ebusinessforum

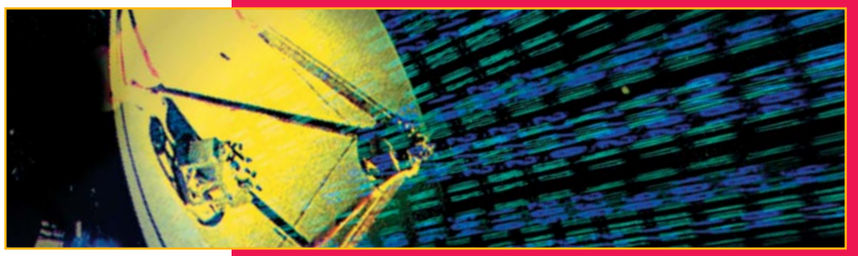
www.ebusinessforum.gr

Ο ΔΕΚΑΛΟΓΟΣ

ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

Γ' ΚΟΙΝΟΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΡΙΞΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
"ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ"
ΥΠ. ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΥΠ. ΕΣΩΤΕΡΙΚΩΝ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΠΟΚΕΝΤΡΩΣΗΣ

Ο ΔΕΚΑΛΟΓΟΣ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ



01]
Πού και γιατί είναι αναγκαία η χρήση “ηλεκτρονικών υπογραφών” και “ηλεκτρονικών πιστοποιητικών ταυτοποίησης”;

Η διενέργεια “**ολοκληρωμένων** ηλεκτρονικών συναλλαγών” μέσα από τα σύγχρονα “ανοικτά δίκτυα επικοινωνιών”, -*όπως είναι το internet και τα δίκτυα κινητής τηλεφωνίας*-, προσφέρει **σημαντικά οφέλη** στους συναλλασσόμενους, όπως ταχύτητα και ευελιξία στις συναλλαγές και προηγμένες δυνατότητες αυτόματης διαχείρισής τους.

Παρόλα αυτά, η προώθηση και η μαζική αποδοχή “ολοκληρωμένων ηλεκτρονικών μεθόδων” (*χωρίς να είναι απαραίτητη η φυσική παρουσία των συναλλασσομένων*) για την διεκπεραίωση **σημαντικών καθημερινών συναλλαγών** στους βασικούς τομείς της οικονομίας (*διοίκηση, εμπόριο, τραπεζικές υπηρεσίες, κ.λπ.*), εξακολουθεί να αναπτύσσεται τόσο στην Ελλάδα όσο και στο ευρωπαϊκό και διεθνές περιβάλλον *με αρκετές επιφυλάξεις*.

Οι βασικές, σήμερα, *μέθοδοι* ηλεκτρονικής “**ταυτοποίησης των συναλλασσόμενων**” (*π.χ. “κωδικός χρήστη/κωδικός πρόσβασης”*) και “**διαφύλαξης της ακεραιότητας των δεδομένων**” (*π.χ. συμμετρική κρυπτογράφηση*), λειτουργούν με την χρήση *κοινών “κλειδιών” ή “κωδικών”* από τους συναλλασσόμενους, με συνέπεια ***να μην μπορούν*** να υποστηρίξουν εφαρμογές που *απαιτούν ασφαλή, αξιόπιστη και εγγυημένη* πιστοποίηση της ταυτότητας (*“ταυτοποίηση”*) των χρηστών αυτών των κλειδιών έναντι κάθε τρίτου, ***ούτε και να*** εξασφαλίσουν την πιστοποίηση της προέλευσης (*“αυθεντικότητα”*), την *“ακεραιότητα”* και την *“εμπιστευτικότητα”* των διακινούμενων ή/και αρχειοθετούμενων *“ηλεκτρονικών δεδομένων”*.

Έτσι, τα ***“έντυπα μέσα”*** που χρησιμοποιούνται για την καταγραφή και την απόδειξη μιας συναλλαγής *(π.χ. ενυπόγραφα ιδιωτικά έγγραφα, επικυρωμένα φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι, θεωρημένα τιμολόγια, κ.λπ.) αποτελούν τα κύρια αποδεικτικά στοιχεία μιας συναλλαγής.* Η πλήρης αντικατάστασή τους με αντίστοιχα “ψηφιακά δεδομένα” που επιτρέπουν ολοκληρωμένες ηλεκτρονικές συναλλαγές, ***προϋποθέτει*** την χρήση *ασφαλών* και τεχνικώς *αξιόπιστων* μεθόδων πιστοποίησης της “προέλευσης” και της “ακεραιότητας” των δεδομένων και κυρίως αποδείξεων για την “μη αποκήρυξη” της συναλλαγής.

Οι ***“προηγμένες ηλεκτρονικές (ή ψηφιακές) υπογραφές”*** και τα ***“ψηφιακά πιστοποιητικά ταυτοποίησης”***, που στηρίζονται στην σύγχρονη τεχνολογία της *“ασύμμετρης κρυπτογραφίας”* ικανοποιούν τις παραπάνω απαιτήσεις, αφού μπορούν να εξασφαλίσουν την ***“αυθεντικότητα”*** *(authentication)* και την ***“ακεραιότητα”*** *(integrity)* των σχετικών δεδομένων, την ***“ταυτοποίηση”*** *(identification)* των συναλλασσόμενων και -κάτω από προϋποθέσεις- τη ***“νομική δέσμευση”*** του υπογράφοντα ή αλλιώς την ***“μη αποκήρυξη”*** *(non repudiation)* της συναλλαγής ενώ, παράλληλα, μπορούν να προσφέρουν αξιόπιστη λύση και στο ζήτημα της ***“εμπιστευτικότητας”*** *(confidentiality)* των δεδομένων κατά την διακίνηση ή/και την αρχειοθέτησή τους. ■

02]
Τι προβλέπει το 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*:

Τη ***"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»*.

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

Έτσι, η 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, κ.λπ.)*, ως τις πιο "σύνθετες" *(π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κ.λπ.)*, 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).*

Ως ***"προηγμένες ηλεκτρονικές υπογραφές"*** *(οι οποίες στο εθνικό μας δίκαιο –π.δ. 150/2001- αποκαλούνται και "ψηφιακές υπογραφές")*, η Οδηγία προσδιορίζει τις ηλεκτρονικές υπογραφές που ικανοποιούν τις εξής απαιτήσεις: ***α)*** *συνδέονται μοναδικά 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 *(-βλέπε ερώτηση 3).*

Ως ***"αναγνωρισμένο πιστοποιητικό"*** ορίζεται από την Οδηγία η *"ηλεκτρονική βεβαίωση"* που εκδίδεται από κάποιον *"Πάροχο Υπηρεσιών Πιστοποίησης" (-βλ. ερώτηση 6)* και η οποία συνδέει μονοσήμαντα τα "δεδομένα επαλήθευσης μιας υπογραφής" *(ή "δημόσιο κλειδί")* με *ένα συγκεκριμένο φυσικό πρόσωπο*, τηρώντας κάποιους **βασικούς όρους** *(-περισσότερα για τα πιστοποιητικά βλέπε στην ερώτηση 4).*

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 (-βλ. ερώτηση 5).*

Η **Οδηγία** προβλέπει την *ελεύθερη* παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, απαγορεύοντας οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης (εφεξής, ΠΥΠ), προσδιορίζοντας, όμως τις *προϋποθέσεις λειτουργίας* (Παράρτημα ΙΙ) και την *ευθύνη* (ά. 6) των ΠΥΠ που εκδίδουν *"αναγνωρισμένα πιστοποιητικά προς το κοινό"*. Παράλληλα προβλέπει την δυνατότητα ***"Εθελοντικής Διαπίστευσης"*** των ΠΥΠ, 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** όπου παρέχεται μια αρχική, αλλά *περιορισμένη αναγνώρισή τους* σε διαδικασίες του δημόσιου τομέα.

Ακολούθησε το **π.δ. 150/2001** (ΦΕΚ Α/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία και καθόρισε την ***"Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων"*** (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για την λειτουργία μηχανισμών "Εθελοντικής Διαπίστευσης" των ΠΥΠ και "Διαπίστωσης" της συμμόρφωσης των "προϊόντων ηλεκτρονικής υπογραφής". Τον Οκτώβριο του 2002, εκδόθηκε το **π.δ. 342/02** το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων *"μηνυμάτων ηλεκτρονικού ταχυδρομείου"* στις επικοινωνίες του δημόσιου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό ***"Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής"***, καθώς και τρεις Κανονισμούς σχετικά με την ***"Εθελοντική Διαπίστευση"*** των ΠΥΠ, την ***"Διαπίστωση"*** *(της συμμόρφωσης με τις απαιτήσεις της Οδηγίας)* βασικών "προϊόντων ηλεκτρονικής υπογραφής" *(-βλέπε σχετικά και απάντηση 5)*, και τον ορισμό των **"Φορέων"** που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ. ■

03]
Πώς λειτουργούν οι προηγμένες (ψηφιακές) ηλεκτρονικές υπογραφές;

Η τεχνολογία της ***"ασύμμετρης κρυπτογραφίας"***, βάσει συγκεκριμένων *"μαθηματικών αλγορίθμων" (π.χ. RSA, DSA, κ.ά.),* παράγει *τυχαία ζεύγη κρυπτογραφικών "κλειδιών"* (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από **δύο σημαντικές ιδιότητες:**

- το καθένα κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν *μόνο* από το άλλο *(συμπληρωματικό του)* κλειδί, και

- *δεν* είναι δυνατό, *με τις παρούσες δυνατότητες της τεχνολογίας,* να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.

Με την τεχνολογία της ασύμμετρης κρυπτογραφίας διατηρώντας μυστικό το ένα κλειδί ως **"ιδιωτικό"** *("δεδομένα δημιουργίας υπογραφής")* και διανέμοντας ελεύθερα το άλλο κλειδί ως **"δημόσιο"** *("δεδομένα επαλήθευσης υπογραφής"), εξασφαλίζουμε* ότι όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να "επαληθεύσουν" μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού.

Πρέπει να σημειωθεί ότι κατά την ***"δημιουργία"*** μιας "ψηφιακής υπογραφής" *δεν κρυπτογραφούνται* τα *"προς υπογραφήν"* δεδομένα, αλλά μία μικρή μαθηματική ***"σύνοψή"*** ("digest") τους, η οποία παράγεται από την χρήση *"μονόδρομων αλγορίθμων κατακερματισμού δεδομένων" ("one-way hashing algorithms" -π.χ. MD5, SHA-1 κ.ά.).* Αυτή η "σύνοψη" των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και *επισυνάπτεται (πιθανώς μαζί και με άλλες χρήσιμες σχετικές πληροφορίες, π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη "πολιτική υπογραφής", κ.ά.),* στα αρχικά δεδομένα, αποτελώντας την ***"προηγμένη ηλεκτρονική υπογραφή"*** τους.

Κατά την αντίστροφη διαδικασία της ***"επαλήθευσης"*** *(verification)* μιας ψηφιακής υπογραφής, εφαρμόζεται στα υπό εξέταση δεδομένα *ο ίδιος "αλγόριθμος κατακερματισμού"* που χρησιμοποιήθηκε κατά την "υπογραφή" τους. Έτσι, η νέα "σύνοψη" που παράγεται, *συγκρίνεται* με την αντίστοιχη "σύνοψη" που προέρχεται από την αποκρυπτογράφηση της "προηγμένης ηλεκτρονικής υπογραφής" με το υποδεικνυόμενο δημόσιο κλειδί του υπογράφοντα εάν ταυτίζονται οι δύο συνόψεις, τότε η υπογραφή *"επαληθεύεται"* και *επιβεβαιώνεται ότι:*

- *τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού*

- *τα αρχικά δεδομένα δεν έχουν αλλοιωθεί*

Παρόλα αυτά διατηρείται ακέραια η ***ανάγκη,*** -ιδίως σε ανοικτές εφαρμογές με πολλαπλούς ή ακόμη και άγνωστους αποδέκτες-, για την ύπαρξη μιας ***"Εμπιστης Τρίτης Οντότητας"*** που ονομάζεται ***"Πάροχος Υπηρεσιών Πιστοποίησης"*** (ΠΥΠ) η οποία, επιπλέον, *πιστοποιεί* προς οποιοδήποτε τρίτο αποδέκτη μιας ψηφιακής υπογραφής:

- *την καταγραφή (registration) της ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο συγκεκριμένο δημόσιο κλειδί, και*

- *τη πραγματική κατοχή του σχετικού ιδιωτικού κλειδιού από τον πιστοποιούμενο (proof of possession).*

Η παραπάνω πιστοποίηση (προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής) γίνεται με την έκδοση ***"ψηφιακών πιστοποιητικών"*** τα οποία περιέχουν το δημόσιο κλειδί και τα στοιχεία ταυτοποίησης του κατόχου του πιστοποιητικού, και

τα οποία *υπογράφονται ψηφιακά* από τον "εκδότη" τους.

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

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

Η ιεραρχική πιστοποίηση δημόσιων κλειδιών των συναλλασσόμενων-τελικών οντοτήτων από μια τεκμηριωμένη υποδομή "PKI" ενός (ή περισσότερων) ΠΥΠ, θεωρείται *ιδανική* για την έκδοση **"αναγνωρισμένων πιστοποιητικών",** τα οποία παρέχουν ικανοποιητικές εγγυήσεις στις συναλλαγές -ακόμη και μεταξύ αγνώστων.

Άλλη ευρείας χρήσης εναλλακτική τεχνολογία "προηγμένης ηλεκτρονικής υπογραφής" βασίζεται στα "αυτό-ϋπογραφόμενα" πιστοποιητικά *που εκδίδονται από τον ίδιο τον (τελικό) χρήστη-κάτοχο ζεύγους κρυπτογραφικών κλειδιών,* ο οποίος λειτουργεί και ως αποδέκτης αντίστοιχων πιστοποιητικών. Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους ***"εξυπηρετητές κλειδιών"*** *(key servers)* όπου αξιολογούνται και *υπογράφονται και από άλλους χρήστες,* οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο-κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Αυτή η μέθοδος πιστοποίησης, η οποία είναι ήδη **πολύ διαδεδομένη διεθνώς** -ιδίως σε κλειστές ομάδες προγραμματιστών Η/Υ και γενικότερα σε κοινότητες με κοινές δραστηριότητες, π.χ. σωματεία, σύλλογοι κ.λπ.- **αποκαλείται "Pretty Good Privacy"** (PGP) και βασίζεται στην δημιουργία ενός (αποκεντρωμένου) ***"δικτύου εμπιστοσύνης"*** *("web of trust")* που αναπτύσσεται με την μεταβίβαση της εμπιστοσύνης μεταξύ των χρηστών της.

Η μέθοδος PGP και οι παραλλαγές της (GPG, OpenPGP, κ.λπ.) 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. ■

04]

Ποιες είναι οι βασικές λειτουργίες και ποιες οι κατηγορίες των ηλεκτρονικών πιστοποιητικών;

Ως **"ηλεκτρονικά πιστοποιητικά",** με την ευρεία έννοια, νοούνται *όλα* τα αποδεικτικά στοιχεία που βρίσκονται σε ηλεκτρονική μορφή και τα οποία δημιουργούνται είτε αυτόματα είτε με πρωτοβουλία ενός συναλλασσόμενου κατά την διενέργεια μιας ηλεκτρονικής συναλλαγής. Συνήθως όμως ο όρος αναφέρεται ειδικότερα στα ***"ψηφιακά πιστοποιητικά ταυτοποίησης"*** ή ***"Πιστοποιητικά Δημοσίου Κλειδιού"*** *("Public Key Certificates")* τα οποία υποστηρίζουν την λειτουργία των "προηγμένων ηλεκτρονικών" (ή "ψηφιακών") υπογραφών. Τα πιστοποιητικά αυτά είναι τυποποιημένες ηλεκτρονικές βεβαιώσεις που εκδίδονται και υπογράφονται ηλεκτρονικά από έναν ΠΥΠ *(ή και από φυσικό πρόσωπο στην περίπτωση της μεθόδου PGP)* με **σκοπό** να πιστοποιήσουν την κατοχή συγκεκριμένου ζεύγους (ασύμμετρων) κρυπτογραφικών κλειδιών από ένα υποκείμενο *(Proof of Possession)* και να περιγράψουν στοιχεία ταυτοποίησης *(Identification)* του υποκειμένου αυτού.

Το πιο διαδεδομένο διεθνώς πρότυπο για την σύνταξη ενός ηλεκτρονικού (ψηφιακού) πιστοποιητικού είναι το **"X.509"** το οποίο αποτελεί *"Σύσταση" (Recommendation)* της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Το πρότυπο **X.509** διαθέτει αρκετά **προκαθορισμένα πεδία** για την αναγραφή των απαραίτητων πληροφοριών *(αριθμός ταυτοποίησης του πιστοποιητικού, εκδότης, περιγραφή υποκειμένου-θέματος, δημόσιο κλειδί υποκειμένου, υπογραφή εκδότη, διάρκεια ισχύος, χρήσεις κλειδιού, πολιτική πιστοποιητικού, διευθύνσεις πληροφοριών ανάκλησης, κ.ά.),* καθώς και τη δυνατότητα (στην έκδοση "3") να συμπεριλάβει και επιπλέον **εκτεταμένα πεδία** *(extensions)* που καθορίζονται από τον Εκδότη των πιστοποιητικών.

Λόγω της διαρκούς τεχνολογικής εξέλιξης, *θεωρείται δεδομένη η εξασθένηση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών* στο πέρασμα του χρόνου. Έτσι, τα πιστοποιητικά δημοσίου κλειδιού, που αναφέρονται σε -αλλά και που υπογράφονται από τέτοια κρυπτογραφικά κλειδιά, εκδίδονται **με περιορισμένη διάρκεια ισχύος** *(συνήθως 1 έως 3 έτη),* η οποία και αναγράφεται μέσα στα προκαθορισμένα για τον σκοπό αυτό πεδία τους.

Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού **μπορεί οποτεδήποτε να ανακληθεί** οριστικά (revocation) **ή να ανασταλεί** προσωρινά (suspension), ύστερα από αίτημα του ίδιου του τελικού χρήστη *(π.χ. επειδή έχασε τον φορέα των κρυπτογραφικών κλειδιών του)* ή/και από σχετική απόφαση του Εκδότη τους *(π.χ. λόγω λάθους στην αναγραφή στοιχείων).* Η **"ανάκληση"** και η **"αναστολή"** ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του "σειριακού αριθμού" του πιστοποιητικού (certificate's serial number) σε μια *"Λίστα Ανακληθέντων Πιστοποιητικών" (Certificate Revocation List ή "CRL")* η οποία υπογράφεται και δημοσιεύεται *σε τακτά χρονικά διαστήματα* από τον ίδιο τον Εκδότη των πιστοποιητικών.

Ένα "ζεύγος κρυπτογραφικών κλειδιών" μπορεί πρακτικά να χρησιμοποιηθεί από τον κάτοχό του σε *διάφορες εφαρμογές.* Μεταξύ αυτών περιλαμβάνονται:

- η απλή ***"κρυπτογράφηση δεδομένων"*** ή άλλων κρυπτογραφικών κλειδιών, κ.λπ.

Η έκδοση ενός πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών από έναν ΠΥΠ, *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 (βλ. και ερώτημα 8)-,* 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 Αποκήρυξη" 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 ΠΥΠ και η οποία συμπεριλαμβάνει *όλους τους ειδικότερους όρους έκδοσης και χρήσης* που καθορίζει ο ΠΥΠ 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 κ.λπ.),* 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 – "AA")* 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.λπ.).* 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" ή "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".* ■

05]
Τι εξοπλισμός απαιτείται για τη δημιουργία και την επαλήθευση των η-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 υλισμικού (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 ΠΔ 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 ΠΥΠ οι οποίες μεταφέρουν *άμεσα* τα δημιουργηθέντα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη για τον οποίο προορίζονται, *χωρίς* να τα εκθέτουν ή να διατηρούν αντίγραφά τους,

β) ***«δεν μπορούν, 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 "α.δ.δ.υ." *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). ■

06]

Ποιες είναι οι υποχρεώσεις, οι ευθύνες και οι λειτουργίες ενός Παρόχου Υπηρεσιών Πιστοποίησης (ΠΥΠ);

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 ΠΥΠ και να εκδώσει αναγνωρισμένα ή όχι πιστοποιητικά. Μόνη υποχρέωση ενός ΠΥΠ προς την εποπτεύουσα αρχή (ΕΕΤΤ), είναι η ***"Δήλωση Έναρξης Λειτουργίας"*** και η εγγραφή του στο σχετικό ***"Μητρώο ΠΥΠ"***, καθώς και η αποστολή, προς την αρχή, ***"Ετήσιων Εκθέσεων"*** σχετικά με την λειτουργία τους.

Για να εκδώσει ένας ΠΥΠ ***"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 ΠΥΠ 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 ΠΥΠ αποκτά "δικαίωμα επίκλησης" της συγκεκριμένης διαπίστευσής του προς κάθε τρίτο, υποβάλλεται όμως σε περαιτέρω υποχρεώσεις και ελέγχους που συνήθως επιβάλλει ο σχετικός φορέας.

Κάθε ΠΥΠ, 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 εκδόμενου 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 ΠΥΠ ***("σύμβαση αποδέκτη")***.

Στην περίπτωση, όμως, που ο ΠΥΠ 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 παράλειψη του ΠΥΠ 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 ΠΥΠ).

Η ευθύνη του ΠΥΠ 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 ΠΥΠ μπορεί να απαλλαχθεί εντελώς από την ευθύνη εκ του νόμου εάν αποδείξει ότι η σχετική πράξη ή παράλειψή του δεν προήλθε από αμέλεια.

Οι **βασικές υπηρεσίες** που προσφέρει υποχρεωτικά ένας ΠΥΠ μπορούν να διακριθούν σε οργανωμένες *ξεχωριστές λειτουργικές οντότητες*, και συγκεκριμένα σε:

- ***Υπηρεσία Εγγραφής/Καταχώρησης*** *(Registration Authority –"**RA**")*, η οποία 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,
- ***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 & Revocation Status Service)*, η οποία αναλαμβάνει την δημοσίευση των κειμένων τεκμηρίωσης των υπηρεσιών του ΠΥΠ *(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 ΠΥΠ.

Εκτός από τις παραπάνω υποχρεωτικές υπηρεσίες, *-οι οποίες προβλέπονται έμμεσα από την Οδηγία αλλά και από σχετικά νομικοτεχνικά πρότυπα-* ένας ΠΥΠ 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 συχνά και ως "Notary Services")*, κ.λπ.

Είναι επιτρεπτό για έναν ΠΥΠ να ***εκχωρήσει σε τρίτους*** *(outsourcing)* τη διεκπεραίωση ***μέρους*** ή ακόμη και του ***συνόλου*** των παραπάνω παρεχόμενων υπηρεσιών του. Εφόσον όμως ο ΠΥΠ 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. ■

07]
Τι πρέπει να προσέχει ο 'υπογράφων' και τι ο 'αποδέκτης' (relying party) των ηλεκτρονικών υπογραφών;

Τόσο ο ***υπογράφων*** όσο και ο ***αποδέκτης*** μιας ηλεκτρονικής υπογραφής, πρέπει, κατ' αρχήν, 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 ΠΥΠ (π.χ. Σύμβαση Συνδρομητή με τον ΠΥΠ, Πολιτική Πιστοποιητικού κ.λπ.)* 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 ΠΥΠ για την απόκτηση του σχετικού πιστοποιητικού του, διότι, σε αντίθετη περίπτωση, είναι πιθανόν *να επωμισθεί ο 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 ΠΥΠ, 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 ΠΥΠ 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 ΠΥΠ 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 ΠΥΠ ***"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 ΠΥΠ),*

- 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 ΠΥΠ 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 ευρωπαϊκούς οργανισμούς προτυποποίησης, η "Πολιτική Υπογραφής"* μπορεί να προσδιορίζει, *-εκτός από τα αποδεκτά είδη/πολιτικές πιστοποιητικών-, τις τυχόν "απαραίτητες ιδιότητες"* του υπογράφοντα, την πιθανή υποχρέωση για εναπόθεση *"αξιόπιστης χρονοσήμανσης"* στην δημιουργηθείσα υπογραφή, την ανάγκη για *"επανέλεγχο της ανάκλησης"* του πιστοποιητικού πριν την οριστική αποδοχή της υπογραφής, κάποιες συγκεκριμένες *"ρίζες εμπιστοσύνης"* που απαιτείται να χρησιμοποιηθούν για την επαλήθευση των πιστοποιητικών, κ.ά. ■

08]
Ποιες είναι σήμερα οι σημαντικότερες εφαρμογές και ποιες οι προοπτικές των ηλεκτρονικών υπογραφών;

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)*
- Ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη απο 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, κ.λπ.) του κατόχου τους
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου *(S/MIME)*
- Συστήματα "υπογραφής αυθεντικότητας" διακινούμενου λογισμικού *(π.χ. Microsoft Authenticode)*
- Κλειστές υποδομές "PKI" για εφαρμογές ασφαλείας μεγάλων οργανισμών *(π.χ. NATO)*
- Πιστοποίηση της ταυτότητας "εξυπηρετητών διαδικτύου" *(web servers), κ.ά.*

Στην Ευρωπαϊκή Ένωση, εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κλπ, έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία "τυπικές εφαρμογές" των η-υπογραφών, *οι προϋποθέσεις των οποίων πηγάζουν απο το νόμο.* Τα ***"ηλεκτρονικά δελτία ταυτότητας"*** σε χώρες όπως το Βέλγιο, Φινλανδία, Ιταλία, Εσθονία 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,* εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.

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"***, 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, τη δημοσίευση προκηρύξεων, κ.λπ.).*

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"*** *(ή "H.E.R.M.E.S." -Hellenic Exchanges Remote MEssaging Services)* και βασίζεται στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων ("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)* εναποθετημένα *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, 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)***, κ.ά. Σημαντικότατη εξέλιξη προς την γενικευμένη χρήση ηλεκτρονικών υπογραφών στην Ελληνική Δημόσια Διοίκηση θα αποτελέσει ιδίως η υλοποίηση και η ολοκλήρωση του *"Υποέργου 9"* του *-ήδη σε εξέλιξη-* συνολικού έργου ***"Σύζευξις"***, όπου προβλέπεται 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. ■

09]

Ποια είναι τα σημαντικότερα εμπόδια και ποιες οι προϋποθέσεις για την ευρεία διάδοση και χρήση των ηλεκτρονικών υπογραφών;

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, κ.λπ.),* 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, **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 "profile"*** των χρηστών.

Η ***τεχνική πολυπλοκότητα***, οι ***παραλλαγές*** των εφαρμογών προηγμένων ηλεκτρονικών υπογραφών, και τα ***διαφορετικά επίπεδα νομικής αναγνώρισής*** τους *(-βλέπε και ερώτηση 2),* 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, κ.λπ.).*

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 ***αναστολικούς 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.

Ο ΔΕΚΑΛΟΓΟΣ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

- 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 ΠΥΠ που λειτουργούν στο ίδιο κράτος,* όπως παρατηρήθηκε -στο πλαίσιο της λειτουργίας της ΟΕ "Ε2" του eBusinessForum- ότι συμβαίνει και στην Ελλάδα.

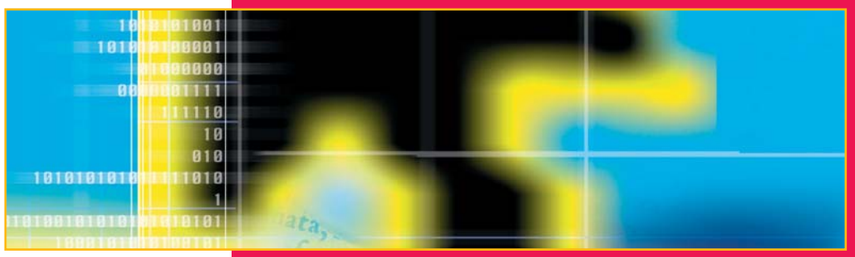
Τα ***σημαντικότερα προβλήματα διαλειτουργικότητας*** μεταξύ των υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών που παρατηρούνται, αναφέρονται κυρίως στην *"περιγραφή των στοιχείων του υποκειμένου"* των πιστοποιητικών *("naming policy/conventions")*, στον *"τρόπο προσδιορισμού των επιτρεπόμενων χρήσεων"* των σχετικών κρυπτογραφικών κλειδιών *(-βλέπε και απάντηση 4 σχετικά με τη χρήση του πεδίου "Key Usage")* 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 *"αλληλοδιαπίστευση των ΠΥΠ"*, κ.ά. Όλα αυτά έχουν ως πρόσθετο αρνητικό αποτέλεσμα την *έλλειψη κοινώς αποδεκτών εφαρμογών λογισμικού* για τη δημιουργία και την επαλήθευση ηλεκτρονικών υπογραφών, οι οποίες να εφαρμόζουν 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 ***"Διαπίστωση"*** *(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 ΠΥΠ.

Παράλληλα, η σύνταξη ***"Πολιτικών (Ηλεκτρονικής) 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")*, 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. ■



10] Που μπορώ να βρω πηγές για περισσότερη και αξιόπιστη ενημέρωση για τα θέματα αυτά;

Στο δικτυακό τόπο της ***"Εθνικής Επιτροπής Τηλεπικοινωνιών & Ταχυδρομείων"*** (ΕΕΤΤ): **www.eett.gr** και στην θεματική ενότητα *"Τηλεπικοινωνίες- Ηλεκτρονικές Υπογραφές"* θα βρείτε το *επίσημο* ***"Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης"*** που ασκούν την δραστηριότητα τους στην Ελλάδα και άλλες χρήσιμες πληροφορίες, όπως τις σχετικές *"Αποφάσεις"* της ΕΕΤΤ *(οι οποίες αποτελούν το* ***"εθνικό ρυθμιστικό πλαίσιο")***, καθώς και ενημέρωση σχετικά με την άσκηση της εποπτείας στη λειτουργία των ΠΥΠ από την ΕΕΤΤ.

Μια αξιόπιστη πηγή για το ισχύον εθνικό, κοινοτικό και διεθνές δίκαιο, καθώς και για την υπάρχουσα σχετική νομολογία για τις ηλεκτρονικές υπογραφές, αποτελεί η σχετική θεματική ενότητα για τις ηλεκτρονικές υπογραφές στην ***"Τράπεζα Νομικών Πληροφοριών Ηλεκτρονικού Εμπορίου"***, την οποία συντηρεί και δημοσιεύει δωρεάν το ***"Εμπορικό & Βιομηχανικό Επιμελητήριο Αθηνών"*** (ΕΒΕΑ) στη διεύθυνση: **http://www.acci.gr/ecomm/legal/index.htm.**

Στην διεύθυνση **http://www.ict.etsi.org/EESSI_home.htm** βρίσκεται η κεντρική σελίδα του ***"European Electronic Signature Standardization Initiative"*** (EESSI) που έχει την ευθύνη του σχεδιασμού και του συντονισμού των ευρωπαϊκών προτύπων στη βάση της Οδηγίας 99/93/ΕΚ. Η σελίδα του EESSI διαθέτει συγκεντρωμένες χρήσιμες πληροφορίες σχετικά με την διαδικασία προτυποποίησης των ηλεκτρονικών υπογραφών, καθώς και συνδέσεις (links) προς τις λίστες με **όλα τα πρότυπα** που έχουν συνταχθεί και δημοσιεύονται από τους *ευρωπαϊκούς οργανισμούς προτυποποίησης* ***"Electronic Telecommunication Standardization Institute"*** (ETSI) και ***"European Committee for Standardization/Information Society Standardisation System" (CEN/ISSS)***.

Τέλος, στο δικτυακό τόπο του **"e-Business Forum" (www.e-businessforum.gr)** και συγκεκριμένα της ιστοσελίδας της **Ομάδας Εργασίας "Ε2",** βρίσκεται ένας ευρύς κατάλογος συνδέσμων προς σχετικές πηγές, κείμενα και μελέτες. ■

Ο ΔΕΚΑΛΟΓΟΣ ΓΙΑ ΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

ΣΥΝΤΟΝΙΣΤΕΣ:

Δρακούλης Μαρτάκος
Αναπληρωτής Καθηγητής Τμήματος Πληροφορικής και Επικοινωνιών
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
martakos@di.uoa.gr

Νίκος Κυρλόγλου
Ειδικός Επιστήμονας Πληροφορικής
ΕΒΕΑ
nikoky@acci.gr

Ανδρέας Μητράκας
Δ.Ν. - Legal Practices Manager
Ubizen NV (BE)
andreas@mitrakas.com

ΕΙΣΗΓΗΤΕΣ:

Μαρία Γιαννακάκη
Δικηγόρος, LL.M σε IT Law
giannakaki.m@dsa.gr

Χρήστος Σιουλής
Δικηγόρος - Νομικοτεχνικός Σύμβουλος
csioulis@dsa.gr

ΕΔΕΤ Α.Ε.
ΕΘΝΙΚΟ ΔΙΚΤΥΟ ΕΡΕΥΝΑΣ & ΤΕΧΝΟΛΟΓΙΑΣ

GRNET S.A.
GREEK RESEARCH & TECHNOLOGY NETWORK

Το e-Business Forum αποτελεί έργο του Ε.Π. Κοινωνία της Πληροφορίας (Μέτρο 3.1), υλοποιείται από την ΕΔΕΤ Α.Ε. και συγχρηματοδοτείται κατά 75% από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης και κατά 25% από εθνικούς πόρους.

Λ.Μεσογείων 56, 11527 Αθήνα
Τηλ.: 210 7474274, Fax: 210 7474490
email: info@grnet.gr http://www.grnet.gr