Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ηλεκτρονική κατάρτιση συμβάσεων-Ψηφιακές υπογραφές**
Ονοματεπώνυμο Φοιτητή	**Παναγιώτης Βαλαχέας**
Πατρώνυμο	**Πέτρος**
Αριθμός Μητρώου	**ΜΠΠΛ/ 07041**
Επιβλέπουσα	**Αριστέα Σινανιώτη-Μαρούδη Καθηγήτρια**

Τριμελής Εξεταστική Επιτροπή

Αριστέα Σινανιώτη-Μαρούδη Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής	Νικόλαος Αλεξανδρής Καθηγητής

Ημερομηνία Παράδοσης **Μάιος 2011**

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΚ	Αστικός Κώδικας
Α.Π.	Άρειος Πάγος
Αρμ.	Αρμενόπουλος
άρ.	άρθρο
αρ.	αριθμός
βλ.	βλέπε
Δ	Δίκη
ΔΕΕ	Δίκαιο Επιχειρήσεων και Εταιρειών
εδ.	εδάφιο
Ε.Ε.	Ευρωπαϊκή Ένωση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕλλΔνη	Ελληνική Δικαιοσύνη
ΕπισκΕμπΔ	Επισκόπηση Εμπορικού Δικαίου
Η/Υ	ηλεκτρονικός υπολογιστής
ιταλΑΚ	Ιταλικός Αστικός Κώδικας
ΚΠολΔ	Κώδικας Πολιτικής Δικονομίας
ΜΠρΑθ	Μονομελές Πρωτοδικείο Αθηνών
ΝοΒ	Νομικό Βήμα
ό.π.	όπως παραπάνω
παρ.	παράγραφος
Π.Δ.	Προεδρικό Διάταγμα
ΠΚ	Ποινικός Κώδικας
σελ.	σελίδα
ΧρΙΔ	Χρονικά Ιδιωτικού Δικαίου
ΕΚ	Ευρωπαϊκό Κοινοβούλιο

2 ΠΕΡΙΛΗΨΗ

Η Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές και το Π.Δ. 150/2001 το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία, εξομοιώνει απ ευθείας τις προηγμένες ηλεκτρονικές (ή ψηφιακές) υπογραφές με τις ιδιόχειρες υπογραφές. Οι προηγμένες ηλεκτρονικές (ή ψηφιακές) υπογραφές και τα ψηφιακά πιστοποιητικά ταυτοποίησης, που στηρίζονται στην σύγχρονη τεχνολογία της ασύμμετρης κρυπτογραφίας μπορούν να εξασφαλίσουν την αυθεντικότητα (authentication) και την ακεραιότητα (integrity) των σχετικών δεδομένων, την ταυτοποίηση (identification) των συναλλασσόμενων τη νομική δέσμευση του υπογράφοντα ή αλλιώς την μη αποκήρυξη (non repudiation) της συναλλαγής ενώ, παράλληλα, μπορούν να προσφέρουν αξιόπιστη λύση και στο ζήτημα της εμπιστευτικότητας (confidentiality) των δεδομένων κατά την διακίνηση ή/και την αρχειοθέτησή τους. Η τεχνολογία της ασύμμετρης κρυπτογραφίας, βάσει συγκεκριμένων μαθηματικών αλγορίθμων (π.χ. RSA, DSA, κ.ά.), παράγει τυχαία ζεύγη κρυπτογραφικών κλειδιών (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από δύο σημαντικές ιδιότητες: το καθένα κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το άλλο (συμπληρωματικό του) κλειδί, και δεν είναι δυνατό, με τις παρούσες δυνατότητες της τεχνολογίας, να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.

Παρόλα αυτά διατηρείται ακέραια η ανάγκη, -ιδίως σε ανοικτές εφαρμογές με πολλαπλούς ή ακόμη και άγνωστους αποδέκτες-, για την ύπαρξη μιας Έμπιστης Τρίτης Οντότητας που ονομάζεται Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) η οποία, επιπλέον, πιστοποιεί προς οποιοδήποτε τρίτο αποδέκτη μιας ψηφιακής υπογραφής. Ως ηλεκτρονικά πιστοποιητικά, με την ευρεία έννοια, νοούνται όλα τα αποδεικτικά στοιχεία που βρίσκονται σε ηλεκτρονική μορφή και τα οποία δημιουργούνται είτε αυτόματα είτε με πρωτοβουλία ενός συναλλασσόμενου κατά την διενέργεια μιας ηλεκτρονικής συναλλαγής. Συνήθως όμως ο όρος αναφέρεται ειδικότερα στα ψηφιακά πιστοποιητικά ταυτοποίησης ή Πιστοποιητικά Δημοσίου Κλειδιού (Public Key Certificates) τα οποία υποστηρίζουν την λειτουργία των προηγμένων ηλεκτρονικών (ή ψηφιακών) υπογραφών. Τα πιστοποιητικά αυτά είναι τυποποιημένες ηλεκτρονικές βεβαιώσεις που εκδίδονται και υπογράφονται ηλεκτρονικά από έναν ΠΥΠ με σκοπό να πιστοποιήσουν την κατοχή συγκεκριμένου ζεύγους (ασύμμετρων) κρυπτογραφικών κλειδιών .

ABSTRACT

The Directive 99/93/EC of the European Parliament on the Community framework for electronic signatures and Presidential Decree 150/2001 which aligned our national legislation with this Directive , treats directly the advanced electronic (or digital) signatures as handwritten signatures. The advanced electronic (or digital) signatures and digital certificates identity , based on modern technology asymmetric cryptography can guarantee the authentication and integrity of data, identification of transacting the legal commitment of the signatory or otherwise non-repudiation of the transaction while they can offer a credible alternative and the issue of confidentiality of data in the handling and storage. The technology of asymmetric cryptography**,** based on specific mathematical algorithms (eg. RSA, DSA, etc.), generates random cryptographic key pairs (digital data) which are characterized by two important properties**:** each key to encrypt digital data that can be decrypted only the other (complementary) key, and is not possible with current technology capabilities, to conclude or recreate a key when you know each other.

Still intact are necessary especially with multiple applications open or even unknown recipients, on the existence of a trusted third party entities called Certification Service Provider which also attests to any third recipient of a digital signature. The term electronic certificates, in the broadest sense, means all the evidence found in electronic format and are created either automatically or initiated by a trader when conducting an online transaction. But usually the term refers specifically to digital identity certificates or Public Key Certificate which support the operation of advanced electronic (or digital) signatures. These certificates are standard electronic certificates issued and signed electronically by a Certification Service Provider in order to certify the possession of this pair (asymmetric) cryptographic keys .

Ηλεκτρονική κατάρτιση συμβάσεων
Ψηφιακές υπογραφές

3 ΕΙΣΑΓΩΓΗ

Ανοιχτά δίκτυα όπως το Internet χρησιμοποιούνται σε ευρύτατη κλίμακα ως βάση επικοινωνίας σε διεθνές επίπεδο. Ανοιχτά και συνεπώς προσιτά, επιτρέπουν γρήγορη και αποτελεσματική ανταλλαγή πληροφοριών σε όλα τα μήκη και πλάτη της γης με πολύ χαμηλό κόστος. Επίσης τα ανοιχτά δίκτυα είναι κατάλληλα για την οργάνωση δημόσιων υπηρεσιών (π.χ φορολογική δήλωση ηλεκτρονικά), ενώ έχουν την δυνατότητα να συμβάλουν στο παγκόσμιο ηλεκτρονικό εμπόριο αγαθών και υπηρεσιών. Ωστόσο οι παραπάνω εξελίξεις της ηλεκτρονικής επικοινωνίας συνοδεύονται από τους ακόλουθους κινδύνους: τα μηνύματα μπορούν να παραποιηθούν, το κύρος των ηλεκτρονικών εγγράφων μπορεί να αμφισβητηθεί, η συλλογή των προσωπικών δεδομένων μπορεί να γίνει κατά τρόπο παράνομο. Για το λόγο αυτό η ανταλλαγή σημαντικών ηλεκτρονικών εγγράφων γίνεται συνήθως μόνο μέσω των λεγόμενων κλειστών δικτύων, όπου τα μέρη συνδέονται συμβατικά και μεταξύ αυτών υπάρχει αμοιβαία εμπιστοσύνη. Το μοντέλο αυτό δεν μπορεί να μεταφερθεί σε ανοιχτά δίκτυα, διότι απουσιάζουν τέτοιες σχέσεις μεταξύ των μερών. Το αποτέλεσμα λοιπόν είναι ότι η πρόκληση και τα πλεονεκτήματα του ηλεκτρονικού εμπορίου και της ηλεκτρονικής επικοινωνίας δεν μπορούν να αξιοποιηθούν στο μέγιστο βαθμό.

Η διενέργεια ολοκληρωμένων ηλεκτρονικών συναλλαγών μέσα από τα σύγχρονα ανοικτά δίκτυα επικοινωνιών, -όπως είναι το Internet και τα δίκτυα κινητής τηλεφωνίας-, προσφέρει σημαντικά οφέλη στους συναλλασσόμενους, όπως ταχύτητα και ευελιξία στις συναλλαγές και προηγμένες δυνατότητες αυτόματης διαχείρισής τους Παρόλα αυτά, η προώθηση και η μαζική αποδοχή ολοκληρωμένων ηλεκτρονικών μεθόδων (χωρίς να είναι απαραίτητη η φυσική παρουσία των συναλλασσομένων) για την διεκπεραίωση σημαντικών καθημερινών συναλλαγών στους βασικούς τομείς της οικονομίας (διοίκηση, εμπόριο, τραπεζικές υπηρεσίες, κ.λ.π.), εξακολουθεί να αναπτύσσεται τόσο στην Ελλάδα όσο και στο ευρωπαϊκό και διεθνές περιβάλλον με αρκετές επιφυλάξεις. Έτσι, τα έντυπα μέσα που χρησιμοποιούνται για την καταγραφή και την απόδειξη μιας συναλλαγής (π.χ. ενυπόγραφα ιδιωτικά έγγραφα, επικυρωμένα φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι, θεωρημένα τιμολόγια, κ.λπ.) αποτελούν τα κύρια αποδεικτικά στοιχεία μιας συναλλαγής. Η πλήρης αντικατάστασή τους με αντίστοιχα ψηφιακά δεδομένα που επιτρέπουν ολοκληρωμένες ηλεκτρονικές συναλλαγές, προϋποθέτει την χρήση ασφαλών και τεχνικώς αξιόπιστων μεθόδων πιστοποίησης της προέλευσης και της ακεραιότητας των δεδομένων και κυρίως αποδείξεων για την μη αποκήρυξη της συναλλαγής.

Συνεπώς για μια ωφέλιμη χρήση των προσφερόμενων μέσω ανοιχτών δικτύων ευκαιριών εμπορικής συναλλαγής είναι απαραίτητο ένα ασφαλές και αξιόπιστο ηλεκτρονικό περιβάλλον. Η τεχνολογική εξέλιξη των κρυπτογραφικών μεθόδων θεωρείται σημαντικό εργαλείο για την εξασφάλιση σιγουριάς και εμπιστοσύνης στην ηλεκτρονική επικοινωνία. Δύο σημαντικές εφαρμογές είναι οι ψηφιακές υπογραφές και η κρυπτογραφία. Οι ψηφιακές υπογραφές μπορούν να συμβάλουν στην απόδειξη της προέλευσης των δεδομένων (πιστοποίηση) και να επιβεβαιώσουν κατά πόσο τα δεδομένα έχουν υποστεί αλλοίωση ή όχι (ακεραιότητα). Η κρυπτογραφία συμβάλλει στη διατήρηση των δεδομένων και της επικοινωνίας κατά τρόπο εμπιστευτικό. Αποκλίνουσες νομικές και τεχνικές προσεγγίσεις θα δημιουργούσαν ένα σημαντικό εμπόδιο για την αγορά του Internet και θα παρακώλυαν την εξέλιξη νέων οικονομικών δραστηριοτήτων συναρτώμενων με το ηλεκτρονικό εμπόριο, Έτσι από νωρίς διαπιστώθηκε η επιτακτική ανάγκη για ένα κοινό κοινοτικό πλαίσιο για την εξασφάλιση ασφάλειας και εμπιστοσύνης στο ηλεκτρονικό εμπόριο καθώς και για την διασφάλιση της απρόσκοπτης λειτουργίας της αγοράς του Internet. Για το λόγο ότι η Ευρωπαϊκή Ένωση δεν θα μπορούσε να έχει ένα διάσπαρτο κανονιστικό πλαίσιο σε ένα πεδίο τόσο ζωτικό για την οικονομία ψηφίστηκε στις 13.12.1999 η οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις ηλεκτρονικές υπογραφές.

Η ανάπτυξη των συναλλαγών του ηλεκτρονικού εμπορίου (e-commerce) μέσω ανοικτών δικτύων προϋποθέτει την τόνωση της ασφάλειας και της εμπιστοσύνης των συναλλασσομένων μερών, σχετικά με την προέλευση και τη γνησιότητα των στοιχείων της συναλλαγής τους. Οι ηλεκτρονικές υπογραφές, εφαρμογή των πλέον σύγχρονων τεχνολογιών υλικού και λογισμικού

ηλεκτρονικών υπολογιστών, επιτελούν αξιόπιστα τις λειτουργίες αυτές εφόσον πληρούν συγκεκριμένες προδιαγραφές υψηλής ασφάλειας και πιστοποιούνται από ανεξάρτητα τρίτα πρόσωπα. Η Οδηγία 99/93/ΕΚ διαμορφώνει το κοινοτικό πλαίσιο αναγνώρισης των ηλεκτρονικών υπογραφών προβλέποντας ενδελεχείς ρυθμίσεις τεχνικού περιεχομένου και προϋποθέσεις υπό τις οποίες η ηλεκτρονική υπογραφή εξομοιούται με την ιδιόχειρη, τόσο από πλευράς ουσιαστικού όσο και δικονομικού δικαίου. Η πρόσφατη σχετική ρύθμιση του Έλληνα νομοθέτη (ΠΔ 150/2001) περιλαμβάνει αντίστοιχες προβλέψεις αναφορικά με τα αναγνωριζόμενα είδη ηλεκτρονικών υπογραφών, τις έννομες συνέπειες και τη διεθνή αναγνώρισή τους, καθώς και με τη λειτουργία, ευθύνη και εποπτεία των Παρόχων Υπηρεσιών Πιστοποίησης.

Οι ηλεκτρονικές συναλλαγές έχουν γνωρίσει τα τελευταία χρόνια τεράστια ανάπτυξη σε παγκόσμια κλίμακα, χάρη στην ταχεία τεχνολογική πρόοδο και την αλματώδη διάδοση του Διαδικτύου (Internet). Διεθνείς μελέτες έχουν προβλέψει, μάλιστα, σημαντικά μεγαλύτερη άνθηση τα αμέσως προσεχή έτη, υπογραμμίζοντας την αναγκαία προϋπόθεση να υπάρξει περισσότερη ασφάλεια και εμπιστοσύνη στις ηλεκτρονικές επικοινωνίες από τα ηλεκτρονικώς συναλλασσόμενα μέρη.

Εύλογες φαίνονται, επομένως, οι πρωτοβουλίες που λαμβάνουν τα περισσότερα ανεπτυγμένα κράτη για τη θέσπιση νομοθετικού πλαισίου σχετικά με την αναγνώριση των ηλεκτρονικών υπογραφών που, όπως αναπτύσσεται διεξοδικά κατωτέρω , παρέχουν τη δυνατότητα απόδειξης της γνησιότητας των στοιχείων των συναλλαγών. Στα πλαίσια αυτά, η Ευρωπαϊκή Ένωση υιοθέτησε έπειτα από νομοπαρασκευαστική διαδικασία διάρκειας δυόμιση ετών, η οποία έλαβε υπόψη της τις πλέον σύγχρονες τεχνολογικές εξελίξεις και τις διαφορετικές απόψεις των οργάνων της Ένωσης και των κρατών μελών, την Οδηγία 99/93 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές . Αναλύοντας τη ρύθμιση του προεδρικού διατάγματος 150/2001 το οποίο ενσωματώνει τη ρύθμιση της Οδηγίας στο ελληνικό δίκαιο, η παρούσα μελέτη οριοθετεί καταρχήν, την έννοια της ηλεκτρονικής υπογραφής και εξειδικεύει τις διάφορες μορφές υπό τις οποίες αναμένεται να εμφανιστεί στο συναλλακτικό πεδίο. Στη συνέχεια, αναπτύσσεται η έννοια, οι υποχρεώσεις και η ευθύνη των Παρόχων Υπηρεσιών Πιστοποίησης, που προβλέπεται να διαδραματίσουν εξαιρετικά σπουδαίο ρόλο στα πλαίσια της νέας ρύθμισης. Σε τελικό επίπεδο παρουσιάζονται, αντιπαραβάλλονται και εντάσσονται στο ισχύον σύστημα του αστικού και δικονομικού δικαίου μας τα είδη ηλεκτρονικών υπογραφών που προβλέπονται από τη νέα νομοθεσία, καθώς και διατυπώνονται συνολικά παρατηρήσεις και κριτικά σχόλια αναφορικά με την εφαρμογή της.

4 ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

4.1 Διαδίκτυο

Το 1957 η πρώην ΕΣΣΔ εκτοξεύει στο διάστημα τον πρώτο τεχνητό γήινο δορυφόρο, τον Σπούτνικ. Ως απάντηση, οι ΗΠΑ ιδρύουν την υπηρεσία ερευνητικών προγραμμάτων ARPA (Advanced Research Projects Agency) με σκοπό την αξιοποίηση της επιστήμης και της τεχνολογίας για στρατιωτικούς σκοπούς. Η Πολεμική Αεροπορία των ΗΠΑ αναθέτει στον Paul Baran , στέλεχος της κυβερνητικής υπηρεσίας Rand Corporation, να κάνει μια μελέτη για τον τρόπο με τον οποίο θα μπορούσε η Αεροπορία να διατηρήσει τον έλεγχο των βλημάτων και των βομβαρδιστικών αεροπλάνων της μετά από πυρηνική επίθεση. Ο Paul Baran το1962 προτείνει τη δημιουργία δικτύου Η/Υ, ενώ το 1969 η αμερικανική εταιρία συμβούλων BBN προτείνει το Network Control Protocol ως πρωτόκολλο επικοινωνίας μεταξύ των χρηστών ενός δικτύου. Έτσι, δημιουργείται το δίκτυο ARPANET (Advanced Research Projects Agency Network), το οποίο περιελάμβανε τέσσερις κόμβους: τα πανεπιστήμια της Γιούτα, της Σάντα Μπάρμπαρα, του Λος Άντζελες και το Ινστιτούτο Ερευνών του Στράτφορντ. Το 1972 δημιουργείται το πρώτο πρόγραμμα ηλεκτρονικού ταχυδρομείου από τον Ray Tomlinson και το 1973 μια ομάδα επιστημόνων, καθοδηγούμενη από τον Vinton Cerf του Πανεπιστημίου του Στάνφορντ και τον Robert Kahn, μέλος της ARPA, ξεκινά ένα ερευνητικό πρόγραμμα επιδιώκοντας να διερευνήσει πιθανές νέες τεχνικές και τεχνολογίες για τη σύνδεση δικτύων

Η/Υ μεταξύ τους. Ο στόχος ήταν να αναπτυχθούν εκείνα τα πρωτόκολλα επικοινωνίας που θα επέτρεπαν στους δικτυωμένους Η/Υ να επικοινωνούν. Αυτό το πρόγραμμα ονομάστηκε Internetting και το σύστημα των δικτύων που προέκυψε από την έρευνα έγινε γνωστό ως Internet, η πρώτη φορά που χρησιμοποιείται αυτός ο όρος. Το σύστημα των πρωτοκόλλων που αναπτύχθηκε κατά τη διάρκεια αυτής της ερευνητικής προσπάθειας έγινε γνωστό ως TCP/IP, από τα δύο αρχικά πρωτόκολλα που αναπτύχθηκαν, δηλαδή το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο Διαδικτύου (IP) (Kristula, The History of the Internet, 2001, στην ηλεκτρονική διεύθυνση http://www.davesite.com/ webstation/net-history.html) .

Πριν από μερικά χρόνια, όταν το Internet έπαψε να χρησιμοποιείται μόνο για στρατιωτικούς σκοπούς και η χρήση του επιτράπηκε στο ευρύ κοινό, πολλοί πίστεψαν ότι το δίκτυο δεν αποτελεί παρά μία απασχόληση για έφηβους και παθιασμένους τεχνικούς ηλεκτρονικών υπολογιστών. Τελευταία πολύς λόγος γίνεται για τα δίκτυα, τα οποία αναπτύσσονται ταχύτατα και αποτελούν τη βάση εφαρμογής των νέων τεχνολογιών. Τα πεδία ηλεκτρονικής επικοινωνίας συμβάλλουν στη διάδοση του διαδικτύου ως ενός ανοικτού δικτύου. Στο διαδίκτυο μπορεί καθένας να απολαμβάνει ελεύθερη πρόσβαση και με ελάχιστες διατυπώσεις, να καρπώνεται τις υπηρεσίες του (Καράκωστας , Δίκαιο & Internet- Νομικά ζητήματα του διαδικτύου, Σάκκουλας Αθήνα 2003, 2η έκδοση , σελ. 3-4).

Είναι λοιπόν προφανές ότι το διαδίκτυο έχει εισβάλλει στην καθημερινή μας ζωή. Πολλές δραστηριότητες εξελίσσονται μέσω του παγκόσμιου ιστού Από το σύνολο των σύγχρονων εφαρμογών σημειώνουμε ενδεικτικά την επικοινωνία, την ενημέρωση, τις συναλλαγές (Ιγγλεζάκης Ιωάννης, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Σάκκουλας Αθήνα - Θεσσαλονίκη 2003, σελ.25-29). Η χρήση του διαδικτύου είναι ευρεία και η εξάπλωσή του ραγδαία. Οι δε υπηρεσίες που λειτουργούν είναι κυρίως το world wide web, το ηλεκτρονικό ταχυδρομείο, ενώ αναμένεται στο μέλλον να δημιουργηθούν επιπρόσθετες καινοτόμες εφαρμογές με φιλικότερη προσέγγιση από το χρήστη (Καράκωστας, ο.π , σελ. 8-10).

4.2 Σύγχρονες συναλλαγές

Κοινή διαπίστωση αποτελεί η ιδιαίτερη ώθηση που δόθηκε από το διαδίκτυο στις σύγχρονες συναλλαγές. Το προσβάσιμο σε όλους δίκτυο του Internet παρέχει μία ιδανική βάση για εμπορικές συναλλαγές σε παγκόσμια βάση, οι οποίες δεν περιορίζονται μόνο μεταξύ επιχειρήσεων αλλά περιλαμβάνουν και απευθείας συναλλαγές μεταξύ επιχειρήσεων και καταναλωτών Αυτό επέδρασε καταλυτικά στη διαμόρφωση και διάδοσή τους (Takach , Internet Law: Dynamics, Themes and Skill Sets, The Canadian Business Law Journal, Volume 32 ,1999, 1). Η άνθηση των συναλλαγών που πραγματοποιούνται μέσω του διαδικτύου οφείλεται κυρίως στο γεγονός ότι η διαδικασία αυτή είναι σχεδόν ανέξοδη, ταχύτατη και ασφαλής για τους συναλλασσομένους.

Είναι δε σαφές ότι με την εγκαθίδρυση της νέας τεχνολογίας η συναλλακτική σχέση έχει ξεπεράσει τα όποια εμπόδια γεωγραφικά με παράλληλη ανάπτυξη πτυχών και δυνατοτήτων άγνωστων έως σήμερα όπως για παράδειγμα η ροή των πληροφοριών και η κατ'επέκταση άμεση συμμετοχή του κοινού στη διακίνηση προϊόντων και υπηρεσιών. Ευρύτερα οι διαδικτυακές συναλλαγές είναι αυτές οι οποίες συντελούνται στα πλαίσια της υποδομής του διαδικτύου, έστω και με διάφορες εφαρμογές. Οι διαδικτυακές συναλλαγές, ως η πιο σύγχρονη τεχνολογική έκφραση των συναλλαγών, εκφράζουν τη σημερινή πραγματικότητα, αλλά και την τάση του μέλλοντος. Η παγκόσμια οικονομία μετακινείται πλέον από μία κατεξοχήν μεταβιομηχανική οικονομία των υπηρεσιών σε μία ψηφιακή οικονομία, που ανήκει στην κοινωνία της πληροφορίας (Αριστέα Σινανιώτη-Μαρούδη, Ιωάννης Δ. Φαρσαρώτας, Ηλεκτρονική τραπεζική , Σάκκουλας 2005 ,σελ.75).

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

- Να πιστοποιεί την αυθεντικότητα (authentication) της ταυτότητας του κάθε συναλλασσομένου.

- Να διαφυλάσσει την ακεραιότητα (integrity), δηλαδή το αναλλοίωτο του περιεχομένου του μηνύματος.
- Να εξασφαλίζει την εμπιστευτικότητα (confidentiality), δηλαδή, την προστασία του αποστελλόμενου μηνύματος από την πρόσβαση σε αυτό μη εξουσιοδοτημένων προσώπων .
- Να εξασφαλίζει τη μη αποποίηση (non-repudiation) ευθύνης, δηλαδή την ανυπαρξία δυνατότητας των εμπλεκομένων σε μια ηλεκτρονική συναλλαγή μερών να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή (Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία μετά τις νέες κοινοτικές ρυθμίσεις, Σάκκουλας 2001, σελ. 11).

4.3 Η σύγχρονη οικονομική διάσταση

Η ώθηση των εμπορικών συναλλαγών σε παγκόσμια διάσταση είναι κυρίως προϊόν του διαδικτύου (Γεωργιάδης Γ., Η σύναψη συμβάσεως μέσω του διαδικτύου, Σάκκουλας Αθήνα Κομοτηνή 2003, σελ.17-20). Βασικός λόγος αυτής της πραγματικότητας είναι και η διάχυση της πληροφόρησης των καταναλωτών - χρηστών του διαδικτύου (Ψούνη - Ζορμπά, Δήλωση βουλήσεως μέσω ηλεκτρονικού υπολογιστή. Ένταξη στο σύστημα του Α.Κ. - Δυνατότητες ακύρωσης, Σάκκουλας Θεσσαλονίκη 1988 , σελ.4-5). Εξάλλου, ο ρόλος που έχει αναλάβει το Internet δεν περικλείεται μόνο στην ολοκλήρωση της συναλλαγής, αλλά και στην προετοιμασία της. Η ενημέρωση αποτελεί πρόγονο μιας συναλλαγής και σε πολλές περιπτώσεις ακρογωνιαίο λίθο στην επισφράγισή της. Ενώ, σε πολλές περιπτώσεις η διαδικτυακή συναλλαγή δύναται να εκπληρωθεί μόνο δια μέσω της υποδομής αυτής (Δελούκα - Ιγγλέση, Νομικά Θέματα Ηλεκτρονικού Εμπορίου, Σάκκουλας Αθήνα Κομοτηνή 2005, σελ. 25). Εν προκειμένω, ο λόγος για τις συναλλαγές μη απευθείας σύνδεσης (off line) και τις συναλλαγές απευθείας σύνδεσης (on line) με το Internet. Οι πρώτες παρουσιάζουν ομοιότητες με τις συμβάσεις από απόσταση με τη χρήση τηλεφώνου, ταχυδρομείου ή άλλων τεχνικών. Οι on line συναλλαγές αποτελούν μια νέα συναλλακτική μορφή, η οποία σε όλο της το φάσμα διακρίνεται για τη συμβολή της διαδικτυακής υποδομής. (Οδηγία 2000/31/ΕΚ). Σε κάθε περίπτωση η ψηφιακή οικονομία αρχίζει να αποδίδει σε ένα παγκοσμιοποιημένο περιβάλλον, όπου στοιχεία, όπως ο αυξημένος ανταγωνισμός και η ροή πληροφοριών, καταλύουν τους φραγμούς της οικονομίας και σχηματίζουν την πραγματικότητα της νέας αγοράς.

Το ηλεκτρονικό εμπόριο προσφέρει στον καταναλωτή μια σειρά πλεονεκτημάτων σε σχέση με τον παραδοσιακό τρόπο αγοράς προϊόντων και υπηρεσιών, όπως είναι το χαμηλότερο κόστος των αγορών και η ταχύτερη ολοκλήρωση των συναλλαγών, πλεονεκτήματα που οφείλονται στην αμεσότερη επικοινωνία που επιτυγχάνεται μεταξύ προμηθευτή και καταναλωτή και στη μείωση του ρόλου του ανθρώπινου παράγοντα. Επιπλέον, το ηλεκτρονικό εμπόριο εξασφαλίζει στον καταναλωτή άνεση κατά τις αγορές του, προσφέροντας του τη δυνατότητα να έχει από το σπίτι του πρόσβαση σε υπηρεσίες και αγαθά προερχόμενα από κάθε περιοχή του πλανήτη όπως ηλεκτρονική μεταφορά κεφαλαίων, οι ηλεκτρονικές αγοραπωλησίες μετοχών ηλεκτρονικοί πλειστηριασμοί, η διαφήμιση και προώθηση προϊόντων (Καραδημητρίου Κοσμάς, Ηλεκτρονικές υπογραφές: προβλήματα και σκέψεις με αφορμή το Π.Δ. 150/2001. Αρμ. 2002, σελ. 1535).

Προκειμένου όμως οι ηλεκτρονικά συναλλασσόμενοι να έχουν τη δυνατότητα να ολοκληρώνουν απρόσκοπτα τις εμπορικές τους συναλλαγές, απαιτείται η συνδρομή των παρακάτω προϋποθέσεων:

- Να υπάρχει ένα σύγχρονο τηλεπικοινωνιακό δίκτυο, πράγμα που επιβάλλει τον εκσυγχρονισμό των υφισταμένων εθνικών δικτύων αλλά και τη δημιουργία ενός σύγχρονου παγκόσμιου δικτύου, το οποίο θα επιτρέπει την ταχεία μετάδοση των δεδομένων και των εφαρμογών, όπως η τηλεϊατρική.
- Να προσφέρονται στον καταναλωτή τηλεπικοινωνιακές υπηρεσίες σε προσιτή τιμή. Για το λόγο αυτό απαραίτητη είναι η απελευθέρωση της αγοράς των τηλεπικοινωνιών, ώστε να αυξηθεί ο ανταγωνισμός και να υποχωρήσει το κόστος πρόσβασης στο Διαδίκτυο.
- Να διατηρεί κάθε δραστηριοποιούμενη στο ηλεκτρονικό εμπόριο επιχείρηση ιστοσελίδα, η οποία θα είναι λειτουργική και ενημερωμένη(Σιδηρόπουλος, Εισαγωγή στο δίκαιο του ηλεκτρονικού εμπορίου, 2000, σελ. 17 -18).

Ηλεκτρονική κατάρτιση συμβάσεων

Ψηφιακές υπογραφές

Στις τραπεζικές συναλλαγές πραγματοποιείται μια επανάσταση. Η ηλεκτρονική μεταφορά κεφαλαίων σε οποιοδήποτε σημείο του πλανήτη είναι πλέον εφικτή σε λίγα δευτερόλεπτα. Με εφαρμογές όπως το electronic banking, οι τραπεζικοί πελάτες έχουν τη δυνατότητα να διαβιβάζουν ηλεκτρονικά εντολές χρέωσης ή πίστωσης του λογαριασμού τους, να παρακολουθούν την κίνηση του λογαριασμού τους σε κάθε μέρος του πλανήτη, να ζητούν την έκδοση εγγυητικών επιστολών, να εξοφλούν λογαριασμούς πιστωτικών καρτών και να ενημερώνονται για τις τιμές συναλλάγματος. Η ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές και η ευκολία στη χρήση που έχει επιτευχθεί είναι ο βασικότερος παράγων επιτυχίας της ηλεκτρονικής τραπεζικής στις καθημερινές συναλλαγές. Η παραδοσιακή τράπεζα χωρίζεται σε κέντρα παραγωγής και κέντρα διανομής τραπεζικών προϊόντων, και με τον τρόπο αυτό επιτυγχάνεται η επιθυμητή εξειδίκευση.

Οι περισσότερες εμπορικές τράπεζες προσφέρουν τη δυνατότητα βασικών τραπεζικών εργασιών και υπηρεσιών μέσω του Internet όπως η μεταφορά χρηματικών ποσών μεταξύ λογαριασμών, η πληρωμή λογαριασμών κοινής ωφελείας και πιστωτικών καρτών, η παρακολούθηση της κίνησης του λογαριασμού, η κατάθεση αίτησης για πιστωτική κάρτα ή δάνειο, η αναλυτική ενημέρωση για προσφερόμενα προϊόντα και υπηρεσίες, αλλά και η διεξαγωγή διάφορων χρηματιστηριακών συναλλαγών, χορήγηση δάνειου μέσω του Internet ή παροχή καταθετικών προϊόντων. Τα προσφερόμενα με ηλεκτρονικό τρόπο τραπεζικά προϊόντα «επιδοτούνται» από τις τράπεζες, καθώς τα επιτόκια τους είναι καλύτερα από αυτά που προσφέρονται στα καταστήματα. Ειδικότερα σε ό,τι αφορά τα καταθετικά προϊόντα, τα διατιθέμενα αποκλειστικά προς τους χρήστες του διαδικτύου, έχουν υψηλότερο επιτόκιο σε σχέση με τα προσφερόμενα από τα τραπεζικά γκισέ. Αντίστοιχα τα δάνεια μέσω Internet έχουν χαμηλότερο επιτόκιο. Οι τράπεζες με τις ηλεκτρονικές τραπεζικές εργασίες μειώνουν σημαντικά το λειτουργικό κόστος τους και είναι σε θέση να τιμολογούν και να πωλούν φθηνότερα και πιο κερδοφόρα τα προϊόντα τους. Υπολογίζεται ότι μια τραπεζική συναλλαγή κοστίζει στις τράπεζες τέσσερις έως πέντε φορές ακριβότερα όταν πραγματοποιείται μέσω του παραδοσιακού δικτύου από ό,τι μέσω του Internet. Σε γενικές γραμμές τα λειτουργικά έξοδα μιας ηλεκτρονικής τράπεζας υπολογίζονται περίπου στο μισό αυτών μιας συμβατικής τράπεζας. Το όφελος όσων χρησιμοποιούν τις προσφερόμενες υπηρεσίες είναι κυρίως το γεγονός ότι μπορούν με μεγαλύτερη άνεση να κάνουν τραπεζικές συναλλαγές 24 ώρες το 24ωρο(Σινανιώτη-Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης, Ηλεκτρονική τραπεζική , Σάκκουλας 2005 ,σελ.139).

5 ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΣΥΜΒΑΣΕΙΣ

5.1 Ηλεκτρονικά μέσα και δικαιοπραξίες

Η έννοια των ηλεκτρονικών μέσων δεν θα ήταν εύστοχο να περιοριστεί με την τρέχουσα τεχνολογική ανάπτυξη σε εξέλιξη. Ωστόσο, θα μπορούσε να δοθεί ένας περιγραφικός ορισμός, ώστε να γίνουν αντιληπτά τα μέσα αυτά. Στο πλαίσιο αυτό, μπορούν να παρατεθούν ενδεικτικά ως ηλεκτρονικά μέσα όλα τα επιτεύγματα τα οποία λειτουργούν με βάση τις ηλεκτρονικές υπηρεσίες και τις υποστηρίζουν περαιτέρω. Ουσιαστικά αυτά είναι προγράμματα τα οποία λειτουργούν με βάση ειδικό software και δραστηριοποιούνται στο διαδίκτυο. Ενώ δε σημειώνεται και το νομοθετικό ενδιαφέρον της Ε.Ε. για τη χρήση των μέσων αυτών, παράδειγμα θεσμοθέτησής τους αποτελεί και η αναφορά που γίνεται στην Οδηγία 2001/115/ΕΚ για την διαβίβαση τιμολογίων με ηλεκτρονικά μέσα.Εντοπίζεται λοιπόν άμεση σχέση μεταξύ της ηλεκτρονικής τεχνολογίας και υπηρεσιών. Έτσι, μια σειρά προϊόντων και υπηρεσιών διακρίνονται ως προς το κοινό τεχνολογικό τους επίπεδο. Σε κάθε περίπτωση, κύριο ρόλο διαδραματίζει το επίπεδο της τεχνολογίας και δευτερεύοντα τα μέσα που λειτουργούν σε αυτό το επίπεδο(Χάνος Αντώνιος, Δίκαιο και τεχνολογική εξέλιξη στην κοινωνία των πληροφοριών - Με παράδειγμα το διοικητικό δίκαιο – ΕΕΝ, 2000 ,σελ. 7).

Η σύγχρονη τεχνολογία καθιστά δυνατή την κατάρτιση δικαιοπραξιών και με ηλεκτρονικά μέσα. Όμως και ως προς την εκτέλεση της δικαιοπραξίας μπορεί να λεχθεί ότι, ανάλογα με το αντικείμενο, μπορεί επίσης να εκτελείται αποκλειστικά με ηλεκτρονικά μέσα.

Πρόκειται για τις περιπτώσεις που αφορούν στη μεταβίβαση άυλων προϊόντων ή υπηρεσιών, όπως η αγορά λογισμικού, οι χρηματοπιστωτικές συναλλαγές κ.α.. Η συνάρτηση της χρήσης των ηλεκτρονικών μέσων και του αντικειμένου μιας δικαιοπραξίας την προσδιορίζουν περαιτέρω. Εδώ γίνεται η διάκριση των δικαιοπραξιών σε δικαιοπραξίες απευθείας σύνδεσης και μη απευθείας σύνδεσης. Στο ενδιάμεσο τοποθετούνται οι δικαιοπραξίες σχεδόν απευθείας σύνδεσης, οι οποίες μπορεί να καταρτίζονται ηλεκτρονικά και να εκτελούνται με τους παραδοσιακούς τρόπους ή αντιστρόφως να συντάσσονται με κλασικά μέσα και να εκπληρώνονται οι παροχές ηλεκτρονικά (Γεωργιάδης Γ., ο.π , σελ.6-28 , Ιγγλεζάκης, ο.π , σελ.17-19).

Η διάσταση πάντως μιας ηλεκτρονικής δικαιοπραξίας συνοψίζεται κυρίως στη χρήση του διαδικτύου, γεγονός που τροφοδοτεί και τη χρήση των ηλεκτρονικών μέσων. Έτσι η συμβολή του Internet σε μια δικαιοπραξία επιφέρει μεταβολή στο κανονιστικό της πλαίσιο .Ο καταναλωτής πρέπει να έχει εγκαίρως την σχετική πληροφόρηση τόσο για το στάδιο πριν από την κατάρτιση της σύμβασης όσο και για το στάδιο κατά την εκτέλεση της(Σινανιώτη-Μαρούδη, Αριστέα , Ιωάννης Δ. Φαρσαρώτας, ο.π, σελ.126).

Όπως θα καταδειχθεί η διαδικτυακή τεχνολογία επηρεάζει σημαντικά τη σύσταση των εν λόγω δικαιοπραξιών τυπικά και ουσιαστικά. Η εξέλιξη των συναλλαγών με την ανάπτυξη του ηλεκτρονικού εμπορίου δια του διαδικτύου (Internet) τείνει να έχει επιπτώσεις στην εξέλιξη της διαμεσολαβητικής λειτουργίας. Συγκεκριμένα, η τεχνολογία έχει επιτρέψει στον παραγωγό να έρχεται σε απευθείας επαφή με τον καταναλωτή (direct marketing), ο οποίος μπορεί να παραγγείλει τα εμπορεύματα μέσω του υπολογιστή του, γεγονός που παρατηρείται ιδιαίτερα στα συστήματα δικαιόχρησης (franchising) στο εξωτερικό. Οι νέες τεχνολογίες μαζί με την παγκοσμιοποίηση, εντείνουν τον διεθνή ανταγωνισμό και αλλάζουν τον ρυθμιστικό ρόλο του κράτους, αλλά ταυτόχρονα δίνουν νέες δυνατότητες συμμετοχής στη διεθνή αγορά, στις μικρομεσαίες επιχειρήσεις και στις χώρες της περιφέρειας. Η τεχνολογία αποτελεί πλέον προϋπόθεση για την ανταγωνιστικότητα των επιχειρήσεων και τον κύριο υποκινητή της παραγωγικότητας και της οικονομικής ανάπτυξης. Οι παραδοσιακές οικονομικές δραστηριότητες και ο παραγωγικός ιστός υφίστανται δραστικές μεταβολές, τόσο ως προς τον τρόπο λειτουργίας τους όσο και ως προς την ίδια τους την ταυτότητα και δομή. Παράλληλα, καινοτόμες δραστηριότητες δημιουργούν νέα προϊόντα και υπηρεσίες και αλλάζουν τη διάρθρωση της οικονομίας, ενώ παρουσιάζονται νέοι τρόποι ενίσχυσης και ανάπτυξης της οικονομικής και επιχειρηματικής δραστηριότητας όπως franchising, leasing, factoring, κ.ά (Γκοτσοπούλου, Ηλεκτρονικό εμπόριο και δικαιόχρηση (franchising), ΔΕΕ (3) 2002, σελ.250 , Ζέκο, Franchising και Cyberspace, ΔΕΕ (1) 2001, σελ.52).

5.2 Οι συμβάσεις EDI

Ιδιαίτερη κατηγορία ηλεκτρονικών συμβάσεων αποτελούν οι συμβάσεις EDI (Electronic Data Interchange) . (Η Δελούκα-Ιγγλέση, ο.π , σελ.26, το αποδίδει στα ελληνικά ως ηλεκτρονική ανταλλαγή εμπορικών δεδομένων). Πρόκειται για συμβάσεις ανταλλαγής δεδομένων μεταξύ προκαθορισμένων μερών και συνήθως λαμβάνουν χώρα σε κλειστά δίκτυα. Το περιεχόμενο των συμβάσεων αυτών είναι περιορισμένο και αφορά στην ανταλλαγή δεδομένων. Ενώ, της σύναψης των συμβάσεων αυτών προηγείται σύμβαση τυποποίησης, στην οποία εμπεριέχονται οι όροι της ηλεκτρονικής επικοινωνίας(Καράκωστας, ο.π, σελ.188).

Με τη χρήση της τεχνολογίας EDI επιτυγχάνεται η αυτόματη μετάδοση τυποποιημένων μηνυμάτων, καθιστώντας εφικτή την ταχύτερη και ασφαλέστερη μεταβίβαση των πληροφοριών. Η πληροφορία διακινείται από έναν υπολογιστή σε έναν άλλον, χωρίς ανθρώπινη παρέμβαση, επιτρέποντας κατ αυτόν τον τρόπο την εξοικονόμηση πολύτιμου χρόνου και κόστους. Ταυτόχρονα μειώνονται οι πιθανότητες σφαλμάτων οφειλόμενων σε ενδεχόμενη ανθρώπινη παρέμβαση και ελαχιστοποιείται ο χρόνος που παρεμβάλλεται από την ανάληψη μιας παραγγελίας ως την εκτέλεση της. Η χρήση της Ηλεκτρονικής Ανταλλαγής Δεδομένων (EDI) από τις επιχειρήσεις έχει ως αποτέλεσμα την άμεση ανταπόκριση τους στις απαιτήσεις των πελατών μέσα στα πλαίσια του συνεχώς αυξανόμενου ανταγωνισμού, ο οποίος επικρατεί στην παγκόσμια αγορά(Σινανιώτη-Μαρούδη, Αριστέα , Ιωάννης Δ. Φαρσαρώτας, ο.π, σελ.115).

Σημειώνεται ότι τέτοιου είδους συμβάσεις δεν έχουν εδραιωθεί, όπως οι ηλεκτρονικές συμβάσεις των ανοικτών δικτύων. Ζητήματα όπως το υψηλό κόστος, η πολυπλοκότητα χρήσης, η συνήθης πρακτική επαλήθευσης μηνυμάτων, ο μικρός όγκος διακινούμενων δεδομένων και η εν γένει πολυπλοκότητα της επικοινωνίας αποτέλεσαν τροχοπέδη στην ευρεία αποδοχή του εξειδικευμένου αυτού τρόπου επικοινωνίας.

5.3 Ηλεκτρονική δήλωση βουλήσεως

Ουσιώδης παράγοντας για την κατάρτιση συμβάσεων αποτελεί, με βάση το αστικό δίκαιο, η δήλωση βούλησης που περιέχει πρόταση σύναψης σύμβασης και η αποδοχή της (Παπαντωνίου, Γενικές αρχές του αστικού δικαίου, 3η έκδ. 1983, σελ. 303). Στην περίπτωση της κατάρτισης συμβάσεων στο Internet πρέπει κατ'αντιστοιχία να υπάρχει ηλεκτρονική δήλωση βούλησης, που περιέχει πρόταση σύναψης σύμβασης και ηλεκτρονική δήλωση αποδοχής της πρότασης. Ουσιώδη και επουσιώδη στοιχεία θα εξεταστούν με σκοπό να παρουσιαστεί ο βαθμός της διαφοροποίησης της νέας μορφής δικαιοπραξίας. Η ηλεκτρονική δήλωση βούλησης που διαβιβάζεται μέσω Internet δεν διαφέρει από την συνηθισμένη δήλωση βούλησης του αστικού δικαίου, παρά μόνο ως προς τον τρόπο μετάδοσής της, που γίνεται ηλεκτρονικά, δηλαδή μέσω ηλεκτρονικού υπολογιστή. Ως προς τη δεσμευτική χροιά της ηλεκτρονικής δήλωσης βούλησης δεν υπάρχει αμφιβολία, πως και οι ηλεκτρονικά διαβιβαζόμενες δηλώσεις, μέσω για παράδειγμα ηλεκτρονικού ταχυδρομείου, που έχουν συσταθεί από τον ίδιο τον δηλούντα προσωπικά αποτελούν καθόλα έγκυρες δηλώσεις βούλησης, εφόσον βέβαια πληρούνται όλες οι προϋποθέσεις εγκυρότητάς τους με βάση το κοινό αστικό δίκαιο (άρθρα 127. ΑΚ https://www.nbonline.gr/actions).Ειδικότερα, η δήλωση βουλήσεως αποτελεί συστατικό της δικαιοπραξίας και χρονικά το πρώτο στοιχείο της. Στον ΑΚ δεν γίνεται συγκεκριμένη αναφορά στην ηλεκτρονική μορφή με την οποία μπορεί αυτή να εξωτερικεύεται (Ψούνη - Ζορμπά, ο.π, σελ.38).

Γνώμονας της ηλεκτρονικής δήλωσης βουλήσεως είναι η χρήση της ηλεκτρονικής τεχνολογίας στη διαμόρφωσή της, αλλά και στην εξωτερίκευση -μετάδοσή της (Ψούνη - Ζορμπά, ο.π , σελ.36). Σε κάθε περίπτωση, η διαμόρφωση της δήλωσης βουλήσεως ανήκει στον δηλούντα(Γεωργιάδης Γ., ο.π, σελ.32). Έπειτα αυτός αποφασίζει ποιο μέσο θα χρησιμοποιήσει, ώστε να εξωτερικευτεί το περιεχόμενό της. Ο ρόλος του η/υ περιορίζεται στη διαβίβασή της, χωρίς να λαμβάνει περαιτέρω πρωτοβουλίες πριν τουλάχιστον τη συγκατάθεση του χρήστη του (Καράκωστας, ο.π, σελ. 181). Ιδιαίτερο χαρακτηριστικό της ηλεκτρονικής επικοινωνίας αποτελεί το ηλεκτρονικό ταχυδρομείο μέσω του οποίου αναπτύσσεται η επικοινωνία των συμβαλλόμενων μερών. Πιο συγκεκριμένα, η δήλωση βουλήσεως και μάλιστα η πρόταση αποστέλλεται μέσω e-mail προς την ηλεκτρονική διεύθυνση αλληλογραφίας ενός προσώπου. Εκτός όμως από αυτή τη μορφή επικοινωνίας, ταυτόσημη είναι και αυτή που διεξάγεται μέσω του παγκόσμιου ιστού (world wide web). Δηλαδή διατύπωση πρότασης η οποία μορφοποιείται στη βάση προεπιλεγμένων ηλεκτρονικών ενοτήτων, όπως αυτές παρουσιάζονται σε μία ιστοσελίδα, στην οποία προσφέρονται αγαθά ή υπηρεσίες προς το ευρύ κοινό(Καράκωστας , ο.π, σελ.181). Αμεσότερη όμως εμπορική επικοινωνία επιτυγχάνεται με τη χρήση των sites. Εν προκειμένω αυτά θεωρούνται ως προτάσεις και απευθύνονται προς αποδοχή από τους διαδικτυακούς καταναλωτές. Έτσι, ο ενδιαφερόμενος εάν επιθυμεί να ξεκινήσει διαπραγματεύσεις θα πρέπει με δική του πλέον πρωτοβουλία να απευθύνει την πρόταση προς τον πάροχο, ο οποίος με τη σειρά του θα αποφασίσει την επιλογή σύναψης σύμβασης ή όχι.

Αναφορικά με την ηλεκτρονική αποδοχή, αυτή θα πρέπει να είναι σύμφωνη με την πρόταση, άλλως θα επέχει θέσης αντιπρότασης. Πάντως όπως συμβαίνει και με την πρόταση, ομοίως και στις περιπτώσεις της αποδοχής παρατηρείται η συχνή χρήση του ηλεκτρονικού ταχυδρομείου. Ενώ, μια άλλη επιλογή είναι η αποστολή ηλεκτρονικού εγγράφου κυρωμένου με ηλεκτρονική υπογραφή. Ενδεχομένως, δύναται και η αποδοχή μιας ηλεκτρονικής πρότασης να γίνει σιωπηρώς κατά τα πρότυπα του κλασικού δικαίου. Ενόψει αυτών, οι έννοιες της αποστολής και της λήψης των δηλώσεων βουλήσεως θεωρούνται ανάλογες με τον παραδοσιακό κανόνα του γραμματοκιβωτίου.

Ηλεκτρονική κατάρτιση συμβάσεων

Ψηφιακές υπογραφές

Η επιτυχία της αποστολής συντελείται όταν απευθύνθηκε προς την ορθή διεύθυνση του παραλήπτη και στάλθηκε σύμφωνα με τις οδηγίες του. Επιπλέον, το μήνυμα με την περιεχόμενη δήλωση βουλήσεως κρίνεται ως ληφθέν, όταν περιέλθει επιτυχώς στη σφαίρα εξουσίας του παραλήπτη, όπου αναμένεται πως τούτος θα λάβει γνώση του περιεχομένου της. Η θεωρία της λήψης είναι αυτή που ακολουθείται στο εθνικό δίκαιο σύμφωνα με το άρθρο 167 ΑΚ. Εν προκειμένω γίνεται παραλληλισμός του κλασικού γραμματοκιβωτίου του παραλήπτη με το μήνυμα που έχει περιέλθει στο διακομιστή, δηλαδή πριν ακόμη την άφιξή του στον υπολογιστή του παραλήπτη. Θα πρέπει να σημειωθεί ότι η δήλωση βουλήσεως ως προς τα στοιχεία του τόπου και του χρόνου χρήζει περαιτέρω εμβάθυνσης (Μανιώτης ,Η σύναψη της ηλεκτρονικής συμβάσεως και η ευθύνη των παρεχόντων συνδρομή στην κατοχύρωση της γνησιότητας και του αναλλοίωτου των ηλεκτρονικών εγγράφων , Σάκκουλας Αθήνα Κομοτηνή 2003, σελ.17). Εξαιτίας της διατοπικότητας των συναλλαγών και των υψηλών ταχυτήτων που χαρακτηρίζουν το διαδίκτυο, τυχόν σφάλματα διατύπωσης ή αποστολής επιζητούν λύσεις, ώστε να διασφαλίζονται τα συμβαλλόμενα μέρη(Καράκωστας, ο.π, σελ.182).

Ειδικότερα και αναφορικά με τον τόπο αποστολής και λήψης μιας δήλωσης βουλήσεως μπορεί να λεχθεί ότι αυτός δεν είναι άλλος από τον τόπο όπου βρίσκεται εγκατεστημένος ο φορέας υποδοχής του μηνύματος. Συνήθως ο Η/Υ ως τέτοιος φορέας αποτελεί το μέσο εκείνο, το οποίο θα ενημερώσει το ενδιαφερόμενο μέρος της επικοινωνίας. Εκεί ακριβώς θα θεωρηθεί ότι ο αποστολέας έστειλε το μήνυμά του (τη δήλωση βουλήσεώς του) ή ο λήπτης έλαβε γνώση της δήλωσης βουλήσεως του άλλου μέρους. Ο τόπος δε αυτός θα μπορούσε να είναι πολύ κοντινός σχεδόν κοινός για τα επικοινωνούντα μέρη, θα μπορούσε όμως να είναι και πολύ μακρινός. Η συνάρτηση και του στοιχείου του χρόνου δίνει μια άλλη διάσταση αντίληψης της ηλεκτρονικής επικοινωνίας Όποιος χρησιμοποιεί το ηλεκτρονικό του γραμματοκιβώτιο στις εμπορικές του συναλλαγές και γνωστοποιεί την ηλεκτρονική του διεύθυνση στις εμπορικές του σχέσεις, θα πρέπει να αναμένει τη λήψη μηνυμάτων από τους συναλλασομένους του, που περιέχουν δηλώσεις. Και τούτο καθ'όλη τη διάρκεια της επαγγελματικής του ενασχόλησης, δηλαδή μέρες και ώρες εργασίας. Όταν ο παραλήπτης της δήλωσης βούλησης είναι ιδιώτης, τα πράγματα είναι περισσότερο ασαφή. Και τούτο γιατί δεν υπάρχει μία διαμορφωμένη πρακτική στα πλαίσια των ηλεκτρονικών συναλλαγών που να αναγνωρίζει συγκεκριμένο χρόνο διαβίβασης δήλωσης βούλησης σε ιδιώτες. Σε αυτό συντελεί το γεγονός ότι οι ιδιώτες δεν είναι υποχρεωμένοι να ελέγχουν το ηλεκτρονικό τους ταχυδρομείο κάθε μέρα (Καράσης, Τα όρια της ελεύθερης κοινωνικής δράσεως στο Διαδίκτυο, ΕπισκΕμπΔ.Β/2005,σελ.281).

Πάντως, σε περιπτώσεις καταναλωτικών συμβάσεων που καταρτίζονται με ηλεκτρονικά μέσα μπορεί να γίνει επίκληση των διατάξεων του Ν. 2251/1994, όπως προβλέπεται στην Οδηγία 2000/31/ΕΚ.Ακόμη, ξεχωριστή προβληματική αποτελεί η αντιμετώπιση σφαλμάτων κατά τη διαδικασία διαμόρφωσης και εξωτερίκευσης της δήλωσης βουλήσεως. Θεωρείται ότι η επίλυση τέτοιων ελαττωμάτων συντελείται με την επίκληση των γενικών αρχών του ΑΚ και των διατάξεων περί πλάνης (Μανιώτης, Η σύναψη της ηλεκτρονικής συμβάσεως και η ευθύνη των παρεχόντων συνδρομή στην κατοχύρωση της γνησιότητας και του αναλλοίωτου των ηλεκτρονικών εγγράφων, Σάκκουλας Αθήνα Κομοτηνή 2003, σελ.59-63).

6 ΤΟ ΕΓΓΡΑΦΟ

6.1 Το ηλεκτρονικό έγγραφο

Το έγγραφο δεν αποτελεί επουσιώδες στοιχείο, τόσο σε περιπτώσεις παραδοσιακής σύμβασης, όσο και ηλεκτρονικής. Όμως, σε συνάρτηση και με τον τηρούμενο τύπο κάθε φορά, οφείλουμε να διατυπώσουμε μια ολοκληρωμένη σκέψη για αυτή την θεματική. Καταρχήν, οι διαδικτυακές πληροφορίες αποτελούν δημοσιευμένα κείμενα, άποψη η οποία έχει διατυπωθεί στη βάση της ανοιχτής πρόσβασης που χαρακτηρίζει το Internet και όχι στο γεγονός της

τυπικής ενσωμάτωσης της πληροφορίας (Πιτσιρίκος Ιωάννης, Σύγχρονα μέσα επικοινωνίας Σάκκουλας , Αθήνα 2002., σελ. 99).

Γενικά, δεν μπορούν να διαχωριστούν οι έννοιες, τόσο της πληροφορίας που φιλοξενείται στο διαδίκτυο, όσο και της πληροφορίας που διατίθεται προς το κοινό, δηλαδή εξωτερικεύεται. Μια σχέση που οδηγεί στην εννοιολογική ταύτισή τους. Στη βάση αυτή, έγγραφα ή ευρύτερα διακινούμενες πληροφορίες θεωρούνται έντυπες εκδόσεις μόνο και μόνο με τη διάχυσή τους προς το κοινό, μέσω της υποδομής του Internet. Στο σημερινό τεχνολογικό επίπεδο με τις ποικίλες ευκολίες που μας παρέχονται, δεν μπορούμε να αποκλείσουμε και μια σειρά προβληματισμών. Έτσι, στην περίπτωση εσφαλμένης αποστολής μέσω διαδικτύου, δεν μπορεί να επιτευχθεί η ανάκληση του εγγράφου, όποια εξειδικευμένη μορφή και αν αυτό φέρει. Ζήτημα το οποίο προκαλεί προβληματισμό ως προς την ακύρωση ενός ήδη δημοσιευμένου ηλεκτρονικού εγγράφου. Ενώ, από μόνο του ένα χάρτινο έγγραφο μπορεί να καταστραφεί ολοκληρωτικά κατά την επιθυμία του κατόχου του, από την άλλη δεν συμβαίνει το ίδιο με το ηλεκτρονικό έγγραφο. Πιο συγκεκριμένα, είναι δυσχερής η διαγραφή ενός ηλεκτρονικού εγγράφου, διότι αυτό εξακολουθεί να υπάρχει και μετά τη φαινομενική του διαγραφή. Επίσης, η αλλοίωση ενός εγγράφου προβαλλόμενου στο διαδίκτυο θεωρείται εύκολη, ενώ η παρακολούθηση και η ανίχνευσή της κρίνονται αρκετά δύσκολες. Αυτή η πραγματικότητα αποτελεί τροχοπέδη για τη ζητούμενη ασφάλεια και εμπιστοσύνη που θα μπορούσε να παρέχεται στο διαδικτυακό περιβάλλον. Ηλεκτρονικά έγγραφα θεωρούνται οι κάθε είδους εγγραφές στην οθόνη του Η/Υ, όπως οι ηλεκτρονικές επιστολές (e-mail), οι ιστοσελίδες, τα αρχεία που διακινούνται μέσω του Διαδικτύου, οι τηλεδιασκέψεις αποτυπωμένες σε δισκέτες ή βιντεοκασέτες, οι τηλεφωνικές επαφές, και οι συζητήσεις σε Internet Relay Chat (IRC) (Καράκωστας, ο.π, σελ. 183) επίσης ως ηλεκτρονικό έγγραφο θα μπορούσε να νοηθεί κάθε υλικός φορέας καταχωρημένων ηλεκτρονικών δεδομένων (Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία μετά τις νέες κοινοτικές ρυθμίσεις, Σάκκουλας Αθήνα 2001, σελ. 4).

Το ηλεκτρονικό έγγραφο αποτελεί αναμφίβολα μια από τις σπουδαιότερες εφαρμογές των νέων τεχνολογιών. Η πρακτική σημασία από νομικής απόψεως είναι ότι περικλείει ότι και το αντίστοιχο κλασικό έγγραφο, το οποίο και αντικαθιστά, στις ηλεκτρονικές συμβάσεις και ευρύτερα συναλλαγές (Πανάγου, Το ηλεκτρονικό διοικητικό έγγραφο δημιουργία και διαχείριση, ΝοΒ 54, σελ.163-164). Το κριτικό σημείο σε όλη τη διαλεκτική περί ηλεκτρονικών εγγράφων είναι η αξιολόγησή του σε σχέση με το χάρτινο έγγραφο. Το ερώτημα δε που ανακύπτει, είναι κατά πόσο το ηλεκτρονικό έγγραφο δύναται να αντικαταστήσει το παραδοσιακό και σε ποιο βαθμό (Καράκωστας, ο.π, σελ.13).

6.2 Είδη εγγράφων

Ιδιαίτερος λόγος γίνεται για τα είδη των ηλεκτρονικών εγγράφων, καθ΄ ότι εντοπίζονται τεχνικές - τεχνολογικές διαφορές, οι οποίες βέβαια προσδίδουν και διαφοροποίηση ως προς τη νομική αξία του κάθε εγγράφου. Τα ηλεκτρονικά έγγραφα μπορούν να χαρακτηρισθούν ως ρυθμιζόμενα ηλεκτρονικά έγγραφα και μη ρυθμιζόμενα ηλεκτρονικά έγγραφα. Η διάκριση αυτή είναι αποκλειστική σύμφωνα με την κείμενη νομοθεσία περί ηλεκτρονικών υπογραφών, όπως θα δειχθεί παρακάτω (Χριστοδούλου, ο.π , σελ.77 και 173).

Πιο συγκεκριμένα, ρυθμιζόμενα ηλεκτρονικά έγγραφα είναι αυτά ακριβώς τα οποία προβλέπονται ρητά (ρυθμίζονται) από τον κοινοτικό και τον εθνικό νομοθέτη Οδ. 99/93/ΕΚ άρθρο 5 παρ1 και Π.Δ. 150/2001 άρθρο 3 παρ. 1 αντίστοιχα. Αυτά τα έγγραφα κατά τις διατάξεις της Οδηγίας και του Π.Δ. φέρουν προηγμένη ηλεκτρονική υπογραφή, η οποία ισοδυναμεί με την ιδιόχειρη του ουσιαστικού και δικονομικού δικαίου.

Αναφορικά με τα μη ρυθμιζόμενα ηλεκτρονικά έγγραφα, όσα δηλαδή δεν φέρουν την προηγμένη ηλεκτρονική υπογραφή ή δεν φέρουν καθόλου υπογραφή, γι'αυτά δεν προβλέπεται νομοθετική ρύθμιση και θα πρέπει να κρίνονται (η ύπαρξη, η ισχύς και η αποδεικτική τους δύναμη) κατά περίπτωση. Επομένως, το νομοθετικό κενό περί μη ρυθμιζόμενων ηλεκτρονικών εγγράφων θα πρέπει να καλύπτεται μέσω της αντιστοίχησής τους με κάποιο τύπο παραδοσιακού εγγράφου.

Τα ηλεκτρονικά έγγραφα χωρίζονται επίσης σε γνήσια και μη γνήσια. Γνήσια θεωρούνται τα έγγραφα που έχουν αποκλειστικά ηλεκτρονική υπόσταση, δηλαδή καταχωρίσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό όπως ο σκληρός δίσκος, η δισκέτα, ένα συμπιεσμένο αρχείο zip ή ένας ψηφιακός δίσκος (cd). Αντίθετα, τα μη γνήσια ηλεκτρονικά έγγραφα είναι έγγραφα με υλική μορφή, των οποίων το περιεχόμενο αλλά και η υπογραφή είναι ηλεκτρονικά αποτυπωμένα όπως, η τηλεομοιοτυπία (fax) . Η τηλεομοιοτυπία, δηλαδή η, ορίζεται ως «η πιστή αναπαραγωγή από απόσταση κειμένων, σχεδίων και κάθε μορφής εντύπων με τη βοήθεια τερματικών διατάξεων», ενώ ως τηλεομοιότυπο ορίζεται «το λαμβανόμενο στο σταθμό λήψεως αντίτυπο».(Άρθρο 2 § 2 εδ. α' του Κανονισμού Συνδρομητικής Τηλεομοιοτυπίας (απόφαση ΔΣ του ΟΤΕ της 13-12-1988/31-1-1989, ΦΕΚΒ' 167/8-3-1989)., Άρθρο 2 § 2 εδ. β' του Κανονισμού Συνδρομητικής Τηλεομοιοτυπίας (απόφαση ΔΣ του ΟΤΕ της 13-12-1988/31-1-1989, ΦΕΚΒ' 167/8-3-1989).

6.3 Μορφή εγγράφων

Προσδιοριστικό στοιχείο του ηλεκτρονικού εγγράφου αναδεικνύεται η συμβολή της ηλεκτρονικής τεχνολογίας στη δημιουργία του. Ειδικότερα, η σύνταξη αυτών των εγγράφων γίνεται αποκλειστικά με ηλεκτρονικά μέσα (Σιδηρόπουλος, Το δίκαιο του διαδικτύου, Σάκκουλας Αθήνα-Θεσσαλονίκη 2003, σελ.5-76). Ουσιαστικά το ηλεκτρονικά παραχθέν έγγραφο είναι ένα σύνολο δεδομένων ηλεκτρονικά επεξεργασμένων και αποθηκευμένων σε υπόθεμα μνήμης, είτε σταθερής (π.χ. σκληρός δίσκος η/υ), είτε ενός φορητού ενσώματου στοιχείου (π.χ. δισκέτα, cd). Επισημαίνεται ότι η ενδιάμεση διαδικασία επεξεργασίας των δεδομένων τα συμπυκνώνει και τα καθιστά μη αναγνώσιμα, έως ότου επεξεργαστούν και πάλι και επανέλθουν στην αρχική τους μορφή.

Μπορούμε να δεχθούμε ότι τα μηνύματα του ηλεκτρονικού ταχυδρομείου αποτελούν τα πιο διαδεδομένα ηλεκτρονικά έγγραφα. Όμως το κύριο μειονέκτημά του η ανασφάλεια (υποκλοπές, χρήση ψευδωνύμων κ.α.) περιορίζει την αξιοπιστία την οποία προσδοκούν οι χρήστες, αλλά και απαιτείται για μια συναλλαγή. Από την άλλη μια σειρά ηλεκτρονικών αρχείων, βάσεων δεδομένων, ηλεκτρονικών διευθύνσεων, διευθύνσεων ηλεκτρονικής αλληλογραφίας, δεν θα μπορούσαν να μην αποτελούν ηλεκτρονικά έγγραφα (Δελούκα-Ιγγλέση, ο.π, σελ.43). Δεδομένου ότι όλα αυτά είναι κείμενα -στοιχεία, τα οποία έχουν υποστεί ηλεκτρονική επεξεργασία και κυκλοφορούν στο διαδίκτυο (Καράκωστας, ο.π, σελ.192).

Χαρακτηριστικό είναι ότι δεν προβλέπεται μια ειδική κατάταξη των ηλεκτρονικών εγγράφων ως προς τη νομική αξία και τις έννομες συνέπειες που μπορούν να έχουν αυτά. Μόνο μια περίπτωση θεωρείται ως ασφαλής διάκριση και η οποία προβλέπεται ρητά από το νόμο. Ο λόγος για τα ρυθμιζόμενα ηλεκτρονικά έγγραφα. Αυτά εξομοιώνονται πλήρως με τα ιδιωτικά έγγραφα. Αποτελούν πλήρη απόδειξη και συστατικό τύπο δικαιοπραξίας. Αναφορικά με την απόδειξη, από το Π.Δ. 150/2001 άρθρο 3, συνάγεται ότι τα έγγραφα αυτού του τύπου, όσα δηλαδή φέρουν προηγμένη ηλεκτρονική υπογραφή, καθίστανται αναγνωρισμένα αποδεικτικά στοιχεία. Επί του συστατικού τύπου και εδώ επιβεβαιώνεται αντιστοίχιση με τις έννομες συνέπειες των ιδιωτικών εγγράφων (επομένως ταυτίζονται και με αυτά) σύμφωνα με το άρθρο 160 ΑΚ και το Π.Δ. 150/2001 άρθρο 3(Καράκωστας,ο.π, σελ.195).

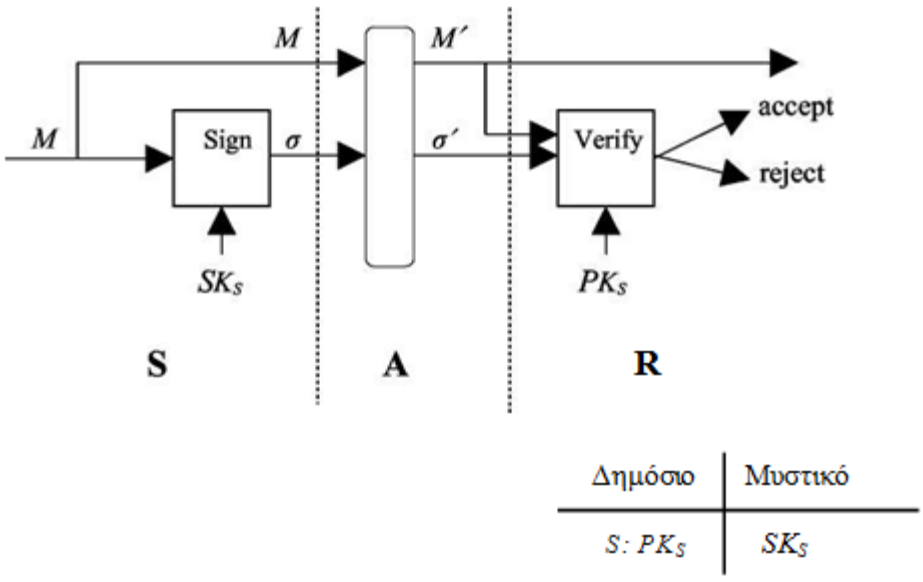
Στις περιπτώσεις των ηλεκτρονικών εγγράφων τα οποία δεν φέρουν προηγμένη ηλεκτρονική υπογραφή ο κοινοτικός νομοθέτης δεν περιέλαβε περιορισμούς στην Οδηγία 99/93/ΕΚ και καλείται ο εθνικός εφαρμοστής του δικαίου να τα αξιολογήσει σύμφωνα με το εσωτερικό δίκαιο (Χριστοδούλου, ο.π, σελ.75 και σελ.173-174).

7 Ο ΘΕΣΜΟΣ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

7.1 Η ηλεκτρονική υπογραφή

Η ηλεκτρονική υπογραφή έχει γίνει αντιληπτή στη θεωρία μας ως μία μέθοδος τεκμηρίωσης με ηλεκτρονικά μέσα που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις εγγραφές δεδομένων σε μαγνητικά μέσα ηλεκτρονικού υπολογιστή, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής δεδομένων και της ηλεκτρονικής αλληλογραφίας(Στ. Κουσούλης, Σύγχρονες Μορφές Έγγραφης Συναλλαγής, Σάκκουλας, Αθήνα-Κομοτηνή 1992, σελ. 138, Δημ. Μανιώτης, Η ψηφιακή υπογραφή ως μέθοδος διαπιστώσεως της γνησιότητας των εγγράφων στο Αστικό Δικονομικό Δίκαιο, Σάκκουλας Αθήνα-Κομοτηνή 1998, σελ. 32-34) με σκοπό να διασφαλίσει αφενός τη γνησιότητα και ακρίβεια της δήλωσης βουλήσεως που περιέχουν και αφετέρου τα στοιχεία του προσώπου που προβαίνει στη δήλωση αυτή (Δημ. Μανιώτης, ό.π. σελ. 32-34, Χρ. Χρυσάνθης, Η ηλεκτρονική εξυπηρέτηση των σύγχρονων τραπεζικών συναλλαγών, Αθήνα-Κομοτηνή 1997, σελ. 383). Η ηλεκτρονική υπογραφή δεν αποτελεί ηλεκτρονική απεικόνιση της ιδιόχειρης υπογραφής, αλλά ουσιαστικά είναι μια ηλεκτρονική σύντμηση που προκύπτει από το ηλεκτρονικό έγγραφο το οποίο συνοδεύει και από απόρρητα δηλωτικά σημεία (π.χ. passwords) του υπογράφοντα (Παπαθωμά-Μπέτγκε, Α., Ηλεκτρονικό εμπόριο: Νομικά ζητήματα κατά τη σύναψη εμπορικών συμβάσεων στο Internet, ΔΕΕ 1999, σελ. 1237-1242).

Ειδικά, ο θεσμός της υπογραφής διατηρείται, ενώ παράλληλα εμπλουτίζεται και με νέα στοιχεία συμβατά με τις απαιτήσεις της σύγχρονης εποχής και των νέων τεχνολογιών, την ηλεκτρονική υπογραφή. Ηλεκτρονική υπογραφή είναι το σύνολο των ηλεκτρονικών δεδομένων, τα οποία συνοδεύουν ένα ηλεκτρονικό έγγραφο και επιτελούν ότι ακριβώς και η παραδοσιακή υπογραφή επί χάρτινων εγγράφων (Γεωργιάδης Γ.,ο.π, σελ.166, Σιδηρόπουλος, ο.π, σελ.85 και Ιγγλεζάκης, ο.π , σελ.41). Ουσιαστικά η ηλεκτρονική υπογραφή είναι μονοσήμαντη και εξατομικεύει απόλυτα τον υπογράφοντα. Επίσης, η θέση της σε ένα έγγραφο υποδηλώνει τη γνησιότητα του εγγράφου.



Εικόνα 1 Σχήμα ψηφιακής υπογραφής. Η υπογραφή σ συνοδεύει το μήνυμα Μ.

Ο παραλήπτης R την χρησιμοποιεί για να αποφασίσει αν το μήνυμα προέρχεται πράγματι από τον αποστολέα S ο οποίος έχει το δημόσιο κλειδί Pks .

7.2 Τα είδη της ηλεκτρονικής υπογραφής

Με τον όρο «ηλεκτρονική υπογραφή» νοούνται «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας»(Άρθρο 2 Π.Δ 150/2001). Η σπουδαιότητα της ηλεκτρονικής υπογραφής έγκειται, πέραν της ειδικής της λειτουργίας, στην ενθάρρυνση του ηλεκτρονικού εμπορίου, αλλά και στο γεγονός ότι διαβαθμίζει το ηλεκτρονικό έγγραφο, στο οποίο έχει τεθεί (Ιγγλεζάκης,ο.π, σελ. 624). Σύμφωνα με την κείμενη κοινοτική και εθνική νομοθεσία οι ηλεκτρονικές υπογραφές αξιολογούνται ανάλογα με τα τεχνικά στοιχεία βάσει των οποίων εκδίδονται. Έτσι, όσο πιο προηγμένη είναι η τεχνολογία στην οποία στηρίζεται, τόσο πιο ασφαλής δύναται να χαρακτηρισθεί αυτή η ηλεκτρονική υπογραφή (Σιδηρόπουλος,ο.π, σελ. 85). Τα είδη των ηλεκτρονικών υπογραφών αναφέρονται στα νομοθετήματα Οδηγία 1999/93/ΕΚ , Π.Δ. 150/2001. Ουσιαστικά, όπως αναφέρεται στο Π.Δ. 150/2001 γίνεται λόγος για δύο ηλεκτρονικές υπογραφές: την «ηλεκτρονική υπογραφή» και την «προηγμένη ηλεκτρονική υπογραφή». Συγκεκριμένα, η προηγμένη ηλεκτρονική υπογραφή ανταποκρίνεται στις εξής απαιτήσεις: i) συνδέεται μονοσήμαντα με τον υπογράφοντα, ii) είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος, iii) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και iv) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων. Οι μεταξύ τους διαφοροποιήσεις περιγράφονται με σαφήνεια στο Π.Δ. 150/2001, ενώ καθίσταται από το διάταγμα προδήλως ενισχυμένη η αξία της προηγμένης υπογραφής σε σχέση με την «απλή» ηλεκτρονική υπογραφή.

7.3 Κρυπτογραφικοί Αλγόριθμοι

Οι μαθηματικές ιδιότητες των πρώτων αριθμών, δηλαδή αυτών που, μόνο όταν διαιρούνται με τον εαυτό τους και με τον αριθμό ένα, δίνουν πηλίκο έναν ακέραιο αριθμό καθώς και η μαθηματική δυσκολία της εύρεσης των δύο αρχικών πρώτων αριθμών, όταν μόνο το γινόμενο αυτών των αριθμών είναι γνωστό, είναι η μαθηματική βάση της σύγχρονης ασύμμετρης κρυπτογραφίας.

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων. Μαζί με τον κλάδο της Κρυπτανάλυσης, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της Κρυπτολογίας. Έτσι, Κρυπτολογία είναι η επιστήμη της απόκρυψης από τη μία πλευρά και, από την άλλη, της αποκάλυψης του περιεχομένου κωδικοποιημένων μηνυμάτων ή δεδομένων. Θα εστιάσουμε, κυρίως, στην Κρυπτογραφία. Ωστόσο, θα προσπαθήσουμε να καλύψουμε και ορισμένα θέματα, που αποτελούν αντικείμενο της Κρυπτανάλυσης (Ζορκάδης, Β, Κρυπτογραφία, ΕΑΠ,2002, σελ.3).

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων, τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιο τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου των κατά τη μετάδοσή ή αποθήκευσή των και, βεβαίως ,την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται κρυπτογράφηση και η αντίστροφός της αποκρυπτογράφηση.

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται κρυπτογραφικός αλγόριθμος. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται κρυπτογραφικό σύστημα. Μερικές φορές ο κρυπτογραφικός αλγόριθμος καλείται και κωδικοποιητής (cipher). Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται κρυπτογραφικά πρωτόκολλα Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, (κρυπτογραφικά) κλειδιά (keys), η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση. Το σύνολο των δυνατών τιμών των κλειδιών λέγεται πεδίο τιμών αυτών (keyspace). Υπάρχουν δύο κατηγορίες

κρυπτογραφικών αλγορίθμων και, κατά συνέπεια, συστημάτων: οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι.

Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση και για το λόγο αυτό καλούνται, επίσης, αλγόριθμοι μυστικού κλειδιού ή αλγόριθμοι μονού κλειδιού. Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν ένα ζεύγος κρυπτογραφικών κλειδιών, το δημόσιο κλειδί για την κρυπτογράφηση και το ιδιωτικό κλειδί για την αποκρυπτογράφηση. Έτσι, ο κάθε χρήστης ενός ασύμμετρου συστήματος έχει δύο κλειδιά, το δημόσιο και το ιδιωτικό. Το πρώτο το κοινοποιεί σε όλους που επιθυμούν να επικοινωνήσουν μαζί του. Όμως, δεν είναι δυνατό από το δημόσιο να υπολογίσουμε το ιδιωτικό κλειδί ενός χρήστη. Οι ασύμμετροι αλγόριθμοι ονομάζονται και αλγόριθμου δημόσιου κλειδιού.Οι συμμετρικοί αλγόριθμοι χωρίζονται, με τη σειρά τους, σε δύο κατηγορίες: στους κωδικοποιητές ροής (stream ciphers) και κωδικοποιητές τμημάτων (block ciphers). Οι πρώτοι εφαρμόζονται σε κάθε bit ή χαρακτήρα ενός μηνύματος, ενώ οι δεύτεροι σε τμήματα (blocks) του μηνύματος σταθερού μήκους. Συνήθως, το μήκος αυτό ανέρχεται σε 64 bits(D. W. Davies and W. L. Price, Security for Computer Networks, John Wiley & Sons, 1989).

Ο ακόλουθος αλγόριθμος κρυπτογράφησης αντικαθιστά κάθε γράμμα του απλού αγγλικού κειμένου με εκείνο το γράμμα που είναι 13 θέσεις μετά από αυτό στο αλφάβητο, δηλαδή το A αντικαθίσταται από το N, το B από το O, κτλ.

Απλός αλγόριθμος κρυπτογράφησης

while δεν έχει εξαντληθεί το κείμενο loop

επανέλαβε την ανάγνωση, από την οθόνη ή από αρχείο, του

επόμενου γράμματος του κειμένου

if το γράμμα είναι ένα από τα πεζά ‘a,..m’ ή τα κεφαλαία ‘A,..,M’

then εμφάνισε στην οθόνη το αντίστοιχο πεζό ή κεφαλαίο γράμμα που

είναι 13 θέσεις δεξιά του στο αλφάβητο

end if

if το γράμμα είναι κάποιο από τα ‘n,..,z’ ή τα ‘N,..,Z’

then εμφάνισε στην οθόνη το αντίστοιχο πεζό ή κεφαλαίο που βρίσκεται 13

θέσεις πριν από αυτό στο αλφάβητο

end if

end loop

Ο παραπάνω αλγόριθμος κωδικοποιημένος σε γλώσσα προγραμματισμού C:

```
#include <stdio.h>
main()
{
int c;
while ((c = getchar()) != EOF)
{
if (c >= 'a' && c <= 'm')
c = c + 13;
else if (c >= 'n' && c <= 'z')
c = c - 13;
else if (c >= 'A' && c <= 'M')
c = c + 13;
else if (c >= 'N' && c <= 'Z')
c = c - 13;
putchar(c);
```

```
}
}
```

⊕ = πράξη αποκλειστικής διάζευξης XOR

Αποστολέας (κλειδί ⊕ μήνυμα =κώδικας)

Κλειδί: 1 1 0 1 0 0 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 0 1

Μήνυμα: 0 0 1 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0

Κώδικας: 1 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 1 1 1 0 0 1 1

Παραλήπτης (κλειδί ⊕ κώδικας = μήνυμα)

Κλειδί: 1 1 0 1 0 0 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0 1 1 1 0 1

Κώδικας: 1 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 1 1 1 0 0 1 1

Μήνυμα: 0 0 1 1 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0 1 0 0 1 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0

Για να ελέγξουμε αν δύο αριθμοί είναι σχετικά πρώτοι αρκεί να βρούμε ότι ο μέγιστος κοινός διαιρέτης τους είναι ίσος με τη μονάδα. Μία μέθοδος υπολογισμού του μέγιστου κοινού διαιρέτη είναι ο αλγόριθμος του Ευκλείδη, που περιγράφεται στο βιβλίο του ‘Στοιχεία’, το οποίο έγραψε το 300 π.Χ. περίπου. Ο αλγόριθμος του Ευκλείδη, καθώς και η κωδικοποίησή του στη γλώσσα προγραμματισμού C παρατίθενται στη συνέχεια. Έστω οι δύο ακέραιοι, μη μηδενικοί, αριθμοί a και b. Μπορούμε ακόμα να υποθέσουμε ότι οι δύο αυτοί αριθμοί είναι θετικοί, αφού ο μέγιστος κοινός διαιρέτης τους (a,b) είναι ίσος με τον μέγιστο κοινό διαιρέτη των απολύτων τιμών τους (|a| ,|b|). Ο αλγόριθμος του
Ευκλείδη αποτελείται από τα ακόλουθα βήματα:

1. Υπολογίζουμε a = p b+ r, όπου 0≤r≤b≤a και 0≤p

2. Αν r=0 τότε (a, b) =b. Τερματισμός.

3. Διαφορετικά, θέτουμε a = b και b= r. Επαναλαμβάνουμε τα βήματα 1 και 2 έως ότου ληφθεί r=0 και τερματιστεί η αναζήτηση με αποτέλεσμα την τελευταία τιμή του b (ή την προτελευταία τιμή του r).

Μια δυνατή κωδικοποίηση στη γλώσσα προγραμματισμού C είναι η ακόλουθη:

```
int gcd (int a, int b)
{
int g;
if (a < 0)
a = -a;
```

```
if (b < 0)
b = -b;
g = b;
While  (a > 0)
{
g = a;
a = b % a;
b = g;
}
return g;
}
```

Στη C, ο τελεστής *a%b* επιστρέφει το υπόλοιπο της διαίρεσης του *a* από το *b*.

7.3.1 Ασφάλεια Κρυπτογραφικών Συστημάτων

Στην Κρυπτογραφία παρατηρήθηκε συχνά η τάση αναζήτησης προβλημάτων, τα οποία είναι δύσκολα στην επίλυσή τους και έχουν πάρα πολλές δυνατές λύσεις, ως βάσεις κρυπτογραφικών συστημάτων. Τα δύσκολα επιλύσιμα προβλήματα (NP), λοιπόν, είναι θεμελιώδη στην Κρυπτογραφία. Ωστόσο, η επιλογή ενός NP προβλήματος ως βάσης δεν είναι αρκετή για τη σχεδίαση ασφαλών κρυπτογραφικών συστημάτων. Στη συνέχεια θα συζητήσουμε ορισμένες σχετικές πτυχές. Τα προβλήματα που ανήκουν στην NP κλάση, έχουν όπως είπαμε μη-ντετερμινιστική πολυωνυμική χρονική πολυπλοκότητα και ασφαλώς ντετερμινιστική εκθετική χρονική πολυπλοκότητα, δηλαδή ανάλογη του 2^n. Ας παρατηρήσουμε ως παράδειγμα το πρόβλημα της κρυπτανάλυσης κρυπτογραφημένου μηνύματος με κλειδί πολύ μικρού μήκους, n. Τότε το 2^n δεν είναι μεγάλο και συνεπώς η κρυπτανάλυση είναι εφικτή δοκιμάζοντας όλα τα δυνατά κλειδιά (brute force attack). Επομένως, δεν είναι αρκετό να στηριζόμαστε σε ένα πρόβλημα με εκθετική πολυπλοκότητα αν το μέγεθος της εισόδου είναι μικρό. Αντίθετα, μόνο αν το n είναι επαρκώς μεγάλο, τότε και το 2^n είναι τόσο μεγάλο που καθιστά μη εφικτή τη δοκιμή όλων των δυνατών κλειδιών.

Στον Πίνακα 1 βλέπουμε τα μεγέθη των εισόδων που μπορούν να εκτελεσθούν στη μονάδα του χρόνουμε δεδομένη τη διαθέσιμη υπολογιστική ισχύ και την πολυπλοκότητα του αλγορίθμου.Το να στηριχθούμε για την υλοποίηση ενός κρυπτογραφικού συστήματος σε ένα NP Complete πρόβλημα δεν συνεπάγεται, αυτόματα, την ύπαρξη μόνο λύσης με εκθετική πολυπλοκότητα. Δεν αποκλείεται, δηλαδή, η ύπαρξη μιας πιο εύκολης λύσης, αν και κάτι τέτοιο εκτιμάται ως άκρως απίθανο (ωστόσο, όχι αδύνατο). Στο σημείο αυτό αναφερόμαστε στην περίπτωση να δειχθεί ότι οι κλάσεις P και NP ταυτίζονται. Ακόμα,το ότι ένα κρυπτογραφικό σύστημα βασίζεται σε ένα δύσκολο πρόβλημα δεν σημαίνει ότι και ο κρυπταναλυτής θα πρέπει να λύσει το δύσκολο πρόβλημα για την παραβίασή του.

Ένα σχετικό παράδειγμα είναι αυτό των κρυπτογραφικών συστημάτων τα οποία βασίζονται στο πρόβλημα του σακιδίου (Merkle R., Hellman M., Hiding Information and Signatures in Trapdoor Knapsacks , IEEE Transactions Information Theory, v. 24, n. 5, 1978, 525-530) και τα οποία παραβιάσθηκαν με αξιοποίηση κάποιας μυστικής εύκολης λύσης (trap-door). Η υπολογιστική ισχύς και η αποθηκευτική ικανότητα των συστημάτων αυξάνεται ραγδαία με την ανάπτυξη νέων υπολογιστικών συστημάτων. Η αύξηση της υπολογιστικής ισχύος καθιστά προβλήματα κρυπτανάλυσης αντιμετωπίσιμα. Η χρήση πολυεπεξεργαστών ή

και πολυυπολογιστών στην κρυπτανάλυση αποτελούν μία πραγματικότητα που πρέπει να λαμβάνεται υπόψη από τους σχεδιαστές κρυπτογραφικών συστημάτων. Η περίπτωση της παραβίασης κρυπτογραφημένου μηνύματος με τον DES (με κλειδί μήκους 40 bits), από τη συνεργασία χιλιάδων υπολογιστών συνδεδεμένων στο Internet, γνώρισε ευρεία δημοσιότητα το 1997. Στο μεταξύ είναι δυνατή η κρυπτανάλυση και όταν χρησιμοποιούνται κλειδιά μεγαλύτερου μήκους. Επομένως, η επιλογή των μεγεθών εισόδου θα πρέπει να λαμβάνει υπόψη τόσο τις τωρινές τεχνολογικές δυνατότητες όσο και τις αναμενόμενες μελλοντικές εξελίξεις Ιδιαίτερα, η ανάπτυξη των κβαντικών υπολογιστικών και επικοινωνιακών συστημάτων αναμένεται να ακυρώσει την πρακτική αξία πολλών κρυπτογραφικών συστημάτων που χαρακτηρίζονται ως υπολογιστικά ασφαλή.

Τα διάφορα κρυπτογραφικά συστήματα έχουν διαφορετικά επίπεδα ασφάλειας, ανάλογα με το πόσο δύσκολα παραβιάζονται. Όλοι οι αλγόριθμοι - πλην του one-time pad είναι θεωρητικά παραβιάσιμοι, δεδομένης επαρκούς υπολογιστικής ισχύος και αποθηκευτικής χωρητικότητας. Αν ο χρόνος και οι χρηματικοί πόροι που απαιτούνται για την παραβίαση ενός αλγορίθμου υπερβαίνουν την αξία των κρυπτογραφημένων δεδομένων, τότε ο αλγόριθμος μπορεί να χαρακτηρισθεί ασφαλής. Δηλαδή στα καθοριστικά κριτήρια για το αν ένας κρυπτογραφικός αλγόριθμος είναι ασφαλής ή όχι συγκαταλέγεται και η αξία των αγαθών που προστατεύει. Οι υπολογιστές, όμως, γίνονται ολοένα και πιο γρήγοροι, αλλά και πιο φτηνοί. Την ίδια στιγμή, η αξία των δεδομένων πέφτει με το πέρασμα του χρόνου. Συνεπώς, μας ενδιαφέρει η βελτίωση της υπολογιστικής και αποθηκευτικής δυνατότητας των υπολογιστών να μην είναι τόσο δυσανάλογα ταχύτερη από την πτώση της αξίας των πληροφοριών, γεγονός που θα καθιστούσε το κρυπτογραφικό σύστημα ανασφαλές (Shannon, C. E., Communication Theory of Secrecy Systems, Bell System Technical Journal, v. 28, n. 4, 1999, pp. 656-715).

Μερικοί αλγόριθμοι απαιτούν εκατομμύρια χρόνια για να παραβιαστούν, και απεριόριστους υπολογιστικούς πόρους. Αυτοί οι αλγόριθμοι είναι θεωρητικά παραβιάσιμοι, αλλά όχι πρακτικά. Ένας αλγόριθμος που δεν παραβιάζεται στην πράξη θεωρείται ασφαλής (secure). Ένας αλγόριθμος είναι ασφαλής άνευ όρων (unconditionally secure), αν, άσχετα από το μέγεθος του κρυπτογραφημένου μηνύματος, τους υπολογιστικούς πόρους και τον χρόνο που μπορεί να διαθέτει ο κρυπταναλυτής, δεν υπάρχει δυνατότητα να αποκαλυφθεί το καθαρό μήνυμα. Τα one-time pads, όπως είδαμε, δεν μπορούν να παραβιασθούν, ακόμα και δεδομένων άπειρων πόρων. Η κρυπτογραφία ασχολείται περισσότερο με κρυπτογραφικά συστήματα, τα οποία δεν μπορούν να παραβιαστούν με τις δεδομένες υπολογιστικές δυνατότητες. Ένας αλγόριθμος λέγεται υπολογιστικά ασφαλής (computationally secure), ή δυνατός (strong), αν είναι αδύνατη η παραβίασή του με τους διαθέσιμους (τωρινούς ή μελλοντικούς) πόρους. Το πλήθος των πράξεων, που απαιτούνται για την αποκάλυψη του κρυπτογραφικού κλειδιού, λέγεται παράγοντας εργασίας (work factor). Αν ένας αλγόριθμος έχει παράγοντα εργασίας 2^{128}, τότε απαιτούνται 2^{128} πράξεις για την παραβίασή του. Αυτές οι πράξεις μπορεί να είναι αρκετά πολύπλοκες και χρονοβόρες. Ακόμα και αν θεωρήσει κανείς ότι διαθέτει αρκετά μεγάλη ταχύτητα υπολογισμών, ώστε να εκτελεί ένα δισεκατομμύριο πράξεις το δευτερόλεπτο, και διαθέσει ένα δισεκατομμύριο παράλληλους επεξεργαστές, και πάλι ο χρόνος που θα χρειαστεί για να αποκαλυφθεί το κλειδί θα είναι μεγαλύτερος από 10^{14} χρόνια. (Για λόγους σύγκρισης και μόνον, αξίζει να αναφέρουμε ότι η ηλικία της γης είναι 10^9 και του σύμπαντος περίπου 10^{10} χρόνια).

Κι ενώ ο παράγοντας εργασίας ενός συγκεκριμένου αλγορίθμου είναι σταθερός (μέχρι κάποιος κρυπταναλυτής να βρει μία καλύτερη κρυπταναλυτική επίθεση), ο απαιτούμενος χρόνος για την παραβίαση του αλγορίθμου κάθε άλλο παρά σταθερός είναι, αφού παρατηρείται σημαντική αύξηση της υπολογιστικής ισχύος των νέων επεξεργαστών. Τις τελευταίες δεκαετίες που διανύουμε, έχουμε δει ραγδαίες εξελίξεις της υπολογιστικής ισχύος και μάλλον στα χρόνια που θα έρθουν τα αποτελέσματα θα είναι ακόμα πιο εντυπωσιακά, ιδιαίτερα με τους κβαντικούς υπολογιστές. Σχεδόν όλες οι επιθέσεις κρυπτανάλυσης είναι τέλειες για παράλληλες μηχανές, αφού συνίστανται στη δοκιμή όλων των δυνατών κρυπτογραφικών κλειδιών. Το συνολικό έργο μπορεί να διασπαστεί σε πάρα πολλά μικρά μέρη, ενώ κανένας από τους επεξεργαστές δεν χρειάζεται να επικοινωνεί με τον άλλο. Συμπερασματικά, το να υποστηρίζει κανείς ότι ένας αλγόριθμος είναι ασφαλής, απλώς και μόνο επειδή δε μπορεί να παραβιαστεί - με βάση τα σημερινά τεχνολογικά δεδομένα– είναι

παρακινδυνευμένο. Τα καλά κρυπτογραφικά συστήματα σχεδιάζονται κατά τέτοιον τρόπο, ώστε να είναι αδύνατη η παραβίασή τους, ακόμα και με την υπολογιστική ισχύ που αναμένεται να προκύψει μετά από πολλά χρόνια. Ο κρυπτογραφικός αλγόριθμος DES χρησιμοποιήθηκε με ασφάλεια για περισσότερα από 20 χρόνια. Επίσης, ο νέος πρότυπος κρυπτογραφικός αλγόριθμος, ο AES (Advanced Encryption Standard), εκτιμάται ότι θα είναι ασφαλής για μεγαλύτερο χρονικό διάστημα (Zorkadis, Security vs. Performance Requirements in Data Communication Systems, Proc. of Third European Symposium on Research in Computer Security, Lecture Notes in Computer Science 875, 1994, Springer-Verlag, pp. 19-30).

Πολυπλοκότητα	Μέγεθος εισόδου που εκτελείται στο 1 sec Υπολογιστική ισχύς 10^6 πράξεων/ sec
$\log_n$	$2^{1000000}$
n	1000000
n^2	1000
n^3	100
2^n	20
n!	9

Πίνακας 1 Μεγέθη εισόδου που εκτελούνται στη μονάδα του χρόνου (sec) από υπολογιστή ισχύος ενός εκατομμυρίου πράξεων ανά μονάδα χρόνου.

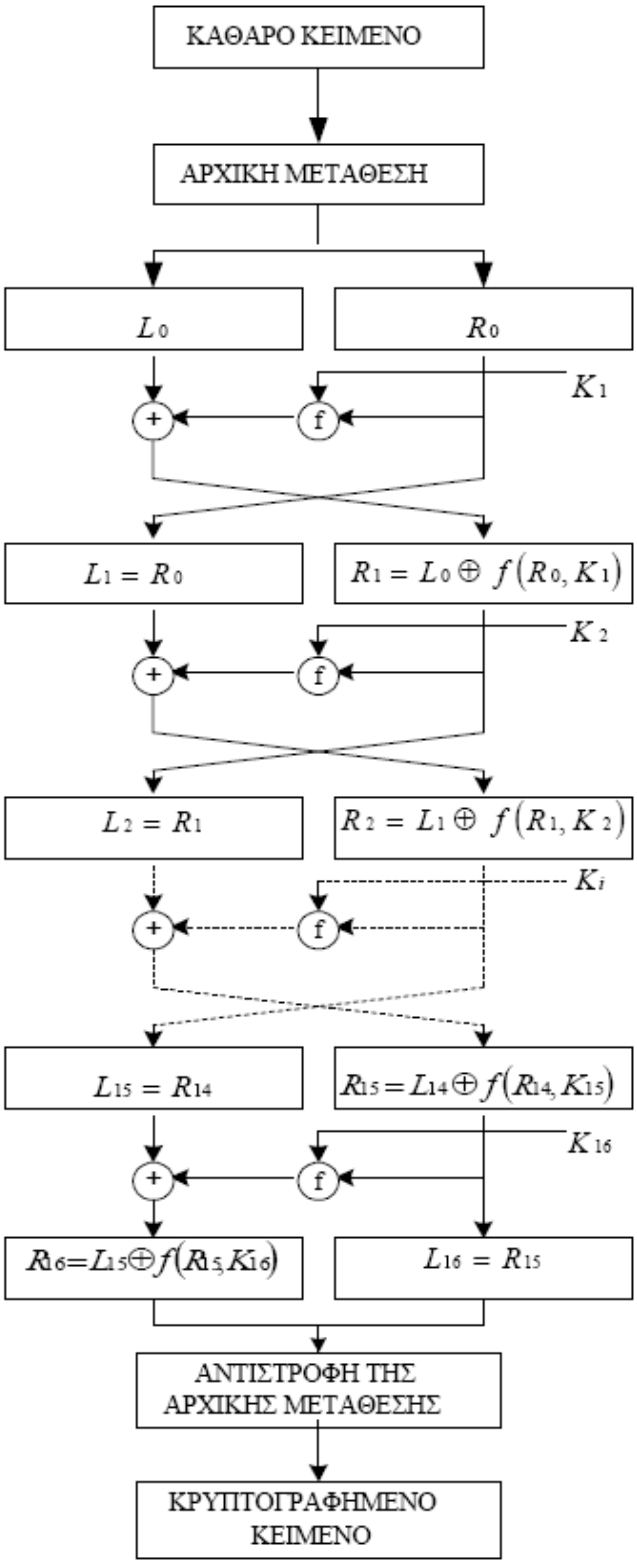
7.3.2 Συμμετρικοί Αλγόριθμοι (Περιγραφή του DES)

Το πιο δημοφιλές και διαδεδομένο σύστημα κρυπτογράφησης αποτέλεσε (και σήμερα ακόμα αποτελεί) το Data Encryption Standard (DES), το οποίο υιοθετήθηκε το 1977 από το National Bureau of Standards (NBS) των Η.Π.Α. - αργότερα γνωστό ως National Institute of Standards and Technology (NIST) - ως πρότυπο επεξεργασίας πληροφοριών των ομοσπονδιακών αρχών (Federal Information Processing Standard 46 - FIPS PUB 46) και για γενική χρήση (V. Zorkadis, Security vs. Performance Requirements in Data Communication Systems, Proc. of Third European Symposium on Research in Computer Security, Lecture Notes in Computer Science 875, 1994, Springer-Verlag, pp. 19-30). Ας δούμε μερικά ιστορικά στοιχεία για αυτόν τον αλγόριθμο. Το 1972 για πρώτη φορά και το 1974 για δεύτερη φορά το NBS εξέδωσε μία πρόσκληση υποβολής προτάσεων αναφορικά με έναν κρυπτογραφικό αλγόριθμο για δημόσια χρήση. Στα επιθυμητά χαρακτηριστικά του αλγόριθμου συγκαταλέγονταν, σύμφωνα με την πρόσκληση, υψηλός βαθμός ασφάλειας, ασφάλεια ανεξάρτητη της μυστικότητας του αλγορίθμου, καταλληλότητα για πολλές εφαρμογές, χαμηλό κόστος υλοποίησης, πληρότητα και ευκολία κατανόησης των προδιαγραφών του αλγόριθμου, διαθεσιμότητα σε όλους τους χρήστες και αποτελεσματικότητα στη χρήση. Η πρώτη πρόσκληση απέβη άκαρπη. Για το λόγο αυτό ακολούθησε η δεύτερη πρόσκληση. Τη φορά αυτή, η IBM πρότεινε μια παραλλαγή του κρυπτογραφικού συστήματος LUCIFER, το οποίο κρυπτογραφεί τμήματα δεδομένων μήκους 128 bits με ένα κλειδί μήκους επίσης 128 bits.

Το κρυπτογραφικό σύστημα που προτάθηκε από την IBM, αφού αναλύθηκε και τροποποιήθηκε σε μεγάλο βαθμό, δημοσιεύθηκε το 1976 με το όνομα DES και έγινε αποδεκτό ως πρότυπο τον επόμενο χρόνο. Πριν την υιοθέτησή του ως πρότυπο, ο DES αποτέλεσε αντικείμενο έντονης κριτικής, η οποία επικεντρώθηκε σε δύο περιοχές. Πρώτα από όλα, το μέγεθος του κλειδιού στον αρχικό αλγόριθμο LUCIFER ήταν 128 bits, ενώ αυτό που υπήρχε στο προτεινόμενο σύστημα ήταν μόνο 56 bits, υπήρχε δηλαδή μία τεράστια διαφορά στο μήκος του κλειδιού κατά 72 bits. Η δεύτερη περιοχή της διαμάχης ήταν η μη δημοσιοποίηση των κριτηρίων σχεδίασης των S-boxes (Αυτά δημοσιοποιήθηκαν στο μεταξύ, αμέσως μετά τη δημοσίευση της διαφορικής κρυπτανάλυσης). Έτσι, οι χρήστες ανησυχούσαν μήπως η εσωτερική δομή του DES έχει κρυμμένα αδύναμα σημεία, τα οποία επιτρέπουν στο NSA να αποκωδικοποιεί μηνύματα χωρίς να

χρησιμοποιεί καν το κλειδί. Ωστόσο, εργασίες στη διαφορική κρυπτανάλυση έδειξαν ότι ο DES έχει πολύ γερή εσωτερική δομή, τουλάχιστον απ' αυτή τη σκοπιά. Ο DES εξακολουθεί να χρησιμοποιείται ευρέως, στη σύνθετη πλέον παραλλαγή του Tripple DES, αφού στην απλή του μορφή δεν επαρκεί να αντιμετωπίσει κρυπταναλυτικές επιθέσεις που εκδηλώνονται με τη βοήθεια ισχυρής υπολογιστικής ισχύος ή ειδικών προς τούτο chips.

Στον αλγόριθμο DES, τα δεδομένα κρυπτογραφούνται σε τμήματα των 64 bits με τη χρήση ενός κλειδιού των 56 bits. Το κλειδί εκφράζεται συνήθως ως ένα τμήμα 64 bits ή 8 bytes, όμως κάθε όγδοο bit χρησιμοποιείται μόνο για τον έλεγχο της ισοτιμίας. Ο αλγόριθμος μετασχηματίζει το καθαρό κείμενο της εισόδου του των 64 bits, εφαρμόζοντας μια σειρά βημάτων, στο κρυπτογραφημένο κείμενο (έξοδο) των 64 bits. Τα ίδια βήματα, με το ίδιο κλειδί, χρησιμοποιούνται και για την αντίστροφη διαδικασία (αποκρυπτογράφηση), μόνο που τα (υπο-)κλειδιά χρησιμοποιούνται με την αντίστροφη σειρά (Zorkadis, Improving the Quality of Secure Distributed Systems, Proc. Of 3rd Intern. Conference on Reliability, Quality & Safety of Software-Intensive Systems, Chapman & Hall, 1997, pp. 186-197).



Εικόνα 2 Γενικό διάγραμμα του αλγορίθμου DES.

Ηλεκτρονική κατάρτιση συμβάσεων
Ψηφιακές υπογραφές

7.3.3 Ασύμμετροι Αλγόριθμοι (Περιγραφή του RSA)

Στη συνέχεια θα ασχοληθούμε με τη σχέση ισοτιμίας. Η σχέση a ≡ b mod n συμβολίζει την ισοτιμία του a με τον b modulo n (ως προς το μέτρο n). Οι a και b είναι ισότιμοι modulo n, αν a = b + kn, για κάποιον ακέραιο k. Αν οι a και b είναι θετικοί και ο b είναι μικρότερος του n, τότε ο b μπορεί να θεωρηθεί ως το υπόλοιπο του a, όταν ο τελευταίος διαιρείται με το n. Γενικά, οι αριθμοί a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με το n και επομένως η διαφορά τους a-b διαιρείται από το n. Το να διαιρείται η διαφορά τους a-b αποτελεί αναγκαία και ικανή συνθήκη για να είναι οι αριθμοί a και b ισοδύναμοι modulo n. Θα θυμηθούμε ορισμένα σημαντικά, από τη σκοπιά της Κρυπτογραφίας, αποτελέσματα της Αριθμοθεωρίας. Η συνάρτηση του Euler, γνωστή και ως συνάρτηση φ(n), είναι το πλήθος των στοιχείων του ανοιγμένου συστήματος υπολοίπων modulo n. Με άλλα λόγια, φ(n) είναι το πλήθος των φυσικών μικρότερων ή ίσων του n, οι οποίοι είναι σχετικά πρώτοι με αυτόν. Αν ο n είναι πρώτος, τότε φ(n) = n-1. Αν n = p q, όπου p και q πρώτοι, τότε φ(n) =φ(p)φ(q)=(p-1)(q-1) (Αυτοί οι αριθμοί εμφανίζονται στους αλγόριθμους δημοσίου κλειδιού).

Στον αλγόριθμο RSA χρησιμοποιούνται υπολογισμοί μεγάλων δυνάμεων ως προς μέτρο ισοτιμίας έναν φυσικό αριθμό n, ο οποίος είναι το γινόμενο δύο πολύ μεγάλων πρώτων αριθμών. Για τον λόγο αυτό, πρώτα δημιουργούνται (επιλέγονται) δύο πολύ μεγάλοι αριθμοί p και q και στη συνέχεια υπολογίζεται το γινόμενό τους, n = p q. Η κρυπτογράφηση ενός μηνύματος M, το οποίο χωρίζεται σε τμήματα M_1, M_2, …,M_K που αναπαριστώνται από αριθμούς μικρότερους του n, καθώς και η αποκρυπτογράφηση επιτυγχάνονται ως εξής:

$C_1 = M_1^{\ e} \pmod n$, $C_2 = M_2^{\ e} \pmod n$,…, $C_k = M_k^{\ e} \pmod n$

$M_1 = C_1^{\ d} \pmod n$, $M_2 = C_2^{\ d} \pmod n$, …, $M_k = C_k^{\ d} \pmod n$.

Ο αποστολέας του μηνύματος χρησιμοποιεί για την κρυπτογράφηση το δημόσιο κλειδί του παραλήπτη, το οποίο αποτελείται από τους αριθμούς e και n, δηλαδή {e, n}. Ο παραλήπτης αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα με το ιδιωτικό του κλειδί, το οποίο αποτελείται από τους αριθμούς d και n, δηλαδή {d, n}. Ας δούμε τώρα πως επιλέγονται οι αριθμοί e και d. Ο αριθμός e επιλέγεται έτσι ώστε να είναι σχετικά πρώτος ως προς το φ(n) και να ικανοποιεί την ακόλουθη σχέση: 3 < e < φ(n) = (p-1) (q-1).Υπενθυμίζουμε ότι το φ(n) είναι η συνάρτηση του Euler, η οποία υποδηλώνει το πλήθος των φυσικών, μικρότερων ή ίσων του n, οι οποίοι είναι σχετικά πρώτοι με αυτόν Αναφορικά με τον φυσικό αριθμό d, αυτός είναι αντίστροφος του e, δηλαδή προσδιορίζεται έτσι ώστε να πληροί την ακόλουθη σχέση ισοτιμίας: d e ≡1 mod φ(n)

Δημιουργία Κλειδιών

1. Επιλογή δύο πολύ μεγάλων πρώτων αριθμών p και q
2. Υπολογισμός του n = p q
3. Υπολογισμός ενός ακεραίου d (ή e), τέτοιου ώστε μκδ(φ(n), d) = 1 και 1<d<φ(n)
4. Υπολογισμός του φυσικού e, τέτοιου ώστε $e = d^{-1} \bmod \varphi(n)$
5. Δημοσιοποίηση του δημόσιου κλειδιού Kp = {e,n}. Το ιδιωτικό (ή μυστικό) κλειδί είναι το Ks = {d,n}

Κρυπτογράφηση Αποκρυπτογράφηση

Καθαρό μήνυμα M, M<n Κρυπτογραφημένο μήνυμα C

Κρυπτογραφημένο μήνυμα $C = M^e \pmod n$

Καθαρό μήνυμα $M = C^d \pmod n = M^{ed} \pmod n$

(R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital sugnatures and public key cryptosystems, Communications of the ACM, vol. 21, 1978, pp. 120-126).

Επιλέγουμε δύο πρώτους αριθμούς p=5 και q=11 και υπολογίζουμε το γινόμενό τους n = p q = 55. (Η επιλογή των μικρών αριθμών έγινε για λόγους απλοποίησης του παραδείγματος. Στην πράξη, οι αριθμοί αυτοί είναι, πάρα πολύ μεγάλοι.) Επίσης, υπολογίζουμε το γινόμενο (p-1) (q-1) = 40. Επιλέγοντας e=7, υπολογίζουμε τον αντίστροφό του, d=23 (ως προς τον αριθμό 40). Υποθέτουμε τώρα ότι θέλουμε να κρυπτογραφήσουμε το M = 2. Το κρυπτογραφημένο μήνυμα υπολογίζεται ως εξής: $C = 2^7 \pmod{55} = 128 \pmod{55} = 18$. Από το

κρυπτογραφημένο μήνυμα και το ιδιωτικό κλειδί {23, 55} υπολογίζεται το καθαρό μήνυμα: $M = 18^{23} \pmod{55}=2$.

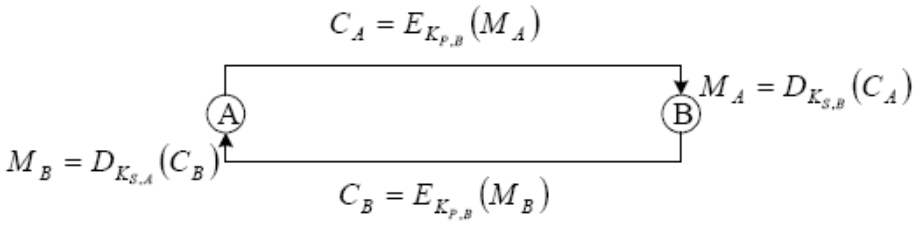
7.4 Τεχνική προσέγγιση της ηλεκτρονικής υπογραφής

Η δημιουργία της ηλεκτρονικής υπογραφής είναι κυρίως μια τεχνική διαδικασία. Η κρυπτογραφία αποτελεί το ιδιαίτερο γνώρισμα για την παραγωγή της ηλεκτρονικής υπογραφής. Μέσα από τη μέθοδο αυτή οδηγούμαστε στη δημιουργία της ψηφιακής υπογραφής (Καράκωστας, ο.π,193-194 Χριστοδούλου, ο.π,13 υποσ. 29). Η κρυπτογράφηση μηνύματος, όπως και η αποκρυπτογράφηση, απαιτεί ένα κλειδί. Διακρίνονται δύο μεγάλες κατηγορίες κρυπτογραφίας: πρώτον, η «συμμετρική» (symmetric) ή «κρυπτογραφία ιδιωτικού κλειδιού» (private key cryptography) και, δεύτερον, η «ασύμμετρη» (asymmetric) ή «κρυπτογραφία δημόσιου κλειδιού» (public key cryptography) ή «υποδομή δημόσιου κλειδιού» (public key infrastructure, PKI). (El Gamal, A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms , IEEE Transactions on Information Theory, Vol. 31, 1981, pp. 469-473) (A. Salomaa, 'Public Key Cryptography', Springer-Verlag, 1990).

Σήμερα, η εφαρμοζόμενη και κοινά αποδεκτή διαδικασία είναι αυτή της ασύμμετρης κρυπτογραφίας. Εν συντομία στην περίπτωση αυτή υπάρχουν δύο κλειδιά το ιδιωτικό και το δημόσιο. Το πρώτο συντελεί στην κωδικοποίηση των αποστελλόμενων δεδομένων, ενώ με το δεύτερο ο παραλήπτης μπορεί να αποκωδικοποιήσει το μήνυμα επιβεβαιώνοντας και αυτός τη γνησιότητα και ακεραιότητα τόσο του μηνύματος, όσο και την ταυτότητα του αποστολέα (Σιδηρόπουλος, ο.π, 84-85). Κάθε συναλλασσόμενος έχει πλέον το δικό του ζεύγος ταξιδιών, δηλαδή το ιδιωτικό κλειδί (private key), το οποίο είναι μυστικό και το γνωρίζει μόνο ο ιδιοκτήτης του, και το δημόσιο κλειδί (public key), το οποίο είναι ελεύθερα προσβάσιμο . Το ΠΔ 150/2001 αποκαλεί το ιδιωτικό κλειδί με το γενικό όρο «δεδομένα δημιουργίας υπογραφής», τα οποία ορίζει ως «μονοσήμαντα δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής», ενώ το δημόσιο κλειδί αποκαλείται με τον επίσης γενικό όρο «δεδομένα επαλήθευσης υπογραφής», τα οποία ορίζονται ως «δεδομένα, όπως κώδικες, ή δημόσια κλειδιά κρυπτογραφίας, τα οποία χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής»(Άρθρο 2 αριθ. 7 του ΠΔ 150/2001).

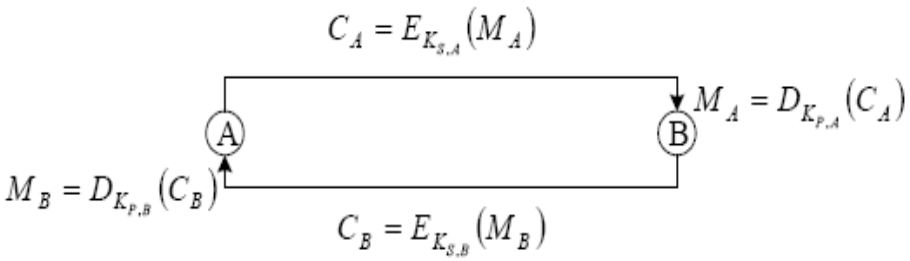
Ζήτημα γεννάται ως προς τη μυστικότητα του ιδιωτικού κλειδιού. Θα πρέπει σε κάθε περίπτωση ο κάτοχός του να το προφυλάσσει και να μην το γνωστοποιεί σε τρίτα πρόσωπα, διαφορετικά η ασφάλεια των ηλεκτρονικών του συναλλαγών θα είναι διάτρητη, επιφέροντας ανασφάλεια για τον ίδιο, αλλά και για κάθε άλλο πρόσωπο με το οποίο θα συνδιαλλαγεί στο μέλλον. Στα πλαίσια αυτά συμπεριλαμβάνεται και ο προβληματισμός κατοχής και χρήσης της μυστικής κλείδας των νομικών προσώπων.

Στην Εικόνα 3 παρουσιάζεται η εμπιστευτική επικοινωνία δύο χρηστών, των Α και Β. Ο Α κατέχει το ιδιωτικό κλειδί $K_{S,A}$ και το δημόσιο κλειδί $K_{P,A}$ και ο Β το ιδιωτικό κλειδί $K_{S,B}$ και το δημόσιο κλειδί $K_{P,B}$. Ο Α επιθυμεί να στείλει στον Β το μήνυμα M_A και ο Β επιθυμεί να στείλει στον Α το μήνυμα M_B. Ο Α κρυπτογραφεί το μήνυμα M_A με το δημόσιο κλειδί του Β, $K_{P,B}$ και του αποστέλλει το κρυπτογραφημένο μήνυμα C_A, το οποίο ο Β αποκρυπτογραφεί με το ιδιωτικό του κλειδί $K_{S,B}$. Από την άλλη πλευρά, ο Β κρυπτογραφεί το μήνυμα M_B με το δημόσιο κλειδί του Α, $K_{P,A}$ και του αποστέλλει το κρυπτογραφημένο μήνυμα C_B, το οποίο ο Α αποκρυπτογραφεί με το ιδιωτικό του κλειδί $K_{S,A}$ (Ζορκάδης, Β, Κρυπτογραφία,ΕΑΠ,2002, σελ.202).



Εικόνα 3 Κρυπτογράφηση και αποκρυπτογράφηση με ασύμμετρο αλγόριθμο

Στην Εικόνα 4 παρουσιάζεται η αυθεντική επικοινωνία δύο χρηστών, του Α και Β. Ο Α επιθυμεί να στείλει στον Β το μήνυμα M_A και ο Β επιθυμεί να στείλει στον Α το μήνυμα M_B. Ο Α κρυπτογραφεί το μήνυμα M_A με το ιδιωτικό του κλειδί $K_{S,A}$ και του αποστέλλει το κρυπτογραφημένο μήνυμα C_A, το οποίο ο Β αποκρυπτογραφεί με το δημόσιο κλειδί του Α, $K_{P,A}$. Παρατηρούμε ότι όλοι οι άλλοι χρήστες είναι σε θέση να αποκρυπτογραφήσουν το C_A, αφού γνωρίζουν το δημόσιο κλειδί του Α. Όμως, αυτό που ενδιαφέρει είναι η αυθεντικότητα της πηγής προέλευσης, δηλαδή η επαλήθευση της αποστολής του μηνύματος από τον Α και όχι η εμπιστευτικότητα του περιεχομένου. Η αυθεντικότητα της πηγής προέλευσης του μηνύματος επιτυγχάνεται ασφαλώς μέσω της κρυπτογράφησής του με το ιδιωτικό κλειδί του αποστολέα, αφού ο αποστολέας είναι ο μόνος που γνωρίζει το μυστικό του κλειδί. Κατά ανάλογο τρόπο, ο Β κρυπτογραφεί το μήνυμα M_B με το ιδιωτικό του κλειδί, $K_{S,B}$ και αποστέλλει στον Α το κρυπτογραφημένο μήνυμα C_B, το οποίο ο Α αποκρυπτογραφεί με το δημόσιο κλειδί του Β, $K_{P,B}$. (Ζορκάδης, Β, Κρυπτογραφία,ΕΑΠ,2002, σελ.203).



Εικόνα 4 Αυθεντική επικοινωνία μεταξύ δύο χρηστών με τη βοήθεια ασύμμετρων κρυπτογραφικών αλγορίθμων.

7.5 Κλειδιά σε συμμετρικούς αλγορίθμους

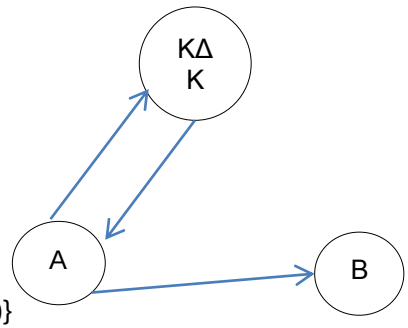
Το θέμα της διαχείρισης κλειδιών αφορά τους συμμετρικούς και τους ασύμμετρους αλγόριθμους κρυπτογραφίας, καθώς και τα σχήματα ψηφιακών υπογραφών και μια κατηγορία συναρτήσεων κατακερματισμού. Η ασφάλειά τους εξαρτάται σε καθοριστικό βαθμό όχι μόνο από την επιλογή

ενός επαρκώς δύσκολου μαθηματικού προβλήματος αλλά και από τη δημιουργία, μεταφορά και συντήρηση κατάλληλων κρυπτογραφικών κλειδιών. Η διαχείριση κλειδιών αναφέρεται στη δημιουργία, μεταφορά, πιστοποίηση, αποθήκευση, αντικατάσταση, χρήση και καταστροφή κρυπτογραφικών κλειδιών. Τα κλειδιά πρέπει να είναι τυχαία και μη προβλέψιμα και για το λόγο αυτό απαιτείται η αξιοποίηση πηγών πραγματικά τυχαίων ακολουθιών. Μόνο στην περίπτωση που δεν είναι δυνατή η χρήση πηγών τυχαίων ακολουθιών και μόνο για κλειδιά με πολύ μικρή διάρκεια ζωής, όπως τα κλειδιά συνόδου, μπορούν να χρησιμοποιούνται για τη δημιουργία τους ισχυρές γεννήτριες ψευδοτυχαίων αριθμών.

Κατά τη μεταφορά μυστικών κλειδιών συμμετρικών αλγορίθμων πρέπει να διασφαλιστεί η γνησιότητα της προέλευσης, η ακεραιότητα και η εμπιστευτικότητά τους. Στη διανομή των κρυπτογραφικών κλειδιών εμπλέκονται κατά κανόνα κέντρα διανομής κλειδιών ή αρχές πιστοποίησης ή πάροχοι υπηρεσιών πιστοποίησης. Επίσης, στη διανομή ή ανταλλαγή ή διαδικασία συμφωνίας κλειδιών συμμετρικών συστημάτων χρησιμοποιούνται πλέον πρωτόκολλα που βασίζονται σε μεγάλο βαθμό και σε ασύμμετρα κρυπτογραφικά συστήματα, αφού αυτός ήταν και ένας από τους λόγους που επιδιώχτηκε η επινόηση των τελευταίων Στη μεταφορά (διανομή) κλειδιών συμμετρικών αλγορίθμων με τη βοήθεια μόνο συμμετρικών αλγορίθμων απαιτείται από τη μια η αποστολή κάποιων κλειδιών με φυσικό τρόπο και από την άλλη η φυσική προστασία των κλειδιών κατά τη δημιουργία και την αποθήκευσή τους. Η φυσική προστασία επιτυγχάνεται με τη χρήση ειδικών στοιχείων ασφάλειας υλικού, ανθεκτικών στην παραβίαση (tamper-resistant modules).Τα κέντρα διανομής κρυπτογραφικών κλειδιών (ΚΔΚ) μπορεί να εμπλέκονται offline ή on-line. Σε κάθε περίπτωση, ένα ΚΔΚ μοιράζεται με καθέναν από τους χρήστες ένα μυστικό κλειδί. Με τη βοήθεια αυτού του κλειδιού κρυπτογραφούνται άλλα κλειδιά, τα οποία οι χρήστες χρησιμοποιούν σε κάθε επικοινωνία.

Ας δούμε στη συνέχεια ως παράδειγμα ένα πρωτόκολλο on-line διανομής κλειδιών. Έστω ένα ΚΔΚ και δύο χρήστες, ο Α και ο Β, με τους οποίους το ΚΔΚ μοιράζεται το μυστικό κλειδί $K_{A,S}$ και το $K_{B,S}$ αντίστοιχα. Οι Α και Β επιθυμούν να επικοινωνήσουν μεταξύ τους εμπιστευτικά και για το λόγο αυτό χρειάζονται ένα μυστικό κλειδί $K_{A,B}$, το οποίο αποκτούν ως ακολούθως:

1. Ο Α γνωστοποιεί στο ΚΔΚ, με το μήνυμα 1 (Εικόνα 5), την επιθυμία του να επικοινωνήσει εμπιστευτικά με τον χρήστη Β. Κάνει δε χρήση του κλειδιού $K_{A,S}$ που μοιράζεται με το κέντρο.
2. Το ΚΔΚ αποστέλλει στον χρήστη Α το επιθυμητό κλειδί $K_{A,B}$ το οποίο θα χρησιμοποιήσουν οι Α και Β στη μεταξύ τους επικοινωνία. Το κλειδί είναι κρυπτογραφημένο τόσο με το $K_{A,S}$ όσο και με το $K_{B,S}$ (δείτε μήνυμα 2, Εικόνα 5).
3. Ο Α αφού εξάγει από το μήνυμα 2 την κρυπτογραφημένη μορφή του $K_{A,B}$ με το $K_{B,S}$ την αποστέλλει στον Β (δείτε μήνυμα 3, Εικόνα 5). Πλέον οι Α και Β μοιράζονται το μυστικό κλειδί $K_{A,B}$ το οποίο δημιούργησε το ΚΔΚ και μπορούν να επικοινωνήσουν εμπιστευτικά.



1. $\{A,K_{A,S}(A,B)\}$
2. $\{ K_{A,S}[K_{A,B}, K_{B,S}(K_{A,B})]\}$ **Εικόνα 5**

3. {A, $K_{B,S}(K_{A,B})$}

Το ανωτέρω ιεραρχικό σχήμα διανομής κλειδιών βασίζεται στα κλειδιά που μοιράζεται το ΚΔΚ με καθέναν από τους χρήστες για τη μεταφορά ενός άλλου κλειδιού, το οποίο θα χρησιμοποιηθεί για την επικοινωνία των χρηστών Α και Β. Ένα αρκετά αντιπροσωπευτικό ιεραρχικό σχήμα αυτής της κατηγορίας είναι και αυτό της IBM, το οποίο χρησιμοποιήθηκε σε συστήματα αποτελούμενα από έναν κεντρικό υπολογιστή και πολλά τερματικά. Τα δεδομένα που μεταφέρονται μεταξύ του υπολογιστή και των τερματικών κρυπτογραφούνται με κλειδιά, τα οποία αποθηκεύονται στον υπολογιστή. Τα δεδομένα και τα κλειδιά μεταφέρονται μέσω των ίδιων επικοινωνιακών καναλιών. Το σχήμα διανομής κλειδιών της IBM κάνει χρήση τεσσάρων κλειδιών: δύο γενικών κλειδιών, των K_0 και K_1, του κλειδιού του τερματικού K_T και του κλειδιού συνόδου K_S. Το κλειδί του τερματικού K_T χρησιμοποιείται για τη μεταφορά του εκάστοτε κλειδιού συνόδου K_S, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων επικοινωνίας μεταξύ του τερματικού και του κεντρικού υπολογιστή. Όσο για τα κλειδιά K_0 και K_1, αυτά παραμένουν γνωστά μόνο εντός του κεντρικού υπολογιστή και χρησιμοποιούνται για τη διασφάλιση των K_T και K_S,δεν επιτρέπουν δηλαδή σε αυτά τα κλειδιά να εμφανιστούν σε καθαρή μορφή εκτός των ειδικών στοιχείων ασφάλειας υλικού (security modules) (Ζορκάδης, Β, Κρυπτογραφία,ΕΑΠ,2002, σελ.283).

7.6 Κλειδιά σε ασύμμετρους αλγορίθμους

Η ανάπτυξη των ασύμμετρων κρυπτογραφικών συστημάτων επέφερε σημαντικές αλλαγές στα κρυπτογραφικά πρωτόκολλα και στους λοιπούς μηχανισμούς ασφάλειας. Έτσι, κατά κανόνα στο πλαίσιο της αυθεντικοποίησης των εμπλεκομένων στην επικοινωνία, ανταλλάσσονται ή συμφωνούνται και μυστικά κλειδιά συμμετρικών συστημάτων. Στα πρώτα συστήματα αυτής της κατηγορίας συγκαταλέγονται το Kerberos, το SPX και το SELANE. Επίσης, πρότυπα αυτής της κατηγορίας είναι η υπηρεσία αυθεντικοποίησης καταλόγου ITU X.509, Directory Authentication Service(ISO/IEC 9594-8 (ITU X.509), Information Technology – Open Systems Interconnection– The Directory – Authentication Framework) και το ISO/IEC 11770(ISO/IEC 11770, Information Technology – Security techniques – Key management, Part1: Framework, Part I2: Mechanisms using symmetric techniques, Part 3: Mechanisms using asymmetric techniques, 1999). Η καρδιά του προτύπου ITU X.509 (ή ISO/IEC 9594-8) είναι το πιστοποιητικό του δημόσιου κλειδιού, το οποίο συσχετίζεται με κάθε χρήστη και το οποίο εκδίδεται από την αρχή πιστοποίησης ή τον πάροχο υπηρεσιών πιστοποίησης. Από την άλλη πλευρά, στο πιο πρόσφατο πρότυπο ISO/IEC 11770 (1999) ορίζονται, σε τρία μέρη, το γενικό πλαίσιο της διαχείρισης κλειδιών, μηχανισμοί βασισμένοι σε συμμετρικά και μηχανισμοί βασισμένοι σε ασύμμετρα συστήματα, αντίστοιχα. Πιο συγκεκριμένα, στο πρότυπο ISO/IEC 11770-3 ορίζονται μηχανισμοί συμφωνίας μυστικού κλειδιού, μεταφοράς μυστικού κλειδιού και μεταφοράς δημόσιου κλειδιού, που βασίζονται σε ασύμμετρες τεχνικές. Στο πρότυπο αυτό γίνεται διάκριση μεταξύ μηχανισμών συμφωνίας και μεταφοράς μυστικού κλειδιού μεταξύ δύο χρηστών που επιθυμούν να επικοινωνήσουν. Κατά τη συμφωνία μυστικού κλειδιού μεταξύ δύο οντοτήτων Α και Β, το οποίο θα χρησιμοποιηθεί ακολούθως για την μεταξύ τους εμπιστευτική επικοινωνία με τη βοήθεια συμμετρικού αλγορίθμου, το μυστικό κλειδί είναι το αποτέλεσμα ανταλλαγής δεδομένων μεταξύ των Α και Β. Κανένας από τους δύο δεν είναι σε θέση να προκαθορίσει την τιμή του μυστικού κλειδιού που θα μοιραστούν.Σε μηχανισμούς μεταφοράς μυστικού κλειδιού, από την άλλη πλευρά, ο ένας από τους χρήστες, έστω ο Α επιλέγει το μυστικό κλειδί και το αποστέλλει στον άλλο χρήστη, τον Β. Το μυστικό κλειδί προστατεύεται κατά τη μεταφορά του με τη βοήθεια ασύμμετρων αλγορίθμων.

Στους μηχανισμούς μεταφοράς δημόσιων κλειδιών, τέλος, το δημόσιο κλειδί μιας οντότητας (χρήστη) αποστέλλεται σε έναν άλλο χρήστη. Η μεταφορά του δημόσιου κλειδιού πρέπει να λάβει χώρα με παράλληλη διασφάλιση της ακεραιότητας και της αυθεντικότητας προέλευσης του κλειδιού, όχι όμως και της εμπιστευτικότητας.

ΜΗΧΑΝΙΣΜΟΣ ΜΕΤΑΦΟΡΑΣ ΜΥΣΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΒΑΣΙΣΜΕΝΟΣ ΣΤΟΝ RSA

Θεωρούμε ότι τόσο ο Α όσο και ο Β γνωρίζουν ήδη το δημόσιο κλειδί του άλλου,

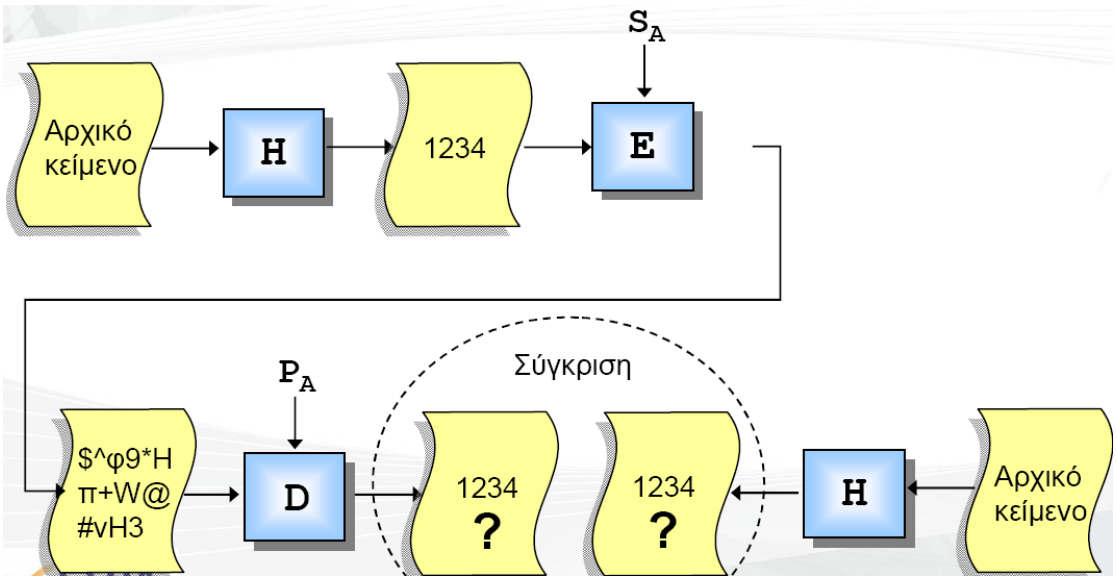
δηλαδή ο Α γνωρίζει το $P_B = \{e_B, n\}$ και ο Β το $P_A = \{e_A, n\}$. Τα μυστικά τους κλειδιά

είναι τα S_A και S_B, αντίστοιχα. Ο μηχανισμός μεταφοράς του μυστικού κλειδιού διακρίνεται στα ακόλουθα βήματα:

1. Ο χρήστης Α επιλέγει ένα μυστικό κλειδί $K_{A,B}$ το οποίο επιθυμεί να στείλει στον Β. Αφού το συνδέσει με την ταυτότητά {Α, $K_{A,B)}$}, το κρυπτογραφεί με το δημόσιο κλειδί του Β και αποστέλλει σ' αυτόν επομένως το μήνυμα: P_B(Α, $K_{A,B}$)
2. Ο Β, αφού λάβει το ανωτέρω μήνυμα, το αποκρυπτογραφεί με το ιδιωτικό του κλειδί και εξάγει από την καθαρή του μορφή την ταυτότητα του Α και το μυστικό κλειδί $K_{A,B}$. (Diffie – Hellman, New Directions in Cryptography, (IEEE Transactions on Information Theory , Vol. 22, n. 6,1976, pp. 644-654).

7.7 Ασφαλείς συναρτήσεις κατακερματισμού

Η συνάρτηση κατακερματισμού είναι ένας αλγόριθμος ο οποίος υπολογίζει μία τιμή βασισμένη σε ένα ηλεκτρονικό αντικείμενο (όπως ένα μήνυμα ή ένα αρχείο, συνήθως πολύ μεγάλο), χαρτογραφώντας το ηλεκτρονικό αντικείμενο σε ένα μικρότερο ηλεκτρονικό αντικείμενο . Το ηλεκτρονικό αντικείμενο που εξάγεται από τον αλγόριθμο κατακερματισμού ονομάζεται σύνοψη του αρχικού μηνύματος. Οποιαδήποτε αλλαγή του ηλεκτρονικού αντικειμένου που εισάγεται στον αλγόριθμο οδηγεί, με μεγάλη πιθανότητα, σε διαφορετική σύνοψη. Αντίθετα, όταν εισάγεται το ίδιο αντικείμενο στον αλγόριθμο κατακερματισμού, η σύνοψη που εξάγεται είναι ακριβώς η ίδια. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο πρωτότυπο μη κρυπτογραφημένο μήνυμα και αποστέλλονται μαζί μέσω του Διαδικτύου (Παπαθωμά — Μπέτγκε, ό.π., σελ. 1241).



Εικόνα 5 Ψηφιακές υπογραφές και συναρτήσεις κατακερματισμού(Η) . S_A , P_A το ιδιωτικό και δημόσιο κλειδί του Α αντίστοιχα.

Η ασφαλής συνάρτηση κατακερματισμού είναι μία συνάρτηση κατακερματισμού με συγκεκριμένες ιδιότητες. Η σημαντικότερη ίσως από αυτές είναι ότι η σύνοψη του μηνύματος δεν μπορεί να πλαστογραφηθεί, υπό την έννοια ότι δεδομένου κάποιου συγκεκριμένου μηνύματος εισόδου είναι υπολογιστικά αδύνατο να παραχθεί από την αρχή ένα άλλο μήνυμα που να έχει την ίδια σύνοψη με το πρώτο.

Το μήκος μίας ασφαλούς σύνοψης καθώς και οι κρυπτογραφικές της ιδιότητες είναι πολύ σημαντικές. Ο λόγος είναι ότι η ιδιότητα της αδυναμίας δημιουργίας ενός εγγράφου που

να παράγει την ίδια σύνοψη με ένα διαφορετικό δεύτερο έγγραφο εξαρτάται από το μέγεθος της σύνοψης. Έτσι, σε περίπτωση που η σύνοψη είναι πολύ μικρή, μπορεί κανείς δοκιμάζοντας διαδοχικές ασήμαντες αλλαγές, όπως τα διαστήματα μεταξύ των λέξεων ή η αντικατάσταση μίας λέξης ή φράσης, να πετύχει την εξαγωγή της επιθυμητής σύνοψης.

7.8 Τρόποι ηλεκτρονικής υπογραφής

7.8.1 Προσωπικός κωδικός επικοινωνίας (PIN)

Η χρήση προσωπικού κωδικού επικοινωνίας (Personal Identification Number- PIN) συνίσταται στην χρησιμοποίηση ενός προσωπικού κωδικού αριθμού, με τον οποίο ο χρήστης δηλώνει την ταυτότητά του. Ο χρήστης φέρει το βάρος να μην αποκαλύπτει τον κωδικό αριθμό του σε τρίτους ενώ υφίσταται τεχνικώς η δυνατότητα ο αριθμός να γνωστοποιηθείς τον χρήστη-δικαιούχο κατά τρόπο που να μην επιτρέπει να καταστεί γνωστός ούτε στην υπηρεσία που τον εξέδωσε (π.χ. στο τμήμα μηχανογράφησης μίας τράπεζας).

Μειονέκτημα της συγκεκριμένης μεθόδου τεκμηρίωσης που αποκλείει την χρήση της στα ανοιχτά δίκτυα, όπως στο Διαδίκτυο, αποτελεί το γεγονός ότι απαιτεί την προκαταρκτική συμβατική επαφή των μερών που πρόκειται να κάνουν χρήση αυτής, αλλά και την ύπαρξη σχέσης εμπιστοσύνης ανάμεσα στα δύο μέρη, ανάγκη που ικανοποιείται στην πράξη εν μέρει από τον απρόσωπο χαρακτήρα των σύγχρονων μαζικών συναλλαγών με την χρήση του ηλεκτρονικού υπολογιστή . Ωστόσο, συνεχίζει να αποτελεί την πιο διαδεδομένη μέθοδο τεκμηρίωσης για συναλλαγές χαμηλού κινδύνου ή μικρού οικονομικού αντικειμένου (π.χ. για την εγγραφή σε συνδρομητικές βάσεις δεδομένων έναντι χαμηλού κόστους).

Η χρήση προσωπικού κωδικού αναγνώρισης αποτελεί μορφή ηλεκτρονικής υπογραφής με την έννοια του άρθρου 2 § 1 του ΠΔ. 150/2001 και της Οδηγίας 99/93/ΕΚ, αφού ο αριθμός PIN όταν εισάγεται σε ένα σύστημα ηλεκτρονικού υπολογιστή αποτελεί δεδομένο σε ηλεκτρονική μορφή, το οποίο είναι συνημμένο σε άλλα ηλεκτρονικά δεδομένα (π.χ. στα στοιχεία της τραπεζικής συναλλαγής) και το οποίο χρησιμεύει ως μέθοδος απόδειξης της γνησιότητας των δεδομένων.

7.8.2 Μέσω των «έξυπνων» καρτών

Ο υπογράφων, χρειάζεται να έχει αποθηκευμένη την ηλεκτρονική υπογραφή σε ένα μέσο εύχρηστο, ελαφρύ και οικονομικό ως προς την κατασκευή του, το οποίο θα έχει πάντα μαζί του και θα χρησιμοποιεί κατά τις ηλεκτρονικές του συναλλαγές. Το μέσο αποθήκευσης της ηλεκτρονικής υπογραφής, είναι οι «έξυπνες» κάρτες (smart cards). Οι «έξυπνες» κάρτες είναι ουσιαστικά μικροσκοπικοί Η/Υ που έχουν το μέγεθος και το σχήμα μιας πιστωτικής κάρτας, επάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο ηλεκτρονικό κύκλωμα (chip) που περιέχει αποθηκευμένη την ηλεκτρονική υπογραφή.

Σημαντική είναι επίσης η ικανότητα τους να αποθηκεύουν το ιδιωτικό κλειδί της ψηφιακής υπογραφής του χρήστη της «έξυπνης» κάρτας, έτσι ώστε να διασφαλίζονται αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα και μη αποποίηση ευθύνης. Ο τρόπος επικοινωνίας με αυτές τις «έξυπνες» κάρτες είναι η τοποθέτηση τους σε συσκευές αποδοχής «έξυπνων» καρτών (card readers) (Κυρλόγλου, «Ασύρματες έξυπνες κάρτες μιάς χρήσης», περιοδικό «Ανάπτυξη» του ΕΒΕΑ, (3) 2003, σελ.86 επ., διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.acci.gr/anaptixi/0303/86_87.pdf).

Εικόνα 6 έξυπνη κάρτα (smart card), καρταναγνώστης (card reader) , USB token.

7.8.3 Βιομετρική υπογραφή

α) Δακτυλικό αποτύπωμα

Φαίνεται πως θα είναι μια από τις βιομετρικές τεχνολογίες που θα χρησιμοποιηθούν ευρύτατα στο μέλλον για να υπογράφουν ηλεκτρονικά οι συναλλασσόμενοι. Συσκευές σάρωσης αποτυπωμάτων έχουν ήδη εγκατασταθεί σε κρατικές και ιδιωτικές εγκαταστάσεις, σε τερματικά μηχανήματα ανάληψης χρημάτων από τράπεζες. Επίσης, η πιστοποίηση της γνησιότητας του αποτυπώματος είναι γρήγορη και αξιόπιστη, χωρίς ο σαρωτής να καταλαμβάνει μεγάλο χώρο και είναι ενσωματωμένος στο «ποντίκι» του Η/Υ.

β) Γεωμετρία χεριού

Μια άρτια συσκευή σάρωσης του αποτυπώματος της παλάμης θα πρέπει να εξετάζει τόσο την επάνω όσο και τις πλαϊνές όψεις του χεριού χρησιμοποιώντας ενσωματωμένη βιντεοκάμερα. Συσκευές ανίχνευσης της γεωμετρίας του χεριού βρίσκονται συνήθως σε εγκαταστάσεις όπως κοινοβούλια, αεροδρόμια.

γ) Σχέδιο ίριδας

Σάρωση της ίριδας του ματιού μπορεί να πραγματοποιηθεί ακόμη και από μερικά μέτρα απόσταση, επιτρέποντας έτσι την ευρεία και εύκολη εφαρμογή της τεχνολογίας αυτής, μεταξύ άλλων, και σε ATM, εφαρμογή που διευκολύνει σημαντικά τις ηλεκτρονικές συναλλαγές.

δ) Σχέδιο αμφιβληστροειδούς

Οι περισσότερες χρήσεις αυτής της βιομετρικής ηλεκτρονικής υπογραφής συναντώνται σε σημεία ελέγχου πρόσβασης σε εγκαταστάσεις ύψιστης ασφάλειας, γιατί εξασφαλίζουν πολύ χαμηλά ποσοστά λανθασμένης απόρριψης.

ε) Δείγμα φωνής

Το δείγμα φωνής δεν θεωρείται τόσο αξιόπιστο όσο άλλες βιομετρικές τεχνικές, αφενός γιατί δεν λειτουργεί σωστά όταν υπάρχουν εξωτερικοί θόρυβοι κατά την προφορά της φράσης - κλειδιού από το χρήστη.

Ηλεκτρονική κατάρτιση συμβάσεων

Ψηφιακές υπογραφές

ζ) Ρυθμός πληκτρολόγησης

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

η) Ηλεκτρονική καταγραφή της χειρόγραφης υπογραφής

Οι συσκευές ηλεκτρονικής καταγραφής της υπογραφής χρησιμοποιούν ηλεκτρονικά «στυλό», επιφάνειες ευαίσθητες σε πίεση, και είναι οικονομικές (Κυρλόγλου, «Βιομετρικά συστήματα πιστοποίησης - οι συνηθέστερες μέθοδοι πιστοποίησης της ταυτότητας», περιοδικό «Ανάπτυξη» του ΕΒΕΑ, (5) 2002, σελ.81 επ., διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.acci.gr/anaptixi/0502/81-82.pdf).

7.9 Ουσιαστική και δικονομική αξία της ηλεκτρονικής υπογραφής

Η ανωτερότητα της προηγμένης ηλεκτρονικής υπογραφής, σε σχέση με τις υπόλοιπες ηλεκτρονικές υπογραφές, συνδέεται στενά με την υψηλότερη διασφάλιση και του ηλεκτρονικού εγγράφου. Έτσι, η προηγμένη ηλεκτρονική υπογραφή επιτελεί ότι και η ιδιόχειρη υπογραφή. Η ως άνω ταύτιση δικαιολογείται με τους τέσσερις χαρακτηριστικούς όρους της προηγμένης ηλεκτρονικής υπογραφής, όπως αυτοί απαριθμούνται στο νομοθετικό ορισμό της(Π.Δ. 150/2001 άρθρο 2 στ. 2).

Σε κάθε περίπτωση, η προηγμένη ηλεκτρονική υπογραφή παράγει όλες τις έννομες συνέπειες της ιδιόχειρης. Τα δε άλλα είδη ηλεκτρονικής υπογραφής αποτελούν ευρύτερα στοιχεία υπογραφής υποβαθμισμένα όμως σε αντιπαραβολή προς την προηγμένη. Ωστόσο , δύνανται και αυτές οι υποβαθμισμένες μορφές υπογραφής να επιτελέσουν το ρόλο τους ανάλογα με τα επιβαλλόμενα από το νόμο και κατά δεύτερον από τη συμφωνία των συμβαλλομένων μερών (ΜΠρΑθ. 1327/2001).

7.10 Πάροχοι Υπηρεσιών Πιστοποίησης

Οδηγούμαστε στην ανάγκη ύπαρξης ενός μηχανισμού, ο οποίος θα εγγυάται και θα πιστοποιεί ανά πάσα στιγμή στο συναλλασσόμενο ότι το δημόσιο κλειδί που χρησιμοποιεί για να αποκρυπτογραφήσει ένα ηλεκτρονικά υπογεγραμμένο αρχείο ανήκει πραγματικά στον αντισυμβαλλόμενο του και, επομένως, ότι η ηλεκτρονική υπογραφή που χρησιμοποιεί ο αντισυμβαλλόμενος ανήκει πράγματι σε αυτόν. Ο μηχανισμός αυτός πρέπει να υλοποιείται από έναν έμπιστο τρίτο, τον οποίο τα συναλλασσόμενα μέρη γνωρίζουν εκ των προτέρων. Ο έμπιστος αυτός τρίτος ονομάζεται «Πάροχος Υπηρεσιών Πιστοποίησης» (ΠΥΠ)(Trusted Third Party (TTP)) και η συμβολή του στην ύπαρξη ασφάλειας και εμπιστοσύνης στις συναλλαγές που πραγματοποιούνται στο περιβάλλον ανωνυμίας του Διαδικτύου είναι πολύτιμη. Σύμφωνα με το άρθρο 2 αριθ. 11 του ΠΔ150/2001, ο ΠΥΠ είναι «φυσικό ή νομικό πρόσωπο ή άλλος φορέας που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές». Ο ενδιαφερόμενος χρήστης παραγάγει - με τη βοήθεια κατάλληλου λογισμικού που έχει προμηθευτεί από τον ΠΥΠ - το ζεύγος ιδιωτικού και δημόσιου κλειδιού που αποτελεί την ψηφιακή του υπογραφή (Κυρλόγλου, «Ασφαλείς συναλλαγές στο Διαδίκτυο», περιοδικό «Ανάπτυξη» του ΕΒΕΑ, (10) 2001, σσ.82 επ., διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.acci.gr/anaptixi/1001/82-85.pdf) Η έκδοση πιστοποιητικών γνησιότητας, με τα οποία πιστοποιείται η μοναδική σχέση μεταξύ του δημόσιου κλειδιού και του νόμιμου ιδιοκτήτη του, είναι η πιο σημαντική λειτουργία του ΠΥΠ,. Ήδη η Οδ. 1999/93/ΕΚ περιλαμβάνει την έννοια αυτών των προσώπων στο άρθρο 2 στ. 11. Η συμβολή των προσώπων αυτών έγκειται, σύμφωνα με την προαναφερόμενη διάταξη, κυρίως στην πιστοποίηση των ηλεκτρονικών υπογραφών. Εννοιολογικά ταυτόσημη είναι και η διάταξη του Π.Δ. 150/2001 και στην ανάλογη μάλιστα θέση (άρθρο 2 στ. 11).

Πέραν των στενών οριοθετήσεων των νομοθετικών κειμένων μπορούμε να τονίσουμε ότι το διαδίκτυο ως ανοικτό δίκτυο δεν προσφέρει την απαιτούμενη ασφάλεια. Αυτός είναι και ο δικαιολογητικός λόγος ύπαρξης των παρόχων. Στα πλαίσια των απρόσωπων διαδικτυακών συναλλαγών οι διαδικασίες πιστοποίησης αποτελούν βασική προϋπόθεση καλής λειτουργίας

του ηλεκτρονικού εμπορίου και ως εκ τούτου η ύπαρξη τρίτων έμπιστων προσώπων κρίνεται επιβεβλημένη. (άρθρο 6 Οδ. 1999/93/ΕΚ και ανάλογα στο άρθρο 6 Π.Δ. 150/2001). Στην ενδυνάμωση της ύπαρξης αυτών των προσώπων η Οδηγία για τις ηλεκτρονικές υπογραφές επιβάλλει ελεύθερο καθεστώς ίδρυσης και λειτουργίας τους(άρθρο 3 παρ.5 Οδ. 1999/93/ΕΚ και άρθρο 4 παρ.4 Π.Δ. 150/2001).

Τα τρίτα αξιόπιστα αυτά μέρη, όπως έχει επικρατήσει στη θεωρία να χαρακτηρίζονται, δεν μετέχουν άμεσα ούτε στις ηλεκτρονικές συναλλαγές, αλλά ούτε και σε κανενός είδους διαδικτυακής επικοινωνίας. Αυτό όμως δεν αποδυναμώνει τη σπουδαιότητα ύπαρξής τους και συμβολή τους στην προαγωγή της διαδικτυακής χρήσης. Εξάλλου και μόνη η λειτουργία της πιστοποίησης των ηλεκτρονικών υπογραφών με την έκδοση των απαιτούμενων πιστοποιητικών αποτελεί κρίσιμο παράγοντα και βασική νομική προϋπόθεση για την εγκυρότητα των προϊόντων της ηλεκτρονικής υπογραφής (άρθρο 2 Οδ. 1999/93/ΕΚ και το Παράρτημα Ι).

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

7.10.1 Οι λειτουργίες των παρόχων υπηρεσιών πιστοποίησης

Η ταυτοποίηση αυτού που υπογράφει ηλεκτρονικά ένα αρχείο με το πρόσωπο στο οποίο ανήκει το δημόσιο κλειδί αποκρυπτογράφησης του αρχείου επιτυγχάνεται χάρη στο δημόσιο κλειδί του ΠΥΠ, ο οποίος έχει στο μεταξύ υπογράψει και επικυρώσει με το ιδιωτικό του κλειδί τα δημόσια κλειδιά των πελατών του, ιδιοκτητών ηλεκτρονικής υπογραφής. Το δημόσιο κλειδί του ΠΥΠ είναι ελεύθερα προσβάσιμο στο Διαδίκτυο και πολλές φορές περιλαμβάνεται στα προϊόντα που αναγνωρίζονται ως φερέγγυα από το ίδιο το πρόγραμμα πλοήγησης του χρήστη.

Ο πάροχος ως υποκείμενο πλέον του κύκλου των ηλεκτρονικών υπογραφών, λόγω ακριβώς της επιβεβαιωτικής του λειτουργίας στην ταυτοπροσωπία του υπογράφοντα, διορθώνει τις ατέλειες της τεχνολογίας της ψηφιακής υπογραφής. Αυτό επιτυγχάνεται με την έκδοση πιστοποιημένων κλειδιών. Συγκεκριμένα η διαδικασία επαλήθευσης της ψηφιακής υπογραφής με τη δημόσια κλείδα του υπογράφοντα δεν εγγυάται την αντιστοίχηση αυτής της κλείδας με το πρόσωπο του υπογράφοντα στον οποίο και ανήκει. Γι΄ αυτό το σκοπό εκδίδονται τα πιστοποιητικά από τον πάροχο για να δηλώσουν την επιβεβαίωση ταύτισης των δημόσιων κλειδιών και του συγκεκριμένου προσώπου που υπογράφει. Η λειτουργία λοιπόν των παρόχων αναδεικνύει τη συμβολή τους στην επισφράγιση προσώπων -υπογραφών, διαδικασία αναγκαία για την ολοκλήρωση των ηλεκτρονικών υπογραφών (Αλεξανδρίδου, Το δίκαιο του ηλεκτρονικού εμπορίου, Σάκκουλας Αθήνα Θεσσαλονίκη 2004,σελ.44).

Η Παροχή Υπηρεσιών Πιστοποίησης ηλεκτρονικών υπογραφών δεν υπόκειται σε καθεστώς αδειοδότησης και άρα μπορεί οποιοσδήποτε (φυσικό ή νομικό πρόσωπο) να λειτουργήσει ως Πάροχος Υπηρεσιών Πιστοποίησης και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός Παρόχου Υπηρεσιών Πιστοποίησης προς την εποπτεύουσα αρχή (ΕΕΤΤ) είναι η" Δήλωση Έναρξης Λειτουργίας" και η εγγραφή του στο σχετικό "Μητρώο Παροχών Υπηρεσιών Πιστοποίησης", καθώς και η αποστολή "Ετήσιων Εκθέσεων" σχετικά με την λειτουργία τους.

Θέματα σχετικά με την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, τα αναγνωρισμένα πιστοποιητικά και την εποπτεία και τον έλεγχο των εγκατεστημένων στην

Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης (ΠΥΠ) οι οποίοι εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά ή παρέχουν άλλες σχετικές με την ηλεκτρονική υπογραφή υπηρεσίες πιστοποίησης ρυθμίζονται με το ΠΔ 150 " προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές" (ΦΕΚ 125/Α/25-6-01) και τον "Κανονισμό παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής" (Απ. ΕΕΤΤ 248/71 ΦΕΚ 603/Β/16-5-2002).

Η ΕΕΤΤ ασκεί την εποπτεία και τον έλεγχο όλων των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης (ΠΥΠ) ηλεκτρονικής υπογραφής.Η παροχή υπηρεσιών πιστοποίησης οποιασδήποτε μορφής είναι ελεύθερη και δεν υπόκειται σε προηγούμενη άδεια ή έγκριση ή άλλο μέτρο ισοδυνάμου αποτελέσματος. Κάθε Πάροχος Υπηρεσιών Πιστοποίησης δύναται να εκδίδει Αναγνωρισμένα Πιστοποιητικά αποκλειστικά και μόνον εφόσον συντρέχουν σωρευτικά οι κάτωθι προϋποθέσεις : α) πληροί του όρους του Παραρτήματος ΙΙ (απαιτήσεις για τους παρόχους που εκδίδουν αναγνωρισμένα πιστοποιητικά) του ΠΔ 150/2001, β) τηρεί κατά την έκδοση των εν λόγω πιστοποιητικών τους όρους του Παραρτήματος Ι (όροι για αναγνωρισμένα πιστοποιητικά) του ανωτέρω Προεδρικού Διατάγματος και γ) δηλώνει ότι συμμορφώνεται με τα παραρτήματα Ι και ΙΙ του ΠΔ 150/2001, σύμφωνα με το άρθρο 10, παράγρ. 3 του Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (Απόφαση ΕΕΤΤ 248/71). Στην περίπτωση αυτή πρόκειται για πάροχο υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά κατά δήλωσή του.

Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος εκδίδει Αναγνωρισμένα Πιστοποιητικά οφείλει ανά πάσα στιγμή να είναι σε θέση να αποδείξει ότι, κατά την έκδοση των Αναγνωρισμένων Πιστοποιητικών, συμμορφώνεται πλήρως με τα Παραρτήματα Ι και ΙΙ του ΠΔ 150/2001.Η ΕΕΤΤ τηρεί μητρώο των εγκατεστημένων στην Ελλάδα ΠΥΠ. Κατά την έναρξη των εργασιών του, κάθε εγκατεστημένος στην Ελλάδα Πάροχος Υπηρεσιών Πιστοποίησης γνωστοποιεί εγγράφως στην ΕΕΤΤ στοιχεία σχετικά με τη νομική του μορφή, τις παρεχόμενες υπηρεσίες τα οποία καταχωρούνται στο Μητρώο.Ειδικότερα σε περίπτωση Παρόχων Υπηρεσιών Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά, μαζί με την γνωστοποίηση προσκομίζονται : α) δήλωση του Παρόχου Υπηρεσιών Πιστοποίησης ότι συμμορφώνεται προς τα Παραρτήματα Ι και ΙΙ του ΠΔ 150/2001, β) Δήλωση Πρακτικής του Παρόχου Υπηρεσιών Πιστοποίησης, γ) έγγραφα με τα οποία αποδεικνύει την οικονομική κάλυψη δ) πιστοποιητικά εκδοθέντα από τις αρμόδιες Δημόσιες ή Δικαστικές Υπηρεσίες από τα οποία να προκύπτει αν τελεί υπό πτώχευση, πτωχευτικό συμβιβασμό, αναγκαστική διαχείριση ή αν έχουν κατατεθεί σχετικές προς αυτά αιτήσεις καθώς και αν τελεί υπό εκκαθάριση και τα οποία οφείλει να ανανεώνει και να υποβάλλει στην ΕΕΤΤ ανά τρεις (3) μήνες. Οι Πάροχοι Υπηρεσιών Πιστοποίησης υποχρεούνται να γνωστοποιούν στην ΕΕΤΤ κάθε τροποποίηση των στοιχείων τους που περιλαμβάνονται στο μητρώο. Οι Πάροχοι Υπηρεσιών Πιστοποίησης υποβάλλουν στην ΕΕΤΤ ετήσιες εκθέσεις με περιγραφή των δραστηριοτήτων τους. Ειδικότερα οι πάροχοι που εκδίδουν αναγνωρισμένα πιστοποιητικά περιλαμβάνουν στις εκθέσεις τους στοιχεία σχετικά με τις εγκαταστάσεις τους, χρησιμοποιούμενα προϊόντα, μέτρα ασφαλείας κ.λπ. τα οποία προβλέπονται στην ελληνική νομοθεσία. Οποτεδήποτε Πάροχος Υπηρεσιών Πιστοποίησης που εκδίδει Αναγνωρισμένα Πιστοποιητικά προβεί σε τυχόν ανάθεση σε τρίτον οποιουδήποτε μέρους της διαδικασίας έκδοσης πιστοποιητικών, υποχρεούται να το γνωστοποιήσει στην ΕΕΤΤ, περιγράφοντας το είδος της ανατεθείσης υπηρεσίας και την διάρκεια της ανάθεσης (http://www.eett.gr/).

Η ΕΕΤΤ, αυτεπαγγέλτως ή κατόπιν καταγγελίας, δύναται να προβαίνει σε έλεγχο της συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης με τις διατάξεις του ΠΔ 150/2001, του Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΑΠ. ΕΕΤΤ 248/71/15-3-2002) και εν γένει της ισχύουσας νομοθεσίας. Για την πραγματοποίηση του εν λόγω ελέγχου, η ΕΕΤΤ ή οριζόμενοι από την ΕΕΤΤ φορείς έχουν το δικαίωμα να ζητούν στοιχεία και να προβαίνουν σε επιθεωρήσεις στους χώρους εγκαταστάσεως και λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης, σύμφωνα με την κείμενη νομοθεσία, οι οποίοι υποχρεούνται να συνεργάζονται με την ΕΕΤΤ και να της παρέχουν κάθε πληροφορία και διευκόλυνση για την πραγματοποίηση των ελέγχων (http://www.eett.gr/).

7.11 Υποδομή Δημοσίου Κλειδιού(Public Key Infrastructure–PKI)

Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, υπογράφει, δημοσιεύει και υποστηρίζει τυποποιημένες ηλεκτρονικές βεβαιώσεις (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών του (υποκειμένων πιστοποίησης) ονομάζεται Υποδομή Δημοσίου Κλειδιού .

Μια υποδομή δημοσίου κλειδιού απαρτίζεται από:

- Αρχές πιστοποίησης: Πρόκειται για το Φορέα (έμπιστη τρίτη οντότητα) που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται, να ανακαλεί και να ανανεώνει πιστοποιητικά Όταν μια οντότητα αιτείται ενός πιστοποιητικού η αρχή πιστοποίησης συγκεντρώνει τα στοιχεία από την αρχή εγγραφής, δημιουργεί το πιστοποιητικό, το υπογράφει,το διανέμει στην οντότητα που το αιτήθηκε, προαιρετικά το δημοσιεύει, και είναι υπεύθυνη για τη διαχείριση του καθ' όλη τη διάρκεια της ζωής του.
- Αρχές εγγραφής(Registration Authority): Είναι υπεύθυνη για: τη συλλογή των στοιχείων μιας οντότητας που αιτείται ένα πιστοποιητικό την επαλήθευση της εγκυρότητας των,την παράδοση ενός πιστοποιητικού, τη διαχείριση αιτημάτων του κατόχου αναφορικά με τη διαχείρισητων πιστοποιητικών Η ΑΕ δε μπορεί να εκδώσει πιστοποιητικά.
- Εντεταλμένα Γραφεία : Φορέας στον οποίο έχουν ανατεθεί κάποια από τα καθήκοντα της Αρχής Εγγραφής Κυρίως η ταυτοποίηση και ο έλεγχος των στοιχείων των τελικών χρηστών καθώς και η εκκίνηση της διαδικασίας αίτησης.
- Πιστοποιητικά :Το πιστοποιητικό είναι ένα ηλεκτρονικό αντικείμενο που συσχετίζει ένα δημόσιο κλειδί (και επιπλέον και το αντίστοιχο ιδιωτικό του) με ορισμένες άλλες πληροφορίες, συνήθως πληροφορίες ταυτότητας ή περιγραφές αδειών. Ένα πιστοποιητικό υπογράφεται, βάση μίας υποδομής, από κάποια αρχή πιστοποίησης (certification authority- CA), η οποία βεβαιώνει με κάποιο τρόπο, τουλάχιστον θεωρητικά, την σύνδεση μεταξύ της ταυτότητας ή της άδειας και του ιδιοκτήτη του ιδιωτικού κλειδιού.
- Τελικούς Χρήστες :Το υποκείμενο για το οποίο έχει εκδοθεί ένα πιστοποιητικό ύστερα από αίτηση του. Ο Τελικός Χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο πιστοποιητικό.
- Τρίτους Συμμετέχοντες :Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος στις πληροφορίες οι οποίες περιέχονται σε ένα ψηφιακό πιστοποιητικό.
- Πολιτικές Πιστοποίησης: Πρόκειται για ένα σύνολο κανόνων αναφορικά με τη χρήση ενός πιστοποιητικού μέσα σε μια κοινωνία ή σύνολο εφαρμογών.
- Μηχανισμό ανάκλησης πιστοποιητικών :Κάθε πιστοποιητικό έχει τυπικά μια ημερομηνία λήξης. Υπάρχουν όμως περιπτώσεις που αυτό το πιστοποιητικό πρέπει να πάψει να είναι έγκυρο πριν την ημερομηνία λήξης του. Τέτοιοι λόγοι περιλαμβάνουν: Αποκάλυψη του αντίστοιχου ιδιωτικού κλειδιού ή υποψία αποκάλυψης. Αλλαγή των στοιχείων της οντότητας για την οποία εκδόθηκε το πιστοποιητικό Αλλαγή της ιδιότητας της οντότητας (προαγωγή, μετάθεση, απόσπαση ,κ.λ.π.) (http://www.eett.gr/).

7.12 Το πρόβλημα της πιστοποίησης

Η πιστοποίηση ηλεκτρονικών υπογραφών σύμφωνα με την κοινοτική νομοθεσία πηγάζει από την Οδηγία 1999/93/ΕΚ. Πολλές και διάσπαρτες είναι οι διατάξεις της εν λόγω Οδηγίας, στις οποίες γίνεται αναφορά στις υπηρεσίες των παρόχων υπηρεσιών πιστοποίησης. Τα πιστοποιητικά διακρίνονται σε δύο είδη στα απλά και στα αναγνωρισμένα. Τα πρώτα επιτελούν τη βασική λειτουργία επιβεβαίωσης της ταυτοπροσωπίας του υπογράφοντα. Η αναβαθμισμένη όμως μορφή των αναγνωρισμένων πιστοποιητικών εμπεριέχει επιπρόσθετα στοιχεία. Αυτά περιγράφονται στο Παράρτημα Ι της Οδηγίας 1999/93/ΕΚ και προσδίδουν τις απαραίτητες προϋποθέσεις δημιουργίας της προηγμένης ηλεκτρονικής υπογραφής. Ορίζεται (άρθρα 5 παρ. 1 και 3 παρ. 1 της Οδηγίας και του ΠΔ αντίστοιχα) 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». Κατά τον τρόπο αυτό η νέα ρύθμιση εξομοιώνει την ηλεκτρονική υπογραφή που πληροί σωρευτικά τις παραπάνω προϋποθέσεις με την ιδιόχειρη .Γενικά η πιστοποίηση συνοδεύει την ηλεκτρονική υπογραφή προσφέροντάς της επιπλέον εχέγγυα και αξιοπιστία στο απαιτητικό ηλεκτρονικό περιβάλλον. Εκτός όμως από αυτή τη λειτουργία της, η ηλεκτρονική πιστοποίηση επιτελεί και το ρόλο του συνδετικού κρίκου μεταξύ υπογραφής και υπογράφοντα.

1

ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΤΟΥ ΑΝΩΤΑΤΟΥ ΕΙΔΙΚΟΥ ΔΙΚΑΣΤΗΡΙΟΥ (Κατ' άρθρον 100 του Συντάγματος) Αρ. Φύλλου 1

8 Φεβρουαρίου 2010

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΠΟΦΑΣΕΙΣ

Άρση αποφατικής σύγκρουσης δικαιοδοσίας μεταξύ του Πολυμελούς Πρωτοδικείου Αθηνών και του Διοικητικού Εφετείου Αθηνών, τα οποία με τις αποφάσεις 6838/2005 και 2604/2008 αντιστοίχως έκριναν ότι στερούνται δικαιοδοσίας για τη διαφορά που ανέκυψε από σύμβαση συναφθείσα μεταξύ της αιτούσης εταιρείας και του Ελληνικού Δημοσίου..... 1

Άρση αποφατικής σύγκρουσης δικαιοδοσίας μεταξύ του Συμβουλίου της Επικρατείας και του

ΑΠΟΦΑΣΕΙΣ

(1)

Αριθμός 16/2009

Άρση αποφατικής σύγκρουσης δικαιοδοσίας μεταξύ του Πολυμελούς Πρωτοδικείου Αθηνών και του Διοικητικού Εφετείου Αθηνών, τα οποία με τις αποφάσεις 6838/2005 και 2604/2008 αντιστοίχως, έκριναν ότι στερούνται δικαιοδοσίας για τη διαφορά που ανέκυψε από σύμβαση συναφθείσα μεταξύ της αιτούσης εταιρείας και του Ελληνικού Δημοσίου.

Το Ανώτατο Ειδικό Δικαστήριο
(κατά το άρθρο 100 του Συντάγματος)

Εικόνα 6 Ψηφιακά υπογεγραμμένο ΦΕΚ.

Μία ακόμη λειτουργία των παρόχων είναι η χρονοσήμανση των ηλεκτρονικών υπογραφών. Το χορηγούμενο πιστοποιητικό επισημαίνει το χρόνο θέσης της ηλεκτρονικής υπογραφής, ενώ στο περιεχόμενό του βεβαιώνεται παράλληλα και η δικαιοπρακτική ικανότητα του υπογράφοντα (Παράρτημα I της Οδηγίας 1999/93).

8 ΝΟΜΟΘΕΣΙΑ

8.1 Οδηγία 1999/93 ΕΚ

Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ, Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 47 παράγραφος 2 και τα άρθρα 55 και 95, την πρόταση της Επιτροπής (1),τη γνώμη της Οικονομικής και Κοινωνικής Επιτροπής (2), της γνώμη της Επιτροπής των Περιφερειών (3), αποφασίζοντας σύμφωνα με τη διαδικασία του άρθρου 251 της συνθήκης(4),εκτιμώντας τα ακόλουθα:

Ηλεκτρονική κατάρτιση συμβάσεων

Ψηφιακές υπογραφές

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

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

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

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

(5) θα πρέπει να προαχθεί η διαλειτουργικότητα των προϊόντων ηλεκτρονικής υπογραφής· σύμφωνα με το άρθρο 14 της συνθήκης, η εσωτερική αγορά περιλαμβάνει ένα χώρο χωρίς εσωτερικά σύνορα μέσα στον οποίο εξασφαλίζεται η ελεύθερη κυκλοφορία των εμπορευμάτων πρέπει να ικανοποιηθούν βασικές απαιτήσεις που αναφέρονται σε προϊόντα ηλεκτρονικής υπογραφής για τη διασφάλιση της ελεύθερης κυκλοφορίας εντός της εσωτερικής αγοράς και για την οικοδόμηση εμπιστοσύνης στις ηλεκτρονικές υπογραφές, με την επιφύλαξη του κανονισμού (ΕΚ) αριθ. 3381/94 του Συμβουλίου, της 19ης Δεκεμβρίου 1994, περί κοινοτικού καθεστώτος ελέγχου της εξαγωγής αγαθών διπλής χρήσης 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, έρχονται όλο και συχνότερα αντιμέτωποι με αρχές κρατών μελών διαφορετικών εκείνου στο οποίο διαμένουν η ηλεκτρονική επικοινωνία θα μπορούσε να αποδειχθεί εξαιρετικά χρήσιμη από αυτή την άποψη·

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

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

(10) η εσωτερική αγορά επιτρέπει στους παρόχους υπηρεσιών πιστοποίησης την ανάπτυξη των διασυνοριακών δραστηριοτήτων τους αποβλέποντας στην αύξηση της ανταγωνιστικότητας τους, προσφέροντας έτσι στους καταναλωτές και τις επιχειρήσεις νέες ευκαιρίες ασφαλούς ανταλλαγής πληροφοριών και ηλεκτρονικών συναλλαγών, ανεξαρτήτως συνόρων για την τόνωση της παροχής υπηρεσιών πιστοποίησης μέσω ανοικτών δικτύων σε

κοινοτική κλίμακα, θα πρέπει οι πάροχοι υπηρεσιών πιστοποίησης να είναι ελεύθεροι να παρέχουν τις υπηρεσίες τους χωρίς προηγούμενη έγκριση· ως προηγούμενη έγκριση νοείται, όχι μόνο κάθε άδεια για την οποία απαιτείται απόφαση των εθνικών αρχών προτού επιτραπεί στον ενδιαφερόμενο να παρέχει υπηρεσίες πιστοποίησης, αλλά και κάθε άλλο μέτρο ισοδυνάμου αποτελέσματος

(11) οι μηχανισμοί εθελοντικής διαπίστευσης που αποσκοπούν σε βελτιωμένο επίπεδο παροχής υπηρεσιών ενδέχεται να προσφέρουν στους παρόχους υπηρεσιών πιστοποίησης το κατάλληλο πλαίσιο για την περαιτέρω ανάπτυξη των υπηρεσιών τους στα επίπεδα εμπιστοσύνης, ασφάλειας και ποιότητας που απαιτούνται από την εξελισσόμενη αγορά· αυτοί οι μηχανισμοί θα πρέπει να ενθαρρύνουν την ανάπτυξη βέλτιστης πρακτικής μεταξύ των παροχών 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 εξασφαλίσουν τον έλεγχο της τήρησης των διατάξεων της παρούσας οδηγίας· η παρούσα οδηγία δεν αποκλείει τη θέσπιση συστημάτων ελέγχου βασισμένων στονιδιωτικό τομέα· η παρούσα οδηγία δεν υποχρεώνει τους παρόχους υπηρεσιών πιστοποίησης να υπόκεινται σε έλεγχο δυνάμει τυχόν μηχανισμών περί διαπίστευσης

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

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

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

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

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

(19) οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται στο δημόσιο τομέα στο πλαίσιο εθνικών και κοινοτικών διοικητικών υπηρεσιών και για την επικοινωνία μεταξύ αυτών των υπηρεσιών και των πολιτών και οικονομικών φορέων, π.χ. για τις δημόσιες συμβάσεις, τη φορολογία, την κοινωνική ασφάλιση, την υγεία και την απονομή δικαιοσύνης

(20) η ύπαρξη εναρμονισμένων κριτηρίων όσον αφορά τις έννομες συνέπειες των ηλεκτρονικών υπογραφών θα διαφυλάξει 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 διάταξη δημιουργίας υπογραφής μπορούν να θεωρηθούν ως νομικά ισοδύναμες προς ιδιόχειρες υπογραφές μόνον εφόσον πληρούνται οι εν λόγω προϋποθέσεις για ιδιόχειρες υπογραφές

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

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

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

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

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

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

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

(28) σύμφωνα με τι αρχές της επικουρικότητας και της αναλογικότητας που αναφέρονται στο άρθρο 5 της συνθήκης, ο στόχος της δημιουργίας εναρμονισμένου νομοθετικού πλαισίου για την παροχή ηλεκτρονικών υπογραφών και συναφών υπηρεσιών δεν μπορεί να επιτευχθεί αποτελεσματικά από τα κράτη μέλη και, ως εκ τούτου, είναι δυνατόν, να

επιτευχθεί καλύτερα από την Κοινότητα· η παρούσα οδηγία δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου.

ΕΞΕΔΩΣΑΝ ΤΗΝ ΠΑΡΟΥΣΑ ΟΔΗΓΙΑ:

Άρθρο 1

Στόχος της παρούσας οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς.

Δεν καλύπτει πτυχές που αφορούν τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου και δεν θίγει κανόνες και περιορισμούς σχετικά με τη χρήση εγγράφων οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας οδηγίας νοούνται ως:

1. "ηλεκτρονική υπογραφή": δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.

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

α) συνδέεται μονοσήμαντα με τον υπογράφοντα.

β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα.

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

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

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

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

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

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

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

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

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

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

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

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

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

Άρθρο 3

Πρόσβαση στην αγορά

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

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

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

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

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

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

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

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

Άρθρο 4

Αρχές της εσωτερικής αγοράς

1. Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις που θεσπίζει κατ' εφαρμογήν της παρούσας οδηγίας για παρόχους υπηρεσιών πιστοποίησης εγκατεστημένους στην επικράτειά του, καθώς και για τις υπηρεσίες που αυτοί παρέχουν. Τα κράτη μέλη δεν μπορούν να

περιορίσουν την παροχή υπηρεσιών πιστοποίησης που προέρχονται από άλλο κράτος μέλος στους τομείς που καλύπτονται από την παρούσα οδηγία.

2. Τα κράτη μέλη διασφαλίζουν ότι τα προϊόντα ηλεκτρονικής υπογραφής που συμμορφούνται 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 κυι οι οποίες δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής:

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

β) γίνονται δεκτές ως αποδεικτικό στοιχείο σε νομικές διαδικασίες.

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

- είναι υπό μορφή ηλεκτρονικών δεδομένων, ή

- δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό, ή

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

- δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Άρθρο 6

Ευθύνη

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

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

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

γ) για τη διαβεβαίωση ότι τα δεδομένα δημιουργίας υπογραφής και τα δεδομένα επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, στις περιπτώσεις που αμφότερα προέρχονται από τον πάροχο υπηρεσιών πιστοποίησης, εκτός εάν ο πάροχος υπηρεσιών πιστοποίησης αποδείξει ότι δεν ενήργησε αμελώς.

2. Τα κράτη μέλη διασφαλίζουν τουλάχιστον ότι ο 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 πιστοποίησης δεν υπέχει ευθύνη για βλάβες που προκύπτουν από χρήση ενός αναγνωρισμένου πιστοποιητικού που υπερβαίνει τους περιορισμούς που αναγράφηκαν σε αυτό.

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

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

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

Άρθρο 7

Διεθνείς πτυχές

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

α) ο πάροχος υπηρεσιών πιστοποίησης πληροί τις απαιτήσεις που καθορίζονται στην παρούσα οδηγία και έχει 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 προερχόμενων από τρίτες χώρες, διατυπώνει προτάσεις για την επίτευξη αποτελεσματικής εφαρμογής προτύπων και διεθνών συμφωνιών που ισχύουν για υπηρεσίες πιστοποίησης. Ειδικότερα, όπου κρίνει απαραίτητο, υποβάλλει προτάσεις προς το Συμβούλιο για την έκδοση κατάλληλων εντολών διαπραγμάτευσης διμερών και πολυμερών συμφωνιών με τρίτες χώρες και διεθνείς οργανισμούς. Το Συμβούλιο αποφασίζει με ειδική πλειοψηφία.

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

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

Άρθρο 8

Προστασία δεδομένων

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

2. Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό δύναται να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν, ή με τη ρητή συγκατάθεσή του, και μόνον στο βαθμό που είναι απαραίτητο για τους σκοπούς έκδοσης και διατήρησης του πιστοποιητικού.

Δεν επιτρέπεται συλλογή ή επεξεργασία των δεδομένων για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου.

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

Άρθρο 9

Επιτροπή

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

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

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

3. Η επιτροπή θεσπίζει τον εσωτερικό κανονισμό της.

Άρθρο 10

Καθήκοντα της επιτροπής

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

Άρθρο 11

Κοινοποίηση

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

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

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

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

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

Άρθρο 12

Επανεξέταση

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

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

Άρθρο 13

Εφαρμογή

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

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

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

Άρθρο 14

Έναρξη ισχύος

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

Άρθρο 15

Αποδέκτες

Η παρούσα οδηγία απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 13 Δεκεμβρίου 1999.

ΠΑΡΑΡΤΗΜΑ I

Όροι ισχύοντες για αναγνωρισμένα πιστοποιητικά

Τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:

α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό·

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

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

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

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

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

ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού

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

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

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

ΠΑΡΑΡΤΗΜΑ II

Όροι ισχύοντες για παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά

Οι πάροχοι υπηρεσιών πιστοποίησης πρέπει:

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

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

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

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

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

κατάλληλες διοικητικές και διαχειριστικές διαδικασίες οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα·

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

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

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

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

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

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

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

- μόνον αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις,

- να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών,

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

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

ΠΑΡΑΡΤΗΜΑ III

Απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής

1. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον, ότι:

α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσίαν μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο·

β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας·

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

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

ΠΑΡΑΡΤΗΜΑ IV

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής

Ηλεκτρονική κατάρτιση συμβάσεων

Ψηφιακές υπογραφές

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

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

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

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

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

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

στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς, και

ζ) μπορούν να εντοπιστούν τροποποιήσεις απτόμενες της ασφάλειας.

8.2 ΠΔ 150/2001

Άρθρο 1

Σκοπός και Πεδίο Εφαρμογής

Με το παρόν Διάταγμα προσαρμόζεται η ελληνική νομοθεσία προς τις διατάξεις της Οδηγίας 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 «Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» (EEL 13/19.1.2000) στο εξής: Οδηγία.

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 ταυτότητα του. 10. «αναγνωρισμένο πιστοποιητικό»: πιστοποιητικό που πληροί τους όρους του Παραρτήματος I και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος πληροί τους οριζόμενους στο Παράρτημα II όρους. 11. «πάροχος υπηρεσιών πιστοποίησης»: φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές. 12. «προϊόν ηλεκτρονικής υπογραφής»: υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την προσφορά υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών. 13. «εθελοντική διαπίστευση»: κάθε άδεια διαπίστευσης των ηλεκτρονικών δεδομένων, στην οποία ορίζονται τα δικαιώματα και οι υποχρεώσεις, που διέπουν την παροχή υπηρεσιών πιστοποίησης και η οποία χορηγείται ύστερα από αίτηση του ενδιαφερόμενου παρόχου υπηρεσιών από τον φορέα που προβλέπεται στην παράγραφο 5 του άρθρου 4 του παρόντος.

Άρθρο 3

Έννομες συνέπειες των ηλεκτρονικών υπογραφών

1.Η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

2.Η ισχύς της ηλεκτρονικής υπογραφής ή τοπαραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο τον λόγο ότι δεν συντρέχουν οι προϋποθέσεις της προηγούμενης παραγράφου.

Άρθρο 4

Πρόσβαση στην αγορά - Αρχές της εσωτερικής αγοράς

1.Τα διατιθέμενα προϊόντα ηλεκτρονικής υπογραφής μπορεί να αφορούν ασφαλείς διατάξεις υπογραφής ή και μη ασφαλείς διατάξεις στον βαθμό που αυτό διατυπώνεται κατά τρόπο απόλυτα σαφή για οποιονδήποτε τρίτο με την επιφύλαξη του άρθρου 3 του παρόντος.

2.Η συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής προς το Παράρτημα III 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 II και στο Παράρτημα III 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 από οριζόμενους από αυτήν δημόσιους ή ιδιωτικούς φορείς, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου παρόχου υπηρεσιών πιστοποίησης, εθελοντική διαπίστευση. Με την εθελοντική διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον πάροχο υπηρεσιών πιστοποίησης. Οι προϋποθέσεις εθελοντικής

διαπίστευσης πρέπει να είναι αντικειμενικές, διαφανείς, ανάλογες με τον επιδιωκόμενο σκοπό και να μην οδηγούν σε διακρίσεις. Η ΕΕΤΤ δεν μπορεί να περιορίσει τον αριθμό των παροχών υπηρεσιών πιστοποίησης, που επιθυμούν τη διαπίστευση τους σύμφωνα με τις διατάξεις του παρόντος.

6.Οι διαπιστευμένοι ή μη, πάροχοι υπηρεσιών πιστοποίησης, που πληρούν τις προϋποθέσεις του Παραρτήματος ΙΙ του παρόντος, εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό.

7.Οι πάροχοι υπηρεσιών πιστοποίησης οφείλουν ιδιαίτερα να μεριμνούν για την από μέρους τους τήρηση των διατάξεων για την προστασία του ανταγωνισμού, για τον αθέμιτο ανταγωνισμό, για την πνευματική και βιομηχανική ιδιοκτησία και για την προστασία του καταναλωτή.

8.Η ΕΕΤΤ έχει την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παροχών υπηρεσιών πιστοποίησης, καθώς και των σύμφωνα με τις παραγράφους 5 και 2 του παρόντος φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το παράρτημα ΙΙΙ.

9.Σε περίπτωση που πάροχος υπηρεσιών πιστοποίησης ενεργεί ως διαπιστευμένος πάροχος υπηρεσιών πιστοποίησης, χωρίς να είναι, η 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 μέλος της Ευρωπαϊκής Ένωσης, συνεπάγονται τις ίδιες έννομες συνέπειες

με τις αντίστοιχες υπηρεσίες πιστοποίησης, που παρέχονται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος είναι εγκατεστημένος στην Ελλάδα.

3.Προϊόντα ηλεκτρονικής υπογραφής, τα οποία συνάδουν με την κείμενη νομοθεσία της Ευρωπαϊκής Ένωσης, συνεπάγονται τις ίδιες έννομες συνέπειες με τα αντίστοιχα προϊόντα ηλεκτρονικής υπογραφής, τα οποία προέρχονται από την Ελλάδα. Ιδιαίτερα, η διαπίστωση συμμόρφωσης προς την κείμενη νομοθεσία της Ευρωπαϊκής Ένωσης, που αφορά προϋποθέσεις για ασφαλείς διατάξεις δημιουργίας της υπογραφής από φορέα στον οποίο έχει ανατεθεί η διαπίστωση αυτή σύμφωνα με τη νομοθεσία κράτους μέλους της Ευρωπαϊκής Ένωσης, έχει άμεση ισχύ και στην Ελλάδα.

4.Τα αναγνωρισμένα πιστοποιητικά, που εκδίδονται στο κοινό από πάροχο υπηρεσιών πιστοποίησης, ο οποίος είναι εγκατεστημένος σε χώρα εκτός της Ευρωπαϊκής Ένωσης, είναι νομικώς ισοδύναμα με τα εκδιδόμενα από πάροχο υπηρεσιών πιστοποίησης εγκατεστημένο στην Ευρωπαϊκή Ένωση, εφόσον: α) ο πάροχος αυτός πληροί τους όρους του παρόντος Διατάγματος και έχει διαπιστευθεί εθελοντικώς σε κράτος - μέλος της Ευρωπαϊκής Ένωσης β) για το συγκεκριμένο πιστοποιητικό έχει εγγυηθεί πάροχος υπηρεσιών πιστοποίησης, που είναι εγκατεστημένος σε κράτος - μέλος και πληροί τους όρους του παρόντος Διατάγματος, γ) το αναγνωρισμένο πιστοποιητικό του παρόχου υπηρεσιών πιστοποίησης αναγνωρίζεται βάσει διμερούς ή πολυμερούς συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και τρίτων χωρών ή διεθνών οργανισμών.

Άρθρο 6

Ευθύνη των παροχών πιστοποίησης

1. Ο πάροχος υπηρεσιών πιστοποίησης, διαπιστευμένος ή μη, που εκδίδει αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυάται για την ακρίβεια τέτοιου πιστοποιητικού, ευθύνεται έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημία που προκλήθηκε σε βάρος

του επειδή το πρόσωπο αυτό εύλογα βασίσθηκε στο πιστοποιητικό, όσον αφορά: α) την ακρίβεια, κατά τη στιγμή της έκδοσης του, όλων των πληροφοριών που περιέχονται στο αναγνωρισμένο πιστοποιητικό, καθώς και την ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοση του. β) τη διαβεβαίωση ότι ο υπογράφων, η ταυτότητα του οποίου βεβαιώνεται στο αναγνωρισμένο πιστοποιητικό, κατά τη στιγμή της έκδοσης του,

κατείχε δεδομένα δημιουργίας υπογραφής, που αντιστοιχούσαν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό δεδομένα επαλήθευσης της υπογραφής, γ) τη διαβεβαίωση ότι αμφότερα τα δεδομένα δημιουργίας υπογραφής και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, εφόσον προέρχονται από πάροχο υπηρεσιών πιστοποίησης.

2.Ο πάροχος υπηρεσιών πιστοποίησης ευθύνεται επίσης, αν παραλείψει να καταγράψει την ανάκληση του πιστοποιητικού.

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

4.Στο αναγνωρισμένο πιστοποιητικό δύνανται να αναγράφονται, από τον πάροχο υπηρεσιών πιστοποίησης, περιορισμοί χρήσης αυτού, υπό την προϋπόθεση ότι οι περιορισμοί τίθενται κατά τρόπο, ο οποίος είναι αναγνωρίσιμος από οποιονδήποτε τρίτο. Σ' αυτή την περίπτωση ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για τη ζημία που προκύπτει από την υπέρβαση των αναφερόμενων περιορισμών κατά τη χρήση του αναγνωρισμένου πιστοποιητικού.

5.Στο αναγνωρισμένο πιστοποιητικό δύνανται να αναγράφονται, από τον πάροχο υπηρεσιών πιστοποίησης, όρια για το ύψος των συναλλαγών , για τις οποίες μπορεί να χρησιμοποιηθεί το σχετικό πιστοποιητικό, με την προϋπόθεση ότι τα όρια αυτά τίθενται κατά τρόπο αναγνωρίσιμο από οποιονδήποτε τρίτο. Στην περίπτωση αυτήν ο πάροχος υπηρεσιών πιστοποίησης δεν ευθύνεται για τη ζημία που προκαλείται από την υπέρβαση των ορίων αυτών.

6.Τα οριζόμενα στις διατάξεις των παραπάνω παραγράφων ισχύουν με την επιφύλαξη των διατάξεων του ν. 2251/1994 (Α' 191) όπως ισχύει για την προστασία καταναλωτών και ιδιαίτερα για τις καταχρηστικές ρήτρες των συμβάσεων, που συνάπτονται με καταναλωτές.

Άρθρο 7

Προστασία δεδομένων

1. Οι πάροχοι υπηρεσιών πιστοποίησης, η 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 ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

2.Ειδικότερα ο πάροχος των υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικό, δύναται να συγκεντρώνει δεδομένα προσωπικού χαρακτήρα για την έκδοση πιστοποιητικών μόνο απευθείας από το ενδιαφερόμενο πρόσωπο ή κατόπιν ρητής συγκατάθεσης του και μόνο στο βαθμό που είναι απαραίτητο για την έκδοση και διατήρηση του πιστοποιητικού. Η συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς απαγορεύεται, χωρίς τη συγκατάθεση του ενδιαφερόμενου προσώπου.

3.Επιτρέπεται στους παρόχους υπηρεσιών πιστοποίησης να αναγράφουν στο αναγνωρισμένο πιστοποιητικό ψευδώνυμο αντί του ονόματος του υπογράφοντος.

Άρθρο 8

Κοινοποίηση

1.Η Γενική Γραμματεία Επικοινωνιών του Υπουργείου Μεταφορών Επικοινωνιών ενημερώνει την Ευρωπαϊκή Επιτροπή το ταχύτερο δυνατόν για την εφαρμογή των διατάξεων του άρθρου 4 του παρόντος.

2.Η ΕΕΤΤ ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών παροχών 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 Ι, ΙΙ, ΙΙΙ και ΙV.

ΠΑΡΑΡΤΗΜΑ Ι.

Όροι ισχύοντες για αναγνωρισμένα πιστοποιητικά.

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

ΠΑΡΑΡΤΗΜΑ ΙΙ.

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 τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά, ζ) να λαμβάνουν μέτρα έναντι της πλαστογράφησης πιστοποιητικών και σε περίπτωση που ο πάροχος πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων, η) να διαθέτουν επαρκείς χρηματικούς πόρους ώστε να λειτουργούν σύμφωνα με τις απαιτήσεις που καθορίζονται στην οδηγία, ιδίως για την ανάληψη της ευθύνης ζημιών, θ) να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν ένα αναγνωρισμένο πιστοποιητικό για χρονικό διάστημα τριάντα (30) ετών, ιδίως για την παροχή αποδεικτικών στοιχείων πιστοποίησης σε νομικές διαδικασίες. Η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα, ι) να μην αποθηκεύουν ή αντιγράφουν δεδομένα δημιουργίας υπογραφής του ατόμου προς το οποίο ο πάροχος υπηρεσιών πιστοποίησης παρέσχε υπηρεσίες διαχείρισης κλειδιών, ια) πριν συνάψουν συμβατική σχέση με πρόσωπο που ζητεί πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, συμπεριλαμβανομένων ενδεχομένων περιορισμών της χρήσης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται

εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων, οι οποίοι βασίζονται στο πιστοποιητικό αυτό, ιβ) να χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση πιστοποιητικών σε επαληθεύσιμη μορφή, ούτως ώστε: - μόνο αρμόδιοι να μπορούν να διενεργούν εισαγωγές και τροποποιήσεις - να μπορεί να ελέγχεται η γνησιότητα των πληροφοριών, - να είναι δυνατή η κοινόχρηστη ανάκτηση πιστοποιητικών μόνον στις περιπτώσεις εκείνες για τις οποίες έχει δοθεί η συγκατάθεση του κατόχου και - οι τυχόν τεχνικές αλλαγές που θέτουν σε κίνδυνο τις εν λόγω απαιτήσεις ασφαλείας να γίνονται εμφανώς αντιληπτές από τον χειριστή.

ΠΑΡΑΡΤΗΜΑ III.

Διασφάλιση αξιοπιστίας της δημιουργίας υπογραφής.

1. Οι ασφαλείς διατάξεις δημιουργίας υπογραφής πρέπει, μέσω ενδεδειγμένων τεχνικών και διαδικαστικών μέσων, να διασφαλίζουν τουλάχιστον ότι: α) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ' ουσία, μόνο μία φορά και ότι το απόρρητο είναι διασφαλισμένο, β) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας, γ) τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.

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

ΠΑΡΑΡΤΗΜΑ IV.

Συστάσεις για την ασφαλή επαλήθευση της υπογραφής.

Κατά τη διαδικασία επαλήθευσης της υπογραφής θα πρέπει να διασφαλίζεται με εύλογη βεβαιότητα ότι: α) τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα, β) η υπογραφή επαληθεύεται με αξιοπιστία και ότι το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο, γ) ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται, δ) η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία, ε) το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζονται με τον ορθό τρόπο, στ) η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς και ζ) μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.

Άρθρο 10

Έναρξη ισχύος

Η ισχύς του παρόντος Διατάγματος αρχίζει από τη δημοσίευση του στην Εφημερίδα της Κυβερνήσεως. Στον Υπουργό Μεταφορών και Επικοινωνιών αναθέτουμε τη δημοσίευση και εκτέλεση του παρόντος Διατάγματος.

9 ΕΙΔΙΚΗ ΝΟΜΟΘΕΣΙΑ Οδηγία 1999/93/ΕΚ Π.Δ 150/2001

Οι λόγοι που ώθησαν το Ευρωπαϊκό Κοινοβούλιο στην υιοθέτηση της κοινοτικής οδηγίας σχετίζονται άμεσα με την ανάγκη θέσπισης ενιαίων κανόνων σχετικά με τις ηλεκτρονικές υπογραφές (Towards a European Framework for Digital And Encryption στην ηλεκτρονική διεύθυνση http://www.ispo.cec.be/eif/policy/97503.html,σελ.9).Συγκεκριμένα ενώ πολλά εμπορικά προϊόντα για τις ψηφιακές υπογραφές ήταν διαθέσιμα στην αγορά, ελάχιστες εταιρείες στην Ευρώπη ήταν πρόθυμες να προσφέρουν υπηρεσίες στον τομέα αυτό. Ένας από του κύριους λόγους γι' αυτό ήταν η έλλειψη ζήτησης λόγω της μη νομικής αναγνώρισης των ψηφιακών υπογραφών. Παράλληλα προβλήματα ανέκυπταν λόγω των διαφορετικών εθνικών

ρυθμίσεων ή της έλλειψης αυτών αναφορικά με τις προϋποθέσεις λειτουργίας των οργανισμών πιστοποίησης, την ύπαρξη τεχνικών και λειτουργικών απαιτήσεων για συγκεκριμένα είδη ηλεκτρονικών υπογραφών και την νομική αναγνώριση των ψηφιακών υπογραφών. Επίσης η νομική έννοια της υπογραφής και οι απαιτήσεις αναφορικά με τον τύπο και τη διαδικασία διαφοροποιούνται στις νομοθεσίες των διαφόρων Κρατών-μελών. Έτσι όταν κάποιος υπογράφει χρησιμοποιώντας ψηφιακή υπογραφή, έρχεται αντιμέτωπος με διάφορα ερωτήματα όπως, εάν έχει η δήλωση βούλησης νομική ισχύ, αν απαιτούνται από το νόμο κάποιες προϋποθέσεις, κ.λ.π. Αναφορικά με τις δηλώσεις βούλησης απαιτείται προσοχή διότι ο τρόπος χρησιμοποίησης τους στην ηλεκτρονική επικοινωνία διαφέρει σημαντικά από τον παραδοσιακό τρόπο έκφρασής τους. Έτσι όταν κανείς αποστέλλει ένα έγγραφο με τη χάρτινη μορφή του θα πρέπει να το τοποθετήσει σε ένα φάκελο, να κολλήσει γραμματόσημο και να το αποστείλει ταχυδρομικά έχοντας όμως πάντα χρόνο να ξανασκεφτεί την αποστολή του. Ένα ηλεκτρονικό έγγραφο όμως παραλαμβάνεται με το απλό πάτημα ενός πλήκτρου. Γι' αυτό σκόπιμο θα ήταν να τεθούν κάποιες προϋποθέσεις αναφορικά με το δεσμευτικό χαρακτήρα των ηλεκτρονικά διαβιβαζόμενων δηλώσεων βουλήσεως. Επιπρόσθετα αναγκαία είναι η ανεύρεση τεχνικών λύσεων, ώστε να καταστεί βέβαιο ότι δεν υπάρχουν ουσιώδεις διαφορές μεταξύ του εγγράφου που είναι ορατό στην οθόνη και του εγγράφου το οποίο στην πραγματικότητα υπογράφεται ηλεκτρονικά.

Ακόμη και όταν ένα ζεύγος κλείδας έχει αποδοθεί σε κλίμα απόλυτης εμπιστοσύνης σε ένα άτομο, κάτι τέτοιο δεν αποδεικνύει ότι το άτομο αυτό έχει απαραίτητα υπογράψει ένα δεδομένο έγγραφο. Αν ληφθεί μάλιστα υπόψη ότι το σύνηθες είναι να υπογράφει το έγγραφο μόνο ο κάτοχος της μυστικής κλείδας, τότε μια ψηφιακή υπογραφή μπορεί να συσχετιστεί με βεβαιότητα με τον κάτοχο της κλείδας αυτής. Η τυχόν παράδοση της κλείδας σε τρίτο πρόσωπο θα έθετε σε διακινδύνευση την παραπάνω υπόθεση. Έτσι σε αντίθεση με την παραδοσιακή υπογραφή, όπου ο υπογράφων υπογράφει με το ίδιο του το χέρι, οι ψηφιακές υπογραφές επιτρέπουν σε ένα τρίτο εξουσιοδοτημένο ή μη - πρόσωπο να υπογράψει το έγγραφο εάν το πρόσωπο αυτό έχει στην κατοχή του την ιδιωτική κλείδα. Περαιτέρω η εξασφάλιση ισοδύναμων εννόμων συνεπειών τόσο για τις παραδοσιακές ιδιόχειρες υπογραφές όσο και για τις ψηφιακές δεν είναι εύκολη υπόθεση αν αναλογιστεί κανείς τα διαφορετικά χαρακτηριστικά τους. Συγκεκριμένα σε αντίθεση με τις ιδιόχειρες υπογραφές δεν είναι δυνατόν στην περίπτωση των ψηφιακών υπογραφών να διακρίνει κανείς ανάμεσα στο πρωτότυπο και στο αντίγραφο. Επίσης κάθε άτομο έχει μια μοναδική ιδιόχειρη υπογραφή, ενώ στην περίπτωση της ψηφιακής υπογραφής ένα άτομο μπορεί να διαθέτει περισσότερα ζεύγη κλειδών.

Ωστόσο οι παραπάνω διαφορές σε καμία περίπτωση δεν εμποδίζουν τις ψηφιακές υπογραφές να απολαύουν ισοδύναμης νομικής αναγνώρισης για συγκεκριμένους νομικούς λόγους. Η αναγνώριση τους πρέπει να κινηθεί σε δύο άξονες. Κατά πρώτο λόγο αναγνώρισή της αποδεικτικής τους αξίας στις νόμιμες διαδικασίες (Σε ορισμένα νομικά συστήματα πχ. Βέλγιο, Γαλλία, Ελλάδα τα ηλεκτρονικά έγγραφα ακόμα και αν είχαν υπογραφεί με ψηφιακές υπογραφές δεν θα μπορούσαν να γίνουν αποδεκτά ως αποδεικτικά στοιχεία σε νόμιμες διαδικασίες διότι η έγγραφη απόδειξη είναι αναγκαία όταν για παράδειγμα η αξία του αντικειμένου μιας σύμβασης υπερβαίνει ένα συγκεκριμένο ποσό. Τέτοιοι περιορισμοί είναι εντελώς βλαπτικοί για τη χρήση των ψηφιακών υπογραφών, (Towards a European Framework, οπ. ,σελ. 10). Κατά δεύτερο λόγο αναγνώριση της ψηφιακής υπογραφής ως νομικά ισοδύναμης με την ιδιόχειρη. Η χρήση του έγγραφου τύπου μπορεί να εκπληρώνει ποικίλες λειτουργίες, όπως προειδοποίηση, απόδειξη ενός γεγονότος ή την αυθεντικότητα. Έγγραφα εξοπλισμένα με ψηφιακές υπογραφές μπορούν κάλλιστα να εκπληρώσουν αυτές τις λειτουργίες με την προϋπόθεση ότι οι ψηφιακές υπογραφές παρέχουν σιγουριά και αξιοπιστία. Τα κράτη- μέλη λοιπόν θα μπορούσαν να θέσουν ειδικούς κανόνες σχετικά με τον ηλεκτρονικό τύπο στο αστικό τους δίκαιο, χωρίς να είναι απαραίτητο να τροποποιήσουν όλους τους κανόνες που απαιτούν έγγραφο τύπο, αλλά να εισάγουν τις ψηφιακές υπογραφές μόνο όπου το θεωρούν απαραίτητο. Παράλληλα σε εκείνες τις μορφές συναλλαγών όπου δεν απαιτείται συγκεκριμένος τύπος και ο έγγραφος τύπος στηρίζεται σε εθελοντική πρακτική των μερών η νομική αναγνώριση των ψηφιακών υπογραφών θα ενίσχυε την ασφάλεια και την εμπιστοσύνη των συναλλαγών στην ταχύτατη αυτή μέθοδο υπογραφής.

Σκοπός λοιπόν της κοινοτικής οδηγίας ήταν η θέσπιση ενιαίων κανόνων για τη χρήση και τη νομική αναγνώριση των ηλεκτρονικών υπογραφών. Επιπλέον λειτούργησε ως προληπτικό μέτρο, αφού στόχος της ήταν να προλάβει κινήσεις διαφόρων κρατών της Ευρωπαϊκής Ένωσης

για επεξεργασία νομικού πλαισίου για τις ηλεκτρονικές υπογραφές. Ήδη στη Γερμανία (Informations- und Kommunikationsdieste -Gesetz(IuKDG), (BGB1), I καθώς και στην ηλεκτρονική διεύθυνση http://www.ukdg.de.) είχε ψηφιστεί από 22 Ιουλίου 1997 νόμος για τα Πολυμέσα, όπου το αρ. 3 αναφερόταν στις ψηφιακές υπογραφές. Επίσης στην Ιταλία (Περισσότερα για το ιταλικό δίκαιο βλ. σχετικά την ηλεκτρονική διευθύνση, www.aipa.it/english/law[s/pdecree51397.asp., επίσης A. Giussani, The Challenge of Information Society: Application of Advanced Technologiew in Civil Litigation and other Procedures. Italien Report, XI. World Congress on Procedural Law, Vienna 1999)είχε ψηφισθεί ο N. 59/1997 για τις ψηφιακές υπογραφές που θεωρούσε την κρυπτογράφηση ενός ηλεκτρονικού εγγράφου με τη χρήση μυστικής κλείδας ως ισοδύναμη με μια ιδιόχειρη υπογραφή (ηλεκτρονική διεύθυνση http://www.law.kuleuven.ac.be/icri.projects/tables.htm). Αξίζει τέλος να σημειωθεί ότι στην Ελλάδα ο νόμος 2672/1998 στο αρ. 14 § 1 στοιχ. ε επιτρέπει τη χρήση της ψηφιακής υπογραφής για τη διακίνηση εγγράφων με ηλεκτρονικά μέσα στις υπηρεσίες του Δημοσίου, των ΝΠΔΔ και των ΟΤΑ.

Αρνητικά, επίσης, αποτιμάται η χρήση μεγάλης ποικιλίας τεχνικών εννοιών όπως «απλή» και «προηγμένη ηλεκτρονική υπογραφή», «απλό» και «αναγνωρισμένο πιστοποιητικό», «διάταξη δημιουργίας υπογραφής» και «ασφαλής διάταξη δημιουργίας υπογραφής», «δεδομένα δημιουργίας υπογραφής» και «δεδομένα επαλήθευσης υπογραφής» (οδηγία 1999/93). Όλη αυτή η σύνθετη τεχνική ορολογία είναι πιθανό να δημιουργήσει ερμηνευτικά προβλήματα σε δικηγόρους, δικαστές, ΠΥΠ και καταναλωτές(Καραδημητρίου Κοσμάς, Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Σάκκουλας Αθήνα,2008, σελ.163).

Η Ελλάδα ενσωμάτωσε στο εθνικό της δίκαιο την οδηγία 1999/93 με το Π.Δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές».Η εν λόγω οδηγία αποτέλεσε το πρώτο χρονικά νομοθέτημα της Ε.Ε. σχετικό με το θέμα των διαδικτυακών συναλλαγών. Το κοινοτικό αυτό νομοθέτημα ασχολείται κυρίως με το θέμα της ηλεκτρονικής υπογραφής και με συναφή ζητήματα για την ολοκλήρωση του θεσμού της.

Ένα σημείο που πρέπει να τονιστεί ως προς το πεδίο εφαρμογής της εν λόγω νομοθεσίας είναι ότι η οδηγία 1999/93, άρα και το Π.Δ. 150/2001, εφαρμόζεται μόνο όταν οι υπηρεσίες πιστοποίησης ηλεκτρονικών υπογραφών παρέχονται προς το κοινό. Σύμφωνα με την αιτιολογική σκέψη 16 του προοιμίου της οδηγίας 1999/93, αυτή δεν εφαρμόζεται σε «κλειστά συστήματα», δηλαδή σε δίκτυα όπου η αναγνώριση του κύρους των ηλεκτρονικά υπογεγραμμένων δεδομένων βασίζεται σε «εθελούσιες συμφωνίες ιδιωτικού δικαίου μεταξύ συγκεκριμένου αριθμού συμμετεχόντων».

Στο κείμενό της (άρθρο 1) συνοψίζονται μια σειρά στοιχείων και προϋποθέσεων, τα οποία παραλληλίζουν τις ηλεκτρονικές υπογραφές με τις κλασικές. Εδώ επισημαίνουμε τη στενότητα αντίληψης και αντιμετώπισης της προβληματικής των ηλεκτρονικών υπογραφών. Το ζητούμενο δεν είναι το πόσο αντίστοιχα είναι τα δύο είδη υπογραφών ή πόσο ανάλογα είναι τα γενόμενα αποτελέσματά τους. Σε κάθε περίπτωση, δεν μπορούμε να περικλείσουμε το νέο είδος υπογραφών στο ήδη υπάρχον πλαίσιο. Ακόμη και αν με την Οδηγία του 1999 ο κοινοτικός νομοθέτης ήθελε να αποδώσει στις ηλεκτρονικές υπογραφές τα χαρακτηριστικά των κλασικών, η δυναμική χρήση του διαδικτύου επιβάλλει ταχεία αναμόρφωση των νομοθετικών κειμένων με πυρήνα τις εξελίξεις και όχι τα παλαιά πρότυπα. Εξάλλου, θα πρέπει να τονισθεί ότι η αναγνώριση των ηλεκτρονικών υπογραφών γίνεται στη βάση προτύπων, τα οποία μεταξύ τους διαφέρουν. Στο άρθρο 5 της Οδηγίας περικλείονται οι έννομες συνέπειες των ηλεκτρονικών υπογραφών, χωρίς όμως να λαμβάνεται υπόψη η μελλοντική τους αναβάθμιση, η οποία αναμένεται να προσδώσει στις ηλεκτρονικές υπογραφές νέα δυναμική και να ξεπεράσει το σημερινό καθεστώς των παραδοσιακών υπογραφών, όπως αυτές ισχύουν σήμερα.

Η τεχνολογική ουδετερότητα είναι ένα ακόμη στοιχείο, το οποίο εντοπίζεται στην Οδηγία. Είναι χαρακτηριστικό ότι ο κοινοτικός νομοθέτης αποφεύγει αναφορές σε συγκεκριμένη τεχνολογία, λαμβάνοντας υπόψη τους ρυθμούς εξέλιξης που μεταβάλλουν την ηλεκτρονική τεχνολογία και το διαδίκτυο (Καραδημητρίου,ο.π,σελ1541). Ιδιαίτερο ενδιαφέρον παρουσιάζει το άρθρο 2 § 2 του Π.Δ. 150/2001, το οποίο ορίζει την προηγμένη ηλεκτρονική υπογραφή

αποκλίνοντας σημαντικά από τον ορισμό της οδηγίας 1999/93. Σύμφωνα με τη διάταξη αυτή, «προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή» είναι η ηλεκτρονική υπογραφή που πληροί τους εξής όρους:

α) Συνδέεται μονοσήμαντα με τον υπογράφοντα. Ο όρος «μονοσήμαντα» έχει την έννοια ότι η κατοχή και η χρήση του ιδιωτικού κλειδιού της ηλεκτρονικής υπογραφής ανήκει σε ένα συγκεκριμένο πρόσωπο.

β) Είναι ικανή να ταυτοποιήσει τον υπογράφοντα. Ταυτοποίηση είναι η δυνατότητα να διαπιστώνεται ότι το ηλεκτρονικό μήνυμα που φέρει την προηγμένη ηλεκτρονική υπογραφή προήλθε πραγματικά από τον φερόμενο ως αποστολέα του.

γ) Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο. Ο υπογράφων πρέπει, με άλλα λόγια, να ελέγχει απόλυτα το ιδιωτικό κλειδί με το οποίο δημιουργεί την υπογραφή του και να αποκλείει τυχόν παρέμβαση από τρίτα πρόσωπα. Για το σκοπό αυτό, συνήθως το ιδιωτικό κλειδί αποθηκεύεται σε μια «έξυπνη κάρτα».

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

Αντίθετα, η οδηγία 1999/93 στο άρθρο 2 αριθ. 2, παρά το γεγονός ότι αναφέρει τους ίδιους ακριβώς τέσσερις όρους που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή, δεν χρησιμοποιεί την ορολογία «ψηφιακή υπογραφή» διαζευκτικά με την ορολογία «προηγμένη ηλεκτρονική υπογραφή». Στην ουσία, δηλαδή, ο Έλληνας νομοθέτης περιορίζει την έννοια της προηγμένης ηλεκτρονικής υπογραφής και την ταυτίζει με την ψηφιακή υπογραφή, θεωρώντας, λανθασμένα, ότι μόνο η ψηφιακή υπογραφή (η οποία, όπως έχει προαναφερθεί, βασίζεται αποκλειστικά στην ασύμμετρη κρυπτογραφία) πληροί τα τέσσερα κριτήρια της προηγμένης ηλεκτρονικής υπογραφής(Καραδημητρίου Κοσμάς, Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Σάκκουλας Αθήνα 2008, σελ.100).

Ο νομοθέτης παρέχει νομική ισχύ σε όλες τις ηλεκτρονικές υπογραφές που δεν πληρούν τις τεχνικές προϋποθέσεις του άρθρου 3 § 1, ωστόσο δεν τις αναγνωρίζει ως ισότιμες με τις ιδιόχειρες υπογραφές. Σύμφωνα με το άρθρο 3 § 2 του Π.Δ. 150/2001, η ισχύς μιας ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο το λόγο ότι η ηλεκτρονική υπογραφή:

α) δεν βασίζεται σε αναγνωρισμένο πιστοποιητικό που εκδίδεται από ΠΥΠ,

ή

β) δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

Τούτο σημαίνει ουσιαστικά ότι η νομική τύχη μιας τέτοιας υπογραφής θα κριθεί με βάση το ισχύον ελληνικό ουσιαστικό και δικονομικό δίκαιο (ΑΚ και ΚΠολΔ). Οι ΠΥΠ είναι ελεύθεροι να προσφέρουν υπηρεσίες πιστοποίησης χωρίς να προϋποτίθεται χορήγηση κρατικής άδειας. Κατά συνέπεια, τις υπηρεσίες αυτές μπορεί να τις προσφέρει οποιοδήποτε φυσικό ή νομικό πρόσωπο, εφόσον τηρεί τις διατάξεις για την προστασία του ανταγωνισμού, για τον αθέμιτο ανταγωνισμό, για την πνευματική και βιομηχανική ιδιοκτησία και για την προστασία του καταναλωτή.

Είναι φανερό ότι στόχος του Π.Δ. 150/2001 και της οδηγίας 1999/93 είναι να καταστήσουν ευέλικτη την αγορά και να προαγάγουν τη χρήση της ηλεκτρονικής υπογραφής ως μέσου ασφάλειας των συναλλαγών, χωρίς την τροχοπέδη της κρατικής γραφειοκρατίας. Πράγματι, η χρονοβόρα διαδικασία της χορήγησης κρατικής άδειας θα αποτελούσε ανασταλτικό παράγοντα για την επιχειρηματική δραστηριότητα αρκετών ΠΥΠ. Στο άρθρο 6 του πδ 150/2001 ρυθμίζεται η ευθύνη του παρόχου υπηρεσιών πιστοποίησης. Ο πάροχος υπηρεσιών πιστοποίησης, εφόσον εκδίδει αναγνωρισμένο πιστοποιητικό στο κοινό ή εγγυάται για την ακρίβεια ενός τέτοιου πιστοποιητικού, ευθύνεται έναντι οποιουδήποτε προσώπου για κάθε ζημία που ενδεχομένως προκληθεί σε βάρος του, επειδή το πρόσωπο αυτό βασίστηκε στο πιστοποιητικό όσον αφορά:

α) στην ακρίβεια των πληροφοριών κατά τον χρόνο έκδοσης του,

β) στη διαβεβαίωση ότι ο υπογράφων κατά τη στιγμή έκδοσης του πιστοποιητικού κατείχε δεδομένα δημιουργίας υπογραφής, τα οποία αντιστοιχούσαν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό ως δεδομένα επαλήθευσης της υπογραφής, και

γ) στη διαβεβαίωση ότι αμφότερα τα δεδομένα δημιουργίας υπογραφής και επαλήθευσης υπογραφής μπορούν να χρησιμοποιηθούν συμπληρωματικά, εφόσον προέρχονται από πάροχο υπηρεσιών πιστοποίησης (άρθρο 6 παρ. 1 πδ 150/2001).

Η ευθύνη του παρόχου υπηρεσιών πιστοποίησης καταλαμβάνει και την παράλειψη καταγραφής της ανάκλησης του πιστοποιητικού (άρθρο 6 παρ. 2 πδ 150/2001). Σε όλες τις προαναφερθείσες περιπτώσεις ο πάροχος δεν ευθύνεται, αν αποδείξει ότι δεν τον βαρύνει πταίσμα (άρθρο 6, παρ. 3 πδ 150/2001).(Αριστέα Σινανιώτη-Μαρούδη, Ιωάννης Δ. Φαρσαρώτας, ο.π,107)

Ο ρόλος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων στον έλεγχο των Παροχών Υπηρεσιών Πιστοποίησης είναι:

α) η παροχή εθελοντικής διαπίστευσης ή η ανάθεση της σε δημόσιους ή ιδιωτικούς φορείς, βάσει του άρθρου 4 § 5 εδ. α' του Π.Δ. 150/2001,

β) η διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής προς το Παράρτημα ΙΙΙ του Π.Δ. 150/2001

γ) η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα ΠΥΠ

Πέρα από τα παραπάνω, η ΕΕΤΤ είναι αρμόδια να επιβάλλει πρόστιμο σε ΠΥΠ που ενεργούν ως διαπιστευμένοι, ενώ δεν είναι, και να ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων στην Ελλάδα ΠΥΠ.

Οσον αφορά τα πιστοποιητικά που εκδίδονται από τους πάροχους υπηρεσιών πιστοποίησης στο κείμενο της Οδηγίας (άρθρο 2 στ. 9) ορίζονται ως «ηλεκτρονικές βεβαιώσεις», στοιχείο θετικό για την ολοκλήρωση της διαδικασίας με πλήρη ηλεκτρονική μορφή. Έτσι, ο αποδέκτης θα λαμβάνει τα πιστοποιητικά με ταχύτητα, ασφάλεια και με το ίδιο modus παραγωγής της ηλεκτρονικής υπογραφής.

Στο θέμα της ευθύνης που έχει ο πάροχος υπηρεσιών πιστοποίησης κατά το άρθρο 6 της Οδηγίας, ειδικά στις παραγράφους 3 και 4, διαβλέπουμε ότι το πιστοποιητικό περιλαμβάνει μια σειρά περιοριστικών στοιχείων. Οι περιορισμοί αυτοί ως γενικές αρχές προστατεύουν τους ηλεκτρονικά συναλλασσόμενους, όμως ταυτόχρονα καταδεικνύουν την αδυναμία των παρόχων να εγγυηθούν σε απόλυτο βαθμό για τη χρήση τους και το ύψος των διενεργούμενων συναλλαγών. Το άρθρο 8 της Οδηγίας στην παρ. 3 εισάγει τη νόμιμη χρήση ψευδωνύμων στα εκδιδόμενα από τους πάροχους υπηρεσιών πιστοποίησης πιστοποιητικά. Τα ψευδώνυμα αποτελούν ανασφαλή δεδομένα και η νομιμοποίησή τους στην ευαίσθητη διαδικασία της πιστοποίησης προκαλεί εμπόδιο στη διαφάνεια των ηλεκτρονικών επικοινωνιών και ανασφάλεια στις ηλεκτρονικές συναλλαγές. Η ελευθερία έκφρασης ως προς την επιλογή ψευδωνύμων θα έπρεπε να παρακαμφθεί, ώστε να ενισχυθεί η πιστότητα των συναλλασσομένων του διαδικτύου (Σπυρόπουλος, ο.π, σελ. 374).

Τέλος, ο κοινοτικός νομοθέτης περιλαμβάνει στο άρθρο 12 της Οδηγίας την υποχρέωση της Επιτροπής να συντάξει και να υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο σχετική έκθεση εφαρμογής και λειτουργίας της Οδηγίας πριν την 19η Ιουλίου 2003. Η αποτίμηση από την εφαρμογή της Οδηγίας σκοπό έχει την αξιολόγησή της στην πράξη και την πρόταση τυχόν τροποποιήσεων σε συνάρτηση με τις ραγδαίες καινοτομίες που συντελούνται στο πεδίο του ηλεκτρονικού εμπορίου.

Εξίσου σπουδαίο είναι το θέμα της χρονοσήμανσης, δεδομένου ότι η ημερομηνία και ώρα της ηλεκτρονικά διαβιβαζόμενης δήλωσης βουλήσεως έχει σημασία ιδιαίτερα όσον αφορά στη σύναψη της συμβάσεως και των δεσμευτικών αποτελεσμάτων της. Καθώς είναι τεχνικά δυνατή η τροποποίηση της ημερομηνίας του ηλεκτρονικού υπολογιστή η χρονοσήμανση αποτελεί ζήτημα κεφαλαιώδους σημασίας για τις συναλλαγές στο ηλεκτρονικό εμπόριο, διότι η ημερομηνία και ώρα υπογραφής της ηλεκτρονικά διαβιβαζόμενης δήλωσης αποδοχής της πρότασης για σύμβαση, καθώς επίσης και η ημερομηνία και ώρα αποστολής και λήψης της, καθορίζουν το χρόνο σύναψης της σύμβασης και το χρόνο επέλευσης των δεσμευτικών αποτελεσμάτων της, ώστε να εξασφαλίζεται η έλλειψη δυνατότητας από τα συμβαλλόμενα

μέρη της αποποίησης της ευθύνης τους (non - repudiation). Επιπλέον, η τεχνική δυνατότητα που υπάρχει για να τροποποιηθεί ανά πάσα στιγμή η ημερομηνία και η ώρα του Η/Υ ή του κινητού τηλεφώνου ή άλλης συσκευής που χρησιμοποιείται στο ηλεκτρονικό εμπόριο, καθιστά απαραίτητη στις συναλλαγές τη χρονοσήμανση της προηγμένης ηλεκτρονικής υπογραφής από έναν αξιόπιστο τρίτο, δηλαδή, στην προκειμένη περίπτωση, από τον ΠΥΠ. Και πέρα όμως απ'αυτά, όπως ήδη έχει επισημανθεί, η αρχή της ανυπαρξίας δυνατότητας αποποίησης της ευθύνης των συμβαλλομένων μερών αποτελεί βασικό στοιχείο μιας ασφαλούς ηλεκτρονικής συναλλαγής. Για όλους τους ανωτέρω λόγους, η προσθήκη της δυνατότητας χρονοσήμανσης στους όρους, τους οποίους πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή, θα συμβάλει αποφασιστικά στην ενδυνάμωση του αισθήματος της ασφάλειας στις ηλεκτρονικές συναλλαγές. (Καραδημητρίου Κοσμάς, Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Σάκκουλας Αθήνα,2008, σελ.165).

10 ΝΟΜΟΛΟΓΙΑ

10.1 Επισκόπηση Νομολογίας

Α.Π. 2/2000

Στην έννοια του εγγράφου περιλαμβάνεται τόσο το τελεμοιότυπο, όσο και το φωτοτυπικό αντίγραφο εγγράφου. Για την αποδεικτική ισχύ του φωτοτυπικού αντιγράφου στο ποινικό δίκαιο δεν απαιτείται η κατά το άρθρο 449 παρ.2 ΚΠολΔ βεβαίωση της ακρίβειάς του από αρμόδιο κατά νόμο πρόσωπο. Στην έννοια του εγγράφου περιλαμβάνεται τόσο το τελεμοιότυπο, όσο και το φωτοτυπικό αντίγραφο εγγράφου που παρότι δεν είναι πρωτότυπα είναι δυνατόν να καταστούν υλικά αντικείμενα πλαστογραφίας. Η δημιουργία εγγράφου με την μέθοδο της φωτοτυπίας και η αλλοίωση κατά την φωτοτύπηση στοιχείων του γνησίου συνιστά κατάρτιση νέου πλαστού εγγράφου, ενώ η χρήση ανεπικύρωτων φωτοτυπικών αντιγράφων εγγράφου, που έχει νοθευτεί συνιστά ειδική μορφή χρήσεως πλαστού. Για την αποδεικτική ισχύ του φωτοτυπικού αντιγράφου στο ποινικό δίκαιο δεν απαιτείται η κατά το άρθρο 449 παρ.2 ΚΠολΔ βεβαίωση της ακρίβειάς του από αρμόδιο κατά νόμο πρόσωπο. Πότε υπάρχει εσφαλμένη ερμηνεία και πότε εσφαλμένη εφαρμογή ουσιαστικής ποινικής διατάξεως. Πότε υπάρχει έλλειψη νομίμου βάσεως. Αναιρείται λόγω ελλείψεως αιτιολογίας και εσφαλμένης ερμηνείας και εφαρμογής ουσιαστικής ποινικής διατάξεως το προσβαλλόμενο βούλευμα με το οποίο κρίθηκε ότι δεν πρέπει να γίνει κατηγορία για πλαστογραφία και για απόπειρα απάτης επι δικαστηρίω κατά του κατηγορουμένου που προσκόμισε στο δικαστήριο ανεπικύρωτα και αχαρτοσήμαντα φωτοαντίγραφα των φερομένων ως πλαστών τελεμοιοτύπων, με τα οποία φέρεται ότι προσπάθησε να παραπλανήσει τους δικαστές ως προς την αλήθεια των ισχυρισμών του , διότι α) δεν προκύπτει αν το Συμβούλιο απεφάνθη να μη γίνει κατηγορία για νόθευση και χρήση των πρωτοτύπων ή των φωτοαντιγράφων τους και 2)το Συμβούλιο ερμήνευσε εσφαλμένα τις διατάξεις των άρθρων 13 γ και 216 ΠΚ, κρίνοντας ότι τα ανεπικύρωτα και αχαρτοσήμαντα φωτοτυπικά αντίγραφα δεν είναι έγγραφα με αποδεικτική δύναμη, υποκείμενα σε πλαστογραφία και ότι περαιτέρω δεν μπορούσαν να ληφθούν υπόψη κατά την τακτική διαδικασία ούτε για τη συναγωγή δικαστικών τεκμηρίων, μη στοιχειοθετούμενης συνεπώς ούτε απόπειρας απάτης (Ολομ.ΑΠ 2/2000, Ποιν.Χρον., Ν.120).

Η απόφαση σταθμός έκρινε ότι συμπεριλαμβάνονται στην ευρεία έννοια των εγγράφων το τηλετύπημα (fax) και το φωτοτυπικό αντίγραφο εγγράφου. Η εφαρμογή της διάταξης του άρθρου 13 εδ. γ΄ ΠΚ ενσωματώνει μια σειρά τεχνολογικών καινοτομιών στην οποία εκτός των άλλων εντάσσονται και τα προαναφερόμενα είδη εγγράφων. Ο νομοθέτης στην τροποποίηση του άρθρου 13 ΠΚ έλαβε υπόψη του νέες τεχνικές από τις οποίες προκύπτουν μια σειρά εγγράφων .Οι κοινωνικές συνθήκες και η διείσδυση νέων τεχνολογιών δημιούργησαν τις ώριμες συνθήκες για την αναγκαία διεύρυνση του όρου «έγγραφο». Από τη νομοθετική προσαρμογή διαφαίνεται η τάση κάλυψης σύγχρονων πρακτικών ώστε να επιτυγχάνεται συγχρονισμός κλασικών όρων του δικαίου και της αναδυόμενης τεχνολογίας. Αναφορικά με τη χρήση του fax, το αποστελλόμενο έγγραφο επεξεργάζεται και με τη συνδρομή των τηλεφωνικών υποδομών λαμβάνεται από τη συσκευή τηλεομοιοτυπίας του παραλήπτη. Κατά την ενδιάμεση διαδικασία της αποστολής αυτό μετατρέπεται από αναγνώσιμο έγγραφο σε μια αλληλουχία δεδομένων τα οποία ανασυντάσσονται σε αναγνώσιμο έγγραφο και υψηλή ακρίβεια αναπαραγωγής στη συσκευή λήψης.

ΜΠρΑθ. 1963/2004

Κατά την αποστολή ενός μηνύματος μέσω ηλεκτρονικού ταχυδρομείου, η δήλωση βουλήσεως του αποστολέα ταυτίζεται με την ηλεκτρονική του διεύθυνση, αποτελεί ένα ενιαίο σύνολο, ώστε να καταστεί δυνατή τεχνικά η παραλαβή της από τον παραλήπτη και είναι ήσσονος σημασίας η μορφή ή η διάταξη με την οποία απεικονίζεται μηχανικά στο έντυπο. Ο καθορισμός συνεπώς της ηλεκτρονικής διεύθυνσης κατά τρόπο μοναδικό από τον ίδιο το χρήστη και η δήλωση της σε κάθε αποστελλόμενο ηλεκτρονικό μήνυμα συνιστά απόδειξη της ταυτότητας του εκδότη του και κατ' αναλογίαν με τα οριζόμενα για το παραδοσιακό έγγραφο του αρ. 443 ΚΠολΔ, η

μηχανική του απεικόνιση του σε έντυπο εμπίπτει στην έννοια του ιδιωτικού εγγράφου, με αποδεικτική δύναμη εις βάρος του εκδότη του, διότι αυτή ακριβώς η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση, που έχει ορισθεί και εφαρμοστεί από τον ίδιο τον αποστολέα, έχει τον χαρακτήρα της ιδιόχειρης υπογραφής, έστω και αν δεν έχει την παραδοσιακή μορφή της τελευταίας. Τα ανωτέρω ισχύουν ανεξαρτήτως της θέσεως στην οποία εμφανίζεται η ηλεκτρονική διεύθυνση του αποστολέα σε σχέση με το κείμενο, το οποίο συνοδεύει, κατά την εμφάνισή του στην οθόνη του υπολογιστή, ή τη μηχανική του απεικόνιση σε χαρτί. Έτσι το επικυρωμένο κατά το νόμο αντίγραφο του αποσταλέντος ηλεκτρονικού μηνύματος, το οποίο περιέχεται στο σκληρό δίσκο του παραλήπτη αποτελεί πλήρη απόδειξη ότι η περιλαμβανόμενη σε αυτό δήλωση προέρχεται από τον εκδότη - αποστολέα του. Η λειτουργία του συστήματος κατά τα ανωτέρω εκτιθέμενα, είναι δυνατόν να υποκρύπτει τον κίνδυνο ότι η αποστολή του συγκεκριμένου μηνύματος έγινε από άλλο πρόσωπο από αυτό στο οποίο ανήκει η συγκεκριμένη ηλεκτρονική διεύθυνση, κάνοντας χρήση αυτής (με οποιαδήποτε τρόπο) χωρίς την έγκρισή του. Η ελαττωματικότητα αυτή του μηνύματος που εστάλη ευθέως παραπέμπει στις διατάξεις περί πλαστότητας του ΚΠολΔ, εγκαθιστώντας αναστροφή του βάρους αποδείξεως στον επικαλούμενο αυτήν, για τον λόγο ότι η λειτουργία του συστήματος του ηλεκτρονικού ταχυδρομείου παρέχει εγγυήσεις για την πιστότητά της και η οποιαδήποτε παθολογία εμφανίζεται δεν προέρχεται από ελάττωμα του συστήματος, αλλά από επέμβαση τρίτου σε αυτό, γεγονός το οποίο ανήκει στη σφαίρα επιρροής του φερόμενου ως αποστολέα. (http://www.dsanet.gr/Epikairothta/Nomologia/mpa1963_04.htm).

Η συγκεκριμένη απόφαση ασχολείται με το θέμα των ηλεκτρονικών εγγράφων, ιδίως του ηλεκτρονικού μηνύματος αλληλογραφίας. Δυστυχώς δεν έχει ληφθεί υπόψη η νομοθεσία περί ηλεκτρονικών υπογραφών, όπως αυτή είχε νωρίτερα τεθεί σε ισχύ με το Π.Δ. 150/2001. Εδώ θα παρουσιαστεί η απόφαση, με έμφαση στο ζήτημα του τύπου του ηλεκτρονικού εγγράφου, υπό το πρίσμα του σύγχρονου πλέον νομοθετικού πλαισίου.

Ήδη στο σκεπτικό της απόφασης δίνεται ορισμός του ηλεκτρονικού εγγράφου: «ως ηλεκτρονικό έγγραφο θεωρείται το σύνολο των έγγραφων δεδομένων στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή, τα οποία αφού γίνουν αντικείμενο επεξεργασίας από την κεντρική μονάδα επεξεργασίας, αποτυπώνονται με βάση τις εντολές του προγράμματος, κατά τρόπο αναγνώσιμο από τον άνθρωπο, είτε στην οθόνη του μηχανήματος, είτε στον προσαρμοσμένο εκτυπωτή του». Από τον περιγραφικό αυτό ορισμό συνάγεται η κρίσιμη συμβολή της τεχνολογίας στη δημιουργία του ηλεκτρονικού εγγράφου και στην υπόστασή του. Σε συνδυασμό όμως και με τη μη ύπαρξη νομοθετικού ορισμού για τα έγγραφα, θα πρέπει να τονισθεί ότι η αξία τους ουσιαστική και δικονομική εξαρτάται από την υπογραφή που τα συνοδεύει.

Ο κεντρικός ρόλος της υπογραφής επί του εγγράφου το ρυθμίζει και το διαβαθμίζει περαιτέρω. Εκ πρώτης κατά το Π.Δ. το ηλεκτρονικό έγγραφο το οποίο φέρει την προηγμένη ηλεκτρονική υπογραφή επέχει θέσης ιδιωτικού εγγράφου, αυτό διότι η υπογραφή του το συνδέει άμεσα και αποκλειστικά με τον εκδότη του, και πιστοποιεί το αναλλοίωτο του περιεχομένου του.

Σε αυτό το νομοθετικό πλαίσιο λοιπόν το μήνυμα ηλεκτρονικού ταχυδρομείου δεν έχει υπόσταση ιδιωτικού εγγράφου, ακριβώς λόγω έλλειψης της προηγμένης ηλεκτρονικής υπογραφής. Η οποιαδήποτε σκέψη περί αντιστοιχίας ηλεκτρονικής διεύθυνσης αλληλογραφίας και προηγμένης ηλεκτρονικής υπογραφής αποκλείεται ρητά. Όμως, αποκλείεται παράλληλα και η έννοια της απλής ηλεκτρονικής υπογραφής για τα e-mail. Αυτό συμβαίνει γιατί και σε αυτή την περίπτωση δεν συναντάμε τα χαρακτηριστικά της υπογραφής του άρθρου 2 στοιχείο 1 Π.Δ. 150/2001. Επομένως, το έγγραφο της υπό κρίση απόφασης εξομοιώνεται με το ανυπόγραφο χάρτινο ιδιωτικό έγγραφο. Η περιεχόμενη δήλωση βουλήσεως στο ηλεκτρονικό μήνυμα αλληλογραφίας δεν θα έπρεπε σε καμία περίπτωση να ληφθεί υπόψη από το δικαστήριο, επειδή δεν πληροί τις προϋποθέσεις των άρθρων 160 ΑΚ και 3 Π.Δ. 150/2001. Θεωρείται ως ανυπόστατη και απολύτως μη δεσμευτική για τον παραλήπτη .

ΜΠρΑθ. 6302/2004

Κατά τη νομολογία αυτή, ο καθορισμός της ηλεκτρονικής διεύθυνσης κατά τρόπο μοναδικό, από τον ίδιο το χρήστη και η δήλωσή της σε κάθε αποστελλόμενο ηλεκτρονικό μήνυμα συνιστά απόδειξη της ταυτότητας του εκδότη του και κατ' αναλογία με τα οριζόμενα για το παραδοσιακό έγγραφο, η μηχανική απεικόνισή του σε έντυπο εμπίπτει στην έννοια του ιδιωτικού εγγράφου, διότι αυτή ακριβώς η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση, που έχει ορισθεί και εφαρμοστεί από τον ίδιο τον αποστολέα, έχει τον χαρακτήρα της ιδιόχειρης υπογραφής, έστω και αν δεν έχει την παραδοσιακή μορφή της τελευταίας (ΜΠρΑθ 6302/2004 Αρμ.2005, 239, ΜΠρΑθ 1963/2004, ΜΠρΑθ 1327/2001, ΔΕΕ 4/2001, σελ. 377) .

Κεντρικό σημείο νομικού προβληματισμού και σε αυτή την απόφαση αποτελεί η έννοια του ηλεκτρονικού εγγράφου. Ομοίως δεν λαμβάνεται υπόψη από το δικαστήριο το ισχύον δίκαιο για το θέμα (Π.Δ. 150/2001).Εσφαλμένα λοιπόν προσδιορίζεται η έννοια του ηλεκτρονικού εγγράφου. Μάλιστα, από την απόφαση προκύπτει ταύτιση του μηνύματος ηλεκτρονικής αλληλογραφίας με το ιδιωτικό έγγραφο. Ενώ ακόμη φαίνεται πως γίνεται δεκτή η σύναψη συμβάσεων με την αποστολή e-mail. Όπως εκτέθηκε ανωτέρω με αφορμή την ΜΠρΑθ. 1963/2004, τόσο από τεχνικής απόψεως, όσο και κυρίως από νομοθετικής, το μήνυμα ηλεκτρονικού ταχυδρομείου αποτελεί ένα ανυπόγραφο έγγραφο με ότι αυτό συνεπάγεται κάθε φορά. Έτσι και στην προκειμένη περίπτωση δεν μπορεί να καλύψει τις προϋποθέσεις του ιδιωτικού εγγράφου όταν ελλείπει από το περιεχόμενό του η προηγμένη ηλεκτρονική υπογραφή.

Επίσης, η ηλεκτρονική διεύθυνση αλληλογραφίας, όπως αυτή εμφαίνεται να συνοδεύει το σχετικό ηλεκτρονικό μήνυμα, δεν μπορεί να εξισωθεί προς την ιδιόχειρη υπογραφή για τεχνικούς λόγους (έλλειψη ασφάλειας) ως προς το πρόσωπο του υπογράφοντος και ως προς το αναλλοίωτο του περιεχομένου, λειτουργίες οι οποίες χαρακτηρίζουν τις ηλεκτρονικές υπογραφές, μάλιστα σε μέγιστο βαθμό τις προηγμένες ηλεκτρονικές υπογραφές. Η νομοθετική πρόβλεψη είναι απολύτως σαφής, οι διαδικασίες παραγωγής και τα έννομα αποτελέσματα της ηλεκτρονικής υπογραφής είναι συγκεκριμένα χωρίς να επιτρέπονται παρεκκλίσεις για το θέμα αυτό. Επομένως, το ηλεκτρονικό μήνυμα αλληλογραφίας δεν μπορεί να χαρακτηρισθεί ως ιδιωτικό έγγραφο στις περιπτώσεις που δεν συνοδεύεται από την ηλεκτρονική υπογραφή του άρθρου 2 Π.Δ. 150/2001.

Α.Π. 2234/2005

Ο Α.Π. απέρριψε την αίτηση αναίρεσης του αναιρεσείοντος Π. Τ. Ο ένοχος κατά την απόφαση 818-818 α/2003 του Τριμελούς Εφετείου Πειραιώς έκανε χρήση πλαστού εγγράφου το οποίο καταρτίστηκε από άγνωστο δράστη. Το αυτοτελές αυτό έγκλημα της χρήσης πλαστού ή νοθευμένου εγγράφου από εκείνον ο οποίος εν γνώσει του το χρησιμοποιεί και όχι από εκείνον ο οποίος το κατήρτισε προβλέπεται από την παρ. 2 του άρθρου 216 ΠΚ. Συνδυαστικά από τον ορισμό του εγγράφου όπως αυτός εμπεριέχεται στο άρθρο 13 περ. γ΄ ΠΚ και κατά τα πραγματικά περιστατικά της απόφασης προκύπτει χρήση αντιγράφου φωτοτυπίας. Τέτοιου είδους αντίγραφο εγγράφου περιλαμβάνεται στον γενικό ορισμό της ανωτέρω διάταξης. Η χρήση της τεχνολογίας και η παραγωγή αντιγράφων με τη μορφή της φωτογραφικής απεικόνισης γίνεται δεκτή κατά τα αναφερόμενα στον ορισμό των εγγράφων. Μάλιστα δε έγινε αποδεκτή η χρήση της μη επικυρωμένης φωτοτυπίας η οποία συνιστά έγγραφο ικανό να αποδείξει ότι και το πρωτότυπο, δηλαδή το γεγονός με την έννομη σημασία. Περαιτέρω κατά τη διαδικασία αναπαραγωγής του πρωτοτύπου με τη φωτοτυπική μέθοδο δολίως επιτεύχθηκαν αλλοιώσεις όπως συνέβη στην προκειμένη περίπτωση. Η πράξη αυτή συνιστά δημιουργία νέου πλαστού εγγράφου και ειδική μορφή χρήσεως πλαστού εγγράφου (Ολ. Α.Π. 2/2002). Εν όψει των όσων εκτέθηκαν, η ανεπικύρωτη φωτοτυπία εγγράφου αποτελεί έγγραφο με όλα τα χαρακτηριστικά του ως συστατικού και αποδεικτικού μέσου.

Α.Π. 203/2006

Με το πρόσφατο αυτό νομολογιακό παράδειγμα το Δ΄ Πολιτικό Τμήμα του Α.Π. απέρριψε την αίτηση αναίρεσης των αναιρεσειόντων. Ειδικά όσον αφορά τον τρίτο λόγο αναίρεσης παρουσιάζεται το ζήτημα της υπόστασης του παραγόμενου με τηλεομοιοτυπία εγγράφου (fax).

Η παροχή εξουσιοδότησης με απλή επιστολή σε περίπτωση ψηφοφορίας, όπως στην προκείμενη απόφαση, ισοδυναμεί κατά το σκεπτικό του Α.Π. με οποιαδήποτε μορφή δύναται να περιβληθεί ο τύπος της επιστολής και με οποιοδήποτε μέσο αποστολής της. Πράγματι, η φράση «απλή επιστολή» δεν προβλέπει ούτε τη μορφή εγκυρότητας της εντολής, αλλά ούτε και περιορίζει τα χρησιμοποιούμενα μέσα για την αποστολή της. Αποτελεί γεγονός η πλήρης ένταξη του παραγόμενου αντιγράφου με την ανωτέρω μέθοδο τηλεομοιοτυπίας στις μηχανικές απεικονίσεις.

Η απαρίθμηση του άρθρου είναι ενδεικτική, όπως υποδηλώνεται στο κείμενό του. Εξάλλου, δεν θα ήταν δυνατή ούτε και ασφαλής η ένταξη όλων των μέσων και μεθόδων τουλάχιστον των μηχανικών απεικονίσεων. Ακόμη ο Α.Π. θεώρησε ότι το έγγραφο τηλεομοιοτυπίας αποτελεί πρωτότυπο. Έτσι η μορφή απεικόνισης ενός εγγράφου σε γραφή με την κλασική έννοια ή άλλη πιστή αναπαραγωγή δεν αποτελούν πρόσχωμα για την αποδοχή νέων μορφών παραγωγής εγγράφων για την ένταξή τους στο πλαίσιο των ιδιωτικών εγγράφων. Περαιτέρω η δυναμική αυτή κρίση του Α.Π. συνάδει και με προτάσεις τις τεχνολογίας που πρόκειται να τεθούν προς χρήση στο μέλλον. Υπό αυτές τις συνθήκες η καινοτόμος αυτή απόφαση θα αποτελέσει οδηγό για μελλοντικές τεχνολογικές εφαρμογές. Η νομιμοποίηση που παρέχεται από την εν λόγω απόφαση στην ισοδυναμία των εγγράφων τηλεομοιοτυπίας προς τα ιδιωτικά έγγραφα επιτρέπει την είσοδο και άλλων μορφών εγγράφων στην κλασική έννοια των ιδιωτικών με πολλαπλές συνέπειες στις καθημερινές μας δραστηριότητες. Εξάλλου και η αντίθετη θέση του μειοψηφούντος εισηγητή δέχεται ανεπιφύλακτα την αναγνώριση του fax ως ιδιωτικού εγγράφου. Η επισημείωση όμως που διατυπώθηκε ως προς την ασφάλεια και το αναλλοίωτο του κειμένου του, δεν μετέβαλαν τη θέση της πλειοψηφίας, γεγονός που καταδεικνύει ότι η ακολουθούμενη διαδικασία αποστολής τηλεομοιοτυπίας συνάδει με τις γενικές αρχές του ιδιωτικού εγγράφου του οποίου εν τέλει αποτελεί μέρος.

10.2 Σύνοψη Νομολογιακών Δεδομένων

Από τη σύντομη παρουσίαση των ανωτέρω αποφάσεων του Α.Π. προκύπτει μια σειρά στοιχείων σχετικών με το έγγραφο όχι τόσο στη στενή μορφή του ηλεκτρονικού όσο κυρίως σε ευρύτερες πληροφοριακές εκφάνσεις του. Τα συμπεράσματα που συνάγονται από τις εν λόγω αποφάσεις αναδεικνύουν το εύρος του εγγράφου ως προς τις μορφές που αυτό μπορεί να λάβει. Τη συμβολή της τεχνολογίας στη διαμόρφωση της έννοιάς του και την τελική αποδοχή του ως έγκυρου συστατικού και αποδεικτικού τύπου. Τα συμπαγή νομοθετικά στεγανά έχουν πλέον εκλάβει το έγγραφο ιδιωτικό και δημόσιο ως μορφή έκφρασης με ιδιαίτερη επιρροή της τεχνολογίας στη δόμησή του.

Από πλευράς αστικού δικαίου από τις ανωτέρω αποφάσεις προκύπτει μια ελαστικότητα στην αποδοχή του εγγράφου. Έγγραφα τα οποία προέρχονται από φωτοτυπική ή άλλη επεξεργασία με τη συμβολή ηλεκτρονικών υπολογιστών εντάσσονται στο πεδίο του συστατικού και αποδεικτικού τύπου των ιδιωτικών εγγράφων. Εκτός των ρυθμίσεων για τα ηλεκτρονικά έγγραφα, στη νομολογία αντιμετωπίζονται ως μορφή νέου τύπου εγγράφου και όσα συστήνονται με τη συνδρομή της τεχνολογίας. Για παράδειγμα φωτοτυπικά αντίγραφα εγγράφων ή τηλεομοιοτυπίες υπό προϋποθέσεις δύνανται να συνιστούν έγγραφο τύπο.

Από τη σκοπιά του ποινικού δικαίου ο γενικός κανόνας που συμπεριλαμβάνεται στο άρθρο 13 εδ. γ΄ ΠΚ, όπως αυτό τροποποιήθηκε με το Ν. 1805/1988, επιτρέπει μια ευρύτερη αναγνώριση εγγράφων τα οποία καταρτίζονται με τεχνολογικά μέσα. Έτσι, αντίγραφα εγγράφων που παράγονται με τη φωτοαντιγραφική μέθοδο, ακόμη έγγραφα τα οποία αποστέλλονται με τη μέθοδο της τηλεομοιοτυπίας (Fax) αποτελούν έγγραφα που παρέχουν πλήρη απόδειξη ως προς το περιεχόμενό τους. Κατ΄ επέκταση δύνανται να αποτελέσουν και μέσα εκδήλωσης αξιόποινης πράξης. Σε κάθε περίπτωση η εισαγωγή του τροποποιηθέντος άρθρου 13 εδ. γ΄ ΠΚ επέφερε σημαντικές μεταβολές σε ουσιαστικό και δικονομικό επίπεδο. Η εμφανής συνεισφορά της νέας διάταξης έγκειται όχι μόνο στη λεκτική διεύρυνση του όρου «έγγραφο» αλλά στην ουσιαστική εξέλιξη και πρακτική του χρήση.

11 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στη σημερινή εποχή της ηλεκτρονικής τεχνολογίας, των ψηφιακών επικοινωνιών και της διαδικτυακής ανταλλαγής δεδομένων, η ασφάλεια των ηλεκτρονικών συναλλαγών είναι απαραίτητη προϋπόθεση και εγγύηση για την ομαλή λειτουργία της οικονομικής και κοινωνικής ζωής. Με γνώμονα το γεγονός αυτό, ο νομοθέτης καλείται να συντελέσει στην επίτευξη συναλλακτικής ασφάλειας με τη συνεχή παρακολούθηση των τεχνολογικών εξελίξεων και την κατάλληλη νομοθετική παρέμβαση στο κατάλληλο χρονικό σημείο, ακούοντας τις απαιτήσεις της εποχής και της κοινωνίας.

Συμπερασματικά, μπορούμε να διατυπώσουμε την εκτίμηση ότι το ρυθμιστικό πλαίσιο για τις ηλεκτρονικές υπογραφές παρέχει σαφώς δυνατότητες για τη διευκόλυνση των συναλλαγών του ηλεκτρονικού εμπορίου κατά τις οποίες θα χρησιμοποιούνται ηλεκτρονικές υπογραφές, τόσο στα πλαίσια αναγνώρισης της ισχύος των σχετικών τυπικών δικαιοπραξιών, όσο και στα πλαίσια της αποδεικτικής διαδικασίας. Βασική καινοτομία που εισάγεται με τη νέα νομοθεσία είναι η πρόβλεψη τρίτου έμπιστου προσώπου με σημαντικό ρόλο στην πιστοποίηση των στοιχείων της ηλεκτρονικά καταρτιζόμενης συναλλαγής, στην εμπέδωση της ασφάλειας στο χώρο του ηλεκτρονικού εμπορίου και στη διατήρηση αποδεικτικών στοιχείων. Κατά τον τρόπο αυτό η λειτουργία της υπογραφής απεκδύεται το αποκλειστικά προσωπικό στοιχείο που τη διακρίνει στην παραδοσιακή της μορφή και συνδυάζεται απαραίτητα με ένα ολοκληρωμένο σύστημα υπηρεσιών πληροφορικής που δεν ελέγχεται απολύτως από τον υπογράφοντα, αλλά βασίζεται στην αξιοπιστία και στην προηγμένη τεχνολογική υποδομή που διαθέτουν οι Πάροχοι Υπηρεσιών Πιστοποίησης. Με δεδομένη, μάλιστα, την ταχύτητα των εξελίξεων στο συγκεκριμένο τεχνολογικό πεδίο κρίνεται απαραίτητη η ανά τακτά χρονικά διαστήματα επανεξέταση των συγκεκριμένων ρυθμίσεων προκειμένου να διασφαλίζεται ότι η ερμηνεία και εφαρμογή τους συνεχίζει να οδηγεί με αξιοπιστία στην επίτευξη του νομοθετικού σκοπού τους.

Η συμβολή της τεχνολογίας σε ποικίλες εφαρμογές της καθημερινής μας ζωής αποτελεί πλέον αναμφισβήτητη πραγματικότητα. Δικαιολογημένα συνεπώς διεθνείς οργανισμοί, κράτη, φορείς, επιχειρήσεις και ιδιώτες θέτουν προτεραιότητα σε νομικά ζητήματα σχετικά με το διαδίκτυο. Θεωρούμε ότι μέχρι σήμερα έχουν επιλυθεί αρκετά προβλήματα που συνδέονται με το διαδίκτυο. Οφείλουμε όμως να δώσουμε περισσότερη έμφαση στη διεθνή συνεργασία, στην προστασία των καταναλωτών και στη συνέργεια τεχνολογίας με τη νομική επιστήμη. Η διαφορετική δικαιϊκή κουλτούρα πρέπει να συγκλίνει, ώστε να αποτελέσει κλείδα ενοποίησης με προβολή στον αναδυόμενο κλάδο του ηλεκτρονικού δικαίου. Η εξέταση θεμάτων όπως τα ψηφιακά έγγραφα αναδεικνύουν την εκτεταμένη επίδραση της τεχνολογίας στη διαμόρφωση των σύγχρονων συναλλακτικών πρακτικών. Παράλληλα, διαφαίνεται η άρρηκτη σχέση μεταξύ εγγράφου και υπογραφής, η ιδιαιτερότητα χρήσης τους και η τελική αλληλεξάρτησή τους στην ολοκλήρωση του ηλεκτρονικού εγγράφου, ως συστατικού της ηλεκτρονικής δικαιοπραξίας.

Πέρα όμως από τις όποιες διευκολύνσεις που μας παρέχονται σε τεχνολογικό επίπεδο, πρέπει να τονίσουμε ότι η εξελιγμένη τεχνολογία απαιτεί εξειδικευμένες γνώσεις από τους χρήστες, γεγονός που αποτελεί ανασταλτικό παράγοντα ακόμη για τις απλές ηλεκτρονικές επικοινωνίες και συναλλαγές. Επιπλέον, το κόστος των καινοτομιών επιβαρύνει τον τελικό χρήστη, ο οποίος επωφελείται μεν από τις τεχνολογικές εφαρμογές, χωρίς όμως να εξασφαλίζεται πλήρως όσον αφορά στο απόρρητο των επικοινωνιών, στη διαχείριση των προσωπικών δεδομένων, καθώς και στην πιστότητα των διακινούμενων ηλεκτρονικών δεδομένων.

Τελικά, οι σύγχρονες τάσεις για την αναμόρφωση του δικαίου αποκτούν ιδιαίτερη βαρύτητα. Στόχος αυτών των αλλαγών πρέπει να είναι η ολοκληρωμένη κάλυψη νομικών θεμάτων, όπως εισάγονται από τη διαδικτυακή χρήση. Πρωτεύουσα σημασία θα πρέπει όμως να αποδίδεται όχι στην ποσοτική αναθεώρηση των κλασικών κανόνων δικαίου, όσο κυρίως σε ποιοτικές νομοθετικές παρεμβάσεις με σκοπό την απρόσκοπτη λειτουργία των εννοιών και των θεσμικών λειτουργιών του όλου δικαιϊκού συστήματος σε εθνικό, κοινοτικό, αλλά και διεθνές επίπεδο.

12 ΨΗΦΙΑΚΗ ΒΙΒΛΙΟΘΗΚΗ DSpace

Το λογισμικό DSpace είναι ένα πρωτοποριακό ψηφιακό σύστημα βιβλιοθηκών που λαμβάνει, αποθηκεύει, ευρετηριάζει, διατηρεί και διανέμει το πνευματικό απόσταγμα της ερευνητικής δραστηριότητας πανεπιστημίων σε ψηφιακή μορφή. Διανέμεται ελεύθερα στους ερευνητικούς οργανισμούς ανά τον κόσμο ως σύστημα ανοικτού κώδικα, εξυπηρετώντας τις ποικίλες ανάγκες ψηφιακής αποθήκευσης, όπως αποθετήρια οργανισμών (Institutional Repositories - IRs), αποθετήρια αντικειμένων εκμάθησης (Learning Object Repositories - LORs), διπλωματικές εργασίες, διατριβές και εν γένει «γκρίζα βιβλιογραφία», διαχείριση ψηφιακών εγγραφών, ψηφιακή διατήρηση, εκδόσεις και άλλα.

Το DSpace είναι προϊόν του από κοινού έργου ανάπτυξης των βιβλιοθηκών του MIT (Massachusetts Institute of Technology – Ίδρυμα Τεχνολογίας της Μασσαχουσέττης) και της εταιρείας Hewlett-Packard (HP). Οι φορείς αυτοί, με τη δημιουργία του DSpace, θέλησαν να χτίσουν ένα σταθερό και μακροπρόθεσμο ψηφιακό αποθετήριο, το οποίο θα συλλέγει, θα διατηρεί και θα διαδίδει το εκπαιδευτικό υλικό και την έρευνα, που παράγονται από τα μέλη της ερευνητικής κοινότητας οποιουδήποτε πανεπιστημίου ή κέντρου, σε τοπικό ή σε παγκόσμιο επίπεδο. Το Dspace δέχεται όλες τις μορφές ψηφιακού υλικού, συμπεριλαμβανομένων κειμένου, εικόνων, βίντεο, αρχείων ήχου. Το περιεχόμενο των παραπάνω μπορεί να περιλαμβάνει τα εξής: Άρθρα, Αναφορές, Εργασίες, Αρχεία διασκέψεων, Διδακτορικές διατριβές, Σύνολα δεδομένων: (στατιστικών, μαθηματικών προγραμμάτων κλπ), Εικόνες: οπτικές, επιστημονικές, κλπ, Αρχεία ήχου, Αρχεία βίντεο, Αντικείμενα εκμάθησης.

Η ψηφιακή βιβλιοθήκη Dspace, όπως και αυτή του Keystone, περιλαμβάνει μια λίστα από τις συλλογές που διαθέτει και επιτρέπει στο χρήστη να επιλέξει από τη λίστα αυτές που τον ενδιαφέρουν. Μπορεί επίσης να γίνει αναζήτηση με βάση τα αρχικά μόνο γράμματα μιας λέξης, οπότε εμφανίζονται όλα τα σχετικά αντικείμενα. Μια από τις βασικές του αδυναμίες είναι η απουσία συνδέσμου που να οδηγεί από μια πηγή πίσω στη σελίδα των αποτελεσμάτων, κάτι που δυσχεραίνει το υποσύστημα πλοήγησης. Τέλος, όσον αφορά την τεκμηρίωση στο πρόγραμμα εγκατάστασης, υπάρχουν πολύ κατανοητά και κατατοπιστικά εγχειρίδια για το διαχειριστή, προκειμένου να διευκολυνθεί η εργασία του.

12.1 Απαραίτητα προγράμματα που θα χρησιμοποιηθούν

1. Java jdk-6u20-windows-i586

http://java.sun.com/javase/downloads/index.jsp

2. postgresql-8.3.10-1-windows

http://www.postgresql.org/download/windows

3. Apache –Ant- 1.8.0

http://ant.apache.org/bindownload.cgi

4. apache-tomcat-6.0.26.

http://tomcat.apache.org/download-60.cgi

5. apache-maven-2.2.1

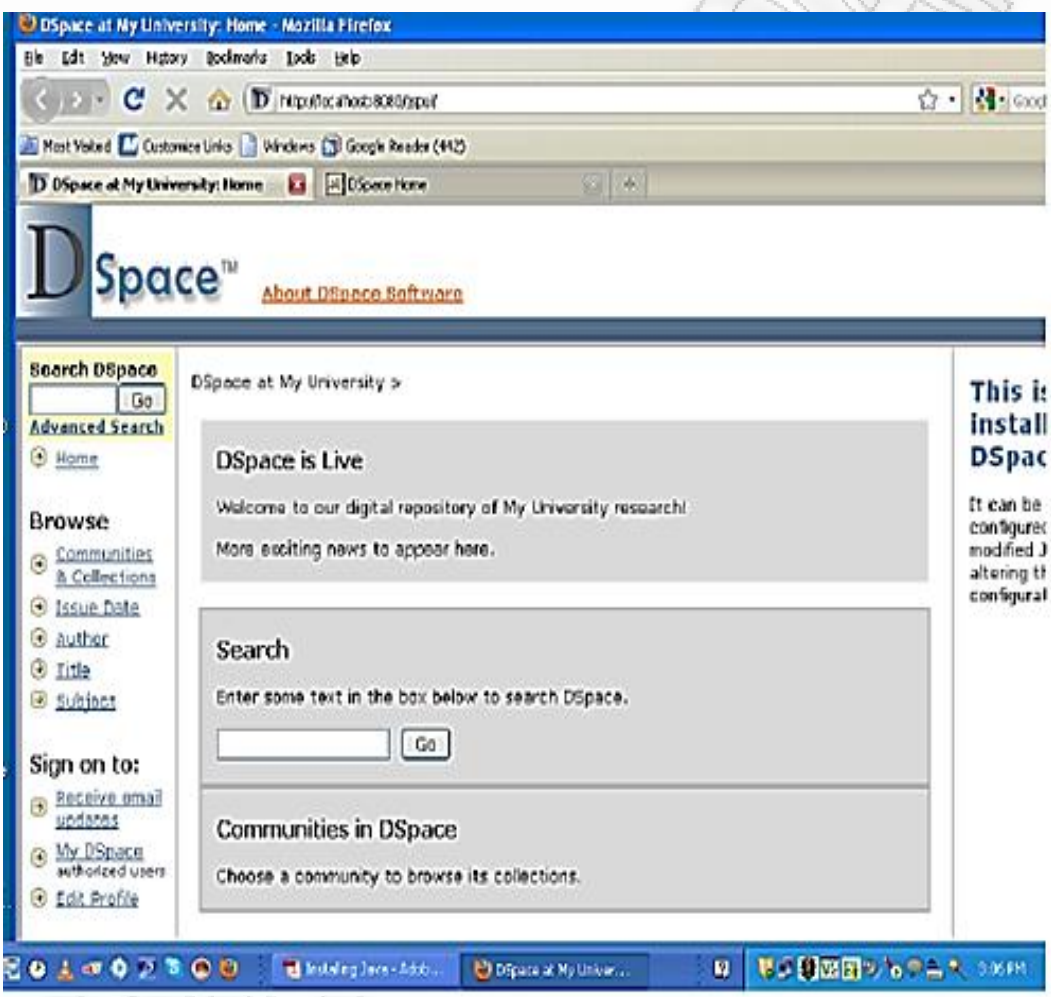
http://maven.apache.org/download.html

6. dspace-1.6.0-src-release

http://sourceforge.net/projects/dspace/files/

Η εγκατάσταση των προγραμμάτων θα πραγματοποιηθεί σε υπολογιστή που τρέχει λειτουργικό Windows VISTA.

Ξεκινώντας το πρόγραμμα Tomcat κάνοντας Restart στο Tomcat και πληκτρογώντας στο browser την διεύθυνση http://localhost:8080/jspui/ βλέπω το DSpace να τρέχει και έχω την παρακάτω οθόνη:



12.2 Δυνατότητες –χαρακτηριστικά του dspace

Το λογισμικό DSpace συλλέγει, διανέμει και συντηρεί ψηφιακά προϊόντα έρευνας. Εδώ θα μπορείτε να βρείτε άρθρα, εργασίες, προδημοσιεύσεις, τεχνικές αναφορές, πρακτικά συνεδρίων και δεδομένα σε διάφορες ψηφιακές μορφές. Το περιεχόμενο αυξάνεται μέρα με τη μέρα καθώς νέες κοινότητες και συλλογές προστίθενται.Το περιεχόμενο είναι οργανωμένο σε κοινότητες που μπορούν να αντιστοιχούν σε διοικητικές οντότητες, όπως Σχολές, Τμήματα, εργαστήρια και ερευνητικά κέντρα. Σε κάθε κοινότητα μπορούν να υπάρχουν άπειρες υποκοινότητες και συλλογές. Κάθε συλλογή μπορεί να περιέχει άπειρο αριθμό τεκμηρίων.

Ηλεκτρονική κατάρτιση συμβάσεων
Ψηφιακές υπογραφές

- Η Πλοήγηση σάς επιτρέπει να δείτε μια λίστα τεκμηρίων με κάποια συγκεκριμένη σειρά.
- Η Πλοήγηση ανά Κοινότητα/ Συλλογή σάς εμφανίζει τις κοινότητες σε αλφαβητική σειρά και σάς επιτρέπει να δείτε τις υποκοινότητες και τις συλλογές τους.
- Η Πλοήγηση ανά Τίτλο σάς εμφανίζει σε αλφαβητική σειρά όλους τους τίτλους τεκμηρίων.
- Η Πλοήγηση ανά Συγγραφέα σάς εμφανίζει σε αλφαβητική σειρά όλους τους συγγραφείς τεκμηρίων.
- Η Πλοήγηση ανά Θέμα/ Λέξη-κλειδί σάς εμφανίζει σε αλφαβητική σειρά όλα τα θέματα που έχουν χρησιμοποιηθεί για να περιγράψουν τεκμήρια.
- Η Πλοήγηση ανά Ημερομηνία σάς εμφανίζει σε αντίστροφη χρονολογική σειρά όλα τα τεκμήρια που υπάρχουν.

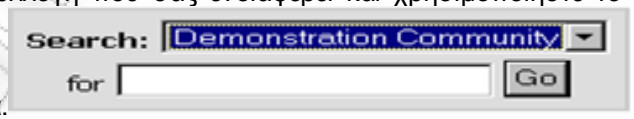
Μπορείτε να εισέλθετε στο σύστημα αν:

- θέλετε να γίνετε συνδρομητής σε μια συλλογή και να λαμβάνετε ειδοποιήσεις μέσω e-mail κάθε φορά που προστίθενται νέα τεκμήρια .
- θέλετε να πάτε στη σελίδα "Το Dspace μου", όπου καταγράφονται οι συνδρομές σας και οι όποιες συναλλαγές σας που απαιτούν εξουσιοδότηση (αν έχετε δικαίωμα υποβολής σε μια συλλογή, για παράδειγμα) .
- επιθυμείτε να επεξεργαστείτε το λογαριασμό σας

- Η Υποβολή είναι η λειτουργία που επιτρέπει στους χρήστες να προσθέσουν ένα τεκμήριο. Η διαδικασία υποβολής συμπεριλαμβάνει τη συμπλήρωση μιας φόρμας μεταδεδομένων με πληροφορίες σχετικά με το τεκμήριο και το "ανέβασμα" του αρχείου/ των αρχείων που συνιστούν το ψηφιακό τεκμήριο. Κάθε κοινότητα μπορεί να έχει τη δική της πολιτική υποβολής.
- Το Dspace μου είναι μια προσωπική σελίδα που υπάρχει για κάθε μέλος. Αυτή η σελίδα μπορεί να περιέχει μια λίστα από τεκμήρια που βρίσκονται σε διαδικασία υποβολής για ένα συγκεκριμένο μέλος, ή μια λίστα με εργασίες που σχετίζονται με τεκμήρια και που χρειάζονται επεξεργασία, διόρθωση ή έλεγχο.
- Η επεξεργασία του προφίλ σας σάς επιτρέπει να αλλάξετε τον κωδικό σας.
- Η σελίδα Σχετικά με το DSpace σάς μεταφέρει στο δικτυακό τόπο του DSpace όπου θα βρείτε πληροφορίες για το πρόγραμμα και την πορεία του.

Για να αναζητήσετε σε όλη την Ψηφιακή βιβλιοθήκη, χρησιμοποιήστε το πλαίσιο αναζήτησης στο επάνω αριστερό μέρος της κεντρικής σελίδας (ή το πλαίσιο αναζήτησης στο κέντρο).

Για να περιορίσετε την αναζήτησή σας σε μια συγκεκριμένη κοινότητα ή συλλογή, πλοηγηθείτε στην κοινότητα ή τη συλλογή που σάς ενδιαφέρει και χρησιμοποιήστε το κουτί αναζήτησης στη συγκεκριμένη σελίδα.



Το λογισμικό DSpace χρησιμοποιεί τη μηχανή αναζήτησης Jakarta Lucene. Διαβάστε κάποιες πληροφορίες σχετικά με την αναζήτηση που ίσως σάς βοηθήσουν:

Τι αναζητείται στη γενική αναζήτηση με λέξεις-κλειδιά

Η λέξη/ οι λέξεις που εισάγετε στο κουτί θα αναζητηθούν στα εξής πεδία: τίτλος, συγγραφέας, θέμα, επιτομή, σειρά και αναγνωριστικό κάθε εγγραφής τεκμηρίου.

ΚΟΙΝΟΤΗΤΕΣ

Το περιεχόμενο είναι οργανωμένο σε κοινότητες που μπορούν να αντιστοιχούν σε διοικητικές οντότητες όπως Σχολές, Τμήματα, εργαστήρια και ερευνητικά κέντρα. Σε κάθε κοινότητα μπορεί να υπάρχει απεριόριστος αριθμός υποκοινοτήτων και συλλογών. Κάθε συλλογή μπορεί να περιέχει απεριόριστο αριθμό τεκμηρίων. Αυτή η οργάνωση δίνει τη

δυνατότητα να προσαρμόζεται στις διαφορετικές ανάγκες των κοινοτήτων επιτρέποντάς τους :

1. Να αποφασίσουν για πολιτικές, όπως:

- ποιος συνεισφέρει περιεχόμενο
- αν θα υπάρχει διαδικασία ελέγχου
- θα έχει πρόσβαση

2. Να προσδιορίσουν τη ροή των εργασιών - έλεγχος, επεξεργασία, μεταδεδομένα

3. Διαχειριστούν τις συλλογές

Κάθε κοινότητα έχει τη δική της σελίδα με πληροφορίες, νέα και συνδέσμους που αντανακλούν τα ενδιαφέροντα της κοινότητας αυτής, καθώς και μια λίστα με συλλογές εντός της κοινότητας

ΣΥΛΛΟΓΕΣ

Οι κοινότητες μπορεί να περιέχουν απεριόριστο αριθμό συλλογών. Οι συλλογές μπορούν να είναι οργανωμένες σε σχέση με ένα θέμα ή είδος πληροφορίας (όπως εργασίες ή δεδομένα) ή οποιαδήποτε άλλη μέθοδο ταξινόμησης θεωρεί μια κοινότητα χρήσιμη για την οργάνωση των ψηφιακών της τεκμηρίων. Οι συλλογές μπορούν να έχουν διαφορετικές πολιτικές και ροές εργασιών.

Κάθε συλλογή έχει τη δική της σελίδα με πληροφορίες, νέα και συνδέσμους που αντανακλούν τα ενδιαφέροντα των χρηστών αυτής της συλλογής.

ΕΙΣΟΔΟΣ ΣΤΗΝ ΨΗΦΙΔΑ

Όταν εισέρχεστε σε μια περιοχή που απαιτεί εξουσιοδότηση, το σύστημα θα απαιτήσει να χρησιμοποιήσετε τα στοιχεία σας για να σας αναγνωρίσει. Όλοι οι χρήστες μπορούν να εγγραφούν για να λαμβάνουν ενημερώσεις. Κάποιες περιορισμένες λειτουργίες, όπως η υποβολή περιεχομένου, απαιτούν εξουσιοδότηση από την κοινότητα.

Πριν εισέλθετε για πρώτη φορά, θα πρέπει να κάνετε κλικ στο σύνδεσμο "Νέος χρήστης; Κάντε κλικ εδώ για να εγγραφείτε" και να ακολουθήσετε τις οδηγίες. Έπειτα, θα χρειαστεί να εισάγετε το e-mail σας και τον κωδικό σας στη φόρμα εισόδου του συστήματος. Το e-mail σας θα πρέπει να εισαχθεί ολόκληρο. Δεν έχει σημασία αν θα γραφεί με κεφαλαία ή μικρά γράμματα. Παράδειγμα: user@unipi.gr Πληκτρολογήστε τον κωδικό σας ακριβώς όπως τον εισήγατε αρχικά. Εδώ ΕΧΕΙ ΣΗΜΑΣΙΑ αν θα χρησιμοποιήσετε κεφαλαία ή μικρά. Πατήστε το κουμπί "Εισέλθετε στο δικτυακό τόπο" για να συνεχίσετε.

ΥΠΟΒΟΛΗ ΤΕΚΜΗΡΙΟΥ

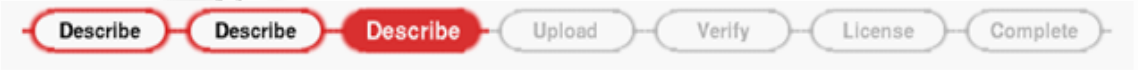
Διακοπή κατά τη διάρκεια της διαδικασίας υποβολής:

Σε οποιαδήποτε στιγμή κατά τη διάρκεια της διαδικασίας υποβολής μπορείτε να σταματήσετε και να αποθηκεύσετε τη δουλειά σας για να συνεχίσετε αργότερα κάνοντας κλικ στο κουμπί "Ακυρώστε/Αποθηκεύστε" στο κάτω μέρος της σελίδας. Τα δεδομένα που έχετε ήδη εισάγει θα αποθηκευτούν έως ότου επιστρέψετε στην υποβολή, και θα σάς γίνει υπενθύμιση από τη σελίδα "Το Dspace μου" ότι έχετε μια υποβολή σε εξέλιξη. Αν για κάποιο λόγο εξέλθετε από τη διαδικασία υποβολής κατά λάθος, μπορείτε να ξαναρχίσετε από τη σελίδα "Το Dspace μου". Μπορείτε, επίσης, να ακυρώσετε την υποβολή σας οποιαδήποτε στιγμή.

Επιλέξτε Συλλογή

Μπάρα προόδου - Τα Οβάλ Κουμπιά στο πάνω μέρος της σελίδας:

Στο πάνω μέρος των σελίδων υποβολής θα βρείτε 7 οβάλ κουμπιά που αναπαριστούν κάθε βήμα της διαδικασίας υποβολής. Καθώς προχωράτε στη διαδικασία, θα αλλάζει το χρώμα των κουμπιών. Αφού ξεκινήσετε, μπορείτε να τα χρησιμοποιήσετε για να πηγαίνετε μπρος ή πίσω με ένα κλικ επάνω τους. Δε θα χάσετε δεδομένα αν μετακινείστε μπρος/ πίσω.



Επιλέξτε συλλογή: Κάντε κλικ στο βέλος στα δεξιά του πτυσσόμενου μενού για να δείτε μια λίστα με τις Συλλογές. Μετακινήστε το δείκτη του ποντικιού σας στην συλλογή όπου επιθυμείτε να προσθέσετε το τεκμήριό σας και κάντε κλικ.

Επιλέξτε συλλογή:

Κάντε κλικ στο βέλος στα δεξιά του πτυσσόμενου μενού για να δείτε μια λίστα με τις Συλλογές. Μετακινήστε το δείκτη του ποντικιού σας στην συλλογή όπου επιθυμείτε να προσθέσετε το τεκμήριό σας και κάντε κλικ.

Κάντε κλικ στο κουμπί "Επόμενη" για να συνεχίσετε ή "Ακυρώστε/Αποθηκεύστε" για να σταματήσετε και να αποθηκεύσετε ή να ακυρώσετε την υποβολή σας.

Αν απαντήσετε "ναι" σε οποιαδήποτε ερώτηση αυτής της σελίδας, θα εμφανιστεί μια τροποποιημένη φόρμα εισαγωγής προσαρμοσμένη στις πληροφορίες που εισήγατε. Διαφορετικά, θα εμφανιστεί η "κανονική" φόρμα εισαγωγής.

● Περισσότεροι από έναν τίτλοι - Μερικές φορές ένα τεκμήριο έχει πάνω από έναν τίτλους, ίσως μια συντόμευση, ακρώνυμο, ή έναν τίτλο σε άλλη γλώσσα. Σε αυτήν την περίπτωση και εφόσον θέλετε να δηλώσετε αυτές τις πληροφορίες, "τσεκάρετε" το κουτί δίπλα από τη σχετική πρόταση.

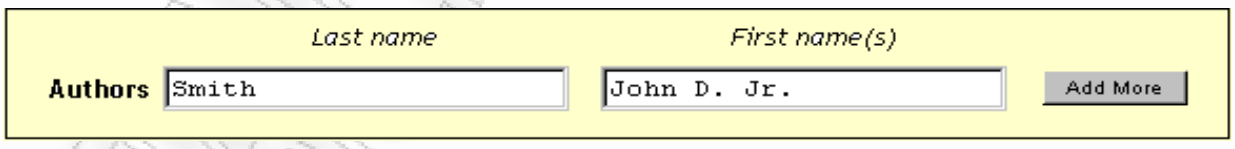
● Προηγούμενη έκδοση - Στα καινούργια τεκμήρια που ΔΕΝ έχουν δημοσιευτεί ή διανεμηθεί στο παρελθόν θα αποδοθεί μια ημερομηνία έκδοσης από το σύστημα με το που θα εισαχθούν. Αν υποβάλλετε παλαιότερα τεκμήρια που έχουν ήδη διανεμηθεί ή δημοσιευτεί, "τσεκάρετε" το κουτί δίπλα από τη σχετική πρόταση. Η φόρμα θα σάς ζητήσει να εισάγετε κάποια στοιχεία σχετικά με την προηγούμενη έκδοση.

● Πολλαπλά αρχεία - Ένα τεκμήριο μπορεί να συνίσταται από περισσότερα από ένα αρχεία. Ένα απλό παράδειγμα είναι ένα αρχείο HTML που παραπέμπει σε αρχεία εικόνας (όπως αρχεία JPG ή GIF). Ένα άλλο παράδειγμα είναι ένα άρθρο που συνοδεύεται από ένα βίντεο και ένα αρχείο δεδομένων. Αν υποβάλλετε περισσότερα από ένα αρχεία για αυτό το τεκμήριο, "τσεκάρετε" το κουτί δίπλα από τη σχετική πρόταση.

Κάντε κλικ στο κουμπί "Επόμενη" για να συνεχίσετε, ή στο "Ακυρώστε/ Αποθηκεύστε" για να σταματήσετε και να αποθηκεύσετε ή να ακυρώσετε την υποβολή σας.
Οι πληροφορίες που θα συμπληρώσετε σε αυτές τις δύο σελίδες θα σχηματίσουν την εγγραφή μεταδεδομένων που θα δώσει τη δυνατότητα στους χρήστες να ανακτούν το τεκμήριό σας μέσω των μηχανών αναζήτησης. Όσο περισσότερα μεταδεδομένα, τόσο πιο εύκολα θα "εντοπίζεται" το τεκμήριό σας, γι'αυτό σας παρακαλούμε να αφιερώσετε λίγο χρόνο για να συμπληρώσετε όσο περισσότερα πεδία μπορείτε σχετικά με το τεκμήριο.

Συγγραφέας:

Μπορεί να είναι ένα άτομο, οργανισμός ή υπηρεσία υπεύθυνη για τη δημιουργία ή συνεισφορά στο περιεχόμενο του τεκμηρίου. Κάνοντας κλικ στο κουμπί "Προσθέστε περισσότερα" μπορείτε να προσθέσετε όσους συγγραφείς χρειάζεται. Παραδείγματα:

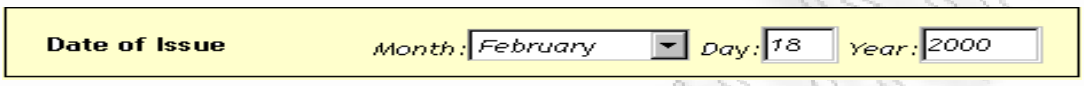


Τίτλος:

Εισάγετε τον πλήρη τίτλο με τον οποίο θα πρέπει να αναγνωρίζεται το τεκμήριο. Όλα τα τεκμήρια πρέπει να έχουν έναν τίτλο!

Ημερομηνία έκδοσης: (σημείωση - αυτό το κουτί θα εμφανιστεί μόνο αν έχετε δηλώσει στην πρώτη σελίδα πως το τεκμήριο έχει δημοσιευτεί ή διανεμηθεί στο παρελθόν. Αν η Ψηφιακή Βιβλιοθήκη είναι το πρώτο μέσο διανομής του τεκμηρίου, μια ημερομηνία θα αποδοθεί από το σύστημα όταν το τεκμήριο ενσωματωθεί στο αποθετήριο.)

Αν το τεκμήριό σας εκδόθηκε στο παρελθόν ή δημοσιοποιήθηκε, εισάγετε εδώ την ημερομηνία αυτού του γεγονότος. Αν δε γνωρίζετε το μήνα, αφήστε το κουτί όπως έχει, "Χωρίς μήνα". Διαφορετικά επιλέξτε ένα μήνα από το μενού. Αν δε γνωρίζετε την ακριβή ημερομηνία, αφήστε το κουτί κενό.



Τύπος:

Επιλέξτε τον τύπο του υλικού που ταιριάζει καλύτερα στο τεκμήριό σας. Για να επιλέξετε περισσότερες από μία τιμές από τη λίστα, ίσως χρειαστεί να κρατήσετε πατημένο το πλήκτρο "ctrl" ή "shift".

Γλώσσα:

Επιλέξτε τη γλώσσα του περιεχομένου του τεκμηρίου. Αν η εξ ορισμού τιμή (Ελληνικά) δεν είναι κατάλληλη, κάντε κλικ στο βέλος στα δεξιά του πτυσσόμενου μενού για να δείτε μια λίστα με τις τιμές που μπορείτε να εισάγετε, π.χ.

ΥΠΟΒΟΛΗ: φορτώστε ένα αρχείο

Υπάρχουν δύο τρόποι που μπορείτε να εισάγετε το όνομα του αρχείου που θέλετε να φορτώσετε:

1. Πληκτρολογήστε τη διεύθυνση και το όνομα του αρχείου στο πλαίσιο και έπειτα πατήστε το κουμπί "Επόμενη" στην κάτω δεξιά γωνία της οθόνης.
2. Κάντε κλικ στο κουμπί "Πλοήγηση" και θα ανοίξει ένα παράθυρο για να βρείτε τα αρχεία σας. Μπορείτε να πλοηγηθείτε στους φακέλους σας μέχρι να βρείτε το σωστό αρχείο που θα φορτωθεί. Κάντε διπλό κλικ στο όνομα του αρχείου που θέλετε να φορτώσετε, και το όνομα θα εισαχθεί στο πλαίσιο εισαγωγής.

Το αρχείο φορτώθηκε

Αφού φορτώσετε το αρχείο, ελέγξτε τις πληροφορίες στον πίνακα για να βεβαιωθείτε πως είναι σωστές. Υπάρχουν δύο επιπλέον τρόποι για να βεβαιωθείτε πως τα αρχεία σας έχουν φορτωθεί σωστά:

- Κάντε κλικ στο όνομα του αρχείου. Αυτό θα ανοίξει το αρχείο σε καινούργιο παράθυρο, ώστε να ελέγξετε τα περιεχόμενά του.
- Συγκρίνετε το checksum του αρχείου που εμφανίζεται εδώ με το checksum που υπολογίζετε εσείς.

Αν φορτώνετε μόνο ένα αρχείο, κάντε κλικ στο "Επόμενη" όταν βεβαιωθείτε πως το αρχείο φορτώθηκε επιτυχώς.

Αν φορτώνετε περισσότερα από ένα αρχεία , κάντε κλικ στο κουμπί "Προσθέστε κι άλλο αρχείο" (αυτό θα εμφανιστεί αν "τσεκάρατε" την επιλογή "Το αρχείο συνίσταται από περισσότερα από ένα αρχεία" στη σελίδα "Υποβάλλετε: Περιγράψτε το τεκμήριό σας"). Αφού βεβαιωθείτε πως όλα τα αρχεία του τεκμηρίου έχουν φορτωθεί επιτυχώς, κάντε κλικ στο κουμπί "Επόμενη".

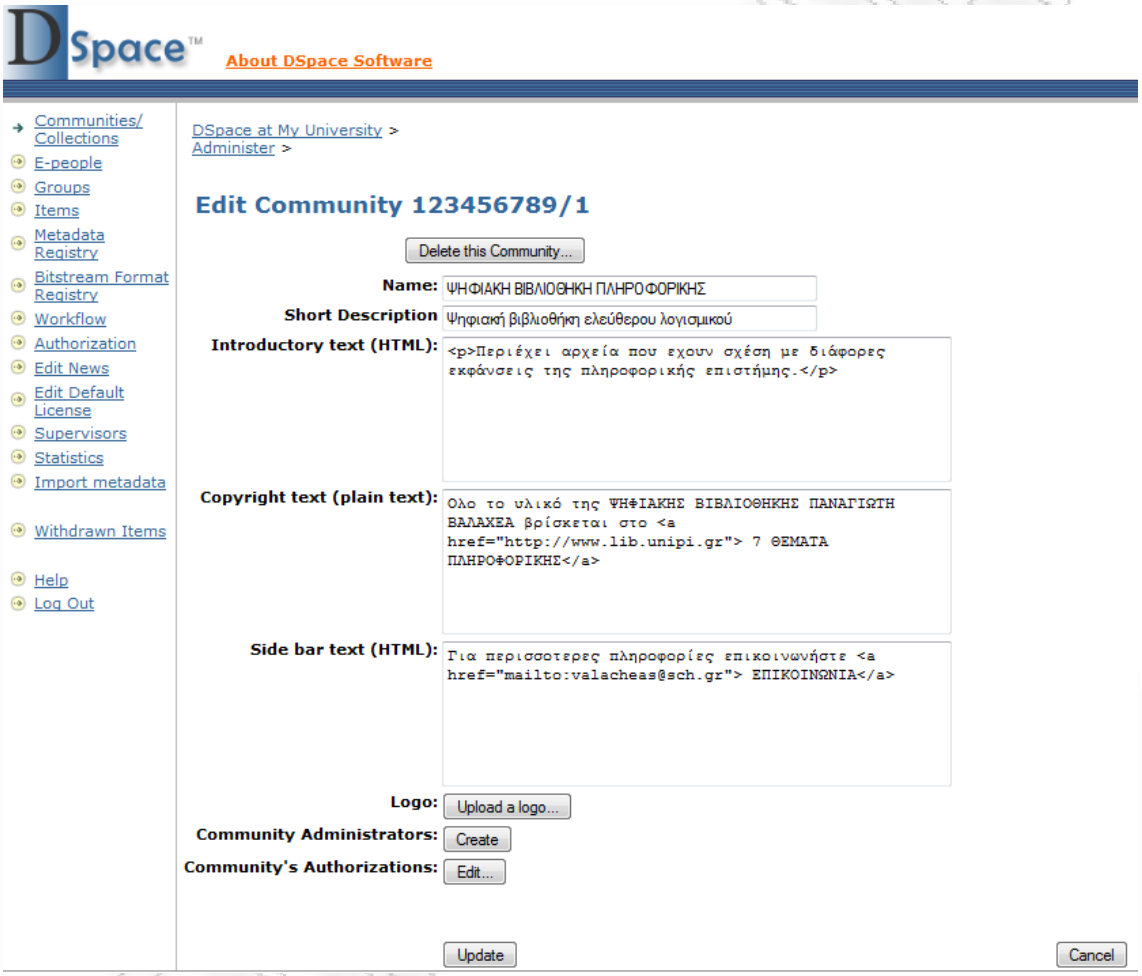
Δημιουργία κοινοτήτων-συλλογών

Ξεκινώντας το στήσιμο της ψηφιακής βιβλιοθήκης δώσαμε σε αυτή το όνομα <<Ψηφιακή βιβλιοθήκη ΠΑΝΑΓΙΩΤΗ ΒΑΛΑΧΕΑ >> που αναφέρεται στο όνομα του δημιουργού της. Σκεφτήκαμε το ψηφιακό υλικό που θα υπάρχει σε αυτή να προέρχεται από το χώρο της πληροφορικής. Να υπάρχουν επιστημονικά, έγκυρα papers που αντλήσαμε από διεθνή επιστημονικά περιοδικά. Βιβλία σε ηλεκτρονική μορφή με αναφορά σε κλάδους της πληροφορικής, όπως τεχνητή νοημοσύνη, δίκτυα. Σημειώσεις από διάφορα μαθήματα του τμήματος πληροφορικής του πανεπιστημίου Πειραιά. Το υλικό αυτό θα μπορεί στη συνέχεια να

εμπλουτίζεται και να είναι διαθέσιμο στο διαδίκτυο , τόσο σε φοιτητές του τμήματος, όσο και σε κάθε ενδιαφερόμενο ερευνητή.

Δημιουργία Κοινότητας (Community) << ΨΗΦΙΑΚΗ ΒΙΒΛΙΟΘΗΚΗ ΠΛΗΡΟΦΟΡΙΚΗΣ >>.

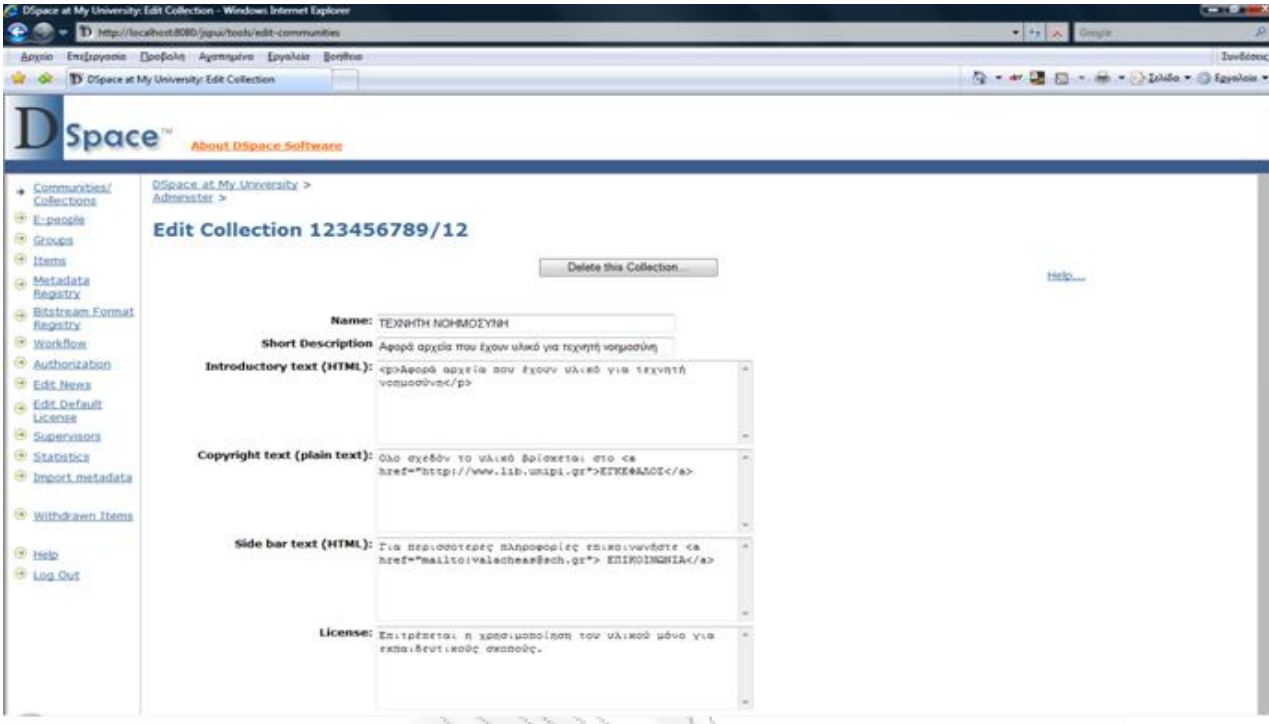
Στην αρχή δημιουργήσαμε μια κοινότητα που ονομάσαμε <<ΨΗΦΙΑΚΗ ΒΙΒΛΙΟΘΗΚΗ ΠΛΗΡΟΦΟΡΙΚΗΣ>>. Η φόρμα δημιουργίας κοινότητας έχει την παρακάτω μορφή.



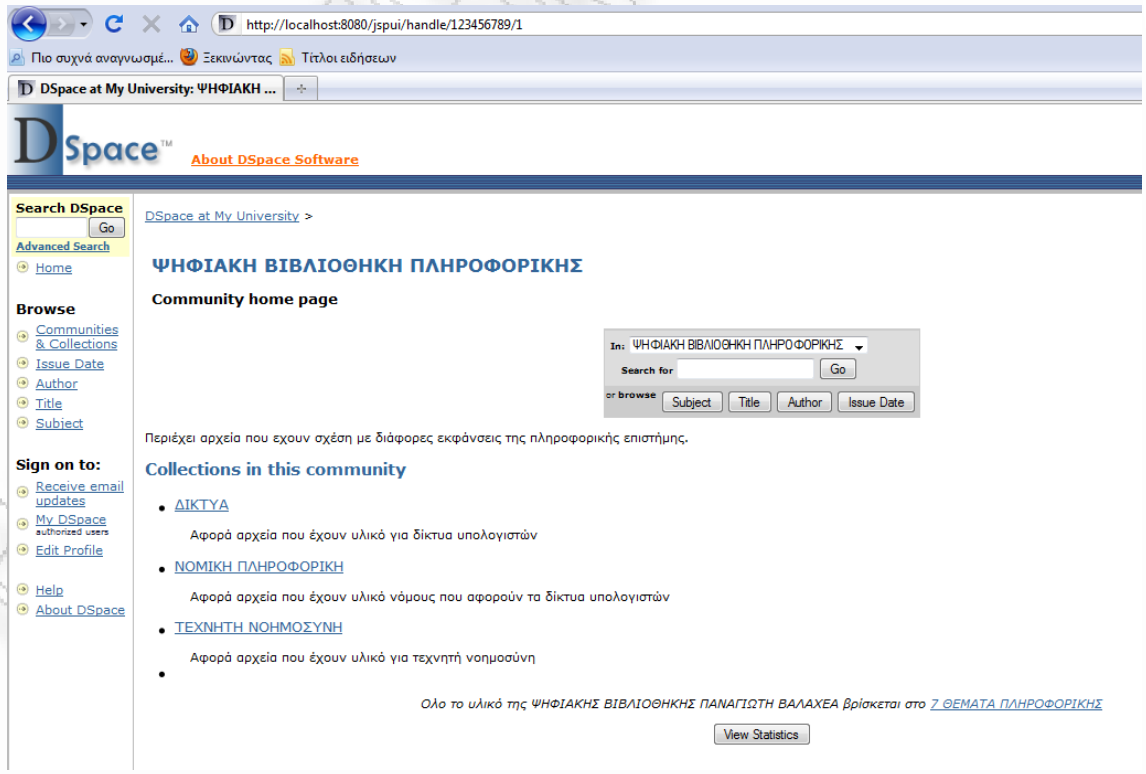
Δημιουργία Συλλογής (Collection)

Δημιουργήσαμε τη συλλογή Τεχνητή νοημοσύνη

Η φόρμα δημιουργίας συλλογής έχει την παρακάτω μορφή.



Με τον ίδιο τρόπο δημιουργήσαμε τις συλλογές ΔΙΚΤΥΑ και ΝΟΜΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ.



Ηλεκτρονική κατάρτιση συμβάσεων
Ψηφιακές υπογραφές

12.3 Παραμετροποίηση dspace

Παραμετροποίηση(configuration) της φόρμας καταχώρησης δεδομένων

Αρχείο input-forms.xml

[dspace]/config/input-forms.xml

[dspace-source]/dspace/ config/ input-forms.xml

Εισάγω τη φόρμα της συλλογής τεχνητή νοημοσύνη που αντιστοιχεί στον αριθμό ="123456789/12" προσθέτοντάς την στο χάρτη φορμών όπως φαίνεται παρακάτω:

```
<input-forms>
<form-map>
<name-map collection-handle="default" form-name="traditional" />
<name-map collection-handle="123456789/12" form-name="panos" />
</form-map>
```

Εισάγουμε πεδία(fields) στην φόρμα με το όνομα panos με τον παρακάτω τρόπο .Τα πεδία αυτά αντιστοιχούν στα 10 μεταδεδομένα (author ,title,date created, identifier,type, language,subject, description, medium, rights).

```
<form name="panos">
<page number="1">
<field>
<dc-schema>dc</dc-schema>
<dc-element>contributor</dc-element>
<dc-qualifier>author</dc-qualifier>
<repeatable>true</repeatable>
<label>Authors</label>
<input-type>name</input-type>
<hint>Enter the names of the authors of this item below.</hint>
<required></required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>title</dc-element>
<dc-qualifier></dc-qualifier>
<repeatable>false</repeatable>
<label>Title</label>
<input-type>onebox</input-type>
<hint>Enter the main title of the item.</hint>
<required>You must enter a main title for this item.</required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>date</dc-element>
<dc-qualifier>created</dc-qualifier>
<repeatable>false</repeatable>
```

<label>Date of creation
</label>
<input-type>date</input-type>
<hint>Please give the date of of creation
below. You can leave out the day and/or month if they aren't
applicable.</hint>
<required>You must enter at least the year.</required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>identifier</dc-element>
<dc-qualifier></dc-qualifier>
<!-- An input-type of qualdrop_value MUST be marked as repeatable -->
<repeatable>true</repeatable>
<label>Identifiers</label>
<input-type value-pairs-
name="common_identifiers">qualdrop_value</input-type>
<hint>If the item has any identification numbers or codes associated with
it, please enter the types and the actual numbers or codes below.</hint>
<required></required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>type</dc-element>
<dc-qualifier></dc-qualifier>
<repeatable>true</repeatable>
<label>Type</label>
<input-type value-pairs-name="common_types">dropdown</input-type>
<hint> Select the type(s) of content of the item. To select more than one
value in the list, you may have to hold down the "CTRL" or "Shift"
key.</hint>
<required></required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>language</dc-element>
<dc-qualifier>iso</dc-qualifier>
<repeatable>false</repeatable>
<label>Language</label>
<input-type value-pairs-
name="common_iso_languages">dropdown</input-type>
<hint>Select the language of the main content of the item. If the language
does not appear in the list below, please select 'Other'. If the content does
not really have a language (for example, if it is a dataset or an image)
please select 'N/A'.</hint>
<required></required>

```
</field>
</page>
<page number="2">
<field>
<dc-schema>dc</dc-schema>
<dc-element>subject</dc-element>
<dc-qualifier></dc-qualifier>
<!-- An input-type of twobox MUST be marked as repeatable -->
<repeatable>true</repeatable>
<label>Subject Keywords</label>
<input-type>twobox</input-type>
<hint> Enter appropriate subject keywords or phrases below. </hint>
<required></required>
<vocabulary>srsc</vocabulary>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>description</dc-element>
<dc-qualifier></dc-qualifier>
<repeatable>false</repeatable>
<label>Description</label>
<input-type>textarea</input-type>
<hint> Enter any other description or comments in this box. </hint>
<required></required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>format</dc-element>
<dc-qualifier>medium</dc-qualifier>
<repeatable>false</repeatable>
<label>Medium</label>
<input-type>onebox</input-type>
<hint> Enter physical medium in this box. </hint>
<required></required>
</field>
<field>
<dc-schema>dc</dc-schema>
<dc-element>rights</dc-element>
<dc-qualifier></dc-qualifier>
<repeatable>false</repeatable>
<label>Rights</label>
<input-type>textarea</input-type>
<hint> Enter the rights of this issue in this box. </hint>
<required></required>
```

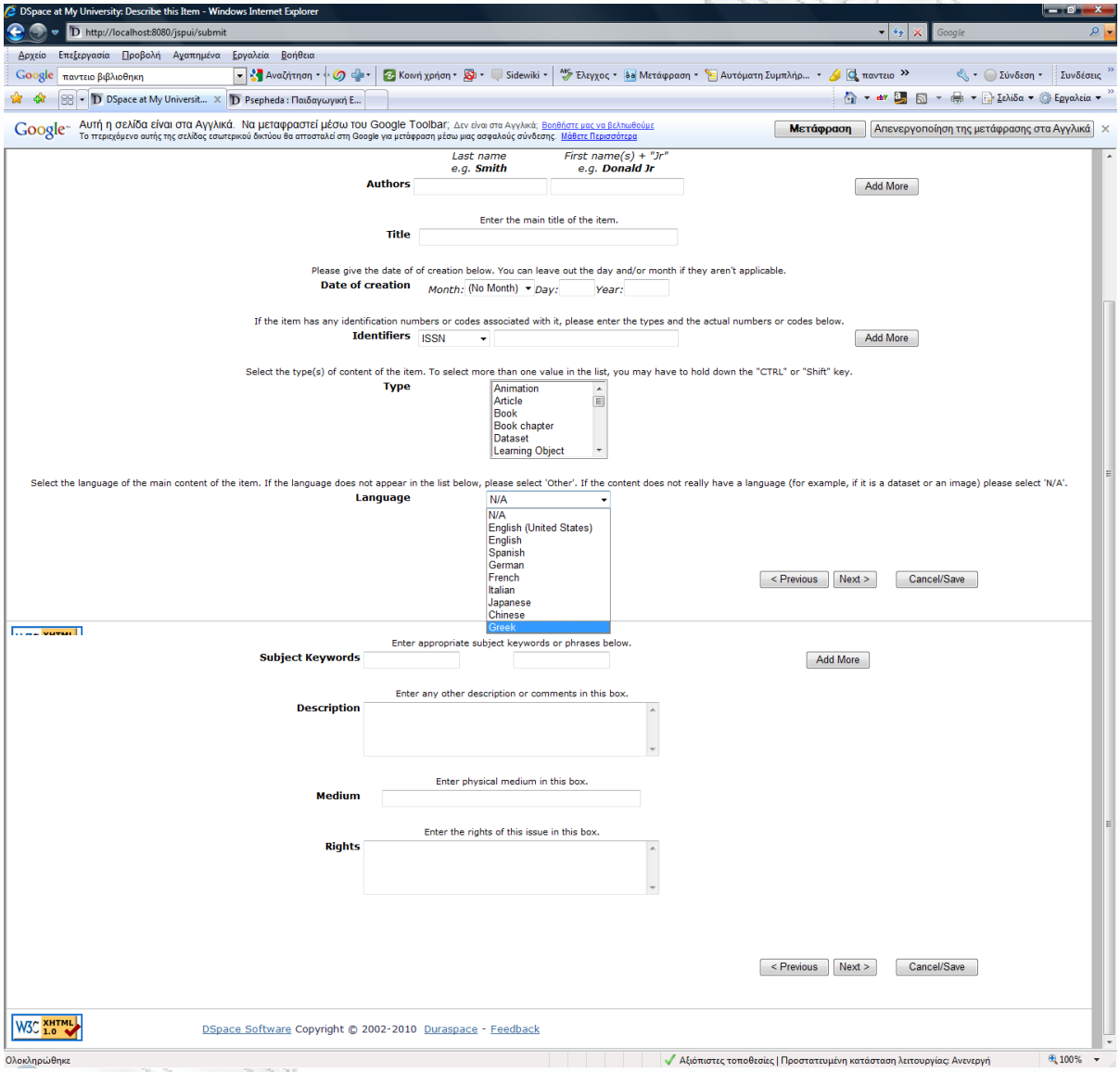
```
</field>
</page>
</form>
```

Παρακάτω φαίνεται ο κώδικας με τον οποίο επιλέγεται η γλώσσα του metadata Language. Εμείς προσθέτουμε κώδικα για την εμφάνιση της ελληνικής γλώσσας.

```
<form-value-pairs>
<value-pairs value-pairs-name="common_iso_languages" dc-term="language_iso">
<pair>
<displayed-value>N/A</displayed-value>
<stored-value></stored-value>
</pair>
<pair>
<displayed-value>English (United States)</displayed-value>
<stored-value>en_US</stored-value>
</pair>
<pair>
<displayed-value>English</displayed-value>
<stored-value>en</stored-value>
</pair>
<pair>
<displayed-value>Spanish</displayed-value>
<stored-value>es</stored-value>
</pair>
<pair>
<displayed-value>German</displayed-value>
<stored-value>de</stored-value>
</pair>
<pair>
<displayed-value>French</displayed-value>
<stored-value>fr</stored-value>
</pair>
<pair>
<displayed-value>Italian</displayed-value>
<stored-value>it</stored-value>
</pair>
<pair>
<displayed-value>Japanese</displayed-value>
<stored-value>ja</stored-value>
</pair>
<pair>
<displayed-value>Chinese</displayed-value>
<stored-value>zh</stored-value>
</pair>
<pair>
```

<displayed-value>Greek</displayed-value>
<stored-value>gr</stored-value>
</pair>
</value-pairs>
</form-value-pairs>
</input-forms>

Η παραπάνω φόρμα καταχώρησης εμφανίζεται ως έξής:



Παραμετροποίηση(configuration) του dspace

Αρχείο dspace.cfg

[dspace]/config/dspace.cfg

[dspace-source]/dspace/ config/dspace.cfg

Εισάγουμε τα μεταδεδομένα που θα έχει το τεκμήριο (item) στο αρχείο dspace.cfg

"metadata.dc.title"

"metadata.dc.contributor.author"

“metadata.dc.date.created"

"metadata.dc.subject"

"metadata.dc.type"

"metadata.dc.format.medium"

"metadata.dc.rights"

"metadata.dc.description"

"metadata.dc.identifier.uri"

"metadata.dc.language.iso"

Τα μεταδεδομένα που θα εμφανισθούν στην απλή μορφή του τεκμηρίου item καθορίζονται από την παρακάτω εντολή :

webui.itemdisplay.default = dc.title, dc.title.alternative,
dc.contributor.author, \
dc.subject, dc.date.issued(date),
dc.publisher, \
dc.identifier.citation,
dc.relation.ispartofseries, \
dc.description.abstract,
dc.description,\
dc.identifier.govdoc, dc.identifier.uri
(link), \
dc.identifier.isbn, dc.identifier.issn,\
dc.identifier.ismn, dc.identifier

Μπορούμε να αλλάξουμε την απλή εμφάνιση του τεκμηρίου (item) επιλέγοντας τα πεδία (fields) καθώς και την σειρά τους .

webui.itemdisplay.default = dc.contributor.author(link), dc.title(link),
dc.subject, dc.date.issued(date),
dc.description , dc.identifier.uri(link),
dc.identifier.isbn,
dc.identifier.issn,dc.identifier.govdoc
dc.identifier.ismn, dc.identifier

Παραμετροποίηση (configuration) του dspace

Αρχείο Messages.properties

[dspace-source]/dspace-api/src/main/resourses /Messages.properties

Εισάγουμε όλα τα μεταδεδομένα και τα ονόματά τους με τα οποία θέλουμε να εμφανίζονται.

metadata.dc.contributor.author = Authors

metadata.dc.contributor.editor = Editors
metadata.dc.date.issued = Issue Date
metadata.dc.description = Description
metadata.dc.description.abstract = ShortAbstract
metadata.dc.identifier = Other Identifiers
metadata.dc.identifier.citation = Citation
metadata.dc.identifier.govdoc = Gov't Doc #
metadata.dc.identifier.isbn = ISBN
metadata.dc.identifier.ismn = ISMN
metadata.dc.identifier.issn = ISSN
metadata.dc.identifier.uri = URI
metadata.dc.publisher = Publisher
metadata.dc.relation.ispartofseries = Series/Report no.
metadata.dc.subject = Keywords
metadata.dc.title = Title
metadata.dc.title.alternative = Other Titles
metadata.dc.date.created = Create Date
metadata.dc.type = Type
metadata.dc.format.medium = Medium
metadata.dc.rights = Rights
metadata.dc.language.iso = Language

Μπορούμε να αλλάξουμε τους τίτλους στην σελίδα του dspace.
Με τον παρακάτω τρόπο τοποθετούμε τους τίτλους στην navigation bar που βρίσκεται στο αριστερό μέρος της σελίδας.

jsp.layout.navbar-default.advanced = Advanced Search
jsp.layout.navbar-default.authors = Authors
jsp.layout.navbar-default.browse = Browse
jsp.layout.navbar-default.communities-collections = Communities
& Collections
jsp.layout.navbar-default.date = By Date
jsp.layout.navbar-default.edit = Edit Profile
jsp.layout.navbar-default.go = Go
jsp.layout.navbar-default.help = Help
jsp.layout.navbar-default.home = Home
jsp.layout.navbar-default.subjects = Subjects
jsp.layout.navbar-default.subjectsearch = Subject Search
jsp.layout.navbar-default.titles = Titles
jsp.layout.navbar-default.users = My DSpace
jsp.layout.navbar-default.users-authorized = <small>authorized users</small>
jsp.layout.navbar-default.display-statistics = View Statistics

13 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Davies D. W and W. L. Price, Security for Computer Networks, John Wiley & Sons, 1989.
2. Salomaa, A. ,Public Key Cryptography, Springer-Verlag, 1990.
3. Αλεξανδρίδου Ελίζα, Το δίκαιο του ηλεκτρονικού εμπορίου, Σάκκουλας Αθήνα Θεσσαλονίκη ,2004.
4. Γεωργιάδης Γεώργιος, Η σύναψη συμβάσεως μέσω του διαδικτύου, Αντ. Σάκκουλας Αθήνα Κομοτηνή, 2003.
5. Δελούκα — Ιγγλέση Κορνηλία, Νομικά Θέματα Ηλεκτρονικού Εμπορίου, Αντ. Σάκκουλας Αθήνα Κομοτηνή, 2005.
6. Ζορκάδης,Β, Κρυπτογραφία, ΕΑΠ,2002.
7. Ιγγλεζάκης Ιωάννης, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Σάκκουλας Αθήνα - Θεσσαλονίκη ,2003.
8. Καράκωστας Ιωάννης, Δίκαιο & Internet - Νομικά ζητήματα του διαδικτύου, Π.Ν. Σάκκουλας Αθήνα ,2003 ,2η έκδοση.
9. Μανιώτης Δημήτριος, Η σύναψη της ηλεκτρονικής συμβάσεως και η ευθύνη των παρεχόντων συνδρομή στην κατοχύρωση της γνησιότητας και του αναλλοίωτου των ηλεκτρονικών εγγράφων, Αντ. Σάκκουλας Αθήνα Κομοτηνή, 2003.
10. Μανιώτης Δημήτριος, Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο, Αντ. Σάκκουλας Αθήνα ,1998.
11. Παπαντωνίου, Γενικές αρχές του αστικού δικαίου, 3η έκδ. 1983 .
12. Πιτσιρίκος Ιωάννης, Σύγχρονα μέσα επικοινωνίας (τηλεομοιότυπο, τηλετύπημα, ηλεκτρονικό έγγραφο) για την κατάρτιση τυπικών δικαιοπραξιών ως ζήτημα της σχέσεως έγγραφου τύπου και δικαιοπραξίας, Αντ. Σάκκουλας Αθήνα ,2002.
13. Σιδηρόπουλος Θεόδωρος, Το δίκαιο του διαδικτύου, Σάκκουλας Αθήνα-Θεσσαλονίκη ,2003.
14. Σινανιώτη-Μαρούδη Αριστέα, Ιωάννης Δ. Φαρσαρώτας, Ηλεκτρονική τραπεζική, Σάκκουλας, 2005 .
15. Χριστοδούλου Κωνσταντίνος, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, Αντ. Σάκκουλας Αθήνα ,2001.
16. Χρυσάνθης Χρ, Η ηλεκτρονική εξυπηρέτηση των σύγχρονων τραπεζικών συναλλαγών, Αθήνα-Κομοτηνή ,1997.
17. Ψούνη — Ζορμπά Νίκη, Δήλωση βουλήσεως μέσω ηλεκτρονικού υπολογιστή. Ένταξη στο σύστημα του Α.Κ. - Δυνατότητες ακύρωσης, Σάκκουλας Θεσσαλονίκη ,1988.
18. Καραδημητρίου Κοσμάς, Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Σάκκουλας Αθήνα, 2008 .

14 ΜΕΛΕΤΕΣ ΑΡΘΡΑ

1. Diffie – Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, n. 6,1976, pp. 644-654.
2. El Gamal, A Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, Vol. 31, 1981, pp. 469-473.
3. Giussani, A. The Challenge of Information Society: Application of Advanced Technologies in Civil Litigation and other Procedures. Italien Report, XI. World Congress on Procedural Law, Vienna 1999.
4. Kristula, The History of the Internet, 2001, στην ηλεκτρονική διεύθυνση http://www.davesite.com/webstation/net-history.html.
5. Merkle R., Hellman M., Hiding Information and Signatures in Trapdoor Knapsacks , IEEE Transactions Information Theory, v. 24, n. 5, 1978, 525-530.
6. R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems , Communications of the ACM, vol. 21, 1978, pp. 120-126.
7. Shannon, C. E., Communication Theory of Secrecy Systems, Bell System Technical Journal, v. 28, n. 4, 1999, pp. 656-715 .
8. Takach , Internet Law: Dynamics, Themes and Skill Sets, The Canadian Business Law Journal, Volume 32 (1999), 1.
9. Zorkadis V, Improving the Quality of Secure Distributed Systems , Proc. Of 3rd Intern. Conference on Reliability, Quality & Safety of Software-Intensive Systems, Chapman & Hall, 1997, pp. 186-197 .
10. Zorkadis, Security vs. Performance Requirements in Data Communication Systems, Proc. of Third European Symposium on Research in Computer Security, Lecture Notes in Computer Science 875, 1994, Springer-Verlag, pp. 19-30.
11. ΑΚ https://www.nbonline.gr/actions.
12. Γκοτσοπούλου, «Ηλεκτρονικό εμπόριο και δικαιόχρηση (franchising)», ΔΕΕ (3) 2002, σελ. 250 .
13. Ζέκο, «Franchising και Cyberspace», ΔΕΕ (1) 2001, σελ. 52 .
14. Καραδημητρίου Κοσμάς, Ηλεκτρονικές υπογραφές: προβλήματα και σκέψεις με αφορμή το Π.Δ. 150/2001., Αρμ. 2002 σελ. 1535 .
15. Καράσης Μαρίνος, Τα όρια της ελεύθερης κοινωνικής δράσεως στο Διαδίκτυο , ΕπισκΕμπΔ. Β/2005 σελ. 281 .
16. Κουσούλης Στέλιος, Παρατηρήσεις σε ΜΠρΑθ 1327/2001, ΔΕΕ 2001, σελ. 377
17. Κυρλόγλου, «Ασφαλείς συναλλαγές στο Διαδίκτυο», περιοδικό «Ανάπτυξη» του ΕΒΕΑ, (10) 2001,σσ.82 επ., διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.acci.gr/anaptixi/1001/82-85.pdf .
18. Κυρλόγλου, «Βιομετρικά συστήματα πιστοποίησης - οι συνηθέστερες μέθοδοι πιστοποίησης της ταυτότητας», περιοδικό «Ανάπτυξη» του ΕΒΕΑ, (5) 2002, σελ.81 επ., διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.acci.gr/anaptixi/0502/81-82.pdf.
19. Λιναρίτης Ιωάννης, Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 της Ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο με το Π.Δ. 150/2001. ΔΕΕ 2002 σελ. 257 .
20. Μακρής Σπύρος, Η προστασία του καταναλωτή στα πλαίσια του ηλεκτρονικού εμπορίου μετά τη μεταφορά των Οδηγιών 97/7/ΕΚ και 2000/31/ΕΚ στο ελληνικό δίκαιο. ΔΕΕ 2004 σελ. 882 .
21. Μιχαηλίδου Χρυσούλα, Το πρόβλημα της ηλεκτρονικής υπογραφής. Δίκη 31 (2000) σελ. 1188 .

22. Πανάγου Θεόδωρος, Το ηλεκτρονικό διοικητικό έγγραφο δημιουργία και διαχείριση. ΝοΒ 54 σελ. 161 .

23. Πανάγου, Το ηλεκτρονικό διοικητικό έγγραφο δημιουργία και διαχείριση. ΝοΒ 54, 163-164.

24. Παπαθωμά-Μπέτγκε Α. Ηλεκτρονικό εμπόριο: Νομικά ζητήματα κατά τη σύναψη εμπορικών συμβάσεων στο Internet, ΔΕΕ 1999, σελ. 1237-1242.

25. Σπυρόπουλος Στέργιος, Η διάκριση των παρόχων υπηρεσιών στο διαδίκτυο και η οριοθέτηση της ευθύνης τους με βάση την κοινοτική Οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο. ΔιΜΕΕ 3/2005 σελ. 372 .

26. Χάνος Αντώνιος, Δίκαιο και τεχνολογική εξέλιξη στην κοινωνία των πληροφοριών - Με παράδειγμα το διοικητικό δίκαιο - ΕΕΝ 2000 σελ. 7 .

27. Χριστοδούλου Κωνσταντίνος, Ουσιαστικού και δικονομικού δικαίου ιδιαιτερότητες του καθεστώτος των ηλεκτρονικών δικτύων. Δ 2004 σελ. 417 .

15 ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

https://www.nbonline.gr/actions

www.statistics.gr

www.pewinternet.org

www.eett.gr

www.naftemporiki.gr

www.icann.org

www.wipo.int

www.uncitral.org

www.dsa.gr

http://www.ukdg.de

http://www.law.kuleuven.ac.be/icri.projects/tables.htm

http://www.dsanet.gr

http://www.ispo.cec.be/eif/policy/97503.html