

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Έμπιστο Περιβάλλον Συνεργασίας και Παροχής
Ασφαλών, Ιδιωτικών και Διαλειτουργικών Υπηρεσιών

Διδακτορική Διατριβή

Γεώργιος Κ. Πενταφρόνιμος

Σεπτέμβριος 2012

.....

Γεώργιος Κ. Πενταφρόνιμος

Πτυχιούχος Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Μεταπτυχιακό Δίπλωμα Ειδίκευσης στα Προηγμένα Συστήματα Πληροφορικής, Πανεπιστήμιο Πειραιώς, Τμήμα Πληροφορικής

Copyright © Γεώργιος Κ. Πενταφρόνιμος, 2012

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πειραιώς.

Αφιερώνεται,

στον πατέρα μου, Κωνσταντίνο, στη μητέρα μου, Ευσταθία,

καθώς και στην πολυαγαπημένη μου αδελφή, Κυριακή.

Πανεπιστήμιο Πειραιώς

Ευχαριστίες

Η παρούσα διδακτορική διατριβή είναι το αποτέλεσμα ερευνητικής εργασίας που πραγματοποιήθηκε στο Πανεπιστήμιο Πειραιώς. Ως εκ τούτου θα ήθελα να εκφράσω τις ευχαριστίες μου τόσο προς το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς, για τη δυνατότητα που μου έδωσε να εκπονήσω την παρούσα διατριβή, όσο και προς όλους όσους συνέβαλαν, με το δικό του τρόπο ο καθένας, στην προσπάθειά μου αυτή.

Αρχικά θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτριά μου, κ. Δέσποινα Πολέμη, για όλα τα εφόδια που μου πρόσφερε όλα αυτά τα χρόνια καθώς επίσης για τη συνεχή καθοδήγηση, και τη βοήθειά της. Είμαι ευγνώμων για τις πολύτιμες εμπειρίες και γνώσεις που αποκόμισα από τη συνεργασία μας. Επίσης ευχαριστώ θερμά τον καθηγητή, κ. Χρήστο Δουληγέρη, για την εμπιστοσύνη, το ενδιαφέρον και τις πολύτιμες συμβουλές του καθ' όλη τη διάρκεια των ερευνητικών μου δραστηριοτήτων αλλά και κατά την εκπόνηση της διατριβής, καθώς και τον επίτιμο καθηγητή, κ. Νικόλαο Αλεξανδρή, για την αμέριστη συμπαράσταση και το συνεχές και ειλικρινές ενδιαφέρον του σχετικά με την εξέλιξη της ακαδημαϊκής και ερευνητικής μου πορείας, από τα πρώτα χρόνια των μεταπτυχιακών μου σπουδών στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς.

Κατά τη διάρκεια εκπόνησης του ερευνητικού μου έργου και της διδακτορικής διατριβής υπήρξαν αρκετοί φίλοι και συνεργάτες οι οποίοι με στήριξαν και τους οποίους οφείλω να ευχαριστήσω. Ο Αθανάσιος Καραντζιάς, διδάκτωρ του Εθνικού Μετσόβιου Πολυτεχνείου, ήταν εκείνος ο οποίος στάθηκε στο πλευρό μου από την αρχή της σταδιοδρομίας μου και με στήριξε στις δύσκολες στιγμές. Τον ευχαριστώ ολόψυχα όχι μόνο για τις πολύτιμες γνώσεις και εμπειρίες που αποκόμισα από τη φιλία και τη συνεργασία μας όλα αυτά τα χρόνια, αλλά πολύ περισσότερο γιατί ήταν πάντα διαθέσιμος να ακούσει τις ανησυχίες, τις σκέψεις, και τους προβληματισμούς μου, και πάντα πρόθυμος να μου προσφέρει πολύτιμες και ειλικρινείς συμβουλές. Επίσης θέλω να ευχαριστήσω τους υποψήφιους διδάκτορες, Θεόδωρο Ντούσκα, Δημήτριο Παπανίκα, Κλεάνθη Δέλλιο, και Εμμανουήλ Γεωργακάκη, για τις αξέχαστες στιγμές που περάσαμε μαζί τα τελευταία χρόνια στο πλαίσιο της συνεργασίας μας για ερευνητικά προγράμματα, καθώς και για το ενδιαφέρον και την υποστήριξή τους. Εύχομαι η φιλία μας να συνεχιστεί για πολλά χρόνια.

Ακόμα, θα ήθελα να εκφράσω ιδιαίτερες ευχαριστίες προς τους συναδέλφους μου στον επαγγελματικό τομέα, την Ε. Σαρμαζανίδου, τον Γ. Καρατζά και τον Ν. Ψιμόγιαννο για την κατανόηση και την υπομονή τους, ιδιαίτερα κατά την τελευταία φάση εκπόνησης της διατριβής, καθώς επίσης και για τη συμπαράσταση και την εμπιστοσύνη τους.

Τέλος, ευχαριστώ ολόψυχα τον Διδάσκαλό μου από τα παλιά κ. Γ. Σούμπαση, τους αδερφικούς μου φίλους Δ. Πεδιαδιτάκη, Κ. Βαρζακάκο, Ν. και Δ. Δημητράκουλα, Γ. Κουτρούλη, Κ. Κώνστα, Σ. Μεσολωρά, Π. Σαμπατάκο, Α. Σκρουμπέλο και Ο. Βαρβιτσιώτη, καθώς και τις αγαπημένες μου Χάρις Γάγκα, Μαρία Κολέττη, Κωνσταντίνα Στέλλιου, και Άννα Φιλιππάκη γιατί πίστεψαν σε μένα και ήταν αυτοί που μου έδιναν κουράγιο και δύναμη να συνεχίζω στα δύσκολα. Χωρίς αυτούς, η ζωή μου κατά τη διάρκεια εκπόνησης της διατριβής θα είχε λιγότερα χαμόγελα και τα ψυχολογικά αδιέξοδα θα είχαν ξεπεραστεί με δυσκολία. Θα παραμείνουν για πάντα στην καρδιά μου.

Σπάρτη, 8 Ιουνίου 2012

Πανεπιστήμιο Πειραιώς

Περίληψη

Η εξάπλωση των εφαρμογών Web 2.0 και η παροχή υπηρεσιών συνεργασίας και κοινωνικής αλληλεπίδρασης από τη μια πλευρά προσφέρουν σημαντικά οφέλη στους χρήστες από την άλλη προκαλούν νέες απειλές στην ιδιωτικότητά τους. Εκτός των τεχνολογικών προκλήσεων που χαρακτηρίζουν την ασφαλή ενσωμάτωση τεχνολογιών Web 2.0 σε ολοκληρωμένα Πληροφοριακά Συστήματα και πλαίσια υπηρεσιών, η διατριβή εντοπίζει την ανάγκη προστασίας της ιδιωτικότητας από τις διαδραστικές δυνατότητες δημιουργίας περιεχόμενου και αλληλεπίδρασης που παρέχονται στους χρήστες.

Έχοντας σαν βασικό στόχο την εύρεση καινοτόμων λύσεων για την προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα, αρχικά καθορίζεται η αρχιτεκτονική ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος (ΕΣΠΣ) ικανού να καλύψει τις σύγχρονες απαιτήσεις για παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών. Η δεύτερη συνεισφορά της διατριβής περιλαμβάνει τη μελέτη επικινδυνότητας των κρίσιμων, ως προς την προστασία της ιδιωτικότητας, συστημάτων που ενσωματώνονται στην αρχιτεκτονική του ΕΣΠΣ εντοπίζοντας ανοιχτά θέματα τα οποία δεν καλύπτονται από τα αποτελέσματα της έρευνας πεδίου και αφορούν στην «ανεξέλεγκτη» χρήση των διαδραστικών υπηρεσιών και λειτουργιών που παρέχουν οι εφαρμογές Web 2.0.

Η τρίτη και τέταρτη συνεισφορά της διατριβής επικεντρώνονται στην κάλυψη των ανοιχτών θεμάτων και αποτελούν τις βασικές καινοτομίες που προτείνονται για την προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα. Αφενός περιλαμβάνουν μια καινοτόμο αρχιτεκτονική διαχείρισης ταυτοτήτων η οποία αναγνωρίζει την αξιοπιστία των χρηστών ως δυναμικό χαρακτηριστικό της ταυτότητάς τους, ικανό να αναβαθμίσει τη χρήση των στατικά προκαθορισμένων ρόλων για την απόδοση προνομίων προσπέλασης στις διαδραστικές υπηρεσίες του συνεργατικού περιβάλλοντος. Αφετέρου, έχοντας σαν στόχο τη συλλογική προστασία της ιδιωτικότητας και τη λήψη έμπιστων αποφάσεων εξουσιοδότησης, καθορίζεται μια αναδρομική μέθοδος υπολογισμού του βαθμού αξιοπιστίας η οποία εκτός από τις αναφορές κακόβουλης συμπεριφοράς λαμβάνει υπόψη και άλλους κρίσιμους παράγοντες του συνεργατικού περιβάλλοντος.

Η πέμπτη και τελική συνεισφορά της διατριβής έχει σαν στόχο να αναδείξει τα οφέλη υιοθέτησης του ΕΣΠΣ σε κρίσιμους τομείς της σύγχρονης Κοινωνίας της Πληροφορίας όπως αυτός της ηλεκτρονικής Διακυβέρνησης, μέσω της εφαρμογής του για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών προς νόμιμους μετανάστες (υπηρεσίες η-Μετανάστευσης).

Πανεπιστήμιο Πειραιώς

Abstract

With the advent of Web 2.0 applications and social networks, modern services are able to offer advanced capabilities to end-users enabling their active participation in collaborative environments and the exchange of personal knowledge and experiences. However, new privacy threats have also appeared. Apart from the technological challenges that need to be addressed for the effective integration of Web 2.0 technologies in trusted Information Systems and service frameworks, the research results of this thesis also identify the need for the protection of privacy with regards to the interactive capabilities offered for publishing personal content and participating in social interactions.

Having as its main goal the introduction of innovative solutions for privacy protection in collaborative workspaces, this thesis primarily specifies the architecture of a Trusted Collaborative Information System (TCIS) that is capable of satisfying modern requirements for the provision of secure, privacy-aware and interoperable services. The second contribution comprises the risk assessment of all critical, in terms of privacy protection, systems integrated within the architecture of TCIS. Also, open issues that are not covered in the literature are identified, which are mostly related to the “loosely” controlled use of the interactive services and capabilities that Web 2.0 applications offer to end-users.

The third and fourth contribution of this thesis focus on effectively addressing the open issues identified and constitute the main innovations for the protection of privacy in collaborative environments. On one hand, these comprise an innovative identity management architecture where the reputation of users is handled as an identity attribute capable of effectively substituting their role for the provision of access privileges to Web 2.0-based services. On the other hand, in order to enable collaborative privacy protection and the enforcement of trusted authorization decisions, a recursive method for computing reputation scores is also specified, which, apart from the privacy-pervasive reports, also takes into consideration other critical factors of the collaborative environment.

The fifth and final contribution of the thesis has as its main goal to highlight the benefits of the adoption of TCIS in critical domains of modern Information Society, as for example the e-Government domain, through demonstrating its applicability for the provision of secure, privacy-aware and interoperable services to legal immigrants (e-Migration services).

Πανεπιστήμιο Πειραιώς

Περιεχόμενα

1	ΕΙΣΑΓΩΓΗ	7
1.1	ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ	8
1.2	ΔΟΜΗ	11
1.3	ΔΗΜΟΣΙΕΥΣΕΙΣ ΑΠΟΤΕΛΕΣΜΑΤΩΝ	14
2	ΕΡΕΥΝΗΤΙΚΟ ΠΕΔΙΟ – ΑΝΟΙΧΤΑ ΘΕΜΑΤΑ	17
2.1	ΕΙΣΑΓΩΓΗ	17
2.2	ΣΥΝΕΡΓΑΣΙΑ	18
2.2.1	Έρευνα πεδίου σε εφαρμογές Web 2.0	20
2.2.2	Έρευνα πεδίου σε συνεργατικά περιβάλλοντα	23
2.2.3	Ανοιχτά θέματα	25
2.3	ΠΡΟΣΒΑΣΙΜΟΤΗΤΑ	25
2.3.1	Έρευνα πεδίου σε μοντέλα ελέγχου προσπέλασης	27
2.3.2	Ανοιχτά θέματα	30
2.4	ΙΔΙΩΤΙΚΟΤΗΤΑ	31
2.4.1	Έρευνα πεδίου σε αρχιτεκτονικές διαχείρισης ταυτοτήτων	32
2.4.2	Έρευνα πεδίου σε πρότυπα και προδιαγραφές διαχείρισης ταυτοτήτων	34
2.4.3	Ανοιχτά θέματα	36
2.5	ΑΞΙΟΠΙΣΤΙΑ	37
2.5.1	Έρευνα πεδίου σε αρχιτεκτονικές συστημάτων αξιοπιστίας	38
2.5.2	Έρευνα πεδίου σε μοντέλα υπολογισμού του βαθμού αξιοπιστίας	40
2.5.3	Ανοιχτά θέματα	41
2.6	ΣΥΜΠΕΡΑΣΜΑΤΑ	42
2.7	ΒΙΒΛΙΟΓΡΑΦΙΑ	44
3	ΑΠΑΙΤΗΣΕΙΣ ΕΝΟΣ ΉΜΠΙΣΤΟΥ ΣΥΝΕΡΓΑΤΙΚΟΥ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ	51
3.1	ΕΙΣΑΓΩΓΗ	51
3.2	ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΑΙΤΗΣΕΩΝ	53
3.2.1	Απαιτήσεις χρηστών	53
3.2.2	Λειτουργικές απαιτήσεις	54
3.2.3	Τεχνικές απαιτήσεις	56
3.3	ΣΥΜΠΕΡΑΣΜΑΤΑ	60
3.4	ΒΙΒΛΙΟΓΡΑΦΙΑ	61
4	ΕΣΠΣ: ΈΝΑ ΉΜΠΙΣΤΟ ΣΥΝΕΡΓΑΤΙΚΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ	63
4.1	ΕΙΣΑΓΩΓΗ	63
4.2	ΜΕΘΟΔΟΛΟΓΙΑ ΣΧΕΔΙΑΣΜΟΥ	63
4.3	ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΣΠΣ	66
4.3.1	Κεντρική πλατφόρμα	68
4.3.2	Περιφερειακά Συστήματα	79

4.3.3	<i>Σύστημα Διασύνδεσης</i>	94
4.4	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	95
4.5	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	97
5	ΜΕΛΕΤΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΟΥ ΕΣΠΣ	99
5.1	ΕΙΣΑΓΩΓΗ.....	99
5.2	ΤΑΞΙΝΟΜΗΣΗ ΠΟΡΩΝ	100
5.3	ΑΠΕΙΛΕΣ, ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ	103
5.3.1	<i>Απειλές ιδιωτικότητας σε συνεργατικά περιβάλλοντα</i>	104
5.3.2	<i>Επιθέσεις ιδιωτικότητας</i>	106
5.3.3	<i>Μέτρα προστασίας</i>	108
5.4	ΣΧΕΔΙΟ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΕΣΠΣ.....	109
5.5	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	110
5.6	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	112
6	ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΩΝ ΣΕ ΣΥΝΕΡΓΑΤΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ	117
6.1	ΕΙΣΑΓΩΓΗ.....	117
6.2	ΠΡΟΚΛΗΣΕΙΣ ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΩΝ	118
6.3	ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΕΝΤΡΙΚΟΠΟΙΗΜΕΝΗΣ ΟΜΟΣΠΟΝΔΙΑΣ.....	120
6.3.1	<i>Μοντέλο Δυναμικού Ελέγχου Προσπέλασης</i>	123
6.3.2	<i>Οντότητες και πόροι</i>	123
6.3.3	<i>Σχέσεις εμπιστοσύνης και συνθήκες εξουσιοδότησης</i>	124
6.4	ΛΕΙΤΟΥΡΓΙΚΟ ΠΛΑΙΣΙΟ	127
6.5	ΕΦΑΡΜΟΓΗ ΔΕΠ-ΕΣΠΣ.....	130
6.6	ΜΕΘΟΔΟΣ ΥΠΟΛΟΓΙΣΜΟΥ ΑΞΙΟΠΙΣΤΙΑΣ	134
6.6.1	<i>Παράγοντας κρισιμότητας των αναφορών κακόβουλης συμπεριφοράς</i>	136
6.6.2	<i>Παράγοντας επιβράβευσης του χρήστη</i>	139
6.6.3	<i>Παράγοντας στάθμισης του συνεργατικού περιβάλλοντος</i>	141
6.7	ΘΕΜΑΤΑ ΥΛΟΠΟΙΗΣΗΣ.....	142
6.7.1	<i>Λίστες δεδομένων</i>	142
6.7.2	<i>Συντελεστές επίδρασης</i>	144
6.8	ΣΥΝΕΙΣΦΟΡΑ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ.....	147
6.9	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	152
6.10	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	154
7	ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: ΕΦΑΡΜΟΓΗ ΕΣΠΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ Η-ΜΕΤΑΝΑΣΤΕΥΣΗΣ	161
7.1	ΕΙΣΑΓΩΓΗ.....	162
7.2	ΈΡΕΥΝΑ ΠΕΔΙΟΥ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ Η-ΜΕΤΑΝΑΣΤΕΥΣΗΣ.....	163
7.3	ΠΡΟΚΛΗΣΕΙΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ Η-ΜΕΤΑΝΑΣΤΕΥΣΗΣ	166
7.4	ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΘΟΡΙΣΜΟΥ ΕΝΝΟΙΟΛΟΓΙΚΟΥ ΠΛΑΙΣΙΟΥ	169
7.5	ΥΠΗΡΕΣΙΕΣ Η-ΜΕΤΑΝΑΣΤΕΥΣΗΣ	173
7.5.1	<i>Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης</i>	176

7.5.2	Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών.....	177
7.5.3	Υπηρεσίες Ανοιχτών Διαβουλεύσεων.....	179
7.5.4	Υπηρεσίες Διαχείρισης Μεταναστευτικών Διαδικασιών.....	181
7.5.5	Υπηρεσίες Εναρμόνισης Διαδικασιών.....	182
7.5.6	Υπηρεσίες Υποστήριξης Αποφάσεων.....	184
7.6	ΣΥΝΕΡΓΑΤΙΚΟ ΠΕΡΙΒΑΛΛΟΝ Η-ΜΕΤΑΝΑΣΤΕΥΣΗΣ.....	185
7.7	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	187
7.8	ΒΙΒΛΙΟΓΡΑΦΙΑ.....	188
8	ΑΝΑΣΚΟΠΗΣΗ ΔΙΑΤΡΙΒΗΣ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ.....	193
8.1	ΣΥΜΠΕΡΑΣΜΑΤΑ.....	193
8.2	ΑΝΑΣΚΟΠΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ.....	195
8.3	ΜΕΛΛΟΝΤΙΚΕΣ ΕΡΕΥΝΗΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ.....	196
	ΠΑΡΑΡΤΗΜΑ Ι - ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΣΥΝΤΕΛΕΣΤΗ Σ.....	199
	ΓΛΩΣΣΑΡΙ.....	201
	ΑΚΡΩΝΥΜΙΑ.....	203

Πανεπιστήμιο Πειραιώς

Κατάλογος Εικόνων

Εικόνα 1: Τεχνικές απαιτήσεις ΕΣΠΣ	56
Εικόνα 2: Συλλογική προστασία της ιδιωτικότητας	149
Εικόνα 3: Συνεργασία στην πλατφόρμα ImmigrationPolicy 2.0	177
Εικόνα 4: Διαχείριση περιεχομένου στην πλατφόρμα ImmigrationPolicy 2.0	179
Εικόνα 5: Ανοιχτές διαβουλεύσεις στην πλατφόρμα ImmigrationPolicy 2.0	180
Εικόνα 6: Μοντελοποίηση διαδικασιών στην πλατφόρμα ImmigrationPolicy 2.0	182
Εικόνα 7: Εναρμόνιση μεταναστευτικών διαδικασιών με ADONIS Web Portal	184
Εικόνα 8: Υποστήριξη αποφάσεων στην πλατφόρμα ImmigrationPolicy 2.0	185

Κατάλογος Πινάκων

Πίνακας 1: Τεχνικές λύσεις και καινοτομίες ΕΣΠΣ	95
Πίνακας 2: Ταξινόμηση πόρων ΕΣΠΣ ως προς τις απαιτήσεις ιδιωτικότητας	101
Πίνακας 3: Σχέδιο Ιδιωτικότητας ΕΣΠΣ	110
Πίνακας 4: Παράγοντας Καταγραφής κακόβουλης συμπεριφοράς	138
Πίνακας 5: Παράγοντας Επιβράβευσης του χρήστη	140
Πίνακας 6: Παράγοντας Στάθμισης αρνητικών ψήφων με τη συχνότητα χρήσης	141
Πίνακας 7: Πολιτικές προστασίας της ιδιωτικότητας	147
Πίνακας 8: Σύγκριση ΣΔΑ-ΕΣΠΣ και παραδοσιακών προσεγγίσεων	151

Κατάλογος Σχημάτων

Σχήμα 1: Μοντέλο RM-ODP	64
Σχήμα 2: Αρχιτεκτονική 3 επιπέδων	65
Σχήμα 3: Αρχιτεκτονική του ΕΣΠΣ	67
Σχήμα 4: Κεντρική πλατφόρμα του ΕΣΠΣ	68
Σχήμα 5: Διάγραμμα UML των υποσυστημάτων της ΜΔΧ	69
Σχήμα 6: Διάγραμμα Κατάστασης UML της ΜΔΧ	70
Σχήμα 7: Διάγραμμα Κατάστασης UML της ΥΜΠΓ	71
Σχήμα 8: Διάγραμμα UML της ΜΕΔ	73
Σχήμα 9: Διάγραμμα Κατάστασης UML της ΥΜΔΠΑ	76
Σχήμα 10: Διάγραμμα Κατάστασης UML της ΥΜΕΠ	77

Σχήμα 11: Διάγραμμα Κατάστασης UML της ΥΜΜΕ.....	78
Σχήμα 12: Διάγραμμα UML των Μονάδων του ΣΔΤΕΠ	81
Σχήμα 13: Διάγραμμα Ροής Πληροφοριών UML του ΣΔΤΕΠ	83
Σχήμα 14: Διάγραμμα UML του ΣΣΚΑ.....	87
Σχήμα 15: Διάγραμμα Κατάστασης Πληροφορίας UML του ΣΣΚΑ	88
Σχήμα 16: Μοντελοποίηση και γραφική αναπαράσταση διαδικασιών.....	89
Σχήμα 17: Μοντέλο PDCA	90
Σχήμα 18: Διάγραμμα UML του ΣΜΔΕΠ.....	91
Σχήμα 19: Διάγραμμα κατάστασης UML της ΜΠΑΠ	93
Σχήμα 20: Αρχιτεκτονική Κεντριοποιημένης Ομοσπονδίας	121
Σχήμα 21: Σύνολο παρεχομένων πόρων του ΕΣΠΣ.....	124
Σχήμα 22: Ομαδοποίηση χρηστών με βάση το ρόλο τους.....	125
Σχήμα 23: Δικαιώματα προσπέλασης στους ΠΥ με βάση το ρόλο των χρηστών	126
Σχήμα 24: Δικαιώματα προσπέλασης στις ΣΥΛ κάθε ΠΥ με βάση το ρόλο	126
Σχήμα 25: Δικαιώματα προσπέλασης στις ΔΥΛ με βάση το βαθμό αξιοπιστίας	127
Σχήμα 26: Λειτουργικό πλαίσιο ΔΕΠ-ΕΣΠΣ.....	128
Σχήμα 27: Εφαρμογή μοντέλου ΔΕΠ-ΕΣΠΣ.....	131
Σχήμα 28: Εννοιολογικό πλαίσιο η-Μετανάστευσης.....	170
Σχήμα 29: Προηγμένες υπηρεσίες η-Μετανάστευσης	174
Σχήμα 30: Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης	176
Σχήμα 31: Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών.....	178
Σχήμα 32: Υπηρεσίες Ανοιχτών Διαβουλεύσεων	180
Σχήμα 33: Υπηρεσίες Διαχείρισης Μεταναστευτικών Διαδικασιών.....	181
Σχήμα 34: Υπηρεσίες Εναρμόνισης Διαδικασιών.....	183
Σχήμα 35: Υπηρεσίες Υποστήριξης Αποφάσεων	185
Σχήμα 36: Εφαρμογή ΕΣΠΣ στον τομέα η-Μετανάστευσης.....	186

Κεφάλαιο 1

Εισαγωγή

Η ευρεία χρήση των εφαρμογών Web 2.0 (π.χ. wikis, φόρουμ, ιστολόγια) από όλες τις κοινωνικές ομάδες χρηστών καθώς και η έντονη εξάπλωσή τους σε ποικίλους τομείς της σύγχρονης Κοινωνίας της Πληροφορίας, όπως η Διακυβέρνηση, η Εκπαίδευση και το Ηλεκτρονικό Εμπόριο οφείλονται στην εξέλιξη του Διαδικτύου σε ένα μέσο στο οποίο μπορεί ο καθένας να δημιουργήσει εύκολα το δικό του περιεχόμενο και να δημοσιεύσει τις προσωπικές του απόψεις και σχολιασμούς.

Το νέο Διαδίκτυο ή αλλιώς Web 2.0 αναβαθμίζει τις παραδοσιακές δυνατότητες του Παγκόσμιου Ιστού δίνοντας έμφαση στη διαδραστικότητα, τη συνεργασία, την κοινωνική αλληλεπίδραση και την ενεργή συνεισφορά των χρηστών στη δημιουργία περιεχομένου. Η παροχή πληροφοριών εξελίχθηκε από το στατικό περιεχόμενο ιστοσελίδων, σε ένα δυναμικό περιβάλλον ψηφιακών κοινοτήτων και δικτύων αλληλεπίδρασης μεταξύ χρηστών και κοινωνικών, κυβερνητικών και άλλων φορέων όπου όλες οι οντότητες συμμετέχουν ισότιμα στη δημοσίευση περιεχομένου.

Σε αυτό το νέο ψηφιακό περιβάλλον, οι δυνατότητες συνεργασίας και κοινωνικής αλληλεπίδρασης που παρέχουν στους χρήστες οι τεχνολογίες Web 2.0 “αναδύονται” ως οι πιο δημοφιλείς και χρήσιμες υπηρεσίες και αποτελούν πλέον αναπόσπαστο συστατικό κάθε ολοκληρωμένου Πληροφοριακού Συστήματος και σύγχρονου πλαισίου ηλεκτρονικών υπηρεσιών.

Από την άλλη πλευρά, η «ανεξέλεγκτη» δημιουργία περιεχομένου και η ενεργή συμμετοχή σε κοινωνικά δίκτυα και περιβάλλοντα συνεργασίας αξιοποιούνται από τους χρήστες άλλες φορές με θεμιτό και άλλες φορές με κακόβουλο τρόπο, ελλοχεύοντας απειλές για την ιδιωτικότητα και τα ευαίσθητα δεδομένα των υπολοίπων συμμετεχόντων. Για παράδειγμα, η δημόσια έκφραση ιδιωτικών πληροφοριών σε ένα ιστολόγιο αποτελεί μια ιδιαίτερα κρίσιμη διαδικασία, δεδομένου ότι ικανοποιώντας την ανάγκη για δημόσια έκφραση και ενεργή συμμετοχή, ο χρήστης ενδέχεται να αποκαλύψει προσωπικά δεδομένα του ίδιου ή άλλων χρηστών.

Δεδομένου ότι σε αντίθεση με τα παραδοσιακά πλαίσια υπηρεσιών, στα σύγχρονα συνεργατικά περιβάλλοντα το ψηφιακό περιεχόμενο δεν δημιουργείται, δημοσιεύεται ή ανταλλάσσεται αποκλειστικά μεταξύ των Παρόχων, αντίστοιχα η ιδιωτικότητα των χρηστών δεν επηρεάζεται

αποκλειστικά από την αξιοπιστία των Παρόχων στο να προστατεύουν τα Προσωπικά και Ευαίσθητα Δεδομένα (ΠΕΔ, Personally Identifiable Information). Σε ακόμα πιο κρίσιμο βαθμό, εξαρτάται από τα κίνητρα των υπολοίπων χρηστών που συμμετέχουν στο περιβάλλον συνεργασίας και από το βαθμό στον οποίο σέβονται με τη συμπεριφορά τους την ιδιωτικότητα, κατά τη δημιουργία ψηφιακού περιεχόμενου.

Προσανατολίζοντας την έρευνα προς αυτή την κατεύθυνση, η διατριβή διαπραγματεύεται το γεγονός ότι στα συνεργατικά περιβάλλοντα δημιουργούνται νέες απειλές για την ιδιωτικότητα, οι οποίες αφορούν στην προστασία της από κακόβουλους χρήστες που έχουν τη δυνατότητα να συμμετέχουν ισότιμα στη δημιουργία περιεχομένου. Πιο συγκεκριμένα, εντοπίζεται η ανάγκη ότι η έννοια της εμπιστοσύνης και οι αντίστοιχοι μηχανισμοί που υιοθετούνται για την προστασία της ιδιωτικότητας των χρηστών θα πρέπει απαραίτητα να καλύπτουν τις μεταξύ τους αλληλεπιδράσεις, αντιμετωπίζοντας τους κινδύνους που ελλοχεύει η δυναμική δημιουργία περιεχομένου για την αποκάλυψη προσωπικών δεδομένων.

Ανακεφαλαιώνοντας, απαιτούνται καινοτόμες λύσεις προστασίας της ιδιωτικότητας σε Πληροφοριακά Συστήματα τα οποία ενσωματώνουν διαδραστικές εφαρμογές και υπηρεσίες Web 2.0, οι οποίες θα αξιοποιούν τη συλλογική γνώση των χρηστών προκειμένου να αξιολογείται με δυναμικό τρόπο η συμπεριφορά τους στο να συνεισφέρουν ψηφιακό περιεχόμενο το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων.

1.1 Αντικείμενο και στόχοι

Ένα κοινό χαρακτηριστικό των εφαρμογών Web 2.0 και των υπηρεσιών κοινωνικής αλληλεπίδρασης αποτελεί το γεγονός ότι όλοι οι χρήστες έχουν ίσα δικαιώματα προσπέλασης των διαδραστικών λειτουργιών που τους παρέχονται από τα συστήματα αυτά. Πολλές φορές μάλιστα, όταν οι εφαρμογές Web 2.0 χρησιμοποιούνται απομονωμένες από κάποιο ολοκληρωμένο πλαίσιο υπηρεσιών ανώνυμοι χρήστες μπορούν να συμμετέχουν ισότιμα στη δημοσίευση πληροφοριών. Έτσι εντοπίζεται αδυναμία στην επίτευξη εμπιστοσύνης μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον καθώς ο καθένας μπορεί «ανεξέλεγκτα» να δημιουργεί κακόβουλο περιεχόμενο χωρίς να αξιολογείται η αξιοπιστία του.

Με βάση την υφιστάμενη τεχνολογική εξέλιξη η αντιμετώπιση αυτού του προβλήματος αποτελεί αρμοδιότητα των *Συστημάτων Διαχείρισης Ταυτοτήτων*, καθώς αυτά είναι υπεύθυνα για την ταυτοποίηση των χρηστών και την απόδοση προνομίων προσπέλασης στις παρεχόμενες υπηρεσίες. Η σύγχρονη πρακτική Διαχείρισης Ταυτοτήτων στον τομέα των διαδικτυακών εφαρμογών και των ολοκληρωμένων Πληροφοριακών Συστημάτων βασίζεται στην απόδοση ρόλων στους χρήστες ανάλογα με κάποια χαρακτηριστικά της ταυτότητάς τους ή με το πλήθος των προσωπικών δεδομένων που είναι διατεθειμένοι να

αποκαλύψουν κατά την ταυτοποίησή τους στον Πάροχο, και στη συσχέτιση του ρόλου τους με ένα σύνολο προνομίων εξουσιοδότησης που αποδίδεται στα μέλη κάθε ομάδας χρηστών. Καθορίζεται, επίσης, από τις σχέσεις εμπιστοσύνης μεταξύ των Παρόχων ώστε να υποστηρίζεται η ομοσπονδιακή διαχείριση των δικαιωμάτων προσπέλασης σε ετερογενή περιβάλλοντα.

Στο πλαίσιο της παρούσας διατριβής αποδεικνύεται ότι η προσέγγιση αυτή αν και είναι ικανή να καλύπτει αποτελεσματικά τις απαιτήσεις διαχείρισης ταυτοτήτων σε παραδοσιακά πλαίσια υπηρεσιών, όταν εφαρμόζεται σε συνεργατικά περιβάλλοντα τα οποία παρέχουν στους χρήστες τη δυνατότητα δημιουργίας περιεχομένου δεν είναι επαρκής για να καλύψει τις νέες απειλές που επιφέρει στην ιδιωτικότητα η χρήση των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0.

Το βασικό της μειονέκτημα, το οποίο καλύπτεται από τα αποτελέσματα της διατριβής, είναι το γεγονός ότι τα συστήματα διαχείρισης ταυτοτήτων που βασίζονται στους ρόλους για την απόδοση προνομίων προσπέλασης δεν είναι σε θέση να αξιολογούν την αξιοπιστία των χρηστών στους οποίους αποδίδονται δικαιώματα δημιουργίας και δημοσίευσης περιεχομένου.

Η καλή ή η κακή συμπεριφορά των χρηστών σε ένα συνεργατικό περιβάλλον, όπως ορίζεται από το βαθμό στον οποίο δημοσιεύουν περιεχόμενο το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων, αν και αποτελεί χαρακτηριστικό της ψηφιακής τους ταυτότητας δεν προσδιορίζεται από το ρόλο που τους αποδίδεται όταν ταυτοποιούνται στον Πάροχο Ταυτοτήτων. Για παράδειγμα, είτε κάποιος χρήστης είναι *Ανώνυμος*, που σημαίνει ότι ο Πάροχος του εμπιστεύεται περιορισμένα προνόμια προσπέλασης, είτε έχει το ρόλο του *Διαχειριστή*, όταν πρόκειται για τη χρήση υπηρεσιών κοινωνικής αλληλεπίδρασης, ο χρήστης είναι εξίσου επιρρεπής στη δημιουργία περιεχομένου το οποίο προσβάλλει την ιδιωτικότητα.

Χαρακτηριστικό της κρισιμότητας τους προβλήματος αποτελεί η παρατήρηση ότι όλα τα πληροφοριακά συστήματα και ιδιαίτερα αυτά που εφαρμόζονται σε κρίσιμους τομείς όπως για παράδειγμα της η-Διακυβέρνησης οι οποίοι χαρακτηρίζονται από υψηλές απαιτήσεις ασφάλειας και ιδιωτικότητας, αναβαθμίζονται με όλο και γρηγορότερους ρυθμούς σε συνεργατικά περιβάλλοντα ενσωματώνοντας διαδραστικές λειτουργίες και εφαρμογές.

Η διατριβή αναγνωρίζει τον κίνδυνο ότι αν δεν ληφθούν κατάλληλα μέτρα προστασίας, τα νέα περιβάλλοντα συνεργασίας και πλαίσια υπηρεσιών να απαξιωθούν λόγω των κινδύνων που ελλοχεύει η χρήση των εφαρμογών Web 2.0 στην ιδιωτικότητα των συμμετεχόντων.

Σε αυτό το πλαίσιο καθορίζεται το αντικείμενο μελέτης της διατριβής το οποίο επιγραμματικά αφορά στην προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

Αναγνωρίζοντας ότι ακόμα και ένας προνομιούχος με βάση το ρόλο του χρήστη έχει την ίδια δυναμική να προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων με έναν *Ανώνυμο* χρήστη, βασικός στόχος της διατριβής είναι να προτείνει ένα *Έμπιστο Συνεργατικό Πληροφοριακό Σύστημα (ΕΣΠΣ)* το οποίο είναι ικανό να καλύψει τις νέες απαιτήσεις ιδιωτικότητας που επιφέρει η ευρεία χρήση των εφαρμογών Web 2.0, ενσωματώνοντας μια νέα αρχιτεκτονική διαχείρισης ταυτοτήτων η οποία εξασφαλίζει την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

Για να επιτευχθεί αυτός ο στόχος εντοπίζονται πέντε (5) συμπληρωματικοί ερευνητικοί άξονες, καθένας από τους οποίους αποτελεί ξεχωριστό κεφάλαιο των τελικών αποτελεσμάτων της διατριβής:

❖ **Αντικείμενο Διατριβής:**

Η προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

❖ **Ερευνητικοί άξονες Διατριβής:**

- 1) Αρχιτεκτονικός σχεδιασμός *Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος (ΕΣΠΣ)* ικανού να παρέχει ασφαλείς, ιδιωτικές και διαλειτουργικές υπηρεσίες [1, 6, 8].
- 2) *Σχέδιο Ιδιωτικότητας για το ΕΣΠΣ (ΣΙΑ-ΕΣΠΣ)*, ικανό να εξασφαλίσει την προστασία της ιδιωτικότητας από τις νέες απειλές που επιφέρει η χρήση εφαρμογών Web 2.0.
- 3) Καινοτόμος αρχιτεκτονική διαχείρισης ταυτοτήτων, ικανή να παρέχει τη δυνατότητα απόδοσης προνομίων προσπέλασης εντός του συνεργατικού περιβάλλοντος αξιολογώντας την αξιοπιστία των χρηστών στο να δημιουργούν περιεχόμενο το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων [2, 3].
- 4) Καθορισμός *μεθόδου υπολογισμού του βαθμού αξιοπιστίας* των χρηστών, ικανή να αξιολογεί όχι μόνο τη συλλογική γνώση των συμμετεχόντων αλλά και βασικά χαρακτηριστικά του συνεργατικού περιβάλλοντος.
- 5) *Μελέτη περίπτωσης:* Η εφαρμογή του ΕΣΠΣ στον τομέα της η-Διακυβέρνησης και, πιο συγκεκριμένα, στην παροχή υπηρεσιών συνεργασίας και κοινωνικής αλληλεπίδρασης σε νόμιμους μετανάστες [4, 7].

Ο τρόπος με τον οποίο τα αποτελέσματα της διατριβής καλύπτουν καθένα από τους πέντε (5) ερευνητικούς άξονες παρουσιάζεται στην επόμενη ενότητα όπου περιγράφεται η δομή και τα περιεχόμενα του κάθε κεφαλαίου.

1.2 Δομή

Τα περιεχόμενα της διατριβής ταξινομούνται σε οχτώ (8) κεφάλαια εκ των οποίων το πρώτο αποτελεί την παρούσα εισαγωγή. Κάθε ένα από τα υπόλοιπα περιλαμβάνει μια εισαγωγική ενότητα, την ανάλυση των αποτελεσμάτων για κάθε ερευνητικό άξονα της διατριβής, μια τελική ενότητα με τα συμπεράσματα κάθε κεφαλαίου καθώς και μια ενότητα όπου παρατίθενται οι βιβλιογραφικές αναφορές που αποτελέσαν την βάση της έρευνας.

Στο **πρώτο κεφάλαιο** γίνεται περιγραφή του αντικειμένου μελέτης της διδακτορικής διατριβής εντοπίζοντας την ανάγκη αντιμετώπισης των απειλών που επιφέρει η εφαρμογή των σύγχρονων τεχνολογιών Web 2.0, μέσω του επαναπροσδιορισμού της έννοιας της εμπιστοσύνης ώστε να περιλαμβάνει και τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών. Παρουσιάζεται ο βασικός στόχος της διατριβής και οι 5 ερευνητικοί άξονες από τους οποίους αποτελείται, η δομή της διατριβής μέσω της παρούσας συνοπτικής περιγραφής κάθε κεφαλαίου και στην τελική ενότητα απαριθμούνται οι εργασίες του Υποψηφίου που έχουν δημοσιευτεί σε διεθνή επιστημονικά περιοδικά, σε πρακτικά διεθνών συνεδρίων με κριτές καθώς και σε κεφάλαια βιβλίων .

Το **δεύτερο κεφάλαιο** περιλαμβάνει την ανάλυση του θεωρητικού και του τεχνολογικού υποβάθρου για κάθε έναν από τους ερευνητικούς τομείς τους οποίους πραγματεύεται η διατριβή και αφορούν: *τη συνεργασία*, όπως καθορίζεται από την εξέλιξη των εφαρμογών Web 2.0, *την ιδιωτικότητα*, η οποία βασίζεται στις σύγχρονες λύσεις Διαχείρισης Ταυτοτήτων, *την προσβασιμότητα*, η οποία καθορίζεται από τους μηχανισμούς λήψης αποφάσεων εξουσιοδότησης, και τα αντίστοιχα μοντέλα ελέγχου προσπέλασης, καθώς και *την αξιοπιστία των χρηστών* η οποία αποτελεί αντικείμενο των *Συστημάτων Φήμης (reputation systems)*. Για κάθε έναν από αυτούς τους τομείς παρουσιάζονται τα αποτελέσματα της έρευνας πεδίου και εντοπίζονται τα ανοιχτά θέματα στα οποία επικεντρώνεται η διατριβή. Για κάθε ένα από αυτά περιγράφεται συνοπτικά η συνεισφορά της διατριβής με βάση τους στόχους που καθορίστηκαν στο πρώτο κεφάλαιο.

Στο **τρίτο κεφάλαιο** αναλύονται οι βασικές απαιτήσεις σχεδιασμού εμπιστων πληροφοριακών συστημάτων συνεργασίας και καθορίζονται οι θεμελιώδεις αρχές για τη διασφάλιση των απαραίτητων επιπέδων ασφάλειας, ιδιωτικότητας και διαλειτουργικότητας. Πιο συγκεκριμένα, εκτός των συνεργατικών εφαρμογών οι οποίες παρέχουν τη δυνατότητα έκφρασης προσωπικών απόψεων, πεποιθήσεων και σχολίων και τη δημιουργία περιεχομένου από τους ίδιους τους χρήστες η διατριβή προτείνει ότι τα σύγχρονα συνεργατικά πληροφοριακά συστήματα θα πρέπει επίσης να ολοκληρώνουν τεχνολογικές υποδομές οι οποίες επιτρέπουν την συλλογή και διαχείριση ποικίλου ψηφιακού περιεχομένου και την παροχή προηγμένων δυνατοτήτων και καινοτόμων υπηρεσιών (π.χ. μοντελοποίηση και εναρμόνιση διαδικασιών, ανοιχτές

διαβουλεύσεις, αναζήτηση εγγράφων, πληροφοριών και συλλογικής γνώσης, και υποστήριξη αποφάσεων).

Σύμφωνα με τις απαιτήσεις που καθορίστηκαν στο τρίτο κεφάλαιο, στο **τέταρτο κεφάλαιο** παρουσιάζεται η βασική συνεισφορά στον πρώτο ερευνητικό άξονα της διατριβής με τον ορισμό του αρχιτεκτονικού σχεδίου ενός ολοκληρωμένου Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος (ΕΣΠΣ). Έτσι καλύπτεται η ανάγκη για τον ορισμό μιας προτυποποιημένης μεθοδολογίας σχεδιασμού αξιόπιστων πληροφοριακών συστημάτων συνεργασίας και προτείνεται μια ασφαλής, διαλειτουργική και επεκτάσιμη αρχιτεκτονική. Η περιγραφή γίνεται υιοθετώντας το προτυποποιημένο μοντέλο RM-ODP και βασικές αρχές ανάλυσης και σχεδιασμού χρησιμοποιώντας τη γλώσσα μοντελοποίησης UML.

Στο **πέμπτο κεφάλαιο** παρουσιάζεται η ανάλυση επικινδυνότητας του ΕΣΠΣ ως προς τις απειλές ιδιωτικότητας που αντιμετωπίζει και παρουσιάζεται η δεύτερη κατά σειρά συνεισφορά της διατριβής η οποία αφορά στον καθορισμό ενός ολοκληρωμένου Σχεδίου Ιδιωτικότητας (ΣΙΑ-ΕΣΠΣ). Για κάθε ένα από τα κρίσιμα συστήματα που ενσωματώνονται στην αρχιτεκτονική του ΕΣΠΣ καταγράφονται οι σημαντικότερες απειλές, επιθέσεις και μέτρα προστασίας και γίνεται αναφορά στον τρόπο με τον οποίο τα αποτελέσματα της διατριβής που παρουσιάζονται στο έκτο κεφάλαιο συνεισφέρουν στην κάλυψη των ανοιχτών θεμάτων που εντοπίστηκαν κατά την έρευνα πεδίου.

Στο **έκτο κεφάλαιο** παρουσιάζονται δύο ακόμα συνεισφορές της διατριβής, οι οποίες αφορούν στη διαχείριση ταυτοτήτων και την προστασία της ιδιωτικότητας στο πλαίσιο λειτουργίας του ΕΣΠΣ. Πιο συγκεκριμένα, η τρίτη κατά σειρά συνεισφορά της διατριβής περιλαμβάνει τον καθορισμό μιας καινοτόμου αρχιτεκτονικής διαχείρισης ταυτοτήτων η οποία βασίζεται στην αξιολόγηση της αξιοπιστίας των χρηστών και όχι του ρόλου τους όπως είναι η κοινή πρακτική, για την απόδοση προνομίων προσπέλασης στις υπηρεσίες του συνεργατικού περιβάλλοντος. Για το σκοπό, αυτό ο βαθμός αξιοπιστίας προσδιορίζεται ως κρίσιμο χαρακτηριστικό της ταυτότητας, καθώς αναπαριστά την εμπιστοσύνη μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον και προσδιορίζει το βαθμό στον οποίο δημιουργούν περιεχόμενο το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων. Η τέταρτη συνεισφορά της διατριβής παρουσιάζεται στη συνέχεια του κεφαλαίου και περιλαμβάνει τον καθορισμό μιας αναδρομικής μεθόδου υπολογισμού του βαθμού αξιοπιστίας η οποία λαμβάνει υπόψιν τόσο τη συλλογική γνώση των χρηστών μέσω των αναφορών κακόβουλης συμπεριφοράς που υποβάλλουν, όσο και άλλων κρίσιμων, στα πλαίσια λειτουργίας του ΕΣΠΣ, χαρακτηριστικών.

Στο **έβδομο κεφάλαιο** παρουσιάζεται η μελέτη περίπτωσης εφαρμογής του ΕΣΠΣ στον τομέα της ηλεκτρονικής Διακυβέρνησης και πιο συγκεκριμένα για την παροχή ηλεκτρονικών υπηρεσιών σε νόμιμους μετανάστες. Στόχος είναι να

αναδειχθούν τα οφέλη και η ευκολία προσαρμογής της προτεινόμενης αρχιτεκτονικής καθώς και η χρησιμότητα τέτοιων υποδομών σε ιδιαίτερα πολύπλοκους τομείς οι οποίοι απαιτούν τη συνεργασία και την αλληλεπίδραση μεταξύ των χρηστών με ασφαλή, έμπιστο και αξιόπιστο τρόπο. Η τελική συνεισφορά της διατριβής αφορά στην ενίσχυση των υφιστάμενων πρακτικών και υπηρεσιών στον τομέα της η-Διακυβέρνησης προδιαγράφοντας τόσο το εννοιολογικό πλαίσιο παροχής υπηρεσιών η-Μετανάστευσης όσο και την τεχνική εφαρμογή του μέσω της αρχιτεκτονικής του ΕΣΠΣ. Προσφέροντας τη δυνατότητα σε όλους τους εμπλεκόμενους φορείς για ενεργή συμμετοχή, κοινωνική αλληλεπίδραση και ανοιχτή πρόσβαση σε συλλογική γνώση η διατριβή διαπιστώνει ότι τα σύγχρονα πλαίσια ηλεκτρονικών υπηρεσιών που βασίζονται σε έμπιστα πληροφοριακά συστήματα θα είναι ικανά να αντιμετωπίσουν τις νέες προκλήσεις και να υποστηρίξουν την αποτελεσματική ανάπτυξη και εναρμόνιση πολιτικών και διαλειτουργικών υπηρεσιών.

Στο **όγδοο κεφάλαιο** γίνεται ανακεφαλαίωση της διατριβής και καθορίζονται μελλοντικές ερευνητικές κατευθύνσεις. Πιο συγκεκριμένα παρουσιάζονται τα συμπεράσματα που προέκυψαν κατά την εκπόνηση της διατριβής και παρουσιάζεται μία σειρά θεμάτων που θα μπορούσαν να αποτελέσουν ανοιχτά πεδία για περαιτέρω έρευνα.

1.3 Δημοσιεύσεις αποτελεσμάτων

- [1] G. Pentafronimos, A. Karantjias, and N. Polemi (2012). “Collaborative information and knowledge management environments: The “what” and “how””. *OR Insight - Operational Research Journal, Special Issue on Facilitating information and knowledge management through Information Systems and Operational Research: from theory to practice*. Vol. 25, no. 2, pp. 105-123. Pallgrave Macmillan, July 2012.
- [2] G. Pentafronimos, T. Karantjias, and N. Polemi (2012). “PEIM2.0: A privacy-enhancing IAM architecture for collaborative environments”. In *Proceedings of the 6th International Conference on Methodologies, Technologies and Tools enabling e-Government, (MeTTeG 2012)*. Belgrade, Serbia, July 3-5 2012. (Προς Δημοσίευση)
- [3] G. Pentafronimos, A. Karantjias, and N. Polemi (2011). “Open Issues on Privacy and Trust in Collaborative Environments”. In *Proceedings of the IEEE Symposium on Computers and Communications (ISCC 2011)*, Kerkyra, Greece, June 28 – July 1 2011, pp. 876-880. IEEE Xplore.
- [4] N. Polemi, G. Pentafronimos, and T. Ntouskas (2011). “IMP2.0 Migration Collaborative Platform and e-Services”. In *Proceedings of the Eleventh IFIP Conference on e-Business, e-Services and e-Society (I3E2011)*, Kaunas, Lithuania, October 12-14 2011, pp. 40-57. Springer Verlag (IFIP-AICT Book Series).
- [5] T. Ntouskas, G. Pentafronimos, S. Papastergiou (2011). “STORM - Collaborative Security Management Environment”. In *Proceedings of the Fifth Workshop In Information Security Theory And Practice (WISTP 2011)*. Security and Privacy of Mobile Devices in Wireless Communication, (WISTP 2011). Heraklion, Greece. Springer Verlag.
- [6] G. Pentafronimos, A. Karantjias, and N. Polemi (2010). “ODYSSEUS: An Advanced, Collaborative and Trusted Framework for the Provision of Migration Services”. In *Proceedings of the Fifth International Conference on Internet and Web Applications and Services (ICIW 2010)*, Barcelona, Spain, May 9-15 2010, pp. 531-537. IEEE Xplore.

- [7] A. Karantjias, N. Polemi, and G. Pentafronimos (2010). "Participatory immigration policy making and harmonization services based on collaborative Web 2.0 technologies". In A. Syed, M. Ilyas (Eds.) *Service Delivery Platforms: Developing Converged Multimedia Services Handbook*, pp. 357–374. CRC Press, Taylor & Francis Group Publishing.
- [8] G. Pentafronimos, A. Karantjias and N. Polemi (2009). "OPIS: An Open, Preventive and Scalable Migration Information System". In *Proceedings of the 3rd International Conference on e-Democracy. Next Generation Society: Technological and Legal Issues, (e-Democracy 2009)*. Athens, Greece, September 23-25 2009. Vol. 26, no. 9, pp. 341-350. Springer Verlag.
- [9] G. Pentafronimos, S. Papastergiou, and N. Polemi (2008). "Interoperability Testing for e-Government Web Services". In *Proceedings of the Second International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008)*, Cairo, Egypt, December 1-4 2008, pp. 316 – 321. ACM.
- [10] Γ. Πενταφρόνιμος, Δ. Πολέμη (2008). 'Υπηρεσία Διαπιστευτηρίων Ψηφιακών Ταυτοτήτων', Ελληνική Εταιρεία Συστημικών Μελετών (ΕΕΣΜ), In *Proceedings of the Fourth National & International Conference on Information and Innovation Management Systems*, Μάιος 2008, Ιωάννινα, Ελλάδα.

Πανεπιστήμιο Πειραιώς

Κεφάλαιο 2

Ερευνητικό Πεδίο - Ανοιχτά Θέματα

Σε αυτό το κεφάλαιο γίνεται ανάλυση του θεωρητικού και του τεχνολογικού υποβάθρου για κάθε έναν από τους τέσσερις ερευνητικούς τομείς των σύγχρονων Πληροφοριακών Συστημάτων τους οποίους πραγματεύεται η διατριβή. Παρουσιάζονται τα αποτελέσματα της έρευνας πεδίου που πραγματοποιήθηκε και εντοπίζονται ανοιχτά θέματα τα οποία καλύπτονται στα επόμενα κεφάλαια.

2.1 Εισαγωγή

Οι τέσσερις ερευνητικοί τομείς τους οποίους περιλαμβάνει το πλαίσιο έρευνας της διατριβής είναι:

1. Η *Συνεργασία*, όπως καθορίζεται από τις δυνατότητες διαδραστικότητας και κοινωνικής αλληλεπίδρασης που παρέχουν οι εφαρμογές Web2.0 και τα σύγχρονα συνεργατικά περιβάλλοντα.
2. Η *Ιδιωτικότητα*, η οποία παραδοσιακά καθορίζεται από τις δυνατότητες που παρέχουν τα Συστήματα Διαχείρισης Ταυτοτήτων και οι πολιτικές ιδιωτικότητας.
3. Η *Προσβασιμότητα*, η οποία καθορίζεται από τους μηχανισμούς ελέγχου που υιοθετούνται για την απόδοση δικαιωμάτων προσπέλασης στους πόρους (π.χ. υπηρεσίες, λειτουργίες) των Πληροφοριακών Συστημάτων.
4. Η *Αξιοπιστία* των χρηστών που συμμετέχουν σε συνεργατικά περιβάλλοντα και έχουν τη δυνατότητα ενεργής συνεισφοράς και δημιουργίας περιεχομένου, η οποία παραδοσιακά αποτελεί αντικείμενο διαχείρισης των συστημάτων φήμης (reputation systems) και εξαρτάται από τη μέθοδο υπολογισμού του βαθμού αξιοπιστίας (reputation score) που υιοθετείται κάθε φορά.

Στο πλαίσιο της διατριβής η έννοια της συνεργασίας υπονομεύει την έννοια της ιδιωτικότητας καθώς οι διαδραστικές δυνατότητες που παρέχουν οι εφαρμογές Web 2.0 αποτελούν απειλές για τα *προσωπικά δεδομένα* των χρηστών αν λάβει κανείς υπόψιν ότι μέσω της κακόβουλης χρήσης τους είναι δυνατή η δημόσια αποκάλυψη ευαίσθητων πληροφοριών χωρίς τη συγκατάθεση του ιδιοκτήτη.

Αναγνωρίζοντας τις νέες προκλήσεις που προκύπτουν από τις δυνατότητες που παρέχουν οι συνεργατικές εφαρμογές, στη διατριβή η έννοια της ιδιωτικότητας επεκτείνεται ώστε να περιλαμβάνει την προστασία των προσωπικών δεδομένων από τους ίδιους τους χρήστες. Πιο συγκεκριμένα, διαπιστώνεται ότι στα πλαίσια ενός συνεργατικού περιβάλλοντος η ιδιωτικότητα καθορίζεται όχι μόνο από τις σχέσεις εμπιστοσύνης και της φερέγγυας αλληλεπίδρασης μεταξύ των Παρόχων (οι οποίες συχνά προδιαγράφονται από πρότυπα ασφάλειας και αρχιτεκτονικές ομοσπονδιακής διαχείρισης υπηρεσιών) και τις σχέσεις μεταξύ χρηστών και Παρόχων (όπως ορίζονται από την αποδοχή των πολιτικών ιδιωτικότητας κατά την ταυτοποίηση των χρηστών στο πληροφοριακό σύστημα) [2] αλλά, πολύ περισσότερο, από τις σχέσεις μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον.

Δεδομένου ότι όλοι οι χρήστες έχουν τις ίδιες δυνατότητες να αποκαλύψουν προσωπικά δεδομένα των υπολοίπων συμμετεχόντων μέσω της χρήσης των εφαρμογών Web 2.0, η διατριβή προτείνει ότι για να θεωρηθεί ένα συνεργατικό περιβάλλον ως *έμπιστο* θα πρέπει η ιδιωτικότητα να προστατεύεται όχι μόνο σε επίπεδο Παρόχων [6], με βάση τις πολιτικές ιδιωτικότητας, αλλά και σε επίπεδο χρηστών αντιμετωπίζοντας τις απειλές αποκάλυψης ευαίσθητων δεδομένων που επιφέρει η χρήση των εφαρμογών Web 2.0 [12. 23].

Έχοντας καθορίσει την έννοια της ιδιωτικότητας έτσι ώστε να περιλαμβάνει τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών, η αξιοπιστία ενός χρήστη αντιπροσωπεύει την εμπιστοσύνη των υπολοίπων χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον ως συνάρτηση των αξιολογήσεων της συμπεριφοράς του. Έτσι, ένας χρήστης με υψηλό βαθμό αξιοπιστίας χαρακτηρίζεται για την καλή φήμη που έχει μεταξύ του συνόλου των συμμετεχόντων στο συνεργατικό περιβάλλον όσον αφορά στον τρόπο με τον οποίο σέβεται την ιδιωτικότητα των υπολοίπων χρηστών.

Συνθέτοντας τα παραπάνω, στο πλαίσιο της διατριβής διαπιστώνεται ότι η απόδοση προνομίων προσπέλασης σε συνεργατικά περιβάλλοντα απαιτεί τον έλεγχο της αξιοπιστίας των χρηστών με δυναμικό τρόπο, έτσι ώστε να λαμβάνονται έμπιστες αποφάσεις εξουσιοδότησης. Αυτό προϋποθέτει την καταγραφή των αναφορών κακόβουλης συμπεριφοράς και την αξιολόγηση του βαθμού αξιοπιστίας των χρηστών κάθε χρονική στιγμή που οι χρήστες αιτούνται να προσπελάσουν τις υπηρεσίες Web 2.0.

Στη συνέχεια παρουσιάζονται τα αποτελέσματα της έρευνας πεδίου που πραγματοποιήθηκε για καθέναν από τους τέσσερις ερευνητικούς τομείς.

2.2 Συνεργασία

Η συνεργασία είναι μια διαδικασία η οποία εξασφαλίζει ότι οι οντότητες που αλληλεπιδρούν βλέπουν ένα συγκεκριμένο πρόβλημα από διαφορετικές οπτικές γωνίες και έτσι είναι σε θέση να αναζητήσουν λύσεις οι οποίες προχωρούν

πέραν της δικής τους περιορισμένης αντίληψης. Μάλιστα στη σύγχρονη εποχή η διαδικτυακή συνεργασία σημαίνει πολλά περισσότερα από τη συνεργασία ανθρώπων σε επίπεδο ομάδας ή κοινότητας [11, 17, 18].

Παλαιότερα μοντέλα συνεργασίας είχαν την τάση να επικεντρώνονται σε ομάδες και τυπικά δομημένες κοινότητες χρηστών. Με την εξέλιξη του Web 2.0 τα σύγχρονα συστήματα είναι σε θέση να παρέχουν περισσότερες δυνατότητες. Έτσι διακρίνονται οι εξής κατηγορίες [13]:

- ✓ **Ομαδική συνεργασία (Group-based collaboration):** Τα μέλη της ομάδας γνωρίζονται μεταξύ τους, έχουν διακριτές αρμοδιότητες και συγκεκριμένους στόχους να επιτελέσουν ενώ, παράλληλα, χαρακτηρίζονται και από σχέσεις αλληλεξάρτησης. Προκειμένου να επιτευχθεί ο γενικότερος στόχος, τα μέλη της ομάδας θα πρέπει να επιτελούν τις αλληλεξαρτώμενες διεργασίες τους συνήθως εντός συγκεκριμένων χρονικών περιορισμών. Στα πλαίσια αυτής της κατηγορίας συνεργασίας παρόλο που είναι απαραίτητος ο ρόλος ενός επικεφαλής, οι συμμετέχοντες συνεργάζονται με ισότιμο τρόπο και λαμβάνουν εξίσου την ίδια αναγνώριση.
- ✓ **Κοινοτική συνεργασία (Community-based collaboration):** Υπάρχει μια κοινή περιοχή ενδιαφέροντος αλλά ο τελικός στόχος τις περισσότερες φορές είναι η απόκτηση γνώσης και όχι η επίτευξη συγκεκριμένων διεργασιών. Οι χρήστες μοιράζονται πληροφορίες και δημιουργούν νέα γνώση χωρίς να είναι απαραίτητο να ακολουθήσουν κάποια συγκεκριμένη διαδικασία. Τα μέλη των κοινοτήτων χρησιμοποιούν αυτά τα πλαίσια συνεργασίας προκειμένου να αναζητούν λύσεις στα προβλήματά τους θέτοντας ερωτήσεις και λαμβάνοντας συμβουλές. Στη συνέχεια χρησιμοποιούν αυτή τη γνώση στα πλαίσια των ομάδων τους προκειμένου να υλοποιηθούν οι απαιτούμενες διεργασίες. Όσον αφορά στα προνόμια των συμμετεχόντων, αν και συνήθως όλα τα μέλη συμμετέχουν με τα ίδια δικαιώματα, οι περισσότερο έμπειροι και αναγνωρισμένοι χρήστες ενδέχεται να έχουν μια πιο διακεκριμένη θέση στην κοινότητα και αντίστοιχα δικαιώματα εξουσιοδότησης όσον αφορά στη διαχείριση του περιεχομένου.
- ✓ **Ανοιχτή συνεργασία (Open collaboration):** Αυτή η προσέγγιση προχωρά ένα βήμα παραπάνω από τις προηγούμενες λαμβάνοντας υπόψιν την προσωπική πρωτοβουλία και την ανάγκη του ατόμου να συνεργαστεί με άλλους χρήστες με κοινά ενδιαφέροντα και στόχους η οποία τελικά καταλήγει σε ανοιχτά δίκτυα συνεργασίας. Σε αυτό το μοντέλο δεν υπάρχουν συγκεκριμένοι ρόλοι ή χρονικοί περιορισμοί και τα μέλη ενδέχεται να μην γνωρίζονται μεταξύ τους. Παρόλα αυτά η συλλογή, επεξεργασία και διασύνδεση των πληροφοριών που παράγονται από την αλληλεπίδραση των μελών εντός του πλαισίου συνεργασίας είναι το πολύτιμο αγαθό που παράγεται και αφορά όχι μόνο στα μέλη του δικτύου συνεργασίας αλλά όλων των εμπλεκόμενων φορέων που σχετίζονται με το συγκεκριμένο θέμα.

Αυτή η μορφή συνεργασίας καθοδηγείται από την εξέλιξη των κοινωνικών μέσων και των εφαρμογών Web 2.0.

Ο όρος Web 2.0 οφείλει την ύπαρξή του σε εφαρμογές, υπηρεσίες και εργαλεία λογισμικού ικανά να παρέχουν εκείνες τις καινοτομίες και ευκολίες χρήσης τις οποίες αναζητούσαν οι χρήστες στις καθημερινές τους αλληλεπιδράσεις, γι' αυτό και έτυχε ευρείας αποδοχής και ταχείας διάδοσης.

Η εξέλιξη των τεχνολογιών και εφαρμογών Web 2.0 παρέχει τη δυνατότητα στον καθένα να διευρύνει το δίκτυο συνεργασίας του λαμβάνοντας βοήθεια και συμβουλές από άλλους χρήστες που έχουν συγκεκριμένη εμπειρία σε κάποιο θέμα. Παρά το γεγονός ότι δεν τους συνδέει κάποια γνωριμία σε φυσικό επίπεδο, οι γνώσεις και οι πληροφορίες που είναι σε θέση να ανταλλάζουν είναι το πολύτιμο αγαθό που παράγεται από τις αντίστοιχες αλληλεπιδράσεις [10].

Αναγνωρίζοντας την ανάγκη που υπάρχει για συλλογική δράση ώστε να επιλυθούν πολύπλοκα προβλήματα σε κρίσιμους τομείς της Ψηφιακής Εποχής, η διατριβή προτείνει ότι η υιοθέτηση συνεργατικών προσεγγίσεων είναι απαραίτητη για την ανάπτυξη καινοτόμων λύσεων υψηλής προστιθέμενης αξίας. Αναφέρεται χαρακτηριστικά ότι τα οφέλη των συνεργατικών πληροφοριακών συστημάτων αφορούν στο σύνολο των εμπλεκόμενων φορέων που σχετίζονται με το πρόβλημα και όχι μόνο στα μέλη που συμμετέχουν ενεργά στο πλαίσιο συνεργασίας.

2.2.1 Έρευνα πεδίου σε εφαρμογές Web 2.0

Οι σύγχρονες εφαρμογές Web 2.0 υποστηρίζουν την απεριόριστη ανταλλαγή πληροφοριών και τη δυναμική δημιουργία περιεχομένου παρέχοντας τη δυνατότητα στους τελικούς χρήστες να γίνουν ενεργά μέλη μιας ψηφιακής κοινότητας, να μοιραστούν τη γνώση τους και να συμμετάσχουν σε ανοιχτές συζητήσεις [43]. Δεδομένου μάλιστα ότι επιφέρουν αλλαγές στην γνώση των χρηστών και των ψηφιακών κοινοτήτων, βοηθούν στην καλύτερη κατανόηση πολύπλοκων θεμάτων και επιτρέπουν τη γόνιμη αλληλεπίδραση μεταξύ συμμετεχόντων με αντικρουόμενες και ανταγωνιστικές απόψεις. Επίσης, είναι ικανά να υποστηρίξουν τη λήψη αποφάσεων και το σχεδιασμό εναρμονισμένων στρατηγικών και πολιτικών [37, 38].

Πιο κάτω γίνεται ανασκόπηση των πιο διαδεδομένων εφαρμογών Web 2.0 δίνοντας έμφαση στα χαρακτηριστικά και τις δυνατότητες που προσφέρει η καθεμία.

2.2.1.1 Ιστολόγια (Blogs)

Τα ιστολόγια αποτελούν διαδραστικά εργαλεία διαδικτυακής επικοινωνίας. Είναι δικτυακοί τόποι οι οποίοι περιέχουν καταχωρίσεις (posts) από χρήστες του διαδικτύου. Οι χρήστες είναι σε θέση να δημοσιεύουν τις σκέψεις τους, τις ιδέες τους, τις προτάσεις τους και τα σχόλιά τους.

Τα ιστολόγια διαθέτουν ιδιαίτερα χαρακτηριστικά τα οποία τα κάνουν να ξεχωρίζουν από τις παραδοσιακές μορφές ηλεκτρονικής επικοινωνίας και παροχής υπηρεσιών. Για παράδειγμα, ο καθένας μπορεί να δημοσιεύει καταχωρίσεις εύκολα και γρήγορα, καθώς και να τοποθετείται σε κάποιο θέμα εισάγοντας το δικό του σχόλιο. Τελικά, οι καταχωρίσεις και τα σχόλια των χρηστών είναι άμεσα διαθέσιμα σε όλο το εύρος του Διαδικτύου.

Ένα αρνητικό χαρακτηριστικό των ιστολογίων αποτελεί το ενδεχόμενο κακόβουλης κριτικής και δημόσιας προσβολής της ιδιωτικότητας των συμμετεχόντων. Έτσι ενώ από τη μια πλευρά είναι σημαντικό να μπορεί κάθε χρήστης να παρουσιάζει τις ιδέες του ελεύθερα στην περίπτωση που προσβάλλουν άλλους χρήστες είναι σημαντικό να υπάρχουν τα κατάλληλα μέτρα προστασίας.

2.2.1.2 Wiki

Οι δυνατότητες των wiki συνίστανται στην ευκολία χρήσης και τις δυνατότητες συνεργασίας που προσφέρουν. Επιτρέπουν την ανταλλαγή γνώσεων και ενθαρρύνουν τους χρήστες να επεξεργάζονται το περιεχόμενο κάθε άρθρου συνεισφέροντας τις γνώσεις τους. Με αυτόν τον τρόπο, παρέχεται η δυνατότητα συνεχούς βελτίωσης και ενημέρωσης του περιεχομένου σε όλη τη διάρκεια του κύκλου ζωής του.

Ένα wiki μπορεί να είναι είτε ανοιχτό είτε κλειστό, ανάλογα με τους στόχους της κοινότητας που το χρησιμοποιεί και τις ανάγκες της εκάστοτε μελέτης εφαρμογής. Ένα ανοιχτό wiki επιτρέπει σε οποιονδήποτε να κάνει αλλαγές και να προσπελάσει το περιεχόμενό του. Ένα κλειστό wiki επιτρέπει μόνο στα εγγεγραμμένα μέλη της κοινότητας να κάνουν αλλαγές ή ακόμα και να προσπελάσουν το περιεχόμενό του.

Γενικά τα περισσότερα wiki επιτρέπουν την πρόσβαση των χρηστών χωρίς κανέναν απολύτως περιορισμό. Έτσι έχουν όλοι τα ίδια δικαιώματα να συμβάλλουν στη συγγραφή του περιεχομένου της ιστοσελίδας χωρίς απαραίτητα να υποβάλλονται σε διαδικασίες αυθεντικοποίησης και εξουσιοδότησης. Αυτό έχει σαν αποτέλεσμα σε πολλές περιπτώσεις να μην είναι δυνατό να ελεγχθεί η εγκυρότητα και η αξιοπιστία των πληροφοριών που δημοσιεύονται.

2.2.1.3 Φόρουμ (Forum)

Το φόρουμ είναι ένας διαδικτυακός τόπος όπου ο καθένας μπορεί να δημοσιεύσει και να ανταλλάξει πληροφορίες. Οποιοσδήποτε χρήστης ακόμη και χωρίς τεχνικές γνώσεις και εμπειρία μπορεί να διαχειριστεί ένα φόρουμ και να συνομιλήσει για το αγαπημένο του θέμα με άλλα άτομα με κοινά ενδιαφέροντα. Γι' αυτό το λόγο θεωρείται και ως μια μικρή κοινότητα.

Κάθε μέλος της κοινότητας ενός φόρουμ έχει τη δυνατότητα να δημοσιεύσει ένα μήνυμα, το οποίο είναι διαθέσιμο σε όλα τα άτομα τα οποία ανήκουν σε αυτήν. Επίσης παρέχεται η δυνατότητα δημοσίευσης σχολίων σχετικών με το κάθε μήνυμα και είναι δυνατόν να δημιουργηθεί μια ανοιχτή συζήτηση χωρίς να είναι απαραίτητο όλοι οι χρήστες να είναι συνδεδεμένοι στο διαδίκτυο την ίδια χρονική στιγμή.

Αν και τα φόρουμ χρησιμοποιούνται συνήθως για να υποβάλλουν οι χρήστες ερωτήσεις, να μοιράζονται πληροφορίες, ή να συζητούν τις ιδέες τους δεν παύουν να αποτελούν μια σημαντική απειλή της ιδιωτικότητας των συμμετεχόντων καθώς οποιοσδήποτε χρήστης έχει τη δυνατότητα να αποκαλύψει ακούσια ή εσκεμμένα ευαίσθητα και προσωπικά δεδομένα ιδιαίτερα όταν το περιεχόμενό τους αναφέρεται σε κρίσιμους τομείς, όπως της Διακυβέρνησης, της Υγείας και της Εκπαίδευσης.

2.2.1.4 Widget

Ένα widget είναι ένα φορητό κομμάτι κώδικα που μπορεί να εγκατασταθεί και να εκτελεστεί από τον τελικό χρήστη σε οποιαδήποτε ιστοσελίδα χωρίς την απαίτηση μεταγλώττισης. Αποτελεί μια αυτόνομη εφαρμογή που μπορεί να ενσωματωθεί εύκολα σε ιστοσελίδες όπου οι χρήστες έχουν δικαιώματα δημιουργίας περιεχομένου, όπως για παράδειγμα σε ένα ιστολόγιο ή στο προσωπικό προφίλ κάποιου ιστοσελίδας κοινωνικής δικτύωσης. Για παράδειγμα, ένα «Widget Δελτίου Καιρού» ενημερώνει για τον καιρό της ημέρας με πρόσβαση σε δεδομένα από την Μετεωρολογική Υπηρεσία και είναι εύκολα μεταφέσιμο σε ετερογενή περιβάλλοντα.

Ένας σημαντικός παράγοντας για τα widgets είναι το ότι οι τελικοί χρήστες δεν ελέγχουν το περιεχόμενο καθώς η λειτουργικότητα που προσφέρεται δεν είναι δυνατόν να τροποποιηθεί. Παρόλα αυτά οι τελικοί χρήστες είναι εκείνοι οι οποίοι έχουν τον έλεγχο εγκατάστασης και εφαρμογής του widget, καθώς χρειάζεται η συγκατάθεση του χρήστη για την ολοκλήρωση των διαδικασιών.

Η διατριβή διαπιστώνει ότι δεν πρέπει όλοι οι χρήστες ενός συνεργατικού περιβάλλοντος να έχουν ίσα δικαιώματα διαχείρισης των widgets καθώς ενδέχεται ορισμένοι από αυτούς να τα χρησιμοποιούν με κακόβουλο τρόπο και, συνεπώς, θα πρέπει να περιορίζονται τα προνόμια προσπέλασης που τους είχαν αρχικά αποδοθεί.

2.2.1.5 Service Mashup

Το *Service Mashup* αποτελεί ένα νέο ευέλικτο μοντέλο ανάπτυξης εφαρμογών. Πιο συγκεκριμένα αναφέρεται σε διαδικτυακές εφαρμογές οι οποίες συγκεντρώνουν δεδομένα από διαφορετικές πηγές, τα επεξεργάζονται και τα δημοσιεύουν σε νέα μορφή. Πολλές φορές τα mashups αφορούν σε υπηρεσίες που απαιτούν κωδικούς πρόσβασης, τους οποίους πρέπει να παρέχει ο χρήστης. Σε αυτή την περίπτωση ο χρήστης πρέπει να εμπιστεύεται σε μεγάλο βαθμό τη λειτουργία του mashup καθώς του επιτρέπει τόσο την πρόσβαση σε προσωπικά δεδομένα όσο και την επεξεργασία τους.

Για παράδειγμα, ένα κακόβουλο κομμάτι κώδικα θα ήταν αρκετό για να αναπαράγει ή να αντλεί προσωπικές πληροφορίες χωρίς τη συγκατάθεση του χρήστη. Τέτοιου είδους εφαρμογές χρησιμοποιούνται σε διάφορους τομείς εξυπηρετώντας πολλές και διαφορετικές ανάγκες των χρηστών. Βρίσκουν χρήση στην ανίχνευση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου, στην εύκολη αναζήτηση πληροφοριών σε συνεργατικά περιβάλλοντα ή πλαίσια ηλεκτρονικής διακυβέρνησης τα οποία συλλέγουν πληροφορίες από διάφορες πηγές και προσαρμόζουν το περιεχόμενό τους με βάση αυτές.

2.2.2 Έρευνα πεδίου σε συνεργατικά περιβάλλοντα

Με βάση τα πιο ευρέως διαδεδομένα μοντέλα υπηρεσιών, τα συνεργατικά περιβάλλοντα διακρίνονται σε δύο βασικές κατηγορίες, τα *Κοινωνικά Δίκτυα (Social Networks) - ΚΔ* και τα *Πληροφοριακά Συστήματα συνεργασίας, ή αλλιώς Συνεργατικά Πληροφοριακά Συστήματα (Collaborative Workspaces) - ΣΠΣ* [13].

Τα ΣΠΣ (όπως για παράδειγμα η πλατφόρμα *ImmigrationPolicy2.0*¹) επικεντρώνονται στη διαχείριση πληροφοριών και ολοκληρώνουν προηγμένες τεχνολογίες και εργαλεία λογισμικού, όπως Συστήματα Διαχείρισης Περιεχομένου, Συστήματα Μοντελοποίησης και Διαχείρισης Επιχειρησιακών Διαδικασιών, και Συστήματα Διαχείρισης Ταυτοτήτων ώστε να επιτυγχάνεται η δυναμική συνεισφορά ψηφιακού περιεχομένου (π.χ. έγγραφα, αρχεία πολυμέσων, μοντέλα επιχειρησιακών διαδικασιών, αρχεία XML, οντολογίες, κ.ά.) εκ μέρους των χρηστών και η συλλογική διαχείριση της παραγόμενης γνώσης. Επιπρόσθετα, προκειμένου να ενισχυθεί περαιτέρω η συνεργασία και η αλληλεπίδραση μεταξύ των χρηστών, ολοκληρώνουν ένα σύνολο συνεργατικών εφαρμογών που βασίζονται σε τεχνολογίες Web 2.0 (π.χ. ιστολόγια, φόρουμ, wiki, κ.ά.) ώστε να διευκολύνεται η έκφραση προσωπικών απόψεων και σχολίων και η δυναμική δημιουργία προσωπικού περιεχομένου.

Από την άλλη πλευρά, τα Κοινωνικά Δίκτυα (π.χ. Facebook, LinkedIn, Hyves, MySpace) επικεντρώνονται στη διαχείριση προσωπικών ή εταιρικών προφίλ και

¹ <http://immigrationpolicy.cs.unipi.gr>

των σχέσεων που αναπτύσσονται μεταξύ των χρηστών που συμμετέχουν στο συγκεκριμένο δίκτυο [13]. Βασικά τους χαρακτηριστικά αποτελούν η παρουσίαση και διαχείριση προσωπικών πληροφοριών ως στοιχεία της κοινωνικής ή επαγγελματικής υπόστασης των χρηστών, καθώς και η ανάπτυξη συνδέσεων μεταξύ τους προκειμένου να επιτυγχάνεται η κοινωνική αλληλεπίδραση και η δημιουργία ηλεκτρονικών κοινοτήτων. Αυτές οι σχέσεις κοινωνικής αλληλεπίδρασης ορίζονται με διαφορετικό τρόπο για κάθε ΚΔ με βάση το επιχειρησιακό μοντέλο της εκάστοτε μελέτης εφαρμογής και τις δυνατότητες που παρέχονται στους χρήστες.

Για παράδειγμα, ο τύπος και ο βαθμός διαδραστικότητας των αλληλεπιδράσεων μεταξύ των χρηστών του Facebook είναι διαφορετικός από αυτόν των χρηστών του LinkedIn δεδομένων των σημαντικών διαφορών στο επιχειρησιακό τους μοντέλο, τα οποία είναι προσανατολισμένα στις προσωπικές σχέσεις και στις επαγγελματικές σχέσεις αντίστοιχα.

Επίσης, εντοπίζονται οι δύο ακόλουθες κατηγορίες συνεργατικών συστημάτων:

- ✓ Τα *Ανοιχτά συνεργατικά περιβάλλοντα (open collaborative environments)* αποτελούνται αποκλειστικά από εφαρμογές Web 2.0 και είτε δεν ενσωματώνεται σύστημα διαχείρισης ταυτοτήτων, είτε είναι υποτυπώδες. Γενικά η ανωνυμία και/ή ψευδωνυμία των χρηστών είναι το κεντρικό χαρακτηριστικό τους.
- ✓ Τα *Έμπιστα συνεργατικά περιβάλλοντα (trusted collaborative environments)* αποτελούν μια πιο εξελιγμένη κατηγορία συνεργατικών συστημάτων καθώς διασυνδέονται και αλληλεπιδρούν με άλλα συστήματα με στόχο την παροχή ολοκληρωμένων πλαισίων υπηρεσιών. Βασικό χαρακτηριστικό τους αποτελεί η απαραίτητη ενσωμάτωση συστήματος διαχείρισης ταυτοτήτων και ελέγχου προσπέλασης.

Τα ΣΠΣ και τα ΚΔ εμφανίζουν ένα σημαντικό αριθμό κοινών χαρακτηριστικών, όπως η δυναμική δημιουργία περιεχομένου από τους ίδιους τους χρήστες, οι ενδεχόμενοι κίνδυνοι αποκάλυψης προσωπικών δεδομένων κατά τη διάρκεια της διαδικασίας και, γενικά, είναι και τα δύο ευάλωτα σε επιθέσεις ασφάλειας στις εφαρμογές Web 2.0 που ολοκληρώνουν (βλ. Κεφάλαιο 5).

Από την άλλη πλευρά, οι απαιτήσεις ιδιωτικότητας διαφοροποιούνται αν λάβει κανείς υπόψη το επιχειρησιακό μοντέλο που αντιπροσωπεύει η κάθε κατηγορία συνεργατικού περιβάλλοντος. Βασικό κριτήριο είναι το γεγονός ότι σε αντίθεση με τα ΣΠΣ, στα ΚΔ οι χρήστες αποδέχονται να αποκαλύψουν μέρος των προσωπικών τους δεδομένων προκειμένου να συμμετέχουν στο δίκτυο ή σε κάποια ηλεκτρονική κοινότητα και να επωφεληθούν των παρεχομένων δυνατοτήτων κοινωνικής ή επαγγελματικής αλληλεπίδρασης.

Για το λόγο αυτό, στο πλαίσιο της διατριβής δεν αποτελεί αντικείμενο μελέτης η προστασία της ιδιωτικότητας σε ΚΔ. Η προστασία της ιδιωτικότητας σε

συνεργατικά περιβάλλοντα μελετάται αποκλειστικά στο πλαίσιο των *έμπιστων Συνεργατικών Πληροφοριακών Συστημάτων*, όπως αυτό που περιγράφεται στο τέταρτο Κεφάλαιο. Παρόλα αυτά, πρέπει να σημειωθεί ότι τα αποτελέσματα της διατριβής που αφορούν στη διαχείριση ταυτοτήτων και την προστασία της ιδιωτικότητας και τα οποία παρουσιάζονται στο έκτο Κεφάλαιο, είναι εύκολο να υιοθετηθούν και να ολοκληρωθούν εξίσου αποτελεσματικά και σε περιβάλλοντα *Κοινωνικής Δικτύωσης*.

2.2.3 Ανοιχτά θέματα

Οι εφαρμογές Web 2.0 (π.χ. ιστολόγια, φόρουμ, wiki) επιτρέπουν τη δυναμική δημιουργία περιεχομένου μέσω των διαδραστικών λειτουργιών που παρέχουν στους χρήστες. Παρόλα αυτά, η χρήση τους τις περισσότερες φορές αποδεικνύεται επισφαλής όταν υιοθετείται ξεχωριστά, από ολοκληρωμένα Πληροφοριακά Συστήματα και πλαίσια υπηρεσιών [3].

Επίσης, στα συνεργατικά περιβάλλοντα που προορίζονται για κρίσιμους τομείς, όπως για παράδειγμα αυτός της ηλεκτρονικής Διακυβέρνησης, οι δυνατότητες δυναμικής δημιουργίας περιεχομένου καθιστούν τους Παρόχους Υπηρεσιών (στην περίπτωση αυτή τους κυβερνητικούς φορείς) υπεύθυνους όχι μόνο για την προστασία των προσωπικών δεδομένων των χρηστών που αποκαλύπτονται με τη συγκατάθεσή τους κατά τη διαδικασία ταυτοποίησης, αλλά και για τη διατήρηση ενός έμπιστου περιβάλλοντος το οποίο σέβεται την προστασία της ιδιωτικότητας των συμμετεχόντων [22]. Η εφαρμογή κατάλληλων μέτρων προστασίας των χρηστών από τέτοιου είδους απειλές αποτελεί και τον πιο κρίσιμο παράγοντα στην περαιτέρω χρήση και αποδοχή τους [4, 5].

Αυτά τα ανοιχτά θέματα αποτελούν το αντικείμενο μελέτης της διατριβής στα πλαίσια του ερευνητικού τομέα της *Συνεργασίας* και τα αντίστοιχα αποτελέσματα παρουσιάζονται στο τρίτο και στο τέταρτο κεφάλαιο. Συνοπτικά, η συνεισφορά της διατριβής περιλαμβάνει τον ορισμό ενός *Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος* μέσω της ενδελεχούς ανάλυσης απαιτήσεων και του ορισμού μιας προτυποποιημένης και επεκτάσιμης αρχιτεκτονικής ικανής να παρέχει ασφαλείς, ιδιωτικές και διαλειτουργικές υπηρεσίες στα πλαίσια ενός έμπιστου περιβάλλοντος συνεργασίας.

2.3 Προσβασιμότητα

Η έννοια της *Προσβασιμότητας* σε Πληροφοριακά Συστήματα ορίζεται από την ανάγκη προστασίας των διαθέσιμων πληροφοριών, πόρων και υπηρεσιών ώστε η πρόσβαση να επιτρέπεται μόνο σε εξουσιοδοτημένες *οντότητες*. Ο όρος «Οντότητα» περιλαμβάνει το σύνολο των φυσικών και των λογικών οντοτήτων που ενεργούν προκειμένου να καλέσουν μια υπηρεσία ή να επιτελέσουν κάποιου είδους υπολογιστική διαδικασία [8].

Γενικά, οι κόμβοι προσπέλασης κατηγοριοποιούνται ως προς τις δυνατότητες «ανάγνωσης» ή «εγγραφής» που παρέχουν είτε σε κάποια διαδικασία εκτελέσιμου κώδικα, είτε σε κάποιο αποθηκευτικό μέσο είτε ακόμα και σε κάποιον δικτυακό πόρο ή συσκευή. Οι δυνατότητες αυτές συνήθως εκφράζονται από σαφώς καθορισμένα προνόμια τα οποία έχει η εκάστοτε οντότητα που αλληλεπιδρά με το Πληροφοριακό Σύστημα και αφορούν στην προσπέλαση υπηρεσιών ή την εκτέλεση διαδικασιών που είναι εξουσιοδοτημένη να εκτελεί.

Η εξέλιξη των σύγχρονων Πληροφοριακών Συστημάτων από περιβάλλοντα ενός χρήστη σε περιβάλλοντα μεγάλων κοινοτήτων χρηστών οδήγησε στην ανάγκη προστασίας τους από τις εκτελέσιμες διαδικασίες και το αντίστροφο. Χαρακτηριστικά, από τους πρώτους μηχανισμούς προστασίας οι οποίοι αποτελούνταν από υλικό και εφαρμογές λειτουργικών συστημάτων, τα συστήματα ελέγχου προσπέλασης εξελίχθηκαν σε μοντέλα πολιτικών εξουσιοδότησης. Δεδομένου μάλιστα ότι ο έλεγχος προσπέλασης στους πόρους ενός Πληροφοριακού Συστήματος αποτελεί το πρώτο και, ίσως, πιο καθοριστικό ανάχωμα προστασίας από την αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένες οντότητες, τα σύγχρονα συστήματα στο περιβάλλον του Διαδικτύου βασίζονται σε μοντέλα εμπιστοσύνης για την αναγνώριση των χρηστών και/ή των Παρόχων που ενεργούν εκ μέρους τους.

Στις μέρες μας, υπάρχουν πολυάριθμα σενάρια εφαρμογών συστημάτων ελέγχου προσπέλασης τα οποία ποικίλλουν ανάλογα με τις ανάγκες, τις απαιτήσεις και τις πολιτικές της εκάστοτε μελέτης εφαρμογής [70]. Στην πλειοψηφία των περιπτώσεων οι χρήστες του ίδιου οργανισμού αποκτούν προνόμια προσπέλασης κοινών και διαμοιράσιμων υπολογιστικών πόρων με βάση το ρόλο που έχει ο καθένας μέσα στον οργανισμό.

Με βάση αυτά, ο έλεγχος προσπέλασης εξελίχθηκε από την παραδοσιακή προσανατολισμένη στον Πάροχο μορφή του σε πόρους και οντότητες οι οποίες αλληλεπιδρούν σε ένα μεγάλο εύρος δικτύων και υποδομών, με πιο χαρακτηριστικό παράδειγμα το περιβάλλον του Διαδικτύου. Έτσι, τα προνόμια προσπέλασης χαμηλού επιπέδου των βασικών λειτουργιών ανάγνωσης και εγγραφής στα σύγχρονα Πληροφοριακά Συστήματα μεταφέρονται σε υψηλότερα επίπεδα ώστε να περιλαμβάνουν χαρακτηριστικά της ταυτότητας των οντοτήτων που τα αιτούνται. Τα στοιχεία αυτά μάλιστα στην πλειοψηφία των περιπτώσεων αναπαριστούν χαρακτηριστικά του φυσικού κόσμου, όπως η ιδιοκτησία ενός τραπεζικού λογαριασμού, ο αριθμός της πιστωτικής κάρτας ή ένας σαφώς καθορισμένος ρόλος.

Οι διαδικασίες που απαιτούνται για τη διατήρηση του προφίλ των χρηστών αποτελούν αυτό που αποκαλείται *Διαχείριση Ταυτοτήτων*, ένα πεδίο το οποίο εξελίχθηκε εν μέρει σε ξεχωριστή κατεύθυνση παρόλα αυτά αποτελεί το πρωταρχικό και αναπόσπαστο «στάδιο προετοιμασίας» για την εφαρμογή του ελέγχου προσπέλασης. Όπως παρουσιάζεται στην επόμενη ενότητα η Διαχείριση Ταυτοτήτων σχετίζεται άμεσα με έμπιστες διαδικασίες οι οποίες αναλαμβάνουν

την ανταλλαγή χαρακτηριστικών ταυτότητας και διαπιστευτηρίων ασφάλειας μεταξύ ετερογενών συστημάτων και οντοτήτων.

2.3.1 Έρευνα πεδίου σε μοντέλα ελέγχου προσπέλασης

Πρωταρχικός στόχος κάθε συστήματος ελέγχου προσπέλασης αποτελεί η ασφαλής και αξιόπιστη αξιολόγηση για το κατά πόσο μια ταυτοποιημένη στο σύστημα οντότητα έχει δικαίωμα πρόσβασης σε κάποιο συγκεκριμένο υπολογιστικό πόρο. Όπως αναφέρθηκε, ως υπολογιστικός πόρος μπορεί να θεωρηθεί κάθε είδους υπηρεσία, αρχείο ή διαδικτυακός υπερσύνδεσμος, ακόμα και διευθύνσεις ευρετηρίων.

Το βασικότερο ίσως εργαλείο για την επίτευξη αυτού του στόχου αποτελούν οι *πολιτικές ελέγχου προσπέλασης ή πολιτικές εξουσιοδότησης*. Ως πολιτική εξουσιοδότησης ορίζεται ένα σύνολο κανόνων το οποίο υιοθετεί ο εκάστοτε οργανισμός προκειμένου να ελέγξει και να διαχειριστεί το *ποιος έχει πρόσβαση και σε ποιους πόρους του Πληροφοριακού Συστήματος*. Σε μια πιο ευρύτερη ερμηνεία, μια πολιτική εξουσιοδότησης είναι μια δήλωση σχετικά με το τι επιτρέπεται και τι δεν επιτρέπεται να συμβεί στα πλαίσια χρήσης του Πληροφοριακού Συστήματος και περιγράφει τις αποδεκτές καταστάσεις προστασίας των πόρων.

Ο ορισμός των πολιτικών ελέγχου προσπέλασης απαιτεί την ενδελεχή ανάλυση της ροής των πληροφοριών στα πλαίσια λειτουργίας του Πληροφοριακού Συστήματος και την κατάλληλη επιλογή του μοντέλου με βάση το οποίο θα αποτιμώνται ώστε τελικά η διαδικασία απόδοσης προνομίων προσπέλασης που θα εφαρμόζεται να προσαρμόζεται πλήρως στις ανάγκες και να ικανοποιεί σε αξιόπιστο βαθμό τις απαιτήσεις της εκάστοτε μελέτης εφαρμογής.

Οι παραδοσιακές πολιτικές εξουσιοδότησης και, κατ' επέκταση, τα μοντέλα ελέγχου προσπέλασης που τις υιοθετούν χωρίζονται σε τρεις βασικές κατηγορίες [8]:

- Ιδιοκτησιακός Έλεγχος Προσπέλασης (Discretionary Access Control).
- Υποχρεωτικός Έλεγχος Προσπέλασης (Mandatory Access Control).
- Έλεγχος Προσπέλασης με βάση τους Ρόλους (Role-based Access Control).

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι τα μοντέλα ελέγχου προσπέλασης χρησιμοποιούνται για να περιγράψουν τις πολιτικές εξουσιοδότησης και βασίζονται στις αρχές της συστημικής ανάλυσης και της θεωρίας συνόλων προκειμένου να είναι ακριβή και τυπικά. Επίσης, η βασική τους συνεισφορά συνίσταται στο ότι είναι ικανά να αποδεικνύουν τη συμπεριφορά της πολιτικής εξουσιοδότησης που μοντελοποιείται. Με βάση αυτές τις παραδοχές η ανάλυση των πολιτικών εξουσιοδότησης είναι εφικτή μέσω της ανάλυσης του αντίστοιχου μοντέλου με το οποίο σχετίζονται [8].

Στις ενότητες που ακολουθούν περιγράφεται καθένα από τα 3 βασικά μοντέλα ελέγχου προσπέλασης και παρουσιάζονται τα βασικά τους χαρακτηριστικά.

2.3.1.1 Μοντέλο Ιδιοκτησιακού Ελέγχου Προσπέλασης

Με βάση το μοντέλο *Ιδιοκτησιακού Ελέγχου Προσπέλασης (ΙΕΠ)* οι πολιτικές εξουσιοδότησης είναι προσανατολισμένες στις ανάγκες των Παρόχων δεδομένου ότι κάθε πόρος του Πληροφοριακού Συστήματος θεωρείται ως ιδιοκτησία τους. Ο ιδιοκτήτης κάθε πόρου έχει μια απόλυτα διακριτή αντίληψη σχετικά με το ποια άλλη οντότητα θα μπορεί να προσπελάσει το συγκεκριμένο πόρο καθώς και με ποιον τρόπο θα επιτευχθεί τελικά η πρόσβαση [8].

Οι πολιτικές εξουσιοδότησης που βασίζονται σε αυτό το μοντέλο ελέγχου προσπέλασης έχουν υιοθετηθεί σε ένα τόσο μεγάλο εύρος που θα μπορούσε να θεωρηθεί ότι υπό μια πιο ευρύτερη διάσταση η πλειοψηφία των σύγχρονων πολιτικών εξουσιοδότησης σχετίζονται με τον έναν ή με τον άλλο τρόπο με αυτή την προσέγγιση. Ο βασικός λόγος για την τόσο μεγάλη απήχηση και ευρεία εφαρμογή αυτού του μοντέλου αποτελεί το γεγονός ότι η κεντρική ιδέα του «ιδιοκτήτης-πόρος» μοντελοποιείται και αντιστοιχίζεται πολύ εύκολα με την πραγματικότητα στο φυσικό κόσμο.

Ένα χαρακτηριστικό παράδειγμα εφαρμογής αυτού του μοντέλου είναι οι *Λίστες Προσπέλασης*, οι οποίες αποτελούν μια προσπάθεια δημιουργίας περισσότερο ευέλικτων συστημάτων τα οποία παρέχουν σε συγκεκριμένες οντότητες προνόμια προσπέλασης συγκεκριμένων πόρων [8]. Οι λίστες προσπέλασης είναι λίστες συγκεκριμένων οντοτήτων ή ομάδων οντοτήτων, οι οποίες έχουν πρόσβαση σε κάποιο συγκεκριμένο πόρο.

Τα βασικά πλεονεκτήματα του ΙΕΠ καθορίζονται από την απλότητα, την ευελιξία και την ευκολία χρήσης, κυρίως σε κλειστά και κεντρικοποιημένα περιβάλλοντα. Από την άλλη πλευρά όμως, η εφαρμογή τους σε δικτυακά και πολύ περισσότερο στα σύγχρονα διαδικτυακά περιβάλλοντα είναι πολλές φορές ανέφικτη. Ο λόγος είναι ότι εκτός του ότι το μοντέλο ΙΕΠ δεν παρέχει καμία τυπική διασφάλιση της ροής των πληροφοριών, η ανάθεση προνομίων εξουσιοδότησης με βάση τα όσα ορίζουν οι διακριτές πολιτικές είναι μη διαχειρίσιμη και δύσκολα προβλέψιμη για κάθε είδους σύγχρονο Πληροφοριακό Σύστημα και ιδιαίτερα για συνεργατικά περιβάλλοντα με μεγάλο πλήθος χρηστών.

2.3.1.2 Μοντέλο Υποχρεωτικού Ελέγχου Προσπέλασης

Σε αντίθεση με τον μοντέλο ΙΕΠ, το μοντέλο *Υποχρεωτικού Ελέγχου Προσπέλασης (ΥΕΠ)* δε βασίζεται στην κεντρική ιδέα «ιδιοκτήτης-πόρος». Η πρόσβαση στους πόρους του Πληροφοριακού Συστήματος καθορίζεται μέσω διαχειριστικών διαδικασιών οι οποίες παραμένουν αμετάβλητες καθ' όλη τη διάρκεια του κύκλου ζωής του. Επίσης, οι οντότητες που συμμετέχουν δεν έχουν

πλέον την ευθύνη ή την αρμοδιότητα να μεταβιβάζουν προνόμια προσπέλασης των πόρων σε άλλες οντότητες [8].

Αντί αυτού οι δυνατότητες προσπέλασης καθορίζονται από μια Έμπιστη Τρίτη Οντότητα, η οποία θέτει τους κανόνες σχετικά με το ποιος έχει πρόσβαση και σε ποιους πόρους του Πληροφοριακού Συστήματος με βάση την ευαισθησία και την κρισιμότητα των πληροφοριών που διαχειρίζεται ο καθένας τους.

Πιο συγκεκριμένα, στα πλαίσια αυτού του μοντέλου ελέγχου προσπέλασης δεν υφίσταται η έννοια της ιδιοκτησίας, καθώς κεντρικό ρόλο έχει ο βαθμός κρισιμότητας των πόρων. Για να αποκτήσει πρόσβαση μια οντότητα σε κάποιον από τους κρίσιμους πόρους θα πρέπει να έχει τα απαραίτητα διαπιστευτήρια αξιοπιστίας και εμπιστοσύνης ώστε να δικαιούται τα προνόμια αυτά. Στη συνέχεια ακολουθεί η σύγκριση του *βαθμού αξιοπιστίας* κάθε οντότητας με τα *κατώφλια* των τιμών που χαρακτηρίζουν και αντιπροσωπεύουν τη διαβάθμιση των πόρων ώστε τελικά η απόφαση εξουσιοδότησης και ο έλεγχος προσπέλασης να βασίζονται σε μαθηματικούς υπολογισμούς με βάση τους τύπους και τα μοντέλα που ορίζονται σε κάθε περιβάλλον εφαρμογής.

Το μοντέλο ΥΕΠ έλαβε μεγάλη αποδοχή σε κρίσιμα Πληροφοριακά Συστήματα στρατιωτικού σκοπού ενώ όσον αφορά στις σύγχρονες διαδικτυακές εφαρμογές χρησιμοποιείται μόνο σε ειδικές περιπτώσεις και πάντα προσαρμοσμένο στις ειδικές απαιτήσεις και συνθήκες του εκάστοτε περιβάλλοντος εφαρμογής.

2.3.1.3 Μοντέλο Ελέγχου Προσπέλασης με βάση τους Ρόλους

Το μοντέλο *Ελέγχου Προσπέλασης με βάση τους Ρόλους (ΕΠΡ)* ή *Προσανατολισμένο στους Ρόλους* μοντέλο εξελίχθηκε ως η πιο σύγχρονη εναλλακτική προσέγγιση των δυο προηγούμενων μοντέλων, δηλαδή του ΙΕΠ και του ΥΕΠ. Σύμφωνα με το μοντέλο ΕΠΡ, η απόδοση προνομίων προσπέλασης των πόρων του Πληροφοριακού Συστήματος και των επιχειρησιακών διαδικασιών γίνεται με βάση το ρόλο της οντότητας που αιτείται κάθε φορά προνόμια εξουσιοδότησης [8]. Όμοια με το φυσικό κόσμο, ως ρόλος ορίζεται η αφηρημένη έννοια που περιλαμβάνει ένα σύνολο κανόνων και αρμοδιοτήτων παρέχοντας παράλληλα ένα αντίστοιχο σύνολο επιτρεπόμενων ενεργειών.

Σε αντίθεση με τα δύο άλλα μοντέλα ελέγχου προσπέλασης τα προνόμια εξουσιοδότησης με βάση το μοντέλο ΕΠΡ αφορούν αποκλειστικά τους ρόλους των χρηστών. Πιο συγκεκριμένα, με βάση τον τρόπο λειτουργίας των σύγχρονων Πληροφοριακών Συστημάτων, όταν εφαρμόζεται ΕΠΡ σε δικτυακά ή διαδικτυακά περιβάλλοντα οι χρήστες εκείνοι οι οποίοι διαμοιράζονται τα ίδια ή παρόμοια προνόμια προσπέλασης των ίδιων πόρων γίνονται μέλη μιας ομάδας ή κοινότητας. Κατόπιν, η ομάδα αυτή σαν μια ενιαία οντότητα αποκτά ή στερείται προνόμια εξουσιοδότησης των πόρων του Πληροφοριακού Συστήματος ενώ, παράλληλα, οι αποφάσεις απόδοσης προνομίων προσπέλασης λαμβάνουν υπόψιν όλες τις ομάδες στις οποίες ανήκει ο κάθε χρήστης.

Από την άλλη πλευρά, ενώ η ομαδοποίηση των χρηστών είναι αδιαμφισβήτητα ένα σημαντικός παράγοντας για τη διαχείριση της επεκτασιμότητας των συστημάτων, παρόλα αυτά δεν αποτελεί τον μοναδικό. Εκτός από τις ομάδες χρηστών, μια εξίσου σημαντική διάσταση αποτελεί η ομαδοποίηση των δικαιωμάτων προσπέλασης.

Ακολουθώντας την κεντρική ιδέα ότι οι χρήστες που μοιράζονται τις ίδιες δυνατότητες πρόσβασης στους πόρους θα αντιμετωπίζονται και θα διαχειρίζονται ως μια ενιαία οντότητα, το μοντέλο ΕΠΡ εξελίχθηκε γρήγορα και βρήκε μεγάλη εφαρμογή σε δικτυακά και διαδικτυακά περιβάλλοντα όπου συνηθίζεται η απόδοση προνομίων προσπέλασης στους πόρους και τις υπηρεσίες να εξαρτάται από την ομάδα στην οποία ανήκει ο κάθε χρήστης, όπως αυτή ορίζεται στο πλαίσιο της εκάστοτε μελέτης εφαρμογής [1, 9].

Από την άλλη πλευρά, ενώ η εφαρμογή του ΕΠΡ στα πλαίσια των παραδοσιακών Πληροφοριακών Συστημάτων θεωρείται μια κοινή και γενικά αποδεκτή πρακτική προσέγγιση, το γεγονός ότι ένα μεγάλο πλήθος χρηστών χαρακτηρίζονται από κοινά δικαιώματα προσπέλασης χωρίς να λαμβάνεται υπόψη η κρισιμότητα των προσπελάσιμων πόρων και η αξιοπιστία του καθενός, καθιστούν το ΕΠΡ εν μέρει ελλιπές όσον αφορά στην εφαρμογή του σε περιβάλλοντα που ενσωματώνουν εφαρμογές Web 2.0 [26].

2.3.2 Ανοιχτά θέματα

Παρά το γεγονός ότι οι απαιτήσεις προσβασιμότητας έχουν εξελιχθεί σημαντικά στα σύγχρονα συνεργατικά περιβάλλοντα, κυρίως λόγω των επιπτώσεων από την ολοκλήρωση τεχνολογιών Web 2.0 και την παροχή διαδραστικών δυνατοτήτων (βλ. Κεφάλαιο 5), ο σχεδιασμός και η ανάπτυξη κατάλληλων μοντέλων ελέγχου προσπέλασης δεν έχει εξελιχθεί στον ίδιο βαθμό ώστε να τις καλύπτει με επιτυχία. Η πλειοψηφία των παραδοσιακών προσεγγίσεων είναι ανεπαρκής όταν υιοθετούνται σε συνεργατικά περιβάλλοντα, καθώς τα περιβάλλοντα αυτά δεν σχεδιάστηκαν με τρόπο που να ικανοποιούν τις επιπρόσθετες απαιτήσεις που επιφέρουν οι διαδραστικές λειτουργίες των συνεργατικών εφαρμογών, όπως για παράδειγμα η δημιουργία περιεχομένου, η δημιουργία σχολίων και η κοινοποίηση περιεχομένου.

Όπως περιγράφεται στο πέμπτο κεφάλαιο της διατριβής στα συνεργατικά περιβάλλοντα δημιουργούνται νέες απαιτήσεις οι οποίες προκύπτουν από τις διαδραστικές δυνατότητες των χρηστών και την ενδεχόμενη αποκάλυψη προσωπικών και ευαίσθητων πληροφοριών για άλλους χρήστες που συμμετέχουν στο συνεργατικό περιβάλλον. Οι διαδικασίες απόδοσης προνομίων προσπέλασης θα πρέπει να λαμβάνουν υπόψη και να καλύπτουν αυτές τις επιπλέον απαιτήσεις.

Ως εκ τούτου, οι ρόλοι των χρηστών πολλές φορές δεν επαρκούν και, σίγουρα, δεν αποτελούν αξιόπιστα κριτήρια για τον έλεγχο προσπέλασης σε κρίσιμους

πόρους, όπως οι διαδραστικές λειτουργίες που παρέχει ένα συνεργατικό περιβάλλον, καθώς αφορούν σε στατικά χαρακτηριστικά της ταυτότητας των χρηστών, τα οποία δε σχετίζονται με τον τρόπο συμπεριφοράς τους, και κατ'επέκταση, με την αξιοπιστία τους, όσον αφορά στη χρήση των παρεχομένων υπηρεσιών. Επίσης δεν αποτελούν κριτήρια αξιολόγησης σχετικά με το κατά πόσο οι δημοσιεύσεις τους σέβονται την ιδιωτικότητα των υπολοίπων συμμετεχόντων ώστε να δικαιούνται να διατηρούν αυτά τα προνόμια.

Όπως περιγράφεται στο έκτο κεφάλαιο, η συνεισφορά της διατριβής σε αυτόν τον ερευνητικό τομέα προτείνει ότι προκειμένου η απόδοση προνομίων προσπέλασης να προσαρμόζεται αποτελεσματικά στις απαιτήσεις προσβασιμότητας σε συνεργατικά περιβάλλοντα, η αξιοπιστία των χρηστών θα πρέπει να λαμβάνεται υπόψη στις αποφάσεις ελέγχου προσπέλασης, ως κρίσιμο χαρακτηριστικό της ταυτότητας, ικανό να κρίνει τη συμπεριφορά των χρηστών στη χρήση των διαδραστικών υπηρεσιών συνεργασίας και κοινωνικής αλληλεπίδρασης.

2.4 Ιδιωτικότητα

Με βάση τις παραδοσιακές αρχιτεκτονικές Πληροφοριακών Συστημάτων, η παροχή ηλεκτρονικών υπηρεσιών συνήθως περιλαμβάνει την αλληλεπίδραση μεταξύ δύο οντοτήτων, του χρήστη και του *Παρόχου Υπηρεσιών (Service Provider) - ΠΥ*. Είτε ο ΠΥ είτε, όπως γίνεται συνήθως στα σύγχρονα πλαίσια υπηρεσιών, κάποια *έμπιστη τρίτη οντότητα (trusted third party)* αναλαμβάνει το ρόλο του *Παρόχου Ταυτοτήτων (Identity Provider) - ΠΤ* και παρέχει υπηρεσίες αυθεντικοποίησης των χρηστών ή άλλων οντοτήτων (π.χ. Πάροχοι Υπηρεσιών) και διαχείρισης των διαπιστευτηρίων ασφάλειας [16].

Σε αυτό το πλαίσιο, όπου ο καταναλωτής της υπηρεσίας συχνά έχει ανεπαρκή γνώση σχετικά με την οντότητα η οποία διαχειρίζεται και αποθηκεύει τις προσωπικές του πληροφορίες, η εμπιστοσύνη καθορίζεται από τα *συμφωνητικά συνεργασίας* μεταξύ των Παρόχων και τις πολιτικές ιδιωτικότητας που εφαρμόζονται [47]. Ειδικότερα, οι χρήστες αποδέχονται ότι οι ΠΤ και ΠΥ θα τηρήσουν την ισχύουσα νομοθεσία και θα σεβαστούν την ιδιωτικότητά τους προστατεύοντας τα προσωπικά δεδομένα που παραχωρούν προκειμένου να δημιουργήσουν τις ψηφιακές τους ταυτότητες και να προσπελάσουν τις παρεχόμενες υπηρεσίες [46].

Αντίθετα, στα συνεργατικά περιβάλλοντα όπου κάθε χρήστης έχει τη δυνατότητα δημιουργίας και δημοσίευσης περιεχομένου, ακόμα και αν οι Πάροχοι ακολουθούν πιστά τις πολιτικές ιδιωτικότητας και συμμορφώνονται με την αντίστοιχη νομοθεσία εφαρμόζοντας αποτελεσματικά κατάλληλους μηχανισμούς ασφάλειας, η ιδιωτικότητα των χρηστών [24, 25] εξακολουθεί να βρίσκεται σε κίνδυνο καθώς εξαρτάται αποκλειστικά από την αξιοπιστία των χρηστών.

2.4.1 Έρευνα πεδίου σε αρχιτεκτονικές διαχείρισης ταυτοτήτων

Ποικίλες αρχιτεκτονικές διαχείρισης ταυτοτήτων έχουν προταθεί κατά καιρούς με σκοπό την ασφαλή διαχείριση των ψηφιακών ταυτοτήτων και την προστασία των προσωπικών δεδομένων των χρηστών, είτε στα πλαίσια κλειστών κεντροποιημένων αρχιτεκτονικών είτε σε πιο ανοιχτές προσεγγίσεις ομοσπονδιακής διαχείρισης. Ειδικότερα, οι βασικοί τύποι αρχιτεκτονικών διαχείρισης ταυτοτήτων αναλύονται στις υποενότητες που ακολουθούν.

2.4.1.1 Αρχιτεκτονική κατανεμημένης διαχείρισης ταυτοτήτων

Στα Πληροφοριακά Συστήματα που υιοθετούν κατανεμημένες αρχιτεκτονικές Διαχείρισης Ταυτοτήτων (silo model) ο ΠΥ λειτουργεί επίσης ως ΠΤ εκδίδοντας διαπιστευτήρια ασφάλειας για τους χρήστες του και ελέγχοντας την προσπέλαση σε όλες τις υπηρεσίες που βρίσκονται υπό την δικαιοδοσία του [8, 16]. Αυτό έχει σαν αποτέλεσμα οι χρήστες να πρέπει να διατηρούν διαφορετικούς λογαριασμούς για κάθε μια από τις υπηρεσίες που επιθυμούν να προσπελάσουν σε διαφορετικούς ΠΥ καταλήγοντας τελικά με πολλαπλά διαπιστευτήρια αυθεντικοποίησης και κωδικούς πρόσβασης τα οποία πρέπει να θυμούνται, να διαχειρίζονται και να ανανεώνουν.

Επιπλέον, απαιτείται οι χρήστες να εμπιστεύονται πολλαπλούς ΠΤ για την προστασία των προσωπικών τους δεδομένων, μια πρακτική η οποία δεν είναι πάντα ασφαλής και αξιόπιστη, λαμβάνοντας υπόψιν το γεγονός ότι οι χρήστες είναι υποχρεωμένοι να δημιουργούν πολλαπλά ίχνη της ταυτότητάς τους σε ένα μεγάλο εύρος ετερογενών συστημάτων.

Συμπερασματικά, η προσέγγιση αυτή είναι περισσότερο κατάλληλη για εφαρμογή σε Κοινωνικά Δίκτυα όπου οι ΠΥ προτιμούν να υιοθετούν κλειστές ιδιοκτησιακές λύσεις διαχείρισης ταυτοτήτων.

2.4.1.2 Αρχιτεκτονική κεντροποιημένης διαχείρισης ταυτοτήτων

Στα πλαίσια των αρχιτεκτονικών *κεντροποιημένης διαχείρισης ταυτοτήτων (centralized identity management)* μια κεντρική οντότητα αναλαμβάνει την αυθεντικοποίηση και εξουσιοδότηση όλων των χρηστών που συμμετέχουν στο πλαίσιο υπηρεσιών που παρέχει το ολοκληρωμένο Πληροφοριακό Σύστημα [8, 16]. Ο κεντρικός ΠΤ προσφέρει τις υπηρεσίες του σε πολλούς ΠΥ προκειμένου να παρέχονται με αποτελεσματικό και διαφανή τρόπο υπηρεσίες *Καθολικής Σύνδεσης (Single Sign-On, SSO)* σε διασυνδεδεμένα και διαλειτουργικά περιβάλλοντα [34].

Για να διασφαλιστούν τα απαραίτητα επίπεδα εμπιστοσύνης τόσο μεταξύ των Παρόχων όσο και μεταξύ των χρηστών, οι διαδικασίες αυθεντικοποίησης και εξουσιοδότησης είναι αρμοδιότητες αποκλειστικά του κεντρικού ΠΤ, ο οποίος είναι υπεύθυνος για τη διαχείριση των διαπιστευτηρίων ασφάλειας και την εφαρμογή των πολιτικών προσπέλασης.

Είναι αξιοσημείωτο, επίσης, το γεγονός ότι για να ικανοποιηθούν αποτελεσματικά όλες οι απαιτήσεις ασφάλειας και προστασίας της ιδιωτικότητας ο ΠΤ αποτελεί το κεντρικό σημείο πρόσβασης στο Πληροφοριακό Σύστημα και αναλαμβάνει την πλοήγηση του χρήστη με βάση τα προνόμια εξουσιοδότησης που του αποδίδονται.

Στο πλαίσιο της παρούσας διατριβής, η προσέγγιση αυτή θεωρείται περισσότερο κατάλληλη για ΣΠΣ όπου ετερογενείς υπηρεσίες ολοκληρώνονται και παρέχονται κάτω από ένα ενιαίο πλαίσιο και επιχειρησιακό μοντέλο υπηρεσιών.

2.4.1.3 Αρχιτεκτονική ομοσπονδιακής διαχείρισης ταυτοτήτων

Με βάση την αρχιτεκτονική της ομοσπονδιακής διαχείρισης ταυτοτήτων (*federated identity management*), οι ΠΤ αναπτύσσουν σχέσεις εμπιστοσύνης μεταξύ τους όσον αφορά στην ανταλλαγή διαπιστευτηρίων αυθεντικοποίησης και εξουσιοδότησης εκ μέρους των χρηστών και συμφωνούν σε αντίστοιχους κανόνες και πολιτικές οι οποίες διασφαλίζουν την τήρηση των απαιτούμενων υποχρεώσεων [8, 16]. Έτσι παρέχονται υπηρεσίες *Καθολικής Σύνδεσης* για ένα μεγάλο πλαίσιο ετερογενών ΠΥ και Πληροφοριακών Συστημάτων χωρίς απαραίτητα να ολοκληρώνονται κάτω από ένα κοινό επιχειρησιακό πλάνο, όπως στην αρχιτεκτονική της κεντρικοποιημένης διαχείρισης.

Μια κριτική για αυτή την προσέγγιση αποτελεί το γεγονός ότι τα πρωτόκολλα επικοινωνίας είναι έτσι σχεδιασμένα ώστε να ικανοποιούν αποκλειστικά τις απαιτήσεις των Παρόχων και όχι αυτές των χρηστών. Σε περιβάλλοντα ομοσπονδίας δεν είναι εύκολη και, τις περισσότερες φορές, δεν είναι εφικτή η χρήση *Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies)* για την ικανοποίηση αντίστοιχων απαιτήσεων [19]. Έτσι, η προστασία της ιδιωτικότητας πρέπει να διασφαλίζεται από τα πρότυπα και τις προδιαγραφές ασφάλειας που θα πρέπει απαραίτητα να υιοθετούνται. Από την άλλη πλευρά, η εμπιστοσύνη παραμένει ένα κριτήριο αξιολόγησης του κατά πόσο οι χρήστες είναι σίγουροι για την αποτελεσματική υλοποίηση των μηχανισμών προστασίας και την αξιοπιστία των ΠΤ για την επεξεργασία και τη διαχείριση των προσωπικών τους δεδομένων [32].

Οι υφιστάμενες τεχνολογικές λύσεις για την υλοποίηση αρχιτεκτονικών ομοσπονδιακής διαχείρισης ταυτοτήτων ορίζουν ένα σύνολο πρωτοκόλλων για την ασφαλή ανταλλαγή πληροφοριών σχετικών με την ταυτότητα των οντοτήτων που συμμετέχουν στην ομοσπονδία. Επίσης υιοθετούν μια βασισμένη σε πρότυπα προσέγγιση η οποία στα σύγχρονα πλαίσια υπηρεσιών βασίζεται στην τεχνολογία *Security Assertion Markup Language (SAML)*. Πρότυπα και προδιαγραφές, όπως, Liberty ID-FF [28], Liberty ID-WSF [29], Liberty IGF Privacy Constraints [31], WS-Policy [27], WS-Trust [30]), παρέχουν

χρήσιμες οδηγίες σχετικά με τον τρόπο που θα πρέπει να υλοποιούνται οι μηχανισμοί επικοινωνίας και ανταλλαγής δεδομένων σε αυτά τα περιβάλλοντα.

Λόγω των αυξημένων δυνατοτήτων επεκτασιμότητας και διαλειτουργικότητας που τη χαρακτηρίζουν, η προσέγγιση αυτή αποτελεί εξίσου αποτελεσματική λύση για συνεργατικά περιβάλλοντα κα δεδομένου ότι υπάρχουν αυξημένες απαιτήσεις αλληλεπίδρασης και διασύνδεσης με ετερογενή πληροφοριακά συστήματα και Παρόχους.

2.4.1.4 Αρχιτεκτονική διαχείρισης ταυτοτήτων προσανατολισμένη στο χρήστη

Η *προσανατολισμένη στο χρήστη αρχιτεκτονική διαχείρισης ταυτοτήτων (user-centric identity management)* και τα σύγχρονα εργαλεία προστασίας της ιδιωτικότητας, όπως είναι χαρακτηριστικά οι *Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (TEI)* [15], παρά το γεγονός ότι αποτελούν αξιόπιστες λύσεις για την προστασία της ιδιωτικότητας των χρηστών δεν κατάφεραν να ανταπεξέλθουν στις προσδοκίες τους και να αποτελέσουν ευρέως διαδεδομένες πρακτικές [16].

Σχετικά με τις TEI θα πρέπει να αναφερθεί ότι, παρά το γεγονός ότι οι τεχνολογίες αυτές επικεντρώνονται στην προστασία της ιδιωτικότητας και της εμπιστοσύνης κυρίως μεταξύ χρηστών και Παρόχων, τα προβλήματα ευχρηστίας που τις χαρακτηρίζουν αποτέλεσαν σημαντικά εμπόδια για την ευρεία αποδοχή και χρήση τους. Ειδικότερα, πέρα από τις τεχνολογικές γνώσεις και την εξοικείωση με εφαρμογές λογισμικού που απαιτούσε η χρήση των TEI (π.χ. Anonymizer [63], PrivacyBird [67], Onion Routing [64], Tor [65, 66], PGP [66]), η συντριπτική πλειοψηφία αυτών των εργαλείων δεν καλύπτουν τις απαιτήσεις προστασίας της ιδιωτικότητας σε επίπεδο χρηστών [15] και, συνεπώς, δεν είναι προσαρμόσιμα στις ανάγκες των ΣΠΣ.

2.4.2 Έρευνα πεδίου σε πρότυπα και προδιαγραφές διαχείρισης ταυτοτήτων

Η ραγδαία εξάπλωση του διαδικτύου και η χρήση όλο και μεγαλύτερου πλήθους εφαρμογών και ηλεκτρονικών υπηρεσιών οδήγησε στην απεριόριστη και μερικές φορές υπερβολική δημιουργία ψηφιακών ταυτοτήτων. Το γεγονός αυτό είχε σαν αποτέλεσμα να προκύψουν σοβαρά προβλήματα όσον αφορά στη διαχείριση των πολλαπλών και διαφορετικών ταυτοτήτων και συνθηματικών από πλευράς των χρηστών αλλά και αυξημένα κόστη διαχείρισης από πλευράς των Παρόχων Υπηρεσιών.

Προσθέτοντας σε αυτά τις αυξανόμενες απαιτήσεις διαλειτουργικότητας μεταξύ ετερογενών συστημάτων, γίνεται εμφανής ο λόγος για τον οποίο η αρχιτεκτονική της κατανεμημένης διαχείρισης ταυτοτήτων κατέστη γρήγορα ανεπαρκής. Παράλληλα, άμεση ήταν η αντίδραση ερευνητικών οργανισμών και

φορέων προτυποποίησης οι οποίοι έστρεψαν τις προσπάθειές τους στη δημιουργία και εφαρμογή του μοντέλου της *Ομοσπονδιακής Διαχείρισης Ταυτοτήτων*.

Όπως αναφέρθηκε στην προηγούμενη ενότητα, με βάση το μοντέλο αρχιτεκτονικής γίνεται πλέον διαχωρισμός μεταξύ των Παρόχων Υπηρεσιών και των Παρόχων Ταυτοτήτων, ενώ παράλληλα προσφέρεται η δυνατότητα σε ετερογενή συστήματα να συνεργάζονται και να οργανώνονται σε κύκλους εμπιστοσύνης – ομοσπονδίες, ώστε να επιτρέπουν την παροχή υπηρεσιών *Καθολικής Σύνδεσης* στους χρήστες τους. Η τεχνολογία στην οποία βασίζονται είναι η *Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας SAML* [69], ένα ανοιχτό πρότυπο βασισμένο στην XML. Σκοπός της SAML είναι να καθορίσει μια πρότυπη αναπαράσταση δεδομένων ασφάλειας, αναγνωρίσιμων από διαφορετικές εφαρμογές ηλεκτρονικών υπηρεσιών, ανεξάρτητα από τις τεχνολογίες ή τις πολιτικές που υιοθετούνται. Ειδικότερα, χρησιμοποιείται για την ανταλλαγή δεδομένων αυθεντικοποίησης και εξουσιοδότησης μεταξύ περιοχών ασφάλειας.

Ο Πάροχος Ταυτοτήτων παράγει “ισχυρισμούς” SAML (SAML assertions) με βάση τα δεδομένα αυθεντικοποίησης που λαμβάνει και ο Πάροχος Υπηρεσιών τους επεξεργάζεται προκειμένου να λάβει αποφάσεις εξουσιοδότησης. Το πιο σημαντικό πρόβλημα που προσπαθεί να επιλύσει η SAML είναι αυτό της *Καθολικής Σύνδεσης* σε φυλλομετρητές Ιστού, ενώ θα μπορούσε να χαρακτηριστεί ως το απόλυτο πρότυπο στον τομέα της διαχείρισης διαπιστευτηρίων αυθεντικοποίησης και εξουσιοδότησης.

Από την άλλη πλευρά και δεδομένου ότι τα τελευταία χρόνια όλο και περισσότερα συστήματα και εφαρμογές βασίζονται στην τεχνολογία των Υπηρεσιών Ιστού, υπάρχουν κάποιες επιπλέον προδιαγραφές οι οποίες ξεπερνούν την ανάγκη δημιουργίας ομοσπονδιών προκειμένου να γίνεται με διαλειτουργικό τρόπο η διαχείριση των διαπιστευτηρίων ασφάλειας.

Το πλαίσιο των προδιαγραφών για την ασφάλεια των Υπηρεσιών Ιστού έχει προτυποποιηθεί από τον οργανισμό *OASIS* και μεταξύ άλλων περιλαμβάνει ένα σύνολο από πρότυπες προδιαγραφές (π.χ. *WS-Security*, *WS-Trust*, *WS-Policy*, *WS-Federation*, *WS-SecurityPolicy*) που σαν σκοπό έχουν την ενίσχυση και την περαιτέρω ανάπτυξη της ασφάλειας και της διαλειτουργικότητας μεταξύ ετερογενών συστημάτων τα οποία βασίζονται στην τεχνολογία των Υπηρεσιών Ιστού. Επίσης, ένα σημαντικό χαρακτηριστικό των προδιαγραφών αυτών είναι το γεγονός ότι είναι συσχετιζόμενες, συμβάλλοντας με αυτόν τον τρόπο στην ανάπτυξη μιας σύνθετης αρχιτεκτονικής.

Όσον αφορά στον τομέα διαχείρισης των ψηφιακών ταυτοτήτων σε περιβάλλον Υπηρεσιών Ιστού, οι προδιαγραφές *WS-Trust* [30] προδιαγράφουν το μοντέλο λειτουργίας μιας *Υπηρεσίας Διαπιστευτηρίων Ασφάλειας (Security Token Service, STS)*. Το πρότυπο αυτό ορίζει τις προδιαγραφές μιας Υπηρεσίας Ιστού η οποία

χρησιμοποιεί την τεχνολογία SAML προκειμένου να παρέχει διαπιστευτήρια ασφάλειας σχετικά με χαρακτηριστικά της ψηφιακής ταυτότητας των χρηστών σε άλλες Υπηρεσίες Ιστού. Έτσι επιτυγχάνεται με διαλειτουργικό, ασφαλή και αξιόπιστο τρόπο η διαδικασία της εξουσιοδότησης, ξεπερνώντας παράλληλα τις απαιτήσεις δημιουργίας ομοσπονδιών.

2.4.3 Ανοιχτά θέματα

Είναι αξιοσημείωτο το γεγονός ότι σε αντίθεση με τα παραδοσιακά πλαίσια υπηρεσιών όπου οι χρήστες βασίζονται στην επικύρωση των πολιτικών ιδιωτικότητας προκειμένου να διασφαλίσουν την εμπιστευτικότητα των προσωπικών τους δεδομένων, στα σύγχρονα Πληροφοριακά Συστήματα συνεργασίας και αλληλεπίδρασης μεταξύ των χρηστών, η πρακτική αυτή δεν επαρκεί για να καλύψει όλες τις ανάγκες. Ακόμα και αν οι ισχύουσες πολιτικές τηρηθούν πιστά από τους Παρόχους, τα προσωπικά και ευαίσθητα δεδομένα των χρηστών συνεχίζουν να αντιμετωπίζουν σημαντικούς κινδύνους αν λάβει κανείς υπόψιν τις διαδραστικές δυνατότητες δημιουργίας περιεχομένου που παρέχουν οι εφαρμογές Web 2.0.

Όπως παρουσιάστηκε στην ενότητα 2.4.1, στην πλειοψηφία τους τα παραδοσιακά μοντέλα διαχείρισης ταυτοτήτων επικεντρώνονται στο να διαχειρίζονται εύκολα τα προσωπικά δεδομένα και τις ψηφιακές ταυτότητες που ανταλλάσσονται σε κάθε αλληλεπίδραση μεταξύ των Παρόχων [35]. Έτσι, παρά το γεγονός ότι υιοθετούν αξιόπιστες λύσεις σχετικά με τη διαχείριση ταυτοτήτων και τις διαδικασίες αυθεντικοποίησης και εξουσιοδότησης, δεν καλύπτουν αποτελεσματικά τις απαιτήσεις της προσανατολισμένης στο χρήστη προσέγγισης με βάση την όποια οι χρήστες θα πρέπει να έχουν ενεργή συμμετοχή στην προστασία των προσωπικών τους δεδομένων.

Όπως περιγράφεται στην ενότητα 2.2.3, όταν τα κλασικά μοντέλα διαχείρισης ταυτοτήτων [45] υιοθετούνται στα πλαίσια των ΣΠΣ, ο σχεδιασμός αξιόπιστων αρχιτεκτονικών επιβάλλει τον επαναπροσδιορισμό των εννοιών της εμπιστοσύνης και της ιδιωτικότητας με βάση τις νέες απαιτήσεις που προκύπτουν από τις δυνατότητες συνεργασίας και κοινωνικής αλληλεπίδρασης που παρέχουν. [36, 39]

Με βάση την έρευνα πεδίου στη διαχείριση ψηφιακών ταυτοτήτων και τις αντίστοιχες απαιτήσεις ιδιωτικότητας των Συνεργατικών Πληροφοριακών Συστημάτων, πέραν του μοντέλου κατανομημένης διαχείρισης το οποίο στερείται ερευνητικού ενδιαφέροντος, η διατριβή προτείνει ότι η υιοθέτηση καθενός από τα κλασικά μοντέλα διαχείρισης ταυτοτήτων ξεχωριστά δεν είναι ικανή από μόνη της να καλύψει όλες τις ανάγκες των ΣΠΣ. Όπως περιγράφεται στο τρίτο και τέταρτο κεφάλαιο, για την αποτελεσματική προστασία της ιδιωτικότητας απαιτείται μια καινοτόμος προσέγγιση ικανή να καλύψει τις νέες απαιτήσεις των εφαρμογών Web 2.0.

Στο πλαίσιο της διατριβής προτείνεται μια νέα αρχιτεκτονική διαχείρισης ταυτοτήτων η οποία ενσωματώνει τις βασικές αρχές και τα θετικά χαρακτηριστικά των τριών παραδοσιακών προσεγγίσεων της κεντρικοποιημένης, ομοσπονδιακής και προσανατολισμένης στο χρήστη διαχείρισης προκειμένου όχι μόνο να καλύπτει τις προδιαγραφές του επιχειρησιακού μοντέλου των ΣΠΣ αλλά και να προσφέρει στους χρήστες αξιόπιστες λύσεις προστασίας της ιδιωτικότητάς σε περιβάλλοντα συνεργασίας και κοινωνικής αλληλεπίδρασης.

2.5 Αξιοπιστία

Οι διαδικτυακές υπηρεσίες και πολύ περισσότερο οι εφαρμογές Web 2.0 απευθύνονται συχνά σε άγνωστες μεταξύ τους οντότητες. Έτσι γίνεται εύκολα κατανοητό ότι η εμπιστοσύνη αν και δύσκολο να επιτευχθεί παίζει πολύ σημαντικό ρόλο στις συναλλαγές και την ποιότητα των παρεχομένων υπηρεσιών. Για το λόγο αυτό, εντοπίζεται η ανάγκη παροχής κάποιου είδους πληροφόρησης σχετικά με τις οντότητες που αλληλεπιδρούν και συμμετέχουν στα εκάστοτε πλαίσια συνεργασίας ώστε να υπάρχει ένα κριτήριο αξιολόγησης της αξιοπιστίας τους και της ποιότητας των υπηρεσιών που παρέχουν [32].

Τα *Συστήματα Διαχείρισης Αξιοπιστίας (ΣΔΑ)* ή *Συστήματα Διαχείρισης Φήμης* τα οποία είναι γνωστά ως *Reputation Management Systems*, αποτελούν τη σύγχρονη τεχνολογική προσέγγιση προστασίας των χρηστών από την προσπέλαση κακόβουλων πηγών πληροφόρησης. Βασίζονται στην ενεργή συνεισφορά των οντοτήτων που συμμετέχουν σε ένα δίκτυο συνεργασίας [44] για την αξιολόγηση της ποιότητας ή της αξιοπιστίας των υπηρεσιών που παρέχονται.

Τα βασικά τους οφέλη διακρίνονται στα ακόλουθα:

- Βοηθούν στη βελτίωση των παρεχομένων υπηρεσιών αξιολογώντας τη συμπεριφορά των συμμετεχόντων με βάση την ανατροφοδότηση των υπολοίπων οντοτήτων/χρηστών.
- Βοηθούν στη λήψη αποφάσεων σχετικά με το αν και πόσο αξιόπιστη είναι μια οντότητα για αλληλεπίδραση ή/και ανταλλαγή πληροφοριών.
- Βοηθούν στην ανάπτυξη εμπιστοσύνης μεταξύ των οντοτήτων που συμμετέχουν σε ένα πλαίσιο υπηρεσιών αξιοποιώντας τη συλλογική εμπειρία και συνεισφορά τους.

Είναι αξιοσημείωτο επίσης το γεγονός ότι τα συστήματα αυτά και οι υπηρεσίες που παρέχουν είναι πιο εύκολα στην κατανόηση, εφαρμογή, χρήση και διαχείριση από άλλες τεχνολογικές λύσεις όπως οι *Υποδομές Δημόσιας Κλείδας (Public Key Infrastructure, PKI)* - ΥΔΚ και τα ψηφιακά πιστοποιητικά ενώ στα πλαίσια ενός συνεργατικού περιβάλλοντος αποτελούν τη μοναδική ίσως λύση επίτευξης εμπιστοσύνης μεταξύ των χρηστών καθώς οι κλασικές προσεγγίσεις

(π.χ. ΥΔΚ) δεν είναι εύκολα εφαρμόσιμες λόγω των υψηλών απαιτήσεων σε πόρους και της δυσκολίας να ολοκληρωθούν με τεχνολογίες Web 2.0 (π.χ. Javascript, Ajax και JSON) [10].

2.5.1 Έρευνα πεδίου σε αρχιτεκτονικές συστημάτων αξιοπιστίας

Σε αυτή την ενότητα γίνεται συνοπτική αναφορά στο ερευνητικό έργο που έχει γίνει τα τελευταία χρόνια στο πεδίο των δικτύων εμπιστοσύνης και παρουσιάζονται οι λόγοι για τους οποίους τα παραδοσιακά μοντέλα εμπιστοσύνης ομότιμων κόμβων [21, 50, 60] δεν καλύπτουν πλήρως τις ανάγκες προστασίας της ιδιωτικότητας σε συνεργατικά περιβάλλοντα [41].

Οι αρχιτεκτονικές που υιοθετούν τα σύγχρονα ΣΔΑ διακρίνονται σε δύο βασικές κατηγορίες ανάλογα με τον τρόπο διαχείρισης του βαθμού αξιοπιστίας που υιοθετούν οι οποίες παρουσιάζονται στη συνέχεια.

2.5.1.1 Αρχιτεκτονικές καταναμημένης διαχείρισης

Η έννοια της αξιοπιστίας, ή φήμης (*reputation*), χρησιμοποιήθηκε για πρώτη φορά αρκετά χρόνια πριν όταν η ανάπτυξη δικτύων ομότιμων κόμβων (*peer to peer networks, P2P*) αποτελούσε κοινή πρακτική. Σε αυτό το πλαίσιο, ο βαθμός αξιοπιστίας υποδεικνύει τον κόμβο του δικτύου ο οποίος ήταν περισσότερο ικανός να προσφέρει την καλύτερη ποιότητα υπηρεσιών με τον πλέον αξιόπιστο τρόπο [42].

Τα δίκτυα P2P ολοκληρώνουν αρχιτεκτονικές που βασίζονται στο μοντέλο της *καταναμημένης διαχείρισης (distributed reputation systems)* του βαθμού αξιοπιστίας. Με βάση αυτή την αρχιτεκτονική, κάθε ομότιμη οντότητα είναι υπεύθυνη για τη συλλογή και συσχέτιση των βαθμών αξιοπιστίας, δεδομένου μάλιστα ότι ο βαθμός αυτός προκύπτει ως ένα υποσύνολο των βαθμών αξιοπιστίας που συγκεντρώνουν οι «γείτονες» του εκάστοτε κόμβου.

Στις αρχιτεκτονικές *TwoHop* [49], *Poblano* [48], *PeerTrust* [61], *GNUnet* [52], *PGP* [53] και *P2Prep* [55] οι οποίες ανήκουν σε αυτή την κατηγορία, ο κάθε κόμβος διατηρεί μια δημόσια βάση δεδομένων στην οποία αποθηκεύει τις αξιολογήσεις που έχει κάνει σε υπηρεσίες άλλων κόμβων ώστε να τη συμβουλεύονται οι γείτονες κόμβοι για να υπολογίσουν το βαθμό αξιοπιστίας του Παρόχου Υπηρεσιών με τον οποίο επιθυμούν να αλληλεπιδράσουν (καθολικές τιμές αξιοπιστίας) ή βασίζεται στις ιδιωτικές πληροφορίες (τοπικές τιμές αξιοπιστίας) που διατηρεί σχετικά με τους υπόλοιπους κόμβους προκειμένου να αξιολογεί στο μέλλον την αξιοπιστία κάθε αλληλεπίδρασης μαζί τους.

Αν και στην πλειοψηφία τους οι προσεγγίσεις αυτές επιτρέπουν τον υπολογισμό των τιμών αξιοπιστίας με γρήγορο και αποδοτικό τρόπο, όπως απαιτείται στα πλαίσια των δικτυακών εφαρμογών στα οποία χρησιμοποιούνται, το γεγονός ότι βασίζονται στην καταναμημένη διαχείριση της εμπιστοσύνης μεταξύ των οντοτήτων που αλληλεπιδρούν καθιστά ανέφικτη την εφαρμογή τους σε

πλαίσια διαδικτυακών υπηρεσιών που δεν βασίζονται στην αρχιτεκτονική ομότιμων κόμβων. Για το λόγο αυτό δεν είναι δυνατό να ενσωματωθούν στις κεντροποιημένες αρχιτεκτονικές που υιοθετούν τα συνεργατικά περιβάλλοντα με σκοπό τη διαχείριση της αξιοπιστίας των χρηστών όσον αφορά στη δημιουργία περιεχομένου.

2.5.1.2 Αρχιτεκτονικές κεντροποιημένης διαχείρισης

Πιο πρόσφατα και προκειμένου τα Πληροφοριακά Συστήματα να προσαρμοστούν αποτελεσματικά στις ανάγκες των σύγχρονων πλαισίων υπηρεσιών, η αρχιτεκτονική των ΣΔΑ εξελίχθηκε σε συστήματα κεντροποιημένης διαχείρισης (*centralized reputation systems*). Με βάση αυτή την προσέγγιση, η πληροφορία σχετικά με τη φήμη ή τη συμπεριφορά και, κατ' επέκταση, την αξιοπιστία μιας οντότητας καθορίζεται από τη συλλογή των διαφορετικών αξιολογήσεων που συνεισφέρουν τα υπόλοιπα μέλη της κοινότητας σε μια κεντρική έμπιστη τρίτη οντότητα [42].

Ο κεντρικός αυτός Πάροχος είναι υπεύθυνος για τη διαχείριση και τον υπολογισμό του τελικού βαθμού αξιοπιστίας κάθε συμμετέχοντα με βάση το εκάστοτε μοντέλο εμπιστοσύνης. Επίσης, έχει σαν αρμοδιότητα τη διαχείριση και ανανέωση των βαθμών αξιοπιστίας προκειμένου οι χρήστες να διευκολύνονται στη λήψη αποφάσεων σχετικά με το αν επιθυμούν να αλληλεπιδράσουν με κάποια άλλη οντότητα χρησιμοποιώντας επίκαιρα και ακριβή δεδομένα.

Παραδείγματα τέτοιων αρχιτεκτονικών αποτελούν οι πλατφόρμες *EigenTrust* [59], *eBay* [51], και *OpenPrivacy* [54], οι οποίες βασίζονται στον υπολογισμό μιας προσέγγισης του βαθμού αξιοπιστίας για κάθε οντότητα του δικτύου μέσω επαναληπτικών διαδικασιών. Σε κάθε επανάληψη υπολογίζεται με μεγαλύτερη ακρίβεια ο βαθμός αξιοπιστίας που χαρακτηρίζει την κάθε οντότητα τη συγκεκριμένη χρονική στιγμή άλλες φορές λαμβάνοντας υπόψιν και άλλες όχι, το ρόλο ή την αξιοπιστία του αξιολογητή, θέτοντας κατάλληλα βάρη.

Δεδομένου ότι το μόνο που απαιτείται για να είναι εφικτή η ενσωμάτωση των δικτύων εμπιστοσύνης που ανήκουν σε αυτή την κατηγορία στις αρχιτεκτονικές ολοκληρωμένων πληροφοριακών συστημάτων είναι η ύπαρξη τουλάχιστον μιας κεντρικής και έμπιστης οντότητας η οποία θα αναλαμβάνει τη διαχείριση των βαθμών αξιοπιστίας, είναι φανερό ότι αποτελούν αποδεκτές λύσεις και για τα σύγχρονα συνεργατικά περιβάλλοντα. Από την άλλη πλευρά, όμως, οι υφιστάμενες προσεγγίσεις κεντροποιημένων ΣΔΑ δεν είναι μέχρι στιγμής ικανές να ικανοποιήσουν τις ανάγκες προστασίας της ιδιωτικότητας που χαρακτηρίζουν τα συνεργατικά περιβάλλοντα καθώς είτε προσανατολίζονται στην βελτίωση της ποιότητας των παρεχομένων υπηρεσιών είτε περιορίζονται στην αξιολόγηση των οντοτήτων που συμμετέχουν στο πλαίσιο εμπιστοσύνης

χωρίς να επιβάλλουν καθολικές πολιτικές διαχείρισης των προνομίων προσπέλασης.

Χαρακτηριστικά αναφέρεται ότι καμία προσέγγιση δεν έχει χρησιμοποιηθεί στα πλαίσια συστημάτων διαχείρισης ψηφιακών ταυτοτήτων, ώστε η απόδοση προνομίων προσπέλασης να γίνεται με δυναμικό τρόπο ανάλογα με την αξιοπιστία των χρηστών κάθε χρονική στιγμή στο να συμμετέχουν στο συνεργατικό περιβάλλον χωρίς να προσβάλλουν την ιδιωτικότητα των υπολοίπων συμμετεχόντων.

2.5.2 Έρευνα πεδίου σε μοντέλα υπολογισμού του βαθμού αξιοπιστίας

Τα μοντέλα υπολογισμού του βαθμού αξιοπιστίας που εφαρμόζουν τα σύγχρονα ΣΔΑ ποικίλλουν από μοντέλα *Διακριτής Εμπιστοσύνης (Discrete Trust)* και *Πεποιθήσεων (Belief)* μέχρι μοντέλα που βασίζονται σε *Ασαφή Λογική (Fuzzy)* και σε *Ροές (Flow)*, παρέχοντας ένα μεγάλο εύρος επιλογών [8]. Από την άλλη πλευρά, τα ΣΔΑ που ενσωματώνονται σε συνεργατικά περιβάλλοντα και σε περιβάλλοντα κοινωνικής δικτύωσης, βασίζονται συνήθως στην *αθροιστική ή αξιολόγηση μέσου όρου (summation or average of ratings)* και στο *μοντέλο ροής (flow model)* για να καλύψουν τις απαιτήσεις των εφαρμογών Web 2.0.

2.5.2.1 Μοντέλο αθροιστικής ή μέσου όρου αξιολόγησης

Η απλούστερη μορφή υπολογισμού της αξιοπιστίας είναι η διαφορά στις άθροισης των θετικών αξιολογήσεων και των αρνητικών αξιολογήσεων. Στο μοντέλο αυτό είναι απολύτως κατανοητή η διαδικασία εξαγωγής του τελικού βαθμού αξιοπιστίας [8]. Το μειονέκτημα είναι ότι παρέχει μια φτωχή εικόνα στους συμμετέχοντες.

Μια πιο εξελιγμένη μορφή του μοντέλου αυτού βασίζεται στον υπολογισμό του σταθμισμένου μέσου όρου όλων των αξιολογήσεων. Η στάθμιση της αξιολόγησης γίνεται με βάση παράγοντες όπως η αξιοπιστία αυτού που αξιολογεί, η χρονική στιγμή της αξιολόγησης, η διαφορά μεταξύ των αξιολογήσεων και του τρέχοντος βαθμού αξιοπιστίας κ.ά. [8].

Ένα παράδειγμα μοντέλου αξιολόγησης αθροιστικού ή μέσου όρου του βαθμού αξιοπιστίας εφαρμόζεται στο e-Bay, μια δημοφιλή ιστοσελίδα για εμπορικές συναλλαγές. Το e-Bay δίνει την δυνατότητα στις οντότητες που συμμετέχουν σε μια συναλλαγή να αξιολογήσουν ο ένας τον άλλο μετά την ολοκλήρωση της συναλλαγής, θετικά, αρνητικά ή ουδέτερα. Το e-Bay συλλέγει και επεξεργάζεται όλη αυτή την πληροφορία και υπολογίζει τους βαθμούς αξιοπιστίας των χρηστών με βάση το αθροιστικό μοντέλο ή το μοντέλο μέσου όρου. Επίσης, έχοντας σαν στόχο να δηλώσει την πιο πρόσφατη συμπεριφορά του συμμετέχοντος παρουσιάζει τρεις διαφορετικούς βαθμούς με χρονική διαφορά έξι μηνών, ενός μήνα και των τελευταίων επτά ημερών.

2.5.2.2 Μοντέλο αξιολόγησης ροών

Μοντέλα αξιολόγησης ροών ονομάζονται αυτά που υπολογίζουν το βαθμό αξιοπιστίας μέσω επαναλήψεων. Σε ορισμένα μοντέλα ροών τίθεται μια αρχική τιμή αξιοπιστίας για όλη την κοινότητα χρηστών ενώ, παράλληλα, τα μέλη της μπορούν να την αυξήσουν σε κόστος άλλων. Σε γενικές γραμμές, ο βαθμός αξιοπιστίας ενός χρήστη αυξάνεται σε συνάρτηση μιας ροής εισόδου και μειώνεται σε συνάρτηση μιας ροής εξόδου [8].

Ένα παράδειγμα εφαρμογής αυτού του μοντέλου υπολογισμού του βαθμού αξιοπιστίας αποτελεί το ΣΔΑ που χρησιμοποιεί το *Advogato*², μια κοινότητα προγραμματιστών ανοικτού κώδικα. Με βάση το μοντέλο αξιολόγησης ροών που χρησιμοποιείται το ΣΔΑ υπολογίζει τη ροή του βαθμού αξιοπιστίας μέσω ενός δικτύου όπου τα μέλη αποτελούν τους κόμβους και οι ενώσεις συνιστούν τις αναφορές μεταξύ των κόμβων. Κάθε μέλος-κόμβος λαμβάνει ένα βαθμό εμπιστοσύνης ανάλογα με την απόστασή του από τον αρχικό κόμβο. Ο αρχικός κόμβος έχει το μέγιστο βαθμό και όσο πιο μακριά από αυτόν βρίσκεται ένας κόμβος, τόσο μικρότερος είναι ο βαθμός του. Τα μέλη διαβαθμίζονται με βάση το βαθμό εμπιστοσύνης τους σε τρεις κατηγορίες (χαμηλού επιπέδου, μεσαίου επιπέδου και ανώτατου επιπέδου). Τελικά ένα ξεχωριστό γράφημα ροής υπολογίζεται για κάθε τύπο αναφοράς.

2.5.3 Ανοιχτά θέματα

Με βάση την έρευνα πεδίου, η διατριβή εντοπίζει την έλλειψη ερευνητικών αποτελεσμάτων τα οποία να αφορούν στην υιοθέτηση ΣΔΑ σε συνεργατικά περιβάλλοντα με στόχο την προστασία της ιδιωτικότητας [40]. Όλες οι διαθέσιμες μέθοδοι υπολογισμού αφορούν στη συλλογή και την καταγραφή δεδομένων με βάση κάποιο συγκεκριμένο πλαίσιο εμπορικών ή άλλων συναλλαγών [56, 57, 62] και, έτσι, δε λαμβάνουν υπόψη τους κρίσιμους εκείνους παράγοντες οι οποίοι επιδρούν και μεταβάλλουν το βαθμό αξιοπιστίας των χρηστών σε συνεργατικά περιβάλλοντα.

Από την άλλη πλευρά, καμία από τις υφιστάμενες μεθόδους υπολογισμού της αξιοπιστίας των χρηστών δε χρησιμοποιείται με στόχο να παρέχει δεδομένα για την απόδοση προνομίων προσπέλασης και έτσι η εφαρμογή τους συνήθως καταλήγει στη γραμμική αύξηση ή μείωση του τελικού αποτελέσματος με βάση τα δεδομένα που συλλέγει το ΣΔΑ χωρίς να λαμβάνεται υπόψη η επίδραση του συνεργατικού περιβάλλοντος.

Η καινοτομία της διατριβής σε αυτό τον ερευνητικό τομέα βασίζεται στο γεγονός ότι τα ΣΔΑ δεν έχουν χρησιμοποιηθεί, προς το παρόν, ως βασικά συστατικά συστημάτων διαχείρισης ταυτοτήτων ώστε με την ενσωμάτωσή

² <http://www.advogato.org/>

τους αυτή να λειτουργούν σαν μηχανισμοί διασφάλισης της εμπιστοσύνης μεταξύ των χρηστών. Η προσέγγιση αυτή η οποία παρουσιάζεται στο έκτο κεφάλαιο αξιοποιεί τη συλλογική γνώση των χρηστών σχετικά με τη συμπεριφορά των υπολοίπων συμμετεχόντων ως προς το κατά πόσο σέβονται την ιδιωτικότητά τους προκειμένου να γίνεται με πιο αξιόπιστο τρόπο η απόδοση προνομίων προσπέλασης στις υπηρεσίες που παρέχει το Πληροφοριακό Σύστημα. Επίσης, προτείνεται μια νέα αναδρομική μέθοδος υπολογισμού του βαθμού αξιοπιστίας η οποία είναι ορισμένη έτσι ώστε να καλύπτει κρίσιμους παράγοντες κάθε συνεργατικού περιβάλλοντος.

2.6 Συμπεράσματα

Παρά το γεγονός ότι τα σύγχρονα πρότυπα και προδιαγραφές διαχείρισης ταυτοτήτων καθώς και τα παραδοσιακά μοντέλα ελέγχου προσπέλασης είναι σήμερα σε ένα αρκετά ώριμο στάδιο εξέλιξης το οποίο επιτρέπει την αποτελεσματική και αξιόπιστη εφαρμογή τους για την προστασία της ιδιωτικότητας σε παραδοσιακά πλαίσια υπηρεσιών και Πληροφοριακά Συστήματα, η εξέλιξη των τεχνολογιών Web 2.0 και η ραγδαία εξάπλωση των αντίστοιχων διαδραστικών εφαρμογών συνεργασίας και κοινωνικής αλληλεπίδρασης άλλαξε το τοπίο και επέφερε νέες απαιτήσεις τις οποίες οι κλασικές προσεγγίσεις δεν είναι πάντα ικανές να καλύπτουν.

Με βάση τα αποτελέσματα της έρευνας πεδίου διαπιστώνεται ότι η αναβάθμιση των παρεχομένων υπηρεσιών από στατικό περιεχόμενο ιστοσελίδων σε διαδραστικές εφαρμογές επικοινωνίας και συμμετοχής των χρηστών αποτελεί παράλληλα μια σημαντική πρόκληση καθώς παρέχεται εύκολα η δυνατότητα στον καθένα να ενεργήσει με κακόβουλο τρόπο και για οποιοδήποτε λόγο, ακούσια ή εσκεμμένα, να αποκαλύψει προσωπικά και ευαίσθητα δεδομένα δημοσιεύοντας προσωπικές απόψεις και σχολιασμούς οι οποίοι προσβάλλουν την ιδιωτικότητα του κατόχου τους χωρίς τη συγκατάθεσή του.

Το γεγονός αυτό μάλιστα είναι ικανό να υποβαθμίσει το κύρος και το πεδίο εφαρμογής ενός Πληροφοριακού Συστήματος καθώς οι χρήστες τελικά δεν θα το εμπιστεύονται για να το προσπελάσουν. Ιδιαίτερα σε κρίσιμους τομείς με υψηλές απαιτήσεις ασφάλειας και ιδιωτικότητας γίνεται αντιληπτό ότι δεν υπάρχει περιθώριο απαξίωσης των παρεχομένων υπηρεσιών.

Διαπιστώνεται, επίσης, ότι η χρήση των εφαρμογών Web 2.0 αποδεικνύεται ελλιπής όσον αφορά στην υιοθέτηση κατάλληλων μηχανισμών ασφάλειας καθώς η διαχείριση ταυτοτήτων και ο έλεγχος προσπέλασης σε αυτές είναι είτε ανύπαρκτος είτε ελλιπής. Στην αδυναμία αυτή έρχεται επίσης να προστεθεί το γεγονός ότι η απόδοση προνομίων προσπέλασης στις διαδραστικές υπηρεσίες και εφαρμογές γίνεται με βάση τους ρόλους που παίρνουν οι χρήστες όταν αυθεντικοποιούνται και έτσι τα προνόμια εξουσιοδότησης παραμένουν σταθερά σε όλη τη διάρκεια χρήσης των παρεχομένων υπηρεσιών.

Για να ικανοποιούνται οι απαιτήσεις προστασίας της ιδιωτικότητας σε συνεργατικά περιβάλλοντα, θα πρέπει να αναβαθμιστούν οι διαδικασίες προσβασιμότητας στις υπηρεσίες Web 2.0 ώστε εκτός από το ρόλο των χρηστών να αξιολογείται και ο βαθμός αξιοπιστίας τους. Όπως περιγράφεται στα ανοιχτά θέματα της έρευνας πεδίου, αυτό απαιτεί την αναβάθμιση των ΣΔΑ, καθώς η συλλογική γνώση των χρηστών όπως αποτυπώνεται από τις αρνητικές ψήφους που υποβάλλουν δεν έχει χρησιμοποιηθεί μέχρι στιγμής ως κριτήριο απόδοσης προνομίων προσπέλασης.

Στη διατριβή προτείνεται ότι παράλληλα με την αξιοποίηση των δυνατοτήτων δυναμικής δημιουργίας περιεχομένου και ενεργής συμμετοχής σε ψηφιακές κοινότητες και υπηρεσίες κοινωνικής αλληλεπίδρασης, θα πρέπει να αντιμετωπιστούν αποτελεσματικά οι απειλές στην ιδιωτικότητα των χρηστών που προκύπτουν από την «ανεξέλεγκτη» χρήση των δραστικών λειτουργιών και εφαρμογών Web 2.0.

Σε αυτές τις προκλήσεις οι οποίες περιγράφονται αναλυτικά στα ανοιχτά θέματα που παρουσιάστηκαν στις προηγούμενες ενότητες παρέχει λύσεις η διατριβή μέσω των αποτελεσμάτων που παρουσιάζονται στα κεφάλαια που ακολουθούν.

2.7 Βιβλιογραφία

- [1] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thuraisingham (2011). "Semantic web-based social network access control". *Computers & Security, Special Issue on Access Control Methods and Technologies*. Vol. 30 (2-3), pp. 108-115. Elsevier.
- [2] Ponemon Institute (2010). "Privacy & Data Protection Practices". *Benchmark Study of the Financial Services Industry*. Research report.
- [3] ENISA (2011). "Report on trust and reputation model: Evaluation and guidelines".
- [4] J. Wang, H. Sun. (2009). "A new evidential trust model for open communities". *Computer Standards & Interfaces*, Vol. 31 (5), pp. 994-1001.
- [5] P. Guarda, N. Zannone (2009). "Towards the development of privacy-aware systems". *Journal of Information and Software Technology*. Vol. 51(2), pp. 337-350. Elsevier.
- [6] D. Wrighta, S. Gutwirthb, M. Friedewaldc, P. Hertb, M. Langheinrichd, A. Moscibrodab (2009). "Privacy, trust and policy-making: Challenges and responses". *The International Journal of Technology Law and Practice, Computer Law & Security Report*. Vol. 25(1), pp. 69-83. Elsevier.
- [7] P. Trudel (2009). "Privacy Protection on the Internet: Risk Management and Networked Normativity". *Reinventing Data Protection?. Part 4, chapter 19*, pp. 317-334. Elsevier. P. Dolog, M. Krotzsch, S. Schaffert, D. Vrande (2009). "Social Web and Knowledge Management". In *Proceedings of the WWW2008 Workshop on Social Web and Knowledge Management*, Beijing, China. Springer Verlag.
- [8] M. Benantar (2006). *Access Control Systems: Security, Identity Management and Trust Models*. Spinger.
- [9] R. Krishnan, R. Sandhu", J. Niut, W. Winsborough (2009). "Towards a Framework for Group-Centric Secure Collaboration". In *Proceedings of 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 1 - 10. IEEE Publications.

- [10] M. Levy (2009). "WEB 2.0 implications on knowledge management". *Journal of Knowledge Management* Vol. 13 (1), pp. 120-134. Emerald.
- [11] J. van Wamelen, D. de Kool (2008). "Web 2.0: A Basis for the Second Society?". In *Proceedings of the 2nd international conference on Theory and practice of electronic governance, ICEGOV2008*, December 1-4, Cairo, Egypt, pp. 349-354. ACM Publishing.
- [12] S. Murugesan (2007). "Understanding Web 2.0". *IT Professional - Second generation Web technologies*. Vol. 9 (4), pp. 34 – 41. IEEE Publications.
- [13] M. Pekárek, S. Pötzsch (2009). "A comparison of privacy issues in collaborative workspaces and social networks". *Identity in the Information Society, Special Issue: Social Web and Identity*. Vol. 2 (1), pp. 81-93. Springer.
- [14] B. Carminati, E. Ferrari, A. Perego (2009). "Enforcing Access Control in Web-Based Social Networks". *ACM Transactions on Information and System Security*. Vol. 13 (1), pp. 1-38. ACM Publishing.
- [15] NIST (2012). "Creating Options for Enhanced Online Security and Privacy". *National Strategy for Trusted Identities in Cyberspace*
- [16] I. Goldberg (2007). "Privacy Enhancing Technologies for the Internet III: Ten Years Later". In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. Vimercati (Eds.) *Digital Privacy: Theory, Technologies, and Practices*, Chapter 1, pp. 3-19.
- [17] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope (2005). "Trust Requirements in Identity Management". In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research, ACSW Frontiers '05*. Volume 44, pp. 99-108. ACM Publications.
- [18] T. Gruber (2008). "Collective knowledge systems: Where the Social Web meets the Semantic Web". *Web Semantics: Science, Services and Agents on the World Wide Web*. Vol. 6 (1), pp. 4–13. Elsevier.
- [19] K. J. Cosh, R. Burns, T. Daniel (2008). "Content clouds: classifying content in Web 2.0". *Library Review*, Vol. 57 (9), pp.722 – 729. Emerald.
- [19] A. Pfitzmann, M. Hansen (2008). "Anonymity, Unlinkability, Undetectability,

Unobservability, Pseudonymity, and Identity Management -- A Consolidated Proposal for Terminology”, Fachterminologie Datenschutz und Datensicherheit, pp. 111-144. Available from dud.inf.tu-dresden.de.

- [20] T. Lauer, X. Deng (2007). “Building online trust through privacy practices”. International Journal of Information Security. Vol. 6(5), pp. 323 – 331. Springer Verlag.
- [21] J. Traupman and R. Wilensky. (2006). "Robust Reputations for Peer-to-Peer Markets", Proc. International Conference on Trust Management (iTrust), 2006.
- [22] C. Tu (2002). “The relationship between social presence and online privacy”. The Internet and Higher Education. Vol. 5(4), pp. 293-318, Elsevier.
- [23] O’ Reilly (2006). “Web 2.0 Principles and Best Practices”. O’Reilly Media Inc.
- [24] M. Stocks (1995). “Perspectives on Privacy”. Psychiatric services Washington DC, Vol. 46(1), pp. 13-14. Academic Press (London) Ltd.
- [25] D. Solove (2006). “A taxonomy of privacy”. University of Pennsylvania Law Review, Vol 154 (3), pp. 447-560.
- [26] W. Tolone, G. Ahn, T. Pai (2005). “Access Control in Collaborative Systems”. Journal of Computing Surveys (CSUR). Vol. 37 (1), pp. 29 – 41. ACM Publishing.
- [27] OASIS (2006). Web Services Policy Framework (WS-Policy).
- [28] Liberty Alliance (2006). Liberty ID-FF Architecture Overview.
- [29] Liberty Alliance (2006). Liberty ID-WSF Web Services Framework Overview
- [30] OASIS (2007). WS-Trust Specifications, version 1.3.
- [31] Liberty Alliance (2007). Liberty IGF Privacy Constraints Specification.
- [32] CSC Study (2009). Identity Management 2nd Edition.
- [33] H. EL Yamany, M. Capretz, D. Allison (2010). “Intelligent security and access control framework for service-oriented architecture”. Information and

Software Technology. Vol. 52 (2), pp. 220–236. Elsevier.

- [34] A. Jøsang, M. Al Zomai, S. Suriadi (2007). "Usability and Privacy in Identity Management Architecture". In Proceedings of the fifth Australasian symposium on ACSW frontiers, ACSW '07. Vol. 68, pp. 143-152. Australian Computer Society.
- [35] J. Koltera, T. Kernchen, G. Pernul (2008). "Collaborative privacy management". In Proceedings of the 2008 International Conference on Information Security and Assurance (isa 2008), pp. 52-56. IEEE Publisher.
- [36] J. Anderson, C. Diaz, J. Bonneau, F. Stajano (2009). "Privacy-enabling social networking over untrusted networks". In Proceedings of the 2nd ACM workshop on Online social networks (WOSN '09). pp. 1-6. ACM Publishing.
- [37] E. Kapetanios (2008). "Quo Vadis computer science: From Turing to personal computer, personal content and collective intelligence". Data & Knowledge Engineering. Vol. 67 (2), pp. 286–292. Elsevier.
- [38] S. Atlag (2009). Collective Intelligence in Action.
- [39] H. C. Choi, S. Kruk, S. Grzonkowski, K. Stankiewicz, B. Davis, J. Breslin (2006). "Trust Models for Community Aware Identity Management". In Proceedings of the Identity, Reference and Web Workshop, in conjunction with WWW 2006.
- [40] ENISA (2007). "Reputation-based Systems: a security analysis". Position Paper.
- [41] W. Zheng, L. Jin (2009). "Online Reputation Systems in Web 2.0 Era". Value Creation in E-Business Management, Business Information Processing. Vol. 36 (4), pp. 296-306. Springer Verlag.
- [42] A. Jøsang, R. Ismail, C. Boyd (2007). "A Survey of Trust and Reputation Systems for Online Service Provision". Journal of Decision Support Systems. Vol. 43 (2), pp. 618-644. Elsevier.
- [43] T. O' Reilly, J. Battalle (2009). "Web Squared: Web 2.0 Five Years On". O' Reilly Publishing.
- [44] B. F. O'Connor, J. L. Griffin (2009). "Mnikr: Reputation Construction

Through Human Trading of Distributed Social Identities”. In Proceedings of the 5th ACM workshop on Digital identity management, DIM '09, pp. 3-12. ACM Publishing.

- [45] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, K. Nahrstedt (2009). “A trust management framework for service-oriented environments”. In Proceedings of the 18th international conference on World wide web, WWW '09, pp. 891-900. ACM Publishing.
- [46] P. A. Bonatti, J. L. De Coi, D. Olmedilla, L. Sauro (2008). “Policy-Driven Negotiations and Explanations: Exploiting Logic-Programming for Trust Management, Privacy & Security”. In Proceedings of the 24th International Conference on Logic Programming (ICLP '08), pp. 779-784.
- [47] L. Lobato, E.B. Fernandez, S.D. Zorzo, (2009). “Patterns to Support the Development of Privacy Policies”. In Proceedings of International Conference on Availability, Reliability and Security, (ARES '09), pp. 744-749. IEEE Publications.
- [48] M. Dekker, S. Etalle, J. Hartog (2006). “Privacy Policies”. Security Privacy and Trust in Modern Data Management. Springer.
- [49] D. Glynos, P. Argyroudis, C. Douligeris (2012). “Collaborative service evaluation with the TwoHop Trst Framework”. Security and Communication Networks. Vol. 5, pp. 549-613.
- [50] R. Chen, W. Yeager (2003). “Poblano: a Distributed Trust Model for Peer-to-Peer Networks”. Technical report. Sun Microsystems.
- [51] eBay Inc. (2012) “Online Auction and Shopping Website”. <http://www.ebay.com>
- [52] D. Kugler (2003). “An analysis of GNUnet and the Implications for Anonymous, Censorship-Resistant Networks”. In Proceedings of 3rd Workshop on Privacy Enhancing Techonologies (PET '03), pp. 161-176.
- [53] P. Zimmermann (1995). The Official PGP User’s Guide. MIT Press.
- [54] F. Labalme, K. Burton (2001). “Enhancing the Internet with Reputations: an OpenPrivacy White Paper” Available at:

<http://openprivacy.org/papers/200103-white.html>

- [55] F. Cornelli, E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati (2002). "Choosing Reputable Servents in a P2P Network". In Proceedings of 11th International World Wide Web Conference (W3C '02). Honolulu, Hawaii.
- [56] T. Jiang, J. Baras (2006). "Trust Evaluation in Anarchy: A case study on Autonomous Networks". In Proceedings of 25th IEEE International Conference on Computer Communications (Infocom '06), pp. 1-12. Barcelona, Spain.
- [57] R. Didgedine, M. Freedman, D. Molnar (2000). "The Free Haven Project: Distributed Anonymous Storage Service". In Proceedings of 2000 Workshop on Design Issues in Anonymity and Unobservability, pp. 67-25.
- [58] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati (2003). "Managing and Sharing Servents' Reputations in P2P Systems". IEEE Transactions on Knowledge and Data Engineering. Vol. 15 (4), pp. 850-854.
- [59] S. Kamvar, M. Schlosser, H. Garcia-Molina (2003). "EigenTrust Algorithm for Reputation Management in P2P Networks". In Proceedings of 12th International World Wide Web Conference (WWW '03), pp. 640-651. Budapest, Hungary.
- [60] R. Prasad, V. Srinivas, V. Kumari, K. Raju (2009). "An effective Calculation of Reputation in P2P Networks". Journal of Networks. Vol. 4(5), pp. 332-342.
- [61] L. Xiong, I. Liu (2004). "PeerTrust: Supporting reputation based trust of peer-to-peer electronic communities". IEEE Transactions on Knowledge and Data Engineering. Vol. 16, pp. 843-857.
- [62] M. G. Uddin, M. Zulkernine, S.I. Ahamed (2008). "CAT: a context-aware trust model for open and dynamic systems". In Proceedings of the 2008 ACM symposium on Applied computing, pp. 2024-2029. New York, USA.
- [63] Anonymizer.com. Anonymizer - Anonymous Proxy, Anonymous Surfing & Anti Spyware. Available at: <http://www.anonymizer.com/>.
- [64] D. Goldschlag, M. Reed, P. Syverson (1999). Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM. Vol. 42(2):

pp. 39–41.

- [65] R. Dingledine, N. Mathewson (2007). Tor: anonymity online. Available at: <http://tor.eff.org/>.
- [66] R. Dingledine, N. Mathewson, P. Syverson (2004). Tor: The Second-Generation Onion Router. In Proceedings of the 13th USENIX Security Symposium, San Diego, CA.
- [67] PrivacyBird. Available at: <http://www.privacybird.org/>
- [68] PGP Corporation. PGP Corporation - Products - PGP Desktop Email. Available at: http://www.pgp.com/products/desktop_email/index.html.
- [69] OASIS (2007). “Technical Committee: ‘Security Assertion Markup Language v.2.0’”. Technical Overview. OASIS Standard Specification.
- [70] P. J. Windley (2005). Digital Identity. O Reilly Press.

Κεφάλαιο 3

Απαιτήσεις Ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος

Στόχος του κεφαλαίου είναι να εντοπιστούν και να καταγραφούν οι απαιτήσεις σχεδιασμού και να καθοριστούν οι προδιαγραφές ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος κατάλληλου να εφαρμοστεί σε κρίσιμους τομείς της σύγχρονης Κοινωνίας της Πληροφορίας για την παροχή έμπιστων, ασφαλών και αξιόπιστων υπηρεσιών.

3.1 Εισαγωγή

Η εξέλιξη και η ευρεία αποδοχή των τεχνολογιών Web 2.0 και των εφαρμογών συνεργασίας και κοινωνικής δικτύωσης δημιούργησε μια νέα τάση στις ηλεκτρονικές υπηρεσίες. Η νέα αυτή προσέγγιση είναι σε θέση να αντιμετωπίσει αποτελεσματικά κοινωνικές, νομικές και τεχνολογικές προκλήσεις όταν βασίζεται σε σωστά τεχνολογικά πλαίσια, καθώς η διαχείριση πληροφοριών πλέον δεν υλοποιείται αποκλειστικά από τους Παρόχους, αλλά και από τους ίδιους τους χρήστες. Ιδιαίτερα σε κρίσιμους τομείς όπου απαιτείται η συνεργασία μεταξύ διαφορετικών φορέων καθώς και η άμεση αλληλεπίδραση μεταξύ των χρηστών με σκοπό την καταγραφή εμποδίων και αδυναμιών των υφιστάμενων πρακτικών, η εφαρμογή συνεργατικών πληροφοριακών συστημάτων αποτελεί ίσως την πιο αξιόπιστη λύση.

Επιπρόσθετα των εφαρμογών Web 2.0, οι οποίες παρέχουν τη δυνατότητα έκφρασης προσωπικών απόψεων, πεποιθήσεων και σχολίων και τη δημιουργία περιεχομένου από τους ίδιους τους χρήστες, η διατριβή προτείνει (βλ. Κεφάλαιο 7) ότι τα σύγχρονα συνεργατικά περιβάλλοντα (collaborative workspaces) θα πρέπει επίσης να επιτρέπουν τη συλλογική συνεισφορά και διαχείριση ποικίλου ψηφιακού περιεχομένου (π.χ. ηλεκτρονικά αρχεία εγγράφων και πολυμέσων, περιγραφές επιχειρησιακών διαδικασιών και μοντέλα αναπαράστασης πολιτικών, αρχεία XML, οντολογίες, κτλ.) και την παροχή προηγμένων δυνατοτήτων και καινοτόμων υπηρεσιών (π.χ. μοντελοποίηση διαδικασιών, εναρμόνιση πολιτικών, ανοιχτές διαβουλεύσεις, αναζήτηση εγγράφων και πληροφοριών και δημιουργία συλλογικής γνώσης).

Από τεχνολογικής απόψεως, όπως παρουσιάστηκε στην έρευνα πεδίου της ενότητας 2.4.2, οι βασικές και πιο δημοφιλείς τεχνολογίες, πρότυπα και προδιαγραφές είναι πλέον ικανές στο να παρέχουν μια σταθερή τεχνολογική υποδομή στην οποία θα βασιστούν και θα αναπτυχθούν διαλειτουργικά, εύρωστα και έμπιστα συνεργατικά περιβάλλοντα. Για παράδειγμα, οι σύγχρονες προσανατολισμένες στις Υπηρεσίες αρχιτεκτονικές θεωρούνται αποδεδειγμένα μια επιτυχημένη προσέγγιση για τη διασύνδεση ετερογενών συστημάτων, κάτι που είναι πολύ σημαντικό για την ανάπτυξη συνεργατικών συστημάτων και διαλειτουργικών πλαισίων υπηρεσιών.

Αντίθετα, η διατριβή διαπιστώνει ότι παρά το γεγονός ότι οι εφαρμογές Web 2.0 αποτελούν την επικρατέστερη προσέγγιση επέκτασης των σύγχρονων υπηρεσιών, δεν υπάρχει σαφής ορισμός των βασικών αρχών και των προδιαγραφών που θα πρέπει να διέπουν την ενσωμάτωσή τους σε έμπιστα συνεργατικά περιβάλλοντα. Αυτό θα βοηθούσε στο σχεδιασμό αξιόπιστων αρχιτεκτονικών ικανών να υποστηρίξουν την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών υποστηρίζοντας παράλληλα τη συνεργασία.

Ανακεφαλαιώνοντας, τα συνεργατικά περιβάλλοντα και δίκτυα κοινωνικής αλληλεπίδρασης αποτελούν πλέον ένα συνεχώς εξελισσόμενο επιχειρησιακό μοντέλο με ιδιαίτερα θετικά οφέλη. Παρόλα αυτά, η χρήση αυτών των εργαλείων λογισμικού τις περισσότερες φορές δεν είναι επαρκής όταν υιοθετείται απομονωμένη από ολοκληρωμένα πληροφοριακά συστήματα και πλαίσια υπηρεσιών. Σε δυναμικά περιβάλλοντα και τομείς με υψηλές απαιτήσεις, όπως για παράδειγμα, οι υπηρεσίες η-Διακυβέρνησης, απαιτείται η ολοκλήρωσή τους με άλλες τεχνολογίες ακολουθώντας ευρέως αποδεκτά πρότυπα και προδιαγραφές ασφάλειας και διαλειτουργικότητας, προκειμένου να υποστηρίζεται η αλληλεπίδραση των χρηστών με αποτελεσματικό και αξιόπιστο τρόπο. Παρόλα αυτά δεν υπάρχει μέχρι στιγμής κάποιο ευρέως αποδεκτό πλαίσιο προδιαγραφών (π.χ. e-GIF³) που να υποστηρίζει την αναβάθμιση των παραδοσιακών Πληροφοριακών Συστημάτων σε έμπιστα περιβάλλοντα συνεργασίας με προτυποποιημένο τρόπο.

Στις ενότητες που ακολουθούν καθορίζονται οι βασικές απαιτήσεις που θα πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό έμπιστων συνεργατικών πληροφοριακών συστημάτων ώστε να εξασφαλίζεται η παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

³ <http://www.e-gif.gov.gr/portal/page/portal/egif/>

3.2 Προσδιορισμός απαιτήσεων

Η επεξεργασία και διαχείριση πληροφοριών και συλλογικής γνώσης και η παροχή υπηρεσιών κοινωνικής αλληλεπίδρασης αποτελούν βασικές απαιτήσεις για το στρατηγικό σχεδιασμό καινοτόμων λύσεων υψηλής προστιθέμενης αξίας. Στοχεύοντας προς αυτή την κατεύθυνση, ο ρόλος των ολοκληρωμένων συνεργατικών πληροφοριακών συστημάτων γίνεται ιδιαίτερα σημαντικός στο να ενισχύσει τη διασύνδεση ετερογενών πηγών δεδομένων καθώς και στο να αξιοποιήσει τη γνώση που παράγεται από τους ίδιους τους χρήστες ικανοποιώντας παράλληλα τις βασικές τους ανάγκες και ενθαρρύνοντας τη συμμετοχή τους.

3.2.1 Απαιτήσεις χρηστών

Η αποτελεσματική χρήση των συνεργατικών πληροφοριακών συστημάτων και των διαδραστικών υπηρεσιών προϋποθέτει και καθιστά ιδιαίτερα κρίσιμη την ικανοποίηση μιας κατηγορίας πολύ σημαντικών απαιτήσεων, αυτών που αφορούν την αποδοχή από τους τελικούς χρήστες.

Η έρευνα των λόγων για τους οποίους οι χρήστες αποδέχονται ή απορρίπτουν τις νέες τεχνολογίες αποτελεί μια πρόκληση, καθώς αρκετά μοντέλα προσπαθούν να εξηγήσουν τους βασικούς παράγοντες που επηρεάζουν την αποδοχή τους ενώ άλλα εστιάζουν στο να προβλέψουν την επίδραση των παραγόντων αυτών στην εξέλιξη και την υιοθέτηση καινοτόμων λύσεων και υπηρεσιών.

Στο πλαίσιο της διατριβής μελετήθηκαν τα πρότυπα ISO/IEC 9126 [15], ISO/DIS 9241-11 [14] και τα αποτελέσματα που προέκυψαν προτείνουν ότι οι πρωταρχικές απαιτήσεις των χρηστών όσον αφορά στη χρήση συνεργατικών πληροφοριακών συστημάτων και διαδραστικών υπηρεσιών, προσδιορίζονται όπως περιγράφεται στις υποενότητες που ακολουθούν.

3.2.1.1 Χρησιμότητα

Αποτελέσματα μελετών [14] αποδεικνύουν ότι η προσωπική διάθεση του καθενός όσον αφορά στη χρήση ενός πληροφοριακού συστήματος επηρεάζεται σε μεγάλο βαθμό από τον παράγοντα της *Χρησιμότητας*. Υψηλός βαθμός χρησιμότητας σαν αυτόν που χαρακτηρίζει την ενσωμάτωση εφαρμογών Web 2.0 σε κατάλληλα πλαίσια υπηρεσιών, οδηγεί σε θετική αποδοχή προηγμένων τεχνολογικών λύσεων και πλαισίων υπηρεσιών.

3.2.1.2 Ευχρηστία

Τα πρότυπα ISO/IEC 9126 [15], ISO/DIS 9241-11 [14] αναγνωρίζουν την υψηλή επίδραση αυτής της απαίτησης στη *Χρησιμότητα* των παρεχομένων υπηρεσιών. Χαρακτηριστικά αναφέρεται ότι η *Ευχρηστία* ως απαίτηση έχει ιδιαίτερα θετική

επίδραση τόσο στη *Χρησιμότητα* όσο και στην επιθυμία του χρήστη να συνεχίσει να χρησιμοποιεί καινοτόμες λύσεις και υπηρεσίες.

3.2.1.3 Πολυγλωσσικότητα

Η ανάμειξη και η συνεργασία διαφορετικών φορέων, κοινωνικών ομάδων και χρηστών στο πλαίσιο ενός συνεργατικού περιβάλλοντος σε διασυνοριακό επίπεδο επιβάλλει την ανάγκη για διαλειτουργικές διεπαφές και υπηρεσίες οι οποίες θα παρέχουν δυνατότητες *Πολυγλωσσικότητας* και προσαρμογής του περιεχομένου στις ανάγκες της κάθε χώρας έτσι ώστε να γεφυρώνονται οι κοινωνικές, θρησκευτικές και πολιτισμικές διαφορές.

3.2.1.4 Εμπιστοσύνη

Όπως διαπιστώνεται στο πλαίσιο της διατριβής, σε συνεργατικά περιβάλλοντα οι χρήστες πρέπει να εμπιστεύονται εκτός από τους Παρόχους που διαχειρίζονται τα προσωπικά τους δεδομένα και τη συμπεριφορά των υπολοίπων χρηστών που συμμετέχουν ενεργά στο πλαίσιο συνεργασίας. Αυτό σημαίνει ότι ακόμα και αν η αξιοπιστία του Παρόχου είναι αναμφισβήτητη και ο τρόπος με τον οποίο υλοποιεί τις πολιτικές ιδιωτικότητας ο πλέον αποτελεσματικός, όσο δεν εφαρμόζονται μηχανισμοί προστασίας από την «ανεξέλεγκτη» δημιουργία περιεχομένου η εμπιστοσύνη των χρηστών για τις παρεχόμενες υπηρεσίες δεν είναι προφανής [2].

3.2.2 Λειτουργικές απαιτήσεις

Ο σχεδιασμός έμπιστων συνεργατικών πληροφοριακών συστημάτων προϋποθέτει ότι θα αξιοποιούν αποδοτικά όλες τις δυνατότητες των σύγχρονων τεχνολογιών ενσωματώνοντας όχι μόνο εφαρμογές Web 2.0 [5] αλλά και άλλες τεχνολογικές λύσεις (π.χ. συστήματα διαχείρισης ταυτοτήτων, συστήματα μοντελοποίησης διαδικασιών, και τεχνολογίες ασφάλειας) [1] ικανοποιώντας την:

- ✓ Συνεργασία και αλληλεπίδραση μεταξύ των χρηστών.
- ✓ Ολοκλήρωση συστημάτων με δυνατότητες αποθήκευσης, αναζήτησης και διαχείρισης πληροφοριακών αγαθών.
- ✓ Συλλογή στατιστικών δεδομένων.
- ✓ Ολοκλήρωση μηχανισμών μοντελοποίησης και ανάλυσης διαδικασιών και μοντέλων πολιτικών.
- ✓ Διασύνδεση ετερογενών βάσεων δεδομένων και πληροφοριακών συστημάτων.
- ✓ Παροχή υπηρεσιών λήψης αποφάσεων.

Προκειμένου να ικανοποιηθούν αυτές οι απαιτήσεις, η διατριβή προτείνει ότι κάθε *Έμπιστο Συνεργατικό Πληροφοριακό Σύστημα (ΕΣΠΣ)* θα πρέπει να

ενσωματώνει αξιόπιστες τεχνολογικές λύσεις διαχείρισης περιεχομένου ικανές να υποστηρίξουν τη διασύνδεση ετερογενών βάσεων δεδομένων, την ανάπτυξη επεκτάσιμων ταξονομιών περιεχομένου, την παροχή διαδραστικών εργαλείων προσθήκης, επεξεργασίας και διαχείρισης πληροφοριών καθώς και προηγμένων μηχανών αναζήτησης [6].

Από την άλλη πλευρά και δεδομένου ότι η χρήση διαδραστικών λειτουργιών (π.χ. δημιουργία περιεχομένου, σχολιασμός, κοινοποίηση πληροφοριών, ηλεκτρονικές ψηφοφορίες) είναι σε θέση να παρέχει λύσεις σε κρίσιμους τομείς της Κοινωνίας της Πληροφορίας, η ενσωμάτωση τεχνολογιών Web 2.0 αποτελεί εξίσου σημαντική απαίτηση [7]. Απαραίτητη, λοιπόν, κρίνεται η παροχή υπηρεσιών συνεργασίας (π.χ. ιστολόγια, φόρουμ, wiki) έτσι ώστε να παρέχεται η δυνατότητα στους χρήστες να συνεργάζονται και να ανταλλάσσουν πληροφορίες και γνώσεις, να μοιράζονται τις εμπειρίες τους και να αλληλεπιδρούν προκειμένου να βρουν λύσεις στα προβλήματα που αντιμετωπίζουν [8].

Ο σχεδιασμός και η υλοποίηση μηχανισμών υποστήριξης αποφάσεων αποτελεί, επίσης, μια βασική λειτουργική απαίτηση η οποία αφορά στη δυνατότητα των χρηστών να αναλύουν και να συνθέτουν χρήσιμες πληροφορίες προερχόμενες από διαφορετικές πηγές έτσι ώστε να εντοπίζουν και να επιλύουν πολύπλοκα προβλήματα και να ενισχύουν τις προσπάθειές τους για τη λήψη σωστών αποφάσεων [4]. Η διατριβή προτείνει ότι κάθε ΕΣΠΣ θα πρέπει να είναι σε θέση να επεξεργάζεται αποτελεσματικά ετερογενή δεδομένα, να παράγει στατιστικές αναλύσεις και αντίστοιχες γραφικές αναπαραστάσεις των αποτελεσμάτων και γενικότερα να αξιοποιεί τη συλλογική γνώση που παράγεται στα πλαίσια του συνεργατικού περιβάλλοντος [3].

Τέλος, εκτός από τις προαναφερόμενες λειτουργίες κάθε ΕΣΠΣ θα πρέπει να ενσωματώνει εργαλεία και μηχανισμούς μοντελοποίησης και διαχείρισης διαδικασιών έτσι ώστε να παρέχεται η δυνατότητα, μέσω φιλικών προς το χρήστη γραφικών διεπαφών, μοντελοποίησης και γραφικής αναπαράστασης επιχειρησιακών μοντέλων. Η υιοθέτηση αυτών των τεχνολογιών είναι επίσης ικανή να συνεισφέρει αποτελεσματικά στον εντοπισμό των διαφορών και αποκλίσεων μεταξύ ετερογενών διαδικασιών και να ενισχύσει τις προσπάθειες προς εναρμονισμένες λύσεις.

Λαμβάνοντας υπόψιν και ικανοποιώντας τις προαναφερθείσες λειτουργικές απαιτήσεις, η αρχιτεκτονική του ΕΣΠΣ θα είναι σε θέση να παρέχει ένα πλαίσιο χρήσιμων υπηρεσιών και να αξιοποιεί αποτελεσματικά τις δυνατότητες συνεργασίας και αλληλεπίδρασης μεταξύ των χρηστών που παρέχει κάθε συνεργατικό περιβάλλον [9].

3.2.3 Τεχνικές απαιτήσεις

Όλες οι απαιτήσεις που παρουσιάστηκαν στις ενότητες 3.2.2 και 3.2.1 επηρεάζουν και καθορίζουν με σαφή τρόπο τα λειτουργικά χαρακτηριστικά που θα πρέπει να λαμβάνονται υπόψιν κατά τον αρχιτεκτονικό σχεδιασμό συνεργατικών πληροφοριακών συστημάτων. Παρόλα αυτά, είναι αναγκαίο να καθοριστεί, επίσης, ο τρόπος με τον οποίο θα πρέπει να ολοκληρωθούν μεταξύ τους όλα τα τεχνικά μέρη και υποσυστήματα προκειμένου τελικά να προκύψει ένα ολοκληρωμένο, αξιόπιστο και έμπιστο συνεργατικό περιβάλλον [3, 4]. Στην Εικόνα 1 εμφανίζονται όλες οι τεχνικές απαιτήσεις που θα πρέπει να ικανοποιούνται [10, 16].



Εικόνα 1: Τεχνικές απαιτήσεις ΕΣΠΣ

Όπως φαίνεται στην εικόνα, κάθε επιτυχημένη προσέγγιση αρχιτεκτονικού σχεδιασμού [11] θα πρέπει να βασίζεται σε ένα ολοκληρωμένο πλαίσιο προδιαγραφών, ικανοποιώντας οχτώ βασικές τεχνικές απαιτήσεις:

1. Διαλειτουργικότητα
2. Ασφάλεια
3. Επαναχρησιμοποίηση
4. Προστασία της ιδιωτικότητας
5. Αρθρωτή αρχιτεκτονική
6. Επεκτασιμότητα
7. Ανοιχτά πρότυπα
8. Διαδραστικότητα.

Κάθε μια από τις τεχνικές απαιτήσεις που εμφανίζονται στην Εικόνα 1 αναλύεται με λεπτομέρεια στις υποενότητες που ακολουθούν.

3.2.3.1 Διαλειτουργικότητα

Η διαλειτουργικότητα αφορά στην ικανότητα του Πληροφοριακού Συστήματος να ανταλλάσσει πληροφορίες με άλλα πληροφοριακά συστήματα. Συγκεκριμένα προϋποθέτει:

1. Μια σαφώς καθορισμένη μορφή για τις πληροφορίες (πρότυπες δομές δεδομένων και μετά-πληροφορίας).
2. Ένα σαφώς καθορισμένο τρόπο για την ανταλλαγή πληροφοριών (τεχνολογίες επικοινωνιών και πρωτόκολλα με τα οποία μεταφέρονται τα δεδομένα στην προκαθορισμένη μορφή).
3. Ένα σαφώς καθορισμένο τρόπο για την πρόσβαση στις πληροφορίες και στα δεδομένα.
4. Ένα σαφώς καθορισμένο τρόπο για την αναζήτηση των πληροφοριών και των δεδομένων (τεχνολογίες μετά-δεδομένων και καταλόγου).
5. Ταξονομίες και οντολογίες περιεχομένου ώστε να επιτυγχάνεται σημασιολογική διαλειτουργικότητα στο επίπεδο των δεδομένων και των πληροφοριακών αγαθών που ανταλλάσσονται μεταξύ ετερογενών συστημάτων.

Η διαλειτουργικότητα μεταξύ των βασικών οντοτήτων μεγάλων πληροφοριακών συστημάτων επιτυγχάνεται υιοθετώντας την τεχνολογία των Υπηρεσιών Ιστού ως το βασικό πρωτόκολλο επικοινωνίας σε συνδυασμό με σύγχρονες τεχνολογίες XML για τη μεταφορά στων δεδομένων. Χαρακτηριστικά αναφέρεται ότι η ολοκλήρωση Διαύλων Διαλειτουργικής Επικοινωνίας (Enterprise Service Bus, ESB) αποτελεί την πιο αποτελεσματική λύση προς αυτή την κατεύθυνση, Το ενδιαμέσο αυτό επίπεδο ολοκλήρωσης αναλαμβάνει τη διαχείριση των εσωτερικών και των εξωτερικών προς το σύστημα αλληλεπιδράσεων μεταξύ ετερογενών συστημάτων με διαφανή τρόπο, αξιοποιώντας τη δυνατότητα επικοινωνίας μέσω ενός διαλειτουργικού διαύλου ανταλλαγής μηνυμάτων.

3.2.3.2 Ασφάλεια

Υπάρχουν πέντε βασικές απαιτήσεις ασφάλειας οι οποίες θα πρέπει να ικανοποιούνται απαραίτητα:

- ✓ *Αυθεντικοποίηση*, η μέθοδος με την οποία μια οντότητα αναγνωρίζεται με μοναδικό τρόπο και επικυρώνει την ταυτότητά της.

- ✓ *Ακεραιότητα*, η μέθοδος που διασφαλίζει ότι κάθε σύστημα, πόρος, αρχείο και πληροφορία είναι δυνατόν να μεταβληθεί μόνο από εξουσιοδοτημένες οντότητες.
- ✓ *Εμπιστευτικότητα*, η μέθοδος με βάση την οποία μόνο οι εξουσιοδοτημένες οντότητες έχουν πρόσβαση στο περιεχόμενο των πληροφοριών.
- ✓ *Μη αποποίηση ευθύνης*, η μέθοδος που παράγει κρυπτογραφικά δεδομένα τα οποία διασφαλίζουν ότι μια οντότητα δεν μπορεί να αποποιηθεί τις ενέργειές της.
- ✓ *Διαθεσιμότητα*, η μέθοδος που διασφαλίζει ότι ένα σύστημα είναι σε θέση να ικανοποιήσει τους στόχους του με ένα συγκεκριμένο βαθμό επιτυχίας.

Κάθε ΕΣΠΣ θα πρέπει να ικανοποιεί τις προαναφερθείσες απαιτήσεις ασφάλειας κάνοντας χρήση αξιόπιστων μέτρων προστασίας και υιοθετώντας τα κατάλληλα πρότυπα [12].

3.2.3.3 Επαναχρησιμοποίηση

Οι στόχοι που εξυπηρετούνται από την απαίτηση της επαναχρησιμοποίησης συνδέονται άμεσα με τους στρατηγικούς στόχους των *Προσανατολισμένων στις Υπηρεσίες Αρχιτεκτονικών (SOA)*, οι οποίες σύμφωνα με τα αποτελέσματα της διατριβής θα πρέπει να υιοθετούνται και στα συνεργατικά περιβάλλοντα.

Ένα σύγχρονο συνεργατικό περιβάλλον θα πρέπει επίσης να προσφέρει προηγμένες και επαναχρησιμοποιήσιμες διεπαφές για υπηρεσίες ασφάλειας, διαχείρισης και συνεργασίας έτσι ώστε να είναι εύκολη η επέκταση των δυνατοτήτων του.

3.2.3.4 Προστασία ιδιωτικότητας

Στα συνεργατικά περιβάλλοντα εντοπίζονται επιπρόσθετες απαιτήσεις προστασίας των προσωπικών δεδομένων κυρίως λόγω των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0 [2]. Για παράδειγμα, συνεργατικές εφαρμογές όπως τα ιστολόγια και τα φόρουμ παρέχουν προνόμια σε ανώνυμους καθώς και σε ταυτοποιημένους χρήστες να διατυπώνουν προσωπικές απόψεις και να αναφέρονται σε ευαίσθητα δεδομένα άλλων χρηστών. Έτσι, η ιδιωτικότητα εξαρτάται σε μεγάλο βαθμό από τα κίνητρα των χρηστών οι οποίοι έχουν προνόμια προσπέλασης του συνεργατικού περιβάλλοντος.

Δεδομένου ότι στα πλαίσια κάθε ΕΣΠΣ η έννοια της εμπιστοσύνης πρέπει να περιλαμβάνει και τις αλληλεπιδράσεις μεταξύ των χρηστών, η διατριβή προτείνει ότι για να χαρακτηριστεί ένα συνεργατικό περιβάλλον ως έμπιστο είναι απαραίτητη η χρήση καινοτόμων λύσεων *Διαχείρισης Ταυτοτήτων* οι οποίες ενσωματώνουν τις δυνατότητες *Συστημάτων Διαχείρισης Αξιοπιστίας*

έτσι ώστε να αξιοποιείται η συλλογική συνεισφορά των χρηστών στην προστασία της ιδιωτικότητας (βλ. Κεφάλαιο 6).

3.2.3.5 Αρθρωτή αρχιτεκτονική

Κάθε επιμέρους σύστημα της αρχιτεκτονικής του ΕΣΠΣ θα πρέπει να αποτελεί μέρος ενός μεγαλύτερου συστήματος και να λειτουργεί σε αυτό το πλαίσιο ανεξάρτητα. Έτσι, το ολοκληρωμένο Πληροφοριακό Σύστημα θα είναι σε θέση να περιορίσει ένα λειτουργικό πρόβλημα σε ένα σύνολο από λιγότερο πολύπλοκα υπό-προβλήματα τα οποία συνήθως είναι συνδεδεμένα μεταξύ τους με μια απλή δομή και είναι αρκετά ανεξάρτητα ώστε να επιτρέπουν την παράλληλη επεξεργασία τους.

Με τον τρόπο αυτό οι αρνητικές επιδράσεις μιας μη συνηθισμένης λανθασμένης λειτουργίας θα περιοριστεί στο συγκεκριμένο υποσύστημα ή στη χειρότερη περίπτωση θα επηρεάσει έναν μικρό μόνο αριθμό γειτονικών διασυνδεδεμένων υποσυστημάτων.

3.2.3.6 Επεκτασιμότητα

Οι προηγμένες και καινοτόμες λύσεις απαιτούν τη δημιουργία ενός μηχανισμού διασύνδεσης μεταξύ των επιχειρησιακών διεργασιών και των ετερογενών συστημάτων προκειμένου οι Πάροχοι να είναι σε θέση να διατηρούν επεκτάσιμα συστήματα ικανά να υποστηρίξουν με αποδοτικό τρόπο τις συνεχώς εξελισσόμενες απαιτήσεις.

Το σημαντικότερο όφελος, όμως, από την υιοθέτηση επεκτάσιμων αρχιτεκτονικών ιδιαίτερα για τα συνεργατικά περιβάλλοντα αποτελεί η δυνατότητα να επεκτείνουν με δυναμικό τρόπο το σύνολο των υπηρεσιών που παρέχουν και κατ' επέκταση τη χρησιμότητά τους για τους τελικούς χρήστες. Επιτρέποντας την εύκολη ολοκλήρωση και διασύνδεσή τους με νέες υπηρεσίες, εφαρμογές και συστήματα ανεξάρτητα από τον τομέα στον οποίο ανήκουν και την πλατφόρμα βάση της οποίας αναπτύχθηκαν, είναι ικανά να παρέχουν ένα ολοκληρωμένο περιβάλλον συνεργασίας.

3.2.3.7 Ανοικτά πρότυπα

Μια από τις βασικότερες απαιτήσεις κατά το σχεδιασμό και την υλοποίηση σύγχρονων συστημάτων, αποτελεί η ελαχιστοποίηση του κόστους όχι μόνο για την συγκεκριμένη ανάπτυξη αλλά, συνήθως, και για κάθε μελλοντική βελτίωσή του. Η προσέγγιση υιοθέτησης ανοιχτών προτύπων εκτός από τα άμεσα οικονομικά οφέλη που προσφέρει παράλληλα παρέχει τη δυνατότητα συμμετοχής σε ενεργές κοινότητες χρηστών που παρέχουν συνεχή και αξιόπιστη υποστήριξη.

3.2.3.8 Διαδραστικότητα

Η διαδραστικότητα αποτελεί ίσως την πιο κρίσιμη τεχνική απαίτηση καθώς είναι αυτή που προκύπτει από τις σύγχρονες ανάγκες των χρηστών για άμεση αλληλεπίδραση και δημιουργία προσωπικού περιεχομένου. Θα πρέπει να αποτελεί αναπόσπαστο χαρακτηριστικό κάθε ΕΣΠΣ, το οποίο συνήθως παρέχεται ή είναι άμεσα εξαρτώμενο από την ολοκλήρωση εφαρμογών Web 2.0 και αντίστοιχων προηγμένων γραφικών διεπαφών και διαδραστικών λειτουργιών [9, 13].

3.3 Συμπεράσματα

Τα οφέλη που προκύπτουν από την ικανοποίηση των οχτώ (8) βασικών τεχνικών απαιτήσεων που παρουσιάστηκαν στην προηγούμενη ενότητα είναι ο σχεδιασμός αξιόπιστων και προτυποποιημένων αρχιτεκτονικών και η ανάπτυξη έμπιστων και διαλειτουργικών συστημάτων συνεργασίας.

Στο πλαίσιο της διατριβής, ελήφθησαν υπόψιν όλες οι προαναφερόμενες απαιτήσεις για τον αρχιτεκτονικό σχεδιασμό του Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος που παρουσιάζεται στο επόμενο κεφάλαιο. Συνολικά, οι λειτουργικές και τεχνικές απαιτήσεις που προαναφέρθηκαν καθορίζουν:

1. Τις τεχνικές προδιαγραφές που πρέπει να υιοθετηθούν.
2. Τη μεθοδολογία σχεδιασμού και ανάπτυξης που πρέπει να ακολουθηθεί.
3. Τις τεχνολογίες που είναι απαραίτητο να χρησιμοποιηθούν.

Η διατριβή προτείνει ότι κάθε έμπιστο συνεργατικό περιβάλλον θα πρέπει να αξιοποιεί:

- ✓ Την συνεργατική χρήση μηχανισμών μοντελοποίησης πολιτικών και διαδικασιών.
- ✓ Την αποτελεσματική σύνθεση διαδραστικών διεπαφών και κατανεμημένων εφαρμογών που βασίζονται σε τεχνολογίες Web 2.0 ώστε να υποστηρίζεται η ενεργή συμμετοχή και συνεισφορά των χρηστών.
- ✓ Την υιοθέτηση συστημάτων διαχείρισης γνώσης καθώς και κατάλληλα σχεδιασμένων ταξονομιών περιεχομένου.
- ✓ Τη διασύνδεση και αξιοποίηση πολλαπλών και κατανεμημένων πηγών πληροφόρησης.

Τα αποτελέσματα της διατριβής που παρουσιάστηκαν σε αυτό το κεφάλαιο αποτελούν το απαραίτητο υπόβαθρο για την πρώτη βασική συνεισφορά της η οποία επικεντρώνεται στην ενσωμάτωση εφαρμογών Web 2.0 σε ολοκληρωμένα Πληροφοριακά Συστήματα και πλαίσια υπηρεσιών, όπως παρουσιάζεται στο επόμενο κεφάλαιο με τον αρχιτεκτονικό σχεδιασμό του ΕΣΠΣ.

3.4 Βιβλιογραφία

- [1] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Collaborative information and knowledge management environments: The "what" and "how"". OR Insight Journal, Special Issue on Facilitating information and knowledge management through Information Systems and Operational Research: from theory to practice.
- [2] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Open Issues on Privacy and Trust in Collaborative Environments". In Proceedings of the IEEE Symposium on Computers and Communications (ISCC 2011), Kerkyra, Greece. IEEE Digital Library.
- [3] G. Pentafronimos, A. Karantjias, N. Polemi (2010). "ODYSSEUS: An Advanced, Collaborative and Trusted Framework for the Provision of Migration Services". In Proceedings of the Fifth International Conference on Internet and Web Applications and Services. pp. 531-537. Barcelona, Spain. IEEE Digital Library.
- [4] G. Pentafronimos, A. Karantjias και N. Polemi (2009). "OPIS: An Open, Preventive and Scalable Migration Information System". In Proceedings of the 3rd International Conference on e-Democracy. Next Generation Society: Technological and Legal Issues, (e-Democracy 2009). Athens, Greece. Springer Verlag.
- [5] D. Richards (2009). "A social software/Web 2.0 approach to collaborative knowledge engineering". Information Sciences, Vol. 179 (15), pp. 2515–252. Including Special Issue on Computer-Supported Cooperative Work-Techniques and Applications. The 11th Edition of the International Conference on CSCW in Design.
- [6] S. Callahan, M. Schenk, N. White (2008). "Building a collaborative workplace," Anecdote Publishing.
- [7] K. Zettsu, K. Yasushi (2006). "Towards Knowledge Management Based on Harnessing Collective Intelligence on the Web". Managing Knowledge in a World of Networks.
- [8] A. Boder (2006). "Collective intelligence: a keystone in knowledge

- management". Journal of Knowledge Management, pp. 81-93.
- [9] P. Isaias, P. Miranda. S. Pifano (2009). "Critical Success Factors for Web 2.0 – A Reference Framework". In Proceedings of the 3d International Conference on Online Communities and Social Computing: Held as Part of HCI International 2009 (OCSC '09), pp. 354-363. Springer Verlag.
- [10] T. O' Reilly (2007). "What Is Web 2.0: Design Patterns and Business" O' Reilly Media.
- [11] A. Karantjias, T. Stamati, N. Polemi, «Migration-aware policy-making in decentralised and dynamic social and collaborative environments,» International Journal of Electronic Governance, Vol. 4(3), pp. 209-229.
- [12] T. Glaser, F. Pallas (2007). "Information Security and Knowledge Management: Solutions Through Analogies?". Social Science Research.
- [13] M. Graeme, M. Reddington, M. B. Kneafsey, M. Sloman (2009). "Scenarios and strategies for Web 2.0". Education & Training, Vol. 51 (5/6) pp. 370-380.
- [14] ISO IEC DIS 9241-11: 1998 Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability. Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883
- [15] ISO IEC 9126-1:2001 Software engineering -- Product quality -- Part 1: Quality model. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22749
- [16] A. Karantjias, S. Papastergiou, N. Polemi (2009). "Design Principles of a Secure Federated e/m-Government Framework". International Journal of Electronic Governance (IJEG), Special Issue on Users and uses of electronic governance 2(4), pp. 402-423.

Κεφάλαιο 4

ΕΣΠΣ: Ένα Έμπιστο Συνεργατικό Πληροφοριακό Σύστημα

Στο κεφάλαιο αυτό παρουσιάζεται η πρώτη βασική συνεισφορά της διατριβής η οποία περιλαμβάνει το αρχιτεκτονικό σχέδιο ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος ικανού να καλύπτει όλες τις τεχνικές και τις λειτουργικές απαιτήσεις που καθορίστηκαν στο 3^ο Κεφάλαιο.

4.1 Εισαγωγή

Στο πλαίσιο της διατριβής, ως Έμπιστο Συνεργατικό Πληροφοριακό Σύστημα ορίζεται κάθε ολοκληρωμένο πληροφοριακό σύστημα το οποίο ενσωματώνει σύγχρονες τεχνολογίες και εφαρμογές Web 2.0 καθώς και προηγμένες διεπαφές διασύνδεσης και διαλειτουργικότητας με άλλα συστήματα, έτσι ώστε να είναι δυνατή η παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών. Ο χαρακτηρισμός του ως «έμπιστο» προκύπτει από την ανάγκη ενσωμάτωσης κατάλληλων μέτρων προστασίας της ιδιωτικότητας από τις απειλές που ελλοχεύει η ολοκλήρωση των εφαρμογών Web 2.0 (βλ. Κεφάλαια 5, 6).

4.2 Μεθοδολογία σχεδιασμού

Παρέχοντας σαν βασική συνεισφορά στον ερευνητικό τομέα της *Συνεργασίας* τον ορισμό μιας ολοκληρωμένης μεθοδολογίας για το σχεδιασμό του ΕΣΠΣ, ένα από τα βασικά αποτελέσματα της διατριβής είναι η αποτελεσματική σύνθεση και εφαρμογή ενός συνόλου προτύπων και μεθοδολογιών προκειμένου τελικά να καθοριστεί μια αξιόπιστη και επεκτάσιμη αρχιτεκτονική [1]. Στο πλαίσιο της διατριβής χρησιμοποιείται το πρότυπο RM-ODP [9, 10], διαγράμματα UML, και οι αρχές της πολυεπίπεδης αρχιτεκτονικής.

Το *Reference Model of Open Distributed Processing (RM-ODP)* αποτελεί ένα μοντέλο αναφοράς στην επιστήμη των υπολογιστών το οποίο παρέχει ένα πλαίσιο διαχείρισης και προτυποποίησης ανοιχτών υπολογιστικών συστημάτων (*Open Distributed Processing, ODP*). Αναφερόμενο επίσης και ως *ITU-T Rec. X.901-X.904* και *ISO/IEC 10746* το πρότυπο RM-ODP αποτελεί μια συλλογική προσπάθεια του Παγκόσμιου Οργανισμού Προτυποποίησης *International*

Organization for Standardization (ISO), του International Electrotechnical Commission (IEC) και του Telecommunication Standardization Sector (ITU-T).

Όπως φαίνεται και στο Σχήμα 1 που ακολουθεί το μοντέλο RM-ODP περιλαμβάνει πέντε (5) συμπληρωματικές προσεγγίσεις ανάλυσης του εκάστοτε πληροφοριακού συστήματος και του ευρύτερου περιβάλλοντος εφαρμογής του οι οποίες αναφέρονται και ως Όψεις.



Σχήμα 1: Μοντέλο RM-ODP

Όπως φαίνεται στο Σχήμα 1, οι πέντε (5) διαφορετικές αλλά αλληλεξαρτώμενες Προσεγγίσεις ανάλυσης του Πληροφοριακού Συστήματος κατά RM-ODP είναι οι εξής:

- ✓ Η *Επιχειρησιακή Προσέγγιση (Enterprise viewpoint)* ορίζει τους στόχους και την εμβέλεια εφαρμογής ενός πληροφοριακού συστήματος σε συνάρτηση με τους κανόνες που θα χρησιμοποιηθούν για την περιγραφή του.
- ✓ Η *Πληροφοριακή Προσέγγιση (Information viewpoint)* καθορίζει τις δομές των δεδομένων και των πληροφοριών που πρόκειται να επεξεργαστεί και να διαχειριστεί το εκάστοτε σύστημα.
- ✓ Η *Υπολογιστική Προσέγγιση (Computational viewpoint)* επικεντρώνεται στη βελτιστοποίηση των προδιαγραφών της αρχιτεκτονικής μέσω του διαχωρισμού των λειτουργιών σε επιμέρους υποσυστήματα τα οποία αλληλεπιδρούν μεταξύ τους.
- ✓ Η *Τεχνική Προσέγγιση (Engineering viewpoint)* καθορίζει την τεχνική αρχιτεκτονική σε επίπεδο λειτουργικών συστημάτων και συσκευών υλικού που θα είναι υπεύθυνη για τη λειτουργία του πληροφοριακού συστήματος.
- ✓ Η *Τεχνολογική Προσέγγιση (Technology viewpoint)* ορίζει τις τεχνολογίες και τα εργαλεία λογισμικού που θα χρησιμοποιηθούν κατά τη φάση της

ολοκλήρωσης καθώς και τα σενάρια δοκιμών που θα πρέπει να πραγματοποιηθούν πριν την τελική εφαρμογή τους συστήματος.

Για την ανάλυση της κάθε προσέγγισης χρησιμοποιούνται κάποιοι βασικοί κανόνες οι οποίοι όμως επιτρέπουν τη χρήση και άλλων προτύπων και μεθόδων σχεδιασμού και ανάλυσης ανάλογα με τις ανάγκες, απαιτήσεις και περιορισμούς της εκάστοτε μελέτης εφαρμογής.

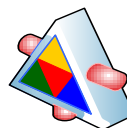
Η γλώσσα μοντελοποίησης *UML* αποτελεί ένα πρότυπο το οποίο αναπτύχθηκε από το *Object Management Group (OMG)* προκειμένου να χρησιμοποιηθεί για την αντικειμενοστρεφή μοντελοποίηση εφαρμογών λογισμικού και συστημάτων γενικότερα. Η *UML* καθορίζει προκαθορισμένες γραφικές αναπαραστάσεις και δομές προκειμένου να περιγράφονται οι οντότητες και οι αλληλεπιδράσεις τους. Αυτό επιτρέπει την ομοιόμορφη περιγραφή των δομικών χαρακτηριστικών και των επιμέρους υποσυστημάτων. Τα διαγράμματα *UML* περιλαμβάνουν αρκετούς τύπους για την αναπαράσταση όλων των απαραίτητων πληροφοριών και δεδομένων ενός μοντέλου από όλες τις διαφορετικές προσεγγίσεις.

Τέλος, η πολυεπίπεδη αρχιτεκτονική (*multi-tier architecture*) αποτελεί μια προτυποποιημένη προσέγγιση αρχιτεκτονικής λογισμικού στην οποία ένα σύστημα χωρίζεται σε διαφορετικά επίπεδα ολοκλήρωσης. Συνήθως, η πολυεπίπεδη ή αρθρωτή αρχιτεκτονική ενός Πληροφοριακού Συστήματος αποτελείται από το επίπεδο των βάσεων δεδομένων, το επίπεδο ολοκλήρωσης της επιχειρησιακής λογικής και το επίπεδο ολοκλήρωσης των γραφικών διεπαφών χρήστη. Κάθε μια από αυτές τις δομικές μονάδες μπορεί να εγκατασταθεί σε διαφορετικό υπολογιστικό σύστημα, επικοινωνώντας με τις υπόλοιπες μέσω προκαθορισμένων διαύλων και πρωτοκόλλων δικτυακής επικοινωνίας. Το Σχήμα 2 αναπαριστά την προσέγγιση της αρχιτεκτονικής τριών επιπέδων.

A: Επίπεδο διεπαφών χρήστη



B: Επίπεδο επιχειρησιακών διεργασιών



Γ: Επίπεδο βάσεων δεδομένων



Σχήμα 2: Αρχιτεκτονική 3 επιπέδων

Όπως φαίνεται στο Σχήμα 2, τα τρία επίπεδα της αρχιτεκτονικής διαχωρίζουν τα βασικά συστατικά μέρη του πληροφοριακού συστήματος με βάση τη λειτουργικότητα που παρέχουν.

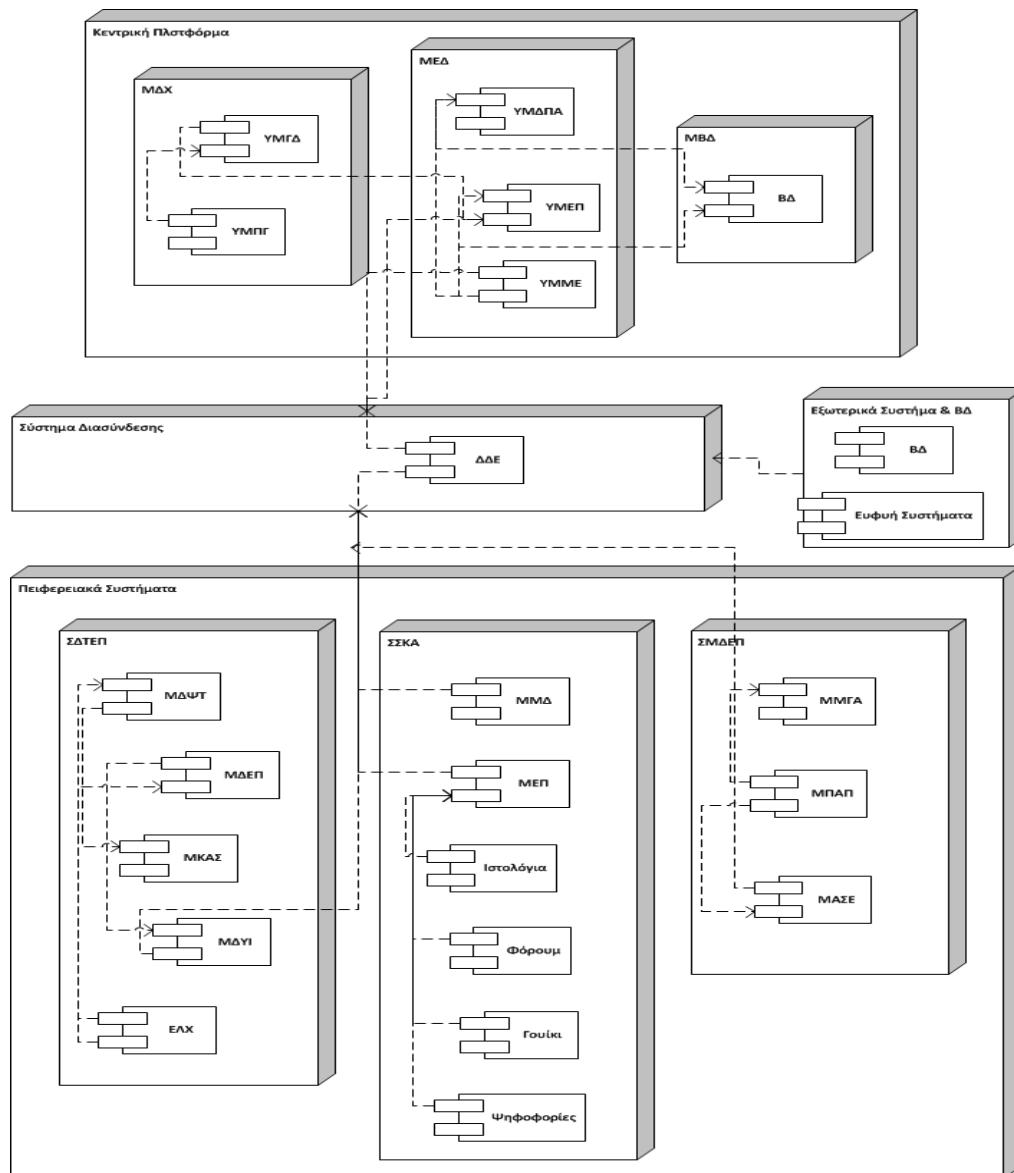
Έχοντας σαν βασικό στόχο τον σαφή καθορισμό ενός έμπιστου συνεργατικού περιβάλλοντος και όλων των βασικών υποσυστημάτων που θα πρέπει να ενσωματώνει ώστε να ικανοποιούνται οι λειτουργικές και οι τεχνικές απαιτήσεις που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, στις ενότητες που ακολουθούν παρουσιάζεται η αρχιτεκτονική του ΕΣΠΣ που προτείνεται στο πλαίσιο της διατριβής. Πιο συγκεκριμένα, η ανάλυση που ακολουθεί περιλαμβάνει δύο από τις Όψεις του προτύπου RM-ODP, την *Υπολογιστική Προσέγγιση* και την *Πληροφοριακή Προσέγγιση*.

Ακολουθώντας την Υπολογιστική Προσέγγιση του μοντέλου RM-ODP περιγράφεται το αρχιτεκτονικό σχέδιο του ΕΣΠΣ το οποίο ικανοποιεί όλες τις προκαθορισμένες απαιτήσεις όπως παρουσιάστηκαν στο Κεφάλαιο 3. Από την άλλη πλευρά, η Πληροφοριακή Προσέγγιση περιγράφει τις μονάδες και τα υποσυστήματα του ΕΣΠΣ όσον αφορά στις καταστάσεις των πληροφοριών που διαχειρίζονται και παρέχουν.

Αξιοποιώντας την εύκολα επεκτάσιμη δομή του προτύπου RM-ODP, η ανάλυση αυτών των δύο Όψεων του είναι ικανή όχι μόνο να ορίσει επαρκώς το Πληροφοριακό Σύστημα αλλά παράλληλα να παρέχει τα απαραίτητα επίπεδα αφαίρεσης καθώς δεν περιλαμβάνει τεχνικούς, τεχνολογικούς και επιχειρησιακούς περιορισμούς. Τελικά προκύπτει ένα ολοκληρωμένο αρχιτεκτονικό σχέδιο, το οποίο δεν εξαρτάται από τις ιδιαιτερότητες κάθε τεχνολογικής πλατφόρμας. Έχει δηλαδή οριζόντια ισχύ για όλα τα ΕΣΠΣ και με βάση τα αποτελέσματα της ερευνητικής εργασίας που έλαβε χώρα στα πλαίσια του Ευρωπαϊκού έργου ImmigrationPolicy2.0 αποδεικνύεται ιδιαίτερα χρήσιμο και αποτελεσματικό για κρίσιμους τομείς της Κοινωνίας της Πληροφορίας, όπως αυτός της η-Μετανάστευσης (βλ. Κεφάλαιο 7).

4.3 Αρχιτεκτονική ΕΣΠΣ

Στο Σχήμα 3 φαίνεται η συνολική αρχιτεκτονική του ΕΣΠΣ καθώς και ο τρόπος με τον οποίο διασυνδέονται και επικοινωνούν μεταξύ τους οι διαφορετικές μονάδες του πληροφοριακού συστήματος. Ο σχεδιασμός της αρχιτεκτονικής ακολούθησε τις τεχνικές απαιτήσεις που καθορίστηκαν στο Κεφάλαιο 3 και ενσωματώνει όλα εκείνα τα χαρακτηριστικά που είναι απαραίτητα για τη σύνθεση ενός αξιόπιστου πλαισίου για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.



Σχήμα 3: Αρχιτεκτονική του ΕΣΠΣ

Όπως φαίνεται στο Σχήμα 3 η αρχιτεκτονική του ΕΣΠΣ αποτελείται από την *Κεντρική Πλατφόρμα* και τα ανεξάρτητα *Περιφερειακά Συστήματα* τα οποία ενσωματώνονται σε αυτή μέσω του *Συστήματος Διασύνδεσης*.

Υιοθετώντας το μοντέλο της αρθρωτής αρχιτεκτονικής και πιο συγκεκριμένα της αρχιτεκτονικής 3 επιπέδων, η κεντρική πλατφόρμα αποτελείται από:

- τη *Μονάδα Διεπαφών Χρήστη (ΜΔΧ)*,
- τη *Μονάδα Επιχειρησιακών Διεργασιών (ΜΕΔ)*, και
- τη *Μονάδα Βάσεων Δεδομένων (ΜΒΔ)*,

οι οποίες ολοκληρώνονται σε τρία διαφορετικά επίπεδα της αρχιτεκτονικής προκειμένου να ικανοποιούνται οι τεχνικές που παρουσιάστηκαν στην ενότητα 3.2.3.

Επίσης, τα Περιφερειακά Συστήματα τα οποία θα πρέπει να περιλαμβάνονται στο αρχιτεκτονικό σχέδιο ώστε να ικανοποιούνται οι προκαθορισμένες λειτουργικές απαιτήσεις είναι:

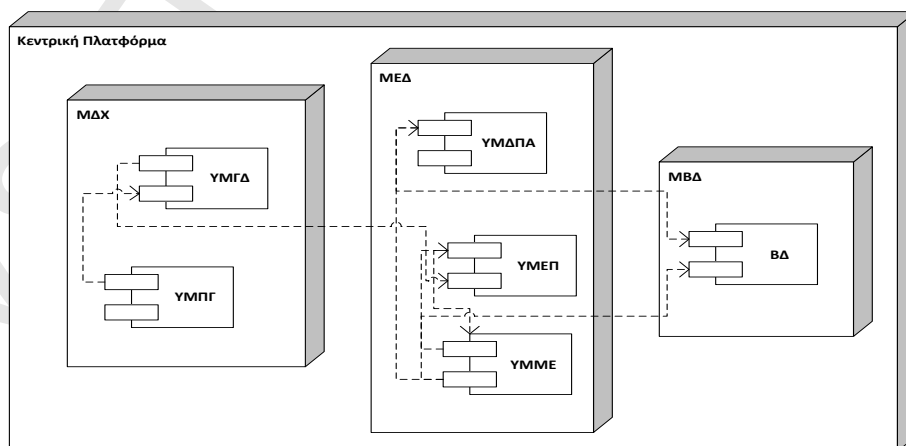
- το Σύστημα Μοντελοποίησης Διαδικασιών και Εναρμόνισης Πολιτικών (ΣΜΔΕΠ),
- το Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης (ΣΔΤΕΠ), και
- το Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης (ΣΣΚΑ).

Τέλος, η επιτυχής και αποτελεσματική διασύνδεση και αλληλεπίδραση της Κεντρικής Πλατφόρμας με τα Περιφερειακά Συστήματα αλλά και με κάθε άλλη εξωτερική του ΕΣΠΣ οντότητα απαιτεί τη διαλειτουργική επικοινωνία με χρήση τεχνολογιών Υπηρεσιών Ιστού. Αυτό επιτυγχάνεται μέσω της ολοκλήρωσης ενός Διαλειτουργικού Διαύλου Επικοινωνίας (ΔΔΕ) για την ανταλλαγή προτυποποιημένων μηνυμάτων στο Σύστημα Διασύνδεσης. Έτσι, κάθε εξωτερική του ΕΣΠΣ οντότητα η οποία ενδεχομένως πρέπει να αλληλεπιδράσει μελλοντικά με το ΕΣΠΣ μπορεί πολύ εύκολα να το κάνει αναπτύσσοντας τις απαιτούμενες διεπαφές Υπηρεσιών Ιστού προκειμένου να επικοινωνήσει με το ΔΔΕ.

Στις ενότητες που ακολουθούν, περιγράφεται αναλυτικά κάθε λειτουργική μονάδα του αρχιτεκτονικού σχεδίου που εμφανίζεται στο Σχήμα 3. Πιο συγκεκριμένα, κάθε σύστημα και μονάδα αναλύονται με βάση τις προκαθορισμένες Όψεις του προτύπου RM-ODP και χρησιμοποιώντας τα κατάλληλα διαγράμματα UML όπως περιγράφονται στην ενότητα 4.2.

4.3.1 Κεντρική πλατφόρμα

Στην ενότητα αυτή παρουσιάζονται οι τεχνικές προδιαγραφές της κεντρικής πλατφόρμας του ΕΣΠΣ (βλ. Σχήμα 3) αναλύοντας τις επιμέρους τεχνικές μονάδες. Στο πιο κάτω διάγραμμα UML φαίνεται ο τρόπος διασύνδεσης μεταξύ των τριών (3) επιπέδων της αρχιτεκτονικής.



Σχήμα 4: Κεντρική πλατφόρμα του ΕΣΠΣ

Όπως φαίνεται στο Σχήμα 4 και αναλύεται με περισσότερη λεπτομέρεια στις ενότητες που ακολουθούν, η ΜΕΔ αποτελεί το συνδετικό κρίκο μεταξύ της ΜΔΧ και της ΜΒΔ. Στη συνέχεια παρουσιάζονται με περισσότερη λεπτομέρεια και οι τρεις αυτές βασικές μονάδες της κεντρικής πλατφόρμας του ΕΣΠΣ οι οποίες ολοκληρώνονται σε τρία διαφορετικά επίπεδα της αρχιτεκτονικής.

4.3.1.1 Μονάδα Διεπαφών Χρήστη

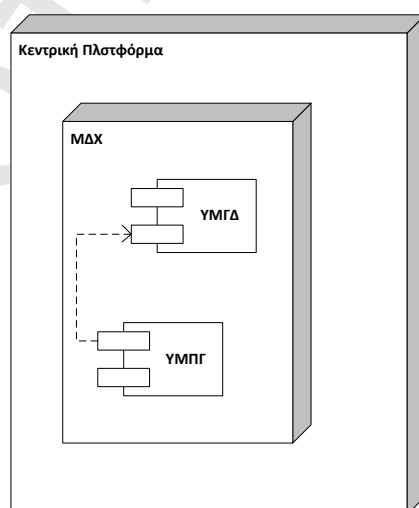
Η Μονάδα Διεπαφών Χρήστη (ΜΔΧ) παρέχει ένα απλό, εύχρηστο και συνεκτικό τρόπο παρουσίασης του περιεχομένου και των λειτουργιών που παρέχονται από τα διάφορα εργαλεία και τα υποσυστήματα που ολοκληρώνονται στη Μονάδα Επιχειρησιακών Διεργασιών (ΜΕΔ). Επίσης, το επίπεδο αυτό αποτελεί ένα ασφαλές σημείο προσπέλασης των παρεχομένων υπηρεσιών.

Βασικός ρόλος της ΜΔΧ είναι η ενσωμάτωση όλων των απαραίτητων γραφικών διεπαφών για την παρουσίαση του περιεχομένου και των παρεχομένων λειτουργιών στους τελικούς χρήστες. Για το λόγο, αυτό βασική προτεραιότητα κατά το σχεδιασμό και την υλοποίηση αυτής της μονάδας είναι η ικανοποίηση των βασικών απαιτήσεων χρηστών που παρουσιάστηκαν στην ενότητα 3.2.1.

Στις υποενότητες που ακολουθούν αναλύεται η ΜΔΧ με βάση την υπολογιστική και πληροφοριακή προσέγγιση του μοντέλου RM-ODP παρουσιάζοντας με περισσότερη λεπτομέρεια τις τεχνικές προδιαγραφές που θα πρέπει να υιοθετούνται.

4.3.1.1.1 Υπολογιστική προσέγγιση

Η ανάλυση με βάση την υπολογιστική προσέγγιση επικεντρώνεται στην τεχνική ολοκλήρωση των οντοτήτων που αποτελούν τη ΜΔΧ.



Σχήμα 5: Διάγραμμα UML των υποσυστημάτων της ΜΔΧ

Το διάγραμμα UML στο Σχήμα 5 αναπαριστά τις βασικές υπολογιστικές μονάδες της ΜΔΧ οι οποίες είναι:

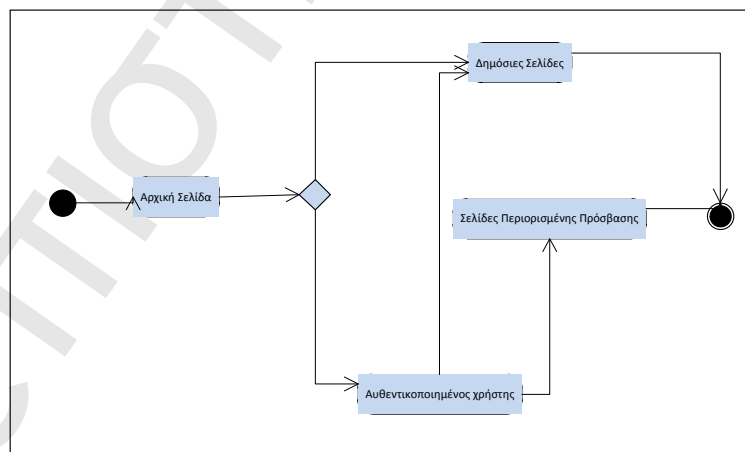
- η Υπό-Μονάδα Γραφικών Διεπαφών (ΥΜΓΔ), και
- η Υπό-Μονάδα Πολυγλωσσικότητας (ΥΜΠΓ)

Οι γραφικές διεπαφές πρέπει να βασίζονται σε ανοιχτές τεχνολογίες διαδικτυακού προγραμματισμού, όπως οι Java/JSP, .NET/ASP, PHP, καθώς και σε πιο σύγχρονες, όπως οι AJAX, Javascript και JSON, προκειμένου να ικανοποιούν τις απαιτήσεις για φιλικότητα προς το χρήστη, διαδραστικότητα και ευχρηστία. Επίσης, αυτή η μονάδα αποτελεί το κεντρικό σημείο διασύνδεσης όλων των υπολοίπων μονάδων της ΜΔΧ καθώς παρέχει τους μηχανισμούς αλληλεπίδρασης με τους τελικούς χρήστες.

Η υπό-μονάδα πολυγλωσσικότητας παρέχει όλους τους απαραίτητους μηχανισμούς για τη μετάφραση του περιεχομένου με συνεπή, αξιόπιστο και εύκολα διαχειρίσιμο τρόπο ανάλογα με την επιλογή του τελικού χρήστη. Για να επιτευχθεί αυτό θα πρέπει να χρησιμοποιούνται καθολικά προσπελάσιμα αρχεία παραμετροποίησης και αντίστοιχοι μηχανισμοί όπως η δημοφιλής βιβλιοθήκη i18n [17], η λειτουργικότητα της οποίας θα πρέπει να ολοκληρώνεται σε αυτή την υπομονάδα της ΜΔΧ. Η εφαρμογή αυτής της προσέγγισης είναι σε θέση να παρέχει τα απαραίτητα επίπεδα επεκτασιμότητας και διαλειτουργικότητας με άλλα συστήματα.

4.3.1.1.2 Πληροφοριακή προσέγγιση

Κάθε φορά που ο χρήστης επιχειρεί να προσπελάσει το ΕΣΠΣ ανακτά τα δεδομένα που παρέχει η ΜΔΧ με τη μορφή ιστοσελίδων μέσω της ΥΜΓΔ. Αυτό σημαίνει ότι κάθε αίτημα προσπέλασης ενεργοποιεί αυτή τη μονάδα και στην ουσία αλλάζει την κατάσταση των πληροφοριών που παρέχει όπως φαίνεται στο Σχήμα 6.

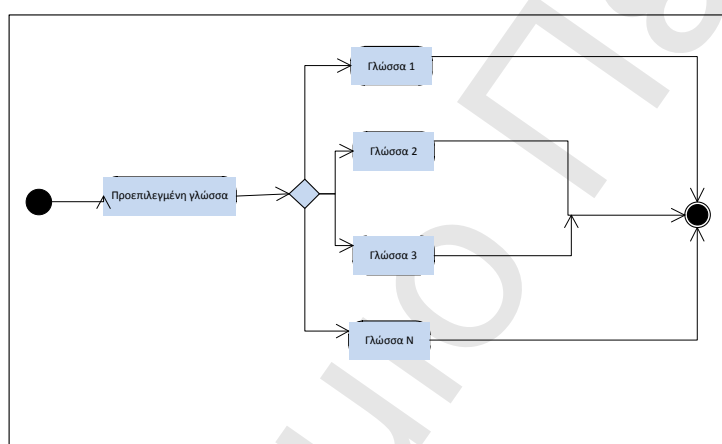


Σχήμα 6: Διάγραμμα Κατάστασης UML της ΜΔΧ

Όπως φαίνεται στο Σχήμα 6, ο χρήστης ζητά την ανάκτηση είτε δημόσιου και ελεύθερα προσπελάσιμου περιεχομένου, γεγονός το οποίο ενεργοποιεί την αντίστοιχη κατάσταση πληροφοριών της ΜΔΧ, είτε περιορισμένης πρόσβασης ιστοσελίδες οι οποίες απαιτούν την αυθεντικοποίηση του χρήστη. Το γεγονός

αυτό απεικονίζεται από την εξάρτηση της κατάστασης *Περιεχόμενο Περιορισμένης Πρόσβασης* με την κατάσταση *Αυθεντικοποιημένος Χρήστης* και είναι απαραίτητο χαρακτηριστικό του ΕΣΠΣ προκειμένου να αντιμετωπίζονται οι αδυναμίες των εφαρμογών Web 2.0.

Όσον αφορά στην ΥΜΠΓ η οποία είναι υπεύθυνη για τον γλωσσικό μετασχηματισμό του περιεχομένου ώστε να ικανοποιούνται βασικές απαιτήσεις των χρηστών όπως η ευχρηστία, η χρησιμότητα και η πολυγλωσσικότητα, όπως είναι φυσικό η κατάσταση των πληροφοριών που παρέχει καθορίζεται επίσης από τις επιλογές του χρήστη. Πιο συγκεκριμένα, το ΕΣΠΣ θα πρέπει να ενσωματώνει κατάλληλους μηχανισμούς μετατροπής του περιεχομένου της ΜΔΧ σε διαφορετικές γλώσσες ανάλογα με τις επιλογές των χρηστών. Η αλληλεξάρτηση αυτή απεικονίζεται στο Σχήμα 7.



Σχήμα 7: Διάγραμμα Κατάστασης UML της ΥΜΠΓ

Όπως φαίνεται στο Σχήμα 7, η αρχική κατάσταση πληροφορίας της ΥΜΠΓ είναι η προκαθορισμένη γλώσσα στην οποία εμφανίζονται οι γραφικές διεπαφές του ΕΣΠΣ ενώ η κατάσταση αυτή αλλάζει ανάλογα με την επιλογή του χρήστη σε οποιαδήποτε άλλη γλώσσα είναι διαθέσιμη στο σύστημα. Ακολουθώντας αυτή τη σχεδιαστική προσέγγιση παρέχεται ένας εύκολα διαχειρίσιμος, ευέλικτος και επεκτάσιμος μηχανισμός μετάφρασης του περιεχομένου σε όλο το εύρος των γραφικών διεπαφών του ΕΣΠΣ.

4.3.1.2 Μονάδα Επιχειρησιακών Διεργασιών

Η *Μονάδα Επιχειρησιακών Διεργασιών (ΜΕΔ)* θα μπορούσε να θεωρηθεί ως το πιο κρίσιμο συστατικό της *Κεντρικής Πλατφόρμας* καθώς αναλαμβάνει την υλοποίηση της επιχειρησιακής λογικής που είναι απαραίτητη για τις βασικές λειτουργίες του ΕΣΠΣ. Επιπρόσθετα, αυτή η μονάδα αναλαμβάνει το ρόλο του ενδιάμεσου μεταξύ της ΜΔΧ και της ΜΒΔ και διαχειρίζεται όλες τις αλληλεπιδράσεις μεταξύ τους. Ανάλογα με την εκάστοτε μελέτη εφαρμογής, η ΜΕΔ ενδέχεται να περιλαμβάνει ένα μεγάλο σε πλήθος αριθμό υπό-μονάδων ικανό να υποστηρίξει όλες τις επιμέρους βασικές λειτουργίες της *Κεντρικής Πλατφόρμας*. Λαμβάνοντας υπόψιν τις απαιτήσεις και τις τεχνικές

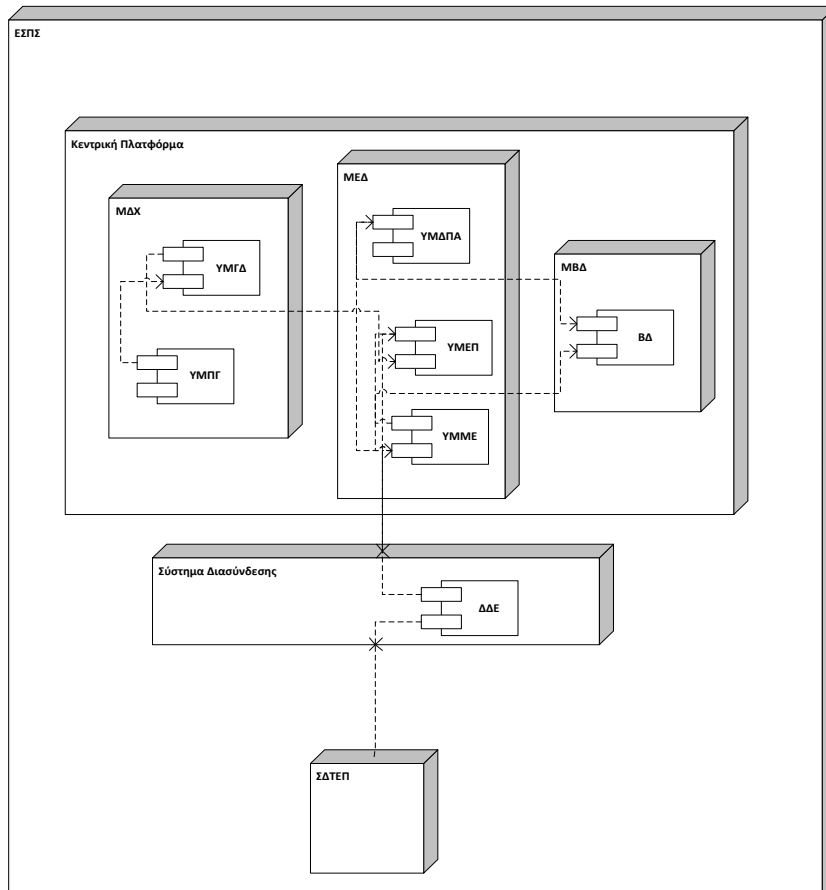
προδιαγραφές που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, η ΜΕΔ κάθε ΕΣΠΣ θα πρέπει να περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:

- *Υπό-Μονάδα Διαχείρισης Πληροφοριακών Αγαθών (ΥΜΔΠΑ)*, η οποία στην ουσία παρέχει τους απαραίτητους μηχανισμούς και λειτουργίες διαχείρισης του περιεχομένου και των πληροφοριακών αγαθών που αποθηκεύονται στις βάσεις δεδομένων του ΕΣΠΣ.
- *Υπό-Μονάδα Επιβολής Πολιτικών (ΥΜΕΠ)*, η οποία αναλαμβάνει την επιβολή των πολιτικών εξουσιοδότησης και του ελέγχου προσπέλασης με βάση την ανατροφοδότηση που λαμβάνει από το *Σύστημα Διαχείρισης Ταυτοτήτων* (βλ. ενότητα 4.3.2.1).
- *Υπό-Μονάδα Μετασχηματισμού και Ενσωμάτωσης (ΥΜΜΕ)*, η οποία είναι υπεύθυνη για τον κατάλληλο μετασχηματισμό των μηνυμάτων και των αιτήσεων που ανταλλάσσονται μεταξύ της *Κεντρικής Πλατφόρμας* και είτε των *Περιφερειακών Συστημάτων* είτε οποιασδήποτε άλλης εξωτερικής οντότητας μέσω του *Συστήματος Διασύνδεσης*.

Πριν περιγραφεί η ανάλυση της ΜΕΔ με βάση την *Υπολογιστική* και την *Πληροφοριακή Προσέγγιση* του προτύπου *RM-ODP* κρίνεται σκόπιμο να αναφερθεί ότι το σύνολο των υπομονάδων που περιλαμβάνει είναι αρκετό ώστε να διασφαλίσει την αποδοτική και αξιόπιστη εφαρμογή του ΕΣΠΣ. Παρόλα αυτά, ενδέχεται να περιλαμβάνει έναν κατά πολύ μεγαλύτερο αριθμό ώστε να ικανοποιούνται όλες οι λειτουργικές απαιτήσεις της *Κεντρικής Πλατφόρμας*.

4.3.1.2.1 Υπολογιστική προσέγγιση

Όπως προαναφέρθηκε, προκειμένου να ικανοποιούνται οι απαιτήσεις και οι τεχνικές προδιαγραφές που καθορίστηκαν στο Κεφάλαιο 3 αλλά και να διασφαλίζεται η εύρυθμη και ασφαλής λειτουργία του ΕΣΠΣ, η ΜΕΔ θα πρέπει κατ' ελάχιστον να περιλαμβάνει τις υπομονάδες που εμφανίζονται στο Σχήμα 8.



Σχήμα 8: Διάγραμμα UML της ΜΕΔ

Όπως φαίνεται στο Σχήμα 8, υπάρχουν ισχυρές αλληλεξαρτήσεις μεταξύ και των τριών βασικών υπομονάδων της ΜΕΔ. Αρχικά θα πρέπει να σημειωθεί ότι η οποιαδήποτε επέκταση της ΜΕΔ θα πρέπει απαραίτητα να περιλαμβάνει την αλληλεπίδραση των πρόσθετων υπομονάδων με την ΥΜΕΠ η οποία αποτελεί και το πιο κρίσιμο στοιχείο για την ασφαλή, έμπιστη και αξιόπιστη λειτουργία του ΕΣΠΣ.

Η Υπό-Μονάδα Διαχείρισης Πληροφοριακών Αγαθών (ΥΜΔΠΑ) αναλαμβάνει την ολοκλήρωση όλων των απαραίτητων μηχανισμών για την ταξινόμηση και τη διαχείριση του περιεχομένου και των πληροφοριακών αγαθών που αποθηκεύονται στη ΜΒΔ (βλ. ενότητα 4.3.1.3). Σε κάθε ΕΣΠΣ και ιδιαίτερα σε αυτά που υπάρχει αυξημένη ανάγκη συλλογής, αναζήτησης και διαχείρισης μεγάλου όγκου πληροφοριών, ηλεκτρονικών εγγράφων ή οποιουδήποτε άλλου τύπου ψηφιακού περιεχομένου, η ΥΜΔΠΑ θα πρέπει να περιλαμβάνει και να παρέχει τις ακόλουθες δυνατότητες:

- Ταξονομίες περιεχομένου των πληροφοριακών αγαθών που αποθηκεύονται στην ηλεκτρονική βιβλιοθήκη ώστε να κατηγοριοποιούνται ανάλογα με τις εκάστοτε απαιτήσεις.
- Προηγμένες διεπαφές με διαδραστικές δυνατότητες οι οποίες θα διευκολύνουν τους χρήστες να συνεισφέρουν, να αναζητούν και να

διαχειρίζονται εύκολα και αποδοτικά τα πληροφοριακά αγαθά του ΕΣΠΣ. Σημειώνεται ότι αν και οι διεπαφές χρήστη ολοκληρώνονται τελικά στη ΜΔΧ, ο σχεδιασμός και η τελική υλοποίησή τους θα πρέπει να είναι πλήρως εναρμονισμένοι με την ΥΜΔΠΑ η οποία στην ουσία θα ενσωματώνει και όλη την επιχειρησιακή λογική.

- Προηγμένες μηχανές αναζήτησης και δυνατότητες δυναμικής ανάκτησης περιεχομένου και πληροφοριακών αγαθών σχετικών με τις απαιτήσεις της εκάστοτε μελέτης εφαρμογής.

Όπως απεικονίζεται στο Σχήμα 8, είναι προφανής η ισχυρή αλληλεξάρτηση της ΥΜΔΠΑ τόσο με την ΜΔΧ όσο και με την ΜΒΔ. Παρά το γεγονός ότι η βασική λειτουργικότητα υλοποιείται σαν ξεχωριστή υπομονάδα στη ΜΕΔ, εξίσου σημαντική και απαραίτητη είναι και η συνεισφορά των υπολοίπων μονάδων της αρχιτεκτονικής: η ΜΔΧ για να παρέχει φιλικούς προς το χρήστη τρόπους αλληλεπίδρασης οι οποίοι ικανοποιούν τις απαιτήσεις που παρουσιάστηκαν στην ενότητα 3.2.1, και η ΜΒΔ για να αναλαμβάνει την ασφαλή και αποδοτική αποθήκευση και διαχείριση των δεδομένων. Αυτό είναι και ένα χαρακτηριστικό παράδειγμα που αναδεικνύει τα πλεονεκτήματα και τα κρίσιμα οφέλη που προκύπτουν από την υιοθέτηση των βασικών αρχών σχεδιασμού, όπως παρουσιάστηκαν στην ενότητα 4.2.

Ο βασικός και πολύ κρίσιμος για την ασφαλή λειτουργία του ΕΣΠΣ ρόλος της *Υπό-Μονάδας Επιβολής Πολιτικών (ΥΜΕΠ)* είναι να αναλαμβάνει την απόδοση προνομίων προσπέλασης με βάση τις αποφάσεις που λαμβάνονται από το *Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης* (βλ. ενότητα 4.3.2.1). Πιο συγκεκριμένα, κάθε φορά που ο χρήστης αιτείται να προσπελάσει κάποια από τις υπηρεσίες ή λειτουργίες του ΕΣΠΣ, η ΥΜΕΠ αναλαμβάνει την ανταλλαγή δεδομένων ασφάλειας με το ΣΔΤΕΠ ώστε να πληροφορηθεί την απόφαση εξουσιοδότησης που αντιστοιχεί στο συγκεκριμένο αίτημα και στη συνέχεια να επιβάλλει τη σχετική πολιτική, σε συνεργασία με τη ΜΔΧ.

Ειδικότερα, τη στιγμή που κάποιος χρήστης επισκέπτεται την πλατφόρμα του ΕΣΠΣ, η ΥΜΕΠ ενεργοποιείται και δίνει εντολή στη ΜΔΧ να παράσχει τις αντίστοιχες ιστοσελίδες. Σε περίπτωση που ο χρήστης αυθεντικοποιηθεί με επιτυχία, η ΥΜΕΠ ενεργοποιείται και πάλι, και είναι στην ουσία υπεύθυνη για την εμφάνιση στον τελικό χρήστη όλων των υπηρεσιών και διαθέσιμων λειτουργιών που ορίζει η πολιτική εξουσιοδότησης η οποία εφαρμόστηκε από το ΣΔΤΕΠ.

Αν και περισσότερες λεπτομέρειες για τον τρόπο λειτουργίας αυτής της υπομονάδας, αλλά και ολόκληρου του ΣΔΤΕΠ, παρουσιάζονται αναλυτικά τόσο στην ενότητα 4.3.2.1 όσο και στο Κεφάλαιο 6, αξίζει σε αυτό το σημείο να αναφερθεί ότι δεδομένου του ότι όλες οι αλληλεπιδράσεις μεταξύ της ΥΜΕΠ και του ΣΔΤΕΠ λαμβάνουν χώρα μέσω του *Συστήματος Διασύνδεσης*, για το λόγο αυτό υπάρχει ισχυρή αλληλεξάρτηση μεταξύ της ΥΜΕΠ και της ΥΜΜΕ, έτσι

ώστε τα δεδομένα να μετατρέπονται στην κατάλληλη μορφή και να ενσωματώνονται σε ασφαλή μηνύματα επικοινωνίας.

Η *Υπό-Μονάδα Μετασχηματισμού και Ενσωμάτωσης (ΥΜΜΕ)* είναι αυτή που επιτρέπει την αποτελεσματική και αξιόπιστη αλληλεπίδραση μεταξύ των διαφορετικών μονάδων και των συστημάτων που ολοκληρώνονται στο ΕΣΠΣ. Λαμβάνοντας υπόψιν την απαραίτητη χρήση του *Συστήματος Διασύνδεσης* ώστε να επιτυγχάνεται η επικοινωνία μεταξύ των ετερογενών συστημάτων και εφαρμογών, η ΥΜΜΕ αναλαμβάνει την κατάλληλη μετατροπή των δεδομένων και την επιτυχή προσαρμογή τους σε ασφαλή μηνύματα επικοινωνίας τα οποία μεταδίδονται από και προς την *Κεντρική Πλατφόρμα*. Πιο συγκεκριμένα η ΥΜΜΕ παρέχει τις ακόλουθες λειτουργίες:

- Το μετασχηματισμό των δεδομένων και τη δημιουργία των μηνυμάτων που αποστέλλονται από την *Κεντρική Πλατφόρμα* σε κάθε άλλο σύστημα, εφαρμογή ή εξωτερική οντότητα του συνεργατικού περιβάλλοντος μέσω του ΔΔΕ.
- Την επεξεργασία και διαχείριση των μηνυμάτων που λαμβάνονται από τον ΔΔΕ και προέρχονται από άλλα συστήματα ή εξωτερικές του ΕΣΠΣ οντότητες.

Επίσης, εκτός του ότι διαχειρίζεται όλα τα μηνύματα Υπηρεσιών Ιστού που απαιτούνται για την αποδοτική και ασφαλή λειτουργία του ΕΣΠΣ, η ΥΜΜΕ παρουσιάζει ισχυρή αλληλεξάρτηση με την ΥΜΕΠ την οποία στην ουσία τροφοδοτεί με όλα τα απαραίτητα δεδομένα ασφάλειας. Το ίδιο ισχύει και για την επικοινωνία της ΥΕΔ με την ΥΒΔ, καθώς η ΥΜΕΕ διαχειρίζεται παράλληλα και όλα τα μηνύματα που ανταλλάσσονται μεταξύ των διαφόρων μονάδων της Κεντρικής Πλατφόρμας. Με άλλα λόγια, η ΥΜΜΕ θα μπορούσε εύστοχα να χαρακτηριστεί ως μια εσωτερική μονάδα διασύνδεσης η οποία ελέγχει και διαχειρίζεται κάθε επικοινωνία εντός και εκτός της *Κεντρικής Πλατφόρμας* του ΕΣΠΣ.

4.3.1.2.2 Πληροφοριακή προσέγγιση

Λαμβάνοντας υπόψιν το γεγονός ότι η ΜΕΔ είναι υπεύθυνη για τη διαχείριση της επιχειρησιακής λογικής του ΕΣΠΣ, γίνεται προφανής ο ρόλος της και στη διαχείριση των πληροφοριών και δεδομένων που διέρχονται μεταξύ:

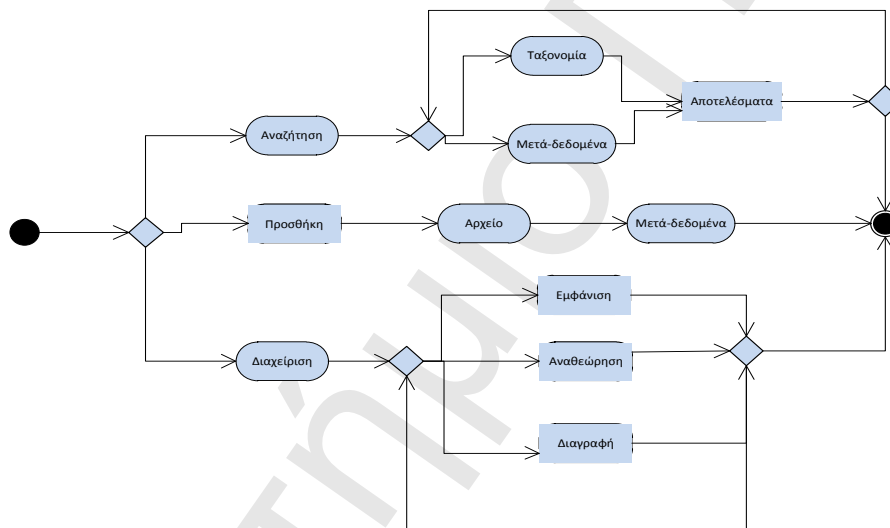
1. των υπομονάδων που ενσωματώνει και των υπόλοιπων μονάδων της *Κεντρικής Πλατφόρμας*, καθώς και
2. μεταξύ της *Κεντρικής Πλατφόρμας* και των *Περιφερειακών Συστημάτων* που συνδέονται στο *Σύστημα Διασύνδεσης*.

Στη συνέχεια της ενότητας περιγράφεται η *Πληροφοριακή Προσέγγιση* του προτύπου *RM-ODP* για κάθε μια από τις υπομονάδες της ΜΕΔ χρησιμοποιώντας *Διαγράμματα Κατάστασης UML* και *Διαγράμματα Ροής*.

Η ΥΜΔΠΑ παρέχει όλες τις απαραίτητες λειτουργίες διαχείρισης περιεχομένου της Κεντρικής Πλατφόρμας. Τα δεδομένα που γίνονται αντικείμενο επεξεργασίας και διαχείρισης συνοψίζονται στα ακόλουθα:

- Ταξονομίες περιεχομένου οι οποίες απεικονίζονται και αποθηκεύονται ως αρχεία XML.
- Ψηφιακά αρχεία κάθε τύπου, όπως ηλεκτρονικά έγγραφα, υπερσύνδεσμοι, εικόνες, βίντεο κ.ά., ανάλογα με τις ανάγκες και απαιτήσεις της εκάστοτε μελέτης εφαρμογής.
- Μετά-δεδομένα τα οποία περιγράφουν με περισσότερη λεπτομέρεια τα πληροφοριακά αγαθά ώστε να γίνεται πιο εύκολη και αποδοτική η αναζήτηση και η αλληλοσυσχέτιση των πληροφοριών.

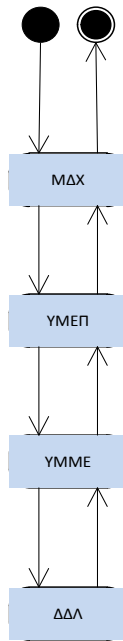
Στο Σχήμα 9 απεικονίζονται οι βασικές καταστάσεις κάθε πληροφοριακού αγαθού που αποθηκεύεται στην ηλεκτρονική βιβλιοθήκη του ΕΣΠΣ.



Σχήμα 9: Διάγραμμα Κατάστασης UML της ΥΜΔΠΑ

Όπως φαίνεται στο Σχήμα 9, οι διάφορες καταστάσεις ενεργοποιούνται από τις τρεις βασικές λειτουργίες της ΥΜΔΠΑ, την προσθήκη, την αναζήτηση και τη διαχείριση πληροφοριακών αγαθών.

Όσον αφορά στην ΥΜΕΠ, δεδομένου ότι αναλαμβάνει την επεξεργασία, τον έλεγχο και την τελική επιβολή των πολιτικών εξουσιοδότησης, ελέγχου προσπέλασης και προστασίας της ιδιωτικότητας (βλ ενότητα 4.3.2.1) εντός της Κεντρικής Πλατφόρμας, είναι απαραίτητη η συχνή επικοινωνία και ανταλλαγή πληροφοριών και δεδομένων ασφάλειας με το ΣΔΤΕΠ μέσω του Συστήματος Διασύνδεσης. Παρόλα αυτά, όπως προαναφέρθηκε, η επικοινωνία αυτή δε γίνεται απευθείας αλλά μέσω της αλληλεπίδρασης της ΥΜΕΠ με την ΥΜΜΕ όπως φαίνεται και στο Σχήμα 10.



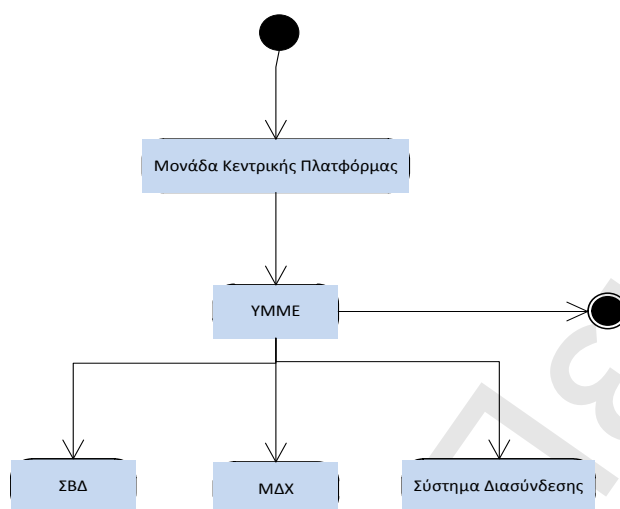
Σχήμα 10: Διάγραμμα Κατάστασης UML της YMEΠ

Όπως φαίνεται στο Σχήμα 10, η YMEΠ επεξεργάζεται τις αιτήσεις εξουσιοδότησης που λαμβάνονται από τη MΔΧ και προωθεί τα απαραίτητα δεδομένα ασφάλειας στην YΜΜΕ, προκειμένου η τελευταία να τα ενσωματώσει σε ασφαλή μηνύματα SOAP, τα οποία με τη σειρά τους θα μεταφερθούν στο ΣΔΤΕΠ μέσω του *Συστήματος Διασύνδεσης*. Η ίδια ροή πληροφορίας ακολουθείται και στην αντίθετη περίπτωση κατά την οποία το ΣΔΤΕΠ απαντά μέσω του *Συστήματος Διασύνδεσης* στην YΜΜΕ και η τελευταία είναι με τη σειρά της υπεύθυνη να μετασχηματίσει κατάλληλα τα δεδομένα που έλαβε και να τα προωθήσει στην YMEΠ προκειμένου να αναλάβει τις κατάλληλες δράσεις για την επιβολή των αποφάσεων εξουσιοδότησης και ελέγχου προσπέλασης.

Τέλος, η YΜΜΕ είναι υπεύθυνη για τον μετασχηματισμό των δεδομένων και την προσαρμογή τους στα μηνύματα που μεταδίδονται εντός και εκτός της ΜΕΔ. Στην ουσία λειτουργεί ως ενδιάμεσος μεταξύ των υπολοίπων μονάδων και υπομονάδων της *Κεντρικής Πλατφόρμας* και του ΔΔΕ του *Συστήματος Διασύνδεσης*.

Όπως φαίνεται στο Σχήμα 11, η YΜΜΕ δεν εμφανίζει κάποια προκαθορισμένη κατάσταση όσον αφορά στις πληροφορίες που διαχειρίζεται. Αντίθετα, θα μπορούσε να χαρακτηριστεί ως η μονάδα η οποία έχει μόνιμη αρμοδιότητα τη μετατροπή της κατάστασης όλων των πληροφοριών που λαμβάνονται από και προς τις υπόλοιπες μονάδες και υπομονάδες της *Κεντρικής Πλατφόρμας*. Για παράδειγμα, η YΜΜΕ λαμβάνει αιτήσεις από κάποια εσωτερική υπομονάδα της ΜΕΔ και ύστερα από τους κατάλληλους μετασχηματισμούς την προωθεί στις Μονάδες της *Κεντρικής Πλατφόρμας* ή στο *Σύστημα Διασύνδεσης*. Στη συνέχεια, αφού λάβει τις αντίστοιχες απαντήσεις, προσαρμόζει τα δεδομένα στην

κατάλληλη κάθε φορά μορφή και προωθεί τις κατάλληλες πληροφορίες στις κατάλληλες μονάδες ή υπομονάδες της Κεντρικής Πλατφόρμας.



Σχήμα 11: Διάγραμμα Κατάστασης UML της ΥΜΜΕ

Χαρακτηριστικά αναφέρεται ότι ως πιθανές καταστάσεις της πληροφορίας που διαχειρίζεται η ΥΜΜΕ θα μπορούσαν να αναφερθούν τα μηνύματα SOAP με ή χωρίς μηχανισμούς ασφάλειας ενσωματωμένους στην επικεφαλίδα του μηνύματος (βλ. Κεφάλαιο 5), επερωτήσεις στη βάση δεδομένων όταν πρόκειται για επικοινωνία μεταξύ της ΥΜΔΠΑ και της ΜΒΔ ή δυναμικές ιστοσελίδες όταν η ΥΜΜΕ μεσολαβεί για την αλληλεπίδραση μεταξύ της ΜΔΧ και της ΜΒΔ.

4.3.1.3 Μονάδα Βάσεων Δεδομένων

Σε αυτό το τρίτο επίπεδο της αρχιτεκτονικής ολοκληρώνονται οι βάσεις δεδομένων που χρησιμοποιεί το ΕΣΠΣ και οι οποίες αναλαμβάνουν την αποθήκευση και τη διαχείριση όλου του περιεχομένου και των πληροφοριακών αγαθών της *Κεντρικής Πλατφόρμας*. Σε κάθε περίπτωση που απαιτείται να συνδεθεί ένα *Περιφερειακό Σύστημα* με την κεντρική βάση δεδομένων αυτό επιτυγχάνεται μέσω του *Συστήματος Διασύνδεσης* χρησιμοποιώντας την *ΥΜΜΠ* της *ΜΕΔ*. Με τον τρόπο αυτό δεν επιτρέπεται η απευθείας σύνδεση με τη βάση δεδομένων ώστε να εξασφαλίζονται τα απαραίτητα επίπεδα ασφάλειας και προστασίας της ιδιωτικότητας (βλ. Κεφάλαιο 5). Επίσης καθίσταται πιο αποδοτική η διαχείριση και η παρακολούθηση των αλληλεπιδράσεων με τις βάσεις δεδομένων, είτε αυτές προέρχονται εσωτερικά από τις μονάδες της *Κεντρικής Πλατφόρμας* είτε από κάποιο *Περιφερειακό ή Εξωτερικό Σύστημα*.

Όσον αφορά στην *Πληροφοριακή Όψη* του προτύπου RM-ODP για τη ΜΒΔ, αν και αποτελεί τη σημαντικότερη προσέγγιση ανάλυσης δεδομένης της άμεσης συσχέτισης της ΜΒΔ με τα πληροφοριακά αγαθά, δεν είναι εφικτός ο καθορισμός ενός γενικευμένου και εύκολα προσαρμόσιμου μοντέλου. Η *Πληροφοριακή Προσέγγιση* της ΜΒΔ για κάθε ΕΣΠΣ ορίζεται με σαφή και

συγκεκριμένο τρόπο από το σχήμα της Βάσης Δεδομένων που χρησιμοποιείται για να καλύψει τις ανάγκες της εκάστοτε μελέτης εφαρμογής.

4.3.2 Περιφερειακά Συστήματα

Όπως έχει ήδη αναφερθεί, στα πλαίσια του ΕΣΠΣ απαιτείται η επιτυχημένη και αποτελεσματική ολοκλήρωση πολυάριθμων συστημάτων, εφαρμογών και εργαλείων λογισμικού προκειμένου τελικά να προκύψει ένα αποδοτικό και αξιόπιστο περιβάλλον παροχής ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

Οποσδήποτε ο σαφής καθορισμός των εκάστοτε συστημάτων και τεχνολογιών οι οποίες κρίνεται απαραίτητο να ενσωματωθούν στο ΕΣΠΣ εξαρτάται από τις ανάγκες και τους περιορισμούς της εκάστοτε μελέτης εφαρμογής, παρόλα αυτά εξ' ορισμού, το αρχιτεκτονικό σχέδιο του ΕΣΠΣ θα πρέπει κατ' ελάχιστο να περιλαμβάνει τα ακόλουθα συστήματα:

- *Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης*, για την ασφαλή διαχείριση των προσωπικών δεδομένων των χρηστών και την προστασία της ιδιωτικότητας, παρέχοντας κατάλληλους μηχανισμούς απόδοσης προνομίων προσπέλασης.
- *Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης (ΣΣΚΑ)*, το οποίο παρέχει τη δυνατότητα συνεργασίας, ανταλλαγής απόψεων και δυναμικής δημιουργίας περιεχομένου.
- *Σύστημα Μοντελοποίησης Διαδικασιών και Εναρμόνισης Πολιτικών (ΣΜΔΕΠ)*, προκειμένου να είναι δυνατή η γραφική απεικόνιση διαδικασιών και μοντέλων πολιτικών καθώς και η ανάλυση και η σύγκρισή τους με τη συνεισφορά των ίδιων των χρηστών.

Στις ακόλουθες ενότητες παρουσιάζεται η ανάλυση της Υπολογιστικής και της Πληροφοριακής Προσέγγισης του προτύπου RM-ODP για καθένα από τα συστήματα αυτά.

4.3.2.1 Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης

Στα πλαίσια του ΕΣΠΣ και, ιδιαίτερα, όταν πρόκειται για την εφαρμογή του σε τομείς με υψηλές απαιτήσεις ασφάλειας και ιδιωτικότητας, όπως για παράδειγμα αυτός της ηλεκτρονικής Διακυβέρνησης [8], όλες οι αλληλεπιδράσεις που λαμβάνουν χώρα εκ μέρους των χρηστών καθώς και η διασύνδεση των ετερογενών συστημάτων και εφαρμογών θα πρέπει να διαχειρίζονται έτσι ώστε να διασφαλίζεται τόσο η εμπιστευτικότητα των δεδομένων όσο και η προστασία της ιδιωτικότητας των χρηστών.

Όπως περιγράφεται εκτενέστερα στο επόμενο κεφάλαιο της διατριβής, εκτός από τις αναγνωρισμένες απειλές των τεχνολογιών Web 2.0, στα πλαίσια εφαρμογής του ΕΣΠΣ απαιτείται η προστασία της ιδιωτικότητας να ικανοποιεί

τις νέες απαιτήσεις που τίθενται από τις δυνατότητες συνεργασίας και αλληλεπίδρασης μεταξύ των χρηστών [7]. Στο έκτο κεφάλαιο προτείνεται μια καινοτόμο λύση διαχείρισης ταυτοτήτων η οποία βασίζεται στη λειτουργία ενός *Συστήματος Διαχείριση Αξιοπιστίας (ΣΔΑ)*, προκειμένου να υποστηρίζεται ο δυναμικός έλεγχος προσπέλασης ανάλογα με το βαθμό στον οποίο οι ενέργειες κάθε χρήστη σέβονται την ιδιωτικότητα των υπολοίπων χρηστών που συμμετέχουν στο σύστημα.

Παρά το γεγονός ότι λόγω της κρισιμότητας και του ερευνητικού ενδιαφέροντος που παρουσιάζει το ΣΔΤΕΠ αναλύεται με περισσότερη λεπτομέρεια σε ξεχωριστό κεφάλαιο, η γενική περιγραφή του στο πλαίσιο της παρούσας ενότητας κρίνεται εξίσου σημαντική και χρήσιμη προκειμένου να καθοριστούν σε υψηλό επίπεδο οι αρμοδιότητές του, οι βασικές μονάδες από τις οποίες αποτελείται καθώς και το είδος των πληροφοριών που διαχειρίζεται.

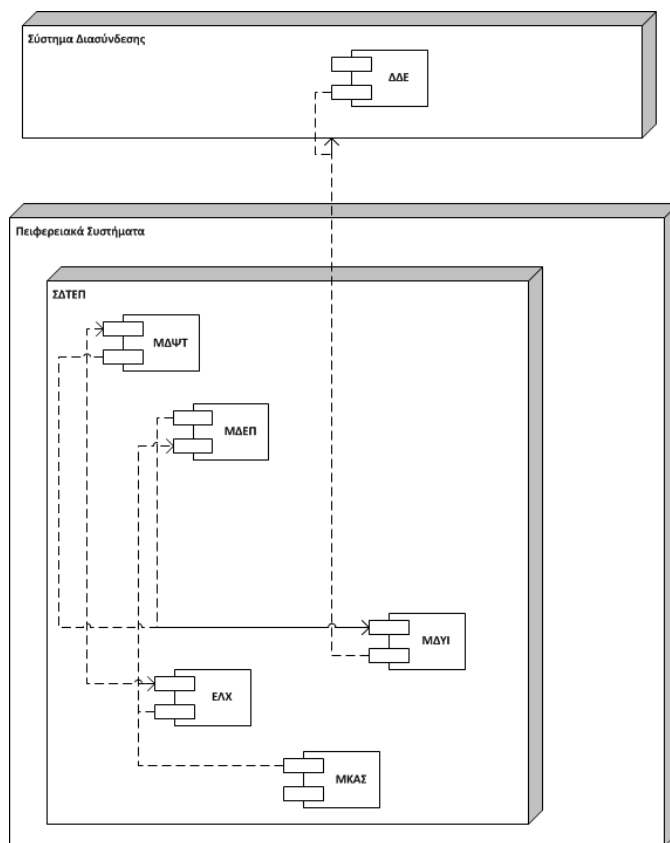
Με βάση τα αποτελέσματα της διατριβής, το ΣΔΤΕΠ του ΕΣΠΣ θα μπορούσε να χαρακτηριστεί ως ένα καινοτόμο σύστημα διαχείρισης ταυτοτήτων το οποίο βασίζεται στην αρχιτεκτονική της *Κεντρικοποιημένης Ομοσπονδίας (centralized federation)* και υποστηρίζει τη δυναμική απόδοση προνομίων προσπέλασης στις υπηρεσίες Web 2.0 (βλ. ενότητα 6.3).

Σημαντικό είναι επίσης το γεγονός ότι με βάση την αρχιτεκτονική του ΕΣΠΣ αλλά και του ίδιου του ΣΔΤΕΠ, όλες οι ανταλλαγές δεδομένων και αλληλεπιδράσεις μεταξύ της Κεντρικής Πλατφόρμας και αυτού επιτυγχάνονται μέσω του *Συστήματος Διασύνδεσης*, οι οποίες βασίζονται στην τεχνολογία των Υπηρεσιών Ιστού (βλ. ενότητα 4.3.3). Έτσι είναι δυνατή η διασύνδεση του ΣΔΤΕΠ με οποιοδήποτε άλλο σύστημα και πλατφόρμα με διαλειτουργικό τρόπο, χωρίς να απαιτείται επανασχεδιασμός των συστημάτων.

4.3.2.1.1 Υπολογιστική προσέγγιση

Όπως φαίνεται και στο Σχήμα 12 το ΣΔΤΕΠ περιλαμβάνει πέντε (5) βασικές λειτουργικές μονάδες:

- *Μονάδα Διαχείρισης Ψηφιακών Ταυτοτήτων (ΜΔΨΤ)*
- *Μονάδα Διαχείρισης και Επιβολής Πολιτικών (ΜΔΕΠ)*
- *Μονάδα Καταγραφής και Αξιολόγησης Συμπεριφοράς (ΜΚΑΣ)*
- *Μονάδα Διαχείρισης Υπηρεσιών Ιστού (ΜΔΥΙ)*
- *Ευρετήριο Λογαριασμών Χρήστη (ΕΛΧ).*



Σχήμα 12: Διάγραμμα UML των Μονάδων του ΣΔΤΕΠ

Όπως φαίνεται στο Σχήμα 12, η ΜΔΕΠ και η ΜΚΑΣ παρουσιάζουν υψηλά επίπεδα εξάρτησης καθώς, όπως περιγράφεται στο έκτο κεφάλαιο, αποτελούν τις βασικές μονάδες του *Συστήματος Διαχείρισης Αξιοπιστίας* που ενσωματώνει το ΣΔΤΕΠ και διασυνδέονται με την ΜΔΨΤ προκειμένου να υλοποιούν αποτελεσματικά τους απαραίτητους μηχανισμούς αυθεντικοποίησης και απόδοσης προνομίων προσπέλασης.

Το ΕΛΧ μπορεί να αποτελείται είτε από μια ασφαλή βάση δεδομένων είτε από ένα κατάλληλα σχεδιασμένο και προστατευμένο ευρετήριο LDAP, όπου θα αποθηκεύονται τα προσωπικά στοιχεία των χρηστών, τα διαπιστευτήρια εξουσιοδότησης, οι πολιτικές ελέγχου προσπέλασης και προστασίας της ιδιωτικότητας, καθώς και οποιαδήποτε άλλη πληροφορία ασφάλειας απαιτείται για την αξιόπιστη και έμπιστη λειτουργία του ΕΣΠΣ. Τα διαβαθμισμένα πληροφορικά αγαθά του ΕΛΧ είναι διαθέσιμα μόνο στην ΜΔΨΤ και στην ΜΔΕΠ, οι οποίες και αναλαμβάνουν την περαιτέρω επεξεργασία και χρήση τους.

Επίσης, Η ΜΔΥΙ θα μπορούσε να θεωρηθεί ως μια εξίσου κρίσιμη μονάδα καθώς είναι υπεύθυνη για την επικοινωνία με την *Κεντρική Πλατφόρμα* και τα *Περιφερειακά Συστήματα* ώστε να παρέχει τις απαραίτητες υπηρεσίες ασφάλειας ήτοι, εγγραφή, αυθεντικοποίηση και εξουσιοδότηση, στους τελικούς χρήστες.

Πιο συγκεκριμένα, η ΜΔΨΤ έχει σαν βασικές αρμοδιότητες την:

- Δημιουργία, επεξεργασία και διαχείριση των ομάδων χρηστών και των ψηφιακών τους ταυτοτήτων.
- Επικοινωνία και ανταλλαγή πληροφοριών με το ΕΛΧ.
- Αλληλεπίδραση με τη ΜΔΥΙ προκειμένου να ανταλλάσσονται δεδομένα αυθεντικοποίησης και εξουσιοδότησης τόσο με την *Κεντρική Πλατφόρμα* όσο και με τα *Περιφερειακά Συστήματα*, όταν αυτό είναι απαραίτητο.

Κάθε χρήστης που εγγράφεται στο σύστημα αλληλεπιδρά με τη ΜΔΨΤ προκειμένου η τελευταία να εξασφαλίσει την ασφαλή καταχώριση όλων των απαραίτητων δεδομένων στο ΕΛΧ και να συνδέσει το λογαριασμό του εκάστοτε χρήστη με την κατάλληλη ομάδα χρηστών.

Η ΜΔΕΠ είναι υπεύθυνη για τη δημιουργία, τη διαχείριση και την επιβολή των πολιτικών εξουσιοδότησης οι οποίες στην ουσία ορίζουν τα δικαιώματα προσπέλασης που έχει ο εκάστοτε χρήστης ή ομάδα χρηστών στις παρεχόμενες υπηρεσίες και εφαρμογές του ΕΣΠΣ. Κρίσιμης σημασίας είναι η ισχυρή εξάρτηση της ΜΔΕΠ από τη ΜΔΥΙ καθώς με την αποτελεσματική τους συνεργασία επιτυγχάνεται η επιβολή και διαπραγμάτευση των πολιτικών εξουσιοδότησης σε εξωτερικά του ΕΣΠΣ συστήματα, τα οποία, αν και ετερογενή, επιβάλλεται να ολοκληρωθούν αρμονικά στο ενιαίο συνεργατικό περιβάλλον.

Η ΜΚΑΣ έχει σαν βασικό στόχο την προστασία της ιδιωτικότητας των χρηστών μέσω της αξιολόγησης της συμπεριφοράς τους στα πλαίσια λειτουργίας του συνεργατικού περιβάλλοντος. Για να επιτευχθεί αυτό, ενσωματώνει ένα κατάλληλα σχεδιασμένο ΣΔΑ το οποίο παρέχει τους απαραίτητους μηχανισμούς καταγραφής αναφορών κακόβουλου περιεχομένου και υλοποιεί τη μέθοδο υπολογισμού του βαθμού αξιοπιστίας των χρηστών που παρουσιάζεται στο 6^ο Κεφάλαιο προκειμένου να αξιολογεί με δυναμικό τρόπο την απόδοση προνομίων προσπέλασης στις διαδραστικές εφαρμογές Web 2.0.

Η ΜΔΥΙ επικεντρώνεται στη διαχείριση των επικοινωνιών μεταξύ του ΣΔΤΕΠ και των περιφερειακών συστημάτων. Παρέχει διεπαφές Υπηρεσιών Ιστού, οι οποίες τοποθετούνται πάνω από τις λειτουργίες που παρέχουν οι ΜΔΕΠ, ΜΔΨΤ και ΜΚΑΣ, ώστε να υποστηρίζονται όλες οι αναγκαίες αλληλεπιδράσεις που απαιτούνται για την αποτελεσματική και ασφαλή διαχείριση ταυτοτήτων και ελέγχου προσπέλασης. Οι διεπαφές αυτές αφορούν σε:

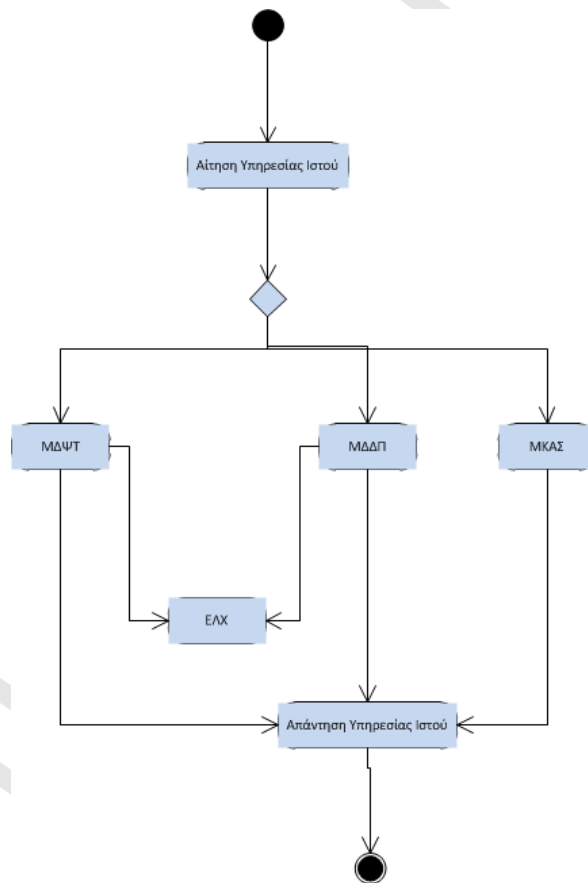
- *Υπηρεσίες Εγγραφής*, οι οποίες επιτρέπουν την εγγραφή νέων χρηστών στο ΕΣΠΣ.
- *Υπηρεσίες Αυθεντικοποίησης*, οι οποίες αναλαμβάνουν την επικοινωνία μεταξύ της ΜΔΨΤ και της Κεντρικής Πλατφόρμας ώστε να αυθεντικοποιούνται οι εγγεγραμμένοι χρήστες.
- *Υπηρεσίες Εξουσιοδότησης*, οι οποίες έχουν σαν βασική αρμοδιότητα την επικοινωνία της ΜΔΕΠ με την Κεντρική Πλατφόρμα ώστε ο έλεγχος

προσπέλασης να επιτυγχάνεται με βάση τα έγκυρα δικαιώματα προσπέλασης των χρηστών.

Τέλος, το ΕΛΧ είναι μια μονάδα αποθήκευσης η οποία θα πρέπει να λειτουργεί ως ένα ασφαλές αποθετήριο των προσωπικών δεδομένων, των πολιτικών ελέγχου προσπέλασης και εξουσιοδότησης, καθώς και των πολιτικών προστασίας της ιδιωτικότητας. Βασίζεται είτε σε κάποια ασφαλή και κατάλληλα σχεδιασμένη βάση δεδομένων είτε σε κάποιο ευρετήριο LDAP, ανάλογα με τις ανάγκες και τις απαιτήσεις της εκάστοτε μελέτης εφαρμογής. Το ΕΛΧ χαρακτηρίζεται από ισχυρές αλληλο-εξαρτήσεις με τη ΜΔΨΤ και τη ΜΔΕΠ.

4.3.2.1.2 Πληροφοριακή προσέγγιση

Αναλύοντας σε αυτή την ενότητα την πληροφοριακή προσέγγιση του ΣΔΤΕΠ, το Σχήμα 13 παρουσιάζει τον τρόπο με τον οποίο διακινούνται οι πληροφορίες ασφάλειας μεταξύ των βασικών του μονάδων.



Σχήμα 13: Διάγραμμα Ροής Πληροφοριών UML του ΣΔΤΕΠ

Όπως φαίνεται και στο Σχήμα 13, το ΣΔΤΕΠ δέχεται τις αιτήσεις που προκύπτουν από τις ενέργειες των χρηστών στη ΜΔΥΙ, η οποία είναι υπεύθυνη για την επεξεργασία τους και την προώθηση των κατάλληλων δεδομένων (τα οποία εξάγονται από τα μηνύματα SOAP) στις υπόλοιπες μονάδες του συστήματος. Ειδικότερα, προκειμένου να επιτευχθεί η αυθεντικοποίηση των

χρηστών η ΜΔΥΙ προωθεί τα δεδομένα ασφάλειας στη ΜΔΨΤ η οποία και κάνει τους απαραίτητους ελέγχους με το ΕΛΧ. Σε περίπτωση που είναι έγκυρα, η ΜΔΨΤ επικοινωνεί με τη ΜΚΑΣ προκειμένου να ανακτηθεί ο βαθμός αξιοπιστίας των χρηστών και να δημιουργηθούν τα κατάλληλα διαπιστευτήρια ασφάλειας τα οποία στη συνέχεια μεταφέρονται στη ΜΔΥΙ προκειμένου η τελευταία να τα προωθήσει στην οντότητα από την οποία έλαβε τη σχετική αίτηση αυθεντικοποίησης.

Επίσης, η ΜΔΥΙ, όταν είναι απαραίτητο, επικοινωνεί με τη ΜΔΕΠ προκειμένου να λάβει μια απάντηση ελέγχου προσπέλασης στους πόρους του ΕΣΠΣ ανάλογα με τα δικαιώματα του χρήστη. Για να επιτευχθεί αυτό, η ΜΔΕΠ λαμβάνει τα διαπιστευτήρια ασφάλειας που προωθούνται από τη ΜΔΥΙ μαζί με το αναγνωριστικό του πόρου που ο χρήστης αιτείται να προσπελάσει και, ύστερα από τους κατάλληλους ελέγχους με τη ΜΚΑΣ και το ΕΛΧ, δημιουργεί τα διαπιστευτήρια εξουσιοδότησης τα οποία και προωθούνται στη ΜΔΥΙ προκειμένου να ενσωματωθούν στα μηνύματα SOAP που θα σταλούν ως απάντηση στην αρχική αίτηση προσπέλασης.

Πιο συγκεκριμένα, η ΜΔΨΤ διαχειρίζεται τις πληροφορίες και τα δεδομένα που αφορούν στις ψηφιακές ταυτότητες των χρηστών και τα διαπιστευτήρια εξουσιοδότησης, συμπεριλαμβανομένου του ρόλου ή της ομάδας χρηστών του κάθε χρήστη, καθώς και του βαθμού αξιοπιστίας που χαρακτηρίζει τη συμπεριφορά του στα πλαίσια του συνεργατικού περιβάλλοντος (βλ. Κεφάλαιο 6). Επίσης είναι υπεύθυνη για τη δημιουργία νέων λογαριασμών χρηστών, καθώς και για την επεξεργασία, ανανέωση, διαγραφή και ανάκτηση των προσωπικών στοιχείων που περιλαμβάνουν. Το είδος και το πλήθος των στοιχείων αυτών θα πρέπει να καθορίζεται ανάλογα με τις ανάγκες της εκάστοτε μελέτης εφαρμογής και να αποτελεί τη χρυσή τομή μεταξύ της αρχής για «αποκάλυψη με βάση την ελάχιστη ανάγκη γνώσης» και των προσωπικών δεδομένων που είναι απαραίτητα για την ασφαλή και αξιόπιστη λειτουργία του ΕΣΠΣ.

Η ΜΔΕΠ αναλαμβάνει τη διαχείριση και την επιβολή των πολιτικών εξουσιοδότησης, ελέγχου προσπέλασης και προστασίας της ιδιωτικότητας που θα πρέπει απαραίτητα να υλοποιούνται από κάθε ΕΣΠΣ και οι οποίες θα πρέπει να αποθηκεύονται με ασφαλή τρόπο στο ΕΛΧ. Η προσπέλαση των πολιτικών και η σύγκρισή τους με τις αιτήσεις προσπέλασης των χρηστών επιτυγχάνεται κάθε φορά που ένας εγγεγραμμένος χρήστης επιθυμεί να προσπελάσει κάποια υπηρεσία. Αρχικά, η ΜΔΕΠ θα πρέπει να ελέγξει εάν η ομάδα χρηστών στην οποία ανήκει ο χρήστης είναι εξουσιοδοτημένη για τη συγκεκριμένη υπηρεσία, και στη συνέχεια, εάν η υπηρεσία αυτή απαιτεί την επιβολή επιπρόσθετων πολιτικών προστασίας της ιδιωτικότητας, θα πρέπει να γίνει ένας ακόμα έλεγχος με βάση το βαθμό αξιοπιστίας του χρήστη και τα προκαθορισμένα κατώφλια εμπιστοσύνης της συγκεκριμένης υπηρεσίας (βλ. Κεφάλαιο 6). Εάν η αρχική αίτηση προέρχεται από χρήστη κάποιου εξωτερικού συστήματος ο

οποίος δεν είναι εγγεγραμμένος στο ΕΣΠΣ, η ΜΔΕΠ θα αναλάβει τη διαπραγμάτευση των ετερογενών πολιτικών, πάντα με τη βοήθεια της ΜΔΥΙ και του ΕΛΧ, ώστε να καταλήξει με μια ασφαλή προς το ΕΣΠΣ απόφαση εξουσιοδότησης (βλ. Κεφάλαιο 6).

Η ΜΚΑΣ, μέσω του ΣΔΑ που ενσωματώνει, περιλαμβάνει όλη την πληροφορία που είναι απαραίτητη για τον υπολογισμό του βαθμού αξιοπιστίας των χρηστών κάθε χρονική στιγμή. Βασίζεται στα δεδομένα που παράγουν δύο βασικές διαδικασίες. Η πρώτη αφορά στη συλλογή και την καταγραφή των αρνητικών ψήφων με τις οποίες αξιολογείται το περιεχόμενο που προσβάλλει την ιδιωτικότητα των χρηστών και η δεύτερη στον υπολογισμό του βαθμού αξιοπιστίας χρησιμοποιώντας επιπρόσθετες πληροφορίες που παρέχονται από το ΕΛΧ και τη ΜΔΨΤ.

Η ΜΔΥΙ διαχειρίζεται όλες τις πληροφορίες που διακινούνται από και προς το ΣΔΤΕΠ ενσωματώνοντας ή εξάγοντας τα δεδομένα ασφαλείας σε/από κατάλληλα ορισμένα με βάση διεθνή πρότυπα ασφαλείας μηνύματα SOAP. Η μονάδα αυτή αναλαμβάνει το ρόλο του διαμεσολαβητή μεταξύ του ΣΔΤΕΠ και των υπολοίπων οντοτήτων του ΕΣΠΣ, καθώς είναι υπεύθυνη για τη μετατροπή των δεδομένων σε μορφή κατάλληλη είτε για επεξεργασία από τις εσωτερικές μονάδες είτε για αποστολή με ασφαλή τρόπο των κατάλληλων διαπιστευτηρίων ασφαλείας που αιτούνται οι χρήστες μέσω της χρήσης του ΕΣΠΣ και των ενσωματωμένων σε αυτό εφαρμογών. Όπως περιγράφεται με περισσότερη λεπτομέρεια στα δύο επόμενα κεφάλαια, η υιοθέτηση και η κατάλληλη προσαρμογή των προδιαγραφών WS-Security και WS-Trust είναι ικανή να καλύψει όλες τις βασικές απαιτήσεις εμπιστευτικότητας, ακεραιότητας και αυθεντικοποίησης που χαρακτηρίζουν την επικοινωνία του ΣΔΤΕΠ με τα υπόλοιπα συστήματα και μονάδες του ΕΣΠΣ ή ακόμα και με εξωτερικές οντότητες.

Τέλος, το ΕΛΧ, όπως έχει ήδη αναφερθεί, αναλαμβάνει την ασφαλή αποθήκευση των προσωπικών δεδομένων και των διαπιστευτηρίων των χρηστών κατηγοριοποιώντας τα δεδομένα σε πολιτικές εξουσιοδότησης, πολιτικές προστασίας της ιδιωτικότητας, ομάδες χρηστών και λογαριασμούς χρηστών. Οι δομές αυτές των δεδομένων ασφαλείας θα πρέπει να δημιουργούνται και να αποθηκεύονται είτε σε ασφαλείς και διαβαθμισμένες βάσεις δεδομένων είτε σε προστατευόμενα με όλους τους απαραίτητους μηχανισμούς ασφαλείας ευρετήρια LDAP. Εδώ αποθηκεύονται επίσης οι λίστες καταγραφής συμπεριφοράς που παράγονται από τη ΜΚΑΣ και οι οποίες ορίζονται αναλυτικά στην ενότητα 6.7.1.

4.3.2.2 Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης

Το Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης (ΣΣΚΑ) είναι η πλατφόρμα που ολοκληρώνει και παρέχει όλες τις εφαρμογές Web 2.0

προσφέροντας με τον τρόπο αυτό τις απαραίτητες συνθήκες συνεργασίας και κοινωνικής αλληλεπίδρασης μεταξύ των χρηστών. Θα πρέπει επίσης να υπογραμμιστεί το γεγονός ότι πέραν των κλασικών δυνατοτήτων που παρέχουν συνεργατικές εφαρμογές, όπως τα ιστολόγια, τα φόρουμ και τα wiki, διαπιστώνεται ότι στα πλαίσια του ολοκληρωμένου πλαισίου συνεργασίας που έχει σχεδιαστεί για να παρέχει το ΕΣΠΣ, κρίσιμο χαρακτηριστικό αποτελεί η ολοκλήρωση των εφαρμογών Web 2.0 με άλλα συστήματα και τεχνολογίες, ώστε να επιτυγχάνεται η σύνθεση και η αποδοτική ενορχήστρωση ετερογενών και υψηλής προστιθέμενης αξίας υπηρεσιών.

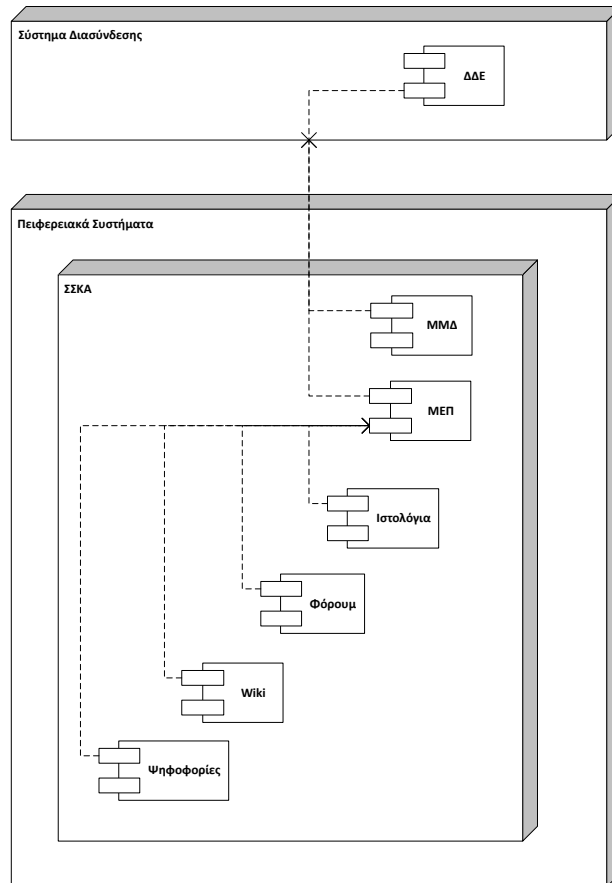
Λαμβάνοντας αυτά υπόψιν η διατριβή προτείνει ότι το ΣΣΚΑ έχει οριζόντια δράση στα πλαίσια του ΕΣΠΣ και ο βασικός του ρόλος είναι να παρέχει δυνατότητες σχολιασμού, κοινοποίησης περιεχομένου, ανταλλαγής απόψεων και κοινωνικής αλληλεπίδρασης μεταξύ των χρηστών και κάθε εμπλεκόμενης οντότητας όποτε και όπου αυτό απαιτείται, είτε πρόκειται για αυτόνομο περιβάλλον συνεργασίας είτε ενσωματώνεται σε κάποια άλλου είδους εφαρμογή και περιεχόμενο. Τα βασικά εργαλεία που ενσωματώνονται στο ΣΣΚΑ είναι τα ακόλουθα:

- *Ιστολόγια*
- *Wiki*
- *Φόρουμ*
- *Ηλεκτρονικές Ψηφοφορίες.*

Στις δύο επόμενες υποενότητες αναλύεται σε υψηλό επίπεδο η *Υπολογιστική και Πληροφοριακή Προσέγγιση* με βάση το μοντέλο *RM-ODP* των βασικών δομικών μονάδων του ΣΣΚΑ.

4.3.2.2.1 Υπολογιστική προσέγγιση

Με βάση την υπολογιστική προσέγγιση, το ΣΣΚΑ αναλύεται όπως φαίνεται στο Σχήμα 14.



Σχήμα 14: Διάγραμμα UML του ΣΣΚΑ

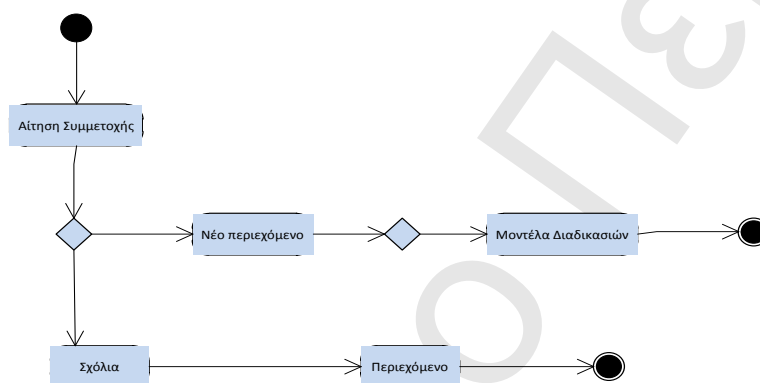
Όπως φαίνεται στο Σχήμα 14, εκτός από τις τέσσερις (4) βασικές μονάδες και εφαρμογές συνεργασίας, όπως είναι τα ιστολόγια, τα φόρουμ, τα wiki και οι ψηφοφορίες, τα οποία και περιγράφηκαν στην αρχή αυτής της ενότητας, το αρχιτεκτονικό σχέδιο του ΣΣΚΑ θα πρέπει επίσης να περιλαμβάνει μια βάση δεδομένων όπου θα αποθηκεύονται όλα τα δεδομένα και η πληροφορία που παράγεται από τη συνεργασία και την κοινωνική αλληλεπίδραση των χρηστών καθώς και δύο ακόμα βασικές μονάδες:

- Η Μονάδα Μοντέλων Διαδικασιών (ΜΜΔ), η οποία αναλαμβάνει την επικοινωνία με το ΣΜΔΕΠ μέσω του Συστήματος Διασύνδεσης προκειμένου να καταστεί δυνατή η αναζήτηση, ανάκτηση και μεταφόρτωση των μοντελοποιημένων διαδικασιών και πολιτικών στις συνεργατικές εφαρμογές και στο περιβάλλον κοινωνικής αλληλεπίδρασης που παρέχει το ΣΣΚΑ (βλ. ενότητα 4.3.2.3).
- Η Μονάδα Ελέγχου Προσπέλασης (ΜΕΠ), η οποία μέσω του Συστήματος Διασύνδεσης αναλαμβάνει την ασφαλή επικοινωνία και ανταλλαγή δεδομένων με το ΣΔΤΕΠ, ώστε η τελική ενσωμάτωση των εργαλείων και των εφαρμογών του ΣΣΚΑ στις υπόλοιπες δυνατότητες που παρέχει το ΕΣΠΣ να γίνεται με διαφανή και αξιόπιστο τρόπο (βλ. Κεφάλαιο 6).

Κρίνεται σκόπιμο, επίσης, να αναφερθεί ότι όλες οι προαναφερθείσες επικοινωνίες και ανταλλαγές δεδομένων επιτυγχάνονται με διεπαφές Υπηρεσιών Ιστού και με κατάλληλα μηνύματα SOAP τα οποία μεταφέρονται με ασφάλεια μέσω του ΔΔΕ του Συστήματος Διασύνδεσης.

4.3.2.2.2 Πληροφοριακή προσέγγιση

Με βάση την Πληροφοριακή Προσέγγιση του προτύπου RM-ODP η κατάσταση της πληροφορίας που δημιουργείται και γίνεται αντικείμενο διαχείρισης στα πλαίσια του ΣΣΚΑ είναι παρόμοια και για τις τέσσερις βασικές του μονάδες, ενώ όπως φαίνεται στο Σχήμα 15, περιλαμβάνει πάντα τη δυνατότητα ενσωμάτωσης δεδομένων που προέρχονται από το ΣΜΔΕΠ.



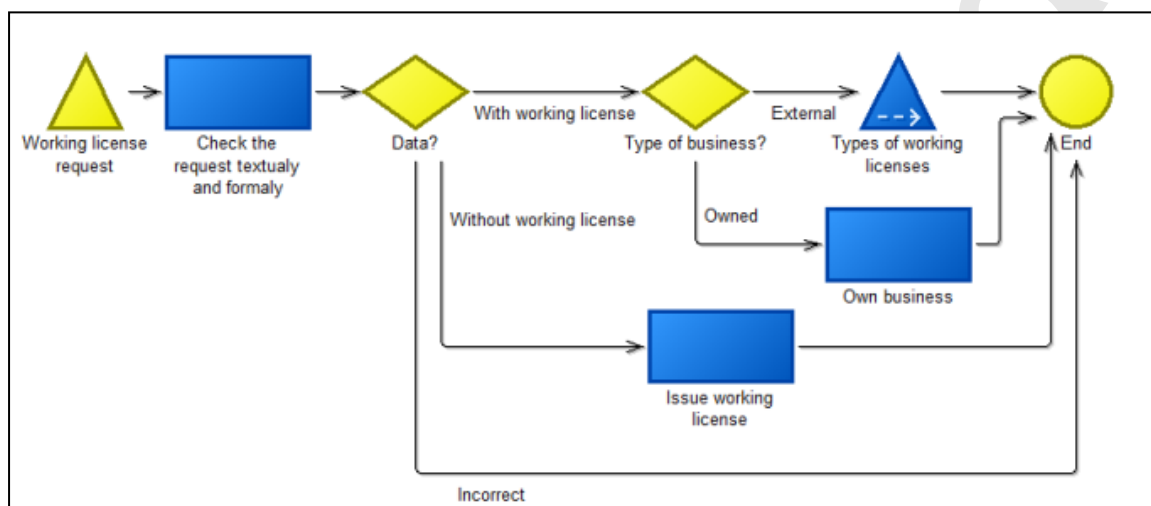
Σχήμα 15: Διάγραμμα Κατάστασης Πληροφορίας UML του ΣΣΚΑ

Στο Σχήμα 15 εμφανίζονται η ροή και η κατάσταση των πληροφοριών του ΣΣΚΑ. Το σύστημα ενεργοποιείται κάθε φορά που ο χρήστης αιτείται προσπέλασης στις συνεργατικές εφαρμογές του ΕΣΠΣ. Καταρχάς, ενεργοποιείται η ΜΔΤΕΠ η οποία αναλαμβάνει την αναγνώριση του χρήστη και του ρόλου του και την επιβολή των πολιτικών και αποφάσεων εξουσιοδότησης που λαμβάνει από το ΣΔΤΕΠ. Στη συνέχεια, ο χρήστης έχει τη δυνατότητα είτε να δημιουργήσει νέο περιεχόμενο δημιουργώντας ένα νέο ιστολόγιο, φόρουμ, wiki, κτλ. είτε να συνεισφέρει τις προσωπικές του γνώσεις και σχολιασμούς στο περιεχόμενο κάποιου άλλου χρήστη.

4.3.2.3 Σύστημα Μοντελοποίησης Διαδικασιών

Ο λόγος για τον οποίο το Σύστημα Μοντελοποίησης Διαδικασιών και Εναρμόνισης Πολιτικών (ΣΜΔΕΠ) αποτελεί απαραίτητο τεχνολογικό στοιχείο του αρχιτεκτονικού σχεδίου του ΕΣΠΣ είναι το γεγονός ότι σε πολλούς και ιδιαίτερα κρίσιμους τομείς της σύγχρονης Κοινωνίας της Πληροφορίας υπάρχει η ανάγκη για μοντελοποίηση ετερογενών διαδικασιών και για την από κοινού συνεργασία και ανάλυσή τους με σκοπό την εναρμόνιση των αντίστοιχων πολιτικών. Λαμβάνοντας υπόψιν το γεγονός ότι το πληροφορικό περιεχόμενο του ΣΜΔΕΠ μπορεί να ποικίλλει, αναφέρεται ενδεικτικά ότι ενδέχεται να αφορά σε κυβερνητικές διαδικασίες, διαδικασίες ασφάλειας ή επιχειρησιακές διαδικασίες.

Στόχος του ΣΜΔΕΠ είναι να παρέχει τη γραφική αναπαράσταση διαδικασιών, οι οποίες με τη σειρά τους συνθέτουν μια πολιτική. Αυτή η γραφική απεικόνιση των διαδικασιών συνοδεύεται από τις κατάλληλες πληροφορίες και μετά-δεδομένα (π.χ. τίτλος, περιγραφή βημάτων, σχόλια), ενώ μέσω διαδραστικών λειτουργιών παρέχεται η δυνατότητα να δημοσιευτούν σε ιστολόγια και φόρουμ προκειμένου να γίνουν αντικείμενο κοινωνικού σχολιασμού.



Σχήμα 16: Μοντελοποίηση και γραφική αναπαράσταση διαδικασιών

Στο Σχήμα 16 παρουσιάζεται η γραφική αναπαράσταση μιας διαδικασίας έκδοσης άδειας εργασίας, η οποία, όπως περιγράφεται στο έβδομο κεφάλαιο, έγινε με χρήση της πλατφόρμας Adonis Process Portal⁴ [12] για τις ανάγκες των του Ευρωπαϊκού έργου Immigration Policy 2.0⁵ [15].

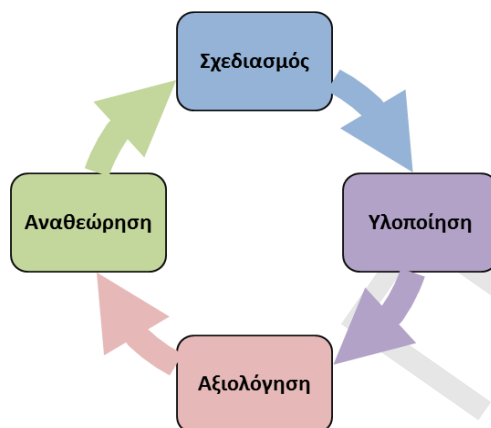
Ακολουθώντας αυτή την προσέγγιση επιτυγχάνεται η ενίσχυση και η εξέλιξη των κλασικών εργαλείων και συστημάτων μοντελοποίησης και διαχείρισης επιχειρησιακών διεργασιών μέσω της ενσωμάτωσης και της αποτελεσματικής ολοκλήρωσής τους με τις καινοτόμες λειτουργίες των τεχνολογιών Web 2.0 και τις δυνατότητες συνεργασίας που παρέχουν στα πλαίσια ενός ευρύτερου ασφαλούς και έμπιστου περιβάλλοντος.

Σε τεχνικό επίπεδο, η μοντελοποίηση και η γραφική αναπαράσταση διαδικασιών βοηθά τους αρμόδιους φορείς να κατανοήσουν τις δυσκολίες και τα εμπόδια αναβάθμισης και εξέλιξης των υφιστάμενων διαδικασιών καθώς και να εκφράσουν αποδοτικά τις προσωπικές τους γνώσεις. Επίσης, ως μέσο επικοινωνίας και συνεργασίας είναι ιδιαίτερα φιλικά προς τον τελικό χρήστη και, αν και απλά στην κατανόηση, είναι δυνατόν να περιέχουν κρίσιμες και πολύ λεπτομερείς πληροφορίες σχετικά με τα αντικείμενα που απεικονίζουν.

⁴ <http://www.boc-group.com/gr/products/adonis/>

⁵ <http://www.immigrationpolicy2.eu>

Η μοντελοποίηση διαδικασιών σαν μέθοδος συνεργασίας είναι ικανή να βελτιώσει τις υφιστάμενες δομές της πληροφορίας και να καθορίσει παράλληλα τα στάδια εξέλιξης μιας διαδικασίας και κατ' επέκταση των σχετικών πολιτικών. Με την ενσωμάτωση αυτού του βασικού τεχνολογικού συστήματος και της κατάλληλης ολοκλήρωσής του με τις υπόλοιπες μονάδες του ΕΣΠΣ είναι εφικτή η υιοθέτηση και η επιτυχής εφαρμογή του μοντέλου *PDCA* (*Plan - Do - Check - Act*) το οποίο απεικονίζεται στο Σχήμα 17.

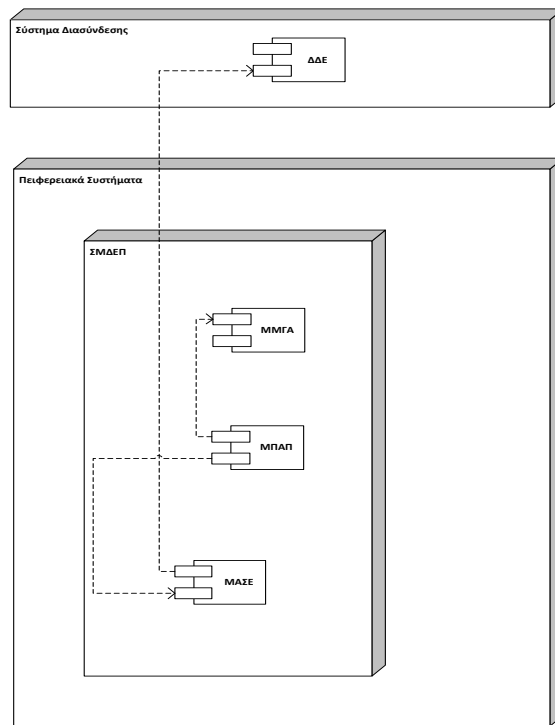


Σχήμα 17: Μοντέλο PDCA

Σύμφωνα με το μοντέλο αυτό, με την κατάλληλη ολοκλήρωση του ΣΜΔΕΠ το ΕΣΠΣ θα είναι σε θέση να παρέχει μια δυναμική και επαναλαμβανόμενη διαδικασία μοντελοποίησης και ανάλυσης διαδικασιών προκειμένου να αντιμετωπίζονται έγκαιρα οι απαιτούμενες αλλαγές στις επιχειρησιακές διαδικασίες και να επιτυγχάνονται τα πλέον αποδοτικά αποτελέσματα. Το γεγονός αυτό προσφέρει μια νέα διάσταση στον τρόπο με τον οποίο αναλύονται οι υφιστάμενες διαδικασίες και πολιτικές με συνεργατικό τρόπο.

4.3.2.3.1 Υπολογιστική προσέγγιση

Παρά το γεγονός ότι το αρχιτεκτονικό σχέδιο του ΣΜΔΕΠ πρέπει να βασίζεται στις προδιαγραφές του εκάστοτε τεχνολογικού πλαισίου που υιοθετείται, στο Σχήμα 18 παρουσιάζονται με βάση το μοντέλο RM-ODP οι βασικές μονάδες οι οποίες θα πρέπει κατ' ελάχιστο να ενσωματώνονται ώστε τελικά να ικανοποιούνται οι λειτουργικές απαιτήσεις του ΕΣΠΣ (βλ ενότητα 3.2.2).



Σχήμα 18: Διάγραμμα UML του ΣΜΔΕΠ

Όπως φαίνεται στο Σχήμα 18, το ΣΜΔΕΠ αποτελείται από τρεις βασικές μονάδες:

- Τη *Μονάδα Μοντελοποίησης και Γραφικής Απεικόνισης (ΜΜΓΑ)*, η οποία είναι υπεύθυνη για την αποτελεσματική και αποδοτική αλληλεπίδραση με τους τελικούς χρήστες ώστε να συλλέγονται με επιτυχία όλα τα απαραίτητα δεδομένα και πληροφορίες.
- Τη *Μονάδα Πληροφοριακών Αγαθών και Προτύπων (ΜΠΑΠ)*, η οποία παρέχει τη βασική υποδομή και όλα τα απαραίτητα πληροφοριακά αγαθά και αντικείμενα μοντελοποίησης που χρησιμοποιούνται από την ΜΜΓΑ. Η ΜΠΑΠ περιλαμβάνει τη δομημένη περιγραφή και τη σημασιολογική απεικόνιση όλων των βασικών εργαλείων μοντελοποίησης και αποτελεί την πιο κρίσιμη ίσως μονάδα, καθώς εκτός των απαιτήσεων για χρήση αποδοτικών λεξικών, εργαλείων και αντικειμένων, θα πρέπει να ικανοποιεί και βασικές απαιτήσεις διαλειτουργικότητας με άλλα ομότιμα συστήματα.
- Τη *Μονάδα Αξιολόγησης και Συνεργατικής Εναρμόνισης (ΜΑΣΕ)*, η οποία αναλαμβάνει τη δημοσίευση των μοντέλων και των γραφικών απεικονίσεων στις συνεργατικές εφαρμογές του ΕΣΠΣ ώστε να παρέχεται η δυνατότητα συνεργασίας και κοινωνικής αλληλεπίδρασης με σκοπό την παραγωγή νέων εναρμονισμένων μοντέλων και πολιτικών ικανών να παρέχουν λύσεις σε πολύπλοκα θέματα.

Η ΜΜΓΑ παρέχει στους τελικούς χρήστες τη δυνατότητα προσπέλασης μοντέλων και διαδικασιών, την εύκολη αλληλεπίδραση με διαδραστικές

γραφικές διεπαφές οι οποίες επιτρέπουν την επεξεργασία και ανάλυση των μοντέλων, καθώς και την εισαγωγή επιπλέον στοιχείων και μετά-δεδομένων. Σε επίπεδο επικοινωνίας, η ανταλλαγή όλων των απαραίτητων δεδομένων με τη ΜΠΑΜ γίνεται μέσω προτυποποιημένων και ασφαλών μηνυμάτων SOAP ενώ για την αποτελεσματική γραφική απεικόνιση των μοντέλων είναι απαραίτητη η χρήση διαδραστικών τεχνολογιών Web 2.0 (π.χ. Javascript, Ajax, JSON).

Η ΜΠΑΠ, εκτός του να παρέχει όλα τα απαραίτητα πληροφοριακά αγαθά και αντικείμενα μοντελοποίησης στη ΜΜΓΑ προκειμένου να χρησιμοποιούνται από τους χρήστες κατά τη διαδικασία της μοντελοποίησης, παρέχει και όλη την απαραίτητη διαλειτουργικότητα ώστε να είναι δυνατή η ανταλλαγή δεδομένων με άλλα συστήματα χρησιμοποιώντας προτυποποιημένους τύπους δεδομένων. Χαρακτηριστικά αναφέρεται ότι δημοφιλείς τύποι δεδομένων για την ανταλλαγή πληροφοριών μοντελοποίησης και γραφικής απεικόνισης διαδικασιών είναι της μορφής XML, MS Excel και ADL. Επίσης πρέπει να αναφερθεί ότι η ΜΠΑΠ είναι υπεύθυνη για την επικοινωνία με τη βάση δεδομένων ή το ευρετήριο στο οποίο αποθηκεύονται τα αντικείμενα και τα εργαλεία μοντελοποίησης, τα μοντέλα των διαδικασιών και η μετα-πληροφορία που τα συνοδεύει.

Τέλος, η ΜΑΣΕ είναι αυτή η οποία προσφέρει τη δυνατότητα στους χρήστες να αναλύσουν και να επεξεργαστούν με συνεργατικό τρόπο τα γραφικά μοντέλα, να τα συγκρίνουν και, τελικά, να καταλήξουν σε νέα εναρμονισμένα και πιο αποδοτικά μοντέλα.

Η πληροφορία που παράγεται από αυτή τη μονάδα του ΣΜΔΕΠ είναι ικανή να βοηθήσει του φορείς λήψης αποφάσεων στον επανασχεδιασμό νέων βελτιωμένων διαδικασιών: αυτός είναι ένας βασικός λόγος για τον οποίο κρίνεται απαραίτητη η ενσωμάτωσή του στην βασική αρχιτεκτονική του ΕΣΠΣ. Για να επιτευχθεί αυτό θα πρέπει να προηγηθεί η αποτελεσματική ολοκλήρωση του ΣΜΔΕΠ με το ΣΣΚΑ ώστε να υποστηρίζεται η κοινοποίηση των γραφικών μοντέλων σε συνεργατικά περιβάλλοντα και εφαρμογές με σκοπό τη συλλογή ανατροφοδότησης, σχολίων και χρήσιμων προτάσεων από τους χρήστες που συμμετέχουν στο εκάστοτε πλαίσιο συνεργασίας. Έτσι, διευκολύνεται η από κοινού λήψη αποφάσεων και η συνεργατική εναρμόνιση ετερογενών διαδικασιών και πολιτικών.

Δύο είναι οι υπό-μονάδες που περιλαμβάνει η ΜΑΣΕ:

- Η *Υπό-Μονάδα Σύγκρισης Διαδικασιών (ΥΜΣΔ)*, η οποία επιτρέπει τη σύγκριση ετερογενών διαδικασιών ή μοντέλων πολιτικών σχετικά με τα αντικείμενα (στοιχεία) μοντελοποίησης (π.χ. έναρξη, λήξη, αποφάσεις, επαναλαμβανόμενες διαδικασίες) και τις οντότητες που περιλαμβάνουν.
- Η *Υπό-Μονάδα Εναρμόνισης Διαδικασιών (ΥΜΕΔ)*, η οποία παρέχει τη δυνατότητα επέκτασης των υπάρχοντων μοντέλων και διαδικασιών με την εισαγωγή νέων αντικειμένων και συνδέσμων έτσι ώστε να

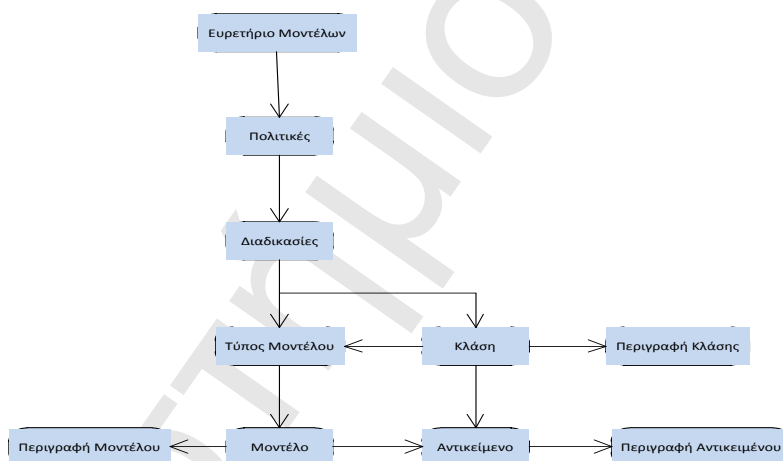
καλύπτονται οι αποκλίσεις που προκύπτουν κατά τη σύγκριση των μοντέλων. Τονίζεται, μάλιστα, ότι για την επιτυχημένη απόδοση της συγκεκριμένης λειτουργίας είναι ιδιαίτερα κρίσιμη η δυνατότητα εισαγωγής μετά-δεδομένων καθώς και η συλλογή και η ανάλυση σχολιασμών, αξιολογήσεων και αποτελεσμάτων κοινωνικής αλληλεπίδρασης.

Στην επόμενη ενότητα αναλύονται οι τρεις βασικές μονάδες του ΣΜΔΕΠ με βάση την *Πληροφοριακή Προσέγγιση* του προτύπου RM-ODP.

4.3.2.3.2 Πληροφοριακή προσέγγιση

Λαμβάνοντας υπόψιν το γεγονός ότι στόχος είναι ο καθορισμός ενός γενικευμένου και πλήρως επεκτάσιμου αρχιτεκτονικού μοντέλου για ΕΣΠΣ, σε αυτή την ενότητα η ανάλυση περιορίζεται στην περιγραφή της πληροφοριακής όψης εκείνων μόνο των μονάδων του ΣΜΔΕΠ οι οποίες είναι δυνατόν να προκαθοριστούν σε υψηλό επίπεδο.

Στο Σχήμα 19 φαίνονται οι καταστάσεις που περιλαμβάνει η πληροφορία που σχετίζεται με την αναπαράσταση των διαδικασιών που ενσωματώνει η ΜΠΑΠ.



Σχήμα 19: Διάγραμμα κατάστασης UML της ΜΠΑΠ

Όπως φαίνεται στο Σχήμα 19, βασικά στοιχεία κάθε μοντέλου θα πρέπει μεταξύ άλλων να είναι ο τύπος του, τα αντικείμενα που περιλαμβάνει και οι κλάσεις των αντικειμένων στις οποίες ανήκουν.

Όσον αφορά στην ΥΜΕΔ, θα πρέπει να καθοριστεί η κατάλληλη δομή δεδομένων με βάση την οποία γίνεται η ανάλυση της σύγκρισης των μοντέλων όπως αυτή θα προκύπτει από την ΜΠΑΠ. Η ΥΜΕΔ πρέπει κατ' ελάχιστον να περιλαμβάνει τα ακόλουθα κριτήρια:

- Αριθμό βημάτων διαδικασίας
- Οντότητες που συμμετέχουν
- Περιγραφές αντικειμένων

- Χαρακτηριστικά κόμβων απόφασης
- Σχετικά έγγραφα
- Παραγόμενα αποτελέσματα
- Έναρξη/Τέλος διαδικασίας.

Ο σαφής καθορισμός των καταστάσεων της πληροφορίας που θα περιλαμβάνει η ΥΜΕΔ θα πρέπει να είναι υπό συνεχή αναθεώρηση και προσαρμογή.

4.3.3 Σύστημα Διασύνδεσης

Όλα τα περιφερειακά συστήματα της *Κεντρικής Πλατφόρμας*, τα οποία περιγράφηκαν πιο πάνω αλλά και οποιαδήποτε άλλα απαιτείται να συνδεθούν με το ΕΣΠΣ, θα πρέπει να αλληλεπιδρούν με ενιαίο και προτυποποιημένο τρόπο. Στην προτεινόμενη αρχιτεκτονική αυτό επιτυγχάνεται μέσω της ενσωμάτωσης ενός ενδιάμεσου επιπέδου το οποίο περιλαμβάνει το *Σύστημα Διασύνδεσης*. Αυτό επιτρέπει τη διασύνδεση της *Κεντρικής Πλατφόρμας* με τα ετερογενή *Περιφερειακά Συστήματα* αλλά και κάθε άλλη υπάρχουσα ή μελλοντική εφαρμογή, σύστημα ή βάση δεδομένων που απαιτείται να συνδεθεί με το ΕΣΠΣ.

Έτσι, βασικές δυσκολίες κατά την ολοκλήρωση ενός ΕΣΠΣ με ετερογενή συστήματα, όπως οι ακόλουθες, αντιμετωπίζονται με επιτυχία:

- η πλειοψηφία των επιχειρησιακών συστημάτων βασίζονται σε δικές τους ιδιοκτησιακές διεπαφές,
- υλοποιούν περιορισμένα πρωτόκολλα επικοινωνίας, και
- δεν παρέχουν ιδιαίτερες δυνατότητες διασύνδεσης και επεκτασιμότητας.

Ένας κατάλληλα σχεδιασμένος *Διάυλος Διαλειτουργικής Επικοινωνίας* είναι ικανός να παρέχει επαρκείς λύσεις στα εμπόδια που αναφέρθηκαν πιο πάνω εξασφαλίζοντας ότι κάθε επικοινωνία με την *Κεντρική Πλατφόρμα* βασίζεται σε πρότυπα μηνύματα ενώ η επικοινωνία με το κάθε *Περιφερειακό Σύστημα* ή εξωτερική εφαρμογή μπορεί να συνεχίζει να υλοποιείται με την εκάστοτε τεχνολογία και ιδιοκτησιακή μέθοδο την οποία απαιτεί η τελευταία χωρίς να επηρεάζεται η βασική αρχιτεκτονική του όλου συστήματος.

Το *Σύστημα Διασύνδεσης* και, πιο συγκεκριμένα, ο ΔΔΕ θα πρέπει να ολοκληρώνεται πάνω από την *Κεντρική Πλατφόρμα* προκειμένου να επιτρέπεται η περαιτέρω αποτελεσματική ολοκλήρωσή της με ετερογενή συστήματα, εφαρμογές και υπηρεσίες [6]. Επίσης, είναι υπεύθυνο για τη διαχείριση των αλληλεπιδράσεων μεταξύ των διαφορετικών συστημάτων και την αρμονική διασύνδεση των εκάστοτε υπηρεσιών με διαφανή τρόπο, επιτρέποντας την επικοινωνία μεταξύ τους μέσω ενός ενιαίου διαύλου προτυποποιημένων μηνυμάτων. Στην ουσία αποτελεί το σημείο ελέγχου και διαχείρισης όλων των διεπαφών Υπηρεσιών Ιστού που χρησιμοποιούνται στα πλαίσια λειτουργίας του ΕΣΠΣ.

4.4 Συμπεράσματα

Στον Πίνακα 1 παρουσιάζονται περιληπτικά όλες οι λειτουργικές και τεχνικές απαιτήσεις καθώς και οι απαιτήσεις χρηστών οι οποίες καταγράφηκαν στο τρίτο κεφάλαιο και γίνεται αναφορά στον τρόπο με τον οποίο ικανοποιούνται από την αρχιτεκτονική του ΕΣΠΣ που προτείνεται στα πλαίσια αυτού του κεφαλαίου της διατριβής.

A	Λειτουργικές Απαιτήσεις	Δυνατότητες ΕΣΠΣ
1.	Ολοκλήρωση συστημάτων με δυνατότητες αποθήκευσης, αναζήτησης και διαχείρισης πληροφοριακών αγαθών	ΜΕΔ (βλ. ενότητα 4.3.1.2)
2.	Συλλογή στατιστικών δεδομένων και αξιολόγηση της κοινής γνώμης	ΣΣΚΑ (βλ. ενότητα 4.3.2.2)
3.	Ολοκλήρωση συνεργατικών εφαρμογών και εργαλείων κοινωνικής αλληλεπίδρασης	ΣΣΚΑ (βλ. ενότητα 4.3.2.2)
4.	Ολοκλήρωση μηχανισμών μοντελοποίησης και ανάλυσης διαδικασιών.	ΣΜΔΕΠ (βλ. ενότητα 4.3.2.3)
5.	Διασύνδεση ετερογενών πληροφοριακών συστημάτων	Σύστημα Διασύνδεσης (βλ. ενότητα 4.3.3)
B	Απαιτήσεις Χρηστών	
6.	Χρησιμότητα	ΣΜΔΕΠ (βλ. ενότητα 4.3.2.3)
7.	Ευχρηστία	ΜΔΧ (βλ. ενότητα 4.3.1.1)
8.	Εμπιστοσύνη	ΣΔΤΕΠ (βλ. Κεφάλαιο 6)
9.	Πολυγλωσσικότητα	ΜΔΧ (βλ. ενότητα 4.3.1.1)
Γ	Τεχνικές Απαιτήσεις	
10.	Διαλειτουργικότητα	Σύστημα Διασύνδεσης (βλ. ενότητα 4.3.3)
11.	Ασφάλεια	ΣΔΤΕΠ (βλ. ενότητα 4.3.2.1)
12.	Επαναχρησιμοποίηση	Περιφερειακές Μονάδες (βλ. ενότητα 4.3.2)
13.	Προστασία ιδιωτικότητας	ΣΔΤΕΠ (βλ. Κεφάλαιο 6)
14.	Αρθρωτή αρχιτεκτονική	ΕΣΠΣ (βλ. Ενότητα 4.3)
15.	Επεκτασιμότητα	Σύστημα Διασύνδεσης (βλ. ενότητα 4.3.3)
16.	Ανοιχτά πρότυπα	Μεθοδολογία σχεδιασμού (βλ. ενότητα 4.2)
17.	Διαδραστικότητα	ΣΣΚΑ (βλ. ενότητα 4.3.2.2)

Πίνακας 1: Τεχνικές λύσεις και καινοτομίες ΕΣΠΣ

Συνθέτοντας τις δυνατότητες που παρέχουν οι σύγχρονες τεχνολογίες, όπως οι Υπηρεσίες Ιστού και οι προσανατολισμένες στις υπηρεσίες αρχιτεκτονικές, η μοντελοποίηση και διαχείριση διαδικασιών, οι διαδραστικές υπηρεσίες και εφαρμογές Web 2.0 και τα συστήματα ασφαλούς διαχείρισης των ψηφιακών ταυτοτήτων των χρηστών, η αρχιτεκτονική του ΕΣΠΣ που παρουσιάστηκε σε αυτό το κεφάλαιο είναι ικανή να προσφέρει ένα ολοκληρωμένο και ασφαλές περιβάλλον συνεργασίας. Επιπρόσθετα, το περιβάλλον αυτό είναι εύκολα επεκτάσιμο και πλήρως διαλειτουργικό με οποιοδήποτε άλλο σύστημα, εφαρμογή ή βάση δεδομένων απαιτείται να αλληλεπιδράσει μαζί του, ενώ παράλληλα ικανοποιεί και όλες τις απαραίτητες λειτουργικές απαιτήσεις και τεχνικές προδιαγραφές οι οποίες καθορίστηκαν στις ενότητες 3.2.2 και 0.

Πέραν του ολοκληρωμένου αρχιτεκτονικού σχεδίου οι βασικές καινοτομίες στην προτεινόμενη αρχιτεκτονική του ΕΣΠΣ αφορούν στα ακόλουθα:

- Την ολοκλήρωση του *Συστήματος Μοντελοποίησης και Διαχείρισης Διαδικασιών (ΣΜΔΔ)* [14] με το πλαίσιο υπηρεσιών του ΕΣΠΣ έτσι ώστε να υποστηρίζεται η συνεργατική μοντελοποίηση και η ανάλυση ετερογενών διαδικασιών, καθώς και η συλλογική λήψη αποφάσεων [11, 14].
- Την ολοκλήρωση του *Συστήματος Συνεργασίας και Κοινωνικής Αλληλεπίδρασης (ΣΣΚΑ)* και των εφαρμογών Web 2.0 που περιλαμβάνει με ένα σύνολο εξίσου απαραίτητων τεχνολογιών και προτύπων ασφάλειας ώστε να αντιμετωπίζονται αποτελεσματικά οι απειλές που ελλοχεύει η εφαρμογή τους και να μεγιστοποιείται η προστιθέμενη αξία που είναι ικανές να προσφέρουν.
- Την προδιαγραφή ενός κατάλληλα σχεδιασμένου *Συστήματος Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης (ΣΔΤΕΠ)*, το οποίο είναι ικανό να καλύψει τις απαιτήσεις ιδιωτικότητας ενσωματώνοντας στην αρχιτεκτονική του ένα *Σύστημα Διαχείρισης Αξιοπιστίας (ΣΔΑ)*.

Στο επόμενο κεφάλαιο παρουσιάζονται τα αποτελέσματα της ανάλυσης επικινδυνότητας του ΕΣΠΣ ως προς την κρισιμότητα των συστημάτων που ενσωματώνονται στην αρχιτεκτονική του για την προστασία των προσωπικών δεδομένων των χρηστών.

4.5 Βιβλιογραφία

- [1] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Collaborative information and knowledge management environments: The "what" and "how"". OR Insight Journal, Special Issue on Facilitating information and knowledge management through Information Systems and Operational Research: from theory to practice.
- [2] A. Karantjias, S. Papastergiou, N. Polemi (2009). "Design Principles of a Secure Federated e/m-Government Framework". International Journal of Electronic Governance (IJEG), Special Issue on Users and uses of electronic governance 2(4), pp. 402-423.
- [3] T. Ntouskas, G. Pentafronimos, S. Papastergiou (2011). "STORM - Collaborative Security Management Environment". In Proceedings of the Fifth Workshop In Information Security Theory And Practice: Security and Privacy of Mobile Devices in Wireless Communication, (WISTP 2011). Heraklion, Greece. Springer Verlag.
- [4] G. Pentafronimos, A. Karantjias, N. Polemi (2010). "ODYSSEUS: An Advanced, Collaborative and Trusted Framework for the Provision of Migration Services". In Proceedings of the Fifth International Conference on Internet and Web Applications and Services. pp. 531-537. Barcelona, Spain. IEEE Digital Library.
- [5] G. Pentafronimos, A. Karantjias και N. Polemi (2009). "OPIS: An Open, Preventive and Scalable Migration Information System". In Proceedings of the 3rd International Conference on e-Democracy. Next Generation Society: Technological and Legal Issues, (e-Democracy 2009).Greece. Springer Verlag.
- [6] G. Pentafronimos, P. Spyridon, N. Polemi (2008). "Interoperability Testing for e-Government Web Services". In Proceedings of the Second International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008), Cairo, Egypt. ACM Publisher.
- [7] A. Nouredine, M. Damodaran (2008). "Security in web 2.0 application development". In Proceedings of the 10th International Conference on

- Information Integration and Web-based Applications & Services. pp, 681-685. Linz, Austria. ACM Publications.
- [8] A. Dais, M. Nikoloaidou, D. Anagnostopoulos (2009). "Facilitating business to government interaction using a citizen-centric web 2.0 model". In Proceeding of 9th IFIP WG 6.1 Conference on e-Business, e-Services and e-Society, (I3E 2009). Vol. 305, pp. 134-147. Nancy, France. Springer Verlag.
- [9] RM-ODP Reference Model, Sytmemic Modelling Laboratory, LAMS, Ecole Polytechnique Federale de Lausanne, <http://lams.epfl.ch/reference/rm-odp>
- [10] Information Technology - Open Distributed Processing— Reference Model—Enterprise Language, Proposed new version, ISO/IEC JTC1/SC7/WG17 W17N0222, ITU-T X.911 ISO/IEC 15414, March 2006.
- [11] N. Rolland (2004). "Knowledge management impacts on decision making process". Journal of Knowledge Management. Vol. 8 (1), pp. 20-31. Emerald Group Publishing.
- [12] Open Model Initiative (OMI), University of Vienna - Faculty of Computer Science, <http://openmodels.at/web/omi/home>
- [13] D. Harel, B. Rumpe (2004). "Meaningful Modeling: What's the Semantics of 'Semantics'?". IEEE Computer. Vol. 37 (10), pp. 64-72.
- [14] W. Xiaojun, G. Yu (2009). "Collaborative Knowledge Management System (CKMS) and Strategic Management". In Proceedings of the International Joint Conference on Artificial Intelligence, (IJCAI '09), pp. 190-193.
- [15] ImmigrationPolicy 2.0. EU Project, <http://immigrationpolicy2.cs.unipi.gr>
- [16] M. Alavi, R. Smith (1999). Knowledge Management Systems: Issues, Challenges Benefits. Communications of the Association for Information Systems, Vol. 1(7).
- [17] The I18N Custom Tag Library. Jakarta Tag Libs. Available at: <http://jakarta.apache.org/taglibs/doc/i18n-doc/intro.html>

Κεφάλαιο 5

Μελέτη Ιδιωτικότητας του ΕΣΠΣ

Η συνεισφορά της διατριβής στο δεύτερο κατά σειρά ερευνητικό άξονα που αναλύεται σε αυτό το κεφάλαιο περιλαμβάνει την καταγραφή των απειλών και την αξιολόγηση των επιθέσεων ιδιωτικότητας που αντιμετωπίζουν τα συνεργατικά περιβάλλοντα καθώς και την πρόταση κατάλληλων μέτρων προστασίας. Με βάση τα αποτελέσματα της μελέτης ιδιωτικότητας, προκύπτει τελικά ένα ολοκληρωμένο *Σχέδιο Ιδιωτικότητας (ΣΙΑ-ΕΣΠΣ)* το οποίο μεταξύ άλλων προτείνει καινοτόμες λύσεις, ικανές να αντιμετωπίζουν τις νέες απειλές που ελλοχεύει η χρήση των εφαρμογών Web 2.0.

5.1 Εισαγωγή

Μέχρι και πριν την εξέλιξη των εφαρμογών Web 2.0 η προστασία της ιδιωτικότητας αποτελούσε αρμοδιότητα αποκλειστικά των Παρόχων και αφορούσε στον τρόπο με τον οποίο επεξεργάζονταν και διαχειρίζονταν τα προσωπικά δεδομένα των χρηστών [15]. Βασικά μέτρα προστασίας αποτελούσαν οι πολιτικές ιδιωτικότητας και οι συμφωνίες σε επίπεδο παροχής υπηρεσιών μεταξύ των χρηστών και των Παρόχων [14, 19, 21] καθώς και η αξιοπιστία των τελευταίων στο να τηρούν το νομοθετικό πλαίσιο [13, 25, 26] και να εφαρμόζουν όλους τους απαραίτητους μηχανισμούς ασφάλειας και προστασίας των ευαίσθητων δεδομένων.

Από την άλλη πλευρά, με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάζονται στην ενότητα 2.4 διαπιστώνεται ότι αντίθετα με το πλαίσιο λειτουργίας των παραδοσιακών Πληροφοριακών Συστημάτων, όπου η ιδιωτικότητα είναι σε άμεση εξάρτηση από την κάλυψη των βασικών απαιτήσεων ασφάλειας, ήτοι της ακεραιότητας, της εμπιστευτικότητας, της αυθεντικοποίησης και της εξουσιοδότησης, η κάλυψη των τεσσάρων (4) αυτών απαιτήσεων δεν είναι αρκετή να εξασφαλίσει την προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα [9, 10, 12].

Στα πλαίσια των σύγχρονων Πληροφοριακών Συστημάτων, όπου με τη χρήση υπηρεσιών Web 2.0 οι χρήστες έχουν τη δυνατότητα να δημιουργούν περιεχόμενο με δυναμικό τρόπο προσβάλλοντας πολλές φορές, είτε ακούσια είτε εσκεμμένα, την ιδιωτικότητα των υπόλοιπων συμμετεχόντων στο περιβάλλον

συνεργασίας, οι απαιτήσεις ιδιωτικότητας λαμβάνουν νέες διαστάσεις [12, 20, 23].

Όπως έχει ήδη αναφερθεί σε προηγούμενα κεφάλαια, στα συνεργατικά περιβάλλοντα ακόμα και αν εφαρμόζονται σύγχρονοι μηχανισμοί ασφάλειας και οι Πάροχοι τηρούν στην πράξη τις πολιτικές ιδιωτικότητας με τον πιο αποτελεσματικό τρόπο, το ενδεχόμενο αποκάλυψης προσωπικών δεδομένων παραμένει. Βασική αιτία για αυτό αποτελεί το γεγονός ότι οι χρήστες με προνόμια χρήσης των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0 έχουν τη δυνατότητα να δημοσιεύουν πληροφορίες «ανεξέλεγκτα», κάθε φορά που αποκτούν πρόσβαση στο συνεργατικό περιβάλλον [6].

Επίσης διαπιστώνεται ότι οι νέοι κίνδυνοι για την ιδιωτικότητα των χρηστών τους οποίους ελλοχεύει η συμμετοχή τους στο συνεργατικό περιβάλλον δεν είναι εφικτό να αντιμετωπιστούν αποτελεσματικά με την εφαρμογή παραδοσιακών προσεγγίσεων [7].

Έχοντας σαν βασικό στόχο τη μελέτη ιδιωτικότητας και τον καθορισμό ενός ολοκληρωμένου πλαισίου προστασίας για το ΕΣΠΣ και για κάθε συνεργατικό περιβάλλον, οι ενότητες που ακολουθούν περιλαμβάνουν τα ακόλουθα:

- Ταξινόμηση πόρων του ΕΣΠΣ με βάση τις απαιτήσεις ιδιωτικότητας.
- Καταγραφή απειλών και επιθέσεων ιδιωτικότητας.
- Καταγραφή αντίμετρων για την προστασία της ιδιωτικότητας.
- Καθορισμό *Σχεδίου Ιδιωτικότητας* για το ΕΣΠΣ (*ΣΙΑ-ΕΣΠΣ*).

Τελικά προτείνεται η αποτελεσματική αντιμετώπιση των νέων προκλήσεων ιδιωτικότητας σε συνεργατικά περιβάλλοντα μέσω της εφαρμογής μιας καινοτόμου λύσης διαχείρισης ταυτοτήτων η οποία παρουσιάζεται στο έκτο κεφάλαιο.

5.2 Ταξινόμηση πόρων

Έχοντας σαν στόχο την ταξινόμηση και τη διαβάθμιση των κρίσιμων, ως προς την προστασία της ιδιωτικότητας, πόρων του ΕΣΠΣ στον Πίνακα 2 παρουσιάζεται η αποτίμηση των βασικών πληροφοριακών αγαθών καθώς και των επιμέρους συστημάτων τα οποία είναι υπεύθυνα για τη διαχείρισή τους.

Η κλίμακα που χρησιμοποιείται για την αποτίμηση της κρισιμότητας ως προς τις απαιτήσεις ιδιωτικότητας αποτελείται από τρία (3) επίπεδα, όπου:

1. ο βαθμός κρισιμότητας ένα (1) αντιστοιχεί σε προσωπικά δεδομένα,
2. ο βαθμός κρισιμότητας δύο (2) σε ενδεχομένως ευαίσθητα δεδομένα, και
3. ο βαθμός κρισιμότητας τρία (3) σε δημόσιες πληροφορίες.

Στη συνέχεια ακολουθεί αιτιολόγηση της κάθε επιλογής και ανάλυση των αποτελεσμάτων με βάση τις υφιστάμενες απαιτήσεις και τις διαθέσιμες τεχνολογικές λύσεις.

	Σύστημα / Μονάδα	Πληροφοριακά Αγαθά	Βαθμός Κρισιμότητας
Κεντρική Πλατφόρμα ΕΣΠΣ	ΜΔΧ	Δημόσιες πληροφορίες που παρέχονται μέσω των γραφικών διεπαφών, δεδομένα πλοήγησης και χρήσης του Πληροφοριακού Συστήματος, περιεχόμενο που δημοσιεύεται από τους Παρόχους.	3
	ΜΕΔ	Επιχειρησιακές διεργασίες και ροές εργασιών απαραίτητες για την αξιόπιστη και αποτελεσματική λειτουργία του πληροφοριακού συστήματος	2
	ΜΒΔ	Δεδομένα επιχειρησιακού περιεχομένου, τα οποία ανάλογα με την εκάστοτε μελέτη εφαρμογής ενδέχεται να περιλαμβάνουν προσωπικά δεδομένα.	2
Σύστημα Διασύνδεσης	ΔΔΕ	Μηνύματα SOAP και δεδομένα που αφορούν από δημόσιες πληροφορίες σύνδεσης στην Υπηρεσία Ιστού μέχρι προσωπικά και ευαίσθητα δεδομένα.	1
Περιφερειακά Συστήματα ΕΣΠΣ	ΣΔΤΕΠ	Προσωπικά και ευαίσθητα δεδομένα (διαπιστευτήρια εξουσιοδότησης, στοιχεία αυθεντικοποίησης, πολιτικές απόδοσης προνομίων).	1
	ΣΣΚΑ	Προσωπικό περιεχόμενο και σχόλια χρηστών με ενδεχόμενη αναφορά σε προσωπικά και ευαίσθητα δεδομένα.	1
	ΣΜΔΕΠ	Γραφικές αναπαραστάσεις και διαδικασίες επιχειρησιακών διεργασιών.	3

Πίνακας 2: Ταξινόμηση πόρων ΕΣΠΣ ως προς τις απαιτήσεις ιδιωτικότητας

Σχετικά με τη *Μονάδα Διεπαφών Χρήστη* ο βαθμός κρισιμότητας ορίζεται στο χαμηλότερο επίπεδο της κλίμακας και είναι ίσος με τρία (3). Αν και εξαρτάται από το βαθμό στον οποίο οι γραφικές διεπαφές εξασφαλίζουν την ασφάλεια των δεδομένων κατά τη μεταφορά στους από και προς τον εξυπηρετητή, όσον αφορά στις απαιτήσεις ιδιωτικότητας, τα δεδομένα των γραφικών διεπαφών και των βασικών μενού πλοήγησης αλλά και το δημόσια διαθέσιμο περιεχόμενο που δημοσιεύουν οι Πάροχοι κατά τη διάρκεια του κύκλου ζωής του Πληροφοριακού Συστήματος, δεν εμφανίζουν επιπρόσθετους κινδύνους.

Διαπιστώνεται ότι η ικανοποίηση αυτής της απαίτησης αφορά περισσότερο στην εμπιστευτικότητα και την ακεραιότητα των δεδομένων και για το λόγο αυτό εξαρτάται αποκλειστικά από την αποτελεσματικότητα των μέτρων

ασφάλειας που υιοθετούνται, ιδιαίτερα όταν χρησιμοποιούνται τεχνολογίες Web 2.0.

Παρά τις απαιτήσεις ασφάλειας που τη χαρακτηρίζουν, η *Μονάδα Επιχειρησιακών Διεργασιών* η οποία είναι υπεύθυνη για τη διαχείριση των επιχειρησιακών διαδικασιών που ενσωματώνει η κεντρική πλατφόρμα του ΕΣΠΣ, δεν σχετίζεται με την επεξεργασία και την ανταλλαγή προσωπικών δεδομένων και έτσι δεν θεωρείται κρίσιμη για την προστασία της ιδιωτικότητας των χρηστών. Αξιολογείται με βαθμό κρισιμότητας δύο (2).

Όπως φαίνεται στον Πίνακας 2 η *Μονάδα Βάσεων Δεδομένων* αξιολογείται επίσης με βαθμό κρισιμότητας δύο (2), καθώς οι απαιτήσεις ιδιωτικότητας που τη χαρακτηρίζουν είναι σε άμεση εξάρτηση από το περιεχόμενό της. Υπάρχει το ενδεχόμενο οι βάσεις δεδομένων που ενσωματώνονται στην κεντρική πλατφόρμα του ΕΣΠΣ να αποθηκεύουν και να διαχειρίζονται διαβαθμισμένα, εμπιστευτικά ή ακόμη και απόρρητα δεδομένα και υπάρχει το ενδεχόμενο να αποθηκεύουν δημόσιες πληροφορίες οι οποίες δεν απαιτούν ιδιαίτερα μέτρα προστασίας. Διαπιστώνεται επίσης ότι η προστασία της ιδιωτικότητας εξαρτάται αποκλειστικά από τα τεχνολογικά μέτρα ασφάλειας που υιοθετούνται.

Η αποτελεσματική και αξιόπιστη προστασία των βάσεων δεδομένων απαιτεί τη χρήση μεθόδων κρυπτογράφησης και άλλων μηχανισμών προστασίας κατάλληλων για μεγάλες αποθήκες δεδομένων. Επίσης εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των Παρόχων στο να εφαρμόζουν τα κατάλληλα μέτρα προστασίας και να τηρούν την ισχύουσα νομοθεσία.

Ο *Δίαυλος Διαλειτουργικής Επικοινωνίας* που ολοκληρώνεται στο *Σύστημα Διασύνδεσης* ταξινομείται στο μέγιστο βαθμό κρισιμότητας ένα (1), καθώς τα μηνύματα SOAP και τα δεδομένα που περιέχουν ενδέχεται να αφορούν σε προσωπικά δεδομένα των χρηστών. Όπως περιγράφεται στην ενότητα 2.4.2, η εφαρμογή προτύπων και προδιαγραφών ασφάλειας Υπηρεσιών Ιστού καθώς και σύγχρονων τεχνολογιών, όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές, είναι ικανή να διασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που ανταλλάσσονται [2, 27, 33]. Για το λόγο αυτό, παρά τις υψηλές απαιτήσεις ασφάλειας που χαρακτηρίζουν το ΔΔΕ δεν εντοπίζονται επιπλέον κίνδυνοι για την ιδιωτικότητα των χρηστών κι έτσι δεν αποτελεί ανοιχτό πεδίο έρευνας.

Όσον αφορά στα *Περιφερειακά Συστήματα* του ΕΣΠΣ και, πιο συγκεκριμένα, στο *Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης*, όπως είναι αναμενόμενο ταξινομείται στο μέγιστο επίπεδο κρισιμότητας με βαθμό κρισιμότητας ένα (1) καθώς τα πληροφοριακά αγαθά που διαχειρίζεται περιλαμβάνουν στη συντριπτική πλειοψηφία τους προσωπικά δεδομένα και δεδομένα ασφάλειας (π.χ. στοιχεία αυθεντικοποίησης, διαπιστευτήρια εξουσιοδότησης).

Με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάζονται στην ενότητα 2.4.3 διαπιστώνεται η ανάγκη αναβάθμισης των παραδοσιακών προσεγγίσεων διαχείρισης ταυτοτήτων έτσι ώστε να ανταποκρίνονται αξιόπιστα στις νέες απαιτήσεις που χαρακτηρίζουν τα συνεργατικά περιβάλλοντα και προτείνεται μια καινοτόμος λύση η οποία παρουσιάζεται στο επόμενο κεφάλαιο.

Το Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης ταξινομείται επίσης στο μέγιστο βαθμό κρισιμότητας ένα (1), δεδομένου ότι το περιεχόμενο και οι πληροφορίες που δημοσιεύονται από τους χρήστες μέσω των εφαρμογών Web 2.0 ενδέχεται να αποκαλύπτουν προσωπικά δεδομένα.

Η διατριβή συνεισφέρει στην προστασία της ιδιωτικότητας από την «ανεξέλεγκτη» δημιουργία περιεχομένου σε συνεργατικά περιβάλλοντα, προτείνοντας μια καινοτόμο προσέγγιση για την απόδοση προνομίων προσπέλασης στις εφαρμογές Web 2.0 η οποία βασίζεται στη δυναμική αξιολόγηση της αξιοπιστίας των χρηστών (βλ. ενότητα 6.4).

Τέλος, το Σύστημα Μοντελοποίησης Διαδικασιών και Εναρμόνισης Πολιτικών και τα δεδομένα που διαχειρίζεται αφορούν αποκλειστικά σε πληροφορίες επιχειρησιακού ενδιαφέροντος και δεν ελλοχεύει κινδύνους για την ιδιωτικότητα των χρηστών. Ταξινομείται στο χαμηλότερο επίπεδο της κλίμακας και έχει βαθμό κρισιμότητας ίσο με τρία (3).

Με βάση την ανάλυση των αποτελεσμάτων του Πίνακας 2, τα κρίσιμα όσον αφορά στην προστασία της ιδιωτικότητας συστήματα που ενσωματώνονται στην αρχιτεκτονική του ΕΣΠΣ είναι:

- Το Σύστημα Διαχείρισης Ταυτοτήτων και Ελέγχου Προσπέλασης.
- Το Σύστημα Συνεργασίας και Κοινωνικής Αλληλεπίδρασης.
- Ο Δίαυλος Διαλειτουργικής Επικοινωνίας.

Στις ενότητες που ακολουθούν παρουσιάζονται τα αποτελέσματα της μελέτης ιδιωτικότητας για τα τρία (3) αυτά κρίσιμα στοιχεία της αρχιτεκτονικής του ΕΣΠΣ.

5.3 Απειλές, επιθέσεις και μέτρα προστασίας

Στο πλαίσιο της διατριβής γίνεται η διαπίστωση ότι η κρισιμότητα των ΣΔΤΕΠ, ΣΣΚΑ και ΔΔΕ οφείλεται στα βασικά χαρακτηριστικά των σύγχρονων συνεργατικών Πληροφοριακών Συστημάτων, δηλαδή στην ενσωμάτωση εφαρμογών Web 2.0 και στη διασύνδεσή τους με εξωτερικά συστήματα.

Όσον αφορά στις απειλές στην ιδιωτικότητα που ελλοχεύει η διασύνδεση και η ανταλλαγή πληροφοριών με εξωτερικά συστήματα, αυτές αφορούν το ΔΔΕ και, όπως έχει ήδη αναφερθεί, εξαρτώνται αποκλειστικά από την υιοθέτηση διεθνών προτύπων και προδιαγραφών ασφάλειας (π.χ. WS-Security, WS-Trust) και την

εφαρμογή κατάλληλων τεχνολογιών (π.χ κρυπτογράφηση, ψηφιακές υπογραφές).

Δεδομένου ότι η υιοθέτηση αυτών των μεθόδων είναι ικανή να εγγυηθεί την επίτευξη σημαντικών στόχων όσον αφορά στην ασφάλεια και την προστασία της ιδιωτικότητας κατά την αλληλεπίδραση ετερογενών συστημάτων, γίνεται η παραδοχή ότι στα πλαίσια λειτουργίας του ΕΣΠΣ η εμπιστευτικότητα και η ακεραιότητα των μηνυμάτων προστατεύεται με αξιόπιστο τρόπο ώστε να μην τίθενται επιπλέον κίνδυνοι στην ιδιωτικότητα για λόγους ασφάλειας των δεδομένων.

Πιο συγκεκριμένα, η διατριβή θεωρεί ότι στα πλαίσια λειτουργίας του ΔΔΕ το πρωτόκολλο επικοινωνίας που χρησιμοποιείται βασίζεται σε τεχνολογίες Υπηρεσιών Ιστού, καθώς και ότι εφαρμόζονται αποτελεσματικά τα μέτρα ασφάλειας που ορίζουν οι προδιαγραφές WS-Security [32], οι οποίες εκτός των άλλων απαιτούν την κρυπτογράφηση του διαύλου επικοινωνίας μεταξύ δύο οντοτήτων [3, 5]. Έτσι, δεν αποτελεί αντικείμενο περαιτέρω έρευνας για τις ανάγκες της μελέτης ιδιωτικότητας του ΕΣΠΣ.

Αντίθετα, οι απειλές στην ιδιωτικότητα που προκαλούνται από την εφαρμογή και την ευρεία χρήση των εφαρμογών Web 2.0 και των διαδραστικών δυνατοτήτων που παρέχουν στους χρήστες απαιτούν καινοτόμες λύσεις καθώς δεν είναι δυνατό να αντιμετωπιστούν με την εφαρμογή τεχνολογιών ασφάλειας. Για το λόγο αυτό οι απειλές ιδιωτικότητας που αφορούν στη συμπεριφορά των χρηστών στα πλαίσια λειτουργίας του συνεργατικού περιβάλλοντος αποτελούν ένα ανοιχτό ερευνητικό πεδίο και τον βασικό άξονα στον οποίο επικεντρώνεται η μελέτη ιδιωτικότητας που ακολουθεί.

5.3.1 Απειλές ιδιωτικότητας σε συνεργατικά περιβάλλοντα

Οι απειλές ιδιωτικότητας που εμφανίζονται στα πλαίσια λειτουργίας του ΕΣΠΣ και κάθε συνεργατικού περιβάλλοντος προκύπτουν κατά κύριο λόγο από τις διαδραστικές δυνατότητες που παρέχουν στους χρήστες οι εφαρμογές Web 2.0. Αποτελούν μάλιστα μια νέα κατηγορία απειλών, καθώς μέχρι πριν την εξέλιξη και ευρεία χρήση των τεχνολογιών Web 2.0 δεν υπήρχε η δυνατότητα «ανεξέλεγκτης» δημιουργίας και δημοσίευσης περιεχομένου, και, συνεπώς, ο κίνδυνος καταπάτησης της ιδιωτικότητας από τους ίδιους τους χρήστες ήταν ανύπαρκτος.

Με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάζονται στην ενότητα 2.3.2 το πρόβλημα εντοπίζεται κυρίως στην έλλειψη ολοκληρωμένων λύσεων διαχείρισης ταυτοτήτων και στην αδυναμία των παραδοσιακών προσεγγίσεων να παρέχουν μηχανισμούς δυναμικής απόδοσης δικαιωμάτων προσπέλασης ανάλογα με το κατά πόσο οι χρήστες σέβονται την ιδιωτικότητα των υπολοίπων συμμετεχόντων και κατά συνέπεια δικαιούνται να χρησιμοποιούν τις διαδραστικές λειτουργίες [18].

Πιο συγκεκριμένα, η διατριβή εντοπίζει τις ακόλουθες απειλές, οι οποίες αφορούν σε κάθε συνεργατικό περιβάλλον:

- *Παραπληροφόρηση:* Μέσω της χρήσης των εφαρμογών Web 2.0 είναι δυνατή η δημιουργία και εξάπλωση λανθασμένων ειδήσεων με απώτερο στόχο την εξυπηρέτηση των συμφερόντων του κακόβουλου χρήστη.
- *Προσβολή ευαίσθητων δεδομένων:* Για κάθε χρήστη που συμμετέχει στο συνεργατικό περιβάλλον υπάρχει ο κίνδυνος προσβολής της ιδιωτικότητάς του (π.χ. θρησκεία, εθνικότητα, οικογενειακή κατάσταση) από το περιεχόμενο που δημοσιεύουν οι υπόλοιποι συμμετέχοντες.
- *Δυσφήμιση:* Κακόβουλοι χρήστες έχουν τη δυνατότητα να αλλοιώνουν τη φήμη άλλων χρηστών ή ακόμα και του Παρόχου Υπηρεσιών διαχέοντας ψευδή σχόλια και κριτικές.
- *Προπαγάνδα/Παραπλάνηση:* Μέσω της δημιουργίας περιεχομένου το οποίο περιέχει διαστρεβλωμένες πληροφορίες κακόβουλοι χρήστες στοχεύουν στην προπαγάνδα και την παραπλάνηση της κοινής γνώμης.
- *Συκοφαντία:* Μέσω της δημιουργίας κακόβουλου περιεχομένου το οποίο περιέχει ψευδείς πληροφορίες υπάρχει ο κίνδυνος συκοφαντίας χρηστών ή άλλων οντοτήτων.
- *Αποκάλυψη προσωπικών πληροφοριών:* Η χρήση εφαρμογών Web 2.0 δίνει τη δυνατότητα στους χρήστες να αποκαλύπτουν, είτε ακούσια είτε εσκεμμένα, προσωπικές πληροφορίες των ίδιων ή άλλων χρηστών.
- *Αλλοίωση βαθμού αξιοπιστίας:* Σε συνεργατικά περιβάλλοντα που ενσωματώνουν μηχανισμούς αξιολόγησης της αξιοπιστίας των χρηστών υπάρχει ο κίνδυνος συνεργασίας μεταξύ κακόβουλων χρηστών με κοινό στόχο την τροποποίηση του βαθμού αξιοπιστίας με μη εξουσιοδοτημένο τρόπο.
- *Υποβάθμιση ποιότητας παρεχομένων υπηρεσιών:* Χρησιμοποιώντας συστηματικά τις εφαρμογές Web 2.0 με τρόπο που προσβάλλει την ιδιωτικότητα, δημιουργείται ο κίνδυνος απαξίωσης των παρεχομένων υπηρεσιών λόγω της αποστροφής των χρηστών στο να συμμετέχουν στο συνεργατικό περιβάλλον.

Με βάση τις παραπάνω απειλές ιδιωτικότητας στην επόμενη ενότητα παρουσιάζονται οι αντίστοιχες επιθέσεις που καλείται να αντιμετωπίσει αποτελεσματικά το ΕΣΠΣ καθώς και κάθε συνεργατικό περιβάλλον.

5.3.2 Επιθέσεις ιδιωτικότητας

Δεδομένου ότι οι παραδοσιακές επιθέσεις σε συστήματα διαχείρισης ταυτοτήτων δεν αποτελούν πλέον ανοιχτό ερευνητικό πεδίο (βλ. ενότητα 2.4.2), η μελέτη ιδιωτικότητας όσον αφορά στο ΣΔΤΕΠ επικεντρώνεται στις επιθέσεις ιδιωτικότητας που αφορούν στα *Συστήματα Διαχείρισης Αξιοπιστίας*, καθώς όπως παρουσιάζεται και στο έκτο κεφάλαιο η χρήση τους σε συνεργατικά περιβάλλοντα αποτελεί αδήριτη ανάγκη για τη διασφάλιση της εμπιστοσύνης μεταξύ των χρηστών [16, 17]. Επιπρόσθετα, εντοπίζονται οι επιθέσεις ιδιωτικότητας που προκαλούνται από τις δυνατότητες δημιουργίας περιεχομένου που παρέχουν στους χρήστες οι εφαρμογές Web 2.0 του ΣΣΚΑ [4].

➤ **Επίθεση Whitewashing**

Στην επίθεση *Whitewashing* ο χρήστης που έχει αποκτήσει χαμηλό βαθμό αξιοπιστίας απαλλάσσεται από αυτόν διαγράφοντας την ταυτότητα που είχε και δημιουργώντας ένα νέο προφίλ. Συστήματα που επιτρέπουν την εύκολη δημιουργία ψηφιακών ταυτοτήτων είναι ευάλωτα σ' αυτή την επίθεση. Γενικά, στα συνεργατικά περιβάλλοντα είναι περιορισμένη η υιοθέτηση μηχανισμών ταυτοποίησης των χρηστών οπότε ευνοούνται τέτοιου είδους επιθέσεις. Μια εκδοχή της επίθεσης αυτής ονομάζεται και *'strike and recharge'* κατά την οποία ο επιτιθέμενος χτίζει μια καλή αξιοπιστία στην αρχή ώσπου ξαφνικά συμπεριφέρεται διαφορετικά.

➤ **Επίθεση Sybil**

Στην επίθεση *Sybil* ο χρήστης δημιουργεί πολλαπλές ψηφιακές ταυτότητες (*Sybil*s) με στόχο να μπορεί να αλλοιώσει την αξιοπιστία άλλων χρηστών ή να επηρεάσει το βαθμό αξιοπιστίας σε κάποια από αυτές. Για παράδειγμα, η κακόβουλη χρήση πολλαπλών ταυτοτήτων είναι σε θέση να αυξήσει ή να μειώσει το *βαθμό αξιοπιστίας* ενός χρήστη και μάλιστα με εξουσιοδοτημένο τρόπο. Η κύρια ευπάθεια σε τέτοιες επιθέσεις είναι η ευκολία στη δημιουργία πολλαπλών προφίλ.

➤ **Πλαστοπροσωπία**

Όταν ένας χρήστης αποκτά πρόσβαση με μη εξουσιοδοτημένο τρόπο στην ταυτότητα ενός άλλου χρήστη είναι σε θέση να υποκλέψει και να εκμεταλλευτεί το *βαθμό αξιοπιστίας* του. Ο σκοπός του επιτιθέμενου μπορεί να είναι διττός: Να επωφεληθεί από τα προνόμια που αποκτά, ή να λειτουργήσει με συκοφαντικό τρόπο για το θύμα. Η ευθύνη για τον περιορισμό αυτής της επίθεσης επιβαρύνει το κεντρικό σύστημα διαχείρισης ταυτοτήτων το οποίο θα πρέπει να ενσωματώνει ισχυρούς μηχανισμούς για την προστασία των ψηφιακών ταυτοτήτων.

➤ **Επιθέσεις συνωμοσίας**

Η επίθεση αυτή προϋποθέτει τη συνεργασία πολλών χρηστών οι οποίοι συνωμοτούν προκειμένου να επηρεάσουν το *βαθμό αξιοπιστίας* του θύματος. Αυτό επιτυγχάνεται είτε δυσφημίζοντας το θύμα σε άλλους χρήστες είτε χρησιμοποιώντας συκοφαντίες και παραπληροφόρηση προκειμένου να μειώσουν το βαθμό αξιοπιστίας του με έμμεσο τρόπο. Μάλιστα οι επιθέσεις αυτές είναι ιδιαίτερα επικίνδυνες, καθώς όταν διενεργούνται συστηματικά και με προσχεδιασμένο τρόπο είναι δυνατό να πλήξουν ακόμα και την ποιότητα των παρεχομένων υπηρεσιών και τη φήμη του Παρόχου.

➤ **Επιθέσεις ανώνυμων χρηστών**

Η απουσία διαδικασιών αυθεντικοποίησης δίνει το δικαίωμα σε ανώνυμους χρήστες να συμμετέχουν ισότιμα στο συνεργατικό περιβάλλον με σκοπό τη συκοφαντία, τη δυσφήμιση, την προπαγάνδα ή ακόμα και την προσβολή ευαίσθητων δεδομένων. Επίσης, η παροχή διαδραστικών υπηρεσιών οι οποίες επιτρέπουν τη συμμετοχή ανώνυμων χρηστών καθιστά εύκολη τη χρήση τους για κλοπή στοιχείων ταυτότητας καθώς και για παρενόχληση ή προσβολή του θύματος. Οι επιπτώσεις αυξάνονται ανάλογα με το βαθμό δυσκολίας στη διαγραφή δημοσιευμένων πληροφοριών και την ανεπάρκεια των μηχανισμών προστασίας της ιδιωτικότητας.

➤ **Επιθέσεις με χρήση πολλαπλών ταυτοτήτων**

Μια ευρέως διαδεδομένη πρακτική ταυτοποίησης των χρηστών στα πλαίσια των εφαρμογών Web 2.0 είναι συνήθως με τη συμπλήρωση μιας φόρμας με το *Όνομα Χρήστη* και τον *Κωδικό*. Αυτή η προσέγγιση αποτελεί μια ιδιαίτερα επισφαλής μέθοδο καθώς καθιστά εύκολη τη δημιουργία πολλαπλών προφίλ από κακόβουλους χρήστες έτσι ώστε να έχουν τη δυνατότητα να επηρεάζουν το βαθμό αξιοπιστίας τους μέσω επιθέσεων Sybil και Whitewashing.

➤ **Επιθέσεις από νόμιμα εξουσιοδοτημένους χρήστες**

Οι ελλιπείς διαδικασίες αυθεντικοποίησης και εξουσιοδότησης αποτελούν κίνδυνο για την ιδιωτικότητα των χρηστών καθώς δεν παρέχουν τη δυνατότητα επιβολής περιοριστικών μέτρων σε κακόβουλους χρήστες. Στα σύγχρονα συνεργατικά περιβάλλοντα, όταν η απόδοση προνομίων προσπέλασης των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0 γίνεται με βάση τους ρόλους των χρηστών και όχι με βάση την αξιοπιστία τους στη δημιουργία περιεχομένου το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων, υπάρχει ο κίνδυνος νόμιμα εξουσιοδοτημένοι χρήστες να ενεργούν συστηματικά με κακόβουλο τρόπο.

5.3.3 Μέτρα προστασίας

Με βάση τις απειλές ιδιωτικότητας που παρουσιάστηκαν στην ενότητα 5.3.1 και τις αντίστοιχες επιθέσεις που είναι δυνατόν να πραγματοποιηθούν στα πλαίσια λειτουργίας του ΕΣΠΣ (βλ ενότητα 0), πιο κάτω παρουσιάζονται τα μέτρα προστασίας της ιδιωτικότητας που προκύπτουν από τα αποτελέσματα της έρευνας πεδίου που πραγματοποιήθηκε στο πλαίσιο της διατριβής.

➤ Ψευδωνυμία

Η ψευδωνυμία αποτελεί μια κρίσιμη συνιστώσα της ιδιωτικότητας η οποία είναι ικανή να βελτιώνει την αποτελεσματικότητα των ΣΔΑ καθώς περιορίζει τον φόβο των χρηστών στο να διατυπώσουν ελεύθερα την αρνητική τους γνώμη. Αυτό είναι δυνατόν να επιτευχθεί ολοκληρώνοντας με αποτελεσματικό τρόπο το ΣΔΑ στο Σύστημα Διαχείρισης Ταυτοτήτων ώστε να παρέχεται η δυνατότητα στους χρήστες να επιλέγουν ψευδώνυμα κατά την ταυτοποίηση τους στο συνεργατικό περιβάλλον.

➤ Ενσωμάτωση βαθμού αξιοπιστίας στα διαπιστευτήρια ασφάλειας

Ενσωματώνοντας το βαθμό αξιοπιστίας στα διαπιστευτήρια ασφάλειας ως χαρακτηριστικό της ταυτότητας των χρηστών, είναι δυνατή η απόδοση προνομίων προσπέλασης στις υπηρεσίες Web 2.0 με δυναμικό τρόπο, αξιολογώντας την αξιοπιστία τους κάθε χρονική στιγμή και όχι με βάση το ρόλο που έχουν λάβει κατά την αυθεντικοποίησή τους στο συνεργατικό περιβάλλον.

➤ Ισχυρές διαδικασίες ταυτοποίησης

Στα πλαίσια λειτουργίας του ΕΣΠΣ θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί ταυτοποίησης των χρηστών, ώστε να παρέχεται προστασία από επιθέσεις whitewashing, επιθέσεις sybil και άλλες αυτοματοποιημένες μεθόδους. Ένα παράδειγμα τέτοιων μέτρων προστασίας αποτελεί η σύνδεση της ψηφιακής ταυτότητας με έναν έγκυρο λογαριασμό ηλεκτρονικού ταχυδρομείου. Επίσης, θα πρέπει η όλη διαδικασία να είναι αρκετά χρονοβόρα ώστε να αποθαρρύνεται η συχνή χρήση της για δημιουργία πολλαπλών ταυτοτήτων.

➤ Ενσωμάτωση και προτυποποίηση ΣΔΑ με το ΣΔΤΕΠ

Δεδομένου του κρίσιμου ρόλου του ΣΔΑ για την αξιολόγηση της συμπεριφοράς των χρηστών σε συνεργατικά περιβάλλοντα, το ΣΔΑ θα πρέπει απαραίτητα να ενσωματώνεται στην αρχιτεκτονική του ΣΔΤΕΠ και να συμμετέχει στις διαδικασίες ελέγχου πρόσβασης και απόδοσης προνομίων προσπέλασης. Για να είναι επιτυχημένη και αξιόπιστη αυτή η προσέγγιση θα πρέπει να εφαρμόζονται σύγχρονα πρότυπα και προδιαγραφές (π.χ. WS-Security, WS-Trust [28], SAML [29], WS-Federation [30]), ώστε να διασφαλίζονται τα απαραίτητα επίπεδα ασφάλειας και διαλειτουργικότητας.

➤ **Χρήση ισχυρών μηχανισμών αυθεντικοποίησης**

Οι ισχυροί μηχανισμοί αυθεντικοποίησης που παρέχουν τα ολοκληρωμένα *Συστήματα Διαχείρισης Ταυτοτήτων* βοηθούν στο να προστατευθούν τα ευαίσθητα δεδομένα των χρηστών και για το λόγο αυτό θα πρέπει να αποτελούν βασικό χαρακτηριστικό κάθε συνεργατικού περιβάλλοντος. Δύο από τα σημαντικότερα μέτρα προστασίας τα οποία θα πρέπει επίσης να λαμβάνονται υπόψιν είναι η ενσωμάτωση των μηχανισμών αυθεντικοποίησης στις εφαρμογές Web 2.0 στις διαδικασίες που ισχύουν για όλο το Πληροφοριακό Σύστημα και η παροχή ασφαλών διεπαφών.

➤ **Προστασία ενάντια στην αυτόματη δημιουργία περιεχομένου**

Τεχνολογίες όπως αυτή των CAPTCHAs, οι οποίες περιορίζουν την ανεξέλεγκτη χρήση των εφαρμογών Web 2.0 μόνο σε φυσικούς χρήστες και όχι σε εξωτερικές οντότητες οι οποίες επιθυμούν να εκμεταλλευτούν τη δυνατότητα αυτόματης δημιουργίας κακόβουλου περιεχομένου, αποτελούν ένα απαραίτητο μέσο προστασίας το οποίο θα πρέπει να υιοθετείται.

➤ **Χρήση SAML**

Υπολογίζοντας το συνολικό βαθμό αξιοπιστίας που συγκεντρώνει ο κάθε χρήστης με βάση τις απόψεις των υπολοίπων συμμετεχόντων είναι εφικτή η έμπιστη εξουσιοδότηση εντός του συνεργατικού περιβάλλοντος και η εφαρμογή διαδικασιών δυναμικού ελέγχου προσπέλασης. Σαν βασικό μέτρο προστασίας και διαχείρισης αυτού του χαρακτηριστικού της ταυτότητας προτείνεται η ενσωμάτωσή του σε διαπιστευτήρια ασφάλειας SAML, ώστε να υποστηρίζεται με ασφαλή και διαλειτουργικό τρόπο η ανταλλαγή των δεδομένων και να μην είναι εφικτή η μη εξουσιοδοτημένη τροποποίησή τους κατά τη μεταφορά.

5.4 Σχέδιο Ιδιωτικότητας ΕΣΠΣ

Έχοντας ολοκληρώσει τη μελέτη ιδιωτικότητας με την καταγραφή των απειλών που αντιμετωπίζουν τα κρίσιμα συστήματα που ενσωματώνει το ΕΣΠΣ καθώς και την ανάλυση των αντίστοιχων επιθέσεων και μέτρων προστασίας, η συνεισφορά της διατριβής σε αυτόν τον ερευνητικό άξονα καταλήγει με τον καθορισμό ενός ολοκληρωμένου *Σχεδίου Ιδιωτικότητας (ΣΙΑ-ΕΣΠΣ)*.

Στόχος είναι με βάση τα αποτελέσματα της μελέτης που παρουσιάστηκαν στην προηγούμενη ενότητα αρχικά να προσδιοριστούν τα ευάλωτα σημεία του ΕΣΠΣ, καθώς και κάθε συνεργατικού περιβάλλοντος, και στη συνέχεια για τα πεδία εκείνα στα οποία δεν υπάρχουν μέχρι στιγμής διαθέσιμα μέτρα προστασίας να προταθούν νέες καινοτόμες λύσεις ικανές να καλύπτουν τις ιδιαίτερες απαιτήσεις ιδιωτικότητας που χαρακτηρίζουν τις εφαρμογές Web 2.0.

Απειλές	Επιθέσεις	Αντίμετρα	Καινοτόμες Λύσεις
Υποβάθμιση ποιότητας παρεχομένων υπηρεσιών	Sybil	Ισχυρές διαδικασίες ταυτοποίησης	Αρχιτεκτονική διαχείρισης ταυτοτήτων Κεντρικοποιημένης Ομοσπονδίας. βλ. ενότητα 6.3
Προσβολή ευαίσθητων δεδομένων	Whitewashing	Ενσωμάτωση βαθμού αξιοπιστίας στα διαπιστευτήρια ασφάλειας	
Προπαγάνδα / Παραπλάνηση	Πλαστοπροσωπίας	Ψευδωνυμία	Χρήση ΣΔΑ για την αξιολόγηση της αξιοπιστίας των χρηστών με βάση το μοντέλο Δυναμικού Ελέγχου Προσπέλασης. βλ. ενότητες 6.4, 6.5
Συκοφαντία	Από νόμιμα εξουσιοδοτημένους χρήστες	Ισχυροί μηχανισμοί αυθεντικοποίησης	
Δυσφήμιση	Με χρήση πολλαπλών ταυτοτήτων	Ενσωμάτωση ΣΔΑ στα συστήματα διαχείρισης ταυτοτήτων	
Αποκάλυψη προσωπικών πληροφοριών	Ανώνυμων χρηστών	CAPTCHA	Αναδρομική μέθοδος υπολογισμού του βαθμού αξιοπιστίας. βλ. ενότητα 6.6
Αλλοίωση βαθμού αξιοπιστίας	Συνωμοσίας	Χρήση SAML	
Παραπληροφόρηση			

Πίνακας 3: Σχέδιο Ιδιωτικότητας ΕΣΠΣ

Στην τελευταία στήλη του Πίνακας 3 παρουσιάζεται η συνεισφορά της διατριβής για την κάλυψη των θεμάτων που δεν καλύπτονται από τις παραδοσιακές λύσεις ασφάλειας και γίνεται αναφορά στις ενότητες που παρουσιάζονται τα αντίστοιχα αποτελέσματα. Επιγραμματικά αναφέρεται ότι η παρουσίαση των αποτελεσμάτων γίνεται με λεπτομέρεια στο επόμενο κεφάλαιο όπου παρουσιάζεται μια καινοτόμος λύση διαχείρισης ταυτοτήτων και προστασίας της ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

5.5 Συμπεράσματα

Οι παραδοσιακές προσεγγίσεις διαχείρισης ταυτοτήτων δεν είναι αρκετές για να καλύψουν αποτελεσματικά τις απαιτήσεις ιδιωτικότητας που επιφέρει η εξάπλωση των εφαρμογών Web 2.0. Οι δυνατότητες διαδραστικότητας και κοινωνικής αλληλεπίδρασης δημιουργούν νέες προκλήσεις που αφορούν στην προστασία των προσωπικών δεδομένων από την ασυνείδητη ή κακόβουλη αποκάλυψή τους από τους ίδιους τους χρήστες.

Με βάση τις απειλές ιδιωτικότητας που παρουσιάστηκαν στην ενότητα 5.3.1, εντοπίζεται η ανάγκη ότι στα πλαίσια εφαρμογής του ΕΣΠΣ, η απόδοση δικαιωμάτων προσπέλασης θα πρέπει να γίνεται αξιολογώντας δυναμικά χαρακτηριστικά της ταυτότητας των χρηστών και όχι τους στατικά προκαθορισμένους ρόλους τους. Η διατριβή προτείνει ότι για να καλυφθεί αυτή η ανάγκη απαιτούνται καινοτόμες λύσεις διαχείρισης ταυτοτήτων οι οποίες θα

περιλαμβάνουν κατάλληλες διαδικασίες για τη διαχείριση του βαθμού αξιοπιστίας των χρηστών ως κριτήριο αξιολόγησης της συμπεριφοράς τους στη χρήση των υπηρεσιών Web 2.0. Για το λόγο αυτό είναι απαραίτητη η αναβάθμιση των σύγχρονων *Συστημάτων Διαχείρισης Ταυτοτήτων* έτσι ώστε να ενσωματώνουν κατάλληλα σχεδιασμένα *Συστήματα Διαχείρισης Αξιοπιστίας* και να επιτρέπουν το δυναμικό έλεγχο προσπέλασης.

Αναλύοντας τα αποτελέσματα που προέκυψαν από τη μελέτη ιδιωτικότητας, τα οποία παρουσιάζονται στον Πίνακα 3, διαπιστώνεται ότι η υλοποίηση του ΣΙΑ-ΕΣΠΣ με σκοπό την εφαρμογή αξιόπιστων πολιτικών και ολοκληρωμένων λύσεων ιδιωτικότητας απαιτεί:

- Μια καινοτόμο αρχιτεκτονική Διαχείρισης Ταυτοτήτων, ικανή να καλύπτει τις απαιτήσεις για διαλειτουργικότητα, ασφάλεια και ιδιωτικότητα που χαρακτηρίζουν τα συνεργατικά περιβάλλοντα.
- Την αναβάθμιση του παραδοσιακού μοντέλου απόδοσης προνομίων προσπέλασης με βάση τους ρόλους, ενσωματώνοντας μηχανισμούς δυναμικής αξιολόγησης του βαθμού αξιοπιστίας όταν πρόκειται για αποφάσεις εξουσιοδότησης που αφορούν υπηρεσίες Web 2.0.
- Τον καθορισμό μιας αναδρομικής μεθόδου υπολογισμού του βαθμού αξιοπιστίας, η οποία εκτός από τη συνεισφορά των χρηστών για την αναφορά κακόβουλου περιεχομένου θα αξιολογεί και άλλους κρίσιμους παράγοντες (π.χ. τη συχνότητα χρήσης των υπηρεσιών, το βαθμό συμμόρφωσης του χρήστη, τη συμμετοχή του στο συνεργατικό περιβάλλον) ώστε να αντιμετωπίζονται αποτελεσματικά οι επιθέσεις ιδιωτικότητας που αφορούν στα ΣΔΑ.

Η συνεισφορά της διατριβής που παρουσιάζεται στο επόμενο κεφάλαιο καλύπτει τα πιο πάνω ζητήματα συνθέτοντας μια ολοκληρωμένη προσέγγιση Διαχείρισης Ταυτοτήτων, προσανατολισμένης στην προστασία της ιδιωτικότητας των χρηστών, η οποία είναι ικανή να καλύπτει τις απαιτήσεις του ΕΣΠΣ και κάθε συνεργατικού περιβάλλοντος για παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

5.6 Βιβλιογραφία

- [1] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Open Issues on Privacy and Trust in Collaborative Environments". In Proceedings of the IEEE Symposium on Computers and Communications (ISCC 2011), Kerkyra, Greece. IEEE Digital Library.
- [2] G. Pentafronimos, P. Spyridon, N. Polemi (2008). "Interoperability Testing for e-Government Web Services". In Proceedings of the Second International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008), Cairo, Egypt. ACM Publisher
- [3] Karantjias A, Papastergiou S, Polemi N (2009). Design Principles of a Secure Federated e/m-Government Framework. International Journal of Electronic Governance (IJEG), Special Issue on Users and uses of electronic governance 2(4): 402-423
- [4] M. Pekárek, S. Pöttsch (2009). "A comparison of privacy issues in collaborative workspaces and social networks", Identity in the Information Society, vol. 2 (1), pp. 81-93
- [5] M. Jensen, N. Gruschka (2010). A Survey of Attacks in the Web Services World. In C. Gutiérrez, E. Fernández-Medina, & M. Piattini (Eds.), Web Services Security Development and Architecture: Theoretical and Practical Issues. pp. 212-227, IGI Global.
- [6] S. Weiss (2009). Privacy threat model for data portability in social network applications. International Journal of Information Management, 29 (4), pp. 249-254.
- [7] H. F. EL Yamanya, M. Capretzb, D. S. Allisonb (2009). "Intelligent security and Access control framework for service oriented architecture". Information and Software Technology. Vol. 52 (2). pp. 220-236, Elsevier.
- [8] S. Preibusch, B. Hoser, S. Gürses, B. Berendt (2007). Ubiquitous social networks: opportunities and challenges for privacy-aware user modeling. Discussion Papers of DIW Berlin 698, DIW Berlin, German Institute for Economic Research

- [9] A. Nouredine, M. Damodaran (2008). "Security in web 2.0 application development". In Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services. pp. pp 681-685. Linz, Austria. ACM Publications.
- [10] S. Murugesan, "Understanding Web 2.0" (2008). IT Professional. Vol. 9 (4), pp. 34-41.
- [11] E. Franz, K. Liesebach, and K. Pfitzmann (2006). "Privacy-aware user interfaces within collaborative environments", In Proceedings of the International workshop on Context in conjunction with AVI 2006 in advanced interfaces, (CAI 06). pp. 45-48. ACM Press.
- [12] ENISA (2009). "Web 2.0 Security and Privacy". Position paper. <http://www.enisa.europa.eu/act/it/oar/web2sec/report>
- [13] The European Parliament (2002). Directive 02/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal, 2002.
- [14] S. Papastergiou, A. Karantjias, N. Polemi, (2007). "A Federated Privacy-Enhancing Identity Management System (FPE-IMS)", Proc. 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 07.
- [15] The Ponemon Institute (2007). "Survey on Identity Compliance", <http://www.ponemon.org/index.php>
- [16] ENISA (2007). "Reputation-based Systems: a security analysis", Position paper.
- [17] ENISA (2007). "Security Issues and Recommendations for Online Social Networks", Position paper.
- [18] W. Tolone, G. Ahn, T. Pai, S. Hong, (2005). "Access control in collaborative systems", ACM Computing Surveys, vol. 37 (1), pp. 29-41.
- [19] PrimeLife (2008), <http://www.primelife.eu>

- [20] A. Richter, M. Koch (2007). "Social software—Status quo und Zukunft", Technischer Bericht Nr. 2007-01, Fakultät für Informatik, Universität der Bundeswehr München.
- [21] G. Ahn and J. Lam (2005). "Managing privacy preferences for federated identity management". In Proceedings of 2005 Workshop on Digital identity management (DIM 05), pp. 28-36. ACM Press.
- [22] The Open Web Application Security Project (OWASP), www.owasp.org
- [23] T. Glaser, F. Pallas (2007). "Information Security and Knowledge Management: Solutions through Analogies?". Technical University of Berlin, Report no. 2007-18.
- [24] C. Ardagna, M. Cremonini, E. Damiani, S. Capitani, F. Frati, and P. Samarati (2006). "Privacy-Enhanced Identity Management for e-Services". Secure e-Government Web Services. pp. 162-179. Idea Group INC.
- [25] The European Parliament (1997). Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L L 024 pp. 0001 – 0008.
- [26] The European Parliament (2001). Directive 01/45/EC of the European Parliament and the Council of Ministers on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L 008, pp. 0001 – 0022.
- [27] OASIS (2005). "XACML Technical Committee: eXtensible Access Control Markup Language (XACML) Version 2.0". OASIS Standard Specification, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- [28] OASIS (2007). "Web Service Secure Exchange Technical Committee: OASIS WS-Trust 1.3". OASIS Standard Specification. <http://www.oasis-open.org>
- [29] OASIS (2007). "Technical Committee: 'Security Assertion Markup Language v.2.0". Technical Overview. OASIS Standard Specification.

- [30] OASIS (2008). WSFED Technical Committee: Web Services Federation Language Version 1.2. OASIS Standard Specification, Working Draft, <http://www.oasis-open.org>
- [31] C. Satchell, G. Shanks, S. Howard, J. Murphy (2006). "Beyond security: implications for the future of federated digital identity management systems". In Proceedings of the 20th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design activities, artefacts and environments.
- [32] D. Gollmann (2008). "Securing Web Applications. Information Security". Technical Report, 13(1), pp. 1-9. Elsevier.
- [33] S. Clauß, D. Kesdogan, T. Kölsch (2005). "Privacy enhancing identity management: protection against re-identification and profiling". In Proceedings of the 2005 workshop on Digital identity management (DIM '05), pp. 84-93, ACM Press.

Πανεπιστήμιο Πειραιώς

Κεφάλαιο 6

Διαχείριση Ταυτοτήτων σε Συνεργατικά Περιβάλλοντα

Έχοντας σαν στόχο την αντιμετώπιση των απειλών που προκύπτουν για την προστασία της ιδιωτικότητας από την κακόβουλη χρήση των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0, η συνεισφορά της διατριβής σε αυτό το κεφάλαιο αποτελείται από δύο συμπληρωματικούς άξονες οι οποίοι περιλαμβάνουν:

- 1) Αρχιτεκτονική διαχείρισης ταυτοτήτων για συνεργατικά περιβάλλοντα η οποία αναβαθμίζει τις παραδοσιακές προσεγγίσεις μέσω της αξιολόγησης της αξιοπιστίας των χρηστών για την απόδοση προνομίων προσπέλασης.
- 2) Μέθοδο υπολογισμού του βαθμού αξιοπιστίας των χρηστών όσον αφορά στη χρήση των εφαρμογών Web 2.0 η οποία αξιοποιεί τη συλλογική γνώση των συμμετεχόντων λαμβάνοντας παράλληλα υπόψιν κρίσιμους παράγοντες του συνεργατικού περιβάλλοντος.

Τα αποτελέσματα καταλήγουν με τη σύνθεση μιας καινοτόμου λύσης Διαχείρισης Ταυτοτήτων η οποία επιτρέπει τη συλλογική προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

6.1 Εισαγωγή

Με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάζονται στο δεύτερο κεφάλαιο της διατριβής, διαπιστώνεται ότι στα συνεργατικά περιβάλλοντα εμφανίζονται νέες απαιτήσεις ιδιωτικότητας, τόσο σε επιχειρησιακό όσο και σε τεχνικό επίπεδο, οι οποίες προκαλούνται από την ενσωμάτωση εφαρμογών Web 2.0 και την παροχή αντίστοιχων υπηρεσιών [11, 12].

Διαπιστώνεται επίσης ότι το κοινό χαρακτηριστικό των υπηρεσιών αλληλεπίδρασης και ο παράγοντας εκείνος ο οποίος τις καθιστά κρίσιμους πόρους στα πλαίσια λειτουργία του ΕΣΠΣ και κάθε συνεργατικού περιβάλλοντος είναι οι διαδραστικές λειτουργίες που παρέχουν στους τελικούς χρήστες.

Εξ' ορισμού, τα ιστολόγια, τα φόρουμ, τα wiki και δυνητικά οποιεσδήποτε άλλες εφαρμογές Web 2.0 προσφέρουν είτε σε ταυτοποιημένους είτε πολλές φορές σε ανώνυμους χρήστες προνόμια δημιουργίας και κοινοποίησης περιεχομένου. Πιο

συγκεκριμένα, διακρίνονται κατ' ελάχιστον οι ακόλουθες τρεις (3) βασικές διαδραστικές λειτουργίες που παρέχει κάθε εφαρμογή Web 2.0:

1. Δημιουργία περιεχομένου.
2. Προσθήκη σχολίου σε ήδη δημοσιευμένο περιεχόμενο.
3. Κοινοποίηση ήδη δημοσιευμένου περιεχομένου σε άλλα περιβάλλοντα, κοινωνικά δίκτυα ή εφαρμογές Web 2.0 εκτός του Πληροφοριακού Συστήματος.

Διαπιστώνεται ότι το σύνολο αυτών των *Διαδραστικών Υπηρεσιών και Λειτουργιών ΔΥΛ*, το οποίο δυναμικά επεκτείνεται ώστε να περιλαμβάνει και κάθε άλλη δυνατότητα δημιουργίας περιεχομένου που παρέχουν οι εφαρμογές Web 2.0, αποτελούν διαβαθμισμένους πόρους δεδομένου ότι η κακόβουλη χρήση τους είναι ικανή να οδηγήσει σε περιστατικά που προσβάλλουν την ιδιωτικότητα των χρηστών.

Από την άλλη πλευρά, στα σύγχρονα Συστήματα Διαχείρισης Ταυτοτήτων οι πολιτικές εξουσιοδότησης εφαρμόζονται με βάση τους ρόλους των χρηστών κι έτσι η πρόσβαση στις διαδραστικές λειτουργίες των εφαρμογών Web 2.0 αφενός αντιμετωπίζεται ως μια κοινή διαδικασία αφετέρου αφορά στο σύνολο των χρηστών που σύμφωνα με το ρόλο τους έχουν δικαίωμα να τις χρησιμοποιήσουν και όχι τον καθένα ξεχωριστά ανάλογα με την αξιοπιστία του κάθε χρονική στιγμή.

Δεδομένου ότι στα συνεργατικά περιβάλλοντα η προστασία της ιδιωτικότητας εξαρτάται σε μεγάλο βαθμό από τη συμπεριφορά των χρηστών που έχουν προνόμια προσπέλασης των ΔΥΛ, διαπιστώνεται η ανάγκη αναβάθμισης των σύγχρονων προσεγγίσεων διαχείρισης ταυτοτήτων και ελέγχου προσπέλασης.

Ο βασικός λόγος είναι ότι ο αρχικός ρόλος που λαμβάνει κάθε χρήστης όταν ταυτοποιείται δεν αρκεί για να περιορίσει την πρόσβαση στις υπηρεσίες αλληλεπίδρασης των εφαρμογών Web 2.0. Σε κάθε ΕΣΠΣ, κριτήριο για την απόδοση προνομίων προσπέλασης στις ΔΥΛ πρέπει να αποτελεί η αξιοπιστία του χρήστη στη δημιουργία περιεχομένου, ως συνάρτηση τόσο των αναφορών κακόβουλης συμπεριφοράς που υποβάλλουν οι υπόλοιποι χρήστες όσο και κάποιων άλλων κρίσιμων παραγόντων του συνεργατικού περιβάλλοντος όπως η συμμόρφωση του χρήστη, η συχνότητα προσπέλασης των υπηρεσιών και το ποσοστό των αναφορών ως προς τη συνολική συμμετοχή (βλ. ενότητα 6.6).

6.2 Προκλήσεις στη Διαχείριση Ταυτοτήτων

Στις σύγχρονες προσεγγίσεις διαχείρισης ταυτοτήτων που παρουσιάστηκαν στο δεύτερο κεφάλαιο, η προστασία της ιδιωτικότητας θεωρείται ως το αντιστάθμισμα μεταξύ της εμπιστοσύνης που δείχνουν οι χρήστες στους Παρόχους και της αξιοπιστίας των τελευταίων στο να τηρήσουν τις δημοσιευμένες πολιτικές και να εφαρμόσουν τους απαραίτητους μηχανισμούς

προστασίας [8, 9]. Επίσης, η έννοια της εμπιστοσύνης περιορίζεται στο να αντιπροσωπεύει το βαθμό στον οποίο οι Πάροχοι που συμμετέχουν στο πλαίσιο υπηρεσιών έχουν δικαιώματα αλληλεπίδρασης μεταξύ τους [5, 32, 38] και δεν περιλαμβάνει τις σχέσεις αλληλεπίδρασης μεταξύ χρηστών που χαρακτηρίζουν τα συνεργατικά περιβάλλοντα.

Αξιολογώντας τα αποτελέσματα της έρευνας που πραγματοποιήθηκε στο πλαίσιο της διατριβής σχετικά με την υιοθέτηση ευρέως αποδεκτών αρχιτεκτονικών διαχείρισης ταυτοτήτων για τις ανάγκες του ΕΣΠΣ, παρατηρούνται ελλείψεις όσον αφορά στην κάλυψη βασικών απαιτήσεων [34, 39, 43]. Πιο συγκεκριμένα, εντοπίζονται τρία βασικά θέματα:

1. Με βάση το σκοπό λειτουργίας του ΕΣΠΣ αν και οι δύο αρχιτεκτονικές της κεντροποιημένης (βλ. ενότητα 2.4.1.2) και ομοσπονδιακής (βλ. ενότητα 2.4.1.3) διαχείρισης ταυτοτήτων, καλύπτουν εν μέρει κάποιες βασικές απαιτήσεις, όταν υιοθετούνται ξεχωριστά δεν επαρκούν για να καλύψουν όλες τις βασικές λειτουργίες ελέγχου προσπέλασης που θα πρέπει να παρέχει το σύστημα διαχείρισης ταυτοτήτων του συνεργατικού περιβάλλοντος [13].
2. Το προσανατολισμένο στους ρόλους μοντέλο ελέγχου προσπέλασης που υιοθετείται στις αρχιτεκτονικές της κεντροποιημένης (βλ. ενότητα 2.4.1.2) και της ομοσπονδιακής διαχείρισης (βλ. ενότητα 2.4.1.3) ταυτοτήτων δεν είναι επαρκές για να διασφαλίσει την προστασία της ιδιωτικότητας των χρηστών από τη δημοσίευση προσβλητικού περιεχομένου [6].
3. Οι παραδοσιακές προσανατολισμένες στο χρήστη προσεγγίσεις διαχείρισης ταυτοτήτων (βλ. 2.4.1.4) είναι ελλιπείς για τις ανάγκες του ΕΣΠΣ καθώς δεν σχεδιάστηκαν για να ικανοποιούν τις επιπρόσθετες απαιτήσεις που προκύπτουν από την χρήση υπηρεσιών Web 2.0, όπως για παράδειγμα η δυναμική δημιουργία περιεχομένου και οι δυνατότητες αλληλεπίδρασης μεταξύ των χρηστών [10, 17].

Επίσης, παρά το γεγονός ότι τα προβλήματα αυθεντικοποίησης και ελέγχου προσπέλασης που χαρακτηρίζουν τις εφαρμογές Web 2.0 καλύπτονται με την ενσωμάτωσή τους σε ολοκληρωμένα Πληροφοριακά Συστήματα και τη διασύνδεσή τους με κεντρικά Συστήματα Διαχείρισης Ταυτοτήτων, όπως γίνεται στην αρχιτεκτονική του ΕΣΠΣ με την ενσωμάτωση του ΣΔΤΕΠ (βλ. ενότητα 4.3.2.1), όταν οι διαδικασίες εξουσιοδότησης δε λαμβάνουν υπόψιν την αξιοπιστία των χρηστών στο να χρησιμοποιούν τις υπηρεσίες Web 2.0 χωρίς να αποκαλύπτουν προσωπικά δεδομένα και να καταπατούν την ιδιωτικότητα των υπολοίπων συμμετεχόντων, η προστασία της ιδιωτικότητας είναι σε κίνδυνο.

Με βάση αυτά, κρίνεται απαραίτητη η αποτελεσματική σύνθεση και αναβάθμιση των σύγχρονων προσεγγίσεων Διαχείρισης Ταυτοτήτων με σκοπό τη δημιουργία μιας καινοτόμου αρχιτεκτονικής κατάλληλης να καλύπτει τις νέες

απαιτήσεις ιδιωτικότητας όσον αφορά στις σχέσεις εμπιστοσύνης μεταξύ των χρηστών.

Η διατριβή προτείνει ότι στα συνεργατικά περιβάλλοντα, εκτός του να λαμβάνονται αποφάσεις εξουσιοδότησης σε επίπεδο συστημάτων και υπηρεσιών με βάση στατικά προκαθορισμένους ρόλους (π.χ. επισκέπτης, εγγεγραμμένος χρήστης, διαχειριστής), όταν πρόκειται για αποφάσεις εξουσιοδότησης που αφορούν σε υπηρεσίες και εφαρμογές Web 2.0 απαιτείται ο έλεγχος προσπέλασης σε επίπεδο λειτουργιών με δυναμικό τρόπο κάθε χρονική στιγμή που ο χρήστης αιτείται να προσπελάσει το συνεργατικό περιβάλλον.

Έχοντας σαν στόχο τη συνεισφορά στην αντιμετώπιση αυτών των προκλήσεων [1, 3], στο πλαίσιο της διατριβής προτείνονται τα ακόλουθα:

- Η ιδιωτικότητα πρέπει να προστατεύεται από τη δυνατότητα των χρηστών να δημιουργούν κακόβουλο περιεχόμενο το οποίο έχει σαν συνέπεια την αποκάλυψη των προσωπικών δεδομένων των υπολοίπων συμμετεχόντων.
- Είναι αδήριτη η ανάγκη για μηχανισμούς αναφοράς της κακόβουλης συμπεριφοράς των χρηστών όσον αφορά στη χρήση των διαδραστικών λειτουργιών και εφαρμογών Web 2.0.
- Το παραδοσιακό μοντέλο ελέγχου προσπέλασης με βάση τους ρόλους δεν αρκεί για να καλύψει τις ανάγκες του ΕΣΠΣ. Το ΣΔΤΕΠ κάθε συνεργατικού περιβάλλοντος πρέπει να αξιολογεί την *αξιοπιστία* των χρηστών για την απόδοση προνομίων προσπέλασης στις εφαρμογές Web 2.0.
- Εκτός από τη συλλογική γνώση σχετικά με την *αξιοπιστία των χρηστών* στη χρήση των εφαρμογών Web 2.0 υπάρχουν και άλλοι εξίσου σημαντικοί παράγοντες (π.χ. συμμόρφωση χρήστη, συχνότητα προσπελάσεων) οι οποίοι θα πρέπει να αποτελούν κριτήρια υπολογισμού του βαθμού αξιοπιστίας ώστε να αξιολογείται με αντικειμενικό τρόπο το ενδεχόμενο ρίσκο των αποφάσεων εξουσιοδότησης.

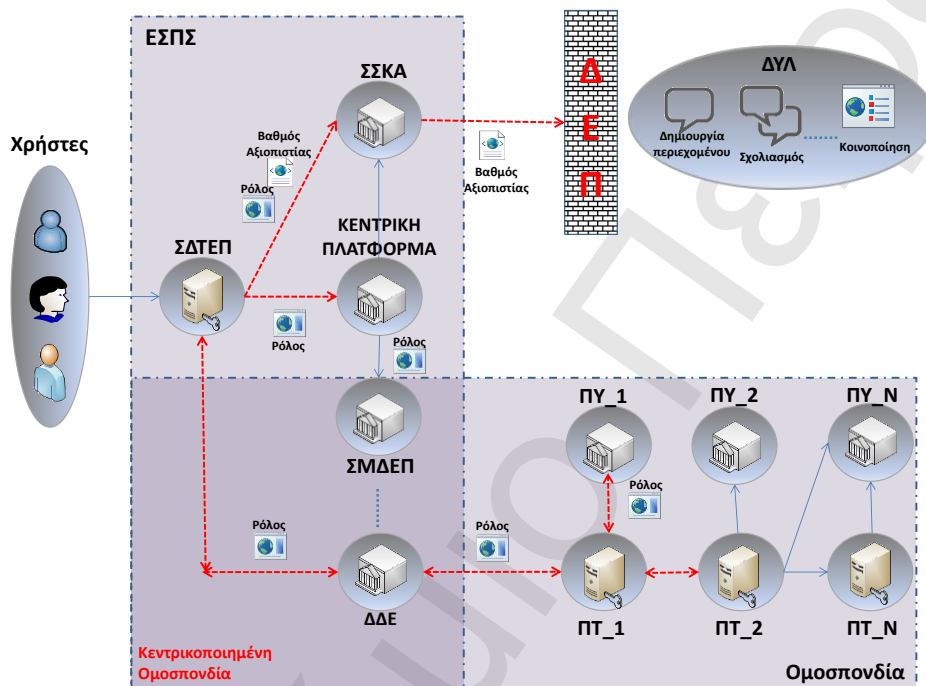
Θεμελιώδης πρόταση της διατριβής αποτελεί το γεγονός ότι στα συνεργατικά περιβάλλοντα η έννοια της εμπιστοσύνης πρέπει απαραίτητα να περιλαμβάνει και τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών. Για το σκοπό αυτό στις ενότητες που ακολουθούν ο βαθμός αξιοπιστίας αντιμετωπίζεται ως κρίσιμο χαρακτηριστικό της ταυτότητας, ικανό να καθορίσει τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον.

6.3 Αρχιτεκτονική Κεντροποιημένης Ομοσπονδίας

Στα συνεργατικά περιβάλλοντα η διαχείριση ταυτοτήτων και ο έλεγχος προσπέλασης από τη μια αποτελούν αρμοδιότητα του κεντρικού ΣΔΤΕΠ που

ενσωματώνεται στην αρχιτεκτονική του ΕΣΠΣ, από την άλλη αφορούν την ανταλλαγή διαπιστευτηρίων ασφάλειας με εξωτερικά συστήματα με τα οποία το ΣΔΤΕΠ, και κατ' επέκταση το ΕΣΠΣ, έχουν αναπτύξει σχέσεις εμπιστοσύνης.

Έτσι, όπως φαίνεται και στο Σχήμα 20, η διαχείριση ταυτοτήτων σε συνεργατικά περιβάλλοντα καταλήγει σε μια υβριδική προσέγγιση των αρχιτεκτονικών της κεντροποιημένης και της ομοσπονδιακής διαχείρισης, η οποία στο πλαίσιο της διατριβής αναφέρεται ως *Κεντροποιημένη Ομοσπονδία*.



Σχήμα 20: Αρχιτεκτονική Κεντροποιημένης Ομοσπονδίας

Όπως συμβολίζουν τα βέλη, οι διαδικασίες απόδοσης προνομίων προσπέλασης που εκτελούνται από το ΣΔΤΕΠ-ΕΣΠΣ αφορούν:

- ✓ ένα σύνολο χαρακτηριστικών της ταυτότητας του χρήστη, τα οποία αποτυπώνονται στο ρόλο του και του δίνουν τη δυνατότητα να προσπελάσει τόσο τις υπηρεσίες που παρέχουν τα συστήματα του ΕΣΠΣ όσο και τις υπηρεσίες άλλων Παρόχων που συνδέονται με το ΕΣΠΣ μέσω του ΔΔΕ.
- ✓ ένα σύνολο χαρακτηριστικών της συμπεριφοράς του χρήστη εντός του συνεργατικού περιβάλλοντος που παρέχει το ΣΣΚΑ, τα οποία αποτυπώνονται στο βαθμό αξιοπιστίας του κάθε χρονική στιγμή που αιτείται να προσπελάσει κάποια από τις υπηρεσίες Web 2.0.

Με βάση το Σχήμα 20, η διατριβή προτείνει ότι οι 2 βασικοί λόγοι για τους οποίους το ΣΔΤΕΠ του ΕΣΠΣ δεν ανήκει αποκλειστικά ούτε στο μοντέλο της κεντροποιημένης διαχείρισης ούτε στο μοντέλο στις ομοσπονδιακής διαχείρισης ταυτοτήτων είναι οι ακόλουθοι:

1. Αν και ο έλεγχος προσπέλασης μεταξύ των ΠΥ που συμμετέχουν στο ΕΣΠΣ είναι αποκλειστική αρμοδιότητα του ΣΔΤΕΠ, αυτό δεν αποκλείει τη διασύνδεση του τελευταίου με άλλους ΠΤ. Έτσι το ΣΔΤΕΠ δεν ανήκει αποκλειστικά στην κατηγορία των κεντροποιημένων αρχιτεκτονικών καθώς μέσω της ολοκλήρωσής του με τον ΔΔΕ είναι σε θέση να αλληλεπιδρά με εξωτερικές του ΕΣΠΣ οντότητες και να συμμετέχει σε ομοσπονδίες υπηρεσιών.
2. Αν και το ΣΔΤΕΠ είναι σε θέση να αλληλεπιδρά με άλλους ΠΤ και να παρέχει υπηρεσίες *Καθολικής Σύνδεσης* και *Ομοσπονδίας Ταυτοτήτων* με εξωτερικά Πληροφοριακά Συστήματα, το γεγονός ότι, όπως παρουσιάζεται στην επόμενη ενότητα, δε βασίζεται αποκλειστικά στο προσανατολισμένο στους ρόλους μοντέλο ελέγχου προσπέλασης (βλ. ενότητα 6.3.3), απαγορεύει την ανταλλαγή διαπιστευτηρίων ασφάλειας απευθείας μεταξύ των ΠΥ του ΕΣΠΣ και των ΠΤ της ομοσπονδίας ταυτοτήτων. Η διαμεσολάβηση του ΣΔΤΕΠ είναι άκρως απαραίτητη για τη διαχείριση της αξιοπιστίας των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον του ΕΣΠΣ και την απόδοση προνομίων προσπέλασης στις ΔΥΛ που παρέχει το ΣΣΚΑ. Έτσι, δεδομένου ότι η πρόσβαση στους ΠΥ του ΕΣΠΣ γίνεται μόνο μέσω του ΣΔΤΕΠ, το τελευταίο δεν ανήκει αποκλειστικά στην κατηγορία των αρχιτεκτονικών ομοσπονδιακής διαχείρισης.

Με βάση αυτά, ο λόγος για τον οποίο το ΣΔΤΕΠ του ΕΣΠΣ θα πρέπει σύμφωνα με την αρχιτεκτονική της *Κεντροποιημένης Ομοσπονδίας* να αναλαμβάνει τη διαχείριση όλων των αλληλεπιδράσεων μεταξύ των ΠΥ του ΕΣΠΣ και των εξωτερικών οντοτήτων, είναι προκειμένου να υλοποιεί αξιόπιστα τις κατάλληλες διαδικασίες απόδοσης προνομίων εξουσιοδότησης στις κρίσιμες όσον αφορά στην προστασία της ιδιωτικότητας διαδραστικές λειτουργίες των εφαρμογών Web 2.0.

Επιπρόσθετα, με βάση την προσανατολισμένη στο χρήστη προσέγγιση διαχείρισης ταυτοτήτων η αρχιτεκτονική της κεντροποιημένης ομοσπονδίας παρέχει η δυνατότητα υιοθέτησης μηχανισμών προστασίας της ιδιωτικότητας οι οποίοι υποστηρίζουν την ενεργή συμμετοχή των χρηστών για τη διασφάλιση των προσωπικών τους δεδομένων (βλ. ενότητα 6.8).

Έτσι, επιτρέποντας μεν τη διασύνδεση με άλλα Πληροφοριακά Συστήματα και ομοσπονδίες ταυτοτήτων αλλά υιοθετώντας παράλληλα τα πλεονεκτήματα της κεντροποιημένης αρχιτεκτονικής όπου υπάρχει μεγαλύτερος έλεγχος των διαδικασιών εξουσιοδότησης, το προτεινόμενο μοντέλο της *κεντροποιημένης ομοσπονδίας* είναι σε θέση να καλύπτει αποτελεσματικά τις απαιτήσεις ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

Όπως παρουσιάστηκε στην ενότητα 4.3.2.1, αυτό επιτυγχάνεται μέσω της ενσωμάτωσης ενός *Συστήματος Διαχείρισης Αξιοπιστίας* στην αρχιτεκτονική του

συστήματος διαχείρισης ταυτοτήτων του ΕΣΠΣ, και πιο συγκεκριμένα στη Μονάδα Καταγραφής και Αξιολόγησης Συμπεριφοράς (ΜΚΑΣ) ώστε να είναι εφικτή η συνεχής αξιολόγηση της συμπεριφοράς των χρηστών και η χρήση του βαθμού αξιοπιστίας για την απόδοση προνομίων προσπέλασης στις κρίσιμες για την προστασία της ιδιωτικότητας εφαρμογές Web 2.0.

6.3.1 Μοντέλο Δυναμικού Ελέγχου Προσπέλασης

Εκτός από την υιοθέτηση της αρχιτεκτονικής της κεντροποιημένης ομοσπονδίας που παρουσιάστηκε στην προηγούμενη ενότητα, η προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα προϋποθέτει την εφαρμογή ενός αναβαθμισμένου μοντέλου Δυναμικού Ελέγχου Προσπέλασης (ΔΕΠ-ΕΣΠΣ) με βάση το οποίο η έννοια της ταυτότητας έχει διττή σημασία:

- ✓ Η ταυτότητα ως ένα σύνολο στατικών χαρακτηριστικών και προσωπικών δεδομένων των χρηστών με βάση τα οποία ταυτοποιούνται και αποκτούν ρόλους και προνόμια προσπέλασης στους πόρους του ΕΣΠΣ.
- ✓ Η ταυτότητα ως ένα σύνολο δυναμικών δεδομένων σχετικών με την αξιοπιστία των χρηστών ως προς τη χρήση των διαδραστικών λειτουργιών τα οποία αλλάζουν κάθε χρονική στιγμή.

Υιοθετώντας τη θεμελιώδη αρχή ότι «η Διαχείριση Ταυτοτήτων αποτελεί τη βάση για τον Έλεγχο Προσπέλασης» προκύπτει ότι στα πλαίσια του ΔΕΠ-ΕΣΠΣ ο ρόλος των χρηστών δεν αποτελεί πλέον το μοναδικό χαρακτηριστικό της ταυτότητας με βάση το οποίο λαμβάνονται οι αποφάσεις εξουσιοδότησης.

Έχοντας σαν γνώμονα την επίτευξη εμπιστοσύνης και την προστασία της ιδιωτικότητας μεταξύ των χρηστών, όπως παρουσιάζεται στις ενότητες που ακολουθούν, το μοντέλο ΔΕΠ-ΕΣΠΣ επιτρέπει τη δυναμική απόδοση προνομίων προσπέλασης των υπηρεσιών του συνεργατικού περιβάλλοντος αξιολογώντας την αξιοπιστία των χρηστών στη δημιουργία και την κοινοποίηση περιεχομένου.

6.3.2 Οντότητες και πόροι

Το σύνολο των *Οντοτήτων*, O , που συμμετέχουν σε ένα συνεργατικό περιβάλλον αποτελείται από το σύνολο των *Χρηστών*, X , που αιτούνται να προσπελάσουν τους διαθέσιμους πόρους και το σύνολο των *Παρόχων*, Π , οι οποίοι τους διαχειρίζονται. Οι *Πάροχοι* ενδέχεται να είναι είτε *Πάροχοι Υπηρεσιών*, $ΠΥ$, οι οποίοι διαθέτουν τους πόρους, είτε *Πάροχοι Ταυτοτήτων*, $ΠΤ$, οι οποίοι ελέγχουν την προσπέλαση σε αυτούς. Πιο συγκεκριμένα:

$$O = X \cup \Pi \quad \text{και} \quad \Pi = ΠΥ \cup ΠΤ$$

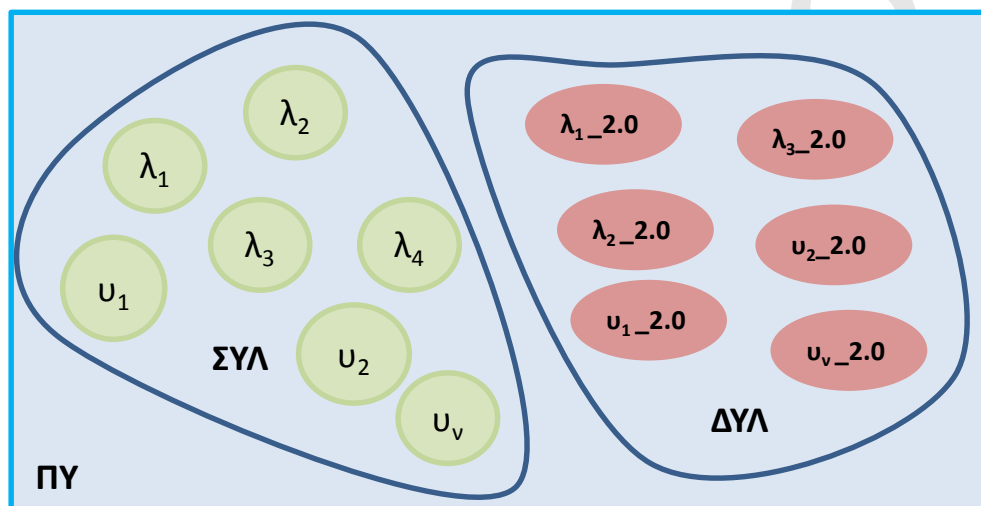
Το σύνολο των πόρων, των *Υπηρεσιών*, $Υ$, και των *Λειτουργιών*, $Λ$, που γίνονται διαθέσιμοι από τους Παρόχους Υπηρεσιών, $ΠΥ$, στα πλαίσια του συνεργατικού

περιβάλλοντος, αποτελείται από τα υποσύνολα των πόρων που παρέχει κάθε Πάροχος Υπηρεσιών, $ΠΥ_{\mu}$ και ισχύει ότι:

$$ΠΥ = Υ \cup Λ \quad \text{και} \quad ΠΥ_{\mu} \subseteq ΠΥ$$

Ορίζοντας ως $\DeltaΥΛ$ το σύνολο των Διαδραστικών Υπηρεσιών και Λειτουργιών που βασίζονται σε εφαρμογές Web 2.0 και ως $\SigmaΥΛ$ το σύνολο των Συμβατικών Υπηρεσιών και Λειτουργιών που δεν βασίζονται σε εφαρμογές Web 2.0 ισχύει ότι:

$$\DeltaΥΛ \subseteq ΠΥ, \quad \SigmaΥΛ \subseteq ΠΥ, \quad \text{και} \quad \SigmaΥΛ \cap \DeltaΥΛ = \emptyset$$



Σχήμα 21: Σύνολο παρεχομένων πόρων του ΕΣΠΣ

Έχοντας σαν κριτήριο την ενσωμάτωση εφαρμογών Web 2.0, όπως φαίνεται στο Σχήμα 21 τα υποσύνολα $\SigmaΥΛ$ και $\DeltaΥΛ$ δεν έχουν κανένα κοινό στοιχείο ενώ η ένωση τους *ισούται* με το σύνολο των πόρων, υπηρεσιών και λειτουργιών, που παρέχει το συνεργατικό περιβάλλον (το σύνολο των *Παρόχων Υπηρεσιών*, $ΠΥ$, που συμμετέχουν σε αυτό).

6.3.3 Σχέσεις εμπιστοσύνης και συνθήκες εξουσιοδότησης

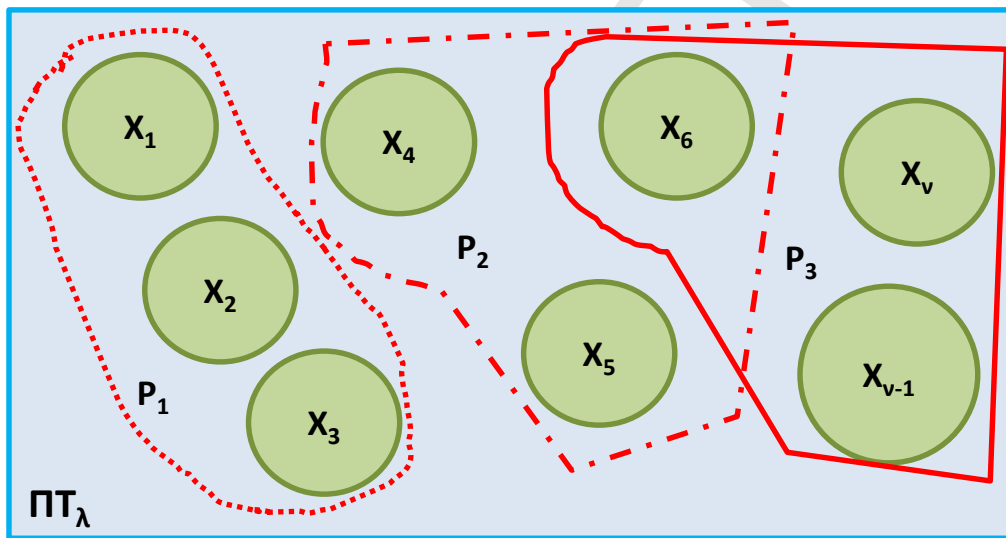
Όπως έχει ήδη αναφερθεί, με βάση την αρχιτεκτονική της *Κεντρικοποιημένης Ομοσπονδίας* (βλ. ενότητα 6.3) το σύστημα Διαχείρισης Ταυτοτήτων του ΕΣΠΣ (ΣΔΤΕΠ) ενσωματώνει ένα *Σύστημα Διαχείρισης Αξιοπιστίας (ΣΔΑ)* το οποίο καθιστά δυνατή την ενεργή συνεισφορά των χρηστών στον εντοπισμό προσβλητικού περιεχομένου. Ακολουθώντας αυτή την προσέγγιση, υποστηρίζεται η συλλογική προστασία της ιδιωτικότητας μέσω της καταγραφής των αναφορών κακόβουλης συμπεριφοράς και της αξιολόγησης του *βαθμού αξιοπιστίας* με δυναμικό τρόπο κάθε χρονική στιγμή που κάποιος χρήστης αιτείται να προσπελάσει το συνεργατικό περιβάλλον.

Στην *Κεντρικοποιημένη Ομοσπονδία* οι σχέσεις εμπιστοσύνης μεταξύ των χρηστών καθορίζονται από το *βαθμό αξιοπιστίας*, $A_i(X_n)$, κάθε χρήστη, X_n , τη

χρονική στιγμή, t , που αιτείται να προσπελάσει τις ΔΥΛ των εφαρμογών Web 2.0, ο οποίος υπολογίζεται με βάση τη μέθοδο που παρουσιάζεται στην ενότητα 6.6.

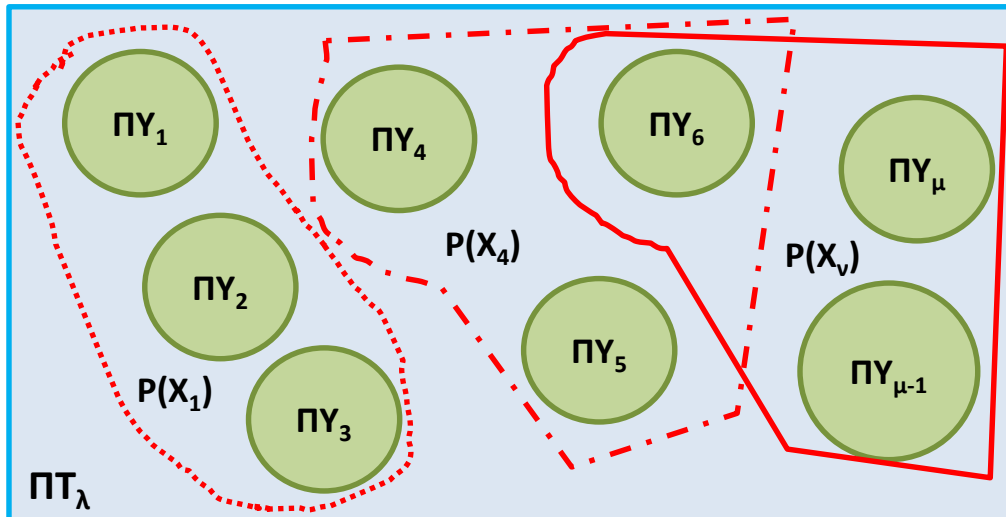
Επίσης, οι *Πάροχοι Ταυτοτήτων που συμμετέχουν στην αρχιτεκτονική της Κεντροποιημένης Ομοσπονδίας αναπτύσσουν μεταξύ τους σχέσεις εμπιστοσύνης* προκειμένου να ανταλλάσσουν διαπιστευτήρια ασφάλειας σχετικά με τους ρόλους των χρηστών όπως ορίζεται από τα πρότυπα και προδιαγραφές της ομοσπονδιακής διαχείρισης ταυτοτήτων (βλ. ενότητα 2.4.1.3).

Τέλος, όπως φαίνεται στο Σχήμα 22, με βάση τις σύγχρονες προσεγγίσεις διαχείρισης ταυτοτήτων, οι σχέσεις εμπιστοσύνης μεταξύ των χρηστών και των *Παρόχων Ταυτοτήτων* καθορίζονται από το ρόλο, P , που αποδίδεται σε κάθε χρήστη, X , ανάλογα με την ομάδα χρηστών στην οποία τον κατατάσσει ο *Πάροχος Ταυτοτήτων, ΠΤ_λ*, στον οποίο αυθεντικοποιείται.



Σχήμα 22: Ομαδοποίηση χρηστών με βάση το ρόλο τους

Επίσης, όπως φαίνεται στο Σχήμα 23, με βάση τις βασικές αρχές του παραδοσιακού μοντέλου ΕΠΡ (βλ. ενότητα 2.3.1.3) κάθε ρόλος αφορά σε ένα σύνολο πόρων, υπηρεσιών και λειτουργιών, στους οποίους επιτρέπεται η πρόσβαση για τη συγκεκριμένη ομάδα χρηστών, .



Σχήμα 23: Δικαιώματα προσπέλασης στους ΠΥ με βάση το ρόλο των χρηστών

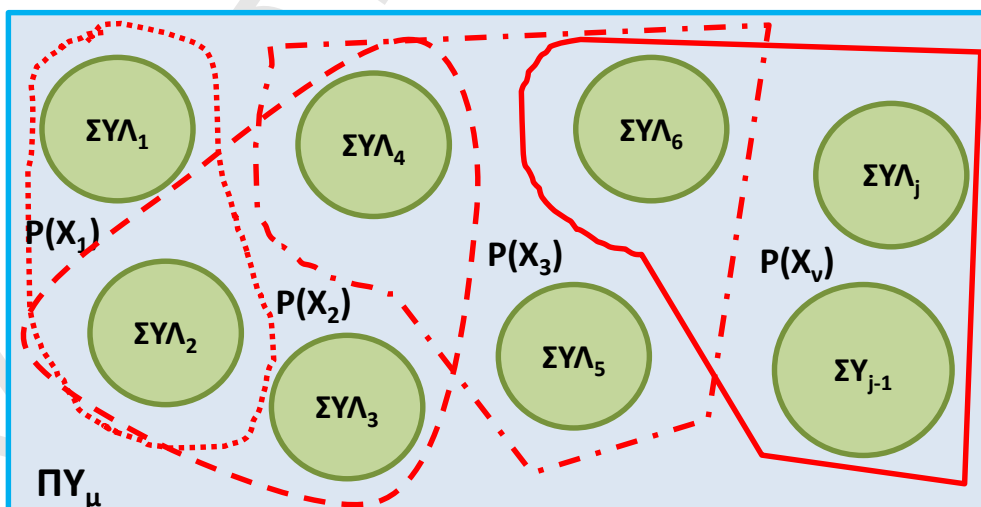
Για να έχει πρόσβαση ο χρήστης, X_v , στους πόρους του Παρόχου Υπηρεσιών, $ΠΥ_μ$, πρέπει να ισχύει η συνθήκη εξουσιοδότησης:

$$ΠΥ_μ \subseteq P(X_v), \text{ με } \mu, v \in \aleph^*.$$

Δηλαδή, το σύνολο των πόρων που παρέχει ο Πάροχος Υπηρεσιών, $ΠΥ_μ$, και τους οποίους αιτείται να προσπελάσει ο χρήστης, X_v , θα πρέπει να είναι υποσύνολο του συνόλου των πόρων, ΠΥ, στους οποίους έχει πρόσβαση με βάση το ρόλο που του έχει αποδώσει ο συγκεκριμένος Πάροχος Ταυτοτήτων, $ΠΤ_λ$, στον οποίο έχει αυθεντικοποιηθεί.

Αντίστοιχα, όπως φαίνεται στο Σχήμα 24, για να έχει πρόσβαση ο χρήστης, X_v , σε κάποιο υποσύνολο πόρων, $ΣΥΛ_j$, του Παρόχου Υπηρεσιών, $ΠΥ_μ$, που δεν βασίζονται σε εφαρμογές Web 2.0 πρέπει να ισχύει η συνθήκη εξουσιοδότησης:

$$ΣΥΛ_j \subseteq P(X_v), \text{ με } j, v \in \aleph^*.$$

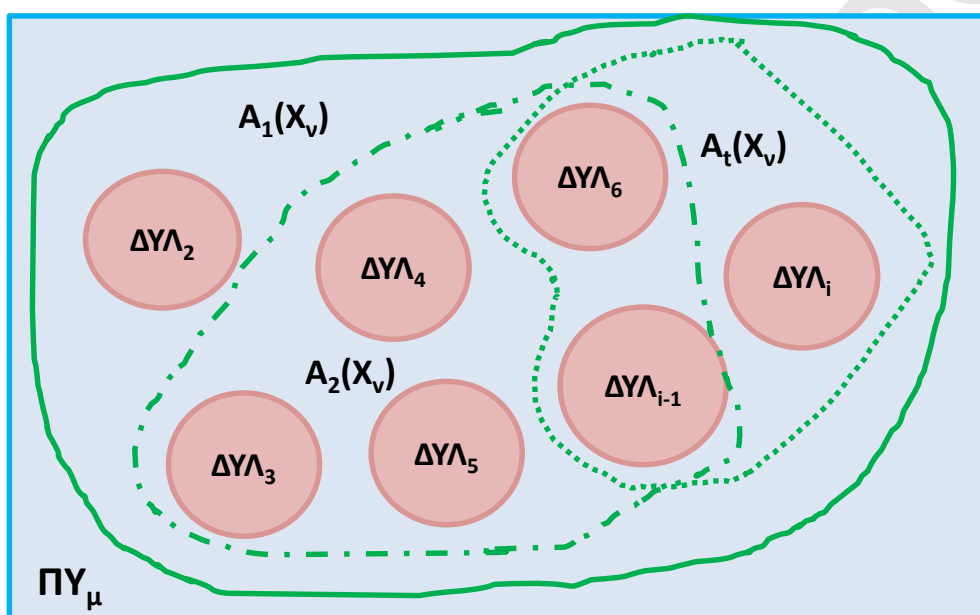


Σχήμα 24: Δικαιώματα προσπέλασης στις ΣΥΛ κάθε ΠΥ με βάση το ρόλο

Δηλαδή, το σύνολο των συμβατικών υπηρεσιών, $\Sigma\Upsilon\Lambda_i$, τις οποίες αιτείται να προσπελάσει ο χρήστης θα πρέπει να είναι υποσύνολο του συνόλου των πόρων που παρέχει ο *Πάροχος Υπηρεσιών ΠΥ_μ* στη συγκεκριμένη ομάδα χρηστών $P(X_v)$.

Αντίθετα, όπως φαίνεται στο Σχήμα 25, για να έχει πρόσβαση ο χρήστης, X_v , σε κάποιο υποσύνολο *διαδραστικών λειτουργιών, ΔΥΛ_i*, του *Παρόχου Υπηρεσιών, ΠΥ_μ*, πρέπει να ισχύει η συνθήκη εξουσιοδότησης:

$$\Delta\Upsilon\Lambda_i \subseteq A_t(X_v), \text{ με } i, t, v \in \mathcal{N}^*$$



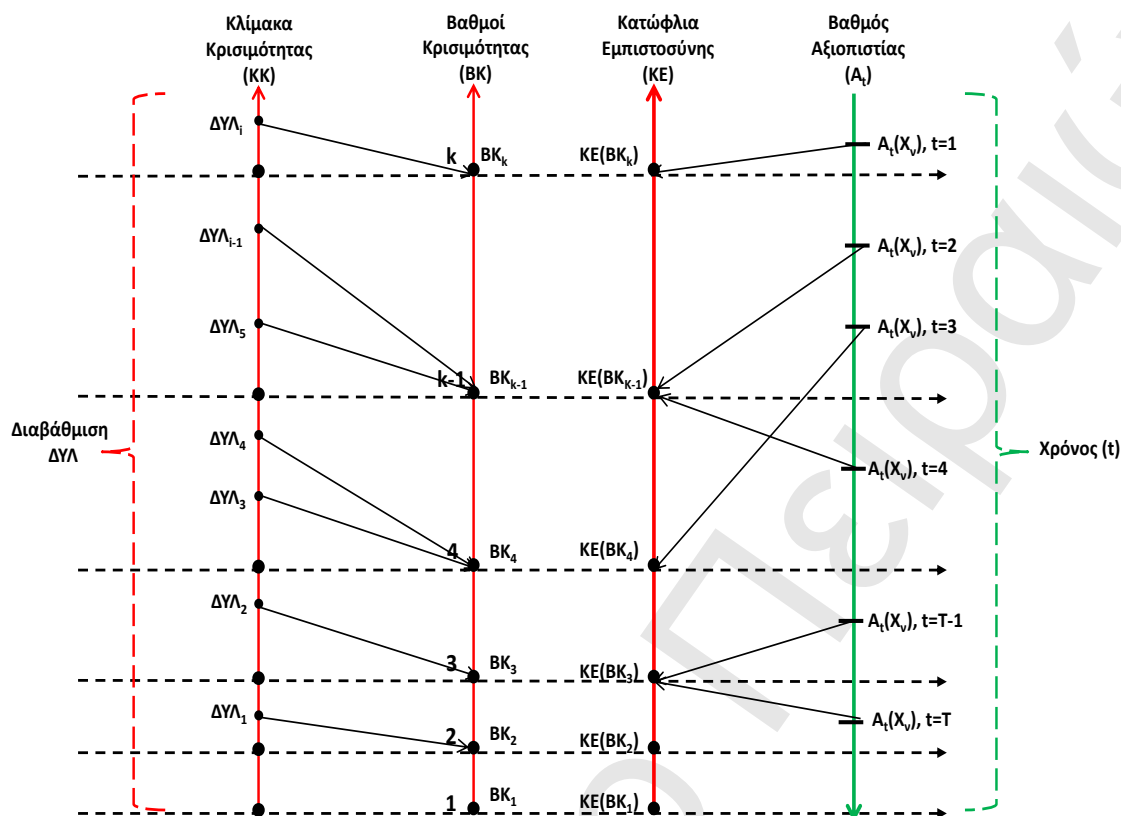
Σχήμα 25: Δικαιώματα προσπέλασης στις ΔΥΛ με βάση το βαθμό αξιοπιστίας

Όπως φαίνεται στο Σχήμα 25, αυτό σημαίνει ότι οι διαδραστικές λειτουργίες που αιτείται να προσπελάσει ο χρήστης θα πρέπει να είναι υποσύνολο του συνόλου των ΔΥΛ στις οποίες έχει πρόσβαση με βάση το βαθμό αξιοπιστίας που συγκεντρώνει τη χρονική στιγμή t .

Με βάση τα παραπάνω, το μοντέλο Δυναμικού Ελέγχου Προσπέλασης (ΔΕΠ-ΕΣΠΣ) επιτρέπει την πρόσβαση στις υπηρεσίες και τις λειτουργίες που παρέχει το συνεργατικό περιβάλλον όχι μόνο με βάση το ρόλο των χρηστών αλλά και ανάλογα με το βαθμό αξιοπιστίας που συγκεντρώνουν κάθε χρονική στιγμή, όταν πρόκειται για πόρους που βασίζονται σε εφαρμογές Web 2.0.

6.4 Λειτουργικό πλαίσιο

Το Σχήμα 26 παρουσιάζει τον τρόπο με τον οποίο καθορίζονται τα προνόμια προσπέλασης των ΔΥΛ του ΕΣΠΣ με βάση το λειτουργικό πλαίσιο του *Δυναμικού Ελέγχου Προσπέλασης (ΔΕΠ-ΕΣΠΣ)*.



Σχήμα 26: Λειτουργικό πλαίσιο ΔΕΠ-ΕΣΠΣ

Βασική προϋπόθεση για την εφαρμογή του μοντέλου ΔΕΠ-ΕΣΠΣ είναι η διαβάθμιση των ΔΥΛ με βάση την κρισιμότητά τους ως προς την ιδιωτικότητα των χρηστών, καθώς και η αναγωγή των τιμών της *Κλίμακας Κρισιμότητας* σε διακριτά επίπεδα ή *Βαθμούς Κρισιμότητας (ΒΚ)*.

Όπως φαίνεται στον πρώτο κάθετο άξονα του Σχήμα 26, τα υποσύνολα των ΔΥΛ αρχικά διαβαθμίζονται ως προς τις απαιτήσεις ιδιωτικότητας που χαρακτηρίζουν το καθένα και διατάσσονται σε αύξουσα σειρά κρισιμότητας με βάση μια ποσοτική κλίμακα διαβάθμισης. Προκειμένου να καλύπτει ένα μεγάλο εύρος μεθοδολογιών και εργαλείων αποτίμησης επικινδυνότητας η κλίμακα θεωρείται ότι είναι συνεχής και παίρνει τιμές στο διάστημα των πραγματικών αριθμών.

Στη συνέχεια, όπως φαίνεται στον δεύτερο κάθετο άξονα, γίνεται ποιοτική ανάλυση των αποτελεσμάτων διαβάθμισης των ΔΥΛ. Αυτό επιτυγχάνεται με την ομαδοποίηση των ΔΥΛ σε k διακριτά επίπεδα κρισιμότητας ή *Βαθμούς Κρισιμότητας, ΒΚ*. Η διατριβή προτείνει ότι η μέθοδος ποιοτικής ανάλυσης της διαβάθμισης των ΔΥΛ ή αλλιώς το πλήθος k των ΒΚ στους οποίους ομαδοποιούνται, πρέπει να καθορίζεται ανάλογα με το εύρος τιμών της κλίμακας διαβάθμισης και την κατανομή των ΔΥΛ στο διάστημα αυτό έτσι ώστε να προκύπτει μια κανονικοποιημένη κλίμακα ταξινόμησης.

Όπως φαίνεται από τα διαγώνια βέλη που ενώνουν τον πρώτο με τον δεύτερο κάθετο άξονα, σε κάθε βαθμό κρισιμότητας BK αντιστοιχίζονται τα υποσύνολα των ΔYL τα οποία ομαδοποιούνται στο ίδιο επίπεδο κρισιμότητας, έστω k , και κατά συνέπεια χαρακτηρίζονται από τον ίδιο Βαθμό Κρισιμότητας BK_k .

Για παράδειγμα, με βάση το Σχήμα 26 το υποσύνολο ΔYL_3 ταξινομείται στον ίδιο βαθμό κρισιμότητας με το υποσύνολο ΔYL_4 , τον BK_4 , ενώ τα ΔYL_5 και ΔYL_{i-1} ταξινομούνται στο επίπεδο κρισιμότητας $k-1$, δηλαδή έχουν βαθμό κρισιμότητας BK_{k-1} .

Στη συνέχεια, όπως φαίνεται στον τρίτο και στον τέταρτο κάθετο άξονα, για κάθε Βαθμό Κρισιμότητας BK και, κατά συνέπεια, για κάθε υποσύνολο ΔYL που αντιστοιχεί στον καθένα, ορίζεται ένα Κατώφλι Εμπιστοσύνης $KE(BK)$ το οποίο θα πρέπει να ικανοποιείται από το βαθμό Αξιοπιστίας $A_t(X_v)$ του χρήστη προκειμένου να αποκτήσει δικαιώματα προσπέλασης. Αυτό σημαίνει ότι για να έχει πρόσβαση ο χρήστης X_v τη χρονική στιγμή t στις υπηρεσίες του υποσυνόλου ΔYL_i , το οποίο με βάση το σχήμα αντιστοιχεί σε βαθμό κρισιμότητας BK_k , θα πρέπει:

$$KE(BK_k) \leq A_t(X_v).$$

Με βάση το λειτουργικό πλαίσιο ΔΕΠ-ΕΣΠΣ η απόδοση προνομίων προσπέλασης στις ΔYL του ΕΣΠΣ είναι μια δυναμική διαδικασία καθώς μεταβάλλεται με το χρόνο ανάλογα με τη συμπεριφορά των χρηστών στη δημιουργία περιεχομένου, η οποία αποτυπώνεται στο βαθμό αξιοπιστίας τους. Όπως φαίνεται στο παράδειγμα που περιγράφει ο τέταρτος κάθετος άξονας στα δεξιά του Σχήμα 26:

Για $t = 1$: Τη χρονική στιγμή στην οποία ο χρήστης X_v συνδέεται για πρώτη φορά στο συνεργατικό περιβάλλον, ο βαθμός αξιοπιστίας του έχει τη μέγιστη τιμή ώστε να ικανοποιεί το μέγιστο κατώφλι εμπιστοσύνης $KE(BK_k)$. Αυτό σημαίνει ότι ο X_v δεν στερείται κανενός δικαιώματος προσπέλασης των ΔYL του ΕΣΠΣ τη συγκεκριμένη χρονική στιγμή.

Για $t = 2$: Με την πάροδο του χρόνου ο χρήστης υιοθετεί κακόβουλη συμπεριφορά χρήσης των ΔYL η οποία προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων, και, όπως φαίνεται τις χρονικές στιγμές $t=2$ και $t=3$ ο βαθμός αξιοπιστίας του $A_t(X_v)$ μειώνεται σταδιακά, επιτρέποντάς του την πρόσβαση σε ΔYL που αντιστοιχούν σε χαμηλότερα κατώφλια εμπιστοσύνης ανάλογα με το Βαθμό Κρισιμότητας στον οποίο κατατάσσονται.

Για $t = 3$: Ο βαθμός αξιοπιστίας $A_t(X_v)$ του χρήστη X_v είναι μεγαλύτερος από το κατώφλι εμπιστοσύνης $KE(BK_4)$ και, κατά συνέπεια, τη συγκεκριμένη χρονική στιγμή έχει προνόμια προσπέλασης των ΔYL που αντιστοιχούν σε Βαθμό Κρισιμότητας μικρότερο ή ίσο από BK_4 , δηλαδή στις ΔYL_1 , ΔYL_2 , ΔYL_3 , και ΔYL_4 .

Για $t = 4$: Όπως φαίνεται από το βέλος που συνδέει τον τρίτο με τον τέταρτο άξονα, ο βαθμός αξιοπιστίας $A_t(X_v)$ του χρήστη X_v έχει βελτιωθεί σε σύγκριση με

την προηγούμενη φορά που προσπέλασε το συνεργατικό περιβάλλον ($t=3$) καθώς ικανοποιεί υψηλότερο κατώφλι εμπιστοσύνης, το $KE(BK_{k-1})$. Αυτό σημαίνει ότι τη συγκεκριμένη χρονική στιγμή ο χρήστης X_n έχει προνόμια προσπέλασης σε όσες ΔΥΛ αντιστοιχούν σε επίπεδο κρισιμότητας μικρότερο ή ίσο του $k-1$. Με βάση το Σχήμα, τη χρονική στιγμή $t=4$, ο χρήστης έχει πρόσβαση στις ΔΥΛ₅ και ΔΥΛ _{$i-1$} , πλέον εκείνων που του εξασφάλιζε ο βαθμός αξιοπιστίας του την προηγούμενη φορά $t=3$ που συνδέθηκε στο συνεργατικό περιβάλλον.

Για $t = T-1$: Υποθέτοντας πως ο χρήστης δεν συμμορφώνεται με καλές πρακτικές χρήσης των ΔΥΛ και συνεχίζει να δημιουργεί περιεχόμενο το οποίο προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων, όπως φαίνεται στο σχήμα, τη χρονική στιγμή $T-1$, θα έχει ελάχιστα προνόμια προσπέλασης των ΔΥΛ του ΕΣΠΣ, όσα περιλαμβάνει ο βαθμός κρισιμότητας BK_3 .

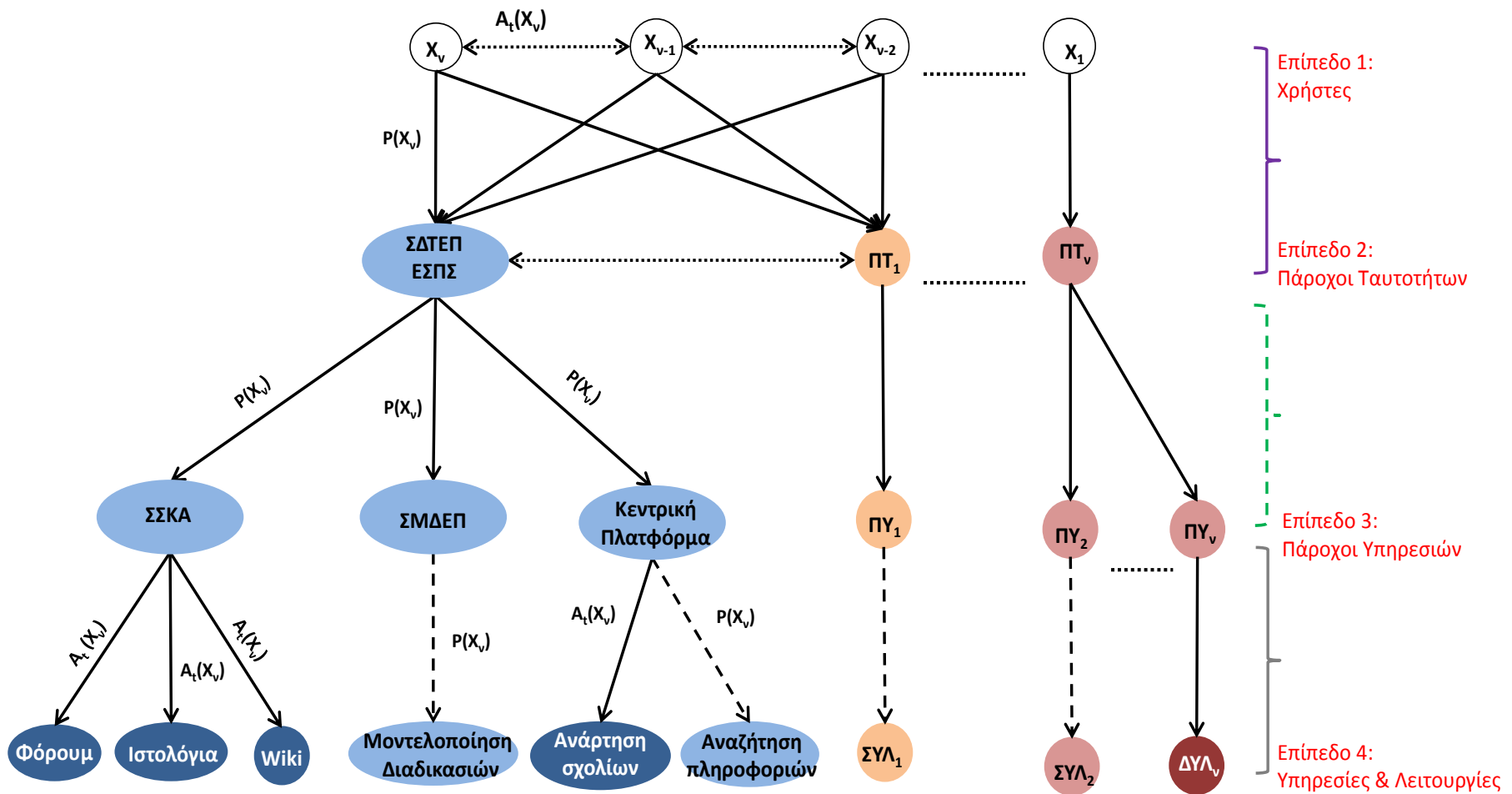
Για $t = T$: Τέλος τη χρονική στιγμή T όπως φαίνεται στο Σχήμα δεν μεταβάλλεται ο βαθμός αξιοπιστίας του χρήστη καθώς διατηρεί προνόμια προσπέλασης των ΔΥΛ που αντιστοιχούν σε βαθμός κρισιμότητας BK_3 .

Ανακεφαλαιώνοντας, με βάση το λειτουργικό πλαίσιο ΔΕΠ-ΕΣΠΣ της αρχιτεκτονικής της κεντροποιημένης ομοσπονδίας, η απόδοση προνομίων προσπέλασης στις κρίσιμες για την προστασία της ιδιωτικότητας διαδραστικές υπηρεσίες και λειτουργίες του ΕΣΠΣ είναι μια δυναμική διαδικασία δεδομένου ότι βασίζεται στη σύγκριση ενός χαρακτηριστικού της ταυτότητας των χρηστών το οποίο μεταβάλλεται με το πέρασμα του χρόνου - βαθμός αξιοπιστίας - με τα κατώφλια εμπιστοσύνης που ορίζουν οι εξίσου δυναμικές πολιτικές απόδοσης προνομίων προσπέλασης στις ΔΥΛ του συνεργατικού περιβάλλοντος.

6.5 Εφαρμογή ΔΕΠ-ΕΣΠΣ

Στόχος της διατριβής σε αυτή την ενότητα είναι να αναδειχθεί ο τρόπος λειτουργίας και χρήσης του προτεινόμενου μοντέλου ελέγχου προσπέλασης μέσω της εφαρμογής του στα πλαίσια του ΕΣΠΣ.

Όπως φαίνεται στο Σχήμα 27, με βάση το λειτουργικό πλαίσιο ΔΕΠ-ΕΣΠΣ (βλ. ενότητα 6.4) οι *Οντότητες* και οι *πόροι*, *Υπηρεσίες* και *Λειτουργίες*, του ΕΣΠΣ ταξινομούνται σε επίπεδα ανάλογα με τις αρμοδιότητες και τη λειτουργικότητά τους αντίστοιχα, σχηματίζοντας μια ιεραρχική δενδρική δομή η οποία καθορίζεται από τις *σχέσεις εμπιστοσύνης* και τις *συνθήκες εξουσιοδότησης* που καθορίστηκαν στην ενότητα 6.3.3.



Σχήμα 27: Εφαρμογή μοντέλου ΔΕΠ-ΕΣΠΣ

Πριν παρουσιαστεί ο τρόπος εφαρμογής του *Δυναμικού Ελέγχου Προσπέλασης* στο πλαίσιο υπηρεσιών του ΕΣΠΣ είναι σημαντικό να αναφερθεί ότι με βάση το προτεινόμενο μοντέλο (βλ. ενότητα 6.3):

- ✓ Όπως απεικονίζεται από τα οριζόντια βέλη που ενώνουν τα στοιχεία του πρώτου επιπέδου, δηλαδή τους χρήστες $X_1, X_2, X_3, \dots, X_n$, αναπτύσσονται μεταξύ τους σχέσεις εμπιστοσύνης οι οποίες καθορίζονται από το βαθμό αξιοπιστίας, $A_i(X_n)$, κάθε χρήστη, X_n , τη χρονική στιγμή t με βάση τη μέθοδο υπολογισμού που παρουσιάζεται στην ενότητα 6.6.
- ✓ Όπως απεικονίζεται από τα κατακόρυφα βέλη που συνδέουν τα στοιχεία του πρώτου και του δεύτερου επιπέδου, οι χρήστες μπορούν να αυθεντικοποιούνται όχι μόνο στον Πάροχο Ταυτοτήτων του ΕΣΠΣ (*ΣΔΤΕΠ-ΕΣΠΣ*), αλλά και σε άλλους Παρόχους Ταυτοτήτων και πλαίσια υπηρεσιών με τους οποίους το ΕΣΠΣ διατηρεί σχέσεις ομοσπονδιακής διαχείρισης ταυτοτήτων. Αυτό απεικονίζεται από τα οριζόντια βέλη που συνδέουν τα στοιχεία του δεύτερου επιπέδου, τα οποία και συμβολίζουν τις σχέσεις εμπιστοσύνης μεταξύ των Παρόχων Ταυτοτήτων ΣΔΤΕΠ-ΕΣΠΣ και ΠΤ₁, ΠΤ₂, ..., ΠΤ_λ.

Όπως φαίνεται στο Σχήμα 27, η εφαρμογή του *Δυναμικού Ελέγχου Προσπέλασης* στα πλαίσια λειτουργίας του ΕΣΠΣ, όπως αυτό προδιαγράφεται στο 4^ο Κεφάλαιο της διατριβής, περιλαμβάνει τα ακόλουθα:

Επίπεδο 1: Για να αποκτήσουν πρόσβαση στις υπηρεσίες που παρέχει το ΕΣΠΣ (Επίπεδο 4), οι χρήστες διατηρούν σχέσεις εμπιστοσύνης με το ΣΔΤΕΠ-ΕΣΠΣ, οι οποίες καθορίζονται από το ρόλο που τους αποδίδεται όταν ταυτοποιούνται στο Πληροφοριακό Σύστημα.

Επίσης αναπτύσσονται σχέσεις εμπιστοσύνης μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον οι οποίες αλλάζουν δυναμικά με το πέρασμα του χρόνου και καθορίζονται από τη μέθοδο υπολογισμού του βαθμού αξιοπιστίας κάθε χρήστη με βάση τις αναφορές κακόβουλης συμπεριφοράς που υποβάλλουν οι υπόλοιποι συμμετέχοντες.

Επίπεδο 2: Ο Πάροχος Ταυτοτήτων ΣΔΤΕΠ-ΕΣΠΣ αναλαμβάνει τη διαχείριση και την απόδοση προνομίων προσπέλασης στο σύνολο των Παρόχων Υπηρεσιών που συμμετέχουν στην αρχιτεκτονική του ΕΣΠΣ με βάση τον ρόλο του κάθε χρήστη. Για παράδειγμα, για να έχει πρόσβαση ο χρήστης X_n στις υπηρεσίες του Παρόχου Υπηρεσιών ΣΣΚΑ, θα πρέπει να αποτελούν υποσύνολο του συνόλου των υπηρεσιών στις οποίες έχει πρόσβαση με βάση το ρόλο του.

Επίπεδο 3: Κάθε Πάροχος Υπηρεσιών του ΕΣΠΣ, όπως για παράδειγμα του ΣΣΚΑ, του ΣΜΔΕΠ, και της Κεντρικής Πλατφόρμας, ολοκληρώνει και παρέχει στους τελικούς χρήστες ένα υποσύνολο υπηρεσιών και λειτουργιών. Για παράδειγμα, με βάση την αρχιτεκτονική του ΕΣΠΣ, οι υπηρεσίες που παρέχει το ΣΣΚΑ αποτελούνται από διαδραστικές λειτουργίες, ΔΥΛ (π.χ. δημοσίευση

περιεχομένου, σχολιασμός, κοινοποίηση), που προσφέρουν τα ιστολόγια, τα φόρουμ και τα wiki, ενώ το ΣΜΔΕΠ παρέχει συμβατικές υπηρεσίες, ΣΥΛ, σχετικές με τη μοντελοποίηση διαδικασιών.

Επίπεδο 4: Οι υπηρεσίες και οι λειτουργίες που παρέχει το ΕΣΠΣ στους τελικούς χρήστες και οι οποίες απεικονίζονται στο τέταρτο επίπεδο του Σχήμα 27 ενδέχεται να αποτελούν είτε υποσύνολα ΣΥΛ (π.χ. Μοντελοποίηση διαδικασιών) είτε υποσύνολα ΔΥΛ (π.χ. ιστολόγια, φόρουμ, wiki) ανάλογα με το αν βασίζονται σε εφαρμογές Web 2.0. Για παράδειγμα, οι υπηρεσίες που παρέχει το ΣΣΚΑ επιτρέπουν τη δημιουργία κακόβουλου περιεχομένου και την προσβολή της ιδιωτικότητας των χρηστών, ενώ οι υπηρεσίες που παρέχει το ΣΜΔΕΠ περιλαμβάνουν λειτουργίες οι οποίες δεν επιτρέπουν την αλληλεπίδραση μεταξύ των χρηστών. Ο διαχωρισμός αυτός ανάμεσα σε συμβατικές και διαδραστικές υπηρεσίες και λειτουργίες απεικονίζεται από τον πιο ελαφρύ και αντίστοιχα πιο έντονο χρωματισμό των κόμβων στο 4^ο επίπεδο του σχήματος.

Όπως απεικονίζεται από τα κατακόρυφα βέλη που συνδέουν τα στοιχεία του τρίτου και τέταρτου επιπέδου, η απόδοση προνομίων προσπέλασης σε κάθε μια από τις 2 αυτές κατηγορίες υπηρεσιών, δηλαδή τις συμβατικές ΣΥΛ και τις διαδραστικές ΔΥΛ, γίνεται με διαφορετικό τρόπο.

Το μοντέλο ΔΕΠ-ΕΣΠΣ εφαρμόζει μια *υβριδική προσέγγιση* όσον αφορά στην απόδοση προνομίων προσπέλασης στις υπηρεσίες που παρέχει το ΕΣΠΣ δεδομένου ότι:

1. Υιοθετεί τις προδιαγραφές του μοντέλου *Ελέγχου Προσπέλασης με βάση τους Ρόλους (ΕΠΡ)* (βλ. ενότητα 2.3.1.3) και ικανοποιεί τις απαιτήσεις της *Ομοσπονδιακής Διαχείρισης Ταυτοτήτων* καθώς υποστηρίζει την απόδοση προνομίων προσπέλασης με βάση τους ρόλους των χρηστών όταν πρόκειται για αποφάσεις εξουσιοδότησης που αφορούν σε συμβατικές υπηρεσίες.
2. Αξιοποιώντας τις δυνατότητες της κεντροποιημένης αρχιτεκτονικής υιοθετεί βασικά χαρακτηριστικά του μοντέλου *Υποχρεωτικού Ελέγχου Προσπέλασης (ΥΕΠ)* (βλ. ενότητα 2.3.1.2) καθώς η απόδοση προνομίων προσπέλασης σε κρίσιμες, ως προς την ιδιωτικότητα των χρηστών, διαδραστικές υπηρεσίες του συνεργατικού περιβάλλοντος προϋποθέτει την ικανοποίηση συγκεκριμένων κατωφλίων εμπιστοσύνης.

Όπως φαίνεται στο Σχήμα 27, για να είναι σε θέση ένας χρήστης, Χ, να προσπελάσει τις υπηρεσίες του ΕΣΠΣ:

1. Αν πρόκειται για υποσύνολο συμβατικών υπηρεσιών, ΣΥΛ_i, θα πρέπει τα προνόμια προσπέλασης που έχει ανάλογα με το ρόλο που του αποδίδει ο Πάροχος Ταυτοτήτων (π.χ. ΣΔΤΕΠ-ΕΣΠΣ), να του επιτρέπουν να προσπελάσει τον Πάροχο Υπηρεσιών ΠΥ_μ (π.χ. ΣΣΚΑ, ΣΜΔΕΠ, Κεντρική Πλατφόρμα) και το συγκεκριμένο υποσύνολο πόρων.

Δηλαδή, αν $\Sigma\Upsilon\Lambda_i \subseteq \Pi\Upsilon_\mu$ τότε θα πρέπει $\Pi\Upsilon_\mu \subseteq P(X_v)$.

2. Αν πρόκειται για υποσύνολο διαδραστικών υπηρεσιών, $\Delta\Upsilon\Lambda_j$, θα πρέπει εκτός του να μπορεί με βάση το ρόλο του να προσπελάσει τους πόρους του Παρόχου Υπηρεσιών (π.χ. ΣΣΚΑ), ο βαθμός αξιοπιστίας του τη χρονική στιγμή που αιτείται να αποκτήσει πρόσβαση σε κάποιο συγκεκριμένο υποσύνολο υπηρεσιών να είναι μεγαλύτερος ή ίσος από, το κατώφλι εμπιστοσύνης του βαθμού κρισιμότητας, BK_j , στον οποίο ταξινομούνται.

Δηλαδή αν $\Delta\Upsilon\Lambda_j \subseteq \Sigma\Sigma\text{ΚΑ}$ θα πρέπει να ισχύει ότι $\Sigma\Sigma\text{ΚΑ} \subseteq P(X_v)$ και $A_t(X_v) \geq KE(BK_j)$.

Για παράδειγμα, για να προσπελάσει ο χρήστης X_v τη χρονική στιγμή t το υποσύνολο των διαδραστικών λειτουργιών «δημοσίευση περιεχομένου» που παρέχει το φόρουμ του ΣΣΚΑ θα πρέπει το συγκεκριμένο υποσύνολο $\Delta\Upsilon\Lambda$ να αντιστοιχεί σε βαθμό κρισιμότητας με κατώφλι εμπιστοσύνης μικρότερο ή ίσο από το βαθμό αξιοπιστίας του χρήστη τη στιγμή που αιτείται να την προσπελάσει. Αντίθετα, για να αποκτήσει πρόσβαση ο χρήστης X_v σε υποσύνολο συμβατικών λειτουργιών, όπως για παράδειγμα το υποσύνολο «Μοντελοποίηση Διαδικασιών» του ΣΜΔΕΠ, οι οποίες δεν βασίζονται σε εφαρμογές Web 2.0, αρκεί ο ρόλος του να περιλαμβάνει αντίστοιχα δικαιώματα προσπέλασης.

Με βάση τα παραπάνω, το μοντέλο ΔΕΠ-ΕΣΠΣ αποτελεί μια καινοτόμο προσέγγιση καθώς αντί να βασίζεται σε ένα σύνολο στατικών κανόνων για την απόδοση προνομίων προσπέλασης με βάση το ρόλο των χρηστών, παρέχει δυνατότητες δυναμικού ελέγχου προσπέλασης στους κρίσιμους πόρους που βασίζονται σε εφαρμογές Web 2.0. Πιο συγκεκριμένα, ο έλεγχος προσπέλασης στα πλαίσια του συνεργατικού περιβάλλοντος γίνεται με βάση τις απαιτήσεις ιδιωτικότητας των κρίσιμων πόρων, χρησιμοποιώντας το βαθμό αξιοπιστίας των χρηστών ως κριτήριο αξιολόγησης της συμπεριφοράς τους.

Βασική απαίτηση για να επιτευχθεί αυτό και γενικά για την εφαρμογή της αρχιτεκτονικής της *Κεντρικοποιημένης Ομοσπονδίας* είναι η απόδοση προνομίων προσπέλασης στα πλαίσια του ΕΣΠΣ να αποτελεί αρμοδιότητα αποκλειστικά του ΣΔΤΕΠ και όχι κάποιου άλλου ΠΤ της ομοσπονδίας, όπως είναι η παραδοσιακή πρακτική.

6.6 Μέθοδος υπολογισμού αξιοπιστίας

Όπως έχει ήδη αναφερθεί, η εφαρμογή του μοντέλου ΔΕΠ-ΕΣΠΣ προϋποθέτει την ενσωμάτωση ενός Συστήματος Διαχείρισης Αξιοπιστίας στην αρχιτεκτονική του Συστήματος Διαχείρισης Ταυτοτήτων έτσι ώστε να είναι δυνατή:

- ✓ Η καταγραφή και η αξιολόγηση των αναφορών κακόβουλης συμπεριφοράς των χρηστών όσον αφορά στη χρήση των εφαρμογών Web 2.0.

- ✓ Ο υπολογισμός του βαθμού αξιοπιστίας των χρηστών κάθε χρονική στιγμή με βάση τόσο την κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς όσο και άλλους σημαντικούς παράγοντες του συνεργατικού περιβάλλοντος.

Ακολουθώντας αυτή την προσέγγιση το ΣΔΤΕΠ με τη βοήθεια του ΣΔΑ που ενσωματώνει έχει τη δυνατότητα να συλλέγει και να επεξεργάζεται δεδομένα τα οποία αλλάζουν με το χρόνο (π.χ. πλήθος αναφορών κακόβουλης συμπεριφοράς, κρισιμότητα αναφορών, συμμόρφωση χρήστη) ώστε να διαχειρίζεται δυναμικά την λήψη αποφάσεων εξουσιοδότησης στους πόρους του συνεργατικού περιβάλλοντος. Έτσι είναι σε θέση να παρέχει διαδικασίες δυναμικού ελέγχου προσπέλασης μέσω της σύγκρισης του βαθμού αξιοπιστίας κάθε χρονική στιγμή που ο χρήστης αιτείται να προσπελάσει τις εφαρμογές Web 2.0 με τα προκαθορισμένα κατώφλια εμπιστοσύνης (πολιτικές απόδοσης προνομίων προσπέλασης) κάθε υποσυνόλου κρίσιμων πόρων.

Χρήστες οι οποίοι αξιολογούνται από τους υπόλοιπους συμμετέχοντες ότι δημοσιεύουν περιεχόμενο το οποίο προσβάλλει την ιδιωτικότητα υποβαθμίζονται σε χαμηλότερους βαθμούς αξιοπιστίας και, αντίστοιχα, σε πολιτικές περιορισμένης πρόσβασης, έτσι ώστε αφενός να προστατεύεται το σύνολο των χρηστών και αφετέρου η κίνηση αυτή να λειτουργεί παραδειγματικά για τους ίδιους.

Όπως παρουσιάστηκε στην προηγούμενη ενότητα ο τρόπος με τον οποίο υπολογίζεται ο βαθμός αξιοπιστίας κάθε χρονική στιγμή καθορίζεται από τις σχέσεις εμπιστοσύνης μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον και επηρεάζεται από τις αναφορές κακόβουλου περιεχομένου που έχει καταγράψει το ΣΔΑ μέχρι τη συγκεκριμένη χρονική στιγμή.

Πριν περιγραφεί η μέθοδος υπολογισμού του βαθμού αξιοπιστίας θα πρέπει να σημειωθεί ότι στόχος της διατριβής είναι ο ορισμός ενός μαθηματικού τύπου ο οποίος:

- ✓ Περιλαμβάνει όλες τις κρίσιμες παραμέτρους οι οποίες επηρεάζουν την αξιοπιστία των χρηστών εντός του συνεργατικού περιβάλλοντος.
- ✓ Παρέχει δυνατότητες επεκτασιμότητας, ευελιξίας και βελτιστοποίησης του τρόπου με τον οποίο υπολογίζεται το τελικό αποτέλεσμα ώστε να προσαρμόζεται εύκολα στις ανάγκες της εκάστοτε μελέτης εφαρμογής και να ικανοποιεί ένα μεγάλο εύρος πολιτικών εξουσιοδότησης.

Πιο συγκεκριμένα, η μέθοδος υπολογισμού του βαθμού αξιοπιστίας η οποία και αποτελεί τη βασική συνεισφορά της διατριβής στον 4^ο ερευνητικό άξονα, αποτελείται από τρεις (3) βασικούς παράγοντες, K_t , E_t , και Π_t , οι οποίοι αλλάζουν δυναμικά με το χρόνο και εξαρτώνται από τους συντελεστές επίδρασης α , β , γ αντίστοιχα.

Ακολουθώντας τη μορφή των αναδρομικών συναρτήσεων ώστε κάθε φορά να υπάρχει συσχέτιση του βαθμού αξιοπιστίας με την προηγούμενη τιμή του, η μέθοδος υπολογισμού καθορίζεται ως εξής:

$$A_t(X_v) = \begin{cases} A_1(X_v), & \text{για } t = 1 \\ \alpha K_t A_{t-1}(X_v) + \beta E_t - \gamma \Pi_t, & \text{για } t > 1 \end{cases}, \text{ όπου}$$

- $A_1(X_v)$, η προκαθορισμένη από τον Πάροχο αρχική τιμή του βαθμού αξιοπιστίας του χρήστη X_v ,
- $A_{t-1}(X_v)$, ο βαθμός αξιοπιστίας του χρήστη X_v την αμέσως προηγούμενη φορά ($t-1$) που προσπέλασε το συνεργατικό περιβάλλον,
- K_t , ο παράγοντας *Κρισιμότητας* των αρνητικών ψήφων που καταγράφηκαν για το χρήστη X_v στο μεσοδιάστημα μεταξύ δύο (2) προσπελάσεων (βλ ενότητα 6.6.1),
- E_t , ο παράγοντας *Επιβράβευσης* του χρήστη X_v για τη συμμετοχή του στο συνεργατικό περιβάλλον (βλ. ενότητα 6.6.2),
- Π_t , ο παράγοντας στάθμισης των αρνητικών ψήφων που έλαβε ο χρήστης X_v ως προς τη συχνότητα χρήσης του συνεργατικού *Περιβάλλοντος* (βλ. ενότητα 0),
- α , ο συντελεστής επίδρασης του παράγοντα K_t ,
- β , ο συντελεστής επίδρασης του παράγοντα E_t ,
- γ , ο συντελεστής επίδρασης του παράγοντα Π_t .

Στις υποενότητες που ακολουθούν παρουσιάζεται ο ορισμός των 3 παραγόντων K_t , E_t , Π_t που λαμβάνονται υπόψιν για τον υπολογισμό του βαθμού αξιοπιστίας κάθε χρονική στιγμή που ο χρήστης αιτείται δικαιωμάτων προσπέλασης στο συνεργατικό περιβάλλον καθώς και ο τρόπος με τον οποίο επιδρούν στο τελικό αποτέλεσμα ανάλογα με τα δεδομένα που συλλέγονται από το ΣΔΑ.

6.6.1 Παράγοντας κρισιμότητας των αναφορών κακόβουλης συμπεριφοράς

Ο παράγοντας K_t είναι αυτός που καθορίζει το ποσοστό μεταβολής του βαθμού αξιοπιστίας κάθε χρήστη ανάλογα με την *Κρισιμότητα* των κακόβουλων ενεργειών του, και εξαρτάται από τις αρνητικές ψήφων που καταγράφονται στο μεσοδιάστημα $[t-1, t)$ μεταξύ δύο προσπελάσεων από το χρήστη του συνεργατικού περιβάλλοντος, και τον βαθμό στον οποίο συμμορφώνεται με τις πολιτικές ιδιωτικότητας διαγράφοντας το περιεχόμενο που έχει προηγουμένως χαρακτηριστεί ως κακόβουλο. Πιο συγκεκριμένα:

$$K_t = \begin{cases} 1, & \text{για } \sum_{i=1}^k \Psi_{i,t} = 0 \\ \frac{\sigma}{\sigma + \mu_t}, & \text{για } \sum_{i=1}^k \Psi_{i,t} > 0 \end{cases} \quad \text{όπου}$$

- $\sum_{i=1}^k \Psi_{i,t}$, το πλήθος των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης στο μεσοδιάστημα μεταξύ [t-1, t) για το σύνολο των ΔΥΛ (ανεξάρτητα από το βαθμό κρισιμότητας),
- σ , ο συντελεστής που καθορίζει το εύρος μεταβολής του βαθμού αξιοπιστίας (βλ. Παράρτημα Ι) και η οποία εξαρτάται από τις απαιτήσεις κάθε συνεργατικού περιβάλλοντος,
- $\mu_t = 1 + \frac{\sum_{i=1}^k BK_i \Psi_{i,t} - \sum_{i=1}^{MBK} BK_i \Psi_{i,t}}{\sum_{i=1}^k BK_i \Psi_{i,t}}$, ο βαθμός μη-συμμόρφωσης του χρήστη ο οποίος εξαρτάται από το εάν ο χρήστης διαγράφει προηγούμενες δημοσιεύσεις του οι οποίες έχουν χαρακτηριστεί ως κακόβουλες προκειμένου να συμμορφώνεται με τις ισχύουσες πολιτικές και να βελτιώνει το βαθμό αξιοπιστίας του,
- MBK, ο Μέγιστος Βαθμός Κρισιμότητας του οποίου το Κατώφλι Εμπιστοσύνης ΚΕ είναι μικρότερο ή ίσο από το βαθμό αξιοπιστίας του χρήστη X_v μέχρι τη χρονική στιγμή t, έτσι ώστε $A_{t-1}(X_v) \geq KE(MBK)$,
- $\sum_{i=1}^k BK_i \Psi_{i,t}$, η συνολική κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς που καταγράφηκαν για όλες τις ΔΥΛ άσχετα από το βαθμό κρισιμότητας στον οποίο ανήκουν,
- $\sum_{i=1}^{MBK} BK_i \Psi_{i,t}$, η συνολική κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς που καταγράφηκαν μόνο σε ΔΥΛ στις οποίες είχε πρόσβαση ο χρήστης μέχρι τη χρονική στιγμή t με βάση το βαθμό αξιοπιστίας του $A_{t-1}(X_v)$,
- $\mu_t - 1$, η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς ως ποσοστό των αναφορών που καταγράφονται σε πόρους για τους οποίους ο χρήστης δεν έχει πλέον δικαιώματα προσπέλασης προς τη συνολική.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι η τιμή της σταθεράς σ αποτελεί βασικό κριτήριο επιλογής του συντελεστή επίδρασης α (βλ. ενότητα 6.7.2) και όπως αναφέρεται πιο πάνω καθορίζεται με βάση τον πίνακα τιμών στο Παράρτημα Ι.

Επίσης με βάση τον τύπο υπολογισμού της μεταβλητής μ_t , ο παράγοντας K_t εξαρτάται από το εάν η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς που καταγράφονται στο μεσοδιάστημα t-1 και t είναι μεγαλύτερη, μικρότερη ή ίση από την κρισιμότητα που θα έπρεπε να έχουν αν ο χρήστης είχε διαγράψει κακόβουλο περιεχόμενο που έχει δημοσιευτεί σε ΔΥΛ που ανήκουν σε μεγαλύτερο βαθμό κρισιμότητας από αυτόν στον οποίο του επιτρέπεται η

πρόσβαση. Έτσι, αξιολογείται ο βαθμός στον οποίο η συμπεριφορά του χρήστη συμμορφώνεται με τις ισχύουσες πολιτικές ιδιωτικότητας με το πέρασμα του χρόνου.

Πιο συγκεκριμένα, στον Πίνακα 4 παρουσιάζεται το ποσοστό μεταβολής του βαθμού αξιοπιστίας ανάλογα με τα πιθανά σενάρια καταγραφής αναφορών κακόβουλης συμπεριφοράς.

Περιπτώσεις	Συμπεριφορά συντελεστών	K_t	Σχόλια
Σύνολο αρνητικών ψήφων στο μεσοδιάστημα μεταξύ 2 προσπελάσεων	μ_t		
$ \Psi = 0$	--	1	Ο βαθμός αξιοπιστίας παραμένει ο ίδιος με τον προηγούμενο όταν δεν καταγράφεται καμία αναφορά κακόβουλης συμπεριφοράς
$\exists \Psi_{i,t} > 0$ με $i > MBK$ Δηλαδή καταγράφονται αρνητικές ψήφοι σε ΔΥΛ που ανήκουν σε μεγαλύτερο BK από αυτό στο οποίο έχει πρόσβαση ο χρήστης μέχρι τη χρονική στιγμή t .	$\sum_{i=1}^k BK_i \Psi_{i,t} > \sum_{i=1}^{MBK} BK_i \Psi_{i,t}$	$\left(\frac{\sigma}{\sigma+2}, \frac{\sigma}{\sigma+1} \right)$ (Παράρτημα Ι)	Όταν η συνολική κρισιμότητα των αρνητικών ψήφων είναι μεγαλύτερη από την κρισιμότητα εκείνων που έχουν καταγραφεί σε ΔΥΛ που αντιστοιχούν σε BK μικρότερο ή ίσο από το MBK στο οποίο είχε πρόσβαση ο χρήστης μέχρι τη συγκεκριμένη χρονική στιγμή, τότε ο βαθμός αξιοπιστίας μειώνεται, καθώς αυτό σημαίνει ότι ο χρήστης δεν έχει διαγράψει περιεχόμενο το οποίο είχε χαρακτηριστεί στο παρελθόν ότι προσβάλλει την ιδιωτικότητα.
$\forall \Psi_{i,t} > 0, 1 < i \leq MBK$ Όλες οι ψήφοι κακόβουλης συμπεριφοράς αναφέρονται σε ΔΥΛ που ανήκουν σε χαμηλότερο ή ίσο BK με αυτό στο οποίο έχει πρόσβαση ο χρήστης μέχρι τη χρονική στιγμή t	$\sum_{i=1}^k BK_i \Psi_{i,t} = \sum_{i=1}^{MBK} BK_i \Psi_{i,t}$	$\frac{\sigma}{\sigma+1}$ (Παράρτημα Ι)	Η ελάχιστη μείωση του βαθμού αξιοπιστίας συμβαίνει όταν όλες οι αναφορές κακόβουλης συμπεριφοράς αφορούν σε ΔΥΛ που ανήκουν σε BK μικρότερο ή ίσο από αυτόν στον οποίο έχει πρόσβαση ο χρήστης μέχρι τη συγκεκριμένη χρονική στιγμή. Αυτό σημαίνει ότι έχει διαγράψει το περιεχόμενο το οποίο είχε χαρακτηριστεί στο παρελθόν ότι προσβάλλει την ιδιωτικότητα.
$\forall \Psi_{i,t} > 0, i > MBK$ Όλες οι ψήφοι κακόβουλης συμπεριφοράς αναφέρονται σε ΔΥΛ που ανήκουν σε μεγαλύτερο BK με αυτό στο οποίο έχει πρόσβαση ο χρήστης μέχρι τη χρονική στιγμή t	$\sum_{i=1}^{MBK} BK_i \Psi_{i,t} = 0$	$\frac{\sigma}{\sigma+2}$ (Παράρτημα Ι)	Η μέγιστη μείωση του βαθμού αξιοπιστίας συμβαίνει όταν όλες οι αναφορές κακόβουλης συμπεριφοράς αφορούν σε ΔΥΛ που ανήκουν σε BK μεγαλύτερο από αυτόν στον οποίο έχει πρόσβαση ο χρήστης μέχρι τη συγκεκριμένη χρονική στιγμή. Αυτό σημαίνει ότι δεν έχει διαγράψει περιεχόμενο το οποίο είχε χαρακτηριστεί στο παρελθόν ότι προσβάλλει την ιδιωτικότητα, δηλαδή ότι δε συμμορφώνεται με τις ισχύουσες πολιτικές.

Πίνακας 4: Παράγοντας Καταγραφής κακόβουλης συμπεριφοράς

Όπως φαίνεται στον Πίνακας 4, ανάλογα με το πώς κατανέμονται οι αναφορές κακόβουλης συμπεριφοράς στα υποσύνολα των κρίσιμων πόρων ΔΥΛ και στους αντίστοιχους Βαθμούς Κρισιμότητας επηρεάζεται και το ποσοστό μεταβολής K_t του βαθμού αξιοπιστίας. Η χαμηλότερη τιμή που μπορεί να πάρει αφορά στην περίπτωση που όλες οι αναφορές κακόβουλης συμπεριφοράς καταγράφονται σε πόρους μεγαλύτερου Βαθμού Κρισιμότητας από αυτό στον οποίο έχει προνόμια προσπέλασης ο χρήστης μέχρι τη χρονική στιγμή t , οπότε και ο βαθμός αξιοπιστίας του χρήστη μειώνεται περισσότερο.

Αυτό σημαίνει ότι διαγράφοντας το περιεχόμενο στο οποίο συγκεντρώνονται οι αναφορές κακόβουλης συμπεριφοράς ο χρήστης μειώνει τις πιθανότητες να λάβει ξανά αρνητικούς ψήφους με μεγάλη βαρύτητα κι έτσι συντελεί αφενός στη μελλοντική βελτίωση του βαθμού αξιοπιστίας του με πιο γρήγορο ρυθμό και αφετέρου στην προστασία της ιδιωτικότητας εντός του συνεργατικού περιβάλλοντος.

6.6.2 Παράγοντας επιβράβευσης του χρήστη

Ο παράγοντας *Επιβράβευσης* του χρήστη για τη συμμετοχή του στο συνεργατικό περιβάλλον ορίζεται από την ακόλουθη σχέση:

$$E_t = \frac{\text{ΑΠ}(X_v) |X|}{\text{ΑΠ}(X)}, \text{ όπου}$$

- $\text{ΑΠ}(X_v)$, ο Αριθμός Προσπελάσεων του συνεργατικού περιβάλλοντος από το χρήστη X_v μέχρι και την τρέχουσα χρονική στιγμή t , και θεωρώντας ότι το t παίρνει διακριτές τιμές ισχύει ότι $\text{ΑΠ}(X_v)=t$,
- $|X|$, το πλήθος των Χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον, και
- $\text{ΑΠ}(X)$, ο Αριθμός Προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών X μέχρι τη χρονική στιγμή t .

Ο τρόπος με τον οποίο επηρεάζεται ο βαθμός αξιοπιστίας των χρηστών από τον παράγοντα προσωπικής επιβράβευσης φαίνεται στον Πίνακας 5.

Περιπτώσεις	Συμπεριφορά συντελεστών	E_t	Σχόλια
Η συμμετοχή του χρήστη στο συνεργατικό περιβάλλον ως προς τη μέση τιμή συμμετοχής για το σύνολο των χρηστών στο μεσοδιάστημα μεταξύ δύο αιτημάτων προσπέλασης του χρήστη.	$\frac{ΑΠ(X_v)}{\frac{ΑΠ(X)}{ X }}$		
$ΑΠ(X_v) = \frac{ΑΠ(X)}{ X }$	Το πλήθος προσπελάσεων του συνεργατικού περιβάλλοντος από το χρήστη X_v ισούται με το μέσο όρο προσπελάσεων για το σύνολο των χρηστών.	1	Ο βαθμός αξιοπιστίας αυξάνεται κατά μια μονάδα όταν το πλήθος συμμετοχών του χρήστη στο συνεργατικό περιβάλλον ισούται με το μέσο όρο συμμετοχών για το σύνολο των χρηστών.
$ΑΠ(X_v) < \frac{ΑΠ(X)}{ X }$	Το πλήθος προσπελάσεων του συνεργατικού περιβάλλοντος από το χρήστη X_v είναι μικρότερο από το μέσο όρο προσπελάσεων για το σύνολο των χρηστών.	(0,1)	Ο βαθμός αξιοπιστίας αυξάνεται σε μικρό βαθμό όταν το πλήθος συμμετοχών του χρήστη στο συνεργατικό περιβάλλον είναι μικρότερο από το μέσο όρο συμμετοχών.
$ΑΠ(X_v) > \frac{ΑΠ(X)}{ X }$	Το πλήθος προσπελάσεων του συνεργατικού περιβάλλοντος από το χρήστη X_v είναι μεγαλύτερο από το μέσο όρο προσπελάσεων για το σύνολο των χρηστών.	(1,+∞)	Ο βαθμός αξιοπιστίας αυξάνεται σε μεγάλο βαθμό όταν το πλήθος συμμετοχών του χρήστη στο συνεργατικό περιβάλλον είναι μεγαλύτερο από το μέσο όρο συμμετοχών.

Πίνακας 5: Παράγοντας Επιβράβευσης του χρήστη

Όπως φαίνεται στον Πίνακα 5 όταν το πλήθος συμμετοχών του χρήστη στο συνεργατικό περιβάλλον ισούται με το μέσο όρο συμμετοχών όλων των χρηστών την τρέχουσα χρονική στιγμή τότε το E_t ισούται με 1, δηλαδή έχει θετική επίδραση στον τελικό βαθμό αξιοπιστίας. Αξιοσημείωτο είναι ότι όταν το πλήθος των φορών που ένας χρήστης αιτείται δικαιωμάτων προσπέλασης του συνεργατικού περιβάλλοντος είναι μικρότερος ή μεγαλύτερος από το μέσο όρο συμμετοχών για το σύνολο των χρηστών τότε ο παράγοντας E_t επηρεάζει σε μικρότερο ή σε μεγαλύτερο βαθμό αντίστοιχα την τελική τιμή του βαθμού αξιοπιστίας.

Τελικά, ο παράγοντας E_t αφορά στην επιβράβευση του χρήστη για τη συμμετοχή του στο συνεργατικό περιβάλλον δεδομένου ότι εξ' ορισμού η ενέργειά του αυτή ενέχει το ρίσκο να προσελκύσει αναφορές κακόβουλης συμπεριφοράς και να έχει αντίκτυπο στο βαθμό αξιοπιστίας του και κατά συνέπεια στα δικαιώματα προσπέλασης των κρίσιμων πόρων. Όσο περισσότερο ενεργή είναι η συμμετοχή του χρήστη τόσο περισσότερο θα πρέπει να επιβραβεύεται στο βαθμό αξιοπιστίας του, ιδιαίτερα όταν δε συγκεντρώνει αναφορές κακόβουλης συμπεριφοράς.

6.6.3 Παράγοντας στάθμισης του συνεργατικού περιβάλλοντος

Ο παράγοντας στάθμισης των αρνητικών ψήφων ως προς τη συχνότητα χρήσης του συνεργατικού Περιβάλλοντος δίνεται από τον ακόλουθο τύπο:

$$\Pi_t = \frac{\sum_{i=1}^k \Psi_{i,t}}{\delta(\text{ΑΠ}(X))}$$

Στον Πίνακα 6 που ακολουθεί παρουσιάζεται ο τρόπος με τον οποίο επηρεάζεται ο βαθμός αξιοπιστίας από τον παράγοντα Π_t .

Περιπτώσεις	Συμπεριφορά συντελεστών		
Το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης στο μεσοδιάστημα μεταξύ των δύο τελευταίων προσπελάσεων του συνεργατικού περιβάλλοντος ως προς το σύνολο των προσπελάσεων του συνεργατικού περιβάλλοντος για το ίδιο χρονικό διάστημα.	$\frac{\sum_{i=1}^k \Psi_{i,t}}{\delta(\text{ΑΠ}(X))}$	Π_t	Σχόλια
$\sum_{i=1}^k \Psi_{i,t} = 0$	Δεν καταγράφηκαν αναφορές κακόβουλης συμπεριφοράς για το χρήστη στο μεσοδιάστημα μεταξύ των δύο τελευταίων προσπελάσεων του συνεργατικού περιβάλλοντος.	0	Ο βαθμός αξιοπιστίας δεν επηρεάζεται.
$\sum_{i=1}^k \Psi_{i,t} = \delta(\text{ΑΠ}(X))$	Το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης στο μεσοδιάστημα μεταξύ των δύο τελευταίων προσπελάσεων του συνεργατικού περιβάλλοντος είναι ίσο με τον αριθμό προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών.	-1	Ο βαθμός αξιοπιστίας μειώνεται κατά μία μονάδα όταν για κάθε προσπέλαση του συνεργατικού περιβάλλοντος στο μεσοδιάστημα μεταξύ των δύο προσπελάσεων του χρήστη αντιστοιχεί μια αναφορά κακόβουλης συμπεριφοράς.
$\sum_{i=1}^k \Psi_{i,t} > \delta(\text{ΑΠ}(X))$	Το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης στο μεσοδιάστημα μεταξύ των δύο τελευταίων προσπελάσεων του συνεργατικού περιβάλλοντος είναι μεγαλύτερο από τον αριθμό προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών.	$(-\infty, -1)$	Ο βαθμός αξιοπιστίας μειώνεται σε μεγάλο βαθμό όταν για κάθε προσπέλαση του συνεργατικού περιβάλλοντος στο μεσοδιάστημα μεταξύ των δύο προσπελάσεων του χρήστη αντιστοιχούν περισσότερες από μία αναφορές κακόβουλης συμπεριφοράς.
$\sum_{i=1}^k \Psi_{i,t} < \delta(\text{ΑΠ}(X))$	Το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης στο μεσοδιάστημα μεταξύ των δύο τελευταίων προσπελάσεων του συνεργατικού περιβάλλοντος είναι μικρότερο από τον αριθμό προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών.	$(-1, 0)$	Ο βαθμός αξιοπιστίας μειώνεται ελάχιστα όταν για κάθε προσπέλαση του συνεργατικού περιβάλλοντος στο μεσοδιάστημα μεταξύ των δύο προσπελάσεων του χρήστη αντιστοιχούν λιγότερες από μία αναφορές κακόβουλης συμπεριφοράς.

Πίνακας 6: Παράγοντας Στάθμισης αρνητικών ψήφων με τη συχνότητα χρήσης

Όπως φαίνεται στον Πίνακα 6, το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης για το μεσοδιάστημα μεταξύ των δύο αιτημάτων προσπέλασης του συνεργατικού περιβάλλοντος είναι σταθμισμένο ως προς τον αριθμό των προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών σε αυτό το μεσοδιάστημα. Αυτό επιτρέπει τη γραμμική μεταβολή του συντελεστή Π_t ανάλογα με τον αριθμό των χρηστών που προσπέλασαν το συνεργατικό περιβάλλον το συγκεκριμένο χρονικό διάστημα και υπέβαλαν κατά μέσο όρο τουλάχιστον μία αναφορά κακόβουλης συμπεριφοράς για το συγκεκριμένο χρήστη.

Για παράδειγμα, όταν ο συνολικός αριθμός των αναφορών κακόβουλης συμπεριφοράς είναι 0 ή πολύ μικρός συγκριτικά με το σύνολο των χρηστών που συνδέθηκαν στο συνεργατικό περιβάλλον το συγκεκριμένο χρονικό διάστημα, τότε η μεταβολή στο βαθμό αξιοπιστίας είναι ανεπαίσθητη. Αντίθετα, όταν ο συνολικός αριθμός των αναφορών κακόβουλης συμπεριφοράς για το συγκεκριμένο χρονικό διάστημα είναι ίσος ή μεγαλύτερος από το σύνολο των προσπελάσεων του συνεργατικού περιβάλλοντος για το συγκεκριμένο μεσοδιάστημα, τότε ο παράγοντας Π_t κυμαίνεται μεταξύ $[1, +\infty)$ και είναι ικανός να επηρεάσει αρνητικά σε μεγάλο βαθμό την αξιοπιστία του χρήστη.

6.7 Θέματα υλοποίησης

Με βάση τα αποτελέσματα της διατριβής που παρουσιάστηκαν στην προηγούμενη ενότητα, ο βαθμός αξιοπιστίας για το χρήστη X_v καθορίζεται από τον ακόλουθο τύπο:

$$A_t(X_v) = \begin{cases} A_1(X_v), & \text{για } t = 1 \\ \alpha \left(\frac{\sigma}{\sigma + \mu_t} \right) A_{t-1}(X_v) + \beta \left(\frac{AP(X_v) |X|}{AP(X)} \right) - \gamma \left(\frac{\sum_{i=1}^k \Psi_i}{\delta(AP(X))} \right), & \text{για } t > 1 \end{cases}$$

Όπως είναι φυσικό, η υλοποίηση του αλγόριθμου υπολογισμού του βαθμού αξιοπιστίας απαιτεί τη δημιουργία ενός συνόλου λιστών ή αρχείων καταγραφής, όλων των απαραίτητων για την εφαρμογή του ΔΕΠ-ΕΣΠΣ, πληροφοριών καθώς και τον σαφή καθορισμό των συντελεστών επίδρασης α , β , γ . Τα θέματα αυτά αναλύονται στις ενότητες που ακολουθούν.

6.7.1 Λίστες δεδομένων

Αρχικά ορίζεται η *Λίστα Ταξινόμησης Κρίσιμων Πόρων*, η οποία ανανεώνεται κάθε φορά που προστίθεται ένα νέο υποσύνολο ΔΥΛ στο σύνολο των διαδραστικών δυνατοτήτων που παρέχει το συνεργατικό περιβάλλον και περιλαμβάνει εγγραφές της μορφής:

$$\{BK_i, \Delta YL_j\}, \text{ όπου}$$

- BK_i , ο Βαθμός Κρισιμότητας i με βάση την κανονικοποιημένη κλίμακα ποιοτικής ταξινόμησης των ΔΥΛ (βλ. ενότητα 6.4), και

- ΔΥΛ_j, το j-οστό υποσύνολο διαδραστικών υπηρεσιών και λειτουργιών που παρέχει το συνεργατικό περιβάλλον το οποίο ταξινομείται στο ΒΚ_i.

Δηλαδή σε αυτή τη λίστα καταγράφονται και ταξινομούνται όλοι οι κρίσιμοι πόροι του ΕΣΠΣ, υποσύνολα ΔΥΛ, σε Βαθμούς Κρισιμότητας.

Για κάθε βαθμό κρισιμότητας ΒΚ_i δημιουργείται μια *Λίστα Διαστημάτων Εμπιστοσύνης*, η οποία περιέχει εγγραφές της μορφής:

$$\{BK_i, [ΔE(BK_i)], [ΔE(BK_i)]\}, \text{ όπου}$$

- ΒΚ_i, ο Βαθμός Κρισιμότητας *i* με βάση την κανονικοποιημένη κλίμακα ποιοτικής ταξινόμησης των ΔΥΛ (βλ. ενότητα 6.4),
- [ΔE(BK_i)], το κάτω όριο του διαστήματος εμπιστοσύνης ή κατώφλι εμπιστοσύνης, ΚE(ΒΚ_i), που αντιστοιχεί σε ΔΥΛ με βαθμό κρισιμότητας ΒΚ_i,
- [ΔE(ΒΚ_i)], το άνω όριο του διαστήματος εμπιστοσύνης ή ανώφλι εμπιστοσύνης που αντιστοιχεί σε ΔΥΛ με βαθμό κρισιμότητας ΒΚ_i.

Για κάθε χρήστη, έστω X_v, που συμμετέχει στο συνεργατικό περιβάλλον δημιουργείται *Λίστα Καταγραφής Συμπεριφοράς* η οποία ανανεώνεται κάθε χρονική στιγμή *t* στην οποία ο χρήστης αιτείται να προσπελάσει το συνεργατικό περιβάλλον και η οποία περιέχει εγγραφές της μορφής:

$$\{ AP(X_v), AP(X), \Psi_t, A_t(X_v), KE(MBK), MBK \}, \text{ όπου}$$

- AP(X_v), ο Αριθμός Προσπελάσεων του χρήστη στο συνεργατικό περιβάλλον τη χρονική στιγμή *t*. Η μεταβλητή αυτή υποδηλώνει το πλήθος των επαναλήψεων που έχει εκτελεστεί η συνάρτηση υπολογισμού του βαθμού αξιοπιστίας για το συγκεκριμένο χρήστη,
- AP(X), ο Αριθμός Προσπελάσεων του συνεργατικού περιβάλλοντος για το σύνολο των χρηστών X τη χρονική στιγμή *t* που γίνεται το αίτημα προσπέλασης του χρήστη X_v. Η μεταβλητή αυτή υποδηλώνει το πλήθος των επαναλήψεων που έχει εκτελεστεί η μέθοδος υπολογισμού του βαθμού αξιοπιστίας για το σύνολο των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον,
- Ψ_t, το σύνολο των αναφορών κακόβουλης συμπεριφοράς που συγκέντρωσε ο χρήστης μέχρι τη χρονική στιγμή *t* για το σύνολο των ΔΥΛ (όπως έχει ήδη αναφερθεί σε κάθε βαθμό κρισιμότητας ΒΚ_i αντιστοιχεί ένα υποσύνολο Ψ_{i,t} το οποίο περιλαμβάνει τις αρνητικές ψήφους που καταγράφηκαν σε ΔΥΛ του συγκεκριμένου επιπέδου κρισιμότητας),
- A_t(X_v), ο βαθμός αξιοπιστίας του χρήστη X_v τη χρονική στιγμή *t*,

- KE(MBK), το μέγιστο Κατώφλι Εμπιστοσύνης το οποίο ικανοποιείται με βάση το βαθμό αξιοπιστίας $A_t(X_v)$ του χρήστη X_v τη χρονική στιγμή t έτσι ώστε $KE(MBK) \leq A_t(X_v)$,
- MBK, ο μέγιστος Βαθμός Κρισιμότητας μέχρι τον οποίο επιτρέπεται η πρόσβαση στο χρήστη τη χρονική στιγμή t . Με άλλα λόγια συμβολίζει το μέγιστο επίπεδο κρισιμότητας των ΔΥΛ τις οποίες επιτρέπεται να προσπελάσει ο χρήστης με βάση το νέο βαθμό αξιοπιστίας του.

Έχοντας ολοκληρώσει την περιγραφή της μεθόδου υπολογισμού του βαθμού αξιοπιστίας, γίνεται σαφές ότι εκτός από τους τρεις (3) βασικούς παράγοντες, σημαντικό ρόλο στον υπολογισμό του τελικού βαθμού αξιοπιστίας διαδραματίζουν και οι τρεις (3) συντελεστές επίδρασης α , β , γ .

Όπως παρουσιάζεται στη συνέχεια, οι συντελεστές αυτοί θα πρέπει να καθορίζονται ανάλογα με τις απαιτήσεις της εκάστοτε μελέτης εφαρμογής και αποτελούν αντικείμενο διαπραγμάτευσης μεταξύ των Παρόχων προκειμένου να καθορίζεται η αποτελεσματικότητα των πολιτικών ιδιωτικότητας οι οποίες θα υιοθετούνται για την προστασία των κρίσιμων πόρων του συνεργατικού περιβάλλοντος.

6.7.2 Συντελεστές επίδρασης

Έχοντας αναλύσει τόσο τη μέθοδο υπολογισμού του βαθμού αξιοπιστίας όσο και τον τρόπο με τον οποίο αυτός επηρεάζεται από τη συμπεριφορά των παραγόντων K_t , E_t , Π_t , γίνεται κατανοητό ότι η αποτελεσματικότητα της εφαρμογής της εξαρτάται σε μεγάλο βαθμό και από την επιλογή των συντελεστών επίδρασης α , β και γ .

Καθένας από αυτούς τους συντελεστές αντιπροσωπεύει τη βαρύτητα κάθε παράγοντα στον υπολογισμό του τελικού βαθμού αξιοπιστίας και, ως εκ τούτου, ο σαφής προσδιορισμός τους εξαρτάται απόλυτα από τις ανάγκες και τις απαιτήσεις του κάθε προκειμένου συνεργατικού περιβάλλοντος [20, 23, 31]. Ενδεικτικά αναφέρονται τα ακόλουθα χαρακτηριστικά τα οποία πρέπει να λαμβάνονται υπόψη για τον προσδιορισμό των α , β , γ :

- Πλήθος κρίσιμων πόρων που περιλαμβάνει το συνεργατικό περιβάλλον.
- Σύνολο επιπέδων ή βαθμών κρισιμότητας που απαιτούνται.
- Πλήθος χρηστών συνεργατικού περιβάλλοντος.
- Κρισιμότητα ΔΥΛ ως προς το γενικότερο επιχειρησιακό περιβάλλον στο οποίο παρέχονται.
- Συχνότητα χρήσης συνεργατικού περιβάλλοντος.
- Διάθεση χρηστών να συμμετέχουν ενεργά στην προστασία της ιδιωτικότητάς.

Το τελικό στάδιο εφαρμογής του μοντέλου ΔΕΠ-ΕΣΠΣ απαιτεί τη διαπραγμάτευση σε επίπεδο Παρόχων σχετικά με τις τιμές που θα λάβουν οι συντελεστές επίδρασης α , β , γ . Χαρακτηριστικά αναφέρεται ότι κάθε τριάδα τιμών $\{\alpha, \beta, \gamma\}$ σε συνδυασμό με τον καθορισμό της τιμής της σταθεράς σ (βλ. Παράρτημα Ι) αποτελούν μια ξεχωριστή πολιτική ιδιωτικότητας δεδομένου ότι καθορίζουν άμεσα τον υπολογισμό του βαθμού αξιοπιστίας των χρηστών με βάση τον οποίο γίνεται τελικά η απόδοση προνομίων προσπέλασης σε κρίσιμους πόρους του συνεργατικού περιβάλλοντος.

Με βάση τις σχέσεις που ισχύουν μεταξύ των τριών συντελεστών επίδρασης, διακρίνονται οι βασικές κατηγορίες πολιτικών ιδιωτικότητας που εμφανίζονται στον Πίνακα 7. Ο λεπτομερής καθορισμός των τιμών των συντελεστών α , β , γ απαιτεί ενδελεχή ανάλυση στατιστικών δεδομένων χρήσης του εκάστοτε συνεργατικού περιβάλλοντος και δεν αποτελεί αντικείμενο έρευνας της διατριβής.

Πολιτικές Ιδιωτικότητας	Περιπτώσεις	Σχόλια
Βαθμός επίδρασης του παράγοντα κρισιμότητας των αναφορών κακόβουλης συμπεριφοράς	$\alpha > 1$	Μεγάλο εύρος μεταβολής του βαθμού αξιοπιστίας όταν οι αναφορές κακόβουλης συμπεριφοράς καταγράφονται σε ΒΚ μεγαλύτερο από το ΜΒΚ.
	$0 < \alpha < 1$	Μικρό εύρος μεταβολής του βαθμού αξιοπιστίας όταν οι αναφορές κακόβουλης συμπεριφοράς καταγράφονται σε ΒΚ μεγαλύτερο από το ΜΒΚ.
Βαθμός επίδρασης παράγοντα προσωπικής επιβράβευσης χρηστών	0	Δεν παρέχεται επιβράβευση στο χρήστη για τη συμμετοχή του στις υπηρεσίες του συνεργατικού περιβάλλοντος.
	$\beta > 1$	Η συχνότητα συμμετοχής του χρήστη στο συνεργατικό περιβάλλον επηρεάζει θετικά και σε μεγάλο βαθμό την αξιοπιστία του.
	$0 < \beta < 1$	Η συχνότητα συμμετοχής του χρήστη στο συνεργατικό περιβάλλον επηρεάζει θετικά αλλά σε μικρό βαθμό την αξιοπιστία του.
Βαθμός επίδρασης του παράγοντα στάθμισης των αναφορών κακόβουλης συμπεριφοράς ως προς τη συνολική συμμετοχή στο συνεργατικό περιβάλλον	0	Η συχνότητα χρήσης του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών δεν επηρεάζει το βαθμό αξιοπιστίας.

	$\gamma > 1$	Ο βαθμός αξιοπιστίας επηρεάζεται αρνητικά και σε μεγάλο βαθμό όταν το πλήθος των αναφορών κακόβουλης συμπεριφοράς είναι μεγαλύτερο από τον αριθμό προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών σε κάθε μεσοδιάστημα.
	$0 < \gamma < 1$	Ο βαθμός αξιοπιστίας επηρεάζεται αρνητικά σε μικρό βαθμό όταν το πλήθος των αναφορών κακόβουλης συμπεριφοράς είναι μικρότερο από τον αριθμό προσπελάσεων του συνεργατικού περιβάλλοντος από το σύνολο των χρηστών σε κάθε μεσοδιάστημα.
Σχέσεις συντελεστών επίδρασης	$\beta = \gamma$	Η επιβράβευση των χρηστών είναι εξίσου σημαντική με τον παράγοντα στάθμισης των αναφορών κακόβουλης συμπεριφοράς.
	$\beta < \gamma$	Η επιβράβευση των χρηστών είναι λιγότερο σημαντική από τον παράγοντα στάθμισης των αναφορών κακόβουλης συμπεριφοράς.
	$\beta > \gamma$	Η επιβράβευση των χρηστών είναι περισσότερο σημαντική από τον παράγοντα στάθμισης των αναφορών κακόβουλης συμπεριφοράς.
	$\alpha = \beta = \gamma$	Η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς είναι εξίσου σημαντική με την επιβράβευση των χρηστών και τον παράγοντα στάθμισης του πλήθους των αναφορών.
	$\alpha > \beta > \gamma$	Η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς είναι περισσότερο σημαντική από την επιβράβευση των χρηστών και από τον παράγοντα στάθμισης του πλήθους των αναφορών.
	$\alpha < \beta < \gamma$	Η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς είναι λιγότερο σημαντική από την επιβράβευση των χρηστών και από τον παράγοντα στάθμισης του πλήθους των αναφορών.

	$\beta < \alpha < \gamma$	Η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς είναι περισσότερο σημαντική από την επιβράβευση των χρηστών και λιγότερο σημαντική από τον παράγοντα στάθμισης του πλήθους των αναφορών.
	$\beta > \alpha > \gamma$	Η κρισιμότητα των αναφορών κακόβουλης συμπεριφοράς είναι λιγότερο σημαντική από την επιβράβευση των χρηστών και περισσότερο σημαντική από τον παράγοντα στάθμισης του πλήθους των αναφορών.

Πίνακας 7: Πολιτικές προστασίας της ιδιωτικότητας

Με βάση τον Πίνακα 7, η εφαρμογή του μοντέλου ΔΕΠ-ΕΣΠΣ και της προτεινόμενης μεθόδου υπολογισμού του βαθμού αξιοπιστίας είναι ικανή να διασφαλίσει τη λήψη έμπιστων αποφάσεων απόδοσης προνομίων προσπέλασης στις διαδραστικές υπηρεσίες κάθε συνεργατικού περιβάλλοντος παρέχοντας τη δυνατότητα τόσο της συνεργατικής προστασίας της ιδιωτικότητας όσο και της διαπραγμάτευσης μεταξύ των Παρόχων σχετικά με τις πολιτικές που θα πρέπει να υιοθετηθούν.

6.8 Συνεισφορά αποτελεσμάτων στην προστασία της ιδιωτικότητας

Όπως παρουσιάστηκε στο δεύτερο κεφάλαιο, οι παραδοσιακές προσεγγίσεις ΣΔΑ χρησιμοποιούνται συνήθως σε περιβάλλοντα όπου είτε λαμβάνουν χώρα εμπορικές συναλλαγές είτε απαιτείται αξιολόγηση της ποιότητας του περιεχομένου και των παρεχομένων υπηρεσιών [18, 19, 21, 38, 39, 41]. Πιο συγκεκριμένα, στα συστήματα ψηφοφορίας δημοφιλών πλαισίων υπηρεσιών (π.χ. e-Bay, Amazon, Wikipedia) η συλλογική γνώση και συνεισφορά των χρηστών χρησιμοποιείται για την υποστήριξη στη λήψη αποφάσεων σχετικά με την ποιότητα των παρεχομένων υπηρεσιών καθώς και με το αν το προϊόν, οι πληροφορίες ή το περιεχόμενο που αναζητούν είναι αξιόπιστα [26, 35]. Αντίθετα, οι καταναμημένες αρχιτεκτονικές ΣΔΑ που υιοθετούνται κυρίως σε δίκτυα ομότιμων κόμβων δεν είναι κατάλληλες για εφαρμογή σε συνεργατικά περιβάλλοντα και ολοκληρωμένα Πληροφοριακά Συστήματα όπου απαιτείται η λειτουργία μια κεντρικής έμπιστης οντότητας.

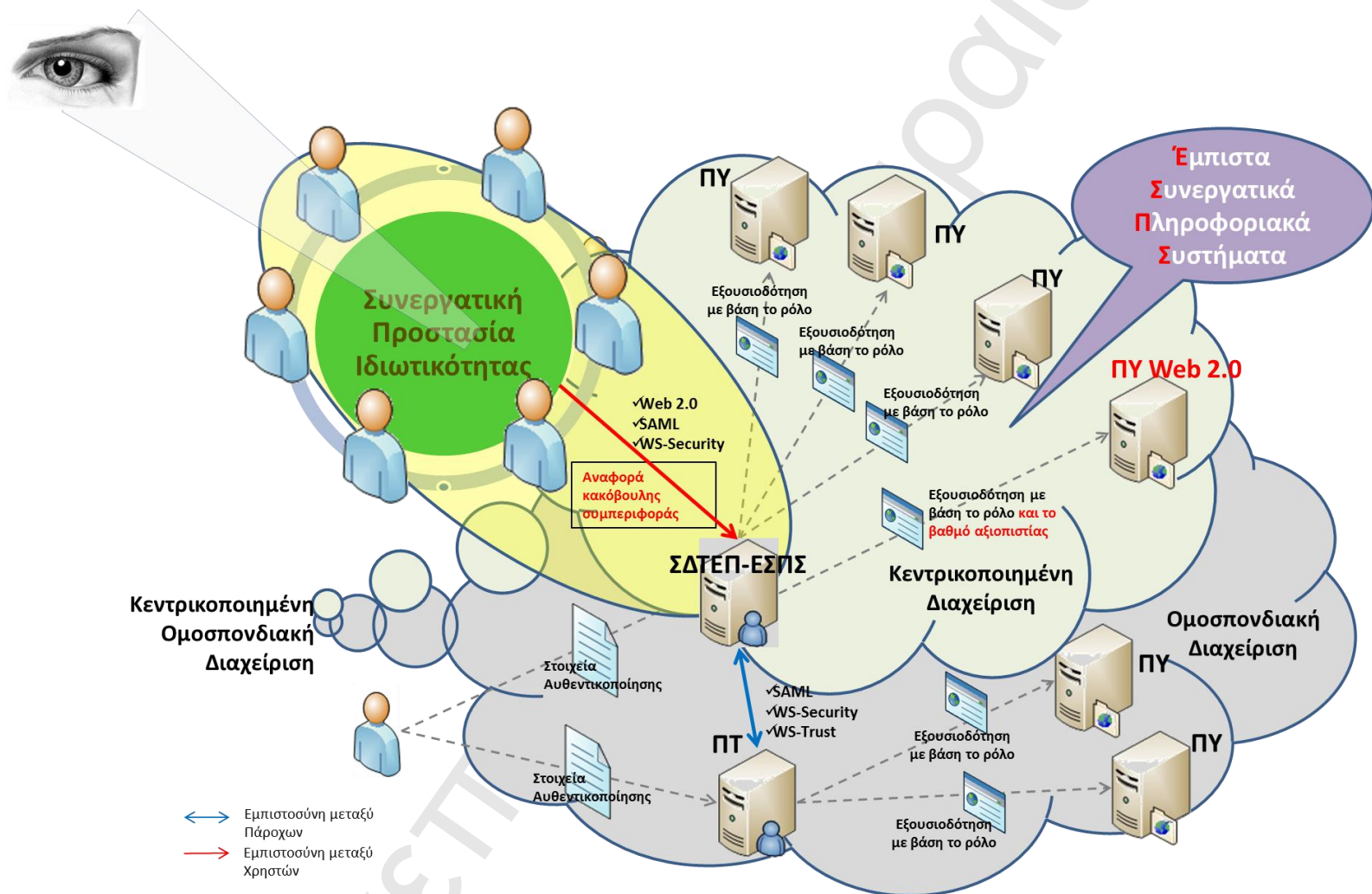
Η διατριβή διαπιστώνει ότι στα πλαίσια του ΕΣΠΣ όπου δε λαμβάνουν χώρα εμπορικές συναλλαγές αλλά απαιτείται η συλλογική συνεισφορά των συμμετεχόντων για τον εντοπισμό της κακόβουλης, ως προς την προστασία της ιδιωτικότητας, συμπεριφοράς που υιοθετεί κάθε χρήστης, ο βαθμός αξιοπιστίας είναι ικανός να χρησιμοποιηθεί αποτελεσματικά προκειμένου να

υποστηρίζονται οι διαδικασίες απόδοσης προνομίων προσπέλασης στις διαδραστικές υπηρεσίες.

Με βάση αυτή τη διαπίστωση, η διατριβή προτείνει την υιοθέτηση της αρχιτεκτονικής των κεντροποιημένων ΣΔΑ έτσι ώστε να καταγράφονται με καθολικό τρόπο οι αναφορές κακόβουλης συμπεριφοράς όσον αφορά στη χρήση των υπηρεσιών του συνεργατικού περιβάλλοντος καθώς και να εξασφαλίζεται ότι η χρήση των εφαρμογών Web 2.0 γίνεται με τρόπο που δεν προσβάλλει την ιδιωτικότητα. Η προσέγγιση αυτή μπορεί να θεωρηθεί ως μια καινοτόμος λύση δεδομένου ότι με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάστηκαν στην ενότητα 2.5.3, τα ΣΔΑ δεν έχουν χρησιμοποιηθεί μέχρι στιγμής ως μηχανισμοί ελέγχου προσπέλασης και προστασίας της ιδιωτικότητας σε συνεργατικά περιβάλλοντα.

Αυτή η καινοτομία της διατριβής επιτρέπει τον υπολογισμό του βαθμού αξιοπιστίας κάθε χρήστη με δυναμικό τρόπο και την ενσωμάτωσή του στα διαπιστευτήρια απόδοσης προνομίων προσπέλασης στις διαδραστικές υπηρεσίες και λειτουργίες που παρέχουν οι εφαρμογές *Web 2.0*, έτσι ώστε να διασφαλίζεται η εμπιστοσύνη και μεταξύ των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον.

Η Εικόνα 2 εμφανίζει τη συνολική εικόνα της προσανατολισμένης στη συλλογική προστασία της ιδιωτικότητας καινοτόμου λύσης διαχείρισης ταυτοτήτων που παρουσιάστηκε στις προηγούμενες ενότητες.



Εικόνα 2: Συλλογική προστασία της ιδιωτικότητας

Όπως φαίνεται στην εικόνα, η αρχιτεκτονική της κεντριοποιημένης ομοσπονδίας είναι σχεδιασμένη έτσι ώστε να καλύπτει τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών και να ικανοποιεί τις επιπρόσθετες απαιτήσεις προστασίας της ιδιωτικότητας που τίθενται στα πλαίσια του συνεργατικού περιβάλλοντος.

Προκειμένου να διασφαλιστεί η εμπιστοσύνη στα πλαίσια του ΕΣΠΣ, το ΣΔΤΕΠ όχι μόνο συνάπτει σχέσεις εμπιστοσύνης με άλλους Παρόχους Ταυτοτήτων (μπλε βέλος μεταξύ ΠΤ) αλλά παράλληλα όπως φαίνεται στη σκιασμένη περιοχή της Εικόνα 2 διαχειρίζεται την αξιοπιστία των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον μέσω της συλλογικής συνεισφοράς των συμμετεχόντων (κόκκινο βέλος μεταξύ ΣΔΤΕΠ και κοινότητας χρηστών).

Ειδικότερα, η συλλογική προστασία της ιδιωτικότητας απαιτεί την εφαρμογή ενός ασύγχρονου μηχανισμού ο οποίος θα υποστηρίζει την ενεργή συνεισφορά των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον στον εντοπισμό κακόβουλου περιεχομένου. Έτσι το ΣΔΑ είναι ικανό να καταγράφει με δυναμικό τρόπο τις αλλαγές στη συμπεριφορά του χρήστη και τελικά να προωθεί αυτή την πληροφορία στο ΣΔΤΕΠ προκειμένου να δημιουργήσει τα κατάλληλα διαπιστευτήρια εξουσιοδότησης κάθε φορά που ο χρήστης αιτείται να προσπελάσει το συνεργατικό περιβάλλον.

Σε τεχνολογικό επίπεδο, αυτό απαιτεί την εφαρμογή διαδραστικών διεπαφών Web 2.0, έτσι ώστε να καταγράφονται οι αρνητικοί ψήφοι των χρηστών με δυναμικό τρόπο. Επίσης, είναι απαραίτητη η ενσωμάτωση του βαθμού αξιοπιστίας σε διαπιστευτήρια εξουσιοδότησης SAML ώστε να χρησιμοποιείται ως κριτήριο απόδοσης δικαιωμάτων πρόσπέλασης στις διαδραστικές υπηρεσίες και λειτουργίες των συνεργατικών εφαρμογών. Τέλος, αποτελεί αδήριτη ανάγκη η εφαρμογή των προδιαγραφών ασφάλειας WS-Security για τη διασφάλιση της ακεραιότητας των μεταφερόμενων δεδομένων.

Εν κατακλείδι, αξιοποιώντας τη συλλογική γνώση όλων των χρηστών σχετικά με την αξιοπιστία του κάθε χρήστη στο να χρησιμοποιεί τις ΔΥΛ των κρίσιμων, ως προς την προστασία της ιδιωτικότητας, εφαρμογών Web 2.0 χωρίς να προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων, τα αποτελέσματα της διατριβής συνεισφέρουν στη δημιουργία έμπιστων πληροφοριακών συστημάτων συνεργασίας και αλληλεπίδρασης, τα οποία είναι ικανά να καλύπτουν αποτελεσματικά τις νέες απαιτήσεις για την προστασία της ιδιωτικότητας.

Η καινοτομία που προτείνεται στο πλαίσιο της διατριβής βασίζεται στο ότι ο βαθμός αξιοπιστίας προκύπτει ως αποτέλεσμα συλλογικής γνώσης και, δεδομένου ότι μπορεί να χρησιμοποιηθεί αποτελεσματικά ως μέτρο αξιολόγησης της συμπεριφοράς των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον, η ενσωμάτωση του ΣΔΑ στο ΣΔΤΕΠ του ΕΣΠΣ αποτελεί μια εξίσου καινοτόμο προσέγγιση [2].

Πιο συγκεκριμένα, ο Πίνακας 8 παρουσιάζει τον τρόπο με τον οποίο διαφοροποιείται η προτεινόμενη εφαρμογή του ΣΔΑ από τις σύγχρονες προσεγγίσεις που ακολουθούνται μέχρι σήμερα [4, 14, 15, 16, 17].

	Παραδοσιακές Προσεγγίσεις Κεντροποιημένης Διαχείρισης Εμπιστοσύνης	Παραδοσιακές Προσεγγίσεις Κατανεμημένης Διαχείρισης Εμπιστοσύνης	Προτεινόμενη Εφαρμογή ΣΔΑ
Στόχος	Βελτίωση Ποιότητας Παρεχομένων Υπηρεσιών	Βελτίωση δικτυακής επικοινωνίας και αλληλεπίδρασης ομότιμων κόμβων	Προστασία Ιδιωτικότητας
Μέθοδος υπολογισμού	Εκτελείται από το κεντρικό ΣΔΑ και βασίζεται στη συνεισφορά των οντοτήτων που συμμετέχουν στο δίκτυο εμπιστοσύνης για τον υπολογισμό του μέσου όρου ή του σταθμισμένου μέσου των ψήφων τους.	Εκτελείται από κάθε οντότητα που συμμετέχει στο δίκτυο εμπιστοσύνης και τα αποτελέσματα αποθηκεύονται τοπικά σε κάθε κόμβο, είτε είναι ευρέως διαθέσιμα είτε αποτελούν ιδιωτικές πληροφορίες του κόμβου.	Εκτελείται από το κεντρικό ΣΔΑ και βασίζεται στη συνεισφορά των οντοτήτων/χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον για να υπολογίσει το βαθμό αξιοπιστίας των χρηστών όσον αφορά στη δημιουργία περιεχομένου το οποίο δεν προσβάλλει την ιδιωτικότητα.
Εφαρμογές	η-Εμπόριο, η-Εκπαίδευση, η-Οικονομία	Δίκτυα ομότιμων κόμβων, Δρομολόγηση σε ασύρματα δίκτυα Δίκτυα αισθητήρων	η-Διακυβέρνηση, η-Δημοκρατία, η-Υγεία
Μοντέλα	e-Bay [47], OpenPrivacy [50]	TwoHop [45], Poblano [46], GNUnet [48], P2Prep [51], PGP [49], Jiang et al. [52]	Κεντροποιημένη Ομοσπονδία, ΔΕΠ-ΕΣΠΣ

Πίνακας 8: Σύγκριση ΣΔΑ-ΕΣΠΣ και παραδοσιακών προσεγγίσεων

Η ολοκλήρωση του ΣΔΑ στο ΣΔΤΕΠ-ΕΣΠΣ με βάση την αρχιτεκτονική της κεντροποιημένης ομοσπονδίας, αποτελεί μια ακόμα καινοτομία καθώς όπως φαίνεται και στον Πίνακα 8 τα ΣΔΑ δεν έχουν χρησιμοποιηθεί μέχρι στιγμής για την απόδοση προνομίων προσπέλασης, και, πιο συγκεκριμένα, για την αξιολόγηση του βαθμού αξιοπιστίας των χρηστών στη χρήση των διαδραστικών υπηρεσιών και λειτουργιών που παρέχει το συνεργατικό περιβάλλον. Όπως παρουσιάστηκε στην ενότητα 6.6, η δεύτερη αυτή καινοτομία συνεισφέρει αποτελεσματικά στη διασφάλιση της ιδιωτικότητας των χρηστών και στην προστασία των προσωπικών τους δεδομένων από κακόβουλη χρήση των εφαρμογών Web 2.0.

Επιπρόσθετα, τα αποτελέσματα της διατριβής συνεισφέρουν στη συνεχή αξιολόγηση του περιεχομένου του συνεργατικού περιβάλλοντος ως προς την καταλληλότητά του καθώς και στον περιορισμό των κακόβουλων ενεργειών. Παρέχουν επίσης θετικά κίνητρα για τη συμμόρφωση της συμπεριφοράς των χρηστών δεδομένου ότι οι

περισσότεροι χρήστες ικανοποιούνται όταν χαρακτηρίζονται από υψηλό βαθμό αξιοπιστίας και ανταποκρίνονται με αντίστοιχες ενέργειες προκειμένου να τον επιτύχουν και να τον διατηρήσουν.

Η διατριβή καταλήγει ότι οι χρήστες όχι μόνο επωφελούνται από τη χρήση ΣΔΑ για τη συλλογική προστασία της ιδιωτικότητας και τη δυναμική απόδοση προνομίων προσπέλασης αλλά παράλληλα εκπαιδεύονται στην υιοθέτηση καλών πρακτικών χρήσης των διαδραστικών λειτουργιών που παρέχουν οι εφαρμογές Web 2.0, δεδομένου ότι χαμηλές τιμές του βαθμού αξιοπιστίας έχουν αντίκτυπο στα προνόμια προσπέλασης των παρεχομένων υπηρεσιών.

Με βάση το Σχέδιο Ιδιωτικότητας του ΕΣΠΣ και τις απειλές που αντιμετωπίζουν τα ΣΔΑ όπως περιγράφηκαν στο πέμπτο κεφάλαιο, είναι σημαντικό να σημειωθεί ότι στην πλειοψηφία τους απειλές, όπως για παράδειγμα οι επιθέσεις whitewashing και οι επιθέσεις Sybil, αντιμετωπίζονται αποτελεσματικά από το γεγονός ότι το ΣΔΑ ολοκληρώνεται στην αρχιτεκτονική του ΣΔΤΕΠ και ως εκ τούτου η ασφαλής και αξιόπιστη λειτουργία του αποτελεί αναπόσπαστο χαρακτηριστικό του ΕΣΠΣ (βλ. ενότητα 6.4).

Επίσης, το γεγονός ότι το ΣΔΑ χρησιμοποιείται για την αναφορά και διαχείριση μόνο της κακόβουλης συμπεριφοράς δεν επιτρέπει τη διενέργεια επιθέσεων με στόχο την αύξηση του βαθμού αξιοπιστίας και των αντίστοιχων προνομίων προσπέλασης. Τέλος, η συμμετοχή και άλλων παραγόντων εκτός των αναφορών κακόβουλης συμπεριφοράς στον υπολογισμό του βαθμού αξιοπιστίας καθιστά πολύ δύσκολη την μη-εξουσιοδοτημένη τροποποίησή του από κακόβουλους χρήστες καθώς και την εφαρμογή επιθέσεων *συνωμοσίας* και *Sybil* [42].

6.9 Συμπεράσματα

Τα χαρακτηριστικά των παραδοσιακού μοντέλου ΕΠΡ (βλ. ενότητα 2.3.1.3) δεν επαρκούν για να καλύψουν τις απαιτήσεις σε συνεργατικά περιβάλλοντα όπου όλοι οι χρήστες ανεξαρτήτως του ρόλου τους έχουν την ίδια δυναμική να προσβάλλουν την ιδιωτικότητα των υπολοίπων συμμετεχόντων μέσω της χρήσης των διαδραστικών υπηρεσιών και εφαρμογών αλληλεπίδρασης. Με βάση τα αποτελέσματα της έρευνας πεδίου που παρουσιάστηκαν στην ενότητα 2.4.1, η αποτελεσματική ολοκλήρωση εφαρμογών Web 2.0 σε έμπιστα Πληροφοριακά Συστήματα και η παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών απαιτεί την αναβάθμιση των παραδοσιακών προσεγγίσεων Διαχείρισης Ταυτοτήτων.

Συνεισφέροντας προς αυτή την κατεύθυνση, η διατριβή προτείνει ότι η απόδοση προνομίων προσπέλασης στις διαδραστικές υπηρεσίες και λειτουργίες που παρέχει το ΕΣΠΣ πρέπει να γίνεται με δυναμικό τρόπο, αξιολογώντας την αξιοπιστία των χρηστών που συμμετέχουν στο συνεργατικό περιβάλλον η οποία αλλάζει κάθε χρονική στιγμή ανάλογα με τη συμπεριφορά τους, και όχι με βάση ένα στατικά προκαθορισμένο ρόλο που τους έχει αποδοθεί. Λαμβάνοντας μάλιστα υπόψιν το γεγονός ότι κανένα άλλο χαρακτηριστικό της ταυτότητας δεν είναι ικανό να

υποδηλώσει το κατά πόσο η συμπεριφορά των χρηστών σέβεται την ιδιωτικότητα των υπολοίπων συμμετεχόντων, το μοντέλο ΔΕΠ-ΕΣΠΣ προτείνει το βαθμό αξιοπιστίας ως βασικό κριτήριο για τη λήψη αποφάσεων εξουσιοδότησης στις υπηρεσίες Web 2.0.

Τέλος, προτείνεται μια αναδρομική μέθοδος υπολογισμού του βαθμού αξιοπιστίας η οποία εκτός από τις αναφορές κακόβουλης συμπεριφοράς των χρηστών συνυπολογίζει και άλλους παράγοντες που επηρεάζουν τις αποφάσεις απόδοσης προνομίων προσπέλασης στις υπηρεσίες του συνεργατικού περιβάλλοντος, όπως για παράδειγμα ο βαθμός συμμόρφωσης του χρήστη, η επιβράβευση συμμετοχή στο συνεργατικό περιβάλλον και ο συντελεστής στάθμισης του πλήθους των αναφορών κακόβουλης συμπεριφοράς. Παράλληλα, η μέθοδος αυτή είναι ικανή να αντιμετωπίζει τις απειλές ιδιωτικότητας που χαρακτηρίζουν τα συνεργατικά περιβάλλοντα καθώς και να ικανοποιεί τις σύγχρονες απαιτήσεις για διαπραγμάτευση των πολιτικών απόδοσης προνομίων εξουσιοδότησης μεταξύ ετερογενών Πληροφοριακών Συστημάτων.

6.10 Βιβλιογραφία

- [1] G. Pentafronimos, T. Karantjias, N. Polemi (2012). "PEIM2.0: A privacy-enhancing IAM architecture for collaborative environments". In Proceedings of the 6th International Conference on Methodologies, Technologies and Tools enabling e-Government, (MeTTeG 2012). Belgrade, Serbia, July 3-5.
- [2] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Collaborative information and knowledge management environments: The "what" and "how"". OR Insight Journal, Special Issue on Facilitating information and knowledge management through Information Systems and Operational Research: from theory to practice.
- [3] G. Pentafronimos, A. Karantjias, N. Polemi (2011). "Open Issues on Privacy and Trust in Collaborative Environments". In Proceedings of the IEEE Symposium on Computers and Communications (ISCC 2011), Kerkyra, Greece, 2011. IEEE Publisher.
- [4] Δ. Γλυνός (2012). «Αρχιτεκτονική, Διαχείριση και Ασφάλεια Προγραμματιζόμενων Δικτυακών Υποδομών». Διδακτορική διατριβή, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς.
- [5] M. Ali, L. Bussard, U. Pinsdorf (2010). "Obligation Language and Framework to Enable Privacy-Aware SOA". Data Privacy Management and Autonomous Spontaneous Security. Lecture Notes in Computer Science, Vol. 5939/2010, pp. 18-32. Springer Verlag.
- [6] A. Jøsang, R. Ismail, C. Boyd (2007). "A Survey of Trust and Reputation Systems for Online Service Provision". Journal of Decision Support Systems. Vol. 43 (2), pp. 618-644. Elsevier.
- [7] K. Cameron, R. Posch, K. Rannenberg (2008). "Proposal for a Common Identity Framework: A User-Centric Identity Metasystem".
- [8] A. Bhargavspantzel, A. Squicciarini, E. Bertino (2005). "Trust Negotiation in Identity Management". IEEE Security & Privacy.
- [9] J. Camenisch, B. Pfitzmann (2007). "Federated Identity Management". Security, Privacy and Trust in Modern Data Management. Data-Centric Systems and

Applications, pp. 213-238. Springer-Verlag,

- [10] A. GailJoon, J. Lam (2005). "Managing privacy preferences for federated identity management" Proceedings of the 2005 workshop on Digital identity management (DIM '05) pp. 28 – 36. ACM Press.
- [11] S. Preibusch, B. Hoser, S. Gurses, B. Berendt (2007). "Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling". In Proceedings of the Data Mining for User Modelling Workshop (DM.UM'07), Corfu.
- [12] S. Pearson, M. C. Mont (2006). "Provision of Trusted Identity Management Using Trust Credentials". Trust Managemen. Lecture Notes in Computer Science, Vol. 3986/2006, pp. 267-282.
- [13] S. Park, L. Liu, C. Pu, M. Srivatsa, J. Zhang. (2005). "Resilient Trust Management for Web Service Integration". In Proceedings of the IEEE International Conference on Web Services (ICWS '05), pp. 499-506.
- [14] L. Mui, M. Mohtashemi, A. Halberstadt. (2002). "A Computational Model of Trust and Reputation". In Proceedings of the 35th Hawaii International Conference on System Sciences.
- [15] Y. Zou, L. Gu, G. Li, B. Xie, H. Mei. (2007). "Rectifying Prejudicial Feedback Ratings in Reputation based Trust Management". In Proceedings of the IEEE International Conference on Services Computing (SCC 2007), pp.530-535.
- [16] S. Steinbrecher. (2007). "Privacy-respecting Reputation System for Future Internet Communities", ENISA eID Workshop.
- [17] S. Crane, M. C. Mont. (2006). "A Customizable Reputation-based Privacy Assurance System using Active Feedback", Securecomm and Workshops.
- [18] K. J. Lin (2005). "A Reputation and Trust Management Broker Framework for Web Applications". In Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Services, pp. 262–269. IEEE CS Press.
- [19] C. Andersson, J. Camenisch, S. Crane, S. Fischer-Hubner, R. Leenes, S. Pearsorr, J.S. Pettersson, D. Sommer (2005). "Trust in PRIME", Fifth IEEE International Symposium on Signal Processing and Information Technology, pp.552-559.

- [20] M. Pekárek, S. Pöttsch (2009). "A comparison of privacy issues in collaborative workspaces and social networks". Identity in the Information Society, Special Issue: Social Web and Identity. Vol. 2 (1), pp. 81-93. Springer. B. Carminati, E. Ferrari, A. Perego (2009). "Enforcing Access Control in Web-Based Social Networks". ACM Transactions on Information and System Security. Vol. 13 (1), pp. 1-38. ACM Publishing.
- [21] S. Kamvar, M. Scholsser, H. Garcia-Molina. (2003). "The EigenTrust Algorithm for Reputation Management in P2P Networks". In Proceedings of the 12th international conference on World Wide Web.
- [22] ENISA (2011). "Report on trust and reputation model: Evaluation and guidelines".
- [23] V. Cahill, B. Shand, E. Gray, (2003). "Using Trust for Secure Collaboration in Uncertain Environments". Pervasive Computing. Vol. 2 (3), pp. 52.61.
- [24] Jøsang (2001). "A Logic for Uncertain Probabilities". International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. Vol. 9(3), pp. 279 - 311.
- [25] J. Sabater, C. Sierra. (2002). "Reputation and Social Network Analysis in Multi-Agent Systems". In Proceedings of the First Int. Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS).
- [26] J. Sabater, C. Sierra. (2002). "Social ReGreT, a reputation model based on social relations", SIGecom Exchanges. Vol. 3 (1) pp. 44.56.
- [27] R. Levien. (2004). "Attack Resistant Trust Metrics", PhD thesis, University of California at Berkeley.
- [28] C.-N. Ziegler, G. Lausen. (2004). "Spreading Activation Models for Trust Propagation". In Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE '04), Taipei.
- [29] S. Sen, N. Sajja. (2002). "Robustness of Reputation-based Trust: Boolean Case". In the first Int. Joint Conference on Autonomous Agents & Multi-agent Systems (AAMAS). ACM Press.
- [30] H. C. Choi, S. Kruk, S. Grzonkowski, K. Stankiewicz, B. Davis, J. Breslin (2006). "Trust Models for Community Aware Identity Management". In Proceedings of

the Identity, Reference and Web Workshop, in conjunction with WWW 2006.

- [31] A. C. Squicciarini, M. Shehab, F. Paci (2009). "Collective privacy management in social networks". In Proceedings of the 18th international conference on World wide web WWW '09, pp. 521-530. ACM Publications.
- [32] R. Bhatti, E. Bertino, A. Ghafoor (2007). "An integrated approach to federated identity and privilege management in open systems". Spam and the ongoing battle for the inbox CACM. Vol. 50 (2) pp. 81-87. ACM Publications.
- [33] E. Franz, K. Liesebach, K. Pfitzmann (2006). "Privacy-aware user interfaces within collaborative environments". In Proceedings of the international workshop in conjunction with AVI 2006 on Context in advanced interfaces, (CAI '06). pp. 45 – 48. ACM Publications.
- [34] E. McCallister, T. Grance, K. Scarfone (2010). "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)". Recommendations of the National Institute of Standards and Technology.
- [35] A. Squicciarini, E. Bertino (2007). "PP-Trust-X: A System for Privacy Preserving Trust Negotiations". ACM Transactions on Information and System Security, Vol. 10 (3), Article 12.
- [36] J. Jang, W. Shi, H. S. Yoo (2007). "Collaborative Privacy Management System". In Proceedings of the 2008 International Conference on Information Security and Assurance (ISA '08). pp. 52-56. Elsevier.
- [37] J. Nin, B. Carminati, E. Ferrari, V. Torra (2009). "Computing Reputation for Collaborative Private Networks". In Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference. Vol. 01, pp. 246-253. IEEE Publications.
- [38] E. Androulaki, M. Johnson, B. Vo, S. Bellovin (2009). "Cybersecurity through an Identity Management System". In Engaging Data Forum, MIT.
- [39] M. Carbone, M. Nielsen, V. Sassone (2003). "A Formal Model for Trust in Dynamic Networks". In Proceedings of International Conference on Software Engineering and Formal Methods (SEFM '03).
- [40] J. B. Lezoray, M. Pasquet (2009). "Enabling collaboration between

heterogeneous circles of trust through innovative identity solutions”. In Proceedings of the 2009 International Symposium on Collaborative Technologies and Systems. pp. 476-484. IEEE Publisher.

- [41] E. Gray, J. Seigneur, C. Jensen, C. Yong, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow, M. Nielson (2003). “Using trust for secure collaboration in uncertain environments”. Pervasive Computing. Vol. 2 (3). pp. 52 – 61. ACM Publications.
- [42] T. Hogg (2009). “Security challenges for reputation mechanisms using online social networks”. In Proceedings of the 2nd ACM workshop on Security and artificial intelligence (AISec '09). pp. 31-34. ACM Publications.
- [43] A. Lampinen (2010). “Practices of balancing privacy and publicness in social network services”. In Proceedings of the 16th ACM international conference on Supporting group work (GROUP '10). pp. 343-344. ACM Publications.
- [44] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thuraisingham (2011). “Semantic web-based social network access control”. Computers & Security, Special Issue on Access Control Methods and Technologies. Vol. 30 (2–3), pp. 108–115. ACM Publications.
- [45] D. Glynos, P. Argyroudis, C. Douligeris (2012). “Collaborative service evaluation with the TwoHop Trst Framework”. Security and Communication Networks. Vol. 5, pp. 549-613.
- [46] R. Chen, W. Yeager (2003). “Poblano: a Distributed Trust Model for Peer-to-Peer Networks”. Technical report. Sun Microsystems.
- [47] eBay Inc. (2012) “Online Auction and Shopping Website”. <http://www.ebay.com>
- [48] D. Kugler (2003). “An analysis of GUNet and the Implications for Anonymous, Censorship-Resistant Networks”. In Proceedings of 3rd Workshop on Privacy Enhancing Technologies (PET '03), pp. 161-176.
- [49] P. Zimmermann (1995). The Official PGP User’s Guide. MIT Press.
- [50] F. Labalme, K. Burton (2001). “Enhancing the Internet with Reputations: an OpenPrivacy White Paper”. <http://openprivacy.org/papers/200103-white.html>

- [51] F. Cornelli, E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati (2002). "Choosing Reputable Servents in a P2P Network". In Proceedings of 11th International World Wide Web Conference (W3C '02). Honolulu, Hawaii.
- [52] T. Jiang, J. Baras (2006). "Trust Evaluation in Anarchy: A case study on Autonomous Networks". In Proceedings of 25th IEEE International Conference on Computer Communications (Infocom '06), pp. 1-12. Barcelona, Spain.

Πανεπιστήμιο Πειραιώς

Κεφάλαιο 7

Μελέτη Περίπτωσης: Εφαρμογή ΕΣΠΣ στον τομέα της η-Μετανάστευσης

Οι υπηρεσίες η-Διακυβέρνησης είναι ικανές να συνεισφέρουν στη γεφύρωση του ψηφιακού χάσματος και στην αξιοποίηση των δυνατοτήτων των σύγχρονων τεχνολογιών ώστε να λειτουργεί πιο αποδοτικά ο κρατικός μηχανισμός και να διευκολύνονται οι αλληλεπιδράσεις των πολιτών με τις δημόσιες υπηρεσίες και οργανισμούς. Τα σύγχρονα πλαίσια υπηρεσιών η-Διακυβέρνησης θα πρέπει παράλληλα να βοηθούν στην αντιμετώπιση της κοινωνικής ανισότητας και στην καταπολέμηση του αποκλεισμού κοινωνικών ομάδων από τη χρήση αντίστοιχων υπηρεσιών.

Με βάση την έρευνα πεδίου που πραγματοποιήθηκε στο πλαίσιο της διατριβής [33, 34, 35, 36], παρατηρείται το φαινόμενο ότι παρά την άνθιση και την ευρεία αποδοχή των υπηρεσιών η-Διακυβέρνησης από τους πολίτες, εντούτοις η παροχή υπηρεσιών σε ευπαθείς κοινωνικές ομάδες όπως οι νόμιμοι μετανάστες δεν παρουσιάζουν αντίστοιχη εξέλιξη [31]. Όπως αναλύεται στις ενότητες που ακολουθούν, η διατριβή διαπιστώνει τις ιδιαίτερες προκλήσεις που χαρακτηρίζουν τον τομέα της μετανάστευσης και συνεισφέρει στην αντιμετώπισή τους με τα αποτελέσματα που παρουσιάζονται στη συνέχεια [32].

Πιο συγκεκριμένα, έχοντας σαν βασικό στόχο σε αυτόν τον ερευνητικό άξονα της διατριβής την αξιολόγηση του βαθμού στον οποίο το ΕΣΠΣ που παρουσιάστηκε στο τέταρτο κεφάλαιο είναι ικανό να ανταποκριθεί στις απαιτήσεις που χαρακτηρίζουν κρίσιμους τομείς της σύγχρονης Κοινωνίας της Πληροφορίας (π.χ. Διακυβέρνηση, Εκπαίδευση, Υγεία, Μετανάστευση) για παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών οι οποίες επιτρέπουν την ενεργή συμμετοχή και διαδραστικότητα των χρηστών προστατεύοντας παράλληλα την ιδιωτικότητά τους, τα αποτελέσματα της διατριβής που παρουσιάζονται στις ενότητες που ακολουθούν προτείνουν την αναβάθμιση των ηλεκτρονικών υπηρεσιών που παρέχονται στον τομέα της μετανάστευσης (υπηρεσίες η-Μετανάστευσης) με την εφαρμογή του ΕΣΠΣ για την παροχή υπηρεσιών προς νόμιμους μετανάστες.

7.1 Εισαγωγή

Η κοινωνική ενσωμάτωση των νόμιμων μεταναστών και η ανάπτυξη εναρμονισμένων πολιτικών και αποτελεσματικών διαδικασιών για την ικανοποίηση αυτού του στόχου αποτελεί στις μέρες μας μείζον πρόβλημα τόσο σε εθνικό όσο και σε Ευρωπαϊκό επίπεδο.

Η Ευρωπαϊκή Ψηφιακή Ατζέντα 2020⁶ (European Digital Agenda –EDA 2020, Pilar VII, article 66) δίνει έμφαση στη δυνατότητα των σύγχρονων Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) να παρέχουν καλύτερες δημόσιες υπηρεσίες για το μεγαλύτερο εύρος της κοινωνίας και πολύ περισσότερο για εκείνες τις κοινωνικές ομάδες οι οποίες αντιμετωπίζουν τον κίνδυνο του κοινωνικο-οικονομικού αποκλεισμού, όπως για παράδειγμα οι νόμιμοι μετανάστες [37, 38, 39]. Με τον τρόπο αυτό θα είναι σε θέση να συμμετέχουν επί ίσοις όροις στις σύγχρονες κοινωνίες της Ψηφιακής Εποχής, ενισχύοντας την οικονομική ανάπτυξη και την ευημερία.[40, 41].

Με βάση την έρευνα πεδίου που παρουσιάζεται στην επόμενη ενότητα, διαπιστώνεται ότι από τη μια πλευρά οι νόμιμοι μετανάστες είναι σε θέση να συνεισφέρουν αποφασιστικά στην οικονομική ανάπτυξη και στην αύξηση του ανταγωνισμού των χωρών που τους φιλοξενούν, ενώ από την άλλη πλευρά το συνεχώς αυξανόμενο μεταναστευτικό κύμα εργασίας θα πρέπει σύντομα να αντιμετωπιστεί καθώς τα ποσοστά παράνομης εργασίας συνεχίζουν να αυξάνονται προκαλώντας κοινωνικές ανισότητες, ξеноφοβία και ρατσισμό [42]. Ιδιαίτερα οι εκπαιδευτικά και επαγγελματικά καταρτισμένοι νόμιμοι μετανάστες και αλλοδαποί επιχειρηματίες, οι οποίοι αναμένεται να ενισχύσουν την ανταγωνιστικότητα τόσο σε εθνικό όσο και σε Ευρωπαϊκό επίπεδο, θα πρέπει να ξεπεράσουν τα εμπόδια που αντιμετωπίζουν στις προσπάθειές τους για κοινωνική ενσωμάτωση [43, 44, 45].

Η αποδοτική αλληλεπίδρασή τους με κρατικούς μηχανισμούς, η κατανόηση και επιτυχημένη συμμόρφωσή τους με τις νόμιμες αλλά μερικές φορές ιδιαίτερα πολύπλοκες διαδικασίες (π.χ. πιστοποίηση πτυχίων και διπλωμάτων, έκδοση μεταναστευτικών εγγράφων, ανταπόκριση και συμμετοχή σε κυβερνητικές πρωτοβουλίες) καθώς και με τις κοινωνικές ιδιαιτερότητες κάθε γεωγραφικής περιοχής, αποτελούν μεταξύ άλλων πρωταρχικές λύσεις για την αντιμετώπιση των υφιστάμενων εμποδίων.[46] Επιτακτική λοιπόν κρίνεται η ανάγκη ανάπτυξης καινοτόμων ηλεκτρονικών υπηρεσιών οι οποίες θα είναι ικανές να επιλύσουν τα σύγχρονα κοινωνικά προβλήματα και προκλήσεις.

Διαπιστώνεται επίσης ότι η ηλεκτρονική διακυβέρνηση περνά μια κρίσιμη καμπή οριακής εξέλιξης καθώς τα σύγχρονα πλαίσια συνεργασίας, οι υφιστάμενες πρωτοβουλίες και οι παρεχόμενες υπηρεσίες δεν καταφέρνουν να αντιμετωπίσουν το πρόβλημα ολιστικά. [47] Εκτός του ότι δεν αξιοποιούν με αποτελεσματικό τρόπο τις δυνατότητες των διαδραστικών εφαρμογών Web 2.0, στοχεύουν είτε στην

⁶ http://ec.europa.eu/information_society/digital-agenda/index_en.htm

ικανοποίηση των απαιτήσεων για αποτελεσματική λήψη αποφάσεων εκ μέρους των κυβερνητικών φορέων, είτε στην παροχή βασικών υπηρεσιών η-Διακυβέρνησης προς τους νόμιμους μετανάστες οι οποίες περιορίζονται στην παροχή πληροφοριών και στοιχείων επικοινωνίας με τους αρμόδιους φορείς.

Όπως αναλύεται στην επόμενη ενότητα, οι αναχρονιστικές αυτές προσεγγίσεις πολύ σπάνια θεωρούνται ως συμπληρωματικές εμποδίζοντας έτσι την ανάπτυξη προηγμένων λύσεων ικανών να αντιμετωπίσουν αποτελεσματικά κρίσιμους τομείς όπως αυτός της η-Μετανάστευσης. Η διατριβή συνεισφέρει προς αυτή την κατεύθυνση προτείνοντας ένα ολοκληρωμένο πλαίσιο καινοτόμων υπηρεσιών, το οποίο αξιοποιεί τις δυνατότητες του ΕΣΠΣ για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

7.2 Έρευνα πεδίου στον τομέα της η-Μετανάστευσης

Λαμβάνοντας υπόψιν την επίδραση της δημογραφικής ύφεσης στην Ευρωπαϊκή οικονομία, το Ευρωπαϊκό Συμβούλιο ανέδειξε την ανάγκη για αναθεώρηση των μεταναστευτικών πολιτικών υπογραμμίζοντας την άμεση επίδραση μιας αποτελεσματικής οικονομικής μεταναστευτικής πολιτικής στην ανταγωνιστικότητα και στην επίτευξη των στόχων της Συνθήκης της Λισσαβόνας. Παρόλα αυτά, στατιστικές μελέτες αποδεικνύουν ότι ακόμα και αν οι στόχοι που τέθηκαν στη Λισσαβόνα επιτευχθούν, τα συνολικά επίπεδα παραγωγικότητας θα μειωθούν λόγω της υφιστάμενης δημογραφικής ύφεσης.

Με βάση τις σύγχρονες μεταναστευτικές ροές, μεταξύ του 2010 και 2030 η ύφεση στην ηλικία του εργατικού δυναμικού εντός των χωρών της Ευρωπαϊκής Ένωσης θα αφορά στη μείωση του αριθμού των εργαζομένων κατά περίπου 20 εκατομμύρια. Αναμφισβήτητα, οι αλλαγές αυτές θα έχουν μια σημαντική επίδραση στην συνολική οικονομική ανάπτυξη, την εύρυθμη λειτουργία της εσωτερικής αγοράς και την ανταγωνιστικότητα των οικονομιών των κρατών μελών [2].

Μια εξίσου σημαντική διαπίστωση αποτελεί το γεγονός ότι προκειμένου να αντιμετωπιστούν οι συνέπειες της υφιστάμενης οικονομικής κρίσης (συνεχώς αυξανόμενες απαιτήσεις για παραγωγικότητα και αποδοτικότητα) τα κράτη μέλη θεωρούν άκρως απαραίτητη και πολύτιμη την ενσωμάτωση καταρτισμένων νόμιμων μεταναστών και αλλοδαπών επιχειρηματιών σε συγκεκριμένους τομείς και γεωγραφικές περιοχές ανάλογα με τις εκάστοτε ανάγκες [31].

Από την άλλη πλευρά, σε παγκόσμιο επίπεδο διαπιστώνεται ότι οι βασικές δυνάμεις του πλανήτη ήδη ανταγωνίζονται σχετικά με το ποια θα προσελκύσει το καλύτερα καταρτισμένο εργατικό δυναμικό, ενισχύοντας παράλληλα τις πρακτικές καταπολέμησης της παράνομης εργασίας με την εφαρμογή σύγχρονων πλαισίων υπηρεσιών. Σε αυτόν τον σκληρό ανταγωνισμό το πλεονέκτημα το έχουν εκείνες οι περιοχές/χώρες οι οποίες παρέχουν τις πιο σύγχρονες υποδομές και υπηρεσίες προς τους νόμιμους κατοίκους και μετανάστες [42].

Με βάση αυτές τις διαπιστώσεις αναδεικνύεται η αξία του να διασφαλιστεί ένα επιτυχημένο πλαίσιο συνεργασίας ικανό να συνεισφέρει στην επιτυχημένη ενσωμάτωση των νόμιμων μεταναστών καθώς επίσης και στο σχεδιασμό αξιόπιστων και εναρμονισμένων μεταναστευτικών διαδικασιών εκ μέρους των φορέων λήψης αποφάσεων.

Τα τελευταία χρόνια έχουν αναπτυχθεί και υλοποιούνται αρκετά προγράμματα με σκοπό την επίλυση των προβλημάτων που υφίστανται στο χώρο της μετανάστευσης. Παρόλα αυτά, στην πλειοψηφία τους δεν προσανατολίζονται στην υιοθέτηση συνεργατικών Πληροφοριακών Συστημάτων και στην παροχή καινοτόμων υπηρεσιών η-Μετανάστευσης.

Αναπτυξιακά προγράμματα και πρωτοβουλίες τα οποία χρηματοδοτούνται από την Ευρωπαϊκή Ένωση, όπως τα *EC-UN Joint Migration* [12] και *ARGO* [13] και ερευνητικά έργα, όπως το *Euromed Migration II* [14] καθώς και εκείνα που περιλαμβάνονται στη δράση *MARRI Initiative* [15], στοχεύουν κυρίως στο να προωθήσουν τη συνεργασία μεταξύ διοικητικών φορέων καθώς και να ενισχύσουν τους κοινωνικούς οργανισμούς και τις τοπικές αρχές με παραδοσιακά μέσα. Επιπλέον, τα ερευνητικά έργα *PROMNISTAT* [16] και *DCIM-EU* [17] επικεντρώνονται στον καθορισμό κατάλληλων δεικτών σύγκρισης για μεταναστευτικά δεδομένα, ενώ οι στόχοι του έργου *ERLAIM* [18] είναι προσανατολισμένοι στις πολιτικές και αφορούν την ενημέρωση και ευαισθητοποίηση για τη σωστή και αποτελεσματική ενσωμάτωση των μεταναστών, ανταλλάσσοντας καλές πρακτικές, πολιτικές και εμπειρίες.

Όλες οι προαναφερθείσες δραστηριότητες, όμως, δεν περιλαμβάνουν την υιοθέτηση και τη χρήση προηγμένων τεχνολογικών μέσων για την προώθηση καινοτόμων συνεργατικών δράσεων, γεγονός που τις καθιστά εν μέρει ελλιπείς και αναποτελεσματικές δεδομένης της πολυπλοκότητας και της δυναμικότητας που χαρακτηρίζει τον τομέα της μετανάστευσης.

Αναγνωρίζοντας την ανάγκη των μεταναστευτικών φορέων και των φορέων λήψης αποφάσεων για αποτελεσματική αντιμετώπιση των υφιστάμενων προκλήσεων στην ανάπτυξη εναρμονισμένων πολιτικών μέσω της παροχής ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης, κάποιες πρωτοποριακές δράσεις χρησιμοποιούν σύγχρονα εργαλεία λογισμικού με σκοπό την ενίσχυση των παραδοσιακών μεθόδων διάχυσης και ανταλλαγής μεταναστευτικών δεδομένων και πληροφοριών. Αντιπροσωπευτικό παράδειγμα είναι η πλατφόρμα *Policy Mix Tool* [25], η οποία παρέχει δυναμικές αναφορές και στατιστικά δεδομένα, καθώς και οι διαδικτυακές υπηρεσίες που προσφέρει το *European Civil Registry Network (ECRN)* [20] και το πληροφοριακό σύστημα *Information Exchange System of European Migration Network (EMN)* [21], βασικός σκοπός του οποίου είναι η ανταλλαγή εγγράφων Κοινωνικών Δράσεων (Civil Acts) και άλλων μεταναστευτικών δεδομένων.

Προγράμματα συνεργασίας όπως τα *CROSSROAD* [23] και *PROGRESS* [22] και επιτυχημένα έργα Πληροφορικής χρηματοδοτούμενα από την Ευρωπαϊκή Επιτροπή που στοχεύουν στην ενίσχυση κυβερνητικών δράσεων και τη μοντελοποίηση

πολιτικών (π.χ. *Cockpit* [24], *Migration Integration Policy Index* [19], *SYNC-3* [26], και *Rural Inclusion* [27]) αν και έχουν σχεδιαστεί έτσι ώστε να επιτρέπουν την παροχή προηγμένων υπηρεσιών διαδραστικότητας και κοινωνικής αλληλεπίδρασης, δεν επικεντρώνονται σε θέματα μετανάστευσης περιορίζοντας έτσι την επίδρασή τους στον κρίσιμο αυτό τομέα.

Όσον αφορά στους νόμιμους μετανάστες, με βάση τα αποτελέσματα που προέκυψαν από την έρευνα που έγινε στα πλαίσια του έργου *ImmigrationPolicy2.0* [1, 2], ένα μεγάλο ποσοστό των νόμιμων υπηκόων τρίτων χωρών είτε κατέχει καλή εκπαιδευτική κατάρτιση (Δευτεροβάθμια/Τριτοβάθμια εκπαίδευση, κολλέγιο ή αντίστοιχος βαθμός 39,84%, Μεταπτυχιακές σπουδές, διδακτορικό ή μεταδιδακτορικό δίπλωμα 2,64%) είτε δεν έχουν ολοκληρώσει ακόμα τις σπουδές τους (Σπουδαστές δευτεροβάθμιας / τριτοβάθμιας εκπαίδευσης, μεταπτυχιακοί φοιτητές ή αντίστοιχο 10,29%). Τα δεδομένα αυτά από τη μία πλευρά υποδεικνύουν την προστιθέμενη αξία της επιτυχημένης κοινωνικής ενσωμάτωσης και επαγγελματικής αποκατάστασης των κοινωνικών αυτών ομάδων και από την άλλη την ανάγκη τους για αλληλεπίδραση με προηγμένες ηλεκτρονικές υπηρεσίες μετανάστευσης (η-Μετανάστευσης) προκειμένου να αναπτύξουν την καριέρα τους.

Οι προσεγγίσεις Ευρωπαϊκών φορέων, όπως οι *European Personnel Selection Office Portal* [28], *European Job Mobility Portal* [29] και *Your Europe Portal* [30], θα μπορούσαν να θεωρηθούν ότι είναι περισσότερο στοχευμένες προς την κατεύθυνση αυτή καθώς είναι σε θέση να υποστηρίζουν κρίσιμες δραστηριότητες όπως η αναζήτηση εργασίας, η δημοσίευση θέσεων εργασίας, η δημιουργία βιογραφικών σημειωμάτων και η αναζήτηση της πιο κατάλληλης γεωγραφικής περιοχής. Από την άλλη πλευρά όμως παρουσιάζουν και σημαντικά μειονεκτήματα καθώς η πρώτη περιορίζεται στο να παρέχει υποστήριξη σχετικά με την ανάπτυξη επαγγελματικής καριέρας ενώ οι δύο επόμενες παρά το γεγονός ότι δίκαια μπορούν να θεωρηθούν ως οι πιο εξελιγμένες προσεγγίσεις, δεν είναι σχεδιασμένες για να παρέχουν δυνατότητες συνεργασίας και αλληλεπίδρασης μεταξύ των χρηστών. Κατά συνέπεια, δεν καταφέρνουν να επωφεληθούν από τις δυνατότητες των διαδραστικών εφαρμογών Web 2.0 για ενεργή συμμετοχή των χρηστών και αξιοποίηση της πολύτιμης γνώσης και εμπειρίας τους.

Ανακεφαλαιώνοντας, οι περισσότερες από τις υφιστάμενες προσεγγίσεις και πλαίσια υπηρεσιών η-Μετανάστευσης που προαναφέρθηκαν περιορίζονται στην παροχή υπηρεσιών ενημέρωσης προς το ευρύ μεταναστευτικό κοινό και αποτυγχάνουν στο να προσφέρουν ένα έμπιστο και διαδραστικό περιβάλλον συνεργασίας μεταξύ όλων των εμπλεκόμενων φορέων. Υπάρχει, λοιπόν, η επείγουσα ανάγκη για καινοτόμες και αξιόπιστες λύσεις στον τομέα της η-Μετανάστευσης, οι οποίες θα είναι ικανές να αναβαθμίζουν την ποιότητα των παρεχομένων υπηρεσιών και ταυτόχρονα να υποστηρίζουν τις προσπάθειες των μεταναστευτικών φορέων και των φορέων λήψης αποφάσεων μέσω της υιοθέτησης προηγμένων λύσεων.

Όπως παρουσιάζεται στη συνέχεια του κεφαλαίου, η συνεισφορά της διατριβής προς αυτή την κατεύθυνση περιλαμβάνει τη μελέτη περίπτωσης εφαρμογής του ΕΣΠΣ για

την παροχή ενός ολιστικού πλαισίου ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης ικανών να καλύψουν τις σύγχρονες απαιτήσεις συνεργασίας και κοινωνικής αλληλεπίδρασης των χρηστών.

7.3 Προκλήσεις στον τομέα της η-Μετανάστευσης

Προκειμένου να αποτελέσουν ένα πολύτιμο αγαθό τόσο για τους νόμιμους μετανάστες όσο και για τους κυβερνητικούς φορείς τα σύγχρονα πλαίσια υπηρεσιών μετανάστευσης θα πρέπει να είναι σε θέση να αντιμετωπίσουν ένα σύνολο από σύγχρονα προβλήματα και προκλήσεις. Αναφέρονται ενδεικτικά κάποια σημαντικά ζητήματα στα οποία είναι απαραίτητη η πληροφόρηση και η ανάδειξη καινοτόμων προσεγγίσεων:

- ✓ Ποιες είναι οι μεταναστευτικές πολιτικές που ισχύουν σε εθνικό και Ευρωπαϊκό επίπεδο; Ποιοι είναι οι παράγοντες οι οποίοι επηρεάζουν τις εθνικές μεταναστευτικές πολιτικές, πρακτικές και διαδικασίες που σχετίζονται με τα μεταναστευτικά έγγραφα;
- ✓ Σε ποιο βαθμό έχουν ενσωματωθεί οι οδηγίες και αποφάσεις της Ε.Ε. στις μεταναστευτικές πολιτικές της κάθε χώρας όσον αφορά στην χάραξη μιας ενιαίας ευρωπαϊκής μεταναστευτικής πολιτικής; Ποιες είναι οι σχετικές οδηγίες οι οποίες δεν έχουν ενσωματωθεί στις εθνικές νομοθεσίες και πώς αυτό επηρεάζει την ανάπτυξη μιας κοινής και ενιαίας μεταναστευτικής πολιτικής;
- ✓ Πώς θα μπορούσαν να εντοπιστούν, να κατηγοριοποιηθούν και να αξιολογηθούν με συνεπή και αποτελεσματικό τρόπο οι ετερογενείς πρακτικές, διαδικασίες και μέθοδοι λήψης αποφάσεων που εφαρμόζονται τόσο από τις χώρες της Ε.Ε. όσο και από άλλα γειτονικά κράτη;
- ✓ Ποιες είναι οι κρίσιμες λειτουργίες και διαδικασίες των φορέων δημόσιας διοίκησης οι οποίες θα πρέπει να επανασχεδιαστούν προκειμένου να χαρακτηρίζονται από τα επιθυμητά επίπεδα διαδραστικότητας και αποδοχής από τους νόμιμους μετανάστες;
- ✓ Ποιες είναι οι ακριβείς απαιτήσεις, όροι και περιορισμοί προκειμένου να επιτευχθεί μια αποτελεσματική και αξιόπιστη μεταναστευτική πολιτική σε εθνικό επίπεδο, η οποία να ικανοποιεί όλα τα απαραίτητα κριτήρια (οργανωτικά, νομικά, κοινωνικά, τεχνολογικά και πολιτικά);
- ✓ Πώς μπορούν οι νόμιμοι μετανάστες να αλληλεπιδρούν με το Δημόσιο (έκδοση πιστοποιητικών, φορολογικών και ασφαλιστικών δηλώσεων), να ενημερώνονται και να συμμετέχουν σε διαβουλεύσεις που τους αφορούν, να εκφράζουν τις απόψεις τους σε διάφορα ζητήματα μετανάστευσης και να δηλώνουν τα προβλήματα και τα εμπόδια που αντιμετωπίζουν στις συναλλαγές τους;

Η διατριβή προτείνει ότι τα σύγχρονα πλαίσια υπηρεσιών στον τομέα της μετανάστευσης θα πρέπει να ενισχύουν την πρόοδο προς τις εξής κατευθύνσεις:

- ✓ Στην ενδυνάμωση των μηχανισμών κοινωνικής ενσωμάτωσης.
- ✓ Στην ανάπτυξη ενός ορθολογιστικού πλαισίου διαβούλευσης με βάση αντικειμενικές πληροφορίες προερχόμενες από όλους τους σχετικούς με θέματα μετανάστευσης φορείς, οργανισμούς και συλλόγους.
- ✓ Στην πάταξη φαινομένων ρατσισμού και ξενοφοβίας μέσω της προώθησης, υιοθέτησης και εφαρμογής αποτελεσματικών εθνικών μεταναστευτικών πολιτικών, οι οποίες να είναι εναρμονισμένες με τις αντίστοιχες της Ευρωπαϊκής Ένωσης (Ε.Ε.) λαμβάνοντας παράλληλα υπόψιν τις ιδιαιτερότητες της κάθε κοινωνίας.
- ✓ Στην παροχή προηγμένων υπηρεσιών εξυπηρέτησης των νόμιμων μεταναστών οι οποίες θα βασίζονται στις υπάρχουσες τεχνολογικές υποδομές και θα αξιοποιούν τα σύγχρονα επιτεύγματα της τεχνολογίας, αναδεικνύοντας τον τομέα της η-διακυβέρνησης για μεταναστευτικά θέματα.
- ✓ Στην αύξηση της εθνικής οικονομικής ανάπτυξης καθώς και στη διασφάλιση της μελλοντικής ευημερίας, ενθαρρύνοντας και διευκολύνοντας τους νόμιμους μετανάστες να εισέλθουν και να κινηθούν ελεύθερα στην ελληνική αγορά εργασίας τηρώντας τις νόμιμες φορολογικές και ασφαλιστικές υποχρεώσεις τους.

Αναγνωρίζοντας τις προαναφερθείσες προκλήσεις καθώς και την έλλειψη προηγμένων υπηρεσιών οι οποίες να επιτρέπουν τη συμμετοχή όλων των εμπλεκόμενων φορέων μετανάστευσης (π.χ. υπουργεία, κυβερνητικοί φορείς, επιτροπές σχεδιασμού μεταναστευτικών πολιτικών, νόμιμοι μετανάστες) σε τεχνολογικά πλαίσια συνεργασίας, πρωταρχικοί στόχοι σε αυτόν τον άξονα της διατριβής είναι να:

- ✓ Αξιολογηθούν οι απαιτήσεις και περιορισμοί για την παροχή καινοτόμων λύσεων και πλαισίων προηγμένων υπηρεσιών σε πολύπλοκους τομείς όπως αυτός της μετανάστευσης.
- ✓ Αναδειχθεί ο ρόλος των σύγχρονων τεχνολογιών και να προδιαγραφεί ο τρόπος με τον οποίο μπορούν να αξιοποιηθούν αποτελεσματικά αναδεικνύοντας την εφαρμογή του ΕΣΠΣ για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-μετανάστευσης;

Όπως περιγράφεται στις ενότητες που ακολουθούν η ικανοποίηση αυτών των προκλήσεων απαιτεί την αποτελεσματική εφαρμογή του ΕΣΠΣ στον τομέα της η-Μετανάστευσης επιτρέποντας έτσι τη διαλειτουργικότητα μεταξύ ετερογενών συστημάτων και υπηρεσιών καθώς και την αξιοποίηση της συνεισφοράς και της συνεργασίας τόσο των νόμιμων μεταναστών όσο και των κυβερνητικών φορέων με στόχο την ενίσχυση των υφιστάμενων πρακτικών [6].

Η πολυπλοκότητα των προκλήσεων που χρήζουν αντιμετώπισης στον τομέα της η-μετανάστευσης προκαλείται από το γεγονός ότι ο τομέας αυτός αφορά δύο επιμέρους συμπληρωματικές κατευθύνσεις:

- Το πεδίο της ανοιχτής διακυβέρνησης, το οποίο ορίζεται από τις ανάγκες των μεταναστευτικών φορέων και των φορέων λήψης αποφάσεων για την εφαρμογή έμπιστων πλαισίων συνεργασίας και αλληλεπίδρασης με τους νόμιμους μετανάστες προκειμένου να καθορίζουν τις μεταναστευτικές πολιτικές και να εναρμονίζουν τις ήδη υπάρχουσες με βάση αξιόπιστα δεδομένα.
- Την παροχή υπηρεσιών η-Διακυβέρνησης σε νόμιμους μετανάστες ώστε να αλληλεπιδρούν εύκολα και αποδοτικά με τον κρατικό μηχανισμό και να αναφέρουν τα εμπόδια που αντιμετωπίζουν ενισχύοντας με αυτό τον τρόπο τις προσπάθειές τους για αποτελεσματική και ισότιμη κοινωνική ενσωμάτωση.

Συνεισφέροντας στην αναβάθμιση των υφιστάμενων προσεγγίσεων, στις ενότητες που ακολουθούν καταρχήν ορίζεται μια ολοκληρωμένη μεθοδολογία εφαρμογής του ΕΣΠΣ στον τομέα της η-Μετανάστευσης, η οποία παρέχει έναν συστηματικό τρόπο για την καταγραφή και τη συλλογή όλης της απαραίτητης πληροφορίας ώστε οι συνεργαζόμενοι φορείς να είναι τελικά σε θέση να καταλήξουν στον σχεδιασμό καινοτόμων υπηρεσιών και τεχνολογικών λύσεων.

Χαρακτηριστικά αναφέρεται ότι η καινοτόμος πρόταση της διατριβής σε αυτόν τον ερευνητικό άξονα βασίζεται στην ενιαία ολοκλήρωση υπηρεσιών η-μετανάστευσης προς νόμιμους μετανάστες και φορείς λήψης αποφάσεων πάνω στα θεμέλια των δυνατοτήτων συνεργασίας και διαδραστικότητας που παρέχει η αρχιτεκτονική του ΕΣΠΣ. Η προσέγγιση αυτή θεωρείται ως ένας κρίσιμος και καταλυτικός παράγοντας για την ανάπτυξη προηγμένων υπηρεσιών καθώς και για την υιοθέτηση περισσότερο αποτελεσματικών λύσεων τόσο στην η-Μετανάστευση όσο και σε άλλους κρίσιμους τομείς της Κοινωνίας της Πληροφορίας.

Επίσης προτείνονται ασφαλείς, ιδιωτικές και διαλειτουργικές υπηρεσίες η-μετανάστευσης, οι οποίες αξιοποιούν με αξιόπιστο τρόπο τα οφέλη των σύγχρονων τεχνολογιών καθώς και των εφαρμογών Web 2.0 [6, 8]. Πιο συγκεκριμένα, οι υπηρεσίες αυτές βασίζονται στην διαλειτουργική ολοκλήρωση ετερογενών συστημάτων και υπηρεσιών καθώς και στην ενσωμάτωση διαδραστικών διεπαφών και σύγχρονων εφαρμογών Web 2.0 προκειμένου να είναι δυνατή η συλλογή, συσχέτιση και ανάλυση πολύτιμων δεδομένων και η δυναμική δημιουργία περιεχομένου και συλλογικής γνώσης εκ μέρους των νόμιμων μεταναστών. Έτσι αποδεικνύονται τα πρακτικά οφέλη που προκύπτουν από την υιοθέτηση του ολιστικού πλαισίου εφαρμογής του ΕΣΠΣ, προδιαγράφοντας ένα σύνολο από υπηρεσίες η-Μετανάστευσης οι οποίες ικανοποιούν τις απαιτήσεις ασφάλειας, ιδιωτικότητας και διαλειτουργικότητας που χαρακτηρίζουν τα έμπιστα και συνεργατικά περιβάλλοντα.

Τέλος, είναι σημαντικό να αναφερθεί ότι ενώ τα όρια της μελέτης περίπτωσης που παρουσιάζεται στο πλαίσιο της διατριβής περιορίζονται στον τομέα της η-Μετανάστευσης, ερευνητικά αποτελέσματα [5] αποδεικνύουν ότι η υιοθέτηση της προτεινόμενης μεθοδολογικής προσέγγισης σε άλλους κρίσιμους και πολύπλοκους τομείς, όπου διαφορετικοί φορείς και κοινωνικές ομάδες έχουν την ανάγκη να συνεργάζονται ακόμα και σε διασυνοριακό επίπεδο για την αντιμετώπιση των υφιστάμενων προκλήσεων, είναι επίσης ικανή να παρέχει ένα αξιόπιστο πλαίσιο για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών.

7.4 Μεθοδολογία καθορισμού εννοιολογικού πλαισίου

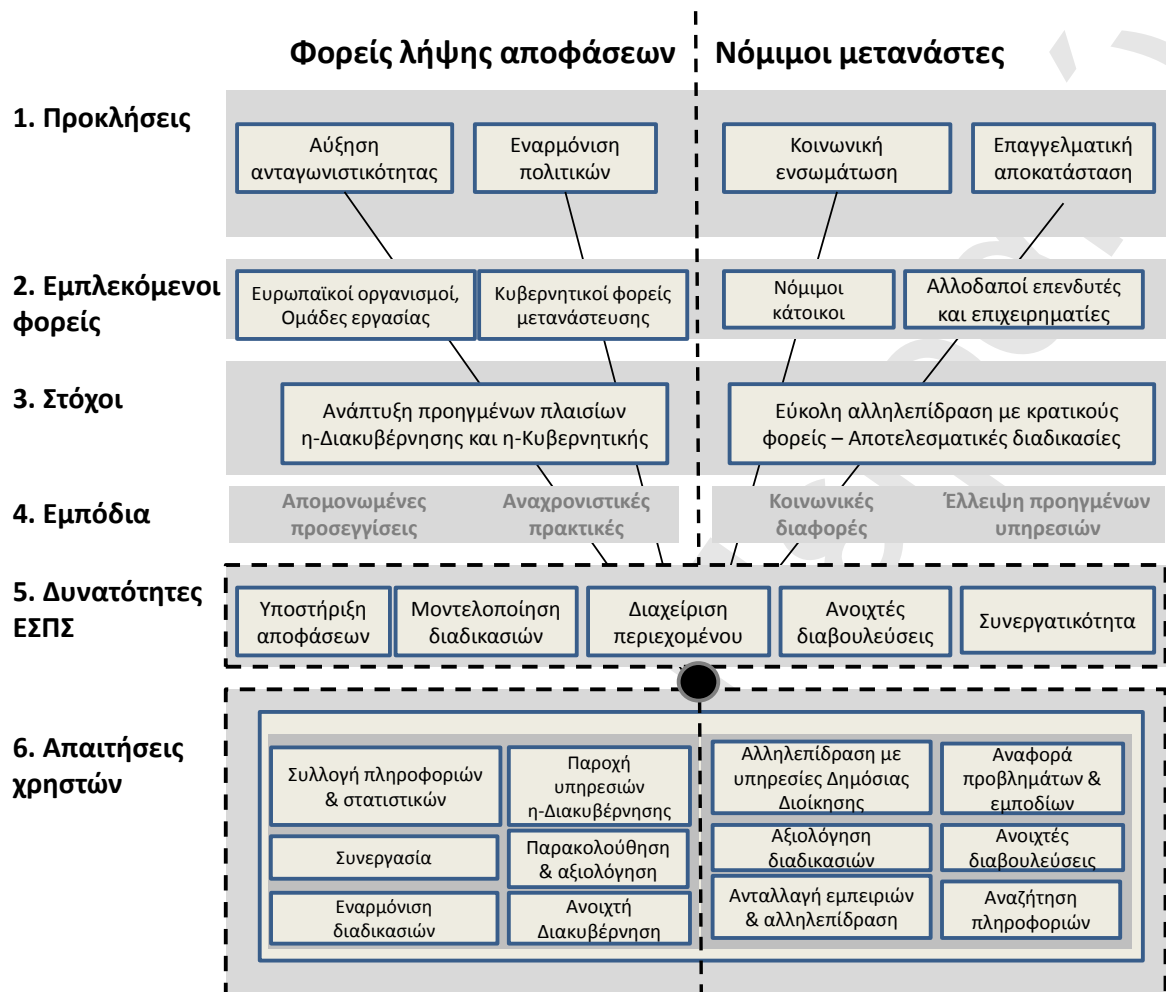
Ικανοποιώντας την ανάγκη αλληλεπίδρασης μεταξύ διαφορετικών ομάδων χρηστών κάτω από ένα κοινό πλαίσιο συνεργασίας στην ενότητα αυτή προτείνεται μια ολοκληρωμένη μεθοδολογία εφαρμογής του ΕΣΠΣ στον τομέα της η-μετανάστευσης, συνεισφέροντας έτσι στη παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών συνεργατικής ανάπτυξης και εναρμόνισης των μεταναστευτικών πολιτικών.

Σκοπός είναι ο καθορισμός του θεωρητικού υπόβαθρου που απαιτείται για την ανάλυση σύνθετων προβλημάτων όπου η συνεργασία μεταξύ των εμπλεκόμενων φορέων θεωρείται ως ένας σημαντικός στόχος για την παροχή αξιόπιστων και έμπιστων υπηρεσιών.

Πιο συγκεκριμένα, η μεθοδολογία που προτείνεται για τον ορισμό του εννοιολογικού πλαισίου η-Μετανάστευσης αποτελείται από τα ακόλουθα βήματα:

- ❖ **Βήμα 1:** Καταγραφή όλων των κρίσιμων συντελεστών (π.χ. Προκλήσεις, Εμπλεκόμενοι Φορείς, Στόχοι, Εμπόδια, Τεχνολογικές δυνατότητες, Απαιτήσεις χρηστών) ανάλογα με τη μελέτη περίπτωσης και την έρευνα πεδίου η οποία έχει προηγηθεί (βλ. ενότητα 7.3).
- ❖ **Βήμα 2:** Ανάλυση των διαφορετικών αναγκών όλων των εμπλεκόμενων φορέων που καθορίστηκαν στο Βήμα 1.
- ❖ **Βήμα 3:** Αξιολόγηση των δυνατοτήτων που είναι ικανή να προσφέρει η εφαρμογή του ΕΣΠΣ.
- ❖ **Βήμα 4:** Καταγραφή των απαιτήσεων των χρηστών με βάση την ανάλυση των προηγούμενων βημάτων.
- ❖ **Βήμα 5:** Σχεδιασμός και παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης.

Η προτεινόμενη μεθοδολογία περιλαμβάνει όλους τους βασικούς παράγοντες που επηρεάζουν την αποτελεσματική ανάπτυξη και την εναρμόνιση των μεταναστευτικών πολιτικών και των ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών, κατηγοριοποιημένους σε επίπεδα ανάλογα με το βαθμό επιρροής τους (κάθετος άξονας) και σε διαστάσεις ανάλογα με τις οντότητες που εμπλέκονται (οριζόντιος άξονας) όπως παρουσιάζεται στο Σχήμα 28.



Σχήμα 28: Εννοιολογικό πλαίσιο η-Μετανάστευσης

Όπως φαίνεται στο Σχήμα 28, το εννοιολογικό πλαίσιο η-Μετανάστευσης απαιτεί τη συμμετοχή όλων των *Εμπλεκόμενων Φορέων* συμπεριλαμβανομένων φορέων μετανάστευσης όπως για παράδειγμα Ευρωπαϊκοί οργανισμοί και δίκτυα συνεργασίας, κυβερνητικοί φορείς και Υπουργεία, επιτροπές σχεδιασμού πολιτικών, φορείς λήψης αποφάσεων και υπηρεσίες Δημόσιας Διοίκησης, αλλά και των νόμιμων αλλοδαπών υπηκόων, όπως είναι για παράδειγμα οι νόμιμοι μετανάστες, οι μετανάστες δεύτερης γενιάς καθώς και οι αλλοδαποί επενδυτές και επιχειρηματίες, καθένας από τους οποίους έχει θέσει διαφορετικούς αλλά, παράλληλα, άμεσα συσχετιζόμενους *Στόχους*.

Όλοι οι κρίσιμοι παράγοντες που συμπληρώνουν το πλαίσιο αναλύονται σε δύο διαφορετικές αλλά συμπληρωματικές διαστάσεις: από την πλευρά των φορέων λήψης αποφάσεων και των αντίστοιχων κρατικών και ευρωπαϊκών μεταναστευτικών φορέων, και από αυτή των πολιτών στην προκειμένη περίπτωση των *νόμιμων μεταναστών* (οι οποίοι αναπαριστώνται στο σχήμα με την κάθετη διακεκομμένη γραμμή).

Καθώς κινούμαστε από τα υψηλότερα στα χαμηλότερα επίπεδα του πλαισίου (βλ Σχήμα 28), οι λύσεις για τις πρωταρχικές *Προκλήσεις* που τέθηκαν στο υψηλότερο

επίπεδο γίνονται όλο και πιο συγκεκριμένες και προφανείς καταλήγοντας στο γεγονός ότι η υφιστάμενη τεχνολογική εξέλιξη είναι αρκετά ώριμη ώστε να ικανοποιήσει τις απαιτήσεις των χρηστών παρέχοντας προηγμένες υπηρεσίες οι οποίες θα βασίζονται στις σύγχρονες *Τεχνολογικές δυνατότητες* προκειμένου να ξεπερνούν τα *Εμπόδια* και να βελτιώνουν τις παραδοσιακές πρακτικές.

Από την πλευρά των *Φορέων Λήψης Αποφάσεων*, οι *Προκλήσεις* που τίθενται τόσο για τους Ευρωπαϊκούς οργανισμούς όσο και για τις εθνικές κυβερνήσεις αφορούν στην εναρμόνιση των ετερογενών πολιτικών και διαδικασιών με σκοπό τη σύγκλιση και εναρμόνιση. Με βάση την ανάλυση που προηγήθηκε, η παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης είναι ικανή να συνεισφέρει προς την κατεύθυνση αυτή. Το σημείο αυτό αποτελεί τον πρωταρχικό κοινό *Στόχο* των προαναφερόμενων *Εμπλεκόμενων Φορέων* ενώ όπως φαίνεται στο τέταρτο επίπεδο του Σχήμα 28, οι προσπάθειές τους θα πρέπει να καλύψουν τα *Εμπόδια* που προκύπτουν από την υιοθέτηση αναχρονιστικών πρακτικών και απομονωμένων προσεγγίσεων. Αυτό επιτυγχάνεται αξιοποιώντας τις δυνατότητες των σύγχρονων τεχνολογιών που ενσωματώνει το ΕΣΠΣ προκειμένου να είναι δυνατή η παροχή υπηρεσιών η-Μετανάστευσης ικανών να συνεισφέρουν στη:

- ✓ συλλογή πληροφοριών από ετερογενή συστήματα και πλαίσια υπηρεσιών,
- ✓ παρακολούθηση, ανάλυση και αξιολόγηση πολιτικών,
- ✓ συλλογή, επεξεργασία και ανάλυση αξιόπιστων και επίκαιρων δεδομένων και πληροφοριών προερχόμενων από τους ίδιους τους χρήστες,
- ✓ συνεργατική ανάπτυξη και εναρμόνιση πολιτικών,
- ✓ παροχή προηγμένων υπηρεσιών προς τους πολίτες
- ✓ συνεργασία σε όλα τα επίπεδα με σκοπό την καταγραφή των προβλημάτων και εμποδίων στην εφαρμογή των πολιτικών, και στην
- ✓ ενίσχυση του μοντέλου ανοιχτής διακυβέρνησης.

Υιοθετώντας την προσέγγιση των *Νόμιμων Μεταναστών*, ως *Εμπλεκόμενοι Φορείς* θεωρούνται οι νόμιμοι κάτοικοι και οι αλλοδαποί επιχειρηματίες και επενδυτές. Όπως φαίνεται στα δύο πρώτα επίπεδα του πλαισίου, προκειμένου να ανταπεξέλθουν στις υφιστάμενες *Προκλήσεις*, όπως είναι η αποτελεσματική κοινωνική τους ενσωμάτωση και η επαγγελματική τους αποκατάσταση [10, 11], (σε συμμόρφωση με τις προβλεπόμενες διαδικασίες για την ένταξή τους στο ενεργό εργατικό δυναμικό της χώρας που φιλοξενούνται) καταλήγουν σε έναν κοινό *Στόχο*. Αντίστοιχα με την προσέγγιση των *Φορέων Λήψης Αποφάσεων*, ο κοινός στόχος των *Νόμιμων Μεταναστών* είναι να μπορούν να αλληλεπιδρούν εύκολα με τους κρατικούς φορείς και τις υπηρεσίες Δημόσιας Διοίκησης και να επωφελούνται από τα πλεονεκτήματα σύγχρονων διαδραστικών υπηρεσιών.

Για να επιτευχθεί αυτό, απαιτείται να αντιμετωπίσουν τα υφιστάμενα *Εμπόδια* τα οποία και καταγράφονται στο τέταρτο επίπεδο του Σχήμα 28 και τα οποία αφορούν στις κοινωνικές και πολιτισμικές διαφορές καθώς και στην έλλειψη προηγμένων και

συνάμα έμπιστων υπηρεσιών. Όμοια, αυτό θα μπορούσε να επιτευχθεί αξιοποιώντας τις δυνατότητες που παρέχει το ΕΣΠΣ με στόχο την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών ικανών να καλύψουν τις ανάγκες των νόμιμων μεταναστών για:

- ✓ αναζήτηση πληροφοριών,
- ✓ δυνατότητα αξιολόγησης των υφιστάμενων πολιτικών και πρακτικών,
- ✓ ανταλλαγή απόψεων και εμπειριών,
- ✓ αναφορά προβλημάτων και εμποδίων,
- ✓ συμμετοχή σε ανοιχτές διαβουλεύσεις,
- ✓ εύκολη αλληλεπίδραση με υπηρεσίες Δημόσιας Διοίκησης και συμμετοχή στις κυβερνητικές διαδικασίες, και
- ✓ κοινωνική αλληλεπίδραση και ενημέρωση σχετικά με τις ιδιαιτερότητες κάθε γεωγραφικής περιοχής.

Η διακεκομμένη γραμμή η οποία χωρίζει το πέμπτο και το έκτο επίπεδο (*Δυνατότητες ΕΣΠΣ, Απαιτήσεις χρηστών*) αναπαριστά τον καταλυτικό ρόλο του ΕΣΠΣ για το σχεδιασμό καινοτόμων υπηρεσιών και την παροχή αξιόπιστων λύσεων στον τομέα της η-Μετανάστευσης [7, 9]. Πιο συγκεκριμένα, οι τεχνολογικές δυνατότητες που παρέχει συνοψίζονται ως εξής:

- ✓ *Σύστημα Διαχείρισης Περιεχομένου*, το οποίο επιτρέπει τη συνεπή και αποτελεσματική διαχείριση εγγράφων, πληροφοριών και άλλων πληροφοριακών αγαθών παρέχοντας διαδραστικές και φιλικές προς τον χρήστη διεπαφές για τη διαχείριση μεγάλων διασυνδεδεμένων βάσεων δεδομένων και την εύκολη χρήση προηγμένων μηχανών αναζήτησης.
- ✓ *Σύστημα μοντελοποίησης διαδικασιών*, το οποίο βασίζεται σε σύγχρονες τεχνολογίες BPEL, XML, OWL (βλ. 4.3.2.3) και παρέχει τη δυνατότητα γραφικής αναπαράστασης κυβερνητικών και άλλων διαδικασιών, ροών εργασίας, και μοντέλων πολιτικών, καθώς επίσης τη σύγκριση και την ανάλυση των διαφορών τους με σκοπό τη δημιουργία νέων, περισσότερο αποδοτικών μοντέλων και διαδικασιών.
- ✓ *Συνεργατικές εφαρμογές* όπως wikis, ιστολόγια, φόρουμ, ηλεκτρονικές ψηφοφορίες και αντίστοιχες διαδραστικές λειτουργίες δυναμικής δημιουργίας περιεχομένου οι οποίες αξιοποιούν τις δυνατότητες των τεχνολογιών Web 2.0 για άμεση αλληλεπίδραση, ανταλλαγή απόψεων και σχολιασμών, καταγραφή προβλημάτων και εμποδίων και παροχή στοχευμένων υπηρεσιών.
- ✓ *Σύστημα ηλεκτρονικών διαβουλεύσεων*, το οποίο βασίζεται σε σύγχρονες τεχνολογίες διαδικτυακών εφαρμογών, βάσεων δεδομένων και άλλων εργαλείων στατιστικής ανάλυσης προκειμένου να παρέχει τη δυνατότητα δημιουργίας ηλεκτρονικών διαβουλεύσεων με σκοπό τη συλλογή αξιόπιστων πληροφοριών

ανατροφοδότησης και πρωτογενών στατιστικών δεδομένων καθώς και την δημιουργία αναφορών.

- ✓ *Σύστημα Υποστήριξης Αποφάσεων* τα οποίο αξιοποιεί την τεχνολογική ολοκλήρωση όλων των προαναφερόμενων συστημάτων μέσω ενός Διαλειτουργικού Δίαυλου Επικοινωνίας (Enterprise Service Bus, ESB) με σκοπό τη σύνθεση κατανεμημένων δεδομένων και πληροφοριών και την παροχή πολύτιμης γνώσης για την υποστήριξη αποφάσεων σε πολύπλοκα θέματα η-Μετανάστευσης.

Όπως παρουσιάζεται στην επόμενη ενότητα, οι υπηρεσίες που είναι δυνατό να αναπτυχθούν και να προσφερθούν από το ΕΣΠΣ στον τομέα της η-Μετανάστευσης είναι ικανές να προάγουν την ενεργή συμμετοχή και την κοινωνική αλληλεπίδραση μεταξύ των νόμιμων μεταναστών, παρέχοντας παράλληλα πολύτιμη ανατροφοδότηση προς τους φορείς λήψης αποφάσεων. Ακολουθώντας αυτή την προσέγγιση, η προτεινόμενη μεθοδολογία εφαρμογής του ΕΣΠΣ στον τομέα της η-Μετανάστευσης καταλήγει σε αποτελέσματα ικανά να συνεισφέρουν στην αντιμετώπιση των υφιστάμενων εμποδίων και την αναβάθμιση των παραδοσιακών γραφειοκρατικών πρακτικών για το σχεδιασμό μεταναστευτικών πολιτικών και την παροχή υπηρεσιών προς τους νόμιμους μετανάστες.

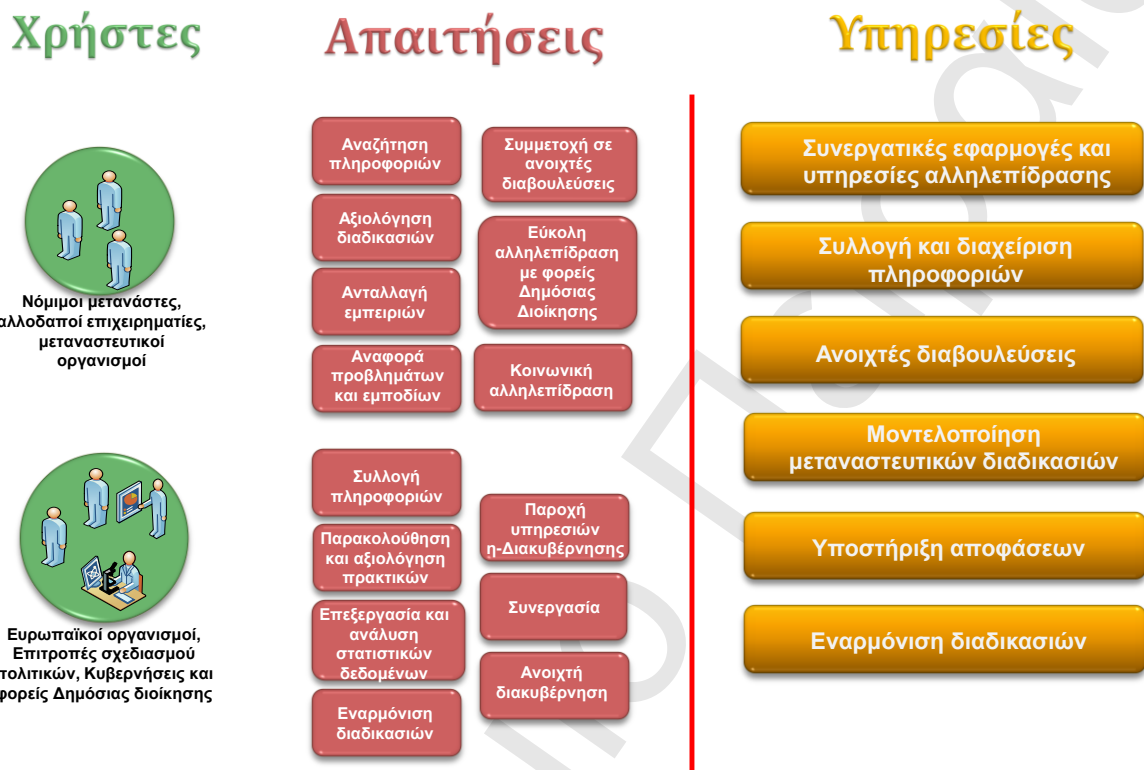
7.5 Υπηρεσίες η-Μετανάστευσης

Με βάση τη μεθοδολογία καθορισμού του εννοιολογικού πλαισίου και την καταγραφή των απαιτήσεων χρηστών, τα αποτελέσματα της διατριβής που παρουσιάζονται στη συνέχεια του κεφαλαίου επικεντρώνονται στο πέμπτο βήμα (*Βήμα 5*) της μεθοδολογίας το οποίο αφορά στην παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών στον τομέα της η-Μετανάστευσης. Πιο συγκεκριμένα, οι νέες υπηρεσίες θα πρέπει να ικανοποιούν τις απαιτήσεις που εντοπίστηκαν στο τέταρτο βήμα της μεθοδολογίας αξιοποιώντας με αποτελεσματικό τρόπο τις δυνατότητες του ΕΣΠΣ. Ο τρόπος με τον οποίο οι δυνατότητες που παρέχει το ΕΣΠΣ είναι ικανές να ικανοποιούν τις απαιτήσεις των νόμιμων μεταναστών και των φορέων λήψης αποφάσεων για συνεργασία και κοινωνική αλληλεπίδραση φαίνεται στο Σχήμα 29 από την προδιαγραφή ενός συνόλου υπηρεσιών η-Μετανάστευσης τις οποίες είναι ικανό να παρέχει [3, 4].

Με βάση τις απαιτήσεις τόσο των νόμιμων μεταναστών όσο και των φορέων λήψης αποφάσεων που καταγράφηκαν στην προηγούμενη ενότητα και οι οποίες παρουσιάζονται στον κεντρικό άξονα του Σχήμα 29, οι υπηρεσίες που παρέχει το ΕΣΠΣ θα πρέπει να είναι σχεδιασμένες έτσι ώστε να:

- ✓ συλλέγουν τις απόψεις και την ανατροφοδότηση των χρηστών,
- ✓ διευκολύνουν την ανάπτυξη και εναρμόνιση μεταναστευτικών πολιτικών και διαδικασιών καθώς και την αλληλεπίδραση των πολιτών/νόμιμων μεταναστών με τους κυβερνητικούς φορείς,

- ✓ είναι διαλειτουργικές ώστε να ανταλλάσουν, να επεξεργάζονται και να συνθέτουν πληροφορίες από διαφορετικές πηγές καθώς και να αξιοποιούν τη συλλογική γνώση όλων των εμπλεκομένων φορέων.



Σχήμα 29: Προηγμένες υπηρεσίες η-Μετανάστευσης

Όπως φαίνεται στη δεξιά πλευρά του Σχήμα 29 και με βάση την ανάλυση των τεχνολογικών δυνατοτήτων του ΕΣΠΣ που παρουσιάστηκε στην προηγούμενη ενότητα, οι καινοτόμες υπηρεσίες που είναι ικανές να παρέχει προκειμένου να ικανοποιεί τις απαιτήσεις των νόμιμων μεταναστών και φορέων λήψης αποφάσεων προδιαγράφονται ως εξής:

- ❖ *Υπηρεσίες συνεργασίας και κοινωνικής αλληλεπίδρασης:* Με τη χρήση συνεργατικών εφαρμογών και τεχνολογιών Web 2.0 οι χρήστες έχουν τη δυνατότητα να αλληλεπιδρούν και να ανταλλάσουν εμπειρίες, να δημιουργούν περιεχόμενο και να σχολιάζουν τις απόψεις άλλων χρηστών σε θέματα σχετικά με τον τομέα της μετανάστευσης καθώς και να συνεισφέρουν τις προσωπικές τους γνώσεις και εμπειρίες προκειμένου να αξιοποιούνται κατάλληλα από τους μεταναστευτικούς φορείς και τους φορείς λήψης αποφάσεων για το σχεδιασμό εναρμονισμένων μεταναστευτικών πολιτικών και αποτελεσματικών διαδικασιών.

Με τη χρήση αυτής της κατηγορίας υπηρεσιών και των αντίστοιχων τεχνολογικών συστημάτων που τις υποστηρίζουν θα ικανοποιούνται οι απαιτήσεις των νόμιμων μεταναστών για ανταλλαγή απόψεων και εμπειριών, αξιολόγηση των υφιστάμενων πρακτικών και πολιτικών, αναφορά

προβλημάτων και εμποδίων, και κοινωνική αλληλεπίδραση και συνεργασία σε όλα τα επίπεδα όπως καθορίστηκαν με βάση την εφαρμογή του εννοιολογικού μοντέλου.

- ❖ *Υπηρεσίες διαχείρισης πληροφοριακών αγαθών:* Αξιοποιώντας τις δυνατότητες των σύγχρονων συστημάτων διαχείρισης περιεχομένου και ολοκλήρωσης κατανεμημένων βάσεων δεδομένων, τόσο η ομάδα χρηστών των νόμιμων μεταναστών όσο και αυτή των κυβερνητικών φορέων θα έχουν πρόσβαση σε αξιόπιστες πηγές πληροφοριών σχετικά με μεταναστευτικές πολιτικές, οδηγίες, πρακτικές, διαδικασίες, οργανωτικές δομές και μελέτες.

Παρέχοντας αυτή την κατηγορία υπηρεσιών, η διατριβή προτείνει ότι η εφαρμογή του ΕΣΠΣ θα είναι ικανή να προσφέρει τη δυνατότητα στους συμμετέχοντες στο συνεργατικό περιβάλλον να αναζητούν και να μεταφορτώνουν σχετικές πληροφορίες καθώς επίσης να ενημερώνονται, να παρακολουθούν και να καταγράφουν ενδεχόμενες αλλαγές με συστηματικό τρόπο ικανοποιώντας έτσι τις απαιτήσεις για αναζήτηση και συλλογή πληροφοριών.

- ❖ *Υπηρεσίες ανοιχτών διαβουλεύσεων:* Οι υπηρεσίες ανοιχτών διαβουλεύσεων υποστηρίζουν την ενεργή συμμετοχή των χρηστών σε κρίσιμα ζητήματα διευκολύνοντάς τους να συνεργαστούν μέσω ανοιχτών δημοσκοπήσεων.

Προτείνεται οι υπηρεσίες αυτές να παρέχονται με τη μορφή ηλεκτρονικών ερωτηματολογίων και άλλων διαδραστικών διεπαφών ικανοποιώντας έτσι τις απαιτήσεις για συλλογή, ανάλυση και επεξεργασία στατιστικών δεδομένων και άλλων αξιόπιστων πληροφοριών.

- ❖ *Υπηρεσίες μοντελοποίησης μεταναστευτικών διαδικασιών:* Αξιοποιώντας τις δυνατότητες που είναι ικανά να παρέχουν τα σύγχρονα συστήματα μοντελοποίησης και διαχείρισης διαδικασιών (Business Process Management, BPM) οι κυβερνητικοί φορείς θα είναι σε θέση να δημιουργούν δομημένα μοντέλα αναπαράστασης των πολιτικών που εφαρμόζουν, περιγράφοντας τις διαδικασίες που περιλαμβάνονται στην κάθε μια.

Κρίνεται απαραίτητη η παροχή αυτής της κατηγορίας υπηρεσιών, καθώς με την αποτελεσματική εφαρμογή τους, οι φορείς λήψης αποφάσεων θα έχουν τη δυνατότητα να αναλύουν και να επεξεργάζονται τις πληροφορίες κάθε μοντέλου μεταναστευτικών πολιτικών και να εντοπίζουν τα ευάλωτα σημεία τους, ικανοποιώντας με αυτό τον τρόπο τις απαιτήσεις για παρακολούθηση, αξιολόγηση και σύγκριση των υφιστάμενων πρακτικών και διαδικασιών.

- ❖ *Υπηρεσίες εναρμόνισης διαδικασιών και υποστήριξης αποφάσεων:* Οι υπηρεσίες που ανήκουν σε αυτή την κατηγορία προσφέρουν τη δυνατότητα στους κυβερνητικούς φορείς να εντοπίζουν ομοιότητες και διαφορές μεταξύ των ετερογενών μεταναστευτικών πολιτικών και διαδικασιών καθώς και να σχεδιάζουν νέα εναρμονισμένα μοντέλα τα οποία θα αποτελούν βέλτιστες πρακτικές.

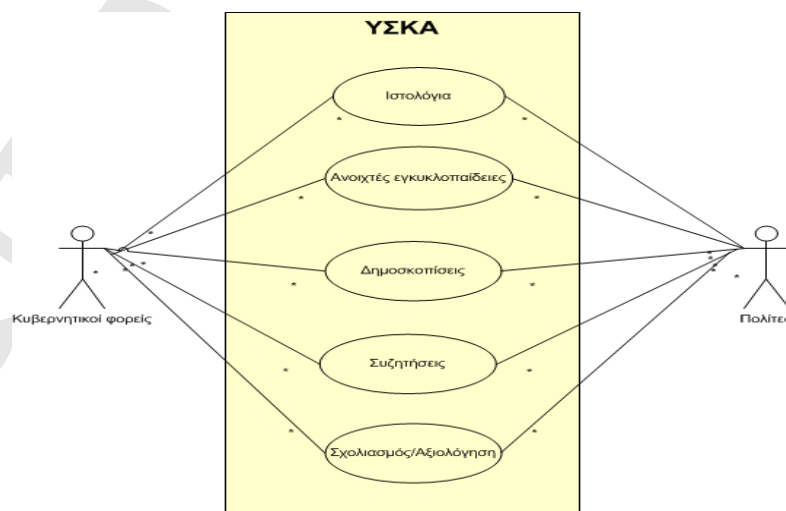
Θα πρέπει να υποστηρίζουν τη συνεργατική αξιολόγηση και συνεισφορά των χρηστών καθώς επίσης και να συνδυάζουν τις πληροφορίες και γνώσεις που συλλέγουν οι υπόλοιπες υπηρεσίες που παρέχει το ΕΣΠΣ ώστε να ενισχύεται η λήψη αποφάσεων σε πολύπλοκα θέματα η-Μετανάστευσης.

Έχοντας αναλύσει διεξοδικά στο τέταρτο κεφάλαιο όλα τα απαραίτητα συστήματα και τεχνολογίες που απαιτούνται για την ολοκλήρωση του ΕΣΠΣ, η ανάλυση που ακολουθεί στις επόμενες ενότητες επικεντρώνεται στην περιγραφή των λειτουργικών προδιαγραφών των υπηρεσιών η-Μετανάστευσης που είναι ικανό να παρέχει το ΕΣΠΣ, και οι οποίες προέκυψαν από την εφαρμογή του εννοιολογικού μοντέλου η-Διακυβέρνησης που παρουσιάστηκε στην ενότητα 7.4.

7.5.1 Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης

Οι Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης (ΥΣΚΑ) βασίζονται σε σύγχρονες τεχνολογίες συλλογής δεδομένων και διαδραστικές διεπαφές προκειμένου να συλλέγουν και να αξιοποιούν τη συλλογική γνώση των συμμετεχόντων η οποία συχνά αναφέρεται και ως «σοφία του πλήθους» (wisdom of the croud). Ειδικότερα, παρέχουν τη δυνατότητα συλλογής και ανάλυσης πρωτογενούς πληροφορίας και διαφορετικών απόψεων, προτάσεων, και σχολιασμών σχετικών με μεταναστευτικά ζητήματα και τα υφιστάμενα προβλήματα. Οι πληροφορίες συλλέγονται από συνεργατικά εργαλεία και εφαρμογές όπως για παράδειγμα μέσω wikis, ιστολογίων, φόρουμ, και ηλεκτρονικών ψηφοφοριών καθώς επίσης και μέσω άλλων υπηρεσιών κοινωνικής αλληλεπίδρασης που οι σύγχρονες τεχνολογίες Web 2.0 είναι ικανές να παρέχουν.

Το διάγραμμα UML του Σχήμα 30 αναπαριστά τη λειτουργικότητα και τις δυνατότητες κοινωνικής αλληλεπίδρασης που παρέχουν οι ΥΣΚΑ και οι οποίες θα πρέπει να είναι διαθέσιμες τόσο στους φορείς λήψης αποφάσεων όσο και στους νόμιμους μετανάστες.



Σχήμα 30: Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης

Το σύνολο των υπηρεσιών που παρουσιάζονται στο Σχήμα 30 είναι ικανό να υποστηρίξει τη ενεργή συμμετοχή των χρηστών, την αποτελεσματική αλληλεπίδραση, τη διενέργεια ανοιχτών διαβουλεύσεων καθώς και τη δυνατότητα εντοπισμού σύγχρονων προβλημάτων και αντίστοιχων αποτελεσματικών και αξιόπιστων λύσεων.

Πιο κάτω παρουσιάζεται η υλοποίηση αυτών των υπηρεσιών στην πλατφόρμα ImmigrationPolicy 2.0.

Εικόνα 3: Συνεργασία στην πλατφόρμα ImmigrationPolicy 2.0

Επίσης, οι φορείς λήψης αποφάσεων έχουν τη δυνατότητα να συνεργάζονται εύκολα και αποδοτικά δημιουργώντας περιεχόμενο και συμμετέχοντας σε ιστολόγια και συζητήσεις σχετικά με κρίσιμα μεταναστευτικά θέματα. Από την άλλη πλευρά, οι νόμιμοι μετανάστες μπορούν να συμμετέχουν ισότιμα στις συνεργατικές εφαρμογές, να εκφράζουν τη γνώμη τους, να σχολιάζουν και να αξιολογούν τις υφιστάμενες και προτεινόμενες λύσεις, να ανταλλάσσουν τις απόψεις τους, να μαθαίνουν από τις εμπειρίες άλλων, καθώς επίσης και να παρέχουν άμεση και αξιόπιστη ανατροφοδότηση σε πολύπλοκα ζητήματα συμμετέχοντας στις ηλεκτρονικές δημοσκοπήσεις.

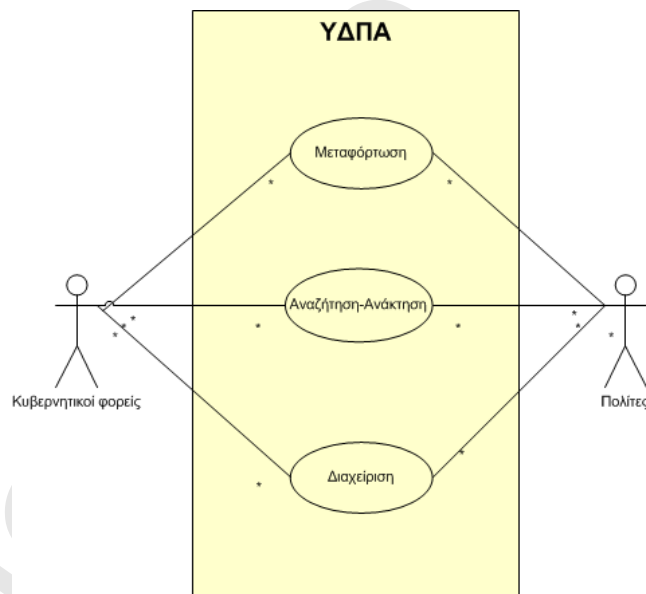
7.5.2 Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών

Εκτός από τις ΥΣΚΑ οι οποίες όπως περιγράφεται στην προηγούμενη ενότητα προσανατολίζονται στη συνεργασία και την κοινωνική αλληλεπίδραση των

χρηστών, η εφαρμογή του ΕΣΠΣ στον τομέα της η-Μετανάστευσης απαιτεί τη δημιουργία και συντήρηση μιας κεντρικής βάσης δεδομένων ηλεκτρονικών εγγράφων, χρήσιμων υπερσυνδέσμων και άλλων σχετικών με τη μετανάστευση πληροφοριακών αγαθών όπως για παράδειγμα:

- ✓ νομοθεσία,
- ✓ πολιτικές,
- ✓ προγράμματα εκπαιδευτικής και επαγγελματικής κατάρτισης και αποκατάστασης,
- ✓ διαδικασίες πιστοποίησης και κοινωνικής ενσωμάτωσης,
- ✓ υποστηρικτικές δράσεις και προγράμματα,
- ✓ στοιχεία επικοινωνίας σχετικών κυβερνητικών φορέων και υπηρεσιών Δημόσιας Διοίκησης, και
- ✓ στατιστικά δεδομένα και ερευνητικές μελέτες.

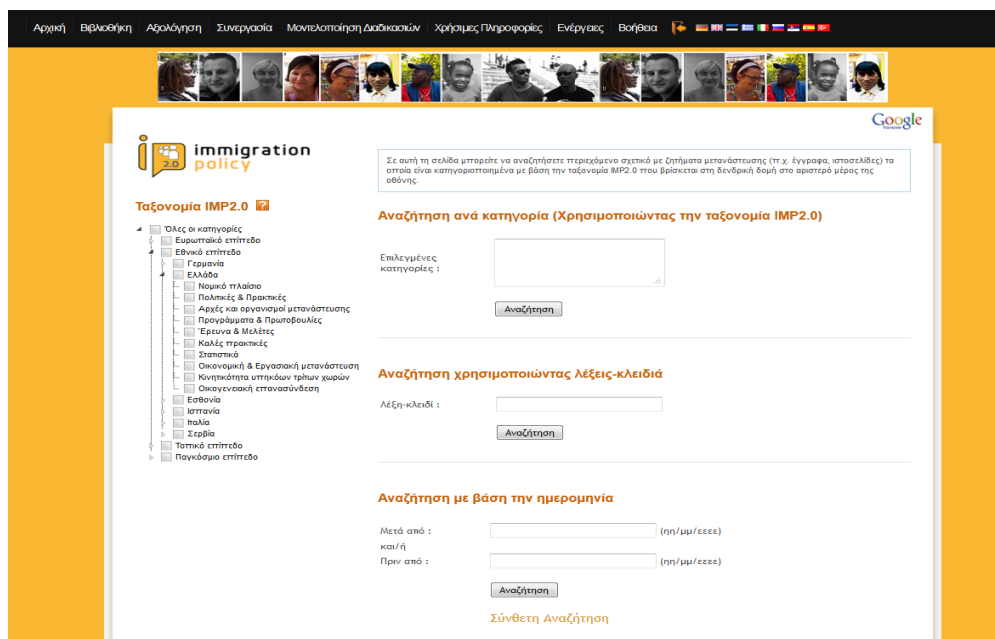
Στο Σχήμα 31 προδιαγράφονται με περισσότερη λεπτομέρεια οι δυνατότητες που παρέχουν οι Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών (ΥΔΠΑ).



Σχήμα 31: Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών

Οι φορείς λήψης αποφάσεων και οι νόμιμοι μετανάστες θα επωφεληθούν από τη δυνατότητα να συνεισφέρουν τις δικές τους πηγές πληροφόρησης και να συμμετέχουν ενεργά στη συλλογή πολύτιμων πληροφοριακών αγαθών. Αξιοποιώντας αυτή την κατηγορία υπηρεσιών που παρέχει το ΕΣΠΣ θα είναι σε θέση να αναζητούν και να ανακτούν αυτές τις πληροφορίες με βάση πολλαπλά κριτήρια αναζήτησης καθώς και χρησιμοποιώντας κατάλληλα σχεδιασμένες ταξονομίες η οποία θα αναλαμβάνουν την κατηγοριοποίηση των πληροφοριακών αγαθών με βάση το περιεχόμενό τους.

Πιο κάτω παρουσιάζεται η υλοποίηση αυτών των υπηρεσιών στην πλατφόρμα ImmigrationPolicy 2.0.



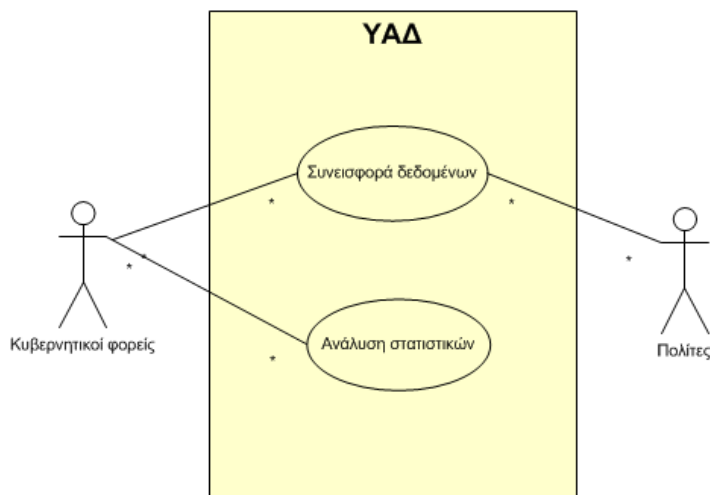
Εικόνα 4: Διαχείριση περιεχομένου στην πλατφόρμα ImmigrationPolicy 2.0

Όπως φαίνεται στην Εικόνα 4, η υλοποίηση αυτών των υπηρεσιών απαιτεί απλές και εύκολες στη χρήση γραφικές διεπαφές οι οποίες θα βοηθούν τους χρήστες να αναζητούν, να μεταφορτώνουν και να διαχειρίζονται τα πληροφοριακά αγαθά παρέχοντας παράλληλα ένα σύνολο απαραίτητων περιγραφικών πληροφοριών για την κάθε εγγραφή συμπεριλαμβανομένων των κατηγοριών της ταξινόμησης στις οποίες ανήκει.

7.5.3 Υπηρεσίες Ανοιχτών Διαβουλεύσεων

Ηλεκτρονικά ερωτηματολόγια, δημοσκοπήσεις, ανοιχτές διαβουλεύσεις και ηλεκτρονικές ψηφοφορίες είναι τα εργαλεία που θα πρέπει χρησιμοποιηθούν για να παρέχουν στους χρήστες τη δυνατότητα να εντοπίσουν τα υπάρχοντα προβλήματα των μεταναστευτικών διαδικασιών, να αναφέρουν τις δυσκολίες και τα εμπόδια που αντιμετωπίζουν, καθώς και να αξιολογούν τις υφιστάμενες πρακτικές.

Για να επιτευχθεί αυτό, η διατριβή προτείνει ότι θα πρέπει να χρησιμοποιούνται σύγχρονες τεχνολογίες Web 2.0 οι οποίες υποστηρίζουν τη διαδραστική συλλογή δεδομένων, τη στατιστική ανάλυση των αποτελεσμάτων με δυναμικό τρόπο καθώς και την αυτοματοποιημένη παραγωγή τελικών αναφορών.



Σχήμα 32: Υπηρεσίες Ανοιχτών Διαβουλεύσεων

Όπως φαίνεται στο Σχήμα 32, χρησιμοποιώντας τις Υπηρεσίες Ανοιχτών Διαβουλεύσεων (YAD) οι νόμιμοι μετανάστες θα έχουν τη δυνατότητα να δηλώνουν τις διαφορετικές απόψεις τους, τη θετική ή αρνητική τους στάση, τις προσωπικές εμπειρίες τους, καθώς και να απαντούν σε ερωτήσεις πολλαπλής επιλογής συμβάλλοντας με τον τρόπο αυτό στη συλλογή πολύτιμων, αξιόπιστων και επίκαιρων στατιστικών δεδομένων τα οποία θα χρησιμοποιούνται από τους φορείς λήψης αποφάσεων.

Ερωτηματολόγιο προς πολιτικούς, εμπειρογνώμονες και διοικητικούς υπαλλήλους σχετικά με θέματα απασχόλησης/ επιχειρηματικότητας των μεταναστών

ΜΕΡΟΣ Β: Συνεργασία Οργανισμών

1) Ανηρτείτε την **Αιθνή** ανερτηρίδι με την F στον τομέα της μετανάστευσης της εργασίας αμνημονί;

Ναι - ηγαίνετε στην ερώτηση 1α
 Όχι - ηγαίνετε στην ερώτηση 2
 Δεν γνωρίζω - ηγαίνετε στην ερώτηση 1α

2) Συμμετέχετε σε κάποια κοινά προγράμματα που αφορούν θέματα μετανάστευσης της εργασίας;

Ναι - ηγαίνετε στην ερώτηση 2α
 Όχι - ηγαίνετε στην ερώτηση 3

3) Ποιοι είναι οι κύριοι λόγοι/ προβλήματα που αποτρέπουν την χώρα σας από το να συμμετάσχει σε σχετικούς οργανισμούς, διεθνείς και της Ε.Ε.; [Επιλέξτε παραπάνω από μια απάντηση, αν χρειάζεται]

Οι δάουλοι επικουινονίαι/ συηκρονισμοί δεν είναι ανοικτοί στην παρατέρα συνεργασία
 Δεν υπάρχει γνώση του κοινού γύρω από τις δραστηριότητες των οργανισμών
 Το πρόσωπο/ τμήμα/ προσωπικό δεν είναι διαθέσιμα για επαφές
 Η υποστηρικτική τεχνολογία για μια τέτοια συνεργασία δεν είναι διαθέσιμη
 Τα θέματα μετανάστευσης της εργασίας δεν θεωρούνται θέματα προτεραιότητας στην εθνική πολιτική ατζέντα.
 Τα θέματα μετανάστευσης της εργασίας πρέπει να διεκρινιστούν επακριβώς μέσα στον εθνικό πολιτικό σκελεασισμό.
 Δεν γνωρίζω.

4) Γύρω από ποια θέματα θα θέλατε να συνεργαστείτε με τις παρακάτω οργανώσεις

	OECD	European Statistical Office	International Organization for Migration	International Center for Migration Policy Development (ICMPD Austria)	Central European Forum for Migration Research (CEFMAR Poland)	E.C. Directorate General Justice Freedom and Security	FRONTEX	International Law Organizations (e.g. UNHCR/ UNCTRAL)
Εθνικό Στέδιο για την Μετανάστευση	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Παρόμοιοι Αποσπασίσεις	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ευρωπαϊκά Οικονομικών μεταναστών	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

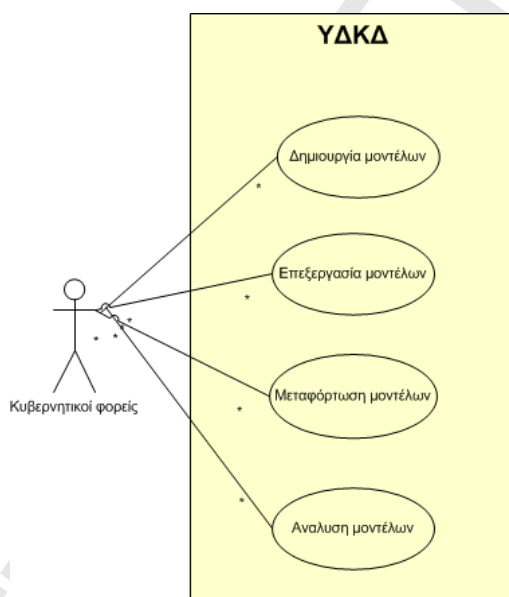
Εικόνα 5: Ανοιχτές διαβουλεύσεις στην πλατφόρμα ImmigrationPolicy 2.0

Στην Εικόνα 5 παρουσιάζεται η υλοποίηση αυτών των υπηρεσιών στην πλατφόρμα ImmigrationPolicy 2.0.

7.5.4 Υπηρεσίες Διαχείρισης Μεταναστευτικών Διαδικασιών

Ο στόχος των Υπηρεσιών Διαχείρισης Μεταναστευτικών Διαδικασιών (ΥΔΜΔ) είναι να παρέχουν ένα πλαίσιο για την γραφική αναπαράσταση δομημένων μεταναστευτικών μοντέλων και διαδικασιών τα οποία περιγράφουν τον τρόπο με τον οποίο υλοποιείται μια μεταναστευτική πολιτική.

Τα μοντέλα των μεταναστευτικών διαδικασιών θα πρέπει να συνδέονται μεταξύ τους καθώς και να αναλύονται σε μικρότερες φάσεις προκειμένου να εντοπίζονται προβλήματα και εμπόδια. Αξιοποιώντας τις πολύτιμες δυνατότητες που προσφέρουν τα σύγχρονα εργαλεία μοντελοποίησης και γραφικής αναπαράστασης διαδικασιών οι ΥΔΜΔ παρέχουν τις δυνατότητες που φαίνονται στο Σχήμα 33.

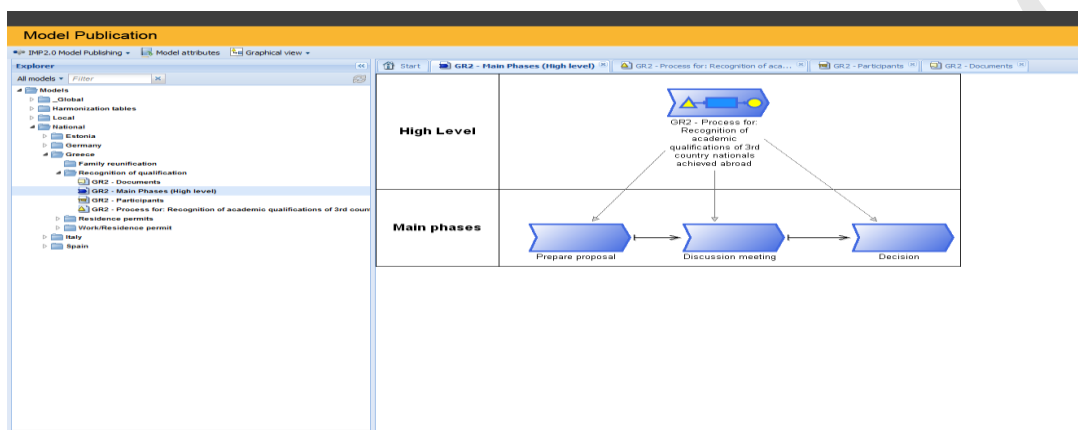


Σχήμα 33: Υπηρεσίες Διαχείρισης Μεταναστευτικών Διαδικασιών

Όπως φαίνεται στο σχήμα χρησιμοποιώντας τις ΥΔΜΔ οι φορείς λήψης αποφάσεων θα είναι σε θέση να:

- ✓ Σχεδιάζουν μεταναστευτικές διαδικασίες.
- ✓ Δημιουργούν και δημοσιεύουν τις μεταναστευτικές διαδικασίες που προτείνουν.
- ✓ Επεξεργάζονται και αναλύουν πληροφορίες σχετικά με τις μεταναστευτικές διαδικασίες άλλων φορέων και χωρών.
- ✓ Παρέχουν τις προτάσεις και σχόλια σχετικά με τις διαθέσιμες διαδικασίες.

Πιο κάτω παρουσιάζεται η υλοποίηση αυτών των υπηρεσιών στην πλατφόρμα ImmigrationPolicy 2.0, μέσω της διασύνδεσης με το Adonis Process Portal⁷.



Εικόνα 6: Μοντελοποίηση διαδικασιών στην πλατφόρμα ImmigrationPolicy 2.0

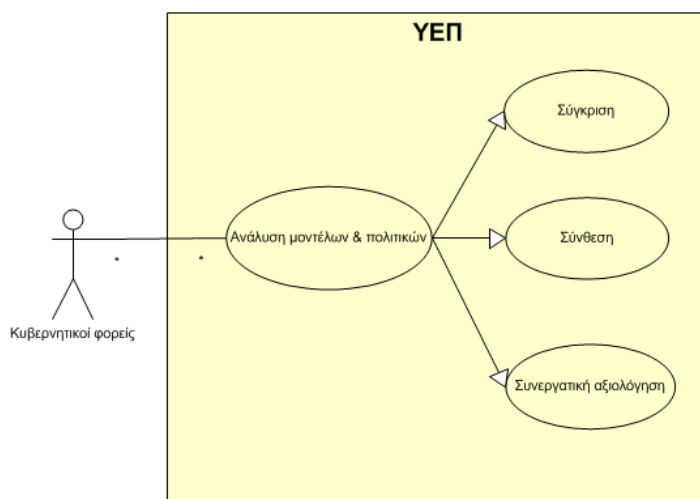
Η συσχέτιση των διαδικασιών με τις περιγραφικές πληροφορίες που χαρακτηρίζουν την κάθε εγγραφή θα βοηθήσει στην κατανόηση των πολύπλοκων σημείων και ιδιαίτερων χαρακτηριστικών των μεταναστευτικών πολιτικών που τις ενσωματώνουν.

7.5.5 Υπηρεσίες Εναρμόνισης Διαδικασιών

Με τη χρήση των *Υπηρεσιών Εναρμόνισης Διαδικασιών (ΥΕΔ)*, οι κυβερνητικοί φορείς θα έχουν τη δυνατότητα να εντοπίζουν τις ιδιαιτερότητες, τα κοινά σημεία και τις υφιστάμενες αποκλίσεις των ετερογενών μεταναστευτικών διαδικασιών προκειμένου να ενισχύουν τις προσπάθειές τους για περισσότερο αποτελεσματικές και εναρμονισμένες λύσεις.

Το Σχήμα 34 παρουσιάζει τη λειτουργικότητα που προτείνει η διατριβή για αυτή την κατηγορία υπηρεσιών του ΕΣΠΣ.

⁷ <http://www.boc-group.com/gr/products/adonis/adonis-process-portal/>

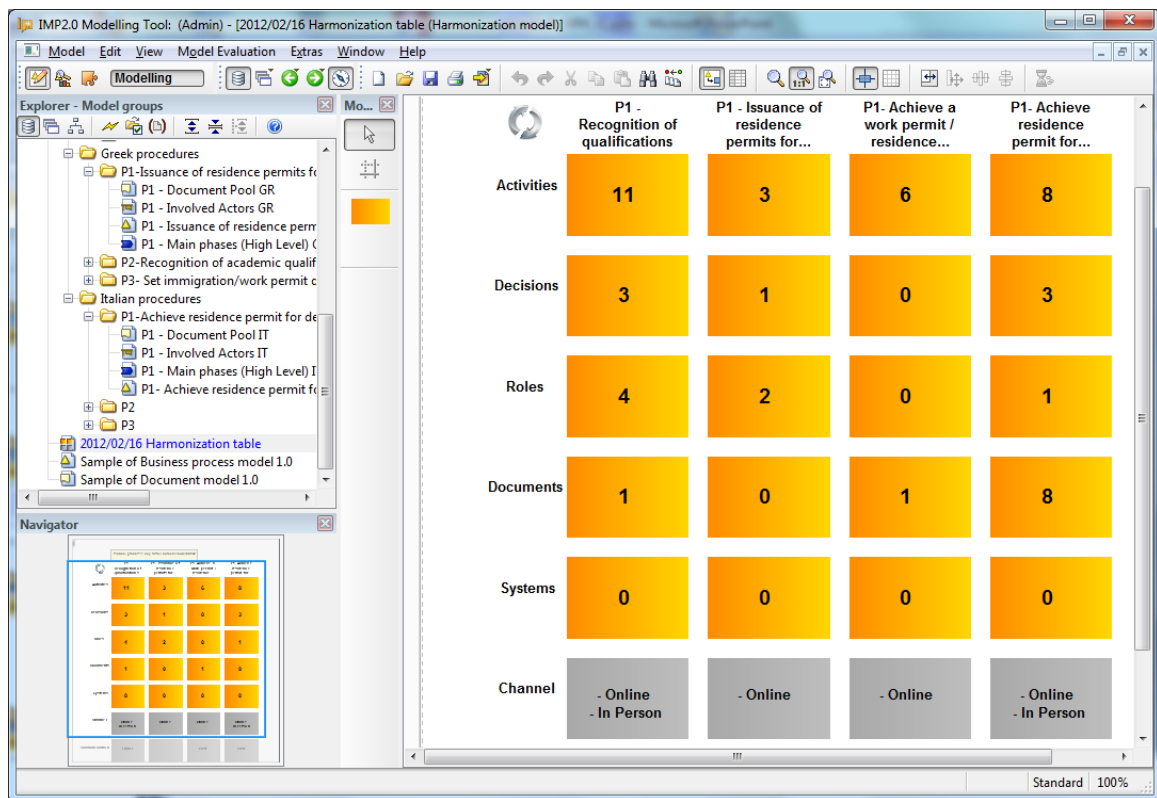


Σχήμα 34: Υπηρεσίες Εναρμόνισης Διαδικασιών

Όπως παρουσιάστηκε στην ενότητα 4.3.2.3 όπου περιγράφεται η ενσωμάτωση του Συστήματος Μοντελοποίησης Διαδικασιών στην αρχιτεκτονική του ΕΣΠΣ, η διατριβή προτείνει ότι οι ΥΕΔ πρέπει να περιλαμβάνουν καταρχάς τη σύγκριση των μεταναστευτικών διαδικασιών που προκύπτουν από την εφαρμογή των ΥΔΜΔ (βλ. ενότητα 7.5.4). Έτσι θα είναι δυνατός ο εντοπισμός των κοινών σημείων, των αποκλίσεων και των ιδιαιτεροτήτων μεταξύ ετερογενών μοντέλων καθώς και η συνεργατική συνεισφορά των εμπλεκόμενων φορέων στην ανάλυση των αποτελεσμάτων.

Επίσης, χρησιμοποιώντας σαν δεδομένα εισόδου δύο διαφορετικά μοντέλα ή διαδικασίες (τα οποία όμως θα πρέπει να αναφέρονται στην ίδια πολιτική), θα παρέχεται η δυνατότητα στους φορείς λήψης αποφάσεων να παράγουν σύνθετα μοντέλα τα οποία θα ενσωματώνουν τα εναλλακτικά σενάρια σε ένα κοινό πλαίσιο. Με τον τρόπο αυτό είναι δυνατός ο σχεδιασμός νέων εναρμονισμένων διαδικασιών σε συλλογικό επίπεδο με βάση τη συνεισφορά όλων των συμμετεχόντων.

Στην Εικόνα 7 παρουσιάζεται μέρος της ερευνητικής εργασίας του Υποψηφίου, όπου με χρήση του εργαλείου μοντελοποίησης διαδικασιών Adonis Process Portal έχει καταστεί δυνατή η σύγκριση δύο ετερογενών μεταναστευτικών διαδικασιών και ο εντοπισμός των αποκλίσεων που εμφανίζουν. Έτσι αποδεικνύεται η χρησιμότητα αυτών των υπηρεσιών και τα σημαντικά οφέλη που παρέχουν στους φορείς λήψης αποφάσεων, ιδιαίτερα όταν ενσωματώνονται στις αρχιτεκτονικές συνεργατικών πληροφοριακών συστημάτων και συνδυάζονται με άλλες τεχνολογίες και σύγχρονα πλαίσια υπηρεσιών.



Εικόνα 7: Εναρμόνιση μεταναστευτικών διαδικασιών με ADONIS Web Portal⁸

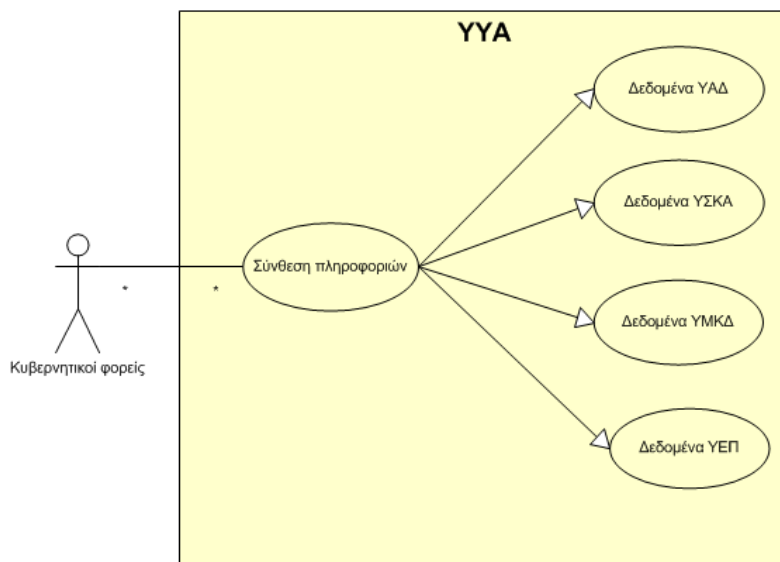
Τέλος, προτείνεται ότι αξιοποιώντας τις δυνατότητες των ΥΔΜΔ και ΥΣΚΑ, οι ΥΕΔ παρέχουν τη δυνατότητα δημοσίευσης των μεταναστευτικών διαδικασιών και των αποτελεσμάτων της αξιολόγησής τους, ενθαρρύνοντας τους χρήστες να συνεισφέρουν τις δικές τους ιδέες και προτάσεις σχετικά με το πώς και προς ποια κατεύθυνση θα πρέπει να βελτιωθούν οι υφιστάμενες πρακτικές.

7.5.6 Υπηρεσίες Υποστήριξης Αποφάσεων

Όπως περιγράφηκε στις προηγούμενες ενότητες, κάθε μια από τις παρεχόμενες υπηρεσίες δημιουργεί και διαχειρίζεται ένα σύνολο από πολύτιμα δεδομένα και πληροφορίες τα οποία συλλέγονται από τις αντίστοιχες εφαρμογές.

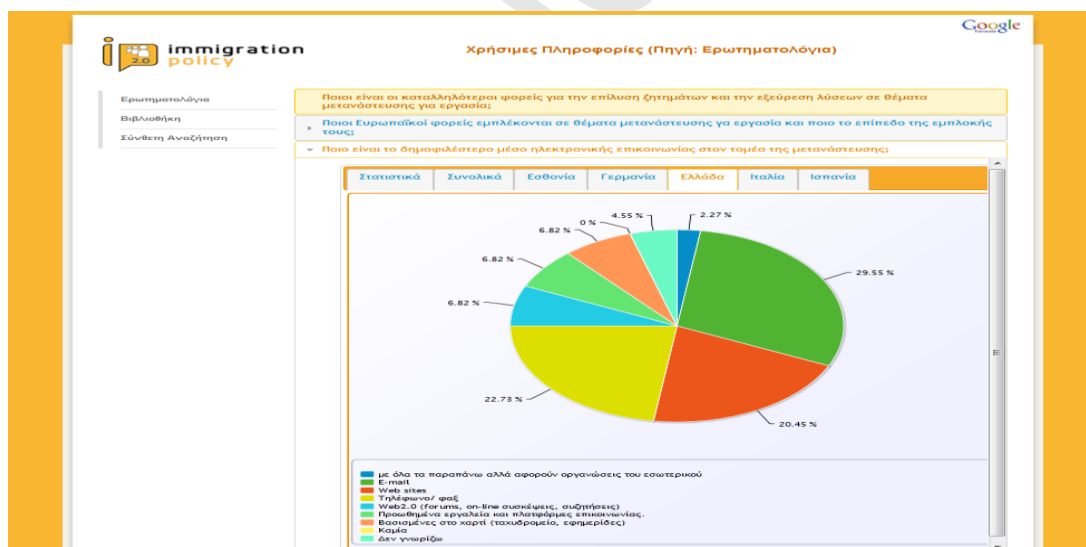
Όπως φαίνεται και στο Σχήμα 35, όλες αυτές οι πολύτιμες πληροφορίες και γνώσεις αποτελούν αντικείμενο επιπρόσθετης επεξεργασίας από το ΕΣΠΣ προκειμένου να καθιστά δυνατή την παροχή των *Υπηρεσιών Υποστήριξης Αποφάσεων (ΥΥΑ)*. Η παροχή των ΥΥΑ απαιτεί τη διασύνδεση και την επικοινωνία όλων των βάσεων δεδομένων που χρησιμοποιούνται στα πλαίσια εφαρμογής του ΕΣΠΣ. Έτσι γίνεται δυνατή η συλλογή και σύνθεση πολύτιμων πληροφοριών και στατιστικών δεδομένων καθώς και η δημιουργία υψηλής ποιότητας αναφορών για την υποστήριξη αποφάσεων σε πολύπλοκα θέματα η-Μετανάστευσης.

⁸ <http://www.boc-group.com/gr/products/adonis/adonis-process-portal/>



Σχήμα 35: Υπηρεσίες Υποστήριξης Αποφάσεων

Όπως προαναφέρθηκε, εκτός από τη συλλογή και τη διαχείριση της απαιτούμενης πληροφορίας η οποία παράγεται από τις ΥΑΔ, ΥΣΚΑ, ΥΜΚΔ και ΥΕΔ για την παροχή των ΥΓΑ απαιτείται και η επιπλέον ανάλυση, επεξεργασία και αξιολόγηση όλων των σχετικών δεδομένων. Πιο κάτω παρουσιάζεται η υλοποίηση αυτών των υπηρεσιών στην πλατφόρμα ImmigrationPolicy 2.0.



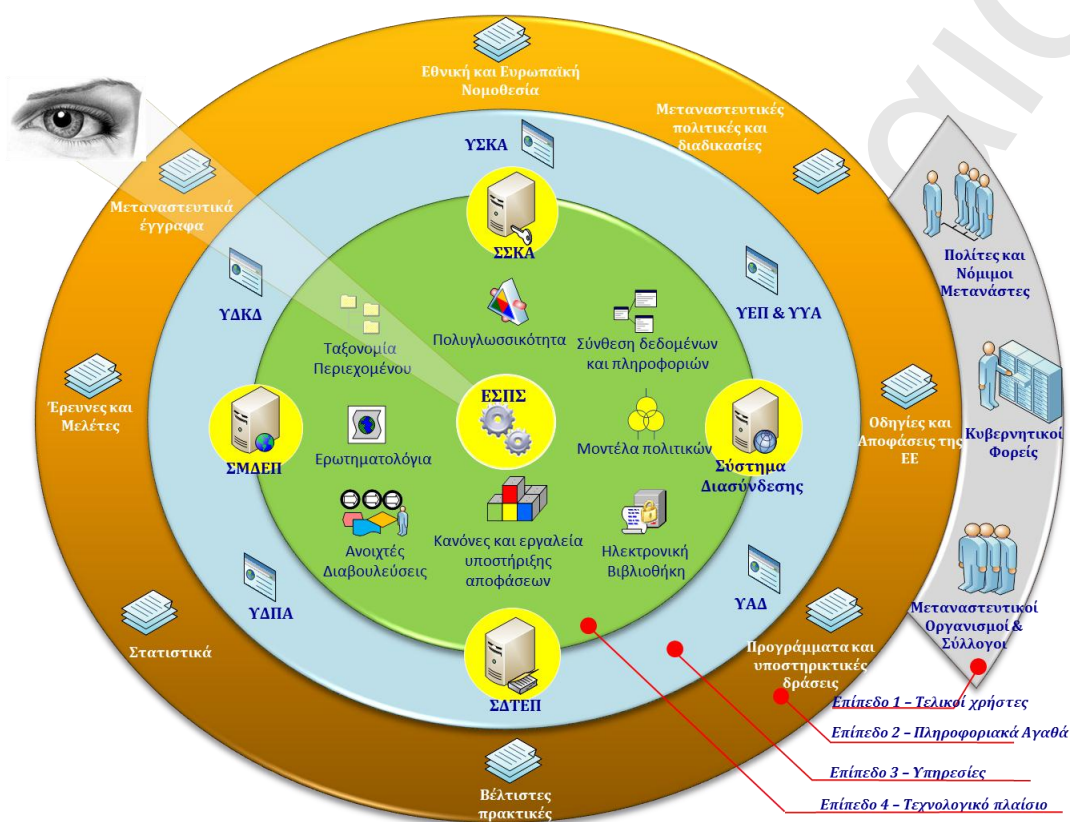
Εικόνα 8: Υποστήριξη αποφάσεων στην πλατφόρμα ImmigrationPolicy 2.0

Όλες οι προαναφερόμενες λειτουργίες και δυνατότητες παρόλο που βασίζονται σε άλλες κατηγορίες υπηρεσιών αποτελούν ξεχωριστή κατηγορία δεδομένου ότι οι λειτουργίες τους παρόλο που είναι προφανής δεν είναι εύκολα υλοποιήσιμες και προδιαγεγραμμένες.

7.6 Συνεργατικό περιβάλλον η-Μετανάστευσης

Σαν κεντρική συνεισφορά της διατριβής σε αυτό τον 5^ο κατά σειρά ερευνητικό άξονα και με βάση τα αποτελέσματα που παρουσιάστηκαν στις προηγούμενες ενότητες

αυτού του κεφαλαίου προτείνεται η εφαρμογή του ΕΣΠΣ για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης όπως παρουσιάζεται στο Σχήμα 36.



4

Σχήμα 36: Εφαρμογή ΕΣΠΣ στον τομέα η-Μετανάστευσης

Όπως φαίνεται στο Σχήμα 36, η εφαρμογή του ΕΣΠΣ στον τομέα της η-Μετανάστευσης περιλαμβάνει τις ακόλουθες οντότητες καταναμημένες σε 4 ξεχωριστά επίπεδα:

- Επίπεδο 1 - Τελικοί χρήστες
- Επίπεδο 2 - Πληροφοριακά Αγαθά
- Επίπεδο 3 - Υπηρεσίες
- Επίπεδο 4 - Τεχνολογικό πλαίσιο

Έχοντας αναλύσει σε προηγούμενες ενότητες τα επίπεδα από 1 έως 3, δηλαδή τους τελικούς χρήστες, τα πληροφοριακά αγαθά και τις υπηρεσίες και στο 4^ο Κεφάλαιο τις τεχνολογικές δυνατότητες που παρέχει το ΕΣΠΣ στο Επίπεδο 4 της αρχιτεκτονικής του, η υιοθέτηση της προτεινόμενης προσέγγισης είναι ικανή να διασφαλίσει την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης οι οποίες επιτρέπουν την ενεργή συμμετοχή και την κοινωνική αλληλεπίδραση των νόμιμων μεταναστών.

7.7 Συμπεράσματα

Διαπιστώνεται ότι η κατάλληλη αξιοποίηση των δυνατοτήτων των διαδραστικών εφαρμογών Web 2.0 είναι ικανή να εγγυηθεί την εφαρμογή καινοτόμων λύσεων σε πολύπλοκους τομείς της Ψηφιακής Εποχής. Πιο συγκεκριμένα, η παροχή ηλεκτρονικών υπηρεσιών οι οποίες προσφέρουν τη δυνατότητα συνεργασίας και ανταλλαγής προσωπικών απόψεων, εμπειριών και γνώσης είναι ικανή να βοηθήσει στην ανάπτυξη αποτελεσματικών προσεγγίσεων ικανών να αναβαθμίσουν τις παραδοσιακές πρακτικές η-Μετανάστευσης.

Αναγνωρίζοντας την έλλειψη σύγχρονων πλαισίων υπηρεσιών τα οποία διευκολύνουν την ενεργή συμμετοχή των νόμιμων μεταναστών και των φορέων λήψης αποφάσεων, η συνεισφορά της διατριβής που παρουσιάστηκε σε αυτό το κεφάλαιο έχει δύο σκέλη. Καταρχάς, αφορά στον ορισμό μιας ολοκληρωμένης μεθοδολογίας καθορισμού του εννοιολογικού πλαισίου παρέχοντας έτσι το απαραίτητο θεωρητικό υπόβαθρο για την παροχή καινοτόμων υπηρεσιών.

Το δεύτερο σκέλος της συνεισφοράς σε αυτόν τον ερευνητικό άξονα αφορά στην υλοποίηση του εννοιολογικού πλαισίου μέσω της υιοθέτησης της αρχιτεκτονικής του ΕΣΠΣ, παρουσιάζοντας τις προδιαγραφές προηγμένων υπηρεσιών η-Μετανάστευσης που είναι ικανό να παρέχει, με βάση τα αποτελέσματα ου παρουσιάζονται στο 4^ο κεφάλαιο της διατριβής.

Επίσης διαπιστώνεται ότι οι σύγχρονες τεχνολογίες για μοντελοποίηση διαδικασιών, διαχείριση γνώσης και διάχυση πληροφοριών είναι σε θέση να διαδραματίσουν έναν κρίσιμο ρόλο στην αποτελεσματική αντιμετώπιση πολύπλοκων κοινωνικών θεμάτων, όπως είναι ο τομέας της μετανάστευσης. Επιπρόσθετα, η εξέλιξη των τεχνολογιών Web 2.0 αποτελεί μια απαραίτητη στρατηγική καθώς παρέχει τη δυνατότητα στους χρήστες να συνεισφέρουν τη δημιουργικότητά τους, να συμμετέχουν σε κοινωνικά δίκτυα και ομάδες κοινού ενδιαφέροντος προκειμένου να ανταλλάσσουν τις γνώσεις και εμπειρίες τους και να διαμοιράζονται χρήσιμες πληροφορίες.

Τελικά, η εφαρμογή του ΕΣΠΣ σε κρίσιμους και πολύπλοκους τομείς όπως αυτός της η-Μετανάστευσης προτείνεται ως μια αποτελεσματική προσέγγιση για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών οι οποίες ενισχύουν την αλληλεπίδραση μεταξύ των χρηστών αλλά και τη συνεργασία μεταξύ των φορέων λήψης αποφάσεων.

7.8 Βιβλιογραφία

- [1] W. Bosswick, V. Krobisch, G. Pentafronimos, N. Polemi, ..., T. Karantjiaw (2011). "D1.1 End User Requirements". Deliverable of the European project Immigrationpolicy 2.0 (CIP-ICT-PSP-2009-3).
Available at: <http://www.immigrationpolicy2.eu/?q=node/22>.
- [2] G. Pentafronimos, N. Rodríguez, N. Polemi, V. Krobisch, ..., T. Karantjias (2010). "D1.2 State-of-the-art and advances in European migration policies". Deliverable of the European project Immigrationpolicy2.0 (CIP-ICT-PSP-2009-3).
Available at: <http://www.immigrationpolicy2.eu/?q=node/22>.
- [3] G. Pentafronimos, T. Karantjias, N. Polemi, N. Rodríguez, W. Bosswick, ..., Tea Tammistu (2011). "D2.1 User and Service Classification". Deliverable of the European project Immigrationpolicy2.0 (CIP-ICT-PSP-2009-3).
Available at: <http://www.immigrationpolicy2.eu/?q=node/22>.
- [4] G. Pentafronimos, T. Karantjias, N. Polemi, N. Rodríguez, W. Bosswick, ..., Andrea Donda (2011). "D2.2 Definition of Services and Service Bundles". Deliverable of the European project Immigrationpolicy2.0 (CIP-ICT-PSP-2009-3).
Available at: <http://www.immigrationpolicy2.eu/?q=node/22>.
- [5] T. Ntouskas, G. Pentafronimos, and S. Papastergiou (2011). "STORM - Collaborative Security Management Environment". In Proceedings of the Fifth Workshop In Information Security Theory And Practice, Security and Privacy of Mobile Devices in Wireless Communication, (WISTP 2011). Heraklion, Greece, June 1-3 2011, Vol. 6633/2011, pp. 320-335. Springer Verlag.
- [6] N. Polemi, G. Pentafronimos, T. Ntouskas (2011). "IMP2.0 Migration Collaborative Platform and e-Services". In Proceedings of the Eleventh IFIP Conference on e-Business, e-Services and e-Society (I3E2011), Kaunas, Lithuania: Springer IFIP-AICT Book Series.
- [7] G. Pentafronimos, A. Karantjias, N. Polemi (2010). "ODYSSEUS: An Advanced, Collaborative and Trusted Framework for the Provision of Migration Services". In Proceedings of the Fifth International Conference on Internet and Web Applications and Services. pp. 531-537. Barcelona, Spain. IEEE Digital Library.

- [8] A. Karantjias, N. Polemi, G. Pentafronimos (2010). "Participatory immigration policy making and harmonization services based on collaborative Web 2.0 technologies". In A. Syed, M. Ilyas (Eds.) Service Delivery Platforms: Developing Converged Multimedia Services HandBook, pp. 357–374. CRC Press, Taylor & Francis Group Publishing.
- [9] G. Pentafronimos, A. Karantjias και N. Polemi (2009). "OPIS: An Open, Preventive and Scalable Migration Information System". In Proceedings of the 3rd International Conference on e-Democracy. Next Generation Society: Technological and Legal Issues, (e-Democracy 2009). Athens, Greece. Springer Verlag.
- [10] R. Süssmuth, W. Weidenfeld (2005). "Managing Integration: The European Union's Responsibilities Towards Immigrants" MPI and the Bertelsmann Foundation.
- [11] ETSI Technical Specification TS 102 182 v1.2.1 (2006). "Emergency Communications (EMTEL); Requirements for communications from authorities/organisations to individuals, groups or the general public during emergencies"
- [12] EC-UN Joint Migration & Development Initiative. Available at:
<http://www.migration4development.org>
- [13] ARGO Project. Available at:
http://ec.europa.eu/justice_home/funding/2004_2007/argo/
- [14] EUROMED Migration II Programme. Available at:
http://www.euromed-migration.eu/e933/index_eng.html
- [15] Migration Asylum Refugees Regional Initiative (MARRI). Available at:
<http://www.marri-rc.org/>
- [16] PROMNISTAT Project. Available at:
<http://www.prominstat.eu/drupal/?q=node/64>
- [17] International Centre for Migration Policy Development, DCIM-EU project. Available at: <http://www.icmpd.org/>
- [18] European Regional and Local Authorities for the Integration of Migrants

- (ERLAIM). Available at:
<http://www.erlaim.eu/wcm/erlaim/sezioni/Mission/objectives.htm>
- [19] Migrant Integration Policy Index (MIPEX). Available at:
<http://www.integrationindex.eu/>
- [20] European Civil Registry Network (ECRN). Available at:
<http://www.ecrn.eu/BBB/>.
- [21] European Migration Network (EMN), Information Exchange System. Available at:
<http://emn.sarenet.es/>.
- [22] PROGRESS, European Project. Available at: <http://www.mutuallearning.net/>
- [23] Crossroad project. “A Participative Roadmap for ICT Research in Electronic Governance and Policy Modelling”. Available at:
<http://is.jrc.ec.europa.eu/pages/EAP/CROSSROAD.html>
- [24] Cockpit project. Available at: <http://www.cockpit-project.eu/>
- [25] Policy Mix Tool. Available at: <http://ec.europa.eu/research/policymix/index.cfm>
- [26] SYNC-3 project. Available at: <http://www.sync3.eu/>
- [27] Rural Inclusion project. Available at: <http://www.rural-inclusion.eu/>
- [28] European Personnel Selection Office (EPSO). Available at:
http://europa.eu/epso/index_en.htm
- [29] European Job Mobility Portal, EURES. Available at:
<http://ec.europa.eu/eures/home.jsp?lang=en>
- [30] Your Europe Portal. Available at:
http://ec.europa.eu/youreurope/citizens/index_en.htm
- [31] Papademetriou (2006). “Europe and Its Immigrants in the 21st Century: A New Deal or a Continuing Dialogue of the Deaf?” MPI and Luso-American Foundation.
- [32] Ινστιτούτο Μεταναστευτικής Πολιτικής, Ι.ΜΕ.ΠΟ. (2008). Μετανάστες στην Ελλάδα: Αμοιβές, Εμβάσματα, Επιχειρηματικότητα, ISBN:978-960-89389-8-4.
- [33] Ινστιτούτο Μεταναστευτικής Πολιτικής, Ι.ΜΕ.ΠΟ. (2008), Managing Migration:

The Greek, EU, and International Contexts, ISBN:960-89389-1-0

- [34] Ινστιτούτο Μεταναστευτικής Πολιτικής, Ι.ΜΕ.ΠΟ. (2007). Capturing the benefits of Migration in Southeastern Europe, ISBN: 978-960-89389-2-2
- [35] Centre for European Policy Studies, Legal Migration-Time for Europe to play its hand, CEPS Working Document (2007), ISBN;978-92-9079-694-7.
- [36] X. Thierry, A. Herm, D. Kupiszewska, B. Nowwok, M. Poulain (2010). How the UN recommendations and the forthcoming EU regulation on international migration statistics are fulfilled in the 25 EU countries?
- [37] Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο: Χώρος 'ελευθερίας, ασφάλειας και δικαίου': Απολογισμός του προγράμματος Tampere και προοπτικές (COM(2004) 401))
- [38] Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Μελέτη σχετικά με την σχέση της νόμιμης και παράνομης μετανάστευσης (COM(2004) 412).
- [39] Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Πρώτη ετήσια έκθεση σχετικά με την μετανάστευση και την ενσωμάτωση (COM(2004) 508).
- [40] A. Anttiroiko (2010). "Innovation in Democratic E-Governance: Benefiting from Web 2.0 Applications in the Public Sector". International Journal of Electronic Government Research, Vol. 6(2), pp. 18-36.
- [41] K. Ergazakis, K. Metaxiotis, T. Tsitsanis (2011). "A State-of-The-Art Review of Applied Forms and Areas, Tools and Technologies for e-Participation". International Journal of Electronic Government Research, Vol. 7(1), pp. 1-19.
- [42] F. Fleischmann, J. Dronkers (2007). The effects of social and labour-market policies of EU- countries on the socio-economic integration of first and second generation immigrants from different countries of origin, EUI working paper, RCSAS 2007/19, European University Institute, Florence, Robert Schuman Centre for Advanced Studies.

- [43] King, S., & Cotterill, S. (2007). Transformational Government? The Role of Information Technology in Delivering Citizen-Centric Local Public Services, *Local Government Studies*, 33(3), 333-354.
- [44] M. Levy (2009). WEB 2.0 implications on knowledge management, *Journal of Knowledge Management*. Vol. 13(1), pp. 120 – 134.
- [45] P. Maglio (2011). “Modeling Complex Service Systems”. *Service Science*, Editorial Office.
- [46] C. Orgeron, D. Goodman (2011). “Evaluating Citizen Adoption and Satisfaction of E-Government”. *International Journal of Electronic Government Research*. Vol. 7(3), pp. 57-78.
- [47] SEC (2006) 892: Second Annual Report on Migration and Integration, Council of the European Union, 03.06.2006, Brussels. Retrieved September 18, 2011 from: <http://register.consilium.europa.eu/pdf/en/06/st11/st11526.en06.pdf>

Κεφάλαιο 8

Ανασκόπηση Διατριβής και Μελλοντικές Κατευθύνσεις

Το κεφάλαιο αυτό επικεντρώνεται στην ανακεφαλαίωση των ερευνητικών αποτελεσμάτων της διατριβής καθώς και στον προσδιορισμό μελλοντικών ερευνητικών κατευθύνσεων.

8.1 Συμπεράσματα

Η ενσωμάτωση εφαρμογών Web 2.0 και η παροχή διαδραστικών λειτουργιών δυναμικής δημιουργίας περιεχομένου και κοινωνικής αλληλεπίδρασης αποτελεί κοινή πρακτική για τα σύγχρονα πληροφοριακά συστήματα και πλαίσια υπηρεσιών. Παρά όμως τα ιδιαίτερα ευεργετικά οφέλη αυτής της νέας προσέγγισης τόσο στην προώθηση της συνεργασίας και στην ανταλλαγή γνώσης μεταξύ των χρηστών όσο και στην παροχή καινοτόμων, υψηλής προστιθέμενης αξίας, υπηρεσιών εκ μέρους των Παρόχων, οι διαδραστικές δυνατότητες ενεργής συμμετοχής των χρηστών ελλοχεύουν νέους κινδύνους για την ιδιωτικότητά τους.

Με βάση την έρευνα πεδίου στον τομέα της διαχείρισης ταυτοτήτων που πραγματοποιήθηκε στο πλαίσιο της διατριβής, ένα από τα βασικά συμπεράσματα αποτελεί η διαπίστωση ότι οι παραδοσιακές προσεγγίσεις δεν λαμβάνουν υπόψιν την ανάγκη των χρηστών να καθορίζουν τον τρόπο με τον οποίο προστατεύεται η ιδιωτικότητά τους στα πλαίσια ενός συνεργατικού περιβάλλοντος. Παρά το γεγονός ότι παρέχουν αξιόπιστες λύσεις για τη διαχείριση ταυτοτήτων και την ασφαλή εκτέλεση των διαδικασιών αυθεντικοποίησης και εξουσιοδότησης, εντούτοις δεν επικεντρώνονται στην αντιμετώπιση των νέων προκλήσεων προστασίας της ιδιωτικότητας από τη συμπεριφορά κακόβουλων χρηστών οι οποίοι, εκμεταλλευόμενοι τις διαδραστικές δυνατότητες που παρέχουν οι εφαρμογές Web 2.0 προσβάλλουν, συνειδητά ή ακούσια, την ιδιωτικότητα των υπολοίπων συμμετεχόντων στο περιβάλλον συνεργασίας.

Όπως περιγράφεται στο δεύτερο κεφάλαιο της διατριβής, σε αντίθεση με το παραδοσιακό μοντέλο παροχής υπηρεσιών όπου σε επιχειρησιακό επίπεδο η προστασία της ιδιωτικότητας διασφαλίζεται από τα Συμφωνητικά Συνεργασίας μεταξύ των Παρόχων που επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα καθώς και από τις δημοσιευμένες πολιτικές ιδιωτικότητας οι οποίες περιγράφουν και κατοχυρώνουν τα δικαιώματα των χρηστών έναντι των Παρόχων, στο σύγχρονο

επιχειρησιακό μοντέλο των συνεργατικών πληροφοριακών συστημάτων τα μέτρα αυτά δεν είναι επαρκή. Στα σύγχρονα συνεργατικά περιβάλλοντα όπου κάθε χρήστης έχει τη δυνατότητα δημιουργίας περιεχομένου και δημοσίευσης πληροφοριών, εκτός από τους Παρόχους, ίση ευθύνη για την προστασία των προσωπικών δεδομένων και ιδιωτικών πληροφοριών έχουν και οι ίδιοι οι χρήστες.

Σε τεχνικό επίπεδο, εκτός από την αξιοπιστία των μηχανισμών ασφάλειας και των συστημάτων διαχείρισης ταυτοτήτων που υιοθετούνται από τα σύγχρονα πληροφοριακά συστήματα, η διατριβή εντόπισε την ανάγκη να προταθούν νέες λύσεις για την προστασία της ιδιωτικότητας από τις απειλές που επιφέρουν οι διαδραστικές λειτουργίες των εφαρμογών Web 2.0, οι οποίες αναβαθμίζουν τις δυνατότητες των παραδοσιακών προσεγγίσεων.

Έχοντας σαν τελικό στόχο το σχεδιασμό ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος το οποίο αξιοποιεί την ενεργή συνεισφορά και τη συλλογική γνώση των χρηστών προκειμένου να προστατεύει με δυναμικό και αξιόπιστο τρόπο την ιδιωτικότητά τους, συμπεραίνεται ότι στα συνεργατικά περιβάλλοντα:

- ✓ Η προστασία της ιδιωτικότητας δεν καθορίζεται αποκλειστικά από την προστασία των προσωπικών δεδομένων που παρέχουν οι χρήστες στους Παρόχους κατά την εγγραφή τους στο Πληροφοριακό Σύστημα. Οι διαδραστικές λειτουργίες των σύγχρονων εφαρμογών Web 2.0 εισάγουν νέες απαιτήσεις οι οποίες προκύπτουν από το ενδεχόμενο αποκάλυψης ιδιωτικών πληροφοριών από τους ίδιους τους χρήστες.
- ✓ Η διασφάλιση της εμπιστοσύνης μεταξύ των χρηστών απαιτεί την αξιολόγηση του βαθμού αξιοπιστίας κάθε χρήστη στο να δημιουργεί περιεχόμενο και να χρησιμοποιεί τις διαδραστικές λειτουργίες των εφαρμογών Web 2.0, χωρίς να προσβάλλει την ιδιωτικότητα των υπολοίπων συμμετεχόντων.
- ✓ Ο βαθμός αξιοπιστίας κάθε χρήστη, όπως προκύπτει από την αξιολόγηση της συμπεριφοράς του από τους υπόλοιπους συμμετέχοντες, αποτελεί βασικό χαρακτηριστικό της ψηφιακής του ταυτότητας το οποίο μεταβάλλεται με την πάροδο του χρόνου. Κατά συνέπεια, είναι απαραίτητος ο υπολογισμός του με δυναμικό τρόπο κάθε φορά που ο χρήστης αιτείται δικαιωμάτων προσπέλασης στις διαδραστικές υπηρεσίες ώστε να εκδίδονται τα κατάλληλα διαπιστευτήρια εξουσιοδότησης κάθε φορά που αιτείται δικαιωμάτων προσπέλασης στις διαδραστικές υπηρεσίες.
- ✓ Η ενεργή συμμετοχή των χρηστών για την καταγραφή της κακόβουλης χρήσης των εφαρμογών Web 2.0 αποτελεί μια καινοτόμο προσέγγιση προστασίας της ιδιωτικότητας η οποία απαιτεί την ενσωμάτωση ενός κατάλληλα σχεδιασμένου Συστήματος Διαχείρισης Αξιοπιστίας, σαν αυτό που παρουσιάζεται στο 6^ο Κεφάλαιο, στην αρχιτεκτονική των παραδοσιακών συστημάτων Διαχείρισης Ταυτοτήτων.

Τα αποτελέσματα που παρουσιάστηκαν στο έκτο κεφάλαιο προτείνουν μια νέα αρχιτεκτονική διαχείρισης ταυτοτήτων η οποία επιτρέπει τη συλλογική προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα. Αυτό επιτυγχάνεται αξιολογώντας τη συμπεριφορά των χρηστών σχετικά με τον τρόπο χρήσης των εφαρμογών Web 2.0, ώστε τελικά η διαχείριση και απόδοση δικαιωμάτων προσπέλασης στις διαδραστικές υπηρεσίες του συνεργατικού περιβάλλοντος να γίνεται με ασφαλή, έμπιστο και δυναμικό τρόπο με βάση το βαθμό αξιοπιστίας τους κάθε χρονική στιγμή που αιτούνται δικαιωμάτων προσπέλασης και όχι τον στατικά προκαθορισμένο ρόλο τους εντός του Πληροφοριακού Συστήματος.

8.2 Ανασκόπηση Αποτελεσμάτων

Η διατριβή ασχολήθηκε με τον ορισμό και τον αρχιτεκτονικό σχεδιασμό ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος το οποίο ενσωματώνει καινοτόμες λύσεις για τη διαχείριση ταυτοτήτων και την προστασία της ιδιωτικότητας σε συνεργατικά περιβάλλοντα. Η κεντρική ιδέα της διατριβής βασίζεται στο γεγονός ότι στα πλαίσια του ΕΣΠΣ εντοπίζεται η επιπρόσθετη ανάγκη για προστασία της ιδιωτικότητας από κάθε ενδεχόμενη αποκάλυψη ιδιωτικών πληροφοριών από κακόβουλους χρήστες που έχουν προνόμια προσπέλασης των διαδραστικών εφαρμογών και υπηρεσιών Web 2.0.

Η έννοια της εμπιστοσύνης επεκτείνεται ώστε να περιλαμβάνει τις σχέσεις αλληλεπίδρασης μεταξύ των χρηστών, αξιολογώντας με δυναμικό τρόπο την αξιοπιστία κάθε χρήστη στο να δημιουργεί περιεχόμενο το οποίο δεν προσβάλλει την ιδιωτικότητα των υπολοίπων. Ο βαθμός αξιοπιστίας ορίζεται ως βασικό χαρακτηριστικό της ταυτότητας και προτείνεται η χρήση του για την έκδοση διαπιστευτηρίων εξουσιοδότησης και την απόδοση προνομίων προσπέλασης αναβαθμίζοντας έτσι τις παραδοσιακές προσεγγίσεις οι οποίες κρίνονται ανεπαρκείς στο να καλύψουν τις νέες απαιτήσεις με βάση το προσανατολισμένο στους ρόλους μοντέλο.

Βασική συνεισφορά της διατριβής αποτελεί επίσης η διαπίστωση ότι παρά το γεγονός ότι τα σύγχρονα πρότυπα και προδιαγραφές διαχείρισης ταυτοτήτων καθώς και τα παραδοσιακά μοντέλα ελέγχου προσπέλασης είναι σήμερα σε ένα αρκετά ώριμο στάδιο εξέλιξης το οποίο επιτρέπει την αποτελεσματική και αξιόπιστη εφαρμογή τους σε σύγχρονα πλαίσια υπηρεσιών, η εξέλιξη των τεχνολογιών Web 2.0 και η ραγδαία εξάπλωση των αντίστοιχων διαδραστικών εφαρμογών συνεργασίας και κοινωνικής αλληλεπίδρασης επέφερε νέες απαιτήσεις τις οποίες οι κλασικές προσεγγίσεις δεν είναι ικανές να καλύψουν.

Η διατριβή προτείνει την αξιοποίηση της ενεργής συμμετοχής των χρηστών για την καταγραφή της κακόβουλης χρήσης των εφαρμογών Web 2.0 ως μια καινοτόμο προσέγγιση προστασίας της ιδιωτικότητας η οποία αξιοποιεί τη συλλογική γνώση των συμμετεχόντων στο συνεργατικό περιβάλλον. Ο βαθμός αξιοπιστίας των χρηστών καθορίζεται ως κριτήριο απόδοσης προνομίων προσπέλασης στις υπηρεσίες του συνεργατικού περιβάλλοντος και έτσι προτείνεται ένα νέο μοντέλο

διαχείρισης ταυτοτήτων το οποίο είναι σε θέση να διαχειρίζεται δυναμικά τις πολιτικές εξουσιοδότησης.

Συνολικά, η συνεισφορά της διατριβής συνοψίζεται στα ακόλουθα:

1. Με στόχο την αναβάθμιση των μηχανισμών αυθεντικοποίησης και ελέγχου προσπέλασης κατά τη χρήση εφαρμογών Web 2.0, προδιαγράφεται η ενσωμάτωσή τους σε ολοκληρωμένα Πληροφοριακά Συστήματα, παρουσιάζοντας την αρχιτεκτονική ενός Έμπιστου Συνεργατικού Πληροφοριακού Συστήματος [1].
2. Καθορίζεται το Σχέδιο Ιδιωτικότητας που θα πρέπει να υιοθετείται κατά την εφαρμογή του ΕΣΠΣ ώστε να αντιμετωπίζονται αποτελεσματικά οι νέες απειλές στην ιδιωτικότητα που επιφέρουν οι διαδραστικές λειτουργίες των εφαρμογών Web 2.0 και να υλοποιούνται όλα τα απαραίτητα μέτρα προστασίας.
3. Προτείνεται μια καινοτόμος αρχιτεκτονική διαχείρισης ταυτοτήτων η οποία καθιστά δυνατή την απόδοση προνομίων προσπέλασης όχι μόνο με βάση το ρόλο των χρηστών αλλά και το βαθμό αξιοπιστίας που χαρακτηρίζει τη συμπεριφορά τους, αναβαθμίζοντας έτσι τις παραδοσιακές προσεγγίσεις.
4. Καθορίζεται μια αναδρομική μέθοδος υπολογισμού του βαθμού αξιοπιστίας η οποία βασίζεται σε ένα σύνολο κρίσιμων χαρακτηριστικών του συνεργατικού περιβάλλοντος προκειμένου να εξασφαλίζεται όχι μόνο η λήψη έμπιστων αποφάσεων εξουσιοδότησης αλλά και η αποτελεσματική αντιμετώπιση επιθέσεων συνομωσίας.
5. Η τελική συνεισφορά της διατριβής αφορά στην ενίσχυση των υφιστάμενων πρακτικών και προσεγγίσεων στον τομέα της η-Διακυβέρνησης προδιαγράφοντας τη μεθοδολογία καθορισμού του εννοιολογικού πλαισίου για την παροχή ασφαλών, ιδιωτικών και διαλειτουργικών υπηρεσιών η-Μετανάστευσης. Πιο συγκεκριμένα, παρουσιάζεται ο τρόπος εφαρμογής του ΕΣΠΣ για την παροχή ηλεκτρονικών υπηρεσιών για νόμιμους μετανάστες και φορείς λήψης αποφάσεων, αναδεικνύοντας την αξία, την ευκολία εφαρμογής καθώς και τη χρησιμότητα του σε ιδιαίτερα πολύπλοκους τομείς οι οποίοι απαιτούν τη συνεργασία και κοινωνική αλληλεπίδραση μεταξύ των χρηστών με ασφαλή, έμπιστο και αξιόπιστο τρόπο.

8.3 Μελλοντικές ερευνητικές κατευθύνσεις

Ανοιχτό πεδίο για μελλοντική ερευνητική εργασία αποτελεί η βελτιστοποίηση της μεθόδου υπολογισμού του βαθμού αξιοπιστίας μέσω του υπολογισμού κατάλληλων τιμών για τους συντελεστές επίδρασης α , β , γ ανάλογα με τις ανάγκες και τις απαιτήσεις διαφορετικών πεδίων εφαρμογής του ΕΣΠΣ. Στόχος είναι να καθοριστούν πίνακες τιμών για καθέναν από τους συντελεστές επίδρασης με βάση τα διαφορετικά χαρακτηριστικά και επιχειρησιακές ανάγκες κάθε συνεργατικού περιβάλλοντος.

Επίσης, ιδιαίτερο ενδιαφέρον χρήζει η μελέτη και ανάλυση της πολυπλοκότητας της μεθόδου υπολογισμού του βαθμού αξιοπιστίας, ανάλογα με τις προδιαγραφές του συνεργατικού περιβάλλοντος στο οποίο θα υλοποιείται καθώς επίσης και τις προκαθορισμένες απαιτήσεις αποδοτικότητας.

Η ανάπτυξη νέων προτύπων και προδιαγραφών Διαχείρισης Ταυτοτήτων, ή η αναβάθμιση των ήδη διαθέσιμων, ώστε να ικανοποιούνται οι απαιτήσεις ιδιωτικότητας σε συνεργατικά περιβάλλοντα μέσω της εφαρμογής του μοντέλου Δυναμικού Ελέγχου Προσπέλασης, αποτελεί ένα εξίσου σημαντικό ερευνητικό πεδίο το οποίο θα πρέπει να διερευνηθεί στο άμεσο μέλλον. Ακολουθώντας αυτή την προσέγγιση, θα καταστεί δυνατή η υλοποίηση και εφαρμογή προτυποποιημένων και διαλειτουργικών συστημάτων τα οποία θα υποστηρίζουν τη συλλογική προστασία της ιδιωτικότητας και την επίτευξη εμπιστοσύνη μεταξύ των χρηστών που αλληλεπιδρούν. Επίσης, θα αντιμετωπιστεί ο κίνδυνος απαξίωσης των παρεχομένων υπηρεσιών και υποβάθμισης της αξιοπιστίας των σύγχρονων συνεργατικών Πληροφοριακών Συστημάτων που εμφανίζεται όταν τα συνεργατικά περιβάλλοντα δεν είναι σε θέση να ικανοποιούν τις απειλές ιδιωτικότητας των εφαρμογών Web 2.0.

Επιπρόσθετα, η ανάπτυξη προτύπων και προδιαγραφών για τη χρήση του βαθμού αξιοπιστίας ως κριτήριο απόδοσης προνομίων προσπέλασης στις διαδραστικές υπηρεσίες κάθε συνεργατικού περιβάλλοντος θα επιτρέψει την εφαρμογή του μοντέλου και πέρα από τα όρια κάθε Πληροφοριακού Συστήματος, καθώς το δυναμικό αυτό χαρακτηριστικό της ταυτότητας των χρηστών θα είναι μεταφέσιμο μεταξύ ετερογενών περιβαλλόντων και θα επιτρέπει στους Παρόχους Ταυτοτήτων να διατηρούν μια συνολική εικόνα σχετικά με της συμπεριφορά του χρήστη. Για παράδειγμα, θα μπορούσε να διατηρείται ένας καθολικός βαθμός αξιοπιστίας του χρήστη για το σύνολο των υπηρεσιών που του προσφέρεται από μια Ομοσπονδία Παρόχων, ο οποίος θα υπολογίζεται με βάση τις επιμέρους αξιολογήσεις της συμπεριφοράς του χρήστη που διατηρεί ο κάθε Πάροχος Ταυτοτήτων στον οποίο ταυτοποιείται.

Τέλος, ερευνητικό ενδιαφέρον παρουσιάζει η μελλοντική μελέτη της κοινωνικής διάστασης των αποτελεσμάτων της διατριβής η οποία αφορά στην τελική αποδοχή των προτεινόμενων λύσεων από τους χρήστες ενός συνεργατικού περιβάλλοντος καθώς και του τρόπου με τον οποίο επιδρούν τα δημογραφικά, πολιτικά, εκπαιδευτικά και κοινωνικά χαρακτηριστικά των χρηστών στην αποτελεσματική εφαρμογή και χρήση του ΕΣΠΣ.

Πανεπιστήμιο Πειραιώς

Παράρτημα Ι – Πίνακας Τιμών Συντελεστή σ

σ	K _{min}	K _{max}	Εύρος Τιμών	σ	K _{min}	K _{max}	Εύρος Τιμών	σ	K _{min}	K _{max}	Εύρος Τιμών	σ	K _{min}	K _{max}	Εύρος Τιμών
1	0,333	0,500	0,168	26	0,929	0,963	0,034	51	0,962	0,981	0,019	76	0,974	0,987	0,013
2	0,500	0,667	0,167	27	0,931	0,964	0,033	52	0,963	0,981	0,018	77	0,975	0,987	0,012
3	0,600	0,750	0,150	28	0,933	0,966	0,032	53	0,964	0,981	0,018	78	0,975	0,987	0,012
4	0,667	0,800	0,133	29	0,935	0,967	0,031	54	0,964	0,982	0,018	79	0,975	0,988	0,012
5	0,714	0,833	0,119	30	0,938	0,968	0,030	55	0,965	0,982	0,017	80	0,976	0,988	0,012
6	0,750	0,857	0,107	31	0,939	0,969	0,029	56	0,966	0,982	0,017	81	0,976	0,988	0,012
7	0,778	0,875	0,097	32	0,941	0,970	0,029	57	0,966	0,983	0,017	82	0,976	0,988	0,012
8	0,800	0,889	0,089	33	0,943	0,971	0,028	58	0,967	0,983	0,016	83	0,976	0,988	0,012
9	0,818	0,900	0,082	34	0,944	0,971	0,027	59	0,967	0,983	0,016	84	0,977	0,988	0,011
10	0,833	0,909	0,076	35	0,946	0,972	0,026	60	0,968	0,984	0,016	85	0,977	0,988	0,011
11	0,846	0,917	0,071	36	0,947	0,973	0,026	61	0,968	0,984	0,016	86	0,977	0,989	0,011
12	0,857	0,923	0,066	37	0,949	0,974	0,025	62	0,969	0,984	0,015	87	0,978	0,989	0,011
13	0,867	0,929	0,062	38	0,950	0,974	0,024	63	0,969	0,984	0,015	88	0,978	0,989	0,011
14	0,875	0,933	0,058	39	0,951	0,975	0,024	64	0,970	0,985	0,015	89	0,978	0,989	0,011
15	0,882	0,938	0,055	40	0,952	0,976	0,023	65	0,970	0,985	0,015	90	0,978	0,989	0,011
16	0,889	0,941	0,052	41	0,953	0,976	0,023	66	0,971	0,985	0,014	91	0,978	0,989	0,011
17	0,895	0,944	0,050	42	0,955	0,977	0,022	67	0,971	0,985	0,014	92	0,979	0,989	0,011
18	0,900	0,947	0,047	43	0,956	0,977	0,022	68	0,971	0,986	0,014	93	0,979	0,989	0,010
19	0,905	0,950	0,045	44	0,957	0,978	0,021	69	0,972	0,986	0,014	94	0,979	0,989	0,010
20	0,909	0,952	0,043	45	0,957	0,978	0,021	70	0,972	0,986	0,014	95	0,979	0,990	0,010
21	0,913	0,955	0,042	46	0,958	0,979	0,020	71	0,973	0,986	0,014	96	0,980	0,990	0,010
22	0,917	0,957	0,040	47	0,959	0,979	0,020	72	0,973	0,986	0,013	97	0,980	0,990	0,010
23	0,920	0,958	0,038	48	0,960	0,980	0,020	73	0,973	0,986	0,013	98	0,980	0,990	0,010
24	0,923	0,960	0,037	49	0,961	0,980	0,019	74	0,974	0,987	0,013	99	0,980	0,990	0,010
25	0,926	0,962	0,036	50	0,962	0,980	0,019	75	0,974	0,987	0,013	100	0,980	0,990	0,010

Πανεπιστήμιο Πειραιώς

Γλωσσάρι

Προσωπικά και Ευαίσθητα Δεδομένα (ΠΕΔ): Τα ΠΕΔ ορίζονται ως κάθε πληροφορία σχετική με έναν συγκεκριμένο χρήστη η οποία είτε περιλαμβάνει δεδομένα τα οποία μπορούν να χρησιμοποιηθούν για να αναγνωρίσουν ή εντοπίσουν την ταυτότητα του χρήστη είτε συνδέεται αποκλειστικά με τον κάτοχό της. Πιο κάτω παρουσιάζεται μια λίστα δεδομένων τα οποία ανήκουν στην κατηγορία των ΠΕΔ:

- ✓ Όνομα, επώνυμο, όνομα γονέα ή ψευδώνυμο
- ✓ ΑΦΜ, αριθμός ταυτότητας, αριθμός διαβατηρίου, αριθμός κοινωνικής ασφάλισης, αριθμός άδειας οδήγησης, δεδομένα πιστωτικών καρτών
- ✓ Διεύθυνση κατοικίας και διεύθυνση ηλεκτρονικού ταχυδρομείου
- ✓ Αριθμός τηλεφώνου
- ✓ Διεύθυνση ip, διεύθυνση MAC
- ✓ Προσωπικά χαρακτηριστικά που αποκαλύπτονται μέσω φωτογραφιών και άλλων πολυμεσικών εφαρμογών
- ✓ Πληροφορίες σχετικά με ιδιοκτησιακά αγαθά όπως οι αριθμοί κυκλοφορίας των αυτοκινήτων
- ✓ Ημερομηνία και τόπος γέννησης, φυλή, εθνικότητα, θρησκεία, βάρος, προσωπικές δραστηριότητες, γεωγραφικές συντεταγμένες, πληροφορίες επαγγελματικής κατάστασης, ιατρικά δεδομένα, οικονομικά δεδομένα.

Διαχείριση Ταυτοτήτων: Ως Διαχείριση Ταυτοτήτων ορίζεται ο συνδυασμός τεχνολογικών συστημάτων, κανόνων και διαδικασιών τα οποία προσδιορίζουν την ιδιοκτησία, τη χρήση και τη διασφάλιση των προσωπικών δεδομένων που περιλαμβάνει η ψηφιακή ταυτότητα των χρηστών. Ο πρωταρχικός στόχος της Διαχείρισης Ταυτοτήτων είναι να εφαρμόσει μια έμπιστη διαδικασία για την απόδοση προνομίων στις ψηφιακές ταυτότητες και τη σύνδεση των τελευταίων με φυσικές οντότητες. Ως οντότητες ορίζονται άτομα, ομάδες χρηστών, επιχειρήσεις, οργανισμοί, υπηρεσίες κτλ. Τέλος η διαχείριση ταυτοτήτων περιλαμβάνει διαδικασίες για τη διαχείριση και προστασία των δεδομένων των ψηφιακών ταυτοτήτων για όλη τη διάρκεια του κύκλου ζωής τους.

Διαπιστευτήρια Αυθεντικοποίησης: Χρησιμοποιούνται για να αποδείξουν την αυθεντικότητα μιας ταυτότητας. Υπάρχουν διάφοροι τύποι διαπιστευτηρίων όπως οι έξυπνες κάρτες, τα βιομετρικά δεδομένα, τα δημόσια και ιδιωτικά κλειδιά των ψηφιακών πιστοποιητικών, τα ίδια τα ψηφιακά πιστοποιητικά ή ένα όνομα χρήστη και το συνθηματικό που το συνοδεύει. Σκοπός τους είναι να αποδεικνύουν στο σύστημα, με έναν αποδεκτό βαθμό εμπιστοσύνης, ότι κάποια

συγκεκριμένη οντότητα έχει πραγματικά το δικαίωμα να χρησιμοποιεί τη συγκεκριμένη ταυτότητα.

Διαπιστευτήρια Εξουσιοδότησης: Τα διαπιστευτήρια εξουσιοδότησης έχουν την ίδια μορφή με τα διαπιστευτήρια αυθεντικοποίησης με τη διαφορά ότι χρησιμοποιούνται για να αποδείξουν την εγκυρότητα των προνομίων προσπέλασης των πόρων του συνεργατικού περιβάλλοντος που δικαιούται ο χρήστης με βάση κάποιο χαρακτηριστικό της ψηφιακής του ταυτότητας όπως ο ρόλος που του έχει αποδοθεί στο σύστημα ή ο βαθμός αξιοπιστίας του εντός του συνεργατικού περιβάλλοντος. Τα διαπιστευτήρια εξουσιοδότησης στα πλαίσια των σύγχρονων υπηρεσιών και Πληροφοριακών Συστημάτων έχουν ταυτιστεί με την τεχνολογία SAML καθώς παρέχει τον πλέον ασφαλή και διαλειτουργικό τρόπο για τη μεταφορά στους.

Διαχείριση Ταυτοτήτων και Έλεγχος Προσπέλασης (ΔΤΕΠ): Περιλαμβάνει ένα σύνολο επιχειρησιακών διαδικασιών, τεχνολογιών υποστηρικτικών υποδομών και πολιτικών για τη δημιουργία, τη διατήρηση και τη χρήση ψηφιακών ταυτοτήτων εντός ενός ολοκληρωμένου πληροφοριακού συστήματος. Στο πλαίσιο της διατριβής βασικός στόχος του προτεινόμενου μοντέλου ΔΤΕΠ είναι να προσφέρει ένα επεκτάσιμο, διαλειτουργικό, ασφαλές και έμπιστο πλαίσιο δυναμικής απόδοσης προνομίων προσπέλασης στα πληροφοριακά αγαθά και τους κρίσιμους πόρους του συνεργατικού περιβάλλοντος με βάση κρίσιμα χαρακτηριστικά της ταυτότητας των χρηστών.

Καθολική Σύνδεση (Single Sign On, SSO): Αναφέρεται στη διαδικασία αυθεντικοποίησης η οποία επιτρέπει στους χρήστες να αυθεντικοποιούνται μια φορά και στη συνέχεια να αποκτούν πρόσβαση στους πόρους ετερογενών πληροφοριακών συστημάτων. Συνήθως παρέχεται στα πλαίσια εφαρμογής κεντροποιημένων ή ομοσπονδιακών Πληροφοριακών συστημάτων και πλαϊσίων υπηρεσιών.

Πάροχος Ταυτοτήτων (ΠΤ): Ο Πάροχος Ταυτοτήτων αποτελεί μια έμπιστη οντότητα η οποία ολοκληρώνει προηγμένους μηχανισμούς και συστήματα ΔΤΕΠ για την επικύρωση της αυθεντικότητας των χρηστών και των υπολοίπων οντοτήτων που συμμετέχουν στο πλαίσιο υπηρεσιών. Ο ΠΤ έχει τη δικαιοδοσία και την ευθύνη να εκδίδει τα διαπιστευτήρια αυθεντικοποίησης και εξουσιοδότησης και συνήθως παρέχει υπηρεσίες ΔΤΕΠ για περισσότερες από μια οντότητες (π.χ. Παρόχους Υπηρεσιών).

Πάροχος Υπηρεσιών (ΠΥ): Ο Πάροχος Υπηρεσιών αποτελεί μια οντότητα η οποία παρέχει ηλεκτρονικές υπηρεσίες σε άλλες οντότητες και/ή χρήστες. Στην πλειοψηφία των περιπτώσεων, ο ΠΥ βασίζεται στις υπηρεσίες ενός έμπιστου ΠΤ για τη διαχείριση των ψηφιακών ταυτοτήτων και τον έλεγχο προσπέλασης των χρηστών που έχουν πρόσβαση σε αυτόν. Μάλιστα είναι υπεύθυνος για την εφαρμογή των αποφάσεων ελέγχου προσπέλασης που του προωθεί ο ΠΤ μέσω των διαπιστευτηρίων εξουσιοδότησης.

Ακρωνύμια

ΒΚ	Βαθμός Κρισιμότητας
ΔΔΕ	Δίαυλος Διαλειτουργικής Επικοινωνίας
ΔΕΠ	Δυναμικός Έλεγχος Προσπέλασης
ΔΤΕΠ	Διαχείριση Ταυτοτήτων & Έλεγχος Προσπέλασης
ΔΥΛ	Διαδραστικές Υπηρεσίες & Λειτουργίες
ΕΛΧ	Ευρετήριο Λογαριασμών Χρήστη
ΕΠΡ	Έλεγχος Προσπέλασης με βάση το Ρόλο
ΕΣΠΣ	Έμπιστο & Συνεργατικό Πληροφοριακό Σύστημα
ΙΕΠ	Ιδιοκτησιακός Έλεγχος Προσπέλασης
ΚΔ	Κοινωνικά Δίκτυα
ΚΕ	Κατώφλι Εμπιστοσύνης
ΜΜΔ	Μονάδα Μοντέλων Διαδικασιών
ΜΑΣΕ	Μονάδα Αξιολόγησης και Συνεργατικής Εναρμόνισης
ΜΒΔ	Μονάδα Βάσης Δεδομένων
ΜΔΕΠ	Μονάδα Διαχείρισης και Επιβολής Πολιτικών
ΜΔΣΠ	Μονάδα Διαχείρισης Συνδέσεων και Προσπέλασης
ΜΔΤΕΠ	Μονάδα Ελέγχου Προσπέλασης
ΜΔΥΙ	Μονάδα Διαχείρισης Υπηρεσιών Ιστού
ΜΔΧ	Μονάδα Διεπαφών Χρήστη
ΜΔΨΤ	Μονάδα Διαχείρισης Ψηφιακών Ταυτοτήτων
ΜΜΓΑ	Μονάδα Μοντελοποίησης και Γραφικής Απεικόνισης
ΜΠΑΠ	Μονάδα Πληροφοριακών Αγαθών και Προτύπων
ΠΕΔ	Προσωπικά & Ευαίσθητα Δεδομένα
ΠΣ	Πληροφοριακό Σύστημα
ΠΤ	Πάροχος Ταυτοτήτων
ΠΥ	Πάροχος Υπηρεσιών
ΣΔΑ	Σύστημα Διαχείρισης Αξιοπιστίας
ΣΔΤΕΠ	Σύστημα Διαχείρισης Ταυτοτήτων & Ελέγχου Προσπέλασης
ΣΙΑ-ΕΣΠΣ	Σχέδιο Ιδιωτικότητας ΕΣΠΣ
ΣΜΔΕΠ	Σύστημα Μοντελοποίησης Διαδικασιών & Εναρμόνισης Πολιτικών
ΣΠΣ	Συνεργατικό Πληροφοριακό Σύστημα
ΣΣΚΑ	Σύστημα Συνεργασίας & Κοινωνικής Αλληλεπίδρασης
ΤΕΙ	Τεχνολογίες Ενίσχυσης Ιδιωτικότητας
ΥΑΔ	Υπηρεσίες Ανοιχτών Διαβουλεύσεων
ΥΔΜΔ	Υπηρεσίες Διαχείρισης Μεταναστευτικών Διαδικασιών
ΥΔΠΑ	Υπηρεσίες Διαχείρισης Πληροφοριακών Αγαθών
ΥΕΔ	Υπηρεσίες Εναρμόνισης Διαδικασιών

ΥΕΠ	Υποχρεωτικός Έλεγχος Προσπέλασης
ΥΜΔΠΑ	Υπό-Μονάδα Διαχείρισης Πληροφοριακών Αγαθών
ΥΜΕΔ	Υπό-Μονάδα Εναρμόνισης Διαδικασιών
ΥΜΕΕ	Υπό-Μονάδα Μετασχηματισμού και Ενσωμάτωσης
ΥΜΕΠ	Υπό-Μονάδας Επιβολής Πολιτικών
ΥΣΚΑ	Υπηρεσίες Συνεργασίας και Κοινωνικής Αλληλεπίδρασης
ΥΥΑ	Υπηρεσίες Υποστήριξης Αποφάσεων
BPM	Business Process Management
ESB	Enterprise Service Bus
IAM	Identity & Access Management
P2P	Peer-to-Peer
PET	Privacy Enhancing Technology
SOA	Service Oriented Architecture
SSO	Single Sign On
STS	Security Token Service
TCIS	Trusted Collaborative Information System

Πανεπιστήμιο Πειραιώς