ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ - ΚΑΤΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΑΥΤΟΠΟΙΗΣΗ ΠΟΛΙΤΩΝ ΣΕ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

(IDENTIFICATION OF CITIZENS IN DIGITAL GOVERNANCE SERVICES)

Επιβλέπουσα : Ευαγγελία (Λίλιαν) Μήτρου Καθηγήτρια Πανεπιστημίου Αιγαίου

Ονοματεπώνυμο: Παπαδοπούλου Ελένη

ΑΜ: icsdm620021

Σάμος, Μάρτιος 2022

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου κ. Λίλιαν Μήτρου για την καθοδήγηση, την βοήθεια και την άμεση ανταπόκριση σε όλη την διάρκεια της εκπόνησης της παρούσας μεταπτυχιακής διπλωματικής. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη, τόσο οικονομικά αλλά και ψυχολογικά, της προσπάθειάς μου, για την υπομονή που έδειξαν στις πολύωρες απουσίες μου και την αγάπη τους.

ΠΕΡΙΛΗΨΗ

Οι Νέες τεχνολογίες, πλέον, προσφέρουν ένα ευρύ φάσμα ευκαιριών για την αύξηση της αποδοτικότητας, της αποτελεσματικότητας, της διαφάνειας και της συμμετοχής σε όλους τους τομείς πολιτικής. Αυτό έχει σαν αποτέλεσμα, οι ΤΠΕ να επηρεάζουν τις κρατικές υπηρεσίες και γενικότερα τον τρόπο με τον οποίο λειτουργούν οι δημόσιοι φορείς. Σκοπός της παρούσας εργασίας, είναι η διερεύνηση μελέτη της ταυτοποίησης των πολιτών κατά την είσοδό τους σε ηλεκτρονικές υπηρεσίες. Πιο συγκεκριμένα, στην εργασία γίνεται προσπάθεια να εξεταστεί η υπάρχουσα βιβλιογραφία που ασχολείται με την ηλεκτρονική διακυβέρνηση και την ψηφιακή ταυτοποίηση. Αρχικά, στην εργασία γίνεται αναφορά στην έννοια της Ηλεκτρονικής Διακυβέρνησης, αλλά και στην έννοια της Ηλεκτρονικής Ταυτοποίησης. Στη συνέχεια γίνεται αναφορά στους νόμους και τους κανόνες της ταυτοποίησης των πολιτών και της ιδιωτικότητας, ενώ περιγράφεται τόσο το Σύστημα Ηλεκτρονικής Ταυτοποίησης στην Ελλάδα, όσο και το Σύστημα Ηλεκτρονικής Ταυτοποίησης στην ΕΕ. Η εργασία ολοκληρώνεται με αναφορά στο μέλλον των συστημάτων ηλεκτρονικής ταυτοποίησης και συγκεκριμένα στις νέες μεθόδους και τεχνολογίες, αλλά και με αναφορά στους προτεινόμενους τρόπους βελτίωσης.

Λέξεις-κλειδιά: Ηλεκτρονική διακυβέρνηση, ηλεκτρονική ταυτοποίηση, νομοθεσία, ιδιωτικότητα

ABSTRACT

New technologies now offer a wide range of opportunities to increase efficiency, effectiveness, transparency and involvement in all policy areas. As a result, ICTs affect government services and, more generally, the way public bodies operate. The purpose of this paper is to investigate the study of the identification of citizens when entering online services. More specifically, the paper attempts to examine the existing literature dealing with e-government and digital identification. Initially, the work refers to the concept of e-Government, but also to the concept of e-Identification. The following is a reference to the laws and rules of citizen identification and privacy, while describing both the Electronic Identification System in Greece and the Electronic Identification System in the EU. The work concludes with a reference to the future of electronic identification systems new methods and technologies, but also with reference to the proposed ways of improvement.

Keywords: e-Government, e-Identification, Legislation, Privacy

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1. Ηλεκτρονική Διακυβέρνηση και Ηλεκτρονική Ταυτοποίηση Πολιτών

Μέχρι σήμερα, οι κυβερνήσεις σε όλο τον κόσμο έχουν αναγνωρίσει ευρέως τη δυνατότητα των νέων τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) να επιφέρουν θεμελιώδη ανανέωση όχι μόνο στις διαδικασίες της κυβέρνησης και του δημόσιου τομέα, αλλά και στη σχέση τους με τις κοινωνικές ομάδες των πολιτών, τον ιδιωτικό τομέα, τους πολίτες και διάφορους άλλους ενδιαφερόμενους. Στις κυβερνητικές σχέσεις με τους πολίτες, την κοινωνία των πολιτών και τις επιχειρήσεις (για παράδειγμα: δημοκρατικές διαδικασίες, παροχή δημόσιων υπηρεσιών ή εφαρμογή πολιτικής), διευθετήσεις μεταξύ των οργανισμών (για παράδειγμα: συντονισμός πολιτικής, εφαρμογή πολιτικής ή παροχή δημόσιας υπηρεσίας) και σε ενδοοργανωτικές δραστηριότητες (για παράδειγμα: ανάπτυξη πολιτικής, επιχειρησιακές δραστηριότητες ή διαχείριση γνώσης), οι ΤΠΕ προσφέρουν ένα ευρύ φάσμα ευκαιριών για την αύξηση της αποδοτικότητας, της αποτελεσματικότητας, της διαφάνειας και της συμμετοχής σε όλους τους τομείς πολιτικής. Σαφώς, οι ΤΠΕ επηρεάζουν τις κρατικές υπηρεσίες, τους όρους και τις προϋποθέσεις υπό τις οποίες λειτουργούν οι πολιτικοί παράγοντες και οι δημόσιοι υπάλληλοι και γενικότερα τον τρόπο με τον οποίο λειτουργούν οι δημόσιοι φορείς (Prins, 2007).

Οι βελτιώσεις στις τεχνολογίες αναγνώρισης, η ταχεία εξάπλωση των προγραμμάτων ψηφιακής ταυτοποίησης και ο αυξανόμενος αριθμός υπηρεσιών και συναλλαγών που εξαρτώνται από την ακριβή αναγνώριση δεν ήταν τίποτα λιγότερο από επαναστατικές. Οι άνθρωποι μπορούν να αναγνωριστούν μοναδικά χρησιμοποιώντας το δακτυλικό τους αποτύπωμα ή τη σάρωση ίριδας και μπορούν να αποδείξουν ποιοι είναι με πρωτοφανή ακρίβεια. Τα συστήματα ψηφιακής ταυτοποίησης αναδιαμορφώνουν τη σχέση μεταξύ πολίτη και κράτους και μεταμορφώνουν τον τρόπο εφαρμογής των αναπτυξιακών πολιτικών και προγραμμάτων. Καθώς αυξάνεται ο αριθμός των ατόμων με επίσημα έγγραφα ταυτότητας, αυξάνεται και η ικανότητά τους να συμμετέχουν πλήρως στην κοινωνική, οικονομική και πολιτική ζωή της χώρας τους. Η ταυτοποίηση βρίσκεται πλέον σταθερά στην αναπτυξιακή ατζέντα. Την τελευταία δεκαετία, η παροχή υπηρεσιών εγγραφής και αναγνώρισης έχει αναδειχθεί ως σημαντικός στόχος πολιτικής για τις κυβερνήσεις των αναπτυσσόμενων χωρών και τους εταίρους τους. Η παροχή «νομικής ταυτότητας για όλους» έως το 2030 είναι πλέον ο στόχος 16,9 στο πλαίσιο των Στόχων Βιώσιμης Ανάπτυξης (SDGs) (Gelb & Metz, 2017).

1.2. Αντικείμενο της Διπλωματικής Εργασίας

Σκοπός της παρούσας εργασίας, είναι η διερεύνηση μελέτη της ταυτοποίησης των πολιτών κατά την είσοδό τους σε ηλεκτρονικές υπηρεσίες. Πιο συγκεκριμένα, στην εργασία γίνεται προσπάθεια να εξεταστεί η υπάρχουσα βιβλιογραφία που ασχολείται με την ηλεκτρονική διακυβέρνηση και την ψηφιακή ταυτοποίηση.

1.3. Διάρθρωση/Μεθοδολογία

Η εργασία αποτελείται από συνολικά επτά κεφάλαια. Το πρώτο κεφάλαιο περιλαμβάνει μια εισαγωγή στο υπό διερεύνηση ζήτημα όπου αναφέρεται ο σκοπός της εργασίας, η διάρθρωση και η μεθοδολογία της. Στο δεύτερο κεφάλαιο γίνεται αναφορά στην έννοια της Ηλεκτρονικής Διακυβέρνησης, όπου αποτυπώνονται οι εφαρμογές Ηλεκτρονικής Διακυβέρνησης, η αρχιτεκτονική των εφαρμογών Ηλεκτρονικής Διακυβέρνησης, τα οφέλη της Ηλεκτρονικής Διακυβέρνησης και τα ζητήματα ιδιωτικότητας που προκύπτουν. Στο τρίτο κεφάλαιο γίνεται αναφορά στην έννοια της Ηλεκτρονικής Ταυτοποίησης, όπου αναφέρονται οι μέθοδοι ταυτοποίησης, η υποδομή των Συστημάτων Ηλεκτρονικής Ταυτοποίησης και η αρχιτεκτονική τους. Το τέταρτο κεφάλαιο ασχολείται με τους νόμους και τους κανόνες της ταυτοποίησης των πολιτών και της ιδιωτικότητας, όπου συζητούνται τα ζητήματα απορρήτου στην ηλεκτρονική διακυβέρνηση και η πολιτική του, οι λόγοι για απειλές ιδιωτικού απορρήτου στην ηλεκτρονική διακυβέρνηση, η ασφάλεια και οι κινδυνοι των πληροφοριακών συστημάτων και των δεδομένων και παρουσιάζεται το ισχύον νομικό πλαίσιο περί απορρήτου, ταυτοποίησης και ηλεκτρονικής διακυβέρνησης. Στο πέμπτο κεφάλαιο περιγράφεται το Σύστημα Ηλεκτρονικής Ταυτοποίησης στην Ελλάδα, το Σύστημα Ηλεκτρονικής Ταυτοποίησης στην ΕΕ και πραγματοποιείται σύγκριση των αυτών. Το έκτο κεφάλαιο ασχολείται με το μέλλον των συστημάτων ηλεκτρονικής ταυτοποίησης και συγκεκριμένα με τις νέες μεθόδους και τεχνολογίες. Το έβδομο και τελευταίο κεφάλαιο είναι ο επίλογος της εργασίας όπου αποτυπώνονται προτεινόμενοι τρόποι βελτίωσης και αναφέρονται τα συνολικά συμπεράσματα της εργασίας.

Για την καλύτερη διεξαγωγή της συγκεκριμένης βιβλιογραφικής επισκόπησης πραγματοποιήθηκε διεξοδική μελέτη αναζήτησης των κατάλληλων βιβλίων, άρθρων και ηλεκτρονικών πηγών σε

αρκετές βάσεις δεδομένων με σκοπό την διασφάλιση μίας όσο το δυνατόν σφαιρικής «εικόνας» για τα ζητήματα που πραγματεύεται η εν λόγω βιβλιογραφική ανασκόπηση. Πιο συγκεκριμένα, οι βάσεις δεδομένων που επιλέχθηκαν αποτελούν έγκυρες και αξιόπιστες πηγές οι οποίες περιλαμβάνουν εγκεκριμένα περιοδικά στα οποία είναι δημοσιευμένα τα σχετικά άρθρα που μελετήθηκαν. Η αναζήτηση των άρθρων, περιοδικών καθώς και ηλεκτρονικών πηγών πραγματοποιήθηκε με τη χρήση λέξεων-κλειδιά ώστε να διασφαλιστεί το όσο δυνατότερο έγκυρο, αξιόπιστο και σύγχρονο αποτέλεσμα. Οι λέξεις-κλειδιά που χρησιμοποιήθηκαν ήταν λέξεις που αφορούν τόσο μεμονωμένες όσο και συνδυαστικές έννοιες έτσι ώστε να καλυφτούν οι πτυχές του θέματος της βιβλιογραφικής ανασκόπησης όσο καλύτερα γίνεται. Ο αριθμός των αποτελεσμάτων που εμφανίστηκαν ύστερα από την χρήση των παραπάνω λέξεων-κλειδιά ήταν αρκετά μεγάλος και οι πηγές που επιλέχθηκαν για τη διερεύνηση του θέματος είναι περιορισμένες και στοχευμένες.

ΚΕΦΑΛΑΙΟ 2: ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ

2.1. Τι είναι η Ηλεκτρονική Διακυβέρνηση

Καθώς οι κοινωνίες προχωρούν τεχνολογικά, οι πολίτες αναμένουν ότι η πρόσβαση, η ευκολία, η αξιοπιστία και η ταχύτητα παροχής υπηρεσιών θα αυξηθούν αντίστοιχα. Η αλλαγή στον δημόσιο τομέα περιορίζεται από εσωτερικούς και εξωτερικούς παράγοντες, όπως μεταξύ άλλων: γραφειοκρατία, υφιστάμενοι νόμοι και κανονισμοί, πολιτικές παρεμβάσεις, ανησυχίες για το απόρρητο, απαρχαιωμένες τεχνολογίες και υποδομές ακατάλληλες για την υιοθέτηση τεχνολογιών υψηλού επιπέδου. Επιπλέον, η λογοδοσία, η διαφάνεια και η έλλειψη εμπιστοσύνης είναι σημαντικά προβλήματα που αντιμετωπίζουν σχεδόν όλες οι κυβερνήσεις. Οι πρόσφατες πρωτοβουλίες που υποστηρίζουν στρατηγικές προσανατολισμένες στον πολίτη που υποστηρίζονται από την ψηφιακή διακυβέρνηση έχουν σχεδιαστεί για να ανταποκρίνονται στις πολλαπλές προκλήσεις που αντιμετωπίζουν οι δημόσιοι φορείς.

Από τα τέλη της δεκαετίας του 1990, οι περισσότερες χώρες έχουν εφαρμόσει ή υιοθετήσει πρωτοβουλίες ηλεκτρονικής διακυβέρνησης. Η ηλεκτρονική διακυβέρνηση είναι ένα πολυδιάστατο θέμα το οποίο αποτελείται από τεχνολογικές επιστήμες, διοικητικές, κοινωνικές αλλά και πολιτικές. Αποτελεί μία από τις μεγαλύτερες προκλήσεις για τη δημιουργία ενός ψηφιακού κράτους, ο μετασχηματισμός του οποίου είναι πολύ σημαντικός καθώς μέσω ψηφιακών τεχνολογιών, τη δημιουργία κανόνων και υποδομών, μπορούν να αντιμετωπιστούν μεγάλα προβλήματα όπως λειτουργικά κόστη, διαφάνεια, μεγαλύτερη αποτελεσματικότητα και λιγότερη αμφισβήτηση, καθώς και να ληφθούν πολιτικές και οργανωτικές αποφάσεις σε όλο το φάσμα του οργανισμού. Ο μετασχηματισμός της δημόσιας διοίκησης οδηγεί στην επένδυση έργων τεχνολογιών και πρωτοβουλιών ηλεκτρονικής διακυβέρνησης δίνοντας με αυτό τον τρόπο τη δυνατότητα στους πολίτες να ενημερώνονται σε άμεσο χρόνο και να αναζητούν τις υπηρεσίες που επιθυμούν μέσα από ένα φιλικό προς το χρήστη περιβάλλον. Στόχος της δημόσιας διοίκησης είναι να προσφέρει περισσότερες , γρήγορες και αποτελεσματικότερες υπηρεσίες προς τους αποδέκτες εξαλείφοντας τη δυσαρέσκειά του πολίτη προς το ελληνικό κράτος. Για να γίνει αυτό ο δημόσιος τομέας οφείλει να εκσυγχρονιστεί χρησιμοποιώντας τεχνολογίες πληροφορικής και επικοινωνιών βελτιώνοντας την αποτελεσματικότητα των παρεχόμενων υπηρεσιών του. Η ηλεκτρονική διακυβέρνηση αποτελεί σημαντική συνιστώσα από την άποψη των συνολικών μεταρρυθμιστικών προγραμμάτων, διότι χρησιμεύει ως εργαλείο για την αναδιαμόρφωση ης δημόσιας διοίκησης, υπογραμμίζοντας τις εσωτερικές συνέπειες και τη δέσμευση για την εξασφάλιση των στόχων της ηλεκτρονικής διακυβέρνησης (OECD, 2003). Σε αυτό το μήκος κύματος χρησιμεύουν οι ΤΠΕ, απευθυνόμενες στην αποτελεσματικότητα των προσφερόμενων υπηρεσιών, στη βελτίωση της δημόσιας διοίκησης και επικεντρώνονται στην μεταρρύθμιση της διακυβέρνησης και στην βελτίωση των σχέσεων μεταξύ των πολιτών και των επιχειρήσεων από την παροχή, σε αυτούς, ολοκληρωμένων συναλλασσόμενων δημόσιων υπηρεσιών.

Η ψηφιακή διακυβέρνηση (Digital Governance) ορίζεται ευρέως ως η προηγμένη χρήση των ΤΠΕ ως στρατηγικές για τη βελτίωση της απόδοσης του οργανισμού (Michael E. Milakovich, 2011). Οι πελατοκεντρικές κυβερνήσεις χρησιμοποιούν τη δύναμη του Διαδικτύου για να συνδέσουν στενότερα τους πολίτες με τους παρόχους δημόσιων υπηρεσιών. Το κόστος συναλλαγών μειώνεται και οι διαδικασίες εξορθολογίζονται προσφέροντας πιο υπεύθυνες,

ικανές και ανταποκρινόμενες υπηρεσίες. Η ψηφιακή διακυβέρνηση είναι μια στρατηγική για τις κυβερνήσεις σε όλα τα επίπεδα για την επίτευξη στόχων οικονομικής ανάκαμψης, τη μείωση του κόστους και την κάλυψη των προσδοκιών των πολιτών.

Γενικά, η ηλεκτρονική διακυβέρνηση περιλαμβάνει τη χρήση τεχνολογιών πληροφοριών και επικοινωνιών για την αύξηση και τη βελτίωση των αλληλεπιδράσεων μεταξύ δημόσιων οργανισμών και πολιτών (ιδιωτών ή επιχειρήσεων) για παροχή υπηρεσιών, ηλεκτρονικές συναλλαγές ή πρόσβαση σε πληροφορίες. Ενώ οι αρχικοί ορισμοί της ηλεκτρονικής διακυβέρνησης υιοθέτησαν κυρίως τεχνικές και τεχνολογικές προοπτικές, σε μια βάθος εξέταση αποκαλύπτονται περισσότερες πτυχές του θεματος. Μπορεί να θεωρηθεί ως ένας γρήγορος και πολυεπίπεδος μετασχηματισμός που επηρεάζει τη σχέση της κυβέρνησης με διαφορετικούς ενδιαφερόμενους φορείς ταυτόχρονα.

2.1.1. Διαστάσεις Ηλεκτρονικής Δημόσιας Διοίκησης

Ως "Ηλεκτρονική Δημόσια Διοίκηση" (e-Government) ορίζεται η χρήση των ΤΠΕ για την ηλεκτρονική υποστήριξη (Λουκής, Αποστολάκης, Χάλαρης, 2008):

- τόσο των εσωτερικών λειτουργιών των Δημόσιων Οργανισμών (μέσω εσωτερικών πληροφοριακών συστημάτων),

- όσο και της επικοινωνίας και συνεργασίας τους με το εξωτερικό τους περιβάλλον (μέσω "εξωστρεφών" πληροφοριακών συστημάτων που σήμερα βασίζονται κυρίως στο Internet), το οποίο περιλαμβάνει πολίτες (Government to Citizen – G2C (ή Administration to Citizen – A2C)), επιχειρήσεις (Government to Business – G2B (ή Administration to Business – A2B)) καθώς επίσης και άλλους Δημόσιους Οργανισμούς (Government to Government – G2G (ή Administration to Administration – A2A)).

Ένας ενδιαφέρον ορισμός της Ηλεκτρονικής Δημόσιας Διοίκησης, ο οποίος δίνει έμφαση στις πολιτοκεντρικές στοχεύσεις της, έχει δοθεί από τον Οργανισμό Ηνωμένων Εθνών (UN Division of Public Economics and Public Administration, American Society for Public Administration, (2002)):" Ηλεκτρονική Δημόσια Διοίκηση σημαίνει μία μόνιμη δέσμευση της Κυβέρνησης για τη βελτίωση των σχέσεων μεταξύ των πολιτών και του Δημόσιου Τομέα μέσω της βελτιωμένης, αποτελεσματικής και αποδοτικής παροχής υπηρεσιών, πληροφοριών και γνώσεων ".

Όταν αναφερόμαστε σήμερα στο πεδίο της Ηλεκτρονικής Δημόσιας Διοίκησης δεν αναφερόμαστε μόνο στην ανάπτυξη πληροφοριακών υποδομών στο εσωτερικό των Δημόσιων Οργανισμών, αλλά και στην ανάπτυξη εξωστρεφών πληροφοριακών συστημάτων, τα οποία απευθύνονται στο εξωτερικό τους περιβάλλον, παρέχοντας στους πολίτες και τις επιχειρήσεις δυνατότητες τόσο ηλεκτρονικής πληροφόρησης, όσο και ηλεκτρονικής πραγματοποίησης των συναλλαγών τους με την Δημόσια Διοίκηση (π.χ. αιτήσεων, δηλώσεων, πληρωμών, κ.λπ.) μέσω του Internet ή και άλλων ηλεκτρονικών μέσων (e-Transactions). Στο πεδίο της Ηλεκτρονικής Δημόσιας Διοίκησης συμπεριλαμβάνεται επίσης και η "Ηλεκτρονική Δημοκρατία" (e-Democracy), η οποία συνίσταται στην χρήση ηλεκτρονικών μέσων (π.χ. του

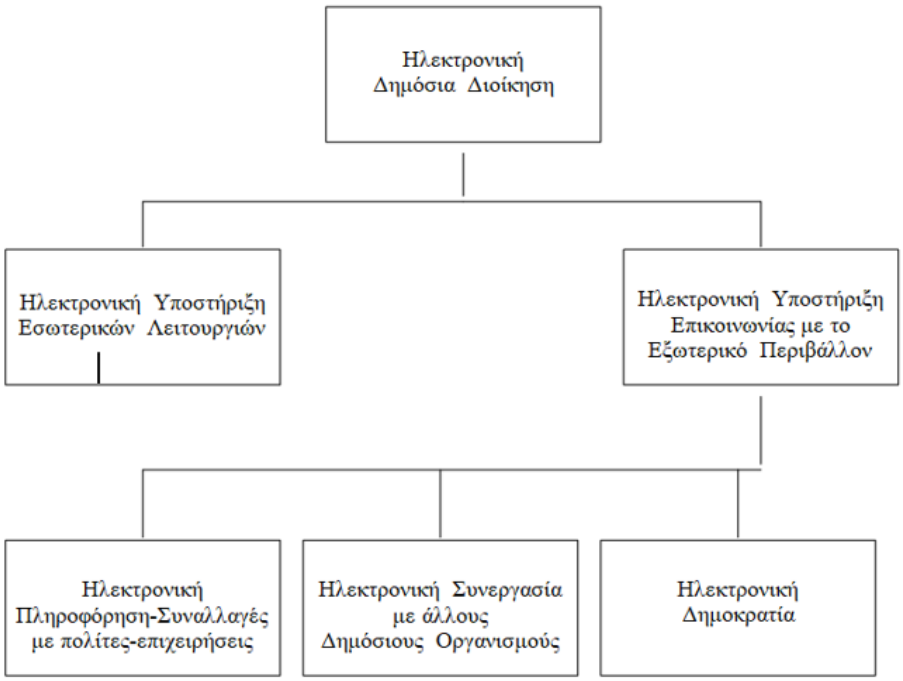
Internet) για την υποστήριξη της επικοινωνίας των πολιτών με την Δημόσια Διοίκηση, καθώς επίσης και της συμμετοχής των πολιτών στα κοινά, μέσω:

- παροχής στους πολίτες εκτεταμένης ηλεκτρονικής πληροφόρησης σχετικά με τις αποφάσεις και τις ενέργειες των Δημόσιων Οργανισμών,

- Ηλεκτρονικών Φορμών Εκφρασης Παραπόνων και Απόψεων (e-Forms),

- Ηλεκτρονικών Διαβουλεύσεων για σημαντικά θέματα (e-Consultations), στις οποίες οι συμμετέχοντες μπορούν να εκφράσουν απόψεις για το υπό διαβούλευση θέμα, να διαβάσουν τις απόψεις που εκφράσθηκαν από άλλους, να εκφράσουν επ' αυτών θετικές/αρνητικές απόψεις, κ.λπ. - Ηλεκτρονικών Ψηφοφοριών (e-Voting),κ.λπ.,

οι οποίες αγγίζουν πλέον τον βασικό πυρήνα του Δημοκρατικού Πολιτεύματος.



ΓΡΑΦΗΜΑ 1: *Διαστάσεις Ηλεκτρονικής Δημόσιας Διοίκησης (Λουκής, Αποστολάκης, Χάλαρης, 2008)*

Αξιοποιώντας δημιουργικά τις δυνατότητες που προσφέρουν οι ΤΠΕ, οι υφιστάμενες μακρές και πολύπλοκες διαδικασίες της Δημόσιας Διοίκησης μπορούν να ανασχεδιασθούν και να βελτιωθούν σημαντικά: κάποια βήματα μπορούν πλέον να καταργηθούν, κάποια άλλα μπορούν να εκτελούνται παράλληλα, κ.λπ., ώστε ο χρόνος και το κόστος υλοποίησής τους να μειωθούν δραστικά. Προκύπτει ότι οι ΤΠΕ τελικά επιφέρουν μείζονες αλλαγές στη Διακυβέρνηση (Governance) σε όλα τα επίπεδα:

- αφενός μετασχηματίζουν τον τρόπο της Διακυβέρνησης, π.χ. μέσω της παροχής ποιοτικότερων υπηρεσιών, της βελτίωσης των διαδικασιών παραγωγής τους, της

βελτίωσης των τρόπων πρόσβασης σε αυτές της από τους πολίτες, μείωσης του κόστους, κ.λπ.

- αφετέρου μετασχηματίζουν και την ίδια την ουσία και το περιεχόμενο της Διακυβέρνησης, μέσω αλλαγών που επιφέρει στην λειτουργία των δημοκρατικών διαδικασιών και πρακτικών, καθώς επίσης και στους στόχους, τις δραστηριότητες και τις υπηρεσίες των Δημόσιων Οργανισμών (Aicholzer and Schmutzer, 2000)

2.1.2. Καταλύτες για την Ανάπτυξη της Ηλεκτρονικής Διακυβέρνησης

NEW PUBLIC MANAGEMENT & OPEN AND PARTCIPATE DEMOCARCY

Τον 21ο αιώνα οι δημόσιες υπηρεσίες σε ολόκληρο τον κόσμο προσπαθούν να ανταποκριθούν στις αυξανόμενες απαιτήσεις ενός συνεχούς μεταβαλλόμενου περιβάλλοντος. Κάποια από τα σημαντικότερα ζητήματα που καλούνται να αντιμετωπίσουν οι σύγχρονες δημόσιες διοικήσεις είναι η αναδιοργάνωση του δημοσίου τομέα. Το κράτος οδηγήθηκε στο να έχει πολλά ζητήματα χωρίς και λίγους διαθέσιμους πόρους προς αξιοποίηση για φτάσει στην λύση τους. Με αυτή την λογική οι δημόσιοι οργανισμοί οδηγούνται στον ενστερνισμό των βασικών αρχών του New Public Management ως προς την αποτελεσματικότητα, την αποδοτικότητα, την οικονομικότητα, αλλά και τη σημασία που δίνεται στον απαιτούμενο έλεγχο των σύγχρονων συστημάτων και διαδικασιών. Στόχος του new public management είναι να μειώσει τα λειτουργικά κόστη, να αυξήσει τον ανταγωνισμό, να προσφέρει ευελιξία στη διοίκηση των οργανισμών, να αυξήσει τους ελέγχους αλλά και τη λογοδοσία για τη σωστή διαχείριση των πόρων, να προσφέρει κίνητρα για την επίτευξη της αποδοτικότητας όπως αμοιβές απόδοσης αλλά και να μπορεί να μετρηθεί η αποδοτικότητα έτσι ώστε να δωθούν καλύτερες υπηρεσίες και να δημιουργηθούν ευέλικτοι οργανισμοί ή παρόμοιοι με τους ιδιωτικούς και πλέον ο πολίτης να αντιμετωπίζεται ως πελάτης (Λουκής, 2008).

Η υιοθέτηση νέων τεχνολογιών παίζει σημαντικό ρόλο στις διοικητικές μεταρρυθμίσεις, η στήριξη των εσωτερικών λειτουργιών του δημοσίου, αλλά και η παροχή δημοσίων υπηρεσιών. Αυτό συνεπάγεται μία μετάβαση από τον παραδοσιακό τρόπο λειτουργίας του κράτους στον ηλεκτρονικό, αναθεωρώντας παραδοσιακές δομές και τον ρόλο του κράτους. Για αυτό και κρίνεται απαραίτητη η διαμόρφωση ενός προγράμματος που στοχεύει στην υποστήριξη της εγκατάστασης και της εφαρμογής νέων τεχνολογιών από τη δημόσια διοίκηση, με την δημιουργία ικανών ομάδων προετοιμασίας και διαχείρισης των νέων ψηφιοποιημένων υπηρεσιών, εκπαιδεύοντας κατάλληλα το προσωπικό και έχοντας ως γνώμονα την αποτελεσματικότερη εξυπηρέτηση του πολίτη.

Στενά συνδεδεμένη με την ηλεκτρονική διακυβέρνηση είναι και δυνατότητα συμμετοχής των πολιτών στη διαδικασία της ηλεκτρονικής διαβούλευσης, στη διαμόρφωση πολιτικών και στην λήψη αποφάσεως, ενισχύοντας τη διαφάνεια αλλά και τη δημοκρατικότητα (Λουκής, 2008). Η διαδικασία αυτή χαρακτηρίζεται ως ηλεκτρονική δημοκρατία καθώς δεν μιλάμε πλέον μόνο για την παροχή υπηρεσιών από δημόσιους φορείς προς τους πολίτες, αλλά ταυτόχρονα για την ενδυνάμωση των δημοκρατικών διαδικασιών. Η ανοιχτή και συνεργατική διακυβέρνηση (Open

and participate government) στοχεύει στον σχεδιασμό του απολογισμού του κράτους προς τον πολίτη και τη συνεργασία του με αυτόν μέσω της αρχής της διαφάνειας. Περιλαμβάνει το δημόσιο, τον ιδιωτικό τομέα και την κοινωνία, όπου επικοινωνούν όλοι και συνεργάζονται μεταξύ τους, για να πετύχουν περισσότερα από όσα μπορεί να πετύχει μόνος του ένας τομέας όσον αφορά την επίλυση προβλημάτων και τη λήψη αποφάσεων. Περιλαμβάνει τη διαφάνεια των δράσεων της κυβέρνησης και την εύκολη προσβασιμότητα σε κοινωνικές υπηρεσίες και πληροφορίες για την ανταπόκριση του δημοσίου τομέα σε νέες ιδέες και ανάγκες των πολιτών και των επιχειρήσεων.

2.1.3. Αρχές Ηλεκτρονικής Διακυβέρνησης

Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά καθώς και της παραγωγής ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του κράτους. Σύμφωνα με τον νόμο 4727/20 οι γενικές αρχές της ψηφιακής διακυβέρνησης είναι (Άρθρο 3 - Νόμος 4727/2020):

α) η αρχή της νομιμότητας και ιδίως την τήρηση των διατάξεων για την προστασία δεδομένων προσωπικού χαρακτήρα, οποιαδήποτε συναλλαγή με το δημόσιο πρέπει να διέπετε διέπεται από συγκεκριμένο νομικό πλαίσιο που διασφαλίζει τη νόμιμη παροχή της υπηρεσίας όπως η προστασία προσωπικών δεδομένων των πολιτών από το δημόσιο φορέα.

β) η αρχή της διαφάνειας, συνδέεται με την ανοιχτή διακυβέρνηση αφού οι δημόσιες υπηρεσίες πρέπει να παρέχουν στους συναλλασσόμενους τη δυνατότητα πρόσβασης στα δεδομένα τους και την παρακολούθηση της διαδικασίας της αίτησης τους.

γ) η αρχή της ισότητας και ιδίως της προσβασιμότητας, οι δημόσιοι φορείς να σχεδιάζουν τις παρεχόμενες ψηφιακές υπηρεσίες με τέτοιο τρόπο ώστε να μην απαιτούνται εξειδικευμένες γνώσεις ηλεκτρονικών υπολογιστών, ενισχύοντας την ισότητα και την εύκολη πρόσβαση σε ηλεκτρονικά δεδομένα και έγγραφα αλλά και την δυνατότητα της διαχείρισης τους με οποιοδήποτε τρόπο.

δ) η αρχή της αποδοτικότητας και της αρχής «μόνον άπαξ» μέσω της διαλειτουργικότητας, της ακρίβειας και της πληρότητας των ψηφιακών υπηρεσιών, των διαδικασιών και των δεδομένων. Συνεργασία όλων των πληροφοριακών συστημάτων του δημοσίου τομέα ώστε να διαλειτουργούν μεταξύ τους, να ανταλλάσσουν αυτοματοποιημένα δεδομένα και πληροφορίες, με αποτέλεσμα ο πολίτης να λαμβάνει το τελικό προϊόν της αιτούμενης υπηρεσίας με εύκολο και γρήγορο τρόπο.

ε) η αρχή της ακεραιότητας, ασφάλειας και εμπιστευτικότητας. Οι δημόσιες υπηρεσίες οφείλουν να παρέχουν ασφάλεια και εμπιστοσύνη κατά τη διαδικασία της παροχής ψηφιακών υπηρεσιών μέσα από διάφορους μηχανισμούς ταυτοποίησης των χρηστών, αλλά και την τήρηση κανόνων προστασίας των δεδομένων τους. Πρέπει να γνωστοποιείται στους πολίτες ο τρόπος με τον οποίον εξασφαλίζεται η προστασία των προσωπικών τους δεδομένων αλλά και η αντιμετώπιση των κινδύνων.

2.1.4. Διαλειτουργικότητα

Η διαλειτουργικότητα σήμερα θεωρείται το πιο σημαντικό χαρακτηριστικό των πληροφοριακών και επικοινωνιακών συστημάτων για την επίτευξη αυξημένης παραγωγικότητας και αποτελεσματικότητας, στην αυτοματοποιημένη παροχή υπηρεσιών για τους πολίτες και τις επιχειρήσεις. Η ανταλλαγή δεδομένων μεταξύ ποικίλων υπολογιστικών συστημάτων πολλές φορές είναι ανέφικτη. Στην ψηφιακή ατζέντα για το 2020, η Ευρωπαϊκή Επιτροπή έχει θέσει ως στόχο τη δημιουργία μιας ενιαίας ψηφιακής αγοράς στην Ευρώπη, η οποία θα υποστηρίζεται από ένα ενιαίο χώρο ταυτοτήτων. Η προσέγγιση αντιμετώπισης της σημερινής ανομοιογένειας των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης είναι η προώθηση της διαλειτουργικότητας των εθνικών συστημάτων. Το γεγονός αυτό απαιτεί ένα επιπρόσθετο επίπεδο διαλειτουργικότητας, το οποίο θα κρύβει την πολυπλοκότητα των διαφόρων συστημάτων σε τεχνικό και τεχνολογικό επίπεδο και θα επιτρέπει τις ελεγχόμενες από το χρήστη συναλλαγές διαπιστευτηρίων ταυτότητας μεταξύ ενός χρήστη από μια χώρα και ενός πάροχου υπηρεσιών από μια άλλη χώρα εντός της Ένωση. Για παράδειγμα αν ένας Έλληνας πολίτης θέλει να αγοράσει ένα διαμέρισμα προς πώληση στο Λονδίνο, τότε θα πρέπει να δοθεί σαν είσοδος η διεύθυνση. Όμως η μορφή της διεύθυνσης διαφέρει ανάμεσα στις δύο χώρες, λόγω της διαφορετικής σειράς με την οποία αναγράφονται ο αριθμός διεύθυνσης και ο Ταχυδρομικός Κώδικας. Εδώ λοιπόν οι εφαρμογές του e-government καλούνται να λύσουν παρόμοια προβλήματα εφαρμόζοντας μεθόδους που ανταλλάσουν δεδομένα με έναν σημασιολογικά διαλειτουργικό τρόπο.

Σύμφωνα με τον νόμο 4727/20 «Η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) του Υπουργείου Ψηφιακής Διακυβέρνησης είναι υπεύθυνη για την ηλεκτρονική ταυτοποίηση και την επιβεβαίωση ταυτότητας (αυθεντικοποίηση) των φυσικών προσώπων σύμφωνα με τα άρθρα 24 και 25 με σκοπό την παροχή ψηφιακών δημόσιων υπηρεσιών. Αποτελεί τον μοναδικό αρμόδιο φορέα για την υλοποίηση διατομεακής διαλειτουργικότητας και διαλειτουργικότητας των επιμέρους μητρώων των φορέων του δημόσιου τομέα σε συνεργασία με την Γενική Γραμματεία Ψηφιακής Διακυβέρνησης και Απλούστευσης Διαδικασιών, τον μοναδικό αρμόδιο φορέα για την ταυτοποίηση των φυσικών προσώπων μεταξύ των μητρώων των φορέων αυτών αξιοποιώντας τα επιμέρους αναγνωριστικά, και είναι αποκλειστικά υπεύθυνη για τη λειτουργία του Κέντρου Διαλειτουργικότητας (ΚΕΔ) και την υλοποίηση όλων των σχετικών δράσεων σε συνεργασία με τους ως άνω φορείς» (Άρθρο 84 - Νόμος 4727/2020).

2.1.4.1. Σημαντικότητα της Διαλειτουργικότητας

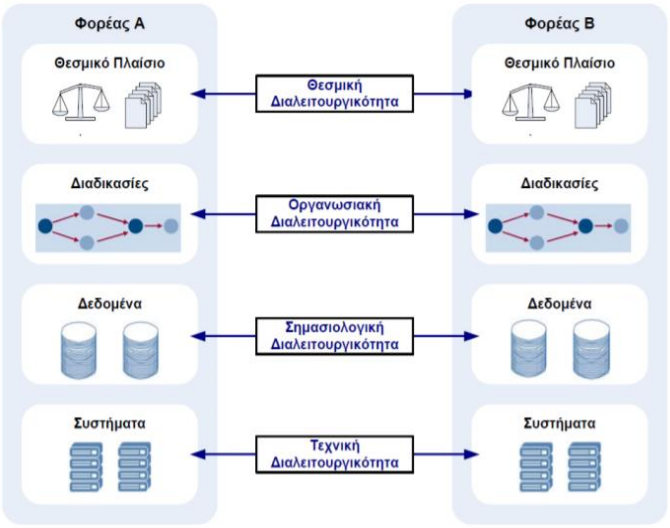
Η διαλειτουργικότητα στην ηλεκτρονική διακυβέρνηση έχει αναγνωριστεί ως ο παράγοντας κλειδί για την επίτευξη γρήγορων υπηρεσιών προς τους πολίτες και τις επιχειρήσεις, ενισχύοντας τη συνεργασία μεταξύ πολιτών, επιχειρήσεων και δημόσιων φορέων, ώστε να μειωθούν οι απαιτούμενες επενδύσεις για συντήρηση και διασύνδεση πολύπλοκων συστημάτων.

Είναι το πιο σημαντικό χαρακτηριστικό των πληροφοριακών συστημάτων για την αύξηση της παραγωγικότητας και αποτελεσματικότητας στην αυτοματοποίηση παρεχόμενων υπηρεσιών στους πολίτες και τις επιχειρήσεις, τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο. Στόχος είναι η δημιουργία one stop services, δηλαδή η εύρεση υπηρεσίας μέσα σε ένα δευτερόλεπτο με ένα κλικ χωρίς να μειώνεται η ασφάλεια, αλλά και η δημιουργία γεφυρών one-to-one διασυνδέοντας δεδομένα με πολλά πληροφοριακά συστήματα, χρησιμοποιώντας πρότυπα διαλειτουργικότητας τα οποία πρέπει να εφαρμοστούν εξαρχής από όλα τα πληροφοριακά συστήματα για να είναι έτοιμα να δια-λειτουργήσουν με αλλά μέσω web. Έτσι, προτείνεται η ψηφιοποίηση τυποποιημένων και συχνά χρησιμοποιούμενων υπηρεσιών όπως φορολογικές πληρωμές, επιστροφές, ασφαλιστικές εισφορές και προμήθειες. Βασικό στοιχείο είναι η όσο το δυνατόν μεγαλύτερη διαθεσιμότητα και χρήση του διαδικτύου στο ευρύ κοινό αφού αυτό είναι το βασικό κανάλι για την υλοποίηση ηλεκτρονικών πληρωμών. Τόσο οι υπηρεσίες G2C όσο και οι C2G πρέπει να είναι χρήσιμες και περιεκτικές. Η ασφαλής αναγνώριση και αυθεντικοποίηση είναι κρίσιμα στοιχεία για την παροχή e-services. Ωστόσο το πρόβλημα της λειτουργικότητας εντοπίζεται σε τρία επίπεδα (COM, 2017):

- Στις διαδικασίες: Απλούστευση διαδικασιών παροχής ηλεκτρονικών υπηρεσιών στους πολίτες και τις επιχειρήσεις από δημόσιους φορείς με άμεσο και αποτελεσματικό τρόπο μειώνοντας τη γραφειοκρατία.
- Στα δεδομένα: Ασφαλή ανταλλαγή των δεδομένων των πολιτών και των επιχειρήσεων στις συναλλαγές με το δημόσιο με το ισχύον νομικό πλαίσιο για την προστασία προσωπικών δεδομένων.
- Στα συστήματα: Ανάπτυξη των πληροφοριακών συστημάτων με τέτοιο τρόπο ώστα να είναι ικανά να διαλειτουργήσουν με ασφαλή μεταξύ τους, περιορίζοντας τις δαπάνες του δημόσιου τομέα μέσα από την ψηφιοποίηση συγκεκριμένων διαδικασιών, αλλά και με την εξοικείωση των πολιτών και των επιχειρήσεων με τη χρήση των τεχνολογιών πληροφορικής και επικοινωνιών.

2.1.4.2. Επίπεδα Διαλειτουργικότητας

Υπήρξαν πολλές προσεγγίσεις για την ανάλυση των εσωτερικών χαρακτηριστικών, των βασικών στοιχείων και της φύσης της διαλειτουργικότητας, κατά τη διάρκεια των τελευταίων ετών. Η διαλειτουργικότητα μπορεί να μελετηθεί υπό το πρίσμα τεσσάρων επιπέδων, τα οποία αφορούν το πλαίσιο με το οποίο θα παρέχονται οι ηλεκτρονικές υπηρεσίες σε επίπεδο κρατών ή Ευρωπαϊκής Ένωσης (COM, 2017)



Γράφημα 2: *Επίπεδα Διαλειτουργικότητας*

1) Η Οργανωσιακή Διαλειτουργικότητα αναφέρεται στην ευθυγράμμιση των επιχειρηματικών διεργασιών (business process) με στόχο τη διαμόρφωση διαδικασιών και την επίτευξη συνεργασίας των φορέων που επιδιώκουν ανταλλαγή πληροφοριών .Στοχεύει στην δημιουργία ηλεκτρονικών υπηρεσιών εύκολα προσβάσιμων ανταποκρίνοντας με αυτό τον τρόπο στις απαιτήσεις των χρηστών.

2) Η Σημασιολογική Διαλειτουργικότητα είναι η ικανότητα δύο ή περισσότερων υπολογιστικών συστημάτων που επικοινωνούν να ερμηνεύουν αυτόματα τις πληροφορίες που ανταλλάσσονται με ακρίβεια, με τη χρήση κοινών προτύπων για την περιγραφή των δεδομένων.

3) Η Τεχνολογική Διαλειτουργικότητα καλύπτει τεχνικά θέματα της σύνδεσης δύο ή περισσότερων υπολογιστικών συστημάτων, δηλαδή τα πρότυπα και οι αρχιτεκτονικές που πρέπει να χρησιμοποιηθούν για την ανάπτυξη συστημάτων σε επίπεδο επικοινωνίας και διαδικασιών για την αποθήκευση και ανάπτυξη δεδομένων, ώστε να δημιουργηθούν ολοκληρωμένες υπηρεσίες. Περιλαμβάνει θέματα που αφορούν πρότυπα για τα συστήματα αρχιτεκτονικής (πως το διαλειτουργικό σύστημα είναι δομημένο), πρότυπα για τα συστήματα διασύνδεσης (επικοινωνία, υπηρεσίες web, ανακάλυψη υπηρεσίας) και πρότυπα για την αποθήκευση και ανάκτηση πληροφοριών (σχήματα, μοντέλα, κλπ.).

4) Η Νομοθετική/Θεσμική Διαλειτουργικότητα αναφέρεται στην εναρμόνιση των νομοθετικών διατάξεων που διέπουν τη λειτουργία δύο ή περισσοτέρων φορέων, που επιθυμούν να συνεργαστούν για τη μεταξύ τους ανταλλαγή πληροφοριών ή/ και την παροχή ολοκληρωμένων ηλεκτρονικών υπηρεσιών προς πολίτες, επιχειρήσεις και άλλους φορείς. Επιπλέον αποσκοπεί στο να διασφαλίσει ότι οι ηλεκτρονικά ανταλλασσόμενες πληροφορίες έχουν την ίδια νομική ισχύ για όλους τους εμπλεκόμενους.

2.1.4.3. Κανόνες Διαλειτουργικότητας / Προϋποθέσεις Εξασφάλισης Διαλειτουργικότητας

- Προκειμένου να πραγματοποιηθεί μία αποτελεσματική επικοινωνία σε επίπεδο ανταλλαγής δεδομένων μεταξύ δημοσίων υπηρεσιών των πολιτών και οργανισμών πρέπει να υπάρχει ομοιομορφία και ισότιμη πρόσβαση σε δημόσιες υπηρεσίες και στα δημόσια δεδομένα

- Υιοθέτηση ανοιχτών αρχιτεκτονικών οι οποίες προωθούν την ελευθερία συστατικών των ΠΣ επιτρέποντας τη σύνδεση τους προσφέροντας

- Η ύπαρξη κοινών αποδεκτών προτύπων (standards) που περιγράφουν τον τρόπο επικοινωνίας των υποσυστημάτων και τη μορφή των πληροφοριών που ανταλλάσσουν.

- Ο έλεγχος των φορέων από ανεξάρτητους οργανισμούς για τη μη συμμόρφωση τους με τα πρότυπα..

Τα πληροφοριακά συστήματα των δημοσίων φορέων σχεδιάζονται ανάλογα με τις ανάγκες του κάθε οργανισμού και το είδος των παρεχόμενων υπηρεσιών προς τους πολίτες. Αυτό σημαίνει ότι κάθε οργανισμός οδηγείται στη δημιουργία εξειδικευμένων πληροφοριακών συστημάτων που εξυπηρετούν τις ανάγκες του, όπως π.χ. να επιτευχθεί η ανταλλαγή πληροφοριών, η γρήγορη εξυπηρέτηση του πολίτη με άντληση στοιχείων από διαφορετικούς οργανισμούς και φορείς του δημοσίου χωρίς τη δική του παρέμβαση, με τη συνεργασία των πληροφοριακών συστημάτων του δημοσίου τομέα. Τη λύση σε αυτό δίνει η θέσπιση διαδικασιών, ώστε να εξασφαλιστεί ένα ικανοποιητικό επίπεδο μεταφοράς και χρησιμοποίησης των πληροφοριών με ομοιογενές και αποτελεσματικό τρόπο μεταξύ των διαφορετικών πληροφοριακών συστημάτων των δημόσιων υπηρεσιών.

2.1.4.3.1. Ελληνικό Πλαίσιο Διαλειτουργικότητας (E-GIF)

Η χώρα μας ακολουθεί το greek interoperability framework που καθορίζεται την τεχνολογία, τις πολιτικές και τους κανονισμούς για την επίτευξη διαλειτουργικότητας και της συνοχής των ελληνικών συστημάτων του δημόσιου τομέα. Περιλαμβάνει κανόνες και πρότυπα που σχετίζονται με την εφαρμογή της στρατηγική της ηλεκτρονικής διακυβέρνησης αφορώντας τη διαλειτουργικότητα των πληροφοριακών συστημάτων, την ανάπτυξη των συναλλαγών ηλεκτρονικά, την ψηφιακή αποτύπωση των πολιτών, τα ανοιχτά δημόσια δεδομένα και έγραφα και την πιστοποίηση του σε διαδικτυακούς τόπους.

Το Ελληνικό Πλαίσιο Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης (Ελληνικό e-GIF) αποτελείται από τα ακόλουθα κύρια έγγραφα: (European Commission, 2010)

- Το Πλαίσιο Πιστοποίησης για ιστοσελίδες και πύλες Δημόσιας Διοίκησης, το οποίο καθορίζει τις κατευθύνσεις και τα πρότυπα που πρέπει να ακολουθούνται κατά την ανάπτυξη δημόσιων ιστοσελίδων για την Ελληνική Δημόσια Διοίκηση

- Το Πλαίσιο Διαλειτουργικότητας και Παροχής Ηλεκτρονικών Υπηρεσιών, το οποίο καθορίζει τις βασικές αρχές και τη γενική στρατηγική που πρέπει να ακολουθούν οι δημόσιοι φορείς κατά την ανάπτυξη Πληροφοριακών Συστημάτων ηλεκτρονικής διακυβέρνησης
- Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης, το οποίο θέτει τα πρότυπα, τις διαδικασίες και τις τεχνολογίες που απαιτούνται για την εγγραφή, την ταυτοποίηση και τον έλεγχο ταυτότητας των χρηστών (Πολίτες / Επιχειρήσεις)
- Το Μοντέλο Τεκμηρίωσης για Διαδικασίες και Δεδομένα Δημόσιας Διοίκησης, το οποίο περιγράφει τη σημείωση, τους κανόνες και τις προδιαγραφές για την τεκμηρίωση διαδικασιών, εγγράφων και ηλεκτρονικής ανταλλαγής δεδομένων.

2.1.4.3.2. Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας

Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας προσφέρει καθοδήγηση στους δημόσιους οργανισμούς για το πώς να βελτιώσουν τη διακυβέρνηση της διαλειτουργικότητας των δραστηριοτήτων τους, μέσα από την απλοποίηση των διαδικασιών, ώστε να υποστηρίζονται πλήρως οι ψηφιακές υπηρεσίες, σύμφωνα με τη νομοθεσία και να μην τίθενται σε κίνδυνο οι προσπάθειες της διαλειτουργικότητας. Στοχεύει στο να βοηθήσει τις κυβερνήσεις τόσο σε ευρωπαϊκό αλλά και σε εθνικό επίπεδο, να αναπτύξουν ψηφιακές υπηρεσίες με χρήση και επαναχρησιμοποίηση δεδομένων και καναλιών επικοινωνίας με διαφάνεια. Παρέχει οδηγίες για τον σχεδιασμό εθνικών στρατηγικών προώθησης της διαλειτουργικότητας, για τη δημιουργία ψηφιακής διασυνοριακής διαλειτουργικότητας και παροχής κοινωνικών υπηρεσιών (COM, 2017).

2.2. Τι Είναι Ηλεκτρονική Υπηρεσία

Ηλεκτρονικές ή ψηφιακές υπηρεσίες (electronic services, e-services) είναι οι υπηρεσίες οι οποίες δίνουν τη δυνατότητα πραγματοποίησης έγκυρων συναλλαγών, χρησιμοποιώντας τεχνολογίες πληροφορικής και επικοινωνιών. Ο όρος αναφέρεται στη χρήση όλων των ηλεκτρονικών καναλιών επικοινωνίας, όπως τηλεφωνικά κέντρα, «έξυπνα» κινητά τηλέφωνα, ψηφιακές τηλεοράσεις κλπ. Όλο και συχνότερα όμως ηλεκτρονικές υπηρεσίες νοούνται οι υπηρεσίες που παρέχονται μέσω διαδικτύου (Wikipedia, 2021)(Wimmer et al, 2008).

Η έκθεση συγκριτικής αξιολόγησης για την ηλεκτρονική διακυβέρνηση της ΕΕ αναφέρει ότι οι διαδικτυακές δημόσιες υπηρεσίες οφείλουν να χαρακτηρίζονται από (European Commission, 2018):

- εξ ορισμού ψηφιακός χαρακτήρας
- αρχή "μόνον άπαξ"
- κατάργηση των αποκλεισμών και προσβασιμότητα
- εξ ορισμού διασυνοριακός χαρακτήρας
- εξ ορισμού διαλειτουργικός χαρακτήρας
- αξιοπιστία και ασφάλεια δεδομένων στο διαδίκτυο

2.2.1. Κατηγοριοποίηση Των Υπηρεσιών Σε Επίπεδα Εμπιστοσύνης

Η κατηγοριοποίηση των υπηρεσιών σε επίπεδα εμπιστοσύνης γίνεται με βάση την κατηγορία των δεδομένων που αξιοποιούν, απλά, ευαίσθητα και οικονομικά, αλλά και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας και διαχείρισης τους. Σε επίπεδο εμπιστοσύνης που ορίζει το πλαίσιο ηλεκτρονικής διακυβέρνησης είναι τα ακόλουθα (Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Ψηφιακής Αυθεντικοποίησης, 2012):

•Επίπεδο Εμπιστοσύνης 0: Στο επίπεδο εμπιστοσύνης 0 εντάσσονται οι υπηρεσίες που αξιοποιούν δημόσια προσπελάσιμες πληροφορίες και έχουν ως στόχο την πληροφόρηση των πολιτών για συγκεκριμένα θέματα. Οι υπηρεσίες αυτές δεν απαιτούν την ανταλλαγή δεδομένων ή κάποιο βαθμό αβεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας ενός πολίτη.

•Επίπεδο Εμπιστοσύνης 1: Στο επίπεδο εμπιστοσύνης 1 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή δεδομένων ελάχιστες χρησιμότητας όπως για παράδειγμα ονοματεπώνυμο, email για τη διεκπεραίωση μιας συναλλαγής. Για αυτό και στο συγκεκριμένο επίπεδο απαιτείται μικρός βαθμός αβεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας του πολίτη ώστε να αποδεικνύεται η ορθότητα των στοιχείων του.

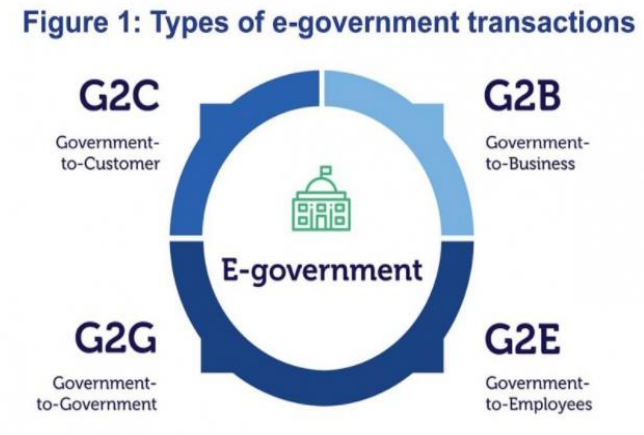
•Επίπεδο Εμπιστοσύνης 2: Στο επίπεδο εμπιστοσύνης 2 εντάσσονται οι υπηρεσίες που απαιτούν ανταλλαγή προσωπικών δεδομένων που μπορούν να χαρακτηριστούν ως ευαίσθητα για παράδειγμα στοιχεία που αφορούν οικογενειακή κατάσταση του χρήστη, ημερομηνία γέννησης, φύλο και άλλα. Στο συγκεκριμένο επίπεδο ο βαθμός αβεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας χαρακτηρίζεται ως μέτριος καθώς πρέπει να εξασφαλίσετε ότι οι υπηρεσίες προσφέρονται μόνο σε εξουσιοδοτημένα άτομα.

•Επίπεδο Εμπιστοσύνης 3: Στο επίπεδο εμπιστοσύνης 3 εντάσσονται οι υπηρεσίες που απαιτούν ανταλλαγή ευαίσθητων προσωπικών δεδομένων όπως ποινικό μητρώο. Ο χρήστης

πραγματοποιεί οικονομικές συναλλαγές με ηλεκτρονικό τρόπο. Συνεπώς οι επιπτώσεις που μπορεί να προκληθούν από κάποιο περιστατικό ασφαλείας είναι ιδιαίτερα σημαντικές για αυτό και είναι απαραίτητο να διασφαλιστεί υψηλός βαθμός εμπιστοσύνης για την ηλεκτρονική ταυτότητα ενός χρήστη.

2.2.2. Εφαρμογές Ηλεκτρονικής Διακυβέρνησης

Μια πρωτοβουλία ηλεκτρονικής διακυβέρνησης απαιτεί την ανάπτυξη συγκεκριμένων τύπων δυνατοτήτων για την παροχή διαφορετικών ειδών δημόσιων υπηρεσιών στο σωστό επίπεδο ωριμότητας (Soumaya et al., 2017). Η ηλεκτρονική διακυβέρνηση προσφέρει υπηρεσίες σε όσους εμπίπτουν στις αρμοδιότητές της να συναλλάσσονται ηλεκτρονικά με την κυβέρνηση. Αυτές οι υπηρεσίες διαφέρουν ανάλογα με τις ανάγκες των χρηστών και στους εμπλεκόμενους με αυτές οι οποίοι είναι οι πολίτες, οι επιχειρήσεις και η ίδια η Δημόσια Διοίκηση. Αυτή η ποικιλομορφία έχει οδηγήσει στην ανάπτυξη διαφορετικών τύπων ηλεκτρονικής διακυβέρνησης. Έτσι, η διάκριση γίνεται ανάλογα με την υπηρεσία που παρέχεται και σε ποιον απευθύνεται αυτή. Συγκεκριμένα, πρόκειται για τους ακόλουθους τομείς:



Γράφημα 3: *Τύποι Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης*

Πηγή: VIR, Vietnam Investment Review-. ‘Spurring E-Government Initiatives’. Vietnam Investment Review - VIR, 20 Απριλίου 2020, https://vir.com.vn/spurring-e-government-initiatives-75704.html.

2.2.2.1. Εφαρμογές Κυβέρνησης προς Πολίτες (G2C)

Η πλειονότητα των κρατικών υπηρεσιών εμπίπτει σε αυτήν την εφαρμογή, με σκοπό την παροχή στους πολίτες και σε άλλους πλήρεις ηλεκτρονικούς πόρους για να ανταποκρίνονται στις συνήθεις ανησυχίες των ατόμων και στις κρατικές συναλλαγές. Κυβέρνηση και πολίτες θα επικοινωνούν συνεχώς κατά την εφαρμογή της ηλεκτρονικής διακυβέρνησης, υποστηρίζοντας έτσι τη λογοδοσία, τη δημοκρατία και τις βελτιώσεις στις δημόσιες υπηρεσίες. Ο πρωταρχικός στόχος της ηλεκτρονικής διακυβέρνησης είναι η εξυπηρέτηση του πολίτη και η διευκόλυνση της αλληλεπίδρασης των πολιτών με την κυβέρνηση, καθιστώντας τις δημόσιες πληροφορίες πιο προσιτές μέσω της χρήσης ιστοσελίδων, καθώς και τη μείωση του χρόνου και του κόστους διεξαγωγής μιας συναλλαγής. Εφαρμόζοντας την ιδέα του G2C, οι πολίτες έχουν άμεση και άνετη πρόσβαση σε κρατικές πληροφορίες και υπηρεσίες από παντού, ανά πάσα στιγμή, μέσω της χρήσης πολλαπλών καναλιών. Εκτός από την πραγματοποίηση ορισμένων συναλλαγών, όπως πιστοποιήσεις, την αίτηση για πιστοποιητικό οικογενειακής κατάστασης από το ΚΕΠ, την πληρωμή κρατικών τελών και την υποβολή αίτησης για παροχές, η ικανότητα των πρωτοβουλιών G2C να ξεπερνούν πιθανά χρονικά και γεωγραφικά εμπόδια μπορεί να συνδέσει πολίτες που διαφορετικά δεν θα έρθουν σε επαφή μεταξύ τους και μπορεί με τη σειρά τους να διευκολύνουν και αύξηση της συμμετοχής των πολιτών στην κυβέρνηση. Στην αλληλεπίδραση του πολίτη με τις δημόσιες υπηρεσίες γίνονται μεγάλα και σημαντικά βήματα για τη μείωση της γραφειοκρατίας, με τη δημιουργία ενός «one-stop shoping» services, όπου οι πολίτες θα μπορούν να διεκπεραιώνουν διάφορες εργασίες τους, ειδικά εκείνες οι οποίες περιλαμβάνουν διάφορες κρατικές υπηρεσίες, χωρίς να είναι απαραίτητη η επικοινωνία του πολίτη με κάθε υπηρεσία ξεχωριστά. Απτά παραδείγματα αυτής της λειτουργίας είναι η ηλεκτρονική παροχή υπηρεσιών υγείας, δικαιοσύνης, εκπαίδευσης κλπ, μέσω της ηλεκτρονικής έκδοσης των απαιτούμενων εγγράφων και της ηλεκτρονικής πληρωμής. Μία επιτυχημένη G2C σχέση ενδυναμώνει την εμπιστοσύνη του πολίτη προς την κυβέρνηση και τις δομές της, ενθαρρύνοντας την ενεργή ηλεκτρονική συμμετοχή.

Το πρώτο νομικό πλαίσιο που θεσπίστηκε για την ηλεκτρονική διακυβέρνηση στην Ελλάδα ήταν ο νόμος ν. 3979/2011 ή «Νόμος για την ηλεκτρονική διακυβέρνηση» που ήταν ένα γενικό πλαίσιο που έδινε έμφαση στα (European Commission, 2016):

- ηλεκτρονική επικοινωνία και ανταλλαγή δεδομένων μεταξύ φυσικών/νομικών προσώπων και του δημόσιου τομέα
- ενημέρωση του δημόσιου τομέα
- ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων και την ιδιωτική ζωή.
- θέματα που αφορούν ηλεκτρονικές πληρωμές και την αυτόματη αναζήτηση αρχείων και εγγράφων

Σύμφωνα με το eGovernment Benchmark 2020 που εξέδωσε η Ευρωπαϊκή Επιτροπή, η Ελλάδα χαρακτηρίζεται από χαμηλό επίπεδο διείσδυσης και ψηφιοποίησης (European Commission, 2020a). Ως εκ τούτου, η Ελλάδα χαρακτηρίζεται ως μια χώρα που δεν εκμεταλλεύεται ακόμη πλήρως τις ευκαιρίες ΤΠΕ. Κατά τα τελευταία τέσσερα χρόνια, αύξησε το επίπεδο των

επιδόσεων της, ωστόσο υπολειτουργεί τόσο στη Διείσδυση όσο και στην Ψηφιοποίηση σε σύγκριση με χώρες με παρόμοια χαρακτηριστικά. Η έκθεση Benchmark (European Commission, 2020a) προτείνει ότι μπορεί να βελτιώσει το επίπεδο διείσδυσης αυξάνοντας τον αριθμό των ατόμων που υποβάλλουν επίσημες φόρμες ηλεκτρονικά στις διοικητικές αρχές ή αυτοματοποιώντας τις διαδικασίες και ζητώντας λιγότερα έντυπα από τους πολίτες.

2.2.2.2. Εφαρμογές Κυβέρνησης προς Επιχειρήσεις (G2B)

Κυβέρνηση προς επιχείρηση, ή G2B, είναι ο δεύτερος σημαντικός τύπος κατηγορίας ηλεκτρονικής διακυβέρνησης. Το G2B περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ επιχειρήσεων και οργανισμών του ιδιωτικού τομέα και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική προμήθεια για δημόσιους φορείς). Το G2B περιλαμβάνει διάφορες υπηρεσίες που ανταλλάσσονται με την κυβέρνηση συμπεριλαμβανομένης της διανομής πολιτικών, κανόνων και κανονισμών που σχετίζονται με το είδος της επιχείρησης. Οι προσφερόμενες επιχειρηματικές υπηρεσίες αδειοδότησης νέας επιχείρησης, νέους κανονισμούς, λήψη εντύπων αιτήσεων, φόρους διαμονής, ανανέωση αδειών, ελέγχου εγκυρότητας ΑΦΜ και φορολογικής ενημερότητας, λήψης πιστοποιητικού Ασφαλιστικής Ενημερότητας από το ΙΚΑ, ο έλεγχος του δικαιώματος χρήσης της επωνυμίας. Οι υπηρεσίες που προσφέρονται μέσω των συναλλαγών G2B διαδραματίζουν επίσης σημαντικό ρόλο στην ανάπτυξη των επιχειρήσεων και συγκεκριμένα στην ανάπτυξη των μικρών και μεσαίων επιχειρήσεων (Pascual, 2003). Οι εφαρμογές G2B οδηγούν ενεργά πρωτοβουλίες ηλεκτρονικών συναλλαγών, όπως οι ηλεκτρονικές προμήθειες και η ανάπτυξη μιας ηλεκτρονικής αγοράς για κρατικές αγορές και διενεργούν διαγωνισμούς κρατικών προμηθειών μέσω ηλεκτρονικών μέσων για ανταλλαγή πληροφοριών και αγαθών. Αυτό το σύστημα ωφελεί την κυβέρνηση από τις διαδικτυακές εμπειρίες των επιχειρήσεων σε τομείς όπως οι στρατηγικές ηλεκτρονικού μάρκετινγκ. Το G2B είναι εξίσου χρήσιμο με το σύστημα G2C, ενισχύοντας την αποτελεσματικότητα και την ποιότητα της επικοινωνίας και των συναλλαγών με τις επιχειρήσεις, αυξάνοντας την ισότητα και τη διαφάνεια των κρατικών συμβάσεων και έργων, μειώνοντας δραστικά την γραφειοκρατία και το χρόνο που χρειάζεται ο εκάστοτε ενδιαφερόμενος να λάβει τα απαιτούμενα έγγραφα ώστε να είναι σε θέση να λειτουργήσει την επιχείρηση του. Σ’ αυτού του είδους τη σχέση ανήκουν υπηρεσίες όπως η ηλεκτρονική δήλωση οικονομικών στοιχείων και η φορολογία των επιχειρήσεων (έναρξη εργασιών, περιοδική δήλωση ΦΠΑ, κατάσταση πελατών προμηθευτών, φορολογία εισοδήματος, υποβολή στοιχείων σε στατιστικές υπηρεσίες κλπ), οι ηλεκτρονικές προμήθειες (διενέργεια διαγωνισμών με δημόσιες υπηρεσίες, κατάθεση προσφορών, ηλεκτρονική αξιολόγηση και κατακύρωση του αποτελέσματος), οι ηλεκτρονικές τελωνειακές υπηρεσίες και οι ηλεκτρονικές αδειοδοτήσεις (Τζίφα, 2017).

Σημαντικά βήματα για τις εφαρμογές Κυβέρνησης προς Επιχειρήσεις στην Ελλάδα αποτελεί η διαδικτυακή παρουσία πληροφοριών για επιχειρήσεις σχετικά με την κυβέρνηση, όπως για παράδειγμα η ηλεκτρονική αναθεώρηση προϊόντων για είδη γραφείου, αλλά και οι υπηρεσίες και έντυπα ηλεκτρονικά και βάσεις δεδομένων για την υποστήριξη των συναλλαγών επιχειρήσεων με την κυβέρνηση, όπως η πραγματοποίηση αγοράς προμηθειών στο διαδίκτυο.

2.2.2.3. Εφαρμογές Κυβέρνησης προς Κυβέρνηση (G2G)

Οι υπηρεσίες G2G αποτελούν τη "ραχοκοκκαλια" της Ηλεκτρονικής Διακυβέρνησης. Αυτό συμβαίνει διότι προκειμένου το κράτος να έχει σωστή και αποτελεσματική επικοινωνία και παροχή υπηρεσιών τόσο στους πολίτες όσο και στις επιχειρήσεις, θα πρέπει πρώτα να υπάρχει το κατάλληλο ηλεκτρονικό υπόβαθρο για την επικοινωνία μεταξύ των διαφόρων κρατικών υπηρεσιών και συστημάτων. Αυτός ο τύπος ηλεκτρονικής διακυβέρνησης αναφέρεται στις διαδικτυακές επικοινωνίες μεταξύ κυβερνητικών οργανισμών, τμημάτων και υπηρεσιών που βασίζονται σε μια υπερκυβερνητική βάση δεδομένων. Περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ φορέων και οργανισμών που εμπίπτουν στη δικαιοδοσία της Δημόσιας Διοίκησης (π.χ. ηλεκτρονική ανταλλαγή πληροφοριών φορέων του Δημοσίου). Παρέχει πληροφορίες σχετικά με τις πολιτικές αποζημίωσης και παροχών, τις ευκαιρίες κατάρτισης και μάθησης των νόμων για τα πολιτικά δικαιώματα με εύκολα προσβάσιμο τρόπο. Η εσωτερική ανταλλαγή αγαθών και πληροφοριών, η συνεργασία πόρων και δεξιοτήτων μεταξύ των υπηρεσιών, η διαδικτυακή επικοινωνία και συνεργασία που επιτρέπει την κοινή χρήση βάσεων δεδομένων, ενισχύουν την αποτελεσματικότητα των διαδικασιών, ώστε να υπάρξει βελτίωση στις ηλεκτρονικές υπηρεσίες που παρέχονται στους πολίτες και τις επιχειρήσεις. (Ndou, 2004)

Ο ζωτικός στόχος της ανάπτυξης του G2G είναι να ενισχύσει και να βελτιώσει τις διακυβερνητικές οργανωτικές διαδικασίες με τον εξορθολογισμό της συνεργασίας και του συντονισμού. Σε ένα άλλο μέτωπο του G2G, η χρήση τεχνολογιών πληροφοριών από διαφορετικούς κυβερνητικούς φορείς για την ανταλλαγή ή τη συγκέντρωση πληροφοριών και την αυτοματοποίηση των διακυβερνητικών επιχειρηματικών διαδικασιών όπως η κανονιστική συμμόρφωση, έχει δημιουργήσει πολυάριθμες περιπτώσεις εξοικονόμησης χρόνου και κόστους και βελτίωσης των υπηρεσιών (Gregory, 2007).

Σε διεθνές επίπεδο Government to Government-international (G2G-I) ανήκουν οι υπηρεσίες, οι οποίες πραγματοποιούνται ανάμεσα σε παραπάνω περισσότερες από μία χώρες. Τέτοιου είδους υπηρεσίες βοηθούν τα κράτη να έρχονται σε επαφή, να επικοινωνούν και να συνεργάζονται για το καλό των πολιτών τους. Συνήθως, προωθούν αρχεία με ηλεκτρονικά μέσα το ένα κράτος στο άλλο για λογαριασμό των πολιτών και των επιχειρήσεων. (Κεραμάρη, 2016; Κόκκαλης, 2015; Wikipedia, 2020). Σε (Government to Government-national (G2G-N) Στην κατηγορία αυτή έχουμε την εκπλήρωση συναλλαγών και υπηρεσιών μεταξύ διαφόρων κρατικών φορέων σε εθνικό επίπεδο. Σκοπός της κυβέρνησης είναι να υλοποιήσει ένα σύστημα πληροφοριών, στο οποίο θα έχουν πρόσβαση όλοι οι δημόσιοι φορείς για την καλύτερη και γρηγορότερη εξυπηρέτηση των πολιτών. Κέντρο αναφοράς της εν λόγω σχέσης είναι η αυτοματοποίηση δια-υπηρεσιακών συναλλαγών, η εύκολη και γρήγορη ηλεκτρονική διακίνηση πληροφοριών, η εύκολη και γρήγορη ηλεκτρονική διακίνηση εγγράφων (Τζίφα, 2017).

2.2.1.4. Εφαρμογές Κυβέρνησης προς Εργαζόμενους (G2E)

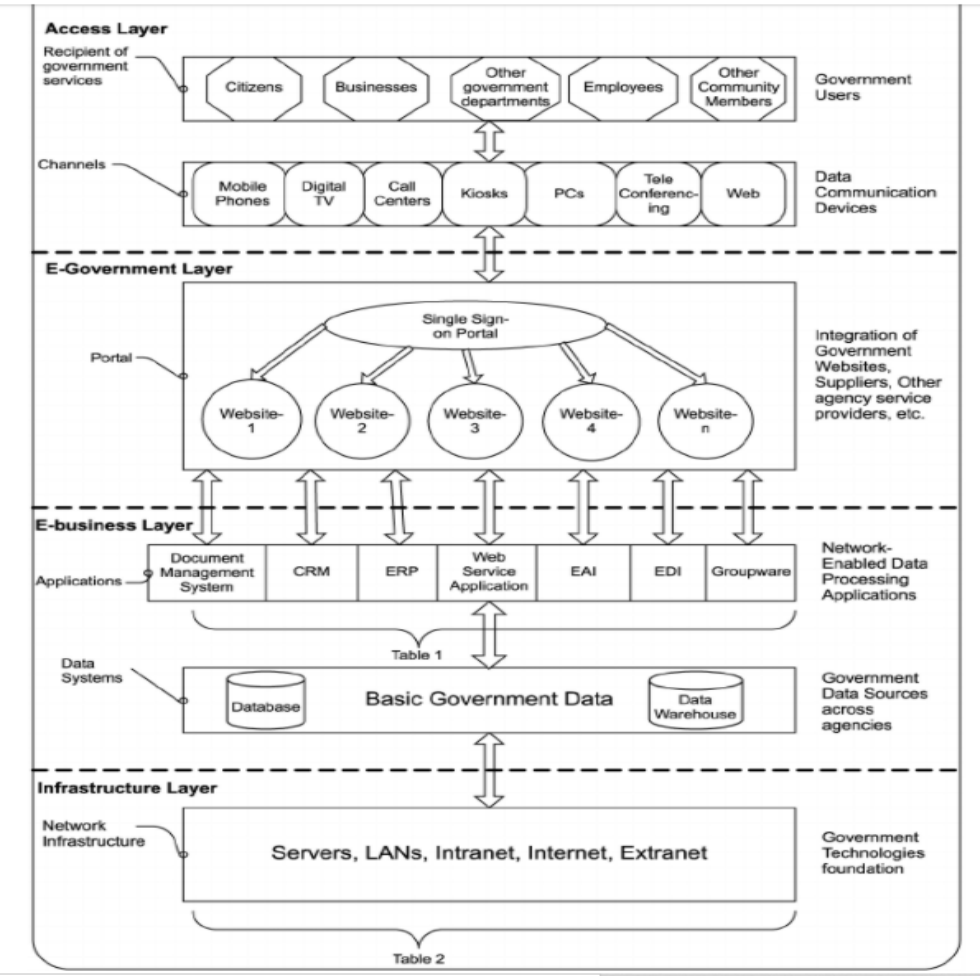
Η κυβέρνηση προς τους εργαζόμενους είναι ο λιγότερο διερευνημένος τομέας της ηλεκτρονικής διακυβέρνησης. Ορισμένοι ερευνητές το θεωρούν ως εσωτερικό μέρος του τομέα G2G και άλλοι το αντιμετωπίζουν ως ξεχωριστό τομέα της ηλεκτρονικής διακυβέρνησης. Το G2E αναφέρεται στη σχέση μεταξύ της κυβέρνησης και των υπαλλήλων της. Ο σκοπός αυτής της σχέσης είναι η εξυπηρέτηση των εργαζομένων και η προσφορά ορισμένων διαδικτυακών υπηρεσιών, όπως η ηλεκτρονική αίτηση για ετήσια άδεια, ο έλεγχος του υπολοίπου της άδειας και η εξέταση των αρχείων πληρωμής μισθών (e-payroll) (Seifert, 2003). Είναι ένας συνδυασμός πληροφοριών και υπηρεσιών που προσφέρονται από κυβερνητικά ιδρύματα στους υπαλλήλους τους για να αλληλεπιδρούν μεταξύ τους και με τη διοίκησή τους. Το G2E είναι ένας επιτυχημένος τρόπος για την παροχή ηλεκτρονικής μάθησης, τη συγκέντρωση των εργαζομένων και την ενθάρρυνση της ανταλλαγής γνώσεων μεταξύ τους. Δίνει στους υπαλλήλους τη δυνατότητα πρόσβασης σε πληροφορίες σχετικά με τις πολιτικές αποδοχών και παροχών, τις ευκαιρίες κατάρτισης και μάθησης (e-training) και τους επιτρέπει να διαχειρίζονται τα οφέλη τους στο διαδίκτυο με ένα εύκολο και γρήγορο μοντέλο επικοινωνίας. Το G2E περιλαμβάνει επίσης στρατηγικούς και τακτικούς μηχανισμούς για την ενθάρρυνση της υλοποίησης των κυβερνητικών στόχων και προγραμμάτων καθώς και τη διαχείριση ανθρώπινων πόρων, τον προϋπολογισμό και την αντιμετώπιση των πολιτών.

2.3. Αρχιτεκτονική Εφαρμογών Ηλεκτρονικής Διακυβέρνησης

Ένας οργανισμός του δημόσιου τομέα που σχεδιάζει να υιοθετήσει μια πρωτοβουλία ηλεκτρονικής διακυβέρνησης και να διαμορφώσει τις στρατηγικές πληροφορικής του, πρέπει να αξιολογήσει τα επιχειρηματικά του μοντέλα και να επιλέξει τις κατάλληλες τεχνολογικές λύσεις που ανταποκρίνονται στην πολιτική του. Αν και υπάρχουν σημαντικές διαφορές στη σύνθεση των οργανισμών, υπάρχουν πολλές τεχνολογίες και υποδομές συστημάτων που πολλοί οργανισμοί πρέπει να υιοθετήσουν, για να παρέχουν διευκολύνσεις στην ολοκλήρωση των συστημάτων τους με τρόπο που τους επιτρέπει να οικοδομήσουν μια πλατφόρμα για την ανταλλαγή των πόρων γνώσης τους (Sharma & Gupta, 2002). Ως εκ τούτου, ο οργανισμός πρέπει να έχει σαφή κατανόηση των πλαισίων αρχιτεκτονικής τόσο από το τεχνικό επίπεδο όσο και από το επίπεδο διαχείρισης πληροφοριών. Η αρχιτεκτονική της ηλεκτρονικής διακυβέρνησης καθορίζει τα πρότυπα, τα στοιχεία υποδομής, τις εφαρμογές, τις τεχνολογίες, το επιχειρηματικό μοντέλο και τις κατευθυντήριες γραμμές για το ηλεκτρονικό εμπόριο μεταξύ οργανισμών, διευκολύνοντας την αλληλεπίδραση της κυβέρνησης και προωθώντας την παραγωγικότητα της ομάδας. Δεδομένου ότι η ηλεκτρονική διακυβέρνηση είναι ένας σχετικά νέος ερευνητικός τομέας, η αρχιτεκτονική και η στρατηγική υιοθέτησής του δεν έχουν συζητηθεί ευρέως στη βιβλιογραφία. Ως εκ τούτου, οι συγγραφείς εξετάζουν και μελετούν αυτές τις έννοιες από άλλους σχετικούς τομείς όπως το ηλεκτρονικό επιχειρείν, οι ηλεκτρονικές υπηρεσίες και οι ηλεκτρονικές υπηρεσίες εμπορίου (Aubakirov & Nikulchev, 2016).

Το πλαίσιο είναι δομημένο σε τέσσερα επίπεδα, τα οποία παρουσιάζουν το ιεραρχικό επίπεδο εφαρμογής της ηλεκτρονικής διακυβέρνησης και απεικονίζουν τη λογική σύνδεση κάθε σχετικού επιπέδου που επιτρέπει αμφίδρομη μετάδοση δεδομένων και υπηρεσιών. Το ανώτερο

επίπεδο του πλαισίου αντιπροσωπεύει το επίπεδο πρόσβασης που δείχνει ποιος μπορεί να χρησιμοποιεί τις κρατικές υπηρεσίες και ποια είναι τα κανάλια πρόσβασης. Σε όλα αυτά τα κανάλια, η πύλη ηλεκτρονικής διακυβέρνησης θα πρέπει να ενσωματώνει όλες τις κυβερνητικές πληροφορίες και υπηρεσίες από διαφορετικά τμήματα και οργανισμούς, που αντιπροσωπεύουν το επίπεδο ηλεκτρονικής διακυβέρνησης. Σε σχέση με το επίπεδο e-government, το επίπεδο e-business αναδύεται για να χειριστεί και να ενσωματώσει τις πηγές δεδομένων της κυβέρνησης σε όλους τους κυβερνητικούς φορείς και να καταστήσει διαθέσιμες πληροφορίες και υπηρεσίες στην πύλη ηλεκτρονικής διακυβέρνησης σε πραγματικό χρόνο. Στο κατώτερο επίπεδο του πλαισίου, η υποδομή ΤΠΕ της ηλεκτρονικής διακυβέρνησης θα πρέπει να κατασκευαστεί έτσι ώστε να προσεγγίζει όλα τα μέρη της κυβέρνησης και, ως εκ τούτου, να υποστηρίζει τη λειτουργία της ηλεκτρονικής διακυβέρνησης και να παρέχει αποτελεσματικές και αξιόπιστες υπηρεσίες ηλεκτρονικής διακυβέρνησης. Συνολικά, το αρχιτεκτονικό πλαίσιο της ηλεκτρονικής διακυβέρνησης χωρίζεται σε τέσσερα επίπεδα: επίπεδο πρόσβασης, επίπεδο ηλεκτρονικής διακυβέρνησης, επίπεδο ηλεκτρονικού επιχειρείν και επίπεδο υποδομής, τα οποία περιγράφονται στη συνέχεια (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).



Γράφημα 4: *Αρχιτεκτονική Εφαρμογών Ηλεκτρονικής Διακυβέρνησης (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).*

- **Επίπεδο πρόσβασης (Access layer)**

Περιλαμβάνει τα κανάλια στα οποία οι κρατικοί χρήστες μπορούν να έχουν πρόσβαση στις διάφορες κρατικές υπηρεσίες. Τα κανάλια πρόσβασης είναι κρίσιμα στοιχεία της ηλεκτρονικής διακυβέρνησης. Για παράδειγμα, οι τοποθεσίες web είναι προσβάσιμες από υπολογιστές, κινητά τηλέφωνα (WAP), ψηφιακή τηλεόραση και κέντρα κλήσεων και επικοινωνίας. Αυτό το επίπεδο αποτελεί το απλούστερο επίπεδο αρχιτεκτονικής ηλεκτρονικής διακυβέρνησης, αφού ελέγχεται και διαχειρίζεται από κυβερνητικούς χρήστες. Ωστόσο, είναι σημαντικό οι οργανισμοί του δημόσιου τομέα να παρέχουν έναν κοινό τρόπο εύρεσης όλων των κυβερνητικών πληροφοριών και υπηρεσιών, να διατηρούν τον συντονισμό των καναλιών, να δημιουργούν μια κοινή εμφάνιση και αίσθηση σε διαφορετικά κανάλια και να συμμορφώνονται με τις κατευθυντήριες γραμμές των τεχνικών προτύπων (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).

- **Επίπεδο ηλεκτρονικής διακυβέρνησης (E-government layer)**

Αυτό το επίπεδο αφορά την ενσωμάτωση ψηφιακών δεδομένων διαφόρων οργανισμών σε μια διαδικτυακή πύλη κυβερνητικών υπηρεσιών με τη μορφή μιας πύλης one-stop. Οι κυβερνητικές δικτυακές πύλες αναδύονται ως βασική προτεραιότητα για τους οργανισμούς του δημόσιου τομέα, καθώς αναπτύσσουν την πρωτοβουλία ηλεκτρονικής διακυβέρνησης και δημιουργούν ηλεκτρονική αλληλεπίδραση μεταξύ κυβέρνησης και πολιτών (G2C), κυβέρνησης και επιχειρήσεων (G2B), κυβέρνησης και των υπαλλήλων της (G2E), και κυβέρνηση και κυβέρνηση (G2G). Σύμφωνα με τους Chan και Chung (2002), αυτό το επίπεδο επιτρέπει στο χρήστη να χρησιμοποιήσει το πρόγραμμα περιήγησης ιστού για να λάβει όλες τις εταιρικές πληροφορίες που χρειάζονται μέσα από ένα μόνο παράθυρο. Η πύλη διαθέτει μια διαδικτυακή εφαρμογή front-end που επιτρέπει τη σύνδεση διάσπαρτων πηγών πληροφοριών μεταξύ τους. Οι κυβερνήσεις μπορούν να έχουν πρόσβαση και να διαχειρίζονται όλα τα δεδομένα και τις πληροφορίες παρέχοντας στους χρήστες την ευκαιρία να προσαρμόσουν αυτό που χρειάζονται από πηγές πληροφοριών (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).

- **Επίπεδο ηλεκτρονικού επιχειρείν (E-business layer)**

Αυτό το επίπεδο επικεντρώνεται στη χρήση εφαρμογών και εργαλείων ΤΠΕ για την αξιοποίηση δικτύων εμπιστοσύνης, ανταλλαγής γνώσης και επεξεργασίας πληροφοριών που λαμβάνει χώρα τόσο εντός όσο και μεταξύ των οργανισμών. Πρακτικά, ενσωματώνει εφαρμογές επιπέδου goverment front-end, όπως διαδικτυακούς καταλόγους και διεπαφές συναλλαγών στην κυβερνητική πύλη με δραστηριότητες back-end όπως υπάρχουσες βάσεις δεδομένων και αποθήκες δεδομένων. Αυτό το επίπεδο περιλαμβάνει αρκετές εφαρμογές και εργαλεία που αναδύονται για να βοηθήσουν στον προσδιορισμό, την αξιολόγηση και την επίτευξη συνεπών και ολοκληρωμένων διαδικασιών και συστημάτων πληροφόρησης σε οργανισμούς του δημόσιου τομέα. Ωστόσο, είναι δύσκολο να προβλεφθεί ποιες εφαρμογές και συστήματα πληροφοριών θα

είναι τα πιο χρήσιμα και προσαρμόσιμα σε αυτό το επίπεδο (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).

- **Επίπεδο υποδομής (Infrastructure layer)**

Η ηλεκτρονική επικοινωνία εντός και μεταξύ των οργανισμών του δημόσιου τομέα είναι δαπανηρή και αναποτελεσματική χωρίς αποτελεσματική υποδομή και συμφωνημένα πρότυπα και πρωτόκολλα μεταξύ συστημάτων επικοινωνίας. Επομένως, αυτό το επίπεδο εστιάζει σε τεχνολογίες που θα πρέπει να υπάρχουν προτού οι υπηρεσίες ηλεκτρονικής διακυβέρνησης μπορούν να προσφερθούν αξιόπιστα και αποτελεσματικά στο κοινό. Οι δυνατότητες αυτών των τεχνολογιών είναι να υποστηρίζουν και να ενσωματώνουν τις λειτουργίες πληροφοριακών συστημάτων και εφαρμογών σε επίπεδο ηλεκτρονικού επιχειρείν σε όλους τους οργανισμούς προσφέροντας τα απαραίτητα πρότυπα και πρωτόκολλα μέσω προσεγγίσεων υποδομής δικτύου και επικοινωνίας (π.χ. intranet, extranet, LAN) (Aubakirov & Nikulchev, 2016; Baheer et al., 2018).

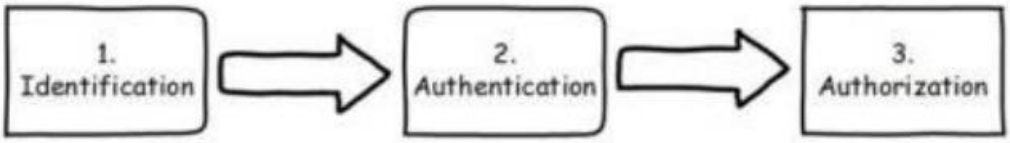
ΚΕΦΑΛΑΙΟ 3: ΗΛΕΚΤΡΟΝΙΚΗ ΤΑΥΤΟΠΟΙΗΣΗ

3.1. Ταυτοποίηση χρηστών

Η ηλεκτρονική ταυτοποίηση (electronic identity, e-ID) αποτελεί ηλεκτρονική λύση για την ταυτοποίηση πολιτών και επιχειρήσεων με σκοπό την υποστήριξη χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, υπηρεσιών ηλεκτρονικής τραπεζικής και άλλων ηλεκτρονικών υπηρεσιών από διάφορες κατηγορίες επιχειρήσεων. Η ηλεκτρονική ταυτότητα αποτελεί πρακτικά ένα τρόπο για να μπορούν να αποδείξουν ηλεκτρονικά τα άτομα πως είναι πράγματι τα πρόσωπα που ισχυρίζονται πως είναι και στη συνέχεια τα αντίστοιχα άτομα να μπορούν να αποκτούν πρόσβαση σε σχετικές ηλεκτρονικές υπηρεσίες. Η ταυτότητα επιτρέπει σε μια οντότητα (πολίτη, επιχειρήσεις, δημόσια διοίκηση) να διακρίνεται από κάθε άλλη σχετική οντότητα (European Commission, 2010).

Η ταυτοποίηση αφορά τον προσδιορισμό των πληροφοριών/δεδομένων που μπορούν να ταυτοποιήσουν μια οντότητα (πολίτες / επιχειρήσεις). Η ψηφιακή ταυτότητα περιλαμβάνει πεπερασμένο αριθμό χαρακτηριστικών μιας οντότητας. Ενδεικτικά, η ψηφιακή ταυτότητα μπορεί να περιλαμβάνει χαρακτηριστικά ενός ατόμου όπως: όνομα και επώνυμο, προσωπικό αναγνωριστικό αριθμό (PIN), αριθμό διαβατηρίου, βιομετρικά δεδομένα, όπως η ίριδα του ματιού ή δακτυλικό αποτύπωμα, καθώς επίσης και πληροφορίες σχετικά με τις δραστηριότητες ενός χρήστη στο διαδίκτυο, συμπεριλαμβανομένου των αναζητήσεων στο διαδίκτυο και συναλλαγές μέσω διαδικτύου.Η ταυτοποίηση των χρηστών στις υπάρχουσες ηλεκτρονικές υπηρεσίες πραγματοποιείται μέσω του μοναδικού αναγνωριστικού που έχει εκδώσει ο αντίστοιχος ιδιωτικός ή δημόσιος φορέας, για κάθε πολίτη ή επιχείρηση. Θα πρέπει να σημειωθεί ότι πρόκειται για μοναδικό αναγνωριστικό, το οποίο αφορά μόνο το συγκεκριμένο φορέα και όχι καθολικό μοναδικό αναγνωριστικό (Blue et al., 2018).

Η ηλεκτρονική ταυτοποίηση χρησιμοποιείται, για να πιστοποιηθεί η ταυτότητα ενός χρήστη και να αποκτήσει πρόσβαση σε συγκεκριμένο πλαίσιο υπηρεσιών. Αρχικά ο χρήστης παρουσιάζει μια ταυτοποίηση (identification), επαληθεύεται (authentication) η σχετική ταυτοποίηση και εάν η σχετική επαλήθευση είναι επιτυχής, επιτρέπεται η πρόσβαση (authorization) στο περιεχόμενο της υπηρεσίας που επιθυμεί ο χρήστης (στάδιο εξουσιοδότησης) (Söderström, 2016).



Γράφημα 5: *Στάδια ηλεκτρονικής ταυτοποίησης (Söderström, 2016)*

Σύμφωνα με την περ. α΄ της παρ. 1 του άρθρου 24 Νόμος 4727/2020 η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης είναι αποκλειστικά υπεύθυνη για την ταυτοποίηση και την αυθεντικοποίηση των φυσικών ή νομικών προσώπων ή νομικών οντοτήτων για σκοπούς παροχής και χρήσης των ψηφιακών δημόσιων υπηρεσιών. Η ταυτοποίηση φυσικών προσώπων είναι απαραίτητη προϋπόθεση για την έκδοση διαπιστευτηρίων, με σκοπό την

αυθεντικοποίησή τους. Η ταυτοποίηση διενεργείται με έναν από τους ακόλουθους τρόπους: (Άρθρο 25 - Νόμος 4727/2020)

α) Μέσω της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, σύμφωνα με τα οριζόμενα στην υπ' αρ. 1178/2010 απόφαση του Υπουργού Οικονομικών «Εγγραφή νέων χρηστών στις ηλεκτρονικές υπηρεσίες TaxisNet» (Β΄ 1916).

β) Με φυσική παρουσία του φυσικού προσώπου στα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ).

γ) Με τη χρήση εξ αποστάσεως ταυτοποίησης που παρέχει διασφάλιση ισοδύναμη με τη φυσική παρουσία. Η ταυτοποίηση αυτή μπορεί να διενεργείται μέσω του Εθνικού Μητρώου Επικοινωνίας Πολιτών του άρθρου 17 του ν. 4704/2020 (Α΄ 133).

Τα πιο σημαντικά θέματα σχετικά με την ηλεκτρονική ταυτοποίηση, είναι η αυξημένη ανάγκη ταυτοποίησης των συναλλασσόμενων και η επιθυμία των χρηστών να διατηρήσουν τις συνήθειες του «πραγματικού» κόσμου. Όσον αφορά την Ηλεκτρονική Διακυβέρνηση, η διαχείριση της ψηφιακής ταυτότητας έχει ακόμη μεγαλύτερη αξία δεδομένου ότι είναι βασικός παράγοντας και προϋπόθεση προκειμένου να διασφαλιστεί η αποτελεσματική και πάνω απ΄ όλα ασφαλή χρήση ηλεκτρονικών και εμπορικών υπηρεσιών. Οι βασικές ανησυχίες των πολιτών αφορούν κυρίως στα δεδομένα που το κάθε κράτος επιλέγει να απαρτίζουν την πληροφοριακή τους ταυτότητα (Informational Identity). Οι ανησυχίες που εγείρει η διαχείριση ταυτότητας στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, σχετίζονται κυρίως με τους φορείς ταυτοποίησης και αυθεντικοποίησης, οι οποίοι συγκεντρώνουν ευαίσθητα και μοναδικά στοιχεία του ατόμου, για τα οποία, φορέας διαχείρισης ήταν το ίδιο το άτομο. Σήμερα, όλα τα Κράτη-Μέλη της ΕΕ, έχουν υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στο πλαίσιο του εκσυγχρονισμού των ηλεκτρονικά παρεχόμενων υπηρεσιών τους.

3.2. Αυθεντικοποίηση Χρηστών

Ως αυθεντικοποίηση ορίζεται η δυνατότητα παροχής αδιαμφισβήτητων στοιχείων για την επαλήθευση της ταυτότητας μιας οντότητας. Είναι η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης (Blue et al., 2018).

Για την αυθεντικοποίηση των χρηστών ο μόνος τρόπος αυθεντικοποίησης σε όλες τις υπάρχουσες ηλεκτρονικές υπηρεσίες που προσφέρονται από τους δημόσιους φορείς είναι μέσω του συνθηματικού που εκδίδεται κατά τη διάρκεια της εγγραφής του χρήστη στην υπηρεσία και αντιστοιχίζεται με το όνομα του χρήστη. Αντιθέτως, στην περίπτωση κάποιων υπηρεσιών ηλεκτρονικής τραπεζικής, ο χρήστης δεν αυθεντικοποιείται μόνο με το συνθηματικό του, αλλά επιπλέον απαιτείται η αξιοποίηση συνθηματικών μιας χρήσης. Τα στοιχεία αυθεντικοποίησης, στις κρίσιμες τουλάχιστον υπηρεσίες στις οποίες γενικότερα συμπεριλαμβάνονται και οι υπηρεσίες ηλεκτρονικής τραπεζικής, προστατεύονται με το πρωτόκολλο Secure Socket Layer (SSL) (Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Ψηφιακής Αυθεντικοποίησης, 2012).

Σύμφωνα με την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, οι υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι απαραίτητο να προσδιορίσουν το επίπεδο αυθεντικοποίησης μιας υπηρεσίας, πριν αποφασιστεί ο μηχανισμός αυθεντικοποίησης σε αυτή. Λαμβάνοντας υπόψη τους υπάρχοντες μηχανισμούς αυθεντικοποίησης και τα αντίστοιχα διακριτικά αυθεντικοποίησης, προκύπτουν τα ακόλουθα επίπεδα αυθεντικοποίησης (Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Ψηφιακής Αυθεντικοποίησης, 2012):

•Επίπεδο Αυθεντικοποίησης 0 (ΕΑ0): Σε αυτό το επίπεδο δεν απαιτείται αυθεντικοποίηση του χρήστη καθώς οποιαδήποτε οντότητα είναι δυνατόν να έχει πρόσβαση στις πληροφορίες που θεωρούνται δημόσιες(π.χ. πληροφοριακό υλικό). Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον η ακεραιότητα του παρεχόμενου πληροφοριακού υλικού, η αυθεντικότητα υπηρεσίας, δεν απαιτείται μηχανισμός αυθεντικοποίησης.

•Επίπεδο Αυθεντικοποίησης 1 (ΕΑ1): Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται μικρή έως μέτρια βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς αφορούν υπηρεσίες στις οποίες δικαίωμα πρόσβασης έχουν μόνον εξουσιοδοτημένες οντότητες. Τέτοιου είδους υπηρεσίες θεωρούνται αυτές που υποστηρίζουν τη δυνατότητα παροχής αιτήσεων στους χρήστες για περαιτέρω (off-line) επεξεργασία και την πραγματοποίηση της συναλλαγής με το φορέα σε φυσικό επίπεδο. Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, τα ακόλουθα:

- Εμπιστευτικότητα των δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (τήρηση κανόνων προστασίας προσωπικών δεδομένων) ο διαπιστευτηρίων του χρήστη

- Ακεραιότητα των δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη ο διαπιστευτηρίων του χρήστη ο δεδομένων που λαμβάνονται από την ηλεκτρονική υπηρεσία

- Οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το συγκεκριμένο επίπεδο συμπεριλαμβάνουν: συνθηματικά, συνθηματικά μιας χρήσης ή συνδυασμό αυτών.

•Επίπεδο Αυθεντικοποίησης 2 (ΕΑ2): Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς είναι εξαιρετικά κρίσιμο να εξασφαλιστεί ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες. Εδώ εντάσσονται οι ηλεκτρονικές υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή υποστηρίζουν τη διενέργεια οικονομικών συναλλαγών. Στο ΕΑ2 θα πρέπει να διασφαλίζονται κατ' ελάχιστον τα ακόλουθα:

- Εμπιστευτικότητα των ο δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (ιδιωτικότητα) ο διαπιστευτηρίων του χρήστη ο δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία ο δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία

- Ακεραιότητα των ο δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη ο διαπιστευτηρίων του χρήστη ο δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία ο δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία

- Μη αποποίηση αποστολής δεδομένων και λήψης δεδομένων

- Υπηρεσίες εποπτείας (auditing)
- Χρονοσήμανση των ενεργειών
- Ο μηχανισμός αυθεντικοποίησης που προτείνεται για το συγκεκριμένο επίπεδο αξιοποιεί ψηφιακά πιστοποιητικά (digital certificates) που θα εκδίδονται από την κατάλληλη Υποδομή Δημόσιου Κλειδιού (PKI) και την Αρχή Χρονοσήμανσης (Time Stamping Authority - TSA). Επιπρόσθετα προτείνεται η αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης.

Σύμφωνα με τη βιβλιογραφία (Blue et al., 2018) τα πιο σημαντικά ζητήματα σχετικά με την ηλεκτρονική ταυτοποίηση, είναι η ταυτόχρονη ανάγκη για ταυτοποίηση των συναλλασσόμενων σε συνθήκες του «πραγματικού» κόσμου. Η διαχείριση της ψηφιακής ταυτότητας στην Ηλεκτρονική Διακυβέρνηση έχει ακόμη μεγαλύτερη αξία, δεδομένου ότι χρησιμοποιεί προσωπικές πληροφορίες των πολιτών, οι οποίες απαρτίζουν την πληροφοριακή ταυτότητα του καθενός (Informational Identity), κάτι που προκαλεί ανησυχία στους πολίτες για το ποια δεδομένα τους επιλέγονται από το κράτος προς ταυτοποίησης τους, διασφαλίζοντας με αυτό τον τρόπο την αποτελεσματική και ασφαλή χρήση ηλεκτρονικών υπηρεσιών. Σήμερα, όλα τα κράτη μέλη της ΕΕ έχουν υιοθετήσει συστήματα διαχείρισης ηλεκτρονικής ταυτότητας ως μέρος του εκσυγχρονισμού των ηλεκτρονικών τους υπηρεσιών. (Melin et al., 2016).

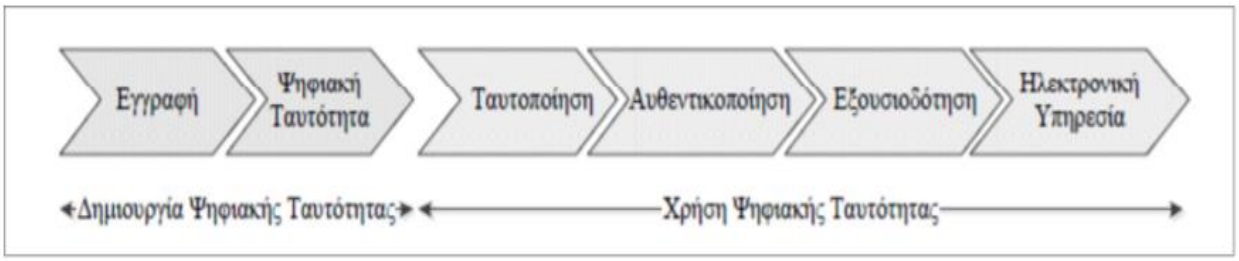
3.3. Μέθοδοι ταυτοποίησης σε ηλεκτρονικές υπηρεσίες

3.3.1. Ψηφιακή Ταυτότητα

Η ψηφιακή ταυτότητα είναι ένας ηλεκτρονικός τρόπος αναγνώρισης και εξακρίβωσης της ταυτότητας κάποιου. Αποτελείται από ένα πιστοποιητικό που περιέχει ένα «δημόσιο κλειδί» που είναι ορατό και ένα «ιδιωτικό κλειδί» που φυλάσσεται μυστικό. Το ιδιωτικό κλειδί υπογράφει ένα ηλεκτρονικό έγγραφο με υπογραφή, η οποία είναι δυνατό να επαληθευτεί από άλλους χρησιμοποιώντας μόνο το δημόσιο κλειδί του υπογράφοντα. Παρομοίως, το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση εγγράφων που κρυπτογραφήθηκαν από άλλους χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντα. Οι αρχές έκδοσης πιστοποιητικών, προκειμένου να διασφαλίσουν την εγκυρότητα μιας ψηφιακής υπογραφής, παρέχουν ψηφιακές ταυτότητες προς άτομα, η ταυτότητα των οποίων έχει επαληθευτεί. Η ταυτότητα κάθε ατόμου αποτελείται από πολλά χαρακτηριστικά τα οποία είναι ικανά ,είτε μόνα τους, είτε σε συνδυασμό μεταξύ τους, να το αναγνωρίσουν μοναδικά. Υπό τη έννοια του όρου στα Π.Σ., χαρακτηρίζεται ως "ηλεκτρονικά αναγνωρίσιμη αντιπροσώπευση μιας ανθρώπινης ταυτότητας" (Camp, 2004). Σκοπός της είναι να συνδέσει μία συγκεκριμένη συναλλαγή ή ένα σύνολο δεδομένων από ένα Π.Σ. με ένα αναγνωρίσιμο άτομο, που το εξουσιοδοτεί να χρησιμοποιήσει υπολογιστικούς πόρους ή ηλεκτρονικές υπηρεσίες.

Για να δοθεί πρόσβαση σε κάποιον χρήστη για μια συγκεκριμένη ηλεκτρονική υπηρεσία, θα πρέπει να προηγηθούν κάποια στάδια επεξεργασίας. Το πρώτο περιλαμβάνει τη δημιουργία της

ψηφιακής ταυτότητας του χρήστη, προηγείται η διαδικασία της εγγραφής (Registration), κατά την οποία ο εκδότης της ψηφιακής ταυτότητας ελέγχει, αν αυτή εκδίδεται για το σωστό πρόσωπο, και έπειτα δημιουργείται η ψηφιακή ταυτότητα που μπορεί να αποτελείται από έναν συνδυασμό ονόματος χρήστη (Username) και συνθηματικού (Password), ένα ψηφιακό πιστοποιητικό (Digital Certificate) ή ένα ανώνυμο διακριτικό διαπιστευτήριο (Anonymous). Ακολουθεί η ταυτοποίηση (Identification), όπου ο χρήστης ισχυρίζεται την ύπαρξη συγκεκριμένης ψηφιακής ταυτότητας, παρέχοντας π.χ. ένα όνομα χρήστη και πραγαμτοποιείται αυθεντικοποίησή (Authentication), δηλαδή ο χρήστης επαληθεύει την ύπαρξη της προαναφερθείσας ψηφιακής ταυτότητας παρέχοντας π.χ. ένα συνθηματικό και ο συνδυασμός τους επαληθεύεται από τον πάροχο της ηλεκτρονικής υπηρεσίας . τέλος, δίνεται η εξουσιοδότηση (Authorization), όπου ο πάροχος προσδιορίζει τα δικαιώματα του χρήστη για τη συγκεκριμένη ηλεκτρονική υπηρεσία. Στην παρακάτω εικόνα δίνονται τα στάδια από την δημιουργία έως τη χρήση της ηλεκτρονικής υπηρεσίας (Δρογκάρης, 2013).



Γράφημα 6: *Στάδια Δημιουργίας Ψηφιακής Ταυτόυητας (Δρογκάρης, 2013)*

3.3.2. Διακριτικά/ Συνθηματικά

Τα διακριτικά αυθεντικοποίησης χρησιμοποιούνται για τον έλεγχο της ορθότητας της ηλεκτρονικής ταυτότητας του χρήστη του συστήματος. Σε ένα τυπικό σύστημα ασφάλειας η αυθεντικότητα των χρηστών μπορεί να ελεγχθεί με τρεις τρόπους (Office of the Privacy Commissioner of Canada, 2016):

• Συνθηματικά/ Something You Know – SYK: Τα συνθηματικά αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του κάνοντας χρήση ενός μυστικού που είναι γνωστό μόνο σε αυτόν. Συνήθως τα συνθηματικά δεν αποθηκεύονται καθώς επιλέγονται με τρόπο ώστε να είναι ευκολομνημόνευτα.

• Φυσικά Χαρακτηριστικά/ Something You Are – SYA: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (συστήματα βιομετρικής τεχνολογίας, πχ.εφαρμογές δακτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού). Παρέχουν μεγαλύτερη ασφάλεια από τα συνθηματικά SYH και SYK, αλλά είναι δυσκολότερα στην κατασκευή αξιόπιστων αναγνωριστικών συσκευών και δεν είναι αλάνθαστα.

• Διακριτικά Χαλαρής Αποθήκευσης (soft tokens)/ Something you Have – SYH: Τα διακριτικά χαλαρής αποθήκευσης αναφέρονται σε μυστικά κλειδιά, τα οποία αποθηκεύονται σε κάποιο μέσο αποθήκευσης όπως σκληρός δίσκος, CD, USB flash, smart card κ.λπ. Τα κλειδιά είναι αποθηκευμένα σε κρυπτογραφημένη μορφή, ενώ η προσπέλασή τους είναι δυνατή μόνο με τη χρήση του κατάλληλου συνθηματικού. Δεν αντιγράφονται εύκολα, καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα, με υψηλό κόστος. Μπορούν να χαθούν ή να κλαπούν.

Ο συνδυασμός τρόπων ταυτοποίησης αποτελεί την ασφαλέστερη μέθοδο. Ωστόσο, εκτός από τις περιπτώσεις όπου απαιτείται ένα υψηλότατο επίπεδο ασφάλειας (π.χ. στρατιωτικές εγκαταστάσεις), σπάνια υιοθετούνται συστήματα που ενσωματώνουν και τους τύπους SYK, SYH, SYA, και αυτό λόγω κόστους και μειωμένης λειτουργικότητας. Η πλέον δημοφιλής τεχνική είναι η ταυτοποίηση SYK (Όνομα χρήστη - user name και κωδικός - password).

3.3.3. Βιομετρικά

Η διαδικασία ταυτοποίησης με εφαρμογή συστημάτων βιομετρικής τεχνολογίας, βασίζεται σε φυσικά χαρακτηριστικά του ανθρώπινου σώματος όπως δακτυλικά αποτυπώματα, ίριδα ματιού, χροιά φωνής, γεωμετρία χεριού, DNA, ως αποδεικτικά στοιχεία για την αναγνωρισιμότητα του λογικού υποκειμένου από ένα ΠΣ. Χαρακτηριστικά των βιομετρικών συστημάτων είναι το μεγάλο ποσοστό ακρίβειας και αξιοπιστίας στην ορθή αναγνώριση ενός εξουσιοδοτημένου ατόμου από ένα μη εξουσιοδοτημένο και η ταχύτητα απόκρισης του συστήματος. Όμως οι υψηλές απαιτήσεις συντήρησης και οι χρήση «μεγάλων» βάσεων δεδομένων, σε συνδυασμό με την αντίσταση των χρηστών (η χρήση ακτινοβολίας βλάπτει την υγεία, η κοινωνική αντίληψη ότι η λήψη δακτυλικών αποτυπωμάτων συνδυάζεται με εγκληματική δραστηριότητα), καθιστούν δύσκολη την εφαρμογή των συστημάτων σε καθημερινές υπηρεσίες. Ωστόσο, η χρήση βιομετρικών στοιχείων είναι μια πεποίθηση που συμμερίζονται πολλοί οργανισμοί σχετικά με το ότι έτσι το πρόβλημα της παραβίασης μπορεί να μετριαστεί. Με δυνατότητες επεξεργασίας και αποθήκευσης, οι βιομετρικοί αναγνώστες μπορούν να λειτουργήσουν ως ασφαλή πορτοφόλια πληροφοριών. Μπορούν να ενισχυθούν έναντι της καταστροφής κακόβουλου λογισμικού και να προστατεύονται από ηλεκτρονικό ψάρεμα και τυχαία αποκάλυψη πληροφοριών (Jakobsson & Taveau, 2014).

3.3.4. Ηλεκτρονική Υπογραφή

Διεθνείς φορείς, οργανισμοί και χώρες έχουν υιοθετήσει διαφορετικούς ορισμούς για τις ηλεκτρονικές υπογραφές. Στην ουσία, οι ηλεκτρονικές υπογραφές είναι προσωπικές ταυτότητες που βασίζονται σε υπολογιστή. Μπορούν να λάβουν μια απλή μορφή, όπως υπογραφές bitmap που είναι σαρωμένες εικόνες χειρόγραφων υπογραφών σε ένα έγγραφο, ή προηγμένη, όπως οι

βιομετρικές υπογραφές (π.χ. σάρωση ίριδας). Η πιο προηγμένη και ευρέως χρησιμοποιούμενη μορφή ηλεκτρονικής υπογραφής είναι η ψηφιακή υπογραφή, η οποία βασίζεται στην κρυπτογραφική μέθοδο δημόσιου κλειδιού (Lentner & Parycek, 2016).

Το βασικό χαρακτηριστικό αυτής της τεχνολογίας ασφαλούς κρυπτογράφησης, είναι ότι δύο διαφορετικά αλλά μαθηματικά συνδεδεμένα κλειδιά, το ιδιωτικό και το δημόσιο κλειδί (το λεγόμενο «ζεύγος κλειδιών»), χρησιμοποιούνται για τη δημιουργία μιας ψηφιακής υπογραφής και την κωδικοποίηση των δεδομένων και την επαλήθευση της υπογραφής και της αποκωδικοποίησης των δεδομένων. Στην συγκεκριμένη περίπτωση χρησιμοποιείται η ασύμμετρη κρυπτογραφία, όπου ο κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση –το δημόσιο κλειδί και το ιδιωτικό κλειδί. Το δημόσιο κλειδί γνωστοποιείται στους τρίτους, ενώ το ιδιωτικό κλειδί το γνωρίζει μόνο ο κατέχων. Έτσι ο,τιδήποτε κρυπτογραφείται με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί χρησιμοποιώντας μόνο το ιδιωτικό κλειδί. Πρακτικά, ο αποστολέας ενός ηλεκτρονικού εγγράφου μπορεί να το υπογράψει χρησιμοποιώντας το ιδιωτικό του κλειδί, το οποίο πρέπει να κρατηθεί μυστικό. Έτσι, η υπογραφή μπορεί να επαληθευτεί μόνο με το δημόσιο κλειδί του αποστολέα, το οποίο είναι διαθέσιμο στο κοινό. Μια διαδικασία που συνδέεται στενά με την κρυπτογράφηση του δημόσιου κλειδιού και εφαρμόζεται τόσο στη δημιουργία όσο και στην επαλήθευση μιας ψηφιακής υπογραφής, είναι η συνάρτηση κατακερματισμού (hash function), η οποία όταν εφαρμόζεται σε ένα συγκεκριμένο μήνυμα δημιουργεί έναν μοναδικό αριθμό με τη μορφή τιμής κατακερματισμού (σύνοψη μηνυμάτων). Έτσι, η διαδικασία δημιουργίας, χρήσης και επαλήθευσης μιας ψηφιακής υπογραφής παρέχει σημαντικές λειτουργίες για νομικούς σκοπούς (Lentner & Parycek , 2016). Η κρυπτογράφηση δημοσίου κλειδιού (public key encryption) θεωρείται η καταλληλότερη για τις δημόσιες συναλλαγές καθώς εξασφαλίζει την εμπιστευτικότητατου μηνύματος, παρέχει πιο ευέλικτα μέσα ελέγχου της ταυτότητας των χρηστών(authentication) και υποστηρίζει τις ψηφιακές υπογραφές (ακεραιότητα μηνύματος). Σύμφωνα με μελέτη του ΙΟΒΕ (“Υιοθέτηση των ΤΠΕ και ψηφιακή ανάπτυξη στην Ελλάδα”, 12/2014), η υιοθέτηση της λύσης της ψηφιακής υπογραφής στην ελληνική ΔΔ μπορεί να οδηγήσει στην εξοικονόμηση έως 380 εκ ευρώ ετησίως.

Τα πιο σημαντικά χαρακτηριστικά της Ψηφιακής Υπογραφής είναι τα παρακάτω (Lentner & Parycek , 2016):

- Αυθεντικοποίηση της πηγής του μηνύματος: Προστατεύει τον αποστολέα ακόμα και σε περίπτωση που ο παραλήπτης τροποποιήσει το αρχικό μήνυμα του αποστολέα

- Μη απάρνηση πηγής: Σε περίπτωση που ο αποστολέας αρνηθεί ότι έστειλε το μήνυμα, ο παραλήπτης του μηνύματος θα πρέπει να είναι σε θέση να αποδείξει ότι το μήνυμα στάλθηκε από τον αποστολέα

- Μη απάρνηση προορισμού: Σε περίπτωση που ο παραλήπτης αρνηθεί ότι παρέλαβε το μήνυμα, θα πρέπει να υπάρχει δυνατότητα απόδειξης ότι το μήνυμα παραλήφθηκε από τον παραλήπτη

- Συνδέεται μονοσήμαντα με τον υπογράφοντα

- Είναι ικανή να προσδιορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
- Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό έλεγχο
- Συνδέεται με τα δεδομένα, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση

3.3.5 Ψηφιακό Πιστοποιητικό

Σε πολλές περιπτώσεις ένας οργανισμός ή μια υπηρεσία δεν αρκείται στην υπογραφή ενός πολίτη, αλλά απαιτεί αυτή η υπογραφή να έχει πιστοποιηθεί για το γνήσιό της από μια έμπιστη αρχή, όπως ένα αστυνομικό τμήμα. Με τον ίδιο τρόπο, στο χώρο των ΤΠΕ ένα δημόσιο κλειδί μπορεί να πιστοποιηθεί από μια τρίτη έμπιστη οντότητα. Τα ηλεκτρονικά πιστοποιητικά είναι αυτή την περίοδο το ωριμότερο εργαλείο ταυτοποίησης των χρηστών ενός συστήματος ηλεκτρονικών συναλλαγών μέσω διαδικτύου (Reddy, 2015). Εάν θα θελήσουμε να ορίσουμε το ψηφιακό πιστοποιητικό, μπορούμε να πούμε ότι είναι ένα «επίσημο έγγραφο», συνήθως σε ηλεκτρονική μορφή, το οποίο συνδέει τα στοιχεία του κατόχου (πληροφορίες ταυτότητας προς όνομα, επάγγελμα) με τα στοιχεία της ηλεκτρονικής του υπογραφής (περιγραφές αδειών και το δημόσιο κλειδί του). Πιστοποιεί ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε συγκεκριμένο χρήστη. Τα ψηφιακά πιστοποιητικά επιτρέπουν, δηλαδή, την επαλήθευση του ισχυρισμού ότι μία συγκεκριμένη δημόσια κλείδα ανήκει σε μια συγκεκριμένη οντότητα, αποτρέποντας κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικης κλείδας. Έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στην Κρυπτογραφία Δημόσιου Κλειδιού. Μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της αποκάλυψης της ταυτότητας του χρήστη, ενσωματώνοντας ψευδώνυμα αντί της πραγματικής ταυτότητάς του.

Ένα πιστοποιητικό περιέχει τις ακόλουθες πληροφορίες:

Τύπος δεδομένων:

- Όνομα της οντότητας προκατόχου
- Δημόσιο κλειδί της οντότητας
- Επιπρόσθετες πληροφορίες: Περίοδος ισχύος του δημοσίου κλειδιού (ημερομηνία έναρξης και λήξης) Σειριακός αριθμός (χαρακτηρίζει μοναδικά το πιστοποιητικό) Πληροφορίες για την οντότητα (π.χ.,διεύθυνση)
- Το όνομα του εκδοτικού οργανισμού CA

Τμήμα υπογραφής: Η ψηφιακή υπογραφή του εκδοτικού οργανισμού

Η τυποποιημένη μορφή ενός πιστοποιητικού ακολουθεί το πρωτόκολλο X.509 v3. , το οποίο είναι ένα διεθνές πρότυπο που καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημοσίου Κλειδιού (Public Key Inπρoςstructure, PKI). Προδιαγράφει τις μορφές διάθεσης της σχετικής

πληροφορίας (κλειδιά, λίστες ανάκλησης), καθώς και προς αλγορίθμους επαλήθευσης του κύρους ενός πιστοποιητικού. (Wikipedia, 2019)

3.3.5.1. Αρχή Πιστοποίησης

Τα πιστοποιητικά εκδίδονται από τις Αρχές Έκδοσης Πιστοποιητικών (Certification Authorities: CA), που μπορεί να είναι οποιοσδήποτε άξιος εμπιστοσύνης οργανισμός που να εγγυηθεί για την ταυτότητα αυτών για τους οποίους εκδίδει πιστοποιητικά. Η CA πρέπει να κατέχει ένα ζεύγος ιδιωτικής/δημόσια κλείδας. Με το ιδιωτικό κλειδί υπογράφει ψηφιακά τα πιστοποιητικά που εκδίδει, ενώ την εγκυρότητα του δημοσίου κελιδιού πρέπει να την επικυρώνει εκδοτικός οργανισμός σε υψηλότερη θέση στην ιεραρχία των CAs. Η ιεραρχική κατάταξη έχει στην κορυφή της τον οργανισμό Internet Policy Registration Authority (IRPA) και αμέσως μετά ακολουθούν ο ι Policy Certification Authorities (PCAs) που δημοσιοποιούν πολιτικές ασφάλισης και έκδοσης πιστοποιητικών. Σ ‘αυτήν την ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν την δημόσια κλείδα και ταυτότητα του χαμηλότερου επιπέδου. Έτσι, πολλές φορές το πιστοποιητικό για έναν χρήστη μπορεί να συνοδεύεται από μία αλυσίδα πιστοποιητικών (certificates chain) που φθάνουν ως την κορυφή της ιεραρχίας.

Σκοπός είναι: α) η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει, β) η εγγύηση γνησιότητας των ψηφιακών δεδομένων και γ) η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί τη συμβολή του στην εν λόγω συναλλαγή.

Οι βασικότερες υπηρεσίες που προσφέρονται υποχρεωτικά από έναν Πάροχο Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι:

• Η Υπηρεσία της Χρονοσήμανσης: Ένας Πάροχος Υπηρεσιών Πιστοποίησης, εκτός από την βασική λειτουργία της χορήγησης της ψηφιακής υπογραφής, μπορεί να προσφέρει και την υπηρεσία της χρονοσήμανσης, με την οποία τίθεται μια ηλεκτρονική σφραγίδα στο έγγραφο που αποστέλλει ένας χρήστης και η οποία δεν μπορεί να τροποποιηθεί ούτε να αμφισβητηθεί και καθορίζει τον ακριβή χρόνο της αποστολής του μηνύματος. Ένα πολύ χαρακτηριστικό παράδειγμα όπου μπορεί να βρει εφαρμογή η υπηρεσία της χρονοσήμανσης είναι η ηλεκτρονική υποβολή δηλώσεων ή αιτήσεων προς μια δημόσια υπηρεσία (π.χ. υποβολή καταστάσεων ΦΠΑ), όπου δεν γίνονται δεκτές αιτήσεις μετά από μια καθορισμένη προθεσμία. Με την υπηρεσία της χρονοσήμανσης μπορεί να αποδειχθεί η ακριβής ημερομηνία και ώρα υποβολής της αίτησης-δήλωσης, όταν βέβαια προκύψει θέμα εκπρόθεσμης υποβολής.

• Η Υπηρεσία της Αποθήκευσης Μηνυμάτων: Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να λειτουργήσει και ως ηλεκτρονικός συμβολαιογράφος, στον οποίο μπορεί κάποιος τρίτος να καταθέσει κείμενα (αντίγραφα) που έχουν αξία, όπως ένα συμβόλαιο ή μια φορολογική δήλωση, έτσι ώστε σ’ οποιονδήποτε φορολογικό ή άλλον έλεγχο να μπορεί να πιστοποιηθεί ποιο ήταν το κείμενο που πράγματι εστάλη αρχικά. Το κείμενο θα πρέπει να είναι ψηφιακά υπογεγραμμένο ή

και κρυπτογραφημένο και σε επικείμενο έλεγχο θα πρέπει να προσκομισθεί το ιδιωτικό κλειδί για την αποκρυπτογράφησή του. Το κείμενο θα μπορεί να είναι και χρονοσημασμένο.

3.3.5.2. Υποδομή Δημοσίου Κλειδιού

Στο πλαίσιο πιστοποίησης των πολιτών και των επιχειρήσεων κατά τη διεξαγωγή ηλεκτρονικών συναλλαγών με το δημόσιο τομέα, πρέπει να υπάρχει ο κατάλληλος μηχανισμός επαλήθευσης των ταυτοτήτων των προσώπων του δημόσιου κλειδιού. Ο μηχανισμός αυτός ονομάζεται «Υποδομή Δημοσίου Κλειδιού», όπου εκδίδει, διαθέτει και διαχειρίζεται τα πιστοποιητικά του δημόσιου κλειδιού. Σύμφωνα με το λεξιλόγιο όρων ασφάλειας ΤΠΕ του NIST το PKI ορίζεται ως ένα ολοκληρωμένο σύστημα από πολιτικές, διαδικασίες και τεχνολογίες κρυπτογραφίας, το οποίο παρέχει στους χρήστες του Διαδικτύου τη δυνατότητα να ανταλάσσουν πληροφορίες με μυστικότητα και ασφάλεια. Επιβεβαιώνει με ασφαλή τρόπο τη σχέση ενός δημόσιου κλειδιού με το όνομα του ιδιοκτήτη/αποστολέα του. Από τεχνολογικής πλευράς, ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημοσίου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό πλαίσιο, ενώ προσφέρει εργαλεία για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.Ο οργανισμός που εκδίδει πιστοποιητικά που πιστοποιούν την ταυτότητα του προσώπου και το δημόσιο κλειδί του ονομάζεται Πάροχος Υπηρεσιών (ΠΥΠ) ή Αρχή Πιστοποίησης (ΑΠ). Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό. Ο ΠΥΠ δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου. Στην Ελλάδα, οι ΠΥΠ και οι βεβαιώσεις για την ασφάλεια της ηλεκτρονικής υπογραφής ελέγχονται από την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (Ε.Ε.Τ.Τ.)(Ελληνικό Παρατηρητήριο για την Κοινωνίας της Πληροφορίας 2007).Η ελληνική νομοθεσία προβλέπει με το Παράρτημα Ι του Προεδρικού Διατάγματος 150/2001 ότι τα αναγνωρισμένα πιστοποιητικά πρέπει να περιλαμβάνουν:

•ένδειξη ότι το πιστοποιητικό εκδίδεται ως ένα αναγνωρισμένα πιστοποιητικό

•τα στοιχεία αναγνώρισης του ΠΥΠ και το κράτος, στο οποίο είναι εγκατεστημένος

•το όνομα του υπογράφοντος

•πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσονείναι σημαντικό σε σχέση με το σκοπό για τον οποίο προορίζεται το πιστοποιητικό

•δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος

•ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού

•τον κωδικό ταυτοποίησης του πιστοποιητικού

•την προηγμένη ψηφιακή υπογραφή του ΠΥΠ που το εκδίδει

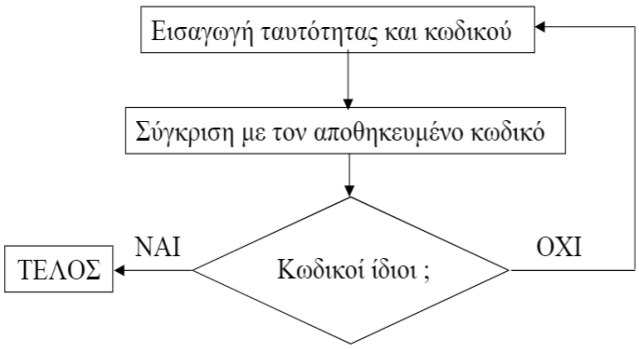
•τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού

3.3.6. Έξυπνες Κάρτες

Οι πρόσφατες εξελίξεις στις έξυπνες τεχνολογίες έχουν οδηγήσει στην ανάπτυξη έξυπνης κάρτας/κάρτας chip που περιλαμβάνει ενσωματωμένο τσιπ για διάφορους και διάφορους σκοπούς. Οι τεχνολογίες σε αυτόν τον τομέα έχουν αναπτύξει νέους τρόπους για τη χρήση της έξυπνης κάρτας σε κάθε πιθανή καθημερινή δραστηριότητα, όπως αγορές με πίστωση/χρέωση, επίσκεψη σε βιβλιοθήκες, θέατρα κ.λπ. Τα εξελισσόμενα χαρακτηριστικά τους, όπως η βελτιωμένη ασφάλεια, η χρηστικότητα και η λειτουργικότητα, είναι οι κύριοι λόγοι για τους οποίους οι έξυπνες κάρτες είναι σημαντικά καλύτερες από άλλες τεχνολογίες. Οι «έξυπνες» είναι μικροσκοπικοί Η/Υ που έχουν το μέγεθος και το σχήμα μιας πιστωτικής κάρτας, επάνω στην οποία είναι ενσωματωμένο ένα ολοκληρωμένο ηλεκτρονικό κύκλωμα (chip), που περιέχει αποθηκευμένα με μεγάλη ασφάλεια, πολλά προσωπικά στοιχεία του ιδιοκτήτη τους, όπως η ηλεκτρονική υπογραφή και το ιδιωτικό κλειδί της ψηφιακή υπογραφή του κατόχου τους. Ο χρήστης της κάρτας διαθέτει και έναν προσωπικό κωδικό αριθμό για μεγαλύτερη ασφάλεια. Το πρωτόκολλο ISO/IEC7816 καθορίζει: την τοποθέτηση των επαφών, το μέγεθος της κάρτας, τα πρωτόκολλα επικοινωνίας με τη συσκευή ανάγνωσης (Ravichandran, 2016).

3.3.7. Τεχνική Ταυτοποίησης

Οι τεχνικές ταυτοποίησης και αυθεντικοποίησης χρηστών, γενικά, βασίζονται στην λογική του παρακάτω σχήματος.



3.3.8. Διευκόλυνση Των Πολιτών Και Των Επιχειρήσεων

Οι ακόλουθες υπηρεσίες ταυτοποίησης και εμπιστοσύνης μπορούν ήδη να χρησιμοποιηθούν με νομική ισχύ σε όλη την ΕΕ χάρη στο πλαίσιο εμπιστοσύνης που δημιουργήθηκε με τον κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης (eIDAS). Αποτελούν βασικά εργαλεία για την οικοδόμηση της εμπιστοσύνης και την επίτευξη της ασφάλειας στην ψηφιακή ενιαία αγορά. Ορισμένες υπηρεσίες, όπως οι ηλεκτρονικές υπογραφές, θα ενσωματωθούν στο πορτοφόλι προκειμένου να διευκολυνθεί η χρήση τους.

Γράφημα 7: *Διευκόλυνση Πολιτών και Επιχειρήσεων (European Commission, 2019)*

(https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_el#---2)

3.4. Απειλές Και Τρόποι Αντιμετώπισης

Στην περίπτωση της ηλεκτρονικής διακυβέρνησης, οι δυνητικά κακοί χρήστες όχι μόνο θα προσπαθήσουν να εκμεταλλευτούν τα τρωτά σημεία του συστήματος, αλλά θα προσπαθήσουν επίσης να εκμεταλλευτούν τις διαδικασίες που καθορίζουν την εγγραφή, τον έλεγχο ταυτότητας και τον έλεγχο ταυτότητας, με οποιαδήποτε μορφή και αν εκτελούνται, είτε ηλεκτρονικά είτε όχι (Ramaraj & Mukherjee, 2012). Οι κακόβουλοι χρήστες επιχείρησαν να επιλέξουν είτε μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή σε προσφερόμενη υπηρεσία, είτε αντιποίηση αρχής εξουσιοδοτημένου χρήστη ή υπηρεσίας, ή άρνηση παροχής υπηρεσιών, παραβιάζοντας την ιδιωτικότητα προσπαθώντας να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα. Στη συνέχεια πραγματοποιείται μια λεπτομερής παρουσίασης των απειλών αυτών που είναι πιθανό να προκύψουν σε επιθέσεις, ώστε να επιτύχει ο κακόβουλος χρήστης κάποιον από τους σκοπούς που προαναφέρθηκαν.

3.4.1. Απειλές Διακριτικών Αυθεντικοποίησης

Σε αυτές τις περιπτώσεις, οι εισβολείς προσπαθούν να πιστοποιήσουν την ταυτότητα τους ως νόμιμοι χρήστες και να αποκτήσουν πρόσβαση σε εξουσιοδοτημένους πόρους χρηστών με συμπεριφορά που χαρακτηρίζεται από πλαστογραφία, εκμεταλλευόμενοι ορισμένες διαφορές στη νομοθεσία περί πιστοποιημένων χρηστών χωρίς να γίνονται αντιληπτοί από τους παραλήπτες. Για παράδειγμα, ο επιτιθέμενος μπορεί να κάνει χρήση κατάλληλου λογισμικού να υποκλέψει από το σύστημα του νόμιμου χρήστη το μυστικό διακριτικό που φυλάτε στο σκληρό δίσκο του όπως είναι το ιδιωτικό του κλειδί.

3.4.2. Απειλές στα Πρωτόκολλα Αυθεντικοποίησης και στις Παρεχόμενες Υπηρεσίες

Ένα σύνολο από τις πιο γνωστές απειλές είναι δυνατό να προκύψουν στα πρωτόκολλα αυθεντικοποίησης και στις προσφερόμενες ηλεκτρονικές υπηρεσίες ή με ενεργή ή με παθητική συμμετοχή του κακόβουλου χρηστή (Gamundani et al., 2018).

- Υποκλοπή επικοινωνίας-δεδομένων : Ο επιτιθέμενος παρακολουθεί το δίκτυο και καταγράφει τα μεταδεδόμενα, με τους εξής τρόπους:

- Επιθέσεις ενδιάμεσου : Ο κακόβουλος χρήστης σε αυτήν την περίπτωση δρα ως μεσάζον, μεταβαλλόντας τα απεσταλμένα μηνύματα, προωθώντας τα ακολούθως στα πιθανά θύματα του, χωρίς να γίνεται αντιληπτό.

- Υποκλοπή Συνόδου : Ο επιτιθέμενος σε αυτή την περίπτωση κάνει χρήση και αξιοποίηση των δεδομένων από την προηγούμενη έγκυρη συνοδό ανάμεσα σε δύο οντοτήτων για τη μη εξουσιοδοτημένη πρόσβαση στους παρεχόμενους υπολογιστικούς πόρους και υπηρεσίες.

- Επιθέσεις επανάληψης : Ο κακόβουλος χρηστής αφού έχει υποκλέψει ένα μέρος από τα δεδομένα αυθεντικοποίησης, κάνει χρήση και αξιοποίηση τους σε μεταγενέστερο χρόνο, για να

επιτύχει πρόσβαση ως νόμιμος χρήστης, χωρίς βεβαίως να γίνεται αντιληπτός ότι δεν είναι πράγματι ο νόμος χρήστης.

- Επιθέσεις πλαστοπροσωπίας : Ο επιτιθέμενος έχει επιτύχει μη εξουσιοδοτημένη πρόσβαση σε κάποιο από τα διακριτικά αυθεντικοποίησης του νόμιμου χρήστη.

- Επιθέσεις πλημμύρας : Ο επιτιθέμενος προσπαθεί να φτιάξει ένα σημαντικό υπολογιστικό φόρτο, με τη λανθασμένη διαχείριση των υπολογιστικών πόρων του συστήματος που προσφέρει την ηλεκτρονική υπηρεσία, με σκοπό την κατανάλωση των υπολογιστικών πόρων του συστήματος για να προκαλέσει άρνηση παροχής υπηρεσιών.

- Επιθέσεις τροποποιήσεων δεδομένων: Σε αυτή την περίπτωση γίνεται είτε επίθεση ενδιάμεσου, είτε περιλαμβάνεται η έγχυση κακόβουλου κώδικα στα μεταδιδόμενα δεδομένα για τη μη εξουσιοδοτημένη τροποποίηση των αποθηκευμένων δεδομένων του συστήματος, η έγχυση κώδικα SQL στα δεδομένα που αποστέλλει στην υπηρεσία με σκοπό τη μεταβολή ορισμένων αποθηκευμένων δεδομένων.

- Επιθέσεις απόκρυψης ταυτότητας : Ο επιτιθέμενος δημιουργεί μια κάλυψη για την πραγματική του ταυτότητα, κάνοντας χρήση μιας άλλης ταυτότητας άλλης εξουσιοδοτημένης οντότητας όπως πλαστής διεύθυνση IP, η οποία δεν αντιπροσωπεύει την πραγματική διεύθυνση των πακέτων που αποστέλλονται, με σκοπό την απόκρυψη της αρχικής πηγής των επιθέσεων.

3.4.3. Απειλές κατά τη διαδικασία εγγραφής τελικού χρήστη

Οι πιο γνωστές απειλές προκύπτουν κατά τη διαδικασία της εγγραφής και είναι η πλαστοπροσωπία, όπου προσπαθεί ψευδώς να αναπαραστήσει μια άλλη οντότητα, και η αποποίηση εγγραφής όπου προσπαθεί να αποφύγει την πεπραγμένη διαδικασία εγγραφής και τα συνθηματικά (Gamundani et al., 2018).

3.4.4. Πιθανές Επιπτώσεις Κινδύνων

Στον ακόλουθο πίνακα ενδεικτικά προσδιορίζονται οι πιθανές επιπτώσεις που είναι δυνατόν να προκύψουν από τους παραπάνω κινδύνους, τόσους στους χρήστες όσο και στους δημόσιους φορείς σε σύγκριση με το επίπεδο εμπιστοσύνης που σχετίζεται η υπηρεσία.

Επίθεση	**Πιθανές Επιπτώσεις σε Τελικούς Χρήστες**	**Πιθανές επιπτώσεις σε Φορείς ως προς την Παροχή Υπηρεσιών**
Υποκλοπή Διακριτικών Αυθεντικοποίησης	Μη εξουσιοδοτημένη Πρόσβαση Παραβίαση Ιδιωτικότητας Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις ενδιάμεσου	Παραβίαση Ιδιωτικότητας Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων Αντιποίηση Υπηρεσίας

Υποκλοπή Επικοινωνίας-Δεδομένων	Παραβίαση Ιδιωτικότητας Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Υποκλοπή Συνόδου	Μη εξουσιοδοτημένη Πρόσβαση	Δημοσίευση Προσωπικών Δεδομένων
Επιθέσεις Επανάληψης	Μη εξουσιοδοτημένη Πρόσβαση Υποβολή λανθασμένων στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλαστοπροσωπίας	Μη εξουσιοδοτημένη Πρόσβαση	Επεξεργασία Λανθασμένων Στοιχείων
Επιθέσεις Πλημμύρας	Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας
Επιθέσεις Τροποποίησης Δεδομένων	Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία Λανθασμένων Στοιχείων
Ιομορφικό Λογισμικό	Άρνηση πρόσβασης στην Υπηρεσία	Μη Παροχή Υπηρεσίας
Υπερχειλίσεις Προσωρινών Χώρων	Άρνηση πρόσβασης στην Υπηρεσία Μη εξουσιοδοτημένη Πρόσβαση	Μη Παροχής Υπηρεσίας Μη εξουσιοδοτημένη Πρόσβαση
Μη εξουσιοδοτημένη Είσοδος	Μη εξουσιοδοτημένη Πρόσβαση	Μη εξουσιοδοτημένη Πρόσβαση

Γράφημα 8: *Επιπτώσεις Κινδύνων*

3.4.5. Τρόποι Αντιμετώπισης Και Ελαχιστοποίησης Απειλών Και Κινδύνων

Για την ελαχιστοποίηση της πιθανότητας μιας απειλής, επιβάλλονται να υπάρχουν μέτρα ασφάλειας που πρέπει να αντιμετωπίζουν ικανοποιητικά τις διάφορες μορφές απειλών και να διατηρούν την ασφάλεια ενός ΠΣ ώστε να παρέχονται υπηρεσίες

- Αυθεντικοποίηση , η οποία αφορά το επίπεδο εμπιστοσύνης το οποίο οι συναλλασσόμενοι θα πρέπει να έχουν, σε σχέση με την ταυτότητα των εμπλεκομένων μερών.
- Εξουσιοδότηση , η οποία σχετίζεται με τα δικαιώματα που έχει κάθε συναλλασσόμενη οντότητα.
- Ακεραιότητα των δεδομένων, που σχετίζεται με την μη μεταβολή του περιεχομένου των μηνυμάτων στα πλαίσια μιας συναλλαγής.
- Μη-αποποίηση αποστολής και λήψης δεδομένων, ώστε μία οντότητα να μην έχει την δυνατότητα σε μεταγενέστερο χρόνο να αρνηθεί ότι έχει συμμετάσχει σε μία συγκεκριμένη ηλεκτρονική συναλλαγή.
- Υπηρεσίες εξασφάλισης της εμπιστευτικότητας των μηνυμάτων, ανάμεσα στους εμπλεκόμενους σε μία ηλεκτρονική δραστηριότητα.

4 Πυλώνες Εμπιστοσύνης Ηλεκτρονικών Συναλλαγών

1.ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ - CONFIDENTIALITY: Στα δεδομένα του αποστολέα να έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα

2.ΑΥΘΕΝΤΙΚΟΤΗΤΑ - AUTHENTICATION: Ο παραλήπτης πρέπει να είναι βέβαιος για την ταυτότητα του αποστολέα

3.ΑΚΕΡΑΙΟΤΗΤΑ - INTEGRITY: Τα δεδομένα δεν επιτρέπεται να αλλοιωθούν

4.ΜΗ ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ - NON REPUDIATION: Οι συναλλασσόμενοι δεν πρέπει να μπορούν να αρνηθούν εκ των υστέρων την συμμετοχή τους

3.4.6. Ελαχιστοποίηση Και Τρόποι Αντιμετώπισης Των Απειλών Στα Συνθηματικά Των Χρηστών

Ενδεικτικές μέθοδοι για την αντιμετώπιση ή τον περιορισμό των κινδύνων στα συνθηματικά του χρήστη προτείνονται οι ακόλουθες πρακτικές:

- Αξιοποίηση ασφαλών συνθηματικών.
- Ασφαλής αποθήκευσή τους σε κρυπτογραφημένη μορφή.
- Ασφαλής μετάδοση και μεταφορά των διαπιστευτηρίων κατά τη διάρκεια της αυθεντικοποίησης.
- Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού.
- Συχνές μεταβολές του συνθηματικού από τον χρήστη.

3.4.7. Ελαχιστοποίηση Και Τρόποι Αντιμετώπισης Των Απειλών Στα Πρωτόκολλα Αυθεντικοποίησης Και Στις Προσφερόμενες Υπηρεσίες

Τα κύρια στοιχεία των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι τα πρωτόκολλα αυθεντικοποίησης και οι ηλεκτρονικές παρεχόμενες υπηρεσίες, με αποτέλεσμα να εξασφαλίζουν την ορθή λειτουργία των συστημάτων αυτών . Για αυτό και πρέπει να ληφθούν τα αντίστοιχα μέτρα ελαχιστοποίησης και αντιμετώπισης αλλά καις τον περιορισμό εμφάνισης των κινδύνων και των πιθανών επιπτώσεών τους (Sable & Bhosale, 2019).

- Υποκλοπή επικοινωνίας-δεδομένων : τα δεδομένα που σχετίζονται με τα πρωτόκολλα αυθεντικοποίησης και τις υπηρεσίες, τουλάχιστον όσον αφορά τις απόρρητες πληροφορίες πρέπει να κάνουν χρήση των απαραιτήτων μηχανισμών ασφάλειας, ώστε να εξασφαλίζεται η εμπιστευτικότητά τους.
- Επιθέσεις Ενδιαμέσου : Ο περιορισμός της συγκεκριμένης επίθεσης μπορεί να πραγματοποιηθεί μόνο με τη χρήση μηχανισμών ασφάλειας, όπως για παράδειγμα το πρωτόκολλο SSL.

- Επιθέσεις Επανάληψης και Υποκλοπής Συνόδων : Τα πρωτόκολλα αυθεντικοποίησης και οι προσφερόμενες υπηρεσίες επιβάλλεται να επεξεργάζονται δεδομένα που έχουν σχέση με προηγούμενες συνόδους και που είναι πιθανόν να επιδράσουν στην ορθή λειτουργία του συστήματος. Έτσι, προτείνεται να μην αποστέλονται σε μη κρυπτογραφημένη μορφή οι πληροφορίες.

- Επιθέσεις Πλαστοπροσωπίας : Στις επιθέσεις πλαστοπροσωπίας ο επιτιθέμενος επιδιώκει να αποδείξει την κατοχή νόμιμων διαπιστευτηρίων. Έτσι, τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να φανερώνουν δεδομένα που είναι δυνατόν να συμβάλουν στην επιθέσεων πλαστοπροσωπίας.

- Επιθέσεις Πλημμύρας : Είναι σχετικά δύσκολο να περιοριστούν, αλλά είναι δυνατό να ανιχνευθούν

- Επιθέσεις Τροποποίησης Δεδομένων : Είναι δυνατόν να αντιμετωπιστούν με την αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας, όπως message authentication code ή message integrity checksum, MAC και ψηφιακές υπογραφές

- Επιθέσεις Απόκρυψης Ταυτότητας : ελαχιστοποιούνται με την αξιοποίηση κατάλληλων μηχανισμών φιλτραρίσματος ή αναχωμάτων ασφάλειας όπως Firewalls.

3.4.8. Ελαχιστοποίηση Και Μορφές Αντιμετώπισης Των Απειλών Με Την Εγγραφή Τελικού Χρήστη

Σε ορισμένες περιπτώσεις οι απειλές οφείλονται στις επιθέσεις που μπορούν να προκύψουν κατά τη διαδικασία εγγραφής. Για το λόγο αυτό και χρειάζεται ξ άμεση αυθεντικοποίηση των οντοτήτων που επιδιώκουν εγγραφή σε κάποια υπηρεσία, με αυστηρή διάρκεια της ορθότητας των υποβληθέντων δικαιολογητικών και στοιχείων, ώστε να είναι δυνατός ο εντοπισμός των ψευδών δικαιολογητικών και να μην επιτρέπεται η αποποίηση εγγραφής σε κάποια υπηρεσία από μια οντότητα.

Απειλή	**Τύπος Απειλής**	**Τρόποι Αντιμετώπισης**
Απειλές στα Πρωτόκολλα Αυθεντικοποίησης και στις Παρεχόμενες Υπηρεσίες	Υποκλοπή δεδομένων επικοινωνίας (Eavesdropping): (δεδομένα συνομιλίας, μηνύματα ηλεκτρονικού ταχυδρομείου αποστολή, κωδικούς κ.α) και η αξιοποίησή τους σε μελλοντική επίθεση (Traffic Analysis).	Χρήση των απαραιτήτων μηχανισμών ασφάλειας, ώστε να εξασφαλίζεται η εμπιστευτικότητά τους
	Επιθέσεις ενδιάμεσου (Main in the middle attack): δρα ως μεσάζον, μεταβαλλόντας τα απεσταλμένα μηνύματα, προωθώντας τα ακολούθως στα πιθανά θύματα του, χωρίς να γίνεται αντιληπτό.	χρήση μηχανισμών ασφάλειας, όπως για παράδειγμα το πρωτόκολλο SSL
	Υποκλοπή συνόδου(Session hijacking): αξιοποίηση των δεδομένων από την προηγούμενη έγκυρη συνοδό ανάμεσα σε δύο οντοτήτων για τη μη εξουσιοδοτημένη πρόσβαση στους παρεχόμενους υπολογιστικούς πόρους και υπηρεσίες	να μην αποστέλλονται σε μη κρυπτογραφημένη μορφή οι πληροφορίες
	Επιθέσεις επανάληψης (Replay attacks): για υποκλοπή δεδομένων αυθεντικοποίησης για νόμιμη πρόσβαση	
	Επιθέσεις πλαστοπροσωπίας (Impersonation attacks): επιτύχει μη εξουσιοδοτημένη πρόσβαση σε κάποιο από τα διακριτικά αυθεντικοποίησης του νόμιμου χρήστη	να αποδείξει την κατοχή τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να φανερώνουν δεδομένα που είναι δυνατόν να συμβάλουν στην επίθεση έτσι ώστε να τα εκμεταλλευτεί ο επιτιθέμενος ως νόμιμα διαπιστευτήρια
	Επιθέσεις πλημμύρας (Flooding attacks): προσπαθεί να φτιάξει ένα σημαντικό υπολογιστικό φόρτο με σκοπό την κατανάλωση των υπολογιστικών πόρων του συστήματος	αξιοποίηση κατάλληλων μηχανισμών ανίχνευσης επιθέσεων πλημμύρας

	για να προκαλέσει άρνηση παροχής υπηρεσιών Επιθέσεις τροποποιήσεων δεδομένων: είτε επίθεση ενδιάμεσου, είτε έγχυση κακόβουλου κώδικα στα δεδομένα για τη μη εξουσιοδοτημένη τροποποίηση των αποθηκευμένων δεδομένων του συστήματος κώδικα SQL στα δεδομένα που αποστέλλει στην υπηρεσία με σκοπό τη μεταβολή ορισμένων αποθηκευμένων δεδομένων κάλυψη για την πραγματική του ταυτότητα, κάνοντας χρήση μιας άλλης ταυτότητας όπως πλαστής διεύθυνση IP , με σκοπό την απόκρυψη της αρχικής πηγής των επιθέσεων	αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας, όπως message authentication code ή message integrity checksum, MAC και ψηφιακές υπογραφές
Απειλές Διακριτικών Αυθεντικοποίησης	Επιθέσεις λεξικών Επιθέσεις εξαντλητικής αναζήτησης Επιθέσεις τυχαίων δοκιμών Υποκλοπή κατά τη μετάδοση των διαπιστευτηρίων Ο επιτιθέμενος μπορεί να κάνει χρήση κατάλληλου λογισμικού να υποκλέψει από το σύστημα του νόμου χρήστη το μυστικό διακριτικό που φυλάτε στο σκληρό δίσκο του χρήστη όπως είναι το ιδιωτικό του κλειδί ή το συνθηματικό PIN	Αξιοποίηση ασφαλών συνθηματικών Ασφαλής αποθήκευσή τους σε κρυπτογραφημένη μορφή Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού Συχνές μεταβολές του συνθηματικού από τον χρήστη Διατήρηση των διακριτικών αποθήκευσης σε ασφαλή μέρη ώστε να μην είναι δυνατή η υποκλοπή του από κακόβουλους χρήστες
Απειλές κατά τη διαδικασία εγγραφής τελικού χρήστη	Πλαστοπροσωπία: όπου προσπαθεί ψευδώς να αναπαραστήσει μια άλλη οντότητα Αποποίηση εγγραφής: όπου προσπαθεί να αποφύγει την πεπραγμένη	άμεση αυθεντικοποίηση των οντοτήτων που επιδιώκουν εγγραφή σε κάποια υπηρεσία, με αυστηρή διάρκεια της ορθότητας των

	διαδικασία εγγραφής και τα συνθηματικά	υποβληθέντων δικαιολογητικών και στοιχείων ώστε να είναι δυνατός ο εντοπισμός των ψευδών δικαιολογητικών και να μην επιτρέπεται η αποποίηση εγγραφής σε κάποια υπηρεσία από μια οντότητα.

Γράφημα 9: *Απειλές και Τρόποι Αντιμετώπισης*

3.4.9. Κανόνες Ελαχιστοποίησης Κινδύνων

Για την ελαχιστοποίηση των κινδύνων κατά τη διάρκεια υλοποίησης προγραμμάτων ηλεκτρονικής διακυβέρνησης, απαιτείται ο σχεδιασμός των έργων πληροφορικής λαμβάνοντας υπόψιν της ιδιαιτερότητες της Δημόσιας Διοίκησης. Οι αλλαγές στο νομοθετικό πλαίσιο μπορεί να απαιτεί πολλές τροποποιήσεις στα πληροφοριακά συστήματα και ο χρόνος προσαρμογής να είναι μικρός. Χρειάζεται ο έγκαιρος εντοπισμός και η αξιολόγηση των κινδύνων για την αποφυγή αποτυχίας. Είναι ιδιαίτερα σημαντικό να αποφεύγονται τα έργα που βασίζονται σε μη ώριμες τεχνολογίες επικοινωνιών και πληροφοριών διότι αποτυγχάνουν πιο εύκολα. Ο εντοπισμός, η διαχείριση και η αξιολόγηση των κινδύνων θα πρέπει να γίνεται μέσω εξειδικευμένων και δοκιμασμένων μεθόδων. Επίσης χρειάζεται η ηγεσία υψηλού επιπέδου καθώς και υπευθυνότητα από τα ανώτερα στελέχη διοικητικού επιπέδου. Απαιτείται η συμμετοχή εξειδικευμένων στελεχών πληροφορικής και η ανάληψη σαφών πλαισίων υπευθυνότητας από όλα τα ανώτερα στελέχη που εμπλέκονται. Χρειάζεται σωστή διαχείριση της γνώσης και αξιοποίηση των ανθρωπίνων πόρων προκειμένου τα ικανά στελέχη με γνώσεις, ικανότητες και ταλέντο να παραμένουν στο Δημόσιο. Τέλος, κρίνεται απαραίτητη η διαχείριση σχέσεων με εξωτερικούς προμηθευτές καθώς αυτοί που δουλεύουν για τον ιδιωτικό τομέα διαθέτουν μεγαλύτερη τεχνογνωσία και εξειδικευμένο προσωπικό. Ένα σημαντικό λάθος που κάνει η Δημόσια Διοίκηση είναι ότι επικεντρώνεται κυρίως σε επιχειρησιακά θέματα και όχι στην ανάπτυξη του πληροφοριακού τομέα.

3.4.10. Ανάλυση Επικινδυνότητας Και Αποτίμηση Κινδύνου

Ως απειλή μπορεί να θεωρηθεί οποιαδήποτε «πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων-χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος». Οι απειλές που εντοπίζονται στα πληροφοριακά συστήματα, δεν οφείλονται αποκλειστικά σε εξωτερικούς ή εσωτερικούς παράγοντες, αλλά και σε σχεδιαστικά λάθη που μπορούν να οδηγήσουν το πληροφοριακό σύστημα σε μη εκπλήρωση των στόχων του. Η ανάλυση επικινδυνότητας (Risk Analysis) είναι η διαδικασία αναγνώρισης κινδύνων και ο υπολογισμός επικινδυνότητας. Η εκτίμηση επικινδυνότητας (Risk Assessment) είναι η

διαδικασία αξιολόγησης της υπολογισμένης επικινδυνότητας σε σχέση με κριτήρια αξιολόγησης της σημαντικότητάς της (Sinha, 2019). Η συνολική διαδικασία ανάλυσης και εκτίμησης επικινδυνότητας αποτελεί την αποτίμηση και διαχείριση επικινδυνότητας (Risk Assessment and Management). Στηρίζεται στην αρχή ότι απόλυτη ασφάλεια δεν είναι δυνατό να υπάρξει, άρα το καλύτερο που μπορεί να γίνει είναι να εξισορροπηθεί η έκταση των πιθανών κινδύνων με το κόστος εφαρμογής των κατάλληλων αντιμέτρων. Γι' αυτό το λόγο πρέπει να υπολογιστεί η επικινδυνότητα ενός συστήματος ως συνάρτηση των εξής παραγόντων:

• της αξίας των περιουσιακών του στοιχείων (A)

• της φύσης και του βαθμού των ευπαθειών του (V)

• της φύσης και της πιθανότητας εμφάνισης απειλών εναντίον του (T)

• της φύσης και έντασης των επιπτώσεων που θα έχουν οι απειλές αν πραγματοποιηθούν (I)

3.5. Υποδομή Συστημάτων Ηλεκτρονικής Ταυτοποίησης

Είτε προσφέρει ασφαλή έλεγχο ταυτότητας βάσει έξυπνης κάρτας, διαπιστευτήρια βάσει λογισμικού ή διαλειτουργικές υπηρεσίες που βασίζονται σε PKI, η αγορά προϊόντων και υπηρεσιών eID βρίσκεται σε ταχεία μετάβαση. Οι υπάρχουσες και οι αναδυόμενες τεχνολογίες διαμορφώνουν τις εξελίξεις, ενώ οι νέες εφαρμογές και οι συνεργασίες δημιουργούν νέες ευκαιρίες. Επιπλέον, οργανωτικές και θεσμικές αλλαγές προκαλούν στρατηγικές των ενδιαφερομένων σε ένα εξελισσόμενο νομικό και ρυθμιστικό πλαίσιο. Δεν μπορούν, ωστόσο, να παρακολουθηθούν ή να προβλεφθούν όλες αυτές οι εξελίξεις χρησιμοποιώντας ποσοτικές προσεγγίσεις. Πρέπει επίσης να ληφθούν υπόψη σημαντικοί ποιοτικοί παράγοντες.

Υπάρχουν σχετικά ισχυρές τεχνολογίες αναγνώρισης και επαλήθευσης ταυτότητας, οι οποίες υποστηρίζουν μια σειρά από υπηρεσίες προστιθέμενης αξίας. Ωστόσο, πολλές δραστηριότητες λαμβάνουν χώρα στα επίπεδα εκμετάλλευσης και υποδομής, καθώς οι επιχειρήσεις και τα κράτη μέλη σκοπεύουν να διευκολύνουν την πρόσβαση σε νέες υπηρεσίες. Οι εξελίξεις στην τεχνολογία και τη χρήση στην αρένα της ηλεκτρονικής ταυτότητας μπορούν να θεωρηθούν βραχυπρόθεσμες (έως τρία χρόνια) και μακροπρόθεσμες (πέραν των τριών ετών).

Βραχυπρόθεσμα, η τεχνολογία eID θα αναπτυχθεί σε πιο ισχυρές ή τυποποιημένες υλοποιήσεις. Δηλαδή, οι γνωστές τεχνολογίες (π.χ. Single-Sign-On, Public-Key-Infrastructure, smart cards) θα γίνουν πιο πρακτικές μέσω της βελτιωμένης ανάπτυξης προϊόντων και της εμπορευματοποίησης. Οι σχετικά μεγάλες εταιρείες (δηλαδή RSA, Verizon, Microsoft) αναμένεται να σημειώσουν τη μεγαλύτερη πρόοδο βραχυπρόθεσμα.

Τα επόμενα χρόνια θα παρατηρηθεί αύξηση της χρήσης ομοσπονδιακών τεχνολογιών για eID (δηλαδή SUN/Oracle με Liberty Alliance, Microsoft με WS-Federation) καθώς οι εφαρμογές μεταξύ επιχειρήσεων γίνονται πιο mainstream. Επιπλέον, καθώς αυξάνεται η εμπιστοσύνη τόσο στην τεχνολογία όσο και στους εκδότες, οι παραδοσιακά «ανταγωνιζόμενοι» πάροχοι θα γίνουν πιο πρόθυμοι να βασίζονται ο ένας στα διαπιστευτήρια του άλλου σε έναν ομοσπονδιακό χώρο. Αυτό ακολουθεί μια μετατόπιση της έμφασης από την υποκείμενη τεχνολογία eID στις

υπηρεσίες προστιθέμενης αξίας (π.χ. συμβουλευτικές υπηρεσίες, βάσεις δεδομένων μάρκετινγκ, διαδικτυακές πληρωμές).

Όλο και περισσότερο, η τεχνολογία eID ενσωματώνεται είτε στην υποδομή (δηλαδή βιομετρική πρόσβαση σε φορητές συσκευές) είτε στην ευρύτερη τεχνολογική υποδομή («σε όλα τα επίπεδα») μέσω συνεργατικής ανάπτυξης και στρατηγικών συνεργασιών. Οργανισμοί που ενσωματώνουν το eID στην υποδομή τους στοχεύουν στην παροχή ενός ολοκληρωμένου, ολιστικού μοντέλου προϊόντος με επίκεντρο τις υπηρεσίες μέσω της ενσωμάτωσης με βασικούς προμηθευτές υποδομής (π.χ. Microsoft, Cisco, Oracle), έτσι ώστε οι δικές τους τεχνολογίες ασφάλειας και ταυτότητας να γίνουν μέρος του ιστού του Διαδικτύου (Berbecaru et al., 2019).

3.6. Αρχιτεκτονική Συστημάτων Ηλεκτρονικής Ταυτοποίησης

Ακολουθώντας την ιδέα του διαχωρισμού της αποθήκευσης προφίλ χρήστη και της χρήσης προφίλ χρήστη, το βασικό στοιχείο της αρχιτεκτονικής των συστημάτων ηλεκτρονικής ταυτοποίησης είναι ένας διακομιστής αποθετηρίου προφίλ χρήστη (IDRepository) που αποθηκεύει ταυτότητες και προσφέρει στους κατόχους των ταυτοτήτων και τις διεπαφές εξουσιοδοτημένων υπηρεσιών να έχουν πρόσβαση σε αυτές τις πληροφορίες. Ο διακομιστής προσφέρει τη δυνατότητα αποθήκευσης πολλαπλών ταυτοτήτων και σύνδεσης ταυτοτήτων μεταξύ τους. Η σύνδεση γίνεται με τον καθορισμό των μονοπατιών διάδοσης δεδομένων, δηλαδή, με τον καθορισμό του τρόπου με τον οποίο διαδίδονται τα χαρακτηριστικά που αλλάζουν σε μία ταυτότητα διαδίδονται σε άλλες ταυτότητες. Κάθε διακομιστής IDRepository έχει σχεδιαστεί για να επιτρέπει την κεντρική αποθήκευση των ταυτοτήτων πολλών ατόμων. Ταυτόχρονα, είναι δυνατό να υπάρχουν αρκετοί διακομιστές IDRepository για ένα άτομο, με τον καθένα να αποθηκεύει διαφορετική ταυτότητα. Όλες οι παρουσίες διακομιστή μπορούν να συνεργαστούν σε ένα ομοσπονδιακό δίκτυο. Το δίκτυο των διακομιστών IDRepository μπορεί επίσης να είναι ένα υποδίκτυο σε ένα μεγαλύτερο σύνολο κόμβων Liberty Alliance. Χρησιμοποιώντας την έννοια του κύκλου εμπιστοσύνης της Liberty Alliance, οι κόμβοι IDRepository μπορούν να προωθήσουν πληροφορίες σε κόμβους μη IDRepository που πληρούν ορισμένες βασικές απαιτήσεις για τη διαχείριση ταυτοτήτων με επίκεντρο τον χρήστη.

Η αρχιτεκτονική αυτή υπογραμμίζει δύο χαρακτηριστικά του IDRepository: (1) Οι ταυτότητες που είναι αποθηκευμένες σε έναν ή περισσότερους διακομιστές μπορούν να συνδεθούν (καθορίζοντας διαδρομές διάδοσης δεδομένων). Ένας τέτοιος σύνδεσμος θα διασφαλίσει ότι οι αλλαγές σε επιλεγμένα χαρακτηριστικά σε ένα προφίλ θα προωθούνται αυτόματα στα συνδεδεμένα προφίλ. Αυτό προσφέρει μια εναλλακτική λύση στο να έχετε ένα προφίλ με διαφορετικές προβολές που ορίζονται από δικαιώματα πρόσβασης και καθιστά δυνατό τον ορισμό διαφορετικών ταυτοτήτων που δεν μπορούν εύκολα να αντιστοιχιστούν στο ίδιο άτομο από εξωτερικούς παρατηρητές. (2) Οι υπηρεσίες ενδέχεται να αποθηκεύουν προσωρινά τις πληροφορίες που ανακτώνται από το δίκτυο IDRepository. Για να διατηρούνται ενημερωμένα τα αποθηκευμένα αντίγραφα των προφίλ χρηστών, το IDRepository παρέχει ειδοποιήσεις ενημέρωσης σε υπηρεσίες που αποθηκεύουν πληροφορίες προσωρινής μνήμης (Páez et al., 2020).

ΚΕΦΑΛΑΙΟ 4: ΝΟΜΟΙ ΚΑΙ ΚΑΝΟΝΕΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΠΟΛΙΤΩΝ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

4.1 Λόγοι για απειλές ιδιωτικού απορρήτου στην ηλεκτρονική διακυβέρνηση

Παρόλο που τα έργα ηλεκτρονικής διακυβέρνησης είναι καλά σχεδιασμένα από τους ειδικούς και από την κυβέρνηση, υπάρχουν διάφοροι λόγοι που μένουν πίσω από τα ζητήματα απορρήτου στην ηλεκτρονική διακυβέρνηση. Ο πρώτος και κύριος λόγος είναι η χαμηλή ασφάλεια για τα δεδομένα. Αυτό καλύπτει την ακατάλληλη συλλογή και αποθήκευση των προσωπικών δεδομένων ενός ατόμου. Δεύτερον, ο τρόπος συλλογής των δεδομένων έχει επίσης ζωτικό ρόλο. Όταν πρόκειται να συλλεχθούν δεδομένα από τους πολίτες για την είσοδο στο έργο ηλεκτρονικής διακυβέρνησης, τα περισσότερα από τα δεδομένα θα μεταφερθούν από τα υπάρχοντα αρχεία και ορισμένες από τις πιο πρόσφατες και σημαντικές πληροφορίες θα συλλεχθούν αυτοπροσώπως, με αυτόν τον τρόπο συλλογής οι πληροφορίες θα γίνουν ανασφαλείς όταν το άτομο που καταγράφει τις χρησιμοποιεί με λάθος τρόπο. Η επόμενη απειλή της ιδιωτικής ζωής που αντιμετωπίζουν οι περισσότερες από τις αναπτυσσόμενες χώρες οφείλεται στην έλλειψη γνώσης. Τα άτομα που δεν γνωρίζουν καλά την παροχή των πληροφοριών τους ζητούν βοήθεια από ορισμένες εξωτερικές ιδιωτικές υπηρεσίες και πάλι από αυτές τις υπηρεσίες εάν υπάρχει διαρροή πληροφοριών, το ζήτημα της ιδιωτικότητας ξεκινά από εκεί (Balakrishnan & Deva, 2017).

4.2 Νομικό πλαίσιο περί απορρήτου στην ηλεκτρονική διακυβέρνηση

Υπάρχουν ορισμένοι νόμοι περί απορρήτου που παρέχονται από την κυβέρνηση που παρακολουθούν τις απειλές απορρήτου στην κοινωνία, αλλά απαισιόδοξα η ηλεκτρονική διακυβέρνηση εμπλέκεται σε όλα αυτά τα ζητήματα του νόμου περί απορρήτου και τα δεδομένα λειτουργούν ως πηγή για πολλές εξωτερικές υπηρεσίες (Balakrishnan & Deva, 2017).

Η στρατηγική της ηλεκτρονικής διακυβέρνησης προϋποθέτει τον εμπλουτισμό και εκσυγχρονισμό του σχετικού θεσμικού πλαισίου, τη προσαρμογή της νομοθεσίας που αφορά στις διοικητικές διαδικασίες, την έκδοση των προβλεπόμενων κανονιστικών πράξεων και την εναρμόνιση της εθνικής προς την ευρωπαϊκή νομοθεσία και τα διεθνή πρότυπα. Το θεσμικό πλαίσιο για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης περιλαμβάνει (Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, 2014):

- τη διαλειτουργικότητα των συστημάτων μεταξύ των φορέων της δημόσιας διοίκησης,
- την αναθεώρηση των ρυθμίσεων της ηλεκτρονικής αυθεντικοποίησης,
- την περαιτέρω εξειδίκευση ως προς τις έννοιες των δεδομένων και τη διάθεση τους σαν δημόσια πληροφορία,
- την αξιολόγηση των αρχών της προσβασιμότητας στις ψηφιακές υπηρεσίες,

- την ασφάλεια και προστασία της ιδιωτικότητας,
- την εποπτεία της εφαρμογής των θεσμικών προβλέψεων,
- την απλούστευση των προδιαγραφών και των διαδικασιών ανάθεσης δημόσιων έργων πληροφορικής,
- την αξιοποίηση των θεσμοθετημένων αρχών, κανόνων και προτύπων,
- την ανάπτυξη δράσεων και τη λήψη μέτρων για τον συστηματικό και αυστηρό έλεγχο της εφαρμογής τους στις ΤΠΕ του δημόσιου τομέα.

Στην Ελλάδα ο πιο πρόσφατος νόμος σχετικά με την πολιτική απορρήτου και την ασφάλεια στην ηλεκτρονική διακυβέρνηση είναι ο Νόμος 4727/2020. Σκοπός του Νόμου αυτού είναι «*η ολοκληρωμένη ρύθμιση όλων των θεμάτων που άπτονται της ψηφιακής διακυβέρνησης και ιδίως εκείνων που σχετίζονται με τη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) από τους φορείς του δημόσιου τομέα για τις ανάγκες της λειτουργίας τους, καθώς και την υποστήριξη της άσκησης των αρμοδιοτήτων και των συναλλαγών τους με φυσικά ή νομικά πρόσωπα ή νομικές οντότητες*».

Σύμφωνα με το Άρθρο 9, που αφορά τις Υπηρεσίες Ψηφιακής Διακυβέρνησης στα Υπουργεία, στην Υπηρεσία Ψηφιακής Διακυβέρνησης υπάγονται όλες οι αρμοδιότητες που σχετίζονται με την αξιοποίηση των ΤΠΕ και γενικότερα τον συντονισμό της υλοποίησης δράσεων ψηφιακής διακυβέρνησης. Ειδικότερα, οι οργανικές μονάδες που υπάγονται στην Υπηρεσία Ψηφιακής Διακυβέρνησης παρέχουν τεχνική υποστήριξη για την κάλυψη των μηχανογραφικών αναγκών του Υπουργείου και την οργάνωση, λειτουργία και συντήρηση των υποδομών πληροφορικής και επικοινωνιών του Υπουργείου και μεριμνούν ιδίως για την ορθολογική αξιοποίηση των πληροφοριακών συστημάτων, την ψηφιοποίηση των διοικητικών διαδικασιών, τη βελτίωση των σχέσεων κράτους - πολίτη, την υποστήριξη προς όλες τις υπηρεσίες του οικείου Υπουργείου και τους εποπτευόμενους φορείς για την υλοποίηση της περαιτέρω χρήσης των πληροφοριών του δημόσιου τομέα.

Σύμφωνα με το άρθρο 11, καθιερώνεται ο προσωπικός αριθμός (Π.Α.) ως ένας αριθμός υποχρεωτικής επαλήθευσης της ταυτότητας των φυσικών προσώπων στις συναλλαγές τους με τους φορείς του δημόσιου τομέα. Ο Π.Α. αποτελείται από δώδεκα (12) αλφαριθμητικά στοιχεία, εκ των οποίων τουλάχιστον τα εννέα (9) είναι αριθμητικά, και χορηγείται άπαξ στο φυσικό πρόσωπο. Ο Π.Α. δεν μεταβάλλεται και απενεργοποιείται με τον θάνατο ή την κήρυξη σε αφάνεια του φυσικού προσώπου. Ο Π.Α. χορηγείται υποχρεωτικά σε κάθε φυσικό πρόσωπο που δικαιούται Αριθμό Φορολογικού Μητρώου (Α.Φ.Μ.) ή Αριθμό Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.), σύμφωνα με την εθνική νομοθεσία. Η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) είναι αποκλειστικά αρμόδια για την παροχή υπηρεσιών επαλήθευσης ταυτότητας των φυσικών προσώπων προς τους φορείς του δημόσιου τομέα και για την αντιστοίχιση των Π.Α. με τους αναγνωριστικούς αριθμούς των μητρώων (ειδικούς τομεακούς αριθμούς) των φορέων του δημόσιου τομέα, ιδίως Α.Φ.Μ. και Α.Μ.Κ.Α., με σκοπό την επαλήθευση της ταυτότητας των φυσικών προσώπων και την επίτευξη

διαλειτουργικότητας των πληροφοριακών συστημάτων των αρμόδιων φορέων μέσω του Κέντρου Διαλειτουργικότητας, υπό τους όρους προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων και την εθνική νομοθεσία. Η Γ.Γ.Π.Σ.Δ.Δ. είναι υπεύθυνη επεξεργασίας για τους σκοπούς της επαλήθευσης της ταυτότητας των φυσικών προσώπων και τηρεί το Μητρώο Προσωπικού Αριθμού.

Οι φορείς του δημόσιου τομέα επεξεργάζονται τον Π.Α., μέσω του Κέντρου Διαλειτουργικότητας της Γ.Γ.Π.Σ.Δ.Δ., με μόνο και αποκλειστικό σκοπό την επαλήθευση της ταυτότητας των φυσικών προσώπων για την παροχή δημόσιων υπηρεσιών προς φυσικά και νομικά πρόσωπα, την εν γένει διεκπεραίωση των υποθέσεων των φυσικών προσώπων και την άσκηση των αρμοδιοτήτων τους, χωρίς να τον συλλέγουν και αποθηκεύουν στα πληροφοριακά συστήματα ή στα συστήματα αρχειοθέτησης και τηρώντας τα απαραίτητα τεχνικά και οργανωτικά μέτρα που ορίζονται στο προεδρικό διάταγμα της παρ. 6 του άρθρου 107. Ο Π.Α. δεν τηρείται από τους επιμέρους φορείς του δημόσιου τομέα, οι οποίοι αποδίδουν στα φυσικά πρόσωπα αναγνωριστικό αριθμό εσωτερικού τους μητρώου, για την επίτευξη της λειτουργικότητας των πληροφοριακών συστημάτων τους και των ειδικών ανεξάρτητων μητρώων τους. Όταν σύμφωνα με τη νομοθεσία απαιτείται η συλλογή και επεξεργασία του Α.Φ.Μ., ιδίως για φορολογικούς ή τελωνειακούς σκοπούς ή για σκοπούς είσπραξης δημοσίων εσόδων χρησιμοποιούνται και αποτελούν αντικείμενο επεξεργασίας μόνο τα τελευταία εννέα (9) αριθμητικά στοιχεία του Π.Α. Ο προσωπικός αριθμός αποτελεί μία απόπειρα ενιαίας ταυτοποίησης των πολιτών στις συναλλαγές τους με το Δημόσιο, όπως συμβαίνει και σε άλλες χώρες εντός αλλά και εκτός της Ευρωπαϊκής Ένωσης (πχ. Εσθονία, Βουλγαρία), η οποία αποβλέπει στην καταπολέμηση της γραφειοκρατίας και στην απλούστευση της διαδικασίας ταυτοποίησης. Σύμφωνα με την αιτιολογική έκθεση του ν.4727/20 για το άρθρο 11, το οποίο προβλέπει τη δημιουργία του Προσωπικού Αριθμού, προβλέπεται ότι η χρήση τού δεν συνεπάγεται την ολοκλήρωση της επαλήθευσης της ταυτότητας των φυσικών προσώπων, αποτελώντας αναγκαίο, αλλά όχι επαρκές στοιχείο. Ωστόσο, θα αποτελεί τον μοναδικό αριθμό που θα απαιτείται στη συντριπτική πλειονότητα των συναλλαγών των φυσικών προσώπων με το Δημόσιο.

4.3 Νομικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και αυθεντικοποίηση

Σύμφωνα με το Άρθρο 10 του Νόμου 4325/2015, κατά την εγγραφή στην υπηρεσία ηλεκτρονικής διακυβέρνησης μπορεί να χρησιμοποιούνται διαπιστευτήρια που έχουν εκδοθεί για την επιβεβαίωση της ταυτότητας του χρήστη από άλλους φορείς του δημόσιου ή ιδιωτικού τομέα και είναι διασυνδεμένα με ένα ή περισσότερα αναγνωριστικά που σχετίζονται με βασικά μητρώα, όπως ιδίως: α) το μητρώο ταυτοτήτων, β) το μητρώο κοινωνικής ασφάλισης, γ) το φορολογικό μητρώο, και δ) το δημοτολόγιο. Οι φορείς που παρέχουν ηλεκτρονικές υπηρεσίες επιβεβαίωσης της ταυτότητας σε άλλους φορείς και συστήματα του δημόσιου τομέα λειτουργούν, σύμφωνα με τον Κανονισμό 910/2014 της 23ης Ιουλίου 2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες

εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της Οδηγίας 1999/93/ΕΚ.

Ο προσφάτως δημοσιευθείς Νόμος 4727/2020 (ΦΕΚ Α' 184/23.09.2020) για την Ψηφιακή Διακυβέρνηση (ενσωμάτωση της Οδηγίας 2016/2102/ΕΕ) και για τις Ηλεκτρονικές Επικοινωνίες (ενσωμάτωση της Οδηγίας 2018/972/ΕΕ) – (εφεξής «Κώδικας») – εισάγει ένα νέο νομοθετικό καθεστώς για το ψηφιακό περιβάλλον και τις Ηλεκτρονικές Επικοινωνίες. Οι διατάξεις του ως άνω νόμου εφαρμόζονται τόσο σε ιδιώτες και επιχειρήσεις όσο και στους φορείς της Γενικής Κυβέρνησης του άρθρου 14 του ν. 4270/ 2014 (Α` 143), στα εκτός αυτής νομικά πρόσωπα δημοσίου δικαίου (Ν.Π.Δ.Δ.), καθώς και στις εκτός αυτής δημόσιες επιχειρήσεις και οργανισμούς του Κεφαλαίου Α` του ν. 3429/2005 (Α` 314), ανεξαρτήτως εάν έχουν εξαιρεθεί από την εφαρμογή του, με σκοπό τη διευκόλυνση των αναγκών τους, καθώς και των διοικητικών διαδικασιών. Παράλληλα ο Κώδικας Ψηφιακής Διακυβέρνησης εναρμονίζεται με τους ορισμούς του Ευρωπαϊκού Κανονισμού 910/2014 (elDAS Regulation) για τις ηλεκτρονικές υπογραφές, ενώ ταυτόχρονα καταργεί το μέχρι πρότινος νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές, ήτοι το ΠΔ 150/2001 (Α' 125).

Σύμφωνα με το Άρθρο 13 του Νόμου 4727/2020 για την έκδοση Ηλεκτρονικών Δημοσίων Εγγράφων, όλες οι διαδικασίες για τη διαχείριση δημοσίων εγγράφων από τους φορείς του δημοσίου τομέα, όπως η σύνταξη, η προώθηση για υπογραφή, η θέση υπογραφής, η έκδοση, η εσωτερική και η εξωτερική διακίνηση, η πρωτοκόλληση, καθώς και η αρχειοθέτησή τους πραγματοποιούνται αποκλειστικά μέσω ΤΠΕ. Τα ηλεκτρονικά δημόσια έγγραφα παράγονται είτε πλήρως αυτοματοποιημένα μέσω ειδικού πληροφοριακού συστήματος που συνθέτει κατάλληλα στοιχεία, είτε μέσω ηλεκτρονικής υποβολής γραφείου, είτε μέσω ψηφιοποίησης έντυπου εγγράφου. Τα ηλεκτρονικά ακριβή αντίγραφα φέρουν υποχρεωτικά: εγκεκριμένη ηλεκτρονική χρονοσφραγίδα, είτε την εγκεκριμένη ηλεκτρονική σφραγίδα του φορέα είτε την εγκεκριμένη ηλεκτρονική υπογραφή του αρμοδίου για την έκδοση του αντιγράφου οργάνου, την ένδειξη «ακριβείς αντίγραφο» και τα στοιχεία του οργάνου που υπέγραψε το έγγραφο ως τελικώς υπογράφων. Τα ψηφιοποιημένα ηλεκτρονικά αντίγραφα εκδίδονται από τους φορείς του δημοσίου τομέα μέσω ψηφιοποίησης ή αναπαραγωγής με χρήση ΤΠΕ έντυπων δημόσιων ή ιδιωτικών εγγράφων που κατέχουν στο πλαίσιο της άσκησης των αρμοδιοτήτων τους.

Όπως συμπληρώνει το Άρθρο 14, τα πρωτότυπα ηλεκτρονικά δημόσια έγγραφα και τα πιστοποιητικά και οι βεβαιώσεις, έχουν την ίδια νομική και αποδεικτική ισχύ με τα δημόσια έγγραφα που φέρουν ιδιόχειρη υπογραφή και σφραγίδα και γίνονται υποχρεωτικά αποδεκτά από τους φορείς του δημοσίου τομέα.

Επιπλέον, στο Άρθρο 15 αναφορικά με τα ηλεκτρονικά ιδιωτικά έγγραφα ορίζεται τα Ηλεκτρονικά ιδιωτικά έγγραφα εκδίδονται από φυσικά ή νομικά πρόσωπα ή νομικές οντότητες με χρήση εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας, γίνονται υποχρεωτικά αποδεκτά από τους φορείς του δημόσιου τομέα, από τα δικαστήρια όλων των βαθμών και τις εισαγγελίες όλης της χώρας και από φυσικά ή νομικά πρόσωπα ή νομικές οντότητες κατά την ηλεκτρονική διακίνησή τους. Επιπρόσθετα, στο Άρθρο 17 που αφορά στην ηλεκτρονική διακίνηση δημοσίων εγγράφων εντός του ίδιου φορέα ορίζεται ότι τα ηλεκτρονικά δημόσια έγγραφα που εκδίδονται και διακινούνται εντός κάθε φορέα του δημοσίου τομέα σε

κλειστά πληροφοριακά συστήματα, όπως τα εσωτερικά συστήματα ηλεκτρονικής διακίνησης εγγράφων (Σ.Η.Δ.Ε.), φέρουν α) προηγμένη ή εγκεκριμένη ηλεκτρονική χρονοσφραγίδα και β) είτε την προηγμένη ή εγκεκριμένη ηλεκτρονική σφραγίδα του φορέα είτε την προηγμένη ή εγκεκριμένη ηλεκτρονική υπογραφή του αρμόδιου οργάνου. Η χρήση των εσωτερικών συστημάτων ηλεκτρονικής διακίνησης εγγράφων προϋποθέτει την αυθεντικοποίηση κάθε χρήστη.

Το Άρθρο 25 αναφέρει ότι για την έκδοση διαπιστευτηρίων η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης είναι αποκλειστικά υπεύθυνη για την ταυτοποίηση και την αυθεντικοποίηση των φυσικών ή νομικών προσώπων ή νομικών οντοτήτων για σκοπούς παροχής και χρήσης των ψηφιακών δημόσιων υπηρεσιών. Η ταυτοποίηση φυσικών προσώπων διενεργείται: α) Μέσω της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, σύμφωνα με τα οριζόμενα στην υπ' αρ. 1178/2010 απόφαση του Υπουργού Οικονομικών «Εγγραφή νέων χρηστών στις ηλεκτρονικές υπηρεσίες TaxisNet» (Β΄ 1916).β) Με φυσική παρουσία του φυσικού προσώπου στα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ). γ) Με τη χρήση εξ αποστάσεως ταυτοποίησης που παρέχει διασφάλιση ισοδύναμη με τη φυσική παρουσία. Η ταυτοποίηση αυτή μπορεί να διενεργείται μέσω του Εθνικού Μητρώου Επικοινωνίας Πολιτών του άρθρου 17 του ν. 4704/2020 (Α΄ 133).

Τέλος, το Άρθρο 24 αφορά τους τρόπους αυθεντικοποίησης για χρήση υπηρεσιών μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης. Σύμφωνα με το εν λόγω άρθρο, η αυθεντικοποίηση του χρήστη γίνεται μετά από επιλογή του χρήστη με έναν από τους ακόλουθους τρόπους: α) Με τη χρήση των κωδικώνδιαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης του Υπουργείου Ψηφιακής Διακυβέρνησης. β) Με τη χρήση των κωδικώνδιαπιστευτηρίων των συστημάτων ηλεκτρονικής τραπεζικής (ebanking) των πιστωτικών ιδρυμάτων όπως ορίζονται στο στοιχείο 1 της παρ. 1 του άρθρου 4 του Κανονισμού (ΕΕ) 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 (ΕΕ L 176).

4.4 Νομικό πλαίσιο για τα μέσα ταυτοποίησης

Σύμφωνα με το Άρθρο 57 του Νόμου 4727/2020 , που αναφέρεται στις μεθόδους ταυτοποίησης, πριν από την έκδοση πιστοποιητικού υπηρεσίας εμπιστοσύνης, ο πάροχος υπηρεσιών εμπιστοσύνης προβαίνει με κατάλληλα μέσα στην εξακρίβωση της ταυτότητας και των ειδικών χαρακτηριστικών του αιτούντος (ταυτοποίηση). Τη διαδικασία του προηγούμενου εδαφίου δύναται να διενεργεί και τρίτος δυνάμει σύμβασης με τον πάροχο υπηρεσιών εμπιστοσύνης. Η δυνατότητα ταυτοποίησης από τρίτο ενεργοποιείται μετά από την ενημέρωση προς την Ε.Ε.Τ.Τ. σύμφωνα με την παρ. 2 του άρθρου 24 του Κανονισμού eIDAS. Η ταυτοποίηση διενεργείται με μία από τις αναφερόμενες στην παρ. 1 του άρθρου 24 του Κανονισμού eIDAS μεθόδους. Ειδικότερα, ο πάροχος υπηρεσιών εμπιστοσύνης ή τρίτος δύναται να χρησιμοποιεί μεθόδους ταυτοποίησης με διασφάλιση ισοδύναμη με τη φυσική παρουσία, όπως την ηλεκτρονική ή την εξ αποστάσεως ταυτοποίηση, σύμφωνα με το άρθρο 24 του Κανονισμού eIDAS. Η ισοδύναμη

διασφάλιση εξετάζεται και επιβεβαιώνεται από οργανισμό αξιολόγησης συμμόρφωσης, όπως ορίζεται στην περ. 18 του άρθρου 3 του ανωτέρω Κανονισμού.

4.5 Από την έννοια της ιδιωτικότητας της πληροφορίας στην έννοια των προσωπικών δεδομένων

Η έννοια της ιδιωτικότητας των πληροφοριών καθίσταται εξαιρετικά σημαντική σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης, εξαιτίας τόσο του χαρακτήρα των πληροφοριών που αξιοποιούνται όσο και του σημαντικού όγκου που συλλέγεται, επεξεργάζεται και αποθηκεύεται (Vrakas, et al., 2010). Οι απαιτήσεις ασφάλειας περιλαμβάνουν (Γκρίτζαλης, 2004):

- Εμπιστευτικότητα (Confidentiality): προστασία από αποκάλυψη δεδομένων από μη εξουσιοδοτημένους χρήστες
- Ακεραιότητα (Integrity): προστασία από μη εξουσιοδοτημένη τροποποίηση ή διαγραφή δεδομένων
- Διαθεσιμότητα (Availability): προστασία από μη-διάθεση των δεδομένων
- Αυθεντικότητα (Authenticity): διασφάλιση της πραγματικής ταυτότητας κάθε εμπλεκόμενης οντότητας
- Μη Αποποίηση (Non Repudiation): προστασία από άρνηση μια οντότητας για πραγματοποίηση συγκεκριμένης δραστηριότητας.

Όσον αφορά τις απαιτήσεις για ασφάλεια ιδιωτικότητας σε τεχνικό επίπεδο (Cannon, 2004) (Καλλονιάτης, 2011) :

- Αυθεντικοποίηση (Authentication): η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας.
- Εξουσιοδότηση (Authorization): η διαδικασία μέσω της οποίας μία οντότητα αποκτά πρόσβαση σε μια υπηρεσία.
- Αναγνώριση (Identification): η διαδικασία μέσω της οποία ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.
- Προστασία Δεδομένων (Data Protection): σύμφωνα με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ διασφαλίζονται οι αρχές της νομιμότητας και της δικαιοσύνης, του σκοπού και της αναγκαιότητας της συλλογής των δεδομένων και της επεξεργασίας τους αυτών, της ασφάλειας και της ακεραιότητας, της εποπτείας και επικύρωσης.

- Ανωνυμία (Anonymity): η διαδικασία μέσω της οποίας διασφαλίζεται ότι μία οντότητα μπορεί να χρησιμοποιήσει μια υπηρεσία χωρίς να αποκαλύψει την ταυτότητά του.
- Ψευδωνυμία (Pseydonymity): η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση μιας οντότητας.
- Μη-συνδεσιμότητα (Unlinkability): η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας απαγορεύοντας στους εισβολείς να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, ώστε να αποκαλυφθεί ταυτότητα.
- Μη-παρατηρησιμότητα (Unobservability): η διαδικασία μέσω της οποία προστατεύεται η ιδιωτικότητα μιας οντότητας από τον εντοπισμό των ιχνών τους από κακόβουλους.

Ο σεβασμός στην ιδιωτική ζωή και η προστασία των προσωπικών δεδομένων είναι έννοιες συνδεδεμένες καθώς και οι δύο αποσκοπούν στον σεβασμό της αυτονομίας του ανθρώπου και της αξιοπρέπειάς του, παρέχοντάς του ένα ασφαλές περιβάλλον μέσα στο οποίο μπορεί να αναπτύσσει ελεύθερα την προσωπικότητά του. (Άρθρο 8 - Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου - Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής'. Lawspot, 2 Δεκεμβρίου 2014). Βάσει του δικαίου της ΕΕ (άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ) η προστασία των προσωπικών δεδομένων αναγνωρίζεται ως θεμελιώδες δικαίωμα του ατόμου. Το δικαίωμα αυτό αναγνωρίζεται και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Ωστόσο τα δύο δικαιώματα διαφέρουν ως προς το πεδίο εφαρμογής τους. Το δικαίωμα της ιδιωτικότητας αναφέρεται σε μία γενική, κατ΄εξαίρεση, απαγόρευση επεμβάσεων στη ζωή του ατόμου. Η προστασία των προσωπικών δεδομένων από την άλλη αφορά ένα πιο «σύγχρονο» και «ευρύτερο» δικαίωμα καθώς ενεργοποιείται όταν υπάρχει επεξεργασία αυτών. Σύμφωνα με το άρθρο 4 του ΓΚΠΔ παράγραφος 1 (Άρθρο 4 - Γενικός Κανονισμός για την Προστασία Δεδομένων - Ορισμοί'. Lawspot, 7 Μάιος 2016) , ως προσωπικά δεδομένα ορίζεται κάθε πληροφορία που αφορά ένα φυσικό πρόσωπο (υποκείμενο δεδομένων) το οποίο μπορεί να ταυτοποιηθεί με ή χωρίς την υπόδειξη ταυτότητας.

4.6 Προσωπικά δεδομένα και προστασία-Νομοθετικό πλαίσιο

Σύμφωνα με το άρθρο 8 του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων (European Court of Human Rights - ECHR), το δικαίωμα του ατόμου στην προστασία σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί μέρος του δικαιώματος σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας. Η Σύμβαση 108 του Συμβουλίου της Ευρώπης είναι η πρώτη και, μέχρι σήμερα, η μόνη διεθνής νομικά δεσμευτική πράξη που ασχολείται με την προστασία δεδομένων. Σύμφωνα με τη νομοθεσία της ΕΕ, η προστασία δεδομένων έχει αναγνωριστεί ως ξεχωριστό θεμελιώδες δικαίωμα. Επιβεβαιώνεται στο άρθρο 16 της Συνθήκης για τη Λειτουργία της ΕΕ, καθώς και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Σύμφωνα με τη νομοθεσία της ΕΕ, η προστασία δεδομένων ρυθμίστηκε για πρώτη φορά από την Οδηγία 95/46/ΕΚ για την Προστασία Δεδομένων το 1995. Λόγω των ραγδαίων τεχνολογικών εξελίξεων, η ΕΕ ενέκρινε νέα νομοθεσία το 2016 για την προσαρμογή των κανόνων προστασίας δεδομένων στην ψηφιακή εποχή. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων τέθηκε σε ισχύ τον Μάιο του 2018, αντικαθιστώντας την Οδηγία για την Προστασία Δεδομένων. Μαζί με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, η ΕΕ ενέκρινε νομοθεσία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις κρατικές αρχές για σκοπούς επιβολής του νόμου. Η Οδηγία (ΕΕ) 2017/680 θεσπίζει τους κανόνες και τις αρχές προστασίας δεδομένων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων (European Court of Human Rights, 2018).

Σύμφωνα με το άρθρο 4 του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) η ταυτότητά του ατόμου εξακριβώνεται άμεσα ή έμμεσα από αναγνωριστικό στοιχείο όπως όνομα, επίθετο, από παράγοντα που προσδιορίζει τη σωματική, φυσιολογική οικονομική κοινωνική ταυτότητα του προσώπου κ.α.

Σύμφωνα με τον ΓΚΠΔ κάθε υποκείμενο δεδομένων έχει συγκεκριμένα δικαιώματα.

Αυτά ορίζονται ως εξής:

- δικαίωμα διαφανούς ενημέρωσης σχετικά με τα δεδομένα. Το υποκείμενο λαμβάνει την ενημέρωση γραπτώς ή με άλλα μέσα (άρθρο 12)
- δικαίωμα πληροφόρησης και δικαίωμα πρόσβασης στα δεδομένα τους και ενημέρωσης σχετικά με την επεξεργασία τους (άρθρα 13 και 14)
- δικαίωμα διόρθωσης των δεδομένων τους από τον υπεύθυνο επεξεργασίας (άρθρο 16)
- δικαίωμα διαγραφής (δικαίωμα στη λήθη) των δεδομένων από τον υπεύθυνο επεξεργασία όταν η επεξεργασία γίνεται κατά την παράβαση του νομού (άρθρο 17)
- δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)
- δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20)
- δικαίωμα εναντίωσης (άρθρο 21)

Η επεξεργασία των δεδομένων αφορά τη διαδικασία που διενεργείται στα δεδομένα προσωπικά χαρακτήρα. Συγκεκριμένα ως «επεξεργασία νοείται κάθε πράξη όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινοποίηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμούς, ο περιορισμός, η διαγραφή ή η καταστροφή» δεδομένων προσωπικού χαρακτήρα (εκσυγχρονισμένη σύμβαση 108, άρθρο 2 στοιχείο β)

Οι αρχές που διέπουν την προστασία των προσωπικών δεδομένων όπως αυτές ορίζονται στον ΓΚΠΔ είναι οι εξής:

- η αρχή της νομιμότητας (άρθρο 5 παρ. 1 στοιχείο α) η οποία συνεπάγεται τη συγκατάθεση του υποκειμένου.
- η αρχή της αντικειμενικότητας (άρθρο 5 παρ. 1 στοιχείο α) διέπει πρωτίστως τη σχέση μεταξύ του υπευθύνου της επεξεργασίας και του υποκειμένου.
- η αρχή της διαφάνειας (άρθρο 5 παρ. 1 στοιχείο α) όπου οι υπεύθυνοι επεξεργασίας οφείλουν να ενημερώσουν το υποκείμενο των δεδομένων για τον σκοπό της επεξεργασίας.
- η αρχή του περιορισμού του σκοπού (άρθρο 5 παρ. 1 στοιχείο β) υπογραμμίζει ότι η επεξεργασία των δεδομένων πρέπει να εκτελείται για συγκεκριμένο καλά καθορισμένο σκοπό.
- η αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 παρ. 1 στοιχείο γ) που περιορίζει την επεξεργασία στο αναγκαίο μέτρο
- η αρχή της ακρίβειας των δεδομένων (άρθρο 5 παρ. 1 στοιχείο δ) διασφαλίζει την βεβαιότητα ότι τα δεδομένα είναι ακριβή και επικαιροποιημένα.
- η αρχή του περιορισμού της αποθήκευσης (άρθρο 5 παρ. 1 στοιχείο στ και άρθρο 32) διασφαλίζει τη διαγραφή ή την ανωνυμία των δεδομένων όταν αυτά δεν είναι πλέον αναγκαία για τον σκοπό που αρχικά συλλέχθηκαν.
- η αρχή της ασφάλειας των δεδομένων (ακεραιότητα και εμπιστευτικότητα) (άρθρο 5 παρ. 1 στοιχείο στ και άρθρο 32) επιβάλλει να εφαρμόζονται τεχνικά και οργανωτικά μέτρα κατά την επεξεργασία των δεδομένων.
- η αρχή της λογοδοσίας (άρθρο 5 παρ. 2) υποχρεώνει τον υπεύθυνο επεξεργασίας να αποδεικνύουν τη συμμόρφωση προς τις διατάξεις περί προστασίας των δεδομένα στα υποκείμενα και στις εποπτικές αρχές.

Σύμφωνα με το άρθρο 5 του ΓΚΠΔ για να είναι νόμιμη και ασφαλής η επεξεργασία των προσωπικών δεδομένων θα πρέπει αυτή να διέπεται από κάποιες αρχές. Συγκεκριμένα προτείνεται για:

- την αρχή της εμπιστευτικότητας (Confidentiality) σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τον τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους

- την αρχή της ακεραιότητας (Integrity) άρθρο 5 ΓΚΠΔ παράγραφος 1 σύμφωνα με την οποία τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια και όχι αλλοιωμένα ή μη ενημερωμένα
- την αρχή της προσφοράς (Availability) σύμφωνα με την οποία τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε χρησιμοποιούν η χρήση τους
- Αυθεντικότητα (Authenticity): αφορά στη διασφάλιση της ταυτότητος κάθε εμπλεκόμενης οντότητας,
- Μη Αποποίηση (Non Reputation): αφορά στην προστασία από άρνηση μια οντότητας για πραγματοποίηση συγκεκριμένης δραστηριότητας

Ο ΓΚΠΔ εφαρμόζεται εάν η εκάστοτε επιχείρηση ή οργανισμός επεξεργάζεται προσωπικά δεδομένα και εδρεύει στην ΕΕ, αν η επιχείρηση εδρεύει εκτός της ΕΕ αλλά επεξεργάζεται προσωπικά δεδομένα που αφορούν την παροχή προϊόντων ή υπηρεσιών σε άτομα εντός της ΕΕ, ή παρακολουθεί τη συμπεριφορά ατόμων εντός της ΕΕ. Αντίθετα ο ΓΚΠΔ δεν εφαρμόζεται εάν το υποκείμενο των δεδομένων είναι νεκρό, αν το υποκείμενο των δεδομένων είναι νομικό πρόσωπο και όταν η επεξεργασία γίνεται από πρόσωπο που ενεργεί για σκοπούς εκτέλεσης εμπορικού ή επαγγελματικού χαρακτήρα.

Το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία/φορέας ο οποίος καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων θεωρείται ο υπέυθυνος επεξεργασίας (άρθρο ΓΚΠΔ 4 παρ. 7). Σύμφωνα με την αιτιολογική σκέψη υπ' αρ. 1/2010 της ομάδας του άρθρου 29 είναι προτιμότερο να θεωρείται υπεύθυνος επεξεργασίας η εταιρεία ή ο φορέας παρά ένα συγκεκριμένο άτομο εντός της εταιρείας ή του φορέα. Επίσης ο ΓΚΠΔ τον προβλέπει ορισμός δύο ή περισσοτέρων υπευθύνων επεξεργασίας εφόσον καθορίζουν από κοινού τους σκοπούς και τα μέσα της. Οι πληροφορίες του υπευθύνου επεξεργασίας σχετικά με την ασφάλεια της επεξεργασία προσδιορίζονταν ρητά στο άρθρο 32 ΓΚΠΔ, ενώ η γενική ευθύνη του για τον προσδιορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να δείχνει και να μπορεί να αποφύγει τη νομιμότητα μιας επεξεργασίας πηγάζει και από το άρθρο 24 ΓΚΠΔ. Επίσης, στο ΓΚΠΔ για πρώτη φορά προσδιορίζεται ρητά αυτοτελής υποχρέωση και των εκτελούντων την επεξεργασία για λήψη μέτρων ασφάλεια. Το άρθρο 33 του ΓΚΠΔ περιέγραφε τις οδηγίες για την υπεύθυνη επεξεργασία δεδομένα προκειμένου να ειδοποιεί την αρμόδια εποπτική αρχή στην περίπτωση της παραβίασης των προσωπικών δεδομένων. Επίσης το πώς θα εντοπίσει ή θα διερευνήσει ο οργανισμος τις παραβιάσεις δεδομένων και αν υπάρχουν τα απαραίτητα εργαλεία και γνώσεις για να αντιδράσει ή να τις διαχειριστεί προληπτικά. Σε αυτό το σημείο είναι όπου τα εργαλεία ανίχνευσης απειλών, πρόληψης και παρακολούθησης απειλών κρίνονται ως εξαιρετικά κρίσιμα.

Από την άλλη ο εκτελών την επεξεργασία είναι το φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία/φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμούς του υπευθύνου της επεξεργασίας (άρθρο ΓΚΠΔ 4 παρ. 8). Για τον λόγο διαφάνειας οι λεπτομέρειες

της σχέσης υπευθύνου και εκτελούν την επεξεργασία πρέπει να καταγραφεί στη σχετική γραπτή σύμβαση (άρθρο ΓΚΠΔ 28 παρ. 3 και 9).

Τέλος, όσον αφορά την τοπική αυτοδιοίκηση, όλοι οι φορείς της τοπικής αυτοδιοίκησης οφείλουν να συμμορφωθούν στις αρχές του ΓΚΠΔ και στην εθνική νομοθεσία που έχει εναρμονιστεί με τον κανονισμό. Συγκεκριμένα οι δήμοι στα πλαίσια των αρμοδιοτήτων τους και για την επίτευξη των στόχων τους, που είναι η εξυπηρέτηση των πολιτών και η παροχή υπηρεσιών πάσης φύσεως, διαχειρίζονται καθημερινά μεγάλο όγκο προσωπικών δεδομένων, ευαίσθητων και μη. Οι κατηγορίες των εποφελούμενων είναι οι εργαζόμενοι με μια κοινή σχέση εργασίας και σε άλλη θέση, οι συνεργαζόμενοι φορείς, οι πολίτες/επιχειρήσεις, οι πολιτιστικοί, αθλητικοί, καλλιτεχνικοί, εθελοντικοί φορείς/σύλλογοι, οι σχολικές μονάδες και τα νομικά πρόσωπα και διάφοροι τομείς.

4.7 Ζητήματα ασφάλειας, απειλές και τρόποι αντιμετώπισης

Η ανάπτυξη της κοινωνίας της πληροφορίας μέσω των νέων τεχνολογιών του ΤΠΕ και κυρίως μέσω της ευρείας χρήσης του διαδικτύου οδήγησαν στην υπερβολική έκθεση της ιδιωτικής ζωής του ατόμου, θέτοντας κατ' επέκταση σε κίνδυνο τα προσωπικά δεδομένα. Σύμφωνα με την Οδηγία 95/46 ΕΚ (άρθρο 17 περί ασφάλειας της επεξεργασίας) ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα απαραίτητα τεχνικά μέτρα για την προστασία των προσωπικών δεδομένων των υποκειμένων, ιδίως συμπεριλαμβάνεται διαβίβαση των δεδομένων μέσω δικτύου. Παράλληλα η ομάδα εργασίας του άρθρου 29 επιχειρεί να αναλύσει την αποτελεσματικότητα της ανωνυμοποίησης και της ψευδωνυμοποίησης ως τεχνικά μέτρα για την προστασία των δεδομένων. Στον ΓΚΠΔ στο άρθρο 4 παρ. 5 ορίζεται επαρκώς η ψευδωνυμοποίηση και η ανωνυμοποίηση. Στην αιτιολογική σκέψη υπ' αρ. 26 του ΓΚΠΔ γίνεται σαφή διευκρίνιση ως προς τις αρχές προστασίας των δεδομένα οι οποίες πρέπει να εφαρμοστούν σε δεδομένα προσωπικού χαρακτήρα που μπορεί να έχουν υποστεί ψευδωνυμοποίηση ωστόσο θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο, φυσικό πρόσωπο και όχι ανώνυμες πληροφορίες που δεν μπορεί να συσχετιστεί με ταυτοποιημένο ή ταυτοποιημένο φυσικό πρόσωπο. Στον ΓΚΠΔ δεν περιλαμβάνεται ένας ακριβής ορισμός της κρυπτογράφησης. Στον άρθρο ΓΚΠΔ 6 παρ. 4 περί νομιμότητας της επεξεργασίας γίνεται λόγος για την υποχρέωση που έχει ο υπεύθυνος επεξεργασίας να λαμβάνει υπόψη του μεταξύ άλλων την ύπαρξη κατάλληλων εγγυήσεων που μπορεί να περιλαμβάνει ψευδωνυμοποίηση ή κρυπτογράφηση. Επιπλέον στο άρθρο 32 του ΓΚΠΔ για την ασφάλεια της επεξεργασίας καταγράφονται ως οργανωτικά και τεχνικά μέτρα ασφάλειας των δεδομένων προσωπικού χαρακτήρα έναντι των κινδύνων η ψευδωνυμοποίηση και η κρυπτογράφηση. Παράλληλα στο άρθρο 34 του ΓΚΠ σχετικά με την ανακοίνωση της παραβίασης δεδομένων στο υποκείμενο διευκρινίζεται ότι δεν χρειάζεται ενημέρωση του υποκειμένου των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που το όνομα, εφόσον τα δεδομένα αυτά (μεταξύ και άλλων προϋποθέσεων) είναι κρυπτογραφημένα. (παρ. 3α).

Σύμφωνα με το Άρθρο 7 της Υπ. Απόφασης 10238 ΕΞ 2020/2020 για τα οργανωτικά μέτρα του Υπουργείου Ψηφιακής Διακυβέρνησης για την ασφάλεια και προστασία δεδομένων προσωπικού χαρακτήρα, αναφέρεται ότι η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης έχει την υποχρέωση λήψης και διαρκούς τήρησης των κατάλληλων και αναγκαίων τεχνικών και οργανωτικών μέτρων ασφάλειας των λαμβανόμενων πληροφοριών και, κατ' ελάχιστον, την καταγραφή και παρακολούθηση των προσβάσεων, τη διασφάλιση ιχνηλασιμότητας και την προστασία των διακινούμενων δεδομένων από κάθε παραβίαση, καθώς και από σκόπιμη ή τυχαία απειλή. Επίσης, η επεξεργασία των δεδομένων της παρ. 3 του άρθ. 4 της παρούσας διενεργείται σύμφωνα με το ισχύον Πλαίσιο Ασφάλειας Πληροφοριακών Συστημάτων της Γ.Γ.Π.Σ.Δ.Δ. του Υπουργείου Ψηφιακής Διακυβέρνησης και τις διατάξεις περί προστασίας δεδομένων προσωπικού χαρακτήρα. Η λήψη του αριθμού κινητού τηλεφώνου του χρήστη όπως περιγράφεται στην παρ. 3 του άρθ. 4 θα χρησιμοποιηθεί α) για τον έλεγχο της ταύτισης του αριθμού επικοινωνίας που δηλώνεται στην εξουσιοδότηση και την υπεύθυνη δήλωση με τον αριθμό κινητού τηλεφώνου που έχει διαβιβαστεί από τα πιστωτικά ιδρύματα και σε περίπτωση που δεν ταυτίζονται η διαδικασία διακόπτεται και β) κατά την διαδικασία αυθεντικοποίησης του χρήστη για την αποστολή κωδικών μιας χρήσης (ενδεικτικά OTP, Push Notifications, Tokens) από το Υπουργείο Ψηφιακής Διακυβέρνησης προς τον χρήστη κατά τη ολοκλήρωση της χρήσης υπηρεσίας υπεύθυνης δήλωσης ή εξουσιοδότησης της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης. Ο αριθμός κινητού τηλεφώνου μπορεί να χρησιμοποιηθεί από το Υπουργείο Ψηφιακής Διακυβέρνησης, και ιδίως από την Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης, για την παροχή υπηρεσιών αυθεντικοποίησης με την χρήση πολλαπλών παραγόντων αυθεντικοποίησης (multi factor authentication) για την πρόσβαση σε άλλες υπηρεσίες της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης. Τέλος, τα διαπιστευτήρια του χρήστη στα συστήματα ηλεκτρονικής τραπεζικής (e-banking) των πιστωτικών ιδρυμάτων δεν γίνονται γνωστά στο Υπουργείο Ψηφιακής Διακυβέρνησης.

4.8. Ο κανονισμός eIDAS

Ο κανονισμός της Ευρωπαϊκής Ένωσης του 2014 για τις υπηρεσίες ηλεκτρονικής αναγνώρισης, επαλήθευσης ταυτότητας και εμπιστοσύνης ενθαρρύνει τα κράτη μέλη να δημιουργήσουν και να αναγνωρίσουν ιδιωτικά και δημόσια διασυνοριακά συστήματα ηλεκτρονικής επαλήθευσης ταυτότητας (European Commission, 2018α). Οι υπηρεσίες εμπιστοσύνης δεν εξαρτώνται από τη φυσική ταυτότητα. Συνεργάζονται με άλλους τύπους επαληθευμένων εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης και διαπιστευτηρίων. Το eIDAS παρέχει το νομικό πλαίσιο για μια αγορά υπηρεσιών εμπιστοσύνης. Η αμοιβαία αναγνώριση μεταξύ των μελών της ΕΕ και η διασυνοριακή ασφάλεια δικαίου είναι ζωτικής σημασίας. Στην ορολογία της ΕΕ, το eID δεν αναφέρεται μόνο σε ηλεκτρονικά δελτία ταυτότητας, αναφέρεται στο ευρύτερο φάσμα των διαπιστευτηρίων ψηφιακής ταυτότητας. Το eIDAS, αντίθετα, αναφέρεται στη στενή διαδικασία ελέγχου ταυτότητας, διασφαλίζοντας ότι οι ηλεκτρονικές σφραγίδες, χρονοσήμανση και άλλες υπηρεσίες ηλεκτρονικής παράδοσης «λειτουργούν διασυνοριακά και έχουν το ίδιο νομικό καθεστώς με τις παραδοσιακές διαδικασίες που βασίζονται σε χαρτί» (European Commission,

2018α). Σύμφωνα με το eIDAS, οι υπηρεσίες εμπιστοσύνης βασίζονται σε νόμιμα αναγνωρισμένα eID. Το eIDAS καθιστά υποχρεωτικό για τις δημόσιες διοικήσεις της Ευρωπαϊκής Ένωσης να αποδέχονται τις ηλεκτρονικές σφραγίδες και υπογραφές από άλλες χώρες, όποτε τις απαιτούν σε εθνικό επίπεδο. Ένα Δίκτυο Συνεργασίας επιτρέπει στα μέλη της ΕΕ να επιτύχουν διαλειτουργικότητα και ασφάλεια για τα συστήματα eID τους.

Ο κανονισμός eIDAS παρέχει μια κοινή βάση για ασφαλή ηλεκτρονική αλληλεπίδραση μεταξύ πολιτών, επιχειρήσεων και δημόσιων αρχών. Ο κανονισμός αποσκοπεί στην αύξηση της αποτελεσματικότητας των δημόσιων και ιδιωτικών διαδικτυακών υπηρεσιών, των ηλεκτρονικών επιχειρήσεων και του ηλεκτρονικού εμπορίου στην ΕΕ. Για το σκοπό αυτό, περιλαμβάνει διατάξεις για υπηρεσίες ηλεκτρονικής ταυτοποίησης και εμπιστοσύνης. Οι διατάξεις για την ηλεκτρονική αναγνώριση είναι νέες, καθώς αυτό το θέμα δεν αντιμετωπίστηκε στην προηγούμενη οδηγία 1999/93/ΕΚ που αντικαταστάθηκε από τον κανονισμό eIDAS. Οι διατάξεις αυτές αναφέρονται λεπτομερώς στα άρθρα 6 έως 16 του κανονισμού και αναφέρονται στις έννοιες της ηλεκτρονικής αναγνώρισης, των μέσων ηλεκτρονικής αναγνώρισης και των συστημάτων ηλεκτρονικής αναγνώρισης (ENISA, 2020):

- Η «Ηλεκτρονική Ταυτοποίηση» σχετίζεται με τη διαδικασία χρήσης προσωπικών δεδομένων ταυτοποίησης σε ηλεκτρονική μορφή, που αντιπροσωπεύουν μοναδικά είτε φυσικό είτε νομικό πρόσωπο, είτε φυσικό πρόσωπο που εκπροσωπεί νομικό πρόσωπο.
- «Ηλεκτρονικά μέσα αναγνώρισης» είναι η υλική ή/και άυλη μονάδα που περιέχει τα προσωπικά δεδομένα αναγνώρισης και η οποία χρησιμοποιείται για τον έλεγχο ταυτότητας σε μια διαδικτυακή υπηρεσία, και
- «Σύστημα ηλεκτρονικής αναγνώρισης» είναι το σύστημα ηλεκτρονικής αναγνώρισης βάσει του οποίου εκδίδονται ηλεκτρονικά μέσα αναγνώρισης σε φυσικά ή νομικά πρόσωπα ή φυσικά πρόσωπα που εκπροσωπούν νομικά πρόσωπα.

Ο κανονισμός εισάγει διάφορες διατάξεις, οι οποίες στοχεύουν στη δημιουργία ενός πλαισίου που θα επιτρέπει στους πολίτες να χρησιμοποιούν τα ηλεκτρονικά μέσα ταυτοποίησής τους διασυνοριακά με κοινό επίπεδο εμπιστοσύνης. Οι διατάξεις περιλαμβάνουν κυρίως τα ακόλουθα στοιχεία, ιδίως:

- Κοινοποίηση: ένα σύστημα ηλεκτρονικής αναγνώρισης μπορεί να κοινοποιηθεί στην Επιτροπή προκειμένου να επωφεληθεί από τη διασυνοριακή αναγνώριση. Τα κράτη μέλη μπορούν να υποβάλλουν συστήματα eID για προειδοποίηση σύμφωνα με ένα προκαθορισμένο πρότυπο που περιγράφει τις βασικές αρχές του συστήματος. Το CID (ΕΕ) 2015/1984 ορίζει τις περιστάσεις, τις μορφές και τις διαδικασίες κοινοποίησης για τα συστήματα eID. Παρέχει επίσης ένα έντυπο κοινοποίησης που χρησιμοποιείται από τα κράτη μέλη. Τα προκοινοποιημένα συστήματα εξετάζονται από εμπειρογνώμονες του eID

κατά τη διάρκεια μιας διαδικασίας αξιολόγησης της ομοτιμίας. Το Δίκτυο Συνεργασίας eIDAS εκδίδει στη συνέχεια γνώμη σχετικά με τη συμμόρφωση του συστήματος ηλεκτρονικής ταυτοποίησης με τις διατάξεις του eIDAS (ειδικά όσον αφορά τη συμμόρφωση με τις απαιτήσεις του αιτούμενου LoA). Το CID (ΕΕ) 2015/296 περιγράφει λεπτομερώς τους όρους συνεργασίας μεταξύ των κρατών μελών, συμπεριλαμβανομένης της αξιολόγησης από ομοτίμους των συστημάτων.

- Αμοιβαία αναγνώριση: τα ηλεκτρονικά μέσα αναγνώρισης που έχουν εκδοθεί στο πλαίσιο κοινοποιημένων συστημάτων ηλεκτρονικής ταυτοποίησης αναγνωρίζονται για διασυνοριακό έλεγχο ταυτότητας για πρόσβαση σε δημόσιες διαδικτυακές υπηρεσίες. Αυτή η αμοιβαία αναγνώριση είναι υποχρεωτική μόνο για διαδικτυακές υπηρεσίες που απαιτούν μέσα ηλεκτρονικής αναγνώρισης με τουλάχιστον ένα ουσιαστικό επίπεδο διασφάλισης (LoA) και για συστήματα eID των οποίων το LoA αντιστοιχεί στο επίπεδο που απαιτείται από την ηλεκτρονική υπηρεσία.
- Επίπεδο διασφάλισης (LoA): ο κανονισμός εισάγει τρία επίπεδα διασφάλισης για μέσα ηλεκτρονικής αναγνώρισης που εκδίδονται στο πλαίσιο κοινοποιημένων συστημάτων ηλεκτρονικής ταυτοποίησης: Χαμηλό, Ουσιαστικό και Υψηλό. Το LoA των μέσων ηλεκτρονικής αναγνώρισης αναφέρεται στον βαθμό εμπιστοσύνης που μπορεί να δοθεί στη διεκδικούμενη ταυτότητα ενός ατόμου κατά τη διάρκεια μιας ηλεκτρονικής

Ο κανονισμός eIDAS εφαρμόζεται σε συστήματα ηλεκτρονικής ταυτοποίησης που κοινοποιούνται από τα κράτη μέλη και σε παρόχους υπηρεσιών εμπιστοσύνης που είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση, με εξαίρεση τις υπηρεσίες εμπιστοσύνης που «χρησιμοποιούνται αποκλειστικά σε κλειστά συστήματα που προκύπτουν από την εθνική νομοθεσία ή από συμφωνίες μεταξύ καθορισμένου συνόλου συμμετεχόντων» (άρθρ. 2). Επιπλέον, οι υπηρεσίες που πληρούν τις ισχύουσες απαιτήσεις που ορίζονται στον Κανονισμό είναι «κατάλληλοι» πάροχοι υπηρεσιών εμπιστοσύνης (άρθρο 3 παράγραφος 17). Ο κανονισμός δεν παρέχει γενικό ορισμό των «παραβιάσεων» ή της «απώλειας ακεραιότητας», αλλά αφορά την «γνωστοποίηση παραβιάσεων και τις εκτιμήσεις κινδύνου ασφάλειας» που είναι «ουσιώδεις για την παροχή επαρκών πληροφοριών στα ενδιαφερόμενα μέρη σε περίπτωση παραβίαση της ασφάλειας ή απώλεια ακεραιότητας». Σύμφωνα με το άρθρο 19 παράγραφος 2, τόσο οι ειδικευμένοι όσο και οι μη εξουσιοδοτημένοι πάροχοι υπηρεσιών εμπιστοσύνης πρέπει «εντός 24 ωρών αφότου λάβουν γνώση, να ενημερώσουν τον εποπτικό φορέα και, κατά περίπτωση, άλλους σχετικούς φορείς, όπως τον αρμόδιο εθνικό φορέα για πληροφορίες ασφάλειας ή την αρχή προστασίας δεδομένων, για τυχόν παραβίαση της ασφάλειας ή απώλεια ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα προσωπικά δεδομένα που διατηρούνται σε αυτήν». Σε περίπτωση που η παραβίαση επρόκειτο να «επηρεάσει

δυσμενώς ένα φυσικό ή νομικό πρόσωπο στο οποίο έχει παρασχεθεί η αξιόπιστη υπηρεσία», τότε ο πάροχος υπηρεσιών εμπιστοσύνης πρέπει να «ειδοποιήσει το φυσικό ή νομικό πρόσωπο . . . χωρίς αδικαιολόγητη καθυστέρηση». Εάν το περιστατικό αφορά δύο ή περισσότερα κράτη μέλη, τότε οι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να ενημερώσουν την εθνική αρχή των οικείων κρατών μελών και τον ENISA. Εάν η «αποκάλυψη της παραβίασης της ασφάλειας ή της απώλειας της ακεραιότητας είναι προς το δημόσιο συμφέρον», τότε η κοινοποιημένη εποπτική αρχή είτε ενημερώνει το κοινό είτε ζητά από τον πάροχο εμπιστοσύνης να το πράξει. Οι ειδικευμένες υπηρεσίες εμπιστοσύνης δέχονται να ελέγχονται τουλάχιστον κάθε δύο χρόνια (με δικά τους έξοδα, άρθρο 20 παράγραφος 1) (Bures & Carrapico, 2018).

Ο κανονισμός θεσπίζει περαιτέρω εποπτικές αρχές για παρόχους υπηρεσιών εμπιστοσύνης, οι οποίοι θα πρέπει να «συνεργάζονται με τις αρχές προστασίας δεδομένων», ιδίως όσον αφορά τις ύποπτες παραβιάσεις των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα, ιδίως σε σχέση με περιστατικά ασφάλειας και παραβιάσεις προσωπικών δεδομένων (αιτιολογική σκέψη 31) (Bures & Carrapico, 2018).

ΚΕΦΑΛΑΙΟ 5: ΜΕΛΕΤΗ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ

Κάθε χώρα έχει πραγματοποιήσει τις προσπάθειές της για τη μετάβαση από την παραδοσιακή διακυβέρνηση, στην ψηφιακή δημόσια διοίκηση, στοχεύοντας στην πλήρη παροχή των κυβερνητικών υπηρεσιών μέσω διαδικτύου, στη διεύρυνση της διαφάνειας και του ελέγχου των έργων των κυβερνήσεων, προωθώντας και τη συμμετοχή των πολιτώ. Αυτό επιτυγχάνεται σταδιακά, και σε διαφορετικά επίπεδα για την κάθε χώρα. Αρχικά, επιτυγχάνεται με την απλή παροχή πληροφοριών στους πολίτες και τις επιχειρήσεις, στη συνέχεια παρέχοντας τη δυνατότητα ενεργού διάδρασης πολίτη-δημόσιας διοίκησης, έπειτα δίνεται η δυνατότητα πραγματοποίησης ηλεκτρονικών συναλλαγών και τέλος η εφαρμογή της Ηλεκτρονικής Δημοκρατίας.

Για την ηλεκτρονική ταυτοποίηση ενός ατόμου μπορούν να χρησιμοποιηθούν διάφοροι τρόποι - μέθοδοι, με βασικότερους τους εξής (Government of Netherlands, 2015):

- χρήση ονόματος χρήστη και κωδικού πρόσβασης,

- χρήση ονόματος χρήστη και κωδικού πρόσβασης με παράλληλη επαλήθευση του χρήστη, ενδεικτικά μέσω της αποστολής μηνυμάτων κειμένου ηλεκτρονικού ταχυδρομείου ή κινητού τηλεφώνου,

- ταυτοποίηση χρήση μέσω λογισμικού (υποδομή δημόσιων κλειδιών PKI),

- έξυπνες κάρτες με απαίτηση επαφής (απαιτείται αναγνώστης καρτών) ή μικροεπεξεργαστή - τσιπ χωρίς επαφή (η κάρτα είναι εξοπλισμένη με πομπό που καθιστά το τσιπ αναγνώσιμο σε ορισμένη απόσταση) επί του οποίου τοποθετείται το πιστοποιητικό,

- κινητό αναγνωριστικό (μέσω της χρήσης κινητού τηλεφώνου ή συνδυασμού κινητού τηλεφώνου και ασύρματης κάρτας δικτύου).

Από την άποψη της τεχνολογίας, τα συστήματα ταυτοποίησης κατατάσσονται σε τρεις βασικές κατηγορίες λύσεων, βασιζόμενα σε (Bour, 2013):

1. Χρήση κωδικού πρόσβασης (Password based systems): τα αντίστοιχα συστήματα επιτρέπουν στους χρήστες να πιστοποιούν την ταυτότητά τους και να υπογράφουν ηλεκτρονικά ένα έγγραφο ή να λαμβάνουν άλλες υπηρεσίες μέσω διαδικτύου, εισάγοντας το όνομα χρήστη και τον κωδικό πρόσβασής τους.
2. Υποδομή δημόσιου κλειδιού (Public Key Infrastructures): τα σχετικά συστήματα επιτρέπουν την ταυτοποίηση των ατόμων μέσω της χρήσης πιστοποιητικών ταυτοποίησης, τα οποία προμηθεύονται από κάποιον πάροχο υπηρεσιών πιστοποίησης. Η ταυτοποίηση μέσω υποδομής δημόσιου κλειδιού βασίζεται στην ασύμμετρη κρυπτογραφία και στη χρήση δύο διαφορετικών κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων αντίστοιχα: ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί του χρήστη αποθηκεύεται σε έναν μικροεπεξεργαστή – τσιπ, το οποίο μπορεί να προστεθεί ενδεικτικά σε μια έξυπνη κάρτα ή σε κάρτα SIM κινητής τηλεφωνίας και το δημόσιο κλειδί είναι διαθέσιμο για την επιβεβαίωση της ταυτότητας

των χρηστών μέσω του αντίστοιχου παρόχου υπηρεσιών πιστοποίησης. Η εφαρμογή υποδομής δημόσιου κλειδιού για την ταυτοποίηση ενός ατόμου είναι σχετικά απλή διαδικασία και ανάλογη της χρήσης μιας πιστωτικής κάρτας και του μυστικού κωδικού PIN της κάρτας. Ως περιορισμό στην εφαρμογή της σχετικής μεθόδους ταυτοποίησης, αποτελεί η ανάγκη εγκατάστασης σχετικών πιστοποιητικών στη συσκευή σύνδεσης – ανάγνωσης της έξυπνης κάρτας που βρίσκεται αποθηκευμένο το ιδιωτικό κλειδί του χρήστη.

3. Χαρακτηριστικά χρήστη (Attribute Based Credentials): αποτελούν τύπους συστημάτων στα οποία οι πληροφορίες σχετικά με τον χρήστη αποθηκεύονται σε οντότητες που ονομάζονται ιδιότητες (attributes). Η χρήση πολλαπλών ιδιοτήτων ενός χρήστη παρέχουν πιστοποίηση του χρήστη από την εκδότρια αρχή. Κατά τη διάρκεια μιας συναλλαγής με έναν πάροχο υπηρεσιών, τα χαρακτηριστικά ενός χρήστη παρέχουν πληροφορίες σχετικά με τα δικαιώματα που έχει ο χρήστης, χωρίς να παρέχονται άμεσα πληροφορίες σχετικά με την ταυτότητα του χρήστη. Για το λόγο αυτό, ονομάζονται επίσης "Διαπιστευτήρια διατήρησης της ιδιωτικής ζωής".

Σε σχετική έρευνα της Bour (2013) σε 31 κράτη της Ευρώπης διαπιστώθηκε πως εφαρμόζονται οι παρακάτω τεχνολογίες εφαρμογής ηλεκτρονικής ταυτοποίησης πολιτών:

- χρήση κωδικού πρόσβασης (17 κράτη),
- υποδομή δημόσιου κλειδιού (26 κράτη),
- σύστημα χαρακτηριστικών χρήστη (1 κράτος).

Επίσης, σε 7 κράτη (Τσεχία, Δανία, Εσθονία, Φινλανδία, Λιθουανία, Νορβηγία και Σουηδία) της Ευρώπης παρέχεται στους πολίτες η δυνατότητα επιλογής μεταξύ της τεχνολογίας χρήσης κωδικού πρόσβασης ή της τεχνολογίας υποδομής δημόσιου κλειδιού.

5.1. ΣΥΣΤΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΣΤΗΝ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

Η Ευρώπη έπρεπε να ξεπεράσει τα διαφορετικά εθνικά νομικά της πλαίσια και ένα πλήθος διαφορετικών τεχνικών προτύπων, όπως σημειώνει μια έκθεση της Ευρωπαϊκής Επιτροπής (European Commission), προκειμένου η ψηφιακή ταυτοποίηση να γίνει πραγματικότητα. Τα συστήματα ψηφιακής ταυτοποίησης της Ευρώπης παραμένουν κατακερματισμένα, ωστόσο η Ευρωπαϊκή Επιτροπή αποδέχτηκε την ποικιλομορφία και προσπάθησε να την εκμεταλλευτεί. Η πολιτική της ΕΕ επικεντρώνεται στην εξασφάλιση των επιθυμητών κοινών αποτελεσμάτων επαλήθευσης, ενώ βασίζεται στην υποδομή ταυτότητας κάθε έθνους. Τα εθνικά συστήματα επαλήθευσης αποφέρουν οφέλη. Βασίζονται στην υπάρχουσα εθνική υποδομή και επιτρέπουν την προσαρμογή της ψηφιακής επαλήθευσης στις τοπικές αγορές και συνθήκες, χωρίς να υπάρχει ανάγκη για ένα μόνο αποδεκτό εθνικό δελτίο ταυτότητας ή ένα μόνο αποδεκτό σύνολο επαληθευμένων διαπιστευτηρίων. Δεν θα πρέπει, θεωρητικά, να έχει σημασία εάν μια έξυπνη κάρτα, ή ένα κινητό τηλέφωνο χρησιμοποιείται για τη διατήρηση και τη μετάδοση διαπιστευτηρίων ταυτότητας. Αυτό που χρειάζεται είναι να διευκολυνθεί η αμοιβαία αναγνώριση – η διαδικασία με την οποία οι ευρωπαϊκές χώρες αναγνωρίζουν και αποδέχονται η

μία τα εθνικά συστήματα επαλήθευσης της άλλης. Η ευρωπαϊκή πολιτική στοχεύει να επιτρέψει αυτή τη διαλειτουργικότητα. Έχει νομοθετήσει και κατασκευάσει ένα φιλόδοξο σύστημα ψηφιακής ταυτότητας και επαλήθευσης. Τρία βασικά δομικά στοιχεία στηρίζουν την ευρωπαϊκή προσπάθεια (Echikson, 2020):

1. Δελτία ταυτότητας: Το 2006, η Ευρωπαϊκή Ένωση συμφώνησε σε κοινό σχεδιασμό και ελάχιστα πρότυπα ασφαλείας για τα εθνικά δελτία ταυτότητας, όπως ότι οι κάρτες πρέπει να είναι κατασκευασμένες από πλαστικοποιημένο χαρτί και να περιέχουν όνομα, ημερομηνία γέννησης, εθνικότητα, φωτογραφία, αριθμό κάρτας και ημερομηνία λήξης ισχύος. Ορισμένες κάρτες περιέχουν περισσότερες πληροφορίες, όπως το ύψος και το χρώμα των ματιών. Είναι σημαντικό ότι οι χώρες δεν υποχρεούνται να εκδίδουν τέτοιου είδους ηλεκτρονικά δελτία ταυτότητας, και ορισμένες δεν το κάνουν, για διάφορους λόγους που κυμαίνονται από το κόστος, στην Ελλάδα, έως τους φόβους παραβίασης των πολιτικών ελευθεριών, στη Δανία (Council of the European Union, 2006).

2. eIDAS: Ο κανονισμός της Ευρωπαϊκής Ένωσης του 2014 για τις υπηρεσίες ηλεκτρονικής αναγνώρισης, επαλήθευσης ταυτότητας και εμπιστοσύνης ενθαρρύνει τα κράτη μέλη να δημιουργήσουν και να αναγνωρίσουν ιδιωτικά και δημόσια διασυνοριακά συστήματα ηλεκτρονικής επαλήθευσης ταυτότητας (European Commission, 2018). Το eIDAS καθιστά υποχρεωτικό για τις δημόσιες διοικήσεις της Ευρωπαϊκής Ένωσης να αποδέχονται τις ηλεκτρονικές σφραγίδες και υπογραφές από άλλες χώρες, όποτε τις απαιτούν σε εθνικό επίπεδο. Ένα Δίκτυο Συνεργασίας επιτρέπει στα μέλη της ΕΕ να επιτύχουν διαλειτουργικότητα και ασφάλεια για τα συστήματα eID τους.

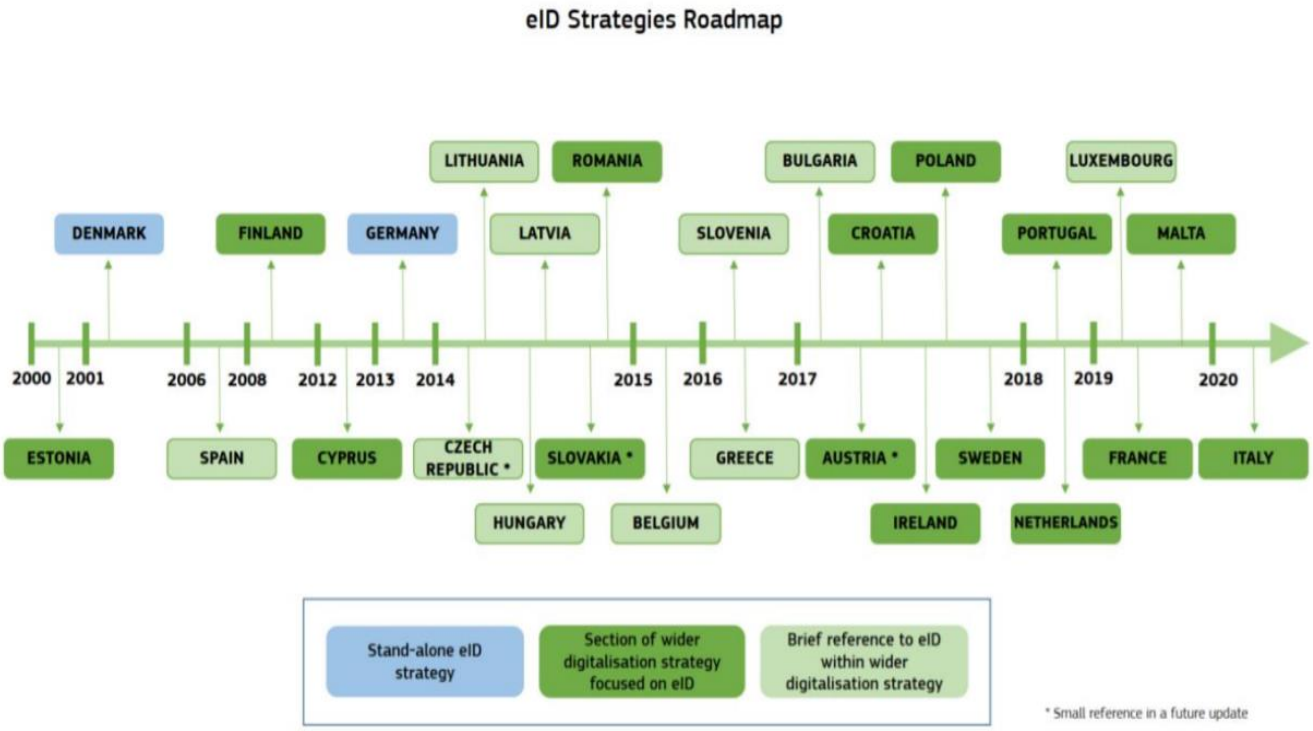
3. Ενιαία ψηφιακή πύλη: Το 2018, η Ευρωπαϊκή Ένωση έδωσε εντολή στα κράτη μέλη να ψηφιοποιήσουν 21 διοικητικές διαδικασίες, συμπεριλαμβανομένου πιστοποιητικού γέννησης, εγγραφής αυτοκινήτου, έναρξης επιχείρησης ή υποβολής εταιρικής φορολογικής δήλωσης έως το τέλος του 2023. Αυτά τα δεδομένα θα είναι διαθέσιμα στο διαδίκτυο μέσω μιας ενιαίας διαδικτυακής πύλης σε ολόκληρη την ΕΕ που ονομάζεται Your Europe. Παράλληλα με αυτό το έργο, ένας ξεχωριστός νέος κανονισμός ενισχύει την ασφάλεια των δελτίων ταυτότητας (Verrando, 2019). Στο πλαίσιο της Ενιαίας Ψηφιακής Πύλης, ένα γαλλικό πανεπιστήμιο θα μπορεί τελικά να επαληθεύσει τα διαπιστευτήρια ενός Γερμανού φοιτητή που υποβάλλει τα ακαδημαϊκά του πτυχία απευθείας από το γερμανικό πανεπιστήμιο χωρίς να χρειάζεται να στείλει έντυπα συμβολαιογραφικά ή να εμφανιστεί αυτοπροσώπως. Η Ευρωπαϊκή Επιτροπή πιστεύει ότι η Ενιαία Ψηφιακή Πύλη θα μπορούσε να εξοικονομήσει στους πολίτες της ΕΕ έως και 855.000 ώρες από τον χρόνο τους ετησίως και στις εταιρείες περισσότερα από 11 δισεκατομμύρια ευρώ ετησίως (European Parliament, 2018).

5.2. ΣΤΡΑΤΗΓΙΚΕΣ E-ID

Οι εθνικές δημόσιες διοικήσεις εντός της ΕΕ διαφέρουν ως προς την έκταση στην οποία παρουσιάζουν στρατηγικό τους όραμα για το eID. Τα κράτη μέλη μπορούν να χωριστούν στις ακόλουθες ομάδες ανάλογα με τον βαθμό στον οποίο έχουν ρητά ορίσει τη στρατηγική eID τους:

- Stand-alone eID strategy document/ Αυτόνομο έγγραφο στρατηγικής eID: Χώρες που έχουν αναπτύξει μια ειδική στρατηγική για την υλοποίηση και προώθηση eID, ταυτοποίηση, στόχους και προθεσμίες για νέα μέτρα. Αυτό το σύμπλεγμα περιλαμβάνει 2 κράτη μέλη: τη Δανία και τη Γερμανία.
- Section of wider digitalisation strategy focused on eID/ Τομέας της ευρύτερης στρατηγικής ψηφιοποίησης που επικεντρώνεται eID: Χώρες που έχουν αφιερώσει μια συγκεκριμένη ενότητα της εθνικής τους στρατηγικής ψηφιοποίησης προς την εφαρμογή των μέτρων eID, τα οποία θα μπορούσαν να είναι η ανάπτυξη νέων μέσων eID, η ενημέρωση του υπάρχοντος προγράμματος ή τη δημιουργία μιας ηλεκτρονικής διακυβέρνησης, όπου το eID διαδραματίζει κρίσιμο ρόλο. Αυτό το σύμπλεγμα περιλαμβάνει 16 κράτη μέλη: Αυστρία, Βέλγιο, Κροατία, Κύπρος, Εσθονία, Φινλανδία, Γαλλία, Ιρλανδία, Ιταλία, Μάλτα, Ολλανδία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβακία και Σουηδία.
- Brief reference to eID within a wider digitalization strategy or strategies/ Σύντομη αναφορά στο eID στο πλαίσιο μιας ευρύτερης στρατηγικής ή στρατηγικές ψηφιοποίησης: Χώρες που έχουν αναπτύξει εθνική στρατηγική ψηφιοποίησης ή στρατηγικές που κάνοντας αναφορά στο eID, αλλά δεν επεκτείνονταιγια το θέμα αυτό αναλυτικά. Αυτό το σύμπλεγμα περιλαμβάνει 9 κράτη μέλη: Βουλγαρία, Τσεχική Δημοκρατία, Ελλάδα, Ουγγαρία, Λετονία, Λιθουανία, Λουξεμβούργο, Σλοβενία και την Ισπανία.

Είναι επίσης ενδιαφέρον να εξεταστεί το έτος κατά το οποίο τα κράτη της ΕΕ δημοσίευσαν επίσημα έγγραφα για να γίνει αντιληπτό ποιες χώρες μπορεί να έχουν απαρχαιωμένες στρατηγικές και δεν έχουν ευθυγραμμιστεί περισσότερο με την πρόσφατη τεχνολογία και τις πολιτικές εξελίξεις. Τα αποτελέσματα αυτής της ανάλυσης παρουσιάζονται στον παρακάτω πίνακα, που δείχνει ότι δεκατέσσερις από τις 26 χώρες έχουν υιοθετήσει μια στρατηγική που επικεντρώνεται ή αναφέρει το eID:



Γράφημα 10: *Στρατηγικές eID*

Σε πολλές περιπτώσεις, το μέσο eID αναπτύχθηκε και υιοθετήθηκε αρκετά χρόνια πριν από την επισημοποίηση των εθνικών στόχων ηλεκτρονικής ταυτότητας. Ως εκ τούτου, η Ελλάδα δεν διαθέτει ισχυρή τάση στις στρατηγικές eID. Ωστόσο, στρατηγικές που υιοθετήθηκαν μετά την παροχή μέσων ηλεκτρονικής ταυτότητας, φαίνεται να έχουν επικεντρωθεί στην επέκταση της ανάπτυξης και της εφαρμογής του eID σε μεγαλύτερο αριθμό περιπτώσεων χρήσης. Ο παρακάτω πίνακας αναφέρει περιληπτικά τους στρατηγικούς στόχους που εκφράζονται στα διάφορα στρατηγικά έγγραφα, κατηγοριοποιώντας τους προκειμένου να προσδιοριστούν αυτά που επιδιώκονται από πολλές χώρες:

ΧΩΡΑ	**ΣΤΡΑΤΗΓΙΚΗ eID**	**ΣΤΟΧΟΙ**
ΕΣΘΟΝΙΑ	1. Περαιτέρω ανάπτυξη κεντρικών τεχνολογικών λύσεων στον τομέα των υπηρεσιών eID και ψηφιακής εμπιστοσύνης (ψηφιακή υπογραφή, ψηφιακή σφραγίδα) 2. Υποστήριξη eID για τις πιο ευρέως χρησιμοποιούμενες πλατφόρμες λογισμικού ανοιχτού κώδικα 3. Διασυνοριακές διαλειτουργικές λύσεις 4. Διασφάλιση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα και της ικανότητάς τους να αντιμετωπίζουν επικίνδυνες καταστάσεις 5. Προώθηση της χρήση της ηλεκτρονικής ταυτότητας μεταξύ αλλοδαπών υπηκόων για να μπορέσουν να	1. Εισαγωγή νέου μέσου Eid 2. Ρύθμιση / αναθεώρηση οικοσυστήματος eID (υποδομή) 3. Διασυνοριακή αναγνώριση eID 4. Συμπράξεις δημόσιου/ιδιωτικού τομέα 5. Αύξηση της διάδοσης του eID 6. Βελτίωση της ασφάλειας 7. Υψηλότερη διοικητική αποτελεσματικότητα και εύκολη πρόσβαση σε ψηφιακές υπηρεσίες 8. Επέκταση περιπτώσεων / δυνατοτήτων χρήσης eID

	χρησιμοποιούν τις εσθονικές ηλεκτρονικές υπηρεσίες και να γίνουν, έτσι, «εικονικοί κάτοικοι» της Εσθονίας 6. Διασφάλιση σταθερότητας στον τομέα της διαχείρισης ταυτότητας και ασφαλούς ταυτοποίησης ενός ατόμου 7. Χρήση σύγχρονων, ασφαλών και φιλικών προς το χρήστη τεχνολογικών λύσεων που επιτρέπουν την όσο το δυνατόν μεγαλύτερη αυτοματοποίηση των διαδικασιών. 8. Εξασφάλιση της χρηστικότητας της ηλεκτρονικής	
ΕΛΛΑΔΑ	Εφαρμογή μιας κοινής μεθόδου ηλεκτρονικής επαλήθευσης ταυτότητας σε συνδυασμό με ένα σύνολο ελέγχων ταυτοποίησης δεδομένων και ασφαλείας, για την πρόσβαση σε διαδικτυακές υπηρεσίες	Εισαγωγή πρώτης κάρτας eID / μέσο eID και η ψηφιακή διαχείριση των δεδομένων
ΙΣΠΑΝΙΑ	1. Ενεργοποίηση μηχνισμού αναγνώρισης μέσω ονόματος χρήστη και κωδικού πρόσβασης, ενσωματωμένοι στην πλατφόρμα Cl@ve 2. Προσβασιμότητα σε δημόσιες υπηρεσίες πολλαπλών πλατφορμών, με στόχο την εξέλιξη των υφιστάμενων συστημάτων αναγνώρισης και υπογραφής προς πιο απλά και χρηστικά μοντέλα, και σε κινητά τηλέφωνα.	1. Ενεργοποίηση ψηφιακής διαχείρισης 2. Επέκταση περιπτώσεων / δυνατοτήτων χρήσης eID και χρήση κινητής ταυτότητας
ΠΟΡΤΟΓΑΛΙΑ	1. Εξασφάλιση ότι οι πληροφορίες είναι διαθέσιμες μέσω ενός μόνο σημείου, προσβάσιμο με χρήση ενός μόνο στοιχείου αναγνώρισης 2. Ανάπτυξη της κάρτας του πολίτη διαθέσιμη με νέες δυνατότητες 3. Επιτρέπει στους πολίτες να πιστοποιούν την ταυτότητά τους σε ιστότοπους και συστήματα δημόσιας διοίκησης	1. Δημιουργία κεντρικής πύλης ηλεκτρονικής διακυβέρνησης 2. eID σημαίνει επέκταση σε πρόσθετες λειτουργίες 3. Επέκταση περιπτώσεων χρήσης eID
ΒΕΛΓΙΟ	1. Διασφάλιση ότι το μέγιστο όριο διαδικτυακών δημόσιων υπηρεσιών είναι διαθέσιμες χρησιμοποιώντας την Ομοσπονδιακή Υπηρεσία ελέγχου ταυτότητας (FAS) και Eid. 2. Η αναγνώριση κινητής τηλεφωνίας ως βασικός μοχλός για ψηφιακής επικοινωνίας	Ενεργοποίηση ψηφιακής διαχείρισης μέσω κινητού
ΣΟΥΗΔΙΑ	1. Δημιουργία μιας κεντρικής κυβερνητικής πύλης μέσω της οποίας πολίτες και επιχειρήσεις μπορούν να έχουν πρόσβαση σε όλες τις διαδικτυακές δημόσιες υπηρεσίες και να συλλέγουν κάθε είδους δημόσια πληροφορία 2. Παροχή εγγράφων eIDs στους πολίτες ώστε που μπορούν να χρησιμοποιηθούν σε όλα τα πλαίσια 3. Εγγύηση ηλεκτρονικής ταυτότητας σε όποιον τη χρειάζεται 4. Εφαρμογή διασυνοριακής ηλεκτρονικής ταυτοποίησης	1. Δημιουργία κεντρικής πύλης ηλεκτρονικής διακυβέρνησης και eID για οργανισμούς 2. Επέκταση περιπτώσεων / δυνατοτήτων χρήσης eID 3. Αύξηση της διάδοσης του eID 4. Διασυνοριακή αναγνώριση eID

ΓΕΡΜΑΝΙΑ	1. Ανοίγοντας το δρόμο για τη διεθνή εφαρμογή της ηλεκτρονικής αναγνώρισης, θέτοντας τα πρότυπα για ασφαλείς και αξιόπιστες ηλεκτρονικές συναλλαγές σε όλη την ΕΕ 2. Ομοσπονδιακές, πολιτειακές και τοπικές κυβερνήσεις να προσφέρουν τις διοικητικές τους υπηρεσίες ψηφιακά έως το 2022 3. Εφαρμογή λειτουργιών έξυπνης κάρτας σε κινητά τηλέφωνα π.χ. λειτουργία ηλεκτρονικής ταυτότητας 4. Εισαγάγετε μια κάρτα eID για χρήση από πολίτες της ΕΕ και μέλη του Ευρωπαϊκού Οικονομικού Χώρου (σε αντίθεση με την απλή) αυξάνοντας έτσι τον πληθυσμό που μπορεί να έχει πρόσβαση σε λύσεις eID στη Γερμανία 5. Συμμετοχή της βιομηχανίας στην εμπορική χρήση της λειτουργίας eID 6. Διευκολύνει τη χρήση της λειτουργίας eID, π.χ. βελτιστοποίηση της διαδικασίας επαναφοράς PIN και χρήση σε εταιρικά δίκτυα	1. Διασυνοριακή αναγνώριση eID 2. Επέκταση περιπτώσεων χρήσης eID 3. Κινητή ταυτότητα 4. Αύξηση της διάδοσης του eID 5. eID για επιχειρήσεις 6. Επέκταση περιπτώσεων / δυνατοτήτων χρήσης eID

Γράφημα 11: *Στρατηγικές και Στόχοι eID*

5.1.2. ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΥΡΩΠΑΙΚΩΝ ΧΩΡΩΝ

5.1.2.1. Εσθονία

Η Εσθονία είναι μία από τις πιο ψηφιοποιημένες Ευρωπαϊκές χώρες διαθέτοντας ένα εξελιγμένο εθνικό δελτίο ταυτότητας στον κόσμο. Η ψηφιακή ατζέντα 2020 για την Εσθονία, συνοψίζει όλους τους στόχους για μία ψηφιακή κοινωνία και επικεντρώνεται στην χρήση των τεχνολογιών πληροφορικής και επικοινωνιών για την ανάπτυξη έξυπνων λύσεων. Το 2020 δημοσιεύθηκε από το υπουργείο εσωτερικών το νέο σχέδιο ανάπτυξης εσωτερικής ασφαλείας 2020 έως 2030. Σύμφωνα με το σχέδιο μέχρι το 2030 η Εσθονία θα πρέπει να θεωρηθεί ως παγκόσμιος ηγέτης στην έκδοση ασφαλών ψηφιακών εγγράφων, λαμβάνοντας υπόψη τις ανάγκες διασφάλισης της δημόσιας και εθνικής ασφάλειας. Για την διασφάλιση των παραπάνω στόχων ακολουθείτε μία σειρά από δράσεις όπως η ασφαλής ταυτοποίηση των πολιτών, φιλικές προς τους χρήστες τεχνολογικές λύσεις, χρηστικότητα ηλεκτρονικής ταυτότητας, πρόληψη απειλών και κινδύνων, συνεργασία δημοσίου και ιδιωτικού τομέα σε επικίνδυνες καταστάσεις.

Περισσότερες από 2.600 δημόσιες υπηρεσίες είναι διαθέσιμες στο διαδίκτυο χάρη στην εφαρμογή της ηλεκτρονικής ταυτοποίησης των πολιτών μέσω της ψηφιακής ταυτότητας, η οποία έχει τη μορφή smart card ως απόδειξη ηλεκτρονικής ταυτότητας σε οποιοδήποτε ηλεκτρονικό περιβάλλον, η οποία μπορεί να χρησιμοποιηθεί για ψηφιακές υπογραφές πρόσβασης, ηλεκτρονική ψηφοφορία, συναλλαγές λογαριασμών, πρόσβαση σε υπηρεσίες υγειονομικής

περίθαλψης κλπ. (E-estonia, 2017). Ειδικότερα είναι διαθέσιμα τέσσερα συστήματα ηλεκτρονικής ταυτοποίησης των ατόμων (Eestonia, 2017):

• ID card: αποτελεί παραδοσιακή μορφή έξυπνης κάρτας με ενσωματωμένο μικροεπεξεργαστή που χρησιμοποιείται για τους λόγους που αναφέρθηκαν παραπάνω. Υπολογίζεται πως το 98% των πολιτών της Εσθονίας χρησιμοποιούν τη σχετική έξυπνη κάρτα.

• Mobile-ID: επιτρέπει στους χρήστες να χρησιμοποιούν ένα κινητό τηλέφωνο ως μέσο ασφαλούς ψηφιακής ταυτοποίησης σε ηλεκτρονικές υπηρεσίες και εφαρμογή ψηφιακής υπογραφής σε έγγραφα, χωρίς τον αναγνώστη καρτών. Τα ιδιωτικά κλειδιά αποθηκεύονται στην κάρτα SIM μαζί με μια μικρή εφαρμογή που παρέχει τις λειτουργίες ελέγχου ταυτότητας και ψηφιακή υπογραφής. Περίπου το 12.2% των ψηφοφόρων στις ηλεκτρονικές εκλογές στην Εσθονία χρησιμοποιούν το Mobile-ID

• e-Residency: παρέχει τη δυνατότητα σε όλους τους ανθρώπους του κόσμου να αποκτήσουνε τη σχετική διακρατική ηλεκτρονική ταυτότητα κατοίκου της Εσθονίας. Οι πολίτες έχουν πρόσβαση στο επιχειρηματικό περιβάλλον της ΕΕ και μπορούν να χρησιμοποιούν δημόσιες ηλεκτρονικές υπηρεσίες με χρήση της ψηφιακής τους ταυτότητας. Άτομα από 138 χώρες έχουν υποβάλει αίτηση για τη σχετική διακρατική ηλεκτρονική ταυτότητα μέχρι το 2017.

• Smart ID: αποτελεί μια εφαρμογή για κινητά που λειτουργεί ως λύση ταυτοποίησης για όσους δεν διαθέτουν κάρτα SIM στην έξυπνη συσκευή τους, αλλά χρειάζεται να αποδείξουν με ασφάλεια την ηλεκτρονική τους ταυτότητα. Για τη χρήση της Smart-ID, απαιτείται μονάχα πρόσβαση σε ασύρματο δίκτυο, χωρίς απαίτηση περιαγωγής δεδομένων ή ειδικές κάρτες SIM.

5.1.2.2. Ισπανία

Η Ισπανία, συμμορφώνεται με τον Κανονισμό της ΕΕ, και επρόκειτο να κυκλοφορήσει Βιομετρικές Ταυτότητες το 2021, που θα περιέχουν το όνομα χρήστη και τον κωδικό πρόσβασης, ενσωματωμένοι στην πλατφόρμα Cl@ve. Ο Νόμος 39/2015 (1 Οκτωβρίου 2015) της Κοινής Διοικητικής Διαδικασίας Δημοσίων Διοικήσεων, ορίζει στο άρθρο 9 τις διαθέσιμες επιλογές ταυτοποίησης για την απόδειξη της ταυτότητάς τους από τους πολίτες. Πιο πρόσφατα, η «Ψηφιακή Ατζέντα 2025» που εφαρμόστηκε από το Υπουργείο Οικονομικών και Ψηφιακού Μετασχηματισμού το 2020, επισήμανε την ανάγκη προώθησης της χρήσης ψηφιακών υπηρεσιών, ιδίως όσον αφορά την ασφαλή ψηφιακή ταυτότητα, ώστε οποιοσδήποτε στην επικράτεια να έχει πρόσβαση σε αυτές τις υπηρεσίες.

Τα ηλεκτρονικά δελτία ταυτότητας στην Ισπανία ονομάζονται “Documento Nacional de Identidad electronic” (DNIe) και είναι διαθέσιμα στους πολίτες της χώρας από το 2006. Το DNIe ικανοποιεί τις σχετικές προϋποθέσεις που θέτει η οδηγία της ΕΕ για την ηλεκτρονική ταυτότητα και αποτελεί μια έξυπνη ταυτότητα, όπου ο ενσωματωμένος μικροεπεξεργαστής περιέχει πιστοποιητικά για την εξακρίβωση της γνησιότητας και την εφαρμογή ψηφιακής υπογραφής. Εκτός από τις σχετικές ορατές πληροφορίες, η κάρτα ηλεκτρονικής ταυτότητας περιλαμβάνει επίσης ένα μικροεπεξεργαστή-τσιπ. Το τσιπ περιέχει επιπρόσθετα προσωπικά στοιχεία του κατόχου της κάρτας, όπως φωτογραφία, χειρόγραφη υπογραφή και δακτυλικά αποτυπώματα.

Επιπλέον, το τσιπ περιλαμβάνει τρία πιστοποιητικά με τα ιδιωτικά κλειδιά τους και τον αντίστοιχο κωδικό πρόσβασής τους (PIN).

Ένα άλλο διαθέσιμο μέσο eID είναι το Cl@ve, μια πλατφόρμα αναγνώρισης, επαλήθευσης ταυτότητας και ηλεκτρονικής υπογραφής, συμπληρώνοντας τα ήδη υπάρχοντα μέσα eID για πρόσβαση σε διαδικτυακές δημόσιες υπηρεσίες. Εν τω μεταξύ, περισσότεροι από 7.600 οργανισμοί έχουν ενσωματώσει το Cl@ve ως μέσο ελέγχου ταυτότητας στον ιστότοπό τους παρέχοντας διαδικτυακές υπηρεσίες.

5.1.2.3. Πορτογαλία

Το έγγραφο, Estrategia TIC 2020 "Estratégia para a Transformação Digital na Administração pública» καθορίζει το όραμα της κυβέρνησης για την εφαρμογή των ΤΠΕ στη δημόσια διοίκηση, δηλώνοντας τη φιλοδοξία να διασφαλιστεί ότι οι πληροφορίες είναι διαθέσιμες μέσω ενός μόνο σημείου και παράλληλα καθορίζει μια σειρά δράσεων για την ανάπτυξη και χρήση της ψηφιακής ταυτότητας. Η ψηφιακή ταυτότητα αναφέρεται επίσης ως ένα από τα μέτρα στο πρόγραμμα Simplex+ της Πορτογαλίας. Αυτό το πρόγραμμα εφαρμόζεται από το 2016 και στοχεύει «να διασφαλίσει ότι η Δημόσια Διοίκηση παρέχει γρήγορες και αποτελεσματικές ανταποκρίσεις στις ανάγκες των ανθρώπων και των επιχειρήσεων».

Αυτήν τη στιγμή, τρία μέσα eID είναι διαθέσιμα στην Πορτογαλία:

• The Cartão de Cidadão: το εθνικό δελτίο ταυτότητας με λειτουργία ηλεκτρονικής ταυτοποίησης. Κοινοποιήθηκε για διασυνοριακή χρήση βάσει του κανονισμού eIDAS το 2019.

• Το Sistema de Certificação de Atributos Profissionais: είναι ένα σύστημα πιστοποίησης που επιτρέπει στους πολίτες να πιστοποιούν την αυθεντικότητά τους και να υπογράφουν έγγραφα με τους ρόλους τους ως επαγγελματίες. Προειδοποιήθηκε για διασυνοριακή χρήση βάσει του κανονισμού eIDAS το 2018.

• Το Chave Móvel Digital (Digital Mobile Key): δημιουργήθηκε το 2017 υπό την εποπτεία του Οργανισμού Διοικητικού Εκσυγχρονισμού. Ειδοποιήθηκε για διασυνοριακή χρήση τον Απρίλιο του 2020. Δίνει τη δυνατότητα στους πολίτες να επαληθεύουν την ταυτότητά τους χρησιμοποιώντας κινητό τηλέφωνο (με κωδικό επιβεβαίωσης που αποστέλλεται στον αριθμό τηλεφώνου). Παρέχει επίσης λειτουργία eSignature.

5.1.2.4. Βέλγιο

Το Βέλγιο ήταν μία από τις πρώτες χώρες στον κόσμο που εφάρμοσε την ηλεκτρονική ταυτότητα σε εθνικό επίπεδο. Για να το πετύχει αυτό ανέπτυξε ένα πλαίσιο από μία σειρά νομοθετικών μέτρων με συνεχή εξέλιξη. Το πιο πρόσφατο νομοθετικό μέτρο που εγκρίθηκε είναι ο βέλγικος νόμος για την ηλεκτρονική ταυτοποίηση στις 18 Ιουλίου του 2017 που συμπληρώνει τον κανονισμό eidas. Ορίζει ότι οι δημόσιοι πάροχοι και η εξωτερική ιδιωτική μπορούν να συνεργαστούν για την ανάπτυξη και τη λειτουργία μέσων ηλεκτρονικής αναγνώρισης για πρόσβαση σε δημόσιες υπηρεσίες.

Συνολικά στο Βέλγιο μέχρι σήμερα υπάρχουν διαθέσιμες τρεις κάρτες για την ηλεκτρονική ταυτοποίηση πολιτών της χώρας (Gemalto, 2017a):

- Η εθνική κάρτα ταυτότητας (national ID card): περιέχει δύο πιστοποιητικά, το ένα για έλεγχο ταυτότητας και το άλλο για την εφαρμογή ηλεκτρονικής υπογραφής. Απεικονίζει το πορτρέτο του πολίτη με το όνομα και το επώνυμο του, την ημερομηνία και τον τόπο γέννησης, το φύλο, την εθνικότητα, τον αριθμό ταυτότητας, την υπογραφή και τον αριθμό εθνικού μητρώου (μοναδικός αριθμός αναγνώρισης που δίνεται κατά τη γέννηση ενός πολίτη στο Βέλγιο) και τον τόπο έκδοσής της. Η σχετική κάρτα χορηγείται στους πολίτες του Βελγίου σε ηλικία από 15 ετών με επιβάρυνση 25 ευρώ.
- Κάρτα παραμονής (Residence card): Με τη χρήση της αντίστοιχης κάρτας είναι δυνατή η ηλεκτρονική ταυτοποίηση των αλλοδαπών που κατοικούν στο Βέλγιο και η πρόσβασή τους σε υπηρεσίες ηλεκτρονικής διακυβέρνησης. Η κάρτα διατίθεται σε όλους τους αλλοδαπούς (εκτός ΕΕ ή Ελβετίας) που διαμένουν στο Βέλγιο. Το κόστος απόκτησης της σχετικής κάρτας είναι 15 ευρώ
- Η κάρτα παιδιών (kids e-ID): επιτρέπει την άμεση αναγνώριση των παιδιών στα 12 χρόνια τους, είτε εντός είτε και εκτός των βελγικών συνόρων. Αποτελεί μια ταυτότητα χρήσης για ανήλικους και ένα ασφαλές ταξιδιωτικό έγγραφο. Επίσης, η αντίστοιχη κάρτα επιτρέπει στα παιδιά να χρησιμοποιούν το διαδίκτυο με ασφαλέστερο τρόπο. Για το μέλλον σχεδιάζονται και άλλες χρήσεις της, όπως για παράδειγμα η εγγραφή στο σχολείο, στις πισίνες και στις βιβλιοθήκες με χρήση της αντίστοιχης κάρτας. Επιπροσθέτως, υπάρχει υπηρεσία έκτακτης ανάγκης, η οποία συνδέεται με τη χρήση της κάρτα Kids-e-ID. Μια ειδοποίηση μπορεί να σταλεί σε περίπτωση που το παιδί έχει πρόβλημα ή βρίσκεται σε κίνδυνο. Το κόστος απόκτησης της κάρτας είναι περίπου 10 ευρώ ανάλογα με την περιοχή κατοικίας ενός παιδιού. Ωστόσο, η χρήση της σχετικής κάρτας δεν είναι υποχρεωτική για τα παιδιά στο Βέλγιο.

5.1.2.5. Σουηδία

Η σουηδική στρατηγική ψηφιοποίησης «Για μια βιώσιμη ψηφιοποιημένη Σουηδία», εφαρμόστηκε από τα Κυβερνητικά Γραφεία το 2017 και έχει μια ενότητα αφιερωμένη στο eID. Σύμφωνα με τη στρατηγική, η ψηφιακή ταυτότητα είναι μια κοινωνικά κρίσιμη υποδομή και αποτελεί προϋπόθεση για τη συνεχή ανάπτυξη ψηφιακών υπηρεσιών για άτομα και εταιρείες. Δύο επιπλέον έργα είναι πολύ σχετικά με τα περαιτέρω ανάπτυξη του eID στη Σουηδία:

• The Nordic Mobility Action Program 2019 που περιλαμβάνει ένα ευρύ φάσμα έργων την εφαρμογή της διασυνοριακής ηλεκτρονικής ταυτοποίησης.

• The Nordic-Baltic eID Project (NOBID) 2018 που στοχεύει στην επιτάχυνση της εφαρμογής του eIDAS στις Σκανδιναβικές χώρες.

Η ηλεκτρονική ταυτοποίηση για τους πολίτες παρέχεται από τον ιδιωτικό τομέα και ειδικότερα από τις τράπεζες (BankID). Ο δημόσιος τομέας χρησιμοποιεί την πιστοποίηση που παρέχεται από τους ιδιωτικούς παρόχους ηλεκτρονικής ταυτοποίησης σε μια εμπορική βάση συνεργασίας (Hansteen et al., 2016). Η κάρτα μπορεί να χρησιμοποιηθεί παράλληλα ως μέσο ηλεκτρονικής ταυτοποίησης και ως μέσο εφαρμογής ψηφιακής υπογραφής (BankID, 2017). Η ηλεκτρονική ταυτοποίηση στη Σουηδία θεωρείται επιτυχημένη με πάνω από 7,5 εκατομμύρια από τους 9 εκατομμύρια πολίτες της χώρας να κατέχουν ηλεκτρονική ταυτότητα και να έχουν

πραγματοποιήσει ενδεικτικά πάνω από 250 εκατομμύρια συναλλαγές σε διάφορες ιδιωτικές και δημόσιες ηλεκτρονικές υπηρεσίες.

Αντίστοιχα, η Σουηδική κάρτα ηλεκτρονικού διαβατηρίου που εκδίδεται από το κράτος θεωρείται ένα από τα πιο ασφαλή ταξιδιωτικά έγγραφα στον κόσμο. Σύμφωνα με την εφημερίδα "The Independent" του Ηνωμένου Βασιλείου (8 Μαΐου 2017), το Σουηδικό ηλεκτρονικό διαβατήριο κατατάσσεται στην πρώτη θέση ως το πιο επιθυμητό διαβατήριο σε παγκόσμιο επίπεδο. Οι παράγοντες που έχουν οδηγήσει στη σχετική εκτίμηση είναι η δυνατότητα χρήσης του ως ταξιδιωτικό έγγραφο χωρίς την απαίτηση VISA και οι υψηλές προδιαγραφές ασφάλειάς που εκείνο διαθέτει (Gemalto, 2017d).

5.1.2.6. Γερμανία

Η στρατηγική της Γερμανίας που δημοσιεύτηκε το 2013 από το υπουργείο εσωτερικών είχε ως στόχο την παροχή μιας ολοκληρωμένης σειράς ασφαλών διαδικασιών που εγγυώνται την ταυτοποίηση, τη γνησιότητα, την ακεραιότητα, την εμπιστευτικότητα και την επαλήθευση σε ηλεκτρονικές συναλλαγές που χρησιμοποιούνται από πολίτες, εταιρείες και τη διοίκηση. Συγκεκριμένα η στρατηγική επισήμανε τρία σημεία, την αποδοχή και την χρήση ηλεκτρονικής ταυτότητας, την ασφάλεια ανάλογα με τις απαιτήσεις της υπηρεσίας κυρίως όσον αφορά τα κομμάτια της αυθεντικοποίησης, της τακτοποίησης, της ακεραιότητας, της επιθετικότητας και της επαλήθευσης, καθώς και την <<οικονομία>> χρησιμοποιώντας σε λίγο χρόνο και με λίγη προσπάθεια δημόσιες υπηρεσίες μέσω διαδικτύου. Η πιο πρόσφατη στρατηγική, η ψηφιακή στρατηγική 2025, αναφέρει το eid αναφερόμενη στην ενίσχυση ασφαλείας δεδομένων, τονίζοντας ότι η χώρα ανοίγει δρόμο για τη διεθνή εφαρμογή ηλεκτρονικής αναγνώρισης, με βάση τα πρότυπα της ευρωπαϊκής ένωσης για ασφαλείς και αξιόπιστες ηλεκτρονικές συναλλαγές.

Η γερμανική ηλεκτρονική κάρτα ταυτότητας βασίζεται σε έξυπνες κάρτες με που έχουν εκδοθεί από την κυβέρνηση (με τη χρήση ισχυρών κρυπτογραφικών πρωτόκολλων). Σήμερα είναι διαθέσιμοι δυο τύποι ηλεκτρονικής κάρτας ταυτότητας (German Federal Office for Information Security, 2017):

- Γερμανικά δελτία ταυτότητας (Personalausweis): χορηγούνται σε γερμανούς υπηκόους που κατοικούν στη Γερμανία ή ζουν στο εξωτερικό.

- Άδειες διαμονής στη Γερμανία (Aufenthaltstitel): χορηγούνται σε υπηκόους τρίτων χωρών που κατοικούν στη Γερμανία

Η κάρτα ηλεκτρονικής ταυτότητας χρησιμοποιεί δύο παράγοντες επαλήθευσης ταυτότητας για έλεγχο ταυτότητας, "κατοχή" (έξυπνη κάρτα) και "γνώση" (6 ψήφιο PIN). Ο μικροεπεξεργαστής της ηλεκτρονικής κάρτας ταυτότητας αποθηκεύει τα προσωπικά δεδομένα και τα σχετικά κλειδιά για να ενεργοποιήσει τον έλεγχο ταυτότητας. Το PIN πρέπει να εισαχθεί από τον κάτοχο της κάρτας για να ξεκινήσει η διαδικασία ελέγχου ταυτότητας. Επιπλέον, το PIN χρησιμεύει για να εκφράσει τη συγκατάθεση του κατόχου για τον έλεγχο ταυτότητας (German Federal Office for Information Security, 2017).

Η γερμανική ηλεκτρονική κάρτα ταυτότητας ικανοποιεί όλες τις απαιτήσεις του υψηλού επιπέδου αξιοπιστίας e-IDAS. Η ασφάλεια των τεχνολογιών πληροφορικής, καθώς και τα ζητήματα προστασίας δεδομένων, η χρηστικότητα και η ευκολία ενσωμάτωσης αποτελούν την κεντρική βάση για το σχεδιασμό ολόκληρου του γερμανικού συστήματος ηλεκτρονικής ταυτοποίησης.

5.1.2.7. Ελλάδα

Ενώ δεν υπάρχει συγκεκριμένο έγγραφο στρατηγικής eID η Ελλάδα υιοθέτησε το 2016 μία Εθνική Ψηφιακή Στρατηγική για την περίοδο 2016 έως 2021 συμπεριλαμβάνοντας μία ολόκληρη ενότητα αφιερωμένη στις δημόσιες υπηρεσίες. Σε αυτή την ενότητα αναφέρεται το eid και επισημαίνεται η ανάγκη ευθυγράμμισης με τον κανονισμό. Σε συμμόρφωση με αυτό, το άρθρο 23 του νόμου 4647 16/10/2019, που τροποποιεί και συμπληρώνει το άρθρο 3 του νόμου 1599/1986, αναφέρει ότι το δελτίο ταυτότητας περιλαμβάνει ηλεκτρονική αποθήκευση της φωτογραφίας του κατόχου σε ψηφιακή μορφή δύο δακτυλικά αποτυπώματα και εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής σύμφωνα με το άρθρο 3 του κανονισμού της ευρωπαϊκής Ένωσης 9/10 κάθετος 2014.

Επί του παρόντος δεν υπάρχουν διαθέσιμα μέσα eID πλήρους κλίμακας στην Ελλάδα. Περιορισμένος ο αριθμός των καρτών eid Ερμής, διατίθεται από το 2018 σε δημοσίους υπαλλήλους και εταιρείες του ιδιωτικού τομέα. Αυτές οι κάρτες ενεργοποιούν την πρόσβαση στην πύλη Ερμής. Έχει εκδοθεί σε 75 χιλιάδες πολίτες και 165 επιχειρήσεις, με σκοπό την παροχή ολοκληρωμένης ηλεκτρονικής διακυβέρνησης. Ο κατάλογος των υπηρεσιών στην οποία στις οποίες έχουν πρόσβαση πολίτες περιλαμβάνει την άμυνα, εκπαίδευση, περιβάλλον, υγεία, ασφάλεια, εργασία.

ΧΩΡΑ	**ΛΥΣΗ**	**ΠΟΣΟΣΤΟ ΧΡΗΣΗΣ ΤΗΣ ΛΥΣΗΣ**	**ΠΑΡΟΧΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ**	**ΕΠΙΠΕΔΟ ΔΙΑΣΦΑΛΙΣΗΣ**	**ΧΡΗΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ**	**ΧΡΗΣΗ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ**	**ΧΡΗΣΗ ΒΙΟΜΕΤΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ**	**ΧΡΗΣΗ ΚΙΝΗΤΟΥ ΤΗΛΕΦΩΝΟΥ**	**ΣΧΕΔΙΑΣΜΟΣ ΕΝΕΡΓΕΙΩΝ ΓΙΑ ΤΗΝ ΑΥΞΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ**
ΕΣΘΟΝΙΑ	ID-card Mobile-ID e-Residency Smart-ID	98%	Δημόσιος Τομέας	Υψηλό	X	X		X	παρακολουθεί συνεχώς τους κινδύνους ασφάλειας απαιτεί καλή συνεργασία μεταξύ διαφορετικών χωρών, κρατών μελών της ΕΕ και εθνικούς εταίρους.

ΙΣΠΑΝΙΑ	DNIe Cl@ve	Υποχρεωτική πάνω από 44 εκατομμύρια	Δημόσιος Τομέας	Υψηλό	X	X			Δεν έχουν εντοπιστεί σχέδια για τη λήψη συγκεκριμένων μέτρων για τη διασφάλιση της συμμόρφωσης με τον Κανονισμό (ΕΕ) 2019/1157
ΠΟΡΤΟΓΑΛΙΑ	- Cartão de Cidadão Português -Sistema de Certificação de Atributos Profissionais -Chave Móvel Digital (Digital Mobile Key)	Υποχρεωτική κ	Δημόσιος Τομέας	Υψηλό	X	X	X	X	Δεν έχουν εντοπιστεί σχέδια για τη λήψη συγκεκριμένων μέτρων για τη διασφάλιση της συμμόρφωσης με τον Κανονισμό (ΕΕ) 2019/1157
ΒΕΛΓΙΟ	-national ID card -residence card -kids e-ID	Υποχρεωτική Για τις εθνικές κάρτες, πάνω από 28 εκατομμύρια. Για το ITSME, το 24,5 % του συνολικού πληθυσμού μέχρι το 2020	Δημόσιος Τομέας	Υψηλό	X	X			δακτυλικά αποτυπώματα, επιτρέποντας στο Βέλγιο να συμμορφώνονται με τον νέο Κανονισμό (ΕΕ) 2019/1157
ΣΟΥΗΔΙΑ	BankID	80%	Ιδιωτικός Τομέας	Υψηλό		X	X	X	Υπάρχει πρόταση για νέα Σουηδική Εθνική ταυτότητα με εθνικό eID (Έκθεση SOU 2019:14) με στόχο την αύξηση της

									ασφάλειας των δελτίων ταυτότητας
ΓΕΡΜΑΝΙΑ	Personalausweis Aufenthaltstitel	Υποχρεωτική 7,5 εκατομμύρια	Δημόσιος Τομέας	Υψηλό	X	X	X	X	Δεδομένου ότι το γερμανικό δελτίο ταυτότητας είναι ήδη αναγνωρίσιμο και έχει τα απαραίτητα φυσικά χαρακτηριστικά ασφαλείας σύμφωνα με το πρότυπο ICAO 9303, οι αλλαγές θα περιοριστούν κυρίως στον σχεδιασμό και στις ελάχιστες προσαρμογές στα πρωτόκολλα πρόσβασης για την ανάγνωση των δεδομένων της ταυτότητας.

***Πηγή*:** Union, Publications Office of the European, 18 Δεκέμβριος 2019

***Πηγή*:** Ευρωπαϊκή Επιτροπή, Επισκόπηση των στρατηγικών eID των κρατών μελών, 2020

Γράφημα 12: *Σύγκριση μεθόδων eID*

5.2. ΣΥΓΚΡΙΣΗ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Σύμφωνα με όσα αναφέρθηκαν σε προηγούμενες ενότητες ο ψηφιακός μετασχηματισμός ενισχύει την αλλαγή του τρόπου με τον οποίο το κράτος εξυπηρετεί τους πολίτες, σχεδιάζει διαδικασίες, υλοποιεί δράσεις και λύνει προβλήματα. Η Ελλάδα κατατάσσεται σε χαμηλή θέση στους διεθνείς δείκτες που αξιολογούν την ψηφιακή ωριμότητα των χωρών ανά τον κόσμο. Για παράδειγμα, στο Δείκτη Ψηφιακής Οικονομίας και Κοινωνίας (Digital Economy and Society Index, DESI)1 η χώρα κατατάσσεται στην 27η θέση μεταξύ των 28 χωρών της ΕΕ για το 2020, στο Δείκτη Ανάπτυξης Ηλεκτρονικής Διακυβέρνησης (E-Government Development Index, EGDI)2 στην 42η θέση μεταξύ των 193 κρατών της έρευνας για το 2020, κατέχοντας τη 27η θέση ανάμεσα στις 28 χώρες της ΕΕ, στο Δείκτη Ανάπτυξης ΤΠΕ (ICT Development Index, IDI)3 η χώρα μας κατατάσσεται 38η μεταξύ 192 κρατών για το 2017 και 25η ανάμεσα στις χώρες της ΕΕ, στο Δείκτη Ψηφιακής Εξέλιξης (Digital Evolution Index, DEI)4 η Ελλάδα βρίσκεται στην 38η θέση μεταξύ των 60 υπό έρευνα κρατών για το 2017, ενώ στο δείκτη Διευκόλυνσης της Ψηφιοποίησης (Enabling Digitalization Index - EDI)5 η Ελλάδα κατατάσσεται 43η μεταξύ 115 κρατών για το 2019 (Υπουργείο Ψηφιακής Διακυβέρνησης, 2021).

Με δεδομένη τη χαμηλή ψηφιακή επίδοση, η Ελλάδα στερείται πλέον πολύτιμου χρόνου, ώστε να εφαρμόσει σταδιακές και «εξελικτικές» ψηφιακές στρατηγικές, όπως έπραξαν άλλες,

ψηφιακά ανεπτυγμένες σήμερα, χώρες (π.χ., η Νορβηγία, η Φινλανδία, το Ηνωμένο Βασίλειο, κ.ά.). Οι χώρες αυτές ξεκίνησαν τον ψηφιακό μετασχηματισμό τους πριν από αρκετά χρόνια, όσο ο ρυθμός των τεχνολογικών εξελίξεων ήταν ακόμα χαμηλός, εφαρμόζοντας σταδιακά βήματα, τα οποία επαναπροσδιορίζονταν ανά τακτά χρονικά διαστήματα, ώστε να ανταποκρίνονται στους μεταβαλλόμενους εθνικούς τους στόχους και να ενσωματώνουν τις αναδυόμενες ψηφιακές τεχνολογίες.

Το Γράφημα που ακολουθεί παρουσιάζει τον ρυθμό ψηφιακού μετασχηματισμού της Ελλάδας σε σχέση με άλλες ευρωπαϊκές χώρες. Όπως φαίνεται στο Γράφημα οι ψηφιακά ανεπτυγμένες χώρες έχουν ήδη ακολουθήσει μια διαδρομή (j-lift) για να πραγματοποιήσουν τον ψηφιακό μετασχηματισμό τους. Αντίθετα, όπως φαίνεται η Ελλάδα δεν έχει ακολουθήσει αντίστοιχο μονομάτι με αποτέλεσμα να πρέπει να ακολουθήσει μια αντίστοιχη διαδικασία (i- lift) ώστε αφενός να επιτύχει ψηφιακό μετασχηματισμό και αφετέρου να τον πετύχει άμεσα.

Γράγημα 13: *Ο ρυθμός ψηφιακού μετασχηματισμού της Ελλάδας σε σχέση με άλλες ευρωπαϊκές*

Πηγή: Ο ρυθμός ψηφιακού μετασχηματισμού της Ελλάδας σε σχέση με άλλες ευρωπαϊκές χώρες (Μελέτη ΣΕΒ- Accenture – Η Ψηφιακή Ελλάδα, 2017)

Η ραγδαία ταχύτητα των τεχνολογικών αλλαγών, σε συνδυασμό με τη χαμηλή ψηφιακή ωριμότητα της Ελλάδας, δημιουργεί την επιτακτική ανάγκη για τη χώρα να ενεργήσει άμεσα, σε πολλαπλούς άξονες, συγχρονισμένα και σε περιορισμένο χρονικό ορίζοντα, μέσω της υλοποίησης μιας «ολιστικής» ψηφιακής προσέγγισης. Ήδη έχουν γίνει βήματα προς αυτή την κατεύθυνση, όπως, για παράδειγμα, οι σημαντικές τεχνολογικές λύσεις που αναπτύχθηκαν με πολύ γρήγορους ρυθμούς από το Υπουργείο Ψηφιακής Διακυβέρνησης για την αντιμετώπιση των συνεπειών της πανδημίας του κορονοϊού. Μόνο μέσα από μία τέτοια άμεση, συντονισμένη

και οργανωμένη προσέγγιση θα καταφέρει η Ελλάδα να επιταχύνει τον ψηφιακό μετασχηματισμό της, βελτιώνοντας έτσι και τη θέση της σε δείκτες σχετικούς με την τεχνολογία και την καινοτομία (Υπουργείο Ψηφιακής Διακυβέρνησης, 2021).

ΚΕΦΑΛΑΙΟ 6: ΠΡΟΤΑΣΕΙΣ ΚΑΙ ΤΡΟΠΟΙ ΒΕΛΤΙΩΣΗΣ

6.1 Αναθεώρηση του ρυθμιστικού πλαισίου eIDAS

Η Ευρωπαϊκή Επιτροπή αξιολογεί επί του παρόντος αυτό το ρυθμιστικό πλαίσιο και διεξήγαγε ανοιχτή διαβούλευση από τις 24 Ιουλίου έως τις 2 Οκτωβρίου 2020, σχετικά με την αναθεώρηση των κανόνων για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.
(http://data.europa.eu/eli/reg/2014/910/oj/eng)

Η αντιπρόεδρος Margrethe Vestager είπε: <<Αυτοί οι κανόνες διευκολύνουν την πρόσβαση των πολιτών στις δημόσιες υπηρεσίες χρησιμοποιώντας ηλεκτρονική αναγνώριση, όπως οι ηλεκτρονικές υπογραφές. Η αναθεώρηση στοχεύει να βελτιώσει την αποτελεσματικότητά της, να επεκτείνει τα οφέλη της στον ιδιωτικό τομέα και να προωθήσει αξιόπιστες ψηφιακές ταυτότητες για όλους τους Ευρωπαίους και να δημιουργήσει μια ασφαλή και διαλειτουργική Ευρωπαϊκή Ψηφιακή Ταυτότητα που δίνει στους πολίτες έλεγχο.>> Ενώ ο επίτροπος για την εσωτερική αγορά, Thierry Breton, πρόσθεσε: <<Η δραστηριότητα πολιτών και επιχειρήσεων αυξήθηκε κατά τη διάρκεια της πανδημίας, η αναθεώρηση αυτών των κανόνων θα ανταποκριθεί στην αυξανόμενη ανάγκη τους για απλό, αξιόπιστο και ασφαλή τρόπο αναγνώρισης του εαυτού τους στο διαδίκτυο. Η βελτίωση αυτών των κανόνων θα παράσχει επίσης το πλαίσιο για την προσφορά ανταγωνιστικών και αξιόπιστων υπηρεσιών ψηφιακής ταυτότητας.>>

Ωστόσο, πολλά έχουν αλλάξει από την έκδοση του κανονισμού eIDAS το 2014. Το πλαίσιο βασίζεται σε εθνικά συστήματα ηλεκτρονικής ταυτοποίησης που ακολουθούν διαφορετικά πρότυπα και επικεντρώνεται σε ένα σχετικά μικρό τμήμα των αναγκών των πολιτών και των επιχειρήσεων όσον αφορά την ηλεκτρονική ταυτοποίηση: στην ασφαλή διασυνοριακή πρόσβαση στις δημόσιες υπηρεσίες. Έκτοτε, η ψηφιοποίηση όλων των λειτουργιών της κοινωνίας έχει αυξηθεί θεαματικά. Η πανδημία COVID-19, μεταξύ άλλων, είχε πολύ ισχυρό αντίκτυπο στην ταχύτητα της ψηφιοποίησης. Ως αποτέλεσμα, τόσο δημόσιες όσο και ιδιωτικές υπηρεσίες παρέχονται όλο και περισσότερο ψηφιακά. Οι προσδοκίες των πολιτών και των επιχειρήσεων περιλαμβάνουν την επίτευξη υψηλής ασφάλειας και ευκολίας για κάθε επιγραμμική δραστηριότητα, όπως η υποβολή φορολογικών δηλώσεων, το άνοιγμα τραπεζικού λογαριασμού η αίτηση για λήψη δανείου εξ αποστάσεως, η ενοικίαση αυτοκινήτου, και άλλα. Κατά συνέπεια, η ζήτηση για μέσα ταυτοποίησης και επαλήθευσης της ταυτότητας επιγραμμικά, καθώς και για ψηφιακή ανταλλαγή πληροφοριών που αφορούν την ταυτότητα, τα χαρακτηριστικά ή τα προσόντα με ασφάλεια και υψηλό επίπεδο προστασίας των δεδομένων, έχει αυξηθεί. Η αύξηση αυτή πυροδότησε μια στροφή προς προηγμένες και εύκολες λύσεις που μπορούν να ενσωματώνουν διάφορα επαληθεύσιμα δεδομένα και πιστοποιητικά του χρήστη.

Σήμερα, η ζήτηση αυτή δεν μπορεί να ικανοποιηθεί από τα μέσα ηλεκτρονικής ταυτοποίησης και τις υπηρεσίες εμπιστοσύνης, όπως ρυθμίζονται από τον κανονισμό eIDAS, δεδομένων των

υφιστάμενων περιορισμών του. Τον Φεβρουάριο του 2020, η Επιτροπή, στη στρατηγική της για τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης , δεσμεύτηκε να προβεί σε αναθεώρηση του κανονισμού eIDAS με σκοπό τη βελτίωση της αποτελεσματικότητάς του, την επέκταση της εφαρμογής του στον ιδιωτικό τομέα και την προώθηση αξιόπιστων ψηφιακών ταυτοτήτων για όλους τους πολίτες και τις επιχειρήσεις της ΕΕ. Ο αναθεωρημένος και ενισχυμένος κανονισμός eIDAS θα είναι σε θέση να ανταποκριθεί στις νέες απαιτήσεις της αγοράς και της κοινωνίας, καλύπτοντας τις ανάγκες για αξιόπιστες λύσεις συνδεδεμένες με δημόσιες ηλεκτρονικές ταυτότητες, αλλά και για χαρακτηριστικά και διαπιστευτήρια που παρέχονται από τον δημόσιο και τον ιδιωτικό τομέα και τα οποία τελούν όλα υπό την πλήρη διαχείριση του χρήστη και αναγνωρίζονται σε ολόκληρη την ΕΕ για την πρόσβαση τόσο σε δημόσιες όσο και σε ιδιωτικές υπηρεσίες. Με τον τρόπο αυτόν θα υποστηριχθεί μεγάλος αριθμός υφιστάμενων ή προτεινόμενων κανονιστικών πλαισίων για την ενίσχυση της ενιαίας αγοράς της ΕΕ.(https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52021DC0290&from=EN)

6.1.1. Η μελέτη του ENISA

Η μελέτη του ENISA παρέχει μια επισκόπηση του τεχνολογικού τοπίου για τα συστήματα eID. Μια τέτοια επισκόπηση μπορεί να υποστηρίξει την ανάπτυξη ενός πλαισίου που θα λαμβάνει υπόψη ζητήματα ασφάλειας που απαιτούνται σε όλη τη διαδικασία ηλεκτρονικής ταυτοποίησης, συμπεριλαμβανομένης της φάσης εγγραφής, της διαχείρισης μέσων eID, του ελέγχου ταυτότητας και της διαχείρισης και οργάνωσης παρόχων. Επεξεργάζονται επίσης θέματα που αξίζει να αναπτυχθούν σε κατευθυντήριες γραμμές για τη διασφάλιση της ομοιογένειας και της συνέπειας σε όλη την Ευρώπη, συμπεριλαμβανομένης για παράδειγμα της απομακρυσμένης ταυτοποίησης (που είναι επίσης βασικό θέμα για υπηρεσίες εμπιστοσύνης), της ασφάλειας των λύσεων eID που βασίζονται σε κινητά, της χρήσης ενσωματωμένων smartphone σε βιομετρικούς αισθητήρες, και πλαισίων πιστοποίησης.

6.2 Νέες μέθοδοι και τεχνολογίες

Για να υπάρξει επέκταση της ψηφιακής ταυτοποίησης είναι προφανές ότι χρειάζεται να υπάρξει βελτίωση της τεχνολογίας και της νομοθεσίας όπου απαιτείται. Η ευκαιρία για δημιουργία αξίας μέσω της ψηφιακής ταυτοποίησης αυξάνεται καθώς η τεχνολογία βελτιώνεται, το κόστος υλοποίησης μειώνεται και η πρόσβαση σε smartphone και στο διαδίκτυο αυξάνεται καθημερινά. Η θεμελιώδης ψηφιακή υποδομή που υποστηρίζει την ψηφιακή ταυτότητα αυξάνεται καθημερινά σε εμβέλεια και μειώνεται το κόστος. Περισσότεροι από τέσσερα δισεκατομμύρια άνθρωποι έχουν αυτήν τη στιγμή πρόσβαση στο Διαδίκτυο και σχεδόν ένα τέταρτο του δισεκατομμυρίου νέοι χρήστες ήρθαν στο διαδίκτυο για πρώτη φορά το 2017. Η τεχνολογία που απαιτείται για την ψηφιακή ταυτότητα είναι πλέον έτοιμη και πιο προσιτή από ποτέ, δίνοντας τη δυνατότητα στις αναδυόμενες οικονομίες να ξεπεράσουν τις προσεγγίσεις που βασίζονται σε χαρτί για την ταυτοποίηση των πολιτών (Bujoreanu et al., 2018). Οι τεχνολογίες ελέγχου

ταυτότητας μπορούν να δώσουν ποσοστά ψευδούς αποδοχής έως και 0,2 τοις εκατό και ποσοστά ψευδούς απόρριψης 0,0001 (McKinsey Global Institute, 2019).

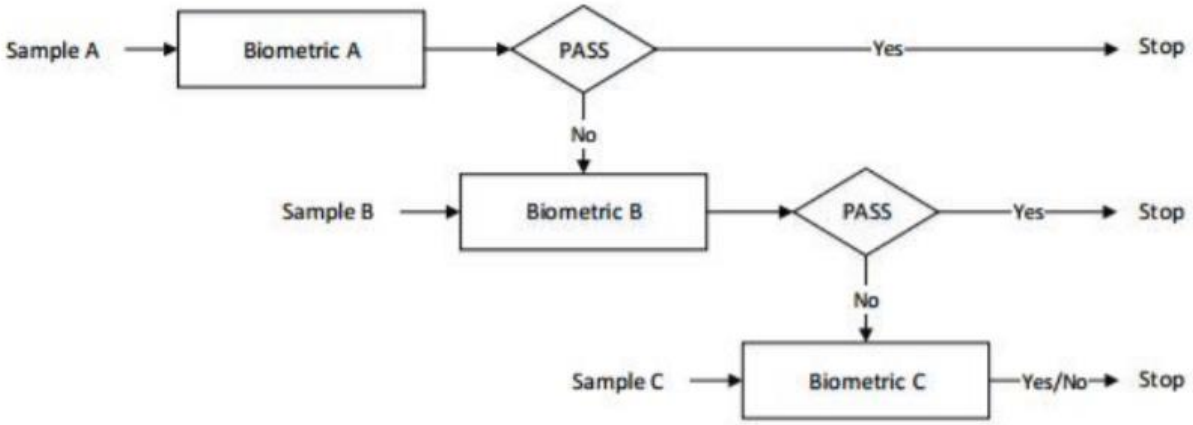
Οι νέες τεχνολογίες και τάσεις προσφέρουν ξεχωριστές ευκαιρίες για προσθήκη αξίας τόσο για τα άτομα όσο και για τους θεσμικούς παράγοντες. Καθώς οι άνθρωποι ζουν όλο και πιο ψηφιακά, οι εφαρμογές μηχανικής μάθησης και αλγοριθμικής ανάλυσης μπορεί να οδηγήσουν σε νέους τρόπους αναγνώρισης ατόμων. Τα δεδομένα από τη χρήση κινητού τηλεφώνου, τη συμμετοχή στα μέσα κοινωνικής δικτύωσης, και το ηλεκτρονικό εμπόριο μπορούν να προσδιορίσουν μοναδικά άτομα με μεγαλύτερη ακρίβεια. Η πρόοδος στα βιομετρικά μπορεί παρομοίως να ανοίξει νέους τρόπους για τον εντοπισμό και τον έλεγχο ταυτότητας ατόμων που επί του παρόντος αποκλείονται ή δεν εξυπηρετούνται από τα υπάρχοντα συστήματα ταυτότητας. Ταυτόχρονα, αυτές οι εξελίξεις εισάγουν νέες ανησυχίες σχετικά με το απόρρητο των δεδομένων, τον έλεγχο της κοινής χρήσης και χρήσης δεδομένων και την επιτήρηση.

Οι αναδυόμενες τάσεις στην ψηφιακή ταυτότητα μπορούν να βοηθήσουν στην αντιμετώπιση ορισμένων προκλήσεων, αλλά να ενισχύσουν άλλες. Για παράδειγμα, η τεχνολογία αναγνώρισης φωνής και προσώπου μπορεί να προσφέρει εναλλακτικές λύσεις που δεν απαιτούν νέο υλικό και αντίθετα βασίζονται στη σχεδόν πανταχού παρουσία των κινητών τηλεφώνων. Ωστόσο, αυτές οι εξελίξεις ενδέχεται να δημιουργήσουν ανησυχίες σχετικά με την επιτήρηση και να αποκλείσουν εκείνους των οποίων τα σώματα δεν περιγράφονται καλά από τα βιομετρικά στοιχεία. Η τεχνολογία Blockchain μπορεί να αντιμετωπίσει ανησυχίες σχετικά με την ακεραιότητα των αρχείων δεδομένων που συνδέονται με ψηφιακά αναγνωριστικά, αλλά να δημιουργήσει νέες ανησυχίες σχετικά με το δικαίωμα κατάργησης ή διαγραφής δεδομένων. Τα αυτοελεγχόμενα αναγνωριστικά υποδηλώνουν τη δυνατότητα των ατόμων να διαχειρίζονται ένα πλήρως φορητό διαπιστευτήριο ταυτότητας, αλλά μπορεί να είναι δύσκολο για τους χρήστες να το διαχειριστούν αποτελεσματικά. Αυτό μπορεί να εδραιώσει περαιτέρω το ψηφιακό χάσμα για εκείνους των οποίων η ψηφιακή εξοικείωση δεν τους επιτρέπει να διαχειρίζονται κατάλληλα μια αυτοελεγχόμενη ψηφιακή ταυτότητα.

6.2.1 Πρόοδοι στα βιομετρικά

Οι μεμονωμένες βιομετρικές μέθοδοι όπως η σάρωση ίριδας, τα δακτυλικά αποτυπώματα και η σάρωση αμφιβληστροειδούς συνήθως καλούνται ως μονοβιομετρικά συστήματα (unibiometric systems), επειδή βασίζονται σε μία μόνο βιομετρική πηγή αναγνώρισης. Τα σχετικά συστήματα παρουσιάζουν ορισμένα μειονεκτήματα όπως ασταθής βιομετρική βάση λόγω αισθητήρα ή χαμηλής ποιότητας λήψης βιομετρικού χαρακτηριστικού από ορισμένα άτομα, με αποτέλεσμα τα συστήματα ταυτοποίησης που απαιτούν υψηλή ασφάλεια να μην μπορούν να καλυφθούν αποτελεσματικά από τα μονοβιομετρικά συστήματα (Scott, 2006). Για τον λόγο αυτόν είναι απαραίτητη η επέκταση του παραδοσιακού μοντέλου βιομετρικής ταυτοποίησης που συνήθως βασίζεται σε ένα βιομετρικό χαρακτηριστικό, σε συστήματα που προκειμένου να επαληθεύσουν την ταυτότητα ενός χρήστη χρησιμοποιούντας πολλαπλές βιομετρικές πηγές αναγνώρισης. Τα

αντίστοιχα συστήματα καλούνται ως πολυβιομετρικά συστήματα (multibiometric systems) και παρουσιάζουν μεγαλύτερη αξιοπιστία και ακρίβεια ταυτοποίησης σε σχέση με τα μονοβιομετρικά συστήματα που βασίζονται σε ένα μεμονωμένο χαρακτηριστικό βιομετρικής επιβεβαίωσης. Η συνδυαστική χρήση πολλαπλών βιομετρικών δεδομένων είναι περισσότερη αποτελεσματική στη χρήση, εξαιτίας του θορύβου, της ανακρίβειας ή της έμφυτης μετατόπισης (που προκαλείται από παράγοντες όπως η γήρανση) σε υποσύνολα των βιομετρικές πηγών δεδομένων. Επιπροσθέτως, πολυβιομετρικά συστήματα μπορούν επίσης να μειώσουν τα ποσοστά αποτυχίας ορθής επαλήθευσης των ατόμων και να μειώσουν τις πιθανότητες προσπαθειών παραποίησης βιομετρικών δεδομένων (Jagadiswary & Saraswady, 2016). Η παράλληλη προσέγγιση, προσφέρει δυνατότητα να βελτιώσει την απόδοση της επαλήθευσης της βιομετρικής συμπεριφοράς, η οποία περιγράφεται παρακάτω (Saevanee et al., 2015):



Σχήμα 15: Σειριακό πολυβιομετρικό σύστημα (Clarke, 2011)

Γράφημα 14: *Σειριακό Πολυβιομετρικό Σύστημα*

Ένα παράλληλο πολυβιομετρικό σύστημα ταυτοποίησης περιλαμβάνει δύο ενότητες λειτουργίας: (i) την ενότητα εγγραφής και την (ii) ενότητα επαλήθευσης του χρήστη. Στην ενότητα εγγραφής με τη χρήση των κατάλληλων βιομετρικών αισθητήρων πραγματοποιείται η καταγραφή - αποτύπωση των ακατέργαστων βιομετρικών δεδομένων του χρήστη. Με βάση την ηλεκτρονική αποτύπωση των βιομετρικών δεδομένων που χρησιμοποιούνται από το σύστημα παράγεται η σύντηξη των ηλεκτρονικών αποτυπώσεων, η οποία και κρυπτογραφείται και στη συνέχεια αποθηκεύεται στη βάση δεδομένων του συστήματος για μελλοντικό έλεγχο ταυτότητας και επαλήθευσης. Κατά το στάδιο της επαλήθευσης λαμβάνονται τα σχετικά βιομετρικά δεδομένα του χρήστη, από τα οποία παράγεται η σύντηξη των βιομετρικών χαρακτηριστικών, η οποία συγκρίνεται με την αντίστοιχη τιμή που βρίσκεται αποθηκευμένη στη βάση του συστήματος μετά τη σχετική αποκρυπτογράφηση των δεδομένων σύγκρισης (Jagadiswary & Saraswady, 2016).

Σύμφωνα με τα παραπάνω διαφαίνεται πως η χρήση βιομετρικών δεδομένων θα αποτελέσει τη βάση λειτουργίας κάθε συστήματος ταυτοποίησης των ατόμων στο μέλλον. Οι δύο μεταβλητές

που επηρεάζουν την εφαρμογή των βιομετρικών στοιχείων στο δημόσιο τομέα είναι: α) η αντίληψη του κοινού για την τεχνολογία και β)απόδοση της τεχνολογίας. Η ανίχνευση με δακτυλικά αποτυπώματα αναγνωρίστηκε ως η μεγαλύτερη ακριβής τεχνολογία, ωστόσο έχει το χαμηλότερο ποσοστό δημόσιας αποδοχής δεδομένου του συσχετίσεις με την εγκληματικότητα. Η τεχνολογία με το υψηλότερο επίπεδο δημόσιας αποδοχής είναι η σάρωση προσώπου, ωστόσο αυτή είναι η πιο αδύναμη τεχνολογία απόδοσης, όπως υπάρχειδυσκολίες στη διάκριση μεταξύ παρόμοιων εικόνων.

6.2.2 Mobile ID

Βασική προϋπόθεση για την επιτυχία εφαρμογής ενός εθνικού ηλεκτρονικού συστήματος ταυτοποίησης αποτελεί η ευκολία χρήσης του από τους πολίτες και η μη απαίτηση εκ μέρους του συστήματος για υποχρεωτική χρήση ειδικών συσκευών (πχ αναγνώστης καρτών). Η μεγάλη διείσδυση χρήσης κινητών τηλεφώνων εκ μέρους των ατόμων, αποτελεί παράγοντα που θα πρέπει να ληφθεί σοβαρά υπόψη από τους παρόχους υπηρεσιών ηλεκτρονικής ταυτοποίησης. Μια πολλά υποσχόμενη λύση ηλεκτρονικής ταυτοποίησης αποτελεί η χρήση κινητών συσκευών ως σχετικό μηχανισμό ταυτοποίησης, παρέχοντας δυνατότητα φορητότητας του token για την αποθήκευση μιας ψηφιακής ταυτότητας και την πραγματοποίηση επαλήθευσης της ταυτότητας σε υπηρεσίες (Kenny Ching, 2021).

Η Επιτροπή Επικοινωνιών και Πολυμέσων της Μαλαισίας (MCMC) ολοκλήρωσε πρόσφατα μια δημόσια διαβούλευση για ένα πλαίσιο Εθνικής Ψηφιακής Ταυτότητας (NDID). Στην έκθεσή της, η MCMC αποκάλυψε ότι ένα συντριπτικό 94% των ερωτηθέντων ενδιαφέρεται να χρησιμοποιήσει το NDID όταν συναλλάσσεται με δημόσιο και ιδιωτικό τομέα. Και συγκεκριμένα, οι τρεις πρώτες περιπτώσεις χρήσης που ταξινομήθηκαν από πολίτες/καταναλωτές αφορούσαν όλες την ηλεκτρονική διακυβέρνηση: ηλεκτρονικά αρχεία υγειονομικής περίθαλψης, έλεγχος ταυτότητας κρατικής βοήθειας και κυβερνητικές διαδικτυακές υπηρεσίες (Kenny Ching, 2021).

6.2.1. ΤΕΧΝΟΛΟΓΙΑ NFC

Μία από τις κεντρικές τεχνολογίες για την ενεργοποίηση του κινητού eID για προγράμματα που βασίζονται σε έξυπνες κάρτες είναι η τεχνολογία Near Field Communication (NFC) . Όταν ενσωματώνεται σε μια έξυπνη κάρτα, η τεχνολογία NFC επιτρέπει την πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στην κάρτα μέσω μιας ανέπαφης σύνδεσης. Το 2019, το ποσοστό διείσδυσης των smartphone με δυνατότητα NFC έχει φτάσει το 81% παγκοσμίως.

Στις 30 Ιανουαρίου 2019, η Ε.Ε. κάλεσε την Apple να ανοίξει την διεπαφή NFC στα τηλέφωνά της και με αυτό τον τρόπο οι κυβερνήσεις να μπορούν να αξιοποιήσουν αυτήν την τεχνολογία

για να επιτρέψουν στους πολίτες να έχουν πρόσβαση στις λειτουργίες ηλεκτρονικής διακυβέρνησης από την κινητή συσκευή τους.

Ένα εμπόδιο που παραμένει είναι ότι μόνο 9 από τα 18 κράτη μέλη με κάρτες eID έχουν ενσωματωμένη αυτή την τεχνολογία NFC. Αυτή η κατάσταση μπορεί να αλλάξει καθώς οι κυβερνήσεις ενημερώνουν τις κάρτες τους για να ενσωματώσουν αυτήν την τεχνολογία, ειδικά δεδομένης της νέας νομοθεσίας της ΕΕ για την ενίσχυση της ασφάλειας των δελτίων ταυτότητας (Κανονισμός (ΕΕ) 2019/1157), ο οποίος απαιτεί ορισμένες πληροφορίες σχετικά με την κάρτα να διατίθενται ανέπαφα.

Η εφαρμογή μιας κινητής ταυτότητας για πολίτες, θα μπορούσε να επηρεάσει σε μεγάλο βαθμό την επιτυχή επίτευξη των στόχων ηλεκτρονικής διακυβέρνησης και εκσυγχρονισμού πολλών κυβερνήσεων. Όχι μόνο παρέχει μια οδό για καλύτερη δέσμευση με τους πολίτες τους, αλλά δημιουργεί επίσης έναν πιο μακροπρόθεσμο οδικό χάρτη για τη δημιουργία μιας ασφαλούς υποδομής ταυτότητας που περιλαμβάνει πολλές πτυχές του εμπορίου.

Με λίγα λόγια, τα κινητά ID προσφέρουν μια ελκυστική πρόταση στις κυβερνήσεις που θέλουν να επιταχύνουν τα σχέδιά τους για την ηλεκτρονική διακυβέρνηση παρέχοντας βολική, ασφαλή και προσανατολισμένη στο απόρρητο πρόσβαση σε υπηρεσίες.

6.2.3 Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

Η τεχνολογία blockchain επιτρέπει την εφαρμογή αποκεντρωμένων συστημάτων υψηλής ασφάλειας και διατήρησης του απορρήτου, όπου οι συναλλαγές δεν βρίσκονται υπό τον έλεγχο τρίτων οργανισμών. Χρησιμοποιώντας την τεχνολογία blockchain, τα δεδομένα εξόδου και τα νέα δεδομένα αποθηκεύονται σε ένα σφραγισμένο μπλοκ (καθολικό) που διανέμονται σε όλο το δίκτυο με επαληθεύσιμο και αμετάβλητο τρόπο. Η ασφάλεια των πληροφοριών και το απόρρητο ενισχύονται από την τεχνολογία blockchain στην οποία τα δεδομένα κρυπτογραφούνται και διανέμονται σε ολόκληρο το δίκτυο. Ενώ οι κυβερνήσεις σε όλο τον κόσμο δεν έχουν υιοθετήσει πλήρως την τεχνολογία blockchain στους δημόσιους τομείς, πολλές χώρες έχουν ξεκινήσει έργα blockchain για να διερευνήσουν τις δυνατότητες της τεχνολογίας blockchain στην προσφορά δημόσιων υπηρεσιών. Κάθε ένα από αυτά τα έργα συνήθως εστιάζει σε μια συγκεκριμένη υπηρεσία, για παράδειγμα ηλεκτρονική κατοικία, ηλεκτρονική υγεία, κτηματολόγιο κ.λπ. βρίσκονται ακόμη στα αρχικά τους στάδια και δεν έχει προταθεί κοινό πλαίσιο για την ενσωμάτωση τεχνολογίας blockchain στα συστήματα ηλεκτρονικής διακυβέρνησης. Επειδή όμως οι χώρες αναπτύσσουν το δικό τους πλαίσιο blockchain, υπάρχουν πολλά και διαφορετικά συστήματα blockchain από διαφορετικές χώρες, οδηγώντας σε δυσκολίες επικοινωνίας εκτός του δικτύου τους για διεθνή ανταλλαγή πληροφοριών. Για αυτό και καθίσταται αναγκαία η χρήση ενός ασφαλούς συστήματος ηλεκτρονικής διακυβέρνησης που βασίζεται σε blockchain, το οποίο μπορεί να υιοθετηθεί από οποιαδήποτε κυβέρνηση με σκοπό τη διασφάλιση τόσο της ασφάλειας όσο και της ιδιωτικής ζωής, ενώ ταυτόχρονα να αυξάνει την εμπιστοσύνη στον

δημόσιο τομέα. Το σύστημα αποτελείται από ένα peer to peer δίκτυο συσκευών ηλεκτρονικής διακυβέρνησης (κόμβοι) και συσκευές χρήστη. Εν συντομία, κάθε νέα συσκευή ηλεκτρονικής διακυβέρνησης ή μεμονωμένη συσκευή που εντάσσεται στο σύστημα θα ελεγχθεί από τους υπάρχοντες ομότιμους του δικτύου και ένας από τους ομοτίμους θα εκλεγεί για να δημιουργήσει έναν κόμβο δικτύου και μια διεύθυνση blockchain μιας νέας συσκευής. Όταν ένας νέος χρήστης επιχειρεί να εγγραφεί στο σύστημα μέσω μιας ή μιας συσκευής των κυβερνητικών υπηρεσιών, ο χρήστης έχει ένα αναγνωριστικό χρήστη και ένα πορτοφόλι blockchain για τη συλλογή και αποθήκευση της συναλλαγής του/της. Με αυτόν τον τρόπο, οι χρήστες ηλεκτρονικής διακυβέρνησης μπορούν να υποβάλλουν και να έχουν πρόσβαση στα αρχεία τους από οπουδήποτε και παντού, χρησιμοποιώντας τα αναγνωριστικά και τις διευθύνσεις blockchain τους.

Τα συστήματα ελέγχου ταυτότητας βασισμένα σε blockchain βασίζονται σε αδιαμφισβήτητη επαλήθευση ταυτότητας χρησιμοποιώντας ψηφιακές υπογραφές που βασίζονται σε κρυπτογράφηση δημόσιου κλειδιού. Κατά τον έλεγχο ταυτότητας με χρήση blockchain, ο μόνος έλεγχος που πραγματοποιείται είναι αν η συναλλαγή υπογράφηκε από το σωστό ιδιωτικό κλειδί. Το σύστημα θεωρεί πως όποιος έχει πρόσβαση στο ιδιωτικό κλειδί ενός ατόμου είναι ο ιδιοκτήτης του και η ακριβής ταυτότητα του ιδιοκτήτη θεωρείται μια μη απαραίτητη πληροφορία (Rosic, 2016).

Με τη χρήση του blockchain δεν υπάρχει άμεση απαίτηση συμμετοχής του παρόχου ταυτότητας στις ηλεκτρονικές συναλλαγές και η άμεση ηλεκτρονική ταυτοποίηση μέσω μιας άλλης οντότητας. Με τον τρόπο αυτόν, άμεσα ενισχύεται η ασφάλεια των προσωπικών δεδομένων των ατόμων, η ιδιωτικότητα προσωπικών δεδομένων και η εμπιστοσύνη των ατόμων απέναντι στο σύστημα χρήσης. Τέλος, η πιθανή χρήση της τεχνολογίας blockchain ως βάση λειτουργίας των συστημάτων ηλεκτρονικής ταυτοποίησης των ατόμων, ίσως μπορεί να αποτελέσει τη βάση μιας παγκόσμιας ηλεκτρονικής ταυτότητας, ενσωματώνοντας στο δίκτυο επαλήθευσης ταυτότητας το σύνολο των πολιτών όλων των κρατών (Rayome, 2017).

6.2.3.1.BIDaaS: Blockchain Based ID As a Service

Το προτεινόμενο αναγνωριστικό ως υπηρεσία που βασίζεται σε blockchain (BIDaaS) είναι ένας νέος τύπος IDaaS. Το BIDaaS έχει σχεδιαστεί για την παροχή μιας υποδομής διαχείρισης ταυτότητας και ελέγχου ταυτότητας από τον πάροχο BIDaaS στους συνεργάτες του. Οι τρεις εμπλεκόμενοι φορείς είναι οι εξής (Lee, 2018)

- Πάροχος BIDaaS: διατηρεί την αλυσίδα μπλοκ BIDaaS, η οποία είναι μια ιδιωτική αλυσίδα μπλοκ. Ο πάροχος BIDaaS γράφει το εικονικό αναγνωριστικό ενός χρήστη, το δημόσιο κλειδί του χρήστη κ.λπ. με μια ψηφιακή υπογραφή τους στην αλυσίδα μπλοκ BIDaaS. Η υπογραφή γίνεται με ιδιωτικό κλειδί του παρόχου BIDaaS.

- Συνεργάτης: Ο συνεργάτης διαβάζει το εικονικό αναγνωριστικό του χρήστη και τις πληροφορίες του δημόσιου κλειδιού του χρήστη από το blockchain BIDaaS όταν ο χρήστης ζητά

πρόσβαση στην υπηρεσία του με το εικονικό αναγνωριστικό. Ο συνεργάτης μπορεί να επιβεβαιώσει εάν το διεκδικημένο εικονικό αναγνωριστικό από τον χρήστη είναι αυτό που έχει εγγραφεί στην αλυσίδα μπλοκ BIDaaS, αποκτώντας πρόσβαση στην αλυσίδα μπλοκ BIDaaS. Εάν επιβεβαιωθεί σωστά, ο συνεργάτης ξεκινά τη διαδικασία αμοιβαίου ελέγχου ταυτότητας για τον χρήστη με το εικονικό αναγνωριστικό του χρήστη και το δημόσιο κλειδί του χρήστη που λαμβάνονται από την αλυσίδα μπλοκ BIDaaS.

• Χρήστης: Είναι ένας χρήστης εγγεγραμμένος στον πάροχο BIDaaS, αλλά δεν είναι εγγεγραμμένος στις υπηρεσίες του συνεργάτη. Ο χρήστης θέλει να χρησιμοποιήσει μια υπηρεσία που προσφέρεται από τον συνεργάτη, αλλά ο χρήστης δεν θέλει τη δημιουργία νέου αναγνωριστικού ούτε να παράσχει προσωπικά στοιχεία στον συνεργάτη για την υπηρεσία.

6.2.4. Ταυτότητα ελεγχόμενη από τον χρήστη self Sovereign Identity (SSI)

Έχει γίνει πολύς λόγος πρόσφατα για την αυτοκυριαρχία ταυτότητα (SSI), καθώς φαίνεται να είναι το επόμενο «νέο πράγμα» στη σφαίρα της ψηφιακής ταυτότητας, ειδικά στο πλαίσιο της πιθανής αντικατάστασης της παραδοσιακής υποδομής δημόσιου κλειδιού (PKI). Ο Κρίστοφερ Άλεν καθιέρωσε δέκα αρχές για ένα σύστημα ταυτότητας που θα μπορούσε να «εξισορροπήσει τη διαφάνεια, τη δικαιοσύνη και την υποστήριξη των κοινών με την προστασία του ατόμου». Αυτές οι δέκα αρχές, ύπαρξη, έλεγχος, πρόσβαση, διαφάνεια, εμμονή, φορητότητα, διαλειτουργικότητα, συναίνεση, ελαχιστοποίηση και προστασία, απεικονίζουν ένα σύστημα με επίκεντρο τον χρήστη όπου οι χρήστες απολαμβάνουν την πλήρη ιδιοκτησία των ιδιωτικά αποθηκευμένων δεδομένων ταυτότητάς τους. Η Αυτοκυρίαρχη Ταυτότητα είναι μια αναδυόμενη έννοια που σχετίζεται με τον τρόπο διαχείρισης της ταυτότητας στον ψηφιακό κόσμο. Σύμφωνα με την προσέγγιση της Αυτοκυρίαρχης Ταυτότητας, οι χρήστες θα πρέπει να μπορούν να δημιουργούν και να ελέγχουν τη δική τους ταυτότητα, χωρίς να βασίζονται σε καμία κεντρική αρχή. Με άλλα λόγια, αυτή η τεχνολογία επιτρέπει στους χρήστες να διαχειρίζονται μόνοι τους τις ψηφιακές τους ταυτότητες χωρίς να εξαρτώνται από τρίτους παρόχους για την αποθήκευση και την κεντρική διαχείριση των δεδομένων (Ross, 2021)

6.2.5.Cloud – Identity As A Service (IDAAS)

Το σύννεφο είναι μια ευρεία συλλογή διακομιστών και υποδομής υποστήριξής τους που είναι προσβάσιμες μέσω του Διαδικτύου. Μια υπηρεσία cloud είναι ένα προϊόν ή μια εφαρμογή που εκτελείται σε διακομιστές που φιλοξενούνται στο cloud αντί να εκτελείται στην τοπική υποδομή ενός οργανισμού. Οι υπηρεσίες Cloud χρησιμοποιούν ένα μοντέλο συνδρομής: αντί να πληρώνουν μία φορά για ένα λογισμικό, οι πελάτες cloud πληρώνουν μηνιαία χρέωση και μπορούν να αυξήσουν το επίπεδο της υπηρεσίας τους κατόπιν ζήτησης (2021).

Οι περισσότερες υπηρεσίες cloud περιγράφονται προσθέτοντας το "as-a-Service" στο όνομα της λειτουργίας τους. Για παράδειγμα:

- Το Software-as-a-Service (SaaS) αναφέρεται σε εφαρμογές λογισμικού που φιλοξενούνται στο cloud
- Το Platform-as-a-Service (PaaS) αναφέρεται σε εργαλεία ανάπτυξης και διακομιστές για τη δημιουργία εφαρμογών που φιλοξενούνται στο cloud
- Το Infrastructure-as-a-Service (IaaS) αναφέρεται σε διακομιστές στο cloud
- Το Function-as-a-Service (FaaS) αναφέρεται σε υπολογιστές χωρίς διακομιστή στο cloud

Το Identity-as-a-Service ή IDaaS είναι ένας τύπος SaaS. Είναι ένα μοντέλο παράδοσης εφαρμογών (όπως λογισμικό-ως-υπηρεσία ή SaaS) που επιτρέπει στους χρήστες να συνδέονται και να χρησιμοποιούν υπηρεσίες διαχείρισης ταυτότητας από το cloud.

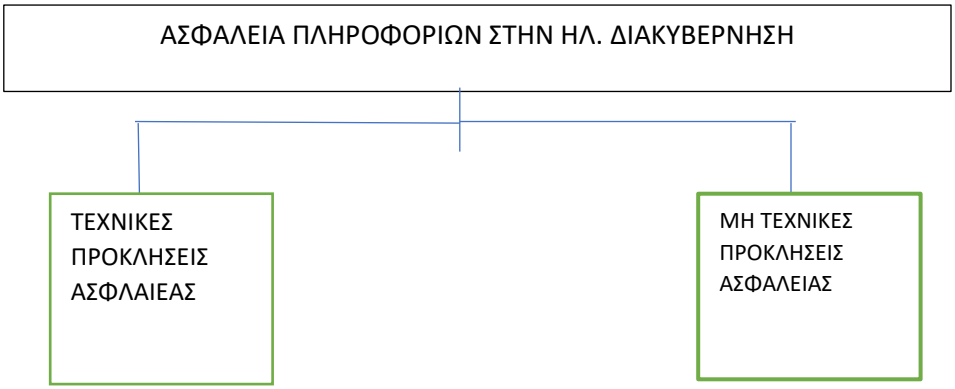
- Single Sign-On –Το Single Sign-On (SSO) βελτιώνει την ικανοποίηση των χρηστών εξαλείφοντας την κόπωση με τον κωδικό πρόσβασης και βελτιστοποιώντας την πρόσβαση. Απλοποιεί τις λειτουργίες πληροφορικής συγκεντρώνοντας και ενοποιώντας τις διοικητικές λειτουργίες. Και ενισχύει την ασφάλεια εξαλείφοντας επικίνδυνες πρακτικές διαχείρισης κωδικών πρόσβασης και μειώνοντας τις επιφάνειες επίθεσης και τα κενά ασφαλείας.
- Προσαρμοστικός έλεγχος ταυτότητας πολλαπλών παραγόντων –Με το MFA, ένας χρήστης πρέπει να παρουσιάσει πολλαπλές μορφές αποδεικτικών στοιχείων (π.χ. κωδικό πρόσβασης ή δακτυλικό αποτύπωμα και κωδικό SMS) για να αποκτήσει πρόσβαση σε ένα σύστημα. Οι σύγχρονες MFA υποστηρίζουν προσαρμοστικές μεθόδους ελέγχου ταυτότητας, χρησιμοποιώντας πληροφορίες συμφραζομένων (τοποθεσία, ώρα της ημέρας, διεύθυνση IP, τύπος συσκευής, κ.λπ.) και επιχειρηματικούς κανόνες για τον προσδιορισμό των παραγόντων ελέγχου ταυτότητας που πρέπει να εφαρμόζονται σε έναν συγκεκριμένο χρήστη σε μια συγκεκριμένη κατάσταση (Cyberark, 2021).

Οι λύσεις IDaaS βοηθούν τις επιχειρήσεις:

- Εξάλειψη του κόστους και της πολυπλοκότητας (αποφυγή δαπανών κεφαλαίου εξοπλισμού και απλοποίηση τρεχουσών λειτουργιών πληροφορικής).
- Μείωση κινδύνων (ενίσχυση της ασφάλειας εξαλείφοντας τις επικίνδυνες πρακτικές διαχείρισης κωδικών πρόσβασης και μειώνοντας τα τρωτά σημεία για επίθεση).
- Βελτίωση εμπειρίας χρηστών (ικανοποίηση των χρηστών εξαλείφοντας την κόπωση με κωδικούς πρόσβασης και επιτρέποντας στους χρήστες να έχουν πρόσβαση σε όλες τις εφαρμογές τους χρησιμοποιώντας ένα ενιαίο σύνολο διαπιστευτηρίων).

6.3. ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ

Το πλαίσιο ασφαλείας της ηλεκτρονικής διακυβέρνησης αποτελείται από τα κύρια τρία στοιχεία. ανθρώπους, διαδικασίες και τεχνολογίες Επομένως, η ασφάλεια της ηλεκτρονικής διακυβέρνησης μπορεί να βρίσκεται σε μια ευρεία περιοχή όπως φαίνεται στο σχήμα (Shareef, 2016):



Γράφημα 15: *Προκλήσεις Ασφάλειας*

Τα θέματα ασφάλειας αναμένεται να πείσουν το κοινό στη χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης και των υπηρεσιών για πρόσβαση, κοινή χρήση και ανταλλαγή πληροφοριών με ασφάλεια. Υπάρχουν διάφορες τεχνικές προκλήσεις που επηρεάζουν την ασφάλεια των πληροφοριών ηλεκτρονικής διακυβέρνησης όπως:

- Ασφάλεια δικτύου, όσον αφορά τις επιθέσεις δικτύου και θέματα αρχιτεκτονικής συστημάτων
- Ταυτοποίηση, η ασφάλεια της ασφάλειας του συμμετέχοντα από την άποψη της μοναδικής αναγνώρισης
- Απόρρητο, απειλή αποκάλυψης εμπιστευτικών πληροφοριών και μη εξουσιοδοτημένη πρόσβαση στα προσωπικά δεδομένα του πολίτη
- Έλεγχος πρόσβασης, προστασία συστημάτων σχετικά με θέματα αναγνώρισης ελέγχου ταυτότητας και εξουσιοδοτήσεις από εισβολείς
- Ηλεκτρονικός έλεγχος ταυτότητας (αξιόπιστο σύστημα προειδοποίησης για το δημόσιο τομέα θεωρείται η υποδομή δημοσίου κλειδιού που έχει αναγνωριστεί ως η καλύτερη ηλεκτρονική πιστοποίηση ταυτότητας για ηλεκτρονική διακυβέρνηση)
- Ανταλλαγή πληροφοριών μεταξύ κρατικών ιδρυμάτων για μία ολοκληρωμένη ηλεκτρονική υπηρεσία
- Κατηγοριοποίηση πληροφοριών και αποτροπή μη εξουσιοδοτημένης πρόσβασης κλοπής η απώλειας

Η αντιμετώπιση των κινδύνων και η κατανόηση των επιπτώσεων από τεχνική άποψη δεν αρκεί. Ως εκ τούτου η πρόκληση για την ασφάλεια των πληροφοριών στην ηλεκτρονική διακυβέρνηση αφορά μη τεχνικές προοπτικές όπως:

- Η έλλειψη διαλειτουργικότητας στα συστήματα ηλεκτρονικής διακυβέρνησης
- Η παροχή εύχρηστων υπηρεσιών προς τους πολίτες με το ανάλογο επίπεδο ασφάλειας

- Πρότυπα ασφαλείας που καθορίζουν τις πολιτικές ασφαλείας της ηλεκτρονικής διακυβέρνησης έτσι ώστε να εγγυηθούν ένα ασφαλές περιβάλλον
- Νομικό πλαίσιο, περιλαμβάνει ένα σχέδιο για τον προσδιορισμό των θεμελιωδών πόρων σε έναν οργανισμό αλλά και τους νόμους και τους κανονισμούς για την αντιμετώπιση απειλών ασφαλείας
- Απόρρητο, η χρήση της τεχνολογίας για την ενίσχυση της εμπιστοσύνης και την προστασία της ιδιωτικής ζωής μεταξύ πολιτών και δημόσιας διοίκησης
- Ευαισθητοποίηση όσον αφορά τα θέματα ασφάλειας και την υιοθέτηση τεχνολογιών για την αντιμετώπιση κινδύνων

ΚΕΦΑΛΑΙΟ 7: ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ψηφιακή ταυτότητα προσφέρει στα άτομα κοινωνικά, πολιτικά και πολιτισμικά οφέλη, από την αυξημένη ένταξη, την επισημοποίηση και τη διαφάνεια έως τον καλύτερο έλεγχο των διαδικτυακών δεδομένων. Σχεδιασμένη προσεκτικά και κλιμακωμένη σε υψηλά επίπεδα σε πολλαπλούς τομείς εφαρμογής, μπορεί επίσης να δημιουργήσει σημαντική οικονομική αξία, ιδιαίτερα στις αναδυόμενες οικονομίες, με οφέλη τόσο για άτομα όσο και για τους οργανισμούς. Ωστόσο, αυτό το δυναμικό συνεπάγεται κίνδυνο από εσκεμμένη κατάχρηση προγραμμάτων ψηφιακής ταυτότητας από κυβερνητικούς και εμπορικούς παράγοντες, καθώς και ευρύτερους κινδύνους που είναι κοινοί σε άλλες μεγάλης κλίμακας ψηφιακές αλληλεπιδράσεις, όπως τεχνολογική αστοχία και παραβιάσεις ασφάλειας. Όπως και άλλες τεχνολογικές καινοτομίες, όπως η πυρηνική ενέργεια, ακόμη και το πανταχού παρόν GPS, μπορεί να χρησιμοποιηθεί για να δημιουργήσει αξία ή να προκαλέσει βλάβη. Χωρίς κατάλληλους ελέγχους, οι διαχειριστές συστημάτων ψηφιακής ταυτότητας με κακόβουλους στόχους, είτε εργάζονται για εταιρείες του ιδιωτικού τομέα είτε για κυβερνήσεις, θα αποκτούσαν πρόσβαση και έλεγχο σε μεμονωμένα δεδομένα. Η ιστορία παρέχει άσχημα παραδείγματα κακής χρήσης παραδοσιακών προγραμμάτων ταυτοποίησης, συμπεριλαμβανομένου του εντοπισμού ή της δίωξης εθνοτικών ή θρησκευτικών ομάδων. Η ψηφιακή ταυτοποίηση, εάν δεν έχει σχεδιαστεί σωστά, θα μπορούσε να χρησιμοποιηθεί με ακόμη πιο στοχευμένους τρόπους ενάντια στα συμφέροντα ατόμων ή ομάδων από την κυβέρνηση ή τον ιδιωτικό τομέα.

ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Εντούτοις, ο σχεδιασμός, η διακυβέρνηση και η χρήση της ψηφιακής ταυτοποίησης είναι ένας ταχέως εξελισσόμενος τομέας που αξίζει πρόσθετη έρευνα. Τα θέματα για περαιτέρω διερεύνηση περιλαμβάνουν το σχεδιασμό του συστήματος, που ενσωματώνει χαρακτηριστικά για τη διασφάλιση της πλήρως ενημερωμένης συγκατάθεσης τόσο κατά την εγγραφή όσο και κατά τη διάρκεια της συνεχούς χρήσης, οικονομική ποσοτικοποίηση των κινδύνων, που περιλαμβάνει αποφάσεις σχεδιασμού και συναφείς δαπάνες, σχετικά πλεονεκτήματα και

μειονεκτήματα διαφορετικών μοντέλων για τη διακυβέρνηση και την ιδιοκτησία του συστήματος ψηφιακής ταυτότητας και συνεχής συσσώρευση μιας βάσης αποδεικτικών στοιχείων που τεκμηριώνει τα οφέλη ανά περιπτώσεις χρήσης, συμπεριλαμβανομένης της σύνδεσης με συγκεκριμένες αποφάσεις σχεδιασμού και οδηγούς χρήσης και υιοθέτησης. Αν και οι λύσεις δεν είναι πάντα σαφείς και περισσότερη έρευνα θα βοηθήσει να διευκρινιστούν τα θετικά και τα αρνητικά, η ψηφιακή ταυτοποίηση είναι αναμφίβολα μια σημαντική ευκαιρία για οικονομίες, κυβερνήσεις, επιχειρήσεις και άτομα σε όλο τον κόσμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΠΗΓΕΣ

Prins, C. (2007). E-government: A Comparative Study of the Multiple Dimensions of Required Regulatory Change. Electronic Journal of Comparative Law, 11(3).

Gelb, A., & Metz, A. (2017). Identification Revolution: Can Digital ID Be Harnessed for Development? https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf

OECD (2003). OECD E-Government Flagship Report "The E-Government Imperative," Public Management Committee, Paris:OECD.

Milakovich, Michael E. Digital Governance. 0 έκδ., Routledge, 2012. DOI.org (Crossref), https://doi.org/10.4324/9780203815991.

UN Division of Public Economics and Public Administration, American Society for Public Administration (2002): "Benchmarking E-government: A Global Perspective, Assessing the progress of the UN Member States"

th
government", Proceedings from 11 International Workshop on Database and Expert Systems
Aicholzer G., Schmutzer R.: "Organizational challenges to the development of electronic government", Proceedings from 11th International Workshop on Database and Expert Systems Applications, Springer, New York, 2000, pp. 379-383

Ε. Λουκής, Ι. Αποστολάκης, Ι. Χάλαρης, *Ηλεκτρονική Δημόσια Διοίκηση: Οργάνωση, Τεχνολογία και Εφαρμογές,* (2008)

Άρθρο 3 - Νόμος 4727/2020 - Γενικές αρχές ψηφιακής διακυβέρνησης'. Lawspot, 16 Οκτώβριος 2020, https://www.lawspot.gr/node/269851

'Άρθρο 84 - Νόμος 4727/2020 - Διαλειτουργικότητα των φορέων του δημόσιου τομέα'. Lawspot, 16 Οκτώβριος 2020, https://www.lawspot.gr/node/269932.

Α. Τάγαρης, Πρόεδρος και Διευθύνων Σύμβουλος Η.ΔΙ.Κ.Α. Α.Ε., *Ανάγκη για Εθνικό Πλαίσιο Διαλειτουργικότητας,* 2016

ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ (EUROPIAN COMMISION), *Ευρωπαϊκό πλαίσιο διαλειτουργικότητας - Στρατηγική εφαρμογής*, ΒΡΥΞΕΛΛΕΣ, 2017

Wimmer, M., Codagnone, C. and Janssen, M. (2008) "Future of e-Government Research: 13 research themes identified in the eGovRTD2020 project'. Proceedings of the 41st Hawaii International Conference on System Sciences, USA

European Commision, *European Semester Thematic Factsheet Quality Public Administration,* 2018 (https://ec.europa.eu/info/sites/default/files/file_import/european-semester_thematic-factsheet_quality-public-administration_el.pdf)

https://wayback.archive-it.org/12090/20170322043858/https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

E-Government-Benchmark der EU 2020 - www.egovernment.ch.

EGovernment Benchmark 2016: A Turning Point for EGovernment Development in Europe?. Volume 2, Final Background Report. Publications Office of the European Union, 2016. Publications Office of the European Union, https://data.europa.eu/doi/10.2759/002688.

Τζίφα, Μ. (2017). Η Ηλεκτρονική Διακυβέρνηση ως μέσον εκσυγχρονισμού της Διοίκησης & του Κράτους. Διπλωματική εργασία. Πανεπιστήμιο Πελοποννήσου, Τρίπολη.

Baheer, B. A., Lamas, D., & Sousa, S. (2018). Towards Development of a Reference Architecture for E-government. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance - ICEGOV '18. doi:10.1145/3209415.3209463

Aubakirov, M., & Nikulchev, E. (2016). Development of System Architecture for EGovernment Cloud Platforms. (IJACSA) International Journal of Advanced Computer Science and Applications, 7(2).

Iyad, D. (2019). Electronic governance: An overview of opportunities and challenges. Munich Personal RePEc Archive, Paper No. 92545. https://mpra.ub.uni-muenchen.de/92545/MPRA.

Bailey, K.O., Okolica, J.S., & Peterson, G.L. (2014). User identification and authentication using multi-modal behavioral biometrics. Comput. Secur., 43, 77-89.

Blue, J., Condell, J., & Lunney, T. (2018). A Review of Identity, Identification and Authentication. International Journal for Information Security Research (IJISR), 8(2).

Melin, U., K. Axelsson, and F. Söderström, (2016),

'Managing the development of e-ID in a public e-service

context: Challenges and path dependencies from a lifecycle perspective', Emerald Insight, Transforming

Government: People, Process and Policy, Volume 10,

Issue 1, pp. 72–98.

Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. Transforming Government: People, Process and Policy, 10(1), 8–25. doi:10.1108/tg-11-2013-0047

Reddy, A. (2015). Review of digital certificates. https://www.researchgate.net/publication/278015879_Review_of_digital_certificates

Gamundani, A. M., Phillips, A., & Muyingi, H. N. (2018). An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). doi:10.1109/cybermatics_2018.2018

Sable, P., & Bhosale, I. (2019). Symposium on Research and Innovations in Cyber SecurityAt: COLLEGE OF ENGINEERING, PUNE, MAHARASHTRA. https://www.researchgate.net/publication/334031584_Security_and_Authentication_Protocol_and_Security

Sinha , T. (2019). Risk Assessment and Management. https://www.researchgate.net/publication/341034867_Risk_Assessment_and_Management

Berbecaru, D., Lioy, A., & Cameroni, C. (2019). Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. Information, 10(6), 210. doi:10.3390/info10060210

Páez, R., Pérez, M., Ramírez, G., Montes, J., & Bouvarel, L. (2020). An Architecture for Biometric Electronic Identification Document System Based on Blockchain. Future Internet, 12(1), 10. doi:10.3390/fi12010010

'Άρθρο 25 - Νόμος 4727/2020 - Ταυτοποίηση για την έκδοση διαπιστευτηρίων'. Lawspot, 16 Οκτώβριος 2020, https://www.lawspot.gr/node/269873.

Antoniou, A., & Mitrou, L. (2011). e-ID card and data protection: A field of controversy or the path for good governance? 4th International Conference on Informational Law Thessaloniki, May 20-21.

Ravichandran, S. (2016). Smart Identity Card. International Journal of Control Theory and Applications 9(31),165-169.

European Commission (2010). Digitizing Public Services in Europe: Putting ambition into action, 9th Benchmark Measurement, Dec 2010, Directorate General for Information Society and Media.

Söderström, F. (2016). Introducing public sector eIDs: The power of actors' translations and institutional barriers (Doctoral dissertation, Linköping University Electronic Press).

Camp, L., 2004. Digital Identity. Technology and Society, IEEE, 23(3), pp. 34 - 41.

Πλαίσιο Ψηφιακής Αυθεντικοποίησης Έκδοση 4.0 Μάρτιος 2012 http://www.e-gif.gov.gr/portal/pls/portal/docs/840023.PDF

Office of the Privacy Commissioner of Canada, (2016). Guidelines for Identification and Authentication.

Jakobsson, M., & Taveau, S. (2014). The Case for Replacing Passwords with Biometrics. Available at: https://fidoalliance.org/wp-content/uploads/2014/12/3.pdf

Balakrishnan, S., & Deva, D. (2017). Issues and Challenges in E-Governance Caused by Privacy Threats. CSI Communications, 41(7), 28-29.

Jha, A. & Bose, I. (2013). A Framework for Addressing Data Privacy Issues In E-Governance Projects. Journal Of Information Privacy & Security, Vol. 9(3), pp. 18-33.

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. Social Psychological and Personality Science, Vol. 4(3), pp. 340-347.

Khasawneh, R., Rabayah, W. & Abu-Shanab, E. (2013). E-Government Acceptance Factors: Trust And Risk. The 6th International Conference on Information Technology (ICIT 2013), 8-10 May, 2013, Amman, Jordan, pp.1-8.

Al-Jamal, M., & Abu-Shanab, E.A. (2015). Privacy Policy of E-Government Websites and the Effect on Users' Privacy. ICIT 2015.

Abu-Shanab, E. & Al-Azzam, A. (2012). Trust Dimensions and the Adoption of E-Government in Jordan. International Journal of Information Communication Technologies and Human Development, Vol. 4(1), pp. 39-51.

Al-Dalou', R. & Abu-Shanab, E. (2013). E-Participation Levels and Technologies. The 6th International Conference on Information Technology (ICIT 2013), 8-10 May, 2013, Amman, Jordan, pp.1-8.

Alhomod, S. & Shafi, M. M. (2013). A Study on Implementation of Privacy Policy in Educational Sector Websites in Saudi Arabia. Global Journal of Computer Science and Technology, Vol. 13(1), pp. 22-26.

Wu, K., Huang, S., Yen, D. C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers In Human Behavior, Vol. 28(3), pp. 889-897.

Stanaland, A. S. & Lwin, M. O. (2013). ONLINE PRIVACY PRACTICES: ADVANCES IN CHINA. Journal Of International Business Research, Vol. 12(2), pp. 33-46.

Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης (2014). Στρατηγική για την Ηλεκτρονική Διακυβέρνηση 2014-2020. http://www.opengov.gr/minreform/wp-content/uploads/downloads/2014/02/stratigiki-ilektron.-diakyv.-teliko-pdf1.pdf

European Commission, Security Considerations and the Role of ENISA, 2020

European Commission, (n.d.-a). Electronic Identities – a brief introduction. https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

European Commission, (2018a). Digital Single Market Policy: Trust Services and Electronic Identification [eID]. European Parliament, (2018). "Single digital gateway: a time saver for citizens and companies," Press Release, December 18.

Echikson, W. (2020). Europe's Digital Verification Opportunity. CEPS Research Paper 17 JUN 2020.

Verrando, P. J. (2019). New EU eID cards regulation - a big move to keep a step ahead. Presentation: The Identity Conference, Eurosmart.

European Commission, (2018a). Digital Single Market Policy: Trust Services and Electronic Identification [eID]. European Parliament, (2018). "Single digital gateway: a time saver for citizens and companies," Press Release, December 18.

Υπουργείο Ψηφιακής Διακυβέρνησης (2021). Βίβλος Ψηφιακού Μετασχηματισμού 2020-2025. https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_strategy.pdf

Government of Netherlands, (2015). International Comparison e-ID Means. Λήψη από: https://www.government.nl/documents/reports/2015/05/13/international-comparison-e-IDmeans

BankID, (2017). This is BankID. https://www.bankid.com/en/om-bankid/detta-arbankid

Aichholzer, G., & Strauß, S. (2010). The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity in the Information Society, 3(1), 65-85.

Bour, I. (2013). Electronic Identities in Europe-Overview of e-ID solutions connecting Citizens to Public Authorities. UL Transaction Security Whitepaper (April 2013).

Torres, J., Nogueira, M., & Pujolle, G. (2013). A survey on identity management for the future network. IEEE Communications Surveys & Tutorials, 15(2), 787-802.

Electronic Identities – a brief introduction.
https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

Echikson, W. (2020). Europe's Digital Verification Opportunity. CEPS Research Paper 17 JUN 2020.

Verrando, P. J. (2019). New EU eID cards regulation - a big move to keep a step ahead. Presentation: The Identity Conference, Eurosmart.

Council of the European Union, (2006). Draft Resolution of the Representatives of the Governments of the Member States meeting within the Council on common minimum security standards for Member States' national identity cards.

European Commission, (2018a). Digital Single Market Policy: Trust Services and Electronic Identification [eID]. European Parliament, (2018). "Single digital gateway: a time saver for citizens and companies," Press Release, December 18.

Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's comp

Goodstadt, L. F., Connolly, R., & Bannister, F. (2015). The Hong Kong e-Identity Card: Examining the Reasons for Its Success When Other Cards Continue to Struggle. Information Systems Management, 32(1), 72-80.

Connectis, (2017). e-IDs in Europe. Λήψη από: https://e-IDas2018.eu/wpcontent/uploads/2016/12/e-IDAS-Leaflet-1-2016.pdf

E-estonia, (2017). France is aiming to reach Estonian e-governance level by 2022. Λήψη από: https://e-estonia.com/france-is-getting-to-estonian-e-administration-level-by-2022/

Gemalto, (2017b). Portuguese Citizen Card : 10 years of e-ID. Λήψη από:
http://www.gemalto.com/govt/customer-cases/portugal-id

Hillenius, G. (2017). Over 40,000 mobile phone ID users in Portugal. Λήψη από:
https://joinup.ec.europa.eu/news/over-40000-mobile-phone-id-u

De Cock, D., Wouters, K., & Preneel, B. (2004, June). Introduction to the Belgian E-ID card. In European Public Key Infrastructure Workshop (pp. 1-13). Springer, Berlin, He-IDelberg.

Gemalto, (2017a). Electronic ID cards in Belgium: the keystone of eGovernment. Λήψη από:
http://www.gemalto.com/govt/customer-cases/belgium

Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης
https://docplayer.gr/1557814-Ilektroniki-diakyvernisi-stin-ee.html

http://data.europa.eu/eli/reg/2014/910/oj/eng

https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52021DC0290&from=EN

Scott, Murray, κ.ά. 'Biometric Identities and E-Government Services': Encyclopedia of E-Commerce, E-Government, and Mobile Commerce, επιμέλεια Mehdi Khosrow-Pour, D.B.A., IGI Global, 2006, σσ. 50–56. DOI.org (Crossref), https://doi.org/10.4018/978-1-59140-799-7.ch009.

'How Mobile ID Facilitates E-Government | Disruptive Tech Asia'. Disruptive Tech Asia | Big Data News, Asia Big Data Jobs, Employment, Events, Big Data Seminars., January 2021, https://disruptivetechasia.com/big_news/how-mobile-id-facilitates-e-government/.

European Comission, Trends report on electronic identification_Mobile_FINAL, May 2020

Lee, Jong-Hyouk. 'BIDaaS: Blockchain Based ID As a Service'. IEEE Access, τ. 6, 2018, σσ. 2274–78. IEEE Xplore, https://doi.org/10.1109/ACCESS.2017.2782733.

Lee, J.-H. (2018). BIDaaS: Blockchain Based ID As a Service. IEEE Access, 6, 2274–2278. doi:10.1109/access.2017.2782733

Clippinger, J, & Bollier, D. (2014). From Bitcoin to Burning Man and Beyond The Quest for Identity and Autonomy in a Digital Society. Published by ID3 in cooperation with Off the Common Books. https://www.researchgate.net/profile/Mihaela-Ulieru/publication/274566666_Organic_Governance/links/5527ca4e0cf2e089a3a1db50/Organic-Governance.pdf

Bures, O., & Carrapico, H. (2018). Security Privatization. How Non-security-related Private Businesses Shape Security Governance. Springer International Publishing.

Terbu, O., Vogl, S., & Zehetbauer, S. (2016). One mobile ID to secure physical and digital Identity. Open Identity Summit 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn.

Rayome, A.D. (2017). The 3 most in-demand cybersecurity jobs of 2017. TechRepublic.

Rayome, A.D. (2018). Industries That Are Using Blockchain to Drive Business Value Right Now. TechRepublic

Rosic, A. (2017). 17 Blockchain Applications That Are Transforming Society [Online]. Blockgeeks. Available: https://blockgeeks.com/guides/blockchain-applications/

Power, Ross. 'SSI: Self-Sovereign Identity Explained'. Medium, November 2021, https://blog.cheqd.io/ssi-self-sovereign-identity-explained-9969cdd0c5da.

Enhancing Security of Information in E-Government'. ResearchGate, https://www.researchgate.net/publication/302385079_Enhancing_Security_of_Information_in_E-Government.

https://www.cyberark.com/what-is/idaas/