ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Διασφάλιση Ιδιωτικότητας σε Κατανεμημένα Συστήματα Μεγάλης Κλίμακας

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μαρία - Ελευθερία Χρ. Παπαδοπούλου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών
Δημοκριτείου Πανεπιστημίου Θράκης

Αθήνα, Μάρτιος 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Διασφάλιση Ιδιωτικότητας σε Κατανεμημένα Συστήματα Μεγάλης Κλίμακας

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μαρία - Ελευθερία Χρ. Παπαδοπούλου

Συμβουλευτική Επιτροπή: Ιάκωβος Στ. Βενιέρης
Δήμητρα-Θεοδώρα Ι. Κακλαμάνη
Νικόλαος Κ. Ουζούνογλου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 6η Μαρτίου 2018.

.....	.....	.....
Ι. Στ. Βενιέρης Καθηγητής Ε.Μ.Π.	Δ.-Θ. Ι. Κακλαμάνη Καθηγήτρια Ε.Μ.Π.	Ν. Κ. Ουζούνογλου Καθηγητής Ε.Μ.Π.
.....	.....	.....
Θ. Α. Βαρβαρίγου Καθηγήτρια Ε.Μ.Π.	Κ. Λαμπρινουδάκης Καθηγητής ΠΑ.ΠΕΙ.	Ν. Γ. Κοζύρης Καθηγητής Ε.Μ.Π.
	.....	
	Γ. Κ. Ματσόπουλος Αν. Καθηγητής Ε.Μ.Π.	

Αθήνα, Μάρτιος 2018

.....
Μαρία - Ελευθερία Χρ. Παπαδοπούλου
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Στους γονείς μου Χρήστο και Χρυσάνθη
και στον αδερφό μου Κωνσταντίνο.

Περίληψη

Η συνεχώς αυξανόμενη εξάρτηση των παρεχόμενων – από κρατικούς και ιδιωτικούς φορείς – υπηρεσιών από τις Τεχνολογίες Πληροφορίας και Επικοινωνίας (ΤΠΕ) αυξάνει δραματικά τις ευπάθειες των συστημάτων, το πλήθος και το εύρος των απειλών και των επιθέσεων, καθώς και τη σοβαρότητα των συνεπειών για τον πάροχο αλλά και τον τελικό χρήστη της εκάστοτε υπηρεσίας σε περίπτωση κάποιου περιστατικού ασφάλειας. Οι σημερινές επιθέσεις προς τις προσφερόμενες ηλεκτρονικές υπηρεσίες και τα πληροφοριακά συστήματα που τις υποστηρίζουν αποτελούν ένα νέο είδος ηλεκτρονικού πολέμου, ενώ μπορεί να έχουν ποινικό, οικονομικό ή τρομοκρατικό κίνητρο και να οδηγήσουν σε αποσταθεροποίηση της κοινωνίας. Διαρροές κρίσιμων πληροφοριών, τροποποίηση ευαίσθητων δεδομένων και μη διαθεσιμότητα βασικών λειτουργιών μπορεί να θέσουν σε κίνδυνο οικονομικά συμφέροντα εταιρειών αλλά και στρατηγικά συμφέροντα κρατών.

Δεδομένου ότι οι επιθέσεις εναντίον των ΤΠΕ εξελίσσονται συνεχώς και η ανίχνευσή τους γίνεται όλο και πιο δύσκολη, η εξασφάλιση ενός επαρκούς επιπέδου ασφάλειας και προστασίας της ιδιωτικότητας των χρηστών κρίνεται αναγκαία. Για τον λόγο αυτό, αποτελεί πλέον επιτακτική ανάγκη κατά τον σχεδιασμό και την ανάπτυξη ασφαλών πληροφοριακών συστημάτων να λαμβάνονται υπόψη: (α) η ποικιλία και ένταση των κινδύνων που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα, (β) οι Νομικές και Κανονιστικές απαιτήσεις για την προστασία ευαίσθητων δεδομένων και δεδομένων προσωπικού χαρακτήρα, καθώς και (γ) το σημαντικό κόστος από τυχόν σκόπιμες παραβιάσεις της ασφάλειας του συστήματος, όπως επίσης και των ακούσιων, τυχαίων και φυσικών γεγονότων που απειλούν ένα σύγχρονο πληροφοριακό σύστημα. Για την αποτελεσματική αντιμετώπιση των ζητημάτων αυτών, καθοριστική συνεισφορά έχει η χάραξη στρατηγικών, ο ορισμός πολιτικών, η ανάπτυξη υπηρεσιών και μηχανισμών καθώς και η - εκ των προτέρων, κατά τη διάρκεια και εκ των υστέρων - αξιολόγηση του συνολικού εγχειρήματος για τη δημιουργία ενός ολοκληρωμένου περιβάλλοντος ασφάλειας και εμπιστοσύνης.

Στόχος της παρούσας διδακτορικής διατριβής είναι η παρουσίαση ενός ολοκληρωμένου πλαισίου ασφάλειας και μίας πλατφόρμας που υιοθετεί τα απαιτούμενα τεχνικά, διαδικαστικά και οργανωτικά μέτρα για την προστασία των πληροφοριακών συστημάτων από τις απειλές στις οποίες εκτίθενται ή/και την ελαχιστοποί-

ηση των όποιων επιπτώσεων από δυνητικά περιστατικά ασφάλειας. Η προαναφερθείσα πλατφόρμα ακολουθεί την προσέγγιση ασφάλειας και προστασίας της ιδιωτικότητας από τον σχεδιασμό του συστήματος, καλύπτοντας ανάγκες σχετικές με τη διαχείριση της μετάδοσης, αποθήκευσης και επεξεργασίας προσωπικών δεδομένων, ενώ παράλληλα ικανοποιεί τις απαιτήσεις που απορρέουν από την ισχύουσα νομοθεσία περί προστασίας της ιδιωτικότητας, υιοθετώντας και επεκτείνοντας καινοτόμους μηχανισμούς και τεχνολογίες ασφάλειας και προστασίας δεδομένων, όπως τον Σημασιολογικό Έλεγχο Πρόσβασης Βάσει Ιδιοτήτων, τη Λειτουργική Κρυπτογράφηση και την Τεχνολογία της Αλυσίδας των Μπλοκ. Η αποτελεσματικότητα της προαναφερθείσας πλατφόρμας εξετάζεται και επαληθεύεται σε συστήματα που διαχειρίζονται δεδομένα (προσωπικά και μη) σε ετερογενή κατανεμημένα περιβάλλοντα, και, συγκεκριμένα, σε συστήματα παροχής υπηρεσιών στους τομείς διαχείρισης παραγωγής, ηλεκτρονικής διακυβέρνησης και παρακολούθησης της υγείας του ατόμου.

Λέξεις κλειδιά: Ιδιωτικότητα, προστασία προσωπικών δεδομένων, έλεγχος πρόσβασης, εμπιστοσύνη, τεχνολογίες σημασιολογικού ιστού, κατανεμημένα συστήματα, έξυπνα ετερογενή περιβάλλοντα.

Abstract

The ever-increasing dependence of services provided in both private and public sectors on Information and Communication Technologies (ICT) has led to the dramatic explosion of system vulnerabilities, the variety and number of threats and attacks, as well as the severity of the consequences for both the service provider and the end-user in case of a security incident. Today's attacks on the electronic services offered and the information systems that support the former constitute a new kind of electronic warfare. They may hide a criminal, economic or terrorist motive and lead to destabilization of society. Leakages of critical information, modification of sensitive data and unavailability of key operations may jeopardize the financial interests of companies as well as strategic interests of states.

Since attacks against ICT are constantly evolving and their detection is becoming more and more difficult, ensuring an adequate level of system's security and user's privacy is necessary. Thus, it is now imperative that during the design and development of secure information systems the following are taken into account: (a) the variety and intensity of the risks faced by modern information systems; (b) the legal and regulatory requirements for the protection of personal and sensitive data; (c) the significant cost of any deliberate violations of system security, as well as any accidental or natural events threatening a modern information system. In order to effectively address the aforementioned issues, the development of security and data protection strategies, policy-making and the adoption of the appropriate mechanisms, as well as the a-priori, ongoing and a-posteriori evaluation of the overall endeavour are crucial for the creation of a secure and trusted environment.

In general, the goal of this thesis is to present an integrated security framework and a platform that adopts the necessary technical, procedural and organizational measures required to protect information systems from the threats to which they are exposed and/or to minimize any impact of potential security incidents. The aforementioned platform follows the security- and privacy-by-design approaches, covering needs related to the management of the transmission, storage and processing of personal data, while meeting the requirements arising from the necessary compliance with the current legal and regulatory framework concerning privacy protection. It leverages the recent advances in security and cryptography, especially Semantic Attribute-Based Access Control, Functional Encryption and Blockchain technology. The effectiveness of the abovementioned platform

is examined and verified in systems that manage data (both personal and non-personal) in heterogeneous distributed environments, and, to be more specific, in service provision systems in the production management, eGovernment and health monitoring domains.

Keywords: Privacy, data protection, access control, trust, semantic web technologies, distributed systems, smart heterogeneous environments.

Αντί Προλόγου

Η παρούσα διδακτορική διατριβή αποτελεί το επιστέγασμα της ερευνητικής μου δραστηριότητας και της μακρόχρονης πορείας μου ως υποψήφιας διδάκτορος και μέλους του Εργαστηρίου Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης (ICBNet) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών (ΣΗΜΜΥ) του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ). Έναυσμα της διατριβής μου αποτέλεσε, αρχικά, η ιδιαίτερή μου αγάπη για τον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων που μου ενέπνευσε ο επιβλέπων καθηγητής της προπτυχιακής διπλωματικής μου εργασίας κύριος Βασίλειος Κάτος, η οποία, όμως, ενισχύθηκε σημαντικά όταν, συζητώντας με τον επιβλέποντα της διδακτορικής μου διατριβής καθηγητή κύριο Ιάκωβο Βενιέρη και γνωρίζοντας τα μέλη της ερευνητικής του ομάδας, ήρθα σε επαφή με ανθρώπους με βαθύ επιστημονικό και τεχνικό υπόβαθρο, καθώς και σημαντική ερευνητική συνεισφορά στον τομέα αυτό. Κάπως έτσι, αργότερα, οι τελευταίοι με μύησαν και στον αγώνα για τη διασφάλιση και την προστασία της ιδιωτικότητας που αποτέλεσε και το κύριο θέμα της παρούσας διατριβής.

Σημαντικό κομμάτι της διατριβής βασίστηκε στις ερευνητικές δραστηριότητες που πραγματοποιήθηκαν κατά τη διάρκεια δύο ερευνητικών προγραμμάτων και, συγκεκριμένα, στο ευρωπαϊκό έργο ARUM και στο εθνικό έργο SPAGOS, στα οποία είχα την τύχη να εμπλακώ άμεσα. Κατά τη διάρκεια εκπόνησης των έργων αυτών, είχα την ευκαιρία να συνεργαστώ με αξιόλογους επιστήμονες και επαγγελματίες, να ανταλλάξω απόψεις και να αποκτήσω ποικίλες γνώσεις και ανεκτίμητη εμπειρία που, δεδομένων των ανεπεξέργαστων μέχρι τότε βασικών προπτυχιακών μου γνώσεων και της επαγγελματικής μου απειρίας, συνέβαλαν σε μεγάλο βαθμό στην προσωπική μου εξέλιξη. Μέσω της άμεσης συμμετοχής και συνεισφοράς μου σε πληθώρα δραστηριοτήτων του εργαστηρίου, έμαθα στην πράξη πώς σκέφτεται και δρα ένας μηχανικός, τόσο σε ερευνητικό-ακαδημαϊκό όσο και σε επαγγελματικό επίπεδο. Μαθήτευσα πλάι σε εξαίρετους επιστήμονες που μου έμαθαν πώς γίνεται σωστά η έρευνα και, παράλληλα, τι θα πει «επαγγελματισμός». Στο σημείο λοιπόν αυτό, θα ήθελα να ευχαριστήσω τους ανθρώπους εκείνους που για χρόνια τώρα αποτελούν για εμένα τη δεύτερή μου οικογένεια.

Ξεκινώντας, τίποτα από όλα αυτά δε θα είχε συμβεί στη ζωή μου αν δεν υπήρχε ο επιβλέπων καθηγητής και πνευματικός μου ταγός κύριος Ιάκωβος Βενιέρης, Καθη-

γητής ΕΜΠ, στον οποίο είμαι ευγνώμων για την εμπιστοσύνη που μου έδειξε και την ευκαιρία που μου έδωσε να αποδείξω εμπράκτως, πρώτα στον εαυτό μου και έπειτα σε εκείνον, ότι αξίζω τη θέση αυτή ως υποψήφια διδάκτωρ και μέλος της ερευνητικής του ομάδας. Τον ευχαριστώ θερμά για την πολύτιμη καθοδήγησή του όλα αυτά τα χρόνια και τη στήριξη και συμπαράστασή του σε στιγμές κρίσιμες που απαιτούσαν από μεριάς μου αυταπάρνηση και επιμονή. Συνεχίζοντας, θα ήθελα να ευχαριστήσω από καρδιάς τη συνεπιβλέπουσα καθηγήτριά μου κυρία Δήμητρα Κακλαμάνη, Καθηγήτρια ΕΜΠ, για την καθοριστική της συμβολή στην πορεία μου αυτή. Την ευχαριστώ ιδιαίτερα για την εκτίμησή της στο πρόσωπό μου, την οποία αποδείκνυε σε κάθε ευκαιρία με τρόπο ουσιαστικό και υποστηρικτικό, μεταδίδοντάς μου σε κάθε μας συζήτηση τις γνώσεις και τις εμπειρίες της. Επίσης, θα ήθελα να ευχαριστήσω τους Καθηγητές ΕΜΠ κύριο Νικόλαο Ουζούνογλου και κυρία Θεοδώρα Βαρβαρίγου για τις καίριες συμβουλές και υποδείξεις τους. Ιδιαίτερες ευχαριστίες θα ήθελα να απευθύνω στον κύριο Κωνσταντίνο Λαμπρινουδάκη, Καθηγητή Πανεπιστημίου Πειραιώς, με τον οποίο είχα τη χαρά να συνεργαστώ στο πλαίσιο ερευνητικού έργου και πλέον έχω την τιμή να αποτελεί ο ίδιος μέλος της επταμελούς επιτροπής μου. Τέλος, θα ήθελα να ευχαριστήσω τον Κοσμήτορα της ΣΗΜΜΥ ΕΜΠ Καθηγητή κύριο Νεκτάριο Κοζύρη, καθώς και τον κύριο Γεώργιο Ματσόπουλο, Αναπληρωτή Καθηγητή ΕΜΠ, για την τιμή που μου έκαναν να συμπεριληφθούν στην επταμελή μου εξεταστική επιτροπή.

Πέραν των όσων ανέφερα παραπάνω, θεωρώ τον εαυτό μου τυχερό για έναν ακόμη λόγο και, συγκεκριμένα, επειδή γνώρισα ανθρώπους που, εν τέλει, ο καθένας τους ξεχωριστά άφησε με τρόπο ιδιαίτερο και μοναδικό το αποτύπωμά του στη διαδρομή μου μέχρι εδώ. Ξεκινώντας χρονολογικά από τα πρώτα μου χρόνια στο εργαστήριο, θα ήθελα να ευχαριστήσω, αρχικά, τον Γιώργο Λιουδάκη και τον Άγγελο Αναδιώτη με τους οποίους συνεργάστηκα στενά για ένα σημαντικό χρονικό διάστημα· η συμβολή τους στη μετέπειτα πορεία μου μέσω των άμεσων αλλά και έμμεσων μαθημάτων που πήρα από εκείνους είναι αδιαμφισβήτητη. Σειρά έχει το παρεάκι και συνοδοιπόρος μου όλα αυτά τα χρόνια, η Δέσποινα Μερίδου, με την οποία περάσαμε πολλά και μάθαμε ακόμα περισσότερα μαζί και την ευχαριστώ για την αδιάκοπη στήριξή της. Επόμενος είναι ο ζεν cloud master Ανδρέας Καψάλης που, πέρα από τις επιστημονικές του συμβουλές, με τον αυθορμητισμό του και το ιδιαίτερο χιούμορ του μου χάριζε άφθονα γέλια και με βοηθούσε να δω τα πράγματα λίγο πιο χαλαρά. Στη συνέχεια, θα ήθελα να ευχαριστήσω το αστέρι του machine learning Παναγιώτη Κασνέση με τον οποίο, έπειτα από άπειρες ώρες spagosυζητήσεων επίλυσης γρίφων και προβλημάτων, καταφέραμε να έχουμε μία άψογη συνεργασία ενώ, αργότερα, με στήριξε εμπράκτως σαν πραγματικός φίλος, χαραμίζοντας άπειρες ώρες του για να ακούει υπομονετικά τους προβληματισμούς μου και να προσπαθεί να μου δώσει λύσεις. Ένα μεγάλο ευχαριστώ για τη διαρκή του υποστήριξη θέλω να απευθύνω στον «γείτονα» και καλό μου πλέον φίλο Κώστα Μπρόμη, με τον οποίο αναζη-

τήσαμε πολλές φορές τρόπους να συνδυάσουμε επιτυχώς τις ερευνητικές μας περιοχές. Ιδιαίτερης μνείας αξίζει η Μαρία Σεϊμένη, την οποία θέλω να ευχαριστήσω για την αγάπη της και το ανιδιοτελές ενδιαφέρον της που πάντα με συγκινούσε και ήταν εμφανές στις συζητήσεις μας. Φυσικά δεν μπορώ να παραλείψω την ήρεμη δύναμη του εργαστηρίου τον Μανόλη Καραμανή και τον «πρόεδρο και γιατρό» μας Πέτρο Μπάκαλο, που, με τον ερχομό τους στο εργαστήριο, έφεραν φρέσκες ιδέες και έναν αέρα κινητής υπολογιστικής, διευρύνοντας έτσι τους ορίζοντες της σκέψης μας. Ένα μεγάλο ευχαριστώ οφείλω στην – πάντα εκεί για όλους εμάς – Σοφία Καπελλάκη για τις συμβουλές της και την απλόχερη βοήθεια που μου πρόσφερε ανά πάσα στιγμή, όπως επίσης και στη Βάσω Γιωτοπούλου, όχι μόνο για τα ευχάριστα «νέα» που μας έφερνε κατά καιρούς αλλά και για τις ιδιαίτερα ενθαρρυντικές για εμένα κουβέντες μας. Τέλος, θα ήθελα να ευχαριστήσω τον Πάνο Γκόνη για τη συνεργασία μας, καθώς και τον κύριο Χαράλαμπο Πατρικάκη, Αναπληρωτή Καθηγητή ΑΕΙ Πειραιά ΤΤ, ο οποίος, μέσω της εποικοδομητικής συνεργασίας μας, μου πρόσφερε εμμέσως μια διαφορετική οπτική των πραγμάτων σε ένα σημείο καμπής της πορείας μου.

Φυσικά δεν έχω ξεχάσει τους συναδέλφους που με καλωσόρισαν στο εργαστήριο και συγκεκριμένα τους Αζίζ Μούσα, Χρίστο Παππά, Νίκο Δέλλα, Μαρίζα Κουκοβίνη, Ευγενία Παπαγιαννακοπούλου, Φώτη Γώγουλο, Άννα Αντωνακοπούλου, Νίκο Τσελίκα, Κώστα Παπαδόπουλο και Γιώργο Λαμπρινάκο. Στο σημείο αυτό, θέλω να αναφέρω δύο ακόμη άτομα που γνώρισα στον χώρο αυτό και εκτιμώ ιδιαιτέρως, τον Λάζαρο Τουμανίδη για την άριστη συνεργασία μας στο πλαίσιο ερευνητικού έργου, καθώς και τον «γείτονα» Αντώνη Σάββα για τις ουκ ολίγες συζητήσεις μας και ανταλλαγές απόψεων επί παντός επιστητού.

Από τους ανθρώπους που είχα δίπλα μου από την πρώτη στιγμή, πρώτη από όλους θέλω να αναφέρω την αδελφική μου φίλη Εύη, που, όσα χιλιόμετρα κι αν μας χωρίζουν, είναι παρούσα στην καθημερινότητά μου να με στηρίζει αδιαλείπτως. Για την πίστη του σε εμένα οφείλω ένα μεγάλο ευχαριστώ στον Πάνο, που έζησε δίπλα μου αμέτρητες φορές τη «συντέλεια του κόσμου» και, παρ' όλα αυτά, παρέμεινε με τον τρόπο του διακριτικός υποστηρικτής μου. Θα ήθελα, επίσης, να ευχαριστήσω τους φίλους μου Κατερίνα, Γιάννη, Δημήτρη και Μίλτο για τις ξέγνοιαστες στιγμές που μοιραστήκαμε τα τελευταία χρόνια. Ιδιαίτερες ευχαριστίες θα ήθελα να απευθύνω στη Μαίρη και στον Σάκη για τη συνεχή και διακριτική τους παρουσία και κατανόηση.

Για το τέλος άφησα εκείνους που είχαν και έχουν τον πιο σημαντικό ρόλο στη ζωή μου. Καθημερινά δίπλα μου, τα στηρίγματά μου, οι γονείς μου Χρήστος και Χρυσάνθη, ήταν εκεί για να με ακούσουν υπομονετικά και να μου δώσουν κουράγιο και δύναμη να συνεχίσω. Μαζί με εκείνους φυσικά και ο αγαπημένος μου αδερφός Κωνσταντίνος που τολμώ να πω ότι κατάφερε και με άντεξε μέχρι τέλους. Τον ευχαριστώ για την αγάπη του, τις βόλτες και τα γέλια μας όσο τον είχα κοντά. Τέλος, είμαι ευγνώμων που είχα για αρκετό καιρό κοντά μου και τον «σοφό» παππού μου Μιχάλη, του οποίου τα 2-3 αγαπημένα ρητά περί ζωής θα με συντροφεύουν για πάντα.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Σελ.

Πίνακας Πινάκων

Σελ.

Κεφάλαιο 1

Εισαγωγή

Ζούμε σε έναν κόσμο ο οποίος αλλάζει με ταχύτατους ρυθμούς, καθώς τα πάντα πλέον περιστρέφονται γύρω από τα δεδομένα. Το γεγονός ότι το *Διαδίκτυο των Πραγμάτων* (Internet of Things) και η *Κινητή και Διάχυτη Υπολογιστική* (Mobile & Ubiquitous Computing) έχουν ενσωματωθεί πλέον στην καθημερινότητα του ατόμου συνδράμει ουσιαστικά στον προαναφερθέντα μετασχηματισμό της κοινωνίας μας, κάτι το οποίο γίνεται περισσότερο εμφανές στις πλέον πιο ποιοτικές, αποτελεσματικές αλλά και διαφανείς ηλεκτρονικές υπηρεσίες τομέων, όπως η Υγεία, η Διακυβέρνηση, η Εφοδιαστική Αλυσίδα, κ.λπ. Η συνεχής εξέλιξη και η ανάπτυξη των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) ως προς τη διασύνδεση ανθρώπων, τοποθεσιών και συσκευών σε ένα παγκόσμιο *Διαδίκτυο των Πάντων* (Internet of Everything – IoE) έχει επηρεάσει σημαντικά όλων των ειδών τις βιομηχανίες, από την ψυχαγωγία των ανθρώπων μέχρι την κατασκευή αυτοκινήτων, την εκπαίδευση και την υγειονομική περίθαλψη.

Παράλληλα, η διασφάλιση της Ιδιωτικότητας αποτελεί ένα ιδιαίτερα σημαντικό θέμα για όλους τους δημόσιους και ιδιωτικούς οργανισμούς. Υπάρχουν πολλοί νόμοι και κανονισμοί που ρυθμίζουν τον τρόπο με τον οποίο οι διάφοροι φορείς πρέπει να επεξεργάζονται τα δεδομένα των πελατών τους και οι νόμοι αυτοί θα γίνουν ακόμη πιο αυστηροί τον Μάιο του 2018. Τα προηγούμενα χρόνια, οι περισσότεροι οργανισμοί παγκοσμίως αποκόμισαν μεγάλα κέρδη λόγω των σημαντικών εξελίξεων τόσο στις τεχνικές ανάπτυξης λογισμικού όσο και σε υποδομές με ιδιαίτερα μεγάλη υπολογιστική ισχύ, εξασφαλίζοντας σε μεγάλο βαθμό την αυτοματοποίηση των επιχειρηματικών διαδικασιών χρησιμοποιώντας ιδιαίτερα εξελιγμένα επιχειρησιακά πληροφοριακά συστήματα. Τα συγκεκριμένα πληροφοριακά συστήματα δεν περιέχουν μόνο τεράστιο όγκο δεδομένων πελατών αλλά προσφέρουν μία μεγάλη ποικιλία μεθόδων επεξεργασίας τους. Η ταχεία αυτή εξέλιξη των πληροφοριακών συστημάτων μετέτρεψε, ουσιαστικά, τα «περιουσιακά στοιχεία» των επιχειρήσεων σε πολύτιμα αγαθά, με ολοένα και μεγαλύτερη λειτουργικότητα.

Η διασφάλιση συμμόρφωσης των πληροφοριακών συστημάτων με τη νομοθεσία περί προστασίας της ιδιωτικότητας του ατόμου και τους αντίστοιχους κανονισμούς ενδέχεται να μην αποτελεί πρώτη προτεραιότητα για τους οργανισμούς, καθώς η αυστηρότητα των κανονισμών αυτών μπορεί να περιορίσει τη λειτουργικότητα των συστημάτων και να καταστήσει πιο δύσκολο τον σχεδιασμό τους. Ωστόσο, η επιδίωξη της συμμόρφωσης με τους νόμους για την προστασία προσωπικών δεδομένων δεν συνιστά προαιρετικό χαρακτηριστικό των συστημάτων αυτών, καθώς υπάρχουν σοβαρές συνέπειες σε περίπτωση μη συμμόρφωσης μέσω της επιβολής προστίμων από τις εθνικές Αρχές Προστασίας Προσωπικών Δεδομένων. Οι συνέπειες αυτές θα γίνουν ακόμα μεγαλύτερες τον Μάιο του 2018, όταν το Ευρωπαϊκό Κοινοβούλιο θα επιβάλει ως δεσμευτικό για κάθε φορέα κράτους-μέλους της Ευρωπαϊκής Ένωσης τον νέο κανονισμό για την προστασία των δεδομένων, γνωστό ως *Γενικός Κανονισμός για την Προστασία Δεδομένων* (General Data Protection Regulation – GDPR) [4]. Ο νέος αυτός κανονισμός δίνει τη δυνατότητα σε Ελεγκτικές Αρχές να επιβάλουν πρόστιμα που ανέρχονται στα 10.000.000 € σε επιχειρήσεις που δεν συμμορφώνονται με τον κανονισμό GDPR.

Προκειμένου να βοηθηθούν οι επιχειρήσεις ως προς τη συμμόρφωση με τη νομοθεσία για την προστασία δεδομένων εισήχθη ο όρος *Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας* (Privacy Enhancing Technologies – PET). Οι τεχνολογίες αυτές μπορούν να περιγραφούν ως ένα ευρύ φάσμα μέτρων για τη διασφάλιση της ιδιωτικότητας των χρηστών ηλεκτρονικών υπηρεσιών. Ορισμένες από αυτές τις τεχνολογίες, όπως η κρυπτογράφηση δεδομένων και μηνυμάτων που ανταλλάσσονται μεταξύ δύο οντοτήτων, έχουν ήδη διερευνηθεί εκτενώς τις τελευταίες δεκαετίες. Ωστόσο, ελάχιστη έρευνα έχει γίνει μέχρι στιγμής για τον σχεδιασμό πληροφοριακών συστημάτων κατά τρόπο τέτοιο ώστε να εξασφαλίζουν την προστασία της ιδιωτικότητας των χρηστών εξαρχής.

Στόχος της παρούσας διδακτορικής διατριβής είναι η μελέτη του προβλήματος διασφάλισης ιδιωτικότητας σε συστήματα μεγάλης κλίμακας, όπου μεγάλου όγκου ετερογενή δεδομένα παράγονται καθημερινά, τόσο από ανθρώπους όσο και από μηχανές. Συγκεκριμένα, αναλύονται οι προκλήσεις που περιλαμβάνει το προαναφερθέν ζήτημα, εστιάζοντας στα ιδιαίτερα χαρακτηριστικά των παραπάνω συστημάτων, όπως επίσης και στις αδυναμίες υφιστάμενων λύσεων. Επιπρόσθετα, παρουσιάζεται σε γενικές γραμμές το ισχύον αλλά και το επικείμενο νομικό και κανονιστικό πλαίσιο αναφορικά με την προστασία προσωπικών δεδομένων, τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση, ούτως ώστε να εξαχθούν οι σχετικές απαιτήσεις που αφορούν στην προδιαγραφή της προσέγγισης που ακολουθείται. Η προσέγγιση αυτή συνδυάζει διάφορες τεχνολογίες PET σε μία αρχιτεκτονική ασφαλούς συστήματος με επίγνωση της ιδιωτικότητας.

1.1 Κίνητρα και Προσέγγιση

Στη συνέχεια του παρόντος κεφαλαίου αναλύονται τα κίνητρα που οδήγησαν στον σχεδιασμό και στην ανάπτυξη του εν λόγω ασφαλούς συστήματος με επίγνωση της ιδιωτικότητας. Τα κίνητρα αυτά αφορούν τόσο στις αδυναμίες των μεθοδολογιών που εφαρμόζουν τα τρέχοντα συστήματα διαχείρισης παραγωγής, ηλεκτρονικής διακυβέρνησης και βελτίωσης της ευημερίας του ατόμου, όσο και στα περιθώρια βελτίωσής τους υιοθετώντας καινοτόμους μηχανισμούς ασφάλειας και προστασίας των δεδομένων.

1.1.1 Ιδιωτικότητα

Η *Ιδιωτικότητα* (Privacy) μπορεί να οριστεί ως "ο ισχυρισμός των ατόμων [...] για να αποφασίσουν για τον εαυτό τους πότε, πώς και σε ποιο βαθμό οι πληροφορίες σχετικά με τους ίδιους μεταδίδονται σε άλλους" [5]. Η ιδιωτικότητα αποτελεί ένα βασικό ανθρώπινο δικαίωμα που ορίζεται σε πολυάριθμους νόμους και κανονισμούς. Το 1995, το Ευρωπαϊκό Κοινοβούλιο εξέδωσε την Οδηγία 95/46/ΕΚ [6] για την προστασία των δεδομένων βάσει της Ευρωπαϊκής Σύμβασης των Ανθρώπινων Δικαιωμάτων (Άρθρο 8) [7] και κάθε ευρωπαϊκό κράτος-μέλος έπρεπε να μεταφράσει την προαναφερθείσα οδηγία σε εθνική νομοθεσία για την προστασία της ιδιωτικότητας. Καθώς, όμως, κάθε κράτος έπρεπε να παράξει δικούς του νόμους βάσει της συγκεκριμένης οδηγίας, υπήρξαν κάποιες μικρές διαφορές στους αντίστοιχους νόμους κάθε χώρας, με αποτέλεσμα μία πολυεθνική επιχείρηση, για παράδειγμα, να πρέπει να συμμορφωθεί με διαφορετικούς κανονισμούς σε κάθε ευρωπαϊκή χώρα. Έτσι, προκειμένου να αντιμετωπιστεί το πρόβλημα αυτό, το Ευρωπαϊκό Κοινοβούλιο δημιούργησε τον *Γενικό Κανονισμό για την Προστασία Δεδομένων* (GDPR). Όταν ο κανονισμός αυτός επιβληθεί στις 25 Μαΐου 2018, όλες οι εθνικές νομοθεσίες για την προστασία των προσωπικών δεδομένων των πολιτών των ευρωπαϊκών κρατώνμελών θα αντικατασταθούν άμεσα και επομένως θα εξαλειφθεί το προαναφερθέν πρόβλημα. Δεδομένου ότι κάθε φορά που ορίζονται νέοι κανονισμοί τείνουν να είναι πιο αυστηροί, η συμμόρφωση με αυτούς αποτελεί αδιαμφισβήτητα μία μεγάλη πρόκληση.

Μια σημαντική πτυχή της ιδιωτικότητας, ιδίως όταν λαμβάνεται υπόψη η μαζική αύξηση της ψηφιακής επεξεργασίας δεδομένων κατά τα προηγούμενα έτη, είναι η προστασία των προσωπικών δεδομένων. Στις μέρες μας, η προστασία δεδομένων συνιστά ένα περίπλοκο ζήτημα, κυρίως επειδή είναι ιδιαίτερα δύσκολο να μεταφραστούν οι νομικές απαιτήσεις των κανονισμών σε τεχνικές απαιτήσεις λογισμικού και υλικού για τα πληροφοριακά συστήματα και τις υποκείμενες επιχειρησιακές διαδικασίες. Επιπλέον, οι νόμοι για την προστασία της ιδιωτικότητας δεν είναι απλά ένα σύνολο κανόνων, καθώς δίνουν πολλά περιθώρια ερμηνείας. Ιστορικά, η προστασία

των δεδομένων καλυπτόταν ως επί το πλείστον από τον τομέα Ασφάλειας Πληροφοριακών Συστημάτων. Ωστόσο, η προστασία της ιδιωτικότητας απαιτεί μια ευρύτερη και πιο ολοκληρωμένη προσέγγιση. Πέραν τούτου, είναι επίσης σημαντικό να εξασφαλισθεί η προστασία των φυσικών μέσων που συνιστούν πηγές δεδομένων (π.χ. προστασία φορητών υπολογιστών και κέντρων δεδομένων), πέρα από την ύπαρξη νομικής βάσης για την επεξεργασία δεδομένων, καθώς και μέτρων για την αποφυγή διαρροής δεδομένων εξαιτίας ανθρώπινου σφάλματος. Η προστασία των προσωπικών δεδομένων αποτελεί ένα επίκαιρο θέμα παγκοσμίως και τα όποια μέτρα λαμβάνονται είναι για να παρακινήσουν οργανισμούς και επιχειρήσεις να επανεξετάσουν τον τρόπο επεξεργασίας αυτών, καθώς και να λάβουν προληπτικά μέτρα για τη διασφάλιση της προστασίας τους [8].

1.1.1.1 Ορισμοί

Στο σημείο αυτό, είναι ιδιαίτερα σημαντικό να παρατεθούν οι ορισμοί συγκεκριμένων εννοιών, όπως αυτές ορίζονται από νομικής απόψεως. Οι παρακάτω περιγραφές των εννοιών αυτών συμβάλλουν στην κατανόηση του τρόπου με τον οποίο αυτές χρησιμοποιούνται σε ένα νομικό πλαίσιο, βάσει του Εγχειριδίου Ιδιωτικότητας και Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας [9], καθώς και της Οδηγίας 95/46/ΕΚ.

- **Υποκείμενο των δεδομένων** (data subject): φυσικό ή νομικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα.
- **Προσωπικά δεδομένα** (personal data): οποιαδήποτε πληροφορία σχετικά με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ένα ταυτοποιήσιμο άτομο μπορεί να αναγνωριστεί, είτε άμεσα είτε έμμεσα, μέσω ενός αριθμού ταυτοποίησης ή βάσει ενός ή περισσοτέρων χαρακτηριστικών του που είναι συγκεκριμένα για τη φυσική, πνευματική, οικονομική, πολιτιστική ή κοινωνική του ταυτότητα. Ένα άτομο είναι άμεσα ταυτοποιήσιμο όταν, βάσει του διαθέσιμου συνόλου δεδομένων, ένα φυσικό πρόσωπο μπορεί να συσχετιστεί με τα δεδομένα αυτά. Ένα άτομο είναι έμμεσα ταυτοποιήσιμο όταν χρειάζεται να πραγματοποιηθούν ορισμένα βήματα προκειμένου να συσχετιστεί ένα φυσικό πρόσωπο με το σύνολο της διαθέσιμης πληροφορίας. Μία τέτοια διαδικασία μπορεί να περιλαμβάνει τη σύνθεση νέας πληροφορίας με βάση την ήδη διαθέσιμη πληροφορία για το άτομο αυτό, καθώς και τον συνδυασμό άλλων πηγών δεδομένων. Για παράδειγμα, η ημερομηνία γέννησης ενός ατόμου και το επώνυμό του μπορεί να αρκούν για τη συσχέτιση ενός φυσικού προσώπου με τα δεδομένα αυτά.
- **Ανωνυμοποίηση δεδομένων** (data anonymisation): μια μη αναστρέψιμη διαδικασία τροποποίησης δεδομένων κατά τρόπο τέτοιο ώστε τα προκύπτοντα δεδομένα να μην είναι άμεσα ή έμμεσα συνδεδεμένα με ένα άτομο.
- **Επεξεργασία δεδομένων προσωπικού χαρακτήρα** (personal data processing):

κάθε πράξη ή σύνολο πράξεων που εκτελείται σε προσωπικά δεδομένα, με αυτοματοποιημένο ή μη τρόπο, όπως είναι η συλλογή, η αποθήκευση, η οργάνωση, η καταγραφή, η προσαρμογή, η τροποποίηση, η ανάκτηση, η διαβούλευση, η χρήση, η αποκάλυψη μέσω διαβίβασης, διάδοσης ή άλλης διάθεσης, η συσχέτιση, ο αποκλεισμός, η διαγραφή ή η καταστροφή προσωπικών δεδομένων.

- **Επιχειρησιακή διαδικασία** (business process): η δομημένη συλλογή σχετικών ενεργειών που παράγουν ένα συγκεκριμένο αποτέλεσμα από συγκεκριμένα στοιχεία εισόδου. Μια επιχειρησιακή διαδικασία είτε απαιτεί προσωπικά δεδομένα για την εκκίνησή της είτε χρησιμοποιούνται προσωπικά δεδομένα κατά τη διάρκεια αυτής.

1.1.1.2 Τρέχον Νομικό και Κανονιστικό Πλαίσιο

Όπως αναφέρθηκε παραπάνω, επί του παρόντος, όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης (Ε.Ε.) έχουν ορίσει και τηρούν δικούς τους κανονισμούς για την προστασία της ιδιωτικότητας βάσει της Οδηγίας 95/46/ΕΚ της Ε.Ε. Επομένως, οι κανονισμοί αυτοί είναι πιθανόν να διαφέρουν ανά χώρα. Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ εφαρμόζεται σε όλες τις (ημι-)αυτοματοποιημένες ή μη διαδικασίες επεξεργασίας δεδομένων από έναν φορέα (είτε είναι ιδιωτικός, είτε δημόσιος, είτε μη-κερδοσκοπικού χαρακτήρα οργανισμός) εκτός των τομέων της δημόσιας ασφάλειας, της άμυνας και της κρατικής ασφάλειας. Η οδηγία αυτή όριζει κατά πόσο είναι νόμιμη η επεξεργασία δεδομένων, όπου και θα πρέπει να ισχύει μία από τις ακόλουθες περιπτώσεις:

- Το υποκείμενο των δεδομένων έχει δώσει ρητή άδεια να επεξεργαστεί κάποιος τα δεδομένα του.
- Απαιτείται επεξεργασία δεδομένων για την εκτέλεση μιας υπηρεσίας με σκοπό την ικανοποίηση αιτήματος του υποκειμένου των δεδομένων. Το πρόσωπο στο οποίο αναφέρονται τα δεδομένα θα πρέπει να έχει συμφωνήσει ρητά για τη χρήση αυτής της υπηρεσίας.
- Η επεξεργασία δεδομένων απαιτείται για την ολοκλήρωση μιας διαδικασίας για το δημόσιο συμφέρον ή κατόπιν αιτήματος δημόσιας αρχής.

Η οδηγία ορίζει, επίσης, ότι η επεξεργασία δεδομένων πρέπει να είναι δίκαιη και νόμιμη, πράγμα που σημαίνει ότι πρέπει να υπάρχει μια νομική βάση για την επεξεργασία των δεδομένων και τα δεδομένα πρέπει να έχουν συγκεκριμένη ποιότητα, να χρησιμοποιούνται επαρκώς και να καταστρέφονται. Επιπλέον, ορίζεται ότι το υποκείμενο των δεδομένων έχει ορισμένα δικαιώματα και συγκεκριμένα:

- **Δικαίωμα απόκτησης πληροφορίας**: Ο οργανισμός που είναι αρμόδιος για την επεξεργασία δεδομένων πρέπει να παρέχει στο υποκείμενο των δεδομένων πληροφορίες σχετικά με την επεξεργασία, όπως: η προέλευση των δεδομένων που συλλέγονται, ποιος επεξεργάζεται τα δεδομένα, ποιος είναι ο σκοπός της

επεξεργασίας κ.λπ.

- **Δικαίωμα πρόσβασης στα δεδομένα**: Το υποκείμενο των δεδομένων μπορεί να ζητήσει από έναν οργανισμό να παράσχει σε αυτόν όλες τις πληροφορίες που έχει στη διάθεσή του ο τελευταίος και σχετίζονται με τον πρώτο.
- **Δικαίωμα άρνησης επεξεργασίας δεδομένων**: Το υποκείμενο των δεδομένων μπορεί να αρνηθεί να δώσει την άδειά του για την επεξεργασία των δεδομένων του, εφόσον αυτό δεν έρχεται σε αντίθεση με άλλους κανονισμούς.
- **Δικαίωμα τροποποίησης**: Το υποκείμενο των δεδομένων μπορεί να ζητήσει να τροποποιήσει ή να ενημερώσει τα δεδομένα του.

Επιπρόσθετα, οι οργανισμοί πρέπει να λαμβάνουν επαρκή μέτρα για να αποτρέψουν την παράνομη πρόσβαση σε δεδομένα. Επιπλέον, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται επαρκώς κατά την επεξεργασία των δεδομένων του και τα δεδομένα πρέπει να χρησιμοποιούνται μόνο για τον σκοπό για τον οποίο προορίστηκαν αρχικά. Τέλος, σύμφωνα με τους κανόνες της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ, η αρμόδια αρχή κάθε κράτους μέλους της Ε.Ε. επιβάλλει επιπρόσθετα μέτρα σε περίπτωση διαρροής δεδομένων.

1.1.1.3 Γενικός Κανονισμός για την Προστασία Δεδομένων

Από τον Απρίλιο του 2016, ο *Γενικός Κανονισμός για την Προστασία Δεδομένων* (GDPR) (Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016) ψηφίστηκε και αντικατέστησε την Οδηγία 95/46/ΕΚ και τις εθνικές νομοθεσίες για την προστασία των δεδομένων. Ο κανονισμός GDPR αφορά όλες τις εταιρείες, τους οργανισμούς αλλά και τους δημόσιους κυβερνητικούς φορείς που επεξεργάζονται δεδομένα των πολιτών της Ευρωπαϊκής Ένωσης. Ο κανονισμός αυτός δεν χρειάζεται να μεταφραστεί σε εθνικές νομοθεσίες, καθώς είναι άμεσα εφαρμόσιμος σε όλα τα κράτη-μέλη της Ε.Ε. Οι ευρωπαϊκές εταιρείες και οργανισμοί είχαν στη διάθεσή του συνολικά σχεδόν δύο χρόνια, από τον Απρίλιο του 2016 μέχρι τον Μάιο του 2018, για να αλλάξουν τις πολιτικές τους σχετικά με τη διασφάλιση ιδιωτικότητας, να τροποποιήσουν κατάλληλα τα πληροφοριακά τους συστήματα, καθώς και τις επιχειρησιακές τους διαδικασίες, ώστε όλα τα προαναφερθέντα να συμμορφώνονται με τον νέο κανονισμό. Ορισμένες σημαντικές αλλαγές του νέου κανονισμού σε σύγκριση με την προηγούμενη ισχύουσα νομοθεσία στην Ευρώπη είναι οι εξής:

- Ο κανονισμός GDPR είναι ένας νόμος της Ε.Ε. Συνεπώς, όλα τα κράτη-μέλη της Ε.Ε. έχουν την ίδια νομοθεσία όσον αφορά την προστασία της ιδιωτικότητας των πολιτών.
- Οι ενδιαφερόμενοι (πελάτες και υπάλληλοι) ενός οργανισμού έχουν το δικαίωμα "να λησμονηθούν"· οι οργανισμοί πρέπει να αναγνωρίσουν αυτό το δικαίωμα και να εφαρμόσουν τις αντίστοιχες πολιτικές και διαδικασίες για την

αντιμετώπιση αιτημάτων που πρέπει "να λησμονούνται".

- Οι οργανισμοί με 250 ή περισσότερους υπαλλήλους πρέπει να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer - DPO).
- Οι διαρροές δεδομένων πρέπει να δηλώνονται εντός 24 ωρών στην εθνική Αρχή Προστασίας Δεδομένων.
- Τα ανεπαρκή μέτρα προστασίας των δεδομένων μπορούν να οδηγήσουν σε πρόστιμα που ανέρχονται στις δύο εκατοστιαίες μονάδες του παγκόσμιου κύκλου εργασιών ή σε 10.000.000 €. Η Αρχή Προστασίας Δεδομένων μπορεί, επίσης, να αναστείλει τη λειτουργία μίας εταιρείας, έως ότου η εταιρεία αυτή συμμορφωθεί με τον νέο κανονισμό GDPR.

Όπως φαίνεται από τα παραπάνω, ο νέος κανονισμός για την προστασία δεδομένων επιβάλλει αυστηρότερες πολιτικές και κανόνες σε σχέση με την προηγουμένως ισχύουσα νομοθεσία. Επίσης, παρέχει πλέον στις Αρχές Προστασίας Δεδομένων τη δυνατότητα να επιβάλουν πολύ υψηλότερα πρόστιμα σε σχέση με παλαιότερα. Όπως αναφέρθηκε και προηγουμένως, όλοι οι φορείς και οι οργανισμοί πρέπει μέχρι τον Μάιο του 2018, όπου και θα τεθεί σε εφαρμογή ο κανονισμός, να προσαρμόσουν το σύστημά τους κατάλληλα, έτσι ώστε αυτό να ικανοποιεί πλήρως τις απαιτήσεις του κανονισμού GDPR. Δεδομένου ότι ο νέος κανονισμός επιβλήθηκε τον Ιούλιο του 2016, δύο χρόνια για την προσαρμογή όλων των επιχειρησιακών διαδικασιών και των πληροφοριακών συστημάτων των ευρωπαϊκών οργανισμών στον νέο κανονισμό μπορούν να θεωρηθούν ως μικρή χρονική περίοδος. Τα ήδη υπάρχοντα συστήματα πρέπει να αξιολογηθούν ως προς τη συμμόρφωσή τους με τον κανονισμό και, αναλόγως, να συνταχθεί μια πρόταση σχετικά με τις απαιτούμενες αλλαγές στα συστήματα αυτά, συμπεριλαμβανομένων τόσο των τεχνικών αλλαγών στην αρχιτεκτονική τους όσο και των αλλαγών που πρέπει να γίνουν σε οργανωτικό επίπεδο. Κατόπιν τούτου, πρέπει να ξεκινήσει η εκπόνηση του έργου τροποποίησης συστημάτων και διαδικασιών και, τελικά, οι αλλαγές που θα πραγματοποιηθούν πρέπει να ελεγχθούν εκτενώς, να εκτιμηθούν ως προς τη συμμόρφωση και αναλόγως να υιοθετηθούν. Η διαδικασία αυτή θα μπορούσε να είναι μακροχρόνια και είναι γεγονός ότι, πλέον, η τήρηση της προαναφερθείσας προθεσμίας αποτελεί πρόκληση.

1.1.2 Κατανεμημένα Συστήματα Μεγάλης Κλίμακας

Συνδυάζοντας τους ορισμούς που έχουν αποδοθεί στον όρο αυτό από πολλούς συγγραφείς [10][11][12], ένα κατανεμημένο σύστημα μπορεί να ορισθεί ως *μια εφαρμογή που επικοινωνεί με πληθώρα κατανεμημένου υλικού και λογισμικού για τον συντονισμό, μέσω ενός δικτύου επικοινωνίας, των ενεργειών πολλαπλών διεργασιών που εκτελούνται σε ετερογενείς και αυτόνομους υπολογιστές, έτσι ώστε όλες οι επιμέρους οντότητες να συνεργάζονται για να εκτελέσουν ένα σύνολο συναφών εργασιών προκειμένου να εκπληρώσουν έναν κοινό στόχο*. Η κατανομή μπορεί να είναι φυσική

(σε μια γεωγραφική περιοχή) ή/και λογική (σε έναν εικονικό χώρο). Συχνά αναπαρίσταται ως ένα συνδεδεμένο γράφημα, οι κόμβοι του οποίου αντιστοιχούν σε υπολογιστές ή διεργασίες και οι ακμές σε κανάλια αμφίδρομης επικοινωνίας ή σε συνδέσεις. Τα συστήματα αυτά έχουν σχεδιαστεί με στόχο την επίτευξη των ακόλουθων ιδιοτήτων: διαφάνεια, ανοικτότητα, αξιοπιστία, απόδοση και επεκτασιμότητα [12]. Προκειμένου να επιτευχθούν οι παραπάνω στόχοι, πρέπει να δοθεί η απαραίτητη προσοχή στην ασφάλεια του εκάστοτε κατανεμημένου συστήματος. Η ενσωμάτωση διαφόρων κατανεμημένων οντοτήτων σε ένα σύστημα δημιουργεί πολλά θέματα ασφάλειας, δεδομένου ότι υπολογιστικά νέφη, έξυπνες συσκευές, ετερογενή δίκτυα και συνεργατικοί σχηματισμοί υπολογιστών συνιστούν ένα κατανεμημένο σύστημα.

Τα κατανεμημένα συστήματα εμφανίζουν γενικά τα εξής χαρακτηριστικά [13]:

- Αυξημένη απόδοση: η ύπαρξη πολλών κόμβων σε ένα κατανεμημένο σύστημα επιτρέπει την παράλληλη επεξεργασία αιτημάτων, βελτιώνοντας έτσι τη συνολική απόδοση του συστήματος.
- Κοινή χρήση πόρων: τα κατανεμημένα συστήματα επιτρέπουν την αποτελεσματική πρόσβαση από όλους τους χρήστες σε διάφορους πόρους του συστήματος, όπως διακομιστές βάσεων δεδομένων, πολυμεσικού περιεχομένου, εικονικής πραγματικότητας κ.ο.κ.
- Αυξημένη επεκτασιμότητα: τα κατανεμημένα συστήματα είναι σχεδιασμένα με τρόπο τέτοιο ώστε να είναι προσαρμόσιμα, παραμετροποιήσιμα και επεκτάσιμα. Ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής σε υπολογιστική ισχύ και χωρητικότητα, ένα κατανεμημένο σύστημα μπορεί να ρυθμιστεί ώστε να περιλαμβάνει τον αναγκαίο αριθμό κόμβων και πόρων.
- Αύξηση της αξιοπιστίας, της διαθεσιμότητας και της ανοχής σε σφάλματα: η συγκέντρωση πολλών υπολογιστικών και αποθηκευτικών πόρων σε ένα κατανεμημένο σύστημα το καθιστά αποδοτικό από πλευράς κόστους, καθώς κάποιο σφάλμα σε έναν κόμβο μπορεί να αντιμετωπιστεί άμεσα αναθέτοντας τις εργασίες του σε άλλον διαθέσιμο.

Ο σχεδιασμός ενός κατανεμημένου συστήματος θεωρείται μια πολύπλοκη διαδικασία. Με την επέκταση του εύρους και της κλίμακας των κατανεμημένων συστημάτων και εφαρμογών, είναι πιθανό οι σχεδιαστές των συστημάτων αυτών να συναντήσουν διαφορετικές προκλήσεις [14][15], όπως:

- **Ετερογένεια** (heterogeneity): τα κατανεμημένα συστήματα επιτρέπουν στους χρήστες τους να έχουν πρόσβαση σε υπηρεσίες και να εκτελούν εφαρμογές μέσω ενός συνόλου ετερογενών υπολογιστών και δικτύων, συμπεριλαμβανομένων υλικού, λειτουργικών συστημάτων, γλωσσών προγραμματισμού κ.α.
- **Ανοικτότητα** (openness): το κατά πόσο ένα σύστημα είναι ανοικτό καθορίζει εάν αυτό μπορεί να επεκταθεί και να χρησιμοποιηθεί εκ νέου με διάφορους τρό-

που μέσω της διάθεσης ανοικτών διεπαφών σε προγραμματιστές λογισμικού, δίνοντας τη δυνατότητα να αναπτυχθούν έτσι νέες υπηρεσίες κοινής χρήσης πόρων του συστήματος και να διατεθούν προς χρήση μέσω ποικίλων προγραμμάτων πελατών.

- **Κλιμακωσιμότητα** (scalability): τα κατανεμημένα συστήματα λειτουργούν αποτελεσματικά και αποδοτικά σε πολλές και διαφορετικές κλίμακες, από ένα μικρό τοπικό δίκτυο έως το Διαδίκτυο. Ένα σύστημα θεωρείται κλιμακώσιμο μόνο εάν παραμείνει αποδοτικό όταν σημειωθεί σημαντική αύξηση του αριθμού των πόρων και των χρηστών του.
- **Διαφάνεια κατανομής** (distribution transparency): η διαφάνεια κατανομής ορίζεται ως η απόκρυψη από τον χρήστη και τον προγραμματιστή εφαρμογών των επιμέρους στοιχείων ενός κατανεμημένου συστήματος.
- **Χρονοπρογραμματισμός** (scheduling): η οργάνωση αποκεντρωμένων χρονοπρογραμματιστών καταργεί τους περιορισμούς της κεντρικής οργάνωσης όσον αφορά την ανοχή σφάλματος, την κλιμακωσιμότητα και την αυτονομία, αλλά δημιουργεί προκλήσεις στη διαχείριση της κατανεμημένης πληροφορίας, στον συντονισμό του συστήματος, στην ασφάλεια, στην αυθεντικοποίηση των χρηστών και στην ετερογένεια των πολιτικών του παρόχου πόρων.
- **Ασφάλεια και εμπιστοσύνη** (security and trust): πολλές από τις πηγές δεδομένων που διατίθενται και διατηρούνται σε κατανεμημένα συστήματα έχουν υψηλή αξία για τους χρήστες τους. Επομένως, η αποκεντρωμένη οργάνωση κατανεμημένων συστημάτων εγείρει σοβαρές προκλήσεις στους τομείς διαχείρισης της ασφάλειας και της εμπιστοσύνης.
- **Ιδιωτικότητα** (privacy): η προστασία προσωπικών και μη δεδομένων αποτελεί ένα ακόμη κρίσιμο ζήτημα των κατανεμημένων συστημάτων, λόγω του γεγονότος ότι τα δεδομένα των χρηστών και η επιχειρησιακή λογική βρίσκονται κατανεμημένα στους διακομιστές του συστήματος. Επομένως, υπάρχει ο κίνδυνος να αποκαλυφθούν εμπιστευτικά δεδομένα (π.χ. οικονομικά δεδομένα, ιατρικά αρχεία κ.α.) ή προσωπικές πληροφορίες (π.χ. προσωπικό προφίλ) σε μη εξουσιοδοτημένες οντότητες. Επομένως, οι χρήστες ενός κατανεμημένου συστήματος πρέπει να εγγυηθούν ότι τα δεδομένα τους προστατεύονται κατάλληλα.

Συνεπώς, η εφαρμογή ενός ασφαλούς κατανεμημένου συστήματος απαιτεί λύσεις που μπορούν να αντιμετωπίσουν αποτελεσματικά διάφορα ζητήματα ασφάλειας.

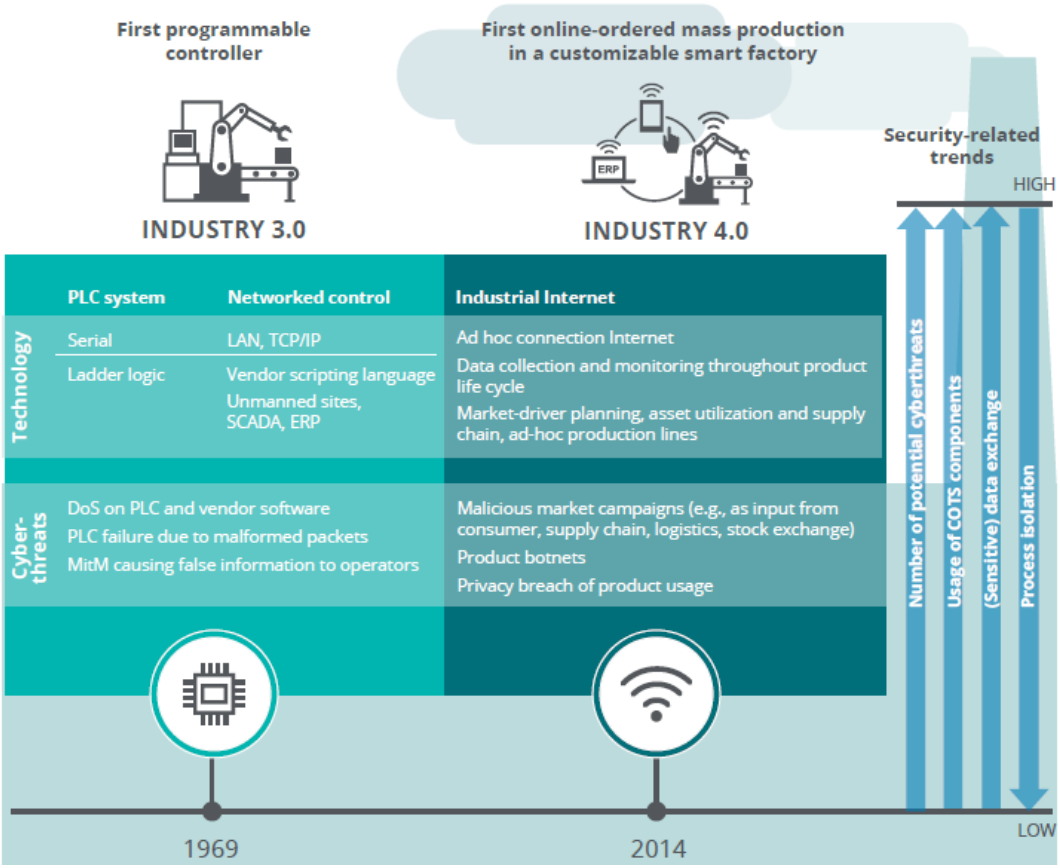
1.1.3 Προκλήσεις

Η ασφάλεια των κατανεμημένων συστημάτων παρέχει μια ολιστική εικόνα των σημερινών ζητημάτων ασφάλειας, των απαιτούμενων διαδικασιών και λύσεων. Στη συγκεκριμένη υποενότητα, εξετάζονται τρεις τομείς στους οποίους βρίσκουν εφαρμογή κατανεμημένα συστήματα, προκειμένου να αναλυθούν λεπτομερώς οι εμπλε-

κόμενες τεχνολογίες και να εξαχθούν οι αντίστοιχες απαιτήσεις ασφάλειας βάσει των οποίων προδιαγράφηκε η προσέγγιση της παρούσας διδακτορικής διατριβής.

1.1.3.1 Διαχείριση Παραγωγής

Στις μέρες μας, ο βιομηχανικός τομέας αντιμετωπίζει πολλές προκλήσεις όσον αφορά στην ασφάλεια των πληροφοριακών συστημάτων που χρησιμοποιούνται για τον έλεγχο και τη διεκπεραίωση πολλών επιχειρησιακών διαδικασιών. Οι επιθέσεις από κακόβουλα άτομα ή κακόβουλο λογισμικό επηρεάζουν, είτε έμμεσα είτε άμεσα, την ποιότητα των προϊόντων και της παραγωγής, τα έσοδα από τις πωλήσεις, τη φήμη μίας επιχείρησης ή ακόμα και την ασφάλεια ανθρώπινων ζωών. Στην προσπάθεια βελτίωσης των υποκείμενων διαδικασιών λήψης αποφάσεων πραγματικού χρόνου και προγραμματισμού των διαδικασιών παραγωγής, η υιοθέτηση προηγμένων τεχνολογικών τάσεων για την επίτευξη του οράματος *Industrie 4.0*, όπως η Κινητή Υπολογιστική, η χρήση φορητών συσκευών και το Διαδίκτυο των Πραγμάτων, έχει αυξήσει τις αδυναμίες των συστημάτων που αξιοποιούνται στον τομέα αυτό (Σχήμα 1).



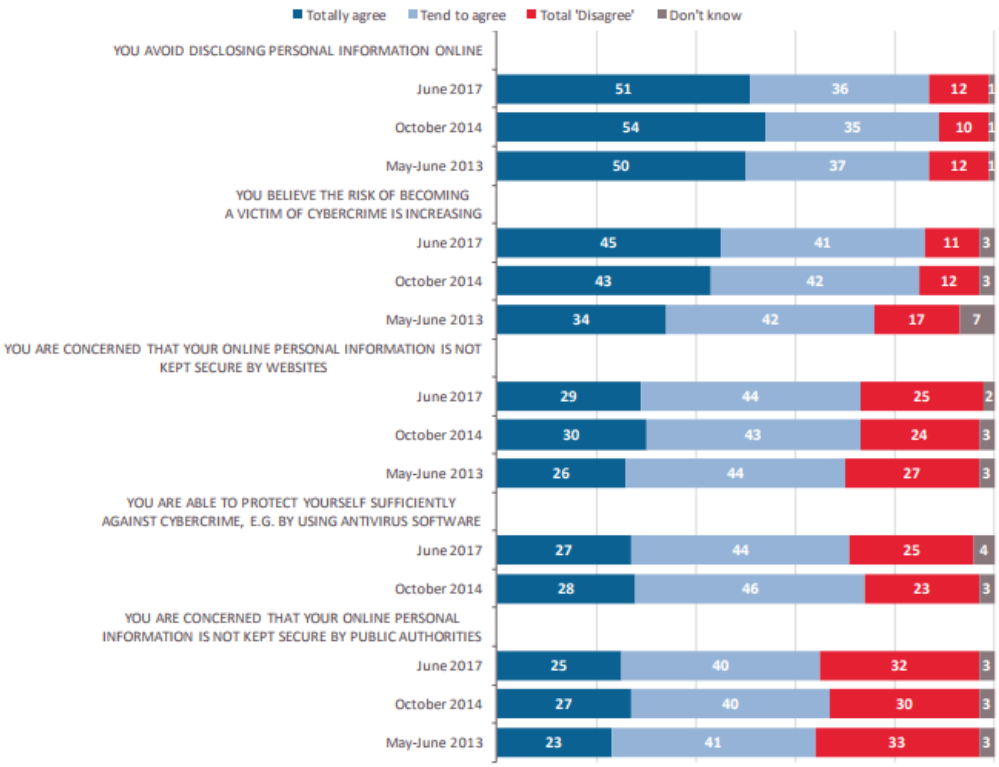
Σχήμα 1: Εξέλιξη των Τεχνολογιών και των Αντίστοιχων Απειλών Ασφάλειας στα Συστήματα Διαχείρισης Παραγωγής [1]

Η προστασία των επιχειρησιακών δεδομένων αποτελεί μία ακόμη πρόκληση, δεδομένου του ιδιαίτερα ανταγωνιστικού περιβάλλοντος στο οποίο δρουν οι σημερινές επιχειρήσεις και βιομηχανίες. Η αποκάλυψη επιχειρησιακών ή και κρίσιμων για την παραγωγή δεδομένων σε ανταγωνιστικές επιχειρίσεις έχει έμμεσες επιπτώσεις στην παραγωγή, καθώς μπορεί να προκαλέσει απώλεια ανταγωνιστικού πλεονεκτήματος και συνάφειας με την αγορά. Συνεπώς, η προστασία των δεδομένων και η διασφάλιση εμπιστευτικότητας είναι ζωτικής σημασίας και στον βιομηχανικό τομέα για την ανταγωνιστικότητα μιας επιχείρησης.

1.1.3.2 Ηλεκτρονική Διακυβέρνηση

Η ηλεκτρονική διακυβέρνηση μπορεί να εξασφαλίσει την αποτελεσματικότητα και τη διαφάνεια κυβερνητικών διαδικασιών και υπηρεσιών. Μέσω της χρήσης Τεχνολογιών Πληροφορίας και Επικοινωνίας, η ηλεκτρονική διακυβέρνηση επιτρέπει σε δημόσιους οργανισμούς να παρέχουν ηλεκτρονικές υπηρεσίες σε πραγματικό χρόνο στους πολίτες. Δεδομένου ότι η ηλεκτρονική συνεργασία μεταξύ δημόσιων υπηρεσιών και οι ηλεκτρονικές συναλλαγές προϋποθέτουν και απαιτούν τη χρήση και διακίνηση μεταξύ άλλων και προσωπικών πληροφοριών και ευαίσθητων προσωπικών τους δεδομένων, μία από τις μεγαλύτερες ανησυχίες των πολιτών και χρηστών των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι η προστασία της ιδιωτικότητάς τους και η διατήρηση του ελέγχου των προσωπικών τους δεδομένων (Σχήμα 2). Λαμβάνοντας υπόψη τη συγκέντρωση σημαντικού όγκου πληροφοριών για κάθε πολίτη, πιθανή αποκάλυψη αυτών μπορεί να οδηγήσει στην ταυτοποίησή του και στην παραβίαση της ιδιωτικότητάς του. Είναι προφανές, λοιπόν, ότι το ζήτημα προστασίας των δεδομένων των πολιτών είναι ιδιαίτερης βαρύτητας, καθώς ο τρόπος και το επίπεδο επίλυσής του επηρεάζει την αποτελεσματικότητα των υπηρεσιών αυτών.

Οι υπηρεσίες ηλεκτρονικής διακυβέρνησης χαρακτηρίζονται από κάποια ιδιαίτερα στοιχεία που τις διαφοροποιούν από άλλες ηλεκτρονικές υπηρεσίες σε ό,τι αφορά το θέμα της προστασίας της ιδιωτικότητας και συγκεκριμένα: (α) πολλά από τα δεδομένα που εμπλέκονται σε συναλλαγές υπηρεσιών ηλεκτρονικής διακυβέρνησης χαρακτηρίζονται από υψηλό βαθμό ευαισθησίας, όπως οικονομικά και φορολογικά δεδομένα, δεδομένα υγείας, ποινικό μητρώο κ.λπ.· (β) η συνδεσιμότητα μεταξύ των δεδομένων που χρησιμοποιούνται από υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι άμεση, καθώς ορισμένοι τύποι δεδομένων αποτελούν ταυτοποιητικά στοιχεία του ατόμου, όπως ο αριθμός δελτίου ταυτότητας, ο αριθμός φορολογικού μητρώου κ.ο.κ.· (γ) οι υποκείμενες διαδικασίες ηλεκτρονικής διακυβέρνησης δημιουργούν πολύπλοκες ροές εργασιών και δεδομένων, καθώς απαιτούν τη συλλογή δεδομένων ή/και την αλληλεπίδραση πολλαπλών ετερογενών φορέων και αντίστοιχα την ανταλλαγή, τον συσχετισμό και τον διαμοιρασμό δεδομένων και αρχείων· (δ) οι ροές εργασιών και δεδομένων είναι δυνατόν να ξεφεύγουν από τα διοικητικά και διαχειριστικά σύνορα



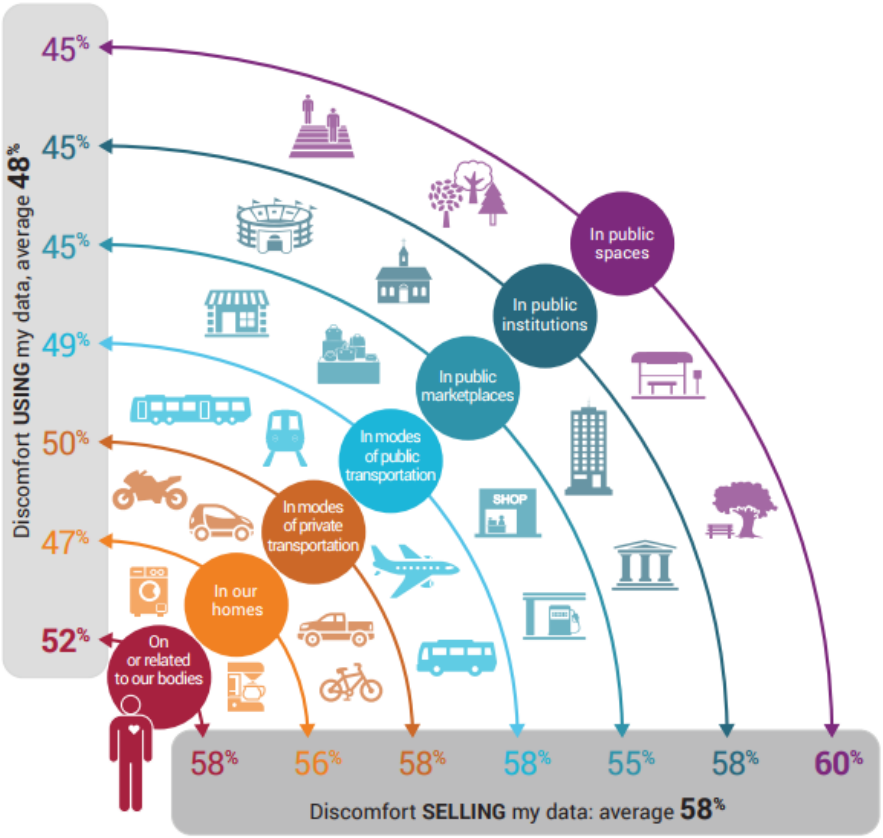
Σχήμα 2: Στάση των Ευρωπαίων Πολιτών σε Θέματα Προστασίας της Ιδιωτικότητας [2]

μίας χώρας· (ε) η χρήση ενός μοναδικού σημείου πρόσβασης στις υπηρεσίες ηλεκτρονικής διακυβέρνησης μέσω μίας κεντρικής διαδικτυακής πύλης δημιουργεί επιπλέον ζητήματα προστασίας δεδομένων, καθώς η πύλη αυτή καθαυτή παίζει το ρόλο ενός διαμεσολαβητή ο οποίος αναλαμβάνει να διατηρεί διάφορους τύπους δεδομένων, προκειμένου να διευκολυνθούν διαδικασίες όπως η ταυτοποίηση των πολιτών· (στ) σε πολλές περιπτώσεις, δημιουργούνται αντιθέσεις μεταξύ του υφιστάμενου νομοθετικού πλαισίου περί της προστασίας προσωπικών δεδομένων και εκείνου που διέπει τις διαδικασίες διακυβέρνησης. Συνεπώς, κρίνεται επιτακτική η ανάγκη ανάπτυξης και χρήσης τεχνολογιών ασφάλειας και προστασίας προσωπικών δεδομένων που λαμβάνουν υπόψη τα ιδιαίτερα χαρακτηριστικά των υπηρεσιών ηλεκτρονικής διακυβέρνησης, με τελικό στόχο την επίλυση όλων των ζητημάτων ιδιωτικότητας που αναφέρθηκαν παραπάνω.

1.1.3.3 Διαδίκτυο των Πραγμάτων

Ο συνεχώς αυξανόμενος ρυθμός με τον οποίο «εισβάλλουν» στη ζωή μας προσωπικές – φορητές και μη – έξυπνες συσκευές και εφαρμογές (π.χ. έξυπνες εφαρμογές κινητού τηλεφώνου, ενδυτές συσκευές, έξυπνες συσκευές στον περιβάλλοντα χώρο του ατόμου) έχει καταστήσει δυνατή τη διαρκή παρακολούθηση των συνηθειών

και των ζωτικών παραμέτρων υγείας των ανθρώπων, με απώτερο σκοπό την αξιολόγηση των συνθηκών διαβίωσής τους και τη βελτίωση της ευημερίας τους. Ωστόσο, η πληθώρα των διαθέσιμων συσκευών και εφαρμογών, καθώς και η – άμεση και έμμεση – εμπλοκή διαφόρων ατόμων και φορέων δημιουργούν προκλήσεις για τη διασφάλιση ασφαλούς διακίνησης και επεξεργασίας των εξαιρετικά ευαίσθητων αυτών δεδομένων, καθώς και την εξασφάλιση εμπιστοσύνης και προστασίας της ιδιωτικότητας του υποκειμένου των δεδομένων (Σχήμα 3).



Σχήμα 3: Ανησυχία των Πολιτών για τη Χρήση των Δεδομένων που Συλλέγονται από Συσκευές στο Διαδίκτυο των Πραγμάτων [3]

Στο Διαδίκτυο των Πραγμάτων, οι τρεις βασικές διαδικασίες στις οποίες υποβάλλονται τα δεδομένα που συλλέγονται από τις συσκευές είναι η συλλογή των δεδομένων, η συγκέντρωσή τους και η εξόρυξη και ανάλυσή τους. Συγκεκριμένα, η διαδικασία συλλογής δεδομένων αφορά στην ανίχνευση και συλλογή των δεδομένων κατάστασης των αντικειμένων· κατά τη συγκέντρωση των δεδομένων ενσωματώνονται σχετικά δεδομένα σε μία ενιαία δομή, ενώ η διαδικασία εξόρυξης και ανάλυσης των δεδομένων περιλαμβάνει την εξαγωγή επιπρόσθετης πληροφορίας από τα συγκεντρωμένα δεδομένα για την ικανοποίηση συγκεκριμένου σκοπού εφαρμογής. Αν και οι τρεις προαναφερθείσες διαδικασίες προσφέρουν μια σειρά υπηρεσιών στην καθημερινότητά μας, τα ζητήματα προστασίας της ιδιωτικότητας που δημιουργούνται είναι πολλά. Η προστασία δεδομένων αποτελεί πρόκληση και στο Διαδίκτυο

των Πραγμάτων, καθώς πιθανή πρόσβαση σε αυτά από μη εξουσιοδοτημένο άτομο ή κακόβουλο λογισμικό μπορεί να οδηγήσει σε απώλεια περιουσιακού στοιχείου ή να θέσει σε κίνδυνο τη ζωή του ατόμου. Για το λόγο αυτό, ανάλογα με το στάδιο επεξεργασίας των δεδομένων, υπάρχουν και οι αντίστοιχες απαιτήσεις για τη διασφάλιση της ιδιωτικότητας.

1.2 Διάρθρωση της Διατριβής

Η παρούσα διδακτορική διατριβή αποτελείται από έξι κεφάλαια. Πέραν του παρόντος κεφαλαίου, το οποίο παρέχει εισαγωγικές πληροφορίες περί του θέματος της διατριβής, συμπεριλαμβανομένων των κινήτρων που οδήγησαν σε αυτή, τα υπόλοιπα κεφάλαια έχουν ως εξής.

Το δεύτερο κεφάλαιο αποτελεί βιβλιογραφική επισκόπηση των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας, συνοψίζοντας τις βασικές τάσεις και τεχνολογίες και εξετάζοντας τις ελλείψεις αυτών. Εν συνεχεία, παρουσιάζονται οι σύγχρονες τεχνολογίες που αξιοποιήθηκαν κατά την ανάπτυξη της ευφυούς υπηρεσίας ασφάλειας και προστασίας της ιδιωτικότητας. Συγκεκριμένα, αναλύονται τεχνολογίες και μηχανισμοί ασφάλειας και κρυπτογραφίας, όπως το μοντέλο *Ελέγχου Πρόσβασης βάσει Ιδιοτήτων*, ο μηχανισμός *Κρυπτογράφησης βάσει Ιδιοτήτων*, καθώς και η τεχνολογία *Blockchain*, τις οποίες αξιοποιεί η προαναφερθείσα υπηρεσία. Ιδιαίτερη έμφαση δίνεται, επίσης, στο ρόλο των οντολογιών και στις τεχνολογίες Σημασιολογικού Ιστού που υιοθετούνται στην παρούσα προσέγγιση.

Στο τρίτο κεφάλαιο, παρουσιάζεται η ευφυής υπηρεσία ασφάλειας ως μέρος μίας ολοκληρωμένης, ασφαλούς κατανεμημένης πλατφόρμας ανάπτυξης και εκτέλεσης υπηρεσιών, διασφαλίζοντας την ιδιωτικότητα των χρηστών. Η προαναφερθείσα πλατφόρμα στοχεύει στην εξυπηρέτηση των αναγκών όλων των οντοτήτων που μπορεί να συμμετέχουν σε ένα σύστημα παροχής υπηρεσιών, καλύπτοντας ανάγκες για τη διαχείριση της μετάδοσης, αποθήκευσης και επεξεργασίας των δεδομένων σε ένα ασφαλές περιβάλλον με σεβασμό στην ιδιωτικότητα. Η βασική αρχή που αξιοποιείται για τη δημιουργία ασφαλών συναλλαγών είναι η πρωτοποριακή χρήση προηγμένων κρυπτογραφικών σχημάτων στην παροχή υπηρεσιών. Στο παρόν κεφάλαιο, περιγράφονται σε γενικές γραμμές οι μηχανισμοί που έχουν υιοθετηθεί και, συγκεκριμένα, το πλαίσιο ελέγχου πρόσβασης, καθώς και ο μηχανισμός κρυπτογράφησης που χρησιμοποιούνται ως βάση λειτουργίας της υπηρεσίας. Τέλος, ιδιαίτερη έμφαση δίνεται στον ρόλο των σημασιολογικών τεχνολογιών που αξιοποιούνται τόσο στο πλαίσιο περιγραφής των δεδομένων όσο και του σχήματός τους από τις αντίστοιχες σημασιολογικές υπηρεσίες του συστήματος, προσδίδοντας με τον τρόπο αυτό ευφυΐα στο σύστημα.

Στο τέταρτο κεφάλαιο, παρουσιάζονται τα σενάρια στα οποία εφαρμόζεται

και εξετάζεται η προαναφερθείσα υπηρεσία. Στην πρώτη ενότητα του παρόντος κεφαλαίου, περιγράφεται ο τομέας διαχείρισης παραγωγής, όπου αναλύονται ορισμένα υφιστάμενα πρότυπα, προσδιορίζοντας τους περιορισμούς τους και τις τρέχουσες προσπάθειες προτυποποίησης για την ευρύτερη αποδοχή τέτοιων συστημάτων από τη βιομηχανία. Στη δεύτερη ενότητα, παρουσιάζονται οι σύγχρονες τάσεις στην παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (ΗΔ), εστιάζοντας στους διαφορετικούς τύπους μοντέλων αυτής, καθώς και σε θέματα όπως η απαιτούμενη διαλειτουργικότητα υπηρεσιών παρεχόμενων από διαφορετικούς κρατικούς φορείς, σκιαγραφώντας έτσι το δεύτερο περιβάλλον εφαρμογής της ευφυούς υπηρεσίας ασφάλειας. Εν συνεχεία, παρουσιάζεται η συγκριτική μελέτη πληθώρας παρεχόμενων υπηρεσιών ΗΔ που πραγματοποιήθηκε βάσει συγκεκριμένων κριτηρίων ασφάλειας και ιδιωτικότητας, συγκρίνοντας την αναγκαιότητα ικανοποίησης αυτών στις προαναφερθείσες υπηρεσίες και καταλήγοντας έτσι στην πιο απαιτητική περίπτωση χρήσης. Επιπλέον, αναλύονται οι λειτουργικές και μη απαιτήσεις, καθώς και οι νομικές και κανονιστικές απαιτήσεις υπηρεσιών παρεχόμενων στο πλαίσιο της ΗΔ, οι οποίες πρέπει να ικανοποιούνται από την ευφυή υπηρεσία ασφάλειας. Στην τρίτη ενότητα, παρουσιάζεται ένα συνεργατικό περιβάλλον διαχείρισης δεδομένων υγείας και ευημερίας που εμπεριέχει ένα Κοινωνικό Διαδίκτυο Πραγμάτων. Ξεκινώντας από τη σύντομη ανάλυση του υπό εξέταση συστήματος παρακολούθησης της υγείας και της ευεξίας του ατόμου ενσωματώνοντας δεδομένα που συλλέγονται από προσωπικές, έξυπνες, ενδυτές και μη συσκευές, παρουσιάζονται πτυχές που σχετίζονται με την ασφάλεια, την προστασία των δεδομένων και την ιδιωτικότητα κατά την υιοθέτηση τέτοιων λύσεων στον τομέα της Υγείας.

Η γενική αρχιτεκτονική του συστήματος που παρουσιάστηκε στο τρίτο κεφάλαιο διαμορφώνεται με τρόπο τέτοιο ώστε να εφαρμοστεί κατάλληλα στα τρία σενάρια που εξετάστηκαν στο προηγούμενο κεφάλαιο. Έτσι, κατ' αντιστοιχία με τις ενότητες του τέταρτου κεφαλαίου, στο πέμπτο κεφάλαιο περιγράφεται η τροποποιημένη ανά περίπτωση μορφή της ευφυούς υπηρεσίας ασφάλειας, ώστε να ικανοποιεί τις απαιτήσεις και τους περιορισμούς που ορίζει ο εκάστοτε τομέας. Στην πρώτη ενότητα του κεφαλαίου αυτού, περιγράφονται αναλυτικά τα δομικά στοιχεία των οντολογικών μοντέλων που χρησιμοποιήθηκαν στο πλαίσιο μοντελοποίησης των δεδομένων παραγωγής και δόμησης των μηνυμάτων που ανταλλάσσονται εντός μίας πλατφόρμας διαχείρισης παραγωγής. Επίσης, παρουσιάζεται ένα γραφικό περιβάλλον χρήστη που σχεδιάστηκε και αναπτύχθηκε για τον ορισμό κανόνων πρόσβασης από τον διαχειριστή του συστήματος, προκειμένου να παρουσιαστεί έπειτα αναλυτικά η λειτουργικότητα της ευφυούς υπηρεσίας ασφάλειας, προσαρμοσμένης στις ανάγκες του συγκεκριμένου σεναρίου. Στη δεύτερη ενότητα, περιγράφονται οι τρόποι ενσωμάτωσης της προαναφερθείσας υπηρεσίας σε υφιστάμενα συστήματα παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, ώστε τα τελευταία να μπορούν να αξιοποιήσουν πλήρως τη λειτουργικότητα της πρώτης, ενώ παρουσιάζονται και τα

σημασιολογικά μοντέλα αναπαράστασης βασικών εννοιών του τομέα, στα οποία βασίζεται και η λειτουργία της υπηρεσίας ασφάλειας. Στην τρίτη ενότητα, για τη διασφάλιση της αξιοπιστίας ενός συνεργατικού περιβάλλοντος διαχείρισης δεδομένων υγείας, πέραν της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των ευαίσθητων δεδομένων που μεταδίδονται και υποβάλλονται σε επεξεργασία σε αυτό, εξετάζεται η χρήση τροποποιημένης δομής μπλοκ αλυσίδας κατά την ανταλλαγή δεδομένων μεταξύ οντοτήτων του Κοινωνικού Διαδικτύου των Πραγμάτων, προκειμένου να διασφαλιστεί η προστασία από τυχόν διαρροή δεδομένων. Η ολοκληρωμένη αρχιτεκτονική ασφάλειας που παρουσιάζεται εδώ (προσαρμοσμένη πλέον στο συγκεκριμένο σενάριο) προσφέρει τη βάση για τον σχεδιασμό, την ανάπτυξη και την επιτυχή λειτουργία ενός συστήματος παρακολούθησης της ευημερίας του ατόμου με επίγνωση της ιδιωτικότητας.

Τέλος, τα συμπεράσματα της διατριβής και οι προτάσεις για μελλοντική έρευνα παρατίθενται στο έκτο κεφάλαιο.

Κεφάλαιο 2

Τεχνολογίες Προστασίας Δεδομένων και Ενίσχυσης Ιδιωτικότητας

Στο παρόν κεφάλαιο αναλύεται η τρέχουσα κατάσταση των μεθοδολογιών και μηχανισμών που υιοθετούνται από το ολοκληρωμένο περιβάλλον ασφάλειας και προστασίας της ιδιωτικότητας που παρουσιάζεται στην παρούσα διδακτορική διατριβή στο πλαίσιο σχεδίασης της αρχιτεκτονικής της, όπως επίσης και οι τεχνολογίες που χρησιμοποιούνται με σκοπό την ικανοποίηση των ιδιαίτερων αναγκών ασφάλειας και προστασίας δεδομένων των κατανεμημένων συστημάτων.

2.1 Έλεγχος Πρόσβασης Βάσει Ιδιοτήτων με Επίγνωση της Ιδιωτικότητας

Ο *Έλεγχος Πρόσβασης Βάσει Ιδιοτήτων* (Attribute-Based Access Control – ABAC) είναι ένα ανερχόμενο μοντέλο ελέγχου πρόσβασης, το οποίο αποτελεί ολοένα και περισσότερο το αντικείμενο μελέτης τόσο ερευνητικών εργασιών όσο και βιομηχανικών εφαρμογών. Σύμφωνα με τον κοινώς αποδεκτό ορισμό υψηλού επιπέδου και τις περιγραφές των λειτουργιών του που έχουν δοθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST), ο Έλεγχος Πρόσβασης Βάσει Ιδιοτήτων είναι *μια μέθοδος ελέγχου πρόσβασης, στην οποία τα αιτήματα των υποκειμένων για την εκτέλεση ενεργειών σε αντικείμενα παραχωρούνται ή απορρίπτονται βάσει των ιδιοτήτων του υποκειμένου και του αντικειμένου (όπως αυτές τους έχουν αποδοθεί), των περιβαλλοντικών συνθηκών και ενός συνόλου πολιτικών που καθορίζονται βάσει των προαναφερθεισών ιδιοτήτων και συνθηκών* [16].

Το μοντέλο ελέγχου πρόσβασης ABAC, σε αντίθεση με τα πιο παραδοσιακά

μοντέλα, επιτρέπει τη δημιουργία δυναμικών πολιτικών πρόσβασης βασισμένων σε υπαρκτές ιδιότητες των χρηστών και των αντικειμένων του εκάστοτε συστήματος, αντί της «χειροκίνητης» ανάθεσης ρόλων, ιδιοκτησίας ή ετικετών ασφάλειας από τον διαχειριστή του συστήματος. Υπάρχουν αρκετές περιπτώσεις, όπως οι εφαρμογές Υπολογιστικού Νέφους, όπου η υιοθέτηση του συγκεκριμένου μοντέλου ελέγχου πρόσβασης προσφέρει πολλά οφέλη, μειώνοντας σημαντικά την ανάγκη παρέμβασης του διαχειριστή κατά την εξουσιοδότηση των χρηστών συγκεκριμένων ρόλων, απλοποιώντας έτσι τη διαχείριση πρόσβασης σε σύνθετα συστήματα με μεγάλο αριθμό χρηστών, δημιουργώντας παράλληλα τη δυνατότητα αυτοματοποίησης της λήψης αποφάσεων ελέγχου πρόσβασης για απομακρυσμένους χρήστες άλλων συστημάτων.

Στη βιβλιογραφία, κάθε προτεινόμενο μοντέλο ABAC επιχειρεί να παρουσιάσει τα επιμέρους στοιχεία του με έναν ελαφρώς διαφορετικό τρόπο. Ωστόσο, τα κοινά στοιχεία των μοντέλων αυτών που ακολουθούν και τις προδιαγραφές του ινστιτούτου NIST είναι τα εξής:

- Το **Υποκείμενο** (Subject) αναφέρεται είτε σε χρήστη είτε σε κάποια υπηρεσία, συσκευή ή εφαρμογή (μη ανθρώπινη οντότητα) που αιτείται να πραγματοποιήσει κάποια ενέργεια σε κάποιο αντικείμενο. Στα υποκείμενα έχουν αποδοθεί ένα ή περισσότερα χαρακτηριστικά.
- Το **Αντικείμενο** (Object) αφορά πόρο του συστήματος όπως συσκευές, αρχεία, διαδικασίες, εφαρμογές, υπηρεσίες, δίκτυα ή οποιαδήποτε οντότητα που περιέχει ή λαμβάνει πληροφορίες. Η διαχείριση της πρόσβασης και εκτέλεσης κάποιας ενέργειας στους προαναφερθέντες πόρους από κάποιο υποκείμενο πραγματοποιείται από το μοντέλο ABAC.
- Η **Λειτουργία** (Operation) αναφέρεται στην εκτέλεση κάποιας ενέργειας σε κάποιο αντικείμενο κατόπιν αιτήματος κάποιου υποκειμένου. Ο όρος αυτός αναφέρεται σε διαδικασίες όπως ανάγνωση, εγγραφή, επεξεργασία, διαγραφή, αντιγραφή, εκτέλεση και τροποποίηση.
- Η **Πολιτική** (Policy) είναι η αναπαράσταση κανόνων ή σχέσεων που καθιστά δυνατή τη λήψη απόφασης σχετικά με την έγκριση ή μη της ενέργειας που ζητείται να πραγματοποιηθεί, δεδομένων των ιδιοτήτων του υποκειμένου και του αντικειμένου και πιθανώς των συνθηκών περιβάλλοντος.
- Οι **Συνθήκες Περιβάλλοντος** (Environment Conditions) αφορούν το επιχειρησιακό ή περιστασιακό πλαίσιο στο οποίο προκύπτει το αίτημα πρόσβασης. Οι συνθήκες περιβάλλοντος διευκρινίζονται βάσει ανιχνεύσιμων χαρακτηριστικών του περιβάλλοντος, όπως ώρα, ημέρα, τοποθεσία ενός χρήστη κ.ο.κ.

Το υποκείμενο, το αντικείμενο και η λειτουργία του μοντέλου ABAC φέρουν κάποια χαρακτηριστικά που αποδίδονται στα προαναφερθέντα, γνωστά ως **Ιδιότητες** (Attributes). Στο κλασικό μοντέλο ABAC, οι ιδιότητες περιέχουν πληροφορία που παρέχεται μέσω ζευγών ονόματος-τιμής. Σε άλλα μοντέλα ABAC της βιβλιογραφίας,

οι ιδιότητες σχετίζονται με κάποιο τύπο ιδιότητας ή ταξινομούνται σε κατηγορίες. Συγκεκριμένα, οι ιδιότητες των επιμέρους οντοτήτων και οι συνθήκες βάσει των οποίων ορίζονται οι κανόνες πρόσβασης στο μοντέλο ABAC μπορούν να ταξινομηθούν στις ακόλουθες κατηγορίες [17]:

- Ιδιότητες Υποκειμένου (Subject Attributes): στην περίπτωση που το υποκείμενο μίας εξουσιοδότησης πρόσβασης αφορά χρήστη, οι ιδιότητες χρήστη περιλαμβάνουν χαρακτηριστικά, όπως ηλικία, όνομα, επάγγελμα, ρόλος, διεύθυνση σπιτιού, ημερομηνία πρόσληψης κ.ο.κ.
- Ιδιότητες Αντικειμένου (Object Attributes): οι ιδιότητες πόρου ενός συστήματος μπορεί να περιλαμβάνουν χαρακτηριστικά που σχετίζονται με τα μεταδεδομένα του, όπως ιδιοκτήτης, ημερομηνία δημιουργίας, ημερομηνία τελευταίας τροποποίησης, μέγεθος, τύπος αρχείου κ.α. ή με το περιεχόμενό του, όπως όνομα ασθενούς στην περίπτωση που ο πόρος αφορά φάκελο υγείας ασθενούς, αριθμός μητρώου φοιτητή σε κάποιο πανεπιστημιακό έγγραφο κ.α.
- Ιδιότητες Περιβάλλοντος (Environmental Attributes): χαρακτηριστικά που προκύπτουν από την τρέχουσα κατάσταση του περιβάλλοντος του συστήματος, όπως, για παράδειγμα, τρέχουσα ώρα, ημέρα της εβδομάδας, αριθμός συνδεδεμένων χρηστών, ελεύθερος αποθηκευτικός χώρος κ.ο.κ.
- Ιδιότητες Σύνδεσης (Connection Attributes): χαρακτηριστικά που ισχύουν μόνο για την τρέχουσα σύνδεση ενός χρήστη, όπως διεύθυνση IP, φυσική τοποθεσία κινητών συσκευών, ημερομηνία και ώρα έναρξης σύνδεσης, αριθμός αιτημάτων πρόσβασης που έγιναν κ.ο.κ.
- Διαχειριστικές Ιδιότητες (Administrative Attributes): χαρακτηριστικά ρυθμιστικών παραμέτρων που ισχύουν για ολόκληρο το σύστημα, τα οποία είτε έχουν οριστεί από το διαχειριστή του συστήματος είτε από κάποια αυτοματοποιημένη διαδικασία, όπως επίπεδο απειλής (π.χ. κατά πόσο είναι πιθανό να δεχτεί το σύστημα κάποια επίθεση), μέγιστη επιτρεπτή διάρκεια σύνδεσης κ.α.

Ιδανικά, οι παραπάνω ιδιότητες αποτελούν χαρακτηριστικά των στοιχείων του συστήματος και δεν χρειάζεται να προσδιορισθούν από τον διαχειριστή. Οι πολιτικές πρόσβασης μπορούν να ορισθούν χρησιμοποιώντας τις γλώσσες έκφρασης πολιτικών, περιορίζοντας την πρόσβαση σε ορισμένους πόρους ή αντικείμενα, με βάση το αποτέλεσμα μιας υπό συνθήκη έκφρασης που συγκρίνει ιδιότητες. Με τον τρόπο αυτό, το μοντέλο ελέγχου πρόσβασης ABAC συνιστά έναν ευέλικτο τρόπο επιβολής πολιτικών που βασίζονται σε χαρακτηριστικά οντοτήτων του πραγματικού κόσμου.

2.1.1 Γλώσσα Έκφρασης Πολιτικών Πρόσβασης

Απαραίτητο στοιχείο των μοντέλων ελέγχου πρόσβασης είναι η γλώσσα έκφρασης πολιτικών που χρησιμοποιείται για τον ορισμό εφαρμόσιμων κανόνων στο εκάστοτε σύστημα. Σύμφωνα με τον Οργανισμό Εξέλιξης Προτύπων Δομημένης Πλη-

ροφορίας (Organization for the Advancement of Structured Information Standards – OASIS) [18], οι βασικές απαιτήσεις που πρέπει να ικανοποιεί μια γλώσσα προδιαγραφής πολιτικών και κανόνων πρόσβασης στους πόρους ενός πληροφοριακού συστήματος πρέπει να παρέχει τα εξής:

- μια μέθοδο συνδυασμού των επιμέρους κανόνων και πολιτικών σε ένα ενιαίο σύνολο πολιτικών που βρίσκει εφαρμογή σε συγκεκριμένο αίτημα απόφασης.
- μια μέθοδο για τον ευέλικτο ορισμό της διαδικασίας με την οποία συνδυάζονται οι κανόνες και οι πολιτικές.
- μια μέθοδο διαχείρισης πολλαπλών υποκειμένων που δρουν διαφορετικά.
- μια μέθοδο για την υποστήριξη της διαδικασίας λήψης απόφασης εξουσιοδότησης βάσει των ιδιοτήτων του υποκειμένου και του πόρου.
- μια μέθοδο διαχείρισης ιδιοτήτων πολλαπλών τιμών.
- μια μέθοδο για να βασίζεται μια απόφαση εξουσιοδότησης στο περιεχόμενο ενός πόρου πληροφορίας.
- ένα σύνολο λογικών και μαθηματικών τελεστών για την εφαρμογή τους σε λογικές εκφράσεις που περιέχουν τις ιδιότητες του υποκειμένου, του αντικειμένου και του περιβάλλοντος.
- μια μέθοδο για τη διαχείριση των κατανεμημένων δομικών στοιχείων εφαρμογής πολιτικών χρησιμοποιώντας ένα αφαιρετικό μοντέλο για τον εντοπισμό, την ανάκτηση και την αυθεντικοποίηση των προαναφερθέντων στοιχείων.
- μια μέθοδο ταχείας ανάκτησης της πολιτικής που βρίσκει εφαρμογή σε μια συγκεκριμένη ενέργεια βάσει των ιδιοτήτων του υποκειμένου, του πόρου και της ενέργειας.
- ένα αφαιρετικό επίπεδο που αποσπά τον υπεύθυνο ορισμού πολιτικών από τις λεπτομέρειες του περιβάλλοντος εφαρμογής.
- μια μέθοδο προσδιορισμού ενός συνόλου ενεργειών που πρέπει να εκτελεστούν σε συνδυασμό με την επιβολή πολιτικής.

Η πιο γνωστή και προτυποποιημένη δομημένη γλώσσα προδιαγραφής κανόνων είναι η *Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης* (eXtensible Access Control Markup Language – XACML) που δημιουργήθηκε από τον οργανισμό OASIS προκειμένου να καλυφθούν οι παραπάνω απαιτήσεις χρησιμοποιώντας μια επέκταση της γλώσσας σήμανσης XML [19].

Για την εφαρμογή του μοντέλου ABAC σε ένα σύστημα, απαραίτητη είναι η χρήση των κατάλληλων μηχανισμών ελέγχου πρόσβασης. Σύμφωνα με το πρότυπο XACML και το αφαιρετικό μοντέλο της Ομάδας Μηχανικής Διαδικτύου (Internet Engineering Task Force – IETF) που ακολουθείται από το πρώτο, στους προαναφερθέντες μηχανισμούς συγκαταλέγονται διάφορα λειτουργικά "σημεία" για τη διαχείριση των πολιτικών, του πλαισίου ή των ροών εργασιών για την ανάκτηση και αξιολόγηση κανόνων και ιδιοτήτων. Οι λειτουργίες αλλά και τα δομικά στοιχεία αυτών των "σημείων" μπορούν να διαχωριστούν λογικά και φυσικά και να κατανεμηθούν

σε μία επιχείρηση, αντί να βρίσκονται συγκεντρωμένα σε ένα μόνο σημείο. Συγκεκριμένα, οι επιμέρους οντότητες που απαρτίζουν ένα ολοκληρωμένο σύστημα ελέγχου πρόσβασης ABAC και διαλειτουργούν για τη λήψη και την επιβολή απόφασης εξουσιοδότησης είναι οι εξής:

- **Σημείο Απόφασης Πολιτικής** (Policy Decision Point – PDP): αξιολόγηση κανόνων και λήψη απόφασης εξουσιοδότησης.
- **Σημείο Εφαρμογής Πολιτικής** (Policy Enforcement Point – PEP): εφαρμογή της απόφασης εξουσιοδότησης ως απάντηση στο αίτημα υποκειμένου για πρόσβαση σε προστατευόμενο αντικείμενο.
- **Σημείο Πληροφόρησης Πολιτικής** (Policy Information Point – PIP): ανάκτηση των ιδιοτήτων ή/και των δεδομένων που απαιτούνται για την αποτίμηση του αιτήματος πρόσβασης, προκειμένου να συγκεντρωθεί η απαραίτητη πληροφορία που χρειάζεται το σημείο PDP για τη λήψη απόφασης.
- **Σημείο Διαχείρισης Πολιτικής** (Policy Administration Point – PAP): γραφικό περιβάλλον χρήστη για τη δημιουργία, τη διαχείριση, τον έλεγχο αλλά και τη διόρθωση κανόνων από το διαχειριστή του συστήματος και τη μετέπειτα αποθήκευσή τους σε κατάλληλο αποθετήριο.
- **Διαχειριστής Πλαισίου** (Context Handler): διαχείριση και εκτέλεση της λογικής ροών εργασιών που καθορίζει τη σειρά με την οποία κανόνες και ιδιότητες ανακτώνται και εφαρμόζονται.

2.1.2 Επεκτασιμότητα, Εφαρμοσιμότητα και Απόδοση

Η επεκτασιμότητα, η εφαρμοσιμότητα και η απόδοση αποτελούν σημαντικά ζητήματα κατά την εξέταση της ανάπτυξης ενός προϊόντος ή μίας τεχνολογίας που βασίζεται στο μοντέλο ελέγχου πρόσβασης ABAC. Το μοντέλο αυτό απαιτεί πολύπλοκη αλληλεπίδραση μεταξύ των δομικών του στοιχείων που αναφέρθηκαν προηγουμένως. Συχνά, αυτά τα στοιχεία κατανέμονται μεταξύ οργανισμών και μερικές φορές βρίσκονται σε διαφορετικά δίκτυα. Όσο μεγαλύτερος και ετερογενής είναι ένας οργανισμός, τόσο πιο σύνθετες είναι οι αλληλεπιδράσεις μεταξύ των στοιχείων. Σε τέτοιες περιπτώσεις, ένα αίτημα πρόσβασης σε ένα έγγραφο που βρίσκεται μέσα σε κάποιο αποθετήριο μπορεί να φαίνεται απλό αλλά στην πραγματικότητα μπορεί να απαιτήσει: (α) τη δημιουργία αιτήματος πρόσβασης από μία υπηρεσία, (β) την ανάκτηση πολλαπλών ιδιοτήτων από πολλές διασκορπισμένες πηγές, (γ) την επικύρωση από τρίτους της ακεραιότητας των ιδιοτήτων του εγγράφου, (δ) τη λήψη απόφασης από το αρμόδιο στοιχείο και (ε) την επιβολή της απόφασης αυτής από το στοιχείο PEP. Για την αντιμετώπιση των ζητημάτων αυτών, έχουν προταθεί στη βιβλιογραφία μοντέλα ελέγχου πρόσβασης που υιοθετούν τον κορμό του ABAC και προτείνουν συγκεκριμένες αρχιτεκτονικές για την εφαρμογή του μοντέλου σε πραγματικά συστήματα.

2.1.3 Θέματα Προστασίας Προσωπικών Δεδομένων

Λόγω της προσωπικής και περιγραφικής φύσης των ιδιοτήτων των υποκειμένων και αντικειμένων ενός συστήματος που χρησιμοποιούνται για τον ορισμό πολιτικών πρόσβασης και την αξιολόγηση αιτημάτων, η υιοθέτηση του μοντέλου ABAC αυξάνει τον κίνδυνο παραβίασης της ιδιωτικότητας είτε λόγω της ακούσιας έκθεσης των προσωπικών, ταυτοποιητικών ιδιοτήτων σε μη αξιόπιστες οντότητες είτε λόγω της συγκέντρωσης ευαίσθητης πληροφορίας σε μη ασφαλή περιβάλλοντα. Για το λόγο αυτό, κρίνεται απαραίτητη η επιβολή κανονισμών σχετικά με τη διαχείριση των ιδιοτήτων. Επιπρόσθετα, απαιτείται προστασία των καναλιών ανταλλαγής μηνυμάτων αιτημάτων-απόκρισης, προστασία των αποθηκευμένων ιδιοτήτων των υποκειμένων του συστήματος κ.α. Η επιλογή και χρήση μηχανισμών προστασίας της ιδιωτικότητας δεν εμπίπτουν στο πεδίο εφαρμογής του XACML.

2.2 Λειτουργική Κρυπτογράφηση

Στις μέρες μας, η *Κρυπτογράφηση Δημόσιου Κλειδιού* (Public-Key Encryption) εφαρμόζεται ευρέως για τη διασφάλιση της διαδικτυακής επικοινωνίας και την προστασία συστημάτων διαχείρισης δεδομένων και των αποθετηρίων αυτών. Ωστόσο, για πολλές εφαρμογές, η κρυπτογράφηση δημόσιου κλειδιού θεωρείται ανεπαρκής [20]. Για παράδειγμα, στην περίπτωση κρυπτογράφησης κάποιων δεδομένων με τη χρήση της προαναφερθείσας μεθόδου κρυπτογράφησης, βάσει συγκεκριμένης πολιτικής την οποία πρέπει να ικανοποιούν όσοι θέλουν να τα αποκρυπτογραφήσουν, τα θέματα που δημιουργούνται είναι τα εξής: (α) πώς πραγματοποιείται η εύρεση των δημόσιων κλειδιών όλων των ατόμων που ικανοποιούν την πολιτική αυτή; (β) τι γίνεται στην περίπτωση που κάποιος συνδεθεί στο σύστημα και λάβει τα διαπιστευτήριά του μετά την αποθήκευση των κρυπτογραφημένων πλέον δεδομένων; (γ) σε περίπτωση που επιβάλλεται να δοθεί μερική πρόσβαση στο αρχικό κείμενο, πώς είναι αυτό εφικτό; (δ) είναι απαραίτητο κάποιος χρήστης ενός συστήματος να μάθει την ταυτότητα όλων των ατόμων που έχουν τα συγκεκριμένα δημόσια κλειδιά στην κατοχή τους;

Για την αντιμετώπιση των προαναφερθέντων ζητημάτων, έχουν προταθεί διάφορα μοντέλα κρυπτογράφησης, ένα εκ των οποίων είναι και η *Λειτουργική Κρυπτογράφηση* (Functional Encryption), όπου το κλειδί αποκρυπτογράφησης επιτρέπει σε έναν χρήστη να έχει πρόσβαση μόνο σε μια συγκεκριμένη λειτουργία των κρυπτογραφημένων δεδομένων [21]. Εν συντομία, σε ένα σύστημα που εφαρμόζει τη λειτουργική κρυπτογράφηση, μια έμπιστη αρχή κατέχει ένα κύριο μυστικό κλειδί (master secret key) γνωστό μόνο στην ίδια. Όταν δίνεται στην αρχή η περιγραφή κάποιας συνάρτησης f ως είσοδο, η πρώτη χρησιμοποιεί το κύριο μυστικό κλειδί της

για να παράξει ένα μυστικό κλειδί $sk[f]$ που σχετίζεται με τη συνάρτηση f. Έτσι, όποιος κατέχει το κλειδί $sk[f]$ μπορεί να υπολογίσει τη συνάρτηση $f(x)$ οποιουδήποτε κρυπτογραφημένου x. Παρόλο που η τιμή του x είναι κρυπτογραφημένη, αποκαλύπτεται στον αιτούντα πρόσβαση μόνο το αποτέλεσμα της συνάρτησης f. Με τον τρόπο αυτόν, ένα σύστημα που εφαρμόζει το σχήμα της λειτουργικής κρυπτογράφησης μπορεί να υποστηρίξει μια ποικιλία λειτουργιών. Το συγκεκριμένο είδος κρυπτογράφησης μπορεί να θεωρηθεί ανάλογο των μεθόδων ασφαλών υπολογισμών [22][23], αλλά με τη βασική διαφορά ότι η λειτουργική κρυπτογράφηση δεν επιτρέπει τη διάδραση με το χρήστη.

Η λειτουργική κρυπτογράφηση βρίσκει εφαρμογή στα εξής πεδία:

Εκφραστικός μηχανισμός ελέγχου πρόσβασης: Σε μεγάλους οργανισμούς, όπως φορείς υγειονομικής περίθαλψης, ασφαλιστικές εταιρείες, κρατικά ιδρύματα και πανεπιστήμια, είναι ιδιαίτερα συχνή η κοινοποίηση δεδομένων μεταξύ ατόμων σύμφωνα με κάποια πολιτική πρόσβασης. Χρησιμοποιώντας τη λειτουργική κρυπτογράφηση, ένας χρήστης μπορεί να εκφράσει άμεσα κατά τη διαδικασία κρυπτογράφησης τον τρόπο με τον οποίο ο ίδιος ή ο οργανισμός στον οποίο ανήκει επιθυμεί κάποιος να αποκτήσει πρόσβαση στα δεδομένα. Συγκεκριμένα, ο χρήστης μπορεί να κρυπτογραφήσει τα δεδομένα $x = (P, m)$, όπου m είναι τα δεδομένα που ο χρήστης επιθυμεί να κρυπτογραφήσει και P η πολιτική πρόσβασης. Η συνάρτηση μυστικού κλειδιού $sk[f]$ του αιτούντα πρόσβαση θα ελέγξει αν τα διαπιστευτήρια ή τα χαρακτηριστικά του χρήστη συμφωνούν με την πολιτική κρυπτογράφησης και ανάλογα θα αποκαλύψει μόνο τα δεδομένα m. Για παράδειγμα, εάν κάποιος χρήστης-εργαζόμενος κάποιας εταιρείας ορίσει την πολιτική ("LOGISTICS" OR "SALES") για την κρυπτογράφηση κάποιων δεδομένων, τότε η συνάρτηση f του αιτούντα πρόσβαση θα ελέγξει κατά πόσο οι ιδιότητες του συγκεκριμένου ικανοποιούν την προαναφερθείσα πολιτική και, αν ναι, θα επιστρέψει σε αυτόν τα δεδομένα m.

Εξόρυξη μεγάλων συνόλων δεδομένων: Η εξόρυξη δεδομένων για την ανάκτηση χρήσιμης πληροφορίας και την περαιτέρω επεξεργασία της χρησιμοποιείται ιδιαίτερα στην ιατρική έρευνα, στα κοινωνικά δίκτυα, στον τομέα της ασφάλειας δικτύων κ.ο.κ. Οι διαχειριστές τέτοιων συστημάτων επιθυμούν να δίνουν στους χρήστες τη δυνατότητα να έχουν πρόσβαση σε δεδομένα μόνο για ορισμένους τύπους ερωτημάτων. Για παράδειγμα, στην ιατρική έρευνα όπου ένας ερευνητής θέλει να ελέγξει κατά πόσο ένας συγκεκριμένος γονότυπος συνδέεται με έναν συγκεκριμένο τύπο καρκίνου σε μια ομάδα ασθενών, ο ίδιος θα πρέπει να έχει πρόσβαση μόνο στις αλληλουχίες γονιδίων και τα ιατρικά ιστορικά των ασθενών, χωρίς όμως να αποκαλυφθούν άλλες λεπτομέρειες για την ταυτότητα των ασθενών ή την κατάσταση της υγείας τους. Στην πραγματικότητα, ο διαχειριστής ενός συστήματος δεν γνωρίζει εκ των προτέρων τα ερωτήματα που μπορεί να γίνουν για την ανάκτηση δεδομένων ή την εφαρμογή κάποιας συνάρτησης σε αυτά προκειμένου να τα κρυπτογραφήσει ανάλογα. Παρ' όλα αυτά, η λειτουργική κρυπτογράφηση δίνει τη δυνατότητα να κρυπτογραφηθούν τα

δεδομένα υπό ένα σύνολο συναρτήσεων F, με αποτέλεσμα ο αιτών πρόσβαση, εφόσον εξουσιοδοτηθεί, να μπορεί να υπολογίσει οποιαδήποτε συνάρτηση f του συνόλου των συναρτήσεων.

2.2.1 Αλγόριθμοι Λειτουργικής Κρυπτογράφησης

Τα συστήματα δημόσιων κλειδιών, όπως είναι το RSA και το El-Gamal, χρησιμοποιούν για την εφαρμογή της κρυπτογράφησης τους εξής τρεις αλγόριθμους:

- `Setup` (S): εξάγει ένα μυστικό κλειδί sk (secret key) και ένα δημόσιο κλειδί pk (public key). Οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το κλειδί pk αλλά μόνο ο κάτοχος του μυστικού κλειδιού sk είναι σε θέση να το αποκρυπτογραφήσει.
- `Encryption` (E): λαμβάνει ως είσοδο ένα δημόσιο κλειδί pk και ένα μήνυμα και δίνει ως έξοδο ένα κρυπτογράφημα.
- `Decryption` (D): λαμβάνει ως είσοδο ένα μυστικό κλειδί sk και ένα κρυπτογράφημα και δίνει ως είσοδο το μήνυμα.

Ένα σύστημα λειτουργικής κρυπτογράφησης περιλαμβάνει τους ίδιους τρεις αλγόριθμους, καθώς επίσης και έναν τέταρτο αλγόριθμο που ονομάζεται `KeyGen`. Στη λειτουργική κρυπτογράφηση, το μυστικό κλειδί που δημιουργείται από τον αλγόριθμο `Setup` ονομάζεται κύριο κλειδί mk (master key). Ο αλγόριθμος `KeyGen` λαμβάνει ως είσοδο το κλειδί mk και την περιγραφή κάποιας συνάρτησης f και δίνει ως έξοδο ένα κλειδί που είναι συγκεκριμένο για τη συνάρτηση f και υποδηλώνεται ως $sk[f]$, άρα $D(sk[f]; c) \rightarrow f(x)$, όπου c το αποτέλεσμα της κρυπτογράφησης του μηνύματος x με τη χρήση του κλειδιού pk.

Στο σημείο αυτό πρέπει να τονιστεί ότι το κλειδί $sk[f]$ δεν αποκρυπτογραφεί πλήρως το κρυπτογράφημα c αλλά εξάγει μόνο το αποτέλεσμα εκτέλεσης μιας συνάρτησης f πάνω στο αρχικό μήνυμα. Σε περίπτωση που ο εξουσιοδοτημένος χρήστης επιθυμεί να αποκρυπτογραφήσει πλήρως το κρυπτογράφημα, μπορεί να χρησιμοποιήσει το μυστικό κλειδί $sk[g]$, όπου g είναι η συνάρτηση ταυτότητας με $g(x) = x \ \forall \ x$. Έτσι, είναι εμφανές πως εάν ένας επιτιθέμενος έχει στη διάθεσή του ένα σύνολο μυστικών κλειδιών $sk[f_1], ..., sk[f_n]$ δεν μπορεί να αποκαλύψει τίποτα παραπάνω εκτός από αυτά που αποκρυπτογραφούνται από τα κλειδιά που έχει ο ίδιος στη διάθεσή του.

Η λειτουργική κρυπτογράφηση μπορεί να θεωρηθεί ως ένα πολύ ισχυρό σχήμα κρυπτογράφησης, καθώς διαθέτει τους τρόπους περιγραφής πολλών προηγμένων μεθόδων κρυπτογράφησης. Για παράδειγμα, ακόμα και η παραδοσιακή κρυπτογράφηση δημόσιου κλειδιού μπορεί να θεωρηθεί ως μια πολύ ειδική περίπτωση λειτουργικής κρυπτογράφησης, όπου η μοναδική υποστηριζόμενη λειτουργία είναι η λειτουργία ταυτότητας και κάποιος μπορεί να αποκρυπτογραφήσει μόνο ολόκληρο το

κρυπτογράφημα.

2.2.2 Κρυπτογράφηση Βάσει Ιδιοτήτων

Η *Κρυπτογράφηση Βάσει Ιδιοτήτων* (Attribute-Based Encryption – ABE) αποτελεί μια μέθοδο κρυπτογράφησης που μπορεί να περιγραφεί από τα επιμέρους στοιχεία της Λειτουργικής Κρυπτογράφησης. Η Κρυπτογράφηση Βάσει Ιδιοτήτων προτάθηκε από τους Sahai και Waters το 2005 [24] και αποτελεί επέκταση της *Κρυπτογράφησης Βάσει Ταυτότητας* (Identity-Based Encryption – IBE) που προτάθηκε από τον Shamir το 1984 [25]. Συγκεκριμένα, στην κρυπτογράφηση βάσει ιδιοτήτων το ιδιωτικό κλειδί του χρήστη αλλά και το κρυπτογράφημα εξαρτώνται από διάφορα χαρακτηριστικά και ιδιότητές του, θεωρώντας την ταυτότητα του χρήστη ως μία ιδιότητα αυτού. Η αποκρυπτογράφηση ενός κρυπτοκειμένου εξαρτάται μόνο από τις ιδιότητες που φέρει αυτός, όπως, για παράδειγμα, το επάγγελμά του, η ηλικία του, ο ασφαλιστικός φορέας στον οποίο ανήκει κ.ο.κ.

Από τις διάφορες προεκτάσεις της κρυπτογράφησης βάσει ιδιοτήτων που έχουν προταθεί ερευνητικά [26], η προσέγγιση που παρουσιάζεται στην παρούσα διδακτορική διατριβή αξιοποιεί την *Κρυπτογράφηση βάσει Ιδιοτήτων με Ενσωμάτωση Κανόνων στο Κρυπτογράφημα* (Ciphertext-Policy Attribute Based Encryption – CP-ABE) και οι κανόνες αυτοί περιλαμβάνουν δέντρα πρόσβασης που αποτελούνται από λογικές σχέσεις μεταξύ ιδιοτήτων [27][28]. Για την εφαρμογή κρυπτογράφησης βάσει ιδιοτήτων με ενσωμάτωση κανόνων στο κρυπτογράφημα, χρησιμοποιούνται οι εξής τέσσερις αλγόριθμοι:

- `Setup`: Ο αλγόριθμος αυτός έχει ως είσοδο μόνο μία παράμετρο ασφάλειας k και δημιουργεί τα κλειδιά pk (public key) και mk (master key).
- `Encrypt(pk, m, A)`: Για την κρυπτογράφηση ενός μηνύματος m (message), χρησιμοποιείται το κλειδί pk και ένα δέντρο πρόσβασης A (access tree), που αναπαριστά το σχετικό κανόνα πρόσβασης ορισμένο βάσει συσχετίσεων μεταξύ ιδιοτήτων του χρήστη. Ο αλγόριθμος αυτός δημιουργεί ένα κρυπτογράφημα ct (ciphertext), τέτοιο ώστε μόνο χρήστες που φέρουν ένα σύνολο ιδιοτήτων που ικανοποιούν τη δομή πρόσβασης να μπορούν να το αποκρυπτογραφήσουν.
- `Key Generation(mk, S)`: Ο αλγόριθμος αυτός χρησιμοποιείται για τη δημιουργία ιδιωτικού κλειδιού sk (secret key) του χρήστη και απαιτεί ως είσοδο το κλειδί mk καθώς και το σύνολο ιδιοτήτων S του χρήστη για τον οποίο θα δημιουργηθεί το κλειδί.
- `Decrypt(pk, ct, sk)`: Για την αποκρυπτογράφηση του κρυπτογραφήματος ct απαιτείται η χρήση του δημόσιου κλειδιού pk, καθώς και του ιδιωτικού κλειδιού του χρήστη sk. Εάν το σύνολο S των ιδιοτήτων του χρήστη που περιέχεται στο κλειδί sk ικανοποιεί τον κανόνα βάσει του οποίου έχει κρυπτογραφηθεί το μήνυμα, πραγματοποιείται τότε και η αποκρυπτογράφηση αυτού.

2.3 Τεχνολογία της Αλυσίδας των Μπλοκ

Η τεχνολογία της *Αλυσίδας των Μπλοκ* (Blockchain) κατακτά ολοένα και περισσότερο την παγκόσμια βιομηχανία Τεχνολογιών Πληροφορίας και Επικοινωνίας, καθώς και τον ερευνητικό κόσμο, κυρίως λόγω της μεγάλης επιτυχίας του κρυπτονομίσματος Bitcoin [29]. Η καθιέρωση των ψηφιακών νομισμάτων (μέχρι στιγμής έχουν εντοπιστεί στην αγορά περισσότερα από 650 ψηφιακά νομίσματα με πιο γνωστά τα Bitcoin, Ethereum, Ripple, Litecoin κ.α.) έχει φέρει στο προσκήνιο την τεχνολογία Blockchain. Το Blockchain σχεδιάστηκε, αρχικά, ως μία κατανεμημένη δομή δεδομένων με στόχο τη διατήρηση ενός δημόσιου «λογιστικού βιβλίου» (ledger) καταγραφής συναλλαγών ψηφιακών νομισμάτων Bitcoin, ενώ, στη συνέχεια, εμπλουτίστηκε με άλλες δυνατότητες προκειμένου, για παράδειγμα, να επιτρέπει τη διατήρηση δεδομένων, καθώς και την εκτέλεση κώδικα μηχανής. Η τεχνολογία αυτή τροφοδότησε μία από τις πιο ενθουσιώδεις εκρήξεις έντονης δραστηριότητας στον τομέα της εφαρμοσμένης κρυπτογραφίας τα τελευταία χρόνια, καθώς, σε συνδυασμό με ισχυρούς κρυπτογραφικούς μηχανισμούς, η τεχνολογία Blockchain μπορεί να συμβάλει στην ασφαλή συλλογή και μετάδοση σημαντικών και ευαίσθητων δεδομένων, όπως προσωπικά δεδομένα που σχετίζονται με την υγεία του ατόμου. Παρόλα αυτά, υπάρχουν αρκετά προβλήματα στην τεχνολογία αυτή ως προς τους τομείς της ασφάλειας και προστασίας της ιδιωτικότητας που πρέπει να αντιμετωπιστούν προκειμένου να αποκαλυφθεί πλήρως η δυναμική της.

2.3.1 Ιδιωτικές και Δημόσιες Μπλοκ Αλυσίδες

Ένα τυπικό σύστημα blockchain αποτελείται από πολλαπλούς κόμβους που δεν εμπιστεύονται πλήρως ο ένας τον άλλον. Οι κόμβοι αυτοί διατηρούν ένα κοινόχρηστο αρχείο καταστάσεων αξιοποιώντας το blockchain ως δομή δεδομένων και εκτελούν συναλλαγές που τροποποιούν τις καταστάσεις αυτές, επιβεβαιώνοντας την εγκυρότητα των πρώτων και τη σειρά με την οποία αυτές εκτελούνται. Στη δομή δεδομένων μπλοκ αλυσίδας, κάθε μπλοκ συνδέεται με το προηγούμενό του μέσω ενός κρυπτογραφικού δείκτη, οδηγώντας έτσι στο πρώτο μπλοκ, γνωστό και ως "γένεση της αλυσίδας" (genesis). Για το λόγο αυτό, το blockchain αναφέρεται συχνά ως κατανεμημένο λογιστικό βιβλίο.

Μια συναλλαγή στο blockchain είναι αντίστοιχη αυτής στις παραδοσιακές βάσεις δεδομένων, δηλαδή περιλαμβάνει μια ακολουθία λειτουργιών που εφαρμόζονται σε ορισμένες καταστάσεις. Ως εκ τούτου, η συναλλαγή του blockchain, προκειμένου να είναι αξιόπιστη, απαιτείται να φέρει τις ιδιότητες Ατομικότητας, Συνέπειας, Απομόνωσης και Μονιμότητας (Atomicity, Consistency, Isolation, Durability – ACID). Η βασική διαφορά έγκειται στο μοντέλο αποτυχίας. Οι τρέχουσες συναλλακτικές, κατανεμημένες βάσεις δεδομένων χρησιμοποιούν κλασσικές τεχνικές ελέγχου ταυ-

τόχρονης προσπέλασης, όπως η εγγραφή δεδομένων σε δύο φάσεις, κι έτσι επιτυγχάνουν υψηλή απόδοση [30][31]. Αντίθετα, ο αρχικός σχεδιασμός του blockchain θεωρεί την ύπαρξη ενός πολύ εχθρικού περιβάλλοντος στο οποίο οι κόμβοι παρουσιάζουν βυζαντινή συμπεριφορά (αυθαίρετη, μη ντετερμινιστική συμπεριφορά). Σύμφωνα με αυτό το μοντέλο, το κόστος ελέγχου ταυτόχρονης προσπέλασης είναι πολύ υψηλότερο [32].

Σε υψηλό επίπεδο, ένα σύστημα blockchain μπορεί να κατηγοριοποιηθεί ως δημόσιο ή ιδιωτικό. Στο πρώτο, οποιοσδήποτε κόμβος μπορεί να ενταχθεί και να αποχωρήσει από το σύστημα, καθιστώντας το blockchain ως ένα πλήρως αποκεντρωμένο δίκτυο που μοιάζει με δίκτυο ομότιμων κόμβων (peer-to-peer) [33]. Στη δεύτερη περίπτωση, το blockchain επιβάλλει αυστηρή συμμετοχή των κόμβων και για το λόγο αυτό υπάρχει ένας μηχανισμός ελέγχου πρόσβασης για να προσδιοριστεί ποιος μπορεί να ενταχθεί στο δίκτυο. Ως αποτέλεσμα, κάθε κόμβος αυθεντικοποιείται και η ταυτότητά του είναι γνωστή στους υπόλοιπους κόμβους.

2.3.1.1 Δημόσια Αλυσίδα των Μπλοκ

Το Bitcoin είναι το πιο γνωστό παράδειγμα εφαρμογής, η λειτουργία της οποίας βασίζεται σε δημόσια μπλοκ αλυσίδα. Στο Bitcoin, οι προαναφερθείσες καταστάσεις αντιστοιχούν σε ψηφιακά νομίσματα (κρυπτονομίσματα) και μια συναλλαγή περιλαμβάνει τη μεταφορά νομισμάτων από μία διεύθυνση σε κάποια άλλη. Κάθε κόμβος διαδίδει το σύνολο συναλλαγών που θέλει να εκτελέσει. Ειδικοί κόμβοι που ονομάζονται εξορύκτες (miners) συγκεντρώνουν τις συναλλαγές αυτές σε μπλοκ, ελέγχουν την εγκυρότητά τους και κοινοποιούν στους υπόλοιπους ένα πρωτόκολλο συναίνεσης προκειμένου να προσαρτήσουν τα μπλοκ που δημιούργησαν στην μπλοκ αλυσίδα. Το Bitcoin χρησιμοποιεί την απόδειξη εργασίας (proof-of-work – PoW) ως πρωτόκολλο συναίνεσης: μόνο ο miner που έχει επιλύσει επιτυχώς ένα δύσκολο υπολογιστικά πρόβλημα (εύρεση του σωστού nonce για την κεφαλίδα του μπλοκ) μπορεί να προσαρτηθεί στο blockchain. Το PoW είναι ανεκτικό στη βυζαντινή αποτυχία, αλλά είναι από τη φύση του πιθανοκρατικό, καθώς είναι πιθανό να προστεθούν ταυτόχρονα δύο μπλοκ στην αλυσίδα. Το Bitcoin επιλύει αυτό το ζήτημα θεωρώντας πως ένα μπλοκ είναι έγκυρο εφόσον αυτό ακολουθείται από έναν συγκεκριμένο αριθμό μπλοκ (τυπικά έξι μπλοκ). Αυτή η πιθανοτική προσέγγιση οδηγεί σε ζητήματα ασφάλειας και επίδοσης, καθώς έχει πραγματοποιηθεί πείραμα όπου ένας επιτιθέμενος έχει υπό τον έλεγχό του το 25% των κόμβων ενός δικτύου [34] και ο ρυθμός εκτέλεσης συναλλαγών Bitcoin παραμένει πολύ χαμηλός (7 συναλλαγές ανά δευτερόλεπτο [35]). Τα περισσότερα δημόσια συστήματα blockchain χρησιμοποιούν παραλλαγές του πρωτοκόλλου PoW για συναίνεση. Το PoW λειτουργεί καλά στα δημόσια περιβάλλοντα επειδή προστατεύει το δίκτυο από Συβιλλικές Επιθέσεις [33]. Εντούτοις, δεδομένου ότι δεν συνιστά έναν ντετερμινιστικό τρόπο συναίνεσης και υπολογιστικά

είναι πολύ δαπανηρός, είναι ακατάλληλος για τραπεζικές και οικονομικές εφαρμογές που απαιτούν τη διαχείριση τεράστιου όγκου συναλλαγών με έναν αιτιοκρατικό τρόπο.

2.3.1.2 Ιδιωτική Αλυσίδα των Μπλοκ

Το Hyperledger [36] είναι ένα από τα δημοφιλέστερα παραδείγματα ιδιωτικών blockchains. Δεδομένου ότι η ταυτότητα των κόμβων που το συνιστούν είναι γνωστή, τα περισσότερα blockchains υιοθετούν ένα από τα πρωτόκολλα κατανεμημένης συναίνεσης που είναι ιδιαίτερα δημοφιλή στη βιβλιογραφία, όπως Raft [37], Paxos [38] και PBFT [32]. Η πρώτη έκδοση του Hyperledger χρησιμοποίησε απευθείας το πρωτόκολλο PBFT, ενώ άλλα συστήματα, όπως τα Parity [39] και ErisDB [40], αναπτύσσουν τις δικές τους παραλλαγές πρωτοκόλλων συναίνεσης. Εκτός από την αιτιοκρατική συναίνεση, μια άλλη βασική ιδιότητα των ιδιωτικών μπλοκ αλυσίδων είναι ότι υποστηρίζουν έξυπνα συμβόλαια που μπορούν να εκφράζουν πολύπλοκες λογικές συναλλαγών. Αυτές οι ιδιότητες είναι ιδιαίτερα επιθυμητές στα επιχειρησιακά και χρηματοπιστωτικά συστήματα. Πράγματι, οι ιδιωτικές μπλοκ αλυσίδες προκαλούν το ενδιαφέρον των μεγάλων τραπεζικών και χρηματοπιστωτικών ιδρυμάτων, επιτρέποντας έτσι σε μερικούς να ισχυριστούν ότι η τεχνολογία αυτή έχει τη δυναμική να ανατρέψει τις τρέχουσες πρακτικές στη διαχείριση δεδομένων [41] [42].

2.3.2 Βασικές Έννοιες των Μπλοκ Αλυσίδων και Τρέχουσες Εξελίξεις

2.3.2.1 Κατανεμημένο Λογιστικό Βιβλίο

Ένα λογιστικό βιβλίο είναι ουσιαστικά μια δομή δεδομένων που αποτελείται από μια λίστα ταξινομημένων συναλλαγών, όπως νομισματικές συναλλαγές μεταξύ πολλαπλών τραπεζών ή συναλλαγές αγαθών που ανταλλάσσονται μεταξύ τρίτων. Στο blockchain, η δομή αυτή αναπαράγεται σε όλους τους κόμβους, όπου συναλλαγές ομαδοποιούνται σε μπλοκ και στη συνέχεια συνδέονται μεταξύ τους. Μία αλυσίδα από μπλοκ ξεκινά με κάποιες αρχικές καταστάσεις και στη συνέχεια καταγράφει ολόκληρο το ιστορικό των διαδικασιών ενημέρωσης που γίνονται στις καταστάσεις αυτές.

Ένα σύστημα που χρησιμοποιεί τη συγκεκριμένη δομή δεδομένων, έχει καθορίσει αρχικά τα εξής: (α) το είδος των δεδομένων που αποθηκεύονται στη δομή αυτή ορίζοντας το μοντέλο δεδομένων που θα ακολουθήσει. Για παράδειγμα, μία εφαρμογή κρυπτονομίσματος μπορεί να υιοθετήσει το μοντέλο χρήστη-λογαριασμού που μοιάζει με αυτό των παραδοσιακών τραπεζικών συστημάτων. Από την άλλη πλευρά, ένα blockchain γενικού σκοπού μπορεί να χρησιμοποιεί μοντέλο χαμηλού επιπέδου, όπως έναν πίνακα ή ζεύγη κλειδιών-τιμών· (β) τον αριθμό των αλυσίδων μπλοκ που

μπορεί να συνδέονται μεταξύ τους. Για παράδειγμα, μια μεγάλη επιχείρηση μπορεί να χρησιμοποιεί ταυτοχρόνως πολλά ledgers, ένα για κάθε τμήμα της (π.χ. εξυπηρέτηση πελατών, αλυσίδα εφοδιασμού, μισθοδοσία κ.λπ.)· (γ) τον κύριο ιδιοκτήτη της δομής αυτής, καθώς η τελευταία μπορεί να είναι είτε ανοιχτή στο κοινό ή να ελέγχεται αυστηρά από έναν και μόνο φορέα. Παραδείγματος χάρη, το Bitcoin είναι εντελώς ανοικτό και ως εκ τούτου απαιτεί ακριβό πρωτόκολλο συναίνεσης προκειμένου να προσδιοριστεί ποιος μπορεί να ενημερώσει ανάλογα την μπλοκ αλυσίδα. Αντιθέτως, το Parity προκαθορίζει ένα σύνολο ιδιοκτητών που μπορούν να γράψουν στην αλυσίδα.

Κρυπτονομίσματα: Η πιο επιτυχημένη υιοθέτηση της τεχνολογίας blockchain έχει γίνει από τις εφαρμογές κρυπτονομισμάτων. Μετά την επιτυχία του Bitcoin, έχουν εμφανιστεί πολλά ανταγωνιστικά νομίσματα. Τα περισσότερα από αυτά τα εναλλακτικά νομίσματα (alt-coins), όπως τα Litecoin ή Dodgecoin, υιοθετούν παρόμοια μοντέλα δεδομένων με το Bitcoin. Το Ethereum ξεφεύγει από το μοντέλο του Bitcoin που βασίζεται στις συναλλαγές και εφαρμόζει ένα μοντέλο βασισμένο σε λογαριασμούς. Η φύση των εφαρμογών κρυπτονομισμάτων απαιτεί η μπλοκ αλυσίδα να είναι ανοιχτή και το σύστημα να διατηρεί μόνο μία.

Ψηφιακά Περιουσιακά Αγαθά: Το κρυπτονόμισμα είναι ένα παράδειγμα ψηφιακού περιουσιακού αγαθού, δηλαδή δεδομένων με αξία στον πραγματικό κόσμο. Σε αντίθεση με τα κρυπτονομίσματα, τα ψηφιακά αγαθά δημιουργούνται από οντότητες του πραγματικού κόσμου και το blockchain αποτελεί απλώς ένα μέσο για την καταγραφή της ύπαρξής τους και των ανταλλαγών τους. Οι εφαρμογές Multichain [43], BigchainDB [44] και Corda [45] προσφέρουν δομές για την αποθήκευση και την παρακολούθηση ιστορικού περιουσιακών στοιχείων. Όπως και το Bitcoin, τα μοντέλα δεδομένων τους βασίζονται σε συναλλαγές και επικεντρώνονται γύρω από τα στοιχεία αυτά. Τα συστήματα αυτά βασίζονται κυρίως σε ιδιωτικές μπλοκ αλυσίδες, στις οποίες πολλοί οργανισμοί μπορούν να στραφούν σε ένα δίκτυο για να ανταλλάξουν περιουσιακά στοιχεία μεταξύ τους. Οι οργανισμοί αυτοί θεωρούνται και οι ιδιοκτήτες των αλυσίδων και είναι λογικό να υπάρχουν περισσότερες από μία αλυσίδες μπλοκ. Τα συστήματα Stellar [46], Ripple [47] και IOTA [48] εκδίδουν τα δικά τους στοιχεία (μάρκες) και προσφέρουν τις μπλοκ αλυσίδες τους ως μέσο ανταλλαγής ή σαν μία πλατφόρμα μικροπληρωμών. Ειδικότερα, η IOTA επιτρέπει τη μικροπληρωμή με μηδενική χρέωση μέσω των μαρκών της, γεγονός που καθιστά την μπλοκ αλυσίδα χρήσιμη για ανταλλαγές μεταξύ συσκευών IoT. Τα λογιστικά βιβλία σε αυτά τα συστήματα υιοθετούν μοντέλα δεδομένων βάσει λογαριασμών. Σε κάθε σύστημα υπάρχει μία μπλοκ αλυσίδα και αυτή είναι ανοιχτή· ο καθένας δηλαδή μπορεί να αγοράσει μάρκες και να λάβει μέρος στις ανταλλαγές.

Γενικές Εφαρμογές: Πέρα από τις δύο προαναφερθείσες εφαρμογές της τεχνολογίας blockchain, ορισμένες αλυσίδες μπλοκ υποστηρίζουν την εκτέλεση γενικών υπολογισμών, καθορισμένων από τον χρήστη (γνωστών ως έξυπνα συμβόλαια). Το Ethereum

και οι απόγονοί του, δηλαδή τα Monax, Parity, Dfinity κ.α., επιτρέπουν στους χρήστες να γράψουν αυθαίρετες επιχειρησιακές λογικές που εκτελούνται πάνω από το blockchain. Για παράδειγμα, τα συμβόλαια του Ethereum χρησιμοποιούνται σε περιπτώσεις απλών εκστρατειών εύρεσης χρηματοδότησης από το πλήθος (crowdfunding) έως σε εφαρμογές Αποκεντρωμένης Αυτόνομης Οργάνωσης (Decentralised Autonomous Organisation – DAO) [49]. Το Dfinity παρέχει ένα ειδικό είδος συμβολαίου, το "συμβόλαιο διακυβέρνησης", το οποίο επιβάλλει κανονισμούς πραγματικού κόσμου σε μπλοκ αλυσίδες τύπου Ethereum. Το Hyperledger υποστηρίζει την εκτέλεση κώδικα. Προσφέρει μοντέλο δεδομένων ζευγών κλειδιού-τιμής, με το οποίο οι εφαρμογές μπορούν να δημιουργούν και να ενημερώνουν τέτοια ζεύγη στην μπλοκ αλυσίδα.

2.3.2.2 Συναίνεση

Το περιεχόμενο της μπλοκ αλυσίδας αντικατοπτρίζει τις ιστορικές και τωρινές καταστάσεις που διατηρεί το blockchain. Η αναπαραγωγή των ενημερώσεων της αλυσίδας πρέπει να συμφωνηθεί από όλα τα μέρη. Με άλλα λόγια, πολλοί κόμβοι πρέπει να συναινέσουν, κάτι το οποίο δεν συμβαίνει σε πολλές εφαρμογές του πραγματικού κόσμου, όπως στις περιπτώσεις που η τράπεζα ή η κυβέρνηση αποφασίζει τις ενημερώσεις των τιμών συναλλάγματος.

Η ερευνητική βιβλιογραφία σχετικά με την κατανεμημένη συναίνεση είναι τεράστια και υπάρχουν πολλές παραλλαγές των προαναφερθέντων προτεινόμενων πρωτοκόλλων που αναπτύσσονται για τις μπλοκ αλυσίδες [50]. Τα πρωτόκολλα αυτά μπορούν να ταξινομηθούν ως εξής:

- Πρωτόκολλα βασισμένα σε υπολογισμούς: χρήση της απόδειξης επιτυχούς υπολογισμού για την τυχαία επιλογή κόμβου που θα αποφασίσει μεμονωμένα την επόμενη ενέργεια. Ένα παράδειγμα τέτοιου πρωτοκόλλου είναι το PoW του Bitcoin.
- Πρωτόκολλα βασισμένα στην επικοινωνία: οι κόμβοι του δικτύου είναι ισότιμοι και περνούν από πολλαπλά στάδια επικοινωνίας για να καταλήξουν σε συναίνεση. Το PBFT είναι ένα χαρακτηριστικό παράδειγμα τέτοιων πρωτοκόλλων. Τα πρωτόκολλα αυτά χρησιμοποιούνται σε ιδιωτικές μπλοκ αλυσίδες επειδή προϋποθέτουν τη γνώση της ταυτότητας των κόμβων.
- Υβριδικά πρωτόκολλα: στοχεύουν στη βελτίωση των επιδόσεων των δύο παραπάνω ειδών πρωτοκόλλων. Για παράδειγμα, το πρωτόκολλο Απόδειξης Παρελθόντος Χρόνου (Proof-of-Elapsed-Time – PoET) εξαλείφει τις ακριβές διαδικασίες εξόρυξης του PoW μέσω της αξιοποίησης αξιόπιστου υλικού, όπως το Intel SGX. Ένα άλλο παράδειγμα είναι το πρωτόκολλο Απόδειξης Αρχής (Proof-of-Authority – PoA) [51], το οποίο βελτιώνει το PBFT μέσω προεπιλογής ενός μικρού συνόλου αξιόπιστων κόμβων που ψηφίζουν μεταξύ τους για την επίτευξη συναίνεσης. Ομοίως, τα Stellar και Ripple βελτιώνουν το PBFT με την επίτευξη

συναίνεσης σε μικρότερα δίκτυα.

2.3.2.3 Κρυπτογράφηση

Τα συστήματα blockchain χρησιμοποιούν τεχνικές κρυπτογράφησης για την εξασφάλιση της ακεραιότητας των περιεχομένων της αλυσίδας μπλοκ. Η ακεραιότητα εδώ αναφέρεται στην ικανότητα ανίχνευσης τυχόν παραβίασης των δεδομένων blockchain. Αυτή η ιδιότητα είναι ζωτικής σημασίας σε δημόσιες εφαρμογές όπου δεν υπάρχει προκαθορισμένη εμπιστοσύνη. Για παράδειγμα, η εμπιστοσύνη του κοινού στα κρυπτονομίσματα όπως το Bitcoin, το οποίο καθορίζει τις αξίες των νομισμάτων, εξαρτάται από την ακεραιότητα του ίδιου του blockchain (δηλαδή το ίδιο πρέπει να είναι σε θέση να ανιχνεύσει διπλές δαπάνες). Ακόμη και σε ιδιωτικές μπλοκ αλυσίδες, η εξασφάλιση ακεραιότητας είναι εξίσου απαραίτητη επειδή, παρόλο που οι κόμβοι έχουν ταυτοποιηθεί, μπορεί να δράσουν κακόβουλα.

Υπάρχουν τουλάχιστον δύο επίπεδα προστασίας της ακεραιότητας των δεδομένων. Αρχικά, οι καταστάσεις προστατεύονται από ένα δέντρο κατακερματισμού (Merkle tree), του οποίου ο κατακερματισμός έχει αποθηκευτεί σε ένα μπλοκ. Οποιαδήποτε αλλαγή κατάστασης έχει ως αποτέλεσμα μία νέα τιμή κατατεμαχισμού ρίζας (root hash). Δεύτερον, το ιστορικό των μπλοκ είναι προστατευμένο, δηλαδή τα μπλοκ είναι αμετάβλητα μόλις προσαρτηθούν στο blockchain. Η βασική τεχνική έγκειται στη σύνδεση των μπλοκ μέσω μίας αλυσίδας κρυπτογραφικών δεικτών κατακερματισμού: το περιεχόμενο του μπλοκ με αριθμό $n + 1$ περιέχει το hash του μπλοκ με αριθμό n. Με αυτόν τον τρόπο, οποιαδήποτε τροποποίηση στο μπλοκ n ακυρώνει αμέσως όλα τα επόμενα μπλοκ. Συνδυάζοντας τα δέντρα Merkle και τους δείκτες κατακερματισμού, το blockchain προσφέρει ένα ασφαλές και αποτελεσματικό μοντέλο δεδομένων που παρακολουθεί όλες τις ιστορικές αλλαγές που έγιναν στις καταστάσεις.

Το μοντέλο ασφάλειας του Blockchain προϋποθέτει την ύπαρξη κρυπτογραφίας δημόσιου κλειδιού. Οι ταυτότητες, συμπεριλαμβανομένων των ταυτοτήτων χρηστών και συναλλαγών, προέρχονται από πιστοποιητικά δημόσιου κλειδιού. Επομένως, η ασφαλής διαχείριση των κλειδιών είναι απαραίτητη για όλες τις μπλοκ αλυσίδες. Όπως και σε άλλα συστήματα ασφάλειας, η απώλεια ιδιωτικών κλειδιών σημαίνει απώλεια πρόσβασης. Όμως, σε εφαρμογές blockchain όπως στα κρυπτονομίσματα, η απώλεια των κλειδιών έχει άμεσες και αμετάκλητες οικονομικές επιπτώσεις. Υπάρχουν πολλά συστήματα υπό έρευνα που επεκτείνουν τον αρχικό σχεδιασμό της μπλοκ αλυσίδας ενσωματώνοντας νέα και πολύπλοκα κρυπτογραφικά πρωτόκολλα. Σκοπός τους είναι να βελτιώσουν την ασφάλεια και την απόδοση με εσωτερικές τεχνικές, όπως αποδείξεις μηδενικής γνώσης (zero-knowledge proofs), υπογραφές ομάδας και αξιόπιστο υλικό.

2.3.2.4 Έξυπνα Συμβόλαια

Ένα *Έξυπνο Συμβόλαιο* (Smart Contract) αναφέρεται στον υπολογισμό που εκτελείται όταν πραγματοποιείται μια συναλλαγή. Μπορεί να θεωρηθεί ως μια αποθηκευμένη διαδικασία που επικαλείται μια συναλλαγή. Ο όρος αυτός αναφέρεται στα συμβόλαια εκείνα που έχουν οριστεί από τους ίδιους τους χρήστες ενός συστήματος κ όχι στην ενσωματωμένη λογική κάθε blockchain για την εκτέλεση των συναλλαγών μεταξύ των κόμβων του δικτύου (λογική που αφορά τον προσδιορισμό της εισόδου και εξόδου κάθε συναλλαγής αλλά και του τρόπου που επηρεάζεται η κατάσταση των κόμβων έπειτα από την εκτέλεσή της).

Στη βιβλιογραφία υπάρχουν πολλές ερευνητικές εργασίες που αφορούν τα έξυπνα συμβόλαια. Για την κατηγοριοποίηση των έξυπνων συμβολαίων της βιβλιογραφίας, χρησιμοποιούνται τα εξής δύο στοιχεία που διαφέρουν ανά περίπτωση: (α) η γλώσσα για τη σύνταξη έξυπνων συμβολαίων και (β) το περιβάλλον εκτέλεσής τους. Όσον αφορά τη γλώσσα, υπάρχουν εφαρμογές που επιτρέπουν τον ορισμό σύνθετων αλλά σημασιολογικά περιορισμένων συμβολαίων, όπως τα Kadena και BigchainDB, προκειμένου αυτά να μπορούν να ελέγχονται για λόγους ασφαλείας. Αντίθετα, το Ethereum επιτρέπει τον καθορισμό αυθαίρετων υπολογισμών. Αναφορικά με τα περιβάλλοντα εκτέλεσής τους, υπάρχουν συστήματα που εκτελούν τα συμβόλαια εκεί όπου βρίσκονται και οι υπόλοιπες οντότητες που συνιστούν το σύστημα blockchain. Αντιθέτως, το Ethereum, για παράδειγμα, διαθέτει τη δική του εικονική μηχανή, ενώ το Hyperledger χρησιμοποιεί το Docker για τη διασφάλιση φορητότητας.

Κεφάλαιο 3

Γενικές Αρχές της Αρχιτεκτονικής Ασφαλούς Συστήματος Διαχείρισης Δεδομένων με Επίγνωση της Ιδιωτικότητας

3.1 Ευφυής Υπηρεσία Ασφάλειας και Προστασίας της Ιδιωτικότητας

3.1.1 Πλαίσιο Ελέγχου Πρόσβασης

Για τον έλεγχο αθέμιτης πρόσβασης σε δεδομένα, παραβίασης ιδιωτικότητας, προστασίας της εμπιστευτικότητας και της ακεραιότητας αλλά και χρήσης υπηρεσιών, χρησιμοποιείται μοντέλο μέσω του οποίου πραγματοποιείται η εξουσιοδότηση ή μη των χρηστών του συστήματος για τη διετέλεση διαφόρων ενεργειών. Για τον έλεγχο των αιτημάτων πρόσβασης χρησιμοποιούνται πολιτικές, οι οποίες καθορίζουν τον τρόπο που δίνεται η πρόσβαση σε δεδομένα και υπηρεσίες και εφαρμόζονται με τη χρήση μηχανισμών ελέγχου πρόσβασης.

Το μοντέλο ελέγχου πρόσβασης λαμβάνει υπόψη του τον υψηλό βαθμό ευαισθησίας από τον οποίο χαρακτηρίζονται τα δεδομένα που εμπλέκονται σε συναλλαγές υπηρεσιών κατανεμημένων-συνεργατικών συστημάτων, καθώς και όλα τα ιδιαίτερα χαρακτηριστικά των υπηρεσιών αυτών, όπως η πολυεπίπεδη φύση των δεδομένων, που μπορεί να είναι ενσωματωμένα σε ψηφιακά «έγγραφα» με τη μορφή XML, αλλά και ο αλυσιδωτός τρόπος παροχής υπηρεσιών, σε περιπτώσεις που απαιτούνται συχνές αλληλεπιδράσεις μεταξύ ετερογενών οργανισμών. Επιπρόσθετα, για την εξουσιοδότηση των χρηστών ακολουθείται πιστά το νομοθετικό πλαίσιο για την

προστασία των προσωπικών δεδομένων των χρηστών, ενσωματώνοντας απαιτήσεις που χαρακτηρίζονται ως «υποχρεώσεις ιδιωτικότητας», καθώς και παραμέτρους χωρικές, ιστορικές και χρονικές.

Πηγαίνοντας ένα βήμα παραπέρα, η συγκεκριμένη προσέγγιση μοντελοποίησης διαλειτουργεί με ένα μοντέλο ελέγχου πρόσβασης που λαμβάνει υπόψη του την προστασία της ιδιωτικότητας, υποστηρίζοντας τον σημασιολογικό ορισμό των αρχών και των πολιτικών προστασίας των δεδομένων [52]. Συγκεκριμένα, το πλαίσιο ελέγχου πρόσβασης βασίζεται σε δύο πλούσια σημασιολογικά μοντέλα που αναπαριστούν τις βασικές οντότητες που μετέχουν στο σύστημα και τις μεταξύ τους συσχετίσεις, καθώς και τις πολιτικές ελέγχου πρόσβασης, αντίστοιχα. Το *Σημασιολογικό Μοντέλο Πληροφοριών* μοντελοποιεί συγκεκριμένα:

- τους τύπους των δεδομένων που δημιουργούνται, συλλέγονται και διακινούνται μεταξύ φορέων και παρόχων υπηρεσιών για την ικανοποίηση αιτημάτων των χρηστών αυτών,
- τις ιδιότητες και τα προσωπικά στοιχεία των χρηστών,
- τη φύση των υπηρεσιών και των υποκείμενων διεργασιών,
- τις πολιτικές και τους κανόνες βάσει των οποίων θα πραγματοποιείται η πρόσβαση σε δεδομένα και υπηρεσίες, και τέλος,
- την ταξινόμηση ρόλων όλων των εμπλεκόμενων οντοτήτων και φορέων που συμμετέχουν στην παροχή υπηρεσιών.

Το *Σημασιολογικό Μοντέλο Πολιτικών*, το οποίο αποτελεί τη βάση λειτουργίας του μοντέλου ελέγχου πρόσβασης, βασίζεται στις νομικές και κανονιστικές απαιτήσεις για την προστασία των προσωπικών δεδομένων των χρηστών κατανεμημένων συστημάτων, οι οποίες ικανοποιούνται από κανόνες που αφορούν:

- τον έλεγχο πρόσβασης, λαμβάνοντας υπόψη τον σκοπό συλλογής, μετάδοσης και επεξεργασίας των δεδομένων,
- τις περιόδους υποχρεωτικής διατήρησης πληροφοριών στις βάσεις δεδομένων αλλά και υποχρεωτικής διαγραφής αυτών,
- τη διαχείριση ταυτοτήτων και ψευδωνύμων κατά την αλληλεπίδραση οργανισμών για την παροχή υπηρεσιών,
- την εφαρμογή μηχανισμών ασφάλειας για την προστασία των προσωπικών δεδομένων κατά την αλληλεπίδραση είτε οργανισμών είτε των επιμέρους οντοτήτων ενός συστήματος και τέλος,
- τη δυνατότητα ορισμού προτιμήσεων ιδιωτικότητας, παροχής ή άρσης συναίνεσης σε πραγματικό ή μη χρόνο για την υποστήριξη ενεργού ρόλου των χρηστών.

Οι σημασιολογικά ορισμένες πολιτικές που περιέχουν συσχετίσεις μεταξύ των εμπλεκόμενων οντοτήτων στην παροχή υπηρεσιών εξετάζονται από το υποσύστημα ελέγχου πρόσβασης και ελέγχουν δεδομένα που μπορεί να απαιτούνται για την παροχή υπηρεσιών και την αλληλεπίδραση ετερογενών οργανισμών για τον διαμοιρα-

σμό δεδομένων, και, βάσει λογικής εξαγωγής συμπερασμάτων, προκύπτουν οι κανόνες εξουσιοδοτήσεων.

Δεδομένου ότι γίνεται χρήση των ιδιαίτερων χαρακτηριστικών που σχετίζονται με τις υπηρεσίες, τα δεδομένα και τους χρήστες του συστήματος για την αποτίμηση των αιτημάτων πρόσβασης, ο έλεγχος πρόσβασης ακολουθεί το μοντέλο Ελέγχου Πρόσβασης Βάσει Ιδιοτήτων (Attribute-Based Access Control – ABAC). Έτσι, κάθε εξουσιοδότηση αναφέρεται σε ιδιότητες του υποκειμένου και αντικειμένου αυτής, όπως, όνομα και ημερομηνία γέννησης των χρηστών και μεταδεδομένων των υπηρεσιών.

Στην ευφυή υπηρεσία ασφάλειας που παρουσιάζεται στην παρούσα διδακτορική διατριβή υπάρχουν οι οντότητες εκείνες που είναι υπεύθυνες για τη διαχείριση των πολιτικών, την επεξεργασία και αξιολόγηση του αιτήματος πρόσβασης σε κάποιο πόρο βάσει των ορισμένων πολιτικών, καθώς και τη λήψη απόφασης εξουσιοδότησης και εφαρμογής αυτής. Όσον αφορά τις πολιτικές, εκτός από εκείνες που αφορούν εξουσιοδοτήσεις για πρόσβαση σε δεδομένα και υπηρεσίες και σχετίζονται άμεσα με φορείς παροχής υπηρεσιών, ορίζονται επίσης πολιτικές σχετικά με τον τρόπο χρήσης προσωπικών δεδομένων των χρηστών σε συστήματα παροχής υπηρεσιών για την εξυπηρέτηση των πρώτων, βάσει σκοπού και συνθηκών υπό των οποίων θα λάβει χώρα η προαναφερθείσα διαδικασία. Έτσι, πραγματοποιείται έλεγχος πρόσβασης τόσο κατά τη συλλογή δεδομένων των χρηστών και τη λήψη αιτημάτων πρόσβασης, όσο και κατά την παραχώρηση των πρώτων σε άλλους οργανισμούς για την ικανοποίηση των προαναφερθέντων αιτημάτων.

Για την εφαρμογή των πολιτικών αυτών και την αποτίμηση δικαιωμάτων με κρυπτογραφικά μέσα, χρησιμοποιείται η Κρυπτογράφηση βάσει Ιδιοτήτων (Attribute-Based Encryption – ABE), εξάγοντας κανόνες ορισμένους βάσει του σημασιολογικού μοντέλου πολιτικών σε μη πραγματικό χρόνο, υλοποιημένους σε ABE.

3.1.2 Μηχανισμός Κρυπτογράφησης

Για την προστασία των δεδομένων που συλλέγονται, επεξεργάζονται και διαμοιράζονται μεταξύ των οντοτήτων που συμμετέχουν στη διαδικασία παροχής υπηρεσιών, χρησιμοποιείται η Κρυπτογράφηση βάσει Ιδιοτήτων (Attribute-Based Encryption – ABE), όπου επεκτείνει την Κρυπτογράφηση βάσει Ταυτότητας (Identity-Based Encryption – IBE) και το ιδιωτικό κλειδί του χρήστη αλλά και το κρυπτογράφημα εξαρτώνται από διάφορα χαρακτηριστικά του, θεωρώντας την ταυτότητα του χρήστη ως ένα χαρακτηριστικό. Η αποκρυπτογράφηση ενός κρυπτοκειμένου εξαρτάται μόνο από τις ιδιότητες που φέρει αυτός, όπως, για παράδειγμα, το επάγγελμά του, η ηλικία του, ο ασφαλιστικός φορέας στον οποίο ανήκει κ.ο.κ. Η κρυπτογράφηση βάσει ιδιοτήτων χρησιμοποιείται για την κρυπτογράφηση δομών δεδομένων και μηνυμά-

των που φέρουν προσωπικά δεδομένα των χρηστών με τρόπο τέτοιο ώστε να είναι αποδοτική η διαδικασία μετάδοσης των δεδομένων αυτών, έχοντας πάντα ως πρωταρχικό στόχο την προστασία της ιδιωτικότητάς τους.

Από τις διάφορες προεκτάσεις της κρυπτογράφησης βάσει ιδιοτήτων που έχουν προταθεί ερευνητικά, χρησιμοποιείται η Κρυπτογράφηση βάσει Ιδιοτήτων με την ενσωμάτωση κανόνων στο κρυπτογράφημα (Ciphertext-Policy Attribute Based Encryption – CP-ABE) και οι κανόνες αυτοί περιλαμβάνουν δέντρα πρόσβασης που αποτελούνται από λογικές σχέσεις μεταξύ χαρακτηριστικών. Για την εφαρμογή κρυπτογράφησης βάσει ιδιοτήτων με την ενσωμάτωση κανόνων στο κρυπτογράφημα, χρησιμοποιούνται οι εξής τέσσερις αλγόριθμοι:

- Setup: Ο αλγόριθμος αυτός έχει ως είσοδο μόνο μία παράμετρο ασφάλειας k και δημιουργεί τα κλειδιά PK και MK.
- Encrypt(PK, M, A): Για την κρυπτογράφηση ενός μηνύματος M, χρησιμοποιείται το κλειδί PK και ένα δέντρο πρόσβασης A, που αναπαριστά το σχετικό κανόνα πρόσβασης ορισμένο βάσει συσχετίσεων μεταξύ ιδιοτήτων του χρήστη. Ο αλγόριθμος αυτός δημιουργεί ένα κρυπτογράφημα CT, τέτοιο ώστε μόνο χρήστες που φέρουν ένα σύνολο ιδιοτήτων που ικανοποιούν τη δομή πρόσβασης A να μπορούν να το αποκρυπτογραφήσουν.
- Key Generation(MK, S): Ο αλγόριθμος αυτός χρησιμοποιείται για τη δημιουργία ιδιωτικού κλειδιού SK του χρήστη και απαιτεί ως είσοδο το κλειδί MK καθώς και το σύνολο ιδιοτήτων του χρήστη S για το οποίο θα δημιουργηθεί το κλειδί.
- Decrypt(PK, CT, SK): Για την αποκρυπτογράφηση του κρυπτογραφήματος CT απαιτείται η χρήση του δημόσιου κλειδιού PK, καθώς και του ιδιωτικού κλειδιού του χρήστη SK. Εάν το σύνολο S των ιδιοτήτων του χρήστη που περιέχεται στο κλειδί SK ικανοποιεί τον κανόνα βάσει του οποίου έχει κρυπτογραφηθεί το μήνυμα, πραγματοποιείται τότε και η αποκρυπτογράφηση αυτού.

3.2 Μηχανισμός Διαφανούς και Αξιόπιστης Διακίνησης Δεδομένων

Το Blockchain αποτελεί ουσιαστικά μία συνδεδεμένη λίστα επικυρωμένων μπλοκ που παρατίθενται σε χρονολογική σειρά. Τα μπλοκ αυτά έχουν ένα μοναδικό αναγνωριστικό 256 bit, το οποίο υπολογίζεται ως το κρυπτογραφικό άθροισμα ελέγχου των περιεχομένων του κάθε μπλοκ. Κάθε μπλοκ αποτελείται από μία κεφαλίδα με πληροφορίες σχετικά με τη μέρα και ώρα που πραγματοποιήθηκε η συναλλαγή, καθώς και από την ίδια τη συναλλαγή που αντιστοιχεί σε μία πράξη σε δεδομένα. Σε συνδυασμό με ισχυρούς κρυπτογραφικούς μηχανισμούς, η τεχνολογία Blockchain αποτελεί μία ασφαλή μέθοδο ανταλλαγής δεδομένων ιδιαίτερα κρίσιμων, όπως είναι τα προσωπικά δεδομένα του κάθε χρήστη. Δεδομένου ότι η πληροφορία λογίζεται ως

ένα πολύτιμο αγαθό στη σημερινή οικονομία, τα προσωπικά δεδομένα πρέπει να αντιμετωπίζονται ομοίως ως χρήματα. Προκειμένου να αποφευχθεί η ανάγκη μιας έμπιστης κεντρικής αρχής και να διασφαλιστεί η εμπιστοσύνη και η ιδιωτικότητα των χρηστών ενός συστήματος, η χρήση μίας απαραβίαστης, ιδιωτικής αλυσίδας μπλοκ επιτρέπει τον αυτόματο έλεγχο μετάδοσης δεδομένων, καθώς παρακολουθείται έτσι η ανταλλαγή τους μεταξύ των διαφορετικών οντοτήτων του συστήματος, ενώ παράλληλα ενσωματώνει κρυπτογραφημένες πληροφορίες σχετικά με την πηγή των δεδομένων, καθώς και τους κανόνες πρόσβασης στα δεδομένα αυτά. Με τον τρόπο αυτό, επιτυγχάνεται διαφάνεια και εξασφαλίζεται ισχυρή προστασία της ιδιωτικότητας του χρήστη. Τέλος, μέσω της χρήσης έξυπνων συμβολαίων πραγματοποιείται η ανταλλαγή των προαναφερθέντων δεδομένων, επιβεβαιώνοντας κάθε φορά την ορθότητα των ανταλλαγών βάσει των πολιτικών πρόσβασης στα δεδομένα που έχει ορίσει ο χρήστης, εξασφαλίζοντας ταυτόχρονα τη συμμόρφωση των υποκείμενων διαδικασιών με το υφιστάμενο νομικό και κανονιστικό πλαίσιο προστασίας της ιδιωτικότητας.

Κεφάλαιο 4

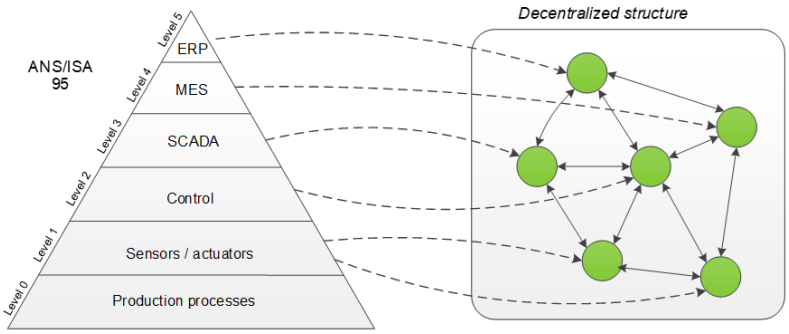
Μελέτη Τομέων Εφαρμογής του Ολοκληρωμένου Πλαισίου Ασφάλειας και Προστασίας της Ιδιωτικότητας

4.1 Συνεργατικά Περιβάλλοντα Διαχείρισης Παραγωγής

Οι σημερινές αγορές επιβάλλουν ισχυρές απαιτήσεις στις βιομηχανικές επιχειρήσεις, απαιτώντας προϊόντα υψηλής ποιότητας και μειωμένης τιμής που χαρακτηρίζονται από έναν υψηλό βαθμό προσαρμοστικότητας. Τα μελλοντικά αυτοματοποιημένα συστήματα θα πρέπει να ενσωματώσουν νέες μεθοδολογίες και τεχνολογίες που θα επιτρέπουν την προσαρμογή τους στις μεταβαλλόμενες αυτές απαιτήσεις, καθώς και στα νέα μοντέλα προϊόντων. Οι προκλήσεις σχετίζονται βασικά με την ανάπτυξη πιο σύνθετων συστημάτων, ικανών να συνεργαστούν με άλλα συστήματα, να παραμετροποιούνται και να ανταποκρίνονται στις υψηλές απαιτήσεις. Αυτό το όραμα χαρακτηρίζει τη *Βιομηχανία 4ης γενιάς* ή όπως αυτή έγινε γνωστή με τον όρο "Industrie 4.0" [53], η οποία προωθεί τη μηχανοργάνωση των παραδοσιακών βιομηχανιών για τον μετασχηματισμό τους σε «έξυπνα» εργοστάσια που χαρακτηρίζονται από προσαρμοστικότητα, αποδοτικότητα, λειτουργικότητα, αξιοπιστία, ασφάλεια και χρηστικότητα, υποστηρίζοντας ταυτόχρονα την ενσωμάτωση πελατών και συνεργατών. Το όραμα αυτό βασίζεται στην αξιοποίηση της κατανεμημένης νοημοσύνης και των ικανοτήτων αυτοπροσαρμογής, αυτοδιαμόρφωσης και αυτοδιάγνωσης των υποκείμενων συστημάτων διαχείρισης παραγωγής.

Οι αναδυόμενες τεχνολογίες του *Διαδικτύου των Πραγμάτων* (Internet of Things – IoT) και των *Κυβερνοφυσικών Συστημάτων* (Cyber-Physical Systems – CPS) υπόσχο-

νται την επίτευξη διαλειτουργικότητας, ευελιξίας και παραμετροποίησης συσκευών και συστημάτων, καθιστώντας τα αποτελεσματικότερα ως προς την παραγωγικότητά τους και την κατανάλωση ενέργειας. Τα Κυβερνοφυσικά Συστήματα μπορούν να οριστούν ως ο συνδυασμός των τομέων Μηχανικής και Πληροφορικής για τον έλεγχο φυσικών διεργασιών και συστημάτων, σχεδιασμένα ως ένα δίκτυο αλληλεπιδρώντων συστημάτων λογισμικού, συσκευών και υλικού, καθένα από τα οποία χαρακτηρίζεται από υψηλό επίπεδο αυτονομίας ως προς τη λήψη αποφάσεων. Τα συστήματα CPS επικεντρώνονται σε ευφυή, δυναμικά και αυτόνομα συστήματα μεγάλης κλίμακας που εξασφαλίζουν δια- και ενδοεπιχειρησιακή ολοκλήρωση και λειτουργούν σε διάχυτα περιβάλλοντα. Χαρακτηριστικά παραδείγματα αυτών αποτελούν οι μονάδες παραγωγής και επεξεργασίας, τα ηλεκτρικά δίκτυα και οι αγωγοί, καθώς και η εφοδιαστική αλυσίδα. Ιδιαίτερα στον κατασκευαστικό τομέα παρατηρείται μία μετάβαση από τις υπάρχουσες δομές ιεραρχικού ελέγχου που βασίζονται στην πυραμίδα αυτοματισμού ISA 95 προς πιο αποκεντρωμένες και αναδιαμορφώσιμες δομές βασισμένες στις αρχές των συστημάτων CPS, όπως απεικονίζεται στο Σχήμα 4 [54].



Σχήμα 4: Μετάβαση Υφιστάμενων Συστημάτων προς τα Κυβερνοφυσικά Συστήματα στον Κατασκευαστικό Τομέα

Η πλήρης υιοθέτηση τέτοιων ιδεών και τεχνολογιών απαιτεί να πεισθούν για τα πλεονεκτήματα αυτών οι φορείς της βιομηχανίας, να εξασφαλιστεί η διαθεσιμότητα των κατάλληλων μεθοδολογιών μηχανικής λογισμικού και να ικανοποιηθούν οι βιομηχανικές απαιτήσεις, ιδίως όσον αφορά στην ανθεκτικότητα των υποδομών, στην ασφάλεια και στην προστασία των δεδομένων. Μια άλλη σημαντική πρόκληση για την ανάπτυξη και υιοθέτηση λύσεων CPS είναι η ομαλή μετάβαση των υφιστάμενων συστημάτων στα κυβερνοφυσικά συστήματα, η οποία "πρέπει να εφαρμοστεί σταδιακά μέσω της ψηφιακής αναβάθμισης των υφιστάμενων εγκαταστάσεων" [55]. Η προτυποποίηση αναλαμβάνει καθοριστικό ρόλο στη βιομηχανική υιοθέτηση λύσεων CPS, καθώς τα πρότυπα ενδέχεται να επηρεάσουν την ανάπτυξη, την εγκατάσταση και τη λειτουργία βιομηχανικών εφαρμογών. Για παράδειγμα, η προτυποποίηση μπορεί να υποστηρίξει την ανάπτυξη κυβερνοφυσικών συστημάτων και ιδιαίτερα την ομαλή μετάβαση σε αυτά διασυνδέοντάς τα εύκολα μέσω των κατάλληλων διεπαφών με υπάρχοντα συστήματα παλαιού τύπου, με συστήματα άμεσης εγκατάστασης και λειτουργίας (plug-and-play) και συσκευές, προσαρμόζοντας σε πραγμα-

τικό χρόνο τη συμπεριφορά τους και τη μεταξύ τους διαλειτουργικότητα.

4.1.1 Υφιστάμενα Πρότυπα Υποστήριξης Λύσεων Κυβερνοφυσικών Συστημάτων

Η ανάπτυξη λύσεων CPS περιλαμβάνει τη χρήση ετερογενών τεχνολογιών υλικού και λογισμικού, οργανωμένων σε ένα δίκτυο κατανεμημένων κόμβων ελέγχου, μερικοί από τους οποίους θα διασυνδέονται με υφιστάμενα επιχειρησιακά συστήματα και συσκευές. Η εφαρμογή τέτοιων συστημάτων συμμορφωμένων με πρότυπα είναι ζωτικής σημασίας για την υιοθέτησή τους στη βιομηχανία. Τα πρότυπα ορίζουν μια σειρά από κατανοητούς και σαφείς κανόνες για τη ρύθμιση προϊόντων, διαδικασιών ή υπηρεσιών, εξασφαλίζοντας την ποιότητα, την ασφάλεια και τη διαλειτουργικότητα [56]. Για τον λόγο αυτό, τα πρότυπα είναι αναγκαία για τη διασφάλιση της σωστής και αναμενόμενης λειτουργίας συστημάτων και της επιθυμητής ποιότητας προϊόντων, καθώς και την εξασφάλιση συμβατότητας με άλλον εξοπλισμό. Τα πρότυπα θεσπίζονται από φορείς προτυποποίησης εθνικής ή διεθνούς εμβέλειας, όπως IEEE, IEC και NIST.

Για τη διευκόλυνση της υιοθέτησής τους από τη βιομηχανία, πρέπει να υποστηριχθούν διάφορες κατηγορίες προτύπων, όπως: (α) ευφυείς, κατανεμημένες τεχνολογίες ελέγχου, (β) διαλειτουργικότητα, (γ) βιομηχανικά δίκτυα επικοινωνιών, (δ) ασφάλεια και (ε) διασύνδεση με έξυπνες συσκευές (π.χ. προσφέροντας τη δυνατότητα ελέγχου μηχανημάτων παραγωγής και διαδικασιών σε πραγματικό χρόνο). Επίσης, πρέπει να ληφθούν υπόψη ορισμένα πρότυπα που σχετίζονται με τον εκάστοτε τομέα εφαρμογής.

4.1.1.1 Κατανεμημένη Νοημοσύνη

Οι εγγενείς στρατηγικές κατανεμημένου ελέγχου στις λύσεις κυβερνοφυσικών συστημάτων μπορούν να υλοποιηθούν ακολουθώντας, για παράδειγμα, τις προσεγγίσεις των *Πολυπρακτορικών Συστημάτων* (Multi-Agent Systems – MASs) και των *Ολονικών Συστημάτων Παραγωγής* (Holonic Manufacturing Systems – HMSs) ή το πρότυπο της *Αρχιτεκτονικής Προσανατολισμένης σε Υπηρεσίες* (Service Oriented Architecture – SOA).

Ο φορέας FIPA (Foundation for Intelligent Physical Agents) [57] δημιούργησε τις προδιαγραφές για τη μηχανική ετερογενούς λογισμικού προσανατολισμένου σε πράκτορες, οι οποίες, προς το παρόν, συνιστούν το μοναδικό πρότυπο για την ανάπτυξη συστημάτων MAS. Οι προδιαγραφές FIPA ομαδοποιούνται σε διάφορες κατηγορίες [58]: εφαρμογές, αφηρημένη αρχιτεκτονική, επικοινωνία πρακτόρων, διαχείριση πρακτόρων και διάδοση μηνυμάτων πράκτορα. Οι προδιαγραφές των εφαρ-

μογών FIPA αναφέρονται στις περιοχές εφαρμογών όπου μπορούν να αναπτυχθούν πράκτορες FIPA, οι οποίοι θα αντιπροσωπεύουν περιγραφές σημασιολογικών μοντέλων και υπηρεσιών για έναν συγκεκριμένο τομέα. Οι προδιαγραφές αφηρημένης αρχιτεκτονικής FIPA αφορούν τις αφηρημένες οντότητες που απαιτούνται για την ανάπτυξη υπηρεσιών πράκτορα και του περιβάλλοντος αυτού. Οι προδιαγραφές επικοινωνίας πρακτόρων FIPA σχετίζονται με τη Γλώσσα Επικοινωνίας Πρακτόρων (Agent Communication Language – ACL), τα πρωτόκολλα αλληλεπίδρασης, τη μεταξύ τους επικοινωνία που βασίζεται στη λογική των ενεργειών τους και τις γλώσσες αναπαράστασης περιεχομένου. Συγκεκριμένα, περιλαμβάνει τις προδιαγραφές των πρωτοκόλλων αλληλεπίδρασης FIPA που καθορίζουν τα προεγκεκριμένα πρωτόκολλα για τα μηνύματα ACL που ανταλλάσσονται μεταξύ πρακτόρων. Οι προδιαγραφές διαχείρισης πρακτόρων FIPA αναφέρονται στον έλεγχο και στη διαχείριση των πρακτόρων εντός και μεταξύ πλατφορμών πρακτόρων και καθορίζουν ένα μοντέλο αναφοράς που ορίζει τη βασική δομή ενός συστήματος MAS που συμμορφώνεται με το πρότυπο FIPA. Τέλος, οι προδιαγραφές μετάδοσης μηνύματος πράκτορα FIPA αφορούν τη μεταφορά και την αναπαράσταση μηνυμάτων σε διάφορα δικτυακά πρωτόκολλα μεταφοράς.

Παρ' όλα αυτά, οι προδιαγραφές του προτύπου FIPA δεν λαμβάνουν υπόψη τους σημαντικές βιομηχανικές απαιτήσεις, όπως:

- Ασφάλεια και ιδιωτικότητα.
- Ενσωμάτωση υφιστάμενων επιχειρησιακών συστημάτων και συσκευών.
- Πρωτόκολλα αλληλεπίδρασης σε πραγματικό χρόνο για συστήματα μεγάλης κλίμακας, διασφαλίζοντας την επεκτασιμότητα και τον μειωμένο χρόνο καθυστέρησης.
- Ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων ACL για την υποστήριξη επεκτασιμότητας σε μεγάλης κλίμακας συστήματα, δεδομένου ότι το πρωτόκολλο μορφοποίησης του FIPA-ACL είναι αρκετά βαρύ, κυρίως λόγω της ύπαρξης κεφαλίδων στα διάφορα πεδία του, απαιτώντας έτσι τη μείωση του μεγέθους του.
- Κατανεμημένος μηχανισμός εξυπηρέτησης και εύρεσης πρακτόρων για τη βελτίωση της ανθεκτικότητας του συστήματος.

Εκτός από το πρότυπο FIPA, η πρωτοβουλία AUML (Agent Unified Modeling Language) επεκτείνει τη γλώσσα UML για να ανταποκριθεί στις απαιτήσεις εφαρμογών μεγάλης κλίμακας που βασίζονται σε πράκτορες [59].

Για την υιοθέτηση της αρχιτεκτονικής προσέγγισης SOA μπορούν να εντοπιστούν αρκετά πρότυπα. Συνήθως, οι υπηρεσιοστρεφείς αρχιτεκτονικές SOA βασίζονται σε *Υπηρεσίες Ιστού* (Web Services – WS), χρησιμοποιώντας πρότυπα και ανοιχτά πρωτόκολλα για την παροχή πλατφόρμας επικοινωνίας μεταξύ κατανεμημένων και ετερογενών συστημάτων και εφαρμογών. Οι περισσότερες πλατφόρμες υπηρεσιών ιστού αξιοποιούν πρότυπα βασισμένα στον Παγκόσμιο Ιστό, όπως το *Πρωτόκολλο*

Πρόσβασης Απλού Αντικειμένου (Simple Object Access Protocol – SOAP) [60][61][62] για τη μετάδοση δεδομένων, τη *Γλώσσα Περιγραφής Υπηρεσιών Διαδικτύου* (Web Services Description Language – WSDL) [63] για την περιγραφή των υπηρεσιών, τη *Γλώσσα Εκτέλεσης Επιχειρησιακών Διαδικασιών Υπηρεσιών Διαδικτύου* (Web Services Business Process Execution Language – WS-BPEL) και το πρότυπο της *Καθολικής Περιγραφής, Ανακάλυψης και Ολοκλήρωσης* (Universal Description, Discovery and Integration – UDDI) [64] για την περιγραφή των επιχειρήσεων και των υπηρεσιών που αυτές προσφέρουν.

Συγκεκριμένα, οι δυνατότητες εγγραφής και εύρεσης υπηρεσιών επιτυγχάνονται με τη χρήση του καταλόγου (μητρώου) UDDI και η περιγραφή της εκάστοτε υπηρεσίας μπορεί να γίνει χρησιμοποιώντας τις δομές περιγραφής WSDL. Η υπηρεσία περιγραφής WSDL παρέχει λειτουργίες για την κλήση της υπηρεσίας, τον ορισμό παραμέτρων εισόδου και της αναμενόμενης εξόδου. Το πρότυπο SOAP ορίζει τη δομή και τον τρόπο ανταλλαγής πληροφορίας μεταξύ των επιμέρους οντοτήτων του συστήματος. Επίσης, έχουν αναπτυχθεί μοντέλα αναφοράς για την καθοδήγηση ανάπτυξης συστημάτων που βασίζονται στην αρχιτεκτονική SOA. Συγκεκριμένα, η αρχιτεκτονική αναφοράς OASIS [65] και η πιο πρόσφατη αρχιτεκτονική αναφοράς SOA από τον οργανισμό Open Group [66] καθορίζουν κατευθυντήριες γραμμές και επιλογές για τον αρχιτεκτονικό σχεδιασμό τέτοιων συστημάτων.

Αναγνωρίζοντας τα οφέλη που προκύπτουν από τον συνδυασμό τεχνολογιών πρακτόρων με τις υπηρεσίες ιστού, ο φορέας FIPA δημιούργησε μία ομάδα εργασίας (Agents and Web Services Interoperability Working Group) με στόχο τον καθορισμό προτύπων που επιτρέπουν στους πράκτορες να μπορούν να αλληλεπιδρούν απρόσκοπτα με τις υπηρεσίες ιστού και αντιστρόφως.

4.1.1.2 Διαλειτουργικότητα

Σε ετερογενή συστήματα CPS, η διαλειτουργικότητα και η κατανόηση της γνώσης που διαμοιράζεται κατά τη διάρκεια των υποκείμενων συνεργατικών διαδικασιών αποτελούν δύο σημαντικές πτυχές. Για τον λόγο αυτό, πρέπει να λαμβάνονται υπόψη τα πρότυπα που αφορούν τη διαλειτουργικότητα, την ανταλλαγή πληροφορίας και την παροχή διεπαφών για την ενσωμάτωση υφιστάμενων επιχειρησιακών συστημάτων.

Το πρώτο εκ των δύο ζητημάτων σχετίζεται με την αναπαράσταση της γνώσης που διαμοιράζονται οι επιμέρους κατανεμημένες οντότητες του συνολικού συστήματος. Ένας τρόπος για την προτυποποίηση της διαμοιρασμένης γνώσης είναι η χρήση τεχνολογιών Σημασιολογικού Ιστού και οντολογικών μοντέλων, οι οποίες παρέχουν έναν κοινό τρόπο αναπαράστασης της γνώσης που διαχειρίζονται οι κατανεμημένοι πράκτορες. Τα υπάρχοντα σχετικά πρότυπα βασίζονται κυρίως στη γλώσσα XML, με πιο γνωστά το *Πλαίσιο Περιγραφής Πόρων* (Resource Description Framework

– RDF) [67] και τη *Γλώσσα Οντολογιών Ιστού* (Web Ontology Language – OWL) [68]. Η γλώσσα OWL διαθέτει ένα πλούσιο σύνολο προκαθορισμένων προτύπων μοντελοποίησης, υποστηρίζοντας, για παράδειγμα, τη συμπερίληψη περιορισμών στις μοντελοποιημένες έννοιες και στις μεταξύ τους σχέσεις.

Με στόχο την πραγματική διαλειτουργικότητα εντός των συστημάτων CPS, το δεύτερο σημαντικό ζήτημα αφορά στη χρήση προτυποποιημένων διεπαφών για την ενσωμάτωση υφιστάμενων επιχειρησιακών συστημάτων (legacy systems). Το πρωτόκολλο *Ελέγχου Διαδικασιών OLE* (OLE for Process Control – OPC) χρησιμοποιεί την τεχνολογία επικοινωνίας COM/DCOM της Microsoft, ενώ καθορίζει πρότυπα για την πρόσβαση σε δεδομένα. Η *Ενοποιημένη Αρχιτεκτονική OPC* (OPC-UA) στοχεύει στην εξάλειψη των περιορισμών της τεχνολογίας COM/DCOM χρησιμοποιώντας προηγμένες τεχνολογίες επικοινωνίας, όπως τις υπηρεσίες ιστού, επιτρέποντας την αντιμετώπιση θεμάτων ασφάλειας και αυτονομίας της πλατφόρμας. Με αυτόν τον τρόπο, η αρχιτεκτονική OPC-UA επικρατεί ως πρότυπο ώστε να καταστεί δυνατή η διαφανής διαλειτουργικότητα των συστημάτων, επιτρέποντας την κάθετη επικοινωνία μεταξύ των επιπέδων της πυραμίδας ISA 95.

4.1.1.3 Ασφάλεια και Προστασία Δεδομένων

Καθώς τα συστήματα CPS βασίζονται σε υπολογιστικές και φυσικές υποδομές, ενσωματώνοντας διαφορετικές στρατηγικές και αρχιτεκτονικές, όπως συστήματα MAS και αρχιτεκτονικές SOA, γίνονται ευάλωτα σε μια ποικιλία απειλών και επιθέσεων λόγω του συνδυασμού και της αλληλεπίδρασης των προαναφερθεισών οντοτήτων και τεχνολογιών. Έτσι, θα πρέπει να λαμβάνονται υπόψη οι πιο πρόσφατες πρακτικές και τεχνολογίες ασφάλειας προκειμένου να αντιμετωπίζονται τα διαφορετικά είδη εξωτερικών ή εσωτερικών απειλών των συστημάτων αυτών, να εντοπίζονται τυχόν τρωτά σημεία και να παρέχονται γενικά: (α) φυσική ασφάλεια, αποτρέποντας την πρόσβαση μη εξουσιοδοτημένου προσωπικού ή ακόμη και τυχαίων εισβολέων σε εφαρμογές λογισμικού και συσκευές, (β) ασφάλεια δικτύου, προστατεύοντας τα κανάλια επικοινωνίας από κακόβουλες δραστηριότητες ή κυβερνοεπιθέσεις, όπως ιοί, εισβολές ή άρνηση παροχής υπηρεσιών (DoS attack) και (γ) ασφάλεια πληροφοριακών συστημάτων και προστασία δεδομένων, αποτρέποντας ενέργειες μη εξουσιοδοτημένων χρηστών, προκειμένου να εξασφαλιστούν η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα δεδομένων και πόρων του συστήματος.

Η υιοθέτηση προτύπων ασφάλειας για την ασφαλή επικοινωνία, την αυθεντικοποίηση και την εξουσιοδότηση, καθώς και τον ορισμό και την επιβολή πολιτικών πρόσβασης είναι ουσιαστικής σημασίας. Όσον αφορά στη διασφάλιση της επικοινωνίας μεταξύ των οντοτήτων του συστήματος, η κρυπτογράφηση μηνυμάτων αποτελεί μια πολύ κοινή τεχνική για να εξασφαλιστεί η εμπιστευτικότητα της ανταλλασσόμενης πληροφορίας. Η ομάδα W3C ανέπτυξε το πρότυπο *XML Κρυπτογραφίας*

(XML Encryption) [69], το οποίο καθορίζει τον τρόπο κρυπτογράφησης των περιεχομένων ενός στοιχείου XML και επομένως μπορεί να χρησιμοποιηθεί για τη διασφάλιση σχημάτων επικοινωνίας που χρησιμοποιούν μηνύματα XML, π.χ. RDF. Επιπλέον, η προτυποποιημένη από την ίδια ομάδα *XML Υπογραφή* (XML Signature) [70] μπορεί να εφαρμοστεί σε οποιοδήποτε ψηφιακό περιεχόμενο, π.χ. μηνύματα SOAP, για λόγους διασφάλισης μη αποποίησης και ακεραιότητας των ανταλλασσόμενων μηνυμάτων.

Όσον αφορά στον έλεγχο ταυτότητας, η *Γλώσσα Σήμανσης Ασφάλειας* (Security Assertion Markup Language – SAML) [71] είναι ένα ανεξάρτητο από τον τρόπο μετάδοσης ανοιχτό πρότυπο του οργανισμού OASIS βασισμένο στη γλώσσα XML, το οποίο βασίζεται σε ένα πρότυπο αιτήματος-απάντησης για την ανταλλαγή πληροφοριών επαλήθευσης ταυτότητας χρήστη μεταξύ ενός παρόχου ταυτότητας και ενός παρόχου υπηρεσιών. Επιπλέον, ο *Έλεγχος Πρόσβασης βάσει Ρόλων* (Role-Based Access Control – RBAC) [72] προτυποποιήθηκε από τον οργανισμό NIST ως μηχανισμός εξουσιοδότησης για την παροχή δικαιωμάτων πρόσβασης στους χρήστες μέσω της εφαρμογής πολιτικών. Όσον αφορά στην προδιαγραφή πολιτικών και στην επιβολή τους, ο οργανισμός OASIS ανέπτυξε ένα πρότυπο που συμπληρώνει το SAML με ένα ευέλικτο σύστημα εξουσιοδότησης που υποστηρίζει την *Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης* (eXtensible Access Control Markup Language – XACML) [19], ένα πρότυπο βασισμένο στη γλώσσα XML που χρησιμοποιεί χαρακτηριστικά των υποκειμένων οντοτήτων και χρηστών του συστήματος για τον καθορισμό πολιτικών ελέγχου πρόσβασης και την αξιολόγηση αιτημάτων πρόσβασης σύμφωνα με τους κανόνες που ορίζονται στις πολιτικές.

4.2 Συστήματα Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Στη βιβλιογραφία συναντά κανείς πολλούς και διαφορετικούς ορισμούς της ηλεκτρονικής διακυβέρνησης, δίνοντας κάθε φορά έμφαση είτε στη συμβολή και εφαρμογή των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) σε αυτήν, είτε στον σκοπό και στον ενεργό ρόλο της καθώς και στους εμπλεκόμενους φορείς και πολίτες ως αποδέκτες των παρεχόμενων υπηρεσιών (π.χ. [73][74][75][76][77]. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, η ηλεκτρονική διακυβέρνηση συνίσταται "στη χρήση Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) στη Δημόσια Διοίκηση σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, με σκοπό τη βελτίωση παροχής δημοσίων υπηρεσιών, την ενδυνάμωση δημοκρατικών διαδικασιών αλλά και την υποστήριξη δημοσίων πολιτικών" [78]. Πράγματι, τα οφέλη της συμβολής των ΤΠΕ στον χώρο της δημόσιας διοίκησης έχουν αναγνωρισθεί ευρέως, καθώς η αξιοποίησή τους έχει ήδη οδηγήσει σε ταχύτερη εξυπηρέτηση των πολιτών και επιχειρήσεων χωρίς την απαίτηση εμπλοκής αυτών σε ενδιάμεσες διαδικασίες διεκπε-

ραίωσης υπηρεσιών, συνεχή πρόσβαση στις υπηρεσίες, μείωση κόστους αυτών και εξοικονόμηση πόρων λόγω βελτιωμένου συντονισμού των φορέων, καταπολέμηση της γραφειοκρατίας και λειτουργία των δημοσίων υπηρεσιών με αποτελεσματικότητα, διαφάνεια και αξιοπιστία.

4.2.1 Κατευθύνσεις Ηλεκτρονικής Διακυβέρνησης

Η έννοια της ηλεκτρονικής διακυβέρνησης είναι ιδιαίτερα σύνθετη καθώς εμπλέκει τον άνθρωπο, την τεχνολογία, κοινωνικές και οργανικές δομές καθώς και διαδικασίες. Με τον ανασχεδιασμό και την αναδιοργάνωση των υποκείμενων διαδικασιών και τη χρήση της τεχνολογίας για την «ψηφιοποίηση» αυτών, προωθείται και η ανασύνταξη του κρατικού μηχανισμού. Οι λειτουργίες που πρέπει να επιτελέσει μία κυβέρνηση είναι πολλές: προάσπιση των πολιτικών δικαιωμάτων και της δημοκρατίας, διατήρηση της τάξης, τήρηση των νόμων, παροχή υπηρεσιών στους πολίτες, διαχείριση των φορέων που την συνιστούν κ.ο.κ. Βάσει αυτών μπορούν να οριστούν και οι βασικές κατευθύνσεις της ηλεκτρονικής διακυβέρνησης, όσον αφορά τις περιοχές εφαρμογής της, οι οποίες είναι οι εξής [79]:

- Ηλεκτρονική διοίκηση (e-Administration), η οποία συνίσταται στη χρήση ΤΠΕ για την υλοποίηση διοικητικών και λειτουργικών διαδικασιών που αφορούν είτε απλές υπηρεσίες γραφείου είτε λειτουργίες όπως οργάνωση, σχεδιασμό και έλεγχο λειτουργίας οργανισμών [80].
- Ηλεκτρονική διαχείριση (e-Management), μία έννοια παρόμοια με αυτήν της ηλεκτρονικής διοίκησης, η οποία αφορά τη χρήση ΤΠΕ για τη βελτίωση του τρόπου διαχείρισης της κυβέρνησης, περιλαμβάνοντας στρατηγικές όπως η αναδιάρθρωση επιχειρηματικών διαδικασιών για τη διατήρηση ηλεκτρονικών αρχείων και η βελτίωση της ροής και της ενσωμάτωσης πληροφορίας [81].
- Ηλεκτρονικές υπηρεσίες (e-Services), οι οποίες αποτελούν την ηλεκτρονική μορφή των συμβατικών παρεχόμενων υπηρεσιών σε πολίτες και άλλους ενδιαφερόμενους φορείς από τους οργανισμούς δημοσίου τομέα, χρησιμοποιώντας ΤΠΕ [82].
- Ηλεκτρονική δημοκρατία (e-Democracy), η οποία περιλαμβάνει τους όρους ηλεκτρονική πληροφορία (e-Information), ηλεκτρονική συμμετοχή (e-Participation) και ηλεκτρονική λήψη απόφασης (e-Decision Making), και συνίσταται στη χρήση ΤΠΕ για την επίτευξη διαφανούς συμμετοχής του πολίτη σε πολιτικά δρώμενα και δημοκρατικής λήψης αποφάσεων σε κυβερνητικές διαδικασίες και πρακτικές (π.χ. ηλεκτρονική αίτηση (e-Petition), ηλεκτρονική διαβούλευση (e-Consultation) και ηλεκτρονική ψηφοφορία (e-Voting)) [83][84].
- Ηλεκτρονική ένταξη (e-Inclusion), μία έννοια που προωθεί την συμμετοχή του πολίτη στην Κοινωνία της Πληροφορίας, ανεξαρτήτως κοινωνικών και οικονομικών δυνατοτήτων, καθώς και μορφωτικού του επιπέδου με απώτερο σκοπό

την καταπολέμηση του κοινωνικού αποκλεισμού [85].

- Ηλεκτρονική προσβασιμότητα (e-Accessibility), η οποία αφορά την εξασφάλιση πρόσβασης όλων των πολιτών στις υπηρεσίες της ηλεκτρονικής διακυβέρνησης με την άρση τεχνικών, οικονομικών ή νομικών εμποδίων με τα οποία μπορεί να έρθουν αντιμέτωποι πολίτες όταν χρησιμοποιούν τις παρεχόμενες ηλεκτρονικές υπηρεσίες [86].
- Ηλεκτρονική ασφάλεια (e-Security), η οποία αφορά την προστασία της ιδιωτικότητας των πολιτών και την ενίσχυση της εμπιστοσύνης του κοινού στα ψηφιακά μέσα και υπηρεσίες, της ακεραιότητας των δεδομένων και των συστημάτων που εκτελούν τις λειτουργίες ηλεκτρονικής διακυβέρνησης καθώς και τη διαθεσιμότητα των προαναφερθέντων στους εμπλεκόμενους φορείς για την επίτευξη ασφάλειας, εγκυρότητας και νομιμότητας των ψηφιακών συναλλαγών.
- Ηλεκτρονικό εμπόριο (e-Commerce), το οποίο αφορά την επιχειρηματική πλευρά κυβερνητικής αλληλεπίδρασης (π.χ. ανταλλαγή χρημάτων για την προμήθεια κυβερνητικών αγαθών και υπηρεσιών γνωστό και ως ηλεκτρονική προμήθεια (e-Procurement), ηλεκτρονική δημοπρασία (e-Auction) κ.ο.κ.) [87].

4.2.2 Μοντέλα Ηλεκτρονικής Διακυβέρνησης

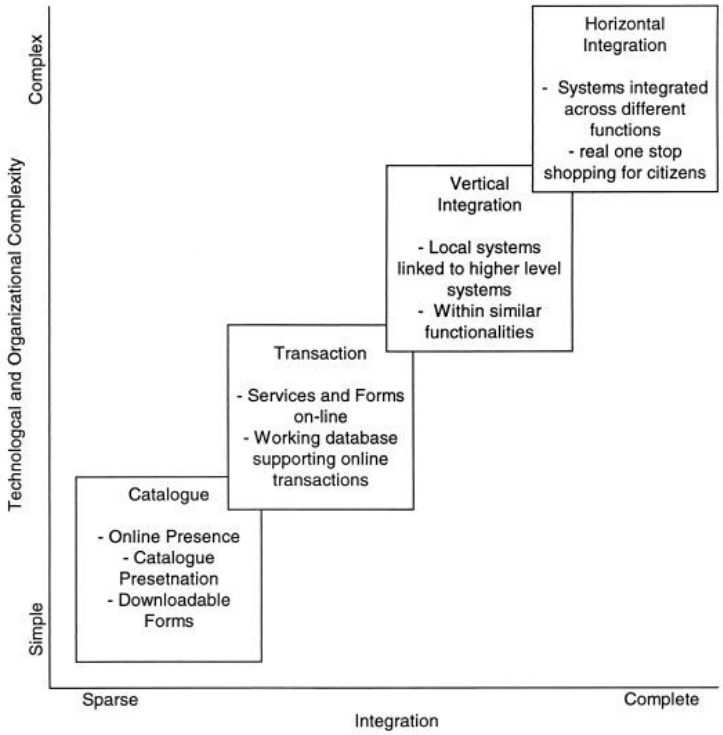
Ανάλογα με τον δέκτη της παρεχόμενης υπηρεσίας ηλεκτρονικής διακυβέρνησης, έχουν προταθεί στη βιβλιογραφία διάφορα μοντέλα σχέσεων, με επικρατέστερα και ευρέως αποδεκτά τα εξής τρία [88][89]:

- Κυβέρνηση-προς-Κυβέρνηση (Government-to-Government – G2G): Διαμοιρασμός πληροφορίας ανάμεσα σε ενδοκυβερνητικούς φορείς σε τοπικό, εθνικό και διεθνές επίπεδο, με απώτερο σκοπό τον συντονισμό και τη συνεργασία αυτών για τη μείωση κόστους συναλλαγών, την καλύτερη λήψη αποφάσεων, την αύξηση παραγωγικότητας της δημόσιας διοίκησης αλλά και την επίτευξη μέγιστης δυνατής ακρίβειας και αποτελεσματικότητας στις υποκείμενες ενδοκυβερνητικές διαδικασίες (π.χ. εθνικό δημοτολόγιο με συνεργασία μεταξύ Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ), Αστυνομίας, Στρατολογίας, Ασφαλιστικών Ταμείων, Υπουργείου Δικαιοσύνης κ.α.).
- Κυβέρνηση-προς-Επιχειρήσεις (Government-to-Business – G2B): Παροχή υπηρεσιών προς τις επιχειρήσεις και τη βιομηχανία για τη διεκπεραίωση των επιχειρηματικών τους συναλλαγών και υποχρεώσεων, καθώς επίσης και την αρμονική και αποτελεσματική συνεργασία δημόσιου και ιδιωτικού τομέα με ταυτόχρονη μείωση της απαιτούμενης γραφειοκρατίας (π.χ. υποβολή δηλώσεων ΦΠΑ, σύσταση νέας εταιρείας, ηλεκτρονική διεξαγωγή δημόσιων προμηθειών κ.α.).
- Κυβέρνηση-προς-Πολίτες (Government-to-Citizens – G2C): Αφορά την παροχή εξατομικευμένων υπηρεσιών προς τους πολίτες για τη βέλτιστη εξυπηρέτησή

τους με διαφανείς, αμερόληπτες και αξιόπιστες διαδικασίες, την εξοικονόμηση χρόνου και την καταπολέμηση της γραφειοκρατίας (π.χ. αίτηση χορήγησης φορολογικής ενημερότητας, υποβολή δηλώσεων φορολογίας εισοδήματος, έκδοση και ανανέωση άδειας οδήγησης, εγγραφή μέλους στην ανώτερη και ανώτατη εκπαίδευση κ.α.).

4.2.3 Ανάπτυξη Ηλεκτρονικής Διακυβέρνησης

Έχει παρατηρηθεί ότι η ηλεκτρονική διακυβέρνηση αναπτύσσεται σε στάδια και κάθε στάδιο χαρακτηρίζεται από διαφορετικά επίπεδα λειτουργικότητας παρεχόμενης υπηρεσίας, χρήσης τεχνολογιών, διοικητικών αλλαγών και προσανατολισμού πολιτών [90]. Στη βιβλιογραφία [91][92] υπάρχουν πολλά μοντέλα ανάπτυξης που έχουν οριστεί και προταθεί, με πιο γνωστό εκείνο των Layne & Lee, το οποίο, όπως προαναφέρθηκε, περιλαμβάνει τα εξής τέσσερα στάδια (Σχήμα 5): παρουσίαση και πληροφόρηση (Catalogue), συναλλαγή (Transaction), κάθετη ολοκλήρωση (Vertical Integration) και, τέλος, οριζόντια ολοκλήρωση (Horizontal Integration).



Σχήμα 5: Στάδια Ανάπτυξης Ηλεκτρονικής Διακυβέρνησης των Layne & Lee

Συνδυάζοντας τα κυριότερα μοντέλα ([93][94]), προκύπτει εκείνο των εξής επτά επιπέδων:

- Αρχική παρουσία (initial presence): Παροχή έγκυρης και ενημερωμένης πληροφόρησης σχετικά με κυβερνητικές γραφειοκρατικές υπηρεσίες μέσω διαδικτυα-

κής πύλης (e-Government Portal).

- Εκτεταμένη παρουσία (extended presence): Ανταλλαγή πληροφορίας και επικοινωνία μεταξύ δημοσίων υπηρεσιών και πολιτών/επιχειρήσεων σε πρώιμο στάδιο, με τη χρήση ηλεκτρονικού ταχυδρομείου ή μηχανών αναζήτησης.
- Διαδραστική παρουσία (interactive presence): Αυξημένη αλληλεπίδραση μεταξύ κρατικών φορέων και πολιτών και παροχή ποικίλων διαδικτυακών πυλών διαφορετικών φορέων.
- Συναλλακτική παρουσία (transaction presence): Παροχή υπηρεσιών, όπως ασφαλή πληρωμή φόρων και προστίμων, λήψη αδειών, κλπ., με τη χρήση τεχνολογιών που επιτρέπουν την ασύγχρονη και σύγχρονη επικοινωνία κυβερνητικών διαδικτυακών πυλών με υποστηρικτικά συστήματα φορέων.
- Κάθετη ολοκλήρωση (vertical integration): Παροχή συνδυασμένων υπηρεσιών που προκύπτουν από την αλληλεπίδραση διαφόρων τμημάτων δημοσίων φορέων με τον συντονισμό τους, την αναδιοργάνωση και τον επανασχεδιασμό ενδοκυβερνητικών διαδικασιών.
- Οριζόντια ολοκλήρωση (horizontal integration): Ενοποίηση όλων των παρεχόμενων υπηρεσιών φορέων του δημόσιου τομέα και πλήρης αξιοποίηση των ΤΠΕ για τη θεώρηση της κυβέρνησης και του συνόλου των υπηρεσιών της ως ολοκληρωμένη οντότητα.
- Ολική ολοκλήρωση (total integration): Οριζόντια και κάθετη ολοκλήρωση της ηλεκτρονικής διακυβέρνησης με παροχή υπηρεσιών μέσω ενός και μόνο σημείου πρόσβασης και εξυπηρέτησης (one-stop shop service) των πολιτών και επιχειρήσεων, με πιθανές απαιτούμενες διοικητικές και θεσμικές μεταρρυθμίσεις.

4.2.4 Πλαίσια Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης

4.2.4.1 Εθνικό Πλαίσιο Ηλεκτρονικής Διακυβέρνησης

Για την παροχή υπηρεσιών των τριών τελευταίων επιπέδων που αναφέρθηκαν στην προηγούμενη ενότητα, απαιτείται αλληλεπίδραση και ασφαλής ανταλλαγή ή ακόμα και επαναχρησιμοποίηση δεδομένων μεταξύ διαφόρων δημοσίων φορέων και οργανισμών ακόμα και διαφορετικών κρατών, οπότε και κρίνεται απαραίτητη η διαλειτουργικότητα όλων των εμπλεκόμενων πληροφοριακών συστημάτων των φορέων που αναλαμβάνουν τη διεκπεραίωση αιτήσεων των πολιτών. Για τον λόγο αυτό, κάθε χώρα οφείλει να ορίζει πολιτικές και τεχνολογικά και επιχειρησιακά πρότυπα, το σύνολο των οποίων αναφέρεται και ως Εθνικό ή Κυβερνητικό Πλαίσιο Διαλειτουργικότητας (National/Government Interoperability Framework – NIF/GIF). Σύμφωνα με το τελευταίο, θα παρέχονται συνδυασμένες υπηρεσίες δημόσιας διοίκησης στους συναλλασσόμενους φορείς, επιχειρήσεις και πολίτες, οι οποίοι θα πρέπει με τη σειρά τους να υιοθετούν το πλαίσιο αυτό και να το εφαρμόζουν. Τα εθνικά πλαί-

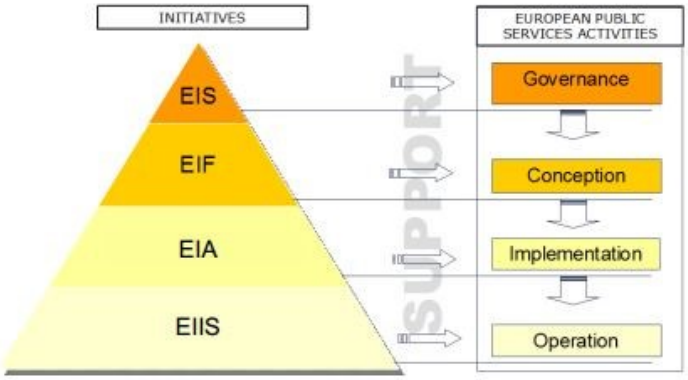
σια διαλειτουργικότητας αναπροσαρμόζονται ανά τακτά χρονικά διαστήματα ανάλογα με τις τεχνολογικές εξελίξεις και τις όποιες διοικητικές αλλαγές απαιτούνται. Στην Ελλάδα, τα προαναφερθέντα πρότυπα ορίζονται στο "Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας" ή αλλιώς "Πλαίσιο Ηλεκτρονικής Διακυβέρνησης" (ΠΗΔ) [95]. Το ΠΗΔ συντάχθηκε στο πλαίσιο έργου για την αποτελεσματική υποστήριξη της ηλεκτρονικής διακυβέρνησης σε κεντρικό, περιφερειακό και τοπικό επίπεδο το 2006, χρηματοδοτήθηκε από το Επιχειρησιακό Πρόγραμμα για την Κοινωνία της Πληροφορίας και επικυρώθηκε τον Δεκέμβριο του 2008. Το ΠΗΔ είναι σύμφωνο με το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας και περιλαμβάνει τα εξής επιμέρους πλαίσια:

- Πλαίσιο Πιστοποίησης Δημόσιων Διαδικτυακών Τόπων (ΠΠΔΔΤ) για τον καθορισμό των σχεδιαστικών κατευθύνσεων και του περιεχομένου των διαδικτυακών πυλών των δημόσιων φορέων.
- Πλαίσιο Διαλειτουργικότητας και Υπηρεσιών Ηλεκτρονικών Συναλλαγών (ΠΔ & ΥΗΣ) για τον καθορισμό των τεχνολογικών προτύπων, βάσει των οποίων πρέπει να αναπτύσσονται τα πληροφοριακά συστήματα, και των γενικών αρχών που θα πρέπει να υιοθετούνται από φορείς της δημόσιας διοίκησης, προκειμένου να επιτευχθεί η ανταλλαγή δεδομένων μεταξύ αυτών και η παροχή ολοκληρωμένων υπηρεσιών προς τους πολίτες.
- Πλαίσιο Ψηφιακής Αυθεντικοποίησης (ΠΨΑ) για τον καθορισμό διαδικασιών και τεχνολογιών που απαιτούνται για την εγγραφή, ταυτοποίηση και αυθεντικοποίηση των χρηστών, καθώς και τη δημιουργία πολιτικών σχετικά με τα ψηφιακά πιστοποιητικά και τις υποδομές δημόσιου κλειδιού. Επίσης, το ΠΗΔ περιλαμβάνει ένα "Μοντέλο Τεκμηρίωσης" για την περιγραφή της σημειογραφίας, των κανόνων και των προδιαγραφών ανάπτυξης μοντέλων διαδικασιών και δεδομένων–μεταδεδομένων, καθώς και το "Μητρώο Διαλειτουργικότητας" ως αποθετήριο μεταδεδομένων υπηρεσιών και εγγράφων, διαγραμμάτων υπηρεσιών, σχημάτων XML για τα δημόσια έγγραφα καθώς και καταλόγων κωδικών για πληροφοριακά στοιχεία των διαδικασιών G2G.

4.2.4.2 Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας

Τον Ιούνιο του 2002 στη σύνοδο κορυφής της Σεβίλλης, η Ευρωπαϊκή Επιτροπή, στο πλαίσιο του σχεδίου δράσης "eEurope Action Plan 2005", όρισε ένα πλαίσιο διαλειτουργικότητας για την υποστήριξη παροχής πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης προς τους πολίτες και τις επιχειρήσεις των κρατών-μελών της Ευρωπαϊκής Ένωσης. Το πλαίσιο αυτό είναι γνωστό ως Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Interoperability Framework – EIF) και αναπτύχθηκε στο πλαίσιο προγράμματος Διαλειτουργικής Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στις Δημόσιες Διοικήσεις, τις Επιχειρήσεις και τους Πολίτες (Interoperable Delivery

of European eGovernment Services to public Administrations, Businesses and Citizens – IDABC), το οποίο διαδέχθηκε το 2010 το πρόγραμμα Λύσεων Διαλειτουργικότητας για Ευρωπαϊκές Δημόσιες Διοικήσεις (Interoperability solutions for European public administrations – ISA). Τα κράτη-μέλη της Ευρωπαϊκής Ένωσης σε συνεργασία με την Ευρωπαϊκή Επιτροπή οφείλουν να ανανεώνουν το EIF ανάλογα με τις τεχνολογικές εξελίξεις και τις όποιες αναγκαίες διοικητικές αλλαγές. Βάσει του EIF, τα πληροφοριακά συστήματα των φορέων δημόσιας διοίκησης θα πρέπει να σχεδιάζονται και να υλοποιούνται με τέτοιο τρόπο έτσι ώστε να τηρούνται οι εξής βασικές αρχές: διαφάνεια και εξωστρέφεια, επαναχρησιμοποίηση στοιχείων (reusability), προσαρμοστικότητα (flexibility), χρήση ευρέως διαδεδομένων προτύπων (standards), κλιμάκωση (scalability), απόδοση (performance) και απόκριση (response), φιλικότητα προς το χρήστη (user-friendliness), διαθεσιμότητα (availability), ανοχή σφαλμάτων (fault tolerance), συντήρηση (maintenance) και αναβάθμιση (updating), καθώς επίσης και ασφάλεια (security) των δεδομένων.



Σχήμα 6: Πρωτοβουλίες Διαλειτουργικότητας από την Ευρωπαϊκή Επιτροπή

Το Σχήμα 6 αναπαριστά τις πρωτοβουλίες διαλειτουργικότητας της Ευρωπαϊκής Επιτροπής καθώς και τους τομείς που αυτές αφορούν. Όπως βλέπουμε, εκτός από το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας που αφορά τον σχεδιασμό των ευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης, ορίζονται παράλληλα η Ευρωπαϊκή Στρατηγική Διαλειτουργικότητας (European Interoperability Strategy – EIS) για τις απαιτούμενες διοικητικές δραστηριότητες προς την επίτευξη διαλειτουργικότητας μεταξύ συστημάτων των κρατών, η Ευρωπαϊκή Αρχιτεκτονική Διαλειτουργικότητας (European Interoperability Architecture – EIA) για την περιγραφή της πρακτικής εφαρμογής του EIF και οι Ευρωπαϊκές Υπηρεσίες Υποδομής Διαλειτουργικότητας (European Interoperability Infrastructure Services – EIIS) για την υποστήριξη των λειτουργιών των ευρωπαϊκών δημόσιων υπηρεσιών.

Τα εκάστοτε Εθνικά Πλαίσια Διαλειτουργικότητας (National Interoperability Frameworks – NIFs) των κρατών μελών της Ευρωπαϊκής Ένωσης θα πρέπει να συμμορφώνονται και να συμφωνούν με το EIF. Το τελευταίο ορίζει τους εξής τέσσερις

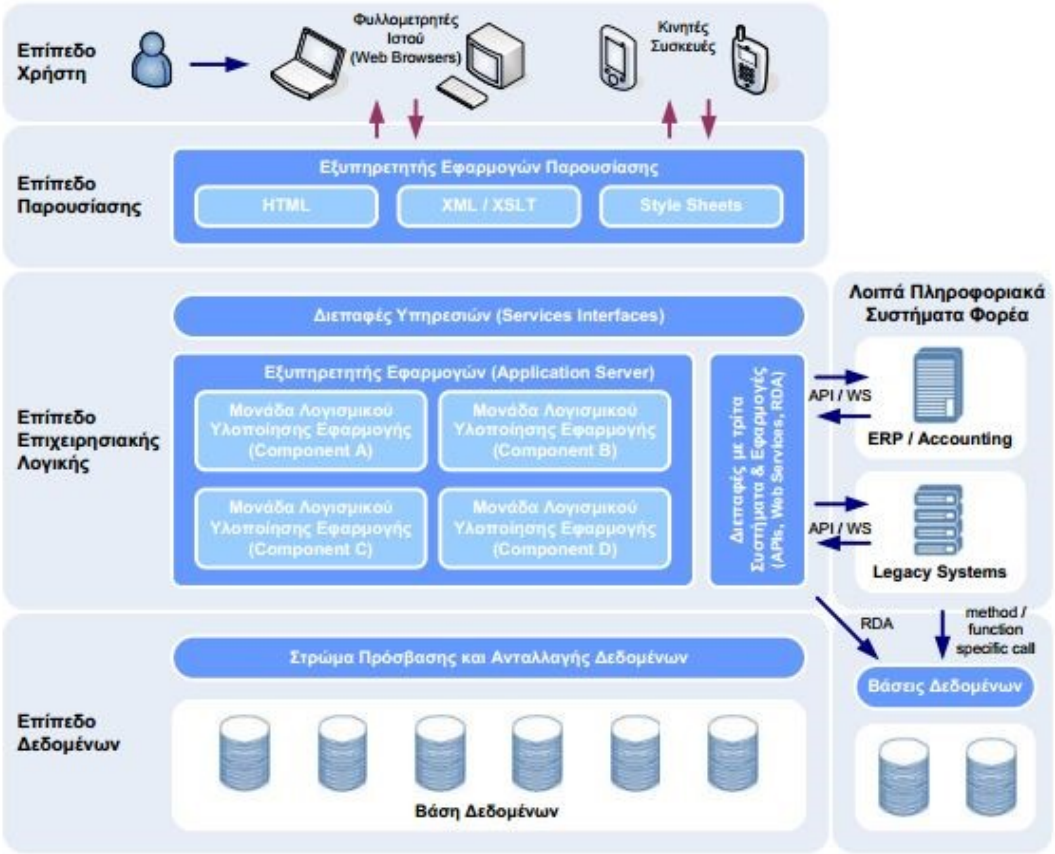
τύπους διαλειτουργικότητας:

- Νομική Διαλειτουργικότητα (Legal Interoperability), η οποία εξασφαλίζεται με την προσεκτική αναθεώρηση από τις δημόσιες διοικήσεις όλων των κρατών–μελών της Ευρωπαϊκής Ένωσης της νομοθεσίας σχετικής με την ανταλλαγή δεδομένων και προστασία αυτών, δεδομένου ότι κάθε χώρα έχει το δικό της νομικό πλαίσιο σύμφωνα με το οποίο παρέχονται οι όποιες δημόσιες υπηρεσίες και για το λόγο αυτό ασυμβατότητες μεταξύ νομοθεσιών διαφορετικών χωρών είναι ιδιαίτερα συνήθεις και δυσχεραίνουν την συνεργασία τους. Το συγκεκριμένο ζήτημα θα λυθεί σε μεγάλο βαθμό με την εφαρμογή του πρόσφατα ψηφισθέντα από την Ευρωπαϊκή Επιτροπή Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).
- Οργανωτική Διαλειτουργικότητα (Organisational Interoperability), η οποία επιτυγχάνεται με την προσυμφωνημένη και ορισμένη νομοθετικά μοντελοποίηση και διαγραμματική απεικόνιση επιχειρησιακών διαδικασιών, τον ορισμό των επιχειρησιακών στόχων, τη συνεργασία των διαφορετικών φορέων και την προσιτή και προσανατολισμένη προς τον χρήστη παροχή υπηρεσιών.
- Σημασιολογική Διαλειτουργικότητα (Semantic Interoperability), η οποία εξασφαλίζει την κοινή ερμηνεία των δεδομένων που ανταλλάσσονται μεταξύ υπηρεσιών διαφορετικών φορέων σύμφωνα με ένα κοινό μοντέλο αναφοράς (π.χ. ορισμός πρότυπων σχημάτων ηλεκτρονικών εγγράφων, οντολογιών, μεταδεδομένων, κωδικολογίων κ.ο.κ.).
- Τεχνική Διαλειτουργικότητα (Technical Interoperability), η οποία αφορά τη διαλειτουργικότητα του λογισμικού και των υποδομών και συνίσταται στη χρήση συμφωνημένων προτύπων για την αναπαράσταση, επεξεργασία και αποθήκευση της πληροφορίας.

Τέλος, στο πλαίσιο του προγράμματος ISA, για την επίτευξη των τελικών στόχων αυτού, ορίστηκαν οι εξής βασικές δράσεις: (α) αξιόπιστη ανταλλαγή πληροφορίας με βελτίωση της σημασιολογικής διαλειτουργικότητας των ευρωπαϊκών συστημάτων ηλεκτρονικής διακυβέρνησης· (β) βελτίωση της διασυνοριακής πρόσβασης σε κυβερνητικά δεδομένα· (γ) πρόσβαση σε πηγές πληροφόρησης των κρατών μελών της Ευρωπαϊκής Ένωσης· (δ) πανευρωπαϊκή διαλειτουργικότητα των ηλεκτρονικών ταυτοτήτων· (ε) ανάπτυξη πανευρωπαϊκής εφαρμογής ηλεκτρονικών προμηθειών· (στ) επίτευξη εκτέλεσης ασφαλών ροών εργασίας μεταξύ Ευρωπαϊκής Ένωσης και εθνικών οργανισμών· (ζ) χρήση εργαλείων ηλεκτρονικής υπογραφής για την υποστήριξη διασυνοριακής πρόσβασης σε υπηρεσίες από επιχειρήσεις· (η) δημιουργία ευέλικτης πλατφόρμας διοικητικής συνεργασίας· (θ) διαχείριση της ανταλλαγής δεδομένων· (ι) επαναχρησιμοποίηση εργαλείων για τη συλλογή πληροφοριών· (ια) επαναχρησιμοποίηση δεδομένων· (ιβ) ασφαλή ψηφιακή επικοινωνία μέσω των δικτύων· (ιγ) επίτευξη διασυνοριακής διαλειτουργικότητας στον τομέα της υγείας.

4.2.5 Αρχιτεκτονική Συστήματος Ηλεκτρονικής Διακυβέρνησης

Για την επίτευξη των τεσσάρων μορφών διαλειτουργικότητας που αναφέρθηκαν παραπάνω και την ολική ολοκλήρωση των υπηρεσιών ηλεκτρονικής διακυβέρνησης, η αρχιτεκτονική των πληροφοριακών συστημάτων των φορέων δημόσιας διοίκησης παίζει ιδιαίτερο ρόλο. Κατευθυντήριες γραμμές για την αρχιτεκτονική που θα πρέπει να ακολουθείται κατά την ανάπτυξη των σχετικών πληροφοριακών συστημάτων όλων των Ευρωπαϊκών χωρών ορίζονται στην Ευρωπαϊκή Αρχιτεκτονική Διαλειτουργικότητας που αναφέρθηκε και στην προηγούμενη ενότητα, η οποία ανανεώνεται και αναπροσαρμόζεται συχνά, ανάλογα με τις τεχνολογικές εξελίξεις και τις απαιτήσεις των κυβερνήσεων. Οι αρχιτεκτονικές και οι τεχνολογίες που έχουν χρησιμοποιηθεί ευρέως για το σχεδιασμό και την ανάπτυξη των διαδικτυακών εφαρμογών των φορέων δημόσιας διοίκησης είναι οι εξής: (α) Πολυ-επίπεδες Αρχιτεκτονικές (Multi-layer Architecture), (β) Ανάπτυξη Βασισμένη σε Αυτόνομες Δομικές Μονάδες (Component-based Development), (γ) Υπηρεσιοστρεφής Αρχιτεκτονική (Service-oriented Architecture – SOA) και (δ) Τεχνολογίες Υπηρεσιών Ιστού (Web Service – WS).



Σχήμα 7: Πρότυπη Τεχνική Αρχιτεκτονική Συστημάτων Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

Στηριζόμενοι στις παραπάνω αρχιτεκτονικές και τεχνολογίες, σε κάθε Εθνικό

Πλαίσιο Διαλειτουργικότητας προτείνεται και ορίζεται ένα πρότυπο αρχιτεκτονικής εφαρμογών ηλεκτρονικής διακυβέρνησης καθώς και λειτουργικότητας συνεργατικών εφαρμογών για το σχεδιασμό και την ανάπτυξη αυτών καθώς και των κυβερνητικών διαδικτυακών πυλών φορέων και οργανισμών του δημόσιου τομέα, τόσο σε επίπεδο ενδο-οργανικό όσο και σε επίπεδο συνεργασίας δύο ή και περισσοτέρων πληροφοριακών συστημάτων για την παροχή συνδυασμένης ηλεκτρονικής υπηρεσίας. Στο Σχήμα 7 αναπαρίσταται η αρχιτεκτονική όπως αυτή προτείνεται από το ελληνικό Πλαίσιο Ηλεκτρονικής Διακυβέρνησης.

4.2.6 Απαιτήσεις Συστημάτων Ηλεκτρονικής Διακυβέρνησης

4.2.6.1 Λειτουργικές και Μη Λειτουργικές Απαιτήσεις

Οι Διαδικτυακοί Τόποι των φορέων της Δημόσιας Διοίκησης (Δημόσιοι Διαδικτυακοί Τόποι - ΔΔΤ) αποτελούν την πύλη εισόδου πολιτών, επιχειρήσεων και άλλων φορέων στις υπηρεσίες που παρέχουν οι φορείς και ακολουθούν τις κάτωθι θεμελιώδεις αρχές [82]:

- Αρχή της ισότητας και της ισονομίας: Οι φορείς της Δημόσιας Διοίκησης δεν θέτουν περιορισμούς στην πρόσβαση στις πληροφορίες και στις υπηρεσίες που παρέχουν μέσω των διαδικτυακών τους τόπων εξασφαλίζοντας ιδίως: (α) τεχνολογική ανεξαρτησία στην πρόσβαση της πληροφορίας, (β) κάλυψη αναγκών ειδικών ομάδων πληθυσμού όπως άτομα με αναπηρία, (γ) προστασία των ανθρωπίνων δικαιωμάτων.
- Αρχή της πληρότητας και της αξιοπιστίας: Το περιεχόμενο των πληροφοριών και των υπηρεσιών που παρέχει ένας φορέας της δημόσιας διοίκησης μέσω του διαδικτυακού του τόπου πρέπει να είναι ορθό, πλήρες, και επίκαιρο.
- Αρχή της εμπιστοσύνης: Ο διαδικτυακός τόπος ενός φορέα της δημόσιας διοίκησης πρέπει να συμβάλει στη δημιουργία σχέσης εμπιστοσύνης με τους επισκέπτες του ιστότοπου και τους χρήστες των ηλεκτρονικών υπηρεσιών του φορέα εφαρμόζοντας κατάλληλους μηχανισμούς ασφάλειας και προστασίας προσωπικών δεδομένων.
- Αρχή της σωστής διαχείρισης των δημόσιων πόρων: Η επένδυση που απαιτείται για την ανάπτυξη και την υποστήριξη της λειτουργίας ενός δημόσιου διαδικτυακού τόπου πρέπει να δικαιολογείται από το όφελος που αναμένεται να προκύψει από τη χρήση των ηλεκτρονικών υπηρεσιών του Δημόσιου Διαδικτυακού Τόπου αλλά και την επαναχρησιμοποίηση των πληροφοριών και των υπηρεσιών του.
- Αρχή της ανοιχτής διάθεσης και περαιτέρω χρήσης της δημόσιας πληροφορίας: Το σύνολο της δημόσιας πληροφορίας που διατίθεται από το διαδικτυακό τόπο ενός φορέα της δημόσιας διοίκησης θα πρέπει: (α) να είναι διαθέσιμο χωρίς τε-

χνικούς, νομικούς ή οργανωτικούς περιορισμούς, (β) να είναι μηχαναγνώσιμο, (γ) να συνοδεύεται από τα κατάλληλα μεταδεδομένα, (δ) να είναι εύκολα ευρέσιμο και (ε) να συνοδεύεται από τυποποιημένες ανοιχτές κυβερνητικές άδειες που προσδιορίζουν τους όρους χρήσης.

Με βάση τα παραπάνω, ακολουθούν τρεις πίνακες που περιλαμβάνουν όλες τις απαιτήσεις ενός συστήματος παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, ανά κατηγορία:

Πίνακας 1: Γενικές Λειτουργικές Απαιτήσεις Συστημάτων Ηλεκτρονικής Διακυβέρνησης

Γενικές Λειτουργικές Απαιτήσεις	
Κωδικός	**Ονομασία**
ΛΑ–01	Εξουσιοδότηση (Authorisation)
ΛΑ–02	Έλεγχος ταυτότητας (Identification – Authentication)

Πίνακας 2: Γενικές Μη Λειτουργικές Απαιτήσεις Συστημάτων Ηλεκτρονικής Διακυβέρνησης

Γενικές Μη Λειτουργικές Απαιτήσεις	
Κωδικός	**Ονομασία**
ΜΛΑ–01	Απαιτήσεις ασφάλειας
ΜΛΑ–01.1	Ακεραιότητα (Integrity)
ΜΛΑ–01.2	Εμπιστευτικότητα (Confidentiality)
ΜΛΑ–01.3	Διαθεσιμότητα (Availability)
ΜΛΑ–01.4	Εμπιστοσύνη (Trust)
ΜΛΑ–01.5	Μη-Αποποίηση Ευθύνης (Non-repudiation)
ΜΛΑ–01.6	Προστασία των δεδομένων (Data protection)
ΜΛΑ–01.7	Αυθεντικότητα (Authenticity)
ΜΛΑ–02	Αποδοτικότητα – Χρόνος απόκρισης (Efficiency – Response Time)
ΜΛΑ–03	Αξιοπιστία Συστήματος (System Reliability)
ΜΛΑ–04	Διαθεσιμότητα υπηρεσιών (Service Availability)
ΜΛΑ–05	Δυναμική επεκτασιμότητα (Scalability)
ΜΛΑ–06	Διαλειτουργικότητα (Interoperability)
ΜΛΑ–07	Ευελιξία (Flexibility)
ΜΛΑ–08	Επαναχρησιμοποίηση της υποδομής (Infrastructure Reusability)
ΜΛΑ–09	Ανοχή σφαλμάτων (Fault Tolerance)
ΜΛΑ–10	Χρηστικότητα (Usability)
ΜΛΑ–10.1	Φιλικότητα προς το χρήστη – Ευκολία (User Friendliness)
ΜΛΑ–10.2	Εξοικονόμηση Κόστους – Χρόνου (Cost-Time Efficiency)

Πίνακας 3: Νομικές και Κανονιστικές Απαιτήσεις Συστημάτων Ηλεκτρονικής Διακυβέρνησης

Νομικές και Κανονιστικές Απαιτήσεις	
Κωδικός	**Ονομασία**
ΝΑ–01	Νομιμότητα της συλλογής και επεξεργασίας των δεδομένων
ΝΑ–02	Σκοπιμότητα της επεξεργασίας των δεδομένων
ΝΑ–03	Αναγκαιότητα των δεδομένων υπό επεξεργασία
ΝΑ–04	Ποιότητα των δεδομένων υπό επεξεργασία
ΝΑ–05	Ταυτοποίηση υποκειμένου των δεδομένων
ΝΑ–06	Ειδικές κατηγορίες δεδομένων – ευαίσθητα δεδομένα
ΝΑ–07	Πληροφόρηση, συγκατάθεση και λοιπά δικαιώματα των υποκειμένων των δεδομένων
ΝΑ–08	Ειδοποιήσεις και λοιπές αρμοδιότητες/εξουσιοδοτήσεις των αρμοδίων Αρχών
ΝΑ–09	Μη συνδεσιμότητα δεδομένων
ΝΑ–10	Χρήση μοναδικού ταυτοποιητικού αναγνωριστικού
ΝΑ–11	Ασφαλής αποθήκευση
ΝΑ–12	Ασφαλής μεταφορά και διάδοση δεδομένων

4.2.6.2 Τεχνικές Απαιτήσεις

Σύμφωνα με όσα έχουν αναφερθεί παραπάνω, μία Διαδικτυακή Πύλη που βασίζεται στην Υπηρεσιοστρεφή Αρχιτεκτονική θα πρέπει να καλύπτει τις παρακάτω τεχνικές απαιτήσεις:

- Σημασιολογική αναπαράσταση πληροφοριών και υπηρεσιών: απαιτείται η φορμαλιστική, σημασιολογική μοντελοποίηση κάθε προσωπικής πληροφορίας, της φύσης κάθε υπηρεσίας ή διεργασίας ηλεκτρονικής διακυβέρνησης, καθώς και του ρόλου της εκάστοτε εμπλεκόμενης οντότητας.
- Σύνθεση ροών εργασίας: σχεδόν όλες οι δημόσιες υπηρεσίες απαιτούν τη διαλειτουργικότητα περισσότερων από μία υπηρεσιών ηλεκτρονικής διακυβέρνησης. Ως εκ τούτου, η πλατφόρμα θα πρέπει να υποστηρίζει τη σύνθεση και εκτέλεση ροών εργασίας για κάθε περίπτωση. Έτσι, το συνολικό σύστημα θα μπορεί να εντοπίσει όλες τις σχετικές υπηρεσίες και να τις συνδυάσει σε μια συγκεκριμένη σειρά προκειμένου να εξυπηρετηθεί το αντίστοιχο αίτημα πολιτών.
- Έλεγχος πρόσβασης: πέρα από τα χαρακτηριστικά των καθιερωμένων μοντέλων ελέγχου πρόσβασης, οι μηχανισμοί που στοχεύουν στην προστασία της ιδιωτικότητας πρέπει να λαμβάνουν υπόψη επιπλέον παραμέτρους: (α) την ελαχιστοποίηση των πληροφοριών που συλλέγονται, υφίστανται επεξεργασία και μεταδίδονται μεταξύ διαφορετικών οργανισμών, (β) τον αλυσιδωτό τρόπο πα-

ροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης, και (γ) την πολυεπίπεδη φύση των δεδομένων. Το μοντέλο ελέγχου πρόσβασης πρέπει να υιοθετεί την τυπική σημασιολογία και οντολογική θεμελίωση κανόνων πρόσβασης και δεδομένων, να ικανοποιεί τις απαιτήσεις της νομοθεσίας για την προστασία προσωπικών δεδομένων και να λαμβάνει υπόψη παραμέτρους χωρικές, χρονικές και ιστορικές.

- Διαχείριση ταυτοτήτων: απαιτείται η εφαρμογή των κατάλληλων μηχανισμών διαχείρισης των προσωπικών πληροφοριών των χρηστών, ούτως ώστε η συνδεσιμότητα των δεδομένων να λαμβάνει χώρα μόνο εφόσον αυτό είναι αναγκαίο για τους σκοπούς παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης.
- Υποχρεώσεις ιδιωτικότητας: η συλλογή, επεξεργασία ή αποκάλυψη προσωπικών δεδομένων των πολιτών πρέπει να συνοδεύεται από την εκτέλεση συμπληρωματικών ενεργειών, που χαρακτηρίζονται από τον όρο «υποχρεώσεις ιδιωτικότητας».
- Ενεργός ρόλος πολιτών: οι πολίτες θα πρέπει να έχουν ενεργό ρόλο όσον αφορά στην προστασία των προσωπικών τους δεδομένων. Μεταξύ των σχετικών δικαιωμάτων που πρέπει να τους παρέχονται περιλαμβάνονται η ρητή πληροφόρηση σχετικά με τη συλλογή, αποκάλυψη και επεξεργασία των δεδομένων τους, η δυνατότητα παροχής και άρσης της ρητής συγκατάθεσής τους, η δυνατότητα προδιαγραφής προτιμήσεων ιδιωτικότητας και η δυνατότητα πρόσβασης στα δεδομένα.
- Διαλειτουργικότητα συστημάτων σε ετερογενή περιβάλλοντα: οι υποκείμενες διαδικασίες και τα επιμέρους συστήματα πρέπει να είναι σε θέση να διαλειτουργούν με ομότιμα συστήματα και υπηρεσίες, καθώς και να ελέγχουν τη διακίνηση των δεδομένων ούτως ώστε να διασφαλίζεται η ιδιωτικότητα των πολιτών. Αναγκαία κρίνεται η υποστήριξη μοναδικής ταυτοποίησης των πολιτών (Single Sign-On – SSO) για την εφάπαξ πιστοποίηση ταυτότητας του πολίτη και τη διάφανη διαβίβαση αυτής σε πολλούς παρόχους υπηρεσιών ηλεκτρονικής διακυβέρνησης.
- Μηχανισμοί ασφάλειας: η ασφάλεια των πληροφοριακών και επικοινωνιακών συστημάτων και των καναλιών επικοινωνίας κρίνεται απαραίτητη. Τα συστήματα θα πρέπει να είναι ασφαλή, ούτως ώστε να είναι σε θέση να εγγυηθούν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, καθώς και να αποτρέπουν την οποιαδήποτε αθέμιτη υποκλοπή ή παρακολούθηση των δεδομένων, ενώ θα πρέπει να εφαρμόζονται οι κατάλληλοι μηχανισμοί προστασίας επικοινωνιών. Ως εκ τούτου, οι οργανισμοί που εμπλέκονται στην παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης θα πρέπει να διαθέτουν και να εφαρμόζουν κατάλληλη πολιτική ασφάλειας. Απαραίτητη κρίνεται η κρυπτογράφηση δεδομένων για την ασφαλή μετάδοση αυτών μεταξύ των οντοτήτων του συστήματος και την αποθήκευσή τους.

4.2.7 Μελέτη Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Στόχος της Ηλεκτρονικής Διακυβέρνησης είναι η αξιοποίηση των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) με τέτοιο τρόπο ώστε να αναβαθμιστούν ουσιαστικά οι υπηρεσίες εξυπηρέτησης και πληροφόρησης προς όλους τους συναλλασσομένους (πολίτες, επιχειρήσεις, κτλ.) με φορείς της Δημόσιας Διοίκησης. Το βασικό μέσο για την πρόσβαση των πολιτών στις ηλεκτρονικά παρεχόμενες υπηρεσίες ενός συστήματος ηλεκτρονικής διακυβέρνησης είναι οι Κυβερνητικές Διαδικτυακές Πύλες (Government Portals), οι οποίες θα πρέπει:

- να επιτυγχάνουν εύκολη και ασφαλή πρόσβαση σε υπηρεσίες εξυπηρέτησης και πληροφόρησης για πολίτες, επιχειρήσεις, κοινότητες και ομάδες πολιτών.
- να παρέχουν εύστοχο και προσαρμοσμένο για τις ανάγκες του κάθε χρήστη περιεχόμενο.
- να προβάλουν ένα φιλικό πρόσωπο προς τον πολίτη.
- να αποτελούν προοδευτικά τον προτιμώμενο για τους πολίτες τρόπο συναλλαγής με τις Δημόσιες Υπηρεσίες.

Σύμφωνα με το Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών, βασικός στόχος της Διαδικτυακής Πύλης ενός κυβερνητικού φορέα είναι να καταστεί ένα κεντρικό σημείο επαφής του πολίτη με ο,τιδήποτε αφορά το συγκεκριμένο φορέα, προσφέροντας:

- ένα μοναδικό σημείο παροχής κάθε πληροφορίας που είναι διαθέσιμη από το φορέα προς το κοινό και κάθε υπηρεσίας-συναλλαγής που διαχειρίζεται ο φορέας.
- ένα σημείο κεντρικής ενημέρωσης για τις πρωτοβουλίες που αναλαμβάνονται ή εκτελούνται καθώς και για τις δραστηριότητες της πολιτικής ηγεσίας.
- έναν χώρο πρόσβασης σε οδηγίες για πρακτικά ζητήματα αρμοδιότητας του φορέα.
- ένα αρχικό σημείο πρόσβασης προς όλους τους επιμέρους φορείς που τελούν υπό την εποπτεία του φορέα.

Για να εκπληρωθεί ο σκοπός αυτός, απαραίτητη προϋπόθεση είναι η δημιουργία κλίματος εμπιστοσύνης στους πολίτες-χρήστες. Η εμπιστοσύνη εμπνέεται εξασφαλίζοντας μια καλή «εμπειρία του χρήστη» από την επίσκεψή του στην κυβερνητική πύλη. Ως εκ τούτου, η χρηστικότητα και η λειτουργικότητα πρέπει να λαμβάνονται υπόψη με ιδιαίτερη βαρύτητα κατά το σχεδιασμό των υπηρεσιών ΗΔ. Σύμφωνα με τις βασικές αρχές σχεδιασμού, η Κυβερνητική Πύλη κάθε φορέα πρέπει:

- να είναι κάτι περισσότερο από μια πηγή παράθεσης πληροφοριών σχετικά με τον φορέα. Ο σχεδιασμός της πρέπει να γίνει με πρώτη προτεραιότητα τις ανάγκες και τα ενδιαφέροντα των χρηστών, όπως αυτά έχουν καθοριστεί από τον φορέα.

- να είναι σε θέση να παρέχει προσωποποιημένες υπηρεσίες σε συγκεκριμένες κατηγορίες χρηστών. Η παροχή αυτών των υπηρεσιών προϋποθέτει την εγγραφή χρηστών και τη δημιουργία διαδικτυακής κοινότητας.
- να αποτελεί για τους πολίτες το μοναδικό εγκεκριμένο σημείο παροχής πληροφοριών που αφορούν τον φορέα, καθώς και το μοναδικό σημείο εισόδου για τη χρήση των ηλεκτρονικών υπηρεσιών που προσφέρει ο φορέας.
- να σχεδιαστεί με τέτοιο τρόπο ώστε να είναι διευκολύνεται η τακτική ενημέρωσή της με νέο περιεχόμενο καθώς και ο έλεγχος του ήδη αναρτημένου περιεχομένου.
- να παρουσιάζει με τρόπο διάφανο προς το χρήστη το περιεχόμενό της και τις όποιες διαδικτυακές υπηρεσίες αυτή προσφέρει.

Οι κατηγορίες χρηστών των Κυβερνητικών Διαδικτυακών Πυλών των φορέων δημόσιας διοίκησης είναι οι εξής: (α) πολίτες, (β) επιχειρήσεις και ομάδες επαγγελματιών, (γ) στελέχη του εκάστοτε δημόσιου φορέα, (δ) άλλοι δημόσιοι φορείς, (ε) συντάκτες ελληνικού και ξένου τύπου, (στ) μέλη της επιστημονικής κοινότητας, (ζ) ομάδες εθελοντών και φορείς ευαισθητοποίησης των πολιτών, και (η) άτομα και φορείς της αλλοδαπής.

Έπειτα από μελέτη της σχετικής βιβλιογραφίας [96][97][98][99][81], στην παρούσα ενότητα παρουσιάζεται ένα πλήθος υπηρεσιών που παρέχονται στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης από το κράτος και καλύπτουν ένα μεγάλο μέρος του φάσματος αυτής:

Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στις Δημόσιες Διοικήσεις (G2G):

- Εθνικό Δημοτολόγιο
- Εθνικό Ληξιαρχείο
- Ελεγκτική Υπηρεσία

Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στις Επιχειρήσεις (G2B):

- Δημόσιες Προμήθειες
- Στατιστικές Υπηρεσίες
- Ηλεκτρονικό Τελωνείο
- Ηλεκτρονική Πολεοδομία

Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στους Πολίτες (G2C):

- Ηλεκτρονική Υγεία
- Φορολογική εξυπηρέτηση
- Εύρεση Εργασίας
- Ηλεκτρονική Ψηφοφορία
- η-ΚΕΠ
- Κάρτα Αποδείξεων
- η-Παιδεία

Η κάθε μία από τις υπηρεσίες αυτές έχει τις δικές της ιδιαιτερότητες και χαρακτηριστικά. Για την αξιολόγηση των υπηρεσιών αυτών ως προς τις απαιτήσεις ασφάλειας, κρίνεται απαραίτητη η χρήση συγκεκριμένων κριτηρίων. Τα κριτήρια αυτά συνίστανται από μερικές από τις κύριες απαιτήσεις ασφάλειας συστημάτων, λαμβάνοντας επίσης υπόψη απαιτήσεις που αφορούν τον χρήστη. Πιο συγκεκριμένα, τα κριτήρια αυτά είναι τα εξής:

- *Αυθεντικοποίηση (Authentication)*: διαδικασία εξακρίβωσης της ταυτότητας του χρήστη μέσω των διαπιστευτηρίων του.
- *Εμπιστευτικότητα (Data Confidentiality)*: διασφάλιση ότι τα δεδομένα είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα.
- *Ακεραιότητα (Data Integrity)*: διασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένο πρόσωπο και παραμένουν πλήρη, ακριβή και ορθά.
- *Εμπιστοσύνη (Trust)*: αξιοπιστία και εγκυρότητα της ταυτότητας των χρηστών στο σύστημα.
- *Μη Αποποίηση Ευθύνης (Non-repudiation)*: διασφάλιση της μη άρνησης του χρήστη για τη τέλεση πράξεων και την συμμετοχή σε μία συναλλαγή.
- *Ανωνυμία Χρήστη (User Anonymity)*: διατήρηση της ανωνυμίας του χρήστη μέσω της αποτροπής αποκάλυψης πληροφοριών που οδηγούν στην ταυτοποίησή του.
- *Ιδιωτικότητα (Privacy)*: δικαίωμα του χρήστη για την προστασία των προσωπικών του δεδομένων και τον έλεγχο αλλά και την επιλογή σχετικά με το ποια στοιχεία του θα είναι προσβάσιμα και από ποιον.
- *Ανίχνευση Τοποθεσίας Χρήστη (User Location Traceability)*: ικανότητα να εντοπίζεται η τοποθεσία του χρήστη.
- *Έλεγχος και Παρακολούθηση Διαδικασιών (Auditability)*: δυνατότητα συλλογής, ανάλυσης και αναφοράς των ενεργειών που λαμβάνουν χώρα σε ένα σύστημα.

Δεδομένου ότι κάθε υπηρεσία έχει κάποια συγκεκριμένα χαρακτηριστικά που μπορεί να υπαγορεύουν συγκεκριμένες απαιτήσεις ασφάλειας, η παρουσίαση και αξιολόγηση του συνόλου των υπηρεσιών βάσει όλων των δυνατών κριτηρίων είναι αδύνατη. Για το λόγο αυτό, η επιλογή των παραπάνω κριτηρίων που αποτελούν τις βασικότερες απαιτήσεις ασφάλειας συστημάτων έγινε με γνώμονα τη μεγαλύτερη δυνατή κάλυψη του εύρους αυτών. Η κλίμακα της αξιολόγησης περιλαμβάνει 3 επίπεδα: 1. Μη απαραίτητο, 2. Επιθυμητό, 3. Αναγκαίο. Ακολουθεί η αξιολόγηση των υπηρεσιών.

4.2.7.1 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στις Δημόσιες Διοικήσεις (G2G)

Υπηρεσία Α: Εθνικό Δημοτολόγιο

Περιγραφή υπηρεσίας:

Το Εθνικό Δημοτολόγιο συνίσταται από την συνένωση των υφιστάμενων δημοτολογίων των Δήμων και Κοινοτήτων όλης της χώρας και περιλαμβάνει τη διαλειτουργικότητα συστημάτων οργανισμών δημοσίου συμφέροντος όπως Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), Αστυνομία, Στρατολογία, Ασφαλιστικά Ταμεία, Υπουργείο Δικαιοσύνης, Υπουργείο Οικονομίας κ.ο.κ. Με τον τρόπο αυτό, δημιουργείται μια κεντρική βάση δεδομένων που περιλαμβάνει το σύνολο των εγγραφών Ελλήνων πολιτών εγγεγραμμένων στα Δημοτολόγια με απώτερο σκοπό την ανταλλαγή στοιχείων μεταξύ πολλών βάσεων δεδομένων που χρησιμοποιούν οι διάφοροι δημόσιοι φορείς αλλά και Οργανισμοί Τοπικής Αυτοδιοίκησης (ΟΤΑ) καθώς και τη γρήγορη και ακριβή διασταύρωση και ταυτοποίηση προσωπικών δεδομένων και στοιχείων πολιτών πάντα στο πλαίσιο διασφάλισης προστασίας αυτών. Επιπλέον, με τη δημιουργία του Εθνικού Δημοτολογίου επιτυγχάνεται και βελτίωση της ποιότητας των πληροφοριών και των εξαρτωμένων από αυτές υπηρεσιών προς τον πολίτη (G2C) λόγω της μείωσης γραφειοκρατικών διαδικασιών, όπως χορήγηση πιστοποιητικού γεννήσεως, βεβαίωσης ιθαγένειας, βεβαίωσης οικογενειακής κατάστασης, απλούστευση διαδικασίας μεταδημότευσης κ.λπ.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και τη διαχείριση δεδομένων των πολιτών
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των αποθηκευμένων προσωπικών δεδομένων των πολιτών στις βάσεις του εθνικού δημοτολογίου κρίνεται απολύτως αναγκαία
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη

Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων, η επεξεργασία και αποθήκευση των οποίων πραγματοποιούνται στο πλαίσιο των παρεχόμενων υπηρεσιών του συστήματος, κρίνεται απολύτως αναγκαία
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Επιθυμητό	Η καταγραφή των δραστηριοτήτων των χρηστών στο σύστημα είναι επιθυμητή για τον έλεγχο πιθανόν κακόβουλων ενεργειών

Υπηρεσία Β: Εθνικό Ληξιαρχείο

Περιγραφή υπηρεσίας:

Το Εθνικό Ληξιαρχείο αποτελεί μία κεντρική βάση δεδομένων στην οποία καταγράφονται στοιχεία δημοτικής κατάστασης πολιτών καθώς και όλες οι υφιστάμενες αλλά και νέες ληξιαρχικές πράξεις που συντάσσονται για κάθε ληξιαρχικό γεγονός (π.χ. γάμος, θάνατος, διαζύγιο, υιοθεσία, μεταβολή ονόματος ή επωνύμου κ.ο.κ.) που δηλώνεται στα τοπικά Ληξιαρχεία της χώρας. Εκτός από τη διασύνδεση των Ληξιαρχείων της χώρας επιτυγχάνεται και η διαλειτουργικότητα μεταξύ συστημάτων άλλων δημόσιων φορέων, όπως Προξενείων, ΚΕΠ, Υπουργείου Εσωτερικών κ.λπ. Ο συνδυασμός παρεχόμενων υπηρεσιών του Εθνικού Ληξιαρχείου αλλά και εκείνων του Εθνικού Δημοτολογίου οδηγεί στην συγκρότηση ενοποιημένου Εθνικού Μητρώου Πολιτών που αποτελεί το πλήρες, αξιόπιστο και επικαιροποιημένο κάθε στιγμή ηλεκτρονικό μητρώο των πολιτών της χώρας, απόρροια του οποία είναι η έκδοση της "Κάρτας Πολίτη". Επιπλέον, με την ύπαρξη του Εθνικού Ληξιαρχείου απλουστεύονται και υπηρεσίες παρεχόμενες στον πολίτη (G2C) μέσω κεντρικών διαδικτυακών πυλών, όπως χορήγηση αντιγράφου ληξιαρχικής πράξης γέννησης, πιστοποιητικού εγγύτερων συγγενών, εντοπιότητας κ.λπ.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και τη διαχείριση δεδομένων των πολιτών
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των αποθηκευμένων προσωπικών δεδομένων των πολιτών στις βάσεις του εθνικού ληξιαρχείου κρίνεται απολύτως αναγκαία
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων, η επεξεργασία και αποθήκευση των οποίων πραγματοποιούνται στο πλαίσιο των παρεχόμενων υπηρεσιών του συστήματος, κρίνεται απολύτως αναγκαία
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Επιθυμητό	Η καταγραφή των δραστηριοτήτων των χρηστών στο σύστημα είναι επιθυμητή για τον έλεγχο πιθανόν κακόβουλων ενεργειών

Υπηρεσία Γ: Ελεγκτική Υπηρεσία

Περιγραφή υπηρεσίας:

Για την κάλυψη των επιχειρησιακών αναγκών των Ελεγκτικών Υπηρεσιών του Υπουργείου Οικονομικών παρέχεται από το κράτος ένα ολοκληρωμένο πληροφοριακό σύστημα μέσω του οποίου οι υπάλληλοι του Υπουργείου Οικονομικών μπορούν να σχεδιάσουν, προγραμματίσουν και διενεργήσουν προληπτικούς ελέγχους διαφόρων υποθέσεων και διαδικασιών καθώς και να αποτιμήσουν τα σχετικά αποτελέσματα αυτών. Οι υποθέσεις που υπόκεινται σε έλεγχο αφορούν είτε φορολογικά στοιχεία πολιτών ή επιχειρήσεων με σκοπό την πάταξη της φοροδιαφυγής, την εύρεση φορολογικών παραβάσεων, την επίτευξη διαφάνειας και νομιμότητας στις οικονομικές τους συναλλαγές, είτε οικονομικά στοιχεία δαπανών για υπηρεσίες υγείας σε ασφαλισμένους, όπως κόστος συνταγών φαρμάκων που συνταγογραφούνται από ιατρούς και εκτελούνται από φαρμακοποιούς κ.λπ.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και τον έλεγχο των επιθυμητών στοιχείων
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον αφορούν στοιχεία επιχειρήσεων
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που ελέγχονται από τους υπαλλήλους της Ελεγκτικής Υπηρεσίας είναι απολύτως αναγκαία για την ακρίβεια και την ορθότητα των αποτελεσμάτων ελέγχου
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη

Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Η προστασία της ιδιωτικότητας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

4.2.7.2 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στις Επιχειρήσεις (G2B)

Υπηρεσία Α: Δημόσιες Συμβάσεις - Προμήθειες

Περιγραφή υπηρεσίας:

Η ηλεκτρονική διεξαγωγή των δημόσιων προμηθειών αποτελεί ένα οργανωμένο σύστημα μέσω του οποίου διασυνδέονται εταιρείες, οργανισμοί και επιχειρήσεις με τους προμηθευτές τους και συνιστά το μέσο για τη μετάβαση όλων των οργανισμών του Δημόσιου και Ιδιωτικού τομέα στις διαδικασίες του Ηλεκτρονικού Επιχειρείν. Το σύστημα αυτό παρέχει όλα τα μέσα για τη δημοσίευση διαγωνισμών με αντικείμενο την εκτέλεση έργων, την προμήθεια αγαθών και την παροχή υπηρεσιών, την αυτόματη ενημέρωση όλων των δυνητικών προμηθευτών σε περίπτωση δημοσίευσης διαγωνισμών που τους αφορούν, την υποβολή προσφορών, τον έλεγχο και την σύγκριση των τιμών των προσφορών από την πλευρά των οργανισμών, την σύναψη συμβάσεων και τη δημιουργία σχετικών συμβολαίων κ.ο.κ. Η χρήση του συστήματος αυτού συμβάλλει στη διασφάλιση διαφάνειας υφιστάμενων διαδικασιών σχετικών με διαγωνισμούς προμήθειας, στην ενίσχυση του δίκαιου ανταγωνισμού των επιχειρήσεων-προμηθευτών (ιδίως των μικρών και μεσαίων επιχειρήσεων), στη μείωση χρόνου διεξαγωγής των διαγωνισμών λόγω απλοποίησής των διαδικασιών ανάθεσης καθώς και στην εξοικονόμηση πόρων (είτε ανθρώπινου δυναμικού είτε χρημάτων) και στη μεγιστοποίηση της αποτελεσματικότητας των δημοσίων δαπανών.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και τη δημοσίευση προκήρυξης ή τη παρουσίαση σχετικής προσφοράς και τη σύναψη συμβάσεων
Εμπιστευτικότητα	Μη απαραίτητο	Εφόσον οι προκηρύξεις διαγωνισμών δημοσιεύονται στο ευρύ κοινό, η εμπιστευτικότητα των δεδομένων δεν κρίνεται απαραίτητη
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων των προκηρύξεων και των αντίστοιχων προσφορών είναι απολύτως αναγκαία
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Εφόσον οι προκηρύξεις διαγωνισμών δημοσιεύονται στο ευρύ κοινό, η διασφάλιση ιδιωτικότητας των δεδομένων δεν κρίνεται απαραίτητη
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

Υπηρεσία Β: Υποβολή στοιχείων σε Στατιστικές Υπηρεσίες

Περιγραφή υπηρεσίας:

Το σύστημα υποβολής στοιχείων σε στατιστικές υπηρεσίες παρέχει τη δυνατότητα στις υπόχρεες επιχειρήσεις και λογιστικά γραφεία να υποβάλουν ηλεκτρονικά μέσω ενός φιλικού περιβάλλοντος τις δηλώσεις ενδοκοινοτικών αφίξεων και αποστολών προϊόντων μεταξύ Ελλάδας και των υπόλοιπων χωρών της Ευρωπαϊκής Ένωσης καθώς και σε τουριστικά καταλύματα να υποβάλουν τα μηνιαία δελτία κίνησής τους. Οι δηλώσεις που υποβάλλονται από τους προαναφερθέντες φορείς ελέγχονται και σε περίπτωση εύρεσης λάθους από τον ελεγκτή ενημερώνεται σε πραγματικό χρόνο ο αρμόδιος για τη διόρθωσή του. Η όλη διαδικασία παρακολουθείται έτσι ώστε να διασφαλίζεται η εκπλήρωση των στατιστικών υποχρεώσεων των επιχειρήσεων και παράλληλα παρέχεται διασύνδεση των υποβληθέντων στοιχείων με τα αντίστοιχα φορολογικά που έχει στη διάθεσή του το Υπουργείο Οικονομικών αλλά και όσα στοιχεία συλλέγονται από τα κατά τόπους τελωνεία της χώρας. Σκοπός των Στατιστικών Υπηρεσιών είναι η παροχή τακτικής, έγκαιρης και αξιόπιστης στατιστικής πληροφόρησης. Τα αποτελέσματα των διαφόρων απογραφών, ερευνών και μελετών που διεξάγονται από αυτές, δημοσιεύονται σε ειδικές θεματικές εκδόσεις του Κυβερνητικού Τύπου ή από τις ίδιες τις Στατιστικές Υπηρεσίες.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και την υποβολή στοιχείων από την επιχείρηση ή τη διαχείριση δεδομένων των επιχειρήσεων από την στατιστική υπηρεσία
Εμπιστευτικότητα	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που υποβάλλονται στην στατιστική υπηρεσία κρίνεται απαραίτητη για την αξιοπιστία των στατιστικών ελέγχων και την ορθότητα των αποτελεσμάτων

Εμπιστοσύνη	Αναγκαίο	Η ύπαρξη εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων κρίνεται αναγκαία
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Εφόσον τα στοιχεία αυτά που συγκεντρώνονται δημοσιεύονται στο ευρύ κοινό, η διασφάλιση ιδιωτικότητας των δεδομένων δεν κρίνεται απαραίτητη
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Μη απαραίτητο	Η παρακολούθηση διαδικασιών δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας

Υπηρεσία Γ: Ηλεκτρονικό Τελωνείο

Περιγραφή υπηρεσίας:

Η λειτουργία των Ηλεκτρονικών Τελωνειακών Συστημάτων αποσκοπεί στη διευκόλυνση και απλούστευση διαδικασιών νόμιμου εμπορίου εισαγωγής και εξαγωγής, στη μείωση κόστους δαπανών, είσπραξη όλων των δασμών και μείωση χρόνου εκτελωνισμού εμπορευμάτων των συναλλασσομένων με τα ελληνικά Τελωνεία καθώς και στη διαλειτουργικότητα μέσω ανταλλαγής δεδομένων μεταξύ των Αρχών των χωρών εξαγωγής και εισαγωγής, των Τελωνειακών Υπηρεσιών και των Οικονομικών Φορέων. Οι παρεχόμενες υπηρεσίες του συστήματος Ηλεκτρονικού Τελωνείου αφορούν την ηλεκτρονική υποβολή αιτημάτων για την έκδοση τελωνειακών αδειών και σχετικών τελωνειακών παραστατικών για τον έλεγχο αυτών από του αρμόδιους φορείς, την ηλεκτρονική πληρωμή τελωνειακών οφειλών αλλά και την συνεχή ενημέρωση του άμεσα ενδιαφερόμενου σε πραγματικό χρόνο για την εξέλιξη της όλης διαδικασίας με τη διατήρηση του ιστορικού αυτής.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον αφορούν στοιχεία επιχειρήσεων
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που υποβάλλονται στο Ηλεκτρονικό Τελωνείο είναι απολύτως απαραίτητη για τη διενέργεια ελέγχων αυτών που ακολουθεί από τους αρμόδιους υπαλλήλους
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Η προστασία της ιδιωτικότητας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

Υπηρεσία Δ: Ηλεκτρονική Πολεοδομία

Περιγραφή υπηρεσίας:

Η Ηλεκτρονική Πολεοδομία συνιστά το ενιαίο σύστημα υποβολής αιτήσεων, έγκρισης και ελέγχου πολεοδομικών αδειών δόμησης, ένα εξαιρετικό εργαλείο για όλες τις υπηρεσίες δόμησης (πολεοδομικές υπηρεσίες) της χώρας αλλά και για τους μηχανικούς. Εκτός από την απλοποίηση και τη βελτίωση ως προς το χρόνο ολοκλήρωσης της διαδικασίας έκδοσης άδειας λόγω της σημαντικής μείωσης της γραφειοκρατίας που προκαλεί καθυστερήσεις, δημιουργείται με αυτόν τον τρόπο και το ηλεκτρονικό αρχείο για την ταυτότητα του εκάστοτε κτιρίου, έτσι ώστε να καταπολεμηθεί η αυθαίρετη δόμηση. Συγκεκριμένα, κατά τη δημιουργία αίτησης έκδοσης άδειας δόμησης, ο μηχανικός υποβάλλει σε ηλεκτρονική μορφή τα απαραίτητα δικαιολογητικά, τα οποία έπειτα ελέγχονται από την αρμόδια Υπηρεσία Δόμησης. Κατά τη διάρκεια του ελέγχου των δικαιολογητικών, ο μηχανικός αλλά και ο ιδιοκτήτης έχουν τη δυνατότητα να παρακολουθούν την όλη διαδικασία σε πραγματικό χρόνο καθώς και να λαμβάνουν τυχόν σχόλια ή παρατηρήσεις των ελεγκτών. Με την ικανοποίηση όλων των απαραίτητων τροποποιήσεων από την πλευρά του μηχανικού εκδίδεται και η σχετική οικοδομική άδεια.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία και τη διαχείριση δεδομένων των πολιτών
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που υποβάλλονται στην Ηλεκτρονική Πολεοδομία είναι απολύτως απαραίτητη για τη διενέργεια ελέγχων αυτών που ακολουθεί από τους αρμόδιους υπαλλήλους
Εμπιστοσύνη	Επιθυμητό	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται επιθυμητή, δεδομένου ότι η αυθεντικοποίηση αυτών είναι απαραίτητη

Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Επιθυμητό	Η προστασία της ιδιωτικότητας του χρήστη είναι επιθυμητή
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

4.2.7.3 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης παρεχόμενες στους Πολίτες (G2C)

Υπηρεσία Α: Υπηρεσίες Υγείας

Περιγραφή υπηρεσίας:

Η Ηλεκτρονική Υγεία συνίσταται από την παροχή υπηρεσιών υγείας με τη χρήση μέσων ΤΠΕ υιοθετώντας το ασθενοκεντρικό μοντέλο με τον ασθενή να αναλαμβάνει πλέον ενεργό ρόλο στη διασφάλιση, προστασία και παρακολούθηση της υγείας του. Πρόκειται ουσιαστικά για τη μετεξέλιξη των παραδοσιακών συστημάτων υγείας και οι υπηρεσίες που παρέχονται πλέον ηλεκτρονικά μέσω ενός τέτοιου συστήματος περιλαμβάνουν υπηρεσίες τηλεϊατρικής, ηλεκτρονικής συνταγογράφησης, διατήρησης ιστορικού ασθενών σε ηλεκτρονικούς ιατρικούς φακέλους, διαχείρισης στοιχείων ασθενών μέσω ηλεκτρονικών μητρώων υγείας, εύρεσης πληροφοριών για εφημερεύοντα νοσοκομεία και φαρμακεία, ηλεκτρονικής αποπληρωμής υπηρεσιών υγείας, ηλεκτρονικών προμηθειών δημόσιων φορέων υγείας με υλικό απαραίτητο για τη λειτουργία τους και την περίθαλψη ασθενών, τηλεφροντίδας και διαχείρισης χρόνιων πασχόντων για την παρακολούθησή του κ.λπ. Στο πλαίσιο της ηλεκτρονικής υγείας επιτυγχάνεται και η διαλειτουργικότητα μεταξύ συστημάτων Φορέων Κοινωνικής Ασφάλισης, διαφόρων επαγγελματιών υγείας, παρόχων υπηρεσιών υγείας καθώς και του Υπουργείου Υγείας. Τα οφέλη της ηλεκτρονικής υγείας είναι πολλά, τόσο σε ατομικό όσο και σε συλλογικό επίπεδο λόγω της αποτελεσματικότητας όλων των παρεχόμενων υπηρεσιών, μέσω των οποίων βελτιώνεται σημαντικά η ποιότητα παρεχόμενης περί-

θαλψης στον ασθενή.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που δημιουργούνται, επεξεργάζονται και αποθηκεύονται στις βάσεις του συστήματος Ηλεκτρονικής Υγείας είναι απολύτως αναγκαία και σημαντική καθώς αφορά άμεσα την υγεία των πολιτών
Εμπιστοσύνη	Αναγκαίο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων του συστήματος κρίνεται απολύτως απαραίτητη
Μη Αποποίηση Ευθύνης	Αναγκαίο	Λόγω της φύσεως των παρεχόμενων υπηρεσιών και της σημαντικότητας αυτών, η μη αποποίηση ευθύνης ενεργειών κρίνεται απολύτως αναγκαία
Ανωνυμία Χρήστη	Αναγκαίο	Η διατήρηση της ανωνυμίας του χρήστη κρίνεται αναγκαία, λόγω του υψηλού βαθμού ευαισθησίας των προσωπικών του δεδομένων
Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων, η επεξεργασία και αποθήκευση των οποίων πραγματοποιούνται στο πλαίσιο των παρεχόμενων υπηρεσιών του συστήματος, κρίνεται απολύτως αναγκαία

Ανίχνευση Τοποθεσίας Χρήστη	Αναγκαίο	Σε ορισμένες περιπτώσεις, η ανίχνευση τοποθεσίας χρήστη σε συνδυασμό με κάποια στοιχεία της ταυτότητάς του κρίνεται απολύτως απαραίτητη για την πρόσβασή του σε υπηρεσίες
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

Υπηρεσία Β: Φορολογική εξυπηρέτηση

Περιγραφή υπηρεσίας:

Για τη φορολογική εξυπηρέτηση των πολιτών της χώρας, μεγάλης κλίμακας ολοκληρωμένα πληροφοριακά συστήματα, τα οποία διαχειρίζεται οργανική μονάδα του Υπουργείου Οικονομικών, παρέχουν ηλεκτρονικές υπηρεσίες σε 24ωρη βάση με σκοπό την ταχύτερη και ευκολότερη εξυπηρέτηση αυτών για την εκπλήρωση των φορολογικών τους υποχρεώσεων και τη διευθέτηση σχετικών εκκρεμοτήτων αλλά και για τον έλεγχο και την παρακολούθηση των αποτελεσμάτων της εκάστοτε εφαρμοζόμενης οικονομικής πολιτικής. Μέσω των συστημάτων αυτών δίνεται η δυνατότητα στον πολίτη να υποβάλει ηλεκτρονικά κάθε είδους φορολογική δήλωση χωρίς να είναι απαραίτητη η προσέλευσή του στη Δημόσια Οικονομική Υπηρεσία (Δ.Ο.Υ.) που ανήκει, να λάβει και να εκτυπώσει τα αντίστοιχα εκκαθαριστικά των δηλώσεών του καθώς και τη φορολογική του ενημερότητα, να εκτυπώσει παράβολα διαφόρων Υπουργείων, να ενημερωθεί για τη λήψη Επιδόματος Κοινωνικής Αλληλεγγύης ή Επιδόματος Κατανάλωσης Πετρελαίου Θέρμανσης σε περίπτωση που είναι δικαιούχος, να εκτυπώσει έντυπα τελών κυκλοφορίας των οχημάτων του κ.λπ.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία

Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που υποβάλλονται στις υπηρεσίες φορολογικής εξυπηρέτησης είναι απαραίτητη για τη διενέργεια των όποιων ενεργειών απαιτούνται σε αυτά
Εμπιστοσύνη	Αναγκαίο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων του συστήματος κρίνεται αναγκαία λόγω της φύσης των παρεχόμενων υπηρεσιών
Μη Αποποίηση Ευθύνης	Επιθυμητό	Η μη αποποίηση ευθύνης κρίνεται επιθυμητή
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Η προστασία της ιδιωτικότητας του χρήστη δεν κρίνεται αναγκαία
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

Υπηρεσία Γ: Εύρεση εργασίας

Περιγραφή υπηρεσίας:

Η ηλεκτρονική υπηρεσία εύρεσης εργασίας παρέχει στον πολίτη τη δυνατότητα να αναζητήσει εργασία ή προσωπικό, αν είναι εργοδότης, βάσει κριτηρίων. Εισάγοντας τα κριτήρια της θέσης εργασίας ή του εργαζόμενου που επιθυμεί, βάσει της γεωγραφικής περιοχής του ενδιαφερόμενου, εμφανίζεται λίστα με στοιχεία επικοινωνίας επιχειρήσεων που ζητούν υπαλλήλους ή λίστα με στοιχεία επικοινωνίας πολιτών που πληρούν τα κριτήρια και ζητούν εργασία αντίστοιχα. Επιπλέον, πέρα από την εισαγωγή κριτηρίων σε ειδικές φόρμες, παρέχεται στον πο-

λίτη η δυνατότητα υποβολής σύντομου βιογραφικού σημειώματος, αίτησης για συμμετοχή σε προγράμματα απασχόλησης ή ακόμα και αίτησης για λήψη βεβαίωσης ανεργίας, δεδομένου ότι υπάρχει διασύνδεση με τον εκάστοτε εθνικό οργανισμό απασχόλησης εργατικού δυναμικού. Σε περίπτωση που υπάρξει ενδιαφέρον από την πλευρά κάποιου εργοδότη ή έχει προκύψει κάποια νέα θέση εργασίας σχετική με την ειδικότητα που ενδιαφέρεται ο πολίτης, ο τελευταίος ενημερώνεται άμεσα από το σύστημα.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Μη απαραίτητο	Η εμπιστευτικότητα των δεδομένων δεν είναι αναγκαία λόγω της φύσης της υπηρεσίας
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που υποβάλλονται είτε από τον εργοδότη είτε από τον πολίτη που ενδιαφέρεται για εργασία είναι απαραίτητη προκειμένου η υπηρεσία στο σύνολό της να είναι αξιόπιστη
Εμπιστοσύνη	Επιθυμητή	Η ύπαρξη εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων είναι επιθυμητή
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Μη απαραίτητο	Η διατήρηση ιστορικού των υποκειμένων διαδικασιών δεν κρίνεται απαραίτητη

Υπηρεσία Δ: Ηλεκτρονική Ψηφοφορία

Περιγραφή υπηρεσίας:

Η Ηλεκτρονική Ψηφοφορία δίνει τη δυνατότητα στους ψηφοφόρους να ασκήσουν το εκλογικό τους δικαίωμα ηλεκτρονικά ψηφίζοντας ανώνυμα από τον τόπο της επιλογής τους χωρίς να απαιτείται να παρευρεθούν σε κάποιο εκλογικό τμήμα. Με τη χρήση αυτοματοποιημένων μεθόδων για τη διεξαγωγή εκλογών, την καταμέτρηση ψήφων και την εξαγωγή αποτελεσμάτων επιτυγχάνεται ταχύτερη οργάνωση της εκλογικής διαδικασίας και διευκολύνεται έτσι ο τρόπος διεξαγωγής της. Το σύστημα Ηλεκτρονικής Ψηφοφορίας μπορεί να χρησιμοποιηθεί για τη διεξαγωγή κάθε είδους εθνικών εκλογών, όπως δημοτικές και κοινοβουλευτικές, δημοψηφισμάτων, εκλογών σε δημόσιους οργανισμούς κ.ο.κ.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Αναγκαίο	Η εμπιστευτικότητα των δεδομένων είναι αναγκαία εφόσον στην πλειοψηφία τους αφορούν προσωπικά δεδομένα πολιτών και η ψήφος υποβάλλεται μυστικά
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα της ψήφου που καταχωρείται είναι ιδιαίτερα σημαντική και απαραίτητη
Εμπιστοσύνη	Αναγκαίο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται απολύτως απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Αναγκαίο	Κατά τη διενέργεια εκλογών, η εξασφάλιση ανωνυμίας του χρήστη και έτσι η διασφάλιση μη σύνδεσης της ψήφου του με εκείνον και την ταυτοποίησή του κρίνεται απαραίτητη

Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων του χρήστη κρίνεται απολύτως αναγκαία
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Αναγκαίο	Η διατήρηση του ιστορικού των δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα και η παρακολούθησή του κρίνονται απολύτως απαραίτητες

Υπηρεσία Ε: η-ΚΕΠ

Περιγραφή υπηρεσίας:

Το η-ΚΕΠ παρέχει στους πολίτες διαδικτυακά τις υπηρεσίες εκείνες που παρέχονται με τον παραδοσιακό τρόπο από τα Κέντρα Εξυπηρέτησης Πολιτών, έχοντας ως κύριο στόχο τη διευκόλυνσή τους και τη βελτίωση του επιπέδου εξυπηρέτησής τους από τη Δημόσια Διοίκηση. Για την επίτευξη παροχής υπηρεσιών μέσω η-ΚΕΠ στους πολίτες είναι απαραίτητη η διασύνδεση υπηρεσιών διαφόρων δημόσιων φορέων, όπως Δημοτολογίων, Ληξιαρχείων, Φορέων Κοινωνικής Ασφάλισης, Στρατολογίας, Τμήματος Ποινικού Μητρώου κ.λπ. Το η-ΚΕΠ δίνει τη δυνατότητα στους πολίτες όχι μόνο να ενημερωθούν σχετικά με απαιτούμενα δικαιολογητικά για χορήγηση διαφόρων πιστοποιητικών/βεβαιώσεων/αδειών αλλά και να υποβάλουν και να διαχειριστούν ηλεκτρονικά τις αιτήσεις τους για όλες τις πιστοποιημένες διαδικασίες, όπως χορήγηση πιστοποιητικού οικογενειακής κατάστασης, ατομικού λογαριασμού ασφάλισης κ.ο.κ. Η αποστολή της ηλεκτρονικής αίτησης γίνεται στο ΚΕΠ της επιλογής τους και όταν το ΚΕΠ διεκπεραιώσει το αίτημά του, ο πολίτης ενημερώνεται έτσι ώστε να παραλάβει το τελικό έγγραφο. Σε περίπτωση επιλογής υπηρεσίας ηλεκτρονικής διεκπεραίωσης, ο πολίτης μπορεί να παρακολουθεί το ιστορικό των ηλεκτρονικών συναλλαγών του και να λάβει ηλεκτρονικά το αιτούμενο έγγραφο, να το αποθηκεύσει στην προσωπική ηλεκτρονική του θυρίδα και να έχει πρόσβαση σε αυτά ανά πάσα στιγμή για το διάστημα της ισχύος του.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**

Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Μη απαραίτητο	Η εμπιστευτικότητα δεν κρίνεται απαραίτητη λόγω της φύσης της υπηρεσίας
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που επεξεργάζονται και αποθηκεύονται στις βάσεις του συστήματος του η-ΚΕΠ είναι απολύτως αναγκαία
Εμπιστοσύνη	Αναγκαίο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων κρίνεται αναγκαία
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων, η επεξεργασία και αποθήκευση των οποίων πραγματοποιούνται στο πλαίσιο των παρεχόμενων υπηρεσιών του συστήματος, κρίνεται απολύτως αναγκαία
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Επιθυμητό	Η καταγραφή των δραστηριοτήτων των χρηστών στο σύστημα είναι επιθυμητή για τον έλεγχο πιθανόν κακόβουλων ενεργειών

Υπηρεσία ΣΤ: Κάρτα Αποδείξεων

Περιγραφή υπηρεσίας:

Η Κάρτα Αποδείξεων αποτελεί το προσωπικό μέσο για τη συλλογή αποδείξεων λιανικής πώλησης και παροχής υπηρεσιών του φορολογούμενου πολίτη ανεξαρτήτου τρόπου πληρωμής, έτσι ώστε να γνωρίζει εκείνος κάθε στιγμή τα έξοδά του, αποφεύγοντας τη χρονοβόρα καταγραφή τους όταν απαιτείται κατά την

υποβολή της ετήσιας φορολογικής του δήλωσης. Η Κάρτα Αποδείξεων είναι μία μαγνητική κάρτα που παρέχεται σε φυσικά πρόσωπα, είναι ανώνυμη, συνδέεται μόνο μέσω του Α.Φ.Μ. του καταναλωτή και καταχωρείται σε αυτή μόνο το κατάστημα στο οποίο πραγματοποιήθηκε η όποια συναλλαγή καθώς και το ποσό της απόδειξης. Σκοπός της χρήσης αυτής, πέρα από τη διευκόλυνση του πολίτη, είναι και η πάταξη της φοροδιαφυγής καθώς και η δικαιότερη κατανομή των φορολογικών βαρών αφού ανά πάσα στιγμή το Υπουργείο Οικονομικών μπορεί να γνωρίζει τα έσοδα της εκάστοτε επιχείρησης.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, για τη χρήση της κάρτας αποδείξεων δεν απαιτείται εξακρίβωση της ταυτότητας του χρήστη
Εμπιστευτικότητα	Μη απαραίτητο	Η εμπιστευτικότητα δεν κρίνεται απαραίτητη λόγω της φύσης της υπηρεσίας
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που αποθηκεύονται στην κάρτα αποδείξεων του πολίτη είναι απολύτως αναγκαία
Εμπιστοσύνη	Μη απαραίτητο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων δεν κρίνεται απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Λόγω της φύσης της υπηρεσίας, η μη αποποίηση ευθύνης δεν κρίνεται απαραίτητη
Ανωνυμία Χρήστη	Αναγκαίο	Η διατήρηση της ανωνυμίας του χρήστη είναι απαραίτητη λόγω της φύσης της υπηρεσίας

Ιδιωτικότητα	Αναγκαίο	Η διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων, η επεξεργασία και αποθήκευση των οποίων πραγματοποιούνται στο πλαίσιο των παρεχόμενων υπηρεσιών του συστήματος, κρίνεται απολύτως αναγκαία. Στην συγκεκριμένη υπηρεσία απαιτείται επίσης η διασφάλιση της ιδιωτικότητας όσον αφορά το είδος της υπηρεσίας αλλά και τα ακριβή προϊόντα που αγοράζονται από τον πολίτη
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Επιθυμητό	Η καταγραφή των δραστηριοτήτων των χρηστών στο σύστημα είναι επιθυμητή για τον έλεγχο πιθανόν κακόβουλων ενεργειών

Υπηρεσία Ζ: η-Παιδεία

Περιγραφή υπηρεσίας:

Στο πλαίσιο της Ηλεκτρονικής Παιδείας, το κράτος και πιο συγκεκριμένα το Υπουργείο Παιδείας παρέχει στους μαθητές και εκπαιδευτικούς της πρωτοβάθμιας και της δευτεροβάθμιας αλλά και στους φοιτητές της τριτοβάθμιας εκπαίδευσης ένα σύνολο υπηρεσιών – εργαλείων για την στήριξή τους κατά τη διάρκεια των σπουδών τους. Στην Ελλάδα, για παράδειγμα, για την πρωτοβάθμια εκπαίδευση έχει δημιουργηθεί το "Ψηφιακό Σχολείο", μία ψηφιακή εκπαιδευτική πλατφόρμα που δίνει τη δυνατότητα σε μαθητές και δασκάλους να έχουν πρόσβαση σε σχολικά βιβλία εμπλουτισμένα με διαδραστικό ψηφιακό υλικό, πλούσιο εκπαιδευτικό υλικό όπως πειράματα, εκπαιδευτικά παιχνίδια και ασκήσεις κ.λπ. Για τους μαθητές της δευτεροβάθμιας εκπαίδευσης, το Υπουργείο Παιδείας ενημερώνει μέσα από την ιστοσελίδα του τους μαθητές σχετικά με τις βάσεις εισαγωγής στα πανεπιστήμια κάθε χρόνο, δίνει τη δυνατότητα πρόσβασης σε θέματα πανελληνίων εξετάσεων καθώς και ηλεκτρονικής συμπλήρωσης και υποβολής του μηχανογραφικού δελτίου των μαθητών της Γ' Λυκείου. Τέλος, για τους φοιτητές της τριτοβάθμιας εκπαίδευσης, οι παρεχόμενες υπηρεσίες αφορούν την απόκτηση ακαδημαϊκής ταυτότητας, την επιλογή διδακτικών συγγραμμάτων, την παροχή δωρεάν αποθηκευτικού χώρου για τα ψηφιακά δεδομένα τους καθώς και πρόσβαση σε δωρεάν λογισμικό.

Αξιολόγηση απαιτήσεων ασφάλειας υπηρεσίας:

Απαιτήσεις Ασφάλειας	**Αξιολόγηση**	**Αιτιολόγηση**
Αυθεντικοποίηση	Αναγκαίο	Η αυθεντικοποίηση του χρήστη κρίνεται αναγκαία για την πρόσβασή του στην υπηρεσία
Εμπιστευτικότητα	Μη απαραίτητο	Η εμπιστευτικότητα δεν κρίνεται απαραίτητη λόγω της φύσης της υπηρεσίας
Ακεραιότητα	Αναγκαίο	Η ακεραιότητα των δεδομένων που δημοσιεύονται στο πλαίσιο των παρεχόμενων υπηρεσιών της η-Παιδείας είναι απολύτως απαραίτητη
Εμπιστοσύνη	Μη απαραίτητο	Η εμπιστοσύνη μεταξύ των εμπλεκόμενων φορέων δεν κρίνεται απαραίτητη
Μη Αποποίηση Ευθύνης	Μη απαραίτητο	Η μη αποποίηση ευθύνης δεν κρίνεται αναγκαία λόγω της φύσης της υπηρεσίας
Ανωνυμία Χρήστη	Μη απαραίτητο	Η διατήρηση της ανωνυμίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ιδιωτικότητα	Μη απαραίτητο	Η προστασία της ιδιωτικότητας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Ανίχνευση Τοποθεσίας Χρήστη	Μη απαραίτητο	Η ανίχνευση τοποθεσίας του χρήστη δεν είναι απαραίτητη λόγω της φύσης της υπηρεσίας
Παρακολούθηση Διαδικασιών	Επιθυμητό	Η καταγραφή των δραστηριοτήτων των χρηστών στο σύστημα είναι επιθυμητή για τον έλεγχο πιθανόν κακόβουλων ενεργειών

4.2.7.4 Συνολική Αξιολόγηση Υπηρεσιών

Στον πίνακα που ακολουθεί παρουσιάζεται συνοπτικά η αξιολόγηση βάσει κριτηρίων όλων των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης που πραγματοποιήθηκε παραπάνω. Όπως βλέπουμε, η Ηλεκτρονική Υγεία είναι η μία εκ των δύο υπηρεσιών Ηλεκτρονικής Διακυβέρνησης που παρουσιάζουν τη μεγαλύτερη αναγκαιότητα για την κάλυψη των περισσότερων απαιτήσεων ασφάλειας βάσει της αξιολόγησης που έγινε και, για το λόγο αυτό, αποτελεί μεγάλη πρόκληση όσον αφορά την αξιολόγηση της προσέγγισης που ακολουθείται στην παρούσα διδακτορική διατριβή.

Απαιτήσεις ασφάλειας / Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης		Αυθεντικοποίηση	Εμπιστευτικότητα	Ακεραιότητα	Εμπιστοσύνη	Μη αποποίηση ευθύνης	Ανωνυμία χρήστη	Ιδιωτικότητα	Ανίχνευση Τοποθεσίας Χρήστη	Παρακολούθηση διαδικασιών
G2B	Δημόσιες Προμήθειες	3	1	3	2	1	1	1	1	3
	Στατιστικές Υπηρεσίες	3	2	3	3	1	1	1	1	1
	Ηλεκτρονικό Τελωνείο	3	3	3	2	1	1	1	1	3
	Ηλεκτρονική Πολεοδομία	3	3	3	2	1	1	2	1	3
G2C	Ηλεκτρονική Υγεία	3	3	3	3	3	3	3	3	3
	Φορολογική εξυπηρέτηση	3	3	3	3	2	1	1	1	3
	Εύρεση Εργασίας	1	1	3	2	1	1	2	1	1
	Ηλεκτρονική Ψηφοφορία	3	3	3	3	1	3	3	1	3
	η-ΚΕΠ	3	1	3	3	1	1	3	1	2
	Κάρτα Αποδείξεων	1	1	3	1	1	3	3	1	2
	η-Παιδεία	3	1	1	1	1	1	1	1	2

Απαιτήσεις ασφάλειας / Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης		Αυθεντικοποίηση	Εμπιστευτικότητα	Ακεραιότητα	Εμπιστοσύνη	Μη αποποίηση ευθύνης	Ανωνυμία χρήστη	Ιδιωτικότητα	Ανίχνευση Τοποθεσίας Χρήστη	Παρακολούθηση διαδικασιών
G2G	Εθνικό Δημοτολόγιο	3	3	3	2	1	1	3	1	2
	Εθνικό Ληξιαρχείο	3	3	3	2	1	1	3	1	2
	Ελεγκτική Υπηρεσία	3	3	3	2	1	1	1	1	3

Επίπεδα αξιολόγησης απαίτησης: 3 – Αναγκαίο, 2 – Επιθυμητό, 1 – Μη απαραίτητο

4.3 Συνεργατικά Συστήματα Βασισμένα στο Διαδίκτυο των Πραγμάτων

Δεδομένης της ευρείας χρήσης έξυπνων κινητών τηλεφώνων (smartphones), κινητών συσκευών (π.χ. tablet), ενδυτών (wearables) και άλλων έξυπνων συσκευών που επιτρέπουν τη συνεχή συλλογή πολύτιμης πληροφορίας σχετικά με την υγεία του χρήστη, καθώς και την ψυχολογική-συναισθηματική και σωματική του ευημερία, τα παραδοσιακά συστήματα υγείας έχουν μετατραπεί σε ένα οικοσύστημα όπου η προσωπική παρακολούθηση της υγείας και της ευεξίας του ατόμου μπορεί να εξασφαλισθεί μέσω της ασφαλούς και άμεσης πρόσβασης στην Τηλεϊατρική (Telemedicine), στην Ηλεκτρονική Συνταγογράφηση (ePrescription), καθώς και μέσω της χρήσης Ηλεκτρονικών Φακέλων Υγείας (Electronic Health Records – EHR). Το νέο τοπίο στον τομέα του *Διαδικτύου των Πραγμάτων* (Internet of Things – IoT) προσφέρει το κατάλληλο έδαφος στο οποίο μπορεί να βασιστεί η υιοθέτηση ενός ασθενοκεντρικού μοντέλου όπου ο ασθενής αναλαμβάνει έναν πιο ενεργό ρόλο στην παρακολούθηση της υγείας του, επιτρέποντας, παράλληλα, αποτελεσματικότερη παροχή υπηρεσιών υγειονομικής περίθαλψης.

Παρ' όλα αυτά, ο δρόμος προς την ενσωμάτωση και τη διαλειτουργικότητα των τεχνολογιών *Υπολογιστικού Νέφους* (Cloud Computing) και του Διαδικτύου των Πραγμάτων με τις εφαρμογές και τις υπηρεσίες Ηλεκτρονικής Υγείας δημιουργεί προκλήσεις ως προς την παρεχόμενη ασφάλεια των τελευταίων. Είναι γεγονός ότι η ανησυχία που υπάρχει σχετικά με την προστασία της ιδιωτικότητας στα συστήματα

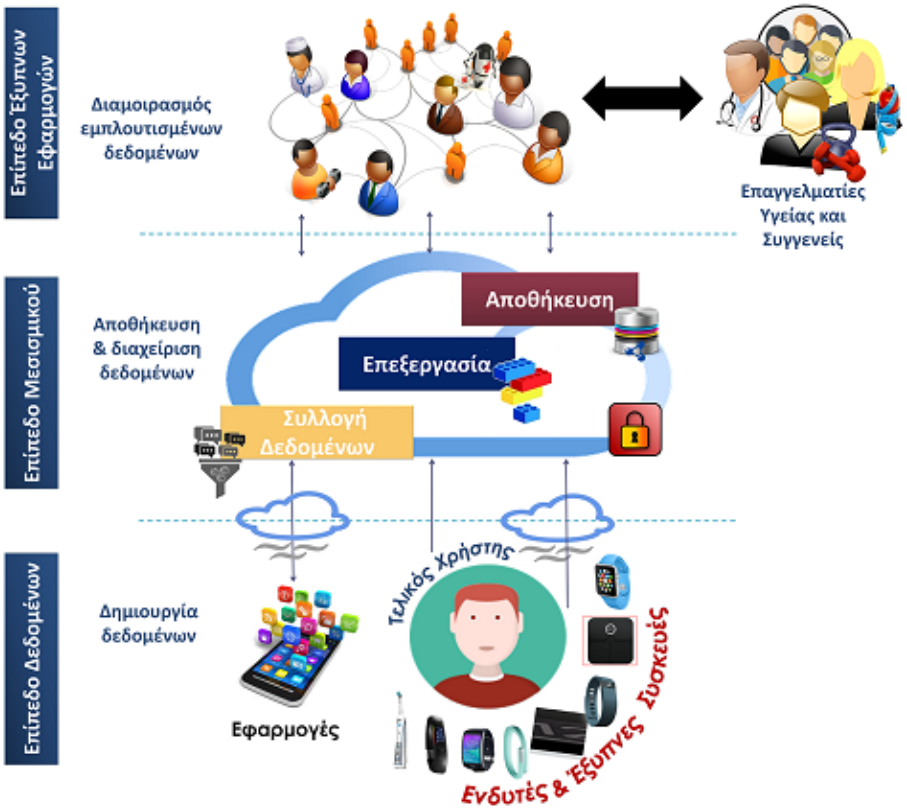
αυτά κατέχει εξέχουσα θέση μεταξύ των εμποδίων για την πλήρη μετάβαση στη *Συλλογική Υπολογιστική* (Collective Computing) [100] και στη νέα εποχή του τομέα της Υγειονομικής Περίθαλψης (Healthcare 3.0). Σε πρόσφατη αναφορά της Ευρωπαϊκής Επιτροπής με τίτλο "Απελευθερώνοντας την προοπτική ανάπτυξης των ΤΠΕ στην Ευρώπη: Ενεργοποιώντας τους ανθρώπους και τις επιχειρήσεις. Χρησιμοποιώντας σενάρια για τη δημιουργία μιας νέας περιγραφής του ρόλου των ΤΠΕ στην ανάπτυξη της Ευρώπης", στο σχετικό τμήμα που γίνεται αναφορά στις υπηρεσίες υγείας, οι λόγοι ανησυχίας που εντοπίζονται σχετίζονται με "την ιδιοκτησία και χρήση προσωπικών δεδομένων, την ιδιωτικότητα και την ασφάλεια, τη στάση ασθενών και επαγγελματιών στις νέες εξελίξεις και τη διαλειτουργικότητα των συστημάτων" [101]. Η ιδιωτικότητα και η εμπιστοσύνη των πολιτών σχετικά με τη χρήση ευαίσθητων προσωπικών τους δεδομένων, καθώς και τα αντίστοιχα νομικά ζητήματα που προκύπτουν πρέπει να λαμβάνονται υπόψη κατά τον σχεδιασμό και την ανάπτυξη οποιουδήποτε συστήματος ή υπηρεσίας που σχετίζεται με την Υγεία. Από την άλλη πλευρά, η συλλογή και επεξεργασία βιομετρικών δεδομένων και δεικτών ευημερίας μπορεί να οδηγήσει σε προηγμένα εργαλεία για εξατομικευμένη παρακολούθηση και, επομένως, βελτίωση των συνθηκών διαβίωσης και της ποιότητας ζωής του ατόμου.

Για την κάλυψη των δύο αυτών αναγκών (βελτιωμένη ποιότητα των παρεχόμενων υπηρεσιών υγείας και συμμόρφωση με το κανονιστικό πλαίσιο για την προστασία της ιδιωτικότητας) από τον σχεδιασμό κιόλας υπηρεσιών Ηλεκτρονικής Υγείας, είναι απαραίτητο να υιοθετηθούν λύσεις που περιλαμβάνουν μηχανισμούς ασφαλούς διαχείρισης δεδομένων για την προστασία ευαίσθητων και ταυτοποιητικών προσωπικών στοιχείων. Μία ακόμη πρόκληση στον σχεδιασμό και στην παροχή υπηρεσιών Ηλεκτρονικής Υγείας αποτελούν, επίσης, η ετερογένεια και η ποικιλία των συσκευών και των τεχνολογιών που χρησιμοποιούνται για την παρακολούθηση της κατάστασης της υγείας του ατόμου. Πέραν αυτού, πρέπει να ληφθεί υπόψη και ο αριθμός των εμπλεκόμενων οντοτήτων και των, είτε άμεσα είτε έμμεσα, ενδιαφερομένων (βλ. νοσοκομεία, ιατροί, ασφαλιστικοί οργανισμοί, φαρμακοποιοί), όπου ο κάθε ένας από τους προαναφθέντες επιτρέπεται να έχει πρόσβαση σε διαφορετικών ειδών δεδομένα, βάσει των αντίστοιχων πολιτικών πρόσβασης.

Ξεκινώντας από τη σύντομη ανάλυση που παρουσιάστηκε στις προηγούμενες παραγράφους, στην ενότητα αυτή, βασιζόμενοι στην ιδέα ενός *Εικονικού Προφίλ για την Υγεία* (Health Avatar) [102], το οποίο συνιστά ένα σύστημα παρακολούθησης της υγείας και της ευεξίας του ατόμου ενσωματώνοντας δεδομένα που συλλέγονται από προσωπικές έξυπνες και ενδυτές συσκευές, στις επόμενες ενότητες εξετάζονται και παρουσιάζονται πτυχές που σχετίζονται με την ασφάλεια, την προστασία των δεδομένων και την ιδιωτικότητα κατά την υιοθέτηση τέτοιων λύσεων στον τομέα της Υγείας. Η αξιοπιστία του συστήματος, επιπλέον της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των σημαντικών δεδομένων που μεταδίδονται και υποβάλλονται σε επεξεργασία σε ένα τέτοιο σύστημα πρέπει να διασφαλίζονται.

4.3.1 Συνεργατικό Περιβάλλον Διαχείρισης Δεδομένων Υγείας και Δεικτών Ευημερίας

Έπειτα από μελέτη πολλών υπαρχόντων συστημάτων και υπηρεσιών που παρέχονται σε διάφορους τομείς (βλ. Ενότητα 4.2.7), λαμβάνοντας υπόψη ότι κάθε μία από αυτές τις υπηρεσίες έχει τις δικές της ιδιαιτερότητες και τα δικά της χαρακτηριστικά, για την επιλογή ενός σεναρίου προς εξέταση προκειμένου να αξιολογηθεί η ενσωμάτωση της τεχνολογίας blockchain σε μια ολιστική αρχιτεκτονική ασφαλούς συστήματος με επίγνωση της ιδιωτικότητας, επιλέχθηκε ένα σύστημα παρακολούθησης της υγείας που βασίζεται στο Διαδίκτυο των Πραγμάτων, και συγκεκριμένα το *Health Avatar* [103]. Ειδικότερα, το Health Avatar αποδείχτηκε ως ένα από τα πιο απαιτητικά σενάρια ως προς την ικανοποίηση των απαιτήσεων ασφάλειας και προστασίας της ιδιωτικότητας, καλύπτοντας το μέγιστο εύρος αυτών, συμπεριλαμβανομένων του Ελέγχου Ταυτότητας (Authentication), της Εμπιστευτικότητας (Data Confidentiality) και της Ακεραιότητας (Data Integrity) των δεδομένων, της Εμπιστοσύνης (Trust), της Μη Αποποίησης Ευθύνης (Non-repudation), της Ανωνυμίας του Χρήστη (User Anonymity), της Ιδιωτικότητας (Privacy), καθώς και της Ανίχνευσης της Τοποθεσίας του (User Location Traceability) και του Ελέγχου και της Παρακολούθησης των Υποκείμενων Διαδικασιών (Auditability).



Σχήμα 8: Επισκόπηση του Οικοσυστήματος Health Avatar

Ουσιαστικά, η πλατφόρμα του Health Avatar προσφέρει ένα σημείο συγκέντρωσης ποικίλων δεδομένων, στο οποίο πραγματοποιείται συλλογή και αναζήτηση πληροφορίας σχετικής με την υγεία και την ευημερία του ατόμου [104]. Συγκεκριμένα, το σημείο αυτό είναι υπεύθυνο για τη συλλογή δεδομένων από αισθητήρες, για τον έλεγχο των δεδομένων αυτών βάσει εσωτερικής λογικής και κανόνων, καθώς και για τη μεταφορά τους στην κύρια πλατφόρμα, όπου ακολουθεί η περαιτέρω επεξεργασία αυτών και η μετατροπή τους σε εμπλουτισμένα δεδομένα ευημερίας. Απώτερος σκοπός είναι να καταστεί δυνατή η συλλογή, ενσωμάτωση και συγχώνευση των δεδομένων όλων των συσκευών στην πλατφόρμα του Health Avatar, στην οποία και θα αποθηκεύονται όλα σε ένα κοινό αποθετήριο και θα τίθενται υπό επεξεργασία με τρόπο συνδυαστικό. Δεδομένου ότι οι τελικοί χρήστες του συστήματος χρησιμοποιούν σε καθημερινή βάση ενδυτές αισθητήριες συσκευές, οι τελευταίες πραγματοποιούν τακτικές μετρήσεις και, έτσι, δίνεται η δυνατότητα μέσω του συστήματος αυτού να συγχρονίζονται τα δεδομένα αυτά αυτόματα με ιατρικά αρχεία που διατηρούνται σε αρμόδιους φορείς, ενθαρρύνοντας με τον τρόπο αυτό την αφοσίωση των επαγγελματιών υγείας στην παρακολούθηση του ατόμου και τη μεγαλύτερη ευαισθητοποίησή τους σχετικά με πραγματικού χρόνου διακυμάνσεις ή αναμενόμενες αλλαγές στη φυσική, κοινωνική, ψυχική ή πνευματική ευημερία.

Όπως φαίνεται στο Σχήμα 8, η πλατφόρμα του Health Avatar βασίζεται σε μία αρχιτεκτονική τριών επιπέδων. Ακολουθώντας την προσέγγιση "από κάτω προς τα επάνω", το πρώτο επίπεδο, δηλαδή το *Επίπεδο Δεδομένων*, συνίσταται από ένα σύνολο αντικειμένων που περιλαμβάνει πολλαπλές ετερογενείς οντότητες, όπως ενδυτές και έξυπνες συσκευές, αισθητήρες, καθώς και έξυπνες εφαρμογές κινητών τηλεφώνων, οι οποίες συγκεντρώνουν πληροφορία σχετική με τα βιομετρικά δεδομένα του χρήστη, τις καθημερινές δραστηριότητές του και τις συνήθειές του. Τα προαναφερθέντα δεδομένα συλλέγονται και συγκεντρώνονται από τις επιμέρους οντότητες του *Επιπέδου Μεσισμικού*. Σε αυτό το επίπεδο, αξιοποιώντας τις δυνατότητες που προσφέρονται από τις τεχνολογίες Υπολογιστικού Νέφους και Ομιχλώδους Υπολογισμού (Fog Computing), υπάρχουν οντότητες λογισμικού και μικροϋπηρεσίες (microservices) που είναι υπεύθυνες για: (α) τον μετασχηματισμό των συλλεχθέντων δεδομένων σύμφωνα με ένα κοινό σχήμα που επιλύει σημασιολογικές διαφορές μεταξύ διαφόρων τύπων δεδομένων σχετικών με την υγεία, καθώς και (β) την περαιτέρω επεξεργασία των δεδομένων, ώστε να προβλεφθεί η κατάσταση της υγείας του χρήστη βάσει παρατηρήσεων. Τέλος, το *Επίπεδο Έξυπνων Εφαρμογών* αποτελεί το τελευταίο επίπεδο της πλατφόρμας, μέσω του οποίου προσφέρονται στον τελικό χρήστη διάφορες εξατομικευμένες εφαρμογές και εργαλεία που συμβάλλουν στον έλεγχο του τρόπου ζωής του. Επιπλέον, η παρεχόμενη λειτουργικότητα του κοινωνικού δικτύου, όπου η έννοια του Avatar χρησιμοποιείται ως εικονική αναπαράσταση ενός ανθρώπου και φέρει το προφίλ του, ενισχύει την παρακολούθηση της ευεξίας του ατόμου και συμβάλλει στην κατεύθυνση της τηλεϊατρικής μέσω της κοινοποίησης

των δεδομένων του χρήστη με τρόπο ασφαλή και με επίγνωση της ιδιωτικότητάς του σε επαγγελματίες υγείας και ειδικούς, όπως σε γιατρούς, διαιτολόγους, γυμναστές, φροντιστές ή και μέλη της οικογένειάς του.

Όπως αναφέρεται στο [103] όπου περιγράφεται λεπτομερώς όλο το σύστημα και τα υποσυστήματα αυτού, η πλατφόρμα Health Avatar έχει σχεδιαστεί έχοντας υπόψη τις εξής τρεις κατευθύνσεις: (α) τη δυνατότητα εύκολης σύνδεσης και ενσωμάτωσης υφιστάμενων αλλά και μελλοντικών συστημάτων εξατομικευμένης παρακολούθησης της υγείας, εργαλείων, μεμονωμένων συσκευών, όπως φορητές συσκευές που παρακολουθούν ειδικές συνθήκες διαβίωσης και παραμέτρους όπως καύση θερμίδων, καθώς και λύσεων μεσισμικού ικανών να υποστηρίζουν τη διαχείριση ολοκληρωμένων ηλεκτρονικών φακέλων υγείας· (β) την ανάγκη να πραγματοποιείται συλλογή, επεξεργασία και ανάλυση των δεδομένων που σχετίζονται με τις συνήθειες, την καθημερινότητα και την υγεία του ατόμου, ενώ θα πρέπει, επίσης, να είναι δυνατή η αποτελεσματική διαχείριση της παραγόμενης - έπειτα από την προαναφερθείσα επεξεργασία - πληροφορίας σε μια προτυποποιημένη μορφή· (γ) τη δυνατότητα εύκολης επέκτασης της συνδεσιμότητας της πλατφόρμας που παρουσιάστηκε και της διασύνδεσής της με άλλες παρόμοιες πλατφόρμες, αξιοποιώντας με τον τρόπο αυτό τις δυνατότητες υφιστάμενων συστημάτων υποστήριξης αποφάσεων για την υγεία, επιτρέποντας παράλληλα στους επαγγελματίες και στους ειδικούς να τη χρησιμοποιούν και να αξιοποιούν πλήρως τις δυνατότητες αυτής μέσω κατάλληλων διεπαφών.

Λαμβάνοντας υπόψη τις προαναφερθείσες τρεις κατευθύνσεις και λόγω της ευαίσθητης φύσης των δεδομένων που συλλέγονται από τους διάφορους αισθητήρες και τις συσκευές που συνδέονται με την πλατφόρμα μέσω της χρήσης ποικίλων τεχνολογιών, κρίνεται απαραίτητη η χρήση και εφαρμογή τρεχουσών πρακτικών ασφάλειας, ώστε να διασφαλιστεί η αξιοπιστία του συστήματος, πέρα από την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των σημαντικών δεδομένων που συλλέγονται, επεξεργάζονται και αποθηκεύονται στο εν λόγω σύστημα. Έτσι, η γενική προσωποκεντρική αρχιτεκτονική του συστήματος ασφάλειας πρέπει να σχεδιαστεί κατά τρόπο τέτοιο που να ακολουθεί την προσέγγιση "ασφάλεια και προστασία της ιδιωτικότητας από το σχεδιασμό" [105]. Ένα σημαντικό ζήτημα, κάθετο προς τις λειτουργίες που προσφέρει η πλατφόρμα Health Avatar, είναι η αντιστάθμιση (trade-off) της ανάγκης για εξατομικευμένες υπηρεσίες υψηλής ποιότητας και της προστασίας της ιδιωτικότητας των χρηστών, δεδομένου ότι τα ευαίσθητα βιομετρικά δεδομένα αυτών πρέπει να προστατεύονται από τυχόν μη επιτρεπτή δημοσιοποίηση, ενώ παράλληλα πρέπει να παραμένουν χρήσιμα για οποιαδήποτε περαιτέρω επεξεργασία. Η κατάλληλη αποθήκευση, διατήρηση και επεξεργασία των συλλεγόμενων δεδομένων προσωπικού χαρακτήρα (είτε αυτά βρίσκονται στην αρχική, πρωτογενή τους μορφή είτε σε μία μορφή εμπλουτισμένη) δεν θεωρούνται τετριμμένες ως διαδικασίες, καθώς μπορεί να καταστεί δυνατή η μη θεμιτή εξαγωγή συμπε-

ρασμάτων σε περίπτωση πρόσβασης τρίτου στα δεδομένα αυτά.

Επιπλέον, ένας από τους πιο αναμενόμενους και άμεσους αντίκτυπους μιας τέτοιας πλατφόρμας είναι η αύξηση της εμπιστοσύνης των χρηστών στην τεχνολογία και στις προσφερόμενες υπηρεσίες. Λόγω της ευαίσθητης φύσης των δεδομένων σχετικών με την υγεία και λαμβάνοντας υπόψη την πιθανότητα έμμεσης εισβολής στην ιδιωτική ζωή των ανθρώπων σε περίπτωση διαρροής δεδομένων, οι χρήστες είναι συνήθως επιρρεπείς στην πλήρη απόρριψη της τεχνολογίας. Ως εκ τούτου, κύριος στόχος κατά την εφαρμογή μηχανισμών ασφάλειας και προστασίας της ιδιωτικότητας πρέπει να είναι η παροχή τεχνικών λύσεων σε ένα μέχρι σήμερα αποκλειστικά ρυθμιστικό και νομοθετικό ζήτημα, δηλαδή την προστασία των προσωπικών δεδομένων των χρηστών, προσφέροντας έναν διαφανή τρόπο διαχείρισης ταυτοτήτων και ρόλων των οντοτήτων της πλατφόρμας, καθώς και τα κατάλληλα εργαλεία για τη διαχείριση και την παρακολούθηση των υποκείμενων διαδικασιών επεξεργασίας και ανταλλαγής των προσωπικών δεδομένων των χρηστών από τους ίδιους.

Για τον σχεδιασμό της γενικής αρχιτεκτονικής του συστήματος ασφάλειας της πλατφόρμας με τρόπο τέτοιο που πληροί όλες τις προαναφερθείσες ειδικές απαιτήσεις της υποδομής και θεωρώντας τη φυσική ασφάλεια και την προστασία ολόκληρης της υποδομής από τυχόν καταστροφή της από φυσικά φαινόμενα ή από μη εξουσιοδοτημένη πρόσβαση κάποιου ατόμου δεδομένες, η έρευνα που πραγματοποιήθηκε επικεντρώθηκε στο Επίπεδο Μεσισμικού, λαμβάνοντας υπόψη την κρίσιμη φύση των δεδομένων που συλλέγονται από τις έξυπνες συσκευές σε συνδυασμό με την ποικιλομορφία των φορέων που εμπλέκονται στο υποκείμενο Διαδίκτυο των Πραγμάτων.

Κεφάλαιο 5

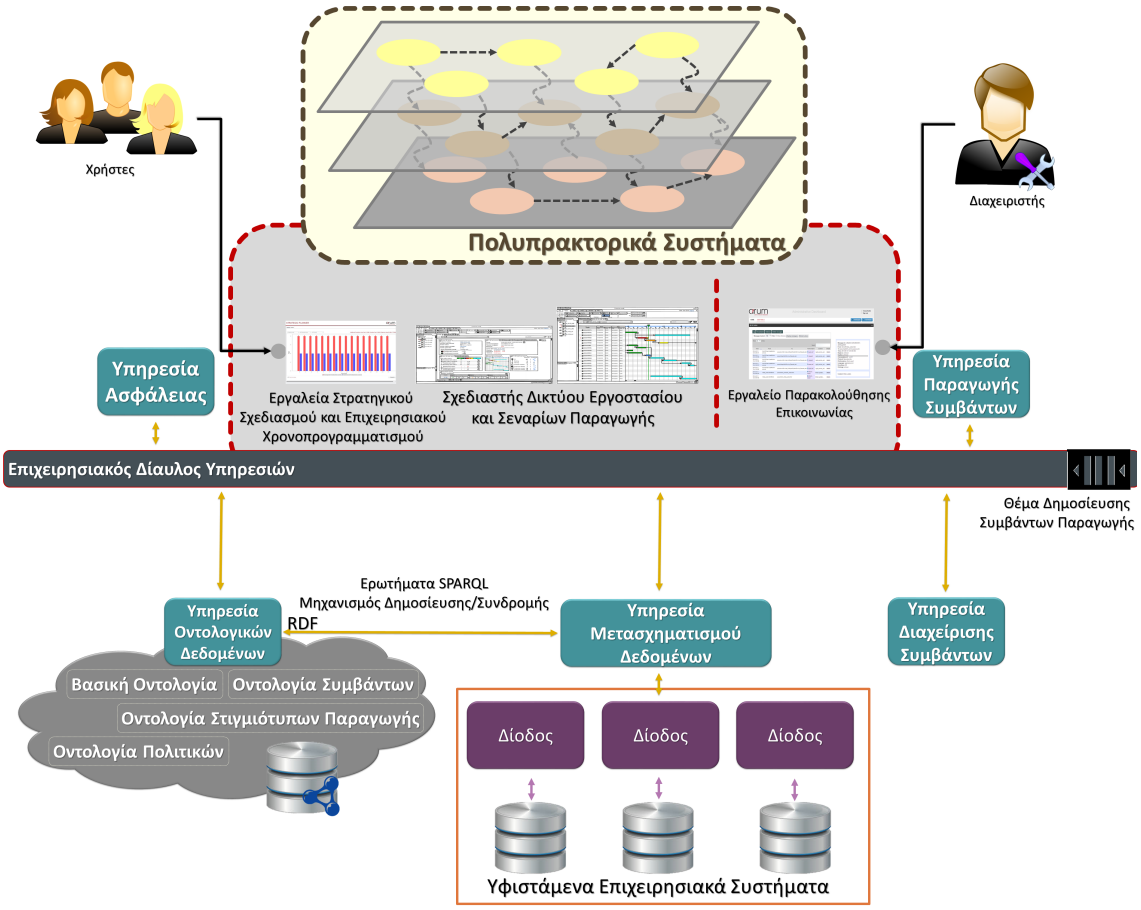
Εφαρμογή Αρχιτεκτονικής Ασφαλούς Συστήματος για τη Διασφάλιση Ιδιωτικότητας σε Ετερογενή Κατανεμημένα Περιβάλλοντα

5.1 Εφαρμογή σε Συνεργατικό Περιβάλλον Διαχείρισης Παραγωγής

5.1.1 Επισκόπηση του Συστήματος

Για την αντιμετώπιση των νέων προκλήσεων κατά την παραγωγή πολύπλοκων και ιδιαίτερα εξατομικευμένων προϊόντων, όπως αεροσκαφών και προϊόντων ναυπηγικών βιομηχανιών, το κυβερνοφυσικό σύστημα διαχείρισης παραγωγής, στο οποίο εφαρμόστηκε η ευφυής υπηρεσία ασφάλειας και προστασίας δεδομένων που παρουσιάζεται στην παρούσα διδακτορική διατριβή, υιοθετεί στραγητικές για την ταχύτερη ανταπόκριση σε μη αναμενόμενα γεγονότα, μέσω της χρήσης εργαλείων υποστήριξης αποφάσεων κατά τον σχεδιασμό και την εκτέλεση διαδικασιών παραγωγής [106][107]. Συγκεκριμένα, η προαναφερθείσα πλατφόρμα διαχείρισης παραγωγής ενσωματώνει έναν ευφυή Επιχειρησιακό Δίαυλο Υπηρεσιών (intelligent Enterprise Service Bus – iESB), όπου ο παραδοσιακός δίαυλος ESB εμπλουτίζεται με πληθώρα προηγμένων οντοτήτων, όπως είναι η Υπηρεσία Οντολογικών Δεδομένων (Ontology Service), η Μηχανή Μετασχηματισμού Δεδομένων (Data Transformation Engine), το Εργαλείο Ανίχνευσης Επικοινωνίας (Sniffer), η Υπηρεσία Διαχείρισης Κόμ-

βων (Node Management) και η Υπηρεσία Διαχείρισης Κύκλου Ζωής (Lifecycle Management). Ο δίαυλος iESB παρέχει μια κοινή υποδομή για την ενσωμάτωση ετερογενών εργαλείων σχεδιασμού και προγραμματισμού της γραμμής παραγωγής και υφιστάμενων επιχειρησιακών συστημάτων, όπως απεικονίζεται στο Σχήμα 9.



Σχήμα 9: Η Αρχιτεκτονική του Συστήματος Διαχείρισης Παραγωγής

Στην υποδομή αυτή, διαλειτουργούν διάφορα εργαλεία σχεδιασμού και προγραμματισμού, όπως το Εργαλείο Επιχειρησιακού Χρονοπρογραμματισμού (Operational Scheduler) για το βραχυπρόθεσμο σχεδιασμό της παραγωγής και την άμεση επίλυση προβλημάτων και το Εργαλείο Στρατηγικού Σχεδιασμού (Strategic Planner) για το σχεδιασμό της παραγωγής και την κατανομή πόρων με τρόπο τέτοιο ώστε μελλοντικά να αυξηθούν οι τιμές των Βασικών Δεικτών Απόδοσης (Key Performance Indicators – KPIs). Η δυνατότητα ενσωμάτωσης των εργαλείων αυτών διευκολύνεται από την παροχή των επιμέρους λειτουργιών τους με τη μορφή υπηρεσιών και τη χρήση υπηρεσιών διαχείρισης οντολογικών δεδομένων για την αναπαράσταση της γνώσης, βελτιώνοντας με τον τρόπο αυτό τη διαλειτουργικότητα των επιμέρους οντοτήτων του συγκεκριμένου κατανεμημένου και ετερογενούς συστήματος.

Βασικές οντότητες της παραπάνω πλατφόρμας διαχείρισης παραγωγής, όπως τα δύο προαναφερθέντα εργαλεία, υιοθετούν την τεχνολογία των πολυπρακτορι-

κών συστημάτων, σύμφωνα πάντα με τις προδιαγραφές του προτύπου FIPA και τα μοντέλα διαλειτουργικότητας και διαπραγμάτευσης μεταξύ πρακτόρων, καθώς και μεταξύ πολλαπλών πολυπρακτορικών συστημάτων χρονοπρογραμματισμού [108]. Επιπλέον, η μορφή των μηνυμάτων που ανταλλάσσονται μεταξύ των οντοτήτων της πλατφόρμας είναι σύμφωνη με το πρωτόκολλο αλληλεπίδρασης FIPA. Δεδομένου ότι η συγκεκριμένη πλατφόρμα ακολουθεί την προσέγγιση της υπηρεσιοστρεφούς αρχιτεκτονικής, μέσω της χρήσης και ενσωμάτωσης των πρωτοκόλλων αλληλεπίδρασης FIPA προσφέρεται ένας μηχανισμός επικοινωνίας ανάλογος της δυναμικής του συστήματος, όπως, για παράδειγμα, για την επικοινωνία ετερογενών εργαλείων χρονοπρογραμματισμού που συνεργάζονται μεταξύ τους. Με αυτόν τον τρόπο, τα προαναφερθέντα εργαλεία μπορούν να αλληλεπιδρούν μεταξύ τους χρησιμοποιώντας τα ήδη γνωστά πρωτόκολλα διαπραγμάτευσης που αναπτύχθηκαν στο πλαίσιο του FIPA.

Καθώς η συγκεκριμένη πλατφόρμα ακολουθεί μια οντολογική προσέγγιση για την επίτευξη των επιχειρησιακών της στόχων, εκτός από τη συμμόρφωση με τα διεθνή πρότυπα, π.χ. τη γλώσσα σημασιολογικού ιστού OWL, η χρήση του πλαισίου περιγραφής πόρων RDF εγγυάται την ορθή ανταλλαγή πληροφοριών μεταξύ εργαλείων ή πρόσβασης δεδομένων αποθηκευμένων σε υφιστάμενα συστήματα [109]. Για τη σημασιολογική αναπαράσταση και περιγραφή των δεδομένων σχετικά με τις διακριτές διαδικασίες παραγωγής, τα πραγματικά και εναλλακτικά στιγμιότυπα της γραμμής παραγωγής, τα δεδομένα αισθητήρων που συλλέγονται κατά τη διάρκεια των διαδικασιών συναρμολόγησης των προϊόντων, τυχόν συμβάντα και οι πολιτικές ελέγχου πρόσβασης βάσει ιδιοτήτων για τη λήψη αποφάσεων εξουσιοδότησης χρησιμοποιούνται τα αντίστοιχα οντολογικά μοντέλα πληροφορίας [110]. Επιπλέον, ένα API βασισμένο στο πρότυπο REST, το οποίο είναι προσβάσιμο μόνο μέσω του πρωτοκόλλου HTTPS, χρησιμοποιείται ως ο μοναδικός τρόπος ασφαλούς πρόσβασης των γραφικών περιβαλλόντων των διεπαφών χρηστών στα δεδομένα.

Η διασύνδεση και η εξασφάλιση συμβατότητας με τα υφιστάμενα επιχειρησιακά συστήματα που χρησιμοποιούνται στις διαδικασίες παραγωγής, όπως συστήματα Προγραμματισμού Επιχειρησιακών Πόρων (Enterprise Resource Planning – ERP), Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (Supervisory Control And Data Acquisition – SCADA) καθώς και Διαχείρισης Σχέσεων Πελατών (Customer Relationship Management – CRM), είναι ιδιαίτερα σημαντικές. Έχοντας αυτό υπόψη, είναι απαραίτητο σε μία πλατφόρμα σαν τη συγκεκριμένη που παρουσιάζεται στην ενότητα αυτή να επιδιώκεται συμμόρφωση με τα πρότυπα που αφορούν τον βιομηχανικό αυτοματισμό και τη διαλειτουργικότητα και την επικοινωνία των επιχειρήσεων. Η καινοτομία της πλατφόρμας διαχείρισης παραγωγής έγκειται στις εξής δύο προσεγγίσεις: (α) στη χρήση τεχνολογιών σημασιολογικού ιστού για την περιγραφή των παρεχόμενων λειτουργιών από τις υπηρεσίες της και (β) στον συνδυασμό εργαλείου μετασχηματισμού δεδομένων που συλλέγονται από υφιστάμενα επιχειρησιακά συστήματα με

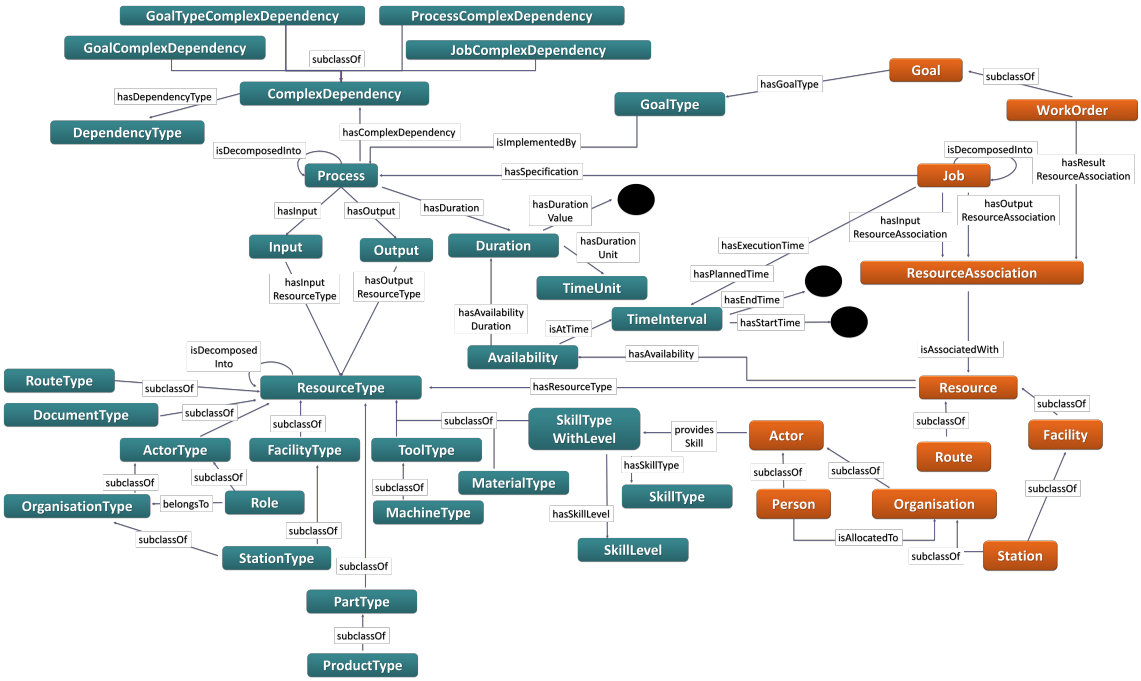
οντολογικά μοντέλα, επιτρέποντας με τον τρόπο αυτό την απρόσκοπτη πρόσβαση στα δεδομένα από τα επιμέρους εργαλεία και τις υπηρεσίες της πλατφόρμας με διαφανή τρόπο [111][112].

Όσον αφορά στον βιομηχανικό αυτοματισμό, σύμφωνα με το πρότυπο ANSI / ISA95, η συγκεκριμένη πλατφόρμα διαχείρισης παραγωγής αντιμετωπίζει τη διαλειτουργικότητα στο Επίπεδο 3, όπου βρίσκεται το δίκτυο των πρακτόρων, καθώς και στο Επίπεδο 4, υποστηρίζοντας την ενσωμάτωση υφιστάμενων συστημάτων. Η χρήση και τήρηση προτύπων που σχετίζονται με τα προαναφερθέντα επίπεδα και τις βιομηχανικές διαδικασίες γενικά είναι αναγκαία, συμπεριλαμβανομένων του IEC/ISO 62264 για την ολοκλήρωση των συστημάτων ελέγχου των επιχειρήσεων, του ISO/IEC 15288 σχετικά με τη διαχείριση του κύκλου ζωής της παραγωγής, καθώς και του ISO 15531 για τη διαχείριση της ανταλλαγής δεδομένων παραγωγής.

5.1.2 Σημασιολογικά Μοντέλα Πληροφορίας

Τα δεδομένα που είναι απαραίτητα από τα εργαλεία και τις υπηρεσίες της πλατφόρμας για τη βελτίωση των διαδικασιών παραγωγής και την έγκαιρη αντιμετώπιση μη αναμενόμενων συμβάντων είναι συνήθως διασκορπισμένα σε ετερογενείς πηγές δεδομένων, οι οποίες διατηρούνται και διαχειρίζονται από εταιρείες. Για την επίτευξη των στόχων τους, οι υπηρεσίες του συστήματος απαιτούν την επεξεργασία των ετερογενών αυτών δεδομένων συνδυαστικά. Ως εκ τούτου, η ετερογένεια των δεδομένων και η κατανεμημένη φύση τους γεννούν την ανάγκη μηχανισμών, οι οποίοι παρέχουν διαφανή πρόσβαση στην πληροφορία. Η ομοιογένεια των δεδομένων παραγωγής επιτυγχάνεται με τη χρήση οντολογιών και με την εκμετάλλευση των λειτουργιών της ευφυούς Υπηρεσίας Οντολογικών Δεδομένων.

Τα δεδομένα της πλατφόρμας μοντελοποιούνται σύμφωνα με το σχήμα τεσσάρων οντολογιών, με την κάθε μία να ορίζει έννοιες σχετικές με την παραγωγή. Η Βασική Οντολογία (Core Ontology) παρέχει τη σημασιολογική περιγραφή των κύριων εννοιών του τομέα της παραγωγής, όπως είναι οι Διαδικασίες (Processes) και οι Πόροι (Resources). Η Οντολογία Στιγμιότυπων Παραγωγής (Scene Ontology) μοντελοποιεί στιγμιότυπα της τρέχουσας κατάστασης της παραγωγής. Η Οντολογία Συμβάντων (Events Ontology) ορίζει έννοιες σχετικές με τα συμβάντα που ενδέχεται να προκύψουν σε ένα σύστημα παραγωγής, είτε είναι αναμενόμενα, όπως είναι η εκκίνηση ή ο τερματισμός μίας εργασίας, είτε μη αναμενόμενα, όπως είναι η έλλειψη ενός πόρου ή η μη συμμόρφωση ενός προϊόντος στη μορφή, η οποία του δόθηκε κατά το σχεδιασμό του. Τέλος, η Οντολογία Πολιτικών (Policy Model Ontology) προσδιορίζει κανόνες ελέγχου πρόσβασης, διασφαλίζοντας την ασφάλεια της πλατφόρμας σε ό,τι αφορά την εσωτερική επικοινωνία και την πρόσβαση σε συγκεκριμένες υπηρεσίες.

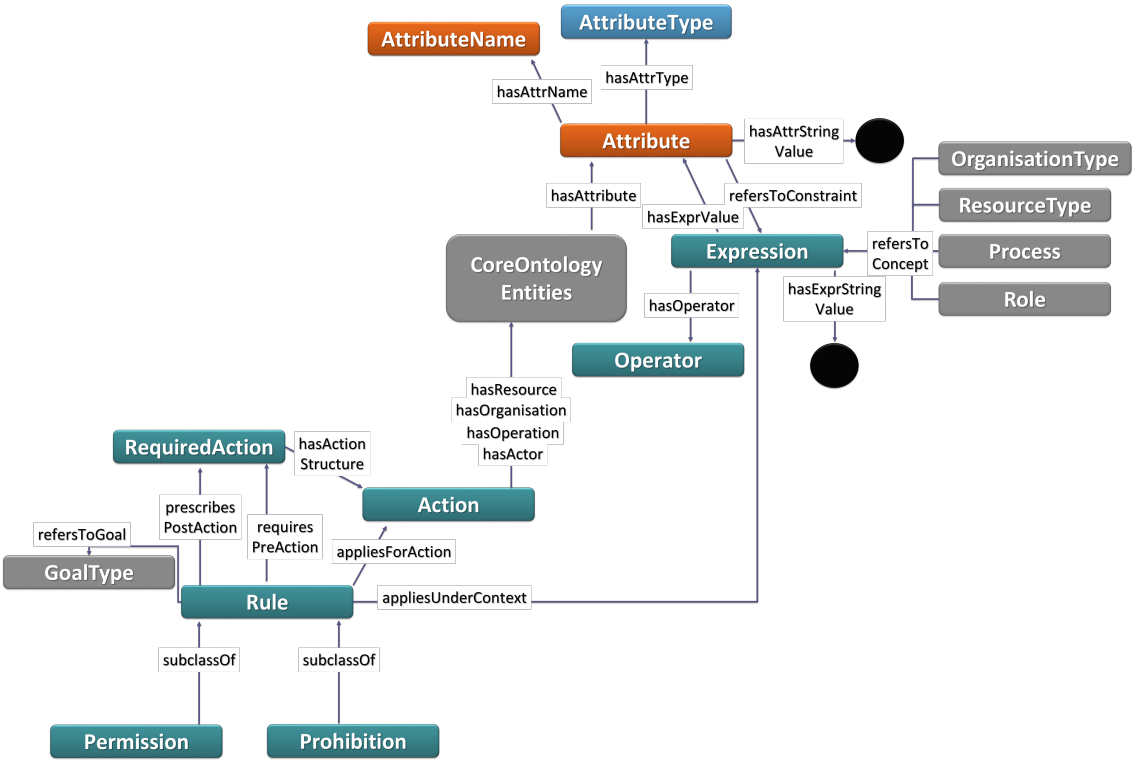


Σχήμα 10: Η Βασική Οντολογία του Συστήματος Διαχείρισης Παραγωγής

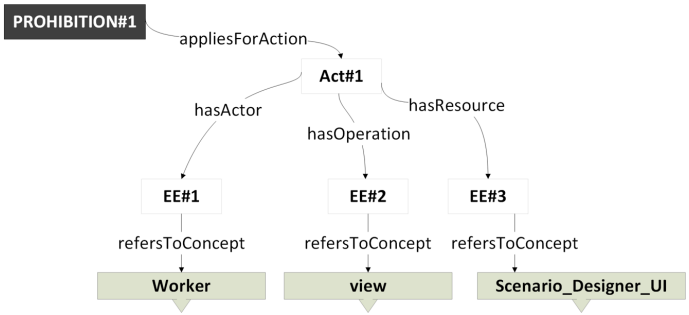
5.1.2.1 Οντολογία Πολιτικών

Η Οντολογία Πολιτικών χρησιμοποιείται στο πλαίσιο της δημιουργίας κανόνων ελέγχου πρόσβασης. Στη συνέχεια, οι κανόνες αυτοί χρησιμοποιούνται από την Υπηρεσία Ασφάλειας κατά την άφιξη αιτήσεων για πόρους (υπηρεσίες ή δεδομένα) του συστήματος από υπηρεσίες της πλατφόρμας.

Οι κανόνες ελέγχου πρόσβασης στους πόρους της ευφυούς πλατφόρμας ορίζονται με βάση τα χαρακτηριστικά των εμπλεκόμενων οντοτήτων, τις παραμέτρους πλαισίου, όπως είναι ο χρόνος ή ο χώρος, ή βάσει πιθανών συμβάντων ή προαπαιτούμενων ή επακόλουθων δράσεων, όπως είναι η διατήρηση αρχείων καταγραφής. Ως εκ τούτου, ένας κανόνας ελέγχου πρόσβασης μοντελοποιείται μέσω της κλάσης των Κανόνων (Rule) ή μέσω των εξειδικεύσεών της, της Άδειας (Permission) και της Απαγόρευσης (Prohibition). Χαρακτηρίζεται από μία Κατάσταση (State), η οποία ορίζει εάν ο κανόνας βρίσκεται σε ισχύ. Κάθε τέτοιος κανόνας ισχύει για μία Δράση (Action), η οποία επιτρέπει ή απαγορεύει σε ένα Συμμετέχοντα (Actor), δηλαδή αιτούντα πρόσβασης, να πραγματοποιήσει μία Πράξη (Operation), όπως είναι η προβολή, η επεξεργασία ή η εκτέλεση, πάνω σε έναν Πόρο (Resource). Οι προαναφερθείσες έννοιες του Συμμετέχοντα, της Πράξης και του Πόρου μοντελοποιούνται με τη χρήση εννοιών της Βασικής Οντολογίας, η οποία μοντελοποιεί γνώση σχετική με τον τομέα της παραγωγής. Το πλαίσιο υπό το οποίο εφαρμόζεται ένας κανόνας, όπως είναι οι εργάσιμες ώρες ή πιθανά συμβάντα, μοντελοποιείται μέσω της κλάσης των Εκφράσεων (Expression). Η κλάση αυτή συνδέεται με μία από τις έννοιες Κατηγορίας



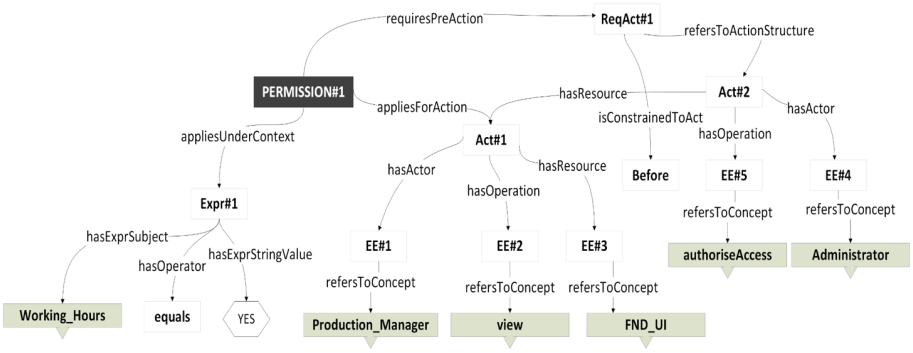
Σχήμα 11: Η Οντολογία Πολιτικών για το Σύστημα Διαχείρισης Παραγωγής



Σχήμα 12: Παράδειγμα 1: Σημασιολογική Αναπαράσταση Πολιτικής Απαγόρευσης

Πόρων, Διαδικασίας, Ρόλου ή Κατηγορίας Οργανισμών της Βασικής Οντολογίας και μπορεί να περιέχει κάποιον Τελεστή (Operator) και μία τιμή. Τέλος, ο στόχος ενός κανόνα παρέχεται μέσω της κλάσης Κατηγορίας Στόχων της Βασικής Οντολογίας.

Στα στιγμιότυπα των κλάσεων της Βασικής Οντολογίας ανατίθενται Χαρακτηριστικά (Attributes), με βάση τα οποία πραγματοποιείται ο έλεγχος πρόσβασης. Τα είδη και τα ονόματα των χαρακτηριστικών των Συμμετεχόντων και των Πόρων μοντελοποιούνται μέσω των κλάσεων Κατηγορία Χαρακτηριστικών (AttributeType) και Όνομα Χαρακτηριστικών (AttributeName), ενώ οι πιθανές τιμές των στιγμιότυπων τους δίνονται μέσω του αντίστοιχου τύπου δεδομένων (hasAttrValue). Χαρακτηριστικά που είναι δυνατό να ανατεθούν σε ένα Συμμετέχοντα αφορούν συνήθως στο ρόλο του, στους οργανισμούς που μπορεί να ανήκει ή στο σταθμό, στον οποίο ερ-



Σχήμα 13: Παράδειγμα 2: Σημασιολογική Αναπαράσταση Πολιτικής Εξουσιοδότησης

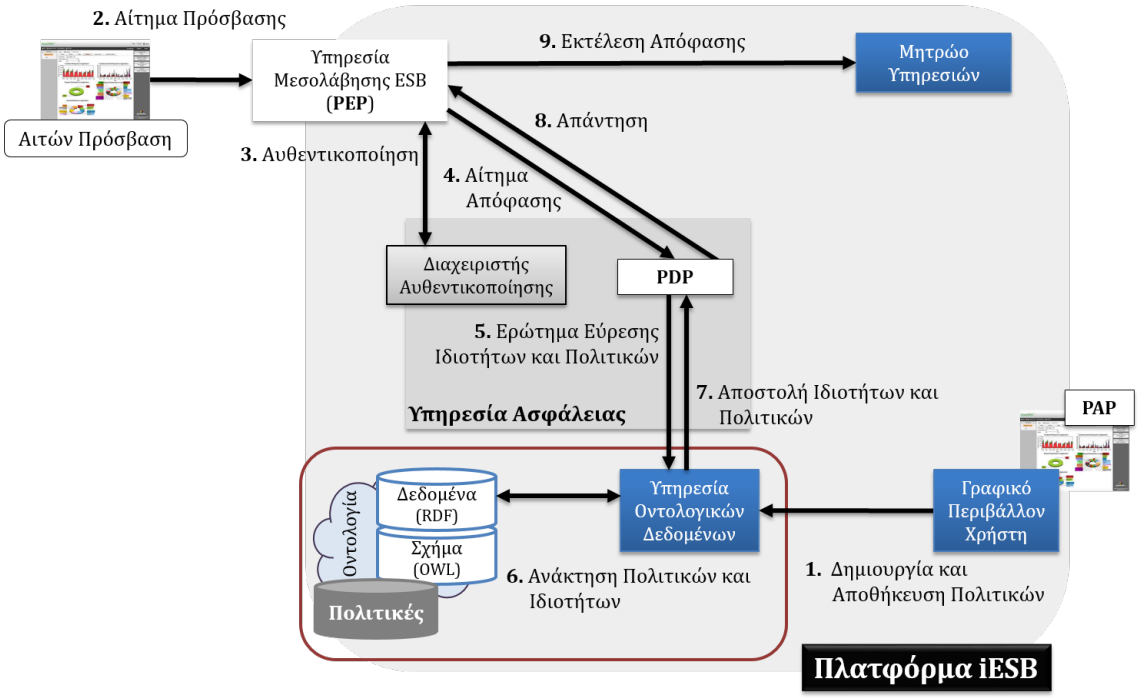
γάζεται. Αντίστοιχα, το είδος ενός πόρου (π.χ., ηλεκτρονικό αρχείο, υπηρεσία, έγγραφο) ή ο οργανισμός στον οποίο ανήκει, είναι πιθανά χαρακτηριστικά ενός Πόρου. Σε ορισμένες περιπτώσεις, η εφαρμογή ενός κανόνα ενδέχεται να απαιτεί την προήγηση μίας πράξης ή τη διαδοχή του από μία πράξη. Η απαίτηση αυτή μοντελοποιείται μέσω της έννοιας της Απαιτούμενης Πράξης (RequiredAction). Παράδειγμα μίας απαιτούμενης επακόλουθης πράξης είναι η καταγραφή της πρόσβασης στον πόρο.

5.1.3 Δίαυλος Επιχειρησιακών Υπηρεσιών: Υπηρεσία Ασφάλειας

Η ενσωμάτωση υπηρεσιών και εργαλείων, τα οποία ακολουθούν διαφορετικές στρατηγικές και έχουν υλοποιηθεί χρησιμοποιώντας διαφορετικές τεχνολογίες, οδηγεί συχνά σε κενά στην ασφάλεια του συστήματος. Τα κενά αυτά καλείται να καλύψει η Υπηρεσία Ασφάλειας (Security Service) της ευφυούς πλατφόρμας και να διασφαλίσει ότι:

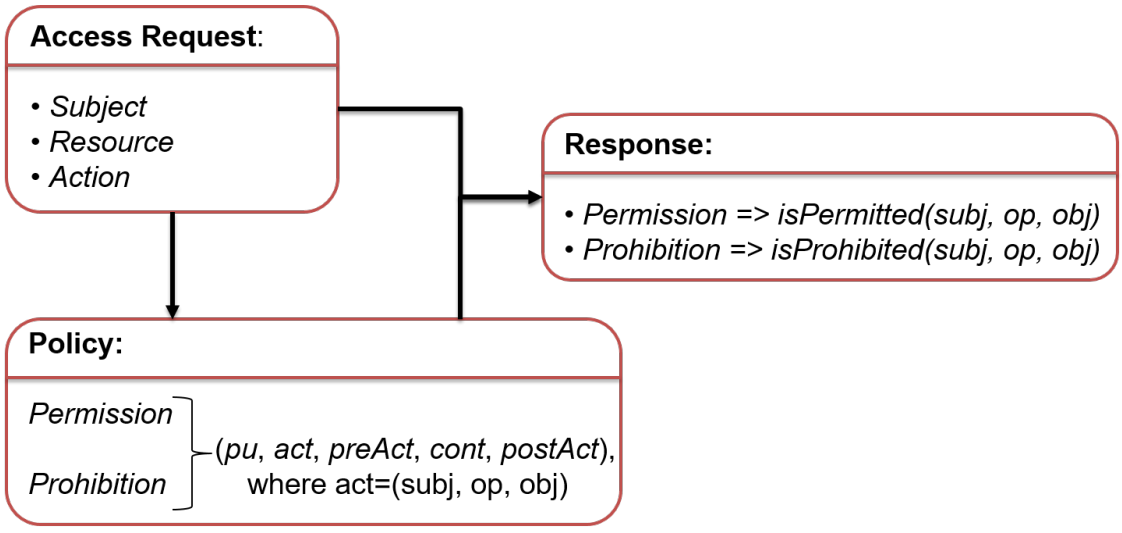
- τα ευαίσθητα εταιρικά δεδομένα παραμένουν προστατευμένα από εσωτερικές και εξωτερικές απειλές,
- οι πόροι του συστήματος, τόσο τα δεδομένα όσο και οι υπηρεσίες, είναι διαθέσιμα ανά πάσα χρονική στιγμή στις εξουσιοδοτημένες οντότητες, ακέραια και αμετάβλητα, προστατεύοντας έτσι τις βασικές αρχές της Ασφάλειας· την Εμπιστευτικότητα, τη Διαθεσιμότητα και την Ακεραιότητα.

Η Υπηρεσία Ασφάλειας παρέχει αυθεντικοποίηση των χρηστών και των υπηρεσιών του συστήματος και εξουσιοδοτεί τις αυθεντικοποιημένες οντότητες ώστε να έχουν πρόσβαση στους διαθέσιμους πόρους, υιοθετώντας δημοσιευμένα πρότυπα. Ο έλεγχος πρόσβασης υλοποιείται με τη χρήση πολιτικών, οι οποίες εισάγονται από το διαχειριστή του συστήματος κάνοντας χρήση της αντίστοιχης Διεπαφής Χρήστη. Η υπηρεσία αυτή ακολουθεί την προσέγγιση ελέγχου πρόσβασης που περιγράφηκε στο Κεφάλαιο 3, ενώ οι πολιτικές πρόσβασης εκφράζονται με τη χρήση οντολογιών.



Σχήμα 14: Ροή Αιτήματος Πρόσβασης

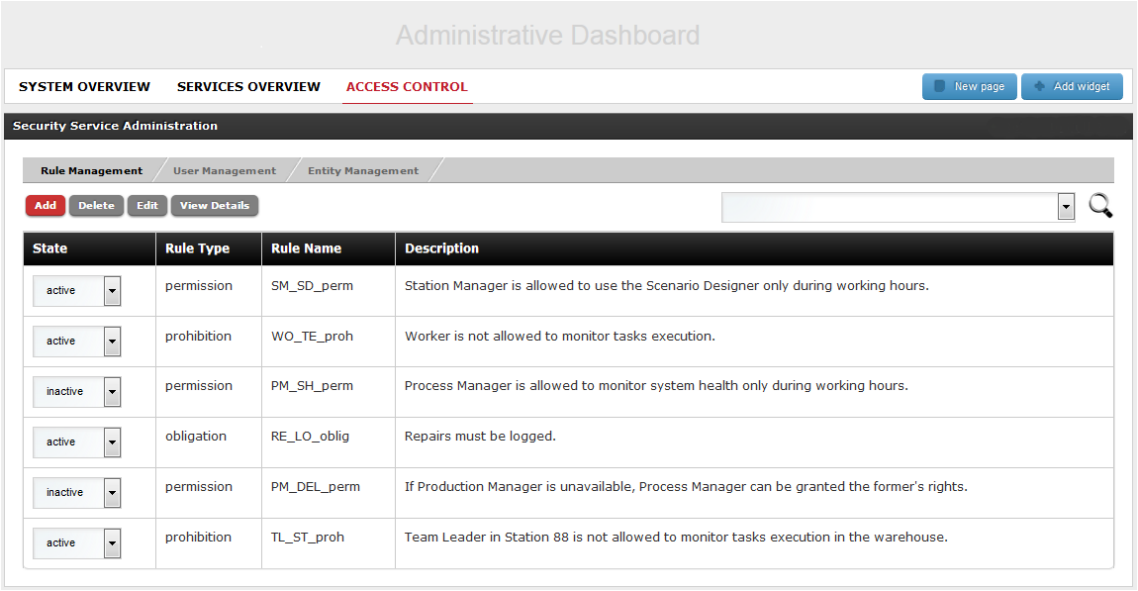
Συγκεκριμένα, ο διαχειριστής του συστήματος είναι υπεύθυνος για τη διαχείριση των χρηστών του συστήματος, καθώς και για τον ορισμό κανόνων που αφορούν στην πρόσβαση των πρώτων σε υπηρεσίες και δεδομένα, λαμβάνοντας υπόψη χαρακτηριστικά των εμπλεκόμενων οντοτήτων, παραμέτρους χωρικού ή/και χρονικού πλαισίου, γεγονότα που μπορεί να συμβούν, καθώς και ενέργειες που μπορεί να απαιτούνται ως συνέπεια της εξουσιοδότησης χρήστη.



Σχήμα 15: Έλεγχος Πρόσβασης: Σχήμα Αιτήματος-Απάντησης

5.1.4 Γραφικό Περιβάλλον Διαχείρισης Κανόνων Ελέγχου Πρόσβασης

Στο Σχήμα 16 απεικονίζεται η Σελίδα Ελέγχου Πρόσβασης (Access Control page), η οποία αποτελείται από τρεις καρτέλες που παρέχουν στο διαχειριστή του συστήματος όλες τις απαραίτητες πληροφορίες που χρειάζεται ο ίδιος για τον ορισμό κανόνων πρόσβασης σε πόρους του συστήματος.



Σχήμα 16: Γραφικό Περιβάλλον Διαχείρισης Κανόνων Πρόσβασης από τον Διαχειριστή του Συστήματος

Όπως φαίνεται και στο παραπάνω σχήμα, ο διαχειριστής μπορεί να επιλέξει την καρτέλα «Διαχείριση Κανόνων» (Rule Management), προκειμένου να ορίσει κανόνες πρόσβασης. Η καρτέλα αυτή περιέχει τρεις επιλογές για την προσθήκη, διαγραφή και επεξεργασία κανόνων, αντίστοιχα. Οι ήδη υπάρχοντες στο σύστημα κανόνες παρουσιάζονται συγκεντρωμένοι σε έναν πίνακα, όπου φαίνεται, επίσης, η κατάστασή τους (State: ενεργοί ή ανενεργοί), ο τύπος του κανόνα (RuleType: Εξουσιοδότηση, Απαγόρευση ή Υποχρέωση), το όνομά τους (RuleName), καθώς και η περιγραφή αυτών (Description). Υπάρχει ακόμα ένα πεδίο αναζήτησης κανόνων στην κορυφή της καρτέλας αυτής (search box), στο οποίο ο διαχειριστής μπορεί να ορίσει κάποιες παραμέτρους προκειμένου να αναζητήσει και να βρει συγκεκριμένους κανόνες που ο ίδιος επιθυμεί.

Σε περίπτωση που ο διαχειριστής του συστήματος θέλει να προσθέσει, για παράδειγμα, έναν κανόνα με τη μορφή εξουσιοδότησης πρόσβασης, επιλέγει το κουμπί «Προσθήκη» (Add) στην καρτέλα διαχείρισης κανόνων και ένα αναδυόμενο παράθυρο εμφανίζεται μπροστά του (AddRule pop-up window). Στο παράθυρο αυτό, ο διαχειριστής πρέπει να ορίσει το όνομα του κανόνα και την περιγραφή του στα σχετικά πεδία κειμένου, και έπειτα να ορίσει τον κανόνα από την καρτέλα «Δράση» (Action tab). Όπως αναφέρθηκε και παραπάνω, κάθε τέτοιος κανόνας αφορά μία

Δράση (Action), η οποία επιτρέπει ή απαγορεύει σε έναν Συμμετέχοντα (Actor), δηλαδή αιτούντα πρόσβασης, να πραγματοποιήσει μία Πράξη (Operation), όπως είναι η προβολή, η επεξεργασία ή η εκτέλεση, πάνω σε έναν Πόρο (Resource). Έτσι, βάσει των χαρακτηριστικών των προαναφερθεισών οντοτήτων, και, αν απαιτείται, βάσει παραμέτρων χωροχρονικού πλαισίου, μπορεί ο ίδιος να ορίσει μία δράση. Ένα παράδειγμα τέτοιου κανόνα είναι η περίπτωση όπου ένας χρήστης με το ρόλο "Station Manager" που ανήκει στο σταθμό εργασίας "Station 88" επιτρέπεται να έχει πρόσβαση στο πρόγραμμα εκτέλεσης εργασιών του εργοστασίου μόνο κατά τις εργάσιμες ημέρες και ώρες. Κανόνες τύπου Απαγόρευσης ή Υποχρέωσης ορίζονται με τρόπο παρόμοιο με αυτόν που περιγράφηκε μόλις για τον ορισμό κανόνων Εξουσιοδότησης.

Τέλος, ο διαχειριστής έχει τη δυνατότητα να διαγράψει ή να επεξεργαστεί έναν κανόνα, καθώς και να δει τις λεπτομέρειες που τον αφορούν, επιλέγοντάς τον από τον πίνακα των κανόνων.

5.1.4.1 Διαχείριση Χρηστών του Συστήματος

Για τη διαχείριση των χρηστών του συστήματος, ο διαχειριστής επιλέγει τη σχετική καρτέλα της σελίδας ελέγχου πρόσβασης (User Management tab). Στην καρτέλα αυτή, υπάρχει ένα πεδίο που φέρει τον τίτλο «Χρήστες» και περιλαμβάνει μία μπάρα αναζήτησης, έναν πίνακα που περιέχει όλους τους χρήστες του συστήματος, καθώς και ένα πεδίο με πέντε διαθέσιμες επιλογές (κουμπιά): «Προσθήκη Χρήστη», «Επεξεργασία Χρήστη», «Διαγραφή Χρήστη», «Προφίλ Χρήστη» και «Ανανέωση». Σε περίπτωση που ο διαχειριστής επιθυμεί να διαγράψει έναν χρήστη, να επεξεργαστεί κάποια χαρακτηριστικά του ή να δει το προφίλ του, θα πρέπει να τον αναζητήσει στην προαναφερθείσα μπάρα αναζήτησης και στη συνέχεια να επιλέξει την αντίστοιχη γραμμή του πίνακα και να πατήσει κάποιο από τα διαθέσιμα κουμπιά. Επίσης, σε περίπτωση που κάποιος χρήστης του συστήματος βρίσκεται, για παράδειγμα, σε διακοπές, μπορεί να απενεργοποιήσει προσωρινά το προφίλ του, επιλέγοντας το αντίστοιχο πεδίο που παρέχεται στο γραφικό περιβάλλον. Εάν ο διαχειριστής επιθυμεί να προσθέσει ένα νέο χρήστη στο σύστημα, επιλέγει το κουμπί «Προσθήκη Χρήστη» και έτσι εμφανίζεται ένα αναδυόμενο παράθυρο. Στο παράθυρο αυτό ο διαχειριστής μπορεί να εισάγει κάποιες προσωπικές πληροφορίες του χρήστη, όπως ονοματεπώνυμο, ηλικία, όνομα χρήστη κ.λπ., το ρόλο που έχει μέσα στο εργοστάσιο, τις ομάδες στις οποίες μπορεί να ανήκει, το τμήμα στο οποίο δουλεύει, τις ημέρες και ώρες εργασίας του, καθώς και άλλες πληροφορίες που αφορούν τις δυνατότητές του.

5.1.4.2 Διαχείριση Οντοτήτων του Συστήματος

Για τη δημιουργία κανόνων, είναι απαραίτητο ο διαχειριστής του συστήματος να ορίσει όλες τις οντότητες που συνιστούν τους κανόνες αυτούς και, συγκε-

κριμένα, το είδος των αιτούντων πρόσβαση και τα χαρακτηριστικά των πόρων του εργοστασίου, επιλέγοντας την καρτέλα «Διαχείριση Οντοτήτων» της σελίδας ελέγχου πρόσβασης (Entity Management tab) και έπειτα την καρτέλα «Χαρακτηριστικών» (Attributes tab). Ένα χαρακτηριστικό που αφορά είδος αιτούντα πρόσβαση μπορεί να είναι οποιοδήποτε χαρακτηριστικό στοιχείο χρήστη, όπως ο ρόλος του, η ομάδα που ανήκει και το τμήμα στο οποίο εργάζεται. Χαρακτηριστικά των πόρων αφορούν, για παράδειγμα, το είδος του πόρου (αρχείο, υπηρεσία, έγγραφο, κ.λπ.) ή και τον ιδιοκτήτη αυτού.

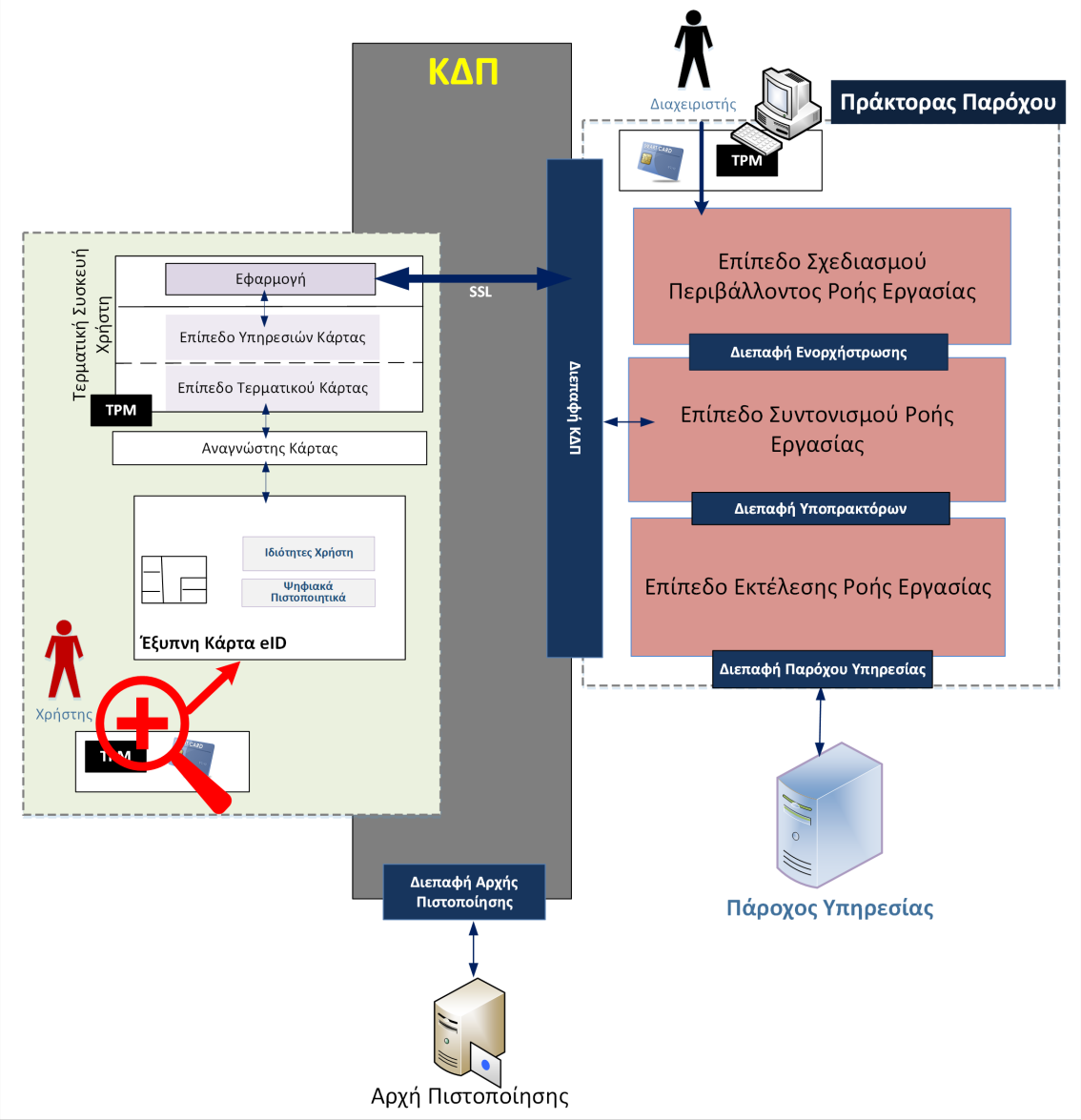
Η καρτέλα «Χαρακτηριστικά» αποτελείται από τα πεδία «Συμμετέχον» και «Πόρος», στο καθένα από τα οποία υπάρχει ένας πίνακας που παρουσιάζει όλα τα ήδη υπάρχοντα είδη χαρακτηριστικών αυτών, καθώς και τις πιθανές τιμές τους. Παράλληλα δίνεται η δυνατότητα στο διαχειριστή να προσθέσει, διαγράψει ή να επεξεργαστεί κάποιο χαρακτηριστικό μέσω της επιλογής των αντίστοιχων κουμπιών. Όπως αναφέρθηκε και παραπάνω, ο διαχειριστής του συστήματος μπορεί να ορίσει κανόνες βάσει παραμέτρων χωροχρονικού πλασίου. Έτσι, μπορεί ο ίδιος μέσω της καρτέλας «Πλαίσια» (Contexts tab) στην καρτέλα «Διαχείριση Οντοτήτων» να ορίσει χωρικά ή χρονικά πλαίσια βάσει δυναμικών παραμέτρων, όπως είναι ο χρόνος ή ακόμα και κάποιο περιστατικό που μπορεί να συμβεί. Τέλος, ο διαχειριστής του συστήματος είναι υπεύθυνος για τον ορισμό πιθανών ενεργειών σε έναν πόρο μέσω της καρτέλας «Λειτουργίες» (Operations tab) στην καρτέλα «Διαχείριση Οντοτήτων» της σελίδας ελέγχου πρόσβασης.

5.2 Εφαρμογή σε Σύστημα Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

5.2.1 Επισκόπηση του Συστήματος

Όπως φαίνεται και στο Σχήμα 17, η Κεντρική Διαδικτυακή Πύλη (ΚΔΠ) αποτελεί για τους πολίτες την πύλη εισόδου στις υπηρεσίες Ηλεκτρονικής Διακυβέρνησης (ΗΔ). Οι Δημόσιοι Φορείς που παρέχουν τις υπηρεσίες τους μέσω αυτής της πύλης έχουν ήδη ενσωματώσει τις τελευταίες στην πλατφόρμα που απεικονίζεται μέσω των κατάλληλων διεπαφών που παρέχονται σε αυτούς. Η πλατφόρμα αποτελεί την οντότητα εμπιστοσύνης μεταξύ των πολιτών και των Δημόσιων Φορέων και φέρει το ρόλο του διαμεσολαβητή ασφάλειας και προστασίας των προσωπικών τους δεδομένων [113].

Οι πολίτες που επιθυμούν να έχουν πρόσβαση σε κάποια από αυτές τις υπηρεσίες δε χρειάζεται να εγγραφούν σε κάθε μία από αυτές ξεχωριστά, καθώς το σύστημα υποστηρίζει εφάπαξ πιστοποίηση ταυτότητας και την εν συνεχεία διάφανη διαβίβαση της πιστοποίησης του χρήστη σε πολλαπλούς παρόχους (Single Sign-On)



Σχήμα 17: Αρχιτεκτονική Υψηλού Επιπέδου Συστήματος Παροχής Υπηρεσιών ΗΔ

για την εξυπηρέτηση των αιτημάτων τους. Για την εγγραφή στην πύλη, ο αιτών χρήστης συμπληρώνει την αίτηση εγγραφής δηλώνοντας τα στοιχεία του και επιλέγει μία προς μία τις ηλεκτρονικές υπηρεσίες που επιθυμεί να χρησιμοποιήσει. Για την ταυτοποίηση και αυθεντικοποίησή του στην πύλη απαιτείται η χρήση της προσωπικής ηλεκτρονικής ταυτότητάς του (electronic IDentity – eID).

Η ανάπτυξη σχέσης εμπιστοσύνης μεταξύ της ΚΔΠ και του χρήστη κρίνεται αναγκαία έτσι ώστε να επιτυγχάνεται η απαιτούμενη βεβαιότητα για τις «ταυτότητες» των οντοτήτων αυτών. Η δημιουργία της σχέσης αυτής βασίζεται στην ανταλλαγή ενός διακριτικού (token) που αξιοποιείται για την ταυτοποίηση και αυθεντικοποίησή τους. Επίσης, η δημιουργία ενός Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network – VPN) μεταξύ τους μπορεί να διασφαλίσει μεταξύ άλλων και την εμπι-

στευτικότητα και ακεραιότητα των δεδομένων τα οποία ανταλλάσσονται πάνω από το ασφαλές κανάλι επικοινωνίας (secure communication channel) το οποίο δημιουργείται.

Η ΚΔΠ δημιουργεί μία σχέση εμπιστοσύνης και με τον εξυπηρετητή της κάθε υπηρεσίας που επιθυμεί να εγγραφεί ο αιτών χρήστης, ελέγχοντας τα στοιχεία του τελευταίου, καθώς και κατά πόσο έχει δικαίωμα χρήσης της ηλεκτρονικής υπηρεσίας. Εφόσον τα αποτελέσματα των παραπάνω ελέγχων είναι θετικά, ο χρήστης ενημερώνεται για την επιτυχημένη εγγραφή του στην ΚΔΠ και στις ηλεκτρονικές υπηρεσίες στις οποίες μπορεί να έχει πρόσβαση. Ακολούθως, προκειμένου να χρησιμοποιήσει κάποια ηλεκτρονική υπηρεσία, ο χρήστης επισκέπτεται την ΚΔΠ και επιλέγει την υπηρεσία αυτή. Η ΚΔΠ, γνωρίζοντας το επίπεδο αυθεντικοποίησης που απαιτείται για τους αιτούντες προσπέλασης στην υπηρεσία αυτή, ενημερώνει το χρήστη για τα διαπιστευτήρια που απαιτείται να παρουσιάσει προκειμένου να του επιτραπεί η πρόσβαση. Έτσι, η ΚΔΠ στέλνει στον Πράκτορα Πελάτη (Client Agent) του χρήστη ένα αίτημα αυθεντικοποίησης μέσω του περιηγητή ιστού (Web Browser) της εφαρμογής του. Για την ικανοποίηση αυτού του αιτήματος, το τερματικό του χρήστη είναι εξοπλισμένο με αναγνώστη έξυπνης κάρτας και έτσι ο χρήστης τοποθετεί την κάρτα του στον αναγνώστη και στη διαδραστική οθόνη εμφανίζεται μήνυμα εισαγωγής προσωπικού κωδικού (PIN) για τη συνέχεια της συναλλαγής. Ο Πράκτορας Πελάτη μέσω της κατάλληλης διεπαφής επικοινωνεί με την κάρτα του χρήστη και η τελευταία του παρέχει την απαιτούμενη πληροφορία (πιστοποιητικό χρήστη). Εν τέλει, ο Πράκτορας Πελάτη, μέσω της κατάλληλης διεπαφής παραδίδει το πιστοποιητικό του χρήστη στην πύλη και η οντότητα αυτής που είναι υπεύθυνη για την αυθεντικοποίηση επικοινωνεί μέσω της Διεπαφής Αρχής Πιστοποίησης (CA Interface) με την Αρχή Πιστοποίησης προκειμένου να ελεγχθεί η περίπτωση άρσης δικαιωμάτων του χρήστη. Εφόσον το αποτέλεσμα του σχετικού ελέγχου είναι αρνητικό, ο χρήστης μπορεί να κάνει πλέον χρήση της αιτούμενης υπηρεσίας. Για την υποστήριξη παροχής επιπρόσθετων υπηρεσιών μη-αποποίησης, η ΚΔΠ διατηρεί αρχείο καταγραφής (log file) κάθε προσπάθειας αυθεντικοποίησης.

Επιπρόσθετα, για την εφαρμογή του δικαιώματος επιλογής αποκάλυψης των προσωπικών τους δεδομένων σε τρίτους βάσει νομοθεσίας, οι πολίτες, μέσω εφαρμογής που βρίσκεται στο τερματικό τους, έχουν τη δυνατότητα να ορίζουν τις δικές τους προτιμήσεις ιδιωτικότητας αναφορικά με την αποκάλυψη και χρήση των προσωπικών τους δεδομένων στους διάφορους δημόσιους φορείς. Ένα παράδειγμα προτίμησης ιδιωτικότητας του χρήστη αφορά την περίπτωση που του ζητείται να συγκατατεθέσει ή όχι αν επιθυμεί κάποια στατιστική υπηρεσία να έχει πρόσβαση σε ορισμένα προσωπικά του στοιχεία και δεδομένα, σε περίπτωση που η τελευταία τα ζητήσει για τη διεξαγωγή κάποιας έρευνας. Με τον τρόπο αυτό, οι υπηρεσίες που παρέχονται μέσω της ΚΔΠ γίνονται περισσότερο προσωποποιημένες στο χρηστή. Η αρχιτεκτονική μεσισμικού (middleware) αναλαμβάνει έπειτα τη διαχείριση των αιτημάτων των

χρηστών για πρόσβαση στις υπηρεσίες, έχοντας πάντα ως γνώμονα την προστασία της ιδιωτικότητάς του.

Η πλατφόρμα παροχής υπηρεσιών ΗΔ που απεικονίζεται στο παραπάνω σχήμα συνιστά ένα κατανεμημένο σύστημα. Η ανταλλαγή των δεδομένων των πολιτών μεταξύ των υποκείμενων οντοτήτων της πλατφόρμας πραγματοποιείται υπό την επιτήρηση μηχανισμών που εφαρμόζουν πολιτικές βασισμένες στη νομοθεσία, θέτοντας με τον τρόπο αυτό όρια στη χρήση προσωπικών δεδομένων. Το μεσισμικό της πλατφόρμας εκτείνεται σε πολλά επίπεδα στην αλυσίδα παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Οι πολιτικές και οι σχετικοί κανονισμοί παρέχονται από την Αρχή Ιδιωτικότητας, η οποία φροντίζει να ενημερώνει το σχετικό αρχείο στο οποίο αποθηκεύονται τα παραπάνω και να το διανείμει αυτόματα σε όλους τους παρόχους. Όσον αφορά στις επιχειρησιακές πολιτικές του εκάστοτε φορέα, η ισχύς αυτών έπεται αυτής των προαναφερθεισών πολιτικών που ορίζει η Αρχή Ιδιωτικότητας.

Η προαναφερθείσα πλατφόρμα διαθέτει τις οντότητες εκείνες που είναι υπεύθυνες για την εφαρμογή των κανόνων αυτών και, συγκεκριμένα, τους πράκτορες λογισμικού. Το συνολικό σύστημα αποτελείται από πολλά πολυπρακτορικά υποσυστήματα, στα οποία κάθε πράκτορας χαρακτηρίζεται από μία ξεχωριστή ταυτότητα (id), την κατάστασή του (state) καθώς και ένα στόχο (goal) που θα πρέπει να εκτελέσει, μόνος ή με την συνεργασία άλλων πρακτόρων. Σε κάθε πάροχο υπηρεσίας ηλεκτρονικής διακυβέρνησης αντιστοιχεί ένα πολυπρακτορικό σύστημα, το Πολυπρακτορικό Σύστημα Παρόχου (ΠΣΠ). Συνεπώς, για την ομαλή εκτέλεση μίας ροής εργασιών, οι πράκτορες λογισμικού που συνιστούν το εκάστοτε ΠΣΠ κατηγοριοποιούνται στις εξής βασικές οντότητες:

- Πράκτορας Διαχείρισης Ταυτότητας
- Πράκτορας Συντονισμού Λειτουργιών
- Πράκτορας Πελάτη
- Πράκτορας Παρόχου

Ο *Πράκτορας Διαχείρισης Ταυτότητας* (IdManagementAgent) είναι υπεύθυνος για τη διαχείριση της εγγραφής ή διαγραφής ενός πράκτορα στο περιβάλλον του παρόχου. Κάθε πολυπρακτορικό σύστημα αποτελείται από έναν μόνο Πράκτορα Διαχείρισης Ταυτότητας. Κάθε πράκτορας που επιθυμεί να εγγραφεί στο ΠΣΠ θα πρέπει αρχικά να επικοινωνήσει με τον IdManagementAgent, έτσι ώστε ο τελευταίος να αποκτήσει μία μοναδική ταυτότητα, ενώ ο πρώτος να ανανεώσει τη λίστα που διατηρεί τις ταυτότητες των πρακτόρων του συστήματος. Η εγγραφή του πράκτορα συνιστά τη «γέννησή» του στο ΠΣΠ και πλέον μπορεί να επικοινωνεί με τους υπόλοιπους που είναι εγγεγραμμένοι σε αυτό. Οι πράκτορες του συστήματος οφείλουν να ενημερώνουν τον Πράκτορα Διαχείρισης για την κατάσταση στην οποία βρίσκονται κάθε στιγμή (π.χ. ενεργή κατάσταση, κατάσταση αναμονής κλπ.). Ο *Πράκτορας Συντονισμού Λειτουργιών* (ServiceCoordinatorAgent) αποτελεί τη μοναδική υπεύθυνη οντό-

τητα για την καταγραφή των υπηρεσιών των πρακτόρων που υπάρχουν σε κάθε ΠΣΠ. Ο Πράκτορας Συντονισμού Λειτουργιών διατηρεί μία λίστα ενημερωμένη με τις πιο πρόσφατες υπηρεσίες των πρακτόρων και μέσω αυτής οι πράκτορες είναι σε θέση να εντοπίσουν τον ή τους κατάλληλους πράκτορες που θα τους βοηθήσουν στην επίτευξη των στόχων τους. Ανά πάσα στιγμή και για οποιονδήποτε λόγο, ένας πράκτορας μπορεί να ζητήσει από τον Πράκτορα Συντονισμού Λειτουργιών να τροποποιήσει την περιγραφή των υπηρεσιών που παρέχει.

Ο *Πράκτορας Πελάτη* (ClientAgent) λειτουργεί ως εκπρόσωπος ενός καταναλωτή υπηρεσιών της πλατφόρμας παροχής υπηρεσιών ΗΔ, δηλαδή του χρήστη. Όσον αφορά στον χρήστη, ο ίδιος μπορεί μέσω του τερματικού του και μίας εφαρμογής που παρέχεται σε αυτόν να ορίσει τις προτιμήσεις ιδιωτικότητας. Σε αντίθεση με τους προηγούμενους πράκτορες, ο πράκτορας χρήστη δεν είναι μοναδικός στο ΠΣΠ καθώς αντιστοιχεί ένας σε κάθε χρήστη της πλατφόρμας. Ο πράκτορας χρήστη είναι υπεύθυνος για την αποστολή αιτημάτων μέσω της Διεπαφής ΚΔΠ (Core Interface) στην πλατφόρμα ενσωματώνοντας τα πιστοποιητικά του χρήστη καθώς και τους προαναφερθέντες κανόνες και διαχειρίζεται τις ταυτότητές του για τη χρήση αυτών στις παρεχόμενες υπηρεσίες. Για το λόγο αυτό, όταν ο χρήστης αιτείται πρόσβαση σε μία υπηρεσία, μαζί με το ψηφιακό πιστοποιητικό της ταυτότητάς του, μεταδίδονται και οι σχετικές προτιμήσεις ιδιωτικότητας σε μία ενιαία δομή. Με τον τρόπο αυτό, ο χρήστης μπορεί να ορίσει κατά πόσο επιθυμεί προσωπικά του δεδομένα να αποκαλυφθούν σε κάποιον φορέα για την παροχή υπηρεσίας καθώς και σε τι βαθμό, τη δυνατότητα να ζητηθεί η συγκατάθεσή του σε περιπτώσεις που επεξεργασία ή αποκάλυψη και χρήση δεδομένων του πρόκειται να λάβει χώρα ή/και το χρονικό διάστημα που επιθυμεί να διατηρηθούν τα προσωπικά του δεδομένα στην πλατφόρμα παροχής υπηρεσιών ΗΔ. Μετά την αυθεντικοποίηση του χρήστη και την επιλογή από τον ίδιο της επιθυμητής υπηρεσίας ηλεκτρονικής διακυβέρνησης, αυτομάτως δημιουργείται ένας πράκτορας που φέρει την ταυτότητά του και τις προτιμήσεις ιδιωτικότητας και έχει ως στόχο (goal) να επικοινωνήσει με τον κατάλληλο πράκτορα για τη εκτέλεση της διαδικασίας που του ζητήθηκε.

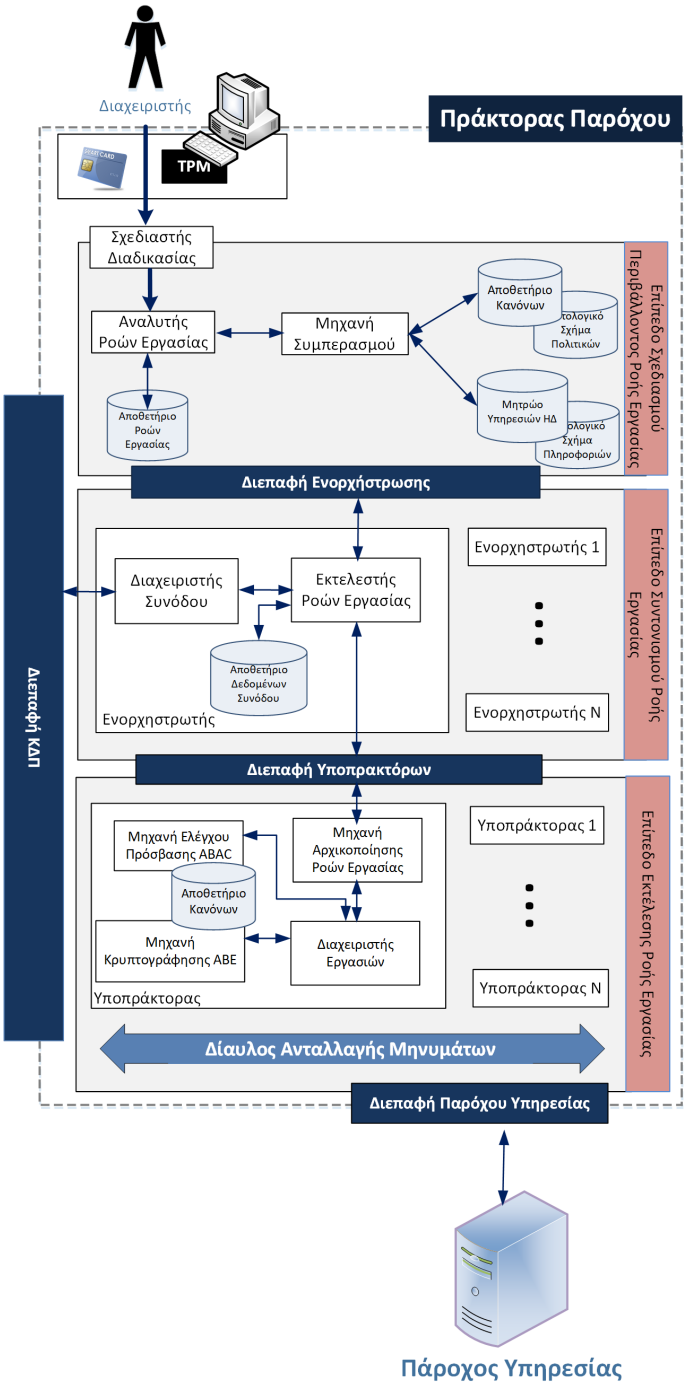
Η βασική λειτουργία του συστήματος παρέχεται από τον *Πράκτορα Παρόχου* (ProviderAgent), ο οποίος αποτελεί μία έξυπνη οντότητα διαμεσολάβησης μεταξύ των χρηστών και του φορέα παροχής υπηρεσιών ΗΔ. Συνεπώς, σε κάθε δημόσιο φορέα που παρέχει υπηρεσίες ηλεκτρονικής διακυβέρνησης αντιστοιχεί ένας Πράκτορας Παρόχου καθώς και ένα ΠΣΠ. Ο Πράκτορας Παρόχου αποτελεί τη σημαντικότερη αλλά και την πιο πολύπλοκα δομημένη οντότητα στην πολυπρακτορική πλατφόρμα. Δεδομένου ότι ο Πράκτορας Παρόχου εγκαθίσταται σε κάθε οργανισμό που ανήκει στην αλυσίδα παροχής υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, η πρόσβαση στα δεδομένα των χρηστών ελέγχεται από αυτόν ενώ, ανά πάσα στιγμή, η Αρχή Ιδιωτικότητας μπορεί να παρακολουθήσει και να ελέγξει τις διαδικασίες που επιτελούνται εσωτερικά στον πράκτορα, προκειμένου να διασφαλιστεί η τήρηση των

κανόνων που προκύπτουν από τη σχετική νομοθεσία. Η μοντελοποίηση της νομοθεσίας για την προστασία της ιδιωτικότητας πραγματοποιείται με τη χρήση σημασιολογικού μοντέλου πληροφορίας που συσχετίζει προσωπικά δεδομένα, υπηρεσίες και ρόλους χρηστών με ρητώς ορισμένους κανόνες. Έτσι, κάθε πληροφορία που σχετίζεται με την παροχή υπηρεσιών ΗΔ μοντελοποιείται σε μία οντολογία, εξασφαλίζοντας έτσι τη σημασιολογική διαλειτουργικότητα μεταξύ των εμπλεκόμενων οργανισμών.

Ο Πράκτορας Παρόχου συνίσταται από 3 επίπεδα (Σχήμα 18): το Επίπεδο Σχεδιασμού Περιβάλλοντος Ροής Εργασιών (Workflow Planning Environment), το Επίπεδο Συντονισμού Ροής Εργασιών (Orchestration Layer) και, τέλος, το Επίπεδο Εκτέλεσης Ροής Εργασιών (Execution Layer) [114]. Το πρώτο επίπεδο αφορά την καταγραφή της ροής εργασιών και περιλαμβάνει όλα τα βήματα για τον γραφικό ορισμό της, τον έλεγχο αυτής και τους απαραίτητους μετασχηματισμούς. Το Επίπεδο Συντονισμού περιλαμβάνει διαδικασίες που αφορούν τον συντονισμό των υποκείμενων οντοτήτων, έτσι ώστε στο Επίπεδο Εκτέλεσης να πραγματοποιηθεί η εκτέλεση της έγκυρης πλέον ροής εργασιών από τους Υποπράκτορες.

Συγκεκριμένα, το *Επίπεδο Σχεδιασμού Περιβάλλοντος Ροής Εργασίας* περιλαμβάνει τις εξής οντότητες:

- Σχεδιαστής Διαδικασίας (Process Modeller): αποτελεί την πλατφόρμα ορισμού διαδικασιών ηλεκτρονικής διακυβέρνησης και παρέχει στον Διαχειριστή κάθε οργανισμού ένα φιλικό προς τον χρήστη γραφικό περιβάλλον για τον σχεδιασμό ροών εργασιών (workflow) καθώς και των αντίστοιχων ροών δεδομένων (dataflow). Αυτό το στάδιο περιλαμβάνει τον σχεδιασμό κατευθυνόμενων γράφων που αντιπροσωπεύουν διαδικασίες, όπου οι κόμβοι είναι οι εμπλεκόμενοι στην παροχή υπηρεσίας οργανισμοί και οι ακμές αφορούν τις μεταξύ τους αλληλεπιδράσεις. Το λογισμικό που χρησιμοποιείται για την υποστήριξη αυτού του σταδίου είναι οι γραφικοί επεξεργαστές (graphical editors), που χειρίζονται τις διαδικασίες και τα αποθετήρια (repositories), όπου αποθηκεύονται τα μοντέλα των ροών εργασιών.
- Αναλυτής Ροών Εργασιών (Workflow Analyst): είναι η υπεύθυνη οντότητα για τη διενέργεια επαλήθευσης της ορθότητας μίας ροής εργασιών και την ενσωμάτωση λειτουργιών για την προστασία της ιδιωτικότητας. Σε συνεργασία με τη Μηχανή Συμπερασμού, ελέγχεται και αναλύεται στο σύνολό της η διαδικασία ώστε να είναι συμβατή με απαιτήσεις προστασίας προσωπικών δεδομένων, οι οποίες αφορούν την ασφάλεια, την πρόσβαση σε προσωπικά δεδομένα των πολιτών από τους φορείς που συμμετέχουν στην όλη διαδικασία και τη διαχείριση ταυτότητας αυτών και μετασχηματίζεται κατάλληλα με την προσθήκη απαραίτητων μηχανισμών προστασίας ιδιωτικότητας βάσει σημασιολογικού μοντέλου ηλεκτρονικής διακυβέρνησης, όπως, ενσωμάτωση ελέγχου πρόσβασης και διαχείρισης ταυτοτήτων, εφαρμογή κρυπτογράφησης για δεδομένα που ανταλλά-



Σχήμα 18: Αρχιτεκτονική Πράκτορα Παρόχου

σονται ή αποθηκεύονται, λειτουργίες ανωνυμίας/ψευδωνυμίας όπου κρίνεται απαραίτητο, περιορισμός ζητούμενων δεδομένων στα απολύτως απαραίτητα, προσαρμοστικότητα στις προτιμήσεις ιδιωτικότητας πολίτη και, τέλος, αλληλεπίδραση με πολίτη (ενημέρωση, συγκατάθεση, καταγραφή συμβάντων). Η τελική μορφή της ροής εργασίας αποθηκεύεται στο αντίστοιχο αποθετήριο (Workflow Repository), έτσι ώστε να είναι διαθέσιμη στο Επίπεδο Ενορχήστρωσης ως

μια έγκυρη ροή εργασιών προς εκτέλεση.

- Μηχανή Συμπερασμού (Reasoner): ενσωματώνει τους κανόνες ορισμένους βάσει του σημασιολογικού μοντέλου πολιτικών και της ισχύουσας νομοθεσίας και διεξάγει μία σειρά από λογικούς υπολογισμούς, προσφέροντας την απαιτούμενη γνώση για τους διάφορους ελέγχους και μετατροπές σε μία ροή εργασίας. Κύριες λειτουργίες της είναι η επιλογή της κατάλληλης υπηρεσίας από ένα σύνολο διαθέσιμων υπηρεσιών (Service Registry) αλλά και η λήψη αποφάσεων σχετικά με τις απαιτήσεις χρήσης προσωπικών δεδομένων από τις υπηρεσίες, λαμβάνοντας υπόψη τις πολιτικές που έχουν οριστεί από την αρμόδια Αρχή Ιδιωτικότητας καθώς και το σύνολο των κανόνων που έχει ορίσει ο ίδιος ο οργανισμός και έχουν αποθηκευτεί προσωρινά στο Αποθετήριο Κανόνων (Policy Repository).

Το *Επίπεδο Συντονισμού Ροής Εργασίας* (Orchestration Layer) αποτελείται από ένα σύνολο Ενορχηστρωτών (Orchestrators), καθένας από τους οποίους παίζει το ρόλο του συντονιστή μιας ροής εργασιών καθ' όλη τη διάρκεια εκτέλεσής της. Ο κάθε Ενορχηστρωτής, αφού λάβει μία ροή εργασίας από τον Αναλυτή Ροών Εργασιών, την κατακερματίζει σε επιμέρους ροές (subflows) εφόσον απαιτείται, επιλέγει τους κατάλληλους Υποπράκτορες (SubAgents) για την εκτέλεση της σχετικής με το αίτημα ροής εργασιών για την ολοκλήρωση της απαιτούμενης διαδικασίας και τους παρέχει κατευθυντήριες εντολές για ανταλλαγή μηνυμάτων μεταξύ τους. Τα προσωπικά δεδομένα των πολιτών που διαχειρίζεται ο Πράκτορας Παρόχου αποθηκεύονται στο αποθετήριο δεδομένων συνόδου (Personal Data Repository) που βρίσκεται εσωτερικά σε κάθε Ενορχηστρωτή και η διατήρηση αυτών στο αποθετήριο μπορεί να διαρκέσει είτε για μικρό είτε για μεγάλο χρονικό διάστημα, ανάλογα με τη φύση της υπηρεσίας και τις απαιτήσεις που υπάρχουν για διαλειτουργικότητα μεταξύ διαφορετικών φορέων, προκειμένου να ικανοποιηθεί το αίτημα του χρήστη. Στο προαναφερθέν αποθετήριο, μαζί με τα προσωπικά δεδομένα αποθηκεύονται και οι σχετικές προτιμήσεις ιδιωτικότητας του χρήστη, οι οποίες, όπως αναφέρθηκε και παραπάνω, ενσωματώνονται στο αίτημά του από τον Πράκτορα Πελάτη και μεταδίδονται από το τερματικό του στην πλατφόρμα μέσω της κατάλληλης διεπαφής που παρέχεται σε αυτόν (Core Interface). Κάθε φορά που ο Πράκτορας Παρόχου λαμβάνει ένα αίτημα για πρόσβαση σε υπηρεσία, το αίτημα αυτό εξετάζεται από τον Συντονιστή και συγκεκριμένα από την υποκείμενη οντότητα αυτού που αναφέρεται ως Διαχειριστής Συνόδου (Session Manager). Έτσι, ο Εκτελεστής Ροής Εργασίας (Workflow Executor) εξετάζει το αίτημα του χρήστη και αποφασίζει αν απαιτούνται άλλες πληροφορίες από το χρήστη, αν και κατά πόσο ο χρήστης επιθυμεί την πλήρη ή μερική αποκάλυψη ή/και απόκρυψη των προσωπικών του δεδομένων, καθώς και αν απαιτεί να πραγματοποιηθούν κάποιες συμπληρωματικές ενέργειες αναφορικά με την παροχή συγκατάθεσης αυτού. Με αυτόν τον τρόπο επιτυγχάνεται η ελάχιστη δυνατή χρήση προσωπικών δεδομένων από τον πάροχο υπηρεσιών, δεδομένου ότι ο όγκος αυτών αρκεί για την ικανο-

ποίηση του αιτήματος του χρήστη.

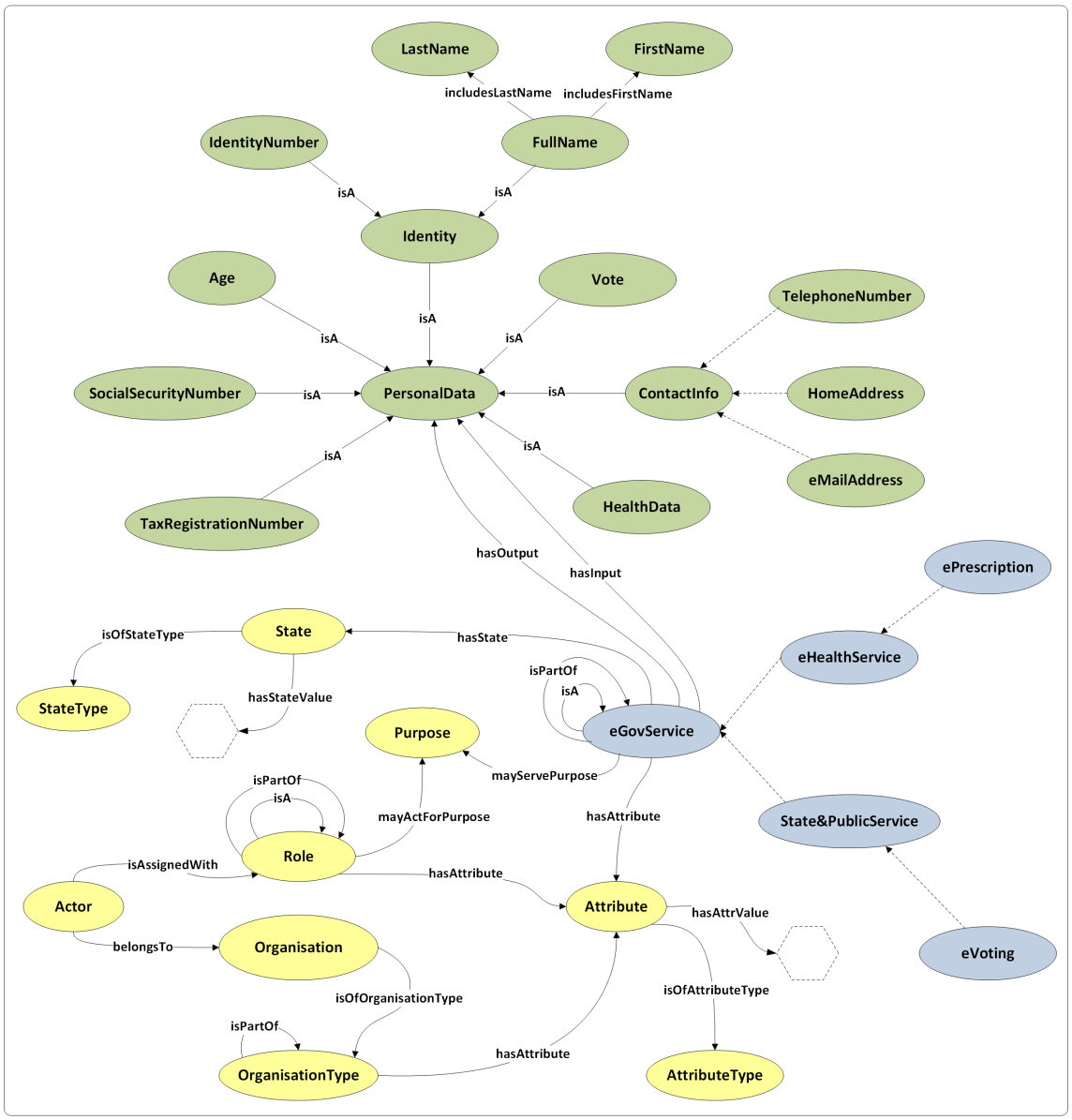
Τέλος, το *Επίπεδο Υποπρακτόρων* (SubAgents Layer) αποτελείται από Υποπράκτορες (SubAgents). Κύρια λειτουργία τους είναι η εκτέλεση ενός συγκεκριμένου καθήκοντος, ορισμένο από το Επίπεδο Συντονισμού Ροής Εργασίας, ενώ βασικό στοιχείο τους αποτελεί η δυνατότητα ανταλλαγής δεδομένων μεταξύ τους μέσω ενός Διαύλου Μηνυμάτων (Message Bus). Μετά την ολοκλήρωση την εργασίας που τους είχε ανατεθεί ενημερώνουν τον υπεύθυνο Ενορχηστρωτή μέσω της κατάλληλης διεπαφής. Αναφορικά με τον προαναφερθέντα Δίαυλο Ανταλλαγής Μηνυμάτων, οι πράκτορες του συστήματος πρέπει να είναι σε θέση να επικοινωνούν με τους χρήστες, με πόρους του συστήματος, καθώς και με κάθε άλλο πράκτορα, εάν πρέπει να συνεργαστούν, να διαπραγματευτούν και ούτω καθεξής. Για την επίτευξη της επικοινωνίας, οι πράκτορες αλληλεπιδρούν μεταξύ τους με τη χρήση ορισμένων ειδικών γλωσσών επικοινωνίας. Τα μηνύματα που ανταλλάσσονται μεταξύ των πρακτόρων φέρουν τις εξής πληροφορίες: (α) ταυτότητα παραλήπτη-πράκτορα, (β) χαρακτηρισμό μηνύματος (Ενημέρωση, Άρνηση, Έγκριση κλπ.) και (γ) περιεχόμενο μηνύματος.

5.2.2 Σημασιολογικά Μοντέλα Πληροφορίας

5.2.2.1 Περιγραφή Σημασιολογικού Μοντέλου Πληροφοριών

Το πλαίσιο ελέγχου πρόσβασης βασίζεται σε ένα σημασιολογικά πλούσιο μοντέλο πληροφοριών που συνιστά την ακριβή σημασιολογική αναπαράσταση των βασικών οντοτήτων που μετέχουν στο σύστημα, καθώς και των μεταξύ τους συσχετίσεων. Οι παράμετροι που πρέπει να λαμβάνονται υπόψη κατά τη διαδικασία παροχής πρόσβασης αφορούν τους τύπους των δεδομένων που δημιουργούνται, συλλέγονται και διακινούνται μεταξύ φορέων και παρόχων υπηρεσιών ηλεκτρονικής διακυβέρνησης και πολιτών για την ικανοποίηση αιτημάτων των τελευταίων, τις ιδιότητες και τα προσωπικά στοιχεία των πολιτών, τη φύση των υπηρεσιών και των υποκείμενων διεργασιών, και τέλος, την ταξινόμηση ρόλων όλων των εμπλεκόμενων οντοτήτων και φορέων που συμμετέχουν στην αλυσίδα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Όπως φαίνεται και στο Σχήμα 19, θεμελιώδες στοιχείο του μοντέλου αυτού είναι τα *Προσωπικά Δεδομένα (PersonalData)* για την αναπαράσταση της πληθώρας διαφορετικών τύπων προσωπικών δεδομένων του χρήστη και των μεταξύ τους συσχετίσεων που συλλέγονται και υπόκεινται σε επεξεργασία για την εκτέλεση μίας ενέργειας. Το σύνολο των δεδομένων αυτών περιλαμβάνει μεταξύ άλλων τον *Αριθμό Φορολογικού Μητρώου (TaxRegistrationNumber)*, τον *Αριθμό Μητρώου Κοινωνικής Ασφάλισης (SocialSecurityNumber)*, την *Ηλικία (Age)*, *δεδομένα Υγείας (HealthData)*, *Πληροφορίες Επικοινωνίας (ContactInfo)* όπως, *Αριθμό Τηλεφώνου (TelephoneNumber)*, *Διεύθυνση Σπιτιού (HomeAddress)* και *Διεύθυνση Ηλεκτρονικού Ταχυδρομείου (eMailAddress)*, κα-



Σχήμα 19: Σημασιολογικό Μοντέλο Πληροφορίας Ηλεκτρονικής Διακυβέρνησης

θώς και την *Ταυτότητά (Identity)* του και συγκεκριμένα τον *Αριθμό Ταυτότητας (IdentityNumber)* και το *Ονοματεπώνυμό του (FullName)*. Οι παραπάνω τύποι προσωπικών δεδομένων χαρακτηρίζονται από τρεις σχέσεις, οι οποίες αντικατοπτρίζουν την κληρονομικότητα χαρακτηριστικών, το επίπεδο λεπτομέρειας της ίδιας έννοιας και τη συμπερίληψη ενός τύπου δεδομένων σε κάποιον άλλο.

Οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης αντανακλώνται από την οντολογική κλάση *eGovService*, η οποία, στο επίπεδο αφαιρέσεων, περιλαμβάνει τους διάφορους τύπους υπηρεσιών ΗΔ, όπως *eHealthService* και *State & PublicService*. Κάθε υπηρεσία χαρακτηρίζεται από μία *Κατάσταση (State)*, η οποία αντανακλά ουσιαστικά το αποτέλεσμα που έχει η εκτέλεση μίας υπηρεσίας στα δεδομένα που λαμβάνει, και ορίζεται από έναν τύπο (*StateType*) και μία τιμή (*StateValue*).

Οι *Δράστες (Actor)* του συστήματος που ανήκουν σε *Οργανισμούς (Organisation)* συσχετίζονται με *Ρόλους (Role)* που τους έχουν ανατεθεί. Το σύνολο των ρόλων καθορίζει σχέσεις κληρονομικότητας σε περίπτωση συμπερίληψης ενός ρόλου σε κάποιον άλλον. Επιπρόσθετα, σχέσεις μεταξύ ρόλων αντικατοπτρίζουν τη ρητή συμμετοχή ορισμένων σε έναν άλλο, υπονοώντας την ανάγκη αλληλεπίδρασης των συμμετεχόντων ρόλων για την εκτέλεση κάποιας ενέργειας.

Η οντολογική κλάση *Purpose* αντανακλά τους σκοπούς για τους οποίους προσωπικά δεδομένα συλλέγονται ή/και υπόκεινται σε επεξεργασία. Η παράμετρος αυτή είναι ιδιαίτερα σημαντική, καθώς μία απόφαση για την παροχή πρόσβασης δεν μπορεί να ληφθεί ανεξάρτητα από τον υποκείμενο σκοπό που μπορεί να διαφοροποιήσει σημαντικά τη συμπεριφορά της εκάστοτε οντότητας. Επιπλέον, η έννοια του σκοπού υποδεικνύει τους συμβατούς σκοπούς για τους οποίους μπορούν να ενεργούν οι χρήστες στους οποίους έχει ανατεθεί ένας συγκεκριμένος ρόλος.

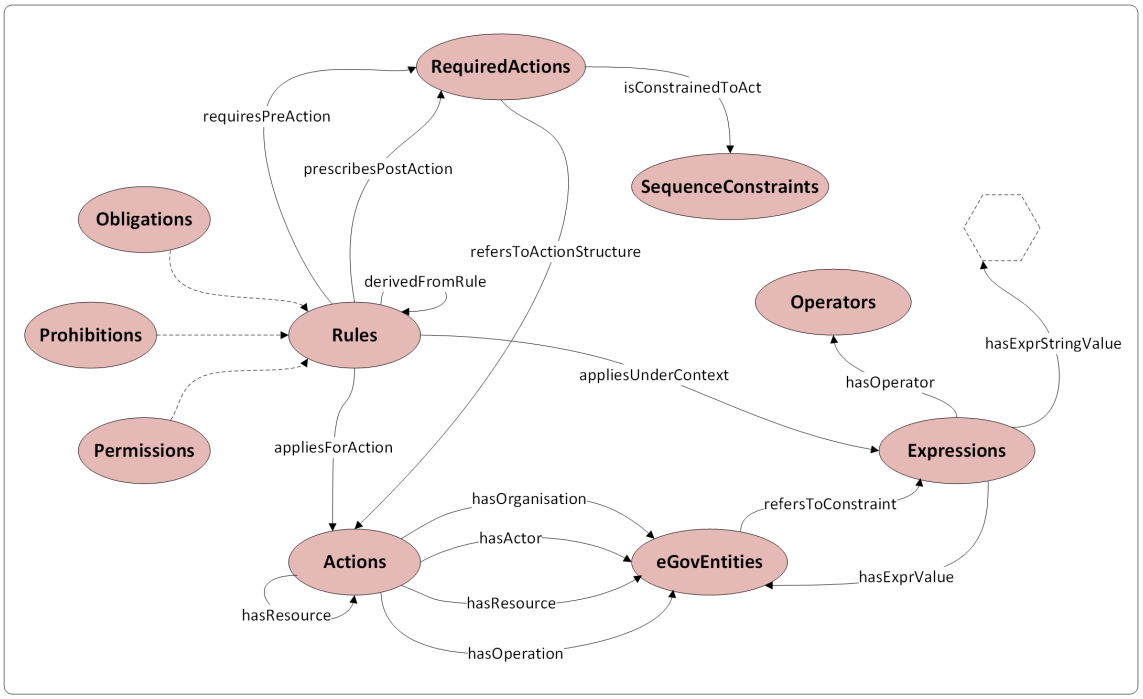
Τέλος, για την ανάθεση ιδιοτήτων σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, οργανισμούς και ρόλους χρησιμοποιείται η κλάση *Attribute*, η οποία συσχετίζεται με έναν τύπο, ο οποίος μπορεί να είναι κάποιος συνήθης τύπος, όπως, π.χ. String, και να αποτελεί στιγμιότυπο της κλάσης *AttributeType* ή κάποια άλλη οντότητα του Σημασιολογικού Μοντέλου Πληροφορίας και προαιρετικά με μία τιμή, η οποία μπορεί να είναι ένα οντολογικό στοιχείο ή μία συμβολοσειρά.

5.2.2.2 Περιγραφή Σημασιολογικού Μοντέλου Πολιτικών

Το Σημασιολογικό Μοντέλο Πολιτικών αποτελεί τη βάση λειτουργίας του μοντέλου ελέγχου πρόσβασης, μέσω του οποίο προδιαγράφονται οι κανόνες που αφορούν:

- τον έλεγχο πρόσβασης σε υπηρεσίες και δεδομένα, λαμβάνοντας υπόψη το σκοπό συλλογής, μετάδοσης και επεξεργασίας των δεδομένων,
- τις περιόδους υποχρεωτικής διατήρησης πληροφοριών στις βάσεις δεδομένων αλλά και υποχρεωτικής διαγραφής αυτών,
- τη διαχείριση ταυτοτήτων και ψευδωνύμων κατά την αλληλεπίδραση οργανισμών στην αλυσίδα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης,
- την εφαρμογή μηχανισμών ασφάλειας για την προστασία των προσωπικών δεδομένων κατά την αλληλεπίδραση οργανισμών, και τέλος,
- τη δυνατότητα ορισμού προτιμήσεων ιδιωτικότητας, παροχής ή άρσης συναίνεσης σε πραγματικό ή μη χρόνο για την υποστήριξη ενεργού ρόλου των πολιτών.

Στο Σχήμα 20 απεικονίζεται το Σημασιολογικό Μοντέλο Πολιτικών. Οι ενέργειες αποτελούν τον πυρήνα των κανόνων ελέγχου πρόσβασης, ορίζοντας επιπρόσθετα προ- και μετα- ενέργειες που πρέπει (ή όχι) να εκτελεστούν πριν και μετά την εφαρμογή ενός κανόνα. Οντολογικά οι ενέργειες υλοποιούνται σαν στιγμιότυπα



Σχήμα 20: Σημασιολογικό Μοντέλο Πολιτικών

της κλάσης *Actions*. Κάθε ενέργεια σχετίζεται με το δράστη (*hasActor*), τη λειτουργία (*hasOperation*), τον πόρο (*hasResource*) και τον οργανισμό (*hasOrganisation*) της ενέργειας. Παρόλα αυτά, οι προαναφερθείσες ιδιότητες δε δείχνουν απευθείας στο στοιχείο αναφοράς και έτσι γίνεται χρήση της κλάσης *eGovEntities* που υποδεικνύει οντότητες που περιλαμβάνονται στο Σημασιολογικό Μοντέλο Πληροφορίας.

Οι κανόνες ελέγχου πρόσβασης υλοποιούνται στην οντολογία πολιτικών μέσω της κλάσης *Rules*. Ουσιαστικά, η κλάση αυτή ενσωματώνει όλες τις υπόλοιπες κλάσεις της οντολογίας, προσφέροντας έτσι την υλοποίηση των κανόνων ελέγχου πρόσβασης. Καθώς οι κανόνες είναι δυνατόν να περιγράφουν άδειες, απαγορεύσεις και υποχρεώσεις, ορίζονται οι αντίστοιχες υπο-κλάσεις της κλάσης Rules, δηλαδή *Permissions*, *Prohibitions* και *Obligations*, αντίστοιχα. Κάθε κανόνας περιγράφεται σαν ένα στιγμιότυπο της κατάλληλης υπο-κλάσης, ενώ προσδιορίζονται και τα πεδία του, δηλαδή η ενέργεια για την οποία βρίσκει εφαρμογή ο κανόνας, οι προ- και μετα-ενέργειες, οι συνθήκες πλαισίου και ο υποκείμενος σκοπός πρόσβασης και χρήσης. Η ιδιότητα *appliesUnderContext* δείχνει σε κάποιο στιγμιότυπο της κλάσης *Expressions* για να δηλωθούν οι παράμετροι πλαισίου κάτω από τις οποίες ο εν λόγω κανόνας ισχύει. Επίσης, ορίζονται οι κατάλληλες ιδιότητες για τα στιγμιότυπα της κλάσης Expressions, οι οποίες υποδεικνύουν το υποκείμενο (*hasExprSubject*), τον τελεστή (*hasOperator*) και την τιμή (*hasExprValue*). Οι τελεστές ορίζονται οντολογικά ως στιγμιότυπα της κλάσης Operators, ενώ το υποκείμενο και η τιμή μίας έκφρασης μπορεί να είναι στιγμιότυπα είτε του Σημασιολογικού Μοντέλου Πολιτικών είτε του αντίστοιχου Μοντέλου Πληροφορίας. Ωστόσο, η τιμή είναι δυνατόν να είναι κάποια αυθαί-

ρετη συμβολοσειρά και για αυτό το λόγο χρησιμοποιείται η ιδιότητα τύπου δεδομένων *hasExprStringValue*.

Η κύρια ενέργεια του κανόνα είναι ένα στιγμιότυπο της κλάσης *Actions* και ορίζεται άμεσα μέσω της ιδιότητας *appliesForAction*. Σε ό,τι αφορά τις προ- και μετα-ενέργειες, αυτές αποτελούν επίσης στιγμιότυπα της κλάσης Actions· ωστόσο, ο κανόνας τελικά συσχετίζεται με στιγμιότυπα της κλάσης *RequiredActions*, η οποία παρεμβάλλεται μεταξύ των κανόνων και των ενεργειών, μέσω των ιδιοτήτων *requiresPreAction* και *prescribesPostAction*. Η ιδιότητα *isConstrainedToAct* χρησιμοποιείται ώστε να εκφραστούν περιορισμοί τόσο χρονικοί όσο και σχετικοί με την αλληλουχία εκτέλεσης, οι οποίοι αντανακλώνται από τα στιγμιότυπα της κλάσης *SequenceConstraints*.

5.2.3 Εργαλείο Σχεδιασμού Ασφαλών Ροών Εργασιών

Μία από τις βασικές υπηρεσίες που προσφέρει στους παρόχους υπηρεσιών ηλεκτρονικής διακυβέρνησης η παραπάνω πλατφόρμα είναι η δυνατότητα να σχεδιάζουν ασφαλείς ροές εργασιών, συμβατές με την πλατφόρμα. Συγκεκριμένα, παρέχει ένα γραφικό περιβάλλον χρήστη (Graphical User Interface – GUI), το οποίο επιτρέπει στους παρόχους να ορίζουν τις υπηρεσίες που προσφέρουν καθώς και τις ιδιότητες των χρηστών αυτών, και, στη συνέχεια, να προδιαγράφουν πολιτικές για τον έλεγχο πρόσβασης στις προαναφερθείσες υπηρεσίες. Μετά τον ορισμό των παραπάνω, ακολουθεί η διαδικασία σχεδίασης της ροής εργασιών μίας υπηρεσίας μέσω του εργαλείου σχεδιασμού ασφαλών ροών εργασιών, καθώς και ο έλεγχος αυτής για το κατά πόσο είναι ασφαλής και συμβατή με τους κανόνες που έχει ορίσει ο πάροχος. Το *Εργαλείο Σχεδιασμού Σημασιολογικών Ροών Εργασιών* (Semantic WORkflow Design – SWORD) αποτελείται από δύο GUIs: (α) το γραφικό περιβάλλον χρήστη για τον ορισμό σημασιολογικών πολιτικών ελέγχου πρόσβασης, υπηρεσιών και χρηστών του συστήματος και (β) το γραφικό περιβάλλον χρήστη για το σχεδιασμό ροών εργασιών.

5.2.3.1 Γραφικό Περιβάλλον Χρήστη για τον Ορισμό Πολιτικών Ελέγχου Πρόσβασης, Υπηρεσιών και Χρηστών

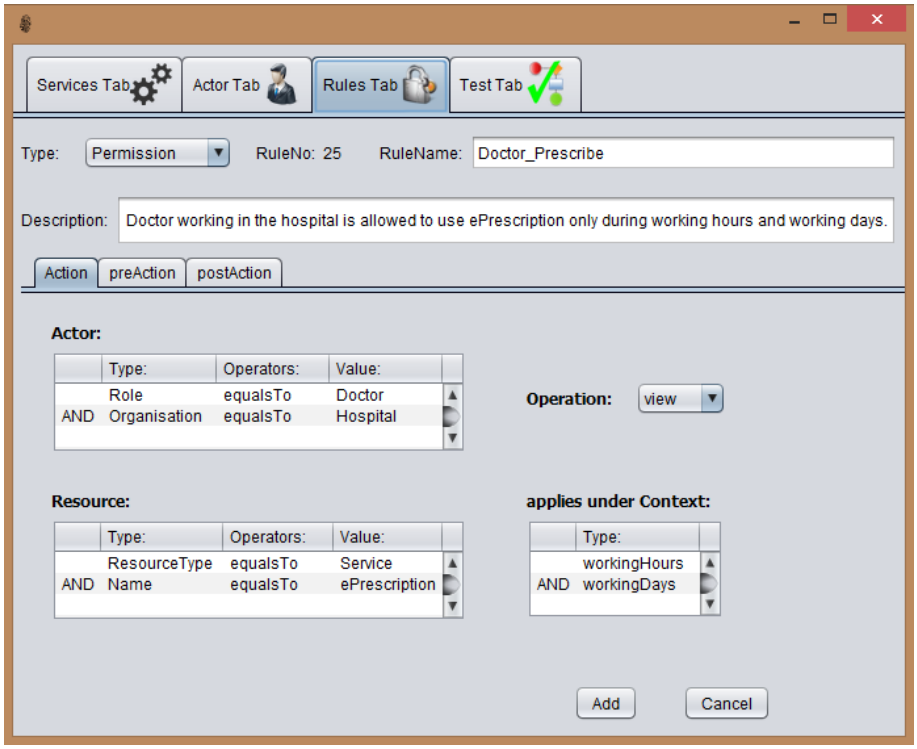
Το *Γραφικό Περιβάλλον Χρήστη για τον Ορισμό Πολιτικών Ελέγχου Πρόσβασης, Υπηρεσιών και Χρηστών* έχει ως αρχικό στόχο την καταχώρηση σημασιολογικά ορισμένων στιγμιοτύπων των υπηρεσιών που προσφέρουν οι πάροχοι στην πλατφόρμα, καθώς και των χρηστών που έχουν πρόσβαση σε αυτές. Ύστερα, εφόσον έχουν οριστεί τα σημασιολογικά στιγμιότυπα πληροφορίας, ακολουθεί ο ορισμός των σημασιολογικών κανόνων ελέγχου πρόσβασης. Το GUI αυτό αποτελείται από τέσσερις καρτέλες (tabs): *Καρτέλα Υπηρεσιών* Services Tab, *Καρτέλα Χρηστών* (Actor Tab), *Καρτέλα Πολιτικών* (Rules Tab) και *Καρτέλα Ελέγχου* (Test Tab). Θα πρέπει να σημειωθεί

πως για την ανάπτυξη του συγκεκριμένου GUI έγινε χρήση της γλώσσας προγραμματισμού Java ενώ για την ανάγνωση του σημασιολογικού μοντέλου πληροφορίας και τη δημιουργία ή διαγραφή σημασιολογικά ορισμένων στιγμιοτύπων χρησιμοποιήθηκε η βιβλιοθήκη Jena.

Η καρτέλα *Services Tab* (ST) δίνει τη δυνατότητα στον πάροχο μίας υπηρεσίας ηλεκτρονικής διακυβέρνησης να καθορίζει το είδος της υπηρεσίας που προσφέρει (π.χ. eHealth), το όνομά της (π.χ. ePrescription), το σκοπό που εξυπηρετεί καθώς και το είδος και το όνομα του οργανισμού που την προσφέρει. Ορίζοντας τα παραπάνω, δημιουργούνται τα αντίστοιχα στιγμιότυπα (instances) των κλάσεων του οντολογικού σχήματος που παρουσιάστηκε σε προηγούμενη ενότητα καθώς και των μεταξύ τους σχέσεων (object & data properties) με έναν αυτοματοποιημένο τρόπο και, έπειτα, αποθηκεύονται στο αντίστοιχο αποθετήριο. Όπως η καρτέλα ST, έτσι και η καρτέλα *Actor Tab* (AT) δίνει τη δυνατότητα στον πάροχο να εγγράψει τους χρήστες της υπηρεσίας του. Για να είναι το πλαίσιο ελέγχου πρόσβασης λειτουργικό, ο πάροχος της υπηρεσίας θα πρέπει να καθορίσει όχι μόνο τον ρόλο του χρήστη αλλά και τις ιδιότητές του.

Όσον αφορά στην καρτέλα *Rules Tab* (RT), τα προσωπικά δεδομένα πρέπει να φυλάσσονται με ασφάλεια και να προστατεύονται από οποιαδήποτε πιθανή απειλή, και, ως εκ τούτου, η προστασία τους αποτελεί μείζον ζήτημα για τους παρόχους υπηρεσιών. Δεδομένου ότι οι χρήστες, τα δεδομένα και οι υπηρεσίες έχουν ήδη οριστεί σημασιολογικά και ταξινομηθεί μέσω των καρτελών Actor και Services Tabs αντίστοιχα, οι πάροχοι υπηρεσιών είναι σε θέση να καθορίσουν τους κανόνες που αφορούν την προστασία των δεδομένων. Αυτό επιτυγχάνεται λαμβάνοντας υπόψη τα χαρακτηριστικά των εμπλεκόμενων φορέων, συναφών παραμέτρων (όπως ο χρόνος ή η τοποθεσία), γεγονότα που μπορεί να συμβούν ή απαιτούμενες ενέργειες που πρέπει να γίνουν ως προϋπόθεση ή ως συνέπεια της έγκρισης πρόσβασης στα δεδομένα ή τις υπηρεσίες (π.χ. καταγραφή της δραστηριότητας). Ο υποκείμενος μηχανισμός που είναι υπεύθυνος για τον έλεγχο πρόσβασης συνδυάζει τη λογική των γλωσσών ορισμού κανόνων «Συμβάν-Κατάσταση-Δράση» με τη λογική των RDF τριάδων (υποκείμενο-κατηγόρημα-αντικείμενο) και εκμεταλλεύεται την αφαιρετική συλλογιστική.

Όπως απεικονίζεται στο Σχήμα 21, σε περίπτωση που ο πάροχος υπηρεσιών επιθυμεί να προσθέσει, για παράδειγμα, έναν κανόνα που ορίζεται ως Άδεια, πρέπει να καθορίσει ο ίδιος το επιθυμητό όνομα του κανόνα (RuleName), καθώς και την περιγραφή του κανόνα στις αντίστοιχες περιοχές κειμένου του GUI και, στη συνέχεια, να τον ορίσει επιλέγοντας την καρτέλα Action. Κάθε κανόνας αφορά μία δράση, όπου ένας χρήστης (Actor, αιτών πρόσβαση) επιτρέπεται, απαγορεύεται ή είναι υποχρεωμένος (ανάλογα με τον τύπο του κανόνα που ο διαχειριστής έχει επιλέξει στη λίστα που βρίσκεται στο πάνω αριστερό μέρος του παραθύρου) για να εκτελέσει μια λειτουργία (π.χ. να δει, να επεξεργαστεί, να εκτελέσει, κ.λπ.) σε έναν πόρο (υπηρεσία ΗΔ ή δεδομένα). Με βάση τα χαρακτηριστικά των προαναφερθέντων φορέων και



Σχήμα 21: Γραφικό Περιβάλλον Ορισμού Πολιτικών Πρόσβασης στο Εργαλείο SWORD

λαμβάνοντας υπόψη παραμέτρους χωρικές ή χρονικές (αν χρειάζεται), μπορεί να καθορίσει τη δράση αυτή.

Αναλυτικότερα, στην καρτέλα Action υπάρχουν δύο πεδία που φέρουν τους τίτλους Δράστης (Actor) και Πόρος (Resource) αντίστοιχα, όπου ο διαχειριστής πρέπει να καθορίσει τα χαρακτηριστικά του Δράστη και του Πόρου στον οποίο ο χρήστης επιτρέπεται να εκτελέσει μια ενέργεια που ορίζεται από τη λίστα που φέρει τον τίτλο Λειτουργία (Operation), επιλέγοντας μία λειτουργία από το σύνολο αυτών που έχουν οριστεί γενικά για το σύστημα. Για παράδειγμα, όπως φαίνεται και στο παραπάνω σχήμα, ο δράστης-αιτών υπηρεσία, του οποίου ο ρόλος είναι γιατρός και ο οργανισμός στον οποίο ανήκει είναι ένα νοσοκομείο, επιτρέπεται να έχει πρόσβαση στην υπηρεσία ηλεκτρονικής συνταγογράφησης και να συνταγογραφεί μόνο κατά τις εργάσιμες ημέρες και ώρες.

Οι φορείς παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης μπορούν επίσης να καθορίσουν τις ενέργειες που θα πρέπει να έχουν προηγηθεί ή ακολουθήσει την εφαρμογή του κανόνα με την επιλογή των preAction και postAction καρτελών, αντίστοιχα, ακολουθώντας την ίδια διαδικασία όπως αυτή περιγράφηκε προηγουμένως αναφορικά με την προδιαγραφή της κύριας δράσης. Μια postAction δράση θα μπορούσε να είναι, για παράδειγμα, η καταγραφή σε αρχείο της επιτρεπόμενης πρόσβασης σε δεδομένα.

Τέλος, στην καρτέλα Test Tab (TT) ο πάροχος μπορεί να επιλέξει έναν από τους χρήστες που έχει εγγράψει στο σύστημα μέσω του Actor Tab και να ελέγξει αν η ροή εργασιών της υπηρεσίας που προσφέρει είναι ασφαλής. Με την ολοκλήρωση της διαδικασίας ελέγχου, ο πάροχος θα ενημερωθεί για την ύπαρξη σφαλμάτων ή μη στα διάφορα στάδια ορισμού των προαναφερθέντων. Ο σχεδιασμός της ροής εργασιών πρέπει να πραγματοποιηθεί πριν την έναρξη ελέγχου της, κάτι το οποίο γίνεται μέσω του γραφικού περιβάλλοντος χρήστη που παρουσιάζεται στην επόμενη ενότητα.

5.2.4 Γραφικό Περιβάλλον Χρήστη για τον Σχεδιασμό Ροών Εργασιών

Σε αυτήν την ενότητα παρουσιάζεται το *Γραφικό Περιβάλλον Χρήστη για το Σχεδιασμό Ροών Εργασιών* του εργαλείου SWORD. Οι ροές εργασιών που προκύπτουν από το συγκεκριμένο εργαλείο αντιστοιχούν στις υπηρεσίες που προσφέρουν οι πάροχοι, είναι απόλυτα συμβατές με την πλατφόρμα και βασίζονται και αυτες στο σημασιολογικό μοντέλο ελέγχου πρόσβασης. Οι μηχανισμοί λήψης αποφάσεων, οι οποίοι βασίζονται στους σημασιολογικούς κανόνες ελέγχου πρόσβασης που ο πάροχος έχει ορίσει στο σύστημα, είναι υπεύθυνοι για τη διαχείριση της εκτέλεσης των επιχειρηματικών διεργασιών. Ως αποτέλεσμα, η ενορχήστρωση των διαδικασιών εξαρτάται από το σημασιολογικό συλλογισμό.

Για τον σχεδιασμό ενός ενιαίου πλαισίου για την ενορχήστρωση ροών εργασιών παρέχεται μια βασική ροή εργασιών που ονομάζεται eGovServiceWorkflow που αρχικοποιεί όλες τις κρίσιμες μεταβλητές που πρέπει να ληφθούν υπόψη και έχουν ορισθεί προηγουμένως στο εργαλείο SWORD. Για την προδιαγραφή της βασικής ροής εργασιών χρησιμοποιήθηκε το πλαίσιο WADE (Workflows and Agents Development Environment) που συνοδεύεται από ένα περιβάλλον ανάπτυξης που ονομάζεται WOLF και μπορεί να εγκατασταθεί στο Eclipse. Το WADE είναι μια πλατφόρμα λογισμικού που βασίζεται στο πλαίσιο JADE (JAVA Agent DEvelopment Framework) και παρέχει υποστήριξη για την εκτέλεση των καθηκόντων που ορίζονται σύμφωνα με μία ροή εργασιών. Η βασική οντότητα της πλατφόρμας WADE είναι η κλάση WorkflowEngineAgent που επεκτείνει τη βασική κλάση Agent της βιβλιοθήκης JADE ενσωματώνοντας ένα μικρό και ελαφρύ μηχανισμό ροής εργασιών. Εάν ο πάροχος υπηρεσιών επιθυμεί να σχεδιάσει από την αρχή τη ροή εργασιών μιας υπηρεσίας που προσφέρει και, στη συνέχεια, να την ελέγξει, πρέπει να δημιουργήσει μια νέα ροή εργασιών που έχει ως μητρική της τη ροή eGovServiceWorkflow και, έπειτα, να κάνει χρήση των υπολοίπων Οντοτήτων Ροής Εργασιών (Workflow Components) που έχουν δημιουργηθεί. Στο Σχήμα 22 παρουσιάζονται οι εννέα οντότητες ροών εργασιών που παρέχονται στο χρήστη για τον σχεδιασμό ροών.

Ο πάροχος υπηρεσιών μπορεί εύκολα να επιλέξει μία από αυτές τις οντότητες μέσω του γραφικού περιβάλλοντος του εργαλείου SWORD, να εισάγει τον κώδικά του σε γλώσσα προγραμματισμού Java στην κύρια μέθοδο και τέλος, να την ενώσει μαζί

Σχήμα 22: Οντότητες Ροών Εργασιών του Εργαλείου SWORD

με τις υπόλοιπες οντότητες της ροής εργασιών. Οι οντότητες ροής εργασιών εκτελούνται από τους υποπράκτορες του συστήματος.

Όσον αφορά στην οντότητα *ABAC*, προκειμένου να ελεγχθεί η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα, τυχόν παραβιάσεις της ιδιωτικότητας, η προστασία της εμπιστευτικότητας και της ακεραιότητας και η χρήση υπηρεσιών που παρέχονται στα πλαίσια της ηλεκτρονικής διακυβέρνησης, χρησιμοποιείται το μοντέλο Ελέγχου Πρόσβασης Βάσει Ιδιοτήτων, λαμβάνοντας υπόψη τον υψηλό βαθμό ευαισθησίας των δεδομένων που εμπλέκονται στις συναλλαγές μεταξύ ετερογενών οργανισμών κατά τη διάρκεια της παροχής υπηρεσιών. Για τον έλεγχο των αιτημάτων πρόσβασης, καθορίζονται πολιτικές οι οποίες ορίζουν τον τρόπο με τον οποίο δίνεται η πρόσβαση σε δεδομένα και υπηρεσίες, καθώς και τον τρόπο που χρησιμοποιούνται τα προσωπικά δεδομένα των πολιτών βάσει του υποκείμενου σκοπού και υλοποιούνται με τη χρήση μηχανισμών ελέγχου πρόσβασης. Στη συγκεκριμένη πλατφόρμα παροχής υπηρεσιών ΗΔ, υπάρχουν επιμέρους οντότητες που είναι υπεύθυνες για τη διαχείριση των πολιτικών, την επεξεργασία και την αξιολόγηση του αιτήματος για πρόσβαση σε έναν πόρο βάσει κανόνων, τη λήψη αποφάσεων και την επιβολή τους. Σχετικά με την οντότητα *ABE_Encryption*, για την προστασία των δεδομένων που συλλέγονται, υποβάλλονται σε επεξεργασία και διακινούνται μεταξύ των φορέων που εμπλέκονται στην αλυσίδα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης, χρησιμοποιείται η Κρυπτογράφηση Βάσει Ιδιοτήτων. Όπως προδιαγράφηκε στο Κεφάλαιο 3, η κρυπτογράφηση βασίζεται σε διάφορα χαρακτηριστικά και ιδιότητες των πολιτών και υλοποιείται με τρόπο τέτοιο ώστε να είναι αποτελεσματική η διαδικασία μετάδοσης των δεδομένων αυτών, έχοντας ως πρωταρχικό στόχο την προστασία της ιδιωτικότητας.

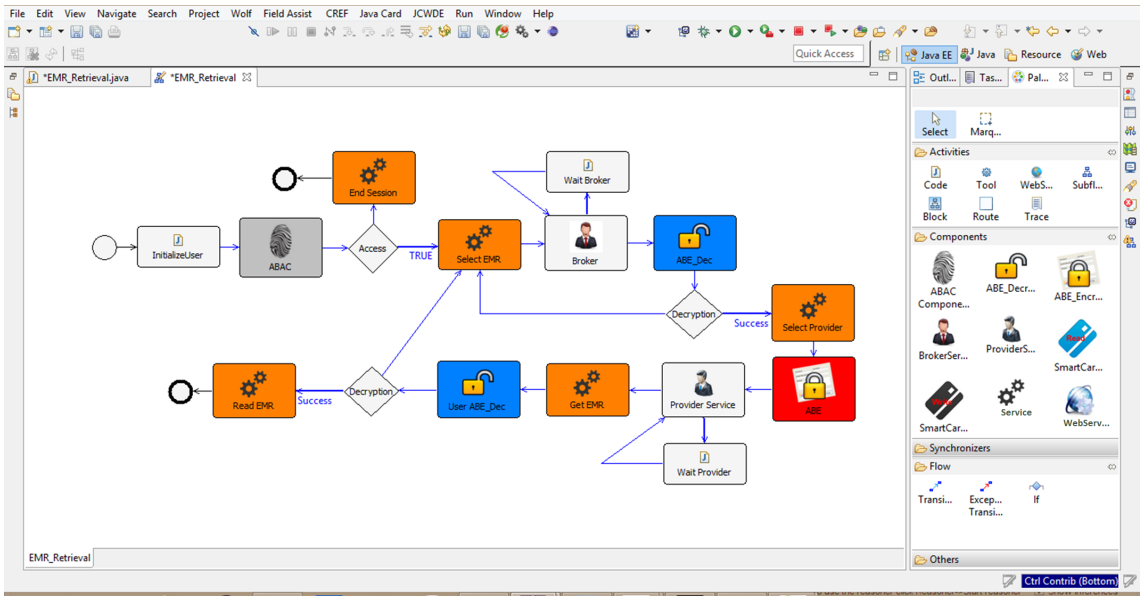
Η οντότητα *Service* εκτελεί τον κώδικα που εισάγει ο πάροχος. Πιο συγκεκριμένα, δέχεται ως είσοδο τις εξής κρίσιμες παραμέτρους:

- `serviceName`: το όνομα της υπηρεσίας.
- `needsAccessControl`: η λογική μεταβλητή για την απαίτηση ελέγχου πρόσβασης ABAC πριν την πρόσβαση σε υπηρεσία ή δεδομένα.
- `needsABE_En`: η λογική μεταβλητή για την απαίτηση κρυπτογράφησης δεδομέ-

νων.

- `user`: ο χρήστης της υπηρεσίας.
- `data`: τα δεδομένα του χρήστη.
- `workflowError`: η λογική μεταβλητή για την ύπαρξη ή μη κάποιου σφάλματος όσον αφορά στην ασφάλεια της υπηρεσίας βάσει των αρχικών προδιαγραφών του παρόχου.

Πριν από την εκτέλεση κάθε υπηρεσίας και αφού οριστούν από τον πάροχο οι παραπάνω μεταβλητές, πρέπει να ελεγχθεί αν η υπηρεσία αυτή είναι ασφαλής. Συγκεκριμένα, εκτελείται μία υπορροή εργασίας που έχει ως στόχο τον εντοπισμό σφαλμάτων ασφάλειας και ιδιωτικότητας κατά την εκτέλεση μιας εργασίας. Η οντότητα *WebService* ακολουθεί την ίδια ροή εργασιών εντοπισμού σφαλμάτων με την οντότητα Service, αλλά η κύρια μέθοδος που εφαρμόζει καταναλώνει υπηρεσίες ιστού.



Σχήμα 23: Παράδειγμα Χρήσης του Εργαλείου SWORD για το Σχεδιασμό Ροής Εργασιών

Η οντότητα *SmartCardRead* χρησιμοποιείται για την ανάκτηση δεδομένων από την ηλεκτρονική κάρτα πολίτη του χρήστη για την ανάκτηση δεδομένων. Για την αποθήκευση των δεδομένων στην κάρτα χρησιμοποιείται η οντότητα *SmartCardWrite*. Σημειώνεται πως και οι δύο αυτές οντότητες ακολουθούν την ίδια ροή εργασιών εντοπισμού σφαλμάτων με την οντότητα Service. Τέλος, οι οντότητες *BrokerAgent* και *ProviderAgent* χρησιμοποιούνται για την αυτοματοποιημένη επικοινωνία με τον Πράκτορα Διαμεσολάβησης και τον Πράκτορα Παρόχου αντιστοίχως. Με αυτόν τον τρόπο, δίνεται η δυνατότητα στον πάροχο μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης να ανταλλάσσει δεδομένα με άλλους παρόχους υπηρεσιών που βρίσκονται σε διαφορετικές πλατφόρμες JADE, ενισχύοντας έτσι τη συνεργασία μεταξύ φορέων. Θα πρέπει να σημειωθεί ότι η ενορχήστρωση ροών εργασιών που αφορούν υπηρεσίες περισσο-

τέρων του ενός παρόχου καθορίζεται από κανόνες.

5.3 Επέκταση Χρήσης του Ολοκληρωμένου Συστήματος Ασφάλειας και Προστασίας της Ιδιωτικότητας στο Διαδίκτυο των Πραγμάτων

5.3.1 Η Τεχνολογία Blockchain και το Διαδίκτυο των Πραγμάτων

Το Blockchain σχεδιάστηκε αρχικά ως κατανεμημένη δομή δεδομένων με στόχο τη διατήρηση ενός δημόσιου λογιστικού βιβλίου για την καταχώρηση συναλλαγών κρυπτονομισμάτων Bitcoin και, στη συνέχεια, γενικεύτηκε έτσι ώστε κάθε συναλλαγή να περιλαμβάνει δεδομένα, καθώς και κώδικα μηχανής για προγράμματα ηλεκτρονικών υπολογιστών, όπως είναι για παράδειγμα το Ethereum [115]. Με απλά λόγια, μια αλυσίδα από μπλοκ είναι μία συνδεδεμένη λίστα επικυρωμένων μπλοκ που έχουν παραταχθεί χρονολογικά. Τα μπλοκ έχουν ένα μοναδικό αναγνωριστικό 256 bit που υπολογίζεται από το κρυπτογραφικό άθροισμα ελέγχου του περιεχομένου του καθενός. Κάθε μπλοκ αποτελείται από μια επικεφαλίδα με πληροφορίες σχετικά με την ημερομηνία και την ώρα που πραγματοποιήθηκε η συναλλαγή, καθώς και από την ίδια τη συναλλαγή που αντιστοιχεί σε μια πράξη σε συγκεκριμένα δεδομένα. Οι συναλλαγές εκτελούνται και επικυρώνονται με βάση προσυμφωνημένα συμβόλαια και scripts, βάσει συγκεκριμένου συνόλου κανόνων. Επομένως, η τεχνολογία blockchain προσφέρει έναν αξιόπιστο τρόπο διαμοιρασμού συγκεκριμένου όγκου δεδομένων, χωρίς να είναι απαραίτητη μια κεντρική ενδιάμεση οντότητα.

Είναι γεγονός ότι ένας ταχέως αυξανόμενος αριθμός εταιρειών στρέφεται στην τεχνολογία blockchain, προσπαθώντας να την ενσωματώσει σε ήδη υπάρχουσες λύσεις. Στην πραγματικότητα, πολλοί είναι εκείνοι που αναρωτιούνται αν αυτή η αναδυόμενη τεχνολογική τάση ταιριάζει σε όλους τους τομείς, τις επιχειρήσεις και τις λύσεις λογισμικού. Όπως προτείνεται σε μερικά άρθρα και ερευνητικές εργασίες [116][43], υπάρχουν επτά βασικές απαιτήσεις τις οποίες ένα έργο, ένα προϊόν ή μία ιδέα πρέπει να ικανοποιεί ώστε η ενσωμάτωση της εν λόγω τεχνολογίας να μην είναι άσκοπη και περιττή. Αυτές οι απαιτήσεις θα μπορούσαν να συνοψιστούν στον εξής κανόνα: "υπάρχει ανάγκη για μια άμεσα επαληθεύσιμη και προσβάσιμη κοινή βάση δεδομένων μεταξύ πολλών οντοτήτων που θέλουν να αλληλεπιδρούν μεταξύ τους με αξιόπιστο τρόπο". Η πρόταση αυτή εμμέσως προβάλλει τα πλεονεκτήματα της τεχνολογίας blockchain, αλλά η περαιτέρω εξέταση της τελευταίας οδηγεί αναπόφευκτα και στην ανακάλυψη των μειονεκτημάτων της.

Στην πραγματικότητα, τα blockchains δημιουργούν μια σειρά πρακτικών προβλημάτων και ειδικότερα όσον αφορά στην ενσωμάτωσή τους στο IoT. Πρώτα απ'

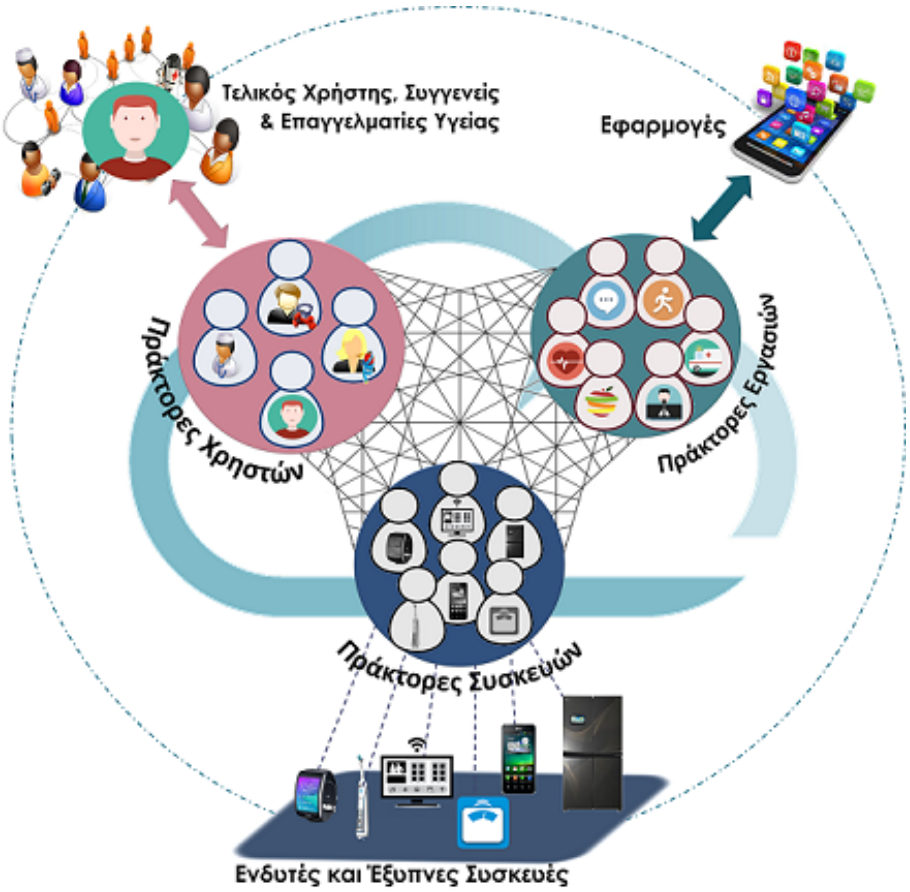
όλα, κάθε διαδικασία συναλλαγής και εξόρυξης μπλοκ αλυσίδας επιβάλλει περιορισμούς ως προς το χρόνο εκτέλεσης και ολοκλήρωσής τους, επεξεργασίας αλλά και κατανάλωσης πόρων. Δεύτερον, παρόλο που διασφαλίζεται η ακεραιότητα και η διαθεσιμότητα των δεδομένων, η διαφανής φύση αυτής της τεχνολογίας μπορεί να επηρεάσει άμεσα την ιδιωτικότητα και την εμπιστευτικότητα των δεδομένων του χρήστη. Επιπλέον, η εγγυημένη αυτονομία κάθε συμμετέχοντος κόμβου του δικτύου blockchain απαιτεί επιπλέον δυνατότητες επεξεργασίας και υψηλή κατανάλωση ενέργειας. Ο απαιτούμενος ελεύθερος αποθηκευτικός χώρος αποτελεί, επίσης, ένα κρίσιμο ζήτημα, καθώς το blockchain συνιστά βασικά ένα μηχανισμό αναπαραγωγής δεδομένων που αποθηκεύει πολλά αντίγραφα των συναλλαγών που πραγματοποιούνται σε όλο το δίκτυο.

Έτσι, λαμβανομένων υπόψη όλων των προαναφερθεισών πτυχών της τεχνολογίας blockchain, προκύπτει ένα απλό ερώτημα: είναι δυνατόν να συνδυαστεί η τεχνολογία blockchain με το IoT, δεδομένων όλων των περιορισμών της συγκεκριμένης τεχνολογίας που παρουσιάστηκαν παραπάνω καθώς και τις περιορισμένες δυνατότητες των περισσότερων συσκευών ενός IoT; Όσον αφορά στα ζητήματα ασφάλειας και ιδιωτικότητας του blockchain, θα μπορούσαμε να πούμε ότι, σε συνδυασμό με ισχυρούς κρυπτογραφικούς μηχανισμούς, η τεχνολογία αυτή θα μπορούσε να αποτελέσει μια ασφαλή μέθοδο πρόσβασης σε δεδομένα, ακόμα και σε ευαίσθητα προσωπικά δεδομένα, όπως αυτά που σχετίζονται με την υγεία. Αλλά τι γίνεται με την απαιτούμενη ενεργειακή και επεξεργαστική απόδοση των έξυπνων συσκευών; Σε περίπτωση που τα δεδομένα που συλλέγονται και ανταλλάσσονται μεταξύ των οντοτήτων του συστήματος πρέπει να επεξεργαστούν άμεσα και να μεταδοθούν, πώς μπορεί να μην αποτελέσει πρόβλημα η χρονική καθυστέρηση που προκαλείται κατά την εξόρυξη μπλοκ αλυσίδων;

5.3.2 Περίπτωση Χρήσης: Συνεργατικό Περιβάλλον Διαχείρισης Δεδομένων Υγείας και Δεικτών Ευημερίας

Επιστρέφοντας στην περίπτωση χρήσης του Health Avatar, προκειμένου να αντιμετωπιστούν πρακτικά όλα τα ζητήματα που συζητήθηκαν στις δύο προηγούμενες ενότητες, αντίθετα με άλλες παρόμοιες ερευνητικές εργασίες [117][118], η πλατφόρμα του Health Avatar αξιοποιεί έξυπνους πράκτορες λογισμικού για την εκπροσώπηση οντοτήτων του IoT στον κυβερνοχώρο. Πιο συγκεκριμένα, όπως απεικονίζεται στο Σχήμα 24, το Επίπεδο Μεσισμικού του οικοσυστήματος Health Avatar εκμεταλλεύεται τις λειτουργίες που προσφέρονται από δύο παραδείγματα IoT που ενδυναμώνουν το τρέχον με ευφυΐα και κοινωνικές ικανότητες, που είναι το *Γνωσιακό Διαδίκτυο των Πραγμάτων* (Cognitive Internet of Things – CIoT) και το *Κοινωνικό Διαδίκτυο των Πραγμάτων* (Social Internet of Things – SIoT), αντίστοιχα. Όπως παρουσιάζεται στο [119], η ιδέα του CIoT αφορά στην ενσωμάτωση γνωστικών και συνεργατικών

μηχανισμών για την παροχή έξυπνων υπηρεσιών και τη βελτίωση επιδόσεων στο IoT, ενώ το SIoT αφορά στις κοινωνικές σχέσεις που μπορούν να δημιουργηθούν μεταξύ των αντικειμένων και επιτρέπουν την ουσιαστική αλληλεπίδραση μεταξύ τους [120]. Επομένως, το Επίπεδο Μεσισμικού του συστήματος Health Avatar βασίζεται στη χρήση πρακτόρων που επιτρέπουν τη συνεργασία μεταξύ ψηφιακών και φυσικών αντικειμένων, έτσι ώστε να ανταλλάσσουν δεδομένα και να επιτυγχάνονται οι στόχοι τους για την παροχή υπηρεσιών.



Σχήμα 24: Έξυπνοι Πράκτορες που Συνιστούν το Μεσισμικό της Πλατφόρμας του Health Avatar

Από την άποψη της ασφάλειας και της ιδιωτικότητας, η χρήση πρακτόρων λογισμικού θεωρείται πλεονεκτική, καθώς με αυτόν τον τρόπο: (α) αντιμετωπίζονται πιθανά ζητήματα ανεπάρκειας που προκαλούνται εξαιτίας της χαμηλής υπολογιστικής ισχύος των έξυπνων συσκευών που εμπλέκονται στο IoT· (β) ο σχηματισμός κατανεμημένων, αξιόπιστων ομοσπονδιών έξυπνων αντικειμένων που σχετίζονται μέσω κοινωνικών συνδέσεων προσφέρει δυνατότητα πλοήγησης στο δίκτυο για αποτελεσματική και κλιμακούμενη εύρεση υπηρεσιών, επιτρέποντας επίσης τη διαλειτουργικότητα και τη συνεργασία μεταξύ τους με αξιόπιστο τρόπο· (γ) δεν υπάρχει ένα και μοναδικό σημείο για τη συγκέντρωση δεδομένων, δηλ. μια κεντρική συσκευή (hub), που συλλέγει δεδομένα από πολλούς αισθητήρες και συσκευές, ούτε μια κε-

ντρική υποδομή που φιλοξενεί τις υποκείμενες οντότητες διαχείρισης δεδομένων και τα αποθετήρια αυτών.

Όπως απεικονίζεται στο Σχήμα 24, υπάρχουν τρία είδη γνωσιακών πρακτόρων: (α) Οι *Πράκτορες Συσκευών* (Device Agents) που συνιστούν τις ψηφιακές αναπαραστάσεις κάθε φυσικής συσκευής που συνδέεται στο σύστημα, όπου κάθε πράκτορας αντιστοιχεί σε μία μόνο συσκευή και διαχειρίζεται τη λογική που συνδέεται με τη λειτουργικότητά της, καθώς και τις αντίστοιχες λειτουργίες επικοινωνίας· (β) Οι *Πράκτορες Χρηστών* (Human Agents) που αποτελούν τις μοναδικές ψηφιακές αναπαραστάσεις ανθρώπων που κατέχουν ενδυτές και άλλες έξυπνες συσκευές και ενδιαφέρονται επίσης να χρησιμοποιήσουν εξατομικευμένες υπηρεσίες για την παρακολούθηση και τη διασφάλιση της ευημερίας τους· (γ) Οι *Πράκτορες Εργασιών* (Task Agents) που εκπροσωπούν εφαρμογές που παρέχονται στον χρήστη και αφορούν στην υγεία, οι οποίες απαιτούν συλλογή και επεξεργασία βιομετρικών δεδομένων του χρήστη, ώστε να προσφέρουν τις επιθυμητές υπηρεσίες βελτίωσης της ευημερίας του. Με βάση τη φύση της πλατφόρμας SIoT, οι προαναφερθέντες πράκτορες σχηματίζουν σχέσεις κάτω από συγκεκριμένους κανόνες, διευθετώντας, κατ' αυτόν τον τρόπο, τα όποια ζητήματα διαλειτουργικότητας προκύπτουν μέσω της συνεργασίας ετερογενών οντοτήτων του IoT.

Επιπρόσθετα, δεδομένης της υιοθέτησης του παραδείγματος SIoT, υποστηρίζονται οι ακόλουθοι πέντε τύποι φιλίας μεταξύ των έξυπνων οντοτήτων της πλατφόρμας: (α) *Σχέση Ιδιοκτησίας Αντικειμένου* (Ownership Object Relationship) όπου συσκευές που ανήκουν στον ίδιο χρήστη συνδέονται μέσω αυτού του τύπου σχέσης· (β) *Γονική Σχέση Αντικειμένου* (Parental Object Relationship) που αφορά αντικείμενα που ανήκουν στην ίδια παρτίδα παραγωγής· (γ) *Σχέση Συνεγκατάστασης Αντικειμένων* (Co-location Object Relationship) που περιγράφει τη σχέση μεταξύ συσκευών που βρίσκονται στην ίδια περιοχή· (δ) *Σχέση Συνεργασίας Αντικειμένων* (Co-work Object Relationship) όπου συνδέονται συσκευές που συνεργάζονται μεταξύ τους προς ένα κοινό στόχο· (γ) *Κοινωνική Σχέση Αντικειμένων* (Social Object Relationship) που χαρακτηρίζει σχέσεις που δημιουργούνται μεταξύ αντικειμένων είτε λόγω της συχνής τους επικοινωνίας είτε επειδή οι ιδιοκτήτες τους έρχονται σε επαφή συχνά. Με βάση την περιγραφή των δύο παραδειγμάτων IoT που χρησιμοποιούνται στο σύστημα του Health Avatar, το επίπεδο μεσισμικού είναι υπεύθυνο για τη διαχείριση των κοινωνικών αλληλεπιδράσεων μεταξύ των προαναφερθέντων έξυπνων πρακτόρων, αντιμετωπίζοντας κατ 'αυτόν τον τρόπο τα ζητήματα διαλειτουργικότητας που προκύπτουν από τη συνεργασία των ετερογενών και έξυπνων οντοτήτων ενός Διαδικτύου των Πάντων που ενσωματώνει ανθρώπους, διαδικασίες, δεδομένα και συσκευές [121].

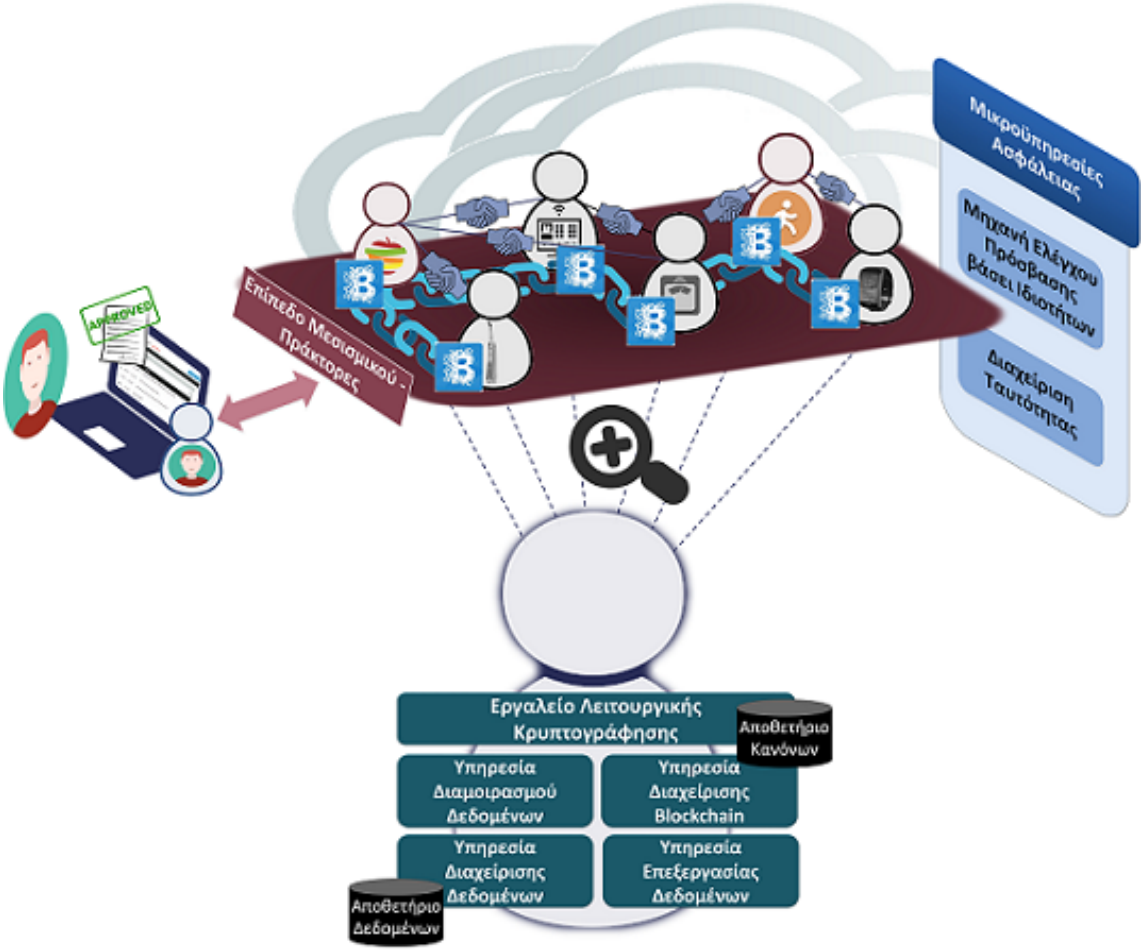
Μεταξύ των ενσωματωμένων μηχανισμών προστασίας δεδομένων και ασφάλειας της αρχιτεκτονικής του συστήματος, υπάρχουν μηχανισμοί που εξασφαλίζουν την εξακρίβωση της ταυτότητας των επιμέρους οντοτήτων που συμμετέχουν στο σύστημα, καθώς και λεπτομερή έλεγχο πρόσβασης. Ο μηχανισμός ελέγχου πρόσβασης

που χρησιμοποιείται είναι επεκτάσιμος, βασίζεται στις ιδιότητες των προαναφερθεισών οντοτήτων και στην επίγνωση χωρικού και χρονικού πλαισίου (context-aware), ενώ καθορίζονται πολιτικές σχετικά με τον τρόπο και για ποιο σκοπό επιτρέπεται η πρόσβαση στα δεδομένα. Μέσω μιας φιλικής προς το χρήστη γραφικής διεπαφής (Graphical User Interface – GUI), ο τελικός χρήστης «τοποθετείται» στο κέντρο της ροής δεδομένων καθώς ελέγχει τα δεδομένα και τον τρόπο με τον οποίο χρησιμοποιούνται τα τελευταία. Κάθε χρήστης είναι σε θέση να καθορίσει τις προτιμήσεις του για την προστασία των δεδομένων του με τη μορφή κανόνων, λαμβανομένων υπόψη παραμέτρων πλαισίου, χαρακτηριστικών και ιδιοτήτων των εμπλεκόμενων οντοτήτων, καθώς και γεγονότων που μπορεί να συμβούν. Οι ρόλοι των δραστών του συστήματος (αιτούντες πρόσβαση) αντιστοιχούν στα τρία είδη πρακτόρων που υπάρχουν στο Επίπεδο Μεσισμικού της πλατφόρμας, ενώ οι συνδέσεις μεταξύ τους καλύπτονται πλήρως από τους πέντε τύπους φιλίας, οι οποίοι αναφέρθηκαν προηγουμένως.

Όσον αφορά στην προστασία των δεδομένων στην πρωτογενή αλλά και στην εμπλουτισμένη μορφή τους, η αρχιτεκτονική ασφάλειας αξιοποιεί τις πρόσφατες εξελίξεις στην κρυπτογραφία και συγκεκριμένα τη Λειτουργική Κρυπτογράφηση [122], όπου η αποκρυπτογράφηση αποκαλύπτει μια συγκεκριμένη λειτουργία των κρυπτογραφημένων δεδομένων και τίποτα παραπάνω. Με αυτόν τον τρόπο, τα δεδομένα που εμπλέκονται στις συναλλαγές αυτές ενσωματώνουν πολιτικές πρόσβασης, μειώνοντας έτσι την ανάγκη για αξιόπιστα συστήματα αποθήκευσης και πολύπλοκα συστήματα διαχείρισης πολιτικών πρόσβασης, παρέχοντας έτσι εμπιστευτικότητα και εξασφαλίζοντας τη λήψη απόφασης εξουσιοδότησης σε μη πραγματικό χρόνο (offline), με τρόπο αποτελεσματικό για την επεξεργασία τέτοιων δεδομένων, έχοντας ως κύριο στόχο την προστασία της ιδιωτικότητας. Η Λειτουργική Κρυπτογράφηση ενσωματώνει πολλές προηγμένες έννοιες κρυπτογράφησης, όπως, για παράδειγμα, την Κρυπτογράφηση βάσει Ιδιοτήτων (CP-ABE), μέσω της οποίας τα δεδομένα κρυπτογραφούνται χρησιμοποιώντας την ίδια την πολιτική ελέγχου πρόσβασης ως κλειδί κρυπτογράφησης. Δηλαδή, αντί των αποφάσεων πρόσβασης σε πραγματικό χρόνο, οι κανόνες πρόσβασης περιέχονται στα ίδια τα κρυπτογραφημένα δεδομένα.

Μετά τις πρόσφατες ερευνητικές εξελίξεις ως προς την αποκεντρωμένη και ανοιχτή τεχνολογία blockchain, στην οποία βασίζεται η λειτουργία συστημάτων διαχείρισης κρυπτονομισμάτων, η υιοθέτησή της στον τομέα της ασφάλειας και στο Διαδίκτυο των Πραγμάτων είναι αναπόφευκτη. Αυτό είναι περισσότερο εμφανές στην περίπτωση εφαρμογών και υπηρεσιών που σχετίζονται με προσωπικές πληροφορίες, όπως στην Ηλεκτρονική Υγεία που χαρακτηρίζεται από μεγάλες απαιτήσεις και περιορισμούς στον σχεδιασμό και στην παροχή υπηρεσιών στους πολίτες. Συνεπώς, εξετάζεται η χρήση της τεχνολογίας blockchain κατά την ανταλλαγή δεδομένων, προκειμένου να διασφαλιστεί η προστασία από τυχόν διαρροή δεδομένων. Η αρχιτεκτονική που παρουσιάζουμε εν συντομία εδώ προσφέρει τη βάση πάνω στην

οποία μπορεί να βασιστεί ο σχεδιασμός, η ανάπτυξη και η επιτυχής λειτουργία ενός συστήματος παρακολούθησης της ευημερίας του ατόμου με επίγνωση της ιδιωτικότητας.



Σχήμα 25: Επιμέρους Αρχιτεκτονικές Οντότητες των Πρακτόρων στο Επίπεδο Μεσισμικού

Ο ρόλος της τεχνολογίας blockchain είναι πλέον σαφής, καθώς χρησιμοποιείται για να εξασφαλιστεί η αξιοπιστία του συστήματος. Καθώς η πληροφορία θεωρείται πολύτιμο αγαθό στη σημερινή οικονομία, η αξία των προσωπικών δεδομένων είναι άμεσα συγκρίσιμη με αυτήν των χρημάτων. Στην περίπτωσή μας, προκειμένου να αποφευχθεί η ανάγκη μιας έμπιστης κεντρικής αρχής και να διασφαλιστεί ο σεβασμός στην ιδιωτικότητα των χρηστών, ένα – σχεδόν αποκεντρωμένο, καθώς ο ιδιοκτήτης των έξυπνων συσκευών ελέγχει και πιστοποιεί τη συμμετοχή των πρακτόρων εργασιών και συσκευών στο δίκτυο – απαραβίαστο (tamper-proof) και ιδιωτικό blockchain επιτρέπει τον αυτόματο έλεγχο των δεδομένων (auditing), καθώς παρακολουθεί την ανταλλαγή των δεδομένων μεταξύ των διαφόρων πρακτόρων του συστήματος, ενσωματώνοντας ταυτόχρονα πληροφορίες σχετικά με την αντίστοιχη πηγή δεδομένων καθώς και κανόνες για την πρόσβαση σε αυτά. Έτσι, αυξάνεται η

διαφάνεια των διαδικασιών και προσφέρεται ισχυρή προστασία της ιδιωτικότητας, καθώς ένα ιδιωτικό, δίκτυο ομότιμων κόμβων (p2p) παρακολουθεί τις συναλλαγές, όπου κάθε κόμβος διατηρεί ένα ακριβές αντίγραφο του blockchain. Η ιδιοκτησία και η ανταλλαγή δεδομένων ρυθμίζονται μέσω έξυπνων συμβολέων, όπου η επαλήθευση της ορθότητας του τρόπου εκτέλεσης αυτών των διαδικασιών γίνεται βάσει των πολιτικών πρόσβασης που έχει ορίσει ο χρήστης.

Το Σχήμα 25 απεικονίζει το Επίπεδο Μεσισμικού του οικοσυστήματος Health Avatar με τους πράκτορές του, εστιάζοντας κυρίως στις λειτουργικές οντότητες των τελευταίων που αναλαμβάνουν σημαντικά καθήκοντα, συμπεριλαμβανομένων αυτών που είναι υπεύθυνες για τον έλεγχο και την προστασία των δεδομένων, τη διαχείριση πολιτικών, την επεξεργασία και εκτίμηση αιτημάτων πρόσβασης, τη λήψη και επιβολή αποφάσεων εξουσιοδότησης, βάσει των προσφερόμενων λειτουργιών της λύσης που περιγράφεται παραπάνω. Αξιοποιώντας προηγμένους μηχανισμούς ασφάλειας και προστασίας της ιδιωτικότητας, το παρόν πλαίσιο ασφάλειας προσαρμοσμένο στην αρχιτεκτονική του συστήματος Health Avatar προτείνει μια ολιστική λύση για την παροχή εξατομικευμένων υπηρεσιών παρακολούθησης και βελτίωσης της ευημερίας του ατόμου με τρόπο ασφαλή και με γνώμονα την προστασία της ιδιωτικότητας, αξιοποιώντας σημαντικές γνώσεις που αντλούνται από διάφορες πηγές δεδομένων (συμπεριλαμβανομένων έξυπνων αισθητήρων και συσκευών) με σεβασμό πάντα στην Ιδιωτικότητά του.

Κεφάλαιο 6

Συμπεράσματα – Μελλοντική Εργασία

Ο βασικός στόχος ενός ολοκληρωμένου σχεδίου ασφάλειας και προστασίας της ιδιωτικότητας είναι η υιοθέτηση όλων των απαιτούμενων τεχνικών, διαδικαστικών, νομικών και οργανωτικών μέτρων που απαιτούνται για την προστασία των Πληροφοριακών Συστημάτων (Π.Σ.) και των δεδομένων που διατηρούν και επεξεργάζονται από τις απειλές στις οποίες εκτίθενται ή/και για την ελαχιστοποίηση των όποιων επιπτώσεων από δυνητικά περιστατικά ασφάλειας. Το σχέδιο ασφάλειας πρέπει να λαμβάνει υπόψη του τις εξής γενικές διαπιστώσεις:

- Η ασφάλεια των Π.Σ. εξαρτάται από πολλούς παράγοντες και δεν είναι, ούτε αποκλειστικά, ούτε κυρίως, τεχνικό ζήτημα.
- Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος.
- Για κάθε επίπεδο ασφάλειας υπάρχει ένα αντίστοιχο κόστος που θα πρέπει να καταβληθεί για την επίτευξή του.
- Στο πλαίσιο της γενικής αρχής της αναλογικότητας, τα μέτρα προστασίας που θα ληφθούν θα πρέπει να αντιστοιχούν στο επίπεδο και τη φύση των πραγματικών κινδύνων που αντιμετωπίζει το πληροφοριακό σύστημα.

Επιπρόσθετα, ιδιαίτερα σημαντική είναι η ευαισθητοποίηση και η ανάπτυξη της λεγόμενης «κουλτούρας ασφάλειας» από τους χρήστες των πληροφοριακών συστημάτων και τους πολίτες γενικότερα.

Στην παρούσα διδακτορική διατριβή, για την προστασία συστημάτων σε ετερογενή κατανεμημένα περιβάλλοντα από μη εξουσιοδοτημένη πρόσβαση, προδιαγράφεται ένα εξειδικευμένο πλαίσιο ασφάλειας για τη διαχείριση, επεξεργασία και αξιολόγηση των αιτημάτων πρόσβασης στους πόρους του. Στα σενάρια που εξετάστηκαν, λόγω της ευαίσθητης φύσης των δεδομένων, το ολοκληρωμένο σύστημα ασφάλειας και προστασίας της ιδιωτικότητας δεν περιορίστηκε στην εφαρμογή σύγχρονων πρακτικών, καθώς ενσωματώνει μία εμπλουτισμένη Υπηρεσία Ασφάλειας, η

οποία προσφέρει έλεγχο πρόσβασης και προστασία δεδομένων με έμφαση στην ιδιωτικότητα βάσει ενός σημασιολογικού μοντέλου πολιτικών. Ο σχεδιασμός και η ανάπτυξη της ολοκληρωμένης αρχιτεκτονικής ασφάλειας του συστήματος πραγματοποιήθηκε με τρόπο τέτοιο ώστε η τελευταία να εγγυάται την προστασία της ιδιωτικότητας του χρήστη, καθώς και να σέβεται και να τηρεί το αντίστοιχο νομικό και κανονιστικό πλαίσιο, περιλαμβάνοντας κανόνες που αφορούν όλες τις υποκείμενες διαδικασίες συλλογής, αποθήκευσης, μετάδοσης και επεξεργασίας των δεδομένων αυτών.

Αρχικά, εξετάστηκαν οι απαιτήσεις ασφάλειας και ιδιωτικότητας συστημάτων μεγάλης κλίμακας, ενώ αναλύθηκαν συγκεκριμένα οι τομείς διαχείρισης παραγωγής, ηλεκτρονικής διακυβέρνησης και παρακολούθησης της υγείας του ατόμου, μελετώντας τις τεχνολογίες που χρησιμοποιούνται σε αυτά για την κάλυψη αναγκών ασφάλειας, εντοπίζοντας έπειτα τις ελλείψεις τους. Στη συνέχεια, παρουσιάστηκε η αρχιτεκτονική του ολοκληρωμένου συστήματος ασφάλειας και προστασίας της ιδιωτικότητας, η οποία αποτελεί και το κύριο αντικείμενο της διατριβής. Συγκεκριμένα, περιγράφηκαν το πλαίσιο ελέγχου πρόσβασης, καθώς και ο μηχανισμός κρυπτογράφησης που χρησιμοποιούνται ως βάση λειτουργίας του συστήματος. Έπειτα, παρουσιάστηκε ο τρόπος με τον οποίο η συνιστώσα υπηρεσία ασφάλειας και προστασίας ιδιωτικότητας του συστήματος μπορεί να ενσωματωθεί σε οποιοδήποτε περιβάλλον, κάτι που αποδεικνύεται μέσως της προσαρμογής της προκειμένου αυτή να εφαρμοστεί και να ελεγχθεί σε σενάρια των τριών προαναφερθέντων τομέων.

Το πρώτο σενάριο στο οποίο εφαρμόσθηκε η ευφυής υπηρεσία ασφάλειας και προστασίας της ιδιωτικότητας είναι αυτό της διαχείρισης παραγωγής. Συγκεκριμένα, εξετάστηκε η αρχιτεκτονική ενός ευφυούς συστήματος διαχείρισης παραγωγής, το οποίο επιτρέπει την εύκολη ενσωμάτωση πολλαπλών λειτουργιών και συσκευών ακολουθώντας τις ανάγκες των διαδικασιών παραγωγής. Το σύστημα αυτό προσφέρει μία σουίτα ευφυών εργαλείων διαχείρισης παραγωγής που αφορούν λειτουργίες σχετικές με την προορατική συντήρηση των μηχανημάτων παραγωγής, τον επιχειρησιακό χρονοπρογραμματισμό και τον στρατηγικό σχεδιασμό των διαδικασιών παραγωγής. Καθώς όλη η υποδομή ενσωματώνει διαφορετικές στρατηγικές, αρχιτεκτονικές και τεχνολογίες που συνδυάζονται και αλληλεπιδρούν, τα σημαντικά δεδομένα σχετικά με τα βιομηχανικά περιουσιακά στοιχεία είναι ευάλωτα σε διάφορες απειλές και επιθέσεις. Για το λόγο αυτό, σχεδιάστηκε και αναπτύχθηκε μια επιμέρους υπηρεσία του συστήματος διαχείρισης παραγωγής, λαμβάνοντας υπόψη τις ειδικές απαιτήσεις ασφάλειας της υποδομής. Λόγω της πληθώρας των οντοτήτων που εμπλέκονται στο σύστημα, υπεύθυνων για τη συλλογή, παραγωγή και τροποποίηση των δεδομένων, χρησιμοποιήθηκαν ένα ισχυρό κρυπτογραφικό εργαλείο και ένας κλιμακώσιμος μηχανισμός ελέγχου πρόσβασης για να εξασφαλιστεί η αυθεντικότητα των δεδομένων και η αξιοπιστία του συστήματος.

Εν συνεχεία, παρουσιάστηκε το πλαίσιο που σχεδιάστηκε και αναπτύχθηκε

για την παροχή μίας ολοκληρωμένης, ασφαλούς πλατφόρμας ανάπτυξης και εκτέλεσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, διασφαλίζοντας την ιδιωτικότητα των χρηστών. Η προαναφερθείσα κατανεμημένη πλατφόρμα εκτείνεται σε όλους τους φορείς που συμμετέχουν στην αλυσίδα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης και είναι υπεύθυνη για τη διαχείριση της μετάδοσης, αποθήκευσης και επεξεργασίας των δεδομένων σε ένα ασφαλές περιβάλλον με σεβασμό στην ιδιωτικότητα. Οι βασικές αρχές που αξιοποιήθηκαν για τη διασφάλιση ασφαλών συναλλαγών είναι η χρήση προηγμένων κρυπτογραφικών σχημάτων που δεν έχουν χρησιμοποιηθεί ποτέ στην παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης. Η έρευνα που πραγματοποιήθηκε κατά τη διάρκεια της διατριβής για την εφαρμογή της προσέγγισης που ακολουθήθηκε στον τομέα της Ηλεκτρονικής Διακυβέρνησης επικεντρώθηκε στις ιδιαίτερες απαιτήσεις του τομέα αυτού. Αφού διερευνήθηκε ο ρόλος της Ηλεκτρονικής Διακυβέρνησης, καθώς και ο τρόπος με τον οποίο οι παρεχόμενες υπηρεσίες αυτής διατίθενται στους πολίτες, μελετήθηκε πληθώρα περιπτώσεων χρήσης που αξιολογήθηκαν βάσει συγκεκριμένων κριτηρίων-απαιτήσεων ασφάλειας και ιδιωτικότητας, καταλήγοντας με τον τρόπο αυτό στα σενάρια χρήσης που απαιτούν την ικανοποίηση των περισσοτέρων αναγκών ασφαλείας συγκριτικά με τις υπόλοιπες.

Εν τέλει, παρουσιάστηκε ο τρόπος εφαρμογής της υπηρεσίας ασφάλειας σε μία πλατφόρμα παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης, συμπεριλαμβανομένων επιμέρους τμημάτων αυτής, καθώς και των σημασιολογικών μοντέλων στα οποία βασίζεται η λειτουργία της. Οι στόχοι που επιδιώχθηκαν είναι: (α) η αξιοποίηση πρόσφατων ερευνητικών τάσεων στους τομείς της κρυπτογραφίας και του ελέγχου πρόσβασης, κυρίως αυτών της Κρυπτογράφησης Βάσει Ιδιοτήτων και του Σημασιολογικού Ελέγχου Πρόσβασης Βάσει Ιδιοτήτων με Επίγνωση της Ιδιωτικότητας, εξασφαλίζοντας έτσι την εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται μεταξύ υπηρεσιών, (β) παροχή πλήρους διαλειτουργικότητας με τα ευρωπαϊκά πρότυπα μοντελοποίησης πληροφορίας χρησιμοποιώντας σημασιολογική γνώση, (γ) ανάπτυξη υπηρεσίας ασφάλειας ως συνιστώσα οντότητα κατανεμημένης πλατφόρμας ηλεκτρονικής διακυβέρνησης που φιλοξενεί όλες τις παρεχόμενες ηλεκτρονικές υπηρεσίες δημόσιων φορέων, υπεύθυνη για την εφαρμογή του συνόλου των διατάξεων περί ασφάλειας και ιδιωτικότητας, συμπεριλαμβανομένης της αποθήκευσης των πληροφοριών, της διαλειτουργικότητας με αντίστοιχες πλατφόρμες πιστοποίησης, αδειοδότησης και ελέγχου πρόσβασης και, τέλος, (δ) παροχή κατάλληλων διεπαφών για την προδιαγραφή κανόνων πρόσβασης, για τον σχεδιασμό ροών εργασιών και τον έλεγχο συμμόρφωσης αυτών με το υφιστάμενο νομικό και κανονιστικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Έπειτα, η προσέγγιση που ακολουθείται στην παρούσα διατριβή για τη διασφάλιση της ιδιωτικότητας εφαρμόστηκε σε ένα σενάριο παρακολούθησης της υγείας του ατόμου. Συγκεκριμένα, εξετάστηκε το σύστημα Health Avatar, όπου τα avatars αποτελούν την ψηφιακή αναπαράσταση των χρηστών του Διαδικτύου σε διαδικτυα-

κούς εικονικούς κόσμους (digital twins). Μπορούν να συλλέγουν δεδομένα μέσω διαφόρων προσωπικών συσκευών των χρηστών (π.χ. έξυπνων βιομετρικών εφαρμογών κινητού τηλεφώνου, αισθητήριων και ενδυτών συσκευών ή/και υφιστάμενων συστημάτων ιατρικού περιεχομένου), να αποθηκεύουν και να ανταλλάσσουν πληροφορίες μεταξύ τους, σύμφωνα πάντα με τις προτιμήσεις ιδιωτικότητας των χρηστών που αντιπροσωπεύουν. Τα Health Avatars συντροφεύουν δια βίου τον άνθρωπο, συγκεντρώνοντας μακροχρόνια ακριβή δεδομένα, όπως αυτά που χαρακτηρίζουν τον τρόπο διαβίωσής του, το ιατρικό του ιστορικό, καθώς και άλλες προσωπικές του πληροφορίες, οι οποίες, ωστόσο, δεν αποτελούν ταυτοποιητικά στοιχεία για τον ίδιο, όπως, για παράδειγμα, η ηλικία του. Τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν σε πολλούς τομείς για ερευνητικούς και μη σκοπούς, έχοντας ως απώτερο στόχο τη βελτίωση της ποιότητας ζωής του ανθρώπου και την ενίσχυση της ευεξίας του. Ο εικονικός αυτός βοηθός του ατόμου, συνδυάζοντας την προαναφερθείσα ποικιλία δεδομένων με τις τακτικές μετρήσεις των ζωτικών του σημείων που λαμβάνονται από τις προσωπικές του συσκευές, και, σε συνδυασμό με άλλες σχετικές πληροφορίες, είναι σε θέση να δημιουργήσει προτάσεις για το χρήστη για τη βελτίωση της ευημερίας του.

Όσον αφορά στην ασφάλεια και στην προστασία των προαναφερθέντων δεδομένων, δεδομένου ότι, τα τελευταία χρόνια, η κοινή χρήση προσωπικών δεδομένων ενθαρρύνεται σημαντικά, απαραίτητη είναι η διασφάλιση προστασίας αυτών στο χρήστη. Έτσι, η παρούσα διδακτορική διατριβή προσφέρει την τεχνική λύση για την επίλυση ενός νομικού ζητήματος, αυτού της προστασίας της ιδιωτικότητας των χρηστών, τοποθετώντας τον άνθρωπο στο επίκεντρο της ροής δεδομένων και επιτρέποντάς του να αλληλεπιδρά με τα δεδομένα αυτά κατά τρόπο που διασφαλίζει την προστασία των προσωπικών του δεδομένων. Για τον λόγο αυτό, πραγματοποιήθηκε μελέτη των προσωπικών δεδομένων που συλλέγονται από το προαναφερθέν σύστημα, εξετάστηκαν αδυναμίες που εντοπίζονται στον τρόπο συλλογής και διάδοσης αυτών και αναλύθηκαν οι απαιτήσεις ασφάλειας και προστασίας της ιδιωτικότητας. Εν συνεχεία, η ευφυής υπηρεσία ασφάλειας επεκτάθηκε με τρόπο τέτοιο ώστε να καλύψει και την ανάγκη διασφάλισης εμπιστοσύνης μέσω της εφαρμογής της τεχνολογίας Blockchain, συμβάλλοντας μάλιστα στην αντιμετώπιση κάποιων ζητημάτων ασφάλειας και προστασίας δεδομένων που χαρακτηρίζουν την τελευταία μέσω ορισμένων τροποποιήσεων στον τρόπο λειτουργίας της. Μέσω της προαναφερθείσας υπηρεσίας πραγματοποιείται η λήψη αποφάσεων εξουσιοδότησης σε ό,τι αφορά τα αιτήματα πρόσβασης που λαμβάνονται από τις επιμέρους οντότητες της πλατφόρμας Health Avatar. Το υποκείμενο μοντέλο ελέγχου πρόσβασης λαμβάνει υπόψη τη ζωτική σημασία των δεδομένων υγείας και ευημερίας, ενώ οι κανόνες ελέγχου πρόσβασης προδιαγράφονται έχοντας ως βάση ένα σημασιολογικό μοντέλο πολιτικών. Η αρχιτεκτονική του συνολικού συστήματος ασφάλειας περιλαμβάνει μηχανισμούς κρυπτογράφησης των δεδομένων έχοντας πάντα ως πρωταρχικό στόχο την προστα-

σία της ιδιωτικότητας των χρηστών, καθώς και λειτουργίες διαχείρισης πολιτικών, επεξεργασίας και αξιολόγησης αιτημάτων πρόσβασης και λήψης αποφάσεων εξουσιοδότησης.

Η τρέχουσα και μελλοντική ερευνητική εργασία αφορά στη μελέτη του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), προκειμένου να εξαχθούν οι σχετικές απαιτήσεις και να τροποποιηθούν κατάλληλα τα επιμέρους συστατικά στοιχεία της αρχιτεκτονικής ασφαλούς συστήματος με επίγνωση της ιδιωτικότητας που παρουσιάστηκε στην παρούσα διδακτορική διατριβή. Συγκεκριμένα, βάσει των απαιτήσεων αυτών, αναμένεται να εμπλουτισθεί το σημασιολογικό μοντέλο πολιτικών πρόσβασης και, αντίστοιχα, να ενσωματωθούν νέες οντότητες στο εργαλείο σχεδιασμού ασφαλών ροών εργασιών SWORD μέσω της προδιαγραφής σχεδίων ιδιωτικότητας (privacy patterns), έτσι ώστε το τελευταίο να διευκολύνει σημαντικά τη μετάβαση των είδη υφιστάμενων συστημάτων και υπηρεσιών στη νέα εποχή που χαρακτηρίζεται από την επιβολή του νέου κανονισμού GDPR.

Επιπρόσθετα, απαραίτητη προϋπόθεση για την εξέλιξη της ευφυούς υπηρεσίας ασφάλειας που ενσωματώνει την τεχνολογία Blockchain είναι η εφαρμογή της σε πληθώρα κατανεμημένων συστημάτων μεγάλης κλίμακας, έτσι ώστε να εντοπιστούν ελλείψεις της και να μελετηθούν τρόποι κάλυψης αυτών [123]. Δεδομένων των υψηλών απαιτήσεων της τεχνολογίας Blockchain σε υπολογιστική ισχύ, ιδιαίτερη έμφαση θα δοθεί στην ενσωμάτωση μηχανισμών ασφάλειας και προστασίας της ιδιωτικότητας που θα επιβαρύνουν το λιγότερο δυνατό το εκάστοτε σύστημα που αξιοποιεί τη συγκεκριμένη τεχνολογία.

Τέλος, κρίνεται επιτακτική η εξέταση τρόπου αξιοποίησης κατανεμημένων τεχνικών Μηχανικής Μάθησης (Machine Learning) συνδυαστικά με τις τεχνολογίες Σημασιολογικού Ιστού, τον Ακροδιαδικτυακό Υπολογισμό (Edge Computing) και την τεχνολογία Blockchain. Σύντομα, οι αλγόριθμοι εκμάθησης μηχανών θα λειτουργούν στις συσκευές άκρων (π.χ. έξυπνες κινητές συσκευές). Έτσι, δεν θα μεταφορτώνονται ευαίσθητα δεδομένα στα υπολογιστικά νέφη και ο χρήστης θα έχει τον έλεγχο των προσωπικών του δεδομένων, ακολουθώντας τις οδηγίες του κανονισμού GDPR. Συγκεκριμένα, τα δεδομένα που εκπέμπονται από συσκευές IoT, τα οποία ενδέχεται να μην έχουν πρόσβαση στο Διαδίκτυο, και τα δεδομένα που παράγονται από διαδικτυακές υπηρεσίες (π.χ. Yahoo), θα συλλέγονται και θα υποβάλλονται σε επεξεργασία στο κινητό τηλέφωνο του χρήστη. Για τον λόγο αυτό, πρέπει να αναπτυχθούν αποδοτικές τεχνικές αναφορικά με τη διασφάλιση της ιδιωτικότητας στις υποκείμενες διαδικασίες. Η επέκταση του πλαισίου ασφάλειας και προστασίας ιδιωτικότητας που παρουσιάζεται στην παρούσα διδακτορική διατριβή, δεδομένων των τεχνολογιών που υιοθετεί, δύναται να ικανοποιήσει τις προαναφερθείσες και άλλες μελλοντικές απαιτήσεις για τη διασφάλιση ιδιωτικότητας σε έξυπνα κατανεμημένα περιβάλλοντα που χαρακτηρίζονται από ετερογένεια και διαχειρίζονται μεγάλο όγκο δεδομένων.

Βιβλιογραφία

[1] Rene Waslo, Tyler Lewis, Ramsey Hajj, and Robert Carton. Industry 4.0 and cybersecurity – Managing risk in an age of connected production. 2017.

[2] TNS opinion & political at the request of the European Commission. Special Eurobarometer 464a – Europeans' attitudes towards cyber security (report), September 2017.

[3] Altimeter. Consumer Perceptions of Privacy in the Internet of Things, June 2015.

[4] The European Commission. The EU General Data Protection Regulation (GDPR). [Online]. Available at: https://www.eugdpr.org/.

[5] Alan Westin. *Privacy and Freedom*. New York: Atheneum Press, 1967.

[6] The European Parliament and the Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[7] European Court of Human Rights. European Convention on Human Rights, 1994.

[8] Mike de Roode. Privacy Enhancing Technologies – A software engineering approach to design PETs. 2016.

[9] John Borking. *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*. CBP, 11 2003.

[10] Andrew S. Tanenbaum and Maarten van Steen. *Distributed Systems: Principles and Paradigms (2nd edition)*. Pearson Higher Education Inc. Press, 2007.

[11] Mohamed Firdhous. Implementation of Security in Distributed Systems – A Comparative Study. *International Journal of Computer Information Systems*, 2(2):1–6, 2012.

[12] George Coulouris, Jean Dollimore and Tim Kindberg, and Gordon Blair. *Distributed Systems: Concepts and Design (5th edition)*. Pearson, 2011.

[13] K.G. Srinivasa and Anil Kumar Muppalla. *Guide to High Performance Distributed Computing – Case Studies with Hadoop, Scalding and Spark*. Springer International Publishing, 2015.

[14] Mustafizur Rahman, Rajiv Ranjan, and Rajkumar Buyya. *Decentralization in Distributed Systems: Challenges, Technologies, and Opportunities*. IGI Global, 2012.

[15] Maarten van Steen, Guillaume Pierre, and Spyros Voulgaris. Challenges in very large distributed systems. *Journal of Internet Services and Applications*, 3(1):59–66, May 2012.

[16] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Technical report, NIST Special Publication 800-162, 2014.

[17] Daniel Servos and Sylvia L. Osborn. Current Research and Open Problems in Attribute-Based Access Control. *ACM Computing Surveys*, 49(4), January 2017.

[18] Organization for the Advancement of Structured Information Standards (OASIS). eXtensible Access Control Markup Language (XACML) Version 3.0, January 2013. [Online]. Available at: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf.

[19] Organization for the Advancement of Structured Information Standards (OASIS). OASIS eXtensible Access Control Markup Language (XACML) TC. [Online]. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[20] Dan Boneh, Amit Sahai, and Brent Waters. Functional Encryption: A New Vision for Public-Key Cryptography. *Communications of the ACM*, 55(11):56–64, November 2012.

[21] Dan Boneh, Amit Sahai, and Brent Waters. Functional Encryption: Definitions and Challenges. In Yuval Ishai, editor, *Theory of Cryptography*, pages 253–273, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[22] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to Play ANY Mental Game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 218–229, New York, NY, USA, 1987. ACM.

[23] Andrew C. Yao. Protocols for Secure Computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS '82, pages 160–164, Washington, DC, USA, 1982. IEEE Computer Society.

[24] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, pages 457–473, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[25] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pages 47–53, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[26] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 89–98, New York, NY, USA, 2006. ACM.

[27] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334, May 2007.

[28] Brent Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography – PKC 2011*, pages 53–70, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[29] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[30] Michael Stonebraker, Samuel Madden, Daniel J. Abadi, Stavros Harizopoulos, Nabil Hachem, and Pat Helland. The end of an architectural era (it's time for a complete rewrite). In *the 33rd International Conference on Very Large Data Bases (VLDB)*, pages 1150–1160, Vienna, Austria, 2007.

[31] James C. Corbett et al. Spanner: Google's Globally-Distributed Database. In *10th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 261–264, Hollywood, CA, USA, 2012.

[32] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *the 3rd USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pages 173–186, New Orleans, Louisiana, USA, 1999.

[33] Quang Hieu Vu, Mihai Lupu, and Beng Chin Ooi. *Peer-to-Peer Computing Principles and Applications*. Springer-Verlag Berlin Heidelberg, 2010.

[34] Ittay Eyal and Emin Gün Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. In *18th International Conference on Financial Cryptography and Data Security (FC)*, pages 436–454, Christ Church, Barbados, 2014.

[35] Kyle et al. Croman. On Scaling Decentralized Blockchains. In *Financial Cryptography and Data Security*, pages 106–125, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[36] Hyperledger. Blockchain technologies for business. [Online]. Available at: https://www.hyperledger.org/.

[37] Diego Ongaro and John Ousterhout. In Search of an Understandable Consensus Algorithm. In *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pages 305–319, Philadelphia, PA, 2014. USENIX Association.

[38] Leslie Lamport. Paxos Made Simple, Fast, and Byzantine. In Alain Bui and Hacène Fouchal, editors, *the 6th International Conference on Principles of Distributed Systems (OPODIS)*, volume 3 of *Studia Informatica Universalis*, pages 7–9, Reims, France, 2002. Suger, Saint-Denis, rue Catulienne, France.

[39] Ethcore. Parity: next generation ethereum browser. [Online]. Available at: https://www.parity.io/.

[40] Monax. Monax: The ecosystem application platfor. [Online]. Available at: https://monax.io/platform/db/.

[41] Oliver Wyman. Unlocking economic advantage with blockchain – A guide for asset managers.

[42] Goldman Sachs group. BLOCKCHAIN – Putting Theory into Practice, May 2016. [Online]. Available at: https://www.unlock-bc.com/news/2017-05-25/blockchain-putting-theory-into-practice.

[43] Gideon Greenspan. Avoiding the pointless blockchain project, November 2015. [Online]. Available at: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.

[44] BigchainDB GmbH. BigchainDB: The scalable blockchain database. [Online]. Available at: https://www.bigchaindb.com/.

[45] Richard G. Brown. Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, April 2016. [Online]. Available at: http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services.

[46] Stellar Development Foundation. Stellar – Move Money Across Borders Quickly, Reliably, And For Fractions Of A Penny. [Online]. Available at: https://www.stellar.org/.

[47] Ripple. Join RippleNet – The world's only enterprise blockchain solution for global payments. [Online]. Available at: https://ripple.com/.

[48] IOTA – The economy of things. [Online]. Available at: https://iota.org/.

[49] Ethereum Foundation. Decentralized Autonomous Organization. [Online]. Available at: https://www.ethereum.org/dao.

[50] Marko Vukolić. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In Jan Camenisch and Doğan Kesdoğan, editors, *Open Problems in Network Security*, pages 112–125, Cham, 2016. Springer International Publishing.

[51] Proof of Authority Chains. [Online]. Available at: https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains.

[52] Eugenia Papagiannakopoulou, Mariza Koukovini, Georgios V. Lioudakis, Joaquin Garcia-Alfaro, Dimitra I. Kaklamani, Iakovos S. Venieris, Frédéric Cuppens, and Nora Cuppens-Boulahia. A Privacy-Aware Access Control Model for Distributed Network Monitoring. *Computers & Electrical Engineering*, 39(7):2263—2281, October 2013.

[53] Tino M. Böhler. Industrie 4.0 - Smarte Produkte und Fabriken revolutionieren die Industrie. *Produktion Magazin*, 2012.

[54] Paulo Leitão, José Barbosa, Maria-Eleftheria C. Papadopoulou, and Iakovos S. Venieris. Standardization in Cyber-Physical Systems: The ARUM case. In *the Proceedings of 2015 IEEE International Conference on Industrial Technology (ICIT)*, pages 2988–2993, March 2015. Nominated to appear in IE Tech News (ITeN), a web-only publication of IEEE Industrial Electronics Society.

[55] S. Sands. Industry 4.0, What's in a Name? *Industrial Technology*, 2014.

[56] Ines Seixas and Paulo Leitao. Standards Compliance in Industrial Agents Applications. In *39th Annual Conference of the IEEE Industrial Electronics Society (IECON'13)*, 2013.

[57] FIPA, Foundation for Intelligent Physical Agents. [Online]. Available at: www.fipa.org.

[58] Vladimír Mařík, Michal Pěchouček, Pavel Vrba, and Václav Hrdonka. *Agent-based Manufacturing: Advances in the Holonic Approach*, chapter FIPA Standards and Holonic Manufacturing, pages 80–121. Springer Verlag, 2003.

[59] Bernhard Bauer and James Odell. UML 2.0 and Agents: How to Build Agent-Based Systems with the New UML Standard. *Journal of Engineering Applications of Artificial Intelligence*, 2005.

[60] The World Wide Web Consortium (W3C). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), April 2007. [Online]. Available at: http://www.w3.org/TR/soap12-part1/.

[61] The World Wide Web Consortium (W3C). SOAP Version 1.2 Part 2: Adjuncts (Second Edition), April 2007. [Online]. Available at: http://www.w3.org/TR/soap12-part2/.

[62] The World Wide Web Consortium (W3C). SOAP Version 1.2 Part 0: Primer (second edition), April 2007. [Online]. Available at: http://www.w3.org/TR/soap12-part0/.

[63] The World Wide Web Consortium (W3C). Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, June 2007. [Online]. Available at: http://www.w3.org/TR/wsdl20/.

[64] Organization for the Advancement of Structured Information Standards (OASIS). UDDI version 3.0.2, October 2004. [Online]. Available at: http://www.uddi.org/pubs/uddi_v3.htm.

[65] OASIS Service Oriented Architecture Reference Model Technical Committee. Reference Architecture Foundation for Service Oriented Architecture Version 1.0. Technical report, OASIS, 2012.

[66] The Open Group. SOA Reference Architecture. [Online]. Available at: http://www.opengroup.org/soa/source-book/soa_refarch/index.htm.

[67] The World Wide Web Consortium (W3C). Resource Description Framework, 2004. [Online]. Available at: https://www.w3.org/RDF.

[68] The World Wide Web Consortium (W3C). OWL Web Ontology Language Reference. W3C Recommendation, 2004. [Online]. Available at: https://www.w3.org/OWL/.

[69] The World Wide Web Consortium (W3C). XML Encryption Syntax and Processing. W3C Recommendation, 2002. [Online]. Available at: https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html.

[70] The World Wide Web Consortium (W3C). XML Signature Syntax and Processing (2nd Edition). W3C Recommendation, 2015. [Online]. Available at: https://www.w3.org/TR/xmldsig-core2/.

[71] Organization for the Advancement of Structured Information Standards (OASIS). OASIS Security Services (SAML) TC. [Online]. Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[72] National Institute of Standards and Technology (NIST). The NIST Model for Role-Based Access Control: Towards A Unified Standard. [Online]. Available at: https://csrc.nist.gov/projects/role-based-access-control.

[73] Brian D. Loader. *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. Routledge, New York, 1997.

[74] Christine Bellamy and John Taylor. *Governing in the Information Age*. Open University Press Buckingham, 1998.

[75] Zhiyuan Fang. E-Government in Digital Era: Concept, Practice, and Development. *International Journal of the Computer, the Internet and Management*, 10:1–22, January 2002.

[76] Mary Maureen Brown. *Encyclopaedia of Public Administration and Public Policy*, chapter Electronic Government, pages 427–432. New York: Marcel Dekker, 2003.

[77] J. Ramón Gil-García and Theresa A. Pardo. E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly*, 22(2):187–216, 2005.

[78] Επιτροπή των Ευρωπαϊκών Κοινοτήτων. Ο ρόλος της ηλεκτρονικής διακυβέρνησης για το μέλλον της Ευρώπης. Technical report, Σεπτέμβριος 2003. Ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, COM(2003) 567.

[79] Ari-Veikko Anttiroiko. *Electronic government : concepts, methodologies, tools and applications*. Hershey PA : Information Science Reference, 2008.

[80] Lori Klamo, Wayne Wei Huang, K.L. Wang, and Taowen Le. Successfully implementing e-government: fundamental issues and a case study in the USA. *Electronic Government, an International Journal*, 3(2):158–173, 2006.

[81] J. Ramon Gil-Garcia and Natalie C. Helbig. *Encyclopedia of Digital Government*, chapter Exploring E-Government Benefits and Success Factors. Hershey, PA: Idea Group Reference, 2007.

[82] Ake Gronlund, editor. *Electronic Government: Design, Applications & Management*. Hershey, PA: Idea Group Publishing, 2002.

[83] Ted Daryl Becker and Christa D. Slaton. *The Future of Teledemocracy*. Westport, Connecticut: Praeger, 2000.

[84] Ari-Veikko Anttiroiko. *eTransformation in Governance*, chapter Introduction to Democratic e-Governance, pages 22–49. Hershey, PA: Idea Group Publishing, 2004.

[85] United Nations. Global e-government readiness report 2005: From e-government to e-inclusion. Technical report, New York: UNPAN, 2005.

[86] Europa. Σύνοψη της νομοθεσίας της ΕΕ. Σχέδιο δράσης i2010 για την ηλεκτρονική διακυβέρνηση. Technical report.

[87] Bernd Stahl. The Paradigm of E-Commerce in E-Government and E-Democracy. 2005.

[88] Latif Al-Hakim. *Global E-Government: Theory, Applications and Benchmarking*. IGI Global, 2006.

[89] UNDESA and ASPA. E-government readiness survey, January 2003. Presented at the Fourth Caribbean Regional Consultation and High-Level Workshop on Public Sector management: Strategies for e-government.

[90] Shannon Howle Schelin. *Public Information Technology: Policy and Management Issues*, chapter E-Government: An Overview, pages 120–138. IGI Global, 2002.

[91] M. Jae Moon. The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review*, 62(4):424–433, 2002.

[92] Stephen H. Holden, Donald F. Norris, and Patricia D. Fletcher. Electronic Government at the Local Level: Progress to Date and Future Issues. *Public Performance & Management Review*, 26(4):325–344, 2003.

[93] Janine S. Hiller and France Belanger. *E-government 2001*, chapter Privacy Strategies for Electronic Government. Lanham, MD: Rowman & Littkefieks Publishers INC, 2001.

[94] UN and ASPA. Benchmarking E-government: A Global Perspective, May 2002.

[95] The Greek e-Government Interoperability Framework. [Online]. Available at: http://www.e-gif.gov.gr/.

[96] Sad Assar, Imed Boughzala, and Isabelle Boydens. *Practical Studies in E-Government: Best Practices from Around the World*. Springer-Verlag New York, Inc., New York, NY, USA, 1st edition, 2010.

[97] William J. McIver Jr. and Ahmed K. Elmagarmid, editors. *Advances in Digital Government - Technology, Human Factors, and Policy*. Springer US, 2002.

[98] Herbert Kubicek, Ralf Cimander, and Hans Scholl. *Organizational Interoperability in E-Government - Lessons from 77 European Good-Practice Cases*. 01 2011.

[99] Hsinchun Chen et al., editor. *Digital Government - E-Government Research, Case Studies, and Implementation*. Springer US, 2008.

[100] Gregory D. Abowd. Beyond Weiser: From Ubiquitous to Collective Computing. *Computer*, 49(1):17–23, January 2016.

[101] The Conference Board. Unlocking ICT growth potential in Europe: Enabling people and businesses – Using Scenarios to Build a New Narrative for the Role of ICT in Growth in Europe. Technical report, October 2013. Report prepared for the European Commission's Directorate-General for Communications Networks, Content and Technology Knowledge Base.

[102] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, Charalampos Z. Patrikakis, Georgios Lamprinakos, Andreas P. Kapsalis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. The Health Avatar: Privacy-Aware Monitoring and Management. *IT Professional*, 17(5):20–27, 2015.

[103] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Andreas P. Kapsalis, Panagiotis Kasnesis, Athanasios I. Delikaris, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra I. Kaklamani. Improving Quality of Life with the Internet of Everything. In *Beyond the Internet of Things: Everything Interconnected*, pages 377–408. Springer International Publishing, 2017.

[104] Despina T. Meridou, Charalampos Z. Patrikakis, Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, and Iakovos S. Venieris. Serving the Needs of Goal Oriented Scenarios through the Deployment of an Intelligent Enterprise Service Bus: A Welfare Use Case. In *Smart Manufacturing & Industry 4.0*, Manchester Business School (East), Manchester, UK, September 2015.

[105] ENISA. Privacy and Data Protection by Design – from policy to engineering, December 2014. [Online]. Available at: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

[106] Cesar Marin et al. A Conceptual Architecture Based on Intelligent Services for Manufacturing Support Systems. In *IEEE International Conference on Systems, Man, and Cybernetics (SMC'13)*, pages 4749–4754, 2013.

[107] Usman Wajid, Vadim Chepegin, Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, and José Barbosa. Adaptive Production Management Using a Service-Based Platform. In Vladimír Mařík, Arnd Schirrmann, Damien Trentesaux, and Pavel Vrba, editors, *Industrial Applications of Holonic and Multi-Agent Systems*, pages 133–144, Cham, 2015. Springer International Publishing.

[108] Vadim Chepegin, Despina Meridou, Maria-Eleftheria Papadopoulou, and Dan Victor Rusu. Turning Your Legacy Systems into Future Profit: Innovation in Production Management. *Cutter IT Journal*, 28(4):21–28, April 2015.

[109] Despina T. Meridou, Andreas P. Kapsalis, Maria-Eleftheria Ch. Papadopoulou, Emmanouil G. Karamanis, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. An Ontology-Based Smart Production Management System. *IT Professional*, 17(6):36–46, 2015.

[110] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Iakovos S. Venieris, Charalampos Z. Patrikakis, Pavel Vrba, Ondrej Harcuba, Cesar Marin, Yaroslav Shepilov, Daria Kazanskaia, Nelson Rodriguez, and Paulo Leitao. Semantics – Architectures and Tools. In *Adaptive Production Planning and Scheduling: The ARUM approach based on MAS and SOA technologies*. Springer, 2016.

[111] Udo Inden, Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Angelos-Christos G. Anadiotis, and Claus-Peter Rückemann. Complex Landscapes of Risk in Operations Systems - Aspects of Modelling and Processing. In *the Proceedings of The Third International Conference on Advanced Communications and Computation (INFOCOMP 2013)*, pages 99–104, 2013.

[112] Udo Inden, Despina T. Meridou, Maria-Eleftheria Papadopoulou, Angelos-Christos Anadiotis, Iakovos S. Venieris, and Claus-Peter Rückemann. Aspects of Modelling and Processing Complex Networks of Operations' Risk. *International Journal On Advances in Software*, 7(3 & 4):501–525, 2014.

[113] Maria-Eleftheria Ch. Papadopoulou, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. On the Use of a Secure and Privacy-Aware eGovernment Infrastructure: The SPAGOS Framework. In Sokratis K. Katsikas and Alexander B. Sideridis, editors, *E-Democracy – Citizen Rights in the World of the New Computing Paradigms*, pages 223–227, Cham, 2015. Springer International Publishing.

[114] Mariza Koukovini, Eugenia Papagiannakopoulou, Georgios V. Lioudakis, Nikos Dellas, Dimitra I. Kaklamani, and Iakovos S. Venieris. An Ontology-Based Approach towards Comprehensive Workflow Modelling. *IET Software*, 8(2):73–85, April 2014.

[115] Vitalik Buterin. Ethereum – A next-generation smart contract and decentralised application platform, 2013. White Paper.

[116] Fabrizio Lamberti, Valentina Gatteschi, Claudio Demartini, Chiara Pranteda, and Victor Santamaria. Blockchain or not blockchain, that is the question of the insurance and other sectors. *IT Professional*, PP(99), 2017.

[117] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. MedRec: Using Blockchain for Medical Data Access and Permission Management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, August 2016.

[118] Zonyin Shae and Jeffrey J.P. Tsai. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 1972–1980, June 2017.

[119] Panagiotis Kasnesis, Charalampos Z. Patrikakis, Dimitris Kogias, Lazaros Toumanidis, and Iakovos S. Venieris. Cognitive friendship and goal management for the social IoT. *Computers & Electrical Engineering*, 58:412–428, 2017.

[120] Luigi Atzori, Antonio Iera, and Giacomo Morabito. SIoT: Giving a Social Structure to the Internet of Things. *IEEE Communications Letters*, 15(11):1193–1195, November 2011.

[121] Dave Evans. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World. 2012. Cisco IBSG.

[122] Dan Boneh, Amit Sahai, and Brent Waters. Functional Encryption: A New Vision for Public-key Cryptography. *Commun. ACM*, 55(11):56–64, 2012.

[123] Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. Blockchained Driverless Cars for Avoiding Machine Deception. *IT Professional*, Nov/Dec 2018. [submitted–under review].

Δημοσιεύσεις

Διεθνή Περιοδικά

J[4] Despina T. Meridou, Andreas P. Kapsalis, Maria-Eleftheria Ch. Papadopoulou, Emmanouil G. Karamanis, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. An Ontology-Based Smart Production Management System. *IT Professional*, 17(6):36–46, 2015.

J[3] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, Charalampos Z. Patrikakis, Georgios Lamprinakos, Andreas P. Kapsalis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. The Health Avatar: Privacy-Aware Monitoring and Management. *IT Professional*, 17(5):20–27, 2015.

J[2] Vadim Chepegin, Despina Meridou, Maria-Eleftheria Papadopoulou, and Dan Victor Rusu. Turning Your Legacy Systems into Future Profit: Innovation in Production Management. *Cutter IT Journal*, 28(4):21–28, April 2015.

J[1] Udo Inden, Despina T. Meridou, Maria-Eleftheria Papadopoulou, Angelos-Christos Anadiotis, Iakovos S. Venieris, and Claus-Peter Rückemann. Aspects of Modelling and Processing Complex Networks of Operations' Risk. *International Journal On Advances in Software*, 7(3 & 4):501–525, 2014.

Κεφάλαια Βιβλίων

B[2] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Andreas P. Kapsalis, Panagiotis Kasnesis, Athanasios I. Delikaris, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra I. Kaklamani. Improving Quality of Life with the Internet of Everything. In *Beyond the Internet of Things: Everything Interconnected*, pages 377–408. Springer International Publishing, 2017.

B[1] Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Iakovos S. Venieris, Charalampos Z. Patrikakis, Pavel Vrba, Ondrej Harcuba, Cesar Marin, Yaroslav Shepilov, Daria Kazanskaia, Nelson Rodriguez, and Paulo Leitao. Semantics – Architectures and Tools. In *Adaptive Production Planning and Scheduling: The ARUM approach based on MAS and SOA technologies*. Springer, 2016.

Πρακτικά Συνεδρίων

C[5] Maria-Eleftheria Ch. Papadopoulou, Charalampos Z. Patrikakis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. On the Use of a Secure and Privacy-Aware eGovernment

Infrastructure: The SPAGOS Framework. In Sokratis K. Katsikas and Alexander B. Sideridis, editors, *E-Democracy – Citizen Rights in the World of the New Computing Paradigms*, pages 223–227, Cham, 2015. Springer International Publishing.

C[4] Despina T. Meridou, Charalampos Z. Patrikakis, Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, and Iakovos S. Venieris. Serving the Needs of Goal Oriented Scenarios through the Deployment of an Intelligent Enterprise Service Bus: A Welfare Use Case. In *Smart Manufacturing & Industry 4.0*, Manchester Business School (East), Manchester, UK, September 2015.

C[3] Usman Wajid, Vadim Chepegin, Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, and José Barbosa. Adaptive Production Management Using a Service-Based Platform. In Vladimír Mařík, Arnd Schirrmann, Damien Trentesaux, and Pavel Vrba, editors, *Industrial Applications of Holonic and Multi-Agent Systems*, pages 133–144, Cham, 2015. Springer International Publishing.

C[2] Paulo Leitão, José Barbosa, Maria-Eleftheria C. Papadopoulou, and Iakovos S. Venieris. Standardization in Cyber-Physical Systems: The ARUM case. In *the Proceedings of 2015 IEEE International Conference on Industrial Technology (ICIT)*, pages 2988–2993, March 2015. Nominated to appear in IE Tech News (ITeN), a web-only publication of IEEE Industrial Electronics Society.

C[1] Udo Inden, Despina T. Meridou, Maria-Eleftheria Ch. Papadopoulou, Angelos-Christos G. Anadiotis, and Claus-Peter Rückemann. Complex Landscapes of Risk in Operations Systems - Aspects of Modelling and Processing. In *the Proceedings of The Third International Conference on Advanced Communications and Computation (INFOCOMP 2013)*, pages 99–104, 2013.

Δημοσιεύσεις υπό Κρίση

[1] Maria-Eleftheria Ch. Papadopoulou, Panagiotis Kasnesis, Iakovos S. Venieris, and Dimitra-Theodora I. Kaklamani. Blockchained Driverless Cars for Avoiding Machine Deception. *IT Professional*, Nov/Dec 2018. [submitted–under review]