ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Ψηφιακές υπογραφές»

Πτυχιακή εργασία της φοιτήτριας
Χρυσοπούλου Ελένης (Α.Μ. 02/07)

Επιβλέπων Καθηγητής: **Στεφανίδης Γεώργιος, Αν. Καθηγητής**

Εξεταστική Επιτροπή: **Στεφανίδης Γεώργιος, Αν. Καθηγητής**
Χρήστου- Βαρσακέλης Δημήτριος, Λέκτορας

Θεσσαλονίκη, Δεκέμβριος 2008

Περιεχόμενα

Σκοπός
Σκοπός αυτής της εργασίας είναι η εξερεύνηση των συνόρων μεταξύ του τεχνικού και του νομικού κόσμου της κρυπτογραφίας, με ιδιαίτερη έμφαση στις υπογραφές, τις συμβάσεις και τις ερμηνείες τους.

Λέξεις- κλειδιά
Κρυπτογραφία, ηλεκτρονικές υπογραφές, ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά, ηλεκτρονικές συμβάσεις, νομοθετικό πλαίσιο, Οδηγία 99/93/ΕΚ, π.δ. 150/2001, Οδηγία 2000/31/ΕΚ, π.δ. 131/2003.

1. ΕΙΣΑΓΩΓΗ

1.1 Η κρυπτογραφία και οι στόχοι της

Η κρυπτογραφία ορίζεται στο Handbook of Applied Cryptography [1] ως η μελέτη των μαθηματικών τεχνικών που σχετίζονται με τομείς της ασφάλειας πληροφοριών όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η ταυτοποίηση αυθεντικότητας οντότητας και η ταυτοποίηση αυθεντικότητας της πηγής των δεδομένων.

Η εμπιστευτικότητα αφορά την απόκρυψη του περιεχομένου μίας μεταβίβασης από οποιονδήποτε πλην των εξουσιοδοτημένων να έχουν πρόσβαση σε αυτήν. Εναλλακτικά, χρησιμοποιούνται οι όροι μυστικότητα και ιδιωτικότητα. Υπάρχουν πολλές προσεγγίσεις για την επίτευξη της εμπιστευτικότητας που κυμαίνονται από φυσική προστασία μέχρι μαθηματικούς αλγορίθμους που καθιστούν τα δεδομένα μη αναγνώσιμα.

Η ακεραιότητα των δεδομένων αφορά την προστασία από μη εξουσιοδοτημένη αλλαγή των δεδομένων που μεταβιβάζονται. Η αλλαγή των δεδομένων μπορεί να έγκειται σε προσθήκη, διαγραφή, ή αντικατάσταση δεδομένων.

Η ταυτοποίηση αυθεντικότητας μπορεί να αφορά την ταυτοποίηση του αποστολέα, του παραλήπτη ή και των ίδιων των δεδομένων που μεταβιβάζονται. Συγκεκριμένα, η ταυτοποίηση αυθεντικότητας σχετίζεται συχνότερα με την δυνατότητα του παραλήπτη να επιβεβαιώνει ότι το μήνυμα προέρχεται πράγματι από τον συγκεκριμένο αποστολέα και δεν έχει τροποποιηθεί καθ' οδόν από τρίτο μη εξουσιοδοτημένο πρόσωπο.

Η μη απάρνηση αφορά την αδυναμία μίας οντότητας να αρνηθεί ότι προέβη σε ενέργειες στις οποίες πράγματι προέβη στο παρελθόν. Για παράδειγμα, αν μία οντότητα εξουσιοδοτήσει μία άλλη οντότητα για την αγορά περιουσιακού στοιχείου για λογαριασμό της πρώτης, η δεύτερη οντότητα θα πρέπει να μπορεί να εξασφαλίσει ότι η πρώτη δεν θα αμφισβητήσει την εξουσιοδότηση που της παρείχε σε προγενέστερο χρόνο. Η μη απάρνηση αναλύεται σε παρακάτω ενότητα.

Δεν είναι δύσκολο να πειστούμε ότι για να επικοινωνούμε με ασφάλεια, πρέπει να υπάρχει κάτι που το γνωρίζει το ένα μέλος, ή που μπορεί να το κάνει, το οποίο ο αντίπαλος δεν γνωρίζει, ή δεν μπορεί να το κάνει. Πρέπει να υπάρχει κάποια "ασυμμετρία" μεταξύ της θέσης (κατάστασης) στην οποία βρίσκονται τα μέλη και της θέσης (κατάστασης) στην οποία βρίσκεται ο αντίπαλος.

Το μοντέλο εμπιστοσύνης (trust model) καθορίζει ποιος, αρχικά, έχει τα κλειδιά (και ποιά). Υπάρχουν δύο κεντρικά μοντέλα εμπιστοσύνης: το συμμετρικό (ή κοινού κλειδιού ή ιδιωτικού κλειδιού) μοντέλο και το ασύμμετρο (ή δημόσιου κλειδιού) μοντέλο εμπιστοσύνης.

2. ΟΙ ΟΡΟΙ

2.1 Ηλεκτρονικό αντικείμενο

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

Κατά την νομική θεωρία, το ηλεκτρονικό έγγραφο είναι ένα σύνολο δεδομένων, τα οποία έχουν εγγραφεί στον μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή και μπορούν να αποτυπωθούν κατά τρόπο αναγνώσιμο στην οθόνη του υπολογιστή, ενδεχομένως δε και να εκτυπωθούν σε υλικό φορέα με την μορφή κειμένου ή εικόνων [2].

Εναλλακτικά χρησιμοποιούνται οι όροι αρχείο ή συλλογή από bytes. Σε περίπτωση αντιγραφής ενός ηλεκτρονικού αντικειμένου, το αντίγραφο που προκύπτει αποτελείται από ταυτόσημη ακολουθία bits και η ηλεκτρονική υπογραφή που θα παραχθεί από το κάθε αντίγραφο θα είναι ίδια με αυτήν του πρωτοτύπου.

2.2 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 [3]. Το ηλεκτρονικό αντικείμενο που εξάγεται από τον αλγόριθμο κατακερματισμού ονομάζεται σύνοψη του αρχικού μηνύματος. Οποιαδήποτε αλλαγή του ηλεκτρονικού αντικειμένου που εισάγεται στον αλγόριθμο οδηγεί, με μεγάλη πιθανότητα, σε διαφορετική σύνοψη. Αντίθετα, όταν εισάγεται το ίδιο αντικείμενο στον αλγόριθμο κατακερματισμού, η σύνοψη που εξάγεται είναι ακριβώς η ίδια.

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.

2.3 Επίθεση γενεθλίων

Είναι σημαντικό να σημειωθεί ότι η δυνατότητα παραγωγής δύο εγγράφων με την ίδια σύνοψη μπορεί να είναι χρήσιμη για κάποιον κακόβουλο και μάλιστα είναι σαφώς ευκολότερο από την παραγωγή ενός εγγράφου με συγκεκριμένη σύνοψη.

Η μέθοδος για να πραγματοποιηθεί αυτό είναι γνωστή ως "επίθεση γενεθλίων" και ονομάζεται έτσι επειδή αν ερωτηθεί μία ομάδα ατόμων άνω των 25 ετών για τα γενέθλιά της, υπάρχει μεγάλη πιθανότητα δύο από αυτούς να έχουν την

ίδια ημέρα γενέθλια, γεγονός που εκπλήσσει τους περισσότερους καθώς θεωρούν ότι θα χρειαζόταν ένας μεγαλύτερος αριθμός ατόμων για να παραχθεί αυτό το αποτέλεσμα. Αυτό είναι γενικά αληθές για οποιαδήποτε τυχαία λίστα επιλεγμένη από ένα πεπερασμένο σύνολο.

Για να εφαρμοστεί αυτή η επίθεση στις συνόψεις αντικειμένων, πρέπει να πραγματοποιηθούν μία σειρά από ανακόλουθες αλλαγές σε δύο αντικείμενα και κάθε φορά να παράγεται μία σύνοψή τους, ώστε να παραχθεί μία λίστα από συνόψεις για το κάθε αντικείμενο. Μετά από ένα πλήθος προσπαθειών, περίπου ίσο με την τετραγωνική ρίζα του πλήθους των πιθανών τιμών σύνοψης, υπάρχει μεγάλη πιθανότητα ότι κάποια εκδοχή των δύο αντικειμένων που παράγουν την ίδια σύνοψη θα έχει κατασκευαστεί.

Στόχος αυτής της επίθεσης συνήθως είναι να υπογραφεί από το θύμα το ένα έγγραφο και στην συνέχεια να χρησιμοποιηθεί η υπογραφή του σαν να υπέγραψε το άλλο. Για την αποφυγή της παραπάνω επίθεσης, οι συναρτήσεις κατακερματισμού θα πρέπει να παράγουν αρκούντως μεγάλες συνόψεις. Συγκεκριμένα, επειδή αυτή η επίθεση ελαττώνει αποτελεσματικά την δυσκολία μίας επίθεσης στο περίπου μισό του πλήθους των bits της σύνοψης, οι συναρτήσεις κατακερματισμού πρέπει να παράγουν διπλάσια σύνοψη για να είναι ασφαλείς.

2.4 Κρυπτογραφία ιδιωτικού κλειδιού (συμμετρικό περιβάλλον)

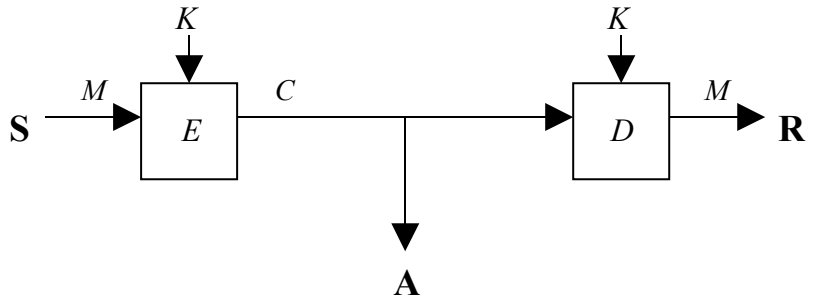
Στην πράξη, το απλούστερο και επίσης συνηθέστερο περιβάλλον είναι αυτό στο οποίο ο αποστολέας και ο παραλήπτης μοιράζονται ένα κλειδί (key) το οποίο δεν γνωρίζει ο αντίπαλος. Αυτό λέγεται συμμετρικό περιβάλλον ή συμμετρικό μοντέλο εμπιστοσύνης. Οι διαδικασίες ενθυλάκωσης και αποθυλάκωσης θα εξαρτώνται από αυτό το ίδιο κοινό κλειδί. Το κοινό κλειδί είναι συνήθως ένα ομοιόμορφα κατανεμημένο τυχαίο αλφαριθμητικό (string) που έχει κάποιο πλήθος bit, k. Ο αποστολέας και ο παραλήπτης πρέπει με κάποιον τρόπο να χρησιμοποιούν το κλειδί K για να παρακάμπτουν την παρουσία του αντιπάλου.

Το συμμετρικό μοντέλο δεν ενδιαφέρεται με το πώς τα δύο μέλη απέκτησαν το κλειδί αλλά με το πώς το χρησιμοποιούν. Στην κρυπτογραφία υποθέτουμε ότι το μυστικό κλειδί διατηρείται με ασφάλεια από το μέλος που το χρησιμοποιεί. Αν διαφυλάσσεται σε έναν υπολογιστή, υποθέτουμε ότι ο αντίπαλος δεν μπορεί να εισδύσει στη μηχανή και να ανακτήσει το κλειδί. Η εξασφάλιση ότι αυτή η υπόθεση είναι αληθής είναι αντικείμενο της ασφάλειας συστημάτων υπολογιστών.

Ένα πρωτόκολλο που χρησιμοποιείται για να παρέχει μυστικότητα στο συμμετρικό περιβάλλον λέγεται ότι είναι ένα "σχήμα συμμετρικής κρυπτογράφησης" (symmetric encryption scheme). Για να καθορίσουμε ένα τέτοιο σχήμα Π, πρέπει να καθορίσουμε τρεις αλγορίθμους, οπότε ένα τέτοιο σχήμα είναι μια τριάδα αλγορίθμων, Π = (□, □, □). Σε αυτά τα πλαίσια, ο αλγόριθμος ενθυλάκωσης που αναφέραμε παραπάνω, λέγεται αλγόριθμος "κρυπτογράφησης" (encryption) και είναι ο αλγόριθμος □. Το μήνυμα M που θέλει να μεταβιβάσει ο αποστολέας είναι το λεγόμενο "απλό κείμενο" (plain text). Ο αποστολέας κρυπτογραφεί το απλό κείμενο με τη βοήθεια του κοινού κλειδιού K εφαρμόζοντας τον αλγόριθμο □ στα K και M προκειμένου να πάρει το "κρυπτοκείμενο" (ciphertext) C. Το κρυπτοκείμενο μεταβιβάζεται στον παραλήπτη. Η αναφερθείσα παραπάνω διαδικασία αποθυλάκωσης, σε αυτά τα πλαίσια, λέγεται αλγόριθμος "αποκρυπτογράφησης" (decryption) και είναι ο αλγόριθμος □. Ο παραλήπτης εφαρμόζει τον □ στα K και C.

Η διαδικασία αποκρυπτογράφησης μπορεί να είναι ανεπιτυχής, κάτι που υποδηλώνεται με την επιστροφή ενός ειδικού συμβόλου ⊥, αλλά αν είναι επιτυχής,

οφείλει να επιστρέψει το μήνυμα που είχε αρχικά κρυπτογραφηθεί. Ο πρώτος αλγόριθμος στο Π είναι ο αλγόριθμος "δημιουργίας κλειδιών" (γεννήτρια κλειδιών — key generator) ο οποίος καθορίζει τον τρόπο με τον οποίο επιλέγεται το κλειδί. Στις περισσότερες περιπτώσεις ο αλγόριθμος αυτός επιστρέφει απλώς ένα τυχαίο αλφαριθμητικό με μήκος το μήκος του κλειδιού. Ο αλγόριθμος κρυπτογράφησης μπορεί να είναι "τυχαιοποιημένος" (randomized) ή όχι.



Εικ. 2.1: Συμμετρική κρυπτογράφηση. Ο αποστολέας *S* και ο παραλήπτης *R* μοιράζονται ένα μυστικό κλειδί, *K*. Ο αντίπαλος *A* στερείται αυτό το κλειδί. Το μήνυμα *M* είναι το απλό κείμενο· το μήνυμα *C* είναι το κρυπτοκείμενο.

Το σχήμα κρυπτογράφησης δεν λέει στον αντίπαλο τι να κάνει. Δεν αποκαλύπτει πως το κλειδί, άπαξ και δημιουργηθεί, περικλείεται στα χέρια των δύο μελών. Δεν λέει επίσης πώς μεταβιβάζονται τα μηνύματα. Λέει μόνο πώς δημιουργούνται τα κλειδιά και πως τα δεδομένα επεξεργάζονται.

Ο σκοπός ενός σχήματος συμμετρικής κρυπτογράφησης είναι να μην είναι σε θέση ένας αντίπαλος, ο οποίος παίρνει το κρυπτοκείμενο, να μάθει οτιδήποτε για το απλό κείμενο. Τι σημαίνει πάντως αυτό δεν είναι σαφές και αποτελεί αντικείμενο συζήτησης ο ορισμός της μυστικότητας.

Ένα πράγμα που δεν κάνει η κρυπτογράφηση είναι η απόκρυψη του μήκους ενός αλφαριθμητικού απλού κειμένου. Αυτό συνήθως είναι ανακτήσιμο από το μήκος του αλφαριθμητικού κρυπτοκειμένου.

Ως ένα παράδειγμα των ζητημάτων που εμπλέκονται στην προσπάθειά μας να ορίσουμε τη μυστικότητα, ας αναρωτηθούμε το κατά πόσο θα μπορούσαμε να πούμε ότι είναι αδύνατο να καταλάβει ο αντίπαλος το *M* δοθέντος του *C*. Κάτι τέτοιο όμως δεν ευσταθεί αφού ο αντίπαλος θα μπορούσε να προβλέψει το *M* εξάγοντας μια τυχαία ακολουθία των $n = |M|$ bit, γιατί όπως προαναφέραμε το μήκος του απλού κειμένου είναι συνήθως υπολογίσιμο από το μήκος του κρυπτοκειμένου. Θα μπορούσε να το πετύχει με πιθανότητα 2^{-n}. Κάτι τέτοιο δεν υποδηλώνει ότι το σχήμα είναι κακό. Απλώς μας λέει ότι η ασφάλεια είναι ένα πιθανοτικό πράγμα. Το σχήμα δεν είναι ασφαλές ή ανασφαλές, απλώς υπάρχει κάποια πιθανότητα να το "σπάσουμε".

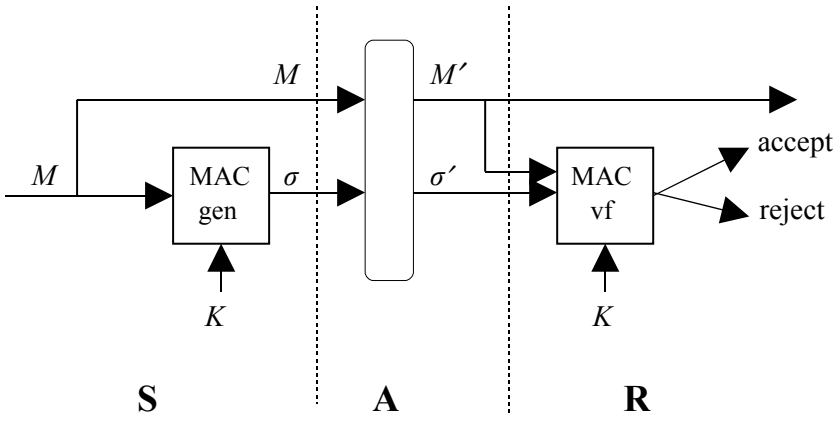
Ένα άλλο θέμα είναι η a priori γνώση. Πριν μεταβιβαστεί το *M*, μπορεί ο αντίπαλος να ξέρει κάτι γι' αυτό. Για παράδειγμα, ότι το M είναι 0^n ή 1^n, κι αυτό γιατί ξέρει ότι πρόκειται για ένα μήνυμα αγοράς ή πώλησης μιας μετοχής. Τώρα, μπορεί πάντα να παίρνει το μήνυμα με πιθανότητα ½. Το ερώτημα που εύλογα τίθεται είναι πώς μπορεί να αντιμετωπιστεί αυτό.

Μέχρι τώρα μπορεί κάποιος να φανταστεί ότι ένας αντίπαλος, ο οποίος προσβάλει τη μυστικότητα ενός σχήματος κρυπτογράφησης, είναι παθητικός λαμβάνοντας απλώς και εξετάζοντας κρυπτοκείμενα. Στην πραγματικότητα αυτό

μπορεί να μη συμβαίνει καθόλου. Πρέπει να θεωρούμε αντιπάλους οι οποίοι είναι πολύ πιο ισχυροί.

Στο πρόβλημα πιστοποίησης της αυθεντικότητας του μηνύματος ο παραλήπτης παίρνει κάποιο μήνυμα το οποίο υποτίθεται ότι προέρχεται από έναν συγκεκριμένο αποστολέα. Το κανάλι μέσω του οποίου διαβιβάζεται αυτό το μήνυμα δεν είναι ασφαλές. Επομένως ο παραλήπτης *R* θέλει να διακρίνει την περίπτωση στην οποία το μήνυμα προέρχεται πράγματι από τον υποτιθέμενο αποστολέα *S*, από την περίπτωση στην οποία το μήνυμα προέρχεται από κάποιον απατεώνα, *A*. Σε μια τέτοια περίπτωση θεωρούμε τη σχεδίαση ενός μηχανισμού ενθυλάκωσης με την ιδιότητα ότι μη αυθεντικές μεταβιβάσεις οδηγούν στον αλγόριθμο αποθυλάκωσης με έξοδο το ειδικό σύμβολο ⊥.

Το πιο κοινό εργαλείο για την επίλυση του προβλήματος πιστοποίησης της αυθεντικότητας μηνύματος στο συμμετρικό περιβάλλον είναι ένα σχήμα πιστοποίησης της αυθεντικότητας μηνύματος το οποίο καλείται "κώδικας πιστοποίησης της αυθεντικότητας μηνύματος" (message authentication code- MAC). Ένα τέτοιο σχήμα καθορίζεται από μια τριάδα αλγορίθμων, Π = (□, □, □). Όταν ο αποστολέας θέλει να στείλει ένα μήνυμα *M* στον παραλήπτη, υπολογίζει μια "ετικέτα" (tag), *σ*, εφαρμόζοντας τον αλγόριθμο □ στο κοινό κλειδί *K* και στο μήνυμα *M* και στη συνέχεια μεταβιβάζει το ζεύγος (*M*, *σ*). Η διαδικασία ενθυλάκωσης που αναφέραμε παραπάνω συνίσταται επομένως στο να πάρουμε το M και να επιστρέψουμε αυτό το ζεύγος. Η ετικέτα λέγεται επίσης ότι είναι ένα MAC. Ο υπολογισμός του MAC μπορεί να είναι πιθανοτικός ή όχι, όπως με την κρυπτογράφηση. Ο παραλήπτης, κατά τη λήψη των *M* και *σ*, χρησιμοποιεί το κλειδί *K* για να ελέγξει αν η ετικέτα είναι OK, εφαρμόζοντας τον αλγόριθμο "επαλήθευσης" ή "επιβεβαίωσης" (verification algorithm) □ στα *K*, *M* και *σ*. Αν αυτός ο αλγόριθμος επιστρέφει 1, δέχεται το M ως αυθεντικό· διαφορετικά θεωρεί ότι το M είναι "πλαστό" (forgery).



Εικ. 2.2: Κώδικας πιστοποίησης της αυθεντικότητας μηνύματος (MAC). Η ετικέτα *σ* συνοδεύει το μήνυμα *M*. Ο παραλήπτης *R* το χρησιμοποιεί για να αποφασίσει αν το μήνυμα προέρχεται πράγματι από τον αποστολέα *S* με τον οποίο μοιράζεται το κλειδί *K*.

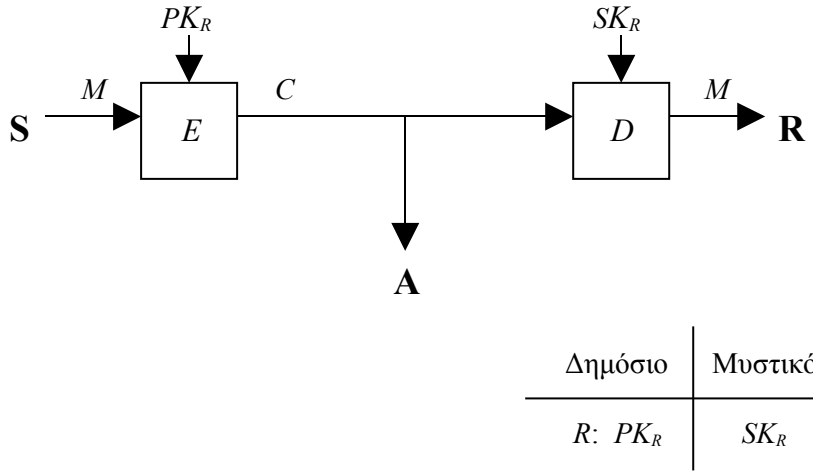
2.5 Κρυπτογραφία δημόσιου κλειδιού (ασύμμετρο περιβάλλον)

Η κρυπτογραφία δημόσιου κλειδιού εμφανίστηκε παγκοσμίως για πρώτη φορά μετά το 1970 [4].

Το κοινό κλειδί *K* μεταξύ του αποστολέα και του παραλήπτη δεν είναι ο μόνος τρόπος για να προκύψει η ασυμμετρία πληροφοριών την οποία χρειαζόμαστε μεταξύ των μελών και του αντιπάλου. Στο ασύμμετρο περιβάλλον, το καλούμενο και περιβάλλον ασύμμετρου κλειδιού, ένα μέλος κατέχει ένα ζεύγος κλειδιών- ένα "δημόσιο κλειδί" (public key) *pk* και το αντίστοιχο "μυστικό κλειδί" (secret key) *sk*. Το δημόσιο κλειδί του μέλους καθίσταται δημόσια γνωστό.

Ο αποστολέας υποτίθεται ότι είναι σε θέση να λάβει ένα αυθεντικό αντίγραφο pk_R του δημόσιου κλειδιού του παραλήπτη (υποτίθεται ότι και ο αντίπαλος ξέρει το *pk*). Για να στείλει ένα μυστικό μήνυμα *M* στον παραλήπτη ο αποστολέας υπολογίζει ένα κρυπτοκείμενο $C \leftarrow \mathsf{E}_{pk_R}(M)$ και στέλνει το C στον παραλήπτη. Όταν ο παραλήπτης παραλαμβάνει το κρυπτοκείμενο C υπολογίζει $M \leftarrow \mathsf{D}_{sk_R}(C)$. Το ασύμμετρο σχήμα κρυπτογράφησης Π = (□, □, □) καθορίζεται από τους αλγορίθμους δημιουργίας κλειδιού, κρυπτογράφησης και αποκρυπτογράφησης.

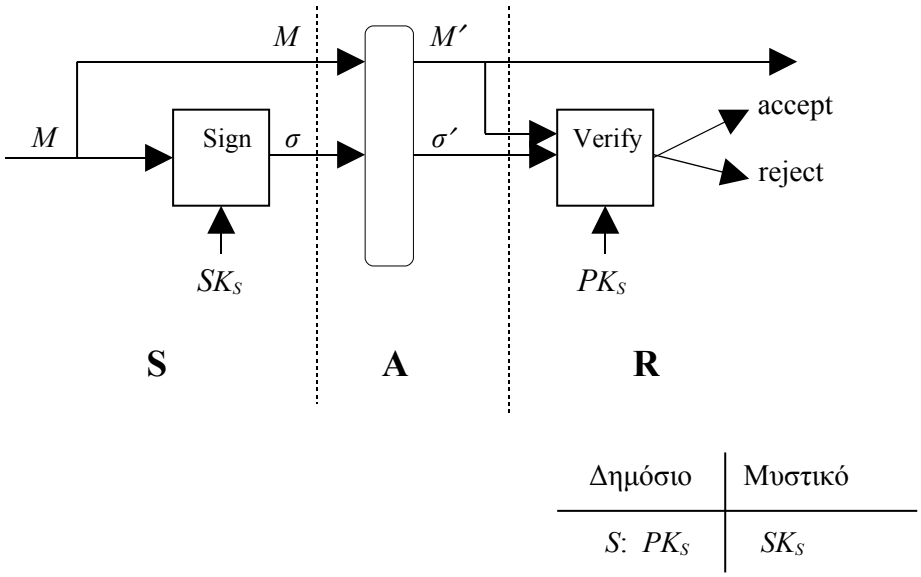
Μια εικόνα της κρυπτογράφησης στο περιβάλλον δημόσιου κλειδιού παρουσιάζεται στην Εικόνα 1.3.



Εικ. 2.3: Ασύμμετρη κρυπτογράφηση. Ο παραλήπτης *R* έχει ένα δημόσιο κλειδί, pk_R, το οποίο ο αποστολέας γνωρίζει ότι ανήκει στον *R*. Ο παραλήπτης έχει επίσης το αντίστοιχο μυστικό κλειδί, sk_R.

Το εργαλείο για την επίλυση του προβλήματος πιστοποίησης της αυθεντικότητας στο ασύμμετρο περιβάλλον είναι η "ψηφιακή υπογραφή" (digital signature). Εδώ ο αποστολέας έχει ένα δημόσιο κλειδί pk_S και το αντίστοιχο μυστικό κλειδί sk_S. Ο παραλήπτης υποτίθεται ότι ξέρει το κλειδί pk_S και ότι ανήκει στο μέλος *S* (υποτίθεται ότι και ο αντίπαλος ξέρει το pk_S). Όταν ο αποστολέας θέλει να στείλει ένα μήνυμα *M* επισυνάπτει σ' αυτό μερικά επιπλέον bit, *σ*, που λέγεται "υπογραφή" του μηνύματος και υπολογίζεται ως συνάρτηση των M και sk_S εφαρμόζοντας σ' αυτό έναν αλγόριθμο "υπογραφής" Sign. Ο παραλήπτης, κατά την παραλαβή των M και σ,

ελέγχει αν είναι ΟΚ χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, pk_S, εφαρμόζοντας έναν αλγόριθμο επαλήθευσης ή επιβεβαίωσης, . Στην περίπτωση αποδοχής από τον αλγόριθμο αυτόν, ο παραλήπτης θεωρεί το Μ ως αυθεντικό, διαφορετικά, θεωρεί το *M* ως μια απόπειρα πλαστογράφησης. Το σχήμα ψηφιακής υπογραφής Π = (, Sign,) καθορίζεται από τους αλγορίθμους δημιουργίας κλειδιού, υπογραφής και επαλήθευσης.



Δημόσιο	Μυστικό
S: PK_S	SK_S

Εικ. 2.4: Σχήμα ψηφιακής υπογραφής. Η υπογραφή *σ* συνοδεύει το μήνυμα *M*. Ο παραλήπτης *R* το χρησιμοποιεί για να αποφασίσει αν το μήνυμα προέρχεται πράγματι από τον αποστολέα *S* ο οποίος έχει το δημόσιο κλειδί pk_S.

Μια διαφορά μεταξύ ενός MAC και μιας ψηφιακής υπογραφής αφορά αυτό που λέγεται "μη απάρνηση" (non-repudiation). Στην περίπτωση του MAC οποιοσδήποτε μπορεί να επιβεβαιώσει ένα μήνυμα μπορεί επίσης να παράγει ένα, οπότε ένα μήνυμα με ετικέτα φαίνεται να είναι μικρής χρησιμότητας προκειμένου να αποδειχθεί η αυθεντικότητα σ' ένα δικαστήριο. Με ένα όμως ψηφιακά υπογεγραμμένο μήνυμα, το μόνο μέλος το οποίο θα ήταν σε θέση να παραγάγει ένα μήνυμα που επαληθεύεται με τη βοήθεια δημόσιου κλειδιού pk_S είναι το μέλος *S*. Επομένως αν το σχήμα υπογραφής είναι καλό, το μέλος *S* δεν μπορεί πλέον να ισχυριστεί ότι το επινόησε ο παραλήπτης, ή αυτός που παρουσιάζει τη μαρτυρία. Αν η υπογραφή *σ* πιστοποιεί την αυθεντικότητα του *M* σε σχέση με το δημόσιο κλειδί pk_S, τότε είναι μόνον ο *S* που θα μπορούσε να έχει επινοήσει την *σ*. Ο αποστολέας δεν μπορεί να το αντικρούσει. Ενδεχομένως ο αποστολέας *S* μπορεί να ισχυριστεί ότι το κλειδί sk_S του το είχαν κλέψει. Ίσως αυτό, αν αληθεύει, μπορεί ακόμη να ερμήνευε το φταίξιμο του αποστολέα.

Έτσι, προκύπτει ότι υπάρχουν δύο συνήθεις σκοποί που αφορούν την απομίμηση ενός ιδεατού δίαυλου επικοινωνίας: η επίτευξη της μυστικότητας μηνύματος και η επίτευξη της αυθεντικότητας μηνύματος. Υπάρχουν δύο κύρια

μοντέλα εμπιστοσύνης στα οποία επικεντρώνουμε το ενδιαφέρον μας προκειμένου να επιτευχθούν αυτοί οι σκοποί: το συμμετρικό μοντέλο εμπιστοσύνης και το ασύμμετρο μοντέλο εμπιστοσύνης. Τα εργαλεία που χρησιμοποιούνται για να επιτευχθούν αυτοί οι τέσσερις σκοποί αναφέρονται επιγραμματικά στην Εικόνα 1.5.

	συμμετρικό μοντέλο εμπιστοσύνης	**ασύμμετρο μοντέλο εμπιστοσύνης**
μυστικότητα μηνύματος	συμμετρική (ιδιωτικού κλειδιού) κρυπτογράφηση	ασύμμετρη (δημόσιου κλειδιού) κρυπτογράφηση
αυθεντικότητα μηνύματος	κώδικας πιστοποίησης της αυθεντικότητας μηνύματος (MAC)	σχήμα ψηφιακής υπογραφής

Εικ. 2.5: Σύνοψη κύριων σκοπών και μοντέλων εμπιστοσύνης.

2.6 SSL/TLS

Το TLS (Transport Layer Security) [5] και το SSL (Secure Socket Layer) [6] είναι στην πραγματικότητα πολύ παρόμοια. Το πρώτο ορίστηκε από την Netscape και έχει γίνει ευρέως αποδεκτό, ενώ το δεύτερο είναι η προτυποποιημένη έκδοση όπως ορίστηκε από την IETF (Internet Engineering Task Force).

Τα SSL και TLS συνήθως χρησιμοποιούν πιστοποιητικά X.509 για να επιβεβαιώσουν τουλάχιστον την μία από τις απολήξεις της σύνδεσης, συνήθως αυτήν του εξυπηρετητή και πιο διαδεδομένη είναι η χρήση τους με το HTTPS.

Ας σημειωθεί ότι αν δεν επιβεβαιωθεί η μία τουλάχιστον από τις απολήξεις της σύνδεσης, η σύνδεση είναι επισφαλής ως προς την πιθανότητα προσβολής της από μία επίθεση τύπου «man in the middle», όπου ένας ωτακουστής βρίσκεται μεταξύ των δύο πλευρών που θέλουν να επικοινωνήσουν και προσποιείται στον καθένα ότι είναι ο άλλος, αναμεταδίδοντας όλα τα μηνύματα που ανταλλάσσονται μεταξύ τους, αλλά μην έχοντας πρόσβαση στα αποκρυπτογραφημένα μηνύματα.

2.7 HTTPS

Το HTTPS είναι απλά το HTTP (Hypertext Transfer Protocol) [7] ασφαλές μέσω του συνδυασμού του με το SSL. Το HTTPS είναι το πρωτόκολλο που χρησιμοποιείται από τους ασφαλείς εξυπηρετητές διαδικτύου. Έχει δύο λειτουργίες, η πρώτη συνοψίζεται στην διαφύλαξη της ιδιωτικότητας των δεδομένων που μεταδίδονται μέσω της κρυπτογράφησης της γραμμής μετάδοσής τους και η δεύτερη, στην επιβεβαίωση της ταυτότητας του εξυπηρετητή που συμμετέχει στην επικοινωνία.

2.8 Συμβάσεις προσχωρήσεως/ Συμβάσεις με ΓΟΣ

Πρόκειται συνήθως για μαζικές συμβάσεις, στις οποίες ο οικονομικά ισχυρότερος προδιατυπώνει τους όρους της σύμβασης, στην οποία ο αντισυμβαλλόμενος μπορεί απλώς να προσχωρήσει ή όχι.

Πρόκειται για συμβάσεις με προδιατυπωμένους γενικούς όρους συναλλαγών (ΓΟΣ), των οποίων ο μελλοντικός αντισυμβαλλόμενος-χρήστης του Διαδικτύου δεν έχει παρά την επιλογή της συμφωνία ή της άρνησης της σύμβασης.

3. ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

3.1 Ψηφιακές υπογραφές και μη απάρνηση

3.1.1 Συμβατικές- ψηφιακές- ηλεκτρονικές υπογραφές

Η "συμβατική" χειρόγραφη υπογραφή που προσαρτάται σε ένα έγγραφο χρησιμοποιείται για να προσδιορίσει το αρμόδιο άτομο. Μια υπογραφή χρησιμοποιείται σε καθημερινές καταστάσεις, όπως συγγραφή επιστολής, ανάληψη χρημάτων από την τράπεζα, υπογραφή συμβολαίου κλπ.

Ψηφιακή υπογραφή ή προηγμένη ηλεκτρονική υπογραφή είναι σύμφωνα με το (ΠΔ 150/2001) η ηλεκτρονική υπογραφή που επιπλέον συνδέεται μονοσήμαντα με τον υπογράφοντα, είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος, δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Στο ΠΔ [8] η ηλεκτρονική υπογραφή ορίζεται ως δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.

Το σχήμα υπογραφής αποτελεί μέθοδο υπογραφής ενός μηνύματος που αποθηκεύεται σε ηλεκτρονική μορφή. Ως τέτοιο, το υπογεγραμμένο μήνυμα μπορεί να μεταδοθεί μέσω δικτύου υπολογιστών.

Σύμφωνα με τους Goldwasser, Micali και Rivest [9] η ισχύς ενός σχήματος υπογραφής εκτιμάται από τα επιτεύγματά της σε μία δεδομένη *προσβολή* ή *επίθεση* (attack). Θεωρούμε τους εξής τέσσερις τύπους επιθέσεων, με πιο ισχυρό τον τελευταίο:

Μόνο κλειδί (key only) Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα.

Επίθεση γνωστού μηνύματος (known message attack) Ο αντίπαλος γνωρίζει έναν αριθμό ζευγών μήνυμα – υπογραφή αλλά δεν μπορεί να επηρεάσει την κατανομή αυτών των μηνυμάτων.

Επίθεση επιλεγμένου μηνύματος (chosen message attack) Ο αντίπαλος κάνει μια λίστα μηνυμάτων και παίρνει την υπογραφή στο καθένα από αυτά.

Επίθεση προσαρμόσιμα επιλεγμένου μηνύματος (adaptively chosen message attack) Σε αυτόν τον τύπο επίθεσης ο αντίπαλος μπορεί να πάρει τη σωστή υπογραφή από τον υπογράφοντα σε έναν αριθμό γύρων. Σε κάθε γύρο ο αντίπαλος μπορεί να επιλέξει τα μηνύματα προς υπογραφή βασιζόμενος στις υπογραφές που έχουν ληφθεί ήδη.

3.1.1.1 Σύγκριση συμβατικών και ψηφιακών υπογραφών

Πρωτίστως προκύπτει το θέμα της υπογραφής ενός εγγράφου. Με τη συμβατική υπογραφή, η υπογραφή αποτελεί μέρος του φυσικού εγγράφου που υπογράφεται. Ωστόσο, η ψηφιακή υπογραφή δεν προσαρτάται φυσικά στο μήνυμα που υπογράφεται, άρα ο αλγόριθμος που χρησιμοποιείται πρέπει κάπως να «δένει» την υπογραφή με το μήνυμα.

Δευτερευόντως, προκύπτει το ζήτημα της επαλήθευσης. Η συμβατική υπογραφή επαληθεύεται από την σύγκρισή της με άλλες, αυθεντικές υπογραφές. Για παράδειγμα, όταν κάποιος υπογράφει αγορά πιστωτικής κάρτας, ο πωλητής υποτίθεται ότι συγκρίνει την υπογραφή στο απόκομμα πώλησης με το πίσω μέρος της πιστωτικής κάρτας για να επαληθεύσει την υπογραφή. Φυσικά, αυτή δεν είναι και πολύ ασφαλής μέθοδος καθώς εύκολα πλαστογραφεί κανείς την υπογραφή του άλλου. Από την άλλη πλευρά, οι ψηφιακές υπογραφές μπορούν να επαληθευτούν χρησιμοποιώντας έναν δημόσια γνωστό αλγόριθμο επαλήθευσης. Έτσι, μπορεί

«οποιοσδήποτε» να επαληθεύσει μια ψηφιακή υπογραφή. Η χρήση ενός ασφαλούς σχήματος υπογραφής προλαμβάνει τη δυνατότητα πλαστογραφήσεων.

Μια άλλη σημαντική διαφορά μεταξύ των συμβατικών και ψηφιακών υπογραφών είναι ότι ένα «αντίγραφο» του υπογεγραμμένου ψηφιακού μηνύματος είναι ταυτόσημο με το πρωτότυπο. Από την άλλη πλευρά, ένα αντίγραφο υπογεγραμμένου εγγράφου μπορούμε συνήθως να το ξεχωρίσουμε από ένα πρωτότυπο. Αυτό το χαρακτηριστικό σημαίνει ότι πρέπει να προσέξουμε ώστε να προληφθεί η νέα χρήση ενός υπογεγραμμένου ψηφιακού μηνύματος. Για παράδειγμα, αν το μέλος *A* υπογράφει ένα ψηφιακό μήνυμα εξουσιοδοτώντας το μέλος *B* για ανάληψη €100 από τον τραπεζικό του λογαριασμό, δηλαδή επιταγή, θέλει απλώς να καταστήσει τον *B* ικανό να το κάνει μία φορά. Έτσι, το ίδιο το μήνυμα θα πρέπει να περιλαμβάνει πληροφορίες όπως η ημερομηνία, που προλαμβάνουν τη δεύτερη χρήση.

3.1.1.2 Σύγκριση ηλεκτρονικών και ψηφιακών υπογραφών

Είναι σημαντικό να αναγνωρίσουμε τη διαφορά μεταξύ της ηλεκτρονικής υπογραφής και της ψηφιακής υπογραφής. Μια ξεκάθαρη κατανόηση των διαφορετικών ορισμών είναι σημαντική στην τεχνολογική και στη νομική αρένα.

Η φράση "ηλεκτρονική υπογραφή" είναι ο όρος με ευρύ περιεχόμενο για την περιγραφή οποιουδήποτε τύπου ψηφιακού σημαδιού που χρησιμοποιείται από μια οντότητα προκειμένου να δεσμευτεί ή να κάνει αυθεντικό ένα αρχείο. Πρόκειται για έναν όρο με φάσμα που θα μπορούσε να συμπεριλαμβάνει σημάδια από ψηφιοποιημένες εικόνες χειρόγραφων υπογραφών ή τυπωμένες σημειώσεις του τύπου "/s/ Tom Jones" στο τέλος ενός ηλεκτρονικού εγγράφου, μέχρι σημειώσεις διευθυνσιοδότησης του τύπου κεφαλίδων ή υποσέλιδων ηλεκτρονικού ταχυδρομείου. Θεωρείται το ψηφιακό ισοδύναμο του παραδοσιακού "X" που χρησιμοποιείται για την υπογραφή ενός συμβολαίου ή εγγράφου. Οι υλοποιήσεις ηλεκτρονικής υπογραφής δεν προσφέρουν μεγαλύτερη ασφάλεια από αυτήν ενός συνθηματικού (password). Επιπλέον στις ηλεκτρονικές υπογραφές δεν υπάρχει τρόπος να πιστοποιηθεί το κατά πόσο έχει τροποποιηθεί ένα έγγραφο από τη στιγμή που υπογράφθηκε. Με άλλα λόγια η τεχνολογία των ηλεκτρονικών υπογραφών δεν παρέχει πιστοποίηση της αυθεντικότητας του υπογράφοντα ή του εγγράφου.

Η ψηφιακή υπογραφή είναι ένας συγκεκριμένος τύπος ηλεκτρονικής υπογραφής και συνήθως αναφέρεται σε μια κρυπτογραφική υπογραφή, είτε σε ένα έγγραφο είτε σε μια κατώτερου επιπέδου δομή δεδομένων. Μια ψηφιακή υπογραφή είναι νομικά περισσότερο αποδεκτή από άλλους τύπους ηλεκτρονικών υπογραφών, καθώς προσφέρει πιστοποίηση αυθεντικότητας και του υπογράφοντα και του εγγράφου. Η πιστοποίηση αυθεντικότητας του υπογράφοντα είναι η δυνατότητα προσδιορισμού της ταυτότητας του προσώπου (της οντότητας) που ψηφιακά υπέγραψε το έγγραφο. Η πιστοποίηση αυθεντικότητας του εγγράφου εγγυάται (εξασφαλίζει) ότι το έγγραφο ή η συναλλαγή (ή η υπογραφή) δεν μπορεί να τροποποιηθεί εύκολα.

Η διαδικασία δημιουργίας μιας ψηφιακής υπογραφής και επαλήθευσης της επιτυγχάνει τα ουσιώδη αποτελέσματα τα οποία κάνει σήμερα μια χειρόγραφη υπογραφή για πολλούς νομικούς σκοπούς:

- *Πιστοποίηση αυθεντικότητας του υπογράφοντα*: Αν ένα δημόσιο και ιδιωτικό κλειδί συσχετίζεται με έναν πιστοποιημένο υπογράφοντα, η ψηφιακή υπογραφή αποδίδει το μήνυμα στον υπογράφοντα. Η ψηφιακή υπογραφή δεν μπορεί να πλαστογραφηθεί, εκτός κι αν ο υπογράφων χάσει τον έλεγχο του

ιδιωτικού κλειδιού, όπως για παράδειγμα αποκαλύπτοντάς το ή χάνοντας το μέσο ή τη συσκευή στην οποία περιέχονταν. Όσο η χρήση των δημόσιων ηλεκτρονικών δικτύων αυξάνεται, από την απλή έρευνα πληροφοριών στο διαδίκτυο μέχρι την ανταλλαγή πληροφοριών και χρημάτων online, χρειαζόμαστε μεγαλύτερη διασφάλιση ότι αυτά τα μηνύματα και οι συναλλαγές είναι ασφαλείς και ότι η ιδιωτικότητά μας προστατεύεται. Η διασφάλιση της αυθεντικότητας των ηλεκτρονικών επικοινωνιών μπορεί να συνεισφέρει σημαντικά στην επίτευξη του επιθυμητού επιπέδου ασφάλειας, όπως αναλύεται στο [10].

- *Πιστοποίηση αυθεντικότητας του μηνύματος*: Η ψηφιακή υπογραφή προσδιορίζει την ταυτότητα του υπογεγραμμένου μηνύματος, τυπικά με μεγαλύτερη βεβαιότητα και ακρίβεια από τις χειρόγραφες υπογραφές. Η επαλήθευση αποκαλύπτει οποιαδήποτε λαθροχειρία αφού η σύγκριση των αποτελεσμάτων κατακερματισμού (αυτού που γίνεται κατά την υπογραφή και του άλλου που γίνεται κατά την επαλήθευση) δείχνει το κατά πόσο το μήνυμα είναι το ίδιο όπως όταν υπογράφθηκε.
- *Μη απάρνηση*: Η δημιουργία μιας ψηφιακής υπογραφής απαιτεί από τον υπογράφοντα να χρησιμοποιήσει το ιδιωτικό κλειδί του υπογράφοντα. Αυτή η πράξη προειδοποιεί τον υπογράφοντα για το γεγονός ότι ολοκληρώνουν μια συναλλαγή με νομικές συνέπειες.
- *Ακεραιότητα*: Η διαδικασία δημιουργίας και επαλήθευσης μιας ψηφιακής υπογραφής παρέχει υψηλό επίπεδο διαβεβαίωσης ότι η ψηφιακή υπογραφή είναι αληθώς του υπογράφοντα. Συγκρινόμενες με μεθόδους επί χάρτου, όπως αυτή του ελέγχου της υπογραφής σε κάρτες, οι ψηφιακές υπογραφές παρέχουν υψηλό βαθμό ασφάλειας χωρίς να απαιτούν περισσότερους πόρους για την επεξεργασία.

3.1.2 Μη απάρνηση

Η μη απάρνηση αναφέρεται στη χρήση των ψηφιακών υπογραφών προς επίλυση αμφισβητήσεων. Έτσι η ψηφιακή υπογραφή, η οποία αποτελεί μέρος μιας συναλλαγής θα πρέπει να αποθηκεύεται και σε περίπτωση αμφισβήτησης πρέπει να είναι σε θέση ένας διαιτητής να την επαληθεύσει. Στο μέρος I του ISO13888 [11] παρέχεται ένα πλαίσιο για τη μη απάρνηση και στο μέρος III [12] ορίζονται συγκεκριμένα χαρακτηριστικά στοιχεία μη απάρνησης. Τα πλέον σημαντικά είναι αυτά που ακολουθούν.

Η μη απάρνηση πηγής (non-repudiation of origin) προστατεύει εναντίον της ψευδούς απάρνησης του αποστολέα ότι από αυτόν προέρχεται το μήνυμα.

Η μη απάρνηση παράδοσης (non-repudiation of delivery) προστατεύει εναντίον της ψευδούς απάρνησης του παραλήπτη ότι παρέλαβε και αναγνώρισε τα περιεχόμενα του μηνύματος (το ISO χρησιμοποιεί τον όρο "non-repudiation of receipt" – "μη απάρνηση απόδειξης παραλαβής" προκειμένου να αναφέρεται σε μια απόδειξη ότι ο παραλήπτης έχει ήδη παραλάβει το μήνυμα).

Εκτός από αυτά, ορίζονται επιπλέον χαρακτηριστικά στοιχεία μη απάρνησης για την υποστήριξη του ηλεκτρονικού ισοδύναμου της συστημένης επιστολής. Όλα τα στοιχεία ακολουθούν μια παρόμοια δομή, οπότε θα περιοριστούμε στο στοιχείο της μη απάρνησης της πηγής. Περιλαμβάνει τις ακόλουθες πληροφορίες οι οποίες είναι υπογεγραμμένες:

- Μια περιγραφή της πολιτικής μη απάρνησης για αυτό το στοιχείο (δηλ. τι αποδεικνύει το στοιχείο).
- Πιστοποίηση της ταυτότητας του αποστολέα.
- Πιστοποίηση της ταυτότητας του προτεινόμενου(ων) παραλήπτη(ών).
- Πιστοποίηση της ταυτότητας της αρχής που δημιούργησε το στοιχείο (συνήθως ο αποστολέας).
- Ημερομηνία και ώρα δημιουργίας του στοιχείου.
- Ημερομηνία και ώρα αποστολής του μηνύματος.
- Περιγραφή του μηχανισμού της υπογραφής (συμπεριλαμβανομένης της συνάρτησης κατακερματισμού).
- Την τιμή κατακερματισμού του μηνύματος.

Το δύσκολο και ουσιαστικό τμήμα να παρασχεθεί σε αυτό το στοιχείο είναι η χρονο-σήμανση, η οποία χρησιμοποιείται προκειμένου να καταστεί το στοιχείο μοναδικό και, σε περίπτωση αμφισβητήσεων, να προσδιορίζεται η ακριβής χρονική στιγμή δημιουργίας του στοιχείου. Ένα πιθανό σενάριο όπου οι χρονο-σημάνσεις είναι σημαντικές, είναι το εξής:

> Ο χρήστης *A* υπογράφει ένα μήνυμα στο οποίο δηλώνει ότι οφείλει στο μέλος *B* 1000 ευρώ και ότι θα εξοφλήσει αυτό το ποσό δύο μήνες αργότερα. Ένα μήνα αργότερα ο *A* μετανιώνει και ανακαλεί το πιστοποιητικό ισχυριζόμενος ότι ενδεχομένως να έχει εκτεθεί το ιδιωτικό του κλειδί. Όταν αργότερα ο *B* θελήσει να πάρει τα χρήματά του, ο *A* αρνείται να πληρώσει ισχυριζόμενος ότι η υπογραφή του έγινε μετά την ανάκληση του πιστοποιητικού.

Προφανώς, αν το αρχικό μήνυμα από τον *A* είχε μια μη πλαστογραφίσιμη χρονο-σήμανση, ο Α δεν θα ήταν σε θέση να ισχυριστεί όσα ισχυρίζεται.

Προκειμένου να παρέχονται τέτοιες χρονο-σημάνσεις χρειάζεται ένα τρίτο μέλος. Το [13] ορίζει ένα στοιχείο χρονο-σήμανσης προκειμένου να περιλαμβάνει την υπογραφή της Αρχής Χρονο-Σήμανσης (Time Stamp Authority) σε ένα μήνυμα που περιέχει

- Μια περιγραφή της πολιτικής μη απάρνησης για τη χρονο-σήμανση
- Ημερομηνία και ώρα δημιουργίας της χρονο-σήμανσης
- Περιγραφή του μηχανισμού υπογραφής (συμπεριλαμβανομένης συνάρτησης κατακερματισμού)
- Τιμή κατακερματισμού του μηνύματος που είναι να χρονο-σημανθεί

Από την ομάδα εργασίας PKIX [14] έχουν αναπτυχθεί πρότυπα πρωτοκόλλων για χρονο-σήμανση στο Internet. Παρουσιάζει ενδιαφέρον το γεγονός ότι η χρονο-σήμανση που ορίζεται από την PKIX στην τρέχουσα έκδοση παρέχει την ευχέρεια επιλογής της συσχέτισης επιπρόσθετων πληροφοριών στο στοιχείο προκειμένου να εμποδίζεται το τρίτο μέλος να μεταχρονολογεί (πχ. η χρονο-σήμανση θα μπορούσε να περιλαμβάνει την πλέον πρόσφατη τιμή κλεισίματος της μέσης τιμής του Dow Jones). Πάντως, όπως δείχνει το παράδειγμα παραπάνω, η προ-χρονολόγηση (back dating) συχνά είναι ένα πιο σοβαρό πρόβλημα. Έχουν προταθεί δύο λύσεις σε αυτό το πρόβλημα [15]. Στη μια λύση, το τρίτο μέλος που κάνει τις χρονο-σημάνσεις συνδέει τις σημάνσεις μεταξύ τους έτσι ώστε η προ-χρονολόγηση (πριν την προηγούμενη χρονο-σήμανση) να μην είναι εφικτή. Αυτή η λύση έχει το πρόβλημα ότι η επίλυση μιας αμφισβήτησης που εμπλέκει χρονο-σημάνσεις μπορεί να απαιτεί ως μάρτυρες άλλα μέλη που έχουν ζητήσει χρονο-σημάνσεις. Η δεύτερη λύση προτείνει να

διανέμεται η χρονο-σήμανση μεταξύ ενός πλήθους τρίτων μελών (με έναν τυχαίο και μη προβλέψιμο τρόπο).

3.1.3 Η πρακτική χρησιμότητα της «μη απάρνησης»

Στην πράξη η έννοια της μη απάρνησης δεν εμφανίζει καμία χρησιμότητα λόγω της ασυνέπειας μεταξύ των εννοιών ενός κανόνα μη απάρνησης και ενός συστήματος κυριότητας μη απάρνησης. Συγκεκριμένα, η εφαρμογή του κανόνα της μη απάρνησης σε μία υπογραφή αποδεικνύεται χωρίς πρακτική αξία, αφού αν θέλει κάποιος να υπογράψει ένα έγγραφο χωρίς να δεσμεύεται από αυτό, υπάρχει ένας τυποποιημένος τρόπος να το πετύχει, διατυπώνοντας στο έγγραφο ότι αυτό δεν είναι νομικά δεσμευτικό.

Αντίθετα, αν κάποιος θέλει να δημιουργήσει ένα καθεστώς στο οποίο οτιδήποτε επαληθεύεται από το ιδιωτικό του κλειδί είναι δεσμευτικό για αυτόν είτε το υπέγραψε ο ίδιος είτε όχι, τότε μπορεί να δημοσιεύσει μία δήλωσή του με ακριβώς αυτό το αποτέλεσμα προς αποδοχή από οποιονδήποτε πρόκειται να βασιστεί σε ένα έγγραφο του οποίου η υπογραφή επαληθεύεται από το συγκεκριμένο δημόσιο κλειδί. Η αποτελεσματικότητα αυτής της νομικής τεχνικής αναγνωρίζεται από τα δικαστήρια από τον δέκατο ένατο αιώνα.

Κάθε μία από τις δύο διαδικασίες που παρατέθηκαν παραπάνω μπορεί να επιτευχθεί πολύ πιο αποτελεσματικά μέσω της διατύπωσης δηλώσεων παρά μέσω της χρήσης κλειδιών με δέσμευση από όρους των οποίων την ερμηνεία πολλοί χρήστες δεν γνωρίζουν επακριβώς.

3.1.4 Ευθύνη προστασίας του ιδιωτικού κλειδιού – ευθύνη υπογράφοντα και αποδέκτη της υπογραφής – όροι Συνδρομητικών Συμβάσεων

Όσο αφορά την ύπαρξη ή μη νομικής ευθύνης του κατόχου του ιδιωτικού κλειδιού ως προς την φύλαξή του σημειώνονται τα παρακάτω.

Δεν υπάρχει συγκεκριμένη νομοθεσία στο Ηνωμένο Βασίλειο που υποχρεώνει τον κάτοχο του ιδιωτικού κλειδιού να φροντίζει για την ασφάλειά του. Υπάρχουν περιπτώσεις στις οποίες ο κάτοχος του ιδιωτικού κλειδιού εξαιτίας όρων συμβολαίου ή ειδικής νομοθεσίας δεσμεύεται νομικά από τις ενέργειες [16] που πραγματοποιήθηκαν με το ιδιωτικό του κλειδί είτε τις πραγματοποίησε αυτός είτε όχι. Αυτό δεν πρέπει να συγχέεται με το duty of care, το οποίο είναι μία δελεαστική αλλά παρανοημένη βάση για την ανάλυση ευθύνης της χρήσης κρυπτογραφικών κλειδιών σε εμπορικά κείμενα.

Στην Μεγάλη Βρετανία παραμένει ανοιχτό το ενδεχόμενο ανάπτυξης από το κοινό δίκαιο[17] ενός αντίστοιχου γενικού κανόνα που θα καλύπτει όλους αυτούς που παρέχουν ή δημοσιεύουν ένα δημόσιο κλειδί Μία ενδεχόμενη λύση είναι να τεθεί ένας αντίστοιχος όρος ως βάση κάθε φορά που παρέχεται ένα κλειδί, τουλάχιστον όσο αφορά εμπορικά κείμενα. Αυτό θα μπορούσε να επιτευχθεί με μία δήλωση του αποδέκτη του ιδιωτικού κλειδιού. Για παράδειγμα, ο αποδέκτης του ιδιωτικού κλειδιού, θα μπορούσε να δηλώσει ότι αποδέχεται ότι είναι δεσμευμένος από ό,τι υπογράφει με το ιδιωτικό κλειδί που αντιστοιχεί σε συγκεκριμένο δημόσιο κλειδί, αλλά παρόλο που δεν γνωρίζει ότι κάποιος άλλος εκτός από αυτόν έχει πρόσβαση σε αυτό το ιδιωτικό κλειδί και παρόλο που σκοπεύει να προσπαθήσει να διασφαλίσει ότι κανένας άλλος εκτός από αυτόν έχει ή θα αποκτήσει πρόσβαση σε αυτό, δεν αποδέχεται καμία νομική υποχρέωση να κάνει τέτοια προσπάθεια, ούτε αποδέχεται καμία νομική ευθύνη για οποιαδήποτε συνέπεια μη εξουσιοδοτημένης πρόσβασης

στο ιδιωτικό κλειδί του, ανεξάρτητα από το αν ο ίδιος δεν κατάφερε να το διαφυλάξει. Επιπλέον δεν εγγυάται ότι είναι το μόνο πρόσωπο με πρόσβαση σε αυτό το κλειδί και δεν αποδέχεται καμία ευθύνη για οτιδήποτε υπογράφεται με αυτό το κλειδί, το οποίο δεν αποδεικνύεται ότι υπογράφηκε από αυτόν ή με εξουσιοδότησή του. Το γεγονός ότι αυτό το κλειδί επαληθεύει μία υπογραφή δεν θα πρέπει να ερμηνεύεται ως ότι αυτός δημιούργησε την υπογραφή.

Όσο αφορά την ευθύνη του υπογράφοντα, αλλά και του αποδέκτη (relying party) της ηλεκτρονικής υπογραφής, πρέπει, κατ' αρχήν και οι δύο, να κατανοούν τον τρόπο χρήσης και λειτουργίας των ηλεκτρονικών υπογραφών που χρησιμοποιούν. Πρέπει, επίσης, να λάβουν γνώση όλων των σχετικών όρων στα κείμενα που τους παρέχει ο Πάροχος Υπηρεσιών Πιστοποίησης (π.χ. Σύμβαση Συνδρομητή με τον Πάροχο, Πολιτική Πιστοποιητικού κλπ.) διότι εκεί αναγράφονται όλοι οι όροι χρήσης και οι περιορισμοί του πιστοποιητικού που υποστηρίζει την συγκεκριμένη ψηφιακή υπογραφή.

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

- Να δηλώνει πραγματικά και ενημερωμένα στοιχεία της ταυτότητάς του κατά την αίτησή του για την έκδοση του σχετικού πιστοποιητικού ηλεκτρονικής υπογραφής του στην Υπηρεσία Εγγραφής του Παρόχου και να ελέγχει την ορθή μεταφορά τους στο πιστοποιητικό, πριν το χρησιμοποιήσει.
- Να τηρεί με επιμέλεια την μυστικότητα και την αποκλειστική χρήση των σχετικών ιδιωτικών κλειδιών του (μη έκθεση σε τρίτους),
- Να ζητά από τον Πάροχο την ανάκληση (ή την αναστολή) του σχετικού πιστοποιητικού του εάν βεβαιωθεί για (ή υποψιασθεί) οποιαδήποτε έκθεση των ιδιωτικών κλειδιών του σε τρίτους, καθώς και στην περίπτωση που απολέσει τον φορέα ή/και τον έλεγχο των ιδιωτικών κλειδιών του.
- Να χρησιμοποιεί τα συγκεκριμένα κρυπτογραφικά κλειδιά του μόνο στις επιτρεπόμενες για το σχετικό πιστοποιητικό τους χρήσεις και να μην υπερβαίνει στις σχετικές συναλλαγές του τα τυχόν όρια που προβλέπονται από την σύμβαση και την εφαρμοζόμενη Πολιτική του συγκεκριμένου πιστοποιητικού.

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

- είναι “αυθεντικό”, με την έννοια ότι υπάρχει τουλάχιστον μία αλληλουχία πιστοποιητικών (με όλους τους μεσολαβούντες υπο-εκδότες) η οποία να καταλήγει σε μια αξιόπιστη -γι' αυτόν- ρίζα εμπιστοσύνης (συνήθως το αυτο-ϋπογραφόμενο πιστοποιητικό “Root CA” ενός γνωστού Παρόχου).

- είναι “έγκυρο”, δηλαδή ότι δεν έχει λήξει ή ανακληθεί η ισχύς του. Αυτό σημαίνει ότι ο αποδέκτης θα πρέπει να ελέγξει, όχι μόνο την διάρκεια ισχύος (ημερομηνία λήξης) που αναγράφεται μέσα στο ίδιο το εξεταζόμενο πιστοποιητικό, αλλά και τις σχετικές Λίστες Ανακληθέντων Πιστοποιητικών που δημοσιεύει ο ίδιος ο εκδότης του. Ο έλεγχος αυτός μπορεί να γίνει είτε μέσω ειδικών αυτοματοποιημένων εφαρμογών που εμπιστεύεται ο χρήστης, είτε μέσω σχετικής “Απ' ευθείας Υπηρεσίας Ενημέρωσης Ανάκλησης Πιστοποιητικών” (Online Certificate Status Protocoll - OCSP) που πιθανώς να παρέχει ο Πάροχος ή τρίτος.

- είναι “κατάλληλο” για την συναλλαγή ή την χρήση στην οποία ο αποδέκτης του πρόκειται να προβεί. Για να θεωρηθεί “κατάλληλο” ένα πιστοποιητικό θα πρέπει η προτιθέμενη χρήση του να μην απαγορεύεται από την σχετική Πολιτική Πιστοποιητικού. Επίσης, εάν από τον τύπο της επιχειρούμενης συναλλαγής έχει καθοριστεί ή/και πρέπει να ακολουθηθεί μια συγκεκριμένη Πολιτική (ηλεκτρονικής) Υπογραφής, τότε η χρήση του συγκεκριμένου πιστοποιητικού θα πρέπει να προβλέπεται ή, έστω, να επιτρέπεται από την εφαρμοζόμενη “Πολιτική Υπογραφής”.

Η “Πολιτική Υπογραφής” (Signature Policy) είναι ένα συγκεκριμένο (και ταυτοποιημένο με μοναδικό κωδικό ‘OID’) κείμενο το οποίο αναφέρει διεξοδικά όλους τους απαραίτητους όρους για την ‘έγκυρη’ εναπόθεση ή/και επαλήθευση μιας ηλεκτρονικής υπογραφής, οι οποίοι εφαρμόζονται σε έναν καθορισμένο κύκλο συναλλαγών. Η ‘Πολιτική Υπογραφής’ επιλέγεται με συμφωνία των μερών ή, συνηθέστερα, επιβάλλεται από την πλευρά του ‘αποδέκτη’ των υπογραφών ως ‘γενικός όρος συναλλαγών’. Αποτελώντας, μάλιστα, και αντικείμενο πρόσφατης προτυποποίησης από τους αρμόδιους

3.1.5 Ισχύον θεσμικό πλαίσιο για τις ηλεκτρονικές υπογραφές

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

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

- Την αναλυτική προσέγγιση (prescriptive approach), σύμφωνα με την οποία «μόνο συγκεκριμένες τεχνολογικές μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφάλειας και αξιοπιστίας, αναγνωρίζονται άμεσα ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές» [18].

Οι ηλεκτρονικές υπογραφές αποτελούν σημαντικό τμήμα της δημιουργίας ενός περιβάλλοντος εμπιστοσύνης στο οποίο το ηλεκτρονικό εμπόριο ενθαρρύνεται και προωθείται. Επίσης, παρέχουν στους πολίτες νέες και αποτελεσματικές μεθόδους για επικοινωνία με τους κυβερνητικούς φορείς. Στα πλαίσια της παραπάνω παγκόσμιας προσπάθειας, το Αμερικανικό Εμπορικό Επιμελητήριο συνέταξε τον Φεβρουάριο του 2004 μία αναφορά [19] προς την Ευρωπαϊκή Ένωση σημειώνοντας τα σημεία που θα έπρεπε να συμπεριληφθούν στην Ευρωπαϊκή Οδηγία για τις ηλεκτρονικές υπογραφές ώστε να δημιουργηθεί ένα ισχυρό νομικό υπόβαθρο για την ασφαλή και παραγωγική χρήση τους.

Πληροφορίες για τα νομικά ζητήματα των ηλεκτρονικών υπογραφών παρέχονται από Τράπεζα Νομικών Πληροφοριών Ηλεκτρονικού Εμπορίου του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών [20].

Η Ευρωπαϊκή Ένωση, με την Οδηγία 99/93/ΕΚ [21] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 "Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές" (EEL 13/19.1.2000) ακολούθησε μία μικτή προσέγγιση δύο επιπέδων (two-tier approach), η οποία συνδυάζει και τις δύο παραπάνω κατευθύνσεις.

Έτσι, η συγκεκριμένη Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως "ηλεκτρονικές υπογραφές" -οι οποίες μπορούν να χρησιμοποιηθούν ως "αποδεικτικά στοιχεία" σε νομικές διαδικασίες (ά. 5 § 2 της Οδηγίας)-, όλα τα: "δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με,άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας" (ά. 2 § 1 της Οδηγίας). Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο απλές (π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής σε ένα e-mail ή του αριθμού του τηλεφώνου αποστολής σε ένα SMS μήνυμα, κλπ), ως τις πιο σύνθετες (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κλπ), ανεξάρτητα, δηλαδή, από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

Από την κανονιστική πλευρά, η Οδηγία διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών -αποκαλούμενες συχνά ως "αναγνωρισμένες ηλεκτρονικές υπογραφές"- στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις "ιδιόχειρες υπογραφές", σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους. Σε αυτήν την κατηγορία ανήκουν όλες οι: "προηγμένες ηλεκτρονικές υπογραφές" που, επιπλέον, βασίζονται σε "αναγνωρισμένο πιστοποιητικό" και δημιουργούνται από "ασφαλή διάταξη δημιουργίας υπογραφής" (ά.. 5 § 1). Οι νομικές και εμπορικές προεκτάσεις της εφαρμογής της παρούσας Οδηγίας, καθώς και οι πρακτικές εφαρμογές των ηλεκτρονικών υπογραφών στα κράτη- μέλη παρουσιάζονται αναλυτικά σε μελέτη για την αντίστοιχη Ευρωπαϊκή Επιτροπή [22] το 2003.

Ως "προηγμένες ηλεκτρονικές υπογραφές" (οι οποίες στο εθνικό μας δίκαιο – π.δ. 150/2001 [23]- αποκαλούνται και "ψηφιακές υπογραφές"), η Οδηγία προσδιορίζει τις ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις: α) συνδέονται μονοσήμαντα με τον υπογράφοντα, β) είναι ικανές να ταυτοποιήσουν τον υπογράφοντα, γ) δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και δ)συνδέονται με τα δεδομένα στα οποία αναφέρονται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε αλλοίωση στα εν λόγω δεδομένα. (ά. 2 § 2). Οι συγκεκριμένες απαιτήσεις μπορούν να ικανοποιηθούν σήμερα μόνο με την χρήση της τεχνολογίας της ασύμμετρης κρυπτογραφίας η οποία κάνει χρήση ιδιωτικών ("δεδομένα δημιουργίας υπογραφής") και δημοσίων ("δεδομένα επαλήθευσης υπογραφής") κρυπτογραφικών κλειδιών που χρησιμοποιούνται συμπληρωματικά το ένα προς το άλλο για την παραγωγή και την επαλήθευση της ηλεκτρονικής υπογραφής.

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

Τέλος, ως "ασφαλής διάταξη δημιουργίας υπογραφής" ορίζεται το διατεταγμένο υλικό ή/και λογισμικό που χρησιμοποιείται για την εφαρμογή του "ιδιωτικού κλειδιού" (ή, των "δεδομένων δημιουργίας υπογραφής") από τον υπογράφοντα και το οποίο διασφαλίζει την αξιοπιστία της δημιουργίας της υπογραφής βάσει συγκεκριμένων απαιτήσεων που αναγράφονται στο Παράρτημα ΙΙΙ της Οδηγίας

Η Οδηγία προβλέπει την ελεύθερη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, απαγορεύοντας οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης, προσδιορίζοντας, όμως τις προϋποθέσεις λειτουργίας (Παράρτημα ΙΙ) και την ευθύνη (ά. 6) των Παρόχων Υπηρεσιών Πιστοποίησης που εκδίδουν "αναγνωρισμένα πιστοποιητικά προς το κοινό". Παράλληλα προβλέπει την δυνατότητα "Εθελοντικής Διαπίστευσης" των Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και διαδικασία "Διαπίστωσης" της συμμόρφωσης των "προϊόντων ηλεκτρονικών υπογραφών" με τις απαιτήσεις ασφάλειας και αξιοπιστίας της Οδηγίας (βάσει σχετικών "γενικώς αναγνωρισμένων προτύπων") από σχετικούς αρμόδιους φορείς.

Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για "ψηφιακές υπογραφές" (οι οποίες ταυτίζονται εννοιολογικά με τις "προηγμένες ηλεκτρονικές υπογραφές" της Οδηγίας) γίνεται ήδη από το άρθρο 14 του ν. 2672/98 [24] όπου παρέχεται μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα. Συγκεκριμένα, το άρθρο 14 του ν. 2672/98 προβλέπει την χρήση της ηλεκτρονικής υπογραφής και κατά την διακίνηση εγγράφων μεταξύ των υπηρεσιών του Δημοσίου, των Ν.Π.Δ.Δ. και των Ο.Τ.Α. ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων, νομικών προσώπων ιδιωτικού δικαίου και ενώσεων προσώπων, με τηλεομοιοτυπία και ηλεκτρονικό ταχυδρομείο.

Ακολούθησε το π.δ. 150/2001 (ΦΕΚ Α'/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία και καθόρισε την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων [25] (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για την λειτουργία μηχανισμών "Εθελοντικής Διαπίστευσης" των Παρόχων Υπηρεσιών Πιστοποίησης και "Διαπίστωσης" της συμμόρφωσης των "προϊόντων ηλεκτρονικής υπογραφής".

Τον Οκτώβριο του 2002, κατ' εξουσιοδότηση του ν. 2672/98 εκδόθηκε το π.δ. 342/02 [26] το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων "μηνυμάτων ηλεκτρονικού ταχυδρομείου" στις επικοινωνίες του δημόσιου τομέα.

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

3.1.6 Νομοθετικές απαιτήσεις για τον εξοπλισμό δημιουργίας και επαλήθευσης υπογραφών

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.

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

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

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

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

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

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

Αντίστοιχα, για την επαλήθευση (verification) των ψηφιακών υπογραφών και τον έλεγχο της εγκυρότητας (validation) των σχετικών πιστοποιητικών, απαιτείται μια ανάλογη διάταξη, η οποία, εκτός του τερματικού επικοινωνίας του χρήστη και του κατάλληλου λογισμικού, θα πρέπει, επιπλέον, να διαθέτει και την δυνατότητα

πρόσβασης –είτε με "on line" σύνδεση, είτε και με συχνές "off-line" ενημερώσεις- σε επικαιροποιημένες πληροφορίες εγκυρότητας ή/και ανάκλησης πιστοποιητικών τις οποίες δημοσιεύει ο εκάστοτε εκδότης (ΠΥΠ) τους. Για τις "διατάξεις επαλήθευσης υπογραφής" η Οδηγία 99/93/ΕΚ "συστήνει" (ά.3§6) προς τα κράτη-μέλη την συνεργασία τους για την ανάπτυξη συστημάτων τα οποία θα πρέπει να διασφαλίζουν τόσο την αξιοπιστία τους, όσο και την ορθή πληροφόρηση του επαληθεύοντα ως προς τα στοιχεία και τα αποτελέσματα της επαλήθευσης (Παράρτημα IV).

3.1.7 Ανάλυση μεθόδων τεκμηρίωσης και νομικός τους χαρακτηρισμός

Παρακάτω εξετάζονται ορισμένες μέθοδοι τεκμηρίωσης από τεχνικής σκοπιάς και το κατά πόσο αυτές μπορούν να χαρακτηριστούν και ως "ηλεκτρονικές υπογραφές" ή ενδεχομένως και "προηγμένες ηλεκτρονικές υπογραφές" (δηλαδή, ψηφιακές υπογραφές) με την έννοια του π.δ. 150/2001 και της Οδηγίας 99/93/ΕΚ και στην συνέχεια κατά πόσο πληρούν τις προϋποθέσεις του νόμου ώστε να είναι εφικτή η πρόσδοση σε αυτές νομικής ισχύος ανάλογης με αυτήν της ιδιόχειρης υπογραφής.

Ι. 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 [27]. 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 π.δ. 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.

ΙΙ. Η κρυπτογράφηση (encryption)

Η έγκρυψη ή κρυπτογράφηση (encryption) διασφαλίζει όχι την γνησιότητα των δεδομένων, αλλά το απόρρητο της επικοινωνίας, την εμπιστευτικότητα, δηλαδή, των διαβιβαζόμενων δεδομένων. Υπό αυτή την έννοια, δεν αποτελεί μέθοδο τεκμηρίωσης της γνησιότητας των δεδομένων, δηλαδή ηλεκτρονική υπογραφή με την έννοια του άρθρου 2 § 1 του π.δ. 150/2001 και της Οδηγίας 99/93/ΕΚ. Η κρυπτογράφηση έχει σαν αποτέλεσμα την προστασία των μεταβιβαζόμενων δεδομένων από τα "αδιάκριτα

βλεμματα", αλλά όχι την εξασφάλιση της γνησιότητας, της ακεραιότητας και της προέλευσης των σχετικών δεδομένων.

Η κρυπτογράφηση χρησιμοποιείται ευρύτατα στις ηλεκτρονικές συναλλαγές σήμερα, ακόμη και σε συναλλαγές προμηθευτών καταναλωτικών προϊόντων ή υπηρεσιών με καταναλωτές. Για παράδειγμα, οι συναλλαγές ηλεκτρονικής τραπεζικής (e-banking) εκτελούνται στο σύνολό τους πλέον κάνοντας χρήση μεθόδων κρυπτογράφησης. Η κρυπτογράφηση επίσης, συνηθίζεται στις συναλλαγές ηλεκτρονικού εμπορίου (e-commerce). Για παράδειγμα, στις αγορές μέσω του Διαδικτύου, κατά το στάδιο που ο χρήστης καλείται να γνωστοποιήσει στον έμπορο ευαίσθητα δεδομένα, όπως τον αριθμό της πιστωτικής του κάρτας, τα δεδομένα αυτά διαβιβάζονται στον τελευταίο κρυπτοθετημένα. Τέλος, στον τομέα της ηλεκτρονικής διακυβέρνησης (e-government) η κρυπτογράφηση των δεδομένων που καταχωρεί ο διοικούμενος στον ηλεκτρονικό υπολογιστή αποτελεί σχεδόν αυτονόητη πρακτική (π.χ. κατά την υποβολή δήλωσης φορολογίας εισοδήματος στο Taxis).

Ευρύτατα διαδομένο σύστημα κρυπτογράφησης είναι το SSL, το οποίο κρυπτογραφεί τα δεδομένα που εισάγουν οι χρήστες του Διαδικτύου προτού αυτά διαβιβασθούν online στον αποδέκτη τους [28]. Στην πράξη συνηθίζεται να γίνεται συνδυασμένη χρήση μεθόδων ηλεκτρονικής υπογραφής και κρυπτογράφησης.

ΙΙΙ. Η κρυπτογράφηση ως μέθοδος απόδειξης της γνησιότητας (ηλεκτρονική υπογραφή)

Η δεύτερη βασική εφαρμογή της κρυπτογράφησης, δηλαδή πέρα από την κρυπτογράφηση, αποσκοπεί στην διασφάλιση της ακεραιότητας των ηλεκτρονικών δεδομένων και συνεπώς, αποτελεί μορφή ψηφιακής υπογραφής [29]. Τα συστήματα κρυπτογράφησης που χρησιμοποιούνται είναι όπως αναλύθηκαν παραπάνω, το συμμετρικό κρυπτογραφικό σύστημα και το ασύμμετρο κρυπτογραφικό σύστημα (δηλαδή η ψηφιακή υπογραφή).

Η μέθοδος της συμμετρικής κρυπτογράφησης αποτελεί μορφή ψηφιακής υπογραφής με την έννοια του π.δ. και της Οδηγίας. Το (μοναδικό) κλειδί κρυπτογράφησης (δηλαδή ο μαθηματικός αλγόριθμος) αποτελεί εκείνα τα δεδομένα σε ηλεκτρονική μορφή, τα οποία συσχετίζονται λογικά με τα δεδομένα που απαρτίζουν την δήλωση βουλήσεως και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητάς τους.

Η μέθοδος της ασύμμετρης κρυπτογράφησης, είτε των ίδιων των δεδομένων, είτε, συνηθέστερα, του "δακτυλικού τους αποτυπώματος" (fingerprint) αποτελεί την χαρακτηριστικότερη περίπτωση ηλεκτρονικής υπογραφής. Να σημειωθεί ότι τόσο ο κοινοτικός όσο και ο εθνικός νομοθέτης, κατά την ρύθμιση του νομικού πλαισίου για την ηλεκτρονική υπογραφή είχαν κυρίως ως πρότυπο της μέθοδο ασύμμετρης κρυπτογράφησης με τον αλγόριθμο RSA [30]. Σε αυτήν την περίπτωση, τόσο το μυστικό κλειδί (κρυπτογράφησης) όσο και το δημόσιο κλειδί (αποκρυπτογράφησης) αποτελούν τα δεδομένα σε ηλεκτρονική μορφή τα οποία συσχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα (το ηλεκτρονικό έγγραφο) και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας (του εγγράφου).

Η μέθοδος της ασύμμετρης κρυπτογράφησης ωστόσο, γνωστή και ως ψηφιακή υπογραφή, δεν αποτελεί μόνο μορφή της ηλεκτρονικής υπογραφής, με την έννοια του άρθρου 2 § 1 του π.δ. 150/2001 και της Οδηγίας 99/93/ΕΚ, αλλά επιπλέον εμπίπτει και στην ειδικότερη έννοια της "προηγμένης ηλεκτρονικής υπογραφής", όπως αυτή ορίζεται στην § 2 του ίδιου άρθρου.

IV. Άλλες μορφές ηλεκτρονικής υπογραφής

Πέραν των παραπάνω μεθόδων τεκμηρίωσης σε τεχνικό επίπεδο προτείνονται και διάφορες άλλες μέθοδοι διακρίβωσης της γνησιότητας της προέλευσης δεδομένων ηλεκτρονικού υπολογιστή. Χαρακτηριστικό παράδειγμα αποτελούν οι βιομετρικές μέθοδοι, οι οποίες συσχετίζουν στα προς διαβίβαση δεδομένα που συνδέονται μονοσήμαντα με τον χρήστη ("υπογράφοντα"), όπως π.χ. το δακτυλικό αποτύπωμα ή την απεικόνιση της ίριδας του ματιού, βιολογικά στοιχεία που θεωρούνται μοναδικά σε κάθε άνθρωπο. Ωστόσο, οι συγκεκριμένες μέθοδοι δεν χρησιμοποιούνται ευρέως στις συναλλαγές μέχρι σήμερα.

Στο ζήτημα που γεννάται κατά πόσο η διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail address) αποτελεί ή όχι μορφή ηλεκτρονικής υπογραφής, η απάντηση είναι καταφατική σύμφωνα με την νομολογία και το Μονομελές Πρωτοδικείο Αθηνών [31].

Να διευκρινιστεί ότι και οι δύο παραπάνω μέθοδοι (βιομετρικά χαρακτηριστικά, διεύθυνση ηλεκτρονικού ταχυδρομείου) αποτελούν απλά μορφές ηλεκτρονικής υπογραφής, έννοια που αντιδιαστέλλεται με αυτήν της προηγμένης ηλεκτρονικής υπογραφής ή ψηφιακής υπογραφής.

3.2 Ψηφιακά πιστοποιητικά, αρχές πιστοποίησης και αρχές εγγραφής

3.2.1 Πιστοποιητικό

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

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

Η πιο συνήθης χρήση των πιστοποιητικών σήμερα είναι με HTTPS για την επαλήθευση της ταυτότητας των ασφαλών εξυπηρετητών διαδικτύου. Σε αυτή την περίπτωση, η ταυτότητα που συνδέεται με το δημόσιο κλειδί είναι το domain name του εξυπηρετητή διαδικτύου. Πριν η αρχή πιστοποίησης εκδώσει ένα πιστοποιητικό που συνδέει το domain name με ένα δημόσιο κλειδί, ελέγχει ότι το domain ανήκει στο πρόσωπο ή την οντότητα, συνήθως εταιρία, που έχει αιτηθεί του πιστοποιητικού. Ελέγχει επίσης ότι πρόκειται για συναλλαγή της με την ίδια την οντότητα και όχι κάποιον τρίτο. Σφάλματα σε αυτούς τους ελέγχους είναι πιθανόν να έχουν σημαντικές συνέπειες. Για παράδειγμα, τον Ιανουάριο του 2001, η VeriSign εξέδωσε εσφαλμένα για λογαριασμό ενός μη εξουσιοδοτημένου τρίτου ένα πιστοποιητικό υπογραφής κωδικού συνδεμένο με την ταυτότητα της Microsoft, το οποίο θα

μπορούσε να χρησιμοποιηθεί για την εισαγωγή αυθαίρετου κώδικα σε μηχανές ανυποψίαστων χρηστών [32].

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

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

Άλλοι περιορισμοί στην χρήση των πιστοποιητικών δημοσίων κλειδιών μπορούν να αναφέρονται στα όρια ως προς την αξία των συναλλαγών στις οποίες αυτά επιτρέπεται να χρησιμοποιηθούν. Οι περιορισμοί αυτοί πρέπει -τουλάχιστον για τα "αναγνωρισμένα πιστοποιητικά"- να αναγράφονται σε κατάλληλα πεδία μέσα στο ίδιο πιστοποιητικό ή/και να αναφέρονται εμφανώς μέσα στο κείμενο της σχετικής "Πολιτικής Πιστοποιητικού" (Certificate Policy) που δημοσιεύει ο Πάροχος Υπηρεσιών Πιστοποίησης και η οποία συμπεριλαμβάνει όλους τους ειδικότερους όρους έκδοσης και χρήσης που καθορίζει ο Πάροχος Υπηρεσιών Πιστοποίησης για το συγκεκριμένο είδος πιστοποιητικών. Το κείμενο μιας "Πολιτικής Πιστοποιητικού" προσδιορίζεται ("ταυτοποιείται") με τη χρήση ενός μοναδικού "κωδικού αριθμού ταυτοποίησης' ("Object Identification number" ή "OID") ο οποίος αναγράφεται στο ομώνυμο πεδίο των πιστοποιητικών X.509, ενημερώνοντας τόσο το υποκείμενο πιστοποίησης ("συνδρομητή" του ΠΥΠ), όσο και κάθε τρίτο-αποδέκτη των πιστοποιητικών του για την εφαρμοζόμενη "Πολιτική Πιστοποιητικού".

Τα "πιστοποιητικά δημοσίου κλειδιού" μπορούν επίσης να διακριθούν σε "επώνυμα" και σε "ψευδώνυμα" πιστοποιητικά, ανάλογα με τη δημοσιοποίηση του πραγματικού ονόματος του υποκειμένου στο οποίο αναφέρονται. Είναι ακόμη δυνατόν να εκδοθούν και "ανώνυμα" πιστοποιητικά, στα οποία συνήθως

πιστοποιείται -μέσω απομακρυσμένης επικοινωνίας- μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου (e-mail address) από το υποκείμενο.

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

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

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

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

3.2.2 Προτυποποίηση

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

Σύμφωνα με το X.509 ένα δημόσιο κλειδί συσχετίζεται με ένα Διακεκριμένο Όνομα (Distinguished Name ή DN), το οποίο είναι μία τεράστια μάζα δεδομένων που προσδιορίζει την ταυτότητα του ιδιοκτήτη του πιστοποιητικού με έναν ιεραρχικό τρόπο. Το παραπάνω, συμβαδίζει με το μοντέλο του X.500, ένα πρότυπο ταχυδρομικού καταλόγου που απέτυχε στο να κερδίσει ευρεία αποδοχή, αλλά στην πραγματικότητα δεν λειτουργεί αποτελεσματικά στις συναλλαγές. Περισσότερες λεπτομέρειες για το συγκεκριμένο πρότυπο [34] αλλά και για ένα δεύτερο [35] παρέχονται αναλυτικά.

3.2.3 Αρχή πιστοποίησης- CA ή Πάροχος Υπηρεσιών Πιστοποίησης και νομική ευθύνη του

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

Οι ιδιωτικές αρχές πιστοποίησης, δηλαδή αυτές που λειτουργούν μόνο στα πλαίσια εντός ενός οργανισμού, ασχολούνται συχνότερα με πιστοποιητικά πελατών.

Ας σημειωθεί ότι ένας από τους ελέγχους που οφείλει να διενεργήσει μία αρχή πιστοποίησης είναι ο έλεγχος του εάν ο αιτών έχει την κατοχή του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού. Αυτό πρέπει να επιτυγχάνεται μέσω μίας υπογραφής με αίτημα του πιστοποιητικού και όχι μέσω της παραγωγής του ιδιωτικού κλειδιού από την ίδια την αρχή πιστοποίησης για λογαριασμό του αιτούντα.

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

Η Παροχή Υπηρεσιών Πιστοποίησης ηλεκτρονικών υπογραφών (και "συναφών υπηρεσιών") δεν υπόκειται σε καθεστώς αδειοδότησης και άρα μπορεί οποιοσδήποτε (φυσικό ή νομικό πρόσωπο) να λειτουργήσει ως Πάροχος Υπηρεσιών Πιστοποίησης και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός Παρόχου Υπηρεσιών Πιστοποίησης προς την εποπτεύουσα αρχή (ΕΕΤΤ) είναι η

"Δήλωση Έναρξης Λειτουργίας" και η εγγραφή του στο σχετικό "Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης", καθώς και η αποστολή "Ετήσιων Εκθέσεων" σχετικά με την λειτουργία τους.

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

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

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

Η ευθύνη του Παρόχου Υπηρεσιών Πιστοποίησης έναντι των "τρίτων" μπορεί να περιοριστεί σε συγκεκριμένα όρια και για συγκεκριμένες χρήσεις του πιστοποιητικού, εφόσον όμως οι περιορισμοί αυτοί προσδιορίζονται ρητά στην "Πολιτική Πιστοποιητικού" (Certificate Policy) που διέπει το συγκεκριμένο πιστοποιητικό και είναι εμφανείς και αναγνωρίσιμοι σε κάθε αποδέκτη του. Ο Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να απαλλαχθεί εντελώς από την ευθύνη εκ του νόμου εάν αποδείξει ότι η σχετική πράξη ή παράλειψη του δεν προήλθε από αμέλεια.

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

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

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

Είναι επιτρεπτό για έναν Πάροχο Υπηρεσιών Πιστοποίησης να εκχωρήσει σε τρίτους (outsourcing) τη διεκπεραίωση μέρους ή ακόμη και του συνόλου των παραπάνω παρεχόμενων υπηρεσιών του. Εφόσον όμως ο Πάροχος εξακολουθεί να αναγράφεται στα εκδιδόμενα πιστοποιητικά ως "Εκδότης", τότε διατηρεί ακέραια την ευθύνη του έναντι των τρίτων για οποιοδήποτε πράξη ή παράλειψη που αναφέρεται στην Οδηγία (ή στο ΠΔ 150/2001) και προξενεί ζημία σε συνδρομητές ή τρίτους.

Σύμφωνα με πληροφορίες που παρέχονται από το ICRI (Interdisciplinary centre for Law and Information Technology) ηγέτης στον χώρο την παροχής πιστοποιητικών στην ελληνική αγορά φαίνεται να είναι η εταιρία VeriSign, η οποία δραστηριοποιείται μέσω της ελληνικής εταιρείας Adacom.

3.2.4 Αρχή εγγραφής- RA

Ορισμένες φορές η αρχή πιστοποίησης αναθέτει την ευθύνη ελέγχου της ταυτότητας ή άλλων χαρακτηριστικών του πιστοποιητικού σε τρίτες οντότητες. Σε αυτήν την περίπτωση η οντότητα που κάνει τον έλεγχο των πιστοποιητικών είναι γνωστή ως Αρχή Εγγραφής (Registration Authority- RA).

Δηλαδή, η Αρχή Εγγραφής ελέγχει τη ταυτότητα των υποκειμένων και συλλέγει τα σχετικά αποδεικτικά στοιχεία -πιθανώς συνεπικουρούμενη από εξουσιοδοτημένες "Τοπικές Υπηρεσίες Υποβολής" (Local Registration Authorities / LRAs)- πριν να δώσει την έγκρισή της για την έκδοση των σχετικών πιστοποιητικών.

3.2.5 Ανάκληση πιστοποιητικών

3.2.5.1 Διαδικασία ανάκλησης πιστοποιητικών

Η ανάκληση είναι η διαδικασία ακύρωσης ενός πιστοποιητικού. Αυτό πραγματοποιείται συνήθως με την υπογραφή ενός οργάνου που υποδεικνύει ποιο πιστοποιητικό έχει ανακληθεί. Αυτή η υπογραφή μπορεί να γίνει με το ίδιο κλειδί το οποίο χρησιμοποιήθηκε για την υπογραφή του αυθεντικού πιστοποιητικού ή με ένα διαφορετικό κλειδί. Η βασική ιδέα πίσω από την ανάκληση είναι ότι εφόσον ένα πιστοποιητικό έχει ανακληθεί, κανένας δεν πρέπει να βασίζεται σε αυτό.

Το πρόβλημα με την ανάκληση είναι ότι η ανάγκη ελέγχου της κατάστασης ενός πιστοποιητικού, δηλαδή του αν είναι εν ισχύ ή έχει ανακληθεί ή λήξει, εξαλείφει κατά μεγάλο ποσοστό το πλεονέκτημα χρήσης των πιστοποιητικών. Το μεγαλύτερο επιχείρημα για την παραπάνω άποψη είναι ότι αντί του ελέγχου της κατάστασης του πιστοποιητικού για τον αποκλεισμό της πιθανότητας αυτό να έχει ανακληθεί, θα μπορούσε να προσλαμβάνεται απευθείας η οποιαδήποτε πληροφορία περιέχεται στο πιστοποιητικό από την αρμόδια αρχή στην συγκεκριμένη χρονική στιγμή.

3.2.5.2 Λίστα ανάκλησης πιστοποιητικών

Η λίστα ανάκλησης πιστοποιητικών είναι ακριβώς η λίστα που περιέχει τα πιστοποιητικά τα οποία έχουν ανακληθεί. Στην περίπτωση του X.509 πρόκειται συνήθως για μία λίστα των domain names των πιστοποιητικών που έχουν ανακληθεί.

3.2.6 Μοντέλο απειλής

Σπάνια αποδεικνύεται χρήσιμος ο προσδιορισμός ενός κρυπτογραφικού συστήματος χωρίς τον προηγούμενο προσδιορισμό του ενδεχόμενου κινδύνου. Αυτό είναι γνωστό ως «μοντέλο απειλής». Ουσιαστικά, ο ορισμός ενός θεωρητικά ασφαλούς σχήματος χωρίς τον ορισμό του αντίστοιχου μοντέλου απειλής δεν έχει καμία πρακτική σημασία.

Για παράδειγμα, το μοντέλο απειλής που συνήθως χρησιμοποιείται για το διαδίκτυο είναι ότι οι επιτιθέμενοι θα προσπαθήσουν να κλέψουν πληροφορίες πιστωτικών καρτών ή άλλες προσωπικές πληροφορίες. Δύο ευρέως γνωστοί τρόποι για να επιτευχθεί αυτό είναι με το να κρυφακούσει κάποιος ή με το να εμφανιστεί στην συνομιλία σαν να ήταν ο ίδιος ο εξυπηρετητής διαδικτύου. Το SSL υποστηρίζεται ότι επιλύει και τα δύο αυτά προβλήματα. Το πρώτο πρόβλημα επιλύεται επιτυχώς με την κρυπτογράφηση της συνομιλίας με ένα κλειδί το οποίο είναι γνωστό μόνο στα δύο άκρα της γραμμής επικοινωνίας. Ωστόσο, η επίλυση του δεύτερου προβλήματος είναι επισφαλής, αφού το SSL επιβεβαιώνει την ταυτότητα του εξυπηρετητή ελέγχοντας ότι το domain name του αντιστοιχεί στο πιστοποιητικό του και επιπλέον, ότι το πιστοποιητικό εκδόθηκε από μία αναγνωρισμένη αρχή πιστοποίησης. Ωστόσο, υπάρχουν τουλάχιστον τρία προβλήματα αναφορικά με αυτόν τον έλεγχο. Πρώτον, αν ο έλεγχος αποτύχει, παρέχονται στον χρήστη μία σειρά από αυστηρές προειδοποιήσεις οι οποίες είναι σχεδόν βέβαιο ότι θα αγνοηθούν. Δεύτερον,

η αρχή πιστοποίησης, όπως σημειώθηκε και παραπάνω, ενδέχεται να μην επιδείξει την δέουσα επιμέλεια κατά την διενέργεια του ελέγχου που αφορά την εξακρίβωση της ταυτότητας και των υπολοίπων στοιχείων του και επίσης ενδέχεται να αποποιηθεί των ευθυνών της για οποιοδήποτε σφάλμα. Τρίτον και μάλλον σημαντικότερο, το URL δεν είναι ένα ισχυρό ενδεικτικό στοιχείο της πραγματικής ταυτότητας ενός εξυπηρετητή διαδικτύου.

Ως παράδειγμα παρατίθεται η URL διεύθυνση WWW.MIC0SOFT.COM, η οποία είναι πολύ δύσκολο να διακριθεί από την WWW.MICROSOFT.COM. Η δεύτερη σαφώς ανήκει στην Microsoft, όμως η πρώτη όχι. Ωστόσο στην πράξη, παρόλο που το πιστοποιητικό περιέχει την ταυτότητα του ιδιοκτήτη και υποθέτοντας ότι η αρχή πιστοποίησης έχει εκπληρώσει σωστά τις υποχρεώσεις της, κανένας δεν ελέγχει το ίδιο το πιστοποιητικό ή την λίστα ανάκλησης.

3.2.7 Υποδομή Δημόσιου Κλειδιού – PKI

Θα προσπαθήσουμε να περιγράψουμε πρακτικά θέματα της χρήσης των ψηφιακών υπογραφών, αρχίζοντας από τα πιστοποιητικά τα οποία από τη μια μεριά συνιστούν μια απλή εφαρμογή των ψηφιακά υπογεγραμμένων μηνυμάτων και, από την άλλη, καθιστούν δυνατές άλλες εφαρμογές.

Προκειμένου να χρησιμοποιήσουμε ψηφιακές υπογραφές είναι συνήθως αναγκαίο να έχουμε μια Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) [36]. Καθώς ένα υπογεγραμμένο μήνυμα επαληθεύεται έναντι του δημόσιου κλειδιού, αποδεικνύει, υποθέτοντας ότι η υπογραφή δεν έχει πλαστογραφηθεί, ότι το μήνυμα προέρχεται από το μέλος που γνωρίζει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί. Έτσι το δημόσιο κλειδί παίζει το ρόλο της ηλεκτρονικής ταυτότητας και η κύρια επιδίωξη μιας PKI είναι να συνδέει αυτή την ηλεκτρονική ταυτότητα με την πραγματική ταυτότητα του κατόχου (ή σε ορισμένες περιπτώσεις με ένα ψευδώνυμο που έχει επιλεγεί από τον κάτοχο).

Στην πράξη αυτό γίνεται με χρήση των πιστοποιητικών δημόσιου κλειδιού (public key certificates). Το πιστοποιητικό, όπως αναλύθηκε παραπάνω, είναι ένα ηλεκτρονικό μήνυμα που δηλώνει ότι ένα δοθέν κλειδί ανήκει σε συγκεκριμένο πρόσωπο και εκδίδεται από ένα τρίτο μέλος που λέγεται αρχή πιστοποίησης, όπως επίσης αναλύθηκε. Ο καθένας που γνωρίζει το δημόσιο κλειδί της αρχής πιστοποίησης μπορεί να επαληθεύει πιστοποιητικά τα οποία εκδόθηκαν από αυτήν την αρχή πιστοποίησης και επομένως να χρησιμοποιεί τα δημόσια κλειδιά σε αυτά τα πιστοποιητικά.

Ενώ ο ρόλος του CA είναι κεντρικός για την εδραίωση ενός PKI, εμπλέκονται συχνά και δύο άλλοι ρόλοι:

- Η αρχή εγγραφής (registration authority – RA) η οποία όπως αναλύθηκε παραπάνω, επαληθεύει πληροφορίες για το χρήστη (ειδικότερα την ταυτότητα του χρήστη) και συνδέει το δημόσιο κλειδί στο χρήστη. Σε μερικές εφαρμογές απαιτείται ένας αριθμός τοπικών RA όπου οι αιτούντες πρέπει να αποκαλύπτονται προσωπικά πριν λάβουν ένα πιστοποιητικό.
- Ο κατάλογος (directory – D) ο οποίος διατηρεί έναν μητρώο δημόσιων πληροφοριών για τους χρήστες και τα πιστοποιητικά. Πιστοποιητικά μπορούν να δημοσιεύονται σε έναν κατάλογο και επομένως να ανακτώνται από έναν κατάλογο. Το πρωτόκολλο LDAP [37] είναι ένα καθιερωμένο πρωτόκολλο για προσπέλαση σε τέτοιες πληροφορίες.

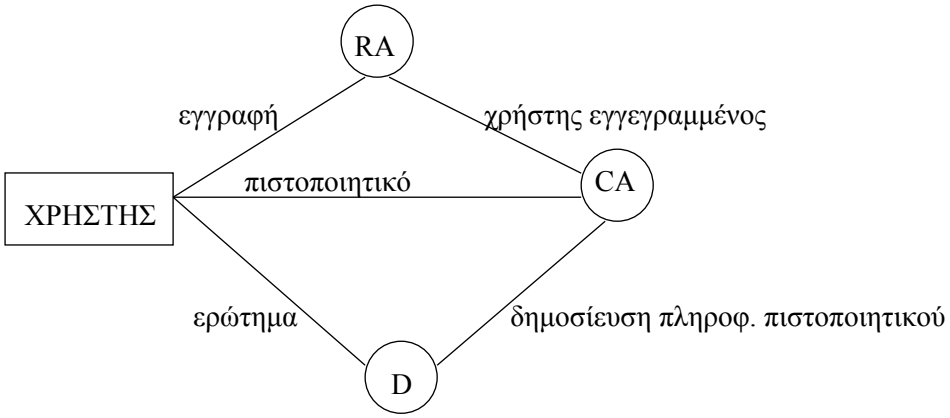
Ένας χρήστης εγγράφεται σε αρχή εγγραφής και παίρνει ένα πιστοποιητικό από την αρχή πιστοποίησης. Αργότερα το πιστοποιητικό μπορεί να χρησιμοποιηθεί είτε περιλαμβάνοντας στα ηλεκτρονικά μηνύματα το πιστοποιητικό αυτό ή επιτρέποντας το άλλο μέλος να πάρει πληροφορίες για το πιστοποιητικό από ένα τρίτο μέλος όπως είναι το D ή το ίδιο το CA. (βλ. Εικόνα χχ)

Επειδή ο σκοπός ενός πιστοποιητικού είναι να συνδέει μεταξύ τους ένα μέλος με ένα δημόσιο κλειδί, είναι φυσικά σημαντικό να γίνεται προσεκτικά η πιστοποίηση της ταυτότητας του μέλους όπως και η επαλήθευση της ορθότητας του κλειδιού: πρέπει να επιβεβαιώνεται ότι το όνομα του μέλους είναι σωστό και ότι αυτό το μέλος δέχεται ότι το πιστοποιημένο δημόσιο κλειδί ανήκει σε αυτό.

Αν και υπάρχουν διάφορες άλλες διαδικασίες, ένα πιστοποιητικό τυπικά εκδίδεται ως ακολούθως:

1. Ο αιτών εγγράφεται στην αρχή εγγραφής. Διάφορες εκδοχές είναι εδώ δυνατές
   - Ηλεκτρονική εγγραφή (πχ. Πιστοποίηση ταυτότητας έναντι μιας διεύθυνσης email). Αυτό γίνεται ως επί το πλείστον σήμερα, αλλά δεν ενδείκνυται αν το πιστοποιητικό πρόκειται να χρησιμοποιηθεί για μη απάρνηση.
   - Εγγραφή που βασίζεται σε μια ήδη εδραιωμένη σχέση.
   - Φυσική εγγραφή, όπου ο αιτών πρέπει να εμφανισθεί προσωπικά και ο αρμόδιος στην αρχή εγγραφής να επαληθεύσει την ταυτότητα του αιτούντος.

   Στις δύο τελευταίες περιπτώσεις ο αιτών μπορεί να πρέπει να υπογράψει (ιδιόχειρα) μια αίτηση (αυτή η αίτηση μπορεί να περιλαμβάνει ένα δακτυλικό αποτύπωμα του δημόσιου κλειδιού, το οποίο πρόκειται να πιστοποιηθεί).



Εικ. 3.1: Ρόλοι σε ένα PKI

2. Η αρχή εγγραφής ενημερώνει την αρχή πιστοποίησης για την εγγραφή.
3. Η αρχή πιστοποίησης στέλνει το επονομαζόμενο IAK (Initial Authentication Key – αρχικό κλειδί πιστοποίησης αυθεντικότητας) στο χρήστη σε μια σφραγισμένη επιστολή.
4. Ο αιτών στέλνει μια ηλεκτρονική αίτηση για το πιστοποιητικό. Σε αυτή την αίτηση ο αιτών πιστοποιεί τον εαυτό του χρησιμοποιώντας το IAK (πχ.

Υπολογίζοντας ένα MAC στην αίτηση) και αποδεικνύει τη γνώση του ιδιωτικού κλειδιού του αντίστοιχου με το προς πιστοποίηση δημόσιο κλειδί.

5. Η αρχή εγγραφής επιστρέφει το αιτούμενο πιστοποιητικό, αν η αίτηση είναι εντάξει μετά τον έλεγχο (και το δημόσιο κλειδί δεν έχει προηγουμένως πιστοποιηθεί).

Πάντως, ανεξάρτητα από το πόσους πόρους έχουν τεθεί στην επαλήθευση των πληροφοριών στα πιστοποιητικά όταν αυτά εκδίδονται, η υποδομή δημοσίου κλειδιού πρέπει να υποστηρίζει μέσα για την ανάκληση ή ακύρωση πιστοποιητικών. Και το πιο αξιοσημείωτο, αυτό θα συμβεί αν το πιστοποιημένο ζεύγος κλειδιών (υπάρχει υποψία ότι) είναι εκτεθειμένο, αλλά μπορεί επίσης να είναι αναγκαίο σε λιγότερο δραματικές περιπτώσεις, λ.χ., αν κάποιες πληροφορίες στο πιστοποιητικό είναι απαρχαιωμένες. Σε περίπτωση που έχει ανακληθεί ένα πιστοποιητικό, η υποδομή δημοσίου κλειδιού πρέπει να βεβαιωθεί ότι η αλλαγή της κατάστασης του πιστοποιητικού (status) έχει ανακοινωθεί δεόντως. Αυτό μπορεί για παράδειγμα, να γίνει μέσω ανακοινώσεων λιστών ανακλημένων πιστοποιητικών, ή παρέχοντας μια on-line υπηρεσία η οποία μπορεί με ασφαλή τρόπο να δίνει πάντα την πραγματική κατάσταση του οποιουδήποτε πιστοποιητικού.

Μια σημαντική δυσκολία που προκύπτει κατά την εδραίωση μιας υποδομής δημοσίου κλειδιού είναι η δημοσιοποίηση του δημόσιου κλειδιού της αρχής πιστοποίησης. Αυτό το κλειδί είναι στην καρδιά της ασφάλειας οποιουδήποτε συστήματος, καθώς όλα τα πιστοποιητικά που εκδίδονται από την αρχή πιστοποίησης επαληθεύονται έναντι αυτού του κλειδιού. Έτσι κάποιος που είναι σε θέση να αντικαταστήσει αυτό το κλειδί με ένα άλλο θα είναι σε θέση να εκδώσει (ψευδή) πιστοποιητικά και επομένως να κάνει υποτιθέμενες υπογραφές ότι προέρχονται από κάποιον άλλο. Η διανομή του κλειδιού της αρχής πιστοποίησης μπορεί να γίνει εκτός ομάδας, λ.χ., με δημοσίευση σε εφημερίδες ή με επιστολές όταν εγγράφεται ο χρήστης, ή με πιστοποίησή του χρησιμοποιώντας έναν άλλο CA. Το τελευταίο μπορεί να αποτελέσει αφορμή να δημιουργηθεί μια ιεραρχία από CA στην οποία μόνο η διανομή του κλειδιού στη ρίζα πρέπει να γίνει εκτός ομάδας.

3.2.8 Αρχές πιστοποίησης (CAs), αρχές εγγραφής (RAs) και νομική ευθύνη

Οι αρχές πιστοποίησης προσπαθούν συχνά να αποποιηθούν την νομική ευθύνη για τα πιστοποιητικά τους. Προκύπτουν έτσι τα ζητήματα, του αν μπορούν πραγματικά να το πετύχουν και αν δημιουργεί κάποια διαφοροποίηση το γεγονός ότι οι χρήστες των πιστοποιητικών βασίζονται στην αρχή πιστοποίησης, αλλά αυτοί που λαμβάνουν τα πιστοποιητικά συναλλάσσονται μόνο με την αρχή εγγραφής, στην οποία η αρχή πιστοποίησης μπορεί να έχει παραχωρήσει μέρος των δραστηριοτήτων της.

Η δήλωση αποποίησης ευθύνης μίας αρχής πιστοποίησης αποκτά νομική ισχύ αν ενσωματωθεί με αναφορά στους όρους των πιστοποιητικών που αυτή εκδίδει. Είναι πιθανό σε ορισμένα συστήματα δικαιοδοσίας, όπως του Ηνωμένου Βασιλείου και άλλων ευρωπαϊκών κρατών, αυτή η δήλωση αποποίησης ευθύνης να αμφισβητηθεί ως όρος συμβολαίου που αποκλείει την αμέλεια. Αυτό όμως είναι αποτελεσματικό, μόνο στην περίπτωση απόδειξης, του γενικά δυσαπόδεικτου γεγονότος, της αμέλειας. Επιπλέον, με λογικά επιχειρήματα αμφισβητείται ο σκοπός μίας ευρείας δήλωσης αποποίησης της νομικής ευθύνης από πλευρά της αρχής πιστοποίησης, αφού ακριβώς αυτό που αναμένεται από μία αρχή πιστοποίησης να επιβεβαιώσει είναι ότι αυτή έχει λάβει ορισμένα συγκεκριμένα μέτρα για να ελέγξει ότι κάποιο πρόσωπο υπήρξε σε κάποια στιγμή στο παρελθόν τουλάχιστον ένας από τα πρόσωπα που είχαν πρόσβαση στο κλειδί. Αυτό το γεγονός μπορεί στην καλύτερη

περίπτωση να λειτουργήσει μόνο σαν ένα επιχείρημα για την εξαγωγή του συμπεράσματος ότι ένα συγκεκριμένο ηλεκτρονικό αντικείμενο υπογράφηκε από ένα συγκεκριμένο πρόσωπο σε κάποια χρονική στιγμή. Αν ένα τέτοιο συμπέρασμα δεν μπορεί να αιτιολογηθεί , μπορεί να μην υπάρχει αιτιώδης σύνδεσμος με κάποια ανακρίβεια στο πιστοποιητικό και μπορεί όντως να μην υφίσταται τέτοια ανακρίβεια.

Αν μεταξύ των μέτρων που υπόσχεται η αρχή πιστοποίησης να τηρηθούν, βρίσκεται ο έλεγχος των γεγονότων με την αρχή εγγραφής, η αρχή πιστοποίησης δεν υπέχει νομικής ευθύνης για οποιαδήποτε ανακρίβεια απορρέει από σφάλμα της αρχής εγγραφής. Ακόμη και αν αποδειχθεί το γενικά δυσαπόδεικτο γεγονός του σφάλματος της αρχής εγγραφής, μπορεί και η ίδια να προστατευτεί αποτελεσματικά από μία δήλωση αποποίησης ευθύνης.

Η κατάσταση είναι διαφορετική και η θέση του θύματος πιο πλεονεκτική αν η αρχή πιστοποίησης εκδώσει «αναγνωρισμένο πιστοποιητικό», σύμφωνο με την ευρωπαϊκή οδηγία για τις ψηφιακές υπογραφές, επειδή σε ένα πλήθος περιπτώσεων η αρχή πιστοποίησης θα πρέπει να αποδείξει ότι δεν υπέδειξε αμέλεια. Δηλαδή, σε αυτήν την περίπτωση το βάρος της απόδειξης μεταβιβάζεται από το θύμα στην αρχή πιστοποίησης. Ωστόσο και αυτό μπορεί να μην αποδειχθεί ιδιαίτερα χρήσιμο, αφού η αρχή πιστοποίησης σε πολλές περιπτώσεις μπορεί να αποδείξει ότι το σφάλμα προέκυψε παρόλη την τήρηση από μέρους της των προβλεπόμενων διαδικασιών και έτσι να απαλλαγεί των ευθυνών της.

3.3 Εφαρμογές ηλεκτρονικών υπογραφών και πιστοποιητικών – εμπόδια και προϋποθέσεις ευρύτερης χρήσης

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

- Τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange -EDI) [38] (ά. 2 1994/820/ΕΚ)
- Ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη από EDI
- Ηλεκτρονικές δημόσιες προμήθειες
- Ηλεκτρονική ψηφοφορία
- Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες EuroPay, MasterCard, VISA μέσω του κοινού πρωτοκόλλου τους "EMV")
- Ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες (γενικής ή ειδικής χρήσης – π.χ. ναυτικές διεθνείς ταυτότητες) που συνήθως φέρουν ενσωματωμένα και κάποια βιομετρικά στοιχεία (φωτογραφία, δακτυλικά αποτυπώματα, κλπ.) του κατόχου τους
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου (S/MIME)
- Συστήματα υπογραφής αυθεντικότητας διακινούμενου λογισμικού (π.χ. Microsoft Authenticode [39])
- Κλειστές υποδομές PKI για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. NATO)
- Πιστοποίηση της ταυτότητας εξυπηρετητών διαδικτύου (web servers).

Στην Ευρωπαϊκή Ένωση, εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κλπ., έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία τυπικές εφαρμογές των ηλεκτρονικών υπογραφών, οι προϋποθέσεις των οποίων πηγάζουν από τον νόμο. Τα "ηλεκτρονικά δελτία ταυτότητας" σε χώρες όπως το Βέλγιο, Φινλανδία Ιταλία, Εσθονία [40] και αλλού, τα οποία χρησιμοποιούν την τεχνολογία PKI σε συνδυασμό με "έξυπνες κάρτες", αποτελούν ένα παράδειγμα τέτοιων τυπικών εφαρμογών.

Ένας άλλος τομέας εφαρμογής ηλεκτρονικών υπογραφών στην ΕΕ είναι τα ηλεκτρονικά τιμολόγια, τα οποία σύμφωνα και με την Ευρωπαϊκή Οδηγία 01/115/ΕΚ [41], εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών [42].

Άλλη εφαρμογή αποτελούν οι ηλεκτρονικές δημόσιες προμήθειες στο πλαίσιο των σχετικών σχεδίων Οδηγιών της ΕΕ. Επίσης, θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως η Υπηρεσία Επίσημων Δημοσιεύσεων [43], σχεδιάζουν την χρήση των ηλεκτρονικών υπογραφών για τα έγγραφα που εκδίδουν σε ηλεκτρονική μορφή (π.χ. την Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, τα περιεχόμενα των νομικών βάσεων δεδομένων CELEX, EUR-Lex & OEIL).

Στην Ελλάδα, μια από τις πρώτες εφαρμογές νομικά έγκυρης ηλεκτρονικής υπογραφής επίσημων εγγράφων, η οποία λειτουργεί ήδη από το 2002, είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αθηνών (ΧΑ) με τις εισηγμένες σ' αυτό εταιρίες. Το σύστημα αυτό ονομάζεται "ΕΡΜΗΣ" [44] (ή H.E.R.M.E.S -Hellenic Exchanges Remote MEssaging Services) και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων, δηλαδή εκπροσώπων των εισηγμένων, στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών (ένα για την ταυτοποίησή τους στο σύστημα και ένα για την αναγνωρισμένη ηλεκτρονική υπογραφή τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους) τοποθετημένα σε μια προσωποποιημένη έξυπνη κάρτα.

Παράλληλα, η υποστήριξη και η χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσότερων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια του προγράμματος για την Κοινωνία της Πληροφορίας και των σχετικών Επιχειρησιακών Προγραμμάτων των φορέων του ευρύτερου Δημόσιου Τομέα. Χαρακτηριστικά παραδείγματα αποτελούν τα έργα ψηφιοποίησης του Ποινικού Μητρώου του Υπουργείου Δικαιοσύνης [45], οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση Εμπορικών Σημάτων καθώς και το σύστημα ηλεκτρονικών Δημόσιων Προκηρύξεων & Προμηθειών στο Υπουργείο Ανάπτυξης (Γ.Γ. Εμπορίου), τα σχέδια για ηλεκτρονικές υπογραφές των ηλεκτρονικών Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ) του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ (e-ΚΕΠ).

Σημαντικότατη εξέλιξη προς την γενικευμένη χρήση ηλεκτρονικών υπογραφών στην Ελληνική Δημόσια Διοίκηση αποτελεί η υλοποίηση και η ολοκλήρωση του Υποέργου 9 του συνολικού έργου "Σύζευξις", όπου προβλέφθηκε η χρήση "Υποδομής Δημοσίου Κλειδιού" (PKI) και η πιστοποίηση ψηφιακών υπογραφών για έναν μεγάλο αριθμό (50.000) δημοσίων υπαλλήλων, οι οποίοι θα μπορούν να εκδίδουν, να υπογράφουν και να διακινούν "επίσημα" ηλεκτρονικά δημόσια έγγραφα.

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

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

Η τεχνική πολυπλοκότητα, οι παραλλαγές των εφαρμογών προηγμένων ηλεκτρονικών υπογραφών, και τα διαφορετικά επίπεδα νομικής αναγνώρισής τους, αναδεικνύουν ιδιαίτερες δυσκολίες ως προς την επίτευξη πλήρους διαλειτουργικότητας μεταξύ των υφιστάμενων εφαρμογών ηλεκτρονικής υπογραφής σε διεθνές και ευρωπαϊκό επίπεδο. Έχει παρατηρηθεί σχετικά ότι η διαλειτουργικότητα επιτυγχάνεται ευκολότερα σε κλειστές ή κεντρικά ελεγχόμενες εφαρμογές οι οποίες επιβάλλουν οι ίδιες συγκεκριμένες αναλυτικές προδιαγραφές (π.χ. τα πρότυπα 'EMV' για τις πιστωτικές κάρτες, συντονισμένες εφαρμογές 'ηλεκτρονικής διακυβέρνησης' ενός κράτους, κλπ.). Στα πλαίσια της Ευρωπαϊκής Ένωσης, παρά τα τέσσερα και πλέον χρόνια από την έκδοση της σχετικής Ευρωπαϊκής Οδηγίας που είχε ως στόχο την εναρμόνιση του σχετικού θεσμικού πλαισίου μεταξύ των κρατών-μελών, η παροχή πανευρωπαϊκώς αναγνωρισμένων και διαλειτουργικών μεταξύ τους υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, εξακολουθεί να εμφανίζει ακόμα αρκετές δυσχέρειες. Το γεγονός αυτό οφείλεται σε κάποιους ανασταλτικούς παράγοντες μεταξύ των οποίων περιλαμβάνονται:

- Ορισμένες ασάφειες του ευρωπαϊκού κανονιστικού πλαισίου, το οποίο προσπαθώντας να εξισορροπήσει μεταξύ τεχνολογικής ουδετερότητας και ασφάλειας δικαίου, καταλήγει σε ορισμένες αοριστίες .
- Η ανάπτυξη αυτόνομων εθνικών κανονιστικών πλαισίων σε ορισμένα κράτη-μέλη πριν από την έκδοση της Οδηγίας, και η διαφορετική ερμηνευτική προσέγγιση της Οδηγίας από αυτά τα κράτη μέλη, ώστε να διατηρηθεί απαράλλακτη η υφιστάμενη υποδομή τους.
- Οι αργοί ρυθμοί ανάπτυξης της προβλεπόμενης σχετικής προτυποποίησης από τους ευρωπαϊκούς οργανισμούς, δεδομένου ότι επιχειρείται η όσο το δυνατόν μεγαλύτερη συμβατότητα με τις υφιστάμενες (διαφορετικές) υποδομές και τα εφαρμοζόμενα συστήματα στα διάφορα κράτη-μέλη.

Μάλιστα, με εξαίρεση ορισμένα κράτη μέλη (π.χ. Ιταλία, Γερμανία και Φιλανδία) που είχαν προβεί εγκαίρως σε αναλυτικές ρυθμίσεις για την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, σοβαρά ζητήματα διαλειτουργικότητας υπάρχουν ακόμη και ανάμεσα στις σχετικές υπηρεσίες που παρέχονται από τους Παρόχους Υπηρεσιών Πιστοποίησης που λειτουργούν στο ίδιο κράτος, όπως παρατηρήθηκε -στο πλαίσιο της λειτουργίας της Ομάδας Εργασίας 'E2' του eBusinessForum- ότι συμβαίνει και στην Ελλάδα.

Τα σημαντικότερα προβλήματα διαλειτουργικότητας μεταξύ των υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών που παρατηρούνται, αναφέρονται κυρίως στην περιγραφή των στοιχείων του υποκειμένου των πιστοποιητικών (naming policy/conventions), στον τρόπο προσδιορισμού των επιτρεπόμενων χρήσεων των σχετικών κρυπτογραφικών κλειδιών και στα μέσα που χρησιμοποιούνται για την ενημέρωση των κατόχων και των αποδεκτών των ηλεκτρονικών πιστοποιητικών ως προς τους λοιπούς όρους έκδοσης και χρήσης που θέτονται από την εφαρμοζόμενη Πολιτική των εκδιδόμενων πιστοποιητικών. Επίσης σημαντικά ζητήματα υφίστανται και με άλλα σχετιζόμενα θέματα, όπως η χρονοσήμανση των υπογραφών, η πιστοποίηση των ιδιοτήτων των υποκειμένων, οι υπηρεσίες ενημέρωσης για την ανάκληση των πιστοποιητικών, η αλληλο-διαπίστευση των Παρόχων. Όλα αυτά έχουν ως πρόσθετο αρνητικό αποτέλεσμα την έλλειψη κοινώς αποδεκτών εφαρμογών

λογισμικού για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, οι οποίες να εφαρμόζουν και να ερμηνεύουν σωστά όλες τις παραπάνω παραμέτρους, ανεξάρτητα από τον εκδότη, το υποκείμενο, ή/και τον αποδέκτη των σχετικών πιστοποιητικών.

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

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

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

Τέλος, η υιοθέτηση ανοικτών προτύπων (όπως π.χ. τα OpenXades, Digi-Doc που έχουν υιοθετηθεί σε Φιλανδία και Εσθονία) και η χρήση της γλώσσας XML στην ανάπτυξη των σχετικών εφαρμογών ηλεκτρονικών υπογραφών (σύμφωνα και με τα σχετικά ευρωπαϊκά πρότυπα που έχουν εκδοθεί στα πλαίσια της πρωτοβουλίας European Electronic Signature Standardization Initiative ή EESSI [46]), μπορούν να παράσχουν πιο αναλυτικές και τυποποιημένες πληροφορίες στην λειτουργία των εφαρμογών αυτών και να συμβάλλουν στην επίτευξη μεγαλύτερης διαλειτουργικότητας και αναγνώρισης των σχετικών συναλλαγών σε πανευρωπαϊκό και διεθνές επίπεδο.

Η Ευρωπαϊκή Επιτροπή σε έκθεσή της [47] που ανακοινώθηκε τον Μάρτιο του 2006 επισημαίνει ότι η απροθυμία του περιβάλλοντος που συνοδεύει την χρήση των εργαλείων ηλεκτρονικής υπογραφής, επιβραδύνει σημαντικά την ανάπτυξη του εμπορίου αγαθών και υπηρεσιών μέσω του διαδικτύου. Ωστόσο, η χρήση των ηλεκτρονικών καρτών ταυτοποίησης και των ηλεκτρονικών υπογραφών στις υπηρεσίες ηλεκτρονικής διακυβέρνησης, αναμένεται να αυξηθούν στο εγγύς μέλλον. Η έκθεση επιβεβαιώνει επίσης ότι η Οδηγία του 1999 για ένα ενιαίο ευρωπαϊκό νομικό πλαίσιο που αφορά τις ηλεκτρονικές υπογραφές, συνεχίζει να αποτελεί την βάση για την χρήση των ηλεκτρονικών υπογραφών στις εσωτερικές αγορές.

3.4. PGP υπογραφές

3.4.1 Το σύστημα PGP

Το PGP (Pretty Good Privacy) είναι ένα σύστημα για την κρυπτογράφηση και την υπογραφή ηλεκτρονικών αντικειμένων, χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού. Το PGP κρυπτογραφεί τα μηνύματα με IDEA, διανέμει τα κλειδιά κρυπτογραφώντας τα με RSA και δημιουργεί ψηφιακές υπογραφές στα μηνύματα με MD5 και RSA [48]. Για την κυριότητα των κλειδιών το PGP δεν επαφίεται σε κάποια κεντρική αρχή, αλλά σε ένα δίκτυο εμπιστοσύνης, δηλαδή κάθε κλειδί υπογράφεται από άλλα κλειδιά και τελικά η εμπιστοσύνη του χρήστη σε κάποιο κλειδί εξαρτάται από την εμπιστοσύνη του ίδιου στα κλειδιά που υπέγραψαν το συγκεκριμένο κλειδί. Το PGP έχει τυποποιηθεί ως OpenPGP [49].

Το PGP χρησιμοποιείται συχνότερα για την κρυπτογράφηση και την αποστολή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνήθως μεταξύ ιδιωτών και οργανισμών, αλλά χρησιμοποιείται επίσης και ως τμήμα μίας ασφαλούς υποδομής ηλεκτρονικού εμπορίου, για παράδειγμα για την κρυπτογράφηση παραγγελιών από τον εξυπηρετητή διαδικτύου στο τμήμα που θα τις εκτελέσει.

3.4.2 Έννοια των PGP υπογραφών

Σε αυτή την παράγραφο εξετάζεται η νομική δέσμευση αυτού που υπογράφει με PGP υπογραφή ένα λογισμικό πακέτο κατά την διανομή του. Η ευθύνη, δηλαδή, του υπογράφοντος σε περίπτωση που το λογισμικό περιέχει ένα σφάλμα, έναν ιό ή οτιδήποτε μπορεί να βλάψει τον χρήστη που θα προμηθευτεί το λογισμικό.

Η υπογραφή έχει την έννοια που της προσδίδει το περιεχόμενο του αντικειμένου που υπογράφεται. Αν ο υπογράφων δεν είναι βέβαιος για αυτό, πρέπει να το διευκρινίσει, για παράδειγμα, εισάγοντας ένα σχόλιο σχετικά με το ότι η υπογραφή του αποσκοπεί στην ταυτοποίηση αυθεντικότητας της πηγής του κώδικα και δεν παρέχει εγγυήσεις ως προς το περιεχόμενο του κώδικα.

Ας σημειωθεί ότι γενικά είναι αδύνατη η απευθείας ανάγνωση του αντικειμένου που υπογράφεται ηλεκτρονικά, αφού μπορεί να πρόκειται για ένα έγγραφο κειμενογράφου ή ένα οποιοδήποτε φύλλο εργασίας. Ακόμη και το «απλό κείμενο» δεν μπορεί να αναγνωριστεί χωρίς την βοήθεια ενός text editor, παρόλο που σε αυτήν τουλάχιστον την περίπτωση δεν υπάρχει ο κίνδυνος εκπλήξεων, όπως για παράδειγμα η διατήρηση από έναν κειμενογράφο μίας παλαιότερης έκδοσης του κειμένου χωρίς αυτό να το παρουσιάζει στον δημιουργό του.

Το παραπάνω γεγονός βρίσκεται σε αντίθεση με τα έντυπα έγγραφα, όπου είναι πάντα ευδιάκριτο το περιεχόμενο του κειμένου που υπογράφεται. Ο σχεδιασμός πολλών σύγχρονων συστημάτων αγνοεί αυτό το πρόβλημα. Μία πιθανή επίθεση σε έναν ανυποψίαστο χρήστη είναι η μετατροπή του λογισμικού που παρουσιάζει το έγγραφο στον χρήστη και τελικά το γεγονός της υπογραφής του ηλεκτρονικού εγγράφου από τον χρήστη με την πεποίθηση ότι υπογράφει κάτι διαφορετικό από αυτό που πραγματικά υπογράφει. Ακόμη και η πιο διαδεδομένη πανάκεια για όλες τις απειλές της ασφάλειας, η έξυπνη κάρτα, δεν μπορεί να αντιμετωπίσει αυτό το πρόβλημα.

Η ευρεία χρήση των επισφαλών λειτουργικών συστημάτων και λογισμικού φαίνεται πιθανό να προκαλέσει προβλήματα σε αυτόν τον τομέα όσο διευρύνεται η χρήση των ηλεκτρονικών υπογραφών.

3.4.3 Νομική δεσμευτικότητα των PGP υπογραφών

Για να διερευνηθεί το ζήτημα της δεσμευτικότητας ή μη της PGP υπογραφής, πρέπει πρωτίστως να αναλυθεί το ζήτημα της δεσμευτικότητας ή μη της ιδιόχειρης υπογραφής.

Εξετάζοντας την περίπτωση της ιδιόχειρης υπογραφής μίας κάρτας γενεθλίων, δεν διαπιστώνουμε καμία νομική δέσμευση του υπογράφοντος, ακριβώς λόγω του ίδιου του περιεχομένου του κειμένου που υπογράφεται.

Στην πιο πολύπλοκη περίπτωση της ιδιόχειρης υπογραφής μίας επιταγής με μολύβι από το αριστερό χέρι του υπογράφοντος (ενώ αυτός είναι δεξιόχειρας), σημειώνεται ότι η τράπεζα μπορεί να θεωρήσει την επιταγή αναπόδεκτη εφόσον δεν αναγνωρίσει την επιταγή εφόσον αυτή δεν αναγνωρίσει την υπογραφή. Ωστόσο, ο αποδέκτης της επιταγής μπορεί να εγείρει αγωγή κατά του υπογράφοντος αν μπορεί να αποδείξει ότι εκείνος ήταν όντως ο υπογράφων, παραδείγματος χάρη, επειδή τον είδε ο ίδιος να υπογράφει την επιταγή. Στην τελευταία περίπτωση, η απόδειξη του γεγονότος ότι πράγματι ο εναγόμενος είναι ο υπογράφων, μπορεί να στηρίζεται απλά στην μαρτυρία του ενάγοντος και στην επιστημονική κρίση γραφολόγου. Η όποια άρνηση του εναγόμενου σχετικά με την υπογραφή της επιταγής από τον ίδιο τίθεται στην κρίση του δικαστηρίου. Τελικά, τα αποδεικτικά μέσα του ενάγοντος αρκεί να πείσουν το δικαστήριο ότι είναι περισσότερο πιθανό ο εναγόμενος να υπέγραψε την επιταγή από ότι να μην την υπέγραψε.

Στην περίπτωση πλαστογραφημένης υπογραφής σε επιταγή, η οποία εξαργυρώνεται από την τράπεζα και στην συνέχεια ο πελάτης της τράπεζας του οποίου η υπογραφή πλαστογραφήθηκε στραφεί κατά της τράπεζας για την χρέωση που έγινε στον λογαριασμό του λόγω της εξόφλησης της επιταγής αμφισβητώντας την υπογραφή, τότε η απόδειξη του γεγονότος ότι η υπογραφή ήταν πράγματι του πελάτη της τράπεζας εναπόκειται στην τράπεζα. Η τράπεζα, δηλαδή, πρέπει να πείσει το δικαστήριο ότι σύμφωνα με τον νόμο των πιθανοτήτων η ιδιόχειρη υπογραφή είναι πράγματι του πελάτη της και δεν πλαστογραφήθηκε από κακόπιστο τρίτο. Αν η υπογραφή είναι έντονα όμοια με αυτήν του πελάτη της τράπεζας, τότε αυτός μπορεί να προσκομίσει την μαρτυρία ειδικού γραφολόγου ότι πρόκειται πράγματι για πλαστογραφημένη υπογραφή.

Στην περίπτωση υπογραφής ενός εγγράφου για την μαρτυρία της υπογραφής άλλου προσώπου, η δέσμευση του υπογράφοντος έγκειται ακριβώς στο περιεχόμενο της υπογραφής του, δηλαδή ο υπογράφων δεσμεύεται μόνο ως προς το ποιόν είδε ο ίδιος να υπογράφει το έγγραφο και ως προς τίποτα περισσότερο. Στην περίπτωση που κληθεί ως μάρτυρας από το δικαστήριο για να επιβεβαιώσει τον ισχυρισμό του, δεν φέρει καμία ευθύνη ως προς το υπόλοιπο περιεχόμενο του κειμένου.

Η ιδιόχειρη υπογραφή είναι οποιοδήποτε σύμβολο χρησιμοποιεί κάποιος σαν υπογραφή για να δηλώσει την υιοθέτηση ή την αποδοχή από τον ίδιο του περιεχομένου ενός εγγράφου. Τα σημαντικό σημείο είναι ότι η έννοια της υπογραφής δεν εξαρτάται από σύμφυτα στοιχεία της υπογραφής, αλλά από το περιεχόμενο το οποίο υπογράφεται.

Οι κανόνες που ισχύουν για τις ηλεκτρονικές υπογραφές είναι ακριβώς οι ίδιοι. Η PGP υπογραφή κάποιου, όπως και η ιδιόχειρη υπογραφή του είναι έγκυρη αν όντως αυτός υπέγραψε.

Εν κατακλείδι, η μέθοδος PGP και οι παραλλαγές της (GPG, OpenPGP, κ.λ.π.) δημιουργούν μεν "ψηφιακές υπογραφές" (δηλαδή υπογραφές που ικανοποιούν τους όρους της νομοθεσίας για "προηγμένες" ηλεκτρονικές υπογραφές), όμως δεν μπορούν να παράξουν "αναγνωρισμένες" ηλεκτρονικές υπογραφές -εφόσον δεν υποστηρίζονται από ένα "αναγνωρισμένο πιστοποιητικό". Επειδή κανένας από τους

πιστοποιούντες δεν αναλαμβάνει ιδιαίτερη ευθύνη και υποχρεώσεις έναντι των τρίτων, η μέθοδος αυτή δεν πληροί προϋποθέσεις ασφάλειας για διενέργεια "σημαντικών συναλλαγών" μεταξύ αγνώστων, εφόσον δεν εξασφαλίζει "επαρκείς αποδείξεις" και δεν παρέχει εγγυήσεις ως προς την πραγματική ταυτότητα των συναλλασσομένων.

3.5 Τυχαιότητα, εντροπία και νομική ευθύνη του παροχέα λογισμικού

3.5.1 Τυχαιότητα και εντροπία

Μεγάλο μέρος της επιστήμης της κρυπτογραφίας ασχολείται με τους τυχαίους αριθμούς για την επίτευξη της ασφάλειας. Για παράδειγμα, κατά την επιλογή ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού είναι σημαντικό να διασφαλιστεί ότι ο επιτιθέμενος δεν θα μπορέσει να τα μαντέψει εύκολα. Αυτό επιτυγχάνεται με την τυχαία επιλογή τους. Παρομοίως, όταν πραγματοποιείται μία σύνοδος HTTP, επιλέγεται τυχαία ένα συμμετρικό κλειδί ώστε να κρυπτογραφηθεί αυτή η σύνοδος με ζητούμενη και εδώ την δυσκολία του επιτιθέμενου να μαντέψει το κλειδί. Ο τεχνικός όρος για το πόσο «καλοί» είναι οι τυχαίοι αριθμοί που επιλέγονται κάθε φορά, είναι εντροπία. Η εντροπία, δηλαδή, είναι το μέτρο του «μεγέθους» της διαθέσιμης κάθε φορά τυχαιότητας. Τις περισσότερες φορές, ενδείκνυται η ύπαρξη τουλάχιστον τόσης εντροπίας όσο το μέγεθος του τυχαίου αριθμού που επιλέχθηκε.

3.5.2 Εντροπία και νομική ευθύνη του παροχέα του λογισμικού

Η καλή κρυπτογραφία συνήθως βασίζεται στην καλή εντροπία. Δυστυχώς, η καλή εντροπία δεν είναι κάτι πάντα εύκολο να επιτευχθεί, αφού είναι λίγες οι μηχανές που έχουν μικρή διάδραση με το πραγματικό κόσμο. Αυτό συμβαίνει επειδή οι συνήθεις πηγές εντροπίας είναι πράγματα όπως οι κινήσεις του ποντικιού, τα χτυπήματα στο πληκτρολόγιο και τα συμβάντα στο δίκτυο. Το ερώτημα που απασχολεί είναι αν σε περίπτωση κακής εντροπίας ευθύνεται ο ιδιοκτήτης του κλειδιού.

Η απάντηση σε αυτό το ερώτημα εξαρτάται από τις εγγυήσεις ή τους υπόλοιπους όρους του συμβολαίου που ρυθμίζουν την σχέση μεταξύ του θύματος και του παροχέα του εμπλεκόμενου λογισμικού. Αν ο χρήστης μπορούσε να επέμβει με ενέργειές του για να αυξήσει την εντροπία με το χέρι (manually) δεν θα υπήρχε νομική ευθύνη. Διαφορετικά, μπορεί να υπήρχε νομική ευθύνη, ιδίως αν μπορούσε να αποδειχθεί ότι η διαδικασία που χρησιμοποιήθηκε δεν ανταποκρινόταν στα πρότυπα που συνήθως χρησιμοποιούνται για αυτόν τον σκοπό. Αλλά πρόκειται ούτως ή άλλως για δυσαπόδεικτες διαδικασίες αφού ο ας σημειωθεί, ότι ο όρος εντροπία, συχνά δεν εξηγείται στα εγχειρίδια που προορίζονται για τον τελικό χρήστη.

Η αποτυχία διασφάλισης καλής εντροπίας δημιουργεί πλήθος προβλημάτων. Δυστυχώς, οι μηχανές που τυπικά χρειάζονται περισσότερο την εντροπία, δηλαδή οι εξυπηρετητές (servers) είναι οι λιγότερο ικανοί να την έχουν. Για παράδειγμα, ο Netscape είχε ένα poor random seeding για το HTTPS στο οποίο πραγματοποιήθηκε επιτυχής επίθεση [50].

4. ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΜΒΑΣΕΙΣ

4.1 Από το π.δ. 150/2001 στο π.δ. 131/2003

Η νομική και η τεχνική διάσταση του όρου «υπογραφή» διαφέρουν σημαντικά. Για παράδειγμα, μία εικόνα σαρωτή της γραφής κάποιου δεν μπορεί να θεωρηθεί υπογραφή με καμία τεχνική έννοια, αλλά ο νόμος ενδεχομένως να την αναγνώριζε ως τέτοια.

Για να γίνει κατανοητή αυτή η διαφοροποίηση, είναι σημαντικό να σημειωθεί ότι η κατάρτιση συμβολαίων, τα οποία αποτελούν το βασικό συστατικό όλων των συναλλαγών, πρακτικά δεν εξαρτάται από την ασφαλή ταυτοποίηση αυθεντικότητας. Πολλά συμβόλαια, συγκεκριμένα η μεγάλη πλειοψηφία τους, ακόμη και στις εμπορικές συναλλαγές, δεν χρειάζονται υπογραφή για την ισχύ τους αλλά βασίζονται στις εμπορικές συνήθειες.

Το π.δ. 131/2003 [51] περιέχει μία σειρά διατάξεων στο κεφάλαιο 3 (ά. 8 ως 11) που ρυθμίζουν ζητήματα κατάρτισης συμβάσεων με ηλεκτρονικά μέσα. Αυτές οι διατάξεις λειτουργούν συμπληρωματικά προς τις γενικές διατάξεις του ΑΚ που αφορούν τις δηλώσεις βουλήσεως και αναφέρθηκαν στο οικείο κεφάλαιο. Σημαντικότερο, όμως, κρίνεται το γεγονός ότι με την αναγνώριση της εγκυρότητας της κατάρτισης συμβάσεων με ηλεκτρονικά μέσα, γίνεται ένα σημαντικό βήμα για την υπέρβαση του εμποδίου που συνιστά η υποχρέωση για την τήρηση συστατικού ή αποδεικτικού έγγραφου τύπου.

Ειδικότερα, θεμελιώδης είναι η διάταξη του άρθρου 8§1, η οποία ορίζει ότι με την επιφύλαξη των διατάξεων του π.δ. 150/2001 επιτρέπεται η κατάρτιση συμβάσεων με ηλεκτρονικά μέσα. Με την διάταξη αυτή ικανοποιείται η απαίτηση του κοινοτικού νομοθέτη, ο οποίος ορίζει στο άρθρο 9 § 1 της Οδηγίας 2000/31/ΕΚ [52] ότι "τα κράτη μέλη εξασφαλίζουν, ιδίως, ότι οι νομικές προϋποθέσεις που ισχύουν για την διαδικασία σύναψης των συμβάσεων δεν παρακωλύουν την χρήση των συμβάσεων που συνάπτονται με ηλεκτρονικά μέσα ούτε αποστερούν τις συμβάσεις αυτές εννόμου αποτελέσματος ή ισχύος λόγω του ότι έχουν συναφθεί με ηλεκτρονικά μέσα". Δηλαδή, ο εθνικός νομοθέτης υποχρεούται να άρει όλα τα νομικά και πρακτικά εμπόδια και να προσαρμόσει την νομοθεσία του ώστε να καταστήσει εφικτή την κατάρτιση συμβάσεων με ηλεκτρονικά μέσα σύμφωνα με την Οδηγία 2000/31/ΕΚ. Επίσης, στο άρθρο 9 § 1 της Οδηγίας γίνεται αναφορά και στην "χρήση" των συμβάσεων που συνάπτονται ηλεκτρονικά και επομένως καθίσταται σαφές ότι η προσαρμογή των νομοθεσιών δεν περιορίζεται μόνο στην κατάρτιση των ηλεκτρονικών συμβάσεων.

Έτσι, ο έλληνας νομοθέτης με το π.δ. 131/2003 θέσπισε τις αναγκαίες- γενικές διατάξεις για την προσαρμογή της ελληνικής νομοθεσίας στην παραπάνω Οδηγία. Η διάταξη του άρθρου 8 § 1 π.δ. 131/2003 συμπληρώνει τις διατάξεις των άρθρων 160 ΑΚ και 443 ΚΠολΔ και ουσιαστικά σημαίνει ότι όταν προβλέπεται έγγραφος τύπος, αυτός αναπληρώνεται από το ηλεκτρονικό έγγραφο, εφόσον αυτό, σύμφωνα με το άρθρο 3 §1 π.δ. 150/2001, φέρει προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής [53]. Επίσης, από τον συνδυασμό των διατάξεων 8 § 2 π.δ. 150/2001 και 8 § 1 π.δ. 131/2003 προκύπτει ότι η κατάρτιση συμβάσεων με ηλεκτρονικά μέσα είναι δυνατή με την χρήση απλής ηλεκτρονική υπογραφής, όταν από τον νόμο δεν προβλέπεται συστατικός τύπος για την κατάρτιση ορισμένης σύμβασης.

Ο έλληνας νομοθέτης εφάρμοσε και ορισμένες εξαιρέσεις κατά πρόβλεψη της αντίστοιχης κοινοτικής οδηγίας (ά. 9 § 2). Συγκεκριμένα, όρισε στο άρθρο 8 § 2 ότι

δεν εφαρμόζεται η προηγούμενη διάταξη που ορίζει ότι επιτρέπεται η κατάρτιση συμβάσεων με ηλεκτρονικά μέσα: (α) στις συμβάσεις που θεμελιώνουν ή μεταβιβάζουν εμπράγματα δικαιώματα επί ακινήτων, (β) στις συμβάσεις, οι οποίες απαιτούν εκ του νόμου προσφυγή στα δικαστήρια, δημόσιες αρχές ή επαγγέλματα που ασκούν δημόσια εξουσία και (γ) στις συμβάσεις, οι οποίες εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο.

Στις παραπάνω εξαιρέσεις δεν περιλαμβάνεται η κατάρτιση συμβάσεων μέσω ηλεκτρονικού ταχυδρομείου, όπως στην περίπτωση των άρθρων 9 § 3, 10 § 2 και συνεπώς, η κατάρτιση με την μέθοδο αυτή είναι καθ' όλα έγκυρη.

4.2 Παρεχόμενες πληροφορίες σε σχέση με την κατάρτιση της σύμβασης

Με το άρθρο 9 του π.δ. 131/2003 θεσπίζεται η υποχρέωση του φορέα παροχής υπηρεσιών να παρέχει τις απαραίτητες πληροφορίες, ώστε η διαδικασία κατάρτισης συμβάσεων να γίνεται με τρόπο σαφή, κατανοητό κι αδιαφιλονίκητο. Αξίζει να σημειωθεί ότι για την θέσπιση της αντίστοιχης κοινοτικής οδηγίας λήφθηκε υπόψη ότι οι ηλεκτρονικές συναλλαγές πραγματοποιούνται σε διάφορα στάδια, με αποτέλεσμα να μην είναι διαφανείς για τον αποδέκτη των υπηρεσιών, καθώς και ότι είναι δυνατόν να εμφιλοχωρήσουν σφάλματα ηλεκτρονικού χειρισμού [55].

Ειδικότερα, η διάταξη του άρθρου 9, ορίζει ότι εκτός από άλλες αιτήσεις παροχής πληροφοριών προβλεπόμενες από τις κείμενες διατάξεις, δηλαδή τις διατάξεις των άρθρων 4 και 5 του π.δ. 131/2003 και εφόσον δεν έχουν συμφωνήσει διαφορετικά τα συμβαλλόμενα μέρη που δεν είναι καταναλωτές, ο φορέας παροχής υπηρεσιών πρέπει να παρέχει τουλάχιστον τις εξής πληροφορίες κατά τρόπο σαφή, κατανοητό κι αδιαφιλονίκητο, πριν από την ανάθεση της παραγγελίας από τον αποδέκτη της υπηρεσίας:

α) τα διάφορα τεχνικά στάδια έως την σύναψη της σύμβασης, όπως εάν η πρόταση για κατάρτιση της σύμβασης πραγματοποιείται με την επιλογή εικονιδίου με το ποντίκι ή του πλήκτρου «ΟΚ» στην ιστοσελίδα του φορέα παροχής πληροφοριών ή με την συμπλήρωση φόρμας παραγγελίας ή με την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου, εάν η επιβεβαίωση της παραγγελίας θα αποσταλεί στον αποδέκτη της υπηρεσίας με μήνυμα ηλεκτρονικού ταχυδρομείου ή με διαφορετικό τρόπο κλπ.,

β) εάν ο φορέας παροχής υπηρεσιών θα αρχειοθετήσει ή όχι την σύμβαση μετά την σύναψή της, καθώς και εάν θα προβλέπεται δυνατότητα πρόσβασης σε αυτήν,

γ) τα τεχνικά μέσα που θα επιτρέπουν τον εντοπισμό και την διόρθωση σφαλμάτων ηλεκτρονικού χειρισμού πριν από την ανάθεση της παραγγελία και

δ) τις γλώσσες στις οποίες μπορεί να συναφθεί η σύμβαση.

Οι παραπάνω διατάξεις έχουν τεθεί με σκοπό την προστασία του καταναλωτή- αποδέκτη των υπηρεσιών της κοινωνίας της πληροφορίας και τα σχετικά ζητήματα μπορούν να ρυθμιστούν διαφορετικά μεταξύ των μελών που δεν είναι καταναλωτές (για παράδειγμα μεταξύ των επιχειρήσεων). Η παραπάνω διάταξη του άρθρου 9 § 1, ωστόσο, δεν εφαρμόζεται σε συμβάσεις που συνάπτονται αποκλειστικά μέσω ηλεκτρονικού ταχυδρομείου (με την προϋπόθεση ότι η σύναψη της σύμβασης πραγματοποιείται αποκλειστικά μέσω ηλεκτρονικού ταχυδρομείου και όχι μετά από επίσκεψη του αποδέκτη της υπηρεσίας στον ιστοχώρο του φορέα παροχής υπηρεσιών) ή άλλων ισοδύναμων ατομικών μέσων επικοινωνίας, όπως οι χώροι συνομιλιών (chat rooms).

Επίσης, το άρθρο 9 § 2 ορίζει ότι οι ατομικοί όροι της σύμβασης και οι ΓΟΣ πρέπει να διατίθενται κατά τρόπο που να επιτρέπει την αποθήκευση και αναπαραγωγή τους.

4.3 Χρόνος κατάρτισης της σύμβασης και διόρθωση λαθών

Με την διάταξη του άρθρου 10 § 1 ρυθμίζονται ζητήματα σχετικά με την κατάρτιση της ηλεκτρονικής σύμβασης. Συγκεκριμένα: α) καθιερώνεται η υποχρέωση του φορέα παροχής υπηρεσιών να αποστείλει αποδεικτικό παραλαβής της παραγγελίας του αποδέκτη χωρίς περιττή καθυστέρηση και με ηλεκτρονικά μέσα, β) ορίζεται ότι η παραγγελία και το αποδεικτικό παραλαβής θεωρείται ότι έχουν παραληφθεί όταν τα μέρη στα οποία απευθύνονται έχουν πρόσβαση σε αυτά καθώς και γ) ότι ο πρώτος οφείλει να θέτει στην διάθεση του αποδέκτη της υπηρεσίας κατάλληλα, αποτελεσματικά και προσιτά μέσα, που θα επιτρέψουν σ' αυτόν να επισημάνει και να διορθώσει τα λάθη του κατά τον ηλεκτρονικό χειρισμό πριν από την ανάθεση της παραγγελίας. Παρόμοια με το άρθρο 9 και εδώ, ορίζεται ότι τα μέρη που δεν είναι καταναλωτές μπορεί να συμφωνήσουν διαφορετικά στα πλαίσια μίας ηλεκτρονικής επικοινωνίας.

Έτσι, σύμφωνα με τα άρθρα 9 και 10 του π.δ. 131/2003, η διαδικασία σύναψης συμβάσεων πρέπει να γίνει σαφής, ενώ η σύμβαση δεν μπορεί να θεωρηθεί ως συναφθείσα, προτού ο φορέας παροχής υπηρεσιών αποστείλει το αποδεικτικό παραλαβής.

Όσο αφορά τα λάθη κατά τον ηλεκτρονικό χειρισμό πριν από την ανάθεση της παραγγελίας, καθιερώνεται η υποχρέωση του φορέα παροχής υπηρεσιών να διαμορφώνει τεχνικά την διαδικασία παραγγελίας προϊόντων ή υπηρεσιών έτσι, ώστε η παραγγελία να πραγματοποιείται σε διακριτά μεταξύ τους στάδια, να παρέχει την δυνατότητα στον αποδέκτη της υπηρεσίας για διόρθωση ενδεχομένων σφαλμάτων χειρισμού και να ζητεί επιβεβαίωση της παραγγελίας από τον χρήστη σε κάθε επόμενο στάδιο. Και εδώ, ορίζεται ότι η παράγραφος 1, πρώτη και τρίτη περίπτωση, δεν εφαρμόζεται σε συμβάσεις που συνάπτονται αποκλειστικά μέσω ηλεκτρονικού ταχυδρομείου ή άλλων ισοδύναμων ατομικών μέσων επικοινωνίας.

4.4 Online συμβάσεις

Το Διαδίκτυο αποτελεί προέκταση της κοινωνίας μας και κατά συνέπεια εφαρμόζονται σ' αυτό, κατ' αναλογία, οι ισχύουσες νομοθετικές ρυθμίσεις. Το Διαδίκτυο παρέχει τεράστιες δυνατότητες εμπορικής εκμετάλλευσής του, αποτελώντας ένα νέο χώρο εμπορικών συναλλαγών. Το ηλεκτρονικό ταχυδρομείο, ο Παγκόσμιος Ιστός αλλά και άλλοι τρόποι επικοινωνίας διευκολύνουν σε μεγάλο βαθμό τη σύναψη συμβάσεων. Το μεγαλύτερο μέρος του ηλεκτρονικού εμπορίου διενεργείται με τη σύναψη συμβάσεων μεταξύ των χρηστών του διαδικτύου που είναι οι καταναλωτές και των προμηθευτών αγαθών και υπηρεσιών. Στην περίπτωση των εμπορικών συναλλαγών μέσω Διαδικτύου, κάνουμε λόγο για συναπτόμενες με ηλεκτρονικά μέσα συμβάσεις, τις λεγόμενες online συμβάσεις.

Οι συμβάσεις στο Διαδίκτυο (on-line συμβάσεις) λαμβάνουν συνήθως δύο μορφές:

Α) είτε είναι συνήθεις ηλεκτρονικές συμβάσεις μη τυποποιημένου μηνύματος, είτε Β) είναι συμβάσεις Ηλεκτρονικής Ανταλλαγής Δεδομένων – EDI (electronic data interchange), δηλαδή βασίζονται σε τυποποιημένο μήνυμα.

Σχετικά με τις συμβάσεις EDI σημειώνεται ότι η ανάγκη πιο άνετης ανταλλαγής δεδομένων στο Διαδίκτυο, οδήγησε στην ανάπτυξη μεθόδων τυποποιήσεως των δεδομένων. Οι συμβάσεις EDI περιέχουν τυποποιημένες πληροφορίες, προσφέροντας τη δυνατότητα αυτοματοποίησης, τόσο της διαδικασίας παραγγελίας και σύναψης της σύμβασης, όσο και της πληρωμής

Ένα κοινό χαρακτηριστικό των συμβάσεων που καταρτίζονται στο Διαδίκτυο είναι ότι καταρτίζονται ως επί το πλείστον είτε βάσει προσυντεταγμένων ηλεκτρονικών εγγράφων, ως συμβάσεις προσχώρησης, είτε με προδιατυπωμένους γενικούς όρους συναλλαγών (ΓΟΣ).

Αυτές οι συμβάσεις που αναρτώνται σε κάθε ιστοσελίδα είναι γνωστές ως online συμβάσεις. Online συμβάσεις είναι οι συμβατικοί όροι (ΓΟΣ) των οποίων τα σημεία πρόσβασης (links) τοποθετούνται σε εμφανές σημείο της κεντρικής σελίδας κάθε δικτυακού τόπο και περιέχουν τους Όρους Χρήσης (Terms of Use) και την Πολιτική Διαχείρισης Προσωπικών Δεδομένων (Privacy Policy). Οι online συμβάσεις αφορούν όλους τους ιδιοκτήτες-διαχειριστές δικτυακών τόπων, είναι υποχρεωτικές και πρέπει να είναι προσιτές στους επισκέπτες.

Οι συγκεκριμένες συμβάσεις είναι συμβάσεις προσχωρήσεως. Δεν αποτελούν αντικείμενο διαπραγμάτευσης μεταξύ των μερών αλλά είναι δεδομένα κείμενα που ορίζουν κάθε φορά οι ιδιοκτήτες-διαχειριστές των δικτυακών τόπων και οι επισκέπτες, είτε τους αποδέχονται και κάνουν χρήση του δικτυακού τόπου, είτε όχι οπότε και αλλάζουν διεύθυνση. Επειδή οι online συμβάσεις αποτελούν μαζικές συμβάσεις στις οποίες ο ιδιοκτήτης του δικτυακού τόπου προδιατυπώνει τους όρους της σύμβασης και ο καταναλωτής-χρήστης του Διαδικτύου μπορεί απλώς να προσχωρήσει ή όχι είναι απαραίτητη η προστασία των τελευταίων από καταχρηστικούς όρους τέτοιων συμβάσεων.

Όσο αφορά την δήλωση βουλήσεως στην περίπτωση κατάρτισης on-line συμβάσεων, εδώ, η ηλεκτρονική δήλωση βούλησης πρέπει να περιέχει πρόταση σύναψης σύμβασης και δήλωση αποδοχής αυτής, ενώ ο Η/Υ χρησιμεύει απλά για τη διαβίβασή της, η οποία είναι δυνατή κυρίως μέσω e-mail. Ελαττωματική είναι η ηλεκτρονική δήλωση βούλησης όταν είναι αποτέλεσμα απάτης ή απειλής. Η απειλή είναι πάντα έμμεση, ασκείται δηλαδή στον χρήστη του Η/Υ.

Η απάτη μπορεί να είναι έμμεση, ή και άμεση, όταν π.χ. τρίτος, μέσω hacking, εισάγει με πρόθεση λανθασμένα δεδομένα στον Η/Υ, ο οποίος αυτόματα διαβιβάζει ελαττωματική δήλωση βούλησης.

4.5 Νομικό πλαίσιο προστασίας των καταναλωτών σε σχέση με τις online συμβάσεις

Ιδιαίτερα σημαντικές είναι οι πρωτοβουλίες της Ευρωπαϊκής Ένωσης προκειμένου να ενισχυθεί το νομικό πλαίσιο προστασίας των καταναλωτών σε σχέση με τις online συμβάσεις. Στην Ευρώπη ισχύουν [56]:

- Η Οδηγία 87/102/ΕΟΚ όπως τροποποιήθηκε από την Οδηγία 90/88/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη

- Η Σύσταση 92/295/ΕΟΚ σχετικά με τους κώδικες δεοντολογίας για την προστασία των καταναλωτών όσον αφορά συμβάσεις διαπραγματευόμενες από απόσταση

- Η Οδηγία 2000/31/ΕΚ για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική

αγορά όπου γίνεται εκτενής αναφορά στις συμβάσεις που συνάπτονται με ηλεκτρονικά μέσα

- Η Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών

- Η Σύσταση 97/489/ΕΚ σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου όπου αναφέρονται οι απαραίτητοι όροι που πρέπει να περιλαμβάνονται στις συμβάσεις

- Η Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις

- Η Οδηγία 99/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές

Στην Ελλάδα ισχύει ο ν. 2251/1994 για την προστασία Καταναλωτή που παρέχει επαρκή προστασία τους καταναλωτές.

Οι διαδικτυακές συμβάσεις και η χρήση των ΓΟΣ ενέχουν τον κίνδυνο της καταπλεονεκτικότητας σε βάρος του οικονομικά ασθενέστερου συμβαλλόμενου, δηλαδή του καταναλωτή-χρήστη του διαδικτύου, μια και ο τελευταίος δεν έχει την δυνατότητα διαπραγμάτευσής των όρων. Γι' αυτό κρίνεται απαραίτητη η προστασία του χρήστη με τις διατάξεις των παραπάνω νομοθετημάτων.

5. ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΝΟΜΟΘΕΤΙΚΩΝ ΠΡΟΒΛΗΜΑΤΩΝ ΚΑΙ ΠΑΡΑΛΕΙΨΕΩΝ

Στην βιβλιογραφία [62] εμφανίζεται κριτική ορισμένων διατάξεων των νομοθετημάτων π.δ. 150/2001 και 1999/93/ΕΚ σχετικά με ασάφειες ή/ και παραλείψεις που εμφανίζουν, ενώ παράλληλα προτείνονται λύσεις για την αντιμετώπισή τους.

Τα παραπάνω οφείλονται σε μεγάλο βαθμό στο ότι ο Έλληνας νομοθέτης, στην προσπάθειά του να εναρμονίσει την ελληνική νομοθεσία με την αντίστοιχη κοινοτική, υπέδειξε ως ένα βαθμό διστακτικότητα και δεν αξιοποίησε στον βαθμό που θα μπορούσε την δυναμική και τις δυνατότητες της Οδηγίας, χωρίς να μεριμνήσει παράλληλα για τις ειδικές συνθήκες που ισχύουν στην Ελλάδα.

5.1 Αναφορικά με το ΠΔ 150/2001

Το άρθρο 1 § 2 του παρόντος π.δ., ορίζει ότι «οι διατάξεις του παρόντος διατάγματος δεν θίγουν διατάξεις που, αναφορικά με την σύναψη και την ισχύ συμβάσεων ή εν γένει την σύσταση νομικών υποχρεώσεων, επιβάλλουν την χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων, ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα». Ωστόσο, αν λάβει κανείς υπόψη τη βούληση και τον σκοπό του κοινοτικού νομοθέτη, όπως αναφέρονται στο προοίμιο της Οδηγίας 1999/93, να προάγει δηλαδή τη χρήση των ηλεκτρονικών υπογραφών, η ανωτέρω διατύπωση θα έπρεπε να είναι πιο συγκεκριμένη. Θα ήταν χρήσιμο δηλαδή, να προβλέπεται συμπληρωματικά πως σε περίπτωση που κάποιος κανόνας του ελληνικού δικαίου προάγει την χρήση των ηλεκτρονικών υπογραφών, τότε αυτός ο κανόνας θα έπρεπε να εφαρμόζεται. Αντίθετα, αν κάποιος κανόνας του εσωτερικού δικαίου εμποδίζει ή αποτρέπει την χρήση των ηλεκτρονικών υπογραφών, τότε αυτός ο κανόνας ενδεχομένως θα έπρεπε να παραμεριστεί.

Μία συμπλήρωση και διευκρίνιση του παραπάνω άρθρου θα ήταν ίσως αναγκαία, ώστε ο δικαστής να μην αποφασίζει με αποκλειστικό κριτήριο το γράμμα του νόμου (δηλαδή το 1 § 2) ποιος κανόνας δικαίου πρέπει να εφαρμοστεί, αλλά να είναι ελεύθερος να κρίνει κατά περίπτωση με κριτήρια τελεολογικά, δηλαδή τον σκοπό διάδοσης των ηλεκτρονικών υπογραφών.

Εντοπίζεται επίσης η ανεξήγητη, ομολογουμένως, διαφοροποίηση του Έλληνα νομοθέτη σε σχέση με το κείμενο της Οδηγίας 1999/93, όσο αφορά στον ορισμό της προηγμένης ηλεκτρονικής υπογραφής. Το άρθρο 2 § 2 του π.δ. 150/2001 χρησιμοποιεί την ορολογία «ψηφιακή υπογραφή» διαζευκτικά με την ορολογία «προηγμένη ηλεκτρονική υπογραφή». Στο σημείο αυτό ο Έλληνας νομοθέτης περιορίζει χωρίς προφανή λόγο την έννοια της προηγμένης ηλεκτρονικής υπογραφής ταυτίζοντάς την με την ψηφιακή, θεωρώντας έτσι λανθασμένα ότι μόνο η ψηφιακή υπογραφή, η οποία βασίζεται στην ασύμμετρη κρυπτογραφία, πληροί τα τέσσερα κριτήρια (α. Να συνδέεται μονοσήμαντα με τον υπογράφοντα, β. Να είναι ικανή να ταυτοποιήσει τον υπογράφοντα, γ. Να δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, δ. να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων) της προηγμένης ηλεκτρονικής υπογραφής.

Αντίθετα, η Οδηγία 1999/93, παρά το γεγονός ότι έχει υποστηριχθεί πως αναφέρεται κατά βάση στις ψηφιακές υπογραφές, καλύπτει με τη διατύπωσή της κάθε προηγμένη ηλεκτρονική υπογραφή που πληροί τα τέσσερα κριτήρια, έστω κι αν αυτή

δεν στηρίζεται στην ασύμμετρη κρυπτογραφία (επιθυμητή η τεχνολογική ουδετερότητα της νομοθεσίας).

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

Αξίζει να σημειωθεί η αναξιοποίητη δυνατότητα πρόβλεψης πρόσθετων απαιτήσεων για την χρήση ηλεκτρονικών υπογραφών στον δημόσιο τομέα, κάτι που δόθηκε σαν δυνατότητα από τον άρθρο 3 § 7 της Οδηγίας 1999/93 και ο Έλληνας νομοθέτης δεν αξιοποίησε παρόλο που στην χώρα μας πολλές δημόσιες υπηρεσίες διαχειρίζονται ευαίσθητα προσωπικά δεδομένα πολιτών και ο δημόσιος τομέας είναι πολύ ευρύς και παίζει πρωταγωνιστικό ρόλο στις συναλλαγές.

Τέλος, αξιόλογες πρωτοβουλίες εκ μέρους του Έλληνα νομοθέτη προκειμένου να ενθαρρύνει την χρήση των ηλεκτρονικών υπογραφών θα ήταν η μέριμνα για την σύνταξη κωδίκων δεοντολογίας μεταξύ καταναλωτικών κι επαγγελματικών οργανώσεων, αλλά και η σύνταξη πολιτικών ηλεκτρονικής υπογραφής, δηλαδή κειμένων με σκοπό την διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών και των πιστοποιητικών τους σε εφαρμογές ομοειδών συναλλακτικών κύκλων, όπως ο δημόσιος τομέας και οι τράπεζες.

5.2 Αναφορικά με την Οδηγία 1999/93/ΕΚ

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

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

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

νομοθεσίες στο συγκεκριμένο ζήτημα θα μπορούσε να διασφαλιστεί μόνο μέσα από σαφείς οδηγίες του κοινοτικού νομοθέτη.

Ζωτικής σημασίας κρίνεται και η θέσπιση υποχρεωτικής ασφάλισης αστικής ευθύνης από τον Πάροχο Υπηρεσιών Πιστοποίησης, κάτι το οποίο δεν προβλέφθηκε από τον κοινοτικό νομοθέτη. Δικαιολογημένα θα υποστήριζε κανείς ότι η υποχρεωτική σύναψη σύμβασης ασφάλισης που να καλύπτει τους κινδύνους από την έκδοση αναγνωρισμένων πιστοποιητικών είναι επιβεβλημένη, λόγω των τεράστιων οικονομικών συμφερόντων που μπορεί να διακυβεύονται κατά την διακίνηση εγγράφων μέσω ηλεκτρονικών δικτύων. Μάλιστα, η σύναψη σύμβασης ασφάλισης ίσως επιβάλλεται και από την πιθανή πληθώρα δικών που αναμένεται να προκαλέσει η αντιστροφή του βάρους της απόδειξης στις περιπτώσεις του άρθρου 6 της Οδηγίας.

Συγκεκριμένα, στο άρθρο 6 § 1, 2 της Οδηγίας ο νομοθέτης επέλεξε να θεσπίσει την περιορισμένη εφαρμογή της δικονομικής αντιστροφής του βάρους της απόδειξης (νόθα αντικειμενική ευθύνη των Παρόχων), δηλαδή μόνο για τις περιπτώσεις που περιγράφονται στο συγκεκριμένο άρθρο. Ωστόσο, με την πάροδο του χρόνου, όταν η λειτουργία της αγοράς και οι ηλεκτρονικές συναλλαγές των καταναλωτών και των σχέσεών τους με τους Παρόχους είναι πιο ώριμες, θα καταδειχθεί το κατά πόσο απαιτείται ή όχι να έχει ο Πάροχος Υπηρεσιών Πιστοποίησης το βάρος της απόδειξης μόνο για τις περιπτώσεις που περιγράφονται στις § 1 και § 2 του άρθρου 6.

Τέλος, ένα σημείο που ίσως πρέπει να τροποποιηθεί στο άρθρο 6 της Οδηγίας είναι η ανυπαρξία οποιασδήποτε αναφοράς σε υποχρεώσεις από την πλευρά του κατόχου της ηλεκτρονικής υπογραφής, του κατόχου του σχετικού πιστοποιητικού και του καλόπιστου τρίτου. Βέβαια, το βάρος της απόδειξης που έχει ο Πάροχος στις περιπτώσεις § 1 και § 2 του άρθρου 6 ενθαρρύνει τους καταναλωτές να εμπιστευτούν τις ηλεκτρονικές υπογραφές και να συμμετάσχουν στην Κοινωνία της Πληροφορίας. Όμως, ίσως το βάρος αυτό να είναι δυσανάλογο για τον Πάροχο, λόγω της ευκολίας με την οποία οποιοσδήποτε, καλόπιστος ή κακόπιστος κάτοχος ηλεκτρονικής υπογραφής ή αναγνωρισμένου πιστοποιητικού ή ένας τρίτος που βασίζεται σε αυτό μπορεί να κατηγορήσει τον Πάροχο για πταίσμα. Η δυσκολία του Παρόχου να αποδείξει δικαστικά ότι δεν ευθύνεται θα μπορούσε να οδηγήσει σε ατέρμονους και δαπανηρούς δικαστικούς αγώνες, άρα μία πιο επιεικής για τον Πάροχο νομοθετική πρόβλεψη θα έπρεπε να θεσπιστεί στις περιπτώσεις των § 1 και § 2 του άρθρου 6 (π.χ., ειδική νομική υποχρέωση των προσώπων που βασίζονται στο αναγνωρισμένο πιστοποιητικό να ενημερώνουν χωρίς υπαίτια καθυστέρηση τον Πάροχο, όταν ανακαλύπτουν ότι μια ηλεκτρονική υπογραφεί έχει κλαπεί ή πλαστογραφηθεί ή ότι ένα πιστοποιητικό έχει αλλοιωθεί).

Βιβλιογραφία

[1] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. pp. 5, CRC Press, 1996. www.cacr.math.uwaterloo.ca/hac

[2] Στέλιος Ν. Κουσούλης. Σύγχρονες μορφές έγγραφης συναλλαγής. σελ. 138, Σάκκουλας Αντ. Ν. 1992.

[3] R. Shirey. Internet Security Glossary. RFC 2828, 2000. http://www.ietf.org/rfc/rfc2828.txt

[4] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Trns, Inform. Theory, pp. 644- 654 IT- 22, 6, 1976. Rivest, R.L., Shamir, A., Adleman, L.A.. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, pp.120- 126, Vol.21, Nr.2, 1978.

[5] T. Dierks, C. Allen. RFC 2246 – The TLS Protocol. January 1999. http://www.ietf.org/rfc/rfc2246.txt

[6] A. Frier, P. Karlton and P. Kocher. The SSL 3.0 Protocol, Netscape Communications Corp., November, 1996.

[7] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners- Lee. RFC 2068 – Hyperterxt Transfer Protocol – HTTP/1.1. January 1997. http://www.ietf.org/rfc/rfc2068.txt

[8] ΠΔ 150/2001 (ΦΕΚ 125 Α'/25-6-2001).

[9] S.Goldwasser, S.Micali, and R.Rivest. A digital Signature Scheme Secure against Adaptive Chosen Message Attack. SIAM Journal on Computing, 17(2): 281- 308, 1988.

[10] Principles for Electronic Authentication - A Canadian Framework. The digital economy in Canada. http://www.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html

[11] ISO/IEC JTC 1/SC27. Information technology Securitytechniques – Non repudiation – Part 1: General Model. ISO International Standard 13888-1, 1997.

[12] ISO/IEC JTC 1/SC27. Information technology – Security techniques – Non repudiation – Part 3: Using asymmetric techniques. ISO International Standard 13888-3, 1997.

[13] ISO/IEC JTC 1/SC27. Information technology – Security techniques – Non repudiation – Part 1: General model. ISO International Standard 13888-1, 1997

[14] Public-Key Infrastructure (X.509) (pkix). Internet Working Group.

[15] S. Haber and W.S. Stornetta. How to Time-Stamp a digital Document. *Journal of Cryptology*, 3(2):99-111, 1991.

[16] Law Commission. Electronic Commerce: Formal Requirements in Commercial Transactions, December, 2001.http://www.lawcom.gov.uk

[17] Αστικό εθιμικό δίκαιο βάσει του δεδικασμένου (common law)

[18] Δ.Μαρτάκος, Ν.Κυρλόγλου, Α.Μητράκας, Μ.Γιαννακάκη, Χ.Σιουλής. Δεκάλογος για τις ηλεκτρονικές υπογραφές & τα ηλεκτρονικά πιστοποιητικά ταυτοποίησης. Ε- business forum, Ομάδα εργασίας Ε-2.

[19] Position paper on e-Signatures review, American Chamber of Commerce to the European Union (AMCHAM EU).
http://www.amchameu.be/Pops/2004archive/esignatures02162004.pdf

[20] Νομικά θέματα ηλεκτρονικού εμπορίου, Ψηφιακές υπογραφές, Τράπεζα Νομικών Πληροφοριών Ηλεκτρονικού Εμπορίου του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών. http://www.acci.gr/ecomm/legal/index.htm

[21] Ευρωπαϊκή Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 "Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές".

[22] J.Dumortier, S.Kelm, H.Nilsson, G.Skouma, P.V.Eecke. The legal and market aspects of electronic signatures, Interdisciplinary Centre for Law and Information Technology, Study for the European Commission, DG Information Society, 2003
[23] ΠΔ 150/2001 (ΦΕΚ 125 Α'/25-6-2001).
[24] Ν. 2672/1998 (ΦΕΚ 290 Α'/28-12-1998).
[25] Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων. http://www.eett.gr
[26] ΠΔ 340/2002 (ΦΕΚ 283/Α΄/2002)
[27] Μανιώτης. Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο, σ. 40, Σάκκουλας Αντ. Ν., 1998.
[28] Ε. Αλεξανδρίδου. Η πρόταση Οδηγίας της Ε.Ε. για το ηλεκτρονικό εμπόριο και η προστασία του καταναλωτή. Δίκαιο Επιχειρήσεων και Εταιριών (ΔΕΕ), σελ.122, 2/ 2000.
[29] Για τους ειδικούς κανόνες, κυρίως κοινοτικής προέλευσης, που ρυθμίζουν τις τεχνικές πτυχές της κρυπτογράφησης Ιγγλεζάκης, Οι νομικές ρυθμίσεις για τις ψηφιακές υπογραφές. Η Οδηγία 1999/93/ ΕΚ και οι εθνικές νομοθεσίες. Επισκόπηση Εμπορικού Δικαίου (ΕπισκΕΔ), σελ. 621, Γ/ 2000.
[30] Κ. Χριστοδούλου, Ηλεκτρονικά έγγραφα, Σάκκουλας Αντ. Ν., σελ. 77, 2001.
[31] Μονομελές Πρωτοδικείο Αθηνών (ΜΠρΑθ) 1327/2001, Δίκαιο Επιχειρήσεων και Εταιριών (ΔΕΕ), σελ.377, 2001, με σημ. Κουσούλη. Νομολογία (Πιστωτικοί τίτλοι). Πρόεδρος: Π. Λυμπερόπουλος, Δικηγόρος: Ι. Βρέλλος.
[32] Microsoft Security Bulletin MS01-017. http://www.microsoft.com/-technet/treeview/default.asp?url=/technet/security/bulletin/MS01-017.asp
[33] ITU-T Recommendation X.509 (1997 E): Information Technology- Open Systems Interconnection- The Directory: Authentication Framework, June 1997.
[34] Information technology – open systems interconnection – the directory: Authentication framework. ISO/IEC 9594-8, 1995.
[35] ISO/DIS 9735-9.
[36] Μια απλή κατάσταση στην οποία δεν απαιτείται κάποια PKI είναι αυτή της τοπολογίας αστέρος, όπου όλοι οι συμμετέχοντες επικοινωνούν με ασφάλεια μόνο με ένα κεντρικό μέλος. Σε αυτή την περίπτωση το κεντρικό μέλος μπορεί να διατηρεί έναν πίνακα με τα δημόσια κλειδιά όλων των άλλων μελών. Αυτά από τη μεριά τους χρειάζεται να ξέρουν μόνο το δημόσιο κλειδί του κεντρικού μέλους.
[37] Y. Yeong, T. Howes, and S. Kille. Lightweight Directory Access Protocol. RFC 1777, 1995.
[38] Άρθρο 2 της Σύστασης 1994/820/ΕΚτης Ευρωπαϊκής Επιτροπής, της 19ης Οκτωβρίου 1994 (Επίσημη εφημερίδα Ευρωπαϊκής Κοινότητας Ε.Κ. EL 388/28-12-1994)
[39] Microsoft TechNet, http://technet.microsoft.com/en-us/library/cc750035.aspx
[40] The Estonian ID card and Digital Signature concept, Principles and solutions, Whitepaper, Version: June 5, 2003.
[41] Ευρωπαϊκή Οδηγία 2001/115/ΕΚ του Συμβουλίου της 20ής Δεκεμβρίου 2001 για την τροποποίηση της οδηγίας 77/388/ΕΟΚ με στόχο την απλοποίηση, τον εκσυγχρονισμό και την εναρμόνιση των όρων που επιβάλλονται στην τιμολόγηση όσον αφορά το φόρο προστιθέμενης αξίας.

[42] Μ. Γυφτάκη. Ηλεκτρονική τιμολόγηση (e-invoicing), διαβίβαση και αποθήκευση ηλεκτρονικών τιμολογίων, γλώσσα διατύπωσης τιμολογίων, ανάθεση εκτύπωσης τιμολογίων σε τρίτους., Epsilon7, σελ. 1923.
[43] Υπηρεσία εκδόσεων Ευρωπαϊκής Ένωσης,
http://publications.europa.eu/index_el.htm

[44] H.E.R.M.E.S -Hellenic Exchanges Remote MEssaging Services. https://hermes D_EXT/ ase.gr/HERMES_PR
[45] Ψηφιοποίηση του Ποινικού Μητρώου του Υπουργείου Δικαιοσύνης. http://www.teg.cti.gr/Projects/Ergo12.htm
[46] European Electronic Signature Standardization Initiative (EESSI), The European Electronic Signature Standardisation Initiative (EESSI) open meeting: "European Signatures vs Global Signatures". http://ec.europa.eu/idabc/en/document/1441/5848
[47] Europa, Press releases RAPID, IP 06/325. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/325&format=HTML&aged=0&language=EN&guiLanguage=en
[48] R. Shirey. Internet Security Glossary. RFC 2828, 2000. http://www.ietf.org/rfc/rfc2828.txt
[49] J. Callas, L. Donnerhacke, H. Finney, R. Thayer. RFC 2440 - OpenPGP Message Format. RFC 2440, 1998. http://www.ietf.org/rfc/rfc2440.txt
[50] I. Goldberg and D. Wagner. Randomness and the Netscape Browser. Berkeley, Dr. Dobb's Journal, pp. 66- 70, January 1996. http://www.cs.berkeley.edu/daw/papers/ddj-netscape.html.
[51] ΠΔ 131/2003 (ΦΕΚ 116 Α΄ /16.05.2003).
[52] Ευρωπαϊκή Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).
[53] Ι. Ιγγλεζάκης. Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, σελ. 141, Σάκκουλας ΑΕ, 2003.
[54] Θ. Σιδηρόπουλος. Το δίκαιο του Διαδικτύου, Ηλεκτρονικές συμβάσεις, Πνευματική ιδικτησία, Προστασία προσωπικών δεδομένων, Κατοχύρωση και χρήση "domain name". Σάκκουλας ΑΕ, 2003.
[55] Ι. Ιγγλεζάκη. Προστασία του καταναλωτή στις τηλεαγορές μέσω Internet. Επιθεώρηση του Εμπορικού Δικαίου (ΕΕμπΔ), σελ. 835, 2000.
[56] Δικτυακός τόπος η- επιχειρείν. On-line συμβάσεις. http://www.go-online.gr/ebusiness/specials/article.html?article_id=71
[57] Ευρωπαϊκή Οδηγία 87/102/ΕΟΚ του Συμβουλίου, της 22ας Δεκεμβρίου 1986, για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.
[58] Ευρωπαϊκή Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990.
[59] Σύσταση 92/295/ΕΟΚ σχετικά με τους κώδικες δεοντολογίας για την προστασία των καταναλωτών όσον αφορά συμβάσεις διαπραγματευόμενες από απόσταση
[60] Ευρωπαϊκή Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικάμε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).
[61] Σύσταση 97/489/ΕΚ της 30ής Ιουλίου 1997 σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου.
[62] Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.
[61] Ν. 2251/1994 (ΦΕΚ 191 Α΄/ 16-11-1994).

[62] Κ.Α. Καραδημητρίου. Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο. Σάκκουλας ΑΕ, σελ. 155- 176, 2008.