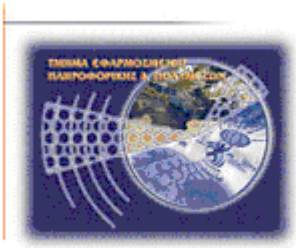
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος: "*Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης (Τεχνική & Νομική προσέγγιση)* "

Πέτρος Κωνσταντίνου (ΑΜ: 649)

Ηράκλειο 01-01-2007

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ Ι: ΕΙΣΑΓΩΓΗ

ΟΙ η-ΥΠΟΓΡΑΦΕΣ & ΤΑ η-ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ

Οι τεχνικώς ασφαλείς αλλά και νομικώς αναγνωρισμένες ηλεκτρονικές συναλλαγές μέσω των 'ανοικτών δικτύων' (όπως το διαδίκτυο, κ.λ.π.), αποτελούν τη βασική προϋπόθεση για την περαιτέρω ανάπτυξη του 'ηλεκτρονικού επιχειρείν' και τη παροχή προηγμένων ηλεκτρονικών υπηρεσιών στην «Κοινωνία της Πληροφορίας».

Η ανάγκη για σταδιακή αντικατάσταση των παραδοσιακών μέσων για την καταγραφή και απόδειξη μιας 'συμβατικής συναλλαγής' (ενυπόγραφα ιδιωτικά έγγραφα, φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι, θεωρημένα τιμολόγια, κ.λ.π.) με αντίστοιχα 'ηλεκτρονικά δεδομένα' που θα δημιουργούνται, υφίστανται επεξεργασία, επαληθεύονται και αρχειοθετούνται με ηλεκτρονικά μέσα (χωρίς, δηλαδή, την ανάγκη ενσωμάτωσής τους σε υλικό φορέα, όπως είναι το χαρτί), έχει οδηγήσει στην ανάπτυξη συγκεκριμένων τεχνολογιών και μεθόδων (π.χ. 'Υποδομές Δημοσίων Κλειδιών'–PKI, 'Pretty Good Privacy'–PGP, βιομετρικές μεθόδους κλπ.). Σχετικές νομοθετικές ρυθμίσεις προσφέρουν στις ηλεκτρονικές συναλλαγές το κύρος, την ασφάλεια, την αναγνωρισιμότητα και την εμπιστοσύνη που διαθέτουν οι συμβατικές μέθοδοι.

Έτσι, με την συνδυασμένη χρήση κρυπτογραφικών εργαλείων (αλγόριθμοι), κατάλληλα διαμορφωμένου λογισμικού (software), ειδικού υλισμικού και υποδομών (hardware) και συγκεκριμένων διαδικασιών (procedures), είναι δυνατόν σήμερα να προσφερθούν λύσεις που ικανοποιούν τις απαιτήσεις και τις λειτουργίες των συμβατικών συναλλαγών. Τέτοιες είναι οι (προηγμένες) ***«ηλεκτρονικές υπογραφές»*** και τα ***«ηλεκτρονικά πιστοποιητικά ταυτοποίησης»*** τα οποία εξασφαλίζουν 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 αποποίηση'*** (*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.

ΜΕΡΟΣ ΙΙ: ΑΝΑΠΤΥΞΗ ΘΕΩΡΗΤΙΚΟΥ ΥΠΟΒΑΘΡΟΥ

ΤΕΧΝΙΚΗ ΑΝΑΛΥΣΗ

Μέθοδοι ασφάλειας ηλεκτρονικών συναλλαγών και ηλεκτρονικές υπογραφές

Στις καθημερινές **συμβατικές συναλλαγές** έχουν καθιερωθεί *–είτε εθιμικά είτε νομοθετικά-* η χρήση διαφόρων μεθόδων για την εξακρίβωση της ταυτότητας των συναλλασσόμενων και την συγκέντρωση και διατήρηση αποδείξεων για την πραγματοποίηση μιας συναλλαγής, που βασίζονται κυρίως σε **πρωτότυπα ενυπόγραφα έγγραφα** που αρχειοθετούνται για όσο και επιδεικνύονται όποτε χρειάζεται.

Αντιθέτως, **στις ηλεκτρονικές συναλλαγές**, τα χρησιμοποιούμενα ψηφιακά δεδομένα, λόγω της μη ενσωμάτωσής τους σε ένα μοναδικό υλικό φορέα, είναι δύσκολο να προστατευθούν από αλλοίωση ή/και αντιγραφή, ενώ και η απόδειξη της προέλευσής τους καθίσταται, επίσης, ιδιαίτερα προβληματική.

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'. Σχετική με την παραπάνω ανεπάρκεια των χρησιμοποιούμενων μεθόδων, αποτελεί και η διαπίστωση πρόσφατης μεγάλης έρευνας[1], σύμφωνα με την οποία, η «έλλειψη ασφάλειας στις ηλεκτρονικές συναλλαγές» αποτελεί τον πρώτο (με ποσοστό 77%!) αρνητικό λόγο που δικαιολογούν οι επιχειρήσεις την απροθυμία τους να ενασχοληθούν με το «ηλεκτρονικό εμπόριο».

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.*) εξακολουθούν να αποτελούν σήμερα τα κύρια αποδεικτικά στοιχεία μιας συναλλαγής.

Η **πλήρης αντικατάστασή** τους με αντίστοιχα 'ψηφιακά δεδομένα' (τα οποία επιτρέπουν ολοκληρωμένες ηλεκτρονικές συναλλαγές) –ιδίως σε περιπτώσεις 'σημαντικών' συναλλαγών- , ***προϋποθέτει*** την χρήση *ασφαλών* και τεχνικώς *αξιόπιστων* μεθόδων πιστοποίησης της 'προέλευσης' και της 'ακεραιότητας'

[1] που πραγματοποιήθηκε στα πλαίσια του έργου 'La Mer' (9/2003) με την συμπλήρωση σχετικού ερωτηματολογίου από πολλές συμμετέχουσες ΜΜΕ.

των δεδομένων και κυρίως την παροχή αποδείξεων για την 'μη αποκήρυξη' της συναλλαγής, κάτι που, με τις υπαρχουσες σήμερα τεχνολογικές δυνατότητες, μπορεί να παράσχει άμεσα μόνο η χρήση '***προηγμένων ηλεκτρονικών υπογραφών***' και σχετικών '***ηλεκτρονικών πιστοποιητικών ταυτοποίησης***'.

Χρήση Ασύμμετρης Κρυπτογράφησης και Σχετικών Αλγόριθμων

Η τεχνολογία της '***ασύμμετρης κρυπτογράφησης***', 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 δυνατόν (*με τις παρούσες δυνατότητες της τεχνολογίας)* να συμπεράνει κανείς *ή* να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.

Χάρις σε αυτήν την τεχνολογία, 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 το '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.

Πιστοποίηση Δημόσιου Κλειδιού (PKI και PGP)

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

- την καταγραφή (registration) της πραγματικής ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο χρησιμοποιούμενο δημόσιο κλειδί, και
- τη σύνδεση του σχετικού ιδιωτικού κλειδιού με τον κάτοχο του πιστοποιητικού (proof of possession).

Η παραπάνω πιστοποίηση (προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής) γίνεται με την έκδοση '**ψηφιακών πιστοποιητικών**' τα οποία υπογράφονται ηλεκτρονικά από τον ΠΥΠ και τα οποία περιέχουν τα στοιχεία ταυτοποίησης του κατόχου του ιδιωτικού κλειδιού, καθώς και (αυτούσιο!) το σχετικό δημόσιο κλειδί του.

Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, δημοσιεύει και υποστηρίζει 'τυποποιημένες ηλεκτρονικές βεβαιώσεις' (πιστοποιητικά) για τους συνδρομητές του (υποκείμενα πιστοποίησης) ονομάζεται '**Υποδομή Δημοσίων Κλειδιού'** (Public Key Infrastructure – 'PKI'),

Μια άλλη εναλλακτική μέθοδος πιστοποίησης των δημοσίων κλειδιών ενός χρήστη βασίζεται στα «αυτό-ϋπογραφόμενα πιστοποιητικά» που εκδίδονται από το ίδιο τον (τελικό) χρήστη (κάτοχο του συγκεκριμένου ζεύγους κρυπτογραφικών κλειδιών), ο οποίος λειτουργεί παράλληλα και ως 'αποδέκτης'. Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους 'εξυπηρετητές κλειδιών' (key servers), απ' όπου λαμβάνονται, αξιολογούνται και πιθανώς υπογράφονται και από άλλους χρήστες, οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο-κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Ένα πολύ διαδεδομένο τέτοιο σύστημα (αλληλο-)πιστοποίησης είναι το '**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.

Είδη ηλεκτρονικών πιστοποιητικών

Τα 'πιστοποιητικά δημοσίου κλειδιού' μπορούν 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 on-line επικοινωνίας- μόνο η χρήση ενός συγκεκριμένου λογαριασμού ηλεκτρονικού ταχυδρομείου (*e-mail address*) από το υποκείμενο.

Εκτός από στοιχεία ταυτοποίησης του υποκειμένου τους, τα πιστοποιητικά δημοσίου κλειδιού μπορούν να περιλαμβάνουν και αναφορά σε συγκεκριμένες (πιστοποιημένες ή μη) **ιδιότητες** του υποκειμένου (*π.χ. επάγγελμα κ.λ.π.*). Μια άλλη σχετική δυνατότητα είναι η χρήση άλλων (πρόσθετων) ειδικών '***πιστοποιητικών ιδιοτήτων***' (attribute certificates) τα οποία χρησιμοποιούνται παράλληλα με τα ***'βασικά πιστοποιητικά δημοσίου κλειδιού'***, και τα οποία μπορούν να εκδίδονται από μια 'Αρχή Πιστοποίησης Ιδιοτήτων' (Attribute Authority – 'AA'),.

Πέρα των πιστοποιητικών για φυσικά πρόσωπα, μια **άλλη κατηγορία πιστοποιητικών** δημοσίων κλειδιών αποτελεί αυτή που εκδίδεται με 'υποκείμενο' τηλεπικοινωνιακά ή πληροφορικά συστήματα και συσκευές (*web servers, routers, client devices, κ.λ.π.*). Η χρήση των κρυπτογραφικών κλειδιών που σχετίζονται με τα συγκεκριμένα πιστοποιητικά, γίνεται συνήθως με αυτόματο τρόπο από τους servers αυτούς και περιορίζεται κυρίως: **α)** σε «υπογραφές ταυτοποίησης» των συσκευών αυτών (*server authentication*) και, **β)** σε «κρυπτογράφηση άλλων συμμετρικών κλειδιών» τα οποία 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 'εξυπηρετητή διαδικτύου' (web server) -*στον οποίον έχουν εγκατασταθεί τα σχετικά κρυπτογραφικά κλειδιά*- επιτρέποντας παράλληλα και την 'κρυπτογράφηση παροδικών συμμετρικών κλειδιών' (*session keys*) για την επίτευξη ασφαλούς (εμπιστευτικής) επικοινωνίας τύπου «**SSL**» ή «**TSL**».

Τέλος, μια άλλη **κατηγορία ηλεκτρονικών πιστοποιητικών**, αποτελούν τα '**πιστοποιητικά χρονοσήμανσης**' 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'* 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 μια συγκεκριμένη χρονική στιγμή, αποκλείοντας έτσι την δυνατότητα μελλοντικής 'αποποίησης' της από τον υπογράφοντα με τον ισχυρισμό ότι αυτή δημιουργήθηκε **μετά** την λήξη ή την ανάκληση του σχετικού 'πιστοποιητικού δημοσίου κλειδιού' (*π.χ. λόγω έκθεσης του συγκεκριμένου κρυπτογραφικού κλειδιού σε τρίτους*).

Μορφή και περιεχόμενο των η-Πιστοποιητικών (X.509).

Τα ηλεκτρονικά '***Πιστοποιητικά Δημοσίου Κλειδιού***' ('Public Key Certificates' ή 'PKC') είναι τυποποιημένα ηλεκτρονικά έγγραφα τα οποία εκδίδονται και υπογράφονται από έναν ΠΥΠ (*που μπορεί να είναι και 'φυσικό πρόσωπο', όπως π.χ. 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 'πιστοποιητικού δημοσίου κλειδιού' 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, υποκείμενο-θέμα, 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.

Ο έλεγχος του κύρους των η-πιστοποιητικών και των η-υπογραφών

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 (suspension), ύστερα από αίτημα 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 'αριθμού ταυτοποίησης 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[2].

Επίσης, επειδή τα '***πιστοποιητικά δημοσίων κλειδιών***' (*public key certificates –'PKC'*) που εκδίδει ένας ΠΥΠ προς τις 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

[2] Βέβαια, τελευταία, έχει αρχίσει να χρησιμοποιείται ευρέως η τεχνολογία/υπηρεσία της «Άμεσης Επιβεβαίωσης της Κατάστασης του Πιστοποιητικού» ('Online Certificate Status Provision' ή 'OCSP') η οποία έχει ως σημαντικό πλεονέκτημα τον άμεσο έλεγχο της πραγματικής κατάστασης ενός πιστοποιητικού, ακόμη και ελάχιστες στιγμές μετά την οριστική αποδοχή του 'αιτήματος ανάκλησης' από τον ΠΥΠ.

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'.

Έτσι, για να ελέγξει κάποιος την εγκυρότητα μιας προηγμένης ηλεκτρονικής υπογραφής, θα πρέπει να ελέγξει το κύρος του συγκεκριμένου πιστοποιητικού που την υποστηρίζει, και συγκεκριμένα θα πρέπει να ελέγξει:

- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα 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).

- Ότι το συγκεκριμένο πιστοποιητικό 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 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 ('*Online Certificate Status Protocoll'* - 'OCSP') που πιθανώς να παρέχει ο ΠΥΠ.

- Ότι το συγκεκριμένο πιστοποιητικό του υπογράφοντα 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 ισχύουσα «*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.

Διατάξεις Δημιουργίας και Επαλήθευσης υπογραφής

Για την **δημιουργία** μίας 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 τελικής επικοινωνίας' (interface) με τον χρήστη, το οποίο χρησιμοποιείται στην διαδικασία δημιουργίας μιας ηλεκτρονικής υπογραφής

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.

Πολιτική (έκδοσης) Πιστοποιητικών & περιορισμοί στη χρήση των κρυπτογραφικών κλειδιών

Η έκδοση πιστοποιητικού από έναν ΠΥΠ για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδών ενός 'υποκειμένου', υπόκειται σε συγκεκριμένες διαδικασίες και, στις περισσότερες περιπτώσεις, συνοδεύεται από συγκεκριμένους περιορισμούς για την χρήση των πιστοποιημένων κλειδιών από το υποκείμενο. Η περιγραφή των διαδικασιών έκδοσης και οι όροι χρήσης ενός πιστοποιητικού καθορίζονται σε μία συγκεκριμένη '**Πολιτική Πιστοποιητικού'** (Certificate Policy) η οποία δημοσιεύεται από τον ΠΥΠ (*εκδότη του πιστοποιητικού*).

Το αρχικό κείμενο μιας '**Πολιτικής Πιστοποιητικού**', αλλά και κάθε επόμενη έκδοσή του, 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 έτσι *τόσο* το ίδιο το 'υποκείμενο πιστοποίησης' (τον 'υπογράφοντα' -ο οποίος είναι συμβεβλημένος 'συνδρομητής' του ΠΥΠ!), *όσο* και κάθε τρίτο-αποδέκτη των πιστοποιητικών του για την (επακριβή) εφαρμοζόμενη Πολιτική.

Πέρα, όμως, από τους όποιους σχετικούς όρους και περιορισμούς που (μπορεί να) αναφέρονται στο κείμενο μιας 'Πολιτικής Πιστοποιητικού', επιβάλλεται η παράλληλη ύπαρξη ενός 'τεχνικού' τρόπου για την αυτόματη αναγνώριση (από τους ίδιους τους υπολογιστές) κάποιων περιορισμών και όρων στην χρήση των πιστοποιούμενων 'κρυπτογραφικών κλειδιών' από τον κάτοχό τους, οι οποίοι θέτονται και αναλύονται «σε ανθρώπινη γλώσσα» στο παραπάνω κείμενο.

Ένας άμεσος τρόπος για να **περιορίζεται η χρήση** ενός πιστοποιημένου ζεύγους κλειδιών σε συγκεκριμένες εφαρμογές, είναι η 'αναγραφή' -*στο πεδίο «Χρήση Κλειδιού» ('Key Usage') των πιστοποιητικών X.509*- των σχετικών 'τυποποιημένων ενδείξεων' που έχουν προσδιοριστεί από το διεθνές πρότυπο RFC 2459 (X.509 v3 Profile).

Άλλοι περιορισμοί στην χρήση των 'πιστοποιητικών δημοσίων κλειδιών' μπορούν να αναφέρονται στα **όρια στην αξία των συναλλαγών** στις οποίες αυτά επιτρέπεται να χρησιμοποιηθούν. Μάλιστα, νεότερα διεθνή

και ευρωπαϊκά πρότυπα[3], προβλέπουν την 'σύσταση' συγκεκριμένου 'νέου' πεδίου στα πιστοποιητικά τύπου X.509, το οποίο θα χρησιμοποιείται για να εκδηλώσει με τυποποιημένο τρόπο τα συγκεκριμένα όρια που ορίζει η εφαρμοζόμενη 'Πολιτική Πιστοποιητικού'.

ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

Νομική αναγνώριση των ηλεκτρονικών υπογραφών

Διεθνής Νομική Αναγνώριση – Διαφορετικές νομικές προσεγγίσεις

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*» την οποία ακολούθησαν κράτη όπως οι Η.Π.Α., ο Καναδάς, η Μεγ. Βρετανία[4],η Αυστραλία, κ.α. ***(ιδίως κράτη του 'common law')*** 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» σύμφωνα με την οποία είχαν διαμορφώσει την εθνική τους νομοθεσία χώρες όπως η Γερμανία, Ιταλία, Εσθονία, Πολιτεία Utah[5],κ.α.* ***(ιδίως κράτη του 'civil law')*** .

Ευρωπαϊκή Οδηγία (99/93/ΕΚ): Μικτή Προσέγγιση

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, αφενός, η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως '***ηλεκτρονικές υπογραφές***' –που μπορούν να χρησιμοποιηθούν ως 'αποδεικτικά στοιχεία' σε νομικές διαδικασίες (*ά. 5§2 της Οδηγίας, αρχή της μη διακρίσεως*)-, όλα τα: «***δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά***

[3] Συγκεκριμένα τα IETF RFC 3039 και ETSI TS 101862 που αναφέρονται σε 'Qualified Certificate Profile'

[4] *Στο προϊσχύον της σχετικής Ευρωπαϊκής Οδηγίας εθνικό δίκαιο*

[5] *Πριν την έκδοση του Ομοσπονδιακού Νόμου των ΗΠΑ (200) η οποία υιοθετεί την μινιμαλιστική προσέγγιση*

συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (*ά. 2§1 της Οδηγίας*).

Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο 'απλές' (*π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής σε ένα e-mail ή του αριθμού του τηλεφώνου αποστολής σε ένα SMS μήνυμα, κλπ*), ως την πιο 'σύνθετες' (*π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κλπ*), ανεξάρτητα, δηλαδή, από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

- Αφετέρου, (από την κανονιστική πλευρά), η Οδηγία (ά.5§1) διακρίνει ποιοτικά μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών -αποκαλούμενες στη πράξη στην πλειοψηφία των ευρωπαϊκών κρατών ως '***αναγνωρισμένες ηλεκτρονικές υπογραφές'***- στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις 'ιδιόχειρες υπογραφές', όπως οι τελευταίες ορίζονται και ό,τι και αν αποδεικνύουν σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους[6].

Εθνική σχετική νομοθεσία – κείμενα

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.[7]

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό '***Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής***', καθώς και τρεις Κανονισμούς[8]

---

[6] Η προσέγγιση των δύο επιπέδων υιοθετήθηκε επίσης από την ***Μαλαισία, Σιγκαπούρη, κ.ά.***

[7] Σχετικά θέματα για την ηλεκτρονική επικοινωνία μεταξύ των φορέων του Δημοσίου και των πολιτών ρυθμίζονται επίσης στον **«Κανονισμό Επικοινωνίας Δημόσιων Υπηρεσιών» (ΚΕΔΥ).**

[8] Πρόκειται για την απόφαση υπ' αριθμόν 295/63 με τίτλο « Κανονισμός ορισμού φορέων για την διαπίστωση συμμόρφωσης ΑΔΔΥ και ΑΚΜ και προς τα κριτήρια της εθελοντικής διαπίστευσης», την απόφαση 295/64 σχετικά με τον

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.

Ανάλυση βασικών σημείων του ευρωπαϊκού θεσμικού πλαισίου

Πεδίο εφαρμογής της Οδηγίας

Η Οδηγία δεν απαιτεί την εφαρμογή της σε '*κλειστά συστήματα*' (δηλαδή μεταξύ συγκεκριμένου αριθμού συμμετεχόντων) στα οποία η αναγνώριση του κύρους των ηλεκτρονικά υπογεγραμμένων δεδομένων βασίζεται σε 'εθελούσιες συμφωνίες ιδιωτικού δικαίου' σύμφωνα με την αρχή της 'ελευθερίας των συμβάσεων', παρά μόνο στη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών «προς το κοινό». (προοίμιο 16). Επίσης δεν καλύπτει πτυχές που αφορούν τη σύναψη και την ισχύ των συμβάσεων, ούτε θίγει κανόνες & περιορισμούς του εθνικού ή κοινοτικού δικαίου σχετικά με τη χρήση των εγγράφων (άρθρο 1).

Προϋποθέσεις εξομοίωσης ηλεκτρονικής υπογραφής με ιδιόχειρη

Σύμφωνα με την Ευρωπαϊκή Οδηγία (*ά. 5§1*) αλλά και το σχετικό ελληνικό π.δ. (ά. 3§1), οι (αναγνωρισμένες) ηλεκτρονικές υπογραφές που αποκτούν άμεσα την ίδια νομική αξία με τις "παραδοσιακες" ιδιόχειρες υπογραφές, ορίζονται: «οι '***προηγμένες ηλεκτρονικές υπογραφές'*** *που, επιπλέον, βασίζονται σε* ***'αναγνωρισμένο πιστοποιητικό'*** *και δημιουργούνται από* ***'ασφαλή διάταξη δημιουργίας υπογραφής***»'.

Για τις έννοιες αυτές, και από τα δύο νομοθετικά κείμενα, δίνονται οι εξής ορισμοί:

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

«Έλεγχο συμμόρφωσης ΑΔΔΥ και ΑΚΜ» και την απόφαση 295/63 η οποία αποτελεί τον «Κανονισμό για την εθελοντική διαπίστευση των ΠΥΠ».

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

- 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 Παράρτ. ΙΙΙ*.

Ελεύθερη Παροχή Υπηρεσιών Πιστοποίησης και Εθελοντική Διαπίστευση

Η Οδηγία ορίζει ως 'Παρόχους Υπηρεσιών Πιστοποίησης' όχι μόνο αυτούς που εκδίδουν «ηλεκτρονικά πιστοποιητικά δημοσίων κλειδιών» ('αναγνωρισμένα' ή όχι), αλλά και όλους όσους παρέχουν υπηρεσίες 'σχετικές' με την ηλεκτρονική υπογραφή, όπως υπηρεσίες (ηλεκτρονικής) χρονοσήμανσης, καταλόγου, καταχώρησης, αλλά και σχετικές συμβουλευτικές υπηρεσίες! (*άρθρο 2, περ. 11, και Προοίμιο 9*).

Η **Οδηγία** προβλέπει επίσης, την ελεύθερη παροχή υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, *απαγορεύοντας* οποιοδήποτε σύστημα αδειοδότησης της λειτουργίας των Παρόχων Υπηρεσιών Πιστοποίησης (εφεξής, ΠΥΠ). Προσδιορίζει, όμως τις προϋποθέσεις λειτουργίας (Παράρτημα ΙΙ), την ευθύνη (ά. 6) και την επιτήρηση από εθνικούς φορείς (ά. 3§3) των ΠΥΠ που εκδίδουν '***αναγνωρισμένα πιστοποιητικά προς το κοινό***'.

Παράλληλα προβλέπεται (ά. 3§2) η συγκρότηση μηχανισμών '***Εθελοντικής Διαπίστευσης***' των ΠΥΠ, από δημόσιους ή/και από ιδιωτικούς φορείς, που αποσκοπούν στην παροχή '*βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης'*. Οι φορείς αυτοί πρέπει να θέτουν αντικειμενικούς και διαφανείς κανόνες -οι οποίοι δεν οδηγούν σε περιορισμό στον αριθμό των διαπιστευμένων ΠΥΠ-, και να ελέγχουν την τήρηση των κανόνων αυτών, καθορίζοντας συγκεκριμένα δικαιώματα και υποχρεώσεις στους ΠΥΠ που διαπιστεύονται κάτω από το συγκεκριμένο μηχανισμό.

Υποχρεώσεις και Ευθύνη των Π.Υ.Π.

Οι ΠΥΠ που δεν εκδίδουν «αναγνωρισμένα πιστοποιητικά» (*παρά μόνο απλά 'πιστοποιητικά δημοσίων κλειδιών' των υπογραφόντων*), υπόκεινται στις «γενικές διατάξεις περί ευθύνης», στις διατάξεις περί «προστασίας του καταναλωτή» και «προστασίας των προσωπικών δεδομένων» καθώς και σε τυχόν άλλες ειδικότερες σχετικές διατάξεις από το εθνικό δίκαιο του κράτους-μέλους που είναι εγκατεστημένοι,. Σε γενικές γραμμές, οι συγκεκριμένοι ΠΥΠ δεν υποχρεούνται -άμεσα τουλάχιστον- στην τήρηση κάποιων συγκεκριμένων προδιαγραφών στα προϊόντα και τις υπηρεσίες τους, εκτός από αυτών που ο ίδιος ο ΠΥΠ αναλαμβάνει

συμβατικά έναντι των συνδρομητών-πελατών του (Subscriber Agreement) και έναντι των τρίτων-αποδεκτών των πιστοποιητικών του (Relying Party Agreement) και που τυχόν δημοσιοποιεί για την τεκμηρίωση των υπηρεσιών του (με κείμενα όπως Certification Practice Statement, Certificate Policies, PKI Disclosure Statement, κ.ά.)

Όσον αφορά, όμως, τους ΠΥΠ που εκδίδουν «αναγνωρισμένα πιστοποιητικά», εκτός της ισχύος των παραπάνω, η Οδηγία προβλέπει επιπρόσθετα την υποχρέωση συμμόρφωσης με δώδεκα όρους που αναφέρονται στο Παράρτημα ΙΙ καθώς και **συγκεκριμένες ευθύνες τους** (ά. 6) έναντι κάθε τρίτου που βασίζεται '*εύλογα'* στα «αναγνωρισμένα πιστοποιητικά» τους!

Ειδικότερα, οι όροι του Παραρτήματος ΙΙ αναφέρονται σε **αυστηρές απαιτήσεις** οικονομικής και τεχνολογικής αξιοπιστίας, σε υποχρεώσεις παροχής ασφαλών υπηρεσιών 'καταλόγου' και 'ανάκλησης' των πιστοποιητικών τους, καθώς και ενημέρωσης κάθε ενδιαφερόμενου τρίτου για τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης των πιστοποιητικών τους, στην επαλήθευση της ταυτότητας των πιστοποιούμενων υποκειμένων τους και στην διατήρηση των σχετικών αποδεικτικών στοιχείων για 'κατάλληλη χρονική περίοδο'[9], στην τήρηση απορρήτου κατά την περίπτωση παραγωγής ιδιωτικών κλειδιών ('*δεδομένων δημιουργίας υπογραφής'*) των 'συνδρομητών' τους και σε πολλές ακόμη διαχειριστικές και διοικητικές υποχρεώσεις του ΠΥΠ[10].

Περαιτέρω, οι **ιδιαίτερες ευθύνες** που αναλαμβάνει εκ του νόμου (*άρθρο 6 της Οδηγίας)* ο ΠΥΠ που εκδίδει «αναγνωρισμένα πιστοποιητικά προς το κοινό» αφορούν:

- την ακρίβεια όλων των στοιχείων που αναφέρονται στο αναγνωρισμένο πιστοποιητικό κατά την στιγμή της έκδοσής του[11], καθώς και την πληρότητά τους, σύμφωνα με τα οριζόμενα στο Παράρτημα Ι,
- την διαβεβαίωση ότι ο υπογράφων που ταυτοποιείται στο 'αναγνωρισμένο πιστοποιητικό', ήταν κάτοχος, –τουλάχιστον κατά την στιγμή της έκδοσης του πιστοποιητικού-, των 'δεδομένων δημιουργίας υπογραφής' (=*ιδιωτικό κλειδί*) που αντιστοιχούν στα 'δεδομένα επαλήθευσης υπογραφής' (=*δημόσιο κλειδί*) που αναφέρεται στο πιστοποιητικό, και

[9] Η οποία για την Ελλάδα καθορίσθηκε σε **30 χρόνια**, σύμφωνα με την ***περ. θ΄*** του Παραρτήματος ΙΙ του π.δ. 150/2001 και το ***άρθρο 7§2*** της παραπάνω Απόφασης ('*Κ.Π.Υ.Π.Η.Υ*') της ΕΕΤΤ!

[10] Πολλές από τις απαιτήσεις του Παραρτήματος ΙΙ εξειδικεύονται στα πρότυπα CEN CWA 14167-1 & ETSI TS 101456.

[11] Αν αργότερα αυτά τροποποιηθούν και ο ΠΥΠ δεν λάβει γνώση για αυτό, τότε δεν ευθύνεται αυτός, αλλά το 'υποκείμενο' της πιστοποίησης (=ο κάτοχος των δεδομένων δημιουργίας υπογραφής) που οφείλει να ενημερώσει τον ΠΥΠ για την συγκεκριμένη αλλαγή, ώστε να 'ανακληθεί' το σχετικό πιστοποιητικό!

- την διαβεβαίωση, εφόσον παράγει και παρέχει ο ίδιος ο ΠΥΠ το ιδιωτικό κλειδί στον 'συνδρομητή' του, ότι αυτό μπορεί να χρησιμοποιηθεί 'συμπληρωματικά' με το δημόσιο κλειδί που αναγράφεται στο σχετικό πιστοποιητικό που του εκδίδει.

Η Οδηγία προβλέπει ακόμη και το δικαίωμα του ΠΥΠ-Εκδότη «αναγνωρισμένων πιστοποιητικών» να περιορίζει 'συμβατικά' την παραπάνω ευθύνη του από την χρήση των πιστοποιητικών που εκδίδει, με την αναγραφή '***ορίων στις οικονομικές συναλλαγές***'[12] για τις οποίες αυτά επιτρέπεται να χρησιμοποιηθούν, *ή/και* με κάθε άλλο '***περιορισμό στην χρήση***' των πιστοποιητικών που ρητώς καθορίζει ο ΠΥΠ. Επίσης, ο ΠΥΠ απαλλάσσεται από κάθε ευθύνη του αν αποδείξει ότι ***δεν έπραξε*** '***αμελώς***'!

Περιεχόμενο των «αναγνωρισμένων πιστοποιητικών»

Η Οδηγία ορίζει ότι τα «**αναγνωρισμένα πιστοποιητικά**» πρέπει να περιλαμβάνουν -*στα σχετικώς προβλεπόμενα πεδία τους*- τουλάχιστον τα παρακάτω στοιχεία:

« ***α)*** *ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό,*

β) *τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος,*

γ) *το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο,*

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

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

στ) *ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού,*

ζ) *τον κωδικό ταυτοποίησης του πιστοποιητικού,*

η) *την προηγμένη ηλεκτρονική υπογραφή του ΠΥΠ που το εκδίδει,*

θ) *τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και*

ι) *τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί* ».

Προϊόντα ηλεκτρονικής υπογραφής και «Διαπίστωση» (συμμόρφωσης)

Σύμφωνα με τον ορισμό που δίνεται στο άρθρο 2§12, «προϊόν ηλεκτρονικής υπογραφής» θεωρείται κάθε υλικό ή λογισμικό ή συναφή στοιχεία, τα οποία προορίζονται:

[12] Βλ. το πρότυπο **TS 101 862: 'Qualified Certificate Profile'** του ευρωπαϊκού οργανισμού **ETSI**, καθώς και το ομώνυμο **RFC 3039** του διεθνούς οργανισμού **IETF** σχετικά με τον τρόπο αναγραφής στα αναγνωρισμένα πιστοποιητικά των διαφόρων 'δηλώσεων' ('qcStatements') που προβλέπονται από την Οδηγία,.

- Είτε για χρήση από τον ΠΥΠ σχετικά με την παροχή των σχετικών υπηρεσιών του (π.χ. κρυπτογραφικές μονάδες για την δημιουργία κρυπτογραφικών κλειδιών),
- Είτε για τη φιλοξενία και ενεργοποίηση των ιδιωτικών κλειδιών και τη δημιουργία της ηλεκτρονικής υπογραφής («*διατάξεις δημιουργίας υπογραφής*»),
- Είτε, τέλος, για την αυτόματη επαλήθευση μιας ηλεκτρονικής υπογραφής («*διατάξεις επαλήθευσης υπογραφής*»).

Ειδικότερα για την έκδοση «αναγνωρισμένων πιστοποιητικών» και τη δημιουργία «αναγνωρισμένης ηλεκτρονικής υπογραφής», η Οδηγία θέτει κάποιες **βασικές απαιτήσεις ασφάλειας** στα παραπάνω προϊόντα, και συγκεκριμένα αναφέρεται σε «ασφαλείς κρυπτογραφικές μονάδες» (Παράρτημα ΙΙ περ. στ΄), καθώς και σε «ασφαλείς διατάξεις δημιουργίας υπογραφής» (Παράρτημα ΙΙΙ), ενώ για τις «ασφαλείς διατάξεις επαλήθευσης υπογραφής» περιορίζεται μόνο σε 'συστάσεις' (Παράρτημα IV).

Για την συμμόρφωση των '*προϊόντων ηλεκτρονικών υπογραφών*' με τις συγκεκριμένες απαιτήσεις ασφάλειας βάσει σχετικών 'γενικώς αναγνωρισμένων προτύπων', προβλέπεται από την Οδηγία (άρθρο 3§2) διαδικασία '***Διαπίστωσης***' από σχετικούς αρμόδιους φορείς.

Ιδιαίτερες απαιτήσεις για 'ασφαλείς διατάξεις δημιουργίας υπογραφής'

Η χρήση '***ασφαλούς διάταξης δημιουργίας υπογραφής***' (*α.δ.δ.υ.*) θεωρείται αναγκαία για την δημιουργία '***αναγνωρισμένης ηλεκτρονικής υπογραφής'***. Ως τέτοια προσδιορίζεται (*Παράρτημα ΙΙΙ Οδηγίας*) 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' ουσία, 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 (*αναγνωριζεται δηλαδή η αρχή '**What You See Is What You Sign**' ή '**WYSIWYS**'*).

Συστάσεις της Οδηγίας για 'ασφαλείς διατάξεις επαλήθευσης υπογραφής'

Για τη διαδικασία επαλήθευσης της ηλεκτρονικής υπογραφής, η Οδηγία προβαίνει σε «***Συστάσεις***», σύμφωνα με τις οποίες, μια «ασφαλής διάταξη επαλήθευσης υπογραφής» θα πρέπει να διασφαλίζει με εύλογη βεβαιότητα ότι:

« ***α)*** *τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα,*

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

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

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

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

στ) *η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς, και*

ζ) *μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.*»

Επιτροπή άρθρου 9 και Αναθεώρηση Οδηγίας

Η Οδηγία προβλέπει, τέλος, την σύσταση ειδικής «**Επιτροπής Ηλεκτρονικής Υπογραφής**» (*άρθρο 9*) η οποία είναι αρμόδια να 'διευκρινίζει' τις λεπτομέρειες των όποιων κριτηρίων ή/και των προτύπων που σχετίζονται με την εφαρμογή της (*άρθρο 10*), καθώς και να επανεξετάζει την εφαρμογή της Οδηγίας κάθε τρία

χρόνια**,** με σκοπό την αξιολόγηση της «κτηθείσας εμπειρίας από την εφαρμογή της» και την σύνταξη σχετικών προτάσεων σε περίπτωση που τυχόν κριθεί αναγκαία η αναθεώρησή της (*άρθρο 12*)[13].

ΜΕΡΟΣ ΙΙΙ: ΔΙΕΡΕΥΝΗΣΗ-ΑΠΟΤΥΠΩΣΗ ΥΦΙΣΤΑΜΕΝΗΣ ΚΑΤΑΣΤΑΣΗΣ

ΧΡΗΣΗ η-ΥΠΟΓΡΑΦΩΝ ΣΕ ΔΙΕΘΝΕΣ ΕΠΙΠΕΔΟ

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 από EDI*
- *Ηλεκτρονικές δημόσιες προμήθειες*
- *Ηλεκτρονική ψηφοφορία*
- *Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες EuroPay, MasterCard & VISA μέσω του κοινού πρωτοκόλλου τους 'EMV')*
- *Ηλεκτρονικά 'διαβατήρια' και ηλεκτρονικές 'ταυτότητες' (γενικής ή ειδικής χρήσης –π.χ. 'ναυτικές διεθνείς ταυτότητες') που συνήθως φέρουν ενσωματωμένα και κάποια 'βιομετρικά στοιχεία' (φωτογραφία, δακτυλικά αποτυπώματα, κ.λ.π.) 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.

[13] Η σχετική μελέτη που εκδόθηκε πρόσφατα από το Πανεπιστήμιο Leuven (ICRI) και την νομική εταιρία «Landwell» (Βελγίου) για λογαριασμό της Επιτροπής, απεφάνθη ότι «*δεν διακρίνονται ιδιαίτεροι λόγοι για αναθεώρηση της υφιστάμενης Οδηγίας, και ότι απλώς αρκεί κάποια 'επανερμηνεία' συγκεκριμένων σημείων της, λαμβάνοντας υπ' όψιν την (παν)ευρωπαϊκή της διάσταση*».

ΕΥΡΩΠΑΪΚΕΣ ΕΦΑΡΜΟΓΕΣ η-ΥΠΟΓΡΑΦΩΝ & ΣΧΕΤΙΚΑ PROJECTS

Ένας πρώτος σημαντικός τομέας εφαρμογής των ηλεκτρονικών υπογραφών είναι τα **ηλεκτρονικά τιμολόγια**. Σύμφωνα με την Ευρωπαϊκή Οδηγία 115 της 20ης Δεκεμβρίου 2001, η χρησιμοποίηση ηλεκτρονικής υπογραφής ή του τυποποιημένου συστήματος EDI (Electronic Data Interchange) κατά την έκδοση 'ηλεκτρονικών τιμολογίων' (e-invoicing) υποχρεώνει τις αρχές των κρατών μελών να δεχθούν τα εκδιδόμενα ηλεκτρονικά τιμολόγια, ενώ, παράλληλα, διευκολύνει την αρχειοθέτηση και την άμεση ανταλλαγή τους**.**

Οι **ηλεκτρονικές ταυτότητες (ή/και διαβατήρια),** αποτελούν μία άλλη περίπτωση ευρείας εφαρμογής των ηλεκτρονικών υπογραφών, και ήδη έχουν θεσμοθετηθεί ή/και βρίσκονται σε λειτουργία σε αρκετά ευρωπαϊκά κράτη, όπως π.χ. Βέλγιο, Φινλανδία, Ιταλία, Εσθονία, κ.ά. Η κυρίαρχη τάση σ' αυτές είναι η χρήση δύο (ή και τριών) ζευγών κλειδιών και σχετικών πιστοποιητικών, (ένα για 'ταυτοποίηση' και ένα για 'αναγνωρισμένες' ηλεκτρονικές υπογραφές –και πιθανώς και ένα τρίτο για την κρυπτογράφηση δεδομένων). Τα στοιχεία αυτά δημιουργούνται ή τοποθετούνται σε ένα μικροεπεξεργαστή που βρίσκεται σε έναν ασφαλή φορέα όπως για παράδειγμα μία έξυπνη κάρτα. Στην κάρτα αυτή αναγράφονται επίσης και τα στοιχεία του κατόχου και περιλαμβάνεται και η φωτογραφία του, ώστε να διευκολύνεται ο οπτικός έλεγχος. Η ταυτότητα αυτή χρησιμοποιείται όπως κάθε άλλη ταυτότητα από τα κράτη-μέλη. Παραδείγματα αποτελούν η FINeID της Φινλανδίας, η eID στο Βέλγιο, Σουηδία κλπ. Από τα μέλη της Ο.Ε. Ε2 εκφράσθηκαν προβληματισμοί σχετικά με την προστασία των προσωπικών δεδομένων των πολιτών, λόγω της ηλεκτρονικής διαχείρισής τους και με την ενδεχομένως μειωμένη διαλειτουργικότητα ανάμεσα στις τεχνολογίες που χρησιμοποιούνται στα ηλεκτρονικά δελτία ταυτότητας διαφορετικών χωρών.

Σχετική με τις ταυτότητες και τα διαβατήρια είναι η σχεδιαζόμενη (ηλεκτρονική) '***Ευρωπαϊκή Κάρτα Υγείας***' με την οποία ο κάτοχός της θα ταυτοποιείται και θα μπορεί να έχει πρόσβαση στα διαφορετικά συστήματα υγειονομικής περίθαλψης όλων των κρατών-μελών.

Σε πολλά κράτη-μέλη της Ε.Ε. αναπτύσσονται σε εθνικό επίπεδο αρκετές άλλες εφαρμογές σχετικές με τις ηλεκτρονικές υπογραφές. Ενδεικτικά:

- Στην **Ιταλία**, έχοντας ξεκινήσει την θεσμοθέτηση της χρήσης των ηλεκτρονικών υπογραφών ειδικά για την Δημόσια Διοίκηση από το 1997 υπό την εποπτεία τότε της AIPA (Autorita *per l' Informatica nella Publica Amministrazione*) και πρόσφατα του CNIPA (www.cnpa.it - '*Centro Nationale per l' Informatica nella Publica Amministrazione*) έχουν καταφέρει να έχουν ευρύτατη χρήση και αποδοχή (υπογεγραμμένων) ηλεκτρονικών εγγράφων στις δημόσιες υπηρεσίες τους. Σ' αυτό βοήθησε ο καθορισμός συγκεκριμένου τύπου ηλεκτρονικών

υπογραφών που χρησιμοποιούνται αποκλειστικά για την υπογραφή ηλεκτρονικών έγγραφων (‘Firme Sicure’) και η θέσπιση αυστηρών κανόνων[14] για την διαλειτουργικότητα των σχετικών πιστοποιητικών που εκδίδουν οι 'εγγεγραμμένοι ΠΥΠ' στο μητρώο του CNIPA , γεγονός που οδήγησε και στην ανάπτυξη εφαρμογών λογισμικού για την δημιουργία και επαλήθευση ηλεκτρονικών υπογραφών το οποίο λειτουργεί με τα πιστοποιητικά όλων των ΠΥΠ της Ιταλίας, βάσει των κοινών προδιαγραφών!

- Στην **Γερμανία**, -όπου υπήρχε ‘αυστηρή’ νομοθεσία για την αποδοχή των ηλεκτρονικών υπογραφών από το 1997- προσφέρεται και χρησιμοποιείται από την δημόσια διοίκηση ένας ακόμη πιο ‘βελτιωμένος’ –σε σχέση με τις ‘αναγνωρισμένες ηλεκτρονικές υπογραφές’ του άρθρου 5§1 της Οδηγίας 99/93/ΕΚ- τύπος ηλεκτρονικών υπογραφών (οι αποκαλούμενες ‘***enhanced signatures***’) οι οποίες παρέχονται μόνο από τους ‘**εθελοντικά διαπιστευμένους ΠΥΠ**’ (‘*accredited CAs*) και προβλέπουν την υποχρεωτική χρήση ‘**χρονοσήμανσης’** (timestamping) στα υπογεγραμμένα ηλεκτρονικά έγγραφα, ώστε αυτά να μπορούν να εξετασθούν για την εγκυρότητά τους και μετά από την λήξη του πιστοποιητικού που υποστήριξε την ηλεκτρονική υπογραφή τους. Μάλιστα, η αρμόδια εθνική αρχή ‘*Regulierungsbehφrde fόr Telekommunikation und Post*’ (RegTP / www.regtp.de) έχει προχωρήσει στην ‘**διαπίστωση’** και στην δημοσίευση της συμμόρφωσης συγκεκριμένων ‘***προϊόντων ηλεκτρονικών υπογραφών***’ (*συσκευές/φορείς ιδιωτικών κλειδιών, αυτόνομα ή πρόσθετα προγράμματα (plug-ins) δημιουργίας και επαλήθευσης ηλεκτρονικών υπογραφών, βιβλιοθήκες σχετικών ‘ρουτινών’, αναγνώστες καρτών, κ.λ.π.*) με αυστηρές προδιαγραφές.

- Στην **Εσθονία**, σε συνδυασμό με την ‘ηλεκτρονική ταυτότητα’ που εκδίδεται υποχρεωτικά προς όλους τους πολίτες της και η οποία ενσωματώνει πιστοποιητικά ηλεκτρονικής υπογραφής, έχουν προχωρήσει στο σχεδιασμό ενός ολοκληρωμένου συστήματος ηλεκτρονικής ταυτοποίησης και υπογραφής εγγράφων (επονομαζόμενο ‘DigiDoc’), τόσο για χρήση του μεταξύ των υπαλλήλων της Δημόσιας Διοίκησης, όσο και μεταξύ αυτών και των πολιτών. Χαρακτηριστικά της εφαρμογής τους είναι η δυνατότητα ταυτόχρονης ενσωμάτωσης πληροφοριών επαλήθευσης των πιστοποιητικών και χρονοσήμανσης της υπογραφής στο υπογεγραμμένο έγγραφο*, (όπως στις ‘**enchanced signatures**’ της Γερμανίας*), καθώς και η απόδοση μιας σταθερής, αλλά ‘εικονικής’ διεύθυνσης ηλεκτρονικού ταχυδρομείου, για κάθε πολίτη και δημόσιο υπάλληλο! Με την χρήση αυτής της ‘εικονικής’ διεύθυνσης (*της μορφής **Name.Surname.XXXX@eesti.ee**, όπου XXX=τυχαίος αριθμός!*) μπορούν να στέλνουν και να λαμβάνουν υπογεγραμμένα και κρυπτογραφημένα μηνύματα από την εκάστοτε πραγματική διεύθυνση ηλεκτρονικού ταχυδρομείου τους την οποία ‘διασύνδεουν με αυτή! (περισσότερες πληροφορίες στο κείμενο ‘*The Estonian ID Card andDigital Signature Concept*’ που δημοσιεύεται στις ιστοσελίδες της Ε2).

[14] «*Linee guida per l'interoperabilita tra i certificatori iscritti nell' elenco pubblico*» CIRCOLARE n. AIPA/CR/24, 19 giugno 2000.

- Στη **Γαλλία**, αναφέρθηκε ότι έχει ολοκληρωθεί εφαρμογή με την οποία οι δικηγόροι μπορούν ήδη να καταθέτουν ηλεκτρονικά κάποιους τύπους δικογράφων προς την υπηρεσίες συγκεκριμένων δικαστηρίων, με την χρήση της ηλεκτρονικής υπογραφής τους.

ΣΕ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ

Πάροχοι Υπηρεσιών Πιστοποίησης στην Ελλάδα

Η **ΑΣΥΚ Α.Ε**., μέλος του Ομίλου Ε.Χ.Α.Ε. και υπεύθυνη για την ανάπτυξη και ολοκληρωμένη τεχνική διαχείριση, λειτουργία και υποστήριξη των υποδομών πληροφορικής και επικοινωνιών του Χρηματιστηρίου Αθηνών (ΧΑ) και του Ομίλου ΕΧΑΕ γενικότερα, δημιούργησε και τεκμηρίωσε δική της Υποδομή Δημοσίου Κλειδιού (PKI), πρωτίστως για να καλύψει τις ανάγκες του Χ.Α. για ασφαλή και νομικά έγκυρη ηλεκτρονική επικοινωνία-αλληλογραφία με τις εισηγμένες σ' αυτό εταιρίες, αντικαθιστώντας τα "συμβατικά έγγραφα" με αντίστοιχα "ηλεκτρονικά", τα οποία αποστέλλονται ψηφιακά υπογεγραμμένα μέσω του συστήματος "ΕΡΜΗΣ" (H.E.R.ME.S. - Hellenic Exchanges Remote MEssaging Services). Για την υποστήριξη της εφαρμογής αυτής η ΑΣΥΚ λειτουργεί ως ΠΥΠ, εκδίδοντας σε εξουσιοδοτημένα φυσικά πρόσωπα μία 'ψηφιακή ταυτότητα' (τύπου 'SMART-SIGN' της ΑΣΥΚ) η οποία περιέχει δύο πιστοποιητικά (ένα 'αναγνωρισμένο' και ένα για 'ταυτοποίηση'/ 'αυθεντικότητα') που αντιστοιχούν σε δύο διαφορετικά κλειδιά και τα οποία παραδίδονται στον συνδρομητή υποχρεωτικά σε μια εξατομικευμένη –για αυτόν- έξυπνη κάρτα. Παράλληλα εκδίδει και πιστοποιητικά ταυτοποίησης & SSL επικοινωνίας (TRUST-SERVER) για εξυπηρετητές διαδικτύου (web servers). Ο σχεδιασμός της υποδομής PKI και η τεκμηρίωσή των υπηρεσιών της ΑΣΥΚ ως ΠΥΠ έγιναν σύμφωνα με τα σχετικά διεθνή και κυρίως τα ευρωπαϊκά standards, με σκοπό την όσο δυνατόν μεγαλύτερη εγκυρότητα και διαλειτουργικότητα των υπηρεσιών της, προσδοκώντας την περαιτέρω εμπορική εκμετάλλευσή τους και για άλλες σχετικές εφαρμογές.

Η **ADACOM A.E.,** μέλος του Ομίλου IDEAL, παρέχει υπηρεσίες ψηφιακής πιστοποίησης και γενικότερα ασφάλειας πληροφοριακών συστημάτων που έχουν ως βάση την τεχνολογική πλατφόρμα της VeriSign (leader παγκοσμίως της αγοράς των υπηρεσιών Δημοσίου Κλειδιού). Έχοντας πραγματοποιήσει τη μεγαλύτερη σε μέγεθος επένδυση στα Βαλκάνια για τη δημιουργία Υποδομής Δημοσίου Κλειδιού (PKI) η ADACOM είναι Πάροχος Υπηρεσιών Πιστοποίησης προς τελικούς χρήστες, προς νομικά πρόσωπα τα οποία επιθυμούν να λειτουργήσουν ως Αρχές Πιστοποίησης, καθώς και προς εξυπηρετητές (servers) και δικτυακές συσκευές. Οι υπηρεσίες αυτές υλοποιούνται είτε με την χρησιμοποίηση ιδιωτικής ιεραρχίας της ADACOM, η οποία χρησιμοποιείται για την έκδοση 'αναγνωρισμένων πιστοποιητικών' σύμφωνα με την Ευρωπαϊκή Οδηγία, είτε είναι ενταγμένες στη δημόσια ιεραρχία της VeriSign η οποία εξασφαλίζει τη μεγαλύτερη δυνατή αναγνωρισιμότητα από τους web browsers (MSIE, Netscape). Παράλληλα παρέχεται ένα σύνολο σχετικών υπηρεσιών όπως Διαχείριση Ιδιωτικών Κλειδιών Κρυπτογράφησης, Χρονοσήμανσης, Περιαγωγής, και

O.C.S.P. (On line Certificate Status Protocol). Η εταιρεία έχει υλοποιήσει ποικίλα έργα PKI τόσο στην Ελλάδα όσο και στο εξωτερικό (π.χ. Ρουμανία), ακολουθώντας τα σημαντικότερα σχετικά ευρωπαϊκά και διεθνή πρότυπα. Η ADACOM είναι πιστοποιημένη κατά ISO 9002/94 ενώ ταυτόχρονα βρίσκεται σε διαδικασία διαπίστευσής της σύμφωνα με το πρότυπο ETSI TS 101 456 (Policy Requirements for Certification Authorities Issuing Qualified Certificates) από διεθνή ελεγκτικό οργανισμό (KPMG B.V.)

Η **Eurobank/EFG e-Solutions** δημιουργεί και υποστηρίζει υπηρεσίες e- και m- banking, οι οποίες καλύπτουν ένα ευρύ φάσμα τραπεζικών υπηρεσιών, όπως από ανάγκες απλής ενημέρωσης για τις κινήσεις και το υπόλοιπο των λογαριασμών, έως και την πληρωμή καρτών, πάγιες ή περιοδικές εντολές πληρωμής και εμβάσματα. Η έκδοση πιστοποιητικών ταυτοποίησης από την Eurobank παρέχει την δυνατότητα για εξελιγμένο έλεγχο της πρόσβασης των χρηστών στο σύστημα και τις ηλεκτρονικές υπηρεσίες του Ομίλου (user authentication /authorization), ενώ εισάγεται η δυνατότητα της χρήσης ηλεκτρονικής υπογραφής ως απόδειξης της βούλησης για την διενέργεια κρίσιμων συναλλαγών (λειτουργία 'non repudiation'). Η υποδομή της Eurobank, αν και έχει την δυνατότητα, δεν εκδίδει 'αναγνωρισμένα πιστοποιητικά', μιας και η χρήση των εκδιδόμενων πιστοποιητικών προορίζεται προς το παρόν αποκλειστικά σε 'κλειστές εφαρμογές' για τις οποίες δεν εφαρμόζεται η Οδηγία 99/93/ΕΚ (η αποδοχή της χρήσης ηλεκτρονικών υπογραφών στηρίζεται σε συμβατικούς όρους). Παρόλα αυτά, η έκδοση των πιστοποιητικών συμμορφώνεται *–βάσει και εξωτερικών ελέγχων από τρίτους φορείς*- με το πρότυπο ETSI TS 102 042 ('*Normalized Certificate Policy + Secure Device'*), το οποίο δεν έχει ουσιαστικές διαφορές από τις απαιτήσεις ασφαλείας του αντίστοιχου προτύπου του ETSI για την έκδοση των 'αναγνωρισμένων πιστοποιητικών' (TS 101 456 – '*Qualified Certificate Policy + Secure Signature Creation Device'*).

Το **ΕΒΕΑ** (Εμπορικό και Βιομηχανικό Επιμελητήριο Αθηνών) έχει δημιουργήσει και λειτουργεί δική του υποδομή PKI με σκοπό να παρέχει σχετικές υπηρεσίες και να εκδίδει ηλεκτρονικά πιστοποιητικά δημοσίων κλειδιών στα μέλη του. Προς το παρόν, η παροχή των υπηρεσιών ψηφιακής πιστοποίησης βρίσκεται ακόμα σε πιλοτικό και δοκιμαστικό στάδιο.

Επίσης, στην Ελλάδα δραστηριοποιούνται ως ΠΥΠ (και *περιλαμβάνονται στο σχετικό επίσημο Μητρώο ΠΥΠ της ΕΕΤΤ) και οι εταιρίες* **SPACE HELLAS** και **Delta-Singular.**

Άλλες εταιρίες με συναφή δραστηριότητα που συμμετέχουν στην ΟΕ 'Ε2'

Η **INTRACOM** δεν διαθέτει δική της υποδομή PKI και δεν παρέχει υπηρεσίες πιστοποίησης. Είναι όμως προμηθευτής έξυπνων καρτών για πολλές εφαρμογές (τηλεκάρτες, κάρτες προπληρωμένων μονάδων, κ.λ.π.), οι οποίες μπορεί να υποστηρίζουν ταυτόχρονα τα 'δεδομένα δημιουργίας ηλεκτρονικής υπογραφής' μαζί με άλλες εφαρμογές, όπως π.χ. ηλεκτρονικό πορτοφόλι, χρησιμοποιώντας multi application operation systems.

Η **MELLON Technologies** ασχολείται με συστήματα αυτοματισμού και ασφάλειας (φυσικής και τεχνολογικής) σε μεγάλες υπηρεσίες και οργανισμούς, ιδίως του Τραπεζικού τομέα. Σε σχέση με τις ηλεκτρονικές υπογραφές, η MELLON TECHNOLOGIES αντιπροσωπεύει στην Ελλάδα σχετικά προϊόντα γνωστών διεθνών οίκων, όπως έξυπνες κάρτες της SchlumbergerSema, αναγνώστες έξυπνων καρτών της Towitoko, λογισμικό διαχείρισης υποδομής PKI της Nexus/Smart-Trust, κ.ά.

Η **UNISYSTEMS**, ως integrator μηχανογραφικών λύσεων σε μεγάλους ιδιωτικούς και δημόσιους οργανισμούς, ενσωματώνει δυνατότητες ηλεκτρονικής υπογραφής και πιστοποίησης στις εφαρμογές που αναπτύσσει. Ένα τέτοιο έργο, το οποίο έχει αναλάβει ως ανάδοχος, είναι και το 'Ηλεκτρονικό Ποινικό Μητρώο του Υπουργείου Δικαιοσύνης το οποίο περιλαμβάνει την δημιουργία και χρήση Υποδομής Δημοσίου Κλειδιού.

Η **Ubizen** εταιρία με έδρα στο Βέλγιο, είναι πάροχος υπηρεσιών ασφάλειας με έμφαση στους τομείς Firewalls, intrusion detection systems, διαχείριση πιστοποιητικών και συμβουλευτικές υπηρεσίες. Η Ubizen παρέχει υπηρεσίες μεταξύ άλλων σε μεγάλο αριθμό χρηματοπιστωτικών και κυβερνητικών οργανισμών. Στις ηλεκτρονικές ταυτότητες η Ubizen είναι πάροχος υπηρεσιών πιστοποίησης στο σχέδιο των ηλεκτρονικών δελτίων ταυτότητας στο Βέλγιο και προσφέρει υπηρεσίες σε σχέδια δημόσιου τομέα σε χώρες όπως η Ολλανδία, Βουλγαρία, Λουξεμβούργο κ.λ.π.

Η **Expertnet** παρέχει συγκεκριμένες λύσεις στις απαιτήσεις ασφάλειας των εφαρμογών με τη χρήση προηγμένης τεχνολογίας 'XML υπογραφών' (συμβατές με το ευρωπαϊκό πρότυπο 'XAdES' – ETSI TS 101 933) που ενσωματώνουν διαχείριση σημαντικών στοιχείων ασφάλειας, όπως χρονοσημάνσεις και πληροφορίες ανάκλησης πιστοποιητικών. Παράλληλα διαθέτει ολοκληρωμένες εφαρμογές σε σχετικούς τομείς όπως τα ηλεκτρονικά τιμολόγια (e-invoices / Οδηγία 01/115/ΕΕ) και τα 'ηλεκτρονικά εισιτήρια' (που θα χρησιμοποιούνται κυρίως από το φορητό ' τηλέφωνο' τρίτης γενιάς). Άλλο σχετικό προϊόν που παρέχεται από την Expernet είναι η αυτόνομη εφαρμογή 'File Signer' για την ηλεκτρονική υπογραφή και επαλήθευση των ψηφιακών δεδομένων, με την οποία ελέγχεται αυτόματα η εγκυρότητα των χρησιμοποιούμενων πιστοποιητικών.

Η **OMNIS-Hellas** αντιπροσωπεύει την πλατφόρμα της Cryptomathic η οποία συνεργάζεται με κινητά τηλέφωνα 2.5G/GPRS-10 και 3G/UMTS τα οποία φέρουν στην SIM card τους ψηφιακή υπογραφή τύπου PKI και η οποία ήδη λειτουργεί στην πράξη σε εφαρμογές m-Payments της BeamTrust σε Σκανδιναβικές χώρες. Μάλιστα η Cryptomathic έχει αναπτύξει έναν εξελιγμένο κρυπτογραφικό αλγόριθμο "Ελλειπτικής Κρυπτογράφησης" ο οποίος διευκολύνει την επεξεργασία των δεδομένων και την ψηφιακή υπογραφή τους μέσα από τα δίκτυα κινητής τηλεφωνίας. Παράλληλα, η Cryptomathic έχει αναπτύξει μια ειδική μέθοδο για την εφαρμογή προηγμένων ηλεκτρονικών υπογραφών, τον Cryptomathic Signer, ο οποίος χαρακτηρίζεται από την

χρησιμοποίηση ενός κεντρικού εξυπηρετητή (signature server) για την αποθήκευση και ενεργοποίηση των ιδιωτικών κλειδιών των χρηστών

Το **Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών** (**ΕΑΙΤΥ**), είναι ΝΠΙΔ μη κερδοσκοπικού χαρακτήρα εποπτευόμενο από το Υπ. Εθνικής Παιδείας & Θρησκευμάτων και από το 1995 παρέχει υπηρεσίες τεχνικού και επιστημονικού συμβούλου σε Υπουργεία και φορείς του δημοσίου τομέα της χώρας. Στα πλαίσια αυτά, το ΕΑΙΤΥ παρέχει σήμερα, μεταξύ άλλων, υπηρεσίες τεχνικού συμβούλου σε θέματα πληροφορικής στο Υπουργείου Δικαιοσύνης, στα οποία περιλαμβάνεται και το έργο του 'Ηλεκτρονικού Ποινικού Μητρώου"

Σχετικά εθνικά έργα και σχεδιαζόμενες εφαρμογές

Το Υπουργείο Δικαιοσύνης στα πλαίσια της Μηχανοργάνωσης του Ποινικού Μητρώου και της δημιουργίας μιας κεντρικής βάσης δεδομένων, προβαίνει στην εγκατάσταση μιας αυτόνομης Υποδομής Δημόσιου Κλειδιού (PKI) και την έκδοση ψηφιακών πιστοποιητικών τα οποία θα χρησιμοποιούνται για την εξουσιοδοτημένη πρόσβαση στην 'Κεντρική Βάση Ποινικού Μητρώου' και την ενημέρωσή της, στην 'αυθεντικοποίηση' των εκδιδόμενων ηλεκτρονικών εγγράφων (ατομικών βεβαιώσεων ποινικής κατάστασης) και στην ασφαλή και εμπιστευτική μεταβίβασή τους μεταξύ των αρμοδίων φορέων (κρυπτογράφηση).

Το Εθνικό Τυπογραφείο έχει ήδη προκηρύξει διαγωνισμό για την αναβάθμιση και τον αυτοματισμό της παραγωγικής διαδικασίας του (έκδοση ΦΕΚ και άλλων εντύπων του Δημοσίου) το οποίο ήδη προβλέπει στις προδιαγραφές του την 'συμβατότητα' του νέου συστήματος με τις ηλεκτρονικές υπογραφές της υποδομής δημοσίου κλειδιού (PKI) του Δημοσίου που προβλέπει το Σύζευξις.

Επίσης έχουν αναφερθεί και άλλα έργα του ευρύτερου Δημοσίου Τομέα που σχετίζονται ή προβλέπουν ηλεκτρονικές υπογραφές, όπως το έργο για τα **e-Σήματα** του Υπουργείου Ανάπτυξης, το **Police On Line** του Υπουργείου Δημόσιας Τάξης, η σχεδιαζόμενη '**κάρτα του Πολίτη'** (ηλεκτρονική ταυτότητα?) και το **Σύζευξις** (Υποέργο 9) του ΥΠΕΣΔΔΑ, κ.ά.

ΜΕΡΟΣ IV: ΔΙΑΠΙΣΤΩΣΕΙΣ & ΣΥΜΠΕΡΑΣΜΑΤΑ

Η γενική διαπίστωση για τις ηλεκτρονικές υπογραφές και τα ηλεκτρονικά πιστοποιητικά, είναι ότι, παρά την μεγάλη τους χρησιμότητα και την σχετική ανάγκη της αγοράς για ασφάλεια στις συναλλαγές, παρατηρείται ακόμη σήμερα μια 'δυστοκία' στην ανάπτυξη ευρείας χρήσης σχετικών εφαρμογών που να τις χρησιμοποιούν. Και αυτό παρατηρείται όχι μόνο στην Ελλάδα, αλλά και σε ολόκληρη την Ευρώπη (τουλάχιστον όσον αφορά την έκδοση '***πανευρωπαϊκώς αναγνωρισμένων ηλεκτρονικών υπογραφών***'), παρά τα 4 και πλέον χρόνια από την έκδοση της Οδηγίας και την πραγματοποιηθείσα -έως τώρα- σχετική ευρωπαϊκή προτυποποίηση στα πλαίσια του EESSI.

Έτσι, προσπάθησα να εντοπίσω και να καταγράψω αναλύσεις σε επιμέρους ζητήματα που αποτελούν ή δημιουργούν τεχνικά, νομικά, ή/και πρακτικά εμπόδια κατά τον σχεδιασμό 'εφαρμογών ηλεκτρονικών υπογραφών' καθώς και τις προτάσεις για πιθανές λύσεις ή/και πρωτοβουλίες για την υπερπήδησή τους που ήδη υπάρχουν. Τα βασικότερα θέματα στα οποία επικεντρώθηκα διακρίνονται στις παρακάτω 'θεματικές ενότητες':

ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΚΗΣ ΜΕΘΟΔΟΥ

Δυνατότητα πολλών διαφορετικών χρήσεων των ίδιων κλειδιών – Χρήση πεδίου 'Key Usage'

Διαπιστώθηκε ότι ένα 'ζεύγος κρυπτογραφικών κλειδιών' μπορεί πρακτικά να χρησιμοποιηθεί από τον κάτοχό του σε πολύ διαφορετικές μεταξύ τους εφαρμογές. Μεταξύ αυτών περιλαμβάνονται:

- οι '***αναγνωρισμένες ηλεκτρονικές υπογραφές***' με σκοπό τη 'μη αποκήρυξη' (*non Repudiation*) δήλωσης ή εκφρασμένης βούλησης,
- οι '***υπογραφές ταυτοποίησης***' για την απλή επίδειξη του σχετικού πιστοποιητικού που περιέχει τις πληροφορίες σχετικά με την ταυτότητα του υπογράφοντα (*client ή/και server identification*),
- οι '***υπογραφές αυθεντικότητας***' διακινούμενων δεδομένων (*π.χ. ασφαλές η-ταχυδρομείο*),
- η απλή '***κρυπτογράφηση δεδομένων***' ή άλλων κρυπτογραφικών κλειδιών,
- καθώς και **άλλες ειδικότερες χρήσεις** (π.χ. *ταυτοποίηση server, υπογραφή κώδικα, υπογραφή πιστοποιητικών και CRL, κά*)

Η παράλληλη, όμως, χρήση του ίδιου κρυπτογραφικού κλειδιού σε διαφορετικές εφαρμογές επιφέρει σημαντική ευπάθεια στην ασφάλεια της κάθε εφαρμογής, και πολλές φορές προσκρούει σε

αντιφατικές ανάγκες σχετικά με την 'ορθή' διαχείρισή του (*π.χ. στις εφαρμογές ηλεκτρονικών υπογραφών δεδομένων απαιτείται το υποκείμενο να κατέχει το μοναδικό ιδιωτικό κλειδί, ενώ στις εφαρμογές κρυπτογράφησης απαιτείται να υπάρχει αρχειοθετημένο και ένα τουλάχιστον αντίγραφο του ιδιωτικού κλειδιού ώστε να εξασφαλισθεί η δυνατότητα της αποκρυπτογράφησης σημαντικών δεδομένων*). Έτσι, η έκδοση ενός πιστοποιητικού για ένα συγκεκριμένο ζεύγος κρυπτογραφικών κλειδιών από έναν ΠΥΠ, συνήθως περιορίζεται σε συγκεκριμένες χρήσεις, οι οποίες προσδιορίζονται και από το σχετικό πεδίο '***Χρήση Κλειδιού***' ('*Key Usage*') των πιστοποιητικών X.509 το οποίο δέχεται συγκεκριμένες προκαθορισμένες τιμές.

Έχει μάλιστα, 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.

Επισημάνθηκε, μάλιστα, ότι ο συνδυασμός και των δύο τιμών ('***NonRepudiation***' *και* '***DigitalSignature***') στο ίδιο πιστοποιητικό ΔΕΝ είναι αποδεκτός από τα **ευρωπαϊκά πρότυπα** (*σύμφωνα με τον όρο **Κ.Μ. 3.4 του προτύπου CEN CWA 14167-1** που δημοσιεύθηκε και στην Εφημερίδα των Ε.Κ.*) και ας επιτρέπεται κάτι τέτοιο από το **διεθνές 'σχέδιο'** ('***R**equest **F**or **C**omments*') **προτύπου** 'RFC 3280' του IETF (*σ.σ.: αυτό απαγορευόταν και στο παλιότερο 'διεθνές πρότυπο' '**RFC 2459**', όμως, η απαγόρευση αυτή 'άρθηκε' στην νέα έκδοση του προτύπου RFC '3280' -μετά από επιμονή κυρίως των εκπροσώπων του 'Αγγλοσαξονικού δικαίου' (common law)*).

Παρ' όλα αυτά, μόνο η χρήση του πεδίου '***Χρήση Κλειδιού***' ('*Key Usage*') στα εκδιδόμενα πιστοποιητικά (τύπου X.509) **ΔΕΝ αρκεί** για να προσδιορίσει πλήρως τους ακριβείς όρους και τους

περιορισμούς που θέτει ο Εκδότης τους για την χρήση των σχετικών κρυπτογραφικών κλειδιών. Έτσι θεωρείται επιβεβλημένη (ιδίως στα 'αναγνωρισμένα πιστοποιητικά') η σύνταξη (ή η υιοθέτηση) συγκεκριμένης και αναλυτικής «**Πολιτικής** (έκδοσης) **Πιστοποιητικού**» (Certificate Policy) και η αναγραφή στο σχετικό πεδίο του πιστοποιητικού του μοναδικού '***κωδικού αριθμού ταυτοποίησης***' ('*Object Identification number' ή 'OID'*) της, ώστε να μπορεί να ενημερωθεί *τόσο* το υποκείμενο πιστοποίησης ('συνδρομητής' του ΠΥΠ/Εκδότη), *όσο* και κάθε τρίτος-αποδέκτης, για τους ακριβείς όρους που διέπουν την χρήση του συγκεκριμένου πιστοποιητικού.

Ευπάθεια αλγόριθμων & διαχρονικότητα των η- Υπογραφών

Η **ευπάθεια (Vulnerability)** των χρησιμοποιούμενων αλγόριθμων κρυπτογράφησης με το πέρασμα του χρόνου και την εξέλιξη της τεχνολογίας**,** και η -σχετιζόμενη μ' αυτήν- περιορισμένη διάρκεια ισχύος των 'πιστοποιητικών δημόσιου κλειδιού' (Public Key Certificates), δημιουργεί πολλά προβλήματα στην μακροχρόνια επαλήθευση της εγκυρότητας μιας ηλεκτρονικής υπογραφής. Παράλληλα, η πιθανότητα ανάκλησης της ισχύος ενός πιστοποιητικού πριν από την προκαθορισμένη λήξη του (π.χ. λόγω έκθεσης των σχετικών κρυπτογραφικών κλειδιών σε τρίτους), δημιουργεί επιπρόσθετα προβλήματα για τον έλεγχο της εγκυρότητας μιας η-υπογραφής σε μεταγενέστερο χρονικό σημείο.

Μία λύση για την μακρόχρονη επαλήθευση της εγκυρότητας μιας υπογραφής κατά τον χρόνο εναπόθεσής της, είναι η (πρόσθετη) χρήση '**Χρονοσήμανσης'** (time-stamping ή/και time-marking) στα υπογεγραμμένα ηλεκτρονικά έγγραφα ώστε να αποδεικνύεται έτσι ευκολότερα η σύνδεση μιας συγκεκριμένης υπογραφής σε ένα έγγραφο πριν τη λήξη ή ανάκληση της ισχύος του σχετικού πιστοποιητικού!

Η χρονοσήμανση δεν αποτελεί υποχρεωτικό στοιχείο της δομής της ηλεκτρονικής υπογραφής, αλλά επαφίεται στην εφαρμοζόμενη 'Πολιτική Υπογραφής' να καθορίσει -*ανάλογα με το είδος των σχετικών συναλλαγών*- την επιβολή της ή όχι και για το ποιος από τα δύο μέρη (υπογράφων και αποδέκτης) θα φέρει την ευθύνη της απόκτησής της.

Εναλλακτικά, αντί για χρονοσήμανση μπορεί να γίνει χρήση 'Τρίτων Έμπιστων Οντοτήτων'/ΠΥΠ ('ηλεκτρονικά συμβολαιογραφεία') που αναλαμβάνουν την ασφαλή διαφύλαξη (αρχειοθέτηση) των υπογεγραμμένων ηλεκτρονικών εγγράφων και την επιβεβαίωση της μη αλλοίωσης και του χρόνου κατάθεσης των εγγράφων αυτών μετά από μεγάλο χρονικό διάστημα.

Μια άλλη σχετική παρατήρηση είναι ότι η ευπάθεια των χρησιμοποιούμενων κρυπτογραφικών μεθόδων, εμπεριέχει και τον κίνδυνο της αποκρυπτογράφησης 'έμπιστευτικών'

δεδομένων που συλλέχθησαν 'κρυπτογραφημένα', αμέσως μόλις η τρέχουσα τεχνολογία 'αποδυναμώσει' του σχετικούς αλγόριθμους που χρησιμοποιήθηκαν.

Δύο διαφορετικές φιλοσοφίες (PKI – PGP) με διαφορετικά πεδία εφαρμογής

Η **ιεραρχική** πιστοποίηση δημόσιων κλειδιών των συναλλασσόμενων-τελικών οντοτήτων από μια τεκμηριωμένη υποδομή 'PKI' ενός (ή περισσότερων) ΠΥΠ, αποτελεί το αντικείμενο των περισσότερων προσπαθειών προτυποποίησης, μιας και θεωρείται το 'ιδανικό μοντέλο' για την έκδοση '**αναγνωρισμένων πιστοποιητικών**', που παρέχουν ικανοποιητικές εγγυήσεις στις συναλλαγές -ακόμη και μεταξύ αγνώστων.

Όμως, μια εντελώς διαφορετική φιλοσοφία από την 'ιεραρχική πιστοποίηση' του PKI, προβάλλει η ευρείας χρήσης εναλλακτική μέθοδος πιστοποίησης (προσωπικών) δημοσίων κλειδιών που αποκαλείται '**Pretty Good Privacy**' (PGP).

Η μέθοδος αυτή, παράγει εξίσου 'προηγμένες ηλεκτρονικές υπογραφές', αλλά βασίζεται σε 'αυτό-ϋπογραφόμενα' πιστοποιητικά που εκδίδονται από το ίδιο τον (τελικό) χρήστη-κάτοχο ζεύγους κρυπτογραφικών κλειδιών και τα οποία τα δημοσιεύει σε έναν ή περισσότερους δημόσιους '***εξυπηρετητές κλειδιών***' (*key servers*). Τα πιστοποιητικά αυτά αξιολογούνται από άλλους χρήστες με τους οποίους αναπτύσσει διαπροσωπική επικοινωνία το υποκείμενο-κάτοχος των κλειδιών, οι οποίοι, αφού πρώτα επιβεβαιώσουν την ισχυριζόμενη ταυτότητα του υποκειμένου, πιστοποιούν την συγκεκριμένη συσχέτιση υπογράφοντας και αυτοί το συγκεκριμένο πιστοποιητικό. Αυτή η μέθοδος πιστοποίησης δημοσίων κλειδιών 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.*- 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.λ.π.*) δημιουργούν μεν '*ψηφιακές υπογραφές'* (δηλαδή υπογραφές που ικανοποιούν τους όρους της νομοθεσίας για '*προηγμένες' ηλεκτρονικές υπογραφές*), **όμως δεν μπορούν** να παράξουν '*αναγνωρισμένες' ηλεκτρονικές υπογραφές* -εφόσον δεν υποστηρίζονται από ένα '***αναγνωρισμένο πιστοποιητικό***'. Επειδή κανένας από τους πιστοποιούντες δεν αναλαμβάνει ιδιαίτερη ευθύνη και υποχρεώσεις έναντι των τρίτων, το μοντέλο αυτό ***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.

Παρόλα αυτά, το μοντέλο PGP εξασφαλίζει περισσότερο την άμεση διαχείριση των προσωπικών δεδομένων από τον ίδιο το υποκείμενό τους, και **δεν θα πρέπει να παραγνωριστεί η**

χρησιμότητά του, ιδίως για τις προσωπικές-κοινωνικές (ηλεκτρονικές) επικοινωνίες των χρηστών του. Για τον λόγο αυτό θα πρέπει να ληφθεί υπ' όψιν στους σχεδιασμούς υπηρεσιών που δεν απαιτούν 'αυστηρή πιστοποίηση' των προσωπικών στοιχείων των αποδεκτών τους.

Πιστοποίηση 'ιδιοτήτων' και 'ρόλων' των υποκειμένων (attribute certificates)

Η ύπαρξη και η επίκληση μιας συγκεκριμένης 'ιδιότητας' ή 'ρόλου' (ή 'εξουσιοδότητησης') του υπογράφοντα, σε πάρα πολλές περιπτώσεις, παίζει ιδιαίτερο ρόλο στο κύρος ή στην αξιοπιστία αυτής καθ' αυτής της υπογραφής. Έτσι και στις ηλεκτρονικές υπογραφές υπάρχει συχνά ανάγκη για επίκληση μιας συγκεκριμένης ιδιότητας του υπογράφοντα κατά την εναπόθεση μιας συγκεκριμένης ηλεκτρονικής υπογραφής του. Η '**ιδιότητα'** αυτή μπορεί να είναι είτε πιστοποιημένη από κάποιον αρμόδιο φορέα, είτε κατά απλή δήλωση του υπογράφοντα.

Ένας τρόπος να γίνει αυτό, είναι η μόνιμη αναφορά μιας συγκεκριμένης ιδιότητας του υπογράφοντα (π.χ. στοιχεία της εταιρίας που εργάζεται, ή αναφορά του ελεύθερου επαγγέλματός του) στο ίδιο το 'βασικό' πιστοποιητικό δημοσίου κλειδιού, μαζί δηλαδή, με τα άλλα στοιχεία ταυτοποίησής του. Όμως, αυτό περιορίζει την δυνατότητα να διακρίνουμε σε ποιες υπογραφές επικαλείται ο υπογράφων την συγκεκριμένη ιδιότητά του και σε ποιες όχι. Το πρόβλημα λύνεται εάν θεωρήσουμε ότι το πιστοποιητικό αυτό (και τα σχετικά κλειδιά) θα πρέπει να χρησιμοποιείται πάντα και μόνο για υπογραφές σχετικές με την συγκεκριμένη ιδιότητα του υπογράφοντα ('dedicated certificate'). Επίσης, σ' αυτήν την περίπτωση θα πρέπει να υπάρξει κάποιος 'standard' διακριτός τρόπος για να ενημερώνεται ο αποδέκτης για το εάν η συγκεκριμένη ιδιότητα είναι πιστοποιημένη ή όχι, και αν ναι, από ποιόν φορέα *(-τον ίδιο τον ΠΥΠ?, -την εταιρία που εργάζεται?, -τον Επαγγελματικό ή άλλο Σύλλογο του?)*.

Η πιστοποίηση μιας ιδιότητας του υπογράφοντα μπορεί να γίνει όμως και με την χρήση ξεχωριστών '**πιστοποιητικών ιδιοτήτων ή εξουσιοδότησης**' ('attribute certificates' - IETF RFC 3281) τα οποία θα συνδέονται με το βασικό πιστοποιητικό (δημοσίου κλειδιού) της υπογραφής ενός χρήστη). Τα πιστοποιητικά αυτά θα εκδίδονται από τους αρμόδιους φορείς (*π.χ. επαγγελματικοί σύλλογοι για την πιστοποίηση του επαγγέλματος*) και με την επιλεκτική χρησιμοποίησή τους από τον 'ιδιοκτήτη' τους, θα μπορούν να βοηθήσουν στην 'διαφοροποίηση' της εκάστοτε υπογραφής του, όπου οι ανάγκες μιας συγκεκριμένης εφαρμογής το απαιτούν (*π.χ. υπογραφή ως 'ιδιώτης' ή ως εκπρόσωπος εταιρίας, ως δικηγόρος, κ.λ.π.*).

Η δεύτερη μέθοδος προσφέρει την δυνατότητα για παροχή δικαιωμάτων ή απόδοση ιδιοτήτων σε ένα υποκείμενο τα οποία μπορούν να έχουν περιορισμένη διάρκεια ή να ανακληθούν άμεσα, χωρίς να επηρεάσουν το βασικό πιστοποιητικό ταυτοποίησης του υπογράφοντα που

παραμένει σε ισχύ. Επίσης, η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για επιλεκτική παροχή πραγματικών στοιχείων ταυτοποίησης του υπογράφοντα σε περίπτωση που αυτός χρησιμοποιεί ψευδώνυμο βασικό πιστοποιητικό ηλεκτρονικής υπογραφής.

Πληθώρα ζητημάτων για την επίτευξη ολοκληρωμένων και διαλειτουργικών εφαρμογών

Πολύ σημαντικά ζητήματα διαλειτουργικότητας σχετίζονται με τη μέθοδο δημοσίευσης των **ανακλήσεων των πιστοποιητικών** (*CRLs, delta-CRLs, OCSPs*), τον τρόπο **ταυτοποίησης** των υποκειμένων (*χρήση ψευδώνυμων, αναγραφόμενα στοιχεία υποκειμένου, κ.λ.π.*), καθώς και με την αναγνώριση των **ειδικότερων όρων** που διέπουν την χρήση των εκδιδόμενων πιστοποιητικών (*πολιτική πιστοποιητικού, όρια στην αξία των συναλλαγών, περιορισμοί στην χρήση τους, κ.λ.π.*).

Οι **πολλαπλές υπογραφές** σε ένα ηλεκτρονικό έγγραφο, αποτελούν ένα άλλο σημαντικό ζήτημα που περιπλέκει ακόμη περισσότερο την εφαρμογή και τον έλεγχο των ηλεκτρονικών υπογραφών. Για την **έγκυρη κατάρτιση μιας σύμβασης,** οι υπογραφές των συμβαλλόμενων τίθενται στο σώμα του εγγράφου, αλλά πρέπει να συνδεθούν με μια λογική σειρά με αυτό. Για μια τέτοια ηλεκτρονικά καταρτιζόμενη σύμβαση πρέπει να μπορεί να αποδειχθεί ο σύνδεσμος ανάμεσα στις ηλεκτρονικές υπογραφές των συμβαλλόμενων και το περιεχόμενο της συμβάσεως. Στις άτυπες συμβάσεις ένα ζήτημα μπορεί να προκύψει από τη σχέση των συμβαλλόμενων μεταξύ τους. Ενδεχομένως τα συμβαλλόμενα μέρη να χρειαστεί να συμφωνήσουν μεταξύ τους την σειρά με την οποία θα πρέπει να υπογραφεί η σύμβαση. Για παράδειγμα, αν για μια συναλλαγή απαιτείται η έγκριση, η σχετική υπογραφή που υποδεικνύει έγκριση θα πρέπει να τεθεί μετά την υπογραφή που δηλώνει αποδοχή. Στις τυπικές συμβάσεις θα πρέπει να αναλυθούν σε κάθε περίπτωση χωριστά οι επιπτώσεις που μπορεί να έχει η χρήση ηλεκτρονικών υπογραφών σε λειτουργίες όπως η αποδοχή των όρων της συμβάσεως, η έγκριση, ο έλεγχος κ.λ.π. Η χρήση **πολιτικών υπογραφής** μπορεί να είναι μια διέξοδος για τη χρήση πολλαπλών υπογραφών, καθώς και σε θέματα που άπτονται συγκεκριμένων τυπικών συναλλαγών

Ιδιαίτερα σε **διεθνείς συναλλαγές**, τα παραπάνω προβλήματα διαλειτουργικότητας γίνονται εντονότερα, καθώς προσθέτονται **ανάγκες έγκυρης πληροφόρησης** για την αξιοπιστία του (αλλοδαπού) ΠΥΠ, και το **ζήτημα της γλώσσας** στην οποία παρέχονται οι σχετικές πληροφορίες.

Σχετική είναι η ανάγκη για τεχνολογική μέθοδο **αμοιβαίας αναγνώρισης** (cross-certifying) μεταξύ των ΠΥΠ και κυρίως μεταξύ των εθνικών ρυθμιστικών αρχών που εποπτεύουν την λειτουργία τους.

Υψηλές προδιαγραφές του κατάλληλου λογισμικού δημιουργίας & επαλήθευσης η-υπογραφών

Με βάση τις παραπάνω παρατηρήσεις, διαπιστώνεται ότι ένα **πλήρες λογισμικό** δημιουργίας και επαλήθευσης ηλεκτρονικών υπογραφών, θα πρέπει να καλύπτει ικανοποιητικά πάρα πολλές – και δύσκολες από τεχνική άποψη- προδιαγραφές, μεταξύ των οποίων:

- Διάκριση Πολιτικής/Είδους της υπογραφής (*Non Repudiation, Authentication, κ.λ.π. / "Commitment type"*)
- Χειρισμό πρόσθετων πιστοποιητικών ιδιοτήτων/ρόλων, πολλαπλών υπογραφών, κ.λ.π.)
- Ολοκληρωμένο έλεγχο και διαχείριση πρόσθετων στοιχείων/πληροφοριών εγκυρότητας (χρονοσημάνσεις, λίστες ανάκλησης, OCSP, κ.λπ.)
- Κατάλληλη και επαρκή πληροφόρηση του χρήστη για τους όρους και την πολιτική πιστοποίησης (ανάδειξη κειμένου 'Πολιτικής Πιστοποιητικού', συμβατότητα με πρόσθετα πεδία του ETSI TS 101862, πολυγλωσσική πληροφόρηση, κ.λ.π.)
- Τεχνολογική ασφάλεια, πιστή προβολή του πλήρους εγγράφου πριν την υπογραφή του (WYSIWYS), (αποδεδειγμένη) συνεργασία με 'α.δ.δ.υ.', κ.ά.

ΥΦΙΣΤΑΜΕΝΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ & ΕΦΑΡΜΟΓΗ ΤΟΥ

Αρχή ουδετερότητας/ισορροπίας – Ασάφειες/ελλείψεις θεσμικού πλαισίου

Η ανάγκη για **διατήρηση ουδετερότητας** προς την υπάρχουσα αγορά και τις σχετικές τεχνολογίες, σε συνδυασμό με την **αποφυγή της επέμβασης** σε ήδη υφιστάμενες σχετικές εφαρμογές και εθνικές επιλογές των κρατών-μελών, αλλά και το γεγονός ότι η Οδηγία **δεν στόχευε στην ρύθμιση θεμάτων** «*που αφορούν την σύναψη και την ισχύ των συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή του κοινοτικού δικαίου*»[15], **είχε ως αποτέλεσμα την ύπαρξη πολλών ασαφειών και παραλείψεων** στο υφιστάμενο ευρωπαϊκό θεσμικό πλαίσιο, γεγονός που οδηγεί σε αντιμετώπιση αρκετών προβλημάτων κατά την ερμηνεία του και την προσπάθεια εφαρμογής του.

Συγκεκριμένα, η Οδηγία:

---

[15] Άρθρο 2 εδ. β΄ της Οδηγίας 99/93/ΕΚ

- Δεν αποσαφηνίζει εάν οι 'αναγνωρισμένες η-υπογραφές' (του ά. 5§1) μπορούν να χρησιμοποιηθούν εξίσου για 'απλή γνησιότητα δεδομένων' και για την απλή 'επίδειξη ταυτότητας' (ηλεκτρονικές ταυτότητες) του υπογράφοντα.
- Δεν αναφέρεται καθόλου στα στοιχεία που απαιτούνται για την 'διαχρονική ισχύ' των ηλεκτρονικών υπογραφών (*Χρονοσήμανση, Αρχειοθέτηση*), ούτε αναφέρεται διεξοδικότερα στην παροχή των σχετικών υπηρεσιών από τους ΠΥΠ.
- Δεν αποσαφηνίζει τον ρόλο των προβλεπόμενων 'Εθελοντικών Διαπιστεύσεων' των ΠΥΠ (εάν θα είναι σε εθνικό ή σε πανευρωπαϊκό/κλαδικό επίπεδο)[16]
- Κάνει μόνο 'απλές συστάσεις' για την ασφαλή επαλήθευση των υπογραφών (Παράρτημα IV)

Τα ζητήματα αυτά αποτελούν ακόμη αντικείμενο συζητήσεων και αντιπαραθέσεων στα πλαίσια των σχετικών διεργασιών προτυποποίησης, με περιορισμένα –έως τώρα- αποτελέσματα.

Ρυθμιστικό πλαίσιο και εθνικές διαφοροποιήσεις στην ενσωμάτωση της Οδηγίας

Με δεδομένη την αοριστία της Οδηγίας σε αρκετά ζητήματα, οι αρμόδιες εθνικές αρχές κάθε κράτους μέλους, -εκδίδοντας σχετικούς 'Κανονισμούς'-, προχώρησαν σε διαμόρφωση λεπτομερέστερων **εθνικών ρυθμιστικών πλαισίων**, τα οποία όμως εμφανίζουν αρκετές διαφοροποιήσεις μεταξύ τους, γεγονός που εντείνει ακόμη περισσότερο το πρόβλημα της διαλειτουργικότητας και της ελεύθερης διακίνησης των σχετικών προϊόντων και υπηρεσιών στην εσωτερική αγορά.

Μια χαρακτηριστική περίπτωση διαφοροποίησης, αφορά τον τρόπο εποπτείας ή/και εθελοντικής διαπίστευσης των ΠΥΠ από τους αρμόδιους εθνικούς φορείς, και ιδίως τις διαφορετικές τεχνολογικές υποδομές που χρησιμοποιούν οι αρμόδιες αρχές για την δημοσιοποίηση των αποτελεσμάτων των σχετικών ελέγχων τους (*Root CA, Υπογεγραμμένες Λίστες, Bridge CA, κ.λπ.*).

Αντίστοιχα, παρατηρείται μια μεγάλη διαφορά και σε ότι αφορά τον βαθμό εξειδίκευσης των συγκεκριμένων κανόνων. Έτσι, κάποια κράτη-μέλη (π.χ. Γερμανία) έχουν προχωρήσει σε ρύθμιση πολύ εξειδικευμένων μηχανισμών διαπίστωσης και αξιολόγησης της ασφάλειας των 'προϊόντων ηλεκτρονικής υπογραφής', ενώ άλλα (π.χ. Μ. Βρετανία), για το συγκεκριμένο θέμα, επαφίενται στην σχετική πρωτοβουλία της ιδιωτικής αγοράς!

[16] *Βλέπε σχετική μελέτη «The Legal and Market Aspects of Electronic Signatures», παρ. 1.2.2.4*

Η σύντομη ολοκλήρωση ενός «***κοινώς αποδεκτού*** *(από όλα τα κράτη-μέλη της Ε.Ε.)* ***συστήματος προτυποποίησης των ηλεκτρονικών υπογραφών***», στο οποίο θα μπορούν να αναφέρονται με ασφάλεια όλες οι εθνικές ρυθμιστικές αρχές, διαπιστώνεται ως απαραίτητη προϋπόθεση για την μελλοντική συμβατότητα των εθνικών ρυθμιστικών πλαισίων μεταξύ τους!

ΖΗΤΗΜΑΤΑ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

Μεγάλο κόστος υποδομής - Έλλειψη 'κρίσιμης μάζας'

Θεωρείται ότι το **μεγάλο κόστος** για την ανάπτυξη και την συντήρηση μιας υποδομής για την υποστήριξη εφαρμογών ηλεκτρονικών υπογραφών, καθιστούν ασύμφορη -σήμερα τουλάχιστον- την επένδυση σ' αυτόν το τομέα, καθώς οι σχετικές εφαρμογές είναι περιορισμένες και ο κύκλος των αποδεκτών πολύ μικρός. Μια **λύση** στο θέμα της εξυπηρέτησης του κόστους της παροχής των υπηρεσιών πιστοποίησης είναι η εξάπλωση της χρήσης των ηλεκτρονικών πιστοποιητικών σε περισσότερες εφαρμογές (και άρα με περισσότερους δυνητικούς αποδέκτες), ώστε να καταστεί αναγκαία και χρήσιμη **η απόκτησή τους από ευρύτερο κοινό**.

Οι **αποσπασματικές πρωτοβουλίες** από φορείς της αγοράς δεν μπορούν να φέρουν ικανοποιητικά αποτελέσματα σχετικά με την αύξηση της χρήσης των ηλεκτρονικών υπογραφών και τη δημιουργία της **απαραίτητης 'κρίσιμης μάζας'** στους αποδέκτες των εφαρμογών τους. Ο κυριότερος λόγος για αυτό είναι το μικρό μέγεθος αυτών των εφαρμογών και η **έλλειψη διαλειτουργικότητας** των σχεδιαζόμενων προϊόντων και υπηρεσιών, που απευθύνονται προς τους τελικούς χρήστες.

Διαφορετικές προσεγγίσεις των ΠΥΠ στις Πολιτικές Πιστοποίησης

Η τυποποίηση και αποδοχή συγκεκριμένων "**Πολιτικών (έκδοσης) πιστοποιητικού"** (Certificate Policies) όπου θα προσδιορίζονται συγκεκριμένοι όροι έκδοσης και χρήσης των ηλεκτρονικών πιστοποιητικών (π.χ. τρόποι ταυτοποίησης του υποκειμένου, profile (δομή) του πιστοποιητικού, επιτρεπόμενες χρήσεις και υποχρεώσεις του συνδρομητή και του αποδέκτη του πιστοποιητικού, εγγυήσεις και όρια ευθύνης του ΠΥΠ, κ.λ.π.) αποτελεί σημαντικό στοιχείο για την διαλειτουργικότητα μεταξύ των πιστοποιητικών που εκδίδονται από διαφορετικούς ΠΥΠ.

Στο πλαίσιο αυτό εξετάστηκαν οι '***Πολιτικές Πιστοποιητικών***' (*Certificate Policies*) που εφαρμόζουν οι υφιστάμενοι ΠΥΠ στην Ελλάδα που έχουν καταχωρηθεί στην ΕΕΤΤ ως ***'εκδότες αναγνωρισμένων πιστοποιητικών***'. Και οι δύο Πάροχοι Υ.Π. δηλώνουν την συμμόρφωσή τους με το πρότυπο **ETSI TS 101 456** το οποίο καθορίζει τις βασικές απαιτήσεις για τις δύο τυποποιημένες '*Πολιτικές Αναγνωρισμένων Πιστοποιητικών*' τις οποίες προτείνει (*την* ***'QCP public'*** *για*

*αναγνωρισμένα πιστοποιητικά και την '**QCP public+SSCD**' για αναγνωρισμένα πιστοποιητικά με υποχρεωτική χρήση '**ασφαλούς διάταξης δημιουργίας υπογραφής**'*). Ως προς τον τρόπο προσέγγισης, όμως, των δύο ΠΥΠ στην υλοποίηση του συγκεκριμένου προτύπου, παρατηρήθηκαν οι εξής διαφορές:

Η μεν **ADACOM** στα αναγνωρισμένα πιστοποιητικά που εκδίδει αναγράφει τον κωδικό OID (*'Object Identification'*) της πρότυπης πολιτικής *'**QCP+SSCD**'* του ETSI, δηλώνοντας με αυτό τον τρόπο την συμμόρφωσή της με τις γενικές απαιτήσεις αυτής της Πολιτικής. Παράλληλα δηλώνει συμμόρφωση με το πρότυπο **ETSI TS 101 862** στο οποίο ορίζεται, μεταξύ άλλων, ο τρόπος ενσωμάτωσης των '***δηλώσεων του Εκδότη***' ως προς τα «*επιτρεπόμενα όρια στην αξία των συναλλαγών*» που θα χρησιμοποιείται το πιστοποιητικό, δίνοντας την δυνατότητα στην ADACOM να ορίζει κατά περίπτωση τα επιθυμητά όρια σε κάθε εκδιδόμενο πιστοποιητικό. Στην «***Διακήρυξη Πρακτικής (ή Κανονισμό) Πιστοποίησης***» (*Certification Practice Statement*) που δημοσιεύει η ADACOM μπορούν να βρεθούν οι **εξειδικεύσεις** για την εφαρμογή της παραπάνω Πολιτικής Πιστοποιητικού, καθώς και το Ανώτατο Όριο (συνολικής) Ευθύνης της για κάθε πιστοποιητικό (το οποίο ισχύει στην περίπτωση που δεν αναφέρονται ειδικότεροι περιορισμοί μέσα στο ίδιο το πιστοποιητικό) και το οποίο φθάνει στο ύψος των **100.000 €** (*ποσό που προβλέπεται και από το 'πρόγραμμα ασφάλισης' της συνεργαζόμενης εταιρίας Verisign*). Ο τρόπος επιβολής-ελέγχου της απαιτούμενης χρήσης «ασφαλούς διάταξης δημιουργίας υπογραφής» διενεργείται με την δημιουργία -*μέσω ειδικής εφαρμογής*- των κλειδιών από τον ίδιο τον χρήστη μέσα σε μία 'έξυπνη κάρτα' (*την οποία τον έχει προμηθεύσει η 'Υπηρεσία Εγγραφής' της ADACOM κατά τον έλεγχο της ταυτότητάς του*) και την επακόλουθη 'on-line' εγκατάσταση των σχετικών πιστοποιητικών στην κάρτα αυτή.

Η δε **ΑΣΥΚ,** έχει προχωρήσει στην σύνταξη δικού της κειμένου 'Πολιτικής Πιστοποιητικού', το οποίο δηλώνει πλήρη συμμόρφωση με τη γενική πολιτική αναγνωρισμένων πιστοποιητικών '***QCP+SSCD***' του προτύπου **TS 101 456** του **ETSI**, αλλά προχωρά και σε περαιτέρω εξειδίκευση της. Ιδιαίτερο χαρακτηριστικό του κειμένου αυτού είναι ότι συμπεριέχει και συνδυάζει ταυτόχρονα και άλλη μία πολιτική πιστοποιητικού για '***μη αναγνωρισμένα πιστοποιητικά***' (*συμβατή με την πολιτική '**NCP+**' του αντίστοιχου προτύπου **ETSI TS 102 042***) προβλέποντας την συνέκδοση και συνύπαρξη δύο διαφορετικών κλειδιών και πιστοποιητικών σε μία προσωποποιημένη έξυπνη κάρτα (*smart-card*) του υποκειμένου, που διέπονται από τις δύο αυτές διακριτές Πολιτικές. Μάλιστα, η ΑΣΥΚ προχώρησε με πρωτοβουλία της και στην τυποποίηση τριών συγκεκριμένων κλάσεων που σχετίζονται με τους περιορισμούς στην χρήση και τα επιτρεπόμενα όρια συναλλαγών (*0=Demo, 1=για συναλλαγές χωρίς οικονομικό αντικείμενο, και 2=για συναλλαγές έως 10,000 €*). Και οι 6 διαφορετικές παραλλαγές της βασικής πολιτικής της (2

πολιτικές Χ 3 κλάσεις) τεκμηριώνονται στο κοινό κείμενο, αλλά διακρίνονται από ξεχωριστό κωδικό ταυτοποίησης (*'OID'*) που έχει αντιστοιχίσει η ΑΣΥΚ σε κάθε μία παραλλαγή της πολιτικής, ο οποίος αναγράφεται πάντα στο σχετικό πεδίο 'Certificate Policy' του πιστοποιητικού που την εφαρμόζει. Η δε χρήση 'α.δ.δ.υ.' από το υποκείμενο, εξασφαλίζεται με την ασφαλή προετοιμασία και αποστολή της προσωποποιημένης κάρτας στον δικαιούχο χρήστη απευθείας από τη σχετική υπηρεσία της ΑΣΥΚ.

Ιδιαίτερες ανάγκες των εφαρμογών – Τυποποίηση των Υπηρεσιών Πιστοποίησης

Το **ETSI ESI**[17] (στα πλαίσια του **EESSI**[18]) έχει εκδώσει δύο πρότυπα (τα **TS 101 456** και **TS 101042**) στα οποία ορίζονται **πέντε βασικές 'Πολιτικές Πιστοποιητικού'**, -οι '**QCP**' και '**QCP+SSCD**' για αναγνωρισμένα πιστοποιητικά και οι '**LCP**', '**NCP**' & '**NCP+**' για άλλου είδους πιστοποιητικά- με στόχο την καθοδήγηση των παρόχων αναγνωρισμένων πιστοποιητικών και γενικών κλάσεων πιστοποιητικών κατά τη σύνταξη και εφαρμογή των δικών τους 'πολιτικών πιστοποιητικών' οι οποίες θα εξειδικεύονται περαιτέρω, ανάλογα με τις ιδιαίτερες ανάγκες των εφαρμογών στις οποίες θα απευθύνονται. Τα πρότυπα αυτά, μάλιστα, αποτελούν και τη βάση αξιολόγησης συμμόρφωσης των παρόχων με τα κριτήρια σχημάτων πιστοποίησης σε χώρες όπως το Ηνωμένο Βασίλειο, Ολλανδία και αλλού.

Στα πλαίσια των διαβουλεύσεων της ομάδας Ο.Ε. 'Ε2', τέθηκε ο **προβληματισμός** κατά πόσον μια προσπάθεια για τυποποίηση (βάσει των παραπάνω προτύπων) και 'συντονισμό' των παρεχόμενων υπηρεσιών από τους ΠΥΠ που λειτουργούν στην Ελλάδα (με σκοπό να αποφευχθούν προβλήματα διαλειτουργικότητας μεταξύ τους) θα είχε νόημα και αποτέλεσμα. Χαρακτηριστικά, αναφέρθηκε ότι η ρύθμιση θεμάτων όπως το 'profile' (δομή και περιεχόμενο) των εκδιδόμενων πιστοποιητικών και η τυποποίηση 'πολιτικών (έκδοσης) πιστοποιητικών' (Certificate Policies), από την μία πλευρά αποτελούν **αντικείμενο προτυποποίησης σε διεθνές και ευρωπαϊκό επίπεδο** (και άρα θα ήταν ανώφελο να συζητήσουμε κάτι τέτοιο σε εθνικό επίπεδο), από την άλλη ότι – πιθανότατα- **μια 'τυποποιημένη λύση' θα ερχόταν σε αντίθεση με τις ιδιαίτερες ανάγκες και τις εξειδικευμένες απαιτήσεις** των επιθυμητών εφαρμογών (*π.χ. στην εφαρμογή e-banking μιας τράπεζας*).

Σε απάντηση στους παραπάνω προβληματισμούς, αντιτάχθηκαν τα εξής:

---

17 European Telecommunication Standards Institute, www.etsi.org

18 European Electronic Signatures Standardization Initiative, http://www.ict.etsi.org/EESSI_home.htm

α) ότι η υπάρχουσα (διεθνής και ευρωπαϊκή) προτυποποίηση παρέχει ήδη μια πληθώρα **κανόνων για την επίτευξη μιας 'ελάχιστης' διαλειτουργικότητας**, -δηλαδή, ενός 'πυρήνα' (core) από απαραίτητες κοινές προδιαγραφές- και ότι, δυστυχώς, πολλοί από αυτούς (*λόγω της πρόσφατης σχετικά έκδοσής τους, αλλά και της συνθετότητάς τους*) αγνοούνται ή παρερμηνεύονται από την αγορά, -οπότε μια κοινή 'αναψηλάφηση' των ακολουθούμενων πρακτικών θα μπορούσε να φέρει στην επιφάνεια τέτοια ζητήματα και να ενεργοποιήσει διαδικασίες αλληλο-ενημέρωσης και συνεργασίας των ελληνικών ΠΥΠ για την συμμόρφωσή τους με αυτούς τους κανόνες,

β) ότι η ίδια αυτή η προτυποποίηση αφήνει σκόπιμα πολλά **'ανοικτά και αόριστα' σημεία, με πολλές 'δυνατές επιλογές' (***options***),** ακριβώς διότι αντιλαμβάνεται ότι αυτά θα πρέπει να αποτελέσουν αντικείμενο συζήτησης και συμφωνίας μεταξύ ομοειδών ομάδων ή συναλλακτικών κύκλων σε τοπικό ή/και κλαδικό επίπεδο (π.χ. στον τραπεζικό τομέα). Χαρακτηριστικά αναφέρθηκε ότι, ενώ καθορίζεται συγκεκριμένος τρόπος (ETSI TS 101862) αναγραφής των '*ορίων στην αξία των συναλλαγών*' που θα επιτρέπονται από τον εκδότη για την χρήση ενός συγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής, εν τούτοις δεν έχουν οριστεί τυποποιημένες 'κλάσεις' πιστοποιητικών για τα όρια αυτά (*π.χ. μία κλάση για συναλλαγές έως 1.000€, μια άλλη για περισσότερο όριο, μία άλλη για συναλλαγές χωρίς οικονομική αξία, κ.ό.κ*) -κάτι που μπορεί, όμως, να ορίσει από κοινού μια ομάδα ΠΥΠ (σε τοπικό επίπεδο), αφού εξετάσει τις ανάγκες των αποδεκτών στους οποίους απευθύνεται.

γ) ότι ειδικότερα στην Ελλάδα, λόγω και του **διαφορετικού αλφαβήτου** που χρησιμοποιούμε, θέτονται πολλά ζητήματα τα οποία θα πρέπει να αντιμετωπιστούν ομοιόμορφα από τους ΠΥΠ, όπως π.χ. η χρήση ελληνικών ή/και λατινικών χαρακτήρων στην περιγραφή των υποκειμένων, τα χρησιμοποιούμενα πρότυπα (π.χ. ΕΛΟΤ 743) και οι πρακτικές μετατροπής των ελληνικών χαρακτήρων σε λατινικούς, η κωδικοποίησή τους (π.χ. ISO 8859-7 ή UTF-8), καθώς και άλλα θέματα όπως η χρησιμοποιούμενη ορολογία (για παράδειγμα*: 'Subject' = 'Θέμα'* ή *'Υποκείμενο'?* Πώς μεταφράζουμε το *'Certificate Practice Statement?* κ.ά.),

δ) ότι σε κάθε περίπτωση, ακόμη και για χρήση τους σε '*κλειστές εφαρμογές*' (σ.σ.: όπου **δεν** επιβάλλεται καμιά συμμόρφωση με συγκεκριμένες προδιαγραφές), θα παρείχε αρκετά οφέλη μια ευθυγράμμιση των εκδιδόμενων πιστοποιητικών σε '***κοινώς αποδεκτούς κανόνες***' (*π.χ. εάν θα χρησιμοποιείται το πεδίο 'Common Name' ή τα πεδία 'Surname' και 'Given Name' για την αναγραφή του ονοματεπώνυμου του υποκειμένου*) οι οποίοι, -*ακόμη κι αν δεν καθορίζονται σαφώς από την υφιστάμενη προτυποποίηση*-, θα μπορούσαν να υιοθετηθούν από εφαρμοσμένες '***best practices***' (*των*

οποίων, βέβαια, η ανάδειξή τους αποτελεί αντικείμενο σχετικής διερεύνησης -σε εθνικό και ευρωπαϊκό επίπεδο- και περαιτέρω συζήτησης).

ε) ότι, εξάλλου, και η έως τώρα επιτευχθείσα διεθνής (και ιδίως η ευρωπαϊκή) προτυποποίηση των ηλεκτρονικών υπογραφών, βασίσθηκε κυρίως πάνω σε προηγούμενες '*de facto*' και, -ελλείψει προτύπων-, '*αυθαίρετες'* επιλογές που έγιναν σε τοπικό ή κλαδικό επίπεδο σε διάφορα κράτη-μέλη της Ε.Ε. (*όπως η Γερμανία, Ιταλία, Φιλανδία κ.λ.π.*) και ότι αυτές οι **πρωτοβουλίες** είχαν σημαντικά αποτελέσματα στην ανάπτυξη των σχετικών εφαρμογών στις χώρες αυτές. Αναφέρθηκε, μάλιστα, και το παράδειγμα των σκανδιναβικών χωρών, όπου πολλές Τράπεζες και Τηλεπικοινωνιακοί Φορείς συνεργάστηκαν στην υιοθέτηση και την τυποποίηση συγκεκριμένου συστήματος ηλεκτρονικών υπογραφών και ηλεκτρονικών πληρωμών (για mobile & home banking) το οποίο συμμορφώνεται με (και παράλληλα εξειδικεύει) τις απαιτήσεις της υφιστάμενης ευρωπαϊκής νομοθεσίας, και το οποίο λειτουργεί αρκετό καιρό με ιδιαίτερη επιτυχία.

Πιστοποίηση (Διαπίστωση και Διαπίστευση) προϊόντων & υπηρεσιών

Υπάρχει η προσδοκία ότι η δημοσίευση του πλαισίου για την **διαπίστωση συμμόρφωσης των προϊόντων ηλεκτρονικής υπογραφής** και την **εθελοντική διαπίστευση των ΠΥΠ** από την αρμόδια εθνική ρυθμιστική αρχή (ΕΕΤΤ) θα συμβάλει θετικά στη διαμόρφωση του επιχειρηματικού πλαισίου. Παρατηρήθηκε όμως σχετικά, ότι υπήρξαν άλλες χώρες-μέλη της ΕΕ, όπου οι υπηρεσίες ηλεκτρονικής υπογραφής αναπτύχθηκαν επιτυχώς πολύ πριν υλοποιηθούν οι σχετικοί μηχανισμοί διαπίστωσης και (εθελοντικής) διαπίστευσης που προβλέπονται στα πλαίσια της Οδηγίας 1999/93/ΕΚ. Στο Βέλγιο, για παράδειγμα, η παροχή υπηρεσιών πιστοποίησης άρχισε ήδη από το 1996 (π.χ GlobalSign, Isabel), ενώ το σχήμα διαπίστευσης των ΠΥΠ εμφανίσθηκε μόλις το 2003 (BE.SIGN). Αντίστοιχα είναι τα παραδείγματα και σε άλλες χώρες όπως η Γερμανία, Ιταλία, Σουηδία, Φιλανδία κ.ά., χώρες όμως που χαρακτηρίζονται από το γεγονός ότι είχαν αναπτύξει από νωρίς ιδιαίτερη εθνική νομοθεσία για τις ηλεκτρονικές υπογραφές ή είχαν θεσπίσει σχετικούς κανόνες διαλειτουργικότητας και τεχνικά πρότυπα ασφάλειας τα οποία ίσχυαν αποκλειστικά σε εθνικό επίπεδο.

Ειδικότερα για την «**Εθελοντική Διαπίστευση**» των ΠΥΠ, με αφορμή και την έκδοση του νέου σχετικού Κανονισμού από την ΕΕΤΤ, υπενθυμίστηκε ότι η μεγάλη 'νομικο-εμπορική' μελέτη ('***Legal and Market aspects of electronic signatures in EU'***) που έγινε πρόσφατα για λογαριασμό της Commission, προτρέπει στην ερμηνεία των σχετικών προβλέψεων της Οδηγίας, όχι προς «*τη δημιουργία συστημάτων εθελοντικής διαπίστευσης σε 'εθνική βάση' σε κάθε ένα κράτος-μέλος, τα οποία θα εξυπηρετούν μονάχα την διαπίστωση της συμμόρφωσης με τις απαιτήσεις της νομοθεσίας-*

προτυποποίησης» (κάτι που, ούτως ή άλλως, υπόκειται ήδη στον έλεγχο των αρμόδιων εθνικών φορέων για όλους τους ΠΥΠ που δηλώνουν ότι εκδίδουν 'αναγνωρισμένα πιστοποιητικά'). Αντιθέτως, και σύμφωνα με την μελέτη αυτή, *η οργάνωση συστημάτων εθελοντικής διαπίστευσης θα πρέπει να γίνει από μεγάλους 'κλαδικούς' πανευρωπαϊκούς ή πολυεθνικούς φορείς που θα προσανατολίζονται* ***κυρίως*** *στην διαπίστωση της συμμόρφωσης με* ***ειδικότερες*** *απαιτήσεις ασφάλειας και 'εργονομίας',, τις οποίες θα έχουν θέσει ως 'απαραίτητες' για την διαπίστευση αυτή οι εκπρόσωποι του συγκεκριμένου 'κλάδου'* (π.χ. Τράπεζες, Δημόσιο, Telecoms, κ.λ.π.).

ΕΙΔΙΚΟΤΕΡΕΣ ΔΙΑΠΙΣΤΩΣΕΙΣ ΣΕ ΣΥΓΚΕΚΡΙΜΕΝΟΥΣ ΤΟΜΕΙΣ

Χρήση η-υπογραφών στο Δημόσιο Τομέα και εφαρμογή του π.δ. 342/02

Οι ρυθμίσεις του π.δ. 342/02 «*για την διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, ΝΠΔΔ και ΟΤΑ ή μεταξύ αυτών και των φυσικών ή προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων*» (που εκδόθη στα πλαίσια των προβλέψεων των παραγράφων 19 και 20 του άρ. 14 του ν. 2672/98) κρίθηκε ότι είναι **πολύ ασαφής** και ότι δημιουργεί πολλά ερωτηματικά ως προς τον τρόπο εφαρμογής του.

Παρατηρήθηκε επίσης ότι το παραπάνω π.δ. απαιτεί για την ηλεκτρονική διακίνηση των αναφερόμενων σε αυτό δημοσίων εγγράφων (αποφάσεις, πιστοποιητικά, βεβαιώσεις, γνωμοδοτήσεις, πρακτικά, εισηγήσεις, & εκθέσεις) να φέρουν '**ψηφιακή υπογραφή'**, η οποία ταυτίζεται –βάσει των ορισμών του π.δ. 150/01 και του ά. 14 του ν. 2672/98- με την '**προηγμένη ηλεκτρονική υπογραφή**'. Αυτό σημαίνει ότι, 'δεν απαιτείται' η υπογραφή αυτή να στηρίζεται υποχρεωτικά σε «*αναγνωρισμένο πιστοποιητικό»*, ούτε να δημιουργείται με χρήση «*ασφαλούς διάταξης δημιουργίας υπογραφής*» -τα οποία, σύμφωνα με το άρ. 3§1 του π.δ. 150/2001, αποτελούν **βασικές προϋποθέσεις** ώστε μια «ψηφιακή υπογραφή» να θεωρείται 'ex lege' ισοδύναμη με την ιδιόχειρη παραδοσιακή υπογραφή,

Εκτιμήθηκε ότι η συγκεκριμένη προσέγγιση (:όχι χρήση 'αναγνωρισμένων' αλλά χρήση 'απλών ψηφιακών' υπογραφών), επιλέχθηκε -τουλάχιστον προς το παρόν- λόγω του χαμηλού ποσοστού διάθεσης ανάλογων προϊόντων/υπηρεσιών στην ελληνική αγορά, και την έλλειψη έκδοσης –κατά την έκδοση του π.δ.- σχετικού Κανονισμού 'διαπίστευσης' και 'διαπίστωσης' των σχετικών υπηρεσιών και προϊόντων από την ΕΕΤΤ. Πιθανότατα, η προσέγγιση αυτή θα τροποποιηθεί στο μέλλον, μιας και οι προδιαγραφές του εξελισσόμενου έργου 'Σύζευξις' (Υποέργο 9) αναφέρονται σε χρήση '**έξυπνης κάρτας**' (= μέρος 'ασφαλούς διάταξης δημιουργίας υπογραφής') και έκδοση '**αναγνωρισμένων'** ηλεκτρονικών πιστοποιητικών από τον ανάδοχο ΠΥΠ προς τους δημόσιους υπαλλήλους!

Επίσης αναφέρθηκε ότι η 'έκδοση' ενός δημοσίου εγγράφου, σύμφωνα με την υφιστάμενη νομοθεσία και πρακτική, (π.χ. ΚΕΔΥ, αλλά και άλλες ειδικότερες προβλέψεις & εγκυκλίους αναλόγως το είδος του εκδιδόμενου εγγράφου), προϋποθέτει συχνά μια συγκεκριμένη 'ροή' η οποία απαιτεί μια αλληλουχία υπογραφών από διαφορετικά πρόσωπα (π.χ. εισηγητής, προϊστάμενος, αρμόδιος υπάλληλος, κ.λ.π.). Πάντως, διαπιστώθηκε ότι στο τελικό δημόσιο έγγραφο που χρησιμοποιείται στην συναλλαγή με τον πολίτη **αρκεί η ύπαρξη μόνο μιας υπογραφής**, **αυτής του τελευταίου αρμόδιου υπαλλήλου-αποστολέα**, ο οποίος εγγυάται την τήρηση των προϋποθέσεων έκδοσης του εγγράφου ή, άλλως, ότι το ηλεκτρονικό δημόσιο έγγραφο που υπογράφει και στέλνει στον πολίτη ο δημόσιος υπάλληλος (με αυτήν του ιδιότητα, η οποία πρέπει να αναγράφεται στο σχετικό πιστοποιητικό!) μπορεί να θεωρηθεί ότι αποτελεί 'ακριβές αντίγραφο' του επισήμου αντίστοιχου εγγράφου που διατίθεται στο αρχείο της υπηρεσίας.

Επειδή, όμως, η υφιστάμενη ευρωπαϊκή προτυποποίηση των ηλεκτρονικών υπογραφών δεν προβλέπει κάποιο άλλο τρόπο για τον προσδιορισμό της πρόθεσης του υπογράφοντα κατά την εναπόθεση της υπογραφής του σε ένα (ηλεκτρονικό) έγγραφο, (π.χ. για 'δήλωση βουλήσεως', για 'επικύρωση ακριβούς αντιγράφου', για 'επιβεβαίωση της παραλαβής/λήψης γνώσης', κ.λ.π.) θα πρέπει ο ρόλος και η σημασία μιας (μη απόκηρυσσόμενης) υπογραφής **να προσδιορίζεται σαφέστατα** είτε από το περιεχόμενο του ίδιου του εγγράφου (με σχετικές φράσεις στο τέλος του, όπως π.χ. 'Ο δηλών', 'Ο βεβαιών', 'Θεωρείται ως Ακριβές Αντίγραφο', κ.λ.π.). είτε με την χρήση μιας συγκεκριμένης και γνωστής '**Πολιτικής Υπογραφής**' ('Signature Policy' –βλ. σχετικά και πρότυπο ETSI TS 101 733) η οποία θα συνδέεται με το συγκεκριμένο έγγραφο και θα καθορίζει όλους τους κανόνες που θα διέπουν την συγκεκριμένη υπογραφή. (π.χ. το **Εθνικό Τυπογραφείο** μπορεί να καθορίσει και να δημοσιεύσει μια '**Πολιτική Υπογραφής των ΦΕΚ'** που δημοσιεύει ηλεκτρονικά, η οποία να προσδιορίζει ότι η υπογραφή των υπαλλήλων της στα 'έγγραφα' αυτά έχει το νόημα της επιβεβαίωσης της 'γνησιότητας' του (ηλεκτρονικού) ΦΕΚ, ως 'πιστού αντιγράφου' του επίσημου έντυπου ΦΕΚ που έχει εκδώσει!)

Παρατηρήθηκε, ακόμη, ότι τα **προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου** που υπάρχουν σήμερα στην αγορά, δίνουν την δυνατότητα να 'υπογράφει' κανείς, ΜΟΝΟ ΟΛΟΚΛΗΡΟ ΤΟ ΜΗΝΥΜΑ (δηλαδή ως ένα 'σύνολο', μαζί με τα όποια συνημμένα σ' αυτό αρχεία) και όχι κάποιο συγκεκριμένο συνημμένο ηλεκτρονικό έγγραφο χωριστά! Μάλιστα, το νόημα αυτής της 'ψηφιακής υπογραφής' ('Digital Signature') του μηνύματος, σύμφωνα με το σχετικό πρωτόκολλο **S/MIME** (Secure/Multipurpose Internet Mail Extensions) που την προβλέπει, είναι αυτό της '**επιβεβαίωσης της προέλευσης'** ('authentication' ή/και 'identification') και της '**ακεραιότητας'** ('integrity') του μηνύματος, και ΟΧΙ αυτό της απόδοσης '**νομικής δέσμευσης**' ('μη

αποκήρυξη'/'no repudiation') του υπογράφοντα-αποστολέα σε σχέση με το περιεχόμενο του μηνύματος! Με τον τρόπο αυτό όμως, ένα 'ηλεκτρονικό δημόσιο έγγραφο' (π.χ. ένα 'πιστοποιητικό γεννήσεως', ή 'φορολογικής ενημερότητας') **δεν** μπορεί να σταλεί υπογεγραμμένο **ξεχωριστά** από το 'εισαγωγικό μήνυμα' (αυτό που πιθανώς θα γράφει ΄Κύριε τάδε, Σε απάντηση της υπ' αριθμ. ΧΧ αίτησής σας, σας εσωκλείω συννημένο το υπ' αριθ. ΝΝΝ έγγραφο…κ.λ.π.') που του έστειλε ο σχετικός υπάλληλος και στο οποίο θα πρέπει φυσιολογικά να βρίσκεται συνημμένο. Έτσι όμως, ο πολίτης που τυχόν λαμβάνει με αυτό τον τρόπο ένα έγγραφο **θα πρέπει να το χρησιμοποιήσει** (π.χ. για να το στείλει σε μια άλλη υπηρεσία που του το ζήτησε ως δικαιολογητικό για κάποια άλλη αίτησή του!) **μαζί με ολόκληρο το 'μήνυμα αποστολής'** με το οποίο το παρέλαβε (-αλλιώς **δεν** θα επαληθεύεται η υπογραφή!). Η λύση για το θέμα αυτό είναι η χρησιμοποίηση ειδικών προγραμμάτων, -αυτόνομων ή ακόμη και 'πρόσθετων' (plug-ins) στο πρόγραμμα διαχείρισης της αλληλογραφίας-, που αποκαλούνται '**File Signers'** και τα οποία επιτρέπουν την υπογραφή συγκεκριμένων αρχείων (π.χ. μορφής '.doc' ή '.pdf') και μάλιστα με πιστοποιητικά που στο πεδίο τους 'Χρήση Κλειδιού' (Key Usage) έχουν την ένδειξη 'No Repudiation', η οποία θεωρείται ως η πλέον κατάλληλη για την υπογραφή εγγράφων!

Ένα άλλο σημείο που εντοπίστηκε , είναι ότι πολλά εκδιδόμενα δημόσια έγγραφα (π.χ. πιστοποιητικά) έχουν **μια συγκεκριμένη περίοδο ισχύος** (κάποια 3 μήνες, άλλα 6 μήνες, κ.λ.π.) την οποία και αναφέρουν στο 'σώμα' τους. Όμως, για να είναι δυνατόν να επαληθεύεται η ηλεκτρονική υπογραφή τους καθόλο αυτό το διάστημα, ακόμα και στην περίπτωση που έχει λήξει ή έχει ανακληθεί το σχετικό πιστοποιητικό που την υποστηρίζει, απαιτείται η επιπρόσθετη εναπόθεση μιας '**Χρονοσήμανσης'** (ή χρήση άλλης αντίστοιχης μεθόδου εξασφάλισης των στοιχείων επαλήθευσης της ισχύος της υπογραφής σε μια συγκεκριμένη χρονική στιγμή) πάνω στο ίδιο το υπογεγραμμένο έγγραφο!

Μια αξιόπιστη '**Υπηρεσία Χρονοσήμανσης**' των διακινούμενων εγγράφων παρεχόμενη από το ίδιο το Δημόσιο (με δική του υποδομή ή μέσω 'outsourcing'), θα μπορούσε, μάλιστα, εκτός από την μακροχρόνια επικύρωση των εγγράφων, να παίξει και τον ρόλο μιας '**ηλεκτρονικής χαρτοσήμανσης**' των (ηλεκτρονικών) εγγράφων, η οποία θα μπορούσε (όντας αμειβόμενη από τους πολίτες-χρήστες της) να αποφέρει και σχετικά έσοδα στο Δημόσιο!

Τέλος, διαπιστώθηκε ότι το σημαντικότερο εμπόδιο για την πρακτική εφαρμογή του π.δ. 342/02 είναι η **έλλειψη σχετικής υποδομής** (υπολογιστές, κατάλληλο λογισμικό, πρόσβαση στο internet, κ.λ.π.) στις υπηρεσίες του δημοσίου καθώς και η έλλειψη σχετικής εκπαίδευσης του προσωπικού στην χρήση των νέων μεθόδων ηλεκτρονικής επικοινωνίας. Αναφέρθηκε επίσης και το

γεγονός ότι οι περισσότεροι δημόσιοι υπάλληλοι δεν έχουν δική τους (ατομική) διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail) και συνήθως δεν γνωρίζουν πώς να λειτουργούν με τέτοια 'εργαλεία'· εξάλλου, λόγω και της έλλειψης ανάλογης 'συστηματοποίησης' των καθιερωμένων διαδικασιών, είναι σχεδόν αδύνατο να αντικαταστήσουν σήμερα τις 'παραδοσιακές εργασίες/ροές' τους με άλλες 'σύγχρονες' που θα χρησιμοποιούν ηλεκτρονική υπογραφή, διακίνηση και αρχειοθέτηση!

Με δεδομένες τις παραπάνω παρατηρήσεις, προσπάθησα να συνοψίσω και να απαντήσω στο ερώτημα '**-Πώς μπορεί (και πρέπει) να ερμηνευτεί και να εφαρμοστεί το π.δ. 342/02 ?**', δίνοντας τις εξής επιμέρους προτάσεις/απαντήσεις:

1) Τι πρέπει, τελικά, να υπογράφεται ηλεκτρονικά?

Αν και το π.δ αναφέρει ως 'τρόπο διακίνησης' των αναφερόμενων σ' αυτό εγγράφων την χρήση 'ηλεκτρονικού ταχυδρομείου', δεν γίνεται σαφές ποιο ακριβώς δεδομένο θα πρέπει να φέρει την 'ψηφιακή υπογραφή' (το 'μήνυμα' ή το τυχόν 'συνημμένο (δημόσιο) έγγραφο' που διακινείται με αυτό ? Έτσι, θεωρώ ότι το ιδανικότερο είναι **να υπογράφεται το διακινούμενο 'έγγραφο**', και, πιθανώς, (-προαιρετικά & επιπροσθέτως-) και το ίδιο το (συνολικό) 'ηλεκτρονικό μήνυμα'.

2) Πόσοι και Ποιοι πρέπει να υπογράφουν ?

Σύμφωνα και με τις παραπάνω παρατηρήσεις, αρκεί και πρέπει να υπογράφει ένα διακινούμενο δημόσιο ηλεκτρονικό έγγραφο (μόνο) **ο αρμόδιος υπάλληλος για την έκδοση ή την επικύρωσή του** (ανεξάρτητα από την τυχόν προϋπόθεση έγκριση-υπογραφής του εγγράφου από τον προϊστάμενό του) ο οποίος –συνήθως, χωρίς, όμως, να είναι απαραίτητο-, αναλαμβάνει και την αποστολή του εγγράφου στον πολίτη ή σε κάποιον άλλον συνάδελφό του. Όταν αποστολέας είναι ο πολίτης (π.χ μια αίτηση) θα πρέπει να υπογράψει - φυσικά- ο ίδιος, (εκτός και αν ο υπογράφων επισυνάψει σχετική ηλεκτρονική και υπογεγραμμένη εξουσιοδότηση?) με μία πιστοποιημένη υπογραφή του από οποιονδήποτε κατάλληλο ΠΥΠ.

3) Με ποιο τρόπο & με ποια εργαλεία θα τίθεται η ηλεκτρονική υπογραφή?

Για την υπογραφή ενός συγκεκριμένου (ηλεκτρονικού) εγγράφου/αρχείου πρέπει να χρησιμοποιηθεί **ειδικό λογισμικό 'υπογραφής αρχείων' (File Signer)**, το οποίο συνήθως διατίθεται από διάφορους κατασκευαστές λογισμικού είτε ως αυτόνομο λογισμικό. είτε ως πρόσθετο λογισμικό (plug-in) σε εφαρμογές διαχείρισης ηλ. ταχυδρομείου, και το οποίο, ανεξάρτητα από τον τύπο του εγγράφου που υπογράφεται (π.χ. '.txt', '.pdf' ή '.doc'), δημιουργεί ένα τελικό αρχείο του τύπου 'PKCS#7' (συνήθως με κατάληξη '.p7m' ή 'p7k') που περιλαμβάνει το ίδιο

το αρχικό έγγραφο ΜΑΖΙ με την υπογραφή του. Όσον αφορά την (προαιρετική) 'υπογραφή αυθεντικότητας' και του 'συνολικού ηλεκτρονικού μηνύματος', αυτή μπορεί να γίνεται με τις **ενσωματωμένες δυνατότητες ηλεκτρονικής υπογραφής** (S/MIME) που διαθέτουν τα περισσότερα δημοφιλή προγράμματα διαχείρισης ηλ. ταχυδρομείου (και τα οποία μπορούν να ρυθμιστούν να υπογράφουν αυτόματα κάθε εξερχόμενο ηλεκτρονικό μήνυμα!).

4) Τι είδους ψηφιακή υπογραφή πρέπει να χρησιμοποιούν?

Ανεξάρτητα από το εάν η υπογραφή του εγγράφου θα πρέπει να υποστηρίζεται από 'αναγνωρισμένο' ή όχι πιστοποιητικό, το πιστοποιητικό αυτό θα πρέπει να αναγράφει και την **ιδιότητα του δημόσιου υπαλλήλου** (ως τέτοια!). Λόγοι διαλειτουργικότητας[19] αλλά και λόγοι ασφάλειας[20] επιβάλλουν τα (δημόσια) έγγραφα να υπογράφονται με 'δεδομένα δημιουργίας υπογραφής' ('ιδιωτικό κλειδί' του υπογράφοντα) τα οποία θα προορίζονται μόνο για υπογραφές τύπου '**NonRepudiation'** (μη αποκήρυξης) σύμφωνα και με τις ενδείξεις στο σχετικό πιστοποιητικό τους, ενώ τα ηλεκτρονικά μηνύματα καθαυτού, θα πρέπει να υπογράφονται με διαφορετικό 'ιδιωτικό κλειδί' του υπογράφοντα (ή/και του αποστολέα του), του οποίου το πιστοποιητικό θα επιτρέπει την χρήση του για τέτοιες εφαρμογές φέροντας την ένδειξη '**DigitalSignature**' (στο πεδίο 'Χρήση Κλειδιού'/'Key Usage' του πιστοποιητικού)

5) Πώς θα επαληθεύεται η ψηφιακή υπογραφή ?

Η επαλήθευση μιας ψηφιακής υπογραφής από τον αποδέκτη της, απαιτεί την χρήση από αυτόν **κατάλληλου λογισμικού** ('συμβατού' με το λογισμικό δημιουργίας της υπογραφής, με το οποίο μπορεί και να ταυτίζεται). Η ευρύτατη, όμως, χρήση τέτοιου 'διαλειτουργικού' λογισμικού για την επαλήθευση των υπογραφών, προϋποθέτει την τυποποίησή του και τον καθορισμό συγκεκριμένων προδιαγραφών, και σίγουρα θα βοηθούσε η 'διαπίστωση' της τήρησης αυτών των προδιαγραφών από την (αρμόδια) ΕΕΤΤ ή/και από άλλη αρμόδια εθνική αρχή άλλου κράτους-μέλους της ΕΕ. Σε κάθε περίπτωση όμως, όπου ζητείται η δυνατότητα μακροχρόνιας επαλήθευσης της ηλεκτρονικής υπογραφής ενός εγγράφου, θα πρέπει να προβλεφθούν και να ρυθμιστούν και σχετικές υπηρεσίες '**Χρονοσήμανσης'** των υπογεγραμμένων εγγράφων! Οι σχετικοί κανόνες και προϋποθέσεις (για την υπογραφή και) την επαλήθευση των υπογραφών δημοσίων εγγράφων θα

---

*[19] μιας και οι περισσότερες εφαρμογές '**file-signing**' στην Ευρώπη χρησιμοποιούν την συγκεκριμένη 'μέθοδο' υπογραφής των 'ηλεκτρονικών εγγράφων'*

[20] όπως προβλέπει εξάλλου και το –δημοσιευθέν, πλέον, στην επίσημη Εφημερίδα των Ε.Κ.- πρότυπο CWA 14167-1,(παρ. ΚΜ 3.4)

μπορούσαν να καθοριστούν και να κοινοποιηθούν μέσω σχετικών '**Πολιτικών Υπογραφής**' που θα καθορίσει το Δημόσιο.

Η διαλειτουργικότητα των η-υπογραφών στον Τραπεζικό Τομέα

Επισημάνθηκε ότι οι εφαρμογές του Τραπεζικού τομέα (e-banking) που δύνανται να χρησιμοποιήσουν ηλεκτρονικές υπογραφές και πιστοποιητικά, είναι συνήθως '**κλειστές εφαρμογές**' (στις οποίες συναλλάσσεται μία μόνο τράπεζα με τους πελάτες της), και ως τέτοιες, διέπονται κυρίως από **συμβατικούς όρους** -οι οποίοι καθορίζουν την έκταση της αναγνώρισης των χρησιμοποιούμενων υπογραφών- και όχι άμεσα από το σχετικό θεσμικό και ρυθμιστικό πλαίσιο.

Με δεδομένη την **έλλειψη ενός κοινού ρυθμιστικού πλαισίου**, κάθε τραπεζικός οργανισμός αναπτύσσει τις δικές του εφαρμογές με γνώμονα το προφίλ των πελατών και τις ιδιαίτερες ανάγκες των σχεδιαζόμενων υπηρεσιών, χωρίς να λαμβάνονται υπ' όψιν στοιχεία διαλειτουργικότητας των χρησιμοποιούμενων ηλεκτρονικών υπογραφών και πιστοποιητικών με άλλες εφαρμογές τρίτων. Η '**διατραπεζικότητα'** των χρησιμοποιούμενων εργαλείων, δηλαδή η δυνατότητα κοινής χρήσης των ίδιων υπογραφών και πιστοποιητικών των πελατών από όλες τις Τράπεζες, αποτελεί απώτερο στόχο, ο οποίος όμως, προς το παρόν τουλάχιστον, παραγκωνίζεται από την προτεραιότητα που δίνεται στην αντιμετώπιση των εσωτερικών προβλημάτων που αναδεικνύονται κατά την ενσωμάτωση και χρήση των νέων εργαλείων ασφάλειας στα υπάρχοντα συστήματα του κάθε τραπεζικού οργανισμού.

Επισημάνθηκε, επίσης, ότι οι διαφορετικοί τρόποι ονομασίας (*'naming policy', π.χ. χρήση λατινικών ή όχι χαρακτήρων, αναγραφή ή όχι του πατρώνυμου, της ημερομηνίας Γέννησης, χρήση ψευδονύμων, κ.λ.π.*) και η αναγραφή διαφορετικών στοιχείων ταυτοποίησης (*π.χ. ΑΦΜ, αριθμού αστυνομικής ταυτότητας ή αριθμού τραπεζικού λογαριασμού*) των πελατών-υποκειμένων στα ηλεκτρονικά πιστοποιητικά, αποτελεί **ιδιαίτερο πρόβλημα για την διαλειτουργικότητα** των πιστοποιητικών αυτών μεταξύ διαφορετικών τραπεζών. Εκφράστηκε και η άποψη ότι οι διαφορετικές ανάγκες κάθε τράπεζας (και κάθε οργανισμού γενικά) επιβάλλουν την διαφοροποίηση στα στοιχεία που εμφανίζονται στα χρησιμοποιούμενα πιστοποιητικά. Παρατηρήθηκε όμως σχετικά, ότι εάν υπάρξει ένας κοινός και ικανοποιητικός τύπος περιγραφής της ταυτότητας των πελατών, οι ιδιαίτερες ανάγκες για διαχείριση δικαιωμάτων πρόσβασης των πελατών στις υπηρεσίες των τραπεζών (και κάθε άλλου οργανισμού) μπορούν να λυθούν σε 'επίπεδο εφαρμογής' (*π.χ. με την χρήση σχετικών εσωτερικών βάσεων δεδομένων των τραπεζών, ή, ακόμη, και με την έκδοση ξεχωριστών 'πιστοποιητικών ιδιοτήτων' του πελάτη για χρήση τους με τις σχετικές υπηρεσίες της κάθε τράπεζας ή εταιρίας*).

Αν και τα θέματα ασφάλειας κρίνονται ως 'καθοριστικής σημασίας' για την αξιοπιστία των ηλεκτρονικών συναλλαγών -ιδίως στον τραπεζικό τομέα-, το **κόστος ανάπτυξης και συντήρησης** της σχετικής υποδομής είναι μεγάλο και δεν μπορεί να μετατεθεί εύκολα στον πελάτη (μιας και αυτός θεωρεί δεδομένη την παροχή ασφάλειας από την τράπεζά του), και αυτό αποτελεί έναν ακόμη ανασταλτικό παράγοντα για την αντικατάσταση των 'κλασσικών' μεθόδων ασφαλείας που χρησιμοποιούν ως σήμερα οι Τράπεζες. Η υιοθέτηση μιας **κοινής 'Πολιτικής Ηλεκτρονικής Υπογραφής΄** (Π.Η.Υ.) από όλες τις Τράπεζες (μέσω της Ένωσης Τραπεζών Ελλάδος) ενδεχομένως:

- θα έκανε πιο σαφείς τους όρους χρήσης των ηλεκτρονικών υπογραφών και πιστοποιητικών,
- θα διαμοίραζε το κόστος έκδοσης των (κοινών) πιστοποιητικών,
- θα αύξανε την χρησιμότητα και την αξιοπιστία των συγκεκριμένων μεθόδων, και
- τελικά θα αποτελούσε πιθανό κίνητρο για τις Τράπεζες και τους πελάτες τους για την ανάπτυξη και χρήση σχετικών εφαρμογών.

Με αφορμή τα παραπάνω, εξετάσθηκε η προοπτική δημιουργίας μιας **κοινής πολιτικής ηλεκτρονικών υπογραφών μεταξύ των Ελληνικών Τραπεζών**, για την οποία όμως εκφράστηκαν αρκετές επιφυλάξεις και τέθηκαν πολλά 'καυτά' ζητήματα από τους εκπροσώπους των Τραπεζών που συμμετείχαν στις εργασίες.

Στα πλαίσια αυτά επισημάνθηκαν και εξετάσθηκαν **δύο διαφορετικά σενάρια**: Είτε (***α΄ σενάριο***) ένα κοινό αλλά '**κλειστό'** τραπεζικό σύστημα έκδοσης ηλεκτρονικών πιστοποιητικών προς τους πελάτες(με συγκεκριμένα χαρακτηριστικά), τα οποία θα επιτρέπεται (και θα επιβάλλεται) να χρησιμοποιούνται αποκλειστικά για τις τραπεζικές τους συναλλαγές, είτε (***β΄ σενάριο***) προσδιορισμός κάποιων «κοινών βασικών προδιαγραφών-απαιτήσεων» (*π.χ. αναγνωρισμένα πιστοποιητικά με αναγραφή επιθέτου, ονόματος, έτους γέννησης και Α.Φ.Μ. -ή/και άλλου μοναδικού 'κωδικού ταυτότητας' των υποκειμένων-, καθώς και προσδιορισμός συγκεκριμένων ορίων στο ύψος των επιτρεπόμενων συναλλαγών*) και **αποδοχή**, εκ μέρους των τραπεζών, όλων των πιστοποιητικών 'της αγοράς' *(σημ.: -τα οποία ο χρήστης τους θα μπορεί να τα χρησιμοποιεί και σε άλλες εφαρμογές, π.χ. e-government-*) που θα καλύπτουν τις προϋποθέσεις αυτές (*χωρίς να αποκλείεται και ο συνδυασμός και των δύο σεναρίων*)!

Και στις δύο περιπτώσεις τέθηκαν τα εξής ζητήματα-επιφυλάξεις:

α) **Ανταγωνισμού** και **μάρκετινγκ,** όπως π.χ. «*γιατί ο πελάτης ΜΟΥ να χρησιμοποιεί π.χ. μια κάρτα (smart-card) με το λογότυπο ενός τρίτου ή μιας ΆΛΛΗΣ τράπεζας και όχι με το ΔΙΚΟ ΜΟΥ λογότυπο?*». Αντιτάχθηκε όμως και το γεγονός ότι ο χρήστης δεν είναι δυνατόν να υποχρεωθεί στο

να έχει μια διαφορετική ηλεκτρονική υπογραφή (με ό,τι αυτό σημαίνει: *πολλαπλές διαδικασίες πιστοποίησης, άλλα κρυπτογραφικά κλειδιά σε ξεχωριστό φορέα και άλλα πιστοποιητικά με διαφορετικούς το καθένα όρους χρήσης*) για κάθε μία τράπεζα με την οποία συνεργάζεται, και επιπρόσθετα άλλη(-ες) διαφορετική(-ές) για τις εφαρμογές ηλεκτρονικής διακυβέρνησης, και άλλες για άλλες εφαρμογές! Εξάλλου χαρακτηριστικό 'καλό παράδειγμα' αποτελεί η κοινή χρήση των τερματικών VISA, ανεξάρτητα της τράπεζας που τα χορήγησε!

β) **ασφάλεια της ταυτοποίησης των πελατών**, με δεδομένο το ότι οι τράπεζες προβαίνουν οι ίδιες σε αυστηρό έλεγχο της ταυτότητας των πελατών τους και ότι φαντάζει ιδιαίτερα δύσκολο σε μια τράπεζα να προχωρήσει απευθείας σε απομακρυσμένη ηλεκτρονική συναλλαγή με έναν πελάτη που ποτέ δεν έχει αντικρίσει πρόσωπο με πρόσωπο! Το ζήτημα αυτό ξεπερνιέται όμως από το γεγονός ότι οι διαδικασίες ταυτοποίησης ή/και νομιμοποίησης των υποκειμένων είναι –σε μεγάλο βαθμό- 'τυποποιημένες' και ο ΠΥΠ που θα εκδώσει '***αναγνωρισμένα πιστοποιητικά***' (ή κάτι παρόμοιο σε 'κλειστό σύστημα'), υποχρεούται σε έναν τέτοιο έλεγχο, και σε κάθε περίπτωση αναλαμβάνει αυτός την ευθύνη να **εγγυηθεί** '*προς κάθε τρίτο*' (*ή, μόνο προς τις τράπεζες στη περίπτωση του 'α΄ σεναρίου'*) για την ταυτότητα του υποκειμένου. Έτσι, στο βαθμό που οι συναλλαγές της τράπεζας με ένα πιστοποιημένο υποκείμενο δεν ξεπερνούν το ύψος των ορίων ευθύνης που πιθανώς έχει ορίσει ο ΠΥΠ στο χρησιμοποιούμενο πιστοποιητικό, η τράπεζα δεν κινδυνεύει να μην αποζημιωθεί στην περίπτωση κάποιας 'πλαστοπροσωπίας'.

γ) **επίπεδο πληροφοριακών στοιχείων για τα υποκειμένα-πελάτες**, με δεδομένο ότι ένα ηλεκτρονικό πιστοποιητικό περιορίζεται στην αναγραφή ελάχιστων στοιχείων ταυτοποίησης (και πιθανώς και σε κάποια, μόνο, πιστοποιημένη ιδιότητα) του υποκειμένου της. Πράγματι, το πιστοποιητικό δεν αποτελεί 'βιογραφικό σημείωμα' του υποκειμένου και χρησιμεύει μόνο για την 'ταυτοποίησή' του. Έτσι, τα υπόλοιπα στοιχεία που συνήθως ζητάει μια τράπεζα (*π.χ. οικονομικά στοιχεία, εκκαθαριστικό, άλλα στοιχεία ταυτότητας, νομιμοποιητικά έγγραφα για την εκπροσώπηση μιας εταιρίας, κ.λ.π.*) μπορούν να εξακολουθήσουν να συγκεντρώνονται από τις ίδιες πηγές-έγγραφα που χρησιμοποιούνται και σήμερα *(π.χ. αντίγραφο αστ. ταυτότητας, εκκαθαριστικού, καταστατικού κ.λ.π.*) τα οποία θα στέλνονται σ' αυτήν ταχυδρομικά, ή, -στο βαθμό που καταστεί αυτό δυνατόν-, και ηλεκτρονικά (*με ηλεκτρονικές υπογραφές του εκδότη τους ή/και από το ίδιο το υποκείμενο*)!

δ) **πρόσβαση στη συνολική βάση δεδομένων με τα υποκείμενα**. Στην περίπτωση του '*α΄ σεναρίου*', εφόσον υπάρχει μια κοινή Υπηρεσία Καταχώρησης (Registration Authority) για τα στοιχεία των πιστοποιούμενων, μπορεί να συμφωνείται με τους πελάτες (*μέσω της σχετικής '**σύμβασης συνδρομητή**'*) ότι πρόσβαση θα έχουν όλες οι τράπεζες ή ακόμη και καμία (!), ενώ στο

‘*β΄ σενάριο*’ (όπου χρησιμοποιούνται τρίτοι ΠΥΠ) προβλέπεται από την νομοθεσία ότι οι ΠΥΠ (αναγνωρισμένων πιστοποιητικών) πρέπει να δημοσιεύουν καταλόγους στους οποίους ο ‘καθένας’ μπορεί να έχει πρόσβαση, και οι οποίοι πρέπει να περιλαμβάνουν όλα τα (ενεργά) πιστοποιητικά που εκδίδουν, **εκτός** από αυτά των υποκειμένων που έχουν δηλώσει προς τον ΠΥΠ αντίθετη επιθυμία.

ε) **ονομαστικά πιστοποιητικά και παραβίαση τραπεζικού απορρήτου**. Αν και σε πρώτη σκέψη δείχνει ότι μπορεί να προκύψει σχετικό πρόβλημα, η χρήση ‘ονομαστικών’ πιστοποιητικών δημοσίων κλειδιών των υποκειμένων σε τραπεζικές συναλλαγές *(με παράλληλη ή όχι χρήση τους και σε άλλες εφαρμογές ή σε πολλές διαφορετικές τράπεζες*), δεν παραβιάζουν το σχετικό απόρρητο. Κι αυτό διότι όλες οι συναλλαγές μπορεί να γίνονται με κρυπτογραφημένη επικοινωνία (τύπου SSL/TSL) και ακόμη και στην περίπτωση που θα απαιτείται η **χρονοσήμανση** κάποιων ‘εντολών’ ή ‘συμβάσεων’ του πελάτη με την τράπεζα, η ‘σύνοψη’ (digest) των συγκεκριμένων εγγράφων η οποία απαιτείται να στέλνεται στον (‘τρίτο’) ‘*Πάροχο Υπηρεσιών Χρονοσήμανσης*’ είναι αποτέλεσμα εφαρμογής ειδικών αλγόριθμων κατακερματισμού (*π.χ. SHA-1, MD-5, κ.λπ.*) και **δεν** μπορεί να αποκαλύψει τίποτα σχετικά με το περιεχόμενό τους. Απεναντίας, η έκδοση και χρήση ενός συγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής για ‘αποκλειστική χρήση’ σε μία τράπεζα **αποκαλύπτει** την σχέση του υποκειμένου με την τράπεζα και την κατοχή προσωπικού λογαριασμού του σ’ αυτήν!

στ) **συνωνυμίες των υποκειμένων**, οι οποίες δεν επιτρέπουν στην τράπεζα που είναι αποδέκτης ενός ‘επώνυμου’ πιστοποιητικού πελάτη, να συνδέσει χωρίς αμφιβολία το πρόσωπο του πελάτη με τα στοιχεία π.χ. μιας ‘συνώνυμης’ αστυνομικής ταυτότητας ή ενός ‘συνώνυμου’ εκκαθαριστικού σημειώματος της εφορίας που θα της προσκομίσει ο τελευταίος. Το πρόβλημα αυτό θα μπορούσε να λυθεί με την χρήση και αναγραφή ενός πραγματικού (και όχι ενός ‘αυθαίρετου’) κωδικού ταυτοποίησης ή ‘*subject’s serial number*’ του υποκειμένου (*π.χ. το Α.Φ.Μ. ή τον Αριθμό Αστυν. Ταυτότητας*), τον οποίο θα πιστοποιεί ο σχετικός ΠΥΠ αναγράφοντάς τον στο σχετικό πιστοποιητικό. Σ’ αυτή τη περίπτωση, όμως, θα πρέπει να ληφθούν σοβαρά υπόψη τυχόν ζητήματα ‘προστασίας προσωπικών δεδομένων’ του υποκειμένου (*σ.σ.: βλέπε και επόμενη παράγραφο των πρακτικών*).

ζ) **αναγκαία προσαρμογή της υπάρχουσας μηχανογράφησης** με τη χρήση άλλων κωδικών ταυτοποίησης του πελάτη από τον δικό της ‘κωδικό πελάτη’ ή/και τον ‘αριθμό λογαριασμού’ που χρησιμοποιεί ως τώρα η κάθε τράπεζα (και που θα μπορούσε να εξακολουθεί να χρησιμοποιεί τους ίδιους, εάν έκδιδε αυτή τα δικά της πιστοποιητικά προς τον πελάτη). Πράγματι, αποτελεί ένα

πρόβλημα, το οποίο όμως λύνεται εύκολα με την δημιουργία μιας «ενδιάμεσης βάσης δεδομένων αντιστοίχησης» των στοιχείων των πιστοποιητικών με τους υπάρχοντες κωδικούς πελατών της τράπεζας (τους οποίους, έτσι, θα μπορεί να εξακολουθεί να χρησιμοποιεί στην εσωτερική μηχανογράφησή της).

Χρήση η-υπογραφών στην κινητή τηλεφωνία (m-commerce)

Η χρήση των **ηλεκτρονικών υπογραφών μέσω δικτύων κινητής τηλεφωνίας** είναι ακόμα μια εξέλιξη στο χώρο των ηλεκτρονικών υπογραφών. Η ίδια η συσκευή (κινητή) τηλεφώνου που έχουμε όλοι πάνω μας είναι ήδη ένας 'αναγνώστης έξυπνων καρτών' (SIM κάρτες) και θα μπορούσε να αποτελέσει μια διέξοδο στο ζήτημα της εξάπλωσης της χρήσης αναγνωστών έξυπνων καρτών. Τα πρότυπα για ασφαλείς αναγνώστες 'smart-card' (CEN/ISSS 'FINREAD') προβλέπουν την ύπαρξη ξεχωριστού πληκτρολογίου (numeric pad) και οθόνης για τους αναγνώστες καρτών, και τα κινητά τηλέφωνα μπορούν να αποτελέσουν, κάτω από συγκεκριμένες προϋποθέσεις, μια υλοποίηση του παραπάνω προτύπου και να παράσχουν στους χρήστες τους τον απαραίτητο –για δημιουργία αναγνωρισμένων υπογραφών- ασφαλή αναγνώστη 'έξυπνων καρτών' (μέρος της απαιτούμενης συνολικής 'ασφαλούς διάταξης δημιουργίας υπογραφής', σύμφωνα με το θεσμικό πλαίσιο).

Αναγνωρίσθηκε η περιορισμένη δυνατότητα των ως σήμερα χρησιμοποιούμενων κινητών τηλεφώνων 2^{ης} γενιάς για παροχή προηγμένων υπηρεσιών οι οποίες απαιτούν χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών. Αυτό όμως αλλάζει δραματικά με τον ερχομό των **δικτύων και των συσκευών 3^{ης} γενιάς (3G)** *–ακόμα και στο σημερινό περιβάλλον της αποκαλούμενης 2.5 G-* όπου οι δυνατότητες ανάπτυξης σχετικών εφαρμογών είναι εφάμιλλες με αυτές των προσωπικών υπολογιστών και του internet. Επιπροσθέτως, τα κινητά τηλέφωνα και οι συσκευές PDAs, λόγω της φορητότητας και της δυνατότητας για ασύρματη επικοινωνία (*Bluetooth ή/και IR*) με άλλα τερματικά (*ATMs, POSs, κ.λ.π.*) που διαθέτουν, αποτελούν **ιδανικό μέσον** για την ανάπτυξη πολλών σχετικών εφαρμογών, όπως η- πληρωμών (*e-payments*) και η-εισιτηρίων (*e-ticketing*).

Επισημάνθηκε ότι οι **SIM Cards** που χρησιμοποιούνται στα κινητά τηλέφωνα, ως 'smart cards' που είναι, **έχουν** δυνατότητα ασφαλούς αποθήκευσης και χρήσης των κλειδιών του χρήστη και ότι για αυτό τον λόγο τα κινητά τηλέφωνα μπορούν υπό προϋποθέσεις να λειτουργήσουν ως 'ασφαλείς διατάξεις δημιουργίας ηλεκτρονικής υπογραφής' για την δημιουργία 'αναγνωρισμένων ηλεκτρονικών υπογραφών'. Επιπλέον, **νέες τεχνολογίες και μέθοδοι**, όπως αυτή της 'κεντρικής διαχείρισης κλειδιών υπογραφής' (signature server) και νέες εξελιγμένες συσκευές (*π.χ. με την δυνατότητα ελέγχου βιομετρικών στοιχείων, με δυνατότητα υποδοχής άλλων smart-cards κ.λ.π.*),

μπορούν να παράσχουν περισσότερη **ευελιξία** και **ασφάλεια** στην χρήση των κινητών τηλεφώνων ως μέσου δημιουργίας ηλεκτρονικής υπογραφής και διενέργειας προσωπικών συναλλαγών.

Η μελλοντική χρήση των κινητών τηλεφώνων για πρόσβαση σε **προηγμένες υπηρεσίες** και για τη διενέργεια **οικονομικών συναλλαγών** πρέπει να θεωρείται δεδομένη και να ληφθεί υπ' όψιν στους όποιους σχεδιασμούς εφαρμογών 'ηλεκτρονικού επιχειρείν' γίνονται. Οι επενδύσεις για την ανάπτυξη δικτύων και συσκευών 3^{ης} γενιάς θα επιφέρουν πρόσθετες και εξελιγμένες δυνατότητες σε αυτά εφόσον όμως **ανατραπεί η υπάρχουσα αντίληψη των χρηστών**, οι οποίοι συνδέουν την χρήση των συσκευών τους μόνο με εφαρμογές επικοινωνίας (φωνή, SMS, MMS) ή και με απλές υπηρεσίες ψυχαγωγίας (*ring tones, games, MP3/radio player, κ.λπ.*).

ΑΠΑΙΤΗΣΕΙΣ-ΑΝΑΓΚΕΣ ΤΕΛΙΚΟΥ ΧΡΗΣΤΗ

Ανάγκη για μικρό αριθμό απαραίτητων 'ηλεκτρονικών υπογραφών' και φορέων τους.

Η δυνατότητα ενός χρήστη/υπογράφοντα ('*υποκειμένου πιστοποίησης*') να μπορεί να χρησιμοποιήσει τα ίδια μέσα (*π.χ. κρυπτογραφικά κλειδιά, ασφαλείς φορείς, πιστοποιητικά, λογισμικό επικοινωνίας, κ.λ.π.*), τόσο για τη δημιουργία των δικών του 'ηλεκτρονικών υπογραφών' όσο και για την επαλήθευση των ηλεκτρονικών υπογραφών τρίτων, σε περισσότερους από έναν συναλλακτικούς κύκλους, (δηλαδή η '***διαλειτουργικότητα***' όλων των σχετικών εργαλείων και εφαρμογών), αποτελεί ένα σημαντικό ζητούμενο, αφού:

α) θα μειώσει το συνολικό κόστος απαραίτητου εξοπλισμού του χρήστη,

β) θα απλοποιήσει τις λειτουργίες και τις διαδικασίες του χρήστη,

γ) θα περιορίσει τις πολλαπλές 'διαδικασίες ταυτοποίησης' των υποκειμένων,

δ) θα συμβάλει στην δημιουργία της απαραίτητης 'κρίσιμης μάζας' των πιστοποιημένων χρηστών (που θα έχουν την δυνατότητα ηλεκτρονικής υπογραφής τους), που, -*με την σειρά της*-,

ε) θα οδηγήσει σε ανάπτυξη και παροχή περισσότερων υπηρεσιών προς τους χρήστες.

Ανάγκη για προστασία των (ηλεκτρονικών) προσωπικών δεδομένων του

Η 'διαλειτουργικότητα' και η χρήση της ίδιας 'ατομικής' ψηφιακής υπογραφής ενός χρήστη (υποκειμένου πιστοποίησης) σε πολλούς συναλλακτικούς κύκλους, πέρα από τα σημαντικά οφέλη της, θέτει έντονα **ζητήματα προστασίας των προσωπικών δεδομένων** των χρηστών αυτών από πιθανές ανεπίτρεπτες διασταυρώσεις των συναλλαγών τους και την δημιουργία, έτσι, αρχείων με ***ολοκληρωμένα ατομικά 'profile'*** ('**ηλεκτρονικό φακέλωμα'**) τους.

Ιδιαίτερα εξετάσθηκε η περίπτωση της επιλογής και αναγραφής ενός «**πραγματικού» κωδικού ταυτοποίησης** των υποκειμένων (*π.χ. Α.Φ.Μ.* ***ή*** *Αρ. Αστ. Ταυτότητας)*, ο οποίος «*θα αναγράφεται πάντα και σε όλα τα ηλεκτρονικά πιστοποιητικά τους και θα χρησιμοποιείται από όλες τις εφαρμογές*». Κάτι τέτοιο, αν και έχει σχεδόν εφαρμοστεί σε μερικά κράτη (*π.χ. στην Ιταλία όπου σχεδόν όλα τα 'αναγνωρισμένα' πιστοποιητικά χρησιμοποιούν συνδυασμό του ονόματος με τον 'codice fiscale' (ΑΦΜ) του υποκειμένου*) και πραγματικά διευκολύνει τον έλεγχο και την διασταύρωση των πληροφοριών ταυτοποίησης των υποκειμένων, θα ερχόταν σε αντίθεση τόσο με την απόφαση για την μη ισχύ του '***Ενιαίου Κωδικού Αριθμού Μητρώου***' (ΕΚΑΜ) στην Ελλάδα, (*ο οποίος είχε θεσμοθετηθεί με τον ν. 1599/86 και καταργήθηκε -χωρίς ποτέ να ισχύσει- από το ά. 6 του ν. 1988/91*), όσο και με τον σχετικό νόμο 'περί προστασίας προσωπικών δεδομένων' (*ν. 2472/97, άρ. 8§3, το οποίο απαγορεύει την χρήση 'ενιαίου κωδικού' για την διασύνδεση αρχείων προσωπικών δεδομένων, χωρίς προηγούμενη άδεια της σχετικής Αρχής Π.Δ.Π.Χ.*)

Σχετική είναι και η περίπτωση της **Αυστρίας**, όπου έχουν εκδοθεί 'ενιαίοι κωδικοί αριθμοί μητρώου' για κάθε πολίτη, οι οποίοι όμως φυλάσσονται σε μια ασφαλή βάση δεδομένων την οποία διαχειρίζεται η ***Αρχή Προστασίας Προσωπικών Δεδομένων*** της χώρας (η οποία εξασφαλίζει τα εχέγγυα για την σωστή χρησιμοποίηση και προστασία τους). Στο σύστημα που έχουν αναπτύξει σ' αυτήν την βάση, για την κάθε ηλεκτρονική υπηρεσία-εφαρμογή εφαρμόζονται ειδικοί αλγόριθμοι στον ενιαίο αυτό κωδικό, οι οποίοι εξάγουν μόνο τον κατάλληλο κωδικό που απαιτείται απ' τη συγκεκριμένη εφαρμογή, προστατεύοντας έτσι τον πολίτη από την αποκάλυψη της ταυτότητάς του και τη γνωστοποίηση άλλων μη χρήσιμων στοιχείων του στις διαφορετικές εφαρμογές. Σε περίπτωση προβλήματος, ο συναλλασσόμενος με τον υπογράφοντα έχει την δυνατότητα προσφυγής στην Αρχή, η οποία, εφόσον το κρίνει απαραίτητο, διατάσσει την άρση της ανωνυμίας ή/και την διασταύρωση στοιχείων του συγκεκριμένου πολίτη.

Πάντως, η χρήση **διαφορετικών πιστοποιητικών για συγκεκριμένους κύκλους συναλλαγών**, με διαφορετικούς «πραγματικούς» ή/και «αυθαίρετους» (αποδιδόμενους από τους ΠΥΠ) '***κωδικούς ταυτοποίησης***' των υποκειμένων, είναι η πιο ενδεδειγμένη πρακτική που εμποδίζει τη συλλογή και διασταύρωση 'μη ομοειδών πληροφοριών' για το υποκείμενο

Μια τέτοια προσέγγιση, σε συνδυασμό με την παραπάνω απαίτηση για μικρό αριθμό η-υπογραφών κατά χρήστη, εκτιμάται ότι θα μπορούσε να οδηγήσει στην ανάγκη για κατοχή τουλάχιστον 5-6 διαφορετικών (έξυπνων) καρτών για το κάθε χρήστη-υποκείμενο (*με διαφορετικά κρυπτογραφικά κλειδιά και αντίστοιχα πιστοποιητικά)*, που θα συνδέονται και θα αναγράφουν (εκτός από το όνομα ή το ψευδώνυμο) **για παράδειγμα:**

- το '*Α.Φ.Μ.*' του κατόχου στην '***Κάρτα του Πολίτη***' με την οποία θα μπορεί να κάνει συναλλαγές με τις περισσότερες υπηρεσίες e-government (*όπως καταθέσεις φορολογικών και άλλων δηλώσεων και αιτήσεις για έκδοση 'τυπικών' βεβαιώσεων-πιστοποιητικών*),
- τον '*Ενιαίο Αριθμό Κοινωνικής Ασφάλισης*' στην '***Κάρτα Κοινωνικής Ασφάλισης ή Κάρτα Υγείας***' η οποία θα χρησιμοποιείται για συνταξιοδοτικές ή/και ιατροφαρμακευτικές παροχές,
- έναν '*Δια-τραπεζικό Κωδικό*' του (*π.χ. από το σύστημα 'Τειρεσίας'*) για την '***Κάρτα Τραπεζικών (και Χρηματιστηριακών) Συναλλαγών***',
- την επαγγελματική ιδιότητα και τον '*Αριθμό Μητρώου*' του συλλόγου ή του επιμελητηρίου στο οποίο ανήκει στην '***Επαγγελματική Κάρτα***' του την οποία θα μπορεί (ή θα πρέπει) να χρησιμοποιεί στις σχετικές συναλλαγές του εάν είναι ελεύθερος επαγγελματίας (*π.χ. Δικηγόρος, Ιατρός, Μηχανικός, κ.λπ.*),
- τον '*Αριθμό Διαβατηρίου*' για το '***Ηλεκτρονικό Διαβατήριο***' που πιθανότατα θα πρέπει σύντομα (*σ.σ.: βλέπε πρόσφατα μέτρα για είσοδο σε ΗΠΑ*) να αποκτήσει και το οποίο θα μπορεί να χρησιμοποιείται και σε διασυνοριακές συναλλαγές,
- ένα '*αυθαίρετο κωδικό*' που του αποδίδεται από έναν ΠΥΠ σε κάθε (*επώνυμο ή ψευδώνυμο, αναγνωρισμένο ή μη*) '***γενικό πιστοποιητικό'*** του, το οποίο θα μπορεί να χρησιμοποιεί σε διάφορες άλλες δοσοληψίες της ιδιωτικής αγοράς (*on-line shopping, κατάρτιση ιδιωτικών συμβάσεων, κ.λ.π.*), κ.ό.κ.

Σχετική με την παραπάνω απαίτηση είναι και η δυνατότητα του χρήστη να δημοσιοποιεί επιλεκτικά ο ίδιος, όπου και όποτε χρειάζεται, συγκεκριμένα προσωπικά στοιχεία του, αντί να παραθέτει διαρκώς το σύνολο των προσωπικών στοιχείων του που μπορεί να περιέχονται σε ένα πιστοποιητικό. Μια λύση σ' αυτό είναι η έκδοση και η (επιλεκτική) χρήση πρόσθετων «***πιστοποιητικών ιδιοτήτων***» ('attribute certificates') για το χρήστη-υποκείμενο. Τα πιστοποιητικά αυτά 'δένονται' με το βασικό '***πιστοποιητικό δημοσίου κλειδιού***' του υποκειμένου, και μπορούν να συμπεριλάβουν οποιουδήποτε είδους πρόσθετη πληροφορία για το υποκείμενο, όπως π.χ. έναν 'πραγματικό' κωδικό ταυτοποίησης (Α.Φ.Μ.).

Έτσι ο κάθε χρήστης μπορεί να έχει π.χ. ένα '**ψευδώνυμο'** βασικό πιστοποιητικό, για τα οποία θα έχει ζητήσει και θα του έχουν εκδοθεί από τον ΠΥΠ (*ο οποίος σ' αυτήν την περίπτωση λειτουργεί και ως 'Attribute Authority'*) πρόσθετα συνδεόμενα πιστοποιητικά ιδιοτήτων, για όσα στοιχεία ταυτοποίησης ή ιδιότητες/ρόλους του αυτός επιθυμεί ή χρειάζεται να χρησιμοποιήσει, και

τα οποία θα μπορεί να συμπεριλάβει -κατ' επιλογήν του- σε ηλεκτρονικές υπογραφές του ώστε να ενημερώσει έτσι αξιόπιστα τον αποδέκτη τους για την συγκεκριμένη 'ιδιότητά' του.

Ανάγκη για αξιόπιστη ενημέρωση, πληροφόρηση και εκπαίδευση

Με δεδομένη την πολυπλοκότητα της τεχνολογίας, αλλά και τις ασάφειες του θεσμικού πλαισίου[21], διαπιστώνεται μεγάλη ανάγκη για την παροχή έγκυρης και αξιόπιστης ενημέρωσης προς τους πολίτες-δυνητικούς χρήστες, η οποία θα ανατρέψει το κλίμα 'σύγχυσης' που επικρατεί σχετικά με τη χρήση, τις λειτουργίες και την νομική αναγνώριση που τυγχάνουν οι διάφορες παραλλαγές της τεχνολογίας των ηλεκτρονικών υπογραφών.

Κρίθηκε επίσης ότι η ολοκλήρωση και η λειτουργία των μηχανισμών διαπίστωσης της ασφάλειας των 'προϊόντων ηλεκτρονικής υπογραφής' και της εθελοντικής διαπίστευσης των ΠΥΠ, υπό την έννοια της παροχής 'επίσημης πληροφόρησης' προς τους τελικούς χρήστες για την πραγματική ποιότητα και ασφάλεια τους, θα συμβάλλει στην ανάπτυξη της εμπιστοσύνης των χρηστών προς τα παρεχόμενα σχετικά προϊόντα και υπηρεσίες.

ΜΕΡΟΣ V: ΣΥΝΟΨΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ & ΠΡΟΤΑΣΕΙΣ

ΣΥΝΟΨΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ

- Οι **ηλεκτρονικές υπογραφές** και τα **ηλεκτρονικά πιστοποιητικά ταυτοποίησης**, -παρά την πολυπλοκότητα που τα χαρακτηρίζει-, αποτελούν σήμερα την μόνη αξιόπιστη λύση για την ταυτόχρονη πιστοποίηση της προέλευσης και τη διασφάλιση της ακεραιότητας των διακινούμενων δεδομένων σε 'ανοικτά δίκτυα'.
- Η μελέτη και η πιστή **τήρηση των σχετικών ευρωπαϊκών νομικοτεχνικών προτύπων** αποτελεί μια βασική μέθοδος για την τεκμηριωμένη συμμόρφωση των υπηρεσιών και των προϊόντων με τις απαιτήσεις της Οδηγίας –ιδίως για την έκδοση και χρήση «αναγνωρισμένων πιστοποιητικών»- , αλλά και για την επίτευξη ευρύτερης διαλειτουργικότητας από τις σχετικές εφαρμογές.

[21] *που έχουν συμβάλει στην την ύπαρξη πολλών 'παρερμηνειών' από τους εφαρμοστές του σε πολλά ειδικότερα θέματα των ηλεκτρονικών υπογραφών*

- Η **τυποποίηση** και η **διαλειτουργικότητα** των παρεχόμενων υπηρεσιών πιστοποίησης και των προϊόντων ηλεκτρονικής υπογραφής αποτελούν βασική προϋπόθεση για την περαιτέρω διάδοση και ενσωμάτωσή τους σε εφαρμογές «*ηλεκτρονικού επιχειρείν*»
- Η σύνταξη σαφών κανόνων και προδιαγραφών (:**Πολιτική Υπογραφής**) για τη χρήση και αποδοχή ηλεκτρονικών υπογραφών και πιστοποιητικών σε συγκεκριμένους τύπους συναλλαγών, θεωρείται απαραίτητη σε καθεστώς «*ελεύθερης παροχής*» των σχετικών υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής
- Ο **Δημόσιος Τομέας**, αναγνωρίζεται ως ο βασικότερος παράγοντας για την προώθηση της χρήσης ηλεκτρονικών υπογραφών στην Ελλάδα, λόγω των πολυάριθμων σχετικών έργων ηλεκτρονικής διακυβέρνησης (*e-government*) που σχεδιάζει και την δημιουργία της απαραίτητης «κρίσιμης μάζας» πιστοποιημένων χρηστών, η οποία θα συμβάλει στην περαιτέρω ανάπτυξη σχετικών υπηρεσιών!
- Θα πρέπει να ενισχυθεί **η εμπιστοσύνη των χρηστών** στις μεθόδους ηλεκτρονικής υπογραφής και να διασφαλιστεί τεχνολογικά **η προστασία των προσωπικών δεδομένων τους** (*τα οποία θα διακινούνται σε ηλεκτρονική μορφή*), από την μη εξουσιοδοτημένη πρόσβαση και συλλογή, προφανώς με την αποδοχή και χρήση *–όπου αυτό είναι εφικτό-* 'ψευδώνυμων πιστοποιητικών', καθώς και την παράλληλη υποστήριξη των εφαρμογών κρυπτογράφησης δεδομένων.

ΠΡΟΤΑΣΕΙΣ & ΣΥΜΒΟΥΛΕΣ

ΠΡΟΣ ΤΗΝ ΠΟΛΙΤΕΙΑ

- Σύνταξη **ενιαίας 'Πολιτικής Ηλεκτρονικής Υπογραφής' του Δημοσίου** για όλες τις υπηρεσίες e-government που αναπτύσσει
- Σύσταση **κεντρικού συμβουλευτικού οργάνου** για την υποστήριξη των παραπάνω υπηρεσιών και την ανταλλαγή τεχνογνωσίας με την σχετική αγορά
- Άμεση ολοκλήρωση και **λειτουργία των θεσμών πιστοποίησης** («Διαπίστωσης» & «Εθελοντικής Διαπίστευσης») των σχετικών προϊόντων και υπηρεσιών που θα συμβάλουν στην ανάπτυξη της εμπιστοσύνης των χρηστών
- Θα πρέπει να εκπονηθεί **ολοκληρωμένη εκστρατεία ενημέρωσης του πολίτη** για την σωστή χρήση των τεχνολογιών η-υπογραφής

ΠΡΟΣ ΤΟΥΣ ΠΥΠ

- Αυστηρή **συμμόρφωση με τα εκδιδόμενα σχετικά ευρωπαϊκά πρότυπα** για την διασφάλιση ενός ελάχιστου επιπέδου διαλειτουργικότητας τόσο σε εθνικό, όσο και σε ενδοκοινοτικό επίπεδο.
- Ανάπτυξη περαιτέρω συνεργασίας μεταξύ τους για την **προώθηση της τυποποίησης και της συμβατότητας των πολιτικών έκδοσης πιστοποιητικών** (και γενικότερα των υπηρεσιών τους), στο βαθμό που αυτό θα συμβάλλει στην μεγαλύτερη αποδοχή τους από τους χρήστες και την σχετική αγορά
- Σύσταση **κοινού συστήματος 'κλάσεων'** για τα εκδιδόμενα πιστοποιητικών, όπου θα προσδιορίζονται κοινά επίπεδα στα όρια των επιτρεπόμενων συναλλαγών και στην ανάληψη αντίστοιχης ευθύνης εκ μέρους τους, λαμβάνοντας υπ' όψιν τις ανάγκες της εγχώριας αγοράς (*διαβούλευση με Τράπεζες, Δημόσιο, κ.λ.π. που θα είναι οι κύριοι αποδέκτες των πιστοποιητικών*)

ΠΡΟΣ ΠΑΡΟΧΟΥΣ ΑΛΛΩΝ ΥΠΗΡΕΣΙΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ η- ΥΠΟΓΡΑΦΕΣ

- Σύνταξη ή υιοθέτηση **κοινών «Πολιτικών (αποδοχής) Ηλεκτρονικής Υπογραφής»** με άλλους παρόχους συναφών υπηρεσιών (π.χ. τράπεζες, τηλεπικοινωνιακοί φορείς, πάροχοι υπηρεσιών περιεχομένου, κ.λ.π.) γεγονός που θα συμβάλει στην μεγιστοποίηση του αριθμού χρηστών (κατόχους κρυπτογραφικών κλειδιών με τυποποιημένες προδιαγραφές) στους οποίους θα απευθύνουν τις υπηρεσίες τους
- Συμβολή στην **ανάπτυξη κλίματος εμπιστοσύνης των χρηστών**, με την αυστηρή τήρηση όλων των προβλεπόμενων πολιτικών ασφάλειας και την υποστήριξη των κατάλληλων τεχνολογιών και μεθόδων που διασφαλίζουν την εμπιστευτικότητα των προσωπικών δεδομένων των χρηστών-πελατών τους.

ΣΥΜΒΟΥΛΕΣ ΠΡΟΣ ΤΟΝ ΤΕΛΙΚΟ ΧΡΗΣΤΗ

- Να ενημερώνεται διεξοδικά για όλους τους όρους χρήσης των κρυπτογραφικών κλειδιών, των πιστοποιητικών και των συναφών υπηρεσιών του ΠΥΠ κατά την αίτησή του για την έκδοση πιστοποιητικού ηλεκτρονικής υπογραφής
- Να τηρεί με επιμέλεια την μυστικότητα και την αποκλειστική χρήση των σχετικών ιδιωτικών κλειδιών του ('μη έκθεση των κλειδιών υπογραφής του 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 απωλέσει τον φορέα ή/και τον έλεγχο των ιδιωτικών κλειδιών του.
- Να χρησιμοποιεί τα συγκεκριμένα κρυπτογραφικά κλειδιά του μόνο στις επιτρεπόμενες -από το σχετικό πιστοποιητικό του- χρήσεις και να μην υπερβαίνει σε αξία συναλλαγών τα τυχόν 'όρια' που προβλέπονται από την Σύμβαση και την Πολιτική του πιστοποιητικού του.-

ΜΕΡΟΣ VI: ΥΛΟΠΟΙΗΣΕΙΣ

ΥΛΟΠΟΙΗΣΗ ΕΝΟΣ E-SHOP

Στα πλαίσια της πτυχιακής και θέλοντας να δείξω την χρησιμότητα των ψηφιακών υπογραφών προχώρησα στην δημιουργία ενός εικονικού καταστήματος με την χρησιμοποίηση των τεχνολογιών PHP , MySql και Apache η οποία και παρουσιάζεται παρακάτω .

Σχεδιασμός και Δημιουργία των Πινάκων της Βάσης Δεδομένων

Όνομα Πίνακα	**Ονόματα Πεδίων**
store_categories	Id,cat_title,cat_desc
store_items	Id,cat_id,item_title,item_price,item_desc,item_image
Store_item_color	Item_id,item_color
Store_item_size	Item_id,item_size

Αυτοί είναι οι μόνοι πίνακες που απαιτούνται για την δημιουργία μιας απλής εφαρμογής διαχείρισης ενός online καταστήματος για την παρουσίαση των προϊόντων που διατίθενται προς πώληση .Στην συνέχεια θα προσθέσουμε και την άποψη του χρήστη δημιουργώντας ένα καλάθι αγορών .

Εμφάνιση των κατηγοριών των προϊόντων

Το script seestore.php που χρησιμοποιείτε εξυπηρετεί δύο σκοπούς :

1. Εμφανίζει μια λίστα κατηγοριών
2. Εμφανίζει τα προϊόντα που περιλαμβάνει η κατηγορία που επιλέγει ο χρήστης

Ο κώδικας του script

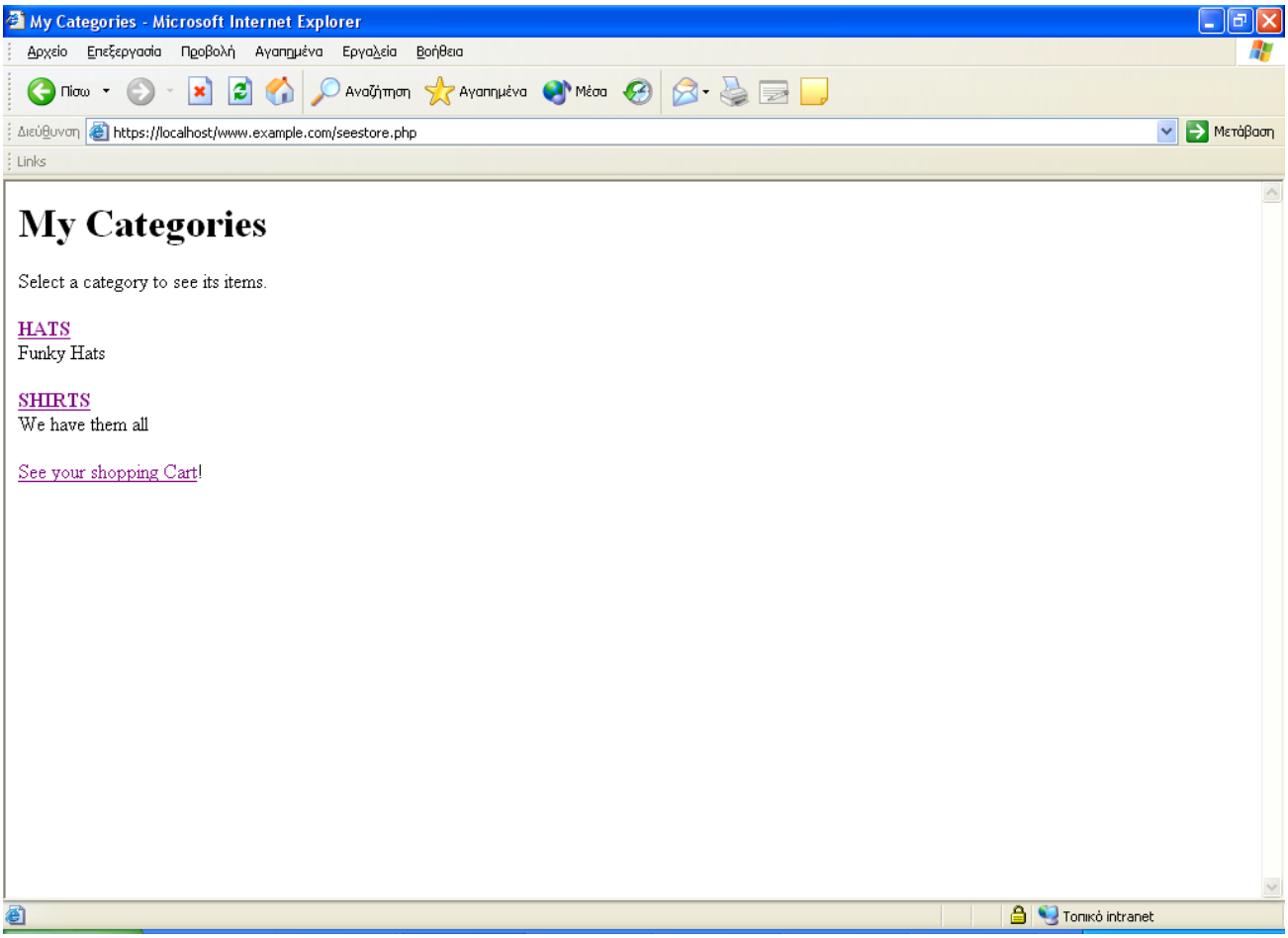
```
<?php
session_start();
//connect to database
$conn = mysql_connect("localhost","root","petros") or die(mysql_error());
mysql_select_db("e_shop",$conn)  or die(mysql_error());

$display_block = "<h1>My Categories</h1>
<P>Select a category to see its items.</p>";

//show categories first
$get_cats = "select id, cat_title, cat_desc from store_categories order by cat_title";
$get_cats_res = mysql_query($get_cats) or die(mysql_error());

if (mysql_num_rows($get_cats_res) < 1) {
   $display_block = "<P><em>Sorry, no categories to browse.</em></p>";
} else {
```

```
  while ($cats = mysql_fetch_array($get_cats_res)) {
      $cat_id  = $cats[id];
      $cat_title = strtoupper(stripslashes($cats[cat_title]));
      $cat_desc = stripslashes($cats[cat_desc]);

      $display_block .= "<p><strong><a
href=\"$_SERVER[PHP_SELF]?cat_id=$cat_id\">$cat_title</a></strong><br>$cat_desc</p>";

      if ($_GET[cat_id] == $cat_id) {
        //get items
        $get_items = "select id, item_title, item_price from store_items where cat_id = $cat_id order
by item_title";
        $get_items_res = mysql_query($get_items) or die(mysql_error());

        if (mysql_num_rows($get_items_res) < 1) {
            $display_block = "<P><em>Sorry, no items in this category.</em></p>";
        } else {
            $display_block .= "<ul>";

            while ($items = mysql_fetch_array($get_items_res)) {
              $item_id  = $items[id];
              $item_title = stripslashes($items[item_title]);
              $item_price = $items[item_price];

              $display_block.="<li><a
href=\"showitem.php?item_id=$item_id\">$item_title</a></strong> (\$$item_price)";
            }
```

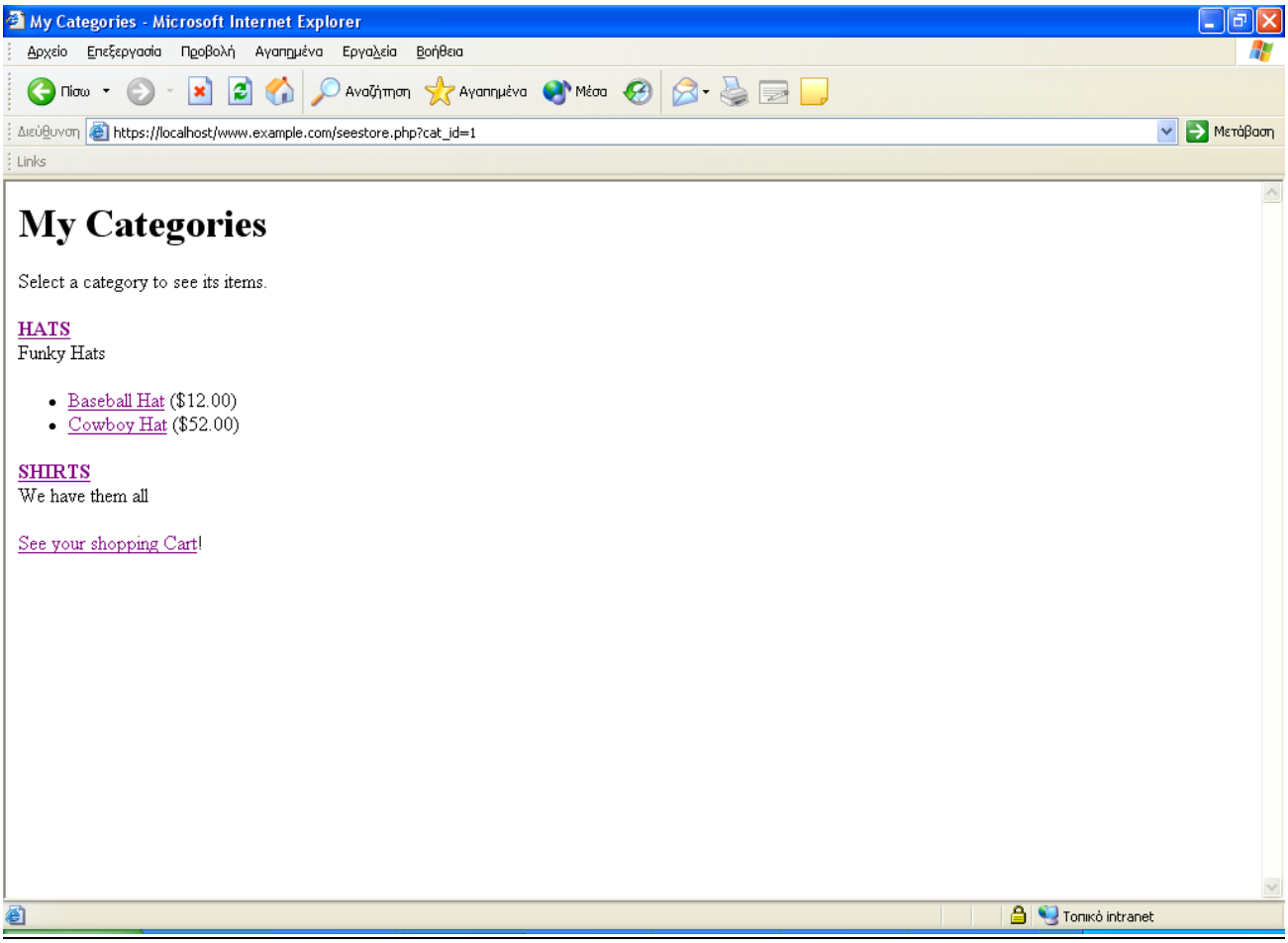
```
            $display_block .= "</ul>";
        }
    }
  }
}
$display_block .= "<p> <a href=\"showcart.php\">See your shopping Cart</a>!</p>";
echo $display_block;
?>
<HTML>
<HEAD>
<TITLE>My Categories</TITLE>
</HEAD>
<BODY>
</BODY>
</HTML>
```

Εκτελώντας τον παραπάνω κώδικα παίρνουμε τα παρακάτω αποτελέσματα :

Οι κατηγορίες προϊόντων του καταστήματος



Εμφάνιση των προϊόντων μιας κατηγορίας



Για την εμφάνιση των επιμέρους προιόντων χρειαζόμαστε ένα ακόμη script το **showitem.php** το οποίο καλείται από το script **seestore.php** όταν επιλέγεται ένα συγκεκριμένο προιόν. Ο κώδικας του **showitem.php** παρατίθεται παρακάτω :

```
<?php
session_start();
//connect to database
$conn = mysql_connect("localhost","root","petros") or die(mysql_error());
mysql_select_db("e_shop",$conn)  or die(mysql_error());

$display_block = "<h1>My Store - Item Detail</h1>";
```

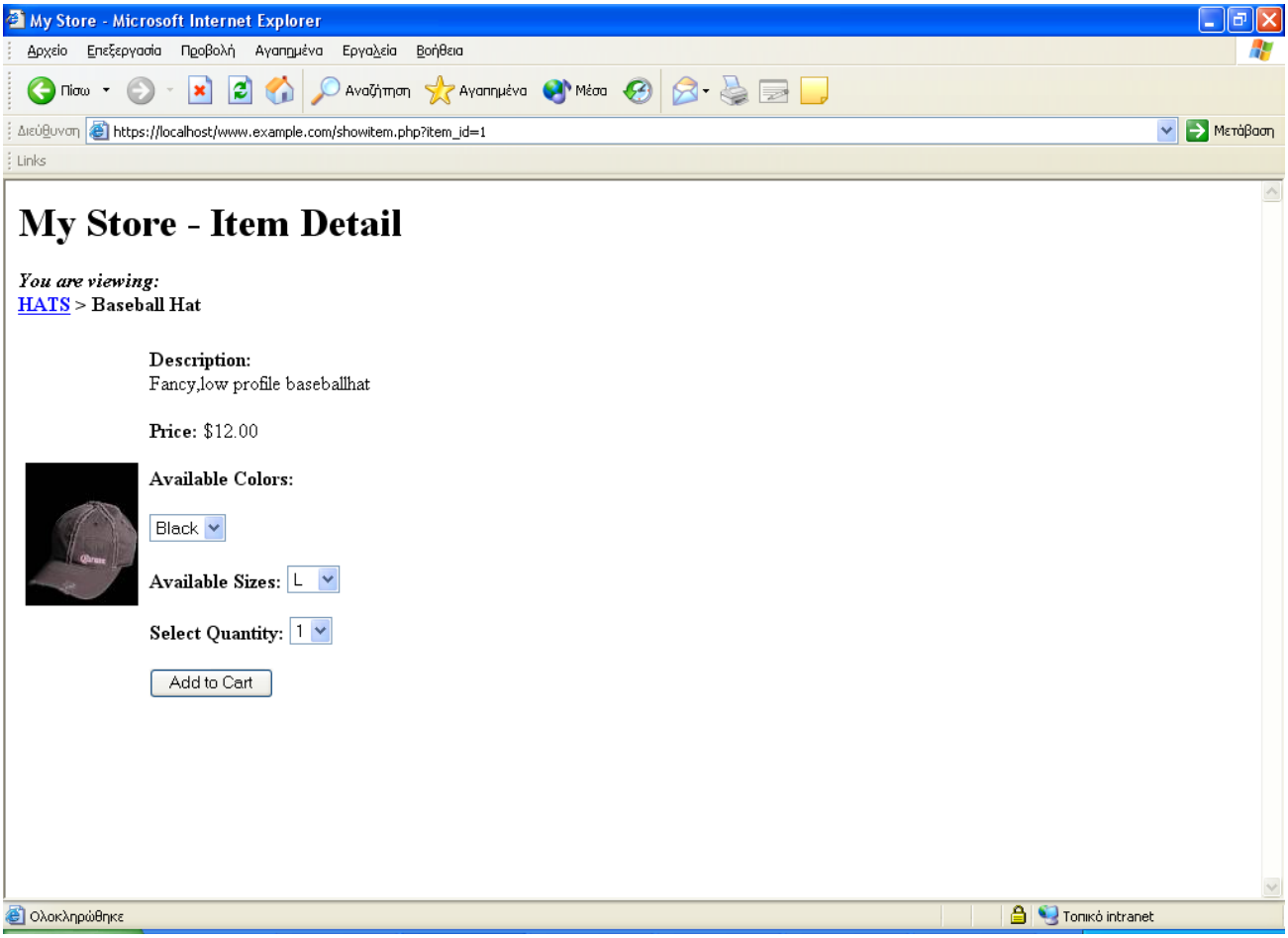
```
//validate item
$get_item = "select c.cat_title, si.item_title, si.item_price, si.item_desc, si.item_image from
store_items as si left join store_categories as c on c.id = si.cat_id where si.id = $_GET[item_id]";
$get_item_res = mysql_query($get_item) or die (mysql_error());

if (mysql_num_rows($get_item_res) < 1) {
  //invalid item
  $display_block .= "<P><em>Invalid item selection.</em></p>";
} else {
  //valid item, get info
  $cat_title = strtoupper(stripslashes(mysql_result($get_item_res,0,'cat_title')));
  $item_title = stripslashes(mysql_result($get_item_res,0,'item_title'));
  $item_price = mysql_result($get_item_res,0,'item_price');
  $item_desc = stripslashes(mysql_result($get_item_res,0,'item_desc'));
  $item_image = mysql_result($get_item_res,0,'item_image');

  //make breadcrumb trail
  $display_block .= "<P><strong><em>You are viewing:</em><br><a
href=\"seestore.php?cat_id=$cat_id\">$cat_title</a> &gt; $item_title</strong></p>
  <table cellpadding=3 cellspacing=3>
  <tr>
  <td valign=middle align=center><img src=\"$item_image\"></td>
  <td valign=middle><P><strong>Description:</strong><br>$item_desc</p>
  <P><strong>Price:</strong> \$$item_price</p>";

 //get colors
```

```
$get_colors = "select item_color from store_item_color where item_id = $_GET[item_id] order by item_color";
$get_colors_res = mysql_query($get_colors) or die(mysql_error());

if (mysql_num_rows($get_colors_res) > 0) {
        $display_block .= "<P><strong>Available Colors:</strong>
        <form method='post' action='addtocart.php'>
            <select name=\"sel_item_color\">";
        while ($colors = mysql_fetch_array($get_colors_res)) {
        $item_color = $colors['item_color'];
        $display_block .= "<option value=\"$item_color\">$item_color</option>";
        }

        $display_block .= "</select>";
}

//get sizes
$get_sizes = "select item_size from store_item_size where item_id = $_GET[item_id] order by item_size";
$get_sizes_res = mysql_query($get_sizes) or die(mysql_error());

if (mysql_num_rows($get_sizes_res) > 0) {
        $display_block .= "<P><strong>Available Sizes:</strong>

            <select name=\"sel_item_size\">";
        while ($sizes = mysql_fetch_array($get_sizes_res)) {
```

```
        $item_size = $sizes['item_size'];
        $display_block .= "
        <option value=\"$item_size\">$item_size</option>";
        }

        $display_block .= "</select> ";
}

$display_block .= "
<P><strong>Select Quantity:</strong>
<select name=\"sel_item_qty\">";

for($i=1; $i<5; $i++) {
        $display_block .= "<option value=\"$i\">$i</option>";

}
$display_block .= "</select> ";
$display_block .= "

<input type=\"hidden\" name=\"sel_item_id\" value=\"$_GET[item_id]\">
<P><input type=\"submit\" name=\"submit\" value=\"Add to Cart\"></p>
</form>
</td>
</tr>
```

```
  </table>";
}
echo $display_block;
?>
<HTML>
<HEAD>
<TITLE>My Store</TITLE>
</HEAD>
<BODY>
</BODY>
</HTML>
```

Η εκτέλεση του παραπάνω κώδικα μας δίνει τα εξής αποτελέσματα για το προϊόν baseball hat:



Προκειμένου να ολοκληρώσουμε την υλοποίηση μας πρέπει να προσθέσουμε και το καλάθι αγορών του καταστήματος μας , αυτό προϋποθέτει την δημιουργία επιπλέον πινάκων στην βάση δεδομένων μας :

Σχεδιασμός και Δημιουργία των Πινάκων της Βάσης Δεδομένων για το καλάθι αγορών

Όνομα Πίνακα	**Ονόματα Πεδίων**
store_shoppertrack	Id,session_id,sel_item_id,sel_item_qty,sel_item_size,sel_item_color,date_added
store_orders	Id,order_date,order_name,order_address,order_city,order_state,order_zip, order_tel,order_email,item_total,shipping_total,authorization,status_enum
Store_orders_itemmap	Id,order_id,sel_item_id,sel_item_qty,sel_item_size,sel_item_color, sel_item_price

Το script που χρειαζόμαστε για την προσθήκη προϊόντων στο καλάθι αγορών είναι το addtocart.php το οποίο θα γράφει απλώς δεδομένα στον πίνακα store_shoppertrack και θα ανακατευθύνει τον χρήστη στην σελίδα εμφάνισης των περιεχομένων του καλαθιού αγορών μέσω του script showcart.php και τα δύο script παρατίθενται παρακάτω :

Addtocart.php :

```
<?php
session_start();


//connect to database
$conn = mysql_connect("localhost","root","petros") or die(mysql_error());
mysql_select_db("e_shop",$conn)  or die(mysql_error());


if ($_POST[sel_item_id] != "") {
  //validate item and get title and price
   $get_iteminfo = "select item_title from store_items where id = $_POST[sel_item_id]";
   $get_iteminfo_res = mysql_query($get_iteminfo) or die(mysql_error());


   if (mysql_num_rows($get_iteminfo_res) < 1) {
          //invalid id, send away
          header("Location: seestore.php");
          exit;
   } else {
          //get info
          $item_title =  mysql_result($get_iteminfo_res,0,'item_title');
              $idtempnum = mysql_query("SELECT * FROM e_shop.store_shoppertrack order by
id desc") or die(mysql_error());
```

```
            $idnum = mysql_result($idtempnum,0,'id');
                //add info to cart table
                $sesid=session_id();
                $addtocart = "insert into store_shoppertrack values ($idnum+1, '$sesid',
'$_POST[sel_item_id]', '$_POST[sel_item_qty]', '$_POST[sel_item_size]',
'$_POST[sel_item_color]', now())";
            mysql_query($addtocart);

            //redirect to showcart page
            header("Location: showcart.php");
            exit;
    }
} else {
    //send them somewhere else
    header("Location: seestore.php");
    exit;
}
?>
```

showcart.php :

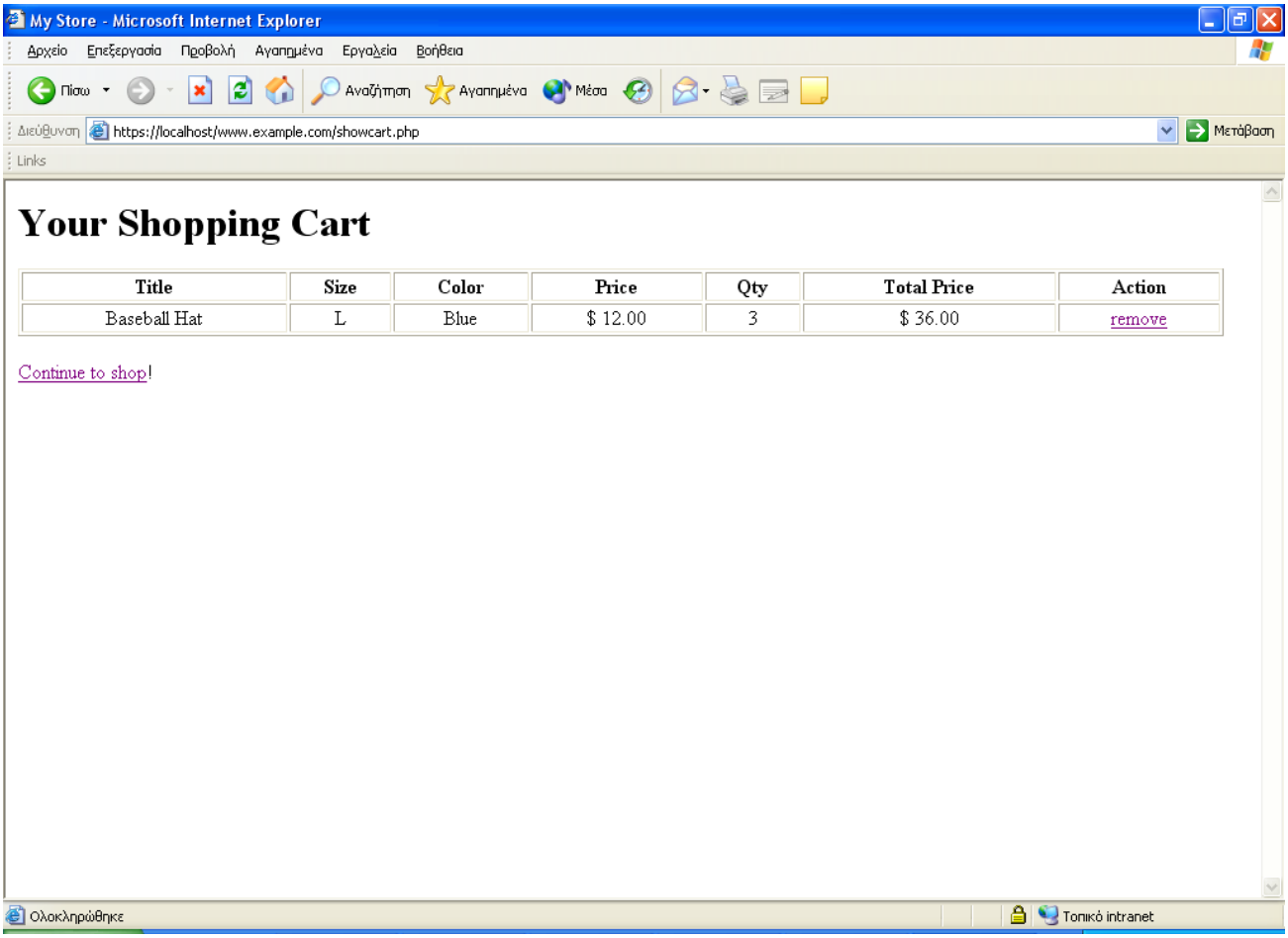
```
<?php
session_start();

//connect to database
```

```
$conn = mysql_connect("localhost","root","petros") or die(mysql_error());

mysql_select_db("e_shop",$conn)  or die(mysql_error());


$display_block = "<h1>Your Shopping Cart</h1>";


//check for cart items based on user session id

$test=session_id();

$get_cart = "select st.id, si.item_title, si.item_price, st.sel_item_qty, st.sel_item_size,
st.sel_item_color from store_shoppertrack as st  left join store_items as si on si.id = st.sel_item_id
where  session_id = '$test'";

$get_cart_res = mysql_query($get_cart) or die(mysql_error());


if (mysql_num_rows($get_cart_res) < 1) {

   //print message

   $display_block .= "<P>You have no items in your cart.

   Please <a href=\"seestore.php\">continue to shop</a>!</p>";


} else {

   //get info and build cart display

   $display_block .= "

   <table celpadding=3 cellspacing=2 border=1 width=98%>

   <tr>

   <th>Title</th>

   <th>Size</th>

   <th>Color</th>

   <th>Price</th>
```

```
<th>Qty</th>
<th>Total Price</th>
<th>Action</th>
</tr>";

while ($cart = mysql_fetch_array($get_cart_res)) {
        $id = $cart['id'];
        $item_title = stripslashes($cart['item_title']);
        $item_price = $cart['item_price'];
        $item_qty = $cart['sel_item_qty'];
        $item_color = $cart['sel_item_color'];
        $item_size = $cart['sel_item_size'];
        $total_price = sprintf("%.02f", $item_price * $item_qty);

        $display_block .= "<tr>
        <td align=center>$item_title <br></td>
        <td align=center>$item_size <br></td>
        <td align=center>$item_color <br></td>
        <td align=center>\$ $item_price <br></td>
        <td align=center>$item_qty <br></td>
        <td align=center>\$ $total_price</td>
        <td align=center><a href=\"removefromcart.php?id=$id\">remove</a></td>
        </tr>";
}

$display_block .= "</table>";
```

```
        $display_block .= "<p> <a href=\"seestore.php\">Continue to shop</a>!</p>";
}
echo $display_block;
?>
<HTML>
<HEAD>
<TITLE>My Store</TITLE>
</HEAD>
<BODY>
</BODY>
</HTML>
```

Η εκτέλεση των παραπάνω script έχει τα εξής αποτελέσματα :



Πώς όμως συνδιάζεται τελικά η υλοποίηση ενός ηλεκτρονικού μαγαζιού με τις ψηφιακές υπογραφές; Την απάντηση μπορει να τιν δώσει κάποιος θέτοντας τον εξής προβληματισμό στον εαυτό του , πώς ξερω ότι αυτό το μαγαζί υπάρχει; Ποιος μου διασφαλίζει πως κάπιος δεν θα με κλέψει;

Οι ψηφιακές υπογραφές στην συγκεκριμένη υλοποίηση έρχονται να λύσουν αυτές τις απορίες και συνάμα να διασφαλήσουν το ασφαλές τις συναλαγής .

Σε κάθε εικόνα που παραθέτω σε αυτήν την υλοποίηση κάτω δεξιά στον browser εμφανίζεται ένα λουκέτο αυτό σημαίνει πως η συναλαγές γίνονται πάνω στην βάση του ssl το οποίο για την υλοποίηση του στηριζεται στις ψηφιακές υπογραφές .

Προκειμένου να ενεργοποιθεί το ssl έπρεπε να γίνουν κάποιες ρυθμίσεις στον configuration file του apache και σιγκεκριμένα στο αρχείο httpd-ssl που βρίσκεται στο φάκελο C:\apache2\conf\extra στο σημείο SSL Virtual Host Context , όπου ορίζουμε το site που μας ενδιαφέρει και καθορίζουμε το path για τις παραμέτρους SSLCertificateFile και SSLCertificateKeyFile έτσι ώστε να δείχνουν στο certificate και στο key file που εχουμε δημιουργίσει με το openssl.

Όσον αφορά το Openssl για την δημιουργία ενός ζεύγους κλειδιών δίνουμε την παρακάτω εντολή : genrsa –out (όνομα site).key (μέγεθος κλειδιού)

Για την δημιουργία πιστοποιητικών έχουμε δύο επιλογές

1) Να αποκτήσουμε ένα πιστοποιητικό από έναν φορέα έκδοσης πιστοποιητικών (CA) υποβάλλοντας μία αίτηση υπογραφής πιστοποιητικού . Για να δημιουργήσουμε μία τέτοια αίτηση , εισάγουμε την ακόλουθη εντολή :

Req –new –key (όνομα site).key –out (όνομα site).csr

Στην συνέχεια μπορούμε να υποβάλουμε το αρχείο (όνομα site).csr με την αίτηση υπογραφής πιστοποιητικού σε έναν φορέα CA .Οι VeriSign και Thawte είναι δύο πολύ γνωστοί και αξιόπιστοι φορείς έκδοσης πιστοποιητικών

2) Μπορούμε να δημιουργήσουμε ένα αυτό-υπογραφόμενο πιστοποιητικό.Δηλαδή ,μπορούμε να λειτουργήσουμε τόσο σαν εκδότες ,όσο και σαν αντικείμενα του πιστοποιητικού .Αν και αυτό δεν είναι ιδιαιτερα χρήσιμο για ένα εμπορικό Web Site. Για να δημιουργήσουμε μία τέτοια αίτηση , εισάγουμε την ακόλουθη εντολή :

X509 –req –days (αριθμός ημερών) –in (όνομα site).csr –signkey (όνομα site).key –out (όνομα site).cert

ΕΦΑΡΜΟΓΗ ΓΙΑ ΤΗΝ ΔΗΜΙΟΥΡΓΙΑ CERTIFICATE'S

Η υλοποίηση αυτήν βασίστηκε στην πλατφόρμα της Java καθώς και στην βιβλιοθήκη που παρέχει ο οργανισμός Bouncy Castle (http://www.bouncycastle.org **) .**

Αφού εγκαταστήσουμε την java στο σύστημα μας πρέπει να κάνουμε μερικές αλλαγές πηγαίνουμε στον φάκελο που έχει να κάνει με το security στο εξής path C:\j2sdk1.4.2_04\jre\lib\security και προσθέτουμε τα παρακάτω αρχεία

local_policy

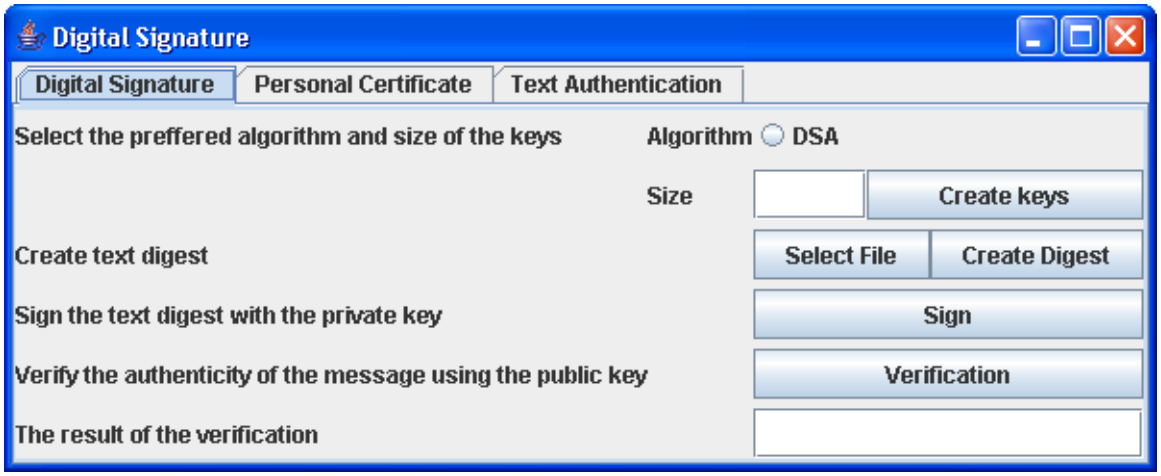
US_export_policy

Η υλοποίηση μας στηρίχτηκε όπως ήδη αναφέραμε σε μία βιβλιοθήκη την οποία πρέπει να προσθέσουμε στο path C:\j2sdk1.4.2_04\jre\lib\ext και προσθέτουμε το αρχείο BouncyCastleProvider.jar

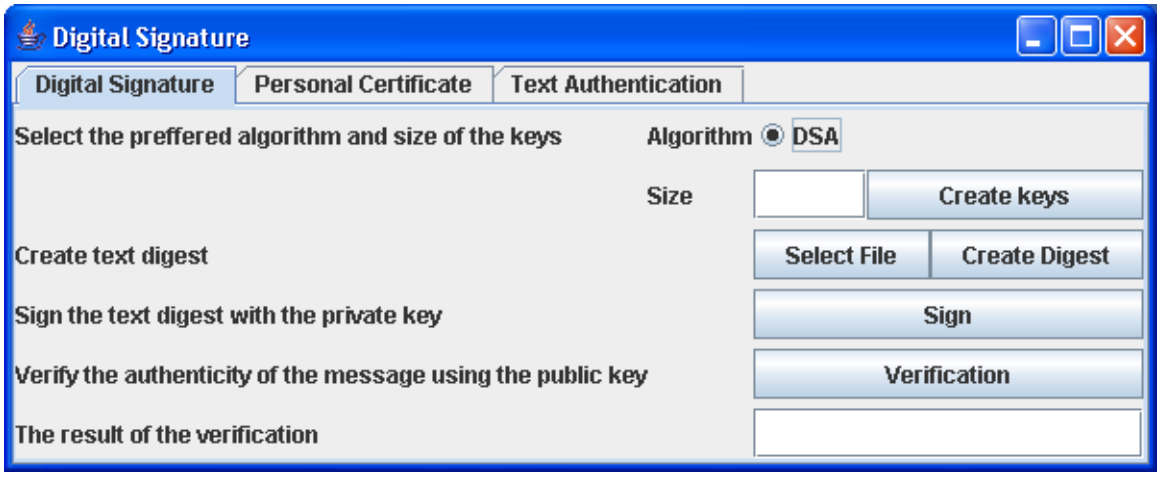
Τοποθετούμε το αρχείο ΠΤΥΧΙΑΚΉ.rar στο path c:\ . Στην συνέχεια για να τρέξουμε την εφαρμογή μας πηγαίνουμε στο φάκελο C:\ΠΤΥΧΙΑΚΉ\JavaExe και κάνουμε διπλό κλικ στο Digital_Signature.exe

ΔΗΜΙΟΥΡΓΙΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

Στο παράθυρο που μας εμφανίζεται επιλέγουμε το πρώτο tab και σε κάθε επιλογή μας πατάμε enter



Επιλέγουμε το DSA radio button



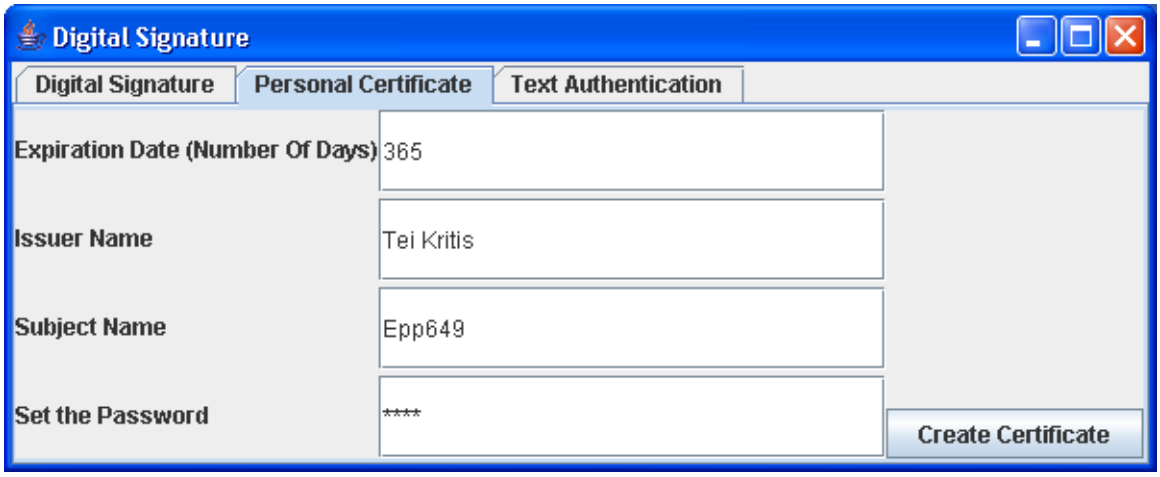
Στο size δίνουμε την τιμή που θέλουμε να έχουν τα κλειδιά μας

μετά πατάμε το κουμπί create keys και δημιουργούνται τα κλειδιά στον φάκελο C:\ΠΤΥΧΙΑΚΉ\Digital_Signature , πατάμε το κουμπί select file και από το menu που εμφανίζεται επιλέγουμε το αρχείο του οποίου την σύνοψη θέλουμε να δημιουργήσουμε , κατόπιν πατάμε το κουμπί sign και υπογράφεται η σύνοψη του αρχείου με το private key , τέλος πατάμε το verification button και ελέγχουμε μέσω της εφαρμογής μας και έχοντας ως σημείο αναφοράς το public key την αυθεντικότητα του κειμένου – αποστολέα.

ΕΝΟΣ CERTIFICATE

Στο παράθυρο που μας εμφανίζεται επιλέγουμε το δεύτερο tab και σε κάθε επιλογή μας πατάμε Enter

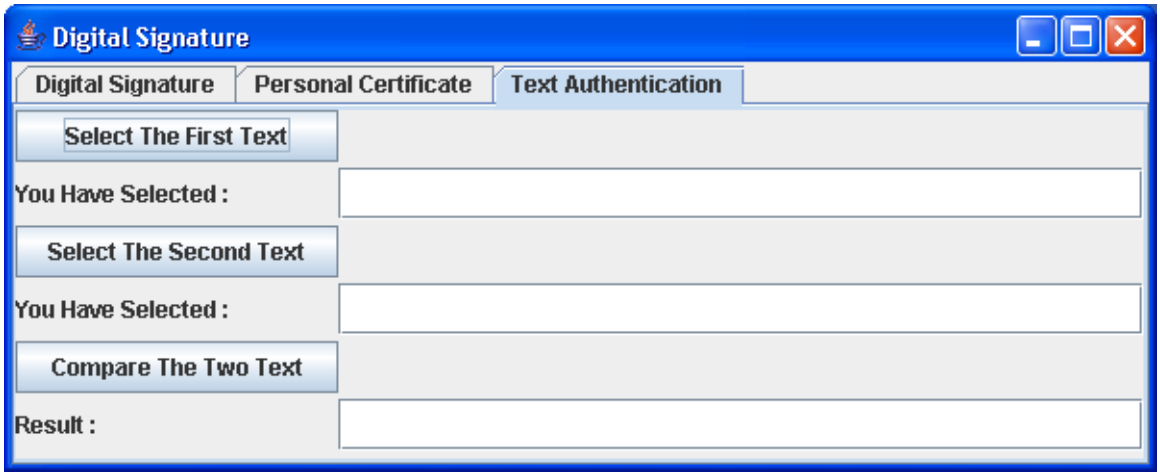
στο πεδίο number of day's επιλέγουμε της μέρες που θέλουμε να έχει ισχύ το Ψηφιακό Πιστοποιητικό μας , ομοίως συμπληρώνουμε και τα υπόλοιπα πεδία μετά από κάθε εισαγωγή τιμής πατάμε Enter.



τέλος πατάμε το κουμπί create certificate και στον φάκελο C:\ΠΤΥΧΙΑΚΉ\Personal_Certificate δημιουργούμε το keystore και το public key.

ΕΛΕΓΧΟΣ ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΕΙΜΕΝΟΥ

Στο παράθυρο που μας εμφανίζεται επιλέγουμε το τρίτο tab



πατάμε το κουμπί select the first text και από το menu που εμφανίζεται επιλέγουμε το κείμενο που θέλουμε ομοίως και για το button select the second text , τέλος με το button compare the two text συγκρίνουμε την ακεραιότητα των κειμένων βάση της σύνοψης που δημιουργείτε για το κάθε ένα και βλέπουμε αν είναι ίδια ή εάν έχουν αλλαχτεί , το αποτέλεσμα εμφανίζεται στο Result textfield

ΠΑΡΑΡΤΗΜΑ 'Α'

Κατάλογος Νομοθετικών-Κανονιστικών κειμένων

Α. ΔΙΕΘΝΗ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

- UNCITRAL «**Νόμος-Πρότυπο για τις ηλεκτρονικές υπογραφές**» 5 Ιουλίου 2001
- United Kingdom, Statutory Instrument 2002 No. 318, «**The Electronic Signatures Regulations 2002**»
- USA, «**The Electronic Signatures in Global and National Commerce Act**»

Β. ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ

- ***Οδηγία 99/93/ΕΕ*** 'για τις ηλεκτρονικές υπογραφές'
- ***Απόφαση 6 Νοεμβρίου 2000*** της Επιτροπής Ηλεκτρονικής υπογραφής (άρθρο 9 Οδηγίας 99/93/ΕΕ) για τα ελάχιστα κριτήρια που θα πρέπει να πληρούν οι αρμόδιοι φορείς για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής.
- ***Οδηγία 98/34/ΕΚ*** για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών καθώς και η τροποποίησή της από την *Οδηγία 98/48/ΕΚ)*
- ***Απόφαση της Επιτροπής της 14ης Ιουλίου 2003*** σχετικά με τη δημοσίευση αριθμών αναφοράς γενικά αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής, σύμφωνα με την Οδηγία 1999/93/ΕΚ .

Γ. ΕΘΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

- ***Π.Δ. 150/2001:*** Προσαρμογή στην Οδηγία 99/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
- ***Π.*Δ. 39.2001:** Καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της Κοινωνίας των Πληροφοριών
- ***Ν.2672/1998* 'Αρθρο 14:** Διακίνηση εγγράφων με ηλεκτρονικά μέσα
- ***Π.Δ. 342/2002:*** Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.
- **Π.Δ. 342/2002**: «Διακίνηση ψηφιακά υπογεγραμμένων 'μηνυμάτων ηλεκτρονικού ταχυδρομείου' στις επικοινωνίες του Δημόσιου Τομέα»
- **Απόφαση 248/71**: «Κανονισμός παροχής υπηρεσιών πιστοποίησης ηλεκ. υπογραφής»
- **Απόφαση 295/63**: « Κανονισμός ορισμού φορέων για την διαπίστωση συμμόρφωσης ΑΔΔΥ και ΑΚΜ και προς τα κριτήρια της εθελοντικής διαπίστευσης»
- **Απόφαση 295/64** : «Κανονισμός για τον έλεγχο συμμόρφωσης ΑΔΔΥ και ΑΚΜ»
- **Απόφαση 295/63:** «Κανονισμός για την εθελοντική διαπίστευση των ΠΥΠ»
- ***«Κανονισμός Επικοινωνίας Δημόσιων Υπηρεσιών»*** *(ΚΕΔΥ)*
- ***Εγκύκλιος ΔΙΑΔΠ/Α1/2523*** του Υπουργείου Δημόσιας Διοίκησης και Αποκέντρωσης Δ/νση Απλούστευσης Διαδικασιών και Παραγωγικότητας-Διευκρινήσεις στις διατάξεις του άρθρου 14 του Ν. 2672/1998

ΠΑΡΑΡΤΗΜΑ 'Β'

Κατάλογος Ευρωπαϊκών Προτύπων/Τεχνικών προδιαγραφών*

A. Electronic Telecommunication Standardization Institute / Electronic Signatures Initiative (ETSI/ESI):

- **ETSI TS 101 862 v.1.2** (Mars 2002) - Qualified Certificate Profile
- **ETSI TS 102 023 v.1.2.1** (January 2003) - Policy requirements for timestamping authorities
- **ETSI TS 102 042** (April 2002) - Policy requirements for certification authorities issuing public key certificates
- **ETSI TS 101 456 v 1.2.1** (April 2002) - Policy requirements for certification authorities issuing qualified certificates
- **ETSI TS 101 733 v 1.4.0** (September 2002) - Electronic Signature Formats
- **ETSI TS 101 861 v 1.2.1** (March 2002) - Time stamping profile
- **ETSI TS 101 903 v. 1.1.1** (February 2002) - XML Advanced Electronic Signatures (XAdES)
- **ETSI SR 002 176** (March 2003) - Algorithms and Parameters for Secure Electronic Signatures
- **ETSI TR 102 045** (March 2003) - Signature policy for extended business model
- **ETSI TR 102 153** (February 2003) - Pre study on Certificate Profiles
- **ETSI TR 102 023** (January 2003) - Policy requirements for time-stamping authorities
- **ETSI TR 102 044** (December 2002) - Identification of requirements for attribute certification

- **ETSI TR 102 038** (April 2002) - XML format for signature policies
- **ETSI TR 102 040** (March 2002) - International Harmonization of Policy Requirements for CAs issuing Certificates
- **ETSI TR 102 041** (February 2002) - Signature Policies Report
- **ETSI TS 102 231** (October 2003) - Harmonized TSP status information
- **ETSI TS 102 280** (March 2004) – X.509 v3 Certificate Profile for Certificates Issued to Natural Persons
- **Frequently Asked Questions** (March 2002)

Β. 'European Committee For Standardisation/ Information Society Standardization System (CEN/ISSS):

- **CWA 14365** Guide on the use of Electronic Signatures
- **CWA 14355** Guidelines for the implementation of Secure Signature-Creation Devices
- **CWA 14172-1** EESSI Conformity Assessment Guidance - Part:1: General
- **CWA14172-2** EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes
- **CWA 14172-3** EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
- **CWA 14172-4** EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification
- **CWA 14172-5** EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices
- **CWA 14171** Procedures for Electronic Signature Verification
- **CWA 14170** Security Requirements for Signature Creation Systems
- **CWA 14169** Secure Signature-Creation Devices, version 'EAL 4+'
- **CWA 14167-1** Revised Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- **CWA14167-2** Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

Γ. Κοινές Προδιαγραφές του eEurope Smart Card Charter (OSCIE v. 2):

- **Vol. 3:** Global interoperability Framework for identification, authentification and electronic signature (IAS) with smart cards
- **Vol. 4:** Public Electronic Identity, Electronic Signature and PKI

* = Ο κατάλογος είναι **ενδεικτικός** και περιλαμβάνει μερικές μόνο από τις εκδόσεις προτύπων από τους Ευρωπαϊκούς Οργανισμούς Προτυποποίησης. Για πλήρη και ενημερωμένη λίστα προτύπων ανατρέξτε στις σχετικές ηλεκτρονικές τοποθεσίες μέσω της εισαγωγικής ιστοσελίδας του EESSI (http://www.ict.etsi.org/EESSI_home.htm)