



ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

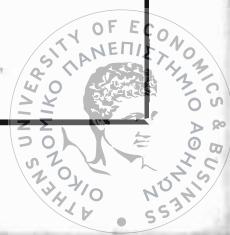
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Υπηρεσίες Προστιθέμενης Αξίας σε Υποδομές
Δημόσιου Κλειδιού**

Ρέντας Νικόλαος

M3020006

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2004



ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ
ΒΙΒΛΙΟΘΗΚΗ
εισ. 76272
Αρ.
παξ.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Υπηρεσίες Προστιθέμενης Αξίας σε Υποδομές
Δημόσιου Κλειδιού**

Ρέντας Νικόλαος

M302006



Επιβλέπων Καθηγητής : Δημήτριος Γκρίζαλης

Εξωτερικός Κριτής : Δημήτριος Λέκκας

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2004





Περιεχόμενα

Πρόλογος και Ευχαριστίες	7
Περίληψη στην ελληνική γλώσσα.....	9
Περίληψη στην αγγλική γλώσσα.....	9
Κεφάλαιο 1 Εισαγωγή	11
1.1 Περιγραφή του προβλήματος	11
1.2 Γενικοί Στόχοι Διπλωματικής Εργασίας.....	11
1.3 Δομή Διπλωματικής Εργασίας	12
1.3.1 Μεθοδολογία προσέγγισης.....	12
1.3.2 Περιγραφή κεφαλαίων.....	12
1.3.3 Εννοιολογικό πλαίσιο	13
Κεφάλαιο 2 Βασικές Έννοιες και Ορισμοί	15
2.1 Ασφάλεια Πληροφοριακών Συστημάτων	15
2.1.1 Πληροφοριακό Σύστημα.....	15
2.1.2 Ασφάλεια Πληροφοριακών Συστημάτων	19
2.2 Υποδομή Δημόσιου Κλειδιού	20
2.2.1 Βασικές έννοιες Κρυπτογραφικών Συστημάτων.....	21
2.2.2 Ασύμμετρη κρυπτογραφία	22
2.2.3 Συμμετρική κρυπτογραφία.....	22
2.2.4 Ψηφιακές Υπογραφές	23
2.2.5 Ψηφιακά Πιστοποιητικά	24
2.3 Συμπεράσματα.....	26
Αναφορές	27
Κεφάλαιο 3 Τεχνολογικό Υπόβαθρο	28
3.1 Βασικά χαρακτηριστικά Υποδομής Δημόσιου Κλειδιού.....	28
3.1.1 Μοντέλο Αναφοράς.....	28
3.1.2 Απαιτήσεις χρηστών	30
3.2 Παρεχόμενες Υπηρεσίες σε Υποδομή Δημόσιου Κλειδιού	31
3.2.1 Βασικές Υπηρεσίες.....	33

3.2.2 Δευτερεύουσες Υπηρεσίες	34
3.2.3 Υπηρεσίες προστιθέμενης αξίας.....	35
3.3 Υποδομή Δημόσιου Κλειδιού και Πρότυπα.....	35
3.3.1 Πρότυπα Διεθνούς Οργανισμού Πιστοποίησης (International Standards Organization - ISO).....	35
3.3.2 Πρότυπα της ITU-T (Διεθνής Ένωση Τηλεπικοινωνιών).....	36
3.3.3 PKCS Πρότυπα – RSA	37
3.3.4 IETF Πρότυπα – Πρότυπα στο περιβάλλον του διαδικτύου	39
3.3.5 Νομικά πλαίσια και ο ρόλος της εμπιστοσύνης	41
3.3.5.1 Νομοθετικά πλαίσια.....	42
3.3.5.2 Ο ρόλος της εμπιστοσύνης.....	43
3.4 XML/Schema και XML	46
3.4.1 Γενικά χαρακτηριστικά.....	46
3.4.2 Παρουσίαση XML Schema και XML	47
3.4.2.1 Τεχνικά χαρακτηριστικά	47
3.4.2.2 Παραδείγματα χρήσης	48
3.5 Συμπεράσματα.....	51
Αναφορές	52
Κεφάλαιο 4 Υπηρεσίες Προστιθέμενης Αξίας σε Υποδομή Δημόσιου Κλειδιού.....	53
4.1 Χρονοσήμανση.....	53
4.1.1 Εισαγωγή	53
4.1.2 Ασφαλής χρόνος.....	54
4.1.3 Αποστολή της αίτησης χρονοσήμανσης	58
4.1.4 Παραγωγή χρονοσφαγίδας.....	60
4.1.5 Επαλήθευση χρονοσφαγίδας	62
4.1.6 Διατήρηση χρονοσφαγίδων.....	63
4.2 Συμβολαιογραφία	65
4.2.1 Εισαγωγή	65
4.2.2 Επικύρωση εγκυρότητας εγγράφου	66

4.2.3 Επαλήθευση συμβολαιογραφικού τεκμηρίου	70
4.3 Παροχή Αποδεικτικών Στοιχείων.....	72
4.3.1 Εισαγωγή	72
4.3.2 Αίτηση για δημιουργία αποδεικτικών στοιχείων.....	73
4.3.3 Συλλογή αποδεικτικών στοιχείων	79
4.3.4 Ανάκτηση τεκμηρίων.....	83
4.4 Διαχείριση Δικαιωμάτων	86
4.4.1 Εισαγωγή	86
4.4.2 Καθορισμός δικαιωμάτων.....	88
4.4.3 Ανάκτηση δικαιωμάτων.....	94
4.5 Υπηρεσία Περιαγωγής (Roaming PKI Service).....	96
4.5.1 Εισαγωγή	96
4.5.2 Παροχή υπηρεσίας Περιαγωγής – Λειτουργικά χαρακτηριστικά	96
4.5.2 Αίτηση παροχής υπηρεσιών περιαγωγής	99
4.6 Βιομετρικές Μέθοδοι Αυθεντικοποίησης	102
4.6.1 Εισαγωγή	102
4.6.2 Καταχώρηση βιομετρικών δειγμάτων και επαλήθευση.....	102
4.6.3 Βιομετρικές τεχνικές.....	103
4.6.4 Βιομετρικές τεχνικές και Υποδομή Δημόσιου Κλειδιού	107
4.6.5 Καταχώρηση – Επιβεβαίωση Βιομετρικών χαρακτηριστικών.....	108
4.6.6 Καταχώρηση νέου Βιομετρικού χαρακτηριστικού.....	112
4.7 Διατήρηση Ανωνυμίας.....	114
4.7.1 Εισαγωγή	114
4.7.2 Αίτηση παροχής ανωνυμίας	115
Αναφορές.....	117
Κεφάλαιο 5 Προτεινόμενη Αρχιτεκτονική υλοποίησης ΥΔΚ για παροχή Υπηρεσιών Προστιθέμενης Αξίας.....	121
5.1 Μοντέλο Αναφοράς και Γενικά Χαρακτηριστικά	121
5.2 Ανάλυση Λειτουργικής Αρχιτεκτονικής.....	122

5.2.1 Βασικά Χαρακτηριστικά.....	122
5.2.2 Προσδιωρισμός Λειτουργικών Μονάδων (Functional Units)	123
5.2.3 Περιγραφή Αρχιτεκτονικής.....	125
5.2.3.1 Μοντέλο υλοποίησης.....	127
5.2.3.2 Περιγραφή Βάσης Δεδομένων	129
5.3 Τεχνολογικές Προτάσεις Υλοποίησης.....	148
5.4 Συμπεράσματα.....	149
Κεφάλαιο 6 Επίλογος.....	150
6.1 Σύνοψη και Συμπεράσματα.....	150
6.2 Ανοικτά θέματα	151
Παράρτημα	152
Ευρετήριο Σχημάτων και Πινάκων	152
Περιγραφή της Βάσης Δεδομένων με τη χρήση του XML Schema	153
Παρουσίαση σχήματος της προτεινόμενης Βάσης Δεδομένων	160



Πρόλογος και Ευχαριστίες

Το παρόν κείμενο αποτελεί το αποτέλεσμα μελέτης και έρευνας που πραγματοποιήθηκε στα πλαίσια Διπλωματικής Εργασίας για το Μεταπτυχιακό Πρόγραμμα Σπουδών των Πληροφοριακών Συστημάτων του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών. Αντικείμενο έρευνας είναι οι Υπηρεσίες πιστοποίησης προστιθέμενης αξίας σε Υποδομές Δημόσιου Κλειδιού και η πρόταση ενός μοντέλου αναφοράς που ενσωματώνει τις υπηρεσίες αυτές.

Η παρούσα Διπλωματική Εργασία δε θα μπορούσε να πραγματοποιηθεί χωρίς τις γνώσεις και το επιστημονικό υπόβαθρο που απέκτησα κατά τη φοίτησή μου στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Αθηνών και τη δυνατότητα που μου παρείχε το Μεταπτυχιακό Πρόγραμμα Σπουδών των Πληροφοριακών Συστημάτων του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών να ανοίξω τους επιστημονικούς μου ορίζοντες πέρα από τα στενά τεχνολογικά πλαίσια αλλά και τη δυνατότητα να εκπονήσω ένα άκρως ενδιαφέρον θέμα.

Ευχαριστώ ιδιαίτερα τον Αναπληρωτή Καθηγητή του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών κ. Δημήτρη Γκρίζαλη για την επιλογή του θέματος που αποδείχτηκε πολύ ενδιαφέρον και αποτέλεσε το κίνητρο να εμπλουτίσω τις επιστημονικές γνώσεις μου σε ένα σύγχρονο και εξελισσόμενο τομέα και για τις εποικοδομητικές και γόνιμες συζητήσεις και συνεργασίες που είχαμε κατά τη διάρκεια της φοίτησής μου στο παρόν Μεταπτυχιακό Πρόγραμμα Σπουδών. Επίσης, ευχαριστώ ιδιαίτερα τον Λέκτορα του Τμήματος Μηχανικών Σχεδίασης Προϊόντων και Συστημάτων του Πανεπιστήμιο Αιγαίου κ. Δημήτρη Λέκκα χωρίς τη συμβολή του οποίου θα ήταν δύσκολο να ολοκληρωθεί η παρούσα Διπλωματική Εργασία καθώς με την επιστημονική του κατάρτιση και εμπειρία με βοήθησε να ξεπεράσω τις όποιες δυσκολίες παρουσιάστηκαν κατά τη διάρκεια της έρευνας.

Επίσης αισθάνομαι υποχρεωμένος να ευχαριστήσω τόσο τους γονείς μου, Ελένη και Παναγιώτη, όσο και τον αδερφό μου Δημήτρη, τόσο για τη συμπαράστασή τους κατά τη διάρκεια της φοίτησής μου όσο και για την ενθάρρυνση και τη συνεχή υποστήριξη που μου παρέχουν.



Τέλος, ευχαριστώ θερμά όσους έδειξαν κατανόηση και με στήριξαν ψυχολογικά και συναισθηματικά ειδικά τους τελευταίους μήνες της προσπάθειάς μου.

Αθήνα, Δεκέμβριος 2003

Νίκος Ρέντας



Περίληψη στην ελληνική γλώσσα

Η ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών στις τελευταίες δεκαετίες έχει δημιουργήσει την ανάγκη για την παροχή ενός συνόλου υπηρεσιών από τη μεριά των Οργανισμών-παρόχων. Σημαντικό ρόλο στη διασφάλιση της Ασφάλειας των Πληροφοριών σε ένα τέτοιο πλαίσιο διαδραματίζουν οι Υποδομές Δημόσιου Κλειδιού που αξιοποιούν την τεχνολογία των ψηφιακών πιστοποιητικών και ψηφιακών υπογραφών. Στο παρόν κείμενο μελετώνται και αναλύονται οι βασικές έννοιες, το τεχνολογικό πλαίσιο και οι Υπηρεσίες Προστιθέμενης Αξίας όπως διατυπώνονται και εκφράζονται μέσα από τις λειτουργικές απαιτήσεις των χρηστών τέτοιων υποδομών. Οι περιγραφόμενες υπηρεσίες είναι η Χρονοσήμανση, η Συμβολαιογραφία, η Διαχείριση Δικαιωμάτων, η παροχή Αποδεικτικών Στοιχείων, η Περιαγωγή, η διατήρηση της Ανωνυμίας και ο συνδυασμός τους με Βιομετρικές Μεθόδους Αυθεντικοποίησης. Για την περιγραφή των υπηρεσιών αυτών χρησιμοποιείται το πρότυπο της XML Schema με στόχο τη μέγιστη δυνατή ενσωμάτωση των υπηρεσιών αυτών σε υπάρχουσες υποδομές. Στη συνέχεια, παράγεται ένα μοντέλο αναφοράς και μιας αρχιτεκτονικής υλοποίησης που ενσωματώνει και υποστηρίζει τις παραπάνω υπηρεσίες με τη συγκεκριμένη απεικόνιση του XML Schema. Τέλος, παρουσίαζεται και αναλύεται μια προτεινόμενη αφαιρετική Βάση Δεδομέων ικανή να υποστηρίξει τόσο τις υπηρεσίες Προστιθέμενης Αξίας ενός Οργανισμού-παρόχου όσο και τις υπόλοιπες υπηρεσίες του, με ιδιαίτερες ικανότητες ευελιξίας και επεκτασιμότητας.

Περίληψη στην αγγλική γλώσσα

The growth of technologies of Information Technology and Communication in the last decades has created the need for the offer of total services from the side of Organisations. Important role in the guarantee of Security of Information in a such frame, plays the Public Key Infrastructure that use the technology of the digital certificates and digital signatures. In the present text are studied and analyzed the following terms : the basic terminology, the technological frame and the Value Added Services as they are formulated and expressed through the functional requirements of users in such infrastructures. The described services are Timestamping, Notarization,

Management of Rights, Evidence Offer, Roaming, Anonymity and their combination with Biometric Methods of Authentication. For the description of these services is used the model of XML Schema aiming at the biggest possible incorporation of these services in the existing infrastructures. Then, it is produced a reference model and an architectural infrastructure that incorporates and supports the above services with the particular depiction of XML Schema. Finally, it is presented and analyzed a proposed DataBase capable to support the Value Added services and the rest services of an Organisation with particular capabilities of flexibility and integration.

Κεφάλαιο 1 Εισαγωγή

1.1 Περιγραφή του προβλήματος

Η ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών στις τελευταίες δεκαετίες έχει δημιουργήσει την ανάγκη για την παροχή υπηρεσιών Προστιθέμενης Αξίας από τη μεριά των Οργανισμών - παρόχων προς τους τελικούς χρήστες. Οι υπηρεσίες αυτές είναι ολοκληρωμένες και διαφέρουν από την απλή διακίνηση των δεδομένων στο γεγονός της ανάγκης για προστασία των βασικών χαρακτηριστικών της Ασφάλειας των Πληροφοριών.

Σημαντικό ρόλο στη διασφάλιση της Ασφάλειας των Πληροφοριών διαδραματίζουν οι Υποδομές Δημόσιου Κλειδιού που αξιοποιούν την τεχνολογία των ψηφιακών πιστοποιητικών και των ψηφιακών υπογραφών. Ιδιαίτερος είναι σε μια τέτοια υποδομή και ο ρόλος των Οργανισμών -παρόχων που λειτουργεί σαν τον έμπιστο διαμεσολαβητή για τις προσφερόμενες υπηρεσίες. Οι κανόνες Ασφαλείας οριθετούνται από τον Οργανισμό και τα συναλλασσόμενα μέρη οφείλουν να τους τηρούν για να μπορούν να αποτελούν μέρος αυτού του ενεργού Πληροφοριακού Συστήματος.

Ωστόσο η αντιμετώπιση των υπηρεσιών Προστιθέμενης Αξίας, στις οποίες διακρίνουμε τη Χρονοσήμανση, τη Συμβολαιογραφία, τη Διαχείριση Δικαιωμάτων, την Παροχή Αποδεικτικών Στοιχείων, την Περιαγωγή, την Ανωνυμία και τις Βιομετρικές Μεθόδους Αυθεντικοποίησης, δεν είναι ενιαία στην ερευνητική περιοχή. Αυτό που προσπαθεί να επιτύχει η παρούσα Διπλωματική Εργασία, είναι να μελετήσει τις υπηρεσίες αυτές και να τις εντάξει σε μια συνολική αρχιτεκτονική, ικανή να υλοποιηθεί από έναν Οργανισμό για την παροχή ολοκληρωμένης λύσης.

1.2 Γενικοί Στόχοι Διπλωματικής Εργασίας

Οι βασικοί στόχοι της παρούσας Διπλωματικής Εργασίας επικεντρώνονται στα :

- Η παρουσίαση των βασικών εννοιών της Ασφάλειας των Πληροφοριακών Συστημάτων και του ρόλου του Οργανισμού σε μια Υποδομή Δημόσιου Κλειδιού.
- Η κατάταξη των υπηρεσιών ενός Οργανισμού που λειτουργεί σε μια Υποδομή Δημόσιου Κλειδιού.

- Ιδιαίτερα, η ανάλυση της λειτουργίας των υπηρεσιών Προστιθέμενης Αξίας και η περιγραφή τους με τη χρήση της XML Schema.
- Η καταγραφή των τεχνολογικών προτάσεων και υλοποιήσεων που σχετίζονται με τις υπηρεσίες Προστιθέμενης Αξίας.
- Η παραγωγή ενός μοντέλου αναφοράς και μιας αρχιτεκτονικής υλοποίησης των υπηρεσιών αυτών.
- Η παρουσίαση μιας αφαιρετικής Βάσης Δεδομένων που μπορεί να υποστηρίξει τις υπηρεσίες ενός Οργανισμού με ιδιαίτερες δυνατότητες ευελιξίας και επεκτασιμότητας.

1.3 Δομή Διπλωματικής Εργασίας

1.3.1 Μεθοδολογία προσέγγισης

Για τη μελέτη του συγκεκριμένου θέματος της παρούσας Διπλωματικής Εργασίας υιοθετήθηκε το Παράδειγμα του Λειτουργισμού. Η κατανόηση του συγκεκριμένου θέματος επιχειρείται μέσα από αφαιρετικές κατασκευές (μοντέλα, τεχνικές απεικόνισης), από θεωρητικά νοητικά σχήματα (έννοιες, θεωρίες, υποθέσεις) και λαμβάνει ισχυρά υπόψη το περιβάλλον μέσα στο οποίο δραστηριοποιείται. Εφαρμόζονται στη μελέτη ξεκάθαρα οι δύο βασικές αρχές του Ρεαλισμού και του Θετικισμού, ενώ μέσα από τη μεθοδολογία της επαγωγής εξάγονται κάποια βασικά συμπεράσματα και δίνονται κάποιες προτάσεις όπου η επιστημονική περιοχή δεν έχει δώσει μια ξεκάθαρη λύση.

1.3.2 Περιγραφή κεφαλαίων

Στο παρόν πρώτο κεφάλαιο οριοθετείται το πρόβλημα και το θέμα της παρούσας Διπλωματικής Εργασίας, περιγράφονται οι γενικοί στόχοι και παρουσιάζεται το εννοιολογικό πλαίσιο το οποίο αναδείχθηκε από τη μελέτη του συγκεκριμένου ερευνητικού πεδίου.

Στο δεύτερο κεφάλαιο παρουσιάζονται οι βασικές έννοιες που σχετίζονται με τη συγκεκριμένη επιστημονική περιοχή. Ειδικότερα αναλύονται οι έννοιες του Πληροφοριακού Συστήματος και της Ασφάλειας των Πληροφοριακών Συστημάτων, ενώ επίσης παρουσιάζονται οι βασικές κρυπτογραφικές έννοιες και οι έννοιες των ψηφιακών υπογραφών και πιστοποιητικών.

Στο τρίτο κεφάλαιο παρουσιάζεται ένα βασικό μοντέλο αναφοράς για μια Υποδομή Δημόσιου Κλειδιού και ποιες είναι οι απαιτήσεις των χρηστών σε μια τέτοια υποδομή. Γίνεται μια κατηγοριοποίηση των Υπηρεσιών ενός Οργανισμού που λειτουργεί σε μια τέτοια υποδομή και αναφέρονται τα πιο γνωστά πρότυπα και εφαρμογές που θα χρησιμοποιηθούν στην ανάλυση. Επίσης, αναδεικνύεται ο ρόλος των νομοθετικών πλαισίων και της εμπιστοσύνης στο χώρο δραστηριοποίησης του Οργανισμού. Τέλος, γίνεται μια σύντομη αναφορά στην XML και το XML Schema, της τεχνολογίας που θα χρησιμοποιηθεί για την περιγραφή των Υπηρεσιών Προστιθέμενης Αξίας στο επόμενο κεφάλαιο.

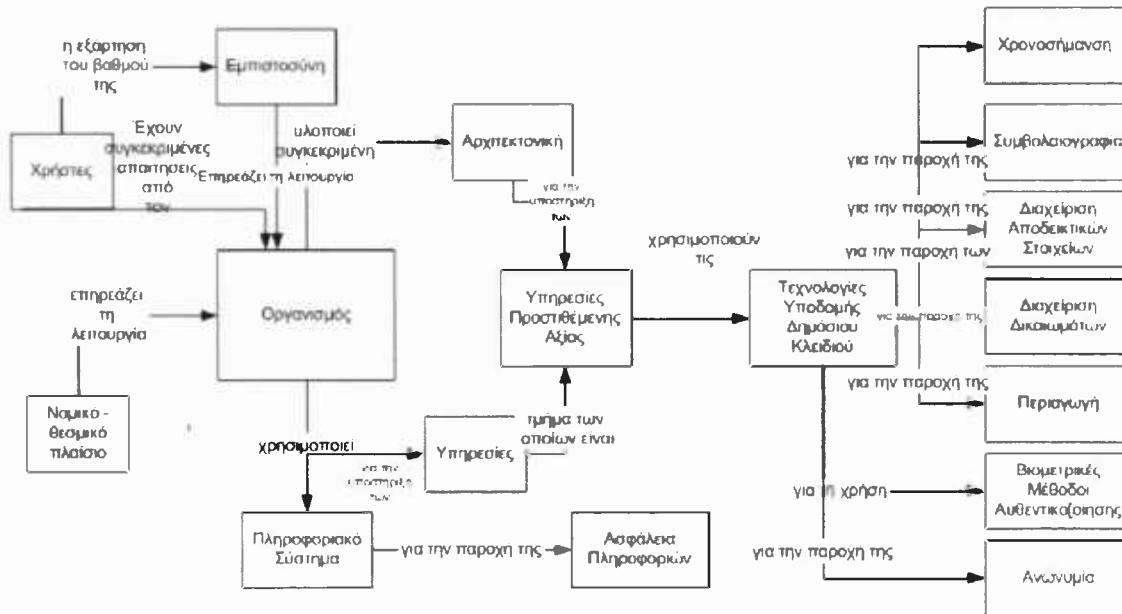
Στο τέταρτο κεφάλαιο αναλύονται οι Υπηρεσίες Προστιθέμενης Αξίας που μελετώνται από άλλα ερευνητικά έργα και σε πολλές περιπτώσεις προτείνονται και νέες τεχνικές υλοποίησης και διάδρασης μεταξύ των αναφερόμενων υπηρεσιών.

Στο πέμπτο κεφάλαιο προτείνεται ένα αφαιρετικό μοντέλο αναφοράς και της αντίστοιχης αρχιτεκτονικής για την υλοποίηση από έναν πάροχο – Οργανισμό. Συγκεκριμένα προσδιορίζονται οι βασικές λειτουργικές μονάδες και ο τρόπος ενοποίησής τους ενώ τέλος προτείνεται η υιοθέτηση μιας συγκεκριμένης Βάσης Δεδομένων. Η συγκεκριμένη πρόταση υλοποίησης είναι άκρως ενδιαφέρουσα μιας και μπορεί να υποστηρίξει κάθε είδους παραγόμενου μοντέλου αναφοράς διαφορετικών Οργανισμών με διαφορετικές διαδικασίες και πολιτικές.

Στον επόμενο της Διπλωματικής εργασίας αναλύονται κάποια βασικά συμπεράσματα και αναφέρονται κάποια ανοικτά θέματα για περαιτέρω έρευνα.

1.3.3 Εννοιολογικό πλαίσιο

Το εννοιολογικό πλαίσιο που χρησιμοποιήθηκε για τη μελέτη του συγκεκριμένου θέματος αλλά και αναδείχθηκε από τη μελέτη των διαφόρων επιστημονικών περιοχών είναι το ακόλουθο :



Σχήμα 1.1 Εννοιολογικό πλαίσιο

Οι βασικές έννοιες που αναδεικνύονται από το Εννοιολογικό πλαίσιο και θα αναλυθούν στην παρούσα διπλωματική εργασία είναι :

- Ο Οργανισμός – πάροχος των υπηρεσιών Προστιθέμενης Αξίας και οι διάφορες αλληλεπιδράσεις του (Χρήστες, Νομικό – Θεσμικό Πλαίσιο, ο ρόλος της Εμπιστοσύνης και τα Πληροφοριακά Συστήματα).
- Η κατάταξη των υπηρεσιών ενός τέτοιου Οργανισμού.
- Ο ρόλος των τεχνολογιών Υποδομής Δημόσιου Κλειδιού στην παροχή των υπηρεσιών ενός τέτοιου Οργανισμού.
- Η ανάλυση των υπηρεσιών Προστιθέμενης Αξίας.
- Η προτεινόμενη αρχιτεκτονική για τη λειτουργία ενός τέτοιου Οργανισμού.

Κεφάλαιο 2 Βασικές Έννοιες και Ορισμοί

2.1 Ασφάλεια Πληροφοριακών Συστημάτων

Για την ανάλυση της έννοιας της Ασφάλειας των Πληροφοριακών Συστημάτων – κεντρικής έννοιας σε μια Υποδομή Δημόσιου Κλειδιού- θα περιγράψουμε τις συνιστώσες του Πληροφοριακού Συστήματος και στη συνέχεια τις ιδιότητες της Ασφάλειας.

2.1.1 Πληροφοριακό Σύστημα

Κάθε Οργανισμός επηρεάζεται από το περιβάλλον στο οποίο εντάσσεται και χρησιμοποιεί τα Πληροφοριακά Συστήματα για την υποστήριξη των λειτουργιών του. Τα πληροφοριακά συστήματα αποτελούνται από τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών, ανθρώπους, διαδικασίες και δεδομένα και οι τέσσερις αυτές συνιστώσες αλληλεπιδρούν μεταξύ τους ανά δύο [Κιουντούζης].

Πληροφοριακό Σύστημα : Πληροφορία , Σύστημα ή κάτι άλλο ;

Είναι γεγονός ότι δεν έχει καταγραφεί μέχρι σήμερα ποιος επινόησε πρώτος τον όρο «Πληροφοριακό Σύστημα». Προφανώς τη χρονική στιγμή που συνέβη, η φράση αυτή φαινόταν ως ο πιο χρήσιμος τρόπος για την εστίαση σ' έναν συγκεκριμένο τύπο συστήματος [Paton]. Στις μέρες μας θεωρείται από πολλούς ότι ο όρος αυτός έχει βλαβερή επίδραση στην τρέχουσα χρήση τους. Η σύγχυση που δημιουργείται εστιάζεται βασικά στις έννοιες πληροφορία και σύστημα.

Το πιο σημαντικό πρόβλημα σχετικά με την έννοια πληροφορία είναι η έλλειψη υπόστασης. Δεν αποτελεί ένα διακριτό αντικείμενο, αλλά περισσότερο διανοητικό οικοδόμημα. Το σημείο κλειδί είναι ότι τα αντικείμενα που μας περιβάλλουν δεν αποτελούν από μόνα τους «πληροφορία». Είναι το πλαίσιο στο οποίο τοποθετούνται και η σημασία η οποία τους αποδίδεται, που σε συνδυασμό δημιουργούν την «πληροφορία»[Paton]. Το ουσιαστικό «πληροφορία» ορίζεται από το ρήμα «πληροφορώ» και κατά συνέπεια φέρει ως ένα μεγάλο βαθμό την σημασία του ρήματος που αποτελεί την ρίζα δημιουργίας του.

Σύμφωνα με τα πρότυπα του ISO, πληροφορία είναι η τρέχουσα σημασία που αποδίδεται στα δεδομένα χρησιμοποιώντας τις συμβατικές παραδοχές που εφαρμόζονται σ' αυτά. Συνεπώς : δεδομένα + ερμηνεία = πληροφορία [Κιουντούζης]. Στο σημείο αυτό αξίζει να αναφέρουμε ότι ο όρος δεδομένα είναι επίσης ένας όρος

στον οποίο αποδίδονται διάφοροι ορισμοί, αλλά ακολουθώντας τα διεθνή πρότυπα ISO, ο όρος δεδομένα σημαίνει μια παράσταση γεγονότων, εννοιών ή εντολών σε τυποποιημένη μορφή που είναι κατάλληλη για επικοινωνία, ερμηνεία ή επεξεργασία από άνθρωπο ή αυτόματα μέσα. Με απλά λόγια, η πληροφορία είναι τα δεδομένα σε χρήση.

Η χρήση του όρου «σύστημα» είναι εξίσου προβληματική με εκείνη του όρου «πληροφορία». Ο όρος «σύστημα» χρησιμοποιήθηκε για πρώτη φορά από τον βιολόγο Ludwig von Bertalanffy όταν μελετούσε τους οργανισμούς ως ολότητες και όχι μέσω των τμημάτων τους [Paton]. Ο ίδιος στη συνέχεια διετύπωσε την άποψη ότι αυτού του είδους η αντιμετώπιση μπορεί να γίνει όχι μόνο για τους οργανισμούς, αλλά και για ολότητες κάθε είδους. Υπάρχουν δύο συγκρούομενες και γενικές χρήσεις όσον αφορά την άποψη με την οποία προσεγγίζουμε τον όρο στην παρούσα μελέτη : η τεχνική και η κοινότυπη.

Σύμφωνα με την τεχνική χρήση ο ορισμός του όρου «σύστημα» είναι ως ακολούθως : «Ως σύστημα ορίζεται ένα σύνολο από αντικείμενα μαζί με τις σχέσεις μεταξύ των αντικειμένων και των χαρακτηριστικών γνωρισμάτων τους, τα οποία είναι σε αλληλοσυγχέτιση μεταξύ τους και με το περιβάλλον, έτσι ώστε ν' αποτελούν μια ενιαία ολότητα», και περιέχεται στο βιβλίο των Schoderbek et al. (1990). Ο ορισμός αυτός είναι κοινά αποδεκτός καθώς έχει το πλεονέκτημα να είναι και γενικός, έχοντας ευρεία εφαρμογή, αλλά και ειδικός, προσδιορίζοντας τα στοιχεία που καθορίζουν ένα σύστημα.

Στον παραπάνω ορισμό περιέχονται λέξεις – κλειδιά με διφορούμενες πολλές φορές ερμηνείες και για το λόγο αυτό αποσαφηνίζονται ακολούθως. Σύνολο, είναι ένα πλήθος καλά ορισμένων στοιχείων καθώς και των αντικειμένων που αποτελούν τμήματα αυτού. Όταν ένα αντικείμενο θεωρείται ως αδιαίρετο, ως μια ενιαία μονάδα στην οποία ανήκει κάθε επί μέρους στοιχείο του, τότε λέμε ότι βλέπουμε το αντικείμενο ως ολότητα. Ως περιβάλλον θεωρείται ότι δεν αποτελεί μέρος του συστήματος, αλλά μπορεί όμως να δράσει επάνω του ή να υποστεί τη δράση του. Κατά τον καθορισμό συνεπώς του περιβάλλοντος ενός συστήματος, πρέπει να λαμβάνονται υπόψη δύο χαρακτηριστικά : πρώτον ότι το περιβάλλον δεν ελέγχεται από το σύστημα και δεύτερον ότι ασκεί σημαντική επίδραση στην απόδοση / συμπεριφορά του συστήματος.

Η αμφισβήτηση σχετικά με τον όρο «σύστημα» προέκυψε λόγω της κοινότυπης χρήσης του. Με την πάροδο του χρόνου ο όρος «σύστημα» ενσωματώθηκε στην κοινή γλώσσα ως χαρακτηριστικό κάθε οργανωμένης ομάδας γεγονός που οδήγησε τον Peter Checkland να επαναλάβει την πρόταση του Arthur Koestler να αναφέρεται ο όρος «σύστημα» με τον όρο «όλον».

Όσον αφορά λοιπόν τον όρο «Πληροφοριακό Σύστημα» είναι απολύτως σίγουρο ότι δεν είναι «πληροφορία», ούτε «σύστημα», ούτε κάποιος συνδυασμός αυτών. Το Πληροφοριακό Σύστημα που χρησιμοποιεί Η/Υ είναι ένα οργανωμένο σύνολο από πέντε αλληλεπιδρώντων στοιχείων που επεξεργάζεται δεδομένα και παράγει πληροφορίες μιας Επιχείρησης ή ενός Οργανισμού. Οι πέντε συνιστώσες του πληροφοριακού συστήματος είναι : άνθρωποι, διαδικασίες (procedures, methods), δεδομένα (data), λογισμικό (software) και υλικός εξοπλισμός (hardware). [Κιουντούζης]

Όλες οι συνιστώσες του συστήματος παίζουν ρόλο στην απόδοσή του, ανεξάρτητα από το εάν η μεθοδολογία ανάπτυξής του δίνει έμφαση σε μία μόνο από αυτές. Επίσης, θα πρέπει να τονιστεί ότι κατά οιονδήποτε τρόπο (άμεσο ή έμμεσο) υπάρχει αλληλεπίδραση μεταξύ των στοιχείων ενός συστήματος.

Το πληροφοριακό Σύστημα είναι ένα ολοκληρωμένο Σύστημα που περιλαμβάνει

Κοσμοθεωρία – Αρχές – Διαδικασίες

Οργανωτική Δομή



Προσωπικό – Λογισμικό
Ηλεκτρονικά Μηχανήματα



Εγκαταστάσεις και
Δίκτυα Υπολογιστών



Και παρέχει έγκαιρα και επαρκή στοιχεία για τη σχεδίαση, διεύθυνση, συντονισμό, έλεγχο και διεξαγωγή των λειτουργιών του Οργανισμού

Σχήμα 2.1 Μοντέλο αναπαράστασης Πληροφοριακού Συστήματος

Για την πληρέστερη αποσαφήνιση της έννοιας του Πληροφοριακού Συστήματος παρατίθεται μια συνοπτική περιγραφή των συνιστώσων του :

1^η συνιστώσα : Άνθρωποι

Οι άνθρωποι που αποτελούν στοιχεία ενός Πληροφοριακού συστήματος μπορούν να ταξινομηθούν σε δύο κατηγορίες : στους χρήστες (users), στους χειριστές (operators) του συστήματος και στους δημιουργούς (developers) που έχουν την ευθύνη της δημιουργίας, της συντήρησης και της ανάπτυξης του συστήματος. Όλοι αυτοί βέβαια είναι ρόλοι, δηλαδή ένα άτομο μπορεί ν' ανήκει ταυτόχρονα σε διαφορετικές κατηγορίες. Παράλληλα, υπάρχει και μια οργανωτική δομή στην οποία εντάσσονται οι άνθρωποι που εργάζονται στο σύστημα.

2^η συνιστώσα : Διαδικασίες

Οι διαδικασίες στην πράξη είναι οδηγίες για τους ανθρώπους που ανήκουν στο σύστημα. Υπάρχουν συνεπώς διαδικασίες που αφορούν τους χρήστες και τους χειριστές και έχουν ένα βαθμό συμπλοκότητας σε άμεση συνάρτηση με αυτή του συστήματος.

3^η συνιστώσα : Δεδομένα

Τα δεδομένα, όπως αναφέρθηκε και παραπάνω, είναι μια παράσταση γεγονότων, εννοιών ή εντολών σε τυποποιημένη μορφή που είναι κατάλληλη για επικοινωνία, ερμηνεία ή επεξεργασία από άνθρωπο ή από αυτόματα μέσα. Το είδος των δεδομένων που εισάγει / εξάγει ένα πληροφοριακό σύστημα εξαρτάται στενά τόσο από τις απαιτήσεις των χρηστών του πληροφοριακού συστήματος, όσο και από τη δυνατότητα της τεχνολογίας να τις ικανοποιήσει.

4^η συνιστώσα : Λογισμικό

Το λογισμικό ενός Πληροφοριακού μπορεί να ταξινομηθεί σε τρεις μεγάλες κατηγορίες : (α) στο λογισμικό του συστήματος (system software) όπου ανήκουν τα προγράμματα που φτιάχνονται από τον κατασκευαστή του υλικού και αγοράζονται μαζί με αυτό είτε χωριστά, (β) στο λογισμικό των εφαρμογών (application software) όπου ανήκουν τα προγράμματα που γράφονται για να υποστηρίξουν γενικές ή συγκεκριμένες εφαρμογές και απαιτούν το λογισμικό του συστήματος για την εκτέλεσή τους, και (γ) στο λογισμικό που αυξάνει την παραγωγικότητα (productivity software) και περιλαμβάνει όλο το λογισμικό εκείνο που στοχεύει στο να διευκολυνθεί ο ίδιος ο χρήστης να δημιουργήσει μόνος του νέες εφαρμογές.

5^η συνιστώσα : Υλικό

Ένα Πληροφοριακό Σύστημα μπορεί να επεξεργάζεται δεδομένα τα οποία δίνονται / ή ζητούνται σε διάφορες μορφές. Είναι φανερό ότι ο υλικός εξοπλισμός του συστήματος έχει στενή σχέση τόσο με την επεξεργασία, όσο και με το είδος των δεδομένων που εισάγονται / εξάγονται.

Στο σημείο αυτό πρέπει να τονιστεί ότι το Πληροφοριακό Σύστημα δεν πρέπει να εξετάζεται μόνο του. Εντάσσεται μέσα σε κάποιο ευρύτερο πλαίσιο, το οποίο είναι συνήθως η επιχείρηση ή ο οργανισμός, τις λειτουργίες των οποίων υποστηρίζει. Ως Οργανισμός ορίζεται «ένα σύνολο από ανθρώπους που μέσα από συντονισμένες ενέργειες επιδιώκουν την επίτευξη ενός συγκεκριμένου στόχου». Αποτελείται από επιμέρους υποσυστήματα, που καθένα από αυτά μπορεί να αποτελέσει ένα ξεχωριστό Πληροφοριακό Σύστημα μες την επιχείρηση, και η κουλτούρα του είναι διαρκώς μεταβαλλόμενη, δύσκαμπτη σε αλλαγές, ιστορικά καθορισμένη, έμφυτη και ολιστική. Το πλαίσιο αυτό είναι γνωστό ως περιβάλλον του Πληροφοριακού Συστήματος, παίζει σημαντικό ρόλο στη λειτουργία του και γι' αυτό πρέπει να εξετάζεται παράλληλα με αυτό.

2.1.2 Ασφάλεια Πληροφοριακών Συστημάτων

Η έννοια της Ασφάλειας των Πληροφοριακών Συστημάτων έχει δεχτεί πολλαπλές ερμηνείες. Στην παρούσα διπλωματική εργασία υιοθετούμε αυτή του Κιουντούζη [Κιουντούζης]. “Η Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.” Ο ορισμός δίνει έμφαση όχι μόνο στο Πληροφοριακό Σύστημα ως ολότητα αλλά και στα επιμέρους στοιχεία του, ενώ η προφύλαξή του σχετίζεται με κάθε είδους απειλή (τυχαία ή σκόπιμη). Η ασφάλεια του Πληροφοριακού Συστήματος συνδέεται άμεσα τόσο με τις τεχνικές, τις διαδικασίες και τα διοικητικά μέτρα όσο και με ηθικοκοινωνικές αντιλήψεις, αρχές και παραδοχές.

Η Ασφάλεια Πληροφοριών αναφέρεται αποκλειστικά στην προστασία των πληροφοριών και είναι στενότερη έννοια από αυτή της Ασφάλειας του Πληροφοριακού Συστήματος μιας και εμπεριέχεται σε αυτό. Βέβαια η ασφάλεια πληροφοριών δεν μπορεί να αγνοήσει το Πληροφοριακό Σύστημα, μιας και αυτό

είναι υπεύθυνο για την επεξεργασία του. Συμπερασματικά, για την Ασφάλεια ενός Πληροφοριακού Συστήματος ενδιαφερόμαστε για την προστασία όλων των συνιστώσων που το απαρτίζουν, ενώ όταν αναφερόμαστε στην Ασφάλεια Πληροφοριών, η ασφάλεια του υλικού μας ενδιαφέρει μόνο στο βαθμό που σχετίζεται με την προστασία των πληροφοριών.

Στη συνέχεια θα αναφερθούμε στα βασικά χαρακτηριστικά της Ασφάλειας Πληροφοριών μιας και οι αναφορές σε αυτή και τις ιδιότητές της στην παρούσα Διπλωματική Εργασία είναι άμεσες και είναι αποτελεσματικότερο να είναι σαφώς ορισμένες. Άλλωστε σε κάθε ειδική περίπτωση που μελετάμε θα πρέπει να ορίζουμε με σαφήνεια τις συγκεκριμένες ιδιότητες της πληροφορίας που καλούμαστε να προστατέψουμε Έτσι ορίζονται [Γκρίτζαλης]:

Ασφάλεια Πληροφοριών (Information Security) είναι ο συνδυασμός της Εμπιστευτικότητας, της Εγκυρότητας, της Αυθεντικότητας, της Ακεραιότητας και της Διαθεσιμότητας των Πληροφοριών.

Εμπιστευτικότητα (Confidentiality) είναι η αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη.

Εγκυρότητα (validity) είναι η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Αυθεντικότητα (authenticity) είναι η αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.

Ακεραιότητα (integrity) είναι η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Διαθεσιμότητα (availability) είναι η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.

Κύριο χαρακτηριστικό των παραπάνω επιμέρους ορισμών είναι πως αποτελούν αρνητικούς ορισμούς και αυτό συμβαίνει γιατί όταν αναφερόμαστε σε ασφάλεια στο μυαλό μας έρχονται πράγματα που δε θέλουν να συμβούν.

2.2 Υποδομή Δημόσιου Κλειδιού

Για να μπορεί να παρέχει ένας Οργανισμός τις βασικές και τις προστιθέμενης αξίας υπηρεσίες στην Υποδομή Δημόσιου Κλειδιού με τη χρήση των ψηφιακών πιστοποιητικών και των ψηφιακών υπογραφών απαιτείται η χρήση κρυπτογραφικών τεχνικών. Με τη χρήση αυτών ικανοποιούνται οι περισσότερες των απαιτήσεων των

χρηστών για τη σωστή και άρτια λειτουργία των υπηρεσιών. Επομένως, κρίνεται χρήσιμη μια σύντομη ανασκόπηση των παραπάνω εννοιών για την αρτιότερη προσέγγιση.

2.2.1 Βασικές εννοιες Κρυπτογραφικών Συστημάτων

Η κρυπτολογία (cryptology) σχετίζεται με τη μυστικότητα και την ακεραιότητα των πληροφοριών και περιλαμβάνει τις εννοιες της κρυπτογραφίας (cryptography) και της κρυπτανάλυσης (cryptanalysis). Η κρυπτογραφία είναι η τεχνική δημιουργίας και χρήσης κρυπτοσυστημάτων (cryptosystems) με τη χρήση των οποίων κρυπτογραφούνται και αποκρυπτογραφούνται πληροφορίες. Η κρυπτανάλυση είναι η τεχνική παραβίασης των κρυπτοσυστημάτων, δηλαδή η προσπάθεια μη εξουσιοδοτημένων οντοτήτων να ανακτήσουν τις πληροφορίες που περιέχονται σε ένα κρυπτογραφημένο μήνυμα, χωρίς να γνωρίζουν τις αντίστοιχες μεθόδους αποκρυπτογράφησης.

Η κρυπτογραφία συναντάται με τον αγγλικό όρο cipher, ο οποίος προέρχεται από την αραβική λέξη Al Sifr που σημαίνει μηδέν και υποδεικνύει την πλήρη απόκρυψη των πληροφοριών που περιέχονται σε ένα κείμενο. Η κρυπτογράφηση (encryption) είναι η μέθοδος με την οποία ένα σύνολο δεδομένων μετασχηματίζεται σε μη αναγνώσιμη μορφή, έτσι ώστε μόνο κάποιος που γνωρίζει τον αλγόριθμο αποκρυπτογράφησης να μπορεί να έχει πρόσβαση στο αρχικό περιεχόμενο των δεδομένων. Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούνται για το μετασχηματισμό του αρχικού κειμένου σε κρυπτογραφημένο κείμενο (ciphertext) με τη χρήση μίας συγκεκριμένης ακολουθίας χαρακτήρων ή δυαδικών αριθμών που ονομάζεται κλειδί (key). Η αντίστροφη διαδικασία μετατροπής του κρυπτογραφημένου κειμένου στο αρχικό κείμενο είναι η αποκρυπτογράφηση (decryption) και απαιτείται κάποιος να γνωρίζει το αρχικό κλειδιού.

Κύριο χαρακτηριστικό των κρυπτογραφικών συστημάτων είναι οι μονόδρομες συναρτήσεις.. Κύρια ιδιότητά τους είναι ότι αν και είναι εύκολο να παράγουν ένα αποτέλεσμα εφαρμοζόμενες σε κάποιο στοιχείο, είναι εξαιρετικά δύσκολο να αντιστραφούν. Μία συνάρτηση $f : A \rightarrow B$ χαρακτηρίζεται ως μονόδρομη, αν η τιμή $f(x)$ είναι «εύκολο» να υπολογισθεί $\forall x \in A$, αλλά είναι «υπολογιστικά ανέφικτο» όταν δοθεί το $y \in f(A)=B$, να βρεθεί $x \in A$ έτσι ώστε $f(x)=y$. Η παραπάνω διατύπωση δεν είναι μαθηματικά ακριβής, αφού υπεισέρχεται η σχετικότητα που περιέχουν οι

όροι «εύκολο» και «υπολογιστικά ανέφικτο». Η μαθηματική τεκμηρίωση των μονόδρομων συναρτήσεων δεν έχει ακόμα και σήμερα απόλυτα αποδειχθεί.

2.2.2 Ασύμμετρη κρυπτογραφία

Είναι κύριο χαρακτηριστικό των κρυπτογραφικών τεχνικών δημόσιου κλειδιού (public key cryptography). Απαιτείται η χρήση ενός δημόσιου κλειδιού (public key) το οποίο είναι γνωστό και διαθέσιμο σε όλους τους χρήστες μέσω καταλόγων ευρετηρίου και ένα ιδιωτικό κλειδί (private key) που είναι μυστικό και το γνωρίζει μία μόνο συγκεκριμένη οντότητα – χρήστης. Η τυπική χρήση του ζεύγους κλειδιών είναι η κρυπτογράφηση ενός κειμένου με το δημόσιο κλειδί μιας οντότητας και η αποκρυπτογράφησή του με το ιδιωτικό κλειδί.

Αν συμβολίσουμε με (p,s) το ζεύγος των κλειδιών όπου p είναι το δημόσιο (public) κλειδί και s είναι το ιδιωτικό (secret) κλειδί, στα ασύμμετρα συστήματα ισχύουν :

- $D(s, E(p,t)) = t = E(p, D(s,t))$ αλλά και $D(sE(s,t)) \neq t \neq E(p, D(p,t))$, όπου $D(x)$ είναι η συνάρτηση αποκρυπτογράφησης , $E(x)$ η συνάρτηση κρυπτογράφησης και t το κείμενο.
- Ο υπολογισμός των $E(p,t)$ και $D(s,c)$ πρέπει να είναι υπολογιστικά εύκολος.
- Χωρίς τη γνώση του s είναι υπολογιστικά ανέφικτος ο υπολογισμός του t δοθέντων των $c=E(p,t)$ και του p .
- Είναι υπολογιστικά ανέφικτος ο υπολογισμός του s δοθέντος του p .

Χαρακτηριστικά παραδείγματα ασύμμετρων κρυπτοσυστημάτων είναι τα Rivest-Shamir-Adleman (RSA) [Rivest], Diffie-Hellmann [Diffie-Hellmann], ElGamal [ElGamal] και Rabin [Rabin]

2.2.3 Συμμετρική κρυπτογραφία

Στη συμμετρική κρυπτογραφία (symmetric encryption) ισχύει $p = s$ για το ζεύγος κλειδιών κρυπτογράφησης και αποκρυπτογράφησης, δηλαδή χρησιμοποιείται ένα κοινό μυστικό κλειδί (secret key) το οποίο γνωρίζουν και τα δύο μέρη. Το κοινό κλειδί s χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση του κειμένου t , δηλαδή ισχύει $D(s, E(s,t)) = t = E(s, D(s,t))$. Σε σχέση με τα ασύμμετρα συστήματα, τα συμμετρικά μετασχηματίζουν τα δεδομένα σε πολλαπλάσιες ταχύτητες και για αυτό το λόγο προτιμούνται στην κρυπτογράφηση μεγάλου όγκου

δεδομένων. Μια δεύτερη διαφορά τους είναι πως τα συμμετρικά συστήματα μπορούν να περιλαβούν στην επικοινωνία περισσότερα από δύο μέρη, δηλαδή όλους όσους γνωρίζουν το μυστικό κλειδί, σε αντίθεση με τα συμμετρικά όπου οι συναλλασσόμενοι είναι αυστηρά δύο.

Οι πιο γνωστοί συμμετρικοί αλγόριθμοι είναι οι Data Encryption Standard (DES) και triple-DES [NBS88], International Data Encryption Algorithm (IDEA) [Lai92] και η σειρά RC2, RC4, RC5 [Rives95].

2.2.4 Ψηφιακές Υπογραφές

Σύμφωνα με την Directive 1999/93/EC [Directive 1999/93/EC] η ηλεκτρονική υπογραφή υποδηλώνει κάποια δεδομένα σε ηλεκτρονική μορφή τα οποία σχετίζονται ή είναι λογικά συνδεδεμένα με κάποια άλλα δεδομένα και εξυπηρετούν τη διαδικασία αυθεντικοποίησης του αποστολέα. Μία ανώτερη ψηφιακή υπογραφή είναι μία ηλεκτρονική υπογραφή με τις εξής ιδιότητες :

- Σχετίζεται μοναδικό με τον υπογράφοντα.
- Παρέχει τη δυνατότητα για αναγνώριση του υπογράφοντα.
- Παράγεται από μέσα απόλυτα ελεγχόμενα από τον υπογράφοντα.
- Συνδέονται με τα υπογραφόμενα δεδομένα σε τέτοιο βαθμό που οποιαδήποτε αλλαγή γίνει στα μεταφερόμενα / απεσταλμένα δεδομένα, αυτή μπορεί να ανιχνευθεί άμεσα.

Για την παραγωγή των ψηφιακών υπογραφών χρησιμοποιούνται οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι και οι συναρτήσεις σύνοψης. Οι συναρτήσεις σύνοψης (hash functions) είναι συναρτήσεις που δέχονται σαν είσοδο ένα κείμενο ή μια σειρά από δυαδικά δεδομένα και επιστρέφει ένα σημαντικά μικρότερο διάνυσμα δυαδικών δεδομένων. Οι πιο διαδεδομένοι αλγόριθμοι σύνοψης είναι οι MD5, ο SHA-1 και ο RIPEMD-160. Για να καταστήσουμε πιο κατανοητή τη λειτουργία των ψηφιακών υπογραφών, θα αναφερθούμε σε ένα συγκεκριμένο παράδειγμα που ο αποστολέας θέλει να υπογράψει ψηφιακά ένα μήνυμα και να το στείλει σε μια άλλη οντότητα, τον παραλήπτη. Η διαδικασία περιλαμβάνει τα παρακάτω βήματα :

1. Χρησιμοποιώντας μια προηγούμενα συμφωνημένη συνάρτηση σύνοψης, ο αποστολέας παράγει τη σύνοψη του μηνύματός του.

2. Ο αποστολέας κρυπτογραφεί την παραγόμενη σύνοψη και την στέλνει στον παραλήπτη μαζί με το αρχικό μήνυμα, τη χρησιμοποιούμενη συνάρτηση σύνοψης και ένα πιστοποιητικό που περιλαμβάνει το δημόσιο κλειδί του.
3. Ο παραλήπτης αποκρυπτογραφεί τη σύνοψη του κειμένου με το δημόσιο κλειδί του αποστολέα.
4. Ο παραλήπτης αναπαράγει τη σύνοψη του αρχικού κειμένου.
5. Ο παραλήπτης συγκρίνει τα παραπάνω δύο αποτελέσματα και αν είναι τα ίδια συμπεραίνει πως η υπογραφή είναι έγκυρη, το μήνυμα δεν τροποποιήθηκε κατά τη μετάδοσή του ενώ από την άλλη ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του συγκεκριμένου μηνύματος.

Όπως προκύπτει από τα παραπάνω η κύρια χρήση των ψηφιακών υπογραφών είναι για την παροχή ισχυρής αυθεντικοποίησης του αποστολέα, της ακεραιότητας του αρχικού μηνύματος κατά τη μετάδοσή του και τη μη αποποίηση της αποστολής του από τη μεριά του αποστολέα, ενώ κύριο χαρακτηριστικό τους είναι η ευκολία και η ταχύτητα στην παραγωγή και την επαλήθευση τους.

2.2.5 Ψηφιακά Πιστοποιητικά

Ένα ψηφιακό πιστοποιητικό είναι μία ηλεκτρονική επικύρωση ενός εγγράφου η οποία συνδέει κάποια υπογραφόμενα δεδομένα (π.χ. ένα δημόσιο κλειδί) με μια οντότητα και πιστοποιεί την ταυτότητα της οντότητας. Τα κύρια στοιχεία ενός πιστοποιητικού είναι :

- Το όνομα του υποκειμένου του αναφερόμενου πιστοποιητικού και άλλες πληροφορίες. Όταν το υποκείμενο πρόκειται για πρόσωπο τότε αναφέρονται πληροφορίες για το όνομα του, την εθνικότητά του, την ηλεκτρονική του διεύθυνση, τον οργανισμό που ανήκει ενώ μπορεί να περιέχονται και επιπλέον δεδομένα όπως τα αποτυπώματά του, η εθνικότητα κ.τ.λ.
- Πληροφορία για το δημόσιο κλειδί. Είναι το δημόσιο κλειδί της οντότητας που πιστοποιείται και χρησιμοποιείται για να το συνδέσει με τις παραπάνω πληροφορίες της πιστοποιούμενης αοντότητας.
- Η υπογραφή του Οργανισμού Πιστοποίησης του (Certification Authority). Χρησιμοποιείται για την υπογραφή των παραπάνω δύο στοιχείων, έτσι ώστε

αυτός που θα το λάβει να μπορεί να ελέγξει την αξιοπιστία του και επομένως να το κάνει αποδεκτό ή όχι.

- Κάποια συμπληρωματικά στοιχεία όπως οι χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης, πληροφορίες για την Αρχή Έκδοσής του, το μέγεθος των κλειδιών και τη χρονική του ισχύ.

Στη συνέχεια αναφέρουμε ένα παράδειγμα ενός ψηφιακού πιστοποιητικού όπως περιγράφεται στο πρότυπο X.509.

Certificate:

Data:

Version: 3 (0x0)

Serial Number: 2003532 (0x0)

Signature Algorithm: md5withRSAEncryption

Issuer: C=GR, L=Athens, O=University of Economics And Business

OU=Certification Authority, CN=ca.aueb.gr,

Email=ca@aueb.gr

Validity

Not Before: Nov 01 17:15:25 2003 GMT

Not After : Dec 31 17:15:25 2003 GMT

Subject: C=GR, L=Athens, O= University of Economics And Business,

OU=aueb, CN=rentas,

Email=rentas@aueb.gr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Modulus:

00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:

55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:

61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:

45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:

a5:94:ac:8a:67

Exponent: 65537 (0x10001)

Key Usage: Digital Signature, Key Encipherment,

Client Authentication

Signature Algorithm: md5withRSAEncryption

7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:

54:39:80:7b:b9:d9:49:b3:b2:2a:fe:8a:52:f4:c2:89:0e:5c:

7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:01:bc:40:

ee:bc:0e:fe:fc:f8:9b:9d:70:e3

Τα ψηφιακά πιστοποιητικά πρέπει να είναι όσο το δυνατό πιο κατανεμημένα και διαθέσιμα σε οποιονδήποτε που θέλει να πιστοποιήσει την ψηφιακή υπογραφή μιας οντότητας ή να της στείλει ένα κρυπτογραφημένο μήνυμα. Δεν περιέχουν καμία εμπιστευτική πληροφορία ενώ το περιεχόμενό τους δεν μπορεί να τροποποιηθεί από τη στιγμή που είναι ψηφιακά υπογεγραμμένο από την Αρχή Πιστοποίησης.

Στις σημερινές Υποδομές Δημόσιου Κλειδιού διακρίνουμε διαφορετικά είδη ψηφιακών πιστοποιητικών :

- Πιστοποιητικό ταυτότητας (identity certificate): είναι το παραπάνω περιγεγραμμένο πιστοποιητικό.
- Πιστοποιητικό εξυπηρέτη (server certificate) : έχει την ίδια δομή με το πιστοποιητικό ταυτότητας αλλά η λειτουργία του είναι για την αυθεντικοποίηση του εξυπηρέτη προς τις άλλες οντότητες.
- Πιστοποιητικό ρόλων (role certificate) : το περιεχόμενο δημόσιο κλειδί χρησιμοποιείται για τη σύνδεση με ένα ρόλο του παρεχόμενου Πληροφοριακού Συστήματος και όχι με ένα φυσικό ρόλο.
- Πιστοποιητικό ιδιοτήτων (attribute certificate) : αντιστοιχίζει την ταυτότητα του ιδιοκτήτη του ή το πιστοποιητικό ταυτότητάς του σε ένα σύνολο από ιδιότητες όπως η συμμετοχή σε ρόλους ή ομάδες και η παραχώρηση δικαιωμάτων χρήσης.
- Πιστοποιητικό ομάδας (group certificate) : πιστοποιεί τη συμμετοχή κάποιων φυσικών οντοτήτων σε μια ομάδα και η χρησιμοποιούμενη υπογραφή μπορεί να χρησιμοποιηθεί από όλα τα μέλη της ομάδας.
- Πιστοποιητικό proxy : είναι ένα ειδικό μικρής διάρκειας πιστοποιητικό δημιουργημένο και υπογεγραμμένο από την ίδια την οντότητα.
- Προσωρινό πιστοποιητικό (temporary certificate): είναι ένα proxy πιστοποιητικό που δημιουργείται όμως από μια Έμπιστη Οντότητα.

2.3 Συμπεράσματα

Η χρήση του όρου των Πληροφοριακών Συστημάτων στην παρούσα διπλωματική εργασία έχει δύο όψεις : υποστηρικτική στη λειτουργία του Οργανισμού που παρέχει υπηρεσίες Υποδομής Δημόσιου Κλειδιού και προστασίας των χαρακτηριστικών της Ασφάλειας των Πληροφοριών του. Το Πληροφοριακό Σύστημα

που χρησιμοποιεί Η/Υ είναι ένα οργανωμένο σύνολο από πέντε αλληλεπιδρώντων στοιχείων που επεξεργάζεται δεδομένα και παράγει πληροφορίες μιας Επιχείρησης ή ενός Οργανισμού. Οι πέντε συνιστώσες του πληροφοριακού συστήματος είναι : άνθρωποι, διαδικασίες (procedures, methods), δεδομένα (data), λογισμικό (software) και υλικός εξοπλισμός (hardware).

Σημαντικός είναι ο ρόλος των κρυπτογραφικών τεχνικών για την παροχή των υπηρεσιών Υποδομής Δημόσιου Κλειδιού από έναν Οργανισμό. Οι χρησιμοποιούμενες τεχνολογίες είναι κατά βάση τα ασύμμετρα και συμμετρικά κρυπτοσυστήματα, οι αλγόριθμοι σύνοψης, οι ψηφιακές υπογραφές και τα διαφορετικά είδη από εκδιδόμενα πιστοποιητικά.

Αναφορές

1. Diffie W., Hellmann M., "New directions in Cryptography", IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.644-654, 1976
2. Directive 1999/93/EC του Ευρωκοινοβουλίου και του Συμβουλίου της 13^{ης} Δεκέμβρης για τη δημιουργία ενός Κοινωνικού Πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών.
3. ElGamal T., "Cryptography and logarithms over finite fields", Phd Thesis, Stanford University
4. Paton, G. (1997), "Information System' as Intellectual Construct – Its Only Valid Form", *Systems Research and Behavioural Science*, Vol. 14, No. 1, pp. 67-72
5. Rabin M.O., "Digitalized signatures" Foundations of Secure Computation, pp.155-168, Academic Press, 1978
6. Rivest R., Shamir A., Adleman L., "A method for obtaining Digital Signatures and Public-Key Cryptosystems Public-Key Cryptosystems", Communications of the ACM, No.21(2), pp.120-126, 1978
7. Γκρίτζαλης Δ., Ασφάλεια στις Τεχνολογίες Πληροφοριών και Επικοινωνιών, Εννοιολογική θεμελίωση, INFOSEC laboratory, Οκτώβριος 2001
8. Κιουντούζης, Μεθοδολογίες Ανάλυσης και Σχεδιασμού Π.Σ., Μπένος 1997

Κεφάλαιο 3 Τεχνολογικό Υπόβαθρο

3.1 Βασικά χαρακτηριστικά Υποδομής Δημόσιου Κλειδιού

3.1.1 Μοντέλο Αναφοράς

Η Υποδομή Δημόσιου Κλειδιού ορίζεται σαν «ένα σύνολο από υλικό, λογισμικό, ανθρώπους, πολιτικές και διαδικασίες που χρειάζονται για τη δημιουργία, αποθήκευση, διανομή και ανάκληση ψηφιακών πιστοποιητικών δημόσιου κλειδιού». Το Σχήμα 3.1 αναπαριστά την αρχιτεκτονική μιας τέτοιας υποδομής όπου τα βασικά συστατικά της ομαδοποιούνται στις παρακάτω λειτουργικές κατηγορίες :

- **Υπηρεσίες Ενεργοποίησης της Ασφάλειας του Συστήματος (System Security Enabling Services) :** παρέχουν την απαραίτητη λειτουργικότητα που επιτρέπουν στο χρήστη ή άλλη οντότητα να αυθεντικοποιείται στο σύστημα με ασφαλείς διαδικασίες
- **Κρυπτογραφικές Αρχές και Μονάδες (Cryptographic Primitives) :** παρέχουν εκείνα τα συστατικά (components) για την πρόσβαση σε χαμηλού επιπέδου κρυπτογραφικές λειτουργίες όπως τη δημιουργία κλειδιών, τη χρήση των συναρτήσεων σύνοψης και των αλγορίθμων κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων κ.τ.λ.
- **Κρυπτογραφικές Υπηρεσίες (Cryptographic Service Components) :** παρέχουν την πρόσβαση σε κρυπτογραφικές συναρτήσεις για την ακεραιότητα των μετακινούμενων δεδομένων, τη διασφάλιση της ιδιωτικότητας, την παραγωγή των ψηφιακών υπογραφών, την ανάκτηση των ιδιωτικών κλειδιών των αυθεντικοποιημένων οντοτήτων κ.τ.λ. Οι λειτουργίες αυτές στηρίζονται στις Κρυπτογραφικές Αρχές που αναφέρθηκαν παραπάνω.
- **Υπηρεσίες Διαχείρισης Κλειδιών (Long-term Key Services) :** παρέχουν όλες εκείνες τις βασικές λειτουργίες για τη διαχείριση των δημόσιων και ιδιωτικών κλειδιών των εμπλεκόμενων οντοτήτων σε μια συναλλαγή και τη διαχείριση των εκδομένων από τον Οργανισμό πιστοποιητικών.
- **Πρωτόκολλα Υπηρεσιών Ασφαλείας (Protocol Security Services) :** παρέχουν την ασφαλή λειτουργικότητα (αυθεντικοποίηση προέλευσης δεδομένων, προστασία ακεραιότητας δεδομένων, προστασία ιδιωτικότητας

δεδομένων, μη-αποποίηση) απαραίτητη την υποστήριξη των ασφαλών πρωτοκόλλων.

- **Ασφαλή Πρωτόκολλα (Secure Protocols)** : παρέχουν την ασφαλή διασύνδεση μεταξύ μη ασφαλών εφαρμογών.
- **Πολιτικές Ασφάλειας (Security Policy Services)**: χρησιμοποιούνται για τον καθορισμό των πολιτικών του Οργανισμού της λειτουργίας των Ασφαλών πρωτοκόλλων και της παροχής των Βασικών και των Δευτερευόντων του υπηρεσιών.
- **Υποστηρικτικές Υπηρεσίες (Supporting Services)**: παρέχουν την λειτουργικότητα των υπηρεσιών που δεν περιλαμβάνονται στις Πολιτικές Ασφάλειας



Σχήμα 3.1 Μοντέλο Αναφοράς ΥΔΚ

3.1.2 Απαιτήσεις χρηστών

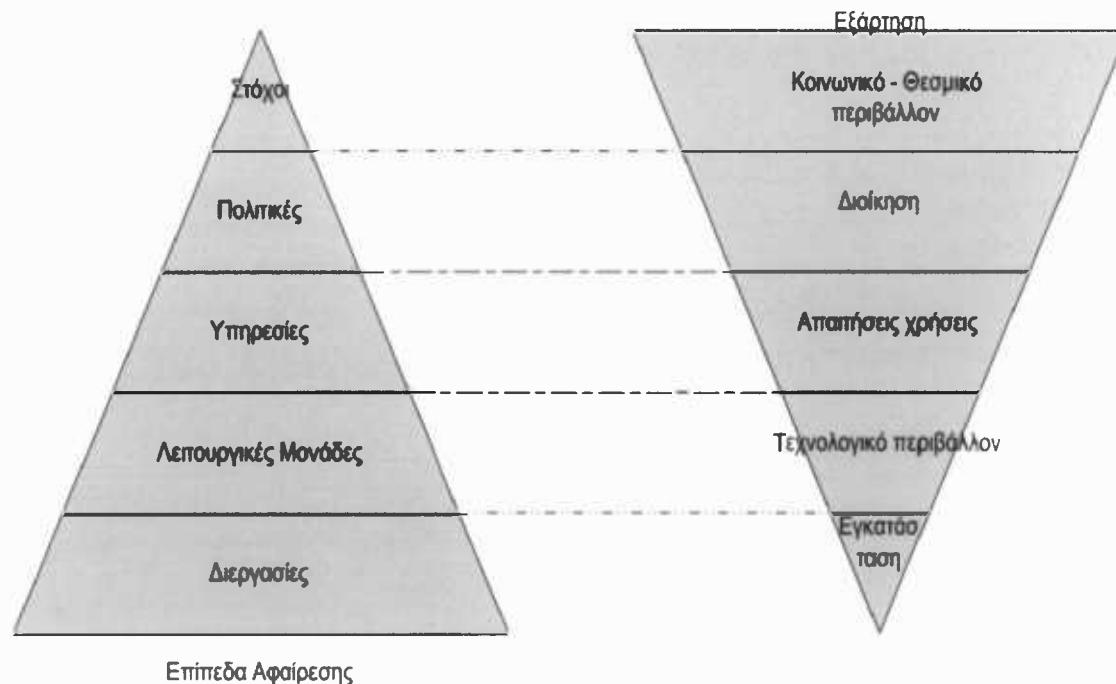
Στην παράγραφο αυτή θα αναφερθούμε σε ένα σύνολο από απαιτήσεις για την εύρυθμη λειτουργία ενός Οργανισμού που παρέχει υπηρεσίες Υποδομής Δημόσιου Κλειδιού όπως αυτές αναδεικνύονται μέσα από κοινωνικές, οργανωτικές και τεχνολογικές συνθήκες. Η βασική κατηγοριοποίηση είναι η ακόλουθη [Λέκκας]:

- **Απαιτήσεις Ασφάλειας :** σχετίζονται με την προστασία των βασικών χαρακτηριστικών της Ασφάλειας των Πληροφοριών. Η εμπιστευτικότητα σχετίζεται με την αποφυγή αποκάλυψης των πληροφοριών χωρίς την άδεια του ιδιοκτήτη και η εγκυρότητα με την απόλυτη ακρίβειά τους. Η ικανοποίηση τους στηρίζεται στην κρυπτογράφηση με τη χρήση των συμμετρικών αλγορίθμων. Η ακεραιότητα των δεδομένων σαν απαίτηση ασφάλειας σχετίζεται με την αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών και συνδέεται άμεσα με την αυθεντικοποίηση των οντοτήτων σε μια υλοποιούμενη υποδομή. Λύση στη συγκεκριμένη απαίτηση δίνουν οι ηλεκτρονικές υπογραφές και η απόδειξη της κατοχής του ιδιωτικού κλειδιού.
- **Λειτουργικές απαιτήσεις :** εδώ εντοπίζουμε την ανάγκη για την υψηλή διαθεσιμότητα των κρίσμων και μη πληροφοριών που σχετίζεται άμεσα με την απαίτηση από τη μεριά του Οργανισμού για επενδύσεις σε υλικό και λογισμικό, την ανάγκη για διαλειτουργικότητα, επεκτασιμότητα και λειτουργικότητα των παρεχόμενων υπηρεσιών. Οι διεπαφές πρέπει να ιδιαίτερα φιλικές προς τον τελικό χρήστη, να απευθύνονται σε ένα μεγάλο αριθμό χρηστών, να παρέχεται η δυνατότητα τεχνικής υποστήριξης αλλά και να εκτείνονται περά από τα στενά όρια της γεωγραφικής επικράτειας του Οργανισμού.
- **Οργανωτικές απαιτήσεις :** διακρίνονται τις απαιτήσεις για ισχυρά Πληροφοριακά Συστήματα από τη μεριά του Οργανισμού, την ανάγκη για ύπαρξη της δήλωσης για Πολιτική Ασφάλειας και πρακτικής πιστοποίησης που συμβαδίζουν με τα διεθνή πρότυπα και εξασφαλίζουν την ποιότητα των παρεχόμενων υπηρεσιών και τέλος, την απαίτηση για την ύπαρξη μιας Ανεξάρτητης Αρχής που σαν κύριο σκοπό έχει την επιθεώρηση της λειτουργίας και της ανταπόκρισης του Οργανισμού προς τα παραπάνω.

- **Κοινωνικές απαιτήσεις** : διακρίνουμε την ανάγκη για εδραίωση της αμοιβαίας εμπιστοσύνης μεταξύ των συναλλαγόμενων οντοτήτων, τη νομική κατοχύρωση πως τόσο οι ηλεκτρονικές συναλλαγές των χρηστών προστατεύονται με επάρκεια όσο και τα προσωπικά δεδομένα διαφυλάσσονται σύμφωνα με την ισχύουσα νομοθεσία στη χώρα την οποία δραστηριοποιείται ο Οργανισμός.
- **Ειδικές απαιτήσεις** : αποτελούν το μεγαλύτερο μέρος των παρεχόμενων υπηρεσιών Προστιθέμενης Αξίας και τις οποίες θα αναλύσουμε στο επόμενο κεφάλαιο. Ενδεικτικά αναφέρουμε την απαίτηση για ανωνυμία, χρονοσήμανση, απόδειξη του δικαιούχου ενός εγγράφου και τη διαχείριση των δικαιωμάτων και εξουσιοδότησης.

3.2 Παρεχόμενες Υπηρεσίες σε Υποδομή Δημόσιου Κλειδιού

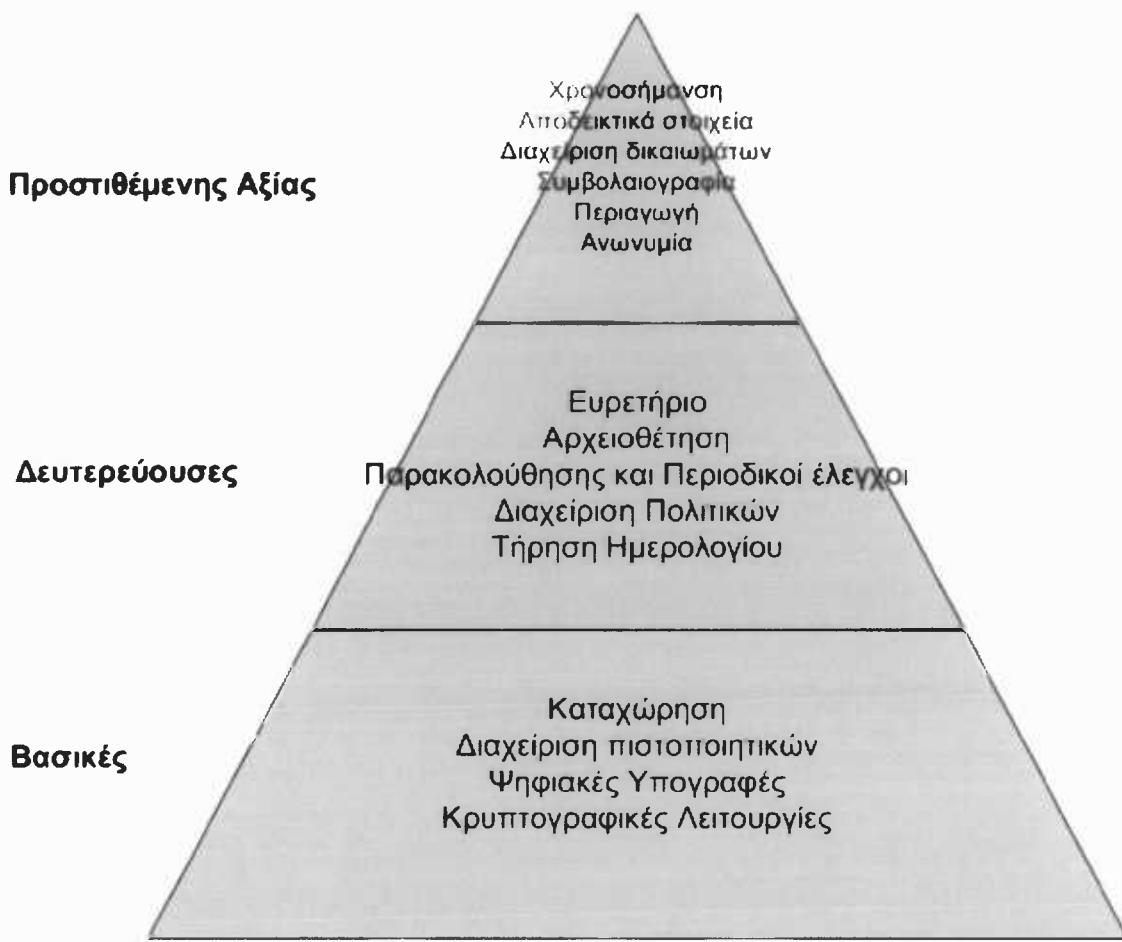
Οι παρεχόμενες υπηρεσίες από έναν Οργανισμό μπορούν να προσεγγισθούν με τη βοήθεια πέντε επιπέδων αφαίρεσης που επηρεάζονται σαφώς από περιβαλλοντικούς και κοινωνικούς παράγοντες που δραστηριοποιείται ένας Οργανισμός, όπως διατυπώθηκε από τον Kowalski [Kowalski]. Η σχηματική αναπαράσταση των επιπέδων αφαίρεσης απεικονίζεται στο Σχήμα 3.2 :



Σχήμα 3.2 Επίπεδα αφαίρεσης και εξαρτήσεις

Στο ανώτερο τμήμα της πυραμίδας, ενδεικτικής της σημασίας τους σε έναν Οργανισμό, είναι οι Στόχοι του όπως αυτοί διατυπώνονται μέσα από τις πρακτικές και την Πολιτική Ασφάλειας. Σαφώς όμως οι στόχοι βρίσκονται σε άμεση εξάρτηση από τους κοινωνικοθεσμικούς παράγοντες του χώρου δραστηριοποίησης του Οργανισμού. Στο επόμενο επίπεδο βρίσκονται οι Πολιτικές, απόρροια των γενικών στόχων που επηρεάζονται άμεσα από τις αποφάσεις τις Διοίκησης, ενώ ένα επίπεδο πιο κάτω διακρίνουμε τις Υπηρεσίες. Οι Υπηρεσίες αποτελούν την εξειδίκευση των στόχων και των πολιτικών με σκοπό την ικανοποίηση των απαιτήσεων χρήσης. Οι απαιτήσεις χρήσης για μια Υποδομή Δημόσιου Κλειδιού αναλύθηκαν στην §3.1.2 και με γνώμονα αυτές θα κατηγοριοποιήσουμε τις Υπηρεσίες στην επόμενη παράγραφο. Οι λειτουργικές μονάδες χρησιμοποιούνται για την υποστήριξη των υπηρεσιών και εξαρτώνται άμεσα από το διαμορφωμένο και προτυποποιημένο τεχνολογικό περιβάλλον. Στο τελευταίο επίπεδο διακρίνουμε τις αναδυόμενες διεργασίες από τη χρήση των λειτουργικών μονάδων για μια συγκεκριμένη εγκατάσταση.

Η έννοια των υπηρεσιών από έναν τέτοιο Οργανισμό είναι κάτι περισσότερο από την υλοποίηση των απαιτήσεων των συναλλασσόμενων οντοτήτων. Σύμφωνα με το ISO-8402 ορίζονται ως «το αποτέλεσμα που παράγεται από δραστηριότητες που λαμβάνουν χώρα στη διεπαφή μεταξύ παρόχου και πελάτη και από τις εσωτερικές δραστηριότητες του παρόχου που έχουν στόχο να ικανοποιήσουν τις ανάγκες του πελάτη.» Στην Υποδομή Δημόσιου Κλειδιού διακρίνονται τριάντα ειδών κατηγορίες υπηρεσιών (όπως φαίνεται και στο σχήμα 3.3)



Σχήμα 3.3 Ταξινόμηση των υπηρεσιών

3.2.1 Βασικές Υπηρεσίες

Αποτελούν το βασικό πυρήνα των υπηρεσιών ενός τέτοιου Οργανισμού. Εδώ διακρίνουμε τις παρακάτω υπηρεσίες :

- **Καταχώρηση:** περιλαμβάνει το σύνολο των λειτουργιών που παρέχονται από τον Οργανισμό για τη λήψη και επεξεργασία των αιτήσεων έκδοσης πιστοποιητικών, τον έλεγχο της εγκυρότητάς τους, την ασφαλή προώθησή τους προς την υπηρεσία διαχείρισης πιστοποιητικών, τη δημιουργία ζεύγους δημόσιων και ιδιωτικών κλειδιών, την παραγωγή κοινών μυστικών μεταξύ των συναλλασσόμενων οντοτήτων για την υποστήριξη της διαδικασίας αυθεντικοποίησης και την πιστοποίηση της κατοχής από μια οντότητα ενός μυστικού κλειδιού.
- **Διαχείριση πιστοποιητικών :** περιλαμβάνει τη διαχείριση ενός ψηφιακού πιστοποιητικού από τη στιγμή της έκδοσής του ως τη λήξη ισχύος του, την

ανανέωσή του, τον έλεγχο της κατάστασής του ή την ανάκλησή του. Πολλές φορές η υπηρεσία αυτή αναφέρεται και ως η πηγή της Εμπιστοσύνης για μια Υποδομή Δημόσιου Κλειδιού.

- **Κρυπτογραφικές λειτουργίες** : παρέχουν όλες εκείνες οι λειτουργίες για την ασφάλεια των μετακινούμενων ή των αποθηκευμένων δεδομένων. Κύριες χρησιμοποιούμενες δομές είναι οι ψηφιακές υπογραφές και τα κρυπτογραφημένα δεδομένα.

3.2.2 Δευτερεύουσες Υπηρεσίες

Κύρια χρήση των υπηρεσιών αυτών είναι η υποστήριξη της ασφαλής επικοινωνίας μεταξύ του πελάτη και του Οργανισμού και η ομαλή λειτουργία των Βασικών υπηρεσιών. Διακρίνουμε τις παρακάτω υπηρεσίες :

- **Ευρετήριο** : με τη χρήση της συγκεκριμένης υπηρεσίας καταχωρούνται πληροφορίες που είναι δημόσια διαθέσιμες και προσπελάσιμες μέσα από αντίστοιχες διεπαφές.
- **Αρχειοθέτηση**: σχετίζεται με τη δημιουργία και διαχείριση ενός εξελιγμένου συστήματος αρχειοθέτησης και Βάσεων Δεδομένων για την υποστήριξη όλων των υπηρεσιών του Οργανισμού σύμφωνα με τη σχετική νομοθεσία περί προστασίας της ιδιωτικότητας.
- **Παρακολούθηση και Περιοδικός Έλεγχος** : σχετίζεται με την εξασφάλιση της άρτιας λειτουργίας του Οργανισμού και των εσωτερικών του διαδικασιών σύμφωνα με κάποιους κανόνες και την εφαρμογή του εφαρμόσιμου συστήματος ποιότητας για τη βελτίωση των παρεχόμενων υπηρεσιών.
- **Διαχείριση Πολιτικών** : σχετίζεται με την καταγραφή, την κατανόηση, την ερμηνεία και τη συντήρηση των Πολιτικών και του κανονιστικού πλαισίου του Οργανισμού.
- **Τήρηση ημερολογίου** : με τη χρήση της συγκεκριμένης υπηρεσίας καταγράφονται οι πληροφορίες που σχετίζονται με μια συναλλαγή χωρίς όμως να συμπεριλαμβάνονται απαραίτητα και τα στοιχεία της συναλλαγής μιας και αυτή είναι η λειτουργία της υπηρεσίας των Αποδεικτικών Στοιχείων.

3.2.3 Υπηρεσίες προστιθέμενης αξίας

Στην κατηγορία αυτή ανήκουν όλες εκείνες οι υπηρεσίες που προσδίδουν πρόσθετη αξία στη χρήση των ψηφιακών υπογραφών και πιστοποιητικών και χρησιμοποιούν τις βασικές και τις δευτερεύουσες υπηρεσίες του Οργανισμού. Η μελέτη των υπηρεσιών αυτών είναι το αντικείμενο της παρούσας Διπλωματικής Εργασίας και θα αναφερθούμε αναλυτικά σε αυτές στο επόμενο κεφάλαιο [Κεφάλαιο 4]. Ενδεικτικά αναφέρουμε πως στην κατηγορία αυτή ανήκουν η Χρονοσήμανση, η Συμβολαιογραφία, η Διαχείριση των Δικαιωμάτων, η Παροχή Αποδεικτικών στοιχείων, η Περιαγωγή, η Διατήρηση της Ανωνυμίας και ο συνδυασμός τους με Βιομετρικές μεθόδους Αυθεντικοποίησης.

3.3 Υποδομή Δημόσιου Κλειδιού και Πρότυπα

Στη συγκεκριμένη ενότητα θα αναφερθούμε σε μια σειρά από τεχνολογικά πρότυπα ανεπτυγμένα από διάφορους διεθνείς Οργανισμούς που σχετίζονται άμεσα με τις παρεχόμενες υπηρεσίες ενός Οργανισμού. Σκοπός αυτής της σύντομης παρουσίασης είναι από τη μία να διαφανεί η σημαντικότητά τους για τις παρεχόμενες υπηρεσίες και από την άλλη επειδή στην παρούσα πτυχιακή εργασία θα γίνονται σαφείς αναφορές σε αυτά, ο αναγνώστης να γνωρίζει το τεχνολογικό τους υπόβαθρο και την εν γένει λειτουργικότητά τους.

3.3.1 Πρότυπα Διεθνούς Οργανισμού Πιστοποίησης (International Standards Organization - ISO)

Αποτελεί τον ευρύτερα αποδεκτό Οργανισμό πιστοποίησης και μέχρι σήμερα έχει εκδώσει περισσότερα από 14.000 πρότυπα. Κάποια που μελετήθηκαν για το σκοπό της παρούσας Διπλωματικής Εργασίας είναι τα :

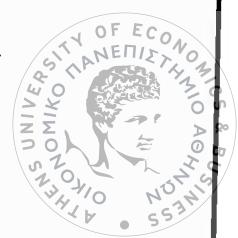
- **ISO /IEC 9594** : περιγράφει τις υπηρεσίες ευρετηρίου που υποστηρίζονται από έναν Οργανισμό. Το τμήμα 8 του συγκεκριμένου προτύπου (σχετικό με την αυθεντικοποίηση) έχει συγχωνευθεί με το πρότυπο X.509 το οποίο θα δούμε παρακάτω.
- **ISO IEC/9798** : περιγράφει μια σειρά από μηχανισμούς που χρησιμοποιούνται για την αυθεντικοποίηση οντοτήτων σε μια Υποδομή Δημόσιου Κλειδιού, δίνοντας κυρίως σημασία στους αλγορίθμους συμμετρικής και ασύμμετρης κρυπτογραφίας.

- **ISO / IEC 9796** : προσδιορίζει ένα σχήμα για την επιβεβαίωση του αποστολέα και την ακεραιότητα των δεδομένων, χρησιμοποιώντας ένα σύστημα που βασίζεται στη χρήση κρυπτογραφίας δημόσιου κλειδιού.
- **ISO / IEC 13888** : στο πρότυπο αυτό στηρίζεται η υπηρεσία της παροχής αποδεικτικών στοιχείων από έναν Οργανισμό.
- **ISO / IEC 14888** : περιγράφει ένα μηχανισμό για την παροχή ψηφιακών υπογραφών με επισύναψη η οποία καθορίζεται από το ίδιο το απεσταλμένο μήνυμα και μια ακολουθία από δυαδικά στοιχεία που το προσδιορίζουν μονοσήμαντα.
- **ISO / IEC 17799** : περιγράφει τα θέματα διαχείρισης ασφάλειας σε έναν οργανισμό που διαθέτει Πληροφοριακά Συστήματα που χρήζουν προστασία..
- **ISO / IEC 15408** : περιγράφει ένα σύνολο κριτηρίων (γνωστά και ως Common Criteria) για την αξιολόγηση της ασφάλειας που παρέχει ένα προϊόν πληροφορικής.

3.3.2 Πρότυπα της ITU-T (Διεθνής Ένωση Τηλεπικοινωνιών)

Η ITU-T (παλαιότερα γνωστή και ως CCITT) είναι ένας διεθνής οργανισμός για την παροχή προτύπων τηλεπικοινωνιακού υλικού και συστημάτων. Σημαντική συνεισφορά του στην Υποδομή Δημόσιου Κλειδιού είναι η παροχή των Διακριτών Ονομάτων (Distinguished Names), μια τυπική μορφή στην ονοματολογία των οντοτήτων, που αποτελείται από ένα διακριτό χαρακτηριστικό και την αντίστοιχη τιμή (π.χ. CN=GR → Country Name = Greece). Σημαντικά πρότυπα της σειράς είναι

- **X.400** : η πρόταση X.400, γνωστή και ως Σύστημα Διαχείρισης Μηνυμάτων (Message Handling System - MHS), είναι μία από τις δύο υπάρχουσες προτάσεις για αρχιτεκτονικές ηλεκτρονικού ταχυδρομείου και τη διασυνδεσιμότητα τέτοιων συστημάτων. Η άλλη αρχιτεκτονική είναι το Simple Mail Transfer Protocol – SMTP. Η δομή ενός MHS μηνύματος είναι αντίστοιχη της MIME και περιλαμβάνει μία επικεφαλίδα και το σώμα του μηνύματος το οποίο μπορεί να διασπάται σε πολλαπλά μέρη με διαφορετική κωδικοποίηση το καθένα. Έτσι κάποιο μέρος του μηνύματος μπορεί να είναι απλό κείμενο, κάποιο άλλο μια φωτογραφία ενώ κάποιο τρίτο μια κωδικοποιημένη πληροφορία.



- **X.435** : βασίζεται στο πρότυπο X.400 και σχεδιάστηκε για την υποστήριξη ανταλλαγής ηλεκτρονικών μηνυμάτων. Παρέχει τις βασικές ιδιότητες της Ασφάλειας Πληροφοριών, ενώ επιπλέον παρέχει και υπηρεσίες μη αποποίησης της αποστολής ενός μηνύματος.
- **X.509** : δημιουργήθηκε για την παροχή υπηρεσιών αυθεντικοποίησης στις υπηρεσίες ευρετηρίου X.500. Η παροχή της αυθεντικοποίησης γίνεται με τη χρήση τεχνικών δημόσιου και μυστικού κλειδιού ενώ σε μια νεότερη έκδοση του και με τη χρήση ειδικών πιστοποιητικών. Αυτά είναι τα X.509 πιστοποιητικά με τα παρακάτω πεδία:
 - Έκδοση
 - Σειριακός αριθμός
 - Αλγόριθμος υπογραφής
 - Το όνομα της Αρχής Πιστοποίησης
 - Την περίοδο εγκυρότητάς του
 - Το όνομα του χρήστη
 - Το δημόσιο κλειδί του χρήστη
 - Ο μοναδικός κωδικός της Αρχής Πιστοποίησης
 - Ο μοναδικός κωδικός του χρήστη
 - Κάποιες επεκτάσεις (ρόλοι, πρόσβαση σε αντικείμενα κ.τ.λ.)
 - Η ψηφιακή υπογραφή στα παραπάνω

3.3.3 PKCS Πρότυπα – RSA

Τα PKCS (Public Key Cryptography Standards) πρότυπα είναι προδιαγραφές ανεπτυγμένες από την RSA Security σε συνεργασία με παγκόσμιες εταιρίες παραγωγής λογισμικού (όπως η Microsoft, η SUN, η Apple κ.τ.λ.) για την ανάπτυξη και την αποδοχή της κρυπτογραφίας του δημόσιου κλειδιού. Περιγράφουν τη σύνταξη των μηνυμάτων σε μια αφαιρετική μορφή δίνοντας ολοκληρωμένες λεπτομέρειες για τους χρησιμοποιούμενους αλγορίθμους. Δεν προδιαγράφουν την αναπαράσταση των μηνυμάτων ωστόσο δίνονται κάποιοι Βασικοί Κανόνες Κωδικοποίησης (Basic Encoding Rules - BER) για την προτεινόμενη δομή. Στον παρακάτω πίνακα δίνεται μια λίστα των ενεργών PKCS με μια μικρή τους περιγραφή:

Πρότυπο	Περιγραφή
PKCS # 1	Το RSA πρότυπο κωδικοποίησης. Ορίζει τους μηχανισμούς για κωδικοποίηση και υπογραφή των δεδομένων χρησιμοποιώντας το RSA σύστημα δημόσιου κλειδιού.
PKCS # 3	Το Diffie – Hellman πρότυπο ανταλλαγής κλειδιών.
PKCS # 5	Το Password Based Encryption πρότυπο. Περιγράφει τη μεθοδολογία για την παραγωγή ενός Μυστικού Κλειδιού (Secret Key) με τη χρήση ενός κωδικού χρήστη.
PKCS # 6	Το πρότυπο σύνταξης ενός πιστοποιητικού βασισμένο στο X.509.
PKCS # 7	Περιγράφει τη γενική σύνταξη ενός κρυπτογραφημένου μηνύματος.
PKCS # 8	Περιγράφει τη μεθοδολογία για την αποθήκευση πληροφοριών βασισμένη στο ιδιωτικό κλειδί.
PKCS # 9	Ορίζει συγκεκριμένους τύπους ιδιοτήτων που περιγράφονται σε άλλα PKCS πρότυπα.
PKCS # 10	Περιγράφει τη σύνταξη ενός αιτήματος για την έκδοση πιστοποιητικών.
PKCS # 11	Ορίζει την τεχνολογία για διεπαφές ανεξάρτητες του προγραμματιστικού περιβάλλοντος όπως οι Έξυπνες Κάρτες.
PKCS # 12	Περιγράφει τη δομή για μεταφέρσιμα και αποθηκεύσιμα ιδιωτικά κλειδιά, πιστοποιητικά κ.τ.λ.
PKCS # 13	Περιγράφει τους μηχανισμούς για την κρυπτογράφηση και την υπογραφή δεδομένων με τη χρήση της ελλειπτικής (elliptic curve) κρυπτογραφίας.
PKCS # 14	Σχετίζεται με την παραγωγή ψευδοτυχαίων αριθμών.
PKCS # 15	Περιγράφει ένα πρότυπο για κρυπτογραφικά τεκμήρια

Πίνακας 3.1 RSA Πρότυπα

Σημείωση : Τα PKCS #2 και #4 δεν υπάρχουν πια μιας και έχουν ενσωματωθεί στο PKCS #1.

3.3.4 IETF Πρότυπα – Πρότυπα στο περιβάλλον του διαδικτύου

Το IETF (Internet Engineering Task Force) είναι μια ομάδα από πωλητές προϊόντων και υπηρεσιών, ερευνητών, και σχεδιαστές συστημάτων που ασχολούνται με την ανάπτυξη εφαρμογών και αρχιτεκτονικών στο διαδίκτυο. Τα προτεινόμενα πρότυπα που παράγουν είναι γνωστά ως RFCs (Request for Comments) και Διαδικτυακές Αναφορές (Internet Drafts). Σημαντικές παραγόμενες εφαρμογές είναι :

- **Privacy Enhancement for electronic Mail (PEM)** : περιγράφεται από τα RFCs 1421 – 1424 ενώ οι αρχικές προδιαγραφές από τα RFCs 7 – 10. Κάθε PEM μήνυμα παρέχει υποστήριξη για αυθεντικοποίηση μηνύματος, ακεραιότητα δεδομένων και υπηρεσίες μη-αποποίησης αποστολής, χρησιμοποιώντας τον έλεγχο ακεραιότητας μηνυμάτων (Message Integrity Check – MIC). Δεν είναι σε θέση να παρέχει έλεγχο πρόσβασης και υπηρεσίες μη-αποποίησης παραλαβής μηνύματος. Η εξέλιξη του PEM οδήγησε στην ανάπτυξη του πρωτοκόλλου PKIX.
- **PKIX (Internet PKI based on X.509)** : είναι μια σειρά από προσχέδια ευρέως αποδεκτά από τους χρήστες του Internet που σχετίζονται με την ανάπτυξη μιας ιεραρχικής Υποδομής Δημόσιου Κλειδιού. Συμπληρώνει την ανάλυση του προτύπου X.509 για μια σειρά από θέματα όπως οι χρησιμοποιούμενοι αλγόριθμοι, οργανωτικά θέματα και τη μορφή και δομή των μηνυμάτων εισόδου και εξόδου για τις παρεχόμενες υπηρεσίες.
- **SPKI (Simple Public Key Infrastructure)** : περιγράφει τα πιστοποιητικά και τις λειτουργικές απαιτήσεις για μια Υποδομή Δημόσιου Κλειδιού μη καθολικού χαρακτήρα. Κύριο χαρακτηριστικό των χρησιμοποιούμενων πιστοποιητικών είναι η αντιστοίχηση των δημόσιων κλειδιών σε κωδικούς αναφοράς και όχι σε φυσικά ονόματα και των ρόλων σε πρόσωπα.
- **PGP (Pretty Good Privacy)** : είναι ένα προϊόν λογισμικού που χρησιμοποιείται ευρύτατα στο Internet για να εξασφαλίζει μηνύματα απλού κειμένου. Παρέχει υποστήριξη για υπηρεσίες εμπιστευτικότητας δεδομένων, αυθεντικοποίησης μηνυμάτων, ακεραιότητας δεδομένων και υπηρεσίες μη-αποποίησης αποστολής μέσω κρυπτογράφησης και ψηφιακών φακέλων. Το PGP βασίζεται στην έννοια της εμπιστοσύνης μεταξύ των χρηστών, ενώ η αντίληψη της μεταβατικής εμπιστοσύνης (transitive trust) που χρησιμοποιείται

και εφαρμόζεται από το PGP λογισμικό παράγει τον αποκαλούμενο ιστό εμπιστοσύνης (web of trust).

- **Secure MIME - S/MIME** : Είναι μία ακόμη προσέγγιση για την παροχή ασφάλειας μηνυμάτων ηλεκτρονικού ταχυδρομείου και αναφέρεται περισσότερο σε προδιαγραφές παρά σε συγκεκριμένο προϊόν λογισμικού. Περιλαμβάνει δύο Internet Drafts : ένα που καθορίζει τη μορφή των μηνυμάτων τύπου S/MIME και ένα που καθορίζει τη μορφή των S/MIME πιστοποιητικών. Η ιεραρχία των πιστοποιητικών βασίζεται στην ITU-T X.509 σύσταση, ενώ η κρυπτογραφική συμβατότητα και διαλειτουργικότητα των προμηθευτών στα PKCS.
- **Lightweight Directory Access Protocol (LDAP)**: παρέχει ένα μηχανισμό πρόσβασης σε υπηρεσίες ευρετηρίου σύμφωνα με το πρότυπο X.500 και η αναγνώριση των μοναδικών εγγραφών γίνεται με βάση το Διακριτικό Όνομά τους (Distinguished Name). Είναι ένα σημαντικό πρωτόκολλο για τις παρεχόμενες υπηρεσίες Υποδομής Δημόσιου Κλειδιού από έναν Οργανισμό.
- **Secure Socket Layer (SSL)**: χρησιμοποιείται για τη μετάδοση κρυπτογραφημένων πληροφοριών μέσω του διαδικτύου και στηρίζεται στην ασύμμετρη και τη συμμετρική κρυπτογραφία. Το SSL στρωματοποιείται στην κορυφή μιας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που προέρχεται από το TCP/IP και είναι σε θέση να παρέχει υπηρεσίες ασφαλείας για αυθαίρετες TCP/IP εφαρμογές. Ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL ειδικότερα, είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει πως μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς σε οποιαδήποτε TCP/IP εφαρμογή που στρωματοποιείται στην κορυφή του. Συνοπτικά, το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες :
 - Οι επικοινωνούντες μπορούν και αυθεντικοποιούνται αμοιβαία με τη χρήση κρυπτογραφίας δημόσιου κλειδιού.
 - Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων, αφού η σύνδεση κρυπτογραφείται διαφανώς μέσα από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.

- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, αφού τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητά τους κατά τη μετάδοση με χρήση MAC's.

Σε μια νεότερη προσπάθεια η Microsoft εξέδωσε ένα αντίστοιχο πρωτόκολλο που ονομάσθηκε Private Communication Technology – PCT και στηρίζεται στο SSL.

- **Microsoft CryptoAPI** : είναι μια βιβλιοθήκη εργαλείων, λειτουργιών και συναρτήσεων για την παροχή κρυπτογραφικών υπηρεσιών από έναν πάροχο απομονώνοντάς αυτές από τις διαφορετικές εφαρμογές. Τέτοιες λειτουργίες είναι η ανταλλαγή κλειδιών, η ψηφιακή υπογραφή, η μορφοποίηση των δυαδικών αντικειμένων κλειδιών, η μορφοποίηση της ψηφιακής υπογραφής και η δημιουργία και αποθήκευση των κλειδιών συνόδου.
- **CORBA Security**: παρέχεται ένα σύνολο από υπηρεσίες ασφάλειας συμπληρωματικά με την τεχνολογία CORBA (Common Object Request Broker Architecture). Τέτοιες είναι η αυθεντικοποίηση, η παρακολούθηση (log files), η ακεραιότητα και εμπιστευτικότητα των διακινούμενων δεδομένων, η δημιουργία αποδεικτικών στοιχείων και η μη-αποκοίνωντας κάποιων ενεργειών.
- **Secure HTTP – S/HTTP** : υποστηρίζει την ασφάλεια των διαδικτυακών συναλλαγών ενσωματώνοντας κρυπτογραφικές βελτιώσεις στην HTTP κυκλοφορία δεδομένων σε επύπεδο εφαρμογών. Συγκεκριμένα στο Internet Draft (drft-ietf-ets-shttp-04.txt) ορίζεται μία επέκταση του HTTP για την παροχή υπηρεσιών ασφαλείας και δίνεται έμφαση στην ευελιξία της επιλογής των μηχανισμών διαχείρισης κλειδιών, στις πολιτικές ασφαλείας και στους κρυπτογραφικούς αλγορίθμους, υποστηρίζοντας τη διαπραγμάτευση επιλογών μεταξύ ενός εξυπηρετούμενου και ενός εξυπηρέτη.

3.3.5 Νομικά πλαίσια και ο ρόλος της εμπιστοσύνης

Η ανάπτυξη των παρεχόμενων υπηρεσιών από έναν Οργανισμό εξαρτάται τόσο από την καθολική αποδοχή τους από το κοινωνικό σύνολο όσο και από την εμπιστοσύνη των διαφορετικών εμπλεκόμενων οντοτήτων προς τον υπεύθυνο Οργανισμό. Επομένως, κρίνεται για το μεν πρώτο η υποστήριξη ενός νομοθετικού πλαισίου ενώ για το δεύτερο μια περιγραφική ανάλυση του ρόλου της εμπιστοσύνης μεταξύ διαδραστικών οντοτήτων.

3.3.5.1 Νομοθετικά πλαίσια

Ανάλογα με τη γεωγραφική θέση και δραστηριοποίηση του Οργανισμού στις παρεχόμενες υπηρεσίες, υπάρχει σημαντική διαφοροποίηση στην αντιμετώπιση του συγκεκριμένου θέματος. Συγκεκριμένα από το 1999 η Ευρωπαϊκή Ένωση έθεσε σε ισχύ μια οδηγία [Οδηγία 1999/93/EK] προς τις χώρες μέλη για τη δημιουργία ενός νομικού πλαισίου για τις ηλεκτρονικές υπογραφές και τη λειτουργία των παρόχων υπηρεσιών πιστοποίησης. Άλλες χώρες της Ευρωπαϊκής Ένωσης όπως η Γερμανία είχαν αναπτύξει προγενέστερα ανάλογη νομοθεσία. Στην Ελλάδα η συγκεκριμένη οδηγία υιοθετήθηκε το 2001. Κάπι αντίστοιχο έχει αναπτυχθεί στις Η.Π.Α. από το 1994 μιας και η χρήση των Υποδομών Δημόσιου Κλειδιού είχε βρει νωρίτερα την αποδοχή που τους αρμόζει.. Ωστόσο οι εφαρμόσιμες νομοθετικές ρυθμίσεις δεν αναφέρονται σε σημαντικά ζητήματα για τη λειτουργία ενός Οργανισμού που παρέχει υπηρεσίες Υποδομής Δημόσιου Κλειδιού όπως τη διαχείριση των κλειδιών, το πλαίσιο της συνεργασίας τέτοιων Οργανισμών, την παράκαμψη της ανωνυμίας μεταξύ των συναλλασσόμενων οντοτήτων και την αναγνώριση και άλλων ηλεκτρονικών τεκμηρίων όπως οι χρονοσφαγίδες και τα αποδεικτικά στοιχεία.

Συσχετίζόμενη με την παραπάνω νομοθεσία και ενδεικτική του τρόπου αντιμετώπισης του ζητήματος είναι και η οδηγία/νομοθεσία περί προστασίας της ιδιωτικότητας. Σημαντικές είναι οι αποκλίσεις μεταξύ Ευρώπης και Η.Π.Α. Απόρροια της ευρωπαϊκής κουλτούρας αποτέλεσε η έκδοση, την 24η Οκτωβρίου 1995, από το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της οδηγίας 95/46/EK [Οδηγία 95/46/EK] για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για τη ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο στόχος της οδηγίας αυτής είναι διπλός. Πρώτον, να διασφαλίσουν τα κράτη - μέλη της Ευρωπαϊκής Ένωσης την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Δεύτερον, να περιορίζουν ή να απαγορεύουν τα κράτη μέλη την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών - μελών για τη διασφάλιση των παραπάνω δικαιωμάτων. Αντίθετα, το νομοθετικό πλαίσιο των Η.Π.Α. αντιμετωπίζει την ιδιωτικότητα διαφορετικά ανά πολιτεία, ανά περίπτωση και ανά προσωπικό δεδομένο, με αποτέλεσμα να μην είναι σαφής και καθορισμένη η έννοια της ιδιωτικότητας. Ένα πολύ σημαντικό χαρακτηριστικό αποτελεί το γεγονός ότι στις

Η.Π.Α. δίνεται μεγάλη αξία στην ιδιωτική πρωτοβουλία. Η Κυβέρνηση δεν υποχρεούται να λαμβάνει μέτρα για την προστασία της ιδιωτικότητας, αλλά υπάρχει πολύ ισχυρή νομοθεσία που προστατεύει τις ιδιωτικές συμφωνίες. Η εστίαση στο άτομο και σε συλλογικές ιδιωτικές πρωτοβουλίες εμποδίζει την κυβέρνηση να ψηφίσει έναν αυστηρό και καθολικό νόμο για την ιδιωτικότητα. Παράλληλα, όμως, διευκολύνει την προστασία προσωπικών δεδομένων μέσω της χρήσης τεχνολογιών (Privacy Enabling Technologies), της αυτορύθμισης των αγορών και των βιομηχανιών (self-regulation), του ανταγωνισμού και της κρίσης του χρήστη - πελάτη. Ρόλος της πολιτείας δε θεωρείται η θεσμοθέτηση της προστασίας της ιδιωτικότητας αλλά η διευκόλυνση της ανάπτυξης ιδιωτικών πρωτοβουλιών. Τέλος, θα πρέπει να σημειωθεί ότι μετά την 11^η Σεπτεμβρίου του 2001, το κοινό είναι ιδιαίτερα ενασθητοποιημένο σε θέματα δημόσιας ασφάλειας, με συνέπεια να δέχεται περιορισμούς στην ιδιωτικότητά του όταν αυτοί προκύπτουν για τη διαφύλαξη του κοινού από παρόμοιου τύπου επιθέσεις.

Τη λύση στο ζήτημα της προσέγγισης των διαφορετικών αντιλήψεων έδωσε η δημιουργία του Safe Harbor [Safe – Harbor]. Το πλαίσιο Safe Harbor αναπτύχθηκε από το Υπουργείο Εμπορίου των Η.Π.Α. σε συνεργασία με την Ευρωπαϊκή Ένωση και εγκρίθηκε από την Ευρωπαϊκή Ένωση τον Ιούλιο του 2000. Στόχος του είναι να γεφυρώσει τις διαφορετικές νομοθετικές προσεγγίσεις και να παρέχει ένα τρόπο στους αμερικανικούς Οργανισμούς να αποκτήσουν ικανοποιητικό επίπεδο προστασίας της ιδιωτικότητας, γεγονός που θα τους επιτρέπει να δέχονται δεδομένα προς επεξεργασία από την Ευρώπη. Για να πιστοποιηθεί ένας Οργανισμός και να συμπεριληφθεί στη λίστα των Safe Harbor Organisations που εκδίδει το Υπουργείο Εμπορίου, πρέπει πρώτα να συμμετάσχει σε ένα πρόγραμμα αυτορύθμισης το οποίο είναι πιστό στις απαιτήσεις του Safe harbor και να συντάξει τη δική του self regulatory πολιτική για την ιδιωτικότητα, η οποία θα είναι σύμφωνη με το Safe Harbor.

3.3.5.2 Ο ρόλος της εμπιστοσύνης

Η έννοια της εμπιστοσύνης είναι θεμελιώδης και κεντρική για τη σωστή λειτουργία ενός Οργανισμού παροχής υπηρεσιών Υποδομής Δημόσιου Κλειδιού. Η εμπιστοσύνη στην αξιοπιστία ενός τρίτου Οργανισμού είναι καθοριστικής σημασίας. Μια τυπική ερμηνεία του όρου της εμπιστοσύνης, προσαρμοσμένη στην περίπτωση

δύο συναλλασσόμενων μερών, δίνεται στο X.509 όπου αναφέρεται ότι : «*Mia ontótēta A θεωρείται ότι εμπιστεύεται μία δεύτερη ontótēta B όταν η ontótēta A αποδέχεται ότι η ontótēta B θα συμπεριφερθεί ακριβώς όπως αναμένεται και απαιτείται*».

Ειδικότερα στην κοινωνία της πληροφορίας εντοπίζονται τέσσερις τύποι εμπιστοσύνης [Λέκκας] :

- **Εμπιστοσύνη βασισμένη στο λογισμό (Calculus-based trust)** : αποτελεί τον πιο συνήθη τύπο εμπιστοσύνης που τη συναντάμε στην έναρξη μιας επιχειρηματικής σχέσης. Τα συναλλασσόμενα μέρη υπολογίζουν το βαθμό εξάρτησης από τις άλλες οντότητες, το προσδοκώμενο κέρδος και τους πιθανούς κινδύνους και στη συνέχεια αποφασίζουν αν θα αναπτύξουν μια σχέση εμπιστοσύνης μεταξύ τους. Αυτό το είδος της εμπιστοσύνης είναι το αποτέλεσμα προσεκτικών υπολογισμών βασισμένων συνήθως σε οικονομικά κριτήρια.
- **Εμπιστοσύνη βασισμένη στην πληροφορία (Information-based trust)** : Όσο οι σχέσεις αναπτύσσονται και οι αλληλεπιδράσεις συνεχίζονται, οι συναλλασσόμενες οντότητες συγκεντρώνουν αρκετές πληροφορίες έτσι ώστε να έχουν τη δυνατότητα να προβλέψουν τη συμπεριφορά των άλλων οντοτήτων. Η αίσθηση της αβεβαιότητας μειώνεται, οι πιθανοί κίνδυνοι ελαχιστοποιούνται και συνεπώς αναπτύσσεται μια σχέση εμπιστοσύνης.
- **Μεταβατική εμπιστοσύνη (Transitiveness-based trust)** : Σε αυτή την κατηγορία ανήκουν οι σχέσεις εμπιστοσύνης που αναπτύσσονται σε μια Υποδομή Δημόσιου Κλειδιού. Η εδραίωση μιας ισχυρής σχέσης εμπιστοσύνης με μια τρίτη οντότητα δίνει την ιδιότητα της μεταβατικότητας στη σχέση αυτή και επομένως ο συναλλασσόμενος που εμπιστεύεται αυτή την οντότητα εμπιστεύεται και τις οντότητες που υποδεικνύει. Σαφώς και η θεώρηση αυτή εμπεριέχει και την έννοια του ρίσκου. Για την καλύτερη εξασφάλιση των δικαιωμάτων του χρήστη σε μία τέτοια υποδομή είναι αναγκαία η ύπαρξη και ενός συστήματος διασφάλισης της ποιότητας των παρεχόμενων υπηρεσιών για την εξουδετέρωση ή την ελαχιστοποίηση των κινδύνων και των ρίσκων. Άλλωστε η μεταβατικότητα της εμπιστοσύνης προτείνεται και δεν επιβάλλεται. Τον τελευταίο λόγο τον έχει πάντα ο

χρήστης και είναι ο απόλυτος υπεύθυνος των πράξεών του, χαρακτηριστικό στοιχείο της ευελιξίας τέτοιων υποδομών.

- **Εμπιστοσύνη μέσα στο κοινωνικό σύστημα (Trust against social system)**
: Η εμπιστοσύνη σε αυτή την περίπτωση πηγάζει από τη συμμετοχή του ανθρώπου στο κοινωνικό σύστημα. Σε μια τέτοια περίπτωση η συνάντηση ή η γνώση μεταξύ των συναλλασσόμενων μερών δεν απαιτείται. Τυπικό σύστημα αυτού του είδους της εμπιστοσύνης είναι οι τραπεζικές συναλλαγές.

Το ζήτημα της εμπιστοσύνης προς έναν Οργανισμό που παρέχει υπηρεσίες Υποδομής Δημόσιου Κλειδιού δεν αντιμετωπίζεται με σαφήνεια στην υπάρχουσα βιβλιογραφία, ωστόσο διακρίνουμε τις παρακάτω διαπιστώσεις [Λέκκας]:

- Λόγω της απομακρυσμένης φύσης των υπηρεσιών τέτοιων Οργανισμών, οι εκτελούμενες διεργασίες δεν είναι απόλυτα διαφανείς προς τους πελάτες, ενώ είναι σχεδόν απίθανο από τη μεριά του πελάτη να γνωρίζει σε βάθος τις λειτουργίες των τεχνολογιών που χρησιμοποιούνται. Συνεπώς, οι σχέσεις Οργανισμών και πελατών στηρίζονται σε κάποιο βαθμό στην εμπιστοσύνη.
- Η εμπιστοσύνη προς έναν Οργανισμό έχει δύο διαστάσεις : η πρώτη σχετίζεται με πίστη προς την ηθική εντιμότητα και τις καλές προθέσεις του Οργανισμού και των εμπλεκόμενων οντοτήτων, ενώ η δεύτερη με την πεποίθηση πως το Πληροφοριακό Σύστημα του Οργανισμού είναι οργανωτικά και τεχνικά άρτιο. Συνεπώς, η εμπιστοσύνη σχετίζεται με τη σωστή λειτουργία των παρεχόμενων υπηρεσιών όπως τις αντιλαμβάνεται ο πελάτης.
- Βασικός παράγοντας στην εδραίωση της εμπιστοσύνης είναι η εκτίμηση των πιθανών κινδύνων που προκύπτουν από την ύπαρξη μιας τέτοιας σχέσης εμπιστοσύνης. Συνεπώς, η έννοια της εμπιστοσύνης σχετίζεται με την αποδοχή ενός βαθμού ρίσκου στις συναλλαγές μας.
- Ένας Οργανισμός είναι έμπιστος για την υποστήριξη της ασφάλειας στις συναλλαγές που υποτίθεται πως παρέχει. Η έννοια της ασφάλειας αναφέρεται σε μια δεδομένη κατάσταση όπου όλοι οι πιθανοί κίνδυνοι είτε εξουδετερώνονται ή περιορίζονται στο ελάχιστο

3.4 XML/Schema και XML

3.4.1 Γενικά χαρακτηριστικά

Η eXtensible Markup Language (XML) είναι μια mark-up γλώσσα που κατασκευάστηκε ως ένα υποσύνολο της γλώσσας Standard Generalized MarkUp Language (SGML) από το World Wide Web Consortium (W3C) [www.w3.org]. Ουσιαστικά πρόκειται για μια πρότυπη αναπαράσταση δομημένων δεδομένων. Δηλαδή δεδομένα τα οποία έχουν κάποιας μορφής δόμηση μπορούν να αναπαρασταθούν με τη βοήθεια της γλώσσας XML και να πάρουν τη μορφή ενός εγγράφου. Ένα λεπτό σημείο στα έγγραφα XML είναι ότι περιγράφουν τον εαυτό τους, δηλαδή εκτός από το ίδιο το κείμενο που εμπεριέχουν, υπάρχει και ένα σύνολο δηλώσεων που στην ουσία ορίζει τη σημασιολογία του περιεχομένου. Η XML είναι μια οικογένεια από τεχνολογίες. Η *XML 1.0* είναι η προδιαγραφή που ορίζει τι είναι οι "ετικέτες" και τα "γνωρίσματα". Πέρα από την *XML 1.0*, "η οικογένεια XML" είναι ένα διαρκώς αναπτυσσόμενο σύνολο λειτουργικών μονάδων οι οποίες προσφέρουν χρήσιμες υπηρεσίες για τη διεκπεραίωση σημαντικών έργων τα οποία ανακύπτουν συχνά. Η *Xlink* περιγράφει έναν προκαθορισμένο τρόπο εισαγωγής υπερσυνδέσμων σε αρχεία XML. Τα *XPointer* και τα *XFragments* είναι συντακτικά υπό διαμόρφωση για την υπόδειξη θέσεων ενός εγγράφου XML. Το *XPointer* μοιάζει λίγο με URL αλλά αντί να υποδεικνύει έγγραφα στον Ιστό, υποδεικνύει κομμάτια πληροφοριών ενός εγγράφου XML. Το *CSS*, η γλώσσα μορφοποίησης σελίδων, είναι δυνατό να εφαρμοστεί σε XML όπως και σε HTML. Το *XSL* είναι προηγμένη γλώσσα μορφοποίησης σελίδων. Βασίζεται στο *XSLT*, μία γλώσσα μετασχηματισμού η οποία χρησιμοποιείται για την αναδιάταξη, την πρόσθεση και την διαγραφή ετικετών και γνωρισμάτων. Το *DOM* είναι ένα προκαθορισμένο σύνολο λειτουργιών για τη διαχείριση αρχείων XML (και HTML) από μία γλώσσα προγραμματισμού. Τα *XML Schemas 1* και *2* επιτρέπουν στους κατασκευαστές λογισμικού να ορίσουν με ακρίβεια τις δομές των δικών τους μορφών XML. Στις επόμενες παραγράφους θα ασχοληθούμε με τα χαρακτηριστικά του XML Schema μιας και αυτή θα είναι η περιγραφική γλώσσα για τη δήλωση των δομών δεδομένων υπηρεσιών προστιθέμενης αξίας στις Υποδομές Δημόσιου Κλειδιού στο επόμενο κεφάλαιο.

με τα Cascading Style Sheets (CSS), και επιτρέπει στους χρήστες να αναπτύξουν XML Σχήματα που εφαρμόζουν καλύτερα στις ανάγκες τους, χωρίς να δημιουργείται ένα τελείως νέο λεξιλόγιο από την αρχή. Το XML Schema επιτρέπει στον συγγραφέα να καθορίσει ποια μέρη ενός εγγράφου ίσως πιστοποιηθούν, ή να αναγνωρίσει μέρη ενός εγγράφου όπου ένα σχήμα ίσως να έχει εφαρμογή. Το XML Schema επίσης παρέχει ένα τρόπο για τους χρήστες των συστημάτων ηλεκτρονικού εμπορίου να διαλέξουν ποιο XML Schema χρησιμοποιούν για πιστοποίηση στοιχείων σε ένα δοσμένο namespace, και κατ' αυτό τον τρόπο παρέχει μεγαλύτερη αυτοπεποίθηση στις συναλλαγές ηλεκτρονικού εμπορίου και μεγαλύτερη ασφάλεια ενάντια ως προς τις μη εξουσιοδοτημένες αλλαγές σε πιστοποιημένους κανόνες. Επιπλέον, από τη στιγμή που τα XML Σχήματα είναι από μόνα τους XML έγγραφα, μπορούν να διαχειριστούν από τα XML συγγραφικά εργαλεία, ή δια μέσου της XSLT.

3.4.2.2 Παραδείγματα χρήσης

Θεωρείται πως ο αναγνώστης της παρούσας διπλωματικής εργασίας έχει γνώση της διάταξης του XML Schema, ώστόσο κρίνεται απαραίτητη μια πιο αναλυτική περιγραφή των βασικών τύπων δεδομένων της XML Schema έστω και μέσα από κάποια παραδείγματα χρήσης.

- **Δήλωση ενός Αρχείου XML Schema :**

```
<xsd:schema
    name="όνομα_σχήματος"
    xmlns="urn:schemas-microsoft-com:xml-data"
    xmlns:dt="urn:schemas-microsoft-com:datatypes">
</xsd:schema>
```

Για να βάλουμε σχόλια σε ένα Σχήμα, χρησιμοποιούμε την σύνταξη :

```
<!-- κείμενο σχολίου -->
```

- **Τοποθέτηση Στοιχείων μέσα σε XML Schema**

Μπορούμε να δημιουργήσουμε σχέσεις container σε ένα Σχήμα (Δήλωση σύνθετων τύπων δεδομένων). Τα στοιχεία container αποτελούνται από ένα ή περισσότερα άλλα προκαθορισμένα στοιχεία. Η σύνταξη για να δημιουργήσουμε ένα στοιχείο container μέσα σε μια διάταξη Schema είναι η εξής :

```
<xsd:schema
    ...
    <xsd:complexType name="όνομα_XML_στοιχείου_container">
        <xsd:element type="όνομα_περιεχόμενου_στοιχείου">
```

```

< xsd:element type="όνομα_περιεχόμενου_στοιχείου2">
  ...
</xsd:complexType >
  ...
</ xsd:schema>

```

Για κάθε στοιχείο δεδομένων ενός XML εγγράφου πρέπει να δηλώσουμε ένα complexType στην διάταξη και με το ίδιο όνομα κατά προτίμηση.

- **Οι Δηλώσεις minOccurs και maxOccurs**

Μπορούμε να δημιουργήσουμε έναν κανόνα επικύρωσης για ένα στοιχείο μιας διάταξης (Schema) ώστε να είμαστε σίγουροι ότι σχετίζεται με μία μόνο ή με περισσότερες τιμές κατά την ώρα εκτέλεσης. Προς τον σκοπό αυτό χρησιμοποιούμε τις δηλώσεις **minOccurs** και **maxOccurs**, όπου η πρώτη αναφέρεται στον ελάχιστο αριθμό τιμών που μπορεί να υπάρχουν γι' αυτό το στοιχείο την ώρα εκτέλεσης (προεπιλογή=1) και η δεύτερη αναφέρεται στον μέγιστο αριθμό τιμών που μπορεί να υπάρχουν γι' αυτό το στοιχείο την ώρα εκτέλεσης (προεπιλογή=1 και το * δηλώνει πολλές τιμές).

Η σύνταξη είναι ως εξής :

```
<xsd:element type="τύπος_στοιχείου"
  [minOccurs="1"]
  [maxOccurs="{1 | *}"] />
```

Ο τύπος_στοιχείου πρέπει να ταιριάζει με το όνομα ενός στοιχείου που έχουμε ήδη ορίσει σαν ElementType. Ακολουθεί ένα παράδειγμα.

```
<xsd:element type="car" minOccurs="1" maxOccurs="*" />
```

Αν ορίσουμε την τιμή 0 για την δήλωση **minOccurs**, το στοιχείο της διάταξης γίνεται προαιρετικό. Για να περιορίσουμε τον αριθμό των τιμών ενός στοιχείου, πρέπει να ορίσουμε μια τιμή για την δήλωση **maxOccurs**, όπως π.χ. 20.

- **Οι Ιδιότητες content, model και type.**

Μπορούμε να χρησιμοποιήσουμε την ιδιότητα **content** ενός στοιχείου ElementType για να δηλώσουμε τον τύπο δεδομένων ενός στοιχείου της XML σαν τύπο κειμένου (*textOnly*) σε μια διάταξη (Schema). Τα στοιχεία που δηλώνονται σαν *textOnly* μπορούν να περιέχουν μόνο χαρακτήρες και όχι άλλα προκαθορισμένα στοιχεία. Η σύνταξη της ιδιότητας content είναι η εξής :

```
<xsd:ElementType      name="όνομα_στοιχείου"      content="textOnly"
  model="closed" />
```

Το όνομα_στοιχείου είναι το όνομα του στοιχείου που θέλουμε να ορίσουμε σαν τύπο κειμένου. Οι διατάξεις (Schemas) προσφέρουν πιο συγκεκριμένους τύπους δεδομένων από τα DTD.

Ακολουθεί ένα παράδειγμα.:

```
<xsd:ElementType name="product" content="textOnly" model="closed"/>
```

Η ιδιότητα *content* ενός ElementType μπορεί να έχει μια από τις εξής τιμές :

1. **empty**, κενό στοιχείο.
2. **textOnly**, στοιχεία που περιέχουν μόνο κείμενο.
3. **elementOnly**, στοιχεία που περιέχουν άλλα στοιχεία και όχι κείμενο.
4. **mixed**, στοιχεία που περιέχουν άλλα στοιχεία και κείμενο. Προκαθορισμένη επιλογή.

Αν δώσουμε την τιμή *open* στην ιδιότητα *model* και όχι την τιμή *closed*, θα επιτρέψουμε σ' ένα στοιχείο διάταξης να μπορεί να περιέχει την ώρα εκτέλεσης μια τιμή κειμένου και ένα ή περισσότερα προκαθορισμένα στοιχεία. Καταργούμε δηλαδή τους περιορισμούς του στοιχείου. Ακολουθεί ένα παράδειγμα.

```
<xsd:ElementType name="product" model="open" />
```

Μπορούμε να χρησιμοποιήσουμε την ιδιότητα *type* για να ορίσουμε τον τύπο δεδομένων ενός στοιχείου σε *boolean*, *integer*, *real*, *time*, *datetime*, *long* κ.τ.λ. Ακολουθεί ένα παράδειγμα.

```
<xsd:ElementType name="product_price" content="textOnly"
type="integer" model="closed"/>
```

• Δήλωση ιδιότητας

Για να μπορέσουμε να δηλώσουμε μια ιδιότητα για μια διάταξη (Schema), πρέπει πρώτα να δηλώσουμε έναν τύπο ιδιότητας (Attribute), με την εξής σύνταξη :

```
<xsd:attribute
default="προκαθορισμένη_τιμή"
type="τύπος_δεδομένων"
values="απαριθμητές_τιμές"
name="idref"
required="{yes | no}" />
```

Το *type* καθορίζει τον τύπο δεδομένων της ιδιότητας και μπορεί να έχει μια από τις τιμές *entity*, *entities*, *enumeration*, *id*, *idref*, *idrefs*, *nmtoken*, *nmtokens*, *notation*, *int*, *boolean* ή *string*. Το *values* καθορίζει τις απαριθμητές τιμές όταν το *type* είναι απαριθμητή τιμή (*enumeration*) και οι απαριθμητές τιμές πρέπει να χωρίζονται με κενά ανάμεσά τους. Το *name* είναι το όνομα της ιδιότητας για να μπορούμε να

αναφερόμαστε σ' αυτήν και το *required* καθορίζει αν απαιτείται μια τιμή γι' αυτή την ιδιότητα την ώρα εκτέλεσης.

Οι ιδιότητες τύπου *nmtoken* ξεχωρίζουν από τις ιδιότητες τύπου *string* στο ότι τα *string* μπορεί να περιέχουν κενά, ενώ οι έγκυρες ιδιότητες τύπου *nmtoken* όχι. Οι ιδιότητες τύπου *nmtoken* χρησιμοποιούνται συνήθως σαν πρωτεύοντα και ξένα κλειδιά. Η δήλωση μιας ιδιότητας με τύπο *id* την κάνει να μπορεί να δέχεται μόνο μοναδικές τιμές σε μια XML εφαρμογή (πρωτεύον κλειδί), ενώ η δήλωση με τύπο *idref* την κάνει να είναι μια αναφορά αναγνωριστικού ή ξένο κλειδί, σε σχέση βέβαια με μια άλλη δήλωση του τύπου *id*.

Οι δηλώσεις των ιδιοτήτων γίνονται μετά από την δήλωση της διάταξης (Schema) και χρησιμοποιούμε την δήλωση `<xsd:attribute type="idref" />` μέσα σε μια δήλωση `<xsd:element ... > ... </xsd:element>` για να καθορίσουμε τον τύπο της ιδιότητας ενός στοιχείου.

Ακολουθεί ένα παράδειγμα δήλωσης μιας ιδιότητας για δεδομένα χαρακτήρων.

```
<xsd:schema name="myName"
    ...
</xsd:schema>
<xsd:attributeType name="attr1" type="string" />
<xsd:element name="element1" content="textOnly" model="closed">
    <xsd:attribute type="attr1" />
</xsd:elementType>
```

3.5 Συμπεράσματα

Στο κεφάλαιο αυτό εξετάσαμε ένα σύνολο από θέματα που σχετίζονται με τη λειτουργία ενός Οργανισμού που παρέχει υπηρεσίες εκμεταλλευόμενος της χρήσης της Υποδομής Δημόσιου Κλειδιού. Η κατηγοριοποίηση των υπηρεσιών σε Βασικές, Δευτερεύουσες και Προστιθέμενης Αξίας σχετίζεται άμεσα με τις απαιτήσεις χρήσεις που διακρίνονται σε απαιτήσεις ασφάλειας, λειτουργικότητας, οργανωτικές, κοινωνικές και ειδικές.

Για την υποστήριξη των υπηρεσιών του Οργανισμού έχουν δημιουργηθεί ένα σύνολο από ευρέως αποδεκτά πρότυπα. Τέτοιοι πρωτοπόροι Οργανισμοί είναι ο ISO, η ITU-T, ο IETF και ο RSA. Βέβαια η λειτουργία του Οργανισμού είναι άρρηκτα συνδεδεμένη και με το ισχύον νομοθετικό πλαίσιο στο περιβάλλον λειτουργίας του. Σημαντικός είναι και οι παράγοντες της διαφύλαξης της ιδιωτικότητας των

συναλλασσόμενων οντοτήτων και της εμπιστοσύνης προς τον πάροχο Οργανισμό. Στο τέλος του κεφαλαίου γίνεται μια ανασκόπηση της XML και του XML Schema, της δομής δεδομένων που θα χρησιμοποιηθεί για την περιγραφή των υπηρεσιών προστιθέμενης αξίας στο Κεφάλαιο 4.

Αναφορές

1. Brian Shapiro, C. Richard Baker, 2001, Information Technology and the social construction of information privacy, Journal of Accounting and Public Policy, Vol. 20, pp 295 – 322
2. Gerhard Steinke 2002, Data privacy approaches from US and EU perspectives, Telematics and Informatics, Vol. 19, pp 193 – 200
3. Jared Strauss, Kenneth S. Rogerson, 2002, Policies for online privacy in the United States and the European Union, Telematics and Informatics, Vol. 19, pp 173 – 192
4. Kowalski S., "Cybernetic Analysis of the National Computer Security", Computers and Security, Vol.10, No.3, pp.217-227, Elsevier Science, 1991
5. Lekkas Dimitrios, "Establishing and managing trust within the Public Key Infrastructure", Computer Communications, Vol.26, No.16 (2003) pp.1815-1825
6. Safe – Harbor Workbook U.S. Department of Commerce, www.export.gov/safeharbor/ SafeHarborWorkbook.htm
7. The European Data Protection Directive and European – U.S. Trade. 95/46/EU www.dpa.gr/Documents/Gre/Nomoi/95-46.rtf
8. Λέκκας Δημήτρης, Διδακτορική διατριβή, «Ασφάλεια Πληροφοριακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας»
9. Οδηγία 1999/93/ΕΚ του Ευρωκοινοβουλίου και του Συμβουλίου της 13^{ης} Δεκέμβρης για τη δημιουργία ενός Κοινωνικού Πλαισίου για τη χρήση των ηλεκτρονικών υπογραφών.

Κεφάλαιο 4 Υπηρεσίες Προστιθέμενης Αξίας σε Υποδομή Δημόσιου Κλειδιού

4.1 Χρονοσήμανση

4.1.1 Εισαγωγή

Ως υπηρεσία χρονοσήμανσης ορίζεται η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε ψηφιακή μορφή, έτσι ώστε να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μία συγκεκριμένη χρονική στιγμή. Με τον όρο ‘υπήρχαν’ εννοείται ότι τα δεδομένα κατασκευάστηκαν το αργότερο τη χρονική στιγμή της χρονοσήμανσης και ταυτόχρονα ότι δεν καταστράφηκαν τουλάχιστο μέχρι αυτή τη χρονική στιγμή. Ουσιαστικά, η υπηρεσία αυτή αντιστοιχίζει ένα ηλεκτρονικό κείμενο με μια συγκεκριμένη χρονική στιγμή και εγγυάται την ακρίβεια του χρόνου και της αντιστοίχησης [Λέκκας]. Επιπρόσθετα, η υπηρεσία αυτή παρέχει αποδεικτικά στοιχεία για το χρόνο εκτέλεσης μιας συναλλαγής, δηλαδή ότι η διακίνηση κάποιων δεδομένων έχει λάβει χώρα σε μια συγκεκριμένη χρονική στιγμή. Η παρεχόμενη υπηρεσία μπορεί να υποστηριχτεί και αυτόνομη στα πλαίσια της λειτουργίας ενός Οργανισμού ως Ανεξάρτητης Αρχής, ευρέως γνωστή στη βιβλιογραφία και ως **Αρχή Χρονοσήμανσης (Time Stamping Authority)**.

Το γενικό σενάριο λειτουργίας της υπηρεσίας χρονοσήμανσης ολοκληρώνεται σε τέσσερα βήματα: (1) αποστολή αιτήματος χρονοσήμανσης από τον πελάτη προς τον Οργανισμό, (2) λήψη, επαλήθευση και αποδοχή του αιτήματος από τον Οργανισμό, (3) παραγωγή χρονοσφραγίδας και επιστροφή στον πελάτη, (4) επιβεβαίωση της εγκυρότητας της χρονοσφραγίδας από τον πελάτη. [Λέκκας] [Keystone Project]. Ωστόσο έχουν υπάρξει υλοποιήσεις και προτάσεις της υπηρεσίας χρονοσήμανσης που αφήνουν ένα πλήθος από τις διαχειρίσμες ιδιότητες του μοντέλου λειτουργίας στο χρήστη [Peyravian, Matyas, Roginsky, Zunic] ενώ σε άλλες προτείνονται νέα μοντέλα λειτουργίας με τη χρήση Έξυπνων Καρτών [Shen] και μιας νέας μεθόδου κρυπτανάλυσης των παραγόμενων χρονοσφραγίδων [Wang].

Η αξία και η ποιότητα των παραγόμενων χρονοσφραγίδων προσμετράται στις παρεχόμενες υπηρεσίες από τον Οργανισμό. Τα χαρακτηριστικά αυτά εξαρτώνται άμεσα από το βαθμό εμπιστευτικότητας των συναλλασσόμενων οντοτήτων, την

ποιότητα και το βαθμό λειτουργίας της Αρχής Χρονοσήμανσης όσον αφορά την παραγωγή και αρχειοθέτηση των παραγόμενων χρονοσφαγίδων και των χρησιμοποιούμενων πιστοποιητικών και τις διαδικασίες ανάκτησης των παραγόμενων δεδομένων. Για παράδειγμα, η ανάκτηση της ασφαλής ώρας και η εμπιστευτικότητα προς την Αρχή Έκδοσης των πιστοποιητικών επηρεάζουν άμεσα τη λειτουργία της αναφερόμενης υπηρεσίας.

Για τη διασφάλιση της σωστής λειτουργίας της υπηρεσίας χρονοσήμανσης γίνεται χρήση των ψηφιακών πιστοποιητικών και υπογραφών – φακέλων ενώ οι αλγόριθμοι σύνοψης μας δίνουν τη δυνατότητα, πέρα από θέματα ασφάλειας των συναλλασσόμενων δεδομένων, για ευέλικτη επικοινωνία.

4.1.2 Ασφαλής χρόνος

Βασικός παράγοντας στη λειτουργία της υπηρεσίας είναι η ανάκτηση του ακριβούς χρόνου από ένα γενικά αποδεκτό σύστημα παροχής ώρας, όπως η υπηρεσία Network Time Protocol (NTP), το δορυφορικό σύστημα εντοπισμού στίγματος Global Positioning System (GPS) ο χρόνος UTC και οι εξυπηρετητές που παρέχουν την υπηρεσία NTP (Network Time Protocol). Επίσης σημαντική είναι η υψηλή διαθεσιμότητα των πόρων της υπηρεσίας, έτσι ώστε οι λειτουργίες της να εκτελούνται σε όσο το δυνατό πραγματικό χρόνο και συνεπώς να διατηρείται η ακρίβεια της χρονοσήμανσης.

Είσοδος : Αίτηση ανάκτησης χρόνου σε κάποια ασφαλή πηγή χρόνου. Σημαντικό στοιχείο αποτελεί η αποστολή του τύπου της ζώνης του αιτούντος. Τυπικά η περιγραφή της με την XML Schema είναι η παρακάτω.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!-- Στο attribute name δηλώνουμε το όνομα του που θα έχει element σε μια δομή XML και για τον τύπο του δηλώνουμε ένα νέο σύνθετο τύπο που δεν υποστηρίζεται από τους βασικούς της XML Schema-->
<xsd:element
    name="request_secure_time"
    type="request_secure_time_Type"/>
<!-- Ο νέος τύπος δεδομένων αποτελείται πάντα από δύο elements-->
<xsd:complexType name="request_secure_time_Type">
    <xsd:sequence>
        <xsd:element name="source" type="source_Type"/>
        <xsd:element name="zone" type="zone_Type"/>
    </xsd:sequence>
</xsd:complexType>
```

```

</xsd:complexType>
<!-- Ο τύπος δεδομένων source_Type μπορεί να έχει ως τιμή κάποια
από τις παρακάτω τιμές-->
<xsd:simpleType name="source_Type">
  <xsd:restriction base="xsd:string">
    <!-- Η λίστα τιμών περιλαμβάνει τις τιμές GPS, UTC και NTP- >
    <xsd:enumeration value="GPS"/>
    <xsd:enumeration value="UTC"/>
    <xsd:enumeration value="NTP"/>
  </xsd:restriction>
</xsd:simpleType>
<!-- Ο τύπος δεδομένων zone_Type μπορεί να έχει ως τιμή κάποια από
τις παρακάτω τιμές-->
<xsd:simpleType name="zone_Type">
  <xsd:restriction base="xsd:string">
    <!-- Η λίστα τιμών περιλαμβάνει όλες πιθανές διαφορές τιμών με
την GMT-->
    <xsd:enumeration value="GMT-12"/>
    <xsd:enumeration value="GMT-11"/>
    <xsd:enumeration value="GMT-10"/>
    <xsd:enumeration value="GMT-9"/>
    <xsd:enumeration value="GMT-8"/>
    <xsd:enumeration value="GMT-7"/>
    <xsd:enumeration value="GMT-6"/>
    <xsd:enumeration value="GMT-5"/>
      <xsd:enumeration value="GMT-4"/>
    <xsd:enumeration value="GMT-3"/>
    <xsd:enumeration value="GMT-2"/>
    <xsd:enumeration value="GMT-1"/>
    <xsd:enumeration value="GMT"/>
    <xsd:enumeration value="GMT+12"/>
    <xsd:enumeration value="GMT+11"/>
    <xsd:enumeration value="GMT+10"/>
    <xsd:enumeration value="GMT+9"/>
    <xsd:enumeration value="GMT+8"/>
    <xsd:enumeration value="GMT+7"/>
    <xsd:enumeration value="GMT+6"/>
    <xsd:enumeration value="GMT+5"/>
    <xsd:enumeration value="GMT+4"/>
    <xsd:enumeration value="GMT+3"/>
    <xsd:enumeration value="GMT+2"/>
  </xsd:restriction>
</xsd:simpleType>

```

```

<xsd:enumeration value="GMT+1"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Έξοδος : Επιστρέφεται η μορφοποιημένη τιμή της ώρας στον αιτούντα. Σημαντικό στοιχείο αποτελεί το πεδίο της ακρίβειας (accuracy) μιας και μη αποδεκτή τιμή ακρίβειας όπως ορίζεται από την πολιτική ασφάλειας του Οργανισμού σημαίνει επανάληψη της διαδικασίας λήψης ακριβούς χρόνου. Περιγράφοντας την έξοδο με XML Schema έχουμε :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="secure_time" type="secure_time_Type"/>
<!-- Ο τύπος δεδομένων secure_time_Type έχει ως elements τα παρακάτω--&gt;
  &lt;xsd:complexType name="secure_time_Type"&gt;
    &lt;xsd:sequence&gt;
      &lt;xsd:element name="source" type="source_Type"/&gt;
<!-- Ο τύπος δεδομένων time είναι υποχρεωτικό να υπάρχει στην παραγόμενη δομή XML (use="required")--&gt;
      &lt;xsd:element name="time" type="xsd:long" use="required"/&gt;
<!-- Ο τύπος δεδομένων format έχει πάντα συγκεκριμένη τιμήσιν παραγόμενη δομή XML (fixed="seconds since 1-1-1900")--&gt;
      &lt;xsd:element name="format" type="xsd:string" fixed="seconds since 1-1-1900"/&gt;
      &lt;xsd:element name="zone" type="zone_Type"/&gt;

      &lt;xsd:element name="accuracy" type="accuracy_Type"/&gt;
    &lt;/xsd:sequence&gt;
  &lt;/xsd:complexType&gt;
<!-- Ο τύπος δεδομένων source_Type μπορεί να έχει ως τιμή κάποια από τις παρακάτω τιμές--&gt;
  &lt;xsd:simpleType name="source_Type"&gt;
    &lt;xsd:restriction base="xsd:string"&gt;
      &lt;xsd:enumeration value="GPS"/&gt;
      &lt;xsd:enumeration value="UTC"/&gt;
      &lt;xsd:enumeration value="NTP"/&gt;
    &lt;/xsd:restriction&gt;
  &lt;/xsd:simpleType&gt;
<!-- Ο τύπος δεδομένων zone_Type μπορεί να έχει ως τιμή κάποια από τις παρακάτω τιμές--&gt;
</pre>

```

```

<xsd:simpleType name="zone_Type">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="GMT-12"/>
    <xsd:enumeration value="GMT-11"/>
    <xsd:enumeration value="GMT-10"/>
    <xsd:enumeration value="GMT-9"/>
    <xsd:enumeration value="GMT-8"/>
    <xsd:enumeration value="GMT-7"/>
    <xsd:enumeration value="GMT-6"/>
    <xsd:enumeration value="GMT-5"/>
    <xsd:enumeration value="GMT-4"/>
    <xsd:enumeration value="GMT-3"/>
    <xsd:enumeration value="GMT-2"/>
    <xsd:enumeration value="GMT-1"/>
    <xsd:enumeration value="GMT"/>
    <xsd:enumeration value="GMT+12"/>
    <xsd:enumeration value="GMT+11"/>
    <xsd:enumeration value="GMT+10"/>
    <xsd:enumeration value="GMT+9"/>
    <xsd:enumeration value="GMT+8"/>
    <xsd:enumeration value="GMT+7"/>
    <xsd:enumeration value="GMT+6"/>
    <xsd:enumeration value="GMT+5"/>
    <xsd:enumeration value="GMT+4"/>
    <xsd:enumeration value="GMT+3"/>
    <xsd:enumeration value="GMT+2"/>
    <xsd:enumeration value="GMT+1"/>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="accuracy_Type">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="(+-)\d.(\d+)\ssseconds"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Λειτουργία : Τα βήματα της συγκεκριμένης διαδικασίας είναι τα ακόλουθα :

- Αποστέλλεται το αίτημα ανάκτησης χρόνου στην ασφαλή πηγή που έχει προεπιλεγεί από τις πολιτικές του Οργανισμού, με τη χρήση ασφαλών συστημάτων επικοινωνίας (π.χ. SMTP, SSL κ.τ.λ),
- Λαμβάνεται ο ασφαλές χρόνος.
- Επανάληψη της διαδικασίας στην περίπτωση που η ακρίβεια δεν είναι η επιθυμητή.
- Προσαρμογή της τιμής στη ζώνη ώρας της γεωγραφικής περιοχής του αιτούντος.
- Επιστροφή των στοιχείων.

4.1.3 Αποστολή της αίτησης χρονοσήμανσης

Η αίτηση χρονοσήμανσης στον Οργανισμό από την οντότητα αποστέλλεται σε ηλεκτρονική μορφή με κάποιο πρωτόκολλο μεταφοράς δυαδικών δεδομένων (π.χ. FTP ή SMTP). Πρέπει να χαρακτηρίζεται από την ασφαλή μεταβίβασή της, τη συγκεκριμένη μορφοποίηση που διευκολύνουν την επεξεργασία τους και την ελαχιστοποίηση του μεγέθους τους. Τα σημαντικότερα πρότυπα που προτείνουν μια συγκεκριμένη δομή είναι το PKITS [FNMT] (και την οποία θα χρησιμοποιήσουμε) και το TIMESEC [TIMESEC].

Είσοδος: Η είσοδος δεν πρέπει να περιέχει τα ίδια τα δεδομένα προς χρονοσήμανση αλλά μια μορφή τους που τα προσδιορίζει μονοσήμαντα και από την οποία δεν είναι δυνατό να εξαχθούν τα αρχικά δεδομένα. Αυτή η μορφή μπορεί να είναι το αποτέλεσμα της κρυπτογράφησης των δεδομένων από τον αιτούντα ή η σύνοψη που παράγεται από έναν αλγόριθμο δημοσίου κλειδιού όπως ο MD5 ή ο SHA-1. Σαφώς και η αίτηση μπορεί να περιλαμβάνει περισσότερα του ενός μηνύματος. Περιγραφικά με την XML Schema έχουμε:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
    name="timestamp_request_Input"
    type="timestamp_request_Input_Type"/>
<!-- To element timestamp_request_Input έχει και ένα απαραίτητο
attribute encoding που δηλώνει το είδος της κωδικοποίησης της
εισόδου-->
<xsd:attribute      name="encoding"      type      ="xsd:base64Binary"
use="required"/>
```

```

<xsd:complexType name=" timestamp_request_Input_Type">
    <xsd:sequence>
        <!-- To element timestamp_request_Input αποτελείται από το
ψηφιακό πιστοποιητικό της αιτούμενης οντότητας, τη σύνοψη του
μηνύματος και την ψηφιοποιημένη τιμή της εισόδου -->
        <xsd:element name="user_certificate" type="xsd:base64Binary"
use="required"/>
        <xsd:element name ="message_hash" type="message_hash_Type"/>
        <xsd:element name = "request_digest" type="xsd:base64Binary"
use="required"/>
    </xsd:sequence>
</xsd:complexType>

<!--Σε κάθε είσοδο μπορεί να έχουμε παραπάνω από ένα μηνύματα προς
χρονοσήμανση. Καθένα από αυτά όμως πρέπει να περιέχει το
χρησιμοποιούμενο αλγόριθμο και την τιμή της σύνοψης-->

<xsd:complexType name ="message_hash_Type">
    <xsd:sequence>
        <xsd:element name="message_hash" minOccurs="0"
maxOccurs="unbounded">
            <xsd:complexType>
                <xsd:element name="algorithm_id" type="xsd:string"
use="required"/>
                <xsd:element name="hash_value" type="xsd:string"
use="required"/>
            </xsd:complexType>
        </xsd:element>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος: Μετά τον έλεγχο της σωστής μορφοποίησης της αίτησης, αυθεντικοποιείται ο αιτών (όχι μόνο για το αν το πιστοποιητικό του είναι ενεργό ή όχι αλλά και για το αν δικαιούται υποστήριξης τέτοιων υπηρεσιών) και επιστρέφεται μια θετική ή αρνητική απάντηση.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element

```

```

name="timestamp_request_Output"
type="timestamp_request_Output_Type"/>
<xsd:attribute name="encoding" type      ="xsd:base64Binary"
use="required"/>

<!-- Η έξοδος περιλαμβάνει το χρησιμοποιούμενο πιστοποιητικό και
μια θετική ή αρνητική απάντηση στο αίτημα --&gt;

&lt;xsd:complexType name=" timestamp_request_Output_Type"&gt;
  &lt;xsd:sequence&gt;
    &lt;xsd:element name="user_certificate" type="xsd:base64Binary"   "
use="required"/&gt;
    &lt;xsd:element
name="timestamp_request_Output_Answer"
type="xsd:boolean" use="required"/&gt;
  &lt;/xsd:sequence&gt;
&lt;/xsd:complexType&gt;
&lt;/xsd:schema&gt;
</pre>

```

4.1.4 Παραγωγή χρονοσφαγίδας

Αποτελεί τη βασική λειτουργία της υπηρεσίας χρονοσήμανσης. Δέχεται σαν είσοδο τη θετική απάντηση στην αίτηση για χρονοσήμανση των δεδομένων του αιτούντος και επιστρέφεται μία ψηφιακά υπογεγραμμένη δομή από τον Οργανισμό των δεδομένων χρονοσήμανσης με τον ασφαλή χρόνο (όπως ορίστηκε παραπάνω) και έναν σειριακό αριθμό που θα χρησιμοποιηθεί για την αποθήκευση της χρονοσφαγίδας και τη γρήγορη ανάκτηση της σε άλλες παρεχόμενες υπηρεσίες από τον Οργανισμό (π.χ. παροχή αποδεικτικών στοιχείων)

Είσοδος

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!-- Ο τύπος της εισόδου είναι αυτός της εξόδου που περιγράφηκε
στην παράγραφο στην παράγραφο [4.1.3] --&gt;

&lt;xsd:element
name="timestamp_input" type="timestamp_request_Output"/&gt;
&lt;/xsd:schema&gt;
</pre>

```

Έξοδος: Επιστρέφεται μία ψηφιακά υπογεγραμμένη δομή από τον Οργανισμό της σύνοψης των δεδομένων χρονοσήμανσης. Η αιτούσα οντότητα με τη σειρά της επιβεβαιώνει την εγκυρότητα της επιστρεφόμενης χρονοσφαγίδας. Δηλαδή, ελέγχει την ψηφιακή υπογραφή του Οργανισμού, αν τα δεδομένα που χρονοσημάνθηκαν είναι αυτά που απεστάλησαν και αν ο χρόνος χρονοσήμανσης είναι αποδεκτός και μέσα στα πλαίσια της Πολιτικής Ασφαλείας του Οργανισμού. Η μορφοποίηση της εξόδου με τη χρήση της XML Schema είναι η παρακάτω :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="timestamp" type="timestamp_Type"/>
  <xsd:complexType name=" timestamp_Type">
    <xsd:sequence>
      <!-- Ο τύπος εξόδου περιλαμβάνει μια σειρά από χρονοσφαγίδες
          αντίστοιχες προς τον αριθμό της εισόδου. Επίσης επιστρέφεται και
          ένας σειριακός αριθμός που προκύπτει από το σύστημα αρχειοθέτησης
          και χρησιμοποιείται για την παροχή της υπηρεσίας της
          Συμβολαιογραφίας και των Αποδεικτικών Στοιχείων-->
    <xsd:element name="user_certificate" type="xsd:base64Binary"
      minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name ="message_hash" type="message_hash_Type"/>
      <xsd:element name ="secure_time" type="secure_time_Type"/>
      <xsd:element name = "serial_no" type="xsd:unsignedLong"
        use="required"/>
      <xsd:element name="timestamp_digest"
        type="xsd:base64Binary" use="required"/>
      <xsd:element name ="digest_algorithm" type="xsd:string"
        use="required"/>
    </xsd:sequence>
  </xsd:complexType>
  <xsd:complexType name ="message_hash_Type">
    <xsd:sequence>
      <xsd:element name="message_hash" use="required">
        <xsd:complexType>
          <xsd:element
            name="algorithm_id" type="xsd:string" use="required"/>
          <xsd:element
            name="hash_value" type="xsd:string" use="required"/>
    
```

```

    </xsd:complexType>
    </xsd:element>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.1.5 Επαλήθευση χρονοσφαγίδας

Είναι σημαντικό όποιος διαθέτει μια χρονοσφαγίδα να μπορεί ανά πάσα στιγμή να επιβεβαιώσει την εγκυρότητά της. Σε αυτή την περίπτωση επαληθεύεται η ψηφιακή υπογραφή του Οργανισμού που υπάρχει στη χρονοσφαγίδα, παράγεται η σύνοψη του αρχικού κειμένου και επαληθεύεται με αυτόν της χρονοσφαγίδας και στο τέλος επιστρέφεται η θετική ή αρνητική απάντηση στον αιτούντα. Περιγραφικά με τη χρήση της XML Schema η είσοδος και η έξοδος της συγκεκριμένης διαδικασίας είναι:

Είσοδος

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="timestamp_verification_Input"
              type="timestamp_verification_Input_Type"/>
<xsd:complexType name=" timestamp_verification_Input_Type">
    <xsd:sequence>
        <xsd:element name="user_certificate" type="xsd:base64Binary"
use="required"/>
        <xsd:element name ="message_hash" type="message_hash_Type"/>
        <xsd:element name="timestamp_digest"
                     type="xsd:base64Binary" use="required"/>
        <xsd:element name      ="digest_algorithm"      type="xsd:string"
use="required"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name ="message_hash_Type">
    <xsd:sequence>
        <xsd:element name="message_hash" use="required">
            <xsd:complexType>
                <xsd:element name="algorithm_id" type="xsd:string"
use="required"/>

```

```

<xsd:element           name="hash_value"          type="xsd:string"
use="required"/>

</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : η έξοδος περιλαμβάνει μια θετική ή αρνητική απάντηση και τον ασφαλή χρόνο επαλήθευσης της χρονοσφαγίδας. Περιγράφεται με τη χρήση της XML Schema με την παρακάτω δομή:

```

<xsd:schema xmlns:xsd = "http://www.w3.org/2001/XMLSchema">
<xsd:element
name="timestamp_verification" type="timestamp_verification_Type"/>
<!-- Η έξοδος περιλαμβάνει μια θετική ή αρνητική απάντηση και τον
ασφαλή χρόνο αναφοράς όπως ορίστηκε στην παράγραφο [4.1.2] -->
<xsd:complexType name=" timestamp_verification_Type">
  <xsd:sequence>
    <xsd:element name      ="verification_value"   type="xsd:boolean"
use="required"/>
    <xsd:element name = "secure_time" type="secure_time_Type"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.1.6 Διατήρηση χρονοσφαγίδων

Αποτελεί μια βασική λειτουργία της χρονοσήμανσης. Οι παραγόμενες χρονοσφαγίδες δεν έχουν καμία αξία για τον χρήστη ή τον Οργανισμό αν αυτές δεν αποθηκευτούν σωστά. Με τον όρο σωστά, εννοούμε την αποθήκευση σε μια Σχεσιακή Βάση Δεδομένων όπου να αναδεικνύεται η αλληλουχία των συσχετιζόμενων χρονοσφαγίδων ικανή να χρησιμοποιηθεί σε άλλες προσφερόμενες υπηρεσίες από τον Οργανισμό (π.χ. παροχή αποδεικτικών στοιχείων). Για την καλύτερη οργάνωση της Βάσης Δεδομένων χρησιμοποιείται ο μοναδικός σειριακός αριθμός κάθε παραγόμενης χρονοσφαγίδας ενώ αποθηκεύεται και η σύνοψη των

κειμένων περιεχόμενων χρονοσφαγίδων. Η προτεινόμενη Σχεσιακή Βάση Δεδομένων [βλ. § 5.2.3.2] υποστηρίζει την παραγωγή αλληλουχίας χρονοσφαγίδων.

Είσοδος

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="timestamp_store" type="timestamp_store_Type"/>

<xsd:complexType name=" timestamp_store_Type">
  <xsd:sequence>
    <xsd:element
      name="serial_no" type="xsd:unsignedLong" use="required"/>
    <xsd:element
      name="timestamp" type="xsd:unsignedLong" use="required"/>
    <!--Ο τύπος της χρονοσφαγίδας που ορίστηκε στην παράγραφο
$4.1.4]-->
    <xsd:element
      name="valid_timestamp" ref="timestamp" use="required"/>
    <!-- Ο διαχειριστής των παραγόμενων χρονοσφαγίδων δηλώνει στο
element timestamp_store_path το σημείο αποθήκευσής τους (κατά βάση
το όνομα της χρησιμοποιούμενης Βάσης Δεδομένων)-->
    <xsd:element      name="timestamp_store_path"      type="xsd:string"
use="required"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

Έξοδος

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
  name="timestamp_store_Output" type="timestamp_store_Output_Type"/>
<!-- Επιβεβαιώνεται η όχι η διαδικασία αποθήκευσης και αν η
απάντηση είναι θετική επιστρέφονται ο σειριακός αριθμός και η
τοποθεσία του μέσου αποθήκευσης-->
<xsd:complexType name=" timestamp_store_Output_Type">
  <xsd:sequence>
    <xsd:element
```

```

name="timestamp_store_response" type="xsd:boolean" use="required"/>
<xsd:element
name="timestamp_serial_no" type="xsd:unsignedLong" use="required"/>
<xsd:element name="timestamp_store_path"
type="xsd:string"
use="required"/>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.2 Συμβολαιογραφία

4.2.1 Εισαγωγή

Μία συμβολαιογραφική πράξη καθιστά έγκυρο και επικυρώνει την ακεραιότητα του περιεχομένου ενός εγγράφου, έτσι όπως διατυπώθηκε μια συγκεκριμένη χρονική στιγμή, δίνοντας τη δυνατότητα επικύρωσης της εγκυρότητάς του από οποιοδήποτε για οποιαδήποτε στιγμή στο μέλλον. Αντίστοιχα, σε ένα ηλεκτρονικό περιβάλλον οι συμβολαιογραφικές υπηρεσίες (notary services) έχουν ως στόχο να πιστοποιήσουν ένα ηλεκτρονικό έγγραφο ως προς την αυθεντικότητά του, την ακεραιότητά του και την ύπαρξή του σε μία συγκεκριμένη χρονική στιγμή [Λέκκας]. Ως ηλεκτρονικό έγγραφο μπορούμε να θεωρήσουμε οποιαδήποτε δυαδικά δεδομένα που σχηματίζουν μία μορφή πληροφορίας και μπορούν να αποθηκευθούν σε μορφή μεγάλου δυαδικού αντικειμένου (Binary Large Object – BLOB). Ηλεκτρονικά έγγραφα μπορεί να είναι μία συναλλαγή, μία εγγραφή μίας βάσης δεδομένων, ένα αρχείο κειμένου και ψηφιοποιημένες εικόνες, ήχοι και βίντεο.

Η παροχή της υπηρεσίας της συμβολαιογραφίας από έναν Οργανισμό κάνει χρήση και άλλων Βασικών και Προστιθέμενης Αξίας υπηρεσιών όπως της Χρονοσήμανσης, της Παροχής Αποδείξεων, της Διαχείρισης Πιστοποιητικών, της υπηρεσίας Ευρετηρίου και της Αρχειοθέτησης. Η λειτουργία της υπηρεσίας αυτής συνίσταται στη λήψη ηλεκτρονικών εγγράφων από τους πελάτες του Οργανισμού, την επικύρωση κάποιων χαρακτηριστικών τους με τη χρήση κρυπτογραφικών τεχνικών και την αποθήκευσή τους μαζί με άλλες πληροφορίες, έτσι ώστε η εγκυρότητά τους να μπορεί να επιβεβαιωθεί στο μέλλον με ανάλογες κρυπτογραφικές

τεχνικές. Σε αντίθεση με την υπηρεσία της Χρονοσήμανσης ελέγχεται το περιεχόμενο του πιστοποιημένου εγγράφου και επισυνάπτονται κάποια χαρακτηριστικά όπως η ιδιοκτησία, τα πνευματικά δικαιώματα, η ορθότητα της μορφοποίησης του περιεχομένου σύμφωνα με κάποιο πρότυπο, η ισχύ των κρυπτογραφικών κλειδιών που χρησιμοποιήθηκαν κατά τη διάρκεια της τεκμηρίωσης και η χρονική συνέπεια του εγγράφου ως προς κάποιο από τα χαρακτηριστικά του [Λέκκας]. Η λειτουργία της υπηρεσίας πρέπει να λαμβάνει υπόψη της τις δυνατότητες για ευελιξία, αποδοτικότητα και ασφάλεια [Tak].

Η συγκεκριμένη υπηρεσία μπορεί να προσφέρεται και ως αυτόνομη υπηρεσία και σε αυτή την περίπτωση ο Οργανισμός αναφέρεται στη σύγχρονη βιβλιογραφία και ως Συμβολαιογραφική Αρχή (Notarization Authority).

4.2.2 Επικύρωση εγκυρότητας εγγράφου

Η διαδικασία περιλαμβάνει τη μέθοδο της ενθυλάκωσης διαφόρων μηχανισμών που προσθέτουν αξία στο ηλεκτρονικό έγγραφο. Για την αποθήκευση του περιεχομένου του εγγράφου υπάρχουν οι λύσεις της σύνοψης του περιεχομένου όπου το περιεχόμενο δεν περιέχεται αυτούσιο στο τεκμήριο και δεν γνωστοποιείται στον Οργανισμό, αλλά εισάγεται μία σύνοψή του η οποία το προσδιορίζει μονοσήμαντα και συνεπώς μόνο ο κάτοχος του εγγράφου μπορεί να αναπαράγει τη σύνοψη και να ελέγξει την εγκυρότητα του τεκμηρίου και η λύση του κρυπτογραφημένου περιεχομένου όπου το περιεχόμενο είναι εμπιστευτικό και μόνο ο κάτοχος του κλειδιού αποκρυπτογράφησης μπορεί να το ανακτήσει και να επιβεβαιώσει την εγκυρότητά του, χωρίς απαραίτητα να κατέχει εκ των προτέρων το έγγραφο.

Η αξία της υπηρεσίας συνίσταται στο βαθμό εμπιστοσύνης που επιδεικνύει ο χρήστης προς τη Συμβολαιογραφική Αρχή για την επικύρωση των δεδομένων και όχι στον κάτοχο ή τον υπογράφοντά τους. Η υπογραφή ενός αντικειμένου δεν αποδεικνύει και την εγκυρότητά του.

Είσοδος : Σαν είσοδος για την επικύρωση αποστέλλεται το BLOB αρχείο, ο τύπος του αρχείου, κάποια στοιχεία αυθεντικοποίησης του αιτούντος και μια ένδειξη εμπιστευτικότητας (π.χ. ένα ή περισσότερα ψηφιακά πιστοποιητικά). Με τη χρήση της XML Schema αυτό περιγράφεται ως εξής :

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

```

<xsd:element name="notarization_Input"
type="notarization_Input_Type"/>

<xsd:complexType name="notarization_Input_Type">
  <xsd:sequence>
    <!-- Η είσοδος μπορεί να περιλαμβάνει ένα ή περισσότερα ψηφιακά
    πιστοποιητικά -->
    <xsd:element name="user_cert"
type="xsd:base64Binary"
minOccurs="1" maxOccurs="unbounded"/>
    <xsd:element name="user_signature" type="xsd:base64Binary"
use="required"/>
    <xsd:element name="BLOB_info" type="BLOB_Type"/>
    <xsd:element name="object_info" type="object_info_Type"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="BLOB_Type">
  <xsd:sequence>
    <xsd:element name="BLOB_info" use="required">
      <xsd:choice>
        <!-- To element BLOB_info μπορεί να περιλαμβάνει είτε το ίδιο το
        δυαδικό αρχείο ή την παραγόμενη σύνοψή του -->
        <xsd:element name="BLOB" type="xsd:string"/>
        <xsd:group name="BLOB_hash_info" ref="BLOB_hash_info_type"/>
      </xsd:choice>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<!-- Στην περίπτωση που περιλαμβάνεται η σύνοψη πρέπει να υπάρχουν
δύο στοιχεία που να υποδεικνύουν τη σύνοψη και το χρησιμοποιούμενο
αλγόριθμο σύνοψης-->
<xsd:group name="BLOB_hash_info_type">
  <xsd:sequence>
    <xsd:element name="BLOB_hash" type="xsd:string"
use="required"/>
  
```

```

<xsd:element      name="hash_algorithm"      type="xsd:string"
use="required"/>
</xsd:sequence>
</xsd:group>

<!-- To element object_info_Type περιέχει τα στοιχεία για την
ψηφιακή διασφάλιση των πνευματικών δικαιωμάτων-->

<xsd:complexType name="object_info_Type">
  <xsd:sequence>
    <xsd:element name="object_info" use="required">
      <xsd:complexType>
        <xsd:element name="title" type="xsd:string" use="required"/>
        <xsd:element name="mime_type" type="xsd:string" use="required"/>
        <xsd:element name="format" type="xsd:string" use="required"/>
        <xsd:element name="copyright" type="xsd:string" use="required"/>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Μετά την επικύρωση του αποστολέα, ελέγχονται κάποια από τα στοιχεία του εγγράφου, επικυρώνονται με την υπογραφή του Οργανισμού, χρονοσημαίνονται (όπως περιγράφηκε στην §4.1.4), αποθηκεύονται από τον Οργανισμό και το συμβολαιογραφικό τεκμήριο αποστέλλεται στον αιτούντα. Περιγράφοντας το συμβολαιογραφικό τεκμήριο με XML Schema έχουμε :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element          name="notarization_token"
type="notarization_token_Type"/>
  <xsd:attribute name="private" type="xsd:string" fixed="no"/>

  <xsd:complexType name="notarization_token_Type">
    <xsd:sequence>
      <xsd:element
name="user_cert"
type="xsd:base64Binary" minOccurs="1" maxOccurs="unbounded"/>

```

```

<xsd:element      name="user_signature"      type="xsd:base64Binary"
use="required"/>

<xsd:element name="BLOB_info" type="BLOB_Type"/>
<!-- Ο σειριακός χρησιμοποιείται για την διαδικασία αποθήκευσης
και ανάκτησης-->

<xsd:element name="serial_no" type="xsd:unsignedLong"/>
<!-- Ο τύπος του αντικειμένου (object_info) έχει την ίδια δομή που
περιγράφηκε κατά την είσοδο της επικύρωσης της εγκυρότητας-->

<xsd:element name="object_info" type="object_info_Type"/>
<xsd:element      name="TTP_signature"      type="xsd:base64Binary"
use="required"/>
<!-- Η χρονοσφαγίδα είναι του τύπου της §4.1.4-->

<xsd:element name="timestamp" type="timestamp_Type"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="BLOB_Type">
<xsd:sequence>
<xsd:element name="BLOB_info" use="required">
<xsd:choice>
<xsd:element name="BLOB" type="xsd:string"/>
<xsd:group name="BLOB_hash_info" ref="BLOB_hash_info_type"/>
</xsd:choice>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:group name="BLOB_hash_info_type">
<xsd:sequence>
<xsd:element      name="BLOB_hash"      type="xsd:string"
use="required"/>
<xsd:element      name="hash_algorithm"      type="xsd:string"
use="required"/>
</xsd:sequence>
</xsd:group>

<xsd:complexType name="object_info_Type">

```

```

<xsd:sequence>
  <xsd:element name="object_info" use="required">
    <xsd:complexType>
      <xsd:element name="title" type="xsd:string" use="required"/>
      <xsd:element name="mime_type" type="xsd:string" use="required"/>
      <xsd:element name="format" type="xsd:string" use="required"/>
      <xsd:element name="copyright" type="xsd:string" use="required"/>
    </xsd:complexType>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.2.3 Επαλήθευση συμβολαιογραφικού τεκμηρίου

Όπως αναφέρθηκε και στην περίπτωση της Χρονοσήμανσης, έτσι και εδώ είναι απαραίτητη η δυνατότητα επαλήθευσης των συμβολαιογραφικών τεκμηρίων για την επίλυση διενέξεων και την παροχή αποδεικτικών στοιχείων. Ουσιαστικά ελέγχεται η παραγόμενη χρονοσφαγίδα του τεκμηρίου, η ψηφιακή υπογραφή του Οργανισμού και του κατόχου και το περιεχόμενο (ανάλογα με τον τρόπο αποθήκευσης του ο οποίος και αναλύθηκε στην εισαγωγή). Αν όλοι αυτοί οι έλεγχοι είναι επιτυχείς τότε επιστρέφεται στον αιτούντα μια τιμή εγκυρότητας του συμβολαιογραφικού τεκμηρίου.

Είσοδος : Περιέχει το ίδιο το έγγραφο ή τη σύνοψη του και το συμβολαιογραφικό τεκμήριο.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
  name="notarization_verification_Input"
  type="notarization_verification_Input_Type"/>

<xsd:complexType name="notarization_verification_Input_Type">
  <xsd:sequence>
    <xsd:element name="BLOB_file" type="BLOB_type"/>
    <!--Είναι του το τεκμήριο του τύπου που ορίστηκε στην §4.2.2-->
    <xsd:element name ="notarization" ref="notarization_token"/>
  </xsd:sequence>
</xsd:complexType>

```

```

</xsd:complexType>

<xsd:complexType name="BLOB_Type">
  <xsd:sequence>
    <xsd:element name="BLOB_info" use="required">
      <xsd:choice>
        <xsd:element name="BLOB" type="xsd:string"/>
        <xsd:group name="BLOB_hash_info" ref="BLOB_hash_info_type"/>
      </xsd:choice>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:group name="BLOB_hash_info_type">
  <xsd:sequence>
    <xsd:element name="BLOB_hash" type="xsd:string"
use="required"/>
    <xsd:element name="hash_algorithm" type="xsd:string"
use="required"/>
  </xsd:sequence>
</xsd:group>
</xsd:schema>

```

Έξοδος : Επιστρέφεται η δυαδική τιμή απόδειξης εγκυρότητας και ένας σειριακός αριθμός για την αποθήκευση στη Βάση Δεδομένων του Οργανισμού παροχής αποδεικτικών τεκμηρίων. Με τη χρήση της XML Schema αυτό περιγράφεται ως εξής

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
  name="notarization_verification"
  type="notarization_verification_Type"/>

<xsd:complexType name="notarization_verification_Type">
  <xsd:sequence>
    <xsd:element name="verification_value" type="xsd:boolean"
use="required"/>

```

```

<xsd:element      name="serial_no"      type=""      xsd:unsignedLong"
use="required"/>

</xsd:sequence>

</xsd:complexType>

</xsd:schema>

```

4.3 Παροχή Αποδεικτικών Στοιχείων

4.3.1 Εισαγωγή

Η υπηρεσία διαχείρισης αποδείξεων (evidence management) παρέχει τις λειτουργίες για τη δημιουργία, αποθήκευση και ανάκτηση των στοιχείων που αποδεικνύουν ότι μια συγκεκριμένη οντότητα επεξεργάστηκε ή εκτέλεσε κάποιες ενέργειες σε ένα σύνολο δεδομένων. Τα στοιχεία πρέπει να είναι τέτοια και σε ανάλογη μορφή ώστε να μπορούν να πείσουν μια ανεξάρτητη οντότητα, σε χρονικά μεταγενέστερη στιγμή από εκείνη της επεξεργασίας, σχετικά με την εγκυρότητα του ισχυρισμού αυτού. Τα στοιχεία που παρέχονται από την υπηρεσία αυτή χρησιμοποιούνται σε περιπτώσεις όπου απαιτείται διαιτησία για την επίλυση διενέξεων μεταξύ δύο ή περισσότερων συναλλασσομένων όταν τουλάχιστον ένας από τους οποίους βρίσκεται μέσα στο πεδίο ασφάλειας του Οργανισμού [Λέκκας]. Η παροχή της υπηρεσίας της διαχείρισης αποδεικτικών στοιχείων από έναν Οργανισμό κάνει χρήση και άλλων βασικών και προστιθέμενης αξίας υπηρεσιών όπως της Χρονοσήμανσης, της Συμβολαιογραφίας, της Αρχειοθέτησης και της υπηρεσίας των ψηφιακών υπογραφών.

Για τη διασφάλιση της υπηρεσίας χρησιμοποιούνται οι δυνατότητες που μας παρέχουν οι υπηρεσίες της Χρονοσήμανσης και της Συμβολαιογραφίας και ιδιαίτερα η χρήση των ψηφιακών υπογραφών και φακέλων [Zhou1], ενώ η εμπιστευτικότητα για τη χρήση της υπηρεσίας πηγάζει από τις δεδηλωμένες Πολιτικές Ασφάλειας και επεξεργασίας των δεδομένων που προσφέρει ο Οργανισμός και από τη μέθοδο μεταφοράς του δυαδικού αρχείου (ποιο πρωτόκολλο χρησιμοποιείται και ποιος είναι ο τύπος των διακινούμενων δεδομένων)[Zhou1].

Η διαχείριση των αποδεικτικών στοιχείων εξελίσσεται στις εξής φάσεις [ISO-10181],[Tak]:

- **Παραγωγή στοιχείων:** Εκτελείται είτε από τον εκτελούντα τη διεργασία είτε από τον Οργανισμό για λογαριασμό του αιτούντα και πραγματοποιείται κατά την εκτέλεση μιας διεργασίας που απαιτείται η καταγραφή.
- **Αποθήκευση και ανάκτηση στοιχείων:** Είναι οι διεργασίες μεταφοράς των αποδεικτικών στοιχείων σε αποθηκευτικά μέσα.
- **Επαλήθευση αποδεικτικών στοιχείων:** κάθε οντότητα θα πρέπει να μπορεί να επαληθεύει τα αποδεικτικά τεκμήρια κάποιων ενεργειών του.
- **Επίλυση διενέξεων και διαιτησία:** Ο διαιτητής συλλέγει τεκμήρια και αποδεικτικά στοιχεία από τα συναλλασσόμενα μέρη ή από τον Οργανισμό για την επίλυση τυχόν διενέξεων μεταξύ τους. Τα τεκμήρια αυτά θα πρέπει να είναι αποδεδειγμένα ακριβή και έγκυρα.

4.3.2 Αίτηση για δημιουργία αποδεικτικών στοιχείων

Ένα αποδεικτικό τεκμήριο για να μπορεί να είναι ολοκληρωτικά ακριβές και έγκυρο θα πρέπει να περιλαμβάνει πέντε (5) ειδών αποδεικτικά στοιχεία [Herda][Tak]. Την απόδειξη προέλευσης (origin) που χρησιμοποιείται για τη μη αποποίησης αποστολής του δημιουργού του μηνύματος ή όταν ο παραλήπτης αμφισβητήσει την προέλευσή του, την απόδειξη υποβολής (submission) που χρησιμοποιείται για την απόδειξη αποστολής ενός μηνύματος ή τουλάχιστον για την πρόθεσή του, την απόδειξη παράδοσης (delivery) που αποδεικνύει πως το μήνυμα έχει τουλάχιστον φτάσει στη μεριά του παραλήπτη, την απόδειξη παραλαβής (receipt) που αποδεικνύει πως ο παραλήπτης έλαβε γνώση του περιεχομένου του μηνύματος και τέλος την απόδειξη ιδιοκτησίας (ownership) που εξετάζει την κατοχή ενός εγγράφου κάποια χρονική στιγμή. Επομένως, μία αίτηση για δημιουργία αποδεικτικών στοιχείων πρέπει να περιλαμβάνει μία από αυτές τις αποδείξεις. Η απόδειξη της μη αποποίησης ενός από τα πέντε αποδεικτικά στοιχεία γίνεται με τη χρήση των δίκαιων πρωτοκόλλων (*fair protocols*). Κύριο χαρακτηριστικό τους είναι πως είτε ο αποστολέας ενός μηνύματος στο τέλος του πρωτοκόλλου λαμβάνει το τεκμήριο υποβολής και ο παραλήπτης το τεκμήριο παραλαβής ή και οι δύο δε λαμβάνουν κανένα τεκμήριο [Kremer]. Ο ρόλος του Οργανισμού σε ένα τέτοιο πρωτόκολλο είναι διαφορετικός, πολλαπλός και εξαρτάται από τη συμμετοχή του Οργανισμού στη δημιουργία των τεκμηρίων. Διακρίνεται σε απόλυτα ενεργός (*inline*), ενεργός (*online*), όταν κρίνεται απαραίτητος (*offline*) και διαφανής (*transparent*)

[Kremer]. Σημαντικές ωστόσο είναι και οι υλοποιήσεις που χρησιμοποιούν τις απλές κρυπτογραφικές λειτουργίες για την παροχή της συγκεκριμένης υπηρεσίας [Zhou2]

Είσοδος : Αίτημα αποστολής αποδεικτικών στοιχείων όπως περιγράφηκε παραπάνω. Περιλαμβάνονται κάποια στοιχεία αυθεντικοποίησης του αιτούντος, το είδος της απόδειξης (προέλευσης, υποβολής, παράδοσης, παραλαβής, ιδιοκτησίας) και η σύνοψη του μηνύματος. Με τη χρήση της XML Schema αυτή περιγράφεται ως εξής :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element
    name="evidence_token_request" type="evidence_token_request_Type">
    <!--To attribute token_type δηλώνει το είδος της απόδειξης (προέλευσης, υποβολής, παράδοσης, παραλαβής, ιδιοκτησίας)-->
  </xsd:element>

  <xsd:attribute name="token_type" type ="Type_Of_Token"/>

  <xsd:complexType name="evidence_token_request_Type">
    <xsd:sequence>
      <!-- Δηλώνεται η ταυτότητα του δημιουργού του τεκμηρίου-->
      <xsd:element name="creator_DN" type="creator_DN_Type"/>
      <!-- Δηλώνεται το ψηφιακό πιστοποιητικό-->
      <xsd:element name="creator_cert" type="xsd:base64Binary"
        use="required"/>
      <!-- Δηλώνεται η οντότητα προέλευσης-->
      <xsd:element name ="origin" type="origin_Type"/>
      <!--Δηλώνονται και δύο elements που προσδιορίζουν τη σύνοψη του μηνύματος-->
      <xsd:element name="message_hash" type="xsd:string"
        use="required"/>
      <xsd:element name="hash_algorithm" type="xsd:string"
        use="required"/>
    </xsd:sequence>
  </xsd:complexType>
  <!-- Τα στοιχεία του δημιουργού πρέπει να περιλαμβάνει τα παρακάτω στοιχεία-->
  <xsd:complexType name ="creator_DN_Type">
    <xsd:sequence>

```

```

<xsd:element name="creator_DN">
  <xsd:complexType>
    <xsd:attribute name="cn" type="xsd:string" use="required"/>
    <xsd:attribute name="ou" type="xsd:string" use="required"/>
    <xsd:attribute name="o" type="xsd:string" use="required"/>
    <xsd:attribute name="c" type="xsd:string" use="required"/>
  </xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<!-- Η ταυτότητα της οντότητας προέλευσης μπορεί να συμπληρώνεται με ένα από τα παρακάτω δύο διακριτικά στοιχεία-->

<xsd:complexType name="origin_Type">
  <xsd:sequence>
    <xsd:choice>
      <xsd:element name="origin_id" type="xsd:string"/>
      <xsd:element name="origin_cert" type="xsd:base64Binary"/>
    </xsd:choice>
  </xsd:sequence>
</xsd:complexType>

<!-- Το είδος της απόδειξης μπορεί να πάρει μία από τις παρακάτω τιμές-->

<xsd:simpleType name="Type_Of_Token">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="origin"/>
    <xsd:enumeration value="submission"/>
    <xsd:enumeration value="delivery"/>
    <xsd:enumeration value="receipt"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Έξοδος : Παράγεται το αποδεικτικό τεκμήριο που περιέχει τουλάχιστο τα παρακάτω στοιχεία: Την ταυτότητα του δημιουργού του, τη χρονική στιγμή που εκτελέστηκε η

πράξη σύμφωνα με αυτή την οντότητα, τις ταυτότητες των οντοτήτων που αποτελούν την αρχική προέλευση και τον τελικό προορισμό των δεδομένων, τον τύπο του τεκμηρίου, μία σύνοψη των διακινούμενων δεδομένων, ένα μοναδικό κωδικό αναφοράς στο μήνυμα και την ψηφιακή υπογραφή του δημιουργού σε ολόκληρο το τεκμήριο. Με την XML Schema αυτή περιγράφεται ως:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="evidence_token" type="evidence_token_Type"/>
  <xsd:attribute name="token_type" type ="Type_Of_Token"/>

  <xsd:complexType name="evidence_token_Type">
    <xsd:sequence>
      <xsd:element name="creator_DN" type="creator_DN_Type"/>
      <xsd:element name="creator_cert" type="xsd:base64Binary"
use="required"/>
      <xsd:element name="origin" type="origin_Type"/>
      <!-- Η ταυτότητα του τελικού προορισμού των δεδομένων-->
      <xsd:element name="destination" type="destination_Type"/>
      <!-- Η χρονική στιγμή εκτέλεσης της πράξης-->
      <xsd:element name="ref_time" type="ref_time_Type"/>
      <!-- Παράγεται ένας μοναδικός κωδικός αναφοράς στο μήνυμα, η
σύνοψη του μηνύματος και ο χρησιμοποιούμενος αλγόριθμος-->
      <xsd:element name="message_id" type="xsd:Long"
use="required"/>
      <xsd:element name="message_hash" type="xsd:string"
use="required"/>
      <xsd:element name="hash_algorithm" type="xsd:string"
use="required"/>
      <!-- Επισυνάπτεται και ψηφιακή υπογραφή του δημιουργού του
τεκμηρίου σε όλο το μήνυμα-->
      <xsd:element name="signature" type="xsd:string"
use="required"/>
    </xsd:sequence>
  </xsd:complexType>
  <!-- Στοιχεία οντότητας παροχής τεκμηρίου-->
  <xsd:complexType name="creator_DN_Type">
    <xsd:sequence>

```

```

<xsd:element name="creator_DN">
  <xsd:complexType>
    <xsd:attribute name="cn" type="xsd:string" use="required"/>
    <xsd:attribute name="ou" type="xsd:string" use="required"/>
    <xsd:attribute name="o" type="xsd:string" use="required"/>
    <xsd:attribute name="c" type="xsd:string" use="required"/>
  </xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<!-- Η ταυτότητα της οντότητας προέλευσης μπορεί να συμπληρώνεται με ένα από τα παρακάτω δύο διακριτικά στοιχεία--&gt;

&lt;xsd:complexType name="origin_Type"&gt;
  &lt;xsd:sequence&gt;
    &lt;xsd:choice&gt;
      &lt;xsd:element name="origin_id" type="xsd:string"/&gt;
      &lt;xsd:element name="origin_cert" type="xsd:base64Binary"/&gt;
    &lt;/xsd:choice&gt;
  &lt;/xsd:sequence&gt;
&lt;/xsd:complexType&gt;

<!-- Η ταυτότητα της οντότητας προορισμού μπορεί να συμπληρώνεται με ένα από τα παρακάτω δύο διακριτικά στοιχεία--&gt;

&lt;xsd:complexType name="destination_Type"&gt;
  &lt;xsd:sequence&gt;
    &lt;xsd:choice&gt;
      &lt;xsd:element name="destination_id" type="xsd:string"/&gt;
      &lt;xsd:element name="destination_cert" type="xsd:base64Binary"/&gt;
    &lt;/xsd:choice&gt;
  &lt;/xsd:sequence&gt;
&lt;/xsd:complexType&gt;

<!-- Παράγεται η χρονική στιγμή εκτέλεσης της πράξης--&gt;

&lt;xsd:complexType name="ref_time_Type"&gt;
  &lt;xsd:sequence&gt;
    &lt;xsd:element name="source" type="xsd:base64Binary"
      fixed="system"/&gt;
</pre>

```

```

<xsd:element name="time" type="xsd:date" use="required"/>
<xsd:element name="zone" type="zone_Type"/>
</xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="zone_Type">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="GMT-12"/>
    <xsd:enumeration value="GMT-11"/>
    <xsd:enumeration value="GMT-10"/>
    <xsd:enumeration value="GMT-9"/>
    <xsd:enumeration value="GMT-8"/>
    <xsd:enumeration value="GMT-7"/>
    <xsd:enumeration value="GMT-6"/>
    <xsd:enumeration value="GMT-5"/>
    <xsd:enumeration value="GMT-4"/>
    <xsd:enumeration value="GMT-3"/>
    <xsd:enumeration value="GMT-2"/>
    <xsd:enumeration value="GMT-1"/>
    <xsd:enumeration value="GMT"/>
    <xsd:enumeration value="GMT+12"/>
    <xsd:enumeration value="GMT+11"/>
    <xsd:enumeration value="GMT+10"/>
    <xsd:enumeration value="GMT+9"/>
    <xsd:enumeration value="GMT+8"/>
    <xsd:enumeration value="GMT+7"/>
    <xsd:enumeration value="GMT+6"/>
    <xsd:enumeration value="GMT+5"/>
    <xsd:enumeration value="GMT+4"/>
    <xsd:enumeration value="GMT+3"/>
    <xsd:enumeration value="GMT+2"/>
    <xsd:enumeration value="GMT+1"/>
  </xsd:restriction>
</xsd:simpleType>
<!-- Επισυνάπτεται το είδος της απόδειξης-->
<xsd:simpleType name="Type_Of_Token">

```

```

<xsd:restriction base="xsd:string">
  <xsd:enumeration value="origin"/>
  <xsd:enumeration value="submission"/>
  <xsd:enumeration value="delivery"/>
  <xsd:enumeration value="receipt"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

4.3.3 Συλλογή αποδεικτικών στοιχείων

Όπως αναφέρθηκε και παραπάνω για να θεωρηθεί μια συναλλαγή επιτυχής ως προς τα αποδεικτικά τεκμήρια πρέπει να δημιουργηθούν όλες οι επιμέρους αποδείξεις (προέλευσης, υποβολής, παράδοσης και υποβολής). Σε διαφορετική περίπτωση χαρακτηρίζεται μερική ή αποτυχημένη. Ο χαρακτηρισμός της συναλλαγής καθορίζεται στην πολιτική πιστοποίησης του Οργανισμού. Ο Οργανισμός είναι υπεύθυνος για τη συλλογή των αποδεικτικών τεκμηρίων που σχετίζονται σε μία συναλλαγή.

Είσοδος : Περιλαμβάνει τη δημιουργία των αποδεικτικών τεκμηρίων που αποστέλλονται από τις εμπλεκόμενες οντότητες και σχετίζονται με μία συναλλαγή.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element
    name="evidence_collection_Input"
    type="evidence_collection_Input_Type">
    <!-- Η είσοδος είναι μια σειρά από αποδεικτικά τεκμήρια απόδειξης-->

    <xsd:complexType name="evidence_token_Input_Type">
      <xsd:sequence>
        <xsd:element name="message_id" type="xsd:unsignedLong"
use="required"/>

```

<!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα τεκμήρια απόδειξης προέλευσης [βλ §4.3.2] και την αντίστοιχη χρονοσφαγίδα [βλ §4.1.4]-->

```

<xsd:element
    name="evidence_token"
    type="evidence_token_Type"
    minOccurs="0" maxOccurs="unbounded">
    <xsd:restriction base="token_type:origin"/>
    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
</xsd:element>

```

<!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα τεκμήρια απόδειξης υποβολής [§4.3.2] και την αντίστοιχη χρονοσφαγίδα [βλ §4.1.4]-->

```

<xsd:element
    name="evidence_token"
    type="evidence_token_Type"
    minOccurs="0" maxOccurs="unbounded">
    <xsd:restriction base="token_type:submission"/>
    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
</xsd:element>
<!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα τεκμήρια απόδειξης παράδοσης §4.3.2 και την αντίστοιχη χρονοσφαγίδα [βλ §4.1.4]-->

```

```

<xsd:element
    name="evidence_token"
    type="evidence_token_Type"
    minOccurs="0" maxOccurs="unbounded">
    <xsd:restriction base="token_type:delivery"/>
    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
</xsd:element>

```

<!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα τεκμήρια απόδειξης παραλαβής §4.3.2 και την αντίστοιχη χρονοσφαγίδα [βλ §4.1.4]-->

```

<xsd:element name="evidence_token"
    type="evidence_token_Type" minOccurs="0"
maxOccurs="unbounded">

    <xsd:restriction base="token_type:receipt"/>

    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>

</xsd:element>

</xsd:sequence>

</xsd:complexType>
</xsd:schema>

```

Έξοδος : Τα αποδεικτικά τεκμήρια συλλέγονται, χρονοσημαίνονται και χαρακτηρίζεται η συναλλαγή από τον Οργανισμό. Στο τέλος, υπογράφονται από αυτόν και αποθηκεύονται στη Βάση Δεδομένων του. Αυτό με τη χρήση της XML Schema περιγράφεται ως εξής :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
    name="evidence_collection" type="evidence_collection_Type"/>
<!--Χαρακτηρίζεται η συναλλαγή σύμφωνα με τις Πολιτικές του
Οργανισμού -->

<xsd:attribute
    name="transaction_success" type="transaction_success_Type"/>

<xsd:complexType name="evidence_token_Type">
    <xsd:sequence>
        <xsd:element name="message_id" type="xsd:unsignedLong"
use="required"/>
        <!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα
τεκμήρια απόδειξης προέλευσης §4.3.2 και την αντίστοιχη
χρονοσφαγίδα [βλ §4.1.4]-->

        <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
            <xsd:restriction base="token_type:origin"/>
            <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>

```

```

</xsd:element>

      <!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα
τεκμήρια απόδειξης υποβολής §4.3.2 και την αντίστοιχη χρονοσφαγίδα
[βλ §4.1.4]-->

    <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
      <xsd:restriction base="token_type:submission"/>
      <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
    </xsd:element>

      <!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα
τεκμήρια απόδειξης παράδοσης §4.3.2 και την αντίστοιχη χρονοσφαγίδα
[βλ §4.1.4]-->

    <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
      <xsd:restriction base="token_type:delivery"/>
      <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
    </xsd:element>

      <!-- Μπορεί να περιλαμβάνει από ένα ως και περισσότερα τεκμήρια
απόδειξης παραλαβής §4.3.2 και την αντίστοιχη χρονοσφαγίδα [βλ
§4.1.4]-->

<xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
      <xsd:restriction base="token_type:receipt"/>
      <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
    </xsd:element>
    <!-- Για την εμπιστευτικότητα της υπηρεσίας περιλαμβάνεται και η
ψηφιακή υπογραφή του Οργανισμού-->

<xsd:element name="org_signature" type="org_signature_Type"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="org_signature_Type">

```

```

<xsd:sequence>
  <xsd:element name="org_signature" use="required">
    <xsd:complexType>
      <xsd:element name="sign_algorithm" type="xsd:string"
use="required"/>
      <xsd:element name="signature" type="xsd:string" use="required"/>
    </xsd:complexType>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
<!-- Ο χαρακτηρισμός της συναλλαγής-->

<xsd:simpleType name="transaction_success_Type">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="successful"/>
    <xsd:enumeration value="partial"/>
    <xsd:enumeration value="unsuccessful"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

4.3.4 Ανάκτηση τεκμηρίων

Για την παροχή λύσεων από τη μεριά του Οργανισμού στην περίπτωση διενέξεων απαιτείται η ανάγκη για ανάκτηση των αποδεικτικών τεκμηρίων από τη Βάση Δεδομένων του Οργανισμού. Αποστέλλεται ο κωδικός της αναφοράς της συναλλαγής για τα οποία ζητούνται τα αποδεικτικά στοιχεία και ο λόγος διένεξης, ανακτούνται τα ζητούμενα τεκμήρια και επαληθεύεται η χρονοσφαγίδα τους, συγκρίνονται οι συνόψεις τους με αυτές που υπάρχουν στα τεκμήρια και επιστρέφονται εφόσον οι έλεγχοι είναι θετικοί.

Είσοδος : Περιλαμβάνει τον κωδικό της αναφοράς της συναλλαγής, το λόγο της διένεξης και τη σύνοψη του μηνύματος για το οποίο υπάρχουν οι διαφορές.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
  name="evidence_recovery_Input"
  type="evidence_recovery_Input_Type"/>

```

```

<!-- Χαρακτηρίζεται και ο λόγος της διένεξης [§4.3.1]-->

<xsd:attribute name="referee_kind" type="referee_kind_Type"/>
<xsd:complexType name="evidence_recovery_Input_Type">
  <xsd:sequence>
    <xsd:element name="message_id" type="xsd:unsignedLong"
      use="required"/>
    <xsd:element name="message_hash" type="xsd:string"
      use="required"/>
    <xsd:element name="hash_algorithm" type="xsd:string"
      use="required"/>
  </xsd:sequence>
</xsd:complexType>
<!--Ο λόγος της διένεξης μπορεί να πάρει μία από τις παρακάτω
τιμές-->

<xsd:simpleType name="referee_kind_Type">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="repudiation of creation"/>
    <xsd:enumeration value="repudiation of submission"/>
    <xsd:enumeration value="repudiation of receipt"/>
    <xsd:enumeration value="assertion of distorted message"/>
    <xsd:enumeration value="assertion of an afterworded message"/>
    <xsd:enumeration value="repudiation of received identity"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

Έξοδος : Επιστρέφονται τα επικυρωμένα αποδεικτικά τεκμήρια.

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="evidence_recovery"
    type="evidence_recovery_Type"/>
  <xsd:complexType name="evidence_recovery_Type">
    <xsd:sequence>
      <xsd:element name="message_id" type="xsd:unsignedLong"
        use="required"/>
      <xsd:element name="evidence_token"
        type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">

```

```

<xsd:restriction base="token_type:origin"/>      <!-- [βλ.
§4.3.2]-->

    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
        </xsd:element>

    <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
        <xsd:restriction base="token_type:submission"/>      <!-- [βλ.
§4.3.2]-->

            <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
                </xsd:element>

            <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
                <xsd:restriction base="token_type:delivery"/>      <!-- [βλ.
§4.3.2]-->

                    <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
                        </xsd:element>

                    <xsd:element name="evidence_token"
type="evidence_token_Type" minOccurs="0" maxOccurs="unbounded">
                        <xsd:restriction base="token_type:receipt"/>      <!-- [βλ.
§4.3.2]-->

                            <xsd:element name="timestamp" type="timestamp_Type"
use="required"/>
                                </xsd:element>

                            <xsd:element name="creator_signature"
type="creator_signature_Type">
                                <xsd:element name="org_signature" type="org_signature_Type"/>
                            </xsd:sequence>
                        </xsd:complexType>
<!-- Η υπογραφή του δημιουργού περιλαμβάνει τα ίδια τα δεδομένα και
τον χρησιμοποιούμενο αλγόριθμο-->

<xsd:complexType name="creator_signature_Type">
    <xsd:sequence>
        <xsd:element name="creator_signature" use="required">
            <xsd:complexType>
                <xsd:element name="sign_algorithm" type="xsd:string"
use="required"/>

```

```

<xsd:element name="signature" type="xsd:string" use="required"/>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<!-- Η υπογραφή του Οργανισμού περιλαμβάνει τα ίδια τα δεδομένα και
τον χρησιμοποιούμενο αλγόριθμο--&gt;

&lt;xsd:complexType name ="org_signature_Type"&gt;
&lt;xsd:sequence&gt;
&lt;xsd:element name="org_signatur" use="required"&gt;
&lt;xsd:complexType&gt;
&lt;xsd:element name="sign_algorithm" type="xsd:string"
use="required"/&gt;
&lt;xsd:element name="signature" type="xsd:string" use="required"/&gt;
&lt;/xsd:complexType&gt;
&lt;/xsd:element&gt;
&lt;/xsd:sequence&gt;
&lt;/xsd:complexType&gt;
&lt;/xsd:schema&gt;
</pre>

```

4.4 Διαχείριση Δικαιωμάτων

4.4.1 Εισαγωγή

Η υπηρεσία διαχείρισης των δικαιωμάτων από έναν Οργανισμό διαχειρίζεται τα δικαιώματα πρόσβασης των πελατών της που βρίσκονται στο πεδίο ασφάλειά της. Περιλαμβάνει τις διαδικασίες του καθορισμού, αναγνώρισης και διαχειρισμού των δικαιωμάτων μιας οντότητας (λογική ή φυσική) πάνω σε έναν πόρο ή αντικείμενο ή πληροφορία όπως περιγράφονται στο πρότυπο X.812 [X.812] και το CDSA (Common Data Security Architecture)[CDSA]. Σύμφωνα με αυτά ο καθορισμός τους από έναν Οργανισμό γίνεται με τις εξής μορφές :

- 1. Απευθείας εξουσιοδότηση (direct authorization).** Εξουσιοδοτείται απευθείας μια λογική ή φυσική οντότητα με συγκεκριμένα δικαιώματα.

2. **Ανάθεση ρόλων (role assignment).** Ο Οργανισμός αναθέτει έναν ή περισσότερους ρόλους σε μία οντότητα. Τα δικαιώματα αυτής καθορίζονται από την περιγραφή των ρόλων του συστήματος διαχείρισης.
3. **Εκχώρηση δικαιωμάτων εξουσιοδότησης (privilege delegation).** Ο Οργανισμός δίνει συγκεκριμένα δικαιώματα σε μία οντότητα ενώ παράλληλα αυτή μπορεί να λειτουργήσει και ως διαχειριστής δικαιωμάτων σε κάποια άλλη.

Σε ένα διαδραστικό μοντέλο καταχώρησης των δικαιωμάτων σημαντικό ρόλο παίζουν και οι παρακάτω οντότητες εννοιών [Cheng]:

- **Χρήστης.** Είναι ο κάτοχος των δικαιωμάτων αντικειμένων ενώ μπορεί με τη συμμετοχή σε έναν από τους ρόλους του συστήματος να είναι και κάτοχος δικαιωμάτων. Οι ρόλοι του συστήματος περιγράφονται μες τις πολιτικές ασφάλειας του Οργανισμού
- **Πολιτικές.** Καθορίζουν το επίπεδο των δικαιωμάτων που είναι απαραίτητα για να επιτραπεί η χρήση μιας μεθόδου ενός αντικειμένου ή πόρου και τους ρόλους του συστήματος με τα αντίστοιχά τους δικαιώματα.
- **Αντικείμενο.** Είναι ο πόρος για τον οποίο ελέγχεται η πρόσβαση. Περιγράφεται από την τετράδα <Μέθοδος, Κατάσταση, Κανόνας Εξακρίβωσης, Δικαίωμα>. Η τιμές της μεθόδου μπορεί να είναι Ανάγνωση, Εισαγωγή, Τροποποίηση, Εκτέλεση, Διαγραφή και Διαχείριση, ενώ αυτές της κατάστασης Εγκρίθηκε, Προς επιμέλεια, Ακυρώθηκε κ.τ.λ και των κανόνων εξακρίβωσης Ελεύθερη Πρόσβαση, Μόνο για μέλη και Επιπλέον Δικαίωμα.
- **Επαληθευτής - Διαχειριστής.** Είναι η οντότητα που αποφασίζει αν κάποια άλλη οντότητα διαθέτει εκείνα τα δικαιώματα για χρήση του αντικειμένου.

Τα πιο γνωστά πιστοποιητικά για τη Διαχείριση των Δικαιωμάτων και είναι ευρέως αποδεκτά και χρησιμοποιήσιμα σε κρίσιμες εφαρμογές είναι [Bacon][Blobel]:

- **Ψηφιακό πιστοποιητικό με επεκτάσεις (Identity Certificate with extensions).** Περιγράφεται στο πρότυπο X.509 [X.509] και αντιστοιχίζει μια φυσική ή λογική οντότητα με το δημόσιο κλειδί της και τα δικαιώματα του κατόχου της. Συγκεκριμένο παράδειγμα θα δούμε στην επόμενη παράγραφο.
- **Πιστοποιητικό ιδιοτήτων (Attribute certificate).** Παρέχουν τα δικαιώματα και άλλες ιδιότητες που αντιστοιχούν στον ιδιοκτήτη του πιστοποιητικού

ταυτότητας που αναφέρονται [Linn, Nystrom]. Συγκεκριμένο παράδειγμα θα δούμε στην επόμενη παράγραφο.

Για τη διασφάλιση της συγκεκριμένης υπηρεσίας γίνεται απόλυτη χρήση των πιστοποιητικών που προκύπτουν από ζητήματα διαχείρισης πάνω σε μια Σχεσιακή Βάση Δεδομένων. Η παρούσα Διπλωματική Εργασία προτείνει το σχεδιασμό μιας αφαιρετικής Βάσης Δεδομένων που διασφαλίζει τόσο τη συγκεκριμένη υπηρεσία όσο και τις βασικές ιδιότητες της Ασφάλειας των Πληροφοριών [βλ. § 5.2.3.2].

4.4.2 Καθορισμός δικαιωμάτων

Η αίτηση για συμμετοχή μιας οντότητας στη λίστα των δικαιωμάτων για ένα αντικείμενο προέρχεται από κάποια οντότητα του Οργανισμού όπως ο διαχειριστής συστήματος ή κάποιον άλλον ρόλο που έχει τέτοια εξουσιοδότηση και απευθύνεται προς τον ίδιο τον Οργανισμό

Είσοδος : Χαρακτηριστικά της εισόδου είναι τα στοιχεία αυθεντικοποίησης του εξουσιοδότη και του χρήστη (συνήθως τα ψηφιακά τους πιστοποιητικά), το χρονικό διάστημα ισχύος των δικαιωμάτων, η ημερομηνίας της αίτησης και η περιγραφή του αντικειμένου και των δικαιωμάτων του χρήστη πάνω σε αυτό [Cheng].

Με τη βοήθεια της XML Schema αυτό περιγράφεται ως εξής :

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
    name="privilege_request_input"
    type="privilege_request_input_Type">

<xsd:complexType name="privilege_request_input_Type">
    <xsd:sequence>
        <!-- Όταν το αίτημα εμπεριέχει και την ερώτηση για τα δικαιώματα ενός άλλου χρήστη πρέπει να περιέχεται και το ψηφιακό πιστοποιητικό του αιτούμενου-->
        <xsd:element      name="requester_cert"      type="xsd:base64Binary"
use="optional"/>
        <xsd:element name="time" type="xsd:datetime" use="required"/>
        <xsd:element      name="user_cert"      type="xsd:base64Binary"
use="required"/>
        <xsd:element name="privilege" type="privilege_Type"/>
        <xsd:element      name="digest_info"      type="xsd:base64Binary"
use="required"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:element>
```

```

    </xsd:sequence>
</xsd:complexType>

<!-- Ο τύπος των δικαιωμάτων είναι η τετράδα &lt; Μέθοδος,
Κατάσταση, Κανόνας Εξακρίβωσης, Δικαίωμα &gt; πάνω σε ένα αντικείμενο-
--&gt;

&lt;xsd:complexType name="privilege_Type"&gt;
    &lt;xsd:sequence&gt;
        &lt;xsd:element name="privilege" use="required"&gt;
            &lt;xsd:complexType&gt;
                &lt;xsd:element name="resource_id" type="xsd:string"
use="required"/&gt;
                &lt;xsd:element name="method" type="method_Type" /&gt;
                &lt;xsd:element name="status" type="status_Type" /&gt;
                &lt;xsd:element name="access_status" type="access_status_Type" /&gt;
                &lt;xsd:element name="privilege_Type" type="type_of_privilege"/&gt;
<!-- Χρησιμοποιείται και η ψηφιακή υπογραφή για τη διασφάλιση της
εμπιστευτικότητας--&gt;

                &lt;xsd:element name="digest_info"
type="xsd:base64Binary" use="required"/&gt;
            &lt;/xsd:complexType&gt;
        &lt;/xsd:element&gt;
    &lt;/xsd:sequence&gt;
&lt;/xsd:complexType&gt;
<!-- Η επιλογή της λίστας των μεθόδων καθορίζεται από τις πολιτικές
του Οργανισμού --&gt;

&lt;xsd:complexType name="method_Type"&gt;
    &lt;xsd:sequence&gt;
        &lt;xsd:element name="method" use="required"&gt;
            &lt;xsd:choice&gt;
                &lt;xsd:element name="read" type="xsd:string"/&gt;
                &lt;xsd:element name="write" type="xsd:string"/&gt;
                &lt;xsd:element name="delete" type="xsd:string"/&gt;
                &lt;xsd:element name="update" type="xsd:string"/&gt;
                &lt;xsd:element name="execute" type="xsd:string"/&gt;
                &lt;xsd:element name="administer" type="xsd:string"/&gt;
</pre>

```

```

      .....
    </xsd:choice>
  </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<!-- Η επιλογή της λίστας των καταστάσεων καθορίζεται από τις
πολιτικές του Οργανισμού -->

<xsd:complexType name="status_Type">
  <xsd:sequence>
    <xsd:element name="status" use="required">
      <xsd:choice>
        <xsd:element name="draft" type="xsd:string"/>
        <xsd:element name="revised" type="xsd:string"/>
        <xsd:element name="cancelled" type="xsd:string"/>
      .....
    </xsd:choice>
  </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<!-- Η επιλογή της λίστας των κανόνων εξακρίβωσης καθορίζεται από
τις πολιτικές του Οργανισμού -->

<xsd:complexType name="access_status_Type">
  <xsd:sequence>
    <xsd:element name="access_status" use="required">
      <xsd:choice>
        <xsd:element name="free" type="xsd:string"/>
        <xsd:element name="members" type="xsd:string"/>
        <xsd:element name="copyright " type="xsd:string"/>
      .....
    </xsd:choice>
  </xsd:element>
  </xsd:sequence>
</xsd:complexType>
<!-- Η επιλογή της λίστας των διακιωμάτων καθορίζεται από τις
πολιτικές του Οργανισμού -->

<xsd:complexType name="type_of_privilege">

```



```

<xsd:sequence>
  <xsd:element name="privilege_type" use="required">
    <xsd:choice>
      <xsd:element name="delegate" type="xsd:string"/>
      <xsd:element name="deny" type="xsd:string"/>
      <xsd:element name="permit" type="xsd:string"/>

      .....
    </xsd:choice>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Ένα πιστοποιητικό ιδιοτήτων ή ένα πιστοποιητικό ταυτότητας με επέκταση

Παρακάτω απεικονίζεται ένα πιστοποιητικό ιδιοτήτων [Linn, Nystrom] και

ένα ψηφιακό πιστοποιητικό με επεκτάσεις όπως προβλέπεται στο πρότυπο X.509

Πιστοποιητικό ιδιοτήτων

```

<AttributeCert>
  <SubjectAndCA>
    <UserDN>cn=Nikos           Rentas;           ou=aueb;o=AUEB;c=gr</UserDN>
    <CADN>cn=Poseidon.Aegean.gr;ou=mailservers;o=Aegean;c=gr
  </CADN>
  </SubjectAndCA>
  <AttrName>printer</AttrName>
  <AttrValue>administer</AttrValue>
  <Condition>
    <Constraint>(IP=131.243.2.11)</Constraint>
    <AttributeInfo type="SYSTEM">
      <AttrName>printer</AttrName>
      <AttrValue>administer;deny</AttrValue>
    </AttributeInfo>
  </Condition>
</AttributeCert>

```

Ψηφιακό πιστοποιητικό με επεκτάσεις

Certificate:

Data:

Version: v3 (0x2)

Serial Number: 12 (0xc)

Signature Algorithm: PKCS #1 MD5 With RSA Encryption

Issuer: CN=Poseidon.Aegean.gr, OU=ICSD, O=Aegean, C=GR

Validity:

Not Before: Wed Fri 7 01:42:20 2003

Not After: Mon Nov 10 00:42:20 2003

Subject: E=rentas@aeueb.gr, CN=Nikos Rentas, UID=mrt,
OU=AUEB, O=AUEB, C=GR

Subject Public Key Info:

Algorithm: PKCS #1 RSA Encryption

Public Key:

Modulus:

00:ac:8f:83:fc:28:82:46:d7:94:f4:69:fc:53:52:86:75:76:

13:d0:1b:88:b4:0d:94:7c:45:79:ec:7c:86:dd:35:63:1d:ae:

67:84:f8:40:2c:88:65:da:6f:9f:1b:0a:b7:88:03:da:c0:16:

3a:f2:1d:43:7c:63:60:09:a1:7d:ef

Public Exponent: 65537 (0x10001)

Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Secure E-mail

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

09:07:1d:ab:52:ef:c1:5a:6b:33:b9:0b:94:f2:e5:ed:f9:96:

e0:fb

Signature:

Algorithm: PKCS #1 MD5 With RSA Encryption

Signature:

96:f6:1f:69:a3:a5:56:01:87:60:a7:43:a8:23:b0:87:60:8e:67:1e:cf:
 71:a9:96:3d:81:7c:de:10:75:a9:7e:43:1e:64:67:1d:48:62:76:49:aa:
 2a:61:24:4d:01:15:4a:79:54:4b:65:a7:3b:09:18:f6:94:9f:83:21:bd:
 f9:10:22:51:af:03:c6:ea:c3:8f:b8:f4:b8:81:8b:70:fc:9a:35:df:22:
 e7:36:6e:2d:8c:42:27:b4:ec:d2:68:9d:5e:f5:7d:a1:0b:c7:80:5d:00:
 31:ed:43:8f:e3:0d:00:8f:a1:5f:e8:9f:29:ab:a1:ae:4e:dd:59:66:83:
 61:38

Λειτουργία : Η διαδικασία που ακολουθείται είναι η ακόλουθη:

- Αυθεντικοποίηση του αιτούντος επαληθεύοντας την ψηφιακή του υπογραφή,
- Έλεγχος για το αν η αιτούσα οντότητα είναι ικανή να αιτηθεί τον καθορισμό δικαιωμάτων για τους συγκεκριμένους πόρους, σύμφωνα με τους ρόλους, τις εικωρήσεις δικαιωμάτων και τις πολιτικές,
- Δημιουργείται το πιστοποιητικό ιδιοτήτων ή το πιστοποιητικό με επεκτάσεις (όπως περιγράφηκαν παραπάνω)
- Το πιστοποιητικό υπογράφεται ψηφιακά από τον Οργανισμό και αποστέλλεται στην οντότητα για την οποία καθορίζονται τα δικαιώματα.

Εναλλακτικά πολλές φορές η αίτηση μπορεί να περιλαμβάνει και την αίτηση για τη συμμετοχή της οντότητας σε ένα ή περισσότερους ρόλους. Οι επιπλέον πληροφορίες που απαιτούνται είναι τουλάχιστο μία μονοσήμαντη αναφορά σε ένα ρόλο, μία αναφορά στην πολιτική που ορίζει το ρόλο, το πιστοποιητικό που περιγράφει τα δικαιώματα του ρόλου και τουλάχιστο μία τοποθεσία ανάκτησης της πολιτικής. Συνεπώς η είσοδος περιγράφεται ως εξής (το πεδίο privilege_request είναι αυτό που ορίστηκε παραπάνω):

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="privilege_request_input"
type="privilege_request_input_Type"/>

<xsd:complexType name="privilege_request_input_Type">
  <xsd:sequence>
```

```

<xsd:element name="privilege_request"
ref="privilege_request_input" use="required"/>
<xsd:element name="role" type="role_Type"/>
</xsd:sequence>
</xsd:complexType>
<!-- Απόδοση δικαιωμάτων σε έναν ή περισσότερους ρόλους-->
<xsd:complexType name="role_Type">
<xsd:sequence>
<xsd:element name="role" minOccurs="1" maxOccurs="unbounded">
<xsd:complexType>
<xsd:element name="role_id" type="xsd:string" use="required"/>
<xsd:element name="role_attribute_cert"
type="xsd:base64Binary" use="required"/>
<xsd:element name="policy_id" type="xsd:string" use="required"/>
<xsd:element name="policy_url" type="xsd:anyURI"
use="required"/>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.4.3 Ανάκτηση δικαιωμάτων

Σύμφωνα με το μοντέλο διαχείρισης δικαιωμάτων, ο επαληθευτής δέχεται μια αίτηση πρόσβασης σε ένα αντικείμενο και αποστέλλει στον αιτούντα ένα μήνυμα επιτρεπτής ή όχι πρόσβασης όπως απορρέει από τους ρόλους και τα επιπλέον δικαιώματα του χρήστη.

Είσοδος : Αποτελείται από τον κωδικό του αντικειμένου προς πρόσβαση, τη μέθοδο πρόσβασής του και την ψηφιακή υπογραφή του αιτούντα χρήστη για τη διασφάλιση της εμπιστευτικότητας .

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="privilege_verification_input"
type="privilege_verification_input_Type"/>

<xsd:complexType name="privilege_verification_input_Type">
<xsd:sequence>

```

```

<xsd:element      name="resource_id"      type="xsd:string"
use="required"/>

<xsd:element name="time" type="xsd:datetime" use="required"/>

<xsd:element name="method" ref="method_Type"/>

<xsd:element      name="digest_info"      type="xsd:base64Binary"
use="required"/>

</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Μια δυαδική τιμή που υποδεικνύει εάν επιτρέπεται ή όχι η εκτέλεση της ζητούμενης μεθόδου για το συγκεκριμένο αντικείμενο, από την αιτούσα οντότητα

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="privilege_verification_output"
              type="privilege_verification_output_Type"/>

<xsd:complexType name="privilege_verification_output_Type">
  <xsd:sequence>
    <xsd:element      name="resource_id"      type="xsd:string"
use="required"/>
    <xsd:element name="privilege_verification" type="xsd:boolean"
use="required"/>
    <xsd:element name="time" type="xsd:datetime" use="required"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Λειτουργία : Ακολουθούνται τα παρακάτω βήματα :

- Επαλήθευση της ψηφιακής υπογραφής της αίτησης και αυθεντικοποίηση της αιτούσας οντότητας.
- Ανάκτηση όλων των πιστοποιητικών που σχετίζονται με απόδοση δικαιωμάτων και έχουν εκδοθεί είτε από τον ίδιο τον Οργανισμό είτε από άλλους.
- Ανάκτηση της πολιτικής του Οργανισμού που σχετίζεται με τη διαχείριση δικαιωμάτων, έτσι ώστε η διαδικασία να συμμορφωθεί με τυχόν καθολικές απαιτήσεις και περιορισμούς,

- Ένωση των δικαιωμάτων που έχουν ανακτηθεί με όλους τους τρόπους και αφορούν στη ζητούμενη μέθοδο του αντικειμένου που αιτείται προσπέλασης και επιστροφή του αποτελέσματος.

4.5 Υπηρεσία Περιαγωγής (Roaming PKI Service)

4.5.1 Εισαγωγή

Είναι κοινά αποδεκτό πως η αποτελεσματικότητα και η ασφάλεια των PKI συστημάτων εξαρτάται σημαντικά από τον τρόπο που οι χρήστες διαχειρίζονται τα ιδιωτικά τους κλειδιά. Οι σύγχρονες ανάγκες για την παροχή υπηρεσιών Υποδομής Δημόσιου Κλειδιού και σε μετακινούμενους χρήστες (mobile users), οδήγησε στην ανάγκη για παροχή υπηρεσιών περιαγωγής.

Οι αρχικές λύσεις της αποθήκευσης των ψηφιακών πιστοποιητικών των μετακινούμενων χρηστών σε μαγνητικά μέσα, δεν υπήρξαν ουσιαστικές και αυτό γιατί :

- Υπάρχει εξάρτηση στην χρησιμοποιούμενη πλατφόρμα. Τυπικά, πιστοποιητικά που εξάγονται από μια πλατφόρμα, μπορούν μόνο να χρησιμοποιηθούν σε πλατφόρμες του ίδιου κατασκευαστή.
- Ανακύπτουν θέματα ασφάλειας. Συνήθως με την παραγωγή του ψηφιακού πιστοποιητικού, το ιδιωτικό κλειδί του χρήστη παραμένει ακόμα στο χρησιμοποιούμενο μηχάνημα και οπότε μπορεί εύκολα να υποκλαπεί.
- Η χρήση μιας τέτοιας λύσης απαιτεί κάποια σημαντικά βήματα και επομένως ο χρήστης ενός τέτοιου συστήματος απαιτείται να είναι να είναι γνώστης αυτών και της χρησιμοποιούμενης τεχνολογίας.

4.5.2 Παροχή υπηρεσίας Περιαγωγής – Λειτουργικά χαρακτηριστικά

Άρτια επιλογή από έναν πάροχο της υπηρεσίας περιαγωγής είναι η λύση των Έξυπνων Καρτών (smart cards) και των φορητών συσκευών αποθήκευσης ιδιωτικού κλειδιού. Οι Έξυπνες Κάρτες θεωρούνται το καλύτερο μέσο για αποθήκευση, κατοχή και διαχείριση των ιδιωτικών κλειδιών και ψηφιακών πιστοποιητικών. Η πρόσβαση σε αυτές ελέγχονται με τη χρήση PIN ή ακόμα και βιομετρικών μεθόδων που είναι ακόμα ασφαλέστερες, δίνοντας έτσι τη δυνατότητα σε αυτών που τις χρησιμοποιεί να έχει πρόσβαση στα αποθηκευμένα δεδομένα και να τα χρησιμοποιεί σε Υποδομή

Δημοσίου Κλειδιού. [Hoover-Kausik] Οι ισχυροί κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται για την αποθήκευση και την πρόσβαση διασφαλίζουν την ακεραιότητα και την διαθεσιμότητα των αποθηκευμένων δεδομένων. Μειονεκτήματα της παρεχόμενης λύσης αποτελούν η ανάγκη για αναγνώστες Έξυπνων Καρτών στο σημείο πρόσβασης και η περιορισμένη χωρητικότητα.

Προς αυτή την κατεύθυνση, της παροχής της υπηρεσίας της περιαγωγής, συνιστάται και η λύση των συσκευών που συνεργάζονται με την USB (Universal Serial Bus) θύρα. Έχουν τις ίδιες κρυπτογραφικές δυνατότητες με τις Έξυπνες Κάρτες (χρήση RSA κλειδιών μήκους 1024 bits) και σαφώς μεγαλύτερες δυνατότητες για αποθηκευτικό χώρο. Αν μάλιστα συνυπολογιστεί και το γεγονός της ευρείας χρήσης τους σαν περιφερειακά των ηλεκτρονικών υπολογιστών (το κύριο μέσο πρόσβασης σε Υποδομές Δημόσιου Κλειδιού), μετατρέπει την προσφερόμενη λύση σε ευρέως αποδεκτή [Wilson]. Ανασταλτικό παράγοντα για την ευρεία χρήση τους αποτελεί η μη συνολική τους αποδοχή και η εξάρτηση της λειτουργίας (πολλές φορές ανεπιτυχής) από συγκεκριμένες πλατφόρμες λογισμικού.

Όπως προκύπτει από τα παραπάνω, οι hardware προτάσεις ίσως να μην αποτελούν τη λύση στην παροχή της περιαγωγής. Ένας σημαντικός αριθμός από PKI σχήματα περιαγωγής αναπτύχθηκαν με παρόμοιο τρόπο με αυτόν των SPX LEAF συστημάτων, όπως για παράδειγμα η μεθοδολογία ανάκτησης του ιδιωτικού κλειδιού με τον αλγόριθμο των Perlman – Kaufman [Perlman – Kaufman]. Ο χρήστης αυθεντικοποιείται σε έναν Έμπιστο Εξυπηρέτη του Οργανισμού και ανακτά είτε το ιδιωτικό του κλειδί για υπογράψει τα μηνύματά του ή τα ψηφιακά του πιστοποιητικά για την παροχή των βασικών υπηρεσιών Υποδομής Δημόσιου Κλειδιού. Σε μια τέτοια περίπτωση όμως τυχόν επιτυχείς «επιθέσεις» προς τον Έμπιστο Εξυπηρέτη του Οργανισμού από έναν τρίτο και άμεσα εμπλεκόμενο, μπορούν να καταστήσουν τη διαδικασία ανενεργή και μη διαθέσιμη. Διαφαίνεται λοιπόν η ανάγκη για την για την υποστήριξη της εμπιστοσύνης προς τις υποδομές του Οργανισμού και ενός ασφαλούς καναλιού επικοινωνίας.

Για τους παραπάνω λόγους η προσέγγιση της χρήσης πολλαπλών εξυπηρετών είναι άκρως ενδιαφέρουσα [Taekyoung Kwon]. Για παράδειγμα οι Ford και Kalinski [Ford-Kalinski] βελτίωσαν την ασφάλεια ανάκτησης ψηφιακών πιστοποιητικών και ιδιωτικού κλειδιού με έναν τρόπο που πολλαπλοί εξυπηρέτες συνεργάζονται στην παραγωγή ενός ισχυρού μυστικού (strong secret) από έναν κωδικό πρόσβασης.

Παρόμοια πρόταση είναι και του Jablon [Jablon] με τη χρήση μιας διακριτής λογαριθμικής μεθόδου – Αλγόριθμος SPEKE (Simple Password Exponential Key Exchange). Αποτελεί έναν αλγόριθμο τύπου Απόδειξης Μηδενικής Γνώσης (Zero-Knowledge Proof), όπου τα δύο συναλλασσόμενα μέρη αποδεικνύουν πως γνωρίζουν το ίδιο μυστικό αλλά δεν αυτό δεν αποκαλύπτεται. Με αυτό τον τρόπο αυθεντικοποιούνται μεταξύ τους, παράγεται ένα session key μήκους από 1024 έως και 2048 bits και στη συνέχεια με τη χρήση του συγκεκριμένου κλειδιού μπορούν και ανταλλάσσουν τις όποιες πληροφορίες. Οι συγκεκριμένοι αλγόριθμοι είχαν αρχικά σχεδιαστεί για να ξεπεραστούν οι μειωμένες υπολογιστικές δυνατότητες των Έξυπνων Καρτών.

Σε μια τέτοια παρεχόμενη λύση κάθε χρήστης της υπηρεσίας της περιαγωγής πρέπει να θυμάται μόνο ένα ζεύγος <προσωπικός κωδικός, κωδικός πρόσβασης>. Η βασική ιδέα είναι να αποκρυφτεί η πραγματική ταυτότητα του χρήστη (παροχή Ανωνυμίας στις υπηρεσίες του Οργανισμού) και να διασπαστεί ο κωδικός πρόσβασης σε πολλαπλούς εξυπηρέτες για περισσότερη ασφάλεια.

Το βασικό διάγραμμα για την παροχή υπηρεσιών περιαγωγής απεικονίζεται στο Σχήμα. 4.1.

Οι βασικές λειτουργίες των οντοτήτων είναι:

<Χρήστης>

- Θυμάται το ζεύγος <προσωπικός κωδικός, κωδικός πρόσβασης>
- Ελέγχει τον εξυπηρετούμενο
- Εισάγει στον εξυπηρετούμενο τον προσωπικό κωδικό και τον κωδικό πρόσβασης

<Εξυπηρετούμενος>

- Πιστοποιεί τη χρήση των Δημόσιων Κλειδιών με την προσπέλαση X.509 καταλόγων
- Επικοινωνεί με κάθε εξυπηρέτη πάνω από ένα δημόσιο δίκτυο

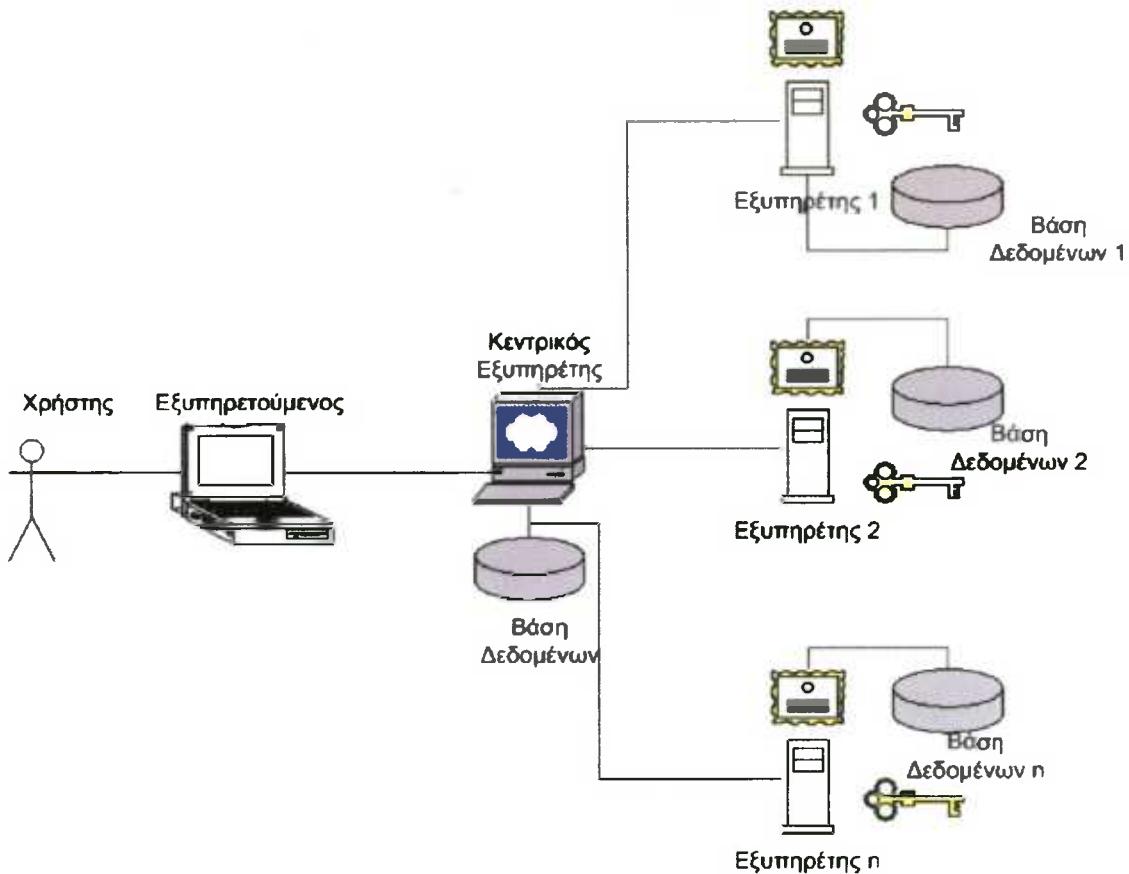
<Εξυπηρέτης>

- Κατέχει τα διαμοιφασμένα δεδομένα (ψηφιακά πιστοποιητικά, ιδιωτικό κλειδί κ.α.)
- Επικοινωνεί με κάθε εξυπηρετούμενο πάνω από ένα δημόσιο δίκτυο

<Κεντρικός Εξυπηρέτης>

- Ελέγχει το συνολικό δίκτυο

- Ενεργοποιεί και απενεργοποιεί τις συνδέσεις με τον εξυπηρετούμενο.



Σχήμα 4.1 Μοντέλο αναφοράς παροχής υπηρεσίας Περιαγωγής

4.5.2 Αίτηση παροχής υπηρεσιών περιαγωγής

Για την παροχή της περιαγωγής όπως γίνεται σαφές από τα προηγούμενα, απαιτείται η συναλλαγή του εξυπηρετούμενου με καθένα από τους εξυπηρέτες και το συνολικό αποτέλεσμα αυτής της διαδικασίας, το οποίο εκτελείται στην εφαρμογή του εξυπηρετούμενου, είναι οι προσφερόμενες υπηρεσίες (ανάκτηση ιδιωτικού κλειδιού, ψηφιακών πιστοποιητικών μέσα από X.509 καταλόγους και τις συναφείς υπηρεσίες προστιθέμενης αξίας, ψηφιακές υπογραφές, κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων).

Είσοδος

Ο εξυπηρετούμενος αιτείται περιαγωγής προς τον κεντρικό Έμπιστο Εξυπηρετητή και αυτός με τη σειρά του δρομολογεί την επικοινωνία με κάθε εξυπηρετητή ξεχωριστά. Για την αυθεντικοποίηση προς κάθε ξεχωριστό εξυπηρέτη

γίνεται χρήση του αλγορίθμου SPEKE (εναλλακτική λύση αποτελεί και ο EKE - Exponential Key Exchange). Η περιγραφή της εισόδου με XML Schema είναι :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="roaming_request" type="roaming_request_Type"/>
  <xsd:complexType name="roaming_request_Type">
    <xsd:sequence>
      <xsd:element name="client_id" type="xsd:unsignedLong"
use="required"/>
      <xsd:element name="client_enc_pwd" type="xsd:base64Binary"
use="required"/>
      <!-- Παραγωγή τυχαίου αριθμού για τη χρήση του αλγορίθμου
SPEKE-->
      <xsd:element name="client_random_number"
type="xsd:unsignedLong" use="required"/>
      <xsd:element name="client_ipaddress" type="xsd:string"
use="required"/>
      <xsd:element name="server_ipaddress" type="xsd:string"
use="required"/>
      <xsd:element name="roaming_algorithm" type="xsd:string"
fixed="SPEKE"/>
      <xsd:element name="client_certificate" type="xsd:base64Binary"
use="required"/>
      <xsd:element name="message_hash" type="xsd:base64Binary"
use="required"/>
      <xsd:element name="hash-algorithm" type="xsd:string"
use="required"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

Έξοδος

Ο κάθε εξυπηρέτης επιστρέφει την κρυπτογραφημένη δυαδική τιμή του μηνύματος του εξυπηρετούμενου που αντιστοιχεί σε αυτόν μαζί με κάποια τυχαία δεδομένα για τη διασφάλιση της αξιοπιστίας του καναλιού επικοινωνίας. Η ανάκτηση των ψηφιακών πιστοποιητικών γίνεται από τον κεντρικό Έμπιστο Εξυπηρέτη. Περιγραφικά η δομή της εξόδου με XML Schema είναι :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="roaming_request_output" type="roaming_request_output_Type"/>
  <xsd:complexType name="roaming_request_output_Type">
    <xsd:sequence>
      <xsd:element name="verification_enc_message"
      type="xsd:unsignedLong" use="required"/>
      <!--Παραγωγή τυχαίων δεδομένων για διασφάλιση της επικοινωνίας-->
    </xsd:sequence>
    <xsd:element name="random_data" type="xsd:base64Binary"
    use="required"/>
    <xsd:element name="client_ipaddress" type="xsd:string"
    use="required"/>
    <xsd:element name="server_ipaddress" type="xsd:string"
    use="required"/>
    <xsd:element name="server_certificate"
    type="xsd:base64Binary" use="optional"/>
    <xsd:element name="message_hash" type="xsd:base64Binary"
    use="required"/>
    <xsd:element name="hash-algorithm" type="xsd:string"
    use="required"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Λειτουργία

- Ο χρήστης εισάγει στον εξυπηρετούμενο τον προσωπικό κωδικό και τον κωδικό πρόσβασης.
- Ο εξυπηρετούμενος αιτείται περιαγωγής στον κεντρικό Έμπιστο Εξυπηρέτη.
- Ο Έμπιστος Εξυπηρέτης δρομολογεί την επικοινωνία με τους διαφορετικούς υποστηριζόμενους εξυπηρέτες.
- Ο εξυπηρετούμενος επικοινωνεί με κάθε εξυπηρέτη ξεχωριστά και αιτείται υπηρεσιών (ανάκτηση ιδιωτικού κλειδιού, ψηφιακών πιστοποιητικών μέσα από X.509 καταλόγους και τις συναφείς υπηρεσίες προστιθέμενης αξίας, ψηφιακές υπογραφές, κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων) [Taekyoung Kwon].

- Ο εξυπηρέτης λαμβάνει τα σωστά δεδομένα και τα συνθέτει για την υποστήριξη των διαδικασιών του.
- Με τη λήξη της διαδικασίας η επικοινωνία εξυπηρετούμενου – Εμπιστού Εξυπηρέτη περνάει σε μια ανενεργή φάση μικρού χρονικού διαστήματος (τυπικά στα 10 sec).
- Διαγράφονται από την προσωρινή μνήμη του εξυπηρετούμενου όλες εκείνες οι κρίσμες πληροφορίες της επικοινωνίας με κάθε εξυπηρέτη (ιδιωτικό κλειδί, ψηφιακά πιστοποιητικά).
- Τερματίζεται η διαδικασία.

4.6 Βιομετρικές Μέθοδοι Αυθεντικοποίησης

4.6.1 Εισαγωγή

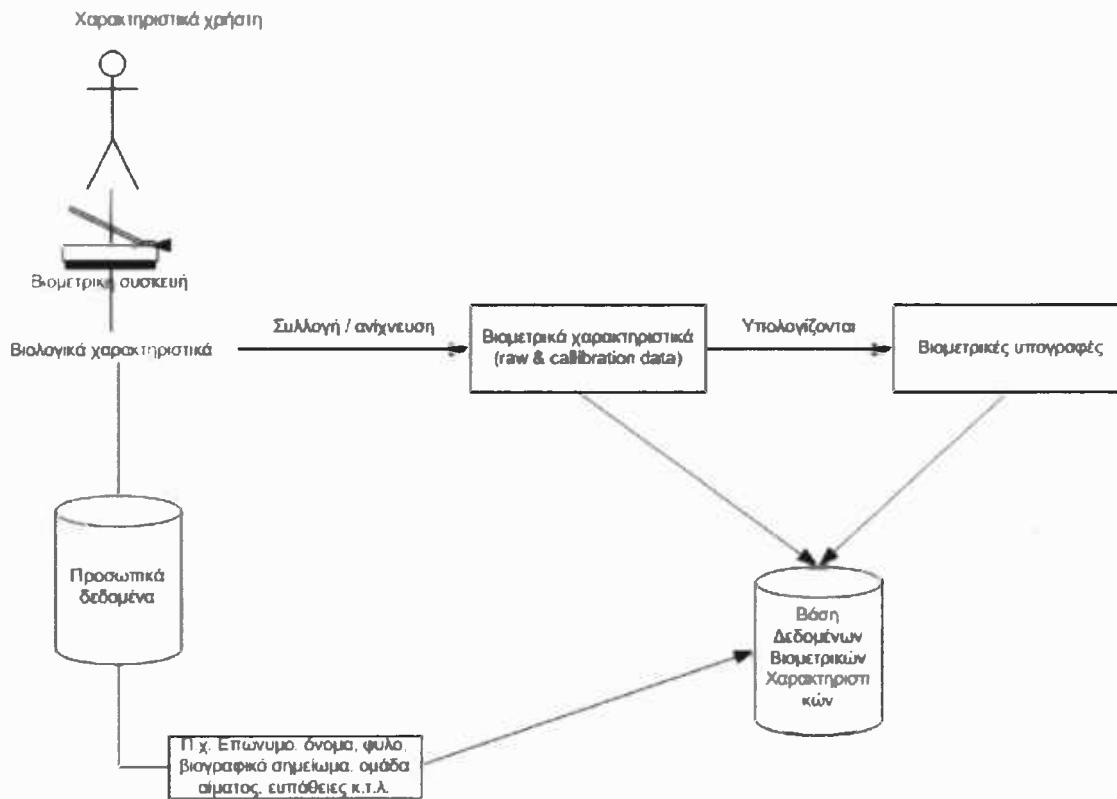
Βιομετρικό χαρακτηριστικό είναι ένα μοναδικό και μετρήσιμο χαρακτηριστικό που ένα άνθρωπος έχει για την αυτόματη αναγνώριση ή για την πιστοποίηση της ταυτότητάς του. Υπάρχουν δύο κατηγορίες στις οποίες κατατάσσονται οι βιομετρικές τεχνικές. Σε εκείνες που βασίζονται σε φυσιολογικά χαρακτηριστικά του χρήστη και σε εκείνες που βασίζονται σε χαρακτηριστικά της συμπεριφοράς του. Στην πρώτη περίπτωση ενδεικτικά παραδείγματα αποτελούν : η αυθεντικοποίηση με τη χρήση δαχτυλικών αποτυπωμάτων, με την ανάλυση της ίριδας του ματιού, των χαρακτηριστικών του προσώπου και της γεωμετρίας του χεριού, ενώ τεχνικές βασισμένες σε μετρήσεις της ανθρώπινης συμπεριφοράς είναι η χειρόγραφη υπογραφή σε ειδικά μηχανήματα, η ανάλυση του χτυπήματος των πλήκτρων και η ανάλυση της φωνής του χρήστη.

Σημαντικό ρόλο της διασφάλισης της υπηρεσίας αποτελούν οι δηλωμένες Πρακτικές Ασφάλειας του Οργανισμού για τη διαχείριση και επεξεργασία των βιομετρικών δειγμάτων μόνο στα πλαίσια λειτουργίας του. Συνεπώς η έννοια της εμπιστοσύνης παίρνει το χαρακτήρα της μεταβατικότητας [βλ. § 3.3.5.2]

4.6.2 Καταχώρηση βιομετρικών δειγμάτων και επαλήθευση

Η διαδικασία είναι η ακόλουθη : την πρώτη φορά που ο χρήστης πλησιάζει στη συσκευή αναγνώρισης καταχωρεί το βιομετρικό του δείγμα. Το δείγμα αυτό μέσα από μια μαθηματική διαδικασία μετατρέπεται σε ένα «προσωπικό δείγμα» (pattern)

και αποθηκεύεται είτε σε μια κεντρική Βάση Δεδομένων είτε σε ένα αντικείμενο που αυτός κατέχει, όπως μια Έξυπνη Κάρτα. Κάθε φορά που ο χρήστης από εδώ και πέρα προσπαθεί να εισέλθει στο Πληροφοριακό Σύστημα ή αιτείται άλλων υπηρεσιών, το προσωπικό του δείγμα ελέγχεται με το αποθηκευμένο pattern και ανάλογα πιστοποιείται ή όχι η ταυτότητά του. Κάτι τέτοιο απεικονίζεται σχηματικά:



Σχήμα 4.2 Διαδικασία Βιομετρικής Αυθεντικοποίησης

Σε κάθε βιομετρικό δείγμα του συστήματος αντιστοιχίζεται ένα σύνολο πληροφοριών διαθέσιμων για επεξεργασία. Όπως φαίνεται και στο σχήμα αλλά θα αναφερθεί και παρακάτω, είναι δυνατή η υπογραφή των συναλλαγών και των μηνυμάτων του χρήστη με κάποιο από τα βιομετρικά του χαρακτηριστικά αντί της χρήσης του ιδιωτικού του κλειδιού.

4.6.3 Βιομετρικές τεχνικές

Οι κυριότερες βιομετρικές με τα αντίστοιχα πλεονεκτήματα και μειονεκτήματά τους είναι [Armington,Polemi]:

- **Δακτυλικά Αποτυπώματα.** Πρόκειται για μία τεχνική που έχει κυρίως τις ρίζες της σε εφαρμογές αντιμετώπισης εγκληματικών δραστηριοτήτων

(αναζήτηση εγκληματιών κ.τ.λ.). Βασίζεται στην μοναδικότητα που εξασφαλίζουν τα δαχτυλικά αποτυπώματα για κάθε διακριτή οντότητα. Δυστυχώς επειδή η χρήση των δακτυλικών αποτυπωμάτων έχει συνδεθεί στο μυαλό του απλού χρήστη με αστυνομικά εγκλήματα δε μπορεί να θεωρηθεί και μια ιδιαίτερα αποδεκτή τεχνολογία για το ευρύτερο κοινό. Επίσης, δε μπορεί να χρησιμοποιηθεί από άτομα που δυστυχώς έχουν ελλιπή δάκτυλα ή η φύση της εργασίας τους, τους επιβάλλει να φορούν γάντια (π.χ. ιατρικά και χημικά εργαστήρια). Η ηλικία, το φύλο, η εργασία και το περιβάλλον επηρεάζουν την ικανότητα τέτοιων συστημάτων αναγνώρισης. Τέλος, παρά τη μεγάλη ανάπτυξη της τεχνολογίας οι συσκευές αναγνώρισης βάση δακτυλικών αποτυπωμάτων είναι ακόμα σε υψηλά χρηματικά κόστη.

- **Ανάλυση της ίριδας.** Εξασφαλίζει τη μοναδικότητα στην ταυτοποίηση μιας οντότητας λόγω των ιδιαιτεροτήτων που κλινικά έχει βρεθεί ότι διαθέτει. Μερικά από τα ιδιαίτερα χαρακτηριστικά της είναι : η προστασία της από το εξωτερικό περιβάλλον, η αδυναμία αναπαραγωγής της χωρίς τον κίνδυνο απώλειας της όρασης όταν συμβεί σε ζωντανό οργανισμό και η αδυναμία τεχνητής αναπαραγωγής της εξαιτίας της ανυπαρξίας αντίδρασης της στο φως όταν δεν βρίσκεται σε ζώντα οργανισμό. Ένα από τα βασικότερα πλεονεκτήματά που εμφανίζει είναι η δυνατότητα να ληφθεί η εικόνα της από απόσταση με τη χρήση βιντεοκάμερας και ειδικών αλγορίθμων που εξασφαλίζουν την ορθότητα και την ακεραιότητα του λαμβανόμενου δείγματος. Έτσι γίνεται πιο εύκολη η εφαρμογή της για τον χρήστη του συστήματος, αφού σχεδόν δεν απαιτείται η ενεργός συμμετοχή του. Παρ' όλη όμως την θετική προσέγγιση που παρέχει η τεχνολογία για την βιομετρική αυτή τεχνική, εξακολουθεί να αντιμετωπίζει έντονα προβλήματα αποδοχής από τους χρήστες, ενώ δεν πρέπει να παραγνωρίζει κανείς και το γεγονός ότι τυφλοί άνθρωποι, άνθρωποι με προβλήματα όρασης ή γενικότερες βαριές ασθένειες που επηρεάζουν τη όραση δεν μπορούν να την χρησιμοποιήσουν.
- **Ανάλυση Προσώπου.** Ο ισχυρισμός της μεθόδου έχει να κάνει με το γεγονός πως χαρακτηριστικά του προσώπου όπως το στόμα, το σχήμα των ματιών, το μέγεθος της μύτης, τα βλέφαρα κ.α. είναι ικανά σε συνδυασμό να μας δώσουν ένα μοναδικό pattern για κάθε άτομο. Το pattern αποθηκεύεται σε μια κεντρική Βάση Δεδομένων και όποτε το άτομο πλησιάζει στο σημείο

αναγνώρισης μια κάμερα συλλέγει τα χαρακτηριστικά του, κατασκευάζει ένα νέο pattern, το συγκρίνει με τα ήδη υπάρχοντα και πιστοποιεί ή όχι την ταυτότητα του ατόμου που δηλώνει πως είναι. Η τεχνική παραμένει και σήμερα ιδιαίτερα αποδεκτή στο ευρύ κοινό. Οι περιορισμοί που τίθενται έχουν να κάνουν με την ανάγκη για συνεχή ανανέωση των patterns των χρηστών όσο τα χαρακτηριστικά τους μεταβάλλονται με το χρόνο και πως η διαδικασία πιστοποίησης απαιτεί από το χρήστη να κοιτά προς την κάμερα από μια συγκεκριμένη γωνία και με τον απαιτούμενο βέβαια φωτισμό, περιορισμοί που κάνουν τη χρήση τέτοιων μεθόδων ικανή σε συγκεκριμένα περιβάλλοντα. Τέλος, τέτοια συστήματα βρίσκουν αρκετή δυσκολία και στην αναγνώριση προσώπων με ιδιαίτερα φυσικά χαρακτηριστικά όπως τα γένια ή ιδιαίτερα μαλλιά ή με ιδιαίτερες εκφράσεις στο πρόσωπό τους.

- **Γεωμετρία χεριού.** Η συγκεκριμένη βιομετρική μέθοδος βασίζεται στα ιδιαίτερα χαρακτηριστικά του χεριού όπως το εξωτερικό περίγραμμα, τις εσωτερικές γραμμές, το μήκος και το μέγεθος των δακτύλων και της παλάμης ακόμα και τις φλέβες που βρίσκονται στο πάνω μέρος του χεριού. Ο χρήστης τοποθετεί το χέρι του σε μια ειδική συσκευή, παράγεται ένα pattern και συγκρίνεται με το ήδη εγγεγραμμένο. Συνήθως, η τεχνική απαιτεί και τη χρήση ενός αριθμού ταυτοποίησης για καλύτερα αποτελέσματα. Τέτοια συστήματα είναι από τα γρηγορότερα στην αναγνώριση. Απαιτούν λίγα δεδομένα για αποθήκευση και έχουν από τα μικρότερα templates. Από την άλλη όμως, υπάρχουν περιορισμοί που έγκεινται στο γεγονός πως το pattern είναι διαφορετικό ανάλογα με την κλίση του χεριού και πως εξωτερικά χαρακτηριστικά όπως η σκόνη, τα μεγάλα δακτυλίδια και πιθανώς η έλλειψη κάποιων δακτύλων από κάποιο άτομο να επηρεάσει την αναγνώριση. Μια τέτοια τεχνική δεν μπορεί να δουλέψει για άτομα με κινητικά προβλήματα στα άνω άκρα ή για ανθρώπους με την ασθένεια του Πάρκινσον. Επίσης, οι αναγνώστες (readers) τέτοιων μηχανισμών είναι ακόμα και σήμερα σε υψηλά χρηματικά κόστη και όσοι έχουν κατασκευαστεί έχουν ελεγχθεί σε συγκεκριμένες συνθήκες.
- **Ανάλυση φωνής.** Η χροιά, οι φωνητικές χορδές και ο ήχος που βγαίνει από το στόμα του κάθε ατόμου είναι ιδιαίτερη και επομένως εύκολα αναγνωρίσιμη υπό κάποιες συνθήκες περιβάλλοντος. Η διαδικασία είναι απλή : ο χρήστης

τοποθετείται απέναντι από ένα μικρόφωνο, καταγράφεται η φωνή του, με τη χρήση μαθηματικών μοντέλων (ανάλυση κατά Fourier) δημιουργείται ένα pattern και είναι αυτό με το οποίο θα γίνεται η σύγκριση κάθε φορά που θα προσπαθεί να εισέλθει στο σύστημα. Η συγκεκριμένη τεχνική είναι από τις περισσότερο αποδεκτές γιατί θεωρείται απόλυτα φυσιολογικό η ταυτοποίηση ενός προσώπου, όπως κάνουμε και στην καθημερινότητά μας, να γίνεται με τη συσχέτιση εξωτερικών χαρακτηριστικών και φωνής. Ωστόσο, για την αναγνώριση μέσω υπολογιστικών συστημάτων απαιτούνται πολύπλοκοι αλγόριθμοι όπως τα Νευρωνικά Δίκτυα. Από την άλλη όμως η αναγνώριση μέσω φωνής απαιτεί ιδανικές συνθήκες γιατί κάθε επιπρόσθετος θόρυβος είναι ικανός μειώσει την ικανότητα της συσκευής για αναγνώριση. Όπως είναι λογικό μια τέτοια τεχνική δεν μπορεί να χρησιμοποιηθεί σε άτομα με προβλήματα ομιλίας. Δυσκολίες επίσης παρουσιάζονται όταν δίνεται στη φωνή μια ιδιαίτερη χροιά που πηγάζει από συναισθηματική φόρτιση μέχρι και προσωρινά προβλήματα υγείας (π.χ. κρυολόγημα). Τέλος, επειδή ακόμα και με την πάροδο του χρόνου η φωνή του κάθε ατόμου μπορεί να αλλάξει, απαιτείται η ενημέρωση των αποθηκευμένων patterns.

- **Προσωπική υπογραφή.** Η συγκεκριμένη βιομετρική μέθοδος βασίζεται στο γεγονός πως ο τρόπος υπογραφής του κάθε ατόμου διαφέρει τόσο και στο τελικό αποτέλεσμα όσο και στον τρόπο γραφής όπως η ταχύτητα, η διαφορετική πίεση που ασκείται πάνω στο χαρτί και το στυλό, ο συνολικός χρόνος υπογραφής, η απόσταση των γραμμάτων κ.α.. [Newham]. Κάθε φορά που άτομο αναγκάζεται να πιστοποιήσει την ταυτότητά του μετρώνται τα παραπάνω χαρακτηριστικά και ανάλογα με το βαθμό ικανοποίησης παράγεται το τελικό αποτέλεσμα πιστοποίησης. Οι βασικοί περιορισμοί σχετίζονται με το γεγονός πως οι άνθρωποι αρκετά συχνά αλλάζουν την υπογραφή τους, ακόμα και υπό διαφορετικές συνθήκες (συναισθηματική φόρτιση, μέθη κ.α.) και πως μια τέτοια τεχνική απαιτεί μεγάλο τεχνολογικό υπόβαθρο. Όπως είναι φυσιολογικό άτομα με προβλήματα στα άνω άκρα τους δεν είναι ικανά να χρησιμοποιήσουν μια τέτοια τεχνική.
- **Ανάλυση μέσω πατήματος πλήκτρων.** Η συγκεκριμένη τεχνική μοιάζει αρκετά με την παραπάνω. Μετρώνται ο χρόνος πατήματος των πλήκτρων, το διάστημα μεταξύ δύο διαδοχικών πατημάτων, η πίεση που ασκείται πάνω σε

αυτά, η συχνότητα των λαθών κ.α. Συνήθως βρίσκει εφαρμογή σε παράλληλη χρήση με κάποια από τις άλλες μεθόδους.

- **Ανάλυση DNA.** Το DNA για κάθε άνθρωπο είναι διαφορετικό και επομένως μπορεί να χρησιμοποιηθεί εύκολα για ταυτοποίηση. Έχει απόλυτη επιτυχία εδώ και δυο δεκαετίες που χρησιμοποιείται στα εγκληματολογικά εργαστήρια και ίσως το επόμενο βήμα είναι να χρησιμοποιηθεί και στις καθημερινές μας συναλλαγές. Δύο όμως είναι τα βασικά προβλήματα : η διαδικασία πιστοποίησης ακόμα και σήμερα είναι αρκετά ακριβή και χρονοβόρα και δεν υπάρχει η διαβεβαίωση πως η συλλογή των DNA των ατόμων σε μια κεντρική Βάση Δεδομένων δε θα χρησιμοποιηθεί για άλλους σκοπούς
- **Άλλες Βιομετρικές τεχνικές.** Σε αυτή την κατηγορία βρίσκονται τεχνικές όχι ιδιαίτερα διαδεδομένες γιατί δεν υπάρχουν αρκετές μελέτες και όποιες έχουν γίνει βρίσκονται ακόμα σε πρώιμο στάδιο. Τέτοιες είναι : η αναγνώριση μέσω των ιδιαίτερων χαρακτηριστικών του αυτιού κάθε ατόμου, η αναγνώριση μέσω των πόρων που εκκρίνουν τον ιδρώτα στα δάκτυλα και η διαφορετική οσμή που πιθανώς έχει το κάθε ανθρώπινο σώμα.

4.6.4 Βιομετρικές τεχνικές και Υποδομή Δημόσιου Κλειδιού

Η χρήση κάποιων από τις «ισχυρές» Βιομετρικές τεχνικές μπορεί να λύσει κάποια από τα προβλήματα αυθεντικοποίησης που συναντώνται στις Υποδομές Δημόσιου Κλειδιού. Η αναγκαία χρήση των κωδικών χρήστη και προσωπικών κωδικών δεν είναι σε πολλές εφαρμογές αρεστή. Οι πολύπλοκοι χρησιμοποιούμενοι αλγόριθμοι πολλές φορές μετατρέπουν την ανάγκη χρήσης των υποστηριζόμενων υπηρεσιών σε δυσαρέσκεια. Με τη χρήση των βιομετρικών τεχνικών αυθεντικοποίησης κάποιες από τις διαδικασίες παραλείπονται ή αλλάζουν μορφή. Για παράδειγμα για την χρήση των δυνατοτήτων της Περιαγωγής η αναγνώριση του απομακρυσμένου χρήστη μπορεί να γίνεται με κάποιο από τα βιομετρικά του χαρακτηριστικά που κατέχει σε μια Έξυπνη Κάρτα ή που καταθέτει για επιβεβαίωση στο σημείο επαφής. Από την άλλη ο χρήστης είναι δυνατόν να χρησιμοποιεί το βιομετρικό του δείγμα αντί για το ιδιωτικό του κλειδί και έτσι να υπογράφει τις συναλλαγές του με τη χρήση των ασύμμετρων αλγορίθμων. Σε ένα απόλυτα ασφαλές περιβάλλον είναι δυνατή η χρήση τόσο των βιομετρικών χαρακτηριστικών όσο και

του ζεύγους δημόσιου και ιδιωτικού κλειδιού του χρήστη εξασφαλίζοντας όλα τα βασικά χαρακτηριστικά της ασφάλειας των πληροφοριών.

Παρά την αναγνώριση της ανάγκης για χρήση των βιομετρικών τεχνικών και στις Υποδομές Δημόσιου Κλειδιού, πλήρης προτυποποίηση ακόμα δεν έχει υπάρξει. Το πρότυπο ANSI X9.84 – 2001 [www.x9.org] καθορίζει τις απαιτήσεις για τη διαχείριση και την ασφάλεια των βιομετρικών πληροφοριών στον οικονομικό τομέα (π.χ. αναγνώριση πελατών, επαλήθευση υπαλλήλων) ενώ παράλληλα αναγνωρίζει τεχνικές σαν τις ψηφιακές υπογραφές και την κωδικοποίηση για την ακεραιότητα και την ιδιωτικότητα των βιομετρικών δεδομένων. Το πρότυπο X9.84 αναπτύχθηκε με τη συνεργασία και με άλλους Οργανισμούς συμπεριλαμβανομένου του BioAPI Consortium, του NIST/ITL, του CBEFF και του IBIA (International Biometric Industry Association). Το ANSI πρότυπο μόλις πρόσφατα έγινε δεκτό και από την τεχνική επιτροπή 68 του ISO. Σημαντική δουλειά στην προτυποποίηση των βιομετρικών τεχνικών έχει προσφέρει και το πρόσφατα εκδιδόμενο BioAPI Specification [www.bioapi.org]. Αναφέρεται εκτενώς στον τρόπο συλλογής, αποθήκευσης και διαχείρισης των βιομετρικών δειγμάτων και θέτει τις ασφαλιστικές δικλείδες για την ανάπτυξη τέτοιων εφαρμογών. Αντίστοιχες εργασίες έχουν γίνει και από το National Institute for Standards and Technologies (NIST) [www.nist.gov/cbeff], την ομάδα εργασίας B10.8 του National Committee for Information Technology Standards [www.aamva.org] και από το ISO/OEC Joint Technical Committee One [www.jtc1.org].

Τα ζητήματα εμπιστοσύνης που ανακύπτουν από τη χρήση της συγκεκριμένης υπηρεσίας είναι μείζονος σημασίας και σχετίζονται άμεσα με τη διασφάλιση της ιδιωτικότητας [3.3.5.1]. Υπεύθυνη για τη λειτουργία της συγκεκριμένης υπηρεσίας προτείνεται να είναι η Αρχή Πιστοποίησης (Certification Authority) και οι διαδικασίες επεξεργασίας και ανάκτησης των βιομετρικών δειγμάτων πρέπει να καθορίζονται μέσα από τη δήλωση των Πρακτικών Ασφάλειας του Οργανισμού.

4.6.5 Καταχώρηση – Επιβεβαίωση Βιομετρικών χαρακτηριστικών

Για τη διασφάλιση της υπηρεσίας καταχώρηση των βιομετρικών χαρακτηριστικών στην Εμπιστη Τρίτη Οντότητα από την οντότητα αποστέλλεται σε ηλεκτρονική μορφή με κάποιο πρωτόκολλο μεταφοράς δυαδικών δεδομένων (π.χ. FTP ή SMTP). Σε κάθε περίπτωση θα πρέπει να χαρακτηρίζεται από την ασφαλή

μεταβίβασή τους, τη συγκεκριμένη μορφοποίηση που διευκολύνουν την επεξεργασία τους και την ελαχιστοποίηση του μεγέθους τους. Η αποστολή του βιομετρικού δείγματος μπορεί να γίνεται είτε από ένα αποθηκευτικό μέσο (π.χ. Έξυπνη Κάρτα) ή μέσω μιας online διαδικασίας. Η είσοδος δεν πρέπει να περιέχει τα ίδια τα βιομετρικά δείγματα αλλά μια μορφή τους που τα προσδιορίζει μονοσήμαντα και από την οποία δεν είναι δυνατό να εξαχθούν τα αρχικά δεδομένα. Αυτή η μορφή μπορεί να είναι το αποτέλεσμα της κρυπτογράφησης των δεδομένων από τον αιτούντα ή η σύνοψη που παράγεται από έναν αλγόριθμο δημοσίου κλειδιού όπως ο MD5 ή ο SHA-1 [X.812].

Είσοδος - Καταχώρηση : Η είσοδος αίτησης καταχώρησης περιλαμβάνει το ίδιο το βιομετρικό δείγμα και κάποια στοιχεία ταυτοποίησης του αιτούντος. Περιγράφοντάς την με τη χρήση του XML Schema έχουμε :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element
    name="biometric_registration_input"
    type="biometric_registration_input_Type"/>

  <xsd:complexType name="biometric_registration_input_Type">
    <xsd:sequence>
      <xsd:element
        name="bio_pattern_hash"
        type="xsd:base64Binary" use="required"/>
      <xsd:element name="name" type="xsd:string" use="required"/>
      <xsd:element name="surname" type="xsd:string" use="required"/>
      <xsd:element name="contact_info" type="xsd:string"
        use="required"/>
      <!-- Η χρήση της IPAddress είναι απαραίτητη για την
          αυθεντικοποίηση της συσκευής εισόδου του βιομετρικού δείγματος-->
      <xsd:element name="client_ipaddress" type="xsd:string"
        use="required"/>
      <!-- Η χρήση του δημόσιου κλειδιού θα επιτρέψει τη δημιουργία
          ενός νέου ψηφιακού πιστοποιητικού-->
      <xsd:element name="client_pk" type="xsd:base64Binary"
        use="optional"/>
      <xsd:element name="hash_algorithm" type="xsd:string"
        use="required"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

```

</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Είσοδος - Επιβεβαίωση : Η είσοδος αίτησης επιβεβαίωσης περιλαμβάνει το ίδιο το βιομετρικό δείγμα και την χρονικό διάστημα ισχύος του. Στην περύπτωση της χρήσης Έξυπνης Κάρτας ή άλλου ασφαλούς αποθηκευτικού μέσου, το βιομετρικό δείγμα καταχωρείται και σε αυτό. Περιγράφοντάς την με τη χρήση του XML Schema έχουμε:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element
    name="biometric_verification_input"
    type="biometric_verification_input_Type"/>

  <xsd:complexType name="biometric_verification_input_Type">
    <xsd:sequence>
      <!--Το βιομετρικό δείγμα κρυπτογραφείται σύμφωνα με τους
κανόνες ασφαλείας του Οργανισμού-->

      <xsd:element
        name="bio_pattern_encrypted"
        type="xsd:base64Binary" use="required"/>

      <xsd:element
        name="client_id" type="xsd:unsignedLong" use="required"/>

      <xsd:element
        name="bio_pattern_validity_from"
        type="xsd:datetime" use="required"/>

      <xsd:element
        name="bio_pattern_validity_to"
        type="xsd:datetime" use="required"/>
      <!--Χρησιμοποιούνται οι IPAddress των δύο οντοτήτων για τη
σύναψη ασφαλούς επικοινωνίας-->

      <xsd:element name="client_ipaddress"
        type="xsd:string" use="required"/>

      <xsd:element name="server_ipaddress"
        type="xsd:string" use="required"/>

```

```

<xsd:element name="client_pk"
              type="xsd:base64Binary" use="optional"/>

<xsd:element
              name="bio_pattern_encrypted_hash"
              type="xsd:base64Binary" use="required"/>

<xsd:element name="hash_algorithm"
              type="xsd:string" use="required"/>

</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Δυαδική τιμή που υποδεικνύει επιτυχή ή ανεπιτυχή λήψη και επιβεβαίωση της εγκυρότητας της αίτησης, το χρονικό διάστημα ισχύος του βιομετρικού δείγματος και πιθανώς ένα κρυπτογραφημένο session key για την περαιτέρω επικοινωνία. Περιγράφοντάς την με τη χρήση του XML Schema έχουμε:

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
          name="biometric_verification_output"
          type="biometric_verification_output_Type"/>

<xsd:complexType name="biometric_verification_output_Type">
  <xsd:sequence>
    <xsd:element name="validation"
                type="xsd:boolean" use="required"/>
    <xsd:element name="bio_pattern_validity_from"
                type="xsd:datetime" use="required"/>
    <xsd:element
                name="bio_pattern_validity_to"
                type="xsd:datetime" use="required"/>
    <xsd:element name="client_id"
                type="xsd:unsignedLong" use="required"/>
    <xsd:element name="client_ipaddress"
                type="xsd:string" use="required"/>
    <xsd:element name="server_ipaddress"
                type="xsd:string" use="required"/>
    <xsd:element name="client_pk"

```

```

        type="xsd:base64Binary" use="optional"/>
<xsd:element name="session_key"
        type="xsd:base64Binary" use="optional"/>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

4.6.6 Καταχώρηση νέου Βιομετρικού χαρακτηριστικού

Όπως αναφέρθηκε και στην ανάλυση των βιομετρικών τεχνικών αυθεντικοποίησης κάποια από τα αυτά με την πάροδο του χρόνου είναι δυνατό να τροποποιούνται (π.χ. φωνή, γεωμετρία χεριού κ.τ.λ.). Για αυτό το λόγο είναι απαραίτητη η ανανέωση αυτών των δειγμάτων από τη μεριά του χρήστη για την καλύτερη λειτουργία της διαδικασίας. Άλλες πάλι φορές είναι πιθανή η λήξη της ισχύος τους (όπως και στα ψηφιακά πιστοποιητικά) και για αυτό υπάρχει η ανάγκη για καταχώρηση νέων έγκυρων βιομετρικών δειγμάτων.

Είσοδος : Η είσοδος αίτησης καταχώρησης περιλαμβάνει το νέο και το παλιό βιομετρικό δείγμα και κάποια στοιχεία ταυτοποίησης του αιτούντος. Περιγράφοντάς την με τη χρήση του XML Schema έχουμε :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
name="biometric_update_input" type="biometric_update_input_Type"/>

<xsd:complexType name="biometric_update_input_Type">
    <xsd:sequence>
        <xsd:element
            name="bio_new_pattern_encrypted"
            type="xsd:base64Binary" use="required"/>
        <xsd:element
            name="bio_old_pattern_encrypted"
            type="xsd:base64Binary" use="required"/>
        <xsd:element
            name="bio_pattern_validity_from"
            type="xsd:datetime" use="required"/>
        <xsd:element
            name="bio_pattern_validity_to"
```

```

    type="xsd:datetime" use="required"/>
<xsd:element name="client_id"
    type="xsd:unsignedLong" use="required"/>
<xsd:element name="name" type="xsd:string" use="required"/>
<xsd:element name="surname" type="xsd:string" use="required"/>
<xsd:element name="contact_info"
    type="xsd:string" use="required"/>
<xsd:element name="client_ipaddress"
    type="xsd:string" use="required"/>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Μετά την επιβεβαίωση των ιδιοτήτων του αιτούντος επιστρέφεται μια δυαδική τιμή που υποδεικνύει επιτυχή ή ανεπιτυχή λήψη και επιβεβαίωση της εγκυρότητας της αίτησης, το χρονικό διάστημα ισχύος του βιομετρικού δείγματος και πιθανώς ένα κρυπτογραφημένο session key για την περαιτέρω επικοινωνία.

Περιγράφοντάς την με τη χρήση του XML Schema έχουμε :

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element
    name="biometric_verification_output"
    type="biometric_update_output_Type"/>

<xsd:complexType name="biometric_update_output_Type">
<xsd:sequence>
    <xsd:element name="validation"
        type="xsd:boolean" use="required"/>
    <xsd:element name="bio_pattern_validity_from"
        type="xsd:datetime" use="required"/>
    <xsd:element name="bio_pattern_validity_to"
        type="xsd:datetime" use="required"/>
    <xsd:element name="client_id"
        type="xsd:unsignedLong" use="required"/>
    <xsd:element name="client_ipaddress"
        type="xsd:string" use="required"/>
    <xsd:element name="server_ipaddress"

```

```

    type="xsd:string" use="required"/>
<xsd:element name="client_pk"
    type="xsd:base64Binary" use="optional"/>
<xsd:element name="session_key"
    type="xsd:base64Binary" use="optional"/>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

4.7 Διατήρηση Ανωνυμίας

4.7.1 Εισαγωγή

Η διατήρηση της ανωνυμίας του χρήστη κατά τις περισσότερες ηλεκτρονικές του συναλλαγές αποτελεί για το σημερινό πληροφοριακό περιβάλλον επιτακτική ανάγκη. Με τον όρο ανωνυμία αναφερόμαστε στην απουσία αναγνώρισης του εμπλεκόμενου σε μια συναλλαγή ούτε από τα δεδομένα της ίδιας της συναλλαγής ούτε και από συνδυασμό δεδομένων από άλλες συναλλαγές. Η διατήρηση της ανωνυμίας επιτυγχάνεται με τη χρήση ψευδώνυμων, ενός χαρακτηριστικού αναγνωριστικού που αντιστοιχίζεται στο χρήστη του ψηφιακού πιστοποιητικού ή που παίρνει μέρος σε μια συναλλαγή. Η αντιστοίχηση αυτή πρέπει να είναι μονοσήμαντη και όχι πολλαπλά χρησιμοποιήσιμη. Δηλαδή το παραγόμενο ψευδώνυμο (την ευθύνη της παραγωγής και της αντιστοίχησης την έχει ο Οργανισμός) δεν θα πρέπει να συνεπάγεται έστω και κάποια από τα στοιχεία του χρήστη αλλά και επίσης το ψευδώνυμο αυτό δε θα πρέπει να χρησιμοποιείται περισσότερες από μία φορές έτσι ώστε να εμποδίζεται οποιαδήποτε προσπάθεια ταυτοποίησης.[Chaum]

Μια πρώτη λύση στη χρήση ψευδωνύμων και την υποστήριξη της ανωνυμίας έδωσε το Transport Layer Security (TLS) πρωτόκολλο κάνοντας μια προσπάθεια ταξινόμησης των ψευδωνύμων ξεκινώντας από τα προσωπικά (όπως τα nicknames π.χ. nick2478) που χρησιμοποιούνται για πάντα από το χρήστη έως τα ψευδώνυμα βασισμένο στο ρόλο του χρήστη (π.χ. Secretary of Defense) και τα ψευδώνυμα μονής χρήσης (π.χ. n7ic456). Σε άλλες λύσεις, στο πρότυπο SDSI (Simple Distributed Security Infrastructure) [SDSI] η ανωνυμία παρέχεται σε βάρος της αυθεντικοποίησης ενώ στο PEM (Privacy Enhanced for Internet electronic Mail)

[PEM] καθορίζονται ειδικές οντότητες ανωνυμίας για τις οποίες όμως δεν καθορίζονται μηχανισμοί απόδειξης της ταυτότητας του χρήστη.

Η χρήση της ανωνυμίας σε κάποιες περιπτώσεις συνδυάστηκε με τη χρήση των ψηφιακών υπογραφών [Asokan], με τη διακριτική παρουσία σε όλα τα βήματα της συναλλασσόμενης διαδικασίας μιας Έμπιστης Οντότητας που επεμβαίνει μόνο όταν αυτή το κρίνει απαραίτητο [Bao] και άλλες φορές με τη συνολική παρακολούθηση της συναλλαγής [Ray]. Στα α μερικά προβλήματα των παραπάνω προτάσεων φαίνεται να δίνει λύση το πρωτόκολλο που προτείνεται από την ομάδα FIDES (Fair Integrated Data Exchange Services) [Zhang].

4.7.2 Αίτηση παροχής ανωνυμίας

Η χρήση του ψευδωνύμου γίνεται για την παροχή ισχυρής αυθεντικοποίησης και των αποδεικτικών τεκμηρίων για ένα σύνολο συναλλαγών.

Για τη διασφάλιση της υπηρεσίας γίνεται χρήση των συναρτήσεων σύνοψης και των ψηφιακών πιστοποιητικών. Είναι ευθύνη του Οργανισμού και των διαδικασιών του να ελέγξει την εγκυρότητα των στοιχείων και να προσφέρει με επάρκεια τη συγκεκριμένη υπηρεσία. Η εμπιστοσύνη προς τον Οργανισμό συνεπάγεται την παραγωγή μοναδικών ψευδωνύμων μίας χρήσης.

Είσοδος : Πρέπει να περιέχει κάποια στοιχεία αυθεντικοποίησης του χρήστη (π.χ. Identification number, email κ.τ.λ.) και το λόγο της παρεχόμενης δυνατότητας (π.χ. περιαγωγή, χρήση βιομετρικών τεχνικών, χρονοσήμανση, παροχή αποδεικτικών στοιχείων). Περιγράφοντας την με τη χρήση της XML Schema έχουμε:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="anonymity_usage" type="anonymity_usage_Type"/>

<xsd:complexType name="anonymity_usage_Type">
  <xsd:sequence>
    <xsd:element name="identification_number"
      type="xsd:unsignedLong" use="required"/>
    <!-- Η αποστολή του ηλεκτρονικού ταχυδρομείου είναι απαραίτητη για
    την επιστροφή του ψευδωνύμου [Chaum] διαφορετικά θα αποσταλεί στη
    διεύθυνση που ορίζεται μέσα από τον έλεγχο των στοιχείων και
    πιθανώς να παραμένει ανενεργή-->
```

```

<xsd:element name="email" type="xsd:string" use="required"/>
<xsd:element name="name" type="xsd:string" use="optional"/>
<xsd:element name="surname" type="xsd:string" use="optional"/>
<!-- Η χρήση του ψηφιακού πιστοποιητικού είναι απαραίτητη για
την αυθεντικοποίηση της οντότητας [Zhang]-->

<xsd:element name="user_cert"
              type="xsd:base64Binary" use="required"/>
<!-- Πρέπει να δηλώνεται ξεκάθαρα ο λόγος χρήσης της ανωνυμίας
έτσι ώστε να υποστηρίζονται οι περισσότερες από τις υπηρεσίες του
Οργανισμού-->

<xsd:element name="roaming" type="xsd:boolean" use="required"/>
<xsd:element name="biometric_authentication"
              type="xsd:boolean" use="required"/>
<xsd:element name="timestamping"
              type="xsd:boolean" use="required"/>
<xsd:element name="evidence"
              type="xsd:boolean" use="required"/>
<xsd:element name="any_other_reason"
              type="xsd:boolean" use="required"/>
<xsd:element name="time" type="xsd:datetime" use="required"/>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Έξοδος : Στο χρήστη επιστρέφεται ένα τυχαίο ψευδώνυμο και το χρονικό διάστημα ισχύος του. Με αυτό θα μπορεί να χρησιμοποιήσει κάποιες από τις βασικές και τις υποστηρικτικές υπηρεσίες του Οργανισμού. Προτείνεται η αναπαραγωγή των υπαρχόντων ψηφιακών πιστοποιητικών της αυθεντικοποιημένης οντότητας με αντικατάσταση του διακριτικού του ονόματος με το παραγόμενο ψευδώνυμο και διάρκεια χρήσης τους όση και το ψευδώνυμο χωρίς όμως να καταστρέφονται τα πρωτότυπα πιστοποιητικά που θα χρησιμοποιηθούν και σε επόμενες συναλλαγές (τα ίδια ή τροποποιημένα)

```

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<xsd:element name="anonymity_usage" type="anonymity_Type"/>

```

```

<xsd:complexType name="anonymity_Type">
    <xsd:sequence>
        <xsd:element name="identification_number"
            type="xsd:unsignedLong" use="required"/>
        <!-- Αποστέλεται η σύνοψη του ψευδωνύμου για τη διασφάλιση της
        ακεραιότητάς του -->

        <xsd:element name="pseudonym_hash"
            type="xsd:string" use="required"/>
        <xsd:element name="hash_algorithm"
            type="xsd:string" use="optional"/>
        <!-- Το παραγόμενο ψευδώνυμο συνήθως έχει μικρή διάρκεια
        ισχύος -->

        <xsd:element name="valid_from"
            type="xsd:datetime" use="required"/>
        <xsd:element name="valid_to"
            type="xsd:datetime" use="required"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

Αναφορές

1. Armington John, Purdy Ho, Paul Koznek, and Richard Martinez, Biometric Authentication in Infrastructure Security
2. Asokan N., V. Shoup, M. Waidner, Optimistic fair exchange of digital signatures, IEEE Journal on Selected Areas in Communications 18 (2000) 593–610.
3. Bacon J., Moody K., Yao W. “A model of OASIS role-based access control and its support for active security”, ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002, Pages 492–540.
4. Bao F., R. Deng, W. Mao, Eficient and practical fair exchange protocols with off-line TTP, Proc. IEEE Symposium on Security and Privacy, Oakland, CA, May 1998, pp. 77–85.
5. Blobel B., Hoepner P., Joop R., Kanouskos S., Kleinhuis G., Stasinopoulos G. “Using a privilege management infrastructure for secure web-based e-health

- applications”, Computer Communications, Volume 26, Issue 16, 15 October 2003, Pages 1863-1872
6. CDSA, Common Data Security Architecture
<http://developer.intel.com/ial/security>
 7. Chaum D.L., Untraceable electronic mail return addresses and digital pseudonyms, Communications of the ACM 24(1981) 84–88.and Industry (DTI).
 8. Cheng E. “An object-oriented organizational model to support dynamic role-based access control in electronic commerce”, Decision Support Systems 9 (2000) 357 - 369
 9. FNMT group, “PKITS – Public Key Infrastructure with Time-Stamping Authority”, Deliverable D3, EU project 23.192, April 1998
 10. Ford W. and Kaliski B., “Server-assisted generation of a strong secret from a password,” Proc. IEEE International Workshop on Enterprise Security, 2000.
 11. Herda S., “Non-repudiation: Constituting evidence and proof in digital cooperation”, Computer Standards & Interfaces, No.17, pp.69-79, Elsevier Science, 1995
 12. Hoover D. and B. Kausik, “Software smart cards via cryptographic camouflage,” Proc. IEEE Symp. on Security and Privacy, 1999.
 13. <http://www.surety.com>, Digital Notary Services
 14. ISO/IEC DIS 10181-4, “Draft International Standard: non-repudiation Framework”, 1993
 15. Jablon D., “Password authentication using multiple servers,” Topics in Cryptology– RSA 2001, Lecture Notes in Computer Science, Vol. 2020, Springer-Verlag, pp.344–360, 2001
 16. KEYSTONE, "Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture", Stefanos Gritzalis, Socrates Katsikas, Dimitrios Lekkas, Konstantinos Moulinos, Eleni Polydorou, Computers & Security, Vol.19,No.8 (2000) pp.731-746 Keystone Project, European Cross Domain PKI Architecture, 1998
 17. Kremer S., Markowitch O. Zhou J. “An intensive survey of fair non-repudiation protocols”, Computer Communications, Volume 25, Issue 17, 1 November 2002, Pages 1606-1621
 18. Linn J., Nystrom M., “Attribute Certification: An enabling Technology for Delegation and Role-Based Controls in Distributed Environments”,

- Proceedings of the 4th ACM Workshop on RBAC, Fairfax, VA, USA, October 1999
19. Newham E., Survey : Signature Verification Technologies, Elsevier Science,2000
20. Perlman R. and C. Kaufman, "Secure password-based protocol for downloading a private key," Proc. ISOC Network and Distributed System Security Symposium,1999
21. Peyravian Mohammad, Stephen M. Matyas, Allen Roginsky,Nevenko Zunic, "Ticket and Challenge-Based Protocols for Timestamping", Computers & Security, Volume 19, Issue 6, 1 October 2000, Pages 551-558
22. Polemi D., Biometric techniques, European Commission, European trusted Services Programme
23. Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, RFC1424, IETF, 1993
24. Ray, I. Ray, An anonymous fair exchange e-commerce protocol, Proc. First International Workshop on Internet Computing and E-Commerce, San Francisco, CA, April 2001, pp. 1790–1797.
25. RFC 2246, The TLS Protocol Version 1.0, <http://www.faqs.org/rfcs/rfc2246.html>
26. SDSI: A Simple Distributed Security Infrastructure, Laboratory for Computer Science, MIT, <http://theory.lcs.mit.edu/~rivest/sdsi10.html>, 1996
27. Shen Jau-Ji, Chih-Wei Lin, Min-Shiang, Hwang, "An enhancement of timestamp-based password authentication scheme", Computers & Security, Volume 21, Issue 7, November 2002, Pages 665-667
28. Taekyoung Kwon, Virtual Software Tokens – A Practical Way to Secure PKI Roaming
29. Tak S., Lee Y, Park E. "A software framework for non-repudiation service in electronic commerce based on the Internet", Microprocessors and Microsystems, Volume 27, Issues 5-6, 11 June 2003, Pages 265-276
30. TIMESEC": Digital Timestamping and the Evaluation of Security Primitives", Katholieke Universiteit Leuven, December 1999
31. Wang, Li, Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme", Computers & Security, Volume 22, Issue 7, October 2003, Pages 643-645

32. Wilson Stephen, «A vulnerability assessment of roaming soft certificate PKI solutions», March 2002
33. www.aamva.org, National Committee for Information Technology Standards
34. www.bioapi.org , BioAPI Consortium
35. www.jtc1.org , ISO/OEC Joint Technical Committee One
36. www.nist.gov/cbeff , National Institute for Standards and Technologies (NIST)
37. www.x9.org, ANSI X9.84 – 2001
38. X-509 | ISO/IEC 9594-8, International Telecommunication Union, “The directory: Public-key and attribute certificate frameworks”, ITU, X-Series
39. X-812, International Telecommunication Union, “Security frameworks for open systems: Access control framework”, ITU, X-Series
40. X-812, International Telecommunication Union, “Security frameworks for open systems: Access control framework”, ITU, X-Series
41. Zhang N., Q. Shi, M. Merabi An efficient protocol for anonymous and fair document exchange, Computer Networks, Volume 41, Issue 1, 15 January 2003, Pages 19-28
42. Zhou1 J., Gollman D. “Evidence and non-repudiation”, Journal of Network and Computer Application (1997) 20, 267-281
43. Zhou2 J., Iam K.Y. “Securing digital signatures for non-repudiation”, Computer Communications, Volume 22, Issue 8, 25 May 1999, Pages 710-716
44. Λέκκας Δημήτρης, Διδακτορική διατριβή, «Ασφάλεια Πληροφοριακών Συστημάτων με χρήση υπηρεσιών Έμπιστης Τρίτης Οντότητας»



Κεφάλαιο 5 Προτεινόμενη Αρχιτεκτονική υλοποίησης ΥΔΚ για παροχή Υπηρεσιών Προστιθέμενης Αξίας

5.1 Μοντέλο Αναφοράς και Γενικά Χαρακτηριστικά

Η δημιουργία ενός αφαιρετικού μοντέλου αναφοράς για την ενσωμάτωση των Υπηρεσιών Προστιθέμενης Αξίας στην υπάρχουσα λειτουργική αρχιτεκτονική του παρόχου θα πρέπει να είναι το δυνατότερο εφικτή και εύκολα υλοποιήσιμη και μεταβιβάσιμη. Στο αναφερόμενο μοντέλο (Σχήμα 5.1) διαφαίνεται η λειτουργική θέση των δρώντων οντοτήτων και το είδος της σχέσης τους. Σαν δρώντες αναφέρονται οι χρήστες των Υπηρεσιών Προστιθέμενης Αξίας (μεμονωμένοι ή ως μέλη μιας ομάδας ή ενός Οργανισμού) ενώ το είδος της σχέσης τους είναι είτε συναλλακτική είτε συνεργατική ή υποστηρικτική. Χαρακτηριστικά διακρίνονται :

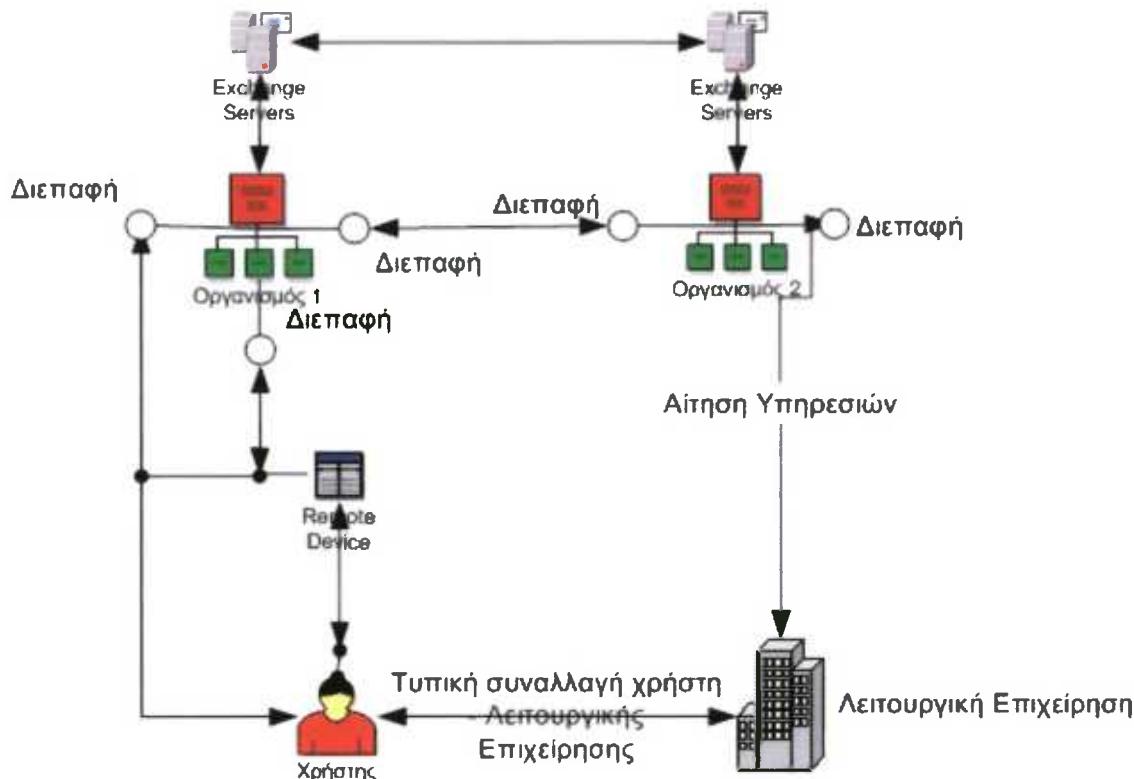
- Το χρήστη των Υπηρεσιών που μέσα από συγκεκριμένες διεπαφές χρησιμοποιεί αυτές τις υπηρεσίες.
- Το χρήστη να συνδιαλέγεται με άλλους χρήστες και ο ρόλος του Οργανισμού να είναι καθαρά υποστηρικτικός.
- Το μεμονωμένο χρήστη να υποστηρίζεται από τη χρήση των μεταφέρσιμων συσκευών (Remote Devices), ενώ οι τελευταίες είναι υπεύθυνες για την επικοινωνία με τον Οργανισμό μέσω κατάλληλων διεπαφών.
- Τους πάροχους των Υπηρεσιών να συνεργάζονται τόσο σε λογικό όσο και σε φυσικό επίπεδο για την υποστήριξη των λειτουργιών τους.

Το αναφερόμενο μοντέλο αναφοράς θα πρέπει να χαρακτηρίζεται από τις παρακάτω ιδιότητες για την καλύτερη υποστήριξή του :

- **Ευελιξία** : εξαρτάται άμεσα από το βαθμό της αφαιρετικότητάς του κατά τη φάση της σχεδίασης. Μεγαλύτερη αφαίρεση κατά τη σχεδίαση σημαίνει πως η υλοποιημένη αρχιτεκτονική θα έχει τη δυνατότητα στο μέλλον να ενσωματώσει και νέες τεχνολογικές απαιτήσεις.
- **Κλιμάκωση** : στη φάση του σχεδιασμού του συστήματος θα πρέπει να ληφθεί υπόψη και η συμμετοχή μεγάλου αριθμού δρώντων οντοτήτων.
- **Επεκτασιμότητα** : στο αναφερόμενο μοντέλο θα πρέπει να υπάρχει η δυνατότητα προσθήκης και νέων υποστηρικτικών υπηρεσιών χωρίς να απαιτείται η επαναδημιουργία του αναφερόμενου μοντέλου.

- Χρησιμότητα :** οι υλοποιούμενες διεπαφές θα πρέπει να είναι όσο το δυνατό περισσότερο φιλικές προς τον τελικό χρήστη και συμβατές με πιθανές υπάρχουσες υλοποιήσεις.
- Προτυποποίηση:** η αναφερόμενη αρχιτεκτονική θα πρέπει να είναι συμβατή με την υπάρχουσα τεκμηρίωση των υπηρεσιών.

Στο επόμενο σχήμα υλοποιούνται οι παραπάνω ιδιότητες και χαρακτηριστικά:



Σχήμα 5.1 Μοντέλο Αναφοράς

5.2 Ανάλυση Λειτουργικής Αρχιτεκτονικής

5.2.1 Βασικά Χαρακτηριστικά

Όπως διαπιστώσαμε στο Κεφάλαιο 4, οι παρεχόμενες Υπηρεσίες Προστιθέμενης Αξίας από έναν Οργανισμό εμπλέκουν διαφορετικές τεχνολογίες που δε σχετίζονται μεταξύ τους αλλά συνεργάζονται μεταξύ τους για την παροχή μιας συγκεκριμένης υπηρεσίας. Για παράδειγμα η υλοποίηση της υπηρεσίας Αποδεικτικών Στοιχείων χρησιμοποιεί την Υπηρεσία της Χρονοσήμανσης και τις τεχνολογίες κρυπτογράφησης δημόσιου κλειδιού για την παροχή μιας ολοκληρωμένης υπηρεσίας.

Για αυτό το λόγο είναι αναγκαίος ο διαχωρισμός της συνολικής αρχιτεκτονικής σε επιμέρους τμήματα – λειτουργικές μονάδες (functional units)- έτσι ώστε να είναι εύκολα διαχειρίσιμα και υλοποιήσιμα. Οι λειτουργικές μονάδες επικοινωνούν μεταξύ τους και με τις φυσικές και λογικές διεπαφές του χρήστη, έχοντας σαν είσοδο τις λειτουργικές απαιτήσεις των χρηστών και σαν έξοδο την παροχή μεμονωμένων ή συνολικών υπηρεσιών μέσω ενός ενδιάμεσου επιπέδου (middleware). Η περιγραφή τους παρουσιάστηκε στο Κεφάλαιο 4 όπου αναδείχτηκε η ανάγκη της τυποποίησης κάθε αιτήματος έτσι ώστε να διευκολύνεται η επεξεργασία του και η ανάγκη για υποστήριξη της διαλειτουργικότητας. Η χρήση ενός τέτοιου επιπέδου απομονώνει τις εσωτερικές λειτουργίες κάθε μονάδας προσφέροντας πλεονεκτήματα στην κλιμάκωση, ανάπτυξη και συντήρηση ενός τέτοιου συστήματος, ενώ παράλληλα αυξάνει τη δυνατότητα επικοινωνίας μεταξύ διαφορετικών Οργανισμών. Από τη στιγμή μάλιστα που κάθε μονάδα δεν δεσμεύεται στη χρήση συγκεκριμένης τεχνολογίας, είναι στη διακριτική ευχέρεια του κάθε Οργανισμού να επιλέξει οποιαδήποτε τεχνολογία για την παροχή της απαιτούμενης λειτουργικότητας. Τα κριτήρια επιλογής είναι ανεξάρτητα της δομής της αρχιτεκτονικής του κάθε Οργανισμού και περιορίζονται μόνο από θέματα προτυποποίησης και λειτουργικής συμβατότητας.

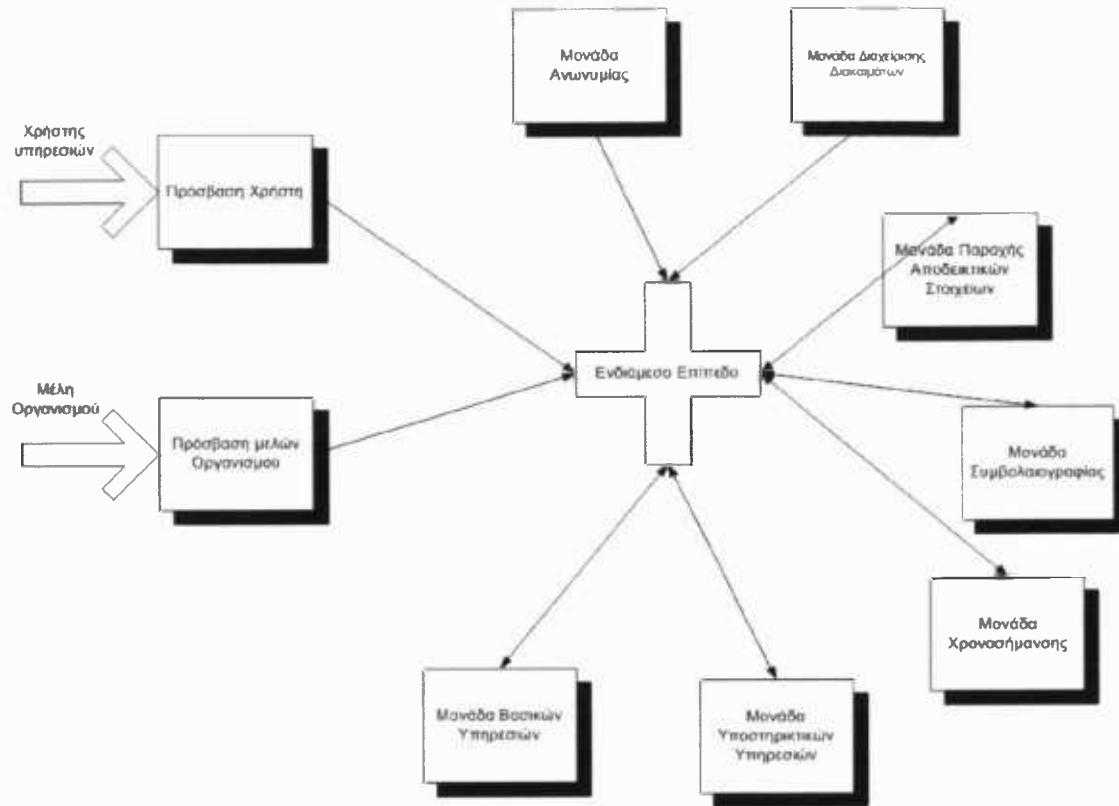
5.2.2 Προσδιορισμός Λειτουργικών Μονάδων (Functional Units)

Η ομαδοποίηση των διαφορετικών λειτουργιών σε μονάδες είναι η ακόλουθη :

- **Πρόσβαση χρήστη:** ανήκουν τα μέσα και οι διεπαφές που παρέχονται στο χρήστη των υπηρεσιών για την ασφαλή πρόσβαση σε αυτές. Εδώ διακρίνουμε και τη χρήση των συσκευών για την παροχή υπηρεσιών Περιαγωγής και των Βιομετρικών μεθόδων αυθεντικοποίησης [βλ. §4.5 και §4.7 αντίστοιχα].
- **Πρόσβαση μελών Οργανισμού :** ανήκουν τα μέσα και οι διεπαφές που χρησιμοποιεί το προσωπικό του Οργανισμού για τη διαχείριση των υπηρεσιών.
- **Μονάδα Βασικών υπηρεσιών :** διακρίνουμε το βασικό σύνολο των υπηρεσιών ενός Οργανισμού. Η συγκεκριμένη μονάδα διαχωρίζεται σε μικρότερες για την καλύτερη διαχείριση και επικοινωνία με τις υπόλοιπες μονάδες μιας και η υποστήριξή τους είναι απαραίτητη για την παροχή των υπηρεσιών Προστιθέμενης Αξίας [βλ. §3.2.1].

- **Μονάδα Υποστηρικτικών υπηρεσιών** : διακρίνουμε όλες τις δευτερεύουσες υπηρεσίες που απαιτούνται από τη λειτουργία των άλλων υπηρεσιών με σημαντικότερη την παροχή κρυπτογραφικών λειτουργιών [βλ. §3.2.2].
- **Μονάδα Χρονοσήμανσης** : υποστηρίζει την υπηρεσία της Χρονοσήμανσης [βλ. §4.1].
- **Μονάδα Συμβολαιογραφίας** : υποστηρίζει την υπηρεσία της Συμβολαιογραφίας [βλ. §4.2].
- **Μονάδα Αποδεικτικών Στοιχείων** : υποστηρίζει την υπηρεσία των Αποδεικτικών Στοιχείων. Συνεργάζεται με τη μονάδα Χρονοσήμανσης και Συμβολαιογραφίας [βλ. §4.3].
- **Μονάδα Διαχείρισης Δικαιωμάτων** : υποστηρίζει την υπηρεσία Διαχείρισης Δικαιωμάτων [βλ. §4.4].
- **Μονάδα Ανωνυμίας** : παρέχει τη δυνατότητα ανωνυμίας στο χρήστη των υπηρεσιών και συνεργάζεται με όλες τις παραπάνω μονάδες [βλ. §4.7].
- **Ενδιάμεσο Επίπεδο** : παίζει το ρόλο του ρυθμιστή της λειτουργίας των επιμέρους τμημάτων. Δέχεται στην είσοδο διάφορα αιτήματα και παράγει τις αντίστοιχες δομές ή λειτουργίες.

Όλες οι μονάδες είναι σε επικοινωνία με το ενδιάμεσο επίπεδο που είναι υπεύθυνο για την επικοινωνία μεταξύ των διαφορετικών μονάδων και την κατάλληλη μορφοποίηση και μετασχηματισμό των αιτήσεων εισόδου και εξόδου. Οι μονάδες και η μεταξύ τους επικοινωνία απεικονίζεται στο παρακάτω σχήμα :



Σχήμα 5.2 Προσδιορισμός Λειτουργικών Μονάδων

5.2.3 Περιγραφή Αρχιτεκτονικής

Η προτεινόμενη αρχιτεκτονική ακολουθεί την Αρχιτεκτονική Τριών Επιπέδων (3 Tier Architecture). Σύμφωνα με το Σχήμα 5.3 η διαστρωμάτωση μιας τέτοιας εφαρμογής αποτελείται από τρία επίπεδα :



Σχήμα 5.3 Αρχιτεκτονική Τριών Επιπέδων

Το πρώτο επίπεδο, η διεπαφή του χρήστη του συστήματος, περιλαμβάνει τις λειτουργίες του χρήστη όπως ένα κείμενο εισόδου, ένα κείμενο διαλόγου και οθόνες διαχείρισης λειτουργιών. Το τρίτο επίπεδο παρέχει τις λειτουργίες για τη διαχείριση της Βάσης Δεδομένων και δεν είναι ανάγκη να χρησιμοποιεί κάποια συγκεκριμένη γλώσσα διαχείρισης Βάσεων Δεδομένων, ώστόσο προτείνεται η χρήση της SQL (Structure Query Language) σαν την ευρέως πιο αποδεκτή γλώσσα. Το μεσαίο επίπεδο παρέχει τις λειτουργίες διαχείρισης διαδικασιών (όπως διαδικασία ανάπτυξης, παρακολούθησης διαδικασιών κ.α.) οι οποίες διαμοιράζονται από πολλαπλές εφαρμογές. Το μεσαίο επίπεδο εξυπηρετητή (το οποίο αναφέρεται και σαν Εφαρμογή Εξυπηρέτη – Application Server) βελτιώνει την απόδοση, την ευελιξία, τη συντηρησιμότητα, την επαναχρησιμοποίηση και τη δυνατότητα διαβάθμισης με το να κεντρικοποιεί τη διαδικαστική λογική. Η κεντρικοποιημένη διαχειριστική λογική κάνει τη διαχείριση (administration) και τη διαχείριση των αλλαγών (change

management) πιο εύκολη γιατί οι αλλαγές γράφονται μόνο μια φορά και να τοποθετούνται στο ενδιάμεσο επίπεδο του εξυπηρετητή έτσι ώστε να είναι διαθέσιμες σε όλα τα συστήματα. Επιπλέον, το ενδιάμεσο επίπεδο ελέγχει τις συναλλαγές και τις ασύγχρονες μεταδόσεις με τη Βάση Δεδομένων έτσι ώστε να επιβεβαιώσει ή όχι την τελική επίτευξη των διαδικασιών. Ουσιαστικά είναι αυτό που ελέγχει και καθορίζει τη Δύο Φάσεων Διαδικασία Επίτευξη Συναλλαγής με τη Βάση Δεδομένων.(Database Two Phase Commit).

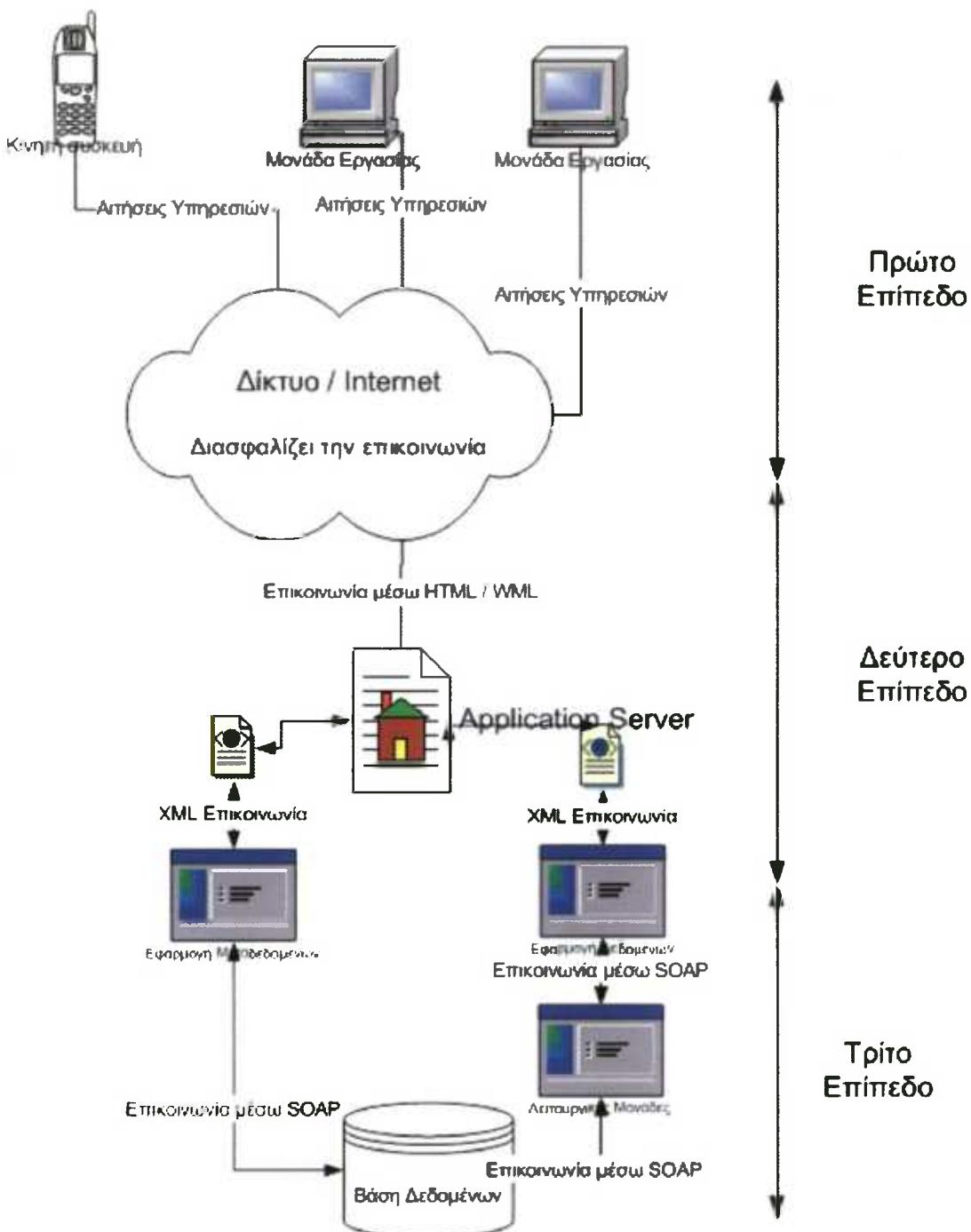
5.2.3.1 Μοντέλο υλοποίησης

Τα βασικά χαρακτηριστικά της προτεινόμενης υλοποίησης [Σχήμα 5.4] συνοψίζονται στα :

- **Ευελιξία και Επεκτασιμότητα :** Η σχεδίαση της προτεινόμενης υλοποίησης έγινε με γνώμονα τη λειτουργική επικοινωνία των διαφορετικών μονάδων και τη δυνατότητα ενσωμάτωσης νέων τεχνολογιών ή αντικατάστασης των ήδη υπαρχόντων.
- **Συμβατότητα :** Ο Οργανισμός πρέπει να υποστηρίζει όλες τις υπηρεσίες σε απόλυτη σύμβαση με τις υπάρχουσες υλοποίησεις πρωτοκόλλων ή τις υλοποίησεις άλλων Οργανισμών.
- **Κλιμάκωση :** Η προτεινόμενη αρχιτεκτονική δίνει τη δυνατότητα στον Οργανισμό να εκμεταλλευτεί τις κορυφαίες τεχνολογικές προτάσεις της αγοράς και μέσω αυτών να μπορέσει να αντεπεξέλθει σε πιθανή αύξηση των χρηστών – πελατών του.
- **Διαλειτουργικότητα :** Η προτεινόμενη υλοποίηση δίνει τη δυνατότητα στις διαφορετικές μονάδες να επικοινωνούν μεταξύ τους μέσω του μεσαίου επιπέδου με πλήρη διαφάνεια (χρήση Application Server με υποστήριξη XML Web Services).
- **Ανοικτή υλοποίηση (Open System) :** Οι παρεχόμενες υπηρεσίες μπορούν να χρησιμοποιηθούν ασφαλώς και πάνω από ανοικτά ανασφαλή δίκτυα όπως το Internet. Η χρήση της και σε κλειστά ιδιωτικά δίκτυα ωστόσο δεν απορρίπτεται.

Τα βασικά στοιχεία της προτεινόμενης υλοποίησης [Σχήμα 5.4] συνοψίζονται στα :

- **Μονάδα διεπαφών :** αποτελεί το μέσο επικοινωνίας των διαφόρων χρηστών με την προτεινόμενη υλοποίηση. Η πρόσβαση σε αυτή μπορεί να γίνεται είτε μέσω τερματικών σταθμών ή και ακόμα μετακινούμενων συσκευών (mobile devices). Για τη δημιουργία των διεπαφών προτείνεται η χρήση HTML αντικειμένων που παράγονται από τον ορισμό των ιδιοτήτων των οντοτήτων μέσα από την Εφαρμογή των Μεταδεδομένων. Πρόσβαση στην Εφαρμογή αυτή έχουν μόνο σαφώς ορισμένες οντότητες του Οργανισμού. Πληρέστερος ορισμός αυτών γίνεται στην Παράγραφο 5.2.3.2.
- **Μονάδα εξυπηρέτησης (Application Server) :** αποτελεί το ενδιάμεσο επίπεδο επικοινωνίας ανάμεσα τις διεπαφές των χρηστών και την προτεινόμενη Βάση Δεδομένων. Εδώ διαχειρίζεται όλη η επιχειρηματική λογική, επιτυγχάνεται η επικοινωνία με τις διαφορετικές λειτουργικές μονάδες μέσω της χρήσης των XML Web Services και είναι υπεύθυνη για την αποθήκευση των δεδομένων στη Βάση Δεδομένων μέσω της χρήσης του πρωτοκόλλου SOAP (Εφαρμογή Δεδομένων). Στο επίπεδο αυτό διακρίνουμε και την Εφαρμογή Μεταδεδομένων που χρησιμοποιείται για τον ορισμό των νέων οντοτήτων του μοντέλου και της διαχείρισης των προσβάσεων σε αυτά. Διακρίνουμε επίσης την Εφαρμογή Δεδομένων η οποία αποτελεί την επαφή για τη διαχείριση συγκεκριμένων στιγμιότυπων των ορισμένων οντοτήτων (π.χ. Χρονοσφαγίδα) και την επικοινωνία με τις επιμέρους λειτουργικές μονάδες. Μέσω της εφαρμογής αυτής οι διαφορετικοί δρώντες αιτούνται υπηρεσιών και διαχειρίζονται τις παραγόμενες πληροφορίες.
- **Υποστηρικτική Βάση Δεδομένων :** Η συγκεκριμένη υλοποίηση προτείνει και το σχεδιασμό μιας αφαιρετικής Βάσης Δεδομένων που δίνει στον Οργανισμό μεγάλο βαθμό ευελιξίας για την υλοποίηση της παρεχόμενης υποδομής



Σχήμα 5.4 Προτεινόμενη Υλοποίηση

5.2.3.2 Περιγραφή Βάσης Δεδομένων

Για την υποστήριξη των υπηρεσιών του Οργανισμού προτείνεται μια αφαιρετική Βάση Δεδομένων που κύριοι σκοποί που τέθηκαν κατά τη φάση σχεδιασμού της ήταν η υποστήριξη της πολυγλωσσίας από τον Οργανισμό, η δυνατότητα ενσωμάτωσης της Ασφάλειας των δεδομένων μέσα από ένα κεντρικό

σύστημα διαχείρισης ρόλων (Role based System) πάνω στις ορισμένες από τον Οργανισμό οντότητες, η δυνατότητα κλιμάκωσης των δεδομένων μέσω του ορισμού νέων οντοτήτων και η δυνατότητα επικοινωνίας και με άλλες Βάσεις Δεδομένων άλλων Οργανισμών. Οι ρόλοι του συστήματος δεν είναι δεσμευτικό να ανταποκρίνονται και σε πραγματικούς ρόλους του Οργανισμού ή να υπάρχει μία προς μία αντιστοίχιση. Η συγκεκριμένη πρόταση υλοποίησης είναι άκρως ενδιαφέρουσα μιας και μπορεί να υποστηρίξει κάθε είδους παραγόμενου μοντέλου αναφοράς διαφορετικών Οργανισμών με διαφορετικές διαδικασίες και πολιτικές. Αυτό που έχει να κάνει κάθε Οργανισμός είναι να ενσωματώσει τις διαδικασίες υποστήριξης των υπηρεσιών που προσφέρει μέσα στο μοντέλο της Βάσης Δεδομένων.

Η περιγραφή των πινάκων της προτεινόμενης Βάσης Δεδομένων παρουσιάζεται στον Πίνακα 5.1 ενώ στο Παράρτημα υπάρχει η περιγραφή της Βάσης Δεδομένων με τη χρήση του XML Schema.

Όνομα Πίνακα	Περιγραφή
tblLanguages	Ορίζονται οι χρησιμοποιούμενες γλώσσες του συστήματος.
tblClasses	Ο πίνακας κλάσης αντικειμένων περιγράφει τις κλάσεις των αντικειμένων. Μέσω αυτού του πίνακα γνωρίζουμε όταν δημιουργούμε ένα αντικείμενο ποιες θα είναι οι ιδιότητες του αντικειμένου. Συνδέεται με τον tblClassesMlg για την υποστήριξη της δυνατότητας πολυγλωσσίας της ορισμένης οντότητας. Ένα παράδειγμα είναι η δήλωση μιας νέας οντότητας αντικειμένων με το όνομα «Ψηφιακό Πιστοποιητικό»
tblClassRelationTypes	Καθορίζει τον τόπο της σχέσης μεταξύ δύο κλάσεων οντοτήτων. Για παράδειγμα συσχετίζω την κλάση «Χρονοσφαγίδα» με την «Αποδεικτικό Τεκμήριο» και τη σχέση την ονομάζω «Παροχή

	Αποδεικτικών Τεκμηρίων».
tblClassStructure	Ορίζεται η δενδροειδής μορφή της απεικόνισης των κλάσεων – οντότητων. Για παράδειγμα κάτω από την οντότητα «Ψηφιακό Πιστοποιητικό» μπορώ να «κρεμάσω» άλλη οντότητα «Ψηφιακό Πιστοποιητικό» ή την οντότητα «Βιομετρικό χαρακτηριστικό».
tblProperties	Ορίζονται νέες ιδιότητες του συστήματος. Π.χ. η ιδιότητα «Όνομα» είναι τύπου string, το μέγεθος της είναι 50 χαρακτήρες, και η ελάχιστη τιμή της μπορεί να έχει 2 χαρακτήρες. Συνδέεται με τον πίνακα tblPropertiesMlg για την υποστήριξη της πολυγλωσσίας.
TblTypesOfPropertyData	Καθορίζει το είδος της αναφερόμενης ιδιότητας π.χ. string, numeric, bit κ.τ.λ.
tblClassToPropertyRelations	Συσχετίζει μία οντότητα – κλάση με μία συγκεκριμένη ιδιότητα δίνοντας και πιθανόν και νέα χαρακτηριστικά. Για παράδειγμα, η οντότητα «Ψηφιακό Πιστοποιητικό» περιλαμβάνει την ιδιότητα «Όνομα Εκδότη».
tblPropertyValues	Καθορίζει μια λίστα από πιθανές τιμές για μια συγκεκριμένη ιδιότητα μιας κλάσης. Έτσι η ιδιότητα «Αλγόριθμος Σύνοψης» του «Ψηφιακού Πιστοποιητικού» μπορεί να πάρει τις τιμές MD5 ή SHA-1.
tblMethods	Καθορίζει τις χρησιμοποιούμενες μεθόδους του συστήματος (π.χ. Ανάγνωση, Εισαγωγή, Διαγραφή, Τροποποίηση, Αναζήτηση, Αντιγραφή

	κ.τ.λ). Συνδέεται με τον tblMethodsMlg για την υποστήριξη της πολυγλωσσίας.
tblStatus	Καθορίζει τις χρησιμοποιούμενες μεθόδους του συστήματος (π.χ. ενεργό, ανενεργό, προσωρινά απενεργοποιημένο, εκδομένο κ.τ.λ). Συνδέεται με τον tblStatusMlg για την υποστήριξη της πολυγλωσσίας.
tblRoles	Δηλώνονται οι χρησιμοποιούμενοι ρόλοι του συστήματος. Για χρησιμοποιούμενοι ρόλοι σε ένα τέτοιο σύστημα μπορεί να είναι :«PKI Χρήστης», «PKI Manager», «Certificate Manager» κ.τ.λ. Συνδέεται με τον tblRolesMlg για την υποστήριξη της πολυγλωσσίας.
tblTreePermissions	Χρησιμοποιείται για την αναπαραγωγή των δυνατών μεθόδων του συγκεκριμένου χρήστη με συγκεκριμένο ρόλο ή πλήθος από ρόλους, για συγκεκριμένη κλάση οντότητας που βρίσκεται σε συγκεκριμένη κατάσταση. Για παράδειγμα ο ρόλος «PKI Χρήστης» θα μπορεί να διαβάζει μία κλάση τύπου «Ψηφιακού Πιστοποιητικού» που βρίσκεται σε κατάσταση «Εκδομένο».
tblEditPermissions	Αποτελείται πάλι από μια τετράδα <Κλάση, Κατάσταση, Μέθοδο, Ρόλο> μόνο που τώρα υποδεικνύεται σε ποια κατάσταση μπορεί ο συγκεκριμένος ρόλος να μεταφέρει τη συγκεκριμένη οντότητα – κλάση. Π.χ. ο ρόλος «PKI Manager» μπορεί να τροποποιήσει μια

	οντότητα «Ψηφιακό Πιστοποιητικό» και να την κάνει «Ανενεργή».
tblRoleToRoleRelations	Καθορίζει τον τρόπο διαχείρισης μεταξύ των ρόλων του συστήματος. Για παράδειγμα ο ρόλος «PKI Manager» επικοινωνεί με το ρόλο «PKI Χρήστης» και μπορεί να διαχειριστεί το είδος των προσβάσεων του (Το πεδίο Manage Access).
tblAccessStatus	Καθορίζει το είδος των Προσβάσεων πάνω στα αντικείμενα του χρησιμοποιήσιμου συστήματος. Για παράδειγμα η πρόσβαση σε ένα αντικείμενο τύπου «Application» μπορεί να είναι σε Κατάσταση Πρόσβασης «Ελεύθερη Πρόσβαση» ενώ για τον τύπο «Ψηφιακό Πιστοποιητικό» σε Κατάσταση Πρόσβασης «Μέλος του PKI».
tblLogins	Ορίζονται οι χρήστες του συστήματος με την καταγραφή κάποιων στοιχείων.
tblGroups	Ορίζονται οι Ομάδες του Συστήματος.
tblGroupLoginRelations	Καθορίζεται η συσχέτιση μιας Ομάδας και ενός χρήστη.
tblIPAddresses	Καθορίζεται η συσχέτιση ενός Χρήστη του συστήματος με την πρόσβαση σε αυτό από συγκεκριμένη IP Διεύθυνση.
tblPublicItems	Καθορίζει τα παραγόμενα αντικείμενα του συστήματος περιλαμβάνοντας τον Τίτλο, το είδος της Κλάσης, της Κατάστασης, του είδους Πρόσβασης, το αντικείμενο Γονέα και το ID του χρήστη στο οποίο πιθανώς να ανήκει. Η

	πρόσβαση στο αντικείμενο αυτό, ανάλογα με το είδος του Κανόνα Εξακρίβωσης και της Κατάστασής του, καθορίζεται από τους πίνακες tblAccessOnPublicItems, tblAccessOnPublicItemsByGroups και tblTreePermissions. Η χρήση του πεδίου «Αντικείμενο Γονέας» μας επιτρέπει τη δημιουργία αλληλουχίας συνδεδεμένων αντικείμενων.
tblAccessOnPublicItems	Συσχετίζει την πρόσβαση σε ένα αντικείμενο με ένα χρήστη συγκεκριμένου Ρόλου για μια περίοδο χρήσης. Για παράδειγμα ορίζεται η πρόσβαση στο αντικείμενο “Ψηφιακό Πιστοποιητικό PKI” για το χρήστη “Νίκος Ρέντας” όταν έχει το ρόλο “PKI Χρήστης” για την περίοδο 20/11/2003 έως 20/11/2004.
tblAccessOnPublicItemsByGroups	Συσχετίζει την πρόσβαση σε ένα αντικείμενο με μια Ομάδα Χρηστών συγκεκριμένου Ρόλου για μια περίοδο χρήσης.
tblPublicToPublicRelations	Ορίζονται τα συσχετιζόμενα αντικείμενα. Για παράδειγμα μπορώ να συσχετίσω ένα στιγμότυπο του αντικειμένου Χρονοσφαγίδα με ένα στιγμότυπο του αντικειμένου Αποδεικτικό Τεκμήριο.
tblPublicDataTypeString, tblPublicDataTypeText, tblPublicDataTypeNumber, tblPublicTypedDateTime, tblPublicDataTypeLookUp,	Αποθηκεύονται τα δεδομένα του αντίστοιχου τύπου με συγκεκριμένες ιδιότητες για συγκεκριμένο αντικείμενο.

tblPublicDataTypeBoolean	
tblSessions	Αποθηκεύονται οι διεργασίες Συνόδου για την ασφαλή επικοινωνία με το Πληροφοριακό Σύστημα της αναφερόμενης Υποδομής.
tblSystemVariables	Αποθηκεύονται οι Σταθερές Μεταβλητές του Συστήματος.
tblErrorMessages	Αποθηκεύονται τα μηνύματα λάθους.

Πίνακας 5.1 Ανάλυση των πινάκων της Βάσης Δεδομένων

Για να αποσαφηνιστεί καλύτερα η προτεινόμενη υλοποίηση και πως αυτή είναι δυνατή να υποστηρίξει τις Υπηρεσίες Προστιθέμενης Αξίας ενός Οργανισμού αλλά και τις υπόλοιπες Βασικές υπηρεσίες αναφέρουμε ένα συγκεκριμένο παράδειγμα και δείχνουμε την απεικόνιση του με δεδομένα στη συγκεκριμένη Βάση Δεδομένων.

Θεωρούμε το παράδειγμα της παράδειγμα της παραγωγής της Χρονοσφαγίδας. Καταρχήν, ορίζουμε τους περφιφερειακούς πίνακες. Έτσι έχουμε :

tblLanguages :

LanguageID	UISortingNumber	UIName
1	1	En
2	2	El

tblStatus :

StatusID
1
2

tblStatusMlg:

StatusID	LanguageID	UIName	UIDescription
1	1	Active	
1	2	Ενεργό	
2	1	Inactive	
2	2	Ανενεργό	

tblMethods :

MethodID
1
2
3
4

tblMethodsMlg:

MethodID	LanguageID	UIName	UIDescription
1	1	Read	
1	2	Ανάγνωση	
2	1	Insert	
2	2	Εισαγωγή	
3	1	Delete	
3	2	Διαγραφή	
4	1	Modify	
4	2	Τροποποίηση	

tblRoles

RoleID	RoleIsManager
1	0
2	1

tblRolesMlg

RoleID	LanguageID	UIName	UIDescription
1	1	PKI_User	
1	2	Χρήστης ΥΔΚ	
2	1	PKI_Manager	
2	2	Διαχειριστής ΥΔΚ	

tblRoleToRoleRelations

RoleID	RelatedRoleID	ManageAttributes	ManageAccess
2	1	1	1
1	1	0	0

1	2	0	0
2	2	0	0

tblTypesOfPropertyData

TypeOfPropertyDataID	UIName
1	String
2	Numeric
3	Boolean
4	DateTime
5	LongText
6	LookUp

tblAccessStatus

1
2
3

TblAccessStatusMlg

AccessStatusID	LanguageID	UIName	UIDescription
1	1	Free Access	
1	2	Ελεύθερη Πρόσβαση	
2	1	Members Only	
2	2	Μόνο για μέλη	
3	1	More Access	
3	2	Επιπλέον Δικαίωμα	

Έχοντας ορίσει τα δεδομένα των περιφερειακών πινάκων μέσα από την Εφαρμογή των Μεταδεδομένων, ο εξουσιοδοτημένος χρήστης του Οργανισμού μπορεί να ορίσει και τις νέες οντότητες με τις αντίστοιχες ιδιότητές τους και πάλι μέσα από την Εφαρμογή των Μεταδεδομένων. Έτσι έχουμε τον ορισμό μιας κλάσης «Ψηφιακό Πιστοποιητικό» και της κλάσης «Χρονοσφαγίδα».

tblClassess

ClassID	DefaultAccessStatusID	ClassPrefixName
1	Null	Root
2	Null	Cert
3	Null	Timestamp

tblClassesMlg

ClassID	LanguageID	UIName	UIDescription
1	1	Root	
1	2	Root	Είναι η αρχική κλάση κάτω από την οποία δημιουργείται μια δενδροειδής μορφή αλληλουχίας κλάσεων.
2	1	Certificate	
2	2	Ψηφιακό Πιστοποιητικό	Είναι η κλάση με την οποία συσχετίζεται μια φυσική οντότητα με μια ψηφιακή υπογραφή.
3	1	Timestamp	
3	2	Χρονοσφαγίδα	Είναι η κλάση για την υποστήριξη της συγκεκριμένης υπηρεσίας.

tblClassStructure

ClassID	ParentClassID
1	Null
2	1
3	1
3	3

tblProperties

PropertyID	TypeOfProperty	UISize	UIMaxLength	VarName	VarMinValue	VarMaxValue
1	2	10	10	SerialNo	0	1000000000

2	1	100	200	Issuer	Null	Null
3	4	30	null	ValidityFrom	1/1/1970	1/1/2003
4	4	30	Null	ValidityTo	1/1/2004	1/1/2040
5	6	Null	Null	SigAlgorithm	Null	Null
6	5	Null	Null	SigData	Null	Null
7	6	Null	Null	Valid	Null	Null
8	1	100	150	Title	10	150

TblPropertiesMlg

PropertyID	LaguageID	UILabel	VarDefaultValue
1	1	Serial Number	null
1	2	Σειριακός Αριθμός	null
2	1	Issuer	null
2	2	Εκδότης	Null
3	1	Valid not Before	1/1/2003
3	2	Έγκυρο όχι πριν	1/1/2003
4	1	Valid not After	1/1/2040
4	2	Έγκυρο όχι μετά	1/1/2040
5	1	Signature Algorithm	Null
5	2	Αλγόριθμος Υπογραφής	Null
6	1	Signature Data	Null
6	2	Δεδομένα Υπογραφής	Null
7	1	Valid	Null
7	2	Έγκυρο	Null
8	1	Title	Null
8	2	Τίτλος	null

tblPropertyValues

PropertyValueID	PropertyID
1	5
2	5
3	5
4	7
5	7

tblPropertyValuesMlg

PropetyValueID	LanguageID	UIName
1	1	MD5
1	2	MD5
2	1	SHA-1
2	2	SHA-1
3	1	RIPEMD-160
3	2	RIPEMD-160
4	1	YES
4	2	ΝΑΙ
5	1	NO
5	2	ΟΧΙ

tblClassToPropertyRelations

ClassID	PropertyID	PropertyIsHidden	PropertyIsSearchable	PropertyIsMandatory	PropertyIsDefault	PropertyIsReadOnly
1	8	0	1	1	0	0
2	1	0	0	0	0	1
2	2	0	0	1	1	1
2	3	0	0	1	0	0
2	4	0	0	1	0	0
2	5	0	0	1	0	0
2	6	0	0	1	0	0

2	8	0	1	1	0	0
3	1	0	0	0	0	0
3	3	0	1	0	0	0
3	4	0	1	0	0	0
3	5	0	0	1	0	0
3	6	0	0	1	0	0
3	7	0	1	0	0	1
3	8	0	1	1	0	0

tblClassRelationTypes

ClassRelationTypeID	ClassID	RelatedClassID	RelationIsSearchable
1	3	2	1
2	3	3	1

tblClassRelationTypesMlg

ClassRelationTypeID	LanguagelD	UIName	UIDescription
1	1	RelatedCert	Null
1	2	Σχετικό Πιστοποιητικό	Null
2	1	RelatedStamp	Null
2	2	Σχετική Χρονοσφαγίδα	null

tblTreePermissions

RoleID	ClassID	MethodID	StatusID	OverrideLoginID
1	1	1	1	0
1	1	2	1	0
1	1	3	1	0
1	1	3	2	0
1	1	4	1	0
1	1	4	2	0
2	1	1	1	0

1	2	1	1	1
1	2	2	1	1
1	2	3	1	1
1	2	3	2	1
1	2	4	1	1
1	2	4	2	1
2	2	1	1	0
2	2	4	1	0
1	3	1	1	1
1	3	2	1	1
1	3	3	1	1
1	3	3	2	1
1	3	4	1	1
1	3	4	2	1
2	3	1	1	0
2	3	2	1	0
2	3	4	1	0

tblEditPermissions

RoleID	MethodID	ClassID	StatusID
1	3	1	1
1	3	1	2
1	4	1	1
1	4	1	2
1	2	2	1
1	3	2	1
1	3	2	2
2	2	2	1
2	4	2	1
1	2	3	1
1	3	3	1
1	3	3	2

1	4	3	1
2	2	3	1
2	4	3	1

Με την περιγραφή και αυτού του πίνακα, έχουμε ολοκληρώσει και την περιγραφή των δυνατοτήτων της Εφαρμογής των Μεταδεδομένων. Σε αυτή ορίζουμε νέες οντότητες – κλάσεις, αντιστοιχίζουμε σε αυτές νέες ή δηλωμένες ιδιότητες και καθορίζουμε το είδος των προσβάσεων στις συγκεκριμένες οντότητες. Επομένως, με τη διαδικασία αυτή μπορούμε να παρουσιάζουμε και τις οθόνες των διεπαφών των δρώντων φυσικών οντοτήτων μέσα από ένα μηχανισμό παραγωγής HTML elements που καθορίζονται από το αναφερόμενο μοντέλο παραγωγής της Εφαρμογής των Μεταδεδομένων. Για παράδειγμα μια οθόνη αίτησης Χρονοσήμανσης θα πρέπει να περιλαμβάνει ένα αναφερόμενο Ψηφιακό Πιστοποιητικό με τις δηλωμένες παραπάνω ιδιότητές του, ενώ πρόσβαση σε αυτό μπορούν να έχουν οι Ρόλοι “PKI Manager” και “PKI User” με συγκεκριμένες μεθόδους σε συγκεκριμένες καταστάσεις. Οι παραγόμενες «Χρονοσφαγίδες» αποθηκεύονται στους Πίνακες των Δεδομένων σαν στιγμιότυπα των δηλωμένων κλάσεων. Πρίν προχωρήσουμε στην καταγαφή των στιγμιοτύπων θα αναφερθούμε στους περιφερειακούς πίνακες της Εφαρμογής των Δεδομένων για την καλύτερη κατανόηση. Έτσι έχουμε :

tblLogins

LoginID	FirstName	LastName	Pwd	Email	PrivateKey
1	Nikos	Rentas	****	rentas@aueb.gr	SQDFSD23442355333.....
2		AUEB	****	aueb@aueb.gr	SDFGFD2454566003.....
3	Dimitris	Lekkas	****	dlek@aegean.gr	77373JDIDPSSDFSDLSD..

tblGroups

GroupID	Name	Description
1	Χρήστες ΥΔΚ	Ανήκουν οι χρήστες που αιτούνται υπηρεσιών Προστιθέμενης Αξίας από τον Οργανισμό.
2	Administrators	Ανήκουν οι βασικοί διαχειριστικοί ρόλοι του Οργανισμού

tblGroupLoginRelations

GroupID	LoginID
1	1
1	3
2	2

Τα στιγμιότυπα των παραγόμενων χρονοσφαγίδων εμφανίζονται στον πίνακα tblPublicItems ενώ οι περιφερειακοί tblPublicDataTypeXXX είναι υπεύθυνοι για την παροχή των στοιχείων των ιδιοτήτων των δηλωμένων κλάσεων. Οι πίνακες AccessOnPublicitems και AccessOnPublicitemsByGroups αποθηκεύουν το είδος των προσβάσεων πάνω στα συγκεκριμένα στιγμιότυπα. Έτσι έχουμε:

tblPublicItems

Public ItemID	Parent ItemID	Title	Access status	Class ID	Status ID	Login ID	Hierarchy Path	Hierarchy Level
1	Null	Root	1	1	1	null	_1_	1
2	1	Cert1	2	2	1	1	_1_2_	2
3	1	Cert2	2	2	1	2	_1_3	2
4	1	Timestamp1	3	3	1	Null	_1_4	2
5	1	Timestamp2	3	3	1	Null	_1_5	2
6	4	Timestamp3	3	3	1	Null	_1_4 _6_	3
7	6	Timestamp4	3	3	1	1	_1_4 _6_7	4

Για χάρη της αναφοράς στα ουσιαστικά χαρακτηριστικά των στιγμιοτύπων δε θα αναφερθούμε αναλυτικά στους πίνακες tblPublicDataTypeXXX αλλά σε ένα μόνο στιγμότυπο του πίνακα tblPublicDataTypeDateTime για μια ενδεικτική προσέγγιση.

tblPublicDataTypeDateTime

PublicItemID	PropertyID	Data
3	3	1/12/2003
3	4	31/12/2003

Ιδιαίτερα σημαντικός είναι και ο πίνακας που κρατά τις συσχετίσεις των στιγμότυπων. Στο αναφερόμενο παράδειγμα μια απεικόνιση των στοιχείων του πίνακα είναι:

tblPublicToPublicRelations

PublicItemID	RelatedPublicItemID	ClassRelationTypeID
4	2	1
4	3	1
5	2	1
5	3	1
6	2	1
7	3	1

Τέλος, ο καθορισμός των προσβάσεων θα έχει την παρακάτω μορφή:

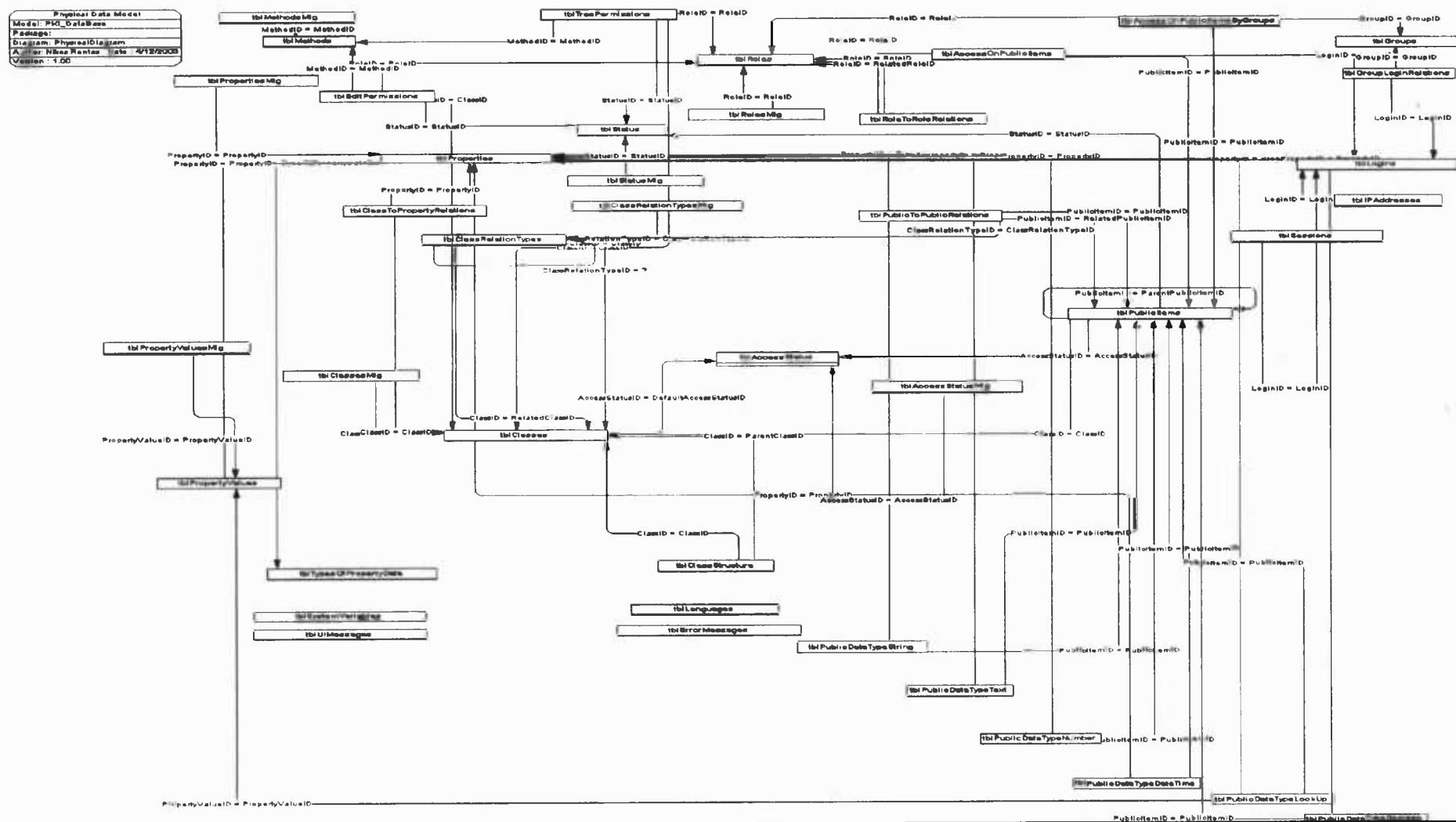
tblAccessOnPublicItemsByGroups

PublicItemID	GroupID	RoleID	Enabled From Date	Enabled To Date	Enabled Status
1	1	1	Null	Null	1
1	2	2	Null	Null	1

tblAccessOnPublicItems

PublicItemID	LoginID	RoleID	Enabled From Date	Enabled To Date	Enabled Status
7	1	1	1/12/2003	31/12/2003	1
4	3	1	1/12/2003	2/12/2003	1

Συνεπώς ο καθορισμός των προσβάσεων σε στιγμιότυπα των δηλωμένων οντοτήτων γίνεται μέσα από την Εφαρμογή των Δεδομένων και είναι σε άμεση συνάρτηση της κλάσης του στιγμιότυπου, του ρόλου της φυσικής οντότητας και των δυνατοτήτων του συγκεκριμένου ρόλου της Εφαρμογής πάνω στον τύπο της κλάσης. Με αυτή τη διαδικασία υπάρχει πλήρης διαφάνεια και καθορίζεται σαφώς η πρόσβαση πάνω σε συγκεκριμένα στιγμιότυπα.



Σχήμα 5.5 Περιγραφή του σχήματος της Βάσης Δεδομένων

5.3 Τεχνολογικές Προτάσεις Υλοποίησης

Για την υλοποίηση της αναφερόμενης αρχιτεκτονικής προτείνονται μια σειρά από πρότυπα και υπάρχουσες εφαρμογές που τυγχάνουν ευρείας αποδοχής από το σύνολο των χρηστών και των επιστημόνων, υποστηρίζουν τα ανοικτά δίκτυα και έχουν ένα βαθμό αυτονομίας κάτι το οποίο αυξάνει το βαθμό της ευελιξίας και της κλιμάκωσης της προτεινόμενης υλοποίησης. Στον παρακάτω πίνακα [Πίνακας 5.2] αναφέρονται οι βασικές λειτουργικές περιοχές του Οργανισμού που σχετίζονται με την προτεινόμενη αρχιτεκτονική και οι αντίστοιχες τεχνολογίες ή πρότυπα που τις υλοποιούν και μπορεί να επιλέξει ένας Οργανισμός για την παροχή Υπηρεσιών Προστιθέμενης Αξίας σε μια Υποδομή Δημόσιου Κλειδιού.

Περιοχή	Τεχνολογίες
Πρόσβαση χρήστη ή μέλους του Οργανισμού	HTTP over SSL S/MIME SSH Εφαρμογή Μεταδεδομένων Εφαρμογή Δεδομένων
Ενδιάμεσο Επίπεδο (middleware)	COM ή COM+ XML Web Services CORBA
Μορφοποίηση Εισόδων – Εξόδων	XML Schema / XML
Επικοινωνία Ενδιάμεσου Επιπέδου με Βάση Δεδομένων	XMLHTTP SOAP COM ή COM+
Βάση Δεδομένων	Μια Σχεσιακή Βάση Δεδομένων
Ψηφιακά Πιστοποιητικά	X.509
Κρυπτογραφικές Λειτουργίες	Microsoft CryptoAPI RSA Cryptoki
Χρονοσήμανση	PKITS TIMESEC
Συμβολαιογραφία	IETF-Notary
Διαχείριση Δικαιωμάτων	X.812

		X.509 Role based proposed RDBMS
Αποδεικτικά τεκμήρια		ISO/IEC DIS 10181-4
Περιαγωγή		SPEKE EKE Smart Cards (Secure portable devices) Virtual Software Tokens
Βιομετρικές Αυθεντικοποίησης	Μέθοδοι	Smart Cards ANSI X9.84 SSL
Ανωνυμία		Zhang Protocol TLS SDSI PEM

Πίνακας 5.2 Αντιστοίχηση Προτύπων και Υπηρεσιών

5.4 Συμπεράσματα

Στόχος στο συγκεκριμένο κεφάλαιο είναι η παρουσίαση μιας λογικής και ανοικτής αρχιτεκτονικής για την παροχή Υπηρεσιών Προστιθέμενης Αξίας από έναν Οργανισμό. Προς αυτή την κατεύθυνση προτείνεται ένα μοντέλο αναφοράς που χαρακτηρίζεται από ευελιξία, επεκτασιμότητα, κλιμάκωση και προτυποποίηση. Η προτεινόμενη αρχιτεκτονική αναλύεται σε επιμέρους μονάδες και αναλύεται ο τρόπος διασύνδεσής τους. Προτείνεται μάλιστα μια ανοικτή αρχιτεκτονική που υποστηρίζεται από όλες τις υψηλού επιπέδου σημερινές τεχνολογίες ενώ η πρόταση για την υποστηριζόμενη Βάση Δεδομένων είναι αρκετά αφαιρετική και ενδιαφέρουσα, διαφορετική από τις μέχρι τώρα υλοποιήσεις, επεκτάσιμη και ικανή να υποστηρίξει κάθε διαφορετικά παραγόμενο μοντέλο ενός Οργανισμού όταν μάλιστα γνωρίζουμε πως κανένας Οργανισμός δεν είναι ίδιος με κανέναν άλλον.

Κεφάλαιο 6 Επίλογος

6.1 Σύνοψη και Συμπεράσματα

Η ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών στις τελευταίες δεκαετίες έχει δημιουργήσει την ανάγκη για την παροχή υπηρεσιών Προστιθέμενης Αξίας από τη μεριά των Οργανισμών - παρόχων προς τους τελικούς χρήστες. Κεντρική έννοια στην παροχή αυτών των υπηρεσιών αποτελεί η Ασφάλεια των Πληροφοριών και η ανάπτυξη Ασφαλών Πληροφοριακών Συστημάτων. Σημαντικό ρόλο στη διασφάλιση της Ασφάλειας των Πληροφοριών διαδραματίζουν οι Υποδομές Δημόσιου Κλειδιού που αξιοποιούν την τεχνολογία των ψηφιακών πιστοποιητικών και των ψηφιακών υπογραφών.

Τα κύρια σημεία και συμπεράσματα της παρούσας Διπλωματικής Εργασίας συνοψίζονται στα :

- Γίνεται μια σύντομη ανασκόπηση των ιδιοτήτων της Ασφάλειας των Πληροφοριακών Συστημάτων και των βασικών χαρακτηριστικών της Υποδομής Δημόσιου Κλειδιού στο οργανωτικό πλαίσιο της οποίας δραστηριοποιείται ο Οργανισμός – πάροχος.
- Εξετάζονται οι περιβαλλοντικοί παράγοντες που επηρεάζουν τη λειτουργία του Οργανισμού μέσα σε μια τέτοια υποδομή. Ιδιαίτερη σημασία δίνεται στα νομοθετικά πλαίσια, στην προσπάθεια σύγκλισής τους, στον ιδιαίτερο ρόλο της εμπιστοσύνης και της προστασίας της ιδιωτικότητας στο υπάρχον πληροφοριακό περιβάλλον. Επίσης, καταγράφονται τα αναγνωρισμένα πρότυπα και τεχνολογίες που επηρεάζουν και κατευθύνουν τις παρεχόμενες υπηρεσίες από έναν Οργανισμό.
- Σημαντικό μέρος της παρούσας Διπλωματικής Εργασίας καταλαμβάνει η αναλυτική μελέτη και η περιγραφή των υπηρεσιών Προστιθέμενης Αξίας με τη χρήση της XML Schema έτσι ώστε να μπορούν να ενσωματωθούν σε μια γενική αρχιτεκτονική στα πλαίσια λειτουργίας της υπάρχουσας Υποδομής Δημόσιου Κλειδιού. Παράλληλα καταγράφονται οι διάφορες υλοποιήσεις και προτάσεις για την παροχή μιας ολοκληρωμένης άποψης πάνω στο συγκεκριμένο ζήτημα.
- Προτείνεται η υλοποίηση μιας αφαιρετικής αρχιτεκτονικής για την ενσωμάτωση των υπηρεσιών αυτών και η ανάπτυξη μιας αφαιρετικής Βάσης Υπηρεσίες πιστοποίησης Προστιθέμενης Αξίας σε ΥΔΚ

Δεδομένων για την υποστήριξη όλων των υπηρεσιών του Οργανισμού με γνώμονα την παροχή δυνατοτήτων ευελιξίας και επεκτασιμότητας.

6.2 Ανοικτά Θέματα

Για την παρουσίαση του συγκεκριμένου επιστημονικού πεδίου κατεβλήθη σημαντική προσπάθεια για την παροχή μιας ολοκληρωμένης και άρτιας μελέτης. Ωστόσο για κάποια από τα θέματα με τα οποία ασχοληθήκαμε η παρούσα βιβλιογραφία και οι προτεινόμενες λύσεις δεν είναι επαρκείς είτε γιατί δεν έχουν μελετηθεί διεξοδικά ή υπάρχουν πολλές διαφορετικές και αντικρουόμενες απόψεις για τις οποίες απαιτείται περισσότερη έρευνα και μελέτη. Τα ανοικτά θέματα που ανακύπτουν συνοψίζονται στα :

- Οι περισσότερες από τις προτάσεις για την παροχή της Ανωνυμίας δεν πείθουν για την προστασία των συναλλασσόμενων μερών. Κάθε λύση έχει τα πλεονεκτήματα και τα μειονεκτήματά της.
- Απαιτείται μεγαλύτερη ολοκλήρωση των υπαρχόντων τεχνολογικών προτύπων και υλοποιήσεων για τη δυνατότητα διαλειτουργικότητας των Οργανισμών.
- Είναι επιτακτική η ανάγκη για τη σύγκλιση των διαφορετικών νομοθετικών πλαισίων που εφαρμόζονται σε διαφορετικές χώρες ή και ακόμα διαφορετικές πολιτείες για να κατευθυνθούμε σε μια παγκόσμια Κοινωνία της Πληροφορίας και σε μεγαλύτερη ανάπτυξη της ανάγκης για χρήση των Υποδομών Δημόσιου Κλειδιού.
- Η αυξανόμενη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών θα οδηγήσει στη δημιουργία και νέων υπηρεσιών Προστιθέμενης Αξίας και επομένως αυτές πρέπει να ενσωματωθούν μέσα στις υπάρχουσες υποδομές με όσο το δυνατόν πιο «ανάδυνο» τρόπο (να μην επαναπροσδιοριστεί δηλαδή η λειτουργία των Οργανισμών - παρόχων).

Παράρτημα

Ευρετήριο Σχημάτων και Πινάκων

Σχήμα 1.1 Εννοιολογικό πλαίσιο	14
Σχήμα 2.1 Μοντέλο αναπαράστασης Πληροφοριακού Συστήματος	17
Σχήμα 3.1 Μοντέλο Αναφοράς ΥΔΚ	29
Σχήμα 3.2 Επίπεδα αφαίρεσης και εξαρτήσεις	31
Σχήμα 3.3 Ταξινόμηση των υπηρεσιών.....	33
Πίνακας 3.1 RSA Πρότυπα.....	38
Σχήμα 4.1 Μοντέλο αναφοράς παροχής υπηρεσίας Περιαγωγής.....	99
Σχήμα 4.2 Διαδικασία Βιομετρικής Αυθεντικοποίησης.....	103
Σχήμα 5.1 Μοντέλο Αναφοράς	122
Σχήμα 5.2 Προσδιορισμός Λειτουργικών Μονάδων	125
Σχήμα 5.3 Αρχιτεκτονική Τριών Επιπέδων	126
Σχήμα 5.4 Προτεινόμενη Υλοποίηση.....	129
Πίνακας 5.1 Ανάλυση των πινάκων της Βάσης Δεδομένων	135
Σχήμα 5.5 Περιγραφή του σχήματος της Βάσης Δεδομένων	147
Πίνακα 5.2 Αντιστοίχηση Προτύπων και Υπηρεσιών	149

Περιγραφή της Βάσης Δεδομένων με τη χρήση του XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema name="PKI_DataBase.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<xsd:element name="tblPublicItems">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="ParentPublicItemID" type="NO"/>
    <xsd:element name="Title" type="xsd:string"/>
    <xsd:element name="AccessStatusID" type="xsd:double"/>
    <xsd:element name="ClassID" type="xsd:double"/>
    <xsd:element name="StatusID" type="xsd:double"/>
    <xsd:element name="LoginID" type="xsd:double"/>
    <xsd:element name="HierarchyPath" type="xsd:string"/>
    <xsd:element name="HierarchyLevel" type="xsd:short"/>
</xsd:element>
<xsd:element name="tblAccessStatus">
    <xsd:element name="AccessStatusID" type="NO"/>
</xsd:element>
<xsd:element name="tblStatus">
    <xsd:element name="StatusID" type="NO"/>
</xsd:element>
<xsd:element name="tblLanguages">
    <xsd:element name="LanguageID" type="xsd:string"/>
    <xsd:element name="UISortingNumber" type="xsd:short"/>
    <xsd:element name="UIName" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPublicToPublicRelations">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="RelatedPublicItemID" type="NO"/>
    <xsd:element name="ClassRelationTypeID" type="NO"/>
</xsd:element>
<xsd:element name="tblClasses">
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="DefaultAccessStatusID" type="NO"/>
```

```

<xsd:element name="ClassPrefixName" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblTreePermissions">
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="MethodID" type="NO"/>
    <xsd:element name="StatusID" type="NO"/>
    <xsd:element name="OverrideLoginID" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblRoles">
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="RoleIsManager" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblMethods">
    <xsd:element name="MethodID" type="NO"/>
</xsd:element>
<xsd:element name="tblProperties">
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="TypeOfPropertyDataID" type="NO"/>
    <xsd:element name="UISize" type="xsd:double"/>
    <xsd:element name="UIMaxLength" type="xsd:double"/>
    <xsd:element name="VarName" type="xsd:string"/>
    <xsd:element name="VarMinValue" type="xsd:string"/>
    <xsd:element name="VarMaxValue" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPropertyValue">
    <xsd:element name="PropertyValueID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeString">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="Data" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeText">
    <xsd:element name="PublicItemID" type="NO"/>

```

```

<xsd:element name="PropertyID" type="NO"/>
<xsd:element name="Data" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeNumber">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="Data" type="xsd:float"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeDateTime">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="Data" type="xsd:date"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeLookUp">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="PropertyValueID" type="NO"/>
</xsd:element>
<xsd:element name="tblLogins">
    <xsd:element name="LoginID" type="NO"/>
    <xsd:element name="FirstName" type="xsd:string"/>
    <xsd:element name="LastName" type="xsd:string"/>
    <xsd:element name="LoginName" type="xsd:string"/>
    <xsd:element name="Password" type="xsd:string"/>
    <xsd:element name="Email" type="xsd:string"/>
    <xsd:element name="Birthday" type="xsd:date"/>
    <xsd:element name="PhoneNumber" type="xsd:string"/>
    <xsd:element name="MobileNumber" type="xsd:string"/>
    <xsd:element name="CitizenID" type="xsd:string"/>
    <xsd:element name="PrivateKey" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblAccessOnPublicItems">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="LoginID" type="NO"/>
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="EnabledFromDate" type="xsd:date"/>

```

```

<xsd:element name="EnabledToDate" type="xsd:date"/>
<xsd:element name="EnabledStatus" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblSystemVariables">
    <xsd:element name="SystemVariableID" type="xsd:string"/>
    <xsd:element name="SystemVariableValue" type="xsd:string"/>
    <xsd:element name="HelpText" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblEditPermissions">
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="MethodID" type="NO"/>
    <xsd:element name="StatusID" type="NO"/>
    <xsd:element name="StatusIsDefault" type="xsd:short"/>
</xsd:element>
<xsd:element name="tblIPAddresses">
    <xsd:element name="IPAddressID" type="NO"/>
    <xsd:element name="LoginID" type="NO"/>
    <xsd:element name="IPAddressA" type="xsd:short"/>
    <xsd:element name="IPAddressB" type="xsd:short"/>
    <xsd:element name="IPAddressC" type="xsd:short"/>
    <xsd:element name="IPAddressD" type="xsd:short"/>
</xsd:element>
<xsd:element name="tblSessions">
    <xsd:element name="LoginID" type="NO"/>
    <xsd:element name="CookieID" type="xsd:string"/>
    <xsd:element name="IPAddress" type="xsd:string"/>
    <xsd:element name="ExpiresAtDateTime" type="xsd:date"/>
    <xsd:element name="SessionData" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblUIMessages">
    <xsd:element name="UIMessageID" type="xsd:string"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIMessageValue" type="xsd:string"/>
    <xsd:element name="UIMessageDescription" type="xsd:string"/>
</xsd:element>

```

```

<xsd:element name="tblErrorMessages">
    <xsd:element name="ErrorMessageID" type="xsd:double"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="ErrorMessageValue" type="xsd:string"/>
    <xsd:element name="ErrorMessageDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblTypesOfPropertyData">
    <xsd:element name="TypeOfPropertyDataID" type="xsd:double"/>
    <xsd:element name="UIName" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblAccessOnPublicItemsByGroups">
    <xsd:element name="PublicItemID" type="NO"/>
    <xsd:element name="LoginID" type="NO"/>
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="EnabledFromDate" type="xsd:date"/>
    <xsd:element name="EnabledToDate" type="xsd:date"/>
    <xsd:element name="EnabledStatus" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblGroups">
    <xsd:element name="GroupID" type="NO"/>
    <xsd:element name="Name" type="xsd:string"/>
    <xsd:element name="Description" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPropertiesMlg">
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UILabel" type="xsd:string"/>
    <xsd:element name="VarDefaultValue" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblClassesMlg">
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIName" type="xsd:string"/>
    <xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblRolesMlg">

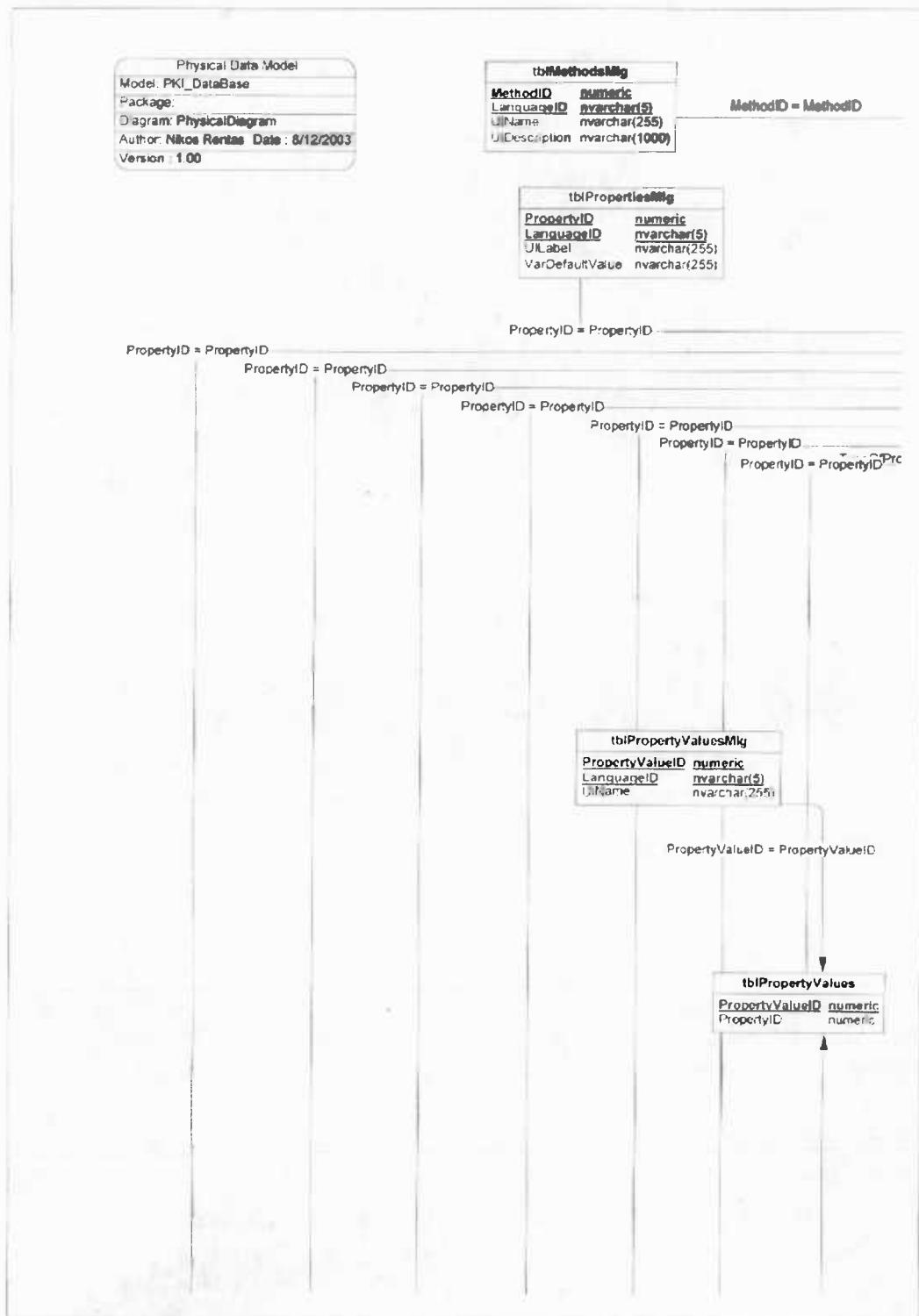
```



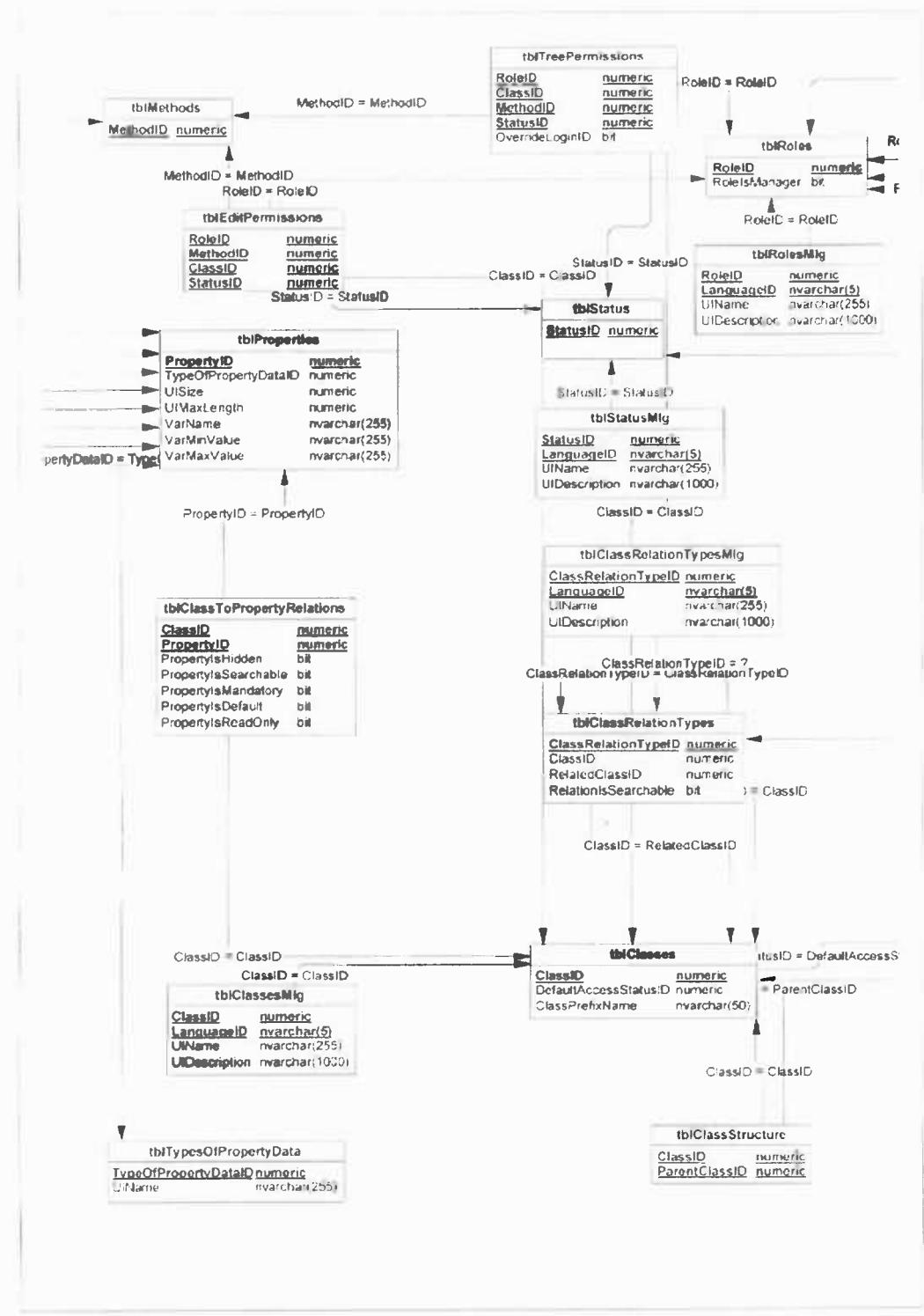
```
<xsd:element name="RoleID" type="NO"/>
<xsd:element name="LanguageID" type="NO"/>
<xsd:element name="UIName" type="xsd:string"/>
<xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblMethodsMlg">
    <xsd:element name="MethodID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIName" type="xsd:string"/>
    <xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblStatusMlg">
    <xsd:element name="StatusID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIName" type="xsd:string"/>
    <xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblClassRelationTypes">
    <xsd:element name="ClassRelationTypeID" type="NO"/>
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="ClassRelationTypeID" type="NO"/>
    <xsd:element name="RelationIsSearchable" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblAccessStatusMlg">
    <xsd:element name="AccessStatusID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIName" type="xsd:string"/>
    <xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblClassRelationTypesMlg">
    <xsd:element name="ClassRelationTypeID" type="NO"/>
    <xsd:element name="LanguageID" type="NO"/>
    <xsd:element name="UIName" type="xsd:string"/>
    <xsd:element name="UIDescription" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblPublicDataTypeBoolean">
```

```
<xsd:element name="PublicItemID" type="NO"/>
<xsd:element name="PropertyID" type="NO"/>
<xsd:element name="Data" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblPropertyValuesMlg">
    <xsd:element name="PropertyValueID" type="NO"/>
    <xsd:element name="LanguageID" type="xsd:string"/>
    <xsd:element name="UIName" type="xsd:string"/>
</xsd:element>
<xsd:element name="tblClassToPropertyRelations">
    <xsd:element name="ClassID" type="NO"/>
    <xsd:element name="PropertyID" type="NO"/>
    <xsd:element name="PropertyIsHidden" type="xsd:boolean"/>
    <xsd:element name="PropertyIsSearchable" type="xsd:boolean"/>
    <xsd:element name="PropertyIsMandatory" type="xsd:boolean"/>
    <xsd:element name="PropertyIsDefault" type="xsd:boolean"/>
    <xsd:element name="PropertyIsReadOnly" type="xsd:boolean"/>
</xsd:element>
<xsd:element name="tblRoleToRoleRelations">
    <xsd:element name="RoleID" type="NO"/>
    <xsd:element name="RelatedRoleID" type="NO"/>
    <xsd:element name="ManageAttributes" type="xsd:short"/>
    <xsd:element name="ManageAccess" type="xsd:short"/>
</xsd:element>
```

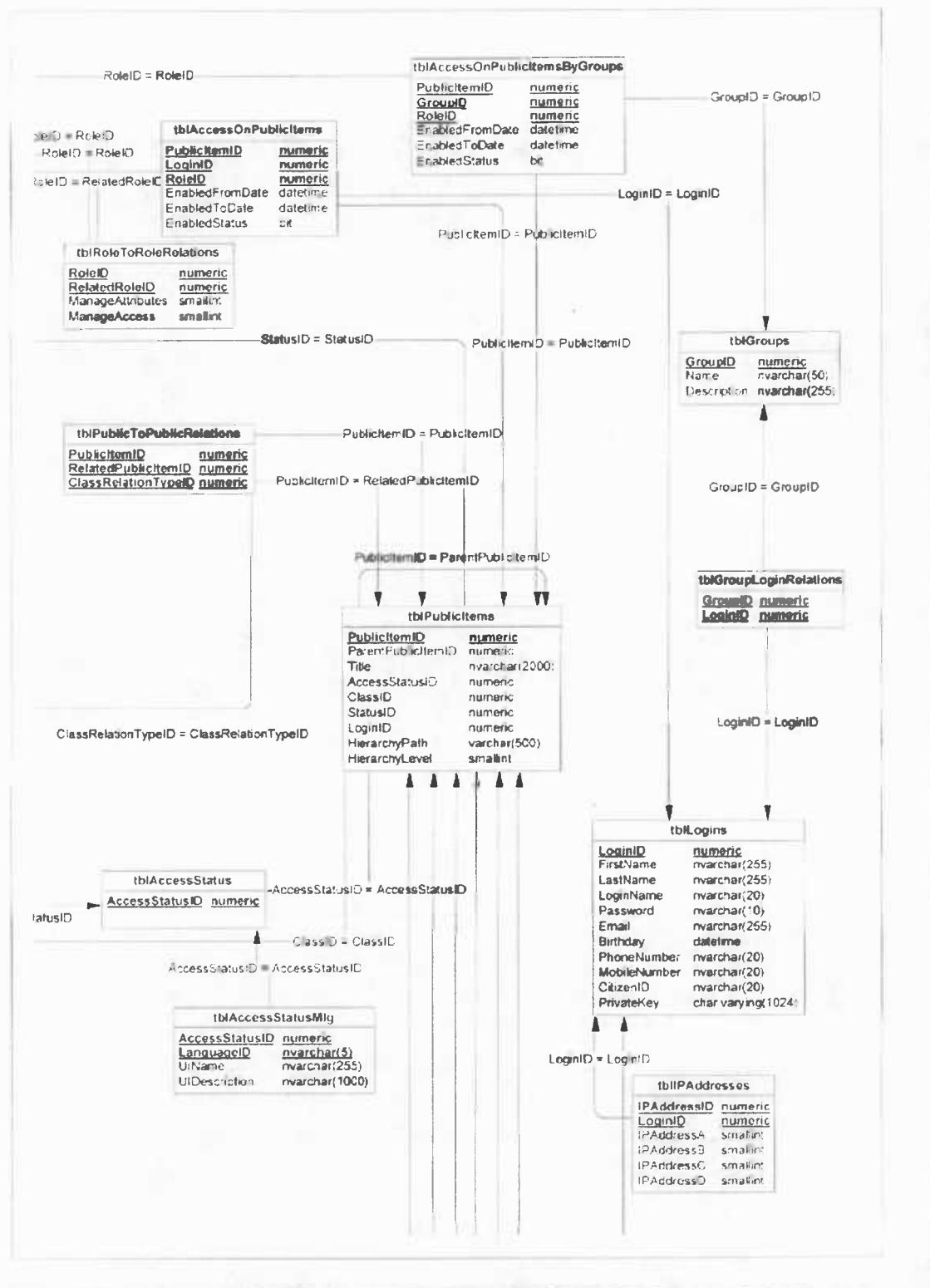
Παρουσίαση σχήματος της προτεινόμενης Βάσης Δεδομένων

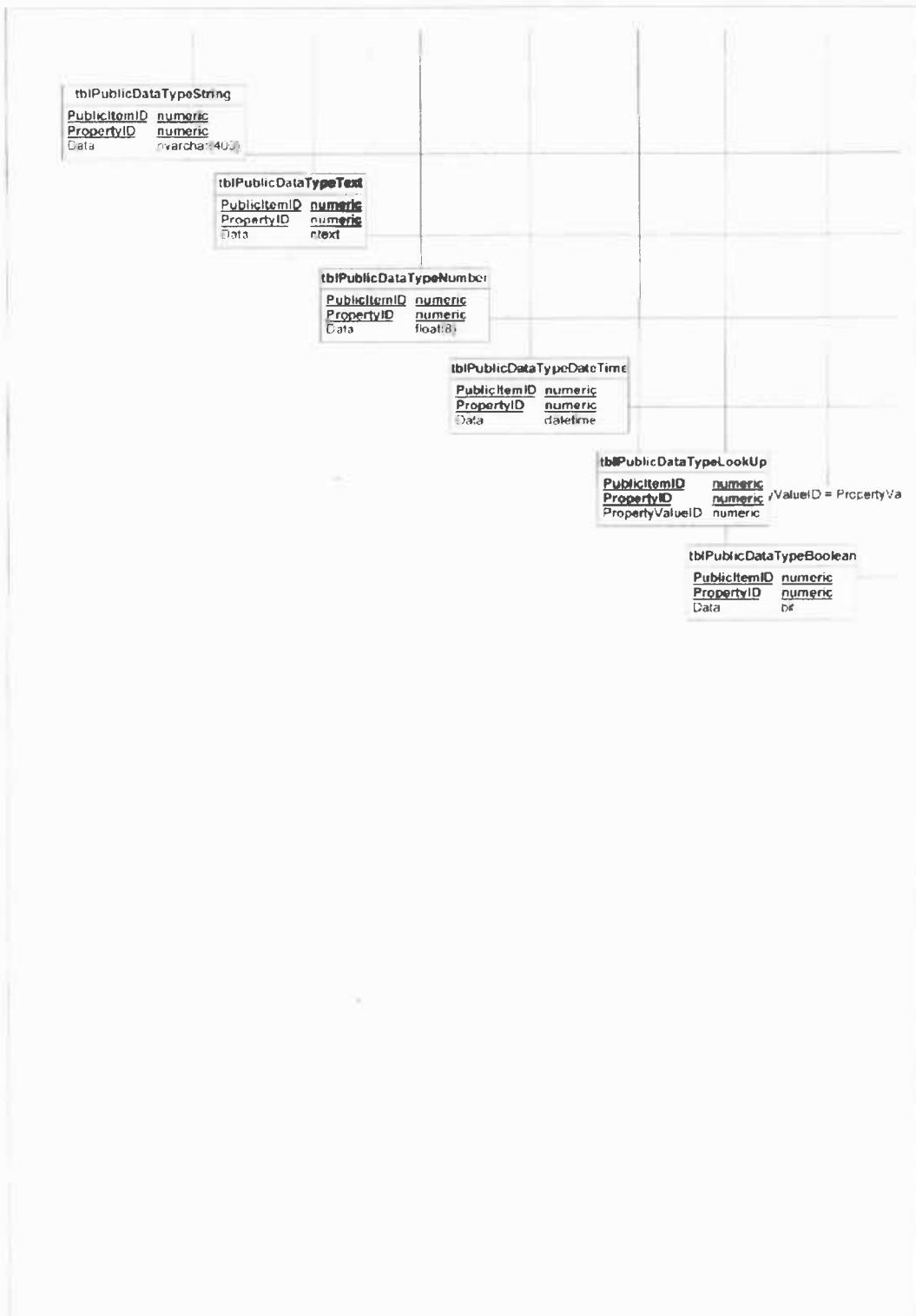


Σελίδα 1 από 6



Σελίδα 2 από 6



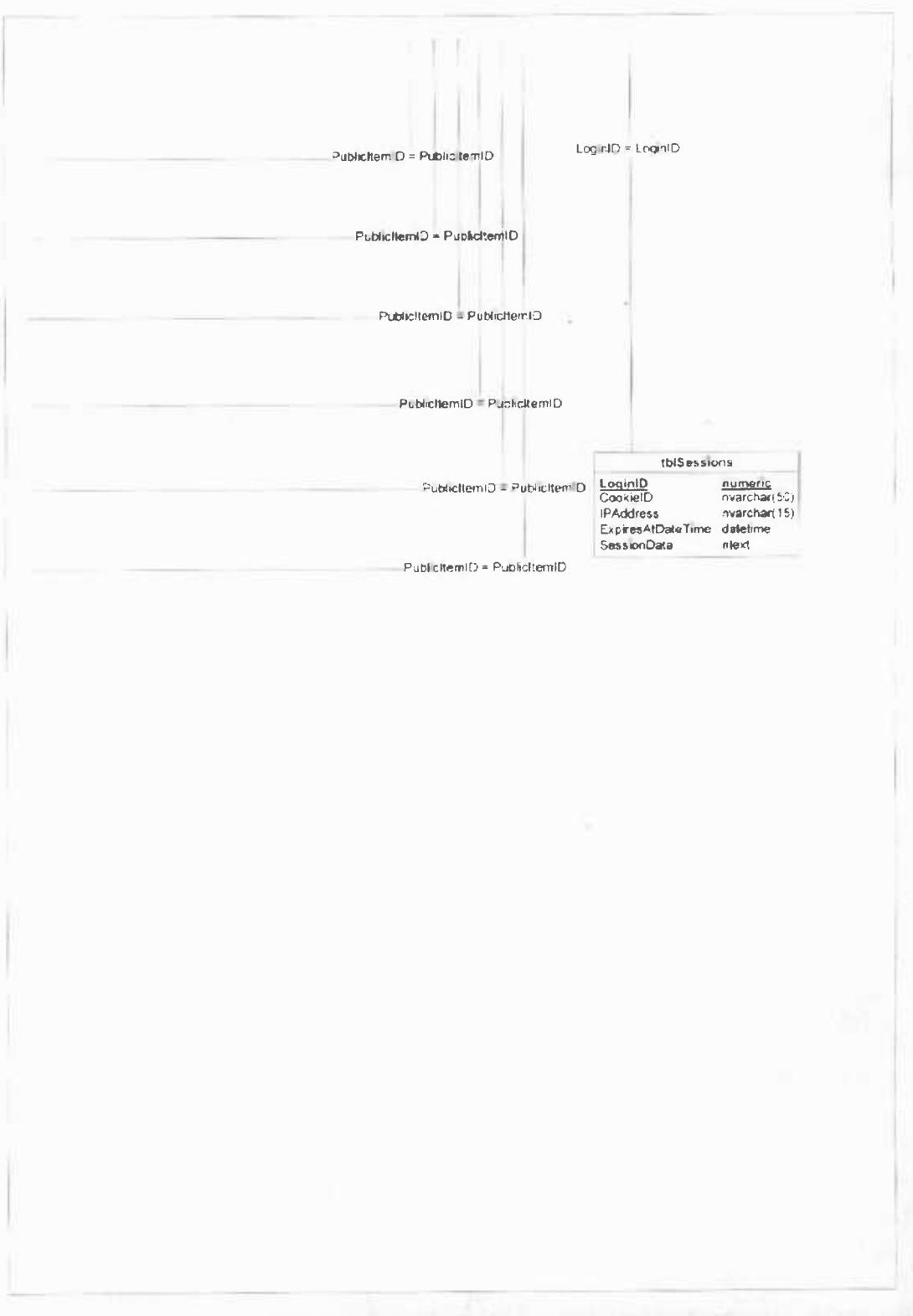


Σελίδα 4 από 6

lueG

tblSystemVariables		tblLanguages	
SystemVariableID	nvarchar(50)	LanguageID	nvarchar(5)
SystemVariableValue	nvarchar(1000)	UISortingNumber	smallint
HelpText	nvarchar(1000)	UIName	nvarchar(255)
tblUIMessages		tblErrorMessages	
UIMessageID	nvarchar(30)	ErrorMessageID	numeric
LanguageID	nvarchar(5)	LanguageID	nvarchar(5)
UIMessageValue	nvarchar(1000)	ErrorMessageValue	nvarchar(1000)
UIMessageDescription	nvarchar(255)	ErrorMessageDescription	nvarchar(255)

Σελίδα 5 από 6



Σελίδα 6 από 6

