ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Ηλεκτρονικές Υπογραφές *και* Διαπίστευση Παρόχων Υπηρεσιών Πιστοποίησης»

Γροντάς Παναγιώτης

Μ3000004

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2002

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

«Ηλεκτρονικές Υπογραφές *και* Διαπίστευση Παρόχων Υπηρεσιών Πιστοποίησης»

Γροντάς Παναγιώτης

M3000004

Επιβλέπων Καθηγητής: **Εμμανουήλ Γιακουμάκης**

Εξωτερικός Κριτής: **Καθηγητής Ευάγγελος Κιουντούζης**

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2002

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΚΥΡΙΩΣ ΜΕΡΟΣ

1 Εισαγωγή

Η ταχύτατη ανάπτυξη του Διαδικτύου (Internet) που έχουμε ήδη ζήσει και συνεχίζουμε να ζούμε, οφείλεται πιθανότατα στην προοπτική που το συνοδεύει: να αντικατοπτρίσει όλες τις λειτουργίες της καθημερινής μας ζωής, με τρόπο όμως που όλα θα γίνονται πιο γρήγορα, πιο εύκολα, πιο αποτελεσματικά και με λιγότερο κόστος. Την προοπτική αυτή αναγνώρισαν πρώτα τα ακαδημαϊκά ιδρύματα, έπειτα οι επιχειρήσεις και μέσω αυτών οι διάφοροι κρατικοί και περιφερειακοί οργανισμοί. Μέσω αυτών οι διάφορες χώρες έχουν ήδη ξεκινήσει την αναθεώρηση αρκετών πτυχών της 'λειτουργίας' τους, προβαίνοντας ακόμα και σε αναθεώρηση νομικών διατάξεων και θεσμών. Με τον τρόπο αυτό οι νέες τεχνολογίες αποκτούν ένα ευρύτατο κοινό, το οποίο κάθε άλλο παρά έτοιμο να τις αποδεχτεί είναι.

Όπως είναι λογικό, η μετάβαση αυτή ούτε αυτόματη είναι ούτε απλή. Είναι δε αποδεκτό από όλους ότι, παράδοξα μεν, αλλά, η τεχνολογία έχει τον τελευταίο λόγο σε αυτήν, καθώς από την μία κάνει τα πάντα δυνατά, από την άλλη όμως δεν τα πραγματοποιεί κιόλας. Τον κύριο λόγο στην αλλαγή και την προσαρμογή έχουν οι διαδικασίες και οι συχνά εφαρμοζόμενες συνήθειες, πρακτικές - πολλές από τις οποίες έχουν εξελιχθεί σε νόμους – οι οποίες θα πρέπει να μεταλλαχθούν.

Στην εργασία αυτή θα ασχοληθούμε, έχοντας βέβαια μία διαφορετική σκοπιά με μία από τις παραμέτρους της αλλαγής, που ίσως είναι και η πρώτη που θα επηρεάσει το ευρύ κοινό. Θα ασχοληθούμε με τις ηλεκτρονικές υπογραφές και τις σχετιζόμενες με αυτές υπηρεσίες, οι οποίες καλούνται να αντικαταστήσουν τις ιδιόχειρες υπογραφές, μία ανθρώπινη πρακτική με ηλικία ίσως και χιλιάδων χρόνων.

1.1 Ηλεκτρονικές Συναλλαγές.

Από πολύ νωρίς, εδώ και περίπου 30 χρόνια σύμφωνα με το **[Turban, 2000]**, οι διάφορες επιχειρήσεις αναγνώρισαν τα πλεονεκτήματα σε κόστος, χρόνο, αποδοτικότητα της διεξαγωγής των συναλλαγών τους μέσω ηλεκτρονικών δικτύων. Για τον σκοπό αυτό ανέπτυξαν συγκεκριμένα πρότυπα για την ανταλλαγή δεδομένων, όπως παραγγελίες, τιμολόγια, πληρωμές μέσω *ιδιωτικών* δικτύων δεδομένων. Το πιο γνωστό τέτοιο πρότυπο είναι το EDIFACT (**E**lectronic **D**ata **I**nterchange **F**or **A**dministration, **C**ommerce And **T**rade) του Οργανισμού Ηνωμένων Εθνών.

Η είσοδος του Διαδικτύου και του Παγκόσμιου Ιστού (WWW) στο προσκήνιο στις αρχές της δεκαετίας του '90, δημιούργησε αρκετές νέες προοπτικές και πολύ σημαντικές προκλήσεις. Ως ένα δημόσιο δίκτυο, με ήδη έτοιμη υποδομή, το Internet μείωνε σημαντικά τα τεράστια κόστη ανάπτυξης ενός ιδιωτικού δικτύου μεταξύ δύο οργανισμών. Επίσης δημιούργησε και νέες ευκαιρίες, καθώς καθιστούσε άμεση την πρόσβαση σε ένα τεράστιο πλήθος εν δυνάμει αγοραστών. Οι δυνατότητες του δεν ήταν πλέον χρήσιμες μόνο για την ανταλλαγή δεδομένων μεταξύ επιχειρήσεων (*Business to Business - B2B*), αλλά μεταξύ επιχειρήσεων και

κοινού (*Business to Consumer - B2C*) και σχετικά πρόσφατα μεταξύ κράτους, κοινού (*Government to Citizen - G2C*) και επιχειρήσεων (*Government to Business - G2B*). Δικαιολογείται έτσι η διαπίστωση που έγινε νωρίτερα, ότι σήμερα ο ρόλος του διαδικτύου είναι να αντικατοπτρίσει όλες τις πτυχές της καθημερινής ζωής, σε μία βελτιστοποιημένη εκδοχή όμως.

Παρ' όλα αυτά ο δημόσιος χαρακτήρας του Διαδικτύου, κάνει τα ανταλλασσόμενα δεδομένα και τις πληροφορίες που αυτά εμπεριέχουν, εν δυνάμει προσβάσιμα στον καθένα. Το γεγονός αυτό έχει ως συνέπεια την άρση πολλών βασικών ιδιοτήτων που παραδοσιακά χαρακτήριζαν μία συναλλαγή ως σήμερα. Οι ιδιότητες αυτές δεν έχουν να κάνουν μόνο με την ηλεκτρονική φύση της συναλλαγής, καθώς δεν χαρακτήριζαν αυτές που εκτελούνταν πάνω από ιδιωτικά, κλειστά δίκτυα δεδομένων. Συγκεκριμένα σε μία διαδικτυακή συναλλαγή είναι δυνατές μεταξύ άλλων οι παρακάτω καταστάσεις:

- Παθητική παρακολούθηση των ανταλλασσόμενων δεδομένων, από μία μη εξουσιοδοτημένη οντότητα.
- Ενεργή συμμετοχή στην επικοινωνία από κάποια μη εξουσιοδοτημένη οντότητα μέσω εκούσιας τροποποίησης των δεδομένων, χωρίς αυτό να γίνει αντιληπτό από τους συμμετέχοντες.
- Αποποίηση συμμετοχής σε μία συναλλαγή από ένα ή περισσότερα μέρη της (repudiation), κάτι που είναι εφικτό λόγω της ανωνυμίας που χαρακτηρίζει το Διαδίκτυο.
- Αμφισβήτηση των περιεχομένων ενός ή περισσοτέρων μηνυμάτων που απαρτίζουν μια ηλεκτρονικής συναλλαγής.
- Αμφισβήτηση της χρονικής στιγμής στην οποία έλαβε χώρα μία συναλλαγή.

Η ύπαρξη των παραπάνω καταστάσεων, έχει ως συνέπεια την διαφορετική αντιμετώπιση μιας ηλεκτρονικής συναλλαγής από μία παραδοσιακή. Ουσιαστικά όμως οι δύο τύποι συναλλαγών είναι εννοιολογικά ταυτόσημοι, παρά το γεγονός ότι η υλοποίηση τους γίνεται διαφορετικά. Υπό κανονικές συνθήκες για παράδειγμα, μία αγορά από ένα ηλεκτρονικό κατάστημα έχει τα ίδια αποτελέσματα με μία αγορά από ένα παραδοσιακό. Ο αγοραστής γίνεται ιδιοκτήτης των προϊόντων και ο πωλητής λαμβάνει το αντίτιμο. Το πρόβλημα έγκειται στο ότι υπάρχει δυσκολία απόδοσης των χαρακτηριστικών της εγκυρότητας και εφαρμοσιμότητας σε μία ηλεκτρονική συναλλαγή[1]. Οι παραπάνω ιδιότητες έχουν άμεση σχέση με την νομική αναγνώριση της. Συγκεκριμένα με την εγκυρότητα εννοούμε, ότι είναι επιτρεπτό, δηλαδή σύμφωνο με τον νόμο μία συγκεκριμένη συναλλαγή να είναι σε ηλεκτρονική μορφή. Με τον όρο εφαρμοσιμότητα, εννοούμε ότι υπάρχουν τα τεκμήρια εκείνα με τα οποία η συγκεκριμένη συναλλαγή, μπορεί να ανταπεξέλθει σε αμφισβητήσεις είτε της ίδιας είτε επιμέρους λεπτομερειών της **[Ford, 2001]**. Τα παραπάνω ισχύουν όχι μόνο για την ουσία των συναλλαγών, αλλά και για την αναπαράσταση τους. Συγκεκριμένα κάθε παραδοσιακή συναλλαγή συνοδεύεται από παραστατικά και συμβόλαια, τα οποία ως στόχο έχουν να βοηθήσουν στην απόδοση των ιδιοτήτων της εγκυρότητας και της εφαρμοσιμότητας.

[1] Με τον όρο ηλεκτρονική συναλλαγή θα εννούμε στο εξής, την ηλεκτρονική συναλλαγή, η οποία γίνεται πάνω από μη ασφαλή δίκτυα όπως το Internet.

Προφανώς τα ίδια πρέπει να ισχύουν και για τις ηλεκτρονικές συναλλαγές. Μόνο που και τα τεκμήρια εδώ πρέπει να είναι σε ηλεκτρονική μορφή καθώς σε διαφορετική περίπτωση χάνονται τα πλεονεκτήματα τα οποία προαναφέραμε.

Για την απόδοση των παραπάνω ιδιοτήτων, πρέπει να εφαρμοστούν ένα σύνολο από μέτρα διασφάλισης στις ηλεκτρονικές συναλλαγές που θα τις κάνουν *τουλάχιστον* το ίδιο ασφαλείς και εφαρμόσιμες. Τα μέτρα αυτά παρέχονται από τον κλάδο της επιστήμης της πληροφορικής που ασχολείται με την ασφάλεια των πληροφοριών. Έτσι πρέπει οι ηλεκτρονικές συναλλαγές να αποκτήσουν τις 'κλασικές ιδιότητες' της ασφάλειας, δηλαδή της **Μυστικότητας, Ακεραιότητας, Αυθεντικότητας.** Με άλλα λόγια **[Gritzalis, 1998],** πρέπει τα ανταλλασσόμενα δεδομένα να μην μπορούν να αναγνωσθούν και να τροποποιηθούν από μη εξουσιοδοτημένα άτομα, ενώ πρέπει όντως να προέρχονται από τα άτομα που φαίνεται ότι προέρχονται.

Με την υλοποίηση των παραπάνω μηχανισμών, δίδονται κάποιες ιδιότητες στις ηλεκτρονικές συναλλαγές που τις φέρνουν πιο κοντά στις παραδοσιακές. Δεν εξασφαλίζουν όμως την παροχή των ιδιοτήτων της εγκυρότητας και της εφαρμοσιμότητας, που θα τις καταστήσουν και νομικά ισοδύναμες, καθώς αφορούν κυρίως τις συναλλαγές καθ'αυτές και όχι την αντιμετώπιση τους από τον 'έξω' κόσμο.
Απαιτούνται επιπλέον τα εξής:

- Ένας μηχανισμός ο οποίος θα μπορεί να χρησιμοποιηθεί για την παροχή στοιχείων σχετικά με τις ηλεκτρονικές συναλλαγές, τα οποία θα διαβεβαιώνουν ότι αυτές έλαβαν χώρα και θα προσδιορίζει την χρονική στιγμή
- Ένας μηχανισμός, ο οποίος εκτός από την αυθεντικοποίηση των συμμετεχόντων θα εξασφαλίζει ότι αυτοί έδωσαν την συναίνεση τους για την συναλλαγή.
- Ένας μηχανισμός, ο οποίος θα επιλύει τυχούσες διαφορές μεταξύ των συμμετεχόντων.

Οι παραπάνω μηχανισμοί δεν είναι ούτε άγνωστοι ούτε καινούριοι. Υπάρχουν εδώ και εκατοντάδες χρόνια και έχουν εξελιχθεί από απλές και καθημερινές πρακτικές σε πολύπλοκα νομικά συστήματα. Η πρόκληση είναι πώς θα εφαρμοστούν αυτές στο ηλεκτρονικό περιβάλλον, χωρίς να αλλάξουν τα εννοιολογικά τους χαρακτηριστικά.

1.2 Ιδιόχειρες και Ηλεκτρονικές Υπογραφές.

Η υπογραφή είναι ένας από τους βασικούς μηχανισμούς παροχής εγκυρότητας και εφαρμοσιμότητας σε μία συναλλαγή. Σε γενικό επίπεδο, παρέχει στοιχεία για την αυθεντικοποίηση ενός κειμένου και την αποδοχή του από τον συγγραφέα του. Επιπλέον δίνει το νόημα της τέλεσης (ceremony) σε μία πράξη, επισείοντας την προσοχή των συμμετεχόντων στο ότι η συναλλαγή ή συμφωνία τους κ.ο.κ. είναι δεσμευτική και μπορεί να έχει νομικές συνέπειες.

Η ιδιόχειρη υπογραφή βασίζεται στην δημιουργία ενός χαρακτηριστικού σημαδιού χρησιμοποιώντας κάποιο είδος γραφής, το οποίο χαρακτηρίζει τον υπογράφοντα και τοποθετείται στο τέλος ενός κειμένου. Οι

χημικές ιδιότητες του μελανιού και του χαρτιού διασφαλίζουν την φυσική σύνδεση της υπογραφής με το κείμενο. Η φυσική αυτή σύνδεση έχει ως συνέπεια την λογική συσχέτιση, έτσι ώστε η υπογραφή να είναι ένδειξη για **[Kuner, 1999]:**

- Την αποδοχή του κειμένου από τον υπογράφοντα και την συμφωνία του με αυτό.
- Το γεγονός ότι ο υπογράφων έλαβε γνώση του κειμένου και αναλαμβάνει την ευθύνη για το περιεχόμενο του.
- Την ταυτότητα του υπογράφοντα ως συντάκτη του κειμένου.
- Την πραγματοποίηση μιας συναλλαγής.

Οι ιδιόχειρες υπογραφές μπορούν να αμφισβητηθούν από τους υποτιθέμενους υπογράφοντες. Οι λεπτομέρειες ποικίλουν ανάλογα και με το συγκεκριμένο νομικό πλαίσιο, σε γενικές γραμμές πάντως οι παρακάτω ισχυρισμοί είναι καθ' όλα θεμιτοί σε μία δικαστική αίθουσα :

- Μία ιδιόχειρη υπογραφή δεν γίνεται αποδεκτή, καθώς είναι προϊόν πλαστογραφίας.
- Μία ιδιόχειρη υπογραφή που δεν είναι προϊόν πλαστογραφίας, δεν γίνεται αποδεκτή καθώς:
    - Ο υπογράφων εξαπατήθηκε.
    - Ασκήθηκε ψυχολογική και άλλου είδους πίεση, στον υπογράφονται προκειμένου να υπογράψει.

Είναι προφανές, ότι οι υπογραφές με την παραδοσιακή τους μορφή και υλοποίηση δεν μπορούν να εφαρμοστούν στις ηλεκτρονικές συναλλαγές. Κατά συνέπεια απαιτείται ένας νέος τύπος υπογραφής, μία ηλεκτρονική υπογραφή δηλαδή, η οποία θα μπορεί να προσαρτηθεί σε και να συνδεθεί με ηλεκτρονικά δεδομένα με τον ίδιο τρόπο, που μία ιδιόχειρη υπογραφή αφορά χειρόγραφα κείμενα. Εκτός όμως από την αναπαράστασή της, θα χρειαστεί πιθανότατα μία αναθεώρηση της όλης έννοιας της υπογραφής. Η βασική τεχνολογία η οποία κάνει δυνατή τις ηλεκτρονικές υπογραφές είναι η *Κρυπτογραφία Δημοσίου Κλειδιού*. Θα αναφερθούμε αναλυτικά σε αυτήν στο δεύτερο κεφάλαιο της εργασίας καθώς επίσης και σε άλλες τεχνολογίες οι οποίες μπορούν να χρησιμοποιηθούν από μόνες τους ή σε συνδυασμό με την συγκεκριμένη για την παροχή ηλεκτρονικών υπογραφών.

Σε κάθε περίπτωση πάντως, φαίνεται, ότι δεν θα καταστεί δυνατή η εξομοίωση του γεγονότος που χαρακτηρίζει τις συμβατικές υπογραφές, ότι δηλαδή ο υπογράφων έχει υπό τον πλήρη έλεγχο του το σύστημα δημιουργίας υπογραφής, κατά την ώρα υπογραφής. Όπως θα δούμε, εκτός αν δεν υπάρξει καμία θεαματική τεχνολογική εξέλιξη τα επόμενα χρόνια, για την δημιουργία μίας ηλεκτρονικής υπογραφής και για την μετέπειτα χρήση της, απαιτείται ένας ολόκληρος μηχανισμός, ο οποίος δρα ως γέφυρα μεταξύ της οντότητας η οποία υπογράφει και βρίσκεται στον φυσικό κόσμο, και της αναπαράστασης της στον ηλεκτρονικό κόσμο, η οποία και θα είναι αυτή που ουσιαστικά θα λαμβάνει μέρος στις ηλεκτρονικές συναλλαγές.

Το κύριο χαρακτηριστικό του συγκεκριμένου μηχανισμού είναι η ύπαρξη μιας νέας κατηγορίας παροχής υπηρεσιών, των *υπηρεσιών ηλεκτρονικής πιστοποίησης*, μέσω των οποίων θα γίνεται η

προαναφερθείσα αντιστοίχηση μεταξύ φυσικού και ηλεκτρονικού κόσμου. Οι οντότητες που θα προσφέρουν την συγκεκριμένη υπηρεσία, συμμετέχουν ως ενδιάμεσοι σε κάθε ηλεκτρονική συναλλαγή, αποκτώντας έτσι κυρίαρχο ρόλο. Οι συγκεκριμένες οντότητες συνήθως δεν περιορίζονται μόνο στην παροχή της συγκεκριμένης υπηρεσίας, αλλά δραστηριοποιούνται σε όλο το φάσμα των υπηρεσιών που σχετίζονται με την αντιστοίχηση μιας συμβατικής και μιας ηλεκτρονικής συναλλαγής. Λειτουργούν έτσι ως *Έμπιστες Τρίτες Οντότητες*, με την ευρεία έννοια, για τα συναλλασσόμενα μέρη. Όπως είναι φυσικό, η παρουσία τους και ο ρόλος τους ανατρέπει ισορροπίες οι οποίες είχαν εδραιωθεί εδώ και αρκετά χρόνια. Κρίνεται απαραίτητη, κατά συνέπεια η διαμόρφωση ενός συγκεκριμένου πλαισίου το οποίο και θα ρυθμίζει την λειτουργία τους. Η μελέτη ακριβώς αυτού του πλαισίου θα μας απασχολήσει στην εργασία που ακολουθεί.

1.3 Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικών Υπογραφών.

Από τα μέσα της προηγούμενης δεκαετίας διεθνείς και περιφερειακοί οργανισμοί συνειδητοποίησαν την ανάγκη για την δημιουργία ενός πλαισίου που θα ρυθμίζει την παροχή υπηρεσιών πιστοποίησης και έμπιστης τρίτης οντότητας και για τον σκοπό αυτό προέβησαν στην δημιουργία των πρώτων κανονισμών. Η συγκεκριμένη τάση δεν άργησε να μεταβεί και στα νομικά καθεστώτα των πιο ανεπτυγμένων χωρών.

Κεντρική έννοια στις περισσότερες από αυτές τις προσπάθειες είναι αυτή της *διαπίστευσης (accreditation)*. Η διαπίστευση είναι το αποτέλεσμα μίας διαδικασίας αποτίμησης των διοικητικών, λειτουργικών και τεχνικών διαδικασιών/συστημάτων μιας έμπιστης τρίτης οντότητας, στην συγκεκριμένη περίπτωση, η οποία *ενδεχομένως* συνοδεύεται με κάποια αδειοδότηση ή νομική αναγνώριση των υπηρεσιών που παρέχονται από τον συγκεκριμένο οργανισμό. Είναι εύλογη η σχέση της διαπίστευσης με τα διάφορα πρότυπα αξιολόγησης της ασφάλειας υπολογιστικών και πληροφοριακών συστημάτων. Η χρήση των προτύπων έχει διπλό ρόλο. Αφενός να ελέγξει τα πληροφοριακά συστήματα των παρόχων υπηρεσιών, όπως και τις λειτουργικές και διοικητικές τους διαδικασίες (ποιοτικά πρότυπα). Σε πιο τεχνικό επίπεδο έχει ως στόχο την παροχή συμβατότητας για τις διάφορες εφαρμογές (τεχνικά πρότυπα). Η διαπίστευση δεν περιορίζεται όμως μόνο στα πρότυπα που έχουν σχέση με τα πληροφοριακά συστήματα, καθώς αφορά και υπηρεσίες οι οποίες δεν έχουν υπαρκτή σχέση με πληροφορική, όπως για παράδειγμα η εξακρίβωση της ταυτότητας μιας οντότητας.

Πρέπει να σημειωθεί πάντως ότι η ρυθμιστική δραστηριότητα των τελευταίων ετών έχει οδηγήσει σε μία πληθώρα κανονισμών, συστάσεων, νομικών πράξεων και οδηγιών, με αποτέλεσμα ενώ σε τεχνικό επίπεδο έχει επιτευχθεί συμβατότητα, να παρατηρούμε το ‘παράδοξο’ ασύμβατων καθεστώτων. Εισαγωγικά αξίζει να αναφέρουμε ορισμένους από τους εθνικούς και περιφερειακούς φορείς που εμπλέκονται στην διαδικασία προτυποποίησης και ρύθμισης.

Σε ότι αφορά τους νομικούς κανονισμούς η όλη κινητικότητα ξεκίνησε από τον οργανισμό Ηνωμένων Εθνών και την νομική επιτροπή του για το διεθνές εμπόριο (UNCITRAL), η οποία το 1996 εξέδωσε ένα

πρότυπο νόμου για το ηλεκτρονικό εμπόριο (UNCITRAL Model Law on Electronic Commerce) το οποίο είχε θετική αποδοχή. Την ίδια χρονιά ο σύνδεσμος ABA (American Bar Association) εξέδωσε συστάσεις για ψηφιακές υπογραφές (ABA Digital Signature Guidelines). Από τις πρώτες χώρες που νομοθέτησαν για ψηφιακές υπογραφές ήταν η Γερμανία, η οποία διέθετε νόμο για ψηφιακές υπογραφές από το 1997. Επίσης, στις ΗΠΑ, η πρώτη πολιτεία που νομοθέτησε ήταν η Utah (1995), η νομική πράξη της οποίας είναι η πρώτη που εισάγει ένα πλαίσιο διαπίστευσης. Τα δύο σημαντικότερα σημεία, σε όλες αυτές τις νομοθετικές παρεμβάσεις είναι η *Οδηγία του Ευρωπαϊκού Συμβουλίου σχετικά με ένα Κοινοτικό Πλαίσιο για Ηλεκτρονικές Υπογραφές* (Δεκέμβριος 1999), καθώς επίσης και η *Ομοσπονδιακή Πράξη για τις Ηλεκτρονικές Υπογραφές στο Διεθνές και Εθνικό Εμπόριο* (Ιούνιος 2000). Τέλος, από τις πιο σημαντικές προσπάθειες διεθνώς, έχουν γίνει στην Αυστραλία και στον Καναδά.

Πολλές φορές οι νομικές και ρυθμιστικές προσπάθειες συνοδεύτηκαν και με μία ευρείας έκταση διαδικασία προτυποποίησης. Αυτό συμβαίνει ήδη σε όλη την Ευρώπη, όπου βρίσκεται σε εξέλιξη η *EESSI (European Electronic Signature Standardization Initiative)*, η οποία έχει ως στόχο την δημιουργία εκείνων των προτύπων τα οποία θα βοηθήσουν την αποτελεσματική εφαρμογή της οδηγίας. Βέβαια πρότυπα τόσο τεχνικά όσο και ποιοτικά τα οποία έχουν εφαρμογή στην διαπίστευση υπάρχουν εδώ και πολύ καιρό. Έτσι για παράδειγμα έχουμε τα πρότυπα του *ISO (International Standards Organization)* για ένα πλαίσιο αυθεντικοποίησης, τα πρότυπα (Request For Comments - RFCs) της *IETF (Internet Engineering Task Force)* καθώς επίσης και τα πρότυπα του *NIST (National Institute Of Standards And Technology)*. Επίσης όπως είναι φυσικό υπάρχουν και πρότυπα που προέρχονται από φορείς της αγοράς, όπως η σειρά προτύπων *PKCS* από την RSA Securities Inc.

Με τα παραπάνω θέματα θα ασχοληθούμε διεξοδικά σε όλη την έκταση της εργασίας. Σημειώνουμε εξ' αρχής ότι η πληθώρα αυτή, περισσότερο δυσχεραίνει παρά διευκολύνει την χρήση ηλεκτρονικών υπογραφών. Αξίζει επίσης να σημειωθεί ότι, οι ρυθμιστικές και νομικές προσπάθειες αυτές, κάθε άλλο παρά εύκολες μπορούν να χαρακτηριστούν, καθώς από την φύση τους απαιτούν τον συμβιβασμό ετερογενών γνωστικών χώρων. Απαιτείται για παράδειγμα η προσαρμογή των νομικών συστημάτων στους ρυθμούς της τεχνολογίας και της αγοράς, έτσι ώστε να μην υπάρχει η διαφορά φάσης που παρατηρείται σήμερα και αποτελεί την αιτία αφ' ενός για επιχειρηματικές πρακτικές που ζημιώνουν τον τελικό καταναλωτή και αφ' ενός για την συγκάλυψη εγκληματικών δραστηριοτήτων. Επιπλέον οι συγκεκριμένες προσπάθειες διακρίνονται, όπως θα δούμε, από αντικρουόμενους στόχους, καθώς καλούνται αφενός να βοηθήσουν την ανάπτυξη των υπηρεσιών πιστοποίησης και αφετέρου να προστατεύσουν τα συμφέροντα του καταναλωτή. Στην εργασία αυτή θα ασχοληθούμε εκτεταμένα με αυτά τα διλήμματα, καθώς επίσης και με τις περισσότερες από τις βασικές νομικές και ρυθμιστικές προσπάθειες.

1.4 Σκοπός και Διάρθρωση της εργασίας.

Στην εργασία που ακολουθεί, αρχικά, θα παρουσιάσουμε αναλυτικά όλα τις τεχνολογίες, τα πρότυπα

και τις διαδικασίες που κρίνονται απαραίτητες για την παροχή υπηρεσιών πιστοποίησης. Η παρουσίαση αυτή έχει ως στόχο την κατανόηση της απαιτούμενης υποδομής για ηλεκτρονικές υπογραφές και του αναπόσπαστου ρόλου των παρόχων υπηρεσιών πιστοποίησης. Έχοντας αναπτύξει την συγκεκριμένη βάση, θα προχωρήσουμε στην ανάλυση των πιο σημαντικών ρυθμιστικών πλαισίων για τις συγκεκριμένες οντότητες για την ανάδειξη του ρόλου της διαπίστευσης. Στόχος μας είναι η κριτική ανάλυση των απαιτήσεων λειτουργίας των παρόχων υπηρεσιών πιστοποίησης, οι οποίες τίθενται μέσω της διαπίστευσης, καθώς επίσης και των συνεπειών τους στο ηλεκτρονικό περιβάλλον συναλλαγών και καταναλωτή.

Η εργασία έχει δομηθεί ως εξής:

- Στο κεφάλαιο 2, γίνεται μία επισκόπηση των διάφορων τεχνολογιών δημιουργίας ηλεκτρονικών υπογραφών, της υποδομής την οποία απαιτούν καθώς επίσης και των μειονεκτημάτων και πλεονεκτημάτων τους. Αναδεικνύεται έτσι ο σημαντικός ρόλος των έμπιστων τρίτων οντοτήτων. Στόχος του κεφαλαίου αυτού είναι να αποτελέσει μία σωστή τεχνολογική βάση, πάνω στην οποία θα στηριχθούν τα επιχειρήματα τα οποία θα αναπτυχθούν στα επόμενα κεφάλαια.
- Στο κεφάλαιο 3, έχοντας παρουσιάσει όλες τις τεχνολογικές λύσεις σε ό,τι αφορά τις ηλεκτρονικές υπογραφές θα εξετάσουμε τα ολοκληρωμένα συστήματα τα οποία μπορούν να χρησιμοποιηθούν για την εφαρμογή των συγκεκριμένων τεχνολογιών στην πράξη. Τα συστήματα αυτά αφορούν τόσο τις λειτουργίες που σχετίζονται με την δημιουργία και επαλήθευση μιας ηλεκτρονικής υπογραφής, όσο και με την υποδομή για τις υπηρεσίες πιστοποίησης. Για τα συστήματα αυτά θα επικεντρωθούμε τόσο στις λειτουργικές απαιτήσεις όσο και στις απαιτήσεις ασφαλείας που τα χαρακτηρίζουν. Τέλος θα εισάγουμε τις έννοιες της πολιτικής υπογραφής και πιστοποίησης, οι οποίες δίνουν νόημα στην χρήση των παραπάνω συστημάτων. Απώτερος στόχος όλων αυτών των συστημάτων είναι να εξομοιωθεί το περιβάλλον συμβατικής υπογραφής, με όλες τις ‘ανέσεις’ που το χαρακτηρίζουν, στον ηλεκτρονικό κόσμο.
- Στο κεφάλαιο 4, θα αλλάξουμε οπτική γωνία και θα μεταβούμε από την τεχνολογική στην νομική σκοπιά. Στόχος του είναι η παρουσίαση των πιο σημαντικών νομικών και ρυθμιστικών πρωτοβουλιών σχετικών με της ηλεκτρονικές υπογραφές και τις υπηρεσίες πιστοποίησης. Συγκεκριμένα παρουσιάζονται τα πλαίσια διαπίστευσης που έχουν προκύψει στις ΗΠΑ, την Αυστραλία, τον Καναδά και την Ευρωπαϊκή Ένωση, όπου δίνουμε και ιδιαίτερη έμφαση, λόγω των άμεσων επιπτώσεων της. Επίσης σε ό,τι αφορά την Ευρωπαϊκή Ένωση περιγράφουμε και τις σημαντικότερες εθνικές πρωτοβουλίες, της Αγγλίας και της Γερμανίας.
- Το κεφάλαιο 5, λαμβάνει ως βάση τις διαφορές στις αρχές, την υλοποίηση και τα λοιπά χαρακτηριστικά των νομικών προσπαθειών, που θα έχουμε παρουσιάσει μέχρι εκείνο το σημείο και προχωρά σε μία κριτική ανάλυση τους.
- Τέλος στο κεφάλαιο 6, συνοψίζουμε τα σημαντικότερα σημεία της εργασίας και καταλήγουμε στα συμπεράσματα της όλης μελέτης.

2 Βασικές Έννοιες.

2.1 Εισαγωγή

Στο παρόν κεφάλαιο θα θέσουμε τα θεμέλια της μελέτης που ακολουθεί. Αρχικά θα περιγράψουμε τις τεχνολογικές λύσεις, που υπάρχουν στον τομέα της αυθεντικοποίησης και των ηλεκτρονικών υπογραφών. Όπως είναι λογικό θα επικεντρώσουμε την προσοχή μας στην Τεχνολογία Δημοσίου Κλειδιού, καθώς η υποδομή που αυτή απαιτεί είναι συνήθως ο στόχος της διαπίστευσης. Εκ των προτέρων αξίζει να σημειώσουμε, ότι η συγκεκριμένη τεχνολογία δεν είναι δυνατόν να παρέχει από μόνη της όλες τις λύσεις. Θα εξηγήσουμε την αιτία γι' αυτό, έτσι ώστε να φανεί το ότι η παρέμβαση από τα 'ανώτερα' επίπεδα (λειτουργικό, διαδικαστικό ρυθμιστικό-νομικό) είναι αναγκαία για να καλύψει τις όποιες ατέλειες. Για να είναι εφικτή όμως μία τέτοια παρέμβαση, αλλά και για να μπορέσει στοιχειωδώς να λειτουργήσει μία τέτοια υποδομή, απαιτείται η θεμελίωση της σε τεχνικό επίπεδο με μία σειρά από πρότυπα. Έτσι, για όλες τις τεχνολογίες που θα περιγράψουμε θα αναφέρουμε ποια τεχνικά πρότυπα υπάρχουν και θα αναπτύξουμε συνοπτικά τα πιο σημαντικά από αυτά.

2.2 Αυθεντικοποίηση

Η αυθεντικοποίηση (authentication) είναι από τα πιο σημαντικά χαρακτηριστικά μιας ηλεκτρονικής συναλλαγής, αφού παρέχει μία ένδειξη – για να μην είμαστε και υπερβολικά αισιόδοξοι – της ταυτότητας των οντοτήτων που συμμετέχουν. Ακόμα και στην περίπτωση όμως, που η συγκεκριμένη ένδειξη είναι βεβαιότητα, σημειώνουμε, ότι καμία μέθοδος αυθεντικοποίησης δεν πληροί από μόνη της ιδιότητες που πρέπει να έχει μία υπογραφή, όπως αυτές αναφέρθηκαν στην εισαγωγή. Ως παράδειγμα στην παραπάνω διαπίστωση μπορούμε να αναφέρουμε την επίδειξη πρόθεσης, η οποία επιτυγχάνεται με τις ιδιόχειρες υπογραφές.

Σύμφωνα, λοιπόν με το **[Gritzalis, 1998]** η αυθεντικοποίηση είναι η διαδικασία εκείνη, η οποία έχει ως στόχο την επιβεβαίωση της ταυτότητας ενός χρήστη. Η αυθεντικοποίηση αποτελεί την συνέχεια της αναγνώρισης (identification) μιας οντότητας και δεν πρέπει να συγχέεται με αυτήν. Στην βιβλιογραφία αναφέρονται οι εξής κατηγορίες μεθόδων αυθεντικοποίησης **{[Ford, 2001], [Polemi, 1997]}**:

- *Επίδειξη Γνώσης*: Η οντότητα που αυθεντικοποιείται επιδεικνύει στο σύστημα ότι όντως γνωρίζει κάτι που το σύστημα θεωρεί ότι μόνο αυτή θα έπρεπε να γνωρίζει. Παραδείγματα της κλασικής αυτής μεθόδου είναι τα συνθηματικά και τα PINs (Personal Identification Numbers).
- *Επίδειξη Κατοχής*: Η οντότητα που αυθεντικοποιείται επιδεικνύει στο σύστημα ότι όντως κατέχει ένα αντικείμενο που το σύστημα έχει αποδώσει σε αυτή. Ένα παράδειγμα της μεθόδου αυτής αποτελεί η χρήση μαγνητικής κάρτας.
- *Επίδειξη Ιδιότητας*: Η οντότητα που αυθεντικοποιείται επιδεικνύει στο σύστημα μία μοναδική της

ιδιότητα. Ως παραδείγματα εδώ μπορούμε να αναφέρουμε τις βιομετρικές τεχνικές, οι οποίες μπορούν να χρησιμοποιηθούν για να αναγνωρίσουν ανθρώπινες οντότητες, με βάση μοναδικά φυσικά τους χαρακτηριστικά (ίριδα, δακτυλικό αποτύπωμα, DNA κτλ.).

Οι μέθοδοι αυθεντικοποίησης που προαναφέρθηκαν, σε οποιαδήποτε κατηγορία και αν ανήκουν, είναι ατελείς από μόνες τους. Στην πράξη εφαρμόζεται ένας συνδυασμός από αυτές (*two factor authentication*), ενώ είναι απαραίτητη η ύπαρξη κάποιας υποστηρικτικής υποδομής. Για παράδειγμα, τα συνθηματικά αποθηκεύονται πολλές φορές σε μαγνητικές κάρτες, ενώ συγχρόνως απαιτείται ένα αρχείο στο οποίο θα υπάρχουν ήδη για σύγκριση. Στις βιομετρικές μεθόδους απαιτείται είτε μία βάση δεδομένων όπου θα υπάρχουν αποθηκευμένα βιομετρικά χαρακτηριστικά και με τα οποία θα συγκρίνεται η μέτρηση που γίνεται κατά την διάρκεια της αυθεντικοποίησης. Εναλλακτικά μπορεί κάθε οντότητα να έχει στην κατοχή της ένα αντικείμενο, το οποίο θα περιέχει καταχωρημένα τα βιομετρικά χαρακτηριστικά της με τα οποία θα γίνει σύγκριση κατά την αυθεντικοποίηση. Βλέπουμε έτσι πώς μπορούν να συνδυαστούν οι μέθοδοι διαφορετικών κατηγοριών, σε ένα ευρύτερο σύστημα αυθεντικοποίησης.

2.2.1 Κρυπτογραφία Δημοσίου Κλειδιού

Η αυθεντικοποίηση μπορεί να επιτευχθεί και με χρήση ασύμμετρων κρυπτοσυστημάτων. Η συγκεκριμένη εφαρμογή της Κρυπτογραφίας προτάθηκε[2] από τους Diffie και Hellman **[Diffie, 1976].** Η κρυπτογραφία δημοσίου κλειδιού αναπτύχθηκε για να λύσει το πρόβλημα της ασφαλούς επικοινωνίας μεταξύ πολλών χρηστών οι οποίοι χρησιμοποιούν μη ασφαλή δίκτυα. Συγκεκριμένα, μέχρι την εμφάνιση της, η παραδοσιακή συμμετρική κρυπτογραφία απαιτούσε την ύπαρξη ενός ασφαλούς διαύλου, μέσω του οποίου θα μπορούσε να μεταδοθεί το κλειδί κρυπτογράφησης και αποκρυπτογράφησης το οποίο καλούνται να χρησιμοποιήσουν οι οντότητες που επικοινωνούν. Εφ΄όσον κάθε οντότητα πρέπει να χρησιμοποιεί διαφορετικά κλειδιά για κάθε άλλη οντότητα με την οποία επικοινωνεί (μέσω ασφαλούς διαύλου, φυσικά) είναι φανερό ότι η συμμετρική κρυπτογραφία είναι δύσκολο να αναπτυχθεί σε μεγάλη κλίμακα.

Οι Diffie και Hellman, έλυσαν το συγκεκριμένο πρόβλημα με την άρση της βασικής υπόθεσης της κρυπτογραφίας, η οποία ήθελε την ύπαρξη του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση. Πρότειναν, έτσι, την χρήση δύο κλειδιών από κάθε χρήστη, τα οποία βέβαια σχετίζονται μαθηματικά. Το ένα θα χρησίμευε για κρυπτογράφηση και το άλλο για αποκρυπτογράφηση. Η ειδοποιός διαφορά της συγκεκριμένης τεχνικής είναι ότι το κλειδί της κρυπτογράφησης ενός χρήστη, δεν χρειαζόταν πλέον να είναι μυστικό. Επιβάλλεται μάλιστα να είναι δημόσια προσβάσιμο, έτσι ώστε οποιοσδήποτε να μπορούσε να το χρησιμοποιήσει για να αποστείλει μηνύματα με ασφάλεια. Το κλειδί της αποκρυπτογράφησης ήταν αυτό το οποίο κάθε χρήστης έπρεπε να διατηρεί ιδιωτικό, έτσι ώστε μόνο αυτός να μπορούσε έχει πρόσβαση στα κρυπτογραφημένα μηνύματα.

[2] Για την ακρίβεια, όπως αναφέρεται και στο [Diffie, 1976] αλλά και στο [Schneier, 1996], η ιδέα της κρυπτογραφίας δημοσίου κλειδιού ανήκει στον Merkle, η προσέγγιση του [Diffie, 1976] ήταν όμως πιο ολοκληρωμένη.

Αυτό που είναι ενδιαφέρον, είναι ότι οι Diffie και Hellman, παρατήρησαν ότι το ασύμμετρο κρυπτοσύστημα τους μπορούσε να λειτουργήσει και σε μία άλλη κατάσταση. Αν η κρυπτογράφηση γινόταν όχι με το δημόσιο κλειδί του παραλήπτη, αλλά με το ιδιωτικό κλειδί του αποστολέα και υπό την υπόθεση ότι ο κάθε ιδιωτικό κλειδί *βρισκόταν με βεβαιότητα και υπό τον πλήρη έλεγχο κάθε χρήστη*, τότε έχουμε μία μέθοδο αυθεντικοποίησης με επίδειξη κατοχής (του ιδιωτικού κλειδιού). Η μέθοδος αυτή ονομάστηκε από τους δημιουργούς της *ψηφιακή υπογραφή*...

2.2.2 Ψηφιακές Υπογραφές

2.2.2.1 Δημιουργία και Επαλήθευση.

Ο όρος ψηφιακή υπογραφή έχει ταυτιστεί με την μέθοδο αυθεντικοποίησης με χρήση ασύμμετρων κρυπτοσυστημάτων. Μία ψηφιακή υπογραφή μπορεί να παραχθεί ως εξής:

1. Ο υπογράφων συντάσσει το μήνυμα το οποίο θέλει να υπογράψει.
2. Επειδή το μήνυμα μπορεί να έχει αυθαίρετα μεγάλο μήκος, το σύστημα χρησιμοποιεί μία μονόδρομη συνάρτηση σύνοψης *(one way hash function)*, η οποία μετατρέπει το μεταβλητού μήκους κείμενο, σε μία συμβολοσειρά σταθερού μήκους (συνήθως 128 ή 160 bits).
3. Ο υπογράφων χρησιμοποιώντας το ιδιωτικό του κλειδί, κρυπτογραφεί την σύνοψη του μηνύματος.
4. Η κρυπτογραφημένη σύνοψη προσαρτάται στο μήνυμα και αποστέλλεται.

Ο παραλήπτης του μηνύματος, μπορεί να καταλάβει ότι το μήνυμα προήρθε από τον υπογράφοντα με την παρακάτω διαδικασία:

1. Ο παραλήπτης αποσπά την κρυπτογραφημένη σύνοψη από το μήνυμα που έλαβε.
2. Χρησιμοποιώντας την ίδια συνάρτηση σύνοψης με τον αποστολέα, παράγει ξανά την σύνοψη του μηνύματος.
3. Χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα αποκρυπτογραφεί την κρυπτογραφημένη σύνοψη.
4. Τέλος συγκρίνει τις δύο συνόψεις: αυτή που παρήγαγε κατευθείαν από το μήνυμα και αυτή που προέκυψε από την αποκρυπτογράφηση. Αν ταυτίζονται, τότε το δημόσιο κλειδί που χρησιμοποιήθηκε για την αποκρυπτογράφηση της σύνοψης, αντιστοιχεί στο ιδιωτικό κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση.

Η συγκεκριμένη μέθοδος δημιουργίας ψηφιακών υπογραφών εγγυάται την *ακεραιότητα* του μηνύματος. Πράγματι, αν το μήνυμα έχει μεταβληθεί έστω και κατά το ελάχιστο καθ' οδόν, η σύνοψη που θα παραχθεί από τον παραλήπτη θα είναι διαφορετική από την κρυπτογραφημένη. Αν έχει αλλαχθεί η κρυπτογραφημένη σύνοψη, πάλι δεν θα υπάρξει ταύτιση. Τέλος, οι μαθηματικές ιδιότητες των συναρτήσεων σύνοψης μας εξασφαλίζουν, ότι δεν είναι δυνατόν τυχαία αλλαγή και του μηνύματος και της κρυπτογραφημένης σύνοψης να οδηγήσουν σε επιτυχή επαλήθευση. Μία σημαντική ιδιότητα των ψηφιακών υπογραφών λοιπόν την οποία δεν διαθέτουν οι συμβατικές, είναι ότι μια ψηφιακή υπογραφή είναι *διαφορετική* για κάθε

κείμενο. Υπό αυτή την σκοπιά, είναι πιο ασφαλής, καθώς στις συμβατικές υπογραφές είναι πολύ εύκολο, για παράδειγμα, σε περίπτωση που η υπογραφή βρίσκεται στην τελευταία σελίδα ενός πολυσέλιδου κειμένου, να αλλαχθούν οι προηγούμενες και η υπογραφή να ισχύει. Κάτι τέτοιο δεν είναι δυνατό με τις ψηφιακές υπογραφές.

Αν υποτεθεί τώρα, ότι *το ιδιωτικό κλειδί, ανήκει αποκλειστικά στον υπογράφοντα και βρίσκεται πάντα υπό την κατοχή του*, μπορούμε να πούμε ότι η ταυτότητα του υπογράφοντος έχει *αυθεντικοποιηθεί*. Επιπλέον με δεδομένη την τήρηση της παραπάνω συνθήκης, ο υπογράφων δεν μπορεί να αρνηθεί ότι όντως υπέγραψε, καθώς, εφ'όσον η επαλήθευση έγινε με το δημόσιο κλειδί που έχει αποδοθεί στον ίδιο, μόνο με το ιδιωτικό κλειδί (το οποίο υποθέσαμε ότι ανήκει αποκλειστικά σε αυτόν) μπορούσε να έχει δημιουργηθεί η υπογραφή. Επιτυγχάνεται έτσι και η ιδιότητα της μη αποποίησης (non – repudiation), από τις ιδιότητες μιας ηλεκτρονικής συναλλαγής που παραθέσαμε αρχικά.

Η παραπάνω λεπτομέρεια, της κατοχής του ιδιωτικού κλειδιού, είναι πολύ σημαντική όπως θα δούμε στην συνέχεια. Προτού προχωρήσουμε, όμως αξίζει να σχολιάσουμε, για λόγους πληρότητας, ορισμένα σημαντικά στοιχεία, τεχνικής κυρίως φύσεως, που προέκυψαν από την παραπάνω περιγραφή.

2.2.2.2 Συναρτήσεις Σύνοψης.

Μία ασφαλής μονόδρομη συνάρτηση σύνοψης είναι μία μαθηματική συνάρτηση, η οποία έχει τις εξής ιδιότητες **[Schneier, 1996]:**

- Για κάθε μήνυμα παράγει με εύκολο και γρήγορο τρόπο μοναδική σύνοψη σταθερού μεγέθους.
- Είναι υπολογιστικά αδύνατο, να παραχθεί το αρχικό μήνυμα δεδομένης της σύνοψης.
- Είναι υπολογιστικά αδύνατο, να βρεθεί ένα μήνυμα διάφορο του αρχικού το οποίο να παράγει την ίδια σύνοψη με αυτό.
- Είναι υπολογιστικά αδύνατο να βρεθούν δύο τυχαία και διαφορετικά μεταξύ τους μηνύματα τα οποία να παράγουν την ίδια σύνοψη.

Στην πράξη χρησιμοποιούνται οι εξής συναρτήσεις σύνοψης: η **MD5**, η οποία παράγει συνόψεις μήκους 128 bits και η **SHA** (Secure Hash Algorithm), η οποία παράγει συνόψεις μήκους 160 bits και η **RIPEMD-160** (Race Integrity Primitives Evaluation Message Digest – 160) με σύνοψη μήκους 160 bits επίσης. Όλες έχουν προτυποποιηθεί εκτενώς. Το κυρίαρχο πρότυπο για την SHA είναι το πρότυπο του NIST FIPS 180-1, ενώ για την RIPEMD-160 το πρότυπο ISO 10118-3. Από τις παραπάνω κρυπτογραφικά, πιο ασφαλείς θεωρούνται οι δύο τελευταίες, οι οποίες αναμένεται να επικρατήσουν πλήρως τα επόμενα χρόνια.

2.2.2.3 Πρότυπα και Αλγόριθμοι Κρυπτογράφησης

Οι ασύμμετροι αλγόριθμοι κρυπτογράφησης, οι οποίοι μπορούν να χρησιμοποιηθούν για τις ψηφιακές υπογραφές μπορούν να χωριστούν σε τρεις κατηγορίες, κάθε μία από τις οποίες βασίζεται σε ένα

δυσεπίλυτο μαθηματικό πρόβλημα.

- **Σχήματα Παραγοντοποίησης Ακεραίων** (**Integer Factorization Schemes - IFS**). Οι αλγόριθμοι που χρησιμοποιούν βασίζουν την ασφάλεια τους στην δυσκολία παραγοντοποίησης ενός πολύ μεγάλου ακεραίου. Παραδείγματα τέτοιων αλγορίθμων είναι οι RSA και οι Rabin.
- **Σχήματα Ακεραίου Λογαρίθμου** (**Discrete Logarithm Schemes – DLS**). Οι αλγόριθμοι της κατηγορίας αυτής βασίζουν την ασφάλεια τους στην δυσκολία εύρεσης του λογαρίθμου ενός ακεραίου σε οποιοδήποτε πεπερασμένο σώμα. Τέτοιοι αλγόριθμοι είναι οι El Gamal, Schnorr, DSA.
- **Σχήματα Ελλειψοειδών Καμπυλών** (**Elliptic Curve Schemes – ECS**). Οι αλγόριθμοι της συγκεκριμένης κατηγορίας βασίζουν την δυσκολία τους στην εύρεση του διακριτού λογαρίθμου σε ελλειψοειδείς καμπύλες.

Για κάθε μία από τις παραπάνω κατηγορίες υπάρχει εκτενής προτυποποίηση. Τα πρότυπα που αναφέρονται στους αλγόριθμους IFS, και κυρίως στον αλγόριθμο RSA είναι τα εξής:

- **PKCS 1: RSA Cryptography Standard**
- **ANSI X9.31**

Το πιο σημαντικό από τα δύο αυτά πρότυπα είναι το PKCS#1 **[PKCS#1, 2001]**. Αν θέλαμε να συνοψίσουμε το συγκεκριμένο πρότυπο με μία φράση, θα λέγαμε ότι είναι ένας οδηγός υλοποίησης του συγκεκριμένου αλγορίθμου. Γενικά τα πρότυπα της συγκεκριμένης οικογένειας καλύπτουν όπως προαναφέραμε ανάγκες υλοποίησης. Το πρότυπο ANSI X9.31 είναι η επίσημη προτυποποίηση για τις ΗΠΑ του συγκεκριμένου αλγορίθμου και σε γενικές γραμμές καλύπτει τις ίδιες περιοχές με το PKCS#1.

Τα πρότυπα που αναφέρονται στους αλγόριθμους **DLS** είναι τα εξής:

- **FIPS 186-1. Digital Signature Standard.**

Τα πρότυπα της οικογένειας FIPS εκδίδονται από το NIST, τον εθνικό φορέα προτυποποίησης των ΗΠΑ σε θέματα τεχνολογίας. Τα πρότυπα που εκδίδει ο συγκεκριμένος φορέας απευθύνονται στα ομοσπονδιακά πρακτορεία των ΗΠΑ, όπου η εφαρμογή τους είναι υποχρεωτική, αλλά χρησιμοποιούνται εκτενέστατα και ως σημείο αναφοράς από άλλους δημοσίους και ιδιωτικούς οργανισμούς των ΗΠΑ.

Το πρότυπο 186-1 είναι ευρύτερα γνωστό και ως **DSS** (Digital Signature Standard). Στο συγκεκριμένο πρότυπο περιγράφεται λοιπόν αναλυτικά ο αλγόριθμος ψηφιακών υπογραφών DSA και παρέχεται τεκμηρίωση του με μαθηματικές αποδείξεις. Παρέχονται επίσης και διάφορες οδηγίες για την υλοποίηση όλων των σημείων του συγκεκριμένου αλγόριθμου – για παράδειγμα πώς θα δημιουργηθούν οι διάφοροι τυχαίοι αριθμοί, οι διάφοροι πρώτοι κτλ. Επίσης παρέχονται οδηγίες για το πώς μπορούν να γίνουν κάποιες βελτιώσεις ως προς την ταχύτητα του, χωρίς να υπάρχει κίνδυνος για μείωση της ασφάλειας του.

Τέλος τα πρότυπα τα οποία αναφέρονται στους αλγόριθμους **ECS** είναι τα:

- **ANSI X9.62**
- **FIPS 186-2**

- **IEEE P1363-2000**
- **ISO 14888**
- **SEC-1, SEC-2.**
- **PKCS 13: Elliptic Curve Cryptography Standard**

Περισσότερες λεπτομέρειες για το καθένα αναφέρουμε παρακάτω:

- **ANSI X9.62**

Το συγκεκριμένο πρότυπο υιοθετήθηκε από τον ANSI τον Ιανουάριο του 1999. Παρέχει συστάσεις για το ποια είδη πεπερασμένων σωμάτων μπορούν να χρησιμοποιηθούν για κρυπτοσυστήματα δημοσίου κλειδιού που βασίζονται σε ελλειψοειδείς καμπύλες και άλλα τέτοια χαρακτηριστικά τα οποία μπορούν να προσδώσουν ασφάλεια και συμβατότητα σε ένα τέτοιο κρυπτοσύστημα.

- **FIPS 186-2**

Το συγκεκριμένο πρότυπο **[FIPS 186-2, 2000]** επεκτείνει το DSS (FIPS 186-1)**,** ώστε να είναι δυνατή η χρήση για την οποιουδήποτε αλγόριθμου δημοσίου κλειδιού (RSA, DSA, ECDSA) για την δημιουργία και επαλήθευση των ψηφιακών υπογραφών. Παρ' όλα αυτά το συγκεκριμένο πρότυπο καθορίζει ότι για να είναι συμβατά με αυτό συστήματα ψηφιακών υπογραφών πρέπει να χρησιμοποιούν την συνάρτηση σύνοψης SHA-1 η οποία έχει προτυποποιηθεί με το FIPS 180-1.

- **IEEE P1363-2000.**

Το συγκεκριμένο πρότυπο ενεκρίθη από την IETF, τον Αύγουστο του 2000. Δεν είναι πρότυπο με την στενή έννοια του όρου καθώς περιγράφει γενικά ένα σύνολο από τεχνικές δημοσίου κλειδιού τόσο για κρυπτογράφηση όσο και για ψηφιακές υπογραφές, χωρίς να θέτει ελάχιστες προδιαγραφές ασφαλείας. Μπορεί καλύτερα να θεωρηθεί ως ένα σύνολο αναφοράς τεχνικών από τις οποίες μπορούν να επιλέξουν οι διάφορες εφαρμογές.

- **SEC-1 και SEC-2.**

Τα παραπάνω πρότυπα εκδίδονται από το **SECG** (Standards For Efficient Cryptography Group), έναν οργανισμό που ως στόχο έχει να προωθήσει την συμβατότητα μεταξύ των διαφόρων κρυπτογραφικών πρωτοκόλλων. Το SEC-1 περιγράφει διάφορους αλγόριθμους ελλειψοειδών καμπύλων (και του ECDSA). Το SEC-2 περιγράφει ορισμένες παραμέτρους των παραπάνω αλγορίθμων με στόχο την συμβατότητα αλλά και την παροχή ενός ελάχιστου επίπεδου ασφάλειας.

- **ISO 14888.**

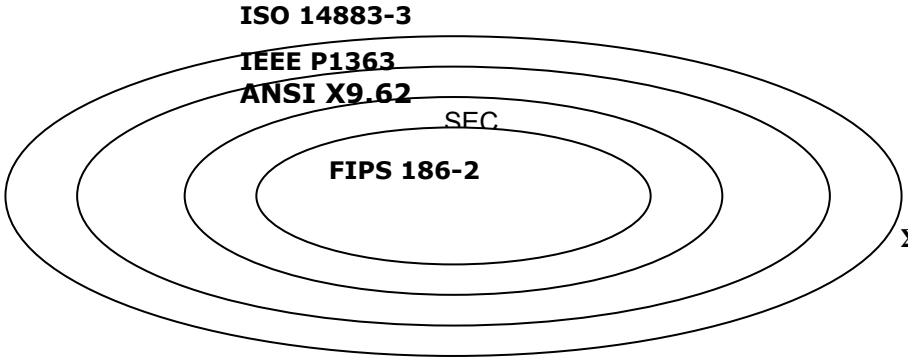
Το συγκεκριμένο πρότυπο του ISO περιγράφει σε γενικές γραμμές αλγόριθμους δημοσίου κλειδιού, όπως και τον ECDSA.

- **PKCS #13: Elliptic Curve Cryptography Standard**

Δεν έχει ολοκληρωθεί ακόμα αλλά στην πλήρη του έκδοση θα είναι κάτι αντίστοιχο του PKCS #1 για κρυπτοσυστήματα σε ελλειψοειδείς καμπύλες.

Ο 'ελάχιστος κοινός παρονομαστής' συμβατότητας για τα συγκεκριμένα πρότυπα είναι το FIPS

186-2. Δηλαδή όποιο κρυπτοσύστημα είναι συμβατό με αυτό είναι συμβατό και με όλα τα υπόλοιπα. Οι σχέσεις συμβατότητας μεταξύ των συγκεκριμένων προτύπων είναι οι εξής:



Σχήμα 1. Σχέση Προτύπων Αλγορίθμων ECS

2.2.3 Άλλα είδη 'υπογραφών'.

Οι ψηφιακές υπογραφές δεν είναι η μόνη τεχνολογία η οποία μπορεί να χρησιμεύσει για αυθεντικοποίηση και υπογραφή. Ανάμεσα στις πιο συχνά χρησιμοποιούμενες είναι και οι παρακάτω:

- **Συνθηματικά:** Είναι η πιο παλιά ηλεκτρονική μέθοδος αυθεντικοποίησης. Βασίζεται σε κάποια γνώση που διαθέτει ο υπογράφων. Δεν θεωρούνται καθόλου ασφαλείς, για χρήση σε κρίσιμα περιβάλλοντα.
- **Ψηφιοποιημένες Υπογραφές:** Η χρήση σύγχρονων τεχνικών εργαλείων, όπως οι ψηφιοποιητές (digitizers), επιτρέπουν την δημιουργία συμβατικών υπογραφών σε ψηφιακά μέσα, τα οποία μπορούν να προσκολληθούν ως εικόνες σε ηλεκτρονικά έγγραφα. Η επαλήθευση μπορεί να γίνει με βάση το πόσο μία τέτοια ψηφιοποιημένη υπογραφή ταυτίζεται με ένα πρότυπο της που έχει αποθηκευθεί νωρίτερα.
- **Βιομετρική Τεχνολογία:** Είναι η πιο ενδιαφέρουσα εναλλακτική τεχνολογία για ηλεκτρονικές υπογραφές, καθώς θεωρητικά μπορεί να ταυτοποιήσει με σιγουριά τον υπογράφοντα. Είναι και η πιο παλιά μέθοδος αυθεντικοποίησης (για τους ανθρώπους). Πιο συγκεκριμένα η συγκεκριμένη τεχνολογία λειτουργεί ως εξής:
    - Γίνεται κάποια μέτρηση ενός βιολογικού χαρακτηριστικού του υπογράφοντα. Τέτοια χαρακτηριστικά είναι:
        - Η ίριδα.
        - Το δακτυλικό αποτύπωμα.
        - Το DNA.
        - Η χροιά της φωνής.
    - Η μέτρηση αυτή, ανάλογα με την υλοποίηση, αποθηκεύεται είτε σε μία κεντρική βάση δεδομένων είτε σε ένα αποσπώμενο (μαγνητικό) μέσο.
    - Κατά την αυθεντικοποίηση, μετράται η τιμή του χαρακτηριστικού αυτού και συγκρίνεται με την τιμή του αποθηκευμένου.

    Η επιτυχία μιας βιομετρικής μεθόδου έγκειται στο πόσο 'καλά' μπορεί να γίνει το ταίριασμα μεταξύ

των δύο χαρακτηριστικών. Για τον σκοπό αυτό χρησιμοποιούνται τεχνικές της αναγνώρισης προτύπων, οι οποίες όμως χαρακτηρίζονται από σημαντικό περιθώριο σφάλματος **[Polemi, 1997].**

Αν και οι βιομετρικές τεχνολογίες δεν συναρτούν την αυθεντικοποίηση με την κατοχή κάποιου αντικειμένου, που διατρέχει κινδύνους κλοπής ή απώλειας και βασίζονται σε κάτι που μοναδικά ταυτοποιεί κάθε ανθρώπινη οντότητα, θεωρούνται γενικά ως μη επαρκείς τεχνολογίες και θα πρέπει να υπάρχει προσοχή στην χρήση τους.

Σαν παράδειγμα θα αναφέρουμε την τεχνολογία δυναμικής επαλήθευσης υπογραφής (*Dynamic Signature Verification*), η οποία έχει λάβει πολύ μεγάλη δημοσιότητα τον τελευταίο καιρό. Η συγκεκριμένη τεχνολογία λειτουργεί ως εξής: Χρησιμοποιείται ένας ψηφιοποιητής σε συνδυασμό με μία συσκευή η οποία διαθέτει κατάλληλη οθόνη αφής. Ο χρήστης σχηματίζει την υπογραφή του με τον ίδιο τρόπο με τον οποίο θα την σχημάτιζε και συμβατικά. Παράλληλα η οθόνη αφής μετρά κάποια βιομετρικά χαρακτηριστικά, όπως για παράδειγμα η ταχύτητα γραφής, η πίεση του υπογράφοντα, ο αριθμός των διακριτών σημείων επαφής του ψηφιοποιητή με την οθόνη, η σειρά τους κ.ά. Με βάση τα συγκεκριμένα χαρακτηριστικά, δημιουργείται ένα πρότυπο το οποίο θεωρητικά χαρακτηρίζει μοναδικά τον υπογράφοντα, και με βάση το οποίο θα επαληθεύτεται κάθε υπογραφή του. Με τον τρόπο αυτό, αυθεντικοποιείται ο ίδιος ο χρήστης και όχι κάποια διεργασία λογισμικού, ή κάποιος υπολογιστής ή κάποιο τμήμα δεδομένων (κρυπτογραφικό κλειδί). Επίσης, η παραπάνω τεχνολογία έχει το σαφές πλεονέκτημα ότι ταυτίζεται σε αντίληψη για τον τελικό χρήστη, με την συμβατική διαδικασία υπογραφής. Το τελευταίο όμως δεν συνιστά και αποδοχή της από το κοινό, όπως θα δούμε αμέσως.

Μία τεχνολογία όπως η παραπάνω, αλλά και οι βιομετρικές τεχνολογίες γενικότερα, έχουν σημαντικά μειονεκτήματα σε δύο τομείς. Ο πρώτος είναι αυτός της ασφάλειας. Στο **[Schneier, 1999a]** αναφέρεται ότι μία βιομετρική τεχνική χρησιμοποιεί σε όλες τις συναλλαγές το ίδιο βιομετρικό χαρακτηριστικό, ανεξάρτητα από την κρισιμότητα της. Έτσι, η αναπαραγωγή με κάποιο τρόπο του συγκεκριμένου χαρακτηριστικού ή η κλοπή του αντίγραφου επαλήθευσης, θα εκθέσει όλες τις συναλλαγές μιας οντότητας. Ακόμα ένα βιομετρικό χαρακτηριστικό δεν διαθέτει τα χαρακτηριστικά ενός κρυπτογραφικού κλειδιού όπως η ανανέωση και η ανάκληση κάτι που προσθέτει δυσκολίες και σε διαχειριστικό επίπεδο. Έτσι *αν χαθεί ένα βιομετρικό κλειδί, χάνεται για πάντα*. Τέλος, δεν εγγυάται την ακεραιότητα του μηνύματος, κάτι που συμβαίνει με την κρυπτογραφία δημοσίου κλειδιού. Ο δεύτερος τομέας είναι αυτός της δυσκολίας πρακτικής εφαρμογής. Ένας παράγοντας που συντελεί σε αυτό, είναι η δυσκολία ακριβούς μέτρησης και ακριβούς σύγκρισης με το πρότυπο. Αυτό έχει δύο συνέπειες: την ευκολότερη πλαστογράφηση αλλά και το ακριβώς αντίθετο, την αποτυχία αυθεντικοποίησης του πραγματικού κάτοχου λόγω σφάλματος μέτρησης. Επιπλέον αντιμετωπίζουν συγκεκριμένα προβλήματα άρνησης αποδοχής από το ευρύ κοινό. Η άρνηση αυτή οφείλεται στο γεγονός, ότι αφενός η διαδικασία μέτρησης ενός τόσο προσωπικού χαρακτηριστικού, εκλαμβάνεται όχι και τόσο άδικα ως παραβίαση της ιδιωτικότητας. Επίσης, προσδίδει μία αίσθηση ύψιστης ασφάλειας η οποία δεν θεωρείται απαραίτητη, καθώς η κοινή πρακτική σε ανάλογες περιπτώσεις είναι η εισαγωγή ενός τετραψήφιου αριθμού. Επιπλέον,

ορισμένα από τα είδη αυθεντικοποίησης έχουν συνδυαστεί με τις διαδικασίες που ακολουθούνται κατά την διάπραξη αδικημάτων (έλεγχος αποτυπωμάτων και προσαγωγή), κάτι που περαιτέρω μειώνει την δυνατότητα αποδοχής. Τέλος, όπως αναφέρεται στο **[Aalberts, 1999]**, δεν είναι καθολικά αποδεκτό, ότι συγκεκριμένα βιομετρικά χαρακτηριστικά είναι μοναδικά.

Από όλες τις τεχνολογίες που αναφέραμε πιο σημαντική μπορούμε να θεωρήσουμε την κρυπτογραφία δημοσίου κλειδιού, καθώς παρέχει εκτός από αυθεντικοποίηση και ακεραιότητα. Η ως τώρα πρακτική εφαρμογή μας έχει δείξει ότι πιθανότερα δεν θα επικρατήσει καμία μεμονωμένη τεχνολογία, αλλά ένας συνδυασμός τους. Συγκεκριμένα η όλη υποδομή αυθεντικοποίησης θα βασίζεται σε κρυπτοσυστήματα δημοσίου κλειδιού. Το ιδιωτικό κλειδί θα βρίσκεται κρυπτογραφημένο και αποθηκευμένο σε μία κάρτα και η αποκρυπτογράφηση του θα βασίζεται στην παροχή του σωστού συνθηματικού ή σε κάποια βιομετρική μέτρηση.

2.2.3.1 Μη αποποιήσιμες υπογραφές

Στην βιβλιογραφία **[Schneier, 1996]**, αναφέρονται και άλλες πολύπλοκες κρυπτογραφικές τεχνικές οι οποίες έχουν σκοπό την βελτίωση ορισμένων χαρακτηριστικών των παραπάνω ειδών υπογραφής και ιδιαίτερα των ψηφιακών υπογραφών. Οι τεχνικές αυτές, λόγω της πολυπλοκότητας εφαρμογής τους και της δυσκολίας υλοποίησης τους, μάλλον δεν θα επικρατήσουν στην πράξη. Πιο ενδιαφέρον από αυτές, παρουσιάζουν οι λεγόμενες μη αποποιήσιμες ψηφιακές υπογραφές *(undeniable digital signatures)*. Σε αυτές η διαδικασία της υπογραφής παραμένει ίδια, διαφέρει όμως αυτή της επαλήθευσης, η οποία γίνεται με τέτοιο τρόπο ώστε να μην είναι εφικτή από τον καθένα και χωρίς την ενεργό συμμετοχή (συγκατάθεση) του υπογράφοντα. Η διαδικασία αυτή αναφέρεται στην ορολογία των μη αποποιήσιμων υπογραφών, ως επιβεβαίωση. Η συγκεκριμένη τεχνολογία παρέχει επίσης και την δυνατότητα της άρνησης. Είναι εφικτό δηλαδή με απολύτως τεχνικά μέσα, για τον υπογράφοντα να αρνηθεί μία συγκεκριμένη υπογραφή του. Το συγκεκριμένο είδος υπογραφών, προστατεύει τεχνικά τόσο τον υπογράφοντα όσο και τον επαληθεύοντα και παρέχει πραγματική μη αποποίηση. Ο επαληθεύων προστατεύεται καθώς η επαλήθευση θα γίνει με την συμμετοχή του υπογράφοντα, οπότε η άρνηση δεν έχει πρόβλημα, ενώ ο υπογράφων προστατεύεται καθώς ‘επιλέγει’ ποιοι θα μπορέσουν να επαληθεύσουν την υπογραφή του. Η συγκεκριμένη τεχνολογία, μπορεί να εφαρμοστεί με οποιοδήποτε είδος αλγορίθμου δημιουργίας ψηφιακών υπογραφών είδαμε νωρίτερα.

2.2.3.2 Πολλαπλές Υπογραφές

Πολλές καταστάσεις του πραγματικού κόσμου απαιτούν την προσάρτηση πολλών υπογραφών σε ένα ηλεκτρονικό κείμενο. Ένα παράδειγμα σε αυτό αποτελούν τα συμβόλαια, όπου τυπικά έχουμε τουλάχιστον δύο υπογραφές. Είναι φανερό ότι στις πολλαπλές υπογραφές εκτός από την ταυτότητα του υπογράφονται σημαντικό ρόλο παίζει και η σχέση του ως προς το κείμενο. Για παράδειγμα σε ένα συμβόλαιο αγοράς, μία οντότητα θα παίζει τον ρόλο του αγοραστή ενώ η άλλη του πωλητή. Η τεχνική απεικόνιση της

συγκεκριμένης διαδικασίας είναι δυνατή. Στο **[PESV, 2000]**, αναφέρονται τα παρακάτω είδη πολλαπλών υπογραφών:

- **Παράλληλες Υπογραφές (Independent / Parallel):** Οι παράλληλες υπογραφές εφαρμόζονται στο κείμενο ανεξάρτητα η μία από την άλλη. Είναι ισοδύναμες, δηλαδή με την υπογραφή του αρχικού κειμένου από ένα σύνολο από ανεξάρτητες οντότητες. Δεν έχει σημασία δηλαδή η σειρά της υπογραφής.
- **Εμφωλιασμένες Υπογραφές (Embedded / Wrapping Signatures):** Πρόκειται για ηλεκτρονικές υπογραφές οι οποίες έχουν εφαρμοστεί διαδοχικά σε κάποιο κείμενο. Με άλλα λόγια, η αρχική υπογραφή εφαρμόζεται στο κείμενο – και ονομάζεται εσωτερική ή embedded – ενώ οι υπόλοιπες (εξωτερικές ή wrapping) εφαρμόζονται στην εσωτερική. Είναι φανερό εδώ ότι η σειρά υπογραφής έχει πολύ μεγάλη σημασία στην επαλήθευση, καθώς για να είναι σωστή η επαλήθευση πρέπει να ακολουθηθεί αντίστροφη σειρά από αυτήν της υπογραφής.
- **Συνολικές Υπογραφές (Overall Signatures):** Εδώ ακολουθείται μία παρόμοια διαδικασία με τις εμφωλιασμένες υπογραφές, με την διαφορά ότι κάθε εξωτερική υπογραφή, λαμβάνει ως είσοδο τόσο το κείμενο, όσο και την προηγούμενη υπογραφή. Οι συγκεκριμένες υπογραφές χρησιμοποιούνται τόσο για επιπλέον ασφάλεια, όσο και για αρχειοθέτηση.

Οι παραπάνω έννοιες γίνονται καλύτερα κατανοητές με τον παρακάτω συμβολισμό από το **[PESV, 2000]**:

⇒ **M:** Το κείμενο το οποίο θα υπογραφεί.

⇒ **A:** Το σύνολο των ιδιοτήτων που αφορά κάθε υπογράφοντα.

⇒ **S:** Η ηλεκτρονική υπογραφή, δηλαδή το αποτέλεσμα του αλγόριθμου κρυπτογράφησης, πάνω στην σύνοψη του M και του A. Πιο απλά: *S = sig(M, A)*.

Με βάση τα παραπάνω λοιπόν και αν S1 = sig(M, A1) τα διαφορετικά είδη πολλαπλών υπογραφών μπορούν να εκφραστούν ως:

⇒ Παράλληλη υπογραφή: S2 = sig(M, A2).

⇒ Εμφωλιασμένη υπογραφή: S3 = sig(S1, A3)

⇒ Συνολική Υπογραφή: S4 = sig(X, A4), όπου το X είναι το (M, S1).

2.2.4 Ηλεκτρονικές Υπογραφές

Όπως είδαμε, οι ψηφιακές υπογραφές, είναι σήμερα, η πλέον υποσχόμενη τεχνολογία που μπορεί να χρησιμοποιηθεί για την αυθεντικοποίηση δύο χρηστών σε ένα ηλεκτρονικό περιβάλλον. Βέβαια δεν αποκλείεται η εμφάνιση κάποιας νέας τεχνολογίας ή ένας νέος συνδυασμός από τις παραπάνω τεχνολογίες, η οποία θα καταστεί μία καλύτερη λύση από τις υπογραφές οι βασίζονται αποκλειστικά σε κρυπτοσυστήματα δημοσίου κλειδιού. Για τον λόγο αυτό πολλές από τις νομικές και ρυθμιστικές προσπάθειες, τις οποίες θα αναλύσουμε και αργότερα, υιοθετούν τον πιο γενικό όρο ηλεκτρονική υπογραφή, στοχεύοντας στην τεχνολογική ουδετερότητα, δηλαδή σε μεθόδους δημιουργίας υπογραφών οι

οποίες δεν θα σχετίζονται με κάποια συγκεκριμένη τεχνολογία.

Έτσι, οι ηλεκτρονικές υπογραφές ορίζονται στα περισσότερα τέτοια κείμενα, *ως ηλεκτρονικά δεδομένα ή σύμβολα τα οποία έχουν κάποια συσχέτιση με ένα ηλεκτρονικό κείμενο*, ώστε να προσομοιάζεται η σχέση που έχουν οι ιδιόχειρες υπογραφές με τα κείμενα τα οποία συνοδεύουν. Η προσέγγιση αυτή αν και είναι έχει υιοθετηθεί στην πλειοψηφία των κανονιστικών προσπαθειών με το επιχείρημα της τεχνολογικής ουδετερότητας, έχει αμβισβητηθεί από πολλούς, καθώς όπως υποστηρίζεται υπάρχει δυνατότητα ένα σύστημα το οποίο δεν έχει την πρακτική εφαρμογή της υποδομής δημοσίου κλειδιού, αλλά ικανοποιεί τις τυπικές νομικές προϋποθέσεις να χρησιμοποιηθεί σε μεγάλη κλίμακα, εισάγοντας έτσι κινδύνους ασφαλείας. Ένα παράδειγμα σε αυτό μπορεί να αποτέλεσει η βιομετρική τεχνολογία δυναμικής επαλήθευσης μιας ηλεκτρονικής υπογραφής. Μία επίσκεψη στον διαδικτυακό κόμβο μιας εταιρείας τέτοιων προϊόντων μπορεί να πείσει τον τελικό χρήστη, που πιθανότατα δεν θα έχει σημαντικές τεχνικές γνώσεις για την αξιοπιστία της συγκεκριμένη μεθόδου, κάτι που όπως είδαμε αμφισβητείται έντονα. Τα επιχειρήματα υπέρ ή κατά της τεχνολογικής ουδετερότητας θα αναλυθούν σε επόμενο κεφάλαιο.

2.3 Ψηφιακά Πιστοποιητικά.

Στην συζήτηση που κάναμε νωρίτερα, για τις ψηφιακές υπογραφές, επίτηδες παραλείψαμε ορισμένες λεπτομέρειες, οι οποίες όμως έχουν πολύ σημαντικές συνέπειες. Πρώτα από όλα, δεν αναφέραμε το πώς ο επαληθεύων αποκτά το δημόσιο κλειδί του υπογράφοντα. Μία λύση είναι να συνοδεύει το μήνυμα, κάτι που θεωρητικά δεν επηρεάζει την ασφάλεια του μηνύματος, αφού έτσι κι αλλιώς το δημόσιο κλειδί είναι προσβάσιμο σε όλους.

Η παραπάνω λύση είναι ευάλωτη στην κρυπτογραφική *επίθεση του ενδιαμέσου* **[Schneier, 1996].** Συγκεκριμένα, κάποιος ενεργός παρεμβολέας μπορεί να εισέρθει μεταξύ των δύο οντοτήτων, να αφαιρέσει την ψηφιακή υπογραφή από το κείμενο, και να υπολογίζει εκ νέου την δική του ψηφιακή υπογραφή, όπως περιγράψαμε. Αν αλλάξει και το δημόσιο κλειδί του υπογράφοντα με το δικό του, τότε ο επαληθεύων δεν θα καταλάβει τη διαφορά.

Στο συγκεκριμένο πρόβλημα έχουν προταθεί αρκετές λύσεις. Η πιο εφαρμόσιμη από αυτές θέλει την ανάκτηση του δημοσίου κλειδιού του υπογράφοντα από μία τρίτη οντότητα στην οποία και οι δύο συμμετέχοντες έχουν εμπιστοσύνη. Η τρίτη αυτή οντότητα εγγυάται – πιστοποιεί ότι το δημόσιο κλειδί με το οποίο γίνεται η επαλήθευση της υπογραφής είναι αυτό που αντιστοιχεί στο ιδιωτικό κλειδί του χρήστη. Οι οντότητες αυτές αναφέρονται στην βιβλιογραφία, ως *αρχές πιστοποίησης (Certification Authorities – CAs)* ή *έμπιστες τρίτες οντότητες (Trusted Third Parties – TTPs)*. Παρ΄όλο που πολλές φορές οι παραπάνω έννοιες χρησιμοποιούνται ως ταυτόσημες, στην πραγματικότητα διαφέρουν. Επειδή στον τομέα της ορολογίας, επικρατεί μία σύγχυση, παρακάτω θα προσπαθήσουμε να θέσουμε μία κοινή βάση την οποία θα ακολουθήσουμε σε όλη την διάρκεια της εργασίας. Η βάση αυτή βασίζεται στην προσωπική μας αντίληψη και δεν συμφωνεί κατ' ανάγκη με την σημασία που αποδίδεται συνήθως στους παραπάνω όρους.

Η έννοια της έμπιστης τρίτης οντότητας είναι η πιο γενική, καθώς παρέχει επιπλέον υπηρεσίες από την εγγύηση της αντιστοιχίας οντότητας με δημόσιο κλειδί, που τυπικά υλοποιεί μία αρχή πιστοποίησης. Οι έμπιστες τρίτες οντότητες είναι ένας όρος που αφορά οποιαδήποτε οντότητα, η οποία δεν έχει άμεσο συμφέρον σε μία ηλεκτρονική συναλλαγή και η οποία παρέχει υπηρεσίες στις οντότητες που συμμετέχουν, κυρίως σε ότι αφορά την επίλυση διαφορών. Επίσης στην οδηγία της Ευρωπαϊκής Επιτροπής **[EDCF, 1999]**, πρωτοχρησιμοποιήθηκε ο όρος *πάροχος υπηρεσιών πιστοποίησης (Certification Service Provider - CSP)*, ο οποίος χρησιμοποιείται σε όλα τα κείμενα της προτυποποίησης που σχετίζονται με την Ευρώπη. Επειδή ορίζεται ως οποιαδήποτε οντότητα προσφέρει υπηρεσίες σχετικές με ηλεκτρονικές υπογραφές και όχι μόνο με την πιστοποίηση, η σημασία του συγκεκριμένου όρου τον φέρνει πιο κοντά στην έννοια της έμπιστης τρίτης οντότητας, χωρίς όμως να υπάρχει ταύτιση, καθώς όπως είπαμε οι έμπιστες τρίτες οντότητες δεν σχετίζονται κατ' ανάγκη με τις ηλεκτρονικές υπογραφές.

Μετά την παρένθεση σχετικά με την ορολογία, επανερχόμαστε στο πρόβλημα της πιστοποίησης. Η πιστοποίηση της αντιστοιχίας του δημοσίου κλειδιού με κάποιον χρήστη, γίνεται με την έκδοση ψηφιακών πιστοποιητικών. Η ιδέα του ψηφιακού πιστοποιητικού αποδίδεται στον *Kohnfelder*, και στην διπλωματική του εργασία στο MIT, το 1978. Στην γενική τους μορφή τα πιστοποιητικά αυτά, πρέπει τουλάχιστον να προσδιορίζουν τον υπογράφοντα και βέβαια να παραθέτουν το δημόσιο κλειδί του. Το όλο πιστοποιητικό πρέπει οπωσδήποτε να υπογράφεται ψηφιακά από την αρχή πιστοποίησης, κάτι που θα εξασφαλίσει αφενός την ακεραιότητα του πιστοποιητικού, ότι δηλαδή κάποιος δεν θα μπορέσει να τροποποιήσει τα περιεχόμενα του και αφετέρου θα λειτουργήσει ως εγγύηση της αρχής πιστοποίησης για την πραγματική ταυτότητα του υπογράφοντα. Το πώς η αρχή πιστοποίησης διαπιστώνει την ταυτότητα του, δεν έχει μόνο τεχνικές πτυχές.

Στην πράξη τα ψηφιακά πιστοποιητικά, έχουν αρκετά πολύπλοκη δομή. Είναι προφανές ότι για την χρήση τους από όσο το δυνατόν περισσότερες εφαρμογές, είναι απαραίτητη η προτυποποίηση των περιεχομένων τους. Η βασική προτυποποίηση στον τομέα αυτόν προέρχεται από τον ISO, ο οποίος έχει δημοσιεύσει το βασικό πρότυπο για ψηφιακά πιστοποιητικά, το *X.509*. Αξίζει εδώ να σημειώσουμε ότι το συγκεκριμένο πρότυπο στην αρχική του μορφή δεν προοριζόνταν για την χρήση που προαναφέραμε. Αποτελούσε τμήμα του προτύπου X.500 του για την πρόσβαση σε κατανεμημένες υπηρεσίες ενός παγκόσμιου καταλόγου, του οποίου την λειτουργία θα είχαν οι μεγαλύτεροι τηλεπικοινωνιακοί οργανισμοί. Η αυθεντικοποίηση των οντοτήτων για την πρόσβαση στον συγκεκριμένο κατάλογο βασίζονταν σε ασύμμετρα κρυπτοσυστήματα. Τα πιστοποιητικά X.509 συσχέτιζαν ένα δημόσιο κλειδί σε μία οντότητα του καταλόγου. Με βάση την παραπάνω συσχέτιση γινόταν ο έλεγχος πρόσβασης. Στα ψηφιακά πιστοποιητικά υπάρχει επίσης προτυποποίηση από την πλευρά οργανισμών όπως η IETF {**[RFC2459, 1999], [RFC3039, 2001]**} και η RSA. Επειδή το κυρίαρχο πρότυπο είναι το X.509 και όλα τα υπόλοιπα βασίζονται σε αυτό θα το αναλύσουμε διεξοδικά. Εκ των προτέρων αναφέρουμε ότι η συγκεκριμένη συζήτηση για τα τεχνικά πρότυπα, έχει και νομικές συνέπειες, καθώς οι τιμές σε ορισμένα πεδία, μπορεί να αλλάξουν την αντιμετώπιση του πιστοποιητικού από ορισμένα πλαίσια.

Το X.509, λοιπόν, πρωτοδημοσιεύτηκε το 1988 και βρίσκεται σήμερα στην τρίτη έκδοση του. Η

βασική μορφή του πιστοποιητικού περιγράφεται στην έκδοση 1 (1988) και αποτελείται από τα εξής πεδία:

- *Αριθμός Έκδοσης*: Είναι ένας ακέραιος αριθμός ο οποίος υποδεικνύει, όπως είναι φανερό, σε ποια από τις εκδόσεις ανήκει ένα πιστοποιητικό.
- *Αριθμός Σειράς*: Ένας μοναδικός αριθμός για τον απόλυτο προσδιορισμό του πιστοποιητικού.
- *Αλγόριθμος Ψηφιακής Υπογραφής*: Στο πεδίο αυτό υπάρχει μία συμβολοσειρά η οποία προσδιορίζει μοναδικά τον αλγόριθμο με τον οποίο η αρχή πιστοποίησης έχει υπογράψει ψηφιακά το συγκεκριμένο πιστοποιητικό. Η συμβολοσειρά αυτή ακολουθεί την σύνταξη του αναγνωριστή τύπων της ASN.1. Η ASN.1 είναι μία γλώσσα ορισμού τύπων δεδομένων και των τιμών τους. Η βασική χρήση της είναι στα πρωτόκολλα δικτύων υπολογιστών, όπου χρησιμοποιείται κυρίως για τον ορισμό των μονάδων δεδομένων (PDUs – Protocol Data Units) που χρησιμοποιούν τα διάφορα πρωτόκολλα για την επικοινωνία των εφαρμογών. Στόχος της είναι η αναπαράσταση των δεδομένων με ομοιόμορφο τρόπο, έτσι ώστε να είναι κατανοητά από όλα τα συστήματα. Ένα παράδειγμα πρωτοκόλλου που χρησιμοποιεί ASN.1 είναι το SNMP (Simple Network Management Protocol). Σε κάθε τύπο που ορίζουμε με την βοήθεια της ASN.1, μπορούμε να αναθέσουμε ένα μοναδικό αναγνωριστή (object identifier) έτσι ώστε να μπορεί να ταυτοποιηθεί μονοσήμαντα. Η μοναδικότητα τους βασίζεται σε ένα ιεραρχικό σχήμα, καθώς κάθε αναγνωριστής ASN.1 είναι μία ακολουθία από ακέραιους ξεκινώντας από την ρίζα του δένδρου και καταλήγοντας στα φύλλα. Οι αναγνωριστές που ξεκινούν από 0 ανατίθενται από την ITU, αυτοί που ξεκινούν από 1 από τον ISO, ενώ αυτοί που ξεκινούν από 2 ανατίθενται κοινά από την ITU και τον ISO. Με την χρήση των αναγνωριστών καθίσταται δυνατή η χρήση των τύπων που ορίζουμε με την ASN.1 από τα διάφορα προγράμματα. Αρκεί βέβαια οι ανταλλασσόμενες τιμές να συνοδεύονται από τον αναγνωριστή του τύπου. Στο σημείο αυτό πρέπει να επισημάνουμε ότι ο όρος τύπος εδώ χρησιμοποιείται με την ευρεία έννοια του, δεν αναφερόμαστε δίπλα στενά στους τύπους που χρησιμοποιούνται στις γλώσσες προγραμματισμού. Ένας τύπος μπορεί να παριστάνει ένα αλγόριθμο ψηφιακής υπογραφής. Για παράδειγμα ο αναγνωριστής του αλγορίθμου RSA με συνάρτηση σύνοψης την SHA-1 είναι: {1-2-840-113549-1-1-5}.
- *Εκδούσα αρχή*: Εδώ υπάρχει το όνομα κατά το πρότυπο X.500 το οποίο αντιστοιχεί στην αρχή πιστοποίησης που έχει εκδώσει το συγκεκριμένο πιστοποιητικό. Το πρότυπο X.500 της ITU ανήκει στην ίδια οικογένεια προτύπων με το πρότυπο X.509. Ορίζει ένα σύνολο κανόνων ονοματοδοσίας για οντότητες οι οποίες καταχωρούνται σε έναν κατάλογο. Το όνομα κάθε καταχώρησης του καταλόγου, το οποίο αναφέρεται στο πρότυπο ως **Distinguished Name - DN**, προκύπτει μοναδικά και εδώ από μία ιεραρχική δομή **(Directory Information Tree – DIT)** και πιο από την συνένωση των ονομάτων που υπάρχουν σε κάθε επίπεδο του δέντρου και αναφέρονται στο πρότυπο ως **Relative Distinguished Name - RDN**. Κάθε σχετικό όνομα RDN είναι ουσιαστικά ένα ζεύγος της μορφής *{ιδιότητα = τιμή}*, όπου η ιδιότητα είναι ένα μοναδικό χαρακτηριστικό. Ένα παράδειγμα ονόματος κατά X.500, μπορεί να βρεθεί στο πιστοποιητικό της Γενικής Γραμματείας Πληροφοριακών Συστημάτων:

E = gsis-ca@gsis.gov.gr
CN = www.gsis.gov.gr
OU = GSIS-Ministry of Finance
O = General Secretariat for Information Systems
L = Athens
S = Attiki
C = GR

Σχήμα 2. Όνομα X.500

Η ονοματοδοσία τόσο της εκδούσας αρχής όσο και του υποκειμένου, έχει πολύ μεγάλη σημασία, καθώς καθορίζει εν μέρει το περιβάλλον στο οποίο κάθε όνομα είναι μοναδικό, κάτι που έχει άμεση συνέπεια στην αυθεντικοποίηση. Η ιεραρχική φύση του προτύπου θεωρητικά θα εγγυόταν την μοναδικότητα των ονομάτων. Το πρόβλημα όμως που προέκυψε ήταν το αντίθετο, δηλαδή κάθε οντότητα διέθετε πολλαπλά ονόματα καθώς δεν υπήρξε ξεκάθαρη ερμηνεία των RDN. Η βαθύτερη αιτία ήταν ότι η διαχείριση ενός ιεραρχικού συστήματος ονοματοδοσίας σε ένα κατανεμημένο και μη αυστηρά ορισμένο περιβάλλον αποδείχθηκε αδύνατη καθώς δεν μπορούν να διαχειριστούν την περίπτωση που πολλές διαφορετικές οντότητες έχουν τα ίδια RDN (πχ. όλοι οι λογιστές μιας εταιρείας). Δεν είναι τυχαίο άλλωστε ότι τέτοια σχήματα έχουν 'επιτυχία' μόνο σε οργανισμούς όπως ο στρατός.

- *Περίοδος Ισχύος* : Στο συγκεκριμένο πεδίο υπάρχουν δύο ημερομηνίες οι οποίες περιβάλλουν την περίοδο ισχύος του πιστοποιητικού – οι ημερομηνίες έναρξης και λήξης.

- *Υποκείμενο*: Το όνομα κατά X.500 για την οντότητα της οποίας τα στοιχεία πιστοποιείται ότι αντιστοιχούν στο συγκεκριμένο δημόσιο κλειδί.

- *Δημόσιο κλειδί οντότητας*: Στο συγκεκριμένο πεδίο υπάρχουν τα bytes του δημοσίου κλειδιού καθώς επίσης πληροφορίες για τον αλγόριθμο με τον οποίο θα χρησιμοποιηθεί το δημόσιο κλειδί αυτό. Ο αλγόριθμος προσδιορίζεται μονοσήμαντα με την χρήση του αναγνωριστή τύπων της ASN.1

Η έκδοση 2 του X.509 (1993) δεν πρόσθεσε σημαντικά στοιχεία στο πρότυπο. Ουσιαστικά πρόσθεσε δύο πεδία μόνο τα οποία περιέχουν αναγνωριστές ASN.1 για τα ονόματα της εκδούσας αρχής και του υποκειμένου. Αυτό συνέβη για την επίλυση των περιπτώσων που δύο οντότητες είχαν πολλά ονόματα X.500.

Οι μεγάλες αλλαγές στο πρότυπο X.509 ήρθαν με την έκδοση 3 (1998), η οποία πρόσθεσε το πεδίο επεκτάσεις (*extensions*) στο πιστοποιητικό.Η συγκεκριμένη προσθήκη είναι τεράστιας σημασίας καθώς το συγκεκριμένο πεδίο δεν συνιστά έναν απλό νέο τύπο δεδομένων, αλλά αντιπροσωπεύει έναν ολόκληρο μηχανισμό δημιουργίας κατά παραγγελίας, θα έλεγε κανείς, πιστοποιητικών τα οποία όμως είναι το ίδιο εύκολα χρησιμοποιήσιμα και έγκυρα. Για τον λόγο αυτό τα πιστοποιητικά με επεκτάσεις έχουν προτυποποιηθεί και από διαφορετικούς οργανισμούς εκτός του ISO. Τα σχετικά πρότυπα είναι το **[PKCS #6, 1993]** και το **[RFC 2459, 1999]**. Τα βασικά στοιχεία καλύπτονται από την προτυποποίηση του ISO, στην οποία και θα αναφερθούμε στην συνέχεια.

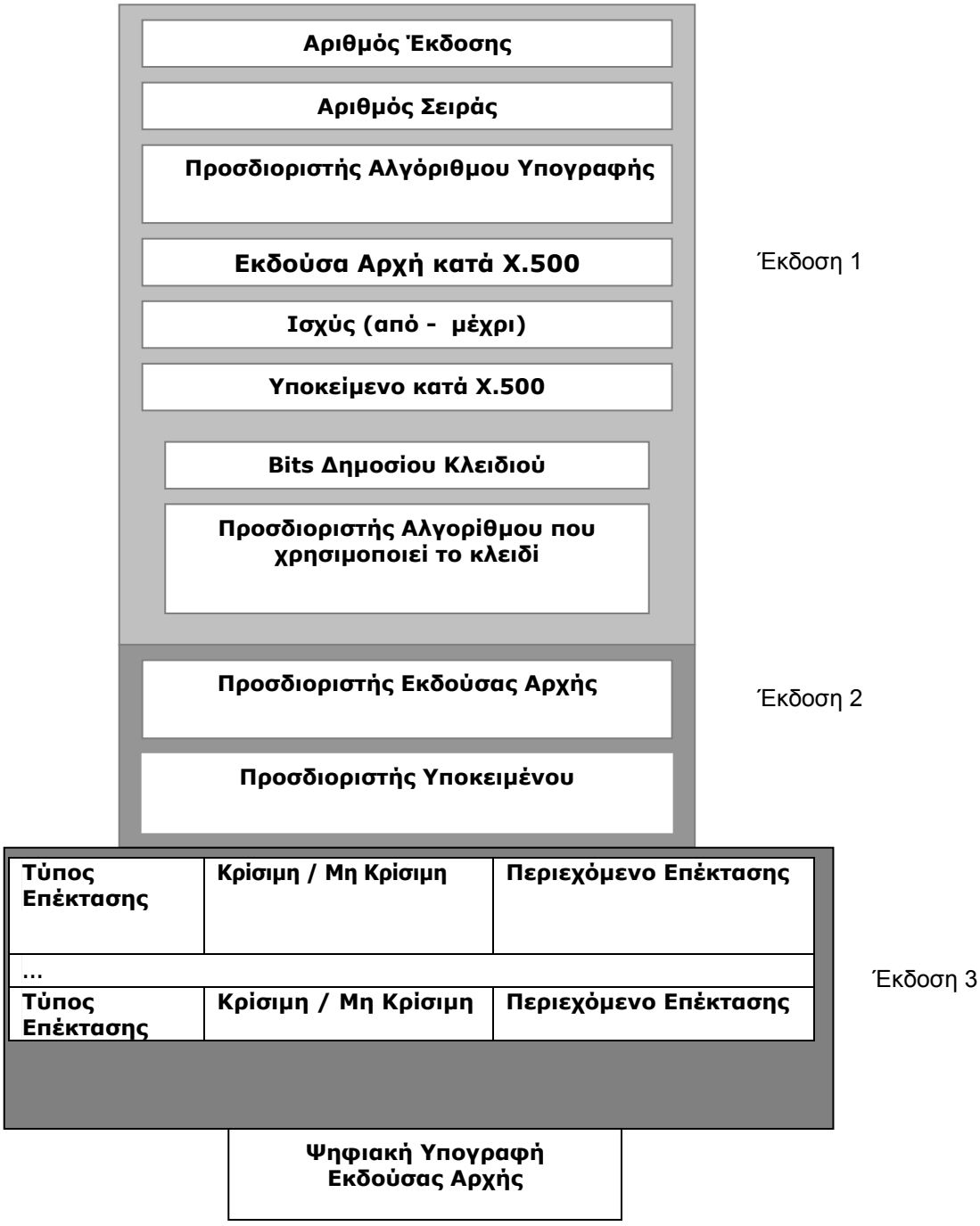
Η έκδοση 3 αυτή του πιστοποιητικού ονομάζεται και εκτεταμένη (extended) λόγω ακριβώς αυτού του μηχανισμού, ο οποίος έρχεται να αντιμετωπίσει κάποιες ανεπάρκειες στις μορφές 1, 2 που έγιναν εμφανείς όταν στην περίοδο του 1993, 1994 επιχειρήθηκε η χρήση σε ευρεία κλίμακα των πιστοποιητικών X.509. Η πιο σημαντική από αυτές είναι ότι κάθε πιστοποιητικό *εκδίδεται από διαφορετική αρχή πιστοποίησης, με διαφορετικους κανόνες έκδοσης και πιθανότατα για διαφορετική χρήση*. Όλοι οι χρήστες ενός πιστοποιητικού πρέπει να είναι ενήμεροι για όλες τις παραπάνω παραμέτρους, καθώς αυτές επηρεάζουν σίγουρα την εμπιστοσύνη που επιδεικνύουν στο πιστοποιητικό. Η πληροφορία αυτή δεν είναι δυνατό να αποκτηθεί μόνο από ένα πιστοποιητικό X.509 έκδοσης 2. Υπάρχουν και άλλα μειονεκτήματα στην αρχική έκδοση, όπως για παράδειγμα το ότι όλα τα ονόματα σε αυτά αναφέρονται κατά το πρότυπο X.500, κάτι που τα κάνει δύσχρηστα, επιπλέον των άλλων προβλημάτων, καθώς οι εφαρμογές πρέπει να εμφανίζουν εύκολα κατανοητά ονόματα. Αντίθετα στην τρίτη έκδοση των πιστοποιητικών, μέσω των επεκτάσεων μπορεί να υπάρξει μία ποικιλία ονομάτων, για το υποκείμενο του πιστοποιητικού. Τα ονόματα αυτά μπορεί να είναι:

- Διεύθυνση Ηλεκτρονικού Ταχυδρομείου (pangron@aueb.gr)
- Διεύθυνση Domain Name (www.aueb.gr)
- Uniform Resource Identifier (URI).
- Διεύθυνση IP.
- Οποιοδήποτε όνομα είναι μοναδικό στο περιβάλλον του.

Το πιστοποιητικό X.509 στην τρίτη έκδοση του, λοιπόν έχει ακριβώς τα ίδια υποχρεωτικά πεδία όπως και στη δεύτερη έκδοση. Προαιρετικά όμως μπορεί να υπάρχει ένα πεδίο επεκτάσεων (extensions). Στο συγκεκριμένο πεδίο μπορεί να μπει απεριόριστος αριθμός εγγραφών. Κάθε εγγραφή (επέκταση) είναι μία δομή που απαρτίζεται από τρία πεδία:

- **Τύπος**: Στο συγκεκριμένο πεδίο δηλώνεται το είδος της επέκτασης, το οποίο προσδιορίζεται από έναν αναγνωριστή, με τρόπο ανάλογο με τα πεδία αλγόριθμος, εκδούσα αρχή και όνομα υποκειμένου. Γίνεται εύκολα κατανοητό ότι για να υπάρξει συμβατότητα, δεν μπορεί ο καθένας να ορίζει μια επέκταση, αλλά πρέπει να υπάρχουν κάποιες κοινά αποδεκτές επεκτάσεις τις οποίες θα καταλαβαίνουν οι εφαρμογές.
- **Ένδειξη Κρισιμότητας**: Στο συγκεκριμένο πεδίο υπάρχουν αποκλειστικά οι τιμές *κρίσιμο* ή *όχι κρίσιμο*. Μία επέκταση που έχει χαρακτηριστεί ως μη κρίσιμη μπορεί να αγνοηθεί από μία εφαρμογή που δεν την 'καταλαβαίνει'. Σε αντίθετη περίπτωση, δηλαδή αν μία άγνωστη επέκταση είναι κρίσιμη, τότε η εφαρμογή δεν πρέπει να αποδεχθεί το πιστοποιητικό. Ίσως ένας καλύτερος όρος για το συγκεκριμένο πεδίο θα ήταν υποχρεωτική αποδοχή για ένα έγκυρο πιστοποιητικό. Οι περισσότερες επεκτάσεις είναι μη κρίσιμες, καθώς έτσι καθίσταται δυνατή η προσθήκη νέων τύπων πιστοποιητικών. Αντίθετα οι κρίσιμες επεκτάσεις αφορούν σημαντικά θέματα ασφαλείας.
- **Τιμή**: Στο πεδίο αυτό περιέχεται η τιμή της συγκεκριμένης επέκτασης, η οποία βέβαια πάντα ερμηνεύεται με βάση τον τύπο.

Έτσι η πλήρης μορφή ενός πιστοποιητικού X.509 έχει ως εξής:



Σχήμα 3. Μορφή Πιστοποιητικού X.509

Όπως είναι λογικό ο μηχανισμός των επεκτάσεων θα ήταν άχρηστος αν δεν υπήρχε κάποια προτυποποίηση στους τύπους τους. Σε αυτήν την διαδικασία έχουν εμπλακεί οι οργανισμοί ISO, ITU, ANSI με παρόμοιες περίπου πρότυπες επεκτάσεις. Οι προτυποποιημένες επεκτάσεις μπορούν να χωριστούν στις εξής κατηγορίες **[RFC 2459, 1999]**:

- Επεκτάσεις που αφορούν τα κλειδιά του υποκειμένου και της αρχής πιστοποίησης. Στόχος τους είναι να παρέχουν περισσότερη πληροφορία σχετικά με την επιτρεπτή χρήση τους. Για παράδειγμα μία προτυποποιημένη επέκταση αφορά την χρήση του κλειδιού που συνοδεύει το πιστοποιητικό.

Προδιαγράφονται οι εξής χρήσεις οι οποίες είναι και όλες οι δυνατές χρήσεις ενός πιστοποιητικού και μπορούν να χρησιμοποιηθούν για την ανάκτηση του κατάλληλου πιστοποιητικού σε περίπτωση που μία οντότητα διαθέτει πολλά.

- Ψηφιακή Υπογραφή.
- Μη Αποποίηση (non - Repudiation).
- Κρυπτογράφηση Κλειδιού.
- Κρυπτογράφηση Δεδομένων.
- Χρήση σε πρωτόκολλο συμφωνίας κλειδιού.
- Ψηφιακή Υπογραφή Πιστοποιητικού.
- Ψηφιακή Υπογραφή Λίστας Ανάκλησης.
- Μόνο Κρυπτογράφηση.
- Μόνο Αποκρυπτογράφηση.

Η ύπαρξη τους έχει δημιουργήσει αρκετές αμφιβολίες. Για παράδειγμα, δεν είναι ξεκάθαρη η διαφορά χρήσης για ψηφιακή υπογραφή από την χρήση για μη αποποίηση. Τυπικά οι περισσότερες υλοποιήσεις χρησιμοποιούν την χρήση *ψηφιακή υπογραφή* για αυθεντικοποίηση οντοτήτων ή δεδομένων, η οποία υλοποιείται με την 'υπογραφή' και επαλήθευση ενός δείγματος δεδομένων (token) το οποίο όμως μετα καταστρέφεται και την χρήση *μη αποποίηση* για την αναπαράσταση της συμβατικής υπογραφής που αφορά ηλεκτρονικά δεδομένα με μεγάλη διάρκεια.

- Επεκτάσεις που αφορούν την πολιτική έκδοσης της αρχής πιστοποίησης για το συγκεκριμένο πιστοποιητικό. Οι τιμές τους μπορεί να δείχνουν δεδηλωμένες πολιτικές πιστοποίησης ή κάποια αντιστοιχία μεταξύ των πολιτικών πιστοποίησης διαφορετικών αρχών. Η έννοια της πολιτικής πιστοποίησης θα αναλυθεί σε επόμενο κεφάλαιο.
- Επεκτάσεις που αφορούν εναλλακτικά ονόματα για την αρχή πιστοποίησης και το υποκείμενο.

Ο μηχανισμός των επεκτάσεων έχει άμεση σχέση με την ευρωπαϊκή οδηγία για τις ηλεκτρονικές υπογραφές. Πράγματι στο παράρτημα 1 της οδηγίας αυτής, αναφέρονται κάποιες ιδιότητες που πρέπει να έχει κάποιο πιστοποιητικό ώστε να θεωρείται αναγνωρισμένο (qualified). Ως αποτέλεσμα η ομάδα PKIX της IETF, εξέδωσε πολύ πρόσφατα το **[RFC 3039, 2001]**, το οποίο περιγράφει τις προδιαγραφές που πρέπει να διαθέτει ένα πιστοποιητικό ώστε να θεωρείται αναγνωρισμένο. Οι προδιαγραφές αυτές συνιστούν ένα προφίλ πιστοποιητικού, κατά την ορολογία του PKIX. Το συγκεκριμένο προφίλ δεν έχει ως αποκλειστικό στόχο την ταύτιση με την οδηγία, αλλά έχει ως στόχο την παροχή μίας περιγραφής για ένα πιστοποιητικό προηγμένου τύπου το οποίο θα χρησιμοποιείται για την αυθεντικοποίηση φυσικών προσώπων με ικανοποιητικό ποσοστό βεβαιότητας σε συναλλαγές κυρίως με δημόσιες υπηρεσίες, οι οποίες θα έχουν την ιδιότητα της μη αποποίησης.

Για να είναι λοιπόν ένα πιστοποιητικό αναγνωρισμένο, *σύμφωνα με το RFC 3039*, πρέπει να ικανοποιεί τις παρακάτω ιδιότητες:

- Πρέπει να εκδίδεται από μία αρχή πιστοποίησης, η οποία θα δηλώνει δημόσια ότι το συγκεκριμένο πιστοποιητικό είναι αναγνωρισμένο. Η πληροφορία αυτή μπορεί να είναι προσβάσιμη από το ίδιο το πιστοποιητικό, είτε στην επέκταση όπου προσδιορίζεται η πολιτική πιστοποίησης της οποία θα είναι μέρος, είτε σε ειδική επέκταση όπου θα αναφέρονται δηλώσεις που συνοδεύουν το πιστοποιητικό.
- Πρέπει να εκδίδεται υπό μία πολιτική έκδοσης πιστοποιητικών αρχής πιστοποίησης.
- Πρέπει να εκδίδεται σε φυσικό πρόσωπο.
- Πρέπει να ταυτοποιεί μοναδικά το υποκείμενο φυσικό πρόσωπο με βάση κάποιο όνομα.

Σε πιο τεχνικό επίπεδο το συγκεκριμένο πρότυπο παρέχει οδηγίες για τις αποδεκτές τιμές των πεδίων εκδούσα αρχή και υποκείμενο του βασικού πιστοποιητικού. Επίσης ορίζει καινούριες επεκτάσεις και θέτει απαιτήσεις για τις ήδη υπάρχουσες:

- *Ιδιότητες Καταλόγου*. Στην συγκεκριμένη επέκταση ορίζονται κάποιες ιδιότητες οι οποίες μπορούν να παρέχουν περισσότερες πληροφορίες για το υποκείμενο. Η ύπαρξη της είναι προαιρετική.
- *Πολιτικές Πιστοποίησης*. Η συγκεκριμένη επέκταση, η οποία θα είναι υποχρεωτικά παρούσα σε ένα αναγνωρισμένο πιστοποιητικό, θα περιέχει έναν ASN.1 αναγνωριστή, ο οποίος θα προσδιορίζει την πολιτική έκδοσης πιστοποιητικού. Η έννοια της πολιτικής πιστοποίησης θα περιγραφεί αναλυτικά στην επόμενη ενότητα.
- *Χρήση Κλειδιού*. Και αυτή η επέκταση η οποία ορίστηκε στο **[RFC 2459, 1999]** είναι υποχρεωτικά παρούσα και καθορίζει την χρήση του κλειδιού η συσχέτιση του οποίου πιστοποιείται. Αναφέρει δηλαδή ότι αν τεθεί ως χρήση η μη αποποίηση τότε δεν πρέπει να συνοδεύεται από καμία άλλη χρήση.
- *Βιομετρική Πληροφορία*. Η προαιρετική αυτή επέκταση περιέχει την σύνοψη μίας βιομετρικής πληροφορίας ή έναν δείκτη στην τοποθεσία της. Είναι ενδιαφέρον ότι στο συγκεκριμένο πεδίο μπορεί να υπάρξει η σύνοψη ή ένας δείκτης στην ψηφιακή εικόνα μιας χειρόγραφης υπογραφής.
- *Δηλώσεις*. Η τελευταία επέκταση για το πιστοποιητικό μπορεί να περιέχει δηλώσεις που το αφορούν, όπως για παράδειγμα ότι το συγκεκριμένο πιστοποιητικό είναι ένα αναγνωρισμένο πιστοποιητικό.

Τα παραπάνω μπορεί να φαίνονται υπερβολικά τεχνικά και λεπτομερή στο παρόν σημείο. Η σημασία τους θα γίνει όμως περισσότερο κατανοητή στην συνέχεια, καθώς θα δούμε ότι η ύπαρξη ή όχι κάποιων bytes έχει αντίκτυπο στην αποδοχή μιας υπογραφής.

2.3.1 Επαλήθευση με χρήση πιστοποιητικών

Έχοντας ορίσει την έννοια του ψηφιακού πιστοποιητικού θα περιγράψουμε πώς τροποποιείται η διαδικασία της επαλήθευσης μιας ψηφιακής υπογραφής, στην οποία αναφερθήκαμε νωρίτερα. Συγκεκριμένα, ο παραλήπτης αποκτά από μία υπηρεσία καταλόγου, το ψηφιακό πιστοποιητικό του υπογράφοντα. Από το ψηφιακό πιστοποιητικό αυτό θα αποσπάσει το δημόσιο κλειδί που θα χρησιμοποιηθεί

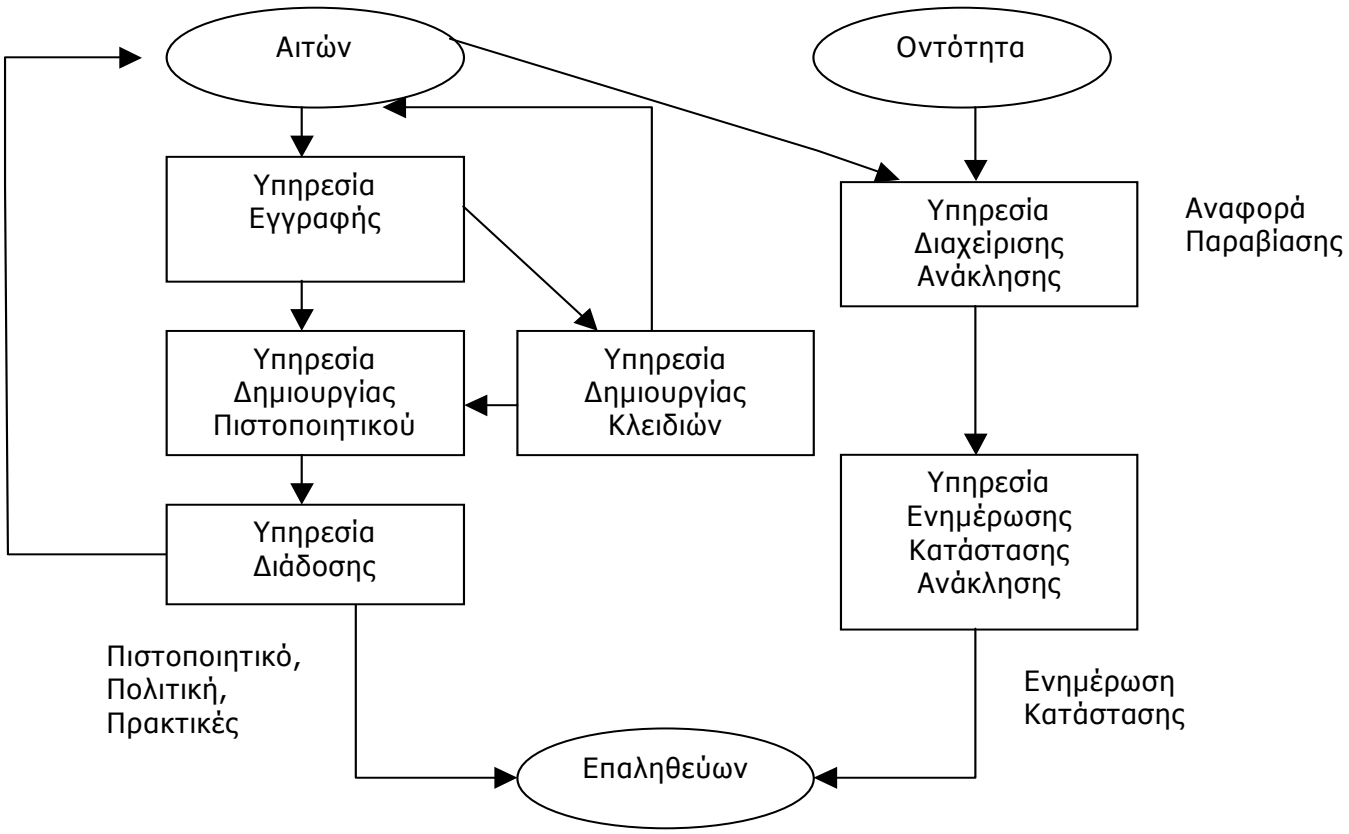
για την επαλήθευση. Πρέπει όμως πρώτα να επαληθεύσει, την εγκυρότητα της υπογραφής που υπάρχει στο ίδιο το πιστοποιητικό και να βεβαιωθεί έτσι για την εγκυρότητα. Για τον σκοπό αυτό είναι απαραίτητη, η απόκτηση του δημοσίου κλειδιού της αρχής πιστοποίησης.

2.4 Αρχές Πιστοποίησης

Όπως προαναφέραμε, οι αρχές πιστοποίησης λειτουργούν ως ενδιάμεσοι στην εκτέλεση μιας ηλεκτρονικής συναλλαγής. Η χρησιμότητα τους έγκειται στο γεγονός, πως πιστοποιούν ότι το δημόσιο κλειδί του υπογράφοντα αντιστοιχεί στο ιδιωτικό του κλειδί, και ό,τι ο κάτοχος του ιδιωτικού κλειδιού είναι μία υπαρκτή φυσική οντότητα. Οι αρχές πιστοποίησης μπορεί να παρέχουν και επιπλέον υπηρεσίες, εκτός από την δημιουργία και υπογραφή πιστοποιητικών όπως **[ETSI, 178T2]**:

- *Υπηρεσίες Διάδοσης / Ανάκτησης Πιστοποιητικών (Directory / Dissemination Services).* Με τις υπηρεσίες αυτές, τα πιστοποιητικά διατίθενται στις οντότητες που θέλουν να επαληθεύσουν ηλεκτρονικές υπογραφές. Η διάδοση αυτή γίνεται μέσω μιας υπηρεσίες καταλόγου (directory service), στην οποία τοποθετούνται τα ψηφιακά πιστοποιητικά και οι ενδιαφερόμενες οντότητες τα ανακτούν. Η οικογένεια προτύπων αυθεντικοποίησης στην οποία εντάσσεται και το πρότυπο X.509 του ISO, ορίζει ένα πρωτόκολλο για την ανάκτηση των πιστοποιητικών, το *DAP (Directory Access Protocol).* Λόγω, όμως της ιδιαίτερα πολύπλοκης δομής του, το πρότυπο αυτό δεν χρησιμοποιήθηκε ποτέ σε ευρεία κλίμακα. Η IETF, ανέλαβε την δημιουργία μίας πιο απλής έκδοσης του για χρήση στο Internet, η οποία ονομάστηκε *LDAP (Lightweight Directory Access Protocol)* **[RFC 1777, 1995]**.
- *Υπηρεσίες Εγγραφής / Ταυτοποίησης Οντοτήτων (Registration Services).* Οι συγκεκριμένες υπηρεσίες έχουν ως στόχο την λειτουργία ενός τμήματος καταχώρησης στοιχείων των οντοτήτων που θέλουν να αποκτήσουν ένα πιστοποιητικό και επαλήθευσης της ταυτότητας τους.
- *Υπηρεσίες Διαχείρισης Ανάκλησης Πιστοποιητικών (Revocation Management Services):* Οι συγκεκριμένες υπηρεσίες είναι υπεύθυνες για την παραλαβή και εξέταση των αιτήσεων για ανάκληση πιστοποιητικών.
- *Υπηρεσίες ενημέρωσης για την κατάσταση των πιστοποιητικών (Revocation Status Service).* Οι συγκεκριμένες υπηρεσίες είναι υπεύθυνες για την δημοσίευση των αποτελεσμάτων των ενεργειών της προηγούμενης υπηρεσίας. Η υλοποίηση της συγκεκριμένης υπηρεσίας μπορεί να γίνεται σε πραγματικό χρόνο ή σε τακτά χρονικά διαστήματα, όπως θα δούμε και στην συνέχεια.
- Προαιρετικά, *υπηρεσίες δημιουργίας κρυπτογραφικών κλειδιών* (Private Key Generation Service) και *υπηρεσίες παροχής ασφαλών συσκευών δημιουργίας υπογραφών (Subscriber Device Provision Service)*. Εδώ η αρχή πιστοποίησης, είτε παρέχει στον συνδρομητή το ιδιωτικό του κλειδί, είτε αρχικοποιεί την ασφαλή διάταξη δημιουργίας υπογραφής, η οποία θα χρησιμοποιείται για την δημιουργία των υπογραφών.
- Προαιρετικά υπηρεσίες χρονοσήμανσης και αρχειοθέτησης, στις οποίες θα αναφερθούμε στην συνέχεια.

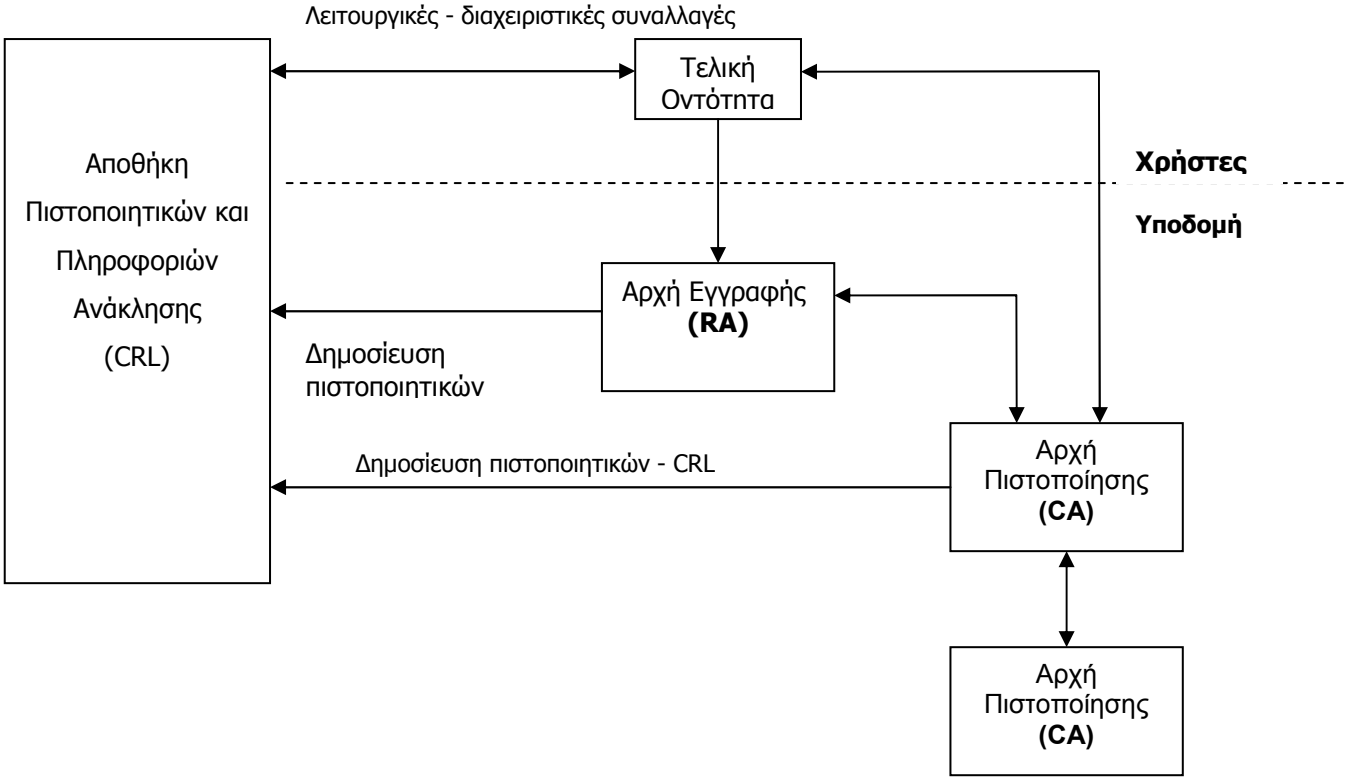
Στο παρακάτω σχήμα φαίνονται οι σχέσεις μεταξύ των υπηρεσιών που προαναφέραμε:



Σχήμα 4. Υπηρεσίες Αρχής Πιστοποίησης

Με άλλα λόγια οι αρχές πιστοποίησης παρέχουν θεωρητικά όλη την υποδομή εκείνη που χρειάζεται για να λειτουργήσει ένα κρυπτοσύστημα δημοσίου κλειδιού. Ο όρος θεωρητικά χρησιμοποιείται καθώς μία αρχή πιστοποίησης έχει *τουλάχιστον* την ευθύνη για την υλοποίηση των παραπάνω λειτουργιών, δεν τις υλοποιεί κατ' ανάγκη η ίδια. Μπορεί να υλοποιούνται με εξωτερική ανάθεση (outsourcing). Το σημαντικό εδώ είναι ποιος έχει την ευθύνη και σε ποιον έχει εκδοθεί το ιδιωτικό κλειδί που χρειάζεται για την δημιουργία και υπογραφή πιστοποιητικών. Ένα σύνηθες παράδειγμα, είναι η όλη διαδικασία προσδιορισμού και επαλήθευσης της ταυτότητας ενός υποκειμένου να γίνεται από μια ξεχωριστή μονάδα της αρχής πιστοποίησης, την *αρχή εγγραφής (Registration Authority)*. Ο τρόπος με τον οποίο έχουν διασπαστεί οι λειτουργίες μίας αρχής (αν έχει συμβεί κάτι τέτοιο) έχει πάρα πολύ μεγάλη επίδραση στην ασφάλεια του όλου συστήματος, όπως αναφέρεται και στο **[Ellison, 2000]**.

Η παρεχόμενη υποδομή και υπηρεσίες για την υλοποίηση ενός συστήματος δημοσίου κλειδιού, ονομάζεται *Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI)*. Έτσι με τον όρο PKI εννοούμε τις αρχές πιστοποίησης, τις υπηρεσίες τους , τα τεχνικά συστατικά τους, όπως ο κατάλογος ανάκτησης πιστοποιητικών, την διεπαφή μέσω της οποίας έρχονται σε επαφή οι εφαρμογές με τις υπηρεσίες καθώς επίσης και όλες τις διαδικασίες που σχετίζονται με τα παραπάνω. Η IETF στο πρότυπο **[RFC2459, 1999]**, προτυποποιεί την υποδομή δημοσίου κλειδιού για το Internet. Η αρχιτεκτονική αυτή φαίνεται στο παρακάτω σχήμα:



Σχήμα 5. Υποδομή Δημοσίου Κλειδιού για το Διαδίκτυο

2.4.1 Μοντέλα Εμπιστοσύνης

Μία εύλογη ερώτηση που προκύπτει μετά από όλη αυτή την ανάλυση είναι, γιατί κάποιος χρήστης να εμπιστευθεί ότι τα στοιχεία και το δημόσιο κλειδί που του παρέχει μία αρχή πιστοποίησης, μέσω των πιστοποιητικών είναι ακριβή; Η τεχνική λύση που δίνεται στα συστήματα είναι η πιστοποίηση της αρχής από μία τρίτη (μάλλον τέταρτη...) οντότητα. Η πιστοποίηση αυτή λειτουργεί ακριβώς όπως και αυτή με τον απλό χρήστη. Με άλλα λόγια, μία αρχή πιστοποίησης εκδίδει και υπογράφει ένα πιστοποιητικό που στο πεδίο υποκείμενο περιέχει το όνομα μιας άλλης αρχής πιστοποίησης. Η διαδικασία αυτή, ονομάζεται δια – πιστοποίηση (cross - certification). Η συγκεκριμένη λύση, όπως γίνεται εύκολα αντιληπτό, δεν λύνει το πρόβλημα. Απλά το μεταθέτει ένα επίπεδο παραπάνω. Η διαδικασία αυτή θα επαναλαμβάνεται, έως ότου βρεθεί κάποια οντότητα την οποία ο επαληθεύων εμπιστεύεται για κάποιο λόγο. Με τον τρόπο αυτόν δημιουργούνται μεταξύ των αρχών πιστοποίησης, σχέσεις *εμπιστοσύνης*. Με τον όρο *εμπιστοσύνη*, εννοούμε απλώς το ότι μία αρχή πιστοποίησης έχει εκδόσει (και κατά συνέπεια υπογράψει) ψηφιακά ένα πιστοποιητικό που έχει ως υποκείμενο του μία άλλη αρχή πιστοποίησης. Τα *μοντέλα εμπιστοσύνης* αποτελούνται ουσιαστικά από ένα σύνολο σχέσεων μεταξύ αρχών πιστοποίησης. Η σημασία των μοντέλων εμπιστοσύνης είναι πολύ μεγάλη στην διαδικασία επαλήθευσης ψηφιακών υπογραφών, καθώς η επαλήθευση ισοδυναμεί με την εύρεση του μονοπατιού που συνδέει την εκδούσα αρχή ενός πιστοποιητικού με μία αρχή την οποία εμπιστεύεται ο επαληθεύων. Το συγκεκριμένο μονοπάτι αναφέρεται ως μονοπάτι

πιστοποίησης (*certification path*).

Τα πιο γνωστά μοντέλα εμπιστοσύνης που αναφέρονται στην βιβλιογραφία είναι τα εξής:

- *Ιεραρχικό:* Στο συγκεκριμένο μοντέλο, όλοι οι χρήστες 'εμπιστεύονται' μία αρχή πιστοποίησης (root certification authority). Οι υπόλοιπες αρχές πιστοποίησης διατάσσονται σε επίπεδα, κάτω από την βασική αρχή αυτή. Στο πρώτο επίπεδο, βρίσκονται όλες οι αρχές πιστοποίησης, για τις οποίες η βασική αρχή έχει εκδώσει πιστοποιητικά. Στο δεύτερο επίπεδο, βρίσκονται όλες οι αρχές πιστοποίησης οι οποίες έχουν λάβει πιστοποιητικά για το δημόσιο κλειδί τους από οποιαδήποτε αρχή πιστοποίησης του πρώτου επιπέδου, κ.ό.κ. Τα φύλλα του δένδρου που σχηματίζεται είναι οι τελικοί χρήστες.
- *Λίστα Πιστοποιητικών:* Το συγκεκριμένο μοντέλο, το οποίο είναι αυτό που έχει υλοποιηθεί στους σύγχρονους web browsers. Συγκεκριμένα κάθε χρήστης διαθέτει ένα σύνολο από αρχές πιστοποίησης τις οποίες εμπιστεύεται και τα πιστοποιητικά τους. Μπορεί κατά συνέπεια να επαληθεύσει ψηφιακές υπογραφές, οι οποίες συνοδεύονται από πιστοποιητικά τα οποία έχουν εκδώσει οι αρχές που βρίσκονται στην λίστα του. Βέβαια τα πιστοποιητικά αυτά έχονται συνήθως προεγκατεστημένα με τον browser, οπότε μάλλον αφορούν αυτούς που εμπιστεύονται οι κατασκευαστές τους. Η λίστα αυτή μπορεί βέβαια να τροποποιηθεί, αλλά πόσοι χρήστες θα το κάνουν;
- *Γενικευμένο:* Οι σχέσεις εμπιστοσύνης μεταξύ των αρχών πιστοποίησης είναι αυθαίρετες. Με άλλα λόγια οποιαδήποτε αρχή πιστοποίησης, μπορεί να έχει υπογράψει το πιστοποιητικό οποιαδήποτε άλλης αρχής πιστοποίησης.
- *Γέφυρα:* Το συγκεκριμένο μοντέλο μπορεί να απλοποιήσει τις σχέσεις εμπιστοσύνης σε ένα γενικευμένο μοντέλο εμπιστοσύνης. Ουσιαστικά πρόκειται για μία τοπολογία αστέρα στην οποία αντί κάθε αρχή πιστοποίησης να διαπιστοποιείται με κάθε άλλη, διαπιστοποιείται με μία κεντρική.

Οι διαδικασίες για την επαλήθευση μιας ψηφιακής υπογραφής θα αναπτυχθούν εκτενώς στο επόμενο κεφάλαιο. Η σημασία των μοντέλων εμπιστοσύνης που αναπτύξαμε, στην συγκεκριμένη παράγραφο είναι κυρίως θεωρητική. Λίγες είναι οι περιπτώσεις που έχουν βρει πρακτική εφαρμογή και αυτό κυρίως έχει συμβεί σε ελεγχόμενα περιβάλλοντα, όπως για παράδειγμα στο εσωτερικό ενός οργανισμού. Αυτό άλλωστε είναι λογικό, καθώς όπως είδαμε, βασίζονται σε υποθέσεις, οι οποίες μεταθέτουν την ευθύνη ένα επίπεδο πιο πάνω. Επειδή δεν είναι δυνατό να βασιστεί κανείς στην συγκεκριμένη λύση, χρειάζεται μία εξωτερική παρέμβαση, η οποία θα έχει την μορφή διαπίστευσης ή μίας δημόσιας (και κατ' επέκταση έμπιστης) αρχής πιστοποίησης.

2.5 Ανάκληση Πιστοποιητικών

Η διαδικασία της πιστοποίησης όπως την περιγράψαμε νωρίτερα, γίνεται μία φορά. Δηλαδή η οντότητα που διαθέτει το ιδιωτικό κλειδί ταυτοποιείται στην αρχή πιστοποίησης, η οποία και εκδίδει το πιστοποιητικό. Από την στιγμή που αυτό τοποθετείται στον κατάλογο και μέχρι την ημερομηνία λήξης του, είναι διαθέσιμο σε όποια οντότητα επιθυμεί να το χρησιμοποιήσει. Υπάρχει βέβαια και η περίπτωση

απώλειας του ιδιωτικού κλειδιού ή παραβίασης της ασφάλειας του. Προφανώς, η διαδικασία που θα ακολουθηθεί τότε από τον κάτοχο, θα είναι ανάλογη με την διαδικασία που ακολουθείται με την απώλεια μιας πιστωτικής κάρτας. Το τεχνικό θέμα που θα μας απασχολήσει εδώ είναι πώς μια οντότητα που θα λάβει το πιστοποιητικό για να επαληθεύσει μία ψηφιακή υπογραφή, θα μπορέσει να καταλάβει ότι δεν αναφέρεται πλέον σε έγκυρο κλειδί έτσι ώστε να μην το χρησιμοποιήσει. Οι τεχνικές λύσεις που δίνονται στο συγκεκριμένο πρόβλημα ανήκουν σε δύο κατηγορίες:

- Λίστες ανάκλησης πιστοποιητικών.
- Πρωτόκολλα ενημέρωσης κατάστασης πιστοποιητικών.

Μία απλή λίστα ανάκλησης πιστοποιητικών αρκεί να περιέχει έναν αριθμό που προσδιορίζει κάθε άκυρο πιστοποιητικό και την ημερομηνία ανάκλησης του μαζί με την ψηφιακή υπογραφή της αρχής πιστοποίησης.

Λόγω της ευρείας χρήσης των πιστοποιητικών X.509, το πιο δημοφιλές πρότυπο για τις λίστες ανάκλησης είναι το X.509. Το συγκεκριμένο πρότυπο έχει υιοθετηθεί και από την κοινότητα του Internet με το **[RFC2459, 1999]**. Η ιστορία του είναι σχεδόν παρόμοια με αυτή του πιστοποιητικού, καθώς πέρασε και αυτή από δύο βασικές εκδόσεις και συμπληρώθηκε στα μέσα της δεκαετίας του ’90 από τον μηχανισμό των επεκτάσεων.

Μία λίστα ανάκλησης πιστοποιητικών X.509 αποτελείται λοιπόν από τα εξής πεδία:

- **Έκδοση:** Ένας αριθμός ο οποίος προσδιορίζει την έκδοση της λίστας. Σε περίπτωση που η λίστα έχει την μορφή της πρώτης έκδοσης, δεν υποστηρίζονται οι επεκτάσεις.
- **Αλγόριθμος Ψηφιακής Υπογραφής:** Στο συγκεκριμένο πεδίο αναφέρεται ο αναγνωριστής ASN.1 του αλγορίθμου ψηφιακής υπογραφής, που χρησιμοποιείται για να υπογράψει η εκδούσα αρχή την λίστα.
- **Εκδούσα Αρχή :** Πρόκειται για το όνομα κατά X.500 της αρχής πιστοποίησης που εκδίδει την CRL και που συνήθως είναι η αρχή η οποία εκδίδει τα πιστοποιητικά τα οποία ακυρώνονται.
- **Ημερομηνία Έκδοσης:** Η ώρα και ημέρα που εκδίδεται η λίστα.
- **Επόμενη Έκδοση:** Η ημέρα και ώρα που θα υπάρξει έκδοση της επόμενης CRL. Το συγκεκριμένο πεδίο είναι προαιρετικό, αλλά η χρήση του συνίσταται.
- Για κάθε πιστοποιητικό που ανακαλείται με την συγκεκριμένη λίστα αναφέρεται ο σειριακός αριθμός του, η ημερομηνία ανάκλησης του καθώς και κάποιες επεκτάσεις.
- **Επεκτάσεις CRL**: Στο συγκεκριμένο πεδίο μπορούν αν υπάρχουν επεκτάσεις που έχουν την ίδια δομή, όπως στο πιστοποιητικό X.509, δηλαδή τύπος – ένδειξη κρισιμότητας – τιμή.

Η γενική αυτή μορφή φαίνεται στο παρακάτω σχήμα:

Σχήμα 6. Μορφή Λίστας Ανάκλησης για Πιστοποιητικά X.509

Όπως και για τις επεκτάσεις των πιστοποιητικών, έτσι και για τις επεκτάσεις που αναφέρονται στις λίστες ανάκλησης η ύπαρξη τους δεν έχει νόημα αν δεν συνοδεύεται από κάποια προτυποποίηση. Εδώ μπορούμε να διακρίνουμε δύο κατηγορίες επεκτάσεων. Αυτές που αντιστοιχούν σε όλη την λίστα ανάκλησης και αυτές που αφορούν κάθε ένα άκυρο πιστοποιητικό, ξεχωριστά. Από τις προτυποποιημένες επεκτάσεις οι πιο σημαντικές είναι οι εξής:

- **Λόγος Ανάκλησης**: Στο συγκεκριμένο πεδίο αναφέρεται ένας λόγος για την ακύρωση του πιστοποιητικού. Προφανώς αντιστοιχεί σε κάθε 'εγγραφή' πιστοποιητικού στην λίστα. Οι επιτρεπτές τιμές για το συγκεκριμένο πεδίο μπορεί να είναι: διαρροή ιδιωτικού κλειδιού, αλλαγή πληροφορίας υποκειμένου, λήξη περιόδου ισχύος, παύση σκοπού ύπαρξης.
- **Ημερομηνία Ακύρωσης**: Η συγκεκριμένη επέκταση αναφέρει την ημερομηνία που ένα συγκεκριμένο πιστοποιητικό έχασε την ισχύ του.
- **CRL Distribution Point**: Είναι το υποσύνολο των πιστοποιητικών τα οποία καλύπτει η συγκεκριμένη λίστα, δηλαδή τα πιθανά εκείνα πιστοποιητικά τα οποία μπορούν να εισαχθούν στην λίστα αν χάσουν την ισχύ τους. Η συγκεκριμένη επέκταση είναι ένας μηχανισμός με τον οποίο υφίσταται κάποιος έλεγχος στον μέγιστο αριθμό των πιστοποιητικών που μπορούν να υπάρξουν σε μία λίστα.
- **Επέκταση Αναστολής**: Η συγκεκριμένη επέκταση είναι πολύ χρήσιμη σε περιπτώσεις, όπου δεν είναι ξεκάθαρο αν η ασφάλεια του ιδιωτικού κλειδιού, για παράδειγμα, έχει παραβιαστεί. Μπορεί να τεθεί

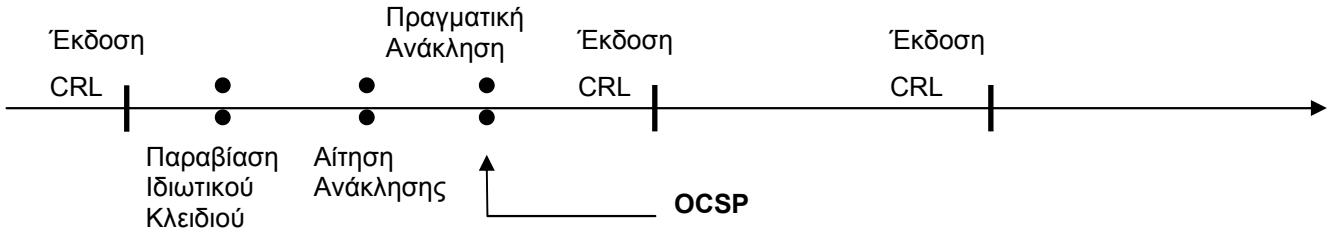
μόνο από την αρχή πιστοποίησης και χρησιμοποιείται σε περιπτώσεις, όπου φαίνεται να υπάρχει κάποια υποψία σχετικά με ένα πιστοποιητικό, χωρίς όμως να υπάρχει αίτηση ανάκλησης. Τότε, εκδίδεται μία λίστα ανάκλησης, η οποία θα περιέχει το συγκεκριμένο πιστοποιητικό, το οποίο όμως θα συνοδεύεται από την επέκταση της αναστολής. Σε επόμενη λίστα, το πιστοποιητικό είτε θα έχει ανακληθεί είτε δεν θα περιέχεται στην λίστα κάτι που σημαίνει, ότι δεν υπάρχει πραγματικά κάποιος σχετικός λόγος ανησυχίας για το συγκεκριμένο πιστοποιητικό.

- **Δ – CRLs :** Ο μηχανισμός των επεκτάσεων, μπορεί να χρησιμοποιηθεί για να μειωθεί ο φόρτος συνεχούς δημιουργίας και διανομής καινούριων λιστών. Συγκεκριμένα, αντί κάθε φορά μία λίστα επέκτασης να περιέχει όλα τα πιστοποιητικά που έχουν ανακληθεί, θα περιέχει εκείνα τα πιστοποιητικά που έχουν ανακληθεί από την τελευταία φορά, που εκδόθηκε λίστα ανάκλησης ή Δ – CRL. Αυτό υλοποιείται με δύο επεκτάσεις, η πρώτη από τις οποίες χαρακτηρίζει μία CRL, ως Δ και μίας δεύτερης, η οποία αναφέρει την πλήρη λίστα ανάκλησης με την οποία σχετίζεται (δηλαδή στην οποία φέρει αλλαγές).

Ο δεύτερος τρόπος για την ενημέρωση σχετικά με την κατάσταση ενός πιστοποιητικού είναι μέσω πρωτοκόλλων τα οποία λειτουργούν σε πραγματικό χρόνο. Το πιο διαδεδομένο από αυτά είναι το **OCSP (Online Certificate Status Protocol)**, του οποίου η χρήση για το Internet έχει προτυποποιηθεί με το RFC 2560**.** Η λειτουργία του μπορεί να περιγραφεί συνοπτικά ως εξής: Η εφαρμογή η οποία θέλει να επαληθεύσει την κατάσταση ενός πιστοποιητικού στέλνει μία αίτηση OCSP (request) στον εξυπηρετητή της αρχής πιστοποίησης. Η αίτηση αυτή περιέχει τον αριθμό σειράς του πιστοποιητικού. Ο εξυπηρετητής OCSP ελέγχει μία Βάση Δεδομένων και επιστρέφει την απάντηση του στον πελάτη. Η απάντηση πρέπει να είναι ψηφιακά υπογεγραμμένη. Σε αυτήν, παρατίθεται για την κατάσταση του πιστοποιητικού μία από τις παρακάτω τιμές:

- **Έγκυρο:** Το ψηφιακό πιστοποιητικό δεν έχει ανακληθεί και μπορεί να χρησιμοποιηθεί ελεύθερα για την επαλήθευση της υπογραφής.
- **Άκυρο:** Το ψηφιακό πιστοποιητικό έχει ανακληθεί.
- **Άγνωστο:** Η κατάσταση του ψηφιακού πιστοποιητικού είναι άγνωστη.

Και οι δύο παραπάνω τρόποι παρουσιάζουν αρκετά μειονεκτήματα. Τα μειονεκτήματα των λιστών ανάκλησης εντοπίζονται στο γεγονός ότι αυτές εκδίδονται περιοδικά και φαίνονται καλύτερα με το παρακάτω σχήμα **[Ford, 2001]**:



Σχήμα 7. Κρίσιμα χρονικά διαστήματα για την ανάκληση πιστοποιητικού

Μεταξύ της παραβίασης του ιδιωτικού κλειδιού και της αίτησης ανάκλησης ούτε η αρχή πιστοποίησης και κατά συνέπεια κανένας παραλήπτης της υπογραφής δεν μπορεί να γνωρίζει για την πραγματική τύχη του ιδιωτικού κλειδιού. Κατά συνέπεια όλες οι ψηφιακές υπογραφές που θα επαληθευθούν στο συγκεκριμένο χρονικό διάστημα θα θεωρηθούν έγκυρες, παρόλο που μπορεί να έχουν δημιουργηθεί και από κάποιον τρίτο. Το ίδιο θα συμβεί και σε οποιαδήποτε άλλη χρονική στιγμή γίνει προσπάθεια για επαλήθευση μιας υπογραφής, πριν την έκδοση της επόμενης λίστας.

Αν αντί για τις λίστες ανάκλησης χρησιμοποιείται το πρωτόκολλο OCSP, προφανώς η νωρίτερη στιγμή της γνωστοποίησης θα είναι η στιγμή κατά την οποία γίνεται η ανάκληση του πιστοποιητικού από την αρχή. Διαπιστώνουμε έτσι ότι το OCSP υπερτερεί της μεθόδου των λιστών ανάκλησης σε αυτό το σημείο. Παρ' όλα αυτά το OCSP, χαρακτηρίζεται από το μειονέκτημα της συνεχούς διαθεσιμότητας την οποία απαιτεί. Οι απαιτήσεις δικτύου και επεξεργασίας αυξάνονται κατακόρυφα, αν αναλογιστούμε το γεγονός ότι πρέπει να υπογράφεται ψηφιακά κάθε απόκριση, διαδικασία υπολογιστικά δαπανηρή. Γίνεται έτσι εύκολος στόχος για επιθέσεις **DoS (Denial of Service).** Είναι κοινώς αποδεκτό ότι στο Internet σήμερα το συγκεκριμένο πρωτόκολλο δεν μπορεί να υλοποιηθεί επιτυχώς.

Για τον παραπάνω λόγο, κυρίως, και παρά τα μειονεκτήματα που εμφανίζουν, οι λίστες ανακλήσης χρησιμοποιούνται στην πρακτική εφαρμογή. Ακολουθείται η πολιτική της συχνής έκδοσης ενημερώσεων, σε χρονικά διαστήματα περίπου μιας ημέρας. Διαπιστώνουμε, εν κατακλείδι, ότι το θέμα της ανάκλησης, δεν μπορεί να λυθεί αποκλειστικά με την χρήση τεχνικών μέτρων.

2.6 Έμπιστες Τρίτες Οντότητες – Επιπλέον Υπηρεσίες

Όπως προαναφέραμε, οι έμπιστες τρίτες οντότητες παρέχουν επιπλέον υπηρεσίες από τις αρχές πιστοποίησης. Οι πιο σημαντικές από αυτές είναι:

- **Χρονοσήμανση (Time Stamping).**

Μία υπηρεσία χρονοσήμανσης έχει ως σκοπό να προσδιορίσει με ακρίβεια την χρονική στιγμή, κατά την οποία έλαβε χώρα ένα μήνυμα. Εύλογα καταλαβαίνουμε, ότι ο συγκεκριμένος μηχανισμός δεν είναι καινούριος ούτε υφίσταται αποκλειστικά στις ηλεκτρονικές συναλλαγές. Ένα παράδειγμα χρονοσήμανσης, στον συμβατικό κόσμο, αποτελούν οι ταχυδρομικές σφραγίδες. Σε ένα ηλεκτρονικό περιβάλλον, η χρονοσήμανση λειτουργεί ως εξής:

- Η οντότητα που κατέχει το μήνυμα, το αποστέλλει στην έμπιστη τρίτη οντότητα. Αν το μήνυμα είναι εμπιστευτικό μπορεί αντί γι' αυτό να αποσταλεί είτε η σύνοψη του, είτε μία κρυπτογραφημένη έκδοση του. Ανάλογα με τις απαιτήσεις που τίθενται από το περιβάλλον, το συγκεκριμένο κείμενο μπορεί να είναι ψηφιακά υπογεγραμμένο.
- Η έμπιστη τρίτη οντότητα, λειτουργεί μία υπηρεσία η οποία αναφέρει την τρέχουσα ημέρα και ώρα. Έτσι, όταν λάβει το μήνυμα προσαρτά την τιμή της υπηρεσίας αυτής σε αυτό.
- Τέλος, υπογράφει ψηφιακά το αποτέλεσμα.

Η διαδικασία που περιγράψαμε εξασφαλίζει την ύπαρξη του μηνύματος πρίν από την χρονική στιγμή κατά την οποία έγινε η χρονοσήμανση.

Η ύπαρξη και χρήση μιας υπηρεσίας χρονοσήμανσης μπορεί να χρησιμοποιηθεί και για την ασφαλή επαλήθευση μιας ψηφιακής υπογραφής, έτσι ώστε να μειωθούν τα κρίσιμα χρονικά διαστήματα τα οποία είδαμε στο σχήμα 7, Για τον σκοπό αυτό πρέπει να αλλαχθεί (πάλι) η διαδικασία επαλήθευσης και δημιουργίας (αυτή την φορά) μιας ψηφιακής υπογραφής. Σύμφωνα λοιπόν με το **[RFC 3161, 2001]** η διαδικασία ψηφιακής υπογραφής με χρονοσήμανση μπορεί να διαμορφωθεί ως εξής:

1. Δημιουργία Ψηφιακής Υπογραφής.
2. Μέσα σε ένα όσο το δυνατόν συντομότερο χρονικό διάστημα, αποστέλλεται αυτή στην υπηρεσία χρονοσήμανσης.
3. Επιστρέφεται η χρονοσήμανση. Η ορθότητα του μηνύματος επαληθεύεται από τον υπογράφοντα και προσαρτάται στο μήνυμα.
4. Κατά την διάρκεια επαλήθευσης αποσπάται η χρονοσήμανση και ελέγχεται η ορθότητα της.
5. Αποσπάται από την χρονοσήμανση η παράμετρος του χρόνου.
6. Επαληθεύεται του πιστοποιητικό, όπως προαναφέραμε.
7. Ελέγχεται αν η χρονική στιγμή η οποία αποσπάσθηκε στο (5), είναι μέσα στην περίοδο ισχύος του πιστοποιητικού.
8. Ανάκτηση πληροφορίας ανάκλησης, η οποία ισχύει την χρονική στιγμή του (5).
9. Αν το πιστοποιητικό, έχει ανακληθεί, τότε ελέγχεται εάν η στιγμή ανάκλησης του είναι μεγαλύτερη από την χρονική στιγμή του (5).

Άν όλοι οι παραπάνω έλεγχοι είναι επιτυχείς, τότε η ψηφιακή υπογραφή είναι έγκυρη.

- **Τήρηση Ηλεκτρονικών Αρχείων (Records Archival).**

Με μία λειτουργία, όπως αυτή της χρονοσήμανσης, η έμπιστη τρίτη οντότητα αποκτά στοιχεία ότι ένα μήνυμα υπήρξε μία συγκεκριμένη χρονική στιγμή και βρισκόταν στην κατοχή κάποιας οντότητας – η οποία μπορεί να προσδιοριστεί αν χρησιμοποιείται κάποιος μηχανισμός αυθεντικοποίησης, όπως οι ψηφιακές υπογραφές. Η έμπιστη τρίτη οντότητα, μπορεί να αρχειοθετεί, τα ηλεκτρονικά αυτά στοιχεία για ένα μεγάλο χρονικό διάστημα, ανάλογα με τις απαιτήσεις που τίθενται σε μία συναλλαγή, από τους συμμετέχοντες ή από το περιβάλλον στο οποίο αυτή υφίσταται.

Οι υπηρεσίες των έμπιστων τρίτων οντοτήτων εντάσσονται κυρίως στην περιοχή της μη αποποίησης ευθύνης (non repudiation). Πρόκειται για μία ιδιότητα που αν διαθέτει μία (ηλεκτρονική) συναλλαγή, προστατεύεται από επιτυχή άρνηση της συμμετοχής σε αυτήν. Αν δεν την διαθέτει τότε οι έμπιστες τρίτες οντότητες θα κληθούν να παίξουν ένα σημαντικό ρόλο στην επίλυση διαφορών (*Dispute Resolution*), η οποία κατά πάσα πιθανότητα δεν θα γίνει σε τεχνικό αλλά πιθανότατα σε νομικό επίπεδο.

2.7 Συμπεράσματα

Στο συγκεκριμένο κεφάλαιο κάναμε μία τεχνική προσέγγιση στο ζήτημα των ηλεκτρονικών υπογραφών. Περιγράψαμε τους αλγόριθμους καθώς και τις υπηρεσίες που χρειάζονται για την υποστήριξη τους, αναφέροντας και τα διεθνή πρότυπα τα οποία τους συνοδεύουν. Μπορούμε να συνοψίσουμε τα συμπεράσματα μας στο γεγονός, ότι αφενός καμία τεχνική μέθοδος ή οποιοσδήποτε συνδυασμός της δεν είναι *υπογραφή* με την έννοια που όλοι γνωρίζουμε. Η υποστηρικτική υποδομή (δημοσίου κλειδιού) λύνει κάποια θέματα, προσθέτει όμως ακόμη περισσότερα.

Πιο αναλυτικά, διαπιστώνουμε ότι από τις μορφές αυθεντικοποίησης μόνο οι βιομετρικές τεχνολογίες, αν υλοποιηθούν σωστά, μπορούν να ταυτοποιήσουν πλήρως το υποκείμενο, καθώς συναρτούν την έννοια της αυθεντικοποίησης με κάτι που πραγματικά το χαρακτηρίζει. Χαρακτηρίζονται όμως από δυσκολίες υλοποίησης και μειωμένη αποδοχή από το ευρύ κοινό. Σε όλες τις άλλες μεθόδους, η αυθεντικοποίηση γίνεται έμμεσα, καθώς η ταυτότητα επιβεβαιώνεται με κάτι που νομίζουμε ότι κατέχει ή γνωρίζει ο χρήστης. Για παράδειγμα, στις ψηφιακές υπογραφές επιβεβαιώνεται μόνο η μαθηματική σχέση του ιδιωτικού με το δημόσιο κλειδί. Το ποιος κατέχει το ιδιωτικό δεν μπορεί να προσδιοριστεί από την συγκεκριμένη τεχνική.

Επίσης καμία από τις παραπάνω τεχνικές δεν μπορεί να χαρακτηριστεί ως υπογραφή, καθώς δεν φαίνεται να πληροί τις προϋποθέσεις που έχουν αναπτυχθεί γι' αυτές μέσα στους αιώνες. Είναι απλά μέθοδοι αυθεντικοποίησης, οι οποίες μπορούν καταχρηστικά να χαρακτηριστούν ως υπογραφές σε περίπτωση που το υπογεγραμμένο κείμενο έχει μεγάλη διάρκεια ζωής. Για παράδειγμα, σε επίπεδο υλοποίησης, η αυθεντικοποίηση με χρήση ασύμμετρων κρυπτοσυστημάτων, γίνεται με την δημιουργία της ψηφιακής υπογραφής σε μια τυχαία δυαδική συμβολοσειρά, η οποία μετά καταστρέφεται. Πώς μπορεί να ξεχωρίσει κανείς την τυχαία αυτή συμβολοσειρά, από την δυαδική συμβολοσειρά που προκύπτει ώς η σύνοψη ενός συντακτικά σωστού κειμένου; Η απάντηση είναι πώς δεν μπορεί. Η πρακτική λύση σε αυτό δίδεται με την χρήση διαφορετικών κλειδιών για αυθεντικοποίηση, υπογραφή και βέβαια κρυπτογράφηση. Φαίνεται δηλαδή πώς είναι κυρίως θέμα διαχείρισης ασφάλειας. Επίσης, καμία από τις παραπάνω μεθόδους δεν παρέχει ένδειξη, τουλάχιστον, ότι ο υπογράφων έλαβε εις γνώση του το κείμενο προτού υπογράψει.

Ίσως όλα να έχουν προκύψει από μία άτυχη ιστορική συγκυρία, δηλαδή την χρήση του όρου *ψηφιακή υπογραφή*, από τον Diffie και Hellman για την λειτουργία αυθεντικοποίησης των ασύμμετρων κρυπτοσυστημάτων. Βέβαια, η παραπάνω διαπίστωση μας, μπορεί να διαψευσθεί αν επιχειρήσουμε μία τεχνική ανάλυση της συμβατικής υπογραφής, η οποία ούτε και αυτή εγγυάται ότι υπέγραψε πραγματικά η οντότητα που φαίνεται ότι υπέγραψε. Είναι ίσως το σύνολο των πρακτικών που συνοδεύουν την πράξη της υπογραφής που της δίνει αξία και μπορεί η εξέλιξη των ηλεκτρονικών υπογραφών να οδηγήσει σε ανάλογες πρακτικές, οι οποίες θα αίρουν τις επιφυλάξεις που διαπιστώσαμε νωρίτερα. Εξ' άλλου, όπως προαναφέραμε τεχνικά οι ψηφιακές υπογραφές παρέχουν επιπλέον χαρακτηριστικά από τις συμβατικές, όπως για παράδειγμα το ότι εγγυώνται πλήρως την ακεραιότητα του κειμένου.

Η υποδομή που υποστηρίζει τις ψηφιακές υπογραφές, θέτει από μόνη της κάποια πολύ σημαντικά ερωτήματα, τόσο τεχνικά όσο και διαχειριστικά. Για παράδειγμα η ακριβής ονοματοδοσία των οντοτήτων είναι δύσκολη, από την φύση του X.500. Οι λίστες ανάκλησης είναι κατάλοιπο μίας πρακτικής που ίσχυε στην δεκαετία του 1970 για τις πιστωτικές κάρτες και η οποία εγκαταλείφθηκε...

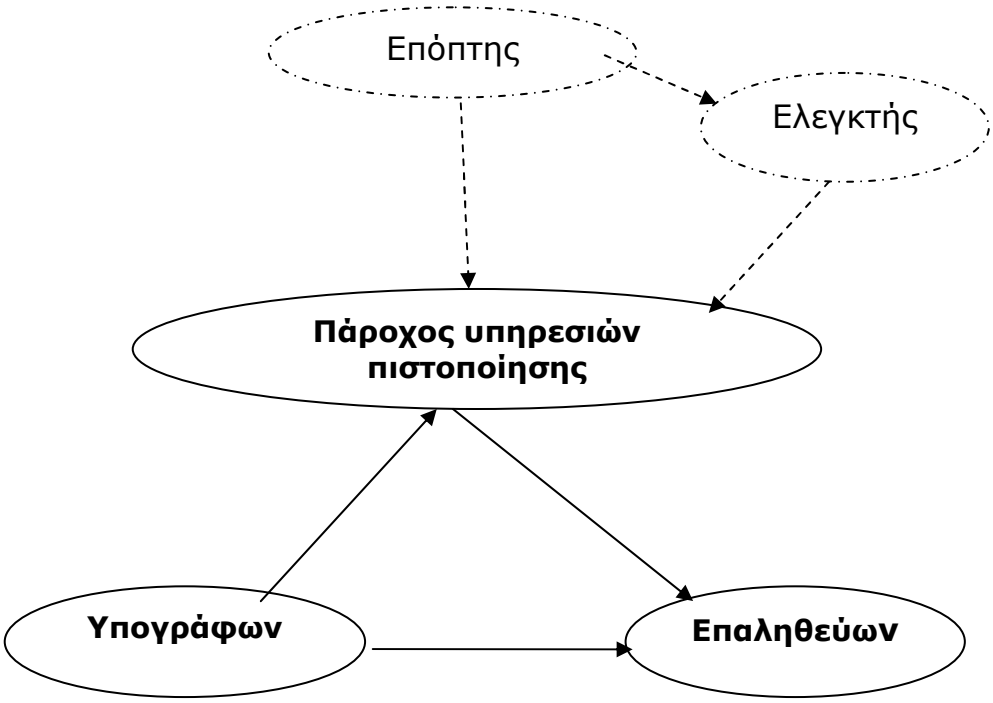
Δημιουργεί δε ένα καινούριο είδος παροχής υπηρεσιών, το οποίο παίζει κεντρικό ρόλο σε κάθε ηλεκτρονική συναλλαγή. Οι καινούριοι αυτοί πάροχοι υπηρεσιών διαφέρουν από ανάλογους που έχουμε γνωρίσει μέχρι σήμερα, όπως για παραδείγματα τους εκδότες πιστωτικών καρτών, καθώς συμμετέχουν σε κάθε συναλλαγή παρά το γεγονός ότι δεν έχουν όφελος από αυτή καθ' αυτή. Καθίστανται έτσι ως ο πιο σημαντικός κρίκος σε κάθε ηλεκτρονική συναλλαγή. Φέρουν έτσι ευθύνη για πιθανές ατυχείς καταλήξεις των συναλλαγών. Το πόση από την ευθύνη αυτή θα αναλάβουν και νομικά και το αν είναι οι μόνοι που έχουν ευθύνη είναι θέματα που θα αναλυθούν διεξοδικά στην συνέχεια της εργασίας. Παράλληλα, οι πάροχοι υπηρεσιών πιστοποίησης αποτελούν και στόχο για πιθανές επιθέσεις, τόσο ηλεκτρονικές (απειλές εισβολής και κλοπής ιδιωτικού κλειδιού) όσο και μη ηλεκτρονικές (εξαπάτηση). Αποτελεί εύλογη απαίτηση λοιπόν η ρύθμιση της λειτουργίας τους με τέτοιο τρόπο, ώστε να μπορούν να παρέχουν με τον καλύτερο δυνατό τρόπο τις υπηρεσίες τους προς όφελος του τελικού χρήστη, που στην περίπτωση των ηλεκτρονικών υπογραφών θα είναι πιθανότατα ο κάθε απλός πολίτης.

3 Συστήματα Ηλεκτρονικών Υπογραφών.

3.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο παραθέσαμε τις βασικές τεχνολογίες που συναντάει κανείς σε ένα περιβάλλον ηλεκτρονικών υπογραφών. Διαπιστώσαμε ότι δημιουργήθηκαν αρχικά και για άλλες χρήσεις, εκτός από ηλεκτρονικές υπογραφές. Στο κεφάλαιο αυτό λοιπόν θα δούμε πώς οι συγκεκριμένες τεχνολογίες μπορούν να ενσωματωθούν σε ολοκληρωμένα συστήματα με χρήση στις ηλεκτρονικές υπογραφές. Για αυτά θα προβούμε σε μία λειτουργική μοντελοποίηση και θα αναφέρουμε τις απαιτήσεις ασφαλείας τους.

Το πρώτο πράγμα το οποίο θα προσπαθήσουμε στο συγκεκριμένο κεφάλαιο είναι να βάλουμε τις ηλεκτρονικές υπογραφές σε ένα περιβάλλον. Όπως θα δούμε σε όλη την διάρκεια της εργασίας το συγκεκριμένο περιβάλλον δεν διαμορφώνεται μόνο από τεχνικούς παράγοντες. Κάθε άλλο, μάλιστα καθώς καθοριστική σημασία έχει το νομικό και κανονιστικό πλαίσιο το οποίο τις αναγνωρίζει. Το τυπικό λοιπόν περιβάλλον χρήσης τους φαίνεται συνολικά στο παρακάτω σχήμα:



Σχήμα 8. Σχέσεις Συμμετεχόντων Σε Περιβάλλον Ηλ. Υπογραφών

Από τις παραπάνω οντότητες, δεν αναφερθήκαμε νωρίτερα στον επόπτη και τον ελεγκτή. Στο συγκεκριμένο κεφάλαιο θα τους δώσουμε λόγο ύπαρξης και αντικείμενο εργασίας, καθώς θα παραθέσουμε τα πιο σημαντικά πρότυπα για συστήματα ηλεκτρονικών υπογραφών. Στον συγκεκριμένο τομέα η διεθνής πραγματικότητα έχει να επιδείξει δύο προσεγγίσεις. Η μία θεωρεί τα διάφορα συστήματα τα οποία χρησιμοποιούνται για ηλεκτρονικές υπογραφές ως ένα υποσύνολο των διατάξεων με αυξημένες απαιτήσεις ασφαλείας. Έτσι για την αποτίμηση τους χρησιμοποιεί έτοιμα πρότυπα, τα οποία δεν έχουν δηλαδή

δημιουργηθεί έχοντας υπόψη ότι η αξιολόγηση θα αφορά συστήματα ηλεκτρονικών υπογραφών. Τέτοια πρότυπα είναι τα κλασικά *TCSEC, ITSEC, FIPS PUB 140-1 και ISO 17799*. Η δεύτερη θέτει απαιτήσεις ασφαλείας και προδιαγράφει λειτουργίες έχοντας υπ'όψη το περιβάλλον ηλεκτρονικών υπογραφών στο οποίο θα χρησιμοποιηθούν τα συγκεκριμένα συστήματα, χωρίς όμως να 'ανακαλύπτει ξανά τον τροχό'. Βασίζεται σε πρότυπα όπως αυτά που παραθέσαμε παραπάνω, τα οποία όμως διαμορφώνει έτσι ώστε να τα προσαρμόσει στο συγκεκριμένο περιβάλλον.

Θεωρούμε πάντως πως το πρώτο βήμα για να θέσουμε τις ηλεκτρονικές υπογραφές στο περιβάλλον τους είναι να εξετάσουμε τα διάφορα 'κείμενα' τα οποία εκδίδει ένας πάροχος υπηρεσιών πιστοποίησης. Τα κείμενα αυτά, αποτέλεσαν στα προηγούμενα χρόνια, που διακρίνονταν από ανυπαρξία νομικών πλαισίων και κατά συνέπεια του επόπτη του παραπάνω σχήματος, τον μόνο τρόπο με τον οποίο μπορούσαν να ρυθμιστούν οι σχέσεις μεταξύ χρηστών και παρόχων πιστοποίησης. Κάτι τέτοιο εξακολουθεί να ισχύει και σήμερα και είναι αποδεκτό μάλιστα από αρκετά κανονιστικά πλαίσια, όπως θα δούμε και στην συνέχεια. Αρχικά λοιπόν θα ξεκινήσουμε περιγράφοντας τις έννοιες της πολιτικής πιστοποίησης, δήλωσης πρακτικών πιστοποίησης και πολιτικής υπογραφής. Έπειτα θα αναφερθούμε στα πρότυπα.

3.2 Πολιτική Πιστοποίησης

Η πολιτική πιστοποίησης είναι απαραίτητο στοιχείο οποιασδήποτε υποδομής δημοσίου κλειδιού και άρα αφορά συγκεκριμένα τις ψηφιακές υπογραφές.

Ο πιο συχνά χρησιμοποιούμενος ορισμός της είναι αυτός που υπάρχει στο πρότυπο X.509 και αφορά τα συγκεκριμένα πιστοποιητικά. Λόγω της γενικής αποδοχής του, όμως θα λέγαμε ότι είναι και ο μοναδικός ορισμός για την πολιτική πιστοποίησης, όποιος και αν είναι ο τύπος των χρησιμοποιούμενων πιστοποιητικών. Ο συγκεκριμένος ορισμός λοιπόν ο οποίος έχει υιοθετηθεί και από την κοινότητα του διαδικτύου με το **[RFC 2527, 1999]** αναφέρει ότι:

> *'Πολιτική Πιστοποίησης είναι ένα προκαθορισμένο σύνολο κανόνων, οι οποίοι καθορίζουν την καταλληλότητα ενός πιστοποιητικού σε μία κοινότητα χρηστών ή / και κατηγορία εφαρμογών με κοινές απαιτήσεις ασφάλειας*'.

Με άλλα λόγια, η πολιτική πιστοποίησης δείχνει κατά πόσο ο χρήστης ενός πιστοποιητικού μπορεί να εμπιστευτεί την διαβεβαίωση της αρχής πιστοποίησης, ότι το δημόσιο κλειδί αντιστοιχεί όντως στην φυσική οντότητα που αναφέρεται.

Η πολιτική πιστοποίησης αναφέρεται στις απαιτήσεις που πρέπει να διαθέτουν οι πρακτικές οι οποίες ακολουθούνται στην έκδοση ενός πιστοποιητικού και σε όλες τις λειτουργίες / διαδικασίες μιας αρχής πιστοποίησης που σχετίζονται με αυτό και έχουν άμεση ή έμμεση επιρροή στην ασφάλεια του ή στην χρήση του γενικότερα. Έτσι περιέχει μεταξύ άλλων:

- Επιτρεπτή χρήση των πιστοποιητικών.

- Απαιτήσεις για την αυθεντικοποίηση των αντικειμένων.
- Απαιτήσεις των λειτουργικών διαδικασιών της αρχής πιστοποίησης.
- Απαιτήσεις αξιοπιστίας και ασφάλειας των χρησιμοποιούμενων συστημάτων.
- Υποχρεώσεις του υποκειμένου του πιστοποιητικού.
- Εγγυήσεις που τυχόν δίνει η αρχή πιστοποίησης.

3.2.1 Πιστοποιητικά και πολιτική πιστοποίησης.

Η πολιτική πιστοποίησης, παρ'ότι από την παραπάνω περιγραφή φαίνεται ότι είναι ένας μηχανισμός υψηλού επιπέδου, έχει άμεσο αντίκτυπο στις λεγόμενες τεχνικές λειτουργίες. Όπως προαναφέραμε το πιστοποιητικό X.509 από την τρίτη έκδοση του και μετά μπορεί να υποστηρίζει επεκτάσεις. Από τις πιο σημαντικές και ήδη προτυποποιημένες επεκτάσεις είναι αυτές που αφορούν την πολιτική πιστοποίησης. Όπως είδαμε για να θεωρείται ένα πιστοποιητικό αναγνωρισμένο σύμφωνα με το **[RFC 3039, 2001]**, πρέπει να περιέχει μία επέκταση, η οποία να αναφέρει την πολιτική πιστοποίησης που καλύπτει το συγκεκριμένο πιστοποιητικό. Απαραίτητη για την συγκεκριμένη αναφορά είναι η κατοχύρωση και η απόδοση σε κάθε πολιτική πιστοποίησης ενός μοναδικού αναγνωριστή, όπως αυτοί που ισχύουν για τους τύπους ASN.1. Η επέκταση του πιστοποιητικού το οποίο θα εκδίδεται από την συγκεκριμένη πολιτική θα περιέχει ως τιμή τον συγκεκριμένο αναγνωριστή. Αν μία αρχή πιστοποίησης συμπεριλάβει σε ένα πιστοποιητικό της ένα κατοχυρωμένο αναγνωριστή πολιτικής πιστοποίησης, σημαίνει ότι πληροί όλες τις απαιτήσεις που ορίζονται σε αυτήν και ανάλογα με το νομικό πλαίσιο στο οποίο λειτουργεί πιθανώς να κληθεί να τις αποδείξει.

Ανάλογα με τον χαρακτηρισμό της συγκεκριμένης επέκτασης ως κρίσιμης ή μη κρίσιμης η χρήση του πιστοποιητικού αποκτά άλλο νόημα **[RFC 2527, 1999]**:

- Αν η επέκταση, η οποία δηλώνει την πολιτική πιστοποίησης έχει χαρακτηριστεί *ως μη-κρίσιμη*, τότε ο ρόλος των πολιτικών πιστοποίησης είναι ενδεικτικός. Με άλλα λόγια συνίσταται αλλά δεν επιβάλλεται η χρήση της συγκεκριμένης πολιτικής.
- Αν η συγκεκριμένη επέκταση έχει δηλωθεί ως *κρίσιμη*, τότε απαιτείται από την αρχή πιστοποίησης η χρήση του συγκεκριμένου πιστοποιητικού μόνο υπό την πολιτική η οποία αναφέρεται. Σε κάθε άλλη περίπτωση, η χρήση του πιστοποιητικού θα θεωρείται μη επιτρεπτή, και κατά συνέπεια η αρχή πιστοποίησης δεν θα φέρει ευθύνη για όποιες ζημιές.

Άλλες επεκτάσεις του πιστοποιητικού που έχουν σχέση με την πολιτική πιστοποίησης είναι:

- Η επέκταση περιορισμού πολιτικών πιστοποίησης *(Policy Constraints Extension)*: Θέτει απαραίτητη την ύπαρξη ενός συνόλου πολιτικών πιστοποίησης από όλες τις αρχές πιστοποίησης που συμμετέχουν σε ένα μονοπάτι πιστοποίησης για να είναι έγκυρο το πιστοποιητικό.
- Η επέκταση λεπτομερειών πολιτικής (*Policy Qualifier Extension)*: Εδώ μπορούν να ενσωματωθούν αναφορές (με ένα μηχανισμό by reference) για άλλα σημαντικά κείμενα τα οποία σχετίζονται με την

πολιτική πιστοποίησης, όπως για παράδειγμα η δήλωση πρακτικών πιστοποίησης, την οποία θα περιγράψουμε αργότερα. Τονίζουμε και τώρα ότι για την χρήση του παραπάνω μηχανισμού πρέπει να έχει προηγηθεί απόδοση μοναδικού αναγνωριστή στα παραπάνω κείμενα.

- Η επέκταση αντιστοίχισης πολιτικών (*Policy Mappings Extension*): Η συγκεκριμένη επέκταση υπάρχει μόνο σε πιστοποιητικά που εκδίδονται μεταξύ αρχών πιστοποίησης για διαπιστοποίηση. Χαρακτηρίζεται πάντα ως μη κρίσιμη και χρησιμοποιείται για να δείξει ποιες είναι οι ισοδύναμες πολιτικές πιστοποίησης μεταξύ των δύο αρχών.

3.2.2 Πολιτική Πιστοποίησης: Επαλήθευση και Μοντέλα Εμπιστοσύνης

Εύκολα καταλαβαίνουμε ότι η υλοποίηση της πολιτικής πιστοποίησης μέσω των επεκτάσεων θα έχει σημαντική επίδραση στην διαδικασία επαλήθευσης των ψηφιακών υπογραφών, καθώς πλέον δεν θα απαιτείται μόνο η ανάκτηση της λίστας ανάκλησης και ο έλεγχος για το αν περιέχει το συγκεκριμένο πιστοποιητικό, αλλά και η επαλήθευση ότι όλα τα πιστοποιητικά στο μονοπάτι πιστοποίησης έχουν εκδοθεί με βάση την ίδια ή 'ισοδύναμες' πολιτικές. Με πιο απλά λόγια δεν αρκεί να υπάρχει το μονοπάτι πιστοποίησης. Πρέπει να είναι και έγκυρο υπό ένα σύνολο πολιτικών πιστοποίησης. Αυτό δεν περιορίζεται μόνο σε ιεραρχικές υποδομές δημοσίου κλειδιού. Ισχύει και για άλλες όπως για παράδειγμα στο μοντέλο της γέφυρας, αλλά και στην γενική περίπτωση.

Για παράδειγμα, έστω ότι το πιστοποιητικό του υπογράφοντα καλύπτει μόνο ένα συγκεκριμένο τύπο συναλλαγών. Τι θα συμβεί, αν κατά την διαδικασία δημιουργίας του μονοπατιού πιστοποίησης, βρεθεί ένα πιστοποιητικό το οποίο δεν καλύπτει τον συγκεκριμένο τύπο συναλλαγών, ή για παράδειγμα είναι πιο αυστηρό, στο ύψος των ποσών που καλύπτει; Κατά συνέπεια γίνεται φανερή η ανάγκη, κατά την επαλήθευση μιας ψηφιακής υπογραφής, όχι μόνο για την εύρεση του μονοπατιού πιστοποίησης, αλλά και για την επαλήθευση της εγκυρότητας του. Το πώς θα γίνεται αυτό, εξαρτάται, από τα υπάρχοντα πρότυπα τόσο για την μορφή των πιστοποιητικών όσο και για την διαπιστοποίηση μεταξύ των ετερογενών αρχών πιστοποίησης.

Για την εύρεση του μονοπατιού πιστοποίησης σε ένα γενικευμένο μοντέλο εμπιστοσύνης απαιτείται μία από τις παρακάτω υπηρεσίες:

1. Η πρώτη δέχεται ως είσοδο το όνομα μιας αρχής πιστοποίησης και επιστρέφει όλα τα πιστοποιητικά που έχουν εκδωθεί γι' αυτήν από άλλες.
2. Η δεύτερη δέχεται ως είσοδο το όνομα μιας αρχής πιστοποίησης και επιστρέφει όλα τα πιστοποιητικά που αυτή έχει εκδώσει για άλλες..

Έχοντας έτσι ένα σημείο εμπιστοσύνης μπορούμε να βρούμε το μονοπάτι πιστοποίησης με κατάληξη αυτό ξεκινώντας από οποιοδήποτε πιστοποιητικό μας δωθεί.

Για την επαλήθευση του μονοπατιού πιστοποίησης που βρήκαμε πρέπει να ελεγχθούν τα εξής στοιχεία **[Ford, 2001]**:

1. Η ψηφιακή υπογραφή για κάθε ένα από τα πιστοποιητικά που ανήκουν σε αυτό.
2. Έλεγχος του ότι σε κάθε πιστοποιητικό ως υποκείμενο αναφέρεται η εκδούσα αρχή του επόμενου πιστοποιητικού στο μονοπάτι πιστοποίησης.
3. Έλεγχος της χρονικής περίοδος ισχύος κάθε πιστοποιητικού. Πρέπει να υπερκαλύπτει την χρονική περίοδο στην οποία υποθέτουμε ότι έγινε η υπογραφή.
4. Ανάκτηση της λίστας ανάκλησης για κάθε ένα πιστοποιητικό, για την συγκεκριμένη χρονική περίοδο.
5. Έλεγχος ότι οι απαιραίτητες πολιτικές πιστοποίησης περιέχονται στις προκαθορισμένες επεκτάσεις: Πρέπει δηλαδή οι πολιτικές που αποδέχεται ο χρήστης να περιέχονται μέσα στις επεκτάσεις περιορισμού έχοντας την κατάλληλη ένδειξη κρισιμότητας.
6. Έλεγχος των ονομάτων σε κάθε πιστοποιητικό. Μπορεί να υπάρχει απαίτηση ότι όλα τα ονόματα που αναφέρονται σε κάθε πιστοποιητικό πληρούν κάποιους περιορισμούς, όπως για παράδειγμα ότι ανήκουν στο ίδιο υποδένδρο του X.500, ανάλογα βέβαια και με το σχήμα ονοματοδοσίας.

3.3 Δήλωση Πρακτικών Πιστοποίησης

Η πολιτική πιστοποίησης συμπληρώνεται με την δήλωση πρακτικών πιστοποίησης (certification practice statement). Ο συγκεκριμένος όρος πρωτοχρησιμοποιήθηκε στις συστάσεις για τις ψηφιακές υπογραφές του συνδέσμου ABA **[ABA, 1996].** Ο ορισμός που δόθηκε εκεί είναι και ο πιο αποδεκτός:

Η δήλωση πρακτικών πιστοποίησης είναι μία λεπτομερής δήλωση των πρακτικών τις οποίες υιοθετεί μία αρχή πιστοποίησης κατά την έκδοση πιστοποιητικών.

Ενώ λοιπόν η πολιτική πιστοποίησης περιγράφει τους κανόνες που σχετίζονται με την πιστοποίηση και τις συνέπειες τους, η δήλωση των πρακτικών περιγράφει το πώς αυτοί υλοποιούνται, με δεδομένο το οργανωτικό και λειτουργικό περιβάλλον μιας αρχής πιστοποίησης. Η περιγραφή αυτή δεν αφορά μόνο την οντότητα που εκδίδει το συγκεκριμένο κείμενο, αλλά και όλες τις οντότητες οι οποίες ανήκουν στην υποδομή δημοσίου κλειδιού.

Η δομή των παραπάνω κειμένων έχει προτυποποιηθεί με το **[RFC 2527, 1999]**. Τα περιεχόμενα της είναι τα εξής:

1. Εισαγωγή

Στην αρχική αυτή ενότητα γίνεται μία γενική εισαγωγή στους τύπους εφαρμογών και στις περιπτώσεις γενικότερα στις οποίες απευθύνεται η συγκεκριμένη δήλωση πρακτικών πιστοποίησης. Επίσης γίνεται μία αφαιρετική αναφορά στην υπάρχουσα υποδομή δημοσίου κλειδιού και ποιες απαιτήσεις πρέπει να έχει μία υπάρχουσα αρχή πιστοποίησης για να ενταχθεί σε αυτήν. Επίσης στην εισαγωγή τίθενται γενικοί όροι για την χρήση του πιστοποιητικού. Επίσης μπορεί να γίνει αναφορά στον νομικό πλαίσιο το οποίο καλύπτει τις ηλεκτρονικές υπογραφές που επαληθεύονται με το συγκεκριμένο πιστοποιητικό.

2. Γενικές Διατάξεις

Η ενότητα αυτή της δήλωσης πρακτικών πιστοποίησης θα μπορούσε να χαρακτηριστεί ως η πιο σημαντική. Παρέχει διατάξεις οι οποίες αναφέρονται σε ένα σύνολο σημαντικών θεμάτων, μη τεχνικής φύσεως. Εδώ, για παράδειγμα αναφέρονται όλες οι υποχρεώσεις της αρχής πιστοποίησης προς τους χρήστες, είτε αυτοί υπογράφουν είτε αυτοί επαληθεύουν. Επίσης αναφέρονται οι υποχρεώσεις και τα δικαιώματα των υποκειμένων των πιστοποιητικών. Μπορούν να συμπεριληφθούν και οι εγγυήσεις που παρέχει η αρχή, για ποια θέματα μπορεί να θεωρηθεί υπεύθυνη (και σε ποια δεν μπορεί). Ακόμα μπορεί να δηλώσει από ποιο νομικό καθεστώς καλύπτονται οι υποχρεώσεις της. Επίσης πιθανότατα, μπορεί να αναφέρει ποια μέτρα λαμβάνει για την τήρηση του αρχείου με τα προσωπικά δεδομένα που παρέχουν οι χρήστες κατά την εγγραφή τους.

3. Αναγνώριση και Αυθεντικοποίηση

Εδώ περιγράφεται κυρίως η διαδικασία με την οποία επαληθεύεται η ταυτότητα της οντότητας, η οποία κάνει αίτηση για το πιστοποιητικό. Αναφέρονται ακόμα και στοιχεία για την ονοματολογία που χρησιμοποιείται για την αναπαράσταση των οντοτήτων.

4. Λειτουργικές Απαιτήσεις

Στην συγκεκριμένη ενότητα περιγράφονται για όλες τις υπηρεσίες μιας αρχής πιστοποίησης, οι απαιτήσεις, που τίθενται από την πολιτική πιστοποίησης και ο τρόπος με τον οποίο αυτές υλοποιούνται. Για παράδειγμα περιγράφεται ο τρόπος έκδοσης πιστοποιητικών, οι διαδικασίες ανάκλησης, η τήρηση αρχείων, αλλά και η διαδικασία που θα ακολουθηθεί σε περίπτωση τερματισμού της λειτουργίας της αρχής.

5. Μηχανισμοί Ασφαλείας για το προσωπικό, τις διαδικασίες και την φυσική ασφάλεια.

Εδώ περιγράφονται τα μέτρα ασφάλειας που λαμβάνονται για την αξιοπιστία όλων των συστημάτων και υπηρεσιών της αρχής πιστοποίησης,

6. Τεχνικοί Μηχανισμοί Ασφάλειας

Στην ενότητα αυτή περιγράφονται όλοι οι μηχανισμοί που χρησιμοποιούνται για την προστασία των κλειδιών των χρηστών αλλά και της ίδιας της αρχής. Αναφέρονται έτσι οι διαδικασίες εκείνες, οι οποίες που χρησιμοποιούνται για την παραγωγή κλειδιών αν κάτι τέτοιο υφίσταται. Στο συγκεκριμένο σημείο δεν αναφέρονται μόνο απαιτήσεις σχετικά με τον πάροχο πιστοποίησης αλλά και απαιτήσεις για τους ίδιους τους χρήστες και ποια μέτρα θα πρέπει να λαμβάνουν οι ίδιοι για την προστασία των κλειδιών τους.

7. Περιεχόμενα Πιστοποιητικών και Λίστας Ανάκλησης

Η ενότητα αυτή θα περιγράφει αναλυτικά την ακριβή μορφή που έχουν τα πιστοποιητικά και οι λίστες ανάκλησης που χρησιμοποιεί η συγκεκριμένη αρχή πιστοποίησης. Αναφέρονται τυχόν πρότυπα που χρησιμοποιούνται, αλλά και ποια προαιρετικά στοιχεία των προτύπων αυτών ισχύουν. Έτσι για παράδειγμα στην συγκεκριμένη ενότητα θα αναφερθούν και στην περίπτωση του X.509 ποιες επεκτάσεις του όντως χρησιμοποιούνται στην πράξη.

8. Διαχείριση Αλλαγών.

Η συγκεκριμένη ενότητα περιγράφει την διαδικασία που θα εφαρμόζεται σε περίπτωση που υπάρχουν αλλαγές σε κάποια από τα περιεχόμενα του κειμένου που προαναφέραμε και βέβαια στα στοιχεία της

υποδομής δημοσίου κλειδιού που τα συνοδεύουν. Περιγράφεται για παράδειγμα πώς θα ενημερωθούν οι χρήστες και οι άλλες αρχές πιστοποίησης που έχουν συνάψει σχέσεις με αυτή.

Ένα τυπικό παράδειγμα δήλωσης πρακτικών πιστοποίησης αποτελεί το **[Verisign, 1997].** Αν θέλαμε να κάνουμε ένα σχόλιο πάνω σε αυτό, αρκεί να αναφέρουμε ότι αρνείται κάθε ευθύνη για οποιεσδήποτε ζημιές προκύψουν από ανακρίβειες στα πιστοποιητικά που εκδίδει. Το συγκεκριμένο θέμα θα αναλυθεί σε βάθος αργότερα στην εργασία.

3.4 Πολιτική Υπογραφής

Η πολιτική υπογραφής, προσθέτει ένα περιβάλλον στην διαδικασία δημιουργίας υπογραφής, με τον ίδιο τρόπο που η πολιτική πιστοποίησης, προσθέτει ένα περιβάλλον (context) και δίνει νόημα στην διαδικασία πιστοποίησης. Η πολιτική υπογραφής μπορεί να οριστεί ως *ένα σύνολο κανόνων για την δημιουργία και επαλήθευση μιας υπογραφής, οι οποίοι καθορίζουν την ισχύ της* **[ETSI, 101 733].** Τόσο ο υπογράφων όσο και ο επαληθεύων χρησιμοποιούν την ίδια πολιτική υπογραφής. Τυπικά ο επαληθεύων την ορίζει και ο υπογράφων την επιλέγει, όταν πρόκειται να υπογράψει. Η πολιτική υπογραφής μπορεί να έχει οριστεί και από έναν 'κοινό παρανομαστή' που συνδέει τον υπογράφοντα με τον επαληθεύοντα, όπως για παράδειγμα ένα εμπορικό επιμελητήριο. Οι υπογραφές που θα παράγονται με την συγκεκριμένη πολιτική θα έχουν νόημα, μόνο για τα μέλη του επιμελητηρίου και όχι για οποιαδήποτε εξωτερική οντότητα.

Ο μηχανισμός για την δημοσίευση της πολιτικής υπογραφής είναι παρόμοιος με τον μηχανισμό δημοσίευσης της πολιτικής πιστοποίησης που προαναφέραμε. Έτσι, κάθε πολιτική υπογραφής παριστάνεται όπως ένας τύπος ASN.1, και έχει ένα μοναδικό αναγνωριστή. Ο αναγνωριστής της συγκεκριμένης πολιτικής υπογραφής πρέπει να περιέχεται στα δεδομένα στα οποία εφαρμόζεται ο κρυπτογραφικός μηχανισμός της υπογραφής, που περιγράψαμε στο κεφάλαιο 2. Με τον τρόπο αυτό δηλώνεται η αποδοχή της συγκεκριμένης πολιτικής. Επιπλέον, μπορεί να αναφέρεται ρητά στα δεδομένα τα οποία υπογράφονται. Όπως και η πολιτική πιστοποίησης, έτσι και η πολιτική υπογραφής πρέπει να είναι διαθέσιμη σε αναγνώσιμη μορφή, ώστε ο υπογράφων να γνωρίζει το πλαίσιο το οποίο καλύπτει την υπογραφή του. Επιπλέον όμως πρέπει να είναι και σε μορφή κατανοητή από τον υπολογιστή για την δημιουργία και επαλήθευση της υπογραφής. Οι κανόνες, αυτοί είναι γνωστοί και ως κανόνες επαλήθευσης της υπογραφής ή πολιτική επαλήθευσης της υπογραφής, καθώς επιτρέπουν σε ανεξάρτητους παρατηρητές να επαληθεύσουν μία ηλεκτρονική υπογραφή και να καταλήξουν στο ίδιο αποτέλεσμα.

Πιο συγκεκριμένα τώρα μία πολιτική υπογραφής περιέχει τα εξής στοιχεία **[ETSI, 101 733].**:

- *Μοναδικό αναγνωριστή:* Ο αναγνωριστής ο οποίος σχηματίζεται όπως προαναφέραμε και μπορεί να προσδιορίσει την πολιτική υπογραφής.
- *Όνομα εκδούσας αρχής.*
- *Ημερομηνία Έκδοσης.*
- *Πεδίο Εφαρμογής* .Το νομικό / συμβατικό πεδίο εφαρμογής στο οποίο θα χρησιμοποιηθεί η

συγκεκριμένη πολιτική.

- Πολιτική Επαλήθευσης Υπογραφής
    - *Περίοδος Υπογραφής:* Οι ημερομηνίες μεταξύ των οποίων ισχύει η συγκεκριμένη πολιτική για την δημιουργία και επαλήθευση υπογραφών.
    - *Σύνολο αναγνωρισμένων τύπων δέσμευσης:* Ένας τύπος δέσμευσης περιγράφει τις συνέπειες χρήσης μίας υπογραφής.
    - *Κανόνες Χρήσης Παρόχων Πιστοποίησης*: Οι συγκεκριμένοι κανόνες περιγράφουν το πώς θα χρησιμοποιηθούν τα διάφορα σημεία εμπιστοσύνης και θέτουν περιορισμούς στον σχηματισμό του μονοπατιού εμπιστοσύνης. Οι περιορισμοί αυτοί εξαρτώνται και από την πολιτική πιστοποίησης όλων των ενδιάμεσων πολιτικών πιστοποίησης.
    - *Κανόνες Χρήσης Πληροφορίας Ανάκλησης:* Καθορίζουν τον τρόπο χρήση μιας λίστας ανάκλησης ή πληροφορίας OCSP.
    - *Κανόνες για την χρήση ρόλων:* Αφορούν τα πιστοποιητικά ιδιοτήτων και ρυθμίζουν τον τρόπο χρήσης τους.
    - *Κανόνες Αποδοχής Χρονοσήμανσης - Χρόνου:* Εδώ ορίζονται ορισμένες παράμετροι χρόνου. Για παράδειγμα, ορίζεται το μέγιστο χρονικό διάστημα μέσα στο οποίο πρέπει να υπάρξει χρονοσήμανση μιας υπογραφής. Επίσης, μπορεί να οριστεί το μέγιστο αποδεκτό χρονικό διάστημα μεταξύ παραβίασης ιδιωτικού κλειδιού και ανάκλησης του πιστοποιητικού.
    - *Απαραίτητα Δεδομένα Επαλήθευσης:* Καθορίζει επιπλέον δεδομένα από τα κλασικά που μπορούν να χρησιμοποιηθούν και ποιος (υπογράφων / επαληθεύων) θα τα παρέχει.
    - *Περιορισμοί σε αλγόριθμους και μήκη κλειδιών*: Αφορούν τόσο τις διαδικασίες υπογραφής, όσο και τις διαδικασίες πιστοποίησης σε όλο το μονοπάτι εμπιστοσύνης.

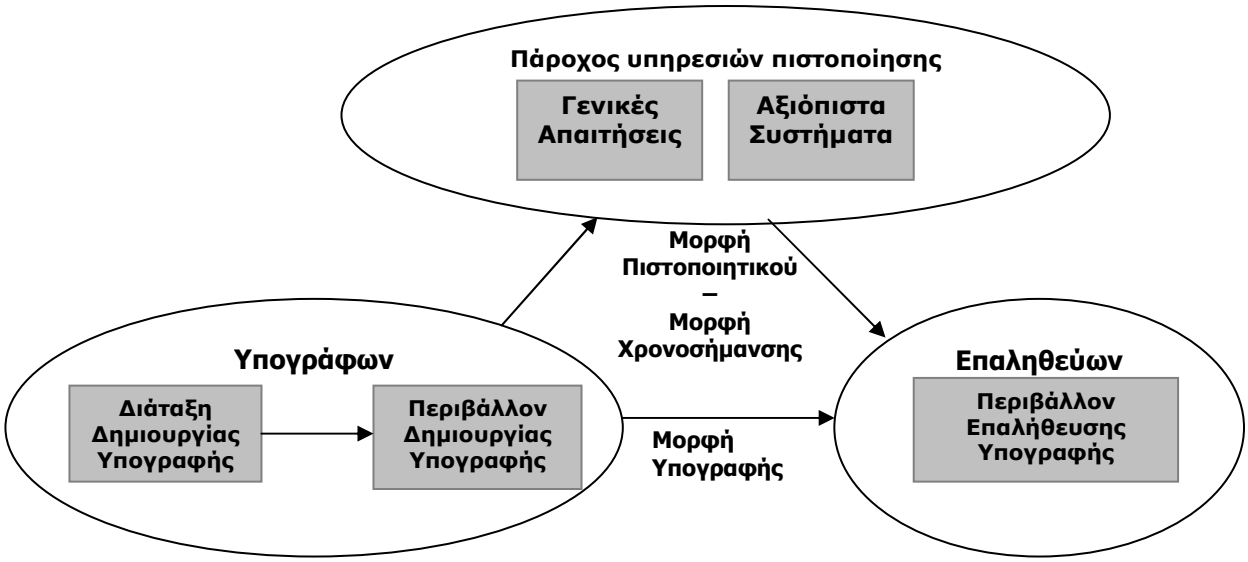
3.5 Πρότυπα για Υπηρεσίες Ηλεκτρονικών Υπογραφών

Η δήλωση πρακτικών πιστοποίησης και η πολιτική πιστοποίησης ρύθμιζαν τις σχέσεις σε ένα περιβάλλον ηλεκτρονικών υπογραφών, όταν απουσίαζε ένα κανονιστικό πλαίσιο με αυτόν ακριβώς το στόχο. Σήμερα, τέτοια πλαίσια έχουν ήδη εμφανιστεί, και έχουν διπλό στόχο. Να βοηθήσουν την ευρείας κλίμακας ανάπτυξη και χρήση όλων των συστημάτων και προϊόντων που σχετίζονται με ηλεκτρονικές υπογραφές και αφετέρου να εξασφαλίσουν ένα αποδεκτό επίπεδο ποιότητας και ασφάλειας για τα παραπάνω συστήματα. Αυτό επιτυγχάνεται με την προτυποποίηση των απαραίτητων στοιχείων και συγκεκριμένα με δύο τρόπους: Ο πρώτος θέλει την χρήση ήδη διαθέσιμων προτύπων για την υποστήριξη των πλαισίων, ενώ ο δεύτερος τα θέλει να συνοδεύονται και με μια ευρείας σε έκταση, δραστηριότητα προτυποποίησης, κατά την οποία δεν δημιουργούνται κατ' ανάγκη καινούρια πρότυπα, αλλά τουλάχιστον επικυρώνονται ή επεκτείνονται ήδη διαθέσιμα πρότυπα.

Πιο συγκεκριμένα η προτυποποίηση στον συγκεκριμένο χώρο εξυπηρετεί τους εξής σκοπούς:

- *Συμβατότητα των τεχνολογιών που χρησιμοποιούνται*. Η προτυποποίηση εδώ εφαρμόζεται είτε στην μορφή των ανταλλασσόμενων μηνυμάτων (υπογραφών, πιστοποιητικών) είτε στους διάφορους αλγόριθμους που χρησιμοποιούνται, όπως άλλωστε είδαμε και στο προηγούμενο κεφάλαιο. Απώτερος στόχος εδώ είναι η επίτευξη της συνεργασίας μεταξύ εφαρμογών που προέρχονται από διαφορετικούς κατασκευαστές, κάτι που κρίνεται απαραίτητο σε περίπτωση που οι υπηρεσίες πιστοποίησης εφαρμοστούν σε ευρεία κλίμακα. Εδώ πρέπει να επισημάνουμε πώς οι τεχνολογίες ηλεκτρονικών υπογραφών πρέπει να είναι ανεξάρτητες από τα συστήματα που χρησιμοποιούνται για την δημιουργία και επαλήθευση τους. Πρέπει δηλαδή να είναι απόλυτα εφικτό, η υπογραφή να δημιουργείται από ένα κινητό τηλέφωνο, ενώ η επαλήθευση να γίνεται από έναν εξυπηρετητή μιας τράπεζας. Είναι φανερές λοιπόν οι μεγάλες απαιτήσεις για πρότυπα, σχετικά με την μορφή των ηλεκτρονικών υπογραφών.
- *Εξασφάλιση / Αξιολόγηση της ασφάλειας, της ποιότητας και της αξιοπιστίας των χρησιμοποιούμενων συστημάτων*. Εδώ πλέον αναφερόμαστε σε απαιτήσεις πληροφοριακών συστημάτων και κατά συνέπεια, εμπλέκονται εκτός από τεχνικές, λειτουργικές, οργανωτικές και διοικητικές παράμετροι.

Τα πρότυπα που έχουν σχέση με τις υπηρεσίες ηλεκτρονικών υπογραφών, φαίνονται στο παρακάτω σχήμα **[PPEU,2001]**:



Σχήμα 9. Πρότυπα Συστημάτων Ηλεκτρονικών Υπογραφών

Η παραπάνω ταξινόμηση έχει ακολουθηθεί στην Ευρωπαϊκή Πρωτοβουλία Προτυποποίησης για Ηλεκτρονικές Υπογραφές (EESSI), η οποία στόχο έχει να βοηθήσει την υλοποίηση της οδηγίας. Θεωρούμε πώς είναι εφαρμόσιμη σε οποιοδήποτε πλαίσιο υπηρεσιών πιστοποίησης, και για τον λόγο αυτό θα την αναλύσουμε διεξοδικά. Εκτός όμως από τα πρότυπα που απορρέουν από αυτή, υπάρχει ένα σύνολο διεθνών και ιδιαίτερα καθιερωμένων προτύπων στο συγκεκριμένο πεδίο.

3.5.1 Αξιόπιστα Συστήματα

Η πρώτη κατηγορία προτύπων, που θα εξετάσουμε αφορά την χρήση αξιόπιστων συστημάτων. Τα πρότυπα που ανήκουν εδώ, αφορούν όλες τις οντότητες που σχετίζονται με ηλεκτρονικές υπογραφές, ιδιαίτερα όμως τους πάροχους υπηρεσιών πιστοποίησης, καθώς τα δικά τους συστήματα χειρίζονται κρίσιμα δεδομένα, όπως κρυπτογραφικά κλειδιά, πιστοποιητικά και λίστες ανάκλησης. Για παράδειγμα, τα συστήματα που χειρίζονται το κλειδί με το οποίο υπογράφει η αρχή πιστοποίησης τα πιστοποιητικά που εκδίδει πρέπει να ικανοποιούν αυστηρές απαιτήσεις ασφάλειας. Επίσης τα συστήματα με τα οποία λειτουργεί η υπηρεσία καταλόγου ανάκτησης των πιστοποιητικών, πρέπει να χαρακτηρίζονται από συνεχή διαθεσιμότητα (τουλάχιστον). Για την πιστοποίηση της αξιοπιστίας των συστημάτων μπορούν να χρησιμοποιηθούν τα κλασικά πρότυπα ασφάλειας TCSEC και ITSEC, αλλά και το νεώτερο Common Criteria το οποίο θα περιγράψουμε παρακάτω. Εξαρχής επισημαίνουμε, ότι στόχος της παρακάτω περιγραφής δεν είναι η πλήρης περιγραφή των παρακάτω προτύπων, αλλά η παράθεση βασικών στοιχείων τους, ώστε να μπορούν να γίνουν κατανοητές οι απαιτήσεις που τίθενται με βάση αυτά, σε ένα περιβάλλον ηλεκτρονικών υπογραφών.

3.5.1.1 TCSEC

Το πρότυπο **TCSEC** (**Trusted Computer System Evaluation Criteria** - ευρύτερα γνωστό και ως Orange Book - είναι ίσως το πιο διαδεδομένο πρότυπο ασφάλειας υπολογιστικών συστημάτων και σίγουρα το πρώτο πρότυπο που έτυχε τόσης αποδοχής. Η πρώτη έκδοση του έγινε το 1983, ενώ ευρύτατης διάδοσης στάθηκε η δεύτερη έκδοση του 1985. Ο υπεύθυνος φορέας για την ανάπτυξη του ήταν το Υπουργείο Εθνικής Άμυνας των ΗΠΑ. Απευθύνεται κυρίως σε λειτουργικά συστήματα ή κατά την ορολογία του σε αυτοματοποιημένα συστήματα προστασίας δεδομένων (ADP - Automated Data Processing Systems), τα οποία κατατάσσονται σε τέσσερις υποδιαιρέσεις (divisions) (στην πραγματικότητα σε 7 κλάσεις) ανάλογα με τα χαρακτηριστικά τους στους παρακάτω τομείς:

- **Πολιτική Ασφαλείας (Security Policy),** όπου εξετάζεται η ύπαρξη και η εφαρμογή μίας καλά ορισμένης πολιτικής ασφαλείας. Η έννοια της πολιτικής ασφάλειας ορίζεται στο **[Gritzalis, 1998b]** ως ένα σύνολο κριτηρίων για την παροχή υπηρεσιών ασφάλειας. Υλοποιείται με μία σειρά διαδικασιών καθημερινής εφαρμογής, μια σειρά διαδικασιών έκτακτης ανάγκης και ένα σύνολο κειμένων τεκμηρίωσης.
- **Ελεγξιμότητα (Accountability),** όπου εξετάζεται το κατά πόσο υπάρχει ένας μηχανισμός αναγνώρισης των χρηστών του συστήματος και καταγραφής των ενεργειών τους, έτσι ώστε να είναι δυνατός ο εντοπισμός του υπεύθυνου σε περίπτωση που κάτι δεν πάει όπως ήταν αναμενόμενο.
- **Διαβεβαίωση (Assurance),** όπου εξετάζεται το κατά πόσο σωστά εφαρμόζονται οι απαιτήσεις ασφαλείας από τα συστατικά υλικού και λογισμικού που αποτελούν το σύστημα.
- **Τεκμηρίωση (Documentation),** όπου εξετάζεται η πληρότητα της τεκμηρίωσης που συνοδεύει το

σύστημα συνολικά και τα επιπλέον χαρακτηριστικά του.

Με βάση τις επιδόσεις του στα παραπάνω χαρακτηριστικά ασφαλείας ένα υπολογιστικό σύστημα και πιο συγκεκριμένα το υποσύστημα του το οποίο ασχολείται με την ασφάλεια (Trusted Computer Base – TCB), κατατάσσεται στις εξής κλάσεις:

1. **Κλάση D: Ελάχιστη προστασία (Minimum Protection).**

Στην συγκεκριμένη κλάση κατατάσσονται όσα υπολογιστικά συστήματα παρέχουν στοιχειώδη ή καμία ασφάλεια και έχουν αποτύχει να ενταχθούν σε κάποια ανώτερη κατηγορία. Τα συστήματα της κλάσης D δηλαδή έχουν αποτιμηθεί με αποτυχία.

2. **Κλάση C1: Προαιρετική Ασφάλεια (Discretionary Security Protection).**

Τα συστήματα τα οποία έχουν καταταγεί στην κλάση C1 παρέχουν κάποιο διαχωρισμό των δεδομένων των χρηστών, έτσι ώστε να μην είναι δυνατή η τυχαία ή εσκεμμένη διαγραφή / τροποποίηση των δεδομένων ενός χρήστη από κάποιον άλλο. Κατά συνέπεια πρέπει να υπάρχουν μηχανισμοί για την εφαρμογή περιορισμών πρόσβασης σε κάθε μεμονωμένο χρήστη ή ομάδα χρηστών. Για την εφαρμογή των συγκεκριμένων μηχανισμών απαιτείται η χρήση μηχανισμού αυθεντικοποίησης. Οι απαιτήσεις τεκμηρίωσης προσανατολίζονται κυρίως στους χρήστες του συστήματος και λιγότερο στον σχεδιασμό και στον έλεγχο του.

3. **Κλάση C2: Προστασία Ελεγχόμενης Πρόσβασης (Controlled Access Protection).**

Η κλάση C2 εγγυάται παρόμοιους μηχανισμούς διαχωρισμού των δεδομένων των χρηστών με την κλάση C1, προσθέτοντας ένα επιπλέον επίπεδο ελεγξιμότητας με μηχανισμούς καταγραφής (auditing) των σημαντικών γεγονότων. Για τους συγκεκριμένους μηχανισμούς υπάρχει προστασία από μη εξουσιοδοτημένους χρήστες. Επιπλέον υπάρχει περιορισμός σε ότι αφορά τους μηχανισμούς διάδοσης προνομίων των χρηστών. Κάθε αντικείμενο συμπεριλαμβάνεται στον έλεγχο πρόσβασης. Θέτει επίσης απαιτήσεις που πρέπει να ισχύουν κατά την επαναχρησιμοποίηση αντικειμένων.

4. **Κλάση B1: Διαβαθμισμένη Προστασία (Labelled Security Protection).**

Τα υπολογιστικά συστήματα τα οποία κατατάσσονται στην συγκεκριμένη ομάδα διαθέτουν υποχρεωτικό έλεγχο προσπέλασης (**Mandatory Access Control – MAC**), όπου τα διάφορα υποκείμενα (χρήστες) και αντικείμενα (πόροι) έχουν χαρακτηριστεί κατάλληλα (labels). Ανάλογα με αυτή την διαβάθμιση γίνεται και ο έλεγχος προσπέλασης.

5. **Κλάση B2: Δομημένη Προστασία (Structured Protection).**

Τα υπολογιστικά συστήματα της συγκεκριμένης κατηγορίας παρέχουν τόσο προαιρετικό προσπέλασης (**Discretionary Access Control - DAC**) όσο και υποχρεωτικό (MAC). Το σύστημα παρέχει επίσης και λειτουργίες αυτοπροστασίας (για παράδειγμα από μεταβολές κώδικα).

6. **Κλάση B3: Περιοχές Ασφαλείας (Security Domains).**

Τα υπολογιστικά συστήματα τα οποία εντάσσονται στην συγκεκριμένη κατηγορία πρέπει να βασίζονται σε ένα ολοκληρωμένο, θεμελιωμένο και εννοιολογικά απλό μοντέλο. Πρέπει να παρέχουν οπωσδήποτε ένα συστατικό επόπτη (reference monitor) το οποίο θα αντιμετωπίζει τις αιτήσεις των χρηστών

για προσπέλαση. Επίσης κατά την αξιολόγηση τους πρέπει να ανθίστανται σε προσπάθειες διείσδυσης εξειδικευμένων ομάδων (penetration testing).

7. **Κλάση A: Επαληθευμένη Προστασία (Verified Protection).**

Τα υπολογιστικά συστήματα τα οποία εντάσσονται στην συγκεκριμένη κατηγορία είναι λειτουργικά ισοδύναμα με αυτά της κλάσης B3. Η ουσιαστική διαφορά είναι ότι η ανάλυση των προδιαγραφών τους γίνεται με κάποια αυστηρή και τυπική (formal) μέθοδο. Αντίστοιχη αυστηρότητα απαιτείται και στην διαδικασία της τεκμηρίωσης.

3.5.1.2 ITSEC (Information Technology Security Evaluation Criteria)

Το συγκεκριμένο πρότυπο αποτέλεσε την απάντηση της Ευρώπης στο TCSEC (1991). Δυστυχώς όμως δεν προχώρησε παραπέρα καθώς η πρακτική εφαρμογή του δεν ήταν πολύ μεγάλη.

Το πρότυπο αυτό είναι το πρώτο το οποίο διαχωρίζει σαφώς την λειτουργικότητα από την διαβεβαίωση (μια ιδέα που ακολουθήθηκε και στο Common Criteria, όπως θα δούμε σε λίγο). Σε ότι αφορά την λειτουργικότητα χρησιμοποιεί 9 κλάσεις. Οι 5 από αυτές αντιστοιχούν στις κλάσεις του TCSEC (F-B1, F-B2, F-B3, F-C1, F-C2), ενώ οι υπόλοιπες αφορούν τομείς ασφάλειας όπως η ακεραιότητα δεδομένων (F-IN), η διαθεσιμότητα (F-AV), η εμπιστευτικότητα (F-DC) και συνδυασμό εμπιστευτικότητας – ακεραιότητας (F- DX).

Σε ότι αφορά την διαβεβαίωση ασφάλειας κατατάσσει τον στόχο αξιολόγησης σε 7 επίπεδα από το E0 έως το E6 με αυξανόμενες εγγυήσεις. Κάθε προϊόν προς αξιολόγηση ισχυρίζεται ότι πρέπει να ενταχθεί σε ένα από τα επτά αυτά επίπεδα και το αποτέλεσμα της αξιολόγησης επιβεβαιώνει ή καταρρίπτει τον συγκεκριμένο ισχυρισμό. Το συγκεκριμένο πρότυπο συνοδεύεται και από μία μεθοδολογία αποτίμησης (ITSEM - **I**nformation **T**echnology **S**ecurity **E**valuation **M**ethodology).

Τα επτά επίπεδα του ITSEC είναι τα εξής **[ITSEC, 1991]:**

1. **E0:** Το σύστημα παρέχει μη επαρκή διαβεβαίωση. Ισοδύναμο με την κλάση D του TCSEC.
2. **E1:** Στο συγκεκριμένο επίπεδο το σύστημα έχει θέσει ένα στόχο ασφαλείας και υπάρχει μη τυπική περιγραφή του αρχιτεκτονικού σχεδιασμού του. Η απόδειξη του ότι ο στόχος ασφαλείας ικανοποιείται γίνεται με λειτουργικό τρόπο και προαιρετικά.
3. **E2:** Εκτός από το E1, περιέχεται και μία λεπτομερής περιγραφή της λεπτομερούς σχεδίασης. Υπάρχει αποτίμηση των αποτελεσμάτων του λειτουργικού ελέγχου και σύστημα ελέγχου διαμόρφωσης (configuration control system)
4. **E3:** Επιπλέον ελέγχεται ο πηγαίος κώδικας και τα σχεδιαγράμματα του υλικού καθώς επίσης και αποτελέσματα δοκιμών.
5. **E4:** Επιπλέον υπάρχει τυπικός καθορισμός της πολιτικής ασφάλειας για την επίτευξη του στόχου ασφαλείας. Ο αρχιτεκτονικός και λεπτομερής σχεδιασμός, πρέπει να προσδιοριστεί με ημι-τυπικό τρόπο.

6. **E5:** Επιπλέον υπάρχει στενή σχέση μεταξύ πηγαίου κώδικα / υλικού με την λεπτομερή σχεδίαση.
7. **E6:** Επιπλέον υπάρχει τυπική περιγραφή του αρχιτεκτονικού σχεδιασμού και των λειτουργιών ασφάλειας σε συνάρτηση με το τυπικό μοντέλο της πολιτικής ασφάλειας.

Αξίζει πάντως να σημειώσουμε ότι εννοιολογικά τα συγκεκριμένο πρότυπο ήταν πιο 'μπροστά' από το αντίστοιχο αμερικάνικο, καθώς δεν αφορά μόνο υπολογιστικά συστήματα αλλά αφορά γενικότερα πληροφοριακά συστήματα.

3.5.1.3 Common Criteria

Το πρότυπο Common Criteria αποτελεί την πρώτη προσπάθεια ενός προτύπου ασφάλειας πληροφοριακών συστημάτων και προϊόντων λογισμικού που θα είναι αποδεκτό σε παγκόσμια κλίμακα. Η ανάπτυξη του έγινε (και εξακολουθεί να γίνεται) από ένα σύνολο οργανισμών από όλες τις προηγμένες χώρες – ΗΠΑ, Μεγάλη Βρετανία, Καναδάς, Γερμανία, Γαλλία, Ολλανδία. Ξεκίνησε το 1993, ως μία προσπάθεια γεφύρωσης του χάσματος που υπήρχε με την έκδοση των τριών μέχρι τότε χρησιμοποιούμενων προτύπων – του TCSEC και των λιγότερο επιτυχημένων ITSEC και CTCPEC (Καναδάς). Η πρώτη έκδοση του δημοσιεύθηκε το 1996, ενώ το 1998 υπήρξε και μία δεύτερη έκδοση. Το πρότυπο Common Criteria έχει εγκριθεί και από τον ISO (ISO 15408). Επειδή το συγκεκριμένο πρότυπο αποτελεί το μέλλον των προτύπων στην αποτίμηση της ασφάλειας που παρέχει ένα προϊόν ή πληροφοριακό σύστημα, κάτι που με την σειρά του είναι ένα ουσιώδες στοιχείο στην διαδικασία της διαπίστευσης, θα ασχοληθούμε με αυτό εκτενέστερα από τα προηγούμενα.

Τα βασικά χαρακτηριστικά του Common Criteria είναι τα εξής:

1. Παρέχει μία κοινή 'γλώσσα', για τον προσδιορισμό του *τι κάνει* και τι *δεν κάνει* ένα σύστημα.
2. Ορίζει, με βάση την κοινή γλώσσα αυτή, ένα σύνολο από λειτουργίες σχετιζόμενες με την ασφάλεια. Δεν είναι απαραίτητο όλες οι λειτουργίες που ορίζονται από το πρότυπο να υλοποιούνται από ένα προϊόν – πληροφοριακό σύστημα. Αντίθετα, κάθε προϊόν - πληροφοριακό σύστημα, επιλέγει και συνδυάζει τις προτεινόμενες λειτουργίες.
3. Μία μεθοδολογία αποτίμησης των απαιτήσεων για τις προκαθορισμένες απαιτήσεις ασφαλείας. Οι απαιτήσεις καθορίζονται με βάση τις απειλές που αντιμετωπίζει το σύστημα.

Οι απαιτήσεις που παρέχει ένα προϊόν / πληροφοριακό σύστημα σχετικά με την ασφάλεια χωρίζονται στο Common Criteria σε δύο κατηγορίες:

- **Λειτουργικές Απαιτήσεις (Functional Requirements)**: Ουσιαστικά περιγράφουν τις σχετικές με την ασφάλεια λειτουργίες του προϊόντος / πληροφοριακού συστήματος και το επίπεδο ασφαλείας που προσφέρουν.
- **Απαιτήσεις διαβεβαίωσης (Assurance Requirements)**: Επιβεβαιώνουν ότι οι λειτουργικές

απαιτήσεις όντως υλοποιούν αυτό που υπόσχονται.

Καταλαβαίνουμε λοιπόν ότι το Common Criteria παρέχει δύο πράγματα: αφ' ενός ένα τρόπο να περιγραφούν οι απαιτήσεις ασφαλείας για ένα σύστημα και αφ' ετέρου ένα τρόπο για να υπάρχει σιγουριά ότι οι απαιτήσεις ασφάλειας όντως ισχύουν (αποτίμηση). Για την ακριβή περιγραφή των παραπάνω το πρότυπο ορίζει τις εξής έννοιες:

- **Στόχος Αποτίμησης (Target Of Evaluation – TOE):** Είναι κάποιο τμήμα ή ολόκληρο το προϊόν ή πληροφοριακό σύστημα του οποίου η ασφάλεια αποτιμάται. Η αποτίμηση αφορά εξίσου το υλικό, το λογισμικό, αλλά και την τεκμηρίωση του συστήματος.
- **Προφίλ Προστασίας (Protection Profile - PP):** Είναι ένα σύνολο απαιτήσεων σχετικών με την ασφάλεια οι οποίες αφορούν κάποιο στόχο αποτίμησης. Οι απαιτήσεις αυτές έχουν ως στόχο την ικανοποίηση κάποιας ανάγκης,. Το σύνολο αυτό των απαιτήσεων είναι ανεξάρτητο από την όποια υλοποίηση τους. Θα μπορούσαμε ίσως να πούμε ότι εκφράζει τον ιδανικό στόχο αποτίμησης για μία συγκεκριμένη περιοχή εφαρμογής. Στην πρώτη έκδοση του προτύπου υπήρχαν παραδείγματα των προφίλ προστασίας για συστήματα βάσεων δεδομένων, λειτουργικά συστήματα, προγράμματα προστασίας δικτύων κτλ. Μαζί με τις απαιτήσεις το προφίλ προστασίας, ορίζει το περιβάλλον στο οποίο θα εφαρμοστούν οι συγκεκριμένες απαιτήσεις, ένα σύνολο από στόχους οι οποίοι θα οδηγήσουν στην επίτευξη των απαιτήσεων, και το σύνολο από μέτρα ασφαλείας τα οποία θα οδηγήσουν στην επίτευξη των παραπάνω στόχων.
- **Επιδίωξη Ασφαλείας (Security Target – ST):** Αποτελεί την βάση για την αποτίμηση της ασφάλειας ενός πληροφοριακού συστήματος: Ουσιαστικά είναι το προφίλ προστασίας ενός TOE, εξειδικευμένο για ένα συγκεκριμένο προϊόν, μαζί με μία καταγραφή των απειλών που αντιμετωπίζει και τους διάφορους στόχους ασφάλειας που έχουν τεθεί γι' αυτό αλλά και τα μέτρα που έχουν ληφθεί για την αντιμετώπιση όλων των παραπάνω. Η αποτίμηση γίνεται με τον στόχο αποτίμησης να δηλώνει ότι η επιδίωξη ασφαλείας του ταυτίζεται με κάποιο ή κάποια προφίλ ασφαλείας. Η αποτίμηση αποφαίνεται για το αν η παραπάνω πρόταση είναι αληθής ή όχι.

Ένα από τα πιο σημαντικά σημεία στο Common Criteria είναι η ονοματολογία που χρησιμοποιεί για τον καθορισμό των απαιτήσεων ασφαλείας και ο τρόπος οργάνωσης τους. Συγκεκριμένα μία απαίτηση ασφάλειας αναφέρεται στο πρότυπο ως ένα συστατικό ασφαλείας (security component). Τα διάφορα συστατικά οργανώνονται σε οικογένειες (families) αν διαθέτουν κάποιο κοινό στόχο ασφαλείας. Ομογενείς οικογένειες οργανώνονται σε κλάσεις (classes). Το κείμενο που ακολουθεί ίσως είναι υπερβολικά τεχνικό και λεπτομερές (παρ' όλο που είναι μία πολύ γενικού επιπέδου περιγραφή του προτύπου), μπορεί όμως να φανεί χρήσιμο ως μία αναφορά στις απαιτήσεις ασφάλειας που αναφέρονται σε πρότυπα που ακολουθούν (FIPS-140-2).

Κάθε κλάση ονομάζεται χρησιμοποιώντας τρεις χαρακτήρες (π.χ. **FAU**). Μία οικογένεια ονομάζεται με την παράθεση του ονόματος της κλάσης ακολουθούμενο από τον χαρακτήρα (_) και τρεις χαρακτήρες

για το όνομα της οικογένειας (π.χ. FAU_ARP). Τέλος τα διάφορα συστατικά μέσα στην οικογένεια καθορίζονται με την χρήση αριθμών. Μία από τις χρησιμότητες του συγκεκριμένου προτύπου είναι ότι ορίζει μία αποθήκη συστατικών με τα οποία μπορούν να κατασκευαστούν οι απαιτήσεις ασφάλειας για ένα στόχο αποτίμησης. Όλη η δεξαμενή αυτή ασφαλείας των συστατικών ασφαλείας περιγράφεται στο μέρος 2 του προτύπου. Η ταξινόμηση των μεμονωμένων συστατικών ασφαλείας είναι ιεραρχική, δηλαδή κάθε συστατικό ικανοποιεί όλες τις απαιτήσεις του προηγούμενου και ορίζει κάποιες επιπλέον.

Ενδεικτικά, οι κλάσεις ασφαλείας που ορίζονται στην δεύτερη έκδοση του προτύπου **[CC, 1998]** είναι οι εξής:

Λειτουργικές Κλάσεις	
FAU: Λειτουργίες Ελέγχου Ασφάλειας.	**FCO**: Λειτουργίες Επικοινωνιών.
FCS: Λειτουργίες Κρυπτογραφίας.	**FDP**: Λειτουργίες Προστασίας Δεδομένων.
FIA: Λειτουργίες Αυθεντικοποίησης.	**FMT**: Λειτουργίες Διαχείρισης Ασφάλειας.
FPR: Λειτουργίες Ιδιωτικότητας.	**FPT**: Προστασία των Λειτουργιών Ασφάλειας.
FRU: Χρησιμοποίηση Πόρων.	**FTA**: Λειτουργίες Πρόσβασης.
FTP: Ασφαλή Κανάλια.	
Κλάσεις Διαβεβαίωσης	
APE: Αποτίμηση Προφίλ Προστασίας.	**AGD:** Εγχειρίδια.
ASE: Αποτίμηση Στόχου Ασφαλείας.	**ALC:** Διαχείριση Κύκλου Ζωής.
ACM: Διαχείριση Διαμόρφωσης (Configuration Management).	**ATE :** Έλεγχος.
ADO : Εγκατάσταση και Λειτουργία. (Delivery and Operation).	**AVA:** Αποτίμηση Αδυναμιών.
ADV: Ανάπτυξη Συστήματος.	

Σχήμα 10. Κλάσεις Ασφαλείας για το Common Criteria.

Κάθε μία από τις παραπάνω κλάσεις ορίζει έναν αριθμό από οικογένειες, που απαρτίζονται με την σειρά τους από μία σειρά συστατικών. Η αναλυτική περιγραφή τους ξεφεύγει από τους σκοπούς της συγκεκριμένης εργασίας και μπορεί να αναζητηθεί στο ίδιο το πρότυπο Όπου στην συνέχεια του κειμένου κριθεί απαραίτητο, θα δίνεται μία περιγραφή της κλάσης ή του συστατικού που συναντάται.

Το πρότυπο αποτυπώνει το βαθμό στον οποίο ένα πρότυπο ικανοποιεί τις απαιτήσεις ασφαλείας του με χρήση 7 επιπέδων βεβαιότητας τα οποία ονομάζονται **EAL** (**Evaluation Assurance Levels**). Προφανώς κάθε προφίλ ασφαλείας συσχετίζεται και με ένα EAL. Και εδώ όπως και στα πρότυπα TCSEC και ITSEC η βεβαιότητα είναι επαυξητική, δηλαδή κάθε επίπεδο προϋποθέτει ότι ικανοποιούνται όλες οι απαιτήσεις που ορίζονται στο προηγούμενο επίπεδο. Οι επιπλέον απαιτήσεις που εισάγει κάθε επίπεδο προκύπτουν με την αντικατάσταση των συστατικών που απαρτίζουν τις διάφορες προδιαγραφές με ανώτερα (στην ιεραρχία) συστατικά της ίδιας οικογένειας ή / και με την προσθήκη νέων συστατικών από άλλες οικογένειες.
Τα επτά επίπεδα ασφαλείας και η αντιστοιχία τους με τα αυτά των TCSEC, ITSEC είναι τα εξής:

		TCSEC	ITSEC
		D	E0
EAL-1	Λειτουργικά Δοκιμασμένο	-	
EAL-2	Δομικά Δοκιμασμένο	C1	E1
EAL-3	Μεθοδικά Δοκιμασμένο και Ελεγμένο	C2	E2
EAL-4	Μεθοδικά Σχεδιασμένο, Δοκιμασμένο και Αξιολογημένο	B1	E3
EAL-5	Ημί-Τυπικά Σχεδιασμένο και Δοκιμασμένο	B2	E4
EAL-6	Ημί-Τυπικά Σχεδιασμένο, Επαληθευμένο και Δοκιμασμένο	B3	E5
EAL-7	Τυπικά Επαληθευμένος Σχεδιασμός και Έλεγχος	A	E6

Σχήμα 11. Common Criteria - ITSEC -TCSEC

Παρακάτω θα περιγράψουμε συνοπτικά κάθε επίπεδο διαβεβαίωσης:

EAL-1: Το συγκεκριμένο επίπεδο είναι αυτό στο οποίο παρέχονται οι λιγότερες εγγυήσεις. Στόχος του είναι να διαπιστώσει 'κραυγαλέα' και μόνο κενά ασφαλείας στο σύστημα χωρίς εξονυχιστικό έλεγχο. Εξετάζει τις λειτουργίες ασφάλειας του συστήματος με βάση μόνο την διεπαφή τους και χωρίς κανένα έλεγχο του γενικότερου σχεδιασμού του.

EAL-2: Και σε αυτό το επίπεδο ο έλεγχος που γίνεται στο σύστημα είναι κυρίως σε λειτουργικό επίπεδο. Στον έλεγχο χρησιμοποιείται επίσης και ο υψηλού επιπέδου σχεδιασμός του όλου συστήματος.

EAL-3: Στο επίπεδο αυτό επιβεβαιώνεται ουσιαστικά ότι οι διάφορες απαιτήσεις ασφάλειας έχουν εισαχθεί στο σύστημα από τα θεμέλια του – δηλαδή είναι ενσωματωμένες στον σχεδιασμό του.

EAL-4: Το συγκεκριμένο επίπεδο παρέχει ένα μέτριο επίπεδο ασφάλειας.

EAL-5: Το συγκεκριμένο επίπεδο παρέχει επιβεβαίωση ασφάλειας που γίνεται μόνο μετά από πλήρη έλεγχο της υλοποίησης ενός συγκεκριμένου προϊόντος. Οι λειτουργικές προδιαγραφές και η υψηλού επιπέδου σχεδίαση παρέχονται με ένα ημί - τυπικό τρόπο

EAL-6: Το επίπεδο 6 παρέχει ασφάλεια υψηλού επιπέδου η οποία έχει προκύψει από εφαρμογή εγγυημένων πρακτικών ασφαλείας και ένα συγκεκριμένο περιβάλλον ανάπτυξης. Αφορά εξειδικευμένα προϊόντα ασφαλείας για καταστάσεις υψηλού κινδύνου, οι οποίες δικαιολογούν το υψηλό κόστος ανάπτυξης που θα προκύψει με την εφαρμογή τόσο εξειδικευμένων τεχνικών ασφαλείας.

EAL-7: Το συγκεκριμένο επίπεδο διαβεβαιώνει ότι το TOE παρέχει ασφάλεια υψηλού επιπέδου για καταστάσεις ιδιαίτερα υψηλού κινδύνου. Απαιτείται η ύπαρξη ανάλυσης του με τυπικές μεθόδους.

Η διαδικασία αποτίμησης ενός TOE γίνεται σε τρία βήματα:

- Αρχικά έχουμε αποτίμηση της πρότασης ότι το προϊόν ανήκει σε ένα συγκεκριμένο προφίλ προστασίας.

- Έπειτα αποτιμάται ο στόχος ασφαλείας που έχει θέσει το TOE.
- Τέλος αποτιμάται η πρόταση ότι το TOE ικανοποιεί ένα στόχο ασφαλείας.

Από την παραπάνω περιγραφή καταλαβαίνουμε ότι το Common Criteria, παρέχει ένα πολύ ευέλικτο μηχανισμό με τον οποίο μπορούν να περιγραφεί και να αποτιμηθεί οποιοδήποτε προϊόν. Στο θέμα που εξετάζουμε στην συγκεκριμένη εργασία θα το Common Criteria, χρησιμεύει όπως θα δούμε σε 2 περιστάσεις:

- Στην διαμόρφωση ενός προφίλ προστασίας και των αντίστοιχων επιδιώξεων ασφαλείας για τις διατάξεις δημιουργίας υπογραφής (π.χ. έξυπνες κάρτες).
- Στην διαμόρφωση ενός προφίλ προστασίας και των αντίστοιχων επιδιώξεων ασφαλείας για τα προϊόντα και συστήματα υλικού και λογισμικού, τα οποία χρησιμοποιούνται από μία αρχή πιστοποίησης.

Βέβαια, τα παραπάνω στοιχεία δεν επαρκούν από μόνα τους για την αξιολόγηση ενός συστήματος ηλεκτρονικών υπογραφών, καθώς όπως έχει ήδη ξεκινήσει να διαφαίνεται αυτό αποτελείται και από πολλές μη τεχνικές πλευρές.

3.5.1.4 FIPS PUB 140-2: Security Requirements For Cryptographic Modules

Το συγκεκριμένο πρότυπο του NIST αφορά τα τεχνικά χαρακτηριστικά που πρέπει να έχουν κρυπτογραφικά συστήματα ασφαλείας, αλλά και τα τεχνικά και διαδικαστικά μέτρα τα οποία πρέπει να λάβουν οι οργανισμοί που τα χρησιμοποιούν για να προστατεύσουν ευαίσθητα ή / και σημαντικά δεδομένα. Διαφέρει δηλαδή από τα πρότυπα με τα οποία ασχοληθήκαμε νωρίτερα, τα οποία ασχολούνται γενικά με την αξιοπιστία προϊόντων και συστημάτων. Είναι το πιο αποδεκτό πρότυπο σε παγκόσμιο επίπεδο για την αξιολόηση κρυπτοσυσκευών.

Ορίζει κάποιες απαιτήσεις οι οποίες πρέπει να ικανοποιούνται από τέτοια κρυπτογραφικά συστήματα και με βάση το ποσοστό συμμόρφωσης *τα κατατάσσει σε 4 επίπεδα ασφαλείας* (Security Levels 1, 2, 3, 4). Οι απαιτήσεις που ορίζονται από το πρότυπο και πρέπει να ικανοποιούν οι κρυπτογραφικές μονάδες (cryptographic modules) αφορούν αρκετές περιοχές. Παρακάτω θα τις περιγράψουμε μαζί με τις προδιαγραφές που θέτει για κάθε ένα από τα επίπεδα ασφάλειας που ορίζει.

- **Προδιαγραφές Κρυπτογραφικών Μονάδων**

Η συγκεκριμένη περιοχή αφορά όλη την *τεκμηρίωση* που πρέπει να παρέχεται για την κρυπτογραφική μονάδα, από τον κατασκευαστή της. Η τεκμηρίωση αυτή περιλαμβάνει τα συστατικά υλικού και λογισμικού που απαρτίζουν την μονάδα, την ακριβή διάρθρωση τους, την διεπαφή τους με το περιβάλλον τόσο σε φυσικό (ports), όσο και λογικό επίπεδο (interfaces). Ο βαθμός λεπτομέρειας τους πρέπει να είναι σημαντικός καθώς ακόμα και τα ηλεκτρικά χαρακτηριστικά μιας τέτοιας μονάδας επηρεάζουν την ασφάλεια της. Επίσης πρέπει να αναφέρει και τις λειτουργίες ασφάλειας (κρυπτογράφηση, διαχείριση κλειδιών, αυθεντικοποίηση) που παρέχει αυτό.

- **Διεπαφή Κρυπτογραφικών Μονάδων**

Η περιοχή αυτή ορίζει την διεπαφή της κρυπτογραφικής μονάδας σε ότι αφορά την είσοδο και έξοδο πληροφορίας, είτε αυτή αφορά δεδομένα ελέγχου είτε δεδομένα για την υλοποίηση των κρυπτογραφικών λειτουργιών. Συγκεκριμένα ορίζεται ότι κάθε κρυπτογραφική μονάδα θα διαθέτει τις εξής λογικές διεπαφές και μόνο:

- είσοδο και έξοδο για δεδομένα
- είσοδο για πληροφορία ελέγχου
- έξοδο για πληροφορίες κατάστασης.

Στα επίπεδα ασφαλείας 1 και 2 επιτρέπεται να διαμοιράζεται (φυσικά) η διεπαφή που χρησιμοποιείται για δεδομένα ασφαλείας (κλειδιά, δεδομένα αυθεντικοποίησης κτλ.) με τις άλλες διεπαφές. Αντίθετα στα επίπεδα 3 και 4 οι διεπαφές πρέπει να διαχωρίζονται αυστηρά (είτε με φυσικό είτε με λογικό τρόπο).

- **Αυθεντικοποίηση, Ρόλοι και Υπηρεσίες.**

Κάθε κρυπτογραφική μονάδα θα πρέπει να υποστηρίζει διακριτούς ρόλους για τους χειριστές της και διαφορετικές υπηρεσίες για κάθε ρόλο. Η διαδικασία της αυθεντικοποίησης θα πρέπει να εξακριβώνει την ταυτότητα του κάθε χειριστή και να επαληθεύει ότι αυτός μπορεί να αναλάβει τον συγκεκριμένο ρόλο. Γενικά το πρότυπο καθορίζει τρεις ρόλους για κάθε χειριστή:

- Χρήστης: Ο συγκεκριμένος ρόλος θα εκτελεί τις γενικής φύσεως λειτουργίες ασφαλείας της μονάδας. Εννοούμε δηλαδή τις λειτουργίες για τις οποίες προορίζεται η συγκεκριμένη μονάδα.

- Υπεύθυνος Ασφαλείας: Ο συγκεκριμένος ρόλος θα εκτελεί τις λειτουργίες αρχικοποίησης της μονάδας, και τις εισαγωγής παραμέτρων.

- Υπεύθυνου Διαχείρισης: Ο συγκεκριμένος ρόλος θα εκτελεί τις λειτουργίες διαχείρισης (διαγνωστικούς ελέγχους). Η διαφορά με τον ρόλο του υπεύθυνου ασφαλείας είναι ότι στον πρώτο μπορούν να αποκαλύπτονται οι τιμές των παραμέτρων ασφαλείας, ενώ στον δεύτερο όχι.

Επίσης το πρότυπο καθορίζει ακριβώς ποιες υπηρεσίες θα υποστηρίζει μία κρυπτογραφική μονάδα. Πρέπει να υποστηρίζονται τουλάχιστον 3 υπηρεσίες:

- Ένδειξη Κατάστασης
- Αυτοέλεγχοι
- Λειτουργία Ασφαλείας.

Η κρυπτογραφική μονάδα μπορεί να παρέχει αυθεντικοποίηση είτε σε επίπεδο ρόλου είτε σε επίπεδο ταυτότητας ατόμου Στο πρότυπο αναφέρονται προδιαγραφές για την ισχύ των μηχανισμών αυθεντικοποίησης. Ενδεικτικά αναφέρουμε ότι για μία μεμονωμένη τυχαία προσπάθεια εισόδου η πιθανότητα επιτυχίας πρέπει να είναι το πολύ 10^{-6}, ενώ για επαναλαμβανόμενες προσπάθειες διάρκειας 1 λεπτού η πιθανότητα επιτυχίας ορίζεται σε 10^{-5}.

Στο επίπεδο ασφαλείας 1 το πρότυπο ορίζει ότι δεν είναι απαραίτητη η παροχή αυθεντικοποίησης. Στο επίπεδο ασφαλείας 2 ορίζεται ότι αρκεί να παρέχεται αυθεντικοποίηση ρόλου, ενώ στα επίπεδα

ασφαλείας 3 και 4 πρέπει να παρέχεται αυθεντικοποίηση ταυτότητας.

- **Μοντέλο Πεπερασμένων Καταστάσεων.**

Το πρότυπο απαιτεί για την κρυπτογραφική μονάδα να τεκμηριώσει όλες τις δυνατές καταστάσεις, στις οποίες είναι δυνατόν να περιέλθει αυτή, με ένα πεπερασμένο διάγραμμα καταστάσεων. Οι δυνατές καταστάσεις μίας κρυπτογραφικής μονάδας διακρίνονται σε:

  - Λειτουργικές.
  - Μεταβάσεις.
  - Γεγονότα Εισόδου.
  - Γεγονότα Εξόδου.

- **Φυσική Ασφάλεια**

Κάθε κρυπτογραφική μονάδα πρέπει να παρέχει φυσική ασφάλεια, έτσι ώστε να αποτρέπει την φυσική πρόσβαση στα περιεχόμενα της και μη εξουσιοδοτημένη χρήση της. Η φυσική ασφάλεια δεν αφορά κρυπτογραφικές μονάδες που είναι υλοποιημένες εξ' ολοκλήρου σε software. Στόχος της φυσικής ασφάλειας είναι αφενός η ανίχνευση μιας 'εισβολής' εκ των υστέρων (τουλάχιστον) ή και κατά την διάρκεια της 'εισβολής' οπότε θα πρέπει να ληφθούν μέτρα προστασίας από την ίδια την κρυπτογραφική μονάδα (για παράδειγμα μηδενισμός όλων ή μόνο των μη κρυπτογραφημένων περιεχομένων της).

Στο επίπεδο 1 απαιτείται ελάχιστη φυσική ασφάλεια. Στο επίπεδο 2 απαιτείται τουλάχιστον η ύπαρξη ενός μηχανισμού που θα δείξει εκ των υστέρων εάν η μονάδα έχει παραβιαστεί (tamper evidence). Στο επίπεδο 3 θεωρείται αναγκαία η ύπαρξη μηχανισμών ανίχνευσης (tamper detection) και αντίδρασης (tamper response) που θα καταστρέψουν τα ευαίσθητα δεδομένα της μονάδας σε περίπτωση παραβίασης. Τέλος στο επίπεδο 4 απαιτείται επιπλέον προστασία έναντι κατάρρευσης του λειτουργικού περιβάλλοντος της μονάδας.

- **Λειτουργικό Περιβάλλον**

Με τον όρο λειτουργικό περιβάλλον εννοούμε το τμήμα μιας κρυπτογραφικής μονάδας το οποίο είναι υπεύθυνο για την διαχείριση των τμημάτων υλικού και λογισμικού της. Προφανώς και το λειτουργικό σύστημα ανήκει στην συγκεκριμένη κατηγορία, όπως επίσης και οι διάφοροι μηχανισμοί που διαχωρίζουν την εξωτερική μονάδα από το περιβάλλον της. Το λειτουργικό περιβάλλον μιας κρυπτογραφικής μονάδας μπορεί να είναι είτε σταθερό είτε τροποποιήσιμο, γενικό είτε συγκεκριμένο.

Το πρότυπο ορίζει απαιτήσεις για το λειτουργικό περιβάλλον για κάθε ένα από τα επίπεδα ασφαλείας. Οι απαιτήσεις αυτές εκφράζονται πολλές φορές σε σχέση με γνωστά πρότυπα ασφάλειας όπως το πρότυπο Common Criteria.

- **Επίπεδο Ασφαλείας 1:**

Όπως είναι φυσικό οι προδιαγραφές που τίθενται στο συγκεκριμένο επίπεδο είναι οι πιο ελαστικές. Το πρότυπο προδιαγράφει απλά ότι δεν επιτρέπεται η ταυτόχρονη χρήση καθώς επίσης και η πρόσβαση από τις διάφορες διεργασίες στις διάφορες παραμέτρους λειτουργίας της μονάδας (π.χ. κλειδιά), όταν αυτές

είναι μη κρυπτογραφημένες. Επίσης αναφέρεται απλώς ότι το λειτουργικό πρέπει να προστατεύει τα περιεχόμενα της μονάδας από εξωτερική πρόσβαση. Τέλος η κρυπτογραφική μονάδα πρέπει να ενσωματώνει κάποιον μηχανισμό ακεραιότητας.

- **Επίπεδο Ασφαλείας 2:**

Στο συγκεκριμένο επίπεδο απαιτείται επιπλέον η ύπαρξη ενός λειτουργικού συστήματος το οποίο θα ικανοποιεί συγκεκριμένες λειτουργικές προδιαγραφές και θα έχει πιστοποιηθεί σύμφωνα με το πρότυπο Common Criteria σε επίπεδο EAL2. Επίσης το λειτουργικό σύστημα θα είναι επιφορτισμένο με τον καθορισμό και εφαρμογή των ρόλων που μπορούν να εκτελέσουν, να τροποποιήσουν και να διαβάσουν κρυπτογραφικές παραμέτρους. Επίσης το λειτουργικό σύστημα θα παρέχει μηχανισμό καταγραφής (audit) της πρόσβασης, εισαγωγής, διαγραφής και τροποποίησης των κρυπτογραφικών παραμέτρων της μονάδας.

- **Επίπεδο Ασφαλείας 3:**

Εκτός από τις προδιαγραφές των προηγούμενων επιπέδων το λειτουργικό περιβάλλον πρέπει να φέρει την πιστοποίηση κατά Common Criteria σε EAL3. Επίσης θα χρησιμοποιείται ένας ασφαλής μηχανισμός (trusted path) για την μετάδοση όλων των παραμέτρων του συστήματος. Οποιαδήποτε πρόσβαση στον ασφαλή αυτόν μηχανισμό θα καταγράφεται από το σύστημα.

- **Επίπεδο Ασφαλείας 4:**

Στο συγκεκριμένο επίπεδο το λειτουργικό περιβάλλον θα πρέπει να έχει πιστοποιηθεί τουλάχιστον ως EAL4 σύμφωνα με το Common Criteria.

- **Διαχείριση Κρυπτογραφικών Κλειδιών.**

Η συγκεκριμένη περιοχή περιλαμβάνει όλες τις φάσεις του κύκλου ζωής των κλειδιών που χρησιμοποιεί η κρυπτογραφική μονάδα, δηλαδή:

  - Παραγωγή Τυχαίων Αριθμών.
  - Δημιουργία Κλειδιών.
  - Ανάθεση Κλειδιών.
  - Είσοδος και Έξοδος Κλειδιών.
  - Αποθήκευση Κλειδιών.
  - Μηδενισμός-Καταστροφή Κλειδιών.

- **Ηλεκτρομαγνητική Συμβατότητα.**

Το πρότυπο ορίζει φυσικά μεγέθη και τις τιμές που περιγράφουν την ηλεκτρονική συμπεριφορά της κρυπτογραφικής μονάδας, κάτι που είναι απαραίτητο, καθώς είναι πλέον εφικτό με την χρήση ειδικών συσκευών και πολύπλοκων στατιστικών μεθόδων να μπορούν να διαβάζονται τα δεδομένα μιας μονάδας από την ηλεκτρική της τάση. Επιπλέον καλύπτονται φυσικά μεγέθη για το φαινόμενο van Eck, σύμφωνα με το οποίο η ηλεκτρομαγνητική ακτινοβολία την οποία εκπέμπουν επεξεργαστές, οθόνες και όλες οι σχετικές συσκευές, μπορεί να καλύψει μεγάλες αποστάσεις, διαπερνώντας τοίχους και να συλλεχθεί και να γίνει αντικείμενο επεξεργασίας οπουδήποτε.

- **Αυτό – Έλεγχος.**

Ορίζονται συγκεκριμένοι έλεγχοι οι οποίοι θα πρέπει να πραγματοποιούνται αυτόματα από την κρυπτογραφική μονάδα, έτσι ώστε να εξασφαλιστεί ότι αυτή λειτουργεί σωστά. Ορίζονται 2 είδη ελέγχων. Αυτοί που πραγματοποιούνται κατά την έναρξη και λήξη της τροφοδοσίας της συσκευής.(power up tests) και αυτοί που πραγματοποιούνται πριν από κάθε λειτουργία ασφαλείας (conditional test). Ένα παράδειγμα ενός τέτοιου ελέγχου είναι η δοκιμαστική κρυπτογράφηση ενός μικρού τμήματος δεδομένων και η αποκρυπτογράφηση τους. Αποτυχία σε οποιονδήποτε αυτοέλεγχο δεν θα επιτρέψει την πραγματοποίηση των κανονικών λειτουργιών της μονάδας.

- **Ορθότητα Σχεδιασμού.**

Στον συγκεκριμένο τομέα γίνεται αναφορά στις πρακτικές που ακολούθησε ο κατασκευαστής του συγκεκριμένου προτύπου κατά τον σχεδιασμό, υλοποίηση, εγκατάσταση και λειτουργία της μονάδας. Ο κατασκευαστής λοιπόν πρέπει να παρέχει εγγυήσεις ότι οι λειτουργικές απαιτήσεις που υποτίθεται ότι υλοποιεί η συγκεκριμένη μονάδα, όντως έχουν υλοποιηθεί. Επίσης πρέπει να φροντίζει, ώστε η κρυπτογραφική μονάδα να παραδοθεί, να εγκατασταθεί και να λειτουργήσει με ασφάλεια, παρέχοντας και τα απαραίτητα τεχνικά εγχειρίδια.

3.5.2 Διαχείριση Ασφάλειας: ISO 17799 – BS 7799.

Τα παραπάνω πρότυπα ασχολήθηκαν κυρίως με τεχνικές προδιαγραφές που πρέπει να ικανοποιούν τα διάφορα συστήματα, ώστε να μπορούν να χαρακτηριστούν αξιόπιστα και λιγότερο ή καθόλου στις διαδικασίες του οργανισμού που πρέπει να υποστηρίζουν την συγκεκριμένη διαδικασία. Δεν χρειάζεται να σχολιάσουμε την σημασία των διαδικασιών αυτών και γενικότερα της διοικητικής υποστήριξης σε ότι αφορά την ασφάλεια. Οδηγίες για τον σκοπό αυτό περιέχει το βρετανικό πρότυπο BS7799 (*Code of Practice for Information Security Management)*, το οποίο έχει υιοθετηθεί και από τον ISO (*17799*). Οι οδηγίες αυτές εκφράζονται στις εξής περιοχές:

1. **Διαχείριση Συνέχειας (Business Continuity Planning).** Η ενότητα αυτή προδιαγράφει ποια μέτρα πρέπει να λάβει η διοίκηση έτσι ώστε να ξεπεραστούν αποτυχίες συστημάτων ή παραβιάσεις ασφάλειας χωρίς αυτές να επηρεάσουν την κανονική λειτουργία του οργανισμού.
2. **Απαιτήσεις Ελέγχου Πρόσβασης (System Access Control).** Ρυθμίζει τους κανόνες που πρέπει να διέπουν την πρόσβαση στην πληροφορία, στους υπολογιστές και στα πληροφοριακά συστήματα και τρόπους ώστε να ανιχνευθούν οι παραβιάσεις.
3. **Ανάπτυξη και Συντήρηση Συστημάτων (Systems Development And Maintenance).** Θέτει αρχές που πρέπει να διέπουν τον κύκλο ζωής των πληροφοριακών συστημάτων, έτσι ώστε η ασφάλεια να είναι μέρος της διαδικασίας ανάπτυξης πληροφοριακών συστημάτων.
4. **Φυσική Ασφάλεια (Physical and Environmental Security).** Στόχος της συγκεκριμένης περιοχής είναι η προστασία των φυσικών χώρων (κτιρίων, δωματίων κτλ.) από καταστροφή ή μη

εξουσιοδοτημένη πρόσβαση. Επίσης στοχεύει στην προστασία της φυσικής υπόστασης όλων των αγαθών.

5. **Οδηγίες Εφαρμογής (Compliance).** Περιέχει κατευθύνσεις προς την διοίκηση έτσι ώστε να συμβαδίζει με το κανονιστικό πλαίσιο στο οποίο εντάσσεται ο οργανισμός και οδηγίες σχετικά με την εφαρμογή τους. Επίσης ασχολείται με την δημιουργία και χρήση πληροφορίας ελέγχου.
6. **Ασφάλεια Προσωπικού (Personnel Security).** Η περιοχή αυτή ασχολείται με τον ανθρώπινο παράγοντα και στόχο έχει την εκπαίδευση του προσωπικού ώστε να αποκτήσει επίγνωση ασφάλειας και να μειώσει την πιθανότητα ανθρώπινου λάθους.
7. **Οργάνωση Ασφάλειας (Security Organisation).** Στόχος της συγκεκριμένης ενότητας είναι η παροχή συστάσεων στην διοίκηση για την διαχείριση της ασφάλειας τόσο όταν οι σχετικές λειτουργίες υλοποιούνται μέσα στο οργανισμό είτε με εξωτερική ανάθεση.
8. **Διαχείριση Υπολογιστών & Δικτύου (Computer & Network Management).** Η ενότητα αυτή ασχολείται με την καθημερινή λειτουργία των συστημάτων του οργανισμού, με στόχο την ελαχιστοποίηση προβλημάτων, την διασφάλιση της ακεραιότητας και διαθεσιμότητας της πληροφορίας, ακόμα και όταν αυτή δεν ρέει μόνο μέσα στον οργανισμό αλλά αποτελεί αντικείμενο ανταλλαγής.
9. **Ταξινόμηση και Έλεγχος Αγαθών (Asset Classification & Control).** Εδώ παρέχονται οδηγίες αποτίμησης και κατάλληλης προστασίας των αντικειμένων που έχουν αξία για τον οργανισμό.
10. **Πολιτική Ασφάλειας (Security Policy).** Οδηγίες Δημιουργίας και Εφαρμογής Πολιτικής ασφάλειας.

3.5.3 Απαιτήσεις Ασφάλειας ειδικά για υπηρεσίες πιστοποίησης

Έχοντας περιγράψει τα πρότυπα τα οποία χρησιμοποιούνται για την αξιολόγηση αξιόπιστων συστημάτων, θα αναφέρουμε στην ενότητα αυτή, τις απαιτήσεις που τίθενται σε διεθνές επίπεδο για τα συστήματα των παρόχων υπηρεσιών πιστοποίησης. Είναι φανερό, πώς για να υπάρξει κάποιο πρότυπο, με βάση το οποίο θα αξιολογηθούν οι απαιτήσεις ασφάλειας αυτές, απαιτείται πολύ σαφής καθορισμός των υπηρεσιών στις οποίες αναφέρονται. Το πρότυπο **[TSMC, 2000],** θέτει μία πολύ καλή θεμελίωση χωρίζοντας τις σε τρεις κατηγορίες που θα περιγράψουμε στην συνέχεια. Ο σαφής καθορισμός αυτός έχει δύο πλεονεκτήματα:

1. μπορεί να οδηγήσει στην δημιουργία ενός προφίλ, με βάση το οποίο θα γίνεται η αποτίμηση, κατά το Common Criteria.
2. Μπορεί να διευκολύνει την διαδικασία δημιουργίας της πολιτικής πιστοποίησης και των σχετικών κειμένων.

Οι κατηγορίες των απαιτήσεων ασφάλειας λοιπόν σε ότι αφορά τις υπηρεσίες πιστοποίησης είναι:

- **Γενικές απαιτήσεις ασφάλειας:**

Οι συγκεκριμένες απαιτήσεις αφορούν την ασφάλεια, όλων των λειτουργιών ενός πάροχου υπηρεσιών πιστοποίησης, είτε αυτές είναι οι υπηρεσίες που προσφέρει στο κοινό, είτε αυτές είναι απαραίτητες για την εσωτερική του λειτουργία.

- **Διοικητικές Απαιτήσεις**: Οι απαιτήσεις αυτές αφορούν τα μέτρα που πρέπει να λάβει η διοίκηση του οργανισμού.
    - *Διαχείριση Ασφάλειας*: Οι λειτουργίες που σχετίζονται με την ασφάλεια πρέπει να ανατίθενται στους κατάλληλους ρόλους. Για την λειτουργία αξιόπιστων συστημάτων θεωρούνται απαραίτητοι οι εξής ρόλοι:
        - *Αξιωματικός Ασφάλειας*: Έχει την γενική ευθύνη για την υλοποίηση των πρακτικών που αναφέρονται στην δήλωση πρακτικών πιστοποίησης.
        - *Διαχειριστής Ασφάλειας*: Έχει την ευθύνη εγκατάστασης, ρύθμισης και συντήρησης των αξιόπιστων συστημάτων.
        - *Χειριστής Ασφάλειας:* Λειτουργεί τα αξιόπιστα συστήματα σε καθημερινή βάση και έχει την ευθύνη της δημιουργίας και ανάκτησης αντιγράφων ασφαλείας.
        - *Ελεγκτής Ασφάλειας*: Διατηρεί και εποπτεύει την καταγραφή των δραστηριοτήτων.

      Οι παραπάνω ρόλοι πρέπει να ανατίθενται στους κατάλληλους χρήστες.
    - *Ασφάλεια Προσωπικού*: Οι λειτουργίες ενός πάροχου πιστοποίησης πρέπει να υποστηρίζονται από το προσωπικό το οποίο έχει κατάλληλα προσόντα.
    - *Εφαρμογή Νομικών Ρυθμίσεων*: Η αρχή πιστοποίησης πρέπει να εφαρμόζει το νομικό πλαίσιο το οποίο ισχύει σε όλες τις περιοχές δραστηριοποίησης της. Ένα παράδειγμα αφορά την προστασία των προσωπικών δεδομένων και την τήρηση αρχείων.
    - *Οργανωτικές Απαιτήσεις:* Η αρχή πιστοποίησης πρέπει να τηρεί συγκεκριμένα οργανωτικά μέτρα τα οποία μπορούν να βοηθηθούν με ένα συστήμα διαχείρισης ποιότητας.
- **Λειτουργικές Απαιτήσεις**: Οι συγκεκριμένες απαιτήσεις ασφάλειας αφορούν την λειτουργία των συστημάτων σε καθημερινή βάση.
    - *Διαχείριση Λειτουργιών:* Πρέπει να εξασφαλίζεται ότι τα συστήματα μιας αρχής πιστοποίησης λειτουργούν με ασφάλεια και διατρέχουν μικρό κίνδυνο κατάρρευσης. Η ακεραιότητα των συστημάτων πρέπει να διασφαλίζεται ενάντια σε ιομορφικό λογισμικό αλλά και φυσικές απειλές, όπως για παράδειγμα κλοπή. Επίσης πρέπει να υπάρχει σχεδιασμός για μελλοντικές ανάγκες των συστημάτων (αναβαθμίσεις, επεκτάσεις), και λήψη των κατάλληλων μέτρων.
    - *Εξασφάλιση Συνέχειας:* Πρέπει να εξασφαλίζεται ότι υπάρχει δυνατότητα ανάνηψης από οποιαδήποτε καταστροφή (ακόμα και από την απώλεια του ιδιωτικού κλειδιού). Η ίδια η πράξη της μετάβασης σε εφεδρικά συστήματα δεν πρέπει να επιδρά στην αξιοπιστία τους.
    - *Φυσική Ασφάλεια:* Απαιτούνται μέτρα για την φυσική πρόσβαση στους χώρους όπου υπάρχει

ασφάλεια (πχ. αυθεντικοποίηση με βιομετρικές μεθόδους) και την παρακολούθηση τους (κλειστά κυκλώματα – κάμερες κτλ.). Επίσης πρέπει να παρέχεται προστασία σε ότι αφορά φυσικές καταστροφές (πχ. φωτιά, πλημμύρα, σεισμός).

- *Ασφάλεια Επικοινωνιών:* Αφορά απαιτήσεις που πρέπει να τηρούνται στην περίπτωση που υπάρχει διασύνδεση με κάποιο μη ασφαλές δίκτυο. Οι απαιτήσεις αυτές ορίζουν ένα αυστηρό πλαίσιο στο οποίο υπάρχει άρνηση σε κάθε υπηρεσία, εκτός αν αυτή είναι απολύτως απαραίτητη.
- *Κύκλος Ζωής Συστημάτων*: Αφορά απαιτήσεις για την τήρηση σωστών διαδικασιών ανάπτυξης εφαρμογών, εγκατάστασης, αρχικοποίησης και καταστροφής συσκευών κτλ.
- *Χρονισμός:* Λόγω της ιδιαίτερης σημασίας των ενδείξεων που αφορούν τον χρόνο στα πιστοποιητικά, είναι απαραίτητος ο συγχρονισμός των συστημάτων με μία σταθερή πηγή.

- **Απαιτήσεις για ταυτοποίηση και αυθεντικοποίηση**: Οι απαιτήσεις της συγκεκριμένης κατηγορίας εξασφαλίζουν την χρήση των συστημάτων μόνο από τις εξουσιοδοτημένες οντότητες.
  - *Αυθεντικοποίηση Οντοτήτων*: Κάθε χρήστης πρέπει να δηλώνει την ταυτότητα του στο σύστημα, πριν προβεί σε κάποια ενέργεια που απαιτεί ο ρόλος του.
  - *Χειρισμός Αποτυχίας Αυθεντικοποίησης*: Το σύστημα πρέπει να επιτρέπει περιορισμένο αριθμό αποτυχιών.
  - *Εμπιστευτικότητα Δεδομένων Αυθεντικοποίησης*: Η μετάδοση των δεδομένων αυθεντικοποίησης (συνθηματικών, PINs) πρέπει να γίνεται με ασφάλεια. Για παράδειγμα, τα παραπάνω ευαίσθητα δεδομένα μπορεί να μεταδίδονται κρυπτογραφημένα.
- **Απαιτήσεις για Διαχείριση Κλειδιών**. Ένα πάροχος υπηρεσιών πιστοποίησης εμπλέκεται αναγκαστικά σε όλη την φάση των λειτουργιών του με κρυπτογραφικά κλειδιά, είτε αυτά αφορούν συμμετρικά είτε ασύμμετρα κρυπτοσυστήματα. Γενικά μπορούμε να ταξινομήσουμε τα χρησιμοποιούμενα κλειδιά σε δύο κατηγορίες. Σε αυτά που χρησιμοποιούνται για την παροχή υπηρεσιών πιστοποίησης (υπογραφή πιστοποιητικών, δεδομένων ανάκλησης, δεδομένων χρονοσήμανσης, μυστικότητα) και σε αυτά που χρησιμοποιούνται εσωτερικά στον οργανισμό (αυθεντικοποίηση οντοτήτων κτλ.).
  - *Δημιουργία Κλειδιών:* Τα χρησιμοποιούμενα κλειδιά, πρέπει να παράγονται σε υλικό. Αν προορίζονται για την παροχή υπηρεσιών πιστοποίησης, πρέπει το σύστημα να έχει πιστοποιηθεί σύμφωνα με το πρότυπο FIPS-PUB 140-1 σε επίπεδο 3, ενώ για τα κλειδιά εσωτερικής χρήσης πρέπει η πιστοποίηση να είναι σε επίπεδο 2. Σε περίπτωση που η αρχή πιστοποίησης, παρέχει υπηρεσίες δημιουργίας κλειδιών, η δημιουργία αυτή πρέπει να πραγματοποιείται από σύστημα σε υλικό, με πιστοποίηση κατά FIPS-PUB 140-1 σε επίπεδο 3.
  - *Διανομή Κλειδιών:* Η διανομή ιδιωτικών κλειδιών πρέπει να γίνεται με την χρήση

κρυπτογραφικών μεθόδων. Η διανομή των δημοσίων κλειδιών πρέπει να γίνεται με τέτοιο τρόπο, ώστε να εξασφαλίζεται η ακεραιότητα τους.

- *Χρήση Κλειδιών:* Απαιτείται η χρήση διαφορετικών κλειδιών για κάθε υπηρεσία που παρέχει ο πάροχος υπηρεσιών πιστοποίησης. Επιπλέον, απαιτείται ένας μηχανισμός διαχωρισμού κλειδιών (key escrow), ως εγγύηση για την συνεχή διαθεσιμότητα των πιο σημαντικών υπηρεσιών. Επίσης απαιτείται η χρήση διαφορετικών κλειδιών για τις υπηρεσίες μυστικότητας και για τις υπηρεσίες αυθεντικοποίησης.
- *Αλλαγή / Ανανέωση Κλειδιών:* Πρέπει να γίνεται το πολύ σε ετήσια βάση, και να χαρακτηρίζεται από ασφάλεια.
- *Καταστροφή Κλειδιών:* Η καταστροφή κλειδιών, η οποία συμβαίνει όταν για παράδειγμα αποσύρονται οι συσκευές υπογραφής πιστοποιητικών, πρέπει να γίνεται με ασφάλεια έτσι ώστε να μην καθίσταται δυνατή η ανάκτηση των διεγραμμένων κλειδιών.
- *Αποθήκευση Δημιουργία και Ανάκτηση Εφεδρικών Αντιγράφων Κλειδιών:* Η κανονική αποθήκευση των κλειδιών πρέπει να γίνεται και εδώ σε διάταξη πιστοποιημένη από το πρότυπο FIPS-PUB 140-1. Όταν πρόκειται για κλειδιά τα οποία χρησιμοποιούνται για την παροχή των υπηρεσιών πιστοποίησης, πρέπει η αποτίμηση να τα κατατάσσει σε επίπεδο 3, ενώ όταν πρόκειται για εσωτερικές λειτουργίες, η αποτίμηση πρέπει να τα κατατάσσει σε επίπεδο 2. Αν τα κλειδιά δεν αποθηκεύονται σε τέτοιο σύστημα πρέπει τουλάχιστον να κρυπτογραφούνται από ένα τέτοιο σύστημα, πριν αποθηκευθούν. Η εφεδρική αποθήκευση τώρα των κρυπτογραφικών κλειδιών, και ιδιαίτερα του κρυπτογραφικού κλειδιού για την υπογραφή των πιστοποιητικών πρέπει να γίνεται με συστήματα διαχωρισμού κλειδιού (key escrow), τα οποία απαιτούν την παρουσία m από n οντότητες για την αποκρυπτογράφηση, με απαίτηση $(n-m) > 2$. Τέλος, απαγορεύεται, η αποθήκευση ή ο διαχωρισμός κλειδιού όταν αυτό ανήκει σε κάποιον συνδρομητή.
- *Αρχειοθέτηση Κλειδιών:* Απαγορεύεται η αρχειοθέτηση κλειδιών υπογραφής.

- **Απαιτήσεις ελέγχου.** Όλες οι λειτουργίες που σχετίζονται με την ασφάλεια, πρέπει να καταγράφονται και τα δεδομένα που προκύπτουν από την καταγραφή να είναι διαθέσιμα για έλεγχο.
  - *Επιλογή Δεδομένων Ελέγχου:* Τα δεδομένα που πρέπει να καταγράφονται για την επίτευξη ελεγξιμότητας και καταλογισμού είναι τα εξής:
    - Κάθε πρόσβαση στο σύστημα.
    - Ασυνήθιστη δραστηριότητα χρηστών.
    - Παράμετροι της ίδιας της λειτουργίας ελέγχου και αλλαγή αυτών.
    - Υπερβάσεις ρόλων ή προσπάθειες υπέρβασης.
    - Όλες οι αιτήσεις δημιουργίας πιστοποιητικών.

- Όλες οι αιτήσεις ανάκλησης ή αναστολής πιστοποιητικών.
- Όλες οι αιτήσεις ανανέωσης πιστοποιητικών.

o *Διαθεσιμότητα και ακεραιότητα δεδομένων ελέγχου:* Τα δεδομένα ελέγχου πρέπει να είναι διαθέσιμα. Έτσι για παράδειγμα πρέπει να υπάρχει πρόβλεψη ακόμα για την ύπαρξη επαρκούς χώρου για την μελλοντική αύξηση των αναγκών αποθήκευσης. Επίσης πρέπει κάθε εγγραφή να χαρακτηρίζεται από ακεραιότητα (κάτι που μπορεί να επιτευχθεί με την χρήση συναρτήσεων σύνοψης, ή ακόμα και ψηφιακές υπογραφές).

o *Μορφή Αρχείων Ελέγχου*: Η μορφή κάθε εγγραφής των αρχείων ελέγχου πρέπει να είναι η εξής:

- Ημερομηνία που έγινε η καταχώρηση.
- Τύπος καταχώρησης (παίρνει μία τιμή από τους παραπάνω).
- Τοποθεσία από την οποία έγινε το γεγονός.
- Ταυτότητα της οντότητας, η οποία προκάλεσε το γεγονός που καταχωρείται.
- Επιτυχία / Αποτυχία του ελέγχου.

o *Πρόσβαση στα δεδομένα ελέγχου*: Η ανάγνωση των δεδομένων ελέγχου πρέπει να επιτρέπεται μόνο σε εκείνους τους χρήστες οι οποίοι έχουν εξουσιοδοτηθεί. Η παρουσίαση των περιεχομένων πρέπει να παρέχεται σε μία μορφή, η οποία να ερμηνεύεται εύκολα.

- **Απαιτήσεις Αρχειοθέτησης**: Κάθε αξιόπιστο σύστημα, θα πρέπει να παρέχει υπηρεσίες αρχειοθέτησης προκαθορισμένων δεδομένων, στα οποία όμως δεν θα περιλαμβάνονται δεδομένα σχετιζόμενα με την ασφάλεια (όπως για παράδειγμα κλειδιά). Οι υπηρεσίες αρχειοθέτησης, θα πρέπει να υποστηρίζουν αναζήτηση. Η ακεραιότητα των δεδομένων πρέπει να διασφαλίζεται. Σε τακτά χρονικά διαστήματα επίσης θα πρέπει προστίθεται στα δεδομένα που αρχειοθετούνται κάποιο είδος χρονοσήμανσης.
- **Απαιτήσεις Δημιουργίας και Ανάκτησης Εφεδρικών Αντιγράφων**: Ένα αξιόπιστο σύστημα πρέπει να παρέχει λειτουργίες δημιουργίας και ανάκτησης εφεδρικών αντιγράφων. Οι λειτουργίες αυτές πρέπει να οδηγούν στην επαναφορά του συστήματος στην ακριβή κατάσταση που ήταν πριν από την μετάβαση. Επιπλέον, η ακεραιότητα των δεδομένων πρέπει να προστατεύεται με μία από τις γνωστές μεθόδους. Επιπρόσθετα, οποιαδήποτε δεδομένα είναι κρίσιμα πρέπει να αποθηκεύονται κρυπτογραφημένα.

❑ **Απαιτήσεις Ασφαλείας Βασικών Υπηρεσιών.**

Οι απαιτήσεις ασφαλείας στις οποίες θα αναφερθούμε στην συγκεκριμένη ενότητα, σχετίζονται με τις βασικές υπηρεσίες που αναφέραμε ότι παρέχει μία αρχή πιστοποίησης. Μία γενική απαίτηση, θέλει όλα τα μηνύματα τα οποία προέρχονται από την αρχή και χρησιμοποιούνται για τις συγκεκριμένες υπηρεσίες να συνοδεύονται με τους γνωστούς μηχανισμούς διασφάλισης της εγκυρότητας. Επίσης είναι πολύ σημαντική η χρονική τοποθέτηση των μηνυμάτων.

- **Υπηρεσία Εγγραφής**.
  - *Αίτηση Πιστοποιητικού*: Η αίτηση πιστοποιητικού είναι η διαδικασία εκείνη μέσω της οποίας μία συγκεκριμένη οντότητα συνδέεται με ένα δημόσιο κλειδί. Οι απαιτήσεις που τίθενται για την συγκεκριμένη υπηρεσία είναι:
    - Συλλογή των κατάλληλων στοιχείων για την ταυτοποίηση του συνδρομητή. Το ποια στοιχεία απαιτούνται για την απόκτηση βεβαιότητας σχετικά με την ταυτότητα του συνδρομητή εξαρτώνται από πολλούς εξωγενείς παράγοντες, όπως για παράδειγμα το ρυθμιστικό πλαίσιο λειτουργίας της αρχής πιστοποίησης.
    - Απόδειξη κατοχής του ιδιωτικού κλειδιού. Ο συνδρομητής πρέπει να αποδείξει ότι όντως κατέχει το ιδιωτικό κλειδί με το οποίο σχετίζεται το δημόσιο κλειδί που πιστοποιείται. Για τον σκοπό αυτό αναφέρονται στην βιβλιογραφία πολλοί τρόποι, με τον πιο απλό από τους οποίους να είναι η υπογραφή ενός απλού μηνύματος και η αποστολή του στην αρχή για επαλήθευση.
    - Ασφάλεια μετάδοσης των δεδομένων του συνδρομητή. Συνδέεται άμεσα με την επόμενη απαίτηση.
  - *Διαχείριση Δεδομένων Συνδρομητή*: Επειδή τα δεδομένα που υποβάλλει ο συνδρομητής προκειμένου να πιστοποιηθεί, είναι πολλές φορές ιδιωτικά, απαιτείται η προστασία της ιδιωτικότητας αυτής η οποία μπορεί να επιτευχθεί μέσω της διατήρησης της μυστικότητας των δεδομένων.
- **Υπηρεσία Δημιουργίας Πιστοποιητικών.**
  - Δημιουργία Πιστοποιητικών: Επειδή η υπηρεσία της πιστοποίησης ταυτίζει για ένα χρονικό διάστημα, μία οντότητα με ένα δημόσιο κλειδί, οι απαιτήσεις ασφαλείας που την συνοδεύουν είναι πολύ σημαντικές. Έτσι, για παράδειγμα, απαιτείται η διασφάλιση της γνησιότητας και εγκυρότητας της αίτησης πιστοποίησης, η οποία πιθανότατα έχει προέλθει από μία αρχή καταχώρησης. Το πιο σημαντικό στοιχείο της όλης διαδικασίας είναι η υπογραφή των πιστοποιητικών, η οποία πρέπει να γίνει σε περιβάλλον υψηλής ασφάλειας (FIPS-PUB 140-1 επιπέδου 3).
  - Ανανέωση Πιστοποιητικού: Όπως προαναφέραμε ένα πιστοποιητικό, ισχύει για συγκεκριμένο χρόνο διάστημα, μετά την λήξη του οποίου απαιτείται ανανέωση του. Το ανανεωμένο πιστοποιητικό μπορεί να αφορά το ίδιο δημόσιο κλειδί, και κατά συνέπεια και το ίδιο ιδιωτικό κλειδί ή ένα νέο ζεύγος κλειδιών. Οι απαιτήσεις ασφάλειας για την ανανέωση του πιστοποιητικού είναι παρόμοιες με αυτές για την δημιουργία του.
  - Διαπιστοποίηση (Cross - Certification): Ο μηχανισμός της διαπιστοποίησης δημιουργεί όπως προαναφέραμε μία σχέση ‘εμπιστοσύνης’ μεταξύ δύο παρόχων πιστοποίησης. Εκτός από τις απαιτήσεις που συναντήσαμε για τις προηγούμενες υπηρεσίες, τίθεται εδώ ένα μεγάλο θέμα: το θέμα της συμβατότητας των πολιτικών πιστοποίησης. Πρέπει να διασφαλιστεί εκ των

προτέρων ότι οι πολιτικές πιστοποίησης της αρχής πιστοποίησης που ζητά την διαπιστοποίηση (η οποία δηλαδή γίνεται έμπιστη) γίνεται αποδεκτή από τους χρήστες της αρχής πιστοποίησης που την παρέχει, ώστε να διασφαλιστεί η δυνατότητα για επαλήθευση της εγκυρότητας του πιστοποιητικού. Επίσης πρέπει να τηρηθούν ορισμένες τοπικές νομικές απαιτήσεις.

- **Υπηρεσία Διάδοσης Πιστοποιητικών.** Η συγκεκριμένη υπηρεσία είναι γνωστή και ως ο κατάλογος των πιστοποιητικών. Οι απαιτήσεις που τίθενται για την λειτουργία του καταλόγου αφορούν αφενός την διαθεσιμότητα του και αφετέρου τον καθορισμό μιας πολιτικής πρόσβασης για τον έλεγχο των οντοτήτων που μπορούν να διαβάζουν και να τροποποιούν τα περιεχόμενα του.
- **Υπηρεσία Διαχείρισης Ανάκλησης Πιστοποιητικών.** Όπως αναφέραμε και στο δεύτερο κεφάλαιο, η συγκεκριμένη υπηρεσία χειρίζεται τις αιτήσεις για ανάκληση των πιστοποιητικών.
    - *Αιτήσεις Ανάκλησης \ Αναστολής Πιστοποιητικών:* Ο χειρισμός των αιτήσεων της κατηγορίας έχει την ίδια ίσως και μεγαλύτερη σημασία από τις αντίστοιχες αιτήσεις για πιστοποίηση. Απαιτείται αυθεντικοποίηση όλων των αιτήσεων και εξέταση της εγκυρότητας τους. Οι παραπάνω διαδικασίες πρέπει να γίνουν άμεσα, ώστε να ελαχιστοποιηθούν τα κρίσιμα χρονικά διαστήματα που είδαμε νωρίτερα.
    - *Ανάκληση και Αναστολή Πιστοποιητικών:* Αν το αποτέλεσμα της εξέτασης των παραπάνω αιτήσεων είναι η ακύρωση του πιστοποιητικού (μέσω ανάκλησης \ αναστολής), η αλλαγή κατάστασης πρέπει να περάσει άμεσα στην υπηρεσίες ενημέρωσης για την κατάσταση των πιστοποιητικών.
- **Υπηρεσία Ενημέρωσης Κατάστασης Πιστοποιητικού**.

Η συγκεκριμένη υπηρεσία πρέπει να είναι διαθέσιμη 24 ώρες την μέρα και 7 ώρες την εβδομάδα. Όλα τα μηνύματα τα οποία παράγονται από αυτήν πρέπει να συνοδεύονται απο τεχνικές εξασφάλισης εγκυρότητας και αυθεντικότητας και να είναι δημόσια διαθέσιμα (σε διεθνές επίπεδο).

- **Απαιτήσεις Ασφαλείας Προαιρετικών Υπηρεσιών.**
    - **Υπηρεσία Χρονοσήμανσης.** Οι απαιτήσεις ασφάλειας για την υπηρεσία χρονοσήμανσης είναι οι εξής:
        - *Σωστή Επαλήθευση των Αιτήσεων*: Είναι φανερό, ότι προτού δημιουργηθεί η χρονοσήμανση σε μία αίτηση, πρέπει να υπάρξει κάποια εξέταση της εγκυρότητας της. Έτσι για παράδειγμα, πρέπει να επαληθευθεί η ακεραιότητα και η αυθεντικότητα της.
        - *Σωστή ανάκτηση της παραμέτρου του χρόνου*, που θα χρησιμοποιηθεί ως είσοδο στην παράμετρο της χρονοσήμανσης. Ένα από τα συστήματα ανάκτησης χρόνου που πιθανότατα μπορεί να χρησιμοποιηθεί είναι το UTC (Universal Time Coordinator), το οποίο έχει προταθεί από την ITU.
        - *Προστασία των δεδομένων* στα οποία θα εφαρμοστεί η χρονοσήμανση, τα οποία μπορεί να είναι εμπιστευτικά, και οποιαδήποτε διαρροή τους ενδεχομένως βλάψει τον υπογράφοντα.

Κάτι τέτοιο πρέπει να μπορεί να εξασφαλιστεί και από τον συνδρομητή.

Η συγκεκριμένη υπηρεσία μπορεί να παρέχεται είτε από την ίδια οντότητα που παρέχει τις υπηρεσίες πιστοποίησης, είτε από μία ξεχωριστή οντότητα. Στην δεύτερη περίπτωση ισχύουν και οι απαιτήσεις που προαναφέραμε σχετικά με την διαχείριση κλειδιών και την οργάνωση της αρχής χρονοσήμανσης, επιπλέον. Σε κάθε περίπτωση εισάγονται και εδώ έννοιες όπως πολιτικές χρονοσήμανσης και δήλωση πρακτικών χρονοσήμανσης. Μάλιστα υπάρχουν και τα αντίστοιχα πρότυπα **[ETSI, 178T1].**

- **Υπηρεσίες Παροχής Ασφαλών Διατάξεων Δημιουργίας Υπογραφών.**

Οι πάροχοι υπηρεσιών πιστοποίησης μπορούν να εξοπλίζουν τους συνδρομητές με τις διατάξεις εκείνες οι οποίες θα χρησιμοποιούνται για την δημιουργία των ηλεκτρονικών υπογραφών. Για παράδειγμα μπορούν να παρέχουν έξυπνες κάρτες οι οποίες θα περιέχουν το ιδιωτικό κλειδί κρυπτογράφησης με τρόπο ανάλογο με τον οποίο οι τράπεζες παρέχουν μαγνητικές κάρτες για τα μηχανήματα αυτόματης ανάληψης. Σε μία τέτοια περίπτωση θα πρέπει η συγκεκριμένη διάταξη να αποθηκεύεται και να διανέμεται με ασφάλεια. Πολλές φορές θα συνοδεύεται και από δεδομένα ενεργοποίησης, όπως για παράδειγμα ένα PIN, το οποίο πρέπει για προφανείς λόγους να διανέμεται ξεχωριστά από την υπόλοιπη διάταξη. Αυτό μπορεί να γίνει είτε με την διανομή με διαφορετικές μεθόδους, είτε σε διαφορετικές χρονικές στιγμές.

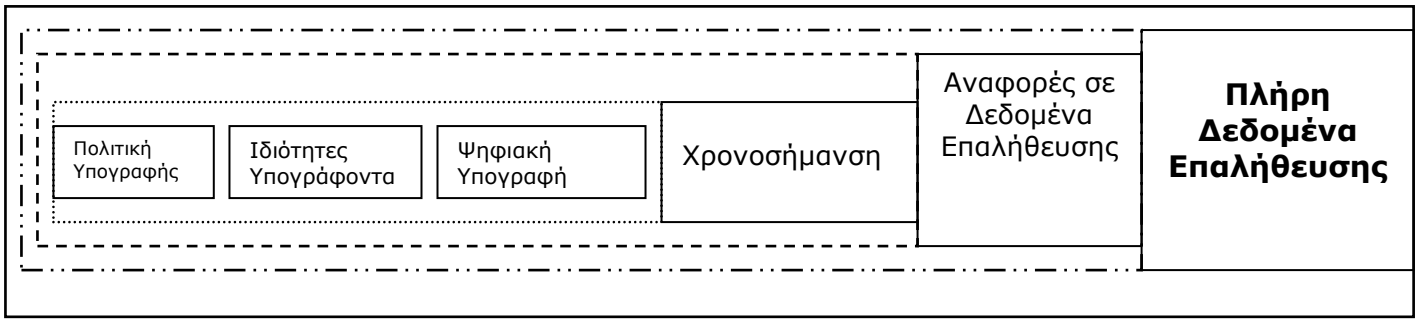
3.6 Μορφή Ηλεκτρονικών Υπογραφών.

Στο κεφάλαιο 2, αναφερθήκαμε στα είδη των ηλεκτρονικών υπογραφών. Εκεί περιγράψαμε ποιες τεχνολογίες μπορούν να χρησιμοποιηθούν για την δημιουργία τους. Βέβαια, η απλή συμφωνία στην τεχνολογία που μπορεί να χρησιμοποιηθεί για τις ηλεκτρονικές υπογραφές δεν αρκεί για να παρέχει την απαραίτητη συμβατότητα, που απαιτείται, όπως προαναφέραμε νωρίτερα έτσι ώστε να μπορούν να χρησιμοποιηθούν σε οποιοδήποτε περιβάλλον. Επιπλέον, για να μπορούν να ικανοποιηθούν οι απαιτήσεις που αναφέραμε στην εισαγωγή για τις ηλεκτρονικές συναλλαγές, πρέπει οι ηλεκτρονικές υπογραφές να συνοδεύονται από στοιχεία τα οποία να επιτρέπουν την επαλήθευση τους μετά από μεγάλο χρονικό διάστημα για την επίλυση διαφορών, οι οποίες μπορούν να προκύψουν οποτεδήποτε ανάλογα και με την φύση των υπογραφόμενων εγγράφων. Συμπεραίνουμε, λοιπόν ότι η απλή αναφορά της τεχνολογίας η οποία χρησιμοποιείται για την παραγωγή της ηλεκτρονικής υπογραφής, δεν επαρκεί για να καλύψει τις παραπάνω απαιτήσεις. Στην ενότητα αυτή, θα αναφερθούμε λοιπόν στις μορφές ηλεκτρονικών υπογραφών, οι οποίες μπορούν να υποστηρίξουν τις παραπάνω απαιτήσεις. Αρχικά θα αναφερθούμε στις μορφές των ηλεκτρονικών υπογραφών, οι οποίες είναι απαραίτητες για την παροχή επαλήθευσης μετά από μεγάλα χρονικά διαστήματα. Στον τομέα αυτόν υπάρχει σχετική προτυποποίηση **[ETSI, 101 733],** η οποία υιοθετεί την υπόθεση της υποδομής δημοσίου κλειδιού που κάναμε και εμείς στο δεύτερο κεφάλαιο.

Οι μορφές ηλεκτρονικής υπογραφής που ορίζονται στο **[ETSI, 101 733]** είναι:

- Ηλεκτρονική Υπογραφή (ES): Αποτελεί την πιο απλή μορφή. Περιέχει την ψηφιακή υπογραφή του υπογράφοντα και άλλα βασικά στοιχεία.. Πρέπει απαραίτητα να παρέχεται από τον υπογράφοντα.
- Ηλεκτρονική Υπογραφή με Χρονοσήμανση (ES –T): Επεκτείνει την παραπάνω μορφή παρέχοντας χρονοσήμανση. Μπορεί είτε να δημιουργηθεί από τον υπογράφοντα είτε από τον επαληθεύοντα κατά την πρώτη επαλήθευση.
- Ηλεκτρονική Υπογραφή με πλήρη δεδομένα επαλήθευσης (ES-C): Επεκτείνει την παραπάνω μορφή παρέχοντας αναφορές (references) σε όλα εκείνα τα δεδομένα εκείνα τα οποία είναι απαραίτητα για την πλήρη επαλήθευση της υπογραφής, όπως για παράδειγμα ένα σύνολο πιστοποιητικών και λιστών ανάκλησης. Και εδώ δεν πρέπει να παρέχεται απαραίτητα από τον υπογράφοντα, αλλά μπορεί να δημιουργηθεί και από τον επαληθεύοντα.
- Εκτεταμένη Ηλεκτρονική Υπογραφή (ES-X) : Ουσιαστικά πρόκειται για την ίδια μορφή με την προαναφερθείσα με την διαφορά ότι αντί για τις αναφορές υπάρχουν τα πλήρη δεδομένα επαλήθευσης.

Στόχος των δύο εκτεταμένων ειδών υπογραφής είναι η παροχή δυνατοτήτων επαλήθευσης της υπογραφής μετά από πολύ μεγάλα χρονικά διαστήματα. Έτσι δεν θα ήταν υπερβολή να πούμε ότι ο τελευταίος τύπος υπογραφής *αποτελεί ένα πλήρες στιγμιότυπο της υποδομής δημοσίου κλειδιού*, την στιγμή της υπογραφής ή την στιγμή της επαλήθευσης, ανάλογα με το πότε έχουν προσαρτηθεί τα συγκεκριμένα δεδομένα.. Οι παραπάνω μορφές ηλεκτρονικών υπογραφών φαίνονται λεπτομερώς στο σχήμα που ακολουθεί:



Σχήμα 12. Μορφές Ηλεκτρονικών Υπογραφών

Επιπλέον σε περίπτωση που υπάρξει ανάγκη για αρχειοθέτηση των υπογραφών για μεγάλο χρονικό διάστημα, πρέπει να αντιμετωπιστεί το γεγονός ότι οι αλγόριθμοι που θα χρησιμοποιηθούν για την χρονοσήμανση και υπογραφή των παραπάνω δεδομένων θα θεωρούνται πλέον μη ασφαλείς. Για τον σκοπό κατά την αρχειοθέτηση υπογραφών με τέτοιες απαιτήσεις πρέπει να γίνει χρήση ισχυρότερων αλγορίθμων. Η παραπάνω διαδικασία πιθανότατα θα πρέπει να επαναλαμβάνεται σε τακτά χρονικά διαστήματα, ανάλογα βέβαια και με την περίοδο που πρέπει να διατηρηθούν τα δεδομένα. Προκύπτει έτσι και μία επιπλέον μορφή υπογραφών με επαναλαμβανόμενες χρονοσημάνσεις αρχειοθέτησης (*ES-A*). Η ακριβής μορφή της ηλεκτρονικής υπογραφής παίζει πολύ σημαντικό ρόλο στην διαδικασία επαλήθευσης της, όπως θα δούμε

και στην συνέχεια.

Όπως προαναφέραμε, η αξία των ηλεκτρονικών υπογραφών μειώνεται σημαντικά αν αυτές δεν μπορούν να χρησιμοποιηθούν σε ετερογενή υπολογιστικά περιβάλλοντα. Για τον σκοπό αυτό είναι απαραίτητη η αναπαράσταση τους σε μορφή ανεξάρτητη από λειτουργικό σύστημα ακόμα και υλικό. Το παραπάνω γεγονός σε συνδυασμό με την κυριαρχία της **XML** (**eXtensible Markup Language**) για την ανταλλαγή δεδομένων μεταξύ εφαρμογών πάνω από το Internet, έχει οδηγήσει στην ανάπτυξη προδιαγραφών για **Ψηφιακές Υπογραφές XML (XML Digital Signatures).** Προτυποποίηση σε αυτό το επίπεδο υπάρχει τόσο από το W3C, όσο και από την EESSI **[ETSI, 101 903]**.

3.7 Μοντελοποίηση Δημιουργίας Υπογραφής

Η διάταξη δημιουργίας υπογραφής είναι ίσως το σημαντικότερο σύστημα που συναντάει κανείς σε ένα περιβάλλον ηλεκτρονικών υπογραφών. Κάτι τέτοιο ισχύει ιδιαίτερα όταν η χρησιμοποιούμενη τεχνολογία είναι αυτή των ψηφιακών υπογραφών, καθώς σε μία τέτοια περίπτωση το σύστημα δημιουργίας υπογραφής είναι αυτό που έρχεται σε επαφή με το ιδιωτικό κλειδί. Είναι φανερό λοιπόν ότι οι συγκεκριμένες διατάξεις έχουν πολύ αυστηρές απαιτήσεις ασφάλειας. Παρ'όλα αυτά δεν υπάρχει μία συγκεκριμένη τεχνολογία, η οποία να είναι γενικά αποδεκτή ή δοκιμασμένη για ένα τέτοιο σύστημα. Τον συγκεκριμένο ρόλο μπορεί να διαδραματίσει μία 'έξυπνη κάρτα' (*Smart Card*), ένα 'ηλεκτρονικό πορτοφόλι' (*Electronic Wallet*), ένα PDA, ένα κινητό τηλέφωνο, ένας προσωπικός υπολογιστής, ή γενικά οποιαδήποτε συσκεύη με ικανοποιητικό επεξεργαστή. Είναι απαραίτητη λοιπόν η μοντελοποίηση ενός τέτοιου συστήματος, του περιβάλλοντος του, και της διαδικασίας δημιουργίας υπογραφής, ώστε να μπορούν να εκφραστούν οι απαιτήσεις ασφάλειας με βάση το συγκεκριμένο αφαιρετικό μοντέλο. Μία τέτοια μοντελοποίηση αναφέρεται στο **[SSCS,2000]** και στο **[SSCD, 2001].**

Για κάθε λειτουργία που καθορίζεται στο μοντέλο αυτό ορίζονται απαιτήσεις (λειτουργικές και ασφάλειας) με στόχο την παροχή ενός περιβάλλοντος για την δημιουργία ηλεκτρονικών υπογραφών, το οποίο αφενός πληροί τις προϋποθέσεις που θέτει η οδηγία και αφ'ετέρου είναι εύχρηστο και χωρίς λάθη, ώστε να μπορεί να χρησιμοποιηθεί ακόμα και από άτομα με ειδικές ανάγκες. Οι απαιτήσεις αυτές αποσκοπούν (στο απώτερο μέλλον) στην αποδοχή και ανάπτυξη εμπιστοσύνης από το ευρύ κοινό στις ηλεκτρονικές υπογραφές.

Η διάταξη που ικανοποιεί το συγκεκριμένο εννοιολογικό μοντέλο, θα μπορεί να παράγει μία ηλεκτρονική υπογραφή, όταν δεχθεί ως είσοδο:

- Τα δεδομένα προς υπογραφή.
- Ένα πιστοποιητικό του υπογράφοντα (υποχρεωτικά, καθώς χρήστες με πολλαπλά πιστοποιητικά θα πρέπει να δηλώνουν ποιο θα αφορά η υπογραφή).
- Προαιρετικά, μία πολιτική υπογραφής, η οποία καθορίζει ακριβώς την δέσμευση η οποία αντιστοιχεί στην συγκεκριμένη υπογραφή.

Ως έξοδο η διάταξη θα παράγει ένα **Υπογεγραμμένο Αντικείμενο Δεδομένων (Signed Data Object)**, στο οποίο θα βασίζεται η ηλεκτρονική υπογραφή. Είναι μία σύνθετη δομή δεδομένων, η οποία περιλαμβάνει την ίδια την υπογραφή, μαζί με τα υπογεγραμμένα δεδομένα, αλλά και επιπλέον στοιχεία όπως τον αναγνωριστή του πιστοποιητικού, ένα δείκτη σε πολιτική ασφαλείας και άλλα στοιχεία ανάλογα με την μορφή ηλεκτρονικών υπογραφών που προαναφέραμε.

Η υλοποίηση των απαιτήσεων, είναι ανεξάρτητη τόσο από την τεχνολογία που θα χρησιμοποιηθεί για τον σκοπό αυτό, όσο και από το μέσο (υλικό ή λογισμικό).

Αποτελείται από τα εξής στοιχεία:

- **Τον υπογράφοντα**. Έρχεται σε επαφή με το σύστημα με μία προκαθορισμένη διεπαφή (interface).
- **Το σύστημα δημιουργίας υπογραφής (Signature Creation System).** Παραδείγματα συσκευών που μπορούν να ικανοποιούν τις απαιτήσεις ενός τέτοιου συστήματος είναι: επιτραπέζιοι / φορητοί υπολογιστές, υπολογιστές χειρός και κινητά τηλέφωνα. Θα αναφερόμαστε στο εξής στο συγκεκριμένο στοιχείο με τον όρο σύστημα.
- **Την ασφαλή συσκευή δημιουργίας υπογραφής (Secure Signature Creation Device).** Είναι εξωτερική στο προηγούμενο σύστημα και η διαφορά της από αυτό έγκειται στο γεγονός ότι είναι υπεύθυνη για όλες τις λειτουργίες που αφορούν το ιδιωτικό κλειδί με το οποίο θα δημιουργηθεί η ηλεκτρονική υπογραφή και είναι υπεύθυνη για την προστασία του. Είναι η μόνη υπολογιστική συσκευή η οποία θα έρθει σε επαφή με το ιδιωτικό κλειδί. Με βάση το παραπάνω λοιπόν πρέπει να την διακρίνουμε δύο τμήματα:
    - Το τμήμα που έρχεται σε επαφή με το ιδιωτικό κλειδί.
    - Το υπόλοιπο.

  Τα παραπάνω τμήματα δεν μπορούν να διαχωριστούν πλήρως σε θεωρητικό επίπεδο. Ο ακριβής διαχωρισμός εξαρτάται από την υλοποίηση. Στην συγκεκριμένη κατηγορία δεν πρέπει να εντάξουμε μόνο την διάταξη που θα κατέχει ο χρήστης. Αφορά όλες τις διατάξεις που έρχονται σε επαφή με το ιδιωτικό κλειδί. Γενικά διακρίνουμε 3 τύπους:

  Τύπος 1: Διάταξη που χρησιμοποιείται για την παραγωγή του ιδιωτικού και δημοσίου κλειδιού. Τυπικά βρίσκεται σε ένα πάροχο υπηρεσιών πιστοποίησης, ο οποίος παρέχει υπηρεσίες δημιουργίας κλειδιών.

  Τύπος 2: Διάταξη που χρησιμοποιείται για την αποθήκευση του ιδιωτικού κλειδιού και την δημιουργία της υπογραφής. Είναι το συστατικό εκείνο που θα έχει στην καθημερινή κατοχή του ο κάθε χρήστης.

  Τύπος 3: Η συγκεκριμένη διάταξη συνδυάζει τις λειτουργίες των τύπων 1 και 2.

  Οι παραπάνω τύποι φαίνονται καλύτερα στο *σχήμα 13* **[SSCD, 2001]**. Σε αυτό πρέπει να επισημάνουμε ότι τα βέλη είτε μονής, είτε διπλή κατεύθυνσεις, υποδηλώνουν κάποιο έμπιστο μονοπάτι για την μεταβίβαση των δεδομένων, δηλαδή μία διεπαφή που μπορεί να χαρακτηριστεί ασφαλής λόγω του ότι τα δεδομένα μεταδίδονται κρυπτογραφημένα μέσω αυτής.

Η ηλεκτρονική υπογραφή παράγεται με *την συνεργασία* του συστήματος δημιουργίας υπογραφής και

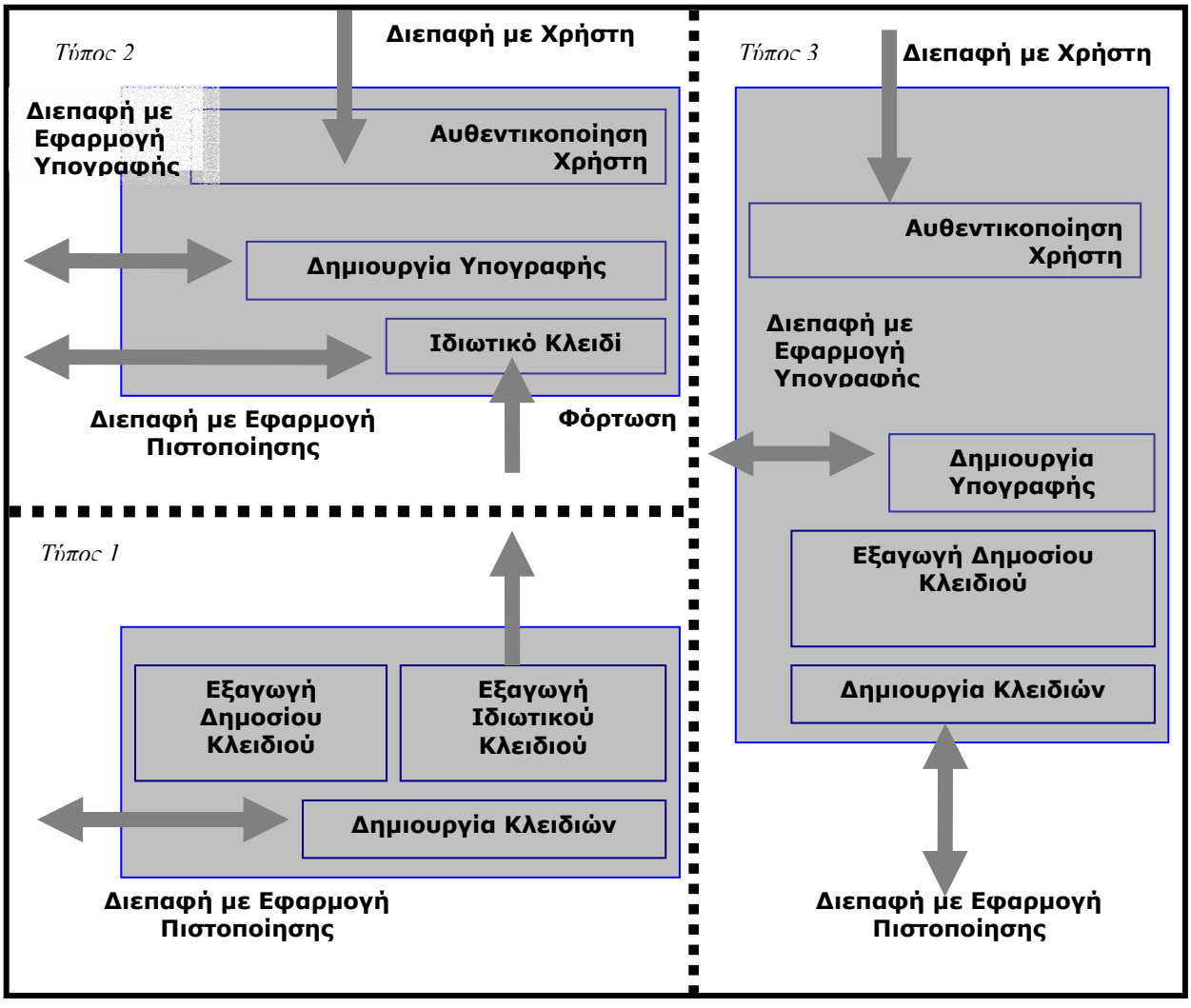
της συσκευής. Τα πιο σημαντικά υποσυστήματα του συστήματος δημιουργίας υπογραφής είναι το ασφαλές ή έμπιστο υποσύστημα (trusted subsystem) και το υποσύστημα εφαρμογών (application subsystem).

Η λειτουργία του συνολικού συστήματος είναι ανεξάρτητη του περιβάλλοντος και περιγράφεται σε γενικές γραμμές ως εξής:

1. Το σύστημα δημιουργίας υπογραφής τίθεται σε λειτουργία με την βοήθεια ίσως της συσκευής δημιουργίας υπογραφής, με τρόπο ανάλογο με τον οποίο μία κάρτα αυτόματης ανάληψης ενεργοποιεί ένα ATM.

2. Τα δύο συστήματα αυθεντικοποιούνται, κάτι απαραίτητο στην περίπτωση που το πρώτο είναι σε δημόσιο χώρο και κατά συνέπεια δεν υπάρχει κάποια πολιτική η οποία να το κάνει έμπιστο. Το βήμα αυτό εξασφαλίζει τον υπογράφοντα.

3. Ο υπογράφων επιλέγει το πιστοποιητικό το οποίο θα χρησιμοποιήσει και το οποίο θα πρέπει αντιστοιχεί στα δεδομένα δημιουργίας της συγκεκριμένης υπογραφής. Κάθε χρήστης μπορεί να διαθέτει περισσότερα από ένα πιστοποιητικά για πολλούς λόγους, όπως για παράδειγμα: το καθένα από τα οποία να προορίζεται για διαφορετική χρήση. Ως παράδειγμα σε αυτό μπορούμε να αναφέρουμε πιστοποιητικά τα οποία έχουν εκδοθεί για διαφορετικά ποσά.

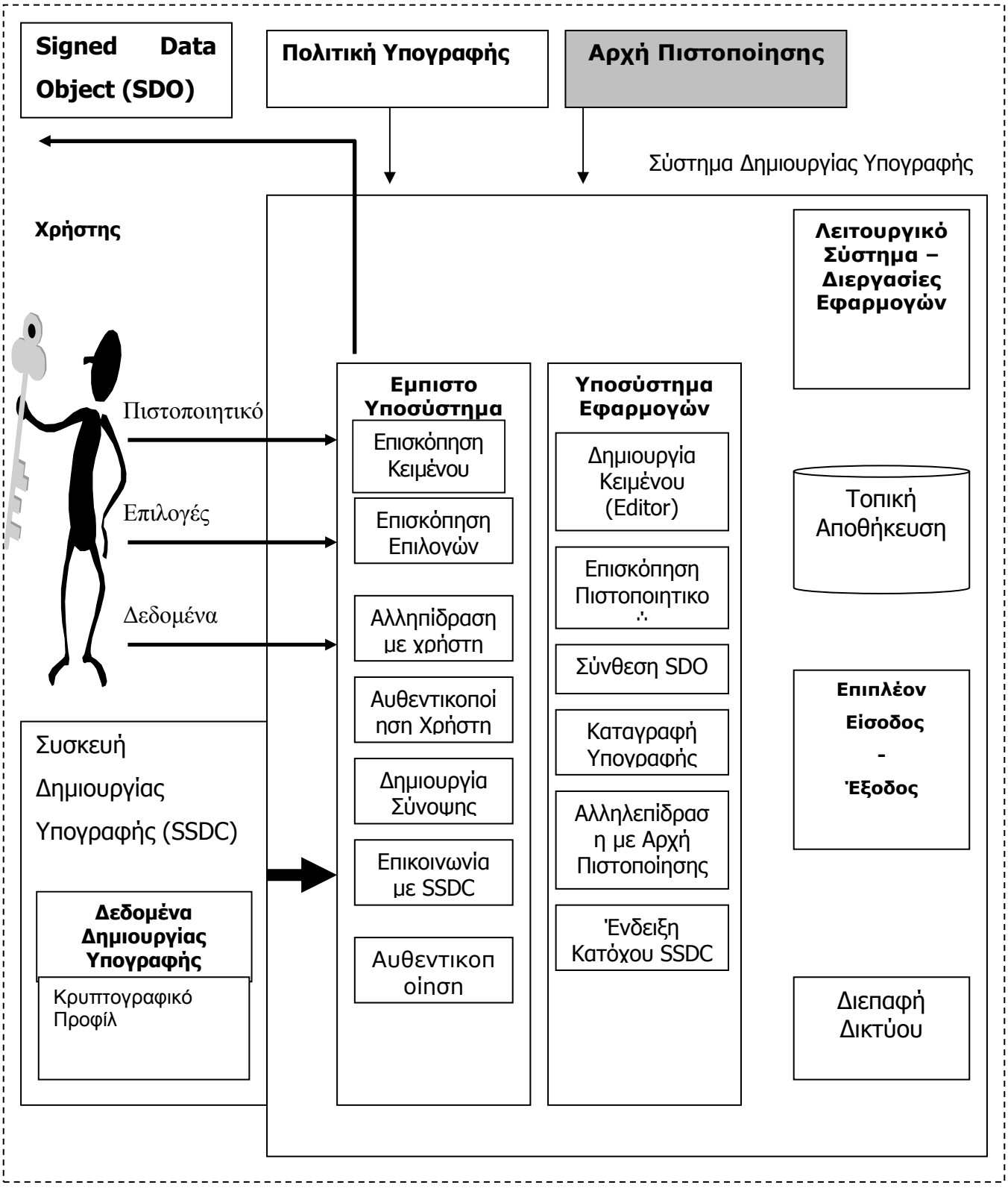


Σχήμα 13. Τύποι Διατάξεων Δημιουργίας Υπογραφής

- Μπορεί να διαθέτει πολλαπλά δεδομένα δημιουργίας υπογραφής, και κατά συνέπεια πολλαπλά δεδομένα επαλήθευσης υπογραφής., άρα και πιστοποιητικά.
- Μπορεί για τα ίδια δεδομένα δημιουργίας υπογραφής να διαθέτει πολλαπλά πιστοποιητικά.

Η διαδικασία επιλογής του πιστοποιητικού δεν είναι ανάγκη να είναι εμφανής στον τελικό χρήστη. Για παράδειγμα στις περισσότερες υλοποιήσεις οι τελικοί χρήστες εφοδιάζονται με διατάξεις δημιουργίας υπογραφής, οι οποίες περιέχουν τρία κλειδιά: το ένα χρησιμοποιείται για κρυπτογράφηση, το άλλο για αυθεντικοποίηση και το τελευταίο για υπογραφή. Τα αντίστοιχα πιστοποιητικά μπορούν να διακρίνονται από την επέκταση χρήσης κλειδιού. Κατά την αυθεντικοποίηση λοιπόν του βήματος 2, χωρίς να καταλάβει τίποτα ο χρήστης η αυθεντικοποίηση θα γίνεται με το αντίστοιχο πιστοποιητικό, ενώ για την υπογραφή ο χρήστης θα επιλέγει ρητά το πιστοποιητικό υπογραφής.

Περιβάλλον Δημιουργίας Υπογραφής



Σχήμα 14.Εννοιολογικό Μοντέλο Περιβάλλοντος Δημιουργίας Υπογραφής

4. Ο υπογράφων επιλέγει, φορτώνει ή δημιουργεί το κείμενο προς υπογραφή. Εισάγει επίσης ενδεχομένως ορισμένες από τις παραμέτρους οι οποίες προαναφέρθηκαν.

5. Υποχρεωτικά το σύστημα δίνει στον υπογράφοντα την δυνατότητα να επισκοπήσει την τελική έκδοση

του κειμένου και των υπόλοιπων επιλογών που έχει εισάγει πριν αρχίσει η διαδικασία της υπογραφής.

6. Ο χρήστης επιλέγει τον τύπο της υπογραφής που θέλει να παράγει το σύστημα.

7. Ο χρήστης εισάγει τα δεδομένα αυθεντικοποίησης του (είτε κάποιο PIN, είτε κάποιες βιομετρικές ενδείξεις), τα οποία θα χρησιμεύσουν για την αποκρυπτογράφηση του ιδιωτικού κλειδιού. Τα δεδομένα αυτά εισάγονται στο σύστημα συνήθως και μεταφέρονται στην συσκευή μέσω της διεπαφής τους. Η διεπαφή αυτή μπορεί να είναι ένας σύνδεσμος οποιουδήποτε είδους από δίαυλος USB, μέχρι υπέρυθρη θύρα, ανάλογα με το σύστημα και την συσκευή. . Αν η διεπαφή με τον χρήστη δεν αποτελεί τμήμα της ασφαλούς διάταξη τότε είναι φανερό ότι τα δεδομένα αυτά πρέπει να μεταφερθούν με ένα έμπιστο μονοπάτι όπως φαίνεται στο σχήμα 13.

8. Το σύστημα δημιουργεί μία σύνοψη του κειμένου και των υπόλοιπων επιλογών που έχει δώσει ο χρήστης (DTBS – Data To Be Signed). Έπειτα την μεταφέρει στην συσκευή. Και εδώ πρέπει να χρησιμοποιηθεί ένα έμπιστο μονοπάτι.

9. Η συσκευή δημιουργεί την ηλεκτρονική υπογραφή με τα δεδομένα δημιουργίας υπογραφής και την σύνοψη.

10. Η ηλεκτρονική υπογραφή μεταφέρεται στο σύστημα από την συσκευή. Σύμφωνα με το σχήμα 13 και εδώ πρέπει η διεπαφή της μεταφοράς να χαρακτηρίζεται από ασφάλεια.

11. Το σύστημα μορφοποιεί την υπογραφή ανάλογα με τις απαιτήσεις του χρήστη.

12. Το σύστημα παρουσιάζει την υπογραφή και τα δεδομένα στον χρήστη, ώστε να έχει μία τελική έγκριση, πριν την αποστολή τους από την σύστημα.

13. Τα δεδομένα και η υπογραφή αποστέλλονται από το σύστημα στον παραλήπτη τους.

14. Προαιρετικά, η όλη συναλλαγή καταγράφεται, σε κάποιο αρχείο (log).

15. Το σύστημα τίθεται στην αρχική του κατάσταση, σβήνοντας όλα τα δεδομένα τα οποία δημιουργήθηκαν από την διαδικασία της υπογραφής. Κάτι τέτοιο πιθανότατα θα γίνεται με την απομάκρυνση της συσκευής.

Όπως προαναφέραμε, οι διατάξεις δημιουργίας υπογραφής έχουν ιδιότυπα χαρακτηριστικά ασφαλείας τα οποία είναι σε άμεση συνάρτηση με το περιβάλλον τους. Στο **[SSCS,2000]**, διακρίνονται δύο περιπτώσεις, για χάρη γενικότητας.

- Το περιβάλλον δημιουργίας υπογραφής είναι υπό τον πλήρη έλεγχο του υπογράφοντα. Μία τέτοια περίπτωση, μπορεί να συναντήσει κανείς στην περίπτωση που η διαδικασία της υπογραφής γίνεται στον υπολογιστή του υπογράφοντα στον οποίο έχει κάποια σχετική εμπιστοσύνη.
- Το περιβάλλον δημιουργίας υπογραφής βρίσκεται σε κάποιον εξωτερικό χώρο και χρησιμοποιείται κάποιο μηχάνημα τύπου ATM. Είναι προφανές, ότι στην δεύτερη περίπτωση οι απαιτήσεις ασφαλείας του συστήματος είναι πάρα πολύ ανώτερες από αυτή του ελεγχόμενου περιβάλλοντος.

Αξίζει να παρατηρήσουμε πάντως ότι οι συνολικές απαιτήσεις ασφαλείας παραμένουν ίδιες ανεξάρτητα από το περιβάλλον. Το μόνο στο οποίο έχει επίδραση το περιβάλλον είναι ο τρόπος υλοποίησης τους. Οι απειλές προς το ιδιωτικό κλειδί (από τις οποίες θα προκύψουν οι απαιτήσεις ασφαλείας) μπορούν

να ταξινομηθούν σε τρείς κατηγορίες:

- Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα δημιουργίας υπογραφής. Πρέπει κατά συνέπεια να υπάρχει έλεγχος προσπέλασης με βάση κάποιο PIN ή πιο αυστηρά με κάποια βιομετρική μέθοδο.
- Θεωρητική κρυπτογραφική επίθεση που βασίζεται αδυναμίες αλγορίθμων, πρωτοκόλλων, μήκους κλειδιών.
- Απόσπαση με του ιδιωτικού κλειδιού, με 'αθέμιστα' μέσα όπως για παράδειγμα το φαινόμενο van Eck.

Μία άλλη μελέτη μπορεί να βρεθεί στο **[Schneier, 1999],** όπου συζητώνται οι επιπτώσεις που έχει στην συνολική ασφάλεια του συστήματος η κατανεμημένη φύση του περιβάλλοντος λειτουργίας στην συγκεκριμένη περίπτωση μιας έξυπνης κάρτας.

Συγκεκριμένα σε ένα τέτοιο περιβάλλον λαμβάνουν μέρος οι εξής οντότητες:

- **Ο κάτοχος της κάρτας (cardholder):** Είναι η οντότητα η οποία έχει στην κατοχή της την κάρτα σε καθημερινή βάση και αυτός που αποφασίζει πότε θα την χρησιμοποιήσει. Μπορεί να ελέγχει τα δεδομένα της κάρτας, αλλά δεν ελέγχει ούτε το λογισμικό της, ούτε το υλικό της, ούτε τα πρωτόκολλα με τα οποία αυτή επικοινωνεί με τον έξω κόσμο.
- **Ο ιδιοκτήτης των δεδομένων της κάρτας (data owner):** Πολλές φορές ταυτίζεται με τον κάτοχο της κάρτας. Αυτό ισχύει σε περιπτώσεις, όπως αυτή των ηλεκτρονικών υπογραφών, όπου ο κάτοχος είναι και ιδιοκτήτης του ιδιωτικού κλειδιού, αλλά όχι πάντα (για παράδειγμα δεν ισχύει στην περίπτωση του ηλεκτρονικού χρήματος).
- **Το τερματικό:** Είναι το σύστημα μέσω της οποία επικοινωνεί η κάρτα με το περιβάλλον της, τόσο με τον κάτοχο της όσο και με άλλες υπηρεσίες, τόσο για να λάβει όσο και για να στείλει δεδομένα.
- **Η εκδούσα αρχή της κάρτας:** Είναι η οντότητα που έχει εκδώσει την κάρτα και κατά συνέπεια ελέγχει το λειτουργικό σύστημα και τα αρχικά περιεχόμενα της κάρτας. Ανάλογα με την περίσταση ελέγχει και αρκετές από τις εφαρμογές που εκτελούνται στην κάρτα.
- **Ο κατασκευαστής της κάρτας:** Είναι η οντότητα η οποία ελέγχει το υλικό και έχει κατασκευάσει την κάρτα. Αυτό βέβαια είναι μία απλοϊκή θεώρηση καθώς αυτός ο κατασκευαστής μπορεί να είναι στην ουσία μόνο προμηθευτής και η πραγματική δημιουργία να έχει δοθεί σε κάποιον τρίτο εργολάβο.
- **Ο κατασκευαστής του λογισμικού της κάρτας:** Σε αυτή την ενότητα εντάσσουμε όλες τις οντότητες οι οποίες κατασκευάζουν λογισμικό το οποίο εκτελείται σε μία έξυπνη κάρτα. Καθώς είναι τεχνολογικά εφικτό μία κάρτα να φορτώνει δυναμικά εφαρμογές από το τερματικό στο οποίο έχει αρχικά εγκατασταθεί, καταλαβαίνουμε πώς εδώ ανήκουν πάρα πολλοί διαφορετικοί φορείς.

Βέβαια, όπως είδαμε, πολλές φορές ορισμένες από τις παραπάνω οντότητες ταυτίζονται στην πράξη. Ο εννοιολογικός όμως διαχωρισμός τους είναι απαραίτητος για την κατανόηση των ιδιαίτερων κινδύνων που συναντά κανείς σε ένα τέτοιο κατανεμημένο περιβάλλον. Αυτό συμβαίνει καθώς δεν θα πρέπει καμία από αυτές τις οντότητες να εμπιστεύεται την άλλη. Εκτός από αυτό, μπορεί και εξωτερικές οντότητες οι

οποίες, να προσπαθήσουν να εξαπατήσουν μία ή περισσότερες από τις προαναφερθείσες. Είναι αποδεκτό πάντως πως σε κάθε περίπτωση ο εξωτερικός επιτιθέμενος, έχει λιγότερες πιθανότητες επιτυχίας και πιο δύσκολη αποστολή, όπως άλλωστε συμβαίνει και σε όλα τα θέματα ασφαλείας.

Οι πιο σημαντικές λοιπόν απαιτήσεις ασφαλείας που συναντάει κανείς σε ένα τέτοιο περιβάλλον είναι οι εξής:

Η διεπαφή μεταξύ της συσκευής και του συστήματος πρέπει να είναι ασφαλής. Με άλλα λόγια δεν θα πρέπει να αλλοιωθούν ή να διαρρεύσουν τα δεδομένα που ανταλλάσσονται μεταξύ τους (το PIN ή τα βιομετρικά δεδομένα αυθεντικοποίησης του χρήστη, η σύνοψη η οποία θα υπογραφεί κτλ.). Για τον λόγο αυτό καλό θα είναι η μετάδοση μέσω της διεπαφής να είναι σε κρυπτογραφημένη μορφή. Επιπλέον τα συγκεκριμένα δεδομένα πρέπει να διαγράφονται από την μνήμη του συστήματος αμέσως μόλις περάσει η περίοδος χρήσης τους. Κάτι τέτοιο πρέπει να ισχύει ειδικά στην περίπτωση που το σύστημα δεν είναι υπό τον έλεγχο του χρήστη, βρίσκεται δηλαδή σε δημόσιο χώρο. Σε μία τέτοια περίπτωση η συγκεκριμένη απαίτηση, λαμβάνει και μία διαφορετική διάσταση, πρέπει να υπάρξει προστασία και από εξωτερικές οντότητες, οι οποίες μπορεί να παράδειγμα να παρακολουθούν το PIN του χρήστη.

Το σύστημα σε περίπτωση μάλιστα που έχει τοποθετηθεί σε δημόσιο χώρο και άρα είναι εκτεθειμένο σε ένα σύνολο από κινδύνους πρέπει να προστατεύει το έμπιστο συστατικό του ακόμα και σε περίπτωση που υπάρχει ‘βίαιη’ επίθεση εναντίον του. Επίσης θα πρέπει να προστατεύεται από τυχούσα επίθεση ιών και άλλων κινδύνων προς το λογισμικό. Για τον σκοπό αυτό καλό θα είναι οι περισσότερες δυνατόν λειτουργίες να εκτελούνται από υλικό.

Ο χρήστης – υπογράφων πρέπει να είναι σίγουρος ότι υπέγραψε αυτό που θεωρεί ότι υπέγραψε. Κατά συνέπεια πρέπει να βλέπει το κείμενο και τις λοιπές ιδιότητες του πριν και μετά την υπογραφή. Για τον λόγο αυτό στο *σχήμα 14* η επισκόπηση τόσο του κειμένου όσο και των λοιπών επιλογών έχει τοποθετηθεί στο έμπιστο υποσύστημα. Επίσης πρέπει να διασφαλιστεί ότι αυτό που βλέπει ο χρήστης, παρουσιάζεται με την σωστή μορφοποίηση, έτσι ώστε να είναι αναγνώσιμο. Παρ’ όλα αυτά το σύστημα πρέπει να προειδοποιεί τον χρήστη για την εισαγωγή εντολών μορφοποίησης στο κείμενο.

Πολύ σημασία πρέπει να δοθεί επίσης στο περιβάλλον διεπαφής με τον χρήστη. Θα έλεγε κανείς ότι η συγκεκριμένη απαίτηση είναι λειτουργική, στην πραγματικότητα όμως πρόκειται για απαίτηση ασφάλειας, καθώς ένα σωστά σχεδιασμένο περιβάλλον διεπαφής με τον χρήστη θα οδηγήσει σε λιγότερα πιθανά λάθη, αλλά και θα διευκολύνει την χρήση του συστήματος. Μία σημαντική απαίτηση που πρέπει να ικανοποιείται είναι η δυνατότητα για χρήση του και από άτομα με ειδικές ανάγκες. Επίσης το σύστημα διεπαφής και η διαδικασία υπογραφής όπως αυτή παρουσιάζεται μέσω του συστήματος διεπαφής πρέπει να είναι η ίδια ανεξάρτητα από τερματικό που χρησιμοποιείται.

Εκτιμάται [**SSCS,2000**] ότι λόγω της πολυπλοκότητας του συστήματος παρουσιάσαμε στην συγκεκριμένη ενότητα, δεν συμφέρει η διαπίστευση του με βάση κάποια κριτήρια συμμόρφωσης για τις διατάξεις τουλάχιστον που δεν πρέπει να ικανοποιούν συγκεκριμένες νομικές συνθήκες (όπως αυτές της Ευρωπαϊκής Οδηγίας). Η λύση που μάλλον θα εφαρμοστεί στην πράξη αφορά δηλώσεις συμμόρφωσης των

κατασκευαστών υλικού / λογισμικού. Κάτι τέτοιο βέβαια δεν ισχύει στην περίπτωση της ίδιας της διάταξης. Οι φορείς της EESSI που έχουν αναλάβει την συγκεκριμένη προτυποποίηση έχουν καταλήξει σε δύο προφίλ προστασίας κατά Common Criteria. Το ένα θέτει ως επίπεδο αποτίμησης το EAL 4, ενώ το άλλο, το οποίο ονομάζεται επαυξημένο, θέτει κάποιες αυξημένες απαιτήσεις σε θέματα ανάλυσης αδυναμιών (vulnerability analysis - οικογένειες AVA_VLA και AVA_MSU του Common Criteria). Στην άποψη που θεωρούσε ως απαραίτητο το EAL4, στην ανάλυση αδυναμιών υπήρχε η απαιτήση AVA_VLA.2 ενώ στο επαυξημένο EAL4, υπήρξε η άποψη ότι η συγκεκριμένη απαίτηση έπρεπε να είναι η AVA_VLA.4. Η διαφορά των απαιτήσεων είναι ότι η AVA_VLA.2, υποθέτει ότι ο επιτιθέμενος έχει μικρές πιθανότητες επιτυχίες, λίγο χρόνο στην διάθεση του και γενικότερα περιορισμένες δυνατότητες. Αντίθετα η AVA_VLA.4, υποθέτει έναν επιτιθέμενο με καλύτερες πιθανότητες και κάποια επιπλέον τεκμηρίωση. Η AVA_MSU, αφορά την επικύρωση της ανάλυσης αδυναμιών.

3.8 Μοντελοποίηση Επαλήθευσης Υπογραφής

Στην προηγούμενη περιγραφή μας, έχουμε αφήσει πολλά κενά σημεία σχετικά με τις διαδικασίες επαλήθευσης ηλεκτρονικών υπογραφών. Στην ενότητα αυτή θα επιχειρήσουμε να καλύψουμε τα σημεία αυτά παρέχοντας μία μοντελοποίηση της διαδικασίας των συστημάτων και του περιβάλλοντος επαλήθευσης ηλεκτρονικών υπογραφών. Για τον σκοπό αυτό θα ακολουθήσουμε την προσέγγιση του **[PESV, 2000]**. Η συγκεκριμένη διαδικασία έχει, όπως θα δούμε πολύ στενή σχέση με την ακριβή μορφή της ηλεκτρονικής υπογραφής, η οποία αναπτύχθηκε σε προηγούμενη παράγραφο.

Η διαδικασία επαλήθευσης μιας ηλεκτρονικής υπογραφής μπορεί να γίνει με 2 τρόπους:

- Από έναν χρήστη, ο οποίος έχει λάβει μία ηλεκτρονική υπογραφή και χρησιμοποιεί ένα υπολογιστή και το κατάλληλο λογισμικό για να την επαληθεύσει.
- Από ένα πρόγραμμα το οποίο με αυτοματοποιημένες διαδικασίες επαληθεύει ηλεκτρονικές υπογραφές, χωρίς να απαιτείται η παρέμβαση του χρήστη. Η συγκεκριμένη διαδικασία πιθανότατα να έχει ενεργοποιηθεί και ρυθμιστεί την πρώτη φορά από κάποιον χρήστη, αλλά γενικά δεν απαιτείται η παρέμβαση του κάθε φορά που γίνεται η επαλήθευση της υπογραφής.

Επιπλέον μπορούν να θεωρηθούν δύο περιπτώσεις επαλήθευσης υπογραφής:

- *Αρχική:* Γίνεται μετά την δημιουργία της υπογραφής με στόχο την απόδειξη της εγκυρότητας της υπογραφής. Ένας δεύτερος στόχος αποτελεί η συλλογή στοιχείων τα οποία θα χρησιμοποιηθούν στην συνήθη επαλήθευση, τον δεύτερο τύπο επαλήθευσης. Η διαδικασία αρχικής επαλήθευσης έχει τρία δυνατά αποτελέσματα:
    - *Επιτυχής Επαλήθευση*: Η ηλεκτρονική υπογραφή είναι τεχνικά έγκυρη και τηρεί την πολιτική υπογραφής.
    - *Ανεπιτυχής επαλήθευση*: Γενικά σημαίνει ότι η ηλεκτρονική υπογραφή δεν επαληθεύεται τεχνικά ή δεν ακολουθεί την πολιτική επαλήθευσης. Αυτό συμβαίνει για παράδειγμα αν έχει ανακληθεί

το πιστοποιητικό του υπογράφοντα, αν δεν υπάρξει ταύτιση των συνάψεων στις διάφορες συγκρίσεις, ακόμα όμως και αν δεν ακολουθείται μια συγκεκριμένη μορφή.

- *Μη πλήρης επαλήθευση*: Το συγκεκριμένο αποτέλεσμα δεν δείχνει κατ' ανάγκη ότι οι έλεγχοι μορφής και επαλήθευσης έχουν αποτύχει, αλλά ότι δεν υπάρχει επαρκής πληροφορία, έτσι ώστε να αποφανθούμε για το αν μια ηλεκτρονική υπογραφή είναι έγκυρη ή όχι. Για παράδειγμα, ένα τέτοιο αποτέλεσμα μπορεί να προκύψει αν όλοι οι έλεγχοι αποδειχτούν σωστοί, χωρίς όμως να είναι διαθέσιμη η τελευταία έκδοση της λίστας ανάκλησης πιστοποιητικών.

- *Συνήθης:* Γίνεται αρκετό καιρό μετά την δημιουργία της υπογραφής και δεν πρέπει να απαιτεί επιπλέον δεδομένα από αυτά που ήταν διαθέσιμα κατά την δημιουργία της υπογραφής. Η συνήθης επαλήθευση έχει δύο δυνατά αποτελέσματα:
  - *Επιτυχής Επαλήθευση:* η ηλεκτρονική υπογραφή συμφωνεί με την πολιτική υπογραφής και κατά συνέπεια θεωρείται έγκυρη.
  - *Ανεπιτυχής Επαλήθευση:* υπάρχει ασυμφωνία μεταξύ των αποτελεσμάτων της επαλήθευσης και της πολιτικής υπογραφής.

  Είναι προφανές, ότι στην συνήθη επαλήθευση μιας υπογραφής δεν υπάρχει περίπτωση η τεχνική επαλήθευση της υπογραφής (όπως την περιγράψαμε στο κεφάλαιο 2) να αποτύχει, καθώς έχει ήδη προηγηθεί η αρχική επαλήθευση. Επίσης δεν υπάρχει περίπτωση μη διαθεσιμότητας κάποιας πληροφορίας, όπως για παράδειγμα κάποιο πιστοποιητικό γιατί όλα αυτά έχουν συλλεχθεί στην αρχική επαλήθευση.

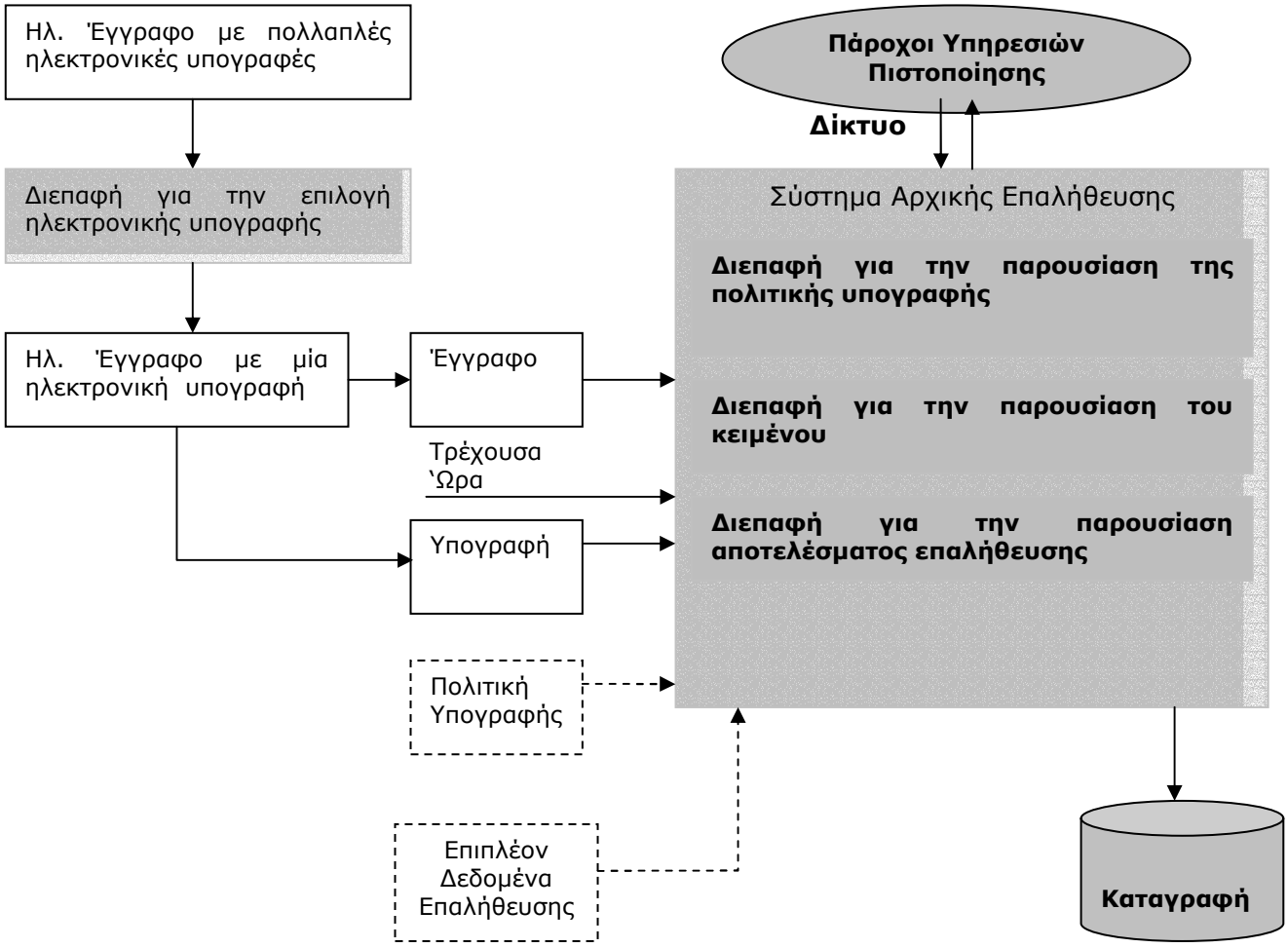
Όπως προαναφέραμε, ο υπογράφων παρέχει τουλάχιστον την ηλεκτρονική υπογραφή, της οποίας η μορφή μπορεί να χρησιμοποιηθεί για την αρχική επαλήθευση. Τα απαραίτητα στοιχεία για την συνήθη επαλήθευση της υπογραφής μπορούν να συλλεχθούν από τον επαληθεύοντα, κατά την πρώτη επαλήθευση. Η συνήθης επαλήθευση είναι απαραίτητη στην περίπτωση που απαιτηθεί επέμβαση κάποιου διαιτητή (arbitrator) για την επίλυση μιας διαφωνίας (dispute settlement) που θα προκύψει από την επαλήθευση της υπογραφής. Κατά συνέπεια, η πιο σημαντική απαίτηση της διαδικασίας επαλήθευσης μιας ηλεκτρονικής υπογραφής αφορά την δυνατότητα για εξαγωγή του ίδιου συμπεράσματος σχετικά με την ισχύ μίας υπογραφής από δύο ανεξάρτητους 'επαληθεύοντες'. Η βάση για την αντικειμενική επαλήθευση μιας υπογραφής είναι η πολιτική υπογραφής, που αναλύσαμε διεξοδικά νωρίτερα.

Επιπλέον απαιτήσεις ασφαλείας μπορούν να προκύψουν από μία αυστηρή μοντελοποίηση ενός συστήματος επαλήθευσης υπογραφής, το οποίο επιτελεί τις εξής λειτουργίες:

- Επιλογή του κειμένου και της υπογραφής που πρόκειται να επαληθευθούν.
- Παρουσίαση του κειμένου προς επαλήθευση στην κατάλληλη μορφή, ώστε να είναι αναγνώσιμο.
- Παρουσίαση των στοιχείων του υπογράφοντα και του αποτελέσματος της επαλήθευσης.
- Συλλογή στοιχείων για μακροπρόθεσμη / συνήθη επαλήθευση.
- Συλλογή πληροφοριών από διάφορους παρόχους υπηρεσιών πιστοποίησης. Οι πληροφορίες αυτές

αφορούν κυρίως την εγκυρότητα των πιστοποιητικών.

Με βάση τις παραπάνω λειτουργίες μπορούμε να εξάγουμε προδιαγραφές για την γενική μορφή ενός συστήματος επαλήθευσης υπογραφής:



Σχήμα 15. Σύστημα Επαλήθευσης Υπογραφής

Στο παραπάνω σχήμα, απεικονίζεται ένα σύστημα το οποίο μπορεί να χρησιμοποιηθεί για την αρχική επαλήθευση της ηλεκτρονικής υπογραφής. Σε αυτό αξίζει να επισημάνουμε ότι η πολιτική υπογραφής μπορεί είτε να προσδιορίζεται έμμεσα από το περιεχόμενο του κειμένου ή να αναφέρεται μέσω κάποιας αναφοράς, οπότε πρέπει να υπάρξει ανάκτηση της. Ένα από τα πιο σημαντικά συστατικά του όλου συστήματος είναι η διεπαφή παρουσίασης του κειμένου στον χρήστη, καθώς εδώ ισχύει το *WIPIWIS* (*What Is Presented Is What Is Signed*, κατ' αναλογία με το WYSIWIS – *What You See Is What Is Signed*). Μία από τις πιο σημαντικές απαιτήσεις ασφάλειας, κατά την επαλήθευση των ηλεκτρονικών υπογραφών είναι η ρητή και άμεση αναφορά στον χρήστη, του οποιουδήποτε προβλήματος για εμφάνισης του κειμένου στην μορφή που το παρέδωσε ο υπογράφοντας.

Πιο συγκεκριμένα οι απαιτήσεις διεπαφής με τον χρήστη για ένα τέτοιο σύστημα είναι οι εξής:

- Παροχή αναλυτικής καθοδήγησης στον χρήστη για την χρήση, εγκατάσταση και διαμόρφωση του

συστήματος.

- Παροχή ενός περιβάλλοντος το οποίο είναι απλό στην χρήση και αυτό – περιγραφόμενο (self – descriptive).
- Ανοχή σε λάθη από την μεριά του χρήστη, ιδιαίτερα αυτά τα οποία γίνονται κατά την εισαγωγή στοιχείων. Ταυτόχρονα πρέπει να παρέχει πληροφόρηση για το αν μια ενέργεια του χρήστη είναι σωστή ή λανθασμένη.
- Παροχή ισότιμης πρόσβασης σε όλους τους χρήστες, ανεξάρτητα από το αν αυτοί το χρησιμοποιούν για πρώτη φορά, ή αν έχουν ειδικές ανάγκες.

Καταλαβαίνουμε λοιπόν πόσο δύσκολος είναι ο σχεδιασμός και η υλοποίηση ενός τέτοιου συστήματος διεπαφής, με δεδομένο μάλιστα το γεγονός ότι πολλά απλούστερα και λιγότερο κρίσιμα συστήματα, αποτυγχάνουν παταγωδώς στον συγκεκριμένο τομέα.

Το σύστημα διεπαφής είναι χρήσιμο μόνο στην πρώτη περίπτωση επαλήθευσης υπογραφής που προαναφέραμε, όταν αυτή δηλαδή γίνεται από μία ανθρώπινη οντότητα. Σε περίπτωση που η όλη διαδικασία είναι αυτοματοποιημένη, το σύστημα επαλήθευσης υπογραφής θα προσφέρει μία *Διεπαφή Προγραμματισμού Εφαρμογών* (*Application Programming Interface*) έτσι ώστε άλλες εφαρμογές να φτιαχτούν σε αυτό.

Στην πράξη ένα σύστημα για την συνήθη επαλήθευση υπογραφής, διαφοροποιείται στα εξής σημεία:

- Δεν χρειάζεται αλληλεπίδραση με παρόχους υπηρεσιών πιστοποίησης, καθώς όπως προαναφέραμε θα είναι διαθέσιμα δεδομένα επαλήθευσης τα οποία θα παρέχουν ένα πλήρες στιγμιότυπο της υποδομής δημοσίου κλειδιού κατά την ώρα της δημιουργίας ή πρώτης επαλήθευσης της υπογραφής.
- Η αλληλεπίδραση με την βάση δεδομένων καταγραφής θα είναι αμφίδρομη, καθώς θα υπάρχει ανάγκη και για ανάκτηση δεδομένων για την αρχική επαλήθευση (χρονικός προσδιορισμός, αποτελέσματα κτλ.)

Κλείνοντας την επισκόπηση της επαλήθευσης υπογραφής θα αναφερθούμε στο περιβάλλον στο οποίο αυτή γίνεται. Η επαλήθευση μιας ηλεκτρονικής υπογραφής από κάποιον χρήστη μπορεί να γίνει σε 4 διαφορετικά περιβάλλοντα, τα οποία και περιγράφονται παρακάτω. Εκ των προτέρων πάντως θεωρούμε ότι παρόλο που ορισμένα από αυτά τα περιβάλλοντα, μπορεί να φαίνονται πιο επικίνδυνα από τα άλλα κάτι τέτοιο δεν ισχύει στην πράξη:

- *Οικιακό Περιβάλλον*. Το συγκεκριμένο περιβάλλον ίσως θεωρηθεί το πιο ασφαλές, καθώς χρησιμοποιείται εξοπλισμός που έχει επιλέξει ο ίδιος ο χρήστης, στον δικό του χώρο. Συνήθως στην συγκεκριμένη περίπτωση το λογισμικό που χρησιμοποιείται είναι αγορασμένο (*COTS – Common Off The Shelf Software*). Για το συγκεκριμένο περιβάλλον θα μπορούσε να πει κανείς ότι δίνει απατηλή αίσθηση ασφάλειας, καθώς ο χρήστης είναι υπεύθυνος αυτήν. Έτσι η ασφάλεια δεν βασίζεται σε συγκεκριμένες διαδικασίες, ούτε σε απόλυτα διαπιστευμένα προϊόντα. Ένα παράδειγμα το οποίο συνηγορεί σε αυτό είναι η ευκολία διάδοσης ιών βλέπει

συχνά το φως της δημοσιότητας. Επιπλέον τα περισσότερα πακέτα λογισμικού *COTS* δεν φημίζονται και για την αξιοπιστία τους.

- *Περιβάλλον Εργασίας*: το συγκεκριμένο περιβάλλον μοιάζει σε αρκετά σημεία με το προηγούμενο, κυρίως σε ότι αφορά την εμπιστοσύνη που δείχνει ο χρήστης στον εξοπλισμό, λόγω της καθημερινής επαφή του. Εδώ όμως δεν είναι ο ίδιος αποκλειστικά υπεύθυνος για την διαμόρφωση αλλά και όλες τις πτυχές χρήσης του συγκεκριμένου περιβάλλοντος. Αυτό είναι θετικό, αν ο οργανισμός ακολουθεί σωστές διαδικασίες με βάση μία καλά καθορισμένη πολιτική ασφαλείας, ενώ σε αντίθετη περίπτωση ίσως θα ήταν καλύτερα να αφεθεί η όλη διαδικασία στον χρήστη. Το παράδειγμα των ιών ισχύει και εδώ, και παρατηρείται με μεγαλύτερη ένταση και μεγαλύτερες συνέπειες.
- *'Κινητό' Περιβάλλον*: Στο συγκεκριμένο περιβάλλον χρησιμοποιείται κάποιο κινητό τηλέφωνο ή κάποιο PDA για την επαλήθευση της υπογραφής. Θα έλεγε κανείς ότι πέρα από το ασύρματο περιβάλλον, ο μεγαλύτερος κίνδυνος αφορά την απώλεια ή κλοπή του εξοπλισμού επαλήθευσης.
- *Δημόσιο Περιβάλλον*. Στο συγκεκριμένο περιβάλλον η χρήση ενός συστήματος επαλήθευσης υπογραφής μπορεί να χαρακτηριστεί ως περιστασιακή καθώς δεν χρησιμοποιείται πάντοτε ο ίδιος εξοπλισμός επαλήθευσης. Εδώ βέβαια σίγουρα θα έχουν τηρηθεί κάποιες διαδικασίες κατά την εγκατάσταση του εξοπλισμού, υπάρχουν όμως πολύ σημαντικοί κίνδυνοι, οι οποίοι δεν συναντώνται σε άλλα περιβάλλοντα, όπως για παράδειγμα το τερματικό επαλήθευσης υπογραφής να είναι ψεύτικο, δηλαδή να μην ανήκει σε κάποια εταιρεία. Πάντως θεωρούμε ότι η χρήση διατάξεων επαλήθευσης υπογραφής σε ένα τέτοιο περιβάλλον είναι αρκετά απίθανη.

3.9 Συμπεράσματα

Το κεφάλαιο αυτό μπορεί να χαρακτηριστεί λίγο ιδιόμορφο, καθώς ασχολήθηκε με τρία διαφορετικά θέματα. Αρχικά δώσαμε ένα περιβάλλον στις τεχνολογίες ηλεκτρονικών υπογραφών μέσω της πολιτικής πιστοποίησης, της δήλωσης πρακτικών πιστοποίησης και της πολιτικής υπογραφής. Εδώ μπορούμε να σχολιάσουμε τα εξής: Πρώτα από όλα, το γεγονός ότι αρχικά η δήλωση πρακτικών πιστοποίησης αποτελούσε το βασικό μέσο επίλυσης διαφορών μεταξύ χρηστών και αρχής πιστοποίησης κάτι που ισοδυναμούσε με την απόρριψη από τις αρχές πιστοποίησης κάθε ευθύνης. Το παράδοξο εδώ είναι ότι η αποποίηση της ευθύνης αυτής δεν αφορούσε κάτι που μπορούσε να πάει γενικώς στραβά στο όλο περιβάλλον. Αφορούσε την ακρίβεια των περιεχομένων του πιστοποιητικού, δηλαδή την ίδια την ουσία του ρόλου που επιτελούσε η αρχή πιστοποίησης στην όλη υποδομή δημοσίου κλειδιού. Αυτό αν και απαράδεκτο είναι συνέπεια δύο παραγόντων, αφενός της απουσίας νομικού πλαισίου (και κατ'επέκταση κυρώσεων) και αφετέρου την προσπάθεια για μείωση επιπλέον κόστους από αυτό που απαιτείται για την δημιουργία μιας βιώσιμης αρχής πιστοποίησης. Επίσης, αξίζει να αναφερθούμε στην πολυπλοκότητα υλοποίησης των εννοιών πολιτικής υπογραφής και πιστοποίησης, έννοιες που δεν υπάρχουν καν στην

συμβατική πραγματικότητα. Στο ηλεκτρονικό περιβάλλον η ανάγκη γι'αυτές προκύπτει από την ύπαρξη ολόκληρου μηχανισμού πιστοποίησης, που λειτουργεί ως ενδιάμεσος μεταξύ των συναλλασσόμενων μερών.

Έπειτα αναλύσαμε όλα τα συστήματα που χρησιμοποιούνται σε ένα περιβάλλον ηλεκτρονικών υπογραφών, θέτοντας και τις βάσεις για την αξιολόγηση των συστημάτων αυτών, μέσω απαιτήσεων ασφαλείας, αλλά και μέσω της παρουσίασης των πιο αποδεκτών προτύπων για την αξιολόγηση τους. Τα πρότυπα είναι χρήσιμα για τους πάροχους πιστοποίησης, καθώς μπορούν να μετατρέψουν τις απαιτήσεις ασφάλειας σε πολιτική πιστοποίησης, ενώ για τα υπόλοιπα συστήματα στα οποία το τεχνολογικό περιβάλλον δεν έχει ξεκαθαρίσει εντελώς, μπορεί να χρησιμεύσει για την δημιουργία ενός εννοιολογικού μοντέλου, το οποίο θα προωθήσει τις υπόλοιπες εξελίξεις. Η αξία των προτύπων στην πληροφορική και ειδικότερα στην ασφάλεια είναι γενικά αποδεκτή και έχει επισημανθεί από πολλούς, καθώς διαβεβαιώνει τους καταναλωτές για την ποιότητα των προϊόντων/συστημάτων και τους δίνει κριτήρια σύγκρισης. Επίσης βοηθά στην διαλειτουργικότητα των προϊόντων. Ιδιαίτερα όμως στην περίπτωση των ηλεκτρονικών υπογραφών όπου εμπλέκονται πολλά και διαφορετικά συστήματα, τα οποία δεν είναι αποκλειστικά τεχνικά και όπου η κρισιμότητα των εφαρμογών είναι πολύ μεγάλη, τα πρότυπα και ιδιαίτερα αυτά που σχετίζονται με την διαχείριση της ασφάλειας, μπορούν να χρησιμεύσουν και ως ένα μέσο για την ρύθμιση των παρόχων πιστοποίησης, των κατασκευαστών διατάξεων με απώτερο στόχο βέβαια την αποδοχή, την ευαισθητοποίηση και την διασφάλιση του τελικού χρήστη.

4 Νομοθετικά και Ρυθμιστικά Πλαίσια

4.1 Εισαγωγή

Στο κεφάλαιο αυτό θα δούμε πώς τίθενται οι προϋποθέσεις για την χρήση των ηλεκτρονικών υπογραφών και των υπηρεσιών πιστοποίησης στον πραγματικό κόσμο. Όπως προέκυψε από το προηγούμενο κεφάλαιο για την αποτελεσματική εφαρμογή των τεχνικών λύσεων ηλεκτρονικής αυθεντικοποίησης και υπογραφής απαιτείται η συμμετοχή ενός 'ανώτερου επίπεδου', το οποίο θα παρέχει λύσεις στα θέματα που δεν επιλύονται τεχνικά, ή θα παρέχει τις εγγυήσεις εκείνες που χρειάζονται για την ανάπτυξη της υποδομής. Ένας τρόπος με τον οποίο μπορεί να γίνει αυτό, είναι μέσω ενεργειών νομικών και ρυθμιστικών σωμάτων. Αν θέλουμε να δούμε το θέμα γενικά θα πρέπει να παρατηρήσουμε ότι όλες οι προσεγγίσεις στον συγκεκριμένο τομέα επικεντρώνονται σε δύο σημεία. Αφενός δίνουν κάποια αναγνώριση στις ψηφιακές ή ηλεκτρονικές υπογραφές, ή σε κάποια μορφή αυτών που πληρεί κάποια κριτήρια ασφάλειας και αφετέρου θέτουν προϋποθέσεις λειτουργίας της υποδομής ηλεκτρονικών υπογραφών χρησιμοποιώντας πρότυπα όπως αυτά που αναφέραμε στις προηγούμενες ενότητες. Η εφαρμογή των προτύπων αυτών εξασφαλίζεται με έννοιες όπως η πιστοποίηση/διαπίστευση και η εποπτεία. Στο παραπάνω γενικό σχήμα υπάρχουν βέβαια και εξαιρέσεις τις οποίες και θα παραθέσουμε. Θα ξεκινήσουμε την περιγραφή μας με τις πρώτες προσπάθειες, οι οποίες έχουν εκδωθεί από ρυθμιστικούς οργανισμούς. Το μεγαλύτερο τμήμα του κεφαλαίου θα αφιερωθεί στην ευρωπαϊκή προσέγγιση, όπως αυτή έχει εκφραστεί μέσω της οδηγίας, αλλά και μέσω της εμηνείας της από διάφορες χώρες. Τέλος θα αναλύσουμε αντίστοιχες προσπάθειες σε άλλες ανεπτυγμένες χώρες, όπως οι ΗΠΑ, ο Καναδάς και η Αυστραλία.

4.2 Οι πρώτες προσεγγίσεις

Οι πρώτες προσπάθειες για την ρύθμιση του περιβάλλοντος των ηλεκτρονικών υπογραφών έγιναν στα μέσα τις δεκαετίας του 1990, από διεθνείς οργανισμούς, όπως ο Ο.Η.Ε. Αν και οι προσπάθειες αυτές είχαν την μορφή συστάσεων ή πρότυπων νόμων, κάτι που σημαίνει πώς δεν υπήρχαν και πολλά περιθώρια πρακτικής εφαρμογής, είναι σημαντικές καθώς αποτέλεσαν την βάση για τις μετέπειτα νομοθετικές προσπάθειες. Στην ενότητα αυτή θα εξετάσουμε τις πιο σημαντικές από τις αρχικές αυτές προσπάθειες, χωρίς να μπούμε σε πολλές λεπτομέρειες, καθώς αρκετά από τα στοιχεία που εισήγαγαν συναντώνται στις προσπάθειες τις οποίες θα εξετάσουμε αργότερα.

Θα ξεκινήσουμε από τις συστάσεις του ABA για τις ψηφιακές υπογραφές **[ABA, 1996]**. Όπως προαναφέραμε ο ABA είναι ο μεγαλύτερος δικηγορικός σύλλογος των ΗΠΑ και κατά συνέπεια ένας από τους μεγαλύτερους δικηγορικούς συλλόγους σε παγκόσμιο επίπεδο. Οι συγκεκριμένες συστάσεις έχουν επηρεάσει όλες τις νομικές προσπάθειες **[Ford, 2001].** Αναφέρεται μάλιστα, ανεπίσημα, ότι υπήρξε συνεργασία μεταξύ των επιτροπών που δημιούργησαν τις συγκεκριμένες συστάσεις και αυτών που

δημιουργήσαν την νομοθεσία της πολιτείας της Utah το 1995, του πρώτου νόμου παγκοσμίως για ψηφιακές υπογραφές.

Οι συγκεκριμένες συστάσεις καλύπτουν το βασικό κύκλωμα ηλεκτρονικών υπογραφών (βλ. *σχήμα 8*) χωρίς τον επόπτη και τον ελεγκτή. Αναφέρονται δηλαδή στον υπογράφοντα ή συνδρομητή υπηρεσιών πιστοποίησης, την αρχή πιστοποίησης και τον επαληθεύοντα. Οι συστάσεις ABA δεν αναφέρονται σε ηλεκτρονικές υπογραφές γενικά, αλλά σε ψηφιακές και στην υποδομή δημοσίου κλειδιού που τις συνοδεύει. Για τον λόγο αυτό, η συγκεκριμένη νομοθετική πράξη έχει χαρακτηριστεί ως ο *'νόμος του X.509'* **[Gutman, 2001]**.

Καλύπτουν έτσι την σχέση του υπογράφοντα με τις αρχές πιστοποίησης (δημιουργία κλειδιών, πιστοποίηση, προστασία ιδιωτικού κλειδιού, υπηρεσίες ανάκλησης) και θέτουν απαιτήσεις ασφαλείας για τις τελευταίες (χρήση αξιόπιστων συστημάτων, διαθεσιμότητα πιστοποιητικών, δήλωση πρακτικών πιστοποίησης, διαδικασίες πρόσληψης προσωπικού, διαδικασίες καταγραφής). Γίνεται επίσης προσπάθεια για την ρύθμιση της ευθύνης μεταξύ αρχής πιστοποίησης, συνδρομητή και επαληθεύοντα. Χαρακτηριστικό της προσπάθειας αυτής είναι το γεγονός ότι οι αρχές πιστοποίησης που τηρούν τις συγκεκριμένες συστάσεις δεν φέρουν καμία ευθύνη για οποιοδήποτε λάθος στα περιεχόμενα του πιστοποιητικού, κάτι που ισχύει και στην νομοθεσία της Utah. Σε περίπτωση λάθους οι τελικοί χρήστες αντιμετωπίζουν το κόστος. Αν και δεν συμφωνούμε με την συγκεκριμένη προσέγγιση, όπως θα εξετάσουμε παρακάτω, πρέπει να συνυπολογίσουμε τις συνέπειες που θα είχε στην ανάπτυξη των υπηρεσιών πιστοποίησης ακόμα και η ελάχιστη ευθύνη, στην πρώιμη εκείνη περίοδο.

Στον αντίποδα, μπορούμε να πούμε ότι βρίσκεται η προσπάθεια του ΟΗΕ, και συγκεκριμένα της επιτροπής του για το διεθνές εμπόριο – UNCITRAL, η έρευνα της οποίας έχει αποτυπωθεί σε δύο κείμενα: τον πρότυπο νόμο για το ηλεκτρονικό εμπόριο (1996) και τον πρότυπο νόμο για τις ηλεκτρονικές υπογραφές (2001). Κύριο χαρακτηριστικό της πρώτης προσπάθειας **[UNCITRAL, 1996]**, αποτελεί η τεχνολογική ουδετερότητα, καθώς δεν αναφέρεται σε συγκεκριμένη μορφή ή τεχνολογία ηλεκτρονικών υπογραφών. Όπως φαίνεται και από την ονομασία του, στόχος του είναι προωθήσει την διάδοση του ηλεκτρονικού εμπορίου απομακρύνοντας τους όποιους εθνικούς περιορισμούς. Όπως αναφέρεται στο **[Ford, 2001],** η συγκεκριμένη προσπάθεια έχει υιοθετηθεί αυτούσια από αρκετές χώρες όπως για παράδειγμα η Αργεντινή και Σιγκαπούρη και έχει επηρεάσει σε μεγάλο βαθμό προσπάθειες όπως αυτή του Καναδά, της Αυστραλίας της Γαλλίας κτλ.

Ο πρότυπος νόμος για τις ηλεκτρονικές υπογραφές δεν είναι μία πρώτη προσέγγιση. Αντίθετα έρχεται σε μία περίοδο, όπου οι περισσότερες χώρες έχουν ήδη θεσπίσει σχετικούς νόμους.'Εχει επηρεαστεί σημαντικά από την οδηγία της Ευρωπαϊκής Ένωσης. Κατά συνέπεια περισσότερο αποτελεί προσπάθεια εναρμόνισης **[UNCITRAL, 2001]** των ήδη υπάρχουσων πρωτοβουλιών, παρά δημιουργίας ενός νέου πλαισίου. Έτσι δεν υιοθετεί καμία συγκεκριμένη τεχνολογία δημιουργίας υπογραφής. Για να είμαστε πιο συγκεκριμένοι, τα περισσότερα άρθρα του έχουν διπλή προσέγγιση: αρχικά αναφέρουν τις γενικές απαιτήσεις που θα πρέπει να ισχύουν για ηλεκτρονικές υπογραφές και μετά τις προσαρμόζει σε περίπτωση

που υπάρχει χρήση πιστοποιητικών, χωρίς βέβαια να αναφέρεται καθόλου στην κρυπτογραφία δημοσίου κλειδιού και την ορολογία της.

Το βασικό στοιχείο του είναι ότι αναγνωρίζει την χρήση μιας ηλεκτρονικής υπογραφής για ένα μήνυμα δεδομένων, αν αυτή καλύπτει τις απαιτήσεις ασφαλείας και αξιοπιστίας που θέτει το μήνυμα. Επιπλέον, προδιαγράφει απαιτήσεις για τον υπογράφοντα, την αρχή πιστοποίησης αλλά και τον επαληθεύοντα.

Ο υπογράφων για παράδειγμα πρέπει:

- να δείχνει την απαραίτητη επιμέλεια για την προστασία των δεδομένων δημιουργίας υπογραφής,
- να προβεί σε άμεση ανάκληση ενός πιστοποιητικού και να γνωστοποιήσει σε οποιονδήποτε θεωρεί ότι βασίζεται στην ηλεκτρονική υπογραφή.
- να παρέχει με ακρίβεια όλα τα στοιχεία τα οποία θα ζητηθούν από την αρχή πιστοποίησης για την δημιουργία του πιστοποιητικού.

Ο επαληθεύων πρέπει:

- να προβαίνει στην επαλήθευση μιας υπογραφής με την τήρηση εύλογων μέτρων, όπως για παράδειγμα τον έλεγχο των πιστοποιητικών.
- να τηρεί τους περιορισμούς που αναγράφονται στο πιστοποιητικό.

Αντίστοιχες απαιτήσεις προδιαγράφονται και για την αρχή πιστοποίησης. Οι απαιτήσεις αυτές αποτελούν τμήμα αυτών που περιγράψαμε νωρίτερα και αφορούν την ποιότητα / αξιοπιστία των διαδικασιών και συστημάτων της, την ακρίβεια των δεδομένων του πιστοποιητικού και την διαθεσιμότητα πληροφορίας ανάκλησης. Δεν αναλύουμε τις παραπάνω πτυχές περισσότερο, καθώς αποτελούν μια σύνοψη των πιο σημαντικών ρυθμίσεων σε διεθνές επίπεδο, μέχρι σήμερα, με τις οποίες και θα ασχοληθούμε εκτενέστερα στην συνέχεια.

Η πιο σημαντική συνεισφορά κατά την γνώμη μας, της παραπάνω προσέγγισης, είναι ο διεθνής χαρακτήρας της, ο οποίος εκφράζεται στο τελευταίο άρθρο της και σύμφωνα με τον οποίο δεν πρέπει να υπάρχει συνάρτηση της νομικής αναγνώρισης μιας ηλεκτρονικής υπογραφής με την γεωγραφική τοποθεσία στην οποία δημιουργείται ή εκδίδεται το πιστοποιητικό. Αντίθετα αναγνωρίζεται η ισοδυναμία τους, αν παρέχεται βέβαια αξιοπιστία πιστοποιημένη με βάση διεθνή πρότυπα. Κάτι τέτοιο βέβαια είναι πολύ εύκολο να γραφεί σε έναν πρότυπο νόμο, όχι όμως τόσο εύκολο να εφαρμοστεί στην πράξη.

Ένα πολύ σημαντικό χαρακτηριστικό των προσπαθειών με τις οποίες ασχοληθήκαμε εδώ είναι ότι ακολουθούν την αρχή της *αντιστροφής του βάρους της απόδειξης (onus of proof)*. Η συγκεκριμένη αρχή θα αναλυθεί σε επόμενη ενότητα. Εισαγωγικά, αναφέρουμε τώρα ότι στην συμβατική υπογραφή, σε περίπτωση που υπάρξει αμφισβήτηση σχετικά με την εγκυρότητα της, τότε πρέπει ο επαληθεύων να αποδείξει ότι η υπογραφή είναι ψευδής. Αντίθετα και οι δύο παραπάνω προσπάθειες θεωρούν ότι ο υπογράφων πρέπει να αποδείξει ότι η υπογραφή δεν είναι έγκυρη, λόγω για παράδειγμα απώλειας του ιδιωτικού κλειδιού.

4.3 Η έννοια της διαπίστευσης

Η έννοια της διαπίστευσης, εξαρτάται σημαντικά από το περιβάλλον στο οποίο την ορίζουμε. Το περιβάλλον αυτό διαμορφώνεται κυρίως από κάποιο νομικό πλαίσιο, οπότε απαιτείται η επισκόπηση των πιο σημαντικών τέτοιων πλαισίων. Αυτό γίνεται καλύτερα κατανοητό αν αντιπαραβάλλουμε την έννοια της διαπίστευσης, όπως είναι ευρέως γνωστή, με τον τρόπο που την χρησιμοποιούμε στην συγκεκριμένη εργασία.

Έτσι η διαπίστευση 'παραδοσιακά' σημαίνει την παροχή επίσημης αναγνώρισης από κάποια κρατική ή παρόμοια οντότητα, σε έναν οργανισμό πιστοποίησης, σε έναν οργανισμό δηλαδή ο οποίος ελέγχει την συμμόρφωση με κάποιο πρότυπο. Αυτό δεν αφορά μόνο προϊόντα ή υπηρεσίες πληροφορικής, αλλά ισχύει για κάθε περιοχή προτυποποίησης. Αντίθετα στην συγκεκριμένη εργασία[3], ο όρος διαπίστευση αφορά την παροχή αναγνώρισης ή την έκδοση άδειας λειτουργίας ενός πάροχου υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών από ένα καθεστώς, με την ευρεία έννοια. Με απλά λόγια, με τον όρο διαπίστευση *δεν* εννοούμε την παροχή εξουσιοδότησης σε έναν ελεγκτικό φορέα, έτσι ώστε τα αποτελέσματα του ελέγχου συμμόρφωσης με κάποιο πρότυπο, να μην είναι αμφισβητήσιμα. Αντίθετα η έννοια της διαπίστευσης, όπως θα την χρησιμοποιήσουμε ταυτίζεται σχεδόν με την έννοια της πιστοποίησης. Όπως θα δούμε, η συγκεκριμένη έννοια είναι αυτή που χρησιμοποιείται στην ευρωπαϊκή οδηγία και στην όλη προσπάθεια προτυποποίησης που την συνοδεύει. Σε άλλα πλαίσια, όπως για παράδειγμα στον Καναδά και στις ΗΠΑ, η διαπίστευση αφορά κυρίως την τεχνική συμβατότητα της υποδομής δημοσίου κλειδιού ενός οργανισμού με την υποδομή που χρησιμοποιείται σε εθνικό επίπεδο, έτσι ώστε να μπορέσει να ο συγκεκριμένος οργανισμός να συνεργαστεί με την τελευταία. Όσο και αν φαίνεται περίεργο, οι δύο αυτοί ορισμοί δεν διαφέρουν ουσιαστικά, καθώς στον όρο τεχνική συμβατότητα εμπεριέχεται και η έννοια της πολιτικής πιστοποίησης, η οποία ουσιαστικά συνδέει ένα πιστοποιητικό με το περιβάλλον του. Η διαφορά είναι θέμα αρχής. Παρέχεται δηλαδή κάποια καθοδήγηση και επίβλεψη από τα κράτη, ή όλα αφήνονται στην τύχη της αγοράς, και το κράτος επεμβαίνει μόνο για να εξασφαλίσει την συμβατότητα;

Αναφέρονται γενικά οι εξής τρόποι ρυθμιστικής παρεμβασης μέσω της διαπίστευσης **[Aalberts, 1999]**:

- **Ορισμός Κυβερνητικού Ρυθμιστικού Σώματος (Government Regulation):** Η προσέγγιση αυτή θέλει τον ορισμό ενός κρατικού (κατά βάση) οργανισμού, ο οποίος αναλαμβάνει την διαπίστευση. Συνοδεύεται και με μεταρρύθιση του νομικού πλαισίου. Οι διατάξεις έχουν υποχρεωτικό χαρακτήρα. Είναι απαραίτητη σε περίπτωση που διακυβεύονται θεμελιώδη δικαιώματα των πολιτών, αλλά χαρακτηρίζεται ως δυσκίνητη. Αντιπροσωπευτικό παράδειγμα εφαρμογής της μεθόδου αυτής είναι η Γερμανία.

[3] Η χρήση της συγκεκριμένης ορολογίας, στο συγκεκριμένο σημείο και γενικά σε όλη την έκταση της εργασίας δεν είναι αυθαίρετη. Είναι σύμφωνη με την ορολογία που χρησιμοποιείται στην ευρωπαϊκή οδηγία [EDCF,1999] και στο ελληνικό προεδρικό διάταγμα.

- **Αυτό – ρύθμιση (self-regulation):** Κατά την προσέγγιση αυτή όλοι οι ενδιαφερόμενοι φορείς (κυρίως της αγοράς) συστήνουν έναν ανεξάρτητο οργανισμό, ο οποίος και αναλαμβάνει την διαπίστευση με βάση κυρίως τεχνικά πρότυπα. Η μέθοδος αυτή ακολουθήθηκε κυρίως στην Αγγλία. Οι υποστηρικτές της θεωρούν ότι προσαρμόζεται πιο εύκολα στις νέες τεχνολογικές εξελίξεις. Το μεγάλο της πλεονέκτημα όμως είναι ότι δεν περιορίζεται γεωγραφικά.
- **Συνδυασμός των παραπάνω (co-regulation):** Η συγκεκριμένη προσέγγιση θέλει την συνεργασία της αγοράς με κυβερνητικούς φορείς. Είναι η συμβιβαστική λύση η οποία έχει ως στόχο να συνδυάσει τα πλεονεκτήματα και των δύο παραπάνω.
- **Δήλωση Κατασκευαστή:** Η προσέγγιση αυτή μπορεί να ακολουθηθεί κυρίως για την διαπίστευση προϊόντων, οπότε έχει εφαρμογή σε όλα τα προϊόντα ηλεκτρονικών υπογραφών και είναι η πιο ελαφράς μορφή διαπίστευση. Αν και φαίνεται χαλαρή, είναι πολλές φορές χρήσιμη όταν η αγορά των συγκεκριμένων προϊόντων δεν έχει αναπτυχθεί ακόμα και το κόστος μιας πιο αυστηρής προσπάθειας είναι δυσανάλογο με τα πλεονεκτήματα που αυτή θα επιφέρει.

4.4 Η ευρωπαϊκή προσέγγιση

Η ευρωπαϊκή προσέγγιση σε ένα πλαίσιο για ηλεκτρονικές υπογραφές, εκφράζεται με την οδηγία του Δεκεμβρίου του 1999 **[EDCF, 1999].** Στην ενότητα αυτή θα συνοψίσουμε τα βασικά σημεία της. Η αναφορά μας δεν φιλοδοξεί να είναι πλήρης από νομική πλευρά. Στόχος μας είναι να αναδείξουμε την σχέση μεταξύ της τεχνικής υποδομής για ηλεκτρονικές υπογραφές και των απαιτήσεων που τίθενται για την ευρεία ανάπτυξη και χρήση τους σε όλες τις ηλεκτρονικές εκφάνσεις της καθημερινής ζωής για την αντικατάσταση της ιδιόχειρης υπογραφής. Στόχος της ευρωπαϊκής οδηγίας είναι η νομική αναγνώριση των ηλεκτρονικών υπογραφών και η παροχή των συνθηκών εκείνων που θα βοηθήσουν την ανάπτυξη της αγοράς των παρόχων υπηρεσιών πιστοποίησης. Εξ' αρχής πρέπει να τονίσουμε ότι η οδηγία εφαρμόζεται για την παροχή υπηρεσιών πιστοποίησης στο *ευρύ κοινό*, και δεν ισχύει σε περιπτώσεις όπου πτυχές της ηλεκτρονικής αυθεντικοποίησης καλύπτονται από κάποιο συμβόλαιο. Δηλαδή, αν ένας οργανισμός έχει αναπτύξει για εσωτερική χρήση υπηρεσίες ηλεκτρονικής αυθεντικοποίησης, τότε οι συγκεκριμένες υπηρεσίες εξαιρούνται από την εφαρμογή της οδηγίας. Το ίδιο συμβαίνει και για τις υπηρεσίες αυθεντικοποίησης που έχουν ιδιωτικά συμφωνήσει δύο οντότητες για να προχωρήσουν σε ηλεκτρονικές συναλλαγές μεταξύ τους. Επίσης αφορά περιπτώσεις όπου επιτρέπεται ήδη από τον εθνικό νόμο η χρήση ηλεκτρονικών εγγράφων. Δηλαδή δεν επιβάλλει την χρήση ηλεκτρονικών εγγράφων, έτσι ώστε να είναι δυνατή η εφαρμογή ηλεκτρονικών υπογραφών.

4.4.1 Ορισμός Ηλεκτρονικής Υπογραφής

Στην οδηγία αναφέρονται ρητά δύο τύποι ηλεκτρονικών υπογραφών, αλλά στην ουσία γίνεται λόγος για τρία είδη και κατά άλλους τέσσερα είδη. Αυτά είναι:

- **Ηλεκτρονική Υπογραφή**: Είναι οποιοδήποτε ηλεκτρονικό σύμβολο μπορεί να προσαρτηθεί σε κάποιο ηλεκτρονικό έγγραφο, έτσι ώστε να έχει συσχετισθεί με αυτό. Κατά συνέπεια, η οδηγία θεωρεί ότι ηλεκτρονική υπογραφή, αποτελεί ένα όνομα στο τέλος κάθε email, ή ακόμα και η ψηφιοποιημένη αναπαράσταση της ιδιόχειρης υπογραφής.
- **Προηγμένη Ηλεκτρονική Υπογραφή (Advanced Electronic Signature)**: Σύμφωνα με την οδηγία είναι μία ηλεκτρονική υπογραφή, η οποία έχει κάποιες επιπλέον ιδιότητες, όπως για παράδειγμα:
    - Συνδέεται μοναδικά με τον υπογράφοντα.
    - Μπορεί να ταυτοποιήσει μοναδικά τον υπογράφοντα.
    - Δημιουργείται με μέσα τα οποία ο υπογράφοντας μπορεί να διατηρήσει υπό τον έλεγχο του.
    - Διασφαλίζει την ακεραιότητα των ηλεκτρονικών δεδομένων με τα οποία συνδέεται.

  Οι παραπάνω προδιαγραφές, είναι τεχνολογικά ουδέτερες. 'Δείχνουν' πάντως έμμεσα τις ψηφιακές υπογραφές και την υποδομή δημοσίου κλειδιού που τις συνοδεύει, κάτι που είναι ιδιαίτερα εμφανές στην τελευταία από αυτές.
- **Αναγνωρισμένη Ηλεκτρονική Υπογραφή (Qualified Electronic Signature)**: Ο συγκεκριμένος τύπος ηλεκτρονικής υπογραφής δεν αναφέρεται ρητά στην οδηγία, αλλά έμμεσα μέσω των ιδιοτήτων του. Έτσι, η αναγνωρισμένη ηλεκτρονική υπογραφή είναι η προηγμένη ηλεκτρονική υπογραφή, η οποία συνοδεύεται από ένα πιστοποιητικό το οποίο πληροί συγκεκριμένες προϋποθέσεις (αναγνωρισμένο) και παράγεται από μία διάταξη με συγκεκριμένα χαρακτηριστικά ασφαλείας.

Σύμφωνα λοιπόν με την οδηγία, σε κανέναν από τους παραπάνω τύπους ηλεκτρονικής υπογραφής δεν μπορεί να υπάρξει άρνηση νομικής ισχύος. Μόνο όμως ο τελευταίος τύπος ηλεκτρονικής υπογραφής θεωρείται ισοδύναμος με την ιδιόχειρη υπογραφή. Το συγκεκριμένο σημείο σίγουρα απαιτεί κάποια επεξήγηση. Σύμφωνα με το **[Dumortier, 1999],** σημαίνει ότι δεν μπορεί κανένα κράτος μέλος να δημιουργήσει νομοθεσία, κανονισμό ή διάταξη που να κάνει διάκριση εναντίον μιας ηλεκτρονικής υπογραφής, μόνο και μόνο επειδή είναι ηλεκτρονική. Με απλά λόγια για να υπάρξει άρνηση της ισχύος μιας ηλεκτρονικής υπογραφής, πρέπει να συντρέχει επιπλέον λόγος, από το ότι είναι σε ηλεκτρονική μορφή. Μπορεί να ειπωθεί **[EESSI, 1999],** ότι έτσι τίθεται γενική ισχύς στις ηλεκτρονικές υπογραφές, αλλά δίνεται υπεροχή στις πιο τεχνολογικά προηγμένες ηλεκτρονικές υπογραφές, τις αναγνωρισμένες. Με την εισαγωγή της έννοιας της διαπίστευσης εισάγεται και ένα τέταρτο είδος ηλεκτρονικών υπογραφών, αυτό που βασίζεται σε πιστοποιητικά ενός διαπιστευμένου πάροχου υπηρεσιών πιστοποίησης. Η πρακτική αξία του συγκεκριμένου είδους υπογραφών είναι περιορισμένη, καθώς δεν αναφέρεται κάποια ιδιαίτερη χρήση τους. Παρ'ολα αυτά, ακόμα και αν πρόκειται για απλές ηλεκτρονικές υπογραφές, πιθανότατα το γεγονός ότι προέρχονται από κάποιον διαπιστευμένο πάροχο θα τους δίνει αυξημένο ειδικό βάρος, σε περίπτωση που χρησιμοποιηθούν σε κάποιες νομικές διαδικασίες. Τα παραπάνω φαίνονται καλύτερα στο σχήμα που ακολουθεί:

Σχήμα 16. Τα είδη ηλεκτρονικών υπογραφών που αναδύονται από την οδηγία

4.4.2 Πάροχοι Υπηρεσιών Πιστοποίησης

Ο πάροχος υπηρεσιών πιστοποίησης ορίζεται στην οδηγία, ως οποιοσδήποτε οργανισμός παρέχει υπηρεσίες σχετιζόμενες με τις ηλεκτρονικές υπογραφές. Κατά συνέπεια, ο συγκεκριμένος ορισμός πλησιάζει περισσότερο την έννοια της *Έμπιστης Τρίτης Οντότητας*, παρά της *Αρχής Πιστοποίησης*, όπως τις ορίσαμε νωρίτερα. Αν και δεν απαγορεύεται στην οδηγία η έμπιστη τρίτη οντότητα αυτή, να είναι ένα φυσικό πρόσωπο, οι περιορισμοί που θέτει είναι δύσκολο να ικανοποιηθούν. Οι αρχές πιστοποίησης μπορεί να είναι είτε δημόσιες, είτε ιδιωτικές. Πάντως ένας πάροχος υπηρεσιών πιστοποίησης υπόκειται στην χώρα μέλος στην οποία έχει την έδρα του, παρόλο που μπορεί να προσφέρει υπηρεσίες (και) σε άλλες ευρωπαϊκές και όχι μόνο χώρες.

Για τους συγκεκριμένους φορείς ορίζει τα εξής:

- Δεν χρειάζεται κάποια άδεια για την έναρξη της λειτουργία τους.
- Βρίσκονται υπό εποπτεία, μόνο όταν εκδίδουν αναγνωρισμένα πιστοποιητικά.

4.4.3 Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής

Η ευρωπαϊκή οδηγία **[EDCF,1999]** για τις ηλεκτρονικές υπογραφές θέτει στο παράρτημα 3, ένα σύνολο από απαιτήσεις, που πρέπει να ικανοποιούν οι συσκευές οι οποίες θα χρησιμοποιηθούν για την δημιουργία των ηλεκτρονικών υπογραφών. Οι απαιτήσεις αυτές και η ερμηνεία τους είναι:

- **τα δεδομένα δημιουργίας υπογραφής** (δηλαδή, το ιδιωτικό κλειδί κρυπτογράφησης στην περίπτωση της υποδομής δημοσίου κλειδιού) **που χρησιμοποιούνται προς παραγωγή υπογραφών απαντούν κατ 'ουσίαν μόνο μια φορά και ότι το απόρρητο είναι διασφαλισμένο** Πράγματι, η ύπαρξη δύο ίδιων κλειδιών υπογραφής θα είχε αρνητικές συνέπειες προς την δυνατότητα μη

άρνησης της υπογραφής (non-repudiation). Η ερμηνεία της συγκεκριμένης απαίτησης, αφορά την χρήση καλών γεννητριών τυχαίων αριθμών – ένα πρότυπο το οποίο θα μπορούσε να χρησιμοποιηθεί γαι τον συγκεκριμένο σκοπό είναι το **[PKCS#13, 2001]**, είτε από τους πάροχους υπηρεσιών πιστοποίησης, είτε από τις διάφορες διατάξεις με τις οποίες οι χρήστες παράγουν μόνοι τους τα κλειδιά τους, τα οποία για να απαντούν μόνο μία φορά, δεν πρέπει να αντιγράφονται ούτε καν για αρχειοθέτηση. Επίσης η αποστροφή για το απόρρητο, θέτει απαιτήσεις ασφαλούς αποθήκευσης των δεδομένων δημιουργίας υπογραφής από εξωτερικές απειλές.

- **τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών δεν μπορούν, με εύλογη βεβαιότητα, να αντληθούν από αλλού και ότι η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας.** Με την παραπάνω απαίτηση προδιαγράφεται η χρήση τέτοιων αλγορίθμων κρυπτογράφησης και σύνοψης αλλά και κρυπτογραφικών κλειδιών συγκεκριμένου μήκους τα οποία να αντιστέκονται στον υπολογισμό για παράδειγμα του ιδιωτικού κλειδιού από το δημόσιο ή από την ηλεκτρονική υπογραφή.
- **τα δεδομένα δημιουργίας υπογραφής που χρησιμοποιούνται προς παραγωγή υπογραφών μπορούν να προστατεύονται αποτελεσματικά από τον νόμιμο υπογράφοντα κατά της χρησιμοποίησης από τρίτους.** Η συγκεκριμένη απαίτηση δημιουργεί νομική ευθύνη στον κάτοχο της, ο οποίος δεν πρέπει να δείχνει αμέλεια στην φύλαξη της διάταξης δημιουργίας υπογραφής συνολικά ή του τμήματος της το οποίο αντιστοιχεί στον ίδιο.
- **Τα δεδομένα προς υπογραφή δεν μεταβάλλονται κατά την παρουσίαση τους στον υπογράφοντα και ο υπογράφων έχει απεριόριστη πρόσβαση σε αυτά.** Με άλλα λόγια, διασφαλίζεται ότι ο υπογράφων έχει πάντοτε πρόσβαση στα πραγματικά δεδομένα στα οποία θα εφαρμόσει την υπογραφή. Θα είναι σίγουρος δηλαδή, ό,τι υπογράφει αυτό που φαίνεται ότι υπογράφει (*WYSIWYS: What You See Is What You Sign*), πράγμα προφανές στις ιδιόχειρες υπογραφές, αλλά καθόλου προφανές στις ηλεκτρονικές υπογραφές.

Αξίζει να σημειωθεί ότι η οδηγία *δεν* θέτει απαιτήσεις δεν καλύπτει όλο το περιβάλλον δημιουργίας υπογραφής. Ασχολείται κυρίως με το τμήμα του που έρχεται σε επαφή με το ιδιωτικό κλειδί, όπως άλλωστε είδαμε. Καταλαβαίνουμε λοιπόν ότι οι συγκεκριμένες απαιτήσεις, θέτουν ένα σύνολο από νομικά και τεχνικά θέματα για τις διατάξεις δημιουργίας υπογραφής. Για τα τεχνικά θέματα, αρμόδιοι είναι οι φορείς της EESSI (Electronic Signature Standardization Initiative). Για το συγκεκριμένο θέμα λοιπόν, έχει εκδοθεί ένα αντίστοιχο συμβουλευτικό κείμενο το οποίο έχει ως σκοπό την παροχή βοήθειας στην υλοποίηση των απαιτήσεων της οδηγίας **[SSCS,2000]**. Η μοντελοποίηση του συστήματος που προκύπτει από το συγκεκριμένο κείμενο, αναφέρθηκε με λεπτομέρεια στο κεφάλαιο 3.

4.4.4 Αναγνωρισμένα Πιστοποιητικά

Η οδηγία ορίζει τα πιστοποιητικά σύμφωνα με την χρήση τους, δηλαδή την σύνδεση δημοσίου

κλειδιού με την ταυτότητα μιας οντότητας. Για την αναγνώριση ενός πιστοποιητικού τίθενται ορισμένες απαιτήσεις τόσο για τα περιεχόμενα του, όσο και για τον εκδότη του. Έτσι, αναγνωρισμένο χαρακτηρίζεται ένα πιστοποιητικό του οποίου τα περιεχόμενα πληρούν κάποιες προϋποθέσεις, οι οποίες εκφράζονται στο παράρτημα 1 και εκδίδεται από έναν πάροχο, ο όποιος πληροί τις προϋποθέσεις του παραρτήματος 2.

4.4.4.1 Περιεχόμενα Πιστοποιητικού

Σε ότι αφορά το περιεχόμενο, το πιο σημαντικό στοιχείο που θα πρέπει να περιέχει το πιστοποιητικό είναι μία ένδειξη που να αναφέρει ότι είναι αναγνωρισμένο. Εδώ επισημαίνεται πολύ σωστά **[Dumortier, 1999],** ότι δεν έχει σημασία αν όντως είναι αναγνωρισμένο. Δηλαδή, αν εκδίδεται ως αναγνωρισμένο, ενώ δεν πληροί τις τυπικές προϋποθέσεις, τότε σε ότι αφορά το ευρύ κοινό είναι αναγνωρισμένο. Για οτιδήποτε άλλο την ευθύνη φέρει ο πάροχος πιστοποίησης, καθώς αυτός ελέγχει το περιβάλλον και τις διατάξεις δημιουργίας του. Ο χρήστης είτε αυτός που δημιουργεί είτε αυτός που επαληθεύει την ηλεκτρονική υπογραφή, δεν μπορεί να έχει άποψη για το αν όντως είναι αναγνωρισμένο το πιστοποιητικό, οπότε εύλογα πρέπει να βασίζεται στην ένδειξη που το συνοδεύει.

Τα ακριβή περιεχόμενα ενός πιστοποιητικού φαίνονται στο παρακάτω σχήμα:

1	Ένδειξη ότι πρόκειται για αναγνωρισμένο πιστοποιητικό
2	Στοιχεία αναγνώρισης του πάροχου πιστοποίησης – και κράτος
3	Όνομα Υπογράφοντος / αναγνωρισμένο ψευδώνυμο
4	Χαρακτηριστικό Υπογράφοντος το οποίο έχει σχέση με το πιστοποιητικό
5	Δεδομένα Επαλήθευσης Υπογραφής.
6	Διάρκεια Ισχύος Πιστοποιητικού
7	Μοναδικός Κωδικός
8	Προηγμένη Ηλεκτρονική Υπογραφή Πάροχου Πιστοποίησης
9	Περιορισμούς στην χρήση του.
10	Όρια στο ύψος συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί

Σχήμα 17. Περιεχόμενα για Αναγνωρισμένο Πιστοποιητικό

Η οδηγία δεν αναφέρεται σε συγκεκριμένο πρότυπο πιστοποιητικού. Είναι όμως φανερό ότι λόγω της ευρύτατης διάδοσης του, μάλλον για τα επόμενα χρόνια θα επικρατήσει το πρότυπο X.509. Ο τρόπος με τον οποίο τα πιστοποιητικά που ακολουθούν το πρότυπο X.509v3, θα περιέχουν τα παραπάνω στοιχεία, ορίζεται στο **[RFC 3039, 2001]** και στο **[ETSI, 101 862].**

- Η ένδειξη ότι το πιστοποιητικό είναι αναγνωρισμένο, θα υλοποιείται με μία επέκταση δήλωσης, την οποία ορίσαμε στο κεφάλαιο 2. Εναλλακτικά, μπορεί η συγκεκριμένη επέκταση να απουσιάζει, εάν στην πολιτική πιστοποίησης, η οποία αναφέρεται στην ομώνυμη επέκταση δηλώνει *ρητά*, ότι το συγκεκριμένο πιστοποιητικό εκδίδεται ως αναγνωρισμένο.
- Τα στοιχεία αναγνώρισης του πάροχου υπηρεσιών πιστοποίησης θα περιέχονται στο πεδίο *εκδούσα αρχή* του πιστοποιητικού. Το όνομα κατά X.500, το οποίο θα περιέχεται εκεί θα πρέπει να περιέχει οπωσδήποτε το όνομα RDN για την χώρα στην οποία είναι εγκατεστημένος. Έτσι για παράδειγμα το πιστοποιητικό της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (σχήμα 2) το οποίο παραθέσαμε, ικανοποιεί την συγκεκριμένη ιδιότητα.

- Το όνομα του υπογράφοντος, θα περιέχεται στο πεδίο *υποκείμενο* και θα έχει και αυτό την μορφή που ορίζει το πρότυπο X.500.
- Το χαρακτηριστικό που αναφέρεται στο πεδίο 4 καθιστά το αναγνωρισμένο πιστοποιητικό, πιστοποιητικό ιδιότητας, όπως το περιγράψαμε στο κεφάλαιο 2. Η υλοποίηση του θα γίνει με μία επέκταση του X.509 (subject directory attributes), η οποία θα περιέχει τις απαιτούμενες ιδιότητες.
- Τα δεδομένα επαλήθευσης υπογραφής θα παρέχονται στο πεδίο *δημόσιο κλειδί* του X.509.
- Η διάρκεια ισχύος του πιστοποιητικού θα περιέχεται στο αντίστοιχο πεδίο του πιστοποιητικού X.509.
- Για τον μοναδικό κωδικό του πιστοποιητικού μπορεί να χρησιμοποιηθεί το πεδίο *σειριακός αριθμός* του X.509.
- Η προηγμένη ηλεκτρονική υπογραφή του πάροχου υπηρεσιών πιστοποίησης, θα περιέχεται στο πεδίο ψηφιακή υπογραφή εκδούσας αρχής του X.509. Ένα ακόμα σημείο που υποστηρίζει την άποψη ότι η οδηγία αν και θεωρητικά είναι τεχνολογικά ουδέτερη, έχει φτιαχτεί έχοντας υπόψη την υποδομή δημοσίου κλειδιού. Παρατηρούμε ότι η οδηγία δεν θέτει απαίτηση για χρήση ασφαλούς διάταξης κατά την υπογραφή των πιστοποιητικών.
- Τα δύο τελευταία πεδία υπάρχουν για να δώσουν την δυνατότητα στον πάροχο πιστοποίησης να περιορίσει την ευθύνη του, σε περίπτωση κάποιας ζημιάς που προέρχεται από το πιστοποιητικό.
    - Οι περιορισμοί στην χρήση του πιστοποιητικού, μπορούν να υλοποιηθούν με την επέκταση χρήσης κλειδιού (key usage) και την επέκταση πολιτικής πιστοποίησης (certificate policy) που ορίζει το **[RFC 3039, 2001].**
    - Οι περιορισμοί στην χρήση των συναλλαγών θα υλοποιούνται με μία επέκταση δήλωσης του RFC 3039. Η δήλωση θα περιέχει ένα ήδη καταχωρημένο ASN.1. Οι τιμές των ποσών θα περιγράφονται με τον τύπο δεδομένων Monetary Value της ASN.1, ο οποίος έχει καταχωρηθεί με το πρότυπο ISO 4217.

4.4.4.2 Εκδότης Πιστοποιητικού

Για την αναγνώριση ενός πιστοποιητικού αναφέρονται και κάποιες σημαντικές προϋποθέσεις για τον πάροχο υπηρεσιών πιστοποίησης που το εκδίδει **[EDCF, 1999],** τις οποίες και παραθέτουμε στην συνέχεια**.** Οι συγκεκριμένες απαιτήσεις αποτελούν υποσύνολο των απαιτήσεων για τα αξιόπιστα συστήματα που αναφέραμε στο προηγούμενο κεφάλαιο. Το πώς θα υλοποιηθούν αναφέρεται στο πρότυπο **[ETSI, 101 456].** Ορισμένα σημεία καλύπτονται και από το **[ETSI, 101 862].** Η ακριβής υλοποίηση των απαιτήσεων εξαρτάται και από το αν τα αναγνωρισμένα πιστοποιητικά που εκδίδει προορίζονται για την επαλήθευση υπογραφών οι οποίες δημιουργούνται από ασφαλείς διατάξεις και άρα θα είναι ισοδύναμες με τις χειρόγραφες υπογραφές. Είναι φανερό, τότε ότι οι συγκεκριμένες απαιτήσεις θα είναι πιο αυστηρές. Στο

[ETSI, 101 456] οι συγκεκριμένες απαιτήσεις μεταφράζονται σε δύο αναγνωρισμένες πολιτικές πιστοποίησης (QCP δηλαδή πολιτικές πιστοποίησης για αναγνωρισμένα πιστοποιητικά), οι οποίες αναφέρονται ως QCP και QCP + SSCD, για χρήση των πιστοποιητικών, με ή χωρίς ασφαλείς διατάξεις. Ένας πάροχος πιστοποίησης, μπορεί να χρησιμοποιεί μία πολιτική πιστοποίησης σε ένα ηλεκτρονικό πιστοποιητικό, δηλώνοντας τον αναγνωριστή της και ενσωματώνοντας τον σε κάποια επέκταση του πιστοποιητικού. Για να μπορέσει να το πράξει αυτό πρέπει να παρέχει όλα τα στοιχεία που το αποδεικνύουν σε οποιοδήποτε συνδρομητή ή χρήστη το ζητήσει ή να έχει υπάρξει θετική αποτίμηση από κάποιον φορέα για την αλήθεια του ισχυρισμού. Οι απαιτήσεις του παραρτήματος 2, είναι λοιπόν:

1. **Επίδειξη της απαραίτητης αξιοπιστίας για την παροχή υπηρεσιών πιστοποίησης.** Αυτό μπορεί να γίνει ως εξής:
    - Ο πάροχος πιστοποίησης θα πρέπει να διεξάγει ανάλυση κινδύνων (risk analysis), πάνω στην οποία θα βασίσει τις απαιτήσεις ασφάλειας του και τις διαδικασίες λειτουργίας του.
    - Ο πάροχος υπηρεσιών πιστοποίησης θα πρέπει να δημοσιεύσει μία λεπτομερή δήλωση πρακτικών πιστοποίησης, στην οποία θα περιγράφει λεπτομερώς το πώς υλοποιείται η πολιτική πιστοποίησης, για τα αναγνωρισμένα πιστοποιητικά. Αν και δεν επιβάλλεται η χρήση μιας υποχρεωτικής δομής για το συγκεκριμένο κείμενο, προτείνεται η δομή του **[RFC 2527, 1999]**, την οποία και περιγράψαμε αναλυτικά, σε προηγούμενο κεφάλαιο. Στην συγκεκριμένη δήλωση θα πρέπει να αναφέρονται και υποχρεώσεις οντοτήτων που έχουν αναλάβει με εξωτερική ανάθεση (outsourcing) την υλοποίηση των υπηρεσιών πιστοποίησης. Ο πάροχος πιστοποίησης, δεν πρέπει να υποχρεούται βέβαια να δημοσιεύσει όλες τις λεπτομέρειες των πρακτικών του. Επίσης, υποχρεούται να διαθέτει ένα διοικητικό σώμα το οποίο θα είναι υπεύθυνο για την έγκριση της δήλωσης πρακτικών πιστοποίησης, για την εφαρμογή των διατάξεων της, και για όλες τις αλλαγές που ενδεχόμενα θα πρέπει να γίνουν σε αυτή, με την πάροδο του χρόνου.
    - Η οργανωτική δομή του πάροχου πιστοποίησης θα πρέπει να είναι σταθερή. Ενδεικτικά αναφέρουμε ορισμένες από τις ενέργειες που θα πρέπει να γίνουν προς την συγκεκριμένη κατεύθυνση:
        - Ύπαρξη συστήματος διαχείρισης ποιότητας (το οποίο μπορεί να είναι πιστοποιημένο με ένα από τα πρότυπα της σειράς 9000 του ISO).
        - Σε περίπτωση που ορισμένες από τις υπηρεσίες υλοποιούνται με εξωτερική ανάθεση, αυτές θα πρέπει να καλύπτονται από λεπτομερή συμβόλαια.
        - Λειτουργία υπηρεσίας για την εξέταση παραπόνων και την επίλυση διαφορών.
    - Ο πάροχος πιστοποίησης θα πρέπει να έχει προβλέψει τις ενέργειες στις οποίες θα πρέπει να προβεί σε περίπτωση που υπάρξει παραβίαση της ασφάλειας του ιδιωτικού κλειδιού του ή σε περίπτωση που αναγκαστεί να τερματίσει την λειτουργία του (λόγω χρεοκοπίας).
2. **Εξασφάλιση της λειτουργίας άμεσου και ασφαλούς καταλόγου και υπηρεσίας ανάκλησης**

πιστοποιητικών.

Η υπηρεσία διάδοσης πιστοποιητικών (κατάλογος), θα είναι διαθέσιμη 24 ώρες την ημέρα και 7 ημέρες την εβδομάδα. Στην δήλωση πρακτικών πιστοποίησης θα αναφέρεται ένα μέγιστο διάστημα το οποίο 'επιτρέπεται' η συγκεκριμένη υπηρεσία να μην λειτουργεί λόγω βλάβης ή συντήρησης, και σε περίπτωση που κάτι τέτοιο συμβεί δεν θα πρέπει να υπάρξει υπέρβαση του συγκεκριμένου χρονικού διαστήματος. Τα περιεχόμενα του πιστοποιητικού θα γνωστοποιούνται και στον συνδρομητή στον οποίον εκδίδεται. Τέλος, είναι φανερό, ότι πρέπει να εφαρμοστούν μηχανισμοί ελέγχου πρόσβασης για την υπηρεσία καταλόγου, έτσι ώστε να μην επιτρέπεται η μη εξουσιοδοτημένη προσθήκη, τροποποίηση και διαγραφή πιστοποιητικού.

Σχετικά με την λειτουργία της υπηρεσίας ανάκλησης πρέπει να εξασφαλίζονται τα παρακάτω στοιχεία, έτσι ώστε να μπορεί αυτή να χαρακτηριστεί ασφαλής και αξιόπιστη.

- Οι διαδικασίες που ακολουθούνται για την ανάκληση ενός πιστοποιητικού καταγράφονται στην δήλωση πρακτικών πιστοποίησης, με πιο σημαντικές τις παρακάτω:
  - Ποιος πρέπει να υποβάλλει αίτηση ανάκλησης.
  - Πώς πρέπει να υποβάλλονται (ηλεκτρονικά, εγγράφως, αυτοπροσώπως).
  - Απαιτήσεις για την επιβεβαίωση της αίτησης ανάκλησης.
  - Πότε και πώς εφαρμόζεται η αναστολή των πιστοποιητικών.
  - Πώς λειτουργεί ο μηχανισμός ανάκλησης των πιστοποιητικών.
  - Τον μέγιστο χρόνο από την αναφορά της ανάκλησης, μέχρι να γίνει διαθέσιμη η αλλαγή της κατάστασης στους επαληθεύοντες. Το συγκεκριμένο χρονικό διάστημα *δεν πρέπει να υπερβαίνει την 1 ημέρα*.
- Οι αιτήσεις ανάκλησης πρέπει να τυγχάνουν άμεσης επεξεργασίας.
- Οι αιτήσεις ανάκλησης πρέπει να αυθεντικοποιούνται και να επιβεβαιώνονται σύμφωνα με τις διατάξεις της δήλωσης πρακτικών πιστοποίησης.
- Αν υποστηρίζεται η προαιρετική λειτουργία της αναστολής του πιστοποιητικού, πρέπει να υπάρχει ειδοποίηση του συνδρομητή στον οποίο έχει εκδοθεί το πιστοποιητικό.

3. **Εξασφάλιση του ότι μπορεί να προσδιοριστεί επακριβώς η ημερομηνία και η ώρα έκδοσης και ανάκλησης του πιστοποιητικού.** Για να ικανοποιήσει ο πάροχος υπηρεσιών πιστοποίησης την συγκεκριμένη απαίτηση πρέπει να καταγράφει όλα τα στάδια του κύκλου ζωής ενός πιστοποιητικού, καθώς επίσης και ο ακριβής χρόνος στον οποίο έλαβαν χώρα. Τα καταγεγραμμένα δεδομένα θα είναι κρυπτογραφημένα, για να εξασφαλίζεται η μυστικότητα τους, ενώ πρέπει να διασφαλίζεται και η ακεραιότητα τους καθώς μπορούν να χρησιμοποιηθούν σε νομικές διαδικασίες, και για τον σκοπό αυτό θα πρέπει να διατηρούνται για τόσο χρονικό διάστημα, όσο μπορεί να αμφισβητηθεί μια συναλλαγή. Το χρονικό διάστημα αυτό καθορίζεται ανάλογα με την συναλλαγή. Πρέπει πάντως να αναφέρεται στην πολιτική πιστοποίησης.

4. **Επαλήθευση με κατάλληλα μέσα της ταυτότητας και των χαρακτηριστικών του ατόμου που πιστοποιείται.** Τα ακριβή στοιχεία που απαιτούνται για την επαλήθευση της ταυτότητας, ρυθμίζονται από την εθνική νομοθεσία. Η επαλήθευση πρέπει να γίνεται με τρόπο που να ισοδυναμεί με φυσική παρουσία, χωρίς να απαγορεύεται η χρήση ηλεκτρονικών μέσων. Ενδεικτικά μπορεί να δοθεί ο αριθμός ταυτότητας (αν κάτι τέτοιο υφίσταται), ημερομηνία και τόπος γέννησης. Πρέπει να παρέχονται επίσης από τον συνδρομητή, οπωσδήποτε τρόποι επικοινωνίας. Είναι φυσικό, ότι ο πάροχος υπηρεσιών πιστοποίησης, θα φροντίσει για την τήρηση όλων των διατάξεων της εθνικής νομοθεσίας προστασίας δεδομένων προσωπικού χαρακτήρα. Η ίδια επαλήθευση πρέπει να γίνει και στην περίπτωση που η πιστοποίηση αφορά κάποιες συγκεκριμένες ιδιότητες του συνδρομητή, όπως για παράδειγμα η οργανωτική του θέση. Τα ίδια πρέπει να ισχύουν και στην περίπτωση της ανανέωσης του πιστοποιητικού. *Ο πάροχος υπηρεσιών πιστοποίησης φέρει ευθύνη για την ακρίβεια των περιεχομένων του πιστοποιητικού.*
5. **Απασχόληση προσωπικού που διαθέτει την εμπειρογνωμοσύνη, την εμπειρία και τα προσόντα που είναι απαραίτητα για τις παρεχόμενες υπηρεσίες, ιδίως ικανότητα σε διαχειριστικό επίπεδο, εμπειρογνωμοσύνη στην τεχνολογία ηλεκτρονικών υπογραφών και εξοικείωση με τις κατάλληλες διαδικασίες ασφαλείας. Χρήση κατάλληλων διοικητικών και διαχειριστικών διαδικασιών οι οποίες να αντιστοιχούν προς αναγνωρισμένα πρότυπα.** Ο πάροχος υπηρεσιών πιστοποίησης πρέπει να τηρεί συγκεκριμένες διαδικασίες πρόσληψης, έτσι ώστε το συγκεκριμένο προσωπικό να έχει τις γνώσεις, τα προσόντα και την εμπειρία για μία τέτοια θέση. Αυτό μπορεί να αποδεικνύεται με τα απαραίτητα αποδεικτικά εκπαίδευσης ή προϋπηρεσίας. Θα υπάρχει αναλυτική περιγραφή των καθηκόντων και ευθυνών κάθε θέσης, ενώ θα υπάρχει σαφής διαχωρισμός των 'κρίσιμων ρόλων', αυτών δηλαδή από τους οποίους εξαρτάται η λειτουργία του πάροχου πιστοποίησης. Οι κρίσιμοι ρόλοι είναι αυτοί που περιγράψαμε στο κεφάλαιο 3. Ο διορισμός ατόμων στους κρίσιμους ρόλους αποτελεί ευθύνη της διοίκησης και πρέπει να γίνεται με τυπικές διαδικασίες. Ένα πρότυπο που μπορεί να χρησιμοποιηθεί για την αξιολόγηση των διοικητικών διαδικασιών είναι το BS 7799 ή ISO 17799.
6. **Χρήση αξιόπιστων συστημάτων και προϊόντων τα οποία προστατεύονται έναντι τροποποίησης και διασφαλίζουν την τεχνική και κρυπτογραφική ασφάλεια των διεργασιών πιστοποίησης οι οποίες υποστηρίζονται από αυτά.** Η συγκεκριμένη απαίτηση αφορά κυρίως την υπηρεσία δημιουργίας πιστοποιητικών, που αναφέραμε στο προηγούμενο κεφάλαιο. Πρέπει λοιπόν το κλειδί υπογραφής των πιστοποιητικών να *δημιουργείται* και να *αποθηκεύεται* σε μία διάταξη, η οποία να έχει πιστοποιηθεί κατά το FIPS–PUB 140-2 σε επίπεδο μεγαλύτερο του 3, ή κατά το Common Criteria σε επίπεδο τουλάχιστον EAL 4. Τα ίδια (τουλάχιστον) πρέπει να ισχύουν και για τα εφεδρικά αντίγραφα ασφαλείας των παραπάνω κλειδιών. Όταν, αυτά βρίσκονται εκτός της προαναφερθείσας συσκευής, πρέπει να είναι κρυπτογραφημένα. Η πρόσβαση σε αυτά θα γίνεται από ειδικά εξουσιοδοτημένο προσωπικό. Πρέπει να διασφαλίζεται επίσης ότι τα συγκεκριμένα κλειδιά χρησιμοποιούνται μόνο για την υπογραφή πιστοποιητικών και όχι για άλλες υπηρεσίες. Εξυπακούεται επιπλέον, ότι θα χρησιμοποιούνται

κατάλληλα προτυποποιημένοι αλγόριθμοι, όπως αυτοί που περιγράψαμε στο κεφάλαιο 2. Επίσης πρέπει να υπάρξει μέριμνα για την καταστροφή των κλειδιών και την διαχείριση των απαιτήσεων κύκλου ζωής των συστημάτων που χρησιμοποιούνται, όπως περιγράψαμε στο προηγούμενο κεφάλαιο. Σε ότι αφορά την προστασία των συγκεκριμένων συστημάτων που αναφέρεται στην απαίτηση πρέπει να υπάρχει πολιτική ελέγχου πρόσβασης, η οποία θα εξασφαλίζει την πρόσβαση στα συστήματα, μόνο από εξουσιοδοτημένες οντότητες και θα καταγράφει σχετικές πληροφορίες έτσι ώστε να είναι δυνατός ο καταλογισμός ευθύνης. Επιπλέον απαιτείται η ύπαρξη και τεχνικών μηχανισμών για την προστασία των συγκεκριμένων συστημάτων (πχ. προστασία του εσωτερικού δικτύου από το εξωτερικό με χρήση firewall κτλ.). Η προστασία των συγκεκριμένων συστημάτων, μπορεί να εξασφαλιστεί και με χρήση ενός κατάλληλου προφίλ προστασίας του προτύπου Common Criteria.

7. **Λήψη μέτρων εναντίον της πλαστογράφησης πιστοποιητικών και, σε περίπτωση που ο πάροχος υπηρεσιών πιστοποίησης παράγει δεδομένα δημιουργίας υπογραφής, να εγγυώνται την τήρηση του απορρήτου κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων.** Όπως έχουμε ήδη προαναφέρει στο κεφάλαιο 3, πρέπει να προστατεύεται η ακεραιότητα και η αυθεντικότητα των πιστοποιητικών. Αυτό, για τα πιστοποιητικά που ακολουθούν το πρότυπο X.509, εξασφαλίζεται με την ψηφιακή υπογραφή της εκδούσας αρχής που συνοδεύει το πιστοποιητικό. Επίσης, αντίστοιχα μέτρα πρέπει να ληφθούν και για την διανομή του δημοσίου κλειδιού του πάροχου πιστοποίησης. Σε περίπτωση, που η εκδούσα αρχή παράγει και υπογράφει μόνη της το πιστοποιητικό για το δημόσιο κλειδί, τότε αυτό πρέπει να συνοδεύεται από μία δήλωση που να αναφέρει ότι το συγκεκριμένο ιδιωτικό κλειδί, ανήκει στην συγκεκριμένη αρχή. Εδώ ισχύουν γενικά και οι προϋποθέσεις που αναφέραμε στο (6). Τα παραπάνω πρέπει να εφαρμόζονται σε όλη την διάρκεια του κύκλου ζωής των πιστοποιητικών, και κατά συνέπεια ισχύουν και σε περίπτωση ανανέωσης τους.

8. **Τα δεδομένα δημιουργίας υπογραφής, σε περίπτωση που παράγονται από τον πάροχο πιστοποίησης, δεν επιτρέπεται να αποθηκεύονται.** Γενικά πρέπει να ισχύουν οι προϋποθέσεις του (6) για την δημιουργία και αποθήκευση κλειδιών. Επίσης η μεταφορά του κλειδιού πρέπει να γίνεται με ασφάλεια. Η παραπάνω απαίτηση απαγορεύει ακόμα και την χρήση μεθόδων διαχωρισμού κλειδιών (key escrow), για την δημιουργία εφεδρικών κλειδιών.

9. **Ύπαρξη επαρκών χρηματικών πόρων, οι οποίοι να εξασφαλίζουν ότι μπορούν να αποκριθούν στις απαιτήσεις που τυχόν προκύψουν από την ευθύνη που υπέχουν σύμφωνα με την οδηγία.** Επειδή από τις λειτουργίες ενός πάροχου υπηρεσιών πιστοποίησης, μπορεί να δημιουργηθούν ζημιές πρέπει ο πάροχος υπηρεσιών πιστοποίησης να μπορεί να παρέχει κατάλληλες αποζημιώσεις. Για τον λόγο αυτό απαιτούνται οικονομικοί πόροι, που μπορούν να κατοχυρωθούν με ασφάλιση και αντίστοιχα μέσα. Αυτό μπορεί να αποδειχθεί με κάποια κατάθεση ενός προκαθορισμένου ποσού (στην Γερμανία για παράδειγμα είναι 500.000 μάρκα).

10. **Καταγραφή των στοιχείων χρήσης ενός πιστοποιητικού για ένα συγκεκριμένο χρονικό διάστημα, για την χρήση τους ως αποδεικτικό στοιχείο.** Εδώ, προφανώς ισχύουν οι απαιτήσεις του

(3). Επίσης πρέπει να υπάρχει κάποια πρόβλεψη για τις διαδικασίες που θα πρέπει να ακολουθηθούν σε περίπτωση τερματισμού των λειτουργιών του παρόχου υπηρεσιών πιστοποίησης. Σε περίπτωση τερματισμού λοιπόν των λειτουργιών, ένας πάροχος υπηρεσιών πιστοποίησης πρέπει να προβεί στις εξής ενέργειες, οι οποίες θα έχουν ως συνέπεια τη νομική ισχύ των καταγεγραμμένων αρχείων:

- Ενημέρωση συνδρομητών και συνεργαζόμενων παρόχων πιστοποίησης.
- Αν εκδίδει πιστοποιητικά στο ευρύ κοινό πρέπει να προβεί σε δημόσια ανακοίνωση.
- Τερματισμός όλων των συμβολαίων εξωτερικής ανάθεσης υπηρεσιών, που έχει συνάψει.
- Καταστροφή ιδιωτικών κλειδιών.
- Κάλυψη τυχών εξόδων χρεοκοπίας.

11. Προτού συνάψουν συμβατική σχέση με πρόσωπο που ζητά πιστοποιητικό από αυτούς για να κατοχυρώσει την ηλεκτρονική του υπογραφή, να το ενημερώνουν με ανθεκτικά μέσα επικοινωνίας σχετικά με τους ακριβείς όρους και προϋποθέσεις χρησιμοποίησης του πιστοποιητικού, συμπεριλαμβανομένων ενδεχόμενων περιορισμών της χρήσης του πιστοποιητικού, της ύπαρξης μηχανισμού εθελοντικής διαπίστευσης και των διαδικασιών υποβολής παραπόνων και επίλυσης διαφορών. Οι πληροφορίες αυτές, οι οποίες δύνανται να διαβιβάζονται ηλεκτρονικώς, πρέπει να παρέχονται εγγράφως, σε εύκολα καταληπτή γλώσσα. Σχετικά αποσπάσματα των πληροφοριών αυτών καθίστανται επίσης προσιτά κατόπιν αιτήματος τρίτων οι οποίοι βασίζονται στο πιστοποιητικό αυτό. Τα στοιχεία για τα οποία πρέπει να υπάρχει ενημέρωση είναι τα εξής:

- Την εφαρμοζόμενη πολιτική πιστοποίησης (για τα αναγνωρισμένα πιστοποιητικά), καθώς επίσης και για το αν αυτή απαιτεί την χρήση ασφαλούς διάταξης υπογραφής και το αν αυτή εκδίδεται στο κοινό.
- Περιορισμοί χρήσης του συγκεκριμένου πιστοποιητικού.
- Πληροφορίες για το πώς θα πρέπει να γίνεται η επαλήθευση του πιστοποιητικού.
- Υποχρεώσεις του συνδρομητή.
- Περιορισμοί Ευθύνης.
- Την χρονική περίοδο για την οποία θα διατηρούνται οι πληροφορίες εγγραφής.
- Την χρονική περίοδο για την οποία θα διατηρούνται τα αρχεία καταγραφής (log files), τα οποία θα περιέχουν πληροφορίες σχετικές με την χρήση του πιστοποιητικού.
- Διαδικασίες που πρέπει να ακολουθηθούν για την υποβολή παραπάνω και την επίλυση διαφορών.
- Το εφαρμοζόμενο νομικό καθεστώς.
- Εάν ο συγκεκριμένο πάροχος υπηρεσιών πιστοποίησης, έχει πιστοποιηθεί ότι τηρεί την συγκεκριμένη αναγνωρισμένη πολιτικής πιστοποίησης, καθώς επίσης και το όνομα του πιστοποιητή.

12. Χρήση αξιόπιστων συστημάτων για την αποθήκευση πιστοποιητικών, έτσι ώστε:

- **να μην μπορεί κάποιος μη εξουσιοδοτημένος χρήστης να τροποποιήσει τα περιεχόμενα του.**
- **να ελέγχεται η γνησιότητα των πληροφοριών.**
- **να υπάρχει ανάκτηση από τρίτο μόνο αν έχει δοθεί συγκατάθεση του συνδρομητή.**
- **οποιαδήποτε τεχνική αλλαγή θέτει σε κίνδυνο την ασφάλεια να γίνεται αντιληπτή.**

Οι συγκεκριμένες απαιτήσεις μπορούν να ικανοποιηθούν από τα στοιχεία που αναφέραμε για το (2), το (6) και το (7).

4.4.5 Συστάσεις για την επαλήθευση υπογραφής

Οι συστάσεις που αναφέρονται στο παράρτημα 4 είναι οι εξής:

- **τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής να αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα.** Με πιο απλά λόγια το σύστημα επαλήθευσης πρέπει να παρουσιάσει σωστά στον επαληθεύοντα όλα τα περιεχόμενα του πιστοποιητικού, συμπεριλαμβανομένων και αυτών που ανακτώνται με την ύπαρξη κάποιας έμμεσης αναφοράς. Μία πιθανή λίστα από δεδομένα τα οποία χρησιμοποιούνται προς επαλήθευση και τα οποία πρέπει να εμφανιστούν είναι αυτή που υπάρχει στο **[EESSI, 1999]**:
  - Ταυτότητα του υπογράφοντα.
  - Τύπος Δέσμευσης, αν κάτι τέτοιο υφίσταται στην πολιτική υπογραφής.
  - Περίοδος Ισχύος του πιστοποιητικού.
  - Πολιτικές Πιστοποίησης που εμφανίζονται στο πιστοποιητικό.
  - Όποιοι περιορισμοί (πχ. για το ύψος των συναλλαγών) αναγράφονται στο πιστοποιητικό.
  - Ταυτότητα της εκδούσας αρχής.
  - Πληροφορία κατάστασης σχετικά με την ανάκληση του πιστοποιητικού, όπως για παράδειγμα η ημερομηνία κατα την οποία εκδώθηκε η λίστα ανάκλησης η οποία ελέγχθηκε για το αν περιέχει το συγκεκριμένο πιστοποιητικό.
  - Πληροφορίες για το μονοπάτι πιστοποίησης που χρησιμοποιήθηκε.
- **η υπογραφή να επαληθεύεται με αξιοπιστία και το αποτέλεσμα της επαλήθευσης να εμφανίζεται με τον ορθό τρόπο.** Η συγκεκριμένη απαίτηση αφορά την μαθηματική διαδικασία επαλήθευσης της ηλεκτρονικής υπογραφής, όπως την περιγράψαμε στο κεφάλαιο 2, αλλά και την έγκαιρη παρουσίαση στον χρήστη όποιων λαθών προκύψουν.
- **ο επαληθεύων να μπορεί, ενδεχομένως, να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται.** Εδώ ισχύει το *WIPIWIS (What Is Presented Is What Is Signed),* όπως αναφέραμε και στο κεφάλαιο 3.
- **η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής να έχουν ελεγχθεί με αξιοπιστία.** Η συγκεκριμένη απαίτηση είναι

τυπική για ένα περιβάλλον επαλήθευσης ηλεκτρονικών υπογραφών, το οποίο βασίζεται στην υποδομή δημοσίου κλειδιού. Υπονοεί την ανάκτηση όλων των πιστοποιητικών που απαρτίζουν το μονοπάτι πιστοποίησης και της πληροφορίας ανάκλησης η οποία αντιστοιχεί σε κάθε ένα από αυτά. Την συγκεκριμένη διαδικασία περιγράψαμε εκτενώς σε προηγούμενο κεφάλαιο.

- **το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος να εμφανίζονται με τον ορθό τρόπο.**
- **η χρησιμοποίηση ψευδωνύμου να δηλώνεται εμφανώς, και**
- **να μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας.** Η συγκεκριμένη απαίτηση αφορά, όπως καταλαβαίνουμε περισσότερο τα περιεχόμενα του κειμένου που υπογράφεται και υπονοεί πως αν διαπιστωθεί οποιαδήποτε παραβίαση της ακεραιότητας του, αυτή πρέπει να αναφέρεται άμεσα.

Από τις παραπάνω συστάσεις συμπεραίνουμε, ότι η οδηγία αναφέρεται στην επαλήθευση υπογραφής από ανθρώπινη οντότητα και όχι από κάποια αυτοματοποιημένη διαδικασία. Βέβαια όπως έχει διαφανεί σε όλη την έκταση της εργασίας, σε ένα περιβάλλον ηλεκτρονικού εμπορίου πιο πιθανή θα είναι η αυτοματοποιημένη επαλήθευση μιας ηλεκτρονικής υπογραφής. Μία τέτοια αυτοματοποιημένη διαδικασία είναι πιθανότερο να συναντηθεί σε ένα κλειστό περιβάλλον, το οποίο θα καλύπτεται προηγουμένως από κάποια σύμβαση, περίπτωση που δεν αφορά την οδηγία.

4.4.6 Εποπτεία

Όπως προαναφέραμε, οι πάροχοι υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά θα βρίσκονται υπό ένα καθεστώς εποπτείας, από έναν φορέα που θα ορίζει κάθε κράτος μέλος. Η εποπτεία αυτή, όπως προκύπτει από την παραπάνω περιγραφή θα αφορά τις προσφερόμενες υπηρεσίες αλλά και τις εσωτερικές διαδικασίες των παρόχων υπηρεσιών πιστοποίησης (διαχείριση υποδομής δημοσίου κλειδιού, γενική διαχείριση ασφάλειας, διαχείριση ποιότητας). Μηχανισμός εποπτείας προβλέπεται επίσης και για τις ασφαλείς διατάξεις υπογραφής. Ενδεχομένως και αν ένα κράτος μέλος επιλέξει την τήρηση των συστάσεων για την ασφαλή επαλήθευση των ηλεκτρονικών υπογραφών να απαιτείται και ένας μηχανισμός εποπτείας στον συγκεκριμένο τομέα. Ορισμένες προδιαγραφές για την εποπτεία αυτή δίνονται στο **[ECAG, 2000].**.

Για την εποπτεία, είναι απαραίτητη μια διαδικασία αποτίμησης, η οποία μπορεί να διεξαχθεί από ένα σύνολο από φορείς, όπως για παράδειγμα ανεξάρτητες αρχές, ειδικά εργαστήρια και άλλοι ειδικοί φορείς (ορκωτοί λογιστές κτλ.). Οι ίδιοι φορείς και οι ίδιες διαδικασίες αποτίμησης πιθανότατα μπορούν να χρησιμοποιηθούν στην περίπτωση της εθελοντικής διαπίστευσης. Όποιος και αν είναι ο υπεύθυνος φορέας πρέπει να διαθέτει κάποια τυπικά προσόντα, είτε ως οργανισμός είτε ως μεμονωμένη οντότητα. Στην περίπτωση του οργανισμού πρέπει να αποδειχθεί η τήρηση ορισμένων προτύπων ειδικά για οργανισμούς πιστοποίησης, ενώ σε άλλη περίπτωση πρέπει να αποδεικνύεται η εμπειρία και οι εξειδικευμένες γνώσεις

τόσο κάθε μεμονωμένου ελεγκτή όσο και συνολικά της ομάδας. Η ευρωπαϊκή επιτροπή έχει εκδώσει και σχετική απόφαση **[CDMC, 2000]** για τα ελάχιστα κριτήρια που πρέπει να πληροί ένας φορέας αποτίμησης

Επιπλέον η συγκεκριμένη διαδικασία ελέγχου δεν είναι απαραίτητο να πραγματοποιείται από τα παραπάνω σώματα, πάντα. Ένας οργανισμός, ιδιαίτερα με τις απαιτήσεις που έχουν οι οργανισμοί που εξετάζουμε σε αυτή την εργασία, σίγουρα θα έχει κάποιον εσωτερικό μηχανισμό ελέγχου. Για τον εσωτερικό μηχανισμό ελέγχου μπορούμε να διακρίνουμε δύο περιπτώσεις: είτε τον καθημερινό λειτουργικό έλεγχο που είναι απαραίτητο συστατικό σε μία τέτοια οντότητας, είτε έναν πιο επίσημο εσωτερικό έλεγχο, που συνήθως γίνεται από άτομα τα οποία δεν εμπλέκονται στην καθημερινή λειτουργία του συγκεκριμένου οργανισμού (και ιδίως στο τμήμα, το οποίο αποτιμάται). Είναι φανερό πώς οι μηχανισμοί εποπτείας οι οποίοι έρχονται ως συνέπεια της οδηγίας δεν είναι δυνατόν να βασίζονται σε κανένα είδος εσωτερικού ελέγχου. Παρ' όλα αυτά ο συγκεκριμένος έλεγχος είναι πολλές φορές προαπαιτούμενο για την αποτίμηση που συνοδεύει την εποπτεία ή την διαπίστευση.

Πιο συγκεκριμένα τώρα, η εποπτεία θα εξετάζει αν τηρούνται οι πολιτικές του **[ETSI, 101 456]** το οποίο και αναλύσαμε νωρίτερα. Η διαδικασία αποτίμησης αφορά τόσο την εξέταση της τεκμηρίωσης που παρέχει η αρχή πιστοποίησης, όσο και την λειτουργική επιθεώρηση. Είναι δηλαδή μία διαδικασία που γίνεται σε δύο στάδια, με το στάδιο της τεκμηρίωσης να προηγείται και να λειτουργεί για τον σχεδιασμό της λειτουργικής επιθεώρησης. Προβλέπεται σε ότι αφορά την παρεχόμενη τεκμηρίωση ότι αν η αρχή πιστοποίησης κρίνει ένα έγγραφο, ως εμπιστευτικό λόγω μεγάλης σημασίας μπορεί να ζητηθεί η εξαίρεση αυτού από την διαδικασία της αποτίμησης. Η απόφαση για το αν κάτι τέτοιο θα γίνει πράξη θα εξεταστεί από τον υπεύθυνο εθνικό φορέα για την εποπτεία. Αν αυτός κρίνει ότι τα συγκεκριμένα έγγραφα είναι απαραίτητα για την ολοκλήρωση της διαδικασίας, οφείλει να το γνωστοποιήσει στην αρχή. Σε περίπτωση που η αποτίμηση έχει ως αποτέλεσμα την εθελοντική διαπίστευση, ο πάροχος υπηρεσιών πιστοποίησης μπορεί και να σταματήσει την όλη διαδικασία, κρίνοντας την σχετική σημασία της διαπίστευσης και της αποκάλυψης του συγκεκριμένου στοιχείου. Σε περίπτωση όμως που αφορά την εποπτεία και ιδιαίτερα σε περίπτωση ελέγχου μετά από καταγγελία, τότε ο πάροχος υπηρεσιών πιστοποίησης μάλλον δεν έχει άλλη επιλογή.

Μετά την ολοκλήρωση της εξέτασης της τεκμηρίωσης, διεξάγεται επίσκεψη στις εγκαταστάσεις του πάροχου υπηρεσιών πιστοποίησης. Η εξέταση αυτή έχει ως στόχο την εξακρίβωση του αν:

- Η αρχή πιστοποίησης τηρεί τις πολιτικές, τις διαδικασίες και τους στόχους της.
- Επιβεβαίωση του ότι το υπάρχει διοικητική πρωτοβουλία για την τήρηση των συγκεκριμένων πολιτικών.
- Η ανάλυση κινδύνων έχει γίνει ακολουθώντας σωστά, ακολουθώντας ίσως κάποια διεθνή πρότυπα.
- Τηρούνται οι τεχνικές απαιτήσεις για τα αξιόπιστα συστήματα και την έκδοση αναγνωρισμένων πιστοποιητικών που αναφέραμε νωρίτερα.
- Υπάρχουν ή όχι παρατυπίες.

Το αποτέλεσμα της παραπάνω εξέτασης είναι μία πρόταση από την ομάδα ελέγχου προς την ανεξάρτητη αρχή, που διαπιστώνει το αν τηρούνται οι απαιτήσεις που προβλέπονται για παράδειγμα για την έκδοση αναγνωρισμένων πιστοποιητικών. Αν η πρόταση αυτή είναι θετική και εγκριθεί από μια αρμόδια επιτροπή της ανεξάρτητης αρχής, τότε εκδίδεται ένα σχετικό κείμενο το οποίο λειτουργεί ως απόδειξη της συμμόρφωσης. Το συγκεκριμένο κείμενο δημιουργεί βέβαια και υποχρεώσεις στον πάροχο, στις οποίες συμπεριλαμβάνεται για παράδειγμα η ενημέρωση για κάθε αλλαγή σε όλα τα επίπεδα (διοικητικό, λειτουργικό και τεχνικό).

Επίσημες διαδικασίες αποτίμησης πρέπει να τηρηθούν και για τις ασφαλείς διατάξεις δημιουργίας υπογραφής, καθώς οι ηλεκτρονικές υπογραφές οι οποίες δημιουργούνται από αυτές (και βασίζονται σε αναγνωρισμένα πιστοποιητικά) είναι ισοδύναμες των ιδιόχειρων υπογραφών. Η αποτίμηση για τα συγκεκριμένα συστήματα θα γίνει με βάση το προφίλ προστασίας που περιγράψαμε νωρίτερα και το Common Criteria. Εδώ αξίζει να επαναλάβουμε αυτό που αναφέραμε και κατά την περιγραφή του προτύπου Common Criteria, σχετικά την από κοινού αναγνώριση μίας πιστοποίησης κατά Common Criteria από ένα σύνόλο από χώρες μεταξύ των οποίων βρίσκεται και η Ελλάδα. Στο πλαίσιο της παραπάνω συμφωνίας αναγνωρίζεται η πιστοποίηση και για οποιαδήποτε διάταξη δημιουργίας υπογραφής πιστοποιηθεί ότι ικανοποιεί τις προϋποθέσεις που ορίζονται στο συγκεκριμένο προφίλ προστασίας.

Για τις υπόλοιπες διατάξεις δημιουργίας (δηλαδή τις ‘μη ασφαλείς’) και επαλήθευσης ηλεκτρονικών υπογραφών, λόγω των πολύπλοκων τεχνικών ζητημάτων που φάνηκαν άλλωστε και από την προηγούμενη περιγραφή μας, ο πιο αποτελεσματικός τρόπος να υπάρξει αποτίμηση, σύμφωνα με το **[ECAG, 2000]**, είναι με δηλώσεις συμμόρφωσης (declaration of conformance) των κατασκευαστών, ότι τα προϊόντα τους τηρούν τις τεχνικές προδιαγραφές των προτύπων που αναφέραμε σε προηγούμενο κεφάλαιο για τις συγκεκριμένες συσκευές. Αυτή η μέθοδος θεωρείται προτιμότερη από την δημιουργία ενός τυπικού συστήματος αποτίμησης από αυτό που περιγράφηκε για τους παρόδους υπηρεσιών πιστοποίησης και τις ασφαλείς διατάξεις υπογραφής. Επιπρόσθετα, σε περίπτωση που το συγκεκριμένο σύστημα έχει εγκατασταθεί σε κάποιον δημόσιο χώρο, απαιτείται αντίστοιχη δήλωση από την οντότητα που είναι υπεύθυνη για τον χειρισμό της συγκεκριμένης διάταξης. Είναι φανερό, ότι οι συγκεκριμένες οντότητες (κατασκευαστής – λειτουργός) φέρουν νομική ευθύνη σχετικά με την ακρίβεια της συγκεκριμένης δήλωσης.

Η απουσία βέβαια ενός επίσημου μηχανισμού αποτίμησης από κάθε κράτος μέλος, δεν αίρει εντελώς την εποπτεία, ούτε την ανάγκη για αποτίμηση με κάποιον άλλο τρόπο, όπως για παράδειγμα ανεξάρτητοι διεθνείς φορείς. Είναι προφανές άλλωστε ότι δηλώσεις συμμόρφωσης που έχουν αποτιμηθεί όπως προαναφέρθηκε θα έχουν μεγαλύτερη πραγματική αξία.

4.4.7 Εθελοντική Διαπίστευση

Η διαπίστευση ορίζεται στην οδηγία ως *‘οποιαδήποτε άδεια η οποία δημιουργεί δικαιώματα και*

υποχρεώσεις στον πάροχο υπηρεσιών πιστοποίησης'. Η διαδικασία αυτή χαρακτηρίζεται ως εθελοντική καθώς η εκκίνηση της γίνεται από τον πάροχο υπηρεσιών πιστοποίησης. Η διαπίστευση θα γίνεται από ένα ιδιωτικό ή δημόσιο φορέα που θα ορίσει το κάθε κράτος μέλος. Η διαδικασία της διαπίστευσης δεν πρέπει να δημιουργεί διακρίσεις, υπέρ των διαπιστευμένων φορέων πιστοποίησης. Βέβαια κάτι τέτοιο είναι παράδοξο, καθώς η ίδια η έννοια της διαπίστευσης αποτελεί ένα σημαντικό όπλο για το τμήμα πωλήσεων οποιασδήποτε εταιρείας. Η εθελοντική διαπίστευση έχει μία σημαντική διαφορά από την διαδικασία εποπτείας καθώς ο στόχος της είναι να παρέχει κίνητρα στους πάροχους υπηρεσιών πιστοποίησης για την βελτίωση των υπηρεσιών τους και θεωρητικά μπορεί να προσαρμόζεται καλύτερα στις αλλαγές της τεχνολογίας. Η οδηγία δεν θέτει συγκεκριμένες απαιτήσεις για την διαπίστευση, απλά κάποιες γενικές κατευθύνσεις, όπως για παράδειγμα ότι πρέπει να βασίζεται σε αντικειμενικά κριτήρια, να μην οδηγούν σε διακρίσεις κτλ. Το πώς θα υλοποιηθεί η διαπίστευση αφήνεται σε κάθε κράτος μέλος. Άλλα κράτη όπως η Γερμανία έχει επιλέξει την διαπίστευση από κάποιον κρατικό οργανισμό, ενώ άλλα όπως η Μ. Βρετανία έχουν αφήσει την όλη διαδικασία στις δυνάμεις τις αγοράς. Επειδή πάντως κανένα πλαίσιο διαπίστευσης δεν πρέπει να κάνει διακρίσεις, ένας πάροχος πιστοποίησης δεν είναι ανάγκη να διαπιστευτεί από την χώρα στην οποία έχει την έδρα. Όπως είναι φανερό, η υλοποίηση από κάθε κράτους ενός διαφορετικού πλαισίου διαπίστευσης, μπορεί να οδηγήσει σε προβλήματα συμβατότητας.

Αν ένας πάροχος υπηρεσιών πιστοποίησης έχει διαπιστευτεί, είναι φανερό ότι οι ηλεκτρονικές υπογραφές που βασίζονται στα πιστοποιητικά του θα έχουν *a priori*, κάποια αναγνωρισμένη αξία. Σε άλλη περίπτωση η αξία των υπογραφών θα αποδεικνύεται *a posteriori*, μέσω της εποπτείας.

4.4.8 Ιδιωτικότητα – Προστασία Προσωπικών Δεδομένων.

Στο άρθρο 8 της οδηγίας, αναφέρονται οι απαιτήσεις για τους πάροχους υπηρεσιών πιστοποίησης αλλά και τους επόπτες σχετικά με την τήρηση αρχείου, δεδομένων προσωπικού χαρακτήρα τα οποία συγκεντρώνονται κυρίως κατά την διαδικασία αίτησης έκδοσης ηλεκτρονικού πιστοποιητικού. Η συγκεκριμένη συλλογή στοιχείων εμπίπτει στην νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα και κατά συνέπεια κάθε πάροχος υπηρεσιών πιστοποίησης υπόκειται στον αντίστοιχο εθνικό νόμο όπου εδρεύει. Επιτρέπει επίσης την χρήση ψευδωνύμων στο πεδίο όπου παρουσιάζεται η ταυτότητα του κατόχου αντί του πραγματικού του ονόματος.

4.4.9 Εθνικές Προσεγγίσεις

Αφού ολοκληρώσαμε την προσέγγιση της Ευρωπαϊκής Επιτροπής, θα εξετάσουμε μεμονωμένα ορισμένες προσεγγίσεις ευρωπαϊκών χωρών στις ηλεκτρονικές υπογραφές και υπηρεσίες πιστοποίησης. Επιλέξαμε την Γερμανία και την Μεγάλη Βρετανία καθώς οι δύο αυτές προσεγγίσεις μπορούν να θεωρηθούν τα δύο άκρα στην Ευρωπαϊκή Ένωση. Τέλος θα αναφέρουμε και τις εξελίξεις στο συγκεκριμένο θέμα για την Ελλάδα. Μία γενική επισκόπηση των ενεργειών που έχουν γίνει σε όλες τις χώρες σχετικά με

την υλοποίηση της οδηγίας φαίνεται στο παρακάτω σχήμα **[EESSI, 2001]**:

0	1	2	3	4	Χώρα	
					Αυστρία	0: Αρχική Ανάλυση
					Βέλγιο	1: Πρωτογενής Νομοθεσία
					Δανία	2: Δευτερογενής Νομοθεσία
					Φινλανδία	3: Νομοθεσία σε Λειτουργική Φάση
					Γαλλία	4: Έγκριση από την αρμόδια ευρωπαϊκή επιτροπή.
					Γερμανία	
					Ελλάδα	
					Ιρλανδία	
					Ιταλία	
					Λουξεμβούργο	
					Ολλανδία	
					Πορτογαλία	
					Ισπανία	
					Σουηδία	
					Μεγάλη Βρετανία	
					Δημοκρατία της Τσεχίας	
					Εσθονία	
					Ουγγαρία	
					Πολωνία	
					Σλοβενία	
					Νορβηγία	
					Ελβετία	

Σχήμα 18. Βαθμός Υλοποίησης της Οδηγίας Σε διάφορες Ευρωπαϊκές Χώρες [EESSI, 2001].

4.4.9.1 Γερμανία

Όπως είναι ίσως γνωστό, η Γερμανία είναι από τις πρώτες χώρες παγκοσμίως που θεσμοθέτησε σε εθνικό επίπεδο την χρήση των ηλεκτρονικών υπογραφών και της υποστηρικτικής γι' αυτές υποδομής (συγκεκριμένα από τον Ιούλιο του 1997, πριν ακόμα από την οδηγία της Ευρωπαϊκής Ένωσης). Κατά συνέπεια είναι λογικό να υπάρχουν σημαντικές αποκλίσεις από την επίσημη ευρωπαϊκή γραμμή. Έτσι είναι φυσικό, πως είναι και η πρώτη χώρα που έχει προχωρήσει στην αναθεώρηση του νομικού της πλαισίου, τον Αύγουστο του 2000, για να συμβαδίσει με την οδηγία. Η δεύτερη έκδοση, λοιπόν την ακολουθεί αρκετά πιστά. Παρά λοιπόν το γεγονός ότι ουσιαστικά με την τροποποίηση του γερμανικού νόμου αρκετές από τις

διαφορές που θα αναφέρουμε παρακάτω έχουν αρθεί, εμείς θα τις αναφέρουμε, καθώς δεν παύουν να αποτελούν εύλογες αντιρρήσεις και μία άλλη οπτική γωνία πέρα από αυτην που έχουμε εξετάσει μέχρι τώρα.

Ο γερμανικός νόμος του 1997, λοιπόν, αναφέρεται σε ψηφιακές υπογραφές και στην υποδομή δημοσίου κλειδιού και όχι σε ηλεκτρονικές υπογραφές, οι οποίες είναι ανεξάρτητες τεχνολογίας. Οι Γερμανοί είχαν αντιρρήσεις σχετικά με την ευρεία έκταση της ευρωπαϊκής προσέγγισης όπως φαίνεται και στο **[SIGGa, 1999]**. Η βάση για τις συγκεκριμένες αντιρρήσεις έγκειται στο γεγονός ότι η εισαγωγή όλων των ηλεκτρονικών υπογραφών, νομιμοποιεί εν δυνάμει έναν μη δοκιμασμένο μηχανισμό, που μπορεί και να μην διαθέτει χαρακτηριστικά όπως η ακεραιότητα των μηνυμάτων.

Το πλαίσιο της Γερμανίας για ψηφιακές υπογραφές μπορεί να διακριθεί σε τρία επίπεδα:

- Νομικό Πλαίσιο (*SigG – SignaturGesetz*): Παρέχει τις γενικές διατάξεις, ορίζοντας το τι είναι οι ψηφιακές υπογραφές, τι είναι οι αρχές πιστοποίησης και τι είναι τα πιστοποιητικά. **[SIGG, 1997].**
- Διατάξεις Υλοποίησης (*SigV – SignaturVerordnung*): Θέτει λειτουργικές λεπτομέρειες και ευθύνες για τις αρχές πιστοποίησης και πιο συγκεκριμένες απαιτήσεις πάνω στα νομικό πλαίσιο **[SIGV, 1997].**
- Τεχνικές Προδιαγραφές (*SigI – SignaturInteroperabilitätspezifikation*): Προδιαγράφει, εξαντλητικά (σε ένα κείμενο 300 σελίδων), αλγόριθμους, πρωτόκολλα υπηρεσιών καταλόγου, χρονοσήμανσης και πρότυπα για τις δομές δεδομένων που ανταλλάσσονται

Τα δύο πρώτα κείμενα είναι αντικείμενο της ομοσπονδιακής κυβέρνησης, ενώ τα τεχνικά πρότυπα εκπονούνται από τον **BSI (Bundesamt für Sicherheit in der Informationstechnik)**. Η γερμανική προσέγγιση έχει δεχθεί κριτική **[Aalberts, 1999],** καθώς δεν αποδίδει νομική ισχύ στις ψηφιακές υπογραφές αλλά θέτει προδιαγραφές ασφαλείας σε ότι αφορά την χρήση τους σε γερμανικό έδαφος. Παρατηρούμε δηλαδή το παράδοξο του ότι ένα νομοθετικό σώμα έχει χρησιμοποιηθεί για την θέσπιση τεχνικών προτύπων. Εμείς δεν συμφωνούμε απόλυτα με την συγκεκριμένη κριτική, καθώς θεωρούμε ότι ο στόχος της ήταν η απόκτηση πρακτικής εμπειρίας με τις ψηφιακές υπογραφές, προτού αυτές εξισωθούν με τις ιδιόχειρες. Οι Γερμανοί διατήρησαν την συγκεκριμένη άποψη και στα επίσημα σχόλια τους για την οδηγία **[SIGGa, 1999].** Δηλαδή κατ' αυτούς θα έπρεπε να υπάρχουν και τα ελάχιστα τεχνικά πρότυπα, τα οποία θα εγγυώνται την ασφάλεια των συστημάτων ηλεκτρονικών υπογραφών. Τα ίδια πρότυπα, σύμφωνα με τον γερμανικό νόμο θα πρέπει να ισχύουν για τις μη ευρωπαϊκές αρχές πιστοποίησης, και όχι αυτές να αναγνωρίζονται με βάση ειδικές σχέσεις που τυχόν θα έχουν με κάποια ευρωπαϊκή αρχή πιστοποίησης, όπως αναφέρεται στην οδηγία.

Για την λειτουργία μιας αρχής πιστοποίησης πρέπει να έχει υπάρξει αδειοδότηση από τον αρμόδιο γερμανικό οργανισμό, τον **RegTP** (Regulatory Authority for Telecommunications and Post). Εδώ βλέπουμε άλλη μία απόκλιση από την ευρωπαϊκή οδηγία. Η αδειοδότηση αυτή θα προέρθει από λεπτομερή

αξιολόγηση κάθε αίτησης για παροχή υπηρεσιών πιστοποίησης και μπορεί να απορριφθεί σε περίπτωση που δεν διαπιστεί αξιοπιστία ή τεχνική γνώση. Οι άδειες αυτές μπορούν να ανακληθούν. Ο RegTP είναι ο φορέας εκείνος που παίζει τον ρόλο της βασικής αρχής πιστοποίησης (root certification authority), που αναφέραμε στο κεφάλαιο 2, που υπογράφει δηλαδή τα πιστοποιητικά για τα δημόσια κλειδιά των αρχών πιστοποίησης. Επίσης ο RegTP είναι υπεύθυνος για την διαπίστευση των αρχών πιστοποίησης. Ο συγκεκριμένος οργανισμός είναι υπεύθυνος για την διαπίστευση της ασφάλειας προϊόντων πληροφορικής και πληροφοριακών συστημάτων, χωρίς να εξειδικεύεται μόνο σε αυτά που αφορούν τις αρχές πιστοποίησης. Όπως συμβαίνει σε πολλές περιπτώσεις, η αποτίμηση των πληροφοριακών συστημάτων γίνεται από κάποιον ελεγκτή, συνήθως έναν ιδιωτικό φορέα και με βάση τα αποτελέσματα της αποτίμησης αυτής, εγκρίνεται η πιστοποίηση. Η επαφή με τον συγκεκριμένο φορέα ελέγχου γίνεται συνήθως από τον ίδιο τον οργανισμό. Ο ελεγκτής όμως πρέπει να έχει λάβει σχετική άδεια από τον **RegTP**. Η πιστοποίηση που παρέχεται βασίζεται στα διεθνώς αναγνωρισμένα πρότυπα ITSEC και Common Criteria, στα οποία και έχουμε αναφερθεί.

Η ταυτοποίηση των υποκειμένων γίνεται με χρήση της ομοσπονδιακής ταυτότητας ή κάποιου διαβατηρίου. Οι αρχές πιστοποίησης δεν πρέπει να αποθηκεύουν ιδιωτικά κλειδιά, μπορούν όμως να τα παράγουν.

Γενικότερα το γερμανικό πλαίσιο, θεωρείται από πολλούς αρκετά αυστηρό με ιδιαίτερα μεγάλο κόστος για την αρχή πιστοποίησης, το οποίο καθίσταται απαγορευτικό όταν πρόκειται για μία αρχή πιστοποίησης εκτός Γερμανίας **[Ford, 2001].** Αυτό επιβαρύνεται και από τον μηχανισμό αδειοδότησης και επιτήρησης. Ενδεικτικά, στο **[Gutman, 2001]** αναφέρεται ότι η αρχή πιστοποίησης Telesec δαπάνησε 12.000.000 δολάρια για να λειτουργήσει με διαπιστευση κατά SigG, SigV.

Μία άλλη αρκετά σημαντική διαφορά αφορά την ευθύνη που έχουν οι αρχές πιστοποίησης. Συγκεκριμένα ο γερμανικός νόμος (γενικότερα, όχι μόνο αυτός που αφορά τις ψηφιακές υπογραφές) απορρίπτει την έννοια της ύπαρξης ευθύνης, αν δεν έχει προηγηθεί η σύναψη συμβολαίου. Πράγματι σύμφωνα με την ευρωπαϊκή οδηγία, η αρχή πιστοποίησης, έχει ευθύνη σε περίπτωση που προκληθεί οικονομική ή άλλης φύσεως ζημιά σε κάποια οντότητα, η οποία βασίστηκε στο πιστοποιητικό. Υποστηρίζεται όμως ότι κάτι τέτοιο είναι αρκετά αυστηρό, καθώς θα επιβαρύνει πάρα πολύ τις ευρωπαϊκές αρχές πιστοποίησης και θα δυσχεραίνει πάρα πολύ την στάση τους απέναντι στον ανταγωνισμό από τις ΗΠΑ, όπου δεν υπάρχει τέτοιο νομικό καθεστώς. Για την υλοποίηση λοιπόν της ευρωπαϊκής οδηγίας χρειάστηκε να γίνουν και αλλαγές στον γερμανικό αστικό κώδικα.

4.4.9.2 Μεγάλη Βρετανία.

Περνάμε τώρα στο άλλο άκρο. Στην Μ. Βρετανία η σχετική νομοθεσία είναι η Electronic Communications Act (ECA) του Ιουλίου του 2000 και υπεύθυνος κυβερνητικός οργανισμός είναι το υπουργείο εμπορίου και βιομηχανίας **(DTI – Department Of Trade And Industry)**. Σχετικά με την

προσαρμογή της οδηγίας έχει ξεκινήσει δημόσια διαβούλευση, τον Μάρτιο του 2001 **[DTI, 2001]**.Τα θέματα τα οποία τέθηκαν είναι τα εξής:

- **Η φύση της εθελοντικής διαπίστευσης.** Εδώ ζητήθηκαν οι απόψεις όλων των εμπλεκόμενων φορέων για το αν πρέπει να διατηρηθεί το υπάρχον καθεστώς διαπίστευσης, το οποίο θα περιγράψουμε στην συνέχεια ή αν η κυβέρνηση πρέπει να διαδραματίσει πιο ενεργό ρόλο.
- **Εποπτεία για τις υπηρεσίες πιστοποίησης.** Σχετικά με την φύση της εποπτείας και τις ακριβείς αρμοδιότητες του εποπτικού φορέα, υπάρχει η πρόταση για την αρχική υλοποίηση τους από το DIT σε συνεργασία με τον φορέα της εθελοντικής διαπίστευσης. Προτείνεται ανάλογα με τις ανάγκες της αγοράς να υπάρξει τροποποίηση του μηχανισμού αυτού σε 2 χρόνια.
- **Διορισμός εποπτικού φορέα για τις ασφαλείς διατάξεις δημιουργίας υπογραφής.** Η βρετανική κυβέρνηση πρότεινε στον συγκεκριμένο τομέα την διεξαγωγή της εποπτείας από τον φορέα που έχει αναλάβει την εθελοντική διαπίστευση με την συνεργασία του αρμόδιου υπουργείου.
- **Τροποποίηση της ECA για να συμβαδίζει με την οδηγία.** Αν και η ECA αναγνωρίζει τις ηλεκτρονικές υπογραφές, πρέπει να γίνουν τροποποιήσεις σχετικά με την εξίσωσης των αναγνωρισμένων ηλεκτρονικών υπογραφών με τις ιδιόχειρες.
- **Ευθύνη Παρόχων Υπηρεσιών Πιστοποίησης.** Η βρετανική κυβέρνηση δεν έχει λάβει καθόλου μέτρα στον συγκεκριμένο τομέα, οπότε για την απόδοση ελάχιστης ευθύνης, την οποία θέλει η οδηγία χρειάζεται η τροποποίηση κάποιων ρυθμίσεων της ECA.
- **Προστασία Δεδομένων Προσωπικού Χαρακτήρα.** Αφορά τις τροποποιήσεις που πρέπει να γίνουν στην εθνική νομοθεσία προστασίας δεδομένων, έτσι ώστε να ικανοποιηθούν οι απαιτήσεις για την συλλογή δεδομένων από τους πάροχους υπηρεσιών πιστοποίησης στο ευρύ κοινό.

Οι Βρετανοί έχουν ακολουθήσει την οδό της αυτορύθμισης. Η διαδικασία της διαπίστευσης γίνεται από τον μη κερδοσκοπικό οργανισμό tScheme. Απαρτίζεται από όλους τους ενδιαφερόμενους φορείς, γύρω από τις υπηρεσίες πιστοποίησης, δηλαδή την κυβέρνηση, πάροχους υπηρεσιών πιστοποίησης και εταιρείες τεχνολογίας. Η διαπίστευση είναι προαιρετική,

Ο συγκεκριμένος οργανισμός είναι υπεύθυνος για τις εξής λειτουργίες:

- Ανάπτυξη των προφίλ προστασίας (protection profiles), των κριτηρίων δηλαδή με βάση τα οποία γίνεται ο έλεγχος και η διαπίστευση.
- Δημιουργία οδηγιών εφαρμογής των προφίλ προστασίας.
- Επεξεργασία των αιτήσεων για διαπίστευση.
- Διαπίστευση και όλες οι σχετικές με αυτήν διαδικασίες (ανανέωση, ανάκληση, επίλυση διαφορών

κτλ.)

- Προώθηση της χρήσης υπηρεσιών πιστοποίησης.

Το πλαίσιο της διαπίστευσης θα μπορούσε να χαρακτηριστεί προσανατολισμένο προς τις υπηρεσίες (service - oriented). Η διαπίστευση γίνεται με βάση τα προφίλ προστασίας, τα οποία αναφέρονται τόσο σε τεχνικό όσο και σε διαδικαστικό επίπεδο. Βασίζονται σε ευρύτατα αποδεκτά πρότυπα, η αναγνώριση των οποίων προέρχεται από την αγορά. Η διαπίστευση αφορά την υλοποίησης *συγκεκριμένων* υπηρεσιών (δηλαδή καταχώρηση, έκδοση πιστοποιητικών, δημιουργία κλειδιών κτλ.) από συγκεκριμένους οργανισμούς. Για κάθε μία υπηρεσία από αυτές εκδίδεται συγκεκριμένο προφίλ προστασίας.

Πιο συγκεκριμένα τώρα τα προφίλ προστασίας που έχει εκδώσει το tScheme είναι τα εξής:

1. **Βασικό Προφίλ - Base Approval Profile.**

   Το συγκεκριμένο προφίλ προστασίας αποτελεί την βάση για την διαπίστευση. Ορίζει τα βασικά κριτήρια που πρέπει να πληροί ένας οργανισμός, έτσι ώστε να μπορεί να διαπιστευτεί στην συνέχεια με βάση ένα ειδικό προφίλ για μια συγκεκριμένη υπηρεσία. Τα κριτήρια που ορίζονται ανήκουν στις παρακάτω γενικές κατηγορίες:

   - Πολιτικές και Διαδικασίες για την Διαχείριση Ασφάλειας.
   - Αποτίμηση Τεχνικής Υποδομής.
   - Αποτίμηση Προσωπικού.
   - Αποτίμηση Σχέσεων με εξωτερικούς πάροχους υπηρεσιών ασφαλείας.
   - Φήμη στην αγορά.

2. **Προφίλ Υπηρεσιών Καταχώρησης - Profile for Registration Services.**

   Το προφίλ αυτό ορίζει τα κριτήρια τα οποία πρέπει να ικανοποιούν οι οργανισμοί οι οποίοι θέλουν να παρέχουν υπηρεσίες επαλήθευσης ταυτότητας και οποιασδήποτε άλλης ιδιότητας.

3. **Προφίλ Αρχής Πιστοποίησης - Profile for a Certification Authority.**

   Εδώ ορίζονται τα κριτήρια τα οποία τα οποία πρέπει να ικανοποιεί κάποιος οργανισμός έτσι ώστε να παρέχει υπηρεσίες πιστοποίησης.

4. **Προφίλ Διαχείρισης Κλειδιών - Profile for Signing Key Pair Management.**

   Τα κριτήρια τα οποία ορίζονται στο συγκεκριμένο προφίλ αφορούν υπηρεσίες διαχείρισης κλειδιών όπως:

   - Δημιουργία Κλειδιών.
   - Μεταφορά των ιδιωτικών κλειδιών στους νόμιμους κατόχους.
   - Ανάκληση Κλειδιών.

5. **Προφίλ Δημιουργίας Πιστοποιητικών - Profile For Certificate Generation.**

   Το συγκεκριμένο προφίλ συνδυάζει τα κριτήρια του προφίλ 1 και 4, για όσους οργανισμούς θέλουν να παρέχουν και τις δύο υπηρεσίες.

6. **Προφίλ Διάδοσης Πιστοποιητικών - Profile For Certificate Dissemination.**

Εδώ περιγράφονται κριτήρια για την λειτουργία και χρήση καταλόγων, μέσω των οποίων θα γίνεται η ανάκτηση των πιστοποιητικών.

7. **Προφίλ Διαχείρισης Κατάστασης Πιστοποιητικών - Profile For Certificate Status Management.**

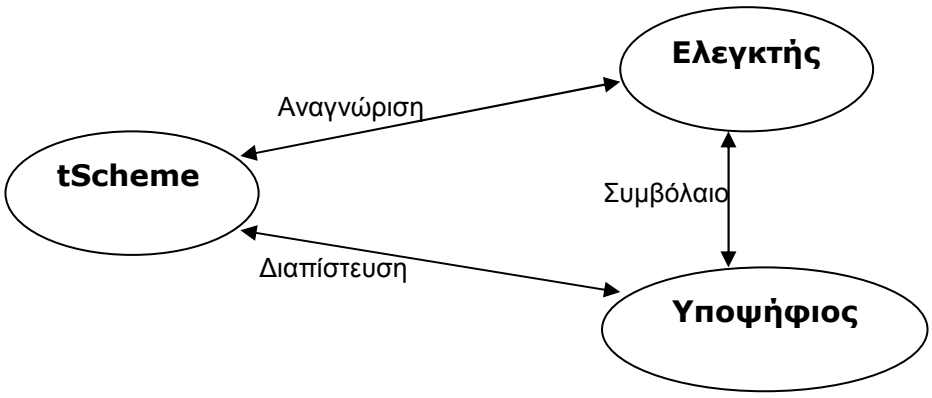
Με τα συγκεκριμένα κριτήρια που ορίζονται στο συγκεκριμένο προφίλ εγκρίνεται η παροχή υπηρεσιών από έναν οργανισμό σχετικά με την αλλαγή της κατάστασης πιστοποιητικών:

- Αυθεντικοποίηση Εντολέα Αίτησης Ανάκλησης, Αναστολής ή Ανανέωσης Πιστοποιητικών.
- Λήψη Απόφασης για την αλλαγή της κατάστασης.
- Ειδοποίηση των χρηστών που βασίζονται στα πιστοποιητικά των οποίων η κατάσταση έχει αλλάξει.

8. **Προφίλ Επαλήθευσης Εγκυρότητας Πιστοποιητικών - Profile For Certificate Status Validation.**

Οι οργανισμοί οι οποίοι έχουν διαπιστευτεί με το συγκεκριμένο προφίλ προστασίας μπορούν να παρέχουν υπηρεσίες επαλήθευσης εγκυρότητας πιστοποιητικών, με απλά λόγια δηλαδή να εκδίδουν λίστες ανάκλησης πιστοποιητικών (CRLs) ή να διατηρούν εξυπηρετητές του πρωτοκόλλου OCSP (On-line certificate status protocol).

Η διαπίστευση μπορεί να γίνει για ένα ή περισσότερα από τα παραπάνω προφίλ. Συγκεκριμένα η ενδιαφερόμενη αρχή πιστοποίησης ετοιμάζει ένα κείμενο στο οποίο περιγράφει με κάθε λεπτομέρεια τις υπηρεσίες για τις οποίες θέλει να διαπιστευτεί (το κείμενο αυτό ονομάζεται **Specification of Service(s) Subject to Assessment.** Έπειτα επιλέγει έναν εγκεκριμένο από το tScheme φορέα ελέγχου, ο οποίος είναι και αυτός που θα κάνει την αποτίμηση. Με αυτόν τον φορέα συνάπτει συμφωνία (χωρίς την παρέμβαση του tScheme) για τις λεπτομέρειες του ελέγχου. Ο ελεγκτής εξετάζει τα στοιχεία που παρείχε ο φορέας πιστοποίησης στα κείμενα του, αλλά και τον τρόπο με τον οποίο θα παρέχεται η υπηρεσία στην πράξη. Τα συμπεράσματα του τα υποβάλλει σε επίσημη αναφορά προς τον φορέα πιστοποίησης, ο οποίος με την σειρά του τα υποβάλλει στο tScheme, μαζί με την επίσημη πλέον αίτηση για πιστοποίηση. Το tScheme επιθεωρεί την αίτηση και αποφασίζει την έγκριση. Η έγκριση συνοδεύεται και από μία σφραγίδα, που δείχνει την πιστοποίηση.



Σχήμα 19. tScheme

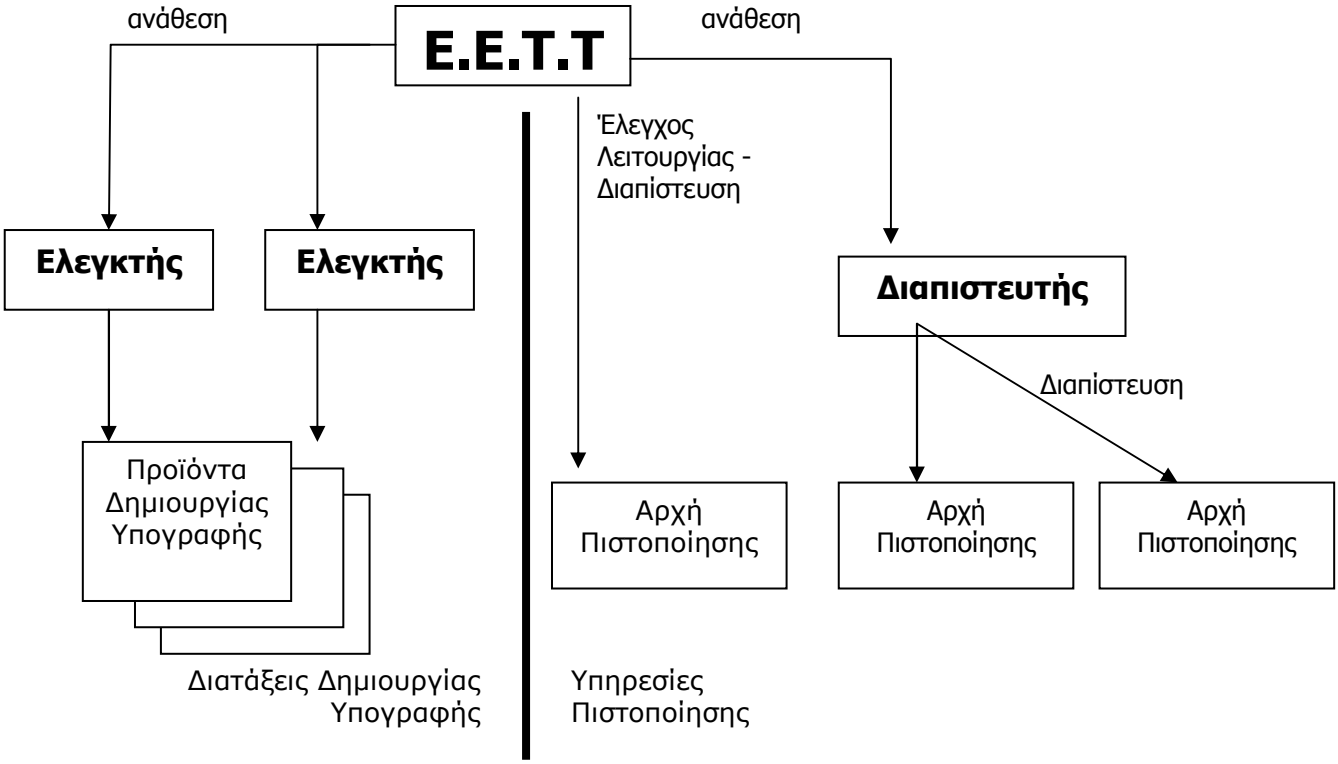
Τα πλεονεκτήματα του πλαισίου διαπίστευσης αυτού, σύμφωνα με τους Βρετανούς, είναι η ανεξαρτησία του, η διαπίστευση πολλών τομέων της παροχής υπηρεσιών πιστοποίησης και η στενή του σχέση με την αγορά η οποία επιτρέπει την γρήγορη αντίδραση στις ταχύτατες αλλαγές. Σε σχέση με την οδηγία της Ευρωπαϊκης Επιτροπής είναι πιο ευρύ καθώς δεν περιορίζεται στην αποτίμηση της διαδικασίας πιστοποίησης, αλλά σε ένα ευρύτερο πλαίσιο παροχής υπηρεσιών, ακόμα και στην περίπτωση που οι συγκεκριμένες υπηρεσίες αποτελούν αντικείμενο εξωτερικής ανάθεσης σε κάποιον τρίτο οργανισμό (outsourcing). Επίσης ένα σημαντικό στοιχείο σύμφωνα με τους Βρετανούς, είναι ότι το δικό τους πλαίσιο, συνδυάζει αφενός τον έλεγχο που ασκεί πάνω στους φορείς πιστοποίησης, ο οποίος όμως τους παρέχει βαθμούς ελευθερίας έτσι ώστε να είναι ανταγωνιστικοί στην αγορά. Γενικότερα, οι Βρετανοί, ως παρεπόμενο ίσως της στενής σχέσης τους με τις ΗΠΑ, προτιμούν την αυτορύθμιση της αγοράς, παρά την επιβολή ενός στενού πλαισίου. Επίσης έχουν τις ίδιες αμφιβολίες σχετικά με το θέμα της ευθύνης που υπέχουν οι φορείς πιστοποίησης προς τους χρήστες των ηλεκτρονικών υπογραφών, οι οποίες παρατηρούνται και σε άλλα κράτη, τείνοντας προς την άποψη της διευθέτησης του συγκεκριμένου θέματος από τον ισχύοντα νόμο σε κάθε κράτος.

4.4.9.3 Ελλάδα

Η Ελλάδα, υιοθέτησε επίσημα την οδηγία της Ευρωπαϊκής Ένωση για τις ηλεκτρονικές υπογραφές με προεδρικό διάταγμα στις 13 Ιουνίου 2001, το οποίο και δημοσιεύτηκε στην εφημερίδα της κυβερνήσεως στις 25 Ιουνίου 2001 **[ΠΔΗΥ, 2001]**. Ο μοναδικός λόγος για τον οποίο παραθέσαμε τις παραπάνω ημερομηνίες είναι γιατί η προθεσμία υιοθέτησης της οδηγίας ήταν η 19^{η} Ιουλίου 2001, (18 μήνες μετά την δημοσίευση της ευρωπαϊκής οδηγίας). Οι ελληνικές κινήσεις ήταν δηλαδή οριακές.

Το προεδρικό διάταγμα αποτελεί ουσιαστικά μια μετάφραση της ευρωπαϊκής οδηγίας. Ουσιαστικά δεν έχει να προσθέσει τίποτα καινούριο, απλώς εξειδικεύει ορισμένα γενικά στοιχεία της οδηγίας για την Ελλάδα. Οι απαιτήσεις για τις διατάξεις δημιουργίας υπογραφών, τα αναγνωρισμένα πιστοποιητικά, τους πάροχους υπηρεσιών πιστοποίησης αλλά και οι συστάσεις για την ασφαλή επαλήθευση μιας ηλεκτρονικής υπογραφής είναι ταυτόσημες με τις ευρωπαϊκές. Δεν θα ήταν βέβαια δυνατή, η εισαγωγή καινοτομιών από την ελληνική πλευρά, καθώς ακόμα και η Γερμανία αναθεώρησε για να συμβαδίσει με την οδηγία.

Συγκεκριμένα ο αρμόδιος φορέας για την διαπίστευση των προϊόντων δημιουργίας ηλεκτρονικών υπογραφών ορίζεται η **Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ)**. Επίσης η εθελοντική διαπίστευση σε πάροχους υπηρεσιών πιστοποίησης δίδεται και πάλι από την ΕΕΤΤ. Το σχήμα λοιπόν του ελληνικού πλαισίου διαπίστευσης φαίνεται παρακάτω:



Σχήμα 20. Αρμοδιότητες που προκύπτουν από το προεδρικό διάταγμα

Στο παραπάνω σχήμα η διάκριση μεταξύ των όρων ελεγκτή και διαπιστευτή είναι τυπική, με σκοπό να τονίσει την διάκριση μεταξύ της διαπίστευσης των προϊόντων δημιουργίας ηλεκτρονικών υπογραφών και των υπηρεσιών πιστοποίησης. Μπορεί κάλλιστα ο ίδιος οργανισμός να είναι υπεύθυνος και για τις δύο αυτές δραστηριότητες. Από το σχήμα λοιπόν φαίνεται πως η ΕΕΤΤ ορίζει τρίτους ή λειτουργεί η ίδια ως φορέας διαπίστευσης παρόχων υπηρεσιών πιστοποίησης και προϊόντων δημιουργίας ηλεκτρονικών υπογραφών. Άσχετα με το αν ένας φορέας είναι διαπιστευμένος ή όχι, μπορεί να υποστεί έλεγχο από την ΕΕΤΤ.

Αξίζει επιπλέον να επισημάνουμε τα εξής στοιχεία, στα οποία, όπως προαναφέραμε δεν υπάρχει, απόκλιση από τη Ευρωπαϊκή Οδηγία:

Ο πάροχος υπηρεσιών πιστοποίησης υπέχει ευθύνη προς το ευρύ κοινό για τυχόν ζημιές που προκαλούνται από ένα πιστοποιητικό που έχει αυτός εκδώσει. Είναι δυνατή η παροχή υπηρεσιών πιστοποίησης από οποιοδήποτε φορέα που ανήκει σε κράτος μέλος της ΕΕ, ή από οποιονδήποτε φορέα οποιασδήποτε χώρας αρκεί να πληροί τις συστάσεις της Ευρωπαϊκής Οδηγίας.

Τον Νοέμβριο του 2001, η ΕΕΤΤ εξέδωσε πρόσκληση υποβολής απόψεων σχετικά με τις ηλεκτρονικές υπογραφές, σε θέματα που άπτονται της παροχής υπηρεσιών πιστοποίησης και της εθελοντικής διαπίστευσης **[ΕΕΤΤ, 2001]**. Τα θέματα που τέθηκαν εκεί, θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο της εργασίας.

4.5 Η αμερικανική προσέγγιση

Οι Ηνωμένες Πολιτείες είναι φυσικό να κατέχουν την πρωτοκαθεδρία στον τομέα των ηλεκτρονικών πιστοποιητικών, καθώς οι αντίστοιχες τεχνολογίες βρίσκονται σε εφαρμογή από την αρχή της έκρηξης του ηλεκτρονικού εμπορίου, περίπου δηλαδή πριν από το 1995. Όπως είναι γνωστό όμως, τα αίτια της πρωτοκαθεδρίας οφείλονται στην χρήση ηλεκτρονικών πιστοποιητικών για Business To Consumer (B2C) εφαρμογές ηλεκτρονικού εμπορίου σε πρωτόκολλα όπως το SSL, με στόχο την απόκρυψη ευαίσθητων οικονομικών στοιχείων, όπως για παράδειγμα των αριθμών πιστωτικών καρτών. Σιγά, σιγά και με τις εξαγγελίες της κυβέρνησης Κλίντον για την *Παγκόσμια Πληροφοριακή Υποδομή (Global Information Infrastructure)* άρχισαν να ακολουθούν και οι διάφορες ομοσπονδιακές υπηρεσίες. Βέβαια δεν υπήρξε κάποιος κεντρικός συντονισμός σε όλες αυτές τις προσπάθειες, με αποτέλεσμα ακόμα και οι τελευταίες να αναπτύσσουν η κάθε μια ξεχωριστά την υποδομή της.

Όπως προαναφέραμε στην εισαγωγή, η Utah ήταν η πρώτη πολιτεία των ΗΠΑ, η οποία από το 1995 υιοθέτησε νομοθετική πράξη για ηλεκτρονικές υπογραφές. Η συγκεκριμένη νομοθετική πράξη, μάλιστα μπορεί να χαρακτηριστεί αρκετά πρωτοποριακή, καθώς ορίζει ένα πλαίσιο διαπίστευσης, για τις αρχές πιστοποίησης. Όσες ενταχθούν σε αυτό και λάβουν την απαιτούμενη άδεια, αντιμετωπίζουν περιορισμένη ευθύνη από λανθασμένα περιεχόμενα πιστοποιητικών. Πολλές πολιτείες ακολούθησαν το παράδειγμα της Utah, ακολουθώντας όμως η κάθε μία διαφορετικές αρχές. Η California για παράδειγμα κινήθηκε σε εντελώς αντίθετη κατεύθυνση, υιοθετώντας μία τεχνολογικά ουδέτερη προσέγγιση στην οποία ηλεκτρονική υπογραφή είναι οποιοδήποτε ηλεκτρονικό σύμβολο έχει συμφωνηθεί από τις ενδιαφερόμενες οντότητες. Η πολιτεία της Μασαχουσέτης, υιοθετεί την παραδοσιακή θέση ότι δεν μπορεί να υπάρξει άρνηση της ισχύος μιας υπογραφής, μόνο και μόνο επειδή είναι σε ηλεκτρονική μορφή. Δεν ορίζεται όμως τίποτα ούτε για υπηρεσίες πιστοποίησης, ούτε για συγκεκριμένες τεχνολογίες. Όπως είναι φυσικό οι τόσο διαφορετικές ρυθμίσεις (αλλά και οι υλοποιήσεις τους) που προτάθηκαν, θα δημιουργούσαν ασυμβατότητες και θα δυσχέραιναν την ανάπτυξη του ηλεκτρονικού εμπορίου στις ΗΠΑ. Κατά συνέπεια, και εκεί υπήρξε απαίτηση για ένα ενιαίο πλαίσιο, σε ομοσπονδιακό αυτή τη φορά επίπεδο.

Η **Νομοθετική Πράξη για τις Ηλεκτρονικές Υπογραφές στο Εθνικό και Διεθνές Εμπόριο** (Electronic Signatures in Global and National Commerce Act), η οποία αναφέρεται και ως **E-Sign Act** υπογράφτηκε το καλοκαίρι του 2000 και η εφαρμογή της ξεκίνησε τον Οκτώβριο της ίδιας χρονιάς. Από τους νόμους των διαφορών προσπαθειών έχει περισσότερες ομοιότητες με αυτόν της Μασαχουσέτης. Η βασική της αρχή είναι ότι δεν μπορεί να αρνηθεί κάποιος νομική ισχύ σε μια συναλλαγή μόνο και μόνο επειδή είναι ηλεκτρονική. Συγκεκριμένα, η παραπάνω διάταξη αφορά τόσο τις ηλεκτρονικές υπογραφές όσο και τα ηλεκτρονικά έγγραφα. Ως παρατήρηση αναφέρουμε, ότι το κεντρικό σημείο της συγκεκριμένης νομοθετικής πράξης δεν είναι οι ηλεκτρονικές υπογραφές καθ'αυτές, αλλά η εξασφάλιση της εγκυρότητας και εφαρμοσιμότητας των ηλεκτρονικών εγγράφων, με μεγαλύτερη βαρύτητα να δίνεται στα ηλεκτρονικά συμβόλαια. Επιπλέον, υπό την πίεση οργανώσεων για την προστασία των καταναλωτών **[Wittie, 2000],**

παρέχει ένα σύνολο από διατάξεις οι οποίες εξασφαλίζουν ότι αφενός το ευρύ κοινό θα είναι δυνατό να έχει πρόσβαση στις ηλεκτρονικές υπηρεσίες και αφετέρου ότι θα έχει δώσει την συναίνεση του. Επίσης δεν καλυπτονται όλα τα είδη ηλεκτρονικών κειμένων. Δεν ισχύει για δικαστικές πράξεις, διαθήκες και άλλα έγγραφα οικογενειακού δικαίου. Τέλος, σε ό,τι αφορά τις ηλεκτρονικές υπογραφές και εδώ, η προσέγγιση που ακολουθείται είναι τεχνολογικά ουδέτερη, καθώς η ηλεκτρονική υπογραφή χαρακτηρίζεται ως '*οποιοδήποτε ηλεκτρονικό σύμβολο, ήχος ή διαδικασία η οποία έχει προσαρτηθεί ή συσχετίζεται λογικά με κάποιο συμβόλαιο ή άλλο έγγραφο, και χρησιμοποιείται για να επιδείξει την πρόθεση του υπογράφοντα να υπογράψει το συγκεκριμένο έγγραφο.* **[E-Sign, 2000].**

Επιπλέον η κυβερνητική πράξη για την εξάλειψη της γραφειοκρατίας (**Government Paperwork Elimination Act)**, επιτάσσει την χρήση από τις ομοσπονδιακές υπηρεσίες ηλεκτρονικών μέσων για την διακίνηση εγγράφων και την τήρηση αρχείων, όπου αυτό είναι δυνατόν. Η συγκεκριμένη πράξη πρέπει να έχει εφαρμοστεί μέχρι το 2003. Με τις παραπάνω πράξεις έγινε επιτακτική η ανάγκη διασύνδεσης της υποδομής που όπως αναφέραμε στην αρχή ανέπτυσσε χωριστά κάθε ομοσπονδιακή υπηρεσία. Κατά συνέπεια, στις ΗΠΑ *η ανάγκη για την δημιουργία ενός ολοκληρωμένου πλαισίου γύρω από τις ηλεκτρονικές υπογραφές βασίζεται κυρίως στην ανάγκη για συμβατότητα σε τεχνικό επίπεδο και σε επίπεδο πολιτικής πιστοποίησης*. Η ολοκλήρωση της υποδομής αυτής αναφέρεται ως **Federal Public Key Infrastructure (FPKI).** Ένα πολύ σημαντικό χαρακτηριστικό της, είναι η ταύτιση της με τα πρότυπα της IETF, για την υποδομή δημοσίου κλειδιού και συγκεκριμένα για τις πολιτικές και πρακτικές πιστοποίησης **[RFC 2527, 1999].**

Κεντρικές οντότητες στο πλαίσιο διαπίστευσης αυτό των ΗΠΑ, είναι μία αρχή που καθορίζει την πολιτική, η **FPKIPA (Federal Public Key Infrastructure Policy Authority)** και μία αρχή που είναι υπεύθυνη σε λειτουργικό επίπεδο για την όλη υποδομή, η **FBCA (Federal Bridge Certification Authority).**

Σε γενικές γραμμές το πλαίσιο αυτό λειτουργεί ως εξής: Κάθε ομοσπονδιακός οργανισμός, αντί να υπογράψει το πιστοποιητικό κάθε άλλου, πράγμα που θα οδηγούσε σε πολύ μεγάλη αύξηση της πολυπλοκότητας και σε δυσκολία διαχείρισης, πιστοποιείται από την FBCA, η οποία διαδραματίζει τον ρόλο γέφυρας μεταξύ όλων των οργανισμών. Έτσι σε περίπτωση συναλλαγής μεταξύ δύο οντοτήτων που έχουν πιστοποιηθεί από δύο ομοσπονδιακούς οργανισμούς, το κοινό σημείο εμπιστοσύνης που κάνει την συναλλαγή αυτή εφικτή είναι η ύπαρξη πιστοποίησης και των δύο οργανισμών από την FBCA. Η διαδικασία αυτή, παρότι έχει προέρθει από την ανάγκη για επίτευξη διαλειτουργικότητας, μπορεί να χαρακτηριστεί ως μια διαδικασία διαπίστευσης, γιατί αφενός έχει έμφυτη την διαδικασία της *έγκρισης* που γίνεται με την εισαγωγή ενός οργανισμού (για την ώρα μόνο ομοσπονδιακού) στην ευρύτερη υποδομή του FPKI, και αφετέρου γιατί όπως θα δούμε και στην συνέχεια έχει έμφυτο το στοιχείο της αξιολόγησης και του ελέγχου. Προτού προχωρήσουμε στην περιγραφή της διαδικασίας της διαπίστευσης αυτής είναι απαραίτητο να επισημάνουμε δύο πράγματα. Πρώτον, ότι δεν είναι υποχρεωτική, δηλαδή δύο ομοσπονδιακές υπηρεσίες μπορούν να πιστοποιηθούν μεταξύ τους και να συναλλάσσονται κανονικά και

δεύτερον όπως, προαναφέραμε ότι δεν υποστηρίζεται ακόμα η εισαγωγή ιδιωτικών οργανισμών και γενικά οποιουδήποτε οργανισμού βρίσκεται εκτός της ομοσπονδιακής κυβέρνησης των ΗΠΑ.

Η πιστοποίηση από την FBCA γίνεται σε δύο επίπεδα. Σε επίπεδο πολιτικής και σε τεχνικό επίπεδο. Το πιο σημαντικό από αυτά τα δύο είναι το επίπεδο πολιτικής. Για να πιστοποιηθεί ένας οργανισμός από την FBCA πρέπει να έχει είτε σε φάση λειτουργίας είτε σε φάση σχεδιασμού μία υποδομή δημοσίου κλειδιού, η οποία θα περιλαμβάνει τουλάχιστον μία αρχή πιστοποίησης, ένα σύστημα καταλόγου για την υποστήριξη της όλης υποδομής, μία ή περισσότερες πολιτικές πιστοποίησης και μία δήλωση πρακτικών πιστοποίησης. Σε περίπτωση που υπάρχουν περισσότερες από μία αρχές πιστοποίησης, ορίζεται μία από αυτές ως κύρια. Αυτή θα είναι εκείνη που θα πιστοποιηθεί από την FBCA.

Η FBCA έχει υιοθετήσει μία πολιτική πιστοποίησης, η οποία έχει συνταχθεί από την FPKIPA και καθορίζει 4 λειτουργικά επίπεδα διαβεβαίωσης (και ένα δοκιμαστικό) για την διαδικασία της πιστοποίησης. Η πολιτική αυτή ακολουθεί πιστά την δομή του **[RFC 2527, 1999].** Τα επίπεδα διαβεβαίωσης αυτά, αντανακλούν την βεβαιότητα που μπορεί να έχει μία οντότητα ότι υπάρχει ταύτιση μεταξύ του πραγματικού κατόχου του δημοσίου κλειδιού που υπάρχει σε ένα πιστοποιητικό και του ονόματος στο οποίο έχει εκδοθεί το πιστοποιητικό. Επίσης αντανακλούν την βεβαιότητα που μπορεί υπάρχει στην ασφάλεια του αντίστοιχου ιδιωτικού κλειδιού και την εμπιστοσύνη προς το σύστημα που χρησιμοποιήθηκε για την παραγωγή τόσο των κλειδιών όσο και των πιστοποιητικών. Τα τέσσερα επίπεδα αυτά είναι τα εξής:

- **Στοιχειώδες (Rudimentary):** Παρέχει την ελάχιστη δυνατή διαβεβαίωση για την ταυτότητα του κατόχου του δημοσίου κλειδιού. Η κύρια χρήση του είναι σε περιβάλλοντα χαμηλού κινδύνου, όπου η απαίτηση για αυθεντικοποίηση είναι μικρή. Υποστηρίζει κυρίως απαιτήσεις ακεραιότητας δεδομένων. Κατά την καταχώρηση του ονόματος του υποκειμένου του πιστοποιητικού, αρκεί να παρέχεται μία οποιαδήποτε τιμή στο πεδίο του ονόματος ή στο εναλλακτικό πεδίο του ονόματος στο πιστοποιητικό X.509. Δεν υπάρχει απαίτηση επαλήθευσης της ταυτότητας του υποκειμένου. Η έκδοση πιστοποιητικού γίνεται με την παροχή μιας έγκυρης διεύθυνσης ηλεκτρονικού ταχυδρομείου. Τα κλειδιά παράγονται είτε από λογισμικό είτε από υλικό.
- **Βασικό (Basic):** Παρέχει μία σχετική διαβεβαίωση και χρησιμοποιείται σε περιβάλλοντα όπου υπάρχουν μεν απειλές αλλά δεν θεωρούνται μείζονος σημασίας. Και εδώ το υποκείμενο αρκεί να παρέχει ένα οποιοδήποτε όνομα κατά την διαδικασία καταχώρησης του στο πιστοποιητικό. Η ταυτότητα του αντικειμένου πιστοποιείται με εμφάνιση του ίδιου ενώπιον της αρχής καταχώρησης ή κάποιας άλλης αναγνωρισμένης αρχής. Η ανανέωση των πιστοποιητικών μπορεί να γίνει με την ηλεκτρονική υποβολή μίας αίτησης, η οποία θα έχει υπογραφεί με το ήδη υπάρχον ιδιωτικό κλειδί. Η ανανέωση του πιστοποιητικού γίνεται όπως και στο προηγούμενο επίπεδο, εκτός αν έχουν περάσει 15 χρόνια από την αρχική εγγραφή, οπότε η διαδικασία της εγγραφής επαναλαμβάνεται πλήρως. . Η αρχή πιστοποίησης υποχρεούται να ανακαλέσει ένα πιστοποιητικό μέσα σε 6 ώρες από την αρχική αίτηση του υποκειμένου.
- **Μέτριο (Medium):** Παρέχει διαβεβαίωση σχετικά με την ταυτότητα η οποία μπορεί να

χρησιμοποιηθεί σε περιβάλλοντα όπου υπάρχουν κίνδυνοι μετρίου επιπέδου, όπως σε περιπτώσεις όπου ανταλλάσσονται χρηματικά ποσά ή υπάρχει κίνδυνος απάτης από ένα από τα εμπλεκόμενα μέρη. Το υποκείμενο του πιστοποιητικού ταυτοποιείται με ένα διακεκριμένο όνομα κατά X.500. Και εδώ απαιτείται φυσική παρουσία του υποκειμένου κατά την αίτηση του πιστοποιητικού, καθώς επίσης και η παροχή των απαραίτητων πιστοποιητικών εγγράφων τα οποία σύμφωνα με την πολιτική πρέπει υποχρεωτικά να περιέχουν φωτογραφία. Η διαδικασία εγγραφής για την ανανέωση πιστοποιητικών επαναλαμβάνεται κάθε 9 χρόνια. Η αρχή πιστοποίησης υποχρεούται να ανακαλέσει ένα πιστοποιητικό μέσα σε 2 ώρες από την αρχική αίτηση του υποκειμένου. Οι λίστες ανάκλησης εκδίδονται τουλάχιστον μία φορά την μέρα ή το πολύ μετά από 18 ώρες από την ειδοποίηση παραβίασης του ιδιωτικού κλειδιού.

- **Υψηλό (High):** Παρέχει διαβεβαίωση σε περιπτώσεις όπου υπάρχει μεγάλος κίνδυνος απώλειας δεδομένων ή σε περίπτωση που η απώλεια των δεδομένων θα έχει καταστροφικές συνέπειες. Το υποκείμενο του πιστοποιητικού ταυτοποιείται με ένα διακεκριμένο όνομα κατά X.500, και εδώ. Οι απαιτήσεις επαλήθευσης της ταυτότητας είναι ίδιες με αυτές του προηγούμενου επιπέδου, μόνο που εδώ διεξάγεται σημαντικός έλεγχος για την εξακρίβωση της νομιμότητας των παρεχόμενων πιστοποιητικών. περιέχουν φωτογραφία. Η διαδικασία εγγραφής για την ανανέωση πιστοποιητικών επαναλαμβάνεται κάθε 3 χρόνια, τουλάχιστον. Η αρχή πιστοποίησης υποχρεούται να ανακαλέσει ένα πιστοποιητικό μέσα σε 30 λεπτά από την αρχική αίτηση του υποκειμένου. Οι λίστες ανάκλησης εκδίδονται τουλάχιστον μία φορά την μέρα ή το πολύ μετά από 6 ώρες από την ειδοποίηση παραβίασης του ιδιωτικού κλειδιού. Τα κλειδιά παράγονται μόνο από υλικό.

Κάθε ομοσπονδιακή υπηρεσία, λοιπόν, που θέλει να εισέλθει στο FPKI υποβάλλει μία αίτηση εισαγωγής στην FPKIPA. Η αίτηση αυτή περιέχει πληροφορίες για τον οργανισμό, τις πολιτικές πιστοποίησης της κύριας αρχής του, τεχνικές λεπτομέρειες της υποδομής δημοσίου κλειδιού του καθώς επίσης και τις διαδικασίες ελέγχου που χρησιμοποιεί έτσι ώστε να εφαρμόζεται η πολιτική πιστοποίησης. Πιο σημαντικά όμως περιέχει την αντιστοίχηση της πολιτικής πιστοποίησης του με αυτήν της FBCA που αναφέραμε νωρίτερα. Η FPKIPA επιθεωρεί την αίτηση και σε περίπτωση που την αποδεχτεί, υπογράφει ένα μνημόνιο συμφωνίας με τον οργανισμό (Memorandum Of Agreement) το οποίο καθορίζει τις ευθύνες κάθε μιας από τις 2 πλευρές. Τυπικά οι ευθύνες της FPKIPA είναι οι εξής:

- Επίβλεψη και εξασφάλιση της λειτουργίας της υποδομής δημοσίου κλειδιού και του καταλόγου της FBCA, σύμφωνα με αυτά που δηλώνει η πολιτική πιστοποίησης της.
- Ειδοποίηση του οργανισμού σε περίπτωση οποιουδήποτε προβλήματος.
- Πρόσβαση σε πληροφορίες σχετικά με την καθημερινή λειτουργία της αρχής πιστοποίησης καθώς επίσης και στα αποτελέσματα των διαφόρων ελέγχων που διεξάγονται.

Με την σύναψη της συγκεκριμένης συμφωνίας η ομοσπονδιακή υπηρεσία υποχρεούται να:

- Αποκρίνεται έγκαιρα σε όποια απαίτηση για παροχή πληροφοριών από την FBCA / FPKIPA.
- Γνωστοποιεί έγκαιρα οποιασδήποτε αλλαγής στις πληροφορίες που αναφέρονται στην αίτηση

της.

- Εξασφάλιζει ότι οι έλεγχοι που αναφέρονται στην δήλωση πρακτικών πιστοποίησης πραγματοποιούνται και να αναφέρει τα αποτελεσμάτα τους στην FBCA / FPKIPA.

Το μνημόνιο αυτό, ρυθμίζει όλες τις σχέσεις μιας αρχής πιστοποίησης με την FPKIPA. Ο ομοσπονδιακός οργανισμός μπορεί να αποχωρήσει οποτεδήποτε από την συμφωνία αυτή, ενώ η FPKIPA θα αποχωρήσει και θα ακυρώσει την πιστοποίηση (κάτι που συνεπάγεται την ανάκληση όλων των πιστοποιητικών) αν διαπιστώσει μη συμμόρφωση με κάποιες από τις παραμέτρους της συμφωνίας.

4.6 Άλλες αξιόλογες κρατικές προσεγγίσεις

4.6.1 Καναδάς

Σε αντίθεση με τις ΗΠΑ, που ακολουθήθηκε μία bottom up προσέγγιση, με την οποία συνδέθηκαν υπάρχουσες αρχής πιστοποίησης, στον Καναδά ακολουθήθηκε μία top – down προσέγγιση. Το πλαίσιο διαπίστευσης του Καναδά (Government Of Canada Public Key Infrastructure – GOCPKI) συμβαδίζει στενά με το κυβερνητικό πρόγραμμα *Government Online*, το οποίο έχει ως στόχο την ηλεκτρονική διεξαγωγή όλων των δραστηριοτήτων της ομοσπονδιακής κυβέρνησης μέχρι το 2004. Επίσης έχει αναπτυχθεί σε στενή συνεργασία με τον NIST, και όπως καταλαβαίνουμε έχει δεχθεί επιρροές από την αμερικανική προσέγγιση (και αντίστροφα). Αρχικά το συγκεκριμένο πρόγραμμα, θα περιοριστεί μόνο στις συναλλαγές μεταξύ κυβερνητικών φορέων και δημόσιων υπηρεσιών. Το GOCPKI ξεκίνησε ως πρωτοβουλία το 1993, οπότε και άρχισε η ανάπτυξη των απαιτήσεων για την υποδομή. Βασική προϋπόθεση ήταν η όλη υποδομή να βασίζεται σε ανοικτά πρότυπα, αλλά και σε εμπορικά διαθέσιμο λογισμικό. Μάλιστα η ομοσπονδιακή κυβέρνηση σύναψε συμφωνία με την εταιρεία Nortel Networks Inc., η οποία αργότερα έγινε η γνωστή για τα προϊόντα της σε ότι αφορά την υποδομή δημοσίου κλειδιού PKI, Entrust Inc. Για να είμαστε ακριβείς δεν είναι ακριβώς ένα πλαίσιο διαπίστευσης, με την τυπική έννοια που προαναφέραμε, δηλαδή της έμπρακτης εμπιστοσύνης προς τα πιστοποιητικά που εκδίδει μια αρχή πιστοποίησης. Η έννοια της διαπίστευσης συνδέεται στενά και εδώ με την έννοια της διαλειτουργικότητας και της συμβατότητας.

Τα πιστοποιητικά που εκδίδονται αφορούν μόνο τις συναλλαγές με την κυβέρνηση. Όπως είναι λογικό δηλαδή δεν μπορεί ένα πιστοποιητικό το οποίο εκδίδεται υπό το GOCPKI να χρησιμοποιηθεί για συναλλαγές με τρίτες οντότητες. Είναι συμβατό τεχνικά με όλες τις υποδομές που έχουν αναπτυχθεί σε παγκόσμιο επίπεδο και στηρίζεται σε ανοικτά πρότυπα (κυρίως αυτά της IETF), παρά το γεγονός ότι η ανάπτυξη του έγινε από συγκεκριμένη εταιρεία.

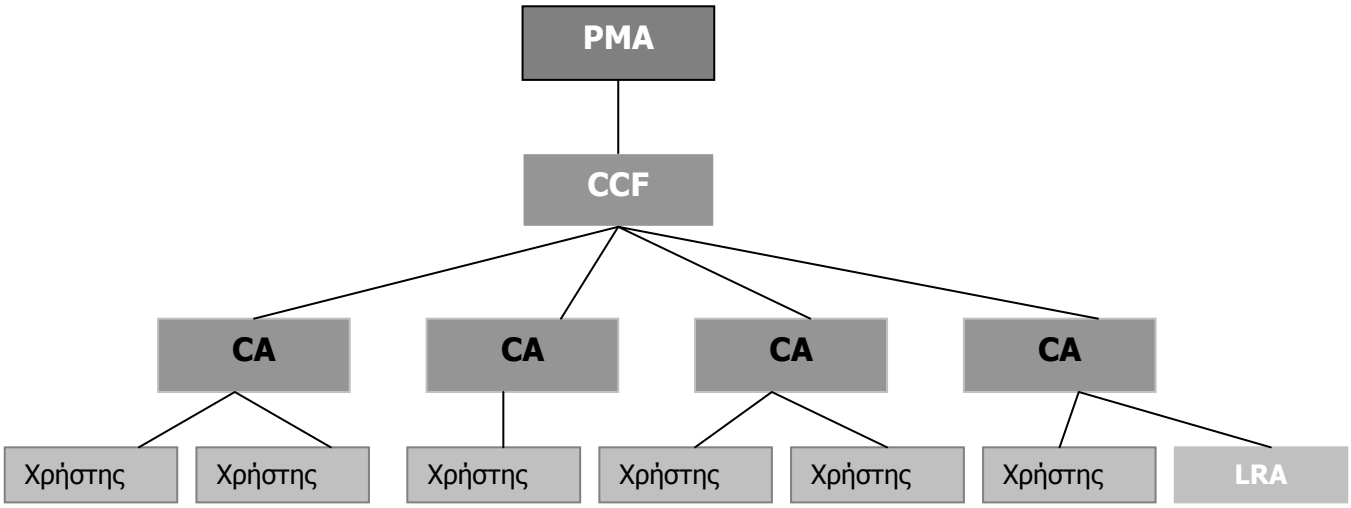
Στο GOCPKI, υποστηρίζονται τα τέσσερα επίπεδα διαβεβαίωσης πιστοποιητικών τα οποία είδαμε και στις ΗΠΑ. Για κάθε ένα επίπεδο έχουν οριστεί δύο πολιτικές πιστοποίησης, μία όταν πρόκειται να χρησιμοποιηθεί για κρυπτογράφηση και μία όταν πρόκειται να χρησιμοποιηθεί για ψηφιακή υπογραφή **[CAN4, 2001]**. Οι πολιτικές πιστοποίησης αυτές ακολουθούν πιστά την δομή του **[RFC 2527, 1999].**

Παρακάτω αναφέρουμε κάποιες γενικές αρχές που διέπουν τις συγκεκριμένες πολιτικές, όταν αυτές

ενσωματώνονται σε πιστοποιητικά που θα χρησιμοποιηθούν για ψηφιακές υπογραφές.

- **Στοιχειώδες Επίπεδο:** Τα συγκεκριμένα πιστοποιητικά μπορούν να χρησιμοποιηθούν για αυθεντικοποίηση σχέσεων και όχι ταυτοτήτων, όπως για παράδειγμα το ότι μια οντότητα εργαζεται σε μία κυβερνητική υπηρεσία. Έτσι για τον συγκεκριμένο τύπο πιστοποιητικών δίνονται οι λιγότερες δυνατές εγγυήσεις. Όπως και στις ΗΠΑ, οι απαιτήσεις ταυτοποίησης που απαιτούνται για την έκδοση τους, είναι μία έγκυρη διεύθυνση email. Δεν απαιτείται η ύπαρξη καταλόγου, οπότε ο κάθε χρήστης θα πρέπει να τα προσαρτά σε κάθε κάθε ηλεκτρονικό κείμενο. Δεν ορίζεται η έννοια της ανάκλησης και κατά συνέπεια δεν υπάρχουν λίστες ανάκλησης πιστοποιητικών. Δεν υπάρχει υποχρέωση επίσης για την καταγραφή σχετικών πληροφοριών. Τέλος σε περίπτωση που υπάρχει κάποια λάθος πληροφορία στα συγκεκριμένα πιστοποιητικά, η κυβέρνηση του Καναδά δεν φέρει καμία ευθύνη.
- **Βασικό Επίπεδο:** Τα πιστοποιητικά βασικού επιπέδου διαβεβαίωσης χρησιμοποιούνται μόνο για την αυθεντικοποίηση οντοτητών και την ακεραιότητα συναλλαγών σε συναλλαγές μικρού οικονομικού κινδύνου.Στο συγκεκριμένο επίπεδο διαβεβαίωσης, καθορίζονται πιο σημαντικοί ρόλοι για την αρχή πιστοποίησης και καταχώρησης, αλλά και για τους συνδρομητές και τους χρήστες. Η ευθύνη για συναλλαγές του συγκεκριμένου τύπου περιορίζεται σε αυτές με χρηματικό ύψος μέχρι 5000 δολλάρια. Για να εκδωθούν πρέπει να υπάρξει κάποια διαδικασία αυθεντικοποίησης του υποκειμένου, με τα δεδομένα τα οποία συλλέγονται κατά την διάρκεια της να μην πρέπει να αποκαλύπτονται. Προδιαγράφονται σαφείς διαδικασίες ανάκλησης, οι οποίες ορίζουν ότι ο χρόνος που μεσολαβεί από την αίτηση ανάκλησης, εώς την ενημέρωση της λίστας ανάκλησης του πιστοποιητικού είναι 24 ώρες. Υπάρχουν σαφείς απαιτήσεις καταγραφής γεγονότων που σχετίζονται με τα ίδια τα πιστοποιητικά αλλά και την λειτουργία της αρχής. Λειτουργίες της αρχής πιστοποίησης που έχουν σχέση με πιστοποιητικά αυτού του επιπέδου, πρέπει να εκτελούνται από 2 άτομα. Τέλος δεν πρέπει να δημιουργούνται αντίγραφα των κλειδιών υπογραφής.
- **Μέτριο Επίπεδο:** Εδώ τα πιστοποιητικά εξυπηρετούν την αυθεντικοποίηση και ακεραιότητα για συναλλαγές μεσαίου οικονομικού κινδύνου, που αμφισβήτηση τους χρειάζεται νομική παρέμβαση. Στο συγκεκριμένο επίπεδο, επαυξάνονται οι απαιτήσεις ασφαλείας. Για παράδειγμα το κρίσιμο διάστημα μεταξύ αίτησης και δημοσίευσης της ανάκλησης περιορίζεται στις 12 ώρες. Έτσι τα πιστοποιητικά αυτά μπορούν να χρησιμοποιηθούν σε συναλλαγές μέχρι 50000 δολλάρια. Οι κρίσιμες λειτουργίες της αρχής πιστοποίησης εκτελούνται τουλάχιστον από τρία άτομα. Ισχύουν οι ίδιες απαιτήσεις καταγραφής.
- **Υψηλό Επίπεδο:** Τα πιστοποιητικά αυτά χρησιμοποιούνται για συναλλαγές υψηλού κινδύνου, των οποίων η αμφισβήτηση μπορεί να οδηγήσει σε απώλεια ζωής ή φυλάκιση για ποσά εώς 1000000 δολλάρια. Η δημοσίευση της πληροφορίας ανάκλησης είναι άμεση. Οι λίστες ανάκλησης ανανεώνονται κάθε τέσσερις ώρες. Οι κρίσιμες λειτουργίες της αρχής πιστοποίησης εκτελούνται τουλάχιστον από τρία άτομα.

Η δομή του GOCPKI απεικονίζεται καλύτερα στο παρακάτω σχήμα:



Σχήμα 21. GOCPKI - Γενική Δομή

Ο ρόλος κάθε οντότητας που εμπλέκεται έχει ως εξής:

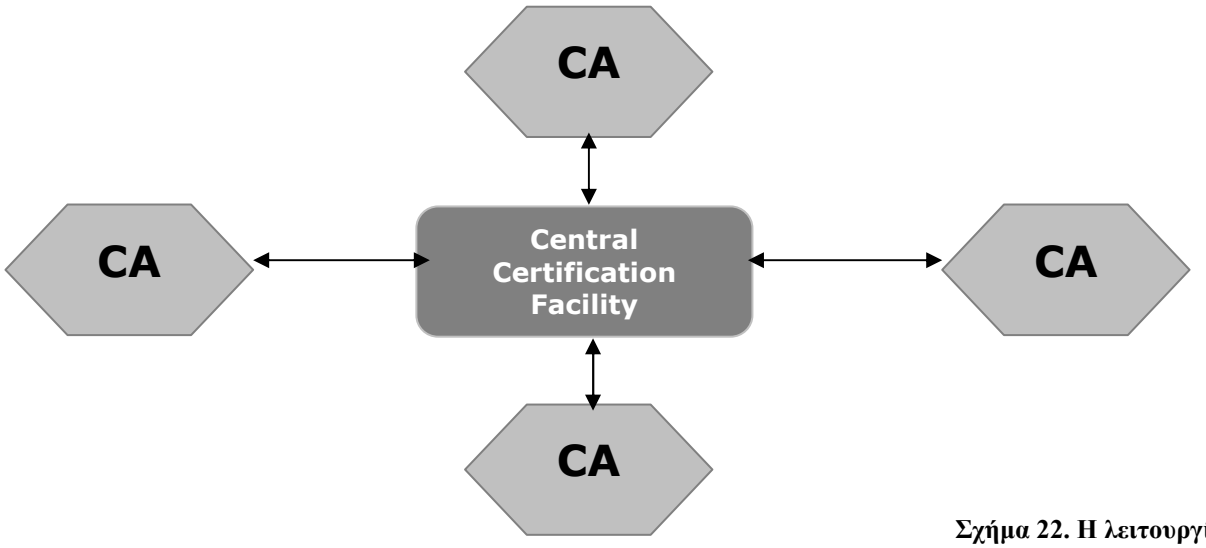
- **PMA (Policy Management Authority):** Ο ρόλος της αρχής διαχείρισης πολιτικής είναι να επιβλέπει την συνολική λειτουργία της υποδομής και να θέτει τις αρχές (σε επίπεδο πολιτικής) πάνω στις οποίες θα βασίζεται αυτή η λειτουργία. Τα μέλη της ανήκουν σε όλους τους εμπλεκόμενους φορείς και διευθύνεται από το υπουργείο οικονομικών. Ιδιαίτερη βαρύτητα έχουν οι υποδείξεις της σε ότι αφορά τις διάφορες φάσεις της διαπιστοποίησης (cross – certification) που θα περιγράψουμε παρακάτω.
- **CCF (Canadian Central Facility):** Ουσιαστικά είναι η βασική αρχή πιστοποίησης (root certification authority). Είναι υπεύθυνη για την υλοποίηση όλων των πολιτικών που θέτει η PMA και για την σύνδεση της συγκεκριμένη υποδομής με εξωτερικούς από αυτήν φορείς, όπως για παράδειγμα άλλες χώρες. Πιο συγκεκριμένα οι λειτουργίες της είναι οι εξής:
    - Να διαπιστεύει όλες τις αρχές πιστοποίησης του επόμενου επιπέδου.
    - Να διαπιστεύει εξωτερικές αρχές πιστοποίησης, οι οποίες πληρούν τις προϋποθέσεις που έχει θέσει η PMA (διαπιστοποίηση)
    - Διαχείριση των καταλόγων πιστοποιητικών και λιστών ανάκλησης.
    - Αρχειοθέτηση όλων των πιστοποιητικών και λιστών που δημιουργούνται από την ίδια αλλά και όλες τις αρχές πιστοποίησης που ανήκουν στο GOCPKI.
    - Αρχειοθέτηση αποτελεσμάτων ελέγχων αλλά και όλων των ευαίσθητων πληροφοριών που παράγουν οι κατώτερες αρχές πιστοποίησης.
- **CA (Αρχές Πιστοποίησης):** Κάθε αρχή πιστοποίησης ανήκει σε έναν κυβερνητικό τομέα. Για παράδειγμα, ο τομέας της φορολογίας θα διαθέτει τις δικές του αρχές πιστοποίησης, ενώ ο τομέας της υγείας δικές του. Παρ' όλο που στο παραπάνω σχήμα φαίνεται ένα επίπεδο από αρχές

πιστοποίησης στην πραγματικότητα και εδώ η δομή είναι ιεραρχική. Οι αρμοδιότητες μιας αρχής πιστοποίησης στο GOCPKI, είναι η έκδοση πιστοποιητικών και λιστών ανάκλησης.

- **LRA (Local Registration Authorities):** Οι συγκεκριμένες αρχές βοηθούν στην γεφύρωση του χάσματος μεταξύ των τελικών χρηστών και των αρχών πιστοποίησης. Σημειώνουμε ότι η ύπαρξη τους δεν είναι απαραίτητη, καθώς μία αρχή πιστοποίησης μπορεί να έρθει κατ' ευθείαν σε επαφή με τον τελικό χρήστη. Όπου υπάρχουν πάντως εκτελούν τις παρακάτω λειτουργίες:
  - Καταχωρούν, τροποποιούν και διαγράφουν ιδιότητες τελικών χρηστών.
  - Είναι υπεύθυνες για την διαδικασία επιβεβαίωσης της ταυτότητας.
  - Χειρίζονται αιτήσεις για την ανάκτηση ιδιωτικού κλειδιού.
  - Χειρίζονται αιτήσεις για την ανάκληση πιστοποιητικών.
  - Παραδίδουν έξυπνες κάρτες και άλλες διατάξεις δημιουργίας υπογραφής στους χρήστες. Φροντίζουν επίσης και για την παράδοση τους.

Όπως φαίνεται και από το σχήμα, ένας τελικός χρήστης μπορεί να έρθει σε επαφή είτε με μία αρχή πιστοποίησης απ' ευθείας, είτε με την τοπική αρχή καταχώρησης.

Η CCF είναι ο φορέας εκείνος που υλοποιεί στην πράξη την διαπιστοποίηση. Το τεχνικό μοντέλο με το οποίο υλοποιείται η διαπιστοποίηση είναι αυτό της γέφυρας ή καλύτερα του αστέρα, που χρησιμοποιείται και στις ΗΠΑ. Δηλαδή αντί κάθε αρχή πιστοποίησης να αναγνωρίζει κάθε άλλη, η CCF τις αναγνωρίζει όλες. Το συγκεκριμένο μοντέλο, όπως εφαρμόζεται στο GOCPKI, γίνεται καλύτερα κατανοητό από το παρακάτω σχήμα:



Σχήμα 22. Η λειτουργία της CCF

Όπως προαναφέραμε η διαδικασία της διαπιστοποίησης είναι ουσιαστικά η διαπίστευση μιας αρχής πιστοποίησης, με την έννοια του ότι μετά την ολοκλήρωση της διαδικασίας αυτή μπορεί να ενταχθεί πλήρως στο GOCPKI. Κάθε οργανισμός που διατηρεί αρχή πιστοποίησης, ακόμα και αν λειτουργεί σε χώρα εκτός Καναδά, μπορεί να συμμετάσχει στην συγκεκριμένη διαδικασία, αρκεί βέβαια οι δραστηριότητες του να σχετίζονται με κάποιον τρόπο με τις κυβερνητικές δραστηριότητες του Καναδά. Αναλυτικά η διαδικασία χωρίζεται σε 4 φάσεις και κάθε μία αποτελείται από τα εξής βήματα:

1. Φάση 1: Έναρξη

i. Υποβολή Αίτησης.

Η υποψήφια αρχή πιστοποίησης συγκεντρώνει τα απαραίτητα έγγραφα από την Γραμματεία του GOCPKI τα οποία θα υποβάλλει για την διαπιστοποίηση και τα οποία έχουν ως στόχο την δημιουργία του προφίλ της υποψήφιας αρχής από το GOCPKI σε θέματα τεχνικά, διαχείρισης ασφάλειας, αλλά και σε θέματα των ιδιοτήτων του οργανισμού. Για τον λόγο αυτό υποβάλλονται μεταξύ άλλων όλες οι πολιτικές πιστοποίησης του οργανισμού, η δήλωση των πρακτικών πιστοποίησης η πλήρης τεχνική περιγραφή των συστημάτων του αλλά και κάποια δήλωση σχετικά με την οικονομική βιωσιμότητα των συστημάτων του.

ii. Θεώρηση Αίτησης.

Η Γραμματεία του GOCPKI με βάση κριτήρια όπως για παράδειγμα τις οικονομικές συστάσεις για την αρχή πιστοποίησης, αποφασίζει αν θα προωθήσει την αίτηση στην PMA.

iii. Απόφαση για παραπομπή σε εξέταση

Μέσα σε 30 ημέρες από την υποβολή της θεώρησης της αίτησης στην PMA, πρέπει να αποφασιστεί αν θα συνεχιστεί η επεξεργασία της αίτησης και αν θα μεταβούμε στην φάση 2. Σε περίπτωση που υπάρχει η σχετική έγκριση, συγκροτείται επιτροπή εξέτασης, η οποία θα είναι αυτή που θα αναλάβει την εξέταση.

2. Φάση 2: Εξέταση

i. Εξέταση Πολιτικών Πιστοποίησης

Το πρώτο βήμα στην διαδικασία της εξέτασης είναι να γίνει σαφές ότι οι πολιτικές πιστοποίησης της αρχής συμβαδίζουν με αυτές που έχει θέσει η αρχή του Καναδά. Η διαπιστοποίηση γίνεται με βάση τις πολιτικές πιστοποίησης, που περιγράψαμε. Μπορούν να ενσωματωθούν και άλλα είδη πιστοποιητικών, όπως για παράδειγμα πιστοποιητικά ιδιότητας. Σε κάθε περίπτωση ακολουθείται μία διαδικασία αντιστοίχησης με τις 8 πολιτικές πιστοποίησης που είναι αποδεκτές κάτι που έχει ως αποτέλεσμα την υποβολή μιας αναφοράς στην PMA, η οποία συνιστά την συνέχιση (με ή χωρίς όρους) ή την διακοπή της διαδικασίας πιστοποίησης. Η τελική απόφαση και πάλι λαμβάνεται από την PMA.

ii. Διεξαγωγή Ελέγχου Συμβατότητας

Στο συγκεκριμένο βήμα, η PMA επιλέγει μία από τις ήδη υπάρχουσες αρχές πιστοποίησης και με βάση την τεχνική περιγραφή των συστημάτων της υποψήφιας αρχής πιστοποίησης διαπιστώνεται αν αυτά είναι συμβατά με τις προδιαγραφές διεπαφής που ισχύουν στο GOCPKI. Στην περίπτωση που κάτι τέτοιο ισχύει, διεξάγεται ένας έλεγχος συμβατότητας μεταξύ των συστημάτων τους και γίνεται μία δοκιμαστική διαπιστοποίηση, δηλαδή ανταλλάσσονται και επικυρώνονται τα πιστοποιητικά των οντοτήτων. Σε αντίθετη περίπτωση του συγκεκριμένου ελέγχου προηγείται μία μελέτη, η οποία καθορίζει πως θα ξεπεραστούν οι διάφορές στα συστήματα.

iii. Προδιαγραφές Συστημάτων.

Η ομάδα ελέγχου ενημερώνει την υποψήφια αρχή πιστοποίησης για τις τρέχουσες προδιαγραφές των συστημάτων του GOCPKI, ένα μέτρο που συντείνει στην εξασφάλιση της συμβατότητας των συστημάτων όταν πλέον βρίσκονται σε φάση παραγωγής.

iv. Διεξαγωγή Ελέγχου Αντιστοιχίας Συστημάτων και Πολιτικής.

Το συγκεκριμένο βήμα είναι ίσως και το πιο σημαντικό στην φάση 4, καθώς διεξάγεται έλεγχος αποτίμησης των πληροφοριακών συστημάτων της υποψήφιας αρχής σε σχέση πάντα με την πολιτική πιστοποίησης της. Ο συγκεκριμένος έλεγχος μπορεί να γίνει είτε με την παροχή τεκμηρίωσης από τον ίδιο τον υποψήφιο, είτε με την συμμετοχή ενός ανεξάρτητου ελεγκτικού φορέα. Τα αποτελέσματα υποβάλλονται στην PMA, η οποία με την σειρά της μπορεί να μεταβεί στις εγκαταστάσεις, ώστε να επιβεβαιώσει τα ευρήματα του ελέγχου.

3. Φάση 3: Διαπραγματεύσεις και απόφαση.

Ο στόχος της τρίτης φάσης είναι η κατάληξη σε συμφωνία σχετικά με τις τελικές λεπτομέρειες της συμφωνίας διαπίστευσης.

i. Διαπραγμάτευση Συμφωνίας

Στο συγκεκριμένο βήμα, στο οποίο συμμετέχει εκτός από την PMA και την υποψήφια αρχή και ένα τεχνικό συμβούλιο, καθορίζεται η μορφή που θα έχει το έντυπο της συμφωνίας δια-πιστοποίησης.

ii. Λήψη απόφασης από την PMA

Στο συγκεκριμένο βήμα λαμβάνεται η τελική απόφαση από την PMA μετά από την τελική πρόταση της επιτροπής πιστοποίησης.

iii. Έκδοση Δια-πιστοποίησης.

Γίνεται η ανταλλαγή των πιστοποιητικών της καινούριας αρχής πιστοποίησης με την CCF. Όσα πιστοποιητικά έχουν εκδοθεί από την υποψήφια γίνονται πλέον αποδεκτά και από όλους τους χρήστες του GOCPKI.

4. Φάση 4: Συντήρηση

Η συγκεκριμένη φάση έχει ως στόχο την διατήρηση της 'εμπιστοσύνης' που επιτεύχθηκε από την προηγηθείσα διαδικασία ελέγχου και τον τερματισμό της διαπιστοποίησης σε περίπτωση παραβιάσεως της συμφωνίας που υπογράφηκε νωρίτερα στην φάση της διαπραγμάτευσης.

i. **Έλεγχος Συμμόρφωσης.**

Η αρχή πιστοποίησης υποβάλλει σε τακτά χρονικά διαστήματα κάποια αναφορά στην Γραμματεία του GOCPKI. Μετά από κάθε μία τέτοια αναφορά ή όχι, μπορεί να δημιουργηθεί μία ομάδα ελέγχου από την PMA, η οποία θα ελέγξει τις εγκαταστάσεις και τους χρήστες της αρχής για τυχόν παραβιάσεις.

ii. Επίλυση Προβλημάτων.

Το συγκεκριμένο βήμα δεν είναι υποχρεωτικό. Συμβαίνει όταν παρουσιάζεται κάποιο πρόβλημα

μεταξύ των οντοτήτων που συμμετέχουν στο GOCPKI και η PMA αναλαμβάνει τη επίλυση του.

iii. Διαχείριση αλλαγής.

Το συγκεκριμένο βήμα έχει ως στόχο την προσαρμογή στην αλλαγή που συμβαίνει όταν μία καινούρια αρχή πιστοποίησης έρχεται στο GOCPKI.

iv. Ανανέωση ή τερματισμός.

Τέλος, οι ενέργειες του συγκεκριμένου βήματος συμβαίνουν κάθε φορά που λήγει η συμφωνία συνεργασίας με μία αρχή πιστοποίησης ή που διακόπτεται η λειτουργία της τελευταίας ή που λόγω των αποτελεσμάτων κάποιου ελέγχου κρίνεται ότι μία αρχή πιστοποίησης δεν μπορεί να συμμετάσχει πλέον στο GOCPKI.

4.6.2 Αυστραλία

Το πλαίσιο διαπίστευσης της Αυστραλίας αποτελεί και αυτό αναπόσπαστο κομμάτι της εθνικής στρατηγικής της χώρας για χρήση της τεχνολογίας δημοσίου κλειδιού στην κυβέρνηση για αυθεντικοποίηση των χρηστών σε ηλεκτρονικές συναλλαγές με τις δημόσιες υπηρεσίες, η οποία έχει ονομαστεί και θα αναφέρεται στο εξής ως *Gatekeeper*. Η έναρξη της συγκεκριμένης προσπάθειας ξεκίνησε στα τέλη του 1997 και το όλο πλαίσιο ολοκληρώθηκε το Μάιο του 1998, με την δημοσίευση του κειμένου της εθνικής στρατηγικής **[OGIT, 1998]**. Η όλη στρατηγική τροποποιήθηκε μερικώς τον Μάρτιο του 2001 **[NOIE, 2001]**.

Αξιοσημείωτο είναι το γεγονός ότι η συγκεκριμένη στρατηγική δεν αποτέλεσε αρχικά κάποιον νόμο. Απλώς όλες οι δημόσιες υπηρεσίες θα χρησιμοποιούν διαπιστευμένα προϊόντα και για να υπάρξει συναλλαγή τους με κάποιον τρίτο πρέπει οι ενδιαφερόμενοι φορείς να έχουν διαπιστευτεί σύμφωνα με το Gatekeeper. Παρ' όλα αυτά το 1999 ψηφίστηκε η **Electronic Transactions Act**, η οποία ήρθε σε ισχύ τον Ιούλιο του 2001 και λειτουργεί σε συνδυασμό με το πλαίσιο διαπίστευσης του Gatekeeper. Το βασικό της νόημα, το οποίο συναντάμε, και σε άλλες νομοθετικές προσπάθειες όπως αυτές των ΗΠΑ και της Ευρωπαϊκής Ένωσης είναι ότι δεν μπορεί να ακυρωθεί μία συναλλαγή μόνο και μόνο επειδή είναι ηλεκτρονική.

Σύμφωνα με την στρατηγική αυτή λοιπόν σχηματίζεται το **GPKI (Gatekeeper Public Key Infrastructure)** το οποίο είναι το σύνολο των προϊόντων, υπηρεσιών και πάροχων υπηρεσιών πιστοποίησης το οποίο έχει διαπιστευτεί για χρήση στις δημόσιες υπηρεσίες. Η διαπίστευση γίνεται με βάση πολιτικές και πρότυπα, για τα οποία υπεύθυνη είναι μία επιτροπή, η οποία αρχικά αναφερόταν ως **GPKA** (**Government Public Key Authority**) και η οποία έχει μετονομαστεί σε **GPAC** (**Gatekeeper Policy Advisory Committee**). Οι αρμοδιότητες της αφορούν την έκδοση και έγκριση διαφόρων προτύπων και την επίβλεψη της γενικότερης λειτουργίας του συστήματος. Ο φορέας της διαπίστευσης είναι ο **NOIE (National Office for Information Economy)** ο οποίος βρίσκεται σε στενή συνεργασία με την παραπάνω αρχή.

Το επόμενο επίπεδο στην ιεραρχία του Gatekeeper είναι οι **Ενδιάμεσοι Φορείς Πιστοποίησης (Intermediary Certification Authorities - ICAs)**. Ο κύριος ρόλος τους είναι να λειτουργούν ως βασικές αρχές (root authorities) για ένα σύνολο από άλλες αρχές πιστοποίησης. Επιπλέον όμως είναι και οι ίδιες αρχές πιστοποίησης και έτσι δημιουργούν και διατηρούν πιστοποιητικά και λίστες. Επίσης δημιουργούν και διατηρούν πολιτικές πιστοποίησης τις οποίες τηρούν οι υφιστάμενες αρχές πιστοποίησης (τις οποίες και πιστοποιούν). Μπορεί να είναι είτε ιδιωτικοί είτε κρατικοί φορείς, αρκεί να έχουν διαπιστευτεί.

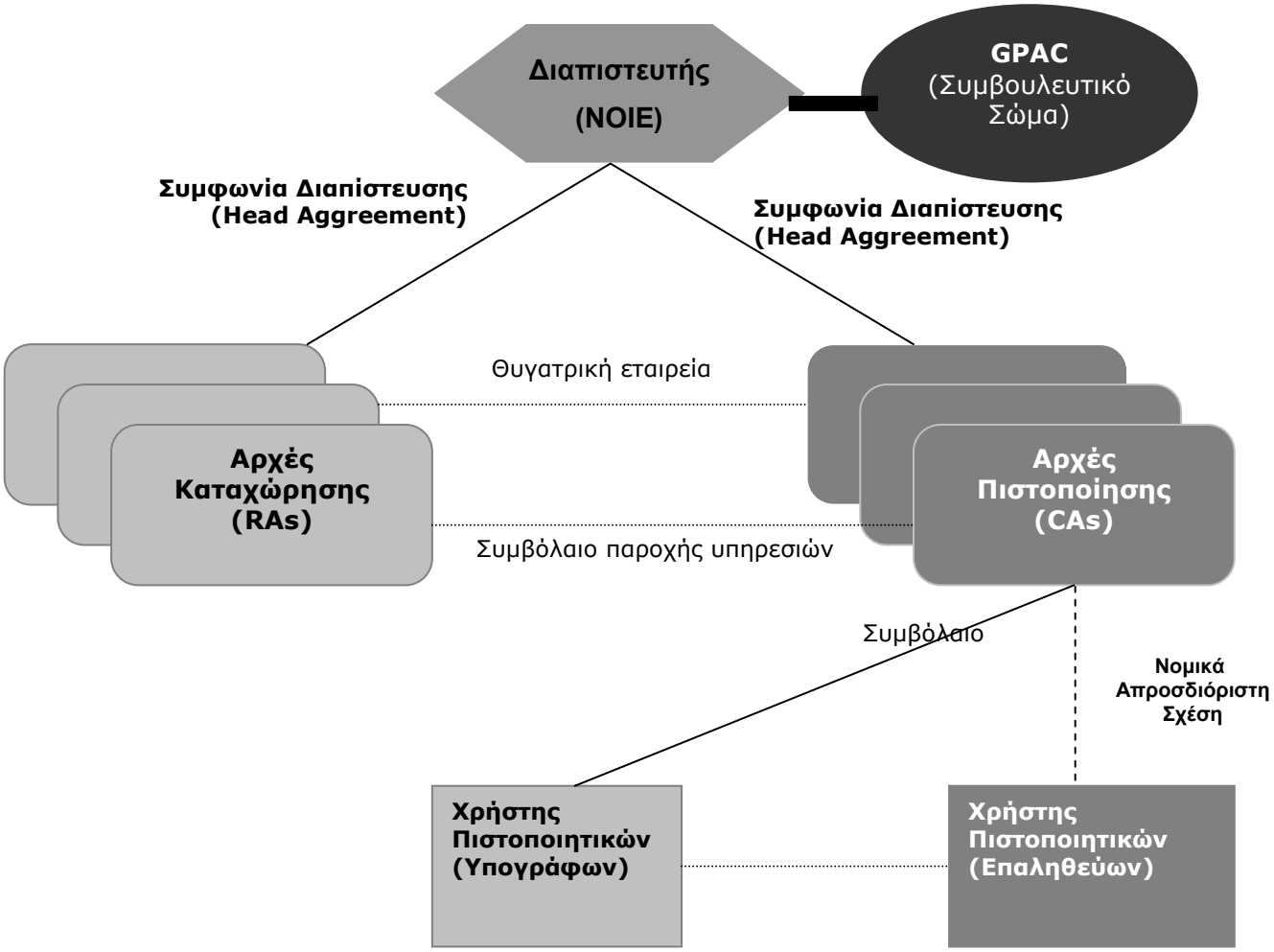
Στο αμέσως επόμενο επίπεδο βρίσκονται οι **Αρχές Πιστοποίησης Οργανισμού (Organization Certification Authorities - OCAs)**, οι οποίες έχουν όλες τις συνήθεις αρμοδιότητες μιας αρχής πιστοποίησης, συν την διενέργεια ελέγχου για το αν ο κάθε χρήστης που πιστοποιείται είναι όντως κάτοχος του ιδιωτικού του κλειδιού. Ανάλογα με την δομή του δημόσιου οργανισμού στον οποίο ανήκουν μπορούν να εκτείνονται σε πολλαπλά επίπεδα. Ένα παράδειγμα οργανισμού ο οποίος μπορεί να διαθέτει πολλά επίπεδα δικών του αρχών πιστοποίησης είναι η εφορία.

Σε άμεση σχέση με τις OCAs, βρίσκονται οι **Αρχές Καταχώρησης Οργανισμού (Organisation Registration Authorities - ORA**s), οι οποίες αναλαμβάνουν την ταυτοποίηση των χρηστών που ζητούν πιστοποίηση, την ψηφιακή υπογραφή των αιτήσεων τους και τον άμεσο χειρισμό των αιτήσεων ανάκλησης. Οι αρχές καταχώρησης δεν έχουν αρμοδιότητες παραγωγής κλειδιών. Οι υπηρεσίες καταχώρησης και πιστοποίησης μπορούν να παρέχονται τόσο από κρατικές όσο και από μη κρατικές οντότητες.

Το Gatekeeper ορίζει δύο επίπεδα διαπίστευσης, τη *βασική (entry - level accreditation)* και την πλήρη διαπίστευση *(full accreditation)*. Η βασική διαπίστευση έχει ως στόχο τον έλεγχο της υποδομής που διαθέτει μία αρχή πιστοποίησης για την υποστήριξη διάφορων προϊόντων και τεχνολογιών και όχι τον έλεγχο των ίδιων των προϊόντων. Οι αρχές πιστοποίησης επιλέγουν οι ίδιες ποιες πτυχές της λειτουργίας τους θα γίνουν αντικείμενο πιστοποίησης. Η διαδικασία του ελέγχου μπορεί να αφορά μόνο την υποβολή της απαραίτητης τεκμηρίωσης στον ελεγκτικό φορέα ή και μία επίσκεψη στις εγκαταστάσεις και ολοκληρώνεται με την έκδοση ενός πιστοποιητικού από τον ελεγκτικό φορέα το οποίο αναφέρει τι έχει πιστοποιηθεί και σε ποιο βαθμό. Το κόστος του ελέγχου επιβαρύνει την αρχή πιστοποίησης. Για την εισαγωγή στο GPKI, η αρχή πιστοποίησης υπογράφει ένα συμφωνητικό (head agreement) με το NOIE, αφού προηγουμένως έχει καταθέσει τα πιστοποιητικά ελέγχου. Το NOIE τότε εκδίδει το διαπιστευτήριο και η αρχή πιστοποίησης γίνεται δεκτή στο GPKI.

Η πλήρης διαπίστευση προϋποθέτει την επιτυχή ολοκλήρωση της βασικής διαπίστευσης καθώς επίσης και την αποτίμηση των τεχνολογιών και προϊόντων που χρησιμοποιούν οι αρχές πιστοποίησης σε EAL4 σύμφωνα με το πρότυπο Common Criteria (παλαιότερα υπήρχε απαίτηση για επίπεδο E3 σύμφωνα με το ITSEC). Η διαδικασία εδώ είναι κάπως διαφορετική καθώς η αποτίμηση δεν γίνεται πλέον από μία σχετιζόμενη οντότητα με το GPKI, αλλά από τον φορέα που πιστοποιεί κατά Common Criteria στην Αυστραλία, ο οποίος είναι ο **AISEP** (Australian Industrial Security Evaluation Program). Όταν ληφθεί ο χαρακτηρισμός EAL4 τότε υποβάλλεται στον NOIE και γίνεται η διαπίστευση.

Οι σχέσεις μεταξύ των οντοτήτων που συμμετέχουν φαίνονται καλύτερα στο παρακάτω σχήμα:



Σχήμα 23. Gatekeeper

Οι αρχές πιστοποίησης και καταχώρησης πρέπει να υπογράψουν μία συμφωνία με τον διαπιστευτή για να συμμετάσχουν στην διαδικασία της διαπίστευσης. Στην συμφωνία αυτή αναφέρονται τα δικαιώματα και οι υποχρεώσεις κάθε ομάδας. Για παράδειγμα αναφέρονται οι υποχρεώσεις των αρχών σε σχέση με τους ελέγχους διαπίστευσης (κάθε πότε πρέπει να δέχονται τους ελέγχους, τι είδους ελέγχους θα δέχονται, κάθε πότε πρέπει να ενημερώνονται, ώστε να είναι σε συμβατότητα με τα πρότυπα). Σύμφωνα πάντα με το πλαίσιο που έχει διαμορφωθεί αν υπάρξει απόκλιση από την συμφωνία τότε η αρχή πιστοποίησης χάνει την διαπίστευση (κάτι που μεταφράζεται εκτός των άλλων και σε χρηματικό πρόστιμο και ποινική δίωξη). Η νομική σχέση μεταξύ αρχής πιστοποίησης και αρχής καταχώρησης ποικίλει: Μπορεί να πρόκειται για την ίδια εταιρεία, για θυγατρική εταιρεία, ή για εντελώς ανεξάρτητες οντότητες. Αντίστοιχη είναι η κατάσταση μεταξύ των χρηστών που ζητούν υπηρεσίες πιστοποίησης από τις αρχές. Υπογράφεται κάποιο συμβόλαιο πριν βέβαια από την έκδοση του πιστοποιητικού. Το συμβόλαιο αυτό θα είναι υποσύνολο των πολιτικών πιστοποίησης και δήλωσης πρακτικών πιστοποίησης που δημοσιοποιούν οι αρχές αυτές. Στο Gatekeeper δεν αναφέρονται πρότυπα των προϊόντων υλικού και λογισμικού που χρησιμοποιούν οι τελικοί χρήστες, ούτε του μέσου που διατηρείται το ιδιωτικό κλειδί. Ειδικά για το τελευταίο μείζονος σημασίας θέμα, έχει το

Gatekeeper αποδέχεται ως ασφαλή τις δισκέτες, τις κάρτες τύπου PCMCIA καθώς επίσης και τις έξυπνες κάρτες.

Το ενδιαφέρον σημείο στο παραπάνω σχήμα είναι η σχέση μεταξύ της αρχής πιστοποίησης και του χρήστη εκείνου που βασίζεται σε μία ηλεκτρονική υπογραφή για την οποία έχει εκδώσει πιστοποιητικό η συγκεκριμένη αρχή. Η συγκεκριμένη βασίζεται στους κοινούς κανόνες δικαίου, της Αυστραλία περί αμέλειας. Δεν προδιαγράφεται δηλαδή κάτι το ιδιαίτερο σχετικά με την ρύθμιση ευθύνης.

Τα πιστοποιητικά τα οποία εκδίδονται στα πλαίσια του GPKI από τις αρχές πιστοποίησης, διακρίνονται σε δύο κατηγορίες ανάλογα με την οντότητα που ταυτοποιείται, κάθε μία από τις οποίες διαβαθμίζεται σε 3 επίπεδα με βάση τις ενέργειες που γίνονται για την επαλήθευση της ταυτότητας της οντότητας. Πιο συγκεκριμένα λοιπόν οι διαθέσιμες κατηγορίες είναι:

- **Κατηγορία 1: Ατομικά Πιστοποιητικά**

Τα συγκεκριμένα πιστοποιητικά εκδίδονται σε φυσικά πρόσωπα και πιστοποιούν την φυσική τους ταυτότητα. Σκοπός τους είναι να χρησιμοποιηθούν σε περιστάσεις όπως η ηλεκτρονική υποβολή απλών αιτήσεων, η συμμετοχή σε διαγωνισμούς προσλήψεων, η ηλεκτρονική υποβολή φορολογικών δηλώσεων και άλλες παρόμοιες, ανάλογα βέβαια με το επίπεδο επιτρεπτής χρήσης του πιστοποιητικού. Τα τρία επίπεδα χρήσης πιστοποιητικών αντιστοιχούν στο σύνολο των βαθμών που έχουν συγκεντρωθεί από μία διαδικασία ταυτοποίησης. Η διαδικασία αυτή της ταυτοποίησης ξεκινά από μία αίτηση του ενδιαφερόμενου (η οποία μπορεί να γίνει και ηλεκτρονικά) και ολοκληρώνεται με την παράδοση των απαιτούμενων εγγράφων στην αρχή καταχώρησης (RA) είτε στην αρχή πιστοποίησης η οποία όμως πρέπει να γίνει *αυτοπροσώπως*. Τα έγγραφα αυτά είναι είτε αποδεικτικά ταυτότητας είτε αποδεικτικά οικονομικής φύσεως είτε αποδεικτικά ταυτότητας (διαβατήρια κτλ.) Ανάλογα λοιπόν με τα στοιχεία που έχει παρουσιάσει συγκεντρώνει ένα σύνολο από πόντους, το οποίο δείχνει την εμπιστοσύνη που μπορεί να έχει κάποιος στο πιστοποιητικό. Όπως προαναφέραμε διακρίνονται 3 επίπεδα:

o **Επίπεδο 1**: Μη ευαίσθητη πληροφορία χωρίς οικονομικές επιπτώσεις.

o **Επίπεδο 2**: Οι συμμετέχουσες στην συναλλαγή οντότητες μπορούν να καθορίσουν το είδος των πληροφοριών που δέχονται να ανταλλάξουν, καθώς επίσης και την μέγιστη επιτρεπόμενη σημασία. Πριν τις αλλαγές του 2001, προορίζονταν για συναλλαγές μέχρι 1000 δολάρια ή / και ανταλλαγή εμπιστευτικής πληροφορίας.

o **Επίπεδο 3**: Το ίδιο με το επίπεδο 2. Πριν τις αλλαγές του 2001, προορίζονταν για συναλλαγές μέχρι 10000 δολάρια ή / και ανταλλαγή προστατευμένης πληροφορίας.

- **Κατηγορία 2: Μη Ατομικά Πιστοποιητικά**.

Τα πιστοποιητικά αυτά πιστοποιούν οργανωτικούς ρόλους οντοτήτων (ατόμων) σε κάποιον οργανισμό ή αφορούν οργανισμούς. Τα συγκεκριμένα πιστοποιητικά αφορούν κυρίως μεγάλες και συχνές συναλλαγές οι οποίες θα γίνονται μεταξύ δύο οργανισμών (B2B συναλλαγές) και οι οποίες θα υπογράφονται με μία αυτοματοποιημένη διαδικασία από υπολογιστές. Εδώ είναι φανερό ότι ο ρόλος του

υπογράφονται στον οργανισμό είναι μεγαλύτερης σημασίας από την φυσική του ταυτότητα. Αντίστοιχη είναι η διαδικασία πιστοποίησης, σε ότι αφορά τα αποδεικτικά στοιχεία. Προφανώς εδώ απαιτούνται και πιστοποιητικά για την σύσταση του οργανισμού και ανάλογα αποδεικτικά στοιχεία.

Οι αρχές πιστοποίησης που έχουν λάβει βασική διαπίστευση, μπορούν να εκδίδουν πιστοποιητικά μόνο για το επίπεδο 1, κάθε μίας από τις παραπάνω κατηγορίες.

Σε κάθε συναλλαγή, οι δημόσιοι φορείς μπορούν να καθορίσουν τι επίπεδο πιστοποίησης απαιτείται τόσο για τους υπαλλήλους τους (οι οποίοι θα χειριστούν την συναλλαγή) είτε σε ατομικό, είτε σε μη ατομικό πιστοποιητικό, όσο και για τους υπαλλήλους της συναλλασσόμενης οντότητας.

Το Gatekeeper καθορίζει επίσης και πρότυπα τα οποία μπορούν να χρησιμοποιηθούν τόσο για σκοπούς συμβατότητας, όσο και για την διαπίστευση. Τα πρότυπα αυτά είτε προέρχονται από διεθνείς οργανισμούς, είτε από οργανισμούς προτυποποίησης της Αυστραλίας. Όπως είναι φυσικό, τα τεχνικά πρότυπα είναι αυτά που ισχύουν και διεθνώς (X.509, LDAP κτλ) ενώ για πρότυπα όπως αυτά της διαχείρισης κινδύνων που δεν ισχύουν διεθνώς έχουν χρησιμοποιηθεί τα αντίστοιχα από τους οργανισμούς της Αυστραλίας.

4.7 Συμπεράσματα

Στην ενότητα αυτή παρουσιάσαμε τα νομικά και όχι μόνο πλαίσια που έχουν εφαρμοστεί σε διεθνές επίπεδο για τις ηλεκτρονικές υπογραφές και την διαπίστευση. Είδαμε ότι αλλού εξετάζονται οι ηλεκτρονικές υπογραφές ανεξάρτητα από τεχνολογία και μορφή, ενώ σε άλλες περιπτώσεις θεσμοθετούνται οι ιδιότητες και η τεχνολογία των ψηφιακών υπογραφών. Ιδιαίτερη έμφαση δόθηκε στην ευρωπαϊκή προσέγγιση. Αυτό δεν έγινε μόνο και μόνο επειδή επηρεάζει άμεσα τις εξελίξεις στην Ελλάδα, αλλά λόγω ενός πολύ σημαντικού χαρακτηριστικού της: αποτελεί ένα ενδιάμεσο βήμα προς την εφαρμογή νομικών πλαισίων σε παγκόσμια κλίμακα. Διαφέρει έτσι από τις υπάρχουσες διεθνείς ρυθμιστικές προσπάθειες, καθώς δεν είναι απλώς ένας πρότυπος νόμος τον οποίο μπορεί να μην εφαρμόσει κανείς, αλλά έχει ήδη βρει πρακτική εφαρμογή στις εθνικές νομοθεσίες των χωρών μελών. Εκτός από την Ευρώπη ασχοληθήκαμε και με την κατάσταση στις ΗΠΑ, τον Καναδά και την Αυστραλία. Συγκρίνοντας τώρα, συνολικά τα διάφορα πλαίσια που διαμορφώνονται διακρίνουμε μία πολύ σημαντική διαφοροποίηση. Η διαπίστευση στην Ευρώπη, έχει ως στόχο την παροχή ενός βελτιωμένου επιπέδου υπηρεσιών, άσχετα με την χρήση των πιστοποιητικών. Αντίθετα στις υπόλοιπες περιπτώσεις που εξετάσαμε χρησιμοποιείται κυρίως για την παροχή υπηρεσιών πιστοποίησης στις συναλλαγές που γίνονται με την κυβέρνηση. Ακόμα υπάρχει μία γενικότερη διαφορά φιλοσοφίας σχετικά με τα πρότυπα. Είδαμε ότι στην Ευρώπη την οδηγία ακολούθησε μία εκτεταμένη πρωτοβουλία προτυποποίησης, η οποία ναι μεν χρησιμοποίησε υπάρχοντα πρότυπα, προσαρμόζοντας τα στις απαιτήσεις της οδηγίας. Στις υπόλοιπες περιπτώσεις χρησιμοποιήθηκαν έτοιμα πρότυπα. Χαρακτηριστικό παράδειγμα αποτελεί ο Καναδάς και οι πολιτικές πιστοποίησης για το GOCPKI που ακολουθούν ευλαβικά το **[RFC 2527, 1999].** Επίσης μία πολύ σημαντική διαφορά την οποία

παρατηρήσαμε στο συγκεκριμένο κεφάλαιο, αφορά την αντιμετώπιση που έχουν οι πάροχοι υπηρεσιών πιστοποίησης από την νομοθεσία. Στην Ευρώπη βλέπουμε ότι υπάρχει προσπάθεια ρύθμισης τους συγκεκριμένου τομέα της αγοράς και παροχή ελάχιστης ευθύνης σε αυτούς ανεξάρτητα από το αν οι υπηρεσίες αφορούν τον δημόσιο τομέα. Αντίθετα στις υπόλοιπες χώρες που εξετάσαμε, η λειτουργία των αρχών πιστοποίησης δεν απασχολεί καθόλου εκ των προτέρων τουλάχιστον τους νομοθέτες, παρά μόνο όταν πρόκειται για την συνεργασία σε τεχνικό επίπεδο με δημόσιους φορείς. Αυτές και άλλες διαφορές θα αναπτυχθούν εκτενέστερα στο επόμενο κεφάλαιο.

5 (Συγ)κριτική Ανάλυση.

5.1 Εισαγωγή

Στην ενότητα αυτή θα γίνει αναλυτικός σχολιασμός και κριτική των όσων προαναφέραμε σε όλη την έκταση της εργασίας. Έχοντας αναπτύξει στις προηγούμενες παραγράφους ένα υπόβαθρο για όλες τις διαδικασίες οι οποίες σχετίζονται με ηλεκτρονικές υπογραφές, μπορούμε να αναφερθούμε τώρα συνολικά σε αυτές. Στόχος της παρακάτω ανάλυσης, είναι η παρουσίαση ορισμένων σκέψεων και συμπερασμάτων, τα οποία έχουν ως στόχο την εξαγωγή κάποιων επιθυμητών ιδιοτήτων, τόσο για το περιβάλλον εφαρμογής ηλεκτρονικών υπογραφών όσο και για το πλαίσιο διαπίστευσης το οποίο προκύπτει από τα διάφορα κείμενα τα οποία εξετάσαμε νωρίτερα. Οι ιδιότητες αυτές μπορούν να χρησιμεύσουν ως απαντήσεις στα διάφορα κρίσιμα σημεία που εμφανίστηκαν. Είναι γεγονός ότι στο συγκεκριμένο θέμα οι λύσεις που έχουν πρακτική εφαρμογή, δεν μπορούν να προκύψουν ως αποτέλεσμα μιας τέτοιας θεωρητικής ανάλυσης. Οι τελικές λύσεις οι οποίες θα δοθούν, θα είναι το αποτέλεσμα εκτεταμένης εμπειρίας πάνω σε πραγματική εφαρμογή σε συστήματα ηλεκτρονικών υπογραφών και λειτουργίας παρόχων υπηρεσιών πιστοποίησης, απο την μια και διαπραγμάτευσης των αντικρουόμενων συμφερόντων από την άλλη.

5.2 Νομική Προσέγγιση προς την τεχνολογία ηλεκτρονικών υπογραφών.

Το πρώτο θέμα που θα εξετάσουμε, αφορά την αντιμετώπιση των ηλεκτρονικών υπογραφών από τα διάφορα νομικά συστήματα. Παρά το γεγονός ότι ειδικά στον συγκεκριμένο τομέα, η ύπαρξη ενός παγκοσμίου πλαισίου θα είχε σημαντικά πλεονεκτήματα τα οποία θα οδηγούσαν στην ευρύτατη αποδοχή των ηλεκτρονικών υπογραφών, παρατηρείται μία πληθώρα ετερογενών και διαφορετικών προσεγγίσεων που οδηγούν σε ένα ‘χάος’ και κάθε άλλο παρά προωθούν τις ηλεκτρονικές υπογραφές. Εμείς εδώ θα προσπαθήσουμε να εξηγήσουμε τα αίτια αυτού του χάους, να κάνουμε κάποια κριτική στην τεχνολογική προσέγγιση που ακολουθείται στα διάφορα νομικά πλαίσια και να προτείνουμε κάποιες αρχές, πάνω στις οποίες θα μπορούσαν να βασιστούν αυτά.

Σε γενικές γραμμές, όπως φάνηκε και από το προηγούμενο κεφάλαιο, υπάρχουν 2 μεγάλες κατηγορίες θεώρησης για τις ‘υπογραφές’ ή γενικότερα για την αναγνώριση ηλεκτρονικών μεθόδων αυθεντικοποίησης. Η μία θέλει την θεσμοθέτηση υπέρ μίας συγκεκριμένης τεχνολογίας, δηλαδή των ψηφιακών υπογραφών, ενώ η δεύτερη, η τεχνολογικά ουδέτερη, θεωρεί την ηλεκτρονική υπογραφή γενικά, ως οποιοδήποτε ηλεκτρονικό σύμβολο το οποίο μπορεί να προσαρτηθεί και να συσχετισθεί με οποιοδήποτε ηλεκτρονικό κείμενο.

Πιο συγκεκριμένα στο **[Aalberts, 1999]** αναφέρονται τρεις προσεγγίσεις στον συγκεκριμένο τομέα:

- Η πρώτη αναφέρεται ρητά στην τεχνολογία των ψηφιακών υπογραφών. Με τον τρόπο αυτό δίδεται στην ψηφιακή υπογραφή ίδια ισχύς με την ιδιόχειρη υπογραφή. Κλασικά παραδείγματα της

συγκεκριμένης κατηγορίας είναι η γερμανική προσέγγιση, η προσέγγιση της Utah και η ιταλική προσέγγιση.

- Η δεύτερη προσέγγιση αναφέρεται ως υβριδική προσέγγιση. Εδώ τίθενται ορισμένες ελάχιστες απαιτήσεις στις γενικές μεθόδους ηλεκτρονικής αυθεντικοποίησης οι οποίες θα έχουν και περιορισμένη νομική ισχύ, ενώ συγκεκριμένες τεχνολογίες όπως για παράδειγμα η ψηφιακή υπογραφή απολαμβάνουν ιδιαίτερη νομική μεταχείριση που μεταφράζεται και ως εξίσωση με τις ιδιόχειρες υπογραφές. Το σημαντικότερο παράδειγμα εδώ είναι η οδηγία της Ευρωπαϊκής Επιτροπής.
- Η τρίτη προσέγγιση αναφέρεται και ως λειτουργική (functionalist) ή μινιμαλιστική (minimalist). Είναι το τυπικό παράδειγμα τεχνολογικής ουδετερότητας, καθώς δεν υπάρχει καθόλου αναφορά σε συγκεκριμένη τεχνολογία. Αντίθετα, αναλύονται από μηδενική βάση, όλες οι απαιτήσεις ασφαλείας που πρέπει να έχει μία ηλεκτρονική υπογραφή για να επιτελεί τον λειτουργικό της σκοπό. Όποια τεχνολογία ικανοποιεί αυτές τις λειτουργικές απαιτήσεις, γίνεται αποδεκτή. Η συγκεκριμένη προσέγγιση έχει χαρακτηριστεί και ως '*hands- off*' **[JUEN, 1998].** Με πιο απλά λόγια οι συγκεκριμένες προσεγγίσεις δεν προδιαγράφουν πώς σε γενικό επίπεδο, η χρήση κάποιας τεχνικής ασφαλείας θα μπορούσε να επηρεάσει την αποδεικτική διαδικασία μιας συναλλαγής. Με άλλα λόγια, αφήνουν στον τελικό δικαστή την απόφαση για το ποια στοιχεία θα ληφθούν υπόψη. Τα στοιχεία αυτά μπορούν επιπλέον να έχουν διαμορφωθεί από μία συγκεκριμένη αγορά ή από ένα σύνολο πρακτικών που έχουν σχέση με κάποιον ιδιαίτερο κλάδο και κατά συνέπεια με τα ιδιαίτερα χαρακτηριστικά και απαιτήσεις ασφαλείας του. Παραδείγματα στον συγκεκριμένο τομέα αποτελούν ο πρότυπος νόμος για το ηλεκτρονικό εμπόριο του ΟΗΕ (**[UNCITRAL, 1996], άρθρο 7)**.

Όλες οι προσεγγίσεις έχουν τα μειονεκτήματα και τα πλεονεκτήματα τους. Για την τεχνολογικά-εξειδικευμένη προσέγγιση, πρώτα από όλα δημιουργεί ένα σταθερό νομικό πλαίσιο, μέσα στο οποίο μπορούν να προδιαγραφούν ρόλοι για όλες τις εμπλεκόμενες οντότητες και να ρυθμιστεί η ευθύνη τους προς το ευρύ κοινό. Επίσης εφ'όσον είναι γνωστή η χρησιμοποιούμενη τεχνολογία μπορούν νομικά να καλυφθούν οι όποιες αδυναμίες της. Από την άλλη πλευρά όμως η συγκεκριμένη προσέγγιση δεν συμβαδίζει με τις τεχνολογικές εξελίξεις. Αυτό έχει ως συνέπεια είτε την απαξίωση της και την ανάγκη για αναθεώρηση της, είτε το 'πάγωμα' της τεχνολογικής εξέλιξης στον συγκεκριμένο τομέα. Το τελευταίο δεν είναι υπερβολικό, καθώς δεν θα υπάρχει αγορά για τους 'εναλλακτικούς' πάροχους πιστοποίησης.

Η τεχνολογικά ουδέτερη προσέγγιση, έχει συμπληρωματικά χαρακτηριστικά από αυτά που αναφέραμε στην προηγούμενη παράγραφο, καθώς δεν εγκλωβίζεται σε μία συγκεκριμένη τεχνολογία. Έτσι έχει την δυνατότητα εξίσωσης εναλλακτικών τεχνολογιών. Επιπλέον η συγκεκριμένη προσέγγιση έχει μεγαλύτερη διάρκεια ζωής. Αντίθετα, επιτρέπει και σε μη αποδεδειγμένες τεχνολογίες να εφαρμοστούν στην πράξη, κάτι που έχει ως συνέπεια να διακινδυνεύεται η ασφάλεια των ηλεκτρονικών συναλλαγών. Ο ορισμός της ηλεκτρονικής υπογραφής ως οποιοδήποτε ηλεκτρονικό σύμβολο ή κομμάτι δεδομένων μπορεί

να συσχετιστεί με οποιοδήποτε ηλεκτρονικό κείμενο, μπορεί να οδηγήσει σε αποδοχή ως ηλεκτρονικών υπογραφών ενέργειες του τύπου '*Πατήστε ENTER εδώ για να αποδεχθείτε την συγκεκριμένη νομικά δεσμευτική συμφωνία*' **[Gutman, 2001]** κάτι που δεν εξασφαλίζει και τόσο μια συναλλαγή.

Το πρόβλημα, κατά την γνώμη μας η 'βιασύνη' και η 'άγνοια' στην θεσμοθέτηση. Η παρουσίαση του κεφαλαίου 2, μας οδήγησε στο συμπέρασμα ότι ο όρος ψηφιακή υπογραφή είναι ίσως μία ιστορική σύμπτωση, η οποία σε συνδυασμό με την έκρηξη του Παγκοσμίου Ιστού στα μέσα της προηγούμενη δεκαετίας και τις ανάγκες που αυτή δημιούργησε οδήγησε στα πλαίσια ηλεκτρονικών υπογραφών τα οποία συναντούμε σήμερα. Πράγματι, θεωρούμε ότι οι Diffie και Hellman, όταν το 1976 πρότειναν τα ασύμμετρα συστήματα και ονόμασαν την λειτουργία αυθεντικοποίησης τους ως ψηφιακή υπογραφή, δεν θα μπορούσαν να είχαν υπ'όψιν τους τη σημασία της υπογραφής σε ένα νομικό πλαίσιο. Ο συγκεκριμένος όρος λειτούργησε όμως παραπλανητικά τα επόμενα χρόνια, κατά την γνώμη μας, με αποτέλεσμα να υπάρχει γενικότερα η εντύπωση ότι έχει βρεθεί το ανάλογο προς την ιδιόχειρη υπογραφή. Η παραπάνω παρεξήγηση καθώς και η βιασύνη θεσμοθέτησης υπέρ των ψηφιακών υπογραφών υπό την πίεση της αγοράς είναι κατά την γνώμη μας μία αιτία για το συγκεκριμένο χάος. Δεν είναι ανάγκη οποιαδήποτε μέθοδος ηλεκτρονικής υπογραφής, να είναι ισοδύναμη με την αντίστοιχη ιδιόχειρη. Τα δύο μέσα έχουν διαφορετικά χαρακτηριστικά, αντιμετωπίζουν διαφορετικούς κινδύνους και λειτουργούν σε διαφορετικά επίπεδα αφαίρεσης για τον τελικό χρήστη. Η μία φέρει τον υπογράφοντα αντιμέτωπο με ένα κομμάτι χαρτί και ένα στυλό, ενώ η άλλη με έναν πολύπλοκο μηχανισμό, στο οποίο εμπλέκονται ανώτερα μαθηματικά και τεχνολογία υπολογιστών, με αποτέλεσμα ο τελικός χρήστης να νιώθει ότι έχει χάσει τον έλεγχο. Ίσως μία καλή λύση θα ήταν η παράλληλη νομοθέτηση για τις ηλεκτρονικές και συμβατικές συναλλαγές, χωρίς να υπάρχει εξίσωση τους, αγνοώντας έτσι την ουσιαστική ισοδυναμία τους. Αν και η προσέγγιση αυτή πιθανότατα να δημιουργούσε προβλήματα εφαρμογής, θα ήταν χρήσιμη ως ένα μεταβατικό στάδιο. Κάτι παρόμοιο, υλοποιήθηκε στην Γερμανία, όπου στόχος της προτυποποίησης του BSI ήταν η δημιουργία του τεχνικού πλαισίου, στο οποίο θα υπάρξει εκτεταμένη εφαρμογή και εμπειρία, προτού εξισωθούν με τις ιδιόχειρες.

5.3 Η φύση της διαπίστευσης

Σε πιο πρακτικό επίπεδο τώρα, το επόμενο θέμα με το οποίο θα ασχοληθούμε προκύπτει από την κύρια διαφορά μεταξύ των διαφόρων προσεγγίσεων που περιγράψαμε στο προηγούμενο κεφάλαιο. Η διαφορά αυτή έγκειται στην φύση και τον ρόλο της διαπίστευσης. Πιο συγκεκριμένα, παρατηρήσαμε δύο προσεγγίσεις: η πρώτη (η ευρωπαϊκή) θέλει την χρήση της διαπίστευσης ως ένα μέσο ρύθμισης του τομέα των ηλεκτρονικών υπογραφών με απώτερο σκοπό την παροχή ενός βελτιωμένου επιπέδου υπηρεσιών πιστοποίησης **[EDCF, 1999].** Η δεύτερη, χρησιμοποιεί την διαπίστευση ως ένα μέσο για δύο σκοπούς:

I) Για την παροχή υπηρεσιών πιστοποίησης ή για την χρήση τους στον δημόσιο τομέα, όπου υπάρχουν αυξημένες απαιτήσεις ασφάλειας.

II) Για την επίδειξη στην πράξη και την διασφάλιση του, ότι υπάρχει τεχνική συμβατότητα μεταξύ των διαφόρων υποδομών υπηρεσιών πιστοποίησης. Αξίζει να διευκρινίσουμε και πάλι, ότι στην περίπτωση μας, η τεχνική συμβατότητα δεν αφορά μόνο την συνεργασία συστημάτων διαφορετικών πρωτοκόλλων. Μέσω της έννοιας της πολιτικής πιστοποίησης, η οποία όπως είδαμε ενσωματώνεται σε κάθε πιστοποιητικό και φέρνει έτσι σε τεχνικό επίπεδο τις πρακτικές και τις διαδικασίες που ακολουθεί ο κάθε πάροχος.

Η παραπάνω διαφορά, αν λάβουμε υπόψη μας ότι:

1. η υποχρεωτική διαπίστευση θα είναι μάλλον σε κάθε περίπτωση, ακόμα και στις πιο 'φιλελεύθερες' προσεγγίσεις (βλ. ΗΠΑ) υποχρεωτική για την περίπτωση παροχής υπηρεσιών πιστοποίησης στον δημόσιο τομέα, λόγω των αυξημένων απαιτήσεων ασφάλειας και ότι
2. η διαπίστευση είναι 'άχρηστη' στην περίπτωση ενός κλειστού περιβάλλοντος ηλεκτρονικών συναλλαγών, που τα πάντα ρυθμίζονται με κάποια σύμβαση

ισοδυναμεί με το εξής ερώτημα: Πρέπει το κάθε κράτος να επεμβαίνει στην παροχή υπηρεσιών πιστοποίησης στο ευρύ κοινό, με σκοπό πιθανότατα να διασφαλίσει καλύτερες υπηρεσίες; Το ίδιο ερώτημα βέβαια αφορά και την εποπτεία των υπηρεσιών πιστοποίησης.

Η απάντηση, πρέπει να λάβει υπ'όψιν τις εξής παραμέτρους:

- την νομική αναγνώριση κάποιου είδους ηλεκτρονικών υπογραφών. Το κοινό στοιχείο όλων των τεχνολογικά ουδέτερων νομικών προσπαθειών είναι ότι δεν στερείται νομικής ισχύος μία υπογραφή μόνο και μόνο επειδή είναι ηλεκτρονική. Έτσι είναι αποδεκτή η χρήση της σε νομικές διαδικασίες, χωρίς κατ' ανάγκη να είναι ισοδύναμη μιας ιδιόχειρης υπογραφής, κάτι που στην Ευρώπη για παράδειγμα έχει επιπλέον απαιτήσεις (αναγνωρισμένο πιστοποιητικό, προηγμένη ηλεκτρονική υπογραφή, ασφαλής διάταξη δημιουργίας).
- το κόστος παροχής υπηρεσιών πιστοποίησης. Είναι φανερό ότι η διαπίστευση θα αυξήσει το καθημερινό κόστος λειτουργίας μιας αρχής πιστοποίησης. Η αύξηση αυτή θα μεταφερθεί στην αύξηση της τιμής των ηλεκτρονικών πιστοποιητικών, κάτι που θα δυσκολέψει και σίγουρα θα επιβραδύνει την ανάπτυξη τους.

Παρ' όλο λοιπόν που μία ηλεκτρονική υπογραφή δεν είναι ισοδύναμη, νομικά τουλάχιστον με μία ιδιόχειρη, δεν σημαίνει ότι δεν πρέπει να διαθέτει κάποια ασφάλεια, καθώς από αυτήν θα κριθεί η αξιοπιστία της σε νομικές διαδικασίες. Αν εξαιρέσουμε τις στοιχειώδεις περιπτώσεις ηλεκτρονικών υπογραφών (όπως για παράδειγμα τις ψηφιοποιημένες υπογραφές), για τις οποίες άλλωστε δεν χρειάζονται υπηρεσίες πιστοποίησης, όλα τα υπόλοιπα είδη ηλεκτρονικών υπογραφών θα μπορούσαν να χρησιμοποιήσουν την διαπίστευση ως εγγύηση ασφάλειας. Ας μην ξεχνάμε άλλωστε πως στην οδηγία μία αναγνωρισμένη ηλεκτρονική υπογραφή δεν είναι κατ' ανάγκη και διαπιστευμένη (και αντίστροφα) (σχήμα 16).

Εφόσον λοιπόν η διαπίστευση δρα ευεργετικά στην όλη ασφάλεια των ηλεκτρονικών υπογραφών

μία λύση που θα μπορούσε να την εξασφαλίσει και εκεί όπου δεν επιβάλλεται ρητά, είναι μέσω της αυτορύθμισης. Βέβαια θα πρέπει να υπάρξει κάποια ώθηση, έτσι ώστε οι διάφορες αρχές πιστοποίησης να αποφασίσουν να συμμετάσχουν σε ένα τέτοιο πλαίσιο. Αυτά κατά την γνώμη μας θα τα δώσει η ίδια η αγορά, καθώς είναι λογικό ότι η σφραγίδα του διαπιστευμένου μπορεί να λειτουργήσει ώς ένα μέσο προσέλκυσης πελατών αν υπάρχει, αλλιώς μπορεί να λειτουργήσει μειονεκτικά. Απομένει βέβαια να δούμε αν αυτό θα ισχύσει και στην πράξη.

5.4 Ρύθμιση Ευθύνης

Όπως, ίσως, έχει διαφανεί από την προηγούμενη μελέτη ένα από τα πιο σημαντικά θέματα που προκύπτουν από τις νομοθετικές και ρυθμιστικές προσπάθειες που αφορούν τις ηλεκτρονικές υπογραφές είναι το θέμα της ευθύνης για τα επισφαλή πιστοποιητικά. Πρέπει να καθοριστεί δηλαδή ποια οντότητα φέρει ευθύνη και σε ποιον βαθμό για τις (οικονομικές και όχι μόνο) ζημίες που θα προκληθούν, αν κάτι πάει στραβά σε κάποια από τις δυνατές αλληλεπιδράσεις ή ένα πιστοποιητικό αποδειχθεί εσφαλμένο και μία τρίτη οντότητα έχει βασιστεί σε αυτό. Το ζήτημα αυτό είναι πάρα πολύ σημαντικό, καθώς αν θεωρηθεί ότι οι πάροχοι πιστοποίησης φέρουν το μεγαλύτερο ποσοστό της ευθύνης για ζημιές, διατρέχουν σημαντικό οικονομικό ρίσκο, κάτι που θα αποτρέψει αρκετούς από δραστηριοποίηση και είσοδο στην αγορά. Επίσης θα σταθεί αιτία για υπερκοστολόγηση των παρεχόμενων υπηρεσιών. Από την άλλη, αν οι τελικοί χρήστες δουν ότι διατρέχουν κινδύνους από την χρήση ηλεκτρονικών υπογραφών δεν θα προχωρήσουν στην υιοθέτηση της τεχνολογίας αυτής. Γίνεται φανερό λοιπόν ότι η αποτελεσματική και δίκαιη επίλυση του θέματος αυτού, είναι ένας κρίσιμος παράγοντας στην εξέλιξη και αποδοχής της υποδομής ηλεκτρονικών υπογραφών.

Προχωρώντας σε μία ανάλυση του θέματος, διαπιστώνουμε ότι οι πιθανοί φορείς της ευθύνης είναι οι τρεις βασικές οντότητες του κυκλώματος:

- Πάροχος Πιστοποίησης.
- Υπογράφων.
- Επαληθεύων.

Πιθανώς κάποιος θα έφερε αντιρρήσεις στις παραπάνω ‘υποψηφιότητες’. Τι ευθύνη μπορεί να φέρει ο υπογράφων, η οντότητα δηλαδή στην οποία εκδίδεται το πιστοποιητικό; Ακόμα περισσότερο, τι ευθύνη μπορεί να φέρει ο επαληθεύων, ο οποίος απλώς έλαβε ένα μήνυμα αναζήτησε το πιστοποιητικό και με αυτό επαλήθευσε την υπογραφή του μηνύματος

Ο υπογράφων δεν μπορεί να φέρει ευθύνη για τα περιεχόμενα του πιστοποιητικού, εκτός βέβαια αν παρέχει ψευδή στοιχεία κατά την εγγραφή του. Το συγκεκριμένο είδος ευθύνης όμως μεταφέρεται στον πάροχο υπηρεσιών πιστοποίησης, ο οποίος δεν διέθετε τις διαδικασίες εκείνες που θα απέτρεπαν κάτι τέτοιο. Μπορεί να φέρει ευθύνη όμως σε περίπτωση που υπάρξει κάποια απώλεια του ιδιωτικού του κλειδιού, υπάρξει πλαστογράφηση και δεν πιαστεί ο πλαστογράφος. Τα ίδια ισχύουν και για την οντότητα

που επαληθεύει την ηλεκτρονική υπογραφή. Δεν φέρει ευθύνη για τα περιεχόμενα του πιστοποιητικού, φέρει ευθύνη για ορισμένες διαδικασίες που σχετίζονται με την επαλήθευση, όπως για παράδειγμα την τήρηση των ορίων που αναγράφονται ή τον σωστό έλεγχο των πληροφοριών ανάκλησης.

Έτσι είναι φανερό, ότι ο κύριος υπεύθυνος για τα περιεχόμενα ενός πιστοποιητικού είναι ο πάροχος πιστοποίησης. Όπως είδαμε και στο δεύτερο κεφάλαιο, σε βασικό επίπεδο, ο ρόλος του είναι ακριβώς αυτός: να εγγυηθεί δηλαδή για την ταυτότητα ή για κάποιες ιδιότητες του υπογράφοντα; Αυτός είναι και ο ρόλος του πιστοποιητικού. Δεν είναι δυνατόν λοιπόν στην δήλωση πρακτικών πιστοποίησης της Verisign, να αποποιείται της ευθύνης για τα περιεχόμενα του πιστοποιητικού **[Verisign, 1997].**[4] Κατά συνέπεια φαίνεται δίκαιο, να φέρει αυτός την ευθύνη για όποια στοιχεία του πιστοποιητικού, προκάλεσαν ζημιές λόγω λαθών. Η διαπίστωση αυτή αν και σωστή, μπορεί να χαρακτηρισθεί ως απλοϊκή και μη εφαρμόσιμη με βάση την δεδομένη κατάσταση.

Όπως προαναφέραμε, ηλεκτρονικά πιστοποιητικά υπάρχουν εδώ και 6 – 7 χρόνια. Αρχικά λοιπόν και λόγω της πλήρους απουσίας νομικών / ρυθμιστικών καθεστώτων οι αρχές πιστοποίησης προσπάθησαν να μειώσουν την ευθύνη τους (άρα και το ρίσκο που συντρέχουν) μεταθέτοντας την στις άλλες οντότητες που συμμετέχουν. Αυτό έγινε με δύο τρόπους: αφενός με την σύναψη ιδιωτικών συμβολαίων με τις οντότητες και αφετέρου με την ύπαρξη ειδικών ενοτήτων αποποίησης ευθύνης στις δηλώσεις πρακτικών πιστοποίησης, οι αναφέρονται στα πιστοποιητικά. Έτσι για παράδειγμα, κατά την έκδοση ενός πιστοποιητικού ο χρήστης (στην γενική περίπτωση) υπέγραφε μία συμφωνία η οποία περιείχε τις πιθανές χρήσεις του. Αν ξέφευγε από αυτές, η αρχή πιστοποίησης δεν έφερε ευθύνη για τυχόν ζημιές. Κάτι αντίστοιχο (μόνο πιο έμμεσα) γινόταν και με την επαλήθευση της υπογραφής με το πιστοποιητικό. Το πιστοποιητικό (βλέπε και κεφάλαιο 3) περιέχει πεδία όπου αναφέρεται η δήλωση πρακτικών πιστοποίησης, όπου δηλώνεται ρητά για ποιες χρήσεις του η αρχή πιστοποίησης φέρει ευθύνη. Χρήση του πιστοποιητικού σημαίνει και αποδοχή των όρων αυτών. Καταλαβαίνουμε έτσι πώς στην σημερινή πραγματικότητα ευθύνη για τις ζημιές που μπορεί να προκληθούν από ένα πιστοποιητικό, φέρουν και οι τρεις οντότητες, που προαναφέραμε.

Το θέμα της ρύθμισης της ευθύνης, με την διάσταση που το εξετάζουμε εδώ αφορά κυρίως την ρύθμιση της ευθύνης με κάποιο νομικό καθεστώς. Το φλέγον ζήτημα είναι αν θα πρέπει να ρυθμιστεί το συγκεκριμένο θέμα: με νομικό καθεστώς, ή να αφεθεί στην αυτορύθμιση, όπως άλλωστε γινόταν και τόσα χρόνια.

Ορισμένα από τα επιχειρήματα εναντίον της νομικής ρύθμισης είναι:

- Οι τεχνολογίες ηλεκτρονικών υπογραφών και υποδομής δημοσίου κλειδιού, είναι σε αρχικό στάδιο (σε ό,τι αφορά την εφαρμογή τους) και έτσι δεν έχουν ακόμα κατανοηθεί πλήρως οι επιπτώσεις της εφαρμογές τους σε μεγάλη κλίμακα (κάτι που περιλαμβάνει και το κόστος λειτουργίας).

[4] Κατ' εμάς δεν είναι επίσης αποδεκτό οι κατασκευαστές λογισμικού να αποποιούνται τις ευθύνες τους, για τυχόν προβλήματα του λογισμικού (πχ. κενά ασφαλείας) πριν την εγκατάσταση του αλλά αυτό είνα μία άλλη ιστορία.

- Δεν είναι δυνατόν, το θέμα της ευθύνης να ρυθμιστεί νομικά και μονοσήμαντα, καθώς υπάρχουν πιστοποιητικά τα οποία εκδίδονται για διαφορετικές χρήσεις και κατά συνέπεια οι ζημιές που προκαλούν είναι διαφορετικές. Έτσι δεν είναι δυνατόν να καθοριστεί επακριβώς η ευθύνη για τις ζημιές που προκαλούνται από ένα πιστοποιητικό.
- Οι πιστοί της ελεύθερης αγοράς, θεωρούν ότι δεν χρειάζονται ρυθμιστικές παρεμβάσεις, καθώς οι δυνάμεις του ανταγωνισμού θα καθορίσουν από μόνες τους την κατανομή της ευθύνης μέσω των ανταγωνιστικών πρακτικών που θα ακολουθούν οι αρχές πιστοποίησης **[Ford, 2001]**.

Από τους υποστηρικτές των παραπάνω απόψεων προτείνεται λοιπόν ο χειρισμός της ευθύνης ανά περίπτωση και με χρήση συμβολαίων.

Η άλλη άποψη θέτει τα εξής επιχειρήματα:

- Οι πάροχοι υπηρεσιών πιστοποίησης φέρουν ευθύνη για τις ζημιές που τυχόν προκληθούν από τα πιστοποιητικά τα οποία εκδίδουν, καθώς αυτή ακριβώς είναι η δουλειά τους. Να διερευνούν τα υποκείμενα των πιστοποιητικών και να 'εγγυώνται' γι' αυτά. Δεν έχει νόημα η ύπαρξη μίας έμπιστης τρίτης οντότητας, η οποία δεν φέρει ευθύνη, ούτε μιας αρχής πιστοποίησης η οποία στην ουσία δεν πιστοποιεί.
- Η μεταβίβαση και η μετρίαση της ευθύνης για τις αρχές πιστοποίησης, η οποία μπορεί να επιτευχθεί πρακτικά, ενδεχομένως λειτουργήσει ανασταλτικά στην αποδοχή των ηλεκτρονικών υπηρεσιών από το ευρύ κοινό. Επίσης η ύπαρξη μίας κοινής αντιμετώπισης των παρόχων πιστοποίησης, κάτι που μπορεί να επιτευχθεί μόνο με κάποια νομική οδηγία, δίνει ένα αίσθημα δίκαιης αντιμετώπισης στο ευρύ κοινό.
- Η ύπαρξη ευθύνης μπορεί να λειτουργήσει ως κίνητρο για τους παρόχους πιστοποίησης για την σωστή λειτουργία και μεγαλύτερη ασφάλεια των συστημάτων τους και καλύτερη εκτέλεση των καθηκόντων τους.

Προτείνεται κατά συνέπεια από αυτή την πλευρά, η ρύθμιση της ευθύνης μέσω καθολικά εφαρμόσιμων κανονιστικών και νομικών κειμένων.

Οι νομικές προσεγγίσεις στις ηλεκτρονικές υπογραφές, μέχρι σήμερα χρησιμοποιούν την έννοια της διαπίστευσης ως μέσο για να γεφυρώσουν τις παραπάνω πλευρές. Και σε αυτές βέβαια παρ' όλο που τηρείται μία κοινή γραμμή υπάρχουν αρκετές αποκλίσεις. Οι τάσεις που παρατηρούνται είναι οι εξής:

- Οι διαπιστευμένες αρχές πιστοποίησης απολαμβάνουν 'ασυλία' από την ευθύνη που ενέχουν σε τυχόν ζημιές που ίσως προκληθούν από ανακρίβειες σε πιστοποιητικά τους, αν αυτά χρησιμοποιηθούν με τρόπο διαφορετικό από αυτόν που αναγράφεται στην δήλωση πρακτικών πιστοποίησης. Για παράδειγμα, δηλαδή αν η χρήση ενός πιστοποιητικού είναι για ποσά κάτω από ένα συγκεκριμένο όριο, και υπάρξει υπέρβαση, δηλαδή το πιστοποιητικό χρησιμοποιηθεί για ανώτερα ποσά, και προκληθούν ζημιές, ο (διαπιστευμένος) πάροχος πιστοποίησης δεν φέρει (νομικά) ευθύνη ακόμα και αν αποδειχθεί ότι έδειξε αμέλεια. Η προσέγγιση αυτή ακολουθείται

κυρίως στα νομικά πλαίσια τα οποία εφαρμόζονται σε αρκετές πολιτείες των Η.Π.Α, με πρωτοπόρους στον συγκεκριμένο τομέα την πολιτεία της Utah.

- Ο πάροχος πιστοποίησης φέρει κάποια ευθύνη (ακόμα και αν είναι διαπιστευμένος) εκτός αν αποδειχθεί ότι δεν επέδειξε αμέλεια. Η προσέγγιση αυτή χαρακτηρίζει την ευρωπαϊκή οδηγία.

Οι συγκεκριμένες προσεγγίσεις ουσιαστικά υπονοούν ότι τα καθήκοντα και οι υπηρεσίες μιας αρχής πιστοποίησης που αναφέρονται στον κανονισμό με βάση τον οποίο γίνεται η διαπίστευση, είναι πλήρη, αφού αλλιώς δεν θα μπορούσαν δεν θα επέτρεπαν τον καταλογισμό ευθύνης στον πάροχο.

Μία άλλη προσέγγιση στο όλο θέμα, εκμεταλλεύεται τον ισομορφισμό του με άλλες περιπτώσεις ρύθμισης ευθύνης τις οποίες και προσπαθεί να προσαρμόσει. Έτσι για παράδειγμα, υπάρχει το ανάλογο των πιστωτικών καρτών. Στην συγκεκριμένη περίπτωση, ο τελικός καταναλωτής, και δεδομένου ότι προβεί σε σωστές ενέργειες, έχει δικαίωμα να απαιτήσει ευθύνη και αποζημίωση για απώλειες λόγω απάτης μέσω πιστωτικής κάρτας, για ποσά μεγαλύτερα των 50$. Ο αντίλογος στην προσέγγιση αυτή αφορά την λογική βάση της παραπάνω υπόθεσης. Κατά πόσο δηλαδή όντως υφίσταται ο συγκεκριμένος ισομορφισμός; Οι λειτουργία των πιστωτικών οργανισμών διαφέρει από την λειτουργία των παρόχων πιστοποίησης σε δύο τουλάχιστον σημεία:

- Οι πάροχοι πιστοποίησης δεν έχουν κανένα κέρδος από την συναλλαγή στην οποία χρησιμοποιείται τα πιστοποιητικό τους, σε αντίθεση με τον εκδότη της πιστωτικής κάρτας.
- Οι συναλλαγές στις οποίες μπορεί να χρησιμοποιηθεί ηλεκτρονική υπογραφή και κατά συνέπεια ηλεκτρονικό πιστοποιητικό δεν μοιράζονται την ομοιομορφία των συναλλαγών πιστωτικών καρτών.

Σε κάθε περίπτωση πάντως, η προσέγγιση που θα ακολουθηθεί θα φέρει αλλαγές στο ισχύον νομικό πλαίσιο για πώληση αγαθών και παροχή υπηρεσιών.

5.5 Αμφισβήτηση Υπογραφής

Ένα σχετικό με το παραπάνω θέμα είναι αυτό που μπορεί να προκύψει από τις δυνατότητες που δίνει το νομικό πλαίσιο που διαμορφώνεται με βάση τα όσα εξετάσαμε εδώ, σχετικά με την ευχέρια ενός χρήστη να αμφισβητήσει την ηλεκτρονική πλέον υπογραφή του. Όπως είδαμε και αρχικά κάποιος χρήστης μπορεί με βάση κάποια κριτήρια να αμφισβητήσει επιτυχώς το ότι ήταν αυτός που υπέγραψε (με συμβατικό τρόπο) κάποιο κείμενο. Το ίδιο θα πρέπει να είναι δυνατόν και στις ψηφιακές υπογραφές.

Όταν λοιπόν πρόκειται να αμφισβητηθεί μία συμβατική υπογραφή το βάρος της απόδειξης, το έχει η οντότητα η οποία βασίζεται σε αυτήν (ο επαληθεύων, θα λέγαμε καλύτερα στην περίπτωση). Ο επαληθεύων καλείται να αποδείξει ότι ο υπογράφων (ο οποίος το αρνείται) όντως υπέγραψε. Αυτό είναι άμεση συνέπεια μίας ιδιότητας που ισχύει παραδοσιακά στις δικαστικές αίθουσες, ότι δηλαδή αυτός που υποστηρίζει κάτι, έχει και το βάρος της απόδειξης του. Τα πρώτα ρυθμιστικά κείμενα σχετικά με τις ηλεκτρονικές – ψηφιακές υπογραφές (**[ABA, 1996], [UNCITRAL, 1996]** και κατά συνέπεια η νομοθεσία της Utah) φαίνεται να έχουν λάβει μία διαφορετική σκοπιά, σχετικά με το συγκεκριμένο θέμα. Εν συντομία θεωρούν, ότι οι

παρακάτω σχέσεις:

- Μία ψηφιακή υπογραφή συνδεέται με ένα δημόσιο κλειδί.
- Ένα δημόσιο κλειδί περιέχεται σε ένα πιστοποιητικό.
- Το πιστοποιητικό έχει εκδοθεί σε ένα συγκεκριμένο υποκείμενο.
- Το υποκείμενο είναι κάτοχος του ιδιωτικού κλειδιού.
- Το ιδιωτικό κλειδί συνδέεται με μαθηματική σχέση με το δημόσιο.
- Άρα, το ιδιωτικό κλειδί έχει χρησιμοποιηθεί για την παραγωγή της υπογραφής που επαληθεύθηκε αρχικά,

αποτελούν μία λογική ακολουθία και κατά συνέπεια είναι αρκετές για αυτά που καλείται να απόδειξει ο επαληθεύων. Έτσι λοιπόν θεωρούν ότι εξ ορισμού τα συστήματα ψηφιακών πιστοποιητικών, ικανοποιούν τις όποιες απαιτήσεις απόδειξεις έχει ο επλαηθεύων. Σε περίπτωση λοιπόν που κάποιο αρνηθεί μία ηλεκτρονική του υπογραφή, καλείται ο ίδιος να αποδείξει ότι δεν υπέγραψε αυτός.

Είναι φανερό ότι το παραπάνω γεγονός θέτει τον υπογράφοντα, σε πιο δεινή σχέση σχετικά αυτήν που κατείχε με τις συμβατικές υπογραφές, καθώς σε περίπτωση που κάποιος του παρουσιάσει ένα κείμενο το οποίο επαληθεύθηκε με το δημόσιο κλειδί του, τότε θα πρέπει αυτός να αποδείξει ότι δεν υπέγραψε.

Από το σημείο και μετά οι δυνατότητες που έχει ο υπογράφων να αρνηθεί την υπογραφή του, είναι υποστηρίζοντας ότι ασκήθηκε ψυχολογική πίεση, ή είχε κλαπεί το ιδωτικό του κλειδί. Αν καταφέρει να αποδείξει κάτι τέτοιο επαρκώς, τότε βέβαια η κατάσταση εξομαλύνεται και καλείται να αποφασίσει η δικαιοσύνη.

Ένα θέμα το οποίο έρχεται ως συνέπεια της παραπάνω συζήτησης αφορά το ότι όλα τα παραπάνω, δεν θα μπορούσε να τα προδιαγράψει κανείς αν δεν υπήρχε γνώση της τεχνολογίας η οποία υλοποιεί τις ηλεκτρονικές υπογραφές.

5.6 Θέματα Διαβούλευσης.

Στην ενότητα αυτή θα εξετάσουμε κάποια από τα θέματα τα οποία απασχόλησαν την δημόσια διαβούλευση που έγινε στην Ελλάδα μετά από σχετική πρόσκληση της ΕΕΤΤ **[ΕΕΤΤ, 2001].** Αντίστοιχες ενέργειες, έγιναν και σε άλλες ευρωπαϊκές χώρες **[DTI, 2001].** Κατά την διάρκεια συγγραφής του συγκεκριμένου κειμένου, δεν ήταν γνωστά τα αποτελέσματα της συγκεκριμένης διαβούλευσης, οπότε οι απόψεις που θα εκφράσουμε εδώ είναι καθαρά προσωπικές. Έχουν δε αποκλειστικά ερευνητικό χαρακτήρα.

Οι ερωτήσεις που τέθηκαν αφορούν τα εξής θέματα:

1. Ανάκληση - Ακύρωση Πιστοποιητικών

Το πρώτο θέμα που θίγει η διαβούλευση είναι οι περιπτώσεις στις οποίες πρέπει να υπάρξει ανάκληση των αναγνωρισμένων πιστοποιητικών. Οι περιπτώσεις που αναφέρονται είναι:

- *Μετά από αίτηση του υποκειμένου*. Η συγκεκριμένη περίπτωση είναι η κλασική και προβλέπεται σε

όλες τα πλαίσια που εξετάσαμε.

- *Μετά από διαπίστωση ότι τα αναγνωρισμένα πιστοποιητικά δεν συμβαδίζουν με το παράρτημα 1 της οδηγίας*. Εδώ προκύπτει ένα θέμα σχετικά με τον ακριβή ορισμό του αναγνωρισμένου πιστοποιητικού, καθώς εκτός από το παράρτημα 1, ο πάροχος πρέπει να ικανοποιεί και τις διατάξεις του παραρτήματος 2. Τι θα γίνει σε περίπτωση που μετά από κάποιο έλεγχο του εποπτικού φορέα, βρεθεί ότι κάτι τέτοιο δεν συμβαίνει; Θα πρέπει να ανακληθούν όλα τα πιστοποιητικά που έχουν εκδοθεί ή μήπως εφ' όσον δεν θα έχει προκύψει κάποιο θέμα ασφαλείας να διατηρηθεί η ισχύς των πιστοποιητικών με τις αυστηρότερες απαιτήσεις που θα έχουν προκύψει μετά από τον έλεγχο. Αν εξετάσουμε την αυστηρότερη προσέγγιση, την γερμανική, θα διαπιστώσουμε ότι στο άρθρο 19(5) του **[SIGGc, 2000],** ορίζει ότι αν μετά από κάποιο έλεγχο υπάρξει κάποια κύρωση ή τερματισμός λειτουργίας ενός αναγνωρισμένου πάροχου υπηρεσιών πιστοποίησης, η ισχύς των αναγνωρισμένων πιστοποιητικών παραμένει.
- *Σε περίπτωση που υπάρξει παύση εργασιών του παρόχου*. Όπως προκύπτει από το θέμα διαβούλευσης (2) αυτό θα γίνει μόνο σε περίπτωση που δεν βρεθεί κάποιος άλλος φορέας ο οποίος να αναλάβει τις απαραίτητες σχετικές υπηρεσίες.

Επιπλέον μπορούν να προστεθούν οι εξής περιπτώσεις:

- Αν συμβεί παραβίαση του ιδιωτικού κλειδιού υπογραφής του παρόχου υπηρεσιών πιστοποίησης
- Αν υπάρχουν σχέσεις εμπιστοσύνης μεταξύ παρόχων εμπιστοσύνης σε ιεραρχική δομή, αν συμβεί παραβίαση του κλειδιού οποιουδήποτε παρόχου υπηρεσιών πιστοποίησης βρίσκεται σε ανώτερο επίπεδο της ιεραρχίας.

2. Παύση Εργασιών Παρόχων Υπηρεσιών Πιστοποίησης.

Το συγκεκριμένο θέμα διαβούλευσης, αφορά τις ενέργειες οι οποίες πρέπει να γίνουν σε περίπτωση που υπάρξει για οποιοδήποτε λόγο παύση εργασιών ενός παρόχου υπηρεσιών πιστοποίησης. Το βασικό θέμα που προκύπτει σε μία τέτοια περίπτωση είναι το τι θα γίνει με τα (αναγνωρισμένα) πιστοποιητικά τα οποία έχει ήδη εκδώσει; Προφανώς η πιο λογική λύση που προτείνεται είναι η μεταφορά σε κάποιον άλλο πάροχο πιστοποίησης, ο οποίος επιλέγεται είτε από το υποκείμενο του πιστοποιητικού είτε από τον ίδιο τον πάροχο. Προφανώς κατά την μεταφορά αυτή πρέπει να τηρηθούν κάποιες αναλογίες. Δηλαδή αν μια αρχή πιστοποίησης είναι διαπιστευμένη τότε και ο αποδέκτης πρέπει να είναι διαπιστευμένος. Σε αυτό το σημείο δεν έχουμε να προτείνουμε τίποτα περισσότερο. Οι μόνες τεχνικές δυσκολίες πιστεύουμε ότι θα υπάρξουν εξαιτίας του γεγονότος ότι και ο κάτοχος του πιστοποιητικού μπορεί να επιλέξει σε ποιον πάροχο υπηρεσιών πιστοποίησης θα μεταφερθούν τα πιστοποιητικά. Δεν θα είναι πρακτικό λοιπόν να υπάρχουν πολλοί αποδέκτες, κάτι που θεωρητικά είναι δυνατό να συμβεί, καθώς δύο υποκείμενα μπορούν να επιλέξουν διαφορετικούς νέους παρόχους πιστοποίησης. Κατά την γνώμη μας πρέπει η ΕΕΤΤ να αποφασίσει σε κάθε περίπτωση για τον αποδέκτη.

3. Προϋποθέσεις για Εθελοντική Διαπίστευση

Οι προϋποθέσεις που αναφέρονται για την εθελοντική διαπίστευση αφορούν την τήρηση του παραρτήματος 1 για το περιεχόμενο των πιστοποιητικών και του παραρτήματος 2 για τον ίδιο τον πάροχο. Επιπλέον επιβάλλεται η χρήση μόνο ασφαλών διατάξεων δημιουργίας υπογραφής (δεν αναφέρεται για ποιον σκοπό, αλλά υποθέτουμε για την υπογραφή των πιστοποιητικών που εκδίδει). Επισημαίνουμε εδώ ότι στο παράρτημα 1 της οδηγίας αναφέρεται ότι το αναγνωρισμένο πιστοποιητικό πρέπει να φέρει την προηγμένη ηλεκτρονική υπογραφή του παρόχου υπηρεσιών πιστοποίησης και όχι την αναγνωρισμένη ηλεκτρονική υπογραφή (που απαιτεί χρήση ασφαλούς διάταξης). Θεωρούμε ότι η χρήση ασφαλούς διάταξης για την υπογραφή των πιστοποιητικών είναι καλή πρακτική και κατά συνέπεια μπορεί να χρησιμοποιηθεί ως κριτήριο διαπίστευσης. Επιπλέον κριτήριο διαπίστευσης θα μπορούσε να θεωρηθεί η χρήση γενικότερα αξιόπιστων προϊόντων ηλεκτρονικών υπογραφών, για όλα τα πιστοποιητικά και όχι μόνο για τα αναγνωρισμένα. Ένα άλλο κριτήριο για την διαπίστευση εφαρμόζεται στην Γερμανία, σύμφωνα με το οποίο αναγνωρισμένα πιστοποιητικά εκδίδονται μόνο όταν το υποκείμενο του πιστοποιητικού αποδεδειγμένα κατέχει ασφαλή διάταξη δημιουργίας υπογραφής. Εδώ ισχύουν όσα αναφέρουμε στο θέμα διαβούλευσης (6), καθώς η συγκεκριμένη διάταξη δεν έχει σχέση με την ποιότητα υπηρεσιών του παρόχου πιστοποίησης, αλλά με την ασφάλεια των υπογραφών του υποκειμένου. Οπότε κατά τη γνώμη μας δεν θα πρέπει να υφίσταται.

Σε ό,τι αφορά τον διαχωρισμό ενός αναγνωρισμένου από ένα μη αναγνωρισμένο πιστοποιητικό, αυτό θα γίνεται με χρήση του συγκεκριμένου πεδίου το οποίο προβλέπει η οδηγία και στο οποίο θα δηλώνεται ξεκάθαρα ότι πρόκειται για αναγνωρισμένο πιστοποιητικό, κάτι που αναφέρεται ρητά και σητν οδηγία. Οι εφαρμογές των ηλεκτρονικών υπογραφών, που θα λαμβάνουν το πιστοποιητικό, θα ενημερώνουν κατάλληλα τον χρήστη. Πώς όμως θα εξασφαλίζεται ότι ένα πιστοποιητικό το οποίο φέρει την ένδειξη του αναγνωρισμένου είναι όντως αναγνωρισμένο; Όπως φαίνεται από το παράρτημα 1, της οδηγίας και σε καθαρά πρακτικό επίπεδο, είναι μάλλον δύσκολο, ένα πιστοποιητικό να μην πληρεί τις προϋποθέσεις του παραρτήματος 1, σχετικά με τα περιεχόμενα ή να ισχυρίζεται ψευδώς ότι τις ικανοποιεί, Κατά συνέπεια, η μόνη περίπτωση που ένα ‘αναγνωρισμένο’ πιστοποιητικό, δεν καλύπτει τις απαιτούμενες από την οδηγία ιδιότητες, είναι να μην ικανοποιεί ο πάροχος πιστοποίησης της απαιτήσεις του παραρτήματος 2. Αυτό θα διαπιστωθεί μέσω του εποπτικού μηχανισμού που προβλέπει η οδηγία για αυτούς που εκδίδουν αναγνωρισμένα πιστοποιητικά. Σε περίπτωση που μέσω του συγκεκριμένου μηχανισμού διαπιστωθεί ότι ο πάροχος δεν πληρεί τις προϋποθέσεις και άρα τα πιστοποιητικά που φέρουν την ένδειξη του αναγνωρισμένου κακώς την φέρουν, τότε ο πάροχος πρέπει να αντιμετωπίσει ευθύνη. Το ίδιο βέβαια θα συμβεί και στην περίπτωση που κάποιος έχει βασιστεί σε ένα ψευδώς φερόμενο ως αναγνωρισμένο πιστοποιητικό για την επαλήθευση μιας υπογραφής και έχει υποστεί ζημιές. Κάτι τέτοιο θα μπορούσε να συμβεί σε περίπτωση που η ανάκληση ενός πιστοποιητικού δεν έχει γνωστοποιηθεί άμεσα μέσω του καταλόγου (υπάρχει παραβίαση δηλαδή της δεύτερης απαίτησης του παραρτήματος 2). Η ευθύνη αυτή

άλλωστε προβλέπεται και από το άρθρο 6 της οδηγίας.

4. Η ΕΕΤΤ ως η κορυφή ιεραρχίας εθελοντικά διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης.

Το προτεινόμενο μοντέλο εφαρμόζεται στην Γερμανία. Η αντίστοιχη αρχή εκδίδει αναγνωρισμένα πιστοποιητικά για τους πάροχους υπηρεσιών πιστοποίησης που έχουν διαπιστευτεί. Όπως είναι φανερό αυτό θα έχει ως συνέπεια την τήρηση από την ΕΕΤΤ του παραρτήματος 2 της οδηγίας καθώς επίσης και οποιουδήποτε επιπλέον κριτηρίου αυτή θεσπίσει για τους εθελοντικά διαπιστευμένους. Ποιος όμως θα μπορέσει να το διαπιστώσει αυτό; Σε ότι αφορά την δημιουργία των ιδιωτικών κλειδιών (δεδομένα δημιουργίας υπογραφής) αυτό ίσως να μπορεί να γίνεται αν η ΕΕΤΤ, διαθέτει πιο ασφαλείς διατάξεις. Εξυπακούεται βέβαια η μη τήρηση αντιγράφου.

Το συγκεκριμένο μοντέλο έχει ως κύριο στόχο την παροχή πληροφορίας κατάστασης σχετικά με το αν ένας πάροχος υπηρεσιών πιστοποίησης είναι διαπιστευμένος από την Ε.Ε.Τ.Τ. Η πληροφορία αυτή μπορεί να χρησιμεύσει σε οποιονδήποτε χρήστη που επαληθεύει μία υπογραφή, καθώς μπορεί να μάθει για την αναγνώριση οποιουδήποτε πάροχου υπηρεσιών πιστοποίησης και να αποκτήσει έτσι περισσότερη (ή λιγότερη) εμπιστοσύνη σε κάποιο πιστοποιητικό. Για τον σκοπό αυτό θα μπορούσαν να χρησιμοποιηθούν και εναλλακτικά μοντέλα, τα πιο σημαντικά από τα οποία αναφέρονται στο **[ETSI, 178T1]** και είναι τα εξής:

- Λίστα Διαπιστευμένων: Το συγκεκριμένο μοντέλο έχει εφαρμοστεί με επιτυχία στην Ιταλία, όπου ο αντίστοιχος φορέας εκδίδει μία λίστα, την οποία υπογράφει ψηφιακά και στην οποία αναφέρει τους παρόχους υπηρεσιών πιστοποίησης τους οποίους έχει αναγνωρίσει. Μαζί με την λίστα αυτή παρέχεται βέβαια και το δημόσιο κλειδί, έτσι ώστε να μπορεί ο ενδιαφερόμενος να επαληθεύσει την υπογραφή.
- Πιστοποιητικά Διαπίστευσης: Η συγκεκριμένη μέθοδος χρησιμοποιείται στην Μ. Βρετανία από τον αρμόδιο οργανισμό tScheme. Κάθε αρχή πιστοποίησης λαμβάνει ένα πιστοποιητικό (όχι με την έννοια που το έχουμε συναντήσει στην παρούσα εργασία) ότι είναι αναγνωρισμένη.
- Λίστες Παραβατών: Η συγκεκριμένη μέθοδος είναι παρόμοια με πρώτη, με την διαφορά πως στην λίστα αναφέρονται μόνο οι πάροχοι υπηρεσιών πιστοποίησης, οι οποίοι αν και ήταν αναγνωρισμένοι μέχρι κάποιο σημείο, έχουν χάσει την αναγνώριση λόγω αποτυχίας σε τακτικό έλεγχο ή αποτυχία σε έκτακτο έλεγχο μετά από καταγγελία.

5. Εξέταση της Αίτησης για Εθελοντική Διαπίστευση από φορείς εκτός της ΕΕΤΤ – Ορισμός Φορέων.

Στο συγκεκριμένο θέμα πιστεύουμε ότι πρέπει να εφαρμοστούν τα ελάχιστα κριτήρια που έχει θέσει η Ευρωπαϊκή Επιτροπή στο **[CDMC, 2000].** Είτε η διαπίστευση γίνεται από την ΕΕΤΤ, είτε από άλλο φορέα και αν κρίνουμε από τις περιπτώσεις που έχουμε μελετήσει το κόστος φέρει ο πάροχος πιστοποίησης που την επιζητά.

Στην ιδανική περίπτωση, βέβαια θα μπορούσε να εφαρμοστεί το μοντέλο διαπίστευσης που

αναφέρεται στο **[ABA, 2001]** και το οποίο συστηματοποιεί την διαδικασία διαπίστευσης. Συγκεκριμένα η ΕΕΤΤ μπορεί να ορίσει ένα προφίλ προστασίας (PP), σύμφωνα με το Common Criteria, το οποίο θα αφορά τις αρχές πιστοποίησης, οι οποίες έχουν έδρα στην Ελλάδα. Επίσης ορίζει μία επιδίωξη ασφαλείας την οποία θα πρέπει να επιτύχουν οι αρχές πιστοποίησης, ώστε να λάβουν την διαπίστευση. Έπειτα αναθέτει σε συγκεκριμένους οργανισμούς, τους οποίους έχει βεβαίως διαπιστεύσει πρώτα, τον έλεγχο των συγκεκριμέων αρχών πιστοποίησης, που ισχυρίζονται ότι έχουν επιτύχει τον συγκεκριμένο στόχο ασφαλείας.

6. Έκδοση αναγνωρισμένων πιστοποιητικών μόνο σε περιβάλλον ασφαλών διατάξεων δημιουργίας υπογραφής.

Εδώ προτείνεται η έκδοση αναγνωρισμένων πιστοποιητικών μόνο σε περίπτωση που το υποκείμενο του πιστοποιητικού, χρησιμοποιεί ασφαλείς διατάξεις για την αποθήκευση των δεδομένων δημιουργίας της υπογραφής και την δημιουργία τους. Κατά την γνώμη μας η συγκεκριμένη πρόταση είναι υπερβολικά αυστηρή και υπερβαίνει το πλαίσιο που έχει θέσει η οδηγία. Η εξήγηση γι' αυτό έγκειται στο γεγονός ότι κατά την γνώμη μας (πάντα), οι απαιτήσεις για τα αναγνωρισμένα πιστοποιητικά ως στόχο έχουν την παροχή κάποιων εγγυήσεων σχετικά με τον πάροχο πιστοποίησης, ότι τηρεί κάποια πρότυπα, διαδικασίες κτλ. Η επιβολή όμως της χρήσης ασφαλών διατάξεων θα επιβαρύνει τον τελικό χρήστη. Έτσι, ένα πρόβλημα που μπορεί να δημιουργηθεί από την συγεκριμένη υποχρέωση, είναι η αύξηση του κόστους χρήσης (από τις τελικές οντότητες) των ηλεκτρονικών υπογραφών. Με την παραπάνω άποψη 'συμφωνεί' και το **[ETSI, 101 456]**, το οποίο ορίζει συστάσεις για δύο πολιτικές έκδοσης στο κοινό αναγνωρισμένων πιστοποιητικών, μία που απευθύνεται στα αναγνωρισμένα πιστοποιητικά και ένας δεύτερος που απευθύνεται στα αναγνωρισμένα πιστοποιητικά που χρησιμοποιούνται για ηλεκτρονικές υπογραφές που παράγονται από ασφαλείς διατάξεις.

7. Συμμόρφωση παρόχου πιστοποίησης με τα κριτήρια για έκδοση αναγνωρισμένων πιστοποιητικών.

Όπως είδαμε νωρίτερα, ο πάροχος υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά πρέπει ως οργανισμός να συμβαδίζει με τις προϋποθέσεις του παραρτήματος 2 της οδηγίας. Στο συγκεκριμένο θέμα διαβούλευσης, αναζητώνται τρόποι με τους οποίους μπορεί να επιτευχθεί αυτό. Όπως είδαμε και στα προηγούμενα κεφάλαια (συγκεκριμένα στο 3^{ο} και στο 4$^{ο)}$, ο καλύτερος τρόπος για τον σκοπό αυτόν είναι η επίδειξη της συμμόρφωσης με το πρότυπο [**ETSI, 101 456]**, όπου αναλύονται οι τεχνικές, διαδικαστικές και οργανωτικές απαιτήσεις του παρόχου ώστε να εκδίδει αναγνωρισμένα πιστοποιητικά. Επίσης άλλα πρότυπα τα οποία πρέπει να χρησιμοποιηθούν είναι το βρετανικό BS 7799 για την διαχείριση ασφάλειας. Όπως είδαμε όμως αυτά ενσωματώνονται στο **[ETSI, 101 456]**. Χρήσιμη θα ήταν επίσης η επίδειξη κάποιου αποδεικτικού ευρωστίας με παράθεση της κατάθεσης ενός συγκεκριμένου ποσού (μία πρόταση είναι τα 250.000€).

8. Επόπτες Ασφαλών Διατάξεων Δημιουργίας Υπογραφής.

Κατά την γνώμη μας και εδώ ισχύουν όσα αναφέραμε στην ενότητα 4.4.6, αλλά και η σχετική απόφαση της Ευρωπαϊκής Επιτροπής **[CDMC, 2000].**

9. Πρότυπα Ασφαλών Διατάξεων Δημιουργίας Υπογραφής.

Τα προτεινόμενα πρότυπα είναι τα πιο συχνά χρησιμοποιούμενα, αν και πιστεύουμε ότι το καταλληλότερο πρότυπο στην συγκεκριμένη περιοχή είναι το προφίλ προστασίας που ορίζεται στα CWA 14168 και 14169 από τον CEN σε επίπεδο διαβεβαίωσης κατά Common Criteria EAL4 και EAL 4+. Επίσης σε ότι αφορά το FIPS-PUB του NIST, θα μπορούσε να χρησιμοποιηθεί η δεύτερη έκδοση του προτύπου την οποία και παρουσιάσαμε στο $3^{ο}$ κεφάλαιο.

10. Πρότυπα για αξιόπιστα συστήματα – προϊόντα.

Ο συγκεκριμένος τομέας αναλύθηκε εκτεταμένα στην εργασία. Οπότε δεν έχουμε τίποτα συμπληρωματικό να πούμε.

11. Εποπτεία Πάροχων Πιστοποίησης.

Στο συγκεκριμένο θέμα διαβούλευσης εξετάζεται η μορφή που θα έχει η εποπτεία των παρόχων υπηρεσιών πιστοποίησης. Ο συγκεκριμένος τομέας, όπως ίσως έχει διαφανεί και από την εξέταση της οδηγίας είναι ο πιο ‘περίεργος’, καθώς θεωρούμε ότι η απαίτηση για μη παροχή εκ των προτέρων έγκρισης και η εποπτεία είναι έννοιες αντικρουόμενες, αφού για την αποτελεσματική άσκηση της εποπτείας είναι απαραίτητη η ύπαρξη γνώσης για τις διατάξεις και τον τρόπο λειτουργίας κάθε φορέα πιστοποίησης. Εξ’ άλλου η προαπαιτούμενη έγκριση ορίζεται στην οδηγία (ορισμός 10), όχι μόνο ως κάθε απαίτηση από εθνική αρχή για άδεια λειτουργίας, αλλά και *κάθε μέτρο που έχει παρόμοιο αποτέλεσμα*. Το κρίσιμο θέμα λοιπόν εδώ, είναι αφενός να μην θεωρηθεί οποιοδήποτε μέτρο ληφθεί ως ισοδύναμο της έκδοσης άδειας. Εφ΄όσον η γνωστοποίηση που παρέχεται εδώ δεν συνοδεύεται από κάποιον έλεγχο και δεν μπορεί με κανέναν τρόπο να αποτρέψει τον πάροχο υπηρεσιών πιστοποίησης να δραστηριοποιηθεί, πιστεύουμε ότι είναι μέσα στο πνεύμα αλλά και το γράμμα της οδηγίας και επιπλέον επιτελεί τον σκοπό ενός ευρετηρίου όπου θα είναι διαθέσιμοι όλοι οι πάροχοι για εφαρμογή του συστήματος ελέγχου. Αυτό όπως είπαμε συνεπάγεται ότι δεν θα ελεγχθεί ούτε η τεκμηρίωση ούτε οποιαδήποτε άλλη πτυχή της λειτουργίας του φορέα πιστοποίησης. Σίγουρα πάντως, δεν προτείνουμε κάποια πιο αυστηρή μέθοδο. Στην Μ. Βρετανία για παράδειγμα, δεν διατηρείται καν κάποιο ανάλογο ευρετήριο. Σχετικός έλεγχος ασκείται μόνο μετά από καταγγελίες και αποτελεί την μόνη μορφή εποπτείας.

Σχετική με την συγκεκριμένη ερώτηση είναι και η πορεία που πρέπει να ακολουθηθεί όταν κάποιος πάροχος υπηρεσιών πιστοποίησης βρεθεί μετά από κάποιον έλεγχο, ότι δεν συμβαδίζει για παράδειγμα με τις απαιτήσεις έκδοσης αναγνωρισμένου πιστοποιητικού. Εδώ υπάρχουν αρκετές πιθανές λύσεις. Η πιο

ελαφράς μορφής ‘αντίδραση’ αποτελεί η απλή δημοσιοποίηση του συγκεκριμένου γεγονότος. Ο πάροχος υπηρεσιών πιστοποίησης μπορεί να συνεχίσει κανονικά την λειτουργία του. Εναλλακτικά βέβαια μπορεί και να διακοπεί η λειτουργία του.

Πιο αναλυτικά στην βιβλιογραφία [ETSI, 10230] αναφέρονται οι παρακάτω προσεγγίσεις:

- **Reactive:**

Η συγκεκριμένη προσέγγιση είναι η τυπική που ακολουθείται στην Μεγ. Βρετανία. Δεν απαιτείται η ειδοποίηση με την έναρξη λειτουργίας, ούτε διατηρείται κάποιο μητρώο με τις αρχές πιστοποίησης. Έλεγχος δε υφίσταται μόνο μετά από κάποια καταγγελία.

- **Notification With Publication:**

Στην προσέγγιση αυτή διατηρείται κάποιο μητρώο. Όταν ξεκινάει η αρχή καταγράφεται χωρίς να υπάρχει έλεγχος για μη συμμόρφωση με τις κανονιστικές απαιτήσεις. Έλεγχος και εδώ γίνεται μετά από καταγγελία. Σε περίπτωση που βρεθεί κάποια απόκκλιση τότε έχουμε δημοσίευση του γεγονότος και απλή συνέχιση της λειτουργίας.

- **Notification With Prohibition:**

Η παραπάνω προσέγγιση είναι ίδια με την προαναφερθείσα με την διαφορά του ότι η εύρεση μη τήρησης κάποιων κριτηρίων μπορεί να οδηγήσει σε απαγόρευση λειτουργίας και αφαίρεση αδείας.

- **Notification With Approval:**

Κατά την έναρξη της λειτουργία παρέχεται από την αρχή πιστοποίησης κάποια τεκμηρίωση η οποία και ελέγχεται σε μικρό συνήθως βαθμό. Αν υπάρξει έγκριση η αρχή καταχωρείται σε κάποιο μητρώο και υποχρεούται να δίνει στοιχεία σχετικά με όποιες αλλαγές υπάρξθουν. Επιβάλλεται επίσης απαγόρευση λειτουργίας σε περίπτωση μη συμμόρφωσης μετά από έλεγχο.

- **Assessment And Approval:**

Το συγκεκριμένο μοντέλο το οποίο είναι και το πιο αυστηρό απαιτεί πλήρης αποτίμηση και έλεγχος, πριν την έναρξη λειτουργίας για να δωθεί έγκρισης. Και εδώ επιβάλλεται απαγόρευση λειτουργίας σε περίπτωση μη συμμόρφωσης μετά από έλεγχο.

ΑΚατά την γνώμη μας το καλύτερο σύστημα το οποίο συμβαδίζει κιόλας με τις ευρωπαϊκές επιταγές είναι αυτό της ενημέρωσης με δημοσίευση. Αξίζει πάντως να επισημάνουμε ότι όλες οι παραπάνω προσεγγίσεις δημιουργούν ένα ευρύτερο πρόβλημα. Πώς μπορεί κατά την διάρκειας επαλήθευσης ενός ηλεκτρονικού πιστοποιητικού, να δοθεί πληροφορία στον τελικό χρήστη όχι μόνο για την κατάσταση της υπογραφής, αλλά και για την κατάσταση όλων των αρχών πιστοποίησης που έχουν επίδραση με τον ένα ή τον άλλο τρόπο στην ισχύ του. Με πιο απλά λόγια πώς μπορεί να ενημερωθεί κατά την στιγμή της επαλήθευσης ο χρήστης για το ότι ο πάροχος υπηρεσιών πιστοποίησης είναι διαπιστευμένος ή ότι ελέγχθηκε και βρέθηκε μία παράβαση. Κάτι τέτοιο δεν προβλέπεται στον μηχανισμό επαλήθευσης που περιγράψαμε και η υλοποίηση του αποτελεί ευθύνη του επόπτη. Η σημασία του είναι πολύ μεγάλη σε ένα διεθνές περιβάλλον, καθώς στα στενά όρια μιας επικράτειας είναι εύκολο να γνωρίζει κανείς τις

προαναφερθείσες πληροφορίες.

12. Εποπτεία / Ελεγχος Φορέων Διαπίστευσης

Το συγκεκριμένο θέμα εξετάστηκε στην ενότητα 4.4.6 και καλύπτεται από το πρότυπο **[ECAG, 2000].**

13. Ασφαλής Επαλήθευση Υπογραφών.

Οι συστάσεις για την ασφαλή επαλήθευση των υπογραφών εξετάστηκαν στο κεφάλαιο 3. Επειδή είναι συστάσεις δεν θεωρείται υποχρεωτική η τήρηση τους. Εδώ θα επαναλάβουμε την θέση που λάβαμε στο συγκεκριμένο κεφάλαιο, ότι ένας καλός και μη δαπανηρός τρόπος για την εφαρμογή του συγκεκριμένου παραρτήματος θα είναι μέσω δηλώσεων κατασκευαστών, στις οποίος θα αναφέρεται με ποια πρότυπα συμβαδίζει η συγκεκριμένη διάταξη, με παράλληλη προώθηση της προτυποποίησης, η οποία ήδη υφίσταται με το **[PESV, 2000].** Θεωρούμε μάλιστα πώς αυτό καλό θα ήταν να εφαρμοστεί στην περίπτωση διατάξεων ηλεκτρονικών υπογραφών που αφορούν την επαλήθευση από ανθρώπους, καθώς έτσι εναρμονίζεται με το πνεύμα της οδηγίας, που είναι η προώθηση της χρήσης των ηλεκτρονικών υπογραφών και η ανάπτυξη της εμπιστοσύνης του κοινού προς αυτές. Σε ότι αφορά την αυτοματοποιημένη επαλήθευση, πιθανότατα κατά την γνώμη μας δεν εμπίπτει στο πεδίο εφαρμογής της οδηγίας, καθώς μάλλον θα αφορά B2B συναλλαγές, οι οποίες θα έχουν ρυθμιστεί με κάποιες συμβάσεις και άρα εκπίπτουν τις οδηγίας.

Κατά την γνώμη μας θα μπορούσαν να είχαν είχαν τεθεί και κάποια επιπλέον θέματα, όπως κάποια που έχουμε ήδη αναφέρει σε όλη την διάρκεια της εργασίας. Ένα από αυτά θα μπορούσε να ήταν το πώς βλέπουν οι πάροχοι υπηρεσιών πιστοποίησης την ευθύνη τους προς το ευρύ κοινό. Επίσης τι μέτρα (σε τεχνικό επίπεδο) σκοπεύουν να λάβουν αυτοί για την προστασία των τηρούμενων προσωπικών δεδομένων.

5.7 Συμπεράσματα

Στην ενότητα αυτή εξετάσαμε ορισμένα ανοικτά θέματα σχετικά με τις ηλεκτρονικές υπογραφές και την διαπίστευση, για τα οποία παραθέσαμε τις δικές μας απόψεις. Αρχικά ασχοληθήκαμε με την νομική προσέγγιση προς τις ηλεκτρονικές υπογραφές, και κυρίως το ερώτημα αν η αυτή πρέπει να είναι τεχνολογικά ουδέτερη ή όχι. Μετά εξετάσαμε τις προσεγγίσεις προς την διαπίστευση και το αν αυτή χρησιμοποιείται ως ένα μέσο για την ρύθμιση μιας αγοράς και την εγγύηση ενός καλύτερου επιπέδου παροχής υπηρεσιών ή ως επίτευξη διαλειτουργικότητας Κάναμε επίσης μία ανάλυση του θέματος της ρύθμισης της ευθύνης μεταξύ των οντοτήτων που συμμετέχουν σε ένα κύκλωμα ηλεκτρονικών υπογραφών. Σε όλα τα παραπάνω θέματα παρατηρήσαμε σημαντικές διαφορές ανάλογα με την χώρα ή την ευρύτερη περιοχή υλοποίησης. Οι διαφορές αυτές δυσκολεύουν την χρήση σε παγκόσμια κλίμακα των ηλεκτρονικών υπογραφών και των παρόχων υπηρεσιών πιστοποίησης. Έμπρακτα αποδεικνύεται έτσι το ότι δεν αρκεί το

να παρέχεται η τεχνολογική δυνατότητα για να υλοποιηθεί κάτι. Κατά την γνώμη μας οι διαφορές αυτές είναι κυρίως θέμα κουλτούρας το οποίο για ξεπεραστεί τελικά πρέπει να περάσουν αρκετά χρόνια χρήσης των υπηρεσιών ηλεκτρονικής πιστοποίησης σε παγκόσμια κλίμακα, ώστε να αφομοιωθούν αυτές συλλογικά.

Τέλος αναφερθήκαμε στα θέματα διαβούλευσης που έχουν ξεκινήσει στην Ελλάδα, για την υλοποίηση του προεδρικού διατάγματος και κατ' επέκταση της οδηγίας, στα οποία προσπαθήσαμε να δώσουμε απαντήσεις με βάση όσα έχουμε ήδη παραθέσει στην εργασία. Εκ των υστέρων ίσως πολλά θα μπορούσε να πεί κανείς. Βέβαια στον συγκεκριμένο τομέα δεν υπάρχει σωστό ή λάθος, καθώς ακόμα υπάρχει λίγη εμπειρία ώστε να αναπτυχθεί η συγκεκριμένη τεχνολογία σε τόσο μεγάλη κλίμακα με ό,τι αυτό συνεπάγεται. Όπως προαναφέραμε όμως, στον συγκεκριμένο τομέα, οι λύσεις δεν μπορούν να εφαρμοστούν μόνο μετά απο θεωρητικές προτάσεις. Πρέπει να υπάρξει εκτεταμένη εφαρμογή σε πραγματικές συνθήκες.

6 Συμπεράσματα

Κλείνοντας, κρίνουμε σκόπιμο να κάνουμε μία ανασκόπηση της όλης προσπάθειας και κάποια κριτική της. Στην εργασία αυτή, λοιπόν, ασχοληθήκαμε με όλες τις πτυχές του θέματος των ηλεκτρονικών υπογραφών, ενός θέματος το οποίο από ό,τι φαίνεται θα αποτελέσει ένα αναπόσπαστο κομμάτι της νέας πραγματικότητας που φαίνεται να αναδύεται με την διείσδυση των τεχνολογιών πληροφορικής και επικοινωνιών σε όλες τις πτυχές της καθημερινής ζωής.

Ξεκινήσαμε την προσέγγιση μας, με την θεώρηση των νέων αναγκών που προκύπτουν από την μετάβαση όλο και περισσότερων συναλλαγών από τον συμβατικό και απτό κόσμο, στον ηλεκτρονικό αντίστοιχο. Η μετάβαση αυτή αν και έχει τεράστια ωφέλη σε ταχύτητα, αποτελεσματικότητα και κόστος, αλλάζει επίπεδο αφαίρεσης στον ανθρώπινο παρατηρητή και συμμετέχοντα και τον κάνει να νιώθει ότι δεν έχει πλέον τον έλεγχο. Όλα γίνονται κάπως, δεν είναι ξεκάθαρο όμως το πώς. Κατά συνέπεια πρακτικές οι οποίες είχαν παγιώσει εδώ και εκατοντάδες χρόνια, πρέπει να αναθεωρηθούν.

Εμείς ασχοληθήκαμε με τις ηλεκτρονικές υπογραφές και το περιβάλλον στο οποίο αυτές λειτουργούν. Κάποιος θα μπορούσε να πεί, πως η μετάβαση σε ένα τέτοιο περιβάλλον δεν είναι απαραίτητη καθώς η υπογραφή δεν αποτελεί μέρος της ουσίας μιας συναλλαγής, αλλά τμήμα της αναπαράστασης της που χρησιμοποιείται για να ικανοποιηθούν νομικές και άλλες απαιτήσεις. Κατά συνέπεια, μπορεί να εξακολουθήσει η αναπαράσταση να έχει την συγκεκριμένη μορφή, παρόλο που η συναλλαγή θα εκτελείται ηλεκτρονικά. Η άποψη αυτή δεν είναι καθόλου παράλογη, καθώς βρισκόταν σε εφαρμογή αρκετά χρόνια. Δεν είναι όμως εφαρμόσιμη σε μεγάλη κλίμακα και δεν εκμεταλλεύεται τα πλεονεκτήματα που χαρακτηρίζουν το ηλεκτρονικό περιβάλλον που προαναφέραμε.

Προχωρήσαμε εξετάζοντας, τις διαθέσιμες τεχνολογίες για την υλοποίηση των ηλεκτρονικών υπογραφών. Η περισσότερη υποσχόμενη, είναι είναι αυτή των ψηφιακών υπογραφών που βασίζεται στην ασύμμετρη κρυπτογραφία. Η συγκεκριμένη τεχνική αριθμεί 25 χρόνια ζωής. Προτάθηκε κυρίως για την επίλυση διαχειριστικών προβλημάτων των συμμετρικών κρυπτοσυστημάτων. Εξ΄αρχής όμως έγινε κατανοητό, ότι παρείχε και έναν τρόπο για την αυθεντικοποίηση των οντοτήτων που συμμετέχουν σε μία συναλλαγή. Η αυθεντικοποίηση αυτή βασίζεται σε δύο στοιχεία: στην ύπαρξη μίας μαθηματικής σχέσης μεταξύ δύο τμημάτων δεδομένων και στην *υπόθεση* ότι κάθε οντότητα, έχει αποκλειστικά υπό την κατοχή της το ένα τμήμα από τα δεδομένα αυτά. Η τεχνική αυτή ονομάστηκε ψηφιακή υπογραφή, αν και είναι μέθοδος αυθεντικοποίησης. Η αυθεντικοποίηση βέβαια είναι μόνο μία από τις ενδείξεις που παρέχει μία υπογραφή και για τον λόγο αυτό και θεωρήσαμε τον όρο αυτόν όχι απόλυτα επιτυχημένο.

Από την περιγραφή που κάναμε φάνηκε ότι η συγκεκριμένη μέθοδος μπορεί να λειτουργήσει μόνο αν είναι διαθέσιμες, συγκεκριμένες υπηρεσίες πιστοποίησης και υποστηρικτική υποδομή. Η πιστοποίηση αυτή πρακτικά επιτυγχάνει την αντιστοίχιση της ταυτότητας μίας οντότητας από τον πραγματικό στον ηλεκτρονικό κόσμο. Επιπλέον όμως δίνει στον πάροχο υπηρεσιών πιστοποίησης έμμεση συμμετοχή σε

κάθε ηλεκτρονική συναλλαγή.

Στην συνέχεια, εξετάσαμε τα διαφορετικά συστήματα τα οποία συμμετέχουν σε μία συναλλαγή ηλεκτρονικών υπογραφών, είτε αυτά χρησιμοποιούνται από τον υπογράφοντα είτε από τον επαληθεύοντα, είτε από τον πάροχο υπηρεσιών πιστοποίησης. Για την πρώτη κατηγορία συστημάτων, αυτά δηλαδή που χρησιμοποιούνται για την δημιουργία μιας υπογραφής, η επικρατέστερη λύση θέλει την χρήση συστήματος που να βασίζεται σε κάποιας μορφής έξυπνη κάρτα. Εμείς χρησιμοποιώντας την σχετική προτυποποίηση, παρουσιάσαμε μία μοντελοποίηση και τις απαιτήσεις ασφαλείας. Το ίδιο κάναμε και στην περίπτωση των διατάξεων επαλήθευση υπογραφής, για τις οποίες δεν υπάρχουν τόσο σαφείς κατευθύνσεις σε ότι αφορά χρησιμοποιούμενα συστήματα. Ιδιαίτερη βαρύτητα δώσαμε στα συστήματα που διαθέτουν οι παροχείς υπηρεσιών πιστοποίησης και στις απαιτήσεις ασφαλείας που πρέπει να διαθέτουν αυτά.

Στην συνέχεια ασχοληθήκαμε με τις διάφορες νομικές προσεγγίσεις στο συγκεκριμένο θέμα, οι οποίες κρίνονται απαραίτητες για την χρήση των συγκεκριμένων υπηρεσιών από πολίτες και την επικύρωση τους. Αναλύσαμε διεξοδικά την ευρωπαϊκή οδηγία, όχι μόνο λόγω του άμεσου αντίκτυπου της, αλλά και λόγω του γεγονότος ότι είναι η πρώτη μη ρυθμιστική προσπάθεια η οποία δεν περιορίζεται μόνο σε εθνικό επίπεδο εφαρμογής. Έπειτα εξετάσαμε την έννοια και την εφαρμογή της διαπίστευσης σε ευρωπαϊκό επίπεδο και στις πιο σημαντικές χώρες διεθνώς. Αξίζει να σημειώσουμε εδώ, ότι σε όλη την διάρκεια της εργασίας θεωρήσαμε την διαπίστευση όπως αυτή ορίζεται στην ευρωπαϊκή οδηγία, και όχι όπως αυτή είναι ευρύτερα γνωστή, ως δηλαδή η παροχή αναγνώρισης σε φορείς που ελέγχουν συμβατότητα με διεθνή πρότυπα. Τα διεθνή πλαίσια τα οποία συνδέονται με την διαπίστευση διεθνώς μπορούν να ενταχθούν σε δύο κατηγορίες: αυτά τα οποία έχουν ως στόχο να παρέχουν κάποιες εγγυήσεις ποιότητας στους τελικούς καταναλωτές και αυτά τα οποία εφαρμόζονται όταν πρόκειται ένας πάροχος να παρέχονται υπηρεσίες πιστοποίησης σε κρατικές υπηρεσίες. Κάτι που διαπιστώσαμε από την συγκεκριμένη εξέταση είναι πάντως η διαφορά κουλτούρας που φαίνεται από τις διάφορες νομοθετικές προσπάθειες αλλά και τις διάφορες απαιτήσεις που θέτει η διαδικασία διαπίστευσης στις ‘χώρες’ που εξετάσαμε. Η διαφορά αυτή είναι κατά την γνώμη μας η πιο σημαντική αιτία, πιο σημαντική ακόμα και από τις διαφορές των νομικών συστημάτων, που δεν φαίνεται ακόμα εύκολη κάποια εφαρμόσιμη διεθνής πρωτοβουλία για ηλεκτρονικές υπογραφές. Η συνολική επικράτηση των ηλεκτρονικών υπογραφών είναι πάντως καθαρά θέμα κουλτούρας, που πιστεύουμε ότι θα έρθει με τον καιρό και όσο περισσότερες συναλλαγές εκτελούνται ηλεκτρονικά, καθώς όπως και να το δει κανείς η ψηφιακή υπογραφή, είναι τεχνολογικά ανώτερη και πιο ασφαλής από την ιδιόχειρη.

Τέλος, ασχοληθήκαμε με κάποια ανοικτά θέματα στον συγκεκριμένο τομέα, όπως για παράδειγμα η φύση της διαπίστευσης, η ρύθμιση της ευθύνης που προκύπτει από τις υπηρεσίες πιστοποίησης, καθώς επίσης. Επίσης δώσαμε την προσωπική μας άποψη στα θέματα τα οποία έχει θέσει για δημόσια διαβούλευση η ΕΕΤΤ, στα πλαίσια της εφαρμογής της ευρωπαϊκής οδηγίας στην Ελλάδα. Αποδείχτηκε έτσι πως η θεωρητική αναφόρα σε κάποια θέματα και η θεωρητική επίλυση κάποιων προβλημάτων είναι ένα σχετικά απλό θέμα όταν συγκριθεί με την πρακτική εφαρμογή τους, ιδιαίτερα σε τόσο μεγάλη κλίμακα και

γνωρίζοντας ότι θα έχει τόση επιρροή σε τόσα καθιερωμένα πράγματα.

Τώρα θα επιχειρήσουμε μία κριτική της όλης προσπάθειας. Λόγω του όγκου του συγκεκριμένου θέματος υπάρχουν πολλά πράγματα τα οποία θα μπορούσαν να είχαν γίνει και δεν έγιναν. Ένα από αυτά αφορά την δοκιμή στην πράξη λογισμικού το οποίο μπορεί να χρησιμοποιηθεί για την αρκετές υπηρεσίες ψηφιακών υπογραφών. Τόσο στο εμπόριο όσο και σε διάφορα open source projects υπάρχουν διαθέσιμες υλοποιήσεις παραδείγματος χάριν LDAP servers για την παροχή υπηρεσιών καταλόγου, ή λογισμικού δημιουργίας πιστοποιητικών. Κάτι τέτοιο θα έδινε μία πολύ καλή εμπειρία από την τεχνική πλευρά σχετικά με την πραγματικότητα και θα βοηθούσε περισσότερο στην κατανόηση των κινδύνων που συναντά κανείς σε ένα περιβάλλον αρχής πιστοποίησης. Βέβαια κάτι τέτοιο καλύπτει μόνο ένα τμήμα του συγκεκριμένου κυκλώματος και δεν θα έδινε καθόλου βοήθεια σε ότι αφορά για παράδειγμα για την κατανόηση της ιδιαίτερης κατάστασης του υπογράφοντα και του επαληθεύοντα. Σε κάθε περίπτωση πάντως θα ήταν κάτι ενδιαφέρον. Γενικότερα λοιπόν ένα μειονέκτημα της εργασίας ήταν ότι κινήθηκε μόνο σε θεωρητικό επίπεδο και δεν ασχολήθηκε καθόλου με κάποια υλοποίηση.

Ένα άλλο μειονέκτημα το οποίο διαπιστώσαμε είναι η υπερβολική επικέντρωση σε κάποια σημεία είτε στην ευρωπαϊκή οδηγία είτε γενικότερα στο ευρωπαϊκό πλαίσιο διαπίστευσης, σε δυσανάλογο βαθμό με άλλα πλαίσια όπως αυτά των ΗΠΑ, που είναι εξίσου σημαντικά. Πιστεύουμε επίσης ότι δεν αποφύγαμε σε ορισμένα σημεία λάθη και ασάφειες σε ό,τι αφορά νομικά θέματα. Γενικότερα, πάντως για την σωστή κάλυψη του συγκεκριμένου θέματος, απαιτούνται γνώσεις και εμπειρία από αρκετούς χώρους, παράγοντας που να εξηγεί τις όποιες ασάφειες.

Το πιο σημαντικό μειονέκτημα κατά την γνώμη μας πάντως είναι ότι δεν εξετάστηκαν σε τόσο βάθος άλλες προσεγγίσεις σχετικά με την υποδομή που θα υποστηρίξει τις ηλεκτρονικές υπογραφές, καθώς επικεντρωθήκαμε αποκλειστικά στην υλοποίηση μιας υποδομής δημοσίου κλειδιού η οποία βασίζεται στο X.509. Αυτό βέβαια προτείνεται από τα περισσότερα πρότυπα τα οποία εξετάσαμε και είναι αυτό το οποίο είναι γενικότερα αποδεκτό, από την αγορά. Σε ακαδημαϊκό επίπεδο βέβαια έχουν επισημανθεί αρκετές αδυναμίες του, τις οποίες εξετάσαμε. Αυτό που θα μπορούσε όμως να είχε γίνει θα ήταν να εξετάσουμε πώς οι συγκεκριμένες εναλλακτικές λύσεις θα μπορούσαν να συνδυαστούν με το υπάρχον νομικό και ρυθμιστικό πλαίσιο, το οποίο όπως έχει φανεί προτάθηκε έχοντας υπ΄όψη το X.509.

Στην εργασία αυτή προσπαθήσαμε γενικότερα να ξεπεράσουμε την υπερβολή που χαρακτηρίζει μεγάλο τμήμα της βιβλιογραφίας γύρω από τις ηλεκτρονικές υπογραφές, ότι δηλαδή έχει βρεθεί το ανάλογο της ιδιόχειρης και ότι όλα τα σχετικά προβλήματα έχουν λυθεί από την υποδομή δημοσίου κλειδιού. Όπως είδαμε κάτι τέτοιο δεν είναι αλήθεια, καθώς υπάρχει ένα κρίσιμο σημείο το οποίο αγνοείται από πολλούς. Η υπόθεση δηλαδή ότι το ιδιωτικό κλειδί βρίσκεται υπό την κατοχή και έλεγχο του νόμιμου ιδιοκτήτη. Κάτι τέτοιο κάθε άλλο παρά μικρή σημασία και είναι αυτό που προσπαθούν να διασφαλίσουν τα διάφορα πρότυπα. Το κατά πόσο αυτό θα επιτευχθεί εξαρτάται από πολλούς παράγοντες. Θα διαπιστωθεί πάντως με τον καιρό και με τον αριθμό των περιπτώσεων αμφισβητούμενων υπογραφών. Τέλος, αξίζει να παρατηρήσουμε το ότι τα θέματα που εξετάσαμε εδώ φέρνουν σε επαφή συστήματα με διαφορετικές αρχές

τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Έτσι παρατηρήσαμε την συνεργασία που αναγκάστηκε να υπάρχει μεταξύ του τεχνολογικού και του νομικού κόσμου. Αυτό δεν ισχύει μόνο για την φάση εφαρμογής τους. Ισχύει για όλη την πορεία που ακολουθεί την αρχική σύλληψη και την πειραματική υλοποίηση μιας νέας τεχνολογίας, εώς ότου αυτή εφαρμοστεί στο ευρύ κοινό και γίνει αφομοιωθεί. Στα πρώτα βήματα της εφαρμογής αυτής βρισκόμαστε σε ότι αφορά τις ηλεκτρονικές υπογραφές. Το αν θα ευδοκιμήσουν αυτά, εξαρτάται κυρίως από την αποδοχή που θα γνωρίσουν οι νέες τεχνολογίες κάτι που δεν εξαρτάται μόνο από αυτές καθ' αυτές, αλλά και από τον τρόπο υλοποίησης τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Εργασίες σε Επιστημονικά Περιοδικά / Συνέδρια

[Diffie, 1976] **W. Diffie and M. Hellman.** *New Directions in Cryptography.* IEEE Transactions on Information Theory, IT-22 (6), November 1976.

[Dumortier, 1999] **Jos Dumortier, P. Van Eecke,** *The European Draft Directive 1999/93/EC On A Community Framework For Electronic Signatures*, Computer Law And Security Report, Vol. 15, No. 2 1999, p. 106-112.

[Ellison, 2000] **Ellison Carl, Schneier Bruce,** *Ten Risks of PKI:what you're not told about Public Key Infrastructure*, Computer Security Journal, Vol. XVI, No. 1, 2000.

[Froomkin, 1996] **A.M. Froomkin**, *The Essential Role of Trusted Third Parties in Electronic Commerce*, Oregon Law Review 49, 1996.

[Kuner, 1999] **C.Kuner, A. MiedBrot**, *Written Signature Requirements and Electronic Authentication: A comparative perspective*, The EDI Law Review 2/3 1999, p. 143-154.

[Rivest, 1978] **R. L. Rivest, A. Shamir, and L. M. Adleman**. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,* Communications of the ACM, Vol. 21, No. 2, February 1978.

[Schneier, 1999] **Bruce Schneier, Adam Shostack**, *Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards*, USENIX Workshop on Smart Card Technology, USENIX Press, Οκτώβριος 1999.

Άρθρα

[Aalberts, 1999] **B. P. Aalberts, S. Van Der Hof,** *Digital Signatures Blindness: Analysis of legislative approaches towards electronic authentication*, Νοέμβριος 1999, Διαθέσιμο online: http://cwis.kub.nl/~frw/people/hof/ds-fr.htm

[ICRI, 1998] **Interdisciplinary Center For Law And Information Technology,** *The Legal Aspects of Digital Signatures Report*, Οκτώβριος 1998, Διαθέσιμο Online: http://www.law.kuleuven.ac.be/icri/projects/digisig_eng.htm

[ILPF, 2000] **International Law And Policy Forum,** *Survey Of International Electronic And Digital Signature Initiatives*. 2000, Διαθέσιμο online: http://www.ilpf.org/groups/survey.htm

[Polemi, 1997] **Polemi Despina,** *Biometric Techniques: Review And Evaluation Of Biometric Techniques For Identification And Authentication, Including An Appraisal Of The Areas Where They Are Most Applicable*, Institute Of Communication And Computer Systems, National Technical University Of Athens, Απρίλιος 1997.

[Schneier 1999a] **Bruce Schneier,** *Biometrics: Uses and Abuses*, Inside Risks 101, Communications Of the ACM, 42, 8 August 1999.

[Schneier, 2000] **Bruce Schneier,** *Why Digital Signatures are not Signatures*, Cryptogram Newsletter, Διαθέσιμο online: http://www.counterpane.com/crypto-gram-0011.html#1, Νοέμβριος 2000.

[SGgrit, 1997] **Γκρίτζαλης Σ., Γεωργιάδης Π**., *Ψηφιακές Υπογραφές: Διεθνής Εμπειρία – Τάσεις και Προοπτικές*, Οικονομικό Πανεπιστήμιο Αθηνών, 2001.

[JUEN, 1998] R R. Jueneman, R. J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 Jurimetrics Journal, Spring 1998.

Βιβλία

[Brands, 1999] **S. Brands,** *Rethinking Public Key Infrastructure And Digital Certificates*, PhD Thesis, 1999. Διαθέσιμο online:http://www.xs4all.nl/~brands/

[Ford, 2001] **Ford W. and Baum M**., *Secure Electronic Commerce 2nd Edition*, Prentice Hall, 2001.

[Schneier, 1996] **Schneier B**., *Applied Cryptography*, 2nd Edition, John Wiley & Sons, 1996.

[Turban, 2000] **Turban Efraim, Jan Lee, David King, H. Michael Chung**, *Electronic Commerce, A Managerial Perspective*, Prentice Hall, 2000.

Εγχειρίδια / Πανεπιστημιακές Παραδόσεις

[Gritzalis, 1998] **Γκρίτζαλης Δ., Μουλίνος Κ.** , Ασφάλεια στις Τεχνολογίες Πληροφοριών και Επικοινωνιών: Εννοιολογική Θεμελίωση - Σημειώσεις για το μάθημα Ασφάλεια Υπολογιστών και Δικτύων, Οικονομικό Πανεπιστήμιο Αθηνών, 1998.

[Gritzalis, 1998a] **Γκρίτζαλης Δ., Μουλίνος Κ.** Πρότυπα Πιστοποίησης και Αξιολόγησης Ασφάλειας Πληροφοριακών συστημάτων – Σημειώσεις για το μάθημα Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων, Οικονομικό Πανεπιστήμιο Αθηνών, 1998.

[Gritzalis, 1998b] **Γκρίτζαλης Δ., Τρύφωνας Θ.** Information Systems Security Policies - Σημειώσεις για το μάθημα Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων, Οικονομικό Πανεπιστήμιο Αθηνών, 1998.

[Gutman, 2001] **Peter Gutman,** *Cryptography Tutorial*, Διαθέσιμο online: http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html

Τεχνικά Πρότυπα

[CC, 1998] **International Standards Organisation (ISO)**, *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation*, Έκδοση 2.1, Νοέμβριος 1998.

[ECAG, 2000] **European Committee For Standardization, Information Society Standardization system (CEN / ISSS)**, *EESI Conformity Assessment Guideline*, Ref. ESV-54, 1.0, 15/11/2000**.** Διαθέσιμο online: http://www.eema.org/ecaf/ecag.pdf

[ETSI, 101 178T2] **European Telecommunications Standards Institute (ETSI),** *Policy requirements for certification authorities issuing public key certificates*, ETSI TS 101 456 V1.1.1 Δεκέμβριος 2000 Διαθέσιμο online: http://portal.etsi.org/sec/ts_101456v010101p.pdf

[ETSI, 101 456] **European Telecommunications Standards Institute (ETSI),** *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 12/2000. Διαθέσιμο online:http://portal.etsi.org/sec/ts_101456v010101p.pdf

[ETSI, 101 733] **European Telecommunications Standards Institute (ETSI),** *Electronic Signature Formats***,** ETSI ES 101 733 V1.2.2, Δεκέμβριος 2000, Διαθέσιμο online: http://portal.etsi.org/sec/ts_101733v010202p.pdf

[ETSI, 101 862] **European Telecommunications Standards Institute (ETSI)**, *Qualified certificate profile*, ETSI TS 101 862 V1.2.1 (2001-06). http://portal.etsi.org/sec/ts_101862v010201p.pdf

[ETSI, 101 903] **European Telecommunications Standards Institute (ETSI)**, *XML Advanced Electronic Signatures*, ETSI 101 903, V. 0.0.8 (draft) (2001-07), Διαθέσιμο online: http://portal.etsi.org/sec/STF178Task3FinalDraftTS.pdf

[ETSI, 10230] **European Telecommunications Standards Institute (ETSI),** *Provision Of Harmonised Trust Service Provider Status Information*, Draft, Δεκέμβριος 2001.

[ETSI, 178T1] **European Telecommunications Standards Institute (ETSI),** *Policy requirements for time stamping authorities*, ETSI draft 178T1, Ιούλιος 2001. http://portal.etsi.org/sec/STF178Task1FinalDraft.pdf

[FIPS 140-2, 2000] U.S. DEPARTMENT OF COMMERCE / National Institute Of Standards And Technology, *Security Requirements For Cryptographic Modules*, Μάιος 2001.

[FIPS 186-2, 2000] U.S. DEPARTMENT OF COMMERCE / National Institute Of Standards And Technology*, Digital Signature Standard (DSS)*, Ιανουάριος 2000

[FMEM, 2001] ***CEN/ISSS WS/E-SIGN*** *Explanatory Memorandum Area F CWA.*

[ITSEC, 1991] **Commission of the European Communities,** *Information Technology Security Evaluation Criteria, Brussels***,** Έκδοση 1.2 Ιούνιος 1991.

[PESV, 2000] **CEN/ISSS**, *Procedures for electronic signature verification, Version 1.0.2*, Δεκέμβριος 2000, http://www.eema.org/ecaf/pesv.pdf

[PKCS#1, 2001] **RSA Laboratories**, *PKCS #1 v2.1: RSA Cryptography Standard, Draft 2 — Ιανουάριος 2001*. Διαθέσιμο Online: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html

[PKCS#13, 2001] **RSA Laboratories,** *PKCS #13: Elliptic Curve Cryptography Standards, Overview and Proposa*l. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-13/index.html.

[PKCS#14, 2001] **RSA Laboratories,** *PKCS #14: Pseudo-Random Number Generation, Overview and*

Proposal. Διαθέσιμο Online: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-14/index.html

[PKCS#6, 1993] **RSA Laboratories**, *PKCS #6: Extended-Certificate Syntax Standard, Version 1.5, Νοέμβριος 1993*. Διαθέσιμο Online: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-6/index.html

[PPEU, 2001] **Herbert Leitold,** *Protection Profiles Supporting the EU Directive*, 2nd International Common Criteria Conference, Brighton July, 2001

[RFC 1777, 1995] **W. Yeong, T. Howes, S. Kille,** *RFC 1777***:** *Lightweight Directory Access Protocol.* Διαθέσιμο online: http://www.ietf.org/rfc/rfc1777.txt

[RFC 2251, 1997] **M. Wahl, T. Howes, S. Kille** *RFC 2251: Lightweight Directory Access Protocol (v3), Δεκέμβριος 1997*. Διαθέσιμο online: http://www.ietf.org/rfc/rfc2251.txt

[RFC 2459, 1999] **R. Housley, W. Ford, W. Polk, D. Solo,** *RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Ιανουάριος 1999*. Διαθέσιμο online: http://www.ietf.org/rfc/rfc2459.txt

[RFC 2527, 1999] **Chochani S., Ford W.,** *RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* Διαθέσιμο online: http://www.ietf.org/rfc/rfc2527.txt

[RFC 2585, 1999] **R. Housley and P. Hoffman,** *RFC 2585: Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*, Μάιος 1999. Διαθέσιμο online: http://www.ietf.org/rfc/rfc2585.txt

[RFC 2587, 1999] **Boeyen S., Howes T., Richard P., RFC 2587**: *Internet X.509 Public Key Infrastructure LDAPv2 Schema, Ιούνιος 1999*. Διαθέσιμο online: http://www.ietf.org/rfc/rfc2587.txt

[RFC 3039, 2001] **Santesson S., Polk W., Barzin P., Nystrom M., RFC 3039**: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*. Ιανουάριος 2001. Διαθέσιμο online: http://www.ietf.org/rfc/rfc3039.txt

[RFC 3161, 2001] **Adams C., Cain P., Pinkas D., Zuccherato R., RFC 3161**:*Internet X.509 Public Key InfrastructureTime-Stamp Protocol (TSP)*, Αύγουστος 2001, Διαθέσιμο online: http://www.ietf.org/rfc/rfc3161.

[SSCD, 2001] **CEN/ISSS, *WS/E-Sign Workshop Agreement Group F: Secure Signature Creation Devices*,** Νοέμβριος 2001.

[SSCS, 2000] **CEN/ISSS,** *Security Requirements For Signature Creation Systems*, v3.0, 2000. Διαθέσιμο online: http://www.eema.org/ecaf/srscs.pdf

[TSMC, 2000] **CEN/ISSS**, *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*, v. 0.5, Σεπτέμβριος 2000. Διαθέσιμο online: http://www.eema.org/ecaf/srscs.pdf

[Verisign, 1997] **Verisign Certification Practice Statement,** Διαθέσιμο online: http://www.verisign.com/repository/CPS/intro.html

[TCSEC, 1985] **U.S. Department of Defense**, *Trusted Computer System Evaluation Criteria*, έκδοση 2. Δεκέμβριος 1985.

Νομικά - Ρυθμιστικά Κείμενα

[ABA, 1996] **American Bar Association, Information Security Committee**, *Digital Signature Guidelines*: *Legal Infrastructure for Certification Authorities and Secure Electronic Commerce,* Αύγουστος 1996.

[ABA, 2001] **American Bar Association, Information Security Committee**, *PKI Assessment Guidelines*: *Guidelines To Help Assess And Facilitate Interoperable, Trustworthy Public Key Infrastructures*, (Public Draft For Comment v0.3), Ιούνιος 2001.

[CAN1,2000] **Treasury Board Secretariat of Canada**, *GOCPKI Cross - Certification Methodology and Criteria,* Έκδοση 1.0, Απρίλιος 2000. Διαθέσιμο Online: http://www.cio-dpi.gc.ca/pki-icp

[CAN2,2001] **Treasury Board Secretariat of Canada**, *GOCPKI FAQ*, Διαθέσιμο online: http://www.cio-dpi.gc.ca/pki-icp/gocpki/faq/faq_e.asp.

[CAN3,1998] **Government Of Canada Communications Security Establishment**, *GOCPKI PKI White Paper*, Φεβρουάριος 1998.

[CAN4, 2001] **Treasury Board Secretariat of Canada**, *Digital Signature and Confidentiality*

Certificate Policies, Διαθέσιμο Online: http://www.cio-dpi.gc.ca/common/doctb.asp

[CDMC, 2000] **Ευρωπαϊκή Επιτροπή**, *Κοινή απόφαση της 6 Νοεμβρίου 2000, σχετικά με τα ελάχιστα κριτήρια που πρέπει να ληφθούν υπ'όψη κατά τον ορισμό φορέων για την τήρηση του Άρθρου 3(4) της οδηγίας 1999/93/ΕΚ.*

[DTI, 2001] **United Kingdom Department Of Trade And Industry**, *'Consultation on EC Directive 1999/93/EK of the European Parliament And Council On A Community Framework For Electronic Signatures'*, Μάρτιος 2001, Διαθέσιμο online:

[EDCF, 1999] **Ευρωπαϊκή Επιτροπή**, *Οδηγία 1999/93/ΕΚ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές.*

[EESSI ,1999] European Electronic Signature Standardization Initiative (EESSI), *Final Report of the EESSI Expert Team*, Ιούλιος 1999.

[EESSI, 2000] **ICTSB**, European Electronic Signature Standardization Initiative (EESSI): Status & International Issues, EESSI Workshop, Barcelona, Σεπτέμβριος 2000.

[EESSI, 2001] **European Electronic Signature Standardization Initiative (EESSI),** *Goals, Structures, Achievements And Future Activities* AG INDI Colloquium – Οκτώβριος 2001, Claude Boulle, Chair EESSI, Bull.

[FPKI, 2000] **US Federal PKI Steering Committee**, '*X.509 Certificate Policy For The Federal Bridge Certification Authority'*, Δεκέμβριος 2000.

[NIST, 2000] **National Institute Of Standards And Technology**, '*Federal Agency Use Of Public Key Technology for Digital Signatures And Authentication*', NIST Special Publication 800-25, Οκτώβριος 2000.

[NOIE, 2001] **The National Office for the Information Economy (NOIE)**, *Changes to Gatekeeper, Αυστραλία*, 21 Μαρτίου 2001.

[NOIE, 2001a] **The National Office for the Information Economy (NOIE)**, *Gatekeeper Frequently Asked Questions*, Διαθέσιμο online: http://www.govonline.gov.au/projects/publickey/faqs.htm#1

[OGIT, 1998] **Office Of Government Information Technology (OGIT),** *Gatekeeper: A strategy for public key technology use in the government*, ISBN: 0642 32032 2, Australia, Μάιος 1998.

[SIGG, 1997] **Government of the Federal Republic of Germany,** *Digital Signature Law (SigG)*, Ιούνιος 1997. Διαθέσιμο online: http://www.kuner.com/digsig4.htm

[SIGGa, 1999] **Government of the Federal Republic of Germany,** *Remarks of the German Government On the EU Draft Directive concerning electronic and digital signatures.* Απρίλιος 1998, http://www.kuner.com/gov_ger_eu-draft.htm

[SIGGc, 2000] **Government of the Federal Republic of Germany,** *Proposed Amendments To The German Digital Signature Law*. Αύγουστος 2000, http://www.kuner.com/sig_august_16.htm

[SIGV, 1997] **Government of the Federal Republic of Germany,** *Digital Signature Ordinance (SIGV)*, Ιούλιος 1997. Διαθέσιμο online: http://www.kuner.com/verord04.htm

[TSCH, 2001] **tScheme**, Digest Of Protection Profiles, Διαθέσιμο Online: http://www.tscheme.org/library/digest.html.

[UNCITRAL, 1996] **United Nations Commission On International Trade Law,** *Uncitral Model Law On Electronic Commerces*, 2001. Διαθέσιμο online: http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm

[UNCITRAL, 2001] **United Nations Commission On International Trade Law,** *Uncitral Model Law On Electronic Signatures*, 2001. Διαθέσιμο online: http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf

[ΕΕΤΤ, 2001] **Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),** '*Πρόσκληση Υποβολής Απόψεων σχετικά με τις ηλεκτρονικές υπογραφές σε θέματα που άπτονται της Παροχής Υπηρεσιών Πιστοποίησης και της Εθελοντικής Διαπίστευσης*', Νοέμβριος 2001, Διαθέσιμο Online : http://www.eett.gr/gr_pages/telec/esign/esigncons.pdf

[ΠΔΗΥ, 2001] **Προεδρικό Διάταγμα 150/2001**, Προσαρμογή στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, Ιούνιος 2001.

ΠΑΡΑΡΤΗΜΑ 1: ΠΕΡΙΛΗΨΗ

Η εργασία ασχολήθηκε με όλη την έκταση του φαινομένου των ηλεκτρονικών υπογραφών, εξετάζοντας τόσο τις τεχνικές, όσο και τις νομικές πτυχές του. Η διπλή φύση του συγκεκριμένου θέματος, παρουσιάζει τόσο ενδιαφέρον, όσο και δυσκολίες καθώς απασχολεί δύο παραδοσιακά ετερογενείς και ασύμβατους χώρους, κάθε ένας από τους οποίους πρέπει να αποκτήσει γνώση ιδιαίτερων λεπτομερειών του άλλου.

Οι ηλεκτρονικές υπογραφές, λοιπόν είναι άμεση συνέπεια της ανάπτυξης των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ). Πιο συγκεκριμένα η ευρεία εξάπλωση των δημοσίων δικτύων δεδομένων, όπως το Internet, έχει καταστήσει δυνατή την διεξαγωγή ηλεκτρονικών συναλλαγών με ιδιαίτερα πλεονεκτήματα σε ό,τι αφορά το κόστος, την ταχύτητα και την αποτελεσματικότητα. Εννοιολογικά, οι ηλεκτρονικές συναλλαγές πάνω από ανοικτά δίκτυα είναι ισοδύναμες με τις παραδοσιακές. Για παράδειγμα, η αγορά από ένα ηλεκτρονικό κατάστημα έχει τα ίδια αποτελέσματα με μία παραδοσιακή αγορά. Ο αγοραστής γίνεται κάτοχος των αγαθών, ενώ ο πωλητής λαμβάνει το αντίτιμο. Τόσο όμως η ηλεκτρονική και μη απτή φύση των ανταλλασσόμενων δεδομένων, όσο και η περιορισμένη ασφάλεια στα δίκτυα μέσω των οποίων αυτά διακινούνται, έχουν αλλοιώσει την αναπαράσταση των συναλλαγών, με αποτέλεσμα την απώλεια των παραδοσιακών ιδιοτήτων της εγκυρότητας και της εφαρμοσιμότητας. Με τον όρο εγκυρότητα εννοούμε την ικανοποίηση των τυπικών ιδιοτήτων που θέτει συνήθως ο νόμος, ώστε μία συναλλαγή να θεωρείται αποδεκτή. Με τον όρο εφαρμοσιμότητα εννοούμε την ύπαρξη των κατά περίπτωση απαιτούμενων τεκμηρίων που θα επιτρέπουν στην συναλλαγή να ανταπεξέλθει τις όποιες αμφισβητήσεις. Ένας παραδοσιακά χρησιμοποιούμενος μηχανισμός που βοηθά στην ικανοποίηση των παραπάνω ιδιοτήτων και σχετίζεται με την αναπαράσταση και όχι την ουσία μιας συναλλαγής, είναι αυτός της υπογραφής. Παραδοσιακά, η υπογραφή εξυπηρετεί τους εξής στόχους: Αφενός την αυθεντικοποίηση του συγγραφέα ενός κειμένου, αφ' έτερου την απόδοση της έννοιας της τέλεσης (ceremony), ότι δηλαδή η πράξη στην οποία θα προβούν τα συναλλασσόμενα μέρη είναι δεσμευτική και τέλος την παροχή μιας ένδειξης ότι υπάρχει αποδοχή των περιεχομένων του. Για την διατήρηση των πλεονεκτημάτων που φέρει η ηλεκτρονική υλοποίηση μιας συναλλαγής, απαιτείται η μεταφορά της υπογραφής στο ηλεκτρονικό περιβάλλον, με παράλληλη διατήρηση της σημασιολογίας που αυτή έχει αποκτήσει μετά από τόσους αιώνες εφαρμογής.

Αρχικά, ασχοληθήκαμε με το θεωρητικό υπόβαθρο των ηλεκτρονικών υπογραφών, το οποίο παρέχεται κυρίως από την Κρυπτογραφία και την Ασφάλεια των Πληροφοριών. Το συμπέρασμα που προέκυψε είναι ότι καμία από τις προτάσεις που έχουν ως τώρα γίνει, δεν μπορεί να μεταφέρει με επιτυχία στο ηλεκτρονικό περιβάλλον την έννοια της υπογραφής. Οι περισσότερες παρέχουν λύσεις σε ότι αφορά το πρόβλημα της ανωνυμίας που παρατηρείται στο Διαδίκτυο. Οι πιο σημαντικές τεχνολογίες στον συγκεκριμένο τομέα είναι οι ψηφιακές υπογραφές και οι διάφορες βιομετρικές τεχνολογίες. Οι ψηφιακές υπογραφές υλοποιούνται με ασύμμετρα κρυπτοσυστήματα, εξασφαλίζουν την ακεραιότητα του

μηνύματος και παρέχουν μία αρκετά σαφή ένδειξη για την ταυτότητα του αποστολέα. Οι βιομετρικές τεχνολογίες βασίζουν την αυθεντικοποίηση σε ένα σύνολο μοναδικών φυσικών χαρακτηριστικών. Έχουν όμως αρκετά μειονεκτήματα, όπως για παράδειγμα το σημαντικό περιθώριο σφάλματος των μετρήσεων, την μη επαρκή θεωρητική θεμελίωση, την έλλειψη διαχειριστικών λειτουργιών, καθώς επίσης και την μειωμένη αποδοχή που συναντούν. Επιπλέον δεν μπορούν να εγγυηθούν την ακεραιότητα του μηνύματος. Για τον τελευταίο αυτό λόγο κυρίαρχη τεχνολογία στο συγκεκριμένο τομέα αποτελούν οι ψηφιακές υπογραφές, καθώς με την διατήρηση της ακεραιότητας βοηθούν στην εξίσωση των ηλεκτρονικών εγγράφων με τα συμβατικά. Επιπλέον με ένα σύνολο παραδοχών σχετικά με την κατοχή και έλεγχο του ιδιωτικού κλειδιού κρυπτογράφησης μπορούν να αυθεντικοποιήσουν τον αποστολέα ενός μηνύματος. Η αυθεντικοποίηση αυτή μπορεί καταχρηστικά να θεωρηθεί ως υπογραφή, σε περίπτωση για παράδειγμα που τα δεδομένα στα οποία χρησιμοποιείται έχουν μεγάλη χρονική διάρκεια. Τόσο για την αποτελεσματική υλοποίηση της τεχνολογίας των ψηφιακών υπογραφών όσο και για την διατήρηση της σημασιολογίας της υπογραφής, απαιτείται η ύπαρξη μιας ολόκληρης υποστηρικτικής υποδομής. Συμπερασματικά εδώ, δεν θα ήταν υπερβολή να ισχυριστούμε ότι ο όρος ψηφιακή υπογραφή (καθ' αυτός) αποτελεί μία ατυχής ιστορική συγκυρία, η οποία έλαβε μεγάλες διαστάσεις από την υπερβολή που διακρίνει συνήθως την περιγραφή των δυνατοτήτων της τεχνολογίας. Ίσως αν είχε επιλεγεί μια ονομασία όπως ψηφιακός φάκελος ή κάτι παρόμοιο, πιστεύουμε ότι αρκετά από τα θέματα τα οποία εξετάζουμε εδώ δεν θα ανέκυπταν.

Η συνοδευτική αυτή υποδομή (υποδομή δημοσίου κλειδιού), ως τελικό στόχο έχει την αντιστοίχιση της ταυτότητας μιας οντότητας από τον φυσικό στον ηλεκτρονικό κόσμο. Κεντρικό συστατικό της είναι το ψηφιακό πιστοποιητικό, το οποίο εκδίδεται από μία νέα μορφή ηλεκτρονικού ενδιαμέσου, που είναι γνωστός ως *Αρχή Πιστοποίησης*, *Έμπιστη Τρίτη Οντότητα* ή πιο πρόσφατα ως *Πάροχος Υπηρεσιών Πιστοποίησης*. Αυτή είναι υπεύθυνη εκτός από την έκδοση, και για άλλες σχετικές με τα ψηφιακά πιστοποιητικά υπηρεσίες, όπως για παράδειγμα την διατήρηση ενός καταλόγου ανάκτησης τους, την επαλήθευση της ταυτότητας των υποκειμένων των πιστοποιητικών, την διαχείριση της ανάκλησης των πιστοποιητικών και της ενημέρωσης για την κατάσταση τους ανά πάσα στιγμή. Επιπλέον μπορεί να είναι υπεύθυνη για την δημιουργία κρυπτογραφικών κλειδιών και την παροχή και αρχικοποίηση διατάξεων δημιουργίας ηλεκτρονικών υπογραφών. Μπορεί όμως να λάβει και πιο εκτεταμένο ρόλο, πέρα από τις ηλεκτρονικές υπογραφές με την παροχή υπηρεσιών χρονοσήμανσης και τήρησης ηλεκτρονικών αρχείων. Οι υπηρεσίες αυτές δεν είναι τίποτα πρωτοποριακό στην σύλληψη τους. Έχουν μοντελοποιηθεί με βάση αντίστοιχες πρακτικές του φυσικού κόσμου, οι οποίες έχουν ενσωματωθεί τόσο σε αυτόν, ώστε να μην μας απασχολεί πλέον η ασφάλεια τους. Εμείς εξετάσαμε τα πιο σημαντικά πρότυπα (X.509) και πρωτόκολλα (LDAP, OCSP) για τα ψηφιακά πιστοποιητικά και τις υπηρεσίες μιας αρχής πιστοποίησης. Το συμπέρασμα στο οποίο οδηγηθήκαμε εδώ, είναι ότι το ίδιο το σύστημα το οποίο ως σκοπό είχε την εξάλειψη ορισμένων μειονεκτημάτων της τεχνολογίας, εισήγαγε

από μόνο του νέα προβλήματα.

Για την αντιμετώπιση των νέων αυτών προβλημάτων απαιτείται η αλλαγή οπτικής γωνίας και η παρέμβαση από ένα ανώτερο επίπεδο. Σήμερα, το ανώτερο αυτό επίπεδο είναι οι διάφορες νομικές και ρυθμιστικές προσπάθειες οι οποίες αναγνωρίζουν ουσιαστικά τις ηλεκτρονικές υπογραφές, και παρέχουν (μη τεχνολογικές κατά βάση) λύσεις για τα όποια προβλήματα. Το ανώτερο αυτό επίπεδο όμως δεν ήταν πάντοτε παρόν. Αρχικά η παραπάνω ρύθμιση γινόταν από τις διάφορες με τα οποία οι ίδιες οι αρχές πιστοποίησης ρύθμιζαν τις σχέσεις με τους συνδρομητές τους και τους υπόλοιπους χρήστες των υπηρεσιών τους. Αντιπροσωπευτικά τέτοιες πρακτικές εκφράζονται με την η πολιτική πιστοποίησης και τη δήλωση πρακτικών πιστοποίησης. Η πολιτική πιστοποίησης θέτει απαιτήσεις για θέματα όπως την επιτρεπτή χρήση πιστοποιητικών, την αυθεντικοποίηση των υποκειμένων καθώς επίσης και απαιτήσεις αξιοπιστίας και ασφάλειας των χρησιμοποιούμενων συστημάτων. Προδιαγράφει επίσης τις υποχρεώσεις των συνδρομητών και τις εγγυήσεις που δίνει η αρχή πιστοποίησης. Η δήλωση πρακτικών πιστοποίησης περιγράφει με λεπτομέρεια την υλοποίηση των παραπάνω απαιτήσεων. Τα παραπάνω κείμενα έχουν και άμεσο τεχνικό αντίκτυπο καθώς αναφορές τους περιλαμβάνονται σε κάθε πιστοποιητικό, και όπως συμβαίνει συνήθως χρήση του σημαίνει και αποδοχή τους. Στην σύνταξη τους, είχε δοθεί ιδιαίτερη βαρύτητα, έτσι ώστε να αποφύγουν οι αρχές πιστοποίησης όσο περισσότερη από την νομική ευθύνη συμπεριλαμβανόταν στην άσκηση της δραστηριότητας τους. Αν και αυτή η πρακτική δεν φαίνεται αρκετά δίκαια, ήταν απαραίτητη για την αρχική επιβίωση τους. Βέβαια δεν βοηθούσε και τόσο στην διάδοση των υπηρεσιών πιστοποίησης.

Η νομική και ρυθμιστική παρέμβαση που συνέβη μεταγενέστερα, σε αρκετές περιπτώσεις διατήρησε τα παραπάνω στοιχεία, ενώ σε άλλες προέβη σε σημαντικές αλλαγές. Τυπικά εισήγαγε δύο επιπλέον οντότητες στο κλασικό κύκλωμα των ηλεκτρονικών υπογραφών, τον επόπτη και τον ελεγκτή. Οι λειτουργίες που επιτελούν είναι τρεις. Ο επόπτης τυπικά θέτει κάποιες πολιτικές οι οποίες σχετίζονται με τις απαιτήσεις ασφαλείας μέσα σε μία υποδομή δημοσίου κλειδιού και εγκρίνει τους ελεγκτές. Οι τελευταίοι ελέγχουν την συμμόρφωση της αρχής πιστοποίησης με τεχνικά και διαχειριστικά πρότυπα, τα οποία συνεπάγονται της πολιτικής. Τα πρότυπα αυτά μπορεί να είναι είτε κλασικά πρότυπα ασφαλείας πληροφοριακών συστημάτων (όπως για παράδειγμα TCSEC, ITSEC, Common Criteria, FIPS PUB 140-2) ή και πρότυπα τα οποία απευθύνονται συγκεκριμένα στις υπηρεσίες των αρχών πιστοποίησης. Εμείς εξετάσαμε πρότυπα και των δύο παραπάνω κατηγοριών. Με βάση αυτά μοντελοποίησαμε τις απαιτήσεις ασφαλείας για όλες τις υπηρεσίες μιας αρχής πιστοποίησης που προαναφέραμε σε τεχνικό, διοικητικό και λειτουργικό επίπεδο. Επιπλέον εξετάσαμε πρότυπα για την μορφοποίηση των ηλεκτρονικών υπογραφών, έτσι ώστε να υποστηρίζουν επαλήθευση σε μελλοντικό χρόνο και να παρέχουν στοιχεία για επίλυση των όποιων διαφορών προκύψουν. Για να είναι κάτι τέτοιο δυνατό πρέπει μέσα σε κάθε ηλεκτρονική υπογραφή να προστίθεται με κάποιον τρόπο ένα στιγμιότυπο ολόκληρης της υποδομής δημοσίου κλειδιού, όπως αυτή ήταν την στιγμή της υπογραφής ή της πρώτης επαλήθευσης της. Ακόμα

ασχοληθήκαμε με τις συσκευές που θα χρησιμοποιούνται καθημερινά για την παραγωγή και επαλήθευση ηλεκτρονικών υπογραφών. Με βάση την τρέχουσα προτυποποίηση στον συγκεκριμένο τομέα, μοντελοποιήσαμε τις διατάξεις και το περιβάλλον δημιουργίας και επαλήθευσης υπογραφής. Φάνηκαν έτσι συγκεκριμένες απαιτήσεις ασφαλείας, για τις οποίες αναφέραμε πώς θα μπορούσαν να ικανοποιηθούν.

Επιπλέον ασχοληθήκαμε με τις πιο σημαντικές ρυθμιστικές προσπάθειες σε διεθνές επίπεδο, αρκετές από τις οποίες έχουν εμφανιστεί από το 1996, ξεκινώντας από διεθνείς οργανισμούς όπως π.χ. ο ABA, η επιτροπή του ΟΗΕ για το διεθνές εμπόριο (UNCITRAL) και καταλήγοντας στις νομικές προσπάθειες των πιο ανεπτυγμένων χωρών (ΗΠΑ, Ευρωπαϊκή Ένωση, Μ. Βρετανία, Γερμανία). Από αυτές διαπιστώσαμε ότι η προαναφερθείσα παρέμβαση γίνεται σε τρία επίπεδα:

- Νομική Ισχύς Ηλεκτρονικών Υπογραφών.
- Πλαίσιο για την Λειτουργία της Υποδομής Δημοσίου Κλειδιού.
- Ρυθμιστικό Πλαίσιο για την Λειτουργία των Αρχών Πιστοποίησης.

Οι διάφορες προσεγγίσεις που εξετάσαμε παρουσιάζουν σημαντικές αποκλίσεις για κάθε ένα από τα επίπεδα αυτά. Συγκεκριμένα σε ότι αφορά την αναγνώριση και την νομική ισχύ των ηλεκτρονικών υπογραφών υπάρχουν 3 κυρίαρχες τάσεις. Η πρώτη θέλει την θεσμοθέτηση υπέρ της τεχνολογίας ψηφιακών υπογραφών συγκεκριμένα, με το επιχείρημα του ότι για αυτήν έχει υπάρξει σημαντική έρευνα και πειραματισμός εδώ και αρκετά χρόνια, είναι γνωστές οι αδυναμίες της και κατά συνέπεια μπορεί να εφαρμοστεί ένα σαφές νομικό πλαίσιο το οποίο θα δίνει συγκεκριμένες λύσεις στα τεχνολογικά προβλήματα. Χαρακτηριστικό παράδειγμα εδώ είναι η προσέγγιση την οποία έχει ακολουθήσει η Γερμανία, όπου αυτή η ιδέα έχει τραβηχτεί στα άκρα, όπως θα δούμε στην συνέχεια. Η δεύτερη θέλοντας να αφήσει περισσότερο χώρο για νέες τεχνολογίες, κινείται σε δύο επίπεδα. Στο πρώτο αποδέχεται γενικά τις ηλεκτρονικές υπογραφές, ανεξάρτητα από τα χαρακτηριστικά που διαθέτουν και την τεχνολογία με την οποία υλοποιούνται. Στο δεύτερο επίπεδο όμως, προδιαγράφει συγκεκριμένες ιδιότητες που θα πρέπει να έχει μία μέθοδος ηλεκτρονικής υπογραφής έτσι ώστε να εξομοιωθεί με μία ιδιόχειρη ή έστω να απολαμβάνει κάποια αυξημένη νομική ισχύ. Αντιπροσωπευτικό παράδειγμα εδώ αποτελεί η Ευρωπαϊκή Ένωση. Η τρίτη προσέγγιση αποφεύγει την θεσμοθέτηση λεπτομερών προτύπων και αφήνει την αγορά να αποφασίσει για το ποιες είναι οι ατέλειες εκείνες όπου πρέπει να υπάρξει νομική ρύθμιση. Από την εξέταση των πλαισίων αυτών έγινε φανερό, ότι μία από τις πιο σημαντικές αιτίες για τις διαφοροποιήσεις αυτές αποτελεί το ήδη υπάρχον νομικό πλαίσιο, το οποίο αντανακλά τις απαιτήσεις αναπαράστασης που υπάρχουν για τις διάφορες συναλλαγές. Αρκετά διαφορετική αντίληψη παρατηρείται λοιπόν σε χώρες με αστικό δίκαιο (civil law) και σε χώρες με εθιμικό δίκαιο (common law). Παραδοσιακά στις τελευταίες, δίνεται περισσότερη έμφαση στην πρόθεση του υπογράφοντα να δεσμευθεί από την συγκεκριμένη πράξη της υπογραφής. Έτσι και ένα απλό σημάδι, επιτελεί τον σκοπό του. Αντίθετα στις χώρες αστικού κώδικα, περισσότερη σημασία δίνεται στην ασφάλεια της τεχνικής της υπογραφής (δηλαδή στην δυσκολία

πλαστογράφησης). Για τον σκοπό αυτό οι τελευταίες είναι γενικά υπέρ της τεχνολογικά εξειδικευμένης προσέγγισης, ενώ οι δεύτερες κλείνουν περισσότερο προς την τεχνολογικά ουδέτερη προσέγγιση.

Σε ό,τι αφορά το πλαίσιο για την λειτουργία της υποδομής δημοσίου κλειδιού, παρατηρήσαμε σύμπλευση σε διεθνές επίπεδο σε ό,τι αφορά τις απαιτήσεις ασφαλείας και τα τεχνικά πρότυπα. Αυτό κατά την γνώμη μας οφείλεται στο γεγονός ότι όλες οι προσπάθειες για την λειτουργία κάποιας υποδομής δημοσίου κλειδιού, έχουν κοινές ρίζες στο πρότυπο X.509 αλλά στην επιτυχία των προτύπων της IETF, τα οποία μετέφεραν το συγκεκριμένο περιβάλλον στο Διαδίκτυο. Ένα παράδοξο το οποίο φάνηκε και αξίζει να αναφερθεί αφορά το γεγονός ότι σε κάποιες από τις προσπάθειες που είδαμε (όπως για παράδειγμα στην Γερμανία) έγινε προσπάθεια προδιαγραφής της υποδομής δημοσίου κλειδιού σε τεχνικό επίπεδο, χωρίς όμως να υπάρξει η απονομή κάποιας ειδικής μεταχείρισης στις ηλεκτρονικές υπογραφές.

Η ρύθμιση της λειτουργίας των αρχών πιστοποίησης είναι το επίπεδο στο οποίο παρατηρούμε τις μεγαλύτερες διεθνείς αποκλίσεις. Κεντρική έννοια εδώ αποτελεί η διαπίστευση, η οποία μπορεί να οριστεί ως το αποτέλεσμα μίας διαδικασίας αποτίμησης των διοικητικών, λειτουργικών και τεχνικών διαδικασιών / συστημάτων μιας έμπιστης τρίτης οντότητας, στην συγκεκριμένη περίπτωση, η οποία *ενδεχομένως* συνοδεύεται με κάποια αδειοδότηση ή νομική αναγνώριση των υπηρεσιών που παρέχονται από τον συγκεκριμένο οργανισμό. Η διαπίστευση αποτελεί και ένα μέσο με το οποίο μπορεί να ρυθμιστεί η αγορά των ηλεκτρονικών υπογραφών. Επιπλέον έγινε φανερό ότι με τα τρέχοντα τεχνολογικά δεδομένα η διαπίστευση είναι δυνατή μόνο σε περίπτωση υποδομής δημοσίου κλειδιού. Επιπλέον η χρήση της ή όχι, σχετίζεται με το αν υπάρχει διάθεση για την ρύθμιση της συγκεκριμένης αγοράς. Σε ορισμένες περιπτώσεις, όπως για παράδειγμα στις ΗΠΑ, διαπίστευση, ή κάτι ανάλογο, υπάρχει μόνο όταν πρόκειται να διασυνδεθεί η υποδομή μίας αρχής πιστοποίησης με την υποδομή κάποιας κρατικής υπηρεσίας. Η διαπίστευση αφορά κυρίως τεχνική συμβατότητα, δεν περιορίζεται όμως μόνο σε επίπεδο π.χ. διαλειτουργικότητας πρωτοκόλλων, αλλά μέσω της πολιτικής πιστοποίησης και στις εσωτερικές διαδικασίες μιας αρχής πιστοποίησης. Δεν υπάρχει παρ' όλα αυτά καμία προσπάθεια ρύθμισης της αγοράς των υπηρεσιών πιστοποίησης.

Αντίθετα, άλλες προσπάθειες, όπως για παράδειγμα η οδηγία της Ευρωπαϊκής Επιτροπής προσπαθούν να θέσουν κάποιους γενικούς κανόνες οι οποίοι θα στοχεύουν τόσο στην προώθηση των συγκεκριμένων υπηρεσιών στο ευρύ κοινό, όσο και στην ανάπτυξη της αγοράς των υπηρεσιών πιστοποίησης. Θέτουν έτσι για παράδειγμα την ελάχιστη ευθύνη την οποία θα αντιμετωπίζουν οι αρχές πιστοποίησης για τα περιεχόμενα των πιστοποιητικών αλλά και για τις υπόλοιπες σχετικές υπηρεσίες που θα παρέχουν. Γενικότερα η Ευρωπαϊκή προσέγγιση προς τις ηλεκτρονικές υπογραφές όπως αυτή εκφράζεται μέσω της οδηγίας του 2000, απασχόλησε πάρα πολύ την εργασία. Αυτό δεν συνέβη μόνο εξαιτίας της ειδικής σημασίας που αυτή έχει για όλα τα μέλη της Ευρωπαϊκής Ένωσης. Η συγκεκριμένη οδηγία είναι το πρώτο διεθνές κείμενο, το οποίο θα συμπεριληφθεί στο εθνικό δίκαιο διαφορετικών χωρών. Διαφέρει δηλαδή από τις υπόλοιπες διεθνείς προσπάθειες, στο ότι δεν δίνει απλώς συστάσεις,

αλλά θα εφαρμοστεί. Ένα από τα θέματα στα οποία επικεντρωθήκαμε, ήταν η αντιστοίχιση των όσων απαιτήσεων αναφέρονται εκεί σε πιο τεχνικό (και πρακτικό) μέσω των διαφόρων προτύπων και η απάντηση στο ερώτημα με ποια πρακτικά κριτήρια θα μπορούσε να γίνει η διαπίστευση μίας αρχής πιστοποίησης κατά την οδηγία. Σίγουρα λοιπόν θα πρέπει να πληροί τις προϋποθέσεις του παραρτήματος 1 για τα περιεχόμενα των πιστοποιητικών, του παραρτήματος 2 για την λειτουργία της και να χρησιμοποιεί ασφαλείς διατάξεις για την υπογραφή των πιστοποιητικών, παρέχοντας δηλαδή αναγνωρισμένες υπογραφές.

Παράλληλα με την οδηγία ασχοληθήκαμε και με τον τρόπο με τον οποίο αντιμετώπισαν το συγκεκριμένο θέμα μεμονωμένες ευρωπαϊκές χώρες, όπως για παράδειγμα η Μ. Βρετανία και η Γερμανία, που βρίσκονται στα δύο άκρα στο συγκεκριμένο θέμα. Επίσης ασχοληθήκαμε με τις εξελίξεις στο συγκεκριμένο θέμα στην Ελλάδα, όπου η οδηγία καθυστερημένα θεσμοθετήθηκε με προεδρικό διάταγμα, και όπου έχει ξεκινήσει δημόσια διαβούλευση σχετικά με τις ηλεκτρονικές υπογραφές και την διαπίστευση, στην όποια προσπαθήσαμε να δώσουμε τεκμηριωμένες απαντήσεις με βάση τα όσα θεωρητικά είχαμε αναπτύξει νωρίτερα.

Κλείνοντας αρκεί να πούμε, ότι η διαπίστευση αν και ξεκίνησε ως ένα μέσο για την επίλυση τεχνολογικών ατελειών της υποδομής δημοσίου κλειδιού εξελίσσεται σήμερα ως το μέσο με το οποίο θα ρυθμιστεί η αγορά των υπηρεσιών πιστοποίησης. Το παραπάνω συμπέρασμα αφορά κυρίως την τεχνολογικά εξειδικευμένη προσέγγιση αναμένεται όμως να επεκταθεί και στις όποιες προσεγγίσεις επικρατήσουν για την υλοποίηση των ηλεκτρονικών υπογραφών, καθώς εκτιμούμε πως σε κάθε περίπτωση κάποιο σύστημα θα μεσολαβεί μεταξύ της δημιουργίας και επαλήθευσης της υπογραφής.

ΠΑΡΑΡΤΗΜΑ 2: EXECUTIVE SUMMARY

This thesis dealt with the issue of electronic signatures in its entirety. We studied both its technological as well as its regulatory aspects, something that turned out to be both interesting and difficult since these areas are traditionally adverse and incompatible.

The advent of Information And Communications Technologies has provided the capability of making electronic transactions over public and freely accessible networks such as the Internet. This new way of doing business has proved faster, cheaper and more efficient. Electronic and traditional transactions share the same semantics. For example a purchase has the same results whether it takes place on your local grocery or at an electronic mall. The buyer receives the goods and the seller receives the price. However since data in electronic form are intangible (merely strings of binary digits), and since there is a long history of security incidents on the Internet, the electronic transactions are treated differently. To be more precise, they lose the fundamental properties of enforceability and validity. By validity we mean that a particular transaction satisfies conditions set by law. By enforceability we mean that there is evidence that the transaction took place, which can provide a solution in the case of a dispute. One of the most effective mechanisms for achieving these properties is that of the signature. A signature can be used to authenticate the author of a document, to indicate acceptance of its contents and to give a sense of ceremony to the action that is about to take place, thus making the consideration that it is (legally) binding. In order to make use of the huge potential electronic transactions provide, mechanisms such as the above, should be transferred to the electronic environment, without of course losing the attributes that they have acquired through the centuries.

The theoretical background for this transition is provided by cryptography and information security. A number of solutions have been provided, but none, in our opinion, could be a precise equivalent of a signature. Most of them merely, hint the identity of the transacting parties, thus helping in overcoming the inherent anonymity of the Internet. The most promising technologies are that of digital signatures and biometrics. Digital signatures which are implemented using asymmetric cryptosystems guarantee the integrity of an electronic message and provide evidence as the identity of the sender. Biometrics use physical characteristics – the oldest form of human identification. Their electronic counterparts though, have a number of shortcomings, such as lack of precision, lack of a solid theoretical foundation, poor management functions (e.g. key renewal), and lack of acceptance to name a few, prevent them from being widely deployed. In addition, a major drawback is that they cannot guarantee the integrity of the message. This property of digital signatures enables them to overcome the intangible nature of the electronic medium and to help equalise electronic and paper documents. In addition, provided that some conditions hold, they can authenticate the sender of an electronic document. This

authentication can be excessively thought of as signature in case the authenticated documents exist for a long time. As a result a digital signature is the most prominent technology in this field. To be precise, we think this technology being dubbed as digital signature is rather unfortunate and has caused some confusion which in part accounts for the different approaches. However, to function properly an underlying infrastructure must be operating.

This underlying infrastructure aims at mapping a subject's identity from the physical to the electronic world. Its main component is a new form of electronic intermediary known as certification authority, trusted third party or more recently certification service provider. This component provides a number of services to this extend such as: certification issuance, a retrieval / directory service, physical identity verification, certificate revocation management and certificate status provision. In addition it can provide for cryptographic key generation services and initialisation of signature creation devices. It can also provided extended services such as records archival and time stamping services. These services are not that extraordinary at all. They are modelled by corresponding physical services, to which we are so accustomed to that go unnoticed. In this project we examined the most widely used standards for all the services provided by a certification authority (X.500, LDAP). This study proved very valuable since many implementation details (such as the value of some fields) can have a great impact on how a certificate (and as a result an accompanying signature) is treated.

The thing that almost instantly became apparent was that even with the underlying public key infrastructure, the digital signature approach has many problematic areas. We figured that there is no acceptable technological solution for these shortcomings. What is needed is intervention from a higher level of abstraction, which will take care of all the technological shortcomings. Nowadays the various legal and regulatory frameworks make up this external level. In the previous years and in absence of this level, the solutions had to be provided from within. This meant that certification authorities and the user of their services had to find and apply solutions themselves. These solutions appeared in the form of certificate policies and certification practice statements, issued by the certification authorities themselves. The certificate policy deals with the allowed use of certificates, the user authentication requirements as well as with security requirements of systems used by the CA. The certification practice statement is the policy implementation guide. References of both can be found in each certificate issued by a trusted third party, which in effect means that use of a certificate results in acceptance of their terms. On of the most prominent of their features is the fact that great effort was put, so that they disclaim any liability for the contents of a certificate, or its complementary services.

The regulatory intervention that followed introduced two new entities. The first one having the overall responsibility of policy setting and the other one with the conformance check. This conformance check makes sure that the standards resulting from the policy setting function, are followed by the certification authority. These standards can be divided in two categories. The first one are the classical

computer security standards (TCSEC, ITSEC, Common Criteria FIPS PUB 140-2) which can be applied to any environment regardless of its use. In addition there are specific standards that stem from the policy settings and apply specifically to electronic signature products. In addition to these assessment standards, we examined interoperability standards that enable applications from different vendors to interoperate. The most important of them was the standards relating to the electronic signature formats. In addition to supporting interoperability requirements these standards enable the validation of an electronic signature in the future, no matter how much time has elapsed from the original signing. This requires that somehow that an instance of the underlying public key infrastructure is present at each electronic signature. We also studied the various standards regarding the devices used in everyday situations in order to create and validate electronic signatures. This resulted in a functional model of its environment which in turned revealed the security requirements, regarding signature creation and validation.

The main focus of our project was however, the international legal and regulatory efforts regarding electronic signatures. We studied the best known such efforts, e.g. the ABA Digital Signature and PKI Assessment Guidelines, the UNCITRAL Model Law On Electronic Commerce And Electronic Signatures, the European Commission Directive as well as the most important national such efforts namely the U. S. E-Sign Act, the German Digital Signature Law etc. All of them make provisions as far as the following in three areas are concerned:

- Legal Validity Of Electronic Signatures
- PKI Operation Rules.
- Regulatory Framework for certification authorities.

Despite the above common classification there are a lot of differences in the way these areas are treated. As far as the legal validity of electronic signatures is concerned there are three common approaches: The first one deals specifically with the digital signature technology. The proponents of this approach find that the extensive research and practical implementation of this technology, provides legal certainty and allows for good solutions as far the technological problems are concerned. Germany is the best example of the technology specific approach. The second approach wants to leave some room for new technologies to develop, while maintaining the benefits of the former approach. As a result, it makes no distinction over the available digital signature technologies, but accepts them all in principle. Technologies that are characterised by a higher degree of security are given, enhanced legal status. Typical of this approach is the European Directive on Electronic Signatures. In the European approach, the only known technology that satisfies the advanced security requirements is the digital signature technology. The last approach to electronic signature legislation is called the minimalist or functionalist approach. Here no specific security requirements are described and no special provisions are granted. The exact requirements an privileges will be set on specific cases or fields, depending on the exact security requirements and other related facts.

One of the most important causes for the observed differentiation is the divergence of the existing legal framework concerning signature and form requirements in transactions which reflect different cultural roots. For example in most common law nations, the most important function of the signature is the intention of the signer, to be bound to a commitment. As a result, a simple mark will do or a simple 'click ok to accept' for that matter. On the other hand, in most civil countries the main focus is on the security of the signing process, meaning the difficulty to be forged. It comes as no surprise that most civil law nations are in favour of the technology specific approach.

As far as the technical framework for the operation of public key infrastructure is concerned, meaning the security requirements and the technical standards required we can see a great deal of similarities. This is a result mainly of the fact that the common root of all the PKIs in the world is the X.509 standard which was successfully migrated to the internet by the work of IETF. One of the things that we noted is Germany's approach, which in essence regulates in this level by a legal and not technical committee, and furthermore gives no legal status to digital signatures.

The level where most differences are noted is the regulatory framework concerning the operation of certification authorities. The primary means of regulating this sector is the concept of accreditation. Accreditation in the field of certification services refers to the assessment of the management, operational and technical process of a certification service provider. It can be easily deducted that there can be no accreditation, if the legal framework regulating digital signatures is technology neutral. The main difference between the approaches examined in this project is that in some countries like the USA or Canada accreditation can be found only where the primary key infrastructure of a public service is to be linked with a commercial PKI. Contrary to that, in Europe, mainly, accreditation results mainly in the enhancement of the level of services provided to the public along with the promotion of the services themselves.

The European approach towards electronic signatures was a main focus point of this project. This did not only happen because of the effect the directive will have on the law of the member states, but mainly because of the fact that it is going to (actually it was) the only international approach that will have a profound effect on the law of a number of nations. As far as the European directive was concerned we tried, using technical standards to map the high level requirements of the directive to more detailed guidelines. It turns out that an excellent guide for accreditation is the annexes I, II as far as the contents of a certificate and the operation of certification service provider is concerned. The European Directive is also one of the few worldwide attempts to regulate the use of signature creation and verification devices. Interesting comparisons were made with the European directive and some interesting European approaches. In Greece, the directive was passed in law with a presidential decree. Since November, there is a public consultation regarding certification services and accreditation, in which we expressed our views.