Οι Ηλεκτρονικες Υπογραφες στο Ευρωπαϊκο και Ελληνικο Δικαιο:

Ζητηματα Εφαρμογων στον Τραπεζικο Τομεα

ΑΝΔΡΕΑ ΜΗΤΡΑΚΑ ΔΝ
Ubizen NV

1. Εισαγωγή

Η χρήση του Internet για εμπορικούς σκοπούς δημιούργησε σημαντικές δυνατότητες ανάπτυξης των ανοικτών ηλεκτρονικών συναλλαγών[1]. Καθώς μαζί με τις εμπορικές ευκαιρίες όμως αυξήθηκε και ο προβληματισμός σχετικά με τη δεσμευτικότητα των ανοικτών ηλεκτρονικών συναλλαγών, την ασφάλειά τους και την ταυτοποίηση των συναλλασσομένων, μια διέξοδο αποτελούν οι ηλεκτρονικές υπογραφές. Ο πρωταρχικός σκοπός της ηλεκτρονικής υπογραφής από τη σκοπιά του δικαίου είναι η μη αποκήρυξη μιας συναλλαγής ή μιας δήλωσης βούλησης. Η ανάπτυξη ανοικτών δικτύων και η δυνατότητα εκτέλεσης ανοικτών συναλλαγών διαμόρφωσε την ανάγκη για μεγαλύτερη βεβαιότητα σε σχέση με το ποιος και υπό ποιους όρους υπογράφει μια συναλλαγή, έτσι ώστε να μπορεί να γίνει γνωστή η πραγματική ταυτότητα του αντισυμβαλλομένου σε ένα ανοικτό δίκτυο όπως το Internet[2].

Από το 1996 έχει ξεκινήσει η δημιουργία ενός διεθνούς νομικού πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών και τη διασφάλιση των συναλλαγών. Το 1999 η Οδηγία 1999/93/ΕΚ (εφεξής Οδηγία) "σχετικά με ένα κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές", έθεσε τις βάσεις του ρυθμιστικού πλαισίου των ηλεκτρονικών υπογραφών στην Ευρωπαϊκή Ενωση (εφεξής ΕΕ). Η σχετική προτυποποίηση σε συνέχεια της Οδηγίας έθεσε τις τεχνικές και διαδικαστικές πλευρές και συνέβαλε στην εξειδίκευση του κανονιστικού πλαισίου. Το Προεδρικό Διάταγμα 150/2000 (εφεξής ΠΔ) "Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές" θέτει το κανονιστικό πλαίσιο και εναρμονίζει το ελληνικό με το ευρωπαϊκό δίκαιο στο ζήτημα των ηλεκτρονικών υπογραφών[3].

Στην παρούσα μελέτη παρατίθενται ορισμένα ζητήματα σχετικά με τις ηλεκτρονικές υπογραφές στο ευρωπαϊκό δίκαιο και την ενσωμάτωσή τους στο ελληνικό δίκαιο και αναφέρονται ορισμένες σχετικές τραπεζικές εφαρμογές.

Σημείωση: Το άρθρο εκφράζει προσωπικές απόψεις.

[1] Mitrakas, A., *Open EDI and Law in Europe: A regulatory framework,* Kluwer Law International, 1997, σελ. 21, επ. βλέπε και Γιανόπουλος, Γ., *Ροή πληροφοριών στο διαδίκτυο*, Νομική Βιβλιοθήκη, Αθήνα 2002 και Lodder, A., Kaspersen H.W.M., *eDirectives: Guide to European Union law on E-Commerce,* Kluwer Law International, 2002, σελ. 21, επ.

[2] Mitrakas, 1997. Επίσης, Σύσταση Επιτροπής Ευρωπαϊκών Κοινοτήτων 94/820, σχετικά με τις νομικές πλευρές της ηλεκτρονικής ανταλλαγής δεδομένων (EDI), OJ 1994 L338/98, που περιλαμβάνει την ευρωπαϊκή πρότυπη σύμβαση για το EDI.

[3] ΦΕΚ Α'/125 25.6.2001.

2. Γενικές παρατηρήσεις

Στο περιβάλλον της ιδιόχειρης υπογραφής, κατά το άρθρο 160 παρ. 1 ΑΚ, το έγγραφο ως συστατικό στοιχείο της δικαιοπραξίας πρέπει να φέρει την ιδιόχειρη υπογραφή του εκδότη του. Επίσης σύμφωνα με το άρθρο 443 ΚΠολΔ, η αποδεικτική δύναμη του εγγράφου καθορίζεται από την ιδιόχειρη υπογραφή του εκδότη του. Στηριζόμενος στις τεχνολογικές δυνατότητες της εποχής ο νομοθέτης τόσο του ουσιαστικού όσο και του δικονομικού δικαίου έχει αποκλείσει τη χρήση μηχανικών μέσων ως υποκατάστατων της ιδιόχειρης υπογραφής ώστε να πληρούνται οι προϋποθέσεις του Νόμου. Σε αυτό το διαχωρισμό όμως δεν είχε περιληφθεί η χρήση ηλεκτρονικών εγγράφων και ηλεκτρονικών υπογραφών, μια τεχνολογική εξέλιξη που ο νομοθέτης δεν μπορούσε να προβλέψει. Η απάντηση στο ερώτημα εάν οι ηλεκτρονικές υπογραφές μπορούν να ενταχθούν στο πλαίσιο των άρθρων 160 παρ. 1 ΑΚ και 443 ΚπολΔ, εξαρτάται από το αν με αυτό τον τρόπο εξασφαλίζεται η γνησιότητα του υπογραφόμενου εγγράφου[4]. Καθώς οι ηλεκτρονικές υπογραφές διασφαλίζουν την ταυτοποίηση του χρήστη, την ακεραιότητα του εγγράφου και τη μη αποκήρυξη της συναλλαγής η απάντηση στο παραπάνω ερώτημα είναι καταρχήν καταφατική.

Στηριζόμενο σε ορισμένες γενικές λειτουργίες που τίθενται από την τεχνολογική λύση που επιλέγεται, το δίκαιο θέτει ορισμένους βασικούς κανόνες για τη λειτουργία ενός συστήματος που χρησιμοποιεί ηλεκτρονικές υπογραφές και εξειδικεύει τις γενικές αρχές χρήσης των υπογραφών στις συναλλαγές. Ενας αρχικός συστηματικός διαχωρισμός θα πρέπει να γίνει σχετικά με τους όρους *ηλεκτρονική υπογραφή και ψηφιακή υπογραφή*[5]. Ως κατηγορία των ηλεκτρονικών υπογραφών θεωρούμε τις ψηφιακές υπογραφές, οι οποίες κάνουν χρήση μιας συγκεκριμένης τεχνολογίας, που βασίζεται στη χρήση της ασύμμετρης κρυπτογραφίας ή κρυπτογραφίας δημοσίου κλειδιού[6].

Οι ηλεκτρονικές υπογραφές γενικά χρησιμοποιούν τεχνικές ασύμμετρης κρυπτογραφίας, που στηρίζονται κυρίως στη χρήση ενός ζεύγους κλειδιών. Μια μοναδική μαθηματική σχέση μεταξύ των δύο μερών του ζεύγους κλειδιών καθιστά δυνατή την επαλήθευση της χρήσης του ενός κλειδιού όταν είναι γνωστό το άλλο. Καθώς είναι μαθηματικά αδύνατο να συμπεράνει κάποιος το ένα κλειδί όταν γνωρίζει το άλλο, η επαλήθευση της χρήσης του κλειδιού γίνεται με την αποστολή στον αντισυμβαλλόμενο ή δημοσιοποίηση του άλλου κλειδιού, που ονομάζεται δημόσιο κλειδί και αποτελεί μέρος του ζεύγους κλειδιών της ηλεκτρονικής υπογραφής [7].

Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών πηγάζει από την ανάγκη αναγνώρισης μιας ηλεκτρονικής μεθόδου ως νομικά έγκυρης και ισότιμης με τη χειρόγραφη μέθοδο παραγωγής υπογραφής, ώστε να μπορεί να χρησιμοποιηθεί κατά την απόδειξη. Παρά το γεγονός ότι στις περισσότερες ιδιωτικές συναλλαγές οποιοδήποτε στοιχείο δηλωτικό της βούλησης του υπογράφοντος να δεσμευθεί μπορεί να ερμηνευθεί ως υπογραφή, η εισαγωγή της τεχνολογίας στις συναλλαγές δημιουργεί την ανάγκη ειδικής αναγνώρισης τόσο των ηλεκτρονικών υπογραφών, όσο και των ηλεκτρονικών εγγράφων επί των οποίων χρησιμοποιούνται[8]. Επιπλέον είναι αναγκαίο να αναδειχθεί η δεσμευτική σύνδεση μεταξύ του υπογράφοντος συναλλασσομένου και της σχετικής τεχνολογίας που χρησι-

---

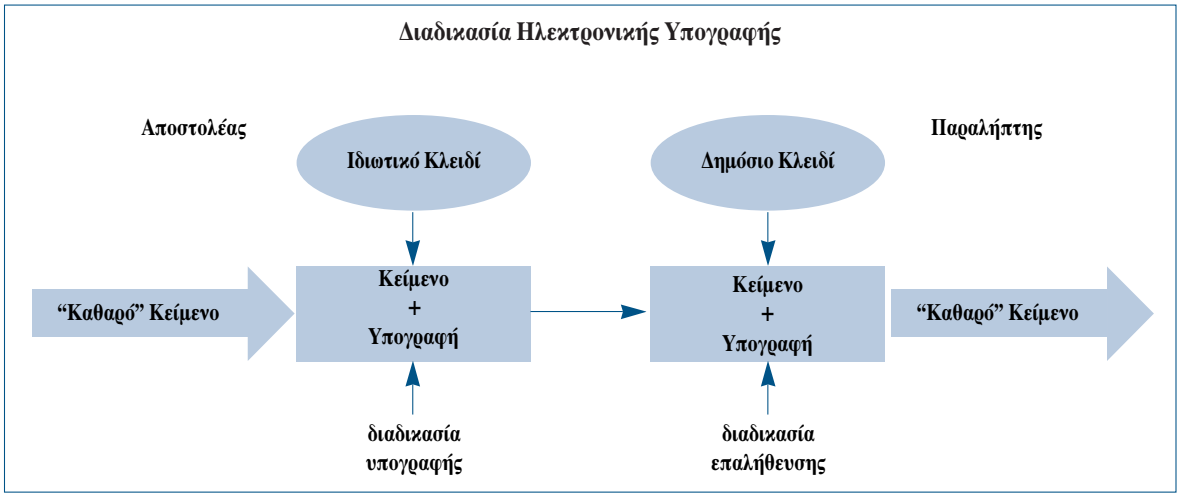
[4] Μανιώτης, Δ., *Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο*, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα, 1998. Βλέπε και Χριστοδούλου, Κ., *Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία μετά τις νέες κοινοτικές ρυθμίσεις,* Αντ. Ν. Σάκκουλας, Αθήνα - Κομοτηνή, 2001.

[5] Illinois Attorney General Jim Ryan's Commission on Electronic Commerce and Crime, Final Report (May, 26, 1998).

[6] Ford, W., Baum, M., *Secure Electronic Commerce,* (2nd edition) Prentice-Hall, Upper River Saddle, 2001. Ψηφιακές υπογραφές που χρησιμοποιούν κρυπτογραφία δημοσίου κλειδιού (Public Key Encryption) στηρίζονται σε μια υποδομή δημοσίου κλειδιού (Public Key Infrastructure – PKI).

[7] Βλέπε επίσης Ford et al. 2001 και Adams, C., Lloyd, S., *Understanding Public Key Infrastructure,* Macmillan Technical Publishing, Indianapolis, 1999, σ. 23.

[8] Νόμος πρότυπο της UNCITRAL για το ηλεκτρονικό εμπόριο (1996).



μοποιεί, προκειμένου να μην είναι δυνατή η εκ των υστέρων αποκήρυξη της συναλλαγής[9].

Σχετικά με το ποια τεχνολογία είναι καταλληλότερη για τη δημιουργία και επαλήθευση ηλεκτρονικών υπογραφών η διεθνής και ευρωπαϊκή νομοθετική θέση στη ρύθμιση των ηλεκτρονικών υπογραφών υιοθετεί γενικά μια τεχνολογικά ουδέτερη στάση στο ερώτημα της καταλληλότητας και της ασφάλειας της τεχνολογίας που χρησιμοποιείται στις ηλεκτρονικές συναλλαγές. Η επιλογή της τεχνολογίας πρέπει να στηρίζεται στην αξιολόγηση του κινδύνου (risk assessment) σε σχέση με την εφαρμογή για την οποία πρόκειται να χρησιμοποιηθεί η ηλεκτρονική υπογραφή[10]. Ο κίνδυνος από τη χρήση ηλεκτρονικών υπογραφών αφορά κυρίως τους τρίτους (relying parties), που βασίζονται στην ηλεκτρονική υπογραφή προκειμένου να αξιολογήσουν τη δεσμευτικότητα της δήλωσης βούλησης του υπογράφοντος που βασίζεται στην επαλήθευση του δημοσίου κλειδιού του. Μια λύση σε αυτά τα προβλήματα δίνουν οι "έμπιστες τρίτες οντότητες" ή "αρχές πιστοποίησης", που πιστοποιούν ότι το δημόσιο κλειδί του υπογράφοντος πράγματι του ανήκει και συνδέεται μονοσήμαντα με το ιδιωτικό του κλειδί που παραμένει μυστικό[11]. Οι έμπιστες τρίτες οντότητες εκδίδουν λοιπόν ηλεκτρονικά πιστοποιητικά, τα οποία είναι ηλεκτρονικά αρχεία που περιλαμβάνουν το δημόσιο κλειδί του υπογράφοντος, το οποίο χρησιμοποιείται για την επαλήθευση της υπογραφής του και στοιχείων που επιβεβαιώνουν την ταυτότητά του. Τα ηλεκτρονικά πιστοποιητικά αποτελούν μονομερείς δηλώσεις βούλησης της εκδίδουσας έμπιστης τρίτης οντότητας, οι οποίες πιστοποιούν στοιχεία απαραίτητα για την ηλεκτρονική υπογραφή και την επαλήθευσή της.

Παραδείγματα εφαρμογών τυπικών συμβάσεων ή δηλώσεων βούλησης που κάνουν χρήση ηλεκτρονικών υπογραφών είτε για μη αποκήρυξη είτε για την πιστοποίηση της ταυτότητας του χρήστη, με βάση το ευρωπαϊκό δίκαιο περιλαμβάνουν ηλεκτρονικά τιμολόγια, ηλεκτρονικές δημόσιες προμήθειες κ.λπ. Στην ηλεκτρονική τραπεζική, ηλεκτρονικές υπογραφές χρησιμοποιούνται τόσο στις συναλλαγές με τους πελάτες, όσο και σε εσωτερικές διαδικασίες, διαδικασίες εκκαθάρισης κ.λπ., ενώ αναμένεται διεύρυνση των σχετικών εφαρμογών με τη χρήση τους και στο εμπόριο μέσω δικτύων κινητής τηλεφωνίας.

---

[9] Βλέπε Reed, C., *Internet Law: Text and Materials*, Butterworths, London 2000, σελ. 154 επ.

[10] Το παρόν άρθρο αναφέρεται κυρίως στις ηλεκτρονικές υπογραφές που δημιουργούνται με τη χρήση κρυπτογραφίας δημοσίου κλειδιού. Βλέπε, Ford et al. 2001, Μαργαρίτης. Χ., Μαρτάκος, Δ., *Κρυπτοτεχνικές σε ανοικτά δίκτυα*, 5ο Banking Forum, ΕΕΔΕ, 1999 και Polemi, N., Rijmen, V., et. al. *Smart Card Based PKI for CoC Services,* IFIP 2003 Proceedings.

[11] Στο άρθρο 2 του ΠΔ 150/2001 χρησιμοποιείται ο όρος "πάροχος υπηρεσιών πιστοποίησης" που ορίζεται ως φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές.

3. Πηγές

Ηδη από τα μέσα της δεκαετίας του 1990 διεθνείς και εθνικές πρωτοβουλίες άρχισαν να εστιάζουν στη ρύθμιση της χρήσης ηλεκτρονικών υπογραφών[12]. Ο πρώτος ολοκληρωμένος Νόμος για τις ηλεκτρονικές υπογραφές ψηφίστηκε στην πολιτεία της Γιούτα των ΗΠΑ και αναφέρεται στο νομικό αποτέλεσμα των ηλεκτρονικών υπογραφών και στη λεπτομερή ρύθμιση και αδειοδότηση της παροχής σχετικών υπηρεσιών ηλεκτρονικής υπογραφής[13]. Σημαντικό εμπόδιο στη νομοθετική ρύθμιση για πολλά χρόνια αποτέλεσε η πολιτική πολλών κυβερνήσεων στον τομέα της κρυπτογραφίας, έναν τομέα που τόσο η αμερικανική όσο και ευρωπαϊκές κυβερνήσεις θεωρούσαν ως αποκλειστικά εθνική τους υπόθεση και συνεπώς αρνούνταν να προχωρήσουν σε συζητήσεις σε διεθνές επίπεδο. Το 1997 μια σύσταση του ΟΟΣΑ δήλωνε ότι η χρήση της κρυπτογραφίας για τη διαπίστωση της ταυτότητας του χρήστη και τη μη αποκήρυξη των συναλλαγών είναι διαφορετική από τη χρήση με σκοπό την εμπιστευτικότητα των δεδομένων και την κρυπτογραφία, οι οποίες παρουσιάζουν διαφορετικά προβλήματα και αποτελούν τελικά ζήτημα εσωτερικής πολιτικής[14]. Αλλες ενέργειες όπως των Ηνωμένων Εθνών, του Διεθνούς Εμπορικού Επιμελητηρίου και του Αμερικανικού Δικηγορικού Συλλόγου εστίασαν στο ζήτημα της ρύθμισης των ηλεκτρονικών υπογραφών ώστε να διασφαλίζεται δια Νόμου ή συμβατικά η δεσμευτικότητά τους στις συναλλαγές[15].

Σύμφωνα με την εισαγωγική παράγραφο 5 της Οδηγίας η διαλειτουργικότητα των διατάξεων ηλεκτρονικών υπογραφών είναι αναγκαία έτσι ώστε διαφορετικά συστήματα να μπορούν να λειτουργήσουν, αναγνωρίζοντας το ένα υπογραφές που δημιουργούνται σε ένα άλλο και να διασφαλίζεται η ελεύθερη κυκλοφορία προϊόντων μέσα στην ΕΕ. Καθώς τα πρότυπα είναι αναγκαία για την εξασφάλιση της διαλειτουργικότητας, η ευρωπαϊκή συνεργασία έχει καταστήσει δυνατό τον καθορισμό τους και στον τομέα των ηλεκτρονικών υπογραφών μέσω των ευρωπαϊκών οργανισμών προτυποποίησης[16].

Σε ευρωπαϊκό επίπεδο η Οδηγία 1999/93/ΕΚ θέτει το γενικό πλαίσιο για τη νομική αναγνώριση των ηλεκτρονικών υπογραφών και τη δημιουργία ενός κοινού ρυθμιστικού πλαισίου στην ΕΕ. Επιπλέον με την Οδηγία διασφαλίζεται η νομική αναγνώριση των ηλεκτρονικών υπογραφών (άρθρο 5.1) ως αντίστοιχων με τις χειρόγραφες, εκεί που ο Νόμος τις απαιτεί. Με το άρθρο 5.1 η Οδηγία θέτει τις προϋποθέσεις εκείνες που είναι απαραίτητες για τη δημιουργία ενός κοινού και ενιαίου επιπέδου ηλεκτρονικών υπογραφών που, υπό προϋποθέσεις, μπορούν να τύχουν αναγνώρισης μεταξύ των κρατών μελών και να χρησιμοποιηθούν κατά την απόδειξη.

Η Απόφαση της 6ης Νοεμβρίου 2000 της Επιτροπής Ηλεκτρονικής Υπογραφής (σύμφωνα με το άρ-

---

[12] Van der Hof, S., Mitrakas, A., *De juridische status van de digitale handetekening,* ITeR Series, No. 7, Samsom Bedrijfsinformatie BV, Alphen aan den Rijn/Diegem, 1997.

[13] Utah Department of Commerce, Utah Digital Signature Law, November 1995 που έχει ενσωματωθεί ως Τίτλος 46, Κεφάλαιο 4 στο Utah Code, Uniform Electronic Transactions Act. Στις ΗΠΑ ισχύει ο Νόμος Electronic Signatures in Global and National Commerce Act που υπογράφηκε από τον πρόεδρο στις 30 Ιουνίου 2000. Richards, J., *The Utah Digital signature Act as "model" legislation: a critical analysis,* The John Marshal Journal of Computer & Information law Vol XVII, Nr. 3, σελ. 873 επ.

[14] ΟΟΣΑ, *Recommendation of the Council concerning guidelines for cryptography policy,* ver. 27 March 1997, Paris 1997 και The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies Initial Elements (1996). Βλέπε και www.wassenaar.org.

[15] Mitrakas, A., Bos, J., *The ICC ETERMS Repository to support Public Key Infrastructure,* Journal of Jurimetrics, Vol. 38, No. 3., 1998. Βλέπε και www.uncitral.org σχετικά με τις εργασίες των Ηνωμένων Εθνών. Σημαντική υπήρξε η συμβολή της επιτροπής Information Security Committee, του Αμερικανικού Δικηγορικού Συλλόγου (American Bar Association – ABA), με το Digital Signature Guidelines (1996).

[16] Δήλωση στην Ευρωπαϊκή Σύνοδο Υπουργών, Βόννη, 6-8 Ιουλίου 1997. Σχετικά με την προτυποποίηση το πλαίσιο θέτει η Οδηγία 83/189/ΕΟΚ για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών, όπως τροποποιήθηκε με τις Οδηγίες 88/182/ΕΟΚ, 94/10/ΕΚ και 98/48/ΕΚ. Βλέπε και Οδηγία 1998/34/ΕΚ σχετικά με την αναγνώριση προτύπων.

θρο 9 της Οδηγίας) για τα ελάχιστα κριτήρια που θα πρέπει να πληρούν οι αρμόδιοι φορείς για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής, αποτελεί μια επιπλέον πηγή[17].

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι επιφορτισμένη με την παρακολούθηση και τη ρύθμιση της αγοράς τηλεπικοινωνιών στην Ελλάδα, μέρος της οποίας αποτελεί η αγορά ηλεκτρονικών υπογραφών[18]. Η ανάπτυξη εφαρμογών ηλεκτρονικών υπογραφών στο δημόσιο τομέα στηρίζεται στις ακόλουθες πηγές:

- Το Προεδρικό Διάταγμα 342/2002 σχετικά με τη διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.
- Το άρθρο 14 του Νόμου 2672/1998 με τίτλο: Διακίνηση εγγράφων με ηλεκτρονικά μέσα.
- Η Εγκύκλιος ΔΙΑΔΠ/Α1/2523 του Υπουργείου Δημόσιας Διοίκησης και Αποκέντρωσης Δ/νση Απλούστευσης Διαδικασιών και Παραγωγικότητας-Διευκρινίσεις στις διατάξεις του άρθρου 14 του Ν. 2672/1998.

4. Ιδίως η "μη αποκήρυξη" της συναλλαγής

Βασικός σκοπός της Οδηγίας είναι η ρύθμιση θεμάτων σχετικών με τη νομική αναγνώριση της χρήσης της ηλεκτρονικής υπογραφής και τους όρους παροχής σχετικών υπηρεσιών. Η Οδηγία κυρίως στοχεύει στη ρύθμιση των ηλεκτρονικών υπογραφών που χρησιμοποιούνται για τη μη αποκήρυξη των συναλλαγών. Ως "μη αποκήρυξη" των συναλλαγών θεωρείται η προστασία εναντίον μιας επιτυχημένης προσβολής σχετικά με την προέλευση, αποστολή, παράδοση ή περιεχόμενο μιας επικοινωνίας[19]. Η μη αποκήρυξη παρέχει υψηλό επίπεδο διαβεβαίωσης ότι μια πληροφορία είναι αυθεντική και δεν μπορεί να γίνει αντικείμενο αποκήρυξης από τον υπογράφοντα[20].

Η δυνατότητα μη αποκήρυξης μπορεί να χρησιμοποιηθεί στην αποδεικτική διαδικασία, στην περίπτωση κατά την οποία τα συμβαλλόμενα μέρη επιχειρήσουν να αποσυνδεθούν από μια συναλλαγή ή από τις συμβατικές ρήτρες που συνδέονται με αυτή τη συναλλαγή. Η Οδηγία δεν διακρίνει κατά της ισχύος οποιασδήποτε κατηγορίας ηλεκτρονικών υπογραφών, συνεπώς οποιοσδήποτε τρόπος ενδεικτικός της πρόθεσης του υπογράφοντος να δεσμευθεί από τη σύμβαση και να έχει χρησιμοποιηθεί θα πρέπει να γίνει δεκτός. Στην ενδεχόμενη διαδικασία επίλυσης διαφορών όμως η Οδηγία αποδίδει τεκμήριο αυξημένης αποδεικτικής αξίας στις αναγνωρισμένες υπογραφές. Στην περίπτωση που έχει χρησιμοποιηθεί κάποιος άλλος τύπος υπογραφών θα πρέπει να εξετασθεί εάν πληρούν τις τεχνικές προϋποθέσεις που τίθενται από τα σχετικά πρότυπα και ότι ο υπογράφων είχε την πρόθεση να δεσμευθεί[21].

Οι ηλεκτρονικές υπογραφές χρησιμοποιούνται με σκοπό τη μη αποκήρυξη, εφόσον είναι λογικά συνδεδεμένες με τα δεδομένα που έχουν υπογραφεί μέσω μιας αναγνωρισμένης τεχνικής μεθόδου που μπορεί να ελεγχθεί. Ετσι, με τις ηλεκτρονικές υπογραφές καθίσταται ένα έγγραφο δεσμευτικό[22].

---

[17] Η Επιτροπή του άρθρου 9 της Οδηγίας, αποτελείται από εκπροσώπους των χωρών μελών.

[18] Η λειτουργία της ΕΕΤΤ διέπεται από το Νόμο 2867/2000, Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις. Το Forum of European Supervisory Authorities for Electronic Signatures (FESA), συντονίζει τις επιβλέπουσες αρχές σε ευρωπαϊκό επίπεδο. Βλέπε, www.fesa.rtr.at/documents.html.

[19] Ford et al. 2001.

[20] Caelli, W., Longley, D., Shain, M., Information Security Handbook, Macmillan. London 1991. Βλέπε και Pfleeger, P., Security in Computing, (2nd edition) Prentice-Hall, Upper River Saddle, 1997.

[21] Βλέπε TS 101 042 Policy requirements for certification authorities issuing public key certificates.

[22] Για την ερμηνευτική ένταξη της ηλεκτρονικής υπογραφής στο πλαίσιο των προϋποθέσεων κύρους των συστατικών εγγράφων μιας δικαιοπραξίας του άρθρου 160 παρ. 1 ΑΚ και της αποδεικτικής τους δύναμης άρθο 443 ΚΠολΔ., βλέπε Μανιώτης, 1998, σελ. 95 επ.

5. Οδηγία 1999/93/ΕΚ

Οι βασικές βλέψεις της Οδηγίας είναι (α) να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική τους αναγνώριση, (β) να θέσει ένα νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για την παροχή υπηρεσιών πιστοποίησης. Η Οδηγία επιδιώκει να συνεισφέρει στην εναρμόνιση της εσωτερικής αγοράς, καθώς ήδη μέχρι το 1999 ορισμένα κράτη μέλη, όπως η Ιταλία και η Γερμανία, είχαν αναλάβει νομοθετικές πρωτοβουλίες με σκοπό τη ρύθμιση της ηλεκτρονικής υπογραφής[23].

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

Στην Ιταλία, από την άλλη πλευρά, αναπτύχθηκε η άποψη ότι, εφόσον οι συμβαλλόμενοι ακολουθούν τους νομοθετημένους κανόνες, οι χρησιμοποιούμενες ηλεκτρονικές υπογραφές μπορούν να θεωρηθούν ως ισότιμες των χειρόγραφων υπογραφών. Παρά την έμφαση του ιταλικού Νόμου σε διαδικασίες αντί της τεχνολογικής ασφάλειας που προϋπέθετε ο αντίστοιχος γερμανικός, η επιλογή των κριτηρίων αξιολόγησης των παροχών στηρίχθηκε αρχικά σε ένα οργανωτικό μοντέλο που δεν ήταν προσαρμοσμένο στις ανάγκες των παρόχων ηλεκτρονικής υπογραφής[24]. Θα πρέπει να γίνεται δεκτό ότι ο επιδιωκόμενος νομικός σκοπός των ηλεκτρονικών υπογραφών είναι η διασφάλιση της νομικής βεβαιότητας της συναλλαγής. Συνεπώς το επίπεδο αξιολόγησης της χρησιμοποιούμενης τεχνολογικής λύσης θα πρέπει να βρίσκεται σε αναλογία με τον ανακύπτοντα κάθε φορά ενδεχόμενο συναλλακτικό κίνδυνο, ο οποίος και θα πρέπει να αξιολογείται σε κάθε περίπτωση συγκεκριμένα. Επιπλέον ένα γενικώς αποδεκτό επίπεδο ασφάλειας μπορεί να ισχύσει δεσμευτικά και έναντι τρίτων, στο βαθμό που η λειτουργία του διασφαλίζεται από το Νόμο και τα γενικώς αναγνωρισμένα πρότυπα.

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

Η Οδηγία στοχεύει επίσης στη ρύθμιση των ηλεκτρονικών υπογραφών που χρησιμοποιούνται σε δημόσια ανοικτά δίκτυα όπως το Internet, ενώ κλειστές ομάδες χρηστών που διαμορφώνουν τις σχέσεις τους στη βάση συμβάσεων μπορούν εξίσου να επωφεληθούν από την Οδηγία, στο βαθμό που το επιθυμούν και εφόσον ακολουθήσουν τις διατάξεις[25]. Η αρχή της ελευθερίας των συμβαλλομένων μερών αναγνωρίζεται στο βαθμό που κλειστές ομάδες χρηστών μπορούν αυτοτελώς να αποφασίζουν ποια κατηγορία ηλεκτρονικών υπογραφών ανταποκρίνεται καλύτερα στις συναλλακτικές ανάγκες τους. Αυτή η διευκρίνιση της εισαγωγικής παραγράφου 16 έχει ιδιαίτερο ενδιαφέρον στις τραπεζικές εφαρμογές, στο βαθμό που μπορεί να θεωρηθεί ότι οι συναλλασσόμενοι πελάτες ή προμηθευτές μιας τράπεζας αποτελούν κλειστή ομάδα χρηστών.

5.1 Τεχνικά πρότυπα και η διαδικασία της "συν-ρύθμισης"

Η Οδηγία ακολουθεί μια τεχνολογικά ουδέτερη στάση, ώστε να επιτρέψει σε νέες τεχνολογίες υπογραφής να αναπτυχθούν, αποφεύγοντας όμως να υποδείξει ένα συγκεκριμένο τύπο υπογραφής, ενώ παράλληλα επιχειρεί να μεγιστοποιήσει τα οφέλη από την εφαρμογή της υπάρχουσας τεχνολογίας. Η

---

[23] Στη Γερμανία ο αρχικός Νόμος 13 Ιουνίου 1997 έχει αντικατασταθεί από το Νόμο της 16 Μαΐου 2001, Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (BGBl Teil I Nr. 22). Επίσης ισχύει και το Διάταγμα της 16 Νοεμβρίου 2001 (BGBl Teil I, Seite 3074). Το ιταλικό Προεδρικό Διάταγμα 10 Νοεμβρίου 1997 (Νόμος Bassanini), αντικαταστάθηκε από το νομοθετικό διάταγμα της 23 Ιανουαρίου 2002, αριθμός 10 (Gazz. Uff. n. 39, 15 Φεβρουαρίου 2002), Recepimento della Direttiva 1999/93/CE sulla firma elettronica.

[24] Το μοντέλο του ιταλικού Νόμου απηχούσε απαιτήσεις συνδεδεμένες με το οργανωτικό πρότυπο αξιολόγησης ISO 9002.

[25] Βλέπε, Οδηγία, εισαγωγική παράγραφο 16.

συνολική διευθέτηση των ζητημάτων τεχνολογίας και διαδικασιών είναι θέμα που αντιμετωπίζεται μέσω της διαδικασίας προτυποποίησης, με σκοπό την εξειδίκευση των απαιτήσεων των παραρτημάτων της Οδηγίας και τη διευκρίνιση άλλων επιμέρους ζητημάτων.

Καθώς τα παραρτήματα απλώς θίγουν ορισμένα από τα ανακύπτοντα ζητήματα, ο καθορισμός των τεχνικών προτύπων εφαρμογής, λειτουργίας και ελέγχου των ηλεκτρονικών υπογραφών αφέθηκε στη διαδικασία προτυποποίησης. Επειδή η Οδηγία αφήνει ανοικτό ένα σημαντικό αριθμό ζητημάτων, η προτυποποίηση θεωρήθηκε από τον ευρωπαϊκό νομοθέτη ότι αποτελεί συνέχεια της νομοθετικής διαδικασίας της Οδηγίας και πρόδρομο άλλων παρόμοιων ενεργειών σε τομείς σχετικούς με τη ρύθμιση της τεχνολογίας στο μέλλον. Η διαδικασία αυτή περιγράφεται με τον όρο "συν-ρύθμιση" (co-regulation)[26].

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

Αναγνωρίζοντας τη δυναμική των τεχνολογικών εξελίξεων, οι σχετικές ρυθμίσεις αφέθηκαν στην πρωτοβουλία που έγινε γνωστή ως European Electronic Signatures Standardisation Initiative (EESSI), που σκοπό έχει τον καθορισμό τεχνικών προτύπων και πολιτικών σχετικών με τις ηλεκτρονικές υπογραφές σε εξειδίκευση της Οδηγίας[27]. Οργανωτικά το EESSI χρησιμοποιεί πόρους και διαδικασίες των ευρωπαϊκών οργανισμών προτυποποίησης CEN/ISSS και ETSI για την εκτέλεση του έργου της προτυποποίησης των ηλεκτρονικών υπογραφών[28].

Η Οδηγία στο άρθρο 3.5 προβλέπει τη δυνατότητα αναγνώρισης προτύπων μέσω της δημοσίευσής τους στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων. Η επιτροπή του άρθρου 9 της Οδηγίας που αποτελείται από εκπροσώπους των κρατών μελών, προαπαιτείται να δώσει θετική γνωμοδότηση σχετικά με τη δημοσίευση τέτοιων προτύπων, πράγμα που το έπραξε την περίοδο 2002-2003 για επιλεγμένα πρότυπα, τα οποία πρόσφατα η Ευρωπαϊκή Επιτροπή δημοσίευσε σε σχετικό κατάλογο[29].

5.2 Το νομικό αποτέλεσμα των ηλεκτρονικών υπογραφών

Η σημαντικότερη συνεισφορά της Οδηγίας συνίσταται στη νομική αναγνώριση των ηλεκτρονικών υπογραφών (άρθρο 5.1) ως αντίστοιχων με τις ιδιόχειρες, εκεί που ο Νόμος τις απαιτεί. Στις τυπικές συναλλαγές η υπογραφή συχνά θεωρείται συστατικό στοιχείο της συναλλαγής. Παράδειγμα αποτελούν οι συμβάσεις που αφορούν ακίνητα, ασφάλειες κ.λπ. Με το άρθρο 5.1 αίρεται η αβεβαιότητα σχετικά με τη χρήση των ηλεκτρονικών υπογραφών στις συναλλαγές, καθώς όπου ο Νόμος το απαιτεί μπορούν πλέον να χρησιμοποιούνται οι αναγνωρισμένες ηλεκτρονικές υπογραφές και να εισάγονται στην αποδεικτική διαδικασία από τους διαδίκους. Ως αναγνωρισμένες ηλεκτρονικές υπογραφές θεωρούνται αυτές που δημιουργούνται εντός μιας ασφαλούς διάταξης υπογραφών και υποστηρίζονται από ένα αναγνωρισμένο πιστοποιητικό, όπως

---

[26] Genghini, R., *Global relevance of the European Electronic Signatures co-regulation process,* Datenschutz und datenschutz, 7 July 2001.

[27] Το EESSI λειτουργεί υπό την αιγίδα του Information and Communications Technologies Standardization Board (ICTSB).

[28] Το EESSI υπό την αιγίδα του ICTSB συντόνισε την εργασία προτυποποίησης που εκτελείται από τους ευρωπαϊκούς οργανισμούς προτυποποίησης CEN/ISSS και ETSI (European Telecommunications Standards Institute). Ο ΕΛΟΤ (Ελληνικός Οργανισμός Τυποποίησης) είναι μέλος του CEN/ISSS. Γενικά για τα πρότυπα του EESSI βλέπε, EESSI, *First Set of Deliverables,* http://www.ict.etsi.fr/eessi/ddd.doc. Βλέπε επίσης και Nilson, H., Van Eecke, P., Medina, M., Pinkas, D., Pope, N., Final Report of the EESSI Expert Team, 1999.

[29] Απόφαση 2003/511/ΕΚ, 14 Ιουλίου 2003, σχετικά με δημοσίευση αριθμών αναφοράς γενικώς αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής σύμφωνα με την Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

αναφέρεται στα Παραρτήματα I-V[30]. Ο όρος αναγνωρισμένες ηλεκτρονικές υπογραφές δεν αναφέρεται ρητά στην Οδηγία, έχει όμως επικρατήσει στην πράξη[31]. Το άρθρο 5.1 δεν δημιουργεί υποχρέωση των κρατών μελών να χρησιμοποιούν τα ίδια ή να ενθαρρύνουν τη χρήση ηλεκτρονικών υπογραφών στις ηλεκτρονικές συναλλαγές, καθώς άλλες Οδηγίες έχουν αναλάβει αυτή την υποχρέωση[32]. Συνεπώς η Οδηγία δεν επηρεάζει την ισχύ κανόνων που ήδη ισχύουν στις συναλλαγές. Τα κράτη μέλη όμως μπορούν να εισάγουν επιπλέον όρους και προϋποθέσεις στις ήδη υπάρχουσες, που αφορούν τις αναγνωρισμένες υπογραφές.

Ο δεύτερος στόχος του άρθρου 5.1 επιτυγχάνεται μόνο ατελώς, καθώς η εισαγωγή των ηλεκτρονικών υπογραφών στην αποδεικτική διαδικασία από τους διαδίκους επιτρέπεται στη βάση της χρήσης οποιουδήποτε μέσου κατά την απόδειξη στα κράτη μέλη. Η διαφοροποίηση εδώ αφορά τη βαρύτητα που το δικαστήριο θα κληθεί να αποδώσει σε κάθε τύπο αποδεικτικού μέσου που χρησιμοποιείται στην αποδεικτική διαδικασία.

Το άρθρο 5.2 αναφέρεται στη μη διάκριση προς τις μη αναγνωρισμένες ηλεκτρονικές υπογραφές σε σχέση με τις αναγνωρισμένες, επειδή μπορεί (α) να βρίσκονται σε ηλεκτρονική μορφή, (β) να μη στηρίζονται σε αναγνωρισμένο πιστοποιητικό, (γ) να μη στηρίζονται σε αναγνωρισμένο πιστοποιητικό που έχει εκδοθεί από διαπιστευμένη αρχή πιστοποίησης, (δ) να μην έχουν δημιουργηθεί εντός μιας ασφαλούς διάταξης.

Η δυσχέρεια εφαρμογής της παραγράφου 5.2 έγκειται στη δυσκολία υιοθέτησης αντικειμενικών κριτηρίων για την απόρριψη μη αναγνωρισμένων ηλεκτρονικών συναλλαγών. Τα κριτήρια αυτά θα πρέπει να στηρίζονται ενδεχομένως στην αναξιοπιστία της χρησιμοποιούμενης τεχνικής μεθόδου. Είναι γενικά παραδεκτό ότι, επειδή ως υπογραφή μπορεί να χρησιμοποιηθεί οποιοδήποτε σημείο που μπορεί να ερμηνευθεί ως δηλωτικό της βούλησης του υπογράφοντος ώστε να δεσμευθεί από τη συναλλαγή, η χρήση οποιασδήποτε τεχνικής μεθόδου για τη σύνταξη της ηλεκτρονικής υπογραφής θα πρέπει να γίνεται γενικά δεκτή. Ο υπογράφων πάντως θα πρέπει να είναι σε θέση να αποδείξει την ακεραιότητα της επιλεγείσας μεθόδου ως κατάλληλης και ασφαλούς για τον επιδιωκόμενο σκοπό[33].

5.3 Ζητήματα ευθύνης

Το άρθρο 6 της Οδηγίας αναφέρεται στα ζητήματα ευθύνης από την παροχή υπηρεσιών αναγνωρισμένων πιστοποιητικών. Στο άρθρο 6 αναφέρονται ζητήματα μόνο σχετικά με υπηρεσίες που αφορούν την έκδοση και διαχείριση αναγνωρισμένων ηλεκτρονικών πιστοποιητικών. Ζητήματα ευθύνης που ενδεχομένως ανακύπτουν από τη χρήση προϊόντων ηλεκτρονικής υπογραφής δεν καλύπτονται από το παρόν άρθρο. Καθώς το άρθρο 6 αποτελεί το ελάχιστο κοινό επίπεδο μεταξύ των κρατών μελών, τα ίδια τα κράτη μέλη μπορούν να εισαγάγουν επιπλέον στοιχεία ευθύνης ή να καλύψουν ζητήματα πέραν των αναγνωρισμένων πιστοποιητικών. Σύμφωνα με τις παραγράφους 6 (1) και (2) η αρχή πιστοποίησης, όταν εκδίδει στο "κοινό", ευθύνεται (α) για το περιεχόμενο των αναγνωρισμένων πιστοποιητικών, (β) την κατοχή του ζεύγους κλειδιών από τον υπογράφοντα τη στιγμή της έκδοσης του αναγνωρισμένου πιστοποιητικού και (γ) τη συμπληρωματική λειτουργία μεταξύ των μερών του ζεύγους ιδιωτικού και δημόσιου κλειδιού. Η έννοια του "κοινού" αφορά την ευθύνη της αρχής πιστοποίησης προς

---

[30] Για τους όρους ασφαλών διατάξεων δημιουργίας υπογραφής, βλέπε Παράρτημα ΙΙΙ της Οδηγίας και του ΠΔ. Για τα αναγνωρισμένα πιστοποιητικά, βλέπε Παράρτημα ΙΙ της Οδηγίας και του ΠΔ. Για τους παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά, βλέπε Παράρτημα Ι της Οδηγίας και του ΠΔ.

[31] Ο ισχύων γερμανικός Νόμος αναφέρεται ρητά στον όρο "αναγνωρισμένες υπογραφές".

[32] Βλέπε για παράδειγμα την Οδηγία 2001/115/ΕΚ σχετικά με τις προϋποθέσεις χρήσης ηλεκτρονικών τιμολογίων.

[33] Βλέπε CWA 14365, *Guide on the use of electronic signatures,* CEN/ISSS N. 14/05/03.

τρίτους ή αποδέκτες των ηλεκτρονικών υπογραφών. Ο αποδέκτης μιας ηλεκτρονικής υπογραφής (relying party) σε ένα ανοικτό περιβάλλον συναλλαγών δεν συνδέεται συμβατικά με την αρχή πιστοποίησης, ενώ αναμένεται να αποδεχθεί την υπογραφή και τους όρους υπό τους οποίους έχει εκδοθεί και χρησιμοποιείται[34]. Οι όροι αυτοί συνήθως περιλαμβάνονται στην πολιτική πιστοποίησης του εκδότη, η οποία είναι υπό προϋποθέσεις δεσμευτική προς τον υπογράφοντα, καθώς συνδέεται άμεσα με υποχρέωση του παρόχου, όπως προκύπτει από τη σχετική νομοθεσία και απαιτήσεις της προτυποποίησης[35]. Περιορισμοί στη δεσμευτικότητα της πολιτικής πιστοποίησης προκύπτουν από την εφαρμογή της νομοθεσίας προστασίας του καταναλωτή[36].

Η ευθύνη της αρχής πιστοποίησης προκύπτει για τα δεδομένα που καταγράφονται στο εκδιδόμενο αναγνωρισμένο πιστοποιητικό καθώς και για τη μη δημοσίευση της ανάκλησης ή λήξης ισχύος του πιστοποιητικού, όταν αυτό απαιτείται. Η αρχή πιστοποίησης που εκδίδει το αναγνωρισμένο πιστοποιητικό είναι ο τελικός αποδέκτης της ευθύνης, ακόμα και αν χρησιμοποιεί βοηθούς εκπλήρωσης ή άλλους τρίτους προκειμένου να εκπληρώσει τα καθήκοντά της (outsourcing)[37].

Από το κείμενο της Οδηγίας προκύπτει ότι η ευθύνη της αρχής πιστοποίησης ανακύπτει από το γεγονός και μόνο ότι εκδίδει το πιστοποιητικό ως "αναγνωρισμένο", χωρίς να σημαίνει ότι αυτό το πιστοποιητικό πρέπει και τεχνικά να λειτουργεί και ως τέτοιο. Η έκδοση του πιστοποιητικού πρέπει να γίνεται προς το "κοινό", το οποίο συνδυαζόμενο με την εισαγωγική παρατήρηση 16 σημαίνει ότι αρχές πιστοποίησης που λειτουργούν εντός κλειστών ομάδων χρηστών, όπως σε μια τράπεζα για παράδειγμα, δεν δεσμεύονται απαραιτήτως από το άρθρο 6. Το άρθρο 6 της Οδηγίας προβλέπει ευθύνη του παρόχου έναντι οποιουδήποτε φορέα ή φυσικού ή νομικού προσώπου για τη ζημία που προκλήθηκε σε βάρος του, επειδή το πρόσωπο αυτό εύλογα βασίστηκε στο πιστοποιητικό που εκδόθηκε. Καθώς το κριτήριο ευθύνης του παρόχου επιδέχεται ανταπόδειξη, είναι ενδιαφέρον να εξετάσει κανείς τη δυνατότητα χρήσης των κριτηρίων που οδηγούν σε περιορισμό της ευθύνης του παρόχου, όπως για παράδειγμα από τη μη επαρκώς εύλογη εφαρμογή διαδικασιών που αναφέρονται στην πολιτική πιστοποίησης του εκδότη, που συνοδεύει κάθε εκδιδόμενο πιστοποιητικό και αποτελεί δεσμευτική μονομερή δήλωση βούλησης[38]. Επιπλέον περιορισμοί είναι δυνατόν να εισαχθούν, όπως χρηματικά όρια συναλλαγής για όλα τα αναγνωρισμένα πιστοποιητικά. Τέτοιοι περιορισμοί μπορούν να ενισχυθούν και από την εισαγωγή ασφαλιστικής κάλυψης του κινδύνου που ενδεχομένως προκύπτει για τον εκδότη[39].

---

[34] Το ETSI TS 101 456, Policy requirements for CAs issuing qualified certificates, απαιτεί τη συμμόρφωση των πολιτικών πιστοποίησης των αρχών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά. Η πολιτική πιστοποίησης είναι μονομερής δήλωση βούλησης του εκδότη πιστοποιητικών σχετικά με το λειτουργικό και οργανωτικό πλαίσιο καθώς και σχετικά με ζητήματα επιμερισμού και περιορισμού της χρήσης και ευθύνης από την έκδοση ηλεκτρονικών πιστοποιητικών. Βλέπε και IETF RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Βλέπε επίσης και το πλαίσιο πολιτικής πιστοποίησης της GlobalSign, και ιδιαίτερα τα GlobalSign Certificate Policy και GlobalSign Certificate Practice Statement στο www.globalsign.net/repository.

[35] Βλέπε ETSI TS 101 456, πρότυπο X.509 και IETF RFC 2527, που καθιστούν υποχρεωτική τη χρήση πολιτικής πιστοποίησης. Βλέπε επίσης απόφαση ΕΕΤΤ 248/71 της 15ης Μαρτίου 2002.

[36] Περιορισμοί στους όρους της πολιτικής πιστοποίησης επιβάλλονται από τη νομοθεσία προστασίας του καταναλωτή. Βλέπε, Οδηγία του Συμβουλίου 93/13/ΕΟΚ της 5 Απριλίου 1993 σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές. (OJ L95 21.04.1993, σελ. 29-34) και Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 20.05.97, Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις (OJ L 144 of 04.06.1997, pp. 19-28). Βλέπε για παράδειγμα πολιτικής προστασίας του καταναλωτή κεφάλαιο 9 στο CPS της GlobalSign, www.globalsign.net/repository.

[37] Το μοντέλο χρήσης τρίτων για την παροχή υπηρεσιών πιστοποίησης είναι ιδιαίτερα διαδεδομένο και στοχεύει στην απόκτηση ικανότητας διάθεσης υπηρεσιών υπό ξεχωριστή επωνυμία. Βλέπε www.globalsign.net για το δίκτυο εμπιστοσύνης της GlobalSign. Περιορισμός της ευθύνης βάσει των άρθρων 330 και 334 ΑΚ.

[38] Για περιορισμό ευθύνης και όρια χρήσης πιστοποιητικών, βλέπε Κεφάλαιο 9 του CPS της GlobalSign, www.globalsign.net/repository.

[39] Για την πολιτική ασφάλισης της GlobalSign, βλέπε κεφάλαιο 10 του CPS, www.globalsign.net/repository.

Η Οδηγία δεν προβλέπει την αντικειμενική ευθύνη του παρόχου από την έκδοση αναγνωρισμένων πιστοποιητικών, όπως ισχύει σε άλλους τομείς, π.χ. στην ευθύνη παραγωγού[40]. Ο εκδότης, σύμφωνα με την Οδηγία, αναμένεται να αποδείξει ότι δεν υπήρξε αμέλεια στην τεχνική και οργανωτική υποδομή έκδοσης των πιστοποιητικών. Κατά συνέπεια προκύπτει ότι ο εκδότης, προκειμένου να ανταποκριθεί σχετικά, πρέπει να είναι προετοιμασμένος και να διαθέτει επαρκώς ελεγμένες πολιτικές και διαδικασίες που να ανταποκρίνονται στις πρακτικές που ακολουθεί. Η διαδικασία αυτή, που στην Οδηγία αναφέρεται ως εθελοντική διαπίστευση, βασίζεται στην εισαγωγή αντικειμενικών κριτηρίων για την αξιολόγηση αυτών των πρακτικών και πολιτικών που εφαρμόζονται στις εσωτερικές διαδικασίες του παρόχου για την ασφαλή έκδοση του πιστοποιητικού[41].

Σχετικά με τον περιορισμό της ευθύνης ανακύπτουν δύο ανοικτά ακόμα ζητήματα και συγκεκριμένα πώς πληροφορείται και δεσμεύεται ο τρίτος αναφορικά με τους όρους και τις διαδικασίες που ισχύουν και πώς η αρχή πιστοποίησης επικοινωνεί την πολιτική πιστοποίησής της και την καθιστά δεσμευτική σε ένα ηλεκτρονικό περιβάλλον. Η σύνδεση της υποχρεωτικής μονομερούς δηλώσεως που είναι η πολιτική πιστοποίησης με μια σύμβαση συνδρομητή είναι αναγκαία προκειμένου να ενισχυθεί η δεσμευτικότητα ιδιαίτερα σε συμβάσεις καταναλωτών. Καθώς ο τρίτος αποδέκτης του πιστοποιητικού έχει την υποχρέωση να εξετάσει την ισχύ του πιστοποιητικού, πρέπει να γίνει δεκτό ότι κανένας περιορισμός δεν μπορεί να επιβληθεί στην πρόσβαση που του παρέχεται στους πόρους δημοσίευσης πιστοποιητικών που έχουν εκδοθεί, ανακληθεί ή εκπνεύσει (certificate revocation list)[42]. Η πολιτική πιστοποίησης μπορεί συνεπώς να χρησιμοποιηθεί προκειμένου τρίτοι να λάβουν γνώση και να συμμορφωθούν προς τους συνιστώμενους κανόνες πρόσβασης σε τέτοιους κρίσιμους πόρους.

Ενα άλλο ζήτημα που ανακύπτει σχετικά με τον τρόπο επικοινωνίας της πολιτικής πιστοποίησης προς τρίτους συνδυάζεται με την αδυναμία ενσωμάτωσης των ίδιων των νομικών όρων, όπως της πολιτικής πιστοποίησης στο ίδιο το αναγνωρισμένο πιστοποιητικό που έχει εκδοθεί[43]. Γίνεται γενικά δεκτό και χρησιμοποιείται στην πράξη ότι η αρχή πιστοποίησης μπορεί να δημοσιεύσει την πολιτική πιστοποίησης στο δικτυακό της χώρο, ενώ οι τρίτοι μπορούν να την ανασύρουν από εκεί. Σε αυτή την περίπτωση θα πρέπει να διασφαλίζεται η έκδοση και γνησιότητα της πολιτικής πιστοποίησης που μπορεί να διασφαλισθεί για παράδειγμα με τη διαπίστευση του παρόχου. Αλλος τρόπος διασφάλισης αφορά τη δημιουργία ενός φορέα δημοσίευσης τέτοιων πολιτικών και νομικών όρων που χρησιμοποιούνται στις συναλλαγές στο διαδίκτυο κατά το μοντέλο του ICC ETERMS[44].

6. Το ΠΔ 150/2000 και το ελληνικό ρυθμιστικό πλαίσιο

Στον απόηχο της Οδηγίας, το σχέδιο Προεδρικού Διατάγματος του 1999, με σκοπό τη ρύθμιση της ηλεκτρονικής υπογραφής και τη χρήση της καταρχήν στο δημόσιο τομέα, δημιούργησε την εντύπωση απόκλισης του ελληνικού από το κοινοτικό δίκαιο. Η προσέγγιση αυτή άφηνε ανοικτό το ενδεχόμενο οι ηλεκτρονικές υπογραφές να μην αναγνωρίζονταν με τον ίδιο τρόπο στις συναλλαγές μεταξύ ιδιωτών, όπως θα αναγνωρίζονταν στις συναλλα-

---

[40] Οδηγία 85/374/ΕΟΚ.

[41] Βλέπε για παράδειγμα το πρότυπο διαπίστευσης WebTrust for CAs όπως και εθνικά πρότυπα π.χ. BE.SIGN στο Βέλγιο, RegTP στη Γερμανία, TTP.NL στην Ολλανδία και tScheme στη Βρετανία.

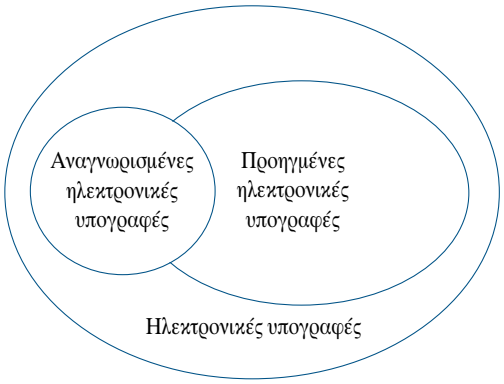
[42] Αλλα πρότυπα που χρησιμοποιούνται για τη δημοσίευση ανακληθέντων ή ανενεργών πιστοποιητικών περιλαμβάνουν τα Online Certificate Status Protocol (RFC 2560) και Single Certificate Validation Protocol. Βλέπε ETSI TS 101456 και Relying Party Obligations, Κεφάλαιο 7 του CPS της GlobalSign, www.globalsign.net/repository.

[43] Wu S., *Incorporation by reference and Public Key Infrastructure: Moving the Law beyond the paper-based world,* Jurimetrics, Vol. 38, Nr. 3, 1998.

[44] Mitrakas, 1997, σελ. 249-264 και Mitrakas et al. 1998.

γές με το δημόσιο τομέα με ενδεχόμενες ερμηνευτικές συνέπειες σχετικά με το άρθρο 444 παρ. 3 του ΚΠολΔ[45]. Καθώς τα ηλεκτρονικά έγγραφα δεν αναφέρονται στο σχετικό άρθρο του ΚΠολΔ, άλλα αποδεικτικά μέσα μπορεί να αντιμετώπιζαν περιορισμούς χρησιμοποίησής τους στην αποδεικτική διαδικασία που θα περιόριζε το ενδιαφέρον χρήσης των ηλεκτρονικών υπογραφών.

Τρεις κατηγορίες ηλεκτρονικών υπογραφών σύμφωνα με την Οδηγία 1999/93/ΕΚ



Σε συμμόρφωση με την Οδηγία, το ΠΔ 150/2000 προσαρμόζει την ελληνική νομοθεσία προς τις διατάξεις της, ενώ αποτελεί πιστή μεταφορά του κειμένου της Οδηγίας στο ελληνικό δίκαιο, μια πρακτική που όμως ακολούθησαν και άλλες χώρες στην ΕΕ. Με το άρθρο 3.2 το ΠΔ αναγνωρίζει χωρίς περιορισμούς την ηλεκτρονική υπογραφή και αναφέρεται στις κατηγορίες ηλεκτρονικών υπογραφών που θέτει η Οδηγία, οι οποίες περιλαμβάνουν τους παρακάτω τύπους:

1. Τις απλές ηλεκτρονικές υπογραφές που μπορεί να περιλάβουν κάθε τύπο ηλεκτρονικής υπογραφής, όπως για παράδειγμα ένα ψηφιακό αποτύπωμα μιας χειρόγραφης υπογραφής, ένα διακριτικό σημάδι κ.λπ.

2. Τις προηγμένες ηλεκτρονικές υπογραφές που πρέπει να πληρούν τις παρακάτω προϋποθέσεις: (α) να συνδέονται μονοσήμαντα με τον υπογράφοντα ώστε να μην υπάρχει σύγχυση σχετικά με το δικαιούχο της ηλεκτρονικής υπογραφής, (β) να είναι ικανές να καθορίσουν ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος, κατά τρόπο ώστε τα στοιχεία που είναι εγγεγραμμένα στο ηλεκτρονικό πιστοποιητικό να είναι ακριβή και το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό να ανταποκρίνεται στο ιδιωτικό κλειδί που κατέχει ο δικαιούχος, (γ) να δημιουργούνται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, κατά τρόπο ώστε να χρησιμοποιούνται οι ασφαλείς διατάξεις του Παραρτήματος ΙΙΙ του ΠΔ για τη δημιουργία του ζεύγους κλειδιών και την ασφαλή φύλαξη του ιδιωτικού κλειδιού και (δ) να συνδέονται με τα δεδομένα στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων, πράγμα το οποίο επιτυγχάνεται μέσω της χρήσης αλγορίθμων κατατεμαχισμού κατά τη διαδικασία δημιουργίας και επαλήθευσης της ηλεκτρονικής υπογραφής[46].

3. Τις προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής. Το άρθρο 3.1 αναφέρει ότι αυτή η υπογραφή επέχει θέση ιδιόχειρης υπογραφής, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο. Αυτές οι υπογραφές συνήθως ονομάζονται αναγνωρισμένες υπογραφές[47].

Ενα επιπλέον ζήτημα που τίθεται με την Οδηγία και αντανακλά το ΠΔ, αφορά τον ορισμό του υπογράφοντος του άρθρου 2 της Οδηγίας[48]. Η ευρεία διατύπωση πάντως αυτού του άρθρου δεν διακρίνει

[45] Κουσούλης. Σ., *Σύγχρονες μορφές έγγραφης συναλλαγής,* Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα, 1992.

[46] Για την ηλεκτρονική υπογραφή δεδομένων στην κρυπτογραφία δημοσίου κλειδιού χρησιμοποιούνται συναρτήσεις κατατεμαχισμού (hash functions) Βλέπε και Μαργαρίτης κ.ά. 1999.

[47] Ο όρος αναγνωρισμένες υπογραφές δεν απαντάται στην Οδηγία. Εχει καθιερωθεί όμως από το EESSI και χρησιμοποιείται και από το νέο γερμανικό Νόμο.

[48] Antoine, M., Gobert, D., *La Directive Européenne sur la signature electronique vers la securisation des transactions sur l'Internet?,* JTDE, Απρίλιος 2000, N° 68, Σελ. 73-78.

μεταξύ φυσικών και νομικών προσώπων και αφήνει ανοικτό το ενδεχόμενο της νομικής αναγνώρισης υπογραφών νομικών προσώπων, όπως συμβαίνει υπό προϋποθέσεις στο κοινό δίκαιο στη Βρετανία και αφορά ειδικά αυτοματοποιημένες εφαρμογές[49].

6.1 Απόφαση 248/71 της 15ης Μαρτίου 2002

Η Απόφαση 248/71 της 15ης Μαρτίου 2002 με τίτλο "Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής" διέπει τη λειτουργία των παρόχων ηλεκτρονικής υπογραφής που είναι εγκατεστημένοι στην Ελλάδα. Ο σκοπός της Απόφασης είναι η ρύθμιση θεμάτων σχετικών με (α) την παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, (β) ζητήματα Αναγνωρισμένων Πιστοποιητικών και (γ) την εποπτεία και έλεγχο παρόχων υπηρεσιών πιστοποίησης με εγκατάσταση στην Ελλάδα που εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά ή παρέχουν άλλες υπηρεσίες πιστοποίησης σχετικές με την ηλεκτρονική υπογραφή.

Η Απόφαση αναγνωρίζει ότι η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών ή άλλων συναφών δεν υπόκειται σε αδειοδότηση, η έκδοση αναγνωρισμένων πιστοποιητικών όμως απαιτεί την εφαρμογή των Παραρτημάτων Ι και ΙΙ του ΠΔ σχετικά με τους όρους που ισχύουν για αναγνωρισμένα πιστοποιητικά και για τους όρους που ισχύουν για παρόχους υπηρεσιών πιστοποίησης, που εκδίδουν αναγνωρισμένα πιστοποιητικά, διασφαλίζοντας την εσωτερική αγορά. Ο πάροχος πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τους σχετικούς κανόνες και αναγνωρισμένα πρότυπα που ισχύουν στην ΕΕ.

Σύμφωνα με το άρθρο 4, οι δικαιούχοι αναγνωρισμένων πιστοποιητικών (τελικοί χρήστες) (α) πρέπει να είναι μόνο φυσικά πρόσωπα, τα οποία έχουν δικαιοπρακτική ικανότητα, (β) πρέπει να κατέχουν τα δεδομένα δημιουργίας της ηλεκτρονικής υπογραφής (ιδιωτικό κλειδί) που συνδέεται με το πιστοποιητικό, (γ) έχουν καθήκον επιμέλειας για την τήρηση των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής και του πιστοποιητικού (ώστε το ιδιωτικό κλειδί να παραμένει εντός της ασφαλούς διάταξης δημιουργίας της ηλεκτρονικής υπογραφής), (δ) έχουν υποχρέωση ενημέρωσης του παρόχου σε περίπτωση απώλειας των δεδομένων δημιουργίας της ηλεκτρονικής υπογραφής ή στην περίπτωση που αυτά περιέλθουν στην κατοχή ή γνώση τρίτου.

Από τη διατύπωση του άρθρου αυτού είναι δύσκολο να κατανοήσει κανείς το ζήτημα της επιμέλειας τήρησης του πιστοποιητικού, καθώς το περιεχόμενο του πιστοποιητικού συνήθως δεν είναι εμπιστευτικό και η χρήση του εξαρτάται επίσης από τις εφαρμογές στις οποίες χρησιμοποιείται. Οι πάροχοι εφαρμογών ηλεκτρονικής υπογραφής όμως δεν υπόκεινται σε έλεγχο σχετικά με την επεξεργασία που τυχόν υφίστανται τα πιστοποιητικά των τελικών χρηστών εντός των εφαρμογών που διαθέτουν στον τελικό χρήστη, ζήτημα το οποίο εμπίπτει στον τομέα ευθύνης του παρόχου υπηρεσιών εφαρμογής (application service provider). Επιπλέον αυτή η ρύθμιση ενδέχεται να δυσχεράνει τη χρήση ηλεκτρονικών υπογραφών σε αυτοματοποιημένες συναλλαγές, καθώς ενδέχεται να απαιτηθεί αυξημένη συμβατική αντιμετώπιση του ζητήματος μεταξύ του οργανισμού που χρησιμοποιεί αυτοματοποιημένες συναλλαγές (π.χ. τραπεζικές συναλλαγές, έκδοση ηλεκτρονικών τιμολογίων κ.λπ.) και του υπογράφοντος εκπροσώπου του οργανισμού[50]. Το άρθρο αυτό θα μπορούσε να βελτιωθεί με τη διευκρίνιση

---

[49] Βλέπε και Επικοινωνία της Ευρωπαϊκής Επιτροπής 8 Οκτωβρίου 1997, σημείο 2.3.

[50] Καθώς ο εκπρόσωπος του οργανισμού θα πρέπει να υπογράφει εξερχόμενα έγγραφα, η επεξεργασία των εγγράφων αυτών θα πρέπει να τίθεται σε ένα προς ένα τα έγγραφα αυτά ξεχωριστά, δυσχεραίνοντας όμως την αυτοματοποιημένη επεξεργασία, καθώς το ιδιωτικό κλειδί μιας αναγνωρισμένης υπογραφής δεν μπορεί να χρησιμοποιηθεί παρά μόνο μέσω της ασφαλούς διάταξης. Βλέπε Mitrakas, A., *Policy constraints and role attributes in electronic invoices,* Information Security Bulletin, Vol. 8, Nr. 5, June 2003, και Mitrakas, A., Policy-driven signing frameworks in open electronic transactions, in G.Doukidis, N. Mylonopoulos, N. Pouloudi *Information Society or Information Economy? A combined perspective on the digital era,* Idea Group Publishing, Hershey, 2004.

ότι πρέπει να γίνεται διάκριση μεταξύ του τελικού δικαιούχου και συνδρομητή της υπηρεσίας[51].

Η παράγραφος 9 του άρθρου 5 δημιουργεί επιπλέον ερωτηματικά, καθώς σε συμμόρφωση με το πρότυπο ETSI TS 101 456, προβλέπει ότι η ενημέρωση του καταλόγου ανακληθέντων πιστοποιητικών μπορεί να γίνεται μια φορά ανά 24 ώρες τουλάχιστον, το οποίο αποτελεί χρονικό διάστημα που δεν διευκολύνει επαρκώς τη χρήση πιστοποιητικών σε μεγάλη κλίμακα ή σε συναλλαγές με έντονο χρονικό ενδιαφέρον, όπως στην κατάθεση χρηματιστηριακών εντολών και πράξεων, για παράδειγμα. Σχετικά με την παύση Εργασιών Παρόχων Υπηρεσιών Πιστοποίησης του άρθρου 6, η εφαρμογή του εδαφίου (στ) εναπόκειται στη δημιουργία αντίστοιχης υποδομής της ΕΕΤΤ ως επιβλέπουσας αρχής, καθώς είναι δυνατό στην πράξη η παύση εργασιών του εκδότη αναγνωρισμένων πιστοποιητικών να μη συνοδεύεται από επιτυχή μεταβίβαση του αρχείου του σε άλλον αντίστοιχο και παρά την απειλή επιβολής κυρώσεων που προβλέπει η Απόφαση. Ελέγχεται βεβαίως το κατά πόσον είναι εφικτή ή σκόπιμη η ανάπτυξη υποδομής δημοσίου κλειδιού από την ίδια την ΕΕΤΤ, δεδομένου και του περιορισμένου βαθμού ανταπόδοσης που ενδεχομένως να προκύψει στην ελληνική αγορά.

Καθώς οι τεχνικές προδιαγραφές για την τήρηση ηλεκτρονικών αρχείων σε βάθος χρόνου δεν έχουν ακόμα προσδιοριστεί με σαφήνεια, είναι δύσκολο να διαπιστώσει κανείς πώς μπορεί να εφαρμοστεί στην πράξη η υποχρέωση τήρησης αρχείου Αναγνωρισμένων Πιστοποιητικών για χρονικό διάστημα τριάντα ετών. Η απαίτηση αυτή θα πρέπει ενδεχομένως να συνοδευτεί και από μέτρα προτυποποίησης προκειμένου να διασφαλιστεί η αξιοπιστία και εμπιστοσύνη στα στοιχεία του αρχείου του άρθρου 7, εδάφιο (2).

Το άρθρο 8, εδάφιο (δ) προβλέπει την υποχρέωση του παρόχου να ενημερώνει το δικαιούχο σχετικά με την πολιτική πιστοποίησης και τη δήλωση Πρακτικής Πιστοποίησής του και οποιαδήποτε τυχόν τροποποίηση αυτών. Με σκοπό η ενημέρωση του δικαιούχου από τον πάροχο ενδεχομένως να μην κριθεί ανεπαρκής στην πράξη και άρα να μπορεί να προσβληθεί για ακυρότητα πρέπει (α) να συνοδεύεται από την αναμφισβήτητη έκδοση της πολιτικής που εφαρμόζεται στο συγκεκριμένο πιστοποιητικό, (β) στο ίδιο το πιστοποιητικό να αναφέρεται ο δικτυακός τόπος, από τον οποίο η πολιτική αυτή μπορεί να ανασυρθεί, (γ) ο δικαιούχος μπορεί να λάβει γνώση αυτής[52].

Το άρθρο 10 της Απόφασης αναφέρεται στην τήρηση Μητρώου από την ΕΕΤΤ των παρόχων που είναι εγκατεστημένοι στην Ελλάδα. Καθώς όμως η ΕΕΤΤ προς στιγμήν δεν διαθέτει τη δυνατότητα ελέγχου των παρόχων και δεν διαχειρίζεται τη δική της ιεραρχία δημοσίου κλειδιού, το μητρώο αυτό δεν μπορεί να χρησιμοποιηθεί σε αυτοματοποιημένες διαδικασίες. Επίσης η παρούσα μέθοδος δημοσίευσης του σχετικού μητρώου από την ΕΕΤΤ ενέχει στοιχειώδεις κινδύνους ασφαλείας για τους χρήστες του, καθώς είναι αδύνατη η χρήση ασφαλούς πρωτοκόλλου επικοινωνίας. Η παρούσα μέθοδος δημοσίευσης από την ΕΕΤΤ πάντως, είτε πρέπει να θεωρηθεί ότι έχει πληροφοριακό και άρα μη δεσμευτικό χαρακτήρα, είτε σε αντίθετη περίπτωση τυχόν ζημία του συμβουλευόμενου τρίτου ενδέχεται να δημιουργήσει ευθύνη της ΕΕΤΤ.

Η ΕΕΤΤ πάντως βρίσκεται σε διαδικασία κατάρτισης σχεδίου ελέγχου και διαπίστευσης που αφορά τους παρόχους που βρίσκονται εγκατεστημένοι στην Ελλάδα και εξετάζει τη δυνατότητα ανάπτυξης της δικής της υποδομής δημοσίου κλειδιού και ιεραρχίας. Η εθελοντική διαπίστευση των παρόχων προβλέπεται στο άρθρο 4 εδάφιο 5 του ΠΔ. Βεβαίως η απαιτητική διαδικασία πιστοποίησης των ασφαλών διατάξεων ηλεκτρονικών υπογραφών που δεν εξαρτάται μόνο από την ΕΕΤΤ είναι πιθανό να

[51] ETSI TS 101 456, για τη διάκριση μεταξύ δικαιούχου (subject) και συνδρομητή (subscriber).

[52] Ενώ η συγκεκριμένη έκδοση ενός πιστοποιητικού μπορεί να προσδιορισθεί με τη χρήση ενός Object Identifier (OID), η κάθε έκδοση μιας πολιτικής δεν είναι απαραίτητο να συνοδεύεται από αλλαγή του OID, που αφήνει περιθώριο κατάχρησης από έναν κακόπιστο πάροχο.

ανατεθεί στην αρμοδιότητα αναγνωρισμένων εργαστηρίων εγκατεστημένων σε άλλα κράτη μέλη[53].

Σχετικά με την ανάπτυξη προτύπων πάντως η ελληνική εμπειρία έχει ακόμα λίγα να συνεισφέρει σε ευρωπαϊκό επίπεδο, εκτός από την αυτούσια χρήση των ευρωπαϊκών προτύπων. Η απόφαση της ΕΕΤΤ αναφέρεται ρητά στα πρότυπα των ευρωπαϊκών οργανισμών CEN/ISSS και ETSI. Η κριτική ενσωμάτωση αυτών των προτύπων στην ελληνική πραγματικότητα ενδεχομένως να πραγματοποιηθεί με τη θέση σε ισχύ ενός συστήματος διαπίστευσης των παρόχων[54].

7. Εφαρμογές στον τραπεζικό τομέα

Στον τραπεζικό τομέα συγκεκριμένα δεν παρατηρείται έλλειψη εφαρμογών ηλεκτρονικών υπογραφών, καθώς τόσο το τραπεζικό δίκτυο SWIFT, όσο και το Identrus αποτελούν σημαντικά παραδείγματα στο χώρο και της παροχής υπηρεσιών πιστοποίησης και της διαπίστευσης και της θέσπισης κανόνων διαλειτουργικότητας των παρόχων. Πρέπει να παρατηρηθεί ότι τόσο το SWIFT, όσο και το Identrus προσφέρουν υπηρεσίες που χρησιμοποιούνται αποκλειστικά εντός του τραπεζικού χώρου, χωρίς απαραίτητα να τυγχάνουν αναγνώρισης σε άλλους χώρους εφαρμογής, καθώς και ότι βασίζονται σε συμβατικά πλαίσια και όχι σε κάποιους γενικούς κανόνες (Code of Practice) ή στο νομοθετικό πλαίσιο για τις ηλεκτρονικές υπογραφές.

Το δίκτυο SWIFT διαθέτει ένα περιβάλλον που χρησιμοποιείται από κοινού από τα μέλη του και διαθέτει υποδομή για την παροχή έμπιστων υπηρεσιών σε εταιρικούς πελάτες. Αυτή η υποδομή εμπιστοσύνης στοχεύει στο επίπεδο της εφαρμογής που οι τραπεζικοί οργανισμοί χρησιμοποιούν. Η υπηρεσία αυτή υποστηρίζει τόσο την ηλεκτρονική υπογραφή όσο και υπηρεσίες διαπίστωσης της αυθεντικότητας της ταυτότητας. Οι τραπεζικοί οργανισμοί χρησιμοποιούν αυτά τα δεδομένα σε περίπτωση ελέγχου και επίλυσης διαφορών.

Το Identrus έχει θέσει σε εφαρμογή ένα ρυθμιστικό πλαίσιο πολιτικών, το οποίο αποτελεί ένα παγκόσμιο de facto πρότυπο για την παροχή υπηρεσιών ψηφιακής υπογραφής και διαπίστωσης ταυτότητας στον τραπεζικό χώρο[55]. Το Identrus προσφέρει τη νομική και τεχνική υποδομή σε τραπεζικούς οργανισμούς, ώστε να διαχειριστούν αποτελεσματικά κινδύνους που συνδέονται με την ηλεκτρονική υπογραφή και τις ηλεκτρονικές συναλλαγές.

Υπηρεσίες ηλεκτρονικής υπογραφής σε τραπεζικούς οργανισμούς προσφέρει ένας μεγάλος αριθμός παρόχων υπηρεσιών ηλεκτρονικής υπογραφής[56]. Αντίστοιχα ένας μεγάλος αριθμός παρόχων τραπεζικών υπηρεσιών διαθέτει τη δυνατότητα να χρησιμοποιεί και να διαχειρίζεται ηλεκτρονικά πιστοποιητικά για ηλεκτρονική υπογραφή, διασφάλιση της ταυτότητας του χρήστη ή κρυπτογραφία, όπως για παράδειγμα με το πρότυπο EMV[57].

Εστιάζοντας στο κρίσιμο ζήτημα της διασύνδεσης και διαλειτουργικότητας των υποδομών των παρόχων, εκτός από τις εξελίξεις στον τραπεζικό χώρο πρέπει να αναφερθεί και η πρωτοβουλία του Bridge CA στη Γερμανία. Στόχος του Bridge CA είναι να διασυνδέσει τις υποδομές εμπιστοσύνης μεταξύ των διάφορων υποδομών δημοσίου κλειδιού, αρχίζοντας από τη Γερμανία, ώστε να διευκολυνθούν οι ασφαλείς επικοινωνίες και να δημιουργη-

---

[53] Βλέπε για παράδειγμα το Αυστριακό A-SIT στο www.a-sit.at

[54] Σχετικά μπορεί να αναφερθεί η δραστηριότητα της Ομάδας Εργασίας 2 (2003) στις ηλεκτρονικές υπογραφές του eBusiness Forum www.ebusinessforum.gr

[55] Βλέπε και Απόφαση της Ευρωπαϊκής Επιτροπής για έγκριση ενός παγκόσμιου δικτύου (Identrus) για την πιστοποίηση των ηλεκτρονικών υπογραφών και άλλων συναλλαγών ηλεκτρονικού εμπορίου, 2001.

[56] Οργανισμοί παροχής τραπεζικών υπηρεσιών, όπως η Audkenni (www.audkenni.is), Erste Bank (www.erstebank.at), Telbank (www.telbank.pl), και κυβερνήσεις, όπως του Βελγίου (www.fedict.be), Βουλγαρίας (http://web.stampit.org/docs.asp), Ολλανδίας (www.pkioverheid.nl) κ.ά., χρησιμοποιούν τις υπηρεσίες και υποδομή ενός τρίτου παρόχου (GlobalSign και Ubizen κ.λπ.) για την παροχή υπηρεσιών ηλεκτρονικής υπογραφής.

[57] Βλέπε για παράδειγμα τις προδιαγραφές EMV στο http://www.emvco.com

θεί μια κοινή βάση για ηλεκτρονικές υπογραφές και σχετικές εφαρμογές. Το μοντέλο εφαρμογής του Bridge CA στηρίζεται στην ανάπτυξη υποδομών επαλήθευσης της ισχύος ενός πιστοποιητικού, στις οποίες να έχουν πρόσβαση όλοι οι συμμέτοχοι. Η προσέγγιση αυτή θεωρείται εναλλακτική λύση προς την αμοιβαία πιστοποίηση (cross-certification) ή στην ιεραρχική δομή (hierarchical subordination) των διάφορων υποδομών.

9. Συμπεράσματα

Το ελληνικό δίκαιο εναρμονίζεται με το ευρωπαϊκό σχετικά με την ισχύ και χρήση ηλεκτρονικών υπογραφών, καθώς και την παροχή υπηρεσιών πιστοποίησης. Μικρές διαφοροποιήσεις που παρουσιάζονται δεν αφορούν τον πυρήνα των διατάξεων που έχουν επιτυχώς μεταφερθεί στο ελληνικό δίκαιο όσο ορισμένες οργανωτικές και λειτουργικές πλευρές του περιβλήματος της κανονιστικής λειτουργίας της ΕΕΤΤ.

Το ΠΔ 150/2000 αναμφίβολα επιτυγχάνει το στόχο της εναρμόνισης του ελληνικού δικαίου με το κοινοτικό στον τομέα των ηλεκτρονικών υπογραφών, αφήνει όμως ένα σημαντικό βαθμό επιπλέον εξειδίκευσης του πλαισίου στην ΕΕΤΤ. Με την Απόφαση 248/71 της 15ης Μαρτίου 2002, η ΕΕΤΤ καλύπτει ορισμένες πτυχές της χρήσης και λειτουργίας ηλεκτρονικών υπογραφών και αφήνει άλλες, όπως για παράδειγμα την εφαρμογή των κανόνων διαπίστευσης παρόχων ηλεκτρονικής υπογραφής, λειτουργίας μιας εθνικής ιεραρχίας δημοσίου κλειδιού και κανόνες για τη διαλειτουργικότητα και χρήση διαφορετικών τύπων πιστοποιητικών στις εφαρμογές. Επίσης πρόκληση αποτελεί η προσαρμογή του ελληνικού δικαίου σε διαδικασίες που επιτρέπουν τη χρήση των ηλεκτρονικών υπογραφών και διαδικασιών.

Παρά τα απτά σημεία προσέγγισης, το ελληνικό νομικό και λειτουργικό πλαίσιο των ηλεκτρονικών υπογραφών υπολείπεται εκείνου χωρών που έχουν από χρόνια ένα σαφές πλαίσιο λειτουργίας και μια εφαρμοσμένη δημόσια πολιτική στο ζήτημα των ηλεκτρονικών υπογραφών και των προϊόντων και υπηρεσιών σχετικά με αυτές. Η διαδικασία αξιολόγησης που έχει ήδη τεθεί σε εφαρμογή του άρθρου 12 της Οδηγίας είναι πολύ πιθανό να σηματοδοτήσει διαφοροποιήσεις και στο ελληνικό κανονιστικό πλαίσιο.

Η διάδοση της χρήσης ηλεκτρονικών υπογραφών στο δημόσιο τομέα και σε τραπεζικές εφαρμογές, όπως για παράδειγμα μέσω των δημοσίων προγραμμάτων και τη μετάβαση των τραπεζικών προτύπων στο EMV, αναμένεται να ενισχύσει τις πιέσεις που ασκούνται για την περαιτέρω εξειδίκευση του κανονιστικού πλαισίου στη χώρα μας και να οδηγήσει σε ενέργειες που να ενισχύουν τη διαλειτουργικότητα, τα πρότυπα και την προσαρμογή τους στις ανάγκες των ελληνικών φορέων, οργανισμών και επιχειρήσεων. Είναι αναγκαίο όμως πέραν της δεδομένης ανάπτυξης εγχώριων κανόνων δικαίου να αναπτυχθούν και τα πρότυπα, κατά τρόπο που οι εγχώριοι φορείς να συνεισφέρουν στις ευρωπαϊκές και διεθνείς πρωτοβουλίες προτυποποίησης, δεδομένου επίσης και του κανονιστικού ενδιαφέροντος που έχουν αποκτήσει τα πρότυπα. Η δραστηριότητα του EESSI σε ευρωπαϊκό επίπεδο αναμένεται να οδηγήσει σε νέες πρωτοβουλίες προτυποποίησης στον ευρύτερο χώρο της ασφάλειας των πληροφοριών, τις οποίες οι παράγοντες της αγοράς και η επιβλέπουσα αρχή θα έχουν την ευκαιρία να παρακολουθήσουν.