ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ανάλυση και μελέτη της ασφάλειας των Πληροφοριακών Συστημάτων Ηλεκτρονικής Διακυβέρνησης

Πρόγραμμα Μεταπτυχιακών Σπουδών

Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων

ΣΑΛΑΓΙΑΝΝΗΣ ΓΡΗΓΟΡΙΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

Δρ. ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΥΡΟΜΜΑΤΗΣ

Φεβρουάριος, 2024

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής καθώς και των μεταπτυχιακών σπουδών μου στο τμήμα Μηχανικών Πληροφορικής και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής θα ήθελα να ευχαριστήσω τους αρωγούς της προσπάθειας.

Αρχικά θα ήθελα να ευχαριστήσω την οικογένεια μου, για την ευκαιρία που μου έδωσε να σπουδάσω και την εμπιστοσύνη που έδειξε στο πρόσωπό μου, τους συμφοιτητές μου και τους φίλους μου που μοιραστήκαμε ατελείωτες ώρες διαβάσματος και τους καθηγητές μου για τις γνώσεις που μου μεταλαμπάδευσαν.

Θα μου επιτρέψετε να κάνω μια ιδιαίτερη αναφορά στον καθηγητή μου Κ. Κωνσταντίνο Μαυρομμάτη, που με τη βοήθεια του και την καθοδήγησή του με ενέπνευσε στη γρήγορη ολοκλήρωση των σπουδών μου.

Εξεταστική επιτροπή:

Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2024.04.25 09:49:06 +03'00'	Ioannis Voyiatzis Digitally signed by Ioannis Voyiatzis Date: 2024.05.06 09:54:00 +03'00'	Christos Troussas Digitally signed by Christos Troussas Date: 2024.04.25 15:27:52 +03'00'
Κωνσταντίνος Μαυρομμάτης	**Ιωάννης Βογιατζής**	**Χρήστος Τρούσσας**
Επιβλέπων Καθηγητής	**Καθηγητής**	**Επίκουρος Καθηγητής**

Ημερομηνία εξέτασης 10/04/2024

Περίληψη

Η Διακυβέρνηση μέσω της Ηλεκτρονικής Διακυβέρνησης συνδέεται άμεσα με τη μεταρρύθμιση και τον εκσυγχρονισμό της Δημόσιας Διοίκησης μέσω της χρήσης σύγχρονων τεχνολογιών και μεθοδολογιών. Ωστόσο, για να επιτύχει μια τέτοια μετάβαση, δεν είναι αρκετή η αυτοματοποίηση των υπαρχουσών διαδικασιών και η παροχή τους μέσω του Διαδικτύου. Είναι απαραίτητο για τη Δημόσια Διοίκηση να ιδρύσει και να διατηρήσει ένα επίπεδο προστασίας και ασφάλειας που δεν είναι μόνο αντίστοιχο με αυτό των υφιστάμενων υπηρεσιών, αλλά επίσης ικανό να διασφαλίσει ότι τα προσωπικά δεδομένα χρησιμοποιούνται με διαφάνεια και σύμφωνα με τους νόμους, λαμβάνοντας υπόψη το συμφέρον των πολιτών. Σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάλυση και μελέτη της ασφάλειας των Πληροφοριακών Συστημάτων Ηλεκτρονικής. Αρχικά, καταγράφονται οι βασικές αρχές, τα χαρακτηριστικά της Ηλεκτρονικής Διακυβέρνησης. Στη συνέχεια, γίνεται λεπτομερής ανάλυση των θεμάτων ταυτοποίησης και πρόσβασης, καθώς και των απαιτήσεων ασφάλειας και ιδιωτικότητας στα Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης. Επιπλέον, παρακαλώ σημειώστε ότι παρέχονται περιληπτικές πληροφορίες για τις πιθανές απειλές και τις επιπτώσεις τους, σχετικά με την απώλεια των απαιτήσεων που έχουν προαναφερθεί. Τέλος, προτείνονται προληπτικοί τρόποι αντιμετώπισης και μείωσης των ενδεχόμενων απειλών.

Abstract

E-Governance is directly linked to the reform and modernization of Public Administration, utilizing modern technologies and methodologies. However, for this transition to be successful, it is not sufficient to merely automate existing processes and provide them through the Internet. Public Administration must ensure a uniform level of protection and security, not only equivalent to that of existing services but also capable of guaranteeing transparent and lawful use of personal data, taking into account the interests of citizens. The purpose of this thesis is to analyze and study the security of Electronic Information Systems. Initially, the basic principles and characteristics of E-Governance are outlined. Subsequently, detailed reference is made to authentication and accessibility, as well as security and privacy requirements in E-Governance Information Systems. Potential threats and their possible impacts concerning the loss of previous requirements are summarized, and ways to address and minimize them are proposed.

Περιεχόμενα

Κεφάλαιο 1 Ηλεκτρονική Διακυβέρνηση

Η Ηλεκτρονική Διακυβέρνηση(ΗΔ) υπάρχει εδώ και πολλά χρόνια στον Δημόσιο τομέα, αλλά έγινε πιο αισθητή όταν δημιουργήθηκαν τα πρώτα πληροφοριακά συστήματα που ξεκίνησε η αλληλεπίδραση των χρηστών και του φορέα. Η Ηλεκτρονική διακυβέρνηση προσδιορίζει πως οι υπηρεσίες της Δημόσιας Διοίκησης κάνουν χρήση και εφαρμόζουν τις τεχνολογίες πληροφοριών και επικοινωνιών.

Οι υπηρεσίες της Ηλεκτρονικής Διακυβέρνησης έχουν έναν τελικό χρήστη. Αυτός μπορεί να είναι είτε ένας πολίτης είτε μια επιχείρηση είτε ένας άλλος φορέας του Δημοσίου. Ο τελικός χρήστης παραλαμβάνει ένα τελικό παραδοτέο, το οποίο πρέπει να είναι αυτοτελές με σκοπό να το χρησιμοποιήσει χωρίς να κάνει επιπλέον διαδικασία. Οι υπηρεσίες αυτές, παρέχονται από ένα πάροχο που είναι υπεύθυνος για την την παροχή και έχει και έναν ρυθμιστή που είναι ένας τομές της Δημόσιας Διοίκησης που είναι υπεύθυνο για το ρυθμιστικό πλαίσιο της υπηρεσίας.

Με τον όρο υπηρεσία θεωρούμε μια διαδικασία που θα φέρει ένα αποτέλεσμα σε έναν πολίτη ή σε μια επιχείρηση ή σε έναν τομέα του Δημοσίου. Για να ολοκληρωθεί αυτή η υπηρεσία και να θεωρηθεί επιτυχημένη θα πρέπει να εκτελεστούν όλες οι απαραίτητες διαδικασίες. Για να ξεκινήσει να εκτελείται μια υπηρεσία θα πρέπει να υπάρξουν οι αιτούντες που είναι και αποδέκτες του αποτελέσματος της υπηρεσίας. Δηλαδή, Οι πολίτες είναι οι αιτούντες και οι αποδέκτες του αποτελέσματος της υπηρεσίας που παρέχεται από τους τομείς της Δημόσιας Διοίκησης.

1.1 Ορισμός

Λόγω του γεγονότος ότι η Ηλεκτρονική Διακυβέρνηση αντιμετωπίζεται διαφορετικά ανά τον κόσμο, η επιβολή ενός ενιαίου και καθολικού ορισμού αποτελεί πρόκληση. Ορισμένες προσεγγίσεις της Ηλεκτρονικής Διακυβέρνησης επικεντρώνονται στη χρήση και την εφαρμογή των Τεχνολογιών Πληροφοριών και Επικοινωνιών, ενώ άλλες αναδεικνύουν την ευρύτερη διάσταση της μετασχηματιστικής διαδικασίας στον κλασικό τομέα της διοίκησης.

Σύμφωνα με τα Ηνωμένα Έθνη, η Ηλεκτρονική Διακυβέρνηση αναφέρεται στη χρήση του Διαδικτύου και του Παγκόσμιου Ιστού με σκοπό την παροχή ηλεκτρονικών πληροφοριών και υπηρεσιών προς τους πολίτες. Από την άλλη πλευρά, σύμφωνα με το Ευρωπαϊκό Παρατηρητήριο για την Τεχνολογία Πληροφοριών, η Ηλεκτρονική Διακυβέρνηση εστιάζεται στη χρήση των τεχνολογιών Διαδικτύου για τη διευκόλυνση, ενίσχυση και υποστήριξη των σχέσεων μεταξύ των κυβερνητικών φορέων, των πολιτών και των επιχειρήσεων.

Εξίσου σημαντικό, σύμφωνα με την Ευρωπαϊκή Επιτροπή, η Ηλεκτρονική διακυβέρνηση ταυτόχρονα με την εκπαίδευση του προσωπικού σε θέματα οργάνωσης, διοίκησης αλλά και την εξέλιξη των δεξιοτήτων τους μπορεί να οδηγήσει στην αποδοτικότερη και γρηγορότερη εξυπηρέτηση των πολιτών, καθώς επίσης να εδραιώσει την δημοκρατία. Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), η κυβέρνηση χρησιμοποιεί εφαρμογές του Διαδικτύου και διαδικασίες που εμπεριέχουν νέες τεχνολογίες καθώς επίσης ταυτόχρονα με την αυξανόμενη πρόσβαση στην πληροφορία του κράτους έχουν σαν αποτέλεσμα την πιο αποτελεσματική ποιότητα των υπηρεσιών του κράτους. Συνολικά, οι παραπάνω προσεγγίσεις εστιάζουν στον μετασχηματισμό των διαδικασιών, την αξιοποίηση των Τεχνολογιών Πληροφοριών και Επικοινωνιών στη Δημόσια Διοίκηση και την παροχή υπηρεσιών χρησιμοποιώντας το Διαδίκτυο.

1.2 Βασικές Αρχές Ανάπτυξης και Αναγκαία Χαρακτηριστικά Υπηρεσιών

Για την υλοποίηση ενός περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης, είναι αναγκαία η συμμετοχή κυβέρνησης στον βασικό σχεδιασμό. Πιο αναλυτικά θα πρέπει, να συμμετέχει ενεργά στην στρατηγική οργάνωση του περιβάλλοντος καθώς επίσης και να δεσμεύεται για την υλοποίηση των στόχων που θέτονται. Επιπλέον, θα πρέπει η κυβέρνηση να εξετάζει και να υλοποιεί τυχόν αλλαγές που προκύπτουν κατά τον σχεδιασμό με αποτελεσματικό τρόπο εξασφαλίζοντας επαρκής χρηματοδότηση. Ακόμη, θα πρέπει η κυβέρνηση από την μεριά της να καλλιεργεί και να αναπτύσσει την «φιλοσοφία» στο Δημόσιο Τομέα, να προγραμματίσει δράσεις και εκπαιδεύσεις, να δημιουργήσει πλαίσιο νομικό, να παρακολουθεί και να αξιολογεί την πορεία του έργου. Τέλος, θα πρέπει να προβάλλει τα πλεονεκτήματα, στους πολίτες και να προσπαθήσει να κερδίσει την εμπιστοσύνη τους.

Δεν είναι αναγκαίο ο τελικός χρήστης να κατέχει γνώσεις για την υποδομή και την λειτουργία της Δημόσιας Διοίκησης όπως για παράδειγμα τις υποχρεώσεις κάθε τομέα. Η σειρά που ακολουθείται για να λάβει ο χρήστης την υπηρεσία είναι, να κάνει το αίτημα στο σημείου εισόδου και να παίρνει το αποτέλεσμα της υπηρεσίας από το τελευταίο σημείο, το σημείο εξόδου ώστε να μην επεμβαίνει στα επιμέρους τμήματα που αναλαμβάνουν την εκτέλεση της υπηρεσίας. Με αυτό τον τρόπο γίνεται πιο γρήγορα η εξυπηρέτηση των χρηστών και πιο αποδοτικά αφού δεν παρεμβαίνουν στα μεσολαβητικά τμήματα. Καθ' όλη τη διάρκεια της αναμονής του αποτελέσματος, ο χρήστης θα πρέπει να ενημερώνεται για την εξέλιξη του αιτήματός του αλλά και για τις αποφάσεις που λαμβάνονται σχετικά με την υπόθεση που ολοκληρώνει ηλεκτρονικά.

Για να πραγματοποιηθούν τα παραπάνω θα πρέπει να υπάρχει ένα πληροφοριακό σύστημα που να συνδέεται με τους φορείς της Δημόσιας Διοίκησης. Πιο αναλυτικά θα πρέπει να συνδέεται η διαδικτυακή πύλη του κάθε φορέα και να υπάρχει πρόσβαση στο περιεχόμενο καθώς και να εκτελούνται σωστά οι λειτουργίες των εμπλεκόμενων φορέων ώστε να υπάρχει το σωστό αποτέλεσμα. Η κατασκευή αυτή θα πρέπει να είναι φιλική προς το χρήστη και να μπορεί να το χρησιμοποιεί οποιοδήποτε άτομο, με ή χωρίς γνώσεις πάνω στα πληροφοριακά συστήματα και στον τρόπο λειτουργίας τους. Τέτοια εξέλιξη, φαίνεται να υπάρχει με την δημιουργία των Κυβερνητικών Δικτυακών Πυλών. Ένα τέτοιο παράδειγμα στην Ελλάδα είναι το gov.gr. Άλλες τέτοιες πύλες αναφέρονται παρακάτω.

Χώρα	Διαδικτυακή Πύλη	Σύνδεσμος
Αυστραλία	Government Portal	www.australia.gov.au
Αυστρία	Government Information Portal	http://help.gv.at
Γαλλία	Service-Public Portal	www.service-public.fr
Γερμανία	Service Portal of the Federal Government	www.bund.de
Ελβετία	Governmental Information & Links	www.ch.ch
Ελλάδα	Διαδικτυακή Πύλη Ερμής	www.ermis.gov.gr
Ηνωμένες Πολιτείες Αμερικής	U.S. Government's Official web portal	www.firstgov.gov
Ηνωμένο Βασίλειο	UK Government On-line	www.gov.uk
Καναδάς	Government of Canada Portal	www.canada.gc.ca
Νέα Ζηλανδία	Government Portal	www.newzealand.govt.nz
Ολλανδία	Integrated Government Portal	www.overheid.nl
Ταϊβάν	Taiwan Government Entry Point	www.taiwan.gov.tw
Χονκ Κονγκ	Hong Kong Government Services	www.gov.hk

Πίνακας 1 Παραδείγματα Διαδικτυακών Πυλών ανά τον Κόσμο

1.3 Ηλεκτρονικές Υπηρεσίες στην Ελλάδα

Υπάρχουν κάποιες βασικές υπηρεσίες στην Ελλάδα που παρακολουθούνται σε ευρωπαϊκό πλαίσιο λόγω του ότι υπάρχουν κοινά στοιχεία και σε άλλες χώρες της Ευρώπης. Κάποιες από αυτές σχετίζονται με τον πολίτη και κάποιες άλλες με τις επιχερήσεις. Παρακάτω φαίνονται οι υπηρεσίες, το επίπεδο ολοκλήρωσής τους αλλά και τον φορέα της Δημόσιας Διοίκησης που αφορά.

	A/A	Βασικές Δημόσιες Υπηρεσίες	Επίπεδο Ολοκλήρωσης	Δημόσιος Φορέας Πάροχος Υπηρεσίας
Ηλεκτρονικές Υπηρεσίες προς Πολίτες	1	Φόρος εισοδήματος: δήλωση και ειδοποίηση εκκαθάρισης	5	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	2	Υπηρεσίες Αναζήτησης Εργασίας	4	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	3	Εισφορές Κοινωνικής Ασφάλισης	2,25[2]	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	4	Προσωπικά έγγραφα (διαβατήριο και άδεια οδήγησης)	2,5	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη - Ελληνική Αστυνομία (διεύθυνση διαβατηρίων)/ Κέντρα Ενημέρωσης Πολιτών (ΚΕΠ)
	5	Καταχώρηση Οχήματος	n/a**[3]	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	6	Έκδοση Οικονομικής Άδειας	2	e- ΠΟΛΕΟΔΟΜΙΑ (Υπουργείο Περιβάλλοντος Ενέργειας & Κλιματικής Αλλαγής (ΥΠΕΚΑ) & Υπουργείο Εσωτερικών (ΥΠΕΣ))
	7	Δήλωση προς την Αστυνομία (π.χ., σε περίπτωση κλοπής)	1	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη – Ελληνική Αστυνομία
	8	Δημόσιες βιβλιοθήκες (διαθεσιμότητα καταλόγων, εργαλεία αναζήτησης)	4	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού

Πίνακας 2-1 Οι ηλεκτρονικές υπηρεσίες στην Ελλάδα

	Α/Α	Βασικές Δημόσιες Υπηρεσίες	Επίπεδο Ολοκλήρωσης	Δημόσιος Φορέας Πάροχος Υπηρεσίας
	9	Πιστοποιητικά (Γεννήσεως και Γάμου): αίτηση & παραλαβή	3	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	10	Εισαγωγή στην Ανώτατη Εκπαίδευση	2	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού
	11	Ανακοίνωση Μετακόμισης – Αλλαγή Διεύθυνσης	4	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	12	Υπηρεσίες Υγείας (διαθεσιμότητα υπηρεσιών & κλείσιμο ραντεβού)	2	Υπουργείο Υγείας
Ηλεκτρονικές Υπηρεσίες προς Επιχειρήσεις	13	Εισφορές Κοινωνικής Ασφάλισης για Εργαζομένους	4	Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ)
	14	Φόρος Επιχειρήσεων: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	15	ΦΠΑ: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	16	Έναρξη Επιχείρησης	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)
	17	Υποβολή Στοιχείων σε Στατιστικές Υπηρεσίες	4	Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ.)
	18	Δηλώσεις στα Τελωνεία	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	19	Περιβαλλοντικές Άδειες	2	Υπουργείο Περιβάλλοντος, Ενέργειας & Κλιματικής Αλλαγής/ Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	20	Δημόσιες Προμήθειες	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)

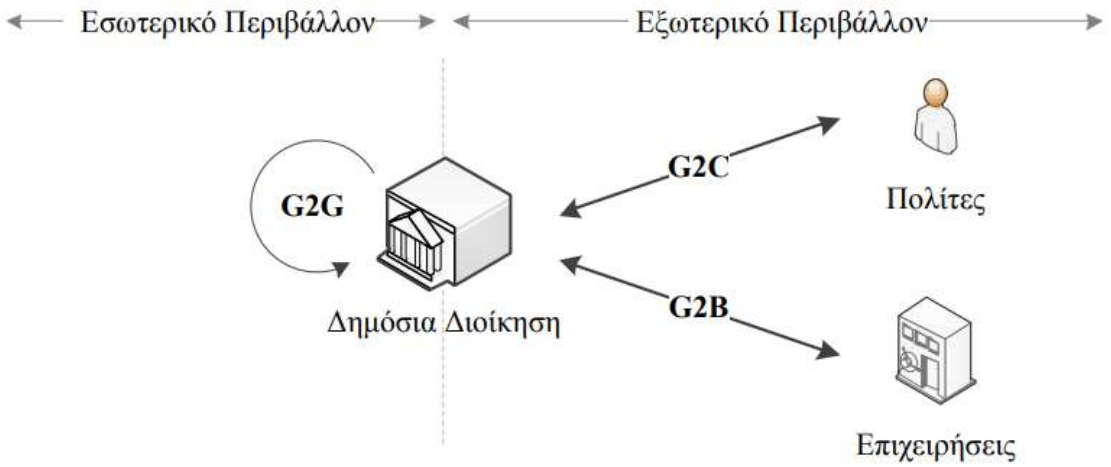
Πίνακας 3-2 Οι ηλεκτρονικές υπηρεσίες στην Ελλάδα

1.4 Στρατηγική για την Ηλεκτρονική Διακυβέρνηση

Κύριος στόχος της Ηλεκτρονικής Διακυβέρνησης είναι να εκσυγχρονίσει και να αναπτύξει την χώρα. Πιο αναλυτικά, βασισμένη στις τεχνολογίες των πληροφοριών και των επικοινωνιών, στην παραγωγικότητα καθώς και σε συνδυασμό με τα αντίστοιχα τμήματα της χώρας ο βασικός σχεδιασμός στηρίζεται στην παροχή όσο το δυνατόν περισσότερων ψηφιακών υπηρεσιών προς τον πολίτη ή την επιχείρηση, αλλά υπηρεσίες που μπορούν να ολοκληρωθούν διαδικτυακά χωρίς ο πολίτης ή κάποιος εκπρόσωπος της επιχείρησης να είναι παρόν. Επίσης, θα πρέπει να δημιουργηθεί ένα περιβάλλον ψηφιακό που να μπορούν να επικοινωνούν και να συνεργάζονται τα τμήματα που παρέχουν υπηρεσίες καθώς και τα στελέχη της δημόσιας διοίκησης. Τέλος, θα πρέπει να χρησιμοποιούνται σύγχρονες υποδομές καθώς και να εξασφαλίζεται οι ποιοτικές και ασφαλείς συνθήκες για την ψηφιακή ανάπτυξη τόσο για τους πολίτες και τις επιχειρήσεις όσο και για το ίδιο το Δημόσιο σύστημα. Τα παραπάνω θα πρέπει να ολοκληρωθούν βασισμένα στους κανόνες προστασίας των προσωπικών δεδομένων και στης προστασία της ιδωτικότητας.

1.5 Τομείς της Ηλεκτρονικής Διακυβέρνησης

Για να εκμεταλλευτεί η δημόσια διοίκηση όλες τις δυνατότητες της ηλεκτρονικής διακυβέρνησης θα πρέπει οι διαδικασίες που υπάρχουν να είναι σχεδιασμένες με τέτοιο τρόπο ώστε να καλύπτονται όλες οι απαιτήσεις των τομέων της Δημόσιας διοίκησης από το εσωτερικό αλλά και το εξωτερικό περιβάλλον της. Οι απαιτήσεις αυτές γίνονται γνωστές από τα εμπλεκόμενα μέλη της Δημόσιας διοίκησης που είναι οι πολίτες οι επιχειρήσεις αλλά και ίδια η δημόσια διοίκηση. Οι τομείς οι οποίοι δημιουργούν τις απαιτήσεις αυτές είναι ο Government to citizen όπου περιέχει όλες τις διαδικασίες μεταξύ των πολιτών και της δημόσιας διοίκησης είναι ο Government to business που περιλαμβάνει τις διαδικασίες μεταξύ των επιχειρήσεων και της δημόσιας διοίκησης και είναι και ο Government to Government που περιλαμβάνει τις διαδικασίες μεταξύ των φορέων της Δημόσιας διοίκησης. Το εξωτερικό περιβάλλον είναι ο τομέας Government to citizen και ο τομέας Government to business και το εσωτερικό περιβάλλον είναι ο τομέας Government to Government.



Εικόνα 1 Τομείς Ηλεκτρονικής Διακυβέρνησης

1.6 Επίπεδα Ολοκλήρωσης Υπηρεσιών

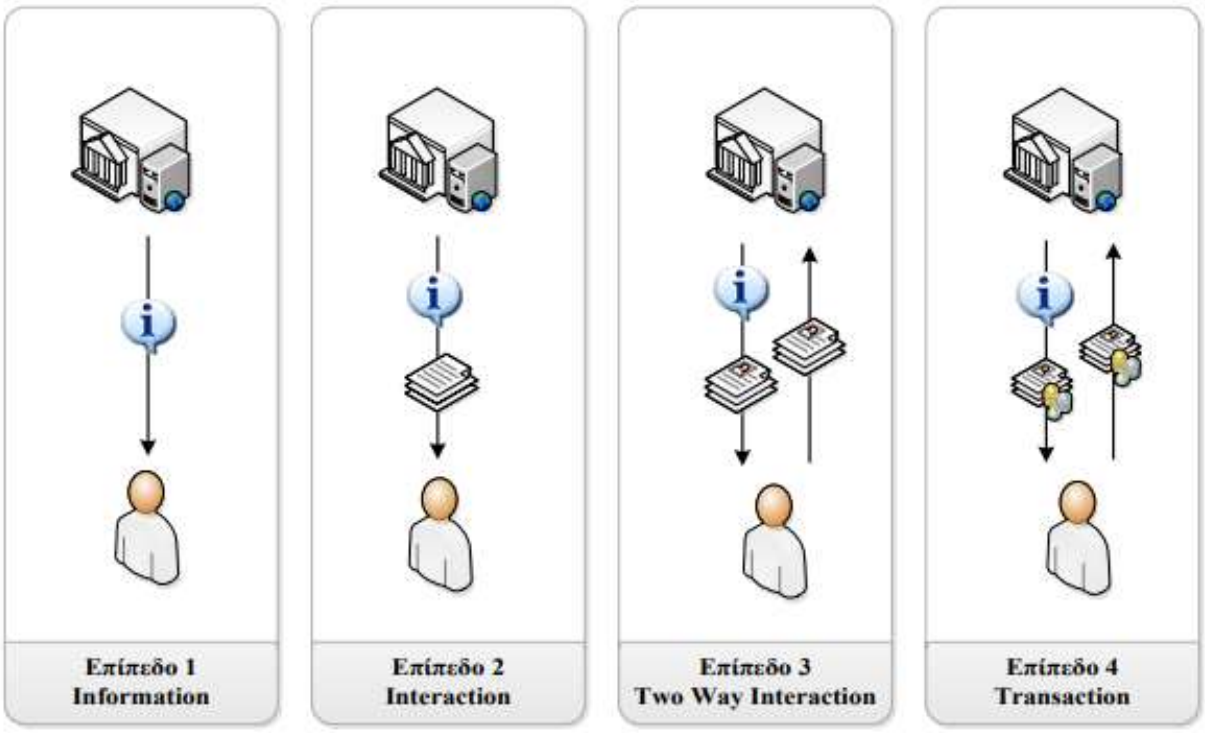
Οι ηλεκτρονικές υπηρεσίες της ελληνικής κυβέρνησης ανάλογα με το βαθμό ολοκλήρωσης της κατατάσσονται και σε κάποιες κατηγορίες. Αυτές οι κατηγορίες είναι τα επίπεδα ολοκλήρωσης των υπηρεσιών. Το πρώτο επίπεδο αφορά πληροφοριακές υπηρεσίες όπου γίνεται παροχή υλικού το οποίο αναφέρει πληροφορίες για το πως διεκπεραιώνεται υπηρεσία δηλαδή ποια δικαιολογητικά θα πρέπει να κατατεθούν στους φορείς για την διεκπεραίωση της υπηρεσίας.

Επόμενο επίπεδο είναι το επίπεδο δύο που αφορά τις επικοινωνιακές υπηρεσίες και παρέχεται υλικό στους χρήστες τόσο για το πως διεκπεραιώνεται υπηρεσία αλλά και πρότυπα διαφόρων εγγράφων που θα πρέπει να καταθέσουν οι χρήστες αφού πρώτα το εξασφαλίσουν με τη χρήση του διαδικτύου το εκτυπώσουν και το χρησιμοποιήσουν στον φορέα όπου γίνεται υπηρεσία. Το επίπεδο τρία αφορά τις διαδραστικές υπηρεσίες όπου εδώ παρέχονται μέσω διαδικτύου τα έγγραφα και

συμπληρώνονται και αποστέλλονται ηλεκτρονικά στον φορέα που εκτελεί την υπηρεσία. Στο επίπεδο τέσσερα εντάσσονται οι συναλλακτικές υπηρεσίες όπου υπηρεσίες που τα έγγραφα συμπληρώνονται και αποστέλλεται ηλεκτρονικά μπορεί να χρειάζονται και οικονομικές συναλλαγές και αυτό παρέχεται σε αυτό το επίπεδο.

Το πέμπτο επίπεδο και τελευταίο σχετίζεται την παροχή υπηρεσιών της Δημόσιας διοίκησης που αφορά την αναβάθμιση και τον εκσυγχρονισμό της ηλεκτρονικής υπηρεσίας καθώς και την βελτίωση της υπηρεσίας προς το χρήστη. Επίσης, το επίπεδο αυτό έχει να κάνει και με τις αυτοματοποιημένες υπηρεσίες όπου παρέχονται σε κάποιες ηλεκτρονικές υπηρεσίες χωρίς να υπάρχει κάποιο αίτημα από το χρήστη. Αυτό ήταν το τελευταίο που προστέθηκε στα επίπεδα ολοκλήρωσης υπηρεσιών ηλεκτρονικής διακυβέρνησης και γενικότερα αφορά τον εκσυγχρονισμό των υπηρεσιών αλλά και του ίδιου του περιβάλλοντος της δημόσιας διοίκησης.

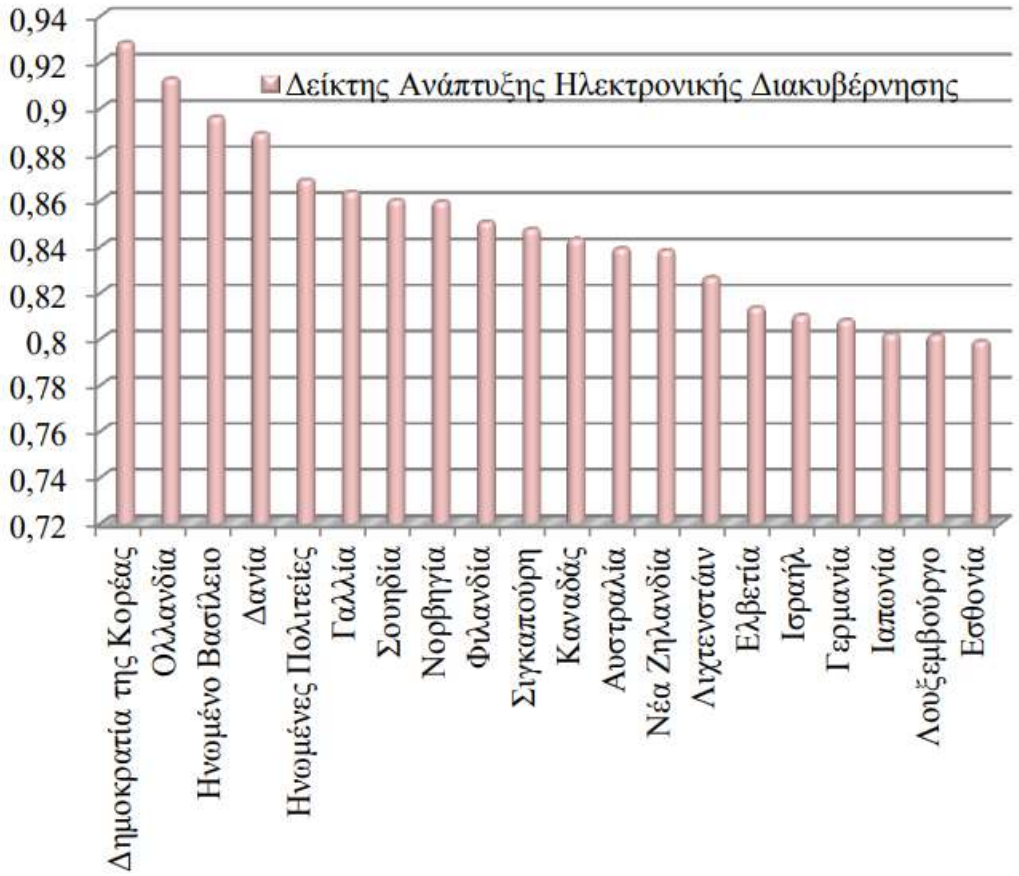
Παρακάτω φαίνονται τα τέσσερα επίπεδα ολοκλήρωσης των υπηρεσιών της ηλεκτρονικής διακυβέρνησης.



Εικόνα 2 Επίπεδα Ολοκλήρωσης Υπηρεσιών

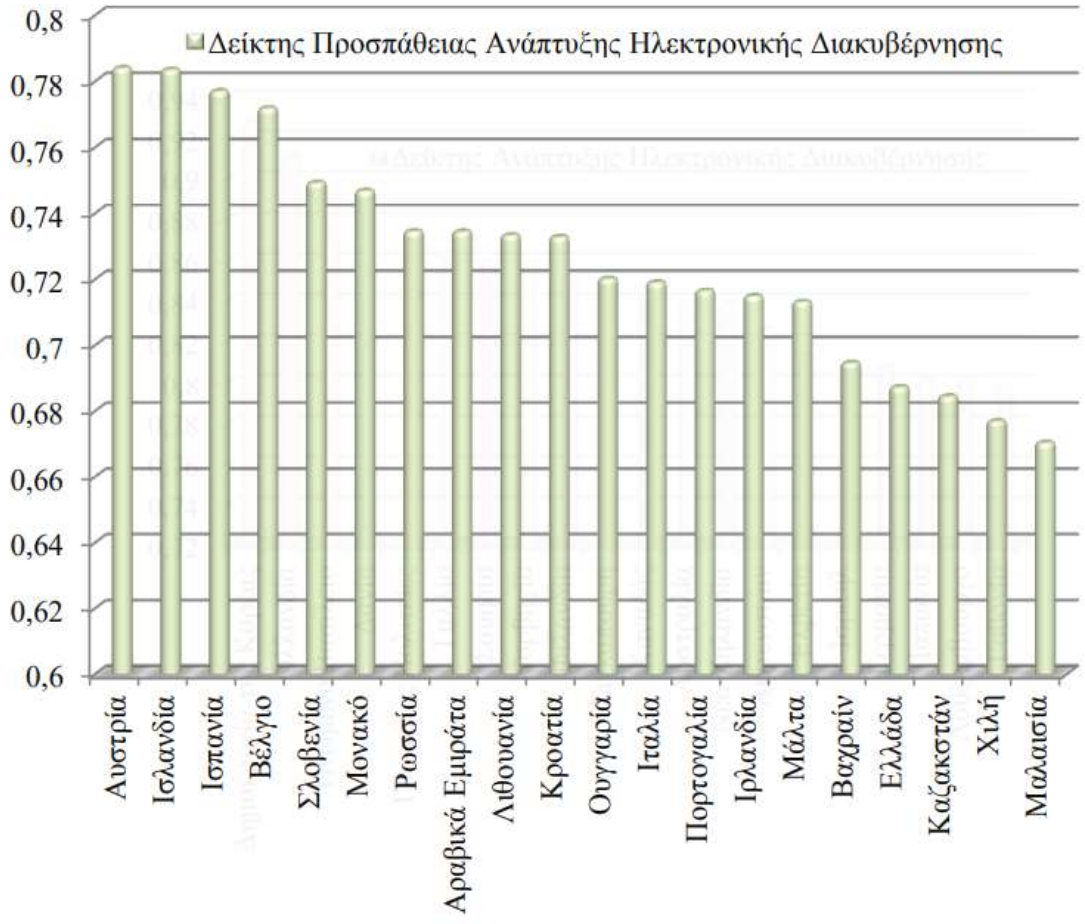
1.7 Εξέλιξη Ηλεκτρονικής Διακυβέρνησης ανά τον Κόσμο

Η εξέλιξη της ηλεκτρονικής διακυβέρνησης στον κόσμο σχετίζεται με τις ενοποιημένες και ολοκληρωμένες υπηρεσίες που είναι υπεύθυνες για τις διασυνδέσεις των υπηρεσιών που βελτιώνουν και εκσυγχρονίζουν την παροχή των ηλεκτρονικών υπηρεσιών, αυξάνουν την παραγωγικότητα καθώς και βελτιώνουν τις διαδικασίες και τους μηχανισμούς της δημόσιας διοίκησης. Σ όλο τον κόσμο υπάρχει ανάπτυξη. Σε κάποιες όμως χώρες που είναι οικονομικά ανεπτυγμένες υπάρχει υψηλή ανάπτυξη. Κάποιες από αυτές βρίσκονται στη βόρεια Αμερική και στην Ευρώπη στην ανατολική Ασία στην ωκεανία. Παρακάτω παρουσιάζονται αυτές οι χώρες οι οποίες είναι οικονομικά ανεπτυγμένες και παρουσιάζουν μεγάλη ανάπτυξη.



Εικόνα 3 Δείκτες Ανάπτυξης

Αυτό που συμπεραίνουμε από την παραπάνω εικόνα είναι ότι όλες οι χώρες προσπαθούν και καταφέρνουν σε πολύ καλό βαθμό να παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης. Δυστυχώς όμως, υπάρχουν και χώρες που δεν είναι οικονομικά αναπτυγμένες όπως οι χώρες της Αφρικής και λόγω της έλλειψης τεχνογνωσίας αλλά και τεχνολογικής υποδομής δημιουργείται μεγάλο κενό στην ανάπτυξη παγκοσμίως. Παρακάτω παρουσιάζονται άλλες χώρες οι οποίες έχουν σημαντική βελτίωση στην ανάπτυξη της ηλεκτρονικής διακυβέρνησης.



Εικόνα 4 Δείκτες Προσπάθειας Ανάπτυξης

1.8 Εξέλιξη Βασικών Δημόσιων Ηλεκτρονικών Υπηρεσιών

έπειτα από έρευνα που έγινε από το παρατηρητήριο τα αποτελέσματα που δόθηκαν στη δημοσιότητα αφορούν βασικές υπηρεσίες ηλεκτρονικής διακυβέρνησης στην Ελλάδα οι οποίες ελέγχθηκαν και αξιολογήθηκαν από την Ευρώπη με συγκεκριμένο τρόπο όπως αξιολογούνται και για τα υπόλοιπα κράτη. Οι παρακάτω βασικές δημόσιες υπηρεσίες κάποιες αφορούν τον πολίτη και κάποιες αφορούν τις επιχειρήσεις. Παρακάτω παρουσιάζονται οι βασικές δημόσιες ηλεκτρονικές υπηρεσίες.

	Α/Α	Βασικές Δημόσιες Υπηρεσίες	Επίπεδο Ολοκλήρωσης	Δημόσιος Φορέας Πάροχος Υπηρεσίας
Ηλεκτρονικές Υπηρεσίες προς Πολίτες	1	Φόρος εισοδήματος: δήλωση και ειδοποίηση εκκαθάρισης	5	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	2	Υπηρεσίες Αναζήτησης Εργασίας	4	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	3	Εισφορές Κοινωνικής Ασφάλισης	2,25[2]	Οργανισμός Απασχόλησης Εργατικού Δυναμικού (ΟΑΕΔ)
	4	Προσωπικά έγγραφα (διαβατήριο και άδεια οδήγησης)	2,5	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη - Ελληνική Αστυνομία (διεύθυνση διαβατηρίων)/ Κέντρα Ενημέρωσης Πολιτών (ΚΕΠ)
	5	Καταχώρηση Οχήματος	n/a**[3]	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	6	Έκδοση Οικονομικής Άδειας	2	e- ΠΟΛΕΟΔΟΜΙΑ (Υπουργείο Περιβάλλοντος Ενέργειας & Κλιματικής Αλλαγής (ΥΠΕΚΑ) & Υπουργείο Εσωτερικών (ΥΠΕΣ))
	7	Δήλωση προς την Αστυνομία (π.χ., σε περίπτωση κλοπής)	1	Υπουργείο Δημοσίας Τάξης & Προστασίας του Πολίτη – Ελληνική Αστυνομία
	8	Δημόσιες βιβλιοθήκες (διαθεσιμότητα καταλόγων, εργαλεία αναζήτησης)	4	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού

Εικόνα 5 Βασικές Δημόσιες Ηλεκτρονικές Υπηρεσίες

	Α/Α	Βασικές Δημόσιες Υπηρεσίες	Επίπεδο Ολοκλήρωσης	Δημόσιος Φορέας Πάροχος Υπηρεσίας
	9	Πιστοποιητικά (Γεννήσεως και Γάμου): αίτηση & παραλαβή	3	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	10	Εισαγωγή στην Ανώτατη Εκπαίδευση	2	Υπουργείο Παιδείας & Θρησκευμάτων, Πολιτισμού & Αθλητισμού
	11	Ανακοίνωση Μετακόμισης – Αλλαγή Διεύθυνσης	4	Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	12	Υπηρεσίες Υγείας (διαθεσιμότητα υπηρεσιών & κλείσιμο ραντεβού)	2	Υπουργείο Υγείας
Ηλεκτρονικές Υπηρεσίες προς Επιχειρήσεις	13	Εισφορές Κοινωνικής Ασφάλισης για Εργαζομένους	4	Ίδρυμα Κοινωνικών Ασφαλίσεων (ΙΚΑ)
	14	Φόρος Επιχειρήσεων: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	15	ΦΠΑ: Δήλωση & Ειδοποίηση Εκκαθάρισης	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	16	Έναρξη Επιχείρησης	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)
	17	Υποβολή Στοιχείων σε Στατιστικές Υπηρεσίες	4	Ελληνική Στατιστική Αρχή (ΕΛ.ΣΤΑΤ.)
	18	Δηλώσεις στα Τελωνεία	4	Γενική Γραμματεία Πληροφοριακών Συστημάτων (ΓΓΠΣ)
	19	Περιβαλλοντικές Άδειες	2	Υπουργείο Περιβάλλοντος, Ενέργειας & Κλιματικής Αλλαγής/ Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ)
	20	Δημόσιες Προμήθειες	2	Γενική Γραμματεία Εμπορίου (ΓΓΕ)

Εικόνα 6 Βασικές Δημόσιες Ηλεκτρονικές Υπηρεσίες

1.9 Εθνική Στρατηγική

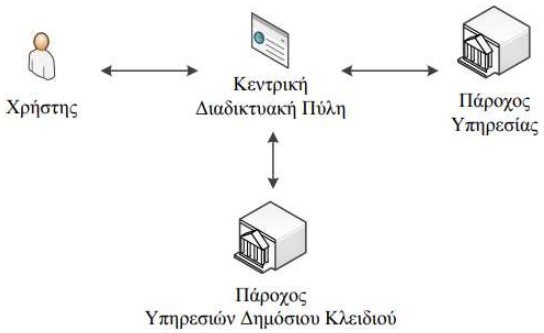
Η εθνική στρατηγική που σχετίζεται με την ηλεκτρονική διακυβέρνηση έχει σκοπό την ανάπτυξη ενός νέου κλάδου της χώρας η οποία θα είναι βασισμένη στη στρατηγική που ακολουθείται για τις τεχνολογίες πληροφοριών και επικοινωνιών. Θα υπάρξει συνεργασία με υπουργεία και η στρατηγική αυτή θα έχει όλα αυτά τα στοιχεία που θα την κάνουν ανταγωνιστική παραγωγική και τελικώς επιτυχημένη. Οι 3 άξονες πού θα κινηθεί η εθνική στρατηγική είναι αρχικά η παροχή λοιπόν όλων και περισσότερων ηλεκτρονικών υπηρεσιών προς το χρήστη επιπέδου 4 και επιπέδου 5 δηλαδή υπηρεσίες που ολοκληρώνονται ηλεκτρονικά. Ο επόμενος άξονας είναι η καθιέρωση της ψηφιακής συνεργασίας και επικοινωνίας στο εσωτερικό περιβάλλον της δημόσιας διοίκησης και τέλος ο εκσυγχρονισμός των υποδομών και η εξασφάλιση μηχανισμών ασφάλειας στην ψηφιακή ανάπτυξη τόσο για τους χρήστες όσο και για τη δημόσια διοίκηση. Η στρατηγική αυτή θα είναι βασισμένη στους κανόνες περί προστασίας των ευαίσθητων προσωπικών δεδομένων και της ιδιωτικότητας.

Κεφάλαιο 2 Ψηφιακή αυθεντικοποίηση

Στο παρακάτω κεφάλαιο παρουσιάζεται ένα μοντέλο ψηφιακής αυθεντικοποίησης που έχει ως στόχο να θέσει κανόνες για τις προτεραιότητες σχετικά με το αν είναι κρίσιμη ή όχι κάθε ηλεκτρονική υπηρεσία, για τους μηχανισμούς αυθεντικοποίησης και εγγραφής. Αυτό θα γίνει με βάση το εθνικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων καθώς και για την εξασφάλιση της ιδιωτικότητας των πολιτών.

2.1 Σκοπός

Στα πλαίσια ενός εθνικού προγράμματος έγινε μελέτη για την διαμόρφωση ενός μοντέλου ψηφιακής αυθεντικοποίησης. Το πλαίσιο αυτό, σχεδιάστηκε για το ελληνικό δημόσιο με σκοπό τη διευκόλυνση των πολιτών κατά την παροχή υπηρεσιών σε αυτούς. Πρωταρχικός στόχος του πλαισίου ψηφιακής αυθεντικοποίησης είναι να βοηθήσει όλους τους τομείς και τους οργανισμούς της δημόσιας διοίκησης που προσφέρουν ή ετοιμάζουν να προσφέρουν υπηρεσές ηλεκτρονικής διακυβέρνησης στην επιλογή μηχανισμών αυθεντικοποίησης, διαδικασιών εγγραφής και ταυτοποίησης. Η εφαρμογή των παραπάνω οδηγιών του πλαισίου ψηφιακής αυθεντικοποίησης θα οδήγησει στην αύξηση του επιπέδου ασφάλειας των υπηρεσιών που προσφέρουν οι φορείς της δημόσιας διοίκησης, θα βελτιώσει με τη σειρά του τη λειτουργία της δημόσιας διοίκησης αφού θα εναρμονιστεί με τα ευρωπαϊκά πρότυπα. Πιο αναλυτικά, οι υπηρεσίες των φορέων της δημόσιας διοίκησης προσφέρονται όπως βλέπουμε στην εικόνα 1, μέσω της κεντρικής Διαδικτυακής Πύλης, αφού πιο πριν έχει καθοριστεί η οποιαδήποτε απαίτηση της υπηρεσίας όπως επίπεδο εμπιστοσύνης, διαδικασία αυθεντικοποίησης, διαδικασία εγγραφής όπως επίσης και τα απαραίτητα στοιχεία που πρέπει να υποβάλλουν οι χρήστες κατά την εγγραφή. Στη συνέχεια μετά την εγγραφή των χρηστών μέσω της κεντρικής διαδικτυακής πύλης, μπορούν να αξιοποιήσουν οποιαδήποτε διαθέσιμη ηλεκτρονική υπηρεσία βλέπουν αφού πρώτα προηγηθεί ο έλεγχος και επιβεβαίωση της ακρίβειας της ηλεκτρονικής ταυτότητας τους.



Εικόνα 7 Γενική Αρχιτεκτονική ΠΨΑ

Πριν δημιουργηθεί το πλαίσιο ψηφιακής αυθεντικοποίησης, για την διαδικασία της ταυτοποίησης και της αυθεντικοποίησης χρησιμοποιούταν τα ονόματα χρήστη(Username) και οι κωδικοί πρόσβασης(password) για την επαλήθευση της ψηφιακής ταυτότητας των χρηστών. Αυτό σημαίνει ότι με αυτό τον τρόπο δεν λαμβάνονταν υπόψη η προτεραιότητα για το αν είναι κρίσιμη ή όχι ηλεκτρονική υπηρεσία. Δηλαδή, λόγω του ότι δεν λαμβάνεται υπόψη η κρισιμότητα της υπηρεσίας με τον παλιό τρόπο θα μπορούσαν να υπάρχουν προβλήματα σχετικά με την ασφάλεια είτε στους φορείς του δημοσίου είτε στον ίδιο το χρήστη. Έτσι το πλαίσιο ψηφιακής αυθεντικοποίησης έρχεται να λύσει το πρόβλημα αυτό αφού όπως είπαμε και παραπάνω είναι βασισμένο στο νομικό και στο κανονιστικό πλαίσιο για την προστασία των δεδομένων όπως επίσης και στην ασφάλεια της ιδιωτικότητας του χρήστη αφού δίνει προτεραιότητες στο αν είναι κρίσιμες ή όχι ηλεκτρονικές υπηρεσίες και επιλέγει κατάλληλους μηχανισμούς αυθεντικοποίησης.

2.1.1 Εφαρμογή

Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης απευθύνεται σε φορείς της Δημόσιας Διοίκησης, οι οποίοι θέλουν να υλοποιήσουν διαδικτυακή πύλη με σκοπό την παροχή πληροφοριών και υπηρεσιών σε πολίτες, επιχειρήσεις και άλλους φορείς. Συγκεκριμένα, απευθύνεται σε Υπουργεία, Γενικές Γραμματείες, περιφέρειες, νομαρχίες, οργανισμούς τοπικής αυτοδιοίκησης, εποπτευόμενους φορείς του Δημοσίου, ανεξάρτητες αρχές, και οργανισμούς του δημόσιου και ιδιωτικού τομέα που συμβάλλουν στην ανάπτυξη και στην παροχή υπηρεσιών.

2.1.2 Η Ιδιωτικότητα στις Υπηρεσίες

Για να αξιοποιηθούν πλήρως οι υπηρεσίες ηλεκτρονικής διακυβέρνησης θα πρέπει να συλλεχθούν και να επεξεργαστούν προσωπικά δεδομένα. Θα πρέπει να τηρηθεί η προστασία των προσωπικών δεδομένων βασισμένη στο νομικό πλαίσιο και η ιδιωτικότητα των πληροφοριών, αφού είναι δικαίωμα κάθε φυσικού προσώπου να ελέγχει την χρήση των δεδομένων του από τρίτους.

2.1.3 Κατηγορίες Δεδομένων

Για την ολοκλήρωση κάθε ηλεκτρονικής υπηρεσίας, μπορούν να χρησιμοποιηθούν τρεις διαφορετικές κατηγορίες δεδομένων, με βάση την ανάγκη προστασίας της ιδιωτικότητάς τους:

1. **Δημόσια (προσπελάσιμα - διαθέσιμα) δεδομένα:** Αναφέρονται σε πληροφορίες που δεν είναι ευαίσθητες ή προσωπικές. Το περιεχόμενο των φορέων του Δημοσίου, οι νόμοι και άλλα τέτοια είναι στατιστικά δεδομένα και δεν είναι απαραίτητα δημόσια. Αν τα δεδομένα δεν μπορούν να προσδιορισθούν μόνο και μόνο τότε μπορούμε να τα χρησιμοποιούμαι και να τα επεξεργαζόμαστε ως δημόσια δεδομένα.
2. **Προσωπικά δεδομένα:** Αναφέρονται σε πληροφορίες που σχετίζονται με το πρόσωπο που αφορούν τα δεδομένα. Η ταυτοποίηση του προσώπου μπορεί να γίνει άμεσα με τον αριθμό ταυτότητας ή άλλων στοιχείων που προσδιορίζουν το υποκείμενο των δεδομένων.
3. **Ευαίσθητα (προσωπικά) δεδομένα:** Αναφέρονται σε πληροφορίες που αφορούν στη προέλευση του φυσικού προσώπου, πολιτικές πεποιθήσεις, θρησκευτικές πεποιθήσεις, υγεία και άλλα.

Είναι σημαντικό να διαχειριζόμαστε τα προσωπικά και τα ευαίσθητα δεδομένα με προσοχή και σεβασμό προς την ιδιωτικότητα των ατόμων, σύμφωνα με τις νομοθετικές διατάξεις που διέπουν το θέμα.

Κατηγορία Δεδομένων	Περιγραφή
Δημόσια Διαθέσιμα Δεδομένα	Σε αυτή τη κατηγορία περιλαμβάνονται τα δεδομένα που είναι δημοσίως προσπελάσιμα και δεν περιέχουν προσωπικές πληροφορίες
Προσωπικά Δεδομένα	Σε αυτή τη κατηγορία δεδομένων περιλαμβάνονται όλα εκείνα τα στοιχεία που σχετίζονται με ένα πρόσωπο όπως Όνομα, Επίθετο, ημερομηνία γέννησης, Αριθμός Φορολογικού Μητρώου (ΑΦΜ), εναλλακτικά αναγνωριστικά, διεύθυνση αλληλογραφίας, ηλεκτρονική διεύθυνση αλληλογραφίας. Επισημαίνεται ότι και ως προς αυτά τα δεδομένα δεν πρέπει να γίνεται καμία χρήση χωρίς να υπάρχει «εξουσιοδότηση» που εν προκειμένω νοείται εν γένει ως νομική βάση της επεξεργασίας (δηλ. νόμος, δημόσιο συμφέρον, συγκατάθεση κλπ.).
Ευαίσθητα Δεδομένα	Σε αυτή την κατηγορία περιλαμβάνονται τα δεδομένα που ορίζει ο Ν. 2472/97 στο άρθρο 2β και την επεξεργασία των οποίων ρυθμίζει στο άρθρο 7 και 7 Α .

Πίνακας 4 Κατηγορίες Δεδομένων

2.1.4 Ευθύνες της Δημόσιας Διοίκησης

Η Δημόσια Διοίκηση θα πρέπει να ακολουθήσει μια σειρά ενεργειών για να αυθεντικοποιήσει τους πολίτες. Αρχικά, θα πρέπει οι πολίτες θα πρέπει να λαμβάνουν έγγραφα που θα πιστοποιούν την εγγραφή των πολιτών. Κατά την εγγραφή θα πρέπει οι πολίτες να ενημερώνονται για τα δεδομένα που είναι απαραίτητα για να ολοκληρωθεί η εγγραφή. Στη συνέχεια θα λαμβάνουν έγγραφα που θα είναι για την συναίνεση στην επεξεργασία δεδομένων γι' αυτό και πρέπει να είναι γραμμένα με σαφήνεια και με κατανοητό τρόπο. Όταν ο πολίτης, φτάσει στο σημείο να λαμβάνει τις υπηρεσίες θα πρέπει η Διοίκηση να ενημερώνει ποια από τα δεδομένα του πολίτη και τι είδους είναι απαραίτητα για την επεξεργασία ώστε να ολοκληρωθεί η αίτηση, δηλαδή ποια δεδομένα έχουν προτεραιότητα και ποια μπορούν να συμπληρωθούν μεταγενέστερα. Επιπλέον, κατά της αίτηση της εγγραφής θα πρέπει η Δημόσια Διοίκηση να ενημερώνει τον πολίτη με τα στοιχεία του ατόμου που τον εξυπηρετεί, τον λόγο που γίνεται η επεξεργασία, για το ποιοι

θα μπορούν να δουν τα δεδομένα του, αλλά και αν υπάρχει δικαίωμα πρόσβασης. Γενικότερα, η Δημόσια Διοίκηση, θα πρέπει να ακολουθεί το πρωτόκολλο της Αρχής Προστασίας Προσωπικών Δεδομένων, και να γνωστοποιεί όταν συλλέγονται και επεξεργάζονται δεδομένα, να γίνεται αίτηση στην Αρχή όταν είναι να επεξεργασθούν ευαίσθητα δεδομένα όπως επίσης και όταν χρειάζεται να γίνει διασύνδεση και το ένα αρχείο από αυτά που θα διασυνδεθούν περιέχει ευαίσθητα δεδομένα. Τέλος, η Δημόσια Διοίκηση, θα πρέπει να ενημερώσει του υπεύθυνους που αναλαμβάνου τις αιτήσεις ότι τα δεδομένα που λαμβάνουν από τους πολίτες θα πρέπει να τα ελέγχουν ότι είναι αληθή και να διαγράφουν αν κάποια δεδομένα δεν είναι αναγκαία ή έχει περάσει η περίοδος που αρχικά είχε οριστεί για την ολοκλήρωση των στόχων.

2.1.5 Κατηγοριοποίηση Δεδομένων για αξιοποίηση σε ηλεκτρονική υπηρεσία

Η κατηγοριοποίηση δεδομένων που μπορούν να αξιοποιηθούν σε μια ηλεκτρονική υπηρεσία είναι βασισμένη στην εθνική στην κοινοτική και στην διεθνή νομοθεσία.

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΑΠΛΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί. *Λόγω της ευρύτητας του ορισμού δεν είναι δυνατός ο ακριβής προσδιορισμός των δεδομένων που εντάσσονται στα «απλά»*	Άρθρο 2α ν. 2472/97 Ορισμός δεδομένων	Με την επιφύλαξη α) της ένταξης ορισμένων από τα αναφερόμενα στον πίνακα 1) στο προστατευτικό πεδίο απορρήτων, όπως το φορολογικό απόρρητο και
	Άρθρο 5 ν. 2690/99 (ΚΔΔ - Εξαιρέσεις από πρόσβαση σε διοικητικά έγγραφα για την προστασία της ιδιωτικής ζωής ή οικογενειακής ζωής)	β) του ενδεχόμενου να εντάσσονται ορισμένα απλά δεδομένα στο πεδίο της ιδιωτικής ή οικογενειακής ζωής σύμφωνα με τον ΚΔΔ
Ενδεικτικά πρόκειται για **Στοιχεία για τον προσδιορισμό της ταυτότητας του προσώπου**. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (κωδικός αναγνώρισης ή πρόσβασης, PIN κ.α.).	Ν. 2472/97	Τηρουμένων των προϋποθέσεων και εγγυήσεων επεξεργασίας που εισάγει ο νόμος 2472/97 και ιδίως τα άρθρα 4, 5 και 6 τα **απλά δεδομένα** μπορούν καταρχήν να ενταχθούν στο επίπεδο εμπιστοσύνης 1, 2

Εικόνα 8-1: Κατηγοριοποίηση Απλών Δεδομένων

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΑΠΛΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Πληροφορίες που αφορούν – **προσωπική ή/και οικογενειακή κατάσταση**		Τα δεδομένα που αφορούν την **προσωπική ή οικογενειακή κατάσταση** μπορεί να ενταχθούν σε υψηλότερο επίπεδο εμπιστοσύνης, καθώς νομολογιακά έχει κριθεί ότι εμπίπτουν στην κατηγορία του ιδιωτικού βίου
Επάγγελμα - Επαγγελματικές ιδιότητες- **Επαγγελματικές** σχέσεις **Οικονομικές σχέσεις** **Οικονομικά στοιχεία – περιουσιακή κατάσταση**		Για τα **οικονομικά στοιχεία** βλ. και στην ειδική κατηγορία του πίνακα
Έννομες σχέσεις και καταστάσεις δημοσίου και ιδιωτικού δικαίου, όπως - σχέσεις προς πράγματα (κινητά και ακίνητα) - συμβατικές σχέσεις - εκπλήρωση υποχρεώσεων έναντι του δημοσίου/τρίτων (φορολογική και ασφαλιστική ενημερότητα) - διοικητικές άδειες κ.λπ.		

Εικόνα 8-2: Κατηγοριοποίηση Απλών Δεδομένων

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΕΥΑΙΣΘΗΤΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Πρόκειται για δεδομένα που αφορούν	Άρθρο 2β ν. 2472/97 Ορισμός ευαίσθητων δεδομένων	Η ρητή ένταξη των δεδομένων αυτών σε κατηγορία αναβαθμισμένης προστασίας επιτάσσει την ένταξή τους στο ανώτερο επίπεδο εμπιστοσύνης
Φυλετική ή Εθνική προέλευση (όχι ιθαγένεια) Τα πολιτικά φρονήματα Θρησκευτικές ή φιλοσοφικές πεποιθήσεις Συμμετοχή σε συνδικαλιστική οργάνωση Την κοινωνική πρόνοια (θα μπορούσαν να θεωρηθούν δεδομένα οικονομικού χαρακτήρα – αφορούν κυρίως την ιδιότητα «πτωχού» - χρήζοντος κοινωνικής υποστήριξης και συνακόλουθα του λήπτη παροχών κοινωνικής πρόνοιας) Ερωτική ζωή, Ποινικές διώξεις ή καταδίκες Συμμετοχή σε ενώσεις προσώπων που μπορεί να σχετίζεται με ή να αποκαλύπτει ευαίσθητα δεδομένα		
Υγείας (Ιατρικά δεδομένα - *Medical Data*) νοούνται όλα τα δεδομένα όσα έχουν μία σαφή και στενή σχέση με την υγεία (παρελθούσα, παρούσα και μέλλουσα κατάσταση). Ως δεδομένα υγείας νοούνται και όσα παρέχουν μία εκτίμηση για την κατάσταση της υγείας ενός προσώπου.		Η ένταξη των δεδομένων αυτών στο ανώτερο επίπεδο εμπιστοσύνης απορρέει και από τις ρυθμίσεις για το ιατρικό απόρρητο που περιέχονται στον Κώδικα Ιατρικής Δεοντολογίας (άρθρο 13 ν. 3418/2005)

Εικόνα 9: Κατηγοριοποίηση Ευαίσθητων Δεδομένων

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΟΙΚΟΝΟΜΙΚΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το Επίπεδο Εμπιστοσύνης**
Τα οικονομικά δεδομένα, σύμφωνα με την τυπολογία και κατηγοριοποίηση της νομοθεσίας για την προστασία προσωπικών δεδομένων, εντάσσονται στα απλά δεδομένα	Άρθρο 2 α ν. 2472/97	Ένταξη σε συνήθη επίπεδα εμπιστοσύνης
Ωστόσο ορισμένα από αυτά τα δεδομένα καλύπτονται από το φορολογικό απόρρητο και συνεπώς θα πρέπει να αντιμετωπίζονται διαφορετικά	Άρθρο 85 Κώδικα Φορολογίας Εισοδήματος	Τα καλυπτόμενα από το φορολογικό απόρρητο στοιχεία, δηλ. «οι φορολογικές δηλώσεις, τα φορολογικά στοιχεία, οι εκθέσεις και κάθε άλλο στοιχείο του φακέλου που έχει σχέση με τη φορολογία ή άπτεται αυτής» θα πρέπει να εντάσσονται στο ανώτερο επίπεδο εμπιστοσύνης

Εικόνα 10 Κατηγοριοποίηση Οικονομικών Δεδομένων

2.1.6 Ψηφιακά Πιστοποιητικά X.509 v3

Για την πιστοποίηση και την αυθεντικοποίηση των χρηστών χρησιμοποιείτε το πρότυπο X 509. Είναι το πιο κατάλληλο διότι περιέχει κάποια πεδία στα οποία καταχωρείται η απαραίτητη πληροφορία του κάθε χρήστη. Όσο προχωράνε οι εκδόσεις του συμπεριλαμβάνει ολοένα και περισσότερα παιδιά τα οποία βοηθούν στην καλύτερη και πιο γρήγορη πιστοποίηση του χρήστη.

Πεδίο	**Field**
Έκδοση	Version
Αριθμός Σειράς	Serial Number
Αλγόριθμος Υπογραφής	Signature Algorithm
Διακριτικό Όνομα Εκδότη	Issuer DN
Ισχύει Από	Valid From
Ισχύει Μέχρι	Valid To
Διακριτικό Όνομα Υποκειμένου	Subject DN
Δημόσιο Κλειδί Υποκειμένου	Subject Public Key
Μοναδικό Αναγνωριστικό Εκδότη	Issuer Unique Identifier
Μοναδικό Αναγνωριστικό Υποκειμένου	Subject Unique Identifier
Επεκτάσεις	Extensions
Ψηφιακή Υπογραφή	Certification Authority's Digital Signature

Εικόνα 11Πεδία ψηφιακού πιστοποιητικού

Πιο αναλυτικά τα πεδία αυτά είναι:

- Έκδοση, που περιγράφει την έκδοση του προτύπου
- Αριθμός Σειράς, που ξεχωρίζει το κάθε πιστοποιητικό και τοποθετείτε από τον εκδοτη
- Αλγόριθμος Υπογραφής
- Διακριτικό Όνομα Εκδότη, που δείχνει το όνομα του εκδότη καθώς και άλλα επιμέρους πεδία όπως η Χώρα, ο Οργανισμός που είναι υποχρεωτικά

- Ισχύει Από, δηλώνεται η ημέρα έκδοσης του πιστοποιητικού
- Ισχύει Μέχρι, δηλώνεται η ημέρα λήξης του πιστοποιητικού
- Διακριτικό Όνομα Υποκειμένου, δείχνει το όνομα του κατόχου του πιστοποιητικού καθώς και άλλα επιμέρους πεδία όπως η Χώρα, ο Οργανισμός που είναι υποχρεωτικά
- Δημόσιο Κλειδί, δηλώνεται από τον εκδότη του πιστοποιητικού
- Ψηφιακή Υπογραφή, που περιλαμβάνει την υπογραφή του εκδότη του πιστοποιητικού
- Επεκτάσεις, που έχει επιμέρους πεδία όπως:
    - Χρήση Κλειδιού, που περιγράφει την χρήση του κλειδιού στο πιστοποιητικό
    - Εναλλακτικό Όνομα Κειμένου, που δηλώνεται ένα εναλλακτικό όνομα για τον κάτοχο του πιστοποιητικού
    - Ταυτοποίηση Χρήστη, δηλώνεται αν το πιστοποιητικό θα μπορεί να κάνει την ταυτοποίηση του χρήστη
    - Σημεία Διανομής Καταλόγου Ανακληθέντων Πιστοποιητικών

2.2 Τα Επίπεδα της Εμπιστοσύνης

Στις υπηρεσίες ηλεκτρονικής διακυβέρνησης που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα διακρίνονται βαθμοί κρισιμότητας της διαφύλαξης της προστασίας των δεδομένων αυτών. Η κρισιμότητα καθορίζεται βάσει της ποιοτικής κατηγορίας των δεδομένων των πολιτών, καθώς και βάσει των συνεπειών που θα είχε για τους χρήστες, την ατομική ιδιωτικότητα ή/και τον φορέα παροχής υπηρεσιών, η ενδεχόμενη πρόκληση βλάβης. Η βλάβη θα μπορούσε να είχε τη μορφή αποκάλυψης δεδομένων, μη εξουσιοδοτημένης τροποποίησης τους, αποποίησης τους, μη διαθεσιμότητας πρόσβασης δεδομένων, λόγω παράνομης/αθέμιτης χρήσης αυτών, ή για άλλους λόγους. Ο βαθμός κρισιμότητας της παρεχόμενης υπηρεσίας υπαγορεύει και το απαιτούμενο προς κατοχύρωση επίπεδο εμπιστοσύνης της υπηρεσίας, το οποίο εξασφαλίζει την ορθότητα και αξιοπιστία των προσωπικών δεδομένων, παράλληλα με την ορθή διαχείρισή τους.

Ο προσδιορισμός του επιπέδου εμπιστοσύνης της κάθε υπηρεσίας πραγματοποιείται λαμβάνοντας υπ’ όψιν τα προαναφερθέντα κριτήρια. Η επιλογή του επιπέδου εμπιστοσύνης εξυπηρετεί την εξασφάλιση του δικαιώματος πρόσβασης και συμμετοχής στην κοινωνία της πληροφορίας και την εξασφάλιση της ελευθερίας ενημέρωσης για θέματα δημόσιας διαβούλευσης. Παράλληλα,

στοχεύει στην κατοχύρωση της ορθής διαχείρισης των προσωπικών δεδομένων των πολιτών, και στην διαφύλαξη του δικαιώματος τους για ασφαλή και αποτελεσματική τέλεση συναλλαγών με τους δημόσιους φορείς.

2.2.1 Καθορισμός Επιπέδων Εμπιστοσύνης

Το επίπεδο εμπιστοσύνης είναι η το επίπεδο βεβαιότητας που έχει μια ηλεκτρονική υπηρεσία και εξαρτάται από δυο παράγοντες. Ο πρώτος παράγοντας έχει να κάνει με το πόσο ακριβής είναι η ηλεκτρονική ταυτότητα του χρήστη και πόσο τα δεδομένα που απαιτούνται για την επιτυχημένη ολοκλήρωση της ηλεκτρονικής υπηρεσίας είναι σωστά συμπεριλαμβανομένου της ιεραρχίας των απλών, των προσωπικών και των ευαίσθητων δεδομένων. Τα επίπεδα εμπιστοσύνης δείχνουν το κατάλληλο μηχανισμό ασφάλειας που πρέπει να έχει κάθε υπηρεσία βάση της κρισιμότητας της για να προστατευτούν τα δεδομένα αλλά και η ιδιωτικότητα. Επίσης τα επίπεδα δηλώνουν, το πόσο ο κάθε χρήστης είναι αυτός που δηλώνεται στα δικαιολογητικά που καταθέτει , δηλαδή την εμπιστοσύνη υπηρεσίας και χρήστη με σκοπό την ολοκληρωμένη παροχή της υπηρεσίας. Η σημασία των συναλλαγών των χρηστών, η ιεραρχία των δεδομένων που επεξεργάζονται, τα επίπεδα ασφάλειας αποτελούν τους κύριους παράγοντας για την διαμόρφωση των επιπέδων. Τα επίπεδα εμπιστοσύνης διακρίνονται σε επίπεδο μηδέν, επίπεδο ένα, επίπεδο δύο και επίπεδο τρία.

2.2.2 Επίπεδο Εμπιστοσύνης 0

Οι υπηρεσίες που διαχειρίζονται δεδομένα τα οποία είναι δημόσια προσπελάσιμα, αξιοποιούν το επίπεδο εμπιστοσύνης μηδέν. Στοχεύοντας κατά κόρον στην παροχή πληροφοριών στους πολίτες, δεν προϋποθέτουν την παραχώρηση προσωπικών ή οικονομικών δεδομένων από τους χρήστες, ούτε την επικύρωση και επιβεβαίωση της ταυτότητάς τους.

Στο επίπεδο εμπιστοσύνης μηδέν, οι προϋποθέσεις καλής και ασφαλούς λειτουργίας της υπηρεσίας είναι η αξιοπιστία και ακεραιότητα των παρεχόμενων πληροφοριών, η αυθεντικοποίηση της υπηρεσίας, και η ελευθερία πρόσβασης σε αυτή, ούσα διαθέσιμη. Ο μοναδικός πιθανός κίνδυνος από παράνομη ή αθέμιτη χρήση των προς αξιοποίηση δεδομένων είναι η εσφαλμένη πληροφόρηση των πολιτών. Αυτό μπορεί να προκύψει μέσω της κακόβουλης δράσης χρήστη ο οποίος

υποδύεται την υπηρεσία, ενόσω τα κύρια μέτρα ασφάλειας δεν εφαρμόζονται.

2.2.3 Επίπεδο Εμπιστοσύνης 1

Οι ηλεκτρονικές υπηρεσίες που αξιοποιούν δεδομένα με μικρό ή ελάχιστο βαθμό κρισιμότητας (π.χ. ονοματεπώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου), εντάσσονται στο επίπεδο εμπιστοσύνης ένα. Στο επίπεδο ένα, εν αντιθέσει με το επίπεδο εμπιστοσύνης μηδέν, η υπηρεσία θέτει ως προϋπόθεση να λάβει στοιχειώδη επικύρωση της εγκυρότητας της ηλεκτρονικής οντότητας του χρήστη, με σκοπό την διασφάλιση της ορθότητας των υποβαλλόμενων στοιχείων.

Το ΠΨΑ προτείνει να λαμβάνονται ορισμένα μέτρα στο επίπεδο εμπιστοσύνης ένα, με σκοπό τη μείωση της πιθανότητας απειλής της ασφάλειάς των προς ανταλλαγή δεδομένων, και την επίτευξη καλύτερης προστασίας και διαφύλαξής τους. Σε ενδεχόμενη εσφαλμένη διαχείρισή των δεδομένων των χρηστών σε αυτό το επίπεδο, οι συνακόλουθες επιπτώσεις χαρακτηρίζονται δευτερεύουσας σημασίας, καθώς πρόκειται κυρίως για την διαρροή προσωπικών δεδομένων, όπως για παράδειγμα κάποιο ηλεκτρονικό μήνυμα.

Τα προτεινόμενα μέτρα ασφαλείας στο επίπεδο εμπιστοσύνης ένα περιλαμβάνουν την αυθεντικοποίηση και διαθεσιμότητα της υπηρεσίας, την ακεραιότητα των ανταλλασσόμενων στοιχείων και την εμπιστευτικότητα των προς αξιοποίηση προσωπικών δεδομένων. Ακόμη, η Διοίκηση οφείλει να μην προβαίνει σε αποποίηση παραλαβής αιτημάτων των χρηστών, σε αποποίηση αποστολής απαντήσεων των υπαλλήλων που εξυπηρετούν τα κατά περίπτωση αιτήματα χρηστών, ούτε σε αποποίηση αποστολής αιτήσεων ή/και παραλαβής απαντήσεων, από πολίτες χρήστες της υπηρεσίας.

2.2.4 Επίπεδο Εμπιστοσύνης 2

Το επίπεδο εμπιστοσύνης 2 εφαρμόζει ηλεκτρονικές υπηρεσίες που επεξεργάζονται σημαντικά προσωπικά δεδομένα, τα οποία δεν χαρακτηρίζονται ως ευαίσθητα, όπως πληροφορίες για το φύλο, την ημερομηνία γέννησης κ.λπ., καθώς και οικονομικά στοιχεία που δεν έχουν ειδική προστασία. Σε αυτό το επίπεδο εμπιστοσύνης, η εξασφάλιση του ότι οι υπηρεσίες χρησιμοποιούνται μόνο από εξουσιοδοτημένα πρόσωπα είναι κρίσιμη. Σε περίπτωση παραβίασης ή απειλής, οι επιπτώσεις μπορεί να είναι σημαντικές, κυρίως σε σχέση με τη διαρροή προσωπικών, μη ευαίσθητων δεδομένων σε μη εξουσιοδοτημένους χρήστες, χωρίς τη συγκατάθεση του ατόμου που παρείχε τα δεδομένα. Αυτά τα δεδομένα προέρχονται από πιστοποιητικά και άλλα έγγραφα που παρέχονται από τους χρήστες

της υπηρεσίας. Εξαιτίας του κινδύνου για την ασφάλεια των προσωπικών δεδομένων, οι απαιτήσεις ασφαλείας σε αυτό το επίπεδο είναι ουσιώδεις, συμπεριλαμβανομένης της αυθεντικότητας και διαθεσιμότητας της υπηρεσίας, της ακεραιότητας των δεδομένων και της εμπιστευτικότητας των προσωπικών δεδομένων που χρησιμοποιούνται. Επιπλέον, η διοίκηση πρέπει να αποφεύγει να απορρίπτει αιτήματα χρηστών, να μην απαντά σε αιτήματα χρηστών ή να απορρίπτει αιτήσεις ή να μην λαμβάνει απαντήσεις από πολίτες που χρησιμοποιούν την υπηρεσία, καθώς και να διασφαλίζει την αυθεντικότητα των πολιτών-χρηστών.Αρχή φόρμας

2.2.5 Επίπεδο Εμπιστοσύνης 3

Το Επίπεδο Εμπιστοσύνης τρία επιλέγουν και εφαρμόζουν οι ηλεκτρονικές υπηρεσίες οι οποίες διαχειρίζονται την ανταλλαγή προσωπικών δεδομένων τα οποία χαρακτηρίζονται ως ευαίσθητα (π.χ. στοιχεία του ποινικού μητρώου), ή οι υπηρεσίες ηλεκτρονικής ολοκλήρωσης επιπέδου 4, στις οποίες πραγματοποιούνται ηλεκτρονικά οικονομικές συναλλαγές. Καθώς τα εμπλεκόμενα δεδομένα στις συναλλαγές των χρηστών με τις υπηρεσίες αυτές είναι ευαίσθητα ή οικονομικά δεδομένα, οι προκληθείσες συνέπειες ενδεχόμενης βλάβης της ασφάλειας της υπηρεσίας θα είναι εξαιρετικά σημαντικές. Συνεπώς είναι ζωτική και απαραίτητη η διασφάλιση υψηλού βαθμού εμπιστοσύνης για την ηλεκτρονική ταυτότητα των χρηστών.

Στις απαιτήσεις ασφαλείας στο επίπεδο εμπιστοσύνης τρία περιλαμβάνονται η αυθεντικότητα και διαθεσιμότητα της υπηρεσίας, η ακεραιότητα των ανταλλασσόμενων στοιχείων και η εμπιστευτικότητα των προς αξιοποίηση προσωπικών δεδομένων. Ακόμη, η Διοίκηση οφείλει να μην προβαίνει σε αποποίηση παραλαβής αιτημάτων των χρηστών, σε αποποίηση αποστολής απαντήσεων των υπαλλήλων που εξυπηρετούν τα κατά περίπτωση αιτήματα χρηστών, ούτε σε αποποίηση αποστολής αιτήσεων ή/και παραλαβής απαντήσεων, από πολίτες χρήστες της υπηρεσίας. Τέλος, απαιτείται η αυθεντικοποίηση των πολιτών – χρηστών της υπηρεσίας.

2.3 Πλαίσιο κανόνων της Ψηφιακής Αυθεντικοποίησης

Η διαδικασία της ψηφιακής αυθεντικοποίησης πραγματοποιείται μέσω της συλλογής και της διαχείρισης δεδομένων που αφορούν τον χρήστη, με σκοπό την εγγραφή, την ταυτοποίηση και την αυθεντικοποίησή του. Υπάρχουν ορισμένοι κανόνες για την επωνυμία και την εκπροσώπηση νομικών προσώπων που ισχύουν

σε ηλεκτρονικές συναλλαγές με το Δημόσιο. Η συμμόρφωση προς αυτούς τους κανονισμούς είναι ουσιώδης, ιδίως κατά την εκτέλεση των διαδικασιών και τον έλεγχο της νομιμότητας των ατόμων που δικαιούνται να συναλλάσσονται με την επιχείρηση. Επιπλέον, οι διαδικασίες εγγραφής, ταυτοποίησης και αυθεντικοποίησης φυσικών προσώπων απαιτούν τη συλλογή και την επεξεργασία προσωπικών δεδομένων. Κατά την επεξεργασία αυτών των δεδομένων, είναι σημαντικό να λαμβάνονται υπόψη η νομική βάση, οι γενικές αρχές και οι διαδικαστικές προϋποθέσεις νομιμότητας, καθώς και τα δικαιώματα των προσώπων σχετικά με την επεξεργασία αυτών των δεδομένων. Το θεσμικό πλαίσιο καθορίζει τις προϋποθέσεις για την επεξεργασία προσωπικών δεδομένων, λαμβάνοντας υπόψη την κατηγορία των δεδομένων και τις εξαιρέσεις που ισχύουν.

2.3.1 Οι νόμοι σχετικά με την επεξεργασία

Η νομική βάση για την επεξεργασία προσωπικών δεδομένων στις διαδικασίες Εγγραφής, Αυθεντικοποίησης και Ταυτοποίησης φυσικών προσώπων που αλληλεπιδρούν με τη Δημόσια Διοίκηση πηγάζει από νόμιμες πηγές. Αυτές μπορεί να περιλαμβάνουν τη συγκατάθεση του ατόμου, τη συμμόρφωση με νόμιμες υποχρεώσεις από τον υπεύθυνο επεξεργασίας ή την εκτέλεση δημόσιων έργων συμφέροντος. Σύμφωνα με τον Νόμο 2472/97, η συγκατάθεση του ατόμου συνήθως θεωρείται η κύρια νόμιμη βάση για την επεξεργασία προσωπικών δεδομένων. Υπάρχουν, ωστόσο, εξαιρέσεις, όπως όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση υποχρεώσεων του υπεύθυνου επεξεργασίας που ορίζονται από τον νόμο. Σύμφωνα με το Προσωπικό Δικαίωμα στην Προστασία των Δεδομένων (ΠΨΑ), δεν προτείνεται η θέσπιση ειδικής νομοθετικής ρύθμισης, καθώς η γενική νομοθεσία και η συνταγματική ρύθμιση αναγνωρίζουν τη συγκατάθεση ως έναν τρόπο προστασίας των προσωπικών δεδομένων. Επιπλέον, η παροχή συγκατάθεσης εξυπηρετεί την ενημέρωση των πολιτών σχετικά με τις συνέπειες της ηλεκτρονικής χρήσης υπηρεσιών. Η συγκατάθεση πρέπει να είναι ρητή, ειδική και να προηγείται πληροφόρησης. Βάσει του Νόμου 2472/97, η έγκριση του ατόμου θεωρείται η κύρια νομική βάση. Σε περίπτωση παρέκκλισης ή έλλειψης έγκρισης, χρησιμοποιούνται άλλες νομικές βάσεις που έχουν προαναφερθεί. Ενδέχεται να μην απαιτείται η συναίνεση του ατόμου, αν δεν παραβιάζεται το δικαίωμα προστασίας των προσωπικών δεδομένων, εφόσον υπάρχει νόμος που καθορίζει τις διαδικασίες εγγραφής, ταυτοποίησης και αυθεντικοποίησης από το Δημόσιο. Η συγκατάθεση πρέπει να είναι ελεύθερη,

ρητή και ειδική δήλωση βούλησης, με πλήρη επίγνωση των σχετικών πληροφοριών. Η ενημέρωση περιλαμβάνει τουλάχιστον τον σκοπό της επεξεργασίας, τα δεδομένα που επεξεργάζονται, τους αποδέκτες των δεδομένων και τα στοιχεία του υπεύθυνου επεξεργασίας και του εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί ανά πάσα στιγμή, χωρίς υποχρέωση αναδρομικής επίδρασης. Σύμφωνα με την Αρχή Προστασίας Προσωπικών Δεδομένων, η νομική βάση της επεξεργασίας είναι η ελεύθερη, ρητή και ειδική συναίνεση των υποκειμένων των δεδομένων, σε συνδυασμό με το νόμο 3471/2006. Σε περίπτωση επεξεργασίας ευαίσθητων δεδομένων, η συναίνεση πρέπει να είναι υποχρεωτικά γραπτή. Η ηλεκτρονική παροχή συγκατάθεσης μπορεί να γίνει δεκτή, υπό την προϋπόθεση της πλήρους επίγνωσης των επιπτώσεων από τον συνδρομητή ή τον χρήστη.

2.3.2 Η χρήση των γενικών Αρχών της επεξεργασίας

Η Αρχή Προστασίας Προσωπικών Δεδομένων έχει θέσει όρους για την επεξεργασία κατά την αυθεντικοποίηση και την ταυτοποίηση, βασιζόμενη στον νόμο 2472/97 στο άρθρο 4. Απαιτείται η συλλογή μόνο των απαραίτητων προσωπικών δεδομένων που είναι απαραίτητα. Συγκεκριμένα, απαγορεύεται η χρήση των δεδομένων για σκοπούς μη συμβατούς με αυτούς για τους οποίους συλλέχθηκαν. Οι παραπάνω αρχές εφαρμόζονται και στη διαδικασία της ταυτοποίησης. Ανάλογα με την υπηρεσία και το επίπεδο εμπιστοσύνης, καθορίζεται αν και ποια προσωπικά δεδομένα επιτρέπεται να συλλέγονται και να επεξεργάζονται. Για υπηρεσίες όπου δεν απαιτείται η ταυτοποίηση του χρήστη, δεν πρέπει να γίνεται συλλογή προσωπικών δεδομένων. Για υπηρεσίες πληροφόρησης, δεν απαιτείται ο προσδιορισμός της IP διεύθυνσης του αποδέκτη εάν δεν είναι απαραίτητος για την παροχή ή τη χρέωση της αντίστοιχης υπηρεσίας. Για απλές υπηρεσίες όπως η αποστολή ενημερωτικών δελτίων, αρκεί μόνο η καταχώριση του ηλεκτρονικού ταχυδρομείου του παραλήπτη, χωρίς την ανάγκη συλλογής και επεξεργασίας προσωπικών του δεδομένων. Σε περίπτωση που απαιτείται αυθεντικοποίηση και ταυτοποίηση του συναλλασσόμενου για την παροχή μιας υπηρεσίας off-line, η συλλογή προσωπικών δεδομένων πρέπει να είναι απαραίτητη και περιορισμένη στο ελάχιστον απαιτούμενο για το σκοπό. Αν η υπηρεσία απαιτεί αυθεντικοποίηση και ταυτοποίηση κατά την ηλεκτρονική διαδικασία, τότε η συλλογή προσωπικών δεδομένων πρέπει να γίνεται με βάση την ανάγκη και την αποτελεσματική παροχή της υπηρεσίας.Για να διασφαλιστεί η ποιότητα των

δεδομένων, είναι ζωτικής σημασίας η ακρίβεια αυτών. Αυτό σημαίνει ότι πρέπει να είναι αληθή και να ενημερώνονται τακτικά. Στοιχεία που μπορούν να θέσουν σε κίνδυνο τα άτομα, όπως ανακρίβειες ή μη ενημερωμένα δεδομένα, πρέπει να αποφεύγονται. Τα δεδομένα είναι αναγκαίο να κρατιούνται σε τέτοια μορφή που να πραγματοποιείται εύκολα η ταυτοποίηση των οντοτήτων που αφορούν τα δεδομένα που υπόκεινται σε επεξεργασία. Για να διαγραφούν ή αλλιώς να καταστραφούν τα δεδομένα υπεύθυνη είναι η Αρχή Προστασίας Προσωπικών Δεδομένων, όπως επίσης είναι αυτή η οποία μπορεί να μην διαγράψει τα δεδομένα αν αυτή κρίνει ότι είναι χρήσιμα είτε για στατιστικούς λόγους.

2.3.3 Τα Δικαιώματα των Προσώπων

Η ενημέρωση της κάθε οντότητας για την συλλογή και την επεξεργασία των δεδομένων της Είναι απαραίτητη. Η νομοθεσία γενικότερα περιλαμβάνει συγκεκριμένους κανόνες για τα δικαιώματα των προσώπων σχετικά με την προστασία των προσωπικών τους δεδομένων. Έτσι λοιπόν ο υπεύθυνος θα πρέπει με επεξηγηματικό τρόπο να ενημερώνει την Κάθε οντότητα που τα δεδομένα της υποστούν επεξεργασία για την ταυτότητα του, Το λόγο που επεξεργάζονται τα δεδομένα, ποιοι είναι οι δέκτες της επεξεργασίας καθώς για το αν υπάρχει όχι δικαίωμα πρόσβασης. Εξίσου σημαντικό είναι ο υπεύθυνος να ενημερώνει Για το αν η οντότητα είναι υποχρεωμένοι η οχι να παρέχει κάποια στοιχεία Καθώς και αν υπάρχουν επιπτώσεις. Σύμφωνα με το νόμο δεν υπάρχει κάποιος άλλος τρόπος ενημέρωσης. Τέλος η οντότητα έχει δικαίωμα πρόσβασης διορθώσεις αλλά και άρνησης για τα δεδομένα που επεξεργάστηκαν.

2.3.4 Συμβιβασμός με Διαδικαστικές Προϋποθέσεις

Όπως έχει προαναφερθεί, η συλλογή των δεδομένων και η επεξεργασία τους θα πρέπει να κοινοποιείται στην αρχή προστασίας προσωπικών δεδομένων. Η διαδικασία που θα πρέπει να ακολουθήσει ο υπεύθυνος είναι να καταγράφει το όνομα και την διεύθυνση, να δηλώνει την διεύθυνση του αρχείου και το λόγο που τα δεδομένα προσωπικού χαρακτήρα θα επεξεργαστούν καθώς επίσης και το είδος των δεδομένων που υπόκειται σε επεξεργασία. Ο υπεύθυνος ακόμη θα πρέπει να δηλώσει την χρονική περίοδο καθώς και το διάστημα που θα γίνει η επεξεργασία, τους δέκτες της επεξεργασίας των δεδομένων να τους ενημερώσει κι αν τυχόν χρειαστεί τα δεδομένα αυτά να σταλθούν σ’ άλλες χώρες θα πρέπει να δηλωθεί. Τελευταίο και εξίσου σημαντικό είναι ότι ο υπεύθυνος θα πρέπει να καταγράψει τα

στοιχεία ασφαλείας του αρχείου. Επιπλέον αν και τις διαδικασίες ταυτοποίησης και αυθεντικοποίησης υπολογίζεται να γίνει κάποια διασύνδεση θα πρέπει να ζητηθεί εκ νέου άδεια από την Αρχή. Πιο αναλυτικά αν κάποιο από τα αρχεία που πρόκειται να γίνει διασύνδεση περιλαμβάνει ευαίσθητα δεδομένα ή Αν κατά τη διάρκεια της διασύνδεσης διαρρεύσουν κάποια ευαίσθητα δεδομένα Πρέπει να ληφθεί εκ νέου άδεια. Για την λήψη της άδειας αυτής θα πρέπει ο υπεύθυνος να αναφερθεί στους λόγους για τους οποίους πρέπει να γίνει διασύνδεση, να περιγράψει το είδος των δεδομένων, Να ενημερώσει για το χρονικό διάστημα για το οποίο θα γίνει ίδια σύνδεση καθώς και περισσότερες λεπτομέρειες για την βέλτιστη προστασία των δεδομένων και της ιδιωτικότητας. Με βάση τα παραπάνω μπορεί να καταλάβει κάποιος ότι το κανονιστικό πλαίσιο σχετικά με την επεξεργασία των προσωπικών δεδομένων είναι πλήρες.

2.4 Ταυτοποίηση κατά την παροχή των υπηρεσιών

Η αναφορά στον τρόπο με τον οποίο ο χρήστης αποκαλύπτει την ταυτότητα του καθώς αλληλεπιδρά με τις ηλεκτρονικές υπηρεσίες της κυβέρνησης είναι η διαδικασία ταυτοποίησης, όπως ορίζεται από το ΠΨΑ. Οι πολίτες χρησιμοποιούν διάφορα μέσα για την ταυτοποίησή τους κατά τις συναλλαγές τους με το Δημόσιο οπότε η επιλογή της διαδικασίας ταυτοποίησης που θα χρησιμοποιηθεί στις αντίστοιχες υπηρεσίες διακυβέρνησης θα έχει σημαντικές επιπτώσεις στο ΠΨΑ. Οι διαφορετικές μέθοδοι ταυτοποίησης επιφέρουν διαφορετικούς νομικούς, θεσμικούς ή ακόμα και τεχνικούς περιορισμούς. Λαμβάνοντας υπόψιν το Σύνταγμα και το νομικό πλαίσιο, καθώς και τις υφιστάμενες μεθόδους ταυτοποίησης για τις συναλλαγές με το Δημόσιο, προτείνεται η ταυτοποίηση των χρηστών με μοναδικά αναγνωριστικά ανά υπηρεσία μέσω της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ).

Η συγκεκριμένη προτεινόμενη τεχνική ταυτοποίησης προβλέπει τη χρήση διαφορετικού αναγνωριστικού για κάθε υπηρεσία, οι διαδικασίες εγγραφής και αυθεντικοποίησης διενεργούνται στην ΚΔΠ, χωρίς την ανάγκη προηγούμενης εγγραφής των χρηστών στις ξεχωριστές ηλεκτρονικές υπηρεσίες. Αυτό έχει ως αποτέλεσμα να μη δημιουργεί κάποιο πρόβλημα στην ολοκλήρωση των παρεχόμενων υπηρεσιών.

Κατά το στάδιο της εγγραφής στην ΚΔΠ, ο χρήστης οφείλει να καταχωρίσει τα διαφορετικά αναγνωριστικά που απαιτούνται από τον εκάστοτε φορέα προκειμένου να τον ταυτοποιήσει και αν επιθυμεί αυτά μπορούν να αποθηκευτούν στον ψηφιακό

του φάκελο αναγνωριστικών του συγκεκριμένου χρήστη. Τέτοια χαρακτηριστικά μπορεί να είναι ο αριθμός δελτίου ταυτότητας, το ΑΜΚΑ, το ΑΦΜ.

Στην περίπτωση αίτησης του χρήστη για αξιοποιήση μιας ψηφιακή υπηρεσίας, η διαδικασία που ακολουθείται είναι ελέγχος του ψηφιακού φακέλου των αναγνωριστικών του από την Κεντρική Διαδικτυακή Πύλη, προκειμένου να εντοπίσει το κατάλληλο αναγνωριστικό για την αυθεντικοποίησή του στην εκάστοτε υπηρεσία. Το αναγνωριστικό αποστέλλεται στον αρμόδιο της συγκεκριμένης υπηρεσίας, εφόσον έχει θετικό αποτέλεσμα η έρευνα, προκειμένου να γίνει η αυθεντικοποίηση του χρήστη και να εκκινήσει η διαδικασία επαλήθευσής του. Σε περίπτωση ανεπιτυχούς αναζήτησης, η Κεντρική Διαδικτυακή Πύλη ενημερώνει τον χρήστη ότι δεν είναι εφικτή η χρήση της εν λόγω ψηφιακής υπηρεσίας.

2.5 Επίπεδα Αυθεντικοποίησης

Η διαδικασία της αυθεντικοποίησης αναφέρεται στον έλεγχο και την επιβεβαίωση της ταυτότητας των χρηστών μέσω των διαπιστευτηρίων που παρέχουν. Υπάρχουν διάφοροι τρόποι αυθεντικοποίησης ανάλογα με το επίπεδο εμπιστοσύνης που απαιτείται. Η υπηρεσία με υψηλότερο επίπεδο εμπιστοσύνης απαιτεί ισχυρότερους μηχανισμούς αυθεντικοποίησης. Η αυθεντικοποίηση ενός χρήστη με ισχυρό μηχανισμό δίνει την δυνατότητα στον χρήστη να αποκτήσει πρόσβαση και σε υπηρεσίες με χαμηλότερο επίπεδο αυθεντικοποίησης, καθώς έχει ήδη επαληθευθεί με πιο αξιόπιστο τρόπο από αυτόν που απαιτείται από την υπηρεσία. Το ΠΨΑ καθορίζει τρία επίπεδα αυθεντικοποίησης με βάση τους μηχανισμούς και τα χαρακτηριστικά αυθεντικοποίησης.

2.5.1 Επίπεδο Αυθεντικοποίησης 0

Η οντότητα μπορεί να αποκτήσει πρόσβαση στις δημόσιες πληροφορίες και δεν χρειάζεται να αυθεντικοποιηθεί ο χρήστης. Τέτοιες υπηρεσίες είναι αυτές που περιλαμβάνουν πληροφοριακό υλικό. Οι απαιτήσεις ασφάλειας του επιπέδου αυθεντικοποίησης 0 είναι η ακεραιότητα του παρεχόμενου πληροφοριακού υλικού και η αυθεντικότητα της υπηρεσίας.

Στο επίπεδο αυτό δεν χρειάζεται επιβεβαίωση της ορθότητας της ψηφιακής ταυτότητας , γι αυτό το λόγο συνδέεται με το επίπεδο εμπιστοσύνης 0. Η αξιοποιήση

υπηρεσιών που εντάσσονται στο επίπεδο αυθεντικοποίησης 0, δεν απαιτεί κάποιον μηχανισμό αυθεντικοποίησης.

2.5.2 Επίπεδο Αυθεντικοποίησης 1

Το επίπεδο 1 σχετίζεται με υπηρεσίες που έχουν πρόσβαση οντότητες οι οποίες είναι εξουσιοδοτημένες, όπως για παράδειγμα, μια υπηρεσία που δίνει την ευκαιρία στους πολίτες να αιτηθούν επεξεργασία ή ολοκλήρωση κάποιας διαδικασίας με κάποιον φορέα του Δημοσίου με φυσική παρουσία. Το επίπεδο αυτό συνδέεται με το επίπεδο εμπιστοσύνης 1 και το επίπεδο εμπιστοσύνης 2 διότι για την επιβεβαίωση της ταυτότητας του χρήστη είναι αναγκαία μέχρι μέτρια βεβαιότητα. Στο επίπεδο αυτό, το πλαίσιο της ασφάλειας απλώνεται σε τρία στάδια. Στην εμπιστευτικότητα και στην ακεραιότητα σχετικά με τα δεδομένα που γίνεται η ταυτοποίηση του πολίτη και στα διαπιστευτήρια του καθώς και στα δεδομένα μου γίνονται λήψη από την υπηρεσία. Το τελευταίο στάδιο της ασφάλειας έχει να κάνει με την αυθεντικότητα της υπηρεσίας.

2.5.3 Επίπεδο Αυθεντικοποίησης 2

Το επίπεδο 2 σχετίζεται με υπηρεσίες που έχουν πρόσβαση οντότητες οι οποίες είναι αναγκαίο να ταυτοποιηθούν και να είναι εξουσιοδοτημένες αφού οι υπηρεσίες που σχετίζεται το επίπεδο αυτό είναι κρίσιμο πρόσβαση να έχουν εξουσιοδοτημένα πρόσωπα. Οι υπηρεσίες που ασχολείται το επίπεδο αυτό είναι υπηρεσίες επεξεργασίας ευαίσθητων προσωπικών δεδομένων και ολοκλήρωση οικονομικών συναλλαγών. Το επίπεδο αυτό συνδέεται με το επίπεδο εμπιστοσύνης 3 διότι για την επιβεβαίωση της ταυτότητας του χρήστη είναι αναγκαία υψηλή βεβαιότητα. Στο επίπεδο αυτό, το πλαίσιο της ασφάλειας απλώνεται σε έξι στάδια. Στην εμπιστευτικότητα και στην ακεραιότητα σχετικά με τα δεδομένα που γίνεται η ταυτοποίηση του πολίτη και στα διαπιστευτήρια του, στα δεδομένα που στέλνει ο χρήστης στην υπηρεσία καθώς και στα δεδομένα μου γίνονται λήψη από την υπηρεσία. Τα επόμενα στάδια είναι αυτά της μη αποποίησης της αποστολής/λήψης δεδομένων, της ύπαρξης εποπτείας, της χρονοσήμανσης των διαδικασιών. Το τελευταίο στάδιο της ασφάλειας έχει να κάνει με την αυθεντικότητα της υπηρεσίας.

2.6 Επίπεδα Εγγραφής

Τα επίπεδα εγγραφής έχουν να κάνουν με τις διαδικασίες που μια οντότητα θέλει να κάνει χρήση και διαθέτει όλα εκείνα τα δικαιολογητικά ώστε να πάρει έγκριση. Για να προσδιοριστεί το κατάλληλο επίπεδο εγγραφής το πλαίσιο ψηφιακής αυθεντικοποίησης αναφέρει ότι θα πρέπει να ληφθεί υπόψη το επίπεδο εμπιστοσύνης της υπηρεσίας. Αν το επίπεδο εμπιστοσύνης είναι υψηλό τότε και το επίπεδο εγγραφής θα είναι υψηλό και θα πρέπει να ληφθεί ακόμη υπόψη και το διακριτικό αυθεντικοποίησης που θα χρησιμοποιηθεί κατά την αυθεντικοποίηση. Για τις υπηρεσίες που ασχολούνται με τις οικονομικές συναλλαγές η εγγραφή δεν θα πρέπει να ολοκληρώνεται μόνο με τη συμπλήρωση μιας φόρμας αλλά θα πρέπει να υπάρξει διαδικασία που θα επικυρώνει την ταυτότητα της οντότητας ώστε να χρησιμοποιήσει την υπηρεσία. Το επίπεδο εγγραφής μιας υπηρεσίας δεν είναι ανάγκη να είναι ίδιο με το επίπεδο εμπιστοσύνης ή με το επίπεδο αυθεντικοποίησης.

2.6.1 Επίπεδο Εγγραφής 0

Στο επίπεδο εγγραφής 0 περιλαμβάνονται όλες εκείνες οι διαδικασίες που παρέχουν απλά πληροφορίες. Για το επίπεδο εγγραφής 0 δεν υπάρχει κανένας μηχανισμός ασφαλείας ή αυθεντικοποίησης και επίσης τις διαδικασίες του επιπέδου αυτού θα πρέπει να ακολουθήσουν οι υπηρεσίες που είναι στο επίπεδο αυθεντικοποίησης 0.

2.6.2 Επίπεδο Εγγραφής 1

Στο επίπεδο εγγραφής 1 περιλαμβάνονται όλες εκείνες οι διαδικασίες που πρέπει να γίνουν ώστε ο χρήστης να έχει πρόσβαση σε υπηρεσίες που γίνεται επεξεργασία δεδομένων. Στο επίπεδο εγγραφής 1 διασφαλίζεται η εμπιστευτικότητα των δεδομένων που στέλνει ο χρήστης, των δεδομένων που στέλνεται στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Επίσης διασφαλίζεται η ακεραιότητα των δεδομένων που αποστέλλει ο χρήστης, των δεδομένων που στέλνετε στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Ακόμη διασφαλίζεται η μη αποποίηση αποστολής και λήψης δεδομένων με την υποβολή μιας αίτησης Και την έκδοση διαπιστευτηρίων.

2.6.3 Επίπεδο Εγγραφής 2

Στο επίπεδο εγγραφής 2 περιλαμβάνονται οι διαδικασίες που πρέπει να γίνουν ώστε ο χρήστης να εγγραφεί σε υπηρεσίες επιπέδου ένα με τη μόνη διαφοροποίηση ότι το έγγραφο του χρήστη μπορεί να σταλθεί ηλεκτρονικά. Στο

επίπεδο εγγραφής 2 διασφαλίζεται η εμπιστευτικότητα των δεδομένων που στέλνει ο χρήστης, των δεδομένων που στέλνεται στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Επίσης διασφαλίζεται η ακεραιότητα των δεδομένων που αποστέλλει ο χρήστης, των δεδομένων που στέλνετε στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Επίσης διασφαλίζεται η μη αποποίηση αποστολής και λήψης δεδομένων καθώς και η συμμετοχή σε ηλεκτρονικές συναλλαγές.

2.6.4 Επίπεδο Εγγραφής 3

Στο επίπεδο εγγραφής 3 περιλαμβάνονται όλες οι διαδικασίες εκείνες που πρέπει να γίνουν ώστε να εγγραφεί ο χρήστης σε υπηρεσίες που γίνεται επεξεργασία ευαίσθητων προσωπικών δεδομένων οικονομικών δεδομένων. Στο επίπεδο εγγραφής 3 διασφαλίζεται η εμπιστευτικότητα των δεδομένων που στέλνει ο χρήστης, των δεδομένων που στέλνεται στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Επίσης διασφαλίζεται η ακεραιότητα των δεδομένων που αποστέλλει ο χρήστης, των δεδομένων που στέλνετε στο χρήστη καθώς και τα διαπιστευτήρια του χρήστη. Επίσης διασφαλίζεται η μη αποποίηση αποστολής και λήψης δεδομένων καθώς και η συμμετοχή σε ηλεκτρονικές συναλλαγές.

Παρακάτω παρουσιάζεται η συσχέτιση μεταξύ των επιπέδων εμπιστοσύνης, των επιπέδων αυθεντικοποίησης, των επιπέδων εγγραφής.

<table>
<tr><th>Επίπεδο Εμπιστοσύνης</th><th>Επίπεδο Εγγραφής</th><th>Επίπεδο Αυθεντικοποίησης</th><th>Μηχανισμός Αυθεντικοποίησης</th></tr>
<tr><td>0</td><td>0</td><td>0</td><td>-</td></tr>
<tr><td>1</td><td>1</td><td rowspan="2">1</td><td>Συνθηματικά</td></tr>
<tr><td>2</td><td>2</td><td>Συνθηματικά μιας Χρήσης</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">3</td><td rowspan="2">2</td><td>Πιστοποιητικά
(Διακριτικό Χαλαρής Αποθήκευσης)</td></tr>
<tr><td>Πιστοποιητικά
(Διακριτικό Σκληρής Αποθήκευσης)</td></tr>
</table>

Εικόνα 12Συσχέτιση Επιπέδων Εμπιστοσύνης, Εγγραφής Αυθεντικοποίησης

Κεφάλαιο 3 Διαθεσιμότητα ,Προσβασιμότητα και Διαλειτουργικότητα

Κύριος στόχος της κυβέρνησης είναι να μπορέσει να δώσει την ευκαιρία στους πολίτες να έχουν πρόσβαση στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης. Οι πολίτες, είναι οι αυστηρότεροι κριτές των έργων της κυβέρνησης, έτσι και του πληροφοριακού συστήματος της ηλεκτρονικής διακυβέρνησης οι πολίτες θέλουν να έχουν πρόσβαση οποιαδήποτε στιγμή της ημέρας, από οποιοδήποτε σημείο του πλανήτη μόνο με τον υπολογιστή τους, σε οποιαδήποτε από τις ηλεκτρονικές υπηρεσίες παρέχει το κράτος.

3.1 Διαλειτουργικότητα

Η διαλειτουργικότητα είναι συνυφασμένη με την ηλεκτρονική διακυβέρνηση, αφού με αυτή μεταφέρονται πληροφορίας με σωστό τρόπο από το ένα πληροφοριακό σύστημα σε ένα άλλο της δημόσιας διοίκησης τέλειο. Η διαλειτουργικότητα ακόμα χωρίζεται σε οργανωσιακή, σε σημασιολογική και σε τεχνική. Η οργανωσιακή διαλειτουργικότητα έχει να κάνει με τη συνεργασία διαφόρων τομέων της διοίκησης ως προς τους στόχους, τις διαδικασίες και τη συνεργασία που έχουν όμως κοινό στόχο την ανταλλαγή πληροφοριών. Η σημασιολογική διαλειτουργικότητα έχει να κάνει με την καθιέρωση ενός κοινού εννοιολογικού συστήματος με σκοπό μετά την ανταλλαγή πληροφοριών μεταξύ των τμημάτων να γίνεται σωστά η κατανόηση και η αξιοποίηση των πληροφοριών. Τέλος η τεχνική διαλειτουργικότητα έχει να κάνει με τις διασυνδέσεις που γίνονται ώστε η πληροφορία να μεταφέρεται και να αξιοποιείται απευθείας.

3.2 Ευρωπαϊκό Πλαίσιο

Η Ευρωπαϊκή Ένωση για να παρέχει υπηρεσίες φιλικές προς το χρήστη εξασφαλίζοντας την διαλειτουργικότητα συστημάτων και υπηρεσιών, θέσπισε το ευρωπαϊκό πλαίσιο διαλειτουργικότητας. Κάποιες από τις αρχές του ευρωπαϊκού πλαισίου είναι, οι αποφάσεις να παίρνονται με γνώμονα το καλό του πολίτη, να γίνεται αξιολόγηση των αναγκών και να προσδιορίζονται ποιες από τις υπηρεσίες θα παρέχονται στους πολίτες πίεση στις επιχειρήσεις και με ποιον τρόπο θα γίνεται αυτό. Οι υπηρεσίες αυτές θα πρέπει να είναι προσβάσιμες από όλους τους πολίτες ή

από όλες τις επιχειρήσεις ακόμα δεν θα πρέπει εξαιρείται κανένας. Θα πρέπει να υπάρχουν σε αρκετές γλώσσες χωρίς να λιώνετε το επίπεδο της υπηρεσίας. Λόγω λοιπόν, της αλληλεπίδρασης που δημιουργείται μεταξύ χρηστών και δημόσιας διοίκησης, είναι αναγκαίο να υπάρχει ένα επίπεδο εμπιστοσύνης που να προσδιορίζεται σε σχετικούς κανόνες. Επιπλέον όλοι οι φορείς της δημόσιας διοίκησης θα πρέπει να συνεργαστούν ώστε οι υπηρεσίες και η πληροφορίες που παρέχει ο κάθε φορέας να διαμοιράζεται με σκοπό τι είναι αποδοτικότερη παροχή υπηρεσιών. Οι πληροφορίες που υπάρχουν στο πληροφοριακό σύστημα θα πρέπει να διατηρούνται λαμβάνοντας υπόψη την εξασφάλιση της αναγνωσιμότητας της αξιοπιστίας και της ακεραιότητας των πληροφοριών. Για να μπορέσει να αναβαθμιστεί το σύστημα και για να αξιοποιούνται πλήρως τυχόν αλλαγές που υλοποιούνται στην διαδικασία του συστήματος, θα πρέπει οι οντότητες να επικοινωνούν μεταξύ τους να ανταλλάσσουν πληροφορίες και γνώσεις για τις πραγματικές ανάγκες που έχουν καθημερινά.

Κεφάλαιο 4 Απαιτήσεις ασφάλειας και ιδιωτικότητας σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης

Το κεφάλαιο αυτό αναφέρεται στην προστασία της διωτικότητας των δεδομένων και τόνιζεται η αναγκαιότητα της στα Πληροριακά Συστήματα. Επίσης παρουσιάζεται και το θεσμικό πλαίσιο που έχει ισχύ στην Ευρώπη και στην Ελλάδα. Γίνεται αναφορά στις απειλές που υπάρχουν κατά της συναλλαγές των πολιτών και των επιχειρήσεων καθώς επίσης και τις επιπτώσεις που έχουν πάνω τους αλλά και στους παρόχους των υπηρεσιών.

4.1 Η Έννοια της Ιδιωτικότητας

Η Ιδιωτικότητα Πληροφοριών (Informational Privacy) εστιάζει στον έλεγχο και τον τρόπο συλλογής, αποθήκευσης, επεξεργασίας και διανομής δεδομένων. Η Εδαφική Ιδιωτικότητα (Territorial Privacy) συνδέεται με την προστασία του προσωπικού χώρου, όπως η οικογένεια και το εργασιακό περιβάλλον. Η Σωματική Ιδιωτικότητα (Bodily Privacy) αφορά την προστασία του ατόμου από ανεπιθύμητες επεμβάσεις, όπως εξετάσεις, ιατρικές επεμβάσεις ή παραβιάσεις του σωματικού απορρήτου.

Τα δεδομένα έχουν αναδειχθεί και καθιερωθεί ως μια "αυτόνομη" έννοια στη διαδικασία της επεξεργασίας τους, ειδικά με την αύξηση και εξάπλωση της αυτοματοποιημένης επεξεργασίας δεδομένων. Αυτή η σύνδεση υποδεικνύει την "δεδομένη" φύση τους ως τεχνικού όρου και μέρους ενός συστήματος επεξεργασίας, με τα "δεδομένα" να αποτελούν στοιχεία μιας "επεξεργασμένης" πληροφορίας, δηλαδή στοιχεία που έχουν υποστεί αυτοματοποιημένη επεξεργασία. Το δεδομένο θεωρείται μια ουδέτερη έννοια που αναφέρεται στο περιεχόμενό του, ενώ η πληροφορία αναφέρεται στην χρησιμότητά του. Αν και υπάρχουν διαφορές στη σημασιολογία τους, οι δύο έννοιες θεωρούνται συνώνυμες.

Στο πεδίο της Ηλεκτρονικής Διακυβέρνησης, η συζήτηση για την ιδιωτικότητα επικεντρώνεται κυρίως στην ιδιωτικότητα των πληροφοριών και την ιδιωτικότητα της επικοινωνίας, καθώς η εδαφική και σωματική ακεραιότητα δεν επηρεάζονται άμεσα. Η αποτελεσματική παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης εξαρτάται σημαντικά από την διασφάλιση της ιδιωτικότητας των δεδομένων και των πληροφοριών που χρησιμοποιούνται για αυτήν. Η επεξεργασία των προσωπικών δεδομένων αποτελεί κριτήριο για τη λήψη αποφάσεων στα πλαίσια των κρατικών ενεργειών και της δράσης του Δημοσίου. Οι απειλές που

προκύπτουν μπορούν να είναι είτε εγγενείς, που σχετίζονται με τη χρήση του Διαδικτύου ως μέσου επικοινωνίας, είτε εστιάζουν σε συγκεκριμένα ζητήματα, όπως η χρήση αναγνωριστικών χρηστών και η σύνδεση δεδομένων και πληροφοριών.

4.1.1 Ιδιωτικότητα Δεδομένων στην Ηλεκτρονική Διακυβέρνηση

Όσον αφορά την ιδιωτικότητα των πληροφοριών, ο πιο γνωστός ορισμός προέκυψε το 1967: "η ιδιωτικότητα είναι η αξίωση ιδρυμάτων, ομάδων και ατόμων να καθορίζουν πώς, πότε και κατά πόσο θα μεταβιβάζονται σε τρίτους οι πληροφορίες που τους αφορούν." Ένα σημαντικό στοιχείο στην έννοια της Ιδιωτικότητας Πληροφοριών είναι η διάκριση μεταξύ δημόσιων και ιδιωτικών πληροφοριών με τις τελευταίες να χρήζουν προστασίας. Η αξιολόγηση κάθε πληροφορίας εξαρτάται από διάφορους νομικούς παράγοντες και βασίζεται στο ισχύον κανονιστικό πλαίσιο.

Λόγω της ευρείας εφαρμογής των Πληροφορικών Συστημάτων Ηλεκτρονικής Διακυβέρνησης και τη συλλογή, επεξεργασία και αποθήκευση τεράστιου όγκου πληροφορίας, η έννοια της Ιδιωτικότητας Πληροφοριών αποκτά ιδιαίτερη σημασία. Οι πληροφορίες αυτές περιλαμβάνουν από οικονομικά, δημογραφικά και ιατρικά δεδομένα, μέχρι πληροφορίες σχετικές με πολιτικές ή θρησκευτικές αντιλήψεις. Επιπλέον, η Δημόσια Διοίκηση, υποχρεούται να παρέχει διαφοροποίηση στις υπηρεσίες παρέχοντας όλο το φάσμα των διαθέσιμων πληροφοριών, κάτι που δεν συμβαίνει στις περιπτώσεις του ηλεκτρονικού εμπορίου ή μάθησης, όπου υπάρχει η επιλογή παροχής μέρους μόνο πληροφοριών μαζί με την παροχή της υπηρεσίας

4.1.2 Απαιτήσεις Ασφάλειας και Ιδιωτικότητας Δεδομένων

Όσον αφορά την ιδιωτικότητα και την ασφάλεια των δεδομένων περιλαμβάνουν: ακεραιότητα, που περιλαμβάνει την προστασία από μη εξουσιοδοτημένη διαγραφή, τροποποίηση ή εισαγωγή δεδομένων, την εμπιστευτικότητα, που αποσκοπεί στην προστασία από διαρροή δεδομένων σε άγνωστες οντότητες και την αυθεντικότητα, που ορίζει η εγγύηση της ταυτότητας κάθε οντότητας. Επιπλέον, τη μη αποποίηση, που περιλαμβάνει την προστασία από την μη πραγματοποίηση συγκεκριμένης διαδικασίας και τέλος, τη διαθεσιμότητα, που αφορά την προστασία από την άρνηση διάθεσης των δεδομένων.

Η ιδιωτικότητα παρουσιάζει επιπλέον απαιτήσεις λόγω της μετάβασής της από μια γενική έννοια σε τεχνική ανάγκη. Αυτές οι απαιτήσεις περιλαμβάνουν την Εξουσιοδότηση, που περιλαμβάνει τη διαδικασία απόκτησης πρόσβασης σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος, την Αυθεντικοποίηση, δηλαδή τη διαδικασία επαλήθευσης της ψηφιακής ταυτότητας του χρήστη, η οποία αν και κυρίως απαίτηση ασφάλειας, συνεισφέρει επίσης στην προστασία της ιδιωτικότητας ενός πληροφοριακού συστήματος. Επιπρόσθετα, περιλαμβάνουν την Προστασία Δεδομένων, δηλαδή τη διασφάλιση της προστασίας των δεδομένων σύμφωνα με τις αρχές της Ευρωπαϊκής Οδηγίας 1995/46/ΕΚ, την Αναγνώριση, που συνδέεται με τη διαδικασία επαλήθευσης των απαιτούμενων στοιχείων για την κάλυψη των πρώτων δύο απαιτήσεων, την Ψευδωνυμία, που αφορά τη διαδικασία προστασίας της αναγνώρισης μιας οντότητας από μη εξουσιοδοτημένα μέρη. Τέλος, την Ανωνυμία, που εγγυάται τη μη αναγκαιότητα αποκάλυψης της ταυτότητας ενός χρήστη που θέλει να επικοινωνήσει με έναν άλλον χρήστη, τη Μη-παρατηρησιμότητα που αφορά στην εξασφάλιση της ιδιωτικότητας ενός χρήστη από ενδεχόμενους επιτιθέμενους, αποφεύγοντας την παρατήρηση ή τον εντοπισμό του και τη Μη-συνδεσιμότητα που αφορά τη διαδικασία προστασίας της ιδιωτικότητας ενός χρήστη από πιθανούς επιτιθέμενους, αποτρέποντάς τους από το να συνδέσουν διαφορετικά τμήματα πληροφοριών.

4.1.3 Τεχνολογίες Προάσπισης της ιδιωτικότητας

Οι τεχνολογίες που μπορούν να προασπίσουν την ιδιωτικότητα είναι οι τεχνολογίες για την προστασία της ιδιωτικότητας που εμπεριέχει μεθοδολογίες για την προστασία ή την απόκρυψη δεδομένων και πληροφοριών και είναι και οι τεχνολογίες για τη διαχείριση της ιδιωτικότητας που εμπεριέχουν μηχανισμούς που ελέγχουν, την πρόσβαση σε δεδομένα και πληροφορίες και τη χρήση μέσων και συστημάτων. Οι κατηγορίες αυτές περιλαμβάνουν κάποιες άλλες υποκατηγορίες που παρουσιάζονται παρακάτω.

Κατηγορία	Υποκατηγορίες	Τυπικά Χαρακτηριστικά
Προστασία Ιδιωτικότητας	Εργαλεία Ψευδωνυμίας	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να απαιτείται αποστολή προσωπικών δεδομένων
	Εργαλεία Ανωνυμίας	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να γίνεται γνω-

		στή η πραγματική ταυτότητα του χρήστη
	Εργαλεία Κρυπτογράφησης	Επιτρέπουν την πραγματοποίηση ηλεκτρονικών συναλλαγών (transactions) χωρίς να γίνονται γνωστά προσωπικά δεδομένα του χρήστη σε μη εξουσιοδοτημένες οντότητες
	Φίλτρα Προστασίας	Αποτρέπουν ανεπιθύμητο περιεχόμενο να κοινοποιηθεί στο χρήστη
	Διαγραφείς Ιστορικού και Πρόσφατης Δραστηριότητας	Απομακρύνουν ηλεκτρονικά ίχνη (electronic traces) από τις δραστηριότητες του χρήστη.
Διαχείριση Ιδιωτικότητας	Εργαλεία Ενημέρωσης	Επιτρέπουν τη δημιουργία και τον έλεγχο των Πολιτικών Ιδιωτικότητας
	Εργαλεία Διαχείρισης	Επιτρέπουν τη διαχείριση της ψηφιακής ταυτότητας του χρήστη και των δικαιωμάτων του

4.2 Θεσμικό Πλαίσιο για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας

Η σημαντικότητα της προστασίας των προσωπικών δεδομένων απορρέει από την ανάγκη να διαφυλαχθεί η ιδιωτικότητα του ατόμου, παρόλο που αυτό ενδέχεται να διαφέρει από την ιδιωτική του ζωή. Η σημασία της πρώτης αντανακλάται στη δυνατότητά της να παρέχει επαρκή προστασία στο άτομο από εξωτερικούς παράγοντες στον προσωπικό του χώρο, καθώς και προστασία από οποιαδήποτε συμπεριφορά που στόχο έχει την καταπίεση ή την υποκίνηση, η οποία πιθανό να στοχεύει στην εδραίωση της ανελευθερίας του ατόμου και θέτει εμπόδια στην προσωπική του ανάπτυξη, καθώς και στην ανεξαρτητοποίησή του, ενώ τον αποτρέπει να αναπτύσσεται και να ψυχαγωγείται μέσα από τις προσωπικές σχέσεις με τους οικείους του. Επιπλέον, αποσκοπεί στην προστασία των επιλογών που καθορίζουν τον χαρακτήρα του και την ιδιοσυγκρασία του. Σύμφωνα με τα παραπάνω, η εξασφάλιση της ιδιωτικότητας του ατόμου προστατεύει την αξιοπρέπεια και την ελευθερία του ανθρώπου, ενισχύοντας την δυνατότητά του να επιλέγει εναλλακτικούς τρόπους ζωής, μη συμβατούς με την πλειοψηφία της κοινωνίας, σε τομείς όπως η σεξουαλικότητα ή άλλες μορφές κοινωνικών σχέσεων, δίχως να υφίσταται επικριτικές-καταπιεστικές συμπεριφορές από το περίγυρό του.

4.2.1 Αρχές της Προστασία της Ιδιωτικότητας

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, οι βασικοί πυλώνες ανά τον κόσμο για την προστασία της ιδιωτικότητας, είναι η Αρχή του περιορισμού της συλλογής κατά την οποία η άντληση δεδομένων οφείλει να είναι αυστηρώς οριοθετημένη και η οποία θα πρέπει να λαμβάνει χώρα με χρήση νόμιμων μέσων, εν γνώση του ατόμου και με τη συγκατάθεσή του, όπου αυτό δύναται. Επιπλέον, είναι η Αρχή ποιότητας των δεδομένων όπου τα δεδομένα οφείλουν να συσχετίζονται με τον λόγο για τον οποίο θα χρησιμοποιηθούν, όσο αυτό κρίνεται αναγκαίο, και θα πρέπει να είναι αυτούσια και με σαφήνεια διατυπωμένα, η Αρχή προσδιορισμού του σκοπού που αφορά στο λόγο για τον οποίο συλλέγονται δεδομένα και κατά τη συγκέντρωσή τους θα πρέπει αυτός να διευκρινίζεται, ενώ η αξιοποίησή τους τους θα πρέπει να γίνεται αποκλειστικά για την επίτευξη του σκοπού αυτού ή κάποιου συναφή. Επίσης, η Αρχή περιορισμού της χρήσης που ορίζει πως τα προσωπικά δεδομένα δε θα πρέπει να γνωστοποιούνται ή να αξιοποιούνται για διαφορετικούς λόγους εκτός από τον αρχικά καθορισμένο σκοπό, με μοναδικές εξαιρέσεις την περίπτωση που το εν λόγο άτομο έχει ενημερωθεί και συναινέσει ή υπάρχει νομική εξουσιοδότηση. Ακόμη, είναι η Αρχή προστασίας της ασφάλειας που ορίζει μέσω κατάλληλων μηχανισμών τη διασφάλιση των δεδομένων απέναντι σε επιθέσεις, όπως η μη εξουσιοδοτημένη χρήση, η διαστρέβλωση των δεδομένων από εξωτερικούς παράγοντες και η καταστροφή τους. Επίσης, είναι η Αρχή της διαφάνειας που αφορά στη διαφάνεια που θα πρέπει να χαρακτηρίζει τους μηχανισμούς άντλησης και ανάλυση δεδομένων, καθώς και την προέλευση του ατόμου που την πραγματοποιεί. Επιπροσθέτως, είναι η Αρχή της συμμετοχής του ατόμου που επιτρέπει για τον κάθε χρήστη, να γνωρίζει, δηλαδή να παίρνει επιβεβαίωση από τον υπεύθυνο για τον αν ο τελευταίος έχει δεδομένα στην κατοχή του που σχετίζονται με τον χρήστη, να ενημερώνεται άμεσα, με εύκολο, σαφή και γρήγορο τρόπο αν τα δεδομένα σχετίζονται με αυτόν και αν υπάρχει κάπου κόστος αυτό θα είναι μικρό. Επίσης, επιτρέπει να ενημερώνεται για τους λόγους τους οποίους κάποια αίτησή του να μην προχώρησε και να απορρίφθηκε έχοντας την δυνατότητα για ένσταση και δικαίωμα για νέα διεκδίκηση του αιτήματος. Τέλος, του επιτρέπει να κάνει ένσταση για δεδομένα που σχετίζονται με αυτόν και μπορεί να τα διορθώσει. Η τελευταία αρχή, είναι αυτή της Αρχής της ευθύνης, όπου ο κάθε υπεύθυνος που επεξεργάζεται τα δεδομένα είναι και ο κύριος υπεύθυνος για να τηρούνται τα μέτρα που επιφέρουν την προστασία των προσωπικών δεδομένων.

4.2.2 Ευρωπαϊκή Οδηγία 1995/46/ΕΚ

Έχει στόχο την εξασφάλιση της ιδιωτικότητας των δικαιωμάτων, τα οποία απειλούνται από την απεριόριστη και μη διαχειρίσιμη μεταφορά και μετατροπή που υφίστανται.Προκειμένου να περιοριστεί η απειλή αυτή, η παραπάνω οδηγία περιλαμβάνει κάποια σενάρια, που μπορούν να επεξεργασθούν τα δεδομένα αλλά με γνώμονα πάντα την ισορροπία με τα συμφέροντα.

Αναλυτικότερα, επιτρέπεται σε περιπτώσεις που το ίδιο το άτομο έχει συμφωνήσει, ή λαμβάνει χώρα εντός των όρων μίας συμβατικής σχέσης στην οποία και ανήκει. Ακόμα, απαραίτητη κρίνεται προκειμένου να εξυπηρετηθούν νομικά συμφέροντα ή επωφελείται σημαντικά το ίδιο το άτομο. Τέλος, χρησιμοποιείται για την εξυπηρέτηση του ατόμου που πραγματοποιεί την επεξεργασία, πάντα στα πλαίσια νομικών συμφερόντων και υπό τον όρο πως δεν υπάρχει δόλος από το άτομο του οποίου τα δεδομένα είναι το αντικείμενο μελέτης.

Από την άλλη πλευρά, στόχος της παραπάνω οδηγίας είναι η όσο το δυνατόν πιο περιορισμένη επεξεργασία δεδομένων εξαιρετικά προσωπικής φύσεως, αφήνοντας περιθώριο μεταποίησης τους σε ελάχιστες περιπτώσεις. Κάποιες από αυτές είναι φυσικά όταν το ίδιο το άτομο συμφωνεί με αυτή ή κρίνεται απαραίτητη από το άτομο που έχει κληθεί να επεξεργαστεί τα δεδομένα, πάντα εντός των νόμιμων πλαισίων που ορίζει η εκάστοτε νομοθεσία. Επίσης, επιτρεπτή χαρακτηρίζεται όταν τίθενται θέματα σωματικής ακεραιότητας ή για ιατρικούς σκοπούς, ακόμα και αν το άτομο δεν είναι ικανό να συμφωνήσει. Όλα τα παραπάνω βέβαια προϋποθέτουν να μην υπάρχουν υποβόσκοντα συμφέροντα και να μην αποσκοπούν σε κέρδη, αλλά να χρησιμοποιούνται εποικοδομητικά στο κοινωνικό πλαίσιο. Τέλος, κρίνεται απαραίτητη και για λόγους υπεράσπισης στα πλαίσια εκδίκασης κάποιας υπόθεσης, που αφορά το αντικείμενο περισυλλογής των δεδομένων.

Η ευθύνη για την απόφαση του αν είναι ή όχι αποδεκτή η επεξεργασία δεδομένων που αφορούν θέματα ασφαλείας ή και νομικά θέματα, ανήκει στη εθνική δημόσια αρχή. Καθώς σκοπός της Οδηγίας 95/46/ΕΚ είναι η ελάχιστη μεταποίηση των δεδομένων που συλλέγονται, η ίδια ορίζει δύο βασικές έννοιες , σύμφωνα με τις οποίες κρίνονται οι λόγοι για τους οποίους η επεξεργασία αυτή κρίνεται απαραίτητη κάθε φορά. Αυτές είναι η αρχή του σκοπού και της αναλογικότητας. Με βάση αυτές, η αιτία για την οποία ξεκινά και πραγματοποιείται η διαδικασία αυτή οφείλει να ορίζεται εξ αρχής, να είναι σαφής, νόμιμη και το ενδιαφερόμενο άτομο να είναι ενημερωμένο και να έχει δώσει την έγκριση του για αυτή και μόνο

αυτή την αιτία. Επίσης, υποδεικνύουν πως τα εν λόγω δεδομένα μπορούν να χρησιμοποιηθούν και να επεξεργαστούν μεταγενέστερα, μόνο για σχετικούς λόγους.

Η Οδηγία 95/46/ΕΚ συμπεριλαμβάνει ακόμα, τους κανόνες οι οποίοι πρέπει να τηρούνται κατά την επεξεργασία δεδομένων προσωπικής φύσεως. Συγκεκριμένα, πέραν του ότι η μεταποίηση των δεδομένων οφείλει να υπάγεται στα νομικά πλαίσια, πρέπει επίσης να είναι σε συμφωνία με αυτά που ορίζουν οι προαναφερόμενες αρχές της αναλογικότητας και του σκοπού. Ακόμα, η διατύπωση των δεδομένων πρέπει να είναι σαφής, δίχως να αφήνουν περιθώρια λανθασμένης ερμηνείας, αλλά και να διατηρούν το προσωπικό του χαρακτήρα, μόνο κατά την περίοδο επεξεργασίας τους.

Το άτομο που φέρει την ευθύνη της επεξεργασίας των δεδομένων οφείλει να γνωστοποιεί στο άτομο για το οποίο συλλέγονται οι πληροφορίες τα εξής:

Τα προσωπικά στοιχεία του ιδίου

Την αιτία περισυλλογής και επεξεργασίας των πληροφοριών

Πληροφορίες σχετικά με το κοινό που θα τις λάβει, καθώς και τις επιπτώσεις της αποδοχής ή όχι της δημοσιοποίησης των δεδομένων αυτών.

Υπό συνθήκες κατά τις οποίες το άτομο αναφοράς δεν ταυτίζεται με το άτομο που πραγματοποιεί την περισυλλογή των δεδομένων, ο πρώτος οφείλει να ενημερώνεται σε περίπτωση κοινοποίησης αυτών από το δεύτερο. Το υποκείμενο επίσης, πρέπει να έχει την δυνατότητα ελέγχου, σχετικά με την διαστρέβλωση ή μη των πληροφορίων και τον λόγο αξιοποίησής τους, για μεγάλο χρονικό διάστημα, άμεσα και με λογικό χρηματικό αντίτιμο. Θα πρέπει επίσης να λάβει γνώση σχετικά με τη μέθοδο επεξεργασίας, ενώ σε κάθε περίπτωση δύναται να αρνηθεί όλα τα παραπάνω.

Τα προαναφερόμενα δεδομένα επιτρέπεται να κοινοποιηθούν από Κράτη Μέλη προς τρίτες χώρες, υπό τον όρο πως τα δεδομένα προστατεύονται επαρκώς, λαμβάνοντας υπόψη πάντα τις εθνικές διατάξεις της χώρας για την οποία προορίζονται. Αν ο παραπάνω όρος δεν εξασφαλίζεται τα Κράτη-Μέλη δεν επιτρέπουν την παραπάνω δημοσιοποίηση προς την εν λόγω τρίτη χώρα.

4.2.3 Ελληνικό Κανονιστικό Πλαίσιο

Η Ελλάδα , η οποία αποτελεί μία από τις πρώτες χώρες που ακολουθούν την Οδηγία 95/46/ΕΚ στο εσωτερικό δίκαιο, έχει διαμορφώσει νόμους που αφορούν στην προστασία των προσωπικών δεδομένων στα πλαίσια του συντάγματος.

4.2.4 Ευρωπαϊκή Οδηγία 2006/24/ΕΚ

Περιλαμβάνει επιπλέον κανόνες σχετικά με την κοινοποίηση δεδομένων προς όλα τα υπόλοιπα Μέλη και την τροποποίηση αυτών. Έχει στόχο την ομαλή λειτουργία, αλλά και την διαφύλαξη των δεδομένων για σε νομικό επίπεδο. Ευθύνη των Κρατών – Μελών είναι να διατηρούν τις πληροφορίες που συλλέγονται και να τις καθιστούν διαθέσιμες στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών. Τέτοιου είδους δεδομένα, τα οποία είναι καθοριστικά για τον προσδιορισμό του πομπού της επικοινωνίας, είναι ο δέκτης της επικοινωνίας, το χρονικό πλαίσιο αυτής καθώς και το είδος της, αλλά και τέλος η τοποθεσία και ο εξοπλισμός που χρησιμοποιήθηκε για να πραγματοποιηθεί αυτή.

Τα παραπάνω δεδομένα πρέπει να διατηρούνται για διάστημα μεγαλύτερο των έξι μηνών και μικρότερο των δύο χρόνων από την ημερομηνία που έλαβε χώρα η επικοινωνία.

4.4 Απειλές και Επιπτώσεις σε Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Ως απειλή αντιμετωπίζεται κάθε ενδεχόμενη πράξη, η οποία πιθανώς να οδηγήσει σε αλλοίωση ή και καταστροφή ενός συστήματος επεξεργασίας δεδομένων. Τέτοιου είδους πράξεις δεν προέρχονται αποκλειστικά από εχθρικές κινήσεις του ευρύτερου περιβάλλοντος , είτε εσωτερικό είτε εξωτερικό, αλλά και από απροσεξίες και ακούσια σφάλματα, τα οποία έχουν ως αποτέλεσμα την μη αποτελεσματική λειτουργία του συστήματος.

Στην προσπάθειας μας να εντοπίσουμε και να εξετάσουμε την εκάστοτε απειλή (Risk Analysis) πρωταρχική σημασία καταλαμβάνουν η αναγνώριση των κινδύνων, αλλά και η εκτίμηση του επιπέδου της ενδεχόμενης απειλής μαζί με τον τρόπο αντιμετώπισής της (Risk Assessment). Στο ευρύτερο πλαίσιο της εκτίμησης του συνόλου του κινδύνου συγκαταλέγονται οι παραπάνω διαδικασίες, οι οποίες όμως έχουν ως κοινή παραδοχή πως πλήρης ασφάλεια σε όλα τα επίπεδα δεν είναι εφικτή. Έχοντας ως γνώμονα την τελευταία, αυτό που προτιμάται είναι η ύπαρξη

μία μέσης κατάστασης, κατά την οποία η αντιμετώπιση των εκάστοτε πιθανών απειλών γίνεται μέσω οικονομικών μέτρων με περιορισμένο κόστος, δίχως όμως να χάνουν την αποτελεσματικότητά τους (Countermeasures). Απαραίτητες λοιπόν, κρίνονται τεχνικές μέσω των οποίων υπολογίζονται και αξιολογούνται οι κίνδυνοι χρησιμοποιώντας κάποιες κοινά αποδεκτές μονάδες μέτρησης, με σκοπό να είναι εφικτή η σύγκριση και η κατηγοριοποίησή τους ανάλογα με την επικινδυνότητά τους. Η αξιολόγηση του ρίσκου που διακατέχει ένα πληροφοριακό σύστημα, πραγματοποιείται μέσω των δύο όρων που παρουσιάστηκαν παραπάνω (Risk Analysis και Rist Assessment), στα πλαίσια των οποίων ο κίνδυνος εντοπίζεται και αξιολογείται, ενώ στο τέλος οδηγούμαστε στην τελική εκτίμηση του κινδύνου αλλά και τους τρόπους που επιλέγονται για να αντιμετωπιστεί (Risk Assessment and Management), λαμβάνοντας και πάλι υπόψη πως είναι αδύνατο να επιτευχθεί η πλήρης προστασία του συστήματος και έχοντας ως στόχο την βέλτιστη προστασία με τη μικρότερη δυνατή οικονομική δαπάνη (Countermeasures).

4.4.1 Κατηγορίες Απειλών

Σε αντίθεση με τις διαδικασίες που λαμβάνουν χώρα σε κάποια Δημόσια Υπηρεσία, και οι οποίες απαιτούν το ίδιο το άτομο με τα διαπιστευτήρια έγγραφα της ταυτότητάς του στο χώρο , γεγονός που καθιστά την εξαπάτηση και την παραποίηση των προσωπικών δεδομένων αρκετά δύσκολη, οι συναλλαγές που πραγματοποιούνται ηλεκτρονικώς με τη βοήθεια της τεχνολογίας είναι αρκετά εύκολο και σύνηθες να παραβιάζονται, οδηγώντας σε υποκλοπές και πλεκτάνες. Τα προηγούμενα αποτελούν απόρροια κακής προστασίας του συστήματος στα πλαίσια της ταυτοποίησης και της αυθεντικοποίησης, έχοντας ως αποτέλεσμα την διαρροή των προσωπικών δεδομένων.

4.4.2 Απειλές Διακριτικών Αυθεντικοποίησης

Οι κίνδυνοι που παρουσιάστηκαν παραπάνω, και οι οποίοι απειλούν κυρίως συστήματα διαχείρισης δεδομένων άκρος προσωπικών και ευαίσθητων, έχουν ως κύριο κίνητρό τους την απόκτηση και εκμετάλλευση αυτών, δίχως ο νόμιμος χρήστης να λάβει γνώση. Οι κίνδυνοι αυτοί χαρακτηρίζονται ανάλογα με τα διακριτικά αυθεντικοποίησης σε δύο κατηγορίες: αυτοί που εξαρχής είμαστε ενημερωμένοι σχετικά με την ύπαρξή τους, όπως είναι η παραβίαση ενός κωδικού χρήστη μέσω συνεχούς αναζήτησης του επιτιθέμενου με χρήση διάφορων μεθόδων (απόπειρες στην τύχη ,χρήση λεξικών κτλ.) και η κλοπή ή αντιγραφή σε βάρος του νόμιμου χρήστη, εν αγνοία του.

4.4.3 Απειλές κατά τη Διαδικασία Εγγραφής Τελικού Χρήστη

Κατά της εγγραφή εμφανίζονται απειλές όπως η πλαστοπροσωπία. Σε αυτή την απειλή, ο χρήστης υποστηρίζει ότι είναι κάποιος άλλος, καταθέτοντας δικαιολογητικά ψεύτικα για να το υποστηρίξει. Άλλη απειλή είναι η αποποίηση εγγραφής. Σε αυτή την απειλή, ο χρήστης προσπαθεί να αρνηθεί την διαδικασία της εγγραφής καθώς και τα συνθηματικά και τα αποτελέσματα τη εγγραφής.

4.4.4 Απειλές στα Πρωτόκολλα Αυθεντικοποίησης

Οι απειλές που μπορεί να κάνουν την εμφάνιση τους στα Πρωτόκολλα μπορούν να διαχωριστούν σε ενεργές ή παθητικές ανάλογα με το αν είναι ενεργή ή όχι η συμμετοχή του επιτιθέμενου. Η πρώτη απειλή που μπορεί να εντοπιστεί είναι η υποκλοπή δεδομένων, όπου σε αυτή την απειλή ο επιτιθέμενος παρακολουθεί τα δεδομένα που μεταφέρονται με σκοπό την υποκλοπή τους και την ανάλυση τους. Πιο αναλυτικά, μπορεί να υποκλαπούν συνομιλίες και στη συνέχεια να αξιοποιηθούν είτε για επόμενη επίθεση είτε για το αν είναι κρυπτογραφημένα τα δεδομένα να αποκαλυφθεί το κλειδί. Άλλη απειλή είναι, να επιτεθεί σαν ενδιάμεσος. Δηλαδή, ο επιτιθέμενος να τροποποιήσει απεσταλμένα μηνύματα, να τα προωθήσει στο θύμα του και με τρόπο που δεν γίνεται αντιληπτός να επιτεθεί στο θύμα. Επόμενη απειλή είναι η υποκλοπή συνόδου, όπου ο επιτιθέμενος εκμεταλλεύεται κάποια προηγούμενη επιτυχημένη μη εξουσιοδοτημένη είσοδο στο σύστημα και τις υπηρεσίες. Οι επιθέσεις επανάληψης είναι μια απειλή που είναι δύσκολο να εντοπιστεί αφού ο επιτιθέμενος έχει κλέψει τα στοιχεία αυθεντικοποίησης και τα αξιοποιεί ως νόμιμος χρήστης με αποτέλεσμα να μην γίνεται αντιληπτός. Η επίθεση πλαστοπροσωπίας είναι μια απειλή που ο επιτιθέμενος έχει καταφέρει να εισέλθει ως μη εξουσιοδοτημένος σε κάποια δεδομένα της αυθεντικοποίησης του χρήστη. Επόμενη επίθεση είναι της πλημμύρας, όπου ο επιτιθέμενος φορτώνοντας το σύστημα με αποτέλεσμα να επιβαρύνονται οι υπολογιστικοί πόροι του συστήματος και να προκαλείται πρόβλημα με την παροχή των υπηρεσιών. Η επίθεση τροποποίησης δεδομένων είναι μια απειλή που γίνεται είτε χρησιμοποιώντας την επίθεση του ενδιάμεσου, είτε χρησιμοποιώντας κακόβουλο λογισμικό στα δεδομένα που μεταφέρονται με σκοπό την αλλοίωση τους κατά την αποθήκευση με μη εξουσιοδοτημένη πρόσβαση. Τέλος, οι επιθέσεις απόκρυψης της ταυτότητας είναι απειλή που δύσκολα μπορεί να γίνει αντιληπτή, γιατί ο επιτιθέμενος χρησιμοποιεί την ταυτότητα ενός εξουσιοδοτημένου χρήστη και αποκρύπτει την δική του. Δηλαδή,

χρησιμοποιεί μια διεύθυνση που μπορεί να μην ανταποκρίνεται στην πραγματικότητα και με αυτό τον τρόπο επιτίθεται χωρίς να αποκαλύπτει την πραγματική του διεύθυνση και με αυτό τον τρόπο επιτυγχάνει την πρόσβαση στο σύστημα.

4.5 Πιθανές Επιπτώσεις Απειλών – Κινδύνων

Οι απειλές, εάν εκμεταλλευθούν σε μια επίθεση, επιφέρουν διάφορες επιπτώσεις στους χρήστες και στους δημόσιους φορείς που παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης. Παρακάτω, παρουσιάζονται συνοπτικά τα αποτελέσματα των κινδύνων τόσο για τους χρήστες όσο και για τους δημόσιους φορείς, όσον αφορά το επίπεδο εμπιστοσύνης της υπηρεσίας. Θα πρέπει το να τονιστεί ότι οι επιπτώσεις διαφέρουν από υπηρεσία σε υπηρεσία και τις ενδεχόμενες επιπτώσεις που μπορεί να υποστεί ο φορέας του Δημοσίου, όπως νομικές ή οικονομικές.

Κίνδυνος	Πιθανές Επιπτώσεις Τελικών Χρηστών	Πιθανές Επιπτώσεις Φορέων Παροχής Υπηρεσιών
Υποκλοπή Διακριτικών Αυθεντικοποίησης	Μη εξουσιοδοτημένη Πρόσβαση Παραβίαση Ιδιωτικότητας Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις ενδιάμεσου	Παραβίαση Ιδιωτικότητας Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων Αντιποίηση Υπηρεσίας
Υποκλοπή Επικοινωνίας-Δεδομένων	Παραβίαση Ιδιωτικότητας Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Υποκλοπή Συνόδου	Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Επιθέσεις Επανάληψης	Μη εξουσιοδοτημένη Πρόσβαση Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλαστοπροσωπίας	Μη εξουσιοδοτημένη Πρόσβαση	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλημμύρας	Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας
Επιθέσεις Τροποποίησης Δεδομένων	Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Ιομορφικό Λογισμικό	Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας
Υπερχειλίσεις Προσωρινών Χώρων	Άρνηση πρόσβασης στην Υπηρεσία Μη εξουσιοδοτημένη Πρόσβαση	Μη Παροχής Υπηρεσίας Μη εξουσιοδοτημένη Πρόσβαση
Μη εξουσιοδοτημένη Είσοδος στο Λ.Σ.	Μη εξουσιοδοτημένη Πρόσβαση	Μη εξουσιοδοτημένη Πρόσβαση

Πίνακας 5: Κίνδυνοι και Πιθανές Επιπτώσεις

4.5.1 Άλλες Απειλές

Μια από τις άλλες απειλές που μπορεί να εμφανιστούν στα συστήματα είναι αυτή του Ιομορφικού λογισμικού, που είναι πρόγραμμα και έχει ως στόχο τη παραβίαση ενός υπολογιστικού συστήματος εκτελώντας κακόβουλο κώδικα και ο υπεύθυνος του συστήματος δεν μπορεί να το εντοπίσει εύκολα. Το λογισμικό αυτό χωρίζεται σε τρεις κατηγορίες και ο διαχωρισμός γίνεται με βάση τις ιδιότητές του. Αρχικά είναι Ιός, όπου είναι ένα πρόγραμμα το οποίο μπορεί να βρίσκεται σε ένα μέρος στο πρόγραμμα του υπολογιστή και ενεργοποιείται όταν ενεργοποιηθεί αυτό το μέρος. Επόμενη κατηγορία είναι, ο Δούρειος Ίππος, όπου είναι ένα πρόγραμμα, που εμπεριέχει λειτουργίες που όταν ενεργοποιηθούν αποκτά ο επιτιθέμενος δικαιώματα διαχειριστή και μπορεί να ολοκληρώσει επίθεση. Τελευταία κατηγορία είναι τα Σκουλήκια, όπου είναι ένα πρόγραμμα που καταφέρνει να διαδίδεται μέσα στον υπολογιστή πολύ εύκολα και συνεχώς να μεγαλώνει. Για να εισβάλλει το ιομορφικό λογισμικό στον υπολογιστή θα γίνει με κάποια αποθήκευση ή μέσω δικτύου. Πιο αναλυτικά, όταν γίνεται υπερχείλιση προσωπικών χώρων, τότε σημαίνει ότι δεν υπάρχει αρκετός χώρος για να αποθηκευτούν δεδομένα με αποτέλεσμα ο επιτιθέμενος να κατευθύνει την αποθήκευση στον δικό του κώδικα και με αυτό τον τρόπο να αποκτήσει πρόσβαση. Επίσης, αν το σύστημα δεν έχει υψηλής προστασίας έλεγχο είναι πιθανό να εισβάλλει κάποιος που δεν είναι εξουσιοδοτημένος και να εκτελέσει το κακόβουλο λογισμικό και να παραβιάσει το σύστημα.

4.6 Τρόποι Αντιμετώπισης

Για να αποφευχθεί ο κίνδυνος μια απειλή να δημιουργήσει προβλήματα στο σύστημα, θα πρέπει οι τρόποι αντιμετώπισης να είναι βασισμένοι στα πλαίσια της ασφάλειας και να ακολουθούν επιπρόσθετες υπηρεσίες ασφάλειας για τον μεγαλύτερο και καλύτερο έλεγχο. Για αρχή, να ακολουθούν την υπηρεσία της αυθεντικοποίησης που έχει να κάνει με το επίπεδο εμπιστοσύνης που απαιτούν οι χρήστες. Επιπλέον, άλλη υπηρεσία ασφάλειας είναι η εξουσιοδότηση που έχει να κάνει με το δικαίωμα που έχει ο κάθε χρήστης στην συναλλαγή, είναι η ακεραιότητα που έχει να κάνει με την αποτροπή της επεξεργασίας των μηνυμάτων κατά την διάρκεια της συναλλαγής. Άλλη υπηρεσία είναι η μη-αποποίηση της αποστολής/λήψης δεδομένων, που σχετίζεται με την απαγόρευση της άρνησης του χρήστη ότι έχει λάβει μέρος σε ηλεκτρονική συναλλαγή. Τελευταία υπηρεσία

ασφάλειας είναι, η εμπιστευτικότητα των μηνυμάτων και η προστασία της ιδιωτηκότητας των χρηστών που εμπλέκονται στην ηλεκτρονική συναλλαγή.

4.6.1 Τρόποι Αντιμετώπισης Διακριτικών Αυθεντικοποίησης

Για να σταματήσουν οι απειλές των διακριτικών αυθεντικοποίησης , θα πρέπει να παρθούν κάποια μέτρα πρόληψης. Σχετικά με την ακεραιότητα των συνθηματικών του χρήστη μπορούν να χρησιμοποιήσουν σύνθετα και ασφαλή συνθηματικά, αν αποθηκεύουν χωρίς κρυπτογράφηση, να αποστέλλουν με ασφαλή τρόπο τα διαπιστευτήρια, να βάλουν όριο στις προσπάθειες καταχώρισης του συνθηματικού και να αναγκάζουν το χρήστη σε μικρό χρονικό διάστημα να αλλάζει το συνθηματικό του. Οι χρήστες με τη σειρά τους θα πρέπει να αποθηκεύουν τα διακριτικά τους σε ασφαλή σημεία ώστε να αποφευχθούν οι περιπτώσεις κλοπής.

Προκειμένου τα συστήματα πληροφοριών να μπορέσουν να πραγματοποιήσουν τον οποιοδήποτε σκοπό τους ομαλά και δίχως δυσκολίες, κρίνεται απαραίτητος ο περιορισμός τυχόν απειλών αλλά και η εύρεση του σωστού τρόπου καταπολέμησής τους. Η χρήση του διαδικτύου και των συστημάτων πληροφοριών για την εξυπηρέτηση των πολιτών σε πολλούς τομείς και θέματα, διενεργώντας πάντα την απαραίτητη ταυτοποίηση, αποτελεί σημαντική διευκόλυνση για τον σύγχρονο άνθρωπο αλλά και τον βασικό τομέα της ηλεκτρονικής διακυβέρνησης. Προκειμένου να προστατευτεί η τελευταία και να εξασφαλιστεί η ομαλή λειτουργία της, οφείλουν να εφαρμόζονται κάποιοι κανόνες. Παρακάτω παρατίθενται κάποιοι βασικοί κίνδυνοι αλλά και οι τρόποι αποφυγής και αντιμετώπισής τους.

- Υποκλοπή επικοινωνίας-δεδομένων: Προκειμένου να αποφευχθεί, στοιχεία πρωταρχικής σημασίας, όπως κωδικοί πρόσβασης και μέθοδοι ταυτοποίησης, πρέπει να προστατεύονται επαρκώς χρησιμοποιώντας κάποιο είδος κρυπτογράφησης αλλά και άλλα ειδικά συστήματα προστασίας. Το ίδιο ισχύει φυσικά και κατά τα στάδια επεξεργασίας τους. Ως αποτέλεσμα η οποιαδήποτε απειλή θα καθίσταται ανίκανη να υποκλέψει πληροφορίες.
- Επιθέσεις Ενδιάμεσου: Για την καταπολέμηση αυτών κρίνεται απαραίτητη η εφαρμογή συστημάτων ασφαλείας, όπως είναι το πρωτόκολλο SSL, κατασκευασμένο ειδικά για τέτοιους κινδύνους, αλλά και πολλά άλλα

προγράμματα, τα οποία όμως δυστυχώς στο παρελθόν έχουν αποτύχει να προστατέψουν αποτελεσματικά τα συστήματα πληροφοριών.

- Επιθέσεις Επανάληψης και Υποκλοπής Συνόδων: κίνδυνοι αυτής της φύσεως περιορίζονται όταν οι μέθοδοι ταυτοποίησης που χρησιμοποιούνται δεν επιλέγουν την ανάλυση δεδομένων τα οποία έχουν συνάφεια με προγενέστερες διαδικασίες και ενδέχεται να παραποιήσουν τα αποτελέσματα. Σημειώνεται επίσης πως και σε αυτή την περίπτωση η χρήση μίας μεθόδου κρυπτογράφησης αλλά και περεταίρω συστημάτων ασφαλείας είναι απαραίτητη.
- Επιθέσεις Πλαστοπροσωπίας: Σε αυτή την περίπτωση η επίθεση γίνεται με στόχο την εξαπάτηση του συστήματος, χρησιμοποιώντας παρανόμως πληροφορίες και στοιχεία ταυτοπροσωπίας, τα οποία δεν πρέπει να δημοσιοποιούνται, από τους εκάστοτε επιτιθέμενους.
- Επιθέσεις Πλημμύρας: Αν και αποτελούν μία από τις κύριες απειλές των ηλεκτρονικών υπηρεσιών αλλά και των συστημάτων ταυτοποίησης, η καταπολέμησή τους είναι εφικτή με τα κατάλληλα συστήματα ασφαλείας.
- Επιθέσεις Τροποποίησης Δεδομένων: Ο τρόπος που χειρίζονται τέτοιου είδους κίνδυνοι, σε κάθε μία από τις προαναφερόμενες περιπτώσεις, είναι με κάποιο ειδικό σύστημα ασφαλείας, με αποστολή μοναδικού κωδικού επιβεβαίωσης (message authentication code), έλεγχο εγκυρότητας μηνύματος (message integrity checksum), το H-MAC και ηλεκτρονικές υπογραφές.
- Επιθέσεις Απόκρυψης Ταυτότητας (Spoofing): Περιορίζονται με εγκατάσταση ειδικών προγραμμάτων, τα οποία αναλαμβάνουν την κατηγοριοποίηση και τον διαλογισμό των πληροφοριών που δέχονται τα συστήματα (Ingress filtering). Τα προαναφερόμενα είναι υπεύθυνα για τον περιορισμό της δημοσιοποίησης των δεδομένων σε όλο το φάσμα του διαδικτύου, ενώ δύναται να εφαρμοστούν σε οποιοδήποτε σημείο ασφαλείας δικτύου (Firewall), σύμφωνα με το πρωτόκολλο που παρουσιάζεται στο RFC 2267.

4.6.2 Τρόποι Αντιμετώπισης κατά την Εγγραφή Τελικού Χρήστη

Πολλές απειλές μπορεί να εμφανιστούν κατά της διαδικασία εγγραφής. Γι’ αυτό και πρέπει γίνεται ταυτοποίηση και αυθεντικοποίηση των χρηστών που θέλουν να εγγραφούν σε κάποια υπηρεσία, να γίνεται ενδελεχώς έλεγχος των δικαιολογητικών που κατατίθεται και να γίνεται πλήρης αξιοποίηση της καταγραφής των διαδικασιών, ώστε να μην μπορεί κανένας χρήστης να αρνηθεί την εγγραφή σε κάποια υπηρεσία.

4.6.3 Τρόποι Αντιμετώπισης Άλλων Απειλών

Όλες οι απειλές που παρουσιάστηκαν παραπάνω έτσι και οι γενικές απειλές θα πρέπει να αντιμετωπίζονται άμεσα. Αυτό σημαίνει οτι, θα πρέπει να υπάρχει άμεση ενημέρωση από τους υπεύθυνους του συστήματος σχετικά με τις εξελίξεις του λογισμικού, ειδικά αν αυτές οι εξελίξεις αφορούν θέματα ασφάλειας ή αναβαθμίσεις.

.

Απειλή		**Τρόποι αντιμετώπισης**
Απειλές Διακριτικών Αυθεντικοποίησης	Υποκλοπή δεδομένων που γνωρίζει ο χρήστης (π.χ. συνθηματικού) με: • Επιθέσεις λεξικών • Επιθέσεις εξαντλητικής αναζήτησης • Επιθέσεις τυχαίων δοκιμών • Υποκλοπή κατά τη μετάδοση των διαπιστευτηρίων	• Αξιοποίηση Ασφαλών Συνθηματικών • Ασφαλή αποθήκευση τους και όχι σε καθαρή μορφή • Ασφαλή μετάδοση των διαπιστευτηρίων κατά τη διαδικασία αυθεντικοποίησης • Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού
	Υποκλοπή δεδομένων που έχει υπό την κατοχή του ο χρήστης με σκοπό την αντιγραφή ή τη χρησιμοποίηση σε κάποια δοσοληψία χωρίς τη γνώση του (π.χ. ιδιωτικό κλειδί)	Διατήρηση των διακριτικών αποθήκευσης σε ασφαλή μέρη ώστε να μην είναι δυνατή η υποκλοπή του από κακόβουλους χρήστες.
Απειλές στα Πρωτόκολλα Αυθεντικοποίησης & στις Παρεχόμενες υπηρεσίες	Υποκλοπή επικοινωνίας-δεδομένων (*Eavesdropping*): • Υποκλοπή δεδομένων • Ανάλυση των δεδομένων (*Traffic analysis*) και αξιοποίηση τους σε μελλοντική επίθεση	Τα δεδομένα δε θα πρέπει να μεταδίδονται σε καθαρή μορφή (clear text) αλλά θα πρέπει να αξιοποιούν κατάλληλους μηχανισμούς ασφάλειας ώστε να διασφαλίζεται η εμπιστευτικότητα των δεδομένων αυτών.
	Επιθέσεις ενδιάμεσου (*Man-in-the-middle attacks*)	Αξιοποίηση ισχυρών μηχανισμών ασφάλειας

Πίνακας 6-1 Πιθανές Απειλές και Τρόποι Αντιμετώπισης

Απειλή		Τρόποι αντιμετώπισης
	Επιθέσεις επανάληψης (*Replay attacks*)	Δε θα πρέπει να γίνεται επεξεργασία δεδομένων που σχετίζονται με προηγούμενες συνόδους και μπορούν να επηρεάσουν την ορθή λειτουργία του συστήματος
	Υποκλοπή Συνόδου (Session hijacking)	
	Επιθέσεις πλαστοπροσωπίας (*Impersonation attacks*)	Τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να αποκαλύπτουν οποιαδήποτε δεδομένα που μπορεί να οδηγήσουν στην επίτευξη επιθέσεων πλαστοπροσωπίας
	Επιθέσεις πλημμύρας (*Flooding attacks*)	Αξιοποίηση κατάλληλων μηχανισμών ανίχνευσης επιθέσεων πλημμύρας
	Επιθέσεις τροποποίησης δεδομένων	Αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας
	Spoofing	Αξιοποίηση κατάλληλων μηχανισμών οι οποίοι δεν επιτρέπουν την κίνηση δεδομένων σε συγκεκριμένα τμήματα του δικτύου
Απειλές κατά τη διαδικασία εγγραφής	Πλαστοπροσωπία (*Impersonation*)	Αξιοποίηση κατάλληλων μηχανισμών ταυτοποίησης
	Αποποίηση Εγγραφής (*Registration Repudiation*)	Αξιοποίηση μηχανισμών μη-αποποίησης (*Non-repudiation*)
Άλλες Απειλές	Ιομορφικό λογισμικό (*Viral software*): • Ιός (*Virus*) • Δούρειος Ίππος (*Trojan horse*) • Σκουλήκια (*Worms*)	Άμεση ενημέρωση των υπολογιστών με τις νέες εκδοχές, τουλάχιστον σε ότι σχετίζεται με την ασφάλεια των υπολογιστικών συστημάτων (patches, ενημερώσεις ιών κτλ).
	Υπερχειλίσεις Προσωρινών Χώρων (B*uffer overflow*)	

Πίνακας 4-2 Πιθανές Απειλές και Τρόποι Αντιμετώπισης

Απειλή		Τρόποι αντιμετώπισης
	Μη εξουσιοδοτημένη είσοδος στο λειτουργικό σύστημα	

Πίνακας 7-3 Απειλές και Τρόποι Αντιμετώπισης

4.6.4 Τρόποι Αντιμετώπισης στα Πρωτόκολλα Αυθεντικοποίησης

Είναι πολύ σημαντικό να ελαχιστοποιηθούν ή αν είναι εύκολο να εξαλειφθούν τελείως οι απειλές στα πρωτόκολλα αυθεντικοποίησης αφού έτσι διασφαλίζεται η σωστή και αποτελεσματική λειτουργία του συστήματος. Έτσι, για κάθε απειλή που αναφέρθηκε για τα πρωτόκολλα αυθεντικοποίησης υπάρχει και ένας τρόπο αντιμετώπισης. Για την επίθεση με υποκλοπή δεδομένων υπηρεσίες και τα πρωτόκολλα Θα πρέπει να εξασφαλίζουν την μυστικότητα σημαντικών δεδομένων που χρησιμοποιούνται για την αυθεντικοποίηση καθώς επίσης και τα ευαίσθητα δεδομένα που μεταδίδονται από τις διαδικασίες αυτές. Μαυτό τον τρόπο δεν δίνεται η δυνατότητα στον επιτιθέμενο να υποκλέψει κάποια πληροφορία που να τον οδηγεί στα διακριτικά δεδομένα του χρήστη. Όταν υπάρχουν σημαντικές πληροφορίες και σημαντικά δεδομένα δεν θα πρέπει Να μεταδίδεται απλά η μη κρυπτογραφημένα αλλά θα πρέπει να χρησιμοποιούνται κατάλληλοι μηχανισμοί ασφαλείας.Οι επιθέσεις ενδιάμεσου, είναι δύσκολο να αντιμετωπιστούν. Για να ελαχιστοποιηθούν θα πρέπει να χρησιμοποιηθούν μηχανισμοί ασφαλείας όπως το πρωτόκολλο SSL που προστατεύει από τέτοιου είδους απειλές. Για την αντιμετώπιση των επιθέσεων επαναλήψεις και υποκλοπή συνόδων θα πρέπει τα δεδομένα που επεξεργάζονται κάθε φορά να είναι μοναδικά και να μην σχετίζονται με προηγούμενες σύνοδος ώστε να αποτρέψουν τον επιτιθέμενο να ακολουθήσει την αλληλουχία των δεδομένων. Στις περιπτώσεις υποκλοπής των δεδομένων θα πρέπει να αναφερθεί ξανά ότι κινδυνεύει όλο το σύστημα γι' αυτό και δεν θα πρέπει να μεταδίδονται σε μη κρυπτογραφημένη μορφή. Για να αντιμετωπιστεί η επίθεση πλαστοπροσωπίας θα πρέπει τα πρωτόκολλα να μην αποκαλύπτουν πληροφορίες που θα βοηθήσουν τον επιτιθέμενο στην εμφάνιση των νόμιμων διαπιστευτηρίων του χρήστη. Οι επιθέσεις πλημμύρας και οι επιθέσεις τροποποιήσεις δεδομένων είναι πολύ δύσκολες να εξαλειφθούν αλλά υπάρχει

τρόπος να εντοπιστούν και να αντιμετωπιστούν με τη χρήση κατάλληλων μηχανισμών ασφαλείας.Τέλος οι επιθέσεις απόκρυψη ταυτότητας μπορεί να ελαχιστοποιηθούν με την μείωση της μετάδοσης των δεδομένων σε περιορισμένα τμήματα του δικτύου.

4.6.5 Ανάλυση Κινδύνου

Τα στοιχεία ενός πληροφοριακού συστήματος Ηλεκτρονικής Διακυβέρνησης που θα πρέπει να προστατεύονται είναι το Υλικό, το Λογισμικό, οι πληροφορίες και τα δεδομένα, οι διαδικασίες, το προσωπικό και οι εγκαταστάσεις.

Αναλόγως το αγαθό έτσι κρίνεται και η αξία του. Πιο αναλυτικά, το αν αξίζει ή όχι ένα υλικό εξαρτάται άμεσα και από τα χρήματα που θα καταβληθούν για την τοποθέτηση, ενώ το αν αξίζει ή όχι ένα αγαθό θα εξαρτηθεί με τα αποτελέσματα που θα έχουν πάνω στο σύστημα από μια παράβαση της ασφάλειας στο πλαίσιο της ακεραιότητας ή της εμπιστευτικότητας. Απειλή (Threat) είναι όποια πράξη έχει αρνητικό αποτέλεσμα στο πληροφοριακό σύστημα. Τέτοιες απειλές είναι φυσικές απειλές-καταστροφές, απώλεια υπηρεσιών, καταστροφή/τροποποίηση/παρακολούθηση δεδομένων, σφάλματα και μη εξουσιοδοτημένες ενέργειες. Ευπάθεια (Vulnerability) είναι η ύπαρξη μιας αδυναμίας του πληροφοριακού συστήματος που μπορεί να οδηγήσει στην πραγματοποίηση μιας απειλής. Τέτοιες ευπάθειες είναι του υλικού, του λογισμικού, του δικτύου, του προσωπικού, της διοίκησης. Επίπτωση είναι το αποτέλεσμα μιας ολοκληρωμένης παραβίασης της ασφάλειας του πληροφοριακού συστήματος. Τέτοιες επιπτώσεις είναι η διαρροή, η τροποποίηση, η καταστροφή, η μη διαθεσιμότητα. Μετά τον υπολογισμό του επιπέδου κινδύνου, ακολουθεί η επιλογή και εφαρμογή μέτρων ασφαλείας (Countermeasures) με σκοπό τη διασφάλιση και προστασία του πληροφοριακού συστήματος. Αντίμετρο είναι μια διαδικασία που λειτουργεί στο πληροφοριακό σύστημα με στόχο να μειώσει την επικινδυνότητα. Τα πιθανά αντίμετρα κατηγοριοποιούνται σε φυσικά, σε διαδικαστικά, σε τεχνικά και σε προσωπικού.

Κεφάλαιο 5 Ηλεκτρονική Διακυβέρνηση και συστήματα Νεφοϋπολογιστικής

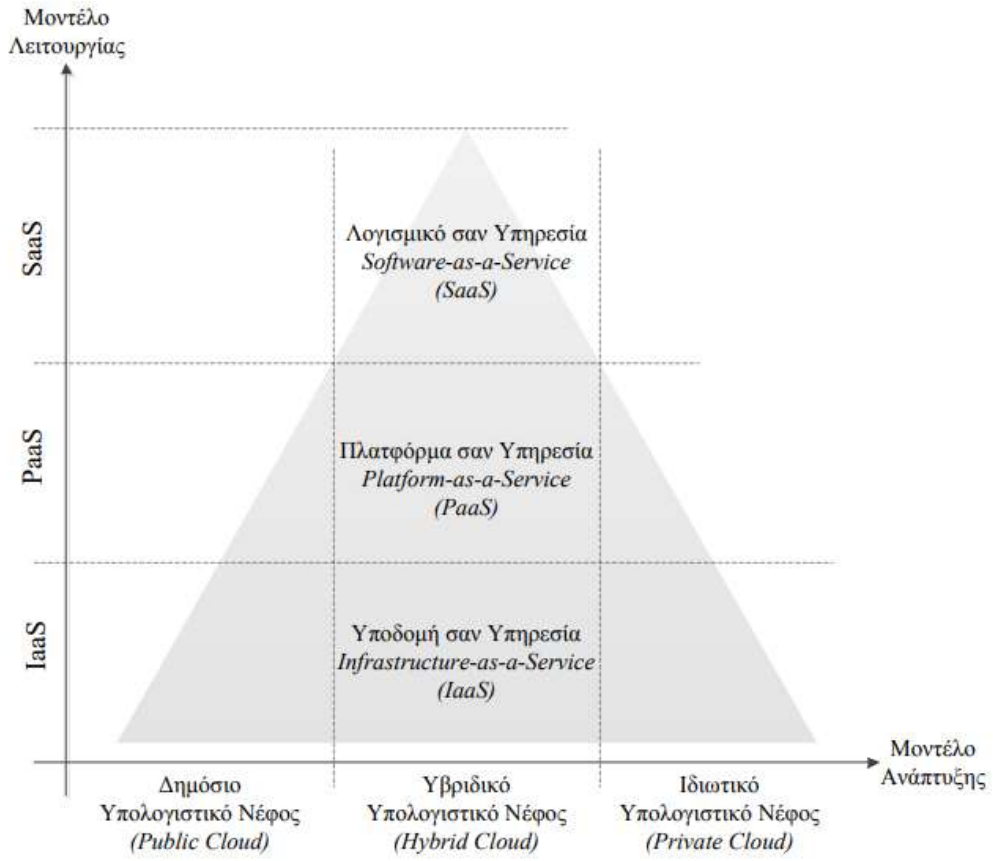
Με τον όρο σύστημα νεφοϋπολογιστικής αναφερόμαστε σε ένα σύστημα το οποίο διευκολύνει την πρόσβαση σε ένα περιβάλλον υπολογιστικών πόρων που μπορούν να τεθούν προς διάθεση και αξιοποίηση με την ελάχιστη αλληλεπίδραση με τον πάροχο τους.

5.1 Χαρακτηριστικά Συστημάτων

Τα χαρακτηριστικά των συστημάτων νεφοϋπολογιστικής είναι αρχικά ότι προσφέρει αυτοεξυπηρέτηση κατά απαίτηση όπου δίνεται η δυνατότητα στο χρήστη να μπορεί να δεσμεύει τους υπολογιστικούς του πόρους που γνωρίζει ότι χρειάζεται χωρίς να υπάρχει κάποια αλληλεπίδραση με τον πάροχο της υπηρεσίας, η ευρεία πρόσβαση στο δίκτυο αφού οι πόροι και οι υπηρεσίες είναι διαθέσιμοι μέσω δικτύου. Άλλο χαρακτηριστικό είναι η διαθεσιμότητα των πόρων, όπου ο συνδυασμός τόσο των φυσικών όσο και των εικονικών πόρων χρησιμοποιώντας το μοντέλο πολλαπλών μισθωτών μπορούν να εξυπηρετήσουν πολλούς χρήστες. Επιπλέον η ταχεία ελαστικότητα που σχετίζεται με τη δέσμευση και την αξιοποίηση των πόρων με γρήγορο ρυθμό ώστε η αλλαγή από μη διαθέσιμοι σε διαθέσιμοι να γίνεται με τον ελάχιστο χρόνο. Τελευταίο χαρακτηριστικό είναι η μετρούμενη υπηρεσία η οποία είναι πολύ σημαντική αφού είναι αυτή που οργανώνει και βελτιώνει τη διάθεση των πόρων με συγκεκριμένες μεθοδολογίες και κατώφλια.
Τα συστήματα νεφοϋπολογιστικής αποτελούνται και από μοντέλα παροχής υπηρεσιών. Αρχικά ένα τέτοιο μοντέλο είναι το λογισμικό σαν υπηρεσία όπου με τη βοήθεια του αξιοποιούνται και χρησιμοποιούνται οι εφαρμογές σε αυτά τα περιβάλλοντα. Επόμενο μοντέλο είναι η πλατφόρμα σαν υπηρεσία, όπου για την παροχή λογισμικού σαν υπηρεσία και για την ανάπτυξη εφαρμογών μαζί με τον σχεδιασμό την εκτέλεση και την αποσφαλμάτωση γίνεται χρήση πλατφορμών. Τελευταίο μοντέλο παροχής υπηρεσιών είναι η υποδομή σαν υπηρεσία όπου υπολογιστικές υποδομές αξιοποιούνται όπως για παράδειγμα η επεξεργαστική ισχύ και ο χώρος αποθήκευσης.
Τα συστήματα νεφοϋπολογιστικής αποτελούνται επίσης και από μοντέλα

ανάπτυξης όπως είναι το ιδιωτικό όπου λειτουργεί μόνο για έναν οργανισμό, το δημόσιο που μπορεί να λειτουργεί σε παραπάνω από έναν οργανισμό, η κοινότητα η οποία λειτουργεί σε μια συγκεκριμένη κοινότητα το υβριδικό όπου λειτουργούν διάφορα μοντέλα ανάπτυξης μαζί και διασυνδέονται και ανταλλάσσουν δεδομένα και πληροφορίες.

Παρακάτω παρουσιάζεται ο συνδυασμός των μοντέλων ανάπτυξης και λειτουργίας στα συστήματα νεφοϋπολογιστικής.

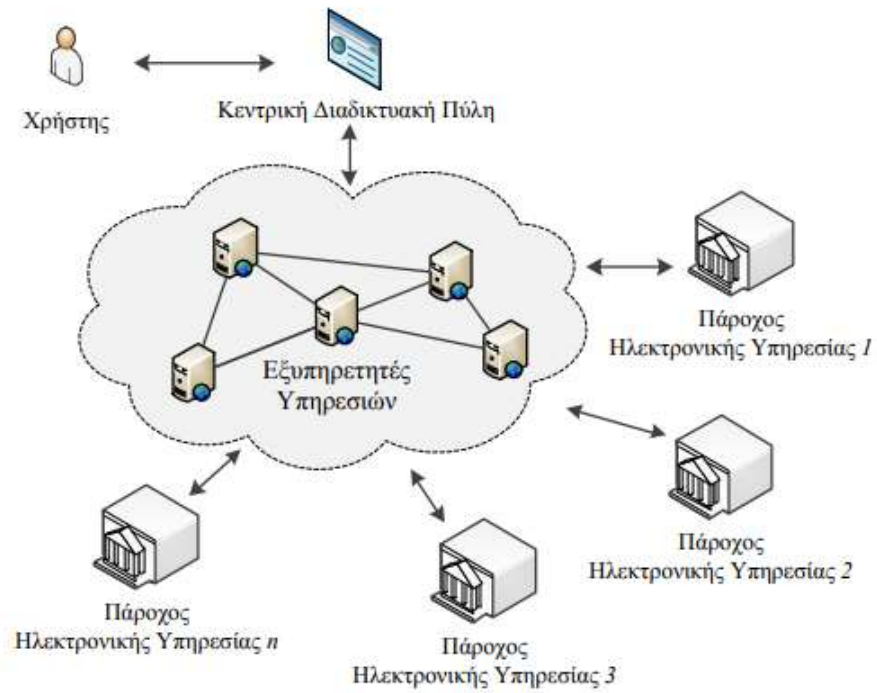


Εικόνα 13 Λειτουργία Συστημάτων Νεφοϋπολογιστικής

5.2 Η εφαρμογή της Ηλεκτρονικής Διακυβέρνησης σε Νεφοϋπολογιστικό Σύστημα

Ένα μεγάλο ερώτημα θα ήταν αν η δημόσια διοίκηση θα μπορούσε να μεταφερθεί σε ένα νεφοϋπολοστικό περιβάλλον. Αυτό θα σήμαινε μια τεράστια αλλαγή όσον

αφορά την δομή της δημόσιας διοίκησης, αλλά και τις λειτουργίες γενικότερα. Στη μορφή που είναι τώρα υπάρχουν και διατηρούνται εξυπηρετητές για κάθε παροχή υπηρεσίας ενώ αν μεταφερθεί στον νεφοϋπολοστικό περιβάλλον δεν θα υπάρχει ξεκάθαρος ρόλος των εξυπηρετών των υπηρεσιών που προσφέρονται στους πολίτες. Με τη μετάβαση αυτή θα μπορεί να γίνει ταυτόχρονη χρήση και αξιοποίηση των υπολογιστικών πόρων καθώς και των υπηρεσιών και των εφαρμογών και των δεδομένων από όλους τους τομείς της δημόσιας διοίκησης και με αυτό τον τρόπο θα αυξηθεί η αποδοτικότητα, η παραγωγικότητα, θα διευκολυνθεί η διασύνδεση των ηλεκτρονικών υπηρεσιών καθώς επίσης θα μειωθεί κατά πολύ το κόστος συντήρησης αλλά και εκσυγχρονισμού σε σχέση με την υπάρχουσα κατάσταση.



Εικόνα 14 Η εφαρμογή της Ηλεκτρονικής Διακυβέρνησης σε Νεφοϋπολογιστικό Σύστημα

Για να γίνει μια τέτοια μετάβαση η δημόσια διοίκηση πρέπει να λάβει υπόψη την επιλογή μοντέλου ανάπτυξης και λειτουργίας βασισμένη στις απαιτήσεις αλλά και στους κανόνες του τομέα που παρέχει την ηλεκτρονική υπηρεσία. Επίσης θα

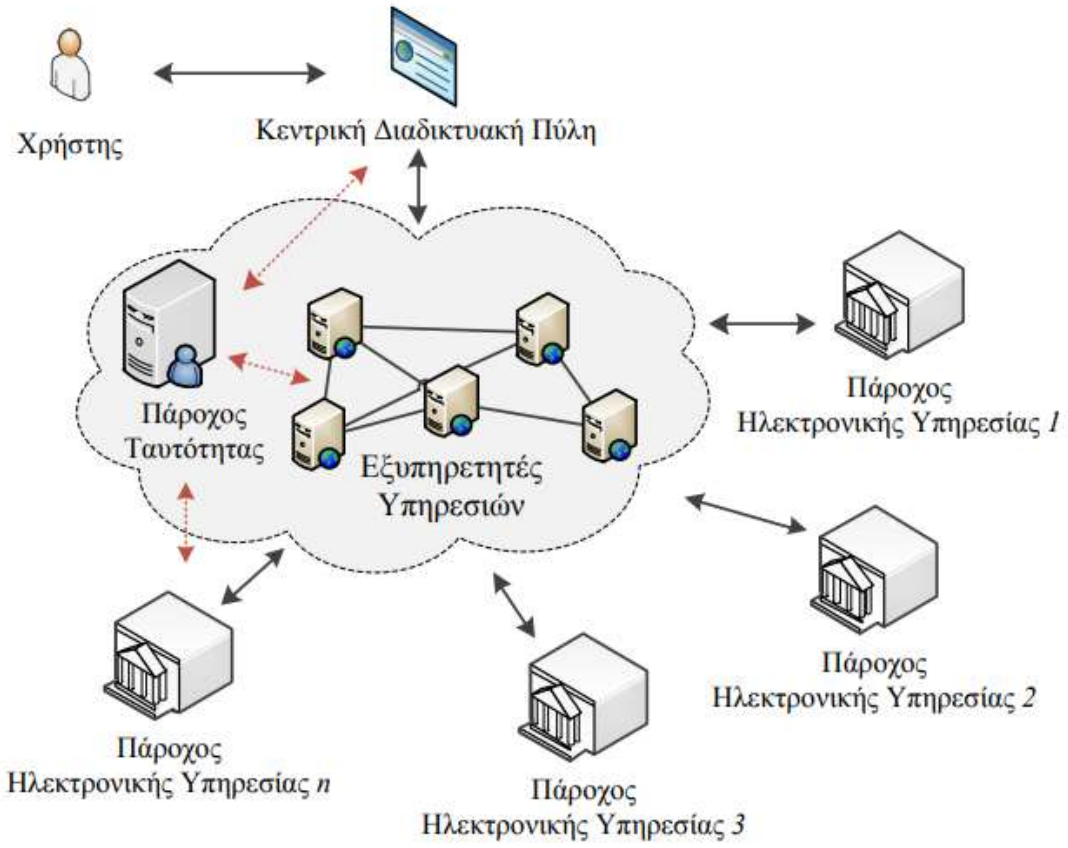
πρέπει να λάβει υπόψη την επεκτασιμότητα ώστε οι υπολογιστικοί πόροι να είναι ευέλικτοι και να παρέχονται οργανωμένα για κάθε υπηρεσία. Η διασφάλιση της διαθεσιμότητας καθώς επίσης και των επιπέδων ασφάλειας και ιδιωτικότητας είναι επίσης κάποια ζητήματα που πρέπει να λάβει υπόψιν της η δημόσια διοίκηση πριν κάνει τη μετάβαση αυτή. Η δημόσια διοίκηση θα πρέπει να λάβει υπόψη τα ανοικτά πρότυπα ώστε να υπάρχει μεγαλύτερη διαλειτουργικότητα για να μην υπάρχουν περιορισμοί από άλλες τεχνολογίες. Τέλος η δημόσια διοίκηση θα πρέπει να διασφαλίσει τις υπηρεσίες και τις διαδικασίες που προσφέρονται ηλεκτρονικά από αυτό το περιβάλλον σε νομικό πλαίσιο να γίνει ανάλυση του προϋπολογισμού της επένδυσης καθώς και να υπάρξει μια στρατηγική συντονισμού όλων των συστημάτων.

5.3 Ασφάλεια και Ιδιωτικότητα

Ένας βασικός παράγοντας στα συστήματα που παρέχουν ηλεκτρονικές υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι η ασφάλεια των δεδομένων καθώς και των υπηρεσιών. Όπως έχει αναφερθεί και παραπάνω αυτό που απειλεί ένα πληροφοριακό σύστημα είναι η μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή σε υπηρεσίες η άρνηση συμμετοχής σε παροχή υπηρεσίας κάποιου χρήστη, η παραβίαση της ιδιωτικότητας και η παράνομη πρόσβαση σε ευαίσθητα δεδομένα. Οι σημαντικότερες απειλές οι οποίες εμφανίζονται στα νεφοϋπολογιστικά συστήματα είναι αρχικά η απώλεια διακυβέρνησης όπου τον πλήρη έλεγχο για θέματα ασφάλειας και ιδιωτικότητας τον έχει πλέον ο πάροχος των νεφοϋπολογιστικών συστημάτων. Άλλος κίνδυνος είναι η εξάρτηση αφού ο πάροχος δεν σιγουρεύει την μεταφορά των δεδομένων και των υπηρεσιών λόγω της μη ύπαρξης χρήσιμων προτύπων και τεχνολογιών. Άλλος κίνδυνος στα νεφοϋπολογιστικά συστήματα είναι λόγω του ότι κάποιοι πόροι είναι κοινόχρηστοι μπορεί να επιφέρει απειλές στην ασφάλεια και στην προστασία των δεδομένων καθώς και των υπηρεσιών σε περίπτωση που υπάρξει κάποια αποτυχία απομόνωσης από τους υπόλοιπους πόρους. Τέλος, η αλλαγή στα νεφοϋπολογιστικά συστήματα μπορεί να δημιουργήσει πρόβλημα Κατά την τήρηση συγκεκριμένων προτύπων ασφαλείας και επίσης είναι δύσκολο να παρακολουθηθεί η απόδοση των μεθοδολογιών και των διαδικασιών που χρησιμοποιούνται για την προστασία των δεδομένων και της ιδιωτικότητας.

5.4 Διαχείριση Ψηφιακών Ταυτοτήτων

Όπως η επιλογή μοντέλου ανάπτυξης είναι άμεσα συνδεδεμένη με τον κίνδυνο που μπορεί να προκληθεί στο σύστημα το ίδιο μπορεί να γίνει και με την διαχείριση των ψηφιακών ταυτοτήτων. Παρακάτω βλέπουμε ότι ένας πάροχος ταυτότητας μπορεί να αλληλεπιδράσει με άλλους παρόχους και έτσι να ολοκληρωθεί η διαδικασία.



Εικόνα 15Πάροχος Ταυτότητας

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΚΤΠ, 2008. Πλαίσιο Διαλειτουργικότητας και Υπηρεσιών Ηλεκτρονικών Συναλλαγών, Αθήνα: Κοινωνία της Πληροφορίας Α.Ε..

e-GIF, 2009. Greek e-Government Interoperability Framework. [Online] Available at: http://www.e-gif.gov.gr/ [Accessed 6 4 2013].

Οδηγίες Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL).

Clarke, R., 1997. Introduction to Dataveillance and Information Privacy, and Definitions and Terms, Australia: Xamax Consultancy Pty Ltd.

Massey, A. & Antón, A., 2008. A Requirements-based Comparison of Privacy Taxonomies. Washington, IEEE CPS.

Μήτρου, Λ., 2002. Το δίκαιο στην κοινωνία της πληροφορίας. 1 ed. Αθήνα: Σάκκουλα.

Μήτρου, Λ., 2006. Προστασία Προσωπικών Δεδομένων, Σάμος: Πανεπιστήμιο Αιγαίου

Ιγγλεζάκης, Ι., 2007. Εισαγωγή στο δίκαιο της πληροφορικής. 1 ed. Αθήνα: Σάκκουλα.

Westin, A., 1967. Privacy and Freedom. 1 ed. London: The Bodley Head.

Vrakas, N., Kalloniatis, C., Tsohou, A. & Lambrinoudakis, C., 2010. Privacy Requirements Engineering for Trustworthy e-Government Services. Berlin, Springer LNCS.

Fischer-Hübner, S., 2001. Design and Use of Privacy-Enhancing Security Mechanisms. In: K. Brunnstein, ed. IT-Security and Privacy. 1 ed. Hamburg: Springer LNCS, pp. 107 - 166.

Ferguson, N. & Schneier, B., 2003. Practical Cryptography. 1 ed. London: Wiley..

Γκρίτζαλης, Σ., Κάτσικας, Σ. & Γκρίτζαλης, Δ., 2003. Ασφάλεις Δικτύων Υπολογιστών. 2003 ed. Αθήνα: Παπασωτηρίου.

Schneier, B., Goodrich, M. & Tamassia, R., 2006. Introduction to Security and Applied Cryptography. 1 ed. London: John Wiley & Sons

Καμπουράκης, Γ., ΓΚρίτζαλης, Σ. & Κάτσικας, Σ., 2006. Ασφάλεια Ασυρμάτων και Κινητών Δικτών Επικοινωνιών. 1 ed. Αθήνα : Παπασωτηρίου.

Burr, W. et al., 2011. Electronic Authentication Guidelines - Special Publication 800-63-1, Gaithersburg: NIST.

Rosenberg, R., 1992. The Social Impact of Computers, San Diego: Academic Press.

Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, Σάμος: Πανεπιστήμιο Αιγαίου