ΠΕΡΙΛΗΨΗ

Η αλματώδης ανάπτυξη των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών έχει επιφέρει μεγάλες κοινωνικές, οικονομικές και οργανωτικές αλλαγές και διαμορφώνει μία καινούργια μορφή κοινωνίας, που ονομάζεται κοινωνία της πληροφορίας. Η ραγδαία αύξηση της χρήσης του Η/Υ, καθώς και η χρησιμοποίηση του Διαδικτύου έχει επηρεάσει τη συναλλαγή ,το εμπόριο ,την επικοινωνία και τη διοίκηση των υπηρεσιών του κράτους.

Η διατριβή περιλαμβάνει μια αναφορά στην Κοινωνία Της Πληροφορίας και του Διαδικτύου και στη συμβολή τους στη βελτίωση της παραγωγικότητας της παγκόσμιας οικονομίας καθώς και στη βελτίωση της ποιότητας ζωής των πολιτών και στη συνέχεια με στόχο την εξοικείωση του αναγνώστη αναλύονται οι ενότητες σχετικά με το θεσμικό πλαίσιο που αναφέρεται στην ηλεκτρονική υπογραφή στην Ελλάδα και σε άλλες χώρες, γίνεται αναφορά στην κοινοτική οδηγία 1999/93 και ανάλυση της ελληνικής νομοθεσίας, που διέπει την ηλεκτρονική υπογραφή (π.δ. 150/2001).

Στην συνέχεια αναλύεται η έννοια της ηλεκτρονικής διακυβέρνησης, η οποία με τις υποστηρικτικές της τεχνολογίες μπορεί να μεταμορφώσει το δημόσιο τομέα, περιορίζοντας τη γραφειοκρατία και τα έξοδα και παρέχοντας περισσότερο ποιοτικές υπηρεσίες και γίνεται εκτενής αναφορά στις σημαντικές απαιτήσεις ασφάλειας του εγχειρήματος ηλεκτρονικής διακυβέρνησης, για την προστασία των πολιτών και των επιχειρήσεων που συναλλάσσονται με το Δημόσιο.

Τέλος η εργασία ολοκληρώνεται με κάποια συμπεράσματα και στη συνέχεια παρατίθεται ένα παράρτημα όπου παρουσιάζεται μια εφαρμογή κρυπτογράφησης και αποκρυπτογράφησης με τη χρήση της ψηφιακής υπογραφής και των νομοθετικών κειμένων ,στα οποία στηρίχθηκε η διατριβή και ακολουθεί η βιβλιογραφία , ελληνική και ξένη.

ABSTRACT

The fast paced development of information technology and of telecommunications has brought about great social financial and organizational changes and has led to the creation of a new form of society which is called the society of information. The ever-increasing use of computers, as well as the use of the Internet, has influenced business transactions, commerce, communications and public administration services.

This thesis comprises a report on the Society of Information and the Internet and is aiming at familiarizing the reader with them. The various units dealing with all legal issues concerning the electronic signature are then analyzed and a report is made concerning the European Union instruction 1999/93. Also, an analysis of the greek legislation concerning the electronic signature (decree number 150/2001) is made.

Another analysis then follows concerning the meaning of the electronic signature, its kinds an its applications; an extensive report on cryptography is also made as well as on the function of signatures, on the Services providing certification of electronic signatures, on the infrastructure of the Public Key for the issuing, the provision and the use of certificates and on the function of electronic administration with the use of the electronic signature in all kinds of electronic documents.

The thesis concludes with some assumptions followed by an index where is a detailed description of the algorithmus of the Public Key and of the legal bibliography on which the thesis was based. Finally, all the greek and foreign bibliography used is mentioned.

Στη μνήμη του πατέρα μου Δημήτρη
και στην αμέριστη υποστήριξη της
μητέρας μου Σταυρούλας

ΕΥΧΑΡΙΣΤΙΕΣ

Η εκπόνηση της διπλωματικής μου εργασίας ήταν μια πολύτιμη διδακτική εμπειρία και φτάνοντας στην ολοκλήρωσή της, αισθάνομαι υποχρεωμένη να εκφράσω τις ευχαριστίες μου σε εκείνους τους ανθρώπους, που μου προσέφεραν. Πρώτα από όλα θα ήθελα να ευχαριστήσω την κ. Αριστέα Σινανιώτη Καθηγήτρια Εμπορικού Δικαίου του Τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων του Πανεπιστημίου Πειραιώς, που μου έδωσε την ευκαιρία να ασχοληθώ με ένα θέμα ιδιαίτερου ενδιαφέροντος, όπως επίσης για τη μέριμνα και την καθοδήγησή της. Ευχαριστώ τον καθηγητή κ. Νικήτα Ασημακόπουλο για το αμείωτο ενδιαφέρον του, τις ουσιαστικές απόψεις και υποδείξεις του καθ' όλη τη διάρκεια μελέτης και συγγραφής της εργασίας καθώς και τον Λέκτορα κ. Χαράλαμπο Κωνσταντόπουλο για το ενδιαφέρον του, την καθοδήγηση, τις ιδέες και το χρόνο του, που μου διέθεσε ως μέλη της τριμελούς εξεταστικής επιτροπής. Τέλος, ευχαριστώ την οικογένειά μου για την υποστήριξη και την αγάπη της.

ΠΕΡΙΕΧΟΜΕΝΑ

1.Η ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

1.1Εισαγωγή

Τα τελευταία χρόνια παρατηρείται ουσιαστική συμβολή των Τεχνολογιών Πληροφορικής και Επικοινωνιών στη βελτίωση της παραγωγικότητας των επιχειρήσεων και των οργανισμών ,η οποία αποτελεί βασικό στοιχείο της ανταγωνιστικότητας των σύγχρονων οικονομιών και συνδέεται με τη δυνατότητα νέων τρόπων του «επιχειρείν», τη δημιουργία καινοτομικών προϊόντων και υπηρεσιών, τη βελτίωση των δεξιοτήτων του εργατικού δυναμικού καθώς και στη βελτίωση της καθημερινής ζωής των πολιτών με πρακτικούς τρόπους ενώ η συνεισφορά των τεχνολογιών πληροφορικής και επικοινωνιών στη βελτίωση της ποιότητας των ζωής του πολίτη είναι αναγνωρισμένη και αποδεδειγμένη διεθνώς.

Επιπλέον οι Τεχνολογίες Πληροφορικής και Επικοινωνιών αποτελούν σημαντικό στοιχείο της κοινωνίας της γνώσης και της βιώσιμης ανάπτυξης και οδηγούν στη βελτίωση της ποιότητας ζωής του πολίτη, αφού καθιστούν δυνατές τις κρίσιμες αλλαγές, που απαιτούνται στη Δημόσια Διοίκηση για την παροχή αποτελεσματικών υπηρεσιών προς τους πολίτες ενώ η εφαρμογή των τεχνολογιών πληροφορικής και επικοινωνιών από Δημόσιους φορείς και οργανισμούς με στόχο την παροχή υπηρεσιών για τη εξυπηρέτηση των πολιτών αυξάνει με ραγδαίους ρυθμούς.

Η ανάπτυξη της νέας αυτής κοινωνίας, της Κοινωνίας της Πληροφορίας δημιουργεί σαφώς νέες μεθόδους εργασίας, νέες δεξιότητες και συμβάλει στη διεύρυνση των αναπτυξιακών δυνατοτήτων των χωρών, στην επιτάχυνση του ρυθμού οικονομικής μεγένθυσης, στη βελτίωση και αύξηση της παραγωγικότητας καθώς και στη βελτίωση της ποιότητας ζωής όλων των πολιτών χωρίς αποκλεισμούς ενισχύοντας την ισότιμη πρόσβαση όλων των πολιτών στις δυνατότητες των νέων τεχνολογιών (Ευρυζωνικότητα νοικοκυριών – Η/Υ σε πολίτες – Προσβασιμότητα σε ΑΜΕΑ)και στοχεύοντας στην αποτελεσματικότερη αξιοποίηση των τεχνολογιών πληροφορικής και επικοινωνιών.

Είναι εμφανής ο ρόλος των Τεχνολογιών Πληροφορικής και Επικοινωνιών στην παραγωγικότητα των οικονομιών αλλά και στην καθημερινή ζωή των πολιτών ενώ αυξάνεται σημαντικά η χρήση τους και σε ευρωπαϊκό επίπεδο. Ειδικότερα, την τελευταία δεκαετία παρατηρείται η εμφάνιση μιας πληθώρας εφαρμογών της Τεχνολογίας της Πληροφορίας, όπως είναι οι ισχυροί προσωπικοί υπολογιστές, η στροφή προς τις ευρυζωνικές υπηρεσίες σε εθνικό και διεθνές επίπεδο και η απλοποίηση της δυνατότητας πρόσβασης σε τέτοιου είδους υπηρεσίες στο ευρύ κοινό.

Πλέον, με τη δυναμική αξιοποίηση των νέων Τεχνολογιών Πληροφορικής και Επικοινωνιών είναι δυνατή η άμεση επικοινωνία μεταξύ ιδιαίτερα απομακρυσμένων ανθρώπων με το ηλεκτρονικό ταχυδρομείο, την τηλεσυνδιάσκεψη, την τηλεργασία, το ηλεκτρονικό εμπόριο, τις ηλεκτρονικές τραπεζικές ή άλλου είδους συναλλαγές, οι οποίες δεν απαιτούν από τους συναλλασσόμενους να βρίσκονται στον ίδιο χώρο και σε καθορισμένες χρονικές στιγμές (π.χ. ωράριο καταστημάτων) για να διεκπεραιωθούν.

Οι αυξημένες απαιτήσεις όμως της σύγχρονης ζωής για μεγαλύτερη ευελιξία και περισσότερες διευκολύνσεις των πολιτών στις συναλλαγές τους με τον δημόσιο τομέα καθιστούν δυνατές τις κρίσιμες αλλαγές που απαιτούνται από την Πολιτεία στο να επαναπροσδιορίσει τις σχέσεις της με τους πολίτες και τις επιχειρήσεις, τις μεθόδους συνεργασίας των διαφόρων κρατικών λειτουργών και τους τρόπους εξυπηρέτησης μεταβάλλοντας τους στόχους του κράτους, θέτοντας ως πρωταρχικό στόχο την εξυπηρέτηση των πολιτών και την άμεση προσφορά απλών και προσβάσιμων ηλεκτρονικών υπηρεσιών ,στοχεύοντας ριζικά στην αλλαγή της κουλτούρας της διακυβέρνησης και βελτιώνοντας την παραγωγικότητα των υπηρεσιών του Δημοσίου Τομέα μέσω της χρήσης Τεχνολογιών Πληροφορικής και Επικοινωνιών.

Ασφαλώς το διαδίκτυο αποτελεί καθοριστικό παράγοντα για την επίτευξη διαρκής οικονομικής ανάπτυξης προσφέροντας τεράστιες δυνατότητες, όπως την ηλεκτρονική αλληλογραφία, την ενημέρωση, τις αγορές on line, την διακίνηση ηλεκτρονικών εγγράφων και μουσικών αρχείων, έχει δημιουργήσει ένα χώρο δίχως όρια μέσα στον οποίο πραγματοποιείται η συναλλαγή πληροφοριών και ανοίγει νέους δρόμους και δυνατότητες, σε εθνικό αλλά και σε διεθνές επίπεδο με τις ηλεκτρονικές συναλλαγές να διαφαίνεται ως ο μελλοντικός τρόπος των εργασιών.

Επίσης η χρήση και η επέκταση των τεχνολογιών πληροφορικής και επικοινωνίας πρέπει να ωφελούν κάθε πτυχή της καθημερινής ζωής. Οι ανωτέρω τεχνολογίες είναι πολύ σημαντικές στις δημόσιες υπηρεσίες, στα νοσοκομεία, στη δημιουργία θέσεων εργασίας, στον πολιτισμό κ.ά. Πρέπει να είναι φιλικές προς τον χρήστη , διαθέσιμες σε όλους και κάθε πρόσωπο πρέπει να έχει την ευκαιρία να αποκτήσει τις απαραίτητες ικανότητες και τη γνώση προκειμένου να κατανοεί τις δυνατότητες της Κοινωνίας της Πληροφορίας, να συμμετέχει ενεργά σε αυτήν και να ωφελείται από αυτήν είτε στον ιδιωτικό είτε στο δημόσιο τομέα.

Απαραίτητη προϋπόθεση όμως για την ανάπτυξη της Κοινωνίας της Πληροφορίας είναι η οικοδόμηση της εμπιστοσύνης του πολίτη στη χρήση νέων τεχνολογιών πληροφορικής και επικοινωνίας και ειδικότερα για τη χρήση του Διαδικτύου ,προέχει να ενισχυθεί η ασφάλεια των συναλλαγών

και να εξασφαλιστεί η προστασία των προσωπικών δεδομένων του χρήστη, όταν συναλλάσσεται στο Διαδίκτυο.

Βέβαια όπως αναφέρθηκε και παραπάνω το κλειδί γα την ανάπτυξη των διεργασιών που επιτελούνται στο Διαδίκτυο είναι κατά βάση η εμπιστοσύνη μεταξύ αυτών που πραγματοποιούν ηλεκτρονικές συναλλαγές για να υπάρξει επιτυχία και διαρκή εξάπλωση των ηλεκτρονικών συναλλαγών. Την ανάγκη αυτή έρχεται να καλύψει το ηλεκτρονικό ισοδύναμο της γραπτής υπογραφής, που έχει την δυνατότητα να επικυρώνει τις διάφορες συναλλαγές στον ιδιωτικό και δημόσιο τομέα με σκοπό την ασφαλή ανταλλαγή εγγράφων ή την ελεύθερη διακίνηση επιταγών, συμβολαίων και τιμολογίων.

Ως συνέπεια αυτής της ηλεκτρονικής πραγματικότητας έρχεται η Κοινοτική Οδηγία που αναφέρεται στις ηλεκτρονικές υπογραφές και ορίζει το νομικό πλαίσιο για την αναγνώρισή τους αποσκοπώντας στην ύπαρξη ενός κοινού πλαισίου και ενός ανοικτού περιβάλλοντος καθώς και της κατάλληλης υποδομής για την πραγματοποίηση ασφαλών ηλεκτρονικών συνδιαλλαγών.

Σύμφωνα με την Κοινοτική Οδηγία είναι δυνατή με την μορφή της ψηφιακής υπογραφής, η διεκπεραίωση με ηλεκτρονικό τρόπο των συναλλαγών μεταξύ των πολιτών, των επιχειρήσεων και των κρατικών λειτουργών , η οποία δημιουργείται και επικυρώνεται με τη βοήθεια της διαδικασίας της κρυπτογράφησης και αποκρυπτογράφησης μέσω μαθηματικών αλγορίθμων ,οι οποίοι κάνουν χρήση δύο κλειδιών, ενός προσωπικού και ενός κοινού, για την πιστοποίησή της.

Ένα άλλο επίσης σημαντικό στοιχείο των συναλλαγών στο Διαδίκτυο και στην Κοινωνίας της Πληροφορίας αποτελεί το ηλεκτρονικό έγγραφο που διαφέρει νομικά από τα έγγραφα του άρθρου 160 Αστικού κώδικα, γιατί ένα από τα χαρακτηριστικά του είναι ότι στερείται ιδιόχειρης υπογραφής αλλά και της σταθερότητας κατά την ενσωμάτωσή του σε υλικό, που να παρουσιάζει διάρκεια ζωής αλλά παρέχει τη δυνατότητα να αναγνωσθεί με τη μορφή κειμένου στην οθόνη του τερματικού με την υποστήριξη της κατάλληλης τεχνικής διαδικασίας που επιτρέπει την μετατροπή των αρχειοθετημένων μαγνητικών εγγραφών σε εικόνα, γράμματα και λέξεις και χρησιμοποιείται σε συμβάσεις που καταρτίζονται ηλεκτρονικά, στο ηλεκτρονικό εμπόριο και σε ηλεκτρονικές βάσεις δεδομένων.

Γίνεται λοιπόν έτσι κατανοητό ότι οι ηλεκτρονικές συναλλαγές πρέπει να υποστηριχθούν με διεθνή συνεργασία ώστε η δημιουργία ενός διεθνούς περιβάλλοντος θα ενθαρρύνει τη διάδοση της τεχνολογίας και την πλήρη και αποτελεσματική συμμετοχή των αναπτυσσόμενων χωρών στη λήψη αποφάσεων για την προστασία του καταναλωτή και για την επίτευξη της ασφάλειας στις ηλεκτρονικές συναλλαγές που είναι απαραίτητη προϋπόθεση και εγγύηση για την ομαλή λειτουργία της οικονομικής και κοινωνικής ζωής της παγκόσμιας κοινότητας.

Τέλος πρέπει να αναφερθεί ότι κάθε δημοκρατική κοινωνία έχει την ηθική και νομική υποχρέωση να αγωνίζεται για την εξάλειψη των κάθε είδους αποκλεισμών και να λαμβάνει πρωτοβουλίες ώστε ο κάθε πολίτης να απολαμβάνει εύκολη και ισότιμη πρόσβαση στις υπηρεσίες του κράτους και στην Ελληνική Πολιτεία, το δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας θεσμοθετείται από το Σύνταγμα της Ελλάδος .

Στην περίπτωση που οι υπηρεσίες του κρατικού μηχανισμού πραγματοποιούνται μέσω ηλεκτρονικών μεθόδων το κράτος είναι υποχρεωμένο με βάση το κατάλληλο στρατηγικό Σχέδιο να φροντίζει για τις δυσκολίες εκείνου του τμήματος του κοινωνικού συνόλου που δυσκολεύονται να προσαρμοστούν στα νέα δεδομένα της ηλεκτρονικής διακυβέρνησης αναπτύσσοντας πρωτοβουλίες επιμόρφωσης, επιδοτήσεων ηλεκτρονικών υπολογιστών, δημιουργίας κέντρων ηλεκτρονικών υπολογιστών και διαδικτύου σε σχολεία, δημόσιες βιβλιοθήκες κ.τ.λ. έτσι ώστε να επιχειρήσει να γεφυρώσει αυτό το «ψηφιακό χάσμα» και να βοηθήσει τους πολίτες να αναζητούν και να διεκπεραιώνουν με επιτυχία τις συναλλαγές που επιθυμούν διατηρώντας για ένα χρονικό διάστημα τις παραδοσιακές μεθόδους παροχής υπηρεσιών, για όσους αδυνατούν να χρησιμοποιήσουν τις ανάλογες ηλεκτρονικές.

Εξίσου σημαντική πρέπει είναι και η μέριμνα της πολιτείας και για το τμήμα εκείνο του πληθυσμού με σωματικές δυσκολίες, όπως περιορισμένη όραση, ή και νοητικές δυσκολίες όπου η κάθε δημόσια υπηρεσία με ηλεκτρονική παρουσία, έχει την υποχρέωση να προσαρμόζει τις ηλεκτρονικές υπηρεσίες σε ένα ειδικά σχεδιασμένο ηλεκτρονικό πρόγραμμα για τους πολίτες που αντιμετωπίζουν τέτοιου είδους δυσκολίες, προκειμένου να προσαρμοστούν στο βαθμό που μπορούν στις απαιτήσεις της νέας ηλεκτρονικής πραγματικότητας.

2.ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

2.1Εισαγωγή

Είναι γνωστό ότι η συνεχώς αυξανόμενη χρήση του Διαδικτύου για την σύναψη των εμπορικών συμβάσεων, το ηλεκτρονικό εμπόριο και οι ανυπολόγιστες επιδράσεις του στην οικονομία δημιούργησε σημαντικές δυνατότητες ανάπτυξης των ανοικτών ηλεκτρονικών συναλλαγών αλλά παράλληλα δημιουργήθηκε και ο προβληματισμός σχετικά με τη δεσμευτικότητά των ανοικτών ηλεκτρονικών συναλλαγών, την ασφάλειά τους καθώς και την ταυτοποίηση των συναλλασσομένων.

Έτσι εν όψει της νέας ηλεκτρονικής πραγματικότητας προέκυψε η ανάγκη για μεγαλύτερη βεβαιότητα σε σχέση με το ποιος και με ποιους όρους υπογράφει μια συναλλαγή ,ώστε να παρέχεται η δυνατότητα γνωστοποίησης της πραγματικής ταυτότητας του αντισυμβαλλομένου σε ένα ανοικτό δίκτυο όπως είναι το Internet.

Επομένως διαπιστώνουμε ότι η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών προκύπτει από την ανάγκη ειδικής αναγνώρισης μιας ηλεκτρονικής μεθόδου εξαιτίας της εισαγωγής της τεχνολογίας στις ηλεκτρονικές συναλλαγές τόσο για τις ηλεκτρονικές υπογραφές όσο και για τα ηλεκτρονικά έγγραφα που θα τις συνοδεύουν και η οποία θα είναι νομικά έγκυρη και ισότιμη με τη χειρόγραφη μέθοδο παραγωγής υπογραφής, ώστε να μπορεί να χρησιμοποιηθεί κατά τη διαδικασία της απόδειξης.

Έτσι γίνεται αντιληπτό ότι η ανάγκη νομοθετικής ρύθμισης των ηλεκτρονικών υπογραφών οδήγησε διεθνείς οργανισμούς, την Επιτροπή Ευρωπαϊκών Κοινοτήτων καθώς και κυβερνήσεις διαφόρων χωρών, να δραστηριοποιηθούν προκειμένου να ορίσουν το νομικό πλαίσιο των ηλεκτρονικών συναλλαγών, που ήταν απαραίτητο για την επίτευξη της ασφάλειας στις ηλεκτρονικές συναλλαγές .

Βέβαια σημαντικό εμπόδιο στη νομοθετική ρύθμιση των ηλεκτρονικών συναλλαγών για πολλά χρόνια αποτέλεσε η πολιτική πολλών κυβερνήσεων στον τομέα της κρυπτογραφίας, που τόσο η αμερικανική κυβέρνηση όσο και οι ευρωπαϊκές κυβερνήσεις θεωρούσαν τον τομέα αυτό ως αποκλειστικά εθνική τους υπόθεση και συνεπώς αρνούνταν να προχωρήσουν σε διεθνές επίπεδο για την νομική αναγνώριση των ηλεκτρονικών υπογραφών , που ήταν απαραίτητη προϋπόθεση για την ασφάλεια των ηλεκτρονικών συναλλαγών. (www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

2.2 Διεθνής αναγνώριση των ηλεκτρονικών υπογραφών

Οι πρώτες προσπάθειες για την νομοθετική ρύθμιση της χρήσης ηλεκτρονικών υπογραφών ξεκίνησαν στα μέσα της δεκαετίας του 1990 και συγκεκριμένα στην Πολιτεία της Γιούτα των ΗΠΑ όπου ψηφίστηκε ο πρώτος ολοκληρωμένος Νόμος για τις ηλεκτρονικές υπογραφές και με ιδιαίτερη αναφορά στο νομικό αποτέλεσμα των ηλεκτρονικών υπογραφών, στη ρύθμιση και στην αδειοδότηση της παροχής σχετικών υπηρεσιών ηλεκτρονικής υπογραφής. (www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Μια ανάλογη προσπάθεια σημειώθηκε πάλι σε διεθνές επίπεδο από την Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) η οποία συνέταξε 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, προσπαθώντας με αυτόν τον τρόπο να ρυθμίσει ζητήματα σχετικά με την εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, την νομική ισχύς της ηλεκτρονικής υπογραφής, την αποδεικτική δύναμη των ηλεκτρονικών κειμένων, τον τόπο , τον χρόνο και την απόδειξη παραλαβής του ηλεκτρονικού μηνύματος. Έτσι οι παραπάνω ενέργειες των Ηνωμένων Εθνών, του Διεθνούς Εμπορικού Επιμελητηρίου και του Αμερικανικού Δικηγορικού Συλλόγου δείχνουν την ανάγκη της ρύθμισης των ηλεκτρονικών υπογραφών ,ώστε να διασφαλίζεται με Νόμο ή συμβατικά η δεσμευτικότητά τους στις συναλλαγές .(νομικά ζητήματα –http://www.go-online.gr)

Ανάλογες ενέργειες έχουμε και σε ευρωπαϊκό επίπεδο , όπου με την Οδηγία 1999/93/ΕΚ ορίζεται για πρώτη φορά το γενικό πλαίσιο για τη νομική αναγνώριση των ηλεκτρονικών υπογραφών και τη δημιουργία ενός κοινού και ενιαίου επιπέδου ρυθμιστικού πλαισίου για τις χώρες τις Ευρωπαϊκής Ένωσης με αποτέλεσμα να διασφαλίζεται η νομική αναγνώριση των ηλεκτρονικών υπογραφών (άρθρο 5.1) ως αντίστοιχες με τις χειρόγραφες.

Επίσης η συγκεκριμένη Οδηγία θέτει τις προϋποθέσεις εκείνες που είναι απαραίτητες για τη δημιουργία ενός κοινού και ενιαίου επιπέδου ηλεκτρονικών υπογραφών ,ενώ το πλεονέκτημα που προκύπτει από την εφαρμογή της οδηγίας στις διάφορες εθνικές νομοθεσίες των χωρών μελών είναι ότι εξασφαλίζεται η ελεύθερη κυκλοφορία των προϊόντων εντός της εσωτερικής αγοράς και ενισχύεται η εμπιστοσύνη στις ηλεκτρονικές υπογραφές απαραίτητη για την ομαλή λειτουργία της οικονομικής ζωής εντός και εκτός των Ευρωπαϊκών συνόρων. (De Wikipedia, la enciclopedia libre)

Στη συνέχεια η Ευρωπαϊκή Ένωση αναγνωρίζοντας την ανάγκη νομικής ρύθμισης των ηλεκτρονικών συναλλαγών προχώρησε ακόμη σε ένα σημαντικό βήμα, και εξέδωσε Οδηγία σχετικά με το Ηλεκτρονικό εμπόριο με αριθμό 2000/31/ΕΚ που τέθηκε σε ισχύ στις 17/07/2000 και σύμφωνα με αυτήν καθιερώθηκε η αρχή της ελευθερίας σύναψης ηλεκτρονικών

συμβάσεων, η αρχή της χώρας προέλευσης, που σημαίνει ότι το Δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το Δίκαιο της χώρας μόνιμης εγκατάστασης του φορέα παροχής υπηρεσιών και ο εξωδικαστικός διακανονισμός των διαφορών που θα προκύψουν. (http://www.go-online.gr - νομικά ζητήματα)

Προκειμένου να διασφαλιστεί ακόμη περισσότερο η γνησιότητα της ηλεκτρονικής υπογραφής το Ευρωπαϊκό Κοινοβούλιο προχώρησε σε μία επιπλέον σημαντική πρωτοβουλία για να επιτευχθεί περισσότερο η ασφάλεια των ηλεκτρονικών συναλλαγών και προέβλεψε την έκδοση ενός αναγνωρισμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, που είναι μια ηλεκτρονική βεβαίωση, η οποία έχει το πλεονέκτημα να συνδέει τα δεδομένα επαλήθευσης της υπογραφής με ένα φυσικό πρόσωπο, επιβεβαιώνοντας έτσι την ταυτότητά του. (http://www.go-online.gr - νομικά ζητήματα)

Έτσι σε ευρωπαϊκό επίπεδο βλέπουμε τις χώρες που ανήκουν στην Ευρωπαϊκή Ένωση η μία μετά την άλλη να προσπαθούν να εναρμονιστούν με την Ευρωπαϊκή Οδηγία όπως και η Ελλάδα με την έκδοση του υπ΄αριθμ. 150/2001/Προεδρικού Διατάγματος εναρμονίστηκε πλήρως με την Κοινοτική Οδηγία και προέβη σε σημαντικά βήματα προς τη θέσπιση ενός « Δικαίου του Internet» με την ψήφιση του νόμου 2672/1999 για τις ηλεκτρονικές υπογραφές και του νόμου 2251/1994 για την προστασία των καταναλωτών. (http://www.go-online.gr - νομικά ζητήματα)

Ανάλογη πρωτοβουλία είχε και το Ηνωμένο Βασίλειο σχετικά με το θέμα για τις Ηλεκτρονικές Επικοινωνίες του 2000 ("2000 Act") και όρισε τον Κανονισμό για τις ηλεκτρονικές υπογραφές 2002, όπου σύμφωνα με αυτόν ορίζεται το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές ως τα ηλεκτρονικά δεδομένα που είναι συνημμένα σε, ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και που χρησιμεύει ως μέθοδος απόδειξης της γνησιότητας.(http://www.out-law.com/page-443)

Επίσης και η Ιταλική κυβέρνηση έκανε σημαντικά βήματα στον τομέα αυτό με το υπ΄αριθμό 513 προεδρικό διάταγμα στις 10 Νοεμβρίου 1997 όπου θεσπίστηκε η εγκυρότητα της ψηφιακής υπογραφής και γινόταν αναφορά στα κριτήρια και τις διαδικασίες για την κατάρτιση, την αποθήκευση και τη διαβίβαση των εγγράφων με χρήση πληροφορικής και τηλεπικοινωνιών που μετά από αρκετές τροποποιήσεις η ιταλική νομοθεσία υιοθέτησε το κοινοτικό δίκαιο που περιλαμβάνεται στην οδηγία 99/93 για τις ηλεκτρονικές υπογραφές.

Σήμερα, ο νόμος που διέπει την ψηφιακή υπογραφή είναι ο " Κώδικας Ψηφιακής Διοίκησης ‘‘(νομοθετικό διάταγμα της 7 Μάρτη του 2005, αρ. 82, όπως τροποποιήθηκε με το νομοθετικό διάταγμα 4 Απρίλη 2006, αρ.159)που

τέθηκε σε ισχύ την 1η Γενάρη του 2006, με στόχο να εξασφαλίσει και να ρυθμίσει τη διάθεση, τη πρόσβαση, τη διαχείριση και τη διαθεσιμότητα των πληροφοριών σε ψηφιακή μορφή χρησιμοποιώντας τις καταλληλότερες τεχνολογίες πληροφοριών και επικοινωνιών εντός της Ιταλικής Κυβέρνησης.

Σε διεθνές επίπεδο έχουμε ανάλογες πρωτοβουλίες ,όπως στη Χιλή τον νόμο 19.799 που ψηφίστηκε στις 15 Σεπτεμβρίου 2003 όπου αναφέρεται στα ηλεκτρονικά έγγραφα και στην ηλεκτρονική υπογραφή και αναγνωρίζει ότι οι πράξεις, οι συμβάσεις και τα έγγραφα που υπογράφονται από ηλεκτρονική υπογραφή είναι έγκυρα και παράγουν τα ίδια αποτελέσματα με αυτά που εκδίδονται σε έντυπη μορφή και στην Κόστα Ρίκα ψηφίστηκε ο Νόμος 8454, που αναφέρεται στις ψηφιακές υπογραφές και στα ηλεκτρονικά έγγραφα και υπογράφτηκε στις 22 Αυγούστου 2005 επιτρέποντας στον εικονικό κόσμο των ηλεκτρονικών συναλλαγών και διαδικασιών να έχουν νομική ισχύ.

Επίσης στη Γουατεμάλα έχουμε τον νόμο του 2008 για την αναγνώριση των επικοινωνιών και των ηλεκτρονικών υπογραφών καθώς δημιουργήθηκε και μητρώο των Παρόχων Υπηρεσιών Πιστοποίησης ,ενώ στις 2 του Ιουλίου του 2010 στη Νικαράγουα, έχουμε την ψήφιση του νόμου για τις ηλεκτρονικές υπογραφές από τη Γενική Διεύθυνση Τεχνολογίας του Υπουργείου Οικονομικών και ο Οργανισμός Δημόσιας Πίστης είναι ο φορέας διαπίστευσης της ηλεκτρονικής υπογραφής και τέλος με την έκδοση νόμου στο Περού περί ψηφιακών υπογραφών και πιστοποιητικών (N. 27 269), ρυθμίζονται τα σχετικά με τη χρήση της ηλεκτρονικής υπογραφής δίνοντας την ίδια νομική ισχύ με τη χρήση της ιδιόχειρης υπογραφής. (De Wikipedia, la enciclopedia libre)

Συμπερασματικά λοιπόν γίνεται κατανοητό ότι σε διεθνές και ευρωπαϊκό επίπεδο παρατηρείται η ανάγκη νομοθετικής ρύθμισης των ηλεκτρονικών συναλλαγών με την θέσπιση ειδικών προεδρικών διαταγμάτων ανά κράτος, με σκοπό την αναγνώριση της ηλεκτρονικής υπογραφής ,τη διασφάλιση με νόμο της δεσμευτικότητά της στις ηλεκτρονικές συναλλαγές των πολιτών και των επιχειρήσεων και την επίτευξη διαρκούς οικονομικής ανάπτυξης.

2.3 Νομική προσέγγιση

Όπως αναφέρθηκε παραπάνω η νομική αναγνώριση των ηλεκτρονικών υπογραφών σε διεθνές επίπεδο ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με τη θέσπιση σχετικών νόμων σε διάφορα κράτη και με την υιοθέτηση δύο διαφορετικών νομικών προσεγγίσεων:

Η μία νομοθετική προσέγγιση είναι η μινιμαλιστική (minimalist approach), όπου σύμφωνα με αυτή έχουμε πλήρη νομική αναγνώριση των ηλεκτρονικών υπογραφών, ανεξάρτητα από τις τεχνολογικές τους προδιαγραφές και η δεύτερη νομική προσέγγιση είναι η αναλυτική (

prescriptive approach) σύμφωνα με την οποία δίνεται η δυνατότητα σε συγκεκριμένες τεχνολογικές μέθοδοι να παρέχουν αναγνώριση των ηλεκτρονικών υπογραφών ως ισότιμες με τις ιδιόχειρες υπογραφές αφού προηγουμένως ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας.

Έτσι γίνεται κατανοητό ότι η νομική εξίσωση όλων των ηλεκτρονικών υπογραφών με τις ιδιόχειρες ενθαρρύνει μεν τους καταναλωτές να διενεργήσουν ηλεκτρονικές συναλλαγές αλλά και το νομικό κόσμο, που θα κληθεί να την εφαρμόσει ,να την ερμηνεύσει και να την προστατεύσει γιατί η νομική προσέγγιση αναγνώρισης των ηλεκτρονικών υπογραφών δεν περιέχει πολλές δύσκολες τεχνικές έννοιες, με αποτέλεσμα να είναι απλή και εύκολα αντιληπτή.

Επίσης η νομική εξίσωση όλων των ηλεκτρονικών υπογραφών με τις ιδιόχειρες ευνοεί μεν την ανάπτυξη νέων τεχνολογιών ηλεκτρονικής υπογραφής, για το λόγο ότι δεν προτείνεται κάποια συγκεκριμένη τεχνολογία και αφετέρου ενισχύει την ομοιόμορφη σε διεθνές επίπεδο νομοθετική αντιμετώπιση της ηλεκτρονικής υπογραφής αλλά παρατηρείται όμως ένα σοβαρό μειονέκτημα αυτής της νομικής προσέγγισης.

Αυτό το μειονέκτημα είναι η ανυπαρξία ορισμού συγκεκριμένου είδους ηλεκτρονικής υπογραφής, η οποία να δεσμεύει αυτόν που υπογράφει ,όπως γίνεται με την χειρόγραφη υπογραφή και να επιτρέπει σε κάθε μέθοδο ηλεκτρονικής υπογραφής, από την πιο απλή μέχρι την πιο περίπλοκη, να είναι το ίδιο δεσμευτική νομικά.

Βέβαια το πιο σημαντικό μειονέκτημα της μινιμαλιστικής νομοθετικής προσέγγισης είναι το γεγονός ότι, επειδή ακριβώς δεν ορίζονται υψηλά στάνταρ στον τομέα των τεχνολογικών προδιαγραφών για τις ηλεκτρονικές υπογραφές, είναι πιθανό κάποιες από τις ηλεκτρονικές υπογραφές να είναι τεχνολογικά επισφαλείς δίνοντας έτσι την ευκαιρία σε επιτήδειους επιχειρηματίες, που εμπορεύονται ελαττωματικής τεχνολογίας ηλεκτρονικές υπογραφές να εξαπατήσουν τους καταναλωτές, με αποτέλεσμα να είναι αδύνατη η λειτουργία και η καθιέρωση της ηλεκτρονικής υπογραφής ως μέσου ασφαλείας των συναλλαγών στο ηλεκτρονικό εμπόριο.

Αντίθετα με τη μινιμαλιστική νομοθετική προσέγγιση η μαξιμαλιστική ή αναλυτική προσέγγιση είναι νομικά πιο δεσμευτική στην αναγνώριση των ηλεκτρονικών υπογραφών, γιατί επιτρέπει νομική ισχύ μόνο σε ορισμένα είδη ηλεκτρονικών υπογραφών που συμμορφώνονται ή όχι με συγκεκριμένα τεχνικά πρότυπα δημιουργώντας έτσι πολύ ασφαλείς ηλεκτρονικές υπογραφές.

Αν όμως εξετάσουμε την μαξιμαλιστική ή αναλυτική προσέγγιση από άλλη οπτική πλευρά διαπιστώνουμε ότι αποτελεί μεν εμπόδιο στην ελεύθερη ανάπτυξη της αγοράς των ηλεκτρονικών υπογραφών γιατί απαιτεί την

ύπαρξη κάποιων συγκεκριμένων τεχνολογικών προδιαγραφών για την εξίσωση ηλεκτρονικής και χειρόγραφης υπογραφής αλλά από την άλλη προστατεύει τον καταναλωτή από αναξιόπιστες τεχνολογικές εφαρμογές της ηλεκτρονικής υπογραφής που διατίθενται στην αγορά.

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 ακολούθησε μια μικτή προσέγγιση που να συνδυάζει και τις δύο παραπάνω κατευθύνσεις γιατί σκοπός του κοινοτικού νομοθέτη είναι η δημιουργία ενιαίου νομικού πλαισίου μέσα στην ΕΕ για την αποτελεσματική και ενιαία αντιμετώπιση των νέων νομικών ζητημάτων που θα προκύψουν από την εφαρμογή των ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές. (www.ebusinessforum.gr Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης Μ. Γιαννακάκη – Χ.Σιουλής).

2.4 Νομοθετική προσέγγιση της τεχνολογίας των ηλεκτρονικών υπογραφών

Σχετικά με την νομοθετική προσέγγιση της τεχνολογίας των ηλεκτρονικών υπογραφών διαπιστώνουμε διεθνώς ότι υπάρχουν δύο προσεγγίσεις: η μία είναι η τεχνολογικά ουδέτερη νομική προσέγγιση των ηλεκτρονικών υπογραφών, η οποία οφείλει να προνοεί τη χρήση ηλεκτρονικών υπογραφών με διαφορετικά μεταξύ τους τεχνικά χαρακτηριστικά, ακόμη και με χαρακτηριστικά που δεν έχουν ως σήμερα εφευρεθεί.

Αντίθετα , η τεχνολογική εξειδικευμένη νομοθεσία που αναφέρεται στις ηλεκτρονικές υπογραφές, επικεντρώνεται περισσότερο στην ασφάλεια και στην αξιοπιστία των ήδη γνωστών τεχνολογιών ,που είναι διαθέσιμες στην αγορά και είναι δοκιμασμένες στο εμπόριο με το σκεπτικό ότι δεν είναι δυνατόν να αναγνωρίσει νομικά άγνωστης τεχνολογίας ηλεκτρονικές υπογραφές, που δεν έχει δοκιμαστεί στην πράξη και δεν έχει γίνει αποδεκτή ακόμη στην αγορά.(Κοσμάς Α Καραδημητρίου Η ηλεκτρονική Υπογραφή)

Σχετικά με το θέμα της ρύθμισης των ηλεκτρονικών υπογραφών η διεθνής και ευρωπαϊκή νομοθετική θέση ακολουθεί μια τεχνολογικά ουδέτερη τάση στο θέμα της καταλληλότητας και της ασφάλειας της τεχνολογίας που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές ,γιατί πιστεύει ότι η επιλογή της τεχνολογίας πρέπει να στηρίζεται στην διαδικασία αξιολόγησης του κινδύνου (risk assessment), που σχετίζεται με την εφαρμογή που θα χρησιμοποιηθεί στην ηλεκτρονική υπογραφή και ότι ο κίνδυνος αφορά τους τρίτους (relying parties) που καλείται να αξιολογήσουν τη δεσμευτικότητα της δήλωσης του υπογράφοντος.(www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Πιο συγκεκριμένα η Ευρωπαϊκή Οδηγία σκοπίμως αποφεύγει να υποδείξει ένα συγκεκριμένο τύπο υπογραφής γιατί επιδιώκει την ανάπτυξη νέων τεχνολογιών ενώ παράλληλα επιχειρεί να μεγιστοποιήσει τα οφέλη από την εφαρμογή της υπάρχουσας τεχνολογίας αφήνοντας έτσι ανοικτό ένα σημαντικό αριθμό ζητημάτων τεχνολογίας και διαδικασιών για να αντιμετωπισθούν μέσω της διαδικασίας της προτυποποίησης, η οποία αποτελεί συνέχεια της νομοθετικής διαδικασίας της Οδηγίας και πρόδρομο παρόμοιων ενεργειών που σχετίζονται με τη ρύθμιση της τεχνολογίας στο μέλλον, που στο εξής καθιερώνεται ο όρος συν-ρύθμιση (co-regulation)για να περιγράφει αυτή τη διαδικασία.

Έτσι στο τελικό περιεχόμενο της Οδηγίας για τις ηλεκτρονικές υπογραφές η συν-ρύθμιση διαπιστώνουμε ότι επιβλήθηκε στην πράξη και η υπηρεσία γνωστή ως European Electronic Signatures Standardization Initiative (EESSI) χρησιμοποιώντας πόρους και διαδικασίες των ευρωπαϊκών οργανισμών προτυποποίησης ασχολήθηκε με θέματα που σχετίζονται με τις ρυθμίσεις των τεχνολογικών εξελίξεων με σκοπό τον καθορισμό τεχνικών προτύπων εφαρμογής , λειτουργίας και ελέγχου των ηλεκτρονικών υπογραφών καθώς επίσης και των πολιτικών, που σχετίζονται για την εκτέλεση του έργου της προτυποποίησης των ηλεκτρονικών υπογραφών ενώ με το άρθρο 3.5 της Οδηγίας ο ευρωπαϊκός νομοθέτης παρέχει τη δυνατότητα αναγνώρισης των προτύπων μέσω της δημοσίευσης στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων.

(www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

3.Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου

Σε ευρωπαϊκό επίπεδο ο κοινοτικός νομοθέτης με την Ευρωπαϊκή Οδηγία 1999/93/ΕΚ ορίζει το γενικό πλαίσιο για τη νομική αναγνώριση των ηλεκτρονικών υπογραφών ως αντίστοιχες με τις χειρόγραφες καθώς και τη δημιουργία ενός κοινού ρυθμιστικού πλαισίου για τις χώρες .

Επιπλέον θέτει με το άρθρο 5.1 της Οδηγίας τις προϋποθέσεις που είναι απαραίτητες για τη δημιουργία ενός κοινού και ενιαίου πλαισίου ηλεκτρονικών υπογραφών που κάτω από ορισμένες προϋποθέσεις μπορούν να τύχουν αναγνώρισης μεταξύ των χωρών που ανήκουν στην Ευρωπαϊκή Ένωση με κύριες επιδιώξεις να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και την παροχή υπηρεσιών πιστοποίησης και να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς , καθώς ορισμένα ευρωπαϊκά κράτη και συγκεκριμένα η Γερμανία και η Ιταλία ήδη είχαν προχωρήσει στο θέμα αυτό με συγκεκριμένες νομοθετικές πρωτοβουλίες , που αποσκοπούσαν στη ρύθμιση των ηλεκτρονικών υπογραφών. (www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Πιο αναλυτικά η Ευρωπαϊκή Οδηγία 1999/93/ΕΚ αναγνωρίζει γενικά ως ηλεκτρονικές υπογραφές, οι οποίες μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες, όλα τα δεδομένα που βρίσκονται σε ηλεκτρονική μορφή ,τα οποία είναι συνημμένα σε ή λογικά συσχετιζόμενα με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας. (www.ebusinessforum.gr Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης Μ. Γιαννακάκη – Χ.Σιουλής).

Επίσης από την κανονιστική πλευρά, η Οδηγία διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών, που αποκαλούνται συχνά ως αναγνωρισμένες ηλεκτρονικές υπογραφές και αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές, σύμφωνα με το ισχύον δίκαιο του κάθε κράτους Μέλους. (www.ebusinessforum.gr Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης Μ. Γιαννακάκη – Χ.Σιουλής).

Σε αυτή την κατηγορία ανήκουν όλες οι προηγμένες ηλεκτρονικές υπογραφές, που βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής, που σύμφωνα με την Οδηγία πρέπει να ικανοποιούν τις εξής απαιτήσεις: να συνδέονται μονοσήμαντα με τον υπογράφοντα, να δημιουργούνται με μέσα τα οποία αυτός, που υπογράφει να έχει τη δυνατότητα να διατηρήσει υπό τον αποκλειστικό του έλεγχο και να συνδέονται με τα δεδομένα στα οποία αναφέρονται με τέτοιο τρόπο ώστε να υπάρχει η δυνατότητα εντοπισμού οποιαδήποτε αλλοίωσης στα εν λόγω δεδομένα. (www.ebusinessforum.gr Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης Μ. Γιαννακάκη – Χ.Σιουλής).

Επιπλέον ως αναγνωρισμένο πιστοποιητικό ορίζεται από την Οδηγία η ηλεκτρονική βεβαίωση ,που εκδίδεται από κάποιον Πάροχο Υπηρεσιών

Πιστοποίησης και η οποία πρέπει διακρίνεται από τα εξής χαρακτηριστικά :να συνδέει μονοσήμαντα τα δεδομένα επαλήθευσης μιας υπογραφής με ένα συγκεκριμένο φυσικό πρόσωπο, τηρώντας κάποιους βασικούς όρους .

Σύμφωνα πάλι με την παραπάνω Οδηγία ως Ασφαλής Διάταξη Δημιουργίας Υπογραφής ορίζεται το διατεταγμένο υλικό ή και λογισμικό που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού από τον υπογράφοντα και το οποίο έχει την ικανότητα να διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής βάσει συγκεκριμένων απαιτήσεων που αναγράφονται στην Οδηγία και σε συνδυασμό με τις οδηγίες της Απόφασης της 6ης Νοεμβρίου 2000 της Επιτροπής Ηλεκτρονικής Υπογραφής ορίζονται επίσης και τα ελάχιστα κριτήρια που πρέπει να πληρούν οι αρμόδιοι φορείς για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας ηλεκτρονικής υπογραφής(οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου)

Η Οδηγία επίσης ανάμεσα στα άλλα προβλέπει και τη δυνατότητα της ελεύθερης παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής ,προσδιορίζοντας ταυτόχρονα τις προϋποθέσεις λειτουργίας των φορέων ,που είναι πιστοποιημένοι να εκδίδουν αναγνωρισμένα πιστοποιητικά προς το κοινό.

Παράλληλα όμως προβλέπει και τη διαδικασία με την οποία διαπιστώνεται η συμμόρφωση των προϊόντων ηλεκτρονικών υπογραφών από σχετικούς αρμόδιους φορείς σύμφωνα με τις απαιτήσεις ασφάλειας και αξιοπιστίας, όπως αυτές ορίζονται από την Οδηγία. (οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου)

Αξίζει επίσης να σημειωθεί ότι ένας από τους βασικούς σκοπούς της Οδηγίας είναι και η ρύθμιση θεμάτων σχετικών με τη χρήση των ηλεκτρονικών υπογραφών για τη μη αποκήρυξη των συναλλαγών δηλαδή για την περίπτωση της παροχής υψηλού επιπέδου διαβεβαίωσης ότι μια πληροφορία είναι αυθεντική και δεν δύναται να αποκηρυχτεί από τον υπογράφοντα ενώ μπορεί να χρησιμοποιηθεί στην αποδεικτική διαδικασία όταν τα συμβαλλόμενα μέρη επιθυμούν να αποσυνδεθούν από μία συναλλαγή ή από τις ρήτρες που συνοδεύουν αυτή τη συναλλαγή καθώς και η ρύθμιση θεμάτων σχετικών με τις ηλεκτρονικές υπογραφές που χρησιμοποιούνται σε δημόσια ανοικτά δίκτυα όπως το Internet.

Στην Ελλάδα η πρώτη νομοθετική πρόβλεψη για ψηφιακές υπογραφές, οι οποίες ταυτίζονται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές της Οδηγίας γίνεται με το άρθρο 4 του νόμου 2672/98 όπου παρέχεται μια αρχική αλλά περιορισμένη αρχικά αναγνώρισή τους σε διαδικασίες του δημοσίου τομέα. (www.ebusinessforum.gr Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης Μ. Γιαννακάκη – Χ.Σιουλής).

Τέλος πρέπει να αναφερθεί ότι κάθε δημοκρατική κοινωνία έχει την ηθική και νομική υποχρέωση εκτός από την εφαρμογή των διεθνών, ευρωπαϊκών και

εθνικών νόμων να αγωνίζεται για την υπεράσπιση των κοινωνικά αδύναμων πολιτών και να μεριμνά ώστε ο κάθε πολίτης να απολαμβάνει εύκολη και ισότιμη πρόσβαση στις υπηρεσίες του κράτους ,όπου στην ελληνική Πολιτεία, το δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας θεσμοθετείται από το Σύνταγμα της Ελλάδος .

4.Προεδρικό διάταγμα 150/2001

Ακολουθώντας την Ευρωπαϊκή Οδηγία 1999/93/ΕΚ, το σχέδιο Προεδρικού Διατάγματος του 1999 που αποσκοπούσε στην ρύθμιση της ηλεκτρονικής υπογραφής και τη χρήση της στο Δημόσιο Τομέα, έδινε την εντύπωση αρχικά ότι υπήρχε κάποιας μορφής απόκλισης του ελληνικού από το κοινοτικό δίκαιο αφήνοντας έτσι ανοικτό το ενδεχόμενο οι ηλεκτρονικές υπογραφές που γίνονταν είτε μεταξύ των ιδιωτών είτε μεταξύ του Δημόσιου Τομέα να μην αναγνωρίζονται με τον ίδιο τρόπο.(www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Σύμφωνα με το άρθρο 1§1 του προεδρικού διατάγματος 150/2001 ο έλληνας νομοθέτης έχει πρωταρχική επιδίωξη την προσαρμογή και συμμόρφωση της ελληνικής νομοθεσίας προς τις κείμενες διατάξεις της Ευρωπαϊκής Οδηγίας 1999/93 με σκοπό να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλλει στη νομική αναγνώρισή τους, ενώ το ίδιο το Προεδρικό Διάταγμα αποτελεί πιστή μεταφορά του κειμένου της Ευρωπαϊκής Οδηγίας στο ελληνικό δίκαιο ,μια πολιτική την οποία σταδιακά ακολούθησαν και οι άλλες χώρες της Ευρωπαϊκής Ένωσης.

(προεδρικό διάταγμα 150/2001)

Στη συνέχεια το άρθρο 2§1 του προεδρικού διατάγματος 150/2001 ορίζει την ηλεκτρονική υπογραφή ως δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας και υιοθετεί την τεχνολογικά ουδέτερη προσέγγιση κατά τον ορισμό της ηλεκτρονικής υπογραφής, στοχεύοντας στο να περιληφθούν στο πεδίο εφαρμογής του νόμου τόσο οι τεχνολογικά απλές, όσο και οι πιο προηγμένες ηλεκτρονικές υπογραφές. (προεδρικό διάταγμα 150/2001)

Σύμφωνα με το άρθρο 3.2 του προεδρικού διατάγματος 150/2001 ο έλληνας νομοθέτης αναγνωρίζει χωρίς περιορισμούς την ηλεκτρονική υπογραφή και αναφέρεται επίσης και στις κατηγορίες ηλεκτρονικών υπογραφών που θέτει η Οδηγία και οι οποίες έχουν τη δυνατότητα να περιλαμβάνουν τις απλές ηλεκτρονικές υπογραφές ,που μπορεί να περιλάβουν κάθε τύπο ηλεκτρονικής υπογραφής ,όπως παραδείγματος χάρη ένα ψηφιακό αποτύπωμα μιας χειρόγραφης υπογραφής. (www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Επιπλέον το προεδρικό διάταγμα 150/2001 αναγνωρίζει τις προηγμένες ηλεκτρονικές υπογραφές οι οποίες όμως πρέπει να πληρούν τις παρακάτω προϋποθέσεις όπως: να συνδέονται μονοσήμαντα με τον υπογράφοντα ώστε να μην υπάρχει σύγχυση σχετικά με τον δικαιούχο της ηλεκτρονικής υπογραφής , να έχουν την ικανότητα να καθορίζουν ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος, κατά τρόπο ώστε τα στοιχεία που είναι εγγεγραμμένα στο ηλεκτρονικό πιστοποιητικό να είναι ακριβή και το δημόσιο

κλειδί που περιέχεται στο πιστοποιητικό να ανταποκρίνεται απόλυτα με το ιδιωτικό κλειδί που έχει στην κατοχή του ο δικαιούχος.

Επίσης σύμφωνα με την Ευρωπαϊκή Οδηγία πρέπει οι προηγμένες ηλεκτρονικές υπογραφές να δημιουργούνται με μέσα τα οποία ο υπογράφων έχει τη δυνατότητα να μπορεί να διατηρήσει κάτω από τον αποκλειστικό του έλεγχο, έτσι ώστε διασφαλίζεται ότι χρησιμοποιούνται οι ασφαλείς διατάξεις του Παραρτήματος ΙΙΙ του προεδρικού διατάγματος που σχετίζονται με τη δημιουργία του ζεύγους κλειδιών και την ασφαλή φύλαξη του ιδιωτικού κλειδιού.(Κοσμάς Καραδημητρίου Η ηλεκτρονική Υπογραφή)

Επίσης σύμφωνα πάλι με την παραπάνω Οδηγία πρέπει οι προηγμένες ηλεκτρονικές υπογραφές να συνδέονται με τα δεδομένα στα οποία επίσης διασφαλίζεται η δυνατότητα εντοπισμού οποιασδήποτε μεταγενέστερης αλλοίωσης των εν λόγω δεδομένων μέσω της χρήσης αλγορίθμων κατατεμαχισμού κατά τη διαδικασία δημιουργίας και επαλήθευσης της ηλεκτρονικής υπογραφής, καθώς έχει επίσης και τη δυνατότητα να μπορεί να αποκαλύπτει τυχόν αλλοιώσεις που επήλθαν στο αρχικό απεσταλμένο ηλεκτρονικό κείμενο.

Στη συνέχεια ο έλληνας νομοθέτης ακολουθώντας τη διατύπωση της οδηγίας 1999/93 θωρακίζει με ειδικά νομικά προνόμια μόνο την προηγμένη ηλεκτρονική υπογραφή του άρθρου 2§2 του προεδρικού διατάγματος 150/2001 όπου με ρητή πρόβλεψη του άρθρου 3§1 του προεδρικού διατάγματος 150/2001 ορίζει ότι η προηγμένη ηλεκτρονική υπογραφή επέχει θέση ιδιόχειρης υπογραφής, , μόνο όμως όταν πληροί δύο συγκεκριμένες τεχνικές προϋποθέσεις, όπως να βασίζεται σε αναγνωρισμένο πιστοποιητικό και να δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής. (Παράρτημα ΙΙ προεδρικό διάταγμα 150/2001)

Σχετικά με την πρώτη προϋπόθεση μια προηγμένη ηλεκτρονική υπογραφή για να είναι νομικά ισότιμη με την ιδιόχειρη πρέπει να βασίζεται σε αναγνωρισμένο πιστοποιητικό και το άρθρο 2§9 του προεδρικού διατάγματος 150/2001 ορίζει ότι πιστοποιητικό είναι μια ηλεκτρονική βεβαίωση, η οποία χορηγείται από τον Πάροχο Υπηρεσιών Πιστοποίησης και συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο επιβεβαιώνοντας την ταυτότητά του και αναγνωρίζει τις προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής (www.ebusinessforum.gr,Ηλεκτρονική Τραπεζική Ανδρέα Μήτρακα)

Σύμφωνα με τη διάταξη αυτή προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή είναι η ηλεκτρονική υπογραφή που διακρίνεται από τα χαρακτηριστικά να συνδέεται μονοσήμαντα με τον υπογράφοντα όπου ο όρος μονοσήμαντα έχει την έννοια ότι η κατοχή και η χρήση του ιδιωτικού κλειδιού της ηλεκτρονικής υπογραφής ανήκει σε ένα συγκεκριμένο πρόσωπο

καθώς επίσης να είναι ικανή να ταυτοποιήσει τον υπογράφοντα. (Παράρτημα ΙΙ οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου)

Αυτό σημαίνει ότι με τον όρο Ταυτοποίηση δίνεται η δυνατότητα να διαπιστώνεται ότι το ηλεκτρονικό μήνυμα που φέρει την προηγμένη ηλεκτρονική υπογραφή προήλθε πραγματικά από τον φερόμενο ως αποστολέα του και ότι έχει δημιουργηθεί με μέσα τα οποία αυτός που υπογράφει μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο.

Κατά συνέπεια αυτός που υπογράφει πρέπει να ελέγχει απόλυτα το ιδιωτικό κλειδί με το οποίο δημιουργεί την υπογραφή του και να αποκλείει την πιθανότητα παρέμβασης από τρίτα πρόσωπα για αυτό το λόγο το ιδιωτικό κλειδί αποθηκεύεται σε μια έξυπνη κάρτα και να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο έτσι ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων. (Κοσμάς Α Καραδημητρίου Η Ηλεκτρονική υπογραφή)

Σύμφωνα με την § 10 του ίδιου άρθρου ορίζεται ως αναγνωρισμένο πιστοποιητικό το πιστοποιητικό που έχει την ιδιαιτερότητα να εκδίδεται από τον Πάροχο Υπηρεσιών Πιστοποίησης ο οποίος πληροί τους όρους του προεδρικού διατάγματος 150/2001 και πρέπει να περιλαμβάνει ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, καθώς να περιλαμβάνει και τα στοιχεία αναγνώρισης του Παρόχου Υπηρεσιών Πιστοποίησης και το κράτος, στο οποίο είναι εγκατεστημένος, το όνομα του αυτού που υπογράφει ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο.

Επίσης περιγράφεται η έννοια της ηλεκτρονικής υπογραφής, τα είδη και οι εφαρμογές της και γίνεται εκτεταμένη αναφορά στην κρυπτογραφία, στην λειτουργία των υπογραφών, στις Υπηρεσίες Παρόχων πιστοποίησης ηλεκτρονικής υπογραφής, στην Υποδομή δημόσιου κλειδιού για την έκδοση διάθεση και διαχείριση των πιστοποιητικών, στην λειτουργία της ηλεκτρονικής διοίκησης με τη χρήση της ηλεκτρονικής υπογραφής στα ηλεκτρονικά έγγραφα . (Κοσμάς Α Καραδημητρίου ,Η Ηλεκτρονική υπογραφή)

Επιπλέον τονίζεται ότι το πιστοποιητικό που εκδίδεται ως αναγνωρισμένο πιστοποιητικό πρέπει να περιλαμβάνει την πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, τα δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής φυσικά κάτω από τον έλεγχο του υπογράφοντος, την ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, τον κωδικό ταυτοποίησης του πιστοποιητικού, την προηγμένη ηλεκτρονική υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που το εκδίδει και αν προκύπτουν τυχόν περιορισμοί του πεδίου χρήσης του πιστοποιητικού καθώς και τα όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί. (Κοσμάς Α Καραδημητρίου, Η Ηλεκτρονική υπογραφή)

Ακόμη οι Υπηρεσίες Παρόχων πιστοποίησης ηλεκτρονικής υπογραφής, πρέπει να αποδεικνύουν την απαραίτητη αξιοπιστία για την παροχή υπηρεσιών

πιστοποίησης, σύμφωνα με τα εκάστοτε κριτήρια, να διασφαλίζουν την παροχή ασφαλών και άμεσων υπηρεσιών καταλόγου και ανάκλησης και να διασφαλίζουν ότι η ημερομηνία και ο χρόνος έκδοσης ή ανάκλησης πιστοποιητικού μπορεί να προσδιοριστεί με ακρίβεια.

Επίσης σύμφωνα με το εθνικό δίκαιο πρέπει να έχουν τη δυνατότητα με τα κατάλληλα μέσα να επαληθεύουν την ταυτότητα του ατόμου, στο όνομα του οποίου έχει εκδοθεί αναγνωρισμένο πιστοποιητικό, ενώ θα πρέπει να απασχολείται επίσης 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 καθώς και εξοικείωση με τις κατάλληλες διαδικασίες ασφάλειας ανάλογες με αναγνωρισμένα πρότυπα.

Ακόμη πρέπει σύμφωνα πάλι με τον έλληνα νομοθέτη πρέπει να εφαρμόζουν αξιόπιστα συστήματα και προϊόντα διασφαλίζοντας με αυτόν τον τρόπο την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά, να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών, και σε περίπτωση που ένας Πάροχος Υπηρεσιών Πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων.(Κοσμάς Α Καραδημητρίου ,Η Ηλεκτρονική υπογραφή)

Επιπλέον πρέπει να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις, που καθορίζονται στην οδηγία 1999/93 κυρίως για την ανάληψη της ευθύνης ζημιών, να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό για χρονικό διάστημα τριάντα ετών, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες, να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών. (οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου)

Τέλος πριν να 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 ακριβούς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών και να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών ώστε μόνο αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις.

Έτσι με αυτή την διαδικασία ελέγχεται η γνησιότητα των πληροφοριών και είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνο 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. (Κοσμάς Α Καραδημητρίου ,Η Ηλεκτρονική υπογραφή)

Επίσης ο Έλληνας νομοθέτης, εναρμονιζόμενος με την επιλογή του κοινοτικού νομοθέτη ακολούθησε μια μικτή, υβριδική προσέγγιση στο θέμα της νομικής αναγνώρισης των ηλεκτρονικών υπογραφών όπου στο πρώτο επίπεδο της νομικής αναγνώρισης η ελληνική νομοθεσία ακολουθεί τη μαξιμαλιστική προσέγγιση και αποδίδει μόνο στις προηγμένες ηλεκτρονικές υπογραφές, που πληρούν συγκεκριμένες τεχνικές προϋποθέσεις, πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές.

Στο δεύτερο και πιο γενικό επίπεδο νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, ο νομοθέτης επιδιώκει να ενθαρρύνει την ελεύθερη ανάπτυξη της αγοράς των ηλεκτρονικών υπογραφών και να αφήσει ανεπηρέαστη την ομαλή λειτουργία τους. (Κοσμάς Α Καραδημητρίου Η Ηλεκτρονική υπογραφή)

Έτσι ακολουθεί τη μινιμαλιστική προσέγγιση, δηλαδή αναγνωρίζει νομικά όλες τις ηλεκτρονικές υπογραφές σε τεχνολογικά ουδέτερη βάση και παρέχει σε όλες, ανεξαιρέτως στοιχειώδη νομική ισχύ με αποτέλεσμα οι ηλεκτρονικές υπογραφές να μην εξισώνονται με τις ιδιόχειρες υπογραφές, γιατί δεν είναι τεχνολογικά ικανές να συνδεθούν μονοσήμαντα με τον υπογράφοντα, ούτε να τον ταυτοποιήσουν, ώστε να εμφανίζεται έλλειμμα ασφαλείας(Κοσμάς Α Καραδημητρίου Η Ηλεκτρονική υπογραφή)

Σχετικά με τη δεύτερη προϋπόθεση που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή προκειμένου να είναι νομικά ισότιμη με την ιδιόχειρη, το άρθρο 2§5 του προεδρικού διατάγματος 150/2001 ορίζει ότι διάταξη δημιουργίας υπογραφής είναι το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής όπου σύμφωνα με το Παράρτημα ΙΙΙ του προεδρικού διατάγματος, οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω συγκεκριμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν ότι τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο. (Παράρτημα ΙΙΙ προεδρικό διάταγμα 150/2001)

Αυτό σημαίνει ότι τα σχετικά κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με τους κατάλληλους αλγόριθμους δημιουργίας τυχαίων κωδικών, είτε απευθείας μέσα σε συσκευή του χρήστη, είτε από κατάλληλες κρυπτογραφικές μονάδες του Παρόχου Υπηρεσιών Πιστοποίησης, οι οποίες μεταφέρουν άμεσα τα ιδιωτικά κλειδιά που δημιουργούνται σε προσωπικές συσκευές του χρήστη γα τον οποίο προορίζονται, χωρίς να τα εκθέτουν ή να διατηρούν αντίγραφά τους με αποτέλεσμα να μην μπορούν να ενεργοποιηθούν αν δεν έχει προηγηθεί η μέθοδος επιβεβαίωσης της ταυτότητας του χρήστη.

Έτσι , αναγνωρίζεται ότι η προηγμένη ηλεκτρονική υπογραφή παρέχει υψηλό επίπεδο ασφάλειας και μπορεί να αντικαταστήσει την ιδιόχειρη

υπογραφή επιτελώντας άριστα τις λειτουργίες της όπως την αποδεικτική λειτουργία, στο βαθμό που με τη βοήθεια του αναγνωρισμένου πιστοποιητικού αποδεικνύεται ότι τα εν λόγω δεδομένα προέρχονται από τον υπογράφοντα καθώς επίσης και την λειτουργία προσδιορισμού της ταυτότητας του εκδότη αφού το κλειδί κρυπτογράφησης της προηγμένης ηλεκτρονικής υπογραφής παρέχεται από τον Πάροχο Υπηρεσιών Πιστοποίησης σε συγκεκριμένο πρόσωπο με το οποίο συνδέεται.

Επίσης η προηγμένη ηλεκτρονική υπογραφή επιτελεί άριστα και τη λειτουργία επιβεβαιώσεως του αναλλοίωτου του εγγράφου εφόσον με τη διαδικασία επαλήθευσης της προηγμένης ηλεκτρονικής υπογραφής διαπιστώνεται αν έχει αλλοιωθεί ή όχι το περιεχόμενο του ηλεκτρονικού εγγράφου και την εγγυητική λειτουργία, διότι αυτός που αποστέλλει ένα έγγραφο υπογεγραμμένο με την προηγμένη ηλεκτρονική του υπογραφή εγγυάται, ουσιαστικά, για την γνησιότητα και την ακρίβεια του περιεχομένου του εγγράφου. (Κοσμάς Α Καραδημητρίου, Η Ηλεκτρονική υπογραφή)

Στη συνέχεια τον Οκτώβριο του 2002, εκδόθηκε το προεδρικό διάταγμα. 342/02 το οποίο προσδιορίζει κάποιους όρους για την διακίνηση ψηφιακά υπογεγραμμένων μηνυμάτων του ηλεκτρονικού ταχυδρομείου μεταξύ των δημοσίων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.

Το παραπάνω προεδρικό διάταγμα καθόρισε και την ύπαρξη και λειτουργία μιας νέας υπηρεσίας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα μηχανισμών ηλεκτρονικής υπογραφής, την λειτουργία μηχανισμών εθελοντικής διαπίστευσης και διαπίστωσης της συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής όπου στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της , η ΕΕΤΤ έχει εκδώσει έναν γενικό Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής καθώς και τον ορισμό των Φορέων που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ. (Π.Δ. 342/02)

Συμπερασματικά λοιπόν διαπιστώνουμε ότι η διαφορά ανάμεσα στην απλή και στην προηγμένη ηλεκτρονική υπογραφή, η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, συνίσταται στο ότι η απλή ηλεκτρονική υπογραφή έχει τη δυνατότητα να χρησιμοποιηθεί σε όσα έγγραφα δεν απαιτείται, κατά το κοινό δίκαιο, η τήρηση τύπου, ενώ η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής μπορεί να λειτουργήσει ως υποκατάστατο της ιδιόχειρης υπογραφής και να χρησιμοποιηθεί εκεί όπου απαιτείται η τήρηση έγγραφου τύπου.

5.Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων που ιδρύθηκε το 1992 με τον Νόμο 2075 και με την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών (ΕΕΤ) και με αρμοδιότητές σχετικές με την εποπτεία της απελευθερωμένης αγοράς των τηλεπικοινωνιών, έχει όλα τα χαρακτηριστικά της Ανεξάρτητης Αρχής και με επιδιωκόμενους στόχους και προτεραιότητες να ελέγχει, και να εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και την ταχυδρομική αγορά, καθώς και οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. (www.eett.gr)

Στη συνέχεια με την ψήφιση του Νόμου 2668/98 ο έλληνας νομοθέτης θέτει το πλαίσιο οργάνωσης και λειτουργίας των ταχυδρομικών υπηρεσιών, και αναθέτει στην Εθνική Επιτροπή Τηλεπικοινωνιών αρμοδιότητες όπως την ευθύνη για την εποπτεία και ρύθμιση της αγοράς των ταχυδρομικών υπηρεσιών η οποία στο εξής μετονομάζεται σε Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, και αργότερα με την ψήφιση ενός άλλου νόμου του 2867/2000 ενισχύεται ο εποπτικός ρόλος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων και σε συνδυασμό με τον ισχύοντα Νόμο 3431/2006 ,που αναφέρεται στις ηλεκτρονικές επικοινωνίες, καθορίζεται το πλαίσιο παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Σύμφωνα με το ευρωπαϊκό δίκαιο σκοπός της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων είναι να προσδιορίζει με ακρίβεια τις αρμοδιότητές της, να διευρύνει και να αναβαθμίζει διαρκώς την Επικοινωνία, να εξασφαλίζει την πρόσβαση όλων σε μεγάλο εύρος δικτύων και υπηρεσιών, να προστατεύει τα δικαιώματα των καταναλωτών , να ενημερώνει διαρκώς τους καταναλωτές για τα δικαιώματα και τις υποχρεώσεις τους, και σύμφωνα με τις αρχές του ανταγωνισμού να συμβάλλει στην ανάπτυξη των αγορών τηλεπικοινωνιακών και ταχυδρομικών υπηρεσιών, στην εξασφάλιση της ομαλής λειτουργίας και στη διασφάλιση των συμφερόντων των χρηστών. (www.eett.gr)

Ακόμη σύμφωνα με τον έλληνα νομοθέτη η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχει τον αποκλειστικό έλεγχο της διαπίστωσης της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής όπως ορίζονται στο Παράρτημα ΙΙΙ του προεδρικού διατάγματος 150/2001 ή της ανάθεσης του έργου αυτού σε δημόσιους ή ιδιωτικούς φορείς, βάσει του άρθρου 4§5 εδάφιο α΄ του προεδρικού διατάγματος 150/2001 καθώς και της εποπτείας και έλεγχου των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.

Έχει επίσης τη δυνατότητα η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων στα πλαίσια των αρμοδιοτήτων της να επιβάλλει πρόστιμο σε Παρόχους Υπηρεσιών Πιστοποίησης που ενεργούν ως διαπιστευμένοι και να ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης.

Τέλος στις αρμοδιότητες της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων είναι και η επίλυση των διαφορών των φορέων που ασχολούνται με τις ηλεκτρονικές επικοινωνίες, με επιδιωκόμενο στόχο την εφαρμογή της νομοθεσίας που αναφέρεται στις ηλεκτρονικές επικοινωνίες, περιλαμβανομένης και της ηλεκτρονικής υπογραφής και για αυτό τον σκοπό έχουν εκδοθεί σημαντικές διοικητικές πράξεις που σχετίζονται με την ηλεκτρονική υπογραφή όπως είναι ο κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής. (www.eett.gr)

Με την Απόφαση με αριθμό 248/71 της 15ης Μαρτίου 2002 της Εθνική Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων με τίτλο '' Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής '' ρυθμίζονται ζητήματα σχετικά με την εποπτεία , την λειτουργία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, οι οποίοι εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά και παρέχουν άλλες υπηρεσίες πιστοποίησης σχετικές με την ηλεκτρονική υπογραφή.(248/71 Απόφαση της ΕΕΤΤ)

Σύμφωνα με το άρθρο 4 της παραπάνω Απόφασης προσδιορίζονται και οι δικαιούχοι αναγνωρισμένων πιστοποιητικών, οι οποίοι πρέπει να πληρούν κάποιες βασικές προϋποθέσεις όπως να ανήκουν στην κατηγορία των φυσικών προσώπων με δικαιοπρακτική ικανότητα, να γνωρίζουν τα δεδομένα δημιουργίας της ηλεκτρονικής υπογραφής ,που συνδέεται με το πιστοποιητικό, να επιμελούνται για την τήρηση των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής και του πιστοποιητικού και τέλος μέσα στις υποχρεώσεις τους πρέπει να ενημερώνουν τους Παρόχους Υπηρεσιών Πιστοποίησης σε περιπτώσεις που προκύπτει απώλεια των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής.

Στη συνέχεια του άρθρου 8 της ίδιας απόφασης ο έλληνας νομοθέτης ορίζει και το πλαίσιο των υποχρεώσεων του Παρόχου Υπηρεσιών Πιστοποίησης που μέσα στις αρμοδιότητές του είναι η ενημέρωση προς τους δικαιούχους για ζητήματα σχετικά με την πολιτική πιστοποίησης και της Δήλωσης Πρακτικής Πιστοποίησης και των τροποποιήσεων που προκύπτουν ενώ το άρθρο 10 αναφέρεται στην διαδικασία τήρησης Μητρώου Παρόχων Υπηρεσιών Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα από την Εθνική Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων.

Αξίζει δε να σημειωθεί ότι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων επειδή διακρίνεται από αδυναμία ελέγχου των Παρόχων

Υπηρεσιών Πιστοποίησης και διαχείρισης της δικής της ιεραρχίας δημοσίου κλειδιού το Μητρώο δεν βρίσκεται σε θέση να χρησιμοποιηθεί σε αυτοματοποιημένες διαδικασίες και να παρέχει ασφαλή χρήση πρωτοκόλλου επικοινωνίας στους χρήστες αλλά βρίσκεται σε μια διαδικασία κατάρτισης σχεδίου ελέγχου και διαπίστευσης σε ζητήματα σχετικά με τους παρόχους που βρίσκονται εγκατεστημένοι στην Ελλάδα ενώ παράλληλα εξετάζεται η δυνατότητα ανάπτυξης δικής της υποδομής δημοσίου κλειδιού και ιεραρχίας.

Επίσης η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων με την Απόφαση με αριθμό 295/63 με τίτλο κανονισμός ορισμού φορέων για τη διαπίστωση συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής και των ασφαλών κρυπτογραφικών μονάδων προσδιορίζει τη διαδικασία που οι εντεταλμένοι φορείς είναι σε θέση να διαπιστώνουν τη συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής και των ασφαλών κρυπτογραφικών μονάδων.

Επίσης με την ίδια απόφαση καθορίζονται και οι προϋποθέσεις των ενταλμένων φορέων ,οι οποίοι θα ελέγχουν τους ενδιαφερόμενους Παρόχους Υπηρεσιών Πιστοποίησης και οι οποίοι στη συνέχεια θα εγγράφονται σε μητρώο που τηρεί η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ενώ παράλληλα προσδιορίζονται τα κριτήρια και η διαδικασία ελέγχου για τη συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής και των ασφαλών κρυπτογραφικών μονάδων. (295/63 Απόφαση της ΕΕΤΤ)

Επιπλέον με τον κανονισμό αυτό της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων προσδιορίζονται τα κριτήρια και η διαδικασία της εθελοντικής διαπίστευσης των Παρόχων Υπηρεσιών Πιστοποίησης, όπου σύμφωνα με την Απόφαση, ο Πάροχος Υπηρεσιών Πιστοποίησης που επιθυμεί να εκμεταλλευτεί τα οφέλη της εθελοντικής διαπίστευσης έχει τη δυνατότητα να επιλέξει κάποιον εντεταλμένο φορέα, που θα διεξάγει τους απαραίτητους ελέγχους και θα διαπιστώνει τη συμμόρφωση ή μη του Παρόχου Υπηρεσιών Πιστοποίησης ως προς τις απαιτήσεις της εθελοντικής διαπίστευσης. (295/63 Απόφαση της ΕΕΤΤ)

5.1Κριτήρια Εθελοντικής διαπίστευσης

Σύμφωνα με την Απόφαση 295/65 με τίτλο«Κανονισμός για την Εθελοντική Διαπίστευση των παρόχων υπηρεσιών πιστοποίησης» (ΦΕΚ 1730/Β/24-11-03) προσδιορίζονται τα κριτήρια και η διαδικασία εθελοντικής διαπίστευσης του Παρόχου Υπηρεσιών Πιστοποίησης , ο οποίος θα πρέπει να αποδεικνύει τη συμμόρφωσή του σύμφωνα με τις απαιτήσεις του προεδρικού διατάγματος 150/2001 και της Απόφασης 248/71/2002 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων καθώς και οποιαδήποτε άλλης ρύθμισης που αφορά την έκδοση Αναγνωρισμένων Πιστοποιητικών. (ΦΕΚ 1730/Β/24-11-03)

Συγκεκριμένα τα κριτήρια που πρέπει να πληρούν οι δικαιούχοι, στους οποίους έχει χορηγηθεί πιστοποιητικό συμμόρφωσης Ασφαλών Κρυπτογραφικών Μονάδων ή Ασφαλών Διατάξεων Δημιουργίας Υπογραφής, σύμφωνα με τις διατάξεις της Απόφασης 295/64/2003 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων» είναι να μεριμνούν για την εκπλήρωση των απαιτήσεων περιβάλλοντος χώρου .

Επίσης ένα άλλο βασικό κριτήριο που πρέπει να πληρούν οι παραπάνω δικαιούχοι είναι να διασφαλίζουν τις ακόλουθες λειτουργίες όπως την παραγωγή των Δεδομένων Δημιουργίας Υπογραφής που χρησιμοποιούν για την υπογραφή των Αναγνωρισμένων Πιστοποιητικών των δικαιούχων και για την υπογραφή της πληροφορίας σχετικά με την κατάσταση των Πιστοποιητικών .

Επίσης γίνεται κατανοητό ότι η ασφάλεια των παρεχόμενων υπηρεσιών του Παρόχου Υπηρεσιών Πιστοποίησης πρέπει να έχει διαπιστωθεί από Φορέα για Εθελοντική Διαπίστευση σύμφωνα με τη διαδικασία που ορίζεται στο άρθρο 5 του Κανονισμού για την Εθελοντική Διαπίστευση. (άρθρο 5 παρ. 2 της Απόφασης 295/65 της ΕΕΤΤ)

5.2 Διαδικασία για την εθελοντική διαπίστευση ενός Παρόχου Υπηρεσιών Πιστοποίησης

Η διαδικασία για την εθελοντική διαπίστευση ενός Παρόχου Υπηρεσιών Πιστοποίησης όπως περιγράφεται στο άρθρο 6 παρ. 2 της Απόφασης 295/65 ακολουθεί κάποια συγκεκριμένα στάδια ξεκινώντας αρχικά με την αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης σε Φορέα για Εθελοντική Διαπίστευση ο οποίος προσκομίζει όλα τα απαραίτητα δικαιολογητικά μαζί και το Πιστοποιητικού Συμμόρφωσης που του εξέδωσε ο Φορέας για Εθελοντική Διαπίστευση, ο οποίος ελέγχει την ασφάλεια των παρεχόμενων υπηρεσιών του Παρόχου Υπηρεσιών Πιστοποίησης σχετικά με την καταλληλότητα των μέτρων ασφάλειας και της υλοποίησης αυτών στην πράξη. (άρθρο 6 παρ. 2 της Απόφασης 295/65)

Επίσης ο Πάροχος Υπηρεσιών Πιστοποίησης ακολουθώντας τη διαδικασία για την εθελοντική διαπίστευση υποβάλει στον Φορέα τα ακόλουθα έγγραφα όπως πιστοποιητικά συμμόρφωσης που χορηγήθηκαν από Φορέα για Προϊόντα, τα οποία πρέπει να υπάρχει αντιστοίχηση με τα προϊόντα που χρησιμοποιεί ο Πάροχος Υπηρεσιών Πιστοποίησης και στη συνέχεια πραγματοποιείται έλεγχος για να διαπιστωθεί η ισχύς των παραπάνω Πιστοποιητικών καθώς και οι απαιτήσεις του περιβάλλοντος χώρου και

εξετάζεται ο βαθμός υλοποίησή τους από τον Πάροχο Υπηρεσιών Πιστοποίησης.

Στην συνέχεια ο Πάροχος Υπηρεσιών Πιστοποίησης υποβάλει στον αρμόδιο φορέα μια έκθεση που αναφέρεται στα μέτρα ασφαλείας που σχετίζονται με την περιγραφή των εγκαταστάσεων και όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων ασφάλειας και της καταλληλότητάς τους, στον κατάλογο των προϊόντων που χρησιμοποιούνται για τη δημιουργία Προηγμένων Ηλεκτρονικών Υπογραφών καθώς και στα μέτρα ασφάλειας που σχετίζονται με την λειτουργία των παρεχόμενων υπηρεσιών, κυρίως σε καταστάσεις έκτακτης ανάγκης όπως είναι τα μέτρα προστασίας αρχείων και δεδομένων, η περιγραφή των διαδικασιών εξασφάλισης της αξιοπιστίας του απασχολούμενου προσωπικού καθώς και τα κείμενα τα οποία περιγράφουν την Πολιτική Πιστοποίησης και τη Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης. (www.eett.gr)

Στο επόμενο στάδιο ο Φορέας για Εθελοντική Διαπίστευση ελέγχει, ακόμη και με τη διαδικασία της αυτοψίας, την υλοποίηση στην πράξη των περιγραφόμενων στην Έκθεση μέτρων ασφάλειας και στην περίπτωση που διαπιστώσει ότι υπάρχει συμμόρφωση του Παρόχου Υπηρεσιών Πιστοποίησης, τότε μόνο ο Φορέας για Εθελοντική Διαπίστευση χορηγεί Πιστοποιητικό Συμμόρφωσης ενώ η διαδικασία της αξιολόγησης του Εθελοντικά Διαπιστευμένου Παρόχου Υπηρεσιών Πιστοποίησης για τη διαπίστωση της συμμόρφωσής του επαναλαμβάνεται κάθε τρία έτη.

Τέλος η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, αξιολογώντας όλα τα παραπάνω στοιχεία, εκδίδει απόφαση για την Εθελοντική Διαπίστευση του αιτούντα και εποπτεύει όλους τους διαπιστευμένους Παρόχους Υπηρεσιών Πιστοποίησης ενώ παράλληλα έχει το δικαίωμα αυτεπαγγέλτως ή μετά από καταγγελία να ζητά στοιχεία και να επιθεωρεί τους χώρους εγκατάστασης και λειτουργίας των διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης. (www.eett.gr)

5.3 Πάροχοι Υπηρεσιών Πιστοποίησης

Όταν αναφερόμαστε στον όρο Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) - Certification Services Provider ή Έμπιστη Τρίτη Οντότητα (ΕΤΟ) - Trusted Third party (TTP) ή και Δημόσια Αρχή Πιστοποίησης (Public Certification Authority) εννοούμε έναν φορέα (οργανισμό) που λειτουργεί ως μια ανεξάρτητη επιχείρηση, η οποία μπορεί και προσφέρει υπηρεσίες ασφάλειας και εμπιστοσύνης στο ηλεκτρονικό εμπόριο και γενικότερα στις ηλεκτρονικές συναλλαγές. (www.security manager)

Οι αρμοδιότητες που έχει ένας Πάροχος Υπηρεσιών Πιστοποίησης είναι να χορηγεί (εκδίδει) ψηφιακά πιστοποιητικά (ψηφιακές ή ηλεκτρονικές υπογραφές) σε μεμονωμένους χρήστες ή και σε εταιρείες και να εξασφαλίζει ότι η ψηφιακή (ηλεκτρονική) υπογραφή που χρησιμοποιεί ένας χρήστης ανήκει όντως σ' αυτόν για να αποφευχθεί η περίπτωση της πλαστογραφίας. Πρόκειται βασικά για έναν ουδέτερο οργανισμό ,που εμπνέει επιχειρηματική εμπιστοσύνη σε μια ηλεκτρονική συναλλαγή και συμμετέχει στη διαδικασία έκδοσης και πιστοποίησης των ψηφιακών υπογραφών. (www.security manager)

Οι συγκεκριμένες λειτουργίες που αφορούν έναν Πάροχο Υπηρεσιών Πιστοποίησης είναι να τηρεί αρχείο με τα δημόσια κλειδιά των πιστοποιημένων οντοτήτων, έτσι ώστε ανά πάσα στιγμή να έχει τη δυνατότητα πρόσβασης σ' αυτά ο κάθε ενδιαφερόμενος και να πιστοποιεί την ταυτότητα των χρηστών πριν τους εκδώσει την ψηφιακή υπογραφή καθώς και να τηρεί αρχείο με όλες τις ψηφιακές υπογραφές που έχουν λήξει ή που έχουν ανακληθεί ώστε να εξασφαλιστούν οι προϋποθέσεις του να μην μπορούν να χρησιμοποιηθούν μετά τη λήξη τους ή ακόμη και για περιπτώσεις κλοπής ή απώλειας ενώ το κόστος μιας τέτοιας υπηρεσίας είναι σχεδόν ανάλογο μ' αυτό μιας συνδρομής σε μια πιστωτική κάρτα. (www.security manager)
Το σημαντικότερο χαρακτηριστικό που θα πρέπει να έχει ένας Πάροχος Υπηρεσιών Πιστοποίησης είναι η αρχή της «τριτότητας» («thirdness»), όπου σύμφωνα με την αρχή θα πρέπει να υπάρχει ένας τρίτος, ουδέτερος οργανισμός που να μην συμμετέχει με κανέναν τρόπο στη ηλεκτρονική συναλλαγή και να εμπνέει απόλυτα επιχειρηματική εμπιστοσύνη στις ηλεκτρονικές συναλλαγές ενώ υπάρχει και η σχετική νομοθεσία που αναφέρεται με λεπτομέρεια στη λειτουργία των Παρόχων Υπηρεσιών Πιστοποίησης και 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, και με τον τίτλο «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής».

Σχετικά με την αναφορά του ζητήματος της ευθύνης ενός Παρόχου Υπηρεσιών Πιστοποίησης αυτό αφορά την ακρίβεια όλων των πληροφοριών (στοιχείων) που περιέχονται στα πιστοποιητικά που εκδίδει καθώς και τη διαβεβαίωση ότι ο υπογράφων είναι πράγματι ο κάτοχος του ιδιωτικού κλειδιού και τη δημόσια ανακοίνωση της ανάκλησης ή της λήξης ενός πιστοποιητικού και άλλα .

Όσο αφορά τις εταιρείες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ηλεκτρονικής υπογραφής αυτές ελέγχονται από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ,η οποία έχει την εποπτεία και τον τελικό έλεγχο όλων των Παρόχων Υπηρεσιών

Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα και έχει τη δυνατότητα να επιβάλλει πρόστιμα σ' όσους Παρόχους ενεργούν ως διαπιστευμένοι χωρίς να είναι. www.securitymanager

Σύμφωνα με την Απόφαση με αριθμό 248/71 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής" (ΦΕΚ 603/Β'/16-5- 2002) οι Πάροχοι Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής που είναι εγκατεστημένοι στην Ελλάδα είναι υποχρεωμένοι να δηλώσουν τα στοιχεία του και τις υπηρεσίες που παρέχουν και να υποβάλλουν ετήσιες εκθέσεις με αναλυτική περιγραφή των δραστηριοτήτων τους .

Επίσης στις άμεσες υποχρεώσεις τους είναι να υποβάλλουν σε ετήσιες εκθέσεις και ζητήματα που έχουν ιδιαίτερη αναφορά σε καταγγελίες ή αιτήματα δικαιούχων που τους έχουν υποβληθεί με χρονική αφετερία από το τέλος Μαρτίου 2003, για όσους εγγράφηκαν μέσα στο 2002- και με λεπτομερή περιγραφή των δραστηριοτήτων τους ,ενώ η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων είναι υποχρεωμένη να τηρεί μητρώο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, οι οποίοι και εκδίδουν πιστοποιητικά γνησιότητας ηλεκτρονικής υπογραφής ακόμη και μη αναγνωρισμένα. (ΦΕΚ 603/Β'/16-5- 2002)

Στην περίπτωση που πραγματοποιείται καταχώρηση / αλλαγή ή παύση των υπηρεσιών ενός Παρόχου στο Μητρώο της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων, καθώς και περιγραφή των υπηρεσιών πιστοποίησης που παρέχει ,ο συγκεκριμένος Πάροχος είναι υποχρεωμένος να συμπληρώσει τη Δήλωση καταχώρησης και να την αποστείλει υπογεγραμμένη και σφραγισμένη στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, ενώ σύμφωνα με τον Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής ορίζεται η καταβολή εφάπαξ ανταποδοτικών τελών για την εκάστοτε γνωστοποίηση των Παρόχων προς την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων. (www.eett.gr)

Να σημειωθεί επίσης ότι στην περίπτωση της καταχώρησης ενός Παρόχου στο Μητρώο της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων ως Παρόχου, ο οποίος εκδίδει αναγνωρισμένα πιστοποιητικά (όπως αυτά ορίζονται στο Π.Δ. 150/2001) αυτή βασίζεται μόνο στη δική του δήλωση ότι εκδίδει Αναγνωρισμένα Πιστοποιητικά ενώ μέσα στις υποχρεώσεις του είναι η τήρηση έντυπης ή και σε ηλεκτρονικής μορφής αρχείου με το σύνολο των πληροφοριών σχετικά με τα αναγνωρισμένα πιστοποιητικά που εκδίδει ή και διαχειρίζεται και ιδιαίτερα όσον αφορά στο χρόνο έκδοσης, ακύρωσης ή αναστολής του και λήξης τους και το αρχείο για κάθε αναγνωρισμένο πιστοποιητικό τηρείται από την έκδοσή του και για χρονική περίοδο τριάντα (30) ετών από τη λήξη ή την ανάκλησή του. (www.eett.gr)

Σε περίπτωση συμμόρφωσης, ο εντεταλμένος φορέας είναι σε θέση να χορηγεί πιστοποιητικό συμμόρφωσης στον Πάροχο Υπηρεσιών Πιστοποίησης, ο οποίος στη συνέχεια μπορεί να προσκομίσει το πιστοποιητικό στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και να ζητήσει τη διαπίστευσή του.

Επίσης σύμφωνα με την απόφαση επιλογής τεχνολογίας για την υλοποίηση του σχήματος εθελοντικής διαπίστευσης η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων υιοθετεί την τεχνολογική λύση της ηλεκτρονικά υπογεγραμμένης λίστας (Signed list) για την υλοποίηση του μητρώου των εθελοντικά διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης και έτσι τα στοιχεία και οι υπηρεσίες για τις οποίες έχουν διαπιστευτεί οι εθελοντικά διαπιστευμένοι Πάροχοι Υπηρεσιών Πιστοποίησης, καταχωρούνται σε μια ηλεκτρονική λίστα που διαχειρίζεται η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων.

Σχετικά τώρα με τη λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο ενώ δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, αν ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται ότι είναι. Κατά συνέπεια, 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 υλοποιείται από τον Πάροχο Υπηρεσιών Πιστοποίησης, ο οποίος πιστοποιεί την ταυτότητα του προσώπου με το δημόσιο κλειδί του.

Η οντότητα αυτή, με την έκδοση ενός πιστοποιητικού, εγγυάται ότι, σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί ενώ το πιστοποιητικό είναι ένα τυποποιημένο ηλεκτρονικό αρχείο που περιέχει κάποια προδιαγεγραμμένα πεδία όπως σειριακός αριθμός πιστοποιητικού, ημερομηνία έκδοσης και λήξης, στοιχεία του εκδότη, στοιχεία του πιστοποιούμενου, το δημόσιο κλειδί που πιστοποιείται. (www.eett.gr)

5.3.1 Υπηρεσίες Πιστοποίησης

Σχετικά με το ζήτημα της αποθήκευσης των ηλεκτρονικών μηνυμάτων ο Πάροχος Υπηρεσιών Πιστοποίησης λειτουργεί ως ένας ηλεκτρονικός συμβολαιογράφος. Αυτό σημαίνει ότι κάθε είδους ηλεκτρονικά έγγραφα που ο συναλλασσόμενος θεωρεί πολύτιμα ή δεν επιθυμεί να αμφισβητηθούν από κανέναν, μπορούν να κατατεθούν στον Πάροχο Υπηρεσιών Πιστοποίησης, ώστε να είναι δυνατή ανά πάσα στιγμή η παρουσίαση του πρωτότυπου αποθηκευμένου μηνύματος. (Κοσμάς Α Καραδημητρίου ,Η Ηλεκτρονική υπογραφή)

Οι Πάροχοι Υπηρεσιών Πιστοποίησης έχουν τη δυνατότητα να είναι ελεύθεροι στο να μπορούν να προσφέρουν υπηρεσίες πιστοποίησης χωρίς να χρειάζεται χορήγηση κρατικής άδειας και τις υπηρεσίες αυτές μπορεί να τις

προσφέρει οποιοδήποτε φυσικό ή νομικό πρόσωπο, εφόσον πληροί ορισμένες προϋποθέσεις όπως να τηρεί τις διατάξεις για την προστασία του ανταγωνισμού, για τον αθέμιτο ανταγωνισμό, για την πνευματική και βιομηχανική ιδιοκτησία και για την προστασία του καταναλωτή.

Σύμφωνα με το κοινοτικό δίκαιο του άρθρου 3§1 της οδηγίας 1999/93 τα κράτη - μέλη δεν εξαρτούν την παροχή υπηρεσιών πιστοποίησης από εκ των προτέρων έγκριση ενώ θεσπίζεται από το άρθρο 4§4 του προεδρικού διατάγματος 150/2001 η αρχή της παροχής υπηρεσιών πιστοποίησης χωρίς άδεια γιατί ο επιδιωκόμενος στόχος του προεδρικού διατάγματος 150/2001 και της οδηγίας 1999/93 είναι να καταστήσουν ευέλικτη την αγορά και να προαγάγουν τη χρήση της ηλεκτρονικής υπογραφής ως μέσου ασφαλείας των συναλλαγών χωρίς την τροχοπέδη της κρατικής γραφειοκρατίας.(προεδρικό διάταγμα 150/2001)

5.3.2 Έλεγχος των Παρόχων Υπηρεσιών Πιστοποίησης

Ο έλληνας νομοθέτης με το άρθρο 4§5 του προεδρικού διατάγματος 150/2001 παρέχει στον Πάροχο Υπηρεσιών Πιστοποίησης τη δυνατότητα εθελοντικής διαπίστευσης, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις που αφορούν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται, ύστερα από αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης από τον φορέα που προβλέπεται στην §5 του άρθρου 4 του προεδρικού διατάγματος 150/2001, δηλαδή από την ΕΕΤΤ ή από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς. (προεδρικό διάταγμα 150/2001)

Πρόκειται για ένα είδος προαιρετικού ελέγχου των Παρόχων Υπηρεσιών Πιστοποίησης, με επιδιωκόμενο στόχο την επίτευξη ενός ικανοποιητικά ασφαλούς επιπέδου παροχής υπηρεσιών πιστοποίησης ιδιαίτερα μεταξύ επαγγελματιών, οι οποίοι εξαιτίας της φύσης του επαγγέλματος, διακινούν μεγάλης σημασίας ηλεκτρονικά έγγραφα, αλλά και μεταξύ απλών καταναλωτών ή εμπόρων, όταν θεωρούν ότι απαιτείται μεγαλύτερη από τη συνήθη ασφάλεια για κάποια ηλεκτρονική συναλλαγή τους. (προεδρικό διάταγμα 150/2001)

Επίσης το προεδρικό διάταγμα 150/2001 μεταξύ άλλων προβλέπει άλλους δύο μηχανισμούς ελέγχου των Παρόχων Υπηρεσιών Πιστοποίησης, οι οποίοι είναι υποχρεωτικοί κατασταλτικοί. Σύμφωνα με το άρθρο 4§2 του προεδρικού διατάγματος 150/2001 ορίζεται ότι η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς το Παράρτημα ΙΙΙ του προεδρικού διατάγματος 150/2001 διαπιστώνεται από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ή από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς. (π προεδρικό διάταγμα 150/2001)

Δεύτερη μορφή υποχρεωτικού κατασταλτικού ελέγχου ορίζεται με το άρθρο 4§8 του προεδρικού διατάγματος 150/2001, όπου σύμφωνα με αυτό η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχει την εποπτεία και

τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, των φορέων εθελοντικής διαπίστευσης και των φορέων ελέγχου της συμμόρφωσης των ηλεκτρονικών υπογραφών προς το παράρτημα ΙΙΙ του προεδρικού διατάγματος 150/2001. (προεδρικό διάταγμα 150/2001)

Σύμφωνα πάντα με τον έλληνα νομοθέτη η ανωτέρω διάταξη θεσπίστηκε κατά εφαρμογή του άρθρου 3§3 της οδηγίας 1999/93, συστήματος που επιτρέπει την επιτήρηση των εγκατεστημένων στο έδαφός τους Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι έχουν στη δικαιοδοσία τους την έκδοση αναγνωρισμένων πιστοποιητικών για το κοινό.(κοινοτική οδηγία 1999/93)

5.3.3 Υπηρεσίες κύκλου ζωής του Πιστοποιητικού

Όπως αναφέρθηκε παραπάνω οι πάροχοι υπηρεσιών πιστοποίησης εκδίδουν τα πιστοποιητικά με στόχο τη δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημόσιου κλειδιού και του δικαιούχου του, αλλά και την οργάνωση μιας αξιόπιστης«Υποδομής Δημόσιου κλειδιού», (PKI Public Key Infrastructure) για την έκδοση, διάθεση και διαχείριση των σχετικών πιστοποιητικών.

Κατά συνέπεια, μέσα στις αρμοδιότητές τους οι Πάροχοι Υπηρεσιών Πιστοποίησης οφείλουν να προσφέρουν στους πιστοποιούμενους-συνδρομητές αλλά και στους τρίτους-χρήστες των πιστοποιητικών, μια σειρά από υπηρεσίες, που δεν περιορίζονται μόνο στην έκδοση του πιστοποιητικού, αλλά αφορούν τον λεγόμενο «κύκλο ζωής του πιστοποιητικού».

Οι υπηρεσίες αυτές που είναι υποχρεωμένοι να προσφέρουν οι Πάροχοι Υπηρεσιών Πιστοποίησης, διασφαλίζονται από τις εξής«λειτουργικές οντότητες» μέσα στα πλαίσια του Παρόχου Υπηρεσιών Πιστοποίησης όπως η Υπηρεσία εγγραφής (Registration Authority), η οποία μέσα στις αρμοδιότητές της είναι να παραλαμβάνει τις αιτήσεις και τα δικαιολογητικά για την έκδοση ενός πιστοποιητικού και είναι υπεύθυνη για τη συλλογή των πληροφοριών που αποτελούν το απαραίτητο περιεχόμενο του πιστοποιητικού και οι οποίες είναι απαραίτητες για την ταυτοποίηση του κατόχου των δεδομένων δημιουργίας με τον αιτούντα το πιστοποιητικό και στη συνέχεια τις μεταβιβάζει στην υπηρεσία έκδοσης των πιστοποιητικών.

Επίσης στις λειτουργικές οντότητες ανήκει και η Υπηρεσία έκδοσης πιστοποιητικών (Certification Authority) που εκδίδει το πιστοποιητικό σύμφωνα με την «Δήλωση Πρακτικής Πιστοποίησης» και μέσα στις άμεσες υποχρεώσεις της είναι να παρέχει πληροφορίες για την έκδοση αυτή στις άλλες οντότητες, ενώ παράλληλα έχει την υποχρέωση που έχει και σε κάθε περίπτωση ανανέωσης, παύσης ή ανάκλησης του πιστοποιητικού, να ενημερώνει την Υπηρεσία Δημοσίευσης και Διανομής (Dissemination Service)

που 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 προσβάσιμο και προσιτό σε κάθε ενδιαφερόμενο. (www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή Γιαννακάκη Μαρία)

Επιπλέον οι Πάροχοι Υπηρεσιών Πιστοποίησης προσφέρουν και την Υπηρεσία Διαχείρισης και δημοσίευσης ανάκλησης (Revocation Management and Status Service) ,η οποία έχει την διαχείριση του κατάλογου με τα υπό έκδοση ή εκδοθέντα πιστοποιητικά και δέχεται και ελέγχει αιτήματα ανάκλησης ή παύσης των πιστοποιητικών και προβαίνει άμεσα στην έγκαιρη ενημέρωση της «Λίστας Ανακληθέντων Πιστοποιητικών» ενώ στις άμεσες αρμοδιότητες της είναι ο επακριβής προσδιορισμός της ημερομηνίας και ο χρόνος της ανάκλησης του.

Επίσης, ένας Πάροχος Υπηρεσιών Πιστοποίησης χωρίς να είναι υποχρεωτικό μπορεί να παρέχει και τις υπηρεσίες Υπηρεσίες χρονοσήμανσης (Time stamping Authority) των εγγράφων, μετά βέβαια από σχετική αίτηση των συνδρομητών καθώς και τις Υπηρεσίες προμήθειας συσκευών δημιουργίας υπογραφής (DeviceProvision Service) υπηρεσίες οι οποίες παρέχουν στο συνδρομητή το ιδιωτικό του κλειδί, συνήθως με τη μορφή μιας «έξυπνης κάρτας».(www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή Γιαννακάκη Μαρία)

Στην περίπτωση τώρα που ένας Πάροχος Υπηρεσιών Πιστοποίησης παρέχει υπηρεσίες προμήθειας συσκευών δημιουργίας υπογραφής και εκδίδει αναγνωρισμένα πιστοποιητικά, πρέπει να εγγυηθεί ότι τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά και ότι οι παραπάνω υπηρεσίες μπορούν να παρέχονται άμεσα από τον ίδιο τον εκδότη των πιστοποιητικών ή από εξουσιοδοτημένους συνεργάτες του(outsourcing).

Εξετάζοντας την περίπτωση αυτή διαπιστώνουμε ότι ο εκδότης των πιστοποιητικών παραμένει αποκλειστικά υπεύθυνος έναντι των δικαιούχων πιστοποιητικών ή τρίτων για πράξεις ή παραλείψεις των αναδόχων του και ότι έχει τη δυνατότητα να στραφεί κατά των εξουσιοδοτημένων συνεργατών του, σύμφωνα με τους προβλεπόμενους όρους του συμβολαίου που έχουν συνάψει και οι οποίοι θα πρέπει να τηρούνται και να εφαρμόζονται και από τις δύο πλευρές. (www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή Γιαννακάκη Μαρία)

Τέλος οι Πάροχοι Υπηρεσιών Πιστοποίησης έχουν την υποχρέωση να ενημερώσουν τους συμβαλλόμενους, πριν από τη σύναψη της σύμβασης, για την πρακτική που ακολουθείται για την έκδοση των πιστοποιητικών, που εκτός από τους όρους που περιέχονται στη σύμβαση (σύμβαση προσχώρησης

με προ διατυπωμένους Γενικούς Όρους Συναλλαγών) οι Πάροχοι Υπηρεσιών Πιστοποίησης εκδίδουν Δήλωση Πρακτικής Πιστοποίησης (Certification Practice Statement) μέσα στην οποία περιγράφεται αναλυτικά η πρακτική που ακολουθείται για την έκδοση, διάθεση και διαχείριση των πιστοποιητικών.

Το έγγραφο αυτό ενσωματώνεται στη σύμβαση με παραπομπή (incorporation par reference) και αναλύει κυρίως: τις παρεχόμενες υπηρεσίες πιστοποίησης, την υλικοτεχνική υποδομή και τα χρησιμοποιούμενα πρότυπα, τις διαδικασίες ανάκλησης ενός πιστοποιητικού ή παύσης των εργασιών του ΠΥΠ ενώ παράλληλα περιλαμβάνει και θέματα ευθύνης και υποχρεώσεων του Παρόχου Υπηρεσιών Πιστοποίησης καθώς και την ασφαλιστική κάλυψη της ζημίας σε περιπτώσεις ευθύνης του. (www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή Γιαννακάκη Μαρία)

5.3.4 Ευθύνη των Παρόχων Υπηρεσιών Πιστοποίησης

Σχετικά με το θέμα της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης για τα μη αναγνωρισμένα πιστοποιητικά αυτό κρίνεται με τις γενικές διατάξεις περί ευθύνης όπου σύμφωνα με το άρθρο 6 του προεδρικού διατάγματος 150/2001 ρυθμίζεται το ζήτημα της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης όπου μια από τις περιπτώσεις που προκύπτει ευθύνης είναι όταν ο Πάροχος Υπηρεσιών Πιστοποίησης εκδίδει ελαττωματικό πιστοποιητικό γνησιότητας μιας ηλεκτρονικής υπογραφής, στο οποίο βασίζεται ο αντισυμβαλλόμενος κατά την ηλεκτρονική συναλλαγή του με τον υπογράφοντα.(προεδρικό διάταγμα 150/2001)

Βέβαια οι πιο συνηθισμένες περιπτώσεις ελαττωματικού πιστοποιητικού και ευθύνης του Παρόχου Υπηρεσιών Πιστοποίησης είναι όταν ο Πάροχος Υπηρεσιών Πιστοποίησης δεν έχει επαρκείς αποδείξεις σχετικά με την ταυτότητα του κατόχου της ηλεκτρονικής υπογραφής, με αποτέλεσμα να εκδίδει ελαττωματικά πιστοποιητικά γνησιότητας της υπογραφής και όταν η κρυπτογραφική τεχνολογία που χρησιμοποιεί ο Πάροχος Υπηρεσιών Πιστοποίησης για να συνδέσει τον κάτοχο της ηλεκτρονικής υπογραφής με το ιδιωτικό και το δημόσιο κλειδί του, καθώς και με το δημόσιο κλειδί του Παρόχου Υπηρεσιών Πιστοποίησης, είναι ελαττωματική, τότε έχει ως αποτέλεσμα να επιτρέπει τη δημιουργία πλαστών πιστοποιητικών γνησιότητας ηλεκτρονικής υπογραφής ή πλαστών δημοσίων κλειδιών.

Επίσης στις περιπτώσεις ελαττωματικού πιστοποιητικού είναι όταν ο Πάροχος Υπηρεσιών Πιστοποίησης δεν τηρεί αρχεία ανάκλησης ή λήξης πιστοποιητικών γνησιότητας ηλεκτρονικής υπογραφής σύμφωνα με το νόμο, με αποτέλεσμα να είναι αδύνατη η επίκληση ενός πιστοποιητικού σε νομικές διαδικασίες, λόγω του κινδύνου ακυρότητάς του και όταν ο Πάροχος

Υπηρεσιών Πιστοποίησης απασχολεί προσωπικό που δεν έχει την απαραίτητη τεχνογνωσία ή που προβαίνει σε παράνομες ενέργειες, όπως σε δημιουργία αντιγράφων ιδιωτικών κλειδιών, με αποτέλεσμα το πιστοποιητικό γνησιότητας ηλεκτρονικής υπογραφής που εκδίδεται να είναι αναξιόπιστο. (Κοσμάς Α Καραδημητρίου , Η ηλεκτρονική Υπογραφή)

Όπως αναφέρθηκε παραπάνω οι §§1 και 3 του άρθρου 6 του προεδρικού διατάγματος 150/2001, ακολουθώντας πιστά τη διατύπωση του άρθρου 6§ 1 της οδηγίας 1999/93 που όρισε ο κοινοτικός νομοθέτης, ρυθμίζουν την ευθύνη των Παρόχων Υπηρεσιών Πιστοποίησης από την έκδοση αναγνωρισμένου πιστοποιητικού καθιερώνοντας ένα σύστημα νόθου αντικειμενικής ευθύνης. (Προεδρικό Διάταγμα 150/2001)

Πιο αναλυτικά η §1 ορίζει ότι ο Πάροχος Υπηρεσιών Πιστοποίησης, διαπιστευμένος ή μη, που εκδίδει αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυάται για την ακρίβεια τέτοιου πιστοποιητικού ευθύνεται έναντι οποιοδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημία που προκλήθηκε σε βάρος του, επειδή το πρόσωπο αυτό που εύλογα βασίστηκε στο πιστοποιητικό, όσον αφορά 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. (Προεδρικό Διάταγμα 150/2001)

Επίσης υπάρχουν διάφοροι λόγοι για τους οποίους ο Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να ανακαλέσει ένα πιστοποιητικό όπως στην περίπτωση που το ιδιωτικό κλειδί του ιδιοκτήτη της υπογραφής έχει χαθεί ή κλαπεί, στην περίπτωση που ο ιδιοκτήτης της υπογραφής δεν επιθυμεί πλέον να τη χρησιμοποιεί, στην περίπτωση επίσης που έχει καταστραφεί το φυσικό μέσο αποθήκευσης της ηλεκτρονικής υπογραφής και στην περίπτωση που ο ιδιοκτήτης της υπογραφής δεν συμμορφώνεται με τους όρους της σύμβασης που έχει συνάψει με τον Πάροχο Υπηρεσιών Πιστοποίησης .

Ακόμη ο Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να ανακαλέσει ένα πιστοποιητικό αν το πιστοποιητικό εκδόθηκε με λανθασμένα στοιχεία και προκειμένου να επιτυγχάνεται η μέγιστη δυνατή ασφάλεια των συναλλαγών, ο Πάροχος Υπηρεσιών Πιστοποίησης πρέπει να υπογράφει ηλεκτρονικά τη λίστα των ανακληθέντων πιστοποιητικών, να τη προστατεύει από ηλεκτρονικούς εισβολείς και να την ενημερώνει διαρκώς. (Κοσμάς Α Καραδημητρίου , Η ηλεκτρονική Υπογραφή)

Η § 2 του άρθρου 6 του προεδρικού διατάγματος 150/2001 ορίζει, σε αρμονία με την § 2 του άρθρου 6 της οδηγίας 1999/93, ότι ο Πάροχος Υπηρεσιών Πιστοποίησης ευθύνεται αν παραλείψει να καταγράψει την ανάκληση του αναγνωρισμένου πιστοποιητικού, ενώ στη συμπληρωματική της παραπάνω διάταξης που είναι η § 3 του άρθρου 6, ορίζεται ότι ο Πάροχος Υπηρεσιών Πιστοποίησης δεν ευθύνεται, αν αποδείξει ότι δεν τον βαραίνει πταίσμα με αποτέλεσμα και στην περίπτωση αυτή να θεσπίζεται

νόθος αντικειμενική ευθύνη για τον Πάροχο Υπηρεσιών Πιστοποίησης. (Προεδρικό Διάταγμα 150/2001)

Επίσης στις παραγράφους 4 και 5 του άρθρου 6 του προεδρικού διατάγματος 150/2001 παρέχεται η δυνατότητα σε κάθε Πάροχο Υπηρεσιών Πιστοποίησης να περιορίζει εκούσια την ευθύνη του. Πιο συγκεκριμένα η παράγραφος 4 δίνει το δικαίωμα στους Παρόχους Υπηρεσιών Πιστοποίησης να αναγράφουν επάνω στο αναγνωρισμένο πιστοποιητικό περιορισμούς στη χρήση του, υπό την προϋπόθεση ότι οι περιορισμοί μπορεί να είναι αναγνωρίσιμοι από οποιονδήποτε τρίτο. (Προεδρικό Διάταγμα 150/2001)

Επιπλέον η παράγραφος 5 δίνει στον Πάροχο Υπηρεσιών Πιστοποίησης το δικαίωμα να θέτει όρια για το ύψος των συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί το αναγνωρισμένο πιστοποιητικό που παρέχει, με την προϋπόθεση κα πάλι τα όρια αυτά είναι αναγνωρίσιμα από οποιοδήποτε τρίτο και ο Πάροχος Υπηρεσιών Πιστοποίησης δεν θα ευθύνεται για τη ζημία που προκαλείται εξαιτίας της κάλυψη της ευθύνης του Παρόχου Υπηρεσιών Πιστοποίησης. (Προεδρικό Διάταγμα 150/2001)

Ζήτημα σχετικό με τα παραπάνω αποτελεί η απουσία διάταξης τόσο στο άρθρο 6 του προεδρικού διατάγματος 150/2001 όσο και στο άρθρο 6 της οδηγίας 1999/93, η οποία να περιορίζει τη συνολική ευθύνη του Παρόχου Υπηρεσιών Πιστοποίησης για το αναγνωρισμένο πιστοποιητικό, που εκδίδει ενώ ούτε στην οδηγία 1999/93, ούτε στο προεδρικό διάταγμα 150/2001 προβλέπεται ρητά ευθύνη του Παρόχου Υπηρεσιών Πιστοποίησης, όταν δεν τηρεί κατάλογο των πιστοποιητικών που έχει εκδώσει. (προεδρικό διάταγμα 150/2001 και κοινοτική οδηγία 1999/93)

5.3.5 Μέθοδοι φερεγγυότητας του Παρόχου Υπηρεσιών Πιστοποίησης

Σχετικά με την πιστοποίηση της φερεγγυότητας του Παρόχου Υπηρεσιών Πιστοποίησης κατά την έκδοση πιστοποιητικών γνησιότητας εφαρμόζονται παγκοσμίως δύο μέθοδοι για να εξασφαλίζονται η φερεγγυότητα ενός Παρόχου Υπηρεσιών Πιστοποίησης.

Η πρώτη μέθοδος έχει σχέση με την θέσπιση μιας << Κορυφαίας Αρχής Πιστοποίησης>> και βασίζεται στην πιστοποίηση της φερεγγυότητας ενός Παρόχου Υπηρεσιών Πιστοποίησης από ένα υψηλότερο ιεραρχικά ανωτέρου επιπέδου Πάροχο Υπηρεσιών Πιστοποίησης, ο οποίος με τη σειρά του μπορεί και αυτός να ελέγχεται και να μπαίνει στη διαδικασία της πιστοποίησης από έναν ακόμη ανώτερο Πάροχο Υπηρεσιών Πιστοποίησης.

Έτσι κατά αυτόν τον τρόπο δημιουργείται μια ιεραρχία, μια αλυσίδα πιστοποιήσεων, η οποία μπορεί να συνεχίζεται μέχρι ένα ορισμένο σημείο στο οποίο βρίσκεται ο τελικός ανώτατος Πάροχος Υπηρεσιών Πιστοποίησης. Στην περίπτωση που ο συναλλασσόμενος αμφιβάλλει για την αξιοπιστία ενός Παρόχου Υπηρεσιών Πιστοποίησης και αυτός ο Πάροχος Υπηρεσιών

Πιστοποίησης έχει δημιουργήσει μια ιεραρχικά σχέση εμπιστοσύνης με έναν άλλο Πάροχο Υπηρεσιών Πιστοποίησης, τον οποίο ο συναλλασσόμενος γνωρίζει και εμπιστεύεται, τότε ο τελευταίος έχει τη δυνατότητα να λάβει πιστοποιητικό γνησιότητας ηλεκτρονικής υπογραφής από τον δεύτερο Πάροχο Υπηρεσιών Πιστοποίησης. (Κοσμάς Α Καραδημητρίου , Η ηλεκτρονική Υπογραφή)

Στην περίπτωση όμως που ο συναλλασσόμενος δεν εμπιστεύεται ούτε τον δεύτερο Πάροχο Υπηρεσιών Πιστοποίησης, μπορεί να ζητήσει πιστοποιητικό από έναν τρίτο Πάροχο Υπηρεσιών Πιστοποίησης. Αυτό δείχνει ότι κάθε πιστοποιητικό περιέχει μέσα του τη λεγόμενη αλυσίδα εμπιστοσύνης, δηλαδή μια σειρά πιστοποιητικών , καθένα από τα οποία εγγυάται την αυθεντικότητα του προηγουμένου.

Με τη μέθοδο αυτή , είναι πιθανό ένας Πάροχος Υπηρεσιών Πιστοποίησης να μην καλύπτεται πλήρως από μια αλυσίδα εμπιστοσύνης, με αποτέλεσμα να γίνεται αναξιόπιστος. Γι αυτό το λόγο ακολουθείται συχνά η δεύτερη μέθοδος πιστοποίησης της φερεγγυότητας ενός Παρόχου Υπηρεσιών Πιστοποίησης, δηλαδή η μέθοδος της λίστας όπου σύμφωνα με αυτή η κρατική μηχανή ελέγχει όσους Παρόχους Υπηρεσιών Πιστοποίησης επιθυμούν να λάβουν κρατική πιστοποίηση και δημιουργεί έτσι μια λίστα, έναν κατάλογο ελεγμένων Παρόχων Υπηρεσιών Πιστοποίησης, που προτείνει στο συναλλακτικό κοινό. (Κοσμάς Α Καραδημητρίου , Η ηλεκτρονική Υπογραφή)

5.3.6 Χρονοσήμανση

Τέλος η Χρονοσήμανση είναι μια υπηρεσία με την οποία ο Πάροχος Υπηρεσιών Πιστοποίησης θέτει στο έγγραφο ηλεκτρονική σφραγίδα, η οποία είναι αδύνατο να αλλοιωθεί και φανερώνει με ακρίβεια την ημερομηνία και ώρα αποστολής και λήψης ενός ηλεκτρονικά υπογεγραμμένου εγγράφου στο πλαίσιο μιας εμπορικής και όχι μόνο συναλλαγής και είναι πολύτιμη σε περιπτώσεις δικαστικής διαμάχης μεταξύ των συναλλασσόμενων. (www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή Γιαννακάκη Μαρία)

6.ΕΝΝΟΙΑ, ΕΙΔΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

6.1Εισαγωγή

Η υπογραφή όπως γνωρίζουμε όλοι είναι ένα τυποποιημένο σενάριο που συνδέεται με ένα πρόσωπο και μπορεί να συγκριθεί με σφραγίδα .Όταν χρησιμοποιείται στο εμπόριο και στο δίκαιο, η υπογραφή σε ένα έγγραφο είναι μια ένδειξη ότι το πρόσωπο εγκρίνει τις προθέσεις που καταγράφονται στο έγγραφο ενώ μια ηλεκτρονική υπογραφή είναι οποιοδήποτε ηλεκτρονικό μέσο που υποδεικνύει ότι ένα άτομο υιοθετεί το περιεχόμενο του ηλεκτρονικού μηνύματος.

6.2 Ορισμός

Οι ΗΠΑ για τους σκοπούς της νομοθεσίας τους ,ορίζουν την ηλεκτρονική υπογραφή ως "ηλεκτρονικό ήχο, το σύμβολο, ή τη διαδικασία, που συνδέονται με ή λογικά συσχετιζόμενη σύμβαση ή άλλη και μπορεί να καταγράφει και να εκτελεσθεί ή εγκριθεί από ένα πρόσωπο με την πρόθεση να υπογράψει την εγγραφή. Επίσης σύμφωνα με την Αμερικάνικη Νομοθεσία μπορεί η ηλεκτρονική υπογραφή να είναι μια ηλεκτρονική διαβίβαση του εγγράφου που φέρει την υπογραφή, όπως στην περίπτωση των τηλεομοιοτυπικών διαβιβάσεων, ή μπορεί να είναι κωδικοποιημένο μήνυμα, όπως η τηλεγραφία χρησιμοποιώντας τον κώδικα Μορς .

Η έννοια της ηλεκτρονικής υπογραφής δεν είναι καινούργια γιατί σύμφωνα με το εθιμικό δίκαιο έχουν αναγνωριστεί υπογραφές τηλεγραφημάτων ήδη από τα μέσα του 19ου αιώνα και με φαξ υπογραφές από το 1980.

Το 1861 πολύ πριν από το Αμερικανικό Εμφύλιο Πόλεμο βλέπουμε να χρησιμοποιείται ο κώδικας Μορς για την αποστολή μηνυμάτων με ηλεκτρονικά μέσα από την ενσύρματη τηλεγραφία όπου μερικά από αυτά τα μηνύματα - συμφωνίες με τους όρους που περιελάμβαναν προορίζονταν ως εκτελεστές συμβάσεις .

Αργότερα στη δεκαετία του 1980,διαπιστώνουμε ότι πολλές εταιρείες, ακόμη και μερικά άτομα άρχισαν να χρησιμοποιούν τις συσκευές φαξ για υψηλής προτεραιότητας ή ευαίσθητες στον παράγοντα χρόνο παράδοσης εγγράφων, που στην περίπτωση αυτή το πρωτότυπο της υπογραφής του αρχικού εγγράφου ήταν σε χαρτί αλλά η εικόνα της υπογραφής και της μετάδοσης της ήταν ηλεκτρονική.

Στη συνέχεια βλέπουμε τα δικαστήρια σε διάφορες χώρες έχουν αποφασίσει ότι οι ηλεκτρονικές υπογραφές μπορούν να περιλαμβάνουν συμφωνίες που γίνονται με ηλεκτρονικό ταχυδρομείο, που εισέρχονται σε προσωπικό αριθμό

αναγνώρισης (PIN) σε μια τράπεζα ATM , την υπογραφή μιας ή δελτίο χρέωσης πιστωτικών με μια ψηφιακή συσκευή μαξιλάρι στυλό (αίτηση του δισκίου γραφικών τεχνολογίας) σε ένα σημείο πώλησης , η εγκατάσταση λογισμικού με clickwrap λογισμικό άδεια χρήσης για το πακέτο, και την υπογραφή ηλεκτρονικών εγγράφων στο διαδίκτυο.

Μια πρώτη συμφωνία που υπογράφεται ηλεκτρονικά από δύο κυρίαρχα έθνη ήταν ένα κοινό ανακοινωθέν ,που αναγνώριζε την αυξανόμενη σημασία της προώθησης του ηλεκτρονικού εμπορίου, η οποία υπογράφηκε το 1998 από τις Ηνωμένες Πολιτείες και την Ιρλανδία.http://en.wikipedia.org/wiki/Electronic_signature

6.3 Μορφές- χαρακτηριστικά

Ένα από τα χαρακτηριστικά της «ηλεκτρονικής υπογραφής» είναι να είναι τεχνολογικά ουδέτερη και γι αυτό το λόγο υπάρχουν ηλεκτρονικές υπογραφές σε ποικίλες μορφές. Στην καθημερινή μας ζωή , υπάρχει βέβαια ένας μεγάλος αριθμός των ανθρώπων που μπορούν να χρησιμοποιούν ηλεκτρονικές υπογραφές χωρίς οι ίδιοι να το γνωρίζουν όπως για παράδειγμα, ένα "Αποδέχομαι" κουμπί που χρησιμοποιείται κατά την αγορά αγαθών ή υπηρεσιών on-line, ένας αριθμός PIN όλα αυτά αποτελούν μορφές της ηλεκτρονικής υπογραφής. (http://www.out-law.com/page-443)

Πιο συγκεκριμένα όμως ,όταν αναφερόμαστε γενικά στην έννοια της υπογραφής εννοούμε την χειρόγραφη αποτύπωση από ένα φυσικό πρόσωπο του ονοματεπωνύμου του και δήλωση της επιθυμίας του υπογράφοντος και της πρόθεσής του να δεσμευτεί από το περιεχόμενο του υπογεγραμμένου εγγράφου το οποίο και αποτελεί ένα ιδιαίτερης σημασίας αποδεικτικό μέσο σε περίπτωση δικαστικής διένεξης.

Μέσα στα χαρακτηριστικά της ιδιόχειρης υπογραφής είναι ότι εξασφαλίζει την εξατομίκευση του συντάκτη του εγγράφου, γιατί σε κάθε πρόσωπο αντιστοιχεί ένας μοναδικός και προσωπικός γραφικός χαρακτήρας, με αποτέλεσμα να γίνεται δύσκολη η απομίμηση της υπογραφής από τρίτα πρόσωπα και διευκολύνεται έτσι ο έλεγχος της γνησιότητας με βάση ατομικά δείγματα υπογραφής.

Επίσης ο έλληνας νομοθέτης θεωρεί την ιδιόχειρη υπογραφή ως μέσο πιστοποίησης της ταυτότητας ενός εγγράφου, όταν εξαρτάται το κύρος της δικαιοπραξίας που συνάπτεται με ιδιωτικό ή δημόσιο έγγραφο από το αν συνοδεύεται από την ιδιόχειρη υπογραφή του προσώπου, που δεσμεύεται με τη σύναψη της παραπάνω δικαιοπραξίας. (Κοσμάς Α Καραδημητρίου , Η ηλεκτρονική Υπογραφή)

Η υπογραφή πρέπει να μπαίνει πάντα στο τέλος του εγγράφου και αρκεί να περιέχει το επώνυμο του εκδότη, καθώς το κύριο όνομα δεν είναι απαραίτητο. Μεγάλη σημασία όμως για την υπογραφή έχει η έννοια του

ιδιοχείρου, στοιχείο που συμβάλλει στην εξασφάλιση της γνησιότητας του εγγράφου και στην πιστοποίηση της ταυτότητας του εκδότη. Η ανάγκη βέβαια των ηλεκτρονικών συναλλαγών κατέστησε αμέσως εμφανή την ανάγκη χρήσης μιας υπογραφής ανάλογης με την ιδιόχειρη, η οποία θα μπορούσε να χρησιμοποιηθεί σε ηλεκτρονικό περιβάλλον, δηλαδή στο διαδίκτυο ή σε συναλλαγές με ηλεκτρονικά μηχανήματα.

Με τον όρο λοιπόν ηλεκτρονική υπογραφή εννοούμε<< δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας>> και μπορεί να είναι ένα οποιοδήποτε ηλεκτρονικό ανάλογο μιας ιδιόγραφης υπογραφής ή με άλλα λόγια, ένα οποιοδήποτε ψηφιακό προσδιοριστικό που επικυρώνει μια ηλεκτρονική συναλλαγή.

Μια πρώτη εφαρμογή και χρήση της υπογραφής που βασίζεται στην εκ προτέρων γνώση κάποιου κωδικού έχει γίνει γνωστή σε όλους μας από τη χρήση του PIN που χρησιμοποιούμε στις τραπεζικές κάρτες που χρησιμεύουν για την ανάληψη ή κατάθεση χρηματικών ποσών στα μηχανήματα αυτόματης ανάληψης ΑΤΜ ,η οποία αποτελεί μια απλή μορφή ηλεκτρονικής υπογραφής γιατί στερείται μοναδικότητας και προσωπικού χαρακτήρα, ενώ απαιτεί από τα μέρη να έχουν μια προϋπάρχουσα μεταξύ τους σχέση, με αποτέλεσμα ο κωδικός να μην μπορεί να κλαπεί ή να υποστεί τέλεια αντιγραφή και να δύναται να χρησιμοποιηθεί από άλλον χρήστη.

Επίσης η λειτουργία της ηλεκτρονικής υπογραφής στηρίζεται στη συμμετρική ή ασύμμετρη κρυπτογραφία όπου ο όρος << κρυπτογραφία σημαίνει μια μέθοδο κωδικοποίησης του περιεχομένου του διαβιβαζόμενου μηνύματος σύμφωνα με προκαθορισμένο μυστικό κώδικα.

Βέβαια υπάρχουν πολλοί τρόποι, περισσότερο ή λιγότερο ασφαλείς για να υπογράψει κανείς ηλεκτρονικά και να δείξει την πρόθεσή του να δεσμευτεί από την υπογραφή του και από το περιεχόμενο του εγγράφου ή ακόμη να επιβεβαιώσει την ταυτότητά του.

Μια από τις περιπτώσεις ηλεκτρονικών υπογραφών που δεν διαθέτουν τις ιδιότητες μιας ασφαλούς ηλεκτρονικής επικοινωνίας είναι η απλή ηλεκτρονική αναφορά του ονόματος του συγγραφέα στο τέλος ενός ηλεκτρονικού εγγράφου, η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση που έχει οριστεί και χρησιμοποιηθεί από τον ίδιο τον αποστολέα ενός e- mail.

Αντίθετα περιπτώσεις αρκετά ασφαλών ηλεκτρονικών υπογραφών, που πληρούν μερικές ή όλες τις ιδιότητες μιας ασφαλούς ηλεκτρονικής επικοινωνίας είναι πρώτον όταν η υπογραφή βασίζεται στην εκ προτέρων γνώση κάποιου κωδικού, όπως μια λέξη – κλειδί ή ένας μυστικός αριθμός PIN, δεύτερον όταν η υπογραφή στηρίζεται στη συμμετρική ή ασύμμετρη

κρυπτογραφία και τέλος όταν η υπογραφή βασίζεται σε βιομετρικό σύστημα πιστοποίησης της ταυτότητας. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

7.ΚΡΥΠΤΟΓΡΑΦΙΑ

7.1Εισαγωγή

Κάνοντας μια αναδρομή στο παρελθόν διαπιστώνουμε ότι τις ρίζες της κρυπτογραφίας τις συναντάμε πολύ πριν το 2000 π.χ ,όπου το ιερατείο των αρχαίων Αιγυπτίων χρησιμοποιούσε τα λεγόμενα ιερογλυφικά για να κρυπρογραφήσει ιερογλυφικά που βρίσκονταν σε κατακόμβες. Επίσης μεθόδους κρυπτογράφησης συναντάμε και στους πολιτισμούς που αναπτύχθηκαν στην περιοχή της Μεσοποταμίας περίπου το 1500 π.χ. όπου βασικό χαρακτηριστικό της εποχής αυτής για την κρυπτογραφία ήταν η αντικατάσταση γραμμάτων κυρίως από μονοαλφαβητικούς αλγορίθμους όπου η πλειοψηφία των αλγορίθμων βασιζόταν στη δημιουργικότητα και τη φαντασία των κατασκευαστών τους. (Κ.Πατσάκης – Ε. Φούντας ,Κρυπτογραφία και Εφαρμογές)

Βέβαια το πρώτο κρυπτογραφημένο κείμενο χρονολογείται από την εποχή του 1500 π.Χ στη Βαβυλώνα, ενώ στην αρχαία Ελλάδα εκείνοι που εμφανίζονται να υιοθετούν πρώτοι και με επιτυχία την τέχνη της κρυπτογράφησης είναι οι Σπαρτιάτες .Κατά τη ρωμαϊκή εποχή επίσης συναντάμε την περίφημη τεχνική κρυπτογραφίας που εφαρμόστηκε κυρίως στην εποχή του Ιουλίου Καίσαρα, με κύριο χαρακτηριστικό την αντικατάσταση και τη μετάθεση των γραμμάτων των λέξεων ενώ εκτεταμένη χρήση της κρυπτογραφίας διαπιστώνουμε στα νεότερα χρόνια κυρίως στη διάρκεια το Β΄ Παγκοσμίου Πολέμου για να φτάνουν στον προορισμό τους τα στρατιωτικά μηνύματα με τη μεγαλύτερη ασφάλεια.

Αργότερα η ανακάλυψη της επιστήμης της κρυπτανάλυσης με τη βοήθεια των στατιστικών της γλώσσας θα οδηγήσει στην δημιουργία νέων αλγορίθμων, των λεγόμενων πολυαλφαβητικών με πρώτο τον Yakub ibn Ishaq al- Sabah al- Kindi, έναν φιλόσοφο των Αράβων του 9^{ο} αιώνα μ.χ ο οποίος θεωρείται και ο πρώτος ο οποίος συνέλαβε ότι οι διαφοροποιήσεις στις συχνότητες εμφάνισης γραμμάτων μπορούν να χρησιμοποιηθούν σαν εργαλείο κρυπτανάλυσης, με αποτέλεσμα να ανατρέπεται η ασφάλεια των αλγορίθμων κρυπτογράφησης που υπήρχαν μέχρι τότε και να προκύπτει η ανάγκη για τη δημιουργία νέων αλγορίθμων οι οποίοι να αλλοιώνουν τα γλωσσικά στατιστικά.

Κατά τη διάρκεια του Μεσαίωνα, η κρυπτογραφία ήταν απαγορευμένη γιατί τη θεωρούσαν ότι αποτελεί μέρος του αποκρυφισμού και της μαύρης μαγείας, καθώς πολλοί αλχημιστές αναγκάστηκαν να τη χρησιμοποιούν για να μην κατηγορηθούν από την εκκλησία, με συνέπεια η κρυπτογραφία να μην γνωρίσει ιδιαίτερη άνθηση την περίοδο αυτή. (Κ.Πατσάκης – Ε. Φούντας ,Κρυπτογραφία και Εφαρμογές)

Αργότερα έχουμε την επιστήμη της Κρυπτολογίας που αποτελείται από την Κρυπτογραφία μαζί με την Κρυπτανάλυση όπου γνωρίζει, μετά την εργασία– σταθμό των Diffie– Hellman, το 1975, μια πραγματική επανάσταση, όπου η μεν επιστήμη της Κρυπτογραφίας επιδιώκει τη δημιουργία ισχυρών κρυπτογραφικών συστημάτων, η δε Κρυπτανάλυση την παραβίαση αυτών . Έτσι η ραγδαία ανάπτυξη που παρατηρείται , κυρίως, στα κρυπτογραφικά συστήματα και πρωτοκόλλα ευνοήθηκε από την επίσης ραγδαία ανάπτυξη συστημάτων υπολογιστών και επικοινωνιών, εξαιτίας της διάθεσης πόρων για την αντιμετώπιση όλων των συναφών ζητημάτων.

Στη συνέχεια οι Κρυπτογραφικοί αλγόριθμοι δημόσιου κλειδιού, βασισμένοι στη δυσκολία παραγοντοποίησης πολύ μεγάλων αριθμών, υπολογισμού διακριτών λογάριθμων και στις ελλειπτικές καμπύλες, στοχαστική κρυπτογράφηση, αλγόριθμοι μηδενικής γνώσης και Κβαντική Κρυπτογραφία αποτελούν ορισμένες από τις πιο αξιόλογες επιτεύξεις των τελευταίων 20 χρόνων ενώ ο αλγόριθμος DES(Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων), από το 1973 που δημιουργήθηκε μέχρι το 1997 που αντικαταστάθηκε από τον AES αποτελούσε πρότυπο αλγόριθμου ισχυρής κρυπτογράφησης. (Βασιλειος Ζορκάδης, Εκπαιδευτικό υλικό,ΕΑΠ)

Τέλος στην πορεία των ετών διαπιστώνουμε ότι η κρυπτογραφία αναπτύχθηκε και αποτελεί βασικό εργαλείο για την ανάπτυξη της Κοινωνίας της Πληροφορίας σε ασφαλές ηλεκτρονικό περιβάλλον, όπου με τη συνεχή ανάπτυξη των μαθηματικών η κρυπτογραφία έχει σήμερα την έννοια του μετασχηματισμού ηλεκτρονικών δεδομένων με τη χρήση αλγορίθμων ώστε να αναγνωσθούν μόνο με τη βοήθεια ενός κλειδιού αποκρυπτογράφησης. (Κ.Πατσάκης – Ε. Φούντας ,Κρυπτογραφία και Εφαρμογές)

7.2 Συμμετρική και Ασύμμετρη Κρυπτογραφία

Η διαδικασία της κρυπτογράφησης μηνύματος καθώς και η αποκρυπτογράφησή του για την πραγματοποίησή της απαιτεί απαραιτήτως την ύπαρξη ενός κλειδιού και αυτό το στοιχείο επιτρέπει την διάκριση της κρυπτογραφίας σε δύο μεγάλες κατηγορίες: την συμμετρική ή κρυπτογραφία ιδιωτικού κλειδιού και την ασύμμετρη ή κρυπτογραφία δημόσιου κλειδιού.

Μια από τις βασικότερες τεχνολογικές εφαρμογές της κρυπτογραφίας είναι η κρυπτοθέτηση όπου η βασική διαφορά της σε σχέση με την ηλεκτρονική υπογραφή είναι ότι στην πρώτη τα δεδομένα, που διαβιβάζονται κρυπτογραφούνται αλλά δεν υπογράφονται ηλεκτρονικά, με συνέπεια αν και διασφαλίζεται το απόρρητο της επικοινωνίας δεν μπορεί να διαπιστωθεί η ταυτότητα του αποστολέα των ηλεκτρονικών δεδομένων σε αντίθεση με την ηλεκτρονική υπογραφή.

Μέχρι το 1976 γινόταν αποκλειστικά χρήση στις ηλεκτρονικές συναλλαγές μόνο της συμμετρικής κρυπτογραφίας, όπου σύμφωνα με αυτή την

διαδικασία έπρεπε οι δύο χρήστες που επιθυμούσαν να ανταλλάξουν ένα κρυπτογραφημένο μήνυμα να γνωρίζουν και οι δύο από πριν το ίδιο κλειδί κρυπτογράφησης και αποκρυπτογράφησης κάτι που οδηγεί σε χρονική καθυστέρηση της συναλλαγής . (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Όπως προκύπτει από τα παραπάνω βασικό χαρακτηριστικό της συμμετρικής κρυπτογραφίας είναι ότι είναι αποτελεσματική μόνο σε περιπτώσεις όπου τα άτομα που πραγματοποιούν ηλεκτρονικές συναλλαγές είναι ολιγάριθμα και υπάρχει αμοιβαία εμπιστοσύνη ανάμεσά τους και ένας ακόμη λόγος που κάνει τη συμμετρική κρυπτογραφία ακατάλληλη για το διαδίκτυο και τις συναλλαγές είναι ότι η κάθε δημόσια υπηρεσία, οργανισμός, εταιρία ή συναλλασσόμενος ιδιώτης θα έπρεπε να κατέχει και από ένα διαφορετικό κλειδί κρυπτογράφησης και αποκρυπτογράφησης. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Αυτό βέβαια δεν συμβαίνει στην περίπτωση της ασύμμετρης κρυπτογραφίας γιατί ο κάθε συναλλασσόμενος έχει το δικό του ζεύγος κλειδιών, δηλαδή το ιδιωτικό κλειδί, που είναι μυστικό και το γνωρίζει μόνο ο ιδιοκτήτης του και το δημόσιο κλειδί που είναι ελεύθερα προσβάσιμο σε όλους όσοι συναλλάσσονται με τον ιδιοκτήτη του ιδιωτικού κλειδιού. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Για να καταλάβουμε πως λειτουργεί η ασύμμετρη κρυπτογραφία πρέπει να κατανοήσουμε ότι τα δύο κλειδιά δηλαδή το ιδιωτικό και το δημόσιο λειτουργούν πάντα ως ζεύγος με την έννοια πως ότι κρυπτογραφεί το ένα αποκρυπτογραφείται μόνο από το άλλο και αντιστρόφως και αυτή η αλληλεξάρτηση των κλειδιών στηρίζεται στις μαθηματικές ιδιότητες των πρώτων αριθμών , δηλαδή αυτών που μόνο όταν διαιρούνται με τον εαυτό τους και με τον αριθμό ένα, δίνουν πηλίκο έναν ακέραιο και όχι δεκαδικό αριθμό. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Επίσης πρέπει να τονίσουμε ότι εκμηδενίζεται τελείως ο κίνδυνος πλαστοπροσωπίας ανάλογα με την τεχνολογία που εφαρμόζεται κατά την διαδικασία της ασύμμετρης κρυπτογραφίας γιατί υπάρχει ένας μηχανισμός, που αναλαμβάνει την εγγύηση και την πιστοποίηση ανά πάσα στιγμή στο συναλλασσόμενο ότι το δημόσιο κλειδί που χρησιμοποιεί για να αποκρυπτογραφήσει ένα ηλεκτρονικά υπογεγραμμένο αρχείο ανήκει στον αντισυμβαλλόμενο του με τον οποίο πραγματοποιείται η ηλεκτρονική συναλλαγή.

Ο μηχανισμός αυτός ονομάζεται <<Πάροχος Υπηρεσιών Πιστοποίησης>> και η συμβολή του στην ύπαρξη ασφάλειας και εμπιστοσύνης στις ηλεκτρονικές συναλλαγές ,που πραγματοποιούνται στο περιβάλλον ανωνυμίας του Διαδικτύου είναι πολύτιμη και απαραίτητη και σύμφωνα με το άρθρο 2 του προεδρικού διατάγματος 150/2001 ο έλληνας νομοθέτης ορίζει ότι μπορεί να είναι ένα φυσικό ή νομικό πρόσωπο ή άλλος φορέας που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις

ηλεκτρονικές υπογραφές και εξασφαλίζει στα συμβαλλόμενα μέρη την απαραίτητη τεχνολογία, δηλαδή το λογισμικό, όπως προγράμματα software, και το υλικό, όπως δισκέτες ή έξυπνες κάρτες για να δημιουργηθεί και να επαληθευτεί μια ηλεκτρονική υπογραφή τηρώντας μια βάση δεδομένων προσβάσιμη σε όλους, η οποία περιέχει τα δημόσια κλειδιά όλων των πελατών του , κατόχων ηλεκτρονικής υπογραφής. (προεδρικό διάταγμα 150/2001)

7.3 Κρυπτογράφηση δημοσίου ή ασύμμετρου κλειδιού

Η διαδικασία της κρυπτογράφησης δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε περίπου στα τέλη της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman όπου το βασικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης που παρείχε ήταν ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες και το δημόσιο κλειδί 1024 bits αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

Σύμφωνα με τα παραπάνω κάθε χρήστης πρέπει να διαθέτει δύο κλειδιά κρυπτογράφησης που το ένα ονομάζεται ιδιωτικό κλειδί (private key) και θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό και το άλλο δημόσιο κλειδί (public key) που θα πρέπει να το ανακοινώνει και να είναι προσβάσιμο σε όλη την διαδικτυακή κοινότητα.

Βέβαια προς αυτή την κατεύθυνση 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 λοιπόν κλειδιά δηλαδή το ιδιωτικό και δημόσιο έχουν μαθηματική σχέση μεταξύ τους, που αυτό σημαίνει ότι το ένα χρησιμοποιείται για την κρυπτογράφηση κάποιου μηνύματος και το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού και η αποτελεσματικότητα αυτού του είδους των κρυπτογραφικών αλγορίθμων που χρησιμοποιούνται βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφηση δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Έτσι με αυτόν τον τρόπο η κρυπτογράφηση του δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού που χρησιμοποιούσαν ένα κοινό μυστικό κλειδί, το οποίο το γνώριζαν μόνο ο αποστολέας του κρυπτογραφημένου μηνύματος και ο παραλήπτης. Αυτό όμως το κοινό μυστικό κλειδί που χρησιμοποιούσαν κατά την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος παρουσίαζε πρόβλημα στην περίπτωση που το κανάλι επικοινωνίας δεν ήταν ασφαλές και ήταν δύσκολο ο

αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα.

Αυτό το πρόβλημα ήταν ιδιαίτερα έντονο και στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις που ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα γι αυτό το λόγο οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ). (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

Πιο αναλυτικά η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού στηρίζεται σε ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών και είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Ο τυχαίος αυτός αριθμός σε σύγχρονα προγράμματα κρυπτογράφησης ακολουθεί μια διαδικασία παραγωγής των κλειδιών ,όπου 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 ο χρήστης 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) και με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στην γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

Επίσης ένα από τα βασικά πλεονεκτήματα των κρυπτογραφικών αλγόριθμων δημοσίου κλειδιού είναι ότι μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη και θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί όμως η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα και στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος να μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Ξεκινώντας με τη βασική προϋπόθεση ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, παρέχεται η δυνατότητα μονάχα στον παραλήπτη να μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει και έτσι με αυτόν τον τρόπο διασφαλίζεται η εμπιστευτικότητα του μηνύματος γιατί ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη.

Η παραπάνω μέθοδος μπορεί μεν να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα του μηνύματος που αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα γιατί , ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο. (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

Επιπλέον ένα βασικό πλεονέκτημα των κρυπτογραφικών αλγόριθμων δημοσίου κλειδιού είναι ότι μπορούν αν χρησιμοποιηθούν κατάλληλα οι κρυπτογραφικοί αλγόριθμοι του δημοσίου κλειδιού να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα και για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος και να στείλει το μήνυμα στον παραλήπτη ο οποίος χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα να αποκρυπτογραφήσει το ηλεκτρονικό μήνυμα του με την προϋπόθεση ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο και ο παραλήπτης με τη σειρά του μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.

Παρόλο όμως που η παραπάνω μέθοδος εγγυάται μεν την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος γιατί το ηλεκτρονικό μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα και όπως έχει ήδη ειπωθεί παραπάνω, το δημόσιο κλειδί είναι γνωστό και προσβάσιμο σε όλη την διαδικτυακή κοινότητα και επομένως ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

Συμπερασματικά καταλήγουμε ότι χρησιμοποιώντας τους κατάλληλους κρυπτογραφικούς αλγόριθμους είναι δυνατό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα δηλαδή το μήνυμα να παραμένει γνωστό μονάχα στον αποστολέα και τον παραλήπτη και ο παραλήπτης να γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα και ότι για να επιτευχθεί αυτό ο αποστολέας έχει τη δυνατότητα να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στην συνέχεια με το δημόσιο κλειδί ο παραλήπτης θα λάβει το μήνυμα και θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στην συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

7.4 Συμμετρικοί και Ασύμμετροι Αλγόριθμοι

Η τεράστια ανάπτυξη των δικτύων υπολογιστών και η επικοινωνία πληροφοριών κάθε μορφής έφερε ένα τεράστιο πρόβλημα στην επιφάνεια,

για την ανάγκη προστασίας αυτής της πληροφορίας όπου σύμφωνα με το ISO 74982, οι υπηρεσίες ασφαλείας που μπορούν να υποστηριχθούν σε ανοικτά συστήματα είναι βασικά πέντε όπως η γνησιότητα χρηστών και πληροφοριών (authentication), ο έλεγχος πρόσβασης (access control),η εμπιστευτικότητα (confidentiality),η ακεραιότητα των δεδομένων (data integrity) και η μη δυνατότητα αποκήρυξης γεγονότων που έχουν συμβεί (non-repudiation).

Όπως αναφέρθηκε και πιο πάνω η Κρυπτογράφηση (encryption) είναι μια διαδικασία που πραγματοποιείται μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανένα παρά μόνο από αυτόν που είναι κάτοχος ενός κατάλληλου κλειδιού και υποστηρίζεται η λειτουργία της από δύο μεγάλες οικογένειες αλγόριθμων κρυπτογράφησης, τους συμμετρικούς αλγόριθμους (ή αλγόριθμους μυστικού κλειδιού) και τους ασύμμετρους (ή αλγόριθμους δημόσιου κλειδιού). (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

Αναλύοντας τους συμμετρικούς αλγόριθμους διαπιστώνουμε ότι το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο και συμβαίνει στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια.

Αυτό προκύπτει από το γεγονός ότι οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια και ότι η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού για όσο διάστημα επιθυμεί ο χρήστης η επικοινωνία να παραμείνει μυστική, για τον ίδιο χρονικό διάστημα πρέπει και το κλειδί να παραμείνει μυστικό.

Οι συμμετρικοί αλγόριθμοι δύναται να διαιρεθούν σε δύο υποκατηγορίες τους αλγόριθμους ροής(stream ciphers) οι οποίοι λειτουργούν bit προς bit και τους μπλοκ αλγόριθμοι (block iphers) οι οποίοι λειτουργούν πάνω σε κομμάτια δεδομένων (συνήθως των 64 bit) όπως λειτουργούν οι συμμετρικοί αλγόριθμοι DES, IDEA, RC5 και SAFER.

Αντίθετα οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού είναι σχεδιασμένοι να λειτουργούν διαφορετικά από τους συμμετρικούς αλγόριθμους όσο αφορά την λειτουργία του κλειδιού που χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης και είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση με αποτέλεσμα το κλειδί αποκρυπτογράφησης δεν δύναται να υπολογιστεί από το κλειδί κρυπτογράφησης. (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

Σχετικά τώρα με την ονομασία που έχουν οι αλγόριθμοι αυτής της κατηγορίας και ονομάζονται ως οι αλγόριθμοι και "δημόσιου κλειδιού" συμβαίνει γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί και ότι υπάρχει η δυνατότητα σε οποιοδήποτε να μπορεί να κρυπτογραφήσει ένα

μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί έχει το δικαίωμα να το αποκρυπτογραφήσει και τέτοιοι ασύμμετροι αλγόριθμοι είναι οι RSA, ElGamal και DSA.

Όταν αναφερόμαστε στον όρο διαχείριση του κλειδιού εννοούμε την διαδικασία παραγωγής, διανομής, επαλήθευσης, χρησιμοποίησης, ενημέρωσης, αποθήκευσης και καταστροφής κλειδιών σε ένα σύστημα κρυπτογράφησης και σαφώς η ασφαλής μέθοδος διαχείρισης των κλειδιών είναι πάρα πολύ σημαντική για τις ηλεκτρονικές συναλλαγές των συναλλασσόμενων μερών ενώ στην πράξη αποδεικνύεται ότι οι περισσότερες επιθέσεις σε συστήματα ασφαλείας έχουν ως στόχο τις διαδικασίες διαχείρισης των κλειδιών και όχι τους ίδιους τους αλγόριθμους.

Στην περίπτωση αυτή που εξετάζουμε οι αλγόριθμοι δημόσιου κλειδιού καθιστούν την διαχείριση πολύ πιο εύκολη γιατί το ιδιωτικό κλειδί δεν υπάρχει περίπτωση να μεταδοθεί αλλά το πιο σημαντικό πρόβλημα που παρουσιάζεται είναι ότι ο κάθε χρήστης πρέπει να διαθέτει ένα δικό τους ζεύγος κλειδιών ενώ στα συστήματα που χρησιμοποιούν ασύμμετρη κρυπτογραφία χρειάζονται μέθοδοι διανομής και επαλήθευσης κλειδιών όπου τα πρωτόκολλα CCITTX.509 παρέχουν κανόνες για τις διαδικασίες αυτές.

Όταν αναφερόμαστε τώρα στην έννοια πρωτόκολλο εννοούμε μια σειρά κανόνων που πρέπει να ακολουθηθούν για την εκτέλεση μιας δεδομένης εργασίας ,όπου τα πρωτόκολλα ασφάλειας δεδομένων συχνά περιέχουν την χρήση κάποιων αλγορίθμων κρυπτογράφησης αλλά σε γενικές γραμμές αυτό που προσπαθούν να επιτύχουν όχι μόνο τη μυστικότητα αλλά και την παροχή των βασικών υπηρεσιών ασφαλείας που αναφέρθηκαν παραπάνω. (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

Συμπερασματικά καταλήγουμε ότι οι συμμετρικοί αλγόριθμοι είναι πολύ πιο γρήγοροι, εφαρμοσμένοι είτε σε υλικό είτε σε λογισμικό από τους ασύμμετρους αλγόριθμους χρησιμοποιούνται για την κρυπτογράφηση του κυρίου μέρους των δεδομένων, ενώ οι αλγόριθμοι δημόσιου κλειδιού βρίσκουν κατάλληλη εφαρμογή σε πρωτόκολλα ανταλλαγής κλειδιών και ψηφιακών υπογραφών.

7.5 Μονόδρομες Συναρτήσεις

Στην ενότητα αυτή αναλύεται η λειτουργία των μονόδρομων συναρτήσεων σύνοψης (one-way hash functions) οι οποίες αποτελούν θεμελιώδη στοιχεία για την ανάπτυξη των περισσότερων πρωτοκόλλων κρυπτογράφησης, δέχονται σαν είσοδο μια ακολουθία χαρακτήρων μεταβλητού μήκους και παράγουν ένα μήνυμα σταθερού μεγέθους (γενικά μικρότερο) που ονομάζεται τιμή σύνοψης (hash value).

Πιο αναλυτικά με τις μονόδρομες συναρτήσεις σύνοψης είναι εύκολο να υπολογιστεί μια τιμή σύνοψης για κάποιο δεδομένο μήνυμα αλλά είναι αδύνατο να υπολογιστεί το μήνυμα στο οποίο αντιστοιχεί μια συγκεκριμένη

τιμή σύνοψης και η καλά σχεδιασμένη μονόδρομη συνάρτηση σύνοψης εξασφαλίζει τη βεβαιότητα να βρεθούν δύο μηνύματα που δίνουν την ίδια τιμή σύνοψης και είναι επίσης ελεύθερη από συγκρούσεις (collision-free).

Οι μονόδρομες συναρτήσεις σύνοψης χρησιμοποιούνται κυρίως για εφαρμογές επαλήθευσης όπου η τιμή σύνοψης αντιστοιχεί πλήρως, και αντιπροσωπεύει το αρχικό μήνυμα ενώ η αλλαγή έστω και ενός bit στο αρχικό μήνυμα αλλάζει κατά μέσο όρο τα μισά bits της τιμής σύνοψης. Μονόδρομες συναρτήσεις σύνοψης αποτελούν και οι κώδικες πιστοποίησης μηνυμάτων (Message authentication codes, MACs) οι οποίες βασίζονται σε μυστικό κλειδί έτσι ώστε μόνο κάποιος που γνωρίζει το κλειδί αυτό μπορεί να επιβεβαιώσει την τιμή σύνοψης και παρέχουν αυθεντικότητα.

Τέλος μία μονόδρομη συνάρτηση σύνοψης μπορεί να μετατραπεί σε κώδικα πιστοποίησης αν η τιμή σύνοψης κρυπτογραφηθεί με ένα συμμετρικό αλγόριθμο. Παραδείγματα μονόδρομων συναρτήσεων σύνοψης είναι οι MD4, MD5 και SHA. (www.encrypted.google.com/ Κ.Σ. Χειλάς, Δίκτυα Η/Υ)

7.6 Έξυπνες κάρτες και η ηλεκτρονική ταυτότητα

Στην τεχνολογία των έξυπνων καρτών βασίζεται και η λειτουργία της Κοινωνίας της Πληροφορίας με επιδιωκόμενο στόχο να γίνει η ευρωπαϊκή οικονομία, πιο ανταγωνιστική και πιο δυναμικά αναπτυσσόμενη οικονομία ενώ επιμέρους στόχοι είναι η δημιουργία νέων θέσεων εργασίας, ο εκσυγχρονισμός των δημοσίων υπηρεσιών μέσω υπηρεσιών ηλεκτρονικής διακυβέρνησης, ηλεκτρονικής υγείας και ηλεκτρονικής εκπαίδευσης και η εξάλειψη των κοινωνικών ανισοτήτων και αποκλεισμών.

Όταν αναφερόμαστε στις έξυπνες κάρτες εννοούμε πλαστικές κάρτες σε μέγεθος πιστωτικών καρτών ,οι οποίες έχουν ενσωματωμένο μικροεπεξεργαστή όπου στο πλαίσιο της ηλεκτρονικής ταυτότητας, είναι να πραγματοποιούν ευαίσθητες από άποψη ασφάλειας, κρυπτογραφικές λειτουργίες (δημιουργία ζεύγος κλειδιών, αποθήκευση και ελεγχόμενη πρόσβαση στο ιδιωτικό κλειδί του ζεύγους), στο προστατευμένο εσωτερικό τους περιβάλλον όπου με αυτόν τον τρόπο, το ιδιωτικό κλειδί δεν αποθηκεύεται στη μνήμη ή σε δίσκο ηλεκτρονικού υπολογιστή, δηλαδή σε περιοχή, από όπου οι πιθανότητες διαρροής του είναι συγκριτικά μεγαλύτερες. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Κύρια γνωρίσματα των έξυπνων καρτών είναι η ικανότητα που έχουν να αποθηκεύουν και να επεξεργάζονται πληροφορίες με ασφαλή τρόπο, δεν απομαγνητίζονται με την πάροδο του χρόνου, όπως συμβαίνει με τις κοινές μαγνητικές κάρτες που χρησιμοποιούμε στις ΑΤΜ, παρέχοντας έτσι αυξημένη προστασία στα δεδομένα που περιέχουν, δεν αντιγράφονται , έχουν φορητότητα, είναι εύχρηστες και οικονομικές στην κατασκευή μπορούν να αποθηκεύουν το ιδιωτικό κλειδί της ψηφιακής υπογραφής του χρήστη της έξυπνης κάρτας, έτσι ώστε να διασφαλίζονται τα μοναδικά πλεονεκτήματα

που προσφέρει η χρήση του ιδιωτικού κλειδιού και άρα της ασύμμετρης κρυπτογραφίας στις ηλεκτρονικές συναλλαγές.

Επίσης το chip μιας έξυπνης κάρτας, το οποίο κατασκευάζεται από άμμο χαλαζία, μπορεί να περιέχει μόνο μνήμη ή και μικροεπεξεργαστή, ενώ έχει τη δυνατότητα να καθιστά δύσκολη τόσο την πρόσβαση στα στοιχεία του ιδιοκτήτη της κάρτας, όσο και την παραποίησή τους, και να αντιλαμβάνεται άμεσα προσπάθειες πρόσβασης οι οποίες δεν είναι έγκυρες.

Μεταξύ των πλεονεκτημάτων της τεχνολογίας των έξυπνων καρτών συγκαταλέγονται το μικρό μέγεθος, η ολοένα μνήμη και υπολογιστική ισχύς, η οποία για παράδειγμα RSA κλειδιών μήκους 1024 ή 2048 bit από τον επεξεργαστή της κάρτας σε εύλογο χρονικό διάστημα (10 – 20 δευτερόλεπτα) ενώ βασικό μειονέκτημα της τεχνολογίας είναι η απαραίτητη για την ύπαρξη συσκευής ανάγνωσης (smart card reader) στον υπολογιστή που θα χρησιμοποιηθεί η κάρτα.

Τέλος στο σχέδιο δράσης Europe 2005, στους στόχους της Κοινωνίας της Πληροφορίας προστέθηκε η ανάπτυξη ασφαλών υπηρεσιών, εφαρμογών και περιεχομένου και μεταξύ των πεδίων εφαρμογής της Κοινωνίας της Πληροφορίας προτεραιότητα έχουν οι ηλεκτρονικές δημόσιες υπηρεσίες, η διαδικτυακή πρόσβαση υψηλών ταχυτήτων και η δικτυακή ασφάλεια. Τα προβλήματα ασφάλειας όμως που προκύπτουν μειώνουν την εμπιστοσύνη των πολιτών στα δίκτυα δεδομένων και στα πληροφορικά συστήματα και κατά συνέπεια παρεμποδίζουν την πλήρη αξιοποίηση των δυνατοτήτων του Διαδικτύου προς όφελος των πολιτών και των επιχειρήσεων και στην ευρύτερη αξιοποίηση των ηλεκτρονικών συναλλαγών.

Σε αυτήν την περίπτωση οι έξυπνες κάρτες μπορούν να κάνουν τον έλεγχο αυθεντικότητας κατά την πρόσβαση σε ηλεκτρονικές υπηρεσίες ασφαλέστερο με την χρήση των ψηφιακών πιστοποιητικών, που βρίσκονται αποθηκευμένα στην κάρτα όπως για παράδειγμα, αντί για όνομα χρήστη και κωδικό ασφάλειας, ο κάτοχος έξυπνης κάρτας και ψηφιακού πιστοποιητικού μπορεί να ακολουθήσει μια διαδικασία πρόκλησης – απόκρισης (challenge - response).(Αλέξανδρος Κ.Σφάγος, Διπλωματική Εργασία,ΕΜΠ,2005)

8.Η ψηφιακή υπογραφή

Η Ευρωπαϊκή Ένωση, σύμφωνα με την Κοινοτική Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές(EEL 13/19.1.2000) αναγνωρίζει γενικά ως ηλεκτρονικές υπογραφές αυτές ,που μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες και συγκεκριμένα στο άρθρο 5 παράγραφο 2 της Οδηγίας αναφέρονται ως ηλεκτρονικές υπογραφές, 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.

Από την κανονιστική πλευρά, επίσης η Κοινοτική Οδηγία διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών τις οποίες τις αποκαλεί αναγνωρισμένες ηλεκτρονικές υπογραφές και τις αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές, σύμφωνα με το ισχύον νομικό καθεστώς του κάθε κράτους μέλους και σε αυτήν την κατηγορία ανήκουν και όλες οι προηγμένες ηλεκτρονικές υπογραφές που, επιπλέον, βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής (κοινοτική οδηγία 1999/93)

Όταν αναφερόμαστε λοιπόν στον όρο προηγμένες ηλεκτρονικές υπογραφές , οποίες στην ελληνική νομοθεσία με το προεδρικό διάταγμα 150/2001- αποκαλούνται και ψηφιακές υπογραφές, η Κοινοτική Οδηγία προσδιορίζει με σαφήνεια ως ηλεκτρονικές υπογραφές αυτές, που ικανοποιούν τις εξής απαιτήσεις όπως στο να συνδέονται μονοσήμαντα με τον υπογράφοντα, να είναι ικανές να ταυτοποιήσουν τον υπογράφοντα, να δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να υπάρχει η δυνατότητα να εντοπιστεί οποιαδήποτε αλλοίωση στα δεδομένα που αναφέρονται. (κοινοτική οδηγία 1999/93)

Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για τις ψηφιακές υπογραφές οι οποίες ταυτίζονται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές της Κοινοτικής Οδηγίας γίνεται με το άρθρο 14 του νόμου 2672/98 όπου αναφέρεται σε μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα.(άρθρο 14 του ν. 2672/98)

Αργότερα το ελληνικό Δίκαιο με ειδική πρόβλεψη (Ν. 2672/1999) προτείνει τον όρο ψηφιακή υπογραφή αντί για ηλεκτρονική, και δίνει τον ορισμό της ψηφιακής μορφής ως η υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, με την προϋπόθεση ότι η εν λόγω υπογραφή συνδέεται μονοσήμαντα με τον υπογράφοντα, ταυτοποιεί τον υπογράφοντα, δημιουργείται με μέσα τα οποία 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 αλλοίωση των εν λόγω δεδομένων". (Ν. 2672/1999)

Παρά τον ορισμό αυτό, ο παραπάνω νόμος δεν εξισώνει νομικά τη ψηφιακή υπογραφή με την ιδιόχειρη και το κενό αυτό ήρθε να καλύψει το Προεδρικό Διάταγμα 150/2001.

Πιο συγκεκριμένα η ψηφιακή υπογραφή αποτελεί τεχνολογία, που βασίζεται αποκλειστικά στην τριμερή ασύμμετρη κρυπτογραφία, έχει όλα τα πλεονεκτήματα της τεχνολογίας αυτής και γι αυτό το λόγο θεωρείται η πιο άρτια και ασφαλής τεχνολογικά μέθοδος διαπίστωσης της ταυτότητας του ηλεκτρονικά συναλλασσόμενου και διαφύλαξης της ακεραιότητας του αποστελλόμενου αρχείου χρησιμοποιώντας κυρίως τη μέθοδο της δημιουργίας του δακτυλικού αποτυπώματος δηλαδή της σύντμησης του αρχείου που πρόκειται να κρυπτογραφηθεί. Στη συνέχεια , το συντμημένο κείμενο που προκύπτει κρυπτογραφείται με το απόρρητο ιδιωτικό κλειδί του αποστολέα – υπογράφοντα και αυτό το κρυπτογραφημένο συντμημένο κείμενο αποτελεί την ψηφιακή υπογραφή. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Σύμφωνα με τη μέθοδο αυτή, ο αποστολέας του ηλεκτρονικού αρχείου ,κειμένου ή άλλου παράγει μια σύντμηση του μεταβιβαζόμενου κειμένου με τη βοήθεια ενός αλγόριθμου, ο οποίος δεν έχει καμιά σχέση με κανένα άλλο αλγόριθμο ,όπου εξαιτίας του αυξημένου χρόνου που χρειάζεται ένα μεγάλο έγγραφο για να κρυπτογραφηθεί με έναν ασύμμετρο αλγόριθμο κρυπτογράφησης, στην πραγματικότητα δεν κρυπτογραφείται το ίδιο, αλλά η περίληψή του.

Στη συνέχεια η περίληψη αυτή δημιουργείται με τη βοήθεια ενός αλγορίθμου τύπου hash (όπως ο MD5) ο οποίος μπορεί να δημιουργεί ένα σύντομο κείμενο σταθερού μήκους (π.χ. 128 χαραχτήρες) που συνδέεται μοναδικά με το αρχικό έγγραφο. Στην περίπτωση που αλλάξει έστω και ένα μόνο bit του αρχικού εγγράφου, τότε δημιουργείται μια τελείως διαφορετική περίληψη και η πιθανότητα να βρεθούν δυο κείμενα με την ίδια περίληψη (χρησιμοποιώντας τον αλγόριθμο MD5) είναι 1 στις 18.446.744.073.709.551.616, ενώ να δημιουργηθεί ένα κείμενο που να έχει μια συγκεκριμένη περίληψη είναι 1 στις $18.446.744.073.709.551.616^2$!

Επομένως είναι κατανοητό ότι δεν είναι δυνατή η δοκιμή όλων των πιθανών συνδυασμών κλειδιών για την αποκρυπτογράφηση ενός εγγράφου γιατί μια τέτοια πιθανότητα είναι πρακτικά αδύνατη. Εξετάζοντας τώρα την περίπτωση της επιλογής κλειδιών μεγέθους 128bit, τότε έχουμε $18.446.744.073.709.551.616^2$ διαφορετικά κλειδιά και για να δοκιμαστούν όλα αυτά τα κλειδιά με 100 υπολογιστές (επεξεργαστικής ισχύος ενός Pentium III) που θα λειτουργούν ταυτόχρονα, θα χρειάζονταν χρόνο ίσο με 10 φορές την ηλικία του σύμπαντος. Στη συνέχεια , το συντμημένο κείμενο που προκύπτει κρυπτογραφείται με το απόρρητο ιδιωτικό κλειδί του αποστολέα – υπογράφοντα. Αυτό το κρυπτογραφημένο συντμημένο κείμενο αποτελεί την ψηφιακή υπογραφή.www.papadi.gr

Μια άλλη μέθοδος δημιουργίας ψηφιακής υπογραφής είναι αυτή του ψηφιακού φακέλου η οποία συνδυάζει τα συστήματα συμμετρικών και

ασύμμετρων αλγορίθμων και μειώνει το χρόνο κρυπτογράφησης του μηνύματος, γιατί οι συμμετρικοί αλγόριθμοι κρυπτογραφούν ένα αρχείο πιο γρήγορα από τους ασύμμετρους.

Σύμφωνα με τη μέθοδο αυτή , η οποία αποκαλείται υβριδικό σύστημα κρυπτογραφίας το μήνυμα κρυπτογραφείται συμμετρικά από τον αποστολέα με τη χρήση ενός σύντομου αλλά ασφαλούς κλειδιού μήκους 128 bits, το οποίο καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και ονομάζεται κλειδί συνεδρίας. Στη συνέχεια το κλειδί αυτό κρυπτογραφείται με τη διαδικασία της ασύμμετρης κρυπτογραφίας, δηλαδή με το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης του εγγράφου πρέπει πρώτα να χρησιμοποιήσει το ιδιωτικό του κλειδί για να βρει το κλειδί της συνεδρίας του αποστολέα και, στη συνέχεια μέσω αυτού του κλειδιού και το αρχικό μήνυμα. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί μόνο στην περίπτωση που ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).Όμως με την διαδικασία της επαλήθευσης ψηφιακής υπογραφής ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή, δηλαδή την κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύντμηση του μηνύματος, και την αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, που είτε αποστέλλεται στο λήπτη μαζί με το κρυπτογραφημένο κείμενο είτε γνωστοποιείται μέσω δημοσίευσης σε ειδικό δημόσιο κατάλογο που τηρεί ο Πάροχος Υπηρεσιών Πιστοποίησης. www.papadi.gr

Στη συνέχεια, ο παραλήπτης δημιουργεί ο ίδιος το δακτυλικό αποτύπωμα του κειμένου που έλαβε, εφαρμόζοντας στο πρωτότυπο μήνυμα τον ίδιο αλγόριθμο που εφάρμοσε ο αποστολέας του μηνύματος και παράγεται εκ νέου μια σύντμηση του μεταβιβαζόμενου ηλεκτρονικού κειμένου, η οποία συγκρίνεται από τον παραλήπτη με τη σύντμηση που παρέλαβε.

Αν από την σύγκριση των δύο συντμήσεων το αποτέλεσμα είναι ίδιο, τότε πιστοποιείται ότι το απεσταλμένο μήνυμα δεν αλλοιώθηκε ώσπου να φτάσει στον παραλήπτη ενώ στην περίπτωση που το μήνυμα έχει μεταβληθεί, η σύνοψη που παράγει ο παραλήπτης είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

Επίσης ο ιδιοκτήτης ψηφιακής υπογραφής, αλλά και κάθε τρίτος συναλλασσόμενος με αυτόν μπορεί ανά πάσα στιγμή να προμηθευτεί από τον αρμόδιο Πάροχο Υπηρεσιών Πιστοποίησης πιστοποιητικό γνησιότητας της υπογραφής, που θα πρέπει ο ενδιαφερόμενος χρήστης να παραγάγει, με τη βοήθεια κατάλληλου λογισμικού που έχει προμηθευτεί από τον Πάροχο Υπηρεσιών Πιστοποίησης, το ζεύγος ιδιωτικού και δημόσιου κλειδιού που αποτελεί την ψηφιακή του υπογραφή.

Στη συνέχεια αφού αποθηκεύσει το ιδιωτικό του κλειδί είτε στο σκληρό δίσκο του Η/Υ του είτε σε κινητό μαγνητικό μέσο προστατευμένο από μυστικό κωδικό, ανάλογο με το PIN στις τραπεζικές κάρτες, ο χρήστης αποστέλλει το δημόσιο κλειδί του στον Πάροχο Υπηρεσιών Πιστοποίησης αιτούμενος την πιστοποίησή του. Στη συνέχεια ο αρμόδιος υπάλληλος-χειριστής του Παρόχου Υπηρεσιών Πιστοποίησης αφού διαπιστώσει την ύπαρξη της αίτησης , επικοινωνεί με τον ενδιαφερόμενο για να του ζητήσει να εμφανιστεί στην Αρχή Εγγραφής δηλαδή στο περιφερειακό όργανο ελέγχου, το οποίο διαπιστώνει την ακριβή ταυτότητα του ενδιαφερομένου.

Μετά τον έλεγχο, ο αρμόδιος υπάλληλος του Παρόχου Υπηρεσιών Πιστοποίησης προχωρεί στην έκδοση του ψηφιακού πιστοποιητικού, το οποίο περιέχει συνήθως το όνομα του ιδιοκτήτη της ψηφιακής υπογραφής, το δημόσιο κλειδί του, την ηλεκτρονική του διεύθυνση, τη διεύθυνση νόμιμης κατοικίας του, τη διάρκεια ισχύος του πιστοποιητικού, τυχόν περιορισμούς για τη χρήση του, τυχόν όρια για το ύψος των συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί το σχετικό πιστοποιητικό, καθώς και τα αρχεία που το εξέδωσε.

Στη συνέχεια το πιστοποιητικό με όλες τις πληροφορίες υπογράφεται ηλεκτρονικά, δηλαδή κρυπτογραφείται, με το ιδιωτικό κλειδί του Παρόχου Υπηρεσιών Πιστοποίησης και αποστέλλεται στον ενδιαφερόμενο και έχει ημερομηνία λήξης, συνήθως έξι μήνες έως ένα χρόνο από την έκδοσή του, όπου μετά τη λήξη του δημοσιεύεται σε δημόσιο κατάλογο ληγμένων πιστοποιητικών, ώστε κάθε ενδιαφερόμενος να είναι σε θέση να πληροφορηθεί το περιεχόμενο του καταλόγου.

Τα πιστοποιητικά διακρίνονται σε επώνυμα και σε ψευδώνυμα ανάλογα με τη δημοσιοποίηση του πραγματικού ονόματος του υποκειμένου στο οποίο αναφέρονται και υπάρχει η δυνατότητα να εκδοθούν και ανώνυμα πιστοποιητικά, στα οποία συνήθως πιστοποιείται μέσω απομακρυσμένης online επικοινωνίας μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου από το υποκείμενο του πιστοποιητικού.

Επίσης μια άλλη κατηγορία πιστοποιητικών είναι εκείνη, που εκδίδεται με υποκείμενο τηλεπικοινωνιακά ή πληροφοριακά συστήματα και συσκευές με χαρακτηριστική εφαρμογή αυτής της κατηγορίας πιστοποιητικών την πιστοποίηση προέλευσης ιστοσελίδων, όπου πιστοποιείται η νόμιμη εξυπηρέτηση μιας διαδικτυακής διεύθυνσης από έναν συγκεκριμένο διακομιστή δικτύου. (Κοσμάς Α Καραδημητρίου, Η ηλεκτρονική Υπογραφή)

8.1 Ενέργειες Αποστολέα -Παραλήπτη

Πιο αναλυτικά η χρήση της ηλεκτρονικής – ψηφιακής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, αναφέρονται βήμα προς βήμα οι ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει και ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων. Στη συνέχεια με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη και αυτό που παράγεται είναι η ψηφιακή υπογραφή, που είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους. Τέλος η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

Αντίθετα ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη) εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

Τέλος όταν συγκριθούν οι δύο συνόψεις και βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί ενώ αν το μήνυμα έχει μεταβληθεί.

Με τη βοήθεια της ψηφιακής υπογραφής διασφαλίζεται η βεβαιότητα για την ταυτότητα του αποστολέα ενός εγγράφου(ή οποιασδήποτε πληροφορίας μπορεί να αποθηκευτεί σε έναν Η/Υ), η ακεραιότητα του εγγράφου (ότι δηλαδή δεν έγινε καμία αλλαγή σε αυτό), καθώς παρέχεται η δυνατότητα εξασφάλισης ότι κάποιος συγκεκριμένος παραλήπτης και μόνον αυτός θα μπορεί να διαβάσει το έγγραφο και αυτό το επιτρέπει η χρήση ισχυρών αλγορίθμων κρυπτογράφησης στους οποίους βασίζεται η λειτουργία της κρυπτογράφησης και αποκρυπτογράφησης ενός εγγράφου .(www.papadi.gr)

8.2 Αδυναμίες εφαρμογής ψηφιακής Υπογραφής

Είναι αρκετοί οι λόγοι που δεν έχει παρατηρηθεί η εφαρμογή των ψηφιακών υπογραφών στην επαγγελματική καθημερινότητα. Πρώτα πρώτα, μέχρι το 2001 δεν υπήρχε το απαραίτητο νομικό πλαίσιο που θα βοηθούσε μια τέτοια πρωτοβουλία αλλά στη συνέχεια το πρόβλημα αυτό αντιμετωπίστηκε με την έκδοση του Προεδρικού Διατάγματος 150/2001 καθώς και με την υπόδειξη της αντίστοιχης οδηγίας του Ευρωπαϊκού Κοινοβουλίου, όπου με το άρθρο 3 του Πρεδρικού Διατάγματος αναγνωρίζεται ότι «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». (www.papadi.gr)

Ένας άλλος λόγος ήταν η έλλειψη της υποδομής σε λογισμικό για την εφαρμογή των ψηφιακών υπογραφών γιατί ήταν ελάχιστες οι κατηγορίες προγραμμάτων που υποστήριζαν ψηφιακές υπογραφές (κυρίως κάποιοι e-mail clients), δηλαδή περιλάμβαναν τους αλγόριθμους δημιουργίας και ελέγχου αυτών. (www.papadi.gr)

Επίσης είναι γνωστό ότι η χρήση ψηφιακών υπογραφών είναι απαραίτητη γιατί τα δεδομένα που αποστέλλει ο κάθε χρήστης στο Διαδίκτυο περνούν από αρκετούς υπολογιστές μέχρι να φτάσουν στον παραλήπτη που επιθυμεί, γεγονός που καθιστά το ηλεκτρονικό ταχυδρομείο μη ασφαλές και είναι πολύ δύσκολο να είναι κάποιος βέβαιος για την πραγματική ταυτότητα του αποστολέα ενός μηνύματος, μια που ένα ηλεκτρονικό έγγραφο δεν παρέχει τα εχέγγυα γνησιότητας και αυθεντικότητας που παρέχει ένα συμβατικό έγγραφο. (www.papadi.gr)

Επιπλέον η χρήση πλασματικής ταυτότητας στην αποστολή ενός e-mail είναι αρκετά εύκολη, ακόμα και για τον μέσο χρήστη αλλά τα κενά ασφάλειας στα λειτουργικά συστήματα και το λογισμικό γενικότερα, καθιστούν τα περιεχόμενα του υπολογιστή μας συχνά στόχο επιθέσεων.

Τέλος, τα δεδομένα που αποθηκεύονται σε έναν απομακρυσμένο διακομιστή χρησιμοποιώντας κάποιο λογισμικό, μπορεί ενδεχομένως να μην είναι προσβάσιμα από μη εξουσιοδοτημένους χρήστες, αλλά σίγουρα είναι από τον διαχειριστή του συστήματος ή τον κατασκευαστή λογισμικού.

Πάντως ένα από τα αδύναμα σημεία της ψηφιακής υπογραφής είναι η διατήρηση του ιδιωτικού κλειδιού κρυφού και στην περίπτωση που κάποιος τρίτος χρήστης 'κλέψει' το ιδιωτικό κλειδί κάποιου ατόμου, τότε θα μπορεί να υπογράφει έγγραφα στη θέση του, ή να διαβάζει έγγραφα που κρυπτογραφήθηκαν έτσι ώστε να μπορούν να διαβαστούν μόνο από αυτόν και επομένως πρέπει να ακυρωθεί το πιστοποιητικό, μέσω της Αρχής που το εξέδωσε. Για το λόγο αυτό για να αποφευχθεί μια τέτοια δυσάρεστη

κατάσταση, το ιδιωτικό κλειδί κάθε χρήστη κρυπτογραφείται (με συμμετρική κρυπτογράφηση αυτή τη φορά) με μια μυστική φράση, έτσι ώστε ακόμα και στην περίπτωση της υποκλοπής, να μην είναι δυνατή η χρήση του χωρίς να είναι γνωστή η μυστική φράση.

Επίσης είναι πολύ σημαντικό λοιπόν να υπάρχει ένα αντίγραφο του ιδιωτικού κλειδιού σε ένα ασφαλές μέρος, στο οποίο έχει πρόσβαση μόνο ο χρήστης. Εξάλλου τα κλειδιά αυτά είναι αρκετά μικρά (μερικές εκατοντάδες bytes) έτσι ώστε να χωράνε σε μια δισκέτα, μια έξυπνη κάρτα ή σε ένα memory stick. (www.papadi.gr)

8.Εφαρμογές και προοπτικές των ηλεκτρονικών υπογραφών

Σε διεθνές επίπεδο η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών παρέχει υψηλότερα επίπεδα ασφάλειας σε συναλλαγές διαφόρων τύπων όπως: τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως είναι η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchangei EDI), ηλεκτρονικές δημόσιες προμήθειες, ηλεκτρονική ψηφοφορία, συστήματα ηλεκτρονικών πληρωμών (πιστωτικές κάρτες MasterCard&VISA), ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες, που συνήθως φέρουν ενσωματωμένα κάποια βιομετρικά στοιχεία (φωτογραφία, δακτυλικά αποτυπώματα…) του κατόχου τους, υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου, συστήματα υπογραφής αυθεντικότητας διακινούμενου λογισμικού, κλειστές υποδομές PKI για εφαρμογές ασφαλείας μεγάλων οργανισμών (NATO),και πιστοποίηση της ταυτότητας εξυπηρετών διαδικτύου(web servers).

Στην Ευρωπαϊκή Ένωση εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κ.τ.λ έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία τυπικές εφαρμογές των ηλεκτρονικών υπογραφών, που είναι σύμφωνες με το θεσμικό πλαίσιο από το νόμο. Τα ηλεκτρονικά δελτία ταυτότητας σε χώρες όπως το Βέλγιο, Φιλανδία ,Ιταλία, Εσθονία και αλλού, τα οποία χρησιμοποιούν την τεχνολογία PKI σε συνδυασμό με έξυπνες κάρτες, αποτελούν ένα παράδειγμα τέτοιων τυπικών εφαρμογών.

Ένας άλλος τομέας που βρήκαν εφαρμογή οι ηλεκτρονικές υπογραφές στην Ευρωπαϊκή Ένωση είναι τα ηλεκτρονικά τιμολόγια, τα οποία σύμφωνα και με την Ευρωπαϊκή Οδηγία 01/115/ΕΚ, εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνουν αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.

Επίσης μια άλλη εφαρμογή αποτελούν οι ηλεκτρονικές δημόσιες προμήθειες στο πλαίσιο των σχετικών σχεδίων Οδηγιών της Ευρωπαϊκής Ένωσης ,όπου θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως η Υπηρεσία Επισήμων Δημοσιεύσεων, σχεδιάζουν την χρήση των ηλεκτρονικών υπογραφών για τα

έγγραφα που εκδίδουν σε ηλεκτρονική μορφή όπως είναι η Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, η δημοσίευση προκηρύξεων και άλλα.

Στην Ελλάδα, μία από τις πρώτες εφαρμογές νομικά έγκυρης ηλεκτρονικής υπογραφής επίσημων εγγράφων αποτελεί το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αξιών Αθηνών (ΧΑΑ) με τις εισηγμένες σε αυτό εταιρίες, με χρόνο λειτουργίας από το 2002.

Το σύστημα αυτό ονομάζεται ΕΡΜΗΣ (Hellenic Exchanges Remote Messaging Services- HERMES) και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων, στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών (ένα για την ταυτοποίησή τους στο σύστημα και ένα για την αναγνωρισμένη ηλεκτρονική υπογραφή τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους) εναποθετημένα σε μια προσωποποιημένη έξυπνη κάρτα.

Παράλληλα η υποστήριξη και η χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσοτέρων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια του προγράμματος γα την Κοινωνία της Πληροφορίας και των σχετικών Επιχειρησιακών Προγραμμάτων των φορέων του ευρύτερου Δημόσιου Τομέα. Χαρακτηριστικά παραδείγματα αποτελούν τα έργα ψηφιοποίησης του Ποινικού Μητρώου του Υπουργείου Δικαιοσύνης, οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση Εμπορικών νημάτων καθώς και το σύστημα ηλεκτρονικών Δημόσιων Προκηρύξεων & Προμηθειών στο Υπουργείο Ανάπτυξης, τα σχέδια για ηλεκτρονικές υπογραφές των ηλεκτρονικών Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ) του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ (e-ΚΕΠ).

Σημαντικότατη εξέλιξη προς την γενικευμένη χρήση ηλεκτρονικών υπογραφών στην Ελληνική Δημόσια Διοίκηση αποτελεί η υλοποίηση και η ολοκλήρωση του έργου Σύζευξις, όπου προέβλεπε τη χρήση Υποδομής Δημόσιου Κλειδιού (PKI) και την πιστοποίηση ψηφιακών υπογραφών για ένα μεγάλο αριθμό (50.000) δημοσίων υπαλλήλων, οι οποίοι θα μπορούν να εκδίδουν, να υπογράφουν και να διακινούν επίσημα ηλεκτρονικά έγγραφα.

(Μαρινοπούλου Μαρία, Εργασία Ηλεκτρονική Υπογραφή)

9.Ηλεκτρονική Διακυβέρνηση

9.1 Εισαγωγή

Είναι γνωστό πλέον ότι η τεχνολογία έχει τη δυνατότητα να μεταμορφώνει τις ανθρώπινες δραστηριότητες, προσφέροντας μεταξύ άλλων, αποτελεσματικότερους τρόπους επικοινωνίας και πιο παραγωγικούς τρόπους εργασίας που κυρίως την τελευταία δεκαετία με την βοήθεια των εφαρμογών της Τεχνολογίας της Πληροφορίας, όπως οι ισχυροί προσωπικοί υπολογιστές και τα δημόσια ευρυζωνικά δίκτυα δεδομένων, οι αλλαγές στην καθημερινότητα είναι εντυπωσιακές.

Είναι επίσης αναγνωρισμένη και αποδεδειγμένη διεθνώς η συνεισφορά των μέσων Τεχνολογίας Πληροφορικής και Επικοινωνίας στη βελτίωση της ποιότητας των ζωής του πολίτη και η εφαρμογή τους από Δημόσιους φορείς και οργανισμούς με στόχο την παροχή υπηρεσιών για τη εξυπηρέτηση των πολιτών να αυξάνει με ραγδαίους ρυθμούς.

Με δεδομένο την εξέλιξη της τεχνολογίας βλέπουμε ότι γίνεται δυνατή η άμεση επικοινωνία μεταξύ ιδιαίτερα απομακρυσμένων ανθρώπων ενώ η τηλεργασία, το ηλεκτρονικό εμπόριο, οι ηλεκτρονικές δημοπρασίες, οι ηλεκτρονικές τραπεζικές ή άλλου είδους συναλλαγές διευκολύνουν τις συναλλαγές των ανθρώπων οι οποίες πλέον δεν απαιτούν από τους συναλλασσόμενους να βρίσκονται στον ίδιο χώρο και σε καθορισμένες χρονικές στιγμές όπως ωράριο καταστημάτων για να διεκπεραιωθούν.

Ταυτόχρονα όμως με τις απαιτήσεις της σύγχρονης ζωής που έχουν με τη σειρά τους μεγαλώσει τις αξιώσεις των πολιτών για μεγαλύτερη ευελιξία και περισσότερες διευκολύνσεις στις συναλλαγές τους με τον δημόσιο τομέα ,η Πολιτεία είναι υποχρεωμένη να επαναπροσδιορίσει τις σχέσεις με τους πολίτες και τις επιχειρήσεις, καθώς και τις μεθόδους συνεργασίας των διαφόρων κρατικών λειτουργών και τους τρόπους εξυπηρέτησης, έτσι ώστε να γίνει πιο αποτελεσματική και περισσότερο ικανή για να ικανοποιήσει τις απαιτήσεις των πολιτών και της σύγχρονης εποχής.

Στις μέρες μας ένας όρος που χρησιμοποιείται συχνά είναι ο όρος της ψηφιακής κυβέρνησης και εννοούμε την κυβέρνηση εκείνη, η οποία εφαρμόζει τεχνολογίες πληροφορίας, συμβάλλει στην αύξηση του αριθμού των ψηφιακά διαθέσιμων Δημοσίων Υπηρεσιών ,στην εξασφάλιση της αδιάλειπτης υψηλής ποιότητας και ασφαλούς παροχής ψηφιακών υπηρεσιών του δημόσιου τομέα προς τους πολίτες καθώς και την εξασφάλιση των όρων εμπιστοσύνης και ασφάλειας κατά την χρήση των νέων τεχνολογιών.

Επιπλέον μια ψηφιακή κυβέρνηση είναι σε θέση να διεκπεραιώνει την πλειονότητα των συναλλαγών της με τους πολίτες, τις επιχειρήσεις και με τους λειτουργούς της, με ηλεκτρονικά μέσα και να συμβάλλει σε μια θεμελιώδη αλλαγή στην κουλτούρα της διακυβέρνησης, θέτοντας ως πρωταρχικό στόχο την εξυπηρέτηση των πολιτών και την άμεση προσφορά απλών και προσβάσιμων ηλεκτρονικών υπηρεσιών για όλους τους πολίτες αυξάνοντας όμως την αποτελεσματικότητα και τη διαφάνεια στις συναλλαγές μεταξύ του Δημοσίου Τομέα και των πολιτών.

Η μετεξέλιξη της παραδοσιακής κυβέρνησης σε ψηφιακή περιλαμβάνει τα εξής στάδια: το πρώτο στάδιο χαρακτηρίζει μια κυβέρνηση που χρησιμοποιεί τοποθεσίες στο Διαδίκτυο (web sites) για να παρέχει πληροφορίες στον κάθε ενδιαφερόμενο με το πιο συνηθισμένο περιεχόμενο αυτών των διαδικτυακών σελίδων είναι δίνει απαντήσεις στα πιο συχνά ερωτήματα του κοινού. Το δεύτερο στάδιο οδηγεί προς την ψηφιακή κυβέρνηση και χαρακτηρίζεται από την προσπάθεια της παραδοσιακής μορφής του κράτους να προσφέρει σε ψηφιακή μορφή σημαντικό αριθμό συναλλαγών οι οποίες μπορούν είτε να πραγματοποιούνται εξ ολοκλήρου ηλεκτρονικά, είτε να πραγματοποιούνται ηλεκτρονικά μέχρις ενός σημείου και να ολοκληρώνονται με παραδοσιακά μέσα και στη συνέχεια ο συναλλασσόμενος να είναι υποχρεωμένος να την εκτυπώσει, να την υπογράψει και να την αποστείλει ταχυδρομικά.

Στην περίπτωση που μια κυβέρνηση έχει φτάσει στο τρίτο στάδιο της πορείας προς τη ψηφιακή πραγματικότητα, έχει τη δυνατότητα να προσφέρει επιπλέον καινοτόμες μεθόδους διαλόγου με τους πολίτες και συμμετοχής στην πολιτική ζωή του τόπου ενώ τα κύρια χαρακτηριστικά της είναι ότι είναι περισσότερο προσβάσιμη, εξαιτίας των μέσων συμμετοχής και αλληλεπίδρασης που προσφέρει και περισσότερο διαφανής, εφόσον τα ηλεκτρονικά μέσα επικοινωνίας, όπως οι δικτυακές τοποθεσίες, κάνουν εύκολη την παρακολούθηση, από τους πολίτες, της πορείας του κυβερνητικού έργου.(Αλέξανδρος Κ. Σφάγγος, Διπλωματική Εργασία)

Όταν αναφερόμαστε τώρα στον όρο ηλεκτρονική Διακυβέρνηση (e-government) εννοούμε την ηλεκτρονική διακυβέρνηση όπου γίνεται η χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ICT – Information and Communications Technologies) και ιδιαίτερα του Διαδικτύου (Internet)από όλες τις δημόσιες υπηρεσίες και τους κρατικούς λειτουργούς με σκοπό να μετασχηματιστούν οι σχέσεις τους με τους πολίτες, τις επιχειρήσεις και άλλες υπηρεσίες της διοίκησης, με αποτέλεσμα την διεκπεραίωση και διευκόλυνση των ηλεκτρονικών συναλλαγών του πολίτη, τη βελτίωση της παραγωγικότητας των επιχειρήσεων και των οργανισμών μέσω χρήσης των ΤΠΕ ,τη βελτίωση της καθημερινής ζωής των πολιτών με

πρακτικούς τρόπους καθώς και την επίτευξη διαρκούς οικονομικής ανάπτυξης.

Οι δυνατότητες που προσφέρει η ηλεκτρονική διακυβέρνηση είναι μεγάλες γιατί μπορεί στην πραγματικότητα να μεταμορφώσει ολόκληρο το δημόσιο τομέα, καταπολεμώντας τα γραφειοκρατικά βάρη με εξοικονόμηση χρόνου και από πλευράς των οργανισμών και από πλευράς των επιχειρήσεων και των πολιτών ,περιορίζοντας τις αδυναμίες της διοικητικής δράσης , που δεν επέτρεψαν τις δημόσιες υπηρεσίες να ανταποκριθούν στις σύγχρονες προκλήσεις και στις αναπτυξιακές ανάγκες της χώρας .

Επιπλέον η εφαρμογή της ηλεκτρονικής διακυβέρνησης στο δημόσιο τομέα έχει τη δυνατότητα να υποστηρίξει την προσφορά περισσότερο ποιοτικών υπηρεσιών ενώ με τις μεθόδους αξιοποίησης των τεχνολογιών επικοινωνίας και πληροφορικής μπορεί να συμβάλλει στη βελτίωση της λειτουργίας του Κράτους και των υπηρεσιών του.

Βέβαια στην περίπτωση αυτή που εξετάζουμε η εφαρμογή κυρίως των τεχνολογιών πληροφορικής βεβαίως κρύβει οπωσδήποτε αρκετούς κινδύνους. Την αντιμετώπιση όμως αυτών των κινδύνων αναλαμβάνει η διαλειτουργικότητα των πληροφοριακών συστημάτων (systems interoperability) ιδιαίτερα εκεί όπου εμπλέκονται περισσότερες Δημόσιες Αρχές και Υπηρεσίες με την κατάλληλη κατάρτιση των στελεχών της Διοίκησης, οι οποίοι θα είναι οι χειριστές των νέων συστημάτων και υπηρεσιών και τους κατάλληλους μηχανισμούς ασφάλειας και κυρίως με τις έξυπνες κάρτες και τις Υποδομές Δημόσιου Κλειδιού θα δημιουργηθούν οι προϋποθέσεις προστασίας για την ασφάλεια των υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Αυτό συμβαίνει γιατί οι έξυπνες κάρτες σε συνδυασμό με τις Υποδομές Δημόσιου Κλειδιού κάτω από την εποπτεία του Κράτους, μπορούν να υλοποιήσουν την ηλεκτρονική ταυτότητα , η οποία αποτελεί το θεμέλιο της ασφάλειας στο πλαίσιο της ηλεκτρονικής διακυβέρνησης, γιατί επιτρέπει την ασφαλή πρόσβαση στις ηλεκτρονικές υπηρεσίες, την προστασία του ιδιωτικού χαρακτήρα των δεδομένων μέσω κρυπτογράφησης καθώς και τη δημιουργία και επαλήθευση ψηφιακών υπογραφών. (Αλέξανδρος Κ. Σφάγγος, Διπλωματική Εργασία)

Εξετάζοντας τώρα τις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης διαπιστώνουμε ότι διακρίνονται σε σχήματα ηλεκτρονικής διοικητικής εξυπηρέτησης των πολιτών (Government - to - Citizen (G2C) services) ή των επιχειρήσεων (Government - to- Business (G2B) Services) με άλλες δημόσιες υπηρεσίες (Government - to - Government (G2C) services) ,με στόχο την απλοποίηση των σχέσεων διοίκησης και εξυπηρετούμενων αποδεκτών ,όπου σε αυτή την

περίπτωση που εξετάζουμε έχουμε την προσέγγιση εκτίμησης του βαθμού ολοκλήρωσης της εξυπηρέτησης σε μία μοναδική στάση, που τα σχήματα ηλεκτρονικής εξυπηρέτησης διακρίνονται σε σχήματα πρώτης επαφής, σχήματα ποικιλίας συναλλαγών, σχήματα πρώτης στάσης και σχήματα μοναδικής στάσης. (ΣΤΑΣΗΣ Α- ΣΑΡΙΔΑΚΗΣΝ Ν Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

Στη συνέχεια τα σχήματα ηλεκτρονικής εξυπηρέτησης διαχωρίζονται σε σχήματα που έχουν σχέση με την πληροφόρηση, την επικοινωνία, την συναλλαγή και την διάχυση των υπηρεσιών και τέλος τα σχήματα ηλεκτρονικής εξυπηρέτησης που αναφέρονται στο πλαίσιο των 4 σταδίων (4- stage framework),που χρησιμοποιείται από την πρωτοβουλία eEurope και σχετ την αξιολόγηση της προόδου των υπηρεσιών ηλεκτρονικής διακυβέρνησης στα κράτη μέλη, σύμφωνα με το οποίο η ολοκλήρωση μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης διακρίνεται από τα στάδια της απλής πληροφόρησης, της μονόδρομης επικοινωνίας, της αμφίδρομης επικοινωνίας και της πλήρους εξυπηρέτησης συναλλαγών. (ΣΤΑΣΗΣ Α- ΣΑΡΙΔΑΚΗΣΝ Ν Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

Βέβαια τα αναμενόμενα οφέλη που προκύπτουν από την εισαγωγή σχημάτων ηλεκτρονικής διοικητικής συνεργασίας και εξυπηρέτησης είναι σαφώς επιχειρησιακά και περιλαμβάνουν τη βελτίωση της παροχής υπηρεσιών προς τους πολίτες, τη διευκόλυνση της αλληλεπίδρασης με τις επιχειρήσεις, την ενίσχυση των πολιτών μέσω της πρόσβασης σε πληροφοριακό περιεχόμενο και τέλος υπάρχει περισσότερο αποδοτική διαχείριση της διοικητικής λειτουργίας με αυξημένη διαφάνεια και μειωμένα λειτουργικά κόστη.

Γίνεται επίσης κατανοητό ότι για να υποστηριχθούν τέτοιες πρωτοβουλίες όπως είναι η εφαρμογή της ηλεκτρονικής διακυβέρνησης σε όλο το δημόσιο τομέα και να επιτευχθούν τα μέγιστα αποτελέσματα, απαραίτητη προϋπόθεση είναι η εξεύρεση και η εξοικονόμηση σημαντικών οικονομικών πόρων, η κατάλληλη τεχνολογία και μεταφορά τεχνογνωσίας, αλλά εκείνο το οποίο απαιτείται για την υποστήριξη των στόχων της ηλεκτρονικής διακυβέρνησης είναι κυρίως η αλλαγή στην νοοτροπία τόσο των δημόσιων λειτουργών, όσο και των πολιτών και των επιχειρήσεων.

Παρά τις δυσκολίες όμως που προκύπτουν για την επιτυχή εφαρμογή της ηλεκτρονικής διακυβέρνησης τα πλεονεκτήματα είναι σημαντικά γιατί με την υιοθέτηση της ηλεκτρονικής παροχής υπηρεσιών εξασφαλίζεται ο περιορισμός του κόστους λειτουργίας των δημόσιων υπηρεσιών, που αυτό σημαίνει ότι μετατρέπεται ενός σημαντικό μέρος των συναλλαγών, από παραδοσιακές σε ηλεκτρονικές και οι οποίες οδηγούν σε απλούστευση και επιτάχυνση των διοικητικών διαδικασιών, στην εν γένει αναδιοργάνωση των δημοσίων υπηρεσιών, στη μείωση του κόστους προμήθειας χαρτιού, των

εκτυπώσεων εντύπων, της ταχυδρομικής αποστολής εγγράφων και εξόδων προσωπικού και επομένως στην αύξηση της αποτελεσματικότητας στα πλαίσια των επιχειρησιακών διαδικασιών, στη βελτίωση της διοικητικής ικανότητας της Δημόσιας Διοίκησης και στην αποδοτική διαχείριση της διοικητικής λειτουργίας των υπηρεσιών του Δημόσιου Τομέα.

Ένα άλλο σημαντικό κίνητρο που προκύπτει από την επένδυση στις ηλεκτρονικές υπηρεσίες, είναι η καλύτερη εξυπηρέτηση των πολιτών γιατί οι δημόσιες υπηρεσίες ανταποκρίνονται άμεσα και αποτελεσματικά στις απαιτήσεις τους, περιορίζοντας σημαντικά τα γραφειοκρατικά τους βάρη, καταργώντας τις ουρές και την πολύωρη αναμονή αλλά κυρίως παρέχουν τη δυνατότητα της εξυπηρέτησης όλο το εικοσιτετράωρο.

Επίσης ένα άλλο σημαντικό κίνητρο είναι η επίτευξη της ισότιμης πρόσβασης των πολιτών στις δυνατότητες νέων τεχνολογιών με την περαιτέρω επέκταση ευρυζωνικών υποδομών και υπηρεσιών για τους πολίτες όλης της χώρας με εξασφάλιση των όρων εμπιστοσύνης και ασφάλειας στη χρήση νέων τεχνολογιών και διασφάλιση των συστημάτων από κακόβουλες επιθέσεις και η ενθάρρυνση της συμμετοχής των πολιτών, στις δημοκρατικές διαδικασίες γιατί ένα από τα χαρακτηριστικά της ηλεκτρονικής διακυβέρνησης είναι ότι κάνει πράξη την άμεση επικοινωνία με τους εκπροσώπους της πολιτικής εξουσίας, την ουσιαστική πληροφόρηση και τη συμμετοχή στα πολιτικά δρώμενα, όλα με αποκλειστική χρήση ηλεκτρονικών μέσων. (Διπλωματική Εργασία Αλέξανδρος Κ. Σφάγγος)

Τέλος ένα άλλο σημαντικό κίνητρο που προκύπτει από την επένδυση στις ηλεκτρονικές υπηρεσίες έχει σχέση με την ικανότητα του εκάστοτε δημόσιου ανώτατου λειτουργού να παρουσιάσει εικόνα σύγχρονης δημόσιας διοίκησης, καταπολεμώντας τη γραφειοκρατία και δημιουργώντας πιο αποδοτικές δομές.

Όμως η μεγαλύτερη πρόκληση για την ηλεκτρονική διακυβέρνηση είναι η ανατροπή του κλίματος αδιαφορίας και απαξίωσης των σημερινών πολιτών για όλα αυτά που διαδραματίζονται στους χώρους της πολιτικής και της διακυβέρνησης, γεγονός που εκφράζεται με σαφή τρόπο, με το αυξανόμενο ποσοστό αποχής από την εκλογική διαδικασία, η δυνατότητα γρήγορης και αποτελεσματικής ανάκτησης και μελέτης επίσημων εγγράφων, όπως προϋπολογισμών δημόσιων υπηρεσιών, της ισχύουσας νομοθεσίας, τα πρακτικά κοινοβουλευτικών συνεδριάσεων και πρακτικά έργου διαφόρων επιτροπών καθώς και η δυνατότητα ενημέρωσης και συμμετοχής στη συζήτηση που προηγείται της λήψης κάθε απόφασης με δημοκρατικό τρόπο, μέσω ηλεκτρονικών μέσων, όπως οι κυβερνητικές ιστοσελίδες, εξασφαλίζοντας προϋποθέσεις συμμετοχής στις διαδικασίες εύκολα και γρήγορα . (Αλέξανδρος Κ. Σφάγγος, Διπλωματική Εργασία)

Γίνεται, λοιπόν, σαφές ότι τα οφέλη για την ηλεκτρονική διακυβέρνηση είναι τόσο ισχυρά, ώστε να δικαιολογούν απολύτως τη σημαντική επένδυση σε χρόνο ,χρήμα και ανάπτυξη ανθρώπινου δυναμικού, που απαιτεί κάθε εγχείρημα ηλεκτρονικής διακυβέρνησης των υπηρεσιών του Δημόσιου Τομέα με στόχο πάντα τη βελτίωση της ποιότητας ζωής του πολίτη, την αύξηση της παραγωγικότητας και την επιτάχυνση της οικονομίας των σύγχρονων κρατών.

9.2 Έρευνα του Παρατηρητηρίου

Μια έρευνα του Παρατηρητηρίου που πραγματοποιήθηκε για την Κοινωνία της Πληροφορίας στην ελληνική δημόσια Διοίκηση, κατά το χρονικό διάστημα μεταξύ Νοεμβρίου 2006 και Απριλίου 2007 έδειξε ότι οι πιο διαδεδομένες εφαρμογές πληροφορικής που εφαρμόζονταν στις Δημόσιες Υπηρεσίες και τους Οργανισμούς αφορούσαν την κάλυψη μόνο των βασικών λειτουργιών των οργανισμών.

Τα συμπεράσματα της ίδιας έρευνας έδειξαν ότι το 53% των δημοσίων φορέων είχε στη διάθεσή του ηλεκτρονικό ταχυδρομείο (e-mail) και ότι το 60% χρησιμοποιούσε ηλεκτρονικό πρωτόκολλο ενώ μόνο το 17% από τους δημόσιους φορείς χρησιμοποιούσε κάποια εφαρμογή ροής της εργασίας (workflow) και διαχείρισης περιεχομένου (content management) εφαρμογές που είναι απαραίτητες για την υποστήριξη της αποτελεσματικής επεξεργασίας αιτημάτων πολιτών.(http:www.myphone.gr/forum)

Στη συνέχεια της ίδιας έρευνας σχετικά με τον εξοπλισμό υποστήριξης των ηλεκτρονικών υπηρεσιών έδειξε ότι σχεδόν οι περισσότεροι εργαζόμενοι στη δημόσια διοίκηση διέθεταν υπολογιστή. Πιο συγκεκριμένα το 92% στην κεντρική διοίκηση και το 97,6% στους οργανισμούς τοπικής αυτοδιοίκησης διέθεταν υπολογιστή ενώ το 50% των υπολογιστών στους οργανισμούς της τοπικής αυτοδιοίκησης ήταν παλιάς τεχνολογίας.

Επίσης η ίδια έρευνα έδειξε ότι το 37% των εργαζομένων στην κεντρική διοίκηση και το 28.8% στους ΟΤΑ γνώριζε βασικές δεξιότητες στην πληροφορική και διέθετε πιστοποιητικό γνώσης χειρισμού υπολογιστών με τα στοιχεία να δείχνουν ότι οι αρκετοί εργαζόμενοι απέφευγαν να παρακολουθούν εκπαιδευτικά σεμινάρια, που διοργανώνονταν για να προσαρμοστούν και να αποκτήσεις βασικές γνώσεις χειρισμού ενός ηλεκτρονικού υπολογιστή απαραίτητες για την ηλεκτρονική διεκπεραίωση των διαφόρων αιτημάτων. (http:www.myphone.gr/for)

Επίσης ένα άλλο στοιχείο που έδειξε η παραπάνω έρευνα σχετικά με τη διασυνδεσιμότητα των εφαρμογών μεταξύ των δημόσιων υπηρεσιών εκτός από κάποιες εξαιρέσεις, δεν υπήρχε συγκεκριμένη διασύνδεση μεταξύ της

κεντρικής διοίκησης και της τοπικής αυτοδιοίκησης για τη συστηματική ροή πληροφοριών με συγκεκριμένο σύστημα πληροφορικής και ότι σε επίπεδο προσφοράς ηλεκτρονικών υπηρεσιών προς τους πολίτες από το σύνολο των 20 βασικών δημοσίων υπηρεσιών οι οποίες θα υπόκεινταν στη διαδικασία αξιολόγησης ετησίως από τα κράτη μέλη της ΕΕ – μέχρι το τέλος του 2006 ήταν διαθέσιμες πλήρως ηλεκτρονικά μόνο οι 8 και ότι το 40% ποσοστό ήταν κοντά στο μέσο όρο .

Αντίθετα για το έτος 2005 το αντίστοιχο ποσοστό προσφοράς ηλεκτρονικών υπηρεσιών ήταν μόνο το 25% νούμερο το οποίο μεταφράζεται ότι μόνο 5 υπηρεσίες ήταν πλήρως ηλεκτρονικά διαθέσιμες και μόλις το 8% του πληθυσμού χρησιμοποιούσε το Διαδίκτυο για τις συναλλαγές με το δημόσιο, σε αντίθεση με το αντίστοιχο ποσοστό για τις επιχειρήσεις (με 10 + εργαζόμενους) το οποίο άγγιζε το 71%. (http:www.myphone.gr/forum)

Σύμφωνα με το ΕΣΠΑ 2007-2013**,** η θέση της Ελλάδας σχετικά με τη συμμετοχή της στις τεχνολογίες πληροφορικής και επικοινωνιών, και συγκριτικά με τις χώρες της ΕΕ-25 όσο και παγκοσμίως, διαπιστώνουμε ότι βρίσκεται σε χαμηλότερα επίπεδα από τα αναμενόμενα και κυρίως την τελευταία δεκαετία, οι νέες τεχνολογίες δεν συνέβαλαν σε μμεγάλο βαθμό στη βελτίωση της παραγωγικότητας της ελληνικής οικονομίας και στη βελτίωση της ποιότητας ζωής των πολιτών.

Παρόλο που η κατάσταση στο χώρο της Τεχνολογίας στην Ελλάδα δεν βρίσκεται σε προχωρημένο επίπεδο, εντούτοις εκφράζεται μία σημαντική δυναμική στη συμβολή των ΤΠΕ στο ΑΕΠ (οι συνολικές επενδύσεις στον κλάδο πληροφορικής και επικοινωνιών βρίσκονται στο 80 % του μέσου όρου ΕΕ) και στη διείσδυση των ευρυζωνικών δικτύων, οι οποίοι τα τελευταία κινούνται σε χαμηλούς βαθμούς (0,7% το 2005 έναντι περίπου 7% του μέσου όρου της ΕΕ-25) και η απασχόληση σε τομείς υψηλής τεχνολογίας είναι ακόμη χαμηλή (30% της ΕΕ) ενώ οι επιδόσεις στην εκπαίδευση των νέων και στην τριτοβάθμια εκπαίδευση είναι ικανοποιητικές και προσεγγίζουν τον μέσο όρο ΕΕ (θετικό στοιχείο για το μέλλον). (ΕΣΠΑ 2007-2013)

9.3 Αδυναμίες

Τέλος πρέπει να αναφέρουμε ότι η τεράστια πρόοδος των τεχνολογιών επικοινωνίας και πληροφορικής, η διάδοση των ηλεκτρονικών συναλλαγών, η ανάγκη για την ηλεκτρονική οργάνωση, τόσο των επιχειρήσεων, όσο και του κράτους και οι ογκώδεις βάσεις δεδομένων (data warehouses) που προκύπτουν, τα νέα δίκτυα επικοινωνιών, όπως το Internet και η ταχύτατη μετάδοση των πληροφοριών σε παγκόσμιο επίπεδο, παρέχουν αυξημένες δυνατότητες συλλογής, αποθήκευσης, διασύνδεσης και επεξεργασίας

δεδομένων ιδιωτικού και ευαίσθητου χαρακτήρα αλλά ταυτόχρονα θέτουν σε νέους κινδύνους την ιδιωτική ζωή των πολιτών.

Αυτό συμβαίνει κατά τη διαδικασία μετάδοσης προσωπικών δεδομένων διαμέσου δημόσιων δικτύων δεδομένων, όπως το Internet, όπου η αποθήκευσή τους γίνεται σε δημόσια προσβάσιμα υπολογιστικά συστήματα και σε συνδυασμό με την αυξημένη πιθανότητα υποκλοπής των δεδομένων αυτών, να δυσχεραίνονται οι προσπάθειες προστασίας και σεβασμού της ιδιωτικής ζωής των πολιτών, που αποτελούν μια από τις θεμελιώδεις αρχές κάθε δημοκρατικής κοινωνίας με αποτέλεσμα κατά την πραγματοποίηση των ηλεκτρονικών συναλλαγών, καθ' όλο το εικοσιτετράωρο, να προκύπτουν ελκυστική περιστατικά απάτης μικρής ή μεγάλης κλίμακας.

Επομένως οι απειλές που αντιμετωπίζει κάθε εγχείρημα ηλεκτρονικής διακυβέρνησης είναι σημαντικές και συνεπώς και προστασίας αντίστοιχα υψηλές πρέπει να είναι και οι απαιτήσεις μηχανισμών ασφάλειας, ώστε να είναι ικανές να εγγυηθούν την αυθεντικότητα της ταυτότητας των συναλλασσόμενων, την ακεραιότητα και την εμπιστευτικότητα του περιεχομένου κάθε συναλλαγής Αλέξανδρος Σφάγος , Διπλωματική εργασία)

9.4 Παρεχόμενες Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

Στην Ελλάδα οι ηλεκτρονικές υπηρεσίες που παρέχονται στους πολίτες (ανάλογα από το ποιος είναι ο Πάροχος και ποιος ο τελικός χρήστης) διακρίνονται σε τέσσερες κατηγορίες ή επίπεδα ανάλογα με το βαθμό ολοκλήρωσης της υπηρεσίας , που μπορεί να πραγματοποιηθεί ηλεκτρονικά. Έτσι με βάση το παραπάνω κριτήριο έχουμε τις Πληροφοριακές Υπηρεσίες (Information), οι οποίες παρέχουν πληροφοριακό υλικό σχετικά με τον τρόπο διεκπεραίωσης της υπηρεσίας, όπως τα δικαιολογητικά που πρέπει να προσκομιστούν, τους φορείς που εμπλέκονται για την ολοκλήρωση της υπηρεσίας, τη σειρά εκτέλεσης των συναλλαγών, που περιλαμβάνει η υπηρεσία .

Μια άλλη κατηγορία ηλεκτρονικών υπηρεσιών είναι οι Επικοινωνιακές Υπηρεσίες (Interaction), οι οποίες παρέχουν πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης μιας υπηρεσίας καθώς και επίσημο υποστηρικτικό υλικό (πρότυπα αιτήσεων, βεβαιώσεων κ.ά)που οι χρήστες μπορούν να έχουν στη διάθεσή τους μέσω του προσωπικού τους υπολογιστή έχοντας παράλληλα τη δυνατότητα να το τυπώσουν και να το χρησιμοποιήσουν κατά τη συναλλαγή του με το φορέα σε επίπεδο φυσικής παρουσίας.

Επίσης στις ηλεκτρονικές υπηρεσίες ανήκουν και οι λεγόμενες Διαδραστικές Υπηρεσίες (Two- way interaction),που εκτός από πληροφορίες έχουν τη δυνατότητα να προσφέρουν online φόρμες για συμπλήρωση και

ηλεκτρονική αποστολή και περιλαμβάνουν και online υποβολή στοιχείων από μέρους του χρήστη, ενώ παράλληλα προϋποθέτουν και μηχανισμό αναγνώρισης, ταυτοποίησης και προστασίας των δεδομένων που αποστέλλει ο χρήστης της υπηρεσίας .

Τέλος τελευταία κατηγορία των ηλεκτρονικών υπηρεσιών είναι οι Συναλλακτικές υπηρεσίες (Transaction), οι οποίες εκτός από τις φόρμες αποστολής στοιχείων, υποστηρίζουν λειτουργίες όπου ο χρήστης ολοκληρώνει τις ηλεκτρονικές του συναλλαγές. (ΣΤΑΣΗΣ Α- ΣΑΡΙΔΑΚΗΣΝ Ν Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

Από τα παραπάνω γίνεται κατανοητό ότι η ταχύτατη διείσδυση και εξάπλωση των Τεχνολογιών και Τηλεπικοινωνιών της Πληροφορικής και ιδιαίτερα του Διαδικτύου και σε συνδυασμό με τις νέες αντιλήψεις για το ρόλο του Κράτους και την αλλαγή κουλτούρας και νοοτροπίας των δημοσίων λειτουργών επέφεραν δραματικές αλλαγές στον τρόπο οργάνωσης και λειτουργίας της δημόσιας διοίκησης.

Βέβαια οι παραπάνω αλλαγές στον τρόπο λειτουργίας και οργάνωσης της νέας εικόνας γίνονται και σε συνδυασμό με τα πρότυπα που διεθνώς αναπτύσσονται για την λεγόμενη Ανταποκριτική Διοίκηση, η οποία θέτει νέες αξίες και νέα πρότυπα εξυπηρέτησης του Κοινού, τη Διοίκηση των Διαδικασιών που εξετάζει τις από άκρη σε άκρη διαδικασίες και την Ηλεκτρονική Διακυβέρνηση, που χρησιμοποιεί το Διαδίκτυο για να παράγει και να διαθέτει πληροφορίες, υπηρεσίες και προϊόντα στους πολίτες και τις επιχειρήσεις.

Τέλος πρέπει να τονίσουμε ότι οι δημόσιες διοικήσεις αντέγραψαν σε ένα μεγάλο βαθμό τον τρόπο οργάνωσης και λειτουργίας των παρεχόμενων υπηρεσιών του ιδιωτικού τομέα όπως την Διοίκηση Ολικής Ποιότητας και τον Ανασχεδιασμό των Επιχειρησιακών Διαδικασιών που έχουν ως επίκεντρο την εξυπηρέτηση των πελατών και τις διαδικασίες διευκόλυνσης των οποιοδήποτε συναλλαγών. (ΣΤΑΣΗΣ Α- ΣΑΡΙΔΑΚΗΣΝ Ν Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

10.ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

10.1 Εισαγωγή

Περίπου στα τέλη του 1990 προέκυψε η ανάγκη για την εφαρμογή ενός Πλαισίου Διαλειτουργικότητας με τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών και με βασική προϋπόθεση την ομαλή διακίνηση πληροφοριών μεταξύ των πληροφοριακών συστημάτων των εμπλεκόμενων φορέων (κεντρική διοίκηση, τοπική αυτοδιοίκηση, πολίτες, επιχειρήσεις, δημόσιες διοικήσεις άλλων κρατών, διεθνών οργανισμών) μέσα από τη συνεργασία των φορέων για την Ηλεκτρονική Διακυβέρνηση που απώτερο στόχο είχαν την ταχύτερη εξυπηρέτηση των πολιτών και επιχειρήσεων και διευκόλυνση των συναλλαγών από τις Δημόσιες Υπηρεσίες .

Στη χώρα μας το Ελληνικό Πλαίσιο Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης δημιουργήθηκε το 2002 και ως Διαλειτουργικότητα (interoperability) ορίστηκε η ικανότητα μεταφοράς και χρησιμοποίησης της πληροφορίας μεταξύ των διαφόρων οργανισμών σε επίπεδο συστημάτων πληροφορικής με ένα ομοιογενές και αποτελεσματικό τρόπο με σκοπό την εξυπηρέτηση των πολιτών .

Στη συνέχεια κατά το 2004 όταν η Ιρλανδία ήταν επικεφαλής της Ευρωπαϊκής Ένωσης οι χώρες της Ευρωπαϊκής Ένωσης συμφώνησαν στην επέκταση του ορισμού της Διαλειτουργικότητας δίνοντας περισσότερη έμφαση στην επιχειρησιακή και οργανωτική διάσταση της συνεργασίας μεταξύ των φορέων πέραν της τεχνολογικής και κατέληξαν να ορίζεται ως Διαλειτουργικότητα η δυνατότητα ενός συστήματος ή μίας διαδικασίας να μοιράζεται και να χρησιμοποιεί πληροφορία ή δυνατότητες ενός άλλου συστήματος ή διαδικασίας (European Public Administration Network).

Έτσι γίνεται κατανοητό ότι η Διαλειτουργικότητα στοχεύει στη διευκόλυνση της επικοινωνίας των πληροφοριακών συστημάτων του δημοσίου μεταξύ τους, με τον πολίτη, τις επιχειρήσεις και στο άμεσο μέλλον με άλλες κυβερνήσεις και διεθνείς οργανισμούς στην ανάπτυξη και υιοθέτηση από ολόκληρο το Δημόσιο τομέα του Πλαισίου Διαλειτουργικότητας και στη διευκόλυνση της ανάπτυξης υποδομών ηλεκτρονικής διακυβέρνησης που θα προσφέρουν αποτελεσματικότερες και με χαμηλότερο κόστος υπηρεσίες.

Επομένως η Διαλειτουργικότητα η οποία διακρίνεται σε τρία επίπεδα: το Οργανωτικό, το Επιχειρησιακό, και το Εννοιολογικό θα πρέπει να εξασφαλίζεται μεταξύ όλων των δημοσίων οργανισμών (Υπουργεία, Νομαρχίες, Δήμοι, Περιφέρειες), ιδιωτικών επιχειρήσεων, του πολίτη, καθώς και μεταξύ συστημάτων άλλων χωρών και να καλύπτει ένα μεγάλο αριθμό

τομέων της οικονομίας για την επιτυχή υλοποίηση της πολιτικής ηλεκτρονικής διακυβέρνησης. (ΣΤΑΣΗΣ Α- ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

Προς αυτή την κατεύθυνση κινείται και το πλαίσιο της στρατηγικής για την Ηλεκτρονική Διακυβέρνηση στο Επιχειρησιακό Πρόγραμμα της Κοινωνίας της Πληροφορίας όπου δίδεται ιδιαίτερη έμφαση στην ανάπτυξη υπηρεσιών διαλειτουργικής εξυπηρέτησης, δηλαδή στην ανάπτυξη των απαραίτητων συνεργασιών μεταξύ των διοικητικών υπηρεσιών της Ελληνικής Δημόσιας Διοίκησης οι οποίες παράγουν πρωτογενώς υπηρεσίες καθώς και των απαραίτητων διεπαφών μεταξύ των πληροφοριακών συστημάτων. (ΣΤΑΣΗΣ Α-ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

10.2 Οργανωτική Διαλειτουργικότητα

Όταν αναφερόμαστε στην οργανωτική διαλειτουργικότητα εννοούμε αλλαγή στον τρόπο οργάνωσης της Δημόσιας Διοίκησης προκειμένου οι παρεχόμενες υπηρεσίες ηλεκτρονικής διακυβέρνησης να γίνεται με στόχο την εξυπηρέτηση και τη διευκόλυνση των πολιτών(πολιτοκεντρική προσέγγιση), με στόχο την επανεξέταση των βασικών διαδικασιών και συναλλαγών με τους πολίτες και επιχειρήσεις, των επιχειρησιακών δομών, κανόνων λειτουργίας και ρόλων μέσα και έξω από κάθε δημόσιο φορέα, προκειμένου να υποστηρίζεται η συνεργασία των εμπλεκόμενων φορέων ,των συστημάτων που μεσολαβούν στην επικοινωνία με τον πολίτη επιχείρηση καθώς και επανεξέταση όλων των οργανωτικών σχημάτων των δημοσίων φορέων (νέα τμήματα, κατάργηση παλαιών κ.ά), του τρόπου αντιμετώπισης των προβλημάτων κατά την μεταβατική περίοδο όπως είναι διαχείριση αλλαγών.

Οπωσδήποτε όλες αυτές οι μεταβολές συνεπάγονται περιορισμός του κόστους λειτουργίας του Δημοσίου Τομέα, αύξηση της αξιοποίησης των δημοσίων πόρων, αλλαγές του θεσμικού πλαισίου και πρωτοβουλίες για την προσαρμογή της νομοθεσίας, ενώ η εφαρμογή τους θα πρέπει να υποστηρίζεται και να ελέγχεται από όλη τη Δημόσια Διοίκηση. (ΣΤΑΣΗΣ Α-ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

10.3 Επιχειρησιακή Διαλειτουργικότητα

Στο επίπεδο της Επιχειρησιακής Διαλειτουργικότητας εξετάζονται οι φορείς που συνεργάζονται για την παροχή μιας υπηρεσίας και γίνεται προσδιορισμός των επιχειρησιακών αναγκών συνεργασίας όπως για να επιτευχθεί η επιχειρησιακή Διαλειτουργικότητα των ΚΕΠ με άλλους φορείς θα πρέπει να παρέχεται η δυνατότητα διασύνδεσης τόσο σε επιχειρησιακό, όσο και σε τεχνολογικό επίπεδο με πληροφοριακά συστήματα του Δημοσίου

Τομέα. (ΣΤΑΣΗΣ Α- ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

Βέβαια οι παρεχόμενες υπηρεσίες έχουν περιθώρια βελτίωσης ιδιαίτερα στο κομμάτι της ηλεκτρονικής αυθεντικοποίησης και όσο αφορά τις υπηρεσίες που δεν έχουν φτάσει στο υψηλότερο σημείο ηλεκτρονικής ολοκλήρωσης θα πρέπει να γίνουν ενέργειες για την περαιτέρω ηλεκτρονικοποίησή τους, ενώ για τις υπηρεσίες εκείνες που είναι πλήρως ηλεκτροποιημένες, θα πρέπει να γίνουν σημαντικές βελτιώσεις αναφορικά με την λειτουργικότητά τους.

Αντίθετα για τις υπηρεσίες που δεν έχουν μπει στη διαδικασία της ηλεκτρονικοποίησης τους, θα πρέπει να σχεδιαστεί εκ νέου η ηλεκτρονική τους παροχή βάσει ενιαίων προδιαγραφών και να καθοριστεί το πλαίσιο ανάπτυξης και παροχής των υπηρεσιών λαμβάνοντας υπόψη τις απαιτήσεις της Διαλειτουργικότητας, το οποίο θα δίνει προτεραιότητα σε συγκεκριμένες υπηρεσίες αλλά και στις γενικότερες αλλαγές που πρέπει να γίνουν για την παροχή τους, σε θεσμικό και λειτουργικό επίπεδο. (ΣΤΑΣΗΣ Α- ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

10.4 Σημασιολογική – Τεχνολογική Διαλειτουργικότητα

Στο επίπεδο της Σημασιολογικής – Τεχνολογικής Διαλειτουργικότητας είναι η υιοθέτηση των προδιαγραφών του Internet και του World Web (WWW)για όλα τα συστήματα πληροφορικής της Δημόσιας Διοίκησης ενώ υπάρχει η στρατηγική απόφαση της υιοθέτησης των XML και XSL ως τα βασικά πρότυπα για την ολοκλήρωση, ανταλλαγή, πρόσβαση και διαχείριση δεδομένων με στόχο την μείωση του κόστους και του ρίσκου των συστημάτων ανάπτυξης πληροφορικής της Δημόσιας Διοίκησης.

Επιπλέον σε αυτό το επίπεδο της Διαλειτουργικότητας καθορίζονται οι πολιτικές για τον προσδιορισμό και την υλοποίηση των μεταδιδομένων (Metadata) σε όλο το Δημόσιο τομέα προκειμένου να επιτραπεί στους πολίτες η πρόσβαση στις προσφερόμενες κυβερνητικές πληροφορίες και πόρους σε συνδυασμό με την κατάλληλη θεσμική και οργανωτική υποστήριξη, την παραγωγή οδηγιών βέλτιστων πρακτικών και υιοθέτησή τους καθώς και την παραγωγή κοινώς αποδεκτών και ανοικτώνXML Medata και Schemas (ΣΤΑΣΗΣ Α- ΚΑΚΛΑΜΑΝΗΣ Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση ΕΚΔΔ-ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ)

11.ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΟΙΚΗΣΗ

11.1 Εισαγωγή

Την τελευταία δεκαετία η αλματώδης ανάπτυξη των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών έχει επιφέρει μεγάλες και σημαντικές κοινωνικές, οικονομικές και οργανωτικές αλλαγές διαμορφώνοντας μία καινούργια μορφή κοινωνίας που ονομάζεται κοινωνία της πληροφορίας. (www.infolaw.gr)

Απέναντι σε αυτές τις εξελίξεις η Ευρωπαϊκή Ένωση δεν έχει μείνει αδιάφορη και με το κείμενο επί του Θέματος στο European Governance : A white paper [COM 2001, 25.07.01] αναφέρεται ότι η Ευρωπαϊκή Επιτροπή αναγνωρίζει ότι η ποιότητα της Δημοκρατίας εξαρτάται από την δυνατότητα του λαού να συμμετέχει στον δημόσιο διάλογο και να επηρεάζει τη λήψη αποφάσεων σε κάθε επίπεδο.(www.infolaw.gr)

Στην Ελλάδα το νέο Σύνταγμα μετά την αναθεώρηση του 2001 στο αρ. 5 προβλέπει το δικαίωμα κάθε ατόμου να συμμετέχει στην Κοινωνία της Πληροφορίας και επομένως αποτελεί υποχρέωση του Κράτους η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά καθώς και της παραγωγής και ανταλλαγής τους.

Οπωσδήποτε η εισαγωγή των νέων τεχνολογιών στους μηχανισμούς του Κράτους προκαλεί σαφώς μία σειρά από αλλαγές αλλά και προκλήσεις που πρέπει να αντιμετωπιστούν γιατί ο εκσυγχρονισμός των δημοσίων υπηρεσιών προϋποθέτει την ενσωμάτωση στη δράση τους των νέων τεχνολογιών και την μετάβαση από την κλασσικού τύπου δημόσια διοίκηση στην Ηλεκτρονική Διοίκηση.

Πιο συγκεκριμένα τα επίπεδα υλοποίησης της ηλεκτρονικής διοίκησης έχουν σχέση με την Εσωτερική οργάνωση του φορέα έτσι ώστε να δημιουργηθεί η κατάλληλη υποδομή με την προμήθεια του απαραίτητου λογισμικού για εφαρμογές γραφείου, διαδικτυακή σύνδεση του υπάρχοντος εξοπλισμού, την καθιέρωση ηλεκτρονικού πρωτοκόλλου, τον ανασχεδιασμός της εσωτερικής ροής των εγγράφων και των εσωτερικών διαδικασιών (business procew Re-Engineering), τη δημιουργία Intranet, τη δημιουργία «πύλης» της διοίκησης (portal),τις ψηφιακές υπογραφές Smart cards και χρήση της ψηφιακής τηλεόρασης για πρόσβαση στην «πύλη» του δημοσίου.

Ο πιο σημαντικός όμως στόχος της ηλεκτρονικής Διοίκησης ήταν και είναι η παροχή δημοσίων υπηρεσιών on line με την εκτεταμένη χρήση του διαδικτύου (internet) με σκοπό τη βελτίωση της επικοινωνίας μεταξύ των δημοσίων υπηρεσιών και τη βελτίωση εξυπηρέτησης του πολίτη και επομένως να μιλάμε για μία σύγχρονη μορφή δημόσιας διοίκησης που ονομάζεται ηλεκτρονική διοίκηση(e – government).

Λέγοντας λοιπόν ηλεκτρονική διοίκηση εννοούμε μία νέα μορφή Δημόσιας Διοίκησης ,η οποία χρησιμοποιεί ευρύτατα τις νέες τεχνολογίες της πληροφορικής και των τηλεπικοινωνιών ώστε να επιτυγχάνεται η ποιοτική αναβάθμιση της εξυπηρέτησης των πολιτών και η βελτίωση των συνθηκών εργασίας των δημοσίων υπαλλήλων.

Ήδη η Ελλάδα έχει ενσωματώσει στο εθνικό της δίκαιο την Ευρωπαϊκή Οδηγία 99/93 του Ευρωπαϊκού Κοινοβουλίου, την οποία την ακολούθησαν και τα άλλα ευρωπαϊκά κράτη και με την ψήφιση του Προεδρικού Διατάγματος 150/12-06-2001 θεσμοθετήθηκε το νομικό πλαίσιο για τη δημιουργία υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) στοιχείο απαραίτητο για την εφαρμογή της ηλεκτρονικής υπογραφής στις υπηρεσίες του ευρύτερου Δημόσιου Τομέα, καθώς ορίστηκε και το πλαίσιο των Αρχών Πιστοποίησης ή των Παρόχων Υπηρεσιών Πιστοποίησης, που θα την υποστηρίξουν.

Η εφαρμογή της ηλεκτρονικής υπογραφής μπορεί να συνδυαστεί με τις έξυπνες κάρτες (smart cards), οι οποίες έχουν τα εξής χαρακτηριστικά: είναι φορητές και έχουν μνήμη δεδομένων και μικροεπεξεργαστή, μπορούν να αποθηκεύουν διάφορα στοιχεία καθώς και την ηλεκτρονική υπογραφή, ενώ η εφαρμογή με τη μορφή πιλοτικών προγραμμάτων έξυπνων καρτών έχει ήδη ξεκινήσει από τη Γενική Γραμματεία Κοινωνικών Ασφαλίσεων καθώς και από το Υπουργείο Υγείας-Πρόνοιας. .(www.infolaw.gr)

11.2 Νόμος 2672/1998

Σαν συνέχεια του προεδρικού διατάγματος 150/2001 έρχεται Προεδρικό Διάταγμα του Υπουργείου Μεταφορών και Επικοινωνιών με αντικείμενο τη ρύθμιση θεμάτων που αφορούν τη διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ δημοσίων υπηρεσιών καθώς και μεταξύ αυτών και φυσικών ή νομικών προσώπων, όπου θα εκδοθεί βάσει του αρ. 14, παρ. 19 και 20 του ν. 2672/1998 και αναφέρεται γενικά σε θέματα διακίνησης εγγράφων με fax και e-mail.

Το σχέδιο του Προεδρικού Διατάγματος αποσκοπεί στη ρύθμιση των θεμάτων που προκύπτουν από τη διακίνηση αποφάσεων, πιστοποιητικών και βεβαιώσεων με ηλεκτρονικό ταχυδρομείο με ψηφιακή υπογραφή, ενώ προβλέπεται επίσης η δυνατότητα διακίνησης εγγράφων χωρίς ψηφιακή υπογραφή, χωρίς όμως να παρέχεται η δυνατότητα σ'αυτήν την περίπτωση να παράγονται έννομα αποτελέσματα ή να ασκούνται δικαιώματα. (Νόμος 2672/1998)

11.3 Ηλεκτρονική Διαχείριση Αρχειοθέτηση των Εγγράφων

Με την "Ηλεκτρονική Διαχείριση Αρχειοθέτηση των Εγγράφων" προωθείται η ορθολογική οργάνωση και διοίκηση των αρχείων των υπηρεσιών με συνέπεια την αποτελεσματικότερη και αποδοτικότερη λειτουργία της Δημόσιας Διοίκησης ,την επαρκέστερη και ταχύτερη εξυπηρέτηση των πολιτών καθώς και τη διευκόλυνση των δημοσίων υπαλλήλων στη διεξαγωγή της εργασίας τους και την εκκαθάριση των αρχείων, η οποία επιβάλλεται να γίνεται περιοδικά από τις δημόσιες υπηρεσίες. (έγγραφο του ΥΠ.ΕΣ.Δ.Δ.Α)

Είναι γνωστό επίσης ότι ο μεγάλος όγκος των εγγράφων που διακινούνται από τις υπηρεσίες (Εισερχόμενα - Εξερχόμενα) και η παντελής έλλειψη συστημάτων διαχείρισής τους σε συνδυασμό με τον περιορισμένο και διαρκώς συρρικνούμενο χώρο αποθήκευσής τους, καθιστούν επιτακτική την ανάγκη λήψης μέτρων προς την κατεύθυνση της εφαρμογής ενός Ολοκληρωμένου Συστήματος Ηλεκτρονικής Διαχείρισης Εγγράφων, το οποίο θα εξασφαλίζει: την ταξινόμηση ως προς οποιοδήποτε από τα στοιχεία των εγγράφων, την εισαγωγή εγγράφων σε χαρτί μέσω scanner, επεξεργαστών κειμένου, λογιστικών φύλλων., την συμπίεση (compression) των εικόνων για αποτελεσματική διαχείριση των μέσων αποθήκευσης, την παρακολούθηση της ροής των εγγράφων και το User interface φιλικό στο χρήση . (έγγραφο του ΥΠ.ΕΣ.Δ.Δ.Α)

Στη συνέχεια την ηλεκτρονική διαχείριση θα εξασφαλίζεται η ελεύθερη αναζήτηση των εγγράφων με πολλαπλούς τρόπους ,η ανάκτηση των εγγράφων ,που το περιεχόμενο τους είναι σχετικό με την έκφραση αναζήτησης ,η ταξινόμηση ως προς κάποιο στοιχείο παραδείγματος χάρη κατηγορία, αριθμός πρωτοκόλλου, ημερομηνία κ.λπ., η εμφάνιση των εγγράφων είτε ολόκληρων είτε σε μορφή λίστας, η επιλογή καταλόγου εμφάνισης, η ενημέρωση και η ροή εγγράφων σχετικά με την αποστολή σε χρήστη, ομάδα χρηστών, τη δυνατότητα παρακολούθησης και καταγραφής ενεργειών όπου περιγράφεται κάθε βήμα, την επιλογή ενέργειας από λίστα, τη δυνατότητα σύνδεσης με υποσύστημα ψηφιακής υπογραφής και τέλος θα εξασφαλίζεται η ασφάλεια και ο έλεγχος των δεδομένων με την υποστήριξη διαφορετικών επιπέδων πρόσβασης.

Αναμφίβολα η υιοθέτηση εφαρμογής ενός συστήματος ηλεκτρονικής διαχείρισης εγγράφων προσφέρει τόσο στην υπηρεσία όσο και στους υπαλλήλους τα ακόλουθα πλεονεκτήματα: την ελαχιστοποίηση της διακίνησης έντυπου υλικού μεταξύ των υπηρεσιακών μονάδων του οργανισμού, την αυτοματοποίηση της διακίνησης εγγράφων από την είσοδό τους στην υπηρεσία έως την έξοδο (εισερχόμενα - εξερχόμενα), την βελτίωση της ταχύτητας αναζήτησης, αποστολής και λήψης εγγράφων καθώς

και την ελαχιστοποίηση των τυχόν καθυστερήσεων λαμβάνοντας υπόψη τον όγκο των διακινούμενων εγγράφων.

Επίσης Ηλεκτρονική Αρχειοθέτηση προσφέρει: την ασφαλέστερη αποθήκευση και διασφάλιση του περιεχομένου σημαντικών εγγράφων, τη μείωση των απαιτούμενων χώρων αποθήκευσης, την αποδοτικότερη και ευέλικτη πρόσβαση σε αρχειοθετημένα έγγραφα, την αυτοματοποίηση της ανάθεσης και παρακολούθησης της υλοποίησης εργασιών της υπηρεσίας, και την ποιοτική αναβάθμιση των υπηρεσιών. (έγγραφο του ΥΠ.ΕΣ.Δ.Δ.Α)

11.4 Ηλεκτρονικό έγγραφο

Επομένως ως ηλεκτρονικό έγγραφο θα μπορούσε να οριστεί κάθε έγγραφο που έχει το χαρακτηριστικό ότι δημιουργείται με τη βοήθεια της ηλεκτρονικής τεχνολογίας, που έχουν εξαρχής ηλεκτρονική υπόσταση αλλά και τα έγγραφα που έχουν υλική υπόσταση αλλά το περιεχόμενό τους αποτυπώνεται με τη βοήθεια της ηλεκτρονικής τεχνολογίας. Έτσι γίνεται φανερό ότι η ειδοποιός διαφορά του ηλεκτρονικού εγγράφου από το παραδοσιακό τύπου έγγραφο βρίσκεται στο μέσο με το οποίο βεβαιώνεται η αυθεντικότητα του εγγράφου.

Η ελληνική νομοθεσία δεν αναφέρεται σαφώς τι είναι ηλεκτρονικό έγγραφο, όμως αυτό προκύπτει έμμεσα από το άρθρο 2 αριθ.1 του προεδρικού διατάγματος 150/2001 περί προσαρμογής στην οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, όπου ως ηλεκτρονική υπογραφή ορίζονται<< τα δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας>>.

Τα ηλεκτρονικά έγγραφα χωρίζονται σε γνήσια και μη γνήσια. Γνήσια θεωρούνται τα έγγραφα που έχουν αποκλειστικά ηλεκτρονική υπόσταση, δηλαδή καταχωρήσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό. Αντίθετα , τα μη γνήσια ηλεκτρονικά έγγραφα είναι έγγραφα με υλική μορφή, που το περιεχόμενό τους αλλά και υπογραφή τους είναι ηλεκτρονικά αποτυπωμένα όπως η τηλεομοιοτυπία(fax)και τηλέτυπο(telex)(www.itlawyers.gr Ηλεκτρονικά έγγραφα με ηλεκτρονική Υπογραφή Γιαννακάκη Μαρία)

11.5 Εγκύκλιοι

Ήδη στις 19 Φεβρουαρίου 2001 έχουμε την εγκύκλιο της Υπουργού εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης , που αφορά τη ρύθμιση θεμάτων ηλεκτρονικής διοίκησης και αποσκοπεί στη ρύθμιση ζητημάτων που άπτονται της εισαγωγής και χρήσεως του ηλεκτρονικού πρωτοκόλλου στις δημόσιες υπηρεσίες, τη γενίκευση της χρήσεως του fax και e-mail για ανταλλαγή κειμένου, την υποχρεωτική χρήση προγραμμάτων επεξεργασίας κειμένου για τη δημιουργία εγγράφων και τέλος την αποστολή των κειμένων προς δημοσίευση στην Εφημερίδα της Κυβερνήσεως σε ηλεκτρονική μορφή συνοδευόμενα και με την αντίστοιχη δισκέτα.

Σύμφωνα με την παραπάνω προκήρυξη καλούνται οι Νομαρχιακές Αυτοδιοικήσεις και Δήμοι να αντικαταστήσουν το χειρόγραφο σύστημα Πρωτοκόλλου με Ηλεκτρονικό μέχρι τον Αύγουστο του 2001 με απώτερο σκοπό η υιοθέτηση του Ηλεκτρονικού Πρωτοκόλλου να ενισχύσει την διαφάνεια και να διευκολύνει την εργασία των υπαλλήλων αλλά και των κάθε είδους χρηστών (έτοιμες καταστάσεις, γρήγορη αναζήτηση κτλ.) ενώ προκύπτει το συμπέρασμα από τα στατιστικά στοιχεία που έχουν συγκεντρωθεί ότι η Κεντρική Διοίκηση και οι Περιφέρειες να έχουν συμμορφωθεί με το περιεχόμενο της εγκυκλίου ενώ ποσοστό συμμόρφωσης είναι μικρότερο στις Νομαρχιακές Αυτοδιοικήσεις και πολύ μικρό δυστυχώς στους Δήμους. (ΔΙΑΔΠ 3753/19.2.2001)

Όπως αναφέρθηκε και παραπάνω με το άρθρο 14 του νόμου 2672/1998 όπου επιτρέπει τη διακίνηση εγγράφων με fax ή e-mail η ανωτέρω εγκύκλιος εφιστά την προσοχή των υπηρεσιών στη χρήση των εν λόγω τεχνολογιών καθώς και στη σύνδεση e-mail και ηλεκτρονικού πρωτοκόλλου ενώ οι υπηρεσίες υποχρεούνται να δημιουργούν τα έγγραφα ηλεκτρονικά και να τα διεκπεραιώνουν με ηλεκτρονικό τρόπο ,να ορίσουν αρμόδιο υπάλληλο για τη λειτουργία του e-mail και παράλληλα να συνταχθούν και οι σχετικοί κατάλογοι με τις ηλεκτρονικές διευθύνσεις των υπηρεσιών .

Επίσης με την με αριθμό ΔΙΑΔΠ 3753/19.2.2001 εγκύκλιο της Υπουργού Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, τέθηκαν και οι ελάχιστοι στόχοι που πρέπει να επιτευχθούν μέσα στο 2001, για την προετοιμασία της Δημόσιας Διοίκησης για την "Ηλεκτρονική Διοίκηση" με ένα από τους στόχους, την εφαρμογή του ηλεκτρονικού πρωτοκόλλου, από 3.9.2001 ενώ παράλληλα επιδιώκεται και η ανάδειξη της σημασίας της ηλεκτρονικής διαχείρισης - αρχειοθέτησης εγγράφων καθώς και η προετοιμασία των υπηρεσιών, (Υπουργεία, Γενικές Γραμματείες, Περιφέρειες, Νομαρχιακές Αυτοδιοικήσεις, Δήμοι), ώστε να είναι σε θέση να την

υιοθετήσουν το συντομότερο δυνατόν, παράλληλα με το ηλεκτρονικό πρωτόκολλο.

Επίσης στο πλαίσιο της ηλεκτρονικής διοίκησης με σκοπό τη μείωση του χρόνου και του κόστους δημοσίευσης, ανήκουν και οι εγκύκλιοι 6699/13-7-2000 και 6700/10-7-2000 του Εθνικού Τυπογραφείου, όπου καλούνται τα Υπουργεία και οι φορείς να αποστέλλουν τα κείμενα στο Εθνικό Τυπογραφείο γραμμένα με σύστημα επεξεργασίας κειμένου και να συνοδεύονται από την αντίστοιχη δισκέτα . (ΔΙΑΔΠ 3753/19.2.2001)

Επιπλέον οι υπηρεσίες υποχρεούνται να αποστέλλουν δύο φορές το χρόνο στο τέλος Ιουλίου και στο τέλος Δεκεμβρίου εκθέσεις προόδου για την παρακολούθηση υλοποίησης του προγράμματος χρησιμοποίησης ηλεκτρονικών μέσων ενώ ο Γενικός Γραμματέας Δημόσιας Διοίκησης υπέγραψε εγκύκλιο για τον έλεγχο και την πάταξη της παράνομης χρήσης λογισμικού στις δημόσιες υπηρεσίες (Υ.ΑΠ/Φ.00/Β/167/266/31-7-02).

Στο πλαίσιο της ηλεκτρονικής διοίκησης ανήκει και η πρωτοβουλία του Υπουργείου Οικονομίας και Οικονομικών μέσω του προγράμματος TAXIS , που αποσκοπεί στη δημιουργία βάσεως δεδομένων, στην οποία έχουν πρόσβαση μέσω των τερματικών τους όλοι οι υπάλληλοι των κεντρικών και αποκεντρωμένων υπηρεσιών του Υπουργείου ενώ το 2002 για πρώτη φορά κατέστη δυνατή η υποβολή φορολογικών δηλώσεων του εισοδήματος των φυσικών και νομικών προσώπων μέσω e-mail ,ενώ για τους πολίτες που θα υπέβαλαν τη φορολογική τους δήλωση μ'αυτόν τον τρόπο ,προβλέπονταν έκπτωση από το τελικό ποσό του φόρου και για το επόμενο έτος προβλεπόταν η δυνατότητα γενίκευσης του μέτρου αυτού.

11.6 Γ΄ Κοινοτικό Πλαίσιο Στήριξης

Προκειμένου να ανταποκριθεί και η Ελλάδα στις νέες αυτές ανάγκες έχει εκπονήσει το Επιχειρησιακό Πρόγραμμα Κοινωνία της Πληροφορίας που ήταν εντεταγμένο στο Γ΄ Κοινοτικό Πλαίσιο Στήριξης και εναρμονισμένο με το πρόγραμμα e – Europe ,το οποίο περιλαμβάνει το σχέδιο Δράσης 2002 [e – Europe2002] όπως εγκρίθηκε στο συμβούλιο κορυφής της Φέιρα στις 19/20 Ιουνίου, 2000 και επιπλέον το Επιχειρησιακό Πρόγραμμα "Πολιτεία" που χρηματοδοτήθηκε από εθνικούς πόρους και περιλάμβανε μέτρα για την επίτευξη των επιδιωκόμενων στόχων της ηλεκτρονικής διοίκησης. όπως η ενίσχυση της επικοινωνίας μεταξύ των διαφόρων φορέων της Κυβέρνησης αλλά περισσότερο η ενίσχυση της συμμετοχής των πολιτών στη λήψη των αποφάσεων για να αποφευχθούν φαινόμενα δυσαρέσκειας όπως αυτά εκδηλώθηκαν με τη μεγάλη αποχή στην τελευταία προεδρική εκλογή των ΗΠΑ, αλλά και στη Γαλλία. (www.infolaw.gr)

Σύμφωνα με τη φιλοσοφία των παραπάνω προγραμμάτων οι εργαζόμενοι στη Δημόσια Διοίκηση θα πρέπει να πιστοποιηθούν όχι ως άτομα, αλλά ως δημόσιοι υπάλληλοι που θα έχουν θεσμοθετημένη αρμοδιότητα ή εξουσιοδότηση να προβαίνουν σε συγκεκριμένες διοικητικές πράξεις και να υπογραφούν ορισμένα έγγραφα. Επομένως η ηλεκτρονική υπογραφή θα χρησιμοποιείται σχετικά σύντομα στο δημόσιο τομέα στο πλαίσιο των διοικητικών υπηρεσιών για την επικοινωνία των υπηρεσιών αυτών μεταξύ τους, με τους πολίτες και με νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου. www.infolaw.gr

11.7 Πρόγραμμα Πολιτεία- Σύζευξις

Όπως αναφέρθηκε παραπάνω το δεύτερο επιχειρησιακό πρόγραμμα που χρηματοδοτήθηκε από εθνικούς πόρους (κρατικός προϋπολογισμός) ήταν το πρόγραμμα εκσυγχρονισμού της δημόσιας διοίκησης υπό τον τίτλο "Πολιτεία" (ν. 2880/2001), που περιλάμβανε 5 υποπρογράμματα εκ των οποίων τα 3 έχουν άμεση ή έμμεση σχέση με την ηλεκτρονική διοίκηση.

Ενδεικτικά το πρώτο υποπρόγραμμα αφορούσε την επιμόρφωση του προσωπικού του δημοσίου τομέα ,όπου το εθνικό Κέντρο Δημόσιας Διοίκησης που υπάγεται στο Υπουργείο Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης είχε εντάξει προγράμματα επιμόρφωσης των δημοσίων υπαλλήλων στις νέες τεχνολογίες ύψους 552.000 € και το δεύτερο υποπρόγραμμα στόχευε στη βελτίωση των υποδομών και κτιριακών εγκαταστάσεων και εντάσσονταν τα μέτρα για την προμήθεια PC, Scanners, νέων servers κτλ

Επίσης το Υπουργείο Εσωτερικών και Δημόσιας Διοίκησης είχε προκηρύξει διαγωνισμό για τη μελέτη έργων που αφορούσε ένα πιλοτικό έργο για την επιμόρφωση των υπαλλήλων του με τη χρήση νέων τεχνολογιών καθώς και για την πιλοτική εφαρμογή διαδικτυακού τόπου διαχείρισης γνώσης στο ΥΠΕΣΔΔΑ.

Τέλος στο τέταρτο υποπρόγραμμα με θέμα τη βελτίωση των σχέσεων δημόσιας διοίκησης με τους πολίτες, συμπεριλαμβάνονταν δράσεις για την ολοκλήρωση του θεσμικού πλαισίου της ηλεκτρονικής υπογραφής, για την ολοκλήρωση της διαδικασίας καθιέρωσης και χρήσης του ηλεκτρονικού πρωτοκόλλου καθώς και για την καθιέρωση συστήματος ηλεκτρονικής διαχείρισης και αρχειοθέτησης των εγγράφων, με αποτέλεσμα ο συνδυασμός των τριών παραπάνω δράσεων να δημιουργήσει ένα ολοκληρωμένο σύστημα ηλεκτρονικής διαχείρισης των εγγράφων στις δημόσιες υπηρεσίες.

Στο ίδιο υποπρόγραμμα προβλέπεται επίσης ως μέτρο η δημιουργία ενός panel πολιτών με σκοπό τη σφυγμομέτρηση της κοινής γνώμης σε θέματα

λειτουργίας της δημόσιας διοίκησης. Ένας από τους τρόπους σφυγμομέτρησης πέρα των κλασικών μεθόδων είναι και η χρήση των νέων τεχνολογιών και του διαδικτύου.

Επίσης το παραπάνω επιχειρησιακό πρόγραμμα με το μέτρο 2.1 "Ηλεκτρονική Κυβέρνηση για την Εξυπηρέτηση του Πολίτη" περιλαμβάνει την κατάρτιση επιχειρησιακών σχεδίων, την εκπόνηση μελετών για οριζόντια θέματα καθώς και την ανάπτυξη πιλοτικών εφαρμογών και με το μέτρο 2.2 "Ηλεκτρονική Διακυβέρνηση" αποσκοπεί στην αξιοποίηση των τεχνολογιών της πληροφορικής και εν γένει των νέων τεχνολογιών με στόχο τη βελτίωση της ποιότητας των παρεχομένων υπηρεσιών από τη δημόσια διοίκηση σε πολίτες και επιχειρήσεις σε κεντρικό και σε περιφερειακό επίπεδο με στόχο την εγκατάσταση 75000 PC STH Δημόσια Διοίκηση, τη διαδικτυακή κάλυψη 1.000 Δημόσιων Υπηρεσιών και τη δημιουργία 900 υπηρεσιών μιας στάσης (infoKiosk).

Τέλος το πρόγραμμα Πολιτεία -Σύζευξις στοχεύει στη δημιουργία της βασικής δικτυακής υποδομής η οποία εξασφαλίζει τις αναγκαίες επικοινωνίες των φορέων της Δημόσιας Διοίκησης και ήδη λειτουργεί πιλοτικά το πρόγραμμα με 20 κόμβους στους οποίους είναι συνδεδεμένοι φορείς του Δημοσίου όπως Υπουργεία, Γεν. Γραμματείες, Περιφέρειες, Νομαρχίες.www.infolaw.gr

11.8 Τομέας Διαδικτυακών Πυλών

Περνώντας τώρα στον τομέα των διαδικτυακών πυλών (portal) του Δημοσίου, θα πρέπει να επισημάνουμε ότι στην Ελλάδα δεν υπάρχει ένα κεντρικό portal αντίστοιχο αυτού της Βρετανικής Κυβερνήσεως ενώ τα Υπουργεία έχουν δικές τους ιστοσελίδες.

Το Υπουργείο Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης έχει δύο ιστοσελίδες, την www.ypes.gr και www.gspa.gr στις οποίες υπάρχουν links για την επιλογή παροχής πληροφοριών σε θέματα αρμοδιότητας του Υπουργείου (πχ εκλογές, οδηγός του πολίτη, νομαρχιακή αυτοδιοίκηση, περιφέρειες κτλ.) ενώ μελετάται η δημιουργία μίας και μόνης ιστοσελίδας για όλη τη Δημόσια Διοίκηση (κάτι όπως gov.gr) ενώ σε ορισμένες υπηρεσίες (του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης συμπεριλαμβανομένου) έχουν τοποθετηθεί infoKiosks στα οποία οι πολίτες μπορούν, χρησιμοποιώντας οθόνες αφής να λαμβάνουν πληροφορίες.

Με τον νόμο 3013/2002 δημιουργήθηκαν τα Κέντρα Εξυπηρέτησης Πολιτών (Κ.Ε.Π.) τα οποία χρησιμοποιώντας την πιλοτική εφαρμογή του προγράμματος Σύζευξις, είναι συνδεδεμένα on line μεταξύ τους αφού έχει προηγουμένως έχει γίνει η καταγραφή των διαδικασιών που διεκπεραιώνει η

Δημόσια Διοίκηση και έχουν γίνει παρεμβάσεις απλούστευσης των διαδικασιών αυτών, δίνονται σταδιακά στο Κ.Ε.Π.

Επίσης έχουν ετοιμαστεί ψηφιοποιημένα έντυπα τα οποία θα εμφανίζονται στις οθόνες computer των Κ.Ε.Π. και οι πολίτες θα τα συμπληρώνουν με τη βοήθεια των υπαλλήλων ,ενώ ο πολίτης μπορεί να απευθύνεται σε οποιοδήποτε Κ.Ε.Π. και όχι υποχρεωτικά σε αυτό του τόπου κατοικίας του και το αίτημά του θα διεκπεραιώνεται ηλεκτρονικά.

Παρέχεται επίσης η δυνατότητα το πιστοποιητικό, βεβαίωση ή άδεια που θα ζητά ο πολίτης, να μπορεί να του αποστέλλεται και ηλεκτρονικά στο άμεσο μέλλον ενώ τώρα το παραλαμβάνει ο ίδιος από το ΚΕΠ ή του αποστέλλεται ταχυδρομικά ενώ παράλληλα τοποθετούνται στους χώρους υποδοχής των Κ.Ε.Π. τοποθετούνται infoKiosk για την ενημέρωση των πολιτών.

Ταυτόχρονα ετοιμάζεται η προκήρυξη για την εκπόνηση μελέτης και στη συνέχεια εφαρμογή πιλοτικού προγράμματος για τη χρήση smart cards στο πλαίσιο του προγράμματος "Πολιτεία όπου μελετάται η συνδυασμένη δυνατότητα χρήσεως των smart cards στα Κ.Ε.Π. (πιθανό αντικείμενο του πιλοτικού προγράμματος θα είναι η χρήση των smart cards στα Κ.Ε.Π. όπου θα προβλέπεται η ύπαρξη τερματικών όπου με την smart card ο πολίτης θα μπορεί να αιτείται πιστοποιητικά και βεβαιώσεις).

Συμπερασματικά γίνεται προσπάθεια να υπάρξει ένας γενικός συντονισμός των θεμάτων που άπτονται της ηλεκτρονικής διοίκησης ενώ ήδη λειτουργεί στο Υπουργείο Οικονομίας και Οικονομικών η Ειδική Γραμματεία της Κοινωνίας της Πληροφορίας και στο Υπουργείο Εσωτερικών , Δημόσιας Διοίκησης και Αποκέντρωσης η Υπηρεσία Ανάπτυξης της Πληροφορικής με στόχο την επίτευξη του αειφόρου εκσυγχρονισμού της Δημόσιας Διοίκησης. www.infolaw.gr

11.9 Επικείμενο Νομοσχέδιο εντός του 2011

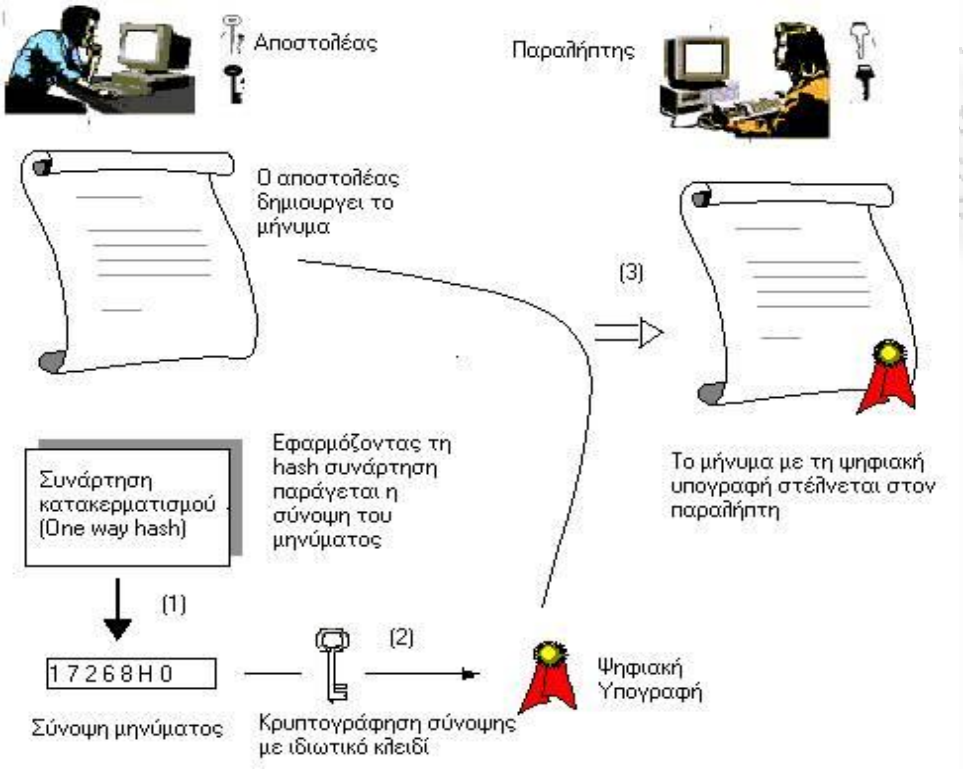
Σε δημόσια διαβούλευση τίθεται τις επόμενες ημέρες το νομοσχέδιο για την ηλεκτρονική διακυβέρνηση, το οποίο θα περιλαμβάνει όλες τις ρυθμίσεις και διαδικασίες για τη μετάβαση στον νέο τρόπο διεκπεραίωσης των συναλλαγών με το Δημόσιο με στόχο να ψηφιστεί έως τον Μάρτιο, προκειμένου να υλοποιηθεί έως το τέλος του έτους με σημαντικές αλλαγές στην καθημερινότητα των πολιτών καθώς υποχρεώνεται η διοίκηση να διεκπεραιώνει ηλεκτρονικά τις υποθέσεις τους, χωρίς να χρειάζονται να προσέρχονται αυτοπροσώπως στα γκισέ των υπηρεσιών».

Σύμφωνα με το νομοσχέδιο κάθε διοικητική διαδικασία θα γίνεται από την αρχή έως το τέλος με ηλεκτρονικό τρόπο και για να επιτευχθεί αυτό

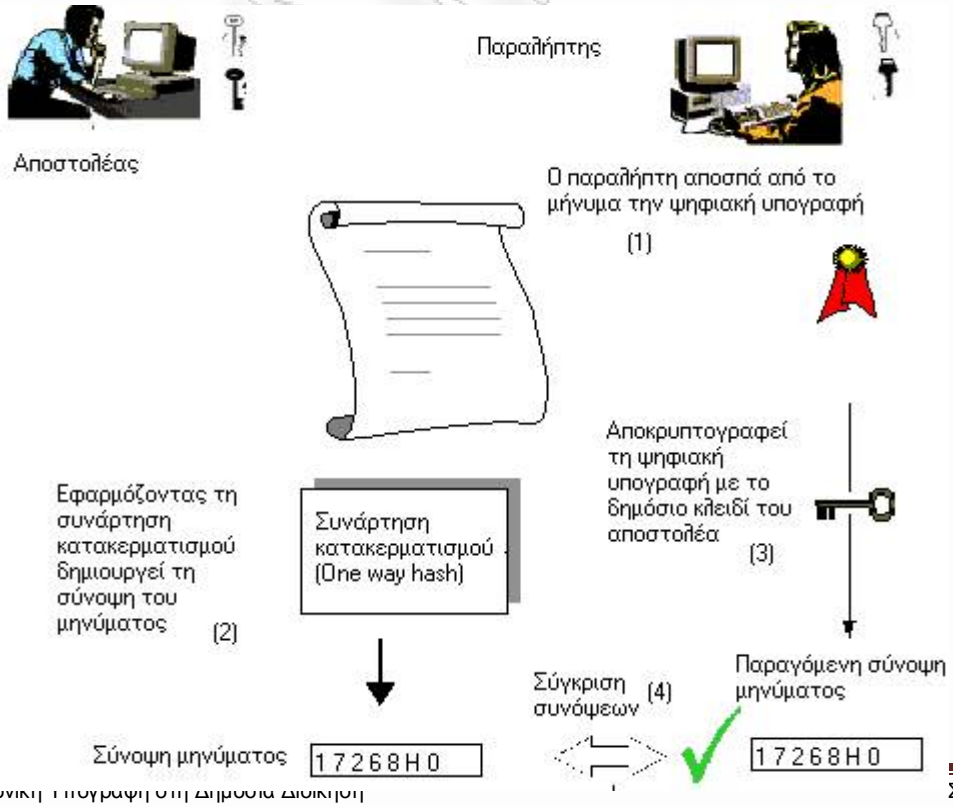
πρωταρχικός στόχος είναι να εφαρμοστεί η λεγόμενη διαλειτουργικότητα μεταξύ των πληροφοριακών συστημάτων και μμητρώων των διαφόρων φορέων που συνεπάγεται την ενοποίηση όλων αυτών των συστημάτων, με σκοπό όλα τα έγγραφα που απαιτούνται για τις συναλλαγές να διακινούνται ηλεκτρονικά ή να αναζητούνται με τον ίδιο τρόπο πιστοποιητικά που μέχρι τώρα ήταν υποχρεωμένος να προσκομίσει ο πολίτης.

Επίσης στις βασικές αλλαγές του συστήματος ηλεκτρονικής διακυβέρνησης που προτείνεται με το νομοσχέδιο είναι και η καθιέρωση υποχρεωτικά του δικαιώματος ηλεκτρονικής υπογραφής των εγγράφων από τους πολίτες καθώς και η απαλλαγή από την κλασική χρονοβόρα διαδικασία επικύρωσης, αφού πλέον προβλέπεται η αποδοχή ηλεκτρονικών αντιγράφων. www.vlioras.gr/Philologia/Composition/Grafeiokratia.htm

12.Δημιουργία ψηφιακής υπογραφής



Επαλήθευση ψηφιακής υπογραφής



13. Συμπεράσματα

Στην σημερινή εποχή της ηλεκτρονικής τεχνολογίας, των ψηφιακών επικοινωνιών και της διαδικτυακής ανταλλαγής δεδομένων, η ασφάλεια των ηλεκτρονικών συναλλαγών αποτελεί απαραίτητη προϋπόθεση και οπωσδήποτε εγγύηση για την ομαλή λειτουργία της οικονομικής και κοινωνικής ζωής, όπου καλείται ο νομοθέτης κάθε φορά να προστατεύσει την επίτευξη συναλλακτικής ασφάλειας με τη συνεχή παρακολούθηση των τεχνολογικών εξελίξεων και την κατάλληλη νομοθετική παρέμβαση.

Γίνεται κατανοητό ότι μια πλευρά αυτής της προσπάθειας του νομοθέτη για επίτευξη ασφάλειας στις ηλεκτρονικές συναλλαγές είναι η νομοθεσία περί των ηλεκτρονικών υπογραφών, η μελέτη της οποίας αποτέλεσε αντικείμενο της διατριβής. Αρχικά αναλύθηκε το θεσμικό πλαίσιο των ηλεκτρονικών υπογραφών κάνοντας αναφορά στην οδηγία 1999/93 ,που ήταν αναγκαία ως ένα πρώτο νομοθετικό βήμα μέσα στην ΕΕ, που πρωταρχικός της σκοπός είναι να παρακολουθεί την τεχνολογική εξέλιξη, την προστασία των καταναλωτών κατά τις ηλεκτρονικές συναλλαγές τους καθώς και την ανάπτυξη της Κοινωνίας της Πληροφορίας.

Επίσης αναλύθηκε η ελληνική νομοθεσία γα τις ηλεκτρονικές υπογραφές, δηλαδή το προεδρικό διάταγμα 150/2001 σε σχέση με την κοινοτική οδηγία 1999/93 , αφού η Ελλάδα οφείλει να ακολουθεί τη νομοθετική πρωτοβουλία της Ευρωπαϊκής Ένωσης και σε συνεννόηση με τα αρμόδια όργανα της Ευρωπαϊκής Ένωσης απαιτείται η ελληνική νομοθεσία να προσαρμόζεται όσον το δυνατόν πιο γρήγορα στις συνεχείς τεχνολογικές εξελίξεις των ηλεκτρονικών υπογραφών.

Χωρίς αμφιβολία οι διατάξεις της οδηγίας 1999/93 ως προς την καταλληλότητα και την επάρκεια όπως προκύπτει μέσα από τη διατριβή θα δοκιμάζονται και θα κρίνονται στο μέλλον σε κάθε συναλλαγή με τη χρήση της ηλεκτρονικής υπογραφής για αυτό και ο κοινοτικός νομοθέτης θα πρέπει να βρίσκεται πάντα σε ετοιμότητα και να προσαρμόζει την κοινοτική νομοθεσία στις κοινωνικές και συναλλακτικές ανάγκες, με σκοπό κάθε φορά την ασφάλεια των συναλλαγών και την αποτελεσματική προστασία του πολίτη.

Γι αυτό ακριβώς το λόγο οι νέες κοινωνικές συνθήκες καθιστούν σαφές ότι η νομοθετική αντιμετώπιση της ηλεκτρονικής υπογραφής πρέπει να έχει τα χαρακτηριστικά της διεθνούς συναίνεσης ώστε να αποφευχθεί ο κίνδυνος η κάθε χώρα να έχει τη δική της διαφορετική νομοθεσία και επομένως μια νομοθετική πρωτοβουλία για τις ηλεκτρονικές υπογραφές με παγκόσμια

απήχηση γίνεται επιτακτικότερη για την εγγύηση της ασφάλειας των ηλεκτρονικών συναλλαγών.

Έτσι γίνεται κατανοητό ότι μέσα από μια τέτοια νομοθετική πρωτοβουλία διεθνούς ακτινοβολίας μπορεί να προωθηθεί νομική αναγνώριση των ηλεκτρονικών υπογραφών μέσα από κοινά συμφωνημένα τεχνικά πρότυπα ώστε να διευκολύνεται η απρόσκοπτη χρήση των ηλεκτρονικών υπογραφών σε παγκόσμιο επίπεδο και η διαμόρφωση ενός καταλόγου διεθνώς αναγνωρισμένων ασφαλών τεχνολογιών ηλεκτρονικής υπογραφής.

Επιπλέον μια τέτοια διεθνής νομοθετική πρωτοβουλία μπορεί να εισηγηθεί για την υιοθέτηση τεχνολογικά ουδέτερης γλώσσας στη χρήση της ηλεκτρονικής υπογραφής , ώστε το νέο νομοθετικό πλαίσιο να επιτρέπει την εφαρμογή του και σε τεχνολογίες ηλεκτρονικών υπογραφών που θα εφευρεθούν στο μέλλον αλλά και να ευνοεί την απρόσκοπτη ανάπτυξη νέων πιο σύγχρονων και πιο αποτελεσματικών τεχνολογιών ηλεκτρονικής υπογραφής.

Ένας άλλος τρόπος εκδήλωσης διεθνούς πρωτοβουλίας για θέματα ηλεκτρονικών πρωτοβουλιών θα μπορούσε να είναι και η άμεση έναρξη συνομιλιών μεταξύ των χωρών, με αντικείμενο την κατάρτιση ,επιμόρφωση και την υιοθέτηση κοινά αποδεκτών νομικών κανόνων και τεχνικών προτύπων, που θα διέπουν τις ηλεκτρονικές υπογραφές με πρωταγωνιστικό ρόλο τις χώρες, όπου οι ηλεκτρονικές επικοινωνίες παρουσιάζουν ιδιαίτερη πρόοδο στο τομέα των ηλεκτρονικών συναλλαγών ενώ παράλληλα θα μπορούσε να αναλάβει ένας διεθνής οργανισμός με αυξημένο κύρος και παγκόσμια ακτινοβολία να συγκαλέσει αυτή την παγκόσμια διάσκεψη.

Προς αυτήν την κατεύθυνση ήδη υπάρχει το επιτυχημένο προηγούμενο των Παγκόσμιων Διασκέψεων για την Κοινωνία της Πληροφορίας στη Γενεύη και την Τύνιδα αλλά και του παγκόσμιου forum για τα προβλήματα του Διαδικτύου το Νοέμβριο του 2006 στην Αθήνα ενώ μια τέτοια ελπιδοφόρα προσπάθεια έχει ξεκινήσει υπό την αιγίδα του ΟΗΕ, μέσω της Επιτροπής UNCITRAL, η οποία έχει θεσπίσει τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, ρυθμίζοντας ζητήματα όπως η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, η νομική ισχύς της ηλεκτρονικής υπογραφής, η αποδεικτική δύναμη των ηλεκτρονικών κειμένων, ο τόπος, χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος όπως αναφέρθηκε στη διατριβή.

Βέβαια έχει διατυπωθεί και μια άλλη εναλλακτική πρόταση κυρίως από Αμερικανούς επιστήμονες και συγγραφείς, οι οποίοι υποστηρίζουν ότι η ηλεκτρονική αγορά θα πρέπει να αφεθεί ελεύθερη να λύσει σταδιακά τα καθημερινά συναλλακτικά προβλήματα που σχετίζονται με τις ηλεκτρονικές

υπογραφές μέσω της αυτορρύθμισης δηλαδή της θέσπισης κωδίκων δεοντολογίας μεταξύ επαγγελματικών και καταναλωτικών οργανώσεων και όχι μέσω της ξαφνικής επιβολής μιας διεθνούς νομοθεσίας.

Από τα παραπάνω γίνεται κατανοητό ότι είναι σαφώς προτιμότερη μια νομοθετική συμφωνία διεθνούς κύρους, η οποία θα ανταποκρινόταν αποτελεσματικά στα τεχνολογικά και κοινωνικά δεδομένα του Διαδικτύου και της Παγκοσμιοποίησης παρέχοντας με αξιόπιστη και ομοιόμορφη νομοθετική ρύθμιση την απαιτούμενη λειτουργικότητα στις ηλεκτρονικές συναλλαγές και την εγγύηση της συναλλακτικής ασφάλειας μέσα σε ένα ασφαλές ηλεκτρονικό περιβάλλον.

Επίσης μέσα από την εκπόνηση της διατριβής γίνεται προσπάθεια να καταλάβει ο αναγνώστης τα σημαντικότερα προβλήματα που παρουσιάζονται για την δημιουργία των δικών του ηλεκτρονικών υπογραφών και την επαλήθευση των ηλεκτρονικών υπογραφών τρίτων, σε περισσότερους από έναν συναλλακτικούς κύκλους είτε πραγματοποιείται στον ιδιωτικό είτε στον δημόσιο τομέα.

Συγκεκριμένα η διαλειτουργικότητα όλων των σχετικών εφαρμογών αποτελεί ένα σημαντικό ζητούμενο για τους εξής λόγους: θα μειώσει το συνολικό κόστος εξοπλισμού, θα απλοποιήσει τις λειτουργίες του χρήστη, θα περιορίσει τις πολλαπλές διαδικασίες ταυτοποίησης των υποκειμένων, θα συμβάλλει στην δημιουργία της κρίσιμης μάζας των χρηστών με δυνατότητα ηλεκτρονικής υπογραφής που θα οδηγήσει στην ανάπτυξη και παροχή περισσότερων σχετικών υπηρεσιών προς τους χρήστες.

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

Η τεχνική πολυπλοκότητα, οι παραλλαγές των εφαρμογών προηγμένων ηλεκτρονικών υπογραφών και τα διάφορα επίπεδα νομικής αναγνώρισής του αναδεικνύουν ιδιαίτερες δυσκολίες ως προς την επίτευξη πλήρους διαλειτουργικότητας μεταξύ των υφιστάμενων εφαρμογών ηλεκτρονικής υπογραφής σε διεθνές κα ευρωπαϊκό επίπεδο.

Στα πλαίσια της Ευρωπαϊκής Ένωσης μετά την έκδοση της σχετικής Ευρωπαϊκής Οδηγίας, που είχε ως πρωταρχικό στόχο την εναρμόνιση του σχετικού θεσμικού πλαισίου μεταξύ των κρατών μελών, η παροχή πανευρωπαϊκώς αναγνωρισμένων και διαλειτουργικών υπηρεσιών

πιστοποίησης ηλεκτρονικής υπογραφής εξακολουθεί να εμφανίζει αρκετές δυσχέρειες.

Μάλιστα , με εξαίρεση ορισμένα κράτη – μέλη όπως η Ιταλία, η Γερμανία και η Φιλανδία οι οποίες είχαν προβεί εγκαίρως σε αναλυτικές ρυθμίσεις για την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, σοβαρά ζητήματα διαλειτουργικότητας υπάρχουν ακόμη και ανάμεσα στις σχετικές υπηρεσίες που παρέχονται από τους Παρόχους Υπηρεσιών Πιστοποίησης που λειτουργούν στο ίδιο κράτος, όπως παρατηρήθηκε στο πλαίσιο λειτουργίας της ΟΕ Έ2΄ΤΟΥ e Business Forum ότι συμβαίνει και στην Ελλάδα.

Τα σημαντικότερα προβλήματα διαλειτουργικότητας μεταξύ των υπηρεσιών πιστοποίησης των ηλεκτρονικών υπογραφών που παρατηρούνται αναφέρονται κυρίως στην περιγραφή των στοιχείων του υποκειμένου των πιστοποιητικών, στον τρόπο προσδιορισμού των επιτρεπόμενων χρήσεων των σχετικών κρυπτογραφικών κλειδιών και στα μέσα που χρησιμοποιούνται γα την ενημέρωση των κατόχων και αποδεκτών των ηλεκτρονικών πιστοποιητικών ως προς τους όρους έκδοσης και χρήσης που θέτονται από την εφαρμοζόμενη πολιτική των εκδιδόμενων πιστοποιητικών.

Επίσης σημαντικά ζητήματα υφίστανται και με την χρονοσήμανση των υπογραφών, την πιστοποίηση των ιδιοτήτων των υποκειμένων, οι υπηρεσίες ενημέρωσης για την ανάκληση των πιστοποιητικών, η αλληλεπίδραση των Παρόχων Υπηρεσιών Πιστοποίησης κ.ά.

Όλα αυτά έχουν ως πρόσθετο αρνητικό αποτέλεσμα την έλλειψη κοινώς αποδεκτών εφαρμογών λογισμικού για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, οι οποίες να εφαρμόζουν κα να ερμηνεύουν σωστά ανεξάρτητα από τον εκδότη, το υποκείμενο ή και τον αποδέκτη των σχετικών πιστοποιητικών.

Επίσης η έλλειψη διαλειτουργικότητας στις εφαρμογές ηλεκτρονικών υπογραφών, το μεγάλο κόστος δημιουργίας και διατήρησης μιας ασφαλούς Υποδομής Δημοσίου Κλειδιού και ο μεγάλος επιχειρηματικός κίνδυνος της ανάπτυξης μιας τέτοιας υποδομής την στιγμή που δεν έχουν προσδιοριστεί σαφώς οι τελικές προδιαγραφές που θα επικρατήσουν, οδηγούν σε συγκράτηση και περιορισμό των σχετικών επενδύσεων και των πρωτοβουλιών για την ανάπτυξη συναφών εφαρμογών.

Παράλληλα διαπιστώνεται ότι σημαντική ενίσχυση της εμπιστοσύνης του κοινού στις σχετικές υπηρεσίες θα προσφέρει η λειτουργία του προβλεπόμενου μηχανισμού για την Διαπίστωση της συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής με τις απαιτήσεις της νομοθεσίας,

καθώς και η εφαρμογή στην πράξη του θεσμού της Εθελοντικής Διαπίστευσης των Παρόχων Υπηρεσιών Πιστοποίησης.

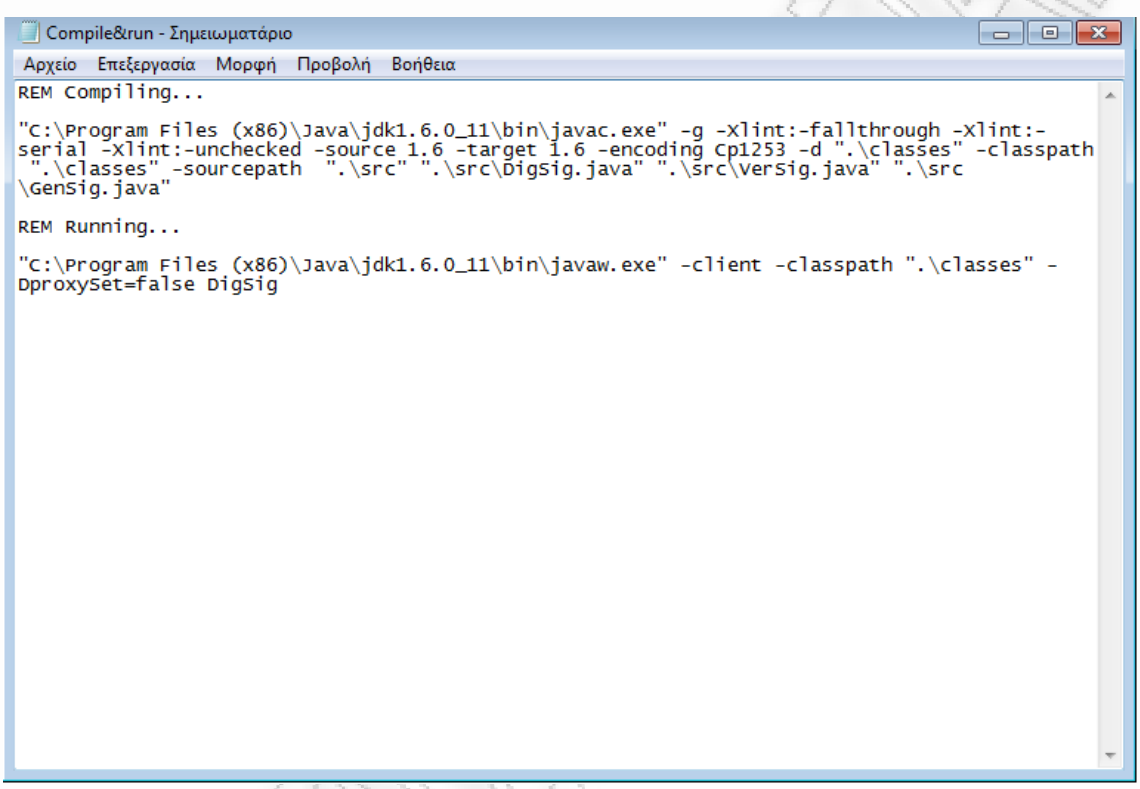
Επίσης η σύνταξη Πολιτικών Ηλεκτρονικής Υπογραφής που θα προσδιορίζουν ακριβείς όρους για την δημιουργία έγκυρων ηλεκτρονικών υπογραφών με εφαρμογή στις υπηρεσίες του Δημόσιου Τομέα, θεωρείται ότι μπορεί να συμβάλλει στην αποσαφήνιση των απαραίτητων προδιαγραφών για τις παρεχόμενες υπηρεσίες πιστοποίησης ηλεκτρονικών υπογραφών και στην περαιτέρω διαλειτουργικότητά τους.

Τέλος η υιοθέτηση ανοικτών προτύπων και η χρήση της γλώσσας XML στην ανάπτυξη των σχετικών εφαρμογών ηλεκτρονικών υπογραφών, μπορούν να παράσχουν πιο αναλυτικές και τυποποιημένες πληροφορίες στην λειτουργία των εφαρμογών αυτών και να συμβάλλουν στην επίτευξη μεγαλύτερης διαλειτουργικότητας και αναγνώρισης των σχετικών συναλλαγών σε πανευρωπαϊκό και διεθνές επίπεδο.

14.ΠΑΡΑΡΤΗΜΑ Α

14.1 Εφαρμογή κρυπτογράφησης και αποκρυπτογράφησης με χρήση ψηφιακής υπογραφής

Εάν τρέξουμε το παρακάτω αρχείο δέσμης (batch file):



Όπου το αρχείο versig.java περιέχει τον εξής κώδικα πηγής:

```
import java.awt.Dimension;

import java.awt.Rectangle;

import java.awt.event.ActionEvent;

import java.awt.event.ActionListener;


import java.io.File;


import javax.swing.JButton;

import javax.swing.JFileChooser;
```

```
import javax.swing.JFrame;
import javax.swing.JLabel;
import javax.swing.JMenu;
import javax.swing.JMenuBar;
import javax.swing.JMenuItem;
import javax.swing.JOptionPane;
import javax.swing.JScrollPane;
import javax.swing.JTextArea;
import javax.swing.JTextField;
import javax.swing.filechooser.FileFilter;
import javax.swing.filechooser.FileNameExtensionFilter;

Public class DigSig extends Frame {
    Private JMenuBar menu Bar = new JMenuBar();
    Private JMenu menu File = new JMenu();
    Private JMenuItem menuFileExit = new JMenuItem ();
    Private JTextField jTextField1 = new JTextField ();
    Private JTextField jTextField2 = new JTextField ();
    Private JTextField jTextField3 = new JTextField ();
    Private JTextField jTextField4 = new JTextField ();
    Private JLabel jLabel1 = new JLabel ();
    Private JLabel jLabel2 = new JLabel ();
    Private JLabel jLabel3 = new JLabel ();
    Private JLabel jLabel4 = new JLabel ();
    Private JButton jButton1 = new JButton ();
    Private JButton jButton2 = new JButton();
```

```
    Private JButton jButton3 = new JButton ();
    Private JButton jButton4 = new JButton ();
    Private JButton DecryptBtn = new JButton ();
   Private JButton jButton6 = new JButton ();
    Private JScrollPane jScrollPane1 = new JScrollPane();
    Private JTextArea log = new JTextArea();

    Public DigSig () {
        Try {
            JbInit ();
        } Catch (Exception e) {
            e.printStackTrace ();
        }
    }

    Private void jbInit () throws Exception {
        This.setJMenuBar (menu Bar);
        This.getContentPane (). Set Layout (null );
        This.setSize (new Dimension(532, 362));
        this.setResizable (false);
        MenuFile.setText( "File" );
        MenuFileExit.setText( "Exit" );
        MenuFileExit.addActionListener (new Action Listener () { public void
action Performed( Action Event ae ) { fileExit_ActionPerformed( ae ); } } );
        JTextField1.setBounds (new Rectangle (115, 30, 245, 20));
        JTextField2.setBounds (new Rectangle(115, 60, 245, 20));
```

```
jTextField3.setBounds(new Rectangle(115, 90, 245, 20));
jTextField4.setBounds(new Rectangle(115, 120, 245, 20));
jLabel1.setText("File to Encrypt");
jLabel1.setBounds(new Rectangle(20, 30, 85, 20));
jLabel2.setText("File to Decrypt");
jLabel2.setBounds(new Rectangle(20, 60, 85, 20));
JLabel3.setText ("Signature File");
JLabel3.setBounds (new Rectangle (20, 90, 85, 20));
JLabel4.setText ("Public Key File");
JLabel4.setBounds (new Rectangle (20, 120, 85, 20));
JButton1.setText ("Browse");
JButton1.setBounds (new Rectangle (390, 30, 95, 20));
JButton1.addActionListener (new ActionListener () {
      public void action Performed(ActionEvent e) {
         JButton1_actionPerformed (e);
      }
   });
JButton2.setText ("Browse");
JButton2.setBounds (new Rectangle (390, 60, 95, 20));
JButton2.addActionListener (new ActionListener () {
      Public void action Performed (ActionEvent e) {
         JButton2_actionPerformed (e);
      }
   });
JButton3.setText ("Browse");
JButton3.setBounds (new Rectangle (390, 90, 95, 20));
```

```
JButton3.addActionListener (new ActionListener () {
        Public void action Performed (ActionEvent e) {
            JButton3_actionPerformed (e);
        }
    });
jButton4.setText("Browse");
jButton4.setBounds(new Rectangle(390, 120, 95, 20));
jButton4.addActionListener(new ActionListener() {
        public void actionPerformed(ActionEvent e) {
            jButton4_actionPerformed(e);
        }
    });
DecryptBtn.setText("Decrypt");
DecryptBtn.setBounds(new Rectangle(355, 165, 110, 25));
DecryptBtn.addActionListener(new ActionListener() {
        public void actionPerformed(ActionEvent e) {
            Decrypt(e);
        }
    });
jButton6.setText("Encrypt");
jButton6.setBounds(new Rectangle(230, 165, 110, 25));
jButton6.addActionListener(new ActionListener() {
        public void actionPerformed(ActionEvent e) {
            Encrypt (e);
        }
    });
```

```
    jScrollPane1.setBounds(new Rectangle(10, 205, 505, 85));
    menuFile.add( menuFileExit );
    menuBar.add( menuFile );
    jScrollPane1.getViewport().add(log, null);
    this.getContentPane().add(jScrollPane1, null);
    this.getContentPane().add(jButton6, null);
    This.getContentPane (). add(DecryptBtn, null);
    This.getContentPane (). add (jButton4, null);
    This.getContentPane(). add(jButton3, null);
    this.getContentPane().add(jButton2, null);
    this.getContentPane().add (jButton1, null);
    this.getContentPane().add(jLabel4, null);
    this.getContentPane().add(jLabel3, null);
    this.getContentPane().add(jLabel2, null);
    this.getContentPane().add(jLabel1, null);
    this.getContentPane().add(jTextField4, null);
    this.getContentPane(). add(jTextField3, null);
    This.getContentPane().add(jTextField2, null);
    This.getContentPane (). add(jTextField1, null);
}

void fileExit_ActionPerformed(ActionEvent e) {
    System.exit(0);
}

public static void main (String [] args){
```

```
        DigSig myDigSig = new DigSig();
        myDigSig.setVisible(true);
    }

    private void jButton1_actionPerformed(ActionEvent e) {
        String newline = "\n";

         JFileChooser fc = new JFileChooser();
            FileFilter XMLfilter = new FileNameExtensionFilter("XML File",
"XML");
            fc.addChoosableFileFilter(XMLfilter);
            int returnVal = fc.showOpenDialog(null);

            if (returnVal == JFileChooser.APPROVE_OPTION) {
                File file = fc.getSelectedFile();
                //This is where a real application would open the file.

                jTextField1.setText(file.getAbsolutePath());
                log.append("Opening: " + file.getName() + "." + newline);
              } else {
                log.append("Open command cancelled by user." +
newline);

              }
              log.setCaretPosition(log.getDocument().getLength());
    }
```

```
    private void jButton2_actionPerformed(ActionEvent e) {
        String newline = "\n";

            JFileChooser fc = new JFileChooser();
            FileFilter XMLfilter = new FileNameExtensionFilter("XML File",
"XML");
            fc.addChoosableFileFilter(XMLfilter);
            int returnVal = fc.showOpenDialog(null);

            if (returnVal == JFileChooser.APPROVE_OPTION) {
                File file = fc.getSelectedFile();
                //This is where a real application would open the file.

                jTextField2.setText(file.getAbsolutePath());
                log.append("Opening: " + file.getName() + "." + newline);
              } else {
                log.append("Open command cancelled by user." +
newline);

              }
             log.setCaretPosition(log.getDocument().getLength());
    }

    private void jButton3_actionPerformed(ActionEvent e) {
        String newline = "\n";

            JFileChooser fc = new JFileChooser ();
```

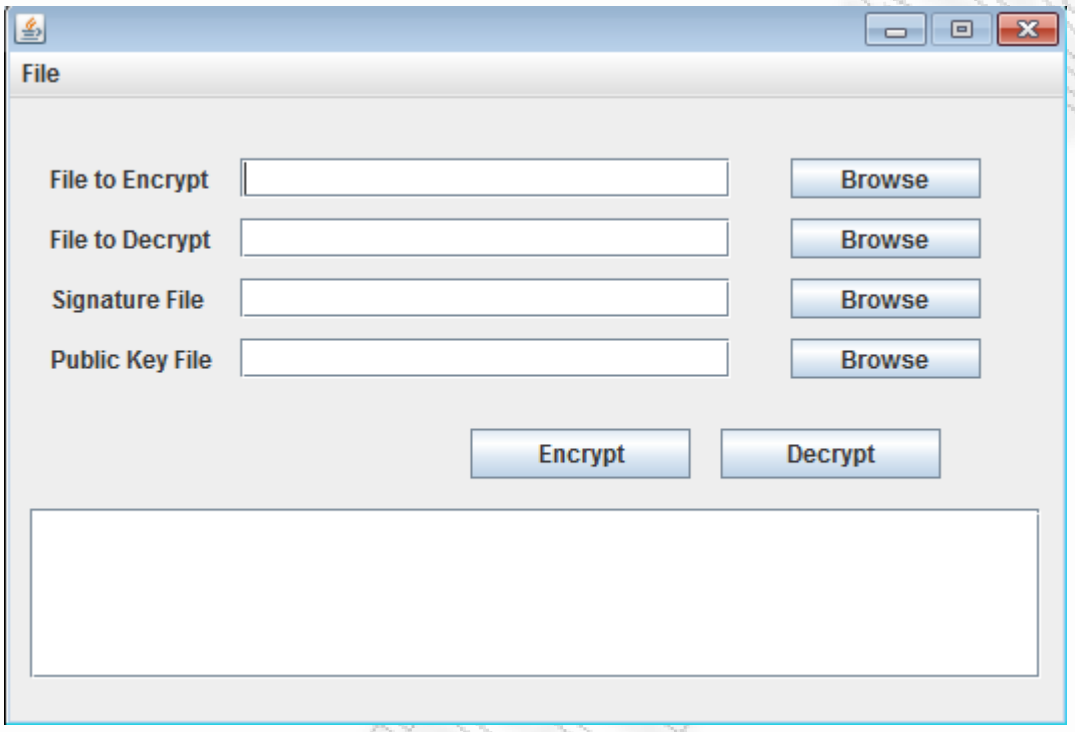
```
            FileFilter XMLfilter = new FileNameExtensionFilter ("XML File",
"XML");
            Fc.addChoosableFileFilter (XMLfilter);
            int returnVal = fc.showOpenDialog (null);

            if (return Val == JFileChooser.APPROVE_OPTION) {
                File file = fc.getSelectedFile();
                //This is where a real application would open the file.

                jTextField3.setText(file.getAbsolutePath());
                log.append("Opening: " + file.getName() + "." + newline);
              } else {
                log.append("Open command cancelled by user." +
newline);

              }
              log.setCaretPosition(log.getDocument().getLength());
   }

   private void jButton4_actionPerformed(ActionEvent e) {
      String newline = "\n";

            JFileChooser fc = new JFileChooser();
            FileFilter XMLfilter = new FileNameExtensionFilter("XML File",
"XML");
            fc.addChoosableFileFilter(XMLfilter);
            int return Val = fc.showOpenDialog(null);
```

```
            if (return Val == JFileChooser.APPROVE_OPTION) {
                File file = fc.getSelectedFile ();
                //This is where a real application would open the file.

                jTextField4.setText(file.getAbsolutePath());
                log.append("Opening: " + file.getName() + "." + new line);
            } Else {
                Log.append ("Open command cancelled by user." + new
line);

            }
            log.setCaretPosition(log.getDocument().getLength());
    }

    Private void jButton6_actionPerformed (ActionEvent e) {
        //jCheckBox1.setSelected(true);
        //jTextField2.setEnabled(false);
        //jTextField1.setEnabled (true);


    }

    Private void Decrypt (ActionEvent e) {
        boolean verification;
```

```
        if (jTextField2.getText().isEmpty()){

          JOptionPane.showMessageDialog (null, "Enter the file name to
decrypt.", "", 1);

          return;

        }


        If (jTextField3.getText (). isEmpty ()){

          JOptionPane.showMessageDialog (null, "Enter the signature file
name.", "", 1);

          return;

        }


        if (jTextField4.getText().isEmpty()){

          JOptionPane.showMessageDialog (null, "Enter the public key file
name.", "", 1);

          Return;

        }


        VerSig S = new VerSig();

        Verification = S.decrypt (jTextField4.getText (), jTextField3.getText (),
jTextField2.getText ());


        String theValueAsString = new Boolean (verification). To String ();


        Log. append ("verification: "+theValueAsString);

    }
```

```
   Private void Encrypt (ActionEvent e) {

      If (jTextField1.getText (). isEmpty ()){

         JOptionPane.showMessageDialog (null, "Enter the file name to
sign.", "", 1);

         return;

    }


      if (jTextField3.getText().isEmpty()){

        JOptionPane.showMessageDialog (null, "Enter the signature file
name.", "", 1);

        return;

      }

      if (jTextField4.getText().isEmpty()){

        JOptionPane.showMessageDialog (null, "Enter the public key file
name.", "", 1);

        Return;

      }

       GenSig S = new GenSig ();


S.encrypt(jTextField1.getText(),jTextField3.getText(),jTextField4.getText())
;

   }
}
```

Σε περιβάλλον Microsoft Windows θα έχουμε την ακόλουθη εφαρμογή:



16.ΠΑΡΑΡΤΗΜΑ Β

16.1 ΒΑΣΙΚΑ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ

16. 1.1 ΟΔΗΓΙΑ 1993/93/ ΕΚ ΤΟΥ ΕΥΡΩΠΑΙΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 13ης Δεκεμβρίου 1999
σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές
ΤΟ ΕΥΡΩΠΑΙΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΙΚΗΣ 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,
τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής,
τη γνώμη της Επιτροπής των Περιφερειών,
αποφασίζοντας σύμφωνα με τη διαδικασία του άρθρου 251 της συνθήκης,
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 τις 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 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) 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, έρχονταν 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 χαρτοσήμανσης, 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 μόνον 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 ποιο τρόπο θα εξασφαλίστουν 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 μια ισορροπία μεταξύ των αναγκών των καταναλωτών και των επιχειρήσεων·

(15) το παράρτημα ΙΙΙ καλύπτει απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφών 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 τον διορισμό των φορέων που θα αναλάβουν την αξιολόγηση της πιστότητας των ασφαλών διατάξεων υπογραφής με το παράρτημα ΙΙΙ· για να ικανοποιούνται αυτές 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 τούς όρους και τις προϋποθέσεις βάσει των οποίων αποδέχονται ηλεκτρονικά υπογεγραμμένα δεδομένα,στο βαθμό που τούτο επιτρέπεται από την εθνική νομοθεσία, θα πρέπει να αναγνωρίζεαι 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 εθνικων κανόνων που αφορούν το ενοχικό δίκαιο, ιδίως την κατάρτιση κα εκτέλεση των συμβάσεων ή άλλες διαπιστώσεις μη συμβατικού χαρακτήρα σχετικά με τις υπογραφές· επομένως, οι διατάξεις που αφορούν τις έννομες συνέπειες των ηλεκτρονικών υπογαφών 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 ένα 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 προηγμένες 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 διάαξη 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 βασίζεαι 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 δέπεται 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 από το δικαστήριο·
(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 τη 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 Συμβουλιου, της 28ης Ιουνίου 1999, για τον καθορισμό των όρων άσκησης των εκτελεστικών αρμοδιοτήτων που ανατίθενται στην Επιτροπή·
(27) η Επιτροπή θα επανεξετάσει την παρούσα οδηγία δύο έτη μετά την εφαρμογή της, μεταξύ των 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 τις 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 παρουσα 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 είανι 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 εξασφαλίζει 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. η «ηλεκτρονική υπογραφή»: δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά σχετιζόμενα 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 εντοποιστεί 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 I απαιτήσεις και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τις οριζόμενες στο παράρτημα II 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 ενδιαφερομένου 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 I , 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 του παρόχων υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν για το κοινό αναγνωρισμένα πιστοποιητκά.
4. Η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς τις απαιτήσεις του παραρτήματος ΙΙΙ 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 ΙΙΙ 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 ΙΙ και στο παράρτημα ΙΙΙ, 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 ΙV 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' 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.

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 πάροχο 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 βεβαίωση ότι, κατά το χρόνο έκδοσης του πιστοποιητικού, ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό ήταν ο 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 πάροχος υπηρεσιών πιστοποίησης που εξέδωσε πιστοποιητικό ως ανεγνωρισμένο πιστοποιητικό στο κοινό υπέχει ευθύνη για τη ζημία που προξενείται 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 πιστοποίσης 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 αναγραφει 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.

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 διαπιστευθεί 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 προερχομένων 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.

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 την 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.
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
Η Επιτροπή

1. Η Επιτροπή επικουρείται από την «επιτροπή ηλεκτρονικής υπογραφής», καλουμένη 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 δημοσιεύτηκαν 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 το ταχύτερα 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 αξιόλογηση, 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

16.1.2 ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 150/2001

Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές

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 κα 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 αυτό 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 τους 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 οποιανδήποτε 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 (ΕΕΤΤ) (άρθρο 3 του ν. 2867/2000) ή από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς. Η ΕΕΤΤ 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 ΕΕΤΤ ή 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 ΕΕΤΤ 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 οι 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 ΕΕΤΤ έχει την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παρόχων 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 ΕΕΤΤ 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 της Ευρωπαϊκής Ένωσης, συνεπάγονται τις ίδιες έννομες συνέπειες με τις αντίστοιχες υπηρεσίες πιστοποίησης, που παρέρχονται 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 περιστατικού, ευθύνεται έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημία που προκλήθηκε σε βάρος του επειδή το πρόσωπο αυτό εύλογα βασίστηκε στο πιστοποιητικό, όσον αφορά: α) την ακρίβεια, κατά τη στιγμή της έκδοσής του, όλων

των πληροφοριών πο 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 είνα αναγνωρίσιμος από οποιονδήποτε τρίτο. Σ᾽αυτή την περίπτωση ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για τη ζημία που προκύπτει απ᾽λο 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 ΕΕΤΤ 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 ατόμπου 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 και Επικοινωνιών ενημερώνει την Ευρωπαϊκή Επιτροπή το ταχύτερο δυνατόν για την εφαρμογή των διατάξεων του άρθρου 4 του παρόντος.
2. Η ΕΕΤΤ ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίε 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 πίστοποιητικού 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 πάροχοι 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 τεχνικήκαι 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 με 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 έχουν 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 ΙΙΙ. 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 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 διασφαλίζεαι 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.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1.Κοσμάς Α. Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», Εκδόσεις Σάκκουλα,2008
2. Κ.Πατσάκης – Ε. Φούντας,«Κρυπτογραφία και Εφαρμογές»,Τόμος Α, Πανεπιστήμιο Πειραιώς
3. Στάσης Α-Σαριδάκης Ν Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση» ΕΚΔΔ- ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ
4.Στάσης Α-Κακλαμάνης Φ Εκπαιδευτικό υλικό «Ηλεκτρονική Διακυβέρνηση» ΕΚΔΔ- ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ
5.Μαρινοπούλου Μαρία, Εργασίας:Ηλεκτρονική Υπογραφή, ΤΕΙ Αθηνών,2008
6. Αλέξανδρος Κ. Σφάγγος, Διπλωματική εργασία,Ε.Μ.Π, 2005
7.ΕΣΠΑ 2007-2013 ΕΠ Ψηφιακή Σύγκλιση

ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

1. Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου
2. Προεδρικό διάταγμα 150/2001
3. Παράρτημα ΙΙΙ προεδρικό διάταγμα 150/2001
4. Π.Δ. 342/02
5. 295/63 Απόφαση της ΕΕΤΤ
6.ΦΕΚ 1730/Β/24-11-03
7.ΦΕΚ 603/Β'/16-5- 2002
8.Έγγραφο του ΥΠ.ΕΣΔΑΑ
9.Εγκύκλιος ΔΙΑΔΠ3753/19-02-2001

ΙΣΤΟΣΕΛΙΔΕΣ

1. http://www.go-online.gr, Νομικά ζητήματα
2. De Wikipedia, la enciclopedia libre
3. www.out-law.com/page-443
4. www.eett.gr
5.http://en.wikipedia.org/wiki/electronic signature
6. www.securitymanager
7. http:www.myphone.gr/forum
8. www.infolaw.gr, Εισήγηση Κ.Τσιμάρα ειδικός σύμβουλος του Γ.Γ Δημόσιας Διοίκησης στο Υπουργείο Εσωτερικών
9. www.vlioras.gr
10.www.papadi.gr,Δημήτρης Παπαδημητρίου,university Cardisoft
11. www.ebusinessforum.gr ,«Δεκάλογος για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά πιστοποίησης »Μ. Γιαννακάκη – Χ.Σιουλής

12 www.ebusinessforum.gr ,«Ηλεκτρονική Τραπεζική» Ανδρέα Μήτρακα
13.www. encrypted.google.com/,« Δίκτυα Η/Υ», Κ.Σ. Χειλάς
14www.dtps.unipi.gr Βασίλειος Ζορκάδης
15www.itlawyers.gr.«Ηλεκτρονικά έγγραφα με ηλεκτρονική υπογραφή», Γιαννακάκη Μαρία

ΣΧΕΔΙΑΓΡΑΜΜΑ

1.Κοσμάς Α. Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο», Εκδόσεις Σάκκουλα,2008