ΤΕΙ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

Ηλεκτρονική διακυβέρνηση: Ζητήματα ασφαλείας και προσβασιμότητας των πληροφοριών που διακινούνται ηλεκτρονικά

THESIS:

E-government: Issues of safety and accessibility of information handled electronically

Σπουδαστές:

Αργυροπούλου Ξανθίππη

Μπεκιάρη Αργυρώ

Εποπτεύων καθηγητής:

Χόχολης Διονύσιος

ΑΜΑΛΙΑΔΑ 2012

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον κ. Χόχολη για την πολύτιμη βοήθεια του για την εκπόνηση της πτυχιακής μας εργασίας, καθώς και όλους τους συγγενείς αλλά και φίλους για την αμέριστη συμπαράσταση τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή στοχεύει στο να αναλύσει τα ζητήματα προσβασιμότητας και ασφάλειας που ανακύπτουν από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης. Αρχικά στο 1^{ο} κεφάλαιο γίνεται μια γενική αναφορά στη φύση της Ηλεκτρονικής Διακυβέρνησης και στους τύπους αλληλεπίδρασης σε αυτήν. Στο 2^{ο} κεφάλαιο ξεκαθαρίζεται η έννοια του όρου «Προσβασιμότητα», διευκρινίζονται οι λόγοι για τους οποίους είναι αναγκαία η Προσβασιμότητα στα πλαίσια μίας επιτυχημένης Ηλεκτρονικής Διακυβέρνησης καθώς και οι παράγοντες εκείνοι που εμποδίζουν την πρόσβαση. Έπειτα παραπείθονται τρόποι με τους οποίους εξασφαλίζεται και διευκολύνεται η προσβασιμότητα. Στο 3^{ο} κεφάλαιο αναλύονται κάποια από τα κυριότερα ζητήματα ασφάλειας τα οποία προκύπτουν από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης όπως η προστασία των προσωπικών δεδομένων των πολιτών, η κακόβουλες ενέργειες με τη χρήση κακόβουλων λογισμικών και εν τέλει παρουσιάζονται κάποιοι από τους τρόπους με τους οποίους κατορθώνεται να διασφαλιστούν τα προσωπικά δεδομένα άλλα και οι ηλεκτρονικές συναλλαγές. Στο 4^{ο} κεφάλαιο γίνεται παρουσίαση των πιο σημαντικών κυβερνητικών Διαδικτυακών τόπων, οι οποίοι παρέχουν ηλεκτρονικές υπηρεσίες προς τους πολίτες, τις επιχειρήσεις και άλλους δημόσιους φορείς. Στόχος είναι να διαπιστωθεί κατά πόσο οι κυβερνητικές ιστοσελίδες και οι πύλες ηλεκτρονικής διακυβέρνησης εξασφαλίζουν την προσβασιμότητα και την ασφάλεια των συναλλαγών καθώς και των προσωπικών δεδομένων των πολιτών. Ως εκ τούτου οι Διαδικτυακοί αυτοί τόποι εξετάζονται ως προς αυτά τα σημεία, την προσβασιμότητα και την ασφάλεια. Τέλος στο 5^{ο} και τελευταίο κεφάλαιο παρατίθενται τα συμπεράσματα για την επικρατούσα κατάσταση σχετικά με την προσβασιμότητα και την ασφάλεια της Ηλεκτρονικής Διακυβέρνησης στην χώρα μας.

ABSTRACT

This thesis aims to analyze the accessibility and safety issues arising from the implementation of e-Government. Initially the first chapter is a general reference to the nature of e-Government and the types of interaction in it. In the second chapter the concept of "Accessibility" is clarified, explaining the reasons why accessibility is necessary in a successful e-Government and mainly the factors that impede access. Then ways are apposed to ensure and facilitate accessibility. In the third chapter some of the major safety issues arising from the implementation of e-Government are analyzed, such as the protection of personal data of citizens, the malicious actions by malicious software, and finally some of the ways which manage to secure personal data and other electronic transactions are presented. In the fourth chapter are introduced some of the most important government Web sites that provide online services to citizens, businesses and other public services. The aim is to be determined whether the government websites and e-government portals ensure accessibility and security of transactions and personal data of citizens. Therefore this websites are examined for these points, accessibility and security. Finally in the fifth and last chapter are presented the conclusions about the situation on the accessibility and security of e-Government in our country.

ΕΙΣΑΓΩΓΗ

Στόχος της παρούσας πτυχιακής, είναι να αποδώσει σε βάθος το περιεχόμενο του όρου της Ηλεκτρονικής Διακυβέρνησης, να καταγραφούν και να μελετηθούν όλα τα θέματα που βοηθούν ώστε να γίνουν οι ηλεκτρονικές υπηρεσίες πιο προσβάσιμες για όλο το κοινωνικό σύνολο, δηλαδή όχι μόνο για έμπειρους χρήστες του υπολογιστή και του διαδικτύου, αλλά και για άλλες κοινωνικές ομάδες που δεν είναι ιδιαίτερα ή και καθόλου εξοικειωμένοι με την χρήση αυτών, ώστε να είναι σε θέση να λάβουν, να διακινήσουν και να ανταλλάξουν πληροφορίες μέσα απ' το διαδίκτυο.

Με γνώμονα την Ευρωπαϊκή Ένωση και όσα προβλέπει για τη λειτουργικότητα μεταξύ των κρατικών υπηρεσιών για την ελάττωση της γραφειοκρατίας, η παροχή ελεύθερης πρόσβασης στους πολίτες είναι πέρα από υποχρέωση του κράτους, απαραίτητη λειτουργία στην εποχή μας. Μέσα σε αυτό το θέμα, θα δούμε τι συμβαίνει όσον αφορά τα παραπάνω ζητήματα στην Ελλάδα και τι πρέπει να γίνει για να μπορούν όλοι να χρησιμοποιήσουν το διαδίκτυο και τις e-υπηρεσίες που προσφέρονται. Επιπλέον, θα εξεταστούν ζητήματα που έχουν να κάνουν με την ασφάλεια των προσωπικών δεδομένων και των προσφερόμενων ηλεκτρονικών συναλλαγών.

Κεφάλαιο 1
Ηλεκτρονική Διακυβέρνηση

Το κεφάλαιο αυτό έχει ως στόχο να εισάγει τον αναγνώστη στην έννοια της ηλεκτρονικής διακυβέρνησης, να διευκρινίσει τους στόχους της και να παρουσιάσει τους τύπους της ηλεκτρονικής διακυβέρνησης βάσει των αλληλεπιδρόμενων κοινοτήτων που δρουν στα πλαίσια της.

1.1. Ορισμός

Η *Ηλεκτρονική διακυβέρνηση* θα μπορούσε να χαρακτηριστεί ως η χρήση των δυνατοτήτων της τεχνολογίας της πληροφορίας και των τηλεπικοινωνιών για τη δημιουργία μοντέλων και εφαρμογών πρόσβασης και παροχής υπηρεσιών από το κράτος προς τους πολίτες και τη δημόσια διοίκηση και περιλαμβάνει τόσο τη ροή πληροφοριών ανάμεσα στα διάφορα τμήματα της δημόσιας διοίκησης, όσο και την παροχή πληροφοριών και υπηρεσιών προς τους πολίτες και τις επιχειρήσεις.

1.2. Ιστορική αναδρομή ηλεκτρονικής διακυβέρνησης

Στις αρχές του νέου αιώνα, οι κυβερνήσεις συνειδητοποίησαν ότι το Internet που είχε ήδη επικρατήσει στον ιδιωτικό τομέα, θα μπορούσε να χρησιμοποιηθεί με ανάλογο τρόπο και από το κράτος για την εξυπηρέτηση των πολιτών και των επιχειρήσεων. Στο πλαίσιο αυτό άρχισε να αναπτύσσεται ένα νέο μοντέλο δημόσιας διοίκησης που ονομάστηκε ηλεκτρονική διακυβέρνηση. Αρχικώς, αυτός ο όρος συνδέθηκε με τη χρήση του Διαδικτύου για τη διεκπεραίωση των συναλλαγών του κοινού με το κράτος. Για παράδειγμα, ένας πολίτης θα μπορούσε να υποβάλει τη φορολογική του δήλωση, απευθείας, από το σπίτι του, χρησιμοποιώντας τον προσωπικό του υπολογιστή. Στη συνέχεια διαπιστώθηκε πως το Διαδίκτυο θα μπορούσε να χρησιμοποιηθεί και για την ενδυνάμωση της συμμετοχής των πολιτών στις δημοκρατικές διαδικασίες. Πολλοί άρχισαν να ομιλούν για την αναβίωση της αθηναϊκής δημοκρατίας.

Όπως είναι γνωστό, στην αρχαία Αθήνα αναπτύχθηκε και άνθισε η άμεση δημοκρατία όπου οι πολίτες συγκεντρώνονταν στην Αγορά και συναποφάσιζαν για τα κοινά. Σήμερα, κατά ανάλογο τρόπο, θα μπορούσε να δημιουργηθεί μια εικονική "Αγορά" στο Διαδίκτυο, όπου οι πολίτες θα έχουν τη δυνατότητα να διαβουλεύονται με τη διοίκησή τους ή και να ψηφίζουν για θέματα που τους αφορούν. Βάσει αυτών η Ευρωπαϊκή Ένωση γενίκευσε τις νέες ιδέες και ορίζει ότι: "Ηλεκτρονική διακυβέρνηση είναι η χρήση των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών στη δημόσια διοίκηση σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό τη βελτίωση της

εξυπηρέτησης του κοινού, την ενδυνάμωση της δημοκρατίας και την υποστήριξη των δημόσιων πολιτικών". Ο ορισμός αυτός καθορίζει δύο θεμελιώδεις αρχές:

1. Οριοθετεί τους στόχους της ηλεκτρονικής διακυβέρνησης σε τρεις συγκεκριμένους τομείς:

   - Εξυπηρέτηση των πολιτών και των επιχειρήσεων
   - Βελτίωση των δημοκρατικών διαδικασιών
   - Υποστήριξη των δημόσιων πολιτικών.

2. Συνδέει άρρηκτα την ηλεκτρονική διακυβέρνηση με ευρύτατες οργανωτικές αλλαγές στο εσωτερικό της δημόσιας διοίκησης

Πράγματι, σήμερα οι κυβερνήσεις δηλώνουν ότι η ηλεκτρονική διακυβέρνηση δεν περιορίζεται στην αυτοματοποίηση των διαδικασιών, αλλά αποτελεί το πιο σημαντικό εργαλείο για μια ευρεία διοικητική μεταρρύθμιση όπου οι νέες τεχνολογίες διαδραματίζουν ένα νέο ρόλο. [1]

1.3. Εφαρμογές Ηλεκτρονικής Διακυβέρνησης

Η ηλεκτρονική δημόσια διοίκηση ("e-government") αποτελεί μία από τις προτεραιότητες που τέθηκαν στο σχέδιο δράσης eEurope2005 . Αποτελεί ουσιαστικό μοχλό για την παροχή αποτελεσματικότερων και καλύτερης ποιότητας δημόσιων υπηρεσιών, για τη μείωση του χρόνου αναμονής των χρηστών, τη βελτίωση της διαφάνειας και της υπευθυνότητας των υπηρεσιών.[2] Η ηλεκτρονική διακυβέρνηση είναι στενά διασυνδεδεμένη και μοιράζεται παρόμοια χαρακτηριστικά με το e-commerce και το e-business σε σχέση με την χρήση και την εφαρμογή της τεχνολογίας του Διαδικτύου, την αναδιοργάνωση των ενδο-επιχειρησιακών δομών και διαδικασιών και την δημιουργία νέων υπηρεσιών προϊόντων και καναλιών για τους τελικούς χρήστες ή καταναλωτές. Οι κύριοι οδηγοί για την εφαρμογή του e-government πηγάζει απ' την αντιγραφή του e-commerce στον ιδιωτικό τομέα. Η κυβέρνηση αναμένει παρόμοια αύξηση της αποτελεσματικότητας, βελτίωση της αποδοτικότητας και οικονομία κόστους, όμοια με αυτές του ιδιωτικού τομέα καθώς οι πολίτες προσδοκούν το ίδιο επίπεδο και υπηρεσίες από την κυβέρνηση με αυτές που τους παρέχονται από τον ιδιωτικό τομέα [3][4]. Ωστόσο, η ηλεκτρονική διακυβέρνηση είναι μοναδική στο είδος της εξαιτίας του ρόλου που διαδραματίζει στη σχέση μεταξύ της κυβέρνησης και των πολιτών της καθώς και της διακυβέρνησης των εθνών.

Η ηλεκτρονική διακυβέρνηση έχει καταστεί πιο σημαντική παρά ποτέ και μπορεί να παρέχει ασταμάτητα κυβερνητικές υπηρεσίες πληροφοριών στους πολίτες, στις επιχειρήσεις, στους δημόσιους υπαλλήλους, στους διαχειριστές της διακυβέρνησης και στις κυβερνητικές υπηρεσίες μέσω ενός δικτύου. Υπάρχουν πολλά ζητήματα στην ηλεκτρονική διακυβέρνηση που χρειάζονται προσεκτική διερεύνηση, όπως ζητήματα ασφαλείας, απαιτήσεις υπηρεσιών του e-government, μοντέλα e-government, στρατηγική και πολιτική της ηλεκτρονικής διακυβέρνησης και των τομέων της.

Εμείς θα εξετάσουμε τα ζητήματα ασφάλειας και προσβασιμότητας που ανακύπτουν στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Πρώτα όμως, θα πρέπει να εξετάσουμε όλα τα συμμετέχοντα μέρη σε ένα σύστημα ηλεκτρονικής διακυβέρνησης.

Υπάρχουν τέσσερις βασικές κατηγορίες αλληλεπιδρόμενων κοινοτήτων, οι εφαρμογές της ηλεκτρονικής διακυβέρνησης βάση αυτών των κοινοτήτων διακρίνονται στις εξής.

Ø Κυβέρνηση προς Κυβέρνηση Ηλεκτρονική διακυβέρνηση (G-to-G e-government)

Αυτή η μορφή υποστηρίζει την ανταλλαγή πληροφοριών μεταξύ εσωτερικών κυβερνητικών υπηρεσιών όπως το σύστημα των επίσημων εγγράφων που λαμβάνονται και αποστέλλονται.

Ø Κυβέρνηση προς Κυβερνητικούς υπαλλήλους (G-to-Officeholders e-government)

Αυτή η μορφή υποστηρίζει τους ενδοεπιχειρησιακούς κυβερνητικούς υπαλλήλους, των οργανισμούς δημοσίων υποθέσεων και τις συνεργατικές διαδικασίες των δευτεροβάθμιων οργανισμών των δημοσίων υποθέσεων.

Ø Κυβέρνηση προς πολίτη ηλεκτρονική διακυβέρνηση(G-to-C e-government)

Οι πολίτες είναι ενήμεροι για τις υπηρεσίες που παρέχονται από την κυβέρνηση μέσω του δικτύου επικοινωνίας και χρησιμοποιούν τις υπηρεσίες με τις προσωπικές τους ταυτότητες μέσω ασφαλών μηχανισμών, το e-voting και το e-assistance είναι δύο χαρακτηριστικά παραδείγματα.

Ø Κυβέρνηση προς επιχείρηση ηλεκτρονική διακυβέρνηση (G-to-B e-government)

Οι επιχειρήσεις είναι ενήμερες για τις υπηρεσίες που παρέχονται από την διακυβέρνηση μέσω του δικτύου επικοινωνίας και χρησιμοποιούν τις υπηρεσίες με την ταυτότητα ενός νομικού προσώπου μέσω ασφαλών μηχανισμών. Παραδείγματα αυτού είναι η τελωνειακή δήλωση και ο εκτελωνισμός αγαθών μέσω Διαδικτύου.

Ø Πολίτης προς πολίτη ηλεκτρονική διακυβέρνηση (C-to-C e-government)

Σε αυτή τη μορφή ηλεκτρονικής διακυβέρνησης, η κυβέρνηση κατέχει μεσάζοντα ρόλο για την ανταλλαγή πληροφοριών. Τυπικό παράδειγμα είναι το ακόλουθο: Η κυβέρνηση στη προσπάθεια της να διορθώσει μια κοινωνική αδικία προσφέρει προσωρινές εργασίες στα θύματα μιας φυσικής καταστροφής, ώστε να μπορέσουν να εργαστούν στο δημόσιο ή στον ιδιωτικό τομέα.

Ø Επιχείρηση προς επιχείρηση ηλεκτρονική διακυβέρνηση (B-to-B e-government)

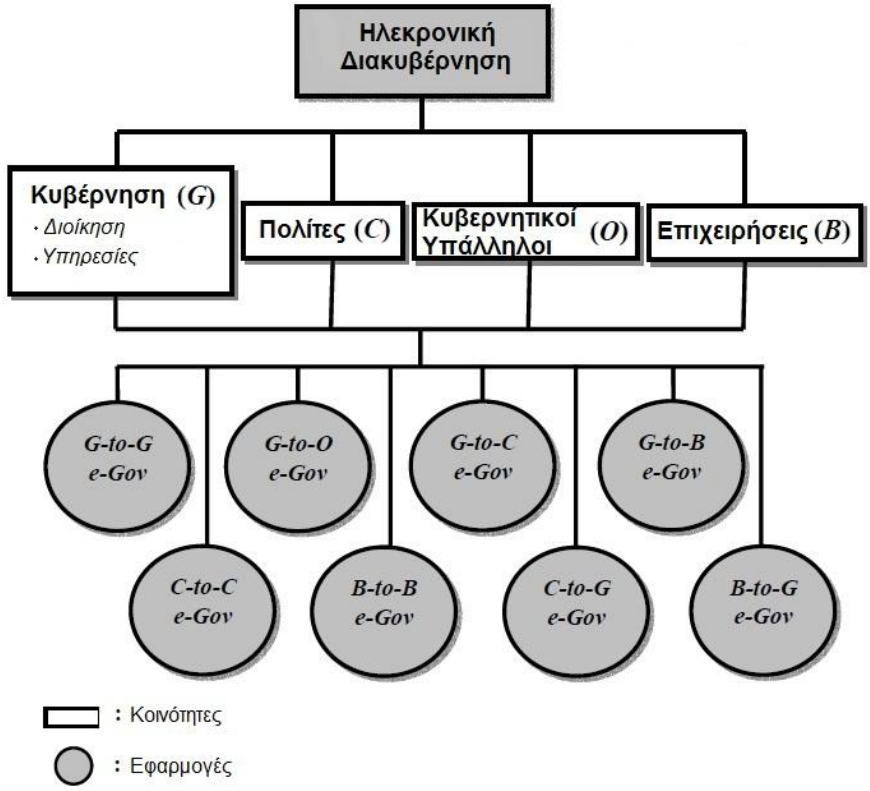
Ομοίως με την προαναφερθείσα εφαρμογή (Πολίτης-προς-πολίτη), σε αυτή την εφαρμογή η κυβέρνηση διαδραματίζει μεσολαβητικό ρόλο στην ανταλλαγή πληροφοριών. Για παράδειγμα, η κυβέρνηση μπορεί να προσκαλέσει επιχειρήσεις να προβούν σε προσφορές για αναθέσεις έργων που περιέχουν ευαίσθητες πληροφορίες. Αυτές οι επιχειρήσεις θα μπορούσαν να παράγουν το πολεμικό υλικό της χώρας.

Ø Πολίτες προς κυβέρνηση ηλεκτρονική διακυβέρνηση(C-to-G e-government)

Αυτή η ηλεκτρονική υπηρεσία έχει διαμορφωθεί βάση των απαιτήσεων των πολιτών (με γνώμονα την συνολική ζήτηση). Οι πολίτες αιτούνται υποστήριξης ή ζητούν ιθαγένεια για παράδειγμα.

Ø Επιχείρηση προς Κυβέρνηση ηλεκτρονική διακυβέρνηση(B-to-G e-government)

Όπως και παραπάνω(C-to-G) αυτή η εφαρμογή έχει διαμορφωθεί βάσει των απαιτήσεων των επιχειρήσεων. Για παράδειγμα, οι επιχειρήσεις ζητούν κυβερνητική υποστήριξη ή προτάσεις από άλλες επιχειρήσεις.[5]



Εικόνα 1: Οι κοινότητες και οι εφαρμογές τους στην Ηλεκτρονική Διακυβέρνηση

Κεφάλαιο 2
Ζητήματα Προσβασιμότητας στην Ηλεκτρονική Διακυβέρνηση

Στο κεφάλαιο 2 αρχικά θα μελετηθεί η έννοια του όρου «Προσβασιμότητα», οι λόγοι για τους οποίους είναι αναγκαία η Προσβασιμότητα στα πλαίσια μίας επιτυχημένης Ηλεκτρονικής Διακυβέρνησης καθώς και οι παράγοντες εκείνοι που εμποδίζουν την πρόσβαση. Έπειτα θα παρατεθούν τρόποι εξασφάλισης της προσβασιμότητας όπως οι οδηγίες για την Προσβασιμότητα και τεχνικής φύσεως τρόποι για τη διευκόλυνση της προσβασιμότητας.

2.1. Τι είναι προσβασιμότητα

Με τον όρο προσβασιμότητα νοείται το χαρακτηριστικό του περιβάλλοντος, που επιτρέπει σε όλα τα μέλη της κοινωνίας χωρίς διακρίσεις φύλου, ηλικίας και λοιπών χαρακτηριστικών (σωματική διάπλαση, δύναμη, αντίληψη κλπ) να μπορούν αυτόνομα, με ασφάλεια και με άνεση να προσεγγίσουν και να χρησιμοποιήσουν τις προσφερόμενες υποδομές, υπηρεσίες και αγαθά. Η προσβασιμότητα είναι το βασικό προαπαιτούμενο για την εξασφάλιση της ισότητας των πολιτών, διασφαλίζοντας το δικαίωμα κάθε ενός στις προσωπικές επιλογές, στην αυτονομία και την αξιοπρέπεια. [6]

2.2. Η προσβασιμότητα στο διαδίκτυο

Η προσβασιμότητα στο διαδίκτυο και ειδικότερα στις σελίδες των κυβερνητικών φορέων και των δημοσίων υπηρεσιών είναι ένα από τα σημαντικότερα ζητήματα που ανακύπτουν με την εφαρμογή της ηλεκτρονικής διακυβέρνησης. Μια πρόσφατη μελέτη δείχνει ότι η χρηστικότητα των ιστοσελίδων είναι σε μέσο όρο τρεις φορές υψηλότερη για τους χρήστες χωρίς αναπηρία παρά για εκείνους που είναι τυφλοί ή έχουν μειωμένη όραση [7]**.**

Ένα άλλο ερευνητικό έργο που δημοσιεύεται από τη Forrester Research [8] διαπίστωσε ότι μόνο ένα στα τέσσερα e-commerce sites που ρωτήθηκαν πληρούν τις στοιχειώδεις απαιτήσεις που προβλέπονται από την Πρωτοβουλία Προσβασιμότητας στον Παγκόσμιο Ιστό *(Web Accessibility Initiative, www.w3.org/WAI/)* για χρήστες με ειδικές ανάγκες του Παγκόσμιου Ιστού, όπως η παροχή κειμένου περιγραφής των εικόνων για τους τυφλούς. Ο Waddell [9] καλεί το Web ως *«την αυξανόμενη ψηφιακή συσκευή στην πρόσβαση για τα άτομα με ειδικές ανάγκες.»* Ακόμα και στο δημόσιο τομέα των ΗΠΑ, όπου πρόσβαση στο διαδίκτυο είναι νομικά επιβεβλημένη, ένας σημαντικός αριθμός των

επίσημων ιστοσελίδων εξακολουθούν να περιέχουν χαρακτηριστικά που δεν παρέχουν εύλογη πρόσβαση σε χρήστες με ειδικές ανάγκες [10].

2.3. Αναγκαιότητα της προσβασιμότητας

Υπάρχουν περισσότερα από 750 εκατομμύρια άτομα με αναπηρίες σε όλο τον κόσμο. Όπως προαναφέρθηκε, σε μια εποχή όπου ο αριθμός των ατόμων με αναπηρίες αυξάνεται καθώς ο πληθυσμός μεγαλώνει, η κοινωνία μας έχει μετατραπεί σε τέτοια που εξαρτάται όλο και περισσότερο από τους υπολογιστές και την ψηφιακή τεχνολογία για την εργασία, την εκπαίδευση και την ψυχαγωγία. Η συμμετοχή στην ψηφιακή οικονομία εξ' ορισμού απαιτεί την ικανότητα της πρόσβασης και την χρήση του διαδικτύου. Είναι επομένως σημαντικό να καταβάλλουμε κάθε δυνατή προσπάθεια ώστε να μετατρέψουμε σε προσβάσιμες όσο το δυνατό περισσότερες ιστοσελίδες. Ως διευθυντής της Κοινοπραξίας του Παγκόσμιου Ιστού (*World Wide Web Consortium*) και εφευρέτης του Παγκοσμίου Ιστού, ο Tim Berners-Lee δήλωσε, «η δύναμη του Διαδικτύου έγκειται στην καθολικότητά του. Η πρόσβαση σε όλους, ανεξάρτητα από αναπηρία είναι μια σημαντική πτυχή.» Εκτός από την κοινή ανθρώπινη αξιοπρέπεια, ο πιο προφανής λόγος να γίνουν οι κυβερνητικές ιστοσελίδες προσβάσιμες για τα άτομα με αναπηρία είναι να συμμορφωθούν με το νόμο. Το νομοσχέδιο Americans with Disabilities Act (ADA) , άρθρο 508, και παρόμοιοι νόμοι και κανονισμοί σε άλλες χώρες [11] συχνά εξουσιοδοτούν τη δημιουργία μέσων ώστε να επιτραπεί η πρόσβαση των ατόμων με αναπηρίες στις ίδιες πληροφορίες και χρησιμοποιούν τα ίδια εργαλεία όπως οποιοσδήποτε άλλος στο Διαδίκτυο. Για παράδειγμα, το ADA απαιτεί «λογικές διαρρυθμίσεις» και "αποτελεσματική επικοινωνία" στους τομείς της απασχόλησης, δημόσιες υπηρεσίες και υπηρεσίες τηλεπικοινωνιών. Με τη δημοτικότητα της ηλεκτρονικής διακυβέρνησης και του ηλεκτρονικού εμπορίου, οι εστιάσεις του νόμου έχουν αλλάξει ώστε να συμπεριλάβουν το Διαδίκτυο [12]. Το τμήμα 508 του Νόμου Αποκατάστασης (Rehabilitation Act) ορίζει τις διεργασίες που χρησιμοποιούνται από την ομοσπονδιακή κυβέρνηση κατά την προμήθεια ηλεκτρονικών και πληροφορικής. Μία από τις πιο σημαντικές εστιάσεις του νόμου είναι να διασφαλιστεί ότι η πρόσβαση στις τεχνολογίες ηλεκτρονικών και πληροφοριών που διατίθενται, είναι διαθέσιμες σε άτομα αναπηρίες οι οποίοι είτε είναι κυβερνητικοί υπάλληλοι ή μέλη του ευρύ κοινού. Στον Καναδά, η Διεύθυνση Ισότητας και Διαφορετικότητα της Επιτροπής Δημόσιας Υπηρεσίας ήταν ο πρώτος εθνικός φορέας που δημοσίευσε κατευθυντήριες γραμμές όσον αφορά την προσβασιμότητα στον Διαδίκτυο, ώστε να διασφαλιστεί ότι όλες οι κυβερνητικές ιστοσελίδες και τα σχετιζόμενα με αυτές ηλεκτρονικά δεδομένα ήταν προσιτά σε κάθε χρήστη του Διαδικτύου.

Αν και οι περισσότερες χώρες του κόσμου δεν έχουν ακόμη αναπτύξει ειδικούς νόμους ή κανονισμούς που αφορούν την προσβασιμότητα του Διαδικτύου, πολλά έχουν θεσπίσει νομοθεσίες και κυβερνητικούς κανονισμούς παρόμοιους με τον ADA των ΗΠΑ. Μέχρι πρόσφατα αυτοί οι νόμοι και οι κανονισμοί αφορούσαν κυρίως τα θέματα της απασχόλησης, της μεταφοράς και των δημόσιων εγκαταστάσεων. Ωστόσο, είναι μόνο θέμα χρόνου πριν οι περισσότερες κυβερνητικές ιστοσελίδες σε όλο τον κόσμο έρθουν αντιμέτωπες με πολιτικές και νομικές προκλήσεις λόγω της μη προσβασιμότητας τους από άτομα με ειδικές ανάγκες. Φαίνεται πιθανό ότι σύντομα οι υπηρεσίες που

βασίζονται στο Διαδίκτυο θα πραγματοποιηθούν βάσει των ίδιων προδιαγραφών με τις υπηρεσίες ή τις αρχιτεκτονικές εγκατάστασης του φυσικού κόσμου, στα δικαστήρια.

Επιπλέον, η μετατροπή μιας ιστοσελίδας σε προσβάσιμη, θα μπορούσε να θεωρηθεί ένα οικονομικά ανταγωνιστικό πλεονέκτημα. Πολλές εταιρείες βρήκαν ότι η δημιουργία της προσβασιμότητας στις ιστοσελίδες τους είναι οικονομικά αποδοτική και γενικά καλή επιχειρηματική πρακτική [13]. Σύμφωνα με έκθεση που δημοσιεύθηκε από την Forrester Research, παγκόσμια 3.500 επιχειρήσεις εκτιμάται ότι θα δαπανήσουν 560 εκατομμύρια δολάρια για να αναβαθμίσουν τις ιστοσελίδες τους και να ανταποκριθούν στις κατευθυντήριες γραμμές της W3C πρωτοβουλίας για την Προσβασιμότητα στο Διαδίκτυο (*W3C Web Accessibility Initiative guidelines*). Εταιρείες ηλεκτρονικού εμπορίου, όπως η Amazon.com, κάνουν προσιτές τις ιστοσελίδες τους έτσι ώστε να αποκτήσουν ένα μερίδιο από τα $ 175 δισ. Από το διακριτικό εισόδημα που ελέγχεται από τους καταναλωτές με ειδικές ανάγκες *(Amazon.com 's δελτίο τύπου 6 Δεκ 2001, Prager, 1999)*. Εξήντα οκτώ τοις εκατό των καταναλωτών, μεταξύ 45 και 54 ετών είναι online και σχεδόν το ένα τέταρτο έχουν κάποια αναπηρία (*Απογραφή των ΗΠΑ*). Οι συγγραφείς συμπεραίνουν: «Οι εταιρείες πρέπει να σχεδιάζουν τον σχεδιασμό των ιστοσελίδων τους έχοντας τα άτομα με αναπηρίες στο μυαλό τους. Κάτι τέτοιο είναι οικονομικά αποδοτικό, ιδιαίτερα αν η προσβασιμότητα αποτελεί μέρος του σχεδιασμού, της ανάπτυξης και της διαδικασίας συντήρησης.»

Πράγματι, χρήστες του διαδικτύου με ειδικές ανάγκες συχνά γίνονται πολύ πιστοί πελάτες από τη στιγμή που βρίσκουν μια τοποθεσία Web που φιλοξενεί ειδικές ανάγκες τους [14] [15]. Μια προσβάσιμη ιστοσελίδα επιτρέπει επίσης την χαμηλή τεχνολογία να έχει πρόσβαση σε υψηλή τεχνολογία. Πιο συγκεκριμένα, τα χαρακτηριστικά μιας προσβάσιμης ιστοσελίδας επιτρέπουν στοιχεία βίντεο και ήχου στο Διαδίκτυο να αρχειοθετηθούν με δυνατότητες αναζήτησης κειμένου, και το κείμενο να μετατραπεί σε ομιλία για τους αναγνώστες οθόνης, και ως εκ τούτου, τους ηλικιωμένους, τους ανθρώπους σε υπανάπτυκτες χώρες, ακόμη και εκείνοι που είναι αναλφάβητοι επίσης ενδέχεται να επωφεληθούν από την σχεδίαση προσβάσιμων ιστοσελίδων, δεδομένου ότι το διαδικτυακό κείμενο μπορεί να παρουσιάζεται ταυτόχρονα ακουστικά μέσω ενός μετατροπέα φωνής. Από την άλλη πλευρά, οργανισμοί που δεν κάνουν προσιτές τις ιστοσελίδες τους σε ανθρώπους με αναπηρίες δεν λείπουν μόνο από τις εμπορικές ευκαιρίες, αλλά αντιμετωπίζουν επίσης τις περαιτέρω οικονομικές παγίδες από οργανώσεις υπέρ των δικαιωμάτων των πολιτών που επιδιώκουν προσφυγή.[16]

Μετά την επίτευξη της προσβασιμότητας στις μεγάλες εμπορικές ιστοσελίδες του ιδιωτικό τομέα, οι άνθρωποι με αναπηρίες θα αναμένουν την ίδια σχέση με τις ηλεκτρονικές κυβερνητικές υπηρεσίες. Για τις υπηρεσίες σε όλα τα επίπεδα διακυβέρνησης, το Διαδίκτυο παρέχει ένα ιδανικό μέσο στους πολίτες οι οποίοι συνήθιζαν να είναι αποξενωμένοι από πολλές δημόσιες υπηρεσίες. Ωστόσο, οι σημερινοί σχεδιαστές των κυβερνητικών ιστοσελίδων και το προσωπικό παραγωγής τους δεν έχουν πλήρη επίγνωση της καθοριστικής σημασίας του θέματος αυτού και ως εκ τούτου, εγείρονται διάφορα εμπόδια μεταξύ των online υπηρεσιών τους και των πολιτών με ειδικές ανάγκες. [17] [18]

2.4. Παράγοντες που επηρεάζουν την πρόσβαση

Σύμφωνα με την μελέτη του Gashaw Kebede (*Addis Ababa University, Ethiopia)* σε περισσότερες από 70 ερευνητικές εκθέσεις και άρθρα σχετικά με τους παράγοντες που επηρεάζουν την πρόσβαση και τη χρήση των IR (Information Retrieval, ανάκτηση πληροφορίας) συστημάτων, τις ψηφιακές βιβλιοθήκες, τα ηλεκτρονικά περιοδικά, και το Διαδίκτυο έχουν δείξει με συνέπεια την ύπαρξη και επικράτηση μιας σειράς παραγόντων που επηρεάζουν την πρόσβαση στην ηλεκτρονική πληροφορία. Αυτοί οι παράγοντες μπορεί να διαχωριστούν στις ακόλουθες τέσσερις κατηγορίες:

- τα χαρακτηριστικά του τελικού χρήστη,
- τα χαρακτηριστικά των ηλεκτρονικών μέσων πληροφόρησης,
- τα χαρακτηριστικά του ηλεκτρονικού περιεχομένου,
- και τα χαρακτηριστικά του περιβάλλοντος των πληροφοριών στο οποίο λαμβάνει χώρα η πρόσβαση.

Πιο αναλυτικά:

1. Τα χαρακτηριστικά του τελικού χρήστη αναφέρονται στις ιδιότητες και τις δυνατότητες που οι τελικοί χρήστες φέρνουν στην διαδικασία της πρόσβασης στην πληροφορία, συμπεριλαμβανομένων των δεξιοτήτων κάποιου στους υπολογιστές, την εμπειρία στη χρήση των πόρων των ηλεκτρονικών πληροφοριών και τις πληροφορίες, το πεδίο γνώσης, τις γλωσσικές ικανότητες, τον ψηφιακό αλφαβητισμό (συμπεριλαμβανομένης της στάσης ως προς την πληροφορία, την αναζήτηση πληροφοριών, και τη χρήση της πληροφορίας), τις πεποιθήσεις σχετικά με την ικανότητα, την ευκολία χρήσης, και τη χρησιμότητα των πληροφοριών, των πληροφοριακών συστημάτων, και του Διαδικτύου, την αντίληψη για τις δεξιότητες και τις γνώσεις του και την οικονομική του δυνατότητα για την απόκτηση ηλεκτρονικών πόρων και κατάρτισης. Ειδικές περιπτώσεις των χαρακτηριστικών του τελικού χρήστη οι οποίες εμποδίζουν την πρόσβαση στην ηλεκτρονική πληροφορία περιλαμβάνουν τα εξής:
    - έλλειψη εμπειρίας στη χρήση πληροφοριακών συστημάτων,
    - δίκτυα,
    - το Διαδίκτυο και η ηλεκτρονική πληροφορία
    - η μη συνειδητοποίηση των διαθέσιμων πόρων, των του δικαιωμάτων χρήστη και των καθηκόντων του όσον αφορά την αξιοποίηση των ηλεκτρονικών πηγών πληροφόρησης
    - η έλλειψη εμπιστοσύνης στις ικανότητές του
    - η έλλειψη γνώσης της γλώσσας στην οποία τα ψηφιακά έγγραφα είναι διαθέσιμα

- και η έλλειψη ενδιαφέροντος και κινήτρων για τη χρήση των ηλεκτρονικών συστημάτων πληροφόρησης και της πληροφορίας

2. Τα χαρακτηριστικά των Ηλεκτρονικών μέσων πληροφόρησης αφορούν τα χαρακτηριστικά της τεχνολογίας της ηλεκτρονικής πληροφορίας και των πηγών της ηλεκτρονικής πληροφορίας, συμπεριλαμβανομένων των δυνατοτήτων του υπολογιστικού και δικτυακού υλικού, του λογισμικού, των διεπαφών, της σύνδεσης στο Διαδίκτυο, την ευκολία χρήσης αυτών των πόρων, και της φυσικής πρόσβασης (ως πρόσβαση θεωρείται η διαθεσιμότητα) της πληροφορικής, των πόρων του δικτύου και των πηγών ηλεκτρονικής πληροφόρησης. Ειδικές περιπτώσεις των χαρακτηριστικών των ηλεκτρονικών μέσων πληροφόρησης στις οποίες παρεμποδίζεται η πρόσβαση στις ηλεκτρονικές πληροφορίες περιλαμβάνουν τα ακόλουθα:

   - φυσική μη διαθεσιμότητα κατάλληλων υπολογιστικών πόρων, δικτυακού υλικού, και πηγών ηλεκτρονικής πληροφόρησης
   - ανεπαρκή ικανότητα των υπολογιστών, του δικτυακού υλικού και λογισμικού
   - φυσική μη διαθεσιμότητα του δικτύου και της σύνδεσης στο Διαδίκτυο
   - χαμηλή ικανότητα του δικτύου και της σύνδεσης στο Διαδίκτυο
   - φυσική ανικανότητα πρόσβασης στις ηλεκτρονικές πηγές πληροφόρησης
   - και δύσκολες ως προς τη χρήση διεπαφές.

3. Τα χαρακτηριστικά του Περιεχομένου: Αυτό αναφέρεται στα χαρακτηριστικά του περιεχομένου, όπως η συνάφεια (σχετικά με το θέμα), του τύπου (κείμενο, γραφικά, ήχο, βίντεο), της μορφής (PDF, Word, PostScript, HTML), της γλώσσας (διεθνής γλώσσες όπως Αγγλικά, τοπική γλώσσα), της μορφής (πλήρες κείμενο, αφηρημένη, αφηρημένη και λέξεις-κλειδιά, περιλήψεις),την ποιότητα του περιεχομένου (ακρίβεια, εύρος, το βάθος, την αξιοπιστία), το επίπεδο της επεξεργασίας του θέματος, την οργάνωση (με δυνατότητα αναζήτησης, τιμαριθμική αναπροσαρμογή) και το μέγεθος του αρχείου που με τη μία ή την άλλη μορφή επηρεάσουν την πρόσβαση στο περιεχόμενο. Ειδικές περιπτώσεις των χαρακτηριστικών του περιεχομένου που εμποδίζουν την πρόσβαση στις ηλεκτρονικές πληροφορίες περιλαμβάνουν τα ακόλουθα:

   - φυσική μη διαθεσιμότητα του σχετικού περιεχομένου (τοπικά) για τις βασικές και τις άμεσες ανάγκες των τελικών χρηστών,
   - φυσική αδυναμία της πρόσβασης του σχετικού περιεχομένου για τις βασικές και άμεσες ανάγκες των τελικών χρηστών,
   - φτωχή παρουσίαση (παράδοση) του περιεχομένου
   - και η κακή ποιότητα του περιεχομένου (όσον αφορά την ακρίβεια, την αξιοπιστία, το εύρος και το βάθος)

4. Χαρακτηριστικά του συνολικού περιβάλλοντος των πληροφοριών: Αυτό αναφέρεται σε χαρακτηριστικά που σχετίζονται με τις πληροφορίες του φυσικού περιβάλλοντος στο οποίο η πρόσβαση στην ηλεκτρονική πληροφορία λαμβάνει χώρα, συμπεριλαμβανομένων των πληροφοριών πολιτικής και κανονισμών, των γενικών υποδομών της χώρας / οργανισμού, τις πληροφορίες του πολιτισμού της χώρας / οργανισμού, τεχνική και άλλη υποστήριξη του συστήματος, το συνολικό οικονομικό επίπεδο της χώρας, και το κόστος των ηλεκτρονικών πηγών πληροφόρησης. Ειδικές περιπτώσεις των χαρακτηριστικών του περιβάλλοντος των πληροφοριών που εμποδίζουν την πρόσβαση στις ηλεκτρονικές πληροφορίες περιλαμβάνουν τα εξής:

    - η απουσία των υποστηρικτικών πολιτικών και κανονισμών της πληροφορίας
    - η απουσία προσωπικού / τεχνικής υποστήριξης,
    - το υψηλό κόστος των ηλεκτρονικών τεχνολογιών,
    - πηγές πληροφοριών,
    - το περιεχόμενο
    - η κακή γενική υποδομή της χώρας.
    - υπανάπτυκτη χώρα / οργανισμός όσον αφορά τη διακίνηση της πληροφορίας,
    - και η απαγόρευση των πολιτιστικών και κοινωνικών προτύπων για την πρόσβαση στο περιεχόμενο και την εύρεση όλων των χρήσιμων πληροφοριών.

Από τα παραπάνω μπορεί να παρατηρηθεί ότι οι παράγοντες που επηρεάζουν την πρόσβαση στις ηλεκτρονικές πληροφορίες είναι περιορισμοί της πρόσβασης στις ηλεκτρονικές τεχνολογίες, στις πηγές των πληροφοριών και το περιεχόμενο, οι οποίοι προκαλούνται από τα χαρακτηριστικά του χρήστη, τα χαρακτηριστικά των ηλεκτρονικών μέσων πληροφόρησης, των χαρακτηριστικών του ηλεκτρονικού περιεχομένου, και των χαρακτηριστικών του περιβάλλοντος.

Επιπλέον, η πρόσβαση στην ηλεκτρονική πληροφορία παρεμποδίζεται όταν υπάρχει αναντιστοιχία μεταξύ των παραγόντων που συζητήθηκαν προηγουμένως. Πιο συγκεκριμένα οι ακόλουθες αναντιστοιχίες οδηγούν την πρόσβαση σε πληροφορίες ηλεκτρονικής μορφής σε αποτυχία:

- Ασυμφωνία μεταξύ των χαρακτηριστικών του τελικού χρήστη και τα χαρακτηριστικά των μεταφορέων των ηλεκτρονικών πληροφοριών. Για παράδειγμα, στο επίπεδο των υπολογιστικών δεξιοτήτων του τελικού χρήστη δεν ταιριάζουν με τις απαιτήσεις ικανοτήτων ή την ευκολία της χρήσης του συστήματος ηλεκτρονικής πληροφορίας, τότε η πρόσβαση σε πληροφορίες επηρεάζεται αρνητικά.

- Ασυμφωνία μεταξύ των χαρακτηριστικών του τελικού χρήστη και του περιεχομένου. Για παράδειγμα, αν ο τελικός χρήστης δεν γνωρίζει τη γλώσσα στην οποία είναι γραμμένο το περιεχόμενο, τότε η πρόσβαση σε πληροφορίες δεν είναι εφικτή.

- Ασυμφωνία μεταξύ των χαρακτηριστικών του τελικού χρήστη και του συνολικού πληροφοριακού περιβάλλοντος. Για παράδειγμα, εάν το κόστος της πρόσβασης στο διαδίκτυο σε μια χώρα είναι πέρα του κόστους το οποίο οι τελικοί χρήστες μπορούν να αντέξουν, τότε η πρόσβαση στις πληροφορίες του Διαδικτύου επηρεάζεται αρνητικά.

- Ασυμφωνία μεταξύ των χαρακτηριστικών των φορέων ηλεκτρονικής πληροφορίας και τα χαρακτηριστικά του περιεχομένου. Για παράδειγμα, εάν η μορφή του περιεχομένου δεν ταιριάζει με τις δυνατότητες του λογισμικού των υπολογιστικών πόρων, τότε το περιεχόμενο δεν είναι προσβάσιμο από τους χρήστες, και έτσι, εμποδίζεται η πρόσβαση στις ηλεκτρονικές πληροφορίες.

- Ασυμφωνία μεταξύ των χαρακτηριστικών του συνολικού περιβάλλοντος των πληροφοριών και των φορέων της ηλεκτρονικής πληροφορίας. Για παράδειγμα, εάν η κλιματολογική κατάσταση μιας χώρας δεν επιτρέπει ένα εισαγόμενο υπολογιστικό σύστημα, τότε το σύστημα δεν μπορεί να λειτουργήσει όπως θα έπρεπε, και έτσι εμποδίζεται η πρόσβαση και η χρήση του συστήματος.

- Ασυμφωνία μεταξύ των χαρακτηριστικών του συνολικού περιβάλλοντος των πληροφοριών και του περιεχομένου. Για παράδειγμα, εάν οι τελικοί χρήστες δεν μπορούν να δουν ορισμένους τύπους περιεχομένου λόγω της οργανωτικής πολιτικής, τότε η πρόσβαση σε τέτοιου είδους πληροφορίες δεν μπορεί να πραγματοποιηθεί ακόμα και αν απαιτείται από τους τελικούς χρήστες.

Η ύπαρξη αυτών των παραγόντων σε ένα δεδομένο φυσικό περιβάλλον (δηλαδή, ένα νοικοκυριό, μια κοινότητα, μια οργάνωση, ή μια χώρα) επηρεάζει την πρόσβαση στις ηλεκτρονικές πληροφορίες με έναν ή περισσότερους από τους ακόλουθους και άλλους παρόμοιους τρόπους:

- Κάνοντας το περιεχόμενο των πληροφοριών φυσικά μη διαθέσιμο,

- Κάνοντας το περιεχόμενο των πληροφοριών φυσικά μη προσβάσιμο,

- Κάνοντας τους τελικούς χρηστές να αντιλαμβάνονται ότι το περιεχόμενο της πληροφορίας είναι φυσικά μη διαθέσιμη,

- Κάνοντας τους τελικούς χρηστές να αντιλαμβάνονται ότι το περιεχόμενο της πληροφορίας είναι φυσικά μη προσβάσιμο,

- Με το να μην είναι βολική η πρόσβαση στο περιεχόμενο των πληροφοριών στους τελικούς χρήστες,

- Με το να μη παρέχονται κίνητρα στους τελικούς χρήστες για να επιχειρήσουν την πρόσβαση στις ηλεκτρονικές πηγές πληροφόρησης και του περιεχομένου,
- Με το να μην εκτιμούν οι τελικοί χρήστες πόσο σημαντική και χρήσιμη είναι η πρόσβαση στο περιεχόμενο των πληροφοριών,
- Με το να είναι η χρήση των διαθέσιμων ηλεκτρονικών πληροφοριών δύσκολη και αποθαρρυντική,
- Με το να επιβάλλεται στους τελικούς χρήστες να έχουν υποανάπτυκτο πολιτισμό όσον αφορά την πληροφόρηση,
- Με το να στερούνται οι τελικοί χρήστες την εμπειρία και τις δεξιότητες της πληροφορικής,
- Με τη διατήρηση των τελικών χρηστών σε πλήρη άγνοια του τι είναι διαθέσιμο και πιθανό,
- Με το να χάνουν τους τελικούς χρήστες την εμπιστοσύνη τους στην ικανότητά τους όσον αφορά την πρόσβαση στο περιεχόμενό της πληροφορίας. [19]

2.5. Εξασφάλιση προσβασιμότητας μέσω καθολικού σχεδιασμού

Ο προσβάσιμος σχεδιασμός της ηλεκτρονικής διακυβέρνησης εξασφαλίζει ότι οι προσφερόμενες υπηρεσίες μπορούν να χρησιμοποιηθούν και από άτομα με ειδικές ανάγκες (προσβασιμότητα). Επιπλέον, η πείρα δείχνει ότι η σαφήνεια και η κατανόηση των υπηρεσιών επωφελούνται από τον προσεκτικό και σκόπιμο σχεδιασμό καθώς και από τη δόμηση τους, διατηρώντας παράλληλα κατά νου τις απαιτήσεις προσβασιμότητας. Ως εκ τούτου, η προσβασιμότητα είναι χρήσιμη για όλους τους πολίτες που επιθυμούν να παρακολουθήσουν τα διοικητικά θέματα μέσω του Διαδικτύου (καθολικός σχεδιασμός).

Πολίτες με ειδικές ανάγκες καθώς και εργαζόμενοι με ειδικές ανάγκες επωφελούνται από την προσβάσιμη ηλεκτρονική διακυβέρνηση. Κατά την εκτέλεση των εφαρμογών της ηλεκτρονικής διακυβέρνησης, υπάρχουν τρεις σημαντικοί τομείς των απαιτήσεων όπου οι αρχές της προσβασιμότητας θα πρέπει να εξεταστούν.

Ø **Πρόσβαση**: Πρέπει να διασφαλίζεται ότι όλοι οι πολίτες γενικά είναι σε θέση να χρησιμοποιούν την εφαρμογή, στο σπίτι, στο χώρο εργασίας ή σε ένα χώρο δημόσιας πρόσβασης. Πρέπει να είναι εξασφαλισμένο, για παράδειγμα, ότι ένα άτομο με δυσλειτουργία στο περπάτημα μπορεί να εισέλθει σε μια δημόσια τοποθεσία πρόσβασης. Για μια ιστοσελίδα, είναι σημαντικό να γίνουν οι σελίδες προσβάσιμες για τα άτομα με αναπηρίες και συμβατές με τις βοηθητικές τεχνολογίες. Εκτός από αυτά τα κριτήρια, τα οποία αφορούν το υλικό, το λογισμικό\ και κατασκευαστικά ζητήματα, ένα σημαντικό ερώτημα είναι αν οι πολίτες είναι αρκετά ικανοί ώστε να χρησιμοποιήσουν τα μέσα: Ξέρουν τι προσφέρει η εφαρμογή; Μπορούν να κρίνουν αν

η εφαρμογή είναι αξιόπιστη όσον αφορά την προστασία της ιδιωτικής ζωής και την ασφάλεια; Αυτό σημαίνει ότι τα μέσα εκπαίδευσης θα πρέπει επίσης να είναι σχεδιασμένα έτσι ώστε να εξυπηρετούν τα άτομα με αναπηρίες.

Ø **Κάθετη ολοκλήρωση**: Η περιοχή των απαιτήσεων ασχολείται με την επεξεργασία στη διοίκηση. Η ηλεκτρονική διακυβέρνηση καθιστά δυνατή την επανεξέταση και την αλλαγή των παραδοσιακών διαδικασιών. Πιθανότατα, τα άτομα με αναπηρίες θα μπορούσαν να αναλάβουν νέα καθήκοντα στο χώρο εργασίας τους, το οποίο μπορεί να σημαίνει μεγαλύτερη ανεξαρτησία από εργασιακή βοήθεια ή βοήθεια από τους συναδέλφους.

Ø **Οριζόντια ολοκλήρωση**: Μέχρι τώρα, κανονικά θα πρέπει να επισκεφθείς διάφορες διοικητικές υπηρεσίες και να συμπληρώσεις σε διάφορες αιτήσεις, αν αλλάξει κάτι στη ζωής σου, για παράδειγμα, αν μετακομίσεις ή αν γεννηθεί ένα παιδί. Η ηλεκτρονική διακυβέρνηση είναι μια πραγματική προστιθέμενη αξία για τους πολίτες αν οι υπηρεσίες προσφέρονται σε πακέτο. Από την οπτική γωνία του πολίτη και ιδιαίτερα των πολιτών με ειδικές ανάγκες, η επιτυχής οριζόντια ολοκλήρωση των υπηρεσιών είναι σαφώς μια διευκόλυνση και μειώνει τον κόπο που απαιτείται τώρα. [20]

2.5.1. Ομάδες χρηστών που επωφελούνται

Οι χρήστες με διαφορετικές ικανότητες και δεξιότητες, επωφελούνται από τον προσβάσιμο σχεδιασμό που προσφέρει το Διαδίκτυο. Αντίστοιχα, αποκλείονται από τη χρήση, εάν οι απαιτήσεις τους αγνοηθούν.

Ø Άτομα με προβλήματα όρασης

Οι τυφλοί εξαρτώνται από τους αναγνώστες οθόνης που τους διαβάζουν το περιεχόμενο, και μια Braille οθόνη μπορεί να τους προσφέρει πρόσθετη βοήθεια. Καθώς οι πληροφορίες για την περιήγηση και τον προσανατολισμό μπορεί κυρίως να γίνουν κατανοητές ακουστικά, αυτό σημαίνει ότι μία ιστοσελίδα πρέπει να δομηθεί πολύ ξεκάθαρα. Ως εκ τούτου, όλα τα γραφικά στοιχεία πρέπει να συνοδεύεται από περιγραφικά κείμενα, θα πρέπει να είναι δυνατή η χρήση κάθε ιστοσελίδας μέσω πληκτρολογίου. Τα προβλήματα όρασης μπορεί να διαφέρουν σημαντικά. Κυμαίνονται από θολή όραση, όραση τούνελ γνωστή και ως «Kalnienk vision», η οποία αφορά την απώλεια της περιφερειακής όρασης με αποτέλεσμα μια κυκλική σήραγγα ως οπτικό πεδίο, και ευαισθησία σχετικά με τις συνθήκες φωτισμού μέχρι και αχρωματοψία. Η μετάβαση στην ομάδα των τυφλών είναι ρευστή. Συχνά λογισμικό μεγέθυνσης και λογισμικό παραγωγής φωνής συνδυάζονται. Με τα προϊόντα λογισμικού, είναι σημαντικό ότι υπάρχει η δυνατότητα μεγέθυνσης της γραμματοσειράς και ότι τα χρώματα μπορούν να προσαρμοστούν ατομικά σε κάθε περίπτωση. Σε περίπτωση ισχυρής μεγέθυνσης, μεγάλες οθόνες υποστηρίζουν τον προσανατολισμό.

Ø Άτομα με κινητικά προβλήματα

Οι άνθρωποι με κινητικά προβλήματα, για παράδειγμα άτομα με σπαστικότητα, δύσκολα μπορούν να χρησιμοποιήσουν το ποντίκι ή το τυπικό πληκτρολόγιο. Άτομα που δεν είναι σε θέση να χρησιμοποιούν πλήρως τα χέρια τους βασίζονται σε εναλλακτικές λύσεις, για παράδειγμα ειδικά πληκτρολόγια, ποντίκια κεφαλής, κουμπιά. Ξεκάθαρος σχεδιασμός και λογική γραμμικοποίηση εισόδου είναι απαραίτητες και για αυτήν την ομάδα.

- **Άτομα με προβλήματα ακοής**

Οι άνθρωποι με προβλήματα ακοής συναντούν εμπόδια όταν οι υπηρεσίες ήχου και βίντεο παρέχονται χωρίς υποστήριξη κειμένου. Μια μεγάλη δυσκολία είναι μια υπερβολικά πολύπλοκη γλώσσα, ειδικά όταν η "μητρική γλώσσα" είναι η νοηματική γλώσσα και η προφορική (αντίστοιχα, γραπτή) γλώσσα πρέπει να θεωρηθεί ως ξένη γλώσσα. Ως εκ τούτου, είναι σημαντικό να παρουσιάζονται οι σχετικές πληροφορίες με ταινίες στη νοηματική γλώσσα ή σε εύκολη γλώσσα.

- **Άτομα με γνωστικές διαταραχές**

Οι άνθρωποι με γνωστικές διαταραχές χρειάζεστε μια ευκολομνημόνευτη δομή σελίδας, μια διαχειρίσιμη πλοήγηση και εύκολη γλώσσα (π.χ., απλά αγγλικά). Τα γραφικά και τα κινούμενα αντικειμένων υποστηρίζουν την προσοχή.

- **Άτομα με ελλιπή εμπειρία**

Οι άνθρωποι που χρειάζονται περισσότερο προσανατολισμό, για παράδειγμα, οι ηλικιωμένοι ή άτομα χωρίς εμπειρία στο Διαδίκτυο, χρειάζονται επίσης μια σαφή δομή σελίδας και διαχειρίσιμη πλοήγηση.

Κατ 'αρχήν, οι άνθρωποι που πάσχουν προσωρινά από κάποιες αδυναμίες (αναπηρίες) αντιμετωπίζουν τα ίδια εμπόδια με μια συγκεκριμένη κατάσταση, όπως τον χειρισμό ενός μηχανήματος, τον ισχυρό φωτισμό ή τον θόρυβο. Με εναλλακτικές μονάδες παραγωγής, όπως PDA (“Personal Digital Assistant”, προσωπικός ψηφιακός βοηθός) ή τα κινητά τηλέφωνα, ο προσανατολισμός και οι απαιτήσεις πλοήγησης πρέπει να εξεταστούν. Γνωρίζοντας και κατανοώντας τις ανάγκες των χρηστών διευκολύνεται η χρήση των υφιστάμενων προτύπων και κατευθυντηρίων γραμμών. [21]

2.6. Οδηγίες για τη δημιουργία προσβάσιμων Ιστοσελίδων

Στα πλαίσια της πολιτική της Ευρωπαϊκής Ένωσης για την προσβασιμότητα του Διαδικτύου όλοι οι επίσημοι δικτυακοί τόποι των οργάνων της Ευρωπαϊκής Ένωσης – γνωστοί συνολικά ως EUROPA – πρέπει να τηρούν τις διεθνείς κατευθυντήριες γραμμές για την προσβασιμότητα του Διαδικτύου, έτσι ώστε όσο το δυνατόν περισσότεροι επισκέπτες να μπορούν να αξιολογούν και να κατανοούν το περιεχόμενό τους. Στόχος είναι να εφαρμοστούν οι κατευθυντήριες γραμμές για την προσβασιμότητα του περιεχομένου του Διαδικτύου WCAG 1.0 που εξέδωσε η World Wide Web

Consortium (W3C, Κοινοπραξία Παγκόσμιου Ιστού) [22] στο πλαίσιο της Πρωτοβουλίας για την προσβασιμότητα του Διαδικτύου (WAI, Web Accessibility Initiative). Όλοι οι νέοι δικτυακοί τόποι της πύλης EUROPA πρέπει να ανταποκρίνονται στο επίπεδο συμμόρφωσης A (προτεραιότητα 1), δηλαδή να πληρούν τα βασικά κριτήρια που θέτουν οι προαναφερθείσες κατευθυντήριες γραμμές του WCAG. Ορισμένες από τις εισαγωγικές σελίδες "προτεραιότητας" της πύλης EUROPA φέρουν ήδη το λογότυπο "W3C – WAI A" που δείχνει ότι πληρούν τα κριτήρια του επιπέδου συμμόρφωσης A. Καταβάλλονται προσπάθειες για να αναβαθμιστούν όσο το δυνατό περισσότερες σελίδες χαμηλού επιπέδου, ώστε να πληρούν τα ίδια κριτήρια προσβασιμότητας (αν και αυτές δεν χρειάζονται λογότυπο).[23] Οι κατευθυντήριες γραμμές για την προσβασιμότητα του περιεχομένου 1.0 (WCAG 1.0), υιοθετήθηκαν το 1999, με 66 σημεία ελέγχου, [24] Έχει να κάνει κυρίως με το σχεδιασμό της Hypertext Markup Language (HTML), στην οποία βασίζονται όσα προσφέρει το Διαδίκτυο (π.χ. ο χειρισμός των πινάκων, ο αυστηρός διαχωρισμός μεταξύ παρουσίασης και μορφής, το χειρισμό των γραφικών και των ηχητικών στοιχείων). Περαιτέρω οι κατευθυντήριες γραμμές WAI ασχολούνται με συγγραφικά εργαλεία, user agents[1] και Extensible Markup Language (XML). Πρόσθετες οδηγίες, από αυτοϋπερασπιζόμενες ομάδες και άτομα συνήθως βασίζονται στο WCAG 1.0. Για παράδειγμα, τον Φεβρουάριο του 2008, η WCAG Samurai, μία ομάδα προγραμματιστών ανεξάρτητοι από την W3C, και καθοδηγούμενοι από τον Joe Clark δημοσιοποίησαν διορθώσεις αλλά και πρόσθετα για τις WCAG 1.0. [25]

[1] Στην πληροφορική, ένας user agent είναι το λογισμικό που ενεργεί για λογαριασμό του χρήστη. Για παράδειγμα, ένας αναγνώστης e-mail είναι ένας Mail User Agent, και για την Session Initiation Protocol (SIP), ο όρος user agent αναφέρεται σε δύο τελικά σημεία μιας συνόδου επικοινωνίας.

2.6.1. Οδηγίες για την Προσβασιμότητα του Περιεχομένου του Ιστού WCAG v 1.0

Οδηγία 1. Παρέχετε ισοδύναμα κείμενα για το ακουστικό και το οπτικό περιεχόμενο.

Παρέχετε περιεχόμενο το οποίο όταν παρουσιάζεται στον χρήστη να μεταφέρει ουσιωδώς την ίδια λειτουργία ή τον ίδιο σκοπό όπως το ακουστικό ή το οπτικό περιεχόμενο.

Παρόλο που κάποιοι άνθρωποι δεν μπορούν να χρησιμοποιήσουν εικόνες, ταινίες, ήχους, προγραμματιστικά σενάρια (scripts) κ.λπ. άμεσα, μπορεί παρ' όλα αυτά να χρησιμοποιούν σελίδες που περιλαμβάνουν πληροφορίες ισοδύναμες με το οπτικό ή ακουστικό περιεχόμενο. Οι ισοδύναμες πληροφορίες πρέπει να εξυπηρετούν τον ίδιο σκοπό όπως το οπτικό ή το ακουστικό περιεχόμενο. Έτσι, ένα κείμενο ισοδύναμο μιας εικόνας ενός ανοδικού βέλους που οδηγεί μέσω συνδέσμου σε έναν πίνακα περιεχομένων θα μπορούσε να είναι «πήγαινε στον πίνακα περιεχομένων». Σε ορισμένες περιπτώσεις, ένα ισοδύναμο κείμενο θα μπορούσε επίσης να περιγράφει την εμφάνιση του οπτικού περιεχομένου (π.χ. για περίπλοκους πίνακες, καταλόγους ή διαγράμματα) ή τον ήχο του ακουστικού περιεχομένου (π.χ. για ακουστικά δείγματα που χρησιμοποιούνται στην εκπαίδευση).

Η παρούσα οδηγία τονίζει τη σημασία της παροχής κειμένων ισοδύναμων με το μη-κειμενικό περιεχόμενο (εικόνες, προ-ηχογραφημένο ακουστικό περιεχόμενο, βίντεο). Η δύναμη των ισοδύναμων κειμένων βρίσκεται στην ικανότητά τους να ερμηνεύονται με τρόπους που είναι προσβάσιμοι σε ανθρώπους οι οποίοι ανήκουν σε διάφορες ομάδες ειδικών αναγκών χρησιμοποιώντας μια ποικιλία από τεχνολογίες. Το κείμενο μπορεί άμεσα να σταλεί σε συνθέτες ομιλίας και συσκευές γραφής Braille, και μπορεί να παρουσιαστεί οπτικά σε διάφορα μεγέθη σε οθόνες υπολογιστών και σε χαρτί. Η συνθετική ομιλία είναι καθοριστικής σημασίας για άτομα που είναι τυφλά και για πολλούς ανθρώπους με δυσκολίες ανάγνωσης οι οποίες συχνά συνοδεύουν γνωσιακές ειδικές ανάγκες, μαθησιακές ειδικές ανάγκες και κωφότητα. Η γραφή Braille είναι σημαντική για άτομα που είναι ταυτοχρόνως κωφά και τυφλά, καθώς επίσης και για πολλά άτομα των οποίων η μόνη αισθητηριακή ανικανότητα είναι η τυφλότητα. Ένα κείμενο που παρουσιάζεται οπτικά ωφελεί χρήστες που είναι κωφοί, καθώς επίσης και την πλειοψηφία των χρηστών του Ιστού.

Η παροχή μη-κειμενικών ισοδύναμων με κείμενα (π.χ. εικόνες, βίντεο και προ-ηχογραφημένο ακουστικό περιεχόμενο) είναι επίσης ωφέλιμη για κάποιους χρήστες, ιδιαίτερα μη-αναγνώστες ή ανθρώπους που έχουν δυσκολίες στην ανάγνωση. Σε ταινίες ή οπτικές παρουσιάσεις, η οπτική δράση, όπως η γλώσσα του σώματος ή άλλα οπτικά στοιχεία, μπορεί να μη συνοδεύεται από αρκετές ακουστικές πληροφορίες έτσι ώστε να μεταφέρονται οι ίδιες πληροφορίες. Εκτός και αν παρέχονται

λεκτικές περιγραφές αυτών των οπτικών πληροφοριών, οι άνθρωποι που δεν μπορούν να δουν (ή να κοιτάξουν προς) το οπτικό περιεχόμενο δεν θα είναι σε θέση να το αντιληφθούν.

Σημεία ελέγχου:

1.1 Παρέχετε ένα ισοδύναμο κείμενο για κάθε μη-κειμενικό στοιχείο (π.χ. μέσω της ιδιότητας (attribute) "alt", της ιδιότητας (attribute) "longdesc" ή στο περιεχόμενο του στοιχείου). *Στα μη-κειμενικά στοιχεία περιλαμβάνονται*: εικόνες, γραφικές αναπαραστάσεις κειμένων (συμπεριλαμβανόμενων των συμβόλων), περιοχές χαρτών εικόνων, κινούμενα σχέδια (π.χ. κινούμενα GIF), ενσωματωμένα προγράμματα και προγραμματιστικά αντικείμενα, τέχνη ascii, πλαίσια (frames), προγραμματιστικά σενάρια (scripts), εικόνες που χρησιμοποιούνται ως κουκίδες σε λίστες, κενά διαστήματα, γραφικά κουμπιά, ήχοι (που αναπαράγονται με ή χωρίς συμμετοχή του χρήστη), αυτοδύναμα ακουστικά αρχεία, ηχητικά κανάλια βίντεο και βίντεο. **[Προτεραιότητα 1]**

Για παράδειγμα, στην HTML:

- Χρησιμοποιείστε την ιδιότητα (attribute) "alt" για τα στοιχεία IMG, INPUT και APPLET, ή παρέχετε ισοδύναμο κείμενο στο περιεχόμενο των στοιχείων OBJECT και APPLET.
- Για περίπλοκο περιεχόμενο (π.χ. ένα διάγραμμα) όπου το κείμενο της ιδιότητας (attribute) "alt" δεν παρέχει ένα πλήρως ισοδύναμο κείμενο, παρέχετε μια επιπρόσθετη περιγραφή, χρησιμοποιώντας, για παράδειγμα, την ιδιότητα (attribute) "longdesc" με τα στοιχεία IMG ή FRAME, έναν σύνδεσμο μέσα στο στοιχείο OBJECT ή έναν περιγραφικό σύνδεσμο.
- Για χάρτες εικόνας, χρησιμοποιείστε είτε την ιδιότητα (attribute) "alt" με το στοιχείο AREA, ή το στοιχείο MAP με στοιχεία A (και άλλο κείμενο) ως περιεχόμενο.

Βλ. επίσης το σημείο ελέγχου 9.1 και το σημείο ελέγχου 13.10.

1.2 Παρέχετε πλεονάζοντες συνδέσμους κειμένου για κάθε ενεργή περιοχή ενός χάρτη εικόνας στην πλευρά του εξυπηρετητή.**[Προτεραιότητα 1]**

Βλ. επίσης το σημείο ελέγχου 1.5 και το σημείο ελέγχου 9.1.

1.3 Μέχρι οι πράκτορες χρηστών να μπορούν αυτόματα να διαβάζουν και να εκφωνούν το ισοδύναμο κείμενο ενός οπτικού καναλιού, παρέχετε μια ακουστική περιγραφή των σημαντικών πληροφοριών που υπάρχουν στο ακουστικό κανάλι μιας παρουσίασης πολυμέσων. **[Προτεραιότητα 1]**

Συγχρονίστε την ακουστική περιγραφή με το ακουστικό κανάλι σύμφωνα με το σημείο ελέγχου 1.4. Βλ. το σημείο ελέγχου 1.1 για πληροφορίες σχετικά με κείμενα ισοδύναμα των οπτικών πληροφοριών.

1.4 Για οποιαδήποτε παρουσίαση πολυμέσων με χρονική παράμετρο (π.χ. μια ταινία ή κινούμενα σχέδια), συγχρονίστε τα εναλλακτικά ισοδύναμα (π.χ. υπότιτλους ή ακουστικές περιγραφές του οπτικού καναλιού) με την παρουσίαση. **[Προτεραιότητα 1]**

1.5 Μέχρι οι πράκτορες χρηστών να ερμηνεύουν τα ισοδύναμα κειμένου για τους συνδέσμους που υπάρχουν σε χάρτες εικόνας στην πλευρά του πελάτη, παρέχετε πλεονάζοντες συνδέσμους κειμένου για κάθε ενεργή περιοχή ενός χάρτη εικόνας στην πλευρά του πελάτη. [Προτεραιότητα 3]

Βλ. επίσης το σημείο ελέγχου 1.2 και το σημείο ελέγχου 9.1.

Οδηγία 2. Μην βασίζεστε μόνο στο χρώμα.

Εξασφαλίστε ότι το κείμενο και τα γραφικά είναι κατανοητά όταν παρουσιάζονται χωρίς χρώμα.

Στην περίπτωση που η μεταφορά των πληροφοριών γίνεται μόνο με τη χρήση χρώματος, οι άνθρωποι που δεν μπορούν να ξεχωρίσουν συγκεκριμένα χρώματα και οι χρήστες με συσκευές που δεν αποδίδουν χρώματα ή οπτικές πληροφορίες δεν θα λαμβάνουν αυτές τις πληροφορίες. Όταν τα χρώματα του προσκήνιου και του υπόβαθρου είναι πολύ κοντά στην ίδια απόχρωση, μπορεί να μην παρέχουν επαρκή αντίθεση όταν προβάλλονται σε μονοχρωματικές επιφάνειες απεικόνισης ή όταν τα βλέπουν άνθρωποι με προβλήματα όρασης που σχετίζονται με χρώματα.

Σημεία ελέγχου:

2.1 Εξασφαλίστε ότι όλες οι πληροφορίες που μεταφέρονται μέσω χρωμάτων είναι επίσης διαθέσιμες χωρίς χρώμα, για παράδειγμα, από τα συμφραζόμενα ή τη σήμανση. **[Προτεραιότητα 1]**

2.2 Εξασφαλίστε ότι οι χρωματικοί συνδυασμοί προσκήνιου και υπόβαθρου παρέχουν επαρκή αντίθεση όταν τους βλέπει κάποιο άτομο με πρόβλημα όρασης που σχετίζεται με χρώματα ή όταν προβάλλονται σε ασπρόμαυρη οθόνη. [Προτεραιότητα 2 για εικόνες, Προτεραιότητα 3 για κείμενο].

Οδηγία 3. Χρησιμοποιείστε σήμανση και style sheets (στυλ φύλλων), και μάλιστα με τον ενδεδειγμένο τρόπο.

Για τη σήμανση των εγγράφων χρησιμοποιήστε τα κατάλληλα δομικά στοιχεία. Καλύτερα ελέγξτε τη μορφή με style sheets, παρά με στοιχεία και ιδιότητες μορφής.

Η χρήση της σήμανσης με τρόπο ακατάλληλο, δηλαδή όχι σύμφωνα με τις προδιαγραφές, παρεμποδίζει την προσβασιμότητα. Κακή χρήση ενός εφέ μορφής (π.χ. η χρήση ενός πίνακα για

σελιδοποίηση ή μιας κεφαλίδας για αλλαγή μεγέθους γραμματοσειράς) καθιστά δύσκολη την κατανόηση της οργάνωσης της σελίδας ή την πλοήγηση μέσα σε αυτήν για τους χρήστες με εξειδικευμένο λογισμικό. Επιπλέον, η χρήση σήμανσης μορφής, αντί της χρήσης σήμανσης δομής (π.χ. κατασκευάζοντας κάτι που μοιάζει με πίνακα δεδομένων με τη χρήση του στοιχείου PRE της HTML), καθιστά δύσκολη την απόδοση μιας σελίδας από άλλες συσκευές με τρόπο κατανοητό.

Οι κατασκευαστές περιεχομένου μπορεί να μπουν στον πειρασμό να χρησιμοποιήσουν (ή να χρησιμοποιήσουν λανθασμένα) κατασκευές που επιτυγχάνουν το επιθυμητό αποτέλεσμα μορφής σε παλαιότερους φυλλομετρητές. Πρέπει να γνωρίζουν ότι αυτές οι πρακτικές προκαλούν προβλήματα προσβασιμότητας και πρέπει να αναλογιστούν κατά πόσο το αποτέλεσμα μορφής είναι τόσο κρίσιμο ώστε να δικαιολογεί το γεγονός ότι το έγγραφο γίνεται μη-προσβάσιμο για ορισμένους χρήστες.

Στο άλλο άκρο, οι κατασκευαστές περιεχομένου πρέπει να μην θυσιάζουν την κατάλληλη σήμανση επειδή ένας συγκεκριμένος φυλλομετρητής ή μια υποστηρικτική τεχνολογία δεν την επεξεργάζεται σωστά. Για παράδειγμα, είναι σωστό να χρησιμοποιείτε το στοιχείο TABLE στην HTML για τη σήμανση *ταξινομημένων πληροφοριών* ακόμα και αν ορισμένοι παλαιότεροι αναγνώστες οθόνης μπορεί να μην χειρίζονται γειτονικά κείμενα σωστά (βλ. το σημείο ελέγχου 10.3). Η σωστή χρήση του στοιχείου TABLE και η δημιουργία πινάκων που μετατρέπονται ομαλά (βλ. την οδηγία 5) επιτρέπει στο λογισμικό να αποδώσει πίνακες και σε άλλες μορφές πέραν των δισδιάστατων πλεγμάτων.

Σημεία ελέγχου:

3.1 Όταν υφίσταται μια κατάλληλη γλώσσα σήμανσης, καλύτερα χρησιμοποιείστε σήμανση, παρά εικόνες για τη μεταφορά πληροφοριών. [Προτεραιότητα 2]

> Για παράδειγμα, χρησιμοποιείστε τη γλώσσα MathML για τη σήμανση μαθηματικών εξισώσεων και τα style sheets για τη μορφοποίηση κειμένου και τον έλεγχο της σελιδοποίησης. Επίσης, αποφύγετε τη χρήση εικόνων για την αναπαράσταση κειμένου -- αντί για αυτό χρησιμοποιείστε κείμενο και style sheets. Βλ. επίσης την οδηγία 6 και την οδηγία 11.

3.2 Δημιουργήστε έγγραφα που είναι έγκυρα σύμφωνα με δημοσιευμένες επίσημες γραμματικές. [Προτεραιότητα 2]

> Για παράδειγμα, συμπεριλάβετε στην αρχή ενός εγγράφου μια δήλωση τύπου εγγράφου η οποία αναφέρεται σε ένα δημοσιευμένο DTD(π.χ. το DTD της αυστηρής [strict] HTML 4.0).

3.3 Χρησιμοποιήστε τα φύλλα στυλ για τον έλεγχο της σελιδοποίησης και της μορφής. [Προτεραιότητα 2]

> Για παράδειγμα, χρησιμοποιήστε την ιδιότητα 'font' των CSS αντί για το στοιχείο FONT της HTML για τον έλεγχο του στυλ των τυπογραφικών στοιχείων.

3.4 Χρησιμοποιήστε καλύτερα σχετικές παρά απόλυτες μονάδες στις τιμές ιδιοτήτων (attributes) της γλώσσας σήμανσης και των ιδιοτήτων των style sheets. [Προτεραιότητα 2]

> Για παράδειγμα, στα CSS, καλύτερα χρησιμοποιείστε τη μονάδα μέτρησης 'em' ή ποσοστιαία μήκη, παρά τις μονάδες μέτρησης 'pt' ή 'cm', οι οποίες είναι απόλυτες μονάδες μέτρησης. Εάν χρησιμοποιηθούν απόλυτες μονάδες μέτρησης, ελέγξτε ότι το αποδιδόμενο αποτέλεσμα είναι χρησιμοποιήσιμο.

3.5 Χρησιμοποιήστε στοιχεία κεφαλίδων για να αποδώσετε τη δομή του εγγράφου και χρησιμοποιήστε τα σύμφωνα με τις προδιαγραφές. [Προτεραιότητα 2]

> Για παράδειγμα, στην HTML χρησιμοποιήστε το στοιχείο H2 για να υποδείξετε μια υπό-ενότητα της κεφαλίδας H1. Μην χρησιμοποιείτε κεφαλίδες για εφέ γραμματοσειράς.

3.6 Χρησιμοποιήστε σήμανση για τις λίστες και τα επιμέρους στοιχεία τους με τον κατάλληλο τρόπο. [Προτεραιότητα 2]

> Για παράδειγμα, στην HTML τοποθετήστε τις λίστες OL, UL και DL τη μία μέσα στην άλλη με τον κατάλληλο τρόπο.

3.7 Χρησιμοποιήστε σήμανση για τα παραθέματα. Μην χρησιμοποιείτε σήμανση παραθεμάτων για εφέ μορφοποίησης όπως η εσοχή παραγράφων. [Προτεραιότητα 2]

> Για παράδειγμα, στην HTML χρησιμοποιείστε τα στοιχεία Q και BLOCKQUOTE για τη σήμανση μικρών και μεγαλύτερων παραθεμάτων αντιστοίχως.

Οδηγία 4. Αποσαφηνίστε τη χρήση φυσικής γλώσσας.

Χρησιμοποιήστε σήμανση που διευκολύνει την προφορά ή την ερμηνεία συντετμημένων κειμένων ή κειμένων σε ξένη γλώσσα.

Όταν οι κατασκευαστές περιεχομένου χρησιμοποιούν σήμανση για να δηλώσουν αλλαγές στη φυσική γλώσσα ενός εγγράφου, οι συνθέτες ομιλίας και οι συσκευές γραφής Braille μπορούν αυτόματα να γυρίσουν στη νέα γλώσσα, καθιστώντας το έγγραφο περισσότερο προσβάσιμο σε πολύγλωσσους χρήστες. Οι κατασκευαστές περιεχομένου πρέπει να επισημαίνουν την κύρια *φυσική γλώσσα* του περιεχομένου ενός εγγράφου (μέσω σήμανσης ή κεφαλίδων HTTP). Οι κατασκευαστές περιεχομένου θα πρέπει επίσης να παρέχουν και την πλήρη ανάπτυξη των συντμήσεων και ακρωνυμίων.

Η σήμανση της φυσικής γλώσσας, εκτός του ότι ενισχύει τις υποστηρικτικές τεχνολογίες, επιτρέπει στις μηχανές αναζήτησης να βρίσκουν λέξεις-κλειδιά και να αναγνωρίζουν έγγραφα στην επιθυμητή γλώσσα. Η σήμανση της φυσικής γλώσσας επίσης βελτιώνει την αναγνωσιμότητα του Ιστού για όλους τους ανθρώπους, συμπεριλαμβανομένων εκείνων με μαθησιακές ειδικές ανάγκες, γνωσιακές ειδικές ανάγκες και ανθρώπων που είναι κωφοί.

Όταν οι συντμήσεις και οι αλλαγές στη φυσική γλώσσα δεν επισημαίνονται, ίσως να μη μπορούν να αποκωδικοποιηθούν όταν παρουσιάζονται φωνητικά ή σε γραφή Braille.

Σημεία ελέγχου:

4.1 Επισημάνετε με τρόπο σαφή αλλαγές στη φυσική γλώσσα του κειμένου του εγγράφου και των ισοδύναμων κειμένων (π.χ. υπότιτλων). **[Προτεραιότητα 1]**

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "lang". Στην XML χρησιμοποιήστε την "xml:lang".

4.2 Καθορίστε την πλήρη ανάπτυξη κάθε σύντμησης ή ακρωνυμίου όταν πρωτοπαρουσιάζεται σε ένα έγγραφο. [Προτεραιότητα 3]

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "title" στα στοιχεία ABBR και ACRONYM. Η παροχή της πλήρους ανάπτυξης στο κυρίως σώμα του εγγράφου επίσης αυξάνει τη χρηστικότητα του εγγράφου.

4.3 Προσδιορίστε τη βασική φυσική γλώσσα του εγγράφου. [Προτεραιότητα 3]

> Για παράδειγμα, στην HTML θέσατε την ιδιότητα (attribute) "lang" στο στοιχείο HTML. Στην XML χρησιμοποιήστε την "xml:lang". Οι διαχειριστές εξυπηρετητών πρέπει να διαμορφώνουν τους εξυπηρετητές κατά τρόπο ώστε να επωφελούνται από τους μηχανισμούς διαπραγμάτευσης περιεχομένου του HTTP, έτσι ώστε οι πελάτες να μπορούν αυτόματα να ανακτούν έγγραφα στην προτιμώμενη γλώσσα.

Οδηγία 5. Δημιουργήστε πίνακες που μετατρέπονται ομαλά.

Εξασφαλίστε ότι οι πίνακες έχουν την απαραίτητη σήμανση για να μετατρέπονται από φυλλομετρητές που υποστηρίζουν την προσβασιμότητα και άλλους πράκτορες χρηστών.

Οι πίνακες θα πρέπει να χρησιμοποιούνται για τη σήμανση πραγματικά ταξινομημένων πληροφοριών («πίνακες δεδομένων»). Οι κατασκευαστές περιεχομένου θα πρέπει να αποφεύγουν τη χρήση πινάκων για σελιδοποίηση («πίνακες σελιδοποίησης»). Πίνακες που χρησιμοποιούνται αδιακρίτως παρουσιάζουν ειδικά προβλήματα για τους χρήστες αναγνωστών οθόνης (βλ. το σημείο ελέγχου 10.3).

Ορισμένοι πράκτορες χρηστών επιτρέπουν στους χρήστες την πλοήγηση ανάμεσα σε κελιά πινάκων και την πρόσβαση σε πληροφορίες κεφαλίδων και άλλων κελιών. Σε περίπτωση ακατάλληλης σήμανσης, αυτοί οι πίνακες δεν παρέχουν στους πράκτορες χρηστών τις κατάλληλες πληροφορίες. (Βλ. επίσης την οδηγία 3.)

Τα ακόλουθα σημεία ελέγχου θα ωφελήσουν άμεσα ανθρώπους που προσπελαύνουν έναν πίνακα χρησιμοποιώντας ακουστικά μέσα (π.χ. έναν αναγνώστη οθόνης ή έναν προσωπικό υπολογιστή αυτοκινήτου) ή οι οποίοι βλέπουν μόνο ένα μέρος της σελίδας τη φορά (π.χ. τυφλοί χρήστες ή χρήστες

με ελαττωμένη όραση που χρησιμοποιούν έξοδο ομιλίας ή *απεικόνιση σε γραφή Braille*, ή άλλοι χρήστες που χρησιμοποιούν συσκευές με μικρές επιφάνειες απεικόνισης, κ.λπ.).

Σημεία ελέγχου:

5.1 Για πίνακες δεδομένων προσδιορίστε κεφαλίδες σειρών και στηλών. **[Προτεραιότητα 1]**

> Για παράδειγμα, στην HTML χρησιμοποιήστε το στοιχείο TD για να προσδιορίσετε κελιά δεδομένων και το στοιχείο TH για να προσδιορίσετε κεφαλίδες.

5.2 Για πίνακες δεδομένων που έχουν δύο ή περισσότερα λογικά επίπεδα σειρών ή στηλών, χρησιμοποιήστε σήμανση για να συσχετίσετε κελιά δεδομένων με κελιά κεφαλίδων. **[Προτεραιότητα 1]**

> Για παράδειγμα, στην HTML χρησιμοποιήστε τα στοιχεία THEAD, TFOOT και TBODY για την ομαδοποίηση σειρών, τα στοιχεία COL και COLGROUP για την ομαδοποίηση στηλών και τις ιδιότητες (attributes) "axis", "scope" και "headers" για την περιγραφή πιο περίπλοκων σχέσεων μεταξύ δεδομένων.

5.3 Μη χρησιμοποιείτε πίνακες για σελιδοποίηση, εκτός αν ο πίνακας βγάζει νόημα όταν απεικονίζεται γραμμικά. Αλλιώς, εάν ο πίνακας δεν βγάζει νόημα, Παρέχετε ένα εναλλακτικό ισοδύναμο (το οποίο μπορεί να είναι μια γραμμική εκδοχή).[Προτεραιότητα 2]

> Σημείωση. *Άπαξ και οι πράκτορες χρηστών* υποστηρίζουν τοποθέτηση μέσω φύλλων στυλ, οι πίνακες δεν θα πρέπει να χρησιμοποιούνται για σελιδοποίηση. Βλ. επίσης το σημείο ελέγχου 3.3.

5.4 Εάν ένας πίνακας χρησιμοποιείται για σελιδοποίηση, μην χρησιμοποιείτε οποιαδήποτε δομική σήμανση με σκοπό τη οπτική μορφοποίηση. [Προτεραιότητα 2]

> Για παράδειγμα, στην HTML μην χρησιμοποιείτε το στοιχείο TH με σκοπό να κάνετε το περιεχόμενο ενός κελιού (που δεν είναι κεφαλίδα πίνακα) να εμφανίζεται κεντραρισμένο και με έντονα γράμματα.

5.5 Παρέχετε περίληψη για κάθε πίνακα. [Προτεραιότητα 3]

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "summary" του στοιχείου TABLE.

5.6 Παρέχετε συντμήσεις για το περιεχόμενο των κεφαλίδων. [Προτεραιότητα 3]

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "abbr" στο στοιχείο TH.
>
> Βλ. επίσης το σημείο ελέγχου 10.3.

Οδηγία 6. Εξασφαλίστε ότι οι σελίδες που εμπεριέχουν νέες τεχνολογίες μετατρέπονται ομαλά.

Εξασφαλίστε ότι οι σελίδες είναι προσβάσιμες ακόμα και όταν οι νεώτερες τεχνολογίες δεν υποστηρίζονται ή είναι απενεργοποιημένες.

Αν και οι κατασκευαστές περιεχομένου ενθαρρύνονται να χρησιμοποιούν νέες τεχνολογίες, οι οποίες λύνουν προβλήματα που έχουν τεθεί από τις υπάρχουσες τεχνολογίες, πρέπει να ξέρουν πώς να κάνουν τις σελίδες τους να εξακολουθούν να λειτουργούν με παλαιότερους φυλλομετρητές, καθώς επίσης και για ανθρώπους που επιλέγουν να απενεργοποιούν ορισμένα χαρακτηριστικά.

Σημεία ελέγχου:

6.1 Οργανώστε τα έγγραφα έτσι ώστε να μπορούν να διαβαστούν χωρίς φύλλα στυλ. Για παράδειγμα, όταν ένα έγγραφο HTML αποδίδεται χωρίς συσχετιζόμενα φύλλα στυλ, πρέπει να παραμένει αναγνώσιμο. **[Προτεραιότητα 1]**

> Όταν το περιεχόμενο είναι λογικά οργανωμένο, αποδίδεται με τρόπο που να έχει νόημα στις περιπτώσεις που τα φύλλα στυλ είναι απενεργοποιημένα ή δεν υποστηρίζονται.

6.2 Εξασφαλίστε ότι τα ισοδύναμα δυναμικού περιεχομένου ενημερώνονται όταν το δυναμικό περιεχόμενο αλλάζει. **[Προτεραιότητα 1]**

6.3 Εξασφαλίστε ότι οι σελίδες είναι χρηστικές όταν τα προγραμματιστικά σενάρια (scripts), τα ενσωματωμένα προγράμματα ή άλλα προγραμματιστικά αντικείμενα είναι απενεργοποιημένα ή δεν υποστηρίζονται. Εάν αυτό δεν είναι δυνατόν, παρέχετε ισοδύναμες πληροφορίες σε μια εναλλακτική προσβάσιμη σελίδα. **[Προτεραιότητα 1]**

> Για παράδειγμα, εξασφαλίστε ότι οι σύνδεσμοι που θέτουν σε λειτουργία τα προγραμματιστικά σενάρια (scripts) λειτουργούν όταν υα προγραμματιστικά σενάρια (scripts) είναι απενεργοποιημένα ή δεν υποστηρίζονται (π.χ. μην χρησιμοποιείτε την έκφραση "javascript:" ως στόχο συνδέσμου). Εάν δεν είναι δυνατόν να κάνετε τη σελίδα χρηστική χωρίς προγραμματιστικά σενάρια (scripts), παρέχετε ένα ισοδύναμο κείμενο με το στοιχείο NOSCRIPT, ή χρησιμοποιήστε ένα προγραμματιστικό σενάριο (script) στην πλευρά του εξυπηρετητή, αντί για ένα προγραμματιστικό σενάριο (script) στην πλευρά του πελάτη, ή παρέχετε μια εναλλακτική προσβάσιμη σελίδα σύμφωνα με το σημείο ελέγχου 11.4. Βλ. επίσης την οδηγία 1.

6.4 Για προγραμματιστικά σενάρια (scripts) και ενσωματωμένα προγράμματα, εξασφαλίστε ότι οι χειριστές γεγονότων του προγράμματος ή της ρουτίνας δεν εξαρτώνται από τη συσκευή εισόδου. [Προτεραιότητα 2]

6.5 Εξασφαλίστε ότι το δυναμικό περιεχόμενο είναι προσβάσιμο ή παρέχετε μια εναλλακτική μορφή ή σελίδα. [Προτεραιότητα 2]

Για παράδειγμα, στην HTML, χρησιμοποιήστε το στοιχείο NOFRAMES στο τέλος κάθε συνόλου πλαισίων (frameset). Για κάποιες εφαρμογές τα προγραμματιστικά σενάρια (scripts) στην πλευρά του εξυπηρετητή είναι πιο προσβάσιμα από προγραμματιστικά σενάρια (scripts) στην πλευρά του πελάτη.

Βλ. επίσης το σημείο ελέγχου 11.4.

Οδηγία 7. Εξασφαλίστε ότι ο χρήστης ελέγχει τις μεταβολές περιεχομένου που εξαρτώνται από τον χρόνο.

Εξασφαλίστε ότι αντικείμενα ή σελίδες που κινούνται, αναβοσβήνουν, κυλάνε ή ενημερώνονται αυτόματα μπορούν να σταματήσουν στιγμιαία ή εντελώς.

Ορισμένοι άνθρωποι με γνωσιακές ειδικές ανάγκες ή προβλήματα όρασης είναι ανίκανοι να διαβάσουν αρκετά γρήγορα ένα κείμενο που κινείται ή δεν μπορούν να το διαβάσουν καθόλου. Η κίνηση μπορεί επίσης να προκαλέσει τέτοια απόσπαση προσοχής ώστε η υπόλοιπη σελίδα να μην μπορεί να διαβαστεί από ανθρώπους με γνωσιακές ειδικές ανάγκες. Οι *αναγνώστες οθόνης* δεν μπορούν να διαβάσουν κινούμενο κείμενο. Άνθρωποι με σωματικές αναπηρίες μπορεί να μην είναι σε θέση να κινηθούν γρήγορα ή με αρκετή ακρίβεια ώστε να αλληλεπιδράσουν με κινούμενα αντικείμενα.

Σημείωση. Όλα τα ακόλουθα σημεία ελέγχου ανήκουν ως ένα βαθμό στη σφαίρα ευθύνης των κατασκευαστών περιεχομένου, μέχρι οι πράκτορες χρηστών να παρέχουν επαρκείς μηχανισμούς ελέγχου των σχετικών χαρακτηριστικών.

Σημεία ελέγχου:

7.1 Μέχρι οι πράκτορες χρηστών να επιτρέπουν στους χρήστες να ελέγχουν το τρεμοπαίξιμο, αποφύγετε να κάνετε την οθόνη να τρεμοπαίζει. **[Προτεραιότητα 1]**

Σημείωση. Οι άνθρωποι με φωτοευαίσθητη επιληψία μπορεί να πάθουν κρίσεις που προκαλούνται από τρεμοπαίξιμο ή στιγμιαίες λάμψεις στο εύρος των 4 ως 59 στιγμιαίων λάμψεων ανά δευτερόλεπτο (Hertz) με μέγιστη ευαισθησία στις 20 στιγμιαίες λάμψεις ανά δευτερόλεπτο. Επίσης μπορεί να προκληθούν κρίσεις από απότομες εναλλαγές μεταξύ σκότους και φωτός (όπως τα στροβοσκοπικά φώτα).

7.2 Μέχρι οι πράκτορες χρηστών να επιτρέπουν στους χρήστες να ελέγχουν περιεχόμενο που αναβοσβήνει, αποφύγετε να κάνετε το περιεχόμενο να αναβοσβήνει (δηλαδή αποφύγετε να αλλάζετε τη μορφή σε τακτά χρονικά διαστήματα κάνοντάς την να αναβοσβήνει). [Προτεραιότητα 2]

7.3 Μέχρι οι πράκτορες χρηστών να επιτρέπουν στους χρήστες να ακινητοποιούν το κινούμενο περιεχόμενο, αποφύγετε τη δημιουργία κινούμενου περιεχομένου στις σελίδες. [Προτεραιότητα 2]

Όταν μια σελίδα περιλαμβάνει κινούμενο περιεχόμενο, παρέχετε έναν μηχανισμό μέσω ενός προγραμματιστικού σεναρίου (script) ή ενός ενσωματωμένου προγράμματος που να επιτρέπει στους χρήστες να σταματούν τη κίνηση ή τις ανανεώσεις. Η χρήση φύλλων στυλ παράλληλα με προγραμματιστικά σενάρια (scripts) για τη δημιουργία κίνησης επιτρέπει στους χρήστες να απενεργοποιούν ή να ξεπερνούν το εφέ πιο εύκολα. Βλ. επίσης την οδηγία 8.

7.4 Μέχρι οι πράκτορες χρηστών να παρέχουν τη δυνατότητα στους χρήστες να εμποδίζουν την επαναφόρτωση, μην δημιουργείτε σελίδες που επαναφορτώνονται αυτόματα σε τακτά χρονικά διαστήματα. [Προτεραιότητα 2]

Για παράδειγμα, στην HTML μην κάνετε τις σελίδες να επαναφορτώνονται αυτόματα με την έκφραση "HTTP-EQUIV=refresh" μέχρι οι πράκτορες χρηστών να επιτρέπουν στους χρήστες να απενεργοποιούν αυτό το χαρακτηριστικό.

7.5 Μέχρι οι πράκτορες χρηστών να παρέχουν τη δυνατότητα στους χρήστες να εμποδίζουν την αυτόματη επαναδρομολόγηση, μη χρησιμοποιείτε σήμανση για να επαναδρομολογείτε σελίδες αυτόματα. Αντιθέτως, διαμορφώστε τον εξυπηρετητή έτσι ώστε να εκτελεί τις επαναδρομολογήσεις. [Προτεραιότητα 2]

Σημείωση. Τα στοιχεία BLINK και MARQUEE δεν ορίζονται σε καμία από τις προδιαγραφές του W3C για την HTML και δεν πρέπει να χρησιμοποιούνται. Βλ. επίσης την οδηγία 11.

Οδηγία 8. Εξασφαλίστε την άμεση προσβασιμότητα των ενσωματωμένων περιβαλλόντων διεπαφής χρήστη.

Εξασφαλίστε ότι η επιφάνεια διεπαφής χρήστη ακολουθεί τις αρχές του σχεδιασμού με στόχο την προσβασιμότητα: πρόσβαση στις λειτουργίες ανεξάρτητα από συσκευές, χειρισμός μέσω πληκτρολογίου, δυνατότητα μετατροπής σε ακουστικό περιεχόμενο κ.λπ.

Όταν ένα ενσωματωμένο αντικείμενο έχει τη «δική του επιφάνεια διεπαφής χρήστη», η επιφάνεια διεπαφής --όπως και η αντίστοιχη του ίδιου του φυλλομετρητή--πρέπει να προσβάσιμη. Εάν η επιφάνεια διεπαφής του ενσωματωμένου αντικειμένου δεν μπορεί να καταστεί προσβάσιμη, πρέπει να παρέχεται μια εναλλακτική προσβάσιμη λύση.

Σημείωση. Για πληροφορίες σχετικά με προσβάσιμες επιφάνειες διεπαφής παρακαλούμε συμβουλευθείτε τον δικτυακό τόπο Οδηγίες Προσβασιμότητας για τους Πράκτορες Χρηστών ([WAI-USERAGENT]) και τον δικτυακό τόπο Οδηγίες Προσβασιμότητας για Εργαλεία Συγγραφής ([WAI-AUTOOL]).

Σημεία ελέγχου:

8.1 Καταστήστε τα προγραμματιστικά στοιχεία, όπως τις προγραμματιστικά σενάρια (scripts) και τα ενσωματωμένα προγράμματα, άμεσα προσβάσιμα ή συμβατά με υποστηρικτικές τεχνολογίες.

[**Προτεραιότητα 1** εάν η λειτουργικότητα είναι σημαντική και δεν παρουσιάζεται αλλού, αλλιώς Προτεραιότητα 2.]

Βλ. επίσης την οδηγία 6.

Οδηγία 9. Σχεδιάστε ανεξάρτητα από συσκευές.

Χρησιμοποιήστε χαρακτηριστικά που ενεργοποιούν τα στοιχεία της σελίδας μέσω μιας ποικιλίας συσκευών εισόδου.

Πρόσβαση ανεξάρτητη από συσκευές σημαίνει ότι ο χρήστης μπορεί να αλληλεπιδρά με τον πράκτορα χρήστη ή το έγγραφο μέσω της προτιμώμενης συσκευής εισόδου (ή εξόδου) --ποντίκι, πληκτρολόγιο, φωνή, ράβδο κεφαλής ή άλλη. Εάν, για παράδειγμα, ένα στοιχείο ελέγχου μιας φόρμας μπορεί να ενεργοποιηθεί μόνο με το ποντίκι ή άλλη συσκευή κατάδειξης, κάποιο άτομο που χρησιμοποιεί τη σελίδα χωρίς όραση, μέσω εισόδου φωνής ή μέσω πληκτρολογίου, ή που χρησιμοποιεί κάποια άλλη συσκευή εισόδου που δεν καταδεικνύει, δεν θα μπορεί να χρησιμοποιήσει τη φόρμα.

Σημείωση. Η παροχή ισοδύναμων κειμένων καθιστά δυνατή για τους χρήστες την αλληλεπίδραση με χάρτες εικόνας ή εικόνες που χρησιμοποιούνται ως σύνδεσμοι χωρίς συσκευή κατάδειξης. Βλ. επίσης την οδηγία 1.

Γενικά, σελίδες που επιτρέπουν την αλληλεπίδραση μέσω πληκτρολογίου είναι επίσης προσβάσιμες μέσω συσκευών εισόδου ομιλίας ή μέσω περιβάλλοντος γραμμής εντολών.

Σημεία ελέγχου:

9.1 Παρέχετε χάρτες εικόνας στην πλευρά του πελάτη αντί για χάρτες εικόνας στην πλευρά του εξυπηρετητή, εκτός από τις περιπτώσεις όπου οι περιοχές δεν μπορούν να οριστούν με ένα διαθέσιμο γεωμετρικό σχήμα. **[Προτεραιότητα 1]**

Βλ. επίσης το σημείο ελέγχου 1.1, το σημείο ελέγχου 1.2 και το σημείο ελέγχου 1.5.

9.2 Εξασφαλίστε ότι οποιοδήποτε στοιχείο το οποίο έχει τη δική του επιφάνεια διεπαφής χρήστη μπορεί να λειτουργήσει κατά τρόπο ανεξάρτητο από συσκευές. [Προτεραιότητα 2]

Βλ. τον ορισμό της ανεξαρτησίας από συσκευές.

Βλ. επίσης την οδηγία 8.

9.3 Για προγραμματιστικά σενάρια (scripts) καλύτερα προσδιορίστε λογικούς χειριστές γεγονότων της ρουτίνας, παρά χειριστές γεγονότων εξαρτώμενους από συσκευές. [Προτεραιότητα 2]

9.4 Δημιουργήστε μια λογική σειρά στηλοθέτησης ανάμεσα στους συνδέσμους, τα στοιχεία ελέγχου φορμών και τα αντικείμενα.[Προτεραιότητα 3]

Για παράδειγμα, στην HTML προσδιορίστε τη σειρά στηλοθέτησης μέσω της ιδιότητας (attribute) "tabindex" ή εξασφαλίστε έναν λογικό σχεδιασμό της σελίδας.

9.5 Παρέχετε συντομεύσεις πληκτρολογίου για σημαντικούς συνδέσμους (συμπεριλαμβανομένων των χαρτών εικόνας στην πλευρά του πελάτη), στοιχεία ελέγχου φορμών και σύνολα στοιχείων ελέγχου φορμών. [Προτεραιότητα 3]

Για παράδειγμα, στην HTML προσδιορίστε συντομεύσεις μέσω της ιδιότητας (attribute) "accesskey".

Οδηγία 10. Χρησιμοποιείστε προσωρινές λύσεις.

Χρησιμοποιήστε προσωρινές λύσεις προσβασιμότητας, έτσι ώστε οι υποστηρικτικές τεχνολογίες και οι παλαιότεροι φυλλομετρητές να λειτουργούν σωστά.

Για παράδειγμα, οι παλαιότεροι φυλλομετρητές δεν επιτρέπουν στους χρήστες να πλοηγούνται σε άδεια κουτιά εισαγωγής δεδομένων. Οι παλαιότεροι αναγνώστες οθόνης διαβάζουν λίστες συνεχόμενων συνδέσμων σαν ένα σύνδεσμο. Αυτά τα ενεργά στοιχεία είναι συνεπώς δύσκολο ή αδύνατο να προσπελαστούν. Επίσης, η αλλαγή του τρέχοντος παράθυρου ή η απροειδοποίητη εμφάνιση νέων παραθύρων μπορεί να είναι ιδιαίτερα αποπροσανατολιστική για χρήστες που δεν μπορούν να δουν ότι κάτι τέτοιο έχει συμβεί.

Σημείωση: Τα ακόλουθα σημεία ελέγχου εφαρμόζονται μέχρι οι πράκτορες χρηστών (συμπεριλαμβανομένων των υποστηρικτικών τεχνολογιών) να αντιμετωπίσουν τα σχετικά ζητήματα. Αυτά τα σημεία ελέγχου χαρακτηρίζονται ως «προσωρινά», υπό την έννοια ότι η Ομάδας Εργασίας για τις Οδηγίες Περιεχομένου του Ιστού τα θεωρεί έγκυρα και απαραίτητα για την προσβασιμότητα του Ιστού από την έκδοση του παρόντος εγγράφου. Παρ' όλα αυτά, η Ομάδα Εργασίας προβλέπει ότι αυτά τα σημεία ελέγχου δεν θα είναι απαραίτητα στο μέλλον, άπαξ οι τεχνολογίες του Ιστού ενσωματώσουν τα προσδοκώμενα χαρακτηριστικά και δυνατότητες.

Σημεία ελέγχου:

10.1 Μέχρι οι πράκτορες χρηστών να επιτρέπουν στους χρήστες να απενεργοποιούν τα παράθυρα που εμφανίζονται ξαφνικά, μην χρησιμοποιείτε παράθυρα που εμφανίζονται απροσδόκητα και μην αλλάζετε το τρέχον παράθυρο χωρίς να ενημερώνετε τον χρήστη. [Προτεραιότητα 2]

Για παράδειγμα, στην HTML αποφύγετε τη χρήση ενός πλαισίου (frame) που ανοίγει σε νέο παράθυρο.

10.2 *Μέχρι οι πράκτορες χρηστών* να υποστηρίζουν σαφείς συσχετισμούς μεταξύ τίτλων και ενεργών στοιχείων φόρμας, για όλα τα ενεργά στοιχεία μιας φόρμας που έχουν ασαφώς

συσχετισμένους τίτλους, εξασφαλίστε ότι ο κάθε τίτλος βρίσκεται στη σωστή θέση. [Προτεραιότητα 2]

> Ο τίτλος πρέπει να βρίσκεται στην ίδια γραμμή ακριβώς πριν το αντίστοιχο ενεργό στοιχείο φόρμας (επιτρέποντας περισσότερους από έναν τίτλους και ενεργά στοιχεία ανά γραμμή) ή στη γραμμή που προηγείται του στοιχείου ελέγχου (με μόνο έναν τίτλο και ένα ενεργό στοιχείο ανά γραμμή). Βλ. επίσης το σημείο ελέγχου 12.4.

10.3 *Μέχρι οι πράκτορες χρηστών* (συμπεριλαμβανομένων των υποστηρικτικών τεχνολογιών) να αποδίδουν γειτονικά κείμενα σωστά, παρέχετε ένα εναλλακτικό γραμμικό κείμενο (στην τρέχουσα σελίδα ή κάποια άλλη) για *όλους* τους πίνακες που παρουσιάζουν κείμενα σε παράλληλες στήλες εντός των οποίων το κείμενο αναδιπλώνεται. [Προτεραιότητα 3]

> Σημείωση. Παρακαλούμε συμβουλευθείτε τον ορισμό του γραμμικού πίνακα. Το παρόν σημείο ελέγχου ωφελεί ανθρώπους με πράκτορες χρηστών (όπως ορισμένους αναγνώστες οθόνης) οι οποίοι δεν μπορούν να χειριστούν γειτονικά μονοκόμματα κείμενα. Το παρόν σημείο ελέγχου δεν πρέπει να αποθαρρύνει τους κατασκευαστές περιεχομένου από το να χρησιμοποιούν πίνακες για την αναπαράσταση ταξινομημένων πληροφοριών.

10.4 Μέχρι οι πράκτορες χρηστών να χειρίζονται σωστά τα άδεια ενεργά στοιχεία των φορμών, συμπεριλάβετε προκαθορισμένες τιμές στα κουτιά και τις περιοχές εισαγωγής δεδομένων. [Προτεραιότητα 3]

> Για παράδειγμα, στην HTML εφαρμόστε το παραπάνω για τα στοιχεία TEXTAREA και INPUT.

10.5 Μέχρι οι πράκτορες χρηστών (συμπεριλαμβανομένων των υποστηρικτικών τεχνολογιών) να αποδίδουν γειτονικούς συνδέσμους ξεχωριστά, συμπεριλάβετε εκτυπώσιμους χαρακτήρες εκτός των συνδέσμων (με διαστήματα δεξιά και αριστερά) ανάμεσα σε γειτονικούς συνδέσμους. [Προτεραιότητα 3]

Οδηγία 11. Χρησιμοποιείστε τις τεχνολογίες και οδηγίες του W3C.

Χρησιμοποιήστε τεχνολογίες του W3C (σύμφωνα με τις προδιαγραφές) και ακολουθήστε τις οδηγίες προσβασιμότητας. Όπου δεν είναι δυνατόν να χρησιμοποιήσετε μια τεχνολογία του W3C, ή η χρήση της έχει σαν αποτέλεσμα υλικό που δεν μετατρέπεται ομαλά, παρέχετε μια εναλλακτική έκδοση του περιεχομένου που να είναι προσβάσιμη.

Οι παρούσες οδηγίες προτείνουν τις τεχνολογίες του W3C (π.χ. HTML, CSS, κ.λπ.) για αρκετούς λόγους:

- Οι τεχνολογίες του W3C περιλαμβάνουν «ενσωματωμένα» χαρακτηριστικά προσβασιμότητας.

- Οι προδιαγραφές του W3C υφίστανται έλεγχο στα αρχικά στάδια για να εξασφαλιστεί ότι τα ζητήματα προσβασιμότητας συνυπολογίζονται κατά της διάρκεια της φάσης σχεδιασμού.
- Οι προδιαγραφές του W3C αναπτύσσονται μέσω μιας ανοιχτής διαδικασίας με τη συναίνεση της βιομηχανίας.

Πολλές μορφές που δεν έχουν αναπτυχθεί από το W3C (π.χ. PDF, Shockwave, κ.λπ.) απαιτούν είτε πρόσθετα λογισμικού είτε αυτοδύναμες εφαρμογές. Συχνά, με τους κλασικούς πράκτορες χρηστών (συμπεριλαμβανομένων των υποστηρικτικών τεχνολογιών). δεν μπορούμε να δούμε αυτές τις μορφές ή δεν μπορούμε να πλοηγηθούμε σε αυτές. Αποφεύγοντας μορφές που δεν έχουν αναπτυχθεί από το W3C και χαρακτηριστικά που δεν είναι καθιερωμένα (ιδιωτικά στοιχεία, χαρακτηριστικά, ιδιότητες και καταλήξεις) θα έχει σαν αποτέλεσμα σελίδες περισσότερο προσβάσιμες για περισσότερους ανθρώπους που χρησιμοποιούν μια ευρύτερη ποικιλία υλικού εξοπλισμού Η/Υ και λογισμικού. Όταν μη-προσβάσιμες τεχνολογίες (ιδιωτικές ή μη) πρέπει να χρησιμοποιηθούν, ισοδύναμες προσβάσιμες σελίδες πρέπει να παρέχονται.

Ακόμα και όταν οι τεχνολογίες του W3C χρησιμοποιούνται, πρέπει να χρησιμοποιούνται σύμφωνα με τις οδηγίες προσβασιμότητας. Όταν χρησιμοποιείτε νέες τεχνολογίες, εξασφαλίστε ότι μετατρέπονται ομαλά (βλ. επίσης την οδηγία 6.).

Σημείωση. Η μετατροπή εγγράφων (από PDF, PostScript, RTF, κ.λπ.) σε γλώσσες σήμανσης του W3C (HTML, XML) δεν δημιουργεί πάντα ένα προσβάσιμο έγγραφο. Συνεπώς, ελέγξτε κάθε σελίδα ως προς την προσβασιμότητα και τη χρηστικότητα μετά τη διαδικασία μετατροπής (βλ. τον τομέα σχετικά με την αξιολόγηση). Εάν μια σελίδα δεν μετατρέπεται εύκολα, είτε αναθεωρήστε τη σελίδα μέχρι η αρχική της μορφή να μετατρέπεται κατάλληλα είτε παρέχετε μια έκδοση HTML ή απλού κειμένου.

Σημεία ελέγχου:

11.1 Χρησιμοποιήστε τεχνολογίες του W3C όταν είναι διαθέσιμες και κατάλληλες για μια εργασία και χρησιμοποιήστε τις πιο πρόσφατες εκδόσεις όταν υποστηρίζονται. [Προτεραιότητα 2]

> Βλ. τη λίστα αναφορών για πληροφορίες σχετικά με το πού να βρείτε τις πιο πρόσφατες προδιαγραφές του W3C και τον δικτυακό τόπο[WAI-UA-SUPPORT] για πληροφορίες σχετικά με την υποστήριξη πρακτόρων χρηστών για τεχνολογίες του W3C.

11.2 Αποφύγετε αποδοκιμαζόμενα χαρακτηριστικά των τεχνολογιών του W3C.[Προτεραιότητα 2]

> Για παράδειγμα, στην HTML μην χρησιμοποιείτε το αποδοκιμαζόμενο στοιχείο FONT. Στη θέση του χρησιμοποιήστε φύλλα στυλ (π.χ. την ιδιότητα 'font' των CSS).

11.3 Παρέχετε πληροφορίες έτσι ώστε οι χρήστες να μπορούν να ανακτούν έγγραφα σύμφωνα με τις προτιμήσεις τους (γλώσσα, τύπο περιεχομένου, κ.λπ.). [Προτεραιότητα 3]

> Σημείωση. Χρησιμοποιήστε διαπραγμάτευση περιεχομένου όπου είναι δυνατόν.

11.4 Εάν, αφού έχετε καταβάλλει κάθε δυνατή προσπάθεια, δεν μπορείτε να δημιουργήσετε μια προσβάσιμη σελίδα, παρέχετε ένα σύνδεσμο προς μία εναλλακτική σελίδα που χρησιμοποιεί σελίδες του W3C, είναι προσβάσιμη, έχει ισοδύναμες πληροφορίες (ή λειτουργικότητα) και ενημερώνεται εξίσου συχνά με τη μη-προσβάσιμη (αρχική) σελίδα. **[Προτεραιότητα 1]**

> Σημείωση. Οι κατασκευαστές περιεχομένου πρέπει να καταφεύγουν σε εναλλακτικές σελίδες μόνο όταν οι άλλες λύσεις αποτυγχάνουν, επειδή οι εναλλακτικές σελίδες γενικά ενημερώνονται λιγότερο συχνά από τις «βασικές» σελίδες. Μια ανεπίκαιρη σελίδα μπορεί να είναι τόσο απογοητευτική όσο και μία μη-προσβάσιμη, από τη στιγμή που, και στις δύο περιπτώσεις, οι πληροφορίες που παρουσιάζονται στην αρχική σελίδα δεν είναι διαθέσιμες. Εναλλακτικές σελίδες που δημιουργούνται αυτόματα μπορεί να έχουν ως αποτέλεσμα πιο συχνές ενημερώσεις, αλλά οι κατασκευαστές περιεχομένου πρέπει παρόλα αυτά να είναι προσεκτικοί έτσι ώστε να εξασφαλίσουν ότι οι σελίδες που δημιουργούνται βγάζουν πάντα νόημα, και ότι οι χρήστες είναι σε θέση να πλοηγηθούν σε έναν δικτυακό τόπο ακολουθώντας τους συνδέσμους των αρχικών σελίδων ή των εναλλακτικών σελίδων ή και των δύο. Πριν καταφύγετε στη λύση μιας εναλλακτικής σελίδας, ξανασκεφτείτε τον σχεδιασμό της αρχικής σελίδας: το να την κάνετε προσβάσιμη είναι πιθανό να τη βελτιώσει για όλους τους χρήστες.

Οδηγία 12. Παρέχετε πληροφορίες σχετικά με το γενικότερο πλαίσιο και τον προσανατολισμό.

Παρέχετε πληροφορίες σχετικά με τα συμφραζόμενα και τον προσανατολισμό για να βοηθήσετε τους χρήστες να καταλάβουν περίπλοκες σελίδες ή στοιχεία.

Η ομαδοποίηση των στοιχείων και η παροχή συμφραζομένων πληροφοριών σχετικά με τις σχέσεις μεταξύ των στοιχείων μπορεί να είναι χρήσιμες για όλους τους χρήστες. Περίπλοκες σχέσεις μεταξύ των τμημάτων της σελίδας μπορεί να ερμηνεύονται δύσκολα από ανθρώπους με γνωσιακές ειδικές ανάγκες ή προβλήματα όρασης.

Σημεία ελέγχου:

12.1 Βάλτε τίτλο σε κάθε πλαίσιο (frame) για να διευκολύνετε τον προσδιορισμό του πλαισίου (frame) και την πλοήγηση. **[Προτεραιότητα 1]**

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "title" σε κάθε στοιχείο FRAME.

12.2 Περιγράψτε τον σκοπό των πλαισίων (frames) και πώς αυτά σχετίζονται το ένα με το άλλο, εάν αυτό δεν είναι προφανές από τους τίτλους τους και μόνο. [Προτεραιότητα 2]

> Για παράδειγμα, στην HTML χρησιμοποιήστε την ιδιότητα (attribute) "longdesc" ή έναν περιγραφικό σύνδεσμο.

12.3 Χωρίστε μεγάλα τμήματα πληροφοριών σε πιο εύκολα ελέγξιμα τμήματα όπου αυτό είναι φυσικό και κατάλληλο.[Προτεραιότητα 2]

Για παράδειγμα, στην HTML χρησιμοποιήστε το στοιχείο OPTGROUP για να ομαδοποιήσετε στοιχεία OPTION μέσα σε ένα στοιχείο SELECT, ομαδοποιήστε στοιχεία ελέγχου φορμών με τα στοιχεία FIELDSET και LEGEND, χρησιμοποιήστε λίστες τη μία μέσα στην άλλη όπου αυτό είναι κατάλληλο, χρησιμοποιήστε τίτλους για να δομήσετε έγγραφα, κ.λπ. *Βλ. επίσης την οδηγία 3.*

12.4 Συσχετίστε τα ενεργά στοιχεία φόρμας με τους αντίστοιχους τίτλους με σαφήνεια. [Προτεραιότητα 2]

Για παράδειγμα, στην HTML χρησιμοποιήστε το στοιχείο LABEL και την ιδιότητά του "for".

Οδηγία 13. Παρέχετε κατανοητούς μηχανισμούς πλοήγησης.

Παρέχετε κατανοητούς και συνεπείς μηχανισμούς πλοήγησης --πληροφορίες προσανατολισμού, μπάρες πλοήγησης, έναν χάρτη του δικτυακού τόπου, κ.λπ.-- για να αυξήσετε την πιθανότητα ένα άτομο να βρει αυτό που ψάχνει στον δικτυακό τόπο.

Οι κατανοητοί και συνεπείς μηχανισμοί πλοήγησης είναι σημαντικοί για ανθρώπους με γνωσιακές ειδικές ανάγκες ή με τυφλότητα, και ωφελεί όλους τους χρήστες.

Σημεία ελέγχου:

13.1 Προσδιορίστε με τρόπο κατανοητό το πού οδηγεί κάθε σύνδεσμος. [Προτεραιότητα 2]

Το κείμενο συνδέσμου πρέπει να είναι τέτοιο ώστε να βγάζει νόημα ακόμα και όταν διαβάζεται εκτός συμφραζομένων --είτε μόνο του είτε ως μέρος μιας σειράς συνδέσμων. Το κείμενο συνδέσμου πρέπει επίσης να είναι λακωνικό.

Για παράδειγμα, στην HTML γράψτε «Πληροφορίες σχετικά με την έκδοση 4.3» αντί για «κάντε κλικ εδώ». οι κατασκευαστές περιεχομένου πρέπει, εκτός από το να παρέχουν κατανοητά κείμενα συνδέσμων, να αποσαφηνίζουν περαιτέρω το πού ένας σύνδεσμος οδηγεί με έναν πληροφοριακό τίτλο συνδέσμου (π.χ. στην HTML με χρήση της ιδιότητας (attribute) "title").

13.2 Παρέχετε μεταδεδομένα για να προσθέσετε σημασιολογικές πληροφορίες σε σελίδες και δικτυακούς τόπους.[Προτεραιότητα 2]

Για παράδειγμα, χρησιμοποιήστε RDF για να δηλώσετε τον συγγραφέα του εγγράφου, τον τύπο του εγγράφου, κ.λπ.

Σημείωση. Ορισμένοι πράκτορες χρηστών μπορούν να κατασκευάσουν εργαλεία πλοήγησης από σχέσεις εγγράφου που περιγράφονται από το στοιχείο LINK της HTML

και τις ιδιότητες "rel" ή "rev" (π.χ. rel="next", rel="previous", rel="index", κ.λπ.). *Βλ. επίσης το σημείο ελέγχου 13.5*.

13.3 Παρέχετε πληροφορίες σχετικά με τη γενική σελιδοποίηση ενός δικτυακού τόπου (π.χ. έναν χάρτη του δικτυακού τόπου ή έναν πίνακα περιεχομένων). [Προτεραιότητα 2]

Στην περιγραφή της σελιδοποίησης του δικτυακού τόπου τονίστε και εξηγήστε τα διαθέσιμα χαρακτηριστικά προσβασιμότητας.

13.4 Χρησιμοποιήστε τους μηχανισμούς πλοήγησης με συνεπή τρόπο. [Προτεραιότητα 2]

13.5 Παρέχετε μπάρες πλοήγησης για να τονίσετε και να κάνετε πιο προσιτούς τους μηχανισμούς πλοήγησης. [Προτεραιότητα 3]

13.6 *Ομαδοποιήστε* σχετιζόμενους συνδέσμους, προσδιορίστε την ομάδα (για τους πράκτορες χρηστών) και, μέχρι οι πράκτορες χρηστών να προσφέρουν τη σχετική λειτουργία, παρέχετε έναν τρόπο για να αποφεύγεται ολόκληρη η ομάδα.[Προτεραιότητα 3]

13.7 Εάν παρέχονται λειτουργίες αναζήτησης, ενεργοποιήστε διαφορετικούς τύπους αναζήτησης για διαφορετικά επίπεδα ικανοτήτων και προτιμήσεων. [Προτεραιότητα 3]

13.8 Τοποθετήστε πληροφορίες διαφοροποίησης στην αρχή τίτλων, παραγράφων, λιστών, κ.λπ. [Προτεραιότητα 3]

Σημείωση. Αυτό συνήθως αναφέρεται ως «προ-εφοδιασμός» και είναι ιδιαίτερα εξυπηρετικό για ανθρώπους που προσπελαύνουν πληροφορίες μέσω σειριακών συσκευών, όπως συνθέτες ομιλίας.

13.9 Παρέχετε πληροφορίες σχετικά με συλλογές εγγράφων (δηλαδή εγγράφων που αποτελούνται από πολλαπλές σελίδες).[Προτεραιότητα 3]

Για παράδειγμα, στην HTML προσδιορίστε συλλογές εγγράφων μέσω του στοιχείου LINK και των ιδιοτήτων (attributes) "rel" και "rev". Ένας άλλος τρόπος να δημιουργήσετε μια συλλογή είναι μέσω αρχειοθέτησης των πολλαπλών σελίδων (π.χ. με προγράμματα zip, tar και gzip, stuffit, κ.λπ.).

Σημείωση. Η βελτίωση της απόδοσης που επιτυγχάνεται μέσω της επεξεργασίας εκτός δικτύου μπορεί να μειώσει σημαντικά το κόστος της περιήγησης για ανθρώπους με αναπηρίες που είναι πιθανόν να περιηγούνται αργά.

13.10 Παρέχετε ένα μέσο υπερπήδησης απεικονίσεων τέχνης ASCII πολλαπλών γραμμών. [Προτεραιότητα 3]

Βλ. το *σημείο ελέγχου 1.1*

Οδηγία 14. Εξασφαλίστε ότι τα έγγραφα είναι κατανοητά και απλά.

Εξασφαλίστε ότι τα έγγραφα είναι σαφή και απλά έτσι ώστε να είναι πιο εύκολα κατανοητά.

Συνεπής σελιδοποίηση, αναγνωρίσιμα γραφικά και εύκολη στην κατανόηση γλώσσα ωφελούν όλους τους χρήστες. Ιδιαίτερα, βοηθούν ανθρώπους με γνωσιακές ειδικές ανάγκες ή ανθρώπους που έχουν δυσκολία στην ανάγνωση. (Παρ' όλα αυτά, εξασφαλίστε ότι υπάρχουν ισοδύναμα κείμενα για τις εικόνες για ανθρώπους που είναι τυφλοί, έχουν ελαττωμένη όραση ή για οποιονδήποτε χρήστη δεν μπορεί να δει ή έχει επιλέξει να μη βλέπει γραφικά**.** *Βλ. επίσης την οδηγία 1***.)**

Η χρήση κατανοητής και απλής γλώσσας προωθεί την αποτελεσματική επικοινωνία. Η πρόσβαση σε γραπτές πληροφορίες μπορεί να είναι δύσκολη για ανθρώπους που έχουν γνωσιακές ή μαθησιακές ειδικές ανάγκες. Η χρήση κατανοητής και απλής γλώσσας ωφελεί επίσης ανθρώπους των οποίων η μητρική γλώσσα διαφέρει από τη δική σας, συμπεριλαμβανομένων των ανθρώπων που επικοινωνούν κυρίως μέσω νοηματικής γλώσσας.

Σημεία ελέγχου:

14.1 Χρησιμοποιήστε την πλέον κατανοητή και απλή γλώσσα που είναι κατάλληλη για το περιεχόμενο ενός δικτυακού τόπου.**[Προτεραιότητα 1]**

14.2 Συμπληρώστε το κείμενο με γραφικές ή ακουστικές παρουσιάσεις σε όποια σημεία αυτές θα διευκολύνουν την κατανόηση της σελίδας. [Προτεραιότητα 3]

14.3 Δημιουργήστε ένα στυλ μορφής που να είναι συνεπές σε όλες τις σελίδες. [Προτεραιότητα 3].[26]

2.6.2. Οδηγίες για την Προσβασιμότητα του Περιεχομένου του Ιστού WCAG v 2.0

Οι οδηγίες WCAG 2.0 που δημοσιεύθηκαν στις 11 Δεκεμβρίου του 2008 βασίζονται σε 4 αρχές (αντιληπτή, λειτουργικότητα, κατανοητή, τεχνικά ισχυρή):

- **Αντιληπτή:**

  Οι πληροφορίες και τα στοιχεία διεπαφής του χρήστη πρέπει να είναι ευπαρουσίαστη για τους χρήστες με τρόπους που να μπορούν να αντιληφθούν,

- **Λειτουργικότητα:**

  Τα στοιχεία διεπαφής χρήστη και πλοήγησης πρέπει να είναι πρακτικά,

- **Κατανοητή:**

Οι πληροφορίες και οι λειτουργίες των χρηστών πρέπει να είναι κατανοητές,

- **Τεχνικά ισχυρή:**

  Το περιεχόμενο πρέπει να είναι αρκετά ισχυρό ώστε να μπορεί να ερμηνευτεί αξιόπιστα από μια ευρεία ποικιλία πρακτόρων χρηστών, συμπεριλαμβανομένων των υποστηρικτικών τεχνολογιών.

Είναι πιο καλά δομημένες από τις WCAG 1.0 και ανεξάρτητες από την τεχνολογία κατά τη διαμόρφωση κριτηρίων. Σημεία ελέγχου τεκμηριώνουν τις αρχές, για παράδειγμα, για να διασφαλιστεί ότι η ιστοσελίδα γίνεται εύκολα αντιληπτή, περιλαμβάνει σημεία ελέγχου σχετικά με τις απαιτήσεις που απαιτούνται για τα άτομα με χαμηλή όραση, καθώς και για όσους έχουν προβλήματα ακοής. Εκτός αυτού, υπάρχει το διεθνές πρότυπο ISO / TS 16071 (Εργονομία της ανθρώπινης αλληλεπίδρασης με τα συστήματα-καθοδήγηση όσον αφορά την προσβασιμότητα των διεπαφών ανθρώπου-υπολογιστή), η οποία δεν είχε προσελκύσει ιδιαίτερη προσοχή μέχρι πρόσφατα. Κυρίως ασχολείται με προϊόντα λογισμικού. Τα πρότυπα για την εργονομία λογισμικού, ειδικά DIN EN ISO 9241 (Εργονομικές απαιτήσεις για δουλειά γραφείου με χρήση τερματικών οπτικής απεικόνισης), περιλαμβάνουν τις απαιτήσεις σχετικά με την προσβασιμότητα, αντιστοίχως για το σχεδιασμό όλων. Αλλά όσον αφορά την εφαρμογή του κανόνα, οι απαιτήσεις αυτές δεν είναι επαρκώς μελετημένες αλλά ούτε και επαρκώς εφαρμοσμένες.

Λόγω νομικού πλαισίου, ιδίως των ΗΠΑ, Αμερικανικές εταιρείες ανέπτυξαν εσωτερικές κατευθυντήριες γραμμές ακολουθώντας το WCAG 1.0 και προσφέρουν λειτουργίες και διεπαφές προγραμματισμού εφαρμογών (Application Programming Interface, API) που κατέστησαν τα προϊόντα τους πιο προσιτά.

Η εξασφάλιση της προσβασιμότητας είναι ένα δύσκολο ζήτημα λόγω της πολυπλοκότητας του θέματος. Ως εκ τούτου είναι αναγκαίο να επικεντρωθούμε στη διαδικασία. Μια καλή μέθοδος είναι ο διάλογος μεταξύ των ατόμων με αναπηρία και η από κοινού ανάπτυξη και διάδοση καινοτόμων προσεγγίσεων. Στην Ευρώπη, το Ευρωπαϊκό Σχέδιο για όλα τα ηλεκτρονικά προσβάσιμα δίκτυα (EdeAN) συντονίζει τις δραστηριότητες των κρατών μελών (www.e-accessibility.org). Αρκετές δραστηριότητες ενημερώνουν το κοινό για τη σημασία του θέματος. Ένα παράδειγμα είναι το BIENE βραβείο που διοργανώθηκε στη Γερμανία (www.biene-award.de). Αυτό το βραβείο απονέμεται για τις περιπτώσεις βέλτιστων πρακτικών προσβάσιμων εφαρμογών του Διαδικτύου σε τομείς του ηλεκτρονικού εμπορίου, της ηλεκτρονικής διακυβέρνησης, των μέσων μαζικής ενημέρωσης, της εκπαίδευσης, της επιστήμης και της έρευνας, καθώς και του πολιτισμού και της κοινωνίας. Η διαδικασία αξιολόγησης περιλαμβάνει τα σύνθετα σχόλια των εμπειρογνωμόνων και τις τελικές δοκιμές των πρακτικών με χρήστες διαφορετικών αναπηριών. Η δημοτικότητα αυτού του καθαρά ιδεώδους βραβείου δείχνει σαφώς ότι η ευαισθητοποίηση έχει αυξηθεί. [27] [28]

2.7. Τρόποι Διευκόλυνσης της πρόσβασης στην πληροφορία

2.7.1. Public Network Access Points - Δημόσια Σημεία Πρόσβασης στο Δίκτυο

Η άνιση πρόσβαση στις τεχνολογίες πληροφόρησης και επικοινωνίας στις μέρες μας ονομάζεται συχνά ψηφιακός διαχωρισμός. Αυτός ο όρος περιγράφει τις ανισότητες στην πρόσβαση στις ΤΠΕ. Μία από τις κύριες στρατηγικές που χρησιμοποιείται για να διαδοθεί η πρόσβαση στις νέες τεχνολογίες είναι η εφαρμογή του δημοσίων σημείων πρόσβασης στο δίκτυο (PNAPs) που παρέχει σε όλους φθηνότερη πρόσβαση κυρίως σε κοινότητες με χαμηλά εισοδήματα. Τα PNAPs μπορεί να οριστούν ως φυσικοί χώροι όπου οι άνθρωποι μπορούν να έχουν πρόσβαση στις ΤΠΕ για προσωπική, εκπαιδευτική, οικονομική, και δημοκρατική ανάπτυξη, χωρίς να χρειάζεται να διατίθενται το απαραίτητο υλικό και λογισμικό. Υπάρχουν τουλάχιστον έξι βασικά μοντέλα της PNAPs, τα οποία διαφέρουν μεταξύ τους σε διάφορες πτυχές. Ωστόσο, πρέπει να θεωρηθούν ως απλώς θεωρητικά καθώς τα PNAPs στην πραγματικότητα συχνά εμφανίζεται ως συνδυασμός των διαφορετικών μοντέλων.

- **Village Information Kiosks**

Τα Village Information Kiosks (περίπτερα πληροφοριών) συχνά επεκτείνονται στα STD / ISD τηλεφωνικά καταστήματα που έχουν ένα ή δύο επιπλέον υπολογιστές συνδεδεμένους στο Internet μέσω σύνδεσης dial-up ή οποιαδήποτε άλλης στενού τύπου σύνδεσης, όπως UHF ή VHF μετάδοσης ραδιοσυχνοτήτων. Πρόσφατα χρησιμοποιείται προηγμένη ασύρματη τεχνολογία (WLL), όπως στην περίπτωση του έργου της SARI.[29] Το περίπτερο του χωριού προσφέρει συνήθως τηλεφωνήματα, σύνδεση στο Internet, υπηρεσίες πληροφόρησης που σχετίζονται με την υγεία, την εκπαίδευση και υπηρεσίες ηλεκτρονικής διακυβέρνησης συμπεριλαμβανομένων και άλλων υπηρεσιών που σχετίζονται με ηλεκτρονικούς υπολογιστές, όπως εφαρμογές επεξεργασίας κειμένου, σάρωση ή εκτύπωση. Όμως, σύμφωνα με τον Colle [30], ο κύριος στόχος αυτών των κέντρων σχετίζεται με την επικοινωνία. Μία από τις πιο ενδιαφέρουσες πτυχές αυτού του μοντέλου είναι ο τρόπος διαχείρισης, καθώς εκτελείται ως επί το πλείστον από ιδιώτες επιχειρηματίες, όπως το πρόγραμμα-SARI, όπου οι τοπικοί επιχειρηματίες, μπορούν να ανοίξουν ένα Village Kiosk (περίπτερο χωριό) με μια επένδυση των 1.000 δολαρίων [31]. Μερικά από τα μεγαλύτερα προβλήματα που μπορούν να εντοπιστούν στο έργο της επίτευξης της βιωσιμότητας, στη δημιουργία ευαισθητοποίησης για τις προσφερόμενες υπηρεσίες, και στη φιλοξενία του χαμηλού μορφωτικού επιπέδου του αγροτικού πληθυσμού. Παρά τα προβλήματα αυτά, το μοντέλο αυτό φαίνεται να είναι τελείως ενδιαφέρον για την εξάπλωση της χρήσης των Τεχνολογιών της Πληροφόρησης και Επικοινωνίας σε αγροτικές περιοχές στις αναπτυσσόμενες χώρες.

v Τηλεκέντρα (Telecenters)

Σύμφωνα με τον Gomez, Hunt και Lamoureux [32], τα τηλεκέντρα είναι ένα από τα πιο συνηθισμένα μοντέλα PNAP που εφαρμόζονται σε αναπτυσσόμενες χώρες. Συνήθως είναι εξοπλισμένα με από πέντε έως οκτώ υπολογιστές, χρησιμοποιούν μια ευρείας ζώνης σύνδεση, και προσφέρουν πιο προηγμένες υπηρεσίες από τα περίπτερα πληροφοριών (village information kiosks). Υπάρχουν παραδείγματα τηλεκέντρων που διοικούνται από ιδιώτες επιχειρηματίες, αλλά κυρίως εφαρμόζονται και διοικούνται από μη κυβερνητικούς οργανισμούς (NGO), καθώς το αρχικό και λειτουργικό κόστος είναι υπερβολικά υψηλό για τις ιδιωτικές επιχειρηματίες στις αναπτυσσόμενες χώρες. Τα τηλεκέντρα επίσης μπορούν να εντοπιστούν και στις ανεπτυγμένες χώρες, όπου συχνά είναι μέρος μιας στρατηγικής περιφερειακής ανάπτυξης. Ένα από τα κύρια καθήκοντα των τηλεκέντρων είναι η ανάπτυξη των δεξιοτήτων, ειδικά στις ανεπτυγμένες χώρες, τα κέντρα αυτά συχνά χρησιμοποιούνται για την υποστήριξη των ανθρώπων όσον αφορά την απόκτηση δεξιοτήτων σχετιζόμενες με τους ηλεκτρονικούς υπολογιστές, οι οποίες τους επιτρέπουν να κάνουν αναζητήσεις εργασίας μέσω διαδικτύου και την προετοιμασία όλων των απαραίτητων έγγραφων που χρειάζεται κάποιος για να αναζητήσει εργασία. [33]

v Πολλαπλών χρήσεων κοινοτικά τηλεκέντρα (Multipurpose Community Telecenters)

Το μοντέλο κοινοτικών τηλεκέντρων πολλαπλών χρήσεων αποτελείται από 10 έως 20 υπολογιστές. Προσφέρει περισσότερα από τη βασική πρόσβαση στο Διαδίκτυο και συχνά επικεντρώνεται κυρίως στα εκπαιδευτικά θέματα και την ανάπτυξη της κοινότητας. Είναι εξοπλισμένο με την τελευταία λέξη της τεχνολογίας και προσφέρει τις καλύτερες εφαρμογές που κυκλοφορούν στην αγορά, όπως η τηλεδιάσκεψη, η ηλεκτρονική διακυβέρνηση και η τηλεϊατρική στις αγροτικές περιοχές. Με πολλούς τρόπους, αυτό το μοντέλο είναι παρόμοιο με τα τηλεκέντρα. Η βασική διάκριση είναι το μέγεθός του και οι υπηρεσίες που προσφέρει. Λόγω του μεγέθους της και την ποικιλία των υπηρεσιών που προσφέρει, τα κοινοτικά τηλεκέντρα πολλαπλών χρήσεων εφαρμόζονται και διοικούνται μόνο από μη κυβερνητικούς οργανισμούς ή τις κυβερνήσεις. Αυτά τα κέντρα συχνά δεν αποσκοπούν μόνο στο να κάνουν δυνατή την πρόσβαση και την κατάρτιση, αλλά συχνά αποτελούν μέρος της ευρύτερης αναπτυξιακής στρατηγικής της κοινότητας. Παρόλο που το μοντέλο αυτό έχει γίνει αρκετά κοινό στον ανεπτυγμένο κόσμο, ειδικά στις αστικές περιοχές, φαίνεται ότι είναι μεγάλο σε μέγεθος και πολύ ακριβό για να εργαστεί αποτελεσματικά στις αναπτυσσόμενες χώρες.

v Δημοτικά Κέντρα Πρόσβασης (Civic Access Centers)

Βασισμένο σε σχολεία, πανεπιστήμια, βιβλιοθήκες, ταχυδρομεία, ή άλλα δημόσια κτίρια, τα δημοτικά κέντρα πρόσβασης συχνά προσφέρουν στο ευρύ κοινό πρόσβαση σε υπολογιστές και δικτυακές συνδέσεις, όπως ακριβώς μερικά σχολεία ή πανεπιστήμια προσφέρουν στο ευρύ κοινό πρόσβαση στον εξοπλισμό τους σε συγκεκριμένες ώρες [34]. Στις περισσότερες ανεπτυγμένες χώρες, όπως οι Ηνωμένες Πολιτείες, η Γερμανία, η Ιαπωνία και η Αυστραλία, οι βιβλιοθήκες προσφέρουν στους πελάτες τους δωρεάν πρόσβαση στο Internet ως πρόσθετη υπηρεσία. Αυτά τα κέντρα συνήθως

δεν δημοσιοποιούν τις υπηρεσίες τους πολύ ανοιχτά ούτε εστιάζουν στην κατάρτιση ή την εκπαίδευση [35]. Ωστόσο, σε ορισμένες περιοχές του κόσμου και για ορισμένες ομάδες, ειδικά στον αναπτυγμένο κόσμο, τα κέντρα αυτά φαίνεται να είναι ένα σημαντικό σημείο πρόσβασης, καθώς η πρόσβαση στο σπίτι ή σε άλλους δημόσιους χώρους μπορεί να μην είναι διαθέσιμη [36][37]. Τα δημοτικά κέντρα πρόσβασης μπορεί να θεωρηθούν ως μια απαραίτητη κυβερνητική υπηρεσία για το ευρύ κοινό, δεδομένου ότι οι πολίτες έχουν το δικαίωμα στην πρόσβαση στην πληροφορία και τις νέες υπηρεσίες και τα κέντρα αυτά μπορούν να μετατραπούν στον πιο βασικό τρόπο για να εξασφαλιστεί ότι τα άτομα τουλάχιστον έχουν τη δυνατότητα να έχουν πρόσβαση σε αυτά.

v Ίντερνετ καφέ (Cyber Cafes)

Τα Ίντερνετ καφέ είναι εμπορικά, καθοδηγούμενα από την αγορά φαινόμενα που εμφανίστηκαν στις αρχές της δεκαετίας του 1990 με τη διάχυση του Internet στις περισσότερες αστικές πόλεις των ανεπτυγμένων χωρών, ιδιαίτερα στις ΗΠΑ. Σύμφωνα με τον Stewart [38] δεν θα πρέπει να αντιμετωπίζονται μόνο ως ένα επιπλέον σημείο πρόσβασης για το Internet, αλλά μάλλον ως ένα νέο δημόσιο χώρο και μέρος της προσωρινής κουλτούρας. Έχουν διαδραματίσει σημαντικό ρόλο στην διάδοση της γνώσης σχετικά με το Διαδίκτυο και έχουν υπηρετήσει ως ένα σημείο πρόσβασης για συγκεκριμένες κοινότητες (π.χ. φοιτητές) κατά τις πρώτες ημέρες του Διαδικτύου, αλλά σήμερα, με τη διάδοση της πρόσβασης στο Διαδίκτυο στο σπίτι στις ανεπτυγμένες χώρες, η σημαντικότητα τους έχει μειωθεί σημαντικά. Ωστόσο, η κατάσταση είναι εντελώς διαφορετική στις αναπτυσσόμενες χώρες, όπου έχουν εμφανιστεί σχεδόν παντού. Τα Ίντερνετ καφέ στις αναπτυσσόμενες χώρες, ιδιαίτερα στις αστικές περιοχές, ξεφυτρώνουν και να υπηρετούν ένα σημαντικό μέρος της κοινωνίας.

v Κινητές Λύσεις Πρόσβασης (Mobile Access Solutions)

Υπάρχουν διάφορα άλλα έργα, όπου τα σημεία πρόσβασης είναι κινητά, προκειμένου να φτάσουν σε μακρινές αγροτικές κοινότητες, όπως το Internet στο έργο Wheels στη Μαλαισία, όπου ένα λεωφορείο εξοπλισμένο με σύγχρονες τεχνολογίες φέρνουν το Internet σε απομακρυσμένες περιοχές, χρησιμοποιώντας μια δορυφορική σύνδεση. Υπάρχουν και άλλα παρόμοια έργα, για παράδειγμα, στην Ινδία και τη Νότια Αμερική. Όλα αυτά τα έργα έχουν μια κινητή μονάδα που προσωρινά φέρνει την τεχνολογία του δικτύου σε απομακρυσμένες και άσχετα αγροτικές περιοχές. Αλλά η σημαντική λέξη είναι «προσωρινή». Προσωρινή σημαίνει ότι η εγκατάσταση θα είναι διαθέσιμη για τις αγροτικές κοινότητες μόνο για ένα μικρό χρονικό διάστημα και μόνο περιστασιακά. Τα σχέδια αυτά μπορεί να είναι πολύ χρήσιμα για τη δημιουργία της ευαισθητοποίησης για τις νέες τεχνολογίες, αλλά δεν μπορούν να θεωρηθούν ως μακροπρόθεσμες λύσεις.

Τα προηγούμενα παραδείγματα δίνουν μια ιδέα των διάφορων πιθανών μοντέλων. Αλλά παρ 'όλες αυτές τις διαφορές, τα Δημόσια Σημεία Πρόσβασης Στο Δίκτυο (PNAPs) έχουν ορισμένα κοινά χαρακτηριστικά:

- θα προσφέρουν πρόσβαση στο δίκτυο σε ανθρώπους που δεν μπορούν να αντέξουν οικονομικά να έχουν το απαραίτητο υλικό και το λογισμικό στο σπίτι,

- οι οποίοι δεν μπορούν να πληρώσουν τη μηνιαία τέλη σύνδεσης,
- ή που χρειάζονται υποστήριξη για να χρησιμοποιήσουν τις νέες τεχνολογίες.

Υπάρχουν σημαντικές διαφορές μεταξύ των Δημοσίων Σημείων Πρόσβασης Στο Δίκτυο (PNAPs) στις αναπτυσσόμενες και αναπτυγμένες χώρες, καθώς και μεταξύ αστικών και αγροτικών περιοχών στο εσωτερικό μιας χώρας. Σε γενικές γραμμές, τα Δημόσια Σημεία Πρόσβασης Στο Δίκτυο (PNAPs) παίζουν πολύ μεγαλύτερο ρόλο στις αναπτυσσόμενες χώρες, όπου δεν είναι απλώς ένα πρόσθετο σημείο πρόσβασης, αλλά συχνά το μόνο σημείο πρόσβασης με το οποίο μπορεί να καταστεί η πρόσβαση στις Τεχνολογίες Πληροφοριών και Επικοινωνίας δυνατή. [39]

Κεφάλαιο 3
Ζητήματα Ασφάλειας

Στο 3^{ο} κεφάλαιο θα αναλυθούν κάποια από τα ζητήματα ασφαλείας τα οποία προκύπτουν από την εφαρμογή της Ηλεκτρονικής Διακυβέρνησης όπως η προστασία των προσωπικών δεδομένων των πολιτών, η κακόβουλες ενέργειες με τη χρήση κακόβουλων λογισμικών και εν τέλει θα αναφερθούν τρόποι με τους οποίους κατορθώνεται να διασφαλιστούν τα προσωπικά δεδομένα άλλα και οι ηλεκτρονικές συναλλαγές.

3.1. Γενικά

Πριν από την έλευση των τεχνολογιών πληροφόρησης και επικοινωνίας, η επικοινωνία μεταξύ των ανθρώπων ήταν κυρίως λεκτική και άμεση [40]. Σήμερα, χρησιμοποιούμε όλο και περισσότερο τους υπολογιστές για να επικοινωνούμε. Με τη μεσολάβηση ενός υπολογιστή, η πληροφορία ταξιδεύει πολύ γρήγορα και σε σχεδόν απεριόριστο αριθμό αποδεκτών, καθώς και αβίαστα [41].[42] Ένα από τα βασικά χαρακτηριστικά της ηλεκτρονικής διακυβέρνησης είναι η διαβίβαση εμπιστευτικών πληροφοριών μέσω δικτύων πληροφορικής. Ανάλογα με την ευαισθησία των πληροφοριών, η ασφάλεια κάποιων πληροφοριών θα πρέπει να αντιμετωπίζονται στο ίδιο επίπεδο με την εθνική ασφάλεια. Αν και κάθε ηλεκτρονική διακυβέρνηση έχει τα δικά της δίκτυα, καμία κυβέρνηση δεν μπορεί να πει όχι στο διαδίκτυο, διότι αυτό θα ήταν μια σπατάλη των πόρων. Ωστόσο, το διαδίκτυο είναι ένα ανοικτό περιβάλλον κι ως εκ τούτου, το να προστατευτούν τα δεδομένα που ρέουν στο διαδίκτυο από τις επιθέσεις είναι ένα καταπιεστικό για την ηλεκτρονική κυβέρνηση θέμα.[43] Επιπλέον σε έρευνα, που ανατέθηκε από την Εταιρεία American Express, τυχαία ρωτήθηκαν 11.410 άτομα σε 10 χώρες, διαπιστώθηκε ότι σχεδόν μισοί από τους ερωτηθέντες κάνουν χρήση κάποιας υπηρεσίας του Διαδικτύου. Όπως ήταν αναμενόμενο, οι περισσότεροι χρήστες του Internet στον κόσμο χρησιμοποιούν το Διαδίκτυο για το ηλεκτρονικό ταχυδρομείο, την περιήγηση και τη ψυχαγωγία. Ωστόσο, λιγότερο από το 28% πραγματοποιεί αγορές μέσω Διαδικτύου, και 24% χρησιμοποιούν το Διαδίκτυο για τραπεζικές και άλλες οικονομικές συναλλαγές. Αλλά όταν χρήστες του Διαδικτύου και μη χρήστες από πολλές χώρες ρωτήθηκαν αν συμφωνούν με τη δήλωση, "*ανησυχώ ή θα έπρεπε να ανησυχώ για την ασφάλεια και τα ζητήματα προστασίας της ιδιωτικής ζωής κατά την αγορά ή τη διάθεση χρηματοδοτικών συναλλαγών μέσω Διαδικτύου*" το 79% συμφώνησε. Πριν από την τραγωδία της 11 Σεπτεμβρίου του 2001, οι πολίτες των ΗΠΑ, σε ποσοστό 85%, εξέφρασαν ανησυχίες προς τα ζητήματα της ιδιωτικής ζωής και της ασφάλειας. Στη δημοσκόπηση που διεξήχθηκε από το Information Technology Association of America, φαίνεται ότι περίπου το 80% έχει αμφιβολίες για την ικανότητα της κυβέρνησης των ΗΠΑ να διασφαλίσει την ασφάλεια των υπολογιστών και την προστασία της ιδιωτικής ζωής. Ως εκ τούτου, η προστασία των

λειτουργικών συστημάτων είναι μια μείζονος σημασίας στρατηγική, εάν η ηλεκτρονική διακυβέρνηση ως σύνολο επιτύχει τις δυνατότητές της. [44]

Οι βασικές αρχές της ασφάλειας των πληροφοριακών συστημάτων και ως εκ τούτου και απαραίτητες προϋποθέσεις για την επιτυχία της ηλεκτρονικής διακυβέρνησης όσον αφορά την ασφάλεια είναι:

- **Ακεραιότητα.** Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.
- **Διαθεσιμότητα.** Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.
- **Εμπιστευτικότητα.** Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

3.2. Κατηγορίες απειλών των συστημάτων της ηλεκτρονικής διακυβέρνησης

Οι διαταραχές των υπηρεσιών ηλεκτρονικής διακυβέρνησης μπορούν να χωριστούν σε δύο κατηγορίες

- *διαταραχές στον κυβερνοχώρο* και
- διαταραχές των *υποδομών ζωτικής σημασίας*

Οι *διαταραχές στον κυβερνοχώρο* περιλαμβάνουν κυβερνο-τρομοκρατία (*cyberterrorism)*, όπως τα Nimda και Code Red σκουλίκια καθώς και εχθροπραξίες πληροφοριών. Πιθανά *"info weapons"* που μπορούν να χρησιμοποιηθούν για να ξεκινήσει μια επίθεση σε μια ηλεκτρονική διακυβέρνηση περιλαμβάνουν ιούς υπολογιστών, λογικές βόμβες, σκουλίκια, δούρειους ίππους, κ.ά. [45 [46] [47]. Διάφορες επιθέσεις σε συστήματα περιλαμβάνουν άρνηση των υπηρεσιών, εικονική κατάληψη και αποκλεισμούς, rootkits (λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών), κ.α.[48]. Οι επιθέσεις με τη χρήση αυτών των κακόβουλων εργαλείων κυμαίνονται από απλές επιθέσεις ακτιβισμού(η χρήση υπολογιστών και δικτύων ως μέσα διαμαρτυρίας για την προώθηση πολιτικών σκοπών), η οποία αναφέρεται σε ενεργές δραστηριότητες hacking με την πρόθεση να διαταράξουν κανονικές συνθήκες λειτουργίας, αλλά δεν προκαλούν σοβαρές ζημιές, μέχρι και την πιο καταστροφική κυβερνο-τρομοκρατία και τις εχθροπραξίες πληροφοριών [49] [50], οι οποίες αυξάνουν την ανησυχία μετά την 9/11. Οι information warfare αναφέρονται στις μεγάλης κλίμακας κακόβουλες δραστηριότητες που ξεκίνησαν από ανεξάρτητα άτομα ή άτομα που μισθώνονται από επιτιθέμενους τρομοκράτες ή

άτομα που ανήκουν σε ανταγωνίστριες χώρες. Η κυβερνο-τρομοκρατία είναι μια πιο επικίνδυνη μορφή των κυβερνο-διαταραχών, η οποία μπορεί να προκαλέσει σοβαρή βλάβη στα συστήματα του έθνους [51]. Ακόμη και μιας ώρας διάρκειας συντονισμένη δραστηριότητα πειρατείας, η οποία επηρεάζει το σύστημα εναέριας κυκλοφορίας της χώρας, η οποία αποτελεί μια από τις πιο κρίσιμες υποδομές, μπορεί να έχει πολύ δραστικές συνέπειες για τις λειτουργίες του δημοσίου. Σε λίγα χρόνια, οι κυβερνο-απειλές αναμένεται να είναι χειρότερες ακόμα και από την σωματική απειλή[52]. Όσον αφορά την Ελλάδα χαρακτηριστικά παραδείγματα κυβερνο-τρομοκρατίας αποτελούν οι πρόσφατες επιθέσεις σε κυβερνητικές ιστοσελίδες, τον Φεβρουάριο του 2012, όπως στη σελίδα του Υπουργείου Δικαιοσύνης, του Υπουργείου Προστασίας του Πολίτη, της Ελληνικής Αστυνομίας, του Πρωθυπουργού, της Βουλής των Ελλήνων καθώς και πολιτικών προσώπων και κομμάτων, οι οποίες δεν προκάλεσαν σοβαρές ζημίες αλλά είχαν σαν στόχο κυρίως την διαμαρτυρία.

Ως Διαταραχές υποδομών ζωτικής σημασίας θα μπορούσαν να θεωρηθούν μια κακόβουλη επίθεση, ένα ατύχημα, ή μια καταστροφή που προκαλεί κρίσιμες δυσλειτουργίες στις υποδομές, οι οποίες αποτελούν πλέον εθνικό ενδιαφέρον. Η προστασία των κρίσιμων υποδομών είναι ένα σημαντικό θέμα, γιατί οποιαδήποτε διαταραχή στη λειτουργία τους θα μπορούσε να προκαλέσει σε εθνικό επίπεδο το χάος, για παράδειγμα, η συσκότιση στις Ηνωμένες Πολιτείες και τον Καναδά, μια διακοπή ρεύματος στις βορειανατολικές περιοχές των Ηνωμένων Πολιτειών και τον Καναδά το 2003, που είχε ως συνέπεια πολλά εξαρτώμενα από τα ηλεκτρικά δίκτυα συστήματα να αποτύχουν παταγωδώς. Η ζημία υπολογίζεται σε περίπου 5 δις Αμερικάνικα δολάρια [53]. [54]

3.3. Κακόβουλο λογισμικό

3.3.1. Ορισμός

Ο όρος «κακόβουλο λογισμικό» (malicious software) η οποία έχει καθιερωθεί, δεν είναι απολύτως δόκιμη. Οι λόγοι είναι οι εξής:

- το λογισμικό, είναι μία άψυχη οντότητα, και ως εκ τούτου δεν έχει βούληση, συνεπώς δεν θα έπρεπε να αναφερόμαστε σε κακόβουλο λογισμικό.
- Ο χαρακτηρισμός «κακόβουλο» δεν είναι δυνατόν να αναφέρεται στους ενδεχομένως δόλιους σκοπούς του προγραμματιστή ή του χρήστη ενός λογισμικού, καθώς δεν είναι ο σκοπός του χρήστη ή του προγραμματιστή που μας οδηγούν στην ονομασία ενός λογισμικού, αφού ένα τμήμα λογισμικού μπορεί να είναι επιβλαβές για ένα υπολογιστικό σύστημα, χωρίς απαραιτήτως να αποτελεί σκοπό του προγραμματιστή ή του χρήστη.

Συνεπώς πιο σωστά ως κακόβουλο λογισμικό ορίζεται ***το λογισμικό που περιέχει τις απαιτούμενες εντολές για μια επίθεση σε ένα υπολογιστικό σύστημα.***

> Επίθεση σε ένα υπολογιστικό σύστημα ή απόπειρα επίθεσης, είναι η παραβίαση ή η απόπειρα παραβίασης της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας του συστήματος. [55]

3.3.2. Κατηγοριοποίηση Κακόβουλου Λογισμικού

Οι δύο πιο σημαντικές ιδιότητες του κακόβουλου λογισμικού είναι η αυτονομία και η αναπαραγωγή και βάσει αυτών κατηγοριοποιείται.

- **Αυτονομία** είναι η δυνατότητα του κακόβουλου λογισμικού να λειτουργεί χωρίς να χρειάζεται να προσκολληθεί σε ένα λογισμικό-ξενιστή (host).
- **Αναπαραγωγή** είναι η δυνατότητα του κακόβουλου λογισμικού να αναπαράγεται από μόνο του όταν το επιτρέπουν οι συνθήκες, για παράδειγμα λόγω χαλαρών μέτρων ασφαλείας, εύρεση ξενιστή κ.ά.

  Έτσι το κακόβουλο λογισμικό διαχωρίζεται σε αυτό που χρειάζεται ξενιστή και σε αυτό που δεν χρειάζεται ξενιστή. [56]

3.3.3. Είδη Κακόβουλου Λογισμικού

Το κακόβουλο λογισμικό διακρίνεται σε δύο είδη:

- Ιομορφικό λογισμικό
- Μη Ιομορφικό λογισμικό

3.3.3.1. Ιομορφικό Λογισμικό

Το ***Ιομορφικό*** είναι ένα λογισμικό το οποίο ενσωματώνει τον κώδικα του σε ένα άλλο πρόγραμμα ξενιστή , αναπαράγεται με αντιγραφή του εαυτού του σε άλλα προγράμματα ξενιστές και εκτελείται στο παρασκήνιο. Τα στάδια ζωής ενός τέτοιου ιού περιλαμβάνει τα παρακάτω στάδια:

- *Φάση επώασης*. Στο στάδιο αυτό ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα και ενεργοποιείται από κάποιο γεγονός όπως η έλευση συγκεκριμένης χρονικής στιγμής, η παρουσία κάποιου αρχείου κ.ά.

- *Φάση αναπαραγωγής*. Η αναπαραγωγή είναι ένα από τα ιδιαίτερα χαρακτηριστικά των ιών, σε αντίθεση με άλλες κατηγορίες κακόβολου λογισμικού. Στη φάση αναπαραγωγής ο ιός δημιουργεί ένα αντίγραφο του εαυτού του και το ενσωματώνει σε προγράμματα ξενιστές.

- *Φάση ενεργοποίησης και εκτέλεσης*. Κατά τη φάση αυτή ο ιός εκτελεί μια σειρά ενεργειών, οι οποίες μπορεί να έχουν επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που το φιλοξενεί. Οι ενέργειες ποικίλουν, από την εμφάνιση απλών μηνυμάτων μέχρι και καταστροφικές ενέργειες όπως είναι η διαγραφή δεδομένων από τον σκληρό δίσκο.

Επίσης ο ιός αποτελείται από τουλάχιστον δύο υπορουτίνες:

- ***Υπορουτίνα αναζήτησης*** κατά την οποία αναζητά νέους ξενιστές στην περιοχή αποθήκευσης και δικτύου, όπου έχει πρόσβαση ο ξενιστής του ιού.

- ***Υπορουτίνα αντιγραφής*** κατά την οποία δημιουργεί ένα αντίγραφο του εαυτού του και το ενσωματώνει στον ξενιστή (αναπαραγωγή).

Τέτοια Ιομορφικά λογισμικά αποτελούν :

- **Οι Ιοί Τομέα Εκκίνησης**

Οι οποίοι εγκαθίστανται στο τμήμα εκείνο του δίσκου το οποίο χρησιμοποιείται για την εκκίνηση του λειτουργικού συστήματος.

- **Παρασιτικοί Ιοί**

Ένας παρασιτικός ιός προσαρτάται σε ένα εκτελέσιμο πρόγραμμα και μολύνει και άλλα προγράμματα.

- **Πολυμερείς Ιοί (Multipartite Viruses)**

Αυτοί οι ιοί μπορούν να μολύνουν είτε εκτελέσιμα αρχεία, είτε τομείς εκκίνησης.

- **Διαμένοντες στην Κύρια Μνήμη**

Αυτοί οι Ιοί παραμένουν ενεργοί και μετά το πέρας της εκτέλεσης του ξενιστή τους. Ο ξενιστής μπορεί να είναι είτε ένα εκτελέσιμο πρόγραμμα είτε ένας τομέας εκκίνησης δίσκου. Μετά το πέρας της εκτέλεσης του ξενιστή οι Διαμένοντες στην Κύρια Μνήμη Ιοί αποκολλώνται από τον ξενιστή και τοποθετούνται στην Κύρια Μνήμη όπου και παραμένουν μέχρι και τον τερματισμό του συστήματος.

- **Κρυφοί Ιοί (Stealth Viruses)**

Οι Ιοί αυτοί αποκρύπτουν τη μόλυνση των αρχείων από τα αντιβιοτικά προγράμματα. Όταν ζητηθούν από το σύστημα οι ιδιότητες ή το περιεχόμενου ενός αρχείου το οποίο έχει προσβληθεί από Κρυφό Ιό τότε Ο Κρυφός Ιός αποστέλλει τις ιδιότητες ή τα δεδομένα του αρχείου πριν αυτό μολυνθεί.

- **Κρυπτογραφημένοι Ιοί**

Αυτοί οι κρυπτογραφημένοι Ιοί (Encrypted Viruses) αποφεύγουν την ανίχνευση από τα αντιβιοτικά προγράμματα κρυπτογραφώντας το μεγαλύτερο τμήμα του Ιού αφήνοντας σε μη κρυπτογραφημένη μορφή μόνο μια απλή ρουτίνα αποκρυπτογράφησης και ένα τυχαίο κλειδί κρυπτογράφησης.

- **Πολυμορφικοί Ιοί**

ι Πολυμορφικοί Ιοί αποτελούν μια εξέλιξη των Κρυπτογραφημένων Ιών. Οι Πολυμορφικοί Ιοί είναι αυτοί που μεταβάλλουν την μορφή τους κάθε φορά που προσβάλουν ένα αρχείο.

- **Ρετρό-Ιοί**

Πρόκειται για Ιούς που προσπαθούν να εντοπίσουν την ύπαρξη αντιβιοτικών προγραμμάτων και να τα καταστήσουν αναποτελεσματικά.

- **Ιοί που διαγράφουν τμήμα του ξενιστή (Overwriters)**

Οι περισσότεροι Ιοί διατηρούν την λειτουργικότητα των εκτελέσιμων ξενιστών ώστε να μη γίνονται ανιχνεύσιμοι. Έτσι οι Ιοί που διαγράφουν τμήμα ή και όλα τα περιεχόμενα του ξενιστή είναι ιδιαίτερα ανιχνεύσιμοι από το αντιβιοτικό λογισμικό.

- **Μακρό-Ιοί**

Οι Ιοί αυτοί δεν προσβάλλουν εκτελέσιμα αρχεία αλλά μάκρο-εντολές. Αυτοί οι Ιοί είναι πιο συνήθεις από όλους τους άλλους λόγω της διευρυμένης χρήσης των προγραμμάτων που χρησιμοποιούν μάκρο-εντολές, όπως για παράδειγμα το Microsoft Word, κ.ά. [57]

3.3.3.2. Μη Ιομορφικό Λογισμικό

- **Κερκόπορτες(Trapdoors ή Backdoors).**

Οι κερκόπορτες είναι σημεία εισόδου που επιτρέπουν την πρόσβαση στο σύστημα, παρακάμπτοντας την συνηθισμένη διαδικασία ασφαλείας.

- **Λογικές Βόμβες(Logic Bombs)**

Οι λογικές βόμβες είναι προγράμματα που εκτελούν μια ενέργεια που παραβιάζει την πολιτική ασφάλειας του συστήματος όταν πληρείται κάποια λογική συνθήκη. Παρόμοιες είναι και οι χρονικές βόμβες οι οποίες παραβιάζουν την πολιτική ασφάλειας σε συγκεκριμένη χρονική στιγμή.

- **Δούρειοι Ίπποι**

Οι Δούρειοι Ίπποι είναι φαινομενικά χρήσιμα προγράμματα που περιλαμβάνουν κρυφές λειτουργίες οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το

πρόγραμμα, με συνέπεια μια απειλή στη ασφάλεια. Οι Δούρειοι Ίπποι δεν αναπαράγονται μόνοι τους. Πρέπει να βασιστούν στους ίδιους τους χρήστες για την εγκατάσταση και την εκτέλεση τους.

- **Αναπαραγωγοί**

Οι Αναπαραγωγοί (worms) είναι προγράμματα που μεταδίδονται από έναν υπολογιστή σε έναν άλλο δημιουργώντας αντίγραφα του εαυτού τους. Σε αντίθεση με τους Ιούς δεν απαιτούν ξενιστή άλλα δημιουργούν αντίγραφα τα οποία στέλνουν σε άλλα μηχανήματα μέσω δικτύου.

- **Βακτήρια (Bacteria)**

Τα βακτήρια αναπαράγονται όπως οι Ιοί και δεν απαιτούν την ύπαρξη ξενιστή. Τα βακτήρια δεν αλλοιώνουν δεδομένα σκόπιμα, μοναδικό στόχο έχουν την αναπαραγωγή όσο το δυνατόν περισσότερων αντιγράφων. Επίσης καταναλώνουν έναν ή περισσότερους πόρους του συστήματος σε μεγάλο βαθμό. Έτσι τα βακτήρια παρόλο που δεν πλήττουν την ακεραιότητα του συστήματος, προσβάλλουν την διαθεσιμότητά του.

- **Παραπλανητική πληροφόρηση**

παράδειγμα αποτελεί ο «ιός» Good Times, το 1994. Τέτοιος Ιός δεν υπήρξε ποτέ, αλλά η φήμη της ύπαρξης του επέφερε μείωση της διαθεσιμότητας των πληροφοριακών συστημάτων σε παγκόσμιο επίπεδο.[58]

3.4. Ζητήματα Διαχείρισης Ιδιωτικότητας και Ταυτότητας στην Ηλεκτρονική Κυβέρνηση

Μια ηλεκτρονική κυβέρνηση παρέχει στους πολίτες υπηρεσίες οι οποίες έχουν να κάνουν με την επεξεργασία και των προσωπικών τους πληροφοριών. Με τον αυξανόμενο αριθμό των αποθηκευμένων προσωπικών πληροφοριών σε ψηφιακή μορφή (κείμενο, εικόνα, ήχο και βίντεο), όλο και περισσότερο ψυχοκοινωνικοί προβληματισμοί μπορούν να εντοπιστούν. Τα τρωτά σημεία του απορρήτου προκύπτουν ακόμη και αν τα δεδομένα είναι διαθέσιμα σε στατιστικές ή υπερβολικές μορφές, ή που επιτρέπουν προσωπικές πληροφορίες να συνάγονται. Επιπλέον, το γεγονός ότι η κυβέρνηση μπορεί να παρακολουθεί προσεκτικά κάθε συναλλαγή και πρόσβαση σε πόρους που γίνεται από πολίτες μπορεί να αποθαρρύνει τη συμμετοχή των πολιτών, επηρεάζοντας έτσι την επιτυχή ανάπτυξη των συστημάτων ηλεκτρονικής διακυβέρνησης. Σε σύγκριση με το γενικό περιβάλλον του ηλεκτρονικού εμπορίου, τα συστήματα ηλεκτρονικής δημόσιας διοίκησης έχουν αυξημένη υποχρέωση / ευθύνη για τη διατήρηση της ιδιωτικότητας των πολιτών. [59]

3.4.1. Προκλήσεις

Αρκετές προκλήσεις σχετικές με την προστασία της ιδιωτικής ζωής και τη διαχείριση ταυτότητας υπάρχουν που πρέπει να αντιμετωπιστούν για να εξασφαλιστεί η επιτυχία ενός περιβάλλοντος ηλεκτρονικής διακυβέρνησης.

Προδιαγραφές Πολιτικής Προστασίας Προσωπικών Δεδομένων

Η ανάπτυξη ενός ολοκληρωμένου πλαισίου πολιτικής για τις προδιαγραφές προστασίας της ιδιωτικής ζωής αποτελεί μια σημαντική πρόκληση. Υπάρχει ανάγκη για εκφραστικές προδιαγραφές πολιτικής προστασίας προσωπικών δεδομένων και για την εκτέλεση του πλαισίου που να υποστηρίζει ευέλικτες προδιαγραφές πολιτικής, και διευκολύνει τον έλεγχο και την παρακολούθηση, ενώ διατηρεί της επεκτασιμότητα καθώς και την σχέση κόστους-αποτελεσματικότητας. Ειδικότερα, οι προτιμήσεις της ιδιωτικής ζωής των χρηστών θα μπορούσε να ποικίλει, και θα μπορούσε να εξαρτάται από το πλαίσιο και το σκοπό της χρήση των προσωπικών πληροφοριών. Σε γενικές γραμμές, η φυσική γλώσσα βασισμένη στις προδιαγραφές, θα ήταν εξαιρετικά επιθυμητή, αλλά θα μπορούσε να δημιουργήσει σοβαρά προβλήματα στην δυνατότητα ανάγνωσης του μηχανήματος, και να προκαλέσει δυσκολία στην αφαίρεση της ασάφειας και στη συνέπεια των πολιτικών. Τυπικές, εκφραστικές γλώσσες είναι αναγκαίες και θα πρέπει να αυξηθούν με επεκτάσιμα ακριβή εργαλεία αξιολόγησης για τη διευκόλυνση της κατάλληλης διοίκησης και την εφαρμογή των πολιτικών προστασίας της ιδιωτικής ζωής. [60]

Ενεργό Περιεχόμενο

Μία πρόκληση απορρήτου εισάγεται από τεχνολογίες του Διαδικτύου όπως προγράμματα περιήγησης στο Web, των οποίων οι αδυναμίες μπορούν να αξιοποιηθούν για την παραβίαση της ιδιωτικής ζωής. Για παράδειγμα, τα cookies, τα δεδομένα που είναι αποθηκευμένα στον υπολογιστή του πελάτη και αντάλλαξαν πληροφορίες μεταξύ των πελατών και του διακομιστή για να διατηρήσουν τη σύνδεσή, μπορούν να χρησιμοποιηθούν με σκοπό τη συγκέντρωση των πληροφοριών του χρήστη. Η χρήση του εκτελέσιμου περιεχομένου όπως Java και στοιχεία ελέγχου ActiveX είναι μια άλλη πηγή τρωτών σημείων της ασφάλειας, που θα μπορούσαν να χρησιμοποιηθούν για την απόκτηση προσωπικών πληροφοριών. Εργαλεία και τεχνικές για να εξασφαλίζουν ότι το ενεργό περιεχόμενο δεν παραβιάζει τις απαιτήσεις της προστασίας της ιδιωτικής ζωής των χρηστών είναι ζωτικής σημασίας. [61]

Περιβάλλον πολλών τομέων

Δύο χαρακτηριστικά των υπηρεσιών ηλεκτρονικής διακυβέρνησης που επιδεινώνουν την ιδιωτική ζωή και τα προβλήματα διαχείρισης ταυτοτήτων είναι:

1. η κατανομή των πληροφοριών των πολιτών μεταξύ των διαφόρων κυβερνητικών οργανισμών και

2. οι διαφορετικές προτιμήσεις ιδιωτικότητας των πολιτών, ετερογενείς απαιτήσεις προστασίας της ιδιωτικής ζωής των διαφόρων υποτομέων της ηλεκτρονικής διακυβέρνησης, και η πιθανή χρήση των ταυτοτήτων για την πρόσβαση σε διάφορα υπό-συστήματα ηλεκτρονικής διακυβέρνησης.

Ενώ η διευκόλυνση των υπηρεσιών προς τους πολίτες, οι τομείς της ηλεκτρονικής διακυβέρνησης μπορεί να χρειαστεί να ανταλλάξουν πληροφορίες των χρηστών, συμπεριλαμβανομένων των ταυτοτήτων τους και των διαπιστευτηρίων τους. Επιπλέον, οι πολιτικές προστασίας προσωπικών δεδομένων των τομέων μπορεί να χρειαστεί να ενσωματωθούν για να παρέχουν διαφάνεια της υφιστάμενης ιδιωτικής ζωής διαφυλάσσοντας τις πληροφορίες που μοιράζονται. Διαφορετικές απαιτήσεις προστασίας της ιδιωτικής ζωής των πολιτών πρέπει να αντιμετωπιστούν από την υποδομή της ηλεκτρονικής διακυβέρνησης για να διασφαλιστεί ότι όλοι οι πολίτες αισθάνονται ασφαλείς να αλληλεπιδρούν με τα συστήματα ηλεκτρονικής δημόσιας διοίκησης. Περαιτέρω πρόκληση είναι να διευκολυνθεί στους άγνωστους χρήστες η αλληλεπίδραση τους με τα συστήματα ηλεκτρονικής διακυβέρνησης που εγείρουν ζητήματα εμπιστοσύνης που σχετίζονται με τις απαιτήσεις προστασίας της ιδιωτικής ζωής. Η δυνατότητα για τη δημιουργία εμπιστοσύνης μεταξύ συστημάτων της ηλεκτρονικής διακυβέρνησης και των χρηστών χωρίς την άσκοπη αποκάλυψη ευαίσθητων πληροφοριών είναι απαραίτητη. Για να επωφεληθεί κάποιος από διαφορετικές εφαρμογές, συχνά απαιτούνται πολλές ταυτότητες, οι οποίες κρύβουν πολλαπλούς κινδύνους έκθεσης και απάτης. Εάν ένας χρήστης πρέπει να αυθεντικοποιείται κάθε φορά που αποκτά πρόσβαση σε ένα διαφορετικό υπό-σύστημα της ηλεκτρονικής διακυβέρνησης, αυτό θα περιλαμβάνει πολλαπλούς κινδύνους για κλοπή της ταυτότητας του. [62]

Ανωνυμία

Οι χρήστες προτιμούν συχνά την ανωνυμία κατά τη διάρκεια των online συναλλαγών τους ιδιαίτερα όταν οι δραστηριότητες τους μπορεί να αποκαλύψουν ευαίσθητες πληροφορίες για το άτομό τους. Μια μερική ταυτότητα που μπορεί να μην χρησιμοποιηθεί για να προσδιορίσει μοναδικά ένα άτομο παρέχει ένα βαθμό ανωνυμίας. Η ανωνυμία δεν σημαίνει ότι καμία πληροφορία δεν απελευθερώνεται, αλλά οι πληροφορίες που αποκαλύπτονται δεν θα πρέπει να προσδιορίζουν την ταυτότητα ενός χρήστη [63]. Για παράδειγμα, ένας ασθενής μπορεί να παραλάβει ή να παραγγείλει ένα φάρμακο από ένα φαρμακοποιό ανώνυμα. Εδώ, ο φαρμακοποιός πρέπει να είναι σε θέση να συνδέσει τη μερική ταυτότητα του ασθενούς στην ιατρική συνταγή. Μερικές αλληλεπιδράσεις, ωστόσο, δεν μπορεί να διεξάγονται ανώνυμα, για παράδειγμα, όταν ένας γιατρός κάνει διάγνωση για έναν ασθενή, η ταυτότητα του ασθενούς πρέπει να επαληθευτεί και το ιατρικό ιστορικό του θα πρέπει να είναι προσβάσιμο.

Συναγωγή Πληροφοριών και Προστασία Προσωπικών Δεδομένων

Η συναγωγή πληροφοριών καθιστά την προστασία της ιδιωτικής ζωής δύσκολη στα περιβάλλοντα των σύγχρονων τεχνολογιών πληροφορικής όπου διαφορετικά κομμάτια των ιδιωτικών πληροφοριών αποθηκεύονται σε διαφορετικές πηγές. Λαμβάνοντας υπόψη την πρόσβαση σε διαφορετικές μέρη των προσωπικών δεδομένων ενός ατόμου που δεν είναι ευαίσθητα, μπορεί να είναι

δυνατό να διεξαχθούν συμπεράσματα άνευ αδείας, για ευαίσθητες προσωπικές πληροφορίες του ατόμου[64]. Αναδυόμενα εξελιγμένα εργαλεία εξόρυξης δεδομένων που μπορεί να συνθέσουν διαφορετικά κομμάτια των προσωπικών πληροφοριών επιδεινώνουν σοβαρά το πρόβλημα. Για παράδειγμα, η εξόρυξη των φαρμακευτικών αγορών θα μπορούσαν να υποδεικνύουν ότι ένας χρήστης πιθανώς πάσχει από μια συγκεκριμένη ασθένεια. Ταυτόχρονα, η χρήση των εργαλείων εξόρυξης δεδομένων μπορεί να είναι χρήσιμη για πολλούς σκοπούς, όπως η ανίχνευση επικείμενης βιο-τρομοκρατίας ή περαιτέρω ανακαλύψεων. Η βασική πρόκληση είναι να εξασφαλιστεί ισορροπημένη χρήση των εργαλείων αυτών για την προστασία της ιδιωτικής ζωής έναντι άλλων οφελών. [65]

3.5. Προστασία προσωπικών δεδομένων

Η προστασία προσωπικών δεδομένων μπορεί να θεωρηθεί ως προστασία δύο ειδών θεμελιωδών δικαιωμάτων:

- **Την προτεραιότητα στον καθορισμό της ταυτότητας του ατόμου:** (Αυτή συνεπάγεται το δικαίωμα του ελέγχου της χρήσης των προσωπικών πληροφοριών που αποκαλύπτονται σε τρίτους, όπως προσωπικές πληροφορίες, που προσδιορίζουν την ταυτότητα σου σε άλλους. Ως ειδική περίπτωση μπορεί να αναφερθεί, η ελευθερία της ανωνυμίας. Σε ορισμένες περιπτώσεις είμαστε έτοιμοι να δανείσουμε τα προσωπικά μας δεδομένα για στατιστικές έρευνες, για ερευνητικούς σκοπούς και άλλα, υπό την προϋπόθεση ότι η ανωνυμία είναι εγγυημένη.)

- **Το δικαίωμα του ιδιωτικού χώρου:** (Αυτό γενικά σημαίνει όχι μόνο τον φυσικό χώρο, αλλά και ειδικά αντικείμενα που σχετίζονται αποκλειστικά με ένα συγκεκριμένο πρόσωπο, όπως ένα ιδιωτικό ημερολόγιο ή ιδιωτικές επιστολές.) Η προστασία της ιδιωτικής ζωής του σπιτιού κάποιου είναι ένα κλασικό παράδειγμα ενός ιδιωτικού χώρου, που, άλλωστε, συνδέεται με την ταυτότητα κάποιου. Είναι επίσης ένα διδακτικό αρχέτυπο γιατί δείχνει τη φύση ενός ιδιωτικού χώρου, σαν κοινωνικό κατασκεύασμα. Είστε, σε γενικές γραμμές, ελεύθεροι να επιλέξετε ποιόν θέλετε να προσκαλέσετε στο σπίτι σας. Ωστόσο, υπό ειδικές περιστάσεις, είναι δυνατόν για την αστυνομία, για παράδειγμα, να εισέλθει στο σπίτι σας χωρίς συναίνεσή σας, κάτι το οποίο ρυθμίζεται αυστηρά από το νόμο.

Ως αποτέλεσμα της εμπειρίας σε διαφορετικούς πολιτισμούς, ένα σύστημα πρακτικών και συνηθειών έχει αναπτυχθεί το οποίο καθορίζει τι πρέπει να θεωρείται προσωπικό και τι δημόσιο [66] [67]. Μια βασική διάκριση στις ανθρώπινες σχέσεις είναι, ότι μεταξύ των ιδιωτιών (κοινό με μερικά άτομα) και των κοινών (κοινό με ευρύτερες ομάδες).[68] Ο Fried [69] υποστηρίζει ότι μόνο στενά συνδεδεμένα πρόσωπα μπορούν να έχουν πραγματική γνώση ενός ατόμου. Σύμφωνα με τον Mason [70], η προστασία της ιδιωτικής ζωής μπορεί να μελετηθεί μέσα από τις σχέσεις των τεσσάρων κοινωνικών ομάδων (μέρη):

1. το άτομο
2. άλλοι στους οποίους απευθύνεται το πρώτο μέρος παρέχει συγκεκριμένες προσωπικές πληροφορίες για λόγους δημιουργίας ή διατήρησης μιας προσωπικής σχέσης ή για την ανταλλαγή υπηρεσιών
3. όλα τα άλλα μέλη της κοινωνίας που μπορούν να έχουν πρόσβαση στις προσωπικές πληροφορίες ενός ατόμου, αλλά δεν έχουν καμία επαγγελματική σχέση με το άτομο και καμία δικαιοδοσία να χρησιμοποιήσουν τις πληροφορίες και
4. το ευρύ κοινό το οποίο δεν έχει καμία άμεση επαφή με το ιδιωτικό χώρο ή τις πληροφορίες του ατόμου.

Κατά τη διάρκεια της αλληλεπίδρασης μεταξύ των μερών, τα άτομα επικαλούνται διάφορα επίπεδα της ιδιωτικής ζωής. Τα πλεονεκτήματα των στενών σχέσεων σε σύγκριση με τους κινδύνους της απελευθέρωσης των πληροφοριών και της ακατάλληλης χρήσης, η οποία θα μπορούσε να οδηγήσει σε απώλεια του προσωπικού χώρου ή βλάβη της ταυτότητας ενός ατόμου.[71]

3.5.1. Αρχές προστασίας της ιδιωτικής ζωής

Για να αντιληφθεί κάποιος τι είναι πραγματικά η προστασία της ιδιωτικής ζωής , πρέπει να ξεκινήσει με τη μελέτη των αρχών προστασίας της ιδιωτικής ζωής που αποτελούν τη βάση της σύγχρονης νομοθεσίας προστασίας της ιδιωτικής ζωής στις χώρες της ΕΕ και σε πολλές άλλες χώρες. Στη νομοθεσία, υπάρχουν φυσικά, πολλές εξαιρέσεις από τις γενικές αρχές, αλλά η πρόθεση της νομοθεσίας είναι να ακολουθούν τις αρχές αυτές στο μέτρο του δυνατού. Οι σημαντικότερες αρχές όσον αφορά το ιδιωτικό απόρρητο είναι οι ακόλουθες:

- **Τα προσωπικά δεδομένα δεν θα πρέπει να χρησιμοποιούνται για άλλο σκοπό πέρα από αυτόν για τον οποίο συγκεντρώθηκαν.** Ο σκοπός της χρήσης των προσωπικών δεδομένων πρέπει να είναι συγκεκριμένος κατά τη συλλογή τους και θα μπορούσε να αλλάξει μόνο εάν η φύση των δεδομένων το επιτρέπει.
- **Η ποσότητα των προσωπικών δεδομένων που συλλέγονται και αποθηκεύονται πρέπει να μειωθεί.** Οι οργανισμοί δεν θα πρέπει να συγκεντρώνουν περισσότερες πληροφορίες από αυτές που πραγματικά χρειάζονται και θα πρέπει να διαγράφουν πληροφορίες που δεν τους είναι πλέον χρήσιμες. Επιπλέον θα πρέπει να ελλατώνουν τη δυνατότητα ταυτοποίησης των δεδομένων χρησιμοποιώντας για παράδειγμα ψευδώνυμα.
- **Το άτομο θα πρέπει να έχει τον έλεγχο της ιδιωτικής του ζωής.** θα πρέπει το άτομο να μπορεί να αποφασίσει ποιο είναι το κατάλληλο επίπεδο προστασίας της ιδιωτικής ζωής έναντι των υπηρεσιών που μπορεί να πάρει.
- **Οι συλλέκτες και οι χρήστες των προσωπικών δεδομένων είναι υπεύθυνοι για την ποιότητα των δεδομένων.** Έχουν την υποχρέωση να διασφαλίζουν ότι τα δεδομένα είναι ακριβή , πλήρη, ενημερωμένα και σχετικά με το σκοπό για τον οποίο έχουν συλλεχθεί. Επιπρόσθετα αν ανιχνευτούν λάθη θα πρέπει να προβούν σε ενέργειες για την ελαχιστοποίηση της βλάβης που μπορεί να προκληθεί στα δεδομένα.

Ø **Η επαρκής ασφάλεια των πληροφοριών αποτελεί προαπαιτούμενο.** Ένας οργανισμός χρειάζεται κατάλληλες τεχνικές λύσεις και υπηρεσιακές διαδικασίες ώστε να διατηρήσει την ασφάλεια. Επίσης για τους οργανισμούς εκείνους που μεταφέρουν τα δεδομένα σε τρίτους θα πρέπει να είναι σίγουροι ότι και οι δέκτες των δεδομένων διαθέτουν ένα αντίστοιχο σύστημα ασφάλειας δεδομένων.[72]

3.5.2. Προστασία της ιδιωτικής ζωής του πολίτη

Οι κυβερνητικοί οργανισμοί πρέπει να λάβουν μια δομημένη προσέγγιση στην προστασία της ιδιωτικότητας των πολιτών που εξυπηρετούν. Η συλλογή και η χρήση των προσωπικών δεδομένων αποτελεί μια σοβαρή απειλή για την προστασία της ιδιωτικής ζωής των πολιτών. Είναι σημαντικό κάθε κυβερνητική οργάνωση να αναλύει τις ανάγκες της για προσωπικά δεδομένα και τους κινδύνους που συνδέονται με την επεξεργασία τους, έτσι ώστε οι επαρκείς έλεγχοι να λαμβάνουν χώρα και να εξασφαλίζουν υψηλό επίπεδο στην ιδιωτική ζωής των πολιτών. Μια προσέγγιση που ταιριάζει σε όλους τους οργανισμούς δεν είναι εφικτή, εφόσον οι οργανισμοί έχουν διαφορετικές ανάγκες και κινδύνους που συνδέονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ένα ικανοποιητικό επίπεδο ασφάλειας των πληροφοριών αποτελεί μια βάση, αλλά οι κυβερνητικές οργανώσεις θα πρέπει να λάβουν έναν αριθμό επιπλέον μέτρων, για να διασφαλίσουν την κατάλληλη προστασία της ιδιωτικής ζωής των πολιτών, τα οποία δεν είναι υποχρεωτικό να πραγματοποιούνται διαδοχικά αλλά θα περίμενε κανείς να πραγματοποιούνται ταυτόχρονα και κατ' επανάληψη.

Τα επιπλέον αυτά μέτρα είναι:

- ü Ανάλυση των αναγκών για δεδομένα και κίνδυνοι για την ιδιωτικότητα.
- ü Σχεδιασμός για την προστασία της ιδιωτικής ζωής
- ü Προδιαγραφή πολιτικής
- ü Εφαρμογή της πολιτικής προστασίας της ιδιωτικής ζωής [73]

3.5.3. Νομικό Πλαίσιο

Όσον αφορά την Ελλάδα σύμφωνα με το Ν.3979 του 2011 ο οποίος αφορά την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις, ο οποίος έχει δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως της Ελληνικής Δημοκρατίας, Τεύχος Πρώτο, Αρ. Φύλλου 138, στις 16 Ιουνίου 2011 και ειδικότερα όσον αφορά τα δικαιώματα των προσώπων, ισχύουν τα κάτωθι σύμφωνα με τα άρθρα 7 και 8 του προαναφερθέντος νόμου:

Άρθρο 7

Γενικές αρχές προστασίας δεδομένων προσωπικού χαρακτήρα

1. Οι φορείς του δημόσιου τομέα παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης με σεβασμό του δικαιώματος προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικότητας των φυσικών προσώπων.

2. Κατά το σχεδιασμό, διαμόρφωση και προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης γίνεται αξιολόγηση των επιπτώσεών τους στην ιδιωτικότητα και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

3. Ο σχεδιασμός, η διαμόρφωση και η προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης πρέπει να γίνεται, λαμβάνοντας υπόψη το δικαίωμα προστασίας των προσωπικών δεδομένων και την ανάγκη διαμόρφωσης των συστημάτων και υπηρεσιών κατά τρόπο ώστε να διασφαλίζεται η επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα.

4. Όπου ο παρών νόμος απαιτεί τη συγκατάθεση του προσώπου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η σχετική δήλωση μπορεί να δίδεται και με χρήση ΤΠΕ. Ο φορέας του δημόσιου τομέα που είναι υπεύθυνος επεξεργασίας εξασφαλίζει ότι η δήλωση , η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη και μπορεί οποτεδήποτε να ανακληθεί χωρίς αναδρομικό αποτέλεσμα.

Άρθρο 8

Δικαιώματα των προσώπων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς ηλεκτρονικής διακυβέρνησης

1. Αν τα φυσικά πρόσωπα επιθυμούν να χρησιμοποιηθούν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και έχουν γνωστοποιήσει σε φορείς του δημόσιου τομέα για μελλοντικές ηλεκτρονικές συναλλαγές τους με τους φορείς αυτούς, παρέχουν προς τούτο την έγγραφη συγκατάθεσή τους μετά από ενημέρωση για τις ενδεχόμενες μελλοντικές χρήσεις και τους σκοπούς που επιδιώκονται, τους αποδέκτες και τις κατηγορίες αποδεκτών καθώς και την ύπαρξη δικαιωμάτων πρόσβασης και αντίρρησης.

2. Περαιτέρω χρήση δεδομένων προσωπικού χαρακτήρα για στατιστικούς λόγους ή για τη βελτίωση των παρεχόμενων υπηρεσιών επιτρέπεται, εφόσον τα δεδομένα αυτά καταστούν ανώνυμα σύμφωνα με το άρθρο 20 παρ. 3 είτε με έγγραφη συγκατάθεση των φυσικών προσώπων ή των νομίμων εκπροσώπων τους.

3. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ρυθμίζονται τα ειδικότερα θέματα που αφορούν την ενημέρωση των προσώπων και την παροχή της συγκατάθεσης σύμφωνα με τις παραγράφους 1 και 2.

4. Οι δημόσιες αρχές δεν επιτρέπεται να εξαρτούν την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης από τη συγκατάθεση των προσώπων για την περαιτέρω επεξεργασία δεδομένων που τα αφορούν είτε για στατιστικούς σκοπούς και για σκοπούς βελτίωσης των παρεχομένων υπηρεσιών είτε για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης στο μέλλον.

5. Με την προϋπόθεση της επιβεβαίωσης ταυτότητας (αυθεντικοποίησης) και της ασφάλειας, τα φυσικά πρόσωπα μπορούν να ασκούν και με χρήση ΤΠΕ τα δικαιώματα πρόσβασης και αντίρρησης που προβλέπονται στα άρθρα 12 και 13 του ν. 2472/1997. [74]

3.6. Διαχείριση Ασφάλειας Πληροφοριών στην Ηλεκτρονική διακυβέρνηση

Η διασφάλιση της ασφάλειας για τα συστήματα πληροφοριών συμπεριλαμβανομένων των υπολογιστών και των δικτύων είναι μια θεμελιώδης αναγκαία προϋπόθεση για μια ψηφιακή διακυβέρνηση ώστε να λειτουργεί σύμφωνα με τις προσδοκίες των πολιτών. Το πρόβλημα ασφαλείας μπορεί να οπτικοποιηθεί διαιρόντας το σε τρία ιεραρχικά επίπεδα:

- επίπεδο διαχείρισης,
- το επίπεδο συστήματος και
- το επίπεδο εφαρμογών και δεδομένων.

στο επίπεδο διαχείρισης περιλαμβάνονται η **εκτίμηση κινδύνου**, η **ανάλυση κόστους**, η **δημιουργία πολιτικής**, ο **καθορισμός διαδικασιών** και η **επιβολή πολιτικής και διαδικασιών**. [75]

3.6.1. Εκτίμηση Κινδύνου

Η εκτίμηση κινδύνου αποτελεί μια συστηματική προσέγγιση για τον εντοπισμό κρίσιμων κινδύνων, αναλύει τις επιπτώσεις των κινδύνων και τους αμβλύνει. Με περιορισμένους πόρους για τη δημιουργία ασφαλούς διαδικασίας, μια ψηφιακή κυβέρνηση πρέπει να αξιολογήσει τους εν δυνάμει κινδύνους για να εξασφαλιστεί ότι οι πόροι χρησιμοποιούνται με τον βέλτιστο τρόπο. Ως εκ τούτου, τα ακόλουθα βήματα, δηλαδή ***αναγνώριση κινδύνου***(*risk identification)*, ***ανάλυση των επιπτώσεων του κινδύνου***(risk impact analysis) και η ***μείωση του κινδύνου***(risk mitigation) που πρέπει να ληφθούν.

- Αναγνώριση κινδύνου: Ο στόχος του εντοπισμού των κινδύνων είναι να οριοθετηθούν οι κίνδυνοι αυτοί, που μπορεί να έχουν σημαντικές επιπτώσεις στην λειτουργικότητα και την αξιοπιστία της ψηφιακής διακυβέρνησης. Πτυχές που πρέπει να εξεταστούν περιλαμβάνουν: τεχνικές πηγές των κινδύνων, διαδικαστικές πηγές κινδύνων και την πιθανότητα παραβίασης της ασφάλειας [76]

- Ø Τεχνικές πηγές κινδύνων: Αδυναμίες και υπάρχοντες περιορισμοί στις τεχνικές που χρησιμοποιούνται, όπως η κρυπτογράφηση, τα firewall πρέπει να προσδιοριστούν. Για παράδειγμα, όπως η υπολογιστική ισχύς αυξάνεται διαρκώς, η δύναμη του προτύπου κρυπτογράφησης δεδομένων (DES) [77], η οποία έχει ευρέως χρησιμοποιηθεί για περίπου 20 χρόνια, ωθείται στα όριά της και πλέον δεν θεωρείται ως ασφαλής για τις κρίσιμες διαδικασίες.

- Ø Διαδικαστικές πηγές κινδύνων: Διαδικαστικοί έλεγχοι στις διαδικασίες διοίκησης και στις διαδικασίες πρόσβασης του συστήματος μπορεί επίσης να έχουν κάποια κενά που πρέπει να καλυφθούν. Η προσωπική συμπεριφορά και η κουλτούρα των οργανισμών μπορεί επίσης να έχουν επιρροή στη διαδικασία και την πράξη.

- Ø Πιθανότητα παραβίαση της ασφάλειας: Πιθανότητα της εμφάνισης των πιθανών κινδύνων πρέπει να μελετηθεί ώστε ο αντίκτυπος του κινδύνου να μπορεί να αναλυθεί αντικειμενικά.

- Ανάλυση Επιπτώσεων Κινδύνου: Με τους πιθανούς κινδύνους να έχουν αναγνωριστεί, οι επιπτώσεις των ακόλουθων πτυχών πρέπει να αναλυθούν.

  - Ø Η αξιοπιστία της κυβέρνησης: "Ορατές" παραβάσεις ασφάλειας, φυσικά σημαντικές ή ασήμαντες, μπορούν να βλάψουν την αξιοπιστία της κυβέρνησης και να μειώσουν την εμπιστοσύνη του λαού προς αυτήν. Για παράδειγμα, η φήμη της ικανότητα της κυβέρνησης να προστατεύσει τις πληροφορίες της ή ακόμα και των πολιτών, μπορεί να μειωθεί εάν οι εικόνες της εθνικής σημαίας στα κυβερνητικά της portal αντικατασταθούν από έναν αντίπαλο του έθνους με εικόνες της εθνικής σημαίας του αντιπάλου.

  - Ø Διαθεσιμότητα πληροφοριών και συνέχεια των υπηρεσιών: Διαθεσιμότητα των πληροφοριών και συνέχεια των υπηρεσιών 24 ώρες το 24ωρο και 7 μέρες την εβδομάδα είναι το κλειδί που απαιτείται και τα χαρακτηριστικά που διακρίνουν τις ψηφιακές κυβερνήσεις από τις παραδοσιακές κυβερνήσεις. Μη διαθεσιμότητα και μη συνέχεια των υπηρεσιών πληροφοριών θα έχει σίγουρα σημαντικές επιπτώσεις στη λειτουργικότητα της κυβέρνησης.

- Μετριασμός του κινδύνου: Ο μετριασμός του κινδύνου είναι η διαδικασία στην οποία χρησιμοποιούνται αποτελεσματικοί τρόποι ελέγχων για την ελαχιστοποίηση των επιπτώσεων των κινδύνων σε ένα αποδεκτό επίπεδο. Αυτή η διαδικασία δίνει τη δυνατότητα στη κυβέρνηση να καθορίσει πόσο ρίσκο είναι διατεθειμένη να αναλάβει και σε ποιο βαθμό τα περιουσιακά της στοιχεία και τα δεδομένα πρέπει να προστατευτούν. Για να μετριαστούν οι επιπτώσεις των πιθανών κίνδυνων στην ψηφιακή κυβέρνηση, που είναι ζωτικής σημασίας

τεχνολογίας ελέγχου της ασφαλείας πρέπει να τεθούν σε λειτουργία, και διαδικασίες και κατευθυντήριες γραμμές ορθής πρακτικής πρέπει να καταρτιστούν. [78]

3.6.2. Ανάλυση Κόστους

Οι αποτελεσματικοί μηχανισμοί ασφαλείας απαιτούν μια διαδικασία που επιτρέπει στην ψηφιακή διακυβέρνηση να καθορίσει το πληροφοριακά αποδεκτό επίπεδο ασφάλειας εντός του οποίου οι κίνδυνοι περιορίζονται στο ελάχιστο. Όταν το επίπεδο ασφάλειας καθοριστεί, το κόστος της ανάλυσης κατορθώνει να φτάσει στο επίπεδο, στο οποίο μπορεί να πραγματοποιηθεί .Η ανάλυση κόστους περιλαμβάνει:

- **Άμεσα χρηματοοικονομικά έξοδα** που πραγματοποιούν την απόκτηση ή τη μίσθωση των στοιχείων ασφαλείας και των υπηρεσιών ασφαλείας, όπως το δίκτυο, τις συσκευές παρακολούθησης, τα firewalls, την κρυπτογράφηση των δρομολογητών και την μίσθωση των υπηρεσιών των εικονικών ιδιωτικών δικτύων (VPN). Εκτός από το hardware και software, μια υπηρεσία, η οποία χρεώνεται την ευθύνη για τη διασφάλιση της ασφάλειας των πληροφοριών πρέπει να καθοριστεί. Εξωτερικοί ή ανεξάρτητοι έλεγχοι πρέπει επίσης να συμμετέχουν τακτικά για την αναθεώρηση των πρακτικών και των διαδικασιών ασφάλειας, την αξιολόγηση των αγνώστων κινδύνων, και να διατυπώνουν συστάσεις και εκθέσεις. Αυτά όλα αθροίζονται σε ένα σημαντικό έξοδο.
- **Οι έμμεσες δαπάνες επίδοσης**, οι οποίες προκύπτουν από την ενσωμάτωσης των διαδικασιών πιστοποίησης και γνησιότητας, της διοίκησης, της κρυπτογράφησης, της ακεραιότητας της επαλήθευσης, της πολιτικής επιβολής και ούτω καθεξής. Μερικές από αυτές τις διαδικασίες θα μειώσουν άμεσα την απόδοση και την αποτελεσματικότητα των πληροφοριακών συστημάτων. Μερικοί (π.χ., η επιβολή της πολιτικής, οι έλεγχοι ασφαλείας και οι έλεγχοι ασφαλείας των λογαριασμών) μπορεί να οδηγήσουν σε αντιπαλότητα μεταξύ των κυβερνητικών υπηρεσιών, η οποία μπορεί να προκαλέσει αρνητικές επιπτώσεις στις επιδόσεις στην ίδια την κυβέρνηση παρά στα πληροφοριακά συστήματα. [79]

3.6.3. Χάραξη Πολιτικής

Η πολιτική ασφαλείας είναι ένα σύνολο κανόνων που καθορίζουν τον τρόπο που μια ψηφιακή διακυβέρνηση διαχειρίζεται τους κινδύνους και προστατεύει τα δεδομένα της και το πληροφοριακό της σύστημα. Αυτό που πρέπει να λάβει υπόψη της η διοίκηση είναι η διαχείριση, η χρήση και η διανομή των πληροφοριών και των πληροφοριακών συστημάτων της. Οι πτυχές που πρέπει να εξεταστούν κατά τη χάραξη πολιτικών ασφάλειας περιλαμβάνουν:

- *Πρότυπα*: Κάθε ψηφιακή κυβέρνηση που δεσμεύεται να εξασφαλίσει την ασφάλεια των πληροφοριών πρέπει να ψάξει για καθοδήγηση, ώστε να επιτύχει συνεκτική, συνολική και αξιολογήσιμη ασφάλεια. Αρκετά πρότυπα τα οποία παρέχουν χρήσιμες οδηγίες είναι διαθέσιμα. BS 7799/ISO 17799 (BS 7799 Μέρος 1, 2000) είναι ένα από τα πιο γνωστά πρότυπα.

- *Ταξινόμηση δεδομένων*: Η υπέρ-προστασία μπορεί να επιφέρει αρνητικές επιπτώσεις στην επίδοση της διακυβέρνησης, ενώ η ελλιπής προστασία μπορεί να θέσει σε κίνδυνο την ασφάλεια. Η ταξινόμηση δεδομένων διευκολύνει εκλεκτικά την επιβολή της ασφάλειας.

- *Κανονισμός της χρήσης των δεδομένων και περιουσιακών στοιχείων:* Για παράδειγμα, η χρήση ζώντων πληροφοριών για την ανάπτυξη και για δοκιμές θα πρέπει να απαγορευτεί και η χρήση των sniffers (δηλαδή, λογισμικού ή των συσκευών παρακολούθησης της ροής των δεδομένων μέσα στο δίκτυο) πρέπει να ρυθμιστεί.

- *Ανθρώπινα Δικαιώματα και Προστασία Προσωπικών Δεδομένων:* Οι κανονισμοί που διέπουν την προστασία των ανθρωπίνων δικαιωμάτων και της ιδιωτικής ζωής είναι εκείνο το μέρος της δέσμευσης μιας ψηφιακής διακυβέρνησης που πρέπει να διευθετηθούν στο πλαίσιο της πολιτικής ασφάλειας.

- *Ανταπόκριση στις Προειδοποιήσεις:* Οι υπηρεσίες της ψηφιακής διακυβέρνησης θα πρέπει να συστήσουν τις προκαθορισμένες διαδικασίες και ενέργειες που πρέπει να λάβει για να αντιμετωπιστούν περιστατικά ασφάλειας διαφόρων επιπέδων της ασφάλειας ή προειδοποιήσεις που εκδίδονται από οργανισμούς ασφάλειας, όπως η Ομάδα Αντιμετώπισης Έκτακτης Ανάγκης Υπολογιστών (CERT), έτσι ώστε οι οργανισμοί να μπορέσουν να ανταποκριθούν άμεσα.

- *Εκπαίδευση σε θέματα ασφάλειας*: Οι κυβερνητικοί υπάλληλοι και οι χρήστες του συστήματος πρέπει να είναι ενήμεροι των πολιτικών ασφαλείας, των κωδικών πρακτικής και της υπευθυνότητας. Η εκπαίδευση σε θέματα ασφάλειας θα πρέπει να παρέχεται σε όλο το προσωπικό που εμπλέκεται στο σχεδιασμό, την υλοποίηση, τη συντήρηση και τη χρήση των πληροφοριακών συστημάτων.

- *Ευθύνη*: Τα άτομα που υπόκεινται στην πολιτική ασφαλείας πρέπει να αντιληφθούν την ευθύνη τους. Η νομοθεσία για την ασφάλεια των κυβερνητικών πληροφοριών πρέπει , επίσης, να υφίσταται και να αναβαθμίζεται. [80]

3.6.4. Ορισμός της Διαδικασίας

Καθώς οι πολιτικές είναι κανόνες που περιγράφουν το *τι* και το *γιατί* της ασφάλειας των πληροφοριών εντός της ψηφιακής διακυβέρνησης, οι διαδικασίες είναι πιο λεπτομερής

και ακριβής έγγραφα που προσδιορίζουν, το ποίος , το πότε και το πώς της ασφάλειας των πληροφοριών. Οι διαδικασίες αυτές θα πρέπει να περιλαμβάνουν:

- *Ασφαλή Backups*: Οι διαδικασίες δημιουργίας αντιγράφων ασφαλείας θα πρέπει να περιλαμβάνουν:
  - Ø Τα αντίγραφα ασφαλείας για διαμορφώσεις των υποδομών πληροφοριών.
  - Ø Τα αντίγραφα ασφαλείας για τους διακομιστές που παρέχουν δίκτυο / Web υπηρεσίες.
  - Ø Κατανεμημένα εκτός του χώρου αποθήκευσης αντιγράφων ασφαλείας.
  - Ø Τακτική εξακρίβωση της ακεραιότητας των αντιγράφων ασφαλείας.
- *Πιστοποίηση Ενεργητικού*: Αυτό για να διασφαλιστεί ότι τα περιουσιακά στοιχεία που χρησιμοποιούνται στα συστήματα πληροφοριών συμμορφώνονται με τις συγκεκριμένες απαιτήσεις ασφαλείας.
- *Λογιστικός έλεγχος*: Οι δραστηριότητες στον τομέα των πληροφοριακών συστημάτων πρέπει να καταγράφονται, να παρακολουθούνται και να αναλύονται έτσι ώστε τα συμβάντα ασφαλείας να μπορούν να εντοπίζονται ή ακόμα να προλαμβάνονται. Οι ρυθμίσεις παραμέτρων της υποδομής του δικτύου πρέπει να εξακριβώνονται ώστε να εξασφαλιστεί η εγκυρότητά τους.
- *Σχέδιο για την αντιμετώπιση καταστροφών:* Δεν υπάρχει κανένα σύστημα, το οποίο να είναι 100% ασφαλές. Για να εξασφαλιστεί η εύρυθμη λειτουργία μιας ψηφιακή διακυβέρνησης όταν το χειρότερο συμβεί, ένα σχέδιο έκτακτης ανάγκης και ένα σχέδιο ανάκαμψης για τη διαχείριση της κρίσης είναι υψίστης σημασίας. Αυτό θα πρέπει να περιλαμβάνει διαδικασίες αντιμετώπισης περιστατικών ασφαλείας (CSIRP).[81]

3.6.5. Επιβολή της Πολιτικής και των Διαδικασιών

Η επιβολή των πολιτικών και των διαδικασιών ασφαλείας είναι μια σταθερή προσπάθεια της ψηφιακής διακυβέρνησης. Η συμμόρφωση με τα πρότυπα είναι ένας αποτελεσματικός τρόπος για την επιβολή της διαδικασίας και της πολιτικής . Δύο καλές πηγές πληροφοριών είναι τα: *BS 7799*, η οποία είναι ένα πρότυπο που αποτελείται από δύο μέρη (BS 7799 Μέρος 1, 2000; BS 7999 Μέρος 2, 2002), το οποίο ορίζει τις απαιτήσεις για ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS). Βοηθούν στον προσδιορισμό, τη διαχείριση και τη μείωση του αντίκτυπου των κινδύνων στους οποίους οι πληροφορίες υποβάλλονται διαρκώς. Το Μέρος 1, διαιρείται σε 10 τμήματα και έχει διεθνώς υιοθετηθεί από το πρότυπο ISO, ISO / IEC 17799, το οποίο περιέχει επεξηγηματικές

πληροφορίες και καθοδήγηση. Το Μέρος 2 προτείνει ένα μοντέλο για τους οργανισμούς ώστε να μπορούν να κατασκευάσουν και να λειτουργήσουν τα δικά τους συστήματα διαχείρισης ασφάλειας πληροφοριών,ISMSs. Μια άλλη χρήσιμη πηγή είναι η έκθεση Turnbull [82], η οποία καθορίζει πώς οι οργανισμοί θα πρέπει να συμμορφώνονται με τις απαιτήσεις για τους οικονομικούς και επιχειρησιακούς ελέγχους για την αντιμετώπιση των ζητημάτων της διαχείρισης των κινδύνων. Ένας άλλος τρόπος για την επιβολή των πολιτικών και των διαδικασιών είναι οι τακτικοί έλεγχοι, οι οποίοι βοηθούν τις κυβερνητικές υπηρεσίες να επανεξετάσουν τα συστήματά τους, τις πρακτικές ασφαλείας του και να προσδιορίσουν κινδύνους που έχουν παραβλεφθεί. [83]

3.7. Ασφάλεια των πληροφοριών

3.7.1. Ταυτοποίηση

Οι επίσημες διαδικασίες απαιτούν την αλάνθαστη ταυτοποίηση του πολίτη. Η ταυτοποίηση είναι αναγκαία για να διασφαλιστεί ότι ο πολίτης που προσεγγίζει την υπηρεσία είναι αυτός ο οποίος έκανε μια αίτηση ή που αιτείται να ενημερωθεί για την κατάσταση ενός αιτήματος του. Έτσι ως ***Ταυτοποίηση ορίζεται η απαραίτητη εκείνη διαδικασία με την οποία πιστοποιείται ή αναγνωρίζεται η ταυτότητα.*** Σε αντίθεση με την ταυτοποίηση, η αυθεντικότητα μίας δήλωσης προθέσεων ή ενεργειών είναι απαραίτητη ώστε να διασφαλιστεί η υποτιθέμενη ταυτότητα. Στις συμβατικές γραφειοκρατικές διαδικασίες η ταυτότητα επικυρώνεται με την επίδειξη ενός αναγνωριστικού ταυτότητος ή μιας μαρτυρίας και η αυθεντικοποίηση διασφαλίζεται από τις χειρόγραφες υπογραφές. Στις διαδικασίες της ηλεκτρονικής διακυβέρνησης οι οποίες πραγματοποιούνται ηλεκτρονικά, η ταυτοποίηση και η αυθεντικοποίηση παραμένουν σημαντικοί παράμετροι και χρειάζονται ηλεκτρονική υποστήριξη. Αυτό μπορεί να πραγματοποιηθεί από την γνωριμία ηλεκτρονικών υποκατάστατων των εγγράφων που βασίζονται στο χαρτί και τις χειρόγραφες υπογραφές. Με μια πρώτη ματιά, οι ηλεκτρονικές υπογραφές, τα ψηφιακά πιστοποιητικά και η Υποδομή Δημόσιου Κλειδιού (PKI) αποτελούν τέτοια υποκατάστατα.

3.7.1.1. Απαιτήσεις ενός μοντέλου ταυτοποίησης

Κατά την εισαγωγή ενός μοντέλου ταυτοποίησης στην ηλεκτρονική διακυβέρνηση συνήθως μια σειρά από σκέψεις γίνονται. Ανεξάρτητα από το αν το μοντέλο ταυτοποίησης εισάγεται σε εθνικό, περιφερειακό ή επίπεδο δήμου, μοναδικά στοιχεία ταυτότητας θα πρέπει να υποστηριχτεί, όπως αυτό απαιτείται από πολλές επίσημες διαδικασίες. Το μοντέλο θα πρέπει να υποστηρίζει μόνιμα, κατά προτίμηση δια βίου αναγνωριστικά που δεν θα υποβληθούν σε αλλαγές των ονομάτων και ούτω καθεξής. Αυτό εξασφαλίζει ότι ένας πολίτης μπορεί να ταυτοποιηθεί μέσα από μια

συγκεκριμένη διαδικασία, όποτε η ταυτοποίηση είναι απαραίτητη. Τα κτηματολόγια είναι ένα ξεκάθαρο παράδειγμα, όπου η ταυτοποίηση μπορεί να χρειαστεί για αρκετό διάστημα. Ειδικότερα, σε μεγαλύτερη κλίμακα, η ίδρυση της ταυτότητας βασιζόμενη σε χαρακτηριστικά όπως το όνομα και ημερομηνία γέννησης δεν είναι επαρκής, διότι διαδεδομένα ονόματα μπορεί να οδηγήσουν σε ψηφιακά δίδυμα. Έτσι, η επεκτασιμότητα αποτελεί ένα ακόμη ζήτημα. Σχετικά με την επεκτασιμότητα, μια πτυχή που δεν πρέπει να υποτιμηθεί είναι ότι τα συστήματα που δουλεύουν καλά με τις πρώτες εφαρμογές που συνήθως είναι στην τεχνολογία μόρφωσης μπορεί να αποδειχθεί ότι δεν αναβαθμίζεται, όταν η τεχνολογία υιοθετείται γενικά. Ένα παράδειγμα-πέρα από τους παράγοντες ασφαλείας-είναι τα ονόματα χρηστών και οι κωδικοί πρόσβασης που τείνουν να γίνουν δαπανηρές σε μεγάλη κλίμακα, καθώς, αν ξεχαστούν οι κωδικοί πρόσβασης, το κόστος υποστήριξης μετατρέπεται σε ένα σημαντικό ζήτημα. Αυτό ιδιαίτερα ισχύει για την ηλεκτρονική διακυβέρνηση, καθώς περισσότεροι πολίτες έχουν συναλλαγές με τις υπηρεσίες του δημόσιου σπάνια, σε πολλές περιπτώσεις μία φορά το χρόνο ή λιγότερο.

Όταν ληφθεί μια ηλεκτρονική ταυτότητα που συνδέεται σε ένα φυσικό πρόσωπο μπορεί να απαιτηθεί αυτοπρόσωπη εμφάνιση για να αποδειχθεί η ταυτότητα του χρήστη με συμβατικά μέσα, όπως η ταυτότητα. Ωστόσο, είναι δύσκολο να υποστηρίξει κανείς ότι από μια εγγραφή πρέπει να ολοκληρωθεί με κάθε αρχή, η οποία στοχεύει την εισαγωγή της ηλεκτρονικής διακυβέρνησης. Μια απλή εγγραφή, η οποία απαιτεί προσωπική εμφάνιση θα πρέπει να αρκεί. Επιπλέον, ένα σύστημα ταυτοποίησης πρέπει να είναι διαλειτουργικό μεταξύ των διοικήσεων, κατά προτίμηση λαμβάνοντας διασυνοριακές διαδικασίες υπόψη, έτσι ώστε ο πολίτης να μπορεί να χρησιμοποιήσει την ηλεκτρονική του ταυτότητα σε διαφορετικούς φορείς. Η διαλειτουργικότητα και οι διαδιοικητικές χρήσεις της ηλεκτρονικής ταυτοποίησης διακινδυνεύει την προστασία ιδιωτικών δεδομένων, καθώς άσχετες μεταξύ τους υποθέσεις μπορεί να συνδεθούν. Αυτό εγείρει ανησυχίες για την προστασία των δεδομένων, ιδίως με την ταυτοποίηση σε εθνικό επίπεδο.[84]

3.7.1.2. Ομόσπονδες Ταυτότητες

Μία κυβέρνηση θα ήθελε να έχει τη δυνατότητα (είτε μέσω της τεχνολογίας, των επιχειρηματικών πρακτικών, των πολιτικών, της εκπαίδευσης ή από τον συνδυασμό αυτών) να πληρούνται οι ακόλουθες φαινομενικά αντικρουόμενες απαιτήσεις:

- Απλοποίηση της πρόσβασης σε υπηρεσίες και εφαρμογές, τόσο εντός και εκτός ενός οργανισμού
- Μείωση της ανάγκης για διατήρηση και να διαχείριση πολλαπλών συνόλων διαπιστευτηρίων ταυτότητας
- Μείωση του κόστους και της πολυπλοκότητας της διαχείρισης ταυτοτήτων
- Ενεργοποίηση δυναμικής δημιουργίας και τη διαχείριση των έμπιστων σχέσεων

- Διατήρηση της ιδιωτικής ζωής και εξασφάλιση της ασφάλειας των δεδομένων.

Η λύση που προσεγγίζει τις παραπάνω απαιτήσεις είναι *η διαχείριση ομόσπονδης ταυτότητας*. Η διαχείριση ομόσπονδης ταυτότητας καθιστά δυνατή για μια επαληθευμένη ταυτότητα να αναγνωρίζεται και να λαμβάνει μέρος σε εξατομικευμένες υπηρεσίες σε πολλούς τομείς. Η ομόσπονδη ταυτότητα αποφεύγει την παγίδα της κεντρικής αποθήκευσης των προσωπικών πληροφοριών ενώ επιτρέπει στους χρήστες να συνδέσουν τις πληροφορίες ταυτότητας τους ανάμεσα σε διάφορους λογαριασμούς. Δεδομένου ότι οι χρήστες μπορούν να ελέγχουν το πότε και πώς οι λογαριασμοί και τα χαρακτηριστικά τους συνδέονται και μοιράζονται, καταφέρνουν να διατηρούν μεγαλύτερο έλεγχο των προσωπικών τους πληροφοριών. Στην πράξη, αυτό σημαίνει ότι οι χρήστες μπορούν να επικυρώνονται από έναν οργανισμό ή τοποθεσία Web , να αναγνωρίζονται και να λαμβάνουν εξατομικευμένο περιεχόμενο και υπηρεσίες σε άλλους τομείς χωρίς να χρειάζεται να επαναλάβουν τον έλεγχο ταυτότητας. Ολοένα και περισσότερο, οι κυβερνήσεις αναζητούν τις ομόσπονδες ταυτότητες ως την προτιμώμενη αρχιτεκτονική ταυτότητας. Οι ομόσπονδες ταυτότητες παρέχουν στις κυβερνήσεις μια ανοικτή και βασισμένη σε πρότυπα προσέγγιση για τη διευκόλυνση της πρόσβασης σε ευαίσθητους εσωτερικούς πόρους για εξωτερικούς φορείς.

Τα πλεονεκτήματα των ομόσπονδων ταυτότητας περιλαμβάνουν:

- Ένα βασισμένο σε πρότυπα μηχανισμό διαμοιρασμού και διαχείρισης των πληροφοριών ταυτότητας καθώς κινείται μεταξύ διακριτικής νομιμότητας, πολιτικής και οργανωτικών τομέων
- Ένα οικονομικά αποδοτικό μέσο για τη θέσπιση ενιαίου Sign-on σε πόρους μεταξύ τομέων
- Έναν απλούστερο τρόπο για τη χορήγηση και την ανάκληση της πρόσβασης των χρηστών σε πληροφορίες
- Μείωση του αριθμού των Sign-ons και των κωδικών πρόσβασης, με τα οποία ένα άτομο πρέπει να δουλεύει, ώστε να έχει πρόσβαση σε πολλαπλά συστήματα και βάσεις δεδομένων
- Μεγαλύτερη ασφάλεια όταν πρόκειται για την πρόσβαση των χρηστών σε πληροφορίες. [85]

3.7.1.3. Οφέλη για το Δημόσιο Τομέα

- Βελτιωμένες συμμαχίες, τόσο εντός της κυβέρνησης όσο και μεταξύ των κυβερνήσεων, μέσω της διαλειτουργικότητας με αυτονομία.
- Γρηγορότερος χρόνος απόκρισης για τις κρίσιμες επικοινωνίες.
- Αποφυγή του κόστους, τη μείωση του κόστους και την αύξηση της λειτουργικής αποδοτικότητας.

- Ενίσχυση της ασφάλειας και της διαχείρισης κινδύνων.
- Διαλειτουργικότητα και μείωση του χρόνου εγκατάστασης. [86]

3.7.1.4. Πρότυπα

Οι ομόσπονδες ταυτότητες δεν θα γίνουν πανταχού παρόντες, χωρίς να υποστηριχθούν ευρέως από πρότυπα που θα ενεργούν ως απαραίτητο δομικό στοιχείο. Μερικά βασικά πρότυπα είναι τα εξής:

- **SAML**

Η πιο επιτυχημένη ομόσπονδη ταυτότητα, όσον αφορά τα δομικά στοιχεία μέχρι τώρα είναι η Security Assertions Markup Language (SAML) (SAML, n.d.), ένα Extensible Markup Language (XML) πλαίσιο για την ανταλλαγή ασφαλών πληροφοριών μεταξύ των διακομιστών. Η SAML 1.0 έγινε ένα πρότυπο της OASIS, το Νοέμβριο του 2002. Η SAML 1.1 ακολούθησε το Σεπτέμβριο του 2003. Η SAML θεωρείται σημαντική επιτυχία στο πλαίσιο της βιομηχανίας, βλέποντας την επιτυχή ανάπτυξη στον τομέα των χρηματοπιστωτικών υπηρεσιών, της τριτοβάθμιας εκπαίδευσης, της κυβέρνησης και άλλων. Η SAML έχει εφαρμοστεί ευρέως από όλους τους σημαντικούς προμηθευτές διαχείρισης πρόσβασης ιστοσελίδων. Η SAML υποστηρίζεται επίσης σε σημαντικές εφαρμογές προϊόντων διακομιστών, και η υποστήριξη της είναι κοινή μεταξύ των υπηρεσιών διαχείρισης διαδικτύου και των προμηθευτών λογισμικού ασφαλείας. Η SAML 2.0 αντανακλά μια τριπλή σύγκλιση μεταξύ της SAML 1.1, της Liberty ID-FF 1,2 (ID-FF 1,2, 2003) και της Shibboleth [87] και, ως εκ τούτου, είναι μια κρίσιμη εξέλιξη για τις ομόσπονδα πρότυπα.

- **Identity-Federation Framework**

Το 2003, η Liberty Alliance ανέλαβε το πρότυπο SAML 1.0 και πρόσθεσε μηχανισμούς για την σύνδεση λογαριασμών και τη διαχείριση της συνεδρίας για τον προσδιορισμό του Identity Federation Framework. Οι επεκτάσεις, τις οποίες η Liberty ορίζει στο SAML 1.0 (και αργότερα SAML 1.1) συνέβαλαν στην SAML 2.0. Παρά το γεγονός ότι το ID-FF έχει καταργηθεί λόγω της προώθησης της SAML 2.0, η Liberty Alliance εξακολουθεί να βασίζεται στην SAML,το Identity Web Services Framework έχει προσαρμοστεί για να συμπεριλάβει υποστήριξη για τη χρήση ισχυρισμών του SAML 2.0 , ώστε να επικοινωνούν οι ταυτότητες μεταξύ υπηρεσιών Web.

- **WS-Federation**

Μια ξεχωριστή προσπάθεια για πρωτόκολλα ομόσπονδης ταυτότητας είναι η πρωτοβουλία WS-Federation [88]-τμήμα της IBM και της Microsoft WS, για ένα ευρύ φάσμα σύνθετων πρότυπων που αφορούν την ασφάλεια των υπηρεσιών Web. Αν και η WS-Federation δεν έχει η ίδια υποβληθεί σε κάποιο φορέα ανοιχτών προτύπων, η WS-Trust, την οποία η WS- Federation στηρίζεται, τώρα αναπτύσσεται στο πλαίσιο της OASIS' WS-Secure Exchange Technical Committee. Η InfoCard της

Microsoft είναι ένα στοιχείο πελάτη της επόμενης έκδοσης των Windows που μπορεί να δώσει στους τελικούς χρήστες μεγαλύτερο έλεγχο στην ταυτότητά τους με την ένταξη της WS-Trust με την ταυτότητα αιτούντων και παροχών. [89]

3.7.2. Κρυπτογραφία και Κρυπτανάλυση

3.7.2.1. Κρυπτογραφία

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιον τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται κρυπτογράφηση και η αντίστροφή της αποκρυπτογράφηση.

3.7.2.1.1. Συμμετρική και Ασσύμετρη Κρυπτογραφία

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται κρυπτογραφικός αλγόριθμος. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται κρυπτογραφικό σύστημα. Μερικές φορές, ο κρυπτογραφικός αλγόριθμος καλείται και κωδικοποιητής (cipher). Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται κρυπτογραφικά πρωτόκολλα. Υπάρχουν δύο είδη κρυπτογραφικών συστημάτων:

- Τα συμμετρικά συστήματα κρυπτογραφίας
- Τα ασσύμετρα συστήματα κρυπτογραφίας

Συμμετρικό σύστημα κρυπτογραφίας είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά συστήματα κρυπτογραφίας προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά. Τέτοιοι αλγόριθμοι είναι οι εξής: Data Encryption Standard,3-Way ,Blowfish, CAST ,CMEA ,Triple-DES,DEAL FEAL , GOST ,IDEA ,LOKI ,Lucifer,MacGuffin,Twofish, MARS , MISTY ,MMB ,NewDES ,RC2, RC5 , RC6 REDOC , Rijndael ,Safer ,Serpent,SQUARE, Skipjack ,Tiny Encryption Algorithm

- Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα. Τέτοιοι αλγόριθμοι είναι οι εξής: ORYX ,RC4 , SEAL

Το ασύμμετρο σύστημα κρυπτογράφησης ή σύστημα κρυπτογράφησης δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο .Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά. [90]

3.7.2.2. Κρυπτανάλυση

Η κρυπτανάλυση έχει ως στόχο την ανάπτυξη τεχνικών και μεθόδων για την παραβίαση κρυπτογραφημένων μηνυμάτων ή κρυπτογραφικών συστημάτων. Μία επιτυχής κρυπτανάλυση μπορεί να αποκαλύψει το αρχικό από το κρυπτογραφημένο μήνυμα. Μπορεί συγχρόνως να εντοπίσει αδυναμίες σε ένα κρυπτογραφικό σύστημα, οι οποίες οδηγούν τελικά στα παραπάνω αποτελέσματα.
Μία επιχειρούμενη κρυπτανάλυση χαρακτηρίζεται και ως επίθεση (attack). Οι κρυπταναλυτές μπορεί να έχουν στη διάθεσή τους κρυπτογραφημένα μηνύματα, τα αντίστοιχα αρχικά μηνύματα, τους αλγόριθμους κρυπτογράφησης που χρησιμοποιήθηκαν, στατιστικά εργαλεία και τεχνικές, κτλ. Επίσης, θεωρείται ότι ο κρυπταναλυτής γνωρίζει τις λεπτομέρειες του κρυπτογραφικού αλγόριθμου, αν και αυτό δε συμβαίνει πάντα στην πράξη. Η υπόθεση αυτή είναι εύλογη γιατί όπως αναφέρεται συχνά στη βιβλιογραφία, αν η ασφάλεια των κρυπτογραφικών συστημάτων στηρίζεται στη μυστικότητά τους, τότε αυτή δεν μπορεί να είναι επαρκής. Αν στηρίζεται εκτός των άλλων και στη μυστικότητα των αλγορίθμων, κάτι το οποίο δεν συνιστάται, τότε πρόκειται κατά κανόνα για συστήματα με περιορισμένο πεδίο εφαρμογής.

Οι τύποι κρυπταναλυτικών επιθέσεων διαφοροποιούνται σύμφωνα με τους πόρους που έχει στη διάθεσή του ο επιτιθέμενος. Όλοι οι τύποι επιθέσεων προϋποθέτουν ότι ο κρυπταναλυτής γνωρίζει πλήρως τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Στη συνέχεια, παρατίθενται βασικοί τύποι επιθέσεων, οι οποίοι αποτελούν τη βάση αξιολόγησης των κρυπτογραφικών συστημάτων.

- Επίθεση κρυπτογραφημένου κειμένου (Ciphertext – only attack). Ο κρυπταναλυτής έχει στη διάθεσή του αρκετά κρυπτογραφημένα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, μηνύματα και

επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει το αρχικό από το κρυπτογραφημένο μήνυμα.

- Επίθεση γνωστού αρχικού κειμένου (Known – plaintext attack). Ο κρυπταναλυτής έχει στη διάθεσή του όχι μόνο κρυπτογραφημένα μηνύματα αλλά και τα αντίστοιχα αρχικά μηνύματα και επιδιώκει να προσδιορίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων ή κάποιον αλγόριθμο που θα του επιτρέπει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο αρχικό που πλέον δεν γνωρίζει.

- Επίθεση επιλεγμένων αρχικών κειμένων (Chosen – plaintext attack). Οι κρυπταναλυτές έχουν στη διάθεσή τους τα κρυπτογράμματα επιλεγμένων από τους ίδιους αρχικών μηνυμάτων. Ο στόχος είναι να βρεθεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων, ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, τα οποία κρυπτογραφούνται με το ίδιο κλειδί.

- Επίθεση επιλεγμένων κρυπτογραφημένων κειμένων (Chosen – ciphertext attack). Οι κρυπταναλυτές μπορούν να επιλέξουν διάφορα κρυπτογραφημένα μηνύματα και διαθέτουν ακόμα τα αντίστοιχα αρχικά μηνύματα, επιδιώκουν δε τον προσδιορισμό του κλειδιού που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση. [91]

3.7.2.3. Ηλεκτρονικές Υπογραφές

Οι ηλεκτρονικές υπογραφές, οι οποίες είναι κατά κύριο λόγο ασύμμετρες κρυπτογραφικές τεχνικές, χρησιμοποιούνται σε μηχανισμούς γνησιότητας ή αυθεντικοποίησης των επικοινωνούντων (entity authentication) για την επαλήθευση της (ταυτότητας της πηγής) προέλευσης δεδομένων (data origin authentication), την ακεραιότητα δεδομένων (data integrity) και σε υπηρεσίες μη αμφισβήτησης (non-repudiation) αποστολής ή και λήψης μηνυμάτων (ή ηλεκτρονικών εγγράφων), καθώς και δημιουργίας ή τροποποίησής τους. Τα σχήματα ηλεκτρονικών υπογραφών αποτελούνται από τρεις βασικές διεργασίες:

1. Διεργασία δημιουργίας ζεύγους κλειδιών (key generation process), κατά αναλογία με τα ασύμμετρα κρυπτογραφικά συστήματα, του μυστικού κλειδιού (ή του υπογράφοντος κλειδιού) και του δημόσιου κλειδιού (ή του επαληθεύοντος κλειδιού).

2. Διεργασία (ή αλγόριθμος) υπογραφής (signature process) με τη βοήθεια του μυστικού κλειδιού. Αντιστοιχεί στη χρήση του μυστικού κλειδιού από τον κάτοχό του.

3. Διεργασία (ή αλγόριθμος) επαλήθευσης (verification process) με τη βοήθεια του δημόσιου κλειδιού. Αντιστοιχεί στη χρήση του δημόσιου κλειδιού από τους άλλους χρήστες.

Στα σχήματα ψηφιακών υπογραφών τίθενται οι ακόλουθες απαιτήσεις:

1. Πρέπει να είναι υπολογιστικά ανέφικτο για κάποιο χρήστη ο οποίος γνωρίζει μόνο το κλειδί επαλήθευσης να υπολογίσει την υπογραφή ενός μηνύματος.

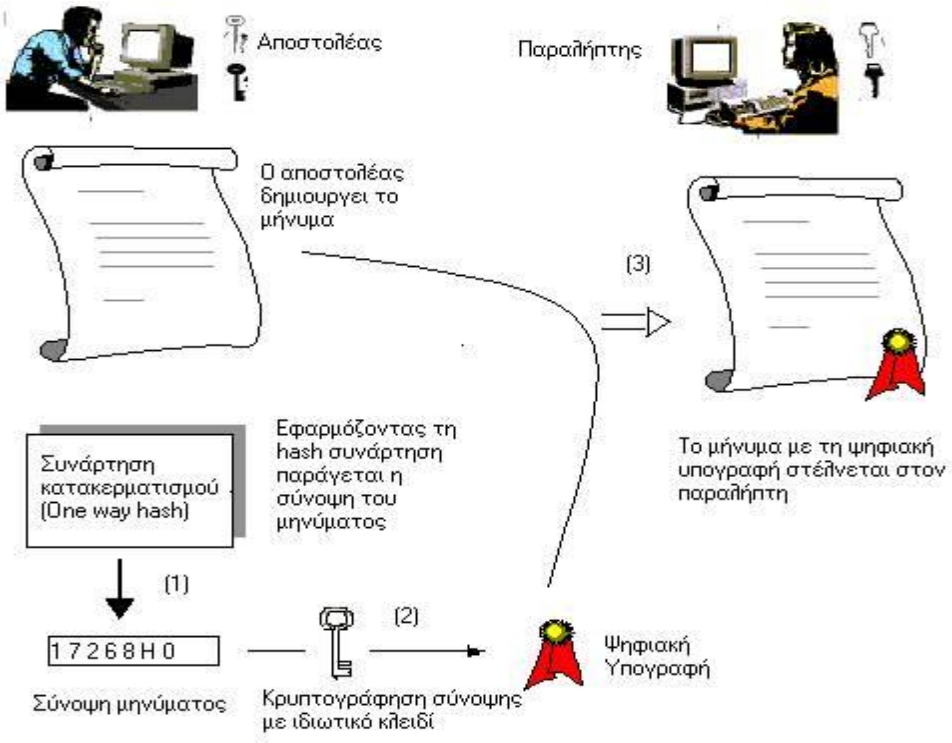
2. Πρέπει να είναι υπολογιστικά ανέφικτο και για τον κάτοχο του κλειδιού υπογραφής να βρει δύο μηνύματα με την ίδια ηλεκτρονική υπογραφή.

3. Όλες οι υπογραφές που υπολογίζονται για διάφορα μηνύματα δεν πρέπει να επτρέπουν σε οποιονδήποτε τρίτο να εξαγάγει το κλειδί υπογραφής ή να μπορεί να υπολογίσει τις ηλεκτρονικές υπογραφές άλλων μηνυμάτων. [92]

3.7.2.3.1. Δημιουργία ψηφιακής υπογραφής

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.
2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).[93]

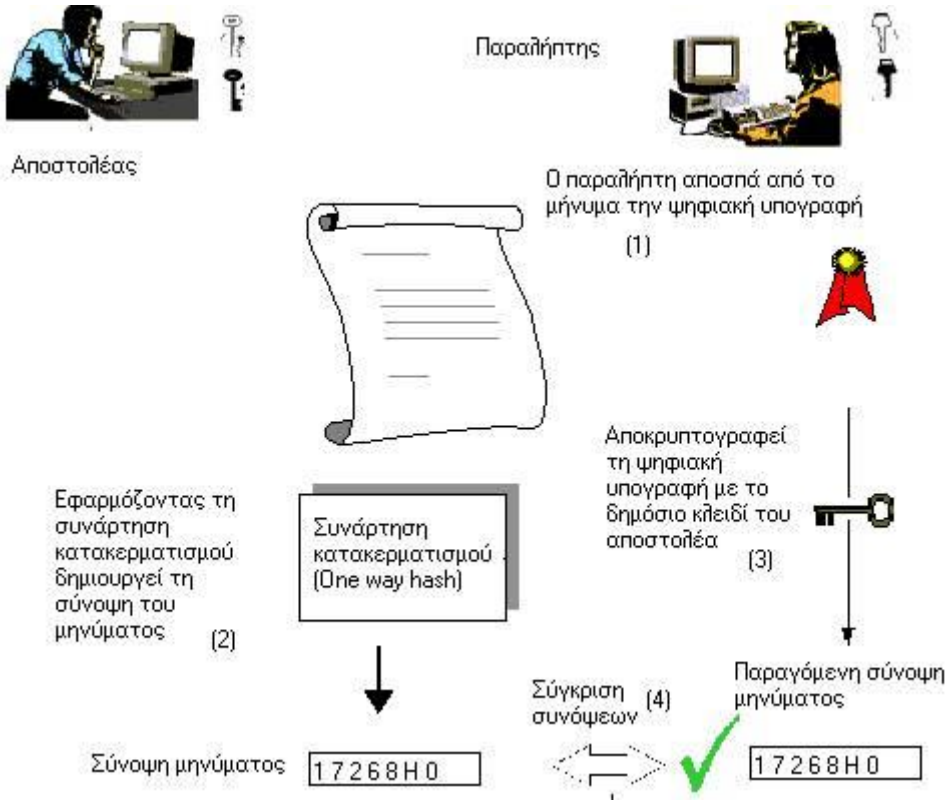


Εικόνα 2 Δημιουργία ψηφιακής υπογραφής

3.7.2.3.2. Επαλήθευση ψηφιακής υπογραφής

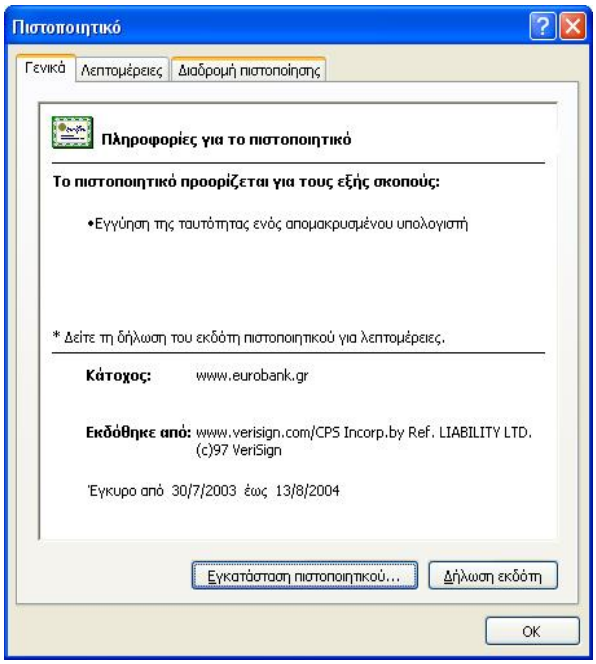
Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).
2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).
4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί. [94]



Εικόνα 3 Επαλήθευση ψηφιακής υπογραφής

3.7.2.4. Ψηφιακά πιστοποιητικά



Εικόνα 4 Ψηφιακό πιστοποιητικό

Τα ψηφιακά πιστοποιητικά είναι δομές δεδομένων, υπογεγραμμένες ψηφιακά, οι οποίες αντιστοιχίζουν κατά μοναδικό τρόπο, μια οντότητα με το δημόσιο κλειδί της. Ένα ψηφιακό πιστοποιητικό περιέχει διάφορα πεδία, μεταξύ των οποίων την ονομασία του ιδιοκτήτη του πιστοποιητικού, το δημόσιο κλειδί του και πιθανότατα κάποια άλλα χαρακτηριστικά. Η δομή του πιστοποιητικού υπογράφεται ψηφιακά από μια έμπιστη οντότητα. Τον ρόλο της έμπιστης οντότητας αναλαμβάνει κατάλληλη οντότητα, ανάλογα με τις ανάγκες της εφαρμογής και τις δυνατότητες της εκάστοτε υποδομής. Στο πλαίσιο της ΥΔΚ, ως έμπιστη οντότητα λειτουργεί η Αρχή Πιστοποίησης (Certification Authority - CA). Η Αρχή Πιστοποίησης βεβαιώνει για την ακεραιότητα του δημόσιου κλειδιού και την αυθεντικότητα της ταυτότητας του φερόμενου ως ιδιοκτήτη του, υπογράφοντας ψηφιακά τη δομή του πιστοποιητικού με το ιδιωτικό της κλειδί. Για τον έλεγχο της εγκυρότητας ενός πιστοποιητικού, υπογεγραμμένου από την Αρχή Πιστοποίησης, απαιτείται, σύμφωνα με τα προαναφερθέντα για τις ψηφιακές υπογραφές, το δημόσιο κλειδί της Αρχής. Ο ενδιαφερόμενος ανακτά το πιστοποιητικό της Αρχής, το οποίο περιέχει το ζητούμενο δημόσιο κλειδί και είναι ψηφιακά υπογεγραμμένο από το αντίστοιχο ιδιωτικό κλειδί. Τα πιστοποιητικά CA είναι τα μοναδικά, που έχουν ως ιδιότητα, να υπογράφονται από το ιδιωτικό κλειδί του ζεύγους κλειδιών, στο οποίο ανήκει το δημόσιο κλειδί που περιέχουν. Για τον λόγο αυτό λέγονται αυτο-υπογεγραμμένα (self-signed) πιστοποιητικά. Μεταξύ των διαφόρων ειδών ψηφιακών πιστοποιητικών συμπεριλαμβάνονται τα X.509 πιστοποιητικά [95] δημόσιου κλειδιού, τα SPKI (Simple Public Key Infrastructure) [96] πιστοποιητικά και τα PGP (Pretty Good Privacy) πιστοποιητικά.[97][98]

3.7.2.5. Υποδομή Δημόσιου Κλειδιού (PKI)

Η Υποδομή Δημόσιου Κλειδιού παρέχει τους μηχανισμούς και τα συστατικά μέρη, που επιτρέπουν τη διάθεση προηγμένων υπηρεσιών ασφάλειας. Οι θεμελιώδεις μηχανισμοί του PKI είναι ο έλεγχος αυθεντικότητας, ο έλεγχος ακεραιότητας και η διατήρηση της εμπιστευτικότητας, μέσω της χρήσης ψηφιακών υπογραφών, ψηφιακών πιστοποιητικών, συμμετρικής και ασύμμετρης

κρυπτογράφησης. Βασικό ρόλο στη λειτουργία της ΥΔΚ έχουν τα ψηφιακά πιστοποιητικά, ως μέσο διανομής και ανάκτησης δημόσιων κλειδιών. Ουσιαστικές, λοιπόν, είναι και οι ανάγκες αναμφισβήτητης συσχέτισης των δημόσιων κλειδιών με τους ιδιοκτήτες τους και απρόσκοπτης ανάκτησης των πιστοποιητικών από τους χρήστες τους. Οι ανάγκες αυτές καλύπτονται από τα συστατικά μέρη της ΥΔΚ, τα οποία και περιγράφονται στη συνέχεια. [99]

3.7.2.5.1. Συστατικά Μέρη Υποδομής Δημόσιου Κλειδιού (PKI Components)

- ***Αρχή Πιστοποίησης (Certification Authority - CA)***

Στο πλαίσιο της Υποδομής Δημόσιου Κλειδιού, η διαδικασία της πιστοποίησης περιλαμβάνει τη συσχέτιση του ονόματος ή άλλου είδους ταυτότητας μιας οντότητας (διεύθυνση IP, όνομα DNS), ενός δημόσιου κλειδιού και πιθανότατα άλλων χαρακτηριστικών της, με μια ψηφιακά υπογεγραμμένη δομή δεδομένων, που αναφέρεται ως πιστοποιητικό δημόσιου κλειδιού. Για την έκδοση των πιστοποιητικών δημόσιου κλειδιού υπεύθυνη είναι η Αρχή Πιστοποίησης. Τα πιστοποιητικά δημόσιου κλειδιού είναι υπογεγραμμένα ψηφιακά με το ιδιωτικό κλειδί της Αρχής. Με την ψηφιακή υπογραφή της Αρχής Πιστοποίησης επιτυγχάνεται η προστασία της ακεραιότητας των πιστοποιητικών δημόσιου κλειδιού. Το περιεχόμενο του πιστοποιητικού βασίζεται, μεταξύ άλλων, σε πληροφορίες που παρέχονται κατά τη διαδικασία εγγραφής (registration). [100]

- ***Αρχή Εγγραφής (Registration Authority - RA)***

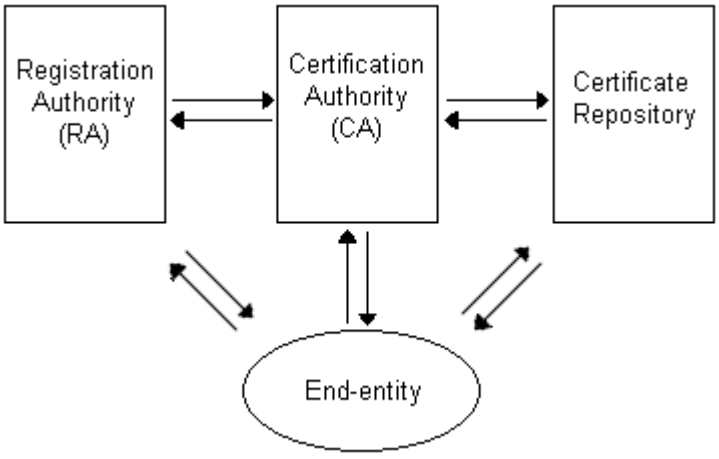
Το πρώτο, απαραίτητο βήμα για να είναι μια οντότητα ικανή να χρησιμοποιήσει τις υπηρεσίες της Υποδομής Δημόσιου Κλειδιού, είναι η εκκίνηση της διαδικασίας έκδοσης πιστοποιητικού. Η πρώτη φάση της διαδικασίας είναι η φάση αρχικοποίησης (initialization phase). Κύριο ρόλο στη φάση αρχικοποίησης παίζει η *Αρχή Εγγραφής*. Κατά την αρχικοποίηση, η Αρχή Εγγραφής επαληθεύει την ταυτότητα της οντότητας που επιχειρεί να αποκτήσει ψηφιακό πιστοποιητικό και υποβάλλει την αίτηση πιστοποιητικού της οντότητας στην Αρχή Πιστοποίησης. Άλλες υπηρεσίες που, ανάλογα με την εφαρμογή, μπορεί να προσφέρει η Αρχή Εγγραφής, είναι η υποστήριξη μεθόδου προσωρινής ασφαλούς πρόσβασης των οντοτήτων για την ολοκλήρωση της φάσης αρχικοποίησης μέσω κοινών μυστικών (shared-secrets), η δημιουργία κλειδιών τελικής οντότητας, η αρχικοποίηση της φάσης ανάκλησης (revocation) πιστοποιητικών και η ανάκτηση κλειδιών (key recovery). Με την ανάθεση των προαναφερθέντων λειτουργιών στην Αρχή Εγγραφής επιτυγχάνεται ελάττωση φόρτου εργασίας της Αρχής Πιστοποίησης, συνεπώς βελτιώνεται η αποδοτικότητα της Υποδομής και περιορίζονται τα λειτουργικά της έξοδα. Παρά τα δυνητικά οφέλη, η ύπαρξη της Αρχής Εγγραφής σε μια ΥΔΚ είναι προαιρετική και ο ρόλος της μπορεί να αναπληρωθεί από την Αρχή Πιστοποίησης. [101]

- ***Αποθετήριο Πιστοποιητικών (Certificate Repository)***

Κατά τη λειτουργία της Υποδομής Δημόσιου Κλειδιού, συχνά προκύπτει η ανάγκη ανάκτησης και επεξεργασίας, από μια οντότητα, πιστοποιητικών δημόσιου κλειδιού που ανήκουν σε τρίτες οντότητες. Στο πλαίσιο της επεξεργασίας μπορεί να περιλαμβάνεται, είτε επαλήθευση ψηφιακών υπογραφών, είτε κρυπτογράφηση δεδομένων για λογαριασμό της τρίτης οντότητας. Τα πιστοποιητικά ανακτώνται από κατάλληλους, ενίοτε δημόσιους, αποθηκευτικούς χώρους πιστοποιητικών, οι οποίοι ονομάζονται *Αποθετήρια Πιστοποιητικών*. Οι χώροι αυτοί έχουν συνήθως τη μορφή καταλόγων LDAP (LDAP directories), οι οποίοι αναλαμβάνουν τη διανομή των πιστοποιητικών δημόσιου κλειδιού. [102]

- ***Τελική Οντότητα (End-entity)***

Ως *τελικές οντότητες* χαρακτηρίζονται οι οντότητες, που έχουν στην ιδιοκτησία τους πιστοποιητικό δημόσιου κλειδιού. Ιδιοκτησία πιστοποιητικού σημαίνει, ότι το πιστοποιητικό αναφέρεται στην τελική οντότητα-ιδιοκτήτη, ενώ το δημόσιο κλειδί που περιέχει και το αντίστοιχο ιδιωτικό ανήκουν στην ίδια τελική οντότητα. Τελική οντότητα μπορεί να είναι είτε φυσικό πρόσωπο, είτε δικτυακός κόμβος, δηλαδή υλικό που περιγράφεται από διεύθυνση δικτύου, όπως εξυπηρετητές ιστού (web servers), firewalls, συσκευές VPN, δρομολογητές (routers), είτε αντικείμενο λογισμικού (software object). [103]



Εικόνα 5: Μια πιθανή μορφή Υποδομής Δημόσιου Κλειδιού

Στην Εικόνα 5 απεικονίζονται τα βασικά συστατικά μέρη μιας ΥΔΚ και οι αλληλεπιδράσεις τους. Παρατηρούμε την Αρχή Πιστοποίησης, την Αρχή Εγγραφής, το Αποθετήριο Πιστοποιητικών και μια τελική οντότητα. [104]

3.7.3. Στενογραφία και Στεγανάλυση

3.7.3.1. Στεγανογραφία

Ο Markus Kahn [105] ορίζει την στεγανογραφία (steganography) σαν την τέχνη και την επιστήμη της επικοινωνίας κατά τρόπο που κρύβει η ύπαρξη της επικοινωνίας. Σε αντίθεση με την κρυπτογραφία, όπου ο εχθρός έχει τη δυνατότητα να ανιχνεύει, να συλλαμβάνει και να τροποποιεί μηνύματα χωρίς να είναι σε θέση να παραβιάσει ορισμένες εγκαταστάσεις ασφαλείας που εγγυώνται από ένα κρυπτογραφικό σύστημα, ο στόχος της στεγανογραφίας είναι να κρύψει τα μηνύματα μέσα σε άλλα αθώα μηνύματα με έναν τρόπο που δεν επιτρέπει στον εχθρό να ανιχνεύσει ακόμη και το ότι υπάρχει ένα δεύτερο μήνυμα από πίσω. Αυτός ο ορισμός έχει γίνει ευρέως αποδεκτός στη κοινότητα της ασφάλειας των πληροφοριών. Η εφαρμογή της στεγανογραφίας μπορεί να αναχθεί από τους αρχαίους χρόνους. Σύμφωνα με τον Ηρόδοτο το 499 π.Χ, ο Histiaus ξύρισε το κεφάλι του πιο έμπιστου δούλου του και έκανε ένα τατουάζ με ένα σημαντικό μήνυμα στο τριχωτό της κεφαλής του. Όταν τα μαλλιά του σκλάβου, μεγάλωσαν πάλι, οι πληροφορίες κρύφτηκαν και ο δούλος εστάλη στον Αρισταγόρα, ο οποίος, στη συνέχεια, ξύρισε το κεφάλι του σκλάβου και πάλι αποκαλύφθηκε το μήνυμα, που του έδωσε εντολή να επαναστατήσει ενάντια στους Πέρσες. Αυτό είναι ίσως το παλαιότερο παράδειγμα της στεγανογραφίας. Με το πέρασμα του χρόνου η τεχνική βελτιώθηκε, το αόρατο μελάνι και τα μικροφίλμ εμφανίστηκαν στις σύγχρονες εφαρμογές. Το υδατογράφημα σε χαρτονομίσματα είναι το πιο κοινό σύγχρονο παράδειγμα της στεγανογραφίας.[106]

Στο σύγχρονο κόσμο, η στεγανογραφία είναι μια τεχνολογία συγκαλυμμένης επικοινωνίας που επιτρέπει τις μυστικές πληροφορίες να κρύβονται σε μηνύματα κάλυψης και μέσα ενημέρωσης. Το μήνυμα που προκύπτει με την κρυμμένη πληροφορία καλείται το stego μήνυμα. Οι τεχνικές στεγανογραφίας μπορούν να χωριστούν σε δύο ευρείες κατηγορίες:

- την ψηφιακή υδατογράφηση και
- τα ψηφιακά αποτυπώματα.

Η ψηφιακή υδατογράφηση επικεντρώνεται στην ενσωμάτωση αλγορίθμων και χρησιμοποιείται για τους σκοπούς της προστασίας των πνευματικών δικαιωμάτων, της ταυτότητας και την επαλήθευση της ακεραιότητας. Οι κρυφές πληροφορίες, δηλαδή, το υδατογράφημα, σε ψηφιακή υδατογράφηση είναι σχετικά απλές, συνήθως η ψηφιακή υπογραφή του ιδιοκτήτη ή ένα μοτίβο που παράγεται με ένα μυστικό κλειδί.

Η ψηφιακή αποτύπωση επικεντρώνεται στην μέθοδο (μερικές φορές αναφέρεται ως πρωτόκολλο) της παραγωγής της κρυφής πληροφορίας, δηλαδή το δακτυλικό αποτύπωμα, έτσι ώστε να ανταποκρίνονται στις απαιτήσεις όπως η μοναδικότητα και τα πλαστά δικαιολογητικά.

Οι τεχνικές ψηφιακών αποτυπωμάτων χρησιμοποιούν πάντα τεχνικές υδατογράφησης για να ενσωματώσουν το παραγόμενο ψηφιακό αποτύπωμα. Με άλλα λόγια, η ουσιαστική διαφορά μεταξύ αυτών των δύο κατηγοριών είναι ότι το ψηφιακό αποτύπωμα που ενσωματώθηκε από τεχνικές ψηφιακών αποτυπωμάτων είναι μοναδικό για κάθε αντίγραφο του καλυπτόμενου μηνύματος, ενώ το υδατογράφημα που χρησιμοποιείται από τεχνικές υδατογράφησης είναι πάντα ίδιο για όλα τα αντίγραφα του κρυφού μηνύματος και σχετίζεται με το κρυφό μήνυμα και τον ιδιοκτήτη του. Διαφορετικά συστήματα των δύο αυτών κατηγοριών επίσης, έχουν και άλλες ειδικές λειτουργίες για να ικανοποιήσουν τις συγκεκριμένες ανάγκες των εφαρμογών τους. Μερικές άλλες κοινές ιδιότητες της τεχνολογίας της στεγανογραφίας είναι οι εξής:

- **Διαφάνεια:** Η παραμόρφωση που παράγεται από την ενσωμάτωση της διαδικασίας πρέπει να είναι ανεπαίσθητη για τους ανθρώπους έτσι ώστε η επίπτωση στην αντιληπτή ποιότητα να είναι ελάχιστη.

- **Ανθεκτικότητα:** Για τις περισσότερες εφαρμογές, όπως η προστασία των πνευματικών δικαιωμάτων, η ικανότητα επιβίωσης έναντι όλων των ειδών κακόβουλων επιθέσεων και άλλες παρεπόμενες πράξεις χειραγώγησης, όπως η συμπίεση με απώλεια και μορφές διευρωπαϊκής-κωδικοποίησης, πρέπει να διατηρηθούν εκτός εάν οι χειρισμοί έχουν καταστήσει κατά μια έννοια άχρηστο το περιεχόμενο.

- **Ωφέλιμο φορτίο:** Ωφέλιμο φορτίο (δηλαδή, η ικανότητα ενσωμάτωσης) είναι σημαντικό για τα ψηφιακά δακτυλικά αποτυπώματα. Δεδομένου ότι η λειτουργία των δακτυλικών αποτυπωμάτων είναι να εντοπίσει τον παραλήπτη / αγοραστή, το δακτυλικό αποτύπωμα πρέπει να είναι αρκετά μακρύ ώστε να είναι δυνατή η διασφάλιση της μοναδικότητας όταν ένας τεράστιος αριθμός από αντίγραφα του μηνύματος πρόκειται να διανεμηθούν. Στην περίπτωση αυτή, η ικανότητα ενσωμάτωσης είναι ο προσδιοριστικός παράγοντας για ένα αποτελεσματικό σύστημα δακτυλικών αποτυπωμάτων [107].[108]

3.7.3.2. Ψηφιακή Υδατογράφηση

Η ιδέα της ψηφιακής υδατογράφησης είναι να ενσωματώσει ένα μικρό ποσό των μυστικών πληροφοριών, το υδατογράφημα, σε μέσα υποδοχής για την επίτευξη των στόχων, όπως τον ισχυρισμό πνευματικών δικαιωμάτων, την αυθεντικοποίηση και την επαλήθευση της ακεραιότητας του περιεχομένου, και ούτω καθεξής. Η ανωτερότητα της ψηφιακής υδατογράφησης σε σχέση με την κρυπτογραφία είναι ότι η τελευταία δεν παρέχει καμία προστασία αφότου αποκρυπτογραφηθεί το περιεχόμενο, ενώ η πρώτη παρέχει "έμπιστη" προστασία ανά πάσα στιγμή, επειδή το υδατογράφημα

έχει αποτελέσει αναπόσπαστο κομμάτι των μέσων υποδοχής. Όλες οι δυνατότητες ενός συστήματος υδατογράφησης, συμπεριλαμβανομένης της ισορροπίας μεταξύ της διαφάνειας και της ανθεκτικότητας ώστε να αποφευχθούν τυχόν αισθητά τεχνουργήματα και οι άλλες ιδιότητες για την κάλυψη των δικών του ειδικών εφαρμογών, εξαρτώνται από το σχεδιασμό του ενσωματωμένου αλγορίθμου. Για να βελτιστοποιήσει την απόδοση, ο ενσωματωμένος αλγόριθμος είναι πάντα ειδικά σχεδιασμένος για έναν ορισμένο τύπο μέσων, όπως την εικόνα, το βίντεο, τον ήχο κ.ά., για να αποφευχθεί κάθε πιθανό κενό ασφαλείας. Τα ψηφιακά υδατογραφικά συστήματα μπορούν να ταξινομηθούν σε τρεις κατηγορίες:

- *ισχυρή υδατογράφηση,*
- *ημι-εύθραυστη υδατογράφηση και*
- *εύθραυστη υδατογράφηση.*

Η ισχυρή υδατογράφηση προορίζεται για τις εφαρμογές της προστασίας της πνευματικής ιδιοκτησίας και διαχείρισης ψηφιακών δικαιωμάτων (DRM), όπου μέσα στο υδατογράφημα περιέχονται πληροφορίες πνευματικών δικαιωμάτων που θα πρέπει να μπορούν να ανιχνευτούν μετά από επιθέσεις που στοχεύουν στην διαγραφή του υδατογραφήματος, διατηρώντας την αξία του μέσου υποδοχής. Οι Cox, Kilian, Leighton, και Shamoon [109] πρότειναν την έννοια του εκτεταμένου φάσματος υδατογραφήματος (spread-spectrum watermarking), η οποία ενέπνευσε ένα μεγάλο αριθμό έργων στον τομέα αυτό. Υιοθετημένη από τη θεωρία της επικοινωνίας, η ιδέα του υδατογραφήματος εκτεταμένου φάσματος είναι να χειριστεί το χαμηλής ενέργειας υδατογράφημα το οποίο θεωρείται ένα σήμα στενής ζώνης και να το εξαπλώσει σε πολλαπλά στοιχεία στο φάσμα των μέσων υποδοχής, το οποίο θεωρείται ως ένα σήμα ευρείας ζώνης. Με την εξάπλωση της υδατογράφησης σε όλο το φάσμα, η ενέργεια του υδατογραφήματος σε μια συχνότητα του σήματος είναι περιορισμένη, και ως εκ τούτου η αντοχή είναι διασφαλισμένη, ακόμη και όταν ορισμένα στοιχεία συχνότητας λείπουν. Ωστόσο, η υψηλή αντοχή των εκτεταμένου φάσματος υδατογραφημάτων επιτυγχάνεται εις βάρος των χαμηλών ωφέλιμων φορτίων, έτσι δεν είναι αρκετά κατάλληλο για το σκοπό των ψηφιακών δακτυλικών αποτυπωμάτων. Για να βελτιώσει περισσότερο την αξιοπιστία χωρίς να προκαλεί περισσότερα τεχνουργήματα, τα ανθρώπινα μοντέλα αντίληψης (HPM), συμπεριλαμβανομένων του ανθρώπινου συστήματος όρασης (HVS) και το ανθρώπινο ακουστικό σύστημα (HAS), έχουν προταθεί και έχουν ενσωματωθεί στην διαδικασία ενσωμάτωσης υδατογραφήματος [110]. Εφικτά αντιληπτικά μοντέλα διευκολύνουν την προσαρμογή υδατογραφήματος σε κατασκευαστικά εξαρτήματα, όπου τα ανθρώπινα μοντέλα αντίληψης (HPM) είναι λιγότερο ευαίσθητα.

Η ημι-εύθραυστη και η εύθραυστη υδατογράφηση έχουν αναπτυχθεί για τους σκοπούς της πιστοποίησης και της επαλήθευσης της ακεραιότητας του περιεχομένου, στην οποία το ενσωματωμένο υδατογράφημα αναμένεται να καταστραφούν όταν πραγματοποιηθούν οι επιθέσεις, έτσι ώστε να σημάνει ο συναγερμός από τον ανιχνευτή όταν αποτύχει να εξάγει το υδατογράφημα. Η διαφορά μεταξύ αυτών των δύο υπο-κατηγοριών είναι ότι οι ημι-εύθραυστη υδατογράφηση αντιμετωπίζει κάποιων συγκεκριμένων λειτουργιών, ως μη-κακόβουλες ενέργειες, ενώ η εύθραυστη

υδατογράφηση αντιμετωπίζει όλα τα είδη των χειρισμών ως κακόβουλες ενέργειες. Τα πλαστά αποδεικτικά είναι ένας βασικός στόχος των ημι- εύθραυστων συστημάτων υδατογράφησης. Οι επιθέσεις παραχάραξης, όπως η αποκοπή-επικόλληση, οι επιθέσεις κβαντοποίησης διανύσματος και οι επιθέσεις μεταμόσχευσης, οι οποίες αντικαθιστούν περιοχές / τμήματα των υδατογραφημένων μέσων με ψεύτικα τμήματα. Αυτό το πρόβλημα μπορεί να επιλυθεί μέσω της συσχέτισης παρακείμενων περιοχών/τμημάτων των μέσων κατά τη διάρκεια της διαδικασίας ενσωμάτωσης, ώστε όταν γειτονικά τμήματα αντικαθίστανται αυτές θα σημάνουν συναγερμό κατά τη διαδικασία επαλήθευσης, εάν οι αυθεντικές περιοχές λείπουν.

Ενώ υπάρχουν πολλά συστήματα υδατογράφησης εικόνων, ήχου και βίντεο, τα συστήματα για το κείμενο σπανίζουν. Δυστυχώς, το κείμενο είναι το κυρίαρχο είδος δεδομένων στις ηλεκτρονικές κυβερνήσεις. Μερικά δημοσιευμένα συστήματα, όπως αυτά που αναπτύχθηκαν από τον Huang και Yan (2001), επικεντρώνονται στην τροποποίηση του σχηματισμού των ψηφιακών εγγράφων, όπως το μέγεθος της γραμματοσειράς, το διάστιχο και η σελιδοποίηση. Αυτές οι τροποποιήσεις είναι ανεπαίσθητες στο ανθρώπινο μάτι, αλλά μπορούν να ανιχνευθούν από τον αποκωδικοποιητή ακόμα και μετά την εκτύπωση και τη δημιουργία αρκετών φωτοαντιγράφων. Ωστόσο, αυτός ο τύπος συστήματος εξαρτάται από τον σχηματισμό των εγγράφων τόσο πολύ, που η εκ νέου πληκτρολόγηση του κείμενου είναι πάντα μια αποτελεσματική, αν και δύσκολη, επίθεση. Οι επιτιθέμενοι με ένα σύστημα οπτικής αναγνώρισης χαρακτήρων (OCR), το οποίο σαρώνει και ψηφιοποιεί έντυπα, θα διαπιστώσουν ότι το να νικήσεις την ασφάλεια του υδατογραφήματος των εγγράφων κειμένου είναι κάτι πολύ εύκολο. Για αυτόν το λόγο χρειάζεται μεγαλύτερη προσπάθεια, έτσι ώστε να αυξηθούν τα επίπεδα ασφαλείας στον τομέα αυτό.[111]

3.7.3.3. Ψηφιακά αποτυπώματα

Το ψηφιακό αποτύπωμα είναι ένα μοναδικό μοτίβο/μήνυμα ενσωματωμένο στο μέσο υποδοχής, το οποίο σα σκοπό έχει τον εντοπισμό του παραλήπτη. Το ψηφιακό αποτύπωμα δεν μπορεί να αντισταθεί στην παράνομη αντιγραφή, αλλά επιτρέπει στους κατόχους πνευματικών δικαιωμάτων ή στους διανομείς των μέσων να εντοπίσουν τους δικαιούχους που διαρρέουν ή αναδιανέμουν το μέσο με το δακτυλικό αποτύπωμα. Ένα *σημείο* είναι μια θέση στο μέσο υποδοχής, το οποίο μπορεί να λάβει μία από τις τιμές k, και το *αποτύπωμα* είναι μια συλλογή σημάτων l. Ως εκ τούτου, ένα σύνολο από k * l αντιγράφων με αποτύπωμα του μέσου υποδοχής μπορούν να παραχθούν. Ένας *διανομέας* παρέχει νόμιμα αντίγραφα με διαφορετικά αποτυπώματα στους χρήστες, και ένας *προδότης*, είναι ο χρήστης που παράνομα αναδιανέμει το αντίγραφο του ή της στον πιθανό *εισβολέα*. Η κύρια ευπάθεια των συστημάτων ψηφιακών αποτυπωμάτων είναι η πιθανότητα μιας συνεννοημένης επίθεσης, στην οποία ένας αρκετά μεγάλος αριθμός αντιγράφων με αποτύπωμα συλλέγονται για την ανίχνευση μερικών σημείων που διαφέρουν σε περισσότερα από ένα από τα συλλεγόμενα αντίγραφα. Βάσει αυτών των σημείων, η ισχύς των αποτυπωμάτων μπορεί να ελαττωθεί με το μέσο όρο των τιμών των σημείων, ώστε να δημιουργηθεί ένα νέο αντίγραφο που δεν

θα φέρει κανένα ίχνος των ταυτοτήτων των συνεννοουμένων. Επομένως, μια πρόσθετη απαίτηση για τα ψηφιακά αποτυπώματα είναι κατά της συνεννόησης, κάτι το οποίο σημαίνει ότι ακόμα και αφότου οι επιτιθέμενοι έχουν συγκεντρώσει έναν επαρκή αριθμός νόμιμων αντιγράφων, ακόμα δεν μπορούν να ανιχνεύσουν και θα μετριάσουν τα αποτυπώματα. Τα ψηφιακά αποτυπώματα είναι εφαρμόσιμα στον *εντοπισμό του προδότη* (traitor tracing) και την *προστασία της ανωνυμίας (anonymity protection)*. Η ιδέα της ανίχνευσης του προδότη είναι αρκετά απλή[112]. Τα εμπιστευτικά δεδομένα ασφαλίζονται με την έλεγχο της πρόσβασης και όποιος έχει το δικαίωμα να έχει πρόσβαση στα δεδομένα πρέπει να έχει την ταυτότητά του ή τον κωδικό πρόσβασης τα οποία είναι γνωστά στο κεντρικό σύστημα. Το κεντρικό σύστημα θα μπορούσε να δημιουργήσει το ψηφιακό αποτύπωμα, σύμφωνα με αυτή την ταυτότητα και να το ενσωματώσει στο αντίγραφο πριν από την κρυπτογράφηση των δεδομένων και πριν επιτρέψει τα δεδομένα με το ψηφιακό αποτύπωμα να ανακτηθούν ή να αποσταλούν μέσω του δικτύου. Σε περίπτωση που τα δεδομένα με το ψηφιακό αποτύπωμα πρέπει να διαρρεύσουν, ο προδότης θα μπορούσε να εντοπιστεί με τον έλεγχο του ψηφιακού αποτυπώματος. Μια άλλη εκτεταμένη εφαρμογή αυτής της ιδέας είναι η διανομή του εγγράφου ανίχνευσης. Όπως γνωρίζουμε, η αποστολή ενός ευαίσθητου εγγράφου μέσω ενός καναλιού στον προορισμό/παραλήπτη θα πρέπει να ακολουθήσει μια διαδικασία καταγραφής και παρακολούθησης. Για την πρόληψη της διανομής πλαστών εγγράφων μέσω του καναλιού, κάθε μονάδα/κόμβος στο κανάλι θα πρέπει να ενσωματώσει το ψηφιακό του αποτύπωμα κατά το πέρασμα του εγγράφου, και η επόμενη μονάδα επαληθεύει όλα τα ψηφιακά αποτυπώματα που το έγγραφο θα πρέπει να μεταφέρει. Αν όλα τα ψηφιακά αποτυπώματα είναι παρόντα, το έγγραφο αυτό θεωρείται επικυρωμένο (authenticated) αν όχι, είναι πλαστό και η πηγή μπορεί να εντοπιστεί βάσει στα υπάρχοντα ψηφιακά αποτυπώματα. Λαμβάνοντας υπόψη το γεγονός ότι η χωρητικότητα ενσωμάτωσης είναι περιορισμένη, το πρόβλημα της παραπάνω ιδέας είναι ότι όταν είναι ενσωματωμένα πάρα πολλά ψηφιακά αποτυπώματα σε ένα μέσο, η ανταπόκριση του κάθε ψηφιακού αποτυπώματος στον ανιχνευτή μπορεί να μειωθεί κάτω από το όριο έτσι ώστε να μην μπορούν να αναγνωριστούν. Ένα άλλο πρόβλημα είναι να υπάρξει διάκριση της ακολουθίας της ενσωμάτωσης των ψηφιακών αποτυπωμάτων.

Η ψήφος είναι ένα σημαντικό όχημα για την εξακρίβωση της δημόσιας γνώμης. Οι ανησυχίες γύρω από την αποτελεσματικότητα, την ακρίβεια και της δικαιοσύνης των παραδοσιακών εκλογών βάσει των χάρτινων ψηφοδελτίων πάντα υπήρχαν. Για να ξεπεραστούν αυτά τα προβλήματα, τα ηλεκτρονικά συστήματα ψηφοφορίας έχουν υποστεί ανάπτυξη τα τελευταία χρόνια. Ωστόσο, ο πιθανός αντίκτυπος της παραβίασης της ασφάλειας των συστημάτων ηλεκτρονικής ψηφοφορίας είναι πολύ μεγαλύτερη από ό, τι με τα παραδοσιακά συστήματα ψηφοφορίας. Η χρήση των ψηφιακών αποτυπωμάτων θα μπορούσε να είναι μεγάλης σημασίας στην άμβλυνση των προβλημάτων αυτών. Μια περίπτωση παρόμοια με την ηλεκτρονική ψηφοφορία είναι η ανώνυμη αναφορά, η οποία βοηθά τις κυβερνήσεις στην καταπολέμηση της διαφθοράς και του εγκλήματος. Τα κοινά σημεία αυτών των δύο περιπτώσεων είναι ότι οι άνθρωποι δεν θέλουν να αποκαλύψουν την ταυτότητά τους και η κυβέρνηση πρέπει να διασφαλίσει ότι η ανώνυμη δράση είναι αξιόπιστη και δεν είναι κακόβουλη. Οι Pfitzmann και Waidner [113] εισήγαγαν την ιδέα των ανώνυμων ψηφιακών αποτυπωμάτων. Ένα τρίτο μέρος, δηλαδή ένα κέντρο εγγραφής, ενημερώνει την κυβέρνηση για την υπογραφή του, και η ανώνυμος πρέπει να εγγραφεί με το κέντρο σε ένα πρωτόκολλο καταχώρισης στην οποία αυτός ή

αυτή πρέπει να αποδείξει την ταυτότητά του και να πάρει ένα πιστοποιητικό από το κέντρο. Αυτό το πιστοποιητικό είναι εγγεγραμμένο στο κέντρο, αλλά δεν περιέχει καμία πληροφορία προς δημοσιοποίηση σχετικά με τον κάτοχο. Κατά τη διάρκεια της ψηφοφορίας ή της υποβολής αναφοράς, ο ανώνυμος και η κυβέρνηση αλληλεπιδρούν σε ένα πολυκομματικό πρωτόκολλο. Ο ανώνυμος πρέπει να παρουσιάσει το πιστοποιητικό το οποίο είναι υπογεγραμμένο από το κέντρο και παίρνει ένα αποδεικτικό με ψηφιακό αποτύπωμα. Η κυβέρνηση δημιουργεί το ψηφιακό αποτύπωμα από το πιστοποιητικό του ανώνυμου και διατηρεί το δακτυλικό αποτύπωμα ως αποδεικτικό στοιχείο, αλλά στην πραγματικότητα δεν ξέρει τίποτα για την πραγματική ταυτότητα του ανώνυμου. Αν περαιτέρω επαλήθευση είναι αναγκαία, η κυβέρνηση θα μπορούσε να αφαιρέσει το πιστοποιητικό από το ψηφιακό αποτύπωμα και να το δείξει στο κέντρο καταχώρισης ως απόδειξη της αντίστοιχης ταυτότητας. [114]

3.7.3.4. Στεγανάλυση (Steganalysis)

Λειτουργώντας όπως η παραδοσιακή κυβέρνηση, μια ηλεκτρονική διακυβέρνηση έχει την ευθύνη της παρακολούθησης της ροής των δημόσιων δεδομένων. Επί του παρόντος, οι περισσότερες κυβερνήσεις πιστεύουν ότι ο περιορισμός της δύναμης του δημόσιου κρυπτοσυστήματος ή απαγόρευσή του είναι επαρκές για τη διασφάλιση της εθνικής ασφάλειας. Για παράδειγμα, η κυβέρνηση των Ηνωμένων Πολιτειών (ΗΠΑ) περιόρισε την Microsoft Co όσον αφορά την πώληση του Internet Explorer,του οποίου το λογισμικό είχε τα υψηλότερα επίπεδα κρυπτογράφησης (128-bit) πριν χαλαρώσει τον έλεγχο των εξαγωγών το 2000. Ένα άλλο παράδειγμα είναι αυτό της PGP, ένα επιτυχημένο κρυπτογραφικό σύστημα, επίσης απαγορεύτηκε από την κυβέρνηση των ΗΠΑ ταυτόχρονα. Από την άποψη της κυβέρνησης, αυτό μπορεί να είναι ένα λογικό βήμα από την στιγμή που υπάρχει ανησυχία για την εθνική ασφάλεια . Ωστόσο, αφήνει την πλειοψηφία των χρηστών του Διαδικτύου εκτεθειμένους σε παραβιάσεις της ιδιωτικής ζωής τους. Η κατάσταση αυτή οδηγεί το κοινό να καταφύγει στη στεγανογραφία για την προστασία της ιδιωτικής ζωής τους. Επειδή η στεγανογραφία δουλεύει κατά τέτοιο ανεπαίσθητο τρόπο, οι κυβερνήσεις θα πρέπει να αντιμετωπίσουν πολλές δυσκολίες στην ανίχνευση μυστικών επικοινωνιών. Η αδυναμία της ανίχνευσης συγκεκαλυμμένων επικοινωνιών μεταξύ διεθνών τρομοκρατών, για παράδειγμα, θα μπορούσε να είναι καταστροφική. Έτσι η στεγανάλυση (steganalysis), το αντίθετο της στεγανογραφίας, μπορεί να θεωρηθεί ακόμα πιο σημαντική από ότι η στεγανογραφία από την προοπτική του ηλεκτρονικού θέματος εθνικής ασφάλειας.

Η στεγανάλυση είναι η τέχνη και η επιστήμη που χρησιμοποιείται για την ανίχνευση ή την παρεμβολή σε κρυφές επικοινωνίες, οι οποίες χρησιμοποιούν τις τεχνικές της στενογραφίας. Η στεγανάλυση περιλαμβάνει τρία στάδια:

- αναζήτηση ύποπτων στοιχείων,
- εξόρυξη του κρυφού μηνύματος

- και καταστροφή του μηνύματος

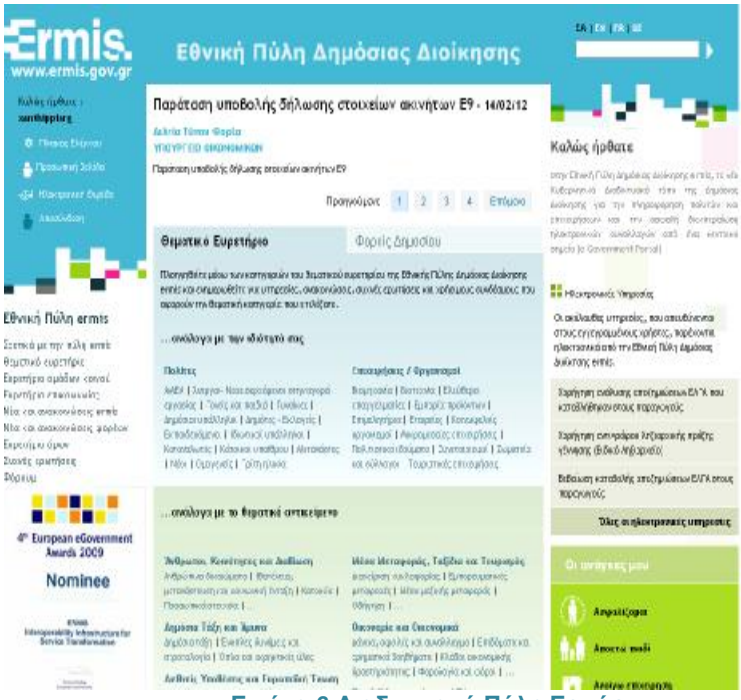
Ενώ η ανάπτυξη αλγόριθμων στεγανάλυσης για ένα συγκεκριμένο σύστημα στεγανογραφίας είναι δυνατή, δεν υπάρχει κάποια συστηματική θεωρία ή γενική τεχνική στεγανάλυσης ακόμα διαθέσιμη. [115]

Κεφάλαιο 4
Παρουσίαση και Σύγκριση Κυβερνητικών Ιστοσελίδων Προσβασιμότητα-Ασφάλεια

Το παρόν κεφάλαιο σκοπό έχει την παρουσίαση κα τη σύγκριση των πιο σημαντικών κυβερνητικών Διαδικτυακών τόπων, οι οποίοι παρέχουν ηλεκτρονικές υπηρεσίες προς τους πολίτες, τις επιχειρήσεις και άλλους δημόσιους φορείς. Στόχος είναι να διαπιστωθεί κατά πόσο οι κυβερνητικές ιστοσελίδες και οι πύλες ηλεκτρονικής διακυβέρνησης εξασφαλίζουν την προσβασιμότητα και την ασφάλεια των συναλλαγών καθώς και των προσωπικών δεδομένων των πολιτών. Ως εκ τούτου οι σελίδες αυτές θα εξεταστούν ως προς αυτά τα σημεία, την προσβασιμότητα και την ασφάλεια.

4.1. Εθνικής Πύλης Δημόσιας Διοίκησης "Ermis"

Η Εθνική Πύλη Δημόσιας Διοίκησης Ermis αποτελεί την ενιαία Κυβερνητική Διαδικτυακή Πύλη της Δημόσιας Διοίκησης για την πληροφόρηση πολιτών και επιχειρήσεων και την ασφαλή διεκπεραίωση υπηρεσιών ηλεκτρονικής διακυβέρνησης. Ο Ermis αποσκοπεί, μέσα από ένα σύνολο δράσεων, στο γενικότερο εκσυγχρονισμό της Δημόσιας Διοίκησης και στην παροχή υπηρεσιών προστιθέμενης αξίας προς τον πολίτη.



Εικόνα 6 Διαδικτυακή Πύλη Ερμής

Η Κυβερνητική Πύλη παρέχει από ένα κεντρικό σημείο ολοκληρωμένη ενημέρωση στους πολίτες και τις επιχειρήσεις σχετικά με όλες τις συναλλαγές τους με την Δημόσια Διοίκηση (φυσικές ή ηλεκτρονικές), καθώς και επιλεγμένες υπηρεσίες Ηλεκτρονικών Συναλλαγών μέσω των οποίων οι πολίτες μπορούν ηλεκτρονικά πλέον να εξυπηρετηθούν από την Δημόσια Διοίκηση. Από

επιχειρησιακής πλευράς, η πύλη Ermis αποτελεί το «ηλεκτρονικό πολυκατάστημα» της Δημόσιας διοίκησης και κινείται σε τρεις βασικούς άξονες που αφορούν:

1. Παροχή πληροφοριών

Η παροχή πληροφοριών αφορά την ολοκληρωμένη συλλογή και οργάνωση της απαιτούμενης πληροφορίας από το σύνολο της Δημόσιας Διοίκησης και την διάθεσή της στο Διαδίκτυο για την αξιόπιστη ενημέρωση πολιτών και επιχειρήσεων όσον αφορά στις συναλλαγές τους και στην αλληλεπίδρασή τους με τον κρατικό μηχανισμό.

Η πληροφορία είναι διαθέσιμη προς το κοινό με 5 διαφορετικούς τρόπους αναζήτησης:

- Από την ενότητα «Οι Ανάγκες μου» μέσω της οποίας είναι διαθέσιμες όλες οι υπηρεσίες/πληροφορίες που σχετίζονται με μια συγκεκριμένη ανάγκη ή γεγονός (π.χ. «Ασφαλίζομαι» , «Ταξιδεύω», «Έχασα το πορτοφόλι μου»).
- Από την ενότητα «Ανάλογα με το Θεματικό Αντικείμενο» μέσω του Θεματικού Ευρετηρίου, στην οποία το σύνολο της πληροφορίας είναι οργανωμένο σύμφωνα με το Θεματικό Αντικείμενο στο οποίο ανήκει το κάθε Θεματικό Αντικείμενο (π.χ. «Άνθρωποι, Κοινότητες και Διαβίωση») , διαιρείται σε αντίστοιχες υποκατηγορίες , για την καλύτερη οργάνωση και προβολή των πληροφοριών (π.χ. Οικογένεια, Κατοικία, Μητρώα και Δημοτολόγιο).
- Από την ενότητα «ανάλογα με την ιδιότητά σας» μέσω του Θεματικού Ευρετηρίου όπου είναι διαθέσιμες όλες οι υπηρεσίες/πληροφορίες που αφορούν σε μια συγκεκριμένη ιδιότητα πολίτη (π.χ. «Δημόσιοι Υπάλληλοι», «Ιδιωτικοί Υπάλληλοι») ή επιχείρησης / οργανισμού (π.χ. «Βιοτεχνία», «Ελεύθεροι Επαγγελματίες»).
- Από την ενότητα «Φορείς Δημοσίου», μέσω της οποίας ο χρήστης έχει την δυνατότητα να εμφανίσει όλες τις διαθέσιμες υπηρεσίες/πληροφορίες και στοιχεία επικοινωνίας που σχετίζονται με τον Φορέα που έχει επιλέξει.
- Από την κεντρική «Αναζήτηση» της πύλης μέσω της οποίας ο χρήστης έχει την δυνατότητα να αναζητήσει με λέξεις κλειδιά υπηρεσίες/πληροφορίες που υπάρχουν στην πύλη.

2. Διαλειτουργικότητα

Ο Ermis παρέχει τις απαραίτητες υποδομές για την πλήρη υποστήριξη της Διαλειτουργικότητας μεταξύ των πληροφοριακών συστημάτων της Δημόσιας Διοίκησης. Επίσης η διαλειτουργικότητα συνδέεται και με την ανάπτυξη εφαρμογών για την παροχή υπηρεσιών Ηλεκτρονικών Συναλλαγών από ένα κεντρικό σημείο.

Οι εγγεγραμμένοι χρήστες του Ermis μπορούν να αξιοποιήσουν ένα μεγάλο πλήθος ηλεκτρονικών υπηρεσιών που είτε μπορούν να υποβληθούν ηλεκτρονικά προς οποιοδήποτε ΚΕΠ είτε διεκπεραιώνονται πλήρως ηλεκτρονικά από τον χρήστη.

3. Ασφάλεια συναλλαγών

Ο Ermis παρέχει ασφαλείς υπηρεσίες Ηλεκτρονικής Διακυβέρνησης σε κάθε επίπεδο με την χρήση κλιμακούμενων μεθόδων ψηφιακής αυθεντικοποίησης. Ανάλογα με τον τύπο των δεδομένων που

διακινούνται στα πλαίσια της υποβολής της εκάστοτε υπηρεσίας, ο Ermis υποστηρίζει διαφορετικά επίπεδα ταυτοποίησης των Πολιτών/Επιχειρήσεων.

Πιο συγκεκριμένα:

- Υπηρεσίες για τις οποίες προσφέρεται μόνο πληροφόρηση για την διαδικασία και τα απαραίτητα δικαιολογητικά, δεν απαιτούν κάποιο αναγνωριστικό ταυτοποίησης (είναι διαθέσιμες σε όλους τους χρήστες του Ermis – εγγεγραμμένους ή όχι).
- Υπηρεσίες για τις οποίες παρέχεται η δυνατότητα ηλεκτρονικής αίτησης, απαιτείται απλή εγγραφή του χρήστη και χρήση του username / password που του παρέχεται.
- Υπηρεσίες για τις οποίες προσφέρεται πλήρης ηλεκτρονική διεκπεραίωση, απαιτείται εγγραφή του χρήστη και φυσική ταυτοποίησή του (μόνο μία φορά) σε οποιοδήποτε ΚΕΠ.
- Σε σύντομο χρονικό διάστημα, θα υποστηρίζεται η δυνατότητα ταυτοποίησης του χρήστη μέσω ψηφιακών πιστοποιητικών που θα χρησιμοποιηθούν για ψηφιακή υπογραφή, αυθεντικοποίηση και κρυπτογράφηση.

Η Εθνική Πύλη Δημόσιας Διοίκησης Ermis συνιστά αντικείμενο του έργου «Μελέτη και Ανάπτυξη της Κεντρικής Κυβερνητικής Διαδικτυακής Πύλης της Δημόσιας Διοίκησης για την Πληροφόρηση & Ασφαλή Διεκπεραίωση Ηλεκτρονικών Συναλλαγών των Πολιτών / Επιχειρήσεων» με φορέα υλοποίησης την Κοινωνία της Πληροφορίας Α.Ε. (ΚτΠ ΑΕ) και φορέα λειτουργίας και χρηματοδότησης το Υπουργείο Εσωτερικών – Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης,[116]

4.1.1. Προσβασιμότητα

Όσον αφορά την προσβασιμότητα η Εθνική Πύλη Δημόσιας Διοίκησης www.ermis.gov.gr έχει υλοποιηθεί ακολουθώντας τις προδιαγραφές, οδηγίες και κατευθύνσεις του World Wide Web Consortium (W3C) για την ανάπτυξη προσβάσιμων διαδικτυακών τόπων, οι οποίες έχουν παρατεθεί στο Κεφάλαιο 2 . Η Εθνική Πύλη Δημόσιας Διοίκησης www.ermis.gov.gr συμμορφώνεται με το πρότυπο Web Content Accessibility Guidelines (WCAG), έκδοση 1.0, στο επίπεδο «Α». [117]

4.1.2. Προστασία Προσωπικών Δεδομένων

Η πολιτική προστασίας των προσωπικών δεδομένων είναι αρκετά ξεκάθαρη και παρατίθεται στην ιστοσελίδα www.Ermis.gov.gr.

Η διαχείριση και προστασία των προσωπικών δεδομένων του επισκέπτη/ χρήστη των υπηρεσιών της Εθνικής Πύλης Ερμής που ανήκει στο ΥΠΕΣ(Υπεύθυνος Επεξεργασίας) υπόκειται στους όρους του παρόντος τμήματος καθώς και από τις σχετικές διατάξεις του ελληνικού δικαίου (Ν. 2472/1997 για την προστασία του ατόμου από την προστασία δεδομένων προσωπικού χαρακτήρα

όπως έχει συμπληρωθεί και τροποποιηθεί με τις αποφάσεις του προέδρου της επιτροπής προστασίας προσωπικών δεδομένων, τα Π. Δ. 207/1998 και 79/2000, το άρθρο 8 του Ν. 2819/2000 και τον Ν. 3471/2006) και του ευρωπαϊκού δικαίου (οδηγίες 95/46/ΕΚ και 97/66/ΕΚ).

Η αξιοποίηση υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί συλλογή και επεξεργασία διαφορετικού είδους πληροφοριών, όπως προσωπικών δεδομένων, των οποίων η προστασία, επεξεργασία και μη αποκάλυψη και δημοσιοποίηση αποτελεί βασική κανονιστική απαίτηση, σύμφωνα με τις ειδικότερες προϋποθέσεις και εγγυήσεις της σχετικής νομοθεσίας (ν. 2472/97),που πρέπει να εκπληρώνεται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Η Εθνική Πύλη Ερμής επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων ("Υποκειμένων") που είναι εγγεγραμμένοι χρήστες της πύλης. Σκοπός της επεξεργασίας είναι η παροχή στους χρήστες της πύλης ολοκληρωμένων και ασφαλών ηλεκτρονικών συναλλαγών της δημόσιας διοίκησης κεντρικά ελεγχόμενες από τον Ερμή. Ειδικότερα, παρατίθενται παρακάτω πληροφορίες για τα προσωπικά δεδομένα που συλλέγονται από τον Ερμή.

- **Εγγραφή χρήστη στον Ερμή**

Για την εγγραφή του επισκέπτη ως χρήστη στον Ερμή, ζητούνται υποχρεωτικά τα εξής στοιχεία: Ονοματεπώνυμο χρήστη, όνομα πατέρα, e-mail, ημερομηνία γέννησης. Ο χρήστης με δική του συγκατάθεση μπορεί να δηλώσει επιπλέον προαιρετικά στοιχεία όπως στοιχεία επικοινωνίας, οικογενειακή κατάσταση κλπ. Τα ανωτέρω στοιχεία – μη ευαίσθητα προσωπικά δεδομένα - διατηρούνται στην βάση δεδομένων του Ερμή που ανήκει στο ΥΠΕΣ. Τα στοιχεία αυτά ουδέποτε γνωστοποιούνται σε τρίτους.

- **Ηλεκτρονικές υπηρεσίες**

Για την λειτουργία αλλά και την σωστή χρήση των ηλεκτρονικών υπηρεσιών απαιτείται η επεξεργασία προσωπικών δεδομένων. Στον Ερμή συλλέγονται τα ελάχιστα απαιτούμενα προσωπικά δεδομένα για την εκπλήρωση του σκοπού, δηλ. της παροχής συγκεκριμένης υπηρεσίας ή κατηγορίας υπηρεσιών. Επίσης συλλέγονται εκείνα και μόνο τα δεδομένα τα οποία είναι αναγκαία και κατάλληλα για την εκπλήρωση του σκοπού αυτού και δεν χρησιμοποιούνται για σκοπούς μη συμβατούς με αυτούς για τους οποίους έχουν συλλεχθεί.

- **Newsletters**

Για την εγγραφή του επισκέπτη / χρήστη στις λίστες παραληπτών (mailing lists) των Ενημερωτικών Δελτίων (newsletters) του Δικτύου ζητείται απλά το e-mail του χρήστη και δεν απαιτείται η εγγραφή του χρήστη στην πύλη. Το portal που ανήκει στο ΥΠΕΣ διατηρεί αρχείο με τις ηλεκτρονικές διευθύνσεις των παραληπτών για την αποστολή Newsletters. Τα στοιχεία αυτά ουδέποτε γνωστοποιούνται σε τρίτους. Ο παραλήπτης των Newsletters μπορεί μόνος του να διαγραφεί από το αρχείο με τις ηλεκτρονικές διευθύνσεις.

- **Cookies**

Τα cookies είναι μικρά αρχεία κειμένου που αποθηκεύονται στο σκληρό δίσκο κάθε επισκέπτη / χρήστη και δεν λαμβάνουν γνώση οποιουδήποτε εγγράφου ή αρχείου από τον υπολογιστή του. Χρησιμοποιούνται για να αναγνωρίζεται ο χρήστης, ή κάποιες συγκεκριμένες ενέργειές του σε προηγούμενες επισκέψεις του στην ιστοσελίδα. Στον ΕΡΜΗ χρησιμοποιούνται cookies για 2 λόγους:

- Για να αναγνωρίζεται ο χρήστης ως αυθεντικοποιημένος από την υπηρεσία αυθεντικοποίησης του συστήματος.
- Για να αναγνωρίζονται συγκεκριμένες ενέργειες του χρήστη σε προηγούμενες επισκέψεις του σε κάποιες ιστοσελίδες (π.χ. το αν ψήφισε ή όχι σε κάποια δημοσκόπηση)

- **Links to other sites ("Σύνδεσμοι")**

Το portal που ανήκει στο ΥΠΕΣ περιλαμβάνει links ("συνδέσμους") προς άλλα websites τα οποία και δεν ελέγχονται από το ίδιο αλλά από τους τρίτους φορείς (φυσικά ή νομικά πρόσωπα) . Σε καμία περίπτωση δεν ευθύνεται το portal που ανήκει στο ΥΠΕΣ για τους Όρους Προστασίας των Προσωπικών Δεδομένων τους οποίους αυτοί ακολουθούν.

- **IP Addresses**

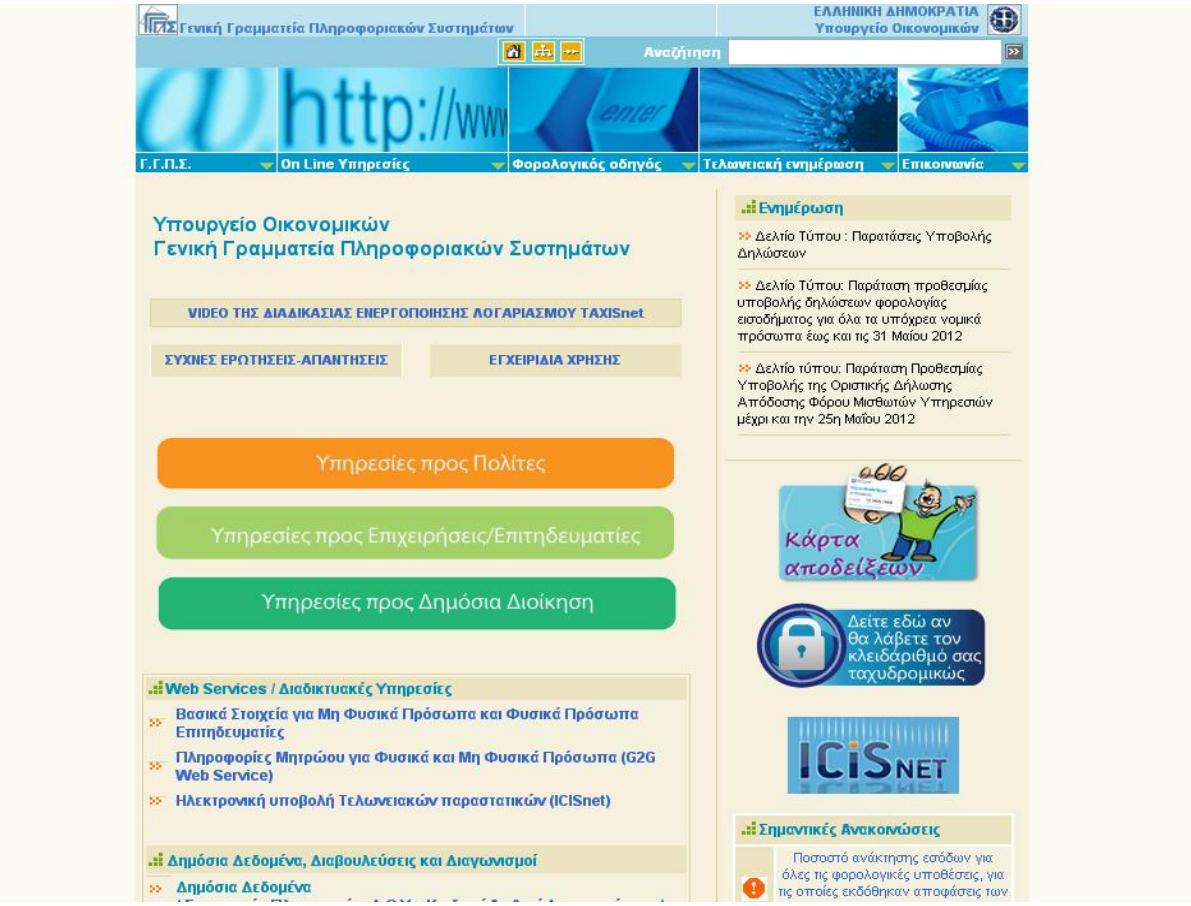
Η διεύθυνση IP μέσω της οποίας ο Η/Υ έχει πρόσβαση στο Internet και στη συνέχεια στο Δίκτυο αξιοποιείται αποκλειστικά για την συγκέντρωση στατιστικών στοιχείων.

- **Ψηφοφορίες**

Για τη συμμετοχή του επισκέπτη / χρήστη σε ψηφοφορία που διενεργείται από το portal που ανήκει στο ΥΠΕΣ ζητούνται τα εξής στοιχεία : Ονοματεπώνυμο και κατά περίπτωση άλλα στοιχεία, μη ευαίσθητα προσωπικά δεδομένα, όπως ιδιότητα, ηλικία κλπ. (ανάλογα με τη φύση των ερωτημάτων που τίθενται προς ψηφοφορία). Η ψήφος του επισκέπτη / χρήστη καταγράφεται αποκλειστικά για την εξαγωγή συμπερασμάτων σε σχέση με τη θέση της κοινής γνώμης πάνω σε ορισμένο ζήτημα και δεν δύναται να χρησιμοποιηθεί για οποιονδήποτε άλλο σκοπό ούτε να γνωστοποιηθεί σε τρίτους. Βέβαια παρέχεται και δυνατότητα συμμετοχής σε ψηφοφορίες και για μη εγγεγραμμένους χρήστες. [118]

4.2. Γενική Γραμματεία Πληροφοριακών Συστημάτων-TAXISnet

Αυτή η κυβερνητική ιστοσελίδα αφορά τους πολίτες G-to-C, τις επιχειρήσεις G-to-B και τις υπηρεσίες δημόσιας διοίκησης G-to-G. Για να επιτραπεί η χρήση όλων των διαθέσιμων, ο χρήστης είτε είναι φυσικό άτομο, νομικό άτομο, επιχείρηση ή φορέας δημόσιας διοίκησης πρέπει να εγγραφεί στην υπηρεσία και να ταυτοποιηθεί με την χρήση ενός κλειδάριθμου, τον οποίο λαμβάνει με την επίδειξη της ταυτότητας του στην αρμόδια εφορία.



Εικόνα 7: Διαδικτυακός τόπος ΓΓΠΣ-TAXISnet

4.2.1. Προσβασιμότητα

Η ιστοσελίδα της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ) και το TAXISnet είναι εύκολα στη χρήση ακόμα και για άπειρους χρήστες αλλά όσον αφορά ομάδες με αναπηρίες και πιο συγκεκριμένα άτομα με προβλήματα όρασης κάθε είδους, είναι αρκετά δύσκολες στη χρήση. Δεν παρέχεται δυνατότητα σμίκρυνσης ή μεγέθυνσης του περιεχομένου, καθώς ούτε και ανάγνωση του περιεχομένου των ιστοσελίδων, κάτι το οποίο είναι ζωτικής σημασίας για τις συγκεκριμένες ιστοσελίδες καθώς όλες οι κοινωνικές ομάδες έχουν αυτού του είδους τις συναλλαγές με το Υπουργείο Οικονομικών και θα μπορούσαν αν τους δινόταν η δυνατότητα να ενημερώνονται και να αλληλεπιδρούν για τις φορολογικές τους υποθέσεις από τον διαδικτυακό τόπο της Γενικής Γραμματείας Πληροφοριακών Συστημάτων.

4.2.2. Ασφάλεια

Η Γενική Γραμματεία Πληροφοριακών Συστημάτων σε μια προσπάθεια να προάγει την ποιότητα και την ασφάλεια των ηλεκτρονικών συναλλαγών εισάγει την τεχνολογία ψηφιακών υπογραφών σε ηλεκτρονικά έγγραφα που παράγονται από τα πληροφοριακά της συστήματα.

Η εφαρμογή αυτής της τεχνολογίας θα διασφαλίσει στο μέγιστο δυνατό βαθμό την ακεραιότητα και γνησιότητα αυτών των εγγράφων ανά πάσα στιγμή, σε οποιαδήποτε συναλλαγή των πολιτών/επιχειρήσεων με φορείς του Δημοσίου (C2G, B2G) ή σε συναλλαγές μεταξύ υπηρεσιών του Δημοσίου (G2G).

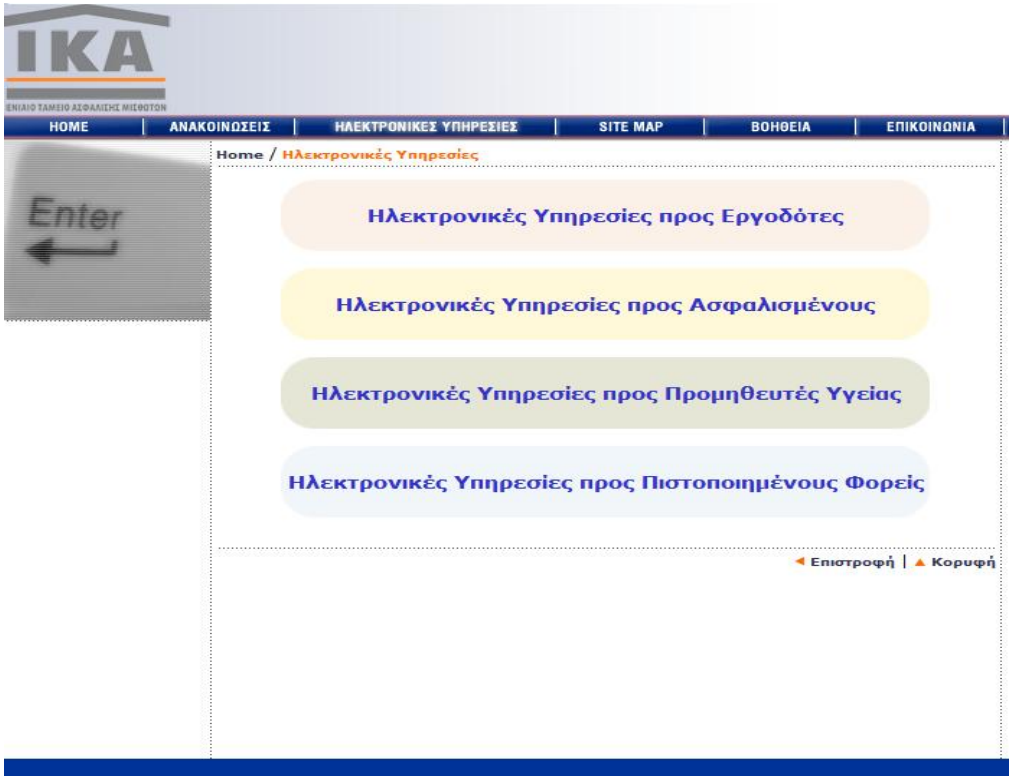
Εικόνα 8: Ψηφιακό πιστοποιητικό για gsis.gr

Για το σκοπό αυτό η ΓΓΠΣ προμηθεύεται Αναγνωρισμένα ψηφιακά πιστοποιητικά Φορέα (Τύπου ΠΠ7) από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), έτσι ώστε να πιστοποιείται από μια ανεξάρτητη Τρίτη Έμπιστη Οντότητα σε ποιο Φορέα ανήκουν τα ψηφιακά πιστοποιητικά. [119]

Η είσοδος των χρηστών, η εγγραφή νέων χρηστών και όλες οι επιλογές που αφορούν διακίνηση προσωπικών δεδομένων διασφαλίζονται από ασφαλή σύνδεση και με τη χρήση κρυπτογράφησης.

4.3. ΙΚΑ-ΕΤΑΜ

Οι υπηρεσίες της ιστοσελίδας του ΙΚΑ-ΕΤΑΜ έχει σκοπό να προάγει τη βέλτιστη παροχή ηλεκτρονικών υπηρεσιών προς τους ασφαλισμένους, τους εργοδότες, τους προμηθευτές υγείας και τους πιστοποιημένους φορείς.[120]



Εικόνα 9: Διαδικτυακός τόπος ΙΚΑ-ΕΤΑΜ

4.3.1. Προσβασιμότητα

Όσον αφορά την προσβασιμότητα το περιεχόμενο δεν είναι αρκετά ξεκάθαρο δεν παρέχεται δυνατότητα μεγέθυνσης της γραμματοσειράς ούτε και ανάγνωση του περιεχομένου. Αυτό καθιστά αδύνατο σε άτομα με προβλήματα όρασης και ηλικιωμένους να έχουν πρόσβαση στην σελίδα του ΙΚΑ παρόλο που αποτελεί τον κυριότερο φορέα ασφάλισης των εργαζομένων.

4.3.2. Ασφάλεια

Η ιστοσελίδα του ΙΚΑ-ΕΤΑΜ χρησιμοποιεί κρυπτογραφημένη σύνδεση με χρήση του πρωτοκόλλου TSL 1.0 για τα μεταφορά δεδομένων καθώς αφορά ευαίσθητα προσωπικά δεδομένα και συναλλαγές με τον οργανισμό.

Εικόνα 10: Ψηφιακό πιστοποιητικό www.ika.gr

4.4. Οργανισμός Απασχολήσεως Εργατικού Δυναμικού (ΟΑΕΔ)

Ο (ΟΑΕΔ) είναι το κύριο όργανο εφαρμογής της Κυβερνητικής Πολιτικής για την απασχόληση, ώστε να εξασφαλιστούν οι αναγκαίες προϋποθέσεις ταχείας προσαρμογής της προσφοράς εργασίας προς τις απαιτήσεις της ζήτησης, σε αρμονία με το εκάστοτε Πρόγραμμα Οικονομικής Ανάπτυξης της Χώρας και τις συναφείς κατευθύνσεις και οδηγίες του Υπουργού Εργασίας και Κοινωνικής Ασφάλισης.

Ειδικότερα, ο Οργανισμός μεριμνά για:

- τον Επαγγελματικό Προσανατολισμό του εργατικού δυναμικού.
- την Τεχνική Επαγγελματική Εκπαίδευση και Κατάρτιση του εργατικού δυναμικού.
- την διευκόλυνση της επαφής μεταξύ προσφοράς και ζήτησης εργασίας.
- διάφορες παροχές, όπως τη με προϋποθέσεις επιδότηση ανέργων, τη συμπλήρωση των επιδομάτων κύησης και μητρότητας που παρέχει το ΙΚΑ κλπ.[121]

Η ιστοσελίδα του ΟΑΕΔ έκτος της ενημέρωσης που παρέχει σε ανέργους και επιχειρηματίες για διάφορα προγράμματα και κρατικές επιδοτήσεις λειτουργεί και ως μεσάζοντας για την ανεύρεση εργασίας (Εικόνα 11) ή την ανεύρεση υπαλλήλου αντίστοιχα (Εικόνα 12).

Εικόνα 11: Αναζήτηση Εργασίας

Εικόνα 12: Αναζήτηση προσωπικού

4.4.1. Προσβασιμότητα

Όσον αφορά την προσβασιμότητα, η ιστοσελίδα του ΟΑΕΔ δεν φαίνεται να ακολουθεί κάποιο πρότυπο προσβασιμότητας και ακόμα και όροι χρήσης είναι δύσκολο να διαβαστούν ακόμα και από πολίτες χωρίς κάποιο πρόβλημα όρασης. (Εικόνα 13)

Εικόνα 13: Όροι Χρήσης ΟΑΕΔ

Παρόλο που στους Όρους Χρήσης γίνεται σαφές ότι οι χρήστες πρέπει να διαβάσουν προσεκτικά τους όρους αυτό στην πράξη είναι πολύ δύσκολο λόγω του μεγέθους και του χρώματος της γραμματοσειράς που έχει χρησιμοποιηθεί.(Εικόνα 14)

Εικόνα 14: Όροι Χρήσης ΟΑΕΔ απόσπασμα

4.4.2. Ασφάλεια

Μέσω της ιστοσελίδας του ΟΑΕΔ δεν πραγματοποιείται κάποια οικονομική συναλλαγή. Παρόλα αυτά διακινούνται μέσω αυτής προσωπικά δεδομένα για τα όποια δεν γίνεται σαφές αν διασφαλίζεται και με ποιό τρόπο η προστασία τους.

- **Περιορισμός ευθύνης ΟΑΕΔ(Απόσπασμα από τους Όρους Χρήσης)**

«Ο ΟΑΕΔ χωρίς να εγγυάται και συνεπώς να ευθύνεται, καταβάλλει τη μέγιστη δυνατή προσπάθεια, ώστε οι πληροφορίες και το σύνολο του περιεχομένου να διέπονται από τη μέγιστη ακρίβεια, σαφήνεια, χρονική εγγύτητα, πληρότητα, ορθότητα και διαθεσιμότητα. Σε καμία περίπτωση, συμπεριλαμβανομένης και αυτής της αμέλειας, δεν προκύπτει ευθύνη του ΟΑΕΔ για οιαδήποτε ζημία τυχόν προκληθεί στον επισκέπτη/ χρήστη εξ αφορμής αυτής της χρήσης του Δικτυακού μας τόπου, στην οποία προβαίνει με δική του πρωτοβουλία και εν γνώσει των παρόντων όρων.

Οι πληροφορίες και οι υπηρεσίες παρέχονται ως έχουν, χωρίς καμία εγγύηση άμεση ή έμμεση, τις οποίες όλες ρητά αρνείται ο ΟΑΕΔ, ακόμη και εκείνες περί εμπορευσιμότητας ή καταλληλότητας.

Ο ΟΑΕΔ σε καμία περίπτωση δεν εγγυάται την αδιάκοπη και άνευ λαθών παροχή των υπηρεσιών και του περιεχομένου του, ούτε ακόμη την έλλειψη ιών, είτε πρόκειται για το Δικτυακό του τόπου, είτε για κάποιο άλλο site server μέσω των οποίων λαμβάνεται το περιεχόμενό του.

Ως εκ τούτου ο ΟΑΕΔ δεν ευθύνεται σε καμία περίπτωση για τυχόν αποθετικές ζημίες ή διαφυγόν κέρδος, άμεση ή έμμεση ζημία.»[122]

4.5. Διαδικτυακή Πύλη για ΑμεΑ

Η ΚτΠ αναγνωρίζοντας τις ανάγκες της καθημερινής διαβίωσης των ΑμεΑ, προχώρησε στην υλοποίηση προσβάσιμων διαδικτυακών εφαρμογών, όπως:

- **Ηλεκτρονικό ΚΕΠ για ΑμεΑ**, με σκοπό τη διάθεση εξειδικευμένης πληροφορίας για ΑμεΑ σε προσβάσιμη μορφή, καθώς και την υποστήριξη μηχανισμών υποβολής και προώθησης αιτημάτων προς φορείς της Δημόσιας Διοίκησης.
- **Υπηρεσία επαγγελματικής ενσωμάτωσης**, για την εξυπηρέτηση της διαδικασίας αναζήτησης εργασίας από ΑμεΑ, χωρίς την απαίτηση της φυσικής παρουσίας τους στον χώρο των εργοδοτών.
- **Υπηρεσία πληροφόρησης για προϊόντα και υπηρεσίες υποστηρικτικής τεχνολογίας ΑμεΑ**, με σκοπό την δημιουργία κοιτίδας πληροφόρησης των φορέων και των μεμονωμένων χρηστών, προκειμένου να βοηθηθούν στην επιλογή των κατάλληλων προϊόντων ή υπηρεσιών.
- **Πρότυπη Διαδικτυακή Πύλη για ΑμεΑ,** η οποία θα αποτελέσει το κομβικό σημείο διάχυσης και διάθεσης των υπηρεσιών, που θα υλοποιηθούν στο πλαίσιο του Έργου, ενώ παράλληλα θα διαθέτει υπηρεσίες που προάγουν την επικοινωνία μεταξύ των εμπλεκομένων φορέων και ωθούν στην ανταλλαγή πληροφοριών και τη συνεργασία.
- **Φωνητική Πύλη**, η οποία θα αποτελέσει εναλλακτικό δίαυλο πρόσβασης των ΑμεΑ στο διαθέσιμο περιεχόμενο με πιο οικεία μέσα, όπως το τηλέφωνο. Η υπηρεσία φωνητικής πύλης

δεν είναι προς το παρόν διαθέσιμη μέχρι την περάτωση των εργασιών διασυνδεσιμότητας της με την Εθνική Πύλη Ερμής.[123]

Εικόνα 15: Διαδικτυακή Πύλη για ΑμεΑ

4.5.1. Προσβασιμότητα

Όσον αφορά την προσβασιμότητα αυτής της πύλης, όπως είναι λογικό πληρούνται όλες οι προτεραιότητες των οδηγιών WCAG v 1.0 και επιπλέον ο κάθε χρήστης ανάλογα με την ιδιαιτερότητα του ,μπορεί να προσαρμόσει την ιστοσελίδα στα μέτρα και τις ανάγκες του. Οι επιλογές του ως προς την προσαρμογή της σελίδας είναι:

- Ενεργοποιήστε το βασικό προφίλ χρήστη
- Ενεργοποιήστε το προφίλ χρήστη με τύφλωση
- Ενεργοποιήστε το προφίλ χρήστη με μειωμένη όραση
- Ενεργοποιήστε το προφίλ χρήστη με κινητική αναπηρία (με εικονικό πληκτρολόγιο
- Ενεργοποιήστε το προφίλ χρήστη με κινητική αναπηρία (χωρίς εικονικό πλήκτρο πληκτρολόγιο)
- Ενεργοποιήστε το προφίλ χρήστη με κώφωση

4.5.2. Ασφάλεια

Η συγκεκριμένη Διαδικτυακή Πύλη έχει ως σκοπό την ενημέρωση των ΑμεΑ και ως εκ τούτου δεν παρέχει κανενός είδους ηλεκτρονική συναλλαγή. Επιπλέον όπως αναφέρεται και στην Πύλη η Διαδικτυακή Πύλη για ΑμεΑ προστατεύεται αποτελεσματικά από ιούς. Ωστόσο, το ειδικό λογισμικό ανίχνευσης ιών, ενδέχεται να μην μπορεί να ανιχνεύσει και να εξουδετερώσει κάθε ιό ή άλλου είδους ζημιογόνο λογισμικό. Υπάρχει πάντα πιθανότητα να προσβληθεί ο υπολογιστής του χρήστη από κάποιο ιό, ενώ είναι συνδεδεμένος στο διαδίκτυο. Η Διαδικτυακή Πύλη στην περίπτωση αυτή, δεν φέρει καμία ευθύνη, για οποιαδήποτε ζημιά προκληθεί στον υπολογιστή από αντίστοιχη χρήση.

Κεφάλαιο 5
Συμπεράσματα

5.1. Γενικά

Τα τελευταία χρόνια η Ελληνική Κυβέρνηση έχει κάνει γιγαντιαία άλματα όσον αφορά το κομμάτι των ηλεκτρονικών υπηρεσιών. Η σύσταση οργανισμών που ειδικεύονται στον τομέα των πληροφοριακών συστημάτων και ως προέκταση αυτών και στην ηλεκτρονική διακυβέρνηση έχει επιφέρει σημαντικές βελτιώσεις στον τομέα της ηλεκτρονική διακυβέρνησης. Παρόλα αυτά παρατηρούνται και σημαντικές ελλείψεις. Οι πρόσφατες οικονομικές και πολιτικές εξελίξεις στη χώρα, δηλαδή η υπογραφή του μνημονίου, έχουν πυροδοτήσει τις διαρθρωτικές αλλαγές στους δημόσιους οργανισμούς όσον αφορά την διαλειτουργικότητα των κυβερνητικών οργανισμών, την διαφάνεια του δημόσιου τομέα και την αποτελεσματικότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών. Επιπλέον το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης το οποίο συστάθηκε στη σημερινή του μορφή στις 27 Ιουνίου του 2011 με το με το Π.Δ. 65/2011 έχει επιφέρει σημαντικές αλλαγές στον τρόπο λειτουργίας της δημόσιας διοίκησης και κατ' επέκταση στις ηλεκτρονικές υπηρεσίες της κυβέρνησης.

5.2. Προσβασιμότητα

Στο κομμάτι που αφορά την προσβασιμότητα οι κυβερνητικές ιστοσελίδες βρίσκονται σε ικανοποιητικό επίπεδο πληρώντας σε πολλές περιπτώσεις τις προτεραιότητες των πιο σύγχρονων οδηγιών προσβασιμότητας. Τέτοιες σελίδες είναι αυτές της Βουλής των Ελλήνων[124] και της Διαδικτυακής Πύλης για ΑμεΑ στις οποίες ικανοποιούνται και οι τρείς προτεραιότητες των οδηγιών WCAG v 1.0. Αντίστοιχα στη Διαδικτυακή Πύλη Ερμής ικανοποιείται μόνο η προτεραιότητα 1 του WCAG v 1.0. Επιπλέον ο δικτυακός τόπος του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης ακολουθεί τις οδηγίες WCAG v 2.0.

Αντίθετα διαδικτυακοί τόποι ηλεκτρονικών υπηρεσιών όπως το TAXISnet, ο ΟΑΕΔ και το ΙΚΑ-ΕΤΑΜ, δεν ικανοποιούν καμία από τις οδηγίες προσβασιμότητας. Όμως καθότι αυτές οι υπηρεσίες αφορούν όλους τους πολίτες και όλοι οι πολίτες ανεξαρτήτου ικανοτήτων έχουν δικαίωμα πρόσβασης στις ηλεκτρονικές αυτές υπηρεσίες, θα πρέπει να σχεδιαστούν οι διαδικτυακοί τόποι αυτοί με τέτοιο τρόπο ούτως ώστε να διευκολύνετε η χρήση των υπηρεσιών ακόμα και από άτομα με ειδικές ανάγκες(ΑμεΑ).

Οι διαδικτυακοί τόποι και οι υπηρεσίες ηλεκτρονικής διακυβέρνησης πρέπει να συμμορφώνονται με το πρότυπο Web Content Accessibility Guidelines (Οδηγίες για την

Προσβασιμότητα του Περιεχομένου του Ιστού) στην εκάστοτε ισχύουσα έκδοση, και σε επίπεδο προσβασιμότητας τουλάχιστον «ΑΑ», ή με άλλο πρότυπο ηλεκτρονικής προσβασιμότητας, το οποίο ορίζεται από κείμενη νομοθεσία και διασφαλίζει αντίστοιχη ή υψηλότερη ποιότητα πρόσβασης των ατόμων με αναπηρία στις ηλεκτρονικές υπηρεσίες, εφαρμογές πληροφορικής και ψηφιακά έγγραφα.

5.3. Ασφάλεια

Στο κομμάτι που αφορά την ασφάλεια παρατηρούμε ότι όλοι οι δικτυακοί τόποι που διαχειρίζονται προσωπικές πληροφορίες χρηστών και παρέχουν ηλεκτρονικές υπηρεσίες χρησιμοποιούν μεθόδους κρυπτογράφησης, ψηφιακά πιστοποιητικά και προβλέπεται να εντάξουν και τις ηλεκτρονικές υπογραφές στις μεθόδους ασφάλειας των συναλλαγών τους. Μοναδική εξαίρεση αποτελεί ο διαδικτυακός τόπος του ΟΑΕΔ, στον οποίο, παρόλο που διακινούνται προσωπικά δεδομένα χρηστών δεν χρησιμοποιείται κάποια μέθοδος κρυπτογράφησης κατά τη μεταφορά αυτών των δεδομένων.

Όπως γνωρίζουμε ο τομέας της πληροφορικής αναπτύσσεται και διευρύνεται ασταμάτητα και νέες μέθοδοι ασφάλειας αναπτύσσονται για να αντιμετωπίσουν τις διάφορες απειλές που προκύπτουν. Πιο συγκεκριμένα στο κομμάτι που αφορά την κρυπτογράφηση των δεδομένων που διακινούνται στα πλαίσια της ηλεκτρονικής διακυβέρνησης, η Στεγανογραφία θα μπορούσε να ενισχύσει την απόκρυψη των πληροφοριών σε μη εξουσιοδοτημένους χρήστες και να καταστήσει την ηλεκτρονική διακυβέρνηση άτρωτη σε επιθέσεις υποκλοπής δεδομένων.

Βιβλιογραφία

[1] Η ηλεκτρονική διακυβέρνηση στην Ευρώπη και στην Ελλάδα: παρόν και μέλλον (www.go-online.gr/ebusiness/specials)

[2] Ηλεκτρονική Διακυβέρνηση Οικονομικό Επιμελητήριο Ελλάδος Ανατολικής Μακεδονίας (http://www.oeeam.gr/el/prog/egov.asp)

[3] Stamoulis D., Gouscos D., Georgiadis P., Martakos, D., 'Revisiting Public information management for effective e-government services'. Information Management and Computer Security, 2001.

[4] Clark, E., 'Managing the transformation to e-government: An Australian Perspective'. Thunderbird International Business Review , 2003.

[5] Hwang M. S., Li C. T., Shen J. J., Chu Y. P., "Challenges in e-Government and security of information", Information and Security: An International Journal, Vol.15, No.1, pp.9-20, 2004

[6] Μαριλύς Χριστοφή, Τοπογράφος Μηχανικός και Εμπειρογνώμονας Προσβασιμότητας, περιοδικό «Θέματα Αναπηρίας» , Αρ. Τεύχους 1. - Μάιος, Ιούνιος, Ιούλιος 2005 (http://www.esaea.gr/index.php?module=announce&ANN_id=33&ANN_user_op=view&ns_news= 1&MMN_position=17:17)

[7] Nielsen, J. Beyond accessibility: Treating users with disabilities as people, Jakob Nielsen's Alertbox , 2001; (http//www.useit.com/alertbox/20011111.html)

[8] Souza, R. & Manning, H, "The Web Accessibility Time Bomb." Forrester Research Tech Strategy Report, Σεπτέμβριος 2000.

[9] Waddell, C. D., Applying the ADA to the Internet: A Web accessibility standard. Paper presented at the request of the American Bar Association for their National Conference.1998 (http://people.rit.edu/easi/law/weblaw1.htm)

[10] Gant, D. B, & Gant, J. P., State Web Portals:Delivering and Financing E-Service. E-Government Series, 2002

[11] Paciello, M. G., Web accessibility for people with disabilities. Lawrence, Kansas: CMP Books, 2000, σ.. 39 - 44)

[12] Sager, R. H. Don't disable the Web: Americans with disabilities need access, not Diktats. The American Spectator, 2000.

[13] Solomon, K., Smart biz: Enabling the disabled. Wired News, 3 November 2000 .

[14] Nielsen J., Designing Web usability, Indianapolis, 2000, New Riders Publishing

[15] Rogers, M., & Rajkumar, T. M, Developing electronic commerce Web sites for the visually impaired, Information Systems Management, 1999

[16] Kautzman, M., Virtuous, virtual access: Making Web pages accessible to people with disabilities, Searcher, 1998

17] Gant, D. B., & Gant, J. P., State Web portals: Delivering and financing e-service. E-Government Series, 2002

[18] Huang J., Accessibility of E-Government Web Sites, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[19] Kebede G., Factors Affecting Access to Electronic Information and their Implications, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[20] Ulrike P.-, Accessible E-Government trough Universal Design, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[21] Ulrike P.-, Accessible E-Government trough Universal Design, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[22] Web Accessibility Initiative (www.w3.org/WAI)

[23] Πολιτική για την προσβασιμότητα του Διαδικτύου, Ευρωπαϊκή Ένωση, (http://europa.eu/geninfo/accessibility_policy_el.htm)

[24] Chisholm, W., Vanderheiden, G., & Jacobs, I.,. Web content accessibility guidelines 1.0 (W3C recommendation), (www.w3.org/TR/WAI-WEBCONTENT/).

[25] Ulrike P.-, Accessible E-Government trough Universal Design, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[26] Web Content Accessibility Guidelines 1.0, W3C Recommendation 5-May-1999, (http://www.w3.org/TR/WCAG10/#priorities)

[27] Pieper, M., Anderweit, R., Schulte, B., Peter, U., Croll, J., & Cornelssen, I, Methodological approaches to identify honorable best practice in barrier-free Web design: Examples from Germany's 1st BIENE Award Competition. In C. Stary & C. Stephanidis (Eds.), User-centered interaction paradigms for universal access in the information society (LNCS Vol. 3196, pp. 360-372)., 2004, Berlin: Springer.

[28] Ulrike P.,Accessible E-Government trough Universal Design, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[29] Jhunjhunwala, A., Ramachandran, A., & Bandyopadhay, A. , N-logue: The story of a rural service provider in India. The Journal of Community Informatics, 2004

[30] Colle, R. D., Communication shops and Telecenters in developing nations. In M. Gurstein (Ed.), Community informatics: Enabling communities with information and communication technologies, Hershey, 2000, Idea Group Publishing.

[31] Jhunjhunwala A., Ramachandran A., & Bandyopadhay A. , N-logue: The story of a rural service provider in India. The Journal of Community Informatics, 2004

[32] Gomez, R., Hunt, P., Lamoureux, E.,. Enchanted by telecenters: A critical look at universal a ccess to information technologies for international development. Paper presented at the Conference New IT and Inequality, 16-17 February 1999, University of Maryland.

[33] Chow, C., Ellis, J., Walker, G., & Wise, B. , Who goes there? Longitudinal case studies of twelve users of community technology centers. Washington, DC: National Science Foundation, Division of Science Resource Statistics, 2000

[34] Proenza, F.J., Bastidas-Buch, R., & Montero, G., Telecenters for socioeconomic and rural development in Latin America and the Caribbean. Washington, DC: FAO, ITU and IADB, 2001

[35] Gomez, R., Hunt, P., Lamoureux, E.,. Enchanted by telecenters: A critical look at universal access to information technologies for international development. Paper presented at the Conference New IT and Inequality, 16-17 February 1999, University of Maryland.

[36] Gordon, A., & Gordon, M. , Sustainability and community technology: The role of public libraries and gates library initiative. Community informatics research network: Sustainability and community technology. What does this mean for community informatics; Australia: Centre for Community Networking Research, Monash University, 2005

[37] Erikson, C. , Advocacy and sustainability: The case of Chile's public library technology network. Community informatics research network: Sustainability and community technology. What does this mean for community informatics; Australia: Centre for Community Networking Research, Monash University, 2005.

[38] Stewart, J., Cafematics: The cybercafe and the community. In M. Gurstein (Ed.), Community informatics: Enabling communities with information and communication technologies, Hershey, 2000, PA: Idea Group Publishing

[39] Haseloff A., Public Access Points, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[40] Moore, B., Jr., Privacy: Studies in social and cultural history, 1994, Armonk: M. E. Sharpe

[41] Weckert, J. , Computer ethics: Future directions, 2001, Ethics and Information Technology.

[42] Dodig-Crnkovic G., Ethics and Privacy of Communications in E-Polis, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[43] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[44] Smith A., Strategic Importance of Security Standards, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[45] Alexander, Y., & Swetnam, M. S., Cyber terrorism and information warfare I: Assessment of challenges. New York, 1999, Oceana Publisher Inc

[46] Denning, D., Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Internet and international systems. 2001, Information Technology and American Foreign Policy Decisionmaking Workshop.

[47] Garfinkel, S., & Spafford, E. H., Web security and commerce. Sebastapol, 1997, CA: O'Reilly and Associates, Inc

[48] Denning, D., Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Internet and international systems. 2001, Information Technology and American Foreign Policy Decisionmaking Workshop.

[49] Alexander, Y., & Swetnam, M. S., Cyber terrorism and information warfare I: Assessment of challenges, New York, 1999, Oceana Publisher Inc.

[50] Denning, D., Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Internet and international systems. 2001, Information Technology and American Foreign Policy Decisionmaking Workshop.

[51] Denning, D., Cyberterrorism. Testimony before the special oversight panel on Terrorism Committee on Armed Services U.S. House of Representatives, 2000.

[52] Alexander, Y., & Swetnam, M. S., Cyber terrorism and information warfare I: Assessment of challenges. New York, 1999, Oceana Publisher Inc Dobbs Ferry.

[53] Anderson, P. L., & Geckil, I., Economic impact of the 2003 blackout, 2003

[54] Joshi J., Chandran S., Walid A., Ghafoor A., Survivability Issues and Challenges, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[55] Κατσίκας Σωκρ.- Γκριτζάλης Δημ.- Γκριτζάλης Στεφ.,Ασφάλεια Πληροφοριακών Συστημάτων, 2004, Εκδόσεις Νέων Τεχνολογιών

[56] Κατσίκας Σωκρ.- Γκριτζάλης Δημ.- Γκριτζάλης Στεφ.,Ασφάλεια Πληροφοριακών Συστημάτων, 2004, Εκδόσεις Νέων Τεχνολογιών

[57] Κατσίκας Σωκρ.- Γκριτζάλης Δημ.- Γκριτζάλης Στεφ.,Ασφάλεια Πληροφοριακών Συστημάτων, 2004, Εκδόσεις Νέων Τεχνολογιών

[58] Κατσίκας Σωκρ.- Γκριτζάλης Δημ.- Γκριτζάλης Στεφ.,Ασφάλεια Πληροφοριακών Συστημάτων, 2004, Εκδόσεις Νέων Τεχνολογιών

[59] Joshi J., Saubhagya R. Joshi, Chandran S., Identity Management and Citizen Privacy, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[60] Joshi J., Saubhagya R. Joshi, Chandran S., Identity Management and Citizen Privacy, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[61] Joshi J., Saubhagya R. Joshi, Chandran S., Identity Management and Citizen Privacy, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[62] Joshi J., Saubhagya R. Joshi, Chandran S., Identity Management and Citizen Privacy, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[63] Damiani, E., di Vimercati, S. D. C., & Samarati, P., Managing multiple and dependable identities., 2003, IEEE Internet Computing.

[64] Thuraisingham B., Data mining, national security, privacy, and civil liberties, 2003, ACM SIGKDD.

[65] Joshi J., Saubhagya R. Joshi, Chandran S., Identity Management and Citizen Privacy, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[66] Warren, S., & Brandeis, L. D., The right to privacy. Harvard Law Review, 1890

[67] Thompson, P. B., Privacy, secrecy and security, Ethics and Information Technology, 2001.

[68] DeCew J., Privacy, the Stanford encyclopedia of philosophy, 2002 (http://plato.stanford.edu/archives/sum2002/entries/privacy).

[69] Rosen, J. (2000). Why privacy matters. Wilson Quarterly, 2000.

[70] Mason, R. O., A tapestry of privacy, a metadiscussion, 2000.

[71] Dodig-Crnkovic G., Ethics and Privacy of Communications in E-Polis, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[72] Arnesen R., Danielsson J., Protecting Citizen Privacy in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[73] Arnesen R., Danielsson J., Protecting Citizen Privacy in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[74] Εφημερίδα της Κυβερνήσεως της Ελληνικής Δημοκρατίας, Τεύχος Πρώτο, Αρ. Φύλλου 138, στις 16 Ιουνίου 2011, (

http://www.et.gr/index.php?option=com_content&view=article&id=209%3A39792011&catid=60&l ang=el)

[75] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[76] Rajput, W.E., E-commerce systems architecture and applications, 2000, Artech House Publishers.)

[77] Stallings, W., Cryptography and network security—Principles and practice. Upper Saddle River, 1998, NJ:Prentice Hall.

[78] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[79] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[80] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[81] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[82] Turnbull, N., Internal control: Guidance for directors on the combined code (The Turnbull Report). Internal Control Working Party, 1999, Institute of Chartered Accountants in England and Wales.

[83] Hui-Feng Shih, Chang-Tsun Li, Information Security Management in Digital Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[84] Leitold H., Posch R., Encyclopedia of Digital Government, 2007, Idea Group Inc.

[85] Candia T., Madsen P., Enabling Federated Identity for E-Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[86] Candia T., Madsen P., Enabling Federated Identity for E-Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[87] Shibboleth. (n.d.). (http://shibboleth.internet2.edu/)

[88] WS-Secure Exchange Technical Committee. (n.d.).

(www.oasis- open.org/committees/tc_home.php?wg_abbrev=ws-sx)

[89] Candia T., Madsen P., Enabling Federated Identity for E-Government, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[90] Κάτος Β. – Στεφανίδης Γ., Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ΖΥΓΟΣ, 396, 2003

[91] Κακαβάς Γ., Δημιουργία Εφαρμογής για την Κρυπτογράφηση και Αποκρυπτογράφηση Γραπτού Κειμένου, Διπλωματική Εργασία, Πάτρα - Φεβρουάριος 2009

[92] Ζορκάδης Βασίλειος Διδάκτωρ Πληροφορικής, Ηλεκτρολόγος Μηχανικός Πανεπιστημίου Αιγαίου, Κρυπτογραφία, Ελληνικό Ανοικτό Πανεπιστήμιο, Πάτρα 2002

[93] Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, (http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroE sign.html)

[94] Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, (http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroE sign.html)

[95] Housley R., Polk W., Ford W., Solo D., RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, 2002; (http://www.faqs.org/rfcs/rfc3280.html)

[96] Simple Public Key Infrastructure (spki) Charter; (http://www.ietf.org/html.charters/spki-charter.html)

[97] Atkins D., Stallings W., Zimmermann P., RFC 1991 - PGP Message Exchange Formats, IETF, 1996; (http://www.faqs.org/rfcs/rfc1991.html)

[98] Callas J., Donnerhacke L., Finney H., Thayer R., RFC 2440 - OpenPGP Message Format, IETF, 1998; (http://www.faqs.org/rfcs/rfc2440.html)

[99] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005

[100] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005

[101] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005

[102] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005

[103] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005

[104] Σφάγγος Αλέξανδρος, Έξυπνες Κάρτες σε Εφαρμογές Ηλεκτρονικής Διακυβέρνησης, Διπλωματική Εργασία, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, Ιούλιος 2005; (artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/.../DT2005-0158.doc)

[105] Kahn, M., Steganography mailing list, 1995.

[106] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[107] Su, J. K., Eggers, J. J., & Girod, B., Capacity of digital watermarks subjected to an optimal collusion attack. Proceedings of European Signal Processing Conference (EUSIPCO 2000), Tampere, 5-8 September 2000, Finland (Vol. 4).

[108] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[109] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997), Secure spread spectrum watermarking for multimedia, 1997, IEEE Transactions on Image Processing.

[110] Barni, M., Bartolini, F., & Piva, A., Improved wavelet-based watermarking through pixel-wise masking, 2001, IEEE Transactions on Image Processing.

[111] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[112] Chor, B., Fiat, A., Naor, M., & Pinkas, B. , Tracing traitors, 2000, IEEE Transactions on Information Theory.

[113] Pfitzmann, B., & Waidner, M. Anonymous fingerprinting. Proceedings of EURO CRYPT'97, Konstanz, 11-15 May 1997, Germany (LNCS Vol. 1223.

[114] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[115] Huayin Si & Chang-Tsun Li, Maintaining Information Security in E-Government through Steganology, Encyclopedia of Digital Government, 2007, Idea Group Inc.

[116] http://www.ermis.gov.gr/portal/page/portal/ermis/aboutErmis

[117] http://www.ermis.gov.gr/portal/page/portal/ermis/webAccessibility

[118] http://www.ermis.gov.gr/portal/page/portal/ermis/personalData

[119] http://www.gsis.gr/digisign/index.html

[120] www.ika.gr

[121] http://www.oaed.gr/Pages/SN_14.pg

[122] http://jobsearch.oaed.gr/default.php?pname=Terms&t=1

[123] http://www.amea.gov.gr/

[124] http://www.hellenicparliament.gr/