μας. Ουσιαστικά η ψηφιακή υπογραφή αποτελεί την πιο προηγμένη και ασφαλή μέθοδο αναγνώρισης της γνησιότητας του εκδότη ηλεκτρονικού εγγράφου, που δημιουργείται βάσει του ασύμμετρου κρυπτογραφικού συστήματος.

Η προηγμένη ηλεκτρονική υπογραφή, όπως φαίνεται και από την ονομασία της, παρέχει περισσότερα εχέγγυα απόδειξης της γνησιότητας του ηλεκτρονικού εγγράφου καθώς το εξοπλίζει με πρόσθετες απαιτήσεις όπως μονοσήμαντη σύνδεση με τον υπογράφοντα, ικανότητα να ταυτοποιήσει τον υπογράφοντα, δημιουργία της υπογραφής με μέσα που είναι υπό τον αποκλειστικό έλεγχο του υπογράφοντα, και δυνατότητα εντοπισμού οποιασδήποτε αλλοίωσης των δεδομένων.[35,σελ.156]

Ο νομοθετικός ορισμός της ηλεκτρονικής υπογραφής επιτυγχάνει να συνδυάζει αφενός την τεχνική ουδετερότητα και άρα και την προσαρμοστικότητα έναντι στις μελλοντικές τεχνολογικές εξελίξεις και αφετέρου τη μη απόρριψη των ήδη εδραιωμένων πρακτικών στο χώρο των ηλεκτρονικών συναλλαγών. Έτσι στο πεδίο εφαρμογής του Π.Δ. 150/2001 περιλαμβάνονται από τις πιο απλές διαδικασίες τεκμηρίωσης, όπως είναι η χρήση προσωπικού κωδικού αριθμού των λεγόμενων PIN (Personal Identification Number), μέχρι και τις πιο σύνθετες, όπως αυτής της ασύμμετρης κρυπτογραφίας με τη μέθοδο RSA, γνωστής και ως ψηφιακή υπογραφή. [36,σελ.167]

3.4.1 Η ηλεκτρονική υπογραφή από τεχνική σκοπιά

3.4.1.1 Η χρησιμοποίηση προσωπικού κωδικού αναγνώρισης- PIN

Ο προσωπικός αριθμός αναγνώρισης - PIN είναι ένας μυστικός κωδικός πρόσβασης που χρησιμοποιεί ο χρήστης για να μπορέσει να αποκτήσει πρόσβαση σ' ένα συγκεκριμένο σύστημα. Χρησιμοποιείται δηλαδή για τον έλεγχο της ταυτότητας του χρήστη. Ο κάθε χρήστης που έχει το δικό του PIN έχει και την ευθύνη για το να μην αποκαλυφθεί αυτός ο κωδικός αριθμός σε τρίτους. Υπάρχει και η περίπτωση ο κωδικός αριθμός να γνωστοποιηθεί στον δικαιούχο με τέτοιο τρόπο ώστε να μην καταστεί γνωστός ούτε στην υπηρεσία που τον εξέδωσε, χαρακτηριστικό παράδειγμα το τμήμα μηχανογράφησης της τράπεζας. [36,σελ.168], [47]

Το είδος αυτό της ηλεκτρονικής υπογραφής είναι ευρύτατα διαδεδομένο στις σύγχρονες συναλλαγές. Μειονέκτημα ωστόσο της διαδικασίας αυτής είναι το γεγονός ότι απαιτεί την επαφή των μερών που πρόκειται να κάνουν χρήση αυτής, ώστε να καθοριστούν οι λεπτομέρειες της διαδικασίας τεκμηρίωσης αλλά και να γνωστοποιηθεί στον δικαιούχο ο κωδικός αριθμός του. Επίσης απαιτεί την ύπαρξη σχέσης εμπιστοσύνης ανάμεσα στα δύο μέρη, κάτι που είναι δύσκολο στην εφαρμογή στα ανοιχτά δίκτυα δηλαδή στο διαδίκτυο. [36,σελ. 169]

3.4.1.2 Η κρυπτογραφία

Μια διαδεδομένη μέθοδος τεκμηρίωσης είναι η κρυπτογραφία. Με τη μέθοδο αυτή μπορεί να εξασφαλιστεί η αυθεντικότητα και η μη αλλοίωση ενός κειμένου, δηλαδή ότι το κείμενο προέρχεται όντως από τον υπογράφοντα και δεν έχει υποστεί αλλοιώσεις κατά τη διαβίβασή του.

Τα συστήματα κρυπτογράφησης που εφαρμόζονται ως μέθοδος τεκμηρίωσης της γνησιότητας κάνουν χρήση κρυπτογραφικών αλγορίθμων, δηλαδή μαθηματικών συναρτήσεων, οι οποίοι χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των σχετικών διαβιβαζόμενων δεδομένων.[36,σελ.170]

Δύο είναι οι βασικές εφαρμογές της κρυπτογράφησης: η έγκρυψη ή κρυπτοθέτηση (encryption) και η ηλεκτρονική υπογραφή (electronic signature). [35, σελ.157]

3.4.1.2.1 Η έγκρυψη ή κρυπτοθέτηση

Στην περίπτωση της κρυπτοθέτησης τα δεδομένα διαβιβάζονται με τέτοιο τρόπο ώστε να διασφαλίζεται το απόρρητο της επικοινωνίας, δεν αποτελεί όμως μέθοδο τεκμηρίωσης προς διακρίβωση της προέλευσης των δεδομένων. Ως εκ τούτου η κρυπτογραφική αυτή μέθοδος δεν αποτελεί είδος ηλεκτρονικής υπογραφής με την έννοια του άρθρου 2 παρ.1 του Π.Δ. 150/2001 και της Οδηγίας 99/93/ΕΚ καθώς διασφαλίζει μόνον την εμπιστευτικότητα των διαβιβαζόμενων δεδομένων και δεν είναι σε θέση να εξασφαλίσει και τη γνησιότητα αυτών.[35,σελ. 157]

Εντούτοις, η κρυπτοθέτηση χρησιμοποιείται ευρύτατα στις ηλεκτρονικές συναλλαγές. Για παράδειγμα οι συναλλαγές ηλεκτρονικής τραπεζικής (e-banking) εκτελούνται στο σύνολό τους πλέον κάνοντας χρήση μεθόδων κρυπτοθέτησης. Η κρυπτοθέτηση συνηθίζεται επίσης στις συναλλαγές του ηλεκτρονικού εμπορίου (e- commerce). Για παράδειγμα στις αγορές μέσω του Παγκόσμιου Ιστού, κατά το στάδιο που ο χρήστης καλείται να γνωστοποιήσει στον έμπορο ευαίσθητα δεδομένα, όπως τον αριθμό της πιστωτικής του κάρτας, τα δεδομένα αυτά διαβιβάζονται στον τελευταίο κρυπτοθετημένα. Τέλος και στον τομέα της ηλεκτρονικής διακυβέρνησης (e-government) η κρυπτοθέτηση των δεδομένων που καταχωρεί ο διοικούμενος στον Η/Υ αποτελεί πλέον σχεδόν αυτονόητη πρακτική π.χ. κατά την υποβολή της δήλωσης φορολογίας εισοδήματος μέσω του συστήματος Taxis. [36,σελ.171]

Όπως αναφέραμε και παραπάνω, αντικείμενο της διαδικασίας της κρυπτοθέτησης δεν είναι να διασφαλίσει τη γνησιότητα, την ακεραιότητα και την προέλευση των διαβιβαζόμενων δεδομένων, αλλά να προστατεύσει αυτά να διαβαστούν από κάποιον ανεπιθύμητο κατά το στάδιο της διαβίβασης. Λόγω της δομής του διαδικτύου κάθε σύνολο δεδομένων για να διαβιβαστεί στον αποδέκτη του διέρχεται από έναν απροσδιόριστο αριθμό Η/Υ. Ο χρήστης καθενός από αυτούς τους Η/Υ μπορεί αν θέλει να διαβάσει τα δεδομένα που διέρχονται από

τον υπολογιστή του. Η μέθοδος λοιπόν, της κρυπτοθέτησης μπορεί να απαλείψει αυτό ακριβώς το χαρακτηριστικό της επικοινωνίας μέσω του διαδικτύου και να προστατεύσει το απόρρητο αυτής. [36,σελ.171-172]

Ένα ευρύτατα διαδεδομένο σύστημα κρυπτοθέτησης είναι το SSL (Secure Socket Layer), το οποίο είναι σε θέση να εξασφαλίσει τη δημιουργία ενός ασφαλούς διαύλου επικοινωνίας σε μια on-line συναλλαγή. Ειδικότερα, η πληροφορία π.χ. ο αριθμός μιας πιστωτικής κάρτας, πρώτα κρυπτογραφείται με βάση ένα μυστικό κλειδί που έχει δημιουργηθεί ειδικά για την περίπτωση αυτή και το οποίο γνωρίζουν ο browser του χρήστη και ο server. Στη συνέχεια μεταδίδεται για να αποκρυπτογραφηθεί από τον λήπτη. Ωστόσο το βασικό μειονέκτημα του συστήματος αυτού είναι ότι δεν προϋποθέτει αναγνώριση της ταυτότητας του δικαιούχου. Γι' αυτό το λόγο αναπτύχθηκε το σύστημα SET (Secure Electronic Transaction) το οποίο χρησιμοποιείται αποκλειστικά ως σύστημα πληρωμών μέσω πιστωτικών καρτών, αν και έχει χαρακτηριστεί αρκετά δύσχρηστο από τους συμβαλλόμενους. [35,σελ. 158]

3.4.1.2.2 Η ηλεκτρονική υπογραφή

Η δεύτερη εφαρμογή της κρυπτογραφίας υπηρετεί τη διακρίβωση της γνησιότητας των ηλεκτρονικών εγγράφων αποτελεί δηλαδή μορφή ηλεκτρονικής υπογραφής. Τα συστήματα κρυπτογράφησης που εφαρμόζονται στο πλαίσιο της ηλεκτρονικής υπογραφής αποτελούνται από κρυπτογραφικούς αλγορίθμους δηλαδή από μαθηματικές συναρτήσεις που χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων, πρόκειται για τα ονομαζόμενα κλειδιά. Δύο είναι οι κυριότεροι τύποι συστημάτων κρυπτογράφησης ηλεκτρονικής υπογραφής, το συμμετρικό κρυπτογραφικό σύστημα και το ασύμμετρο κρυπτογραφικό σύστημα τους οποίους έχουμε αναλύσει στο κεφάλαιο 2. [35,σελ.159]

3.5 Η ηλεκτρονική υπογραφή ως έννοια νομική

Αφού είδαμε τις λύσεις προκειμένου να εξασφαλισθεί η γνησιότητα και η ακεραιότητα ενός συνόλου ηλεκτρονικών δεδομένων, ας δούμε ποιες από αυτές μπορούν να υπαχθούν στον νομοθετικό ορισμό της ηλεκτρονικής υπογραφής αλλά και της προηγμένης ηλεκτρονικής υπογραφής, ώστε να υπαγάγουν τα έννομα αποτελέσματα που προβλέπει το Π.Δ. 150/2001 και η Οδηγία 99/93/ΕΚ. [36,σελ.178]

3.5.1 Η χρήση προσωπικού κωδικού αναγνώρισης -PIN

Η πιο ευρέως χρησιμοποιούμενη μορφή τεκμηρίωσης της γνησιότητας ηλεκτρονικών δεδομένων αποτελεί η χρήση προσωπικού κωδικού αναγνώρισης -PIN. Αποτελεί μορφή ηλεκτρονικής υπογραφής με την έννοια του άρθρου 2 παραγρ.1 του Π.Δ. 150/2001 και της Οδηγίας 99/93/ΕΚ, αφού ο αριθμός PIN όταν εισάγεται σε ένα σύστημα Η/Υ αποτελεί δεδομένο σε ηλεκτρονική μορφή, το οποίο είναι συνημμένο σε άλλα ηλεκτρονικά δεδομένα (π.χ σε στοιχεία της τραπεζικής συναλλαγής) και το οποίο χρησιμεύει ως μέθοδος απόδειξης της γνησιότητας των δεδομένων.[36,σελ.178]

3.5.2 Η συμμετρική κρυπτογραφία

Η μέθοδος της συμμετρικής κρυπτογραφίας αποτελεί και αυτή μορφή ηλεκτρονικής υπογραφής με την έννοια του Προεδρικού Διατάγματος και της Οδηγίας. Το ένα και μοναδικό κλειδί κρυπτογράφησης αποτελεί εκείνα τα δεδομένα σε ηλεκτρονική μορφή, τα οποία συσχετίζονται λογικά με τα δεδομένα που απαρτίζουν τη δήλωση βουλήσεως και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητάς τους. [36,σελ.179]

3.5.3 Η ασύμμετρη κρυπτογραφία

Τη χαρακτηριστική περίπτωση ηλεκτρονικής υπογραφής αποτελεί η μέθοδος ασύμμετρης κρυπτογράφησης. Τόσο ο κοινοτικός όσο και ο εθνικός νομοθέτης κατά τη ρύθμιση του νομικού

πλαισίου για την ηλεκτρονική υπογραφή είχαν σαν βασικό πρότυπο τη μέθοδο ασύμμετρης κρυπτογράφησης με τη διαδικασία RSA. Τόσο το δημόσιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση, όσο και το ιδιωτικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση, αποτελούν τα δεδομένα σε ηλεκτρονική μορφή, τα οποία συσχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα δηλ. το ηλεκτρονικό έγγραφο και τα οποία χρησιμεύουν ως μέθοδος απόδειξης γνησιότητας του εγγράφου.

Η μέθοδος ασύμμετρης κρυπτογράφησης ωστόσο εμπίπτει και στην ειδικότερη έννοια της προηγμένης ηλεκτρονικής υπογραφής, σύμφωνα με το άρθρο 2, παράγρ.2 του π.δ. [36,σελ.179]

Κεφάλαιο 4

4.1 Ψηφιακή υπογραφή

4.1.1 Η έννοια της ψηφιακής υπογραφής

Ο όρος ψηφιακή υπογραφή (digital signature) είναι τεχνικός όρος και υποδηλώνει τη συγκεκριμένη μέθοδο ασύμμετρης κρυπτογράφησης των ηλεκτρονικών δεδομένων με τέτοιο τρόπο ώστε να διασφαλίζεται η γνησιότητά τους. [36,σελ.185]

Με τον όρο ψηφιακή υπογραφή, σύμφωνα με το άρθρο 14 παρ.2 του ν.2672/1998, νοείται η υπογραφή, ψηφιακής μορφής, 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 επακόλουθη αλλοίωση των εν λόγω δεδομένων. [8,σελ.110],[23]

Στην Οδηγία 1999/93/ΕΚ για τις ηλεκτρονικές υπογραφές ο ορισμός αυτός δίνεται με τον τίτλο προηγμένη ηλεκτρονική υπογραφή, ενώ τον ίδιο ορισμό υιοθετεί και το προεδρικό διάταγμα 150/2001. Βλέπουμε λοιπόν ότι υπάρχει διάκριση μεταξύ των απλών ηλεκτρονικών υπογραφών και των προηγμένων ηλεκτρονικών υπογραφών ή αλλιώς ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές έχουν αυξημένη τυπική ισχύ και αναπληρώνουν θέση ιδιόχειρης υπογραφής τόσο κατά τις διατάξεις του ουσιαστικού όσο και του δικονομικού δικαίου, εφόσον βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής (άρθρο 3 παρ.1 Π.Δ.150/2001). [8,σελ.111]

Επίσης ο Ν.2672/1998, παράγρ. 19 και 20 του άρθρου 14, κληροδοτούν στους αρμοδίους Υπουργούς, οι οποίοι προτείνουν την έκδοση σχετικού προεδρικού διατάγματος, τον προσδιορισμό των προϋποθέσεων, τον καθορισμό της διαδικασίας έκδοσης, διακίνησης, διαχείρισης και διασφάλισης της ψηφιακής υπογραφής, τις προϋποθέσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, τους τεχνικούς κανόνες για την κατάρτιση, την αποστολή, τη διατήρηση, την αντιγραφή και την αναπαραγωγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εγγύηση της ακεραιότητας, διάθεσης και διατήρησης των πληροφοριών που περιέχονται στο μήνυμα, όπως και κάθε άλλη αναγκαία λεπτομέρεια. Με το ίδιο προεδρικό διάταγμα μπορεί να καθορίζονται και οι κατηγορίες μηνυμάτων τα οποία έχουν ισχύ και χωρίς να φέρουν ψηφιακή υπογραφή.[8,σελ.112], [23]

Με το παραπάνω προεδρικό διάταγμα ή άλλο μεταγενέστερο, που εκδίδεται με πρόταση των ίδιων Υπουργών, μπορεί να επεκτείνεται η διακίνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ των δημοσίων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών και νομικών προσώπων ιδιωτικού δικαίου σε όλες ή ορισμένες από τις κατηγορίες εγγράφων που αναφέρονται στην παρ. 3 του άρθρου 14. Η επέκταση αυτή επιτρέπεται μόνο σε μηνύματα με ψηφιακή υπογραφή, η οποία είναι σύμφωνη με τους όρους που προβλέπονται από το προεδρικό διάταγμα της προηγούμενης παραγράφου (Ν.2672/1998, άρθρο 14 παρ.20). [8,σελ.112], [23]

4.1.2 Η λειτουργία της ψηφιακής υπογραφής

4.1.2.1 Γενική περιγραφή

Με την τεχνική του όρου έννοια ως ψηφιακή υπογραφή νοείται μια μέθοδος τεκμηρίωσης της γνησιότητας ηλεκτρονικών δεδομένων, η οποία βασίζεται στη μέθοδο της ασύμμετρης κρυπτογραφίας με τη χρήση δημοσίου κλειδιού. Κάθε χρήστης ψηφιακής υπογραφής που είναι και αποστολέας των δεδομένων διαθέτει δύο κλειδιά, το ιδιωτικό και το δημόσιο κλειδί. Αυτά τα δύο διαφορετικά κλειδιά αποτελούν ζευγάρι υπό την έννοια ότι δεδομένα τα οποία

κρυπτογραφούνται με το ιδιωτικού κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο δημόσιο κλειδί.

Η σχέση των κλειδιών είναι τέτοια ώστε αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ιδιωτικό κλειδί χρησιμοποιείται από τον αποστολέα των δεδομένων για τη δημιουργία της υπογραφής ενώ το δημόσιο κλειδί χρησιμοποιείται από τον λήπτη για την επαλήθευσή της. Φυσικά το ιδιωτικό κλειδί πρέπει να παραμένει πάντοτε απόρρητο, ενώ το δημόσιο μπορεί να γνωστοποιηθεί σε οποιονδήποτε τρίτο, αφού η μαθηματική συνάρτηση βάσει της οποίας δημιουργείται κάθε ζεύγος κλειδιών διασφαλίζει ότι δεν είναι δυνατόν κανείς να υπολογίσει το ιδιωτικό κλειδί, εφόσον έχει στην κατοχή του το δημόσιο. [36,σελ.186]

Η διαφορά της ασύμμετρης κρυπτογραφίας από τη μέθοδο της ψηφιακής υπογραφής είναι ότι στη διαδικασία δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής περιέχεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού από ένα σύνολο ηλεκτρονικών δεδομένων ανεξαρτήτου μεγέθους παράγεται η σύνοψή του (ή το δακτυλικό του αποτύπωμα), η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το κάθε μήνυμα και το αντιπροσωπεύει απόλυτα.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από τη σύνοψη που δημιουργεί είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι αδύνατη, γιατί ακόμα και αν τα μηνύματα έχουν πανομοιότυπο περιεχόμενο, θα διαφέρει το όνομα του παραλήπτη ή έστω η ημερομηνία και η ώρα αποστολής. Η παραμικρή διαφοροποίηση οδηγεί στο σχηματισμό μιας εντελώς παραλλαγμένης σύνοψης. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά τη μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). [36,σελ.187]

Βεβαίως αντίστοιχα και ο λήπτης του μηνύματος δεν έχει τη δυνατότητα να προβεί σε νόθευση του εγγράφου που έλαβε, γιατί οποιαδήποτε αλλαγή του μηνύματος σημαίνει και τη δημιουργία μιας διαφορετικής σύνοψης, η οποία δε θα ταυτίζεται με αυτή που αποκρυπτογραφείται με το δημόσιο κλειδί του υπογράφοντος και η οποία είχε επισυναφθεί στο γνήσιο μήνυμα. Επιπλέον, ο λήπτης δεν μπορεί να γνωρίζει το ιδιωτικό κλειδί του υπογράφοντος ώστε να κρυπτογραφήσει ξανά τη σύνοψη που προκύπτει μετά την επέμβασή του στο έγγραφο και στη συνέχεια αποκρυπτογραφώντας την με το δημόσιο κλειδί του υπογράφοντος, να επικαλεστεί την προέλευση του αλλοιωμένου εγγράφου από τον τελευταίο. Βλέπουμε δηλαδή ότι η ψηφιακή υπογραφή παρέχει και την ασφάλεια για την αποτροπή της παραποίησης του εγγράφου από τα ίδια τα συμβαλλόμενα μέρη. [36,σελ.188]

Άρα λοιπόν η ψηφιακή υπογραφή είναι η κρυπτογραφημένη σύνοψη με το ιδιωτικό κλειδί του αποστολέα που σε αντίθεση με την ιδιόχειρη υπογραφή, είναι διαφορετική για κάθε μήνυμα που υπογράφει ο δηλών.

Θεωρώντας ως δεδομένο ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει τη σύνοψη του μηνύματος, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί του αποστολέα την ταυτότητα του αποστολέα (αυθεντικότητα των δεδομένων). Δηλαδή η ψηφιακή υπογραφή αποτελεί και μια μέθοδο πιστοποίησης της ταυτότητας του αποστολέα του μηνύματος.

Πρακτικά μια ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί μόνο εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του, π.χ. εάν χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό του κλειδί.

Η χρήση της ψηφιακής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής από τον αποστολέα των δεδομένων και την επαλήθευσή της από τον παραλήπτη.[36,σελ.189]

Πρέπει να γνωρίζουμε φυσικά ότι για τη δημιουργία μίας ψηφιακής υπογραφής πάνω σε συγκεκριμένα ηλεκτρονικά δεδομένα θα πρέπει κάποιος εκτός από τα απαραίτητα κρυπτογραφικά κλειδιά και το αντίστοιχο έγκυρο πιστοποιητικό, να διαθέτει και μια ολοκληρωμένη διάταξη δημιουργίας υπογραφής η οποία να απαρτίζεται από κατάλληλη

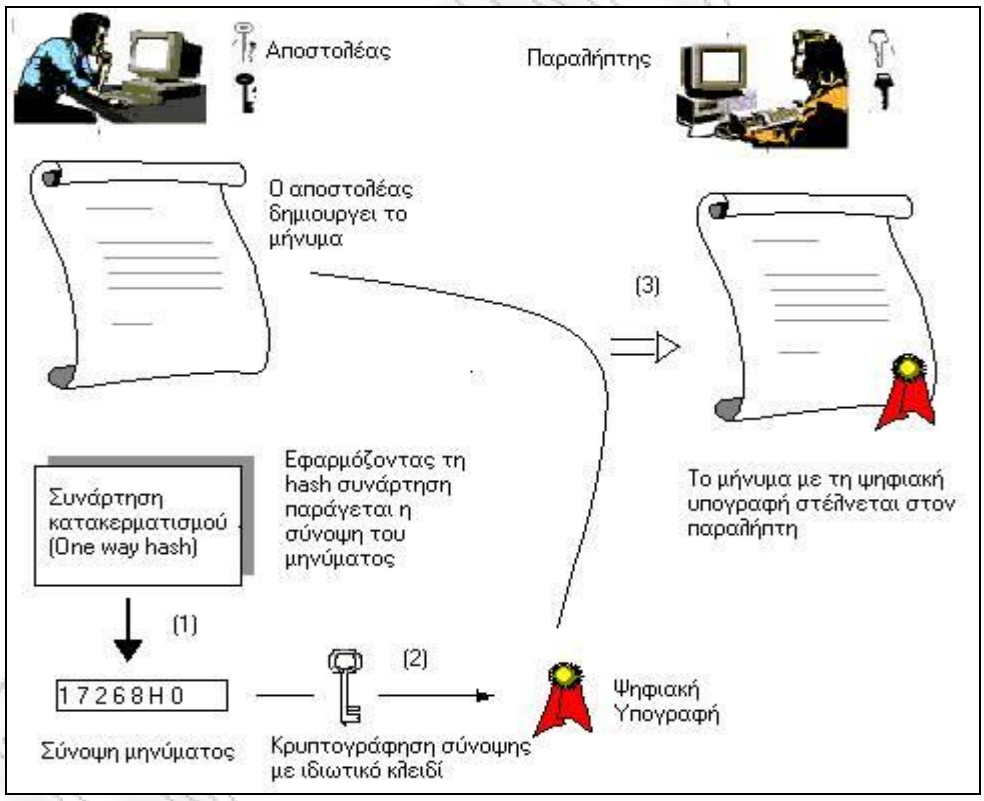
σύνθεση υλικού (hardware) και λογισμικού (software). Στη διάταξη αυτή περιλαμβάνονται ο φορέας των κρυπτογραφικών κλειδιών (π.χ. σκληρός δίσκος υπολογιστή, έξυπνη κάρτα , USB token, κ.λ.π.), ο τυχόν απαραίτητος αναγνώστης του φορέα αυτού (π.χ. αναγνώστης έξυπνης κάρτας , θύρα USB, κ.λπ.), το τερματικό επικοινωνίας του χρήστη (π.χ. PC, pda, smart phone, κ.λπ.), τα λειτουργικά συστήματα και οι οδηγοί (drivers) των συσκευών αυτών, καθώς και το λογισμικό τελικής επικοινωνίας (interface) με τον χρήστη, το οποίο χρησιμοποιείται στην διαδικασία δημιουργίας μιας ηλεκτρονικής υπογραφής.[7]

4.1.2.2 Η δημιουργία της ψηφιακής υπογραφής από τον αποστολέα

1. Ο αποστολέας, αφού ολοκληρώσει τη διατύπωση του μηνύματός του, χρησιμοποιώντας έναν αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος αυτού (message digest) που πρόκειται να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μια συγκεκριμένου μήκους σειρά ψηφίων π.χ. 250AF64R5…-σύνολο 128 ψηφία.

2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη αυτή. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μια πολυπληθής σειρά ψηφίων συγκεκριμένου πλήθους, χωρίς κανένα νοηματικό περιεχόμενο.

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή, το δημόσιο κλειδί και το πιστοποιητικό του αποστολέα διαβιβάζονται μέσω του δικτύου στον παραλήπτη, σχήμα 4.1. [36,σελ.190],[7]



Σχήμα 4.1: Δημιουργία της ψηφιακής υπογραφής από τον αποστολέα

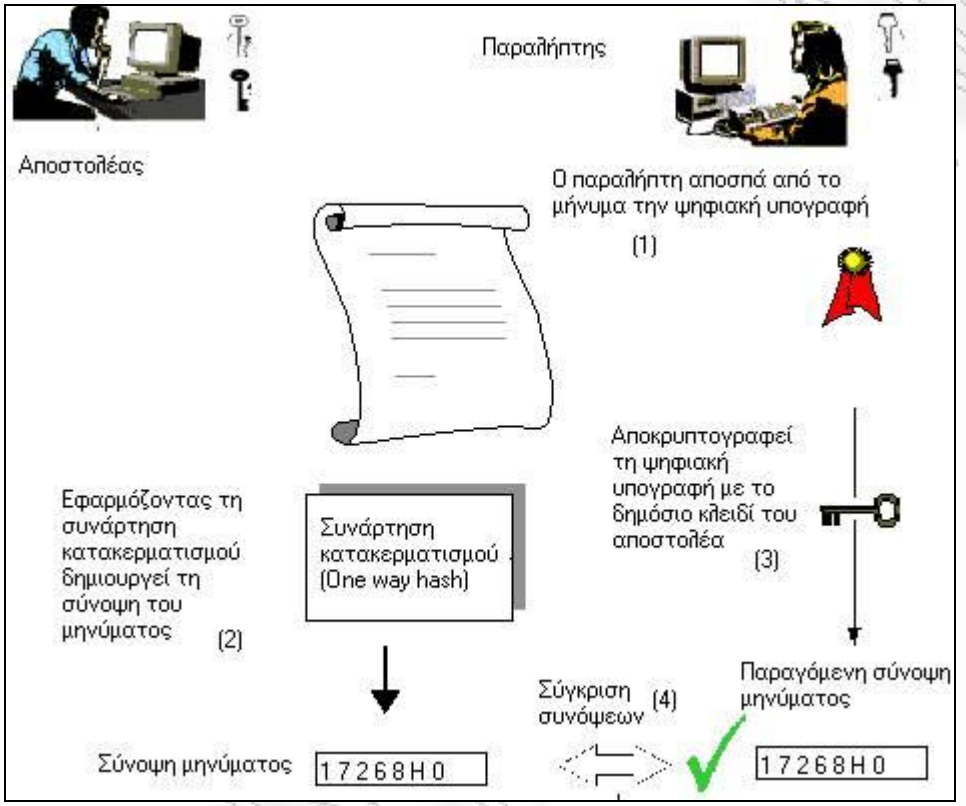
4.1.2.3 Η επαλήθευση της ψηφιακής υπογραφής από τον παραλήπτη

1. Ο παραλήπτης αποσπά από το παραληφθέν μήνυμα την ψηφιακή υπογραφή δηλαδή την 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 δηλαδή την ψηφιακή υπογραφή.

4. Συγκρίνει τις δύο συνόψεις και αν βρεθούν όμοιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο και δεν έχει υποστεί αλλοιώσεις (ακεραιότητα δεδομένων). Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παραγάγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που είχε κρυπτογραφηθεί, σχήμα 4.2. [36,σελ.191],[7]



Σχήμα 4.2: Επαλήθευση της ψηφιακής υπογραφής από τον παραλήπτη

Οι παραπάνω διεργασίες, τόσο της δημιουργίας όσο και της επαλήθευσης γίνονται από το ανάλογο λογισμικό των δύο μερών και διαρκούν ελάχιστα δευτερόλεπτα.

4.2 Ο νομικός χαρακτηρισμός της ψηφιακής υπογραφής

Με όσο αναφέραμε παραπάνω, καταλαβαίνουμε ότι η ψηφιακή υπογραφή παρέχει υψηλότερο βαθμό ασφάλειας απ' ότι οι κοινές ηλεκτρονικές υπογραφές. Η μέθοδος της ψηφιακής υπογραφής ειδικότερα εμπίπτει στον ορισμό του άρθρου 2 παράγρ. 2 της Οδηγίας για την προηγμένη ηλεκτρονική υπογραφή, αποτελεί δηλαδή ηλεκτρονική υπογραφή που πληροί τους παρακάτω όρους του νόμου:

α) Συνδέεται μονοσήμαντα με τον υπογράφοντα: Μόνο ο υπογράφων μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί κρυπτογράφησης που του έχει αποδοθεί. Ο υπογράφων είναι ο υπεύθυνος για να διατηρεί απόρρητα τόσο το συγκεκριμένο αλγόριθμο όσο και τον κωδικό αριθμό που του εξασφαλίζει την πρόσβαση σε αυτόν (άρθρο 4 παρ. 2 του Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικών Υπογραφών). Σε περίπτωση μάλιστα διαρροής του μυστικού αριθμού ο υπογράφων είναι αυτός που έχει την υποχρέωση να ειδοποιήσει τον έμπιστο τρίτο εκδότη του σχετικού πιστοποιητικού (άρθρο 4 παρ. 3 του Κανονισμού).

β) Είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος: η μέθοδος RSA που βασίζεται στην υποδομή δημοσίου κλειδιού είναι πράγματι ικανή να καθορίσει αξιόπιστα την ταυτότητα του υπογράφοντος. Εφόσον τα συγκεκριμένα δεδομένα είναι

δυνατό να αποκρυπτογραφηθούν με το δημόσιο κλειδί του υπογράφοντος, είναι μαθηματικώς βέβαιο ότι η κρυπτογράφηση έχει γίνει με το αντίστοιχο σε αυτό ιδιωτικό κλειδί του. Στο πιστοποιητικό λοιπόν που αντιστοιχεί στο δημόσιο κλειδί, με το οποίο έγινε η κρυπτογράφηση, βεβαιώνει ο εκδότης του ότι ο αποκλειστικός κάτοχος του αντιστοιχούντος ιδιωτικού κλειδιού είναι ο υπογράφων (άρθρο 4 παρ. 2 του Κανονισμού). Επιπλέον στο πιστοποιητικό αναφέρονται τα στοιχεία της ταυτότητας του προσώπου αυτού ή το ψευδώνυμο με το οποίο έχει επιλέξει να εμφανίζεται, τα οποία στοιχεία βεβαιώνει υπεύθυνα ο εκδότης.

γ) Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο: Το μυστικό κλειδί, δηλαδή ο αλγόριθμος, με το οποίο κρυπτογραφούνται τα δεδομένα συνηθίζεται να αποθηκεύονται σε μια έξυπνη κάρτα (chip card) και μάλιστα η πρόσβαση στον αλγόριθμο από τον κάτοχο της κάρτας είναι εφικτή μόνο εφόσον εισαγάγει έναν κωδικό αριθμό αναγνώρισης PIN.

δ) Συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των δεδομένων: Σε περίπτωση που μετά τη ψηφιακή υπογραφή των δεδομένων, δηλαδή την κρυπτογράφηση της σύνοψής τους, γίνει κάποια αλλοίωση σε αυτά, η σύνοψη που θα προκύψει από τη διαδικασία αποκρυπτογράφησης δε θα συμπίπτει με τη σύνοψη δεδομένων που βρίσκονται στα χέρια του λήπτη. Η διαφορά των δύο αυτών συνόψεων θα μαρτυρεί αυτή τη μεταγενέστερη αλλοίωση των δεδομένων και θα συνεπάγεται τη μη επαλήθευση της ψηφιακής υπογραφής.

Από τα παραπάνω γίνεται φανερό ότι η διαδικασία της ασύμμετρης κρυπτογράφησης υπάγεται στην έννοια της προηγμένης ηλεκτρονικής υπογραφής, όπως αυτή ορίζεται στο άρθρο 2 παράγρ. 2 του Π.Δ.150/2001 και της Οδηγίας 99/93/ΕΚ. Ο κοινοτικός νομοθέτης ωστόσο επέλεξε να διατυπώσει τον ορισμό της προηγμένης ηλεκτρονικής υπογραφής κατά τέτοιο τρόπο ώστε να φωτογραφίζει μεν τη συγκεκριμένη μέθοδο, πλην όμως να αφήνει περιθώρια υπαγωγής σε αυτόν νεότερων ανάλογων τεχνικών που μπορεί να αναπτυχθούν στο μέλλον. [36,σελ.196-198]

4.3 Σύγκριση ψηφιακών και χειρόγραφων υπογραφών

Η ψηφιακή υπογραφή υπηρετεί τους ίδιους σκοπούς ύπαρξης με αυτούς της ιδιόχειρης. Παρόλα αυτά, υπάρχουν μεταξύ τους διαφοροποιήσεις όπως φαίνεται στον πίνακα 4.1:

Ιδιόχειρη υπογραφή	Ψηφιακή υπογραφή
Χρησιμοποιείται η ίδια υπογραφή για κάθε σκοπό	Χρησιμοποιείται διαφορετική υπογραφή για κάθε σκοπό
Δυνατή η πλαστογράφηση	Η πλαστογράφηση είναι σχεδόν αδύνατη
Ευκολία στην αλλοίωση του περιεχομένου του εγγράφου	Δύσκολη η τροποποίηση των δεδομένων
Ευκολία για τη δημιουργία της	Απαιτείται ειδικό λογισμικό για να δημιουργηθεί
Η διαδικασία ελέγχου γίνεται μόνο σε περίπτωση διαφωνίας	Η επαλήθευσή της είναι υποχρεωτική
Ο υπογράφων πρέπει να παρίσταται ο ίδιος προσωπικά	Κάτι τέτοιο δεν απαιτείται

Πίνακας 4.1: Σύγκριση ιδιόχειρης και ψηφιακής υπογραφής

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

Στη χώρα μας, κατόπιν της Οδηγίας 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, εκδόθηκε το προεδρικό διάταγμα 150/2001 σχετικά με τις ψηφιακές υπογραφές, όπου σύμφωνα με αυτό οι ψηφιακές υπογραφές αναγνωρίζονται ως ισότιμες με τις ιδιόχειρες.

Κεφάλαιο 5

5.1 Υποδομή Δημόσιου Κλειδιού- PKI

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο ενώ παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Η Υποδομή Δημόσιου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση της PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες, εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Οι βασικές λειτουργίες και υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι:

- **Εμπιστευτικότητα (Confidentiality):** Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).
- **Ακεραιότητα (Integrity):** Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.
- **Μη Άρνηση Αποδοχής (Non-Repudiation):** Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. 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 (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 ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι είτε με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας, είτε με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας όπως μια τραπεζική κάρτα, είτε με δακτυλικά αποτυπώματα. [42]

5.2 Ο ρόλος του Παροχέα Υπηρεσιών Πιστοποίησης

Η δυνατότητα αποκρυπτογράφησης της ηλεκτρονικής υπογραφής του αποστολέα με το δημόσιο κλειδί που έχει στη διάθεσή του ο λήπτης, δημιουργεί βεβαιότητα ότι τα δεδομένα προέρχονται από τον τελευταίο. Και αυτό γιατί το δημόσιο κλειδί που έλαβε ο λήπτης από τον αποστολέα αποτελεί τη μοναδική δυνατότητα αποκρυπτογράφησης των δεδομένων και συγχρόνως καθιστά σαφές ότι τα δεδομένα κρυπτογραφήθηκαν με το μυστικό κλειδί του αποστολέα. Επίσης η ταύτιση των δύο συνόψεων βεβαιώνει το αναλλοίωτο των δεδομένων.

Όμως πρέπει με κάποιον τρόπο να διασφαλιστεί ότι το δημόσιο κλειδί που διαβιβάστηκε στον λήπτη ανήκει πραγματικά σε αυτόν που φέρεται ως συμβαλλόμενο μέρος και όχι σε κάποιον τρίτο που οικειοποιείται την ταυτότητά του. Επιπλέον, θα πρέπει να είναι δυνατή η πιστοποίηση με αντικειμενικό τρόπο ότι η ακολουθούμενη διαδικασία της ψηφιακής υπογραφής και επαλήθευσής της ανταποκρίνονται πράγματι στις προδιαγραφές ενός ασφαλούς ασύμμετρου συστήματος κρυπτογράφησης, όπως αυτές τίθενται στο π.δ. 150/2001. Π.χ. ότι το

ιδιωτικό και το δημόσιο κλειδί συνδέονται πράγματι με μια μονόδρομη συνάρτηση και το ιδιωτικό κλειδί είναι μοναδικό και μπορεί να διατηρηθεί απόρρητο.

Έτσι τις παραπάνω λειτουργίες πιστοποίησης αναλαμβάνει να προσφέρει ένα τρίτο ανεξάρτητο πρόσωπο. Πρόκειται για τον ονομαζόμενο Παροχέα Υπηρεσιών Πιστοποίησης (Certification Service Provider). Οι Πάροχοι Υπηρεσιών Πιστοποίησης- ΠΥΠ αναφέρονται συχνά στην ελληνική και διεθνή βιβλιογραφία και ως Έμπιστοι Τρίτοι Φορείς ή Έμπιστες Τρίτες Οντότητες (Trusted Third Parties - TTP) ή Αρχές Πιστοποίησης (Certification Authorities - CA).

Κύριο αντικείμενο της δραστηριότητάς του είναι η έκδοση πιστοποιητικού ηλεκτρονικής υπογραφής. Το πιστοποιητικό αυτό, σύμφωνα το άρθρο 2 παράγρ. 9 του π.δ. 150/2001, είναι μια βεβαίωση σε ηλεκτρονική μορφή, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής π.χ ένα δημόσιο κλειδί, με ένα άτομο και επιβεβαιώνει την ταυτότητα του. Η βεβαίωση αυτή αποστέλλεται ως συνημμένη στο ψηφιακό υπογεγραμμένο μήνυμα ενώ και μετά τη λήψη της είναι δυνατή η επιβεβαίωση της ισχύος της αυτόματα δια της επικοινωνίας του Η/Υ του λήπτη με τον επί 24ώρου βάσεως διαθέσιμο Η/Υ του Παροχέα. Με τον τρόπο αυτό εξασφαλίζεται επιπλέον ότι το πιστοποιητικό δεν έχει ανακληθεί. [36,σελ.193-194]

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι ένας ουδέτερος οργανισμός που εμπνέει επιχειρηματική εμπιστοσύνη σε μια ηλεκτρονική συναλλαγή και εμπλέκεται στη διαδικασία έκδοσης και πιστοποίησης των ψηφιακών υπογραφών. Ο Πάροχος Υπηρεσιών Πιστοποίησης θα πρέπει:

- να τηρεί αρχείο με τα δημόσια κλειδιά των πιστοποιημένων οντοτήτων, έτσι ώστε να μπορεί να έχει πρόσβαση σ' αυτά ο κάθε ενδιαφερόμενος.
- να πιστοποιεί την ταυτότητα των χρηστών πριν τους εκδώσει την ψηφιακή υπογραφή καθώς και να τηρεί αρχείο με τις ψηφιακές υπογραφές που έχουν λήξει ή που έχουν ανακληθεί ώστε να μην μπορούν να χρησιμοποιηθούν μετά τη λήξη τους ή και για λόγους κλοπής ή απώλειας. Το κόστος μιας τέτοιας υπηρεσίας είναι ανάλογο μ' αυτό μιας συνδρομής σε μια πιστωτική κάρτα.
- να είναι ένας τρίτος, ουδέτερος οργανισμός που να μη συμμετέχει με κανέναν τρόπο στη συναλλαγή και να εμπνέει επιχειρηματική εμπιστοσύνη στις ηλεκτρονικές συναλλαγές (αρχή της τριτότητας (thirdness).

Σχετική νομοθεσία για τη λειτουργία των Παρόχων Υπηρεσιών Πιστοποίησης είναι ο Κανονισμός 248/71/2002 της Ε.Ε.Τ.Τ. (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων), που δημοσιεύθηκε στο ΦΕΚ 603/Β'/16-5-2002, με τον τίτλο «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής».

Η ευθύνη ενός Παρόχου Υπηρεσιών Πιστοποίησης αφορά την ακρίβεια όλων των πληροφοριών που περιέχονται στα πιστοποιητικά που εκδίδει, τη διαβεβαίωση ότι ο υπογράφων είναι όντως κάτοχος του ιδιωτικού κλειδιού, τη δημόσια ανακοίνωση της ανάκλησης ή της λήξης ενός πιστοποιητικού κ.ά. Οι εταιρείες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ηλεκτρονικής υπογραφής ελέγχονται από την Ε.Ε.Τ.Τ., η οποία έχει την εποπτεία και τον έλεγχο όλων των Παρόχων Υπηρεσιών Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα και επιβάλλει πρόστιμα σ' όσους Παρόχους ενεργούν ως διαπιστευμένοι χωρίς να είναι.

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, για την έκδοση, διάθεση και διαχείριση των σχετικών πιστοποιητικών. Κατά συνέπεια, οι ΠΥΠ επιβάλλεται να προσφέρουν μια σειρά από υπηρεσίες που δεν περιορίζονται μόνο στην έκδοση του πιστοποιητικού, αλλά αφορούν τον κύκλο ζωής του. Οι υπηρεσίες αυτές διασφαλίζονται μέσα στα πλαίσια του ΠΥΠ από τις εξής υπηρεσίες:

- **Υπηρεσία Εγγραφής (Registration Authority):** Παραλαμβάνει τις αιτήσεις και τα δικαιολογητικά για την έκδοση του πιστοποιητικού και είναι υπεύθυνη για τη συλλογή των πληροφοριών που αποτελούν το απαραίτητο περιεχόμενο του πιστοποιητικού. Τις πληροφορίες αυτές, που είναι απαραίτητες για την ταυτοποίηση του κατόχου των δεδομένων δημιουργίας με τον αιτούντα το πιστοποιητικό, τις μεταβιβάζει στη συνέχεια στην Υπηρεσία Έκδοσης των πιστοποιητικών.
- **Υπηρεσία Έκδοσης Πιστοποιητικών (Certification Authority):** Εκδίδει το πιστοποιητικό σύμφωνα με τη Δήλωση Πρακτικής Πιστοποίησης.

- **Υπηρεσία Δημοσίευσης και Διανομής (Dissemination Service):** Δημοσιεύει τον κατάλογο με τα εκδοθέντα πιστοποιητικά, τους ιδιαίτερους όρους χρήσης του κάθε είδους πιστοποιητικού (Πολιτικές Πιστοποιητικών) καθώς και τη Δήλωση Πρακτικής Πιστοποίησης, με τρόπο που να τις καθιστά προσβάσιμες σε κάθε ενδιαφερόμενο.
- **Υπηρεσία Διαχείρισης και Δημοσίευσης Ανάκλησης (Revocation Management and Status Service):** Διαχειρίζεται τον κατάλογο με τα εκδοθέντα πιστοποιητικά. Δέχεται και ελέγχει αιτήματα ανάκλησης ή παύσης των πιστοποιητικών και προβαίνει στην έγκαιρη ενημέρωση της Λίστας Ανακληθέντων Πιστοποιητικών.

Προαιρετικά ένας ΠΥΠ μπορεί να παρέχει και τις εξής υπηρεσίες:

- **Υπηρεσίες Χρονοσήμανσης (Time Stamping Authority)** των εγγράφων, ύστερα από αίτηση των συνδρομητών.
- **Υπηρεσίες Προμήθειας Συσκευών Δημιουργίας Υπογραφής (Device Provision Service):** Παρέχουν στο συνδρομητή το ιδιωτικό του κλειδί, συνήθως υπό τη μορφή μιας έξυπνης κάρτας.

Οι παραπάνω υπηρεσίες μπορούν να παρέχονται άμεσα από τον ίδιο τον εκδότη των πιστοποιητικών ή από εξουσιοδοτημένους συνεργάτες του. Στη δεύτερη περίπτωση, ο εκδότης παραμένει αποκλειστικά υπεύθυνος έναντι των δικαιούχων πιστοποιητικών ή τρίτων για πράξεις ή παραλήψεις των αναδόχων του. Στην συνέχεια, ο εκδότης μπορεί να στραφεί κατά των εξουσιοδοτημένων συνεργατών του, σύμφωνα με τους προβλεπόμενους όρους του συμβολαίου που τους συνδέει, οι οποίοι και θα πρέπει να χρήζουν ιδιαίτερης προσοχής.

5.2.1 Πάροχοι Υπηρεσιών Πιστοποίησης στην Ελλάδα

Σύμφωνα με την υπ' αρ. 248/71 Απόφαση της ΕΕΤΤ "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής" (ΦΕΚ 603/Β'/16-5-2002)[40] η ΕΕΤΤ τηρεί Μητρώο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης. Σύμφωνα με τον Κανονισμό αυτόν, όλοι οι Πάροχοι Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής που είναι εγκατεστημένοι στην Ελλάδα υποχρεούνται να δηλώσουν τα στοιχεία τους και τις υπηρεσίες που παρέχουν. Η καταχώρηση ή αλλαγή ή παύση των υπηρεσιών ενός Παρόχου στο Μητρώο της ΕΕΤΤ, καθώς και η περιγραφή των υπηρεσιών πιστοποίησης που παρέχει, πραγματοποιείται με μια δήλωση καταχώρησης που συμπληρώνει και αποστέλλει υπογεγραμμένη και σφραγισμένη στην ΕΕΤΤ. Η καταχώρηση ενός Παρόχου στο Μητρώο της ΕΕΤΤ ως Παρόχου, ο οποίος εκδίδει Αναγνωρισμένα πιστοποιητικά, όπως αυτά ορίζονται στο Π.Δ. 150/2001, βασίζεται μόνο στη δική του δήλωση ότι εκδίδει Αναγνωρισμένα Πιστοποιητικά.[43]

Ενδεικτικά, μερικοί από τους Παρόχους Υπηρεσιών Πιστοποίησης σύμφωνα με αυτούς που αναγράφονται στο Μητρώο Παρόχων Υπηρεσιών Πιστοποίηση της ΕΕΤΤ είναι οι εξής:

Η ADACOM A.E., μέλος του Ομίλου IDEAL, παρέχει υπηρεσίες ψηφιακής πιστοποίησης και γενικότερα ασφάλειας πληροφοριακών συστημάτων που έχουν ως βάση την τεχνολογική πλατφόρμα της VeriSign (οδηγός παγκοσμίως της αγοράς των υπηρεσιών Δημοσίου Κλειδιού). Έχοντας πραγματοποιήσει τη μεγαλύτερη σε μέγεθος επένδυση στα Βαλκάνια για τη δημιουργία Υποδομής Δημοσίου Κλειδιού (PKI) η ADACOM είναι Πάροχος Υπηρεσιών Πιστοποίησης προς τελικούς χρήστες, προς νομικά πρόσωπα τα οποία επιθυμούν να λειτουργήσουν ως Αρχές Πιστοποίησης, καθώς και προς εξυπηρετητές (servers) και δικτυακές συσκευές. Οι υπηρεσίες αυτές υλοποιούνται είτε με τη χρησιμοποίηση ιδιωτικής ιεραρχίας της ADACOM, η οποία χρησιμοποιείται για την έκδοση αναγνωρισμένων πιστοποιητικών σύμφωνα με την Ευρωπαϊκή Οδηγία, είτε είναι ενταγμένες στη δημόσια ιεραρχία της VeriSign η οποία εξασφαλίζει τη μεγαλύτερη δυνατή αναγνωρισιμότητα από τους web browsers. Παράλληλα παρέχεται ένα σύνολο σχετικών υπηρεσιών όπως Διαχείριση Ιδιωτικών Κλειδιών Κρυπτογράφησης, Χρονοσήμανσης και O.C.S.P. (Online Certificate Status Protocol).[28] Η εταιρεία έχει υλοποιήσει ποικίλα έργα PKI τόσο στην Ελλάδα όσο και στο εξωτερικό (π.χ. Ρουμανία), ακολουθώντας τα σημαντικότερα σχετικά ευρωπαϊκά και διεθνή πρότυπα. Η ADACOM είναι πιστοποιημένη κατά ISO 9002/94. [1],[31], [29]

Η Τράπεζα EFG Eurobank Ergasias ΑΕ δημιουργεί και υποστηρίζει υπηρεσίες e-banking και m-banking, οι οποίες καλύπτουν ένα ευρύ φάσμα τραπεζικών υπηρεσιών, όπως από ανάγκες απλής ενημέρωσης για τις κινήσεις και το υπόλοιπο των λογαριασμών και των πιστωτικών καρτών, έως και την πληρωμή καρτών και διαφόρων λογαριασμών π.χ. ΔΕΗ, ΟΤΕ κτλ. Η έκδοση πιστοποιητικών ταυτοποίησης από την Eurobank παρέχει την δυνατότητα για εξελιγμένο έλεγχο της πρόσβασης των χρηστών στο σύστημα και τις ηλεκτρονικές υπηρεσίες του Ομίλου (user authentication /authorization), ενώ εισάγεται η δυνατότητα της χρήσης ηλεκτρονικής υπογραφής ως απόδειξης της βούλησης για την διενέργεια κρίσιμων συναλλαγών. Η υποδομή της Eurobank, αν και έχει την δυνατότητα, δεν εκδίδει αναγνωρισμένα πιστοποιητικά, μιας και η χρήση των εκδιδόμενων πιστοποιητικών προορίζεται προς το παρόν αποκλειστικά σε κλειστές εφαρμογές για τις οποίες δεν εφαρμόζεται η Οδηγία 99/93/ΕΚ (η αποδοχή της χρήσης ηλεκτρονικών υπογραφών στηρίζεται σε συμβατικούς όρους).[1],[44]

Το Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών- ΕΒΕΑ έχει δημιουργήσει και λειτουργεί δική του υποδομή PKI με σκοπό να παρέχει σχετικές υπηρεσίες και να εκδίδει ηλεκτρονικά πιστοποιητικά δημοσίων κλειδιών στα μέλη του.[1], [30]

Η Α.Σ.Υ.Κ. Α.Ε. (Ανάπτυξη Συστημάτων και Υποστήριξης Κεφαλαιαγοράς), μέλος του Ομίλου Ε.Χ.Α.Ε. (Ελληνικά Χρηματιστήρια Ανώνυμη Εταιρεία) και υπεύθυνη για την ανάπτυξη και ολοκληρωμένη τεχνική διαχείριση, λειτουργία και υποστήριξη των υποδομών πληροφορικής και επικοινωνιών του Χρηματιστηρίου Αθηνών (Χ.Α.) και του Ομίλου ΕΧΑΕ γενικότερα, δημιούργησε δική της Υποδομή Δημοσίου Κλειδιού για να καλύψει τις ανάγκες του Χ.Α. για ασφαλή και νομικά έγκυρη ηλεκτρονική επικοινωνία - αλληλογραφία με τις εισηγμένες σ' αυτό εταιρίες, αντικαθιστώντας τα συμβατικά έγγραφα με αντίστοιχα ηλεκτρονικά, τα οποία αποστέλλονται ψηφιακά υπογεγραμμένα μέσω του συστήματος H.E.R.ME.S. (Hellenic Exchanges Remote Messaging Services), ένα σύστημα ηλεκτρονικής διασύνδεσης και επικοινωνίας του ΧΑ με τις εισηγμένες εταιρίες μέσω του Διαδικτύου.[1], [45]

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου η οποία εκδίδει ψηφιακά πιστοποιητικά σε δημοσίους υπαλλήλους με μορφή κάρτας αλλά και σε πολίτες όπως θα δείξουμε αναλυτικά στο Β' μέρος της εργασίας μας, κεφάλαιο 8.

5.3 Πιστοποιητικά δημοσίου κλειδιού

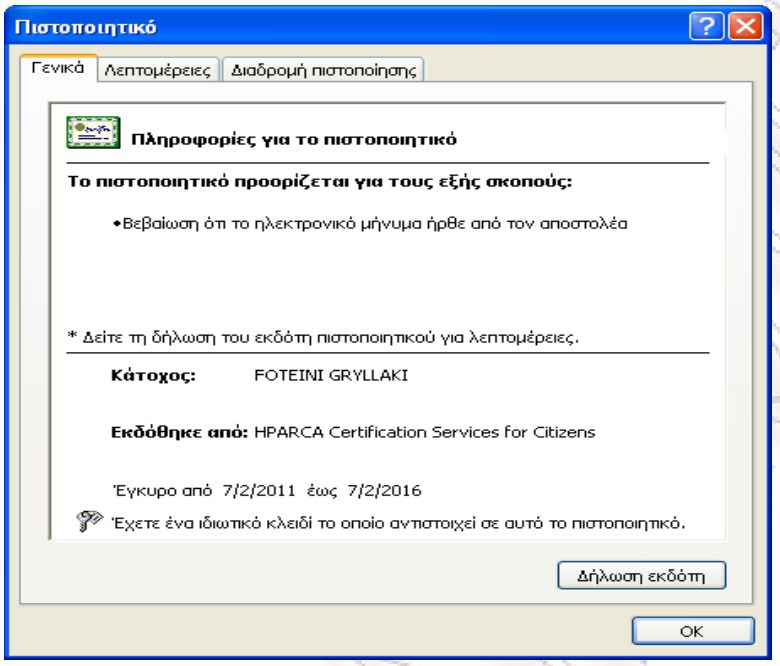
Με τη λήψη ενός μηνύματος που περιέχει ηλεκτρονική υπογραφή, ο παραλήπτης μπορεί επαληθεύοντας την ηλεκτρονική υπογραφή να είναι σίγουρος ότι το μήνυμα είναι ακέραιο. Για την επαλήθευση της ηλεκτρονικής υπογραφής, ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί, ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε, άρα επιτυγχάνεται η μη αποκήρυξη.

Επομένως αυτό που μένει να διασφαλιστεί είναι 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. Δηλαδή, απαιτείται η ύπαρξη ενός μηχανισμού τέτοιου ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί. Σε ένα περιβάλλον Υποδομής Δημοσίου Κλειδιού, οι παραπάνω προϋποθέσεις πληρούνται με τη χρήση των ψηφιακών πιστοποιητικών ή αλλιώς πιστοποιητικά δημοσίου κλειδιού (Public Key Certificate - PKC). Όπως έχουμε αναφέρει και παραπάνω, τα ψηφιακά πιστοποιητικά εκδίδονται από μία Αρχή Πιστοποίησης.

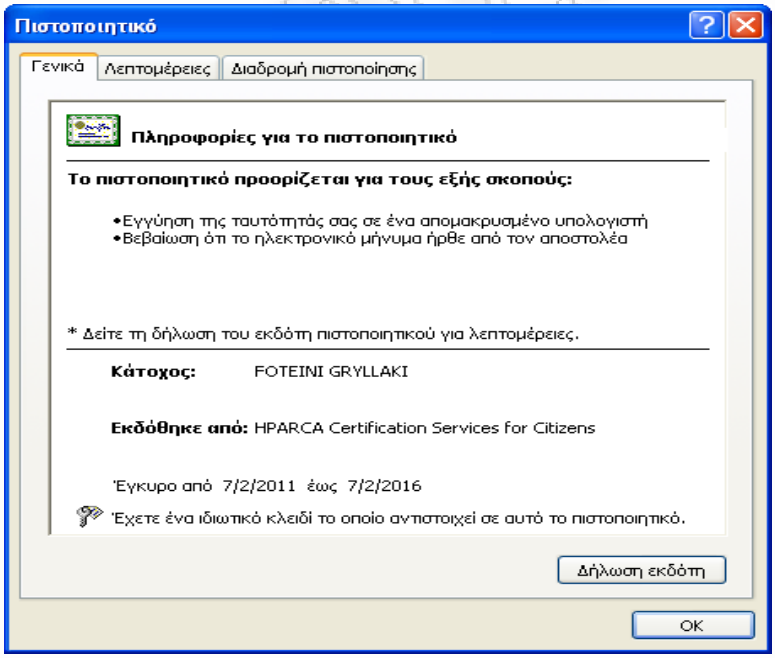
Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και βεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει, αλλά και ότι τα στοιχεία της ταυτότητας του προσώπου αυτού είναι ακριβή.[36 σελ.194]

Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε και περιέχει μια ποικιλία πληροφοριών, συμπεριλαμβανομένων της επωνυμίας του κατόχου, του δημοσίου κλειδιού, της ημερομηνίας λήξης του πιστοποιητικού, των λειτουργιών που πρέπει να εκτελέσει το δημόσιο κλειδί (κρυπτογράφηση, αποκρυπτογράφηση ή επαλήθευση ψηφιακής υπογραφής), της ψηφιακής υπογραφής του εκδότη, του σειριακού του αριθμού και της μεθόδου κρυπτογράφησης.[42]

Παράδειγμα προβολής ενός πιστοποιητικού δημοσίου κλειδιού απεικονίζεται στις εικόνες 5.1 και 5.2 παρακάτω, όπου ο κάτοχος του πιστοποιητικού είναι η Γρυλλάκη Φωτεινή, εκδόθηκε από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου και έχει ισχύ για πέντε χρόνια έως το 2016.



Εικόνα 5.1: Πιστοποιητικό Δημοσίου Κλειδιού για κρυπτογράφηση μηνύματος



Εικόνα 5.2: Πιστοποιητικό Δημοσίου Κλειδιού για εισαγωγή ψηφιακής υπογραφής σε μήνυμα

Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του, τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο, δημόσιο κλειδί, ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λ.π. [7]

Τη γνησιότητα των πιστοποιητικών εγγυώνται διεθνώς αναγνωρισμένες εταιρείες, πάροχοι ψηφιακών πιστοποιητικών, όπως η Verisign (βλέπε Παράρτημα 2) και η Αρχή Πιστοποίησης Ελληνικού Δημοσίου. Υπάρχουν διάφορα πρότυπα για τη σύνταξη ενός πιστοποιητικού, καθένα από τα οποία έχουν και διαφορετική δομή. Το πιο διαδεδομένο διεθνώς πρότυπο είναι το X.509 το οποίο αποτελεί Σύσταση της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU).

5.3.1 Πρότυπο X.509

Το 1988, η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunications Union- ITU) πρότεινε το πρότυπο X.509 για ψηφιακά πιστοποιητικά. Από τότε, το X.509 έχει γίνει πρότυπο για την πιστοποίηση χρηστών σε ανοιχτά συστήματα όπως το Internet.

Το πρότυπο X.509 διαθέτει αρκετά προκαθορισμένα πεδία για την αναγραφή των απαραίτητων πληροφοριών (έναν αριθμό έκδοσης, έναν σειριακό αριθμό, πληροφορίες ταυτότητας, πληροφορίες σχετικές με τον αλγόριθμο και την υπογραφή της αρχής που το εκδίδει). Το πρότυπο X.509 για ψηφιακά πιστοποιητικά έχει παρουσιαστεί σε τρεις εκδόσεις.

Η τρίτη και τελευταία έκδοση, η X509 v3, η οποία είναι και η περισσότερο εφαρμόσιμη, παρέχει τη δυνατότητα να συμπεριλάβει και επιπλέον εκτεταμένα πεδία (extensions) στο πιστοποιητικό δηλαδή πρόσθετα χαρακτηριστικά ανάλογα με την εφαρμογή που πρέπει να υλοποιηθεί, και τα οποία καθορίζονται από τον Εκδότη των πιστοποιητικών. Τα X.509v3 πιστοποιητικά είναι ευρέως χρησιμοποιημένα από πολλά μοντέρνα κρυπτογραφικά πρωτόκολλα όπως το SSL [19,σελ.280]. Στον πίνανα 5.1 παρουσιάζεται η γενική δομή ενός ψηφιακού πιστοποιητικού σύμφωνα με το π.δ.150/2001, και του τύπου X509 v3.

Πεδίο
Έκδοση (Version)
Αριθμός Σειράς (Serial Number)
Αλγόριθμος Υπογραφής (Signature Algorithm)
Διακριτικό Όνομα Εκδότη (Issuer DN)
Ισχύει Από (Valid From)
Ισχύει Μέχρι (Valid To)
Διακριτικό Όνομα Υποκειμένου (Subject DN)
Δημόσιο Κλειδί Υποκειμένου (Subject Public Key)
Υπογραφή (Signature)

Πίνακας 5.1: Βασικά πεδία ψηφιακού πιστοποιητικού

Όπου:

• Έκδοση (Version): αναφέρεται στην έκδοση του προτύπου X.509 πιστοποιητικών και υποστηρίζει εκτεταμένα πεδία.

• Αριθμός Σειράς (Serial Number): αποτελείται από το μοναδικό αριθμό του εκδιδόμενου πιστοποιητικού, ο οποίος καθορίζεται από τον εκδότη των πιστοποιητικών με σκοπό τη διάκριση του πιστοποιητικού.

• Αλγόριθμός Υπογραφής (Signature Algorithm): αναφέρεται στον αλγόριθμό σύνοψης (Hash Function). Προτείνεται η αξιοποίηση του SHA-1.

• Διακριτικό Όνομα Εκδότη (Issuer DN): αναφέρεται στο όνομα του εκδότη του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά.

• Ισχύει Από (Valid From): περιλαμβάνει την ημερομηνία έκδοσης του πιστοποιητικού.

• Ισχύει Μέχρι (Valid To): περιλαμβάνει την ημερομηνία λήξης του πιστοποιητικού.

• Διακριτικό Όνομα Υποκειμένου (Subject DN): Αναφέρεται στον κάτοχο του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά.

• Δημόσιο Κλειδί Υποκειμένου (Subject Public Key): αποτελείται από το Δημόσιο Κλειδί του Υποκειμένου δηλαδή του ιδιοκτήτη του ψηφιακού πιστοποιητικού.

• Υπογραφή (Signature): αποτελείται από την ψηφιακή υπογραφή του εκδότη του ψηφιακού πιστοποιητικού.

Οι επεκτάσεις των ψηφιακών πιστοποιητικών μπορεί να είναι:

• Χρήση Κλειδιού (Key Usage): αναφέρεται ποια θα είναι η χρήση του δημόσιου κλειδιού που περιλαμβάνεται στο ψηφιακό πιστοποιητικό.

• Εναλλακτικό Όνομα Υποκειμένου (Subject Alternative Name): περιλαμβάνεται ένα εναλλακτικό όνομα για τον κάτοχο του ψηφιακού πιστοποιητικού. Δεδομένης της ταυτόχρονης ύπαρξης του πεδίου Διακριτικό Όνομα Υποκειμένου (Subject DN), στο παρόν πεδίο θα περιληφθεί κρυπτογραφημένο το σχετικό αναγνωριστικό του χρήστη που επιθυμεί ο δημόσιος φορέας που προσφέρει την υπηρεσία (π.χ. ΑΦΜ). Η κρυπτογράφηση θα γίνεται με το δημόσιο κλειδί του φορέα που θα τα αξιοποιεί, ώστε να μπορούν να αποκρυπτογραφηθούν μόνον από τον συγκεκριμένο φορέα. Στην περίπτωση που το ίδιο αναγνωριστικό απαιτείται από περισσότερους από ένα φορείς, τότε θα πρέπει να κρυπτογραφηθεί για κάθε φορέα ξεχωριστά.

• Ταυτοποίηση Χρήστη (Clientauth): αναφέρει εάν το συγκεκριμένο πιστοποιητικό μπορεί να χρησιμοποιηθεί για την ταυτοποίηση του χρήστη.

• Σημεία Διανομής Καταλόγου Ανακληθέντων Πιστοποιητικών (CRL distribution List): αναφέρονται τα σημεία διανομής της Λίστας Ανακληθέντων Πιστοποιητικών, σε μορφή URL διεύθυνσης.

• Πολιτικές Πιστοποιητικού (Certificate Policies): αναφέρεται το σημείο εύρεσης του κειμένου των Πολιτικών που διέπουν το ψηφιακό πιστοποιητικό, σε μορφή URL διεύθυνσης.[50]

5.3.2 Είδη πιστοποιητικών δημοσίου κλειδιού

Τα πιστοποιητικά δημοσίου κλειδιού μπορούν να διακριθούν σε αυτά α) που είναι για φυσικά πρόσωπα δηλαδή τα προσωπικά πιστοποιητικά και στα β) πιστοποιητικά δικτυακών τόπων.

Τα προσωπικά πιστοποιητικά (α) αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως το όνομα του χρήστη και ο κωδικός πρόσβασης, όμως μπορούν να περιλαμβάνουν και αναφορά σε συγκεκριμένες πιστοποιημένες ή μη ιδιότητες του υποκειμένου όπως π.χ. το επάγγελμα του. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου

ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

Τα πιστοποιητικά δικτυακών τόπων (β), περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθούμε να συνδεθούμε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Αν οι πληροφορίες αυτές δεν είναι έγκυρες ή αν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα.

Έχουν αναπτυχθεί διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών.Από αυτά σήμερα χρησιμοποιείται το SSL (Secure Socket Layer). Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα πρόσωπα από την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".[42]

5.3.3 Ο έλεγχος του κύρους των ηλεκτρονικών πιστοποιητικών

Λόγω της συνεχής τεχνολογικής εξέλιξης θεωρείται δεδομένη η εξασθένηση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών στο πέρασμα του χρόνου. Έτσι, τα πιστοποιητικά δημοσίου κλειδιού που αναφέρονται αλλά και που υπογράφονται από τέτοια κρυπτογραφικά κλειδιά εκδίδονται με περιορισμένη διάρκεια ισχύος, η οποία και αναγράφεται μέσα στα προκαθορισμένα για τον σκοπό αυτό πεδία τους.

Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού μπορεί οποτεδήποτε να ανακληθεί οριστικά ή να ανασταλεί ύστερα από αίτημα του τελικού χρήστη (π.χ. επειδή έχασε τον φορέα των κρυπτογραφικών κλειδιών του) ή και από σχετική απόφαση του Εκδότη τους (π.χ. λόγω λάθους στην αναγραφή στοιχείων). Η ανάκληση και η αναστολή ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του αριθμού ταυτοποίησης του πιστοποιητικού (certificate's serial number) σε μια Λίστα Ανακληθέντων Πιστοποιητικών (Certificate Revocation List - CRL) η οποία υπογράφεται και δημοσιεύεται σε τακτά χρονικά διαστήματα από τον ίδιο τον Εκδότη των πιστοποιητικών. Βέβαια, τελευταία, χρησιμοποιείται ευρέως η υπηρεσία της «Άμεσης Επιβεβαίωσης της Κατάστασης του Πιστοποιητικού» (Online Certificate Status Provision - OCSP) η οποία έχει ως σημαντικό πλεονέκτημα τον άμεσο έλεγχο της πραγματικής κατάστασης ενός πιστοποιητικού ακόμη και ελάχιστες στιγμές μετά την οριστική αποδοχή του αιτήματος ανάκλησης από τον ΠΥΠ.

Επίσης, επειδή τα πιστοποιητικά δημοσίων κλειδιών (public key certificates –PKC) που εκδίδει ένας ΠΥΠ προς τους ενδιαφερόμενους τελικούς χρήστες είναι και αυτά μια μορφή ηλεκτρονικών εγγράφων, επιβάλλεται να φέρουν και αυτά την ψηφιακή υπογραφή του εκδότη τους. Αυτό προϋποθέτει ότι και ο ίδιος ο Εκδότης - ΠΥΠ διαθέτει το δικό του ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού που κι αυτό με τη σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Η σχηματιζόμενη αλληλουχία πιστοποιητικών τερματίζεται με ένα τελικό και αξιόπιστα δημοσιευμένο αυτοϋπογραφόμενο πιστοποιητικό (self-signed certificate) που εκδίδεται από τον Θεμελιώδη Εκδότη Πιστοποιητικών (Root Certification Authority - Root CA) του ΠΥΠ και το οποίο αποτελεί την κορυφή της πυραμίδας μιας υποδομής δημοσίου κλειδιού.

Έτσι, για να ελέγξει κάποιος την εγκυρότητα μιας προηγμένης ηλεκτρονικής υπογραφής, θα πρέπει να ελέγξει το κύρος του συγκεκριμένου πιστοποιητικού που την υποστηρίζει και συγκεκριμένα θα πρέπει να ελέγξει:

- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα είναι αυθεντικό, με την έννοια ότι υπάρχει τουλάχιστον μία αλληλουχία πιστοποιητικών με όλους τους μεσολαβούντες εκδότες η οποία να καταλήγει σε μια αξιόπιστη γι' αυτόν ρίζα εμπιστοσύνης, συνήθως το αυτοϋπογραφόμενο πιστοποιητικό 'Root CA' ενός γνωστού ΠΥΠ.
- Ότι το συγκεκριμένο πιστοποιητικό είναι έγκυρο, δηλαδή ότι δεν έχει λήξει ή ανακληθεί η ισχύς του. Αυτό σημαίνει ότι ο αποδέκτης θα πρέπει να ελέγξει, όχι μόνο τη διάρκεια ισχύος 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 (Online Certificate Status Protocoll – OCSP) που πιθανώς να παρέχει ο ΠΥΠ.

- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα είναι κατάλληλο για τη συναλλαγή ή τη 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 ισχύουσα Πολιτική Πιστοποιητικού. Επίσης, εάν από τον τύπο της επιχειρούμενης συναλλαγής έχει καθοριστεί ή και πρέπει να ακολουθηθεί μια συγκεκριμένη Πολιτική Ηλεκτρονικής Υπογραφής, τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή έστω να επιτρέπεται από την εφαρμοζόμενη Πολιτική Υπογραφής. [1]

5.4 Ο Ρόλος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων - ΕΕΤΤ

Για την εγκυρότητα μιας καθημερινής συναλλαγής απαιτείται η υπογραφή του συναλλασσόμενου. Η υπογραφή σε ένα κείμενο αποτελεί απόδειξη ότι ο υπογράφων γνωρίζει, και αποδέχεται το κείμενο αυτό. Ο υπογράφων δεν μπορεί να αρνηθεί το από αυτόν υπογεγραμμένο περιεχόμενο, εκτός από συγκεκριμένες περιπτώσεις εκδήλωσης παραβατικής συμπεριφοράς (πλαστογραφία, απάτη κ.λ.π.). Ένα υπογεγραμμένο κείμενο έχει νομική υπόσταση και επικυρώνει τη συναλλαγή.

Το π.δ.150/2001 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν. Επιπλέον, το Προεδρικό Διάταγμα εκτός των άλλων:

- Καθόρισε τους όρους που πρέπει να ισχύουν σε ψηφιακά πιστοποιητικά για να θεωρούνται αναγνωρισμένα πιστοποιητικά και τους όρους που πρέπει να πληρούν οι Πάροχοι Υπηρεσιών Πιστοποίησης για να τα παρέχουν.
- Έθεσε τις αρχές λειτουργίας της εσωτερικής αγοράς όσον αφορά την παροχή υπηρεσιών πιστοποίησης.
- Έθεσε τις προϋποθέσεις νομικής αναγνώρισης εντός ΕΕ των αναγνωρισμένων πιστοποιητικών που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης εγκατεστημένους σε χώρες εκτός ΕΕ και άλλες σχετικές προβλέψεις που αφορούν διεθνείς πτυχές.
- Έθεσε το πλαίσιο της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης.
- Ανέθεσε στην ΕΕΤΤ συγκεκριμένες αρμοδιότητες.

Οι αρμοδιότητες της ΕΕΤΤ όπως απορρέουν από το ΠΔ 150/2001 είναι οι εξής:

- Η παροχή Εθελοντικής Διαπίστευσης, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης, προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης (άρθρο 4 παρ. 5) ή η ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού. Με την Εθελοντική Διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον Πάροχο Υπηρεσιών Πιστοποίησης.
- Η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του πδ. 150/2001 (εφόσον η ΕΕΤΤ αναθέσει τέτοια καθήκοντα σε άλλους φορείς) (άρθρο 4 παρ. 8).

- Η διαπίστωση της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής) προς το Παράρτημα ΙΙΙ του Προεδρικού Διατάγματος 150/2001 (άρθρο 4 παρ. 2) ή ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού.
- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι ενεργούν ως διαπιστευμένοι, χωρίς να είναι (άρθρο 4 παρ.9)
- Η ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και για τυχόν αλλαγές στις παραπάνω πληροφορίες (άρθρα 8 παρ. 2 και 3).

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.[7]

5.5 Η προστασία των προσωπικών δεδομένων

Ειδική πρόβλεψη γίνεται από την Οδηγία και το Π.Δ. για την τήρηση της νομοθεσίας περί προστασίας των δεδομένων και της ιδιωτικής ζωής από τους παρόχους υπηρεσιών πιστοποίησης. Η Οδηγία με το άρθρο 8 παράγρ. 1 παραπέμπει ρητά στις σχετικές διατάξεις της οδηγίας 95/46/ΕΚ ‘’Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών’’, ενώ το άρθρο 7 του ΠΔ ορίζει ότι ‘’Οι πάροχοι υπηρεσιών πιστοποίησης, η ΕΕΤΤ και οι φορείς του άρθρου 4 υπόκεινται στις διατάξεις του ν. 2472/97 και του ν.2774/99 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα’’.

Επιπλέον, ορίζεται ότι ένας Παροχέας Υπηρεσιών Πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό, δύναται να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν ή κατόπιν ρητής συγκατάθεσής του και μόνο στο βαθμό που είναι απαραίτητο για τους σκοπούς έκδοσης και διατήρησης του πιστοποιητικού. Συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου απαγορεύεται. (άρθρο 8 παρ.2 της Οδηγίας και άρθρο 7 παρ.2 του ΠΔ). [35, σελ.181]

Κεφάλαιο 6

6.1 Ψηφιακές υπογραφές και εθνική νομοθεσία- Εισαγωγικά

Προκειμένου να αντιμετωπιστούν τα διάφορα προβλήματα που προκαλεί η έλλειψη ειδικής νομοθετικής ρύθμισης στα διάφορα κράτη-μέλη της ΕΕ αλλά και για τη βελτίωση των εμπορικών συναλλαγών μέσω των ηλεκτρονικών μέσων και την ανταπόκριση τους στις σύγχρονες απαιτήσεις και ανάγκες της αγοράς, η ΕΕ εξέδωσε την Οδηγία 1999/93/ΕΚ η οποία αναφέρεται στις ηλεκτρονικές υπογραφές. Η οδηγία αυτή ενσωματώθηκε στο ελληνικό δίκαιο με το προεδρικό διάταγμα 150/2001. [8, σελ.99]

Στο περιβάλλον της ιδιόχειρης υπογραφής, κατά το άρθρο 160 παρ.1 ΑΚ, το έγγραφο ως συστατικό στοιχείο της δικαιοπραξίας πρέπει να φέρει την ιδιόχειρη υπογραφή του εκδότη του. Επίσης σύμφωνα με το άρθρο 443 ΚΠολΔ (Κώδικας Πολιτικής Δικονομίας), η αποδεικτική δύναμη του εγγράφου καθορίζεται από την ιδιόχειρη υπογραφή του εκδότη του.

Στηριζόμενος στις τεχνολογικές δυνατότητες της εποχής ο νομοθέτης τόσο του ουσιαστικού όσο και του δικονομικού δικαίου έχει αποκλείσει τη χρήση μηχανικών μέσων ως υποκατάστατων της ιδιόχειρης υπογραφής ώστε να πληρούνται οι προϋποθέσεις του Νόμου. Σε αυτό το διαχωρισμό όμως δεν είχε περιληφθεί η χρήση ηλεκτρονικών εγγράφων και ηλεκτρονικών υπογραφών, μια τεχνολογική εξέλιξη που ο νομοθέτης δεν μπορούσε να προβλέψει.

Η απάντηση στο ερώτημα εάν οι ηλεκτρονικές υπογραφές μπορούν να ενταχθούν στο πλαίσιο των άρθρων 160 παρ. 1 ΑΚ και 443 ΚπολΔ, εξαρτάται από το αν με αυτό τον τρόπο εξασφαλίζεται η γνησιότητα του υπογραφόμενου εγγράφου. Καθώς οι ηλεκτρονικές υπογραφές διασφαλίζουν την ταυτοποίηση του χρήστη, την ακεραιότητα του εγγράφου και τη μη αποκήρυξη της συναλλαγής η απάντηση στο παραπάνω ερώτημα είναι καταφατική.

Το δίκαιο στηριζόμενο σε ορισμένες γενικές λειτουργίες που τίθενται από την τεχνολογική λύση που επιλέγεται, θέτει ορισμένους βασικούς κανόνες για τη λειτουργία ενός συστήματος που χρησιμοποιεί ηλεκτρονικές υπογραφές και εξειδικεύει τις γενικές αρχές χρήσης των υπογραφών στις συναλλαγές. Ένας αρχικός συστηματικός διαχωρισμός θα πρέπει να γίνει σχετικά με τους όρους ηλεκτρονική υπογραφή και ψηφιακή υπογραφή. Ως κατηγορία των ηλεκτρονικών υπογραφών θεωρούμε τις ψηφιακές υπογραφές, οι οποίες κάνουν χρήση μιας συγκεκριμένης τεχνολογίας, που βασίζεται στη χρήση της ασύμμετρης κρυπτογραφίας ή κρυπτογραφίας δημόσιου κλειδιού.

Οι ηλεκτρονικές υπογραφές γενικά χρησιμοποιούν τεχνικές ασύμμετρης κρυπτογραφίας, που στηρίζονται κυρίως στη χρήση ενός ζεύγους κλειδιών. Μια μοναδική μαθηματική σχέση μεταξύ των δύο μερών του ζεύγους κλειδιών καθιστά δυνατή την επαλήθευση της χρήσης του ενός κλειδιού όταν είναι γνωστό το άλλο. Καθώς είναι μαθηματικά αδύνατο να συμπεράνει κάποιος το ένα κλειδί όταν γνωρίζει το άλλο, η επαλήθευση της χρήσης του κλειδιού γίνεται με την αποστολή στον αντισυμβαλλόμενο ή δημοσιοποίηση του άλλου κλειδιού, που ονομάζεται δημόσιο κλειδί και αποτελεί μέρος του ζεύγους κλειδιών της ηλεκτρονικής υπογραφής.

Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών πηγάζει από την ανάγκη αναγνώρισης μιας ηλεκτρονικής μεθόδου ως νομικά έγκυρης και ισότιμης με τη χειρόγραφη μέθοδο παραγωγής υπογραφής, ώστε να μπορεί να χρησιμοποιηθεί κατά την απόδειξη. Παρά το γεγονός ότι στις περισσότερες ιδιωτικές συναλλαγές οποιοδήποτε στοιχείο δηλωτικό της βούλησης του υπογράφοντος να δεσμευθεί μπορεί να ερμηνευθεί ως υπογραφή, η εισαγωγή της τεχνολογίας στις συναλλαγές δημιουργεί την ανάγκη ειδικής αναγνώρισης τόσο των ηλεκτρονικών υπογραφών, όσο και των ηλεκτρονικών εγγράφων επί των οποίων χρησιμοποιούνται. Επιπλέον είναι αναγκαίο να αναδειχθεί η δεσμευτική σύνδεση μεταξύ του υπογράφοντος συναλλασσόμενου και της σχετικής τεχνολογίας που χρησιμοποιεί, προκειμένου να μην είναι δυνατή η εκ των υστέρων αποκήρυξη της συναλλαγής.

Σχετικά με το ποια τεχνολογία είναι κατάλληλη για τη δημιουργία και επαλήθευση ηλεκτρονικών υπογραφών η διεθνής και ευρωπαϊκή νομοθετική θέση στην ρύθμιση των ηλεκτρονικών υπογραφών υιοθετεί γενικά μια τεχνολογικά ουδέτερη στάση στο ερώτημα της καταλληλότητας και της ασφάλειας της τεχνολογίας που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές.

Η επιλογή της τεχνολογίας πρέπει να στηρίζεται στην αξιολόγηση του κινδύνου (risk assessment) σε σχέση με την εφαρμογή για την οποία πρόκειται να χρησιμοποιηθεί η ηλεκτρονική υπογραφή. Ο κίνδυνος από τη χρήση ηλεκτρονικών υπογραφών αφορά κυρίως τους τρίτους, που βασίζονται στην ηλεκτρονική υπογραφή προκειμένου να αξιολογήσουν τη δεσμευτικότητα της δήλωσης βούληση του υπογράφοντος που βασίζεται στην επαλήθευση του δημόσιου κλειδιού του.

Μια λύση σε αυτά τα προβλήματα δίνουν οι έμπιστες τρίτες οντότητες ή αρχές πιστοποίησης, που πιστοποιούν ότι το δημόσιο κλειδί του υπογράφοντος πράγματι του ανήκει και συνδέεται μονοσήμαντα με το ιδιωτικό του κλειδί που παραμένει μυστικό. Οι έμπιστες τρίτες οντότητες εκδίδουν λοιπόν ηλεκτρονικά πιστοποιητικά, τα οποία είναι ηλεκτρονικά αρχεία που περιλαμβάνουν το δημόσιο κλειδί του υπογράφοντα, το οποίο χρησιμοποιείται για την επαλήθευση της υπογραφής του και στοιχεία που επιβεβαιώνουν την ταυτότητά του. Τα ηλεκτρονικά πιστοποιητικά αποτελούν μονομερείς δηλώσεις βούλησης της εκδίδουσας έμπιστης τρίτης οντότητας, οι οποίες πιστοποιούν στοιχεία απαραίτητα για την ηλεκτρονική υπογραφή και την επαλήθευσή της.[20, σελ.110-111]

Ήδη από τα μέσα της δεκαετίας του 1990 διεθνείς και εθνικές πρωτοβουλίες άρχισαν να εστιάζουν στη ρύθμιση της χρήση ηλεκτρονικών υπογραφών. Ο πρώτος ολοκληρωμένος νόμος για τις ηλεκτρονικές υπογραφές, ψηφίστηκε στην πολιτεία της Γιούτα των ΗΠΑ και αναφέρεται στο νομικό αποτέλεσμα των ηλεκτρονικών υπογραφών και στη λεπτομερή ρύθμιση και αδειοδότηση της παροχής σχετικών υπηρεσιών ηλεκτρονικής υπογραφής.

Σημαντικό εμπόδιο στη νομοθετική ρύθμιση για πολλά χρόνια αποτέλεσε η πολιτική πολλών κυβερνήσεων στον τομέα της κρυπτογραφίας, έναν τομέα που όσο η αμερικανική όσο και οι ευρωπαϊκές κυβερνήσεις θεωρούσαν ως αποκλειστικά εθνική τους υπόθεση και συνεπώς αρνούνταν να προχωρήσουν σε συζητήσεις σε διεθνές επίπεδο.[20, σελ.112]

Από το 1996 έχει ξεκινήσει η δημιουργία ενός διεθνούς νομικού πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών και τη διασφάλιση των συναλλαγών. Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για ψηφιακές υπογραφές (οι οποίες ταυτίζονται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές της Οδηγίας) γίνεται ήδη από το άρθρο 14 του ν. 2672/98 όπου παρέχεται μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα.[1] Το 1999 η Οδηγία 1999/93/ΕΚ σχετικά με ένα κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές έθεσε τις βάσεις του ρυθμιστικού πλαισίου των ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Ένωση (ΕΕ). [20, σελ.109]

Ακολούθησε το π.δ. 150/2001 (ΦΕΚ Α'/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 τη λειτουργία μηχανισμών Εθελοντικής Διαπίστευσης των ΠΥΠ και Διαπίστωσης της συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής.

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

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής, καθώς και τρεις Κανονισμούς σχετικά με την Εθελοντική Διαπίστευση των ΠΥΠ, 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.[1]

6.2 Νομική αναγνώριση των ηλεκτρονικών υπογραφών

Η νομική αναγνώριση των ηλεκτρονικών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη. Μπορούμε να διακρίνουμε δύο διαφορετικές νομικές προσεγγίσεις:

- Τη μινιμαλιστική προσέγγιση (minimalist approach), όπου κάθε αξιόπιστη τεχνολογική μέθοδος απόδειξης της προέλευσης και της αυθεντικότητας των ψηφιακών δεδομένων πρέπει να γίνεται νομικώς αποδεκτή, την οποία ακολούθησαν κράτη όπως οι Η.Π.Α., ο Καναδάς, η Μεγ. Βρετανία, η Αυστραλία, κ.α.
- Την αναλυτική προσέγγιση (prescriptive approach), σύμφωνα με την οποία μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται άμεσα ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές, σύμφωνα με την οποία έχουν διαμορφώσει την εθνική τους νομοθεσία χώρες όπως η Γερμανία, η Ιταλία, η Εσθονία κ.α. [1]

6.3 Η Οδηγία 1999/93/ΕΚ για τις ηλεκτρονικές υπογραφές

6.3.1 Εισαγωγικές παρατηρήσεις

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

Έτσι, η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως ηλεκτρονικές υπογραφές, που μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες (άρθρο 5 παρ.2 της Οδηγίας), όλα τα δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας (άρθρο 2 §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 τις πιο σύνθετες (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων κλπ), ανεξάρτητα δηλαδή, από το βαθμό τεχνικής ασφάλειας που παρέχουν.

Επίσης η Οδηγία (άρθρο 5 §1) διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών, αποκαλούμενες στη πράξη στην πλειοψηφία των ευρωπαϊκών κρατών ως προηγμένες ηλεκτρονικές υπογραφές (ψηφιακές υπογραφές), στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές, όπως οι τελευταίες ορίζονται σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους.[1]

Οι βασικές βλέψεις λοιπόν της Οδηγίας είναι (α) να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών, (β) να συμβάλει στη νομική τους αναγνώριση και (γ) να θέσει ένα νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για την παροχή υπηρεσιών πιστοποίησης. Η Οδηγία επιδιώκει να συνεισφέρει στην εναρμόνιση της εσωτερικής αγοράς, καθώς η Ιταλία και η Γερμανία, είχαν αναλάβει νομοθετικές πρωτοβουλίες με σκοπό τη ρύθμιση της ηλεκτρονικής υπογραφής.

Στη Γερμανία η κυρίαρχη τάση ήταν η αναζήτηση κανόνων για το πώς οι ηλεκτρονικές υπογραφές μπορούν να χρησιμοποιηθούν με ασφάλεια αντίστοιχα των χειρόγραφων υπογραφών.

Στην Ιταλία, από την άλλη πλευρά, αναπτύχθηκε η άποψη ότι, εφόσον οι συμβαλλόμενοι ακολουθούν τους νομοθετημένους κανόνες, οι χρησιμοποιούμενες ηλεκτρονικές υπογραφές μπορούν να θεωρηθούν ως ισότιμες των χειρόγραφων υπογραφών. Παρά την έμφαση του ιταλικού Νόμου σε διαδικασίες αντί της τεχνολογικής ασφάλειας που προϋπέθεσε ο αντίστοιχος γερμανικός, η επιλογή των κριτηρίων αξιολόγησης των παροχών στηρίχθηκε αρχικά σε ένα οργανωτικό μοντέλο που δεν ήταν προσαρμοσμένο στις ανάγκες των παροχών ηλεκτρονικής υπογραφής. Θα πρέπει να γίνεται δεκτό ότι ο επιδιωκόμενος νομικός σκοπός των ηλεκτρονικών υπογραφών είναι η διασφάλιση της νομικής βεβαιότητας της συναλλαγής. Συνεπώς το επίπεδο αξιολόγησης της χρησιμοποιούμενης τεχνολογικής λύσης θα πρέπει να βρίσκεται σε αναλογία με τον προκύπτοντα κάθε φορά ενδεχόμενο συναλλακτικό κίνδυνο, ο

οποίος και θα πρέπει να αξιολογείται σε κάθε περίπτωση συγκεκριμένα. Επιπλέον, ένα γενικώς αποδεκτό επίπεδο ασφάλειας μπορεί να ισχύσει δεσμευτικά και έναντι τρίτων, στο βαθμό που η λειτουργία του διασφαλίζεται από το Νόμο.

Το τελικό σχέδιο της Οδηγίας είχε τρεις στόχους: την τεχνολογική ουδετερότητα, την αποφυγή κατακερματισμού της εσωτερικής αγοράς και τη νομική αναγνώριση των ηλεκτρονικών υπογραφών στο ευρωπαϊκό και εθνικό δίκαιο.

Η Οδηγία στοχεύει επίσης στη ρύθμιση των ηλεκτρονικών υπογραφών που χρησιμοποιούνται σε δημόσια ανοιχτά δίκτυα όπως το Internet, ενώ κλειστές ομάδες χρηστών που διαμορφώνουν τις σχέσεις τους στη βάση συμβάσεων μπορούν εξίσου να επωφεληθούν από την Οδηγία, στο βαθμό που το επιθυμούν και εφόσον ακολουθήσουν τις διατάξεις. Η αρχή της ελευθερίας των συμβαλλομένων μερών αναγνωρίζεται στο βαθμό που κλειστές ομάδες χρηστών μπορούν αυτοτελώς να αποφασίζουν ποια κατηγορία ηλεκτρονικών υπογραφών ανταποκρίνεται στις συναλλακτικές ανάγκες τους. Αυτό έχει ιδιαίτερο ενδιαφέρον στις τραπεζικές εφαρμογές, στο βαθμό που μπορεί να θεωρηθεί ότι οι συναλλασσόμενοι πελάτες ή προμηθευτές μιας τράπεζας αποτελούν κλειστή ομάδα χρηστών. [20, σελ.109]

6.3.2 Περιεχόμενο της Οδηγίας 1999/93/ΕΚ

Στόχος της οδηγίας 1999/93/ΕΚ είναι σύμφωνα με το **άρθρο 1** να διευκολύνει τη χρήση των ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Με την Οδηγία αυτή θεσπίζεται το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίζεται η ομαλή λειτουργία της εσωτερικής αγοράς.

Δεν καλύπτονται από τις διατάξεις της Οδηγίας πτυχές σχετικές με τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις του εθνικού ή του κοινοτικού δικαίου ως προς τον τύπο και δε θίγονται κανόνες και περιορισμοί σχετικά με τη χρήση εγγράφων, οι οποίοι περιέχονται στο εθνικό ή στο κοινοτικό δίκαιο.

Σύμφωνα με τους ορισμούς που δίνονται στο **άρθρο 2** της Οδηγίας,

‘’ηλεκτρονική υπογραφή’’ είναι 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.

"προηγμένη ηλεκτρονική υπογραφή" είναι η ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις: συνδέεται μονοσήμαντα με τον υπογράφοντα, είναι ικανή να ταυτοποιήσει τον υπογράφοντα, δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και τέλος συνδέεται με δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

"υπογράφων" είναι το φυσικό ή το νομικό πρόσωπο που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή φορέα που αντιπροσωπεύει.

"δεδομένα δημιουργίας υπογραφής" είναι μονοσήμαντα δεδομένα όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής.

"διάταξη δημιουργίας υπογραφής" είναι το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής.

"ασφαλής διάταξη δημιουργίας υπογραφής" νοείται η διάταξη δημιουργίας υπογραφής που πληροί τις απαιτήσεις του παραρτήματος ΙΙΙ και που θα δούμε παρακάτω,

"δεδομένα δημιουργίας υπογραφής" είναι δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής.

"δεδομένα επαλήθευσης υπογραφής" είναι το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής.

"πιστοποιητικό" ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο που επιβεβαιώνει την ταυτότητά του.

"αναγνωρισμένο πιστοποιητικό" είναι το πιστοποιητικό που ανταποκρίνεται στις οριζόμενες στο παράρτημα Ι απαιτήσεις και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τις οριζόμενες στο παράρτημα ΙΙ απαιτήσεις.

"πάροχος υπηρεσιών πιστοποίησης" είναι ο φορέας ή το φυσικό ή το νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.

"προϊόν ηλεκτρονικής υπογραφής" είναι το υλικό ή το λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται για χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την παροχή υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.

"εθελοντική διαπίστευση" είναι κάθε άδεια, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις που διέπουν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται κατόπιν αιτήσεως του ενδιαφερόμενου παρόχου υπηρεσιών πιστοποίησης από το δημόσιο ή ιδιωτικό φορέα ο οποίος είναι υπεύθυνος για τον καθορισμό αυτών των δικαιωμάτων και υποχρεώσεων και για τον έλεγχο της τήρησής τους, όταν ο πάροχος των υπηρεσιών πιστοποίησης δεν δικαιούται να ασκεί τα δικαιώματα που απορρέουν από την άδεια προτού λάβει την απόφαση του εν λόγω φορέα.

Το **άρθρο 3** αφορά στη λειτουργία της ηλεκτρονικής υπογραφής μέσα στην εσωτερική και ευρωπαϊκή αγορά και ορίζει ότι τα κράτη μέλη δεν μπορούν να εξαρτούν την παροχή υπηρεσιών πιστοποίησης από προηγούμενη έγκριση. Έχουν όμως το δικαίωμα να διατηρούν μηχανισμούς εθελοντικής διαπίστευσης και να επιβάλουν την τήρηση ορισμένων πρόσθετων απαιτήσεων, όταν πρόκειται για χρήση της ηλεκτρονικής υπογραφής στο δημόσιο τομέα. Οι εν λόγω απαιτήσεις είναι αντικειμενικές, διαφανείς και δεν οδηγούν σε διακρίσεις. Αναφέρονται μόνο στα ειδικά χαρακτηριστικά της συγκεκριμένης εφαρμογής. Οι απαιτήσεις αυτές δεν πρέπει να αποτελούν εμπόδιο στις διασυνοριακές υπηρεσίες για τους πολίτες.

Το άρθρο 3 παράγραφος 5 προβλέπει τη δυνατότητα αναγνώρισης προτύπων μέσω της δημοσίευσης τους στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Η επιτροπή του άρθρου 9 της Οδηγίας που αποτελείται από εκπροσώπους των κρατών μελών, προαπαιτείται να δώσει θετική γνωμοδότηση σχετικά με τη δημοσίευση τέτοιων προτύπων, πράγμα που το έπραξε την περίοδο 2002-2003 για επιλεγμένα πρότυπα, τα οποία και η Ευρωπαϊκή Επιτροπή δημοσίευσε σε σχετικό κατάλογο.

Στο **άρθρο 4** αναφέρονται οι αρχές της εσωτερικής αγοράς. Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει κατ' εφαρμογή της παρούσας οδηγίας για παρόχους υπηρεσιών πιστοποίησης εγκατεστημένους στην επικράτειά του, καθώς και για τις υπηρεσίες που αυτοί παρέχουν. Τα κράτη μέλη δεν μπορούν να περιορίσουν την παροχή υπηρεσιών πιστοποίησης που προέρχονται από άλλο κράτος μέλος στους τομείς που καλύπτονται από την παρούσα οδηγία. Επίσης, τα κράτη μέλη διασφαλίζουν ότι τα προϊόντα ηλεκτρονικής υπογραφής που συμμορφώνονται με την παρούσα Οδηγία, επιτρέπεται να κυκλοφορούν ελεύθερα στην εσωτερική αγορά.

Η σημαντικότερη συνεισφορά της Οδηγίας συνίσταται στη νομική αναγνώριση των ηλεκτρονικών υπογραφών ως αντίστοιχων με τις ιδιόχειρες. Στις τυπικές συναλλαγές η υπογραφή συχνά θεωρείται συστατικό στοιχείο της συναλλαγής. Παράδειγμα αποτελούν οι συμβάσεις που αφορούν ακίνητα, ασφάλειες κλπ. Με το **άρθρο 5** αναστέλλεται η αβεβαιότητα σχετικά με τη χρήση των ηλεκτρονικών υπογραφών στις συναλλαγές ,καθώς όπου ο Νόμος το απαιτεί μπορούν πλέον να χρησιμοποιούνται οι ηλεκτρονικές υπογραφές και να εισάγονται στην αποδεικτική διαδικασία. Το άρθρο 5 προβλέπει τις έννομες συνέπειες των ηλεκτρονικών υπογραφών. Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής: α) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες. Το άρθρο 5 δε δημιουργεί υποχρέωση των κρατών μελών να χρησιμοποιούν τα ίδια ή να ενθαρρύνουν τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, καθώς άλλες Οδηγίες έχουν αναλάβει αυτή την υποχρέωση (πχ. η Οδηγία 2001/115/ΕΚ σχετικά με τις προϋποθέσεις χρήσης ηλεκτρονικών τιμολογίων). Συνεπώς η Οδηγία δεν επηρεάζει την ισχύ κανόνων που ήδη ισχύουν στις συναλλαγές. Τα κράτη μέλη όμως μπορούν να εισάγουν επιπλέον όρους και προϋποθέσεις στις ήδη υπάρχουσες που αφορούν τις ηλεκτρονικές υπογραφές.

Παράλληλα στο άρθρο 5 παράγραφος 2 τα κράτη μέλη πρέπει να διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού

στοιχείου, επειδή τυχόν είναι υπό μορφή ηλεκτρονικών δεδομένων, ή να μη στηρίζονται σε αναγνωρισμένο πιστοποιητικό, ή σε αναγνωρισμένο πιστοποιητικό που έχει εκδοθεί από διαπιστευμένη αρχή πιστοποίησης, ή να μην έχουν δημιουργηθεί εντός μιας ασφαλούς διάταξης.

Η δυσχέρεια εφαρμογής της παραγράφου 2 άρθρου 5 βρίσκεται στη δυσκολία υιοθέτησης αντικειμενικών κριτηρίων για την απόρριψη μη προηγμένων ηλεκτρονικών υπογραφών. Τα κριτήρια αυτά ίσως θα πρέπει να στηρίζονται στην αναξιοπιστία της χρησιμοποιούμενης τεχνικής μεθόδου. Είναι γενικά παραδεκτό ότι, επειδή ως υπογραφή μπορεί να χρησιμοποιηθεί οποιοδήποτε σημείο που μπορεί να ερμηνευθεί ως δηλωτικό της βούλησης του υπογράφοντος ώστε να δεσμευθεί από τη συναλλαγή, η χρήση οποιασδήποτε τεχνικής μεθόδου για τη σύνταξη της ηλεκτρονικής υπογραφής θα πρέπει να γίνεται γενικά δεκτή. Ο υπογράφων πάντως θα πρέπει να είναι σε θέση να αποδείξει την ακεραιότητα της επιλεγείσας μεθόδου ως κατάλληλης και ασφαλούς για τον επιδιωκόμενο σκοπό.

Το **άρθρο 6** της Οδηγίας αναφέρεται στα ζητήματα ευθύνης από την παροχή υπηρεσιών αναγνωρισμένων πιστοποιητικών. Αναφέρονται ζητήματα μόνο σχετικά με υπηρεσίες που αφορούν την έκδοση και διαχείριση αναγνωρισμένων ηλεκτρονικών πιστοποιητικών. Ζητήματα ευθύνης που ίσως προκύπτουν από τη χρήση προϊόντων ηλεκτρονικής υπογραφής δεν καλύπτονται από το παρόν άρθρο. Καθώς το άρθρο 6 αποτελεί το ελάχιστο κοινό επίπεδο μεταξύ των κρατών μελών, τα ίδια τα κράτη μέλη μπορούν να προσθέσουν επιπλέον στοιχεία ευθύνης ή να καλύψουν ζητήματα πέραν των αναγνωρισμένων πιστοποιητικών.

Το άρθρο 6 καθιερώνει την ευθύνη του παρόχου υπηρεσιών πιστοποίησης για την προκληθείσα ζημία σε οποιοδήποτε φορέα, φυσικό ή νομικό πρόσωπο, που ευλόγως βασίζεται στο πιστοποιητικό: (α) όσον αφορά την ακρίβεια, κατά τη στιγμή έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη στο πιστοποιητικό όλων των απαιτούμενων στοιχείων για ένα αναγνωρισμένο πιστοποιητικό, (β) για τη διαβεβαίωση ότι, κατά το χρόνο έκδοσης του πιστοποιητικού, ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν κάτοχος των δεδομένων δημιουργίας υπογραφής που αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής που αναφέρονται ή ταυτοποιούνται στο πιστοποιητικό και (γ) για τη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και τα δεδομένα επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, στις περιπτώσεις που αμφότερα προέρχονται από τον πάροχο υπηρεσιών πιστοποίησης. Η ευθύνη του παρόχου υπηρεσιών πιστοποίησης ανακαλείται αν αυτός αποδείξει ότι δεν ενέργησε αμελώς.

Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι ο πάροχος υπηρεσιών πιστοποίησης που εξέδωσε πιστοποιητικό ως αναγνωρισμένο πιστοποιητικό στο κοινό έχει την ευθύνη για τη ζημία που προξενείτε σε οποιοδήποτε φορέα ή φυσικό πρόσωπο, που βασίζεται στο πιστοποιητικό, λόγω παράλειψής του να καταγράψει την ανάκληση του πιστοποιητικού, εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.

Επίσης, ένας πάροχος υπηρεσιών πιστοποίησης δύναται να αναγράφει σε αναγνωρισμένο πιστοποιητικό περιορισμούς χρήσεως αυτού του πιστοποιητικού, με την προϋπόθεση ότι οι περιορισμοί αυτοί είναι αναγνωρίσιμοι για τους τρίτους. Ο πάροχος υπηρεσιών πιστοποίησης δεν έχει ευθύνη για βλάβες που προκύπτουν από χρήση ενός αναγνωρισμένου πιστοποιητικού που υπερβαίνει τους περιορισμούς που αναγράφηκαν σε αυτό.

Σχετικά με τον περιορισμό της ευθύνης ανακύπτουν δύο ανοιχτά ζητήματα και συγκεκριμένα πώς πληροφορείται και δεσμεύεται ο τρίτος αναφορικά με τους όρους και τις διαδικασίες που ισχύουν και πώς η αρχή πιστοποίησης επικοινωνεί την πολιτική πιστοποίησής της και την καθιστά δεσμευτική σε ένα ηλεκτρονικό περιβάλλον. Η σύνδεση της υποχρεωτικής μονομερούς δηλώσεως που είναι η πολιτική πιστοποίησης με μια σύμβαση συνδρομητή είναι αναγκαία προκειμένου να ενισχυθεί η δεσμευτικότητα ιδιαίτερα σε συμβάσεις καταναλωτών. Καθώς ο τρίτος αποδέκτης του πιστοποιητικού έχει την υποχρέωση να εξετάσει την ισχύ του πιστοποιητικού, πρέπει να γίνει δεκτό ότι κανένας περιορισμός δεν μπορεί να επιβληθεί στην πρόσβαση που του παρέχεται στους πόρους δημοσίευσης πιστοποιητικών που έχουν εκδοθεί, ανακληθεί ή εκπνεύσει (certificate revocation list). Η πολιτική πιστοποίησης μπορεί συνεπώς να

χρησιμοποιηθεί προκειμένου τρίτοι να λάβουν γνώση και να συμμορφωθούν προς τους συνιστώμενους κανόνες πρόσβασης σε τέτοιους κρίσιμους πόρους.

Ένα άλλο ζήτημα που ανακύπτει σχετικά με τον τρόπο επικοινωνίας της πολιτικής πιστοποίησης προς τρίτους συνδυάζεται με την αδυναμία ενσωμάτωσης των ίδιων των νομικών όρων, όπως της πολιτικής πιστοποίησης στο ίδιο το αναγνωρισμένο πιστοποιητικό που έχει εκδοθεί. Γίνεται γενικά δεκτό και χρησιμοποιείται στην πράξη ότι η αρχή πιστοποίησης μπορεί να δημοσιεύσει την πολιτική πιστοποίησης στο δικτυακό της χώρο, ενώ οι τρίτοι μπορούν να την ανασύρουν από εκεί. Σε αυτήν την περίπτωση θα πρέπει να διασφαλίζεται η έκδοση και γνησιότητα της πολιτικής πιστοποίησης που μπορεί να διασφαλισθεί για παράδειγμα με τη διαπίστευση του παρόχου. Άλλος τρόπος διασφάλισης αφορά τη δημιουργία ενός φορέα δημοσίευσης τέτοιων πολιτικών και νομικών όρων που χρησιμοποιούνται στις συναλλαγές στο διαδίκτυο κατά το μοντέλο του ICC E TERMS.

Τέλος, τα κράτη μέλη διασφαλίζουν ότι ο πάροχος υπηρεσιών πιστοποίησης έχει την υποχρέωση να αναγράφει σε αναγνωρισμένο πιστοποιητικό τους περιορισμούς χρήσης αυτού του πιστοποιητικού, υπό την προϋπόθεση βέβαια ότι οι περιορισμοί αυτοί δύνανται να αναγνωρίζονται από τρίτους.

Φυσικά για κάθε βλάβη προκαλούμενη από την υπέρβαση αυτών των περιορισμών δεν ευθύνεται ο πάροχος.

Η διάταξη του **άρθρου 7** της Οδηγίας εξισώνει τα πιστοποιητικά τα εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο σε τρίτη χώρα με πιστοποιητικά εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Κοινότητα εφόσον τηρούνται οι παρακάτω προϋποθέσεις:

α) ο πάροχος υπηρεσιών πιστοποίησης πληροί τις απαιτήσεις που καθορίζονται στην παρούσα Οδηγία και έχει διαπιστευτεί δυνάμει εθελοντικού μηχανισμού πιστοποίησης, καθιερωμένου σε κράτος μέλος, ή

β) ο πάροχος υπηρεσιών πιστοποίησης, εγκατεστημένος στην Κοινότητα, ο οποίος πληροί τις απαιτήσεις που καθορίζονται στην παρούσα Οδηγία εγγυάται για το πιστοποιητικό, ή

γ) το πιστοποιητικό παρόχου υπηρεσιών πιστοποίησης αναγνωρίζεται δυνάμει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Κοινότητας και τρίτων χωρών ή διεθνών οργανισμών.

Η Επιτροπή, για να διευκολύνει τις διασυνοριακές υπηρεσίες πιστοποίησης με τρίτες χώρες και την αναγνώριση προηγμένων ηλεκτρονικών υπογραφών προερχόμενων από τρίτες χώρες, καθιερώνει στην παράγραφο 2 του εν λόγω άρθρου δυνατότητα να διατυπώνει προτάσεις για την επίτευξη αποτελεσματικής εφαρμογής προτύπων και διεθνών συμφωνιών που ισχύουν για υπηρεσίες πιστοποίησης. Ειδικότερα, όπου κρίνει απαραίτητο, υποβάλλει προτάσεις προς το Συμβούλιο για την έκδοση κατάλληλων εντολών διαπραγμάτευσης διμερών και πολυμερών συμφωνιών με τρίτες χώρες και διεθνείς οργανισμούς. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.

Όσες φορές η Επιτροπή πληροφορείται τυχόν δυσκολίες που συναντούν οι κοινοτικές επιχειρήσεις όσον αφορά την πρόσβαση σε αγορές τρίτων χωρών δύναται να υποβάλει στο Συμβούλιο προτάσεις για τη δέουσα εντολή διαπραγμάτευσης αναλόγων δικαιωμάτων των κοινοτικών επιχειρήσεων σε αυτές τις τρίτες χώρες. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία. Φυσικά τα μέτρα που λαμβάνονται δυνάμει της παρούσας παραγράφου δεν θίγουν τις υποχρεώσεις της Κοινότητας και των κρατών μελών βάσει σχετικών διεθνών συμφωνιών.

Το **άρθρο 8** της Οδηγίας θίγει το θέμα της προστασία δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα τα κράτη μέλη διασφαλίζουν ότι:

- οι πάροχοι υπηρεσιών πιστοποίησης και οι εθνικοί φορείς, αρμόδιοι για πιστοποίηση ή εποπτεία, συμμορφώνονται προς τις απαιτήσεις που καθορίζονται στην οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

- ο πάροχος υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό, μπορεί να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν, ή με τη ρητή συγκατάθεσή του, και μόνον στο βαθμό που είναι απαραίτητο για τους σκοπούς έκδοσης και διατήρησης του πιστοποιητικού. Δεν επιτρέπεται συλλογή ή επεξεργασία

των δεδομένων για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου.

Επιπλέον, τα κράτη μέλη δεν εμποδίζουν τους παρόχους υπηρεσιών πιστοποίησης να αναφέρουν στο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος, βέβαια με την επιφύλαξη των συνεπειών του νόμου των ψευδωνύμων βάσει της εθνικής νομοθεσίας.

Η Οδηγία προβλέπει, σύμφωνα με το **άρθρο 9**, τη σύσταση ειδικής «Επιτροπής Ηλεκτρονικής Υπογραφής» η οποία αποτελείται από εκπροσώπους των κρατών μελών, ενώ στο **άρθρο 10** αναφέρονται τα καθήκοντα της.

Τέλος, σύμφωνα με το **άρθρο 11** τα κράτη μέλη κοινοποιούν στην Επιτροπή και στα λοιπά κράτη μέλη πληροφορίες σχετικά με εθνικά συστήματα εθελοντικής διαπίστευσης, ονομασίες και διευθύνσεις των εθνικών φορέων που είναι αρμόδιοι για διαπίστευση και επίβλεψη, ονομασίες και διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης. Το σύνολο των πληροφοριών αυτών καθώς και τυχόν αλλαγές κοινοποιούνται άμεσα από τα κράτη μέλη.[26], [40]

6.3.3 Περιεχόμενο των αναγνωρισμένων πιστοποιητικών

Η Οδηγία, σύμφωνα με το **Παράρτημα Ι**, ορίζει ότι τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν στα σχετικώς προβλεπόμενα πεδία τους τουλάχιστον τα παρακάτω στοιχεία:

α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό,

β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος,

γ) το όνομα του υπογράφοντος ή το ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο,

δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό,

ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος,

στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού,

ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού,

η) την προηγμένη ηλεκτρονική υπογραφή του ΠΥΠ που το εκδίδει,

θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού και τέλος

ι) τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί. [26]

6.3.4 Όροι ισχύοντες για Παρόχους Υπηρεσιών Πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι πάροχοι υπηρεσιών πιστοποίησης, σύμφωνα με το **Παράτημα ΙΙ** της Οδηγίας, πρέπει:

α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης,

β) να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης,

γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς,

δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση της ταυτότητας και τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό,

ε) να απασχολούν προσωπικό που διαθέτει την εμπειρογνωμοσύνη, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, εμπειρογνωμοσύνη στην τεχνολογία ηλεκτρονικών υπογραφών και εξοικείωση με τις κατάλληλες διαδικασίες ασφαλείας. Επίσης πρέπει να χρησιμοποιούν κατάλληλες διοικητικές και διαχειριστικές διαδικασίες οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα,

στ) να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται έναντι τροποποίησης και διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά,

ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και σε περίπτωση που ο πάροχος υπηρεσιών πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων,

η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην Οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών, π.χ. με τη σύναψη κατάλληλης ασφάλισης,

θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο για κατάλληλη χρονική περίοδο, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα,

ι) να μην αποθηκεύουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης προσφέρει υπηρεσίες διαχείρισης κλειδιών,

ια) προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα κατανοητή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων οι οποίοι βασίζονται στο πιστοποιητικό αυτό και τέλος,

ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, έτσι ώστε:

- μόνον αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις,

- να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

- να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου και

- οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω αιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή. [26]

6.3.5 Απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής

Σύμφωνα με το **Παράρτημα III** της Οδηγίας, οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει να διασφαλίζουν ότι τα δεδομένα δημιουργίας υπογραφής (ιδιωτικά κλειδιά) που χρησιμοποιούνται για την παραγωγή υπογραφών:

α) να απαντούν 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 ΠΥΠ 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 να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας. Δηλαδή στην ουσία επιβάλλεται η χρήση της 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 να αντιγραφούν από τον φορέα τους, ούτε να ενεργοποιηθούν χωρίς την προηγούμενη χρήση μιας επιπλέον μεθόδου επιβεβαίωσης της ταυτότητας του χρήστη π.χ. με τη χρήση μυστικού κωδικού αναγνώρισης- PIN.

Παράλληλα, η νομοθεσία ορίζει ότι οι ασφαλείς διατάξεις δημιουργίας υπογραφής δεν πρέπει να μεταβάλλουν τα προς υπογραφή δεδομένα, ούτε να εμποδίζουν την εμφάνιση των

δεδομένων αυτών στον υπογράφοντα πριν από τη διαδικασία υπογραφής, αναγνωρίζεται δηλαδή η αρχή 'What You See Is What You Sign' ή 'WYSIWYS'. [26]

6.3.6 Συστάσεις της Οδηγίας για ασφαλή διάταξη επαλήθευσης υπογραφής

Για τη διαδικασία επαλήθευσης της ηλεκτρονικής υπογραφής, η Οδηγία στο **Παράρτημα IV** προβαίνει σε συστάσεις, σύμφωνα με τις οποίες, μια ασφαλής διάταξη επαλήθευσης υπογραφής θα πρέπει να διασφαλίζει με εύλογη βεβαιότητα ότι:

α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα,

β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο,

γ) ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται,

δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία,

ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο,

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς και

ζ) μπορούν να εντοπιστούν τυχόν τροποποιήσεις σχετικά με την ασφάλεια. [26]

6.4 Τεχνικά πρότυπα και η διαδικασία της συν-ρύθμισης

Η Οδηγία ακολουθεί μια τεχνολογικά ουδέτερη στάση, ώστε να επιτρέψει σε νέες τεχνολογίες υπογραφής να αναπτυχθούν, αποφεύγοντας όμως να υποδείξει ένα συγκεκριμένο τύπο υπογραφής, ενώ παράλληλα επιχειρεί να μεγιστοποιήσει τα οφέλη από την εφαρμογή της υπάρχουσας τεχνολογίας. Η συνολική διευθέτηση των ζητημάτων τεχνολογίας και διαδικασιών αντιμετωπίζεται μέσω της διαδικασίας προτυποποίησης, με σκοπό την εξειδίκευση των απαιτήσεων των παραρτημάτων της Οδηγίας και τη διευκρίνιση άλλων επιμέρους ζητημάτων.

Καθώς τα παραρτήματα απλώς θίγουν ορισμένα ζητήματα, ο καθορισμός των τεχνικών προτύπων εφαρμογής, λειτουργίας και ελέγχου των ηλεκτρονικών υπογραφών αφέθηκε στη διαδικασία προτυποποίησης. Επειδή η Οδηγία αφήνει ανοιχτό ένα σημαντικό αριθμό ζητημάτων, η προτυποποίηση θεωρήθηκε από τον ευρωπαϊκό νομοθέτη ότι αποτελεί συνέχεια της νομοθετικής διαδικασίας της Οδηγίας και πρόδρομο άλλων παρόμοιων ενεργειών σε τομείς σχετικούς με τη ρύθμιση της τεχνολογίας στο μέλλον. Η διαδικασία αυτή περιγράφεται με τον όρο ''συν-ρύθμιση'' (co- regulation).

Στην περίπτωση των ηλεκτρονικών υπογραφών η ''συν-ρύθμιση'' επιβλήθηκε στην πράξη και από τις αντίρροπες απόψεις μεταξύ κρατών μελών για το τελικό περιεχόμενο της Οδηγίας, κάτι που γίνεται αντιληπτό και από την ιδιαίτερη και ίσως ιδιοσυγκρασιακή αναφορά σε ζητήματα, όπως για παράδειγμα η προστασία δεδομένων, που απηχεί κεντροευρωπαϊκές απόψεις.

Αναγνωρίζοντας τη δυναμική των τεχνολογικών εξελίξεων, οι σχετικές ρυθμίσεις αφέθηκαν στην πρωτοβουλία που έγινε γνωστή ως European Electronic Signatures Standardization Initiative (EESSI), που σκοπό έχει τον καθορισμό τεχνικών προτύπων και πολιτικών σχετικών με τις ηλεκτρονικές υπογραφές σε εξειδίκευση της Οδηγίας. Οργανωτικά το EESSI χρησιμοποιεί πόρους κα διαδικασίες των ευρωπαϊκών οργανισμών προτυποποίησης CEN/ISSS και ETSI για την εκτέλεση του έργου της προτυποποίησης των ηλεκτρονικών υπογραφών. [20, σελ.114-115]

6.5 Το π.δ. 150/2001

6.5.1 Εισαγωγικές παρατηρήσεις

Το π.δ. 150/2001 προσάρμοσε, όπως έχουμε ήδη αναφέρει, την ελληνική νομοθεσία προς την κοινοτική Οδηγία για τις ηλεκτρονικές υπογραφές. Ο Έλληνας νομοθέτης έμεινε προσηλωμένος στο κείμενο της Οδηγίας, επαναλαμβάνοντας το σχεδόν αυτολεξεί, χωρίς να προβαίνει σε καινοτομικές ρυθμίσεις ή σε κάποιες προσπάθειες προσαρμογής του στις συνήθειες της χώρας μας.

Ο Έλληνας νομοθέτης ρύθμιζε το ζήτημα των ηλεκτρονικών εγγράφων και ηλεκτρονικών υπογραφών και πριν τη δημοσίευση του Π.Δ. 150/2001, κατά τρόπο αποσπασματικό. Έτσι, σύμφωνα με το άρθρο 14 του ν.2672/98, επιτρεπόταν μεν η διακίνηση εγγράφων με ηλεκτρονικά μέσα, όπως ηλεκτρονικό ταχυδρομείο και τηλεομοιοτυπία, μόνο όμως μεταξύ των υπηρεσιών του Δημοσίου, των ΝΠΔΔ και των ΟΤΑ ή μεταξύ αυτών και των ενδιαφερομένων φυσικών προσώπων. Οι διατάξεις αυτές δεν καταργήθηκαν από το Π.Δ. 150/2001, ενώ περαιτέρω του ν.2672/98 εκδόθηκε το Π.Δ. 342/2002 ‘’για τη διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ δημοσίων υπαλλήλων, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων’’.

6.5.2 Περιεχόμενο του π.δ. 150/2001

Σκοπός του προεδρικού διατάγματος 150/2001 σύμφωνα με το **άρθρο 1** παρ.1 είναι η προσαρμογή της ελληνικής νομοθεσίας στις διατάξεις της Οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.

Ρητά ορίζεται όμως στην παρ.2 του αρθ.1 ότι οι διατάξεις του παρόντος Διατάγματος δεν θίγουν διατάξεις που, αναφορικά με τη σύναψη και την 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 αντιστοιχεί προς τη διάταξη του αρθ.1 παρ.2 της Οδηγίας, η οποία αναφέρθηκε στο σχετικό με τις διατάξεις της Οδηγίας κεφάλαιο και έχει σκοπό ν’ αποφευχθούν αντιδράσεις κατά της Οδηγίας, τις οποίες ενδεχομένως θα προκαλούσε η προσπάθεια μετάλλαξης κανόνων του αστικού δικαίου στα κράτη μέλη. Με το π.δ. επιδιώκεται απλώς η εναρμόνιση του εσωτερικού δικαίου προς τις επιταγές της Οδηγίας και όχι η κατάργηση θεμελιωδών κανόνων του.

Το **άρθρο 2** του π.δ. υιοθετεί, ως προς τις ηλεκτρονικές υπογραφές, τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής, τα πιστοποιητικά κλπ, τους ορισμούς που η ίδια η Οδηγία αναφέρει στο άρθρο 2. Υιοθετούνται και οι αυστηρές προϋποθέσεις που η Οδηγία καθιερώνει για τις προηγμένες ηλεκτρονικές υπογραφές, μεταξύ των οποίων περιλαμβάνονται η μονοσήμαντη σύνδεση της υπογραφής με τον υπογράφοντα, η ικανότητά της να προσδιορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντα, η δημιουργία της με μέσα του αποκλειστικού ελέγχου του υπογράφοντα και η σύνδεσή της κατά τέτοιον τρόπο με τα δεδομένα στα οποία αναφέρεται ώστε να είναι εύκολη οποιαδήποτε στιγμή η διαπίστωση ενδεχόμενης αλλοίωσης σε αυτά.

Παράλληλα όμως με την τήρηση αυτών των προϋποθέσεων, η προηγμένη ηλεκτρονική υπογραφή (ψηφιακή) πρέπει να βασίζεται σε αναγνωρισμένο πιστοποιητικό και να δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής για να μπορεί να θεωρηθεί ισότιμη με την ιδιόχειρη υπογραφή. Με τη διάταξη του **άρθρου 3** εξομοιώνεται η προηγμένη ηλεκτρονική υπογραφή προς την ιδιόχειρη και συνεπώς καθίσταται δυνατή η ευθεία εφαρμογή των άρθρων 160 ΑΚ και 443 ΚΠολΔ, όπου γίνεται λόγος για την ιδιόχειρη υπογραφή ως προϋπόθεση της εγκυρότητας των ιδιωτικών εγγράφων και της αποδεικτικής τους ισχύος, αντίστοιχα.

Στο **άρθρο 4** του π.δ. αναφέρονται οι αρχές πρόσβασης στην εσωτερική αγορά. Κατ’ εφαρμογή του αρθ.3 παρ.1 της Οδηγίας 1999/93/ΕΚ, το π.δ. ορίζει ότι οι πάροχοι υπηρεσιών

πιστοποίησης είναι ελεύθεροι να προσφέρουν τις υπηρεσίες τους, χωρίς να απαιτείται προηγούμενη κρατική άδεια. Επομένως, είναι δυνατόν ο οποιοσδήποτε να προσφέρει υπηρεσίες πιστοποίησης. Φυσικά αυτό δε σημαίνει ότι ο πάροχος μπορεί να λειτουργεί ανεξέλεγκτα εφόσον δεν υπάρχει κρατική έγκριση, αλλά θα πρέπει οι υπηρεσίες του να μην παραβιάζουν τους όρους του Παραρτήματος ΙΙ του π.δ. και να φροντίζει ιδιαίτερα για την τήρηση των διατάξεων για την προστασία του ανταγωνισμού, για τον αθέμιτο ανταγωνισμό, για την πνευματική και βιομηχανική ιδιοκτησία και τέλος για την προστασία των καταναλωτών.

Ταυτόχρονα καθιερώνεται ως μηχανισμός εθελοντικής διαπίστευσης η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) ή οριζόμενος από αυτήν δημόσιος ή ιδιωτικός φορέας. Η Ε.Ε.Τ.Τ. ή ο δημόσιος ή ιδιωτικός φορέας που αυτή έχει ορίσει μπορεί να απονέμει δικαιώματα και υποχρεώσεις στον πάροχο υπηρεσιών πιστοποίησης. Οι προϋποθέσεις εθελοντικής διαπίστευσης πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες με τον επιδιωκόμενο σκοπό και να μην οδηγούν σε διακρίσεις. Σε καμία περίπτωση η Ε.Ε.Τ.Τ. δεν δύναται να περιορίσει τον αριθμό των παρόχων υπηρεσιών πιστοποίησης, που επιθυμούν τη διαπίστευσή τους σύμφωνα με τις διατάξεις του παρόντος.

Σε περίπτωση που πάροχος υπηρεσιών πιστοποίησης ενεργεί ως διαπιστευμένος πάροχος υπηρεσιών πιστοποίησης χωρίς να είναι, η Ε.Ε.Τ.Τ. επιβάλλει πρόστιμο από εξήντα χιλιάδες ως τριακόσιες χιλιάδες Ευρώ.

Στο **άρθρο 5** του πδ αναγνωρίζεται η εγκυρότητα υπηρεσιών πιστοποίησης παρεχόμενων από πάροχο εγκατεστημένο σε κράτος μέλος της ΕΕ, όπως επίσης και από πάροχο εγκατεστημένο σε τρίτη χώρα. Ειδικά για υπηρεσίες πιστοποίησης προερχόμενες από κράτος μέλος της ΕΕ δεν επιβάλλονται πρόσθετες προϋποθέσεις: αυτές συνεπάγονται τις ίδιες έννομες συνέπειες με τις αντίστοιχες υπηρεσίες πιστοποίησης τις προσφερόμενες από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Ελλάδα. Τα αναγνωρισμένα πιστοποιητικά που εκδίδονται στο κοινό από πάροχο υπηρεσιών πιστοποίησης, ο οποίος είναι εγκατεστημένος σε χώρα εκτός της Ευρωπαϊκής Ένωσης, είναι νομικώς ισοδύναμα με τα εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Ευρωπαϊκή Ένωση, εφόσον τηρούνται κάποιες προϋποθέσεις. Έτσι πρέπει ο εγκατεστημένος σε Τρίτη χώρα πάροχος να πληροί τους καθοριζόμενους από το πδ όρους και να έχει διαπιστευτεί εθελοντικώς σε οποιοδήποτε κράτος μέλος της Ευρωπαϊκής Ένωσης. Απαιτείται ακόμα για το συγκεκριμένο πιστοποιητικό η εγγύηση παρόχου υπηρεσιών πιστοποίησης εγκατεστημένου σε κράτος μέλος και τέλος πρέπει το αναγνωρισμένο πιστοποιητικό να αναγνωρίζεται βάσει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και τρίτων χωρών ή διεθνών οργανισμών.

Στο **άρθρο 6** του πδ ρυθμίζεται η ευθύνη του παρόχου υπηρεσιών πιστοποίησης. Ο πάροχος υπηρεσιών πιστοποίησης, διαπιστευμένος ή μη, εφόσον εκδίδει αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυάται για την ακρίβεια ενός τέτοιου πιστοποιητικού, ευθύνεται έναντι οποιουδήποτε φυσικού ή νομικού προσώπου για κάθε ζημία που ενδεχομένως προκληθεί σε βάρος του, επειδή το πρόσωπο αυτό βασίστηκε στο πιστοποιητικό, όσον αφορά:

α) στην ακρίβεια, κατά τη στιγμή της έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και στην ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοσή του,

β) στη διαβεβαίωση ότι ο υπογράφων, η ταυτότητα του οποίου βεβαιώνεται στο αναγνωρισμένο πιστοποιητικό, κατά τη στιγμή της έκδοσής του, κατείχε δεδομένα δημιουργίας υπογραφής, τα οποία αντιστοιχούσαν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό ως δεδομένα επαλήθευσης της υπογραφής και

γ) στη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, εφόσον προέρχονται από πάροχο υπηρεσιών πιστοποίησης.

Ο παρόχος υπηρεσιών πιστοποίησης ευθύνεται επίσης αν παραλείψει να καταγράψει την ανάκληση του πιστοποιητικού.

Σε όλες τις παραπάνω περιπτώσεις ο πάροχος δεν ευθύνεται, αν αποδείξει ότι δεν τον βαρύνει πταίσμα.

Ο πάροχος έχει ακόμα τη δυνατότητα να θέσει περιορισμούς χρήσης του πιστοποιητικού και να καθορίσει όρια για το ύψος των συναλλαγών. Οπωσδήποτε όμως πρέπει αυτοί οι περιορισμοί να είναι σαφώς αναγνωρίσιμοι στους τρίτους και να μην αντιτίθονται στις

διατάξεις για την προστασία των καταναλωτών. Ο πάροχος δεν ευθύνεται για την προκληθείσα από την υπέρβαση των αναφερόμενων περιορισμών ζημία.

Το **άρθρο 7** του π.δ. εξασφαλίζει την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα ο πάροχος των υπηρεσιών πιστοποίησης που εκδίδει το πιστοποιητικό, μπορεί να συγκεντρώνει δεδομένα προσωπικού χαρακτήρα για την έκδοση πιστοποιητικών μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή κατόπιν ρητής συγκατάθεσής του και μόνο στο βαθμό που είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού. Η συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς απαγορεύεται, χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου. Επίσης στους παρόχους υπηρεσιών πιστοποίησης επιτρέπεται να αναγράφουν στο αναγνωρισμένο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος.

Η Ευρωπαϊκή Επιτροπή ενημερώνεται το ταχύτερο δυνατόν, σύμφωνα με το **άρθρο 8** του π.δ., από την Γενική Γραμματεία Επικοινωνιών του Υπουργείου Μεταφορών και Επικοινωνιών για την εφαρμογή των διατάξεων του άρθρου 4 του π.δ. και από την Ε.Ε.Τ.Τ για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης. Οποιεσδήποτε αλλαγές των παραπάνω πληροφοριών ανακοινώνονται άμεσα στην Επιτροπή από τα ανωτέρω όργανα.

Τέλος, το **άρθρο 9** του π.δ. περιλαμβάνει τους όρους ισχύοντες για τα αναγνωρισμένα πιστοποιητικά (Παράρτημα Ι), τους όρους ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν τα αναγνωρισμένα πιστοποιητικά (Παράρτημα ΙΙ), τη διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής (Παράρτημα ΙΙΙ) και τέλος τις συστάσεις για την ασφαλή επαλήθευση της υπογραφής (Παράρτημα). [25]

6.6 Απόφαση 248/71/15-3-2002

Η Απόφαση 248/71/2002 με τίτλο ‘’Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής ‘’ ρυθμίζει τη λειτουργία των παρόχων ηλεκτρονικής υπογραφής που είναι εγκατεστημένοι στην Ελλάδα. Ο σκοπός της Απόφασης σύμφωνα με το **άρθρο 1** της απόφασης 248/71 είναι η ρύθμιση θεμάτων σχετικά με (α) την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, (β) ζητήματα Αναγνωρισμένων Πιστοποιητικών και (γ) την εποπτεία και τον έλεγχο παρόχων υπηρεσιών πιστοποίησης με εγκατάσταση στην Ελλάδα που εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά ή παρέχουν άλλες υπηρεσίες πιστοποίησης σχετικές με την ηλεκτρονική υπογραφή.

Σύμφωνα με τον ορισμό που δίνεται στο **άρθρο 2** της Απόφασης, ‘’Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης’’ είναι έγγραφο του Παρόχου Υπηρεσιών Πιστοποίησης, στο οποίο περιγράφεται αναλυτικά η πρακτική που ακολουθεί για την έκδοση πιστοποιητικών ηλεκτρονικής υπογραφής ή την παροχή άλλων Υπηρεσιών Πιστοποίησης, σύμφωνα με τα αναφερόμενα στο Παράρτημα Ι του παρόντος.

Η Απόφαση, σύμφωνα με το **άρθρο 3**, αναγνωρίζει ότι η παροχή υπηρεσιών πιστοποίησης οποιασδήποτε μορφής είναι ελεύθερη και δεν υπάγεται σε προηγούμενη άδεια ή έγκριση. Κάθε Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να εκδίδει Αναγνωρισμένα Πιστοποιητικά αποκλειστικά και μόνον εφόσον ισχύουν οι παρακάτω προϋποθέσεις:

- πληροί τους όρους του Παραρτήματος ΙΙ του π.δ. 150/2001,
- τηρεί κατά την έκδοση των πιστοποιητικών τους όρους του Παραρτήματος Ι του π.δ.150/2001 και
- δηλώνει την ανωτέρω υπό στοιχεία (α) και (β) συμμόρφωσή του, σύμφωνα με το άρθρο 10, παράγρ.3.

Ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος εκδίδει Αναγνωρισμένα Πιστοποιητικά πρέπει να είναι σε θέση να αποδείξει ότι κατά την έκδοση των Αναγνωρισμένων Πιστοποιητικών συμμορφώνεται πλήρως με τα Παραρτήματα Ι και ΙΙ του π.δ. 150/2001, δηλαδή σχετικά με τους όρους που ισχύουν για τα αναγνωρισμένα πιστοποιητικά και για τους όρους που ισχύουν για τους παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά.

Σύμφωνα με το **άρθρο 4**, οι δικαιούχοι αναγνωρισμένων πιστοποιητικών πρέπει:

(α) να είναι μόνο φυσικά πρόσωπα, τα οποία έχουν δικαιοπρακτική ικανότητα,

(β) να κατέχουν τα δεδομένα δημιουργίας της ηλεκτρονικής υπογραφής (ιδιωτικό κλειδί) που συνδέονται με το πιστοποιητικό τους,

(γ) να επιδεικνύουν κάθε αναγκαία επιμέλεια για την ασφαλή τήρηση των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής και του πιστοποιητικού (ώστε το ιδιωτικό κλειδί να παραμένει εντός της ασφαλούς διάταξης δημιουργίας της ηλεκτρονικής υπογραφής) και τέλος

(δ) να ειδοποιούν άμεσα τον Πάροχο Υπηρεσιών Πιστοποίησης σε περίπτωση απώλειας των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής ή στην περίπτωση που αυτά περιέλθουν στην κατοχή ή γνώση τρίτου. [21]

Από τη διατύπωση του άρθρου αυτού είναι δύσκολο να κατανοήσει κανείς το ζήτημα της επιμέλειας τήρησης του πιστοποιητικού, καθώς το περιεχόμενο του πιστοποιητικού συνήθως δεν είναι εμπιστευτικό και η χρήση του εξαρτάται επίσης από τις εφαρμογές στις οποίες χρησιμοποιείται. Οι πάροχοι εφαρμογών ηλεκτρονικής υπογραφής όμως δεν υπόκεινται σε έλεγχο σχετικά με την επεξεργασία που τυχόν υφίστανται τα πιστοποιητικά των τελικών χρηστών εντός των εφαρμογών που διαθέτουν στον τελικό χρήστη, ζήτημα το οποίο εμπίπτει στον τομέα ευθύνης του παρόχου υπηρεσιών εφαρμογής.

Επιπλέον, αυτή η ρύθμιση ενδέχεται να δυσχεράνει τη χρήση ηλεκτρονικών υπογραφών σε αυτοματοποιημένες συναλλαγές, καθώς ενδέχεται να απαιτηθεί αυξημένη συμβατική αντιμετώπιση του ζητήματος μεταξύ του οργανισμού που χρησιμοποιεί αυτοματοποιημένες συναλλαγές (π.χ. τραπεζικές συναλλαγές, έκδοση ηλεκτρονικών τιμολογίων κλπ) και του υπογράφοντα εκπροσώπου του οργανισμού. Αυτό θα συμβεί γιατί καθώς ο εκπρόσωπος του οργανισμού θα πρέπει να υπογράφει εξερχόμενα έγγραφα, η επεξεργασία των εγγράφων αυτών θα πρέπει να τίθεται σε ένα προς ένα τα έγγραφα αυτά ξεχωριστά, δυσχεραίνοντας όμως την αυτοματοποιημένη επεξεργασία, καθώς το ιδιωτικό κλειδί μιας αναγνωρισμένης υπογραφής δεν μπορεί να χρησιμοποιηθεί παρά μόνο μέσω της ασφαλούς διάταξης.

Το άρθρο αυτό θα μπορούσε να βελτιωθεί με τη διευκρίνιση ότι πρέπει να γίνεται διάκριση μεταξύ του τελικού δικαιούχου και συνδρομητή της υπηρεσίας. [20, σελ.120],[22]

Με το **άρθρο 5**, ο Πάροχος Υπηρεσιών Πιστοποίησης είναι υποχρεωμένος να προβεί σε άμεση ανάκληση ενός Αναγνωρισμένου Πιστοποιητικού, στις εξής περιπτώσεις:

- μετά από αίτηση του δικαιούχου του πιστοποιητικού ή του νομίμως εξουσιοδοτημένου από αυτόν ατόμου,
- εφόσον διαπιστωθεί από την ΕΕΤΤ, στα πλαίσια της εποπτικής και ελεγκτικής της αρμοδιότητας, ότι το Αναγνωρισμένο Πιστοποιητικό περιέχει ψευδείς ή ανακριβείς πληροφορίες ως προς το Παράρτημα Ι του π.δ.150/2001,
- σε περίπτωση πιστοποιητικού η έκδοση του οποίου βασίστηκε σε ψευδείς ή ανακριβείς πληροφορίες,
- σε περίπτωση παύσης εργασιών του Παρόχου Υπηρεσιών Πιστοποίησης, σύμφωνα με το άρθρο 6 του παρόντος,
- σε περίπτωση απώλειας της δικαιοπρακτικής ικανότητας, κήρυξης σε αφάνεια ή σε περίπτωση θανάτου του δικαιούχου του πιστοποιητικού, λαμβάνοντας υπόψη ότι κάθε πιστοποιητικό είναι αμεταβίβαστο σε κάθε περίπτωση,
- σε περίπτωση που τελεσίδικη δικαστική απόφαση προστάζει τη σχετική ανάκληση ή ακύρωση,

  αν από την μεταξύ σύμβαση Παρόχου Υπηρεσιών Πιστοποίησης και χρήστη, απορρέει σχετική προς αυτό υποχρέωση ή και δικαίωμα, ενός των συμβαλλομένων μερών. Στην περίπτωση αυτή, αν το αίτημα για ανάκληση τεθεί από τον δικαιούχο πιστοποιητικού, ο Πάροχος Υπηρεσιών Πιστοποίησης υποχρεούται να προβεί σε άμεση ανάκληση, δικαιούμενος να επιφυλαχθεί για κάθε νόμιμο ή συμβατικό του δικαίωμα,
- σε περίπτωση που υπάρχουν ενδείξεις ότι τα δεδομένα δημιουργίας υπογραφής του δικαιούχου του πιστοποιητικού έχουν γίνει γνωστά ή χρησιμοποιούνται από τρίτους,
- σε περίπτωση κατά την οποία τα δεδομένα δημιουργίας υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης έχουν γίνει γνωστά σε τρίτους,

- σε περίπτωση κατά την οποία ο δικαιούχος πιστοποιητικού, το οποίο χρησιμοποιεί με συγκεκριμένη ιδιότητα, χάσει την ιδιότητα αυτή (π.χ. σε περίπτωση αποχώρησης εργαζομένου στον οποίο έχει εκδοθεί τέτοιο πιστοποιητικό με την ιδιότητα ως υπαλλήλου συγκεκριμένης υπηρεσίας ή θέσης) ή σε κάθε περίπτωση κατά την οποία στοιχεία που περιλαμβάνονται στο πιστοποιητικό τροποποιηθούν.

Ο Πάροχος Υπηρεσιών Πιστοποίησης δικαιούται, μέχρι την εξακρίβωση και επιβεβαίωση ή όχι των λόγων ανάκλησης πιστοποιητικού, να προβεί σε άμεση αναστολή του.

Σε κάθε περίπτωση, ο Πάροχος Υπηρεσιών Πιστοποίησης πρέπει να ενημερώσει αμέσως τους δικαιούχους ηλεκτρονικών πιστοποιητικών για την αναστολή ή ανάκληση τους και να είναι σε θέση να αποδείξει ότι τους έχει ενημερώσει.

Ο Πάροχος Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών παρέχει υπηρεσία ενημέρωσης σχετικά με την κατάσταση (ισχύ, ανάκληση) των πιστοποιητικών, η οποία λειτουργεί επί 24 ώρες την ημέρα και επί 7 ημέρες την εβδομάδα συμπεριλαμβανομένων αργιών, στην οποία οι κάτοχοι Αναγνωρισμένων Πιστοποιητικών ή και τα νομίμως εξουσιοδοτημένα από αυτούς πρόσωπα, μπορούν να υποβάλουν αίτημα ανάκλησης. Σε κάθε περίπτωση, πριν από την ανάκληση, ο Πάροχος Υπηρεσιών Πιστοποίησης επαληθεύει ότι το αίτημα υποβάλλεται από πρόσωπο που νομιμοποιείται προς αυτό.

Οι αιτήσεις ανάκλησης Αναγνωρισμένων Πιστοποιητικών πρέπει να τυγχάνουν άμεσης επεξεργασίας.

Ο ΠΥΠ διατηρεί μια λίστα ανακληθέντων πιστοποιητικών, στην οποία εγγράφει τα ανακληθέντα ή υπό αναστολή πιστοποιητικά.

Η λίστα αυτή υποχρεωτικά:

α. εκδίδεται, κατ' ελάχιστον, μία φορά ημερησίως,

β. αναγράφει την ώρα της επόμενης ενημέρωσής της,

γ. είναι δυνατόν να ενημερώνεται πριν από την ώρα επόμενης ενημέρωσής της,

δ. περιλαμβάνει, κατ' ελάχιστον, την ημερομηνία, το χρόνο της ανάκλησης, την κατάσταση του πιστοποιητικού (σε αναστολή ή ανάκληση) και τον κωδικό ταυτοποίησης του πιστοποιητικού,

ε. είναι προσπελάσιμη ατελώς από τους δικαιούχους πιστοποιητικών ή τρίτους

Ο Πάροχος Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών υποχρεούται να διασφαλίζει ότι τα αιτήματα για ανάκληση μπορούν να γίνουν και τηλεφωνικά και υποχρεώνεται να ενημερώνει τους δικαιούχους των πιστοποιητικών για αυτό, γνωστοποιώντας τους το σχετικό αριθμό τηλεφώνου.

Ο δικαιούχος πιστοποιητικού πρέπει να γνωρίζει ότι μετά την ανάκληση του πιστοποιητικού δεν είναι δυνατό να επανατεθεί σε ισχύ ξανά. [21]

Σχετικά με την παύση Εργασιών Παροχών Υπηρεσιών Πιστοποίησης του **άρθρου 6,** ο Πάροχος Υπηρεσιών Πιστοποίησης έχει τις ακόλουθες υποχρεώσεις:

- γνωστοποιεί την παύση προς την ΕΕΤΤ, τους δικαιούχους των Πιστοποιητικών και κάθε Πάροχο Υπηρεσιών Πιστοποίησης ή άλλον με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στα πλαίσια της παροχής υπηρεσιών πιστοποίησης εντός αποκλειστικής προθεσμίας τριών μηνών πριν από την επέλευσή της,
- σε περιπτώσεις για τις οποίες προϋποτίθεται η έκδοση δικαστικής απόφασης για την επέλευση της παύσης των εργασιών του Παρόχου Υπηρεσιών Πιστοποίησης, ο τελευταίος οφείλει να ενημερώσει την ΕΕΤΤ από την επομένη της επίδοσης στον Πάροχο Υπηρεσιών Πιστοποίησης σχετικού με την παύση εργασιών του,
- σε περίπτωση αποδεδειγμένης αδυναμίας του Παρόχου Υπηρεσιών Πιστοποίησης να γνωστοποιήσει την παύση στην ΕΕΤΤ πριν από την επέλευσή της, ο Πάροχος Υπηρεσιών Πιστοποίησης υποχρεούται να γνωστοποιήσει την παύση αμέσως μόλις λάβει γνώση αυτής,
- σε κάθε περίπτωση, ο Πάροχος Υπηρεσιών Πιστοποίησης φέρει το βάρος απόδειξης γνωστοποίησης της παύσης των εργασιών του στην ΕΕΤΤ, στους δικαιούχους των πιστοποιητικών και σε κάθε Πάροχο Υπηρεσιών Πιστοποίησης ή άλλον με τον οποίο

έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στα πλαίσια της παροχής υπηρεσιών πιστοποίησης,

- σε κάθε περίπτωση και σε συνέχεια της ενημέρωσης, ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει άμεσα στην ακύρωση όλων των σε ισχύ πιστοποιητικών, εκτός αν άλλος έχει προβλεφθεί στην μεταξύ αυτού και του δικαιούχου σύμβαση ή σε τυχόν τροποποίηση αυτής, και στη Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης,
- ο Πάροχος Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών, σε κάθε περίπτωση, υποχρεούται να έχει ήδη συμφωνήσει εγγράφως με άλλον Πάροχο Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών, για την παράδοση στον τελευταίο του αρχείου που τηρεί σύμφωνα με το άρθρο 7 και ο οποίος το παραλαμβάνει και το διατηρεί για χρόνο που προβλέπεται στο εδάφιο θ του Παραρτήματος ΙΙ του π.δ. 150/2001. Η μη τήρηση αυτής της υποχρέωσης συνεπάγεται την επιβολή των κυρώσεων που προβλέπονται στην παρούσα. Ο Πάροχος Υπηρεσιών Πιστοποίησης, ο οποίος σύμφωνα με τα ανωτέρω παραλαμβάνει και διατηρεί το αρχείο Παρόχου Υπηρεσιών Πιστοποίησης λόγω την παύσης εργασιών του τελευταίου, οφείλει εντός επτά ημερών από την ανάληψη του αρχείου να κοινοποιεί εγγράφως στην ΕΕΤΤ το γεγονός αυτό. Σε περίπτωση μη εφαρμογής των ανωτέρω και χωρίς περιορισμό τους, ο Πάροχος Υπηρεσιών Πιστοποίησης του οποίου οι εργασίες παύουν, παραδίδει τα εν λόγω έγγραφα και στοιχεία προς φύλαξη στην ΕΕΤΤ, ενημερώνοντας σχετικά τους δικαιούχους πιστοποιητικών. Η ΕΕΤΤ μπορεί να αναθέσει τη φύλαξη των ανωτέρω αρχείων σε Παρόχους Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών,
- σε κάθε περίπτωση, οι τυχόν συμβάσεις ανάθεσης σε τρίτους εκτέλεσης μέρους της διαδικασίας πιστοποίησης, λήγουν αυτοδικαίως με την παύση εργασιών του Παρόχου Υπηρεσιών Πιστοποίησης. Για το σκοπό αυτό, οι συμβάσεις οι οποίες υπογράφονται μεταξύ Παρόχου Υπηρεσιών Πιστοποίησης και τρίτων, περιλαμβάνουν όρο ο οποίος προβλέπει, επί ποινή ακυρότητας όλης της σύμβασης, την αυτοδίκαιη λύση της σε περίπτωση παύσης εργασιών του Παρόχου Υπηρεσιών Πιστοποίησης,
- ο Πάροχος Υπηρεσιών Πιστοποίησης υποχρεούται να έχει ρυθμίσει την οικονομική κάλυψη κάθε απαιτούμενης διαδικασίας και εκπλήρωσης υποχρεώσεων που προκύπτουν από την παύση των εργασιών του καθώς και ενδεχόμενης ζημίας που τυχόν προκληθεί σε δικαιούχους πιστοποιητικών ή τρίτους από ενέργεια ή παράλειψή του, κατά την άσκηση των δραστηριοτήτων του, και ειδικότερα, συνεπεία της παύσης εργασιών του. Ο Πάροχος Υπηρεσιών Πιστοποίησης οφείλει να είναι σε θέση να αποδείξει στην ΕΕΤΤ και σε οποιονδήποτε έχει έννομο συμφέρον ότι έχει προβλέψει επαρκώς για την ως άνω αναφερόμενη οικονομική κάλυψη. Η ΕΕΤΤ με απόφασή της μπορεί να ρυθμίσει ελάχιστο ποσό για την οικονομική και ασφαλιστική κάλυψη των ανωτέρω από τους Παρόχους Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών.

Σύμφωνα με το **άρθρο 7**, κάθε Πάροχος Υπηρεσιών Πιστοποίησης τηρεί σε έντυπη ή σε ηλεκτρονική μορφή αρχείο με το σύνολο των πληροφοριών σχετικά με τα Αναγνωρισμένα Πιστοποιητικά που εκδίδει ή διαχειρίζεται, και ιδιαίτερα όσον αφορά το χρόνο έκδοσης, ακύρωσης ή αναστολής και λήξης τους προκειμένου να καθίσταται δυνατή η επιβεβαίωση της ορθότητας και της ακρίβειάς τους.

Το αρχείο για κάθε Αναγνωρισμένο Πιστοποιητικό τηρείται από την έκδοσή του και για χρονική περίοδο τριάντα ετών από τη λήξη ή ανάκλησή του.

Αμέσως μετά την έκδοσή του, κάθε Αναγνωρισμένο Πιστοποιητικό καταχωρείται σε ηλεκτρονική μορφή στο αρχείο, κατά τέτοιο τρόπο ώστε να καθίσταται δυνατός ο εντοπισμός οποιασδήποτε μεταγενέστερης αλλοίωσής του. Η ΕΕΤΤ δύναται με απόφασή της να ρυθμίσει τη διαδικασία που αφορά τον εντοπισμό τέτοιας αλλοίωσης.

Η ΕΕΤΤ δύναται με απόφασή της να ρυθμίζει τα σχετικά με τη διαχείριση του αρχείου του Παρόχου Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών.

Ο Πάροχος Υπηρεσιών Πιστοποίησης παρέχει στο δικαιούχο του πιστοποιητικού πρόσβαση στα δεδομένα που τον αφορούν, κατόπιν υποβολής σχετικού αιτήματός του, στο

οποίο ο Πάροχος υποχρεούται να απαντήσει εντός αποκλειστικής προθεσμίας επτά ημερών από την ημερομηνία υποβολής του αιτήματός του.

Το **άρθρο 8**, προβλέπει την υποχρέωση του παρόχου πριν από τη σύναψη σύμβασης με πρόσωπο που αιτείται πιστοποιητικό, να το ενημερώνει για:

α) την ευθύνη και τις υποχρεώσεις του δικαιούχου πιστοποιητικού που απορρέουν από τη χρήση αυτού,

β) τις υποχρεώσεις του δικαιούχου πιστοποιητικού για την αποθήκευση και προστασία των δεδομένων δημιουργίας υπογραφής του,

γ) τις συνέπειες για τον δικαιούχο πιστοποιητικού από την δημοσιοποίηση των δεδομένων δημιουργίας υπογραφής του,

δ) την πολιτική της πιστοποίησης και τη Δήλωση Πρακτικής Πιστοποίησης του Παρόχου Υπηρεσιών Πιστοποίησης και οποιαδήποτε τυχόν τροποποίηση αυτών,

ε) τις προϋποθέσεις και τη διαδικασία ανάκλησης και αναστολής των πιστοποιητικών,

στ) τις προβλεπόμενες ρυθμίσεις του Παρόχου Υπηρεσιών Πιστοποίησης, στην περίπτωση παύσης των εργασιών του. [21]

Η ΕΕΤΤ ασκεί την εποπτεία και τον έλεγχο όλων των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, σύμφωνα με το **άρθρο 9**.

Το άρθρο 10 της Απόφασης αναφέρεται στην τήρηση Μητρώου από την ΕΕΤΤ των παρόχων που είναι εγκαταστημένοι στην Ελλάδα σε ηλεκτρονική ή και έντυπη μορφή. Κατά την έναρξη των εργασιών του, κάθε εγκατεστημένος στην Ελλάδα Πάροχος Υπηρεσιών Πιστοποίησης γνωστοποιεί εγγράφως στοιχεία στην ΕΕΤΤ, τα οποία καταχωρούνται στο Μητρώο όπως ονοματεπώνυμο/επωνυμία, διεύθυνση/έδρα, τηλέφωνο, φαξ, διεύθυνση ηλεκτρονικού ταχυδρομείου, ιστοσελίδα του Παρόχου, νομική μορφή, νόμιμοι εκπρόσωποι και τυχόν αντίκλητος του Παρόχου, ΑΦΜ του Παρόχου καθώς και άλλες τυχόν παρεχόμενες υπηρεσίες.

Σε περίπτωση Παρόχων Υπηρεσιών Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά, μαζί με την γνωστοποίηση προσκομίζονται:

α) δήλωση του Παρόχου Υπηρεσιών Πιστοποίησης ότι συμμορφώνεται προς τα Παραρτήματα Ι και ΙΙ του π.δ. 150/2001,

β) Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης,

γ) έγγραφα με τα οποία αποδεικνύει την οικονομική κάλυψη,

δ) πιστοποιητικά εκδοθέντα από τις αρμόδιες Δημόσιες ή Δικαστικές Υπηρεσίες από τα οποία να προκύπτει αν τελεί υπό πτώχευση, πτωχευτικό συμβιβασμό, αναγκαστική διαχείριση ή αν έχουν κατατεθεί σχετικές προς αυτά αιτήσεις καθώς και αν τελεί υπό εκκαθάριση και τα οποία οφείλει να ανανεώνει και να υποβάλλει στην ΕΕΤΤ ανά 3 μήνες. Στο μητρώο που τηρείται στην ΕΕΤΤ, σημειώνεται ότι πρόκειται για Πάροχο Υπηρεσιών Πιστοποίησης που, κατά δήλωσή του, εκδίδει Αναγνωρισμένα Πιστοποιητικά.

Για την καταχώρηση των ανωτέρω στοιχείων στο μητρώο, επιβάλλεται τέλος καταχώρησης, ύψους τριακοσίων Ευρώ, το οποίο καταβάλλεται με τη γνωστοποίηση.

Οι Πάροχοι Υπηρεσιών Πιστοποίησης υποχρεούνται να γνωστοποιούν στην ΕΕΤΤ κάθε τροποποίηση των στοιχείων τους που περιλαμβάνονται στο μητρώο εντός αποκλειστικής προθεσμίας επτά ημερών από την επέλευσή της. Για κάθε γνωστοποίηση τροποποίησης στοιχείων, οι Πάροχοι Υπηρεσιών Πιστοποίησης καταβάλλουν στην ΕΕΤΤ τέλος τροποποίησης ύψους εκατό ευρώ. Ενώ για την παύση εργασιών καταβάλλουν στην ΕΕΤΤ τέλος τριακοσίων ευρώ. Η παύση αυτή σημειώνεται στο μητρώο. [21]

Οι Πάροχοι Υπηρεσιών Πιστοποίησης, σύμφωνα με το **άρθρο 11**, υποβάλλουν στην ΕΕΤΤ ετήσιες εκθέσεις με περιγραφή των δραστηριοτήτων τους. Ιδιαίτερη έμφαση δίνεται σε αιτήματα και καταγγελίες δικαιούχων ή τρίτων που τους έχουν υποβληθεί. Οι εκθέσεις υποβάλλονται έως τα τέλη Μαρτίου κάθε έτους, αρχής γενομένης από το Μάρτιο 2003.

Σε περίπτωση Παρόχων Υπηρεσιών Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά, οι εκθέσεις αυτές περιλαμβάνουν τουλάχιστον τα εξής στοιχεία:

α. περιγραφή των εγκαταστάσεων και όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων ασφαλείας και της καταλληλότητάς τους,

β. κατάλογο των προϊόντων που χρησιμοποιούνται για τη δημιουργία ψηφιακών υπογραφών,

γ. προβλεπόμενα μέτρα ασφαλείας προκειμένου να διατηρηθούν σε συνεχή λειτουργία οι παρεχόμενες υπηρεσίες, ιδίως σε καταστάσεις έκτακτης ανάγκης,

δ. μέτρα προστασίας αρχείων και δεδομένων,

ε. περιγραφή των διαδικασιών εξασφάλισης της αξιοπιστίας του απασχολημένου προσωπικού, στ. αντίγραφο της τυποποιημένης Σύμβασης την οποία ο Πάροχος Υπηρεσιών Πιστοποίησης συνάπτει με τους δικαιούχους ηλεκτρονικών πιστοποιητικών ή άλλων υπηρεσιών καθώς και κάθε σχετικό διέπουν τη Σύμβαση έγγραφο. Η ΕΕΤΤ ελέγχει αν οι όροι της Σύμβασης είναι συμβατοί ή όχι με τις διατάξεις περί γενικών όρων συναλλαγών και με τους όρους και διατάξεις του Ν. 2251/1994, όπως εκάστοτε ισχύει. Αν κατά τον έλεγχο, διαπιστωθεί από την ΕΕΤΤ ότι υφίστανται όροι μη νόμιμοι ή και καταχρηστικοί κατά τα ως άνω, εντός αποκλειστικής προθεσμίας εξήντα ημερών από την κατάθεση του Παρόχου Υπηρεσιών Πιστοποίησης στην ΕΕΤΤ των δικαιολογητικών, η ΕΕΤΤ αποστέλλει τις παρατηρήσεις της στον Πάροχο Υπηρεσιών Πιστοποίησης προκειμένου εκείνος να τροποποιήσει την Σύμβασή του.

Ο Πάροχος Υπηρεσιών Πιστοποίησης υποχρεούται εντός αποκλειστικής προθεσμίας δέκα πέντε ημερών να κοινοποιήσει στην ΕΕΤΤ την τροποποιηθείσα Σύμβαση. Σε περίπτωση κατά την οποία η ως άνω προθεσμία εξήντα ημερών παρέλθει άπρακτος, δηλαδή χωρίς κοινοποίηση στον Πάροχο Υπηρεσιών Πιστοποίησης παρατηρήσεων σχετικά με τους όρους της Σύμβασης, αυτή θεωρείται εγκριθείσα.

ζ. κείμενα τα οποία να περιγράφουν την πολιτική και την πρακτική του Παρόχου Υπηρεσιών Πιστοποίησης. Η Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης θα πρέπει να περιλαμβάνει τουλάχιστον τα στοιχεία που αναφέρονται στο Παράρτημα Ι του παρόντος.

Οποτεδήποτε τροποποιηθούν στοιχεία Παρόχου Υπηρεσιών Πιστοποίησης που εκδίδει Αναγνωρισμένα Πιστοποιητικά ο Πάροχος Υπηρεσιών Πιστοποίησης υποχρεούται να κοινοποιεί τις τροποποιήσεις αυτές στην ΕΕΤΤ.

Ο Πάροχος Υπηρεσιών Πιστοποίησης παραμένει αποκλειστικά υπεύθυνος απέναντι στους δικαιούχους πιστοποιητικών ή τρίτων για πράξεις ή παραλείψεις των ως άνω αναδόχων. Ο Πάροχος Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών υποχρεούται να μεριμνά ώστε η κατά τα ως άνω ανάθεση σε οποιονδήποτε τρίτον να μην αντιβαίνει στις προϋποθέσεις έκδοσης των Αναγνωρισμένων Πιστοποιητικών, σύμφωνα με το Προεδρικό Διάταγμα 150/2001 και τον παρόντα Κανονισμό. [21]

Κατά το **άρθρο 12**, η ΕΕΤΤ αυτεπαγγέλτως ή κατόπιν καταγγελίας, δύναται να προβαίνει σε έλεγχο της συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης. Η ΕΕΤΤ ή οριζόμενοι από την ΕΕΤΤ φορείς έχουν το δικαίωμα να ζητούν στοιχεία και να προβαίνουν σε επιθεωρήσεις στους χώρους εγκαταστάσεως και λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης, σύμφωνα με την κείμενη νομοθεσία, οι οποίοι υποχρεούνται να συνεργάζονται με την ΕΕΤΤ και να της παρέχουν κάθε πληροφορία και διευκόλυνση για την πραγματοποίηση των ελέγχων.[21]

6.7 Ελάχιστο περιεχόμενο της Δήλωσης Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης

Σύμφωνα με το **Παράρτημα Ι του κανονισμού** η Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης που εκδίδει Αναγνωρισμένα Πιστοποιητικά πρέπει να αναλύει τουλάχιστον τα εξής θέματα:

1. παρεχόμενες Υπηρεσίες Πιστοποίησης,

2. μηχανισμοί ασφαλείας για το προσωπικό, τις διαδικασίες και την φυσική ασφάλεια,

3. ευθύνη και υποχρεώσεις Παρόχου Υπηρεσιών Πιστοποίησης έναντι των δικαιούχων ή χρηστών ή συνδρομητών, δικαιώματα και υποχρεώσεις τους σχετικά με τη χρήση των πιστοποιητικών και παρεχόμενων διατάξεων δημιουργίας υπογραφής,

4. εξωτερικοί συνεργάτες/φορείς στους οποίους ανατίθεται μέρος της διαδικασίας παροχής Υπηρεσιών Πιστοποίησης,

5. υλικοτεχνική υποδομή, χρησιμοποιούμενα προϊόντα,

6. διαδικασίες για την προστασία απορρήτου και επεξεργασία προσωπικών δεδομένων,

7. διαδικασίες για την προστασία καταναλωτή

8. ασφαλιστική κάλυψη/ευθύνη έναντι τρίτων,

9. διαδικασίες που ακολουθούνται σχετικά με την ανάκληση ενός πιστοποιητικού,

10. διαδικασίες εξασφάλισης κάλυψης πάσης φύσεως υποχρέωσης του Παρόχου Υπηρεσιών Πιστοποίησης μετά την τυχόν παύση των εργασιών του,

11. διαδικασίες για την εκπλήρωση υποχρεώσεων του Παρόχου Υπηρεσιών Πιστοποίησης για και μετά την παύση των εργασιών του, και

12. διαδικασίες για τη διατήρηση, διαχείριση του αρχείου του καθώς και την ανάθεση του αρχείου του σε περίπτωση παύσης των εργασιών του. [21]

6.8 Το π.δ. 342/2002

Το Προεδρικό Διάταγμα ρυθμίζει τους όρους για ‘’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’’.

Το π.δ. 342/2002, σύμφωνα με το **άρθρο 1** ,αποφάσισε να διακινούνται οι αποφάσεις, τα πιστοποιητικά και οι βεβαιώσεις με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α, ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου εφόσον φέρουν ψηφιακή υπογραφή.

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

Σύμφωνα με το **άρθρο 2**, η διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο χωρίς ψηφιακή υπογραφή, επιτρέπεται και έχει ισχύ μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α. ή μεταξύ αυτών και φυσικών ή νομικών προσώπων ιδιωτικού δικαίου, αν δεν συνδέεται με την παραγωγή εννόμων αποτελεσμάτων ή με την άσκηση δικαιώματος, ιδίως όταν έχουν ως περιεχόμενο ερωτήματα, εγκυκλίους, οδηγίες, μελέτες, στατιστικά στοιχεία, αιτήσεις παροχής πληροφοριών και σχετικές απαντήσεις.

Για την εφαρμογή του παρόντος προεδρικού διατάγματος, σύμφωνα με το **άρθρο 3**, ισχύουν οι ορισμοί και οι έννομες συνέπειες των ηλεκτρονικών υπογραφών όπως ορίζονται στα άρθρα 2 και 3 αντίστοιχα του π.δ. 150/2001.

Για τη διακίνηση μηνυμάτων με ηλεκτρονικό ταχυδρομείο, κατά τις διατάξεις του άρθρου 1 του παρόντος π.δ., σύμφωνα με το **άρθρο 4**, ισχύουν οι διατάξεις του π.δ. 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 και τη διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής.[24]

Κεφάλαιο 7

7.1 Ευρωπαϊκές εφαρμογές των ηλεκτρονικών υπογραφών

Ένας πρώτος σημαντικός τομέας εφαρμογής των ηλεκτρονικών υπογραφών είναι τα ηλεκτρονικά τιμολόγια. Σύμφωνα με την Ευρωπαϊκή Οδηγία 115 της 20ης Δεκεμβρίου 2001, η χρησιμοποίηση ηλεκτρονικής υπογραφής ή του τυποποιημένου συστήματος EDI (Electronic Data Interchange) κατά την έκδοση ηλεκτρονικών τιμολογίων υποχρεώνει τις αρχές των κρατών μελών να δεχθούν τα εκδιδόμενα ηλεκτρονικά τιμολόγια, ενώ παράλληλα, διευκολύνει την αρχειοθέτηση και την άμεση ανταλλαγή τους.

Οι ηλεκτρονικές ταυτότητες και τα ηλεκτρονικά διαβατήρια, αποτελούν μία άλλη περίπτωση ευρείας εφαρμογής των ηλεκτρονικών υπογραφών και ήδη έχουν θεσμοθετηθεί και 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 προηγμένες 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 ταυτότητες και τα διαβατήρια είναι η σχεδιαζόμενη ηλεκτρονική 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.

Σε πολλά κράτη μέλη της Ε.Ε. αναπτύσσονται σε εθνικό επίπεδο αρκετές άλλες εφαρμογές σχετικές με τις ηλεκτρονικές υπογραφές.

Στην Ιταλία 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 εγγράφων και η θέσπιση αυστηρών κανόνων για τη διαλειτουργικότητα των σχετικών πιστοποιητικών που εκδίδουν οι εγγεγραμμένοι ΠΥΠ στο μητρώο του CNIPA (Centro Nationale per l' Informatica nella Publica Amministrazione), γεγονός που οδήγησε και στην ανάπτυξη εφαρμογών λογισμικού για τη δημιουργία και επαλήθευση ηλεκτρονικών υπογραφών το οποίο λειτουργεί με τα πιστοποιητικά όλων των ΠΥΠ της Ιταλίας, βάσει των κοινών προδιαγραφών.

Στη 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 προηγμένες ηλεκτρονικές υπογραφές του άρθρου 5§1 της Οδηγίας 99/93/ΕΚ, τύπος ηλεκτρονικών υπογραφών οι enhanced signatures οι οποίες παρέχονται μόνο από τους εθελοντικά διαπιστευμένους ΠΥΠ και προβλέπουν την υποχρεωτική χρήση χρονοσήμανσης 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.

Στην Εσθονία σε συνδυασμό με την ηλεκτρονική ταυτότητα που εκδίδεται υποχρεωτικά σε 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 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 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 έχει ολοκληρωθεί εφαρμογή με την οποία οι δικηγόροι μπορούν ήδη να καταθέτουν ηλεκτρονικά κάποιους τύπους δικογράφων προς την υπηρεσίες συγκεκριμένων δικαστηρίων, με τη χρήση της ηλεκτρονικής υπογραφής τους. [1]

7.2 Εφαρμογές της ηλεκτρονικής υπογραφής στην Ελλάδα

Μερικές από τις εφαρμογές της ψηφιακής υπογραφής στην Ελλάδα είναι:

7.2.1 Ψηφιακή Υπογραφή στα Φ.Ε.Κ.

Το Εθνικό Τυπογραφείο σύμφωνα με το Π.Δ. 150/2001 και την απόφαση 248/71/2002 έχει αναγνωρισμένο ψηφιακό πιστοποιητικό και υπογράφει ψηφιακά την ηλεκτρονική μορφή των Φύλλων Εφημερίδος της Κυβερνήσεως αυτόματα με την παραγωγή τους.

Το Ψηφιακό Πιστοποιητικό του Εθνικού Τυπογραφείου έχει εκδοθεί από την εταιρεία Adacom Qualified Cetificate Services S.A. για τον εξουσιοδοτημένο υπάλληλο του Εθνικού Τυπογραφείου Theodoros Moumouris, έχει διάρκεια 3 χρόνια και χρησιμοποιεί κρυπτογράφηση SHA-1 RSA με δημόσιο κλειδί RSA (2048 bits).

Η ψηφιακή υπογραφή στα Φ.Ε.Κ. εγκαθίσταται με ειδικές διαδικασίες με χρήση κατάλληλου διαμορφωμένου λογισμικού και ειδικού υλικού και υποδομών από εξουσιοδοτημένο υπάλληλο του Εθνικού Τυπογραφείου, σύμφωνα με τα προβλεπόμενα από τον Οργανισμό του. Με αυτό τον τρόπο εξασφαλίζεται η αυθεντικότητα (έκδοση από το Εθνικό Τυπογραφείο) και η μη αλλοίωση του περιεχομένου των ηλεκτρονικών Φ.Ε.Κ. (ακεραιότητα των αρχείων).

Η ψηφιακή υπογραφή είναι μονοσήμαντη και ισχύει μόνο για το ηλεκτρονικό αρχείο Φ.Ε.Κ. για το οποίο εκδίδεται και στο οποίο εμπεριέχεται ως αναπόσπαστο τμήμα του περιεχομένου του. Σε καμία περίπτωση δεν μπορεί να χρησιμοποιηθεί για να πιστοποιήσει την εγκυρότητα του έντυπου Φ.Ε.Κ. ακόμα και αν αυτό προκύπτει από εκτύπωση του αντίστοιχου ηλεκτρονικού αρχείου Φ.Ε.Κ. το οποίο φέρει την ψηφιακή υπογραφή.

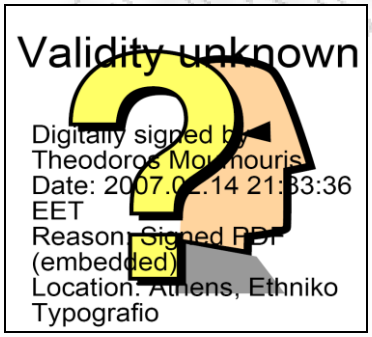
Η Ψηφιακή Υπογραφή εγκαθίστανται σε όλα τα τεύχη της Εφημερίδας της Κυβερνήσεως με έτος έκδοσης από το 2006 και μετά.

Με την χρήση της ψηφιακής υπογραφής το Εθνικό Τυπογραφείο

- εξασφαλίζει την αυθεντικότητα και την ακεραιότητα των ηλεκτρονικών αρχείων,
- παρέχεται η δυνατότητα ενημέρωσης για τις ενδεχόμενες αλλαγές εκδόσεων που μπορεί να προκύπτουν στα Φ.Ε.Κ. (έλεγχος εκδόσεων)

Βέβαια προκειμένου ο παραλήπτης του ηλεκτρονικού Φ.Ε.Κ. να ελέγχει την αξιοπιστία του πιστοποιητικού (εγκυρότητα ψηφιακής υπογραφής, ταυτότητα αποστολέα) πρέπει να εγκαταστήσει το δημόσιο κλειδί που επαληθεύει την υπογραφή του νόμιμου κατόχου του πιστοποιητικού του Εθνικού Τυπογραφείου.

Αν δεν είναι εγκατεστημένο το κλειδί που ελέγχει την αξιοπιστία της ταυτότητας της ψηφιακής υπογραφής στον υπολογιστή του παραλήπτη, τα ηλεκτρονικά Φ.Ε.Κ. με ψηφιακή υπογραφή που ανοίγονται θα έχουν ένδειξη ένα ερωτηματικό στο εικονίδιο της ψηφιακής υπογραφής, εικόνα 7.1. [32]



Εικόνα 7.1: Ψηφιακή υπογραφή

Για να είναι έγκυρη η υπογραφή θα πρέπει να γίνει προσθήκη αξιόπιστης ταυτότητας για το πιστοποιητικό του Εθνικού Τυπογραφείου. Η προσθήκη αξιόπιστης ταυτότητας μπορεί να γίνει στον υπολογιστή μας ακολουθώντας τα βήματα που αναλυτικά περιγράφονται στη σελίδα του εθνικού τυπογραφείου. Η διαδικασία αυτή εκτελείται μόνο μία φορά και θα ενεργοποιείται μέσω του Acrobat, για τον έλεγχο της ταυτότητας στα ηλεκτρονικά Φ.Ε.Κ. [33]

7.2.2 Παράδειγμα ηλεκτρονικού μηνύματος με ψηφιακή υπογραφή

Ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο με ψηφιακή υπογραφή δηλαδή ένα μήνυμα για το οποίο είμαστε σίγουροι για την ταυτότητα του αποστολέα του καθώς και για το ότι το μήνυμα αυτό είναι γνήσιο και όχι παραποιημένο είναι το παρακάτω.

Υποθέτουμε ότι δύο οντότητες Α και Β που μπορεί να είναι ιδιώτες, υπηρεσίες, εταιρείες ή και άλλοι φορείς, επιθυμούν να επικοινωνήσουν με τη χρήση ψηφιακών υπογραφών. Η ψηφιακή υπογραφή της οντότητας Α αποτελείται από το ζεύγος κλειδιών I_A (ιδιωτικό κλειδί) και $Δ_A$ (δημόσιο κλειδί). Αντίστοιχα, η ψηφιακή υπογραφή της οντότητας Β αποτελείται από το ζεύγος κλειδιών I_B (ιδιωτικό κλειδί) και $Δ_B$ (δημόσιο κλειδί). Τα ιδιωτικά κλειδιά I_A και I_B είναι γνωστά μόνο στις οντότητες Α και Β αντίστοιχα, ενώ τα δημόσια κλειδιά τους $Δ_A$ και $Δ_B$ είναι γνωστά σ' όλον τον κόσμο.

Η οντότητα Α πριν στείλει το μήνυμά της, το κρυπτογραφεί κάνοντας χρήση του ιδιωτικού της κλειδιού I_A και έτσι θα μπορεί ο καθένας να χρησιμοποιήσει το αντίστοιχο δημόσιο κλειδί $Δ_A$ για να το αποκρυπτογραφήσει. Η οντότητα Β είναι έτσι σίγουρη ότι το μήνυμα προέρχεται όντως από την οντότητα Α και όχι από κάποιον τρίτο που προσποιείται ότι είναι η οντότητα Α, καθώς το δημόσιο κλειδί $Δ_A$ μπορεί να αποκρυπτογραφήσει μόνο το αντίστοιχο ιδιωτικό κλειδί I_A, το οποίο μόνο η οντότητα Α κατέχει.

Επίσης, η οντότητα Β είναι σίγουρη ότι το μήνυμα δεν έχει αλλοιωθεί καθοδόν προς τον προορισμό του από κάποιον τρίτο, καθώς κανείς δεν είναι σε θέση να γνωρίζει το ιδιωτικό κλειδί I_A που χρησιμοποιήθηκε για την κρυπτογράφησή του, αλλά ακόμα και στην περίπτωση που το κείμενο τροποποιηθεί, η οντότητα Β θα διαπιστώσει ότι το δημόσιο κλειδί δεν θα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα και έτσι θα γνωρίζει ότι το μήνυμα είναι παραποιημένο.

Στην περίπτωση τώρα που η οντότητα Α θελήσει να στείλει ένα μήνυμα στην οντότητα Β που να είναι όμως και κρυπτογραφημένο, δηλ. μόνο η οντότητα Β να μπορεί να το διαβάσει και κανένας άλλος, τότε θα πρέπει να κρυπτογραφήσει το μήνυμα και με το δημόσιο κλειδί $Δ_B$ της οντότητας Β. Μ' αυτόν τον τρόπο μόνο η οντότητα Β θα μπορέσει να αποκρυπτογραφήσει το μήνυμα καθώς μόνο αυτή διαθέτει το αντίστοιχο ιδιωτικό κλειδί I_B. Θα πρέπει επιπλέον να εφαρμόσει και το δημόσιο κλειδί $Δ_A$ της οντότητας Α για να μπορέσει να επαναφέρει το αρχικό μήνυμα.

Το παραπάνω είναι ένα παράδειγμα ενός ηλεκτρονικού μηνύματος που είναι υπογεγραμμένο και κρυπτογραφημένο με ψηφιακή υπογραφή, πρόκειται δηλαδή για ένα μήνυμα για το οποίο όχι μόνο είμαστε σίγουροι για την ταυτότητα του αποστολέα του και για το ότι το μήνυμα είναι γνήσιο και όχι παραποιημένο αλλά και ότι κανείς άλλος δεν μπορεί να το δει και να το αποκρυπτογραφήσει εκτός από αυτόν για τον οποίο προορίζεται.

Βέβαια για να μπορέσουν να έχουν εφαρμογή οι παραπάνω διαδικασίες, θα πρέπει να είμαστε σίγουροι ότι η ψηφιακή υπογραφή έχει εκδοθεί νόμιμα στο όνομα κάποιου χρήστη και ότι αυτός ο χρήστης έδωσε τα πραγματικά του στοιχεία όταν ζήτησε να εκδοθεί η ψηφιακή υπογραφή του. Η λύση είναι η ύπαρξη ενός αξιόπιστου οργανισμού, ο οποίος θα αναλάβει να εκδίδει και να πιστοποιεί τις ψηφιακές υπογραφές. [34]

7.2.3 Χρήση ηλεκτρονικών υπογραφών στον Τραπεζικό Τομέα

Οι εφαρμογές του Τραπεζικού τομέα (e-banking) που μπορούν να χρησιμοποιήσουν ηλεκτρονικές υπογραφές και πιστοποιητικά, είναι συνήθως κλειστές εφαρμογές, δηλαδή συναλλάσσεται μία μόνο τράπεζα με τους πελάτες της και ως τέτοιες, διέπονται κυρίως από συμβατικούς όρους, οι οποίοι καθορίζουν την έκταση της αναγνώρισης των χρησιμοποιούμενων υπογραφών και όχι άμεσα από το σχετικό θεσμικό και ρυθμιστικό πλαίσιο.

Κάθε τραπεζικός οργανισμός αναπτύσσει τις δικές του εφαρμογές με γνώμονα το προφίλ των πελατών και τις ιδιαίτερες ανάγκες των σχεδιαζόμενων υπηρεσιών, χωρίς να λαμβάνονται υπ' όψιν στοιχεία διαλειτουργικότητας των χρησιμοποιούμενων ηλεκτρονικών υπογραφών και πιστοποιητικών με άλλες εφαρμογές τρίτων. Η διατραπεζικότητα των χρησιμοποιούμενων εργαλείων, δηλαδή η δυνατότητα κοινής χρήσης των ίδιων υπογραφών και πιστοποιητικών των πελατών από όλες τις Τράπεζες, αποτελεί απώτερο στόχο, ο οποίος όμως, προς το παρόν τουλάχιστον, υποσκελίζεται από την προτεραιότητα που δίνεται στην αντιμετώπιση των εσωτερικών προβλημάτων που αναδεικνύονται κατά την ενσωμάτωση και χρήση των νέων εργαλείων ασφάλειας στα υπάρχοντα συστήματα του κάθε τραπεζικού οργανισμού.

Επίσης, οι διαφορετικοί τρόποι ονομασίας π.χ. χρήση λατινικών ή όχι χαρακτήρων, αναγραφή ή όχι του πατρώνυμου, της ημερομηνίας γέννησης, κ.λ.π. και η αναγραφή διαφορετικών στοιχείων ταυτοποίησης π.χ. ΑΦΜ, αριθμού αστυνομικής ταυτότητας ή αριθμού τραπεζικού λογαριασμού, των πελατών-υποκειμένων στα ηλεκτρονικά πιστοποιητικά, αποτελεί ιδιαίτερο πρόβλημα για την διαλειτουργικότητα των πιστοποιητικών αυτών μεταξύ διαφορετικών τραπεζών. Οι διαφορετικές ανάγκες κάθε τράπεζας και κάθε οργανισμού γενικά επιβάλλουν την διαφοροποίηση στα στοιχεία που εμφανίζονται στα χρησιμοποιούμενα πιστοποιητικά. Εάν όμως υπάρξει ένας κοινός και ικανοποιητικός τύπος περιγραφής της ταυτότητας των πελατών, οι ιδιαίτερες ανάγκες για διαχείριση δικαιωμάτων πρόσβασης των πελατών στις υπηρεσίες των τραπεζών και κάθε άλλου οργανισμού μπορούν να λυθούν σε επίπεδο εφαρμογής, π.χ. με την χρήση σχετικών εσωτερικών βάσεων δεδομένων των τραπεζών.

Αν και τα θέματα ασφάλειας κρίνονται ως καθοριστικής σημασίας για την αξιοπιστία των ηλεκτρονικών συναλλαγών, ιδίως στον τραπεζικό τομέα, το κόστος ανάπτυξης και συντήρησης της σχετικής υποδομής είναι μεγάλο και δεν μπορεί να μετατεθεί εύκολα στον πελάτη μιας και αυτός θεωρεί δεδομένη την παροχή ασφάλειας από την τράπεζά του και αυτό αποτελεί έναν ακόμη ανασταλτικό παράγοντα για την αντικατάσταση των κλασσικών μεθόδων ασφαλείας που χρησιμοποιούν ως σήμερα οι Τράπεζες. Η υιοθέτηση μιας κοινής Πολιτικής Ηλεκτρονικής Υπογραφής από όλες τις Τράπεζες, μέσω της Ένωσης Τραπεζών Ελλάδος ενδεχομένως:

- θα έκανε πιο σαφείς τους όρους χρήσης των ηλεκτρονικών υπογραφών και πιστοποιητικών,
- θα διαμοίραζε το κόστος έκδοσης των πιστοποιητικών,
- θα αύξανε τη χρησιμότητα και την αξιοπιστία των συγκεκριμένων μεθόδων και
- θα αποτελούσε πιθανό κίνητρο για τις Τράπεζες και τους πελάτες τους για την ανάπτυξη και χρήση σχετικών εφαρμογών. [1]

7.2.4 Χρήση ηλεκτρονικών υπογραφών στην κινητή τηλεφωνία

Η χρήση των ηλεκτρονικών υπογραφών μέσω δικτύων κινητής τηλεφωνίας είναι ακόμα μια εξέλιξη στο χώρο των ηλεκτρονικών υπογραφών. Η ίδια η συσκευή τηλεφώνου που έχουμε όλοι πάνω μας είναι ήδη ένας αναγνώστης έξυπνων καρτών (SIM κάρτες) και θα μπορούσε να αποτελέσει μια διέξοδο στο ζήτημα της εξάπλωσης της χρήσης αναγνωστών έξυπνων καρτών. Τα πρότυπα για ασφαλείς αναγνώστες smart-card προβλέπουν την ύπαρξη ξεχωριστού πληκτρολογίου (numeric pad) και οθόνης για τους αναγνώστες καρτών και τα κινητά τηλέφωνα μπορούν να αποτελέσουν, κάτω από συγκεκριμένες προϋποθέσεις, μια υλοποίηση του παραπάνω προτύπου και να παράσχουν στους χρήστες τους τον απαραίτητο ασφαλή αναγνώστη έξυπνων καρτών, απαραίτητο μέρος για την ασφαλή διάταξη δημιουργίας ψηφιακής υπογραφής σύμφωνα με το θεσμικό πλαίσιο.

Αναγνωρίσθηκε η περιορισμένη δυνατότητα ως σήμερα, των χρησιμοποιούμενων κινητών τηλεφώνων 2ης γενιάς για παροχή προηγμένων υπηρεσιών οι οποίες απαιτούν χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών. Αυτό όμως αλλάζει με τον ερχομό των δικτύων και των συσκευών 3ης γενιάς (3G) όπου οι δυνατότητες ανάπτυξης σχετικών εφαρμογών είναι ισάξιες με αυτές των προσωπικών υπολογιστών και του internet. Επιπλέον, τα κινητά τηλέφωνα και οι συσκευές PDAs, λόγω της φορητότητας και της δυνατότητας για ασύρματη επικοινωνία (Bluetooth) με άλλα τερματικά (ATMs, POSs, κ.λ.π.) που διαθέτουν, αποτελούν ιδανικό μέσο για την ανάπτυξη πολλών σχετικών εφαρμογών, όπως ηλεκτρονικών πληρωμών.

Οι SIM Cards που χρησιμοποιούνται στα κινητά τηλέφωνα ως smart cards που είναι, έχουν δυνατότητα ασφαλούς αποθήκευσης και χρήσης των κλειδιών του χρήστη και γι' αυτό το λόγο τα κινητά τηλέφωνα μπορούν υπό προϋποθέσεις να λειτουργήσουν ως ασφαλείς διατάξεις δημιουργίας ηλεκτρονικής υπογραφής για τη δημιουργία ψηφιακών υπογραφών. Επιπλέον, νέες εξελιγμένες συσκευές π.χ. με τη δυνατότητα ελέγχου βιομετρικών στοιχείων, μπορούν να παρέχουν περισσότερη ευελιξία και ασφάλεια στη χρήση των κινητών τηλεφώνων ως μέσου δημιουργίας ηλεκτρονικής υπογραφής και διενέργειας προσωπικών συναλλαγών.[1]

Μέρος Β΄

Κεφάλαιο 8

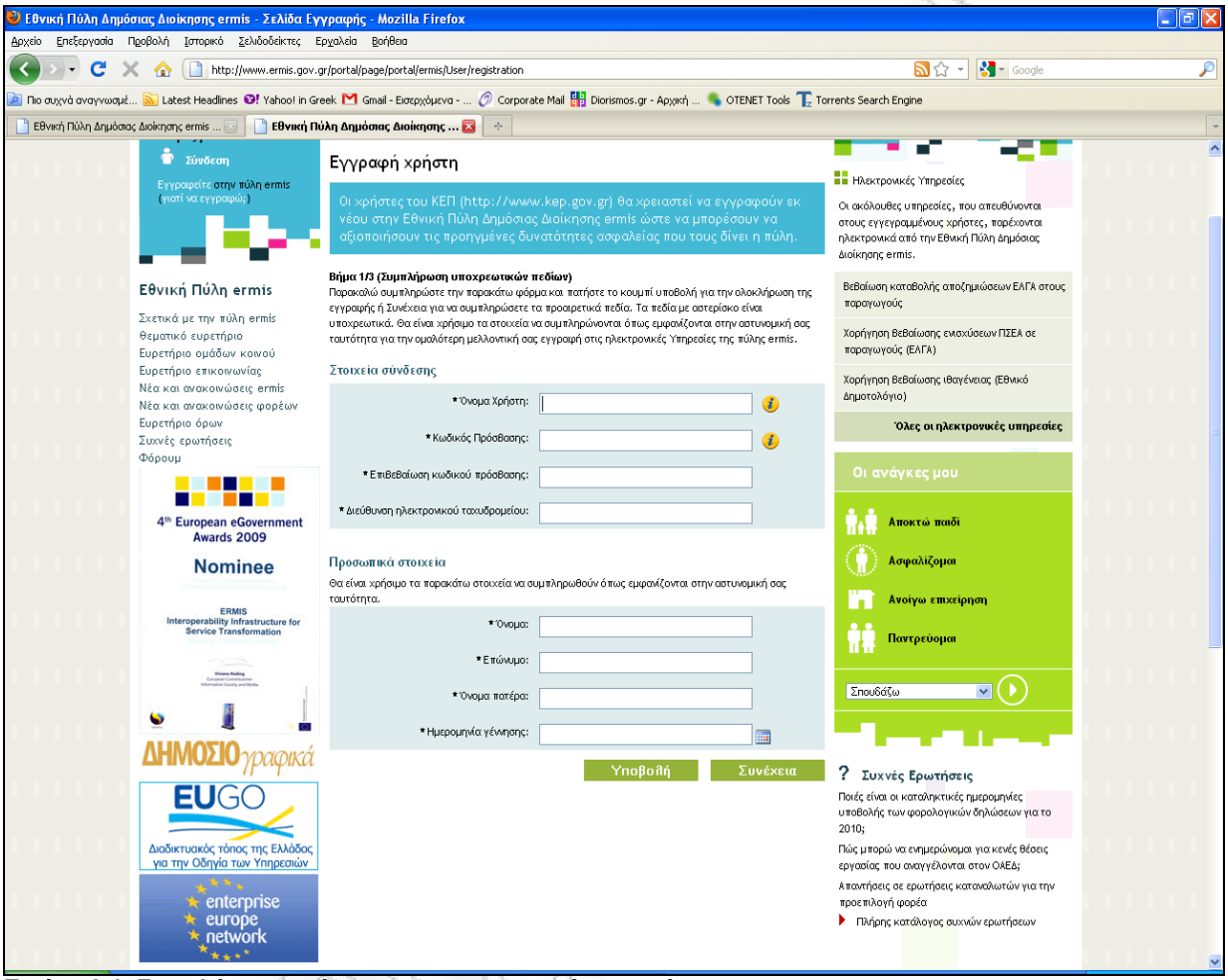
8.1 Έκδοση ψηφιακών πιστοποιητικών από την εθνική πύλη δημόσιας διοίκησης ermis του Υπουργείου Εσωτερικών

8.1.1 Εγγραφή χρήστη στην πύλη ermis & αίτηση έκδοσης ψηφιακών πιστοποιητικών

Στο κεφάλαιο αυτό θα περιγράψουμε τον τρόπο που ένας πολίτης μπορεί να αιτηθεί και στη συνέχεια να προχωρήσει στην έκδοση ψηφιακών πιστοποιητικών από την εθνική πύλη δημόσιας διοίκησης ermis του Υπουργείου Εσωτερικών.

Για την έκδοση ψηφιακών πιστοποιητικών ο χρήστης αρχικά πρέπει να εγγραφεί στην πύλη ermis στην ηλεκτρονική διεύθυνση www.ermis.gov.gr. Εδώ θα του ζητηθούν να συμπληρώσει τα εξής υποχρεωτικά στοιχεία: Όνομα και επώνυμο, όνομα πατέρα, ημερομηνία γέννησης, και e-mail. Ο χρήστης με δική του συγκατάθεση μπορεί να δηλώσει επιπλέον προαιρετικά στοιχεία όπως στοιχεία επικοινωνίας, οικογενειακή κατάσταση κλπ. Αυτά τα στοιχεία που αποτελούν μη ευαίσθητα προσωπικά δεδομένα, διατηρούνται στη βάση δεδομένων του Ερμή που ανήκει στο Υπουργείο Εσωτερικών και ουδέποτε γνωστοποιούνται σε τρίτους βάση του ελληνικού δικαίου (ν. 2472/1997 για την προστασία του ατόμου από την προστασία δεδομένων προσωπικού χαρακτήρα όπως έχει συμπληρωθεί και τροποποιηθεί με τις αποφάσεις του προέδρου της επιτροπής προστασίας προσωπικών δεδομένων, τα π.δ. 207/1998 και 79/2000, το άρθρο 8 του Ν. 2819/2000 και τον ν.3471/2006) και του ευρωπαϊκού δικαίου (οδηγίες 95/46/ΕΚ και 97/66/ΕΚ). Η εθνική πύλη ermis επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων που είναι εγγεγραμμένοι χρήστες της πύλης. Σκοπός αυτής της επεξεργασίας είναι η παροχή στους χρήστες της πύλης ολοκληρωμένων και ασφαλών ηλεκτρονικών συναλλαγών της δημόσιας διοίκησης κεντρικά ελεγχόμενες από τον Ερμή.[48]

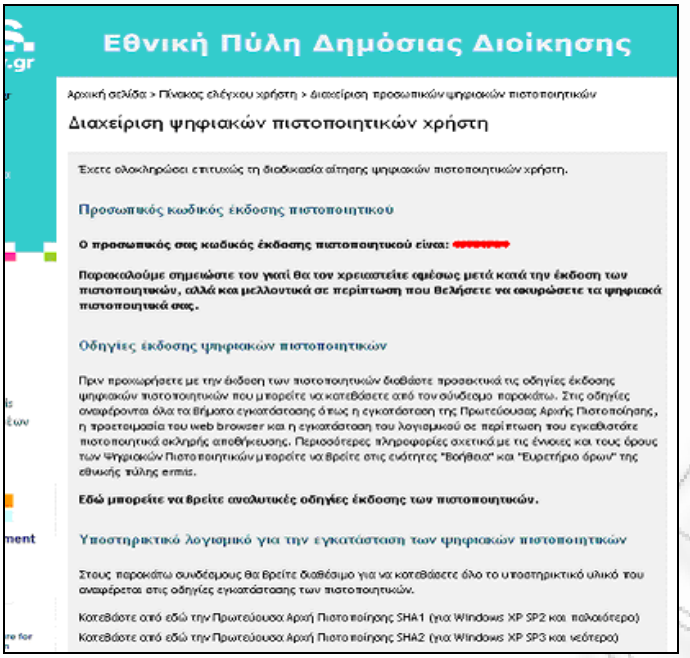
Μετά τη συμπλήρωση της φόρμας, εικόνα 8.1, ο χρήστης πατάει το κουμπί ''Υποβολή'' και η εγγραφή του στην πύλη ermis έχει ολοκληρωθεί.



Εικόνα 8.1: Συμπλήρωση φόρμας για την εγγραφή του χρήστη

Ο εγγεγραμμένος πια χρήστης υποβάλει ηλεκτρονική αίτηση έκδοσης ψηφιακών πιστοποιητικών μέσω του μενού ''πίνακας ελέγχου'' στην πύλη του ermis. Στη συνέχεια αφού επισκεφτεί ένα κέντρο εξυπηρέτησης πολιτών για να γίνει η ταυτοποίηση στοιχείων του υποβάλει στο Υπουργείο Εσωτερικών μία επικυρωμένη φωτοτυπία της ταυτότητας του και μία υπεύθυνη δήλωση με το γνήσιο της υπογραφής του για να ολοκληρωθεί η αίτησή του.

Μετά από αυτά, στο μενού ''διαχείριση ψηφιακών πιστοποιητικών χρήστη'' στην πύλη του ermis ο χρήστης θα δει ότι το σύστημα τον ενημερώνει ότι έχει ολοκληρώσει με επιτυχία τη διαδικασία αίτησης ψηφιακών πιστοποιητικών και θα του έχει σταλεί ο προσωπικός του κωδικός έκδοσης πιστοποιητικού τον οποίο και θα χρειαστεί για την έκδοση των ψηφιακών του πιστοποιητικών ακολουθώντας πιστά τις οδηγίες που του παρέχονται μέσω της πύλης ermis, εικόνα 8.2.



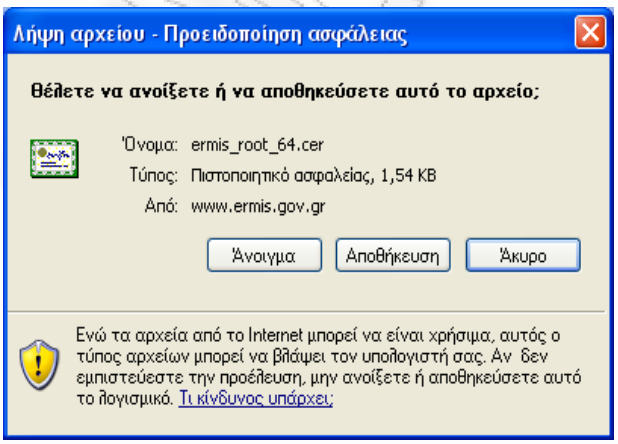
Εικόνα 8.2: Προσωπικός κωδικός έκδοσης πιστοποιητικού

8.1.2 Εγκατάσταση του πιστοποιητικού Πρωτεύουσας Αρχής Πιστοποίησης

Η Αρχή Πιστοποίησης είναι η κοινώς έμπιστη αρχή που εκδίδει τα ψηφιακά πιστοποιητικά. Τα ψηφιακά πιστοποιητικά που εκδίδονται για τους πολίτες - χρήστες του ermis είναι ψηφιακά υπογεγραμμένα με το ιδιωτικό κλειδί της Πρωτεύουσας Αρχής Πιστοποίησης της πύλης ermis. Για να εμπιστευτούμε το ψηφιακό πιστοποιητικό ενός πολίτη - χρήστη θα πρέπει πρώτα να εμπιστευτούμε την Αρχή που το εκδίδει.

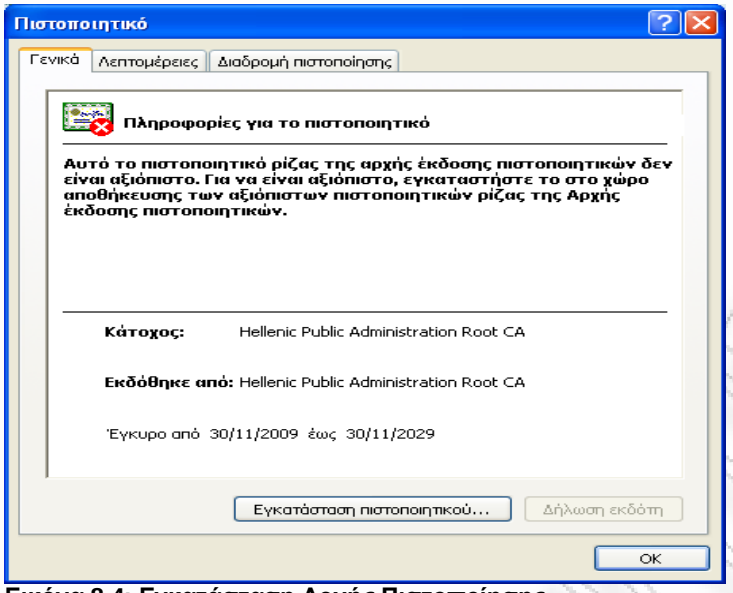
Για να κάνει λοιπόν αυτό τον έλεγχο ο υπολογιστής μας θα πρέπει να έχουμε εγκαταστήσει σ' αυτόν την Πρωτεύουσα Αρχή Πιστοποίησης. Ο ίδιος έλεγχος γίνεται από τον υπολογιστή μας και για τα ψηφιακά πιστοποιητικά που εκδίδουμε για τον εαυτό μας. Επομένως το πρώτο βήμα που πρέπει να κάνουμε πριν την η εγκατάσταση του ψηφιακού πιστοποιητικού μας είναι η εγκατάσταση της Πρωτεύουσας Αρχής Πιστοποίησης της πύλης ermis στον υπολογιστή μας.

Από τη σελίδα διαχείρισης προσωπικών ψηφιακών πιστοποιητικών στον ermis επιλέγουμε την Αρχή Πιστοποίησης που αντιστοιχεί στο λειτουργικό μας σύστημα, (εικόνα 8.2) οπότε και εμφανίζεται το παράθυρο της εικόνας 8.3.



Εικόνα 8.3: Εγκατάσταση Αρχής Πιστοποίησης

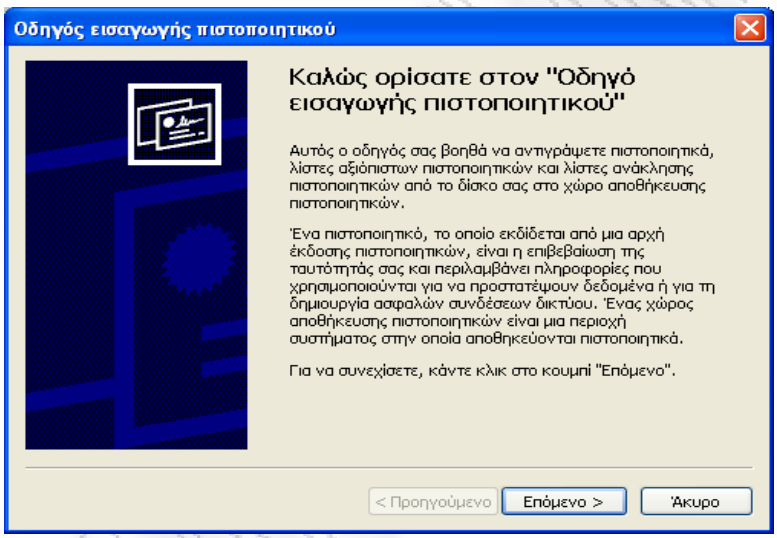
Επιλέγουμε ‘’Άνοιγμα’’ και μας δίνονται διάφορες πληροφορίες σχετικά με το πιστοποιητικό που πρόκειται να εγκαταστήσουμε, εικόνα 8.4.



Εικόνα 8.4: Εγκατάσταση Αρχής Πιστοποίησης

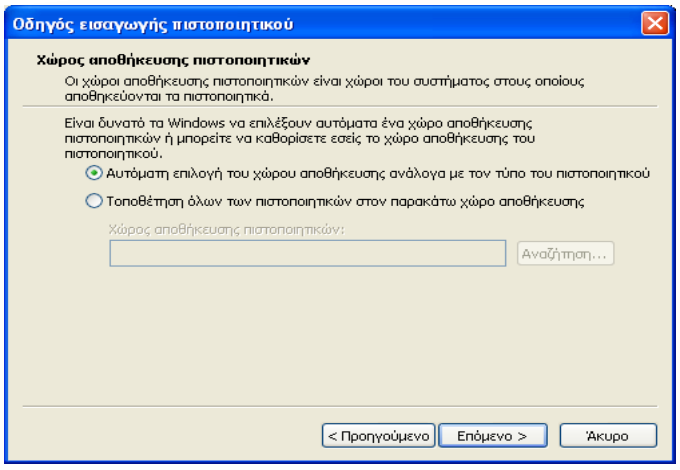
Μπορούμε να παρατηρήσουμε ότι το πιστοποιητικό αυτό της πρωτεύουσας αρχής πιστοποίησης έχει ισχύ για 20 χρόνια από την ημέρα δημιουργίας του.

Επιλέγουμε ‘’εγκατάσταση πιστοποιητικού’’ και εμφανίζεται το παράθυρο ‘’Οδηγός εισαγωγής πιστοποιητικού’’, εικόνα 8.5.



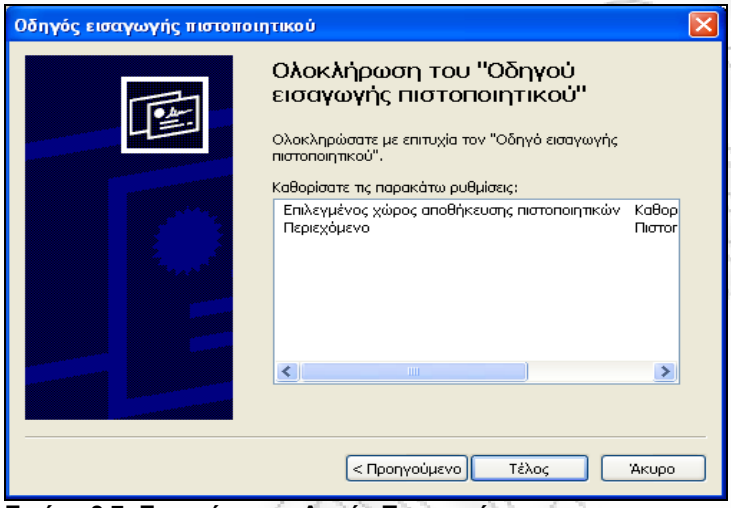
Εικόνα 8.5: Εγκατάσταση Αρχής Πιστοποίησης

Επιλέγουμε ‘’Επόμενο‘‘, όπου καθορίζουμε το χώρο που θέλουμε να αποθηκευτεί το πιστοποιητικό, εικόνα 8.6.



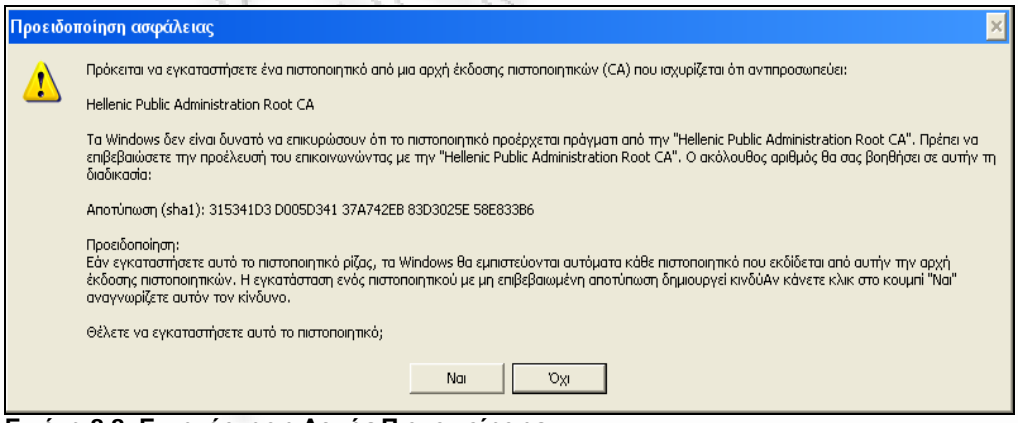
Εικόνα 8.6: Εγκατάσταση Αρχής Πιστοποίησης

Επιλέγουμε πάλι ‘’Επόμενο‘‘ και εμφανίζεται το παράθυρο, εικόνα 8.7, όπου μας ενημερώνει ότι έχουμε ολοκληρώσει με επιτυχία την εισαγωγή του πιστοποιητικού.



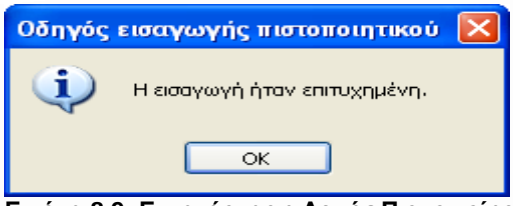
Εικόνα 8.7: Εγκατάσταση Αρχής Πιστοποίησης

Επιλέγουμε ‘’Τέλος’’ και εμφανίζεται το παράθυρο ‘’Προειδοποίηση Ασφάλειας’’, εικόνα 8.8.



Εικόνα 8.8: Εγκατάσταση Αρχής Πιστοποίησης

Επιλέγουμε ‘’Ναι’’ για να εγκαταστήσουμε το πιστοποιητικό της Αρχής Πιστοποίησης και αν όλα έχουν γίνει σωστά θα εμφανιστεί το παρακάτω μήνυμα, εικόνα 8.9.



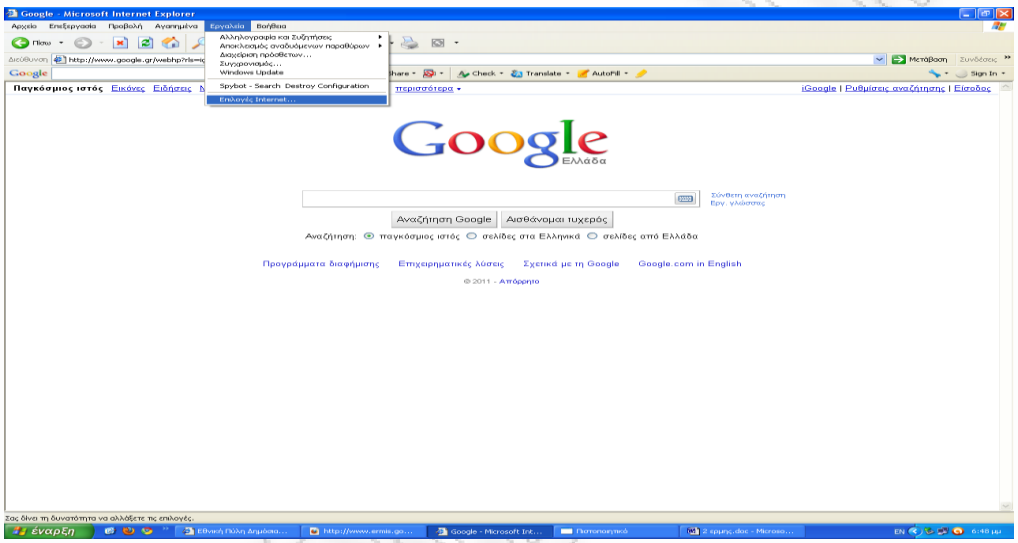
Εικόνα 8.9: Εγκατάσταση Αρχής Πιστοποίησης

Επιλέγουμε ‘’ΟΚ’’. Η εγκατάσταση του πιστοποιητικού της Αρχής Πιστοποίησης έχει ολοκληρωθεί με επιτυχία. Από εδώ και πέρα πια τα windows μας θα εμπιστεύονται αυτόματα κάθε πιστοποιητικό που θα εκδίδεται από αυτήν την Αρχή Πιστοποίησης.

8.1.3 Προετοιμασία του Internet Explorer

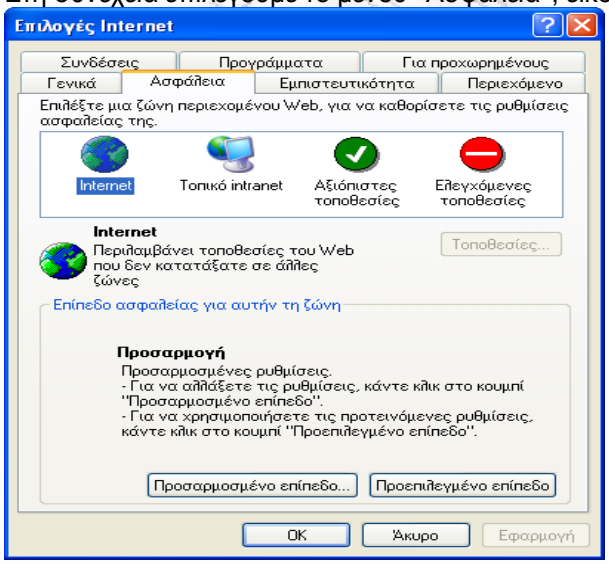
Πριν υποβάλλουμε την ηλεκτρονική αίτηση έκδοσης ψηφιακών πιστοποιητικών πρέπει να κάνουμε κάποιες ρυθμίσεις στον Internet Explorer.

Από το μενού του Internet Explorer επιλέγουμε ‘’εργαλεία’’ και ‘’επιλογές Internet’’, εικόνα 8.10.



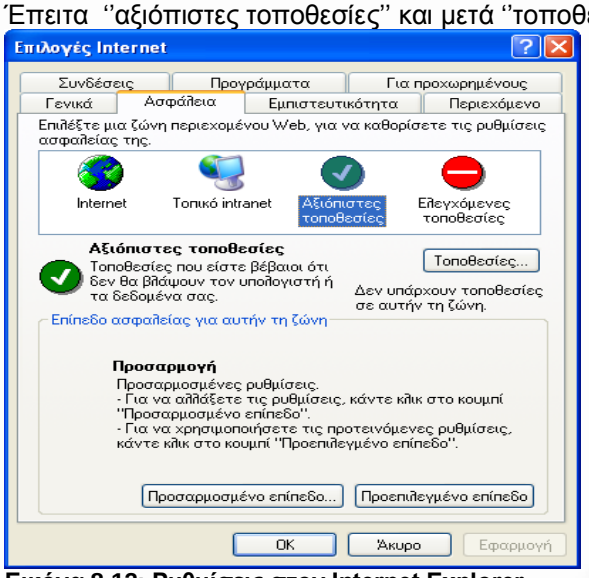
Εικόνα 8.10: Ρυθμίσεις στον Internet Explorer

Στη συνέχεια επιλέγουμε το μενού ‘’Ασφάλεια’’, εικόνα 8.11



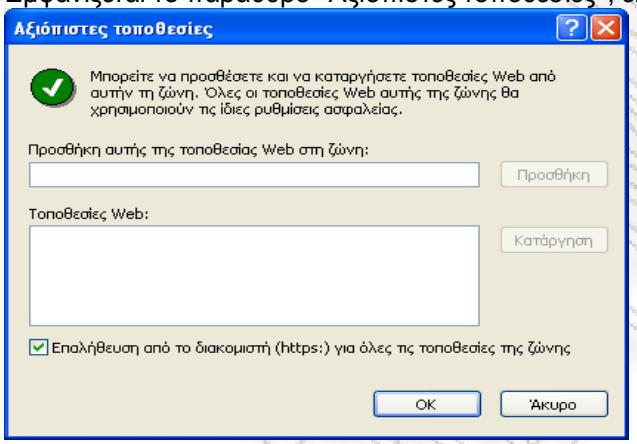
Εικόνα 8.11: Ρυθμίσεις στον Internet Explorer

Έπειτα ‘‘αξιόπιστες τοποθεσίες’’ και μετά ‘‘τοποθεσίες’’, εικόνα 8.12.



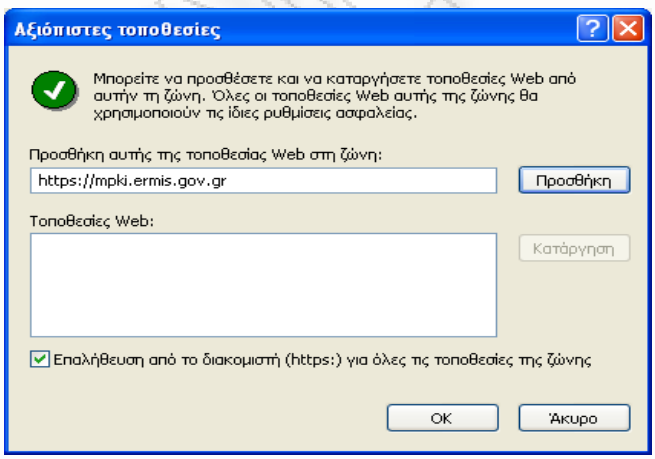
Εικόνα 8.12: Ρυθμίσεις στον Internet Explorer

Εμφανίζεται το παράθυρο ‘‘Αξιόπιστες τοποθεσίες’’, εικόνα 8.13.

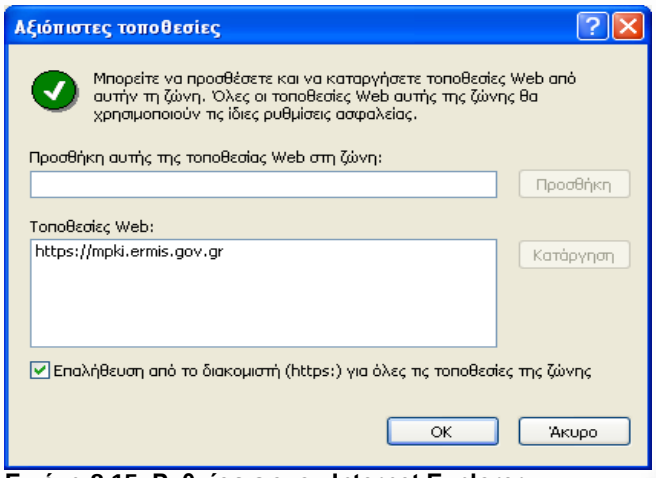


Εικόνα 8.13: Ρυθμίσεις στον Internet Explorer

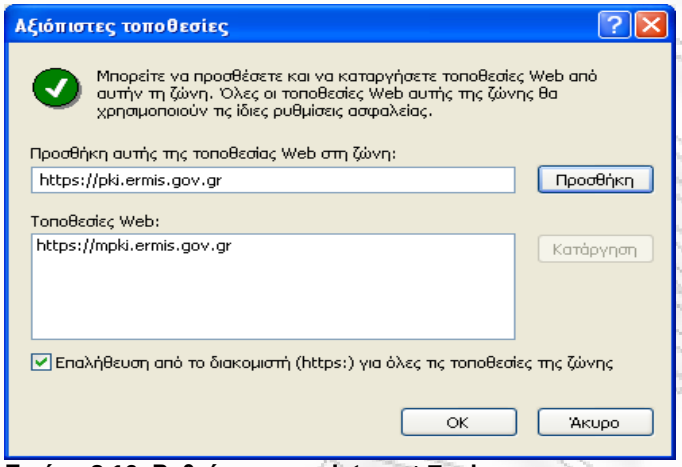
Προσθέτουμε δύο τοποθεσίες στην λίστα, τις https://mpki.ermis.gov.gr & https://pki.ermis.gov.gr και επιλέγουμε ‘‘προσθήκη’’, εικόνα 8.14, εικόνα 8.15, εικόνα 8.16 και εικόνα 8.17.



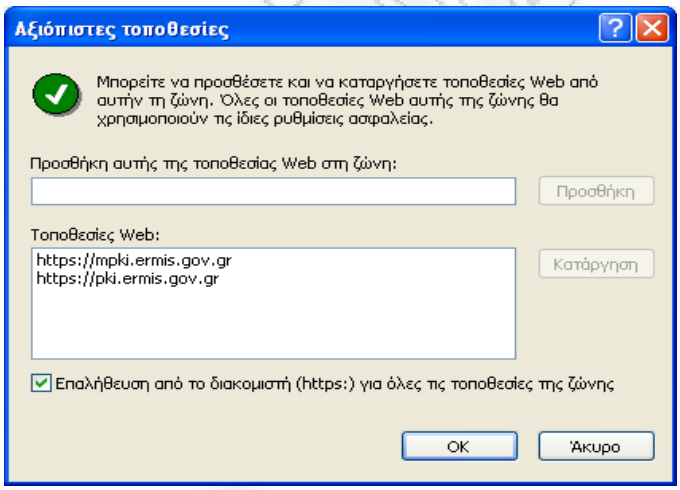
Εικόνα 8.14: Ρυθμίσεις στον Internet Explorer



Εικόνα 8.15: Ρυθμίσεις στον Internet Explorer

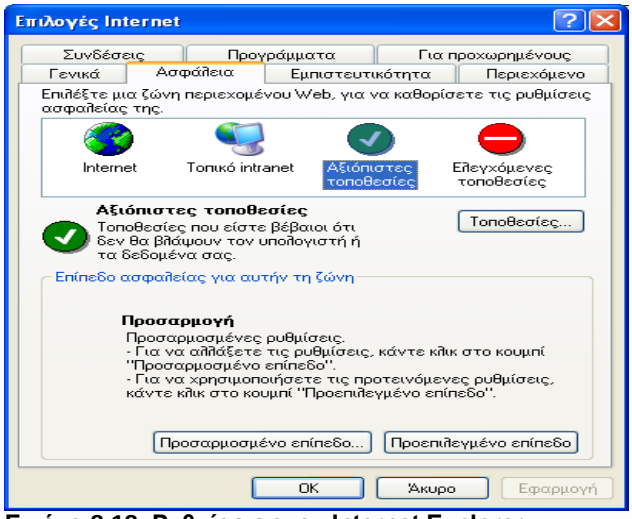


Εικόνα 8.16: Ρυθμίσεις στον Internet Explorer



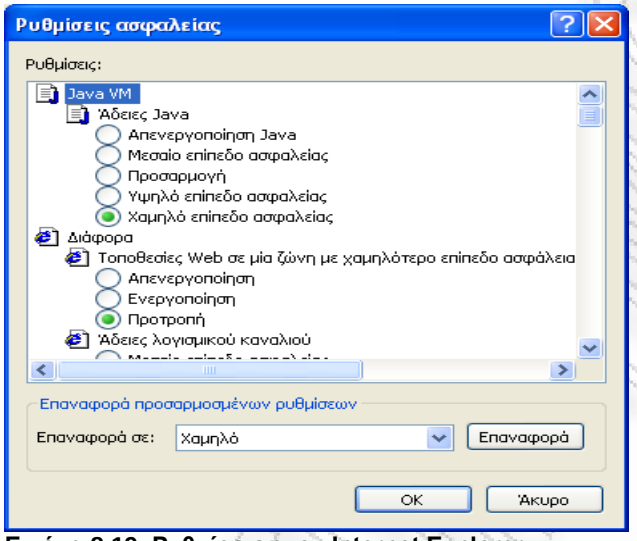
Εικόνα 8.17: Ρυθμίσεις στον Internet Explorer

Στη συνέχεια επιλέγουμε ‘’ΟΚ’’ και εμφανίζεται ξανά το παράθυρο ‘’επιλογές Internet’’ εικόνα 8.18.



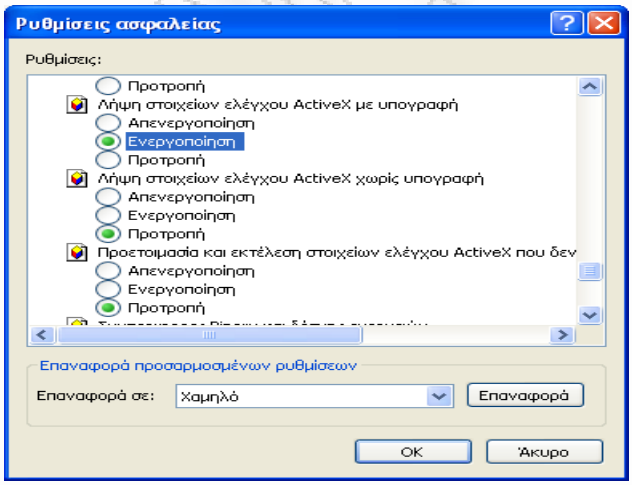
Εικόνα 8.18: Ρυθμίσεις στον Internet Explorer

Επιλέγουμε ‘’προσαρμοσμένο επίπεδο’’ και εμφανίζεται το παρακάτω παράθυρο, εικόνα 8.19.



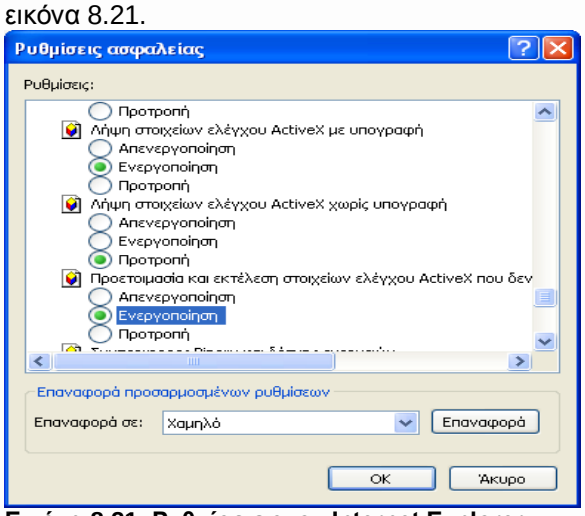
Εικόνα 8.19: Ρυθμίσεις στον Internet Explorer

Στις ρυθμίσεις ασφαλείας ψάχνουμε και ενεργοποιούνε τα εξής:
1) ‘’Λήψη στοιχείων ελέγχου ActiveX με υπογραφή’’, εικόνα 8.20.



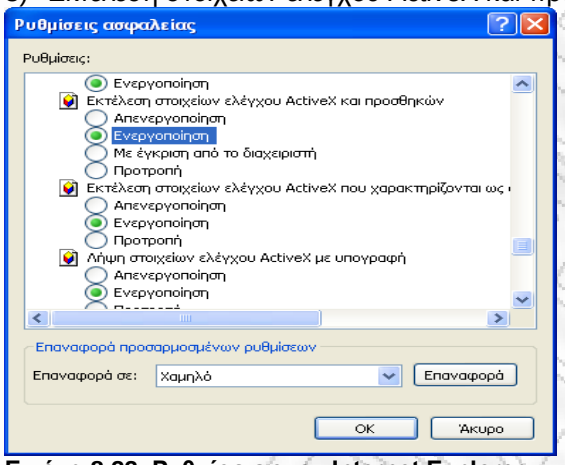
Εικόνα 8.20: Ρυθμίσεις στον Internet Explorer

2) ‘’Προετοιμασία και εκτέλεση στοιχείων ελέγχου ActiveX που δε χαρακτηρίζονται ως ασφαλή’’, εικόνα 8.21.



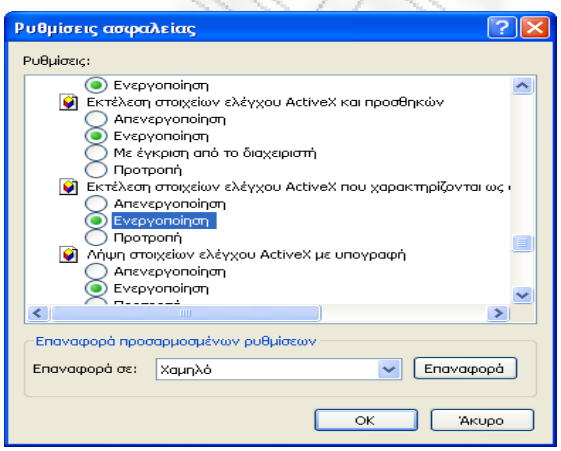
Εικόνα 8.21: Ρυθμίσεις στον Internet Explorer

3) ‘’Εκτέλεση στοιχείων ελέγχου ActiveX και προσθηκών’’, εικόνα 8.22.



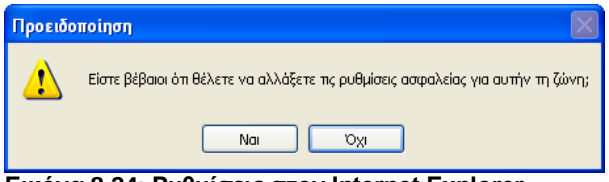
Εικόνα 8.22: Ρυθμίσεις στον Internet Explorer

4) ‘’Εκτέλεση στοιχείων ελέγχου ActiveX που χαρακτηρίζονται ως ασφαλή για εκτέλεση’’, εικόνα 8.23.



Εικόνα 8.23: Ρυθμίσεις στον Internet Explorer

Πατώντας ‘’ΟΚ’’ εμφανίζεται μια προειδοποίηση λόγω των αλλαγών που μόλις κάναμε, εικόνα 8.24, για το αν είμαστε βέβαιοι ότι θέλουμε να αλλάξουμε τις ρυθμίσεις ασφαλείας.

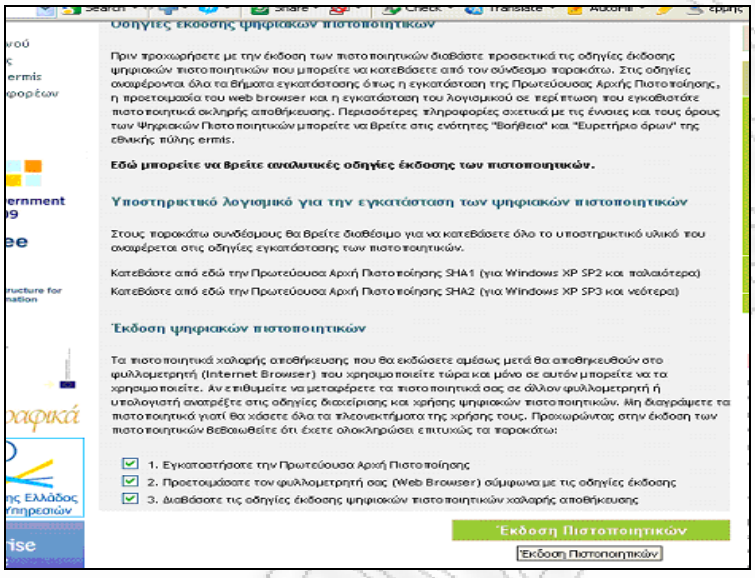


Εικόνα 8.24: Ρυθμίσεις στον Internet Explorer

Επιλέγουμε ‘’Ναι’’ και στη συνέχεια κάνουμε επανεκκίνηση του Internet Explorer. Τώρα πια είμαστε έτοιμοι για την υποβολή της ηλεκτρονικής αίτησής μας για την έκδοση ψηφιακών πιστοποιητικών μας.

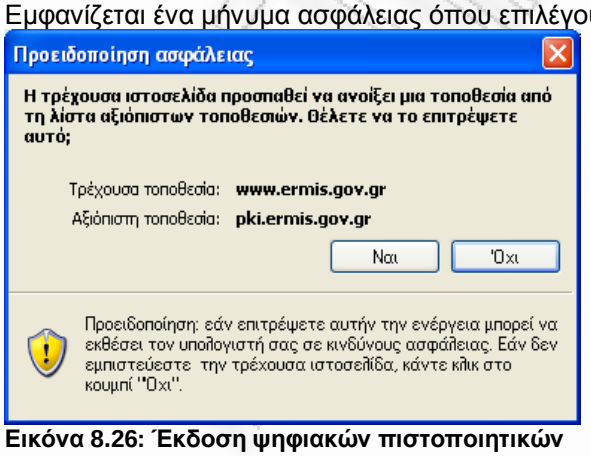
8.1.4 Έκδοση ψηφιακών πιστοποιητικών

Από τον πίνακα ελέγχου του ermis πρέπει να μεταβούμε στην ενότητα ‘’διαχείριση προσωπικών ψηφιακών πιστοποιητικών’’ και να επιλέξουμε το σύνδεσμο ‘’έκδοση πιστοποιητικών’’, εικόνα 8.25.



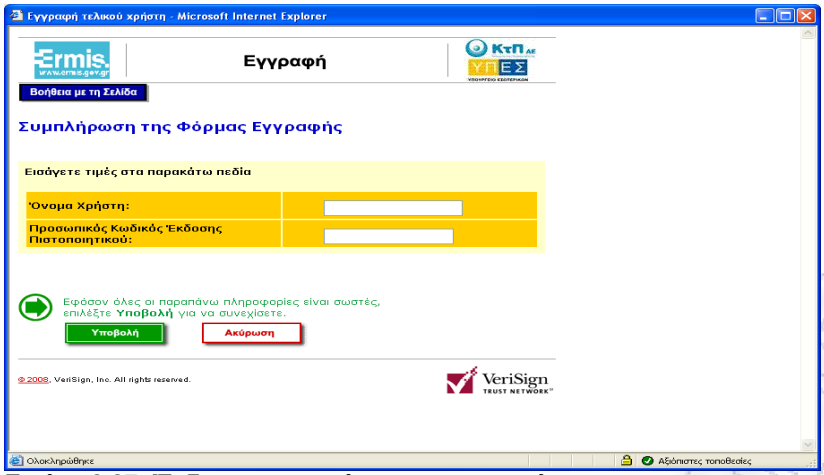
Εικόνα 8.25: Έκδοση ψηφιακών πιστοποιητικών

Εμφανίζεται ένα μήνυμα ασφάλειας όπου επιλέγουμε ‘’Ναι’’, εικόνα 8.26.



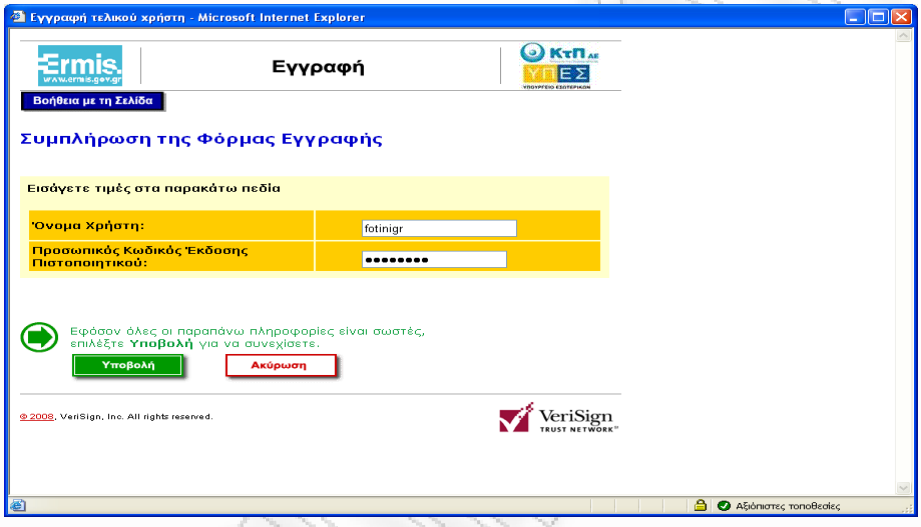
Εικόνα 8.26: Έκδοση ψηφιακών πιστοποιητικών

Στη συνέχεια εμφανίζεται η φόρμα εγγραφής, εικόνα 8.27.



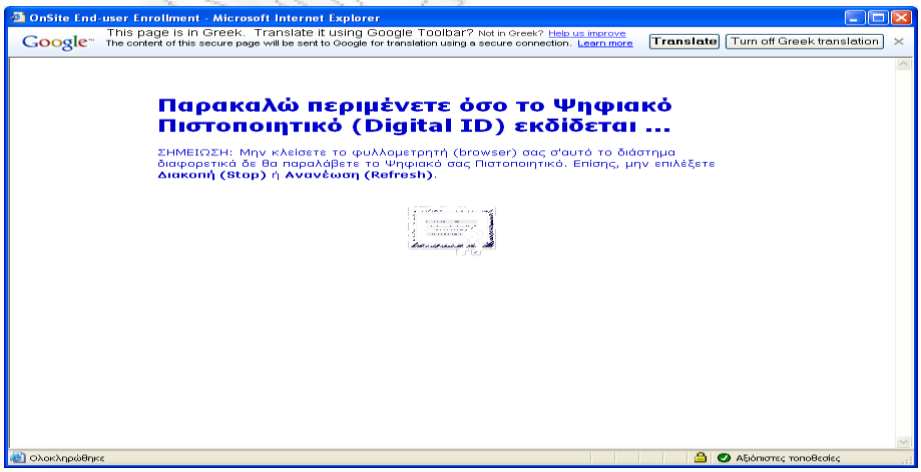
Εικόνα 8.27: Έκδοση ψηφιακών πιστοποιητικών

Συμπληρώνουμε τα στοιχεία που μας ζητάει δηλαδή το όνομα χρήστη που συνδεόμαστε στην πύλη του ermis και τον προσωπικό κωδικό έκδοσης πιστοποιητικού που μας είχε δοθεί στην αρχή (βλ. εικόνα 8.2, κεφάλαιο 8.1.1), εικόνα 8.28.



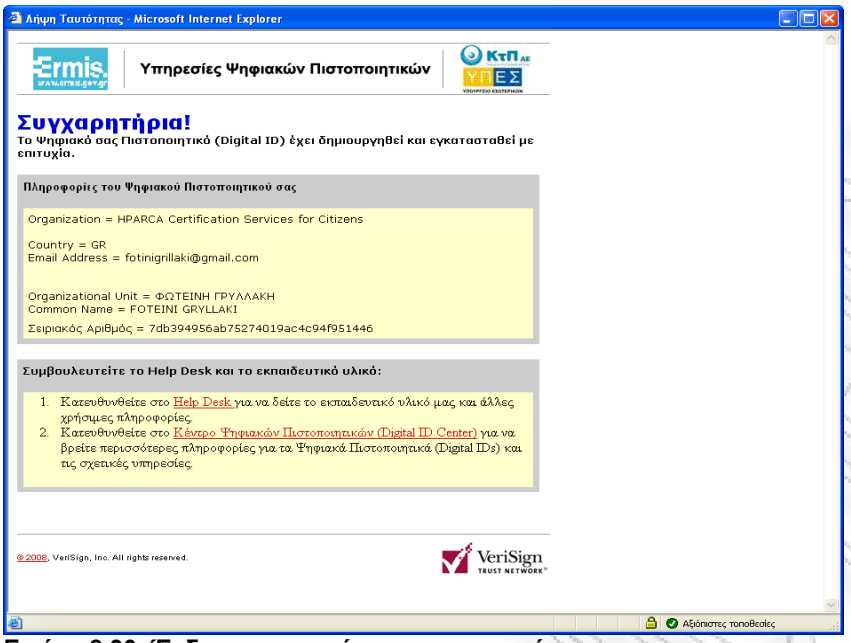
Εικόνα 8.28: Έκδοση ψηφιακών πιστοποιητικών

Πατάμε ''Υποβολή'' και εμφανίζεται μια ηλεκτρονική σελίδα, εικόνα 8.29, όπου μας ενημερώνει ότι βρισκόμαστε σε διαδικασία έκδοσης του ψηφιακού πιστοποιητικού.



Εικόνα 8.29: Έκδοση ψηφιακών πιστοποιητικών

Τέλος, εμφανίζεται μια ηλεκτρονική σελίδα, εικόνα 8.30, όπου μας ενημερώνει ότι τα ψηφιακά πιστοποιητικά εκδόθηκαν και εγκαταστάθηκαν με επιτυχία.

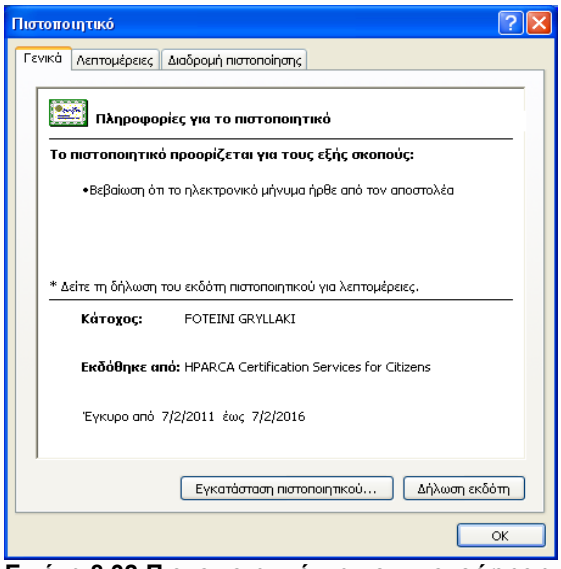


Εικόνα 8.30: Έκδοση ψηφιακών πιστοποιητικών

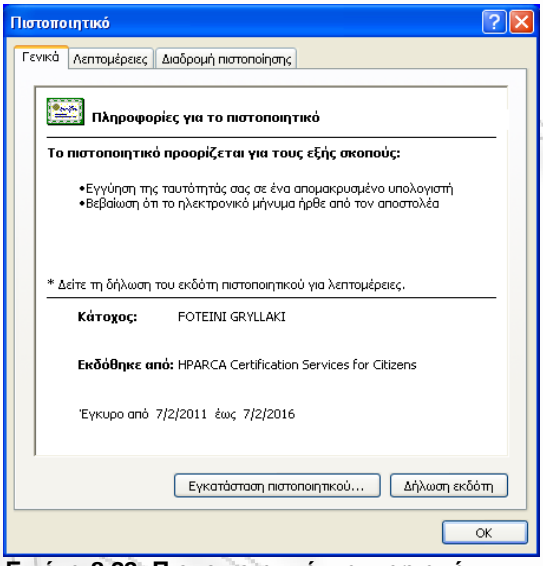
Επιστρέφοντας στην πύλη του ermis, στον πίνακα ελέγχου και στο μενού διαχείριση προσωπικών ψηφιακών πιστοποιητικών μπορούμε να δούμε πληροφορίες για τα ψηφιακά μας πιστοποιητικά που μόλις εγκαταστήσαμε, εικόνα 8.31.

Εικόνα 8.31: Τα ψηφιακά πιστοποιητικά

Τα πιστοποιητικά λοιπόν που ανήκουν στην κατοχή μας είναι δύο. Ένα για κρυπτογράφηση δεδομένων και ένα για ψηφιακή υπογραφή, εικόνες 8.32 και 8.33 αντίστοιχα.



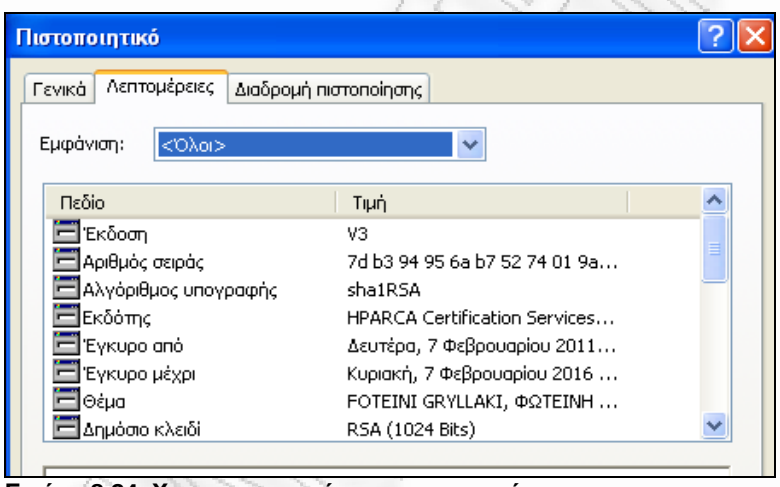
Εικόνα 8.32:Πιστοποιητικό για κρυπτογράφηση



Εικόνα 8.33: Πιστοποιητικό για ψηφιακή υπογραφή

Επιλέγοντας την καρτέλα ‘’Λεπτομέρειες’’ σε κάθε πιστοποιητικό μπορούμε να δούμε διάφορα χαρακτηριστικά που έχουν τα πιστοποιητικά μας.

Στο πιστοποιητικό μας, που εκδόθηκε για κρυπτογράφηση δεδομένων εικόνα 8.32, επιλέγοντας την καρτέλα ‘’Λεπτομέρειες’’ εμφανίζεται ένα παράθυρο με διάφορα πεδία, εικόνα 8.34, όπου βλέπουμε τα χαρακτηριστικά του πιστοποιητικού μας.



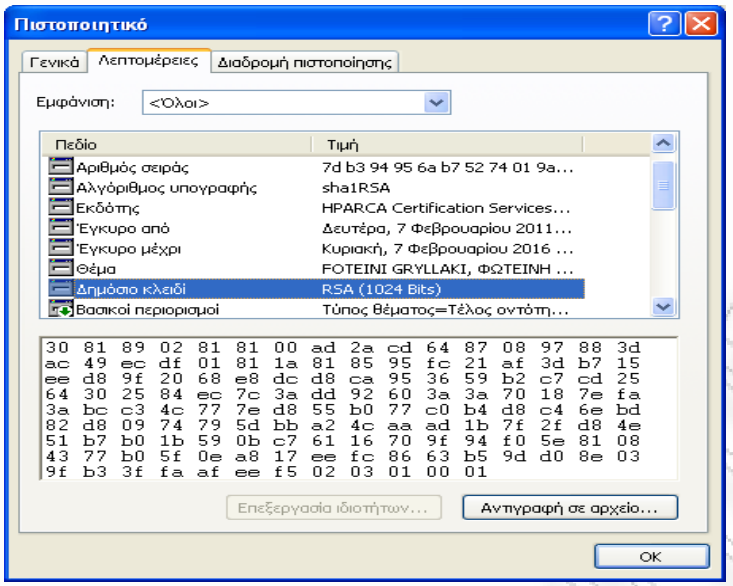
Εικόνα 8.34: Χαρακτηριστικά πιστοποιητικού

Βλέπουμε λοιπόν, εικόνα 8.34, ότι το πιστοποιητικό μας δημιουργήθηκε στις 07/02/2011 και θα ισχύει ως τις 07/02/2016, δηλαδή το πιστοποιητικό αυτό έχει λειτουργική περίοδο 5 χρόνων, όπως ορίζεται σύμφωνα με τον ‘’Κανονισμό πιστοποίησης της αρχής πιστοποίησης του ελληνικού δημοσίου (ΑΠΕΔ)’’ για τα πιστοποιητικά που εκδίδονται για τον τελικό χρήστη [49].

Φυσικά μπορούμε να προβούμε στην ακύρωση των πιστοποιητικών μας πριν τη λήξη αυτών αν για παράδειγμα εκθέσαμε το ιδιωτικό μας κλειδί σε κάποιον άλλον, πατώντας το κουμπί ‘’Ακύρωση’’, εικόνα 8.31.

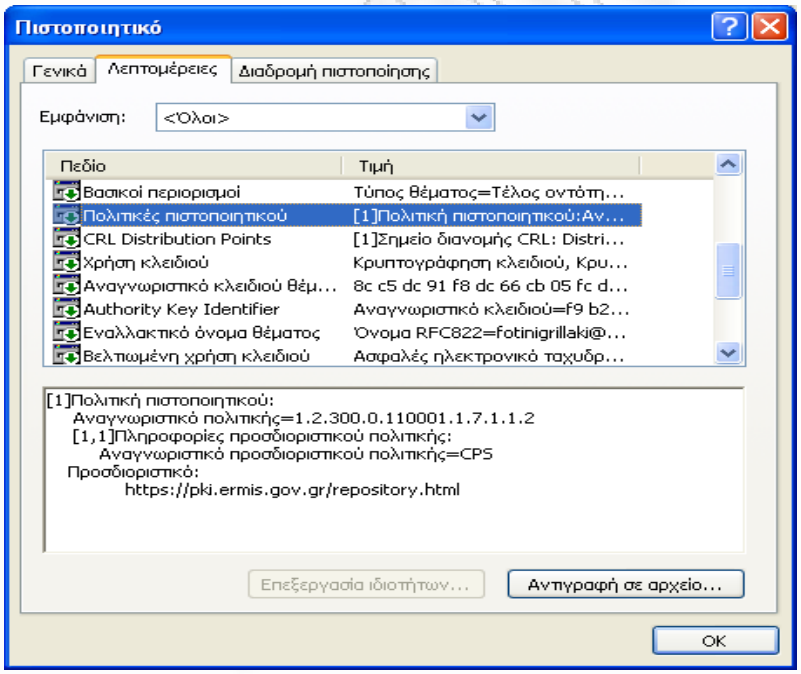
Στο πεδίο θέμα του πιστοποιητικού εμφανίζεται το όνομα του κατόχου του πιστοποιητικού, FOTEINI GRYLLAKI.

Βλέπουμε το δημόσιο κλειδί μας, εικόνα 8.35, που δημιουργήθηκε με το κρυπτοσύστημα RSA και έχει μήκος 1024 bits. Το δημόσιο κλειδί είναι αυτό που ανακοινώνεται σε όλη τη διαδικτυακή κοινότητα.



Εικόνα 8.35: Χαρακτηριστικά πιστοποιητικού

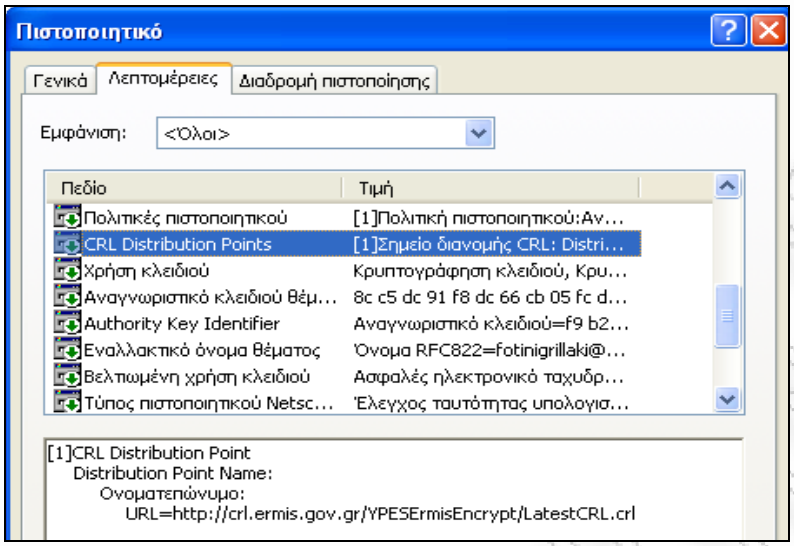
Το συγκεκριμένο πιστοποιητικό, όπως και κάθε πιστοποιητικό τελικού χρήστη που χρησιμοποιείται για κρυπτογράφηση ηλεκτρονικών δεδομένων, σύμφωνα με τον ‘’Κανονισμό πιστοποίησης της αρχής πιστοποίησης του ελληνικού δημοσίου’’ ακολουθεί την πολιτική πιστοποιητικού 2 (ΠΠ2). Υπάρχουν 7 διαφορετικές πολιτικές πιστοποιητικού της ΑΠΕΔ ανάλογα με την κάθε περίπτωση. Η τιμή προσδιοριστή αντικειμένου για την ΠΠ2 είναι η 1.2.300.0.110001.1.7.1.1.**2.,** εικόνα 8.36. Το καταλαβαίνουμε βλέποντας τον τελευταίο αριθμό. Ο τελευταίος αριθμός είναι 2, άρα αντιστοιχεί στην ΠΠ2.



Εικόνα 8.36: Χαρακτηριστικά πιστοποιητικού

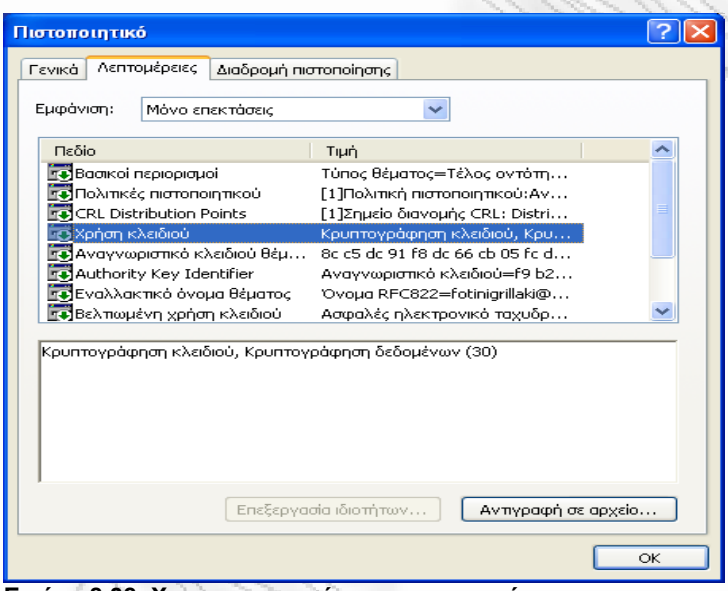
Ο CRL Distribution Points, εικόνα 8.37, περιλαμβάνει τον κατάλογο των ανακληθέντων πιστοποιητικών. Ο υπολογιστής μας κάνει αυτόματα τον έλεγχο κάθε φορά. Σύμφωνα με τον ‘’Κανονισμό πιστοποίησης της αρχής πιστοποίησης του ελληνικού δημοσίου’’, με την ανάκληση

ενός πιστοποιητικού τελικού χρήστη οι εκδότριες αρχές πιστοποίησης πρέπει να δημοσιεύσουν άμεσα την ανάκληση αυτή. Κάθε εκδότρια αρχή πιστοποίησης είναι υποχρεωμένη να εκδίδει καταλόγους ανακληθέντων πιστοποιητικών για τα πιστοποιητικά τελικών χρηστών που έχει εκδώσει.



Εικόνα 8.37: Χαρακτηριστικά πιστοποιητικού

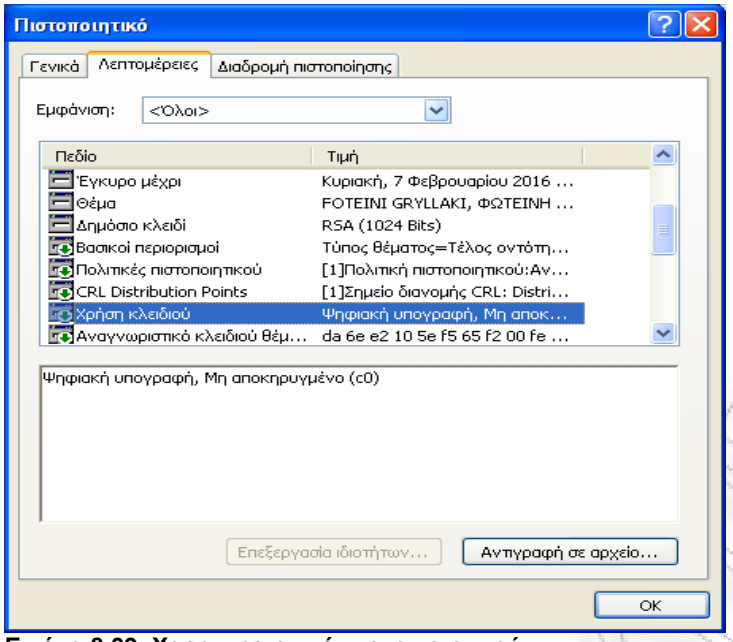
Στο πεδίο ‘’χρήση κλειδιού’’ βλέπουμε το σκοπό που χρησιμοποιείται το πιστοποιητικό. Το συγκεκριμένο χρησιμοποιείται για κρυπτογράφηση δεδομένων, εικόνα 8.38.



Εικόνα 8.38: Χαρακτηριστικά πιστοποιητικού

Ομοίως, κάνοντας τα ίδια βήματα μπορούμε να δούμε τις λεπτομέρειες για το δεύτερο πιστοποιητικό, εικόνα 8.33, που εκδώσαμε.

Έτσι π.χ. στο πεδίο ‘’χρήση κλειδιού’’ βλέπουμε το σκοπό που χρησιμοποιείται το πιστοποιητικό δηλαδή για να υπογράφουμε ψηφιακά κάθε ηλεκτρονικό έγγραφο, εικόνα 8.39.



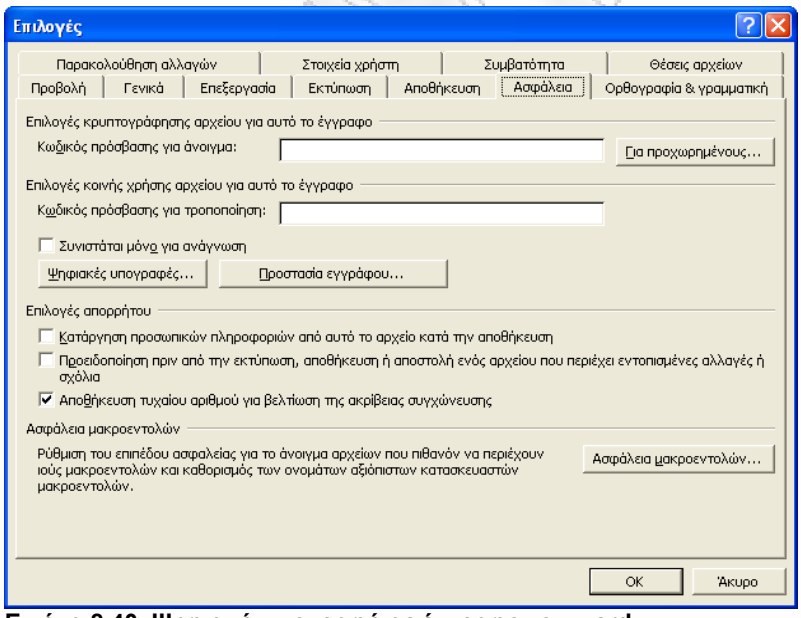
Εικόνα 8.39: Χαρακτηριστικά πιστοποιητικού

8.2 Χρήση των ψηφιακών πιστοποιητικών

8.2.1 Ψηφιακή υπογραφή σ' ένα ηλεκτρονικό έγγραφο του Word

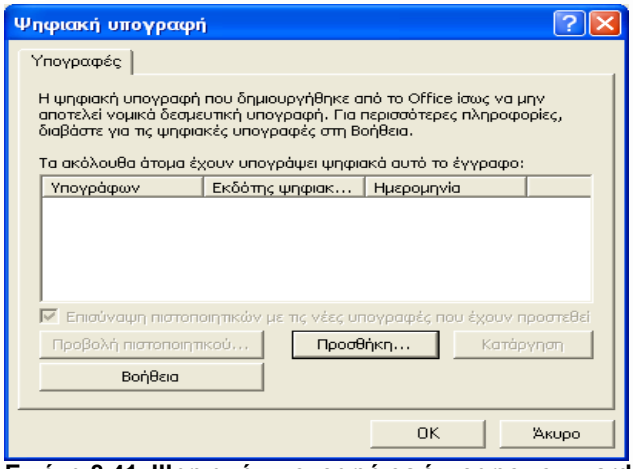
Έστω ότι θέλουμε να υπογράψουμε ψηφιακά ένα έγγραφο του word. Αφού δημιουργήσουμε το έγγραφο πρέπει πρώτα να το αποθηκεύσουμε σε όποιο σημείο του υπολογιστή μας θέλουμε, διαφορετικά δε θα μπορούμε να εισάγουμε τη ψηφιακή μας υπογραφή.

Για να υπογράψουμε ψηφιακά λοιπόν το έγγραφο που έχουμε επιλέξει, από το μενού του εγγράφου επιλέγουμε ''Εργαλεία'' και έπειτα ''Επιλογές''. Στη συνέχεια από την καρτέλα ''Επιλογές'' επιλέγουμε ''Ασφάλεια'', εικόνα 8.40.



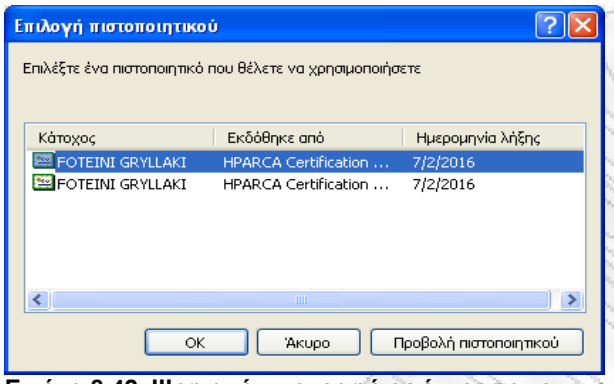
Εικόνα 8.40: Ψηφιακή υπογραφή σε έγγραφο του word

Κάνουμε ''κλικ'' στις ''ψηφιακές υπογραφές'' και εμφανίζεται η καρτέλα ''Υπογραφές'', εικόνα 8.41.



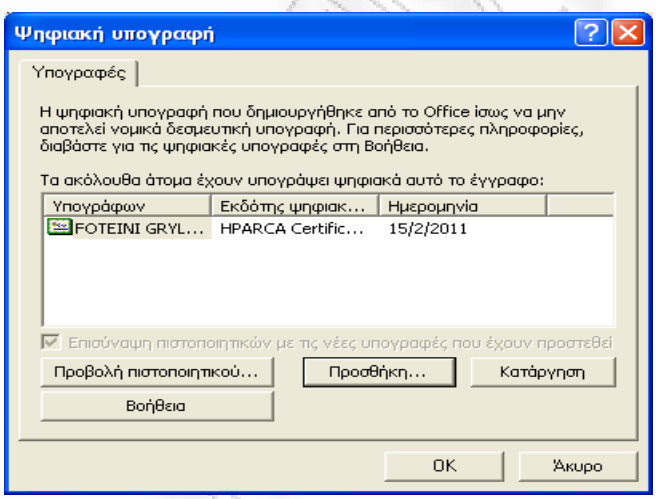
Εικόνα 8.41: Ψηφιακή υπογραφή σε έγγραφο του word

Κάνουμε κλικ στην ‘’Προσθήκη’’ και εμφανίζονται όλα τα πιστοποιητικά που έχουμε στην κατοχή μας, εικόνα 8.42.



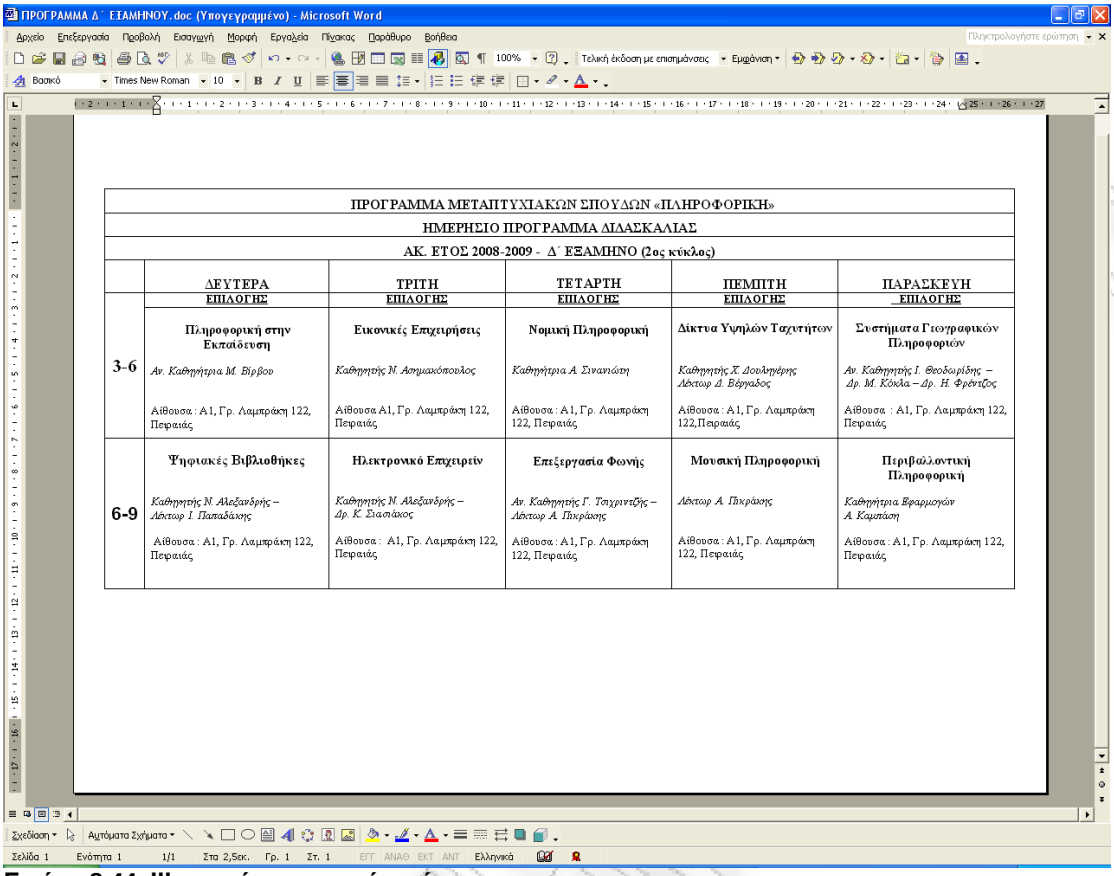
Εικόνα 8.42: Ψηφιακή υπογραφή σε έγγραφο του word

Επιλέγουμε αυτό που χρησιμοποιείται για τη ψηφιακή υπογραφή και κλικ στο ‘’ΟΚ’’, εικόνα 8.43.



Εικόνα 8.43: Ψηφιακή υπογραφή σε έγγραφο του word

Ξανά κλικ στο ‘’ΟΚ’’ και η ψηφιακή μας υπογραφή έχει προστεθεί στο έγγραφό μας. Η ψηφιακή υπογραφή δηλώνεται με ένα μικρό κόκκινο σημάδι στο τέλος του εγγράφου, εικόνα 8.44 και 8.45.



ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΠΛΗΡΟΦΟΡΙΚΗ»

ΗΜΕΡΗΣΙΟ ΠΡΟΓΡΑΜΜΑ ΔΙΔΑΣΚΑΛΙΑΣ

ΑΚ. ΕΤΟΣ 2008-2009 - Δ΄ ΕΞΑΜΗΝΟ (2ος κύκλος)

	ΔΕΥΤΕΡΑ ΕΠΙΛΟΓΗΣ	ΤΡΙΤΗ ΕΠΙΛΟΓΗΣ	ΤΕΤΑΡΤΗ ΕΠΙΛΟΓΗΣ	ΠΕΜΠΤΗ ΕΠΙΛΟΓΗΣ	ΠΑΡΑΣΚΕΥΗ ΕΠΙΛΟΓΗΣ
3-6	**Πληροφορική στην Εκπαίδευση** *Αν. Καθηγήτρια Μ. Βίρβου* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Εικονικές Επιχειρήσεις** *Καθηγητής Ν. Ασημακόπουλος* Αίθουσα Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Νομική Πληροφορική** *Καθηγήτρια Α. Συνοδινού* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Δίκτυα Υψηλών Ταχυτήτων** *Καθηγητής Χ. Δουληγέρης Λέκτωρ Δ. Βέργαδος* Αίθουσα : Α1, Γρ. Λαμπράκη 122,Πειραιάς	**Συστήματα Γεωγραφικών Πληροφοριών** *Αν. Καθηγητής Ι. Θεοδωρίδης – Δρ. Μ. Κόκλα – Δρ. Η. Φρέντζος* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς
6-9	**Ψηφιακές Βιβλιοθήκες** *Καθηγητής Ν. Αλεξανδρής – Λέκτωρ Ι. Παπαδάκης* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Ηλεκτρονικό Επχειρείν** *Καθηγητής Ν. Αλεξανδρής – Δρ. Κ. Σιασιάκος* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Επεξεργασία Φωνής** *Αν. Καθηγητής Γ. Τσιχριντζής – Λέκτωρ Α. Πικράκης* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Μουσική Πληροφορική** *Λέκτωρ Α. Πικράκης* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς	**Περιβαλλοντική Πληροφορική** *Καθηγήτρια Εφαρμογών Α. Καμπάκη* Αίθουσα : Α1, Γρ. Λαμπράκη 122, Πειραιάς

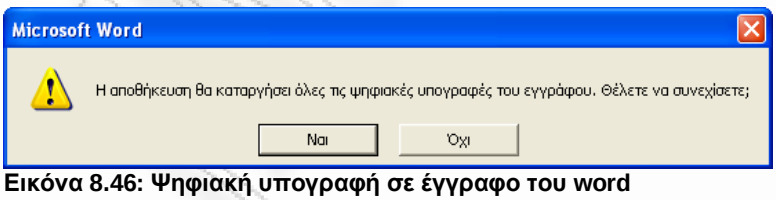
Εικόνα 8.44: Ψηφιακή υπογραφή σε έγγραφο του word

ψηφιακή υπογραφή

ψηφιακή υπογραφή

Εικόνα 8.45: Ψηφιακή υπογραφή σε έγγραφο του word

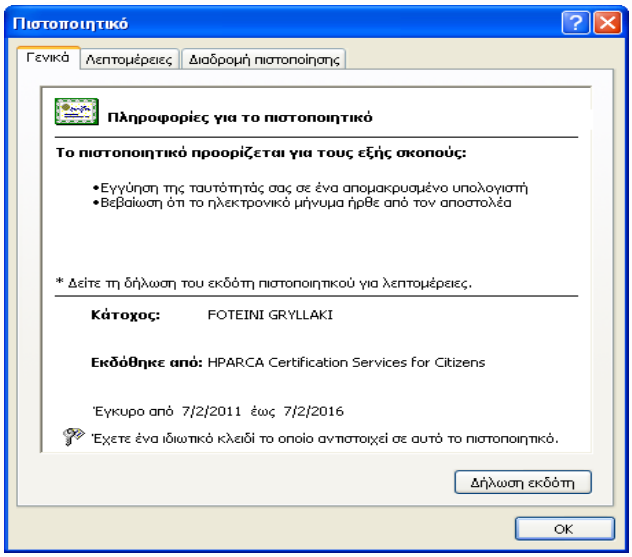
Αν τώρα προσπαθήσουμε να κάνουμε κάποια τροποποίηση στο υπογεγραμμένο μας έγγραφο θα εμφανιστεί μια προειδοποίηση, εικόνα 8.46, όπου θα μας ενημερώνει ότι η ενέργειά μας αυτή θα καταργήσει την ψηφιακή μας υπογραφή στο συγκεκριμένο έγγραφο.



Εικόνα 8.46: Ψηφιακή υπογραφή σε έγγραφο του word

Μ' αυτό τον τρόπο προστατεύουμε τα έγγραφά μας από οποιαδήποτε αλλαγή θελήσει να κάνει κάποιος.

Κάνοντας ''κλικ'' πάνω στο εικονίδιο της ψηφιακής μας υπογραφής, στην εικόνα 8.44, μπορούμε να προβάλουμε το πιστοποιητικό που χρησιμοποιήσαμε για τη προσθήκη της υπογραφής μας, εικόνα 8.47.



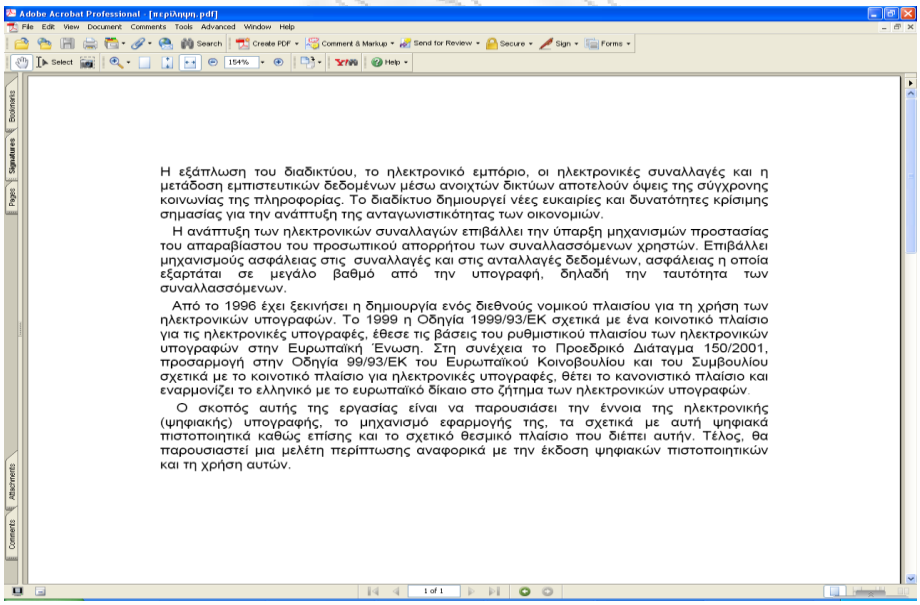
Εικόνα 8.47: Προβολή πιστοποιητικού

Στόχος λοιπόν, με το να υπογράφουμε ένα έγγραφο είναι να πιστοποιούμε την ακεραιότητα του μηνύματος, δηλαδή ότι δεν έχει υποστεί κάποια τροποποίηση από κάποιον ξένο, αλλά και την ταυτοποίηση του δημιουργού του μηνύματος.

8.2.2 Ψηφιακή υπογραφή σ' ένα ηλεκτρονικό έγγραφο του Adobe Acrobat

Θέλουμε να υπογράψουμε ψηφιακά ένα έγγραφο του Adobe Acrobat. Αφού μετατρέψουμε το έγγραφο σε μορφή Adobe Acrobat το αποθηκεύουμε σε όποιο σημείο του υπολογιστή μας θέλουμε για να μπορέσουμε να εισάγουμε τη ψηφιακή μας υπογραφή.

Για να υπογράψουμε ψηφιακά λοιπόν το έγγραφο που έχουμε επιλέξει, εικόνα 8.48, από το μενού του εγγράφου επιλέγουμε ''Document'' έπειτα ''Digital signatures'' και τέλος ''Sign this document'', όπου εμφανίζεται η εικόνα 8.49.



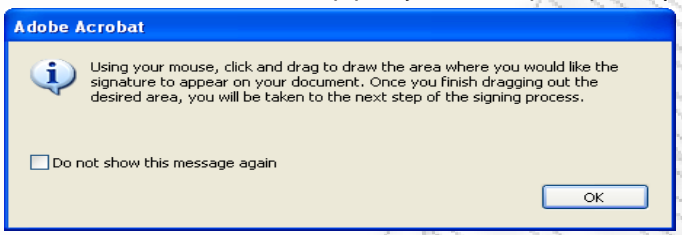
Εικόνα 8.48: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Εικόνα 8.49: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Συνεχίζουμε κάνοντας ‘‘κλικ’’ στο ‘‘Continue signing’’ όπου εμφανίζεται η εικόνα 8.50.

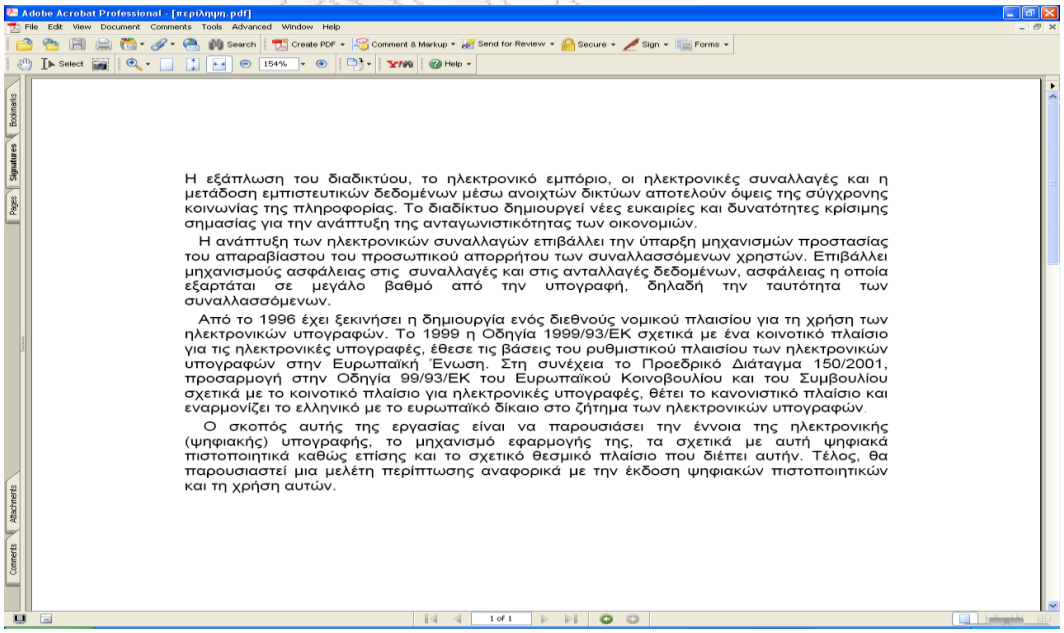
Εικόνα 8.50: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Εδώ ‘‘κλικ’’ στο ‘‘Next’’ και εμφανίζεται το παράθυρο στην εικόνα 8.51.



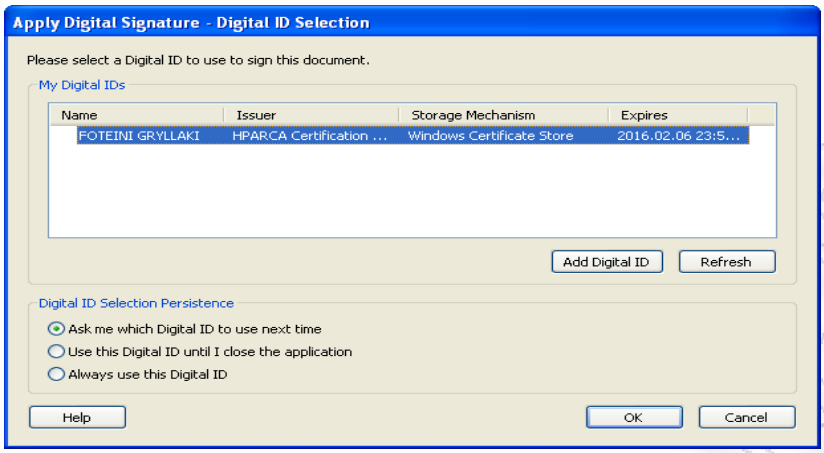
Εικόνα 8.51: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Το παράθυρο αυτό μας περιγράφει τη διαδικασία που πρέπει να ακολουθήσουμε για να εισάγουμε την υπογραφή μας στο έγγραφο. Πατώντας ‘‘ΟΚ’’ εμφανίζεται πάλι το αρχικό μας έγγραφο, εικόνα 8.52.



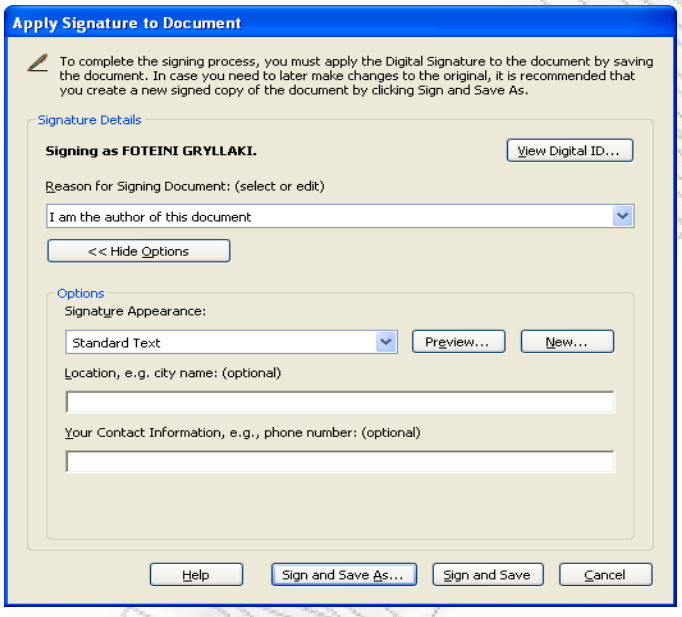
Εικόνα 8.52: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Εδώ λοιπόν, πρέπει χρησιμοποιώντας το ποντίκι μας να ‘’κλικάρουμε’’ και να σύρουμε το ποντίκι μας στο σημείο πάνω στο έγγραφο που θέλουμε να βάλουμε την υπογραφή μας. Εμείς επιλέγουμε να βάλουμε την υπογραφή μας πάνω και δεξιά του εγγράφου. Μόλις ολοκληρώσουμε την παραπάνω ενέργεια εμφανίζεται το παράθυρο στην εικόνα 8.53.



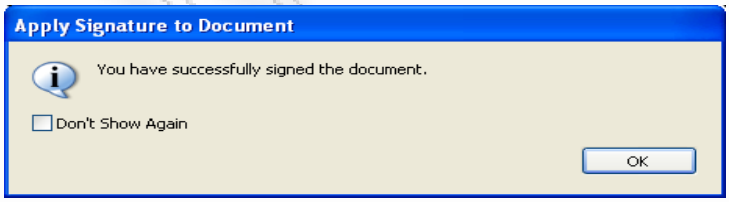
Εικόνα 8.53: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Εδώ εμφανίζεται το πιστοποιητικό που θα χρησιμοποιήσουμε για την ψηφιακή μας υπογραφή, ‘κλικ’ στο ‘OK’ και προχωράμε στην εικόνα 8.54.



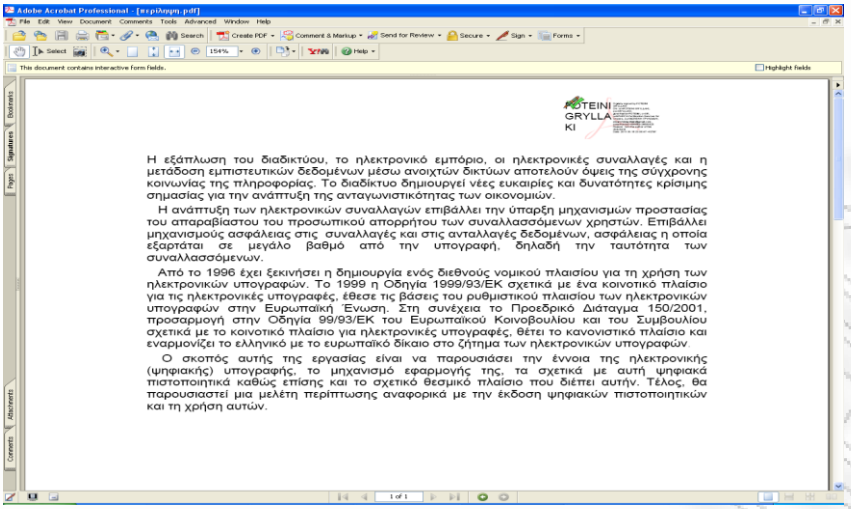
Εικόνα 8.54: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Εδώ χωρίς να είναι υποχρεωτικό μπορούμε να συμπληρώσουμε το λόγο που υπογράφουμε το έγγραφο π.χ. εδώ γράψαμε ‘ I am the author of this document’. Στη συνέχεια κάνουμε ‘κλικ’ στο ‘Sign and save as’ και εμφανίζεται το παράθυρο στην εικόνα 8.55, όπου μας ενημερώνει ότι η υπογραφή εισήχθει στο έγγραφό μας με επιτυχία.



Εικόνα 8.55: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

Πατώντας ‘ΟΚ’ εμφανίζεται το παράθυρο στην εικόνα 8.56, δηλαδή το έγγραφό μας υπογεγραμμένο με την ψηφιακή μας υπογραφή πάνω και δεξιά όπως την είχαμε σχεδιάσει πριν

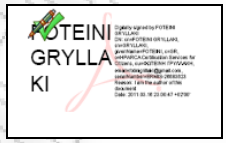


Η εξάπλωση του διαδικτύου, το ηλεκτρονικό εμπόριο, οι ηλεκτρονικές συναλλαγές και η μετάδοση εμπιστευτικών δεδομένων μέσω ανοιχτών δικτύων αποτελούν όψεις της σύγχρονης κοινωνίας της πληροφορίας. Το διαδίκτυο δημιουργεί νέες ευκαιρίες και δυνατότητες κρίσιμης σημασίας για την ανάπτυξη της ανταγωνιστικότητας των οικονομιών.

Η ανάπτυξη των ηλεκτρονικών συναλλαγών επιβάλλει την ύπαρξη μηχανισμών προστασίας του απαραβίαστου του προσωπικού απορρήτου των συναλλασσόμενων χρηστών. Επιβάλλει μηχανισμούς ασφάλειας στις συναλλαγές και στις ανταλλαγές δεδομένων, ασφάλειας η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, δηλαδή την ταυτότητα των συναλλασσόμενων.

Από το 1996 έχει ξεκινήσει η δημιουργία ενός διεθνούς νομικού πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών. Το 1999 η Οδηγία 1999/93/ΕΚ σχετικά με ένα κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, έθεσε τις βάσεις του ρυθμιστικού πλαισίου των ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Ένωση. Στη συνέχεια το Προεδρικό Διάταγμα 150/2001, προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, θέτει το κανονιστικό πλαίσιο και εναρμονίζει το ελληνικό με το ευρωπαϊκό δίκαιο στο ζήτημα των ηλεκτρονικών υπογραφών.

Ο σκοπός αυτής της εργασίας είναι να παρουσιάσει την έννοια της ηλεκτρονικής (ψηφιακής) υπογραφής, το μηχανισμό εφαρμογής της, τα σχετικά με αυτή ψηφιακά πιστοποιητικά καθώς επίσης και το σχετικό θεσμικό πλαίσιο που διέπει αυτήν. Τέλος, θα παρουσιαστεί μια μελέτη περίπτωσης αναφορικά με την έκδοση ψηφιακών πιστοποιητικών και τη χρήση αυτών.



Εικόνα 8.56: Ψηφιακή υπογραφή σε έγγραφο του Adobe Acrobat

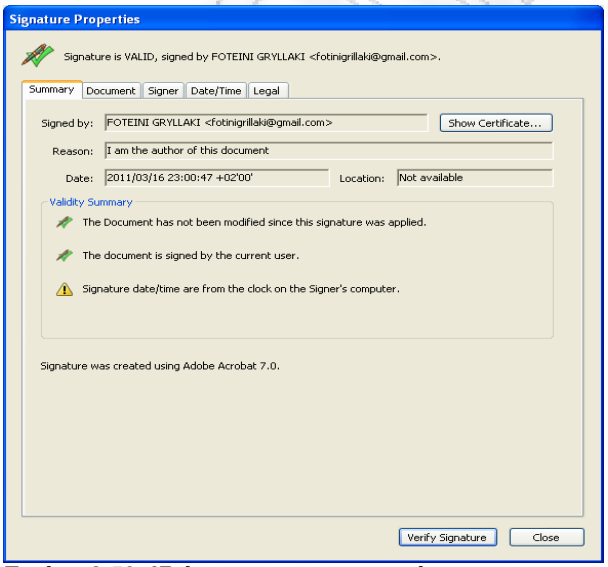
Εικόνα 8.57: Ψηφιακή υπογραφή

Η ψηφιακή μας υπογραφή, εικόνα 8.57, εμφανίζεται με το όνομά μας FOTEINI GRYLLAKI και ένα πράσινο ‘τικ’. Το πράσινο ‘τικ’ δείχνει ότι η υπογραφή είναι έγκυρη μετά τον αυτόματο έλεγχο που έκανε ο υπολογιστής μας.

Για να δούμε τις ιδιότητες της υπογραφής μας αρκεί να κάνουμε ‘κλικ’ πάνω στην υπογραφή μας, όπου πρώτα θα εμφανιστεί το παράθυρο στην εικόνα 8.58 όπου μας ενημερώνει από ποιον έχει υπογραφεί το έγγραφο και το εάν έχει τροποποιηθεί.

Εικόνα 8.58: Ιδιότητες της υπογραφής

Τις ιδιότητες της υπογραφής θα τις δούμε κάνοντας ‘κλικ’ στο ‘Signature Properties’ όπου θα εμφανιστεί και το παράθυρο στην εικόνα 8.59.

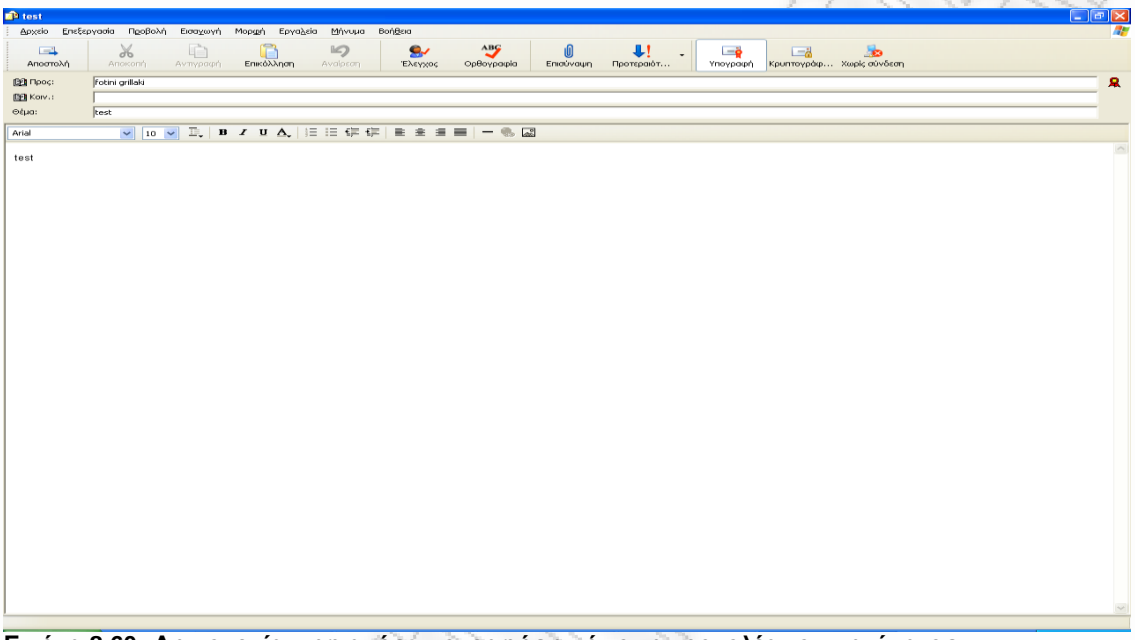


Εικόνα 8.59: Ιδιότητες της υπογραφής

8.2.3 Ψηφιακή υπογραφή σε μήνυμα ηλεκτρονικού ταχυδρομείου

8.2.3.1 Δημιουργία ψηφιακής υπογραφής από τον αποστολέα του μηνύματος

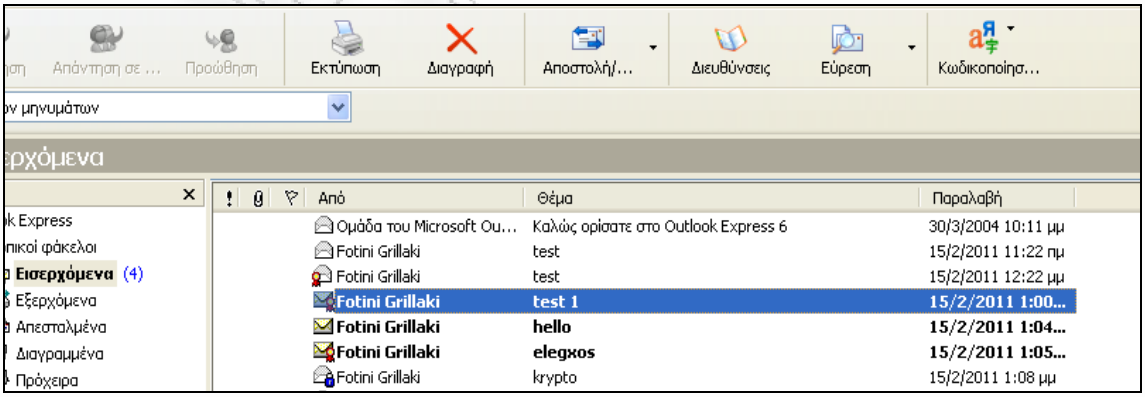
Θέλουμε να στείλουμε με το ηλεκτρονικό ταχυδρομείο (χρησιμοποιώντας το outlook express) ένα μήνυμα υπογεγραμμένο ψηφιακά. Αφού συντάξουμε το μήνυμά μας κάνουμε κλικ στο εικονίδιο ‘’υπογραφή’’(ή από το μενού επιλέγουμε ‘’εργαλεία’’ και έπειτα ‘’ψηφιακή υπογραφή’’) και το μήνυμά μας έχει υπογραφεί, εικόνα 8.60.



Εικόνα 8.60: Δημιουργία ψηφιακής υπογραφής από τον αποστολέα του μηνύματος

Όλη η διαδικασία που περιγράψαμε στο κεφάλαιο 4.1.2.2 για τη δημιουργία της ψηφιακής υπογραφής γίνεται αυτόματα από τον υπολογιστή μας εφόσον έχουμε κάνει τις απαραίτητες εγκαταστάσεις που περιγράψαμε από την αρχή του κεφαλαίου 8. Επομένως το κείμενό μας μαζί με τη ψηφιακή μας υπογραφή, το δημόσιο κλειδί και το πιστοποιητικό μας διαβιβάζονται στον παραλήπτη πατώντας το κουμπί ‘’αποστολή’’.

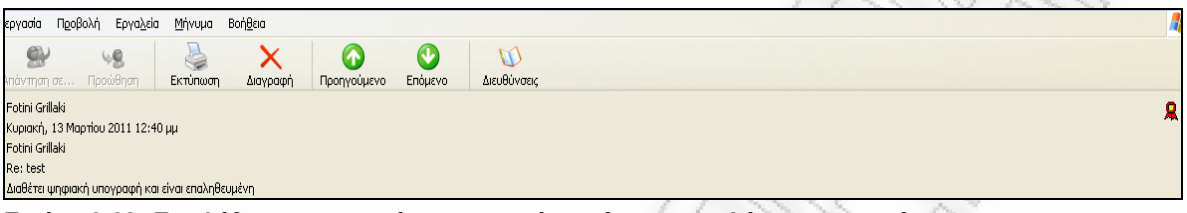
Το υπογεγραμμένο μήνυμα θα φαίνεται στα εισερχόμενα του παραλήπτη μας όπως στην εικόνα 8.61, δηλαδή με το εικονίδιο υπογεγραμμένου μηνύματος.



Εικόνα 8.61: Υπογεγραμμένο μήνυμα

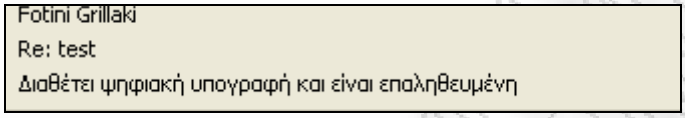
8.2.3.2 Επαλήθευση της ψηφιακής υπογραφής από τον παραλήπτη του μηνύματος

Ο παραλήπτης ανοίγοντας το μήνυμά του, εικόνα 8.62, θα παρατηρήσει ότι υπάρχει στα δεξιά το σχήμα της ψηφιακής υπογραφής, εικόνα 8.63, όπως επίσης μια προειδοποίηση ασφαλείας ότι το μήνυμα διαθέτει ψηφιακή υπογραφή και είναι επαληθευμένη, εικόνα 8.64. Ομοίως, όπως και στη δημιουργία της ψηφιακής υπογραφής, η επαλήθευση της ψηφιακής υπογραφής γίνεται αυτόματα από τον υπολογιστή μας μέσα σε λίγα δευτερόλεπτα χωρίς ο χρήστης να καταλάβει τίποτα, με τη διαδικασία που έχουμε περιγράψει στο κεφάλαιο 4.1.2.3.



Εικόνα 8.62: Επαλήθευση ψηφιακής υπογραφής από τον παραλήπτη του μηνύματος

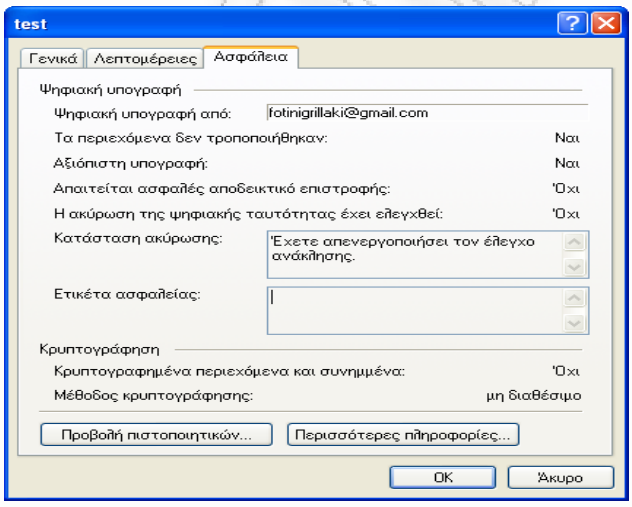
Εικόνα 8.63: Ψηφιακή υπογραφή



Εικόνα 8.64: Προειδοποίηση ασφαλείας

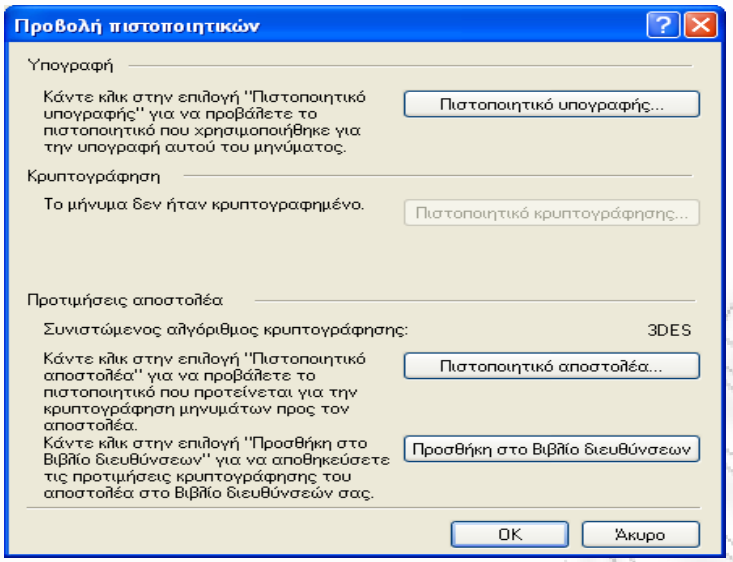
Το μήνυμα ηλεκτρονικού ταχυδρομείου που λαμβάνει ο παραλήπτης με την ψηφιακή υπογραφή του αποστολέα του επιτρέπει να επαληθεύσει την αυθεντικότητα του μηνύματος, δηλαδή ότι το μήνυμα προέρχεται όντως από τον υποτιθέμενο αποστολέα και ότι δεν έχει αλλοιωθεί κατά τη μεταβίβαση.

Κάνοντας ‘’κλικ’’ πάνω στο εικονίδιο της ψηφιακής υπογραφής, εικόνα 8.62, θα εμφανιστεί ένα παράθυρο, εικόνα 8.65, όπου μπορούμε να προβάλουμε το πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή του συγκεκριμένου μηνύματος.

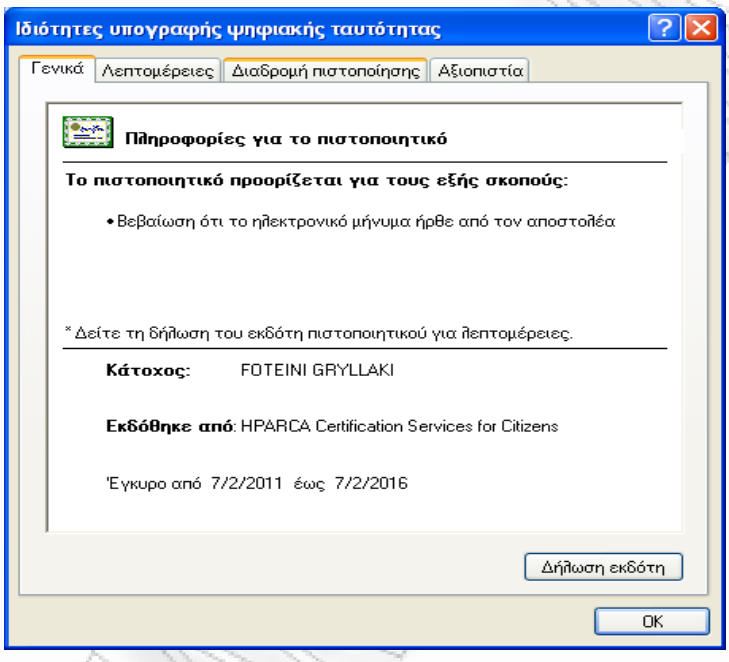


Εικόνα 8.65: Προβολή πιστοποιητικού

Στο παράθυρο της εικόνας 8.65 επιλέγουμε ‘’Προβολή πιστοποιητικών’’ και στη συνέχεια από το παράθυρο που εμφανίζεται, εικόνα 8.66, επιλέγουμε ‘’πιστοποιητικό υπογραφής’’ όπου και εμφανίζεται το πιστοποιητικό μας, εικόνα 8.67.

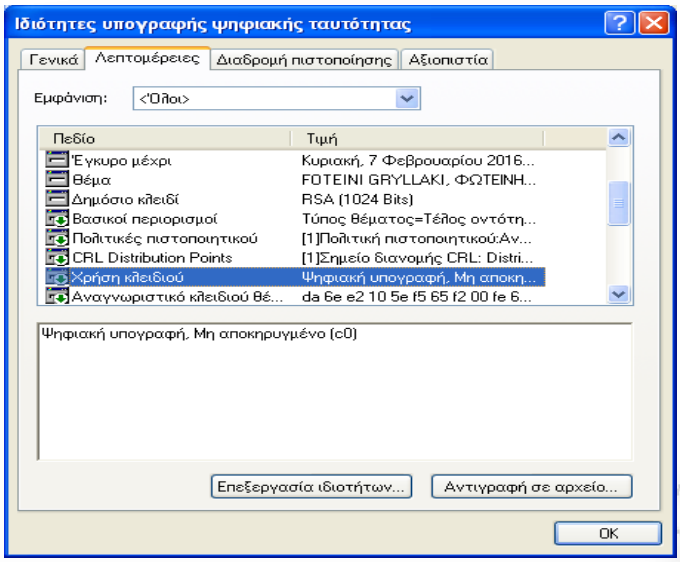


Εικόνα 8.66: Προβολή πιστοποιητικού



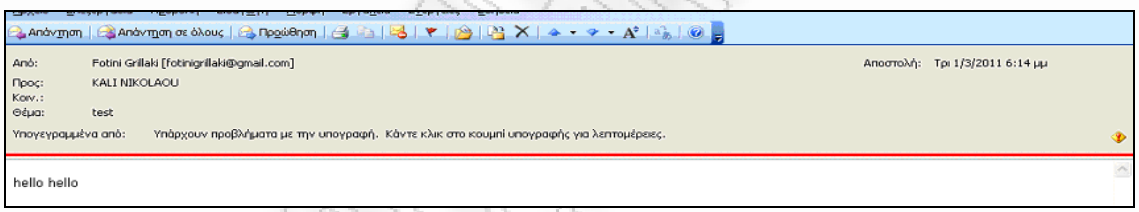
Εικόνα 8.67: Προβολή πιστοποιητικού

Επιλέγοντας τις ‘’λεπτομέρειες’’ του πιστοποιητικού βλέπουμε και τη χρήση του πιστοποιητικού που είναι για ψηφιακή υπογραφή, εικόνα 8.68.

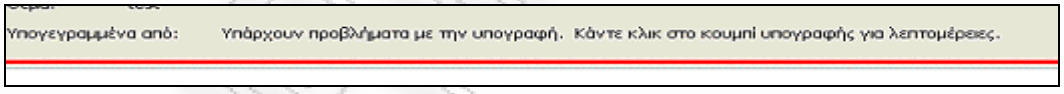


Εικόνα 8.68: Χαρακτηριστικά πιστοποιητικού

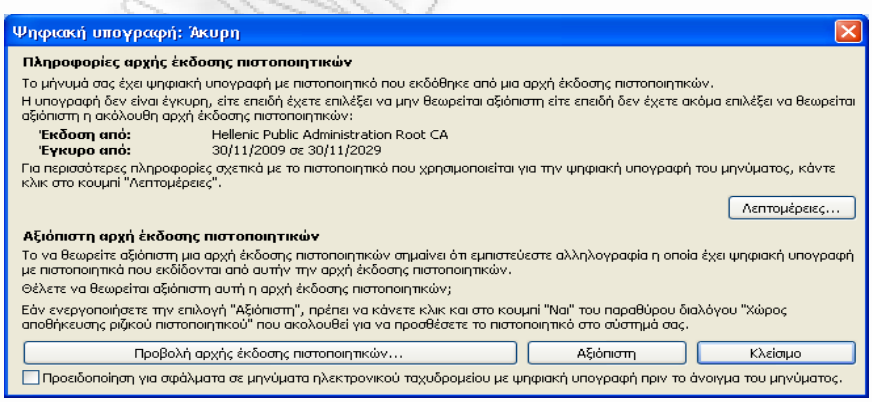
Μπορούμε να στείλουμε σε οποιονδήποτε θέλουμε ένα ηλεκτρονικό έγγραφο υπογεγραμμένο με την ψηφιακή μας υπογραφή, χωρίς ο παραλήπτης απαραίτητα να έχει ψηφιακό πιστοποιητικό. Ο παραλήπτης θα μπορεί να διαβάσει κανονικά το μήνυμα που θα του έχει σταλεί, εικόνα 8.69, απλώς εάν ο παραλήπτης δεν έχει εγκαταστήσει την Αρχή Πιστοποίησης θα εμφανιστεί μια προειδοποίηση, εικόνα 8.70, όπου θα τον ενημερώνει ότι υπάρχει πρόβλημα με την υπογραφή και ότι δεν μπορεί να ελεγχθεί η εγκυρότητά της, εικόνα 8.71, δηλαδή η αυθεντικότητα του ηλεκτρονικού μηνύματος.



Εικόνα 8.69: Αποστολή υπογεγραμμένου μηνύματος



Εικόνα 8.70: Μήνυμα ασφαλείας



Εικόνα 8.71: Μήνυμα ασφαλείας

Ο παραλήπτης όμως μπορεί αν θέλει κάνοντας ‘’κλικ’’ στο ‘’Αξιόπιστη’’, εικόνα 8.71, να θεωρήσει αξιόπιστη την Αρχή Πιστοποίησης Ελληνικού Δημοσίου και να προσθέσει το πιστοποιητικό στο σύστημά του. Οπότε από εδώ και πέρα, ο έλεγχος για την αυθεντικότητα του ηλεκτρονικού μηνύματος θα γίνεται αυτόματα για κάθε υπογεγραμμένο μήνυμα που θα δέχεται ο παραλήπτης και που θα έχει εκδοθεί από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου.

8.2.4 Κρυπτογράφηση ηλεκτρονικού μηνύματος

Έστω ότι θέλουμε να στείλουμε με το ηλεκτρονικό ταχυδρομείο ένα κρυπτογραφημένο μήνυμα σε κάποιον, ώστε να είμαστε σίγουροι ότι κανένας άλλος δε θα διαβάσει το μήνυμά μας.

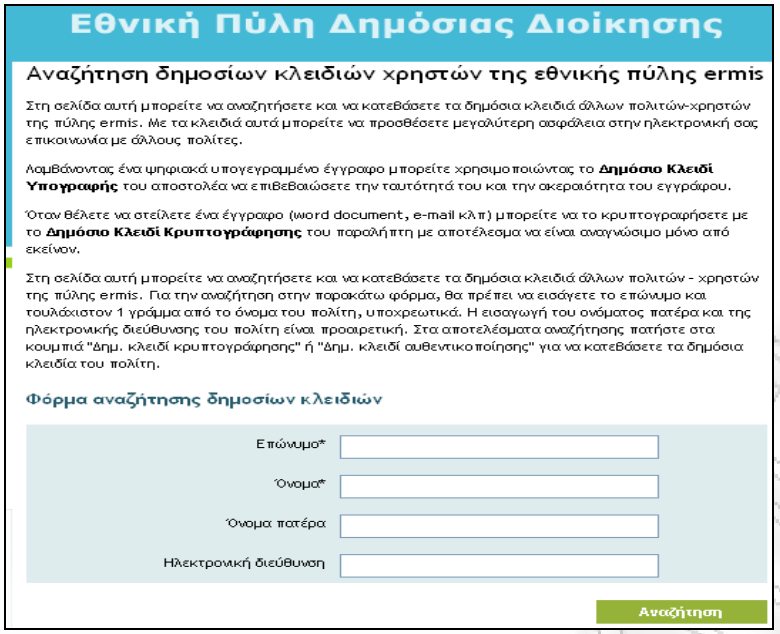
Αυτό που πρώτα πρέπει να κάνουμε είναι να ψάξουμε και να βρούμε το δημόσιο κλειδί του παραλήπτη, αφού με αυτό θα κρυπτογραφήσουμε το μήνυμά μας. Έτσι όταν του στείλουμε το κρυπτογραφημένο μήνυμα, αυτός χρησιμοποιώντας το ιδιωτικό του κλειδί, που το γνωρίζει μόνον ο ίδιος, θα μπορεί να το αποκρυπτογραφήσει και επομένως να το διαβάσει. Δηλαδή το μήνυμα που θα στείλουμε θα κρυπτογραφηθεί από εμάς με το δημόσιο κλειδί του παραλήπτη και θα αποκρυπτογραφηθεί από αυτόν με το ιδιωτικό του κλειδί.

Όλα τα ψηφιακά πιστοποιητικά (δηλαδή τα δημόσια κλειδιά) άλλων πολιτών - χρηστών της Εθνικής Πύλης Δημόσιας Διοίκησης ermis βρίσκονται σ’ ένα χώρο αποθήκευσης υποδομής δημοσίου κλειδιού ermis (Repository) στο σύνδεσμο: https://pki.ermis.gov.gr/repository.html, εικόνα 8.72.

Εικόνα 8.72: Αναζήτηση ψηφιακού πιστοποιητικού

Αξίζει να παρατηρήσουμε ότι στο σύνδεσμο αυτόν υπάρχει ενότητα ‘’κατάλογος ανακληθέντων πιστοποιητικών’’. Ο κατάλογος αυτός είναι μια λίστα που περιέχει όλα τα ψηφιακά πιστοποιητικά που για οποιοδήποτε λόγο έχουν ακυρωθεί. Οι κατάλογοι ανακληθέντων πιστοποιητικών της πύλης ermis ενημερώνονται μία φορά την ημέρα αυτόματα από το σύστημά μας. Με αυτό τον τρόπο είμαστε σίγουροι για το ποια ψηφιακά πιστοποιητικά βρίσκονται σε ισχύ ή όχι.

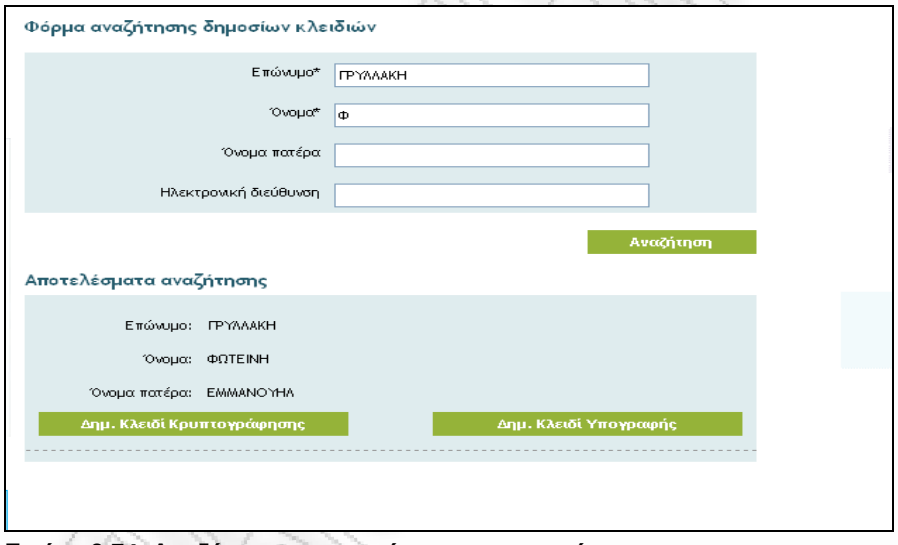
Στο παράθυρο λοιπόν αυτό της εικόνας 8.72, επιλέγοντας ‘’αναζήτηση ψηφιακών πιστοποιητικών τελικών χρηστών’’ εμφανίζεται το παράθυρο αναζήτησης δημοσίων κλειδιών χρηστών της εθνικής πύλης ermis, εικόνα 8.73.



Εικόνα 8.73: Αναζήτηση ψηφιακού πιστοποιητικού

Εδώ μπορούμε να αναζητήσουμε και να κατεβάσουμε τα δημόσια κλειδιά άλλων πολιτών - χρηστών της πύλης ermis που θέλουμε.

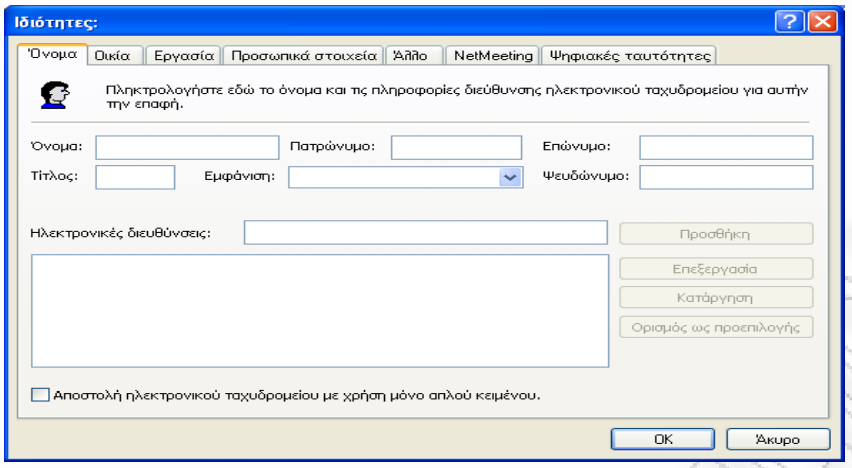
Συμπληρώνουμε τη φόρμα με το επώνυμο και το όνομα αυτού που θέλουμε να στείλουμε το μήνυμα και συνεπώς αυτού που θέλουμε το δημόσιο κλειδί του. Έστω ότι θέλουμε να βρούμε το κλειδί του χρήστη ΓΡΥΛΛΑΚΗ ΦΩΤΕΙΝΗ, εικόνα 8.74.



Εικόνα 8.74: Αναζήτηση ψηφιακού πιστοποιητικού

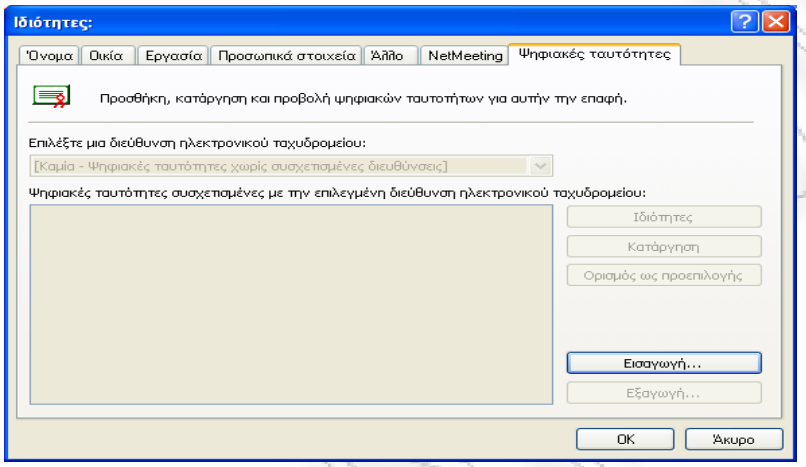
Διαλέγουμε δημόσιο κλειδί κρυπτογράφησης και αποθήκευση. Οπότε και το δημόσιο κλειδί έχει αποθηκευτεί πια στον υπολογιστή μας.

Στη συνέχεια, στο Outlook express στο μενού ‘’εργαλεία’’ επιλέγουμε ‘’βιβλία διευθύνσεων’’. Θέλουμε να δημιουργήσουμε μια νέα επαφή οπότε από το εικονίδιο ‘’δημιουργία’’ επιλέγουμε ‘’νέα επαφή’’, εικόνα 8.75.



Εικόνα 8.75: Δημιουργία νέας επαφής

Συμπληρώνουμε τη φόρμά μας και επιλέγουμε την καρτέλα ‘’ψηφιακές ταυτότητες’’, εικόνα 8.76.

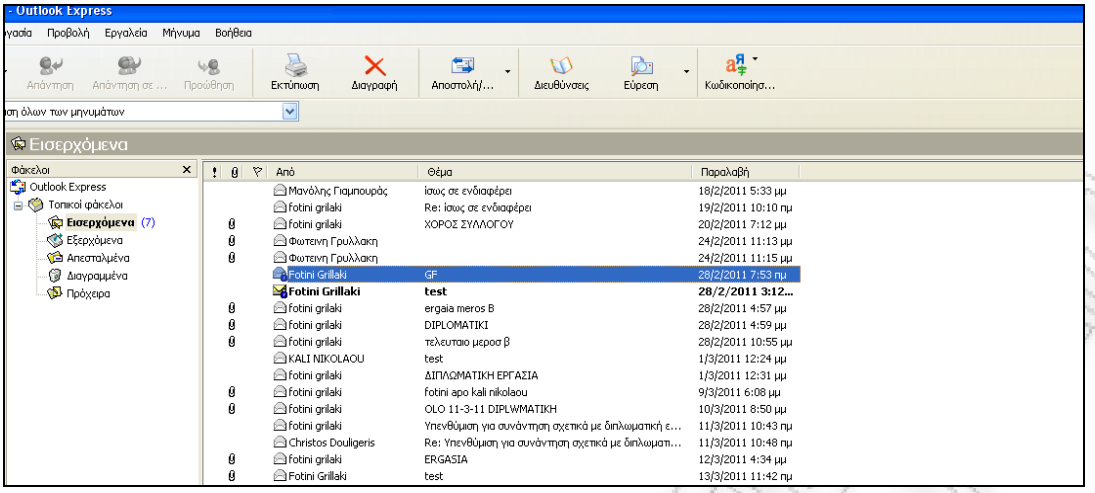


Εικόνα 8.76: Εισαγωγή ψηφιακής ταυτότητας

Κάνοντας κλικ στην ‘’Εισαγωγή’’, ψάχνουμε και εισάγουμε το πιστοποιητικό με το δημόσιο κλειδί του παραλήπτη.

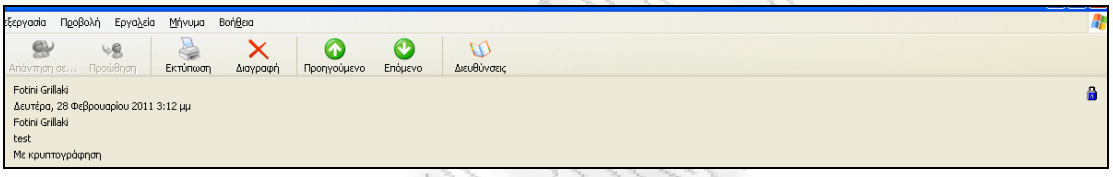
Με αυτό τον τρόπο έχουμε το δημόσιο κλειδί του παραλήπτη μας και μπορούμε πια να κρυπτογραφήσουμε το μήνυμά μας.

Το κρυπτογραφημένο μήνυμα θα φαίνεται στα εισερχόμενα του παραλήπτη μας όπως στην εικόνα 8.77, δηλαδή με μια μπλε κλειδαριά. Αυτό σημαίνει ότι ο αποστολέας έχει κρυπτογραφήσει αυτό το μήνυμα με το δημόσιο κλειδί του παραλήπτη και έτσι ο παραλήπτης μπορεί να είναι βέβαιος ότι κανένας άλλος δεν έχει διαβάσει το μήνυμα αυτό.



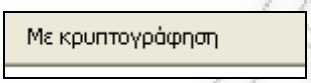
Εικόνα 8.77: Κρυπτογραφημένο μήνυμα

Ο παραλήπτης ανοίγοντας το κρυπτογραφημένο μήνυμα, εικόνα 8.78, θα παρατηρήσει ότι υπάρχει στα δεξιά το σχήμα μιας μπλε κλειδαριάς, εικόνα 8.79, όπως επίσης μια προειδοποίηση ασφαλείας ότι το μήνυμα είναι κρυπτογραφημένο, εικόνα 8.80.



Εικόνα 8.78: Άνοιγμα κρυπτογραφημένου μηνύματος

Εικόνα 8.79: Σχήμα αναγνώρισης κρυπτογραφημένου μηνύματος

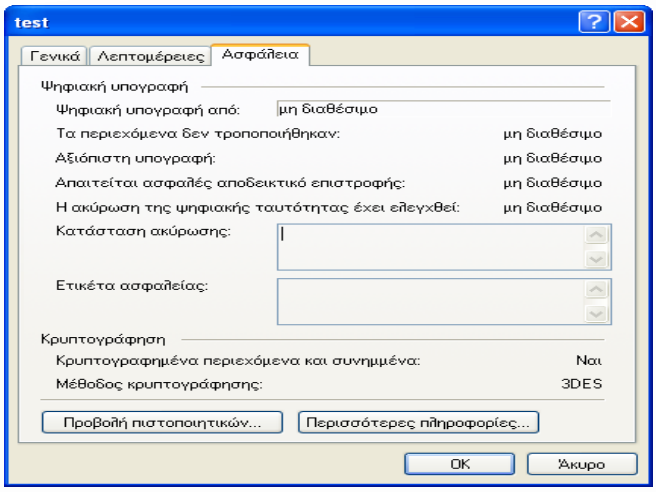


Εικόνα 8.80: Προειδοποίηση ασφαλείας

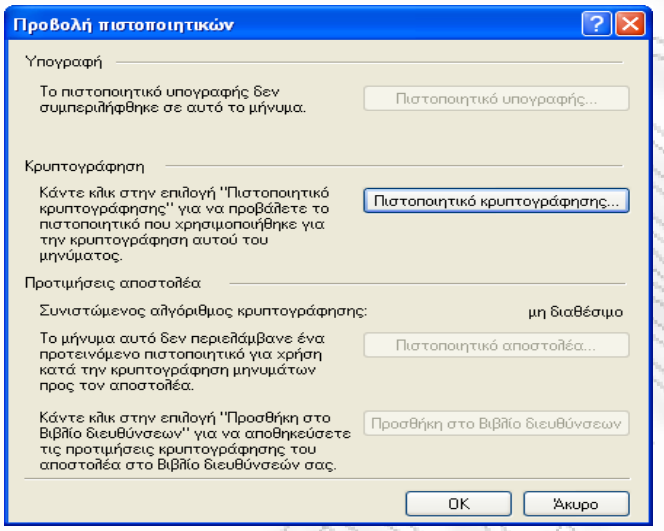
Με την προϋπόθεση ότι ο παραλήπτης έχει τη σωστή ψηφιακή ταυτότητα εγκατεστημένη στον υπολογιστή του, το Outlook Express αποκρυπτογραφεί αυτόματα το κρυπτογραφημένο μήνυμα του ηλεκτρονικού ταχυδρομείου.

Μπορούμε να προβάλουμε και να δούμε το πιστοποιητικό που χρησιμοποιήσαμε για την κρυπτογράφηση, δηλαδή το πιστοποιητικό μαζί με το δημόσιο κλειδί του παραλήπτη κάνοντας ‘’κλικ’’ πάνω στο εικονίδιο της μπλε κλειδαριάς, εικόνα 8.78.

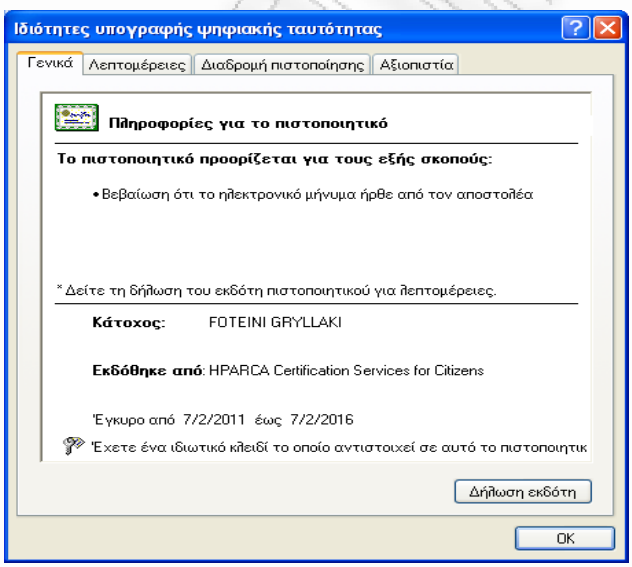
Θα εμφανιστεί το παράθυρο της εικόνας 8.81, όπου πατώντας το κουμπί ‘’προβολή πιστοποιητικών’’ και στη συνέχεια στο παράθυρο που θα εμφανιστεί, εικόνα 8.82, το κουμπί ‘’πιστοποιητικό κρυπτογράφησης’’ προβάλουμε το πιστοποιητικό που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος, εικόνα 8.83.



Εικόνα 8.81: Προβολή πιστοποιητικού



Εικόνα 8.82: Προβολή πιστοποιητικού



Εικόνα 8.83: Προβολή πιστοποιητικού

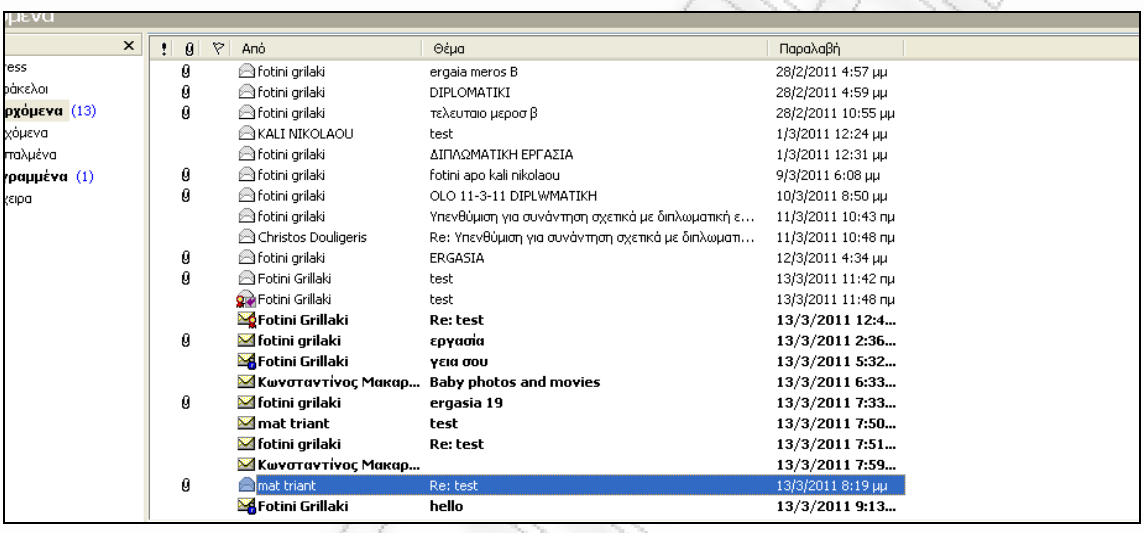
8.2.5 Συνδυασμός ψηφιακής υπογραφής και κρυπτογράφησης σ' ένα μήνυμα ηλεκτρονικού ταχυδρομείου

Φυσικά μπορούμε να κρυπτογραφήσουμε ένα ηλεκτρονικό μήνυμα με το δημόσιο κλειδί του παραλήπτη, να το υπογράψουμε ψηφιακά και να του το στείλουμε με το ηλεκτρονικό ταχυδρομείο. Η διαδικασία είναι ακριβώς όπως περιγράψαμε και για τις δύο περιπτώσεις παραπάνω.

Μ' αυτό τον τρόπο ο παραλήπτης μπορεί να ελέγξει και την αυθεντικότητα του μηνύματος, αλλά και να είναι βέβαιος ότι κανένας άλλος δεν έχει διαβάσει το μήνυμα.

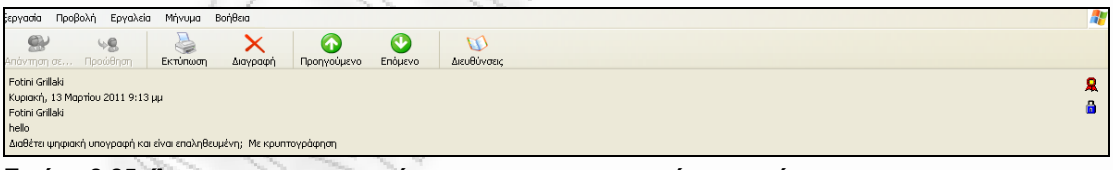
Αν προκύψουν προβλήματα ο παραλήπτης πρέπει να θεωρήσει ότι το μήνυμα έχει αλλοιωθεί ή ότι δεν προέρχεται από τον υποτιθέμενο αποστολέα.

Το υπογεγραμμένο και κρυπτογραφημένο μήνυμα θα φαίνεται στα εισερχόμενα του παραλήπτη όπως στην εικόνα 8.84.

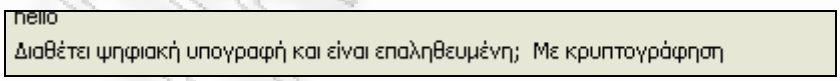


Εικόνα 8.84: Υπογεγραμμένο και κρυπτογραφημένο μήνυμα

Ο παραλήπτης ανοίγοντας το μήνυμα που του έχει στείλει ο αποστολέας για να το διαβάσει, εικόνα 8.85, θα παρατηρήσει μια ειδοποίηση ασφάλειας ότι το μήνυμα διαθέτει ψηφιακή υπογραφή και είναι και κρυπτογραφημένο, εικόνα 8.86. Επίσης στα δεξιά θα υπάρχουν τα σχήματα της ψηφιακής υπογραφής και κρυπτογράφησης, εικόνα 8.87.



Εικόνα 8.85: Άνοιγμα υπογεγραμμένου και κρυπτογραφημένου μηνύματος



Εικόνα 8.86: Μήνυμα ασφαλείας

Εικόνα 8.87:Σχήματα ψηφιακής υπογραφής και κρυπτογράφησης

Όπως και στις προηγούμενες περιπτώσεις, κάνοντας ''κλικ'' πάνω στα σχήματα της ψηφιακής υπογραφής και της κρυπτογράφησης, εικόνα 8.85, μπορούμε να προβάλουμε τα ψηφιακά πιστοποιητικά που χρησιμοποιήθηκαν σε κάθε περίπτωση.

Κεφάλαιο 9

Συμπεράσματα

Οι ψηφιακές υπογραφές αποτελούν σήμερα τη μόνη αξιόπιστη λύση για την ταυτόχρονη πιστοποίηση της προέλευσης και τη διασφάλιση της ακεραιότητας των διακινούμενων εγγράφων μέσω του διαδικτύου. Όμως, παρά τη μεγάλη χρησιμότητα και ασφάλεια που παρέχουν, παρατηρείται ένας φόβος από τη μεριά των δυνητικών χρηστών σχετικά με τη χρήση, την ασφάλεια και τη νομική αναγνώριση αυτών. Ο φόβος αυτός πηγάζει από την έλλειψη ενημέρωσης που έχει ο πολίτης πάνω σε θέματα ψηφιακών υπογραφών και κρυπτογράφησης. Γι' αυτό το λόγο θα πρέπει να καταβληθούν προσπάθειες ώστε να ενισχυθεί η εμπιστοσύνη των πολιτών πάνω σε τέτοιες μεθόδους και να ανατρέψει το κλίμα σύγχυσης που επικρατεί. Μια λύση που μπορεί να δοθεί από το κράτος είναι μια ολοκληρωμένη εκστρατεία ενημέρωσης του πολίτη με ειδικά σεμινάρια από εκπαιδευμένο προσωπικό, που θα φροντίσει τη σωστή πληροφόρηση των πολιτών πάνω στη σωστή χρήση των τεχνολογιών της ηλεκτρονικής υπογραφής.

Μετά την έκδοση και χρήση των ψηφιακών πιστοποιητικών μέσω της εθνικής πύλης δημόσιας διοίκησης ermis του Υπουργείου Εσωτερικών που περιγράψαμε στην παρούσα εργασία, καταλάβαμε ότι η πολιτεία έχει φροντίσει όσο το δυνατόν καλύτερα να παρέχει συστήματα φιλικά, εύχρηστα και ασφαλή προς τον χρήστη.

Ο χρήστης θα πρέπει να ενημερώνεται διεξοδικά για όλους τους όρους χρήσης των κρυπτογραφικών κλειδιών, των πιστοποιητικών και των συναφών υπηρεσιών του Παρόχου Υπηρεσιών Πιστοποίησης κατά την αίτησή του για την έκδοση ψηφιακού πιστοποιητικού. Θα πρέπει όλα τα στοιχεία και οι πληροφορίες που υποβάλει στην αίτησή του για ψηφιακό πιστοποιητικό να είναι αληθείς. Τα εκδοθέντα ψηφιακά πιστοποιητικά πρέπει να χρησιμοποιούνται αποκλειστικά για συγκεκριμένους σκοπούς, σύμφωνα με την εκάστοτε δήλωση πρακτικής. Φυσικά κάθε χρήστης πρέπει να προβαίνει στις απαραίτητες προφυλάξεις των ιδιωτικών του κλειδιών ώστε να αποτρέψει την αποκάλυψη ή ακόμα και την απώλεια αυτών. Σε οποιαδήποτε στιγμή και μόλις υποψιασθεί την έκθεση των ιδιωτικών του κλειδιών σε μη εξουσιοδοτημένα άτομα θα πρέπει να ζητά αμέσως την ακύρωση του σχετικού ψηφιακού πιστοποιητικού του.

Μέχρι σήμερα η χρήση της ψηφιακής υπογραφής δεν είναι υποχρεωτική, αλλά εξαρτάται από τον εκάστοτε φορέα για το αν θα τη χρησιμοποιήσει ή όχι. Όμως αν θέλουμε κάποια στιγμή να μιλάμε για εκσυγχρονισμό στη Δημόσια Διοίκηση θα πρέπει η χρήση της να γίνει υποχρεωτική.

Κεφάλαιο 10

Παραρτήματα

Παράρτημα 1: Σύστημα Kerberos

Το σύστημα Kerberos αναπτύχθηκε από το Massachusetts Institute of Technology (MIT) και είναι ένα σύστημα πιστοποίησης ταυτότητας το οποίο αναπτύχθηκε με την ελπίδα αντικατάστασης του συστήματος που καλείται πιστοποίηση βάσει ισχυρισμού (authentication by assertion).

Η πιστοποίηση βάσει ισχυρισμού στηρίζεται στην εξής αρχή: όταν ο χρήστης τρέχει ένα πρόγραμμα που απαιτεί πρόσβαση σε μία δικτυακή υπηρεσία, το πρόγραμμα ανακοινώνει στον server ότι λειτουργεί εκ μέρους του συγκεκριμένου χρήστη. Ο server πιστεύει τα στοιχεία που του παρέχει ο client (δηλαδή το πρόγραμμα) και εξυπηρετεί τον χρήστη χωρίς να ζητά άλλες αποδείξεις. Όπως καταλαβαίνουμε, η παρεχόμενη ασφάλεια είναι πολύ χαμηλού επιπέδου έως και ανύπαρκτη.

Το Kerberos επιτρέπει στις δικτυακές εφαρμογές να αναγνωρίζουν με ασφάλεια την ταυτότητα του χρήστη που ζητά εξυπηρέτηση, χωρίς να στέλνει στο δίκτυο δεδομένα που μπορούν να επιτρέψουν σε ένα πιθανό εισβολέα να προσποιηθεί ότι είναι ο χρήστης και χωρίς να βασίζεται στις διευθύνσεις των μηχανών του δικτύου. Επίσης, η πιστοποίηση ταυτότητας γίνεται από τον application server και η επικοινωνία γίνεται εν γνώση της πιθανότητας ότι η διακινούμενη πληροφορία μπορεί να τροποποιηθεί και να αναγνωστεί κατά βούληση. Το Kerberos προαιρετικά προσφέρει ακεραιότητα και απόρρητη συναλλαγή για τα δεδομένα που στέλνονται μεταξύ του client και του application server. Σαν application server εννοούμε τον server που προσφέρει υπηρεσίες όπως mail, http κτλ.

Το σύστημα χρησιμοποιεί μια σειρά από κρυπτογραφημένα μηνύματα για να αποδείξει σε έναν application server ότι ο client λειτουργεί εκ μέρους ενός συγκεκριμένου χρήστη. Για την ανταλλαγή των μηνυμάτων ο Kerberos εκμεταλλεύεται το IP επίπεδο σε συνδυασμό με το UDP πρωτόκολλο. Ο client αποδεικνύει την ταυτότητα του χρήστη παρουσιάζοντας στον application server την απόδειξη - ticket, η οποία περιέχει ένα προσωρινό κλειδί κρυπτογράφησης που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ του application server και του χρήστη, και το πιστοποιητικό- authenticator, το οποίο αποδεικνύει ότι ο client έχει στην κατοχή του το session key που έχει εκδοθεί για τον χρήστη που ορίζεται στο ticket. Οι αποδείξεις εκδίδονται από ένα αφιερωμένο υπολογιστή που καλείται authentication server (AS). Ο authentication server έχει αποθηκευμένα μυστικά κλειδιά, που καλούνται server keys και τα μοιράζεται με τους application servers. Τα server keys εγκαθίστανται μέσα από κρυπτογραφημένο κανάλι. Το server key πιστοποιεί την αυθεντικότητα των αποδείξεων tickets που λαμβάνει ο client και ο server. Επιπλέον, ο AS έχει αποθηκευμένα κλειδιά που αναφέρονται σε κάθε χρήστη και καλούνται user keys. Όλα τα κλειδιά εμπεριέχονται σε βάση δεδομένων. Κάθε ticket έχει περιορισμένη διάρκεια ζωής και όταν αυτό το χρονικό διάστημα περάσει τότε είναι άχρηστο. Για περαιτέρω ανταλλαγή μηνυμάτων απαιτείται έκδοση νέου ticket. [37]

Παράρτημα 2: Αρχή Πιστοποίησης VeriSign

Η Verisign είναι μια αμερικανική εταιρία που αποτελεί σήμερα την πιο δημοφιλή εταιρία παροχής υπηρεσιών εμπιστοσύνης- trust services στο Internet. Με τον όρο trust services καθορίζεται μια ευρεία ποικιλία υπηρεσιών επιβεβαίωσης και πιστοποίησης ταυτότητας, ηλεκτρονικών πληρωμών, ψηφιακών πιστοποιητικών κλπ, οι οποίες είναι απαραίτητες για τη διενέργεια ασφαλών συναλλαγών μέσω του Internet.

Η Verisign θεωρείται μέχρι σήμερα η εγκυρότερη Αρχή Πιστοποίησης στο Internet. Οι πελάτες της προέρχονται από όλο τον κόσμο. Μπορεί να είναι εταιρίες που δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου, αλλά και απλοί χρήστες που επιθυμούν να έχουν ασφάλεια στην παρουσία και στις συναλλαγές τους στο διαδίκτυο. Μέχρι σήμερα, η εταιρία έχει εκδώσει πιστοποιητικά για περισσότερα από 300.000 web sites σ' όλο τον κόσμο, ενώ παρέχει

αντίστοιχες υπηρεσίες σε έναν αριθμό ιδιωτικών χρηστών, ο οποίος ξεπερνά τα τέσσερα εκατομμύρια άτομα.

Οι υπηρεσίες που προσφέρει μπορούν να ομαδοποιηθούν στις ακόλουθες 4 ενότητες.

- Υπηρεσίες για εταιρίες: Απευθύνονται σε εταιρίες που θέλουν να πραγματοποιούν με απόλυτη ασφάλεια τις συναλλαγές τους μέσω των ιδιωτικών δικτύων τους.

-Υπηρεσίες ψηφιακής υπογραφής: Παρέχεται η δυνατότητα στο χρήστη για απόλυτη προστασία της ψηφιακής υπογραφής του και των e-mails που στέλνει μέσω Internet.

- Υπηρεσίες ψηφιακής ταυτοποίησης servers: Πρόκειται για μια υπηρεσία που παρέχει την εγγύηση στους πελάτες και στους συνεργάτες μιας εταιρίας ότι οι πληροφορίες και οι συναλλαγές που διακινούνται από ταυτοποιημένους servers είναι αυθεντικές και απολύτως εξασφαλισμένες.

- Υπηρεσίες αυθεντικότητας προγραμμάτων: Σε συνεργασία με τη Microsoft, τη SAP, αλλά και μεγάλες εταιρίες υποστήριξης δικτύων, όπως είναι για παράδειγμα η Cisco, είναι δυνατόν να κωδικοποιηθούν τα προγράμματα που μια εταιρία επιτρέπει να αποκτηθούν μέσω του Internet, ώστε να εξασφαλίζεται η γνησιότητα και η ασφαλής προέλευση τους από την πραγματική πηγή.

Τα ψηφιακά πιστοποιητικά που προσφέρει η Verisign μπορούν να χρησιμοποιηθούν σε πλήθος διαφορετικών εφαρμογών. Έτσι, μπορούν να χρησιμοποιηθούν όχι μόνο για ηλεκτρονικές αγορές, αλλά και για τον καθορισμό της πρόσβασης των χρηστών σε εταιρικά δίκτυα (Intranets). Ένας οργανισμός μπορεί να ορίσει τέτοια πιστοποιητικά στους χρήστες του δικτύου του, λειτουργώντας ουσιαστικά ο ίδιος ως μια αρχή πιστοποίησης, καθορίζοντας την πρόσβαση που μπορεί να έχει ο καθένας από αυτούς στις πληροφορίες του οργανισμού μέσω πιστοποιητικών.

Από τα σημαντικότερα προβλήματα ασφάλειας που αντιμετωπίζουν οι διάφοροι οργανισμοί και επιχειρήσεις είναι η προστασία των «ευαίσθητων» δεδομένων που διατηρούν (οικονομικά στοιχεία, ιατρικά δεδομένα κλπ.) και ο έλεγχος της πρόσβασης σε αυτά. Με τη χρήση των ψηφιακών πιστοποιητικών μπορεί να καθοριστεί ποιοι θα έχουν πρόσβαση με περισσότερο αξιόπιστο και αποτελεσματικό τρόπο σε σχέση με τις συνθηματικές λέξεις (passwords). Το ψηφιακό πιστοποιητικό μπορεί να λειτουργήσει όπως μια κάρτα πιστοποίησης της ταυτότητας για την είσοδο σε κτίρια με υψηλές προδιαγραφές ασφάλειας. Όπως μια τέτοια κάρτα καθορίζει σε ποιους χώρους έχει πρόσβαση ο χρήστης που την κατέχει, με αντίστοιχο τρόπο ο κάτοχος του πιστοποιητικού μπορεί να έχει πρόσβαση σε συγκεκριμένες πληροφορίες, ενώ απαγορεύονται ρητά εκείνοι για τους οποίους δεν έχει εκδοθεί ψηφιακό πιστοποιητικό.

Εκτός όμως από τα πιστοποιητικά των εταιριών, υπάρχουν και τα προσωπικά πιστοποιητικά. Χρησιμοποιούνται για να αποδεικνύει ο χρήστης σε κάθε Web server την ταυτότητα του. Για να αποκτηθούν τα προσωπικά πιστοποιητικά, σε αντιστοιχία με τα «εμπορικά» πιστοποιητικά, χρειάζεται ο χρήστης να απευθυνθεί σε μια αρχή πιστοποίησης. Η Verisign αποτέλεσε την πρώτη αρχή πιστοποίησης που εξέδωσε τέτοιου είδους πιστοποιητικά.

Η χρήση των προσωπικών πιστοποιητικών είναι πολύ αποδοτική. Συγκεκριμένα, οι browsers χρησιμοποιούν το πιστοποιητικό για να αποκρυπτογραφήσουν πληροφορία που στέλνεται προς το χρήστη. Με την απόκτηση του πιστοποιητικού, δημιουργείται ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό). Όποιος θέλει να του στείλει εμπιστευτικές πληροφορίες, τις κρυπτογραφεί με το δημόσιο κλειδί του, οπότε μόνο ο συγκεκριμένος χρήστης (με το ιδιωτικό κλειδί του) μπορεί να τις αποκρυπτογραφήσει.

Τα ψηφιακά πιστοποιητικά και οι ψηφιακές υπογραφές της Verisign είναι σε θέση να προσδώσουν στα e-mails, στα web sites και στις συναλλαγές ηλεκτρονικού εμπορίου υψηλά επίπεδα ασφαλείας. Δεν είναι λοιπόν τυχαίο που η Verisign αποτελεί την πιο δημοφιλή εταιρία σε όλο τον κόσμο, συμπεριλαμβανομένης και της Ελλάδας. [46]

Παράρτημα 3: ΟΔΗΓΙΑ 1999/93/ΕΚ

ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 47 παράγραφος 2 και τα άρθρα 55 και 95,

την πρόταση της Επιτροπής(1),

τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής(2),

της γνώμη της Επιτροπής των Περιφερειών(3),

Αποφασίζοντας σύμφωνα με τη διαδικασία του άρθρου 251 της συνθήκης(4),

Εκτιμώντας τα ακόλουθα:

(1) στις 16 Απριλίου 1997, η Επιτροπή υπέβαλε στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών ανακοίνωση σχετικά με ευρωπαϊκή πρωτοβουλία στο ηλεκτρονικό εμπόριο·

(2) στις 8 Οκτωβρίου 1997 η Επιτροπή υπέβαλε στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών ανακοίνωση για την κατοχύρωση της ασφάλειας και εμπιστοσύνης στις ηλεκτρονικές επικοινωνίες - προς ένα ευρωπαϊκό πλαίσιο για ψηφιακές υπογραφές και κρυπτοθέτηση·

(3) την 1η Δεκεμβρίου 1997, το Συμβούλιο κάλεσε την Επιτροπή να υποβάλει το ταχύτερο δυνατό πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις ψηφιακές υπογραφές·

(4) για τις ηλεκτρονικές επικοινωνίες και το εμπόριο απαιτούνται "ηλεκτρονικές υπογραφές" και συναφείς υπηρεσίες που παρέχουν τη δυνατότητα απόδειξης της γνησιότητας των δεδομένων· η ύπαρξη αποκλινόντων κανόνων όσον αφορά τη νομική αναγνώριση των ψηφιακών υπογραφών και διαπίστευση "παροχών υπηρεσιών πιστοποίησης" στα κράτη μέλη ενδέχεται να αποτελέσει σημαντικό φραγμό για τη χρήση των ηλεκτρονικών επικοινωνιών και του ηλεκτρονικού εμπορίου· από την άλλη πλευρά, ένα σαφές κοινοτικό πλαίσιο σχετικά με τις προϋποθέσεις που θα εφαρμόζονται στις ηλεκτρονικές υπογραφές θα ενισχύσει την εμπιστοσύνη στις νέες τεχνολογίες και θα συμβάλει στη γενική αποδοχή τους· οι νομοθεσίες στα κράτη μέλη δεν θα πρέπει να εμποδίζουν την ελεύθερη κυκλοφορία αγαθών και υπηρεσιών στην εσωτερική αγορά·

(5) θα πρέπει να προαχθεί η διαλειτουργικότητα των προϊόντων ηλεκτρονικής υπογραφής· σύμφωνα με το άρθρο 14 της συνθήκης, η εσωτερική αγορά περιλαμβάνει ένα χώρο χωρίς εσωτερικά σύνορα μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των εμπορευμάτων· πρέπει να ικανοποιηθούν βασικές απαιτήσεις που αναφέρονται σε προϊόντα ηλεκτρονικής υπογραφής για τη διασφάλιση της ελεύθερης κυκλοφορίας εντός της εσωτερικής αγοράς και για την οικοδόμηση εμπιστοσύνης στις ηλεκτρονικές υπογραφές, με την επιφύλαξη του κανονισμού (ΕΚ) αριθ. 3381/94 του Συμβουλίου, της 19ης Δεκεμβρίου 1994, περί κοινοτικού καθεστώτος ελέγχου της εξαγωγής αγαθών διπλής χρήσης(5) και της απόφασης 94/942/ΚΕΠΠΑ του Συμβουλίου, της 19ης Δεκεμβρίου 1994, σχετικά με την κοινή δράση που ενεκρίθη από το Συμβούλιο σχετικά με τον έλεγχο της εξαγωγής αγαθών διπλής χρήσης(6)·

(6) η παρούσα οδηγία δεν εναρμονίζει την παροχή υπηρεσιών όσον αφορά το απόρρητο των πληροφοριών όταν καλύπτονται από εθνικές διατάξεις περί δημόσιας τάξης ή δημόσιας ασφάλειας·

(7) η εσωτερική αγορά εξασφαλίζει την ελεύθερη κυκλοφορία των προσώπων, η οποία έχει ως συνέπεια ότι οι πολίτες και οι κάτοικοι της Ευρωπαϊκής Ένωσης, έρχονται όλο και συχνότερα αντιμέτωποι με αρχές κρατών μελών διαφορετικών εκείνου στο οποίο διαμένουν· η ηλεκτρονική επικοινωνία θα μπορούσε να αποδειχθεί εξαιρετικά χρήσιμη από αυτή την άποψη·

(8) η ταχεία τεχνολογική ανάπτυξη και ο παγκόσμιος χαρακτήρας του Internet επιβάλλουν προσέγγιση που θα είναι ανοικτή σε διάφορες τεχνολογίες και υπηρεσίες ηλεκτρονικής αναγνώρισης της γνησιότητας δεδομένων·

(9) οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται σε πολλές διαφορετικές συνθήκες και εφαρμογές, έχοντας ως αποτέλεσμα ευρύ φάσμα νέων υπηρεσιών και προϊόντων που θα συνδέονται με ή θα χρησιμοποιούν ηλεκτρονικές υπογραφές· ο ορισμός αυτών των προϊόντων και υπηρεσιών δεν θα πρέπει να περιοριστεί στην έκδοση και διαχείριση πιστοποιητικών αλλά θα πρέπει να συμπεριλαμβάνει όλες τις υπηρεσίες και τα προϊόντα που χρησιμοποιούν ή σχετίζονται με ηλεκτρονικές υπογραφές, όπως οι υπηρεσίες καταχώρησης, οι υπηρεσίες χρονοσήμανσης, οι υπηρεσίες καταλόγου, οι υπηρεσίες πληροφορικής ή οι υπηρεσίες μελετών σχετικά με τις ηλεκτρονικές υπογραφές·

(10) η εσωτερική αγορά επιτρέπει στους παρόχους υπηρεσιών πιστοποίησης την ανάπτυξη των διασυνοριακών δραστηριοτήτων τους αποβλέποντας στην αύξηση της ανταγωνιστικότητάς τους, προσφέροντας έτσι στους καταναλωτές και τις επιχειρήσεις νέες ευκαιρίες ασφαλούς ανταλλαγής πληροφοριών και ηλεκτρονικών συναλλαγών, ανεξαρτήτως συνόρων· για την τόνωση της παροχής υπηρεσιών πιστοποίησης μέσω ανοικτών δικτύων σε κοινοτική κλίμακα, θα πρέπει οι πάροχοι υπηρεσιών πιστοποίησης να είναι ελεύθεροι να παρέχουν τις υπηρεσίες τους χωρίς προηγούμενη έγκριση· ως προηγούμενη έγκριση νοείται, όχι μόνο κάθε άδεια για την οποία απαιτείται απόφαση των εθνικών αρχών προτού επιτραπεί στον ενδιαφερόμενο να παρέχει υπηρεσίες πιστοποίησης, αλλά και κάθε άλλο μέτρο ισοδυνάμου αποτελέσματος·

(11) οι μηχανισμοί εθελοντικής διαπίστευσης που αποσκοπούν σε βελτιωμένο επίπεδο παροχής υπηρεσιών ενδέχεται να προσφέρουν στους παρόχους υπηρεσιών πιστοποίησης το κατάλληλο πλαίσιο για την περαιτέρω ανάπτυξη των υπηρεσιών τους στα επίπεδα εμπιστοσύνης, ασφάλειας και ποιότητας που απαιτούνται από την εξελισσόμενη αγορά· αυτοί οι μηχανισμοί θα πρέπει να ενθαρρύνουν την ανάπτυξη βέλτιστης πρακτικής μεταξύ των παρόχων υπηρεσιών πιστοποίησης· οι πάροχοι υπηρεσιών πιστοποίησης θα πρέπει να είναι ελεύθεροι να επιλέγουν και να επωφελούνται από τους εν λόγω μηχανισμούς διαπίστευσης·

(12) οι υπηρεσίες πιστοποίησης μπορούν να παρέχονται είτε από δημόσιο φορέα είτε από νομικό ή φυσικό πρόσωπο, εφόσον είναι εγκατεστημένο σύμφωνα με το εθνικό δίκαιο· τα κράτη μέλη δεν θα πρέπει να απαγορεύουν στους παρόχους υπηρεσιών πιστοποίησης να λειτουργούν εκτός των εν λόγω μηχανισμών εθελοντικής διαπίστευσης· θα πρέπει να διασφαλίζεται ότι οι μηχανισμοί εθελοντικής διαπίστευσης δεν περιορίζουν τον ανταγωνισμό στις υπηρεσίες πιστοποίησης·

(13) τα κράτη μέλη μπορούν να αποφασίζουν με ποιό τρόπο θα εξασφαλίσουν τον έλεγχο της τήρησης των διατάξεων της παρούσας οδηγίας· η παρούσα οδηγία δεν αποκλείει τη θέσπιση συστημάτων ελέγχου βασισμένων στον ιδιωτικό τομέα· η παρούσα οδηγία δεν υποχρεώνει τους παρόχους υπηρεσιών πιστοποίησης να υπόκεινται σε έλεγχο δυνάμει τυχόν μηχανισμών περί διαπίστευσης·

(14) είναι σημαντικό να ευρεθεί μία ισορροπία μεταξύ των αναγκών των καταναλωτών και των επιχειρήσεων·

(15) το παράρτημα III καλύπτει απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής ούτως ώστε να εξασφαλιστεί η λειτουργικότητα των προηγμένων ηλεκτρονικών υπογραφών· δεν καλύπτει ολόκληρο το περιβάλλον του συστήματος στο οποίο λειτουργούν οι διατάξεις αυτές· η λειτουργία της εσωτερικής αγοράς υποχρεώνει την Επιτροπή και τα κράτη μέλη να αναλάβουν ταχέως μέτρα για το διορισμό των φορέων που θα αναλάβουν την αξιολόγηση της πιστότητας των ασφαλών διατάξεων υπογραφής με το παράρτημα III· για να ικανοποιούνται οι ανάγκες της αγοράς η αξιολόγηση της πιστότητας πρέπει να διενεργείται έγκαιρα και αποτελεσματικά·

(16) η παρούσα οδηγία συμβάλλει στη χρήση και νομική αναγνώριση των ηλεκτρονικών υπογραφών εντός της Κοινότητας· δεν απαιτείται κανονιστικό πλαίσιο για ηλεκτρονικές υπογραφές που χρησιμοποιούνται αποκλειστικά μέσα σε συστήματα που στηρίζονται σε εθελούσιες συμφωνίες ιδιωτικού δικαίου μεταξύ συγκεκριμένου αριθμού συμμετεχόντων· θα πρέπει να γίνει σεβαστή η ελευθερία των μερών να συμφωνούν μεταξύ τους όρους και τις προϋποθέσεις βάσει των οποίων αποδέχονται ηλεκτρονικά υπογεγραμμένα δεδομένα, στο βαθμό που τούτο επιτρέπεται από την εθνική νομοθεσία, θα πρέπει να αναγνωρίζεται η νομική ισχύς των ηλεκτρονικών υπογραφών που χρησιμοποιούνται σε αυτά τα διαστήματα καθώς και η αποδοχή τους ως αποδεικτικών στοιχείων σε νομικές διαδικασίες·

(17) η παρούσα οδηγία δεν αποσκοπεί σε εναρμόνιση εθνικών κανόνων που αφορούν το ενοχικό δίκαιο, ιδίως την κατάρτιση και εκτέλεση των συμβάσεων ή άλλες διατυπώσεις μη συμβατικού χαρακτήρα σχετικά με τις υπογραφές· επομένως, οι διατάξεις που αφορούν τις έννομες συνέπειες των ηλεκτρονικών υπογραφών θα πρέπει να ισχύουν με την επιφύλαξη των απαιτήσεων ως προς τον τύπο δυνάμει της εθνικής νομοθεσίας σχετικά με τη σύναψη συμβάσεων ή τους κανόνες που καθορίζουν τον τόπο σύναψης μιας σύμβασης·

(18) η αποθήκευση και η αντιγραφή δεδομένων δημιουργίας υπογραφής θα μπορούσε να αποτελέσει απειλή για την νομική ισχύ των ηλεκτρονικών υπογραφών·

(19) οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται στο δημόσιο τομέα στο πλαίσιο εθνικών και κοινοτικών διοικητικών υπηρεσιών και για την επικοινωνία μεταξύ αυτών των υπηρεσιών και

των πολιτών και οικονομικών φορέων, π.χ. για τις δημόσιες συμβάσεις, τη φορολογία, την κοινωνική ασφάλιση, την υγεία και την απονομή δικαιοσύνης·

(20) η ύπαρξη εναρμονισμένων κριτηρίων όσον αφορά τις έννομες συνέπειες των ηλεκτρονικών υπογραφών θα διαφυλάξει εάν συνεκτικό νομικό πλαίσιο σε ολόκληρη την έκταση της Κοινότητας· στις εθνικές νομοθεσίες προβλέπονται διαφορετικές απαιτήσεις για τη νομική ισχύ των ιδιόχειρων υπογραφών· τα πιστοποιητικά μπορούν να χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας προσώπου που υπογράφει ηλεκτρονικά· οι προηγούμενες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό στοχεύουν υψηλότερο επίπεδο ασφάλειας· οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής μπορούν να θεωρηθούν ως νομικά ισοδύναμες προς ιδιόχειρες υπογραφές μόνον εφόσον πληρούνται οι εν λόγω προϋποθέσεις για ιδιόχειρες υπογραφές·

(21) ως συμβολή στη γενική αποδοχή των ηλεκτρονικών μεθόδων απόδειξης γνησιότητας πρέπει να διασφαλιστεί η δυνατότητα χρησιμοποίησης των ηλεκτρονικών υπογραφών ως αποδεικτικού στοιχείου σε νομικές διαδικασίες σε όλα τα κράτη μέλη· η νομική αναγνώριση των ηλεκτρονικών υπογραφών θα πρέπει να βασίζεται σε αντικειμενικά κριτήρια και να μη συνδέεται με την εξουσιοδότηση του εμπλεκόμενου παρόχου υπηρεσιών πιστοποίησης· ο καθορισμός των τομέων δικαίου στους οποίους επιτρέπεται η χρήση ηλεκτρονικών εγγράφων και ηλεκτρονικών υπογραφών διέπεται από το εθνικό δίκαιο· η παρούσα οδηγία δεν θίγει την αρμοδιότητα εθνικού δικαστηρίου να αποφασίζει ως προς τη συμμόρφωση με τις απαιτήσεις της οδηγίας και δεν επηρεάζει εθνικούς κανόνες που διέπουν την ελεύθερη εκτίμηση αποδείξεων υπό του δικαστηρίου·

(22) οι πάροχοι υπηρεσιών πιστοποίησης που παρέχουν υπηρεσίες πιστοποίησης στο κοινό υπάγονται στους εθνικούς κανόνες περί ευθύνης·

(23) για την ανάπτυξη του διεθνούς ηλεκτρονικού εμπορίου απαιτούνται διασυνοριακές ρυθμίσεις με συμμετοχή τρίτων χωρών· προκειμένου να διασφαλισθεί η διαλειτουργικότητα σε παγκόσμιο επίπεδο, θα μπορούσαν να αποβούν χρήσιμες συμφωνίες με τρίτες χώρες για πολυμερείς ρυθμίσεις όσον αφορά την αμοιβαία αναγνώριση υπηρεσιών πιστοποίησης·

(24) για την τόνωση της εμπιστοσύνης των χρηστών στην ηλεκτρονική επικοινωνία και στο ηλεκτρονικό εμπόριο μέσω της διασφάλισης της εμπιστοσύνης των χρηστών, οι πάροχοι υπηρεσιών πιστοποίησης πρέπει να τηρούν τη νομοθεσία περί προστασίας των δεδομένων και της ιδιωτικής ζωής·

(25) διατάξεις περί της χρήσης ψευδωνύμων στα πιστοποιητικά δεν θα πρέπει να εμποδίζουν τα κράτη μέλη να ζητούν εξακρίβωση της ταυτότητας των προσώπων σύμφωνα με το κοινοτικό ή το εθνικό δίκαιο·

(26) τα αναγκαία μέτρα για την εφαρμογή της παρούσας οδηγίας πρέπει να θεσπισθούν σύμφωνα με την απόφαση 1999/468/ΕΚ του Συμβουλίου, της 28ης Ιουνίου 1999, για τον καθορισμό των όρων άσκησης των εκτελεστικών αρμοδιοτήτων που ανατίθενται στην Επιτροπή(7)·

(27) η Επιτροπή θα επανεξετάσει την παρούσα οδηγία δύο έτη μετά την εφαρμογή της, μεταξύ άλλων για να εξασφαλίσει ότι η πρόοδος της τεχνολογίας ή οι αλλαγές των νομικών συνθηκών δεν έχουν δημιουργήσει εμπόδια για την επίτευξη των στόχων που θέτει η παρούσα οδηγία· θα πρέπει να εξετάσει τις συνέπειες των συνδεδεμένων τεχνικών τομέων και να υποβάλει σχετική έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο·

(28) σύμφωνα με τι αρχές της επικουρικότητας και της αναλογικότητας που αναφέρονται στο άρθρο 5 της συνθήκης, ο στόχος της δημιουργίας εναρμονισμένου νομοθετικού πλαισίου για την παροχή ηλεκτρονικών υπογραφών και συναφών υπηρεσιών δεν μπορεί να επιτευχθεί αποτελεσματικά από τα κράτη μέλη και, ως εκ τούτου, είναι δυνατόν, να επιτευχθεί καλύτερα από την Κοινότητα· η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου,

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1

Πεδίο εφαρμογής

Στόχος της παρούσας οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές

και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς.

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.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας νοούνται ως:

1. "ηλεκτρονική υπογραφή": 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,

2. "προηγμένη ηλεκτρονική υπογραφή": ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις:

α) συνδέεται μονοσήμαντα με τον υπογράφοντα·

β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα·

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

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

3. "υπογράφων": φυσικό ή νομικό πρόσωπο που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε για λογαριασμό του είτε εξ ονόματος φυσικού ή νομικού προσώπου ή φορέα που αντιπροσωπεύει,

4. "δεδομένα δημιουργίας υπογραφής": μονοσήμαντα δεδομένα όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής,

5. "διάταξη δημιουργίας υπογραφής": διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής,

6. "ασφαλής διάταξη δημιουργίας υπογραφής": διάταξη δημιουργίας υπογραφής που πληροί τις απαιτήσεις του παραρτήματος ΙΙΙ,

7. "δεδομένα δημιουργίας υπογραφής": δεδομένα, όπως κώδικες ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής,

8. "δεδομένα επαλήθευσης υπογραφής": διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής,

9. "πιστοποιητικό": ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο που επιβεβαιώνει την ταυτότητά του,

10. "αναγνωρισμένο πιστοποιητικό": πιστοποιητικό που ανταποκρίνεται στις οριζόμενες στο παράρτημα Ι απαιτήσεις και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τις οριζόμενες στο παράρτημα ΙΙ απαιτήσεις,

11. "πάροχος υπηρεσιών πιστοποίησης": φορέας ή φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές,

12. "προϊόν ηλεκτρονικής υπογραφής": υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται για χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την παροχή υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών,

13. "εθελοντική διαπίστευση": κάθε άδεια, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις που διέπουν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται κατόπιν αιτήσεως του ενδιαφερόμενου παρόχου υπηρεσιών πιστοποίησης από το δημόσιο ή ιδιωτικό φορέα ο οποίος είναι υπεύθυνος για τον καθορισμό αυτών των δικαιωμάτων και υποχρεώσεων και για τον έλεγχο της τήρησής τους, όταν ο πάροχος των υπηρεσιών πιστοποίησης δεν δικαιούται να ασκεί τα δικαιώματα που απορρέουν από την άδεια προτού λάβει την απόφαση του εν λόγω φορέα.

Άρθρο 3

Πρόσβαση στην αγορά

1. Τα κράτη μέλη δεν εξαρτούν την παροχή υπηρεσιών πιστοποίησης από εκ των προτέρων έγκριση.

2. Με την επιφύλαξη των διατάξεων της παραγράφου 1, τα κράτη μέλη δύνανται να διατηρούν μηχανισμούς εθελοντικής διαπίστευσης που αποσκοπούν στην επίτευξη βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης. Όλες οι προϋποθέσεις που συνδέονται με τους εν λόγω μηχανισμούς πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες και να μην οδηγούν σε διακρίσεις. Τα κράτη μέλη δεν μπορούν να περιορίζουν τον αριθμό των διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης για λόγους που εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας.

3. Κάθε κράτος μέλος εξασφαλίζει την καθιέρωση κατάλληλου συστήματος που καθιστά δυνατή την επιτήρηση των εγκατεστημένων στο έδαφός τους παρόχων υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητικά.

4. Η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς τις απαιτήσεις του παραρτήματος III διαπιστώνεται από τους αρμόδιους δημόσιους ή ιδιωτικούς φορείς που ορίζουν τα κράτη μέλη. Η Επιτροπή καθορίζει, σύμφωνα με τη διαδικασία του άρθρου 9, κριτήρια βάσει των οποίων τα κράτη μέλη ορίζουν τους φορείς.

Η υπό των εν λόγω φορέων διαπίστωση της συμμόρφωσης προς τις απαιτήσεις του παραρτήματος III αναγνωρίζεται από όλα τα κράτη μέλη.

5. Η Επιτροπή δύναται, σύμφωνα με τη διαδικασία του άρθρου 9, να καθορίζει και να δημοσιεύει αριθμούς αναφοράς γενικώς αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Τα κράτη μέλη τεκμαίρουν συμμόρφωση με τις απαιτήσεις που καθορίζονται στο στοιχείο στ) του παραρτήματος II και στο παράρτημα III, όταν ένα προϊόν ηλεκτρονικής υπογραφής ανταποκρίνεται στα εν λόγω πρότυπα.

6. Τα κράτη μέλη και η Επιτροπή συνεργάζονται για να προωθήσουν την ανάπτυξη και χρησιμοποίηση των διατάξεων επαλήθευσης υπογραφής, με βάση τις συστάσεις για την ασφαλή επαλήθευση της υπογραφής που προβλέπονται στο παράρτημα IV και προς όφελος του καταναλωτή.

7. Τα κράτη μέλη δύνανται να εξαρτούν τη χρήση ηλεκτρονικών υπογραφών στο δημόσιο τομέα από ενδεχόμενες πρόσθετες απαιτήσεις. Οι εν λόγω απαιτήσεις είναι αντικειμενικές, διαφανείς, ανάλογες και δεν οδηγούν σε διακρίσεις, αναφέρονται δε μόνο στα ειδικά χαρακτηριστικά της συγκεκριμένης εφαρμογής. Οι απαιτήσεις αυτές δεν πρέπει να αποτελούν εμπόδιο στις διασυνοριακές υπηρεσίες για τους πολίτες.

Άρθρο 4

Αρχές της εσωτερικής αγοράς

1. Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει κατ' εφαρμογήν της παρούσας οδηγίας για παρόχους υπηρεσιών πιστοποίησης εγκατεστημένους στην επικράτειά του, καθώς και για τις υπηρεσίες που αυτοί παρέχουν. Τα κράτη μέλη δεν μπορούν να περιορίσουν την παροχή υπηρεσιών πιστοποίησης που προέρχονται από άλλο κράτος μέλος στους τομείς που καλύπτονται από την παρούσα οδηγία.

2. Τα κράτη μέλη διασφαλίζουν ότι τα προϊόντα ηλεκτρονικής υπογραφής που συμμορφώνονται με την παρούσα οδηγία επιτρέπεται να κυκλοφορούν ελεύθερα στην εσωτερική αγορά.

Άρθρο 5

Έννομες συνέπειες των ηλεκτρονικών υπογραφών

1. Τα κράτη μέλη διασφαλίζουν ότι οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής:

α) ικανοποιούν τις νομικές απαιτήσεις υπογραφής σε σχέση με τα δεδομένα σε ηλεκτρονική μορφή κατά τον ίδιο τρόπο που μια ιδιόχειρη υπογραφή ικανοποιεί τις απαιτήσεις αυτές σε σχέση με τα δεδομένα που καταχωρούνται επί χάρτου, και

β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

2. Τα κράτη μέλη διασφαλίζουν ότι δεν απορρίπτεται η νομική ισχύς και το παραδεκτό μιας ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι:

- είναι υπό μορφή ηλεκτρονικών δεδομένων, ή

- δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό, ή

- δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εξεδόθη από διαπιστευμένο παροχέα υπηρεσιών πιστοποίησης, ή

- δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Άρθρο 6

Ευθύνη

1. Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι με την έκδοση πιστοποιητικού ως αναγνωρισμένου πιστοποιητικού στο κοινό ή με την εγγύηση τέτοιου πιστοποιητικού στο κοινό, πάροχος υπηρεσιών πιστοποίησης υπέχει ευθύνη για την προκληθείσα ζημία έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου που ευλόγως βασίζεται στο πιστοποιητικό:

α) όσον αφορά την ακρίβεια, κατά τη στιγμή έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη στο πιστοποιητικό όλων των στοιχείων τα οποία απαιτούνται για ένα αναγνωρισμένο πιστοποιητικό·

β) για τη διαβεβαίωση ότι, κατά το χρόνο έκδοσης του πιστοποιητικού, ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν κάτοχος των δεδομένων δημιουργίας υπογραφής που αντιστοιχούν στα δεδομένα επαλήθευσης υπογραφής που αναφέρονται ή ταυτοποιούνται στο πιστοποιητικό·

γ) για τη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και τα δεδομένα επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, στις περιπτώσεις που αμφότερα προέρχονται από τον πάροχο υπηρεσιών πιστοποίησης,

εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.

2. Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι ο πάροχοςς υπηρεσιών πιστοποίησης που εξέδωσε πιστοποιητικό ως ανεγνωρισμένο πιστοποιητικό στο κοινό υπέχει ευθύνη για τη ζημία που προξενείτε σε οιοδήποτε φορέα ή φυσικό πρόσωπο, που ευλόγως βασίζεται στο πιστοποιητικό, λόγω παράλειψής του να καταγράψει την ανάκληση του πιστοποιητικού, εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.

3. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης δύναται να αναγράφει σε αναγνωρισμένο πιστοποιητικό περιορισμούς χρήσεως αυτού του πιστοποιητικού, με την προϋπόθεση ότι οι περιορισμοί αυτοί είναι αναγνωρίσιμοι για τους τρίτους. Ο πάροχος υπηρεσιών πιστοποίησης δεν υπέχει ευθύνη για βλάβες που προκύπτουν από χρήση ενός αναγνωρισμένου πιστοποιητικού που υπερβαίνει τους περιορισμούς που αναγράφηκαν σε αυτό.

4. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης δύναται να αναγράφει στο αναγνωρισμένο πιστοποιητικό όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί, με την προϋπόθεση ότι τα όρια αυτά είναι αναγνωρίσιμα για τους τρίτους.

Ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για ζημίες που απορρέουν από την υπέρβαση αυτών των ορίων.

5. Οι διατάξεις των παραγράφων 1 έως 4 ισχύουν με την επιφύλαξη της οδηγίας 93/13/ΕΟΚ του Συμβουλίου, της 13ης Απριλίου 1993, σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές(8).

Άρθρο 7

Διεθνείς πτυχές

1. Τα κράτη μέλη διασφαλίζουν ότι τα πιστοποιητικά που εκδίδονται στο κοινό ως αναγνωρισμένα πιστοποιητικά από πάροχο υπηρεσιών πιστοποίησης, εγκατεστημένο σε τρίτη χώρα, θεωρούνται νομικώς ισοδύναμα με πιστοποιητικά που εκδίδονται από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Κοινότητα εάν:

α) ο πάροχος υπηρεσιών πιστοποίησης πληροί τις απαιτήσεις που καθορίζονται στην παρούσα οδηγία και έχει διαπιστευτεί δυνάμει εθελοντικού μηχανισμού πιστοποίησης, καθιερωμένου σε κράτος μέλος, ή

β) πάροχος υπηρεσιών πιστοποίησης, εγκατεστημένος στην Κοινότητα, ο οποίος πληροί τις απαιτήσεις που καθορίζονται στην παρούσα οδηγία, εγγυάται για το πιστοποιητικό, ή

γ) το πιστοποιητικό παρόχου υπηρεσιών πιστοποίησης αναγνωρίζεται δυνάμει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Κοινότητας και τρίτων χωρών ή διεθνών οργανισμών.

2. Η Επιτροπή, για να διευκολύνει τις διασυνοριακές υπηρεσίες πιστοποίησης με τρίτες χώρες και την αναγνώριση προηγμένων ηλεκτρονικών υπογραφών προερχόμενων από τρίτες χώρες, διατυπώνει προτάσεις για την επίτευξη αποτελεσματικής εφαρμογής προτύπων και διεθνών συμφωνιών που ισχύουν για υπηρεσίες πιστοποίησης. Ειδικότερα, όπου κρίνει απαραίτητο, υποβάλλει προτάσεις προς το Συμβούλιο για την έκδοση κατάλληλων εντολών διαπραγμάτευσης διμερών και πολυμερών συμφωνιών με τρίτες χώρες και διεθνείς οργανισμούς. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.

3. Οσάκις η Επιτροπή πληροφορείται τυχόν δυσκολίες που συναντούν οι κοινοτικές επιχειρήσεις όσον αφορά την πρόσβαση σε αγορές τρίτων χωρών, δύναται να υποβάλει στο Συμβούλιο, εφόσον παρίσταται ανάγκη, προτάσεις για τη δέουσα εντολή διαπραγμάτευσης αναλόγων δικαιωμάτων των κοινοτικών επιχειρήσεων σε αυτές τις τρίτες χώρες. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.

Τα μέτρα που λαμβάνονται δυνάμει της παρούσας παραγράφου δεν θίγουν τις υποχρεώσεις της Κοινότητας και των κρατών μελών δυνάμει σχετικών διεθνών συμφωνιών.

Άρθρο 8

Προστασία δεδομένων

1. Τα κράτη μέλη διασφαλίζουν ότι οι πάροχοι υπηρεσιών πιστοποίησης και οι εθνικοί φορείς, αρμόδιοι για πιστοποίηση ή εποπτεία, συμμορφώνονται προς τις απαιτήσεις που καθορίζονται στην οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών(9).

2. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό δύναται να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν, ή με τη ρητή συγκατάθεσή του, και μόνον στο βαθμό που είναι απαραίτητο για τους σκοπούς έκδοσης και διατήρησης του πιστοποιητικού. Δεν επιτρέπεται συλλογή ή επεξεργασία των δεδομένων για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου.

3. Με την επιφύλαξη των εννόμων συνεπειών των ψευδωνύμων δυνάμει της εθνικής νομοθεσίας, τα κράτη μέλη δεν εμποδίζουν τους παρόχους υπηρεσιών πιστοποίησης να αναφέρουν στο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος.

Άρθρο 9

Επιτροπή

1. Η Επιτροπή επικουρείται από την "επιτροπή ηλεκτρονικής υπογραφής", καλούμενη εφεξής "επιτροπή".

2. Όταν γίνεται αναφορά στην παρούσα παράγραφο, εφαρμόζονται τα άρθρα 4 και 7 της απόφασης 1999/468/ΕΚ, με την επιφύλαξη των διατάξεων του άρθρου 8 της εν λόγω απόφασης.

Η περίοδος που προβλέπεται στο άρθρο 4 παράγραφος 3 της απόφασης 1999/468/ΕΚ είναι τρεις μήνες.

3. Η επιτροπή θεσπίζει τον εσωτερικό κανονισμό της.

Άρθρο 10

Καθήκοντα της επιτροπής

Η επιτροπή διευκρινίζει, σύμφωνα με τη διαδικασία του άρθρου 9 παράγραφος 2, τις απαιτήσεις που ορίζονται στα παραρτήματα της παρούσας οδηγίας, τα κριτήρια που αναφέρονται στο άρθρο 3 παράγραφος 4 και τα γενικώς αναγνωρισμένα πρότυπα για προϊόντα ηλεκτρονικής υπογραφής, που καθορίστηκαν και δημοσιεύθηκαν σύμφωνα με το άρθρο 3 παράγραφος 5.

Άρθρο 11

Κοινοποίηση

1. Τα κράτη μέλη κοινοποιούν στην Επιτροπή και στα λοιπά κράτη μέλη τα ακόλουθα:

α) πληροφορίες σχετικά με εθνικά συστήματα εθελοντικής διαπίστευσης, συμπεριλαμβανομένων όλων των πρόσθετων απαιτήσεων σύμφωνα με το άρθρο 3 παράγραφος 7·

β) ονομασίες και διευθύνσεις των εθνικών φορέων που είναι αρμόδιοι για διαπίστευση και επίβλεψη, καθώς και των φορέων που αναφέρονται στο άρθρο 3 παράγραφος 4·

γ) ονομασίες και διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης.

2. Τα κράτη μέλη κοινοποιούν τα ταχύτερο δυνατόν το σύνολο των πληροφοριών που υποβάλλονται βάσει της παραγράφου 1 καθώς και τις σχετικές αλλαγές τους.

Άρθρο 12

Επανεξέταση

1. Η Επιτροπή εξετάζει τη λειτουργία της παρούσας οδηγίας και υποβάλλει σχετική έκθεση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, το αργότερο έως τις 19 Ιουλίου 2003.

2. Στην εξέταση εκτιμάται, μεταξύ άλλων, εάν θα πρέπει να τροποποιηθεί το πεδίο εφαρμογής της παρούσας οδηγίας λαμβανομένων υπόψη των τεχνολογικών, εμπορικών και νομοθετικών εξελίξεων. Στην έκθεση περιλαμβάνεται ιδίως αξιολόγηση, βάσει της κτηθείσας εμπειρίας, πτυχών της εναρμόνισης. Η έκθεση συνοδεύεται, κατά περίπτωση, από νομοθετικές προτάσεις.

Άρθρο 13

Εφαρμογή

1. Τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν με την παρούσα οδηγία πριν από τις 19 Ιουλίου 2001. Ενημερώνουν αμέσως την Επιτροπή σχετικά.

Οι διατάξεις αυτές, όταν θεσπίζονται από τα κράτη μέλη, αναφέρονται στην παρούσα οδηγία ή συνοδεύονται από την αναφορά αυτή κατά την επίσημη δημοσίευσή τους. Οι λεπτομερείς διατάξεις της αναφοράς αυτής καθορίζονται από τα κράτη μέλη.

2. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή το κείμενο των ουσιωδών διατάξεων του εσωτερικού δικαίου που θεσπίζουν στον τομέα που διέπεται από την παρούσα οδηγία.

Άρθρο 14

Έναρξη ισχύος

Η παρούσα οδηγία αρχίζει να ισχύει την ημέρα της δημοσίευσής της στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων.

Άρθρο 15

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 13 Δεκεμβρίου 1999.

Για το Ευρωπαϊκό Κοινοβούλιο

Η Πρόεδρος

N. FONTAINE

Για το Συμβούλιο

Ο Πρόεδρος

S. HASSI

(1) ΕΕ C 325 της 23.10.1998, σ. 5.

(2) ΕΕ C 40 της 15.2.1999, σ. 29.

(3) ΕΕ C 93 της 6.4.1999, σ. 33.

(4) Γνώμη του Ευρωπαϊκού Κοινοβουλίου, της 13ης Ιανουαρίου 1999 (ΕΕ C 104 της 14.4.1999, σ. 49)· κοινή θέση του Συμβουλίου, της 28ης Ιουνίου 1999 (ΕΕ C 243 της 27.8.1999, σ. 33) και

απόφαση του Ευρωπαϊκού Κοινοβουλίου, της 27ης Οκτωβρίου 1999 (δεν δημοσιεύθηκε ακόμα στην Επίσημη Εφημερίδα)· απόφαση του Συμβουλίου, της 30ής Νοεμβρίου 1999.

(5) ΕΕ L 367 της 31.12.1994, σ, 1· κανονισμός όπως τροποποιήθηκε από τον κανονισμό (ΕΚ) αριθ. 837/95 (ΕΕ L 90 της 21.4.1995, σ. 1).

(6) ΕΕ L 367 της 31.12.1994, σ, 8· απόφαση όπως τροποποιήθηκε τελευταία από την απόφαση 99/193/ΚΕΠΠΑ (ΕΕ L 73 της 19.3.1999, σ. 1).

(7) ΕΕ L 184 της 17.7.1999, σ. 23.

(8) ΕΕ L 95 της 21.4.1993, σ. 29.

(9) ΕΕ L 281 της 23.11.1995, σ. 31.

ΠΑΡΑΡΤΗΜΑ I

Όροι ισχύοντες για αναγνωρισμένα πιστοποιητικά

Τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:

α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό·

β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένο·

γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο·

δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό·

ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος·

στ) ένδειξη της έναρξης και τέλος της περιόδου ισχύος του πιστοποιητικού·

ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού·

η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης που το εκδίδει·

θ) ενδεχομένως, περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

ι) ενδεχομένως, όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

ΠΑΡΑΡΤΗΜΑ II

Όροι ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι πάροχοι υπηρεσιών πιστοποίησης πρέπει:

α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης·

β) να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης·

γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς·

δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση, της ταυτότητας και ενδεχομένως, τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό·

ε) να απασχολούν προσωπικό που διαθέτει την εμπειρογνωμοσύνη, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, εμπειρογνωμοσύνη στην τεχνολογία ηλεκτρονικών υπογραφών και εξοικείωση με τις κατάλληλες διαδικασίες ασφαλείας· πρέπει επίσης να χρησιμοποιούν κατάλληλες διοικητικές και διαχειριστικές διαδικασίες οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα·

στ) να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται έναντι τροποποίησης και διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά·

ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και, σε περίπτωση που ο πάροχος υπηρεσιών πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων·

η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών, π.χ. με τη σύναψη κατάλληλης ασφάλισης·

θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο για κατάλληλη χρονική περίοδο, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα·

ι) να μην αποθηκεύουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών·

ια) προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων οι οποίοι βασίζονται στο πιστοποιητικό αυτό·

ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, ούτως ώστε:

- μόνον αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις,

- να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

- να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου, και

- οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω αιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή.

ΠΑΡΑΡΤΗΜΑ III

Απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής

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' ουσίαν 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.

ΠΑΡΑΡΤΗΜΑ IV

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής

Κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται, με εύλογη βεβαιότητα, ότι:

α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα

β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με τον ορθό τρόπο

γ) ο επαληθεύων μπορεί, ενδεχομένως, να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται

δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία

ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς και

ζ) μπορούν να εντοπιστούν τροποποιήσεις απτόμενες της ασφάλειας.

Παράρτημα 4: Π.Δ. 150/2001

ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ ΥΠ΄ ΑΡΙΘ.150/2001

ΦΕΚ 125 Α΄/25-6-2001

Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές

Ο ΠΡΟΕΔΡΟΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

Έχοντας υπόψη:

1.Τις διατάξεις:

α) Του άρθρου 3 του Ν. 1338/1983 «Εφαρμογή του Κοινοτικού Δικαίου» (Α΄ 34), όπως αντικαταστάθηκε με το άρθρο 65 του Ν. 1892/1990(Α΄ 101) «Για τον εκσυγχρονισμό και την ανάπτυξη και άλλες διατάξεις» .

β) Του άρθρου 4 του αυτού Ν. 1338/1983, όπως αντικαταστάθηκε με την παράγραφο 4 του άρθρου 6 του Ν.1440/1984 (Α΄ 70) «Συμμετοχή της Ελλάδος στο κεφάλαιο, τα αποθεματικά και τις προβλέψεις της Ευρωπαϊκής Τράπεζας Επενδύσεων, στο κεφάλαιο της Ευρωπαϊκής Κοινότητας Άνθρακος και Χάλυβος και του Οργανισμού ΕΥΡΑΤΟΜ» και τροποποιήθηκε με το άρθρο 22 του Ν. 2789/2000 (Α΄ 21).

2. Τις διατάξεις του δεύτερου άρθρου του Ν. 2077/1992 «Κύρωση της Συνθήκης για την Ευρωπαϊκή Ένωση και των σχετικών πρωτοκόλλων και δηλώσεων που περιλαμβάνονται στην Τελική Πράξη» (Α΄ 136).

3. Τις διατάξεις του άρθρου 29 Α΄ του Ν. 1558/ 1985(Α΄ 137) το οποίο προστέθηκε με το άρθρο 27 του Ν.2081/1992 (Α΄ 154) και αντικαταστάθηκε με την παρ. 2α του άρθρου 1 του Ν.2469/1997 (Α΄ 38).

4. Τις διατάξεις του Ν. 2867/2000 (Α΄ 273) «Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις».

5. Τις διατάξεις του Ν. 2672/98 (Α΄ 290) «Οικονομικοί πόροι της Νομαρχιακής Αυτοδιοίκησης και άλλες διατάξεις».

6. Ότι από την εφαρμογή του παρόντος Διατάγματος δεν προκαλείται δαπάνη σε βάρος του Κρατικού Προϋπολογισμού.

7. Την υπ' αριθμ. 98/2001 γνωμοδότηση του Συμβουλίου της Επικρατείας μετά από πρόταση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Εθνικής Οικονομίας, Δικαιοσύνης και του Υπουργού Μεταφορών και Επικοινωνιών, αποφασίζουμε:

Άρθρο 1

Σκοπός και Πεδίο Εφαρμογής

1. Με το παρόν Διάταγμα προσαρμόζεται η ελληνική νομοθεσία προς τις διατάξεις της Οδηγίας 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) στο εξής: Οδηγία.

2. Οι διατάξεις του παρόντος Διατάγματος δεν θίγουν διατάξεις που, αναφορικά με τη σύναψη και την 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.

Άρθρο 2
Ορισμοί

Για την εφαρμογή του παρόντος Διατάγματος νοούνται ως:

1. «ηλεκτρονική υπογραφή»: 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.

2. «προηγμένη ηλεκτρονική υπογραφή»ή «ψηφιακή υπογραφή»: ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:

α) συνδέεται μονοσήμαντα με τον υπογράφοντα,

β) 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 του έλεγχο και

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

3. «υπογράφων»: φυσικό ή νομικό πρόσωπο, που κατέχει διάταξη δημιουργίας υπογραφής και ενεργεί είτε στο δικό του όνομα είτε στο όνομα άλλου φυσικού ή νομικού προσώπου ή φορέα.

4. «δεδομένα δημιουργίας υπογραφής»: μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής.

5. «διάταξη δημιουργίας υπογραφής»: διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής.

6. «ασφαλής διάταξη δημιουργίας υπογραφής» διάταξη δημιουργίας υπογραφής, που πληροί τους όρους του Παραρτήματος ΙΙΙ.

7. «δεδομένα επαλήθευσης υπογραφής»: δεδομένα, όπως κώδικες, ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής.

8. «διάταξη επαλήθευσης υπογραφής»: διατεταγμένο υλικό ή λογισμικό, που χρησιμοποιείται για την εφαρμογή των δεδομένων επαλήθευσης υπογραφής.

9. «πιστοποιητικό»: ηλεκτρονική βεβαίωση, η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.

10. «αναγνωρισμένο πιστοποιητικό»: πιστοποιητικό που πληροί τους όρους του Παραρτήματος Ι και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος πληροί τους οριζόμενους στο Παράρτημα ΙΙ όρους.

11. «πάροχος υπηρεσιών πιστοποίησης»: φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.

12. «προϊόν ηλεκτρονικής υπογραφής»: υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την προσφορά υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.

13. «εθελοντική διαπίστευση»: κάθε άδεια διαπίστευσης των ηλεκτρονικών δεδομένων, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις, που διέπουν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται ύστερα από αίτηση του ενδιαφερόμενου παρόχου υπηρεσιών από τον φορέα που προβλέπεται στην παράγραφο 5 του άρθρου 4 του παρόντος.

Άρθρο 3

Έννομες συνέπειες των ηλεκτρονικών υπογραφών

1. Η προηγμένη 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.

2. Η ισχύς της ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο τον λόγο ότι δεν συντρέχουν οι προϋποθέσεις της προηγούμενης παραγράφου.

Άρθρο 4

Πρόσβαση στην αγορά - Αρχές της εσωτερικής αγοράς

1. Τα διατιθέμενα προϊόντα ηλεκτρονικής υπογραφής μπορεί να αφορούν ασφαλείς διατάξεις υπογραφής ή και μη ασφαλείς διατάξεις στον βαθμό που αυτό διατυπώνεται κατά τρόπο απόλυτα σαφή για οποιονδήποτε τρίτο με την επιφύλαξη του άρθρου 3 του παρόντος.

2. Η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς το Παράρτημα ΙΙΙ του παρόντος Διατάγματος διαπιστώνεται από την Εθνική Επιτροπή Τηλεπικοινωνιών Ταχυδρομείων (Ε.Ε.Τ.Τ.) (άρθρο 3 του ν. 2867/2000) ή από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς. Η Ε.Ε.Τ.Τ. και οι οριζόμενοι από αυτή δημόσιοι ή ιδιωτικοί φορείς υποχρεούνται στην εφαρμογή των ελαχίστων κριτηρίων που προβλέπονται στην Απόφαση της Επιτροπής της 6.11.2000 (Ε (2000) 3179 τελικό). Η συμμόρφωση των προϊόντων ηλεκτρονικής υπογραφής προς αναγνωρισμένα πρότυπα αποτελεί τεκμήριο συμμόρφωσης με τις απαιτήσεις που καθορίζονται στο σημείο (στ) του Παραρτήματος ΙΙ και στο Παράρτημα ΙΙΙ του παρόντος.

3. Τα παρεχόμενα πιστοποιητικά επαλήθευσης ορίζουν ρητά, κατά τρόπο εύκολα αντιληπτό από μη ειδικό τρίτο, αν πρόκειται για αναγνωρισμένα ή μη αναγνωρισμένα πιστοποιητικά.

4. Με την επιφύλαξη της παραγράφου 5 του παρόντος άρθρου, για την παροχή των υπηρεσιών πιστοποίησης οποιασδήποτε μορφής δεν απαιτείται η χορήγηση άδειας στους παρόχους των υπηρεσιών αυτών.

5. Προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης, παρέχεται από την Ε.Ε.Τ.Τ. ή από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου παρόχου υπηρεσιών πιστοποίησης, εθελοντική διαπίστευση. Με την εθελοντική διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον πάροχο υπηρεσιών πιστοποίησης. Οι προϋποθέσεις εθελοντικής διαπίστευσης πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες με τον επιδιωκόμενο σκοπό και να μην οδηγούν σε διακρίσεις. Η Ε.Ε.Τ.Τ. δεν μπορεί να περιορίσει τον αριθμό των παρόχων υπηρεσιών πιστοποίησης, που επιθυμούν τη διαπίστευσή τους σύμφωνα με τις διατάξεις του παρόντος.

6. Οι διαπιστευμένοι ή μη, πάροχοι υπηρεσιών πιστοποίησης, που πληρούν τις προϋποθέσεις του Παραρτήματος ΙΙ του παρόντος, εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό.

7. Οι πάροχοι υπηρεσιών πιστοποίησης οφείλουν ιδιαίτερα να μεριμνούν για την από μέρους τους τήρηση των διατάξεων για την προστασία του ανταγωνισμού, για τον αθέμιτο ανταγωνισμό, για την πνευματική και βιομηχανική ιδιοκτησία και για την προστασία του καταναλωτή.

8. Η Ε.Ε.Τ.Τ. έχει την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παροχών υπηρεσιών πιστοποίησης, καθώς και των σύμφωνα με τις παραγράφους 5 και 2 του παρόντος φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το παράρτημα ΙΙΙ.

9. Σε περίπτωση που πάροχος υπηρεσιών πιστοποίησης ενεργεί ως διαπιστευμένος πάροχος υπηρεσιών πιστοποίησης, χωρίς να είναι, η Ε.Ε.Τ.Τ. επιβάλλει πρόστιμο από εξήντα χιλιάδες (60.000) έως τριακόσιες χιλιάδες (300.000) Ευρώ.

Άρθρο 5

Διεθνείς πτυχές

1. Η προσφορά υπηρεσιών πιστοποίησης εντός της ελληνικής επικράτειας από πάροχο υπηρεσιών πιστοποίησης, που είναι εγκατεστημένος στην Ελλάδα διέπεται από την κείμενη ελληνική νομοθεσία.

2. Υπηρεσίες πιστοποίησης στους καλυπτόμενους από τη νομοθεσία της Ευρωπαϊκής Ένωσης για την ηλεκτρονική υπογραφή τομείς, εφόσον προέρχονται από άλλη χώρα μέλος της Ευρωπαϊκής Ένωσης, συνεπάγονται τις ίδιες έννομες συνέπειες με τις αντίστοιχες υπηρεσίες πιστοποίησης, που παρέχονται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος είναι εγκατεστημένος στην Ελλάδα.

3. Προϊόντα ηλεκτρονικής υπογραφής, τα οποία συνάδουν με την κείμενη νομοθεσία της Ευρωπαϊκής Ένωσης, συνεπάγονται τις ίδιες έννομες συνέπειες με τα αντίστοιχα προϊόντα

ηλεκτρονικής υπογραφής, τα οποία προέρχονται από την Ελλάδα. Ιδιαίτερα, η διαπίστωση συμμόρφωσης προς την κείμενη νομοθεσία της Ευρωπαϊκής Ένωσης, που αφορά προϋποθέσεις για ασφαλείς διατάξεις δημιουργίας της υπογραφής από φορέα στον οποίο έχει ανατεθεί η διαπίστωση αυτή σύμφωνα με τη νομοθεσία κράτους μέλους της Ευρωπαϊκής Ένωσης, έχει άμεση ισχύ και στην Ελλάδα.

4. Τα αναγνωρισμένα πιστοποιητικά, που εκδίδονται στο κοινό από πάροχο υπηρεσιών πιστοποίησης, ο οποίος είναι εγκατεστημένος σε χώρα εκτός της Ευρωπαϊκής Ένωσης, είναι νομικώς ισοδύναμα με τα εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Ευρωπαϊκή Ένωση, εφόσον:

α) ο πάροχος αυτός πληροί τους όρους του παρόντος Διατάγματος και έχει διαπιστευθεί εθελοντικώς σε κράτος -μέλος της Ευρωπαϊκής Ένωσης.

β) για το συγκεκριμένο πιστοποιητικό έχει εγγυηθεί πάροχος υπηρεσιών πιστοποίησης, που είναι εγκατεστημένος σε κράτος-μέλος και πληροί τους όρους του παρόντος Διατάγματος. γ) το αναγνωρισμένο πιστοποιητικό του παρόχου υπηρεσιών πιστοποίησης αναγνωρίζεται βάσει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και τρίτων χωρών ή διεθνών οργανισμών.

Άρθρο 6

Ευθύνη των παρόχων πιστοποίησης

1. Ο πάροχος υπηρεσιών πιστοποίησης, διαπιστευμένος ή μη, που εκδίδει αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυάται για την ακρίβεια τέτοιου πιστοποιητικού, ευθύνεται έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημία που προκλήθηκε σε βάρος του επειδή το πρόσωπο αυτό εύλογα βασίσθηκε στο πιστοποιητικό, όσον αφορά: α) την ακρίβεια, κατά τη στιγμή της έκδοσής του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοσή του.

β) τη διαβεβαίωση ότι ο υπογράφων, η ταυτότητα του οποίου βεβαιώνεται στο αναγνωρισμένο πιστοποιητικό, κατά τη στιγμή της έκδοσής του, κατείχε δεδομένα δημιουργίας υπογραφής, που αντιστοιχούσαν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό δεδομένα επαλήθευσης της υπογραφής.

γ) τη διαβεβαίωση ότι αμφότερα τα δεδομένα δημιουργίας υπογραφής και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, εφόσον προέρχονται από πάροχο υπηρεσιών πιστοποίησης.

2. Ο πάροχος υπηρεσιών πιστοποίησης ευθύνεται επίσης, αν παραλείψει να καταγράψει την ανάκληση του πιστοποιητικού.

3. Σε όλες τις παραπάνω περιπτώσεις ο πάροχος δεν ευθύνεται, αν αποδείξει ότι δεν τον βαρύνει πταίσμα.

4. Στο αναγνωρισμένο πιστοποιητικό δύνανται να αναγράφονται, από τον πάροχο υπηρεσιών πιστοποίησης, περιορισμοί χρήσης αυτού, υπό την προϋπόθεση ότι οι περιορισμοί τίθενται κατά τρόπο, ο οποίος είναι αναγνωρίσιμος από οποιονδήποτε τρίτο. Σ΄ αυτή την περίπτωση ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για τη ζημία που προκύπτει από την υπέρβαση των αναφερόμενων περιορισμών κατά τη χρήση του αναγνωρισμένου πιστοποιητικού.

5. Στο αναγνωρισμένο πιστοποιητικό δύνανται να αναγράφονται, από τον πάροχο υπηρεσιών πιστοποίησης, όρια για το ύψος των συναλλαγών, για τις οποίες μπορεί να χρησιμοποιηθεί το σχετικό πιστοποιητικό, με την προϋπόθεση ότι τα όρια αυτά τίθενται κατά τρόπο αναγνωρίσιμο από οποιονδήποτε τρίτο. Στην περίπτωση αυτήν ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για τη ζημία που προκαλείται από την υπέρβαση των ορίων αυτών.

6. Τα οριζόμενα στις διατάξεις των παραπάνω παραγράφων ισχύουν με την επιφύλαξη των διατάξεων του ν.2251/1994 (Α΄191) όπως ισχύει για την προστασία καταναλωτών και ιδιαίτερα για τις καταχρηστικές ρήτρες των συμβάσεων, που συνάπτονται με καταναλωτές.

Άρθρο 7

Προστασία δεδομένων

1. Οι πάροχοι υπηρεσιών πιστοποίησης, η Ε.Ε.Τ.Τ και οι φορείς του άρθρου 4 του παρόντος Διατάγματος υπόκεινται στις διατάξεις του ν. 2472 /1997 (Α΄ 50) και του Ν. 2774 /1999 (Α΄ 287) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

2. Ειδικότερα ο πάροχος των υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικό, δύναται να συγκεντρώνει δεδομένα προσωπικού χαρακτήρα για την έκδοση πιστοποιητικών μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή κατόπιν ρητής συγκατάθεσής του και μόνο στο βαθμό που είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού. Η συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς απαγορεύεται, χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου.

3. Επιτρέπεται στους παρόχους υπηρεσιών πιστοποίησης να αναγράφουν στο αναγνωρισμένο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος.

Άρθρο 8

Κοινοποίηση

1. Η Γενική Γραμματεία Επικοινωνιών του Υπουργείου Μεταφορών Επικοινωνιών ενημερώνει την Ευρωπαϊκή Επιτροπή το ταχύτερο δυνατόν για την εφαρμογή των διατάξεων του άρθρου 4 του παρόντος.

2. Η Ε.Ε.Τ.Τ ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών παρόχων υπηρεσιών πιστοποίησης.

3. Τυχόν αλλαγές των παραπάνω πληροφοριών ανακοινώνονται το ταχύτερο δυνατόν στην Επιτροπή από τα ανωτέρω όργανα.

Άρθρο 9

Παραρτήματα

Αποτελούν αναπόσπαστο μέρος του παρόντος τα παρακάτω Παραρτήματα I, II, III και IV

ΠΑΡΑΡΤΗΜΑ I

Όροι ισχύοντες για αναγνωρισμένα πιστοποιητικά

Τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:

α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό,

β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος, στο οποίο είναι εγκατεστημένος,

γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο,
δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό,
ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος,

στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού,
ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού,

η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου των υπηρεσιών πιστοποίησης που το εκδίδει,
θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

ι) τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

ΠΑΡΑΡΤΗΜΑ II

Όροι ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι παρόχοι υπηρεσιών πιστοποίησης πρέπει:

α) να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών πιστοποίησης, σύμφωνα με τα εκάστοτε ισχύοντα κριτήρια,

β) να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης,
γ) να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί επακριβώς,

δ) να προβαίνουν, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε επαλήθευση της ταυτότητας και ενδεχομένως τυχόν ειδικών χαρακτηριστικών του ατόμου στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό.

ε) 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.

στ) 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.

ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και σε περίπτωση που ο πάροχος πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων.
η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών,
θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό για χρονικό διάστημα τριάντα (30) ετών, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα.

ι) να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών.
ια) πριν συνάψουν συμβατική σχέση με πρόσωπο που ζητεί πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, συμπεριλαμβανομένων ενδεχομένων περιορισμών της χρήσης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων, οι οποίοι βασίζονται στο πιστοποιητικό αυτό.

ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, ούτως ώστε:

- μόνο αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις
- να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

- να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου και

- οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω απαιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή.

ΠΑΡΑΡΤΗΜΑ III

Διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής

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 μία φορά και ότι το απόρρητο είναι διασφαλισμένο.
β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας,
γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.

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

ΠΑΡΑΡΤΗΜΑ IV

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής

Κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται με εύλογη βεβαιότητα ότι:

α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα,

β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο,

γ) ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται,

δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία,

ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο,

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς, και

ζ) μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.

Άρθρο 10

Έναρξη ισχύος

Η ισχύς του παρόντος Διατάγματος αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως.

Στον Υπουργό Μεταφορών και Επικοινωνιών αναθέτουμε τη δημοσίευση και εκτέλεση του παρόντος Διατάγματος.

Κεφάλαιο 11

Βιβλιογραφία

[1] Δ.Μαρτάκος, Ν.Κυρλόγλου, Α.Μητράκας, Μ.Γιαννακάκη, Χ.Σιούλης. «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης». E-business forum, ομάδα εργασίας 'Ε2'

[2] Κρυπτογραφία:
http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[3] Scytale: http://en.wikipedia.org/wiki/Scytale

[4] Κρυπτογράφηση συμμετρικού κλειδιού:
http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

[5] Σημειώσεις: Βασικά θέματα κρυπτογραφίας συμμετρική και ασύμμετρη κρυπτογραφία-Ψηφιακές υπογραφές, Διδάσκων της πληροφορικής κ. Καλλονιάτης Χρήστος, Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας, Πανεπιστήμιο Αιγαίου.

[6] Ηλεκτρονική υπογραφή: http://dlib.ionio.gr/gsdl/cgi-bin/library?e=d-01000-00---0ctheses--00-1--0-10-0---0---0prompt-10---4-------0-1l--11-en-50---20-about---00-3-1-00-0011-1-0utfZz-8-00&cl=CL2.11&d=HASH019b625359ef9b8d6f6ac8a7&x=1

[7] Ψηφιακές υπογραφές:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

[8] Α. Σινανιώτη - Μαρούδη & Ι. Δ. Φαρσαρώτας , «Ηλεκτρονική Τραπεζική», Εκδόσεις Σάκκουλα, Αθήνα 2005.

[9] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. , CRC Press, 1996.

[10] Ηλεκτρονικά έγγραφα:
http://www.go-online.gr/ebusiness/specials/article.html?article_id=569

[11] Συνάρτηση κατακερματισμού:
http://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

[12] Κρυπτογράφηση: http://www.go-online.gr/ebusiness/specials/article.html?article_id=710

[13] Κρυπτογράφηση Δημόσιου κλειδιού:
http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3

%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

[14] Ηλεκτρονικές υπογραφές:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/

[15] Κρυπτογραφία: http://www.etender.info/index.php?id=305&L=7

[16] Κρυπτογραφία: http://www.islab.demokritos.gr

[17] Διεθνής Ένωση Τηλεπικοινωνιών (ITU): http://www.unric.org/el/-articles/15773

[18] Σημειώσεις καθ.Μ.Γεωργακόπουλος - υπ.διδάκτωρ Μ.Φραγκάκης από το μάθημα Θεωρία Αριθμών, Περιγραφή και Παραδείγματα της μεθόδου RSA,2007-2008 ,Πανεπιστήμιο Πειραιώς.

[19] Στ.Γκρίτζαλης- Σ.Κ.Κάτσικας & Δ.Γκρίτζαλης, «Ασφάλεια Δικτύων Υπολογιστών», Εκδόσεις Παπασωτηρίου, Αθήνα 2003.

[20] Ένωση Ελληνικών Τραπεζών, ‘’Οι ηλεκτρονικές υπογραφές στο ευρωπαϊκό και ελληνικό δίκαιο’’, κ. Ανδρέας Μητράκας, ειδική έκδοση 2000.

[21] Απόφαση 248/71/15-3-2002 της ΕΕΤΤ "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής", (ΦΕΚ 603/Β’/16-05-2002).

[22] Electronic signatures and infrastructures (ESI)-Policy requirements for certification authorities issuing qualified certificates. ETSI TS:
http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf

[23] Ν.2672/1998, άρθρο 14 (ΦΕΚ 290 - ΤΕΥΧΟΣ Α’): ‘’Διακίνηση εγγράφων μεταξύ Δημοσίου, ΝΠΔΔ και ΟΤΑ και ιδιωτών με ηλεκτρονικά μέσα’’.

[24] Προεδρικό Διάταγμα 342/2002 (ΦΕΚ 284/Α/22-11-2002): ‘’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’’

[25] Προεδρικό Διάταγμα 150/2001 (ΦΕΚ 125/Α/25-06-2001): ‘’Προσαρμογή στην Οδηγία 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές’’.

[26] Οδηγία 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.

[27] Το πρόβλημα της ηλεκτρονικής υπογραφής, άρθρο του καθηγητή κ^{ου} Κ.Μπέη:
http://www.kostasbeys.gr/articles.php?s=5&mid=1479&mnu=3&id=18381

[28] Online Certificate Status Protocol (OCSP):
http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

[29] Adacom: http://www.adacom.com/

[30] ΕΒΕΑ: http://www.acci.gr/acci/Home/tabid/28/language/el-GR/Default.aspx

[31] Πάροχοι Υπηρεσιών Πιστοποίησης:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/EsignProviders.html

[32] Ψηφιακή υπογραφή:
http://www.et.gr/index.php?option=com_content&view=article&id=97&Itemid=190&lang=el

[33] Προσθήκη αξιόπιστης ταυτότητας για τα ηλεκτρονικά Φ.Ε.Κ:
http://www.et.gr/index.php?option=com_content&view=article&id=98%3Aadd-digital-sign-checker-how-to&catid=50&Itemid=97&lang=el

[34] Κρυπτογραφία και Ψηφιακή Υπογραφή, Κέντρο ΠΛΗ.ΝΕ.Τ. Ν. Φλώρινας:
http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cryptography-DigitalSignature.html

[35] Κορνηλία Δελούκα –Ιγγλέση, ‘’Νομικά θέματα ηλεκτρονικού εμπορίου’’, Εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα- Κομοτηνή 2005.

[36] Γεωργίου Α. Γεωργιάδη , ‘’Η σύναψη συμβάσεως μέσω του διαδικτύου ’’, Εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα- Κομοτηνή 2003.

[37] Σύστημα Kerberos: http://www.islab.demokritos.gr

[38] Β.Α. Κάτος Γ.Χ. Στεφανίδης, ‘’Τεχνικές κρυπτογραφίας και κρυπτανάλυσης ‘’, Εκδόσεις Ζυγός, Θεσαλονίκη 2003.

[39] Κωνσταντίνος Ν. Χριστοδούλου, ‘’Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία’’, Εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα- Κομοτηνή 2001.

[40] Δημήτρης Ν. Μανιώτης, ‘’Η σύναψη της ηλεκτρονικής συμβάσεως και η ευθύνη των παρεχόντων συνδρομή στην κατοχύρωση της γνησιότητας και του αναλλοίωτου των ηλεκτρονικών υπογραφών’’, Εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα- Κομοτηνή 2003.

[41] Δημήτρης Ν. Μανιώτης, ‘’Η ψηφιακή υπογραφή ως μέσω διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο’’, Εκδόσεις Αντ.Ν.Σάκκουλα, Αθήνα- Κομοτηνή 1998.

[42] Η υποδομή δημόσιου κλειδιού, είδη πιστοποιητικών:
http://www.go-online.gr/ebusiness/specials/article.html?article_id=714

[43] Πάροχοι Υπηρεσιών Πιστοποίησης:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/GenikesPlirofories.html

[44] e-Banking: http://www.eurobank.gr/online/home/generic.aspx?id=73&mid=467&lang=gr
m-Banking: http://www.eurobank.gr/online/home/generic.aspx?id=74&mid=468&lang=gr

[45] Χρηματιστήριο Αθηνών: http://www.ase.gr/repository/

[46] Αρχή Πιστοποίησης VeriSign: http://en.wikipedia.org/wiki/VeriSign
και http://www.verisign.com/

[47] Προσωπικός αριθμός αναγνώρισης-PIN:
http://en.wikipedia.org/wiki/Personal_identification_number

Για το Β΄ Μέρος της εργασίας

[48] Εθνική πύλη δημόσιας διοίκησης ermis: www.ermis.gov.gr

[49] ‘’Κανονισμός Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου’’
(ΦΕΚ 799 /Β΄ /09-06-2010).

[50] Κοινωνία της Πληροφορίας ΑΕ ‘’Πλαίσιο ψηφιακής αυθεντικοποίησης’’, έκδοση 2.00 ,Μάιος 2008.

[51] Κοινωνία της Πληροφορίας ΑΕ ‘’Πλαίσιο διαλειτουργικότητας & υπηρεσιών ηλεκτρονικών συναλλαγών’’, έκδοση 2.00 ,Μάιος 2008.