ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κατανεμημένη Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων σε Ετερογενή Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Φώτης Ι. Γώγουλος

Αθήνα, Απρίλιος 2013

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Κατανεμημένη Πλατφόρμα Διαχείρισης Εξουσιοδοτήσεων σε Ετερογενή Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Φώτης Ι. Γώγουλος

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

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 22η Απριλίου 2013.

.....	.....	.....
Ιάκωβος Βενιέρης Καθηγητής Ε.Μ.Π.	Δήμητρα-Θεοδώρα Κακλαμάνη Καθηγήτρια Ε.Μ.Π.	Νικόλαος Ουζούνογλου Καθηγητής Ε.Μ.Π.
.....	.....	.....
Συμεών Παπαβασιλείου Αναπλ. Καθηγητής Ε.Μ.Π.	Κώστας Κοντογιάννης Αναπλ. Καθηγητής Ε.Μ.Π.	Μιχαήλ Θεολόγου Καθηγητής Ε.Μ.Π.
	.....	
	Χρήστος Δουληγέρης Καθηγητής Παν. Πειραιώς	

Αθήνα, Απρίλιος 2013

.....

Φώτης Ι. Γώγουλος

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Οι πρόσφατες εξελίξεις στις Τεχνολογίες Πληροφορίας και Επικοινωνιών έχουν σηματοδοτήσει θεμελιώδεις αλλαγές στα χαρακτηριστικά και στις αρχές των παρεχόμενων προς τους χρήστες υπηρεσιών. Οι πάροχοι υπηρεσιών επενδύουν με αυξητικές τάσεις στην αξιοποίηση προσωποποιημένων κατανεμημένων τεχνολογικών λύσεων και στον σχηματισμό δυναμικών συνασπισμών με απομακρυσμένους εταίρους, με στόχο την καλύτερη προσαρμογή στις ανάγκες των χρηστών και την αύξηση της παραγωγικότητας αντίστοιχα. Ωστόσο, οι εμπλεκόμενες ηλεκτρονικές συναλλαγές προϋποθέτουν και συνεπάγονται τη συγκέντρωση, χρήση και διακίνηση προσωπικών δεδομένων πληροφοριών και ευαίσθητων επιχειρηματικών πληροφοριών, γεγονός το οποίο εγείρει σημαντικά θέματα ιδιωτικότητας των χρηστών και εμπιστευτικότητας των πληροφοριών.

Η παρούσα διατριβή πραγματεύεται τον έλεγχο του διαμοιρασμού ευαίσθητων και προσωπικών πληροφοριών, μέσω της κατάλληλης διαχείρισης εξουσιοδοτήσεων για πρόσβαση σε δεδομένα. Απώτερος στόχος του προτεινόμενου συστήματος είναι ο εμπλουτισμός των διαδικασιών λήψης αποφάσεων εξουσιοδότησης, έτσι ώστε να λαμβάνονται υπόψη παράγοντες όπως είναι η ιδιωτικότητα των χρηστών, τα χαρακτηριστικά γνωρίσματα των αλληλεπιδρώντων οντοτήτων και οι τρέχουσες συνθήκες του πλαισίου χρήσης.

Προς τούτο, στον πυρήνα της προδιαγραφόμενης λύσης εντοπίζεται ένα σημασιολογικό μοντέλο ελέγχου πρόσβασης με την κατάλληλη εκφραστικότητα για την κάλυψη των προαναφερθέντων απαιτήσεων, ενώ οι τελικές εξουσιοδοτήσεις προκύπτουν ως αποτέλεσμα της εφαρμογής των απαραίτητων συμπερασματικών αλγορίθμων συγκερασμού των προτιμήσεων των χρηστών και των παρόχων του συστήματος. Προς ενίσχυση της κλιμακοθετησιμότητας των διαδικασιών λήψης αποφάσεων, η εφαρμογή των συμπερασματικών αλγορίθμων πραγματοποιείται πριν την εκκίνηση του συστήματος, ενώ το αποτέλεσμα αυτής αποτυπώνεται στη μορφή ψηφιακών πιστοποιητικών ιδιοτήτων, τα οποία κατά τη διάρκεια της λειτουργίας του συστήματος αξιοποιούνται ως αποδείξεις εξουσιοδότησης. Με αυτόν τον τρόπο, σε πραγματικό χρόνο οι υπολογιστικές ανάγκες της υποδομής αναφορικά με την αποτίμηση των δικαιωμάτων χρηστών περιορίζονται στην αναγνώριση των τρεχόντων συνθηκών πρόσβασης. Τόσο το αναπτυχθέν σημασιολογικό μοντέλο, όσο και η μηχανή παραγωγής αποφάσεων εξουσιοδότησης ενσωματώνονται σε μια κατανεμημένη

Υποδομή Δημόσιου Κλειδιού, με στόχο την εξασφάλιση σχέσεων εμπιστοσύνης μεταξύ των διακριτών οντοτήτων του συστήματος.

Λέξεις κλειδιά: εξουσιοδότηση, έλεγχος πρόσβασης, ιδιωτικότητα, ετερογενή περιβάλλοντα, συλλογισμός, ψηφιακά πιστοποιητικά, σημασιολογικό μοντέλο, Υποδομή Δημόσιου Κλειδιού, Υποδομή Διαχείρισης Δικαιωμάτων

Abstract

Recent advances in Information and Communication Technologies have fundamentally reshaped the principles and characteristics of the provided digital services. Service providers invest with increasing rates into personalized distributed technologies and the formulation of dynamic coalitions with remote stakeholders, in order to adapt more effectively to the needs of their users and to increase productivity, respectively. However, the emerging transactions dictate the concentration, use and circulation of personal data and sensitive corporate information and thus ignite severe privacy and data confidentiality concerns.

The present doctoral thesis deals with the control of sensitive information sharing procedures, through the proper authorization management, as far as access to data is concerned. Ultimate goal of the proposed system is the enhancement of the authorization decision process, in order to capture value from features such as the privacy of the users, the identification of entities' attributes and context awareness.

For these purposes, the core of the specified solution is occupied by a semantic access control model with the required expressiveness to cover the aforementioned requirements, while final authorizations represent the outcome of the enforcement of reasoning algorithms which deal, among others, with the alignment of the users' and providers' confidentiality preferences. Aiming at scalability benefits, the reasoning process is conducted in an offline fashion, while the produced results are coded into digital attribute certificates, which are utilized during the system operation as authorization tokens. Consequently, the system's processing requirements while deciding the privileges of the infrastructure's entities in real time are limited to the evaluation of contextual parameters and conditions. The semantic model as well as the authorization decision engine which have been developed in the scope the thesis, are incorporated into a decentralized Public Key Infrastructure, which works towards the establishment of trust relationships between the distinct entities of the system.

Λέξεις κλειδιά: authorization, access control, privacy, heterogeneous environments, reasoning, digital certificates, semantic model, Public Key Infrastructure, Privilege Management Infrastructure

Αντί Προλόγου

Η παρούσα διδακτορική διατριβή αποτελεί το επιστέγασμα μιας ερευνητικής προσπάθειας που διήρκησε περίπου έξι χρόνια. Μέσω αυτού του σύντομου προλόγου, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντά μου κ. Ιάκωβο Βενιέρη, Καθηγητή Ε.Μ.Π., για την εμπιστοσύνη που επέδειξε στις δυνατότητές μου αλλά και τη στήριξή του σε όλη τη διάρκεια της διατριβής, καθώς και την Καθηγήτρια Ε.Μ.Π. κα. Δήμητρα-Θεοδώρα Κακλαμάνη για τη συνεχή υποστήριξη και καθοδήγηση. Ένα ιδιαίτερο ευχαριστώ αρμόζει στους συναδέρφους μου στο εργαστήριο «Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης», κάποιους εκ των οποίων έχω την τιμή να θεωρώ φίλους, καθώς και σε ανθρώπους εκτός ακαδημαϊκού περιβάλλοντος που υπήρξαν καθημερινά και έμπρακτα αρωγοί στην προσπάθειά μου. Τέλος, το πιο μεγάλο ευχαριστώ αξίζει στη Γεωργία και στην οικογένεια μου, τους γονείς μου Γιάννη και Κατερίνα και την αδερφή μου Νάντη, για τη συνεχή συμπαράσταση και την πίστη που έδειξαν καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

1 Εισαγωγή

Ανέκαθεν το Διαδίκτυο ως μέσο διατηρούσε άρρηκτους δεσμούς με τις Τεχνολογίες Πληροφορίας και Επικοινωνιών (ΤΠΕ), σε σημείο που η εξάπλωσή του να βρίσκεται σε άμεση συνάρτηση με τις εξελίξεις στις εν λόγω τεχνολογίες. Σήμερα το Διαδίκτυο και οι αντίστοιχες παρεχόμενες διαδικτυακές υπηρεσίες, ακολουθώντας τις εξελίξεις στις ΤΠΕ, καλύπτουν ολοένα και μεγαλύτερη ποικιλία εφαρμογών, εξυπηρετούν ένα ευρύτατο φάσμα χρηστών και επιδρούν ουσιαστικά σε ένα αυξανόμενο ποσοστό των εκφάνσεων της καθημερινότητας απλών πολιτών αλλά και οργανισμών. Σε αυτό το κλίμα, ο σύγχρονος παγκόσμιος διαδικτυακός χάρτης κατακλύζεται από κατανεμημένες εφαρμογές και πλαίσια διασύνδεσης γεωγραφικά, διαχειριστικά και διοικητικά απομακρυσμένων οντοτήτων. Απλοί χρήστες και επιχειρηματικοί οργανισμοί αξιοποιούν το Διαδίκτυο ως χώρο μαζικής συνεργασίας και εκτεταμένης αλληλεπίδρασης μετατρέποντας το σε ένα μέσο βελτίωσης της ποιότητας ζωής και ενίσχυσης της επιχειρηματικής καινοτομίας, αναδεικνύοντας ταυτόχρονα τις εμπλεκόμενες ηλεκτρονικές συναλλαγές ως κρίσιμο στοιχείο του σύγχρονου τρόπου ζωής και εργασίας.

Αναπόσπαστο συστατικό για την επιτυχή διεξαγωγή ηλεκτρονικών συναλλαγών αποτελεί η εξασφάλιση σχέσεων εμπιστοσύνης μεταξύ των συναλλαζόμενων οντοτήτων. Όπως και στην καθημερινότητα, η εμπιστοσύνη με την έννοια της βεβαιότητας και πίστης στις δηλωμένες ικανότητες και ιδιότητες κάποιου συναλλασσόμενου εταίρου διατηρεί βαρύνουσα σημασία στον ηλεκτρονικό κόσμο. Ωστόσο, το γεγονός ότι το Διαδίκτυο αποτελεί ένα εγγενώς ανώνυμο μέσο διασύνδεσης ετερογενών περιβαλλόντων καθώς και η αποκεντρωτική λογική και ο κατανεμημένος τρόπος λειτουργίας των παρεχόμενων υπηρεσιών καθιστούν δυσχερές το έργο της εξασφάλισης εμπιστοσύνης μεταξύ δυο συνδιαλεγόμενων μερών. Πράγματι, οι παραγόμενες ηλεκτρονικές συναλλαγές δημιουργούν πολύπλοκες ροές εργασίας και δεδομένων, εμπεριέχουν πληθώρα ενδιάμεσων οντοτήτων αμφιβόλων προθέσεων, προϋποθέτουν την αξιοποίηση ευαίσθητων δεδομένων και πρέπει να ικανοποιούν ετερογενείς στρατηγικές και διαφορετικές στοχεύσεις. Ειδικότερα, η ολοένα και μεγαλύτερη συμμετοχή απλών χρηστών καθώς και η εμπλοκή προσωπικών δεδομένων στις ηλεκτρονικές διαδικασίες προσδίδουν επιπλέον ιδιαιτερότητες στις παρεχόμενες υπηρεσίες και καταστούν την αντιμετώπιση των

θεμάτων εμπιστευτικότητας επιτακτική. Υπό αυτό το πρίσμα και σε εποχές που οι χρήστες του Διαδικτύου εκφράζουν την ανησυχία τους σχετικά με την προστασία των προσωπικών τους δεδομένων και της ιδιωτικής τους ζωής ([1], [2]), η εξασφάλιση της ιδιωτικότητας των χρηστών και της εμπιστευτικότητας και ασφάλειας των επικοινωνιών αποτελούν κίνητρο για τη βιωσιμότητα και απορρόφηση των σύγχρονων παρεχόμενων υπηρεσιών.

Σε διεθνές επίπεδο, επιχειρήσεις και οργανισμοί έχουν φτάσει σε αυτή τη συνειδητοποίηση: η ικανότητα και ευχέρεια προστασίας των πόρων τους, είτε αυτοί αφορούν ευαίσθητα δεδομένα και υπηρεσίες είτε χρήστες, μπορεί να αποτελέσει κινητήρια δύναμη για την αύξηση της επιχειρηματικότητας, την ενίσχυση της ανταγωνιστικότητας και τη βελτίωση της παραγωγικότητάς τους. Για αυτό τον λόγο, μέθοδοι ταυτοποίησης χρηστών και πιστοποίησης των χαρακτηριστικών τους σε συνδυασμό με την εφαρμογή μοντέλων ελέγχου πρόσβασης με στόχο την αποδοτική διαχείριση εξουσιοδοτήσεων έχουν προταθεί και αξιοποιούνται κατά κόρον για την προστασία ευαίσθητων δεδομένων και την εξασφάλιση της εμπιστευτικότητας των ηλεκτρονικών συναλλαγών στον σύγχρονο διαδικτυακό κόσμο. Οι υποδομές διαχείρισης εξουσιοδοτήσεων είναι υπεύθυνες για την απόδοση δικαιωμάτων στους χρήστες που βρίσκονται υπό την αιγίδα τους καθώς και για την έκδοση σχετικών αποφάσεων ελέγχου πρόσβασης, επιτρέποντας σε εφαρμογές και υπηρεσίες να προσαρμόζουν τη συμπεριφορά τους στο περιεχόμενο των συγκεκριμένων αποφάσεων.

1.1 Σύγχρονες Μορφές Αποκεντρωμένων και Ετερογενών Δικτύων

Προς ικανοποίηση της αυξανόμενης ζήτησης για κατακερματισμό εργασιών και αποκέντρωση των ψηφιακών λειτουργιών στις ηλεκτρονικές διαδικασίες, οι πάροχοι υπηρεσιών βαθμιαία απομακρύνονται από τη λογική μονολιθικών αρχιτεκτονικών πελάτη – εξυπηρετητή και υιοθετούν μοντέλα κατανεμημένης πληροφορικής (distributed computing). Κοινό χαρακτηριστικό των εν λόγω μοντέλων πληροφορικής και υπολογιστικής αποτελεί η συνύπαρξη και συνεργασία πολλαπλών παράλληλων και αυτόνομων συστημάτων για την επιτυχή διεξαγωγή μιας ηλεκτρονικής διαδικασίας εν τη απουσία κάποιας κεντρικής συγκεντρωτικής οντότητας. Σύγχρονες διαδικτυακές κατανεμημένες εφαρμογές έχουν σχεδιαστεί και αναπτυχθεί βασισμένες

σε αυτή τη θεμελιώδη αρχή και αξιοποιούνται από απομακρυσμένες οντότητες εντός του Διαδικτύου προς εκπλήρωση των στόχων τους.

Χαρακτηριστικό παράδειγμα κατανεμημένου τύπου υπολογιστικής επεξεργασίας αποτελούν οι τεχνολογίες πλέγματος (grids). Τα περιβάλλοντα υπολογιστικών συστημάτων πλέγματος αποτελούν ομοσπονδίες διαχειριστικά κατανεμημένων υπολογιστικών πόρων που αλληλεπιδρούν και συνεισφέρουν για την επίτευξη ενός συμφωνηθέντος κοινού στόχου. Οι ομοσπονδίες αυτές, που συναντώνται στη βιβλιογραφία ως εικονικοί οργανισμοί (virtual organizations), προσομοιώνουν τη συμπεριφορά μιας μοναδικής και ενιαίας οντότητας – οργανισμού με ενισχυμένη διαθεσιμότητα σε υπολογιστικούς πόρους, δεδομένα και υπηρεσίες προς ικανοποίηση των κοινών στόχων των σχηματιζόμενων ομοσπονδιών. Τα δίκτυα πλέγματος έχουν να επιδείξουν ιδιαιτέρως μεγάλη απορρόφηση και εφαρμοστικότητα σε έναν αριθμό από ετερογενείς τομείς, όπως είναι η βιοϊατρική [3] και τα προγράμματα ηλεκτρονικής μάθησης e-learning [4].

Η υπολογιστική νέφους (cloud computing) αποτελεί ένα ακόμα παράδειγμα κατανεμημένης λογικής στο Διαδίκτυο. Οι τεχνολογίες νέφους παρέχουν υπολογιστική δύναμη, πρόσβαση σε λογισμικό και δεδομένα και λοιπές υπηρεσίες «χωροταξικά» τοποθετημένες σε ένα «σύννεφο» απομακρυσμένων δικτύων, χωρίς να απαιτούν καμία γνώση εκ μέρους του χρήστη σχετικά με την τοπολογία, τη σύνθεση και τη διαμόρφωση του συστήματος που προσφέρει τις υπηρεσίες. Η προσέγγιση αυτή εξασφαλίζει γρήγορη και αποδοτική πρόσβαση σε μεγάλης ποικιλομορφίας περιεχόμενο, πόρους και καινοτόμα συνεργατικά εργαλεία επικοινωνίας. Οι διευκολύνσεις που προσφέρουν στους χρήστες τους οι διαδικτυακές εφαρμογές που βασίζονται σε τεχνολογίες νέφους, κυρίως με την έννοια της ευχρηστίας και του μειωμένου κόστους τους, έχουν ευνοήσει την ακμάζουσα απορροφητικότητά τους στους κόλπους απλών χρηστών αλλά και επιχειρήσεων ([5], [6], [7]).

Επιπλέον, οι τεχνολογίες Ιστού 2.0 (Web 2.0) [8], που αναφέρονται σε καινοτόμες τεχνολογίες όπως τα κανάλια απλής διανομής Really Simple Syndication (RSS), τα ιστολόγια (blogs) και οι ιστότοποι τύπου wikis και mashups, έχουν σηματοδοτήσει ριζικές αλλαγές στη στάση που διατηρούν καθημερινοί χρήστες απέναντι στις ψηφιακές διαδικασίες κυρίως μέσω της ενίσχυσης της σημασίας της ατομικής συμμετοχής. Η θεμελιώδης μεταστροφή στη θεώρηση της θέσης του χρήστη στις ηλεκτρονικές συναλλαγές έχει επεκταθεί και στον επιχειρηματικό κόσμο διαμορφώνοντας καινούριες στρατηγικές διαχείρισης υπηρεσιών και πληροφοριών.

Ως αποτέλεσμα, καθιερωμένα επιχειρηματικά μοντέλα ανανεώνονται και επεκτείνονται για να αξιοποιούν επικερδώς δυναμικές συνεργασίες μεταξύ απομακρυσμένων οντοτήτων. Οι συνεργατικές εφαρμογές Ιστού 2.0 έχουν αποτελέσει την αιχμή του δόρατος σε αυτό το κλίμα αλλαγής και έχουν προσφέρει το υπόβαθρο για την εμφάνιση του φαινομένου Enterprise 2.0. Ο όρος Enterprise 2.0 εισήχθηκε από τον McAfee το 2006 [9] και αναφέρεται στην αξιοποίηση εργαλείων Ιστού 2.0 με στόχο την ενίσχυση της παραγωγικότητας των υπαλλήλων καθώς και την αύξηση της αποτελεσματικότητας και της ανταγωνιστικότητας μιας επιχείρησης. Εκτός από τη χρήση των προαναφερθέντων εργαλείων, τα μοντέλα τόσο του Ιστού 2.0 όσο και του Enterprise 2.0 εισάγουν μια ριζική αναδιάρθρωση της δομής που παίρνουν η ροή της πληροφορίας, η διαχείριση της γνώσης και ο διαμοιρασμός πόρων εντός μιας επιχείρησης. Όπως και τα δίκτυα πλέγματος και νέφους, οι τεχνολογίες Ιστού 2.0 και Enterprise 2.0 τυγχάνουν αυξημένης απορρόφησης και αναγνώρισης μεταξύ απλών χρηστών αλλά και επιχειρήσεων εντός του Διαδικτύου ([10], [11]).

Οι προαναφερθείσες τεχνολογίες έχουν εισάγει μια καινοτόμα προσέγγιση στη διαχείριση της πληροφορίας και της γνώσης εντός του Διαδικτύου. Η προσέγγιση αυτή συνίσταται στην «από κάτω προς τα πάνω» διαμόρφωση καινοτόμων πλαισίων επεξεργασίας, στην ενίσχυση δυναμικών και συνεργατικών συμπράξεων και στην αποδοτική καθοδήγηση των συμμετεχόντων. Σε αυτό κλίμα, η επιχειρηματική αξία της πληροφορίας σχηματίζεται συλλογικά από πλήθος απομακρυσμένων συνεργατών και δεν αποφασίζεται απλά από μειοψηφίες εταίρων. Ανεξάρτητα από επιμέρους τεχνικές ιδιαιτερότητες και λειτουργικά χαρακτηριστικά που τις διακρίνουν, οι σχετικές εφαρμογές παρουσιάζουν μια σειρά από κοινά γνωρίσματα:

- Η λειτουργία των εφαρμογών βασίζεται στην αποκέντρωση εργασιών και διαδικασιών. Προκύπτει δηλαδή η ανάγκη για ανεξαρτησία από κεντρικές συγκεντρωτικές οντότητες χωρίς να αποκλείεται η συμβολή τους αλλά με μειωμένες αρμοδιότητες.
- Καθώς οι προσφερόμενοι πόροι ανήκουν σε διαφορετικές ζώνες εμπιστευτικότητας, η χρήση και διακίνησή τους υπόκειται σε διαφορετικές και ετερογενείς πολιτικές ασφάλειας και περιορισμούς. Στις ροές εργασιών και δεδομένων που προκύπτουν, όπου εμπεριέχεται πληθώρα ενδιάμεσων οντοτήτων, κάθε εμπλεκόμενος φορέας είναι υπεύθυνος για τους χρήστες και

τους πόρους που βρίσκονται υπό την αιγίδα του. Η σχεδίαση και ανάπτυξη δηλαδή των εν λόγω εργαλείων εκτός από την αρχή της αποκέντρωσης είναι συμβατές και με αυτή της αυτονομίας.

- Στόχο των περιγραφόμενων τεχνολογιών εντός του Διαδικτύου αποτελεί η ουσιαστικότερη και εντονότερη ενεργοποίηση του ατόμου, ενεργοποίηση η οποία συνεπάγεται τη μεγαλύτερη εμπλοκή προσωπικών δεδομένων και πληροφοριών στις παραγόμενες ηλεκτρονικές διαδικασίες.
- Τα χαρακτηριστικά των συγκεκριμένων διαδικτυακών εργαλείων ευνοούν τον σχηματισμό συνομοσπονδιών αλληλεπίδρασης και συνεργασίας μεταξύ απομακρυσμένων χρηστών. Η δημιουργία των συνομοσπονδιών πολλές φορές περιλαμβάνει άγνωστες μεταξύ τους οντότητες.
- Σημαντικό στοιχείο για την ασφαλή και αποδοτική λειτουργία των συνεργατικών εφαρμογών αποτελεί η αξιόπιστη πρόσβαση σε κοινούς πόρους, δεδομένα, εφαρμογές και πληροφορίες που προέρχονται από την επεξεργασία των κοινών αυτών δεδομένων.

1.2 Εμπιστοσύνη, Ιδιωτικότητα και Ασφάλεια

Τα εγγενή χαρακτηριστικά των κατανεμημένων δικτύων και των αναδυόμενων τεχνολογιών που παρουσιαστήκαν στην προηγούμενη ενότητα μπορούν να τροφοδοτήσουν σημαντικά προβλήματα εμπιστοσύνης στους κόλπους των χρηστών τους. Αναπόφευκτα, η εμπιστοσύνη διαδραματίζει σημαντικότατο ρόλο στις ψηφιακές συναλλαγές και μπορεί να αποτελέσει εφαλτήριο αλλά και τροχοπέδη για κρίσιμες ψηφιακές διαδικασίες όπως είναι το ηλεκτρονικό εμπόριο. Αναγνωρίζοντας την κρισιμότητα του προβλήματος, πληθώρα ερευνητικών προσεγγίσεων έχει προταθεί προς συγκεκριμενοποίηση της έννοιας εμπιστοσύνη στις διαδικτυακές συναλλαγές ([12], [13], [14]). Η μεγάλη πυκνότητα της βιβλιογραφίας σχετικά με το θέμα της εμπιστοσύνης οφείλεται ακριβώς στα χαρακτηριστικά γνωρίσματα του σύγχρονου διαδικτυακού κόσμου: αβεβαιότητα και απουσία διαφάνειας, καταστάσεις που μπορούν να βλάψουν ανεπανόρθωτα τη χρησιμότητα και την αποδοτικότητα των δικτυακών συναλλαγών. Σε μια πρόσφατη έρευνα ([15]), τα συμπεράσματα αποδεικνύουν ότι τα υπάρχοντα προβλήματα των διαδικτυακών αγορών ενισχύουν την ανασφάλεια των χρηστών, τους αποτρέπουν από το να συμμετέχουν σε ψηφιακές συναλλαγές και τελικά τους οδηγεί στο να αποσύρουν την εμπιστοσύνη τους στις

συγκεκριμένες διαδικασίες. Σε ένα περιβάλλον όπου, οι εμπλεκόμενες ηλεκτρονικές συναλλαγές προϋποθέτουν και συνεπάγονται τη συγκέντρωση, χρήση και διακίνηση προσωπικών πληροφοριών και ευαίσθητων δεδομένων, η εμπιστοσύνη είναι άρρηκτα συνδεδεμένη με την ιδιωτικότητα των χρηστών και την εμπιστευτικότητα και ασφάλεια των επικοινωνιών.

Βασικό συστατικό των ανθρώπινων σχέσεων η ιδιωτικότητα όπως και η εμπιστοσύνη έχει μελετηθεί σε βάθος από ερευνητές, νομικούς και φιλοσόφους. Παρά το πλήθος διαφορετικών προσεγγίσεων που συναντάται στη βιβλιογραφία, θεωρείται δύσκολο να δοθεί ένας ενιαίος και συμπαγής ορισμός για την έννοια της ιδιωτικότητας. Ωστόσο, σημαντική στιγμή στις προσπάθειες συγκεκριμενοποίησης της έννοιας αποτελεί η αναφορά των δικαστών S. Warren και L. Brandeis στην ιδιωτικότητα ως «το δικαίωμα του ατόμου να μείνει μόνος (the right of an individual to be let alone)» στο άρθρο τους «The Right to Privacy» [16] του 1890 το οποίο και σηματοδότησε την απαρχή της επίδρασης της νομικής θεωρίας στη μελέτη του δικαιώματος για ιδιωτικότητα. Έκτοτε, η ιδιωτικότητα έχει αναγνωριστεί ως θεμελιώδες ανθρώπινο δικαίωμα στην Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα (Universal Declaration of Human Rights) [17] και ως τέτοιο συναντάται σε σειρά νομικών, νομοθετικών και συνταγματικών κειμένων. Στη σημερινή πραγματικότητα, η ιδιωτικότητα έχει συνδεθεί στενά με την έννοια της προστασίας προσωπικών ή ευαίσθητων δεδομένων οδηγώντας έτσι στη διαμόρφωση του όρου πληροφοριακή ιδιωτικότητα (informational privacy). Στα πλαίσια της παρούσας αναφοράς ως ιδιωτικότητα λογίζεται η πληροφοριακή ιδιωτικότητα η οποία και ορίζεται ως η θέσπιση και τήρηση κανόνων ελέγχου σχετικά με τον λόγο και τρόπο συλλογής, αποθήκευσης, επεξεργασίας και διάδοσης δεδομένων προσωπικού χαρακτήρα. Πρέπει να σημειωθεί ότι η έννοια της ιδιωτικότητας υπερκαλύπτει αυτή της πληροφοριακής ιδιωτικότητας και μπορεί να βρει εφαρμογή σε πλήθος διαφορετικών τομέων, ωστόσο η τελευταία και η συνεπακόλουθη σύνδεσή της με το δικαίωμα του ατόμου στην προστασία προσωπικών δεδομένων αντιμετωπίζει πληρέστερα τα θέματα και τους κινδύνους που εγείρει η σύγχρονη Κοινωνία της Πληροφορίας.

Συχνά, στα πλαίσια πληροφοριακών συστημάτων η πληροφοριακή ιδιωτικότητα συγχέεται με την ασφάλεια της πληροφορίας (information security). Ως ασφάλεια της πληροφορίας ορίζεται η προστασία της πληροφορίας και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, τροποποίηση ή καταστροφή με στόχο την εξασφάλιση ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας της

πληροφορίας. Αν και σε ορισμένες περιπτώσεις η ασφάλεια ενός πληροφοριακού συστήματος μπορεί να βοηθήσει την επίτευξη εμπιστευτικότητας των επικοινωνιών και ως αποτέλεσμα στη διασφάλιση της τηλεπικοινωνιακής ιδιωτικότητας οι δύο έννοιες αντιμετωπίζουν την προστασία του ατόμου και των πληροφοριών από διαφορετική σκοπιά. Προφανώς η πληροφοριακή ιδιωτικότητα βρίσκεται σε άμεση συνάρτηση με και εξάρτηση από την ασφάλεια των πληροφοριακών συστημάτων, ωστόσο η ύπαρξη μηχανισμών ασφάλειας δεν εξασφαλίζει την προστασία προσωπικών δεδομένων και πολλές φορές αντιτίθεται στους στόχους της ιδιωτικότητας. Χαρακτηριστικό παράδειγμα αποτελούν τα συστήματα παρακολούθησης που θεωρούνται πολλές φορές ο ακρογωνιαίος λίθος της ασφάλειας των πληροφοριακών συστημάτων.

Τα τελευταία χρόνια έχει παρουσιαστεί έντονη ερευνητική εργασία στην προσπάθεια σύζευξης των στόχων της εμπιστοσύνης, της ιδιωτικότητας και της ασφάλειας ή πιο συγκεκριμένα στη σχεδίαση και ανάπτυξη των κατάλληλων μηχανισμών ασφάλειας και διασφάλισης εμπιστοσύνης που λαμβάνουν υπόψη τους την έννοια της ιδιωτικότητας και επιβάλουν την προστασία των προσωπικών και ευαίσθητων δεδομένων των χρηστών. Σε αυτό το πλαίσιο, αντικείμενο της παρούσας διδακτορικής διατριβής αποτελεί η προδιαγραφή και η υλοποίηση ενός κατανεμημένου συστήματος διαχείρισης εξουσιοδοτήσεων με γνώμονα την προστασία της ιδιωτικότητας των χρηστών, την εμπιστευτικότητα των ευαίσθητων δεδομένων και την εξασφάλιση εμπιστοσύνης μεταξύ των αλληλεπιδρώντων οντοτήτων. Το προβλεπόμενο σύστημα παρεμβάλλεται μεταξύ των προστατευόμενων πόρων και των χρηστών και των παρόχων υπηρεσίας, εξασφαλίζοντας αυτόματα και διάφανα την εφαρμογή των προτιμήσεών τους σε σχέση με τον διαμοιρασμό των προσωπικών τους δεδομένων και των ευαίσθητων επιχειρηματικών πληροφοριών τους αντίστοιχα. Παράλληλα διασφαλίζεται ότι οι ηλεκτρονικές συναλλαγές των χρηστών και των παρόχων του συστήματος διεξάγονται σε ένα περιβάλλον όπου η εμπιστοσύνη θεωρείται εξασφαλισμένη και αδιαπραγμάτευτη. Για τη δήλωση και καταγραφή των προσωπικών τους προτιμήσεων, οι οντότητες του συστήματος προδιαγράφουν εξατομικευμένους κανόνες ελέγχου πρόσβασης, όπου ιδιαίτερο βάρος γίνεται στην ενσωμάτωση παραμέτρων επίγνωσης πλαισίου, των γνωρισμάτων των συμμετεχόντων οντοτήτων αλλά και των χαρακτηριστικών της υποκείμενης

υποδομής. Τέλος, με στόχο τη διασφάλιση ενός ελάχιστου επιπέδου κλιμακοθετησιμότητας[1] της προτεινόμενης πλατφόρμας, το μεγάλο μέρος των διαδικασιών λήψης απόφασης εξουσιοδότησης πραγματοποιείται σε χρόνο πριν την εκκίνηση των συστημάτων, διατηρώντας ωστόσο τη απαραίτητη λειτουργικότητα για την προσαρμογή των αποφάσεων εξουσιοδότησης σε δυναμικές μεταβολές του περιβάλλοντος εν ώρα λειτουργίας της πλατφόρμας.

1.3 Διάρθρωση της Διατριβής

Η Διατριβή αποτελείται συνολικά από εννιά κεφάλαια. Εκτός του παρόντος εισαγωγικού κειμένου, το περιεχόμενο του κάθε κεφαλαίου αναλύεται ως εξής:

Στο δεύτερο κεφάλαιο παρουσιάζεται μια ανάλυση των θεμάτων της ιδιωτικότητας και ασφάλειας υπό το πρίσμα της απεικόνισής τους σε επίσημα πρότυπα και νομοθετικά κείμενα. Η ενότητα καταλήγει με την καταγραφή των απαιτήσεων ιδιωτικότητας και ασφάλειας που υπαγορεύονται από τη διεξαχθείσα ανάλυση και που σε σημαντικό βαθμό συναπαρτίζουν τις λειτουργικές και μη λειτουργικές προδιαγραφές των σχετικών τεχνολογικών προσεγγίσεων.

Το τρίτο κεφάλαιο έχει ως αντικείμενο τις τρέχουσες εξελίξεις στην ερευνητική κοινότητα σε σχέση με τους μηχανισμούς διαχείρισης εξουσιοδοτήσεων και τις επεκτάσεις τους προς αντιμετώπιση των προβλημάτων ιδιωτικότητας στις ηλεκτρονικές διαδικασίες. Προς τούτο, αρχικά παρουσιάζονται οι βασικές έννοιες κρυπτογραφίας που αξιοποιούνται για τη διασφάλιση της εμπιστοσύνης μεταξύ αλληλεπιδρώντων οντοτήτων και της εμπιστευτικότητας των επικοινωνιών. Στη συνέχεια μελετούνται τα χαρακτηριστικά των μοντέλων ελέγχου πρόσβασης που εν πολλοίς αποτελούν τον πυρήνα της επιχειρηματικής λογικής των πλαισίων διαχείρισης εξουσιοδοτήσεων. Το κεφάλαιο καταλήγει με την ανάλυση των προτεινόμενων ολοκληρωτικών μηχανισμών πλαισίων διαχείρισης εξουσιοδοτήσεων και των κύριων γνωρισμάτων τους.

Το τέταρτο κεφάλαιο αποτελεί ουσιαστικά την εννοιολογική θεμελίωση της προτεινόμενης λύσης. Έτσι, αφού πραγματοποιηθεί μια συνοπτική καταγραφή των στόχων της προτεινόμενης λύσης, το κεφάλαιο προχωρά με την περιγραφή των

[1] Ο όρος κλιμακοθετησιμότητα αποτελεί μετάφραση του αγγλικού όρου scalability, σύμφωνα με την Ελληνική Εταιρεία Ορολογίας (ΕΛΕΤΟ).

αρχών σχεδίασης που διέπουν την προβλεπόμενη υποδομή και των λειτουργικών απαιτήσεων των σχετικών συστημάτων. Στη συνέχεια, παρουσιάζεται η κατανεμημένη αρχιτεκτονική της πλατφόρμας, ενώ ιδιαίτερη έμφαση δίνεται στο υιοθετημένο μοντέλο εμπιστοσύνης. Ακολούθως, πραγματοποιείται η προδιαγραφή του μοντέλου πληροφοριών που συνιστά το κύριο εργαλείο υποστήριξης της λειτουργίας της πλατφόρμας και της διεξαγωγής των συναλλαγών μεταξύ των διακριτών υποσυστημάτων της. Τέλος, το κεφάλαιο παρουσιάζει τη μοντελοποίηση του προβλήματος παραγωγής εξουσιοδοτήσεων, υπό το πρίσμα μιας μηχανής παραγωγής σχετικών αποφάσεων και στη βάση των προδιαγραφέντων μοντέλων πληροφοριών και εμπιστοσύνης.

Εν συνεχεία, στο πέμπτο κεφάλαιο επιχειρείται η συγκεκριμενοποίηση των τεχνολογικών μέσων και ενεργειών που πραγματοποιήθηκαν στο πλαίσιο της εκπόνησης της διατριβής για την ανάπτυξη των βασικών δομικών συστατικών του συστήματος. Σε αυτό το πλαίσιο, αρχικά αναλύονται οι σχεδιαστικές λεπτομέρειες της Οντολογίας Εξουσιοδοτήσεων, που υιοθετήθηκε για τη σημασιολογική αποτύπωση του μοντέλου πληροφοριών. Έπειτα, παρουσιάζεται ο τρόπος αξιοποίησης των βασικών εννοιών της Οντολογίας για την οργανωμένη παραγωγή συμπερασμάτων από τις προτιμήσεις ιδιωτικότητας και εμπιστευτικότητας των οντοτήτων και εντέλει οριστικών αποφάσεων εξουσιοδότησης. Το κεφάλαιο καταλήγει με την περιγραφή της αναπαράστασης καίριων καταστάσεων του συστήματος με τη μορφή ψηφιακών πιστοποιητικών.

Το έκτο κεφάλαιο πραγματεύεται το πρωτόκολλο εξουσιοδότησης, την αλληλουχία δηλαδή των μηνυμάτων που ανταλλάσουν οι οντότητες και τα συστήματα της πλατφόρμας κατά τη διάρκεια της λειτουργίας της. Σε αυτό το πλαίσιο, διακρίνονται δύο βασικές φάσεις του πρωτοκόλλου: η φάση της διαμόρφωσης της υποδομής που περιλαμβάνει όλες εκείνες τις προκαταρκτικές ενέργειες που προετοιμάζουν τη λειτουργία της πλατφόρμας και τη φάση εκτέλεσης του πρωτοκόλλου, που εμπεριέχει τις ενέργειες ελεγχόμενου διαμοιρασμού πληροφοριών μέσω της εφαρμογής των κατάλληλων εξουσιοδοτήσεων. Πέραν της παρουσίασης των διακριτών βημάτων του πρωτοκόλλου, το κεφάλαιο περιγράφει επιπρόσθετα την επιλογή συγκεκριμένων τεχνολογικών μεθόδων για την κωδικοποίηση των μηνυμάτων.

Το έβδομο κεφάλαιο παρουσιάζει τις δραστηριότητες ανάπτυξης των διακριτών μονάδων της πλατφόρμας για την κατάλληλη ενσωμάτωση των λειτουργιών που παρουσιάστηκαν στα προηγούμενα κεφάλαια σε ένα ολοκληρωμένο σύστημα

διαχείρισης εξουσιοδοτήσεων. Πιο συγκεκριμένα, αναλύονται η εσωτερική αρχιτεκτονική και τα λειτουργικά χαρακτηριστικά των μονάδων των Κέντρων Διαχείρισης Εξουσιοδοτήσεων και του Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας, που αποτελούν και τα βασικά δομικά συστατικά της προτεινόμενης πλατφόρμας.

Το όγδοο κεφάλαιο παρουσιάζει την αξιοποίησή της πλατφόρμας σε ένα ρεαλιστικό σενάριο ροής δεδομένων μεταξύ απομακρυσμένων εταίρων σε επιχειρηματικό περιβάλλον, προκειμένου να γίνει κατανοητή η λειτουργία των συστημάτων αλλά και για να αποσαφηνιστούν οι λεπτομέρειες του πρωτοκόλλου εξουσιοδότησης.

Τέλος, το ένατο Κεφάλαιο αποτελεί τον επίλογο της διατριβής, όπου συνοψίζεται η προτεινόμενη λύση και παρουσιάζονται τα βασικά συμπεράσματα,. Επιπρόσθετα, σκιαγραφούνται οι βασικές κατευθύνσεις που θα αποτελέσουν τους άξονες της επέκτασης της έρευνας έχοντας ως αφετηρία τη λύση που προτείνεται από τη διατριβή.

2 Σχετικό Υπόβαθρο

Η ευαισθητοποίηση του κοινού σχετικά με την προστασία προσωπικών δεδομένων έχει άμεση επίδραση στη στάση και συμπεριφορά τους όταν εμπλέκονται σε διαδικτυακές εμπορικές συναλλαγές [18] και επομένως προσδίδει κίνητρο σε οργανισμούς και επιχειρήσεις να επενδύουν σημαντικά τόσο σε χρόνο όσο και σε κόστος για την υιοθέτηση των κατάλληλων επιχειρηματικών μοντέλων και μηχανισμών ασφάλειας. Εκ των πραγμάτων, παράλληλα με την εμπιστευτικότητα οι μηχανισμοί ασφάλειας και ιδιωτικότητας αποδίδουν σημαντικά εμπορικά οφέλη στους σύγχρονους παρόχους υπηρεσιών στο Διαδίκτυο και κέρδη που ενισχύονται από το γεγονός ότι η ιδιωτικότητα αυξανόμενα αποτελεί αντικείμενο νομοθετικών κειμένων σε εθνικό αλλά και διεθνές επίπεδο. Επιπλέον, ο σημαντικός αριθμός από πρότυπα ασφάλειας για πληροφοριακά συστήματα που έχουν προκύψει τα τελευταία χρόνια κινητοποιούν περαιτέρω τους παρόχους σχετικά με την εμπιστευτικότητα και τους κίνδυνους που μπορεί να ανακύψουν από ενδεχόμενα κενά ασφάλειας ή καταπάτηση ιδιωτικότητας των χρηστών. Στην πραγματικότητα, η νομοθεσία και τα διεθνή πρότυπα ασφάλειας παρέχουν τα μέσα για την αποδοτική ενορχήστρωση τυπικών μηχανισμών προστασίας και την ενσωμάτωσή τους σε ένα ολιστικό πλαίσιο εμπιστευτικότητας στις ψηφιακές διαδικασίες. Έτσι η συμβατότητα με τη νομοθεσία και τα σχετικά πρότυπα ασφάλειας αποκτά γραμμική σχέση με τη διαμόρφωση των λειτουργικών και μη λειτουργικών χαρακτηριστικών των σύγχρονων αναπτυσσόμενων λύσεων ιδιωτικότητας και ασφάλειας.

2.1 Ιδιωτικότητα

Αντικείμενο της παρούσας ενότητας είναι η μελέτη της έννοιας της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων όπως αυτή συναντάται σε διεθνείς συμβάσεις και νόμους. Απώτερος στόχος της ανάλυσης που ακολουθεί είναι η ανάδειξη των γνωρισμάτων της ιδιωτικότητας και των αρχών εκείνων που πρέπει να διέπουν τους αντίστοιχους μηχανισμούς προστασίας.

2.1.1 Ιδιωτικότητα ως Δικαίωμα

Όπως προαναφέρθηκε, η ιδιωτικότητα έχει αναγνωριστεί διεθνώς ως θεμελιώδες ανθρώπινο δικαίωμα από την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου η οποία υιοθετήθηκε το 1948 από τη Γενική Συνέλευση του Ο.Η.Ε. Πιο συγκεκριμένα στο άρθρο 12 αναφέρεται ότι «*κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του*». Το άρθρο καταλήγει τονίζοντας την αναγκαιότητα θέσπισης των σχετικών νόμων προστασίας αναφέροντας ότι «*καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους*». Ταυτόχρονα η ιδιωτικότητα προστατεύεται ως αγαθό σε μια σειρά από σημαίνουσες συνθήκες για τα ανθρώπινα δικαιώματα ανά τον κόσμο με σπουδαιότερες όλων την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (European Convention on Human Rights) [19] και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (International Covenant on Civil and Political Rights) [20].

Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου και των Θεμελιωδών Ελευθεριών συντάχθηκε στις τάξεις του Συμβουλίου της Ευρώπης το 1950 με σκοπό την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών του ατόμου. Στο άρθρο 8 της σύμβασης αναφέρεται ότι κάθε πρόσωπο δικαιούται σεβασμό της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας του και της αλληλογραφίας του. Το άρθρο συμπληρώνει ότι δεν επιτρέπεται η επέμβαση δημοσίας αρχής κατά την άσκηση του παραπάνω δικαιώματος, εκτός εάν η επέμβαση αύτη προβλέπεται από τον νόμο και αποτελεί μέτρο το οποίο, στα πλαίσια μιας δημοκρατικής κοινωνίας, κρίνεται αναγκαίο για την εθνική και δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και άλλων ελευθεριών.

Το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα αποτελεί μια πολυμερή συμφωνία μεταξύ των μελών της Γενικής Συνέλευσης του Ο.Η.Ε που υιοθετήθηκε το 1966 και βρίσκεται σε ισχύ από το 1976. Το σύμφωνο επιβάλει στα υπογράφοντα μέλη τον σεβασμό των ατομικών και πολιτικών δικαιωμάτων των πολιτών ενώ μαζί με την Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα και το Διεθνές Σύμφωνο για τα Οικονομικά, Κοινωνικά και Πολιτιστικά/Μορφωτικά

Δικαιώματα (International Covenant on Economic, Social and Cultural Rights) συναπαρτίζουν τον Διεθνή Χάρτη των Ανθρωπίνων Δικαιωμάτων (International Bill of Human Rights). Το άρθρο 17 του συμφώνου αποτελεί ουσιαστικά μια αναδιατύπωση του άρθρου 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου περί σεβασμού της ιδιωτικής ζωής του ατόμου και της προστασίας του από τον νόμο.

2.1.2 Ιδιωτικότητα και Νομοθεσία

Στα πληροφοριακά συστήματα η ιδιωτικότητα παρουσιάζει άρρηκτους δεσμούς με την προστασία προσωπικών και ευαίσθητων δεδομένων. Υπό τη μορφή της πληροφοριακής ιδιωτικότητας, το δικαίωμα στην ιδιωτικότητα έχει καταγραφεί σε μια σειρά από εθνικά συντάγματα παγκοσμίως. Στην Ελλάδα το δικαίωμα στην προστασία προσωπικών δεδομένων και στο απόρρητο των επικοινωνιών κατοχυρώνεται συνταγματικά. Πιο συγκεκριμένα, το Άρθρο 9Α του Συντάγματος της Ελλάδας [21] αναφέρει ότι «*καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων*», ενώ προβλέπει ότι η προστασία των προσωπικών δεδομένων διασφαλίζεται από κάποια ανεξάρτητη Αρχή. Επιπλέον, το Άρθρο 19 ορίζει ως απόλυτα απαραβίαστο το απόρρητο των επικοινωνιών, προβλέποντας ωστόσο το νομοθετικό ορισμό εγγυήσεων υπό τις οποίες η δικαστική Αρχή δε δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Προβλέπει επίσης το νομοθετικό ορισμό των σχετικών με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης Αρχής που διασφαλίζει το απόρρητο.

Υπό τη μορφή της προστασίας προσωπικών και ευαίσθητων δεδομένων το δικαίωμα στην πληροφοριακή ιδιωτικότητα στην Ελλάδα συναντάται ως επί το πλείστον στους Νόμους 2472/1997 [22], 3471/2006 [23] και 3917/2011 [24]. Ο Νόμος 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματεύεται τη «*θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής*» και αποτελεί υλοποίηση της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ [25] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Αντίστοιχα, ο Νόμος 3471/2006 περί προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των

ηλεκτρονικών επικοινωνιών στόχο έχει αφενός την «*προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών*» και αφετέρου την τροποποίηση του Νόμου 2472/1997. Ο Νόμος 3471/2006 αποτελεί υλοποίηση της Οδηγίας 2002/58/ΕΚ [26] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Τέλος, ο πρόσφατος Νόμος 3917/2011 σχετικά με τη «*διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις*» αντικατοπτρίζει την Ευρωπαϊκή Οδηγία 2006/24/ΕΚ [27] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Πρέπει να σημειωθεί ότι από σχετικές διατάξεις Νόμων του Ελληνικού Συντάγματος προέκυψαν και δύο αρμόδιες ανεξάρτητες Αρχές, οι οποίες υλοποιούν, αντίστοιχα, τα Άρθρα 9Α και 19 του Συντάγματος: η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) [28], η οποία ιδρύθηκε με το Νόμο 2472/1997, και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) [29], η οποία συστάθηκε με το Νόμο 3115/2003 [30]. Τέλος, καθώς τα σχετικά νομοσχέδια βασίζονται στο δικαίωμα στην πληροφοριακή ιδιωτικότητα ο ορισμός των προσωπικών και ευαίσθητων δεδομένων που αποτελούν αντικείμενο προστασίας αποκτά βαρύνουσα σημασία.

Σύμφωνα με το άρθρο 2α του Νόμου 2472/97 ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοείται «*κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων*». Το άρθρο 2γ του ίδιου Νόμου ορίζει ως **υποκείμενο των δεδομένων** «*το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική*». Το άρθρο 2α καταλήγει εξαιρώντας από τον ορισμό των δεδομένων προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Ως ευαίσθητα προσδιορίζονται σαφώς στο άρθρο 2β του ίδιου Νόμου τα δεδομένα «*τα δεδομένα που αφορούν στη φυλετική ή εθνική*

προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων».

Σε αυτό το σημείο κρίνεται σκόπιμη η παράθεση των Κατευθυντήριων Οδηγιών για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) [31], οι οποίες αποτέλεσαν ορόσημο στο θέμα της προστασίας των προσωπικών δεδομένων τουλάχιστον στον ευρωπαϊκό χώρο. Το 1980, σε μια προσπάθεια δημιουργίας ενός σαφούς πλαισίου προστασίας δεδομένων στην Ευρώπη, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development – OECD) [32] συνέταξε τις Κατευθυντήριες Οδηγίες υπό τη μορφή υποδείξεων για τη διαμόρφωση και ενεργοποίηση των κατάλληλων νομοθετημάτων για την προστασία των προσωπικών δεδομένων. Οι Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ και συνεπακόλουθα οι αντίστοιχες εθνικές ενσωματώσεις αποτελούν υλοποιήσεις των οδηγιών του OECD. Συνοπτικά, οι αρχές που διέπουν τις Οδηγίες του OECD είναι οι ακόλουθες:

- **Αρχή της περιορισμένης συλλογής**: Η συλλογή προσωπικών δεδομένων πρέπει να υπόκειται σε περιορισμούς με σύννομα και δίκαια μέσα και όταν είναι απαραίτητο μετά τη συγκατάθεση του υποκειμένου των δεδομένων.
- **Αρχή της ποιότητας των δεδομένων**: Τα προσωπικά δεδομένα πρέπει να σχετίζονται με τον σκοπό χρησιμοποίησής τους ενώ στα πλαίσια αυτού του σκοπού πρέπει να είναι ακριβή, πλήρη και ενημερωμένα.
- **Αρχή του καθορισμού του σκοπού**: Οι σκοποί συλλογής των προσωπικών δεδομένων πρέπει να καθορίζονται όχι αργότερα από τη στιγμή συλλογής τους ενώ η μετέπειτα χρήση τους πρέπει να περιορίζεται στα πλαίσια της επίτευξης των καθορισμένων σκοπών η άλλων σχετικών στόχων οι οποίοι είναι συμβατοί με τους δηλωμένους.
- **Αρχή του περιορισμού της χρήσης**: Τα προσωπικά δεδομένα δεν πρέπει να αποκαλύπτονται, να γίνονται διαθέσιμα ή να χρησιμοποιούνται με οποιονδήποτε τρόπο προς επίτευξη σκοπού διαφορετικού από τους καθορισμένους σύμφωνα με την «Αρχή του καθορισμού του σκοπού», εκτός

εάν υπάρχει συγκατάθεση του υποκειμένου των δεδομένων ή η σχετικές ενέργειες επιβάλλονται από τον Νόμο.

- **Αρχή των εγγυήσεων ασφάλειας**: Τα προσωπικά δεδομένα πρέπει να προστατεύονται από επαρκείς εγγυήσεις ασφάλειας έναντι κινδύνων όπως απώλεια ή μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, αλλοίωση ή αποκάλυψη των δεδομένων.
- **Αρχή της διαφάνειας**: Υλοποιήσεις, πρακτικές και πολιτικές αναφορικά με προσωπικά δεδομένα πρέπει να διέπονται από την αρχή της διαφάνειας. Θα πρέπει να διατίθενται μηχανισμοί εξακρίβωσης της ύπαρξης και της φύσης των προσωπικών δεδομένων, των κύριων σκοπών χρήσης τους καθώς και της ταυτότητας και συνήθους κατοικίας του υπεύθυνου της επεξεργασίας τους.
- **Αρχή της ατομικής συμμετοχής**: Καθένας έχει το δικαίωμα
    - να ενημερώνεται από τον υπεύθυνο επεξεργασίας σχετικά με το αν βρίσκονται στην κατοχή του δεδομένα που τον αφορούν,
    - να λαμβάνει τα δεδομένα αυτά μέσα σε ένα εύλογο χρονικό διάστημα, με όχι υπερβολικά μεγάλο κόστος, με λογικά μέσα και σε κατανοητή μορφή,
    - να του αιτιολογείται πιθανή άρνηση άσκησης των παραπάνω δικαιωμάτων και να δύναται να προσβάλει αυτή την άρνηση και
    - να προσβάλει την ακρίβεια των δεδομένων και να διατηρεί το δικαίωμα διαγραφής, επανόρθωσης, τροποποίησης και ολοκλήρωσής τους.
- **Αρχή της ευθύνης**: Ο υπεύθυνος της επεξεργασίας πρέπει να είναι υπεύθυνος για τη υιοθέτηση μέτρων που τον καθιστούν συμβατό με τις παραπάνω αρχές.

Πρέπει να σημειωθεί ότι σε αντίθεση με την Ευρωπαϊκή Ένωση, οι Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) έχουν διατηρήσει μια λιγότερο ολιστική και διεπιστημονική προσέγγιση στο θέμα της νομοθεσίας περί ιδιωτικότητας, ενεργοποιώντας διαφορετικούς νόμους για διαφορετικά περιβάλλοντα ([33]). Ταυτόχρονα, ενώ η πλειοψηφία των ομοσπονδιακών νόμων για το προσωπικό απόρρητο βρίσκουν εφαρμογή κυρίως στους κυβερνητικούς φορείς ρυθμίζονται επιλεκτικά συγκεκριμένες περιοχές του ιδιωτικού τομέα επιτρέποντας με αυτόν τον τρόπο μια λιγότερο αυστηρή συγκριτικά με την Ε.Ε. προσέγγιση στο θέμα της προστασίας προσωπικών δεδομένων, ενώ χαρακτηριστική είναι η απουσία

συγκεκριμένης σχετικής πρόβλεψης στο αμερικάνικο σύνταγμα [34]. Σημαντική στιγμή αναφορικά με την προστασία της ιδιωτικότητας στις ΗΠΑ θεωρείται η θεσμοθέτηση της «Δράσης για την Ιδιωτικότητα» (Privacy Act) το 1974 [35]. Η «Δράση για την Ιδιωτικότητα» προδιέγραψε τις αρχές που πρέπει να διέπουν τη συλλογή, διατήρηση, χρήση και διακίνηση προσωπικών στοιχείων (Personally Identifiable Information) που βρίσκονται αποθηκευμένα σε αρχεία ομοσπονδιακών φορέων. Έκτοτε, μια σειρά από Νόμους με περιορισμένη και επιλεκτική εφαρμογή έχουν υιοθετηθεί προς ρύθμιση της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων σε μια σειρά από συγκεκριμένους τομείς ([36]).

2.2 Ιδιωτικότητα και Ασφάλεια Πληροφοριών

Ταυτόχρονα με τον ραγδαία αυξανόμενο ρυθμό των εξελίξεων στις ΤΠΕ, ενισχύονται ολοένα και περισσότερο τα χαρακτηριστικά της πολυπλοκότητας, διασποράς και ανομοιογένειας των σύγχρονων δικτυακών πληροφοριακών συστημάτων. Σε αυτό το περιβάλλον η ιδιωτικότητα και δη η εφαρμογή των διατάξεων περί προστασίας προσωπικών δεδομένων που συναντούνται σε νομοθετήματα σε εθνικό και παγκόσμιο επίπεδο είναι δύσκολο έως αδύνατο να ελεγχθεί και να επιβληθεί στις ηλεκτρονικές συναλλαγές χωρίς την αξιοποίηση επαρκών μηχανισμών ασφάλειας. Προς αυτή την κατεύθυνση, στον σύγχρονο ψηφιακό κόσμο σχεδιάζονται και υλοποιούνται συγκεκριμένοι μηχανισμοί ασφάλειας και μοντέλα επικοινωνίας που δίνουν ώθηση στην τήρηση της ιδιωτικότητας. Καθώς η ασφάλεια των πληροφοριακών συστημάτων αποτελεί ένα σύνθετο κοινωνικό και τεχνικό ζήτημα με πολλά εννοιολογικά παρακλάδια, τονίζεται ότι στόχος της ενότητας είναι η μελέτη της έννοιας «ασφάλεια πληροφορίας» υπό το πρίσμα της διασφάλισης της ιδιωτικότητας στις ηλεκτρονικές συναλλαγές και πιο συγκεκριμένα της προστασίας της πληροφορίας αυτής καθαυτής.

2.2.1 Ασφάλεια Πληροφοριών

Η αβεβαιότητα και ανασφάλεια των δικτυακών συναλλαγών και οι σοβαροί κίνδυνοι που αυτές εγείρουν έχουν ανάγει τη διαχείριση της ασφάλειας των επικοινωνιών και των εμπλεκόμενων πληροφοριών από προστιθέμενη αξία σε αναγκαιότητα για τους παρόχους υπηρεσιών. Φυσικά το ζήτημα της ασφάλειας των πληροφοριών δεν αποτελεί αποκλειστικά σύγχρονο πρόβλημα. Υφίσταται ιστορικά από την πρώτη

στιγμή που κάποια πληροφορία αποτιμήθηκε ως έχουσα κάποιο κόστος ή θεωρήθηκε άξια προστασίας. Ανεξάρτητα από την πηγή και το βάρος της σχετικής αξιολόγησης η διαδικασία αποτίμησης της σημασίας της πληροφορίας εισήγαγε την ανάγκη διατήρησης της εμπιστευτικότητάς της ως ολότητα αλλά και προστασίας των επιμέρους δεδομένων που την απαρτίζουν. Σταδιακά οι ραγδαίες αλλαγές στις τεχνολογίες πληροφορικής και υπολογιστικής καθώς και η τεράστια εμπορευματοποίηση των πληροφοριών των ημερών μας επέδρασαν σημαντικά στη διαμόρφωση του όρου ασφάλεια της πληροφορίας. Βέβαια, όπως και στην περίπτωση της ιδιωτικότητας η εξαγωγή ενός σαφούς, πλήρους και κοινά αποδεκτού ορισμού για την ασφάλεια των πληροφοριών δεν αποτελεί απλή διαδικασία. Είθισται μάλιστα η ασφάλεια να περιγράφεται μέσω κάποιων χαρακτηριστικών γνωρισμάτων των οποίων η παρουσία ή απουσία καθορίζει την επίτευξη ασφάλειας ή μη. Σε αυτό το πνεύμα, η ασφάλεια της πληροφορίας βασίζεται στους εξής βασικούς αξιακούς πυλώνες:

- **Ακεραιότητα (integrity)**: Η διατήρηση των δεδομένων σε προκαθορισμένο χώρο και σε συγκεκριμένη κατάσταση. Κάθε μη εξουσιοδοτημένη ενέργεια πρέπει να αποτρέπεται καθώς και κάθε διενέργεια τροποποιήσεων στο περιεχόμενο της προστατευόμενης πληροφορίας πρέπει να υπόκειται σε έλεγχο πρόσβασης.
- **Εμπιστευτικότητα (confidentiality)**: Η ιδιότητα των πληροφοριών να υφίστανται σε κατανοητή, λογική και αναγνώσιμη μορφή μόνο σε εξουσιοδοτημένες προς τούτο οντότητες.
- **Διαθεσιμότητα (availability)**: Η αποτροπή της άρνησης διάθεσης της πληροφορίας σε κάθε εξουσιοδοτημένη οντότητα τη στιγμή της ζήτησής της. Πρέπει να εξασφαλίζεται η συνεχής και εύρυθμη λειτουργία των υπολογιστικών συστημάτων επεξεργασίας και αποθήκευσης της πληροφορίας καθώς και των μηχανισμών ασφάλειας που αξιοποιούνται για την προστασία της και των καναλιών επικοινωνίας που χρησιμοποιούνται για τη διάδοσή της.

Παρόλο που στην ερευνητική κοινότητα οι παραπάνω αρχές αποτελούν σχεδόν ομόφωνα τον πυρήνα της ασφάλειας της πληροφορίας, δεν υπάρχει η αντίστοιχη ομοφωνία σχετικά με την επάρκειά τους για να οριστεί πλήρως η έννοια. Έτσι, στη βιβλιογραφία συναντώνται πρόσθετες ιδιότητες όπως:

- **Αυθεντικότητα (authenticity)**: Η ιδιότητα της γνησιότητας των δεδομένων καθώς και η εξακρίβωση της προέλευσης, του ιδιοκτήτη και του παραλήπτη της πληροφορίας.
- **Μη αποποίηση (non-repudiation)**: Η αποτροπή άρνησης επιτέλεσης ενεργειών επί της πληροφορίας από την υπεύθυνη για τις ενέργειες οντότητα.
- **Εγκυρότητα (validity)**: Η εξακρίβωση της επικαιρότητας και της ακρίβειας των δεδομένων.
- **Μοναδικότητα (uniqueness)**: Η αδυναμία αντιγραφής ή αναπαραγωγής της πληροφορίας από μη εξουσιοδοτημένες προς τούτο οντότητες.
- **Δυνατότητα ελέγχου και απολογισμού (auditability)**: Η δυνατότητα διευκρίνισης της πορείας της επεξεργασίας των δεδομένων και εξακρίβωσης της ορθότητάς της.
- **Υπευθυνότητα (accountability)**: Κάθε οντότητα που εμπλέκεται σε διαδικασίες αποστολής, λήψης ή τροποποίησης των δεδομένων είναι υπεύθυνη για τις σχετικές ενέργειες.

Στην πράξη οι παραπάνω ιδιότητες χρησιμοποιούνται κοινά στην προσπάθεια επίτευξης ασφάλειας καθώς καθορίζουν συγγενή και αλληλεπιδρώντα γνωρίσματα.

2.2.2 Πρότυπα Ασφάλειας

Οι παραπάνω περιγραφόμενες ιδιότητες της ασφάλειας οδηγούν σε μια περισσότερο ποιοτική παρά ποσοτική αποτίμηση της έννοιας. Ωστόσο, η νομοθεσία σε ευρωπαϊκό και εθνικό επίπεδο αντιμετωπίζει την ασφάλεια πληροφοριών ως μέγεθος σχετικό και όχι απόλυτο. Έτσι, στις διατάξεις των σχετικών νόμων και κοινοτικών οδηγιών αποφεύγεται ο σαφής καθορισμός μεθοδολογιών, μοντέλων και τεχνικών μέσων καθώς και οποιασδήποτε μορφής υπόδειξη προς αξιοποίηση συγκεκριμένων τεχνολογιών. Χαρακτηριστικά είναι τα ακόλουθα αποσπάσματα από την Κοινοτική Οδηγία 95/46/ΕΚ. Συγκεκριμένα, το άρθρο 17, περί ασφάλειας της επεξεργασίας δεδομένων, της οδηγίας αναφέρει ότι «*ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα* ***κατάλληλα*** *τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση*». Στη συνέχεια το άρθρο προχωρά σε μια οριοθέτηση των τεχνικών και οργανωτικών μέτρων αναφέροντας ότι «*τα μέτρα αυτά πρέπει να εξασφαλίζουν, λαμβανομένης υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους,*

επίπεδο ασφαλείας ανάλογο προς τους κινδύνους *που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας*». Μάλιστα, στο αντίστοιχο ελληνικό εδάφιο του Νόμου 2472/97 υποδεικνύεται η ΑΠΔΠΧ και η ΑΔΑΕ ως υπεύθυνοι φορείς για τον καθορισμό της επάρκειας τεχνολογικών μέσων ασφάλειας: «*η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας*».

Η αναγκαιότητα εμπεριστατωμένου ελέγχου του επιπέδου της ασφάλειας καθώς και η ανάγκη καταγεγραμμένης κοινής ορολογίας και συναίνεσης αναφορικά με τις προδιαγραφές ασφάλειας έδωσε το έναυσμα για την έκδοση πλήθους διεθνών προτύπων ασφάλειας. Τα διεθνή πρότυπα ασφάλειας δίνουν τη δυνατότητα σε οργανισμούς και επιχειρήσεις να επιτυγχάνουν ένα επιθυμητό ελάχιστο επίπεδο ασφάλειας, να ελαχιστοποιούν τους κίνδυνους από επιθέσεις κατά της ασφάλειας των πληροφοριών και των πληροφοριακών συστημάτων και να μεγιστοποιούν το επίπεδο διαλειτουργικότητάς τους. Σε αρκετές περιπτώσεις η συμμόρφωση με τους υποδειχθέντες κανόνες εξασφαλίζει μια μορφή πιστοποίησης από διαπιστευμένους φορείς, η οποία και μπορεί να αποτελέσει σημείο αναφοράς στους οργανισμούς για την ανάπτυξη σχέσεων εμπιστοσύνης με τους εκάστοτε συνεργάτες τους. Η βαρύνουσα σημασία των προτύπων ασφάλειας είναι ακόμα μεγαλύτερη στις μέρες μας καθώς η ασφάλεια έχει αναδειχθεί σε μείζον ζήτημα γα την Ευρωπαϊκή Ένωση και τους φορείς της. Ειδικότερα, η απόκτηση και διατήρηση **εμπιστοσύνης** και **ασφάλειας** στις ψηφιακές αγορές έχουν αναγνωριστεί ως ένας από τους βασικούς πυλώνες του ψηφιακού θεματολογίου για την Ευρώπη (Digital Agenda for Europe) ([37]). Το ψηφιακό θεματολόγιο για την Ευρώπη αποτελεί μία από τις επτά εμβληματικές πρωτοβουλίες της στρατηγικής *Ευρώπη 2020* ([38]), για την ανάδειξη του καταλυτικού ρόλου που πρέπει να αναλάβουν οι ΤΠΕ, στην προσπάθεια επίτευξης των φιλόδοξων στόχων το 2020 σε ευρωπαϊκό επίπεδο. Στα πλαίσια της ίδιας στρατηγικής η Ευρωπαϊκή Επιτροπή αποφάσισε να υποβάλει μέτρα προς ενίσχυση και εκσυγχρονισμό του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (European Network and Information Security Agency – ENISA) [39], ενός οργανισμού που συστάθηκε το 2004 για να διαδραματίσει συμβουλευτικό και συντονιστικό ρόλο προς την Επιτροπή και τα μέλη της

Ευρωπαϊκής Ένωσης σχετικά με τα μέτρα ασφάλειας των πληροφοριακών τους συστημάτων που λαμβάνουν. Σε αυτό το κλίμα, οργανισμοί και επιχειρήσεις σε διεθνές επίπεδο προωθούν λύσεις και πρακτικές ασφάλειας που αποσκοπούν στην εξασφάλιση συμβατότητας – και συνεπακόλουθα της αντίστοιχης πιστοποίησης – με τις οδηγίες αναγνωρισμένων προτύπων ασφάλειας.

Μεταξύ των διεθνών οργανισμών έκδοσης προτύπων εξέχουσα θέση κατέχει ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization – ISO) [40]. Ο Διεθνής Οργανισμός Τυποποίησης συνιστά κοινοπραξία μεταξύ αντιπροσώπων των εθνικών οργανισμών τυποποίησης και αποτελεί τον πιο δημοφιλή οργανισμό δημιουργίας προτύπων σε παγκόσμιο επίπεδο. Τη δημοφιλία του αυτή την οφείλει στην υψηλή ποιότητα και μεγάλη απορροφητικότητα των προτύπων που παράγει (πρότυπα ISO), πρότυπα τα οποία αποτελούν συχνά αντικείμενο νομοθετημάτων σε εθνικό επίπεδο. Το 2005, ο ISO σε συνεργασία με τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission – IEC) [41], έναν ακόμη δημοφιλή οργανισμό τυποποίησης, εξέδωσε το διεθνές πρότυπο ISO/IEC 27001:2005 ([42]) με πλήρη τίτλο «*Τεχνολογία της πληροφορίας – Τεχνικές ασφάλειας – Συστήματα διαχείρισης ασφάλειας πληροφοριών – Προδιαγραφές*», καθορίζοντας τις προδιαγραφές των μηχανισμών ασφάλειας και ελέγχου για την προστασία των πληροφοριών εμπορικών επιχειρήσεων, κυβερνητικών οργανισμών και μη κερδοσκοπικών οργανώσεων. Στο ίδιο πνεύμα κυμάνθηκαν και οι ακόλουθες εκδόσεις περί διαχείρισης της ασφάλειας των πληροφοριών, αποτέλεσμα της συνεργασίας των δύο οργανισμών τυποποίησης, όπως τα πρότυπα ISO/IEC 27002:2005 ([43]) και ISO/IEC 27005:2011 ([44]). Το ISO/IEC 27002:2005 συνιστά έναν οδηγό σχεδίασης, υλοποίησης και διατήρησης μηχανισμών διαχείρισης ασφάλειας πληροφοριών εντός οργανισμών, ενώ το πρότυπο ISO/IEC 27005:2011 υποστηρίζει τις βασικές αρχές που προδιαγράφηκαν στο ISO/IEC 27001:2005 και προτείνει τρόπους ικανοποίησης των συγκεκριμένων προδιαγραφών από τη σκοπιά της διαχείρισης κινδύνου (risk management).

Αναγνωρίζοντας την αναγκαιότητα για την επίτευξη μιας κοινά αποδεκτής ορολογίας και για την καταγραφή των βασικών απαιτήσεων αναφορικά με την προστασία των πόρων των ΤΠΕ το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST) [45], μια μη κανονιστική αντιπροσωπεία ανάπτυξης προτύπων και οδηγιών του Τμήματος Εμπορίου των Η.Π.Α., εκδίδει ήδη από το 1995 τη σειρά Ειδικών Δημοσιεύσεων 800. Η εν λόγω σειρά αποτελεί μια

διαρκώς αναπτυσσόμενη αναφορά για τις ενέργειες του οργανισμού σχετικά με την παραγωγή οδηγιών και προτύπων για την ασφάλεια των πληροφοριακών συστημάτων. Ενδεικτικά αναφέρονται οι ακόλουθες σημαντικές δημοσιεύσεις του οργανισμού: η έκδοση SP 800-14 (*Generally Accepted Principles and Practices for Securing Information Technology Systems*) του 1996 [46], η έκδοση SP 800-122 (*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*) του 2010 [47] και η SP 800-144 (*Guidelines on Security and Privacy in Public Cloud Computing*) του 2011 [48].

Τέλος αξιοσημείωτη στον χώρο της παραγωγής προτύπων ασφάλειας είναι και η συνεισφορά του Ευρωπαϊκού Φόρουμ για την Ασφάλεια (Information Security Forum – ISF) [49]. Το ISF αποτελεί μια ανεξάρτητη και μη κερδοσκοπική σύμπραξη διεθνών οργανισμών που ιδρύθηκε το 1989 και στις μέρες μας κατέχει σημαντική θέση παγκοσμίως στον τομέα της ασφάλειας της πληροφορίας. Τα Πρότυπα Βέλτιστης Πρακτικής για την Ασφάλεια της Πληροφορίας (Standard of Good Practice for Information Security) [50] συνιστούν σημαίνουσες εκδόσεις της οργάνωσης και συναποτελούν έναν ενδελεχή οδηγό διαχείρισης της ασφάλειας των πληροφοριών και των κινδύνων που μπορεί να προκύψουν από ενδεχόμενα κενά, υπό το πρίσμα μιας επιχείρησης. Η πρόσφατη επικαιροποίηση του προτύπου το 2011 [51] είναι συμβατή με τις προδιαγραφές του ISO/IEC 27001:2005 ενώ ταυτόχρονα καλύπτει μεγαλύτερο εύρος εφαρμογών από το πρότυπο ISO/IEC 27001:2005.

2.3 Απαιτήσεις Ιδιωτικότητας και Ασφάλειας

Η καθιέρωση σχέσεων εμπιστοσύνης στις ηλεκτρονικές διαδικασίες αποτελεί τον απώτερο στόχο των νομοθετικών διατάξεων και των κανονιστικών και συμβουλευτικών εκδόσεων που έχουν προκύψει τα τελευταία χρόνια. Αφενός, οι αρχές της ιδιωτικότητας όπως αυτές εξάγονται μέσα από την ανάλυση των οδηγιών του ΟΑΣΑ και των σχετικών διατάξεων της Ε.Ε. αποσκοπούν στην προστασία του ατόμου ως χρήστη ψηφιακών υπηρεσιών. Αφετέρου, οι αρχές της ασφάλειας πληροφοριών συναγόμενες από δημοφιλή και διαπιστευμένα πρότυπα ασφάλειας εστιάζουν στα μέσα προστασίας των εμπλεκόμενων στις ηλεκτρονικές διαδικασίες και πιο συγκεκριμένα στοχεύουν στη διαφύλαξη του πλέον σημαντικού αγαθού της εποχής μας: την πληροφορία. Γίνεται σαφές ότι η πληροφοριακή ιδιωτικότητα και η ασφάλεια της πληροφορίας αποτελούν έννοιες αλληλένδετες, ενώ χαρακτηριστική

είναι η αναφορά της ασφάλειας στη νομοθεσία περί προστασίας των προσωπικών δεδομένων ως μέσο εξασφάλισης της ιδιωτικότητας και αντίστοιχα η ανάδειξη της ιδιωτικότητας ως λειτουργική απαίτηση των πληροφοριακών συστημάτων από διεθνή πρότυπα ασφάλειας.

Αναφορικά με την ιδιωτικότητα οι διατάξεις της ευρωπαϊκής και εθνικής νομοθεσίας μπορούν να συνοψιστούν στις εξής αρχές:

- Η συλλογή και επεξεργασία προσωπικών δεδομένων πρέπει να υπακούουν στις ισχύουσες νομοθετικές ρυθμίσεις.
- Ο σκοπός συλλογής και επεξεργασίας των δεδομένων πρέπει να καθορίζεται ρητά και να κοινοποιείται στο υποκείμενο των δεδομένων, ενώ η μετέπειτα χρήση τους πρέπει να περιορίζεται στα πλαίσια του σκοπού αυτού ή κάποιου άλλου συμβατού σκοπού.
- Τα απαιτούμενα δεδομένα για την εκπλήρωση του καθορισμένου σκοπού πρέπει να είναι τα απολύτως απαραίτητα και όχι υπέρμετρα. Επίσης, στα πλαίσια του υποκείμενου σκοπού, τα δεδομένα πρέπει να είναι ακριβή, πλήρη και ενημερωμένα.
- Τα δεδομένα πρέπει να διατηρούνται σε μορφή που ταυτοποιεί το υποκείμενο των δεδομένων μόνο για το χρονικό διάστημα που απαιτείται για την εκπλήρωση του καθορισμένου σκοπού. Μετά το πέρας του χρονικού διαστήματος αυτού, τα δεδομένα πρέπει να διαγράφονται ή να τίθενται σε μη ταυτοποιητική μορφή.
- Τα υποκείμενα των δεδομένων πρέπει να πληροφορούνται σχετικά με τη συλλογή και επεξεργασία των δεδομένων τους, τον σκοπό των σχετικών ενεργειών, να τους αναγνωρίζεται το δικαίωμα παροχής και άρσης της ρητής συγκατάθεσής τους και να δικαιούνται πρόσβασης στα δεδομένα.
- Αναγνωρίζεται η αναγκαιότητα λειτουργίας συμβουλευτικών και ρυθμιστικών τρίτων φορέων με τις αρμοδιότητες της εποπτείας και του ελέγχου της εφαρμογής των σχετικών διατάξεων (ΑΠΔΠΧ και ΑΔΑΕ για τον ελληνικό χώρο).
- Η διασύνδεση δεδομένων μπορεί να λάβει χώρα μόνο υπό συγκεκριμένους όρους και σε κάθε περίπτωση κατόπιν ενημέρωσης προς την αρμόδια Αρχή. Ορίζονται μάλιστα ειδικές διατάξεις για τη χρήση μοναδικών ταυτοποιητικών αναγνωριστικών.

- Η πρόσβαση στα δεδομένα πρέπει να υπόκειται σε έλεγχο πρόσβασης και να είναι αποτέλεσμα εξουσιοδότησης του υποκείμενου των δεδομένων και της αρμόδιας Αρχής.
- Πρέπει να παρέχονται εγγυήσεις ασφάλειας έναντι κινδύνων όπως απώλεια ή μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, αλλοίωση ή αποκάλυψη των δεδομένων, εξασφαλίζοντας επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων που απολαύουν προστασίας.

Αντίστοιχα, τα διεθνή πρότυπα ασφάλειας, εστιάζοντας σε διαφορετικά εννοιολογικά επίπεδά (τεχνικό, φυσικό, λειτουργικό και οργανωτικό), υπό το πρίσμα των τεχνολογικών αναφορών τους και σχετικά με την προστασία της πληροφορίας και ενίσχυση της ιδιωτικότητας στις ηλεκτρονικές συναλλαγές συγκλίνουν στις ακόλουθες αρχές ασφάλειας:

- Η αναγνώριση και διαβάθμιση της αξίας της πληροφορίας που υπόκειται προστασίας αποτελεί το πρώτο βήμα για τη σχεδίαση και υλοποίηση των κατάλληλων μηχανισμών ασφάλειας. Η ευαισθησία της πληροφορίας και το μέγεθος του κινδύνου που ανακύπτει από ενδεχόμενο απώλειας της εμπιστευτικότητάς της αποτελεί το κριτήριο αξιολόγησης.
- Σε αναλογία με τη διαπιστωμένη αξία της πληροφορίας θα πρέπει να καθορίζεται ρητά το περιβάλλον και οι συνθήκες χρήσης της πληροφορίας και των δεδομένων που τη συναποτελούν.
- Δεδομένα που χαρακτηρίζονται ως ευαίσθητα ή προσωπικού χαρακτήρα θα πρέπει να προστατεύονται κατά τη διάρκεια της συλλογής, της μετάδοσης, της επεξεργασίας και της αποθήκευσής τους. Σημειώνεται, ότι στα πλαίσια ενός οργανισμού ως **ευαίσθητα δεδομένα** δεν νοούνται αποκλειστικά ατομικά ή προσωπικά δεδομένα αλλά οποιαδήποτε πληροφορία που έχει αξιολογηθεί ως έχουσα **εμπορική, οργανωτική ή επιχειρηματική αξία**. Η προστασία έγκειται στη διασφάλιση της αυθεντικότητας, της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Επιβάλλεται η διατήρηση των δεδομένων σε μη ταυτοποιητική μορφή όπου αυτό είναι δυνατό.
- Η πρόσβαση στα δεδομένα πρέπει να είναι αποτέλεσμα επιτυχούς ελέγχου πρόσβασης και κατάλληλης εξουσιοδότησης. Ο έλεγχος πρόσβασης και οι

παραγόμενες εξουσιοδοτήσεις πρέπει να βασίζονται σε κανόνες που εφαρμόζουν τις αρχές:

- της ιδιωτικότητας, όπως αυτοί ορίστηκαν παραπάνω,
- της ελάχιστης πληροφορίας, της αποκάλυψης δηλαδή μόνο των δεδομένων που είναι απαραίτητοι για την εκπλήρωση ενός στόχου και μόνο αν υφίσταται οι αναγνωρισμένες ως απαιτούμενες συνθήκες χρήσης της πληροφορίας,
- του διαχωρισμού των καθηκόντων, την απαίτηση δηλαδή πολλαπλών εξουσιοδοτήσεων από διαφορετικές οντότητες για την εκπλήρωση ενός στόχου (*Separation of Duty*) και
- της ενεργοποίησης του χρήστη, της αναγνώρισης δηλαδή των δικαιωμάτων του χρήστη κατά την αξιοποίηση προσωπικών του δεδομένων και την παροχή των κατάλληλων μηχανισμών για την εφαρμογή τους.

- Η εφαρμογή μηχανισμών πιστοποίησης των χρηστών και ταυτοποίησης των χαρακτηριστικών τους θα πρέπει να προηγείται οποιασδήποτε αίτησης για πρόσβαση σε δεδομένα. Τα διαπιστωμένα χαρακτηριστικά των χρηστών και το επίπεδο βεβαιότητας (*Level of Assurance – LoA*) που σχετίζεται με τους μηχανισμούς πιστοποίησης μπορεί να αποτελέσει κριτήριο για τον έλεγχο πρόσβασης που ακολουθεί της αίτησης. Το επίπεδο βεβαιότητας προσδιορίζεται ως ο βαθμός της εμπιστοσύνης που μπορεί να αποδοθεί στις τακτικές πιστοποίησης οργανισμών. Για παράδειγμα, ένας οργανισμός που αξιοποιεί κωδικούς πρόσβασης ως μέσο ταυτοποίησης χρηστών υστερεί σε επίπεδο βεβαιότητας ενός οργανισμού που αξιοποιεί ψηφιακά πιστοποιητικά ταυτότητας για τον ίδιο σκοπό. Όπου αυτό δεν αντιτίθεται στην αρχή της ιδιωτικότητας πρέπει να αξιοποιούνται μοναδικά αναγνωριστικά στοιχεία για την τήρηση της αρχής της υπευθυνότητας.
- Επιβάλλεται η συμβατότητα των μέτρων ασφαλείας με το ισχύον νομικό και κανονιστικό πλαίσιο καθώς και η συμμόρφωσή τους με τις απαιτήσεις που πηγάζουν από συναπτόμενα συμβόλαια με αλληλεπιδρούσες οντότητες.
- Οι ανωτέρω αρχές πρέπει να βρίσκονται οργανωμένες σε πολιτικές ασφάλειας πληροφοριών. Η εφαρμοζόμενη πολιτική ασφάλειας πρέπει να αναφέρεται σε ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε

εμπλεκόμενου μέσα σε μία εταιρία ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του. Αναφορικά με προσωπικά ή ευαίσθητα δεδομένα, η πολιτική ασφάλειας θα πρέπει να καθορίζει σαφώς κανόνες πρόσβασης, περιορισμού διατήρησης, σχέδια ειδοποιήσεων και διαδραστικότητας με το υποκείμενο των δεδομένων καθώς και πολιτικές τήρησης των συνεπαγόμενων υποχρεώσεων.

- Η πολιτική ασφάλειας πρέπει να αποτελεί τη βάση για τον σχεδιασμό κάθε συστήματος εντός του οργανισμού. Οι εμπλεκόμενες οντότητες πρέπει να αντιμετωπίζουν εξωτερικά του οργανισμού συστήματα ως επισφαλή ενώ εντός του οργανισμού πρέπει να θεωρείται ασφαλής ο ελάχιστος δυνατός αριθμός οντοτήτων. Επιπλέον, η υλοποίηση των μέτρων ασφάλειας πρέπει να αποτρέπει την ύπαρξη μοναδικού σημείου σφάλματος και να αποσκοπεί στον φυσικό και λογικό κατακερματισμό των μηχανισμών και στη συνακόλουθη διασπορά κινδύνου.
- Προς διατήρηση επαρκούς επιπέδου διαθεσιμότητας των πληροφοριών συνίσταται η εκμετάλλευση πλάνων έκτακτης ανάγκης και η εφαρμογή μηχανισμών αποκατάστασης ζημιών για μετριασμό των επιπτώσεων πιθανών κενών ασφάλειας.
- Επιβάλλεται ο σχεδιασμός και η υλοποίηση μέτρων ελέγχου και παρακολούθησης των συστημάτων για την έγκαιρη αναγνώριση μη εξουσιοδοτημένων ενεργειών και για την υποστήριξη ενεργειών ελέγχου και αξιολόγησης των εμπλεκόμενων ροών δεδομένων.

Οι εξαγόμενες αρχές ιδιωτικότητας και ασφάλειας αποτελούν έναν ενδελεχή οδηγό σχεδίασης και υλοποίησης για πληροφοριακά συστήματα που διαχειρίζονται ευαίσθητα και προσωπικά δεδομένα και εμπλέκονται σε ηλεκτρονικές διαδικτυακές συναλλαγές. Είναι σαφές ότι η μεγάλη απορροφητικότητα των ΤΠΕ, η εισχώρηση των αντίστοιχων εφαρμογών σε ένα μεγάλο μέρος των εκφάνσεων της καθημερινότητας του ανθρώπου και η δομή των σύγχρονων μοντέλων επικοινωνίας έχουν συμβάλλει ουσιαστικά στη διαμόρφωση των συγκεκριμένων οδηγιών και στην αναβάθμισή τους από υπηρεσίες προστιθέμενης αξίας σε λειτουργικές και μη λειτουργικές απαιτήσεις και προϋποθέσεις των σύγχρονων πληροφοριακών συστημάτων. Πράγματι, τα εγγενή χαρακτηριστικά των σύγχρονων αποκεντρωμένων δικτύων, όπως αυτά περιγράφηκαν στην Ενότητα 1.2, ενισχύουν τα προβλήματα

ασφάλειας των πληροφοριών και ιδιωτικότητας των συμμετεχόντων, καθιστώντας την εφαρμογή λύσεων που ικανοποιούν τις παραπάνω αρχές επιβεβλημένη.

2.4 Αριθμητικά Στοιχεία και Εμπιστοσύνη στην Τεχνολογία

Τα υψηλά επίπεδα καινοτομίας, ευελιξίας και δυναμικής των ΤΠΕ και ο ηγετικός ρόλος που αυτές διαδραματίζουν στη διαμόρφωση των μοντέλων εργασίας και αλληλεπίδρασης έχουν αλλάξει ριζικά το τοπίο των ψηφιακών διαδικασιών. Χαρακτηριστικό είναι ότι ο τομέας των ΤΠΕ είναι άμεσα υπεύθυνος για το 5% του ευρωπαϊκού Ακαθάριστου Εγχώριου Προϊόντος και διατηρεί εμπορική αξία ύψους 660 δισεκατομμυρίων €, ενώ συνεισφέρει αρκετά πιο έντονα στη γενική αύξηση της παραγωγικότητας (20% άμεσα από τον χώρο των ΤΠΕ και 30% από επενδύσεις σε ΤΠΕ) ([37]). Την ίδια στιγμή, ενισχύεται σημαντικά ο κοινωνικός αντίκτυπος των ΤΠΕ, με περισσότερους από 250 εκατομμύρια καθημερινούς χρήστες του Διαδικτύου. Μια σχετική σύγκλιση με τα στατιστικά στοιχεία σε ευρωπαϊκό επίπεδο παρουσιάζεται και στην Ελλάδα με τους δείκτες ηλεκτρονικής επιχειρηματικότητας (e-Business) να βρίσκονται κοντά στον ευρωπαϊκό μέσο όρο [52].

Ταυτόχρονα με την υψηλή απορροφητικότητα των ΤΠΕ παρουσιάζεται κι σοβαρή έλλειψη εμπιστοσύνης εκ μέρους των χρηστών στον ευρωπαϊκό χώρο. Σχετική έρευνα το 2008 ([1]) περί των αντιλήψεων πολιτών αναφορικά με την προστασία των δεδομένων και πληροφοριών κατά τη διακίνησή τους στο Διαδίκτυο έδειξε ότι η μεγάλη πλειοψηφία των ερωτηθέντων (82%) θεωρεί μη επαρκή τα υποκείμενα μέτρα ασφάλειας με μόλις το 15% να εμπιστεύεται τις σχετικές διαδικασίες. Επίσης σύμφωνα με μια έρευνα της Eurostat [52], μέσα στο 2009 μία στις 20 επιχειρήσεις εντός των χωρών μέλη της Ε.Ε. έχει αναφέρει περιστατικά καταστροφής ή αλλοίωσης δεδομένων λόγω μόλυνσης των πληροφοριακών τους συστημάτων από κακόβουλο λογισμικό ή εξαιτίας μη εξουσιοδοτημένης πρόσβασης. Επιπρόσθετα, εφαρμογές που αποτελούν την αιχμή του δόρατος στο κλίμα της αυξανόμενης εκμετάλλευσης των ΤΠΕ εγείρουν ταυτόχρονα και τους μεγαλύτερους κινδύνους καταπάτησης της ιδιωτικότητας των χρηστών και της εμπιστευτικότητας των πληροφοριών. Χαρακτηριστικό παράδειγμα αποτελούν οι εφαρμογές κοινωνικής δικτύωσης που έχουν δεχθεί κατά καιρούς δριμεία κριτική για τις πρακτικές τους, ενώ σε πρόσφατες περιπτώσεις η κριτική αυτή έχει μετουσιωθεί σε μηνύσεις χρηστών αλλά και δικαστική έρευνα. Ενδεικτικά αναφέρεται η περίπτωση του, πλέον αποσυρμένου,

λογισμικού Beacon το οποίο απέστελλε δεδομένα από εξωτερικές διαδικτυακές τοποθεσίες στο δίκτυο κοινωνικής δικτύωσης Facebook, με τον στόχο της προσωποποιημένης και στοχευμένης διαφήμισης προϊόντων. Ενδεικτική είναι επίσης η υπόθεση μεταβολής τιμών της πολυεθνικής εταιρίας ηλεκτρονικού εμπορίου Amazon τον Σεπτέμβριο του 2000, όταν αποκαλύφθηκε ότι οι πρακτικές καθορισμού των τιμών προϊόντων της εταιρίας λάμβαναν υπόψη το περιεχόμενο του ιστορικού περιήγησης των χρηστών στο Διαδίκτυο. Μάλιστα, η εν λόγω αποκάλυψη είχε ως αποτέλεσμα την αποζημίωση από την εταιρία όλων των χρηστών που υπήρξαν θύματα διακρίσεων στις τιμές πώλησης προϊόντων. Ταυτόχρονα μια σειρά οργανισμών έχουν αντιμετωπίσει πρόστιμα λόγω παραβίασης των διαφημιζόμενων πολιτικών ιδιωτικότητας τους. Για παράδειγμα, η Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission – FTC) στις Η.Π.Α. γνωμάτευσε υπέρ της αλλαγής των πολιτικών ιδιωτικότητας της φαρμακευτικής εταιρίας Eli Lilly and Company, μετά τη διαρροή μηνύματος ηλεκτρονικού ταχυδρομείου όπου αποκαλύπτονταν πολίτες ως χρήστες συγκεκριμένων φαρμακευτικών προϊόντων. Στο ίδιο κλίμα, η πολυεθνική εταιρία λογισμικού Microsoft ανέπτυξε ένα προηγμένο πρόγραμμα ασφάλειας πληροφοριών, το οποίο υποχρεούται να υποβάλλει σε ετήσιο ενδελεχή έλεγχο από ανεξάρτητο οργανισμό, μετά την παραβίαση των διαφημιζόμενων πολιτικών ιδιωτικότητας για την υπηρεσία .NET Passport.

Προς αντιμετώπιση των προαναφερθέντων προβλημάτων και στα πλαίσια μιας ενορχηστρωμένης στρατηγικής, οργανισμοί, επιχειρήσεις και κυβερνήσεις σε παγκόσμιο επίπεδο υιοθετούν με αυξανόμενους ρυθμούς πρακτικές και προσεγγίσεις που ικανοποιούν εξίσου τις αρχές ασφάλειας πληροφοριών και ιδιωτικότητας, εντείνουν τη συμβατότητα τους με τα διεθνώς καταγεγραμμένα νομοθετήματα και πρότυπα και ευνοούν την κατάκτηση της εμπιστοσύνης του κοινού. Όπως έχει προαναφερθεί ο όρος εμπιστοσύνη έχει αποτελέσει, όπως και η ιδιωτικότητα και η ασφάλεια, αντικείμενο ενδελεχούς έρευνας στους κόλπους της επιστημονικής κοινότητας. Στο πλαίσιο των σχετικών εργασιών προς συγκεκριμενοποίηση της έννοιας έχει προκύψει μια σειρά από διαφορετικές προσεγγίσεις, συνακόλουθων ορισμών και επιλεγόμενων μηχανισμών εγκαθίδρυσης εμπιστοσύνης στις ηλεκτρονικές διαδικασίες. Σε γενικές γραμμές στο σύνολο των σχετικών εργασιών η εμπιστοσύνη των αλληλεπιδρώντων οντοτήτων εμφανίζεται άμεσα συνδεδεμένη με την προστασία ευαίσθητων δεδομένων και την ασφάλεια των πληροφοριών. Μάλιστα, στη βιβλιογραφία συναντάται ο ορισμός της «*εμπιστοσύνης στην*

τεχνολογία» ως η πεποίθηση των εμπλεκόμενων ότι τα υποκείμενα τεχνολογικά μέσα βρίσκονται σε θέση να υποστηρίξουν τις ηλεκτρονικές διαδικασίες σύμφωνα με τις προσδοκίες τους ([53]). Πυλώνες αυτής της διάστασης της εμπιστοσύνης είναι: η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα, η μη αποποίηση, η πιστοποίηση των χρηστών και ο έλεγχος πρόσβασης. Είναι σαφές ότι ο ορισμός αυτός της εμπιστοσύνης συνάδει με τα ευρήματα αυτής της Ενότητας σχετικά με τις γενικές αρχές ιδιωτικότητας και ασφάλειας των πληροφοριών στα σύγχρονα πληροφοριακά συστήματα, ενώ περιγράφει επαρκώς τους επιμέρους στόχους των μηχανισμών διαχείρισης εξουσιοδοτήσεων που αναλύονται στην επόμενη ενότητα.

3 Μηχανισμοί Διαχείρισης Εξουσιοδοτήσεων

Η προστασία της ιδιωτικότητας και η ασφάλεια των πληροφοριών αποτελούν πια στρατηγικό επιχειρηματικό στόχο και βασική λειτουργική απαίτηση οργανισμών που δραστηριοποιούνται στο Διαδίκτυο παγκοσμίως, επιδρώντας ουσιαστικά στη διαμόρφωση και υλοποίηση σχετικών μέτρων προφύλαξης και εγκαθίδρυσης εμπιστοσύνης στις σχέσεις τους με αλληλεπιδρώντες φορείς. Οι μηχανισμοί διαχείρισης εξουσιοδοτήσεων εργάζονται προς αυτή την κατεύθυνση: την εξασφάλιση εξουσιοδοτημένης και ασφαλούς πρόσβασης σε υπηρεσίες και δεδομένα σε δυναμικά περιβάλλοντα συνεργασίας και αλληλεπίδρασης. Ταυτόχρονα, παρέχουν τη δυνατότητα στους παρόχους υπηρεσιών και στα υποκείμενα των δεδομένων να οριοθετήσουν τις εξουσιοδοτήσεις ως προς τον υποκείμενο στόχο, χρόνο και τρόπο πρόσβασης. Επιπλέον αντιμετωπίζουν καίρια ζητήματα όπως είναι η πιστοποίηση των χρηστών (η διευκρίνηση δηλαδή της ταυτότητας και των γνωρισμάτων των χρηστών) και η απόδοση δικαιωμάτων και προνομίων πρόσβασης (ο καθορισμός δηλαδή του επιπέδου της πρόσβασης μιας πιστοποιημένης οντότητας) προσφέροντας με αυτόν τον τρόπο κάλυψη των βασικών αρχών ιδιωτικότητας και ασφάλειας, όπως αυτές αναγνωρίστηκαν στην προηγούμενη ενότητα.

Η διαχείριση εξουσιοδοτήσεων ως σύνολο λύσεων αποτελεί μια διεξοδική προσέγγιση προστασίας δεδομένων και υπηρεσιών που καλύπτει όλες τις εμπλεκόμενες διαδικασίες από την περιγραφή της ισχύουσας πολιτικής ασφάλειας υπό τη μορφή κανόνων ασφάλειας και ιδιωτικότητας μέχρι και την εφαρμογή της πολιτικής στην πράξη. Προς τούτο ενεργοποιούν διακριτούς μηχανισμούς ο καθένας εκ των οποίων αντιμετωπίζει αποσπασματικά συγκεκριμένες σκοπιές του προβλήματος. Έτσι, στον πυρήνα των συγκεκριμένων προσεγγίσεων εδράζονται μοντέλα ελέγχου πρόσβασης, μηχανισμοί ταυτοποίησης, κρυπτογραφικά εργαλεία και αλγόριθμοι συλλογιστικής ανάλυσης, η δυναμικότητα, η εκφραστικότητα και η ευελιξία των οποίων καθορίζουν και τις δυνατότητες του εφαρμοζόμενου πλαισίου διαχείρισης εξουσιοδοτήσεων. Στόχος της παρούσας ενότητας είναι η παρουσίαση των πιο σημαντικών προσεγγίσεων που έχουν προταθεί στη βιβλιογραφία ξεκινώντας από τη μελέτη των βασικών δομικών συστατικών τους και καταλήγοντας στην ανάλυση των κυριότερων μηχανισμών διαχείρισης εξουσιοδοτήσεων.

3.1 Βασικές Έννοιες Κρυπτογραφίας

Η κρυπτογραφία αναφέρεται στη μελέτη, σχεδίαση και ανάπτυξη των μαθηματικών τεχνικών, εργαλείων και πρωτοκόλλων για την επίτευξη στόχων που άπτονται της ασφάλειας πληροφοριών όπως εμπιστευτικότητα, ακεραιότητα, ταυτοποίηση οντοτήτων και πιστοποίηση της προέλευσης των δεδομένων. Ιστορικά η επιστήμη της κρυπτογραφίας και εκείνη της ασφάλειας πληροφοριών έχουν ακολουθήσει κοινή πορεία. Πράγματι, από την πρώιμη αξιοποίησή της από τους αρχαίους Αιγύπτιους, Σπαρτιάτες και Ρωμαίους μέχρι και τα σύγχρονα προηγμένα συστήματα κρυπτογράφησης, η κρυπτογραφία έχει χρησιμοποιηθεί κατά κόρον για τη διαφύλαξη της ασφάλειας και την κωδικοποίηση των πληροφοριών, δηλαδή τη μετατροπή των σχετικών δεδομένων από μια απλή, κατανοητή και ευνόητη απεικόνιση σε μορφή μη αναγνώσιμη από μη εξουσιοδοτημένους προς τούτο οντότητες.

Η κωδικοποίηση των πληροφοριών είναι συνώνυμη με την ενεργοποίηση μαθηματικών μετασχηματισμών, χωρίς γνώση των οποίων δεν μπορεί να υπάρχει καμία γνώση της κωδικοποιημένης πληροφορίας. Η φύση και η δομή των εφαρμοζόμενων μετασχηματισμών συνιστά και την κατηγοριοποίηση της κρυπτογραφίας και των κρυπτογραφικών συστημάτων σε δύο ευρείς κατηγορίες: συστήματα συμμετρικής κρυπτογραφίας και συστήματα ασύμμετρης κρυπτογραφίας. Τα συστήματα συμμετρικής κρυπτογραφίας κάνουν χρήση ενός μοναδικού κλειδιού – μετασχηματισμού για την κρυπτογράφηση ενός μηνύματος. Σε αυτό το σχήμα ο αποστολέας αφού κωδικοποιήσει την πληροφορία με τη χρήση κάποιου μετασχηματισμού, πρέπει παράλληλα με την κωδικοποιημένη πληροφορία να κάνει γνωστό και τον μετασχηματισμό που αξιοποίησε στον παραλήπτη των δεδομένων. Ο τελευταίος, κάνοντας χρήση του κοινοποιηθέντα μετασχηματισμού, μπορεί να επαναφέρει την πληροφορία στην αρχική αποκωδικοποιημένη της μορφή. Είναι προφανές ότι η ποιότητα της ασφάλειας που μπορούν να εξασφαλίσουν τα συστήματα συμμετρικής κρυπτογράφησης είναι εφάμιλλη της εμπιστευτικότητας του κοινού κλειδιού κωδικοποίησης. Η εισαγωγή της έννοιας της κρυπτογραφίας δημοσίου κλειδιού (ή ασύμμετρης κρυπτογραφίας) το 1976 από τους Diffie και Hellman ([54]) αποτέλεσε αναμφίβολα μια από τις πλέον καθοριστικές στιγμές στην ιστορία της κρυπτογραφίας. Στα συστήματα ασύμμετρης κρυπτογραφίας, αξιοποιείται ένα ζεύγος κλειδιών κωδικοποίησης που αποτελείται από ένα δημόσιο κλειδί, η εμπιστευτικότητα του οποίου δεν συνεπάγεται κάτι για την ασφάλεια της

κωδικοποιημένης πληροφορίας και ένα ιδιωτικό κλειδί, το οποίο δεν διαμοιράζεται και δεν κοινοποιείται σε καμία οντότητα εκτός από τον ιδιοκτήτη του κλειδιού. Σε αυτό το σχήμα λειτουργίας ο αποστολέας κωδικοποιεί την πληροφορία με το δημόσιο κλειδί του παραλήπτη καθιστώντας τα εμπλεκόμενα δεδομένα μη αναγνώσιμα από οποιαδήποτε άλλη οντότητα εκτός από τον κάτοχο του ιδιωτικού κλειδιού, δηλαδή τον παραλήπτη.

3.1.1 Γενικά Χαρακτηριστικά

Όπως προαναφέρθηκε βασικοί στόχοι της κρυπτογραφίας αποτελούν η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, η ταυτοποίηση των εμπλεκόμενων οντοτήτων καθώς και η πιστοποίηση της προέλευσης των δεδομένων. Στο πλαίσιο των σχετικών διαδικασιών χρησιμοποιούνται οι ακόλουθοι ορισμοί:

- Αρχικό κείμενο *M* (plaintext), το οποίο αποτελεί το μήνυμα υπό κωδικοποίηση.
- Κρυπτογραφημένο κείμενο *C* (ciphertext), το οποίο αποτελεί το μήνυμα που εξάγεται ως αποτέλεσμα της κρυπτογράφησης.
- Κλειδιά *K, K'* (key), τα οποία συναποτελούν μαζί με το αρχικό κείμενο την είσοδο της συνάρτησης κρυπτογράφησης για την παραγωγή του κρυπτογραφημένου κειμένου.
- Κάθε κλειδί *K* καθορίζει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ *M* και *C* που καλείται συνάρτηση ή μετασχηματισμός κρυπτογράφησης E_K (encryption function).
- Αντίστοιχα κάθε κλειδί *K'* καθορίζει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ *C* και *M* που καλείται συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης $D_{K'}$ (decryption function).
- Η διαδικασία εφαρμογής του μετασχηματισμού E_K στην πληροφορία *M* αναφέρεται ως κρυπτογράφηση.
- Η διαδικασία εφαρμογής του μετασχηματισμού $D_{K'}$ στην πληροφορία *C* αναφέρεται ως αποκρυπτογράφηση.
- Ένα σχήμα κρυπτογράφησης (encryption scheme) συνιστά ένα σύνολο μετασχηματισμών κρυπτογράφησης $\{E_K\}$ καθώς και ένα σύνολο μετασχηματισμών αποκρυπτογράφησης $\{D_{K'}\}$ για τα οποία ισχύει ότι για κάθε κλειδί *K* υπάρχει μοναδικό κλειδί *K'* για τα οποία $D_{K'} = E_K^{-1}$, ισχύει δηλαδή

ότι $D_{K'}(E_K(M)) = M$. Το σχήμα κρυπτογράφησης συναντάται συχνά ως αλγόριθμος κρυπτογράφησης (cipher).

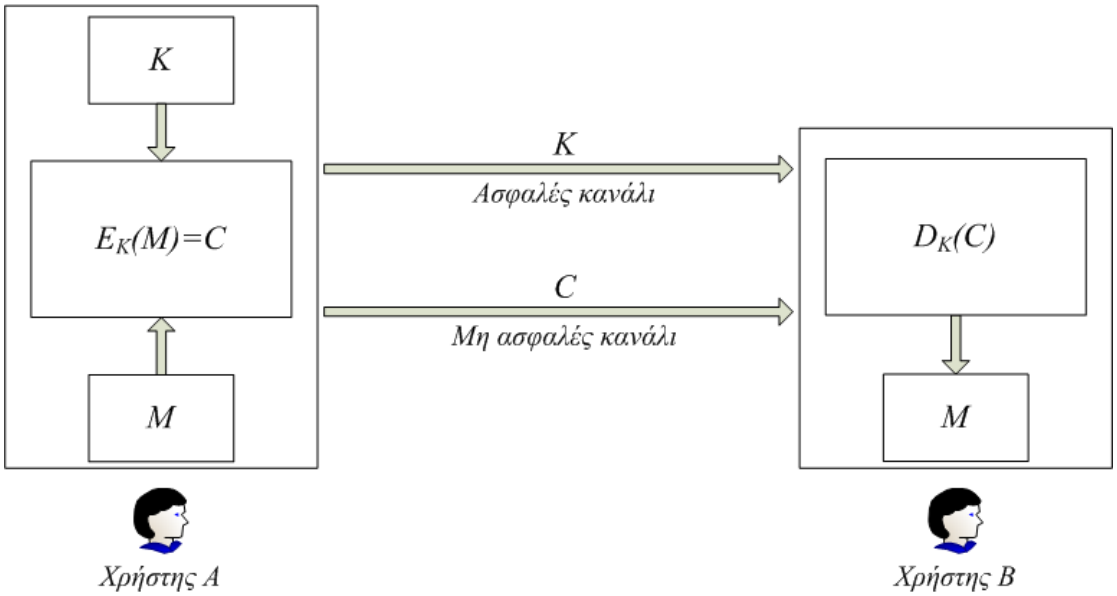
- Τα κλειδιά *K* και *K'* ονομάζονται ζεύγος κλειδιών (*K, K'*). Επισημαίνεται ότι το ζεύγος κλειδιών μπορεί να εμπεριέχει κοινά κλειδιά (δηλαδή *K = K'*).
- Μια συνάρτηση σύνοψης (hash function) αποτελεί μια αποδοτική υπολογιστικά συνάρτηση σύνδεσης δυαδικών αλφαριθμητικών τυχαίου μεγέθους σε δυαδικά αλφαριθμητικά ορισμένου μεγέθους (μικρότερου του αρχικού) που καλούνται συνόψεις (hash-values).
- Μια συνάρτηση σύνοψης καλείται μονόδρομη (one-way hash function) όταν είναι υπολογιστικά ανέφικτος ο υπολογισμός της αντίστροφης συνάρτησης.

Σημειώνεται ότι τα σχήματα κρυπτογράφησης αξιοποιούν κλειδιά για να διευρύνουν την εφαρμοστικότητα και την ευελιξία τους. Ειδικότερα, η χρήση τους επιτρέπει την αξιοποίηση κοινών μετασχηματισμών κρυπτογράφησης/αποκρυπτογράφησης, καθώς στην περίπτωση απώλειας της εμπιστευτικότητάς τους επαρκεί ως ελάχιστο μέτρο η αλλαγή των εμπλεκόμενων κλειδιών. Μάλιστα η περιοδική αλλαγή των χρησιμοποιούμενων κλειδιών συνιστά βέλτιστη πρακτική στα κρυπτογραφικά συστήματα. Υπό αυτό το πρίσμα η εμπιστευτικότητα του συγκεκριμένου ζεύγους κλειδιών (*K, K'*) συνιστά και το μέτρο της ποιότητας της ασφάλειας που προσφέρεται από ένα σχήμα κρυπτογράφησης. Εξάλλου, η δημόσια γνώση των συνόλων όπου ανήκουν τα μεγέθη $M, C, K, E_K, D_{K'}$ αποτελεί αδιαπραγμάτευτη και θεμελιώδη αρχή της κρυπτολογίας.

3.1.1.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία συναντάται στα κρυπτογραφικά συστήματα, όπου το ίδιο κλειδί *K* αξιοποιείται τόσο στη διαδικασία της κρυπτογράφησης όσο και σε αυτή της αποκρυπτογράφησης ((*K, K'*)). Σε αυτό το πλαίσιο λειτουργίας οι επικοινωνούσες οντότητες συμφωνούν και μοιράζονται ένα μοναδικό εμπιστευτικό κλειδί. Ο διαμοιρασμός του κλειδιού στους συμμετέχοντες πρέπει να πραγματοποιηθεί μέσω της χρήσης αποκλειστικά ασφαλών καναλιών επικοινωνίας, καθώς πιθανή διαρροή του κλειδιού κρυπτογράφησης έμμεσα επιφέρει και τη διαρροή του κλειδιού αποκρυπτογράφησης. Πρακτικά, τα κλειδιά *K* και *K'* είναι όμοια στις περισσότερες περιπτώσεις αξιοποίησης της συμμετρικής κρυπτογραφίας. Ωστόσο, θεωρητικά ένα

σχήμα κωδικοποίησης καλείται συμμετρικό αρκεί από τη γνώση του ενός μέλους στο του ζεύγους κλειδιών (*K, K'*) να κρίνεται υπολογιστικά «απλός» ο υπολογισμός του άλλου στελέχους. Καθώς η εμπιστευτικότητα του κοινού μυστικού κλειδιού καθορίζει και το επίπεδο της επιβληθείσας ασφάλειας, τα σχήματα συμμετρικής κωδικοποίησης συχνά συναντούνται ως κωδικοποίηση μοναδικού ή μυστικού κλειδιού ή συμβατική κρυπτογράφηση.



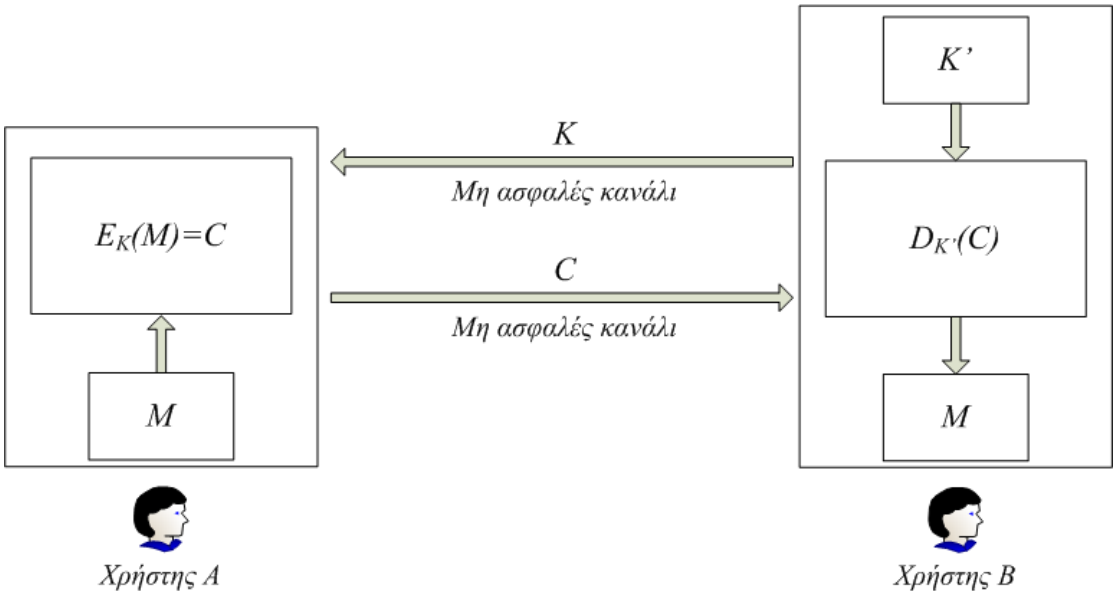
Εικόνα 1: Σχήμα συμμετρικής κρυπτογραφίας

3.1.1.2 Ασύμμετρη Κρυπτογραφία

Ένα από τα μεγαλύτερα προβλήματα των συστημάτων μοναδικού κλειδιού αποτελεί η εφαρμογή αποδοτικών μεθόδων για την παραγωγή και τον ασφαλή διαμοιρασμό του μυστικού κλειδιού (key distribution problem). Την εξάρτηση της κρυπτογράφησης και της αποδοτικότητάς της από την ασφαλή μετάδοση και διαμοιρασμό ενός κοινού μυστικού κλειδιού στα σχήματα συμμετρικής κρυπτογραφίας εκμηδενίζουν τα σχήματα ασύμμετρης κρυπτογραφίας. Ενώ, η έννοια της κρυπτογράφησης δημόσιου κλειδιού είναι απλή, το εύρος των εφαρμογών της είναι εξαιρετικά ευρύ. Ένα σχήμα ασύμμετρης κρυπτογράφησης εμπεριέχει τη χρήση ενός ζεύγους κλειδιών (*K, K'*), που αποτελείται από ένα δημόσιο κλειδί *K* (public key) του οποίου η γνώση δεν απειλεί την ασφάλεια της κωδικοποιημένης πληροφορίας και ένα ιδιωτικό κλειδί *K'* (private key) του οποίου η εμπιστευτικότητα συνιστά τον ακρογωνιαίος λίθο του σχήματος. Σε ένα σχήμα ασύμμετρης

κρυπτογράφησης (E_K, $D_{K'}$) δοθέντος του μετασχηματισμού κρυπτογράφησης E_K και του κρυπτογραφημένου μηνύματος C είναι υπολογιστικά αδύνατη η εξαγωγή του αρχικού μηνύματος M, έτσι ώστε $E_K(M) = C$. Το γνώρισμα αυτό συνεπάγεται ότι αν και το δημόσιο κλειδί παράγεται από το ιδιωτικό δεν υπάρχει μαθηματική μέθοδος αντιστροφής της διαδικασίας προς εξαγωγή του δεύτερου από το πρώτο. Για την αποστολή εμπιστευτικών δεδομένων ο αποστολέας κρυπτογραφεί την πληροφορία κάνοντας χρήση του δημόσιου κλειδιού του παραλήπτη, ενώ ο τελευταίος το αποκωδικοποιεί αξιοποιώντας το αντίστοιχο ιδιωτικό κλειδί.

Ενώ στα συστήματα συμμετρικής κρυπτογραφίας, κάθε κοινότητα χρηστών διατηρεί διαφορετικό μυστικό κλειδί το οποίο πρέπει να διαμοιράζεται με ασφαλή τρόπο, στα σχήματα ασύμμετρης κρυπτογραφίας το δημόσιο μέλος του ζεύγους κλειδιών είναι δημοσίως γνωστό σε σχετικούς καταλόγους και ο καθένας μπορεί να το αξιοποιήσει για την ασφαλή αποστολή δεδομένων στον κάτοχο του κλειδιού. Το γεγονός αυτό καθιστά την ασύμμετρη μέθοδο κρυπτογράφησης σαφώς αποδοτικότερα κλιμακούμενη συγκριτικά με τη συμμετρική. Ταυτόχρονα όμως η κρυπτογράφηση δημόσιου κλειδιού χαρακτηρίζεται από χαμηλές ταχύτητες μετασχηματισμού των δεδομένων και συνεπακόλουθα δεν είναι αποδοτική για την κρυπτογράφηση μεγάλων σε μέγεθος πληροφοριών. Στην πράξη, η κρυπτογράφηση δημόσιου κλειδιού αξιοποιείται για τον ασφαλή διαμοιρασμό μυστικών κλειδιών σε συμμετρικά σχήματα, τα οποία στη συνέχεια αξιοποιούνται για την κωδικοποίηση/ αποκωδικοποίηση του μηνύματος με έναν περισσότερο υπολογιστικά αποδοτικό συμμετρικό μετασχηματισμό. Το υβριδικό σχήμα αυτό αξιοποίησης τεχνικών συμμετρικής και ασύμμετρης κρυπτογραφίας καλείται ψηφιακός φάκελος (digital envelope). Χαρακτηριστικό παράδειγμα χρήσης ψηφιακών φακέλων συνιστά το σχήμα κρυπτογράφησης δεδομένων Pretty Good Privacy (PGP) [55] όπου αξιοποιούνται ο συμμετρικός αλγόριθμος IDEA και ο ασύμμετρος RSA.



Εικόνα 2: Σχήμα ασύμμετρης κρυπτογραφίας

3.1.1.3 Ψηφιακές Υπογραφές

Ο μηχανισμός των ψηφιακών υπογραφών κατέχει σημαντική θέση στις διαδικασίες της ταυτοποίησης χρηστών και της διαχείρισης των εξουσιοδοτήσεων ενώ ταυτόχρονα αξιοποιείται συχνά σε συστήματα ασφάλειας προς τήρηση της αρχή της μη-αποποίησης. Ουσιαστικά, οι ψηφιακές υπογραφές παρέχουν τα μέσα για τη σύνδεση της ταυτότητας μιας οντότητας με ένα κομμάτι πληροφορίας, διαδραματίζοντας τον ρόλο των προσωπικών χειρόγραφων υπογραφών στις ηλεκτρονικές διαδικασίες. Η μεγάλη δυσκολία παραχάραξης, ο ταυτοποιητικός χαρακτήρας και η ευκολία επαλήθευσης της ορθότητας, χαρακτηριστικά γνωρίσματα των χειρόγραφων υπογραφών συνοδεύουν επίσης τις ψηφιακές υπογραφές στα πεδία εφαρμογής τους.

Η υλοποίηση του μηχανισμού των ψηφιακών υπογραφών στηρίζεται στις τεχνικές κρυπτογράφησης δημόσιου κλειδιού. Ειδικότερα, ένας χρήστης προς επικύρωση της ταυτότητάς του ως αποστολέας μιας πληροφορίας κρυπτογραφεί μια σύνοψη της πληροφορίας (που έχει παραχθεί με την εφαρμογή μιας κοινά αποδεκτής μονόδρομης συνάρτησης σύνοψης) με χρήση του ιδιωτικού του κλειδιού παράγοντας ουσιαστικά την ψηφιακή του υπογραφή. Ο λήπτης της πληροφορίας είναι σε θέση να επικυρώσει την ορθότητα της ψηφιακής υπογραφής αποκρυπτογραφώντας τη με το δημόσιο κλειδί του αποστολέα και συγκρίνοντας την εξαχθείσα σύνοψη με μια σύνοψη του μηνύματος που ο ίδιος παράγει. Σε περίπτωση που οι δύο συνόψεις είναι ταυτόσημες,

τότε η ψηφιακή υπογραφή είναι έγκυρη. Ο μηχανισμός των ψηφιακών υπογραφών επιτρέπει στη διαδικασία ανταλλαγής μηνυμάτων να είναι συμβατή με τις ακόλουθες αρχές της ασφάλειας πληροφοριών:

- **Ακεραιότητα**: Εφόσον η εξαχθείσα από την ψηφιακή υπογραφή σύνοψη είναι σωστή και ταυτόσημη με την παραχθείσα από το μήνυμα σύνοψη, η αρχική πληροφορία δεν είναι δυνατό να έχει τροποποιηθεί κατά τη μετάδοσή της.
- **Αυθεντικότητα**: Το μήνυμα έχει αποσταλεί από τη συγκεκριμένη οντότητα και μόνο αυτή, εφόσον μόνο αυτή έχει την κυριότητα του χρησιμοποιηθέντος ιδιωτικού κλειδιού.
- **Μη αποποίηση**: Ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος καθώς αποτελεί τη μοναδική οντότητα σε θέση να παράξει τη συγκεκριμένη υπογραφή.
- **Υπευθυνότητα**: Σε συνέχεια του προηγούμενου γνωρίσματος, ο αποστολέας καθίσταται υπεύθυνος για την αποστολή του μηνύματος και υπόλογος για τις όποιες ενέργειες άπτονται της αποστολής αυτής.

3.1.1.4 Ψηφιακά Πιστοποιητικά

Η ασφαλής λειτουργία ενός κρυπτογραφικού συστήματος δημόσιου κλειδιού είναι σημαντικά εξαρτώμενη από την ισχύ και εγκυρότητα των εμπλεκόμενων δημόσιων κλειδιών και τη σύνδεση τους με τις ιδιοκτήτριες οντότητες. Προς τούτο, στην πράξη τα δημόσια κλειδιά οργανώνονται υπό τη μορφή ψηφιακών πιστοποιητικών τα οποία συνιστούν και τον πλέον δημοφιλή τρόπο επικύρωσης της κατοχής ενός ασύμμετρου ζεύγους κλειδιών από μια οντότητα. Ένα ψηφιακό πιστοποιητικό (συχνά συναντάται ο όρος πιστοποιητικό δημόσιου κλειδιού) συνιστά μια τεκμηριωμένη σύζευξη μεταξύ ενός δημόσιου κλειδιού και της ταυτότητας του κατόχου του. Στο πλαίσιο χρήσης των ψηφιακών πιστοποιητικών, η ταυτότητα μια οντότητας συναποτελείται από οποιοδήποτε σύνολο πληροφοριών που προσδιορίζει πλήρως την οντότητα που κατέχει και χρησιμοποιεί το αντίστοιχο με το δημόσιο ιδιωτικό κλειδί. Επιπλέον, τα ψηφιακά πιστοποιητικά είναι δυνατόν να περιέχουν πλήθος άλλων πληροφοριών όπως είναι το χρονικό διάστημα ισχύος τους, οι χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης και το μέγεθος των σχετικών κλειδιών. Προς επικύρωση της ισχύος τους, τα πιστοποιητικά δημόσιου κλειδιού υπογράφονται ψηφιακά από έμπιστες

τρίτες οντότητες οι οποίες καλούνται Αρχές Πιστοποίησης (Certification Authority – CA). Οι Αρχές Πιστοποίησης επιτελούν μια σειρά από κρίσιμες λειτουργίες καθώς είναι υπεύθυνες για την έκδοση, τη διαχείριση, τη διανομή, την αποθήκευση και την ανάκληση των ψηφιακών πιστοποιητικών. Προφανώς, ο βαθμός εμπιστοσύνης που επιδεικνύει σε μια CA κάποιος χρήστης συνιστά και το επίπεδο εμπιστοσύνης που διατηρεί για τα εκδιδόμενα από εκείνη πιστοποιητικά.

Το πλέον διαδεδομένο και αναγνωρισμένο πρότυπο προδιαγραφής πιστοποιητικών δημόσιου κλειδιού παγκοσμίως εντοπίζεται στην έκδοση ITU-T X.509 [56] της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union – ITU) [57]. Σύμφωνα με το πρότυπο X.509 η δομή των ψηφιακών πιστοποιητικών αποτελείται από πεδία που υποδεικνύουν τις ακόλουθες τιμές: το δημόσιο κλειδί του κατόχου, ένα αναγνωριστικό του ασύμμετρου αλγορίθμου με τον οποίο θα αξιοποιηθεί το κλειδί, το όνομα του κατόχου του ζεύγους κλειδιών, το όνομα της Αρχής Πιστοποίησης που επικυρώνει την ιδιοκτησία αυτή, τον αριθμό της έκδοσης του προτύπου X.509 με το οποίο είναι συμβατό το πιστοποιητικό και μια σειρά από προαιρετικά πεδία που περιέχουν πληροφορίες σχετικά με τις πολιτικές πιστοποίησης της CA. Όπως προαναφέρθηκε, προς επικύρωση της ισχύος του το πιστοποιητικό υπογράφεται κάνοντας χρήση του ιδιωτικού κλειδιού της CA. Η υπογραφή αυτή εκτός από την εγκυρότητα του πιστοποιητικού βεβαιώνει ταυτόχρονα ότι τυχόν τροποποιήσεις στο περιεχόμενο των πληροφοριών δεν μπορούν να πραγματοποιηθούν χωρίς ανίχνευση.

Μια οντότητα για να εξακριβώσει το αληθές και έγκυρο της ψηφιακής υπογραφής μιας CA σε κάποιο πιστοποιητικό πρέπει να έχει πρόσβαση στο δημόσιο κλειδί της. Καθώς το εν λόγω κλειδί είναι δυνατό να πιστοποιείται από μια άλλη, ανώτερη ιεραρχικά CA στη μορφή ψηφιακού πιστοποιητικού, εν τέλει η διαδικασία εξακρίβωσης της εγκυρότητας πιστοποιητικών δημόσιου κλειδιού μπορεί να εμπεριέχει μια αλυσίδα πιστοποιητικών και Αρχών Πιστοποίησης. Στο τέλος της αλυσίδας αυτής εντοπίζεται το πιστοποιητικό μιας CA, η οποία καλείται ρίζα αξιοπιστίας (root of trust). Τα δημόσια κλειδιά των συγκεκριμένων CA εκδίδονται και διαμοιράζονται υπό τη μορφή πιστοποιητικών που υπογράφονται από τις ίδιες (self-signed certificates) και υποδηλώνουν ότι οι ίδιες έχουν στην κατοχή τους τα συγκεκριμένα δημόσια κλειδιά. Ωστόσο, ενώ η υπογραφή των self-signed πιστοποιητικών επιτρέπει την εξακρίβωση της ακεραιότητας των περικλειόμενων πληροφοριών, δεν επιτρέπει την επαλήθευση της ακρίβειάς τους, καθώς η απουσία

κάποιας πιστοποίησης από μια έμπιστη τρίτη οντότητα αφήνει ανοιχτό το ενδεχόμενο αναπαραγωγής λανθασμένων στοιχείων. Επομένως στα κρυπτογραφικά συστήματα δημόσιου κλειδιού ιδιαίτερη προσοχή δίνεται στην ασφαλή και έγκυρη διανομή των δημόσιων κλειδών των Αρχών Πιστοποίησης ρίζας (root CA) έτσι ώστε να βεβαιώνεται ότι τα στοιχεία των εμπλεκόμενων πιστοποιητικών ανήκουν όντως στις σωστές οντότητες – CA. Απουσία ή απώλεια της βεβαιότητας αυτής θέτει σε κίνδυνο ολόκληρη την υποδομή καθώς ενεργοποιεί τη δυνατότητα επίτευξης μια επίθεσης πλαστοπροσωπίας (masquerade attack), όπου μια μη έμπιστη οντότητα μπορεί να υποδυθεί τον ρόλο μιας έμπιστης Αρχή Πιστοποίησης ρίζας.

Πρέπει να σημειωθεί ότι επιπλέον των ψηφιακών πιστοποιητικών και για σκοπούς ταυτοποίησης χρηστών αξιοποιούνται συχνά βιομετρικές μέθοδοι. Στην ταυτοποίηση χρηστών με βιομετρικές μεθόδους, σε αντίθεση με τις κρυπτογραφικές τεχνικές που ενεργοποιούν τα ψηφιακά πιστοποιητικά, αξιοποιούνται φυσικά γνωρίσματα των ατόμων υπό ταυτοποίηση και οδηγούν σε διαδικασίες όπως η σάρωση δαχτυλικών αποτυπωμάτων, η αναγνώριση προσώπου, η σάρωση της ίριδας και η επιβεβαίωση της υπογραφής. Επιπρόσθετα έχουν προταθεί στη βιβλιογραφία υβριδικά μοντέλα που ενσωματώνουν κρυπτογραφικές τεχνικές στις βιομετρικές τεχνολογίες σάρωσης.

3.1.2 Υποδομή Δημόσιου Κλειδιού

Οι Υποδομές Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) συνιστούν μια από τις πιο σημαντικές στιγμές της εφαρμογής της κρυπτογραφίας στα πληροφοριακά συστήματα. Στόχος των υποδομών PKI είναι η οργανωμένη έκδοση και διαχείριση πιστοποιητικών δημόσιου κλειδιού καθώς και η συντεταγμένη διαχείριση των εμπλεκόμενων κλειδιών. Προς τούτο ενεργοποιούν Αρχές Πιστοποίησης, των οποίων ο ρόλος είναι κρίσιμος για την αποδοτικότητα μιας εγκατάστασης PKI καθώς αναπαριστούν το σημείο απόδοσης εμπιστοσύνης και άντλησης αξιοπιστίας χρηστών και λοιπών CA. Μάλιστα η τοποθέτηση των Αρχών Πιστοποίησης εντός μιας υποδομής επηρεάζει ουσιαστικά θεμελιώδη ζητήματα των κρυπτογραφικών συστημάτων, όπως είναι η επαλήθευση της εγκυρότητας των πιστοποιητικών και η σύναψη ασφαλών σχέσεων εμπιστοσύνης με διαφορετικούς τομείς (δηλαδή εκτός της επιρροής μιας CA). Παραδοσιακά σχήματα PKI συνιστούν τα ακόλουθα:

- Αρχιτεκτονική μοναδικής CA: Όλες οι οντότητες του συστήματος αντιλαμβάνονται μια μοναδική CA ως έμπιστη οντότητα, η οποία είναι υπεύθυνη για τη διαχείριση όλων των εμπλεκόμενων πιστοποιητικών.
- Αρχιτεκτονική ιεραρχικά οργανωμένων CA: Οι CA του συστήματος είναι οργανωμένες και συνδεδεμένες ιεραρχικά, με την Αρχή Πιστοποίησης ρίζας να βρίσκεται υπεύθυνη για την πιστοποίηση των υπό αυτή CA και κάθε ενδιάμεση CA να είναι υπεύθυνη για την πιστοποίηση των κατωτέρων τους ιεραρχικά CA και των χρηστών της.
- Αρχιτεκτονική Πλέγματος (mesh architecture): Οι CA βρίσκονται συνδεδεμένες με σχέσεις ομοίου προς όμοιο καταργώντας τις ιεραρχίες του προηγούμενου τύπου αρχιτεκτονικής και καθιστώντας κάθε CA υπεύθυνη για την πιστοποίηση κατά κύριο λόγο των χρηστών της και κατά δεύτερο λόγο των συνδεδεμένων με αυτή CA.

Το πλαίσιο λειτουργίας του κάθε τύπου υποδομής PKI χαρακτηρίζεται από μια σειρά πλεονεκτημάτων και μειονεκτημάτων γεγονός που κατηγοριοποιεί τις συγκεκριμένες αρχιτεκτονικές αναφορικά με την εφαρμοστικότητα, την αποδοτικότητα και την κλιμάκωσή τους σε διαφορετικά πεδία εφαρμογής. Κοινός τόπος της μελέτης των παραδοσιακών σχημάτων Υποδομών Δημόσιου Κλειδιού έχει αποδειχθεί η μη καταλληλότητά τους για την υποστήριξη πολλαπλών και ευρέως κατανεμημένων αλληλεπιδράσεων μεταξύ διαφορετικών τομέων κυρίως για λόγους μη επαρκούς κλιμάκωσης ([58]) αναφορικά με τις διαδικασίες του εντοπισμού του σημείου εμπιστοσύνης απομακρυσμένων χρηστών και του υπολογισμού της ακρίβειας και της εγκυρότητας των εμπλεκόμενων πιστοποιητικών.

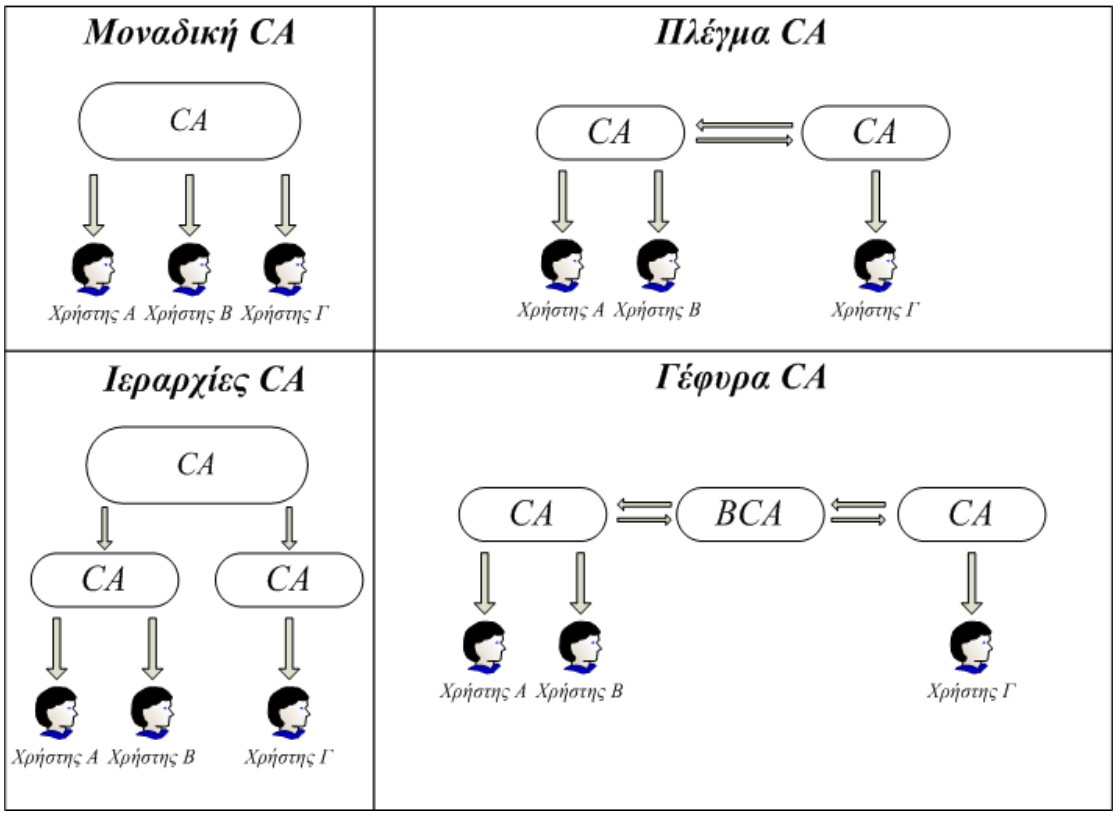
Προς ενεργοποίηση των δυνατοτήτων των υποδομών PKI στα κατανεμημένα περιβάλλοντα των σύγχρονων πληροφοριακών συστημάτων έχει μελετηθεί η έννοια των Αρχών Πιστοποίησης Γέφυρας (Bridge Certification Authorities – BCA). Οι BCA είναι σχεδιασμένες για την αντιμετώπιση των ζητημάτων και των ανεπαρκειών που παρουσιάζουν τα συμβατικά σχήματα PKI, συνδέοντας υπάρχοντες υποδομές PKI υπό την αιγίδα μια ενιαίας συνομοσπονδίας υποδομών, μειώνοντας τα υπολογιστικά κόστη που σχετίζονται με την εξακρίβωση της εγκυρότητας πιστοποιητικών, εξισώνοντας και συσχετίζοντας τις πολιτικές πιστοποίησης των σχετικών CA και καθιστώντας έτσι τα σχήματα BCA συμβατά με τις απαιτήσεις ευρέως κατανεμημένων εφαρμογών. Πρέπει να τονιστεί ότι οι BCA δεν εκδίδουν

πιστοποιητικά σε χρήστες και επομένως δεν αναγνωρίζονται ως σημεία εμπιστοσύνης από κανένα χρήστη εντός της συνομοσπονδίας υποδομών PKI. Συνεπακόλουθα κάθε διακριτός τομέας PKI διατηρεί εσωτερικά το δικό του σχήμα λειτουργίας και την αυτονομία του σε ότι αφορά τις πολιτικές πιστοποίησης που ακολουθεί. Οι πολιτικές και κανόνες πιστοποίησης μιας CA καθορίζουν ρητά τον τρόπο με τον οποίο οι Αρχές λειτουργούν και εργάζονται. Επομένως μια πολιτική πιστοποίησης συνιστά την πλέον χρηστική πληροφορία για τις οντότητες υπό συνεργασία με μια CA καθώς δίνει τη δυνατότητα προσαρμογής της συμπεριφοράς τους στο επίπεδο της ποιότητας της πολιτικής. Μάλιστα στο πρότυπο X.509 προδιαγράφονται οι μηχανισμοί δημοσιοποίησης των σχετικών πολιτικών σε πεδία – επεκτάσεις ψηφιακών πιστοποιητικών που εκδίδονται από την ίδια την CA. Οι πολιτικές και πρακτικές πιστοποίησης αποτελούν τη βάση για την εξακρίβωση του επιπέδου της εμπιστοσύνης που μπορεί να αναγνωριστεί σε πιστοποιητικά που εκδίδονται από τη συγκεκριμένη Αρχή και αποτελούν τον θεμέλιο λίθο της λειτουργίας των BCA σε ότι αφορά τη συσχέτιση και εξίσωση των πολιτικών διαφορετικών CA μιας συνομοσπονδίας PKI. Μάλιστα, στο Request For Comments RFC 5217 [59] ορίζονται συγκεκριμένες προδιαγραφές για τη σύνδεση πολλαπλών υποδομών PKI με τη χρήση Αρχών Πιστοποίησης Γέφυρας καθιστώντας μάλιστα την έννοια του επιπέδου βεβαιότητας (Level of Assurance), που όπως προαναφέρθηκε συνιστά κριτήριο για το επίπεδο της αυθεντικοποίησης και της εξουσιοδότησης χρηστών, κεντρική στη διαδικασία συσχέτισης διαφορετικών πολιτικών πιστοποίησης.

Τα τελευταία χρόνια, έχει προταθεί και υλοποιηθεί μια σειρά από ενδιαφέρουσες λύσεις αξιοποίησης Αρχών Πιστοποίησης Γέφυρας σε παγκόσμιο επίπεδο. Ενδεικτικά, υλοποιήσεις που παρουσιάζουν υψηλό επίπεδο προσαρμοστικότητας, εφαρμοστικότητας και συμμόρφωσης με τις ειδικές απαιτήσεις ετερογενών και κατανεμημένων περιβαλλόντων είναι οι ακόλουθες:

- Η Ευρωπαϊκή Αρχή Πιστοποίησης Γέφυρας (European Bridge-CA – EBCA) [60], η οποία συνδέει με ασφαλή κανάλια επικοινωνίας επιχειρήσεις, τράπεζες, ασφαλιστικές και τηλεπικοινωνιακές εταιρίες και δημόσιους φορείς σε όλη την Ευρώπη.
- Η Ομοσπονδιακή Αρχή Πιστοποίησης Γέφυρας (Federal Bridge Certification Authority – FBCA) ([61]), η οποία εξασφαλίζει ασφαλή διαλειτουργικότητα στις ενός των Η.Π.Α. οντότητες που έχουν διαπιστευτεί από την

ομοσπονδιακή BCA. Αυτή τη στιγμή υπό την αιγίδα της FBCA βρίσκονται δεκαεφτά κυβερνητικοί και επιχειρηματικοί οργανισμοί οι οποίοι με τη σειρά τους είναι υπεύθυνοι για την πιστοποίηση εκατομμυρίων χρηστών.



Εικόνα 3: Διαφορετικές αρχιτεκτονικές οργάνωσης PKI δικτύων

3.1.3 Υποδομή Διαχείρισης Δικαιωμάτων

Οι πρώτες εκδόσεις του προτύπου για τα ψηφιακά πιστοποιητικά X.509 (1988, 1993 και 1997) προδιέγραψαν τα βασικά δομικά και λειτουργικά στοιχεία των πιστοποιητικών δημόσιου κλειδιού και των Υποδομών Δημόσιου Κλειδιού. Οι αναθεωρημένη έκδοση του προτύπου το 2001 (όπως και οι επικαιροποιημένες εκδόσεις το 2005 και το 2008) εισήγαγαν σημαντικές επεκτάσεις και βελτιώσεις με κορυφαία όλων την περιγραφή των πιστοποιητικών ιδιοτήτων (attribute certificates) και του πλαισίου λειτουργίας των Υποδομών Διαχείρισης Δικαιωμάτων (Privilege Management Infrastructure – PMI). Οι Υποδομές Διαχείρισης Δικαιωμάτων διαχειρίζονται τα δικαιώματα χρηστών, παρέχουν υπηρεσίες εξουσιοδότησης οντοτήτων και λειτουργούν πανομοιότυπα αλλά συμπληρωματικά με τις Υποδομές Δημόσιου Κλειδιού που επικεντρώνονται στη διαχείριση της αυθεντικοποίησης

χρηστών. Μάλιστα, η συνεργασία και η ολοκλήρωση συστημάτων PKI και PMI έχει αποτελέσει αντικείμενο ανάλυσης και μελέτης του προτύπου X.509. Οι λειτουργίες και οι μηχανισμοί μιας υποδομής PMI επιτρέπουν τον ορισμό δικαιωμάτων σε χρήστες και την απεικόνισή τους σε πιστοποιητικά ιδιοτήτων εκδιδόμενα από μια Αρχή Εξουσιοδοτήσεων (Source of Authority – SoA) ή από εξουσιοδοτημένες προς τούτο Αρχές Ιδιοτήτων (Attribute Authority – AA). Τα πιστοποιητικά ιδιοτήτων επιτελούν στις υποδομές PMI τον σκοπό των ψηφιακών πιστοποιητικών στις υποδομές PKI, συνδέοντας και συσχετίζοντας δημόσια κλειδιά με ένα πλήθος γνωρισμάτων, χαρακτηριστικών και δικαιωμάτων χρηστών. Μάλιστα, πεδία των πιστοποιητικών ιδιοτήτων μπορούν να υποδεικνύουν τιμές βιομετρικών μεγεθών προς σύζευξη των φυσικών γνωρισμάτων ενός χρήστη με το δημόσιο κλειδί που έχει στην κατοχή του.

3.2 Μοντέλα Ελέγχου Πρόσβασης

Όπως έχει προαναφερθεί, στην καρδία των μηχανισμών εξουσιοδοτήσεων εντοπίζονται μοντέλα ελέγχου πρόσβασης των οποίων οι δυνατότητες και η ευελιξία χαρακτηρίζουν και συνοδεύουν τις επιδόσεις των μηχανισμών που τα ενσωματώνουν. Τα μοντέλα ελέγχου πρόσβασης επιτρέπουν στους μηχανισμούς διαχείρισης εξουσιοδοτήσεων να μοντελοποιούν τις πολιτικές ασφάλειας υπό τη μορφή κατανοητών κανόνων πρόσβασης, να συστηματοποιούν την προστασία ευαίσθητων δεδομένων και υπηρεσιών, να προδιαγράφουν την εμπιστευτικότητα προστατευόμενων αγαθών, να υποστηρίζουν την εγκαθίδρυση σχέσεων εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων, να επιτυγχάνουν συμβατότητα με τη νομοθεσία και τα διεθνή πρότυπα, να συσχετίζουν την πρόσβαση σε πόρους με ποσοτικά και ποιοτικά χαρακτηριστικά χρηστών και οντοτήτων καθώς και με τις ισχύουσες συνθήκες και τέλος να αξιοποιούν προηγμένους αλγόριθμους συλλογιστικής και συμπερασματικής ανάλυσης για την εξαγωγή ακριβών και επικαιροποιημένων αποφάσεων πρόσβασης.

Στο πλαίσιο της λειτουργίας των σύγχρονων αποκεντρωμένων δικτύων, τα παραδοσιακά και συμβατικά σχήματα όπως είναι τα μοντέλα Διακριτικού Ελέγχου Πρόσβασης (Discretionary Access Control – DAC), Υποχρεωτικού Ελέγχου Πρόσβασης Mandatory Access Control – MAC) και Ελέγχου Πρόσβασης Βάσει Ρόλων (Role-Based Access Control – RBAC) [62] αποτυγχάνουν να καλύψουν τις

αρχές ασφάλειας και ιδιωτικότητας όπως αυτές εξάγονται από τη νομοθεσία και τα διεθνή πρότυπα ασφάλειας. Ενώ, παρέχουν τις δυνατότητες για την απάντηση ερωτημάτων όπως «ποια οντότητα και με ποιο ρόλο έχει ποιου είδους πρόσβαση σε ποιο αντικείμενο» αδυνατούν να προσαρμόσουν τις παραχθείσες αποφάσεις πρόσβασης σε πιο απαιτητικά κριτήρια καθώς στερούνται της κατάλληλης εκφραστικότητας. Ωστόσο τα παραδοσιακά σχήματα έχουν διαδραματίσει επιτελικό ρόλο στις εξελίξεις στον χώρο των μοντέλων ελέγχου πρόσβασης, αναδεικνύοντας τη βαρύνουσα σημασία των μοντέλων για την ποιότητα της ασφάλειας των πληροφοριών ενός συστήματος και θέτοντας τη βάση για τη διαμόρφωση νέων προηγμένων πλαισίων.

3.2.1 Μοντέλα με Επίγνωση της Ιδιωτικότητας

Τα μοντέλα ελέγχου πρόσβασης με επίγνωση της ιδιωτικότητας έχουν αποτελέσει αντικείμενο έντονης μελέτης και δραστηριότητας σε ερευνητικό επίπεδο τα τελευταία χρόνια. Αφενός τα σοβαρά προβλήματα ιδιωτικότητας που εγείρουν τα σύγχρονα πληροφοριακά συστήματα και αφετέρου η συνειδητοποίηση των οργανισμών πως η έννοια της προστασίας των προσωπικών δεδομένων είναι ταυτόσημη με την ενίσχυση της παραγωγικότητας και την αύξηση της επιχειρηματικότητας έχουν οδηγήσει στη σχεδίαση και υλοποίηση πληθώρας σχετικών πλαισίων. Αναμφίβολα μια από τις πρώτες και πιο σημαίνουσες προσεγγίσεις σχετικά με την αναγνώριση της ιδιωτικότητας στα πληροφοριακά συστήματα αποτέλεσαν οι «Ιπποκρατικές Βάσεις Δεδομένων» (Hippocratic Databases) που προτάθηκαν το 2002 [63] και εισήγαγαν την έννοια του σκοπού της πρόσβασης ως κεντρική παράμετρο στη λήψη αποφάσεων πρόσβασης σε πληροφορίες. Το αποτέλεσμα ήταν η σχεδίαση ενός πλαισίου μετασχηματισμών αναζητήσεων σε σχεσιακές βάσεις δεδομένων με επίγνωση ιδιωτικότητας. Έκτοτε, μια σειρά από καινοτόμα μοντέλα έχει προταθεί στη βιβλιογραφία, το καθένα από τα οποία εισάγει και ενεργοποιεί διαφορετικούς όρους και έννοιες προς αντιμετώπιση των ζητημάτων ιδιωτικότητας. Στόχος αυτής της ενότητας είναι η παρουσίαση των πιο αντιπροσωπευτικών και σημαντικών από τις υπάρχουσες προσεγγίσεις.

3.2.1.1 Έλεγχος Πρόσβασης Βάσει Σκοπού (Purpose Based Access Control – Pu-BAC)

Η εξακρίβωση του σκοπού της πρόσβασης αποτελεί κεντρική στρατηγική στη νομοθεσία περί ιδιωτικότητας όπως αναλύθηκε σε προηγούμενη ενότητα. Στο μοντέλο Pu-BAC [64] η έννοια του σκοπού κατέχει κεντρική θέση με το σύνολο των προδιαγραμμένων σκοπών να εντοπίζεται οργανωμένο σε μια ιεραρχική δενδρική δομή, στην οποία οι σχέσεις μεταξύ κόμβων δηλώνουν συσχετίσεις γενίκευσης και ειδίκευσης μεταξύ σκοπών. Η εκφραστικότητα του μοντέλου επιτρέπει τον ορισμό κανόνων ιδιωτικότητας όπου πρόσβαση σε δεδομένα επιτρέπεται μόνο αν κάτι τέτοιο συνάδει με τον «προτιθέμενο σκοπό». Το σύνολο των προτιθέμενων σκοπών συνιστά ουσιαστικά τους ισχύοντες κανόνες πρόσβασης, όπου τα δεδομένα υπό προστασία συνδέονται άμεσα με κάποιον σκοπό. Το μοντέλο εισάγει επιπρόσθετα τον όρο του «σκοπού πρόσβασης» ο οποίος αναφέρεται στον ιδιαίτερο σκοπό μίας συγκεκριμένης αίτησης πρόσβασης σε δεδομένα. Στο πλαίσιο λειτουργίας του μοντέλου, πρόσβαση σε δεδομένα επιτρέπεται μόνο στην περίπτωση που ο δηλωμένος σκοπός πρόσβασης υπολογιστεί ότι είναι ταυτόσημος με τον προτιθέμενο σκοπό.

Για την υποστήριξη μεγαλύτερης ευελιξίας και εκφραστικότητας στην προδιαγραφή μια πολιτικής ασφάλειας δεδομένων το μοντέλο υποστηρίζει τη διαμόρφωση τόσο θετικών όσο και αρνητικών κανόνων (με την έννοια της θετικής ή μη απάντησης σε αίτημα πρόσβασης), αποδίδοντας μάλιστα προτεραιότητα στους αρνητικούς κανόνες σε περίπτωση αντικρουόμενων κανόνων. Με αυτόν τον τρόπο, εξασφαλίζεται ότι πρόσβαση σε δεδομένα με σκοπούς για τους οποίους κάτι τέτοιο έχει απαγορευτεί ρητά δεν πρόκειται να επιτραπεί. Ιεραρχικές σχέσεις διατηρούνται και στα σύνολα των ρόλων και των δεδομένων που επίσης συνιστούν βασικές έννοιες του μοντέλου. Οι ιεραρχίες και οι συσχετίσεις που αυτές περικλείουν επιτρέπουν την κληρονομικότητα χαρακτηριστικών μεταξύ των συζευγμένων κόμβων και επομένως μια πιο αποδοτική προδιαγραφή κανόνων. Τέλος, το μοντέλο Pu-BAC αξιοποιεί την έννοια του «ρόλου υπό προϋποθέσεις» (Conditional Role) στοχεύοντας στην περιγραφή του φαινομένου της ενεργοποίησης ή της απενεργοποίησης κάποιου ρόλου ανάλογα με την ισχύ ή μη αντίστοιχα κάποιων δηλωμένων συνθηκών. Οι συνθήκες που λαμβάνονται υπόψη αναφέρονται είτε σε γνωρίσματα των εμπλεκόμενων ρόλων είτε σε μεταβλητές (χωρικές και χρονικές) του συστήματος.

3.2.1.2 Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση του Σκοπού (Purpose-Aware Role-Based Access Control – PuRBAC)

Το μοντέλο Ελέγχου Πρόσβασης Βάσει Ρόλων με Επίγνωση του Σκοπού [65] αποτελεί επέκταση του παραδοσιακού RBAC μοντέλου. Κεντρική θέση στο μοντέλο κατέχει η έννοια της αδειοδότησης (permission) η οποία υποδεικνύει μια θετική απάντηση σε κάποιο αίτημα για πρόσβαση σε δεδομένα. Ο σκοπός πρόσβασης σύμφωνα με το σχήμα PuRBAC αποτελεί εννοιολογικά μια οντότητα ενδιάμεση των εμπλεκόμενων ρόλων και των αδειοδοτήσεων. Μονάδες του συνόλου των ρόλων συσχετίζονται με αυτές του συνόλου των σκοπών και οι τελευταίες με τη σειρά τους συνδέονται με συγκεκριμένες αδειοδοτήσεις. Επομένως, οντότητες οι οποίες επιθυμούν πρόσβαση σε δεδομένα υποχρεούνται να βεβαιώσουν ρητά τον υποκείμενο σκοπό της αιτούμενης πρόσβασης. Το μοντέλο PuRBAC, όπως και το Pu-BAC, αξιοποιεί ιεραρχίες για την αποδοτική προδιαγραφή κανόνων ασφάλειας.
Αναφορικά με τη διαχείριση και τον έλεγχο των αδειοδοτήσεων, εξετάζεται η ισχύς συγκεκριμένων συνθηκών οι οποίες και ενσωματώνουν στις πιθανές αδειοδοτήσεις περιορισμούς πρόσβασης και υποχρεώσεις των συμβαλλόμενων. Οι προδιαγραμμένες συνθήκες έχουν ποιοτικό χαρακτήρα (είτε ισχύουν είτε όχι) και ανάλογα με τον βαθμό της ικανοποίησής τους οδηγούν σε μια βαθμωτή εξουσιοδότηση, σε αντίθεση με τον τρόπο λειτουργίας παραδοσιακών μοντέλων πρόσβασης που επιστρέφουν αποκλειστικά θετικές ή αρνητικές αποφάσεις. Οι συνθήκες καλύπτουν χρονικές παραμέτρους καθώς και πληθώρα άλλων περιορισμών όπως είναι η απαίτηση για συγκατάθεση του χρήστη και η χρονική οριοθέτηση χρήσης των δεδομένων.

3.2.1.3 Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση της Ιδιωτικότητας (Privacy-Aware Role Based Access Control – P-RBAC)

Το σχήμα P-RBAC [66] ενσωματώνει έννοιες για την αντιμετώπιση των πλέον σημαντικών αρχών της προστασίας προσωπικών δεδομένων και ενίσχυσης της ιδιωτικότητας στα πληροφοριακά συστήματα. Η εξέταση του σκοπού αλλά και των συνθηκών της πρόσβασης σε δεδομένα καθώς και η επιβολή περιορισμών και υποχρεωτικών ενεργειών στην πρόσβαση αυτή αποτελούν τμήμα της λογικής και του φορμαλισμού του μοντέλου. Οι προαναφερθείσες έννοιες, όπως και αυτές των ρόλων

και των δεδομένων ορίζονται στο πλαίσιο της συνεργασίας τεσσάρων προηγμένων μοντέλων με διαφορετικές δυνατότητες μοντελοποίησης.

Το κεντρικό μοντέλο (Core P-RBAC) περιγράφει τα σύνολα των οντοτήτων των χρηστών, των ρόλων, των δεδομένων, των ενεργειών, των σκοπών, των υποχρεώσεων και των συνθηκών σε μια προσαρμοστική γλώσσα που καλείται LC_0. Στόχο του Core P-RBAC αποτελεί η διατήρηση εκείνου του επιπέδου της εκφραστικότητας που θα επιτρέψει σε τυχόν υλοποιήσεις του μοντέλου να είναι συμβατές με τις αρχές ιδιωτικότητας διεθνών οργανισμών όπως είναι ο OECD. Βασισμένο στο κλασσικό σχήμα του RBAC το Core P-RBAC στηρίζει τις αποφάσεις πρόσβασης σε συσχετίσεις αδειοδοτήσεων και ρόλων. Ωστόσο οι έννοιες των συνθηκών και των περιορισμών διαχωρίζονται ρητά στο μοντέλο, με τους περιορισμούς να αξιοποιούνται ως μηχανισμός προδιαγραφής πολιτικών και τις συνθήκες ως μέσο επαρκούς καθορισμού μιας αδειοδότησης.

Το ιεραρχικό μοντέλο Hierarchical P-RBAC εισάγει τις δενδρικές ιεραρχίες ρόλων, δεδομένων και σκοπών, ενισχύοντας ουσιαστικά το κεντρικό μοντέλο με μια πιο διεξοδική μοντελοποίηση. Στο ίδιο πνεύμα, το «υπό όρους» μοντέλο (Conditional P-RBAC) ενεργοποιεί σύνολα παροχής αδειοδοτήσεων και μαθηματικών εκφράσεων της άλγεβρας Boole με στόχο την ενίσχυση της εκφραστικότητας του μοντέλου Core P-RBAC αναφορικά με την προδιαγραφή συνθηκών. Τέλος το γενικό μοντέλο Universal P-RBAC συνδυάζει τα γνωρίσματα και τις λειτουργίες των μοντέλων Conditional P-RBAC και Hierarchical P-RBAC.

3.2.2 Μοντέλα με Επίγνωση Πλαισίου

Η έννοια πλαίσιο, υπό το πρίσμα των μοντέλων ελέγχου πρόσβασης, αποτελεί έναν σχετικά ασαφή όρο και χρησιμοποιείται για να συγκεκριμενοποιήσει κάθε είδους πληροφορία που προδιαγράφει ή ταυτοποιεί μια κατάσταση. Ένα μοντέλο με επίγνωση πλαισίου είναι σε θέση να λαμβάνει υπόψη τόσο στατικές πληροφορίες του περιβάλλοντος του μοντέλου, όπως είναι τα χαρακτηριστικά του αιτούντα για πρόσβαση σε δεδομένα όσο και δυναμικές πληροφορίες, όπως είναι η κατάσταση του συστήματος την ώρα της αίτησης. Είθισται τα μοντέλα ελέγχου πρόσβασης με επίγνωση πλαισίου να αξιοποιούν χρονικά, χωρικά και ιστορικά δεδομένα ως κριτήρια στη λήψη αποφάσεων πρόσβασης. Προφανώς, η ενσωμάτωση μηχανισμών επίγνωσης πλαισίου σε ένα μοντέλο ελέγχου πρόσβασης αυξάνει θεαματικά την

εκφραστικότητα του μοντέλου και το εύρος του πεδίου εφαρμογής του, καθώς παρέχει τη δυνατότητα στα πληροφοριακά συστήματα που το υιοθετούν να προσαρμόζουν κλιμακούμενα τη συμπεριφορά τους ανάλογα με την ισχύ ή μη πλήθους διαφορετικών συνθηκών. Ακόλουθα παρουσιάζονται οι πιο σημαντικές προσεγγίσεις αναφορικά με την επίγνωση πλαισίου στα μοντέλα ελέγχου πρόσβασης και πιο συγκεκριμένα σχετικά με την αξιοποίηση γεωγραφικών, χρονικών και ιστορικών δεδομένων για τη λήψη ακριβέστερων και επίκαιρων αποφάσεων πρόσβασης.

3.2.2.1 Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Χωρικών Δεδομένων (Spatially Aware RBAC – GEO-RBAC)

Το μοντέλο GEO-RBAC [67] αποτελεί μια επέκταση του RBAC η οποία ενισχύει το κλασσικό μοντέλο με μια διεξοδική προδιαγραφή χωρικών περιορισμών. Προς τούτο το μοντέλο εισάγει την έννοια του χωρικού ρόλου και αξιοποιεί ένα αναλυτικό γεωμετρικό σχήμα αναπαράστασης χωρικών δεδομένων σχετικά με αντικείμενα, τοποθεσίες και ρόλους. Ένας χωρικός ρόλος στο μοντέλο νοείται ως η ενεργοποίηση του συγκεκριμένου ρόλου μόνο στην περίπτωση που αυτός εμπίπτει εντός των χωρικών περιορισμών που έχουν προδιαγραφεί.

Το GEO-RBAC συναποτελείται από τρία μοντέλα. Το κεντρικό μοντέλο (Core GEO-RBAC) προδιαγράφει τις βασικές οντότητες του μοντέλου, όπως είναι οι χωρικοί ρόλοι και τα χωρικά αντικείμενα, η πραγματική και η λογική θέση χρήστη και η ενεργοποίηση ρόλων. Οι έννοιες αυτές αποτελούν το πεδίο εφαρμογής των υπόλοιπων υπό-μοντέλων του GEO-RBAC. Τουτέστιν το ιεραρχικό GEO-RBAC εμπλουτίζει το κεντρικό μοντέλο με ιεραρχίες ρόλων, υποστηρίζοντας την κληρονομικότητα χαρακτηριστικών, αδειοδοτήσεων αλλά και ενεργοποιήσεων των ρόλων, ενώ το περιοριστικό μοντέλο (Constrained GEO-RBAC) προδιαγράφει περιορισμούς διαχωρισμού των καθηκόντων. Μάλιστα οι εν λόγω περιορισμοί είναι δυνατόν να ορίζονται σε διαφορετικές εννοιολογικές διαστάσεις, καλύπτοντας τις περιπτώσεις διαχωρισμού καθηκόντων βάσει ρόλων, χωρικών δεδομένων καθώς και χρονικών συνθηκών. Το προδιαγραφόμενο σύνολο περιορισμών αποτελεί την κύρια συνεισφορά του μοντέλου αναφορικά με την υποστήριξη ελέγχου πρόσβασης με

χωρικά κριτήρια για εφαρμογές που βασίζονται στην τοποθεσία (location based applications).

3.2.2.2 Γενικευμένος Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Χρονικών Δεδομένων (Generalized Temporal Role Based Access Control – GTRBAC)

Το μοντέλο GTRBAC [68] συνιστά επίσης μια επέκταση του συμβατικού RBAC, η οποία μοντελοποιεί και συστηματοποιεί τη διαχείριση χρονικών εξουσιοδοτήσεων. Προς τούτο, αναγνωρίζεται η ανάγκη για διάκριση των καταστάσεων στις οποίες μπορεί να βρεθεί ένας ρόλος και επομένως το σχήμα προδιαγράφει τις ακόλουθες καταστάσεις ενός ρόλου: απενεργοποιημένος (disabled), ενεργοποιημένος (enabled) και δραστηριοποιημένος (activated). Στην απενεργοποιημένη κατάσταση ο ρόλος δεν δύναται να αξιοποιηθεί από κανένα χρήστη, δηλαδή καμιά οντότητα δεν μπορεί να λάβει τις αδειοδοτήσεις που σχετίζονται με το συγκεκριμένο ρόλο. Στην ενεργοποιημένη κατάσταση, οι χρήστες που είναι εξουσιοδοτημένοι να χρησιμοποιήσουν τον ρόλο τη στιγμή της αίτησης μπορούν να τον μεταφέρουν στη δραστηριοποιημένη του μορφή. Ένας ρόλος σε δραστηριοποιημένη κατάσταση ισοδυναμεί με την ύπαρξη τουλάχιστον μιας οντότητας που τον έχει αξιοποιήσει. Ο - αυτός συνιστά και το βασικό υπόβαθρο του μοντέλου. Επιπρόσθετα, το GTRBAC παρουσιάζει μεγάλη εκφραστικότητα αναφορικά με την προδιαγραφή περιορισμών. Έτσι το μοντέλο υποστηρίζει χρονικούς περιορισμούς για την αδειοδότηση, την ενεργοποίηση και τη δραστηριοποίηση ρόλων καθώς και για την εξουσιοδότηση χρηστών προς αξιοποίηση ρόλων. Επιπλέον επιτρέπει την αναγνώριση δυναμικών γεγονότων (runtime events) και την κατάλληλη πυροδότηση απαντητικών μηχανισμών (triggers).

3.2.2.3 Γενικευμένο Χρονικό Μοντέλο Ελέγχου Πρόσβασης με Επίγνωση Ιστορικών Δεδομένων (Generalized Temporal History Based Access Control Model – GTHBAC)

Το Γενικευμένο Χρονικό Μοντέλο Ελέγχου Πρόσβασης με Επίγνωση Ιστορικών Δεδομένων [69] συνιστά ένα πλαίσιο μοντελοποίησης και αξιοποίησης ιστορικών δεδομένων στη λήψη αποφάσεων πρόσβασης. Σε αντίθεση με τα προαναφερθέντα μοντέλα το GTHBAC δεν είναι επικεντρωμένο στην έννοια του ρόλου και αξιοποιεί πιο γενικευμένες έννοιες, όπως είναι το υποκείμενο, το αντικείμενο και η ενέργεια ως θεμέλιο των κανόνων πρόσβασης. Ωστόσο, ρόλοι και λοιπά χαρακτηριστικά χρηστών λαμβάνονται υπόψη ως γνωρίσματα οντοτήτων κατά την προδιαγραφή των κανόνων. Μάλιστα το μοντέλο αξιοποιεί τη χρήση πιστοποιητικών ιδιοτήτων X.509 για την αναπαράσταση των χαρακτηριστικών του χρήστη.

Κριτήρια στη διαδικασία λήψης αποφάσεων ελέγχου πρόσβασης, συνιστούν τα πιστοποιητικά ιδιοτήτων του χρήστη, τα υπάρχοντα ιστορικά στοιχεία πρόσβασης σε δεδομένα, οι κανόνες πρόσβασης που έχουν προδιαγραφεί καθώς και οι σχετικοί περιορισμοί. Για την περιγραφή πολιτικών πρόσβασης με επίγνωση ιστορικών στοιχείων, οι κανόνες εξουσιοδότησης αναπαριστούνται ως τριάδες που περιέχουν: ένα έγκυρο χρονικό διάστημα εξουσιοδότησης, ένα σύνολο προσδιορισμού του υποκειμένου, του αντικειμένου και της ενέργειας της εξουσιοδότησης και τέλος μια αναλυτική προδιαγραφή χρονικών περιορισμών για τον συγκεκριμένο κανόνα. Σημαντική συνεισφορά του μοντέλου αποτελεί και η ενδελεχής περιγραφή στρατηγικών επίλυσης αντιφάσεων, όπως είναι οι στρατηγικές υπερίσχυσης του αρνητικού ή του θετικού κανόνα ή αυτές της υπερίσχυσης του νεότερου ή του ειδικότερου κανόνα. Αξίζει να σημειωθεί ότι η γενική μοντελοποίηση των περιορισμών σε ιστορικά δεδομένα και η ενσωμάτωσή τους σε ένα αρκετά γενικευμένο μοντέλο ελέγχου πρόσβασης όπως το περιγραφόμενο, αυξάνουν σημαντικά την επεκτασιμότητα και την εφαρμοστικότητα του GTHBAC, καθώς το υποκείμενο μοντέλο δύναται είτε να ενισχυθεί με μεγαλύτερη εκφραστικότητα είτε να αντικατασταθεί πλήρως από κάποιο άλλο προηγμένο μοντέλο.

3.2.2.4 Σημασιολογικό Χρονικό Μοντέλο Ελέγχου Πρόσβασης (Temporal Semantic-Based Access Control Model – TSBAC)

Το μοντέλο TSBAC model [70] ενσωματώνει σε γενικές γραμμές τα ίδια χαρακτηριστικά με το σχήμα GTHBAC που παρουσιάστηκε στην προηγούμενη ενότητα, με τη διαφοροποίηση ότι αξιοποιεί τεχνολογίες σημασιολογικού ιστού και πιο συγκεκριμένα οντολογίες προδιαγραμμένες στη γλώσσα αναπαράστασης γνώσης Web Ontology Language (OWL) [71] για την περιγραφή των βασικών οντοτήτων του πλαισίου λειτουργίας του. Έτσι οι γενικευμένοι όροι του υποκειμένου, αντικειμένου και της ενέργειας του GTHBAC, στο TSBAC οργανώνονται στις ακόλουθες οντολογίες: Οντολογία Υποκειμένων, Οντολογία Αντικειμένων και Οντολογία Ενεργειών. Η ενσωμάτωση των οντολογιών και των σχετικών συσχετίσεων στην περιγραφή του μοντέλου στόχο έχει την εκμετάλλευση των εκφραστικών δυνατοτήτων των σημασιολογικών τεχνολογιών και τη συνεπακόλουθη αποδοτικότερη εξαγωγή συμπερασμάτων κατά τη λήψη αποφάσεων ελέγχου πρόσβασης.

3.2.3 Μοντέλα για κατανεμημένα περιβάλλοντα

Η ολοένα και εντονότερη αποκέντρωση των σύγχρονων πληροφοριακών συστημάτων έχει οδηγήσει τις εμπλεκόμενες οντότητες στην υιοθέτηση μοντέλων ελέγχου πρόσβασης που παρουσιάζουν γνωρίσματα προσαρμοσμένα στις απαιτήσεις κατανεμημένων περιβαλλόντων. Η επίγνωση της υποκείμενης ετερογένειας των αλληλεπιδρώντων φορέων και η αναγνώριση της ανάγκης για διαλειτουργικότητα αποτελούν τον οδηγό σχεδίασης και υλοποίησης των σχετικών μοντέλων. Στη συνέχεια αναλύονται δύο από τις πλέον σημαντικές προσεγγίσεις μοντέλων για κατανεμημένα περιβάλλοντα που έχουν προταθεί στη βιβλιογραφία.

3.2.3.1 Έλεγχος Πρόσβασης Βάσει Οργανισμών (Organization Based Access Control – OrBAC)

Στόχο του μοντέλου Or-BAC [72] συνιστά η υποστήριξη ενός πλαισίου προδιαγραφής πολιτικών με έμφαση στην ιδιωτικότητα και στη σύλληψη των δυναμικών και ευέλικτων σχέσεων μεταξύ οντοτήτων σε περιβάλλοντα

αλληλεπίδρασης οργανισμών. Κεντρική έννοια του μοντέλου αποτελεί αυτή του Οργανισμού, της οντότητας δηλαδή που είναι υπεύθυνη για τη διαμόρφωση μιας πολιτικής ασφάλειας. Οι κανόνες στο Or-BAC μοντελοποιούνται ακολουθώντας μια προσέγγιση ανεξαρτητοποίησης από λεπτομέρειες που υφίστανται σε επίπεδο υλοποίησης. Οι έννοιες του υποκειμένου, του αντικειμένου και της ενέργειας στο Or-BAC αντιμετωπίζονται υπό το πρίσμα του ρόλου που διαδραματίζουν αυτές εντός του Οργανισμού, διαμορφώνοντας έτσι τις έννοιες του ρόλου, της εικόνας και της δραστηριότητας αντίστοιχα. Οι κανόνες πρόσβασης στο μοντέλο αντιστοιχούν σε αδειοδοτήσεις, απαγορεύσεις, υποχρεώσεις και εξαιρέσεις αναφορικά με τις δραστηριότητες που εφαρμόζουν ρόλοι σε εικόνες εντός του Οργανισμού.

Η έννοια του πλαισίου συνιστά για το Or-BAC κεντρική οντότητα και προς τούτο το μοντέλο παρέχει δυνατότητες προδιαγραφής πληθώρας τύπων συνθηκών, όπως χρονικές, χωρικές, προαπαιτούμενες, προσωρινές και καθορισμένες από τον χρήστη. Κάθε προδιαγραφόμενη συνθήκη δύναται να συνδυαστεί με άλλες μέσω συνδυαστικών, συζευκτικών ή αποκλειόμενων σχέσεων. Γενικοί περιορισμοί πρόσβασης προδιαγράφονται στο μοντέλο με τη μορφή συνθηκών που ενσωματώνονται στους κανόνες πρόσβασης και καθορίζουν την ισχύ τους. Επιπρόσθετα, υπό τη μορφή προσωρινών συνθηκών δύνανται να προδιαγραφούν περιορισμοί σχετικά με το ιστορικό των προσβάσεων, ενισχύοντας ακόμα περισσότερο το εύρος της εκφραστικότητας του μοντέλου. Επίσης, ως συνθήκη ορισμένη από τον χρήστη προβλέπεται και η ενσωμάτωση της έννοιας του σκοπού στο μοντέλο [73]. Προς τούτο, τη στιγμή της αίτησης για πρόσβαση σε δεδομένα ο αιτών καλείται να δηλώσει τον σκοπό του, οι οποίοι στο μοντέλο έχουν ήδη συσχετιστεί με συγκεκριμένους ρόλους. Με τον ίδιο τρόπο προδιαγράφεται και η εξασφάλιση της συγκατάθεσης του χρήστη όταν η πρόσβαση αφορά δεδομένα που τον αφορούν, ενώ προσωρινές συνθήκες μπορούν να εξυπηρετήσουν και τους σκοπούς ενός ελέγχου χρήσης των συγκεντρωμένων δεδομένων.

Σημειώνεται ότι προς διευκόλυνση διαμόρφωσης των κανόνων ελέγχου πρόσβασης οι ρόλοι, οι δραστηριότητες, οι εικόνες, οι συνθήκες βρίσκονται οργανωμένες σε ιεραρχίες όπου ισχύει η κληρονομικότητα αδειοδοτήσεων, απαγορεύσεων, υποχρεώσεων και εξαιρέσεων. Καθώς οι κληρονομικότητες των ιεραρχικών σχέσεων μπορεί να οδηγήσουν σε συγκρούσεις μεταξύ θετικών και αρνητικών εξουσιοδοτήσεων, το μοντέλο περιγράφει στρατηγικές αναγνώρισης αλλά και επίλυσης πιθανών αντιφάσεων [74].

3.2.3.2 Προδιαγραφή Πολιτικών και Αρχιτεκτονική για Έλεγχο Πρόσβασης σε Επιχειρήσεις Βάση της Γλώσσας Σήμανσης XML (XML-Based Policy Specification Framework and Architecture for Enterprise-Wide Access Control – X-GTRBAC)

Το σύστημα X-GTRBAC [75] ενσωματώνει όλα τα χαρακτηριστικά του μοντέλου GTRBAC και εμπλουτίζει τη λειτουργία του αξιοποιώντας μια γλώσσα προδιαγραφής πολιτικών βασισμένη στη γλώσσα σήμανσης Extensible Markup Language (XML) [76]. Οι λειτουργικότητές του συστήματος X-GTRBAC έχουν σχεδιαστεί έτσι ώστε να καλύπτουν τις απαιτήσεις για δυναμικό έλεγχο πρόσβασης των σύγχρονων πληροφοριακών συστημάτων σε ετερογενή και κατανεμημένα επιχειρηματικά περιβάλλοντα. Κύριο εργαλείο για την προσαρμογή του συστήματος σε ένα τέτοιο πλαίσιο λειτουργίας αποτελεί η γλώσσα XML η οποία προσφέρει τις ποιότητες της ευελιξίας και διαλειτουργικότητας στην προδιαγραφή και εφαρμογή των κανόνων πρόσβασης. Με αυτό τον τρόπο το μοντέλο ενώ διατηρεί τις δυνατότητες προδιαγραφής χρονικών περιορισμών του μοντέλου GTRBAC τις επεκτείνει με ένα σχήμα προδιαγραφής περιορισμών και διαπιστευτηρίων βασισμένο σε γνωρίσματα. Ο όρος «διαπιστευτήρια» στο X-GTRBAC συνιστά έναν οδηγό ομαδοποίησης χρηστών που παρουσιάζουν κοινά γνωρίσματα. Σε αυτό το πλαίσιο, μια οντότητα για να ενεργοποιήσει ένα ρόλο καλείται να ικανοποιήσει τις απαιτήσεις σε διαπιστευτήρια και γνωρίσματα που έχουν συσχετιστεί με τον συγκεκριμένο ρόλο.

3.2.4 Μοντέλα με επίγνωση γνωρισμάτων χρηστών

Τα μοντέλα ελέγχου πρόσβασης με επίγνωση των χαρακτηριστικών χρηστών αποτελεί μια ειδική κατηγορία μοντέλων, όπου η απόφαση για πρόσβαση δεν βασίζεται στα δικαιώματα που έχουν συσχετιστεί με τον κάθε αιτούντα πρόσβασης αλλά στα χαρακτηριστικά γνωρίσματα του αιτούντα. Τα γνωρίσματα των χρηστών συνιστούν τις δομικές μονάδες προδιαγραφής τόσο των αιτημάτων όσο και των κανόνων ελέγχου πρόσβασης. Σε ένα τέτοιο πλαίσιο λειτουργίας, οι πολιτικές πρόσβασης συσχετίζουν τα δεδομένα υπό προστασία με αδειοδοτήσεις και συγκεκριμένα χαρακτηριστικά χρηστών. Ακόλουθα, ο χρήστης πρέπει να

παρουσιάσει αποδείξεις πιστοποίησης των συγκεκριμένων χαρακτηριστικών για να επιτύχει πρόσβαση στα δεδομένα.

3.2.4.1 Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (Extensible Access Control Markup Language – XACML)

Ίσως το πλέον χαρακτηριστικό παράδειγμα σχήματος με επίγνωση των γνωρισμάτων χρηστών, συνιστά η Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML) [77]. Προδιαγραφή του Οργανισμού για τη Διαμόρφωση Προτύπων Δομημένων Πληροφοριών (Organization for the Advancement of Structured Information Standards – OASIS) [78] η γλώσσα XACML ακολουθεί το αφαιρετικό μοντέλο για την εφαρμογή πολιτικών που έχει προταθεί από τον Διεθνή Οργανισμό Τυποποίησης και την Εντολοδόχο Μηχανολογική Ομάδα Διαδικτύου (Internet Engineering Task Force – IETF) [79] σύμφωνα με το οποίο η διαδικασία έκδοσης απόφασης σχετικά με την πρόσβαση σε προστατευόμενο πόρο εμπλέκει συγκεκριμένες οντότητες με διακριτές λειτουργίες. Πιο συγκεκριμένα, αναγνωρίζονται:

- Το Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point – PEP), το οποίο αποτελεί την οντότητα που είναι υπεύθυνη για τη αποδοχή όλων των αιτημάτων πρόσβασης. Μετά τη συλλογή η οντότητα καλείται να συντάξει διεξοδικά ένα νέο αίτημα εξουσιοδότησης προς αποστολή στο Σημείο Απόφασης Πολιτικής (Policy Decision Point – PDP) το οποίο περιλαμβάνει όλα τα σχετικά με την αίτηση στοιχεία. Μετά την απάντηση που ακολουθεί και ανάλογα με το περιεχόμενο της το σημείο PEP είναι υπεύθυνο για την εφαρμογή ή μη της αδειοδότησης για πρόσβαση.
- Το Σημείο Απόφασης Πολιτικής, συνιστά την οντότητα που βρίσκεται υπεύθυνη για τη λήψη αποφάσεων πρόσβασης μετά από κάποιο σχετικό αίτημα από το σημείο PEP. Προς τούτο, η οντότητα PDP συλλέγει όλες τις πολιτικές πρόσβασης που σχετίζονται με το αίτημα και εξετάσει την ισχύ τους υπό το πρίσμα δεδομένων του αιτήματος αλλά και οποιασδήποτε άλλης πληροφορίας μπορεί να επηρεάζει την εγκυρότητα ή μη κάθε πολιτικής. Το αποτέλεσμα της αποτίμησης των πολιτικών μεταφέρεται πίσω στην οντότητα PEP.
- Το Σημείο Διαχείρισης Πολιτικής (Policy Administration Point – PAP), συνιστά την οντότητα που είναι υπεύθυνη για τη δημιουργία και τη διαχείριση

των πολιτικών ασφάλειας. Καθώς οι προδιαγραφόμενες πολιτικές αποτελούν το πεδίο εργασίας του σημείου PDP, καθήκον του σημείου PAP συνιστά και η διατήρηση των κατάλληλων καναλιών επικοινωνίας και αλληλεπίδρασης για διαμοιρασμό των κατάλληλων πολιτικών.

- Το Σημείο Πληροφοριών Πολιτικής (Policy Information Point – PIP), αναφέρεται στην οντότητα που είναι υπεύθυνη για τη συλλογή πληροφοριών που μπορεί να επηρεάζουν τη λήψη αποφάσεων πρόσβασης του σημείου PDP. Τέτοιες πληροφορίες μπορεί να αφορούν συνθήκες περιβάλλοντος, γνωρίσματα χρηστών και ιδιότητες πόρων. Προς τούτο, το σημείο PIP διατηρεί διόδους επικοινωνίας με το σημείο PDP.

Τα βασικά δομικά συστατικά για τον καθορισμό μιας πολιτικής ελέγχου στη γλώσσα XACML είναι ο κανόνας (Rule), η πολιτική (Policy) και το σύνολο των πολιτικών (Policy Set). Ένας κανόνας αποτελείται από ένα στόχο που αναφέρεται στο σύνολο των αιτημάτων με το οποίο ο κανόνας σχετίζεται, ένα αποτέλεσμα που αναπαριστά την απόφαση που επιφέρει η ισχύς του κανόνα, μια σειρά συνθηκών που καθορίζουν την ενεργοποίηση του κανόνα, μια σειρά υποχρεώσεων που δεσμεύουν την εφαρμογή του κανόνα και ένα σύνολο συμβουλευτικών οδηγιών. Μεταξύ των οντοτήτων ενός συστήματος δεν πραγματοποιείται ανταλλαγή κανόνων αλλά μόνο πολιτικών. Επακόλουθα, βασικό συστατικό των πολιτικών αποτελεί ένα σύνολο από κανόνες που συνδυάζονται υπό την αιγίδα της εκάστοτε πολιτικής. Επιπλέον, μια πολιτική περιλαμβάνει ένα στόχο, που υποδεικνύει τα αιτήματα για τα οποία ενεργοποιείται η πολιτική, έναν αλγόριθμο που προσδιορίζει τη λογική με την οποία το σύνολο των κανόνων ομαδοποιήθηκε και μια σειρά συνοδευτικών υποχρεώσεων και συμβουλευτικών οδηγιών. Τέλος οι πολιτικές ομαδοποιούνται και δημιουργούν σύνολα πολιτικών που δομούνται με τον ίδιο ακριβώς τρόπο.

Η οργανωτική δομή των κανόνων ελέγχου πρόσβασης αλλά και η υποστήριξη του συγκεκριμένου αφαιρετικού μοντέλου αρχιτεκτονικής, όπως περιγράφηκαν παραπάνω επιτρέπουν στη XACML:

- τον συνδυασμό αυτόνομων κανόνων και πολιτικών σε ένα σύνολο Policy Set και την εφαρμογή του σε συγκεκριμένο σημείο PDP,
- τη διαχείριση κατανεμημένων συνόλων πολιτικών,
- την υποστήριξη ενός αφαιρετικού επιπέδου προδιαγραφής πολιτικών ανεξάρτητο από τις λεπτομέρειες του πεδίου εφαρμογής,

- την περιγραφή του τρόπου και του λόγου ομαδοποίησης πολιτικών και κανόνων,
- την υποστήριξη της επίγνωσης χαρακτηριστικών διαφορετικών οντοτήτων, συνθηκών περιβάλλοντος αλλά και ιδιοτήτων των πόρων κατά τη λήψη αποφάσεων και
- τη διαχείριση κατανεμημένων συνόλων πολιτικών

3.2.4.2 Εκτεταμένο Προφίλ Ελέγχου Πρόσβασης Βάσει Ρόλων για τη Γλώσσα Σήμανσης XACML (Extended RBAC Profile of XACML)

Το μοντέλο Extended RBAC Profile of XACML αποτελεί μια προσέγγιση ειδίκευσης ενός πλαισίου βασισμένου σε χαρακτηριστικά χρηστών, όπως είναι το XACML, προς υλοποίηση του κλασσικού RBAC μοντέλου. Η προσέγγιση αυτή υποδηλώνει ότι στον τομέα των μοντέλων ελέγχου πρόσβασης, ο διαχωρισμός των σχημάτων ανάλογα με τις λειτουργικότητές τους δεν είναι απόλυτα ακριβής και συνήθως διεξάγεται με κριτήριο τις ειδικότερες στοχεύσεις και στρατηγικές κάθε μοντέλου. Αφορμή για την προσέγγιση του συγκεκριμένου μοντέλου αποτέλεσε η διάγνωση αδυναμιών στο πρότυπο του οργανισμού OASIS σχετικά το Προφίλ Ελέγχου Πρόσβασης Βάσει Ρόλων για τη Γλώσσα Σήμανσης XACML (RBAC Profile of XACML) [80]. Πιο συγκεκριμένα, το πλαίσιο RBAC Profile of XACML επεκτείνει τη γλώσσα XACML με δυνατότητες επίγνωσης της έννοιας του ρόλου κατά τη διαμόρφωση πολιτικών ελέγχου πρόσβασης. Ωστόσο, το πρότυπο λαμβάνει υπόψη του μόνο το κεντρικό και ιεραρχικό μοντέλο του RBAC και δεν προσφέρει τα απαραίτητα εκφραστικά μέσα για την κάλυψη του περιοριστικού μοντέλου του RBAC. Παραδοσιακά σημαντικές αρχές ιδιωτικότητας και ασφάλειας όπως είναι ο διαχωρισμός καθηκόντων – στατικός και δυναμικός – επίσης δεν υποστηρίζονται. Επιπρόσθετα ο τρόπος με τον οποίον διαχειρίζονται οι ιεραρχίες ρόλων καθιστά αδύνατη τη μερική μεταφορά δικαιωμάτων μεταξύ ρόλων.

Προς διευκόλυνση της διαχείρισης των κανόνων ελέγχου το μοντέλο αξιοποιεί αφηρημένες οντότητες και μάλιστα αξιοποιεί τη ορολογία του μοντέλου OrBAC για την περιγραφή των βασικών του εννοιών. Τουτέστιν, οι εικόνες αναπαριστούν και κατηγοριοποιούν πόρους του συστήματος με κοινές ιδιότητες, οι δραστηριότητες ομαδοποιούν ενέργειες που αντιστοιχούν στην ίδια διαδικασία, ενώ οι ρόλοι

αντιστοιχούν στις οντότητες του συστήματος. Επίσης σε συμφωνία με το OrBAC το σχήμα Extended RBAC Profile of XACML ενεργοποιεί μηχανισμούς επίγνωσης πλαισίου, υποστηρίζοντας την προδιαγραφή διαφορετικούς τύπους συνθηκών όπως χρονικές, χωρικές, προαπαιτούμενες, προσωρινές και καθορισμένες από τον χρήστη.
Το Εκτεταμένο Προφίλ επεκτείνει επίσης τη λειτουργικότητα της οντότητας Αρχή Ενεργοποίησης Ρόλου (AEP) που εισάγεται στο απλό προφίλ. Σύμφωνα με το πρότυπο του οργανισμού OASIS η εν λόγω Αρχή είναι υπεύθυνη για την απόδοση ρόλων σε οντότητες ανάλογα με το περιεχόμενο συγκεκριμένων κανόνων (Κανόνες Απόδοσης Ρόλων). Στο Εκτεταμένο Προφίλ προδιαγράφεται η λειτουργία τεσσάρων Αρχών Ενεργοποίησης κάθε μία από τις οποίες βρίσκεται υπεύθυνη για την απόδοση συγκεκριμένων τιμών στις αφηρημένες έννοιες που βρίσκονται υπό την αιγίδα τους σύμφωνα με τους καθορισμένους κανόνες ενεργοποίησης. Η λειτουργία της AEP παραμένει ίδια με αυτή του πρωτότυπου μοντέλου, ενώ η Αρχή Ενεργοποίησης Δραστηριοτήτων, η Αρχή Ενεργοποίησης Εικόνων και η Αρχή Ενεργοποίησης Πλαισίων είναι υπόλογες για τη συσχέτιση δραστηριοτήτων με αντικείμενα, την αντιστοίχιση ενεργειών σε δραστηριότητες και τη σύνδεση πλαισίων με συγκεκριμένες συνθήκες.

3.2.5 Κοινά γνωρίσματα

Τα ανωτέρω μοντέλα ελέγχου πρόσβασης διακρίνονται από ένα σύνολο επιμέρους χαρακτηριστικών που επηρεάζουν σημαντικά τη λειτουργία τους και τη συμπεριφορά τους σε ειδικές συνθήκες, διαφοροποιούν ουσιαστικά τη στοχοθεσία τους και εν τέλει τα καθιστούν κατάλληλα ή μη για εφαρμογή σε διαφορετικά περιβάλλοντα. Ωστόσο, η ανάλυση των εν λόγω μοντέλων επισημαίνει μια επανάληψη και επαναχρησιμοποίηση εννοιών και στρατηγικών, οι οποίες συναποτελούν μια κοινή δομική βάση για τον σχεδιασμό μοντέλων ελέγχου πρόσβασης τόσο γενικότερα όσο και ειδικότερα στον χώρο της προστασίας προσωπικών δεδομένων. Στόχος της παρούσας ενότητας είναι η αναγνώριση και η επισήμανση των κοινών αυτών στοιχείων.
Η ενσωμάτωση των **ρόλων** στη διαδικασία προσδιορισμού κανόνων πρόσβασης, ως έννοια ενδιάμεση στους χρήστες ενός συστήματος και στις αδειοδοτήσεις για πρόσβαση σε δεδομένα, έδωσε τη δυνατότητα για μια αποδοτικότερη διαχείριση των χρηστών και των δικαιωμάτων τους και πλέον αποτελεί γνώρισμα μιας μεγάλης

ομάδας μοντέλων ελέγχου πρόσβασης που συναντούνται στη βιβλιογραφία ως επεκτάσεις του πρωτότυπου RBAC μοντέλου και όχι μόνο. Πιο συγκεκριμένα, το χαρακτηριστικό αυτό συνίσταται στη μετάβαση από την απλή και άμεση, δύσχρηστη ωστόσο προσέγγιση της προδιαγραφής σειράς κανόνων αδειοδότησης για κάθε συγκεκριμένο χρήστη, προς την πρακτική της συσχέτισης χρηστών και ρόλων καθώς και ρόλων με αδειοδοτήσεις. Με αυτόν τον τρόπο η περιγραφή κανόνων πρόσβασης «απαγκιστρώνεται» από τους πραγματικούς χρήστες του συστήματος και προσαρμόζεται σε κατάλληλα μοντελοποιημένες ομάδες χρηστών.

Ο **σκοπός πρόσβασης** αποτελεί βασική έννοια που ενσωματώνει και τοποθετεί στον πυρήνα των διαδικασιών λήψης απόφασης πρόσβασης η πλειοψηφία των αναλυθέντων μοντέλων. Σε πλήρη αντιστοιχία με τις αρχές και απαιτήσεις ιδιωτικότητας που αναλύθηκαν σε προηγούμενο κεφάλαιο, ο σκοπός αξιοποιείται ως έννοια για την αναπαράσταση τόσο του δηλωθέντος προτιθέμενου όσο και του προσδιοριζόμενου επιτρεπόμενου στόχου πρόσβασης σε δεδομένα.

Ομοίως, στο κέντρο των λειτουργιών λήψης απόφασης μιας σειράς μοντέλων εντοπίζεται η έννοια των **υποχρεώσεων** η οποία αξιοποιείται προς μοντελοποίηση των υποχρεωτικών ενεργειών που δύναται να συνεπάγεται η πρόσβαση σε συγκεκριμένους πόρους. Τυπικά, το σύνολο των υποχρεώσεων κατηγοριοποιείται ανάλογα με το χρονικό πλαίσιο τέλεσης των αντίστοιχων συνεπαγόμενων ενεργειών σε δύο ευρείς ομάδες: η πρώτη περιλαμβάνει υποχρεώσεις που υποδεικνύουν ενέργειες προς εκπλήρωση πριν την πρόσβαση στους ζητηθέντες πόρους και η δεύτερη περιλαμβάνει υποχρεώσεις προς διεκπεραίωση μετά το πέρας της πρόσβασης.

Μια από τις διακριτές κατηγορίες μοντέλων ελέγχου πρόσβασης που μελετήθηκε στην υποενότητα 3.2.2 αφορά τα μοντέλα με **επίγνωση πλαισίου**. Ωστόσο, η επίγνωση πλαισίου αποτελεί μια ιδιότητα που συναντάται οριζόντια σε πλήθος μοντέλων ανεξάρτητα από την εξειδίκευση των λειτουργιών τους σε συγκεκριμένους τομείς. Η επίγνωση πλαισίου μοντελοποιείται με τη μορφή διαφορετικών κατηγοριών **συνθηκών** που αφενός περιγράφουν το περιβάλλον πρόσβασης σε πόρους ενώ αφετέρου οριοθετούν και νομοθετούν την πρόσβαση αυτή. Είθισται η επίγνωση πλαισίου να οργανώνεται σε τέσσερις άξονες συνθηκών, χωρικών, χρονικών, ιστορικών και γνωρισμάτων των χρηστών. Η παράλληλη ενδελεχής μοντελοποίηση των παραπάνω κατηγοριών ωστόσο, δεν συναντάται συχνά στα υπάρχοντα μοντέλα ελέγχου πρόσβασης τα οποία κατά πλειοψηφία επενδύουν σε συγκεκριμένους τύπους

πλαισίου (και οι οποίοι συνήθως τους προσδίδουν και την ονομασία τους, π.χ. GEO-RBAC). Αξίζει να σημειωθεί ότι η επίγνωση πλαισίου σχετικά με παραμέτρους χρόνου και χρονικούς περιορισμούς εμφανίζει συγκριτικά το μεγαλύτερο ποσοστό υποστήριξης ανάμεσα στα μοντέλα που μελετήθηκαν. Σε κάποιες περιπτώσεις παρατηρείται μια σύζευξη της έννοιας των ρόλων με αυτή των συνθηκών, οδηγώντας στην έννοια των **ρόλων υπό συνθήκη** (conditional roles). Η προδιαγραφή των ρόλων υπό συνθήκη μπορεί να αξιοποιηθεί επιτυχώς σε συγκεκριμένα περιβάλλοντα, στη γενική περίπτωση όμως οδηγεί σε τεχνητούς, σύνθετους και διφορούμενους τύπους ρόλων. Για παράδειγμα, αν το στιγμιότυπο (instance) «Org» αναπαριστά έναν οργανισμό και το στιγμιότυπο «manager» συνιστά ένα ρόλο, ο τεχνητός ρόλος «Org manager» μπορεί να ερμηνευτεί είτε ως ο ρόλος «manager» που εργάζεται στον οργανισμό «Org» ή ως είτε ως ο ρόλος «manager» που βρίσκεται εντοπισμένος εντός του οργανισμού «Org».

Επιπλέον, σε συμμόρφωση με τις οδηγίες των διεθνών προτύπων ασφάλειας, οι λειτουργικότητες μιας σειράς μοντέλων ελέγχου πρόσβασης λαμβάνουν υπόψη δύο μορφές **διαχωρισμού καθηκόντων**, δυναμικό (Dynamic Separation of Duty – DSoD) και στατικό (Static Separation of Duty – SSoD). Ο στατικός διαχωρισμός καθηκόντων αναφέρεται στην προδιαγραφή περιορισμών κατά των ανάθεση ρόλων και αδειοδοτήσεων στους χρήστες ενός συστήματος. Πιο συγκεκριμένα, ένας περιορισμός SSoD είναι δυνατό να απαγορεύει την ταυτόχρονη ανάθεση αυτό-αποκλειόμενων ρόλων στον ίδιο χρήστη, καθώς και να αποκλείει την απόδοση επιπλέον δικαιωμάτων στον ίδιο χρήστη, δεδομένων συγκεκριμένων αδειοδοτήσεων. Από τη φύση του ο SSoD διαχωρισμός καθηκόντων συνιστά έναν στατικό περιορισμό που μπορεί να καθοριστεί και να ελεγχθεί ήδη από τη φάση της προδιαγραφής κανόνων πρόσβασης. Τουναντίον, ο δυναμικός διαχωρισμός καθηκόντων αφορά περιορισμούς, η ισχύς των οποίων δύναται να εξακριβωθεί μόνο σε πραγματικό χρόνο κατά τη διάρκεια λειτουργίας του συστήματος υπό προστασία. Σε αντίθεση με τους SSoD που θέτουν με σαφή και αυστηρό τρόπο κριτήρια ανάθεσης ρόλων και εκτέλεσης λειτουργιών, οι DSoD περιορισμοί προτείνουν μια πιο ευέλικτη διαχείριση διαχωρισμών καθηκόντων, αποκλείοντας όχι την ταυτόχρονη **ανάθεση** ρόλων ή αδειοδοτήσεων αλλά την παράλληλη **ενεργοποίηση** ρόλων και την ταυτόχρονη **εκπλήρωση** πρόσβασης. Το παράδειγμα των διαδικασιών πληρωμής των υπαλλήλων μιας επιχείρησης είναι χαρακτηριστικό για τη διευκρίνιση των διαφορών μεταξύ του στατικού και του δυναμικού διαχωρισμού καθηκόντων: ένας κανόνας SoD ορίζει

ρητά ότι απαγορεύεται ένας υπάλληλος που υπολογίζει τις πληρωμές των υπαλλήλων της επιχείρησης (Υπάλληλος Μισθοδοσίας) ταυτόχρονα να αποτελεί το πρόσωπο που τις εγκρίνει (Υπεύθυνος Μισθοδοσίας). Στη στατική του μορφή ο περιορισμός αυτός θα μπορούσε να επιτευχθεί απαγορεύοντας την ταυτόχρονη ανάληψη των συγκεκριμένων ρόλων από τον ίδιο υπάλληλο. Ωστόσο, γίνεται προφανές ότι στην πράξη αυτός ο περιορισμός είναι πέραν του δέοντος στατικός για τις ανάγκες της επιχείρησης, στο οργανόγραμμα της οποίας οι ρόλοι Υπάλληλος Μισθοδοσίας και Υπεύθυνος Μισθοδοσίας δεν είναι απαραίτητα αυτό-αποκλειόμενοι. Αντίθετα, ένας δυναμικός διαχωρισμός καθηκόντων μπορεί να περιγράψει την απαγόρευση έγκρισης πληρωμής από τον χρήστη/υπάλληλο που απασχολήθηκε στις διαδικασίες υπολογισμού της συγκεκριμένης πληρωμής.

Η οργάνωση των δεδομένων σε **δενδρικές ιεραρχικές δομές** αποτελεί κοινό τόπο στα αναλυθέντα μοντέλα καθώς διευκολύνει την κληρονομικότητα χαρακτηριστικών μεταξύ των εννοιών ενώ ευνοεί τη μεγαλύτερη κλιμακοθετησιμότητα προδιαγραφής κανόνων πρόσβασης. Ταυτόχρονα, διαφορετικά **επίπεδα αφαίρεσης** λαμβάνονται υπόψη κατά την οργάνωση της πληροφορίας σε ιεραρχίες, καθώς η προδιαγραφή κανόνων ελέγχου πρόσβασης μπορεί να αφορά τόσο γενικές κατηγορίες δεδομένων όσο και συγκεκριμένα στιγμιότυπα αυτών. Οι πιο σύγχρονες προσεγγίσεις υιοθετούν ένα υψηλό επίπεδο αφαιρετικότητας κατά των σχεδιασμό των εννοιών του ελέγχου πρόσβασης, ομαδοποιώντας έννοιες σε σύνολα με συγγενή χαρακτηριστικά και παρεμφερείς ιδιότητες. Ωστόσο, η ενσωμάτωση συγκεκριμένων στιγμιότυπων πληροφοριών στις διαδικασίες ελέγχου πρόσβασης διευκολύνει την προδιαγραφή κανόνων προς διαχείριση εξειδικευμένων περιπτώσεων και μεμονωμένων περιστατικών. Προς τούτο, συνήθης στρατηγική αποτελεί ο συγκερασμός των διαφορετικών επιπέδων αφαιρετικότητας και η δυνατότητα διαχείρισης τόσο αφηρημένων εννοιών (abstract layer) όσο και συγκεκριμένων οντοτήτων (concrete layer). Ανεξαρτήτως επιπέδου αφαιρετικότητας, τυπικά πεδία εφαρμογής δενδρικών ιεραρχικών συσχετίσεων αποτελούν τα σύνολα των ρόλων, των σκοπών, των συνθηκών, των υποχρεώσεων αλλά και των πόρων υπό προστασία.

	Επίγνωση πλαισίου				Υποχρεώσεις	SoD		Ιεραρχίες			
	Χρόνος	Χώρος	Ιστορικό	Γνωρίσματα		SSoD	DSoD	Ρόλοι	Σκοποί	Πόροι	Πλαίσιο
GEO-RBAC	×	✓	×	×	×	✓	×	✓	×	✓	×
GTRBAC	✓	×	×	×	×	✓	✓	×	×	×	×
X-GTRBAC	✓	×	×	×	×	✓	✓	×	×	×	✓
RBAC for XACML	✓	✓	✓	✓	✓	×	×	✓	×	✓	×
TSBAC	✓	×	✓	×	×	✓	×	✓	×	✓	✓
XACML	✓	×	×	✓	✓	✓	✓	✓	×	×	✓
GTHBAC	✓	×	✓	×	×	✓	×	×	×	×	✓
Pu-BAC	✓	✓	×	×	×	✓	×	✓	✓	✓	✓
PuRBAC	✓	×	×	×	✓	×	×	✓	✓	✓	×
OrBAC	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓
P-RBAC	✓	×	×	×	✓	✓	✓	✓	✓	✓	✓

Πίνακας 1: Συγκριτικός πίνακας χαρακτηριστικών μοντέλων ελέγχου πρόσβασης

3.3 Υποδομές Διαχείρισης Εξουσιοδοτήσεων

Ενώ τα μοντέλα ελέγχου πρόσβασης έχουν σκοπό τη διαχείριση της εμπιστευτικότητας των πόρων ενός συστήματος, στόχευση των υποδομών διαχείρισης εξουσιοδοτήσεων συνιστά η αποτίμηση των δικαιωμάτων των χρηστών του συστήματος. Συγκριτικά δηλαδή με την αφαιρετική και γενικευμένη φύση των μοντέλων που αναλύθηκαν στην προηγούμενη ενότητα, οι μηχανισμοί διαχείρισης εξουσιοδοτήσεων αποτελούν πιο εξειδικευμένες εφαρμογές ελέγχου πρόσβασης προσανατολισμένες στον χρήστη και τις ιδιότητές του. Υπό αυτή την έννοια, οι υποδομές διαχείρισης εξουσιοδοτήσεων εντοπίζονται εννοιολογικά πολύ κοντά στα μοντέλα ελέγχου πρόσβασης με επίγνωση των γνωρισμάτων των χρηστών, όπου αδειοδοτήσεις για πρόσβαση παρέχονται ως αποτέλεσμα της ανάλυσης των ποιοτήτων των χρηστών. Επιπρόσθετα, λόγω των χαρακτηριστικών τους οι

συγκεκριμένοι μηχανισμοί παρουσιάζουν μεγάλη απορροφητικότητα σε κατανεμημένα περιβάλλοντα επιχειρηματικότητας. Ειδικότερα στα δίκτυα πλέγματος οι έννοιες ασφάλεια πληροφορίας και ιδιωτικότητα είναι συνυφασμένες με την αξιοποίηση υποδομών διαχείρισης εξουσιοδοτήσεων ως ένα μέσο υλοποίησης ελέγχου πρόσβασης και ως ένα πρότυπο σχεδίασης της αρχιτεκτονικής και των πρωτοκόλλων επικοινωνίας των εμπλεκόμενων συστημάτων.

Από τις πρώτες προσπάθειες προδιαγραφής της διαχείρισης εξουσιοδοτήσεων και της εγκαθίδρυσης σχέσεων εμπιστοσύνης σε κατανεμημένα περιβάλλοντα αποτέλεσαν οι μηχανισμοί διαχείρισης εμπιστοσύνης (trust management). Η έννοια της διαχείρισης εμπιστοσύνης [81] καθιέρωσε μια γενική αντίληψη απέναντι στην ασφάλεια των πληροφοριών ενός συστήματος επιχειρώντας μια ολιστική αντιμετώπιση των σχετικών ζητημάτων μέσω της διεξοδικής προδιαγραφής πολιτικών ασφάλειας, πιστοποιητικών και σχέσεων. Τα πλαίσια διαχείρισης εμπιστοσύνης αντιλαμβάνονται τη διαχείριση εξουσιοδοτήσεων ως μια ειδίκευση των παραδοσιακών μοντέλων ελέγχου πρόσβασης, υπό το πρίσμα της μη αποδοχής της Υπόθεσης Κλειστού Κόσμου (Closed World Assumption) σύμφωνα με την οποία όλοι οι αλληλεπιδρώντες φορείς είναι γνωστοί στο σύστημα ([82]). Υπό αυτή την έννοια, παραδοσιακοί μηχανισμοί διαχείρισης εμπιστοσύνης, όπως τα [83], [84], [85] διαμόρφωσαν το υπόβαθρο για την ανάπτυξη των σύγχρονων μηχανισμών διαχείρισης εξουσιοδοτήσεων για κατανεμημένα περιβάλλοντα. Στόχος της ενότητας είναι η παρουσίαση και ανάλυση των πλέον ενδεικτικών προσεγγίσεων αναφορικά με τη διαχείριση εξουσιοδοτήσεων σε κατανεμημένα περιβάλλοντα.

3.3.1 Σύστημα Shibboleth

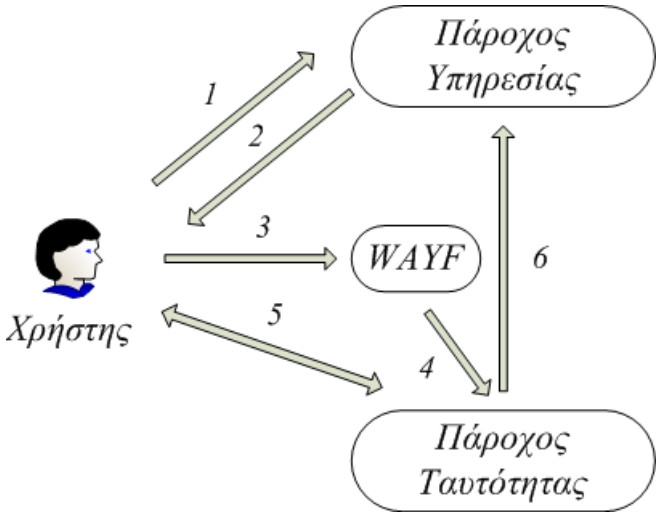
Το σύστημα Shibboleth [86] αποτελεί ένα πακέτο λογισμικού ανοιχτού κώδικα για την υλοποίηση μιας υποδομής ανταλλαγής τιμών γνωρισμάτων μεταξύ απομακρυσμένων φορέων και τη διευκόλυνση της λήψης αποφάσεων με επίγνωση της ιδιωτικότητας σχετικά με την πρόσβαση χρηστών σε προστατευόμενους δικτυακούς πόρους. Βάση του Shibboleth αποτελεί η Γλώσσα Σήμανσης Ισχυρισμών Ασφάλειας (Security Assertion Markup Language – SAML) [87] που συνιστά προτυποποίηση του οργανισμού OASIS. Ο μηχανισμός των ισχυρισμών του προτύπου SAML ενεργοποιείται για την ασφαλή μεταφορά χαρακτηριστικών των χρηστών του συστήματος από έναν Πάροχο Ταυτότητας (Identity Provider – IdP) σε

ένα Πάροχο Υπηρεσίας (Service Provider – SP) που είναι υπεύθυνος για την προστασία ευαίσθητων πόρων εντός μιας συνομοσπονδίας παρόχων. Οι συνομοσπονδίες σχηματίζονται προς διευκόλυνση της σύναψης σχέσεων εμπιστοσύνης μεταξύ των απομακρυσμένων οργανισμών που αποτελούν μέλη της ομάδας.

Σύμφωνα με το πλαίσιο λειτουργίας του Shibboleth ένας SP που βρίσκεται υπεύθυνος για τη διαχείριση ενός ευαίσθητου πόρου καλείται να διαμεσολαβεί σε κάθε αίτημα πρόσβασης για τον εν λόγω πόρο (βήμα 1 στην Εικόνα 4). Στη συνέχει στην πλευρά του SP λαμβάνει χώρα η διαδικασία εύρεσης του IdP που είναι υπόλογος για τη διαχείριση των χαρακτηριστικών του χρήστη (IdP Discovery) μια λειτουργία η οποία μπορεί να περιλαμβάνει μια σειρά επιμέρους διαδικασιών, όπως την ανάγνωση αρχείων διαμόρφωσης του συστήματος, την ενεργοποίηση μηχανισμών «Where Are You From» (WAYF) κ.α. (βήματα 2 και 3). Ανάλογα με το αποτέλεσμα της προηγούμενης ενέργειας στον επιλεχθέντα IdP αποστέλλεται ένα αίτημα ταυτοποίησης του χρήστη (βήμα 4). Σε απάντηση του προηγούμενου αιτήματος, ο IdP είναι υπεύθυνος για τη συλλογή των χαρακτηριστικών του χρήστη από τις πιθανές πηγές αποθήκευσής τους και την ενσωμάτωσή τους σε έναν ισχυρισμό SAML (SAML assertion) προς αποστολή στην πλευρά του SP (βήματα 5 και 6). Προς ενίσχυση της ιδιωτικότητας των χρηστών του, ο IdP είναι σε θέση να προσαρμόζει την ποσότητα και την ποιότητα των αποστελλόμενων χαρακτηριστικών σε κάθε συγκεκριμένο ζεύγος χρήστη – SP. Έτσι, ένας ισχυρισμός SAML μπορεί να περιέχει από βασικές δυαδικές πληροφορίες, όπως η επιβεβαίωση ότι ο χρήστης έχει περάσει επιτυχώς μια διαδικασία τοπικής ταυτοποίησης, μέχρι πολύπλοκους συνδυασμούς πληροφοριών, όπως η επαλήθευση της ηλικίας προσώπων αλλά και του επιπέδου της εκπαιδευτικής μόρφωσής του. Μετά τη λήψη των ζητούμενων βεβαιώσεων ο πάροχος της υπηρεσίας είναι υπεύθυνος για την εξακρίβωση των δικαιωμάτων του χρήστη βάσει της ποιότητας των λαμβανόμενων χαρακτηριστικών.

Στο Shibboleth δεν υπάρχει κάποια πρόβλεψη για τη μοντελοποίηση της λήψης απόφασης πρόσβασης υπό τη μορφή κάποιου μοντέλου ελέγχου πρόσβασης. Αντίθετα παρέχεται η δυνατότητα σε κάθε πάροχο να ενεργοποιήσει διαφορετικό μοντέλο και να το προσαρμόσει στις δικές τους ανάγκες. Κύρια συνεισφορά του μοντέλου επομένως συνιστά η οργάνωση Παρόχων – Ταυτότητας και Υπηρεσίας – υπό την αιγίδα μιας συνομοσπονδίας εντός της οποίας οι σχέσεις εμπιστοσύνης θεωρούνται εξασφαλισμένες και η ανταλλαγή πληροφοριών σχετικά με τον έλεγχο

πρόσβασης πραγματοποιείται μέσω ασφαλών καναλιών επικοινωνίας. Προς τούτο, το Shibboleth προδιαγράφει τη λειτουργία «Μηχανών Εμπιστοσύνης», οι οποίες είναι υπεύθυνες για τη διευκρίνιση του επιπέδου εμπιστοσύνης ισχυρισμών και αλληλεπιδρώντων φορέων με χρήση μηχανισμών ψηφιακών πιστοποιητικών και ψηφιακών υπογραφών καθώς και με αξιοποίηση του πρωτοκόλλου SSL/TLS [88].



Εικόνα 4: Το πλαίσιο λειτουργίας του συστήματος Shibboleth

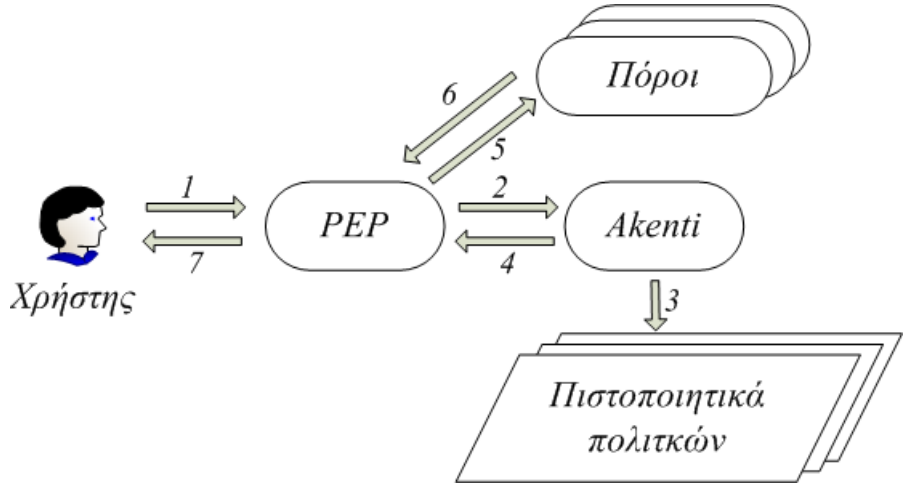
3.3.2 Σύστημα Akenti

Το σύστημα Akenti [89] αποτελεί μια προσέγγιση αποδοτικής παραγωγής εξουσιοδοτήσεων σε περιβάλλοντα που περιλαμβάνουν κατανεμημένους πόρους και γεωγραφικά και διαχειριστικά απομακρυσμένους χρήστες. Η επικοινωνία μεταξύ των φορέων και των πόρων του συστήματος πραγματοποιείται με την αξιοποίηση ασφαλών καναλιών TLS. Βάση του συστήματος αποτελούν πιστοποιητικά δημόσιου κλειδιού, πιστοποιητικά ιδιοτήτων καθώς και ψηφιακά πιστοποιητικά αναπαράστασης πολιτικών πρόσβασης, υπογεγραμμένων από πιστοποιημένες οντότητες. Σύμφωνα με τις προδιαγραφές του συστήματος κάθε κανόνας ασφάλειας διαμορφώνεται στη γλώσσα σήμανσης XML, ενώ το περιεχόμενό του αναπαρίσταται και αντιστοιχίζεται σε τρία διαφορετικά πιστοποιητικά: ένα πιστοποιητικό πολιτικής που προσδιορίζει την οντότητα διαχείρισης κάποιου πόρου, ένα πιστοποιητικό συνθηκών χρήσης που υποδεικνύει τους περιορισμούς που περιβάλλουν την πρόσβαση στον συγκεκριμένο πόρο καθώς και ένα πιστοποιητικό ιδιοτήτων που καθορίζει σαφώς τα χαρακτηριστικά που πρέπει να διέπουν κάποιον αιτούντα για να

του αναγνωριστεί πρόσβαση στον προστατευόμενο πόρο σύμφωνα με το περιεχόμενο του πιστοποιητικού συνθηκών χρήσης.

Το μοντέλο λειτουργίας του συστήματος Akenti καθορίζει την ενεργοποίηση ενός Σημείου Εφαρμογής Πολιτικής PEP το οποίο εργάζεται ως πύλη πρόσβασης στους προστατευόμενους πόρους. Ένας χρήστης που επιθυμεί πρόσβαση σε κάποια υπηρεσία η δεδομένο υπό την προστασία του Akenti, καλείται να πιστοποιηθεί στην οντότητα PEP μέσω της χρήσης ενός προσωπικού πιστοποιητικού δημόσιου κλειδιού X.509 (βήμα 1 στην Εικόνα 5). Στη συνέχεια και στην περίπτωση επιτυχούς αυθεντικοποίησης του χρήστη, η οντότητα PEP επικοινωνεί με το Σημείο Απόφασης Πολιτικής PDP του συστήματος, προς αποτίμηση των δικαιωμάτων του αναφορικά με τον ζητηθέντα πόρο (βήμα 2). Το σημείο PDP συλλέγει όλες τις απαραίτητες πληροφορίες σχετικά με τον αιτούντα και τον πόρο υπό τη μορφή ψηφιακών πιστοποιητικών για τη λήψη μιας επικαιροποιημένης και έγκυρης απόφασης πρόσβασης (βήμα 3). Ανάλογα με το περιεχόμενο των πιστοποιητικών το σύστημα, και πιο συγκεκριμένα η οντότητα PDP μέσω του σημείου PEP, βρίσκεται σε θέση να επιτρέψει ή να αποτρέψει τη ζητηθείσα πρόσβαση (βήματα 4 – 7).

Η δυνατότητα αξιοποίησης πολιτικών ελέγχου πρόσβασης που έχουν διαμορφωθεί από απομακρυσμένους και ασυσχέτιστους φορείς, οι οποίοι διατηρούν με αυτόν τον τρόπο την ανεξαρτησία και την αυτονομία τους, συνιστά την πιο σημαντική συνεισφορά του συστήματος Akenti. Ειδικότερα, η αποτύπωση των κανόνων πρόσβασης στη μορφή ψηφιακών πιστοποιητικών επιτρέπει σε μια οντότητα διαμεσολάβησης μεταξύ των χρηστών και των προστατευόμενων πόρων να ελέγξει την εγκυρότητα και την ακρίβεια των διαμορφωμένων πολιτικών και να προσαρμόσει τις εξουσιοδοτήσεις της στο επίπεδο εμπιστοσύνης που απορρέει από αυτές. Σημειώνεται ότι οι τοποθεσίες αποθήκευσης των εμπλεκόμενων πιστοποιητικών πρέπει να είναι ρητά καθορισμένες και γνωστές στο σημείο PDP του συστήματος. Προς τούτο στο πλαίσιο λειτουργίας του συστήματος τα πιστοποιητικά πολιτικής αποθηκεύονται στις τοποθεσίες διατήρησης του πόρου που ελέγχουν οι σχετικές πολιτικές πρόσβασης.



Εικόνα 5: Το πλαίσιο λειτουργίας του συστήματος Akenti

3.3.3 Υποδομή Προτύπων Διαχείρισης Ρόλων και Δικαιωμάτων (Privilege and Role Management Infrastructure Standards – PERMIS)

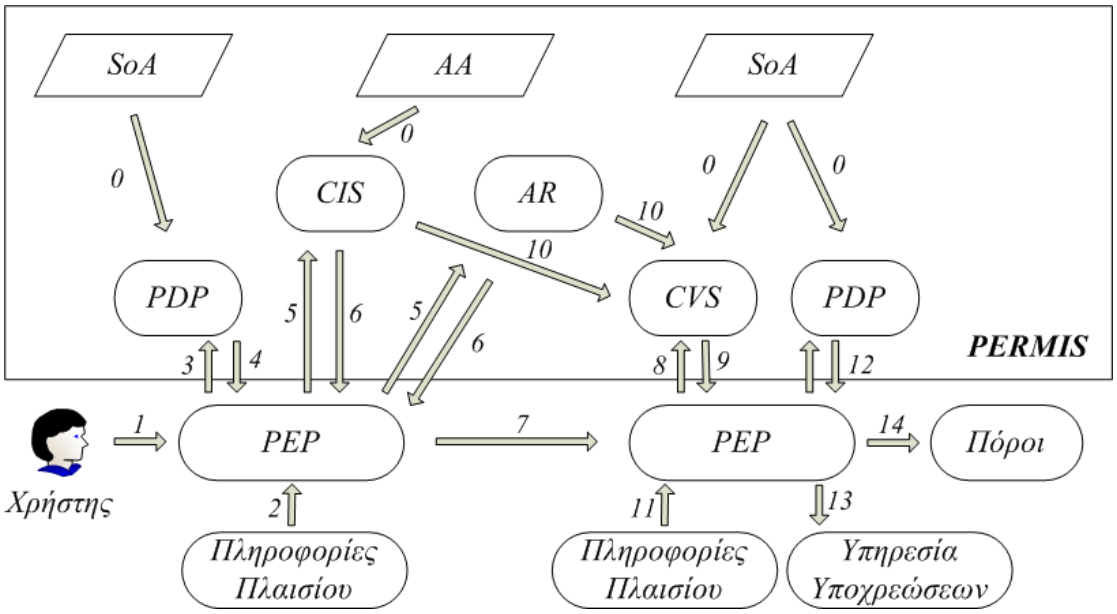
Η υποδομή PERMIS [90] συνιστά μια υποδομή διαχείρισης εξουσιοδοτήσεων της οποίας θεμελιώδη δομικά συστατικά αποτελούν η αξιοποίηση των μηχανισμών των υποδομών PMI και η εφαρμογή ενός γενικευμένου μοντέλου ελέγχου πρόσβασης RBAC στα πρότυπα των μοντέλων με επίγνωση των γνωρισμάτων του χρήστη. Έτσι στα πλαίσια του PERMIS ένας ρόλος δεν αντιστοιχεί εννοιολογικά στη θέση της οντότητας εντός ενός οργανισμού αλλά μπορεί να περικλείει οποιαδήποτε πληροφορία σχετική με τον χρήστη, όπως επαγγελματικά διαπιστευτήρια ή το επίπεδο της ταυτοποίησής του ([91]). Τα γνωρίσματα αυτά του χρήστη παρουσιάζονται εντός του συστήματος με τη μορφή πιστοποιητικών ιδιοτήτων, ψηφιακά υπογεγραμμένων από μία ή πολλαπλές έμπιστες Αρχές Ιδιοτήτων.

Προς εξακρίβωση και επικύρωση της εγκυρότητας αλλά και της επάρκειας των πιστοποιητικών ιδιοτήτων ενεργοποιείται η Υπηρεσία Επικύρωσης Διαπιστευτηρίων (Credential Validation Service – CVS). Κάθε πάροχος για την προστασία των πόρων του και τον επιθυμητό έλεγχο της πρόσβασης διαμορφώνει τις κατάλληλες προσωπικές πολιτικές επικύρωσης διαπιστευτηρίων. Με αυτόν τον τρόπο, η υπηρεσία CVS επιτρέπει την κατανεμημένη διαχείριση πιστοποιητικών στα πλαίσια της αποτίμησης των δικαιωμάτων κάθε χρήστη. Επιπλέον το PERMIS ενισχύει την εκφραστικότητα των μοντέλων RBAC επιτρέποντας την ιεραρχική οργάνωση των

ρόλων και την απόδοση πολλαπλών δικαιωμάτων σε σύνολα ρόλων, σε αντίθεση με τη συμβατική προσέγγιση ανάθεσης αδειοδοτήσεων αποκλειστικά σε μονάδες ρόλων. Ταυτόχρονα η υποδομή υποστηρίζει λειτουργίες μεταφοράς εξουσιοδοτήσεων, κατά τις οποίες επιτρέπεται σε μια οντότητα να μεταβιβάσει τις αδειοδοτήσεις της σε κάποια άλλη, οδηγώντας έτσι σε ακόμα μεγαλύτερη αποκέντρωση της διαχείρισης των πιστοποιητικών. Τέλος στο PERMIS η διαδικασία της λήψης αποφάσεων εμπλουτίζεται με ιστορικά στοιχεία προς υποστήριξη κλασσικών αρχών ιδιωτικότητας και ασφάλειας, όπως ο καταμερισμός των καθηκόντων.

Κάθε χρήστης εντός του συστήματος PERMIS δύναται να διατηρεί στην κατοχή του πιστοποιητικά και διαπιστευτήρια υπογεγραμμένα από πλήθος διαφορετικών Αρχών Ιδιοτήτων. Αναφορικά με τη μορφή των πιστοποιητικών, στο PERMIS υποστηρίζονται τόσο προγεγραμμένα και μακράς διάρκειας πιστοποιητικά που αποθηκεύονται στους κατάλληλους σωρευτικούς χώρους όσο και μικρής διάρκειας διαπιστεύσεις που εκδίδονται μετά από σχετικό αίτημα σε συμφωνία με τις υποκείμενες πολιτικές έκδοσης πιστοποιητικών. Η Αρχή Εξουσιοδοτήσεων του χρήστη υπαγορεύει τα σύνολα πιστοποιητικών που επιτρέπεται να αξιοποιηθούν στον τομέα εμπιστοσύνης του πόρου – στόχου (βήματα 0 στην Εικόνα 6). Όταν ο χρήστης αποδίδει ένα αίτημα πρόσβασης, ένα τοπικό στον χρήστη Σημείο Απόφασης Πολιτικής PDP ενημερώνει το αντίστοιχο Σημείο Εφαρμογής Πολιτικής PEP σχετικά με το σύνολο των πιστοποιητικών που επιτρέπεται να συνοδεύσουν το αίτημα του χρήστη στη ζώνη του ζητηθέντα πόρου (βήματα 1 – 4). Στη συνέχεια, τα υποδεικνυόμενα διαπιστευτήρια συλλέγονται από το σημείο PEP είτε από αποθήκες πιστοποιητικών είτε από Υπηρεσίες Έκδοσης Πιστοποιητικών (Credential Issuing Service – CIS) (βήματα 5 και 6). Στην πλευρά του τομέα στόχου, το αίτημα παραλαμβάνεται από την αντίστοιχη οντότητα PEP (βήμα 7), η οποία συμβουλεύεται την Πολιτική Επικύρωσης Διαπιστευτηρίων (Credential Validation Policy – CVP) προς διευκρίνιση της εμπιστευτικότητας των πιστοποιητικών και των αντίστοιχων Αρχών Ιδιοτήτων καθώς και για την υπόδειξη των δικαιωμάτων που συσχετίζονται με συγκεκριμένα χαρακτηριστικά (βήματα 8 και 9). Μετά τη λήψη τους, τα πιστοποιητικά εξετάζονται ως προς την εγκυρότητά τους, μια διαδικασία που μπορεί να περιλαμβάνει μια σειρά αιτημάτων για την ανάληψη επιπλέον υπαρχόντων ή την έκδοση νέων διαπιστευτηρίων (βήμα 10). Τα τελικά έγκυρα πιστοποιητικά μαζί με πληροφορίες πλαισίου, όπως η ημερομηνία και η ώρα του αιτήματος, προωθούνται στο κατάλληλο σημείο PDP προς ανάλυση και έκδοση της απόφασης ελέγχου

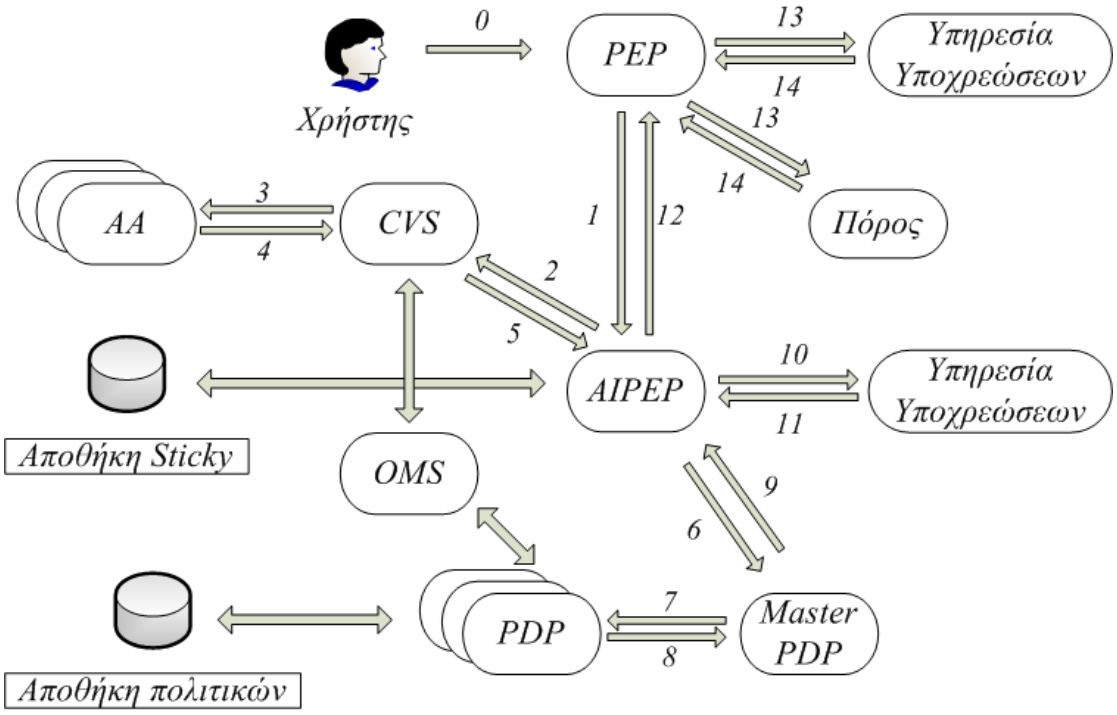
πρόσβασης (βήματα 11 και 12). Στην περίπτωση θετικής απόφανσης του PDP, η πρόσβαση επιτρέπεται από την οντότητα PEP (βήμα 14). Σε κάθε περίπτωση, ένα PDP μπορεί να επιστρέψει συμπληρωματικά ένα σύνολο υποχρεώσεων που σηματοδοτούν ενέργειες που πρέπει να εφαρμοστούν από το PEP παράλληλα με την απόφαση για πρόσβαση ή μη (βήμα 13).



Εικόνα 6: Το πλαίσιο λειτουργίας του συστήματος PERMIS

Σε μια ενδιαφέρουσα επέκταση του μοντέλου [92] προτάθηκε η αξιοποίηση ενός ανεξάρτητου με την εκάστοτε εφαρμογή – στόχο Σημείου Εφαρμογής Πολιτικής (Application Independent Policy Enforcement Point – AIPEP) και ενός Επικεφαλούς Σημείου Απόφασης Πολιτικής (Master PDP). Στο σχήμα αυτό, η οντότητα AIPEP είναι υπεύθυνη για τη διαχείριση sticky policies ([93]), για την επικοινωνία με την οντότητα Master PDP, για τη διεκπεραίωση υποχρεώσεων ανεξάρτητων με την εφαρμογή στόχο και για την επικύρωση πιστοποιητικών με χρήση της υπηρεσίας CVS. Οι πολιτικές sticky policies επιτρέπουν στον χρήστη να καθορίζει ρητά τις επιλογές του για τη διαχείριση των προσωπικών του πληροφοριών είτε στις συναλλαγές του ίδιου με κάποιον οργανισμό είτε στις ηλεκτρονικές διαδικασίες που λαμβάνουν χώρα μεταξύ οργανισμών χωρίς τη διαμεσολάβηση ή εμπλοκή του ίδιου. Αντίστοιχα το σημείο Master PDP είναι υπεύθυνο για την ενορχήστρωση πλήθους ανεξάρτητων οντοτήτων PDP που υποστηρίζουν διαφορετικές γλώσσες προδιαγραφής πολιτικών καθώς και για την τελική έκδοση απόφασης πρόσβασης που λαμβάνει υπόψη του όλες τις υποκείμενες αποφάσεις εξουσιοδότησης.

Στο προτεινόμενο πλαίσιο λειτουργίας, το σημείο AIPEP αποτελεί τον αποδέκτη των αιτημάτων για εξουσιοδότηση (βήματα 0 και 1 στην Εικόνα 7). Μετά τη λήψη κάποιου σχετικού μηνύματος η οντότητα επικοινωνεί με την Υπηρεσία Επικύρωσης Διαπιστευτηρίων προς εξακρίβωση των συνημμένων ιδιοτήτων του χρήστη (βήματα 2 – 5) και σε περίπτωση επιτυχούς απάντησης ενημερώνει το σημείο Master PDP σχετικά με το σύνολο των απομακρυσμένων PDP που πρέπει να ενεργοποιηθούν (βήμα 6). Προς διευκόλυνση της διαχείρισης πολλαπλών ορολογιών και λεξιλογίων μεταξύ των συνεργαζόμενων φορέων (ένα σύνηθες γεγονός στην πραγματικότητα) το σύστημα περιλαμβάνει έναν Εξυπηρετητή Οντολογίας Συσχέτισης (Ontology Mapping Server – OMS) ο οποίος και αναλαμβάνει τη διατήρηση πληροφοριών συσχέτισης μεταξύ διαφορετικών ονομάτων ιδιοτήτων. Έπειτα το σημείο Master PDP είναι υπεύθυνο για την κλήση των απομακρυσμένων PDP, τη λήψη των αποφάσεων τους σχετικά με την εξουσιοδότηση του χρήστη και τέλος τον ορθολογισμό τους και τη σύμπτυξή τους σε μια σαφή απόφαση εξουσιοδότησης συνοδευόμενη από πιθανές υποχρεώσεις. Μετά το πέρας των παραπάνω ενεργειών ενημερώνει την οντότητα AIPEP η οποία και είναι υπεύθυνη για τη συνέχιση της διαδικασίας (βήματα 7 – 9). Για την εξαγωγή πιθανών υποχρεώσεων από το περιεχόμενο των σχετικών με τα δεδομένα πολιτικών, η αρχιτεκτονική του προτεινόμενου συστήματος προδιαγράφει τη λειτουργία μιας αποθήκης πολιτικών, όπου συλλέγονται οι προσωπικές επιλογές και πολιτικές του χρήστη και οι οποίες συνδέονται με συγκεκριμένα σύνολα δεδομένων. Η αποθήκη πολιτικών θεμελιώνει ουσιαστικά την υποστήριξη των μηχανισμών πολιτικών sticky policies από το σύστημα. Πριν την προώθηση της απόφασης πρόσβασης στο τοπικό με τον ζητηθέντα πόρο σημείο PEP, η οντότητα AIPEP διεκπεραιώνει τις υποκείμενες υποχρεώσεις που επισύρει μια θετική εξουσιοδότηση. Τέλος το τοπικό PEP είναι υπεύθυνο για την περαίωση και της τελευταίας κατηγορίας υποχρεώσεων πριν εφαρμόσει την απόφαση – αποτέλεσμα του μηχανισμού. Η κατηγορία αυτή περιλαμβάνει υποχρεώσεις που πρέπει να τηρηθούν είτε κατά τη διάρκεια της αδειοδότησης για πρόσβαση ή μετά το πέρας αυτής. Σημειώνεται ότι πρόσφατα οι εμπνευστές του συγκεκριμένου σχήματος διαχείρισης εξουσιοδοτήσεων πρότειναν μια ενδιαφέρουσα προσέγγιση για την ειδίκευση της λειτουργίας του στα πλαίσια δικτύων υπολογιστικής νέφους ([94]).



Εικόνα 7: Το πλαίσιο λειτουργίας του εκτεταμένου PERMIS

3.3.4 Σύστημα Ελέγχου Πρόσβασης με Επίγνωση της Ιδιωτικότητας PRIME

Στα πλαίσια του ερευνητικού προγράμματος PRIME [95] αναπτύχθηκε ένα εξελιγμένο σύστημα ελέγχου πρόσβασης για ιδιωτικότητα [96] που καλύπτει τα θέματα τόσο της προστασίας των προσωπικών δεδομένων και της αξιοποίησής τους σε ένα μοντέλο με επίγνωση των χαρακτηριστικών των χρηστών όσο και της χρήσης τους σε μελλοντικές συναλλαγές. Προς τούτο το μοντέλο παρουσιάζει και ενσωματώνει την προδιαγραφή μιας ειδικής κατηγορίας πολιτικών ελέγχου πρόσβασης που καλούνται πολιτικές διαχείρισης δεδομένων (data handling policy). Μια πολιτική διαχείρισης δεδομένων καθορίζει και οριοθετεί τον τρόπο μεταχείρισης προσωπικών πληροφοριών PII στις οντότητες – αποδέκτες των πληροφοριών αυτών, ενσωματώνοντας τις έννοιες του παραλήπτη, του σκοπού, του τύπου των δεδομένων και των περιορισμών. Ένας περιορισμός σε μια πολιτική διαχείρισης δεδομένων μπορεί να αναφέρεται σε υποχρεώσεις που πρέπει να εφαρμοστούν πριν, κατά τη διάρκεια ή μετά την παροχή της εξουσιοδότησης ή σε γενικές συνθήκες που εξετάζουν το προφίλ των χρηστών και των ζητηθέντων δεδομένων. Αναφορικά με τον τρόπο καθορισμού των συγκεκριμένων κανόνων το σχήμα εξουσιοδοτήσεων

υιοθετεί τη μετριοπαθή προσέγγιση της αξιοποίησης φορμών πολιτικών ορισμένες από τον πάροχο και παραμετροποιημένες από τον χρήστη. Η προσέγγιση αυτή ορισμού των πολιτικών διαχείρισης δεδομένων αποτελεί μια περισσότερο ισορροπημένη και ευέλικτη λύση συγκριτικά με την ανελαστική στρατηγική της προδιαγραφής των κανόνων από τον πάροχο και της εξασφάλισης της συγκατάθεσης ή μη του χρήστη και την προσέγγιση της αποδοχής των κανόνων που προδιαγράφηκαν αποκλειστικά από τον χρήστη στον πάροχο. Επιπρόσθετα οι πολιτικές διαχείρισης δεδομένων καθορίζονται ανεξάρτητα από τους λοιπούς κανόνες ελέγχου πρόσβασης του παρόχου.

Οι κανόνες ελέγχου πρόσβασης καθορίζουν και παράγουν εξουσιοδοτήσεις σχετικά με την πρόσβαση σε υπηρεσίες και δεδομένα. Παράλληλα με τους κανόνες ελέγχου πρόσβασης το προτεινόμενο σύστημα υποστηρίζει και την προδιαγραφή πολιτικών αποκάλυψης (release Policies) πληροφοριών PII που ακολουθούν τη δομή των κανόνων ελέγχου πρόσβασης και μοντελοποιούν τις προτιμήσεις των χρηστών σχετικά με τις συνθήκες και τον σκοπό αποκάλυψης των δεδομένων τους. Οι κανόνες ελέγχου πρόσβασης/αποκάλυψης σχηματίζονται στη βάση των εννοιών του υποκειμένου, του αντικειμένου, των χαρακτηριστικών υποκειμένων και αντικειμένων, των ενεργειών, των σκοπών και των συνθηκών.

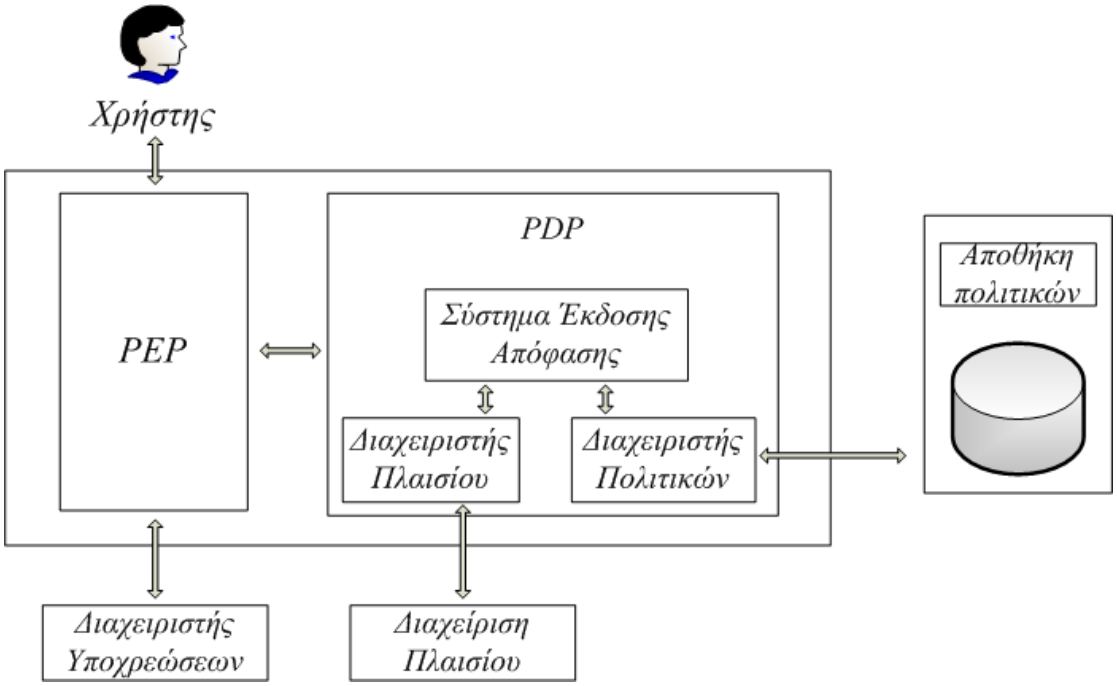
Στα πλαίσια του έργου PRIME, οι προδιαγραφόμενοι τύποι πολιτικών ενσωματώθηκαν σε ένα σύστημα ελέγχου της ιδιωτικότητας. Βασικά συστατικά μέρη του συστήματος αποτελούν τα ακόλουθα:

- Η Αποθήκη Πολιτικών (Policy Repository), που διατηρεί τις πολιτικές ελέγχου πρόσβασης, αποκάλυψης και διαχείρισης δεδομένων και υποστηρίζει λειτουργίες διαχείρισης πολιτικών, όπως δημιουργία, επεξεργασία και διαγραφή.
- Η οντότητα Διαχείρισης Πλαισίου (Context Manager), που είναι υπεύθυνη για τη συλλογή πληροφοριών πλαισίου και τη σύμπτυξή τους σε συμπαγείς προτυποποιημένες μορφές.
- Το υποσύστημα Ελέγχου Πρόσβασης (Privacy Control Module) που εργάζεται στη βάση των λειτουργιών της οντότητας Διαχείρισης Πλαισίου και περιλαμβάνει δύο οντότητες: ένα σημείο PDP και ένα σημείο PEP.
- Η οντότητα PDP είναι υπεύθυνη για την παραγωγή των τελικών αποφάσεων ελέγχου πρόσβασης. Η λειτουργικότητές της διαμοιράζονται στα συστήματα

της Έκδοσης Απόφασης (Decision Maker), του Διαχειριστή Πολιτικών (Policy Handler) και του Διαχειριστή Πλαισίου (Context Administrator).

- Η οντότητα PEP είναι υπεύθυνη για την εφαρμογή των παραχθέντων αποφάσεων ελέγχου πρόσβασης, μέσω της διαμεσολάβησής της στα αιτήματα πρόσβασης και την εξέταση των εξουσιοδοτήσεων. Επιπρόσθετα, στα καθήκοντα του σημείο PEP περιλαμβάνεται και η επικοινωνία με την οντότητα Διαχειριστή Υποχρεώσεων (Obligation Manager). για την εφαρμογή των υποχρεώσεων που εξάγονται από τις πολιτικές Διαχείρισης Δεδομένων.

Αναφορικά με την εφαρμογή του ελέγχου πρόσβασης το σύστημα ακολουθεί την ακόλουθη ροή εργασιών: Δοθείσας μιας αίτησης πρόσβασης η οντότητα PEP εξετάζει το σύνολο των κανόνων που δύναται να εφαρμοστούν στη συγκεκριμένη αίτηση. Σε περίπτωση που δεν βρεθεί σχετικός κανόνας το αίτημα απορρίπτεται. Σε αντίθετη περίπτωση, το σύστημα παράγει μια απάντηση πρόσβασης που μπορεί να λάβει τις τιμές αποδοχή, άρνηση ή απροσδιόριστο. Η τελευταία τιμή υπονοεί την ανάγκη αναγνώρισης περισσότερων στοιχείων για τον χρήστη πριν την παραγωγή μιας τελικής απάντησης. Προς εξακρίβωση των επιπλέον ιδιοτήτων, το σύστημα υποστηρίζει τη διεξαγωγή των κατάλληλων αλληλεπιδράσεων με τον χρήστη. Στην περίπτωση που η απόφαση πρόσβασης είναι θετική, η οντότητα PDP είναι υπεύθυνη για τον προσδιορισμό πιθανών περιορισμών όπως αυτοί προκύπτουν από τις ισχύουσες πολιτικές Διαχείρισης Δεδομένων. Τέλος, οι συγκεκριμένοι περιορισμοί συμμόρφωσης των αποδεκτών των πληροφοριών με τις προτιμήσεις χρηστών αποστέλλονται μαζί με την τελική θετική απάντηση στον αιτούντα.



Εικόνα 8: Σύστημα Ελέγχου Πρόσβασης με Επίγνωση της Ιδιωτικότητας

3.3.5 Εξουσιοδότηση Βάσει Αποδεικτικών Στοιχείων (Proof Carrying Authorization – PCA)

Προς την κατεύθυνση της μείωσης του υπολογιστικού κόστους των μηχανισμών εξουσιοδότησης σε ότι αφορά την παραγωγή αποφάσεων πρόσβασης σε δεδομένα, έχει αναδειχθεί στη βιβλιογραφία ([97], [98]) μια προσέγγιση αντιστροφής της λογικής των μοντέλων ελέγχου πρόσβασης, η οποία προϋποθέτει από τον αιτούντα τη συλλογή και την παράδοση στο μηχανή παραγωγής αποφάσεων, στοιχείων που δικαιολογούν μια ενδεχόμενη πρόσβαση στα ζητηθέντα δεδομένα. Επακόλουθα, στις εν λόγω προσεγγίσεις το υπολογιστικό κόστος εξακρίβωσης των εξουσιοδοτήσεων μεταπηδά από το σύστημα διαχείρισης εξουσιοδοτήσεων στον εκάστοτε χρήστη που επιζητά πρόσβαση σε δεδομένα. Το μοντέλο αυτό λειτουργίας και οι υφιστάμενες διαδικασίες αναφέρονται σχηματικά ως «εξουσιοδότηση βάσει αποδεικτικών στοιχείων» (Proof Carrying Authorization – PCA).

Η κεντρική ιδέα πίσω από την εξουσιοδότηση των PCA μοντέλων, περιλαμβάνει τη μοντελοποίηση των πολιτικών ασφαλείας ενός συστήματος στη μορφή λογικών κανόνων και την κατασκευή εκ μέρους του αιτούντα πρόσβασης ψηφιακά υπογεγραμμένων λογικών αποδείξεων οι οποίες αντιστοιχούν σε λογικά δένδρα συνεπαγωγών (logical derivation trees). Ο αιτών καλείται παράλληλα με το αίτημα

πρόσβασης να προωθήσει και την παραγόμενα αποδεικτικά, ο έλεγχος όμως ορθότητας των οποίων από το σύστημα εξουσιοδοτήσεων αρκεί για την εξαγωγή όμως απόφασης πρόσβασης. Σημειώνεται ότι υπολογιστικά η πολυπλοκότητα της διαδικασίας επαλήθευσης της ορθότητας των λογικών αποδεικτικών είναι γραμμικά ανάλογη με το μέγεθος των αποδεικτικών στοιχείων.

Συστήματα διαχείρισης εξουσιοδοτήσεων PCA έχουν υλοποιηθεί με επιτυχία σε μια σειρά από διαφορετικά πεδία εφαρμογής, όπως είναι οι εφαρμογές διαδικτύου, οι φορητές συσκευές, συστήματα διαχείρισης αρχείων και ο κατανεμημένος προγραμματισμός. Ωστόσο, το πλαίσιο λειτουργίας των PCA συστημάτων εμπεριέχει κινδύνους και περιορισμούς που μπορεί να επιφέρουν ανεπιθύμητες παραβιάσεις της ιδιωτικότητας των χρηστών. Πιο συγκεκριμένα, είναι πιθανή η παραβίαση της ανωνυμίας των χρηστών ή η άνευ λόγου αποκάλυψη ευαίσθητων δεδομένων όμως κατά την επίδειξη των ψηφιακά υπογεγραμμένων λογικών πειστηρίων. Προς τούτο, έχουν προταθεί στη βιβλιογραφία προσεγγίσεις συγκερασμού των υποδομών διαχείρισης εξουσιοδοτήσεων βάσει αποδεικτικών στοιχείων με κρυπτογραφικά πρωτόκολλα αποδείξεων μηδενικής γνώσης ([99]). Στις εν λόγω προτάσεις, ο κόμβος – επαληθευτής δημοσιοποιεί υπογραφές λογικών τύπων, όπως στο παραδοσιακό σχήμα PCA, και ο κόμβος – διεκδικητής παράγει αποδείξεις μηδενικής γνώσης των υπογραφών, στις οποίες τα ευαίσθητα δεδομένα του είναι προστατευμένα. Χάρη στις ιδιότητες της κρυπτογραφίας μηδενικής γνώσης, όπως αναλύθηκε σε προηγούμενη ενότητα, η οντότητα – επαληθευτής είναι σε θέση να βεβαιώσει την ισχύ των σχετικών αποδεικτικών στοιχείων, χωρίς όμως ευαίσθητες ιδιότητες του εμπλεκόμενου χρήστη να δημοσιοποιούνται ασκόπως.

3.3.6 Συμπεράσματα

Η ανάλυση των προαναφερθέντων συστημάτων διαχείρισης εξουσιοδοτήσεων, όπως και στην περίπτωση των μελετηθέντων μοντέλων ελέγχου πρόσβασης, αναδεικνύει επαναλαμβανόμενα κοινά πρότυπα γενικού σχεδιασμού και επιμέρους λειτουργιών. Στόχος της παρούσας ενότητας είναι η συνοπτική παρουσίαση των κοινών αυτών στοιχείων που αποτελούν τα θεμελιώδη δομικά συστατικά των σχετικών λύσεων και τα οποία αποτέλεσαν και τη βάση σχεδιασμού και υλοποίησης της προτεινόμενης λύσης.

Σημασιολογική διαλειτουργικότητα και επίτευξη σχέσεων εμπιστοσύνης: Στο ολοένα και περισσότερο αποκεντρωτικό περιβάλλον της σύγχρονης επιχειρηματικότητας, οι παρεχόμενες υπηρεσίες, οι ενδιάμεσες διαδικασίες και τα διαχειριζόμενα δεδομένα επεκτείνονται σε ένα ευρύ φάσμα διοικητικά και γεωγραφικά απομακρυσμένων φορέων. Εντός των ανεξάρτητων τομέων λειτουργίας και ζωνών ασφαλείας τους, οι εμπλεκόμενες οντότητες διατηρούν διακριτές πρακτικές προστασίας, ενεργοποιούν διαφορετικά κριτήρια επισύναψης σχέσεων εμπιστοσύνης καθώς και αξιοποιούν ανεξάρτητα σημασιολογικά πλαίσια αναφοράς. Ως αποτέλεσμα, η σημασιολογική διαλειτουργικότητα των υφιστάμενων εννοιών και η αποδοτική επίτευξη σχέσεων εμπιστοσύνης μεταξύ των αλληλεπιδρώντων οντοτήτων διαδραματίζουν βασικό ρόλο σε μεγάλο αριθμό προσεγγίσεων διαχείρισης εξουσιοδοτήσεων. Προς τούτο, οι τελευταίοι ενεργοποιούν διαφορετικούς μηχανισμούς ολοκλήρωσης ετερογενών τομέων, που ποικίλουν από στατικές λύσεις, όπως είναι η σύσταση εξειδικευμένων **συνομοσπονδιών** έως πιο δυναμικές προσεγγίσεις επίτευξης διαλειτουργικότητας σε πραγματικό χρόνο.

Σημαντικές κατηγορίες εννοιών: Οι μηχανισμοί διαχείρισης εξουσιοδοτήσεων προσαρμόζουν τη λειτουργία τους σε συγκριμένες έννοιες, η εκφραστική ποιότητα και το εύρος των οποίων καθορίζει τόσο την εύρυθμη και αποδοτική λειτουργία τους όσο και το εύρος του πεδίου εφαρμογής τους. Εν πολλοίς, οι έννοιες αυτές πηγάζουν σημασιολογικά από το εκάστοτε μοντέλο ελέγχου πρόσβασης το οποίο αξιοποιεί κάθε μηχανισμός διαχείρισης εξουσιοδοτήσεων και περιστρέφεται γύρω από το σύνολο εννοιών που αναλύθηκαν στην ενότητα 3.2.5 (ρόλος, σκοπός πρόσβασης, υποχρεώσεις κ.ο.κ.).

Συμπληρωματικές ενέργειες: Σε αρκετές περιπτώσεις, η πρόσβαση σε ευαίσθητα δεδομένα συνεπάγεται τη διενέργεια συγκεκριμένων διαδικασιών και την εκπλήρωση προκαθορισμένων υποχρεώσεων. Οι συγκεκριμένες, συμπληρωματικές στην πρόσβαση, ενέργειες συναντώνται στη βιβλιογραφία ως «υποχρεώσεις ιδιωτικότητας» [100] και μπορεί να περιλαμβάνουν την αλληλεπίδραση του συστήματος διαχείρισης εξουσιοδοτήσεων με το υποκείμενο των δεδομένων και τις αρμόδιες Αρχές καθώς και τη διεκπεραίωση υποχρεώσεων σχετικά με τη διατήρηση των δεδομένων, όταν κάτι τέτοιο υπαγορεύεται από τη νομοθεσία.

Πολιτικές χρήσης δεδομένων: Η πρόσβαση σε ευαίσθητους πόρους, ακόμα και όταν είναι πλήρως σύννομη και θεμιτή από άποψη ελέγχου πρόσβασης, απαιτεί την εφαρμογή μηχανισμών προς εξασφάλιση της κατάλληλης χρήσης και αξιοποίησης

των αποκαλυπτόμενων δεδομένων. Προς τούτο, τα συστήματα διαχείρισης εξουσιοδοτήσεων ενσωματώνουν λειτουργίες προδιαγραφής πολιτικών χρήσης δεδομένων που ακολουθούν τις προτιμήσεις των κατόχων δεδομένων, των παρόχων περιεχομένου καθώς και των αρμόδιων Αρχών. Σημειώνεται ότι, οι πολιτικές χρήσης δεδομένων λειτουργούν συμπληρωματικά με τους κανόνες ελέγχου πρόσβασης, προδιαγράφοντας τη χρήση ευαίσθητων πόρων αποκλειστικά και μόνο έπειτα από μια επιτυχημένη αίτηση πρόσβασης σε αυτούς.

Μηχανή παραγωγής συλλογισμών: Τόσο η κατανεμημένη φύση όσο και η αυξανόμενη πολυπλοκότητα των σύγχρονων ηλεκτρονικών διαδικασιών, εξασφαλίζουν τη συμμετοχή πλήθους οντοτήτων στην αλυσίδα παροχής υπηρεσιών, καθεμία από τις οποίες διατηρεί τις προσωπικές της προτιμήσεις ιδιωτικότητας. Ο εξορθολογισμός και ο συμβιβασμός πολιτικών πρόσβασης και χρήσης δεδομένων με υψηλό βαθμό ετερογένειας, που προκύπτει από την ποικιλομορφία των διαφορετικών πηγών προδιαγραφής κανόνων, διαδραματίζει επιτελικό ρόλο στις λειτουργίες των συστημάτων διαχείρισης εξουσιοδοτήσεων καθώς επιτρέπει την παραγωγή σαφών και αναμφισβήτητων δηλώσεων εξουσιοδότησης. Ένα σύνολο επαγωγικών λογικών κανόνων και αλγορίθμων επίλυσης αντικρουόμενων πολιτικών (conflict resolution) συνθέτουν τον πυρήνα της μηχανής παραγωγής συλλογισμών κάθε συστήματος διαχείρισης εξουσιοδοτήσεων.

4 Προδιαγραφή Προτεινόμενης Λύσης

Η πρόληψη και διαχείριση των κινδύνων απώλειας της ιδιωτικότητας των χρηστών, στις ηλεκτρονικές υπηρεσίες των σύγχρονων κατανεμημένων διαδικτυακών υποδομών έχουν αποτελέσει αντικείμενο έντονης ερευνητικής αλλά και επιχειρηματικής δραστηριότητας τα τελευταία χρόνια. Μάλιστα, η αυξανόμενη ευαισθητοποίηση του κοινού σχετικά με την προστασία ευαίσθητων και προσωπικών δεδομένων [101], έχει δώσει περαιτέρω ώθηση στη σχεδίαση και ανάπτυξη ολοκληρωτικών λύσεων προστασίας. Ιδιαίτερα, στο επίκεντρο των σχετικών προσεγγίσεων έχει βρεθεί η σύζευξη των υποδομών διαχείρισης εξουσιοδοτήσεων με τις αρχές της ιδιωτικότητας των χρηστών και της προστασίας της ασφάλειας των δεδομένων τους. Όπως προκύπτει και από την ενδελεχή μελέτη και τη διεξοδική ανάλυση των υφιστάμενων προτάσεων στον χώρο της διαχείρισης εξουσιοδοτήσεων σε ετερογενή περιβάλλοντα, έχουν προκύψει προσεγγίσεις που τοποθετούν την ιδιωτικότητα των χρηστών στο πυρήνα της λογικής και των λειτουργιών τους.

Ωστόσο, παρατηρείται στη βιβλιογραφία μια σχετικά μονομερής αντιμετώπιση του θέματος και η συνεπακόλουθη απουσία μιας ολιστικής προσέγγισης αντιμετώπισης του προβλήματος της ιδιωτικότητας και της ασφάλειας σε ένα γενικευμένο πλαίσιο. Πιο συγκεκριμένα, σε ένα μεγάλο ποσοστό οι υφιστάμενες *προσεγγίσεις διαχείρισης εξουσιοδοτήσεων* παραλληλίζουν το πρόβλημα της διαχείρισης της ιδιωτικότητας των χρηστών με το πρόβλημα της διατήρησης της ανωνυμίας τους, προωθώντας αποκλειστικά κρυπτογραφικές λύσεις απόκρυψης των στοιχείων των χρηστών (μέθοδοι ανωνυμοποίησης, αποδείξεις μηδενικής γνώσεις, ανώνυμα πιστοποιητικά μεταξύ άλλων). Αν και οι αμιγώς κρυπτογραφικές προτάσεις αποτελούν ένα σημαντικό βήμα προς τη σύζευξη ιδιωτικότητας και διαχείρισης εξουσιοδοτήσεων, η απουσία της οργανωμένης διαχείρισης κανόνων ελέγχου πρόσβασης και πολιτικών προστασίας της ασφάλειας των δεδομένων περιορίζει σημαντικά την πρακτική εφαρμογή τους. Προς τούτο, οι πλέον ολοκληρωμένες λύσεις, ενσωματώνουν κρυπτογραφικές τεχνικές διατήρησης της ανωνυμίας των χρηστών σε πρωτόκολλα διαχείρισης εξουσιοδοτήσεων με ρητές διαδικασίες και συγκεκριμένα βήματα ολοκλήρωσης, ωστόσο ακόμα και σε αυτές τις περιπτώσεις παρατηρείται η έλλειψη μεθόδων διαμόρφωσης σαφών πολιτικών προστασίας που αυτοματοποιούν τις

διαδικασίες στη βάση των προτιμήσεων ιδιωτικότητας των εμπλεκόμενων οντοτήτων. Το εν λόγω κενό, όπου και όταν προκύπτει, δυσχεραίνει σημαντικά την επίτευξη πλήρους συμβατότητας με τις απαιτήσεις ιδιωτικότητας και ασφάλειας, όπως εξάγονται από τη νομοθεσία και τα σχετικά πρότυπα.

Από τη σκοπιά των μοντέλων ελέγχου πρόσβασης και των εργαλείων διαμόρφωσης κανόνων προστασίας που εδράζονται στον πυρήνα των προσεγγίσεων διαχείρισης εξουσιοδοτήσεων, παρατηρείται σε ορισμένες περιπτώσεις η απουσία των απαιτούμενων σημασιολογικών δεδομένων που θα επιτρέψει την κάλυψη και ικανοποίηση του συνόλου των ειδικών απαιτήσεων που απορρέουν από την προστασία της ιδιωτικότητας σε ετερογενείς υποδομές. Χαρακτηριστικά, η χρήση πολιτικών χρήσης δεδομένων, η ικανοποίηση απαιτήσεων μεταφοράς των δικαιωμάτων των χρηστών και η αξιοποίηση λειτουργιών διαχωρισμού καθηκόντων μεταξύ άλλων, είθισται να μην αποτελούν τμήμα της βασικής λογικής των μοντέλων, με αποτέλεσμα να απαιτείται η αξιοποίηση εξειδικευμένων επεκτάσεων ή η προδιαγραφή πολλαπλών και πλεοναζόντων κανόνων για την κάλυψη των συγκεκριμένων αναγκών. Ομοίως, χαρακτηριστικό παράδειγμα αποτελεί το ισχύον επίπεδο της εμπιστοσύνης μεταξύ των εμπλεκόμενων φορέων, που σύμφωνα με τα συμπεράσματα που αναλύθηκαν στην ενότητα 2.3 συνιστά κριτήριο καθορισμού της συμπεριφοράς ενός πληροφοριακού συστήματος αναφορικά με την πρόσβαση σε ευαίσθητες πληροφορίες. Ειδικότερα, το επίπεδο της εμπιστοσύνης που συνοδεύει έναν οργανισμό, χαρακτηρίζει επίσης την ποιότητα των τοπικών πολιτικών έκδοσης και βεβαίωσης πιστοποιητικών και ιδιοτήτων, πληροφορίες που κατέχουν εξέχουσα σημασία κατά τη λήψη αποφάσεων πρόσβασης. Επιπρόσθετα, παρατηρείται μια αγνωστικιστική συμπεριφορά των μοντέλων σε σχέση με την υποκείμενη υποδομή και τις μονάδες της, γεγονός που περιορίζει την πλήρη προσαρμογή της διαμόρφωσης κανόνων ελέγχου πρόσβασης στις συγκεκριμένες δομές των συστημάτων διαχείρισης εξουσιοδοτήσεων. Επίσης, αν και υφίσταται έντονη δραστηριότητα στον τομέα των μοντέλων ελέγχου πρόσβασης για κατανεμημένα περιβάλλοντα, διακρίνεται στις προτάσεις που προκύπτουν η απουσία συγκεκριμένων προβλέψεων για τη διαλειτουργικότητα και τη διατήρηση σχέσεων εμπιστοσύνης μεταξύ των εταίρων μιας κατανεμημένης αρχιτεκτονικής. Ήτοι, οι εν λόγω λύσεις περιορίζονται συχνά στην προδιαγραφή αφαιρετικών κανόνων πρόσβασης, δεν εφαρμόζουν τις δυνατότητές τους σε ρεαλιστικά πρακτικά πρωτόκολλα επικοινωνίας, ενώ εργάζονται στο συμπέρασμα της εξ' ορισμού ύπαρξης εμπιστοσύνης μεταξύ των οντοτήτων των

συστημάτων. Ταυτόχρονα, υποδομές που μπορούν να θεμελιώσουν σχέσεις εμπιστευτικότητας και να αναδείξουν το επίπεδο εμπιστοσύνης που χαρακτηρίζει τις πολιτικές των διαφορετικών οντοτήτων, όπως είναι οι υποδομές PKI και PMI, δεν αξιοποιούνται στο έπακρο από τις υπάρχουσες προσεγγίσεις.

Στόχος της παρούσας διδακτορικής διατριβής αποτελεί η προδιαγραφή και ανάπτυξη ενός ολιστικού συστήματος διαχείρισης εξουσιοδοτήσεων με γνώμονα την προστασία της ιδιωτικότητας σε ετερογενή περιβάλλοντα. Προς τούτο, στα πλαίσια της εκπόνησης της διατριβής προδιαγράφηκε και αναπτύχθηκε ένα σύνολο συστημάτων, οργανωμένων ως μια κατανεμημένη και διασυνδεδεμένη συνομοσπονδία οντοτήτων. Το προτεινόμενο σύστημα παρεμβάλλεται στις διαδικασίες αλληλεπίδρασης και διαμοιρασμού πληροφορίας μεταξύ των οντοτήτων, με στόχο την εξασφάλιση της ιδιωτικότητας των χρηστών και την εμπιστευτικότητα των ευαίσθητων επιχειρηματικών πληροφοριών των οργανισμών. Οι εξουσιοδοτήσεις για πρόσβαση σε ευαίσθητα δεδομένα αποτελούν πληροφορία που εξάγεται μέσα από κανόνες ελέγχου πρόσβασης με ιδιότητες επίγνωσης του ισχύοντος πλαισίου, της ιδιωτικότητας των χρηστών και των γνωρισμάτων των συμμετεχόντων οντοτήτων. Επιπλέον ακολουθείται μια στρατηγική μεταφοράς όσο το δυνατόν μεγαλύτερου μέρους της επιχειρηματικής λογικής των παρόχων εντός της πλατφόρμας σε σχέση με την επεξεργασία των δεδομένων, με στόχο την αποκάλυψη όσο το δυνατόν λιγότερων προσωπικών δεδομένων και ευαίσθητων στοιχείων, ακόμα και αν υπάρχει η σχετική εξουσιοδότηση. Τα χαρακτηριστικά των υποδομών PKI αξιοποιούνται τόσο για τον προσδιορισμό του επιπέδου της εμπιστοσύνης που αποδίδεται στους εμπλεκόμενους φορείς όσο και για τον σαφή διαχωρισμό των διακριτών συνεργαζόμενων αλλά ετερογενών και αυτόνομων τομέων εμπιστοσύνης. Απώτερο σκοπό της προτεινόμενης λύσης συνιστά η προστασία των προσωπικών δεδομένων των χρηστών και ο έλεγχος του διαμοιρασμού τους στα πλαίσια ηλεκτρονικών διαδικασιών καθώς και η ελεγχόμενη πρόσβαση σε ευαίσθητα δεδομένα και υπηρεσίες των εμπλεκόμενων παρόχων.

4.1 Αρχές Σχεδίασης

Ο σχεδιασμός ενός συστήματος διαχείρισης εξουσιοδοτήσεων με επίγνωση της ιδιωτικότητας δεν μπορεί να θεωρηθεί μια αμιγώς τεχνική διαδικασία, αν ληφθούν υπόψη οι σημαντικές «κοινωνικές» επιπτώσεις που επιφέρει η λειτουργία του

συστήματος σχετικά με την προστασία των προσωπικών και ευαίσθητων δεδομένων των χρηστών του αλλά και γενικότερα στο δικαίωμα για ιδιωτικότητα. Το υποκείμενο νομικό και κανονιστικό περιβάλλον μιας υποδομής διαχείρισης εξουσιοδοτήσεων επηρεάζει άμεσα τις προς ικανοποίηση τεχνικές και τεχνολογικές απαιτήσεις, σε βαθμό τέτοιο που ενδεχόμενη απουσία της σαφούς αναγνώρισης των σχετικών νομικών και κανονιστικών διατάξεων να καταστεί την ενσωμάτωση των αναγκαίων και ικανών μηχανισμών προστασίας αδύνατη. Επιπρόσθετα, τα χαρακτηριστικά των μηχανισμών προστασίας πρέπει να παρέχουν δυνατότητες προσαρμογής στις σύγχρονες τεχνικές ηλεκτρονικής επιχειρηματικής δικτύωσης ([102]) των προστατευόμενων οργανισμών, εντός αλλά και εκτός των σχετικών ζωνών ασφάλειάς τους. Γίνεται προφανές, ότι προκειμένου οι οργανισμοί και πάροχοι υπηρεσιών που δραστηριοποιούνται στο Διαδίκτυο να επωφεληθούν ουσιαστικά από τη συμμετοχή τους σε συνεργατικά περιβάλλοντα και ψηφιακά οικοσυστήματα, απαιτείται η υιοθέτηση στρατηγικών, διοικητικών και οργανωτικών αλλαγών, οι οποίες με τη σειρά τους δεν μπορούν παρά να επηρεάζουν τις λειτουργικότητες των υποκείμενων συστημάτων προστασίας. Σε αυτό το πλαίσιο, η προτεινόμενη λύση σχεδιάστηκε στη βάση των παρακάτω αρχών:

- *Ροές πληροφορίας με επίγνωση της ιδιωτικότητας*: Η τάση που κυριαρχεί στις ηλεκτρονικές αγορές προς ανάθεση υπηρεσιών σε τρίτους και προς αποκέντρωση των πηγών δεδομένων, έχει επιφέρει τη διεξαγωγή όλο και μεγαλύτερου ποσοστού ηλεκτρονικών διαδικασιών σε συνεργατικά περιβάλλοντα «εικονικών» οργανισμών και τη δημιουργία «οικουμενικών» ροών δεδομένων. Ως αποτέλεσμα, προκύπτουν αυξανόμενα πολύπλοκες ροές παροχής υπηρεσιών που μπορεί να περιλαμβάνουν μεταξύ άλλων, πολλαπλούς παρόχους υπηρεσιών και περιεχομένου, επιχειρηματικούς φορείς, χρηματοπιστωτικά ιδρύματα, καθώς και απλούς χρήστες. Μάλιστα, όσο περισσότερο ενισχύεται η πολυπλοκότητα των παραγόμενων ροών υπηρεσιών, τόσο πληθύνονται και οι κίνδυνοι απώλειας της ιδιωτικότητας των εμπλεκόμενων οντοτήτων και ασφάλειας των αντίστοιχων δεδομένων. Σε αυτό το κλίμα, όπου οι κάτοχοι και επεξεργαστές δεδομένων δεν είναι υπεύθυνοι μόνο για τις προσωπικές τους πρακτικές αλλά και για τις πολιτικές προστασίας των οντοτήτων-συνδέσμων τους στην αλυσίδα παροχής υπηρεσίας, τα υφιστάμενα συστήματα διαχείρισης εξουσιοδοτήσεων πρέπει

να επιβάλουν τους κατάλληλους μηχανισμούς προστασίας προς παραγωγή ροών δεδομένων με επίγνωση της ιδιωτικότητας.

- *Προσαρμοστικότητα σε περιβάλλοντα πολλαπλών τομέων*: Το μοντέλο της κατανεμημένης λειτουργίας και η αποκεντρωμένη επιχειρηματικότητα των οργανισμών που δραστηριοποιούνται στο Διαδίκτυο, συνεπάγονται τον διαμοιρασμό των εμπλεκόμενων ευαίσθητων πληροφοριών μεταξύ διοικητικά και γεωγραφικά απομακρυσμένων οντοτήτων και τομέων. Σε αυτό το πλαίσιο, οι κατανεμημένες και αποκεντρωτικές προσεγγίσεις παρουσιάζουν μεγαλύτερη αποδοτικότητα και εφαρμοστικότητα από κεντρικοποιημένες προτάσεις.
- *Διαχείριση της ετερογένειας των οντοτήτων*: Οι αλληλεπιδρώντες οντότητες εργάζονται εντός ανεξάρτητων τομέων λειτουργίας και επομένως διατηρούν διακριτά μοντέλα οργάνωσης, υπηρετούν ατομικούς επιχειρηματικούς σκοπούς και αξιοποιούν διαφορετικές μεθόδους συνεργασίας. Ως άμεσο επακόλουθο, εμφανίζονται στις κατανεμημένες υποδομές συστημάτων υψηλά επίπεδα ετερογένειας σε ένα σύνολο χαρακτηριστικών (όπως είναι η σημασιολογία των πληροφοριών και τα κριτήρια επίτευξης σχέσεων εμπιστοσύνης) που επηρεάζουν άμεσα την ομαλή διαλειτουργικότητα των αλληλεπιδρώντων φορέων. Ως εκ τούτου, η αποδοτική διαχείριση της ετερογένειας των συμμετεχόντων είναι άρρηκτα συνδεδεμένη με την ομαλή λειτουργία των υποκείμενων συστημάτων.
- *Αυτονομία των οντοτήτων*: Ως επέκταση των ενεργειών διαχείρισης της ετερογένειας των οντοτήτων, η συγκεκριμένη αρχή αναφέρεται στην απαίτηση της «χαλαρής σύζευξης» (loose coupling) των συμμετεχόντων. Υπό αυτή την έννοια, κάθε εταίρος στην αλυσίδα παροχής υπηρεσιών διατηρεί την αυτονομία του σε ότι αφορά την εσωτερική λειτουργία του, η οποία επηρεάζεται στον ελάχιστο δυνατό βαθμό από ενδεχόμενες τροποποιήσεις ή ανακατατάξεις που μπορούν να ανακύψουν στο μοντέλο λειτουργίας απομακρυσμένων συνεργατών. Στην αντίθετη περίπτωση, αυτή της «αυστηρής σύζευξης» (tight coupling), απλές μεταβολές στο μοτίβο συμπεριφοράς κάποιου μέλους του συστήματος είναι δυνατόν να οδηγήσει σε αλυσιδωτές μετατροπές της λειτουργίας των αλληλεπιδρώντων εταίρων, δημιουργώντας σοβαρά θέματα κλιμακοθετησιμότητας του συστήματος. Σε

αυτό το πλαίσιο, το προτεινόμενο σύστημα διαχείρισης εξουσιοδοτήσεων σχεδιάστηκε στη λογική της οικονομίας της σύναψης σχέσεων αλληλεπίδρασης ομότιμου-προς-ομότιμο (Peer-to-Peer), οι οποίες αποτελούν χαρακτηριστικό παράδειγμα παραγωγής προβλημάτων κλιμακοθετησιμότητας ([103]).

- *Ενδυνάμωση του ρόλου των χρηστών*: Όπως έχει προαναφερθεί, το σύγχρονο επιχειρηματικό τοπίο έχει προσαρμοστεί στη σταδιακή μετατόπιση της επιχειρηματικότητας από την «από πάνω προς τα κάτω» (top-down) προς την «από κάτω προς τα πάνω» (bottom-up) λογική και στη συνεπαγόμενη ενδυνάμωση του ρόλου των τελικών χρηστών. Με αυτή την έννοια, η ενεργή συμμετοχή των χρηστών στην παροχή υπηρεσίας και κατ' επέκταση στις διαδικασίες παραγωγής αποφάσεων ελέγχου πρόσβασης αποτελεί τον ακρογωνιαίο λίθο κάθε συστήματος με επίγνωση της ιδιωτικότητας. Σημειώνεται ότι η συμβολή του χρήστη στις διαδικασίες ελέγχου πρόσβασης δεν πρέπει να περιορίζεται στην απλή παροχή μηνυμάτων συγκατάθεσης, αλλά να περιλαμβάνει την πραγματική προδιαγραφή και εφαρμογή προτιμήσεων ιδιωτικότητας και κανόνων πρόσβασης σε προσωπικά τους δεδομένα.
- *Συμμετρία λύσης*: Η αυξημένη πολυπλοκότητα των επιχειρηματικών συναλλαγών στις κατανεμημένες αρχιτεκτονικές του Διαδικτύου έχει ως αποτέλεσμα την ενεργοποίηση πολλαπλών ρόλων συμπεριφοράς από τα μέλη μιας συναλλαγής προς ικανοποίηση των στόχων της αλληλεπίδρασής τους. Χαρακτηριστικά, οι οντότητες που συμμετέχουν σε πολύπλοκες ροές εργασιών είναι δυνατό να ενεργούν τόσο ως πάροχοι πόρων όσο και ως καταναλωτές. Σε μια χρονική περίοδο που οι ρυθμοί υιοθέτησης των τεχνολογιών ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies – PETs) παρουσιάζονται κατώτεροι των περιστάσεων ([104], [105]) μια συμμετρική και ισορροπημένη στάση στην αντιμετώπιση των προβλημάτων ιδιωτικότητας μπορεί αφενός να αυξήσει θεαματικά την εφαρμοστικότητα των σχετικών λύσεων αφετέρου είναι σε θέση να μειώσει την πολυπλοκότητα και το κόστος της διαχείρισης των αναπτυχθέντων συστημάτων προστασίας. Ως εκ τούτου, η προτεινόμενη υποδομή διαχείρισης εξουσιοδοτήσεων επενδύει στην αξιοποίηση συμμετρικών λύσεων όπου αυτό είναι εφικτό:

- Αξιοποιούνται κοινά πρωτόκολλα επικοινωνίας και μεθοδολογίες επιχειρηματικής λογικής ανεξαρτήτως του ρόλου των εμπλεκόμενων οντοτήτων.
- Αναγνωρίζονται και χρησιμοποιούνται ενιαίες σημασιολογικές δομές για την προδιαγραφή των κανόνων ελέγχου πρόσβασης και των κανόνων χρήσης δεδομένων.
- Εφαρμόζονται κοινές μέθοδοι και τεχνικές διαχείρισης και προστασίας των δεδομένων, είτε αυτά αφορούν προσωπικά δεδομένα χρηστών είτε ευαίσθητα δεδομένα οργανισμών.

- *Διαφορετικοί στόχοι εξουσιοδότησης*: Αναγνωρίζεται και ικανοποιείται η ανάγκη εφαρμογής μηχανισμών εξουσιοδότησης με διαφορετικό πεδίο εφαρμογής από το προφανές, αυτό της απονομής δικαιωμάτων χρήσης ευαίσθητων δεδομένων. Πιο συγκεκριμένα, σε πολλές περιπτώσεις η ίδια η κατάθεση/παραγωγή αιτημάτων για πρόσβαση σε δεδομένα μπορεί να υπόκειται σε έλεγχο από τα εμπλεκόμενα μέλη. Χαρακτηριστικό παράδειγμα αποτελούν οι εργαζόμενοι ενός οργανισμού, που υποχρεούνται να υποβάλουν τις εξερχόμενες αιτήσεις τους για υπηρεσίες τρίτων σε έλεγχο εξουσιοδότησης. Η ικανοποίηση της συνθήκης αυτής απουσιάζει στην πλειοψηφία των προτεινόμενων λύσεων διαχείρισης εξουσιοδοτήσεων στη βιβλιογραφία.
- *Συμβατότητα με το νομικό και κανονιστικό περιβάλλον*: Απαραίτητη προϋπόθεση για την ανάπτυξη ενός ολοκληρωτικού συστήματος διαχείρισης εξουσιοδοτήσεων αποτελεί η ικανοποίηση των απαιτήσεων ασφάλειας και ιδιωτικότητας που αναλύθηκαν στην ενότητα 2.3.

Οι παραπάνω αρχές σχεδίασης υποδεικνύουν συγκεκριμένες επιλογές τεχνολογικών λύσεων που πραγματοποιήθηκαν στο πλαίσιο της εκπόνησης της παρούσας διατριβής και οι οποίες κωδικοποιούνται ως εξής:

- *Σημασιολογικό μοντέλο πληροφοριών*: Στον πυρήνα της προδιαγραφόμενης λύσης εντοπίζεται ένα σημασιολογικό μοντέλο με την κατάλληλη εκφραστικότητα για την κάλυψη των αρχών ιδιωτικότητας και ασφάλειας όπως αυτές αναγνωρίστηκαν και καταγράφηκαν στα πλαίσια της παρούσας διατριβής. Το μοντέλο αξιοποιεί τις δυνατότητες των σημασιολογικών τεχνολογιών τόσο προς ενίσχυση της ευελιξίας των πολιτικών όσο και προς

διευκόλυνση της αναπαράστασης και της διαμόρφωσης των σχετικών κανόνων πρόσβασης. Βασικοί πυλώνες του μοντέλου υπό υλοποίηση αποτελούν η αναγνώριση του σκοπού της πρόσβασης, η επίγνωση των συνθηκών πρόσβασης, η προσαρμογή των εξουσιοδοτήσεων στα χαρακτηριστικά των χρηστών και η επισήμανση των απορρεόντων υποχρεώσεων και περιορισμών. Το σύνολο των επιμέρους εννοιών (που εμπλέκονται στη διαδικασία παραγωγής εξουσιοδοτήσεων και απόδοσης δικαιωμάτων πρόσβασης σε προσωπικά δεδομένα καλείται «πλαίσιο ιδιωτικότητας». Ο τρόπος αξιοποίησης κάθε στοιχείου του πλαισίου ιδιωτικότητας από το σύστημα εξουσιοδοτήσεων επιτρέπει μια επιπλέον κατηγοριοποίηση των αναγνωρισμένων εννοιών, μη σημασιολογική αυτή τη φορά. Έτσι, στοιχεία του πλαισίου ιδιωτικότητας που αναφέρονται σε παραμέτρους και ποιότητες γνωστές στο σύστημα πριν την ενεργοποίησή του για παραγωγή μια απόφασης ελέγχου πρόσβασης συναποτελούν το «**στατικό πλαίσιο ιδιωτικότητας**». Ωστόσο, συγκεκριμένα χαρακτηριστικά του πλαισίου ιδιωτικότητας δεν είναι δυνατόν να είναι γνωστά *a-priori* από το σύστημα εξουσιοδοτήσεων παρά μόνο σε πραγματικό χρόνο και ως εκ τούτου σχηματίζουν το «**δυναμικό πλαίσιο ιδιωτικότητας**».

- *Έλεγχος πρόσβασης και κανόνες χρήσης δεδομένων*: Το σημασιολογικό μοντέλο αξιοποιείται από τις οντότητες του συστήματος (χρήστες και οργανισμοί) για την προδιαγραφή ρητών πολιτικών ελέγχου πρόσβασης αλλά και κανόνων εξειδικευμένης αξιοποίησης/χρήσης των δεδομένων για τα οποία έχει ήδη παραχθεί θετική απόφαση πρόσβασης. Οι κανόνες χρήσης δεδομένων αφορούν βασικά ενέργειες περαιτέρω προώθησης των δεδομένων και μεταφοράς των δικαιωμάτων πρόσβασης σε τρίτες οντότητες.
- *Μηχανή παραγωγής συλλογισμών και κλιμακοθετησιμότητα*: Οι τελικές εξουσιοδοτήσεις παράγονται μετά την εφαρμογή συμπερασματικών αλγορίθμων όπου λαμβάνονται υπόψη τα παραπάνω χαρακτηριστικά καθώς και οι σχετικές ιεραρχίες και συσχετίσεις μεταξύ των εννοιών στα πλαίσια του σημασιολογικού μοντέλου. Προς ενίσχυση της αποδοτικότητας και της κλιμακοθετησιμότητας του υποδομής η εφαρμογή των συμπερασματικών αλγορίθμων πραγματοποιείται πριν την εκκίνηση του συστήματος (φάση διαμόρφωσης και παραμετροποίησης του συστήματος) και το αποτέλεσμα

αυτής αποτυπώνεται στη μορφή πιστοποιητικών ιδιοτήτων τα οποία κατά τη διάρκεια της λειτουργίας του συστήματος αξιοποιούνται ως αποδείξεις εξουσιοδότησης. Με αυτόν τον τρόπο, σε πραγματικό χρόνο οι υπολογιστικές ανάγκες της υποδομής αναφορικά με την αποτίμηση των δικαιωμάτων χρηστών περιορίζονται στην αναγνώριση των τρεχόντων συνθηκών πρόσβασης.

- *Αξιοποίηση Υποδομών Δημόσιου Κλειδιού και Υποδομών Διαχείρισης Δικαιωμάτων*: Οι εμπλεκόμενοι φορείς οργανώνονται ως ζεύγη σημείων PEP/PDP σε μια υποδομή PKI/PMI με ενσωμάτωση μιας Αρχής Πιστοποίησης Γέφυρας. Η συγκεκριμένη επιλογή στόχο έχει τον εμπλουτισμό του μοντέλου με κρίσιμες πληροφορίες που απορρέουν από την υποκείμενη αρχιτεκτονική, όπως είναι το επίπεδο LoA των εμπλεκόμενων φορέων αλλά και η συντήρηση μιας υποδομής εντός της οποίας η εμπιστοσύνη μεταξύ των εταίρων θεωρείται εξασφαλισμένη και αδιαπραγμάτευτη.

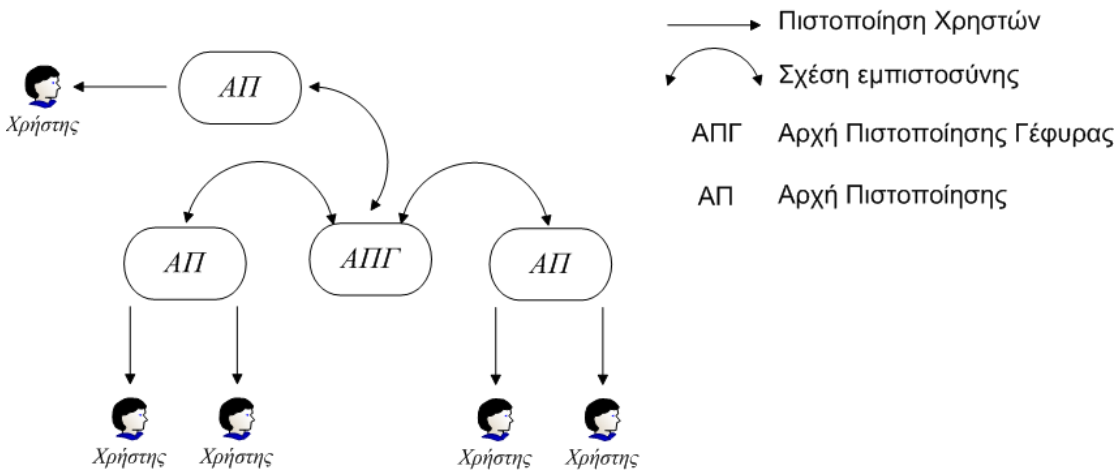
4.2 Αρχιτεκτονική Κατανεμημένης Πλατφόρμας

Η προτεινόμενη πλατφόρμα διαχείρισης εξουσιοδοτήσεων αναπτύχθηκε στη βάση μιας συνεκτικής αρχιτεκτονικής η οποία σχεδιάστηκε με γνώμονα τη διευκόλυνση της σύναψης στρατηγικών και λειτουργικών σχέσεων μεταξύ απομακρυσμένων εταίρων, ενώ παράλληλα ικανοποιείται η συμβατότητα με τις προαναφερθείσες λειτουργικές και μη λειτουργικές απαιτήσεις. Βασική προτεραιότητα κατά τον σχεδιασμό της αρχιτεκτονικής της πλατφόρμας αποτέλεσε η ενσωμάτωση των κατάλληλων δομικών στοιχείων που αφενός θα ενέπλεκε τις εμπλεκόμενες οντότητες σε ένα περιβάλλον εγγυημένης εμπιστοσύνης αφετέρου θα ικανοποιούσε την ανάγκη των συμμετεχόντων για αυτονομία στην προδιαγραφή των ατομικών τους απαιτήσεων ιδιωτικότητας σχετικά με τα ευαίσθητά τους δεδομένα. Σε αυτό το πλαίσιο, το μοντέλο εμπιστοσύνης των διακριτών οντοτήτων της πλατφόρμας που υιοθετήθηκε και επιβλήθηκε στην αναπτυχθείσα λύση διετέλεσε σημαντικό ρόλο για τη διαμόρφωση της τελικής αρχιτεκτονικής των συστημάτων.

Ο όρος **μοντέλο εμπιστοσύνης** αναφέρεται στη συγκεκριμένη στρατηγική και στους εξειδικευμένους μηχανισμούς που ενεργοποιούνται για την αποσαφήνιση της νομιμότητας, εγκυρότητας και εμπιστευτικότητας των αλληλεπιδρώντων φορέων στο πλαίσιο της λειτουργίας της πλατφόρμας. Όπως έχει αναλυθεί τα παραδοσιακά

σχήματα Υποδομών Διαχείρισης Ταυτοτήτων, ιεραρχικά οργανωμένων Αρχών Πιστοποίησης και αρχιτεκτονικής πλέγματος, βασίζουν τη λειτουργία τους στη σύναψη σχέσεων εμπιστοσύνης «ομότιμου-προς-ομότιμο» κι επομένως δεν ικανοποιούν την αρχή της χαλαρής σύζευξης των εμπλεκομένων. Αντίθετα, τα κατανεμημένα μοντέλα εμπιστοσύνης επενδύουν στη *μεταφερσιμότητα* της ποιότητας της εμπιστοσύνης, ήτοι στη δυνατότητα των οντοτήτων να εμπιστεύονται απομακρυσμένους εταίρους ακόμα κι εν τη απουσία άμεσης σχέσης εμπιστοσύνης με την προϋπόθεση της ύπαρξης ενδιάμεσου φορέα κοινής αποδοχής. Με αυτό τον τρόπο, καταπολεμούν μια σειρά μειονεκτημάτων των παραδοσιακών μοντέλων και προσαρμόζονται πιο αποδοτικά στις απαιτήσεις κατανεμημένων υποδομών.

Στα πλαίσια του προτεινόμενου μοντέλου επιλέχθηκε το μοντέλο Αρχής Πιστοποίησης Γέφυρας για τον σχηματισμό μιας συνομοσπονδίας οντοτήτων, οι σχέσεις των οποίων θεωρούνται εκ προοιμίου σχέσεις εμπιστοσύνης. Η επιλογή αυτή άμεσα συνεπάγεται την τοποθέτηση μιας κεντρικής οντότητας εντός της συνομοσπονδίας, τα καθήκοντα της οποίας ταυτίζονται με αυτά μιας Αρχής Πιστοποίησης Γέφυρας. Η συγκεκριμένη μονάδα, αποτελεί τον συνδετικό κρίκο μεταξύ διακριτών και αυτόνομων τομέων εμπιστευτικότητας, οι οποίοι εκπροσωπούνται στη συνομοσπονδία από ανεξάρτητες Αρχές Πιστοποίησης. Οι τελευταίες επισυνάπτοντας σχέσεις εμπιστοσύνης με την Αρχή Πιστοποίησης Γέφυρας, αφενός ελαχιστοποιούν τον αριθμό των απαιτούμενων άμεσων σχέσεων εμπιστοσύνης με τις λοιπές Αρχές Πιστοποίησης, αφετέρου εκμεταλλευόμενες τη μεταφερσιμότητα της ποιότητας της εμπιστοσύνης, επιτυγχάνουν να σχηματίσουν μια συνομοσπονδία εμπιστοσύνης μεταξύ αυτόνομων τομέων εμπιστευτικότητας. Υπενθυμίζεται ότι η Αρχή Πιστοποίησης Γέφυρας δεν αναγνωρίζεται ως σημείο εμπιστοσύνης από τους χρήστες που ενεργοποιούνται εντός της συνομοσπονδίας, καθιστώντας υπεύθυνες για αυτόν τον σκοπό τις ανεξάρτητες Αρχές Πιστοποίησης. Μια σχηματική απεικόνιση του περιγραφόμενου πλαισίου εμπιστοσύνης παρουσιάζεται στην Εικόνα 9.



Εικόνα 9: Πλαίσιο εμπιστοσύνης υποδομής διαχείρισης εξουσιοδοτήσεων

Σε συμφωνία με το υιοθετημένο μοντέλο εμπιστοσύνης, το σύνολο των χαρακτηριστικών και των λειτουργικοτήτων της πλατφόρμας διαχείρισης εξουσιοδοτήσεων εντοπίζονται σε δύο θεμελιώδη δομικά στοιχεία, που στα πλαίσια της παρούσας διατριβής ονομάστηκαν **Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας** (ΕΣΙ) και **Κέντρο Διαχείρισης Εξουσιοδοτήσεων** (ΚΔΕ) αντίστοιχα. Ειδικότερα, η οντότητα ΕΣΙ αναλαμβάνει εξ' ολοκλήρου τα καθήκοντα της ΑΠΓ της υποδομής εμπιστοσύνης ενώ παράλληλα υπηρετεί καθήκοντα επίβλεψης και ελέγχου της συνολικής λειτουργίας του πλαισίου διαχείρισης εξουσιοδοτήσεων. Αναλυτικά τα καθήκοντα της ΕΣΙ είναι τα ακόλουθα:

- Ο σχηματισμός και ο συντονισμός της **Συνομοσπονδίας Ομότιμων Ιδιωτικότητας** (ΣΟΙ) εντός των διοικητικών ορίων της οποίας η εμπιστοσύνη θεωρείται δεδομένη. Προς τούτο, η μονάδα εκδίδει ψηφιακά πιστοποιητικά προς τα Κέντρα Διαχείρισης Εξουσιοδοτήσεων εντός της Συνομοσπονδίας αναγνωρίζοντας τη νομιμότητα και την εγκυρότητα τους. Στα εν λόγω πιστοποιητικά είναι δυνατόν να καταγράφει και πληροφορίες που εξειδικεύουν το επίπεδο εμπιστοσύνης σε συγκεκριμένα χαρακτηριστικά του εκάστοτε ΚΔΕ.
- Η διαμόρφωση του ενιαίου σημασιολογικού μοντέλου πληροφοριών που υποστηρίζει τη λειτουργία της πλατφόρμας και τη διεξαγωγή συναλλαγών εντός των ορίων της. Το διαμορφωθέν μοντέλο περιλαμβάνει το σύνολο των απαραίτητων εννοιών για την προδιαγραφή κανόνων ελέγχου πρόσβασης και διαχείρισης εξουσιοδοτήσεων στο πλαίσιο συναλλαγών που συνεπάγονται πρόσβαση σε δεδομένα υπό προστασία.

- Η προδιαγραφή κοινών κανόνων εξουσιοδότησης για πρόσβαση στα δεδομένα που διακινούνται εντός της Συνομοσπονδίας. Προς τούτο, στη βάση του μοντέλου πληροφοριών της πλατφόρμας, η μονάδα ΕΣΙ παράγει και δημοσιοποιεί γενικευμένους κανόνες πρόσβασης που επηρεάζουν τον διαμοιρασμό πληροφοριών μεταξύ των συμμετεχόντων, όπου αυτό κρίνεται απαραίτητο.

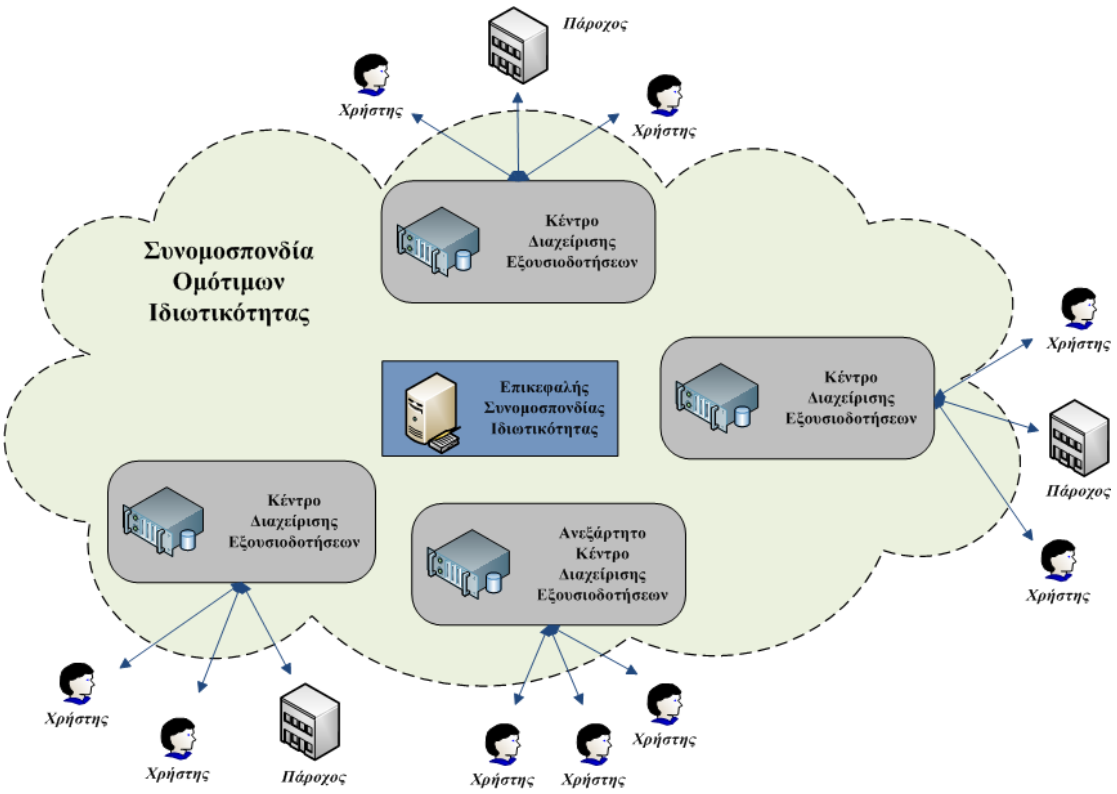
Συνολικά, το υποσύστημα του Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας εξυπηρετεί ως ένας ανεξάρτητος κόμβος εμπιστοσύνης, μέσω του οποίου αυτόνομες οντότητες μπορούν να εισέλθουν σε μια ζώνη συνεταιρισμού και εμπιστευτικότητας. Τον ρόλο του Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας στην υποδομή εξουσιοδοτήσεων μπορεί να διαδραματίσει μια τρίτη οντότητα κοινής εμπιστοσύνης ή ακόμα μια ομάδα μελών-αντιπροσώπων των εταίρων της Συνομοσπονδίας. Ωστόσο, αποκλειστικά η συμμετοχή τους στη Συνομοσπονδία δεν εξασφαλίζει στις εμπλεκόμενες οντότητες την προστασία των ευαίσθητων δεδομένων τους, διαδικασία για την οποία είναι υπεύθυνα τα Κέντρα Διαχείρισης Εξουσιοδοτήσεων. Οι μονάδες ΚΔΕ αποτελούν τους προσωπικούς πράκτορες προστασίας των παρόχων υπηρεσιών και ταυτοτήτων που συμμετέχουν στη Συνομοσπονδία, δρώντας ως μεσολαβητές μεταξύ των πόρων υπό προστασία και των πιθανών καταναλωτών πόρων, σε μια σχέση «ένα προς ένα». Σημειώνεται ότι στο πλαίσιο της Συνομοσπονδίας ένας οργανισμός δύναται να δραστηριοποιείται τόσο ως πάροχος υπηρεσιών όσο και ως πάροχος ταυτοτήτων. Στην πρώτη περίπτωση ο οργανισμός ενεργεί προσφέροντας υπηρεσίες και δεδομένα προς τους λοιπούς «συνομοσπονδιακούς οργανισμούς» και αξιοποιεί τις λειτουργικότητες των ΚΔΕ προς την προστασία των ευαίσθητων επιχειρηματικών του δεδομένων αλλά και των προσωπικών δεδομένων των χρηστών που υπάγονται σε αυτόν, ενώ στη δεύτερη περίπτωση δημιουργεί, διατηρεί και διαχειρίζεται πληροφορίες ταυτότητας των χρηστών του και εκμεταλλεύεται τις μονάδες ΚΔΕ για την προστασία των συγκεκριμένων ταυτοποιητικών προσωπικών δεδομένων. Στη συνέχεια της παρούσας διατριβής και χάριν συντομίας, οι οργανισμοί της Συνομοσπονδίας καλούνται απλά πάροχοι, ανεξαρτήτως του ρόλου που διαδραματίζουν στην εκάστοτε ροή υπηρεσιών. Άλλωστε, όπως έχει προαναφερθεί είναι πολύ πιθανό ένας οργανισμός να ενεργοποιεί τους δύο ρόλους ταυτόχρονα. Ταυτόχρονα, είναι σύνηθες συγκεκριμένα δεδομένα να αποτελούν παράλληλα επιχειρηματικά αλλά και προσωπικά δεδομένα. Χαρακτηριστικό παράδειγμα αποτελούν τα ταυτοποιητικά δεδομένα των υπαλλήλων μιας επιχείρησης, τα οποία

συνιστούν τόσο προσωπικά δεδομένα υπό το πρίσμα του υποκείμενου των δεδομένων όσο και ευαίσθητη επιχειρηματική πληροφορία υπό το πρίσμα του οργανισμού. Εκτός όμως από χρήστες που υπάγονται σε οργανισμούς και οι οποίοι αξιοποιούν το αντίστοιχο ΚΔΕ για την προστασία των προσωπικών τους δεδομένων, η πλατφόρμα εξυπηρετεί χρήστες που δεν ανήκουν σε κάποιον οργανισμό εντός της Συνομοσπονδίας, προβλέποντας τη λειτουργία ενός **Ανεξάρτητου Κέντρου Διαχείρισης Εξουσιοδοτήσεων** (ΑΚΔΕ) το οποίο εργάζεται αποκλειστικά ως πάροχος ταυτοτήτων. Αναλυτικά τα καθήκοντα των ΚΔΕ είναι τα ακόλουθα:

- Η υποστήριξη των κατάλληλων λειτουργιών για την προδιαγραφή και διαχείριση πολιτικών ελέγχου πρόσβασης και κανόνων χρήσης δεδομένων από τους χρήστες του συστήματος και τους οργανισμούς της Συνομοσπονδίας. Οι συγκεκριμένες ενέργειες λαμβάνουν χώρα στη βάση σημασιολογικού μοντέλου που παράγεται τοπικά στο κάθε ΚΔΕ και εξυπηρετεί τον αντίστοιχο οργανισμό και τους αντίστοιχους χρήστες.
- Η εξασφάλιση της σημασιολογικής διαλειτουργικότητας των οργανισμών και της οντότητας ΕΣΙ σχετικά με τα μοντέλο πληροφοριών που έχει παραγάγει ο Επικεφαλής. Προς τούτο, κάθε ΚΔΕ εκδίδει συγκεκριμένες οδηγίες εξίσωσης των τοπικών του σημασιολογιών με τα συγκεκριμένα σημασιολογικά στιγμιότυπα που εξυπηρετούν ως σημείο αναφοράς εντός της Συνομοσπονδίας.
- Η παροχή των κατάλληλων διεπαφών για την εξυπηρέτηση αιτήσεων για πρόσβαση σε δεδομένα καθώς και των απαραίτητων μέσων αποθήκευσης για τα διακινούμενα εντός της Συνομοσπονδίας δεδομένα. Σημειώνεται ότι, κατά τη διάρκεια της λειτουργίας της πλατφόρμας οι πάροχοι και οι χρήστες του συστήματος τροφοδοτούν το σύστημα με τα απαραίτητα δεδομένα τα οποία έκτοτε δεν εγκαταλείπουν τα διοικητικά όρια της Συνομοσπονδίας. Εναλλακτικά, δύνανται οι πάροχοι και οι χρήστες να προ-φορτώσουν κάποια δεδομένα στα ΚΔΕ.
- Η εφαρμογή των απαραίτητων μηχανισμών για τη διεξαγωγή ελέγχου πρόσβασης και διαχείρισης εξουσιοδοτήσεων στο πλαίσιο κατατεθειμένων αιτημάτων για πρόσβαση σε δεδομένα.
- Η διαχείριση των σχέσεων εμπιστοσύνης με τον οργανισμό και τους χρήστες που αξιοποιούν το εκάστοτε ΚΔΕ για την προστασία των ευαίσθητων

δεδομένων τους. Προς τούτο, κάθε μονάδα εκδίδει ψηφιακά πιστοποιητικά προς τους αντίστοιχους χρήστες αναγνωρίζοντας την εγκυρότητα τους, ενώ αναλαμβάνει και τις διαδικασίες πιστοποίησης με την οντότητα ΕΣΙ. Επιπλέον των αρμοδιοτήτων μιας ΑΠ, τα ΚΔΕ αναλαμβάνουν και καθήκοντα Αρχών Εξουσιοδοτήσεων εντός της Συνομοσπονδίας, βρισκόμενα υπεύθυνα για την παραγωγή και τη διάθεση πιστοποιητικών ιδιοτήτων στους χρήστες που υπάγονται σε αυτούς.

Μια επισκόπηση της οργάνωσης των βασικών δομικών μονάδων της Συνομοσπονδίας παρουσιάζεται στην Εικόνα 10.



Εικόνα 10: Εποπτική εικόνα αρχιτεκτονικής της Συνομοσπονδίας Ομότιμων Ιδιωτικότητας

Υπενθυμίζεται ότι κάθε χρήστης που αξιοποιεί έναν κόμβο ΚΔΕ αυτόματα υπάγεται στον αντίστοιχο οργανισμό που εξυπηρετεί ο συγκεκριμένος κόμβος. Το γεγονός αυτό συνεπάγεται ότι αφενός ο πάροχος μπορεί να επηρεάσει άμεσα, αλλά όχι τελεσίδικα, την πρόσβαση στα προσωπικά δεδομένα των χρηστών μέσω της προδιαγραφής κατάλληλων κανόνων, αφετέρου τα αιτήματα των συγκεκριμένων χρηστών για πρόσβαση σε δεδομένα τρίτων ΚΔΕ είναι δυνατόν να υπόκεινται σε επιπρόσθετο έλεγχο εξουσιοδότησης από τον τοπικό οργανισμό.

4.3 Μοντέλο Πληροφοριών

Στόχος της παρούσας ενότητας αποτελεί η περιγραφή του μοντέλου πληροφοριών που συνιστά τη βάση λειτουργίας της πλατφόρμας και της διεξαγωγής των συναλλαγών μεταξύ των διακριτών υποσυστημάτων της. Το εν λόγω μοντέλο σχεδιάστηκε έτσι ώστε να περιλαμβάνει όλες τις απαραίτητες έννοιες για την κατάλληλη μοντελοποίηση του προβλήματος διαχείρισης εξουσιοδοτήσεων και τη διαχείριση των καταγεγραμμένων λειτουργικών απαιτήσεων του συστήματος σε ότι αφορά την προδιαγραφή πολιτικών ιδιωτικότητας και την εξαγωγή αποφάσεων ελέγχου πρόσβασης και εξουσιοδότησης.

4.3.1 Βασικές Έννοιες

Απώτερος σκοπός του προδιαγραφόμενου πληροφοριακού μοντέλου αποτελεί η υποστήριξη ενός μοντέλου ελέγχου πρόσβασης με επίγνωση της ιδιωτικότητας και των γνωρισμάτων των χρηστών του. Υπό αυτή τη σκοπιά οι βασικές έννοιες που ενσωματώνει το μοντέλο είναι οι ακόλουθες:

- *Τύποι Δεδομένων* (Data Types – DT), που αναπαριστούν τους διαφορετικούς τύπους δεδομένων που αποτελούν αντικείμενο προστασίας και που εμπεριέχονται στις ηλεκτρονικές συναλλαγές εντός της Συνομοσπονδίας. Υπενθυμίζεται ότι πληροφορία υπό προστασία μπορεί να συνιστά οποιοδήποτε σύνολο προσωπικών αλλά και ευαίσθητων επιχειρηματικών δεδομένων.
- *Σκοποί Πρόσβασης* (Purposes – Pu), που συναποτελούν το σύνολο των διαφορετικών στοχεύσεων των υποκείμενων αιτήσεων πρόσβασης, ενώ οργανώνονται σε μια αναλυτική ταξινόμηση που περιλαμβάνει τόσο στοιχειώδεις ατομικούς σκοπούς όσο και σύνθετους στόχους.
- *Ρόλοι* (Roles – R), που – σε συμφωνία με την πλειοψηφία των συγγενών προσεγγίσεων – αντικατοπτρίζει τους λειτουργικούς ρόλους που αναλαμβάνουν χρήστες εντός των διοικητικών ορίων οργανισμών.
- *Χρήστες* (Users – U), που αναφέρονται στο σύνολο των ανθρώπων – χρηστών της πλατφόρμας και οι οποίοι συνδυάζονται με έναν ή περισσότερους λειτουργικούς ρόλους.

- *Κανόνες* (Rules – Ru), που αναπαριστούν τους πραγματικούς κανόνες ελέγχου πρόσβασης (αδειοδοτήσεις και απαγορεύσεις), χρήσης δεδομένων (εκμετάλλευσης δεδομένων μετά την αποκάλυψη τους) και μεταφοράς δικαιωμάτων πρόσβασης (μεταφορά αδειοδοτήσεων και απαγορεύσεων).
- *Συνθήκες* (Conditions – C), που θέτουν πραγματικού χρόνου περιορισμούς σχετικά με την πρόσβαση και χρήση των δεδομένων υπό προστασία. Οι Συνθήκες διακρίνονται σε επιμέρους κατηγορίες, καθεμία από τις οποίες εξυπηρετεί συγκεκριμένους σκοπούς μοντελοποίησης. Έτσι αξιοποιούνται,
    - *Χρονικές Συνθήκες*, που περιλαμβάνουν απεικονίσεις χρονικών στιγμιότυπων και διαστημάτων,
    - *Χωρικές Συνθήκες*, που περιλαμβάνουν φυσικές απεικονίσεις γέω-συντεταγμένων και αναπαραστάσεις λογικών τοποθεσιών,
    - *Συνθήκες Γνωρισμάτων*, που επιτρέπουν τη μοντελοποίηση συνθηκών σχετικά με τα γνωρίσματα των χρηστών καθώς και τις ιδιότητες των πόρων υπό προστασία και
    - *Συνθήκες Ασφάλειας*, που προσδιορίζουν περιορισμούς με άμεση συσχέτιση στα χαρακτηριστικά ασφάλειας της υποκείμενης υποδομής και των εμπλεκόμενων μηχανισμών.
- *Υποχρεώσεις* (Obligations – O), που αναπαριστούν επιπρόσθετες συμπληρωματικές ενέργειες που πρέπει να διεξαχθούν στο περιθώριο της εφαρμογής κάποιου κανόνα πρόσβασης ή αξιοποίησης δεδομένων. Οι Υποχρεώσεις εμπίπτουν σε δύο ευρείες κατηγορίες: προ-δραστικές και μετά-δραστικές. Οι πρώτες αντιστοιχούν σε δραστηριότητες που πρέπει να εκτελεστούν πριν την επιβολή του σχετικού κανόνα, ενώ οι δεύτερες αναπαριστούν διαδικασίες που πρέπει να ενεργοποιηθούν μετά την εκτέλεση της απόφασης του κανόνα.

Από την παραπάνω καταγραφή γίνεται φανερό ότι τα σύνολα των Κανόνων, Συνθηκών και Υποχρεώσεων συνιστούν την απαραίτητη πληροφορία για την κατάλληλη μοντελοποίηση των πραγματικών κανόνων εξουσιοδότησης, ήτοι αδειοδοτήσεις και απαγορεύσεις για πρόσβαση σε ευαίσθητα δεδομένα και πραγματικού χρόνου περιορισμοί και υποχρεώσεις σε σχέση με την εφαρμογή των

κανόνων. Τα υπόλοιπα σύνολα συναποτελούν βασικά εργαλεία για τη μοντελοποίηση των σημαντικών εννοιών που απορρέουν από τη λειτουργία της πλατφόρμας.

4.3.2 Συσχετίσεις Συνόλων

Η σημασία και χρησιμότητα των παραπάνω συνόλων αναδεικνύονται μέσω της προδιαγραφής των κατάλληλων εννοιολογικών δομών συσχέτισης αλλά και σχέσεων γενίκευσης και ειδίκευσης για την παραγωγή σύνθετων εννοιών και ολοκληρωμένων νοημάτων. Ιδιαίτερη σημασία αποκτούν οι σχέσεις που προδιαγράφηκαν στο πλαίσιο της συσχέτισης των στιγμιότυπων εκείνων των συνόλων του πληροφοριακού μοντέλου που συνιστούν τα βασικά εργαλεία εκφραστικότητας, ήτοι των συνόλων DT, Pu και R. Στοχεύοντας στον φορμαλισμό των ιδιοτήτων της κληρονομικότητας χαρακτηριστικών μεταξύ των ατόμων των συνόλων και της «εννοιολογικής συμπερίληψης» ενός ατόμου από ένα άλλο άτομο του ίδιου συνόλου, προδιαγράφηκαν και τα αντίστοιχα είδη συσχετίσεων. Οι συγκεκριμένες ιδιότητες αποσκοπούν στην αποφυγή της επανάληψης ορισμού κοινών χαρακτηρισμών και μεθόδων και εν τέλει στη μεγαλύτερη κλιμακοθετησιμότητα της προδιαγραφής κανόνων. Οι εν λόγω σχέσεις δημιουργούν επιμέρους σύνολα μερικής διάταξης (partially ordered sets), ενώ είναι μεταβατικές (transitive) και αντί-συμμετρικές (anti-symmetric).

Πιο συγκεκριμένα:

- Ένας τύπος δεδομένων του συνόλου DT, dt_i κληρονομεί από ένα άλλο τύπο δεδομένων dt_j, όταν τα χαρακτηριστικά του dt_j κληρονομούνται στο dt_i σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $dt_i \blacktriangleleft dt_j$, για $dt_i, dt_j \in DT$ και ουσιαστικά δημιουργεί ιεραρχικούς υπό-γράφους με σχέσεις OR μεταξύ των κόμβων του.
- Ένας τύπος δεδομένων του συνόλου DT, dt_i εμπεριέχεται σε ένα άλλο τύπο δεδομένων dt_j, όταν το αντικείμενο dt_i αποτελεί εννοιολογικά τμήμα του dt_j σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $dt_i \angle dt_j$, για $dt_i, dt_j \in DT$ και ουσιαστικά δημιουργεί ιεραρχικούς υπό-γράφους με σχέσεις AND μεταξύ των κόμβων του.

Ομοίως αναγνωρίζονται και οι ακόλουθες σχέσεις των αντικειμένων των συνόλων Pu και R:

- Ένας σκοπός πρόσβασης του συνόλου Pu, pu_i κληρονομεί από ένα άλλο σκοπό πρόσβασης pu_j, όταν τα χαρακτηριστικά του pu_j κληρονομούνται στο pu_i σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $pu_i \blacktriangleleft pu_j$, για $pu_i, pu_j \in Pu$.
- Ένας σκοπός πρόσβασης του συνόλου Pu, pu_i εμπεριέχεται σε ένα άλλο σκοπό πρόσβασης pu_j, όταν το αντικείμενο pu_i αποτελεί εννοιολογικά τμήμα του pu_j σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $pu_i \angle pu_j$, για $pu_i, pu_j \in Pu$.
- Ένας ρόλος του συνόλου R, r_i κληρονομεί από ένα άλλο ρόλο r_j, όταν τα χαρακτηριστικά του r_j κληρονομούνται στο r_i σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $r_i \blacktriangleleft r_j$, για $r_i, r_j \in R$.
- Ένας ρόλος του συνόλου R, r_i εμπεριέχεται σε ένα άλλο ρόλο r_j, όταν το αντικείμενο r_i αποτελεί εννοιολογικά τμήμα του r_j σε ότι αφορά την εφαρμογή των προδιαγεγραμμένων κανόνων εξουσιοδότησης. Η σχέση δηλώνεται ως $r_i \angle r_j$, για $r_i, r_j \in R$.

Οι εκφράσεις *Προσωπικός Αριθμός Τηλεφώνου* ◄ *Πληροφορίες Επικοινωνίας* και (*Αναγνωριστικό Χρήστη*, *Αναγνωριστικό Τομέα Δικτύου*) ∠ *Διεύθυνση Ηλεκτρονικού Ταχυδρομείου* απεικονίζουν ότι ο τύπος δεδομένων *Προσωπικός Αριθμός Τηλεφώνου* κληρονομεί τα χαρακτηριστικά του τύπου δεδομένων *Πληροφορίες Επικοινωνίας* σε ότι αφορά την εφαρμογή κανόνων εξουσιοδότησης, ενώ ο τύπος *Διεύθυνση Ηλεκτρονικού Ταχυδρομείου* συναποτελείται από τους τύπους *Αναγνωριστικό Χρήστη* και *Αναγνωριστικό Τομέα Δικτύου* αντίστοιχα.

Παράδειγμα 1: Κληρονομικότητα χαρακτηριστικών

Σε ότι αφορά το σύνολο των Συνθηκών (C) και των Υποχρεώσεων (O) ακολουθήθηκε ένα παρόμοιο πρότυπο συσχέτισης των στιγμιότυπων των συνόλων για την παραγωγή σύνθετων νοημάτων μέσω της ενεργοποίησης λογικών σχέσεων AND και OR. Έτσι:

- Μια σύνθετη συνθήκη $c_k \in C$, μπορεί να προδιαγραφεί ως $c_k = (c_{k1} \wedge c_{k2} \wedge \ldots \wedge c_{kn})$, ως $(c_{k1} \vee c_{k2} \vee \ldots \vee c_{kn})$ ή αξιοποιώντας οποιανδήποτε συνδυασμό OR/AND σχέσεων.

- Ομοίως, ένα αντικείμενο $o_k \in O$, μπορεί να προδιαγραφεί ως $o_k = (o_{k1} \wedge o_{k2} \wedge \ldots \wedge o_{kn})$, ως $(o_{k1} \vee o_{k2} \vee \ldots \vee o_{kn})$ ή αξιοποιώντας οποιανδήποτε συνδυασμό OR/AND σχέσεων.

Σημειώνεται ότι, οι OR/AND σχέσεις μεταξύ των αντικειμένων των συνόλων C και O διακρίνονται εννοιολογικά από τις αντίστοιχες που αφορούν τα σύνολα DT, Pu και R καθώς προορίζονται αυστηρά για τη σύνθεση νοημάτων και όχι για την κληρονομική συσχέτιση μεταφοράς κανόνων. Επιπρόσθετα, είναι δυνατός ο προσδιορισμός «αρνητικών συνθηκών» υπό την έννοια της μη ισχύος μια συνθήκης. Έτσι, είναι δυνατή η ακόλουθη έκφραση: $c_k = (c_{k1} \wedge \neg c_{k2})$.

Μια χρονική συνθήκη που συνδέεται με θετική εξουσιοδότηση για πρόσβαση σε δεδομένα καθ' όλη τη διάρκεια της *εβδομάδας* με εξαίρεση τις *Παρασκευές*, μπορεί να προδιαγραφεί ως *Χρονική Συνθήκη(Εβδομάδα)* $\wedge \neg$ *Χρονική Συνθήκη(Παρασκευή)*.

Παράδειγμα 2: Σύνθεση Συνθηκών

Ταυτόχρονα, οι κανόνες εξουσιοδότησης αποτελώντας τη βάση της παραγωγής των τελικών εξουσιοδοτήσεων καθορίζονται μέσω συνδυασμών στιγμιότυπων δεδομένων, σκοπών πρόσβασης και ρόλων ($dt_i \in DT$, $pu_j \in Pu$, $r_k \in R$). Επομένως, τα αντίστοιχα σύνολα και δύο επιπρόσθετοι παράμετροι, αυτοί των συνθηκών και των υποχρεώσεων, συναποτελούν το πεδίο ορισμού των κανόνων: $domRu = DT^n \times Pu^m \times R^k \times C \times O$. Ο συγκεκριμένος ορισμός επιτρέπει στους κανόνες πρόσβασης να συσχετίζονται με πλειάδα τύπων δεδομένων, σκοπών και ρόλων γεγονός που οδηγεί σε οικονομία προδιαγραφής κανόνων (και επομένως καλύτερη κλιμακοθετησιμότητα). Οι κανόνες μπορεί να είναι θετικοί ή αρνητικοί, κατά βάση αφορούν δικαιώματα ανάγνωσης, επεξεργασίας, και προώθησης δεδομένων καθώς και μεταφορά εξουσιοδοτήσεων, ενώ με χρήση κατηγορημάτων ορίζονται ως εξής:

- readAccessPermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απόδοση** δικαιωμάτων **ανάγνωσης** δεδομένων
- writeAccessPermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απόδοση** δικαιωμάτων **επεξεργασίας** δεδομένων
- readAccessProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις ανάγνωσης** δεδομένων

- writeAccessProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις επεξεργασίας** δεδομένων
- readForwardPermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **αδειοδοτήσεις προώθησης** δεδομένων με δικαιώματα **ανάγνωσης**
- writeForwardPermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **αδειοδοτήσεις προώθησης** δεδομένων με δικαιώματα **επεξεργασίας**
- readForwardProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις προώθησης** δεδομένων με δικαιώματα **ανάγνωσης**
- writeForwardProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις προώθησης** δεδομένων με δικαιώματα **επεξεργασίας**
- readDelegatePermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **αδειοδοτήσεις μεταφοράς δικαιωμάτων ανάγνωσης** δεδομένων
- writeDelegatePermission(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **αδειοδοτήσεις μεταφοράς δικαιωμάτων επεξεργασίας** δεδομένων
- readDelegateProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις μεταφοράς δικαιωμάτων ανάγνωσης** δεδομένων
- writeDelegateProhibition(⟨DT⟩, ⟨Pu⟩, ⟨R⟩, C, O), αναπαριστώντας **απαγορεύσεις μεταφοράς δικαιωμάτων επεξεργασίας** δεδομένων

Επιπρόσθετα, στους χρήστες του συστήματος αποδίδονται συγκεκριμένοι ρόλοι, μια διαδικασία η οποία παράγει το σύνολο Απόδοσης Ρόλων (Role Assignments – RA), με $RA \subseteq U \times R$, σε μια σχέση «πολλών προς πολλά» (many-to-many). Ακόμα, οι σκοποί πρόσβασης αποδίδονται σε ρόλους, υπό την έννοια ότι πρακτικά μόνο συγκεκριμένοι ρόλοι μπορούν να ενεργοποιούνται στο πλαίσιο ικανοποίησης εξειδικευμένων στόχων πρόσβασης. Επομένως δημιουργείται το σύνολο Σκοπών-Ρόλων (Purpose-Role – PR), όπου $PR \subseteq P \times R$, με τη δημιουργηθείσα σύνδεση να ακολουθεί ομοίως τη λογική «πολλών προς πολλά». Το τελικό βήμα για την προδιαγραφή κανόνων εξουσιοδότησης συνίσταται στη σύνδεση των τύπων δεδομένων υπό προστασία με συγκεκριμένους σκοπούς πρόσβασης και ρόλους, αντικείμενα δηλαδή του συνόλου PR. Προς τούτο, εισάγεται η έννοια των Επιτρεπτών Τύπων Δεδομένων, η οποία αναπαριστά θετικές εξουσιοδοτήσεις για πρόσβαση σε δεδομένα:

- Μια πλειάδα $\langle dt_1, dt_2, \ldots, dt_m \rangle$ χαρακτηρίζεται ως *επιτρεπτή* για ένα συνδυασμό σκοπού-ρόλου pr_{zy}, όταν όλοι οι εμπλεκόμενοι τύποι δεδομένων θεωρούνται

απαραίτητοι σε κάποιον χρήστη u_x που του έχει αποδοθεί ο ρόλος r_y, έτσι ώστε να εκπληρώσει το σκοπό πρόσβασης pu_z, όπου $pr_{zy} = \langle pu_z, r_y \rangle$. Προδιαγράφεται έτσι το σύνολο των Επιτρεπτών Τύπων Δεδομένων (Permitted Data Types – PDT), με $PDT \subseteq DT^n \times PR$, σε μια σχέση «πολλών με πολλά».

4.3.3 Παραγωγή Συμπερασμάτων

Τα παραπάνω σύνολα του μοντέλου πληροφοριών και οι μεταξύ τους συσχετίσεις προκαλούν γενικεύσεις (generalizations) και εξειδικεύσεις (specializations) ενώ σχηματίζουν σύνθετα εννοιολογικά σύνολα με απώτερο στόχο την προδιαγραφή κανόνων εξουσιοδότησης.

Η έννοια *Administrator* αποτελεί εξειδίκευση της έννοιας *Υπάλληλος*, ενώ η έννοια *Υπάλληλος* αποτελεί γενίκευση της έννοιας *Administrator*.

Παράδειγμα 3: Γενίκευση/εξειδίκευση νοημάτων

Στη βάση ενός πεπερασμένου συνόλου γενικεύσεων, εξειδικεύσεων και συνθέσεων, η ενσωμάτωση κανόνων προϋπόθεσης-αποτελέσματος (κανόνων συλλογιστικής) οδηγεί στην αυτόματη εξαγωγή επιπλέον εννοιολογικών δηλώσεων και επιπρόσθετης γνώσης. Η διαδικασία της εξαγωγής συμπερασμάτων από μια υπάρχουσα βάση υποθέσεων, που στη βιβλιογραφία αναφέρεται ως **συλλογιστική** (reasoning) ή **συμπερασμός** (inference), αποτελεί τον πυρήνα της μηχανής εξαγωγής αποφάσεων της προτεινόμενης λύσης. Οι κανόνες συμπερασμού που σχηματίζουν τη συνολική υιοθετούμενη στρατηγική συλλογιστικής εφαρμόζονται ως εξής: οποτεδήποτε οι προϋποθέσεις του κανόνα ικανοποιούνται από μια δήλωση, αυτόματα συνεπάγεται η δήλωση συμπέρασμα. Οι βασικοί κανόνες συλλογιστικής απορρέουν από την απαίτηση παραγωγής συμπερασμάτων στη βάση των διαμορφωθέντων κανόνων εξουσιοδότησης κι επομένως αφορούν επέκταση της αρχικής γνωσιακής βάσης θετικών και αρνητικών εξουσιοδοτήσεων για πρόσβαση, περαιτέρω προώθηση και μεταφορά δικαιωμάτων. Οι κανόνες συμπερασμού, διαφοροποιούνται ανάλογα με το υποκείμενο θετικό ή αρνητικό πλαίσιο συμφραζόμενων και μέσω κατηγορημάτων λογικής πρώτου βαθμού (first order logic), ορίζονται ως εξής:

$\forall (dt_i, dt_j, pu_n, r_k, c_l, o_m)$,

- readAccessPermission(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readAccessPermission(dt_i, pu_n, r_k, c_l, o_m)
- readAccessProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readAccessProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readAccessPermission(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf (dt_j, dt_i) ⟹ readAccessPermission(dt_i, pu_n, r_k, c_l, o_m)
- readAccessProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readAccessProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readAccessProhibition(dt_i, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readAccessProhibition(dt_j, pu_n, r_k, c_l, o_m)
- readForwardPermission(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readForwardPermission(dt_i, pu_n, r_k, c_l, o_m)
- readForwardProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readForwardProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readForwardPermission(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readForwardPermission(dt_i, pu_n, r_k, c_l, o_m)
- readForwardProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readForwardProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readForwardProhibition(dt_i, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readForwardProhibition(dt_j, pu_n, r_k, c_l, o_m)
- readDelegatePermission(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readDelegatePermission(dt_i, pu_n, r_k, c_l, o_m)
- readDelegateProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ inheritsFrom(dt_j, dt_i) ⟹ readDelegateProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readDelegatePermission(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readDelegatePermission(dt_i, pu_n, r_k, c_l, o_m)
- readDelegateProhibition(dt_j, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readDelegateProhibition(dt_i, pu_n, r_k, c_l, o_m)
- readDelegateProhibition(dt_i, pu_n, r_k, c_l, o_m) ∧ isPartOf(dt_j, dt_i) ⟹ readDelegateProhibition(dt_j, pu_n, r_k, c_l, o_m)

Σημειώνεται ότι, τα κατηγορήματα inheritsFrom(dt_j, dt_i) και isPartOf(dt_j, dt_i) αναπαριστούν τις σχέσεις $dt_i \blacktriangleleft dt_j$ και $dt_i \angle dt_j$ αντίστοιχα, ενώ για την αποφυγή επανάληψης περιεχομένου παραλήφθηκαν οι κανόνες για την περίπτωση των

δικαιωμάτων επεξεργασίας (write) δεδομένων, οι οποίοι ακολουθούν ακριβώς την ίδια λογική παραγωγής συμπερασμάτων με τους κανόνες ανάγνωσης (read). Επιπλέον, ίδια είναι και η πρακτική συλλογιστικής σε ότι αφορά τις ιεραρχικές σχέσεις μεταξύ των αντικειμένων των συνόλων Pu και R.

Συμπληρωματικοί συμπερασματικοί κανόνες προκύπτουν από το γεγονός ότι, όπως προαναφέρθηκε, οι σχέσεις της κληρονομικότητας χαρακτηριστικών και της «εννοιολογικής συμπερίληψης» είναι μεταβατικές και αντί-συμμετρικές. Υπό αυτή τη σκοπιά, ισχύουν τα παρακάτω:

$\forall (dt_i, dt_j, dt_k, pu_i, pu_j, pu_k, r_i, r_j, r_k)$

- $inheritsFrom(dt_j, dt_i) \wedge inheritsFrom(dt_k, dt_j) \Longrightarrow inheritsFrom(dt_k, dt_i)$
- $inheritsFrom(pu_j, pu_i) \wedge inheritsFrom(pu_k, pu_j) \Longrightarrow inheritsFrom(pu_k, pu_i)$
- $inheritsFrom(r_j, r_i) \wedge inheritsFrom(r_k, r_j) \Longrightarrow inheritsFrom(r_k, r_i)$
- $isPartOf (dt_j, dt_i) \wedge isPartOf (dt_k, dt_j) \Longrightarrow isPartOf (dt_k, dt_i)$
- $isPartOf (pu_j, pu_i) \wedge isPartOf (pu_k, pu_j) \Longrightarrow isPartOf (pu_k, pu_i)$
- $isPartOf (r_j, r_i) \wedge isPartOf (r_k, r_j) \Longrightarrow isPartOf (r_k, r_i)$
- $inheritsFrom(dt_j, dt_i) \wedge (dt_j \neq dt_j) \Longrightarrow \neg inheritsFrom(dt_i, dt_j)$
- $inheritsFrom(pu_j, pu_i) \wedge (pu_j \neq pu_j) \Longrightarrow \neg inheritsFrom(pu_i, pu_j)$
- $inheritsFrom(r_j, r_i) \wedge (r_j \neq r_j) \Longrightarrow \neg inheritsFrom(r_i, r_j)$
- $isPartOf (dt_j, dt_i) \wedge (dt_j \neq dt_j) \Longrightarrow \neg isPartOf (dt_i, dt_j)$
- $isPartOf (pu_j, pu_i) \wedge (pu_j \neq pu_j) \Longrightarrow \neg isPartOf (pu_i, pu_j)$
- $isPartOf (r_j, r_i) \wedge (r_j \neq r_j) \Longrightarrow \neg isPartOf (r_i, r_j)$

Τέλος, εξάγονται προφανώς και οι παρακάτω κανόνες συλλογιστικής:

$\forall (dt_i, pu_j, r_k, c_l, o_m)$,

- $readAccessPermission(dt_i, pu_j, r_k, c_l, o_m) \Longrightarrow \neg readAccessProhibition(dt_i, pu_j, r_k, c_l, o_m)$
- $writeAccessPermission(dt_i, pu_j, r_k, c_l, o_m) \Longrightarrow \neg writeAccessProhibition(dt_i, pu_j, r_k, c_l, o_m)$
- $readForwardPermission(dt_i, pu_j, r_k, c_l, o_m) \Longrightarrow \neg readForwardProhibition(dt_i, pu_j, r_k, c_l, o_m)$
- $writeForwardPermission(dt_i, pu_j, r_k, c_l, o_m) \Longrightarrow \neg writeForwardProhibition(dt_i, pu_j, r_k, c_l, o_m)$

- readDelegatePermission(dt_i, pu_j, r_k, c_l, o_m) $\Longrightarrow \neg$ readDelegateProhibition(dt_i, pu_j, r_k, c_l, o_m)
- writeDelegatePermission(dt_i, pu_j, r_k, c_l, o_m) $\Longrightarrow \neg$ writeDelegateProhibition(dt_i, pu_j, r_k, c_l, o_m)

Έστω κανόνας που αποδίδει δικαιώματα ανάγνωσης στον τύπο δεδομένων *Πληροφορίες Στελεχών Ομάδας Έργου* στους υπαλλήλους του *Τμήματος Διαχείρισης Προσωπικού* προς ικανοποίηση του στόχου *Επικύρωση Ανθρωποωρών* σε ένα οργανισμό κατά το χρονικό διάστημα 8:00ΠΜ - 17:00ΜΜ. Ο κανόνας ορίζεται ως: readAccessPermission(*Πληροφορίες Στελεχών Ομάδας Έργου, Επικύρωση Ανθρωποωρών, Τμήμα Διαχείρισης Προσωπικού, Χρονική Συνθήκη(Περίοδος(8:00ΠΜ - 17:00ΜΜ))*. Αναγνωρίζοντας ως δεδομένη τη σχέση: *Λίστα Ονομάτων Στελεχών Ομάδας Έργου* ◄ *Πληροφορίες Στελεχών Ομάδας Έργου*, αυτόματα εξάγεται ο κανόνας: readAccessPermission(*Λίστα Ονομάτων Στελεχών Ομάδας Έργου, Επικύρωση Ανθρωποωρών, Τμήμα Διαχείρισης Προσωπικού, Χρονική Συνθήκη(Περίοδος(8:00ΠΜ - 17:00ΜΜ))*.

Παράδειγμα 4: Συλλογιστική διαδικασία

4.4 Εξαγωγή Αποφάσεων

Τελικός στόχος της μηχανής εξαγωγής αποφάσεων που βρίσκεται στον πυρήνα των διαδικασιών της προτεινόμενης πλατφόρμας αποτελεί η έγχυση ποιοτικών χαρακτηριστικών ιδιωτικότητας στις υπερκείμενες υπηρεσίες υπολογισμού εξουσιοδοτήσεων. Υπό αυτή την έννοια, η πλατφόρμα διαχείρισης εξουσιοδοτήσεων αξιοποιεί κανόνες ελέγχου πρόσβασης, μεταφοράς δικαιωμάτων και προώθησης δεδομένων, σύμφωνα με το μοντέλο πληροφοριών που αναλύθηκε στις προηγούμενες ενότητες και προδιαγράφηκε με τρόπο που να ικανοποιεί τις εξαχθείσες απαιτήσεις ιδιωτικότητας. Προς την ίδια κατεύθυνση, οι διαδικασίες εξαγωγής αποφάσεων βασίζονται στη δημιουργία ενός ολοκληρωμένου και σαφούς «πλαισίου ιδιωτικότητας» (privacy context) το οποίο καθορίζει και οριοθετεί την παραγωγή εξουσιοδοτήσεων. Το πλαίσιο ιδιωτικότητας περιλαμβάνει το σύνολο των παραμέτρων εκείνων, των οποίων τα ποιοτικά και ποσοτικά χαρακτηριστικά επηρεάζουν άμεσα ή έμμεσα τη λήψη αποφάσεων με επίγνωση της ιδιωτικότητας των χρηστών. Πιο συγκεκριμένα, στα πλαίσια της διατριβής τα θεμελιώδη συστατικά του πλαισίου ιδιωτικότητας συναπαρτίζουν: i) οι δηλωθέντες κανόνες και προτιμήσεις των **χρηστών** του συστήματος, ii) των **οργανισμών-παρόχων** της Συνομοσπονδίας και iii) του **Επικεφαλής** της Συνομοσπονδίας καθώς και iv) οι τρέχουσες τιμές

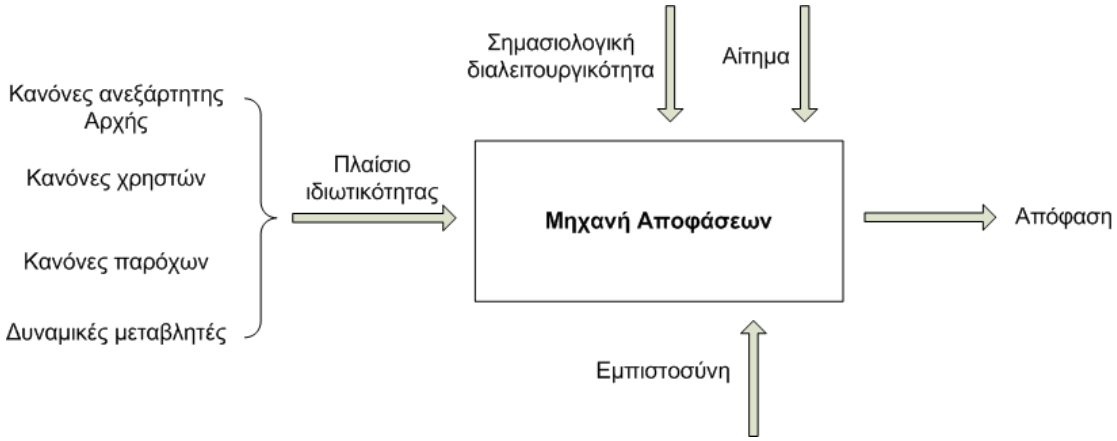
δυναμικών, χωρικών, χρονικών και σχετικών με την υποκείμενη υποδομή **μεταβλητών**. Υπενθυμίζεται εδώ ότι ο Επικεφαλής της Συνομοσπονδίας μπορεί να αναπαριστά μια οντότητα ελέγχου της Συνομοσπονδίας με στόχο τον ορισμό κοινά αποδεκτών κανόνων, ρόλο που μπορεί να διαδραματίσει κάποιος ανεξάρτητος ελεγκτικός φορέας κοινής εμπιστοσύνης.

Το γεγονός ότι οι πολλαπλές απομακρυσμένοι οντότητες της κατανεμημένης αρχιτεκτονικής παράγουν παράλληλα εννοιολογικές δηλώσεις και κανόνες εξουσιοδότησης, αποδίδει ιδιαίτερη αξία στην ορθή αναγνώριση και επικύρωση της **εμπιστοσύνης** μεταξύ των οντοτήτων. Ακόμα, πιθανή σημασιολογική ετερογένεια μεταξύ των διαφόρων πηγών πληροφοριών του πλαισίου ιδιωτικότητας συνιστά κίνδυνο για την απρόσκοπτη λειτουργία του συστήματος. Συμπερασματικά, προς εξασφάλιση της κατηγορηματικότητας των αποφάσεών της, η μηχανή λήψης αποφάσεων σχεδιάστηκε έτσι ώστε να λειτουργεί στη βάση σημασιολογικά ομογενών δεδομένων που προέρχονται από πηγές των οποίων την εγκυρότητα εμπιστεύεται. Οι παραπάνω παράγοντες αποτελούν το σύνολο των παραμέτρων εισόδου της μηχανής εξαγωγής αποφάσεων, η λειτουργία της οποίας καταλήγει στην παραγωγή θετικών ή αρνητικών εισηγήσεων εξουσιοδότησης (Εικόνα 11).

Η ετερογένεια των πηγών δημιουργίας του συνολικού πλαισίου ιδιωτικότητας μπορεί να αφορά, εκτός από σημασιολογικά δεδομένα και ζητήματα εμπιστοσύνης, διαφορές στις προτιμήσεις των απομακρυσμένων οντοτήτων της αρχιτεκτονικής. Σε πολύπλοκες αλυσίδες παροχής υπηρεσιών, όπου εμπλέκονται οντότητες που ικανοποιούν διαφορετικούς στόχους συνεργασίας και διατηρούν διαφορετικά ατομικά κριτήρια προστασίας πόρων, είναι δυνατόν να προκύψουν για τον ίδιο τύπο ευαίσθητων δεδομένων αντικρουόμενες πολιτικές διαχείρισης. Αυτόματα, η διαχείριση αυτού του τύπου της ετερογένειας μέσω του σχεδιασμού και της ενεργοποίησης μιας ολοκληρωμένης στρατηγικής επίλυσης «συγκρουόμενων» κανόνων εξουσιοδότησης αποτελεί απαραίτητο συστατικό της μηχανής παραγωγής αποφάσεων.

Σε συμφωνία με τις λειτουργικές απαιτήσεις της πλατφόρμας, η ενσωματωμένη μηχανή ελέγχου εξουσιοδοτήσεων με επίγνωση ιδιωτικότητας αποδίδει σχετική προτεραιότητα στις προτιμήσεις ιδιωτικότητας των υποκείμενων των δεδομένων υπό προστασία σε σχέση με τις στρατηγικές προστασίας των λοιπών ενδιαφερόμενων. Στη συνέχεια, η μηχανή αποδίδει απόλυτη προτεραιότητα στις διατάξεις, αν υπάρχουν τέτοιες, του Επικεφαλής της Συνομοσπονδίας Ιδιωτικότητας. Παράλληλα,

το σύστημα είναι σε θέση να αναγνωρίζει τις περιπτώσεις εκείνες, όπου οι διακριτές οντότητες είναι πρόθυμες να δεχτούν συμβιβασμούς στις προτιμήσεις τους προκειμένου να ολοκληρωθεί επιτυχώς η διαδικασία (*break the glass* κανόνες [106]). Τέλος, το προτεινόμενο σύστημα ακολουθεί την Υπόθεση Κλειστού Κόσμου (Closed World Assumption – CWA) σε ότι αφορά την εφαρμογή των κατάλληλων κανόνων εξουσιοδότησης, σύμφωνα με την οποία πιθανή αδυναμία απόδειξης της ορθότητας μιας δήλωσης συνεπάγεται αυτόματα ότι η εν λόγω δήλωση είναι ψευδής. Έτσι, η απουσία κατάλληλων κανόνων που να εφαρμόζονται σε συγκεκριμένα αιτήματα χρηστών κατά τη λειτουργία του συστήματος ισοδυναμεί με την ύπαρξη αρνητικής εξουσιοδότησης. Η επιλογή αυτή πραγματοποιήθηκε με στόχο την ελαχιστοποίηση του αριθμού των περιπτώσεων διφορούμενων καταστάσεων όπου η παραγωγή σαφών αποφάσεων εξουσιοδότησης γίνεται αμφίβολη. Διακριτά, τα βήματα παραγωγής αποφάσεων εξουσιοδότησης από την αρμόδια μονάδα του συστήματος απεικονίζονται στην Εικόνα 13.



Εικόνα 11: Μηχανή αποφάσεων εξουσιοδοτήσεων με επίγνωση της ιδιωτικότητας

Με στόχο τη μοντελοποίηση του προβλήματος λήψης απόφασης εξουσιοδοτήσεων αξιοποιούνται τα ακόλουθα κατηγορήματα:

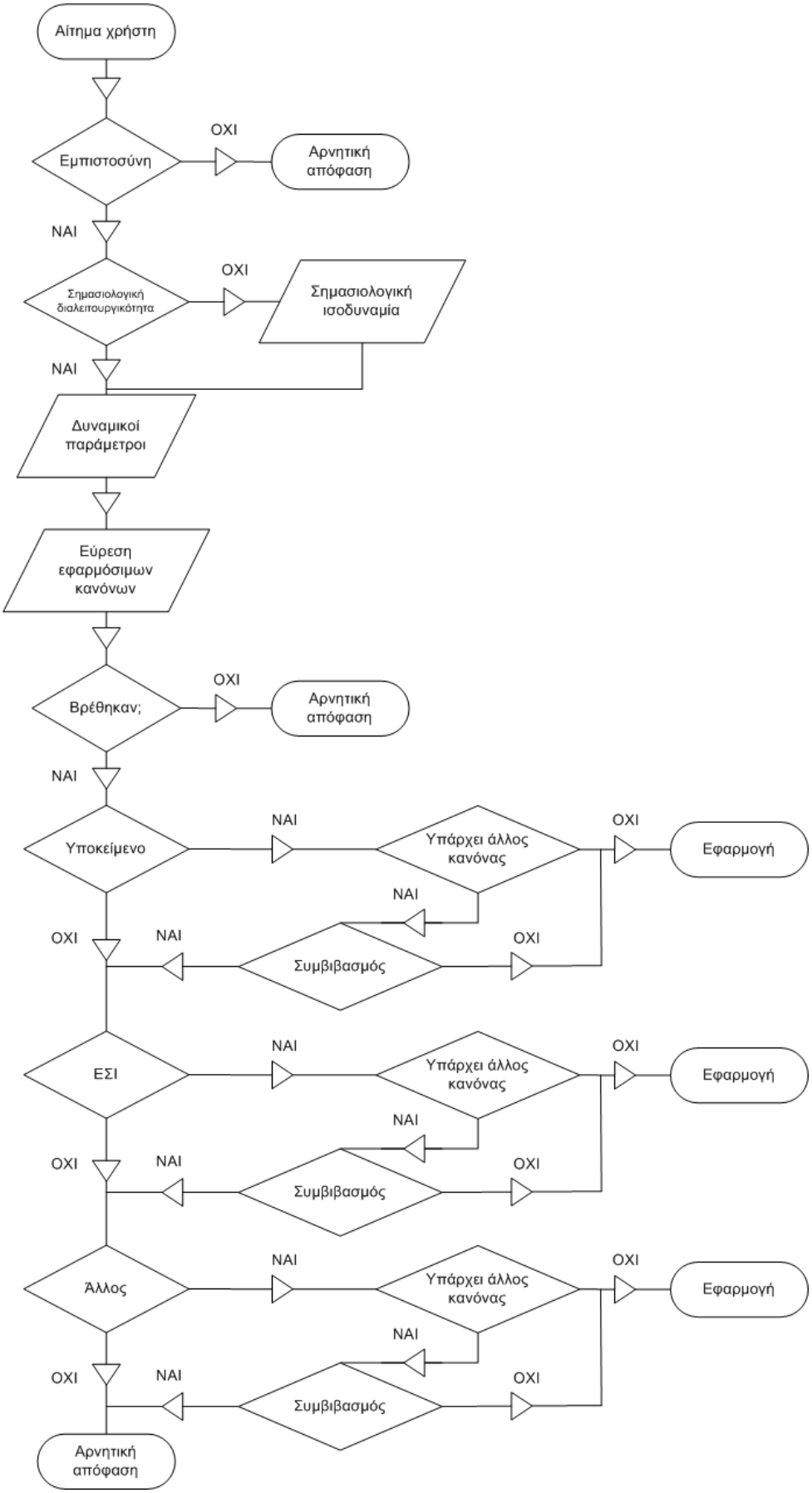
- actorSaysFact(A, F), όπου το στέλεχος A είναι μια οντότητα της αρχιτεκτονικής (Επικεφαλής, πάροχος, ή χρήστης) και το μέλος F ορίζει μια εννοιολογική δήλωση στη βάση του μοντέλου πληροφοριών της πλατφόρμας. Είθισται οι δηλώσεις να αφορούν αντικείμενα των συνόλων RA, PR και PDT. Ουσιαστικά το κατηγόρημα αναπαριστά τους προσωπικούς ισχυρισμούς των οντοτήτων στο πλαίσιο της λειτουργίας της πλατφόρμας.

- actorTrustsActor(A, B), όπου τα μέλη A και B αναπαριστούν οντότητες της αρχιτεκτονικής. Το κατηγόρημα υποδηλώνει την τοποθέτηση εμπιστοσύνης της οντότητας A στην οντότητα B σε ότι αφορά την εγκυρότητα των ισχυρισμών που παράγει η τελευταία.
- actorUnderstandsActor(A, B, F), όπου τα μέλη A και B αναπαριστούν οντότητες της αρχιτεκτονικής. Η σχέση ορίζει την ύπαρξη σημασιολογικής διαλειτουργικότητας μεταξύ των A και B σε ότι αφορά τη δήλωση F.

Συνολικά, η παράγωγη θετικής εξουσιοδότησης, ανεξαρτήτως ειδικότερης στόχευσης (πρόσβαση σε δεδομένα, προώθηση δεδομένων, μεταφορά δικαιωμάτων) ενός χρήστη u_i, που αξιοποιεί τον οργανισμό A ως πάροχο ταυτοτήτων, ενεργοποιεί τον ρόλο r_l και αιτείται εξουσιοδότησης για τον τύπο δεδομένων dt_k που παρέχεται από τον πάροχο υπηρεσιών B στο πλαίσιο ικανοποίησης του σκοπού pu_m, ισοδυναμεί με τη σύνθεση των κατηγορημάτων, όπως παρουσιάζεται στην Εικόνα 12.

$(\exists\ pu_m, r_l, dt_k)$
$(actorSaysFact(A, ur_{il}) \wedge actorTrustsActor(B, A) \wedge actorUnderstandsActor(B, A, r_l) \wedge actorSaysFact(B, pdt_{mlk}))$
όπου $ur_{il} = \langle u_i, r_l \rangle$ και $pdt_{mlk} = \langle pu_m, r_l, dt_k \rangle$

Εικόνα 12: Παράγωγη θετικής εξουσιοδότησης



Εικόνα 13: Πορεία παραγωγής απόφασης εξουσιοδότησης

5 Ανάπτυξη Βασικών Δομικών Στοιχείων

Το προηγούμενο κεφάλαιο παρουσίασε τις βασικές αρχές της προτεινόμενης πλατφόρμας ενώ παρουσίασε τη φορμαλιστική θεμελίωση του προβλήματος διαχείρισης εξουσιοδοτήσεων σε κατανεμημένα περιβάλλοντα. Στόχος του παρόντος κεφαλαίου είναι η συγκεκριμενοποίηση των τεχνολογικών μέσων και ενεργειών που πραγματοποιήθηκαν στο πλαίσιο της εκπόνησης της διατριβής για την ανάπτυξη των βασικών δομικών συστατικών του συστήματος. Έτσι, παρουσιάζονται κατά σειρά το σημασιολογικό μοντέλο που υλοποιήθηκε στη βάση του σχεδιαζόμενου μοντέλου πληροφοριών, η υλοποίηση του αλγορίθμου συλλογιστικής για την εξαγωγή συμπερασμάτων εξουσιοδότησης και η αναπαράσταση των βασικών σχέσεων μεταξύ των οντοτήτων με ψηφιακά πιστοποιητικά ταυτοτήτων και ιδιοτήτων.

5.1 Οντολογία Εξουσιοδοτήσεων

Με στόχο την κάλυψη των λειτουργικών απαιτήσεων της πλατφόρμας ο ορισμός κανόνων εξουσιοδότησης πραγματοποιείται στη βάση ενός συνόλου εννοιών που περιλαμβάνει: τον τύπο των δεδομένων, τον σκοπό αίτησης για πρόσβαση/προώθηση, τον ρόλο και τα χαρακτηριστικά του αιτούντα, τις συνθήκες εξουσιοδότησης καθώς και τις επιπλέον ενέργειες προς εκπλήρωση που απορρέουν μιας θετικής εξουσιοδότησης. Για την αναπαράσταση και οργάνωση των εν λόγω θεμελιωδών εννοιών επιλέχθηκε η χρήση οντολογιών και συγγενών τεχνολογιών του σημασιολογικού ιστού. Οι οντολογίες χρησιμοποιούνται ευρέως για τον ορισμό κοινών λεξιλογίων, για την ολιστική αναπαράσταση τομέων γνώσης και την τυποποίηση εννοιών. Μάλιστα, η χρήση οντολογιών προτιμήθηκε σε σχέση με παραδοσιακές τεχνολογίες αναπαράστασης γνώσης όπως η γλώσσα XACML, λόγω των συγκριτικών πλεονεκτημάτων που παρουσιάζει σε μια σειρά από διαφορετικές πτυχές του τομέα με κυριότερα τα εξής: πλούσια εκφραστική χωρητικότητα, δυνατότητα ελέγχου της συνοχής των ορισμένων μοντέλων, ευκολία ολοκλήρωσης με λοιπά σημασιολογικά μοντέλα και δυνατότητες εφαρμογής συλλογιστικών αλγορίθμων. Η οντολογία που αξιοποιήθηκε καλείται για τους σκοπούς της διατριβής Οντολογία Εξουσιοδοτήσεων και υλοποιήθηκε στη γλώσσα Web Ontology Language (OWL) [107] η οποία έχει προτυποποιηθεί από τον οργανισμό W3C [108], ενώ το

συντακτικό της βασίζεται στο διαδεδομένο πρότυπο Resource Description Framework (RDF) [109]. Σημειώνεται ότι, αν και για τις ανάγκες της διατριβής προδιαγράφηκε ένα σχετικά περιορισμένο σύνολο εννοιών, στόχος είναι η Οντολογία Εξουσιοδοτήσεων να αξιοποιείται για την αναπαράσταση εκτεταμένων συνόλων νοημάτων, έτσι ώστε να καλύπτεται και το μεγαλύτερο δυνατό εύρος πραγματικών μελετών περίπτωσης. Χαρακτηριστικά, ως υπόδειγμα επιπέδου ανάλυσης αναφέρονται τα παραδείγματα του κοινού λεξιλογίου για τις δημόσιες συμβάσεις (Common Procurement Vocabulary – CPV) [110] και το Βορειοαμερικανικό σύστημα ταξινόμησης βιομηχανίας (North American Industry Classification System – NAICS) [111] που αξιοποιούνται για την ταξινόμηση διαδικασιών σύναψης δημοσίων συμβάσεων έργων, προμηθειών και υπηρεσιών στην Ευρώπη και για την ταξινόμηση επιχειρήσεων ανάλογα με τον τύπο της σχετικής οικονομικής δραστηριότητας στη Βόρεια Αμερική αντίστοιχα.

5.1.1 Βασικές Κλάσεις

Σε συμφωνία με το αναλυμένο μοντέλο πληροφοριών της πλατφόρμας εξουσιοδοτήσεων η Οντολογία Εξουσιοδοτήσεων περιλαμβάνει τις ακόλουθες κλάσεις:

- *Data*, στιγμιότυπα της οποίας αναπαριστούν τύπους προσωπικών και ευαίσθητων δεδομένων υπό προστασία.
- *Purposes*, τα μέλη της οποίας που αντιστοιχίζονται στους διαφορετικούς πιθανούς στόχους για πρόσβαση σε δεδομένα.
- *Roles*, αντικείμενα της οποίας περιγράφουν τους διαφορετικούς ρόλους που μπορούν να ενεργοποιούν οι χρήστες του συστήματος.
- *Rules*, που ορίζουν τους κανόνες ελέγχου πρόσβασης σε δεδομένα, προώθησης δεδομένων και μεταφοράς δικαιωμάτων πρόσβασης.
- *Conditions*, που προδιαγράφουν περιορισμούς εκτέλεσης κανόνων και εισάγουν επίγνωση πλαισίου στο σύστημα. Οι τύποι των συνθηκών αναπαριστάνονται μέσω στιγμιότυπων της κλάσης *ContextualTypes*.
- *ConditionSubject*, τα μέλη της οποίας που καταδεικνύουν τα υποκείμενα των συνθηκών, δηλαδή καθορίζουν σημασιολογικά την έννοια που αφορά η ισχύς της συνθήκης. Για παράδειγμα και έχοντας ως βάση χωρικούς περιορισμούς, οι κανόνες: i) «Να επιτρέπεται η πρόσβαση σε δεδομένα όταν ο αιτών

καταθέτει το αίτημά του από κάποιο τερματικό εντός των εγκαταστάσεων ενός οργανισμού» και ii) «Να επιτρέπεται η πρόσβαση σε δεδομένα όταν αυτά βρίσκονται αποθηκευμένα σε βάσεις δεδομένων εντός των εγκαταστάσεων ενός οργανισμού», αν και χρησιμοποιούν σημασιολογικά την ίδια χωρική συνθήκη («εντός των εγκαταστάσεων ενός οργανισμού») αναφέρονται σε διαφορετικά υποκείμενα («αιτούντες» και «βάσεις δεδομένων»).

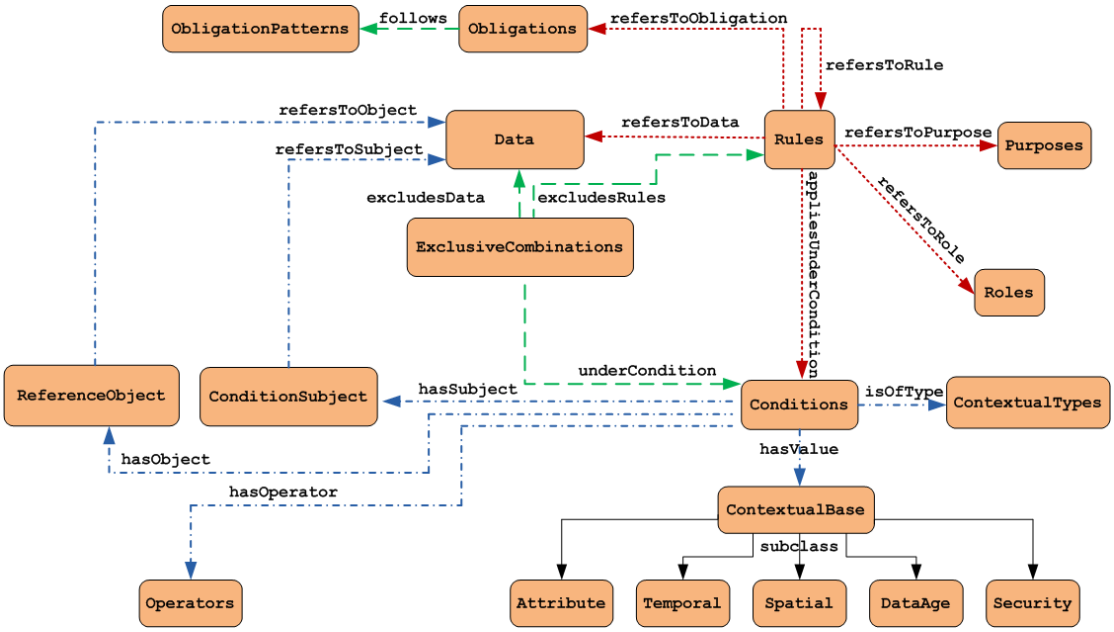
- *ReferenceObject*, που συγκεκριμενοποιεί τους τύπους δεδομένων που επηρεάζονται από την ισχύ της συνθήκης. Για παράδειγμα και σε σχέση με έναν κανόνα που επιτρέπει την πρόσβαση στο σύνολο δεδομένων ⟨*productCode*, *productQuantity*, *productPrice*⟩, μια συνθήκη μπορεί να αποκλείει την πρόσβαση μόνο στον τύπο δεδομένων *productPrice* αν ο αιτών ενεργοποιεί συγκεκριμένο ρόλο.
- *ContextualBase*, κλάση η οποία περιλαμβάνει μια υποκλάση για κάθε αντικείμενο της κλάσης *ContextualTypes* που αναπαριστά συγκεκριμένες ταξινομήσεις για τα στιγμιότυπα συνθήκης ανάλογα με το είδος τους. Ενώ οι παραπάνω υποκλάσεις εμφανίζονται να υποβαθμίζουν τη χρησιμότητα της κλάσης *ContextualTypes*, στην πράξη αποδεικνύεται ότι η άμεση αναγνώριση του σημασιολογικού τύπου της κάθε συνθήκης επιφέρει οφέλη κατά την παραγωγή σύνθετων συνθηκών. Πιο αναλυτικά, προδιαγραφήκαν οι συγκεκριμένες υποκλάσεις συνθηκών:
    - *Temporal*, που περιλαμβάνει αναπαραστάσεις χρονικών στιγμών και διαστημάτων,
    - *Spatial*, που αναφέρεται σε αντικείμενα φυσικών γέω-συντεταγμένων καθώς και σε περιγραφές λογικών τοποθεσιών,
    - *InformationAge*, που περιλαμβάνει λεκτικές περιγραφές της χρονικής διάρκειας αποθήκευσης των δεδομένων σε βάσεις δεδομένων,
    - *Attribute*, παρέχοντας ορισμούς και ταξινομήσεις συνθηκών γνωρισμάτων των χρηστών του συστήματος και ενσωματώνοντας έτσι ένα εξέχον χαρακτηριστικό των μοντέλων ελέγχου πρόσβασης που είναι η επίγνωση των γνωρισμάτων των χρηστών και
    - *Security*, που περιλαμβάνει περιορισμούς εξουσιοδότησης σε άμεση συσχέτιση με τις ποιότητες της υποκείμενης υποδομής και των εμπλεκόμενων διαδικασιών, όπως είναι η ποιότητα ψηφιακών

πιστοποιητικών [112] ή ο τρέχων αριθμός παράλληλων συναλλαγών με το σύστημα.

- *ExclusiveCombinations*, που περιγράφει πως ομάδες τύπων δεδομένων μπορούν να «αλληλό-αποκλείονται» και να επηρεάζουν αρνητικά πιθανές εξουσιοδοτήσεις για πρόσβαση σε αλληλοεξαρτώμενους τύπους δεδομένων. Σημειώνεται ότι, η κλάση είναι δυνατόν να περιλαμβάνει και ομάδες «αλληλό-αποκλειόμενων» κανόνων εξουσιοδότησης, για την κάλυψη απαιτήσεων διαχωρισμού καθηκόντων. Με στόχο τη δυναμική προδιαγραφή «αλληλό-αποκλειόμενων» στιγμιότυπων η κλάση συσχετίζεται με την κλάση των συνθηκών. Ως παράδειγμα στατικού διαχωρισμού καθηκόντων μπορεί να λογιστεί η ακόλουθη περίπτωση: Όταν οι κανόνες i) «Να επιτρέπεται η πρόσβαση σε αρχεία τύπου *RequestsForQuotations* σε υπαλλήλους του *FinancialDepartment* (οικονομικό τμήμα) ενός οργανισμού κατά τη διάρκεια υπερωριών» και ii) «Να επιτρέπεται η πρόσβαση σε αρχεία τύπου *RequestsForQuotations* σε υπαλλήλους του *CommercialDepartment* (εμπορικό τμήμα) ενός οργανισμού κατά τη διάρκεια υπερωριών», συσχετίζονται μέσω της κλάσης *ExclusiveCombinations* ουσιαστικά αποκλείεται η ταυτόχρονη πρόσβαση στον συγκεκριμένο τύπο δεδομένων από υπαλλήλους των δύο τμημάτων κατά τη διάρκεια υπερωριών.
- *Operators*, που περιγράφει ένα σύνολο βασικών μαθηματικών κατηγορημάτων για την αναπαράσταση σχέσεων όπως είναι η ισότητα (*equalTo*) και η «ποιοτικοποίηση ποσοτήτων» (*greaterThan, lesserThan, atLeastOne, isAnonymized* κ.ο.κ.). Τα στιγμιότυπα της κλάσης επιτρέπουν αφενός σαφώς μεγαλύτερη ευελιξία κατά την περιγραφή συνθηκών, καθώς και κανόνων πρόσβασης, αφετέρου διευκολύνουν τον περαιτέρω περιορισμό των δεδομένων υπό αποκάλυψη.
- *Obligations*, που καταγράφει τις συμπληρωματικές ενέργειες που επιβάλλεται να διεξαχθούν παράλληλα με την εφαρμογή ενός κανόνα εξουσιοδότησης.
- *ObligationPatterns*, που περιλαμβάνει στιγμιότυπα τα οποία αναπαριστούν θεμελιώδη χαρακτηριστικά των υποχρεώσεων-αντικείμενα της κλάσης *Obligations*. Ενδεικτικά, κάθε υποχρέωση δύναται να ανήκει σε ένα από δύο γενικά πλαίσια υποχρεώσεων: προ-δραστικές (pro-active) και μετά-δραστικές (post-active) υποχρεώσεις, με τις πρώτες να αντιστοιχούν σε δραστηριότητες

που πρέπει να διεξαχθούν προτού αποδοθούν δικαιώματα πρόσβασης και τις δεύτερες να αφορούν διαδικασίες που ενεργοποιούνται μετά την εφαρμογή κάποιου κανόνα εξουσιοδότησης.

Μια πλήρης απεικόνιση της Οντολογίας Εξουσιοδοτήσεων σε επίπεδο κλάσεων παρουσιάζεται στην Εικόνα 14.



Εικόνα 14: Σχήμα Οντολογίας Εξουσιοδοτήσεων σε επίπεδο κλάσεων

5.1.2 Συμπληρωματικά Στοιχεία

Εμφανώς, η χρησιμότητα κάθε στοιχείου της Οντολογίας Εξουσιοδοτήσεων αναδεικνύεται μέσω των στιγμιότυπων της κλάσης *Rules*, καθώς τα τελευταία εργάζονται προς τη συσχέτιση και ενσωμάτωση των αντικειμένων των λοιπών κλάσεων σε δηλώσεις εξουσιοδότησης. Σε αυτή τη διαδικασία οι σχέσεις μεταξύ των κλάσεων της οντολογίας, που ορίζονται ως OWL αντικειμενικές ιδιότητες (OWL object properties), διαδραματίζουν καταλυτικό ρόλο. Σε δεύτερο επίπεδο, ένα σύνολο από σημαντικά χαρακτηριστικά αποδίδονται σε κάθε στιγμιότυπο κανόνα μέσω της δήλωσης συγκεκριμένων OWL ιδιοτήτων επισημείωσης (OWL annotation properties), όπως οι παρακάτω:

- *disclosureOfData*: Ορίζει αν η πληροφορία του συγκεκριμένου τύπου πρέπει να αποκαλυφθεί στο πλαίσιο των όσων ορίζει ο κανόνας. Ουσιαστικά, η συγκεκριμένη ιδιότητα καθορίζει το αν η παραγόμενη εξουσιοδότηση είναι

θετική ή αρνητική και επομένως συνιστά τον πλέον σημαντικό από τους τύπους ιδιοτήτων επισημείωσης κανόνων που αξιοποιήθηκαν.

- *modificationPermission*: Προδιαγράφει αν θα αποδοθούν στον αιτούντα που διατηρεί συγκεκριμένα χαρακτηριστικά, δικαιώματα επεξεργασίας των δεδομένων του συγκεκριμένου τύπου.
- *creatorConsent*: Επιτρέπει στην οντότητα-δημιουργό του κανόνα να απαιτήσει σε πραγματικό χρόνο να ερωτηθεί σχετικά με τη συγκατάθεσή του για πρόσβαση στα δεδομένα του συγκεκριμένου τύπου.
- *overrideConflictingPreferences*: Επιτρέπει στην οντότητα-δημιουργό του κανόνα να ορίσει αν είναι διατεθειμένος να αποδεχτεί τις προτιμήσεις κάποιας άλλης οντότητας που έχει προδιαγράψει συγγενή κανόνα εξουσιοδότησης προκειμένου να δοθεί λύση σε περίπτωση αντικρουόμενων πολιτικών.
- *refersToOutgoingRequest*: Καθορίζει αν ο προδιαγραφόμενος κανόνας εξουσιοδότησης αφορά εξερχόμενο αίτημα χρήστη ή εισερχόμενο αίτημα για πρόσβαση σε δεδομένα. Στην πρώτη περίπτωση ο κανόνας συνιστά ουσιαστικά εξουσιοδότηση για να προχωρήσει ο χρήστης με το αίτημα στην πλευρά του παρόχου υπηρεσίας, ενώ στη δεύτερη αποτελεί εξουσιοδότηση για πρόσβαση σε δεδομένα.
- *isDelegation*: Προσδιορίζει αν ο κανόνας εξουσιοδότησης αφορά μεταφορά δικαιωμάτων. Σε τέτοια περίπτωση το σώμα του κανόνα περιγράφει τις συνθήκες μεταφοράς των δικαιωμάτων ενώ τα δικαιώματα αυτά κάθε αυτά υποδεικνύονται από άλλο συσχετιζόμενο κανόνα ελέγχου πρόσβασης σε δεδομένα.
- *isForward*: Προσδιορίζει αν ο κανόνας εξουσιοδότησης αφορά περαιτέρω προώθηση δεδομένων. Σε τέτοια περίπτωση το σώμα του κανόνα περιγράφει τις συνθήκες προώθησης των δεδομένων ενώ οι λεπτομέρειες της αρχικής απόδοσης δικαιωμάτων πρόσβασης υποδεικνύονται από άλλο συσχετιζόμενο κανόνα ελέγχου πρόσβασης.

Συνολικά, οι OWL ιδιότητες, αντικειμενικές και επισημείωσης, που αξιοποιήθηκαν για τη σύνθεση νοημάτων στην Οντολογία Εξουσιοδοτήσεων απαριθμούνται στον Πίνακας 2. Όπως προκύπτει και από τα παραπάνω, οι κανόνες μεταφοράς δικαιωμάτων και προώθησης δεδομένων νοούνται και ορίζονται αποκλειστικά **στο πλαίσιο υπαρχόντων θετικών εξουσιοδοτήσεων για πρόσβαση σε δεδομένα**. Προς

τούτο, αξιοποιείται η αυτό-αναφορική OWL ιδιότητα *refersToRule* που συσχετίζει τους κανόνες μεταφοράς δικαιωμάτων και προώθησης δεδομένων με συγκεκριμένους κανόνες εξουσιοδότησης που αποτελούν και το αντικείμενο των ενεργειών μεταφοράς δικαιωμάτων και προώθησης δεδομένων. Επίσης, οι ιδιότητες μετά-δεδομένων *appliesToDataDescendants*, *appliesToServiceDescendants* και *appliesToRoleDescendants* αναφέρονται σε Boolean μεταβλητές, η τιμή των οποίων καθορίζει την κληρονομικότητα των κανόνων εξουσιοδότησης σε στιγμιότυπα των κλάσεων *Data*, *Purposes* και *Roles*, πέραν των άμεσα επηρεαζόμενων από τις ιδιότητες των κανόνων *refersToData*, *refersToPurpose* και *refersToRole* αντίστοιχα.

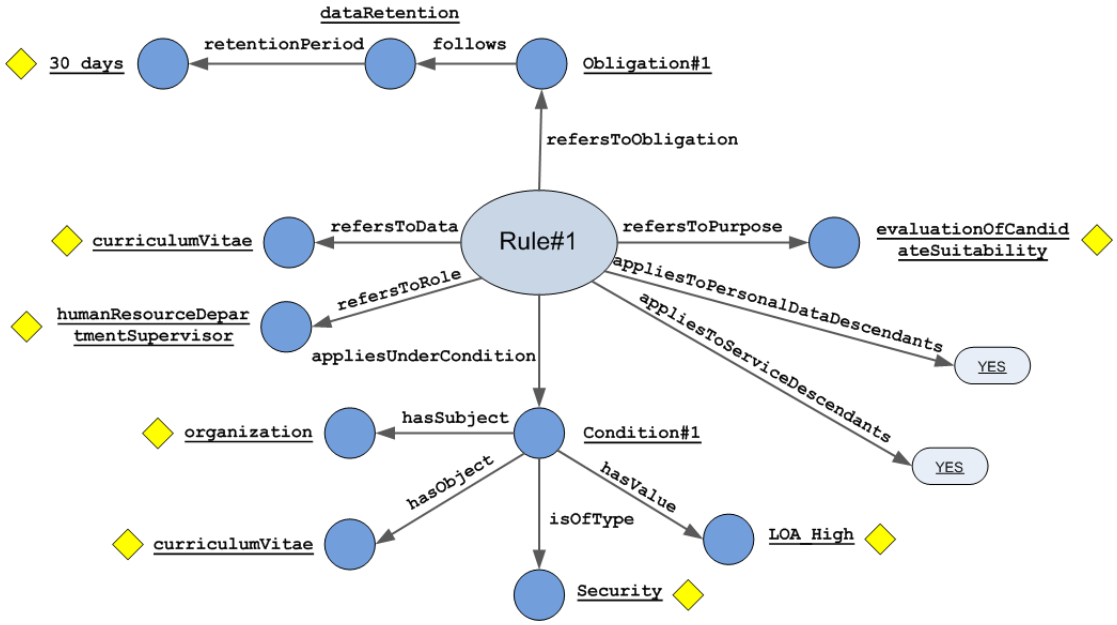
Ιδιότητα	Πεδίο Ορισμού	Πεδίο Τιμών
refersToData	Rules	Data
refersToPurpose	Rules	Purposes
refersToRole	Rules	Roles
refersToObligation	Rules	Obligations
appliesUnderCondition	Rules	Conditions
refersToRule	Rules	Rules
follows	Obligations	ObligationPatterns
excludesRules	ExclusiveCombinations	Rules
excludesData	ExclusiveCombinations	Data
underCondition	ExclusiveCombinations	Conditions
hasSubject	Conditions	ConditionSubject
hasObject	Conditions	ConditionObject
hasOperator	Conditions	Operators
refersToSubject	ConditionSubject	Data
refersToObject	ConditionObject	Data
isOfType	Conditions	CntexualTypes
hasValue	Conditions	ContexualBase
inheritsFromRole	Roles	Roles
isPartOfRole	Roles	Roles
inheritsFromPurpose	Purposes	Purposes
isPartOfPurpose	Purposes	Purposes
inheritsFromData	Data	Data

isPartOfData	Data	Data
appliesToDataDescendants	Rules	-
appliesToServiceDescendants	Rules	-
appliesToRoleDescendants	Rules	-
disclosureOfResource	Rules	-
modificationPermission	Rules	-
creatorConsent	Rules	-
overrideConflictingPreferences	Rules	-
refersToOutgoingRequest	Rules	-
isDelegation	Rules	-
isForward	Rules	-

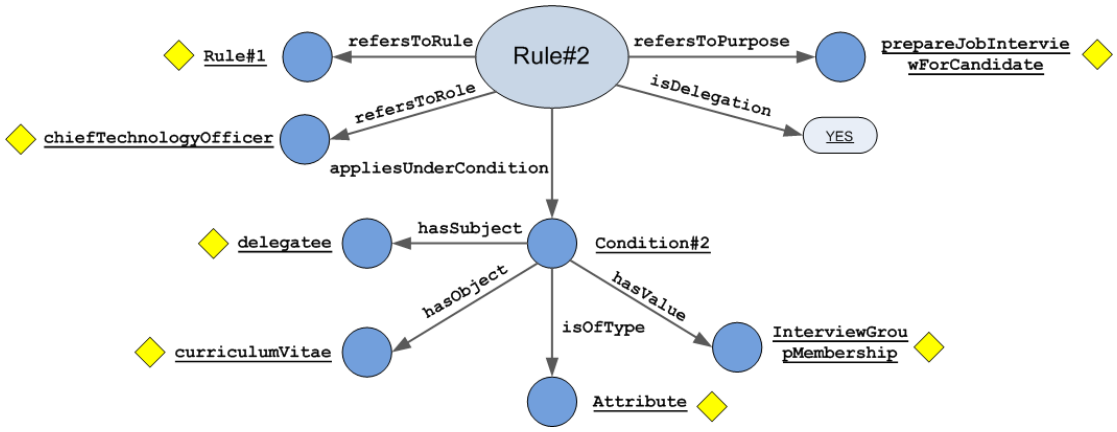
Πίνακας 2: Σύνολο ιδιοτήτων Οντολογίας Εξουσιοδοτήσεων

Οι Εικόνες Εικόνα 15, Εικόνα 16 και Εικόνα 17 αναπαριστούν γραφικά ένα παράδειγμα κανόνων εξουσιοδότησης που προδιαγράφονται από χρήστη της πλατφόρμας και αφενός αφορούν πρόσβαση σε δεδομένα αφετέρου ορίζουν συνθήκες μεταφοράς των εν λόγω δικαιωμάτων και περαιτέρω προώθησης των αναφερόμενων δεδομένων. Περιγραφικά ο κανόνας έχει ως εξής: «Να επιτρέπεται η πρόσβαση στα δεδομένα τύπου *curriculumVitae* (βιογραφικό σημείωμα) με δικαιώματα ανάγνωσης σε αιτούντες που ενεργοποιούν τον ρόλο του *humanResourceDepartmentSupervisor* (επικεφαλής του τμήματος Διαχείρισης Ανθρώπινου Δυναμικού) σε κάποιο οργανισμό, ενώ υπηρετούν τον στόχο *evaluationOfCandidateSuitability* (εξακρίβωση καταλληλότητας υποψηφίου). Η απόδοση δικαιωμάτων ανάγνωσης πραγματοποιείται μόνο σε περίπτωση που ο οργανισμός χαρακτηρίζεται από υψηλό επίπεδο εμπιστοσύνης των πολιτικών πιστοποίησης που αξιοποιεί, όπως καταδεικνύεται από την παράμετρο LoA, και με την υποχρέωση της διατήρησης των δεδομένων στην πλευρά του οργανισμού για χρονικό διάστημα που δεν υπερβαίνει τις 30 μέρες. Η ισχύς του κανόνα μεταφέρεται σε όλα τα στοιχεία που ενσωματώνει ο συγκεκριμένος τύπος δεδομένων και επίσης σε όλους τους σκοπούς πρόσβασης που απορρέουν από τον σκοπό *evaluationOfCandidateSuitability»*. Επιπρόσθετα, ορίζεται «τα συγκεκριμένα δικαιώματα πρόσβασης να μεταφέρονται από τους δικαιούχους σε οντότητες που ενεργοποιούν τον ρόλο του *chiefTechnologyOfficer* (προϊσταμένου τεχνολογίας) για την εξυπηρέτηση του σκοπού *prepareJobInterviewForCandidate* (προετοιμασία συνέντευξης για τον υποψήφιο), εφόσον ανήκουν σε συγκεκριμένη

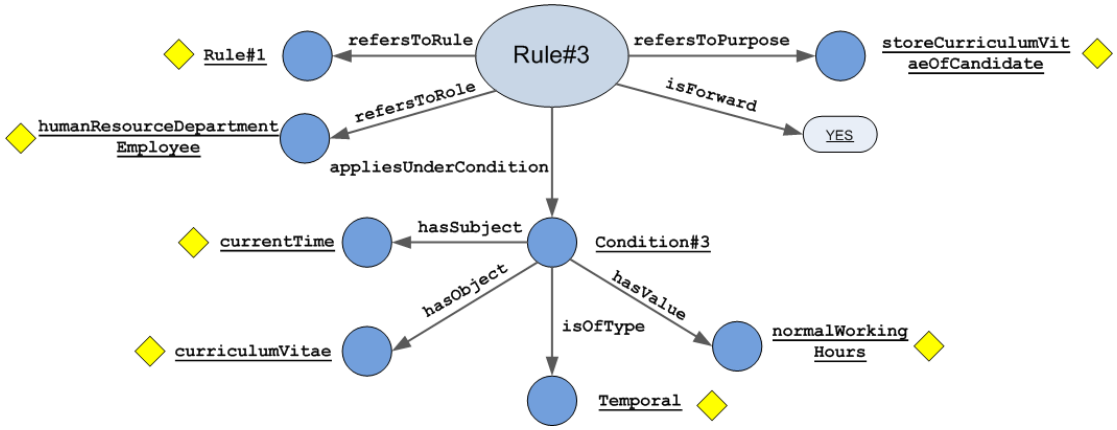
ομάδα υπαλλήλων, στις αρμοδιότητες των οποίων ανήκει η διεξαγωγή συνεντεύξεων με υποψήφιους για εργασία». Τέλος, προδιαγράφεται «τα δεδομένα του συγκεκριμένου τύπου πρόσβασης να μπορούν να προωθηθούν από τους δικαιούχους σε οντότητες που ενεργοποιούν τον ρόλο του *humanResourceDepartmentEmployee* (υπαλλήλου του τμήματος διαχείρισης ανθρώπινου δυναμικού) για την εξυπηρέτηση του σκοπού *storeCurriculumVitaeOfCandidate* (καταχώρηση βιογραφικού σημειώματος) εφόσον η σχετική ενέργεια πραγματοποιείται σε μέρα και σε ώρα που ανήκουν στο χρονικό διάστημα Δευτέρα – Παρασκευή και 8:00ΠΜ – 8:00ΑΜ αντίστοιχα».



Εικόνα 15: Κανόνας ελέγχου πρόσβασης

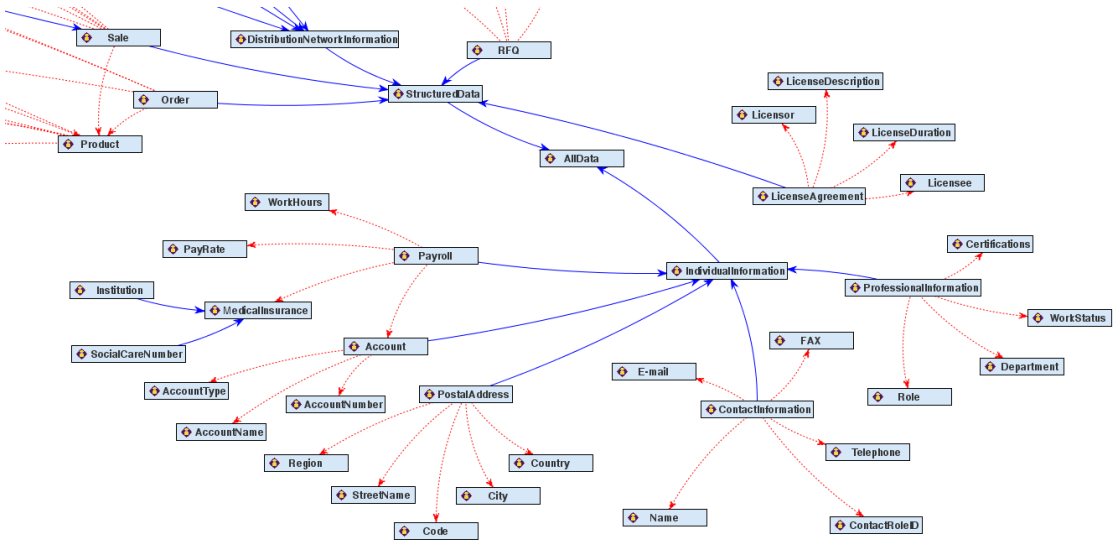


Εικόνα 16: Κανόνας μεταφοράς δικαιωμάτων πρόσβασης



Εικόνα 17: Κανόνας προώθησης δεδομένων

Επιπρόσθετα, κατά την προδιαγραφή των κανόνων εξουσιοδότησης έχει ληφθεί μέριμνα για την ενσωμάτωση εννοιών τόσο σε συγκεκριμένο (concrete level) όσο και σε αφαιρετικό (abstract level) επίπεδο. Επίσης, στις κλάσεις που αποτελούν το πυρήνα των κανόνων εξουσιοδότησης, ήτοι στις κλάσεις *Data*, *Purposes* και *Roles*, ορίζεται όλα τα στιγμιότυπα να κληρονομούν από ένα γενικό αντικείμενο-ρίζα των κλάσεων που ονομάζεται *allData*, *allPurposes* και *allRoles* αντίστοιχα. Η Εικόνα 18 παρουσιάζει τη γραφική αναπαράσταση ενός τμήματος του υπογράφου *Data* της Οντολογίας Εξουσιοδοτήσεων με εμφανείς τις επιμέρους ταξινομήσεις των αντίστοιχων στιγμιότυπων μέσω των ιδιοτήτων *inheritsFromData* και *isPartOfData*.



Εικόνα 18: Ταξινόμηση στιγμιότυπων της κλάσης *Data* της Οντολογίας Εξουσιοδοτήσεων

Ο ορισμός πολιτικών εξουσιοδότησης που ενσωματώνουν τα γενικά στιγμιότυπα ρίζας, συνεπάγεται την ισχύ του κανόνα για κάθε ένα από τα λοιπά στιγμιότυπα-απογόνους των αντίστοιχων κλάσεων. Επιπλέον, η συγκεκριμένη επιλογή επιτρέπει

στη μοντελοποίηση του προβλήματος να παραμείνει εντός του εκφραστικού τμήματος της OWL που αναφέρεται ως OWL DL (από τα αρχικά της Περιγραφικής Λογικής – Description Logic) και διατηρεί τα πλεονεκτήματα της υπολογιστικής πληρότητας (computational completeness) και της συμπερασματικής αποφασισιμότητας (decidability) έναντι της πιο εκφραστικής παραλλαγής της OWL που αναφέρεται ως OWL Full. Πράγματι, η OWL Full, έχοντας τη μεγαλύτερη εκφραστική χωρητικότητα από όλες τις διαθέσιμες παραλλαγές της OWL, επιτρέπει τη σύνδεση στιγμιότυπων με κλάσεις και άρα επιτρέπει την προδιαγραφή σύνθετων δηλώσεων σε αφαιρετικό επίπεδο. Ωστόσο δεν εξασφαλίζει την πληρότητα των προδιαγραφόμενων δηλώσεων και την αποφασισιμότητα της διαδικασίας παραγωγής συλλογισμών, με αποτέλεσμα να μην υπάρχουν διαθέσιμα λογισμικά συλλογιστικής (reasoners) κατάλληλα για εφαρμογή σε OWL Full οντολογίες.

5.2 Μηχανή Παραγωγής Συλλογισμών

Η διαδικασία της εξαγωγής συμπερασμάτων και παραγωγής συλλογισμών στη βάση ενός συνόλου κανόνων εξουσιοδότησης, αποτελεί τον πυρήνα της επιχειρηματικής λογικής της προτεινόμενης λύσης. Με στόχο την αύξηση της κλιμακοθετησιμότητας του συστήματος οι συγκεκριμένες λειτουργικότητες στο πλαίσιο της λειτουργίας της πλατφόρμας πραγματοποιούνται στη λογική του σαφούς διαχωρισμού τους σε διαδικασίες «**στατικής** και **δυναμικής συλλογιστικής**». Πιο λεπτομερώς, ένα βασικό συμπέρασμα που μπορεί να εξαχθεί σε σχέση με το υιοθετημένο μοντέλο πληροφοριών και των ακολουθούμενων κανόνων συλλογιστικής, αφορά το γεγονός ότι η αποσαφήνιση των ισχυόντων εξουσιοδοτήσεων μπορεί να πραγματοποιηθεί πριν καν την καταχώρηση σχετικών αιτημάτων για εξουσιοδότηση, τουλάχιστον σε σχέση με τα θεμελιώδη συστατικά τους (τύπος δεδομένων, ρόλος και σκοπός πρόσβασης). Έτσι, ο όρος της στατικής συλλογιστικής εισήχθηκε για να περιγράψει τις διαδικασίες εκτίμησης του συνόλου των εξουσιοδοτήσεων βάσει παραμέτρων που παραμένουν σταθερές στην πάροδο του χρόνου και περιγράφουν μια *a priori* θεώρηση του συστήματος (π.χ. οι συσχετίσεις μεταξύ ρόλων και σκοπών πρόσβασης, δηλαδή τα στιγμιότυπα του συνόλου PR, ορίζονται άπαξ πριν την εκκίνηση της λειτουργίας του συστήματος). Αντίθετα, η δυναμική συλλογιστική αντιστοιχεί στην εκτίμηση δυναμικών παραμέτρων που αποκτούν υπόσταση μόνο κατά τη διάρκεια της λειτουργίας της πλατφόρμας, δηλαδή σε πραγματικό χρόνο (π.χ. η εξακρίβωση της

τρέχουσας ώρας κατά την καταχώρηση αιτήματος δεν μπορεί παρά να ελεγχθεί σε πραγματικό χρόνο). Με αυτόν τον τρόπο, οι διαδικασίες δυναμικής συλλογιστικής παρέχουν τη δυνατότητα στο σύστημα να διατηρεί χαρακτηριστικά «αυτό-προσαρμοστικότητας» σε σχέση με δυναμικές μεταβολές παραμέτρων του περιβάλλοντος λειτουργίας.

5.2.1 Στατική Συλλογιστική

Στόχος των διαδικασιών παραγωγής στατικών συλλογισμών αποτελεί η αποσαφήνιση του συνόλου των ισχυόντων εξουσιοδοτήσεων στη βάση των κανόνων-προτιμήσεων που έχουν δημιουργηθεί από τις οντότητες του συστήματος και τους κανόνες συλλογιστικής όπως παρουσιάστηκαν στην ενότητα 4.3.3. Πιο συγκεκριμένα, σε αυτή τη φάση της διαδικασίας συλλογισμού εξετάζονται όλες οι πιθανές σημασιολογικές δηλώσεις όπως αυτές προκύπτουν από την Οντολογία Εξουσιοδοτήσεων και υπό το πρίσμα των προαναφερθέντων κανόνων συμπερασμού, με στόχο την καταγραφή όλων εκείνων των συνδυασμών στιγμιότυπων που περιγράφουν **θετικές** εξουσιοδοτήσεις. Οι εξουσιοδοτήσεις-αποτελέσματα των διαδικασιών στατικής συλλογιστικής συνιστούν αντικείμενα του συνόλου PDT, συσχετισμένα με ζεύγη ρόλων και σκοπών πρόσβασης καθώς και δηλώσεις των απαραίτητων συνθηκών που καθορίζουν την ισχύ της εξουσιοδότησης και των υποχρεώσεων που απορρέουν από την εφαρμογή της. Σημειώνεται ότι αντικείμενα του συνόλου PDT δύναται φυσικά να προέρχονται από ευθείς εξουσιοδοτήσεις αλλά και από σχετικές πολιτικές μεταφοράς δικαιωμάτων και προώθησης δεδομένων.

Για την εξασφάλιση της αποφασισιμότητας, συνοχής και σαφήνειας των σχεδιαζόμενων συμπερασματικών αλγόριθμων, στο σύνολο των αξιοποιούμενων κανόνων συλλογισμού προστέθηκαν οι ακόλουθες αρχές ως ασφαλιστικές δικλείδες:

- Ένα στιγμιότυπο της κλάσης *Rules* δεν μπορεί να αποτελεί ταυτόχρονα πολιτική ελέγχου πρόσβασης, μεταφοράς δικαιωμάτων και προώθησης δεδομένων. Σε μια τέτοια περίπτωση ο κανόνας αγνοείται και δεν παράγει θετικές ή αρνητικές εξουσιοδοτήσεις.
- Αποφυγή κυκλικών κληρονομικοτήτων μεταξύ των στιγμιότυπων των κλάσεων της Οντολογίας. Η συγκεκριμένη ασφαλιστική δικλείδα ουσιαστικά εφαρμόζεται ήδη από το στάδιο του ορισμού των αντικειμένων της Οντολογίας.

- Σε περίπτωση που ένα στιγμιότυπο της κλάσης *Rules* συνιστά κανόνα μεταφοράς δικαιωμάτων ή προώθησης δεδομένων, το αντικείμενο της περιγραφείσας ενέργειας καταδεικνύεται από τον αντικείμενο της ιδιότητας *refersToRule.*
- Σε περίπτωση «συγκρούσεων», δηλαδή της ταυτόχρονης ύπαρξης τόσο θετικού όσο και αρνητικού κανόνα πρόσβασης για ένα συνδυασμό αντικειμένων $\langle dt_i, pu_j, r_k \rangle$ ακολουθήθηκε ο κανόνας του «εγγύτερου κανόνα επιρροής», σύμφωνα με τον οποίο αποκτούν προτεραιότητα οι οδηγίες του κανόνα που σχηματίστηκε στη βάση του συνδυασμού των αντικειμένων $\langle dt_l, pu_m, r_n \rangle$, ο οποίος «κληρονομικά» βρίσκεται εγγύτερα στον συνδυασμό $\langle dt_i, pu_j, r_k \rangle$. Μάλιστα, οι περιπτώσεις των «συγκρούσεων» για το σύνολο των κανόνων που προδιαγράφει μια οντότητα αποτελεί σύνηθες φαινόμενο, λόγω των σχέσεων κληρονομικότητας μεταξύ των συστατικών στοιχείων των κανόνων.
- Ομοίως, σε περίπτωση πολλαπλών ορισμών συνθηκών και υποχρεώσεων όπως προκύπτουν από πολλαπλούς θετικούς κανόνες για ένα συνδυασμό αντικειμένων $\langle dt_i, pu_j, r_k \rangle$, καταγράφεται ως ισχύων ορισμός αυτός της συνθήκης του «εγγύτερου κανόνα επιρροής».
- Αν και η λήψη αποφάσεων στη βάση OWL οντολογιών υιοθετεί την Υπόθεση Ανοιχτού Κόσμου (Open World Assumption), όπου η αποτυχία εξακρίβωσης της ισχύος μιας δήλωσης δεν ισοδυναμεί αυτόματα με τη θεώρηση της δήλωσης ως εσφαλμένη, στο πλαίσιο της παρούσας διατριβής και με στόχο την ελαχιστοποίηση των περιπτώσεων ασαφούς κατάστασης εξουσιοδότησης υιοθετήθηκε η Υπόθεση Κλειστού Κόσμου (Closed World Assumption – CWA). Έτσι, σε περίπτωση μη εύρεσης θετικής εξουσιοδότησης για ένα σύνολο $\langle dt_i, pu_j, r_k \rangle$, η διαδικασία συλλογιστικής εξάγει αυτόματα συμπέρασμα αρνητικής εξουσιοδότησης.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι δόθηκε έμφαση στη διατήρηση της ποιότητας της **μη μονοτονικότητας** κατά την παραγωγή εξουσιοδοτήσεων. Αν και προφανής στόχος των λειτουργιών στατικής συλλογιστικής είναι η εξακρίβωση των θετικών εξουσιοδοτήσεων, η δυνατότητα προδιαγραφής αρνητικών πολιτικών εξουσιοδότησης επιτρέπει στο σύστημα να διαχειρίζεται τις δηλώσεις

εξουσιοδότησης με μη μονοτονικό τρόπο, ήτοι η προδιαγραφή προστιθέμενων κανόνων δεν ισοδυναμεί αυστηρά με την προσθήκη περισσότερων εξουσιοδοτήσεων. Για τη διεκπεραίωση των λειτουργιών στατικής συλλογιστικής υιοθετήθηκαν δυο διαφορετικές προσεγγίσεις. Η πρώτη περιλαμβάνει το ευρέως διαδεδομένο εργαλείο λογισμικού Pellet [113] που παρέχει υπηρεσίες συλλογιστικής για οντολογίες σχεδιασμένες στη γλώσσα OWL DL. Η δεύτερη μέθοδος αντιστοιχεί στην αξιοποίηση ενός τυπικού λογισμικού παραγωγής συμπερασμάτων που υλοποιήθηκε στο πλαίσιο της εκπόνησης της παρούσας διατριβής, προσαρμοσμένο ακριβώς στις ανάγκες εξαγωγής συμπερασμάτων του σχήματος της Οντολογίας Εξουσιοδοτήσεων. Το εργαλείο αναπτύχθηκε στη γλώσσα προγραμματισμού Java, ενώ εκμεταλλεύεται της δυνατότητες υποβολής ερωτημάτων σε οντολογίες της βιβλιοθήκης Jena [114]. Πέραν της περιγραφής της λειτουργίας των δύο εργαλείων λογισμικού συλλογιστικής, στη συνέχεια πραγματοποιείται μια συνοπτική σύγκριση της απόδοσής τους όπως αυτή αξιολογήθηκε μέσω μιας σειράς διαφορετικών πειραμάτων λειτουργίας με εικονικές Οντολογίες Εξουσιοδοτήσεων. Οι εικονικές εκδόσεις της Οντολογίας Εξουσιοδοτήσεων δημιουργήθηκαν με στόχο την εκτίμηση της χρονικής διάρκειας των διαδικασιών συλλογιστικής ανάλογα με το συνολικό μέγεθος της οντολογίας δείγματος, σε ότι αφορά το σύνολο των αντικειμένων της. Ο Πίνακας 3 απεικονίζει τις διαφορετικές εκδόσεις της Οντολογίας Εξουσιοδοτήσεων, συνοδευόμενες από το μέγεθός τους. Σημειώνεται, ότι οι εκδόσεις των εικονικών οντολογιών δημιουργήθηκαν αυτόματα από κατάλληλα σχεδιασμένο λογισμικό και επομένως χαρακτηρίζονται από μεγάλο βαθμό τυχαιότητας σε ότι αφορά την πολυπλοκότητα των αντικειμενικών OWL ιδιοτήτων. Το γεγονός αυτό επιτρέπει την εξαγωγή κυρίως γενικών συμπερασμάτων για τις διαδικασίες στατικής συλλογιστικής και τις επιδόσεις τους.

Έκδοση	**Αντικείμενα *Data***	**Αντικείμενα *Purposes***	**Αντικείμενα *Roles***	**Αντικείμενα *Rules***	**Συνολικά Αντικείμενα**
A	500	750	100	300	1650
B	1000	750	100	300	2150
C	500	1500	200	300	2500
D	500	750	100	300	1650
E	500	750	100	600	1950

F	1500	750	100	300	2650
G	2000	750	100	300	3150
H	500	2250	100	300	3150
I	500	3000	100	300	3900
J	500	750	300	300	1850
K	500	750	400	300	1950
L	500	750	100	900	2250
M	500	750	100	1200	2550
N	1000	1500	200	600	3300
O	1500	2250	300	900	4950
P	2000	3000	400	1200	6600

Πίνακας 3: Διαφορετικές εκδόσεις εικονικών Οντολογιών Εξουσιοδότησης

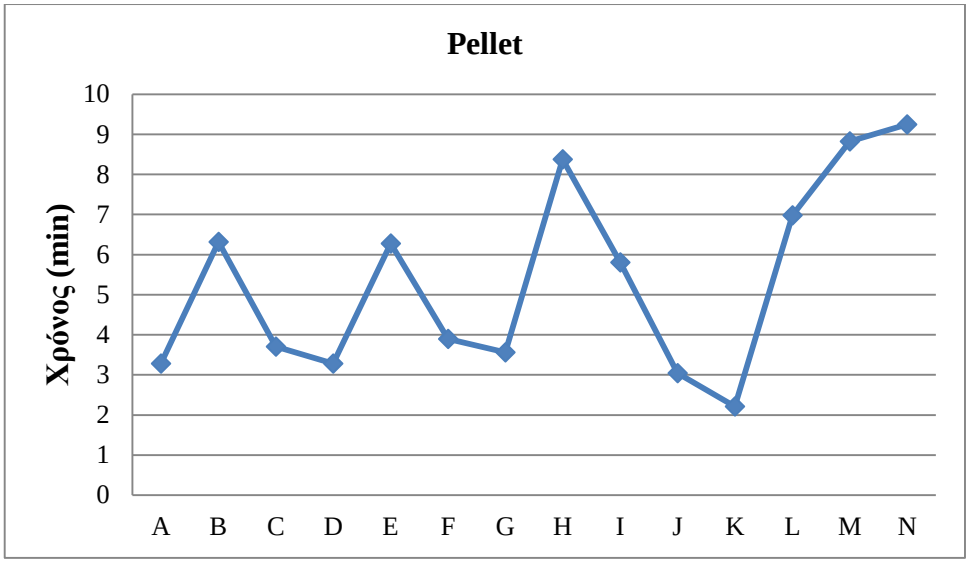
5.2.1.1 Παραγωγή Συμπερασμάτων με Χρήση του Pellet

Το λογισμικό Pellet αποτελεί ένα διαδεδομένο εργαλείο λογισμικού ανοιχτού κώδικα για την παραγωγή συμπερασμάτων σε οντολογίες OWL DL. Ως ολοκληρωμένο εργαλείο προσφέρει μια πλούσια ποικιλία υπηρεσιών συλλογιστικής όπως, ολοκλήρωση με τις βιβλιοθήκες Jena και OWL, αξιοποίηση κανόνων συλλογιστικής της γλώσσας Semantic Web Rule Language (SWRL) και έλεγχο συνοχής οντολογιών μεταξύ άλλων. Για τις ανάγκες της διατριβής, το εργαλείο χρησιμοποιήθηκε σε συνδυασμό με την προδιαγραφή συγκεκριμένων κανόνων συμπερασμού στη γλώσσα SWRL. Πιο συγκεκριμένα, οι κανόνες SWRL δημιουργήθηκαν έτσι ώστε να αντιστοιχούν στους κανόνες συλλογιστικής της ενότητας 4.3.3. Οι κανόνες καταγράφονται στη μορφή επαγωγής μεταξύ μιας υπόθεσης και ενός συμπεράσματος και μπορούν να ερμηνευτούν ως εξής: *όταν οι συνθήκες της υπόθεσης ισχύουν τότε ισχύουν και οι συνθήκες του συμπεράσματος*. Για παράδειγμα, η μεταφερσιμότητα των κανόνων ελέγχου πρόσβασης μεταξύ δύο τύπων δεδομένων που συνδέονται με την OWL ιδιότητα *inheritsFromData*, συμβατή με τη σύνταξη της γλώσσας SWRL, παρουσιάζεται στην Εικόνα 19.

```
<swrl:Imp rdf:about="OntRule1">
	<swrl:head rdf:parseType="Collection">
		<swrl:IndividualPropertyAtom>
		<swrl:propertyPredicate rdf:resource="#refersToData" />
			<swrl:argument1 rdf:resource="#x" />
			<swrl:argument2 rdf:resource="#z" />
		</swrl:IndividualPropertyAtom>
	</swrl:head>
	<swrl:body rdf:parseType="Collection">
		<swrl:ClassAtom>
			<swrl:classPredicate rdf:resource="#Rules" />
			<swrl:argument1 rdf:resource="#x" />
		</swrl:ClassAtom>
		<swrl:IndividualPropertyAtom>
			<swrl:propertyPredicate  rdf:resource="#refersToData"
/>
			<swrl:argument1 rdf:resource="#x" />
			<swrl:argument2 rdf:resource="#y" />
		</swrl:IndividualPropertyAtom>
		<swrl:IndividualPropertyAtom>
		<swrl:propertyPredicate rdf:resource="#inheritsFromData" />
			<swrl:argument1 rdf:resource="#z" />
			<swrl:argument2 rdf:resource="#y" />
		</swrl:IndividualPropertyAtom>
	</swrl:body>
</swrl:Imp>
```

Εικόνα 19: Ενδεικτικός κανόνας SWRL

Η Εικόνα 20 συνοψίζει την επίδοση του εργαλείου Pellet σε ότι αφορά τον συνολικό χρόνο εκτέλεσής του για την εξαγωγή όλων των στιγμιότυπων PDT στη βάση των διαφορετικών εκδόσεων της Οντολογίας Εξουσιοδοτήσεων. Αποδεικνύεται, ότι οι χρόνοι λειτουργίας του εργαλείου επηρεάζονται μερικώς από τον συνολικό αριθμό αντικειμένων της οντολογίας, όσο αυτός διατηρείται εντός κάποιου ορίου (οντολογίες A, D, J, K και E). Ωστόσο, καθώς ο αριθμός των στιγμιότυπων των οντολογικών κλάσεων αυξάνεται, οι μετρήσεις αποδεικνύουν μια πιο άμεση επίδραση στον χρόνο εκτέλεσης, αρχικά μικρή και τελικά απαγορευτική, σε σημείο που το λογισμικό δεν ολοκληρώνει επιτυχημένα την εκτέλεσή του (οντολογίες O και P). Τέλος, απεικονίζεται εμφανώς η επιρροή του μεγέθους του συνόλου των κανόνων εξουσιοδότησης στον συνολικό χρόνο εκτέλεσης, σε μια σχεδόν γραμμική σχέση (οντολογίες A, E, L και M).



Εικόνα 20: Χρόνος εκτέλεσης λογισμικού Pellet

5.2.1.2 Παραγωγή Συμπερασμάτων με Χρήση του Προσαρμοσμένου Λογισμικού

Το λογισμικό παραγωγής συμπερασμάτων που υλοποιήθηκε στο πλαίσιο της εκπόνησης της παρούσας διατριβής βασίστηκε στις δυνατότητες υποβολής οντολογικών ερωτημάτων (ontology queries) της βιβλιοθήκης Jena και στην εφαρμογή ενός αλγορίθμου διάσχισης της Οντολογίας Εξουσιοδοτήσεων. Ο εν λόγω αλγόριθμος αποτελεί ένα σχήμα διάσχισης γράφων οριζόντιας διερεύνησης (Breadth First Search – BFS), όπου κάθε στιγμιότυπο της κλάσης *Roles* αντιστοιχίζεται στιγμιότυπα της κλάσης *Purposes* και τελικά με Επιτρεπτούς Τύπους Δεδομένων. Οι ίδιοι κανόνες συλλογιστικής που εφαρμόστηκαν στην περίπτωση του εργαλείου Pellet προδιαγράφηκαν και εφαρμόστηκαν και στην περίπτωση του προσαρμοσμένου λογισμικού με χρήση της βιβλιοθήκης Jena. Ο αλγόριθμος υπολογισμού των αντικειμένων του συνόλου PDT, σύμφωνα με τους κανόνες ελέγχου πρόσβασης παρουσιάζεται στην Εικόνα 21. Πανομοιότυπος αλγόριθμος, αξιοποιείται και για την εξαγωγή των PDT αντικειμένων, όπως αυτά προκύπτουν από κανόνες μεταφοράς δικαιωμάτων και προώθησης δεδομένων. Επιπλέον των μετρήσεων σχετικά με τον χρόνο εκτέλεσης του λογισμικού στη βάση των διαφορετικών εκδόσεων της Οντολογίας Εξουσιοδοτήσεων, πραγματοποιήθηκαν μετρήσεις του χρόνου εξαγωγής καθενός διακριτού αντικειμένου του συνόλου PDT με στόχο την αναγνώριση των μέσων χρόνων απόκρισης του λογισμικού σε μοναδικά οντολογικά ερωτήματα (Πίνακας 4).

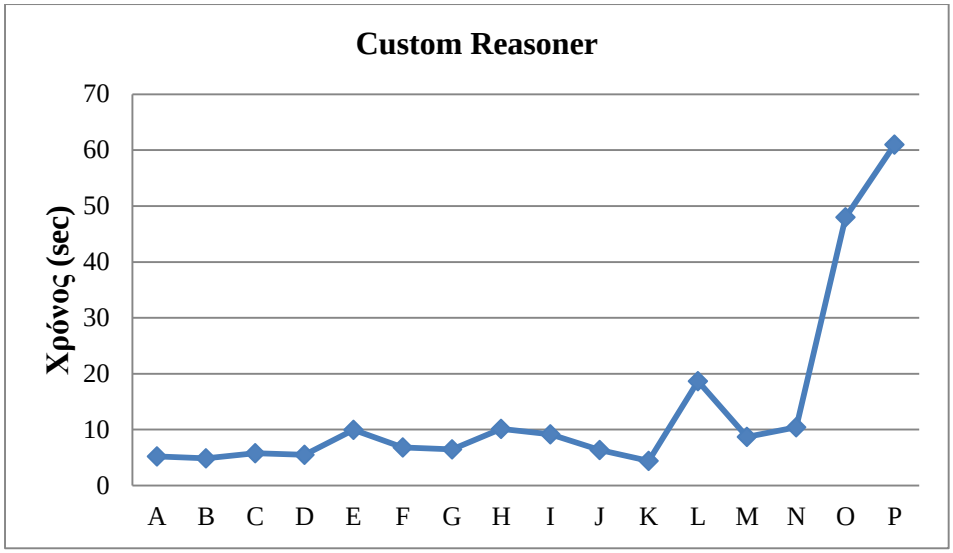
```
PDTAlg ()
{
for each (instance of the Roles class)
{
	for each (instance of the Rules class that has refersToRole
	property referring to the Role instance under investigation)
	{
		associate Role instance to Rule instance in a "Role to
		Rules" map;
	}
}
for each (Role entry of the "Role to Rules" map)
{
	for each (Rule entry)
	{
		if (appliesToRoleDescendants property is YES)
		{
			for each (instance of the Roles class that is linked
			with the Role entry under investigation via an
			inheritsFromRole property)
			{
			add association of Role instance to the Rule entry
			under investigation in the "Role to Rules" map;
			}
			for each (instance of the Roles class that is linked
			with the Role entry under investigation via an
			isPartOfRole property)
			{
				if (DisclosureOfData property is YES)
				add association of Role instance to the Rule
				entry under investigation in the "Role to
				Rules" map;
			}
			for each (instance of the Roles class that is linked
			with the Role entry under investigation via an
			containsRole property)
			{
				if ((DisclosureOfData property is YES)&&(all
				similarly linked instances of the Roles class
				have the same Rule applied with the same
				values))
				add association of Role instance to the Rule
				entry under investigation in the "Role to
				Rules" map;
				if (DisclosureOfData property is NO)
				add association of Role instance to the Rule
				entry under investigation in the "Role to
				Rules" map;
			}
		}
	}
}

for each (instance of the Purposes class)
{
	for each (instance of the Rules class that has refersToPurpose
	property referring to the Purpose instance under investigation)
	{
		associate Purpose instance to Rule instance in a "Purpose to
		Rules" map;
	}
}
for each (Purpose entry of the "Purpose to Rules" map)
{
	for each (Rule entry)
	{
```

```
            if (appliesToPurposeDescendants property is YES)
            {
                  for each (instance of the Purposes class linked
                  with the Purpose entry under investigation via an
                  inheritsFromPurpose property)
                  {
                  add association of Purpose instance to the Rule entry
                  under investigation in the "Purpose to Rules" map;
                  }

                  for each (instance of the Purposes class linked
                  with the Purpose entry under investigation via an
                  isPartOfPurpose property)
                  {
                        if (DisclosureOfData property is YES)
                        add association of Purpose instance to the Rule
                        entry  under investigation in the "Purpose to
                        Rules" map;
                  }
                  for each (instance of the Purposes class linked
                  with the Purpose entry under investigation via an
                  containsOfPurpose property)
                  {
                        if ((DisclosureOfData property is YES)&&(all
                        similarly linked instances of Purposes  have
                        the sane Rule applied with the same values))
                        add association of Purpose instance to the Rule
                        entry under investigation in the "Purpose to
                        Rules" map;
                        if (DisclosureOfData property is NO)
                        add association of Purpose instance to the Rule
                        entry under investigation in the "Purpose to
                        Rules" map;
                  }
            }
      }
}

for each (instance of the Data class)
{
      for  each  (instance  of  the  Rules  class  that  has  refersToData
      property referring to the Data instance under investigation)
      {
            associate Data instance to Rule instance in a
            "Data to Rules" map;
      }
}
for each (Data entry of the "Data to Rules" map)
{
      for each (Rule entry)
      {
            if (appliesToDataDescendants property is YES)
            {
                  for each (instance of the Data class that is
                  linked with the Data entry under investigation
                  via an inheritsFromData property)
                  {
                  add association of Data instance to the Rule
                  entry under investigation in the "Data to
                  Rules" map;
                  }
                  for each (instance of the Data class that is
                  linked with the Data entry under investigation
                  via an isPartOfData property)
                  {
```

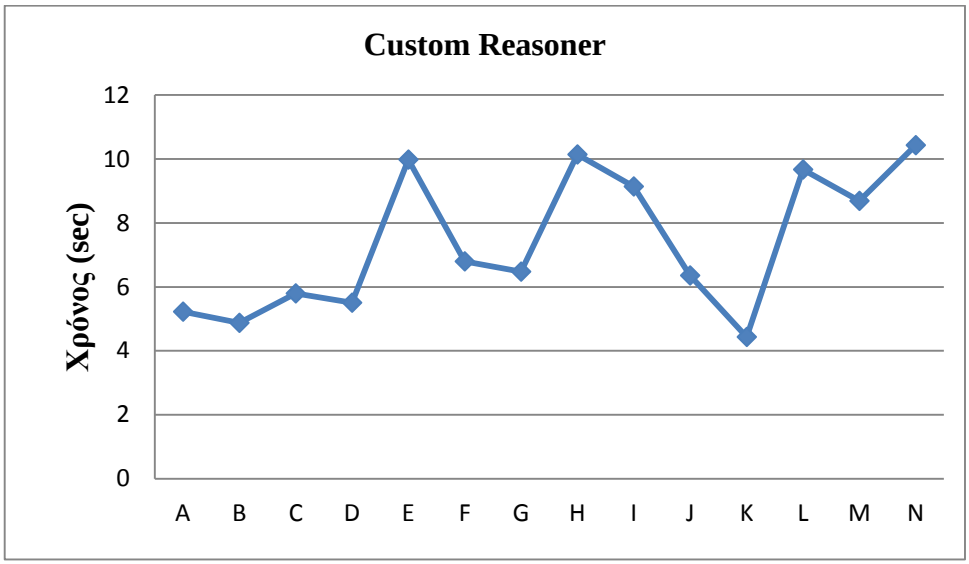
```
                        if (DisclosureOfData property is YES)
                        add association of Data instance to the
                        Rule entry under investigation in the
                        "Data to Rules" map;
                }
                for each (instance of the Data class that is
                linked with the Data entry under investigation
                via a containsData property)
                {
                        if ((DisclosureOfData property is YES)&&(all
                        similarly linked instances of the Data
                        class have the same Rule applied with the same
                        values))
                        add association of Data instance to the
                        Rule entry under investigation in the
                        "Data to Rules" map;
                        if (DisclosureOfData property is NO)
                        add association of Data instance to the
                        Rule entry under investigation in the
                        "Data to Rules" map;
                }
        }
    }
}

for each (instance of the Rules class)
{
    find intersection between "Roles to Rules", "Purposes to Rules" and
    "Data to Rules" maps;
    add Role, Purpose, Data triples into PDT set;
}
for each (instance of the created PDT set)
{
    if ((multiple Rules apply to the PDT instance)&&(these Rules have
    different values in their DisclosureOfData property))
    apply the Rule originally applied to the "closest" Role, Purpose or
    Data instance;
}
return (PDT set);
}
```

Εικόνα 21: Αλγόριθμος υπολογισμού των αντικειμένων του συνόλου PDT

Τα διεξαχθέντα πειράματα ανέδειξαν μια κοινή συμπεριφορά του προσαρμοσμένου λογισμικού με αυτή του εργαλείου Pellet σε ότι αφορά την επίδραση των διαφορετικών εκδόσεων της Οντολογίας Εξουσιοδοτήσεων στον συνολικό χρόνο εκτέλεσης του αλγορίθμου συλλογισμού, καθώς και τα δύο παρουσιάζουν παρόμοια «ευαισθησία» στην αύξηση του αριθμού των κανόνων εξουσιοδότησης (Εικόνα 22). Η ομοιότητα αυτή αποσαφηνίζεται από μια παραλλαγή της γραφικής παράστασης, όπου παραλείπονται τα σημεία στα οποία το εργαλείο Pellet δεν ολοκλήρωσε την εκτέλεσή του (Εικόνα 23).



Εικόνα 22: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (1)



Εικόνα 23: Χρόνος εκτέλεσης λογισμικού παραγωγής συμπερασμάτων (2)

Έκδοση Οντολογίας	Χρόνος εξαγωγής μοναδικού αντικειμένου	Min/Max χρόνος (nsec)
A	32182766	*Max*
	23067	*Min*
B	24787451	*Max*
	22757	*Min*
C	2472278	*Max*
	35779	*Min*
D	5378962	*Max*
	22671	*Min*
E	27663464	*Max*

	38441	*Min*
F	118927123	*Max*
	22590	*Min*
G	1060466	*Max*
	34927	*Min*
H	33868376	*Max*
	37207	*Min*
I	28045845	*Max*
	35237	*Min*
J	25306220	*Max*
	35372	*Min*
K	1087368	*Max*
	35904	*Min*
L	20509455	*Max*
	39127	*Min*
M	5669407	*Max*
	34597	*Min*
N	711351213	*Max*
	35177	*Min*
O	750146683	*Max*
	38335	*Min*
P	987565990	*Max*
	35543	*Min*

Πίνακας 4: Χρόνος εξαγωγής μοναδικών αντικειμένων του συνόλου PDT

5.2.1.3 Σύγκριση Απόδοσης

Αποκρυπτογραφώντας τα παραπάνω διαγράμματα, γίνεται εμφανές ότι η διαδικασία παραγωγής συλλογισμών δεν είναι κατάλληλη για διεξαγωγή σε πραγματικό χρόνο κατά τη διάρκεια λειτουργίας της πλατφόρμας. Ακόμα και στην περίπτωση μοναδικών ερωτημάτων στις οντολογίες προκύπτει ότι η εξαγωγή απόφασης μπορεί να διαρκέσει έως 1 sec. Ωστόσο, οι συγκεκριμένες χρονικές απαιτήσεις δεν είναι απόλυτες, καθώς για να θεωρηθεί η εξαχθείσα απόφαση τελική είναι απαραίτητη η διεξαγωγή πολλαπλών ακόμα αιτημάτων στις οντολογίες για την εύρεση κανόνων που είναι δυνατόν να επηρεάζουν την αρχική απόφαση. Επιπλέον, δεδομένης της καταχώρησης πολλαπλών διαφορετικών ταυτόχρονων ερωτημάτων σε πραγματικές συνθήκες, η διαχείριση των διαδικασιών στατικής συλλογιστικής σε πραγματικό χρόνο κρίνεται υπολογιστικά ασύμφορη. Επομένως στο πλαίσιο της λειτουργίας της πλατφόρμας οι εργασίες στατικής συλλογιστικής πραγματοποιούνται πριν την

εκκίνηση του συστήματος κατά τη φάση διαμόρφωσης της υποδομής, όπως θα περιγραφεί σε επόμενη ενότητα.

Παράλληλα, είναι προφανής η βελτίωση του χρόνου απόκρισης του προσαρμοσμένου λογισμικού έναντι των επιδόσεων του εργαλείου Pellet. Εν μέρει, η σημαντική διαφορά στους χρόνους οφείλεται στην ποικιλία των περιφερειακών ενεργειών που εφαρμόζει το Pellet, όπως είναι ο έλεγχος της συνοχής της οντολογίας και των εμπλεκόμενων δηλώσεων. Αντίθετα, η λογική του προσαρμοσμένου λογισμικού είναι επικεντρωμένη αποκλειστικά στην εξαγωγή των αποτελεσμάτων εξουσιοδότησης, δουλεύοντας στην υπόθεση της δεδομένης συνοχής της οντολογίας. Επιπρόσθετα, το προσαρμοσμένο εργαλείο εργάζεται οικονομώντας χρόνο απόκρισης σε ερωτήματα καθώς συμβουλεύεται μια κατάλληλα σχεδιασμένη γνωσιακή βάση, που δημιουργείται σε προκαταρκτικό επίπεδο. Τέλος, οι επιπτώσεις της διεύρυνσης των οντολογιών από άποψη στιγμιότυπων είναι περισσότερο εμφανείς στην περίπτωση του Pellet, το οποίο μάλιστα ολοκληρώνει εσφαλμένα την εκτέλεσή του όταν λειτουργεί στη βάση των δύο ογκωδέστερων οντολογιών (οντολογίες O και P). Η επίδοση του προσαρμοσμένου λογισμικού επηρεάζεται επίσης αλλά με πιο ανεκτό υπολογιστικά τρόπο.

5.2.2 Δυναμική Συλλογιστική

Οι διαδικασίες στατικής συλλογιστικής καταλήγουν στη δημιουργία ενός ολοκληρωμένου συνόλου PDT, συνοδευμένο από συγκεκριμένα στιγμιότυπα συνθηκών και υποχρεώσεων. Οι διαδικασίες δυναμικής συλλογιστικής είναι επιφορτισμένες με τον έλεγχο εκείνων των δυναμικών παραμέτρων που καθορίζουν την ισχύ των συνθηκών που με τη σειρά τους ορίζουν την ισχύ του κανόνα εξουσιοδότησης και την εφαρμογή των κατάλληλων περιορισμών/υποχρεώσεων. Πιο συγκεκριμένα, εξετάζεται η ισχύς των χωρικών και χρονικών συνθηκών, των συνθηκών ασφάλειας και γνωρισμάτων χρηστών, καθώς και η ύπαρξη των αμοιβαία αποκλειόμενων συνδυασμών τύπων δεδομένων και εξουσιοδοτήσεων. Ουσιαστικά, οι συγκεκριμένοι περιορισμοί επιβάλλουν περαιτέρω οριοθετήσεις στο σύνολο των δεδομένων που θα αποκαλυφθούν στις οντότητες που αιτούνται πρόσβασης, εκκινώντας από το σύνολο των δεδομένων που υποδεικνύεται από τα αποτελέσματα της εργασίας του λογισμικού στατικής συλλογιστικής. Στις περιπτώσεις εξακρίβωσης των συνθηκών σε κανόνες μεταφοράς δικαιωμάτων και προώθησης δεδομένων, το

δυναμικό τμήμα της συλλογιστικής διαδικασίας είναι αρμόδιο να εξετάσει επιπρόσθετα την ισχύ των συνθηκών του καταδεικνυόμενου κανόνα ελέγχου πρόσβασης. Έτσι εξασφαλίζεται, ότι οι ενέργειες μεταφοράς δικαιωμάτων και προώθησης δεδομένων δεν θα διεξαχθούν έχοντας ως αντικείμενό τους δικαιώματα και εξουσιοδοτήσεις που δεν υφίστανται κατά τη χρονική στιγμή του ελέγχου.

Σε ότι αφορά την πιθανότητα ύπαρξης πολλαπλών κανόνων εξουσιοδότησης σε μια μονάδα ΚΔΕ για το ίδιο σύνολο $\langle dt_i, pu_j, r_k \rangle$ από διαφορετικές οντότητες του συστήματος (χρήστες, πάροχος και Επικεφαλής της ΣΟΙ), αναγνωρίζονται δύο περιπτώσεις:

1. Πολλαπλές θετικές εξουσιοδοτήσεις, οπότε το δυναμικό τμήμα της συλλογιστικής διαδικασίας είναι υπεύθυνο για τον έλεγχο του συνόλου των καταδεικνυόμενων συνθηκών αλλά και για την εφαρμογή του συνόλου των υποδεικνυόμενων υποχρεώσεων.
2. Αντικρουόμενοι κανόνες (ύπαρξη τόσο θετικής όσο και αρνητικής εξουσιοδότησης), οπότε η μηχανή αποδίδει απόλυτη προτεραιότητα στις προτιμήσεις των υποκείμενων των δεδομένων για τα οποία προέκυψαν οι αντικρουόμενοι κανόνες και έπειτα στις διατάξεις – αν υπάρχουν τέτοιες – του Επικεφαλής της Συνομοσπονδίας Ιδιωτικότητας. Στο ενδεχόμενο που μια οντότητα παρά την απόλυτη προτεραιότητα που της αναγνωρίζεται είναι διατεθειμένη να αποδεχτεί τις προτιμήσεις κάποιας άλλης οντότητας που έχει προδιαγράψει συγγενή κανόνα (ορίζοντας αρνητικά την OWL σημαία *overrideConflictingPreferences*), η δυναμική συλλογιστική αποδίδει αυτόματα προτεραιότητα στους κανόνες της επόμενης κατά σειρά οντότητας. Η ίδια λογική υιοθετείται και στις περιπτώσεις που προκύπτουν αντιφάσεις μεταξύ των συνθέσεων των συνθηκών (που αναφέρονται στο ίδιο υποκείμενο και αντικείμενο) θετικών εξουσιοδοτήσεων.

Σε αυτό το σημείο, πρέπει να τονιστεί ότι η διαδικασία επίλυσης «συγκρούσεων» κατά το δυναμικό μέρος συλλογισμού αποτελεί διαφορετική δραστηριότητα από αυτή που λαμβάνει χώρα κατά το στατικό μέρος συλλογιστικής, καθώς η μεν δεύτερη εργάζεται για την αποσαφήνιση διαφωνιών που προκύπτουν κατά την προδιαγραφή κανόνων από **κάθε μια οντότητα ξεχωριστά**, η δε πρώτη απασχολείται με αντικρουόμενες πολιτικές **μεταξύ διακριτών οντοτήτων**. Ωστόσο, οι συγκεκριμένες δραστηριότητες θα μπορούσαν να λαμβάνουν χώρα στα τελευταία στάδια της στατικής συλλογιστικής (μετά το πέρας των συμπερασματικών διαδικασιών για το

οντολογικό μοντέλο κάθε οντότητας ξεχωριστά), ενέργεια η οποία όμως θα αφαιρούσε την ευελιξία της πλατφόρμας να διαχειρίζεται αποδοτικά πιθανές αλλαγές στις προτιμήσεις μεμονωμένων χρηστών. Πιο συγκεκριμένα, πιθανές τροποποιήσεις στους κανόνες εξουσιοδότησης ενός από το σύνολο των χρηστών μιας μονάδας ΚΔΕ θα συνεπαγόταν την απαίτηση της επανεκτέλεσης της στατικής συλλογιστικής για τα οντολογικά μοντέλα τόσο του χρήστη όσο και του παρόχου κι ως εκ τούτου η μονάδα δεν θα ήταν σε θέση να εξυπηρετήσει αιτήματα για το συγκεκριμένο χρονικό διάστημα, σε ότι αφορά την παραγωγή αποφάσεων εξουσιοδότησης. Αντίθετα, ενσωματώνοντάς τη διαδικασία επίλυσης αντικρουόμενων πολιτικών μεταξύ διαφορετικών οντοτήτων στις δυναμικές ενέργειες συμπερασμών, επιτρέπεται στις μονάδες ΚΔΕ να λειτουργούν αυτόνομα και ανεξάρτητα από τυχόν αλλαγές στους κανόνες των χρηστών.

Σε ότι αφορά, την εξακρίβωση του συνόλου των αμοιβαία αποκλειόμενων συνδυασμών τύπων δεδομένων κατά τη διενέργεια της δυναμικής συλλογιστικής, οι ακόλουθοι κανόνες συλλογιστικής εφαρμόζονται:

$\forall (dt_i, dt_j, exc_k)$,

- $inheritsFrom(dt_i, dt_j) \wedge excludes(exc_{k,}, dt_i) \Longrightarrow excludes(exc_{k,}, dt_j)$
- $isPartOf(dt_i, dt_j) \wedge excludes(exc_{k,}, dt_i) \Longrightarrow excludes(exc_{k,}, dt_j)$

, όπου exc_k ένα στιγμιότυπο της κλάσης *ExclusiveCombinations* και το κατηγόρημα $excludes(exc_{k,}, dt_i)$ η δήλωση της συμμετοχής του dt_i στο στιγμιότυπο exc_k.

Η εξακρίβωση των αμοιβαία αποκλειόμενων συνδυασμών εξουσιοδοτήσεων συνιστά πιο άμεση διαδικασία καθώς οι κανόνες εξουσιοδότησης (στιγμιότυπα της κλάσης *Rules*) δεν διατηρούν σχέσεις κληρονομικότητας μεταξύ τους κι επομένως δεν συνεπάγεται την εφαρμογή εξειδικευμένων κανόνων συλλογιστικής.

5.3 Ψηφιακά Πιστοποιητικά

Προς την αυτοματοποίηση των διαδικασιών λήψης απόφασης και για την κατάλληλη απόδοση των εννοιών και αναπαράσταση των συσχετίσεων που προκύπτουν από τη λειτουργία της πλατφόρμας, επιλέχθηκε η αξιοποίηση ψηφιακών πιστοποιητικών ταυτότητας (public key certificates) και ιδιοτήτων (attribute certificates) συμβατών με τις κατευθυντήριες οδηγίες του προτύπου X.509 [116]. Η επιλογή των ψηφιακών πιστοποιητικών ταυτότητας και ιδιοτήτων πραγματοποιήθηκε στη βάση της μεγαλύτερης επικάλυψης και ολοκλήρωσης με την υποκείμενη υποδομή

εμπιστευτικότητας, η οποία ως μια Υποδομή Δημόσιου Κλειδιού και Διαχείρισης Δικαιωμάτων, όπως έχει ήδη αναλυθεί, εν πολλοίς βασίζει τις λειτουργίες της σε ψηφιακά πιστοποιητικά που εκδίδονται από τις αντίστοιχες Αρχές Πιστοποίησης και Ιδιοτήτων. Τα αξιοποιούμενα ψηφιακά πιστοποιητικά αποτελούν ουσιαστικά δηλώσεις των έμπιστων Κέντρων Διαχείρισης Εξουσιοδοτήσεων που ανήκουν στη Συνομοσπονδία Ομότιμων Ιδιωτικότητας και του Επικεφαλής της Συνομοσπονδίας, ψηφιακά υπογεγραμμένες και δομημένες με τέτοιο τρόπο που να καταδεικνύουν τα χαρακτηριστικά των εκδοτών και των κατόχων τους. Πρέπει να τονιστεί ότι η επιλογή των ψηφιακών πιστοποιητικών δεν είναι απόλυτη και δεσμευτική καθώς θα μπορούσαν να αξιοποιηθούν παρεμφερείς τεχνολογίες για τη μεταφορά πληροφοριών πιστοποίησης και εξουσιοδότησης μεταξύ απομακρυσμένων οντοτήτων όπως είναι το πρότυπο SAML του οργανισμού OASIS, ακόμα και παράλληλα με τη χρήση των ψηφιακών πιστοποιητικών. Ωστόσο, μια τέτοια επιλογή θα είχε ως αποτέλεσμα η πλατφόρμα εξουσιοδοτήσεων να απολέσει το προνόμιο της *οικονομίας των διαδικασιών* που προκύπτει μέσω της σύζευξης των πιστοποιητικών – που σε κάθε περίπτωση κρίνονται αναγκαία για την αποτύπωση των υπαρχόντων σχέσεων εμπιστοσύνης – και των απαιτήσεων αναπαράστασης των λοιπών ιδιοτήτων και καταστάσεων του συστήματος.

Πιο αναλυτικά, κατά τη διάρκεια της λειτουργίας του συστήματος προκύπτει η απαίτηση κατάλληλης απεικόνισης των ακόλουθων καταστάσεων:

- Ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των παρόχων των ΚΔΕ και της οντότητας ΕΣΙ, στη βάση της οποίας ουσιαστικά θεμελιώνεται η Συνομοσπονδία Ομότιμων Ιδιωτικότητας.
- Προσαρμογή του επιπέδου του προαναφερθέντος τύπου εμπιστοσύνης στο επίπεδο της ποιότητας των στρατηγικών πιστοποίησης χρηστών που ενεργοποιούν οι πάροχοι των ΚΔΕ.
- Αντιστοίχιση των σημασιολογικών εννοιών που αξιοποιούνται τοπικά στα ΚΔΕ και των σημασιολογικών εννοιών της οντότητας ΕΣΙ, με στόχο την επίτευξη σημασιολογικής διαλειτουργικότητας.
- Ταυτοποίηση των τελικών χρηστών και καταγραφή των χαρακτηριστικών τους γνωρισμάτων, από τους ΚΔΕ στους οποίους ανήκουν.
- Προδιαγραφή και εφαρμογή θετικής εξουσιοδότησης χρηστών, είτε για πρόσβαση σε δεδομένα, προώθηση δεδομένων και μεταφορά δικαιωμάτων

είτε για εξουσιοδότηση αιτήματος (σύμφωνα με την αρχή των *διαφορετικών στόχων εξουσιοδότησης* του κεφαλαίου 4.1).

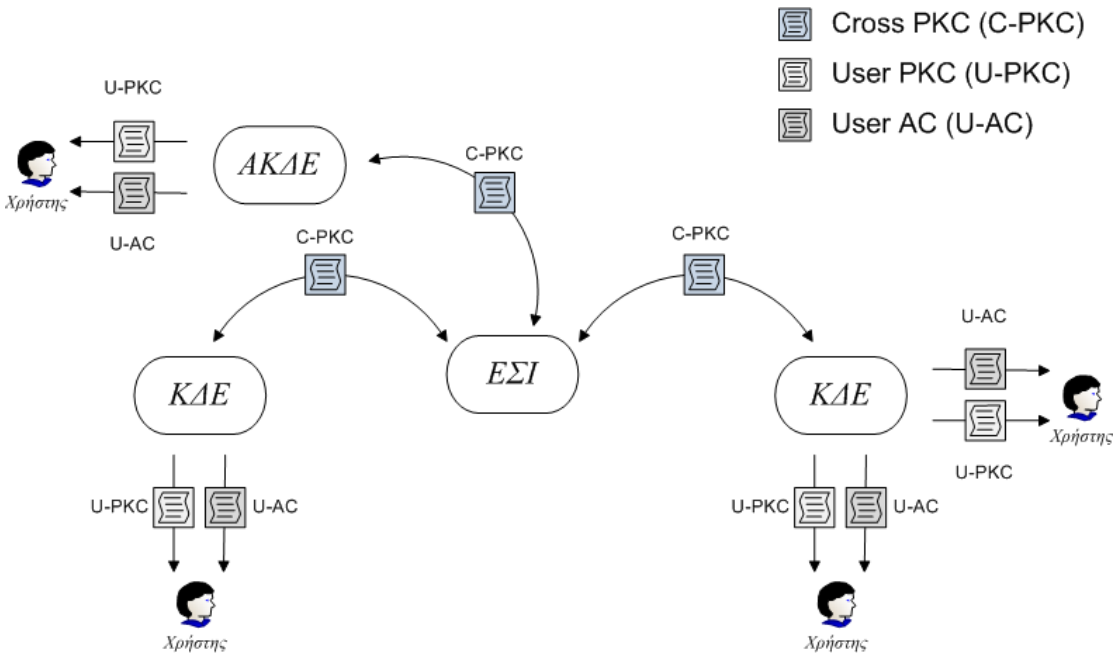
Για την κάλυψη των συγκεκριμένων απαιτήσεων αξιοποιούνται τα ακόλουθα είδη πιστοποιητικών:

- Πιστοποιητικά ταυτότητας X.509v3 μεταξύ Αρχών Πιστοποίησης (Cross Public Key Certificates – C-PKCs) που καταδεικνύουν την ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των παρόχων των ΚΔΕ και της οντότητας ΕΣΙ.
- Πιστοποιητικά ταυτότητας X.509v3 που εκδίδονται από τις Αρχές Πιστοποίησης προς του χρήστες του συστήματος (User Public Key Certificates – U-PKCs) και τα οποία καταγράφουν και επικυρώνουν τα μοναδικά ταυτοποιητικά χαρακτηριστικά του κάθε χρήστη με κυριότερο όλων το προσωπικό δημόσιο κλειδί του κάθε χρήστη.
- Πιστοποιητικά ιδιοτήτων X.509v2 που εκδίδονται από τις Αρχές Πιστοποίησης προς του χρήστες του συστήματος (User Attribute Certificates – U-ACs) και καταγράφουν τα επιπρόσθετα γνωρίσματα του κάθε χρήστη, με κυριότερο όλων τον ρόλο που ενεργοποιεί κατά τη λειτουργία της πλατφόρμας.
- Πιστοποιητικά ιδιοτήτων X.509v2 που εκδίδονται από τις Αρχές Πιστοποίησης του συστήματος (Permitted Data Types Attribute Certificates – PDT-ACs) και καταγράφουν θετικές εξουσιοδοτήσεις χρηστών. Σε αντίθεση με τα παραπάνω πιστοποιητικά (C-PKC, U-PKC και A-PKC) τα PDT-ACs ανήκουν στις Αρχές Πιστοποίησης του συστήματος που τα εκδίδουν (Self-Issued Certificates). Επίσης, τα PDT-ACs δεν αποτελούν τμήμα της υποδομής εμπιστοσύνης και εκδίδονται δυναμικά σε πραγματικό χρόνο κατά τη διάρκεια της λειτουργίας της πλατφόρμας, ενώ χαρακτηρίζονται από **περιορισμένο χρόνο εγκυρότητας για την αποφυγή της επαναχρησιμοποίησής τους**.

Τα Πιστοποιητικά Ταυτότητας (C-PKCs και U-PKCs) υπογράφονται από την Αρχή Πιστοποίησης-εκδότη με χρήση του ιδιωτικού κλειδιού της. Πιο συγκεκριμένα, το πεδίο *signature Algorithm* περιλαμβάνει ένα αναγνωριστικό του κρυπτογραφικού αλγορίθμου που αξιοποιήθηκε για την υπογραφή του πιστοποιητικού, ενώ το πεδίο *signature Value* υποδεικνύει μια ψηφιακή υπογραφή υπολογισμένη στη βάση του χρησιμοποιούμενου ιδιωτικού κλειδιού και του πιστοποιητικού αυτού καθ' αυτού. Επιπλέον, μέσω του πεδίου επέκτασης *Authority Key Identifier* η εκδότρια Αρχή

δημοσιοποιεί το δημόσιο κλειδί της (που αντιστοιχεί στο ιδιωτικό κλειδί της) προς αξιοποίηση από Αρχές Πιστοποίησης-επαληθευτές με στόχο την επιβεβαίωση του γεγονότος της υπογραφής του πιστοποιητικού από την εκδότρια-Αρχή. Πρέπει να σημειωθεί ότι ο συνδυασμός των ενδείξεων των πεδίων *Serial Number* (μοναδικός σειριακός αριθμός πιστοποιητικού) και *Issuer* (μοναδικό αναγνωριστικό της Αρχής-εκδότη) πρέπει να αντιστοιχεί σε μοναδικά πιστοποιητικά εντός της Συνομοσπονδίας. Επιπρόσθετα, το πεδίο *Validity* αναπαριστά το χρονικό διάστημα κατά το οποίο η Αρχή Πιστοποίησης-εκδότης εγγυάται την ισχύ των πληροφοριών που περικλείονται στο πιστοποιητικό. Σε χρονικές στιγμές εκτός του συγκεκριμένου χρονικού διαστήματος τα πιστοποιητικά θα πρέπει να θεωρούνται από τις Αρχές Πιστοποίησης-επαληθευτές άκυρα. Οι κάτοχοι των πιστοποιητικών καταγράφονται μέσω μοναδικών αναγνωριστικών στο πεδίο *Subject*, ενώ το δημόσιο τους κλειδί υποδεικνύεται στο πεδίο *Subject Public Key*. Τέλος, η επέκταση *Subject Directory Attributes* αξιοποιείται στα πιστοποιητικά ταυτοτήτων για να μεταφέρει επιπλέον τιμές γνωρισμάτων των κατόχων των πιστοποιητικών, όπως είναι τιμές LoA για τα πιστοποιητικά C-PKCs και ταυτοποιητικά στοιχεία χρηστών στα πιστοποιητικά U-PKCs (διεύθυνση ηλεκτρονικού ταχυδρομείου, τόπος κατοικίας κ.α.).

Τα Πιστοποιητικά Ιδιοτήτων των χρηστών (U-ACs) αποδίδουν συγκεκριμένες ιδιότητες στους χρήστες-κατόχους των αντίστοιχων U-PKCs. Η σύνδεση των δύο πιστοποιητικών επιτυγχάνεται μέσω της επιλογής *baseCertificateId* του πεδίου *Holder* των U-ACs το οποίο επιλέγεται να αναπαριστά τον σειριακό αριθμό των αντίστοιχων U-PKCs. Επιπρόσθετα, κάθε ζευγάρι συνδεδεμένων U-PKCs – U-ACs διατηρεί κοινές τιμές στα πεδία *Issuer*. Ομοίως με τα πιστοποιητικά ταυτότητας τα πιστοποιητικά ιδιοτήτων υπογράφονται από τις Αρχές Πιστοποίησης-εκδότες, οι οποίες και θέτουν κατάλληλα τιμές στα πεδία *signature Algorithm, signature Value* και *Authority Key Identifier*. Κυρίαρχο στοιχείο στα πιστοποιητικά U-ACs αποτελούν οι ρόλοι και τα λοιπά γνωρίσματα που αποδίδονται από τις Αρχές Ιδιοτήτων των ΚΔΕ και των αντίστοιχων οργανισμών στους χρήστες του συστήματος. Ενδεικτικά, αναφέρονται τα χαρακτηριστικά της συμμετοχής σε συγκεκριμένες υπό-ομάδες του οργανισμού (μέσω της προσαρμοσμένης επέκτασης *Group Membership*) και των χρόνων ενεργοποίησης των Πιστοποιητικών Ιδιοτήτων (μέσω της επέκτασης *Time Specification*). Η Εικόνα 24 αποτυπώνει τη διαμόρφωση της υποδομής εμπιστοσύνης μέσω της ενσωμάτωσης των ψηφιακών Πιστοποιητικών Ταυτότητας και Ιδιοτήτων στις σχέσεις των διακριτών οντοτήτων της πλατφόρμας εξουσιοδοτήσεων.



Εικόνα 24: Ψηφιακά πιστοποιητικά και υποδομή εμπιστοσύνης

Τα Πιστοποιητικά Ιδιοτήτων (PDT-ACs) ακολουθούν σε γενικές γραμμές τη δομή των U-ACs. Ειδικότερα, όμως τα πεδία που περικλείονται στα εν λόγω πιστοποιητικά αφορούν αποκλειστικά έννοιες που σημασιολογικά υποδεικνύουν θετικούς κανόνες πρόσβασης (τύπους δεδομένων, ρόλους και σκοπούς πρόσβασης). Η παραγωγή ενός πιστοποιητικού PDT-AC ισοδυναμεί με την προδιαγραφή ενός θετικού κανόνα πρόσβασης από τις οντότητες του συστήματος. Επιπρόσθετα, αν υπάρχουν κανόνες προώθησης δεδομένων που να επηρεάζουν τους απεικονιζόμενους κανόνες πρόσβασης, αυτοί αντιπροσωπεύονται σε επιπλέον πεδία των πιστοποιητικών μέσω της καταγραφής των εννοιολογικών τους συστατικών. Σε περίπτωση που ένα πιστοποιητικό PDT-AC αποτελεί προϊόν προδιαγραφής κανόνα μεταφοράς δικαιωμάτων, το πιστοποιητικό υποδεικνύει επιπρόσθετα και τα συστατικά του κανόνα-αντικειμένου της μεταφοράς δικαιωμάτων. Ακόμα, στην περίπτωση που ο κανόνας εξουσιοδότησης αφορά εξουσιοδότηση αιτήματος (δηλαδή έχει τεθεί η ιδιότητα-σημαία OWL *refersToOutgoingRequest*) το παραγόμενο PDT-AC αξιοποιείται από την πλατφόρμα για τη μεταφορά από τον πάροχο ταυτοτήτων στον πάροχο υπηρεσίας της απαραίτητης πληροφορίας που συγκεκριμενοποιεί το αίτημα. Επομένως, τα PDT-ACs που προέρχονται από εξουσιοδοτήσεις αιτημάτων προσφέρουν το κατάλληλο έδαφος για την αποτύπωση των σημασιολογικών ισοδυναμιών των στιγμιότυπων της οντολογίας του κάθε ΚΔΕ με τα στιγμιότυπα της

οντότητας ΕΣΙ μέσω του πεδίου επέκτασης *Attribute Mappings*. Με αυτόν τον τρόπο, οι δύο απομακρυσμένοι κόμβοι ΚΔΕ επιτυγχάνουν τον στόχο της σημασιολογικής διαλειτουργικότητας κατά την επικοινωνία τους. Στην περίπτωση που ο αναπαριστάμενος κανόνας αφορά εξουσιοδότηση για πρόσβαση σε δεδομένα, το προκύπτον πιστοποιητικό εμπεριέχει και τη ζητηθείσα πληροφορία, όπου αυτό είναι εφικτό, σε συγκεκριμένο πεδίο επέκτασης με τίτλο *DataValue*.

Για τη δημιουργία των χρησιμοποιούμενων κρυπτογραφικών κλειδιών (δημοσίων και ιδιωτικών) αξιοποιήθηκε ο αλγόριθμος RSA με μήκος κλειδιού 2048 bits, ενώ για την ψηφιακή υπογραφή των πιστοποιητικών έγινε χρήση του αλγορίθμου παραγωγής σύνοψης Secure Hash Algorithm (SHA), με μήκος σύνοψης 512 bits.

6 Πρωτόκολλο Εξουσιοδότησης

Αντικείμενο του παρόντος κεφαλαίου είναι η παρουσίαση των ενορχηστρωμένων διαδικασιών που ενεργοποιούνται στο πλαίσιο της λειτουργίας της πλατφόρμας και οι οποίες διαμορφώνουν το προτεινόμενο πρωτόκολλο επικοινωνίας μεταξύ των διακριτών οντοτήτων της Συνομοσπονδίας. Με στόχο την προσφορά μεγαλύτερου ελέγχου στους χρήστες του συστήματος αλλά και τη μεγαλύτερη κλιμακοθετησιμότητα κατά τη διευθέτηση αιτημάτων, υιοθετήθηκε μια προσέγγιση των πρωτοκόλλων εξουσιοδότησης που τοποθετεί στο επίκεντρο των διαδικασιών τους χρήστες: ο χρήστης στο πλαίσιο μιας αίτησης για δεδομένα συγκεντρώνει τα απαραίτητα ταυτοποιητικά στοιχεία από τους προτιμώμενους οργανισμούς που αξιοποιεί ως Παρόχους Ταυτότητας και τα παρουσιάζει στον Πάροχο Υπηρεσίας που φιλοξενεί τα ζητηθέντα δεδομένα, προς αξιολόγηση. Επίσης, η επιλογή αυτή επιτρέπει στους Παρόχους Ταυτότητας να διαμορφώνουν και να εφαρμόζουν κανόνες εξουσιοδότησης στην περίπτωση που οι ίδιες οι αιτήσεις των χρηστών αφορούν ενέργειες που υπόκεινται έλεγχο εξουσιοδότησης. Το κεφάλαιο διαρθρώνεται ακολουθώντας τις διακριτές φάσεις του πρωτοκόλλου εξουσιοδότησης εκκινώντας από την απαραίτητη φάση διαμόρφωσης (configuration) της υποδομής.

6.1 Ενέργειες Διαμόρφωσης Υποδομής

Οι ενέργειες διαμόρφωσης του συστήματος, τυπικά δεν ανήκουν στο πρωτόκολλο εξουσιοδότησης, ωστόσο για λόγους πληρότητας περιγράφονται ως πρώτο βήμα που διεξάγεται άπαξ πριν την εκκίνηση της λειτουργίας της πλατφόρμας, Αναλυτικά, κατά τη διάρκεια της φάσης διαμόρφωσης διεξάγονται οι ακόλουθες δραστηριότητες:

- Συγκεκριμενοποίηση Οντολογίας Εξουσιοδοτήσεων (ontology instantiation), διαδικασία κατά την οποία ορίζονται όλα τα στιγμιότυπα της Οντολογίας Εξουσιοδοτήσεων στις μονάδες ΚΔΕ και ΕΣΙ. Πιο συγκεκριμένα, κάθε μονάδα ΚΔΕ καθώς και η οντότητα ΕΣΙ διατηρούν ατομικά αντίτυπα της Οντολογίας Εξουσιοδοτήσεων, την οποία ενεργοποιούν κατά βούληση για την προδιαγραφή κανόνων εξουσιοδότησης. Το σύνολο των στιγμιότυπων που ορίζονται στην οντότητα ΕΣΙ και αφορούν τις οντολογικές κλάσεις *Data*, *Purposes*, *Roles*, *Conditions* και *Obligations* αφενός αξιοποιούνται για την προδιαγραφή των κοινά αποδεκτών κανόνων εξουσιοδότησης εντός της

Συνομοσπονδίας, αφετέρου αποτελούν σημεία σημασιολογικών αναφορών για τα στιγμιότυπα των τοπικών οντολογιών στις ΚΔΕ. Ο πάροχος κάθε ΚΔΕ είναι υπεύθυνος για τη συγκεκριμενοποίηση του τοπικού αντίγραφου της Οντολογίας Εξουσιοδοτήσεων καθώς και για την παραγωγή σημασιολογικών ισοδυναμιών με τα στιγμιότυπα που ορίζονται στον Επικεφαλής τα οποία σε πραγματικό χρόνο αποτυπώνει στα παραγόμενα PDT-AC πιστοποιητικά. Στην περίπτωση του Ανεξάρτητου Κέντρου Διαχείρισης Εξουσιοδοτήσεων υιοθετούνται επακριβώς τα στιγμιότυπα της μονάδας ΕΣΙ.

- Παραγωγή Πιστοποιητικών Ταυτότητας και Ιδιοτήτων του πλαισίου εμπιστοσύνης της Συνομοσπονδίας, ήτοι των πιστοποιητικών U-PKC, U-AC και C-PKC, τα οποία αποδίδουν συγκεκριμένα ταυτοποιητικά στοιχεία και χαρακτηριστικά γνωρίσματα στους χρήστες του συστήματος και διακριτά επίπεδα εμπιστοσύνης στις μονάδες ΚΔΕ από τον Επικεφαλής της πλατφόρμας αντίστοιχα. Εμμέσως, η προκειμένη διαδικασία συνεπάγεται ότι οι πάροχοι κάθε ΚΔΕ ενεργοποιούν συγκεκριμένες γνωστές πολιτικές πιστοποίησης για την αναγνώριση και επικύρωση των γνωρισμάτων των χρηστών τους, για την ποιότητα των οποίων κρίνονται με διακριτά επίπεδα εμπιστοσύνης από την οντότητα ΕΣΙ.
- Προδιαγραφή κανόνων εξουσιοδότησης, από όλες της οντότητες της Συνομοσπονδίας στη βάση των στιγμιότυπων των τοπικών αντιγράφων της Οντολογίας Εξουσιοδοτήσεων, μέσω της παραγωγής αντικειμένων της κλάσης *Rules*. Οι πάροχοι υποχρεούνται να ορίσουν τόσο εξουσιοδοτήσεις που αφορούν δικαιώματα και δεδομένα όσο και κανόνες εξουσιοδότησης για εξερχόμενα αιτήματα των χρηστών τους, καθώς όπως αναλύθηκε στο προηγούμενο κεφάλαιο και σύμφωνα με την Υπόθεση Κλειστού Κόσμου απουσία αντικειμένου PDT για οποιοδήποτε αίτημα ισοδυναμεί με την προδιαγραφή αρνητικού κανόνα εξουσιοδότησης. Μετά το πέρας των ενεργειών ορισμού κανόνων εξουσιοδότησης, διεξάγονται οι διαδικασίες της στατικής συλλογιστικής για την παραγωγή των τελικών ισχυόντων θετικών εξουσιοδοτήσεων ανά χρήστη και πάροχο του συστήματος αλλά και για την οντότητα ΕΣΙ.
- Αρχική εισαγωγή δεδομένων στα κατάλληλα αποθετήρια των ΚΔΕ από τους παρόχους και τους χρήστες του συστήματος, όπου αυτό είναι επιθυμητό και

με στόχο τη βελτίωση της απόδοσης των διαδικασιών που διεξάγονται σε πραγματικό χρόνο. Σε κάθε περίπτωση, κατά τη διάρκεια της λειτουργίας της πλατφόρμας, προκύπτει η απαίτηση από τις εμπλεκόμενες οντότητες να τροφοδοτήσουν με δεδομένα τα αποθετήρια των ΚΔΕ.

6.2 Λειτουργία Πρωτοκόλλου Εξουσιοδότησης

Ακολουθώντας τη φάση διαμόρφωσης που πραγματοποιείται πριν την εκκίνηση του συστήματος, η πλατφόρμα είναι έτοιμη να ικανοποιήσει αιτήματα χρηστών για πρόσβαση σε δεδομένα εντός της Συνομοσπονδίας. Σημειώνεται ότι, στην πλευρά κάθε Κέντρου Διαχείρισης Εξουσιοδοτήσεων είναι δυνατόν να καταχωρηθούν δύο τύποι αιτημάτων:

1. εξουσιοδότησης για αίτημα για πρόσβαση σε δεδομένα κάποιου παρόχου υπηρεσίας, οπότε η μονάδα ΚΔΕ που λαμβάνει το αίτημα συμπεριφέρεται ως πάροχος ταυτότητας.
2. εξουσιοδότησης για πρόσβαση σε δεδομένα, οπότε η μονάδα ΚΔΕ που λαμβάνει το αίτημα συμπεριφέρεται ως πάροχος υπηρεσίας.

Πιο λεπτομερώς, η εξυπηρέτηση των αιτημάτων και η λήψη σαφών αποφάσεων διαχείρισης εξουσιοδοτήσεων περιλαμβάνουν τις διακριτές κατηγορίες αλληλεπιδράσεων: Χρήστης – ΚΔΕ παρόχου ταυτοτήτων, χρήστης – ΚΔΕ παρόχου υπηρεσίας και ΚΔΕ παρόχου υπηρεσίας – ΚΔΕ παρόχου ταυτοτήτων.

6.2.1 Χρήστης – ΚΔΕ Παρόχου Ταυτοτήτων

Το πρώτο βήμα του πρωτοκόλλου εξουσιοδότησης αναφέρεται στην **αυθεντικοποίηση** του χρήστη στο Κέντρο Διαχείρισης Εξουσιοδοτήσεων στον οποίο υπάγεται και στην **εξουσιοδότησή** του να προχωρήσει με το αίτημά του στην πλευρά κάποιου παρόχου υπηρεσιών. Ως εκ τούτου, ο χρήστης υποχρεούται να καταθέσει τα προσωπικά του πιστοποιητικά ταυτότητας και ιδιοτήτων και να συγκεκριμενοποιήσει τα δεδομένα για τα οποία πρόκειται να αιτηθεί πρόσβασης στη μονάδα ΚΔΕ στην οποία ανήκει, πριν την υποβολή του πραγματικού αιτήματος στην πλευρά του παρόχου υπηρεσίας. Στην περίπτωση επιτυχούς πιστοποίησης του χρήστη, δηλαδή στην περίπτωση που ο ΚΔΕ είναι σε θέση να επιβεβαιώσει την ισχύ των κατατιθέμενων πιστοποιητικών, η διαδικασία προχωρά στη φάση της αναζήτησης των κατάλληλων στιγμιότυπων PDT που αντιστοιχούν στο αίτημα. Η αναζήτηση

πραγματοποιείται στο υποσύνολο των παραγόμενων από τις δραστηριότητες στατικής συλλογιστικής θετικών εξουσιοδοτήσεων του παρόχου της μονάδας ΚΔΕ που αναφέρονται σε εξερχόμενα αιτήματα (δηλαδή η ιδιότητα OWL *refersToOutgoingRequest* παίρνει τιμή *true*). Σε περίπτωση **αποτυχίας εύρεσης** κατάλληλων αντικειμένων PDT, η διαδικασία διακόπτεται και η αίτηση του χρήστη **δεν εξουσιοδοτείται**. Στην αντίθετη περίπτωση, το δυναμικό μέρος των δράσεων συλλογιστικής αναλαμβάνει να επικυρώσει την ισχύ των υποδεικνυόμενων συνθηκών, να εφαρμόσει τις απορρέουσες υποχρεώσεις, να κατασκευάσει τα κατάλληλα PDT-AC πιστοποιητικά που κωδικοποιούν την εξουσιοδότηση και εντέλει να τα παραδώσει στον χρήστη. Τα PDT-ACs θα συνοδεύσουν το επικείμενο αίτημα του χρήστη στην πλευρά του παρόχου υπηρεσίας. Σε περίπτωση εμπλοκής του Ανεξάρτητου Κέντρου Διαχείρισης Εξουσιοδοτήσεων, προφανώς δεν προκύπτει θέμα εξουσιοδότησης, οπότε μετά την αυθεντικοποίηση του χρήστη, παράγονται αυτόματα τα απαραίτητα PDT-ACs.

Το πρώτο βήμα του πρωτοκόλλου επιτρέπει αφενός στους παρόχους να εξουσιοδοτούν τις ενέργειες των υπαγόμενων χρηστών τους, αφετέρου διευκολύνει τους τελευταίους να προστατέψουν τα ταυτοποιητικά τους γνωρίσματα από μια περιττή έκθεση σε απομακρυσμένες οντότητες. Προς τούτο, τα παραγόμενα πιστοποιητικά ιδιοτήτων PDT-AC εμπεριέχουν αποκλειστικά στοιχεία που ταυτοποιούν το αίτημα του χρήστη, ήτοι τους τύπους των δεδομένων-αντικείμενα της αίτησης, τον εξυπηρετούμενο σκοπό πρόσβασης και τον ενεργοποιημένο ρόλο του χρήστη, και όχι τον ίδιο τον χρήστη, υπό τη έννοια των χαρακτηριστικών του γνωρισμάτων. Πράγματι, από τη σκοπιά του παρόχου υπηρεσίας η πλήρης αναγνώριση του χρήστη που αιτείται πρόσβασης είναι δυνατόν να είναι περιττή για τη θετική εξουσιοδότησή του κι επομένως να έρχεται σε αντίθεση με την «**Αρχή του περιορισμού της χρήσης».** Ταυτόχρονα με τα πιστοποιητικά PDT-AC, το ΚΔΕ προωθεί και το αντίστοιχο C-PKC στον αιτούντα για μελλοντική αξιοποίηση. Τέλος, αξίζει να σημειωθεί ότι είναι δυνατόν να προκύψει **εξουσιοδότηση μέσω μεταφοράς των σχετικών δικαιωμάτων**, οπότε τα εμπλεκόμενα PDT-AC καταγράφουν επιπλέον τα στοιχεία του αντίστοιχου κανόνα εξουσιοδότησης που προκάλεσε τη μεταφορά.

6.2.2 Χρήστης – ΚΔΕ Παρόχου Υπηρεσίας

Μετά τη λήψη των απαραίτητων πιστοποιητικών PDT-AC ο χρήστης είναι σε θέση να καταθέσει το αίτημα του για πρόσβαση σε δεδομένα στην πλευρά του Κέντρου Διαχείρισης Εξουσιοδοτήσεων του παρόχου υπηρεσίας. Εν προκειμένω, ο χρήστης καταθέτει το αίτημα του υποδεικνύοντας τα επιθυμητά δεδομένα και αποδεικνύοντας μέσω των πιστοποιητικών PDT-AC και C-PKC ότι: α) έχει ήδη ταυτοποιηθεί εντός της Συνομοσπονδίας στην πλευρά του παρόχου ταυτοτήτων, β) έχει εξουσιοδοτηθεί για αυτή του την ενέργεια, γ) εξυπηρετεί συγκεκριμένο σκοπό πρόσβασης και ενεργοποιεί τον κατάλληλο ρόλο και δ) έχουν καταγραφεί οι απαραίτητες σημασιολογικές ισοδυναμίες για την επίτευξη διαλειτουργικότητας.

Για την εξακρίβωση της εγκυρότητας των παραδοθέντων πιστοποιητικών, απαιτείται το ΚΔΕ στην πλευρά του παρόχου υπηρεσίας να ελέγξει αφενός ότι ο χρόνος του αιτήματος εμπίπτει στο χρονικό διάστημα ισχύος των πιστοποιητικών, αφετέρου να επικυρώσει ότι ο πάροχος ταυτοτήτων αποτελεί πράγματι έγκυρο εταίρο της Συνομοσπονδίας μέσω εξακρίβωσης της ισχύος του C-PKC (η εγκυρότητα του οποίου εξασφαλίζει και την εγκυρότητα των PDT-ACs). Προς τούτο και σε περίπτωση που δεν προκύπτουν αποκλίσεις από τα υποδεικνυόμενα χρονικά όρια ισχύος των πιστοποιητικών, το ΚΔΕ του παρόχου υπηρεσίας επικοινωνεί με την οντότητα ΕΣΙ καταθέτοντας ερώτημα επιβεβαίωσης του πιστοποιητικού C-PKC μέσω του σειριακού του αριθμού και του δημόσιου κλειδιού του. Παράλληλα, ενημερώνεται για πιθανή ύπαρξη στους κοινούς κανόνες εξουσιοδοτήσεων που προδιαγράφηκαν πριν την εκκίνηση του συστήματος, γνωμάτευσης που να **απαγορεύει** το αίτημα του χρήστη. Σε περίπτωση που όλοι οι παραπάνω έλεγχοι έχουν θετική κατάληξη, το ΚΔΕ του παρόχου υπηρεσίας είναι σε θέση να ελέγξει την ύπαρξη τοπικών αντικειμένων PDT που να εξουσιοδοτούν την αιτηθείσα πρόσβαση. Η αναζήτηση πραγματοποιείται στο υποσύνολο των παραγόμενων από τις δραστηριότητες στατικής συλλογιστικής θετικών εξουσιοδοτήσεων του παρόχου που αναφέρονται σε εισερχόμενα αιτήματα (δηλαδή στους κανόνες όπου η ιδιότητα OWL *refersToOutgoingRequest* παίρνει τιμή *false*) αλλά και των θετικών εξουσιοδοτήσεων των χρηστών της μονάδας ΚΔΕ, καθώς είναι δυνατόν το αίτημά υπό διερεύνηση να αφορά προσωπικά τους δεδομένα. Σε περίπτωση **αποτυχίας εύρεσης** κατάλληλων αντικειμένων PDT, η διαδικασία διακόπτεται και η αίτηση του χρήστη **δεν εξουσιοδοτείται**. Στην αντίθετη περίπτωση, το δυναμικό μέρος των δράσεων

συλλογιστικής αναλαμβάνει να προχωρήσει στην κατάλληλη επίλυση συγκρούσεων μεταξύ πιθανών αντικρουόμενων πολιτικών του παρόχου και των χρηστών, να επικυρώσει την ισχύ των υποδεικνυόμενων συνθηκών, να εφαρμόσει τις απορρέουσες υποχρεώσεις και να κατασκευάσει τα κατάλληλα PDT-AC πιστοποιητικά που κωδικοποιούν την εξουσιοδότηση. Τελικά, προωθούνται στο ΚΔΕ του παρόχου ταυτοτήτων του αιτούντα χρήστη τα δημιουργηθέντα PDT-AC, από όπου ο τελευταίος ενημερώνεται σχετικά με τα ζητηθέντα δεδομένα, ενώ του υποδεικνύονται συγκεκριμένοι τρόποι αξιοποίησής τους και περαιτέρω μετάδοσής τους. Φυσικά, στην περίπτωση που τα ζητηθέντα δεδομένα δεν είναι δυνατό να κωδικοποιηθούν κατάλληλα για μεταφορά εντός ψηφιακών πιστοποιητικών (π.χ. αρχεία εγγράφων), δημιουργούνται τα κατάλληλα ασφαλή κανάλια για τη μεταφορά δεδομένων μεταξύ των δύο ΚΔΕ. Για την αναγνώριση των διεπαφών στις οποίες το ΚΔΕ παρόχου ταυτοτήτων πρέπει να προωθήσει τα αποκαλυφθέντα δεδομένα, αξιοποιείται ένα επιπλέον πεδίο του τελικού PDT-AC, που υποδεικνύει το μοναδικό σειριακό αριθμό του κατατιθεμένου πιστοποιητικού PDT-AC του χρήστη που εκκίνησε το πρωτόκολλο. Ο συγκεκριμένος αριθμός στην πλευρά του ΚΔΕ του παρόχου ταυτοτήτων ουσιαστικά αποτελεί ένα μοναδικό αναγνωριστικό για τις συναλλαγές των χρηστών που εξυπηρετεί.

Τυπικά, ένας πάροχος υπηρεσιών αξιώνει την αποκάλυψη επιπλέον χαρακτηριστικών γνωρισμάτων του αιτούντα, πέραν του σκοπού πρόσβασης που εξυπηρετεί και του ρόλου που ενεργοποιεί, προτού να προβεί σε εξουσιοδότηση του αιτήματός του. Η εν λόγω συνθήκη, καταγράφεται στο τοπικό αντίγραφο της Οντολογίας Εξουσιοδοτήσεων, μέσω της προδιαγραφής κανόνων που ενσωματώνουν αντικείμενα της υποκλάσης *Attribute* της κλάσης *Conditions*. Σε αυτή την περίπτωση, λαμβάνουν χώρα επαναληπτικοί γύροι επικοινωνίας μεταξύ του ΚΔΕ του παρόχου υπηρεσίας και της ΚΔΕ του παρόχου ταυτοτήτων του χρήστη.

6.2.3 ΚΔΕ Παρόχου Υπηρεσίας – ΚΔΕ Παρόχου Ταυτοτήτων

Το παρόν βήμα του πρωτοκόλλου επικοινωνίας διεξάγεται αποκλειστικά και μόνο στην περίπτωση που ο πάροχος υπηρεσίας απαιτεί την αποκάλυψη περισσοτέρων στοιχείων σχετικά με τον αιτούντα ή τον πάροχο ταυτοτήτων πριν εξουσιοδοτήσει οριστικά την πρόσβαση στα δεδομένα του. Σε αυτό το πλαίσιο, το ΚΔΕ του παρόχου υπηρεσίας καταθέτει στον ΚΔΕ του παρόχου ταυτοτήτων αίτημα για πρόσβαση στα

επιπλέον δεδομένα που χρειάζεται, προωθώντας παράλληλα το C-PKC του καθώς κι ένα PDT-AC με στόχο την απόδειξη στον δεύτερο, ότι το αίτημα για επιπλέον πληροφορίες πραγματοποιείται στα πλαίσια ενός έγκυρου αιτήματος χρήστη. Προς τούτο το PDT-AC που προωθείται περιέχει τόσο τα βασικά στοιχεία του αιτήματος (τύπος δεδομένων, σκοπός πρόσβασης και ρόλος) όσο και ένα επιπλέον πεδίο που υποδεικνύει το μοναδικό σειριακό αριθμό του κατατιθεμένου πιστοποιητικού PDT-AC του χρήστη. Από αυτό το σημείο και έπειτα η επιχειρηματική λογική στην πλευρά του παρόχου ταυτοτήτων δε διαφέρει σε τίποτα από αυτή της διαχείρισης του αιτήματος για πρόσβαση σε δεδομένα από τον χρήστη κατά το προηγούμενο βήμα στην πλευρά του παρόχου υπηρεσίας. Έτσι, αφού το ΚΔΕ του παρόχου ταυτοτήτων επιβεβαιώσει την εγκυρότητα των PDT-AC και C-PKC σε ότι αφορά τα χρονικά διαστήματα ισχύος τους και αναγνωρίσει το σειριακό αριθμό του αρχικού PDT-AC που ο ίδιος εξέδωσε για να εκκινήσει το πρωτόκολλο, διεκπεραιώνει τις εξής ενέργειες: α) επικοινωνεί με την οντότητα ΕΣΙ για να διαβεβαιώσει τη συμμετοχή του «συνομιλούντος» ΚΔΕ στη Συνομοσπονδία Εξουσιοδοτήσεων, β) ελέγχει την ύπαρξη γνωμάτευσης από τον ΕΣΙ που να **απαγορεύει** το αίτημα του ΚΔΕ, γ) ελέγχει την ύπαρξη τοπικών αντικειμένων PDT που να εξουσιοδοτούν την αιτηθείσα πρόσβαση, με την αναζήτηση να πραγματοποιείται στις θετικές εξουσιοδοτήσεις του παρόχου που αναφέρονται σε εισερχόμενα αιτήματα (δηλαδή η ιδιότητα OWL *refersToOutgoingRequest* παίρνει τιμή *false*) αλλά και στις θετικές εξουσιοδοτήσεις των χρήστη που εκκίνησε το πρωτόκολλο, δ) εφαρμόζει την απαραίτητη επίλυση συγκρούσεων μεταξύ πιθανών αντικρουόμενων πολιτικών του παρόχου και των χρηστών, ε) επικυρώνει την ισχύ των υποδεικνυόμενων συνθηκών, στ) εφαρμόζει τις απορρέουσες υποχρεώσεις και τέλος ζ) κατασκευάζει τα κατάλληλα PDT-AC πιστοποιητικά που κωδικοποιούν την εξουσιοδότηση. Το τελικό PDT-AC προωθείται στην πλευρά του ΚΔΕ του παρόχου υπηρεσίας, μέσω του οποίου αποκαλύπτονται τα ζητηθέντα δεδομένα, ενώ του υποδεικνύονται συγκεκριμένοι τρόποι αξιοποίησής τους και περαιτέρω μετάδοσής τους. Φυσικά, στην περίπτωση που ο πάροχος ταυτοτήτων αξιώσει την αποκάλυψη επιπλέον στοιχείων σχετικά με τον πάροχο υπηρεσίας, το εν λόγω βήμα επαναλαμβάνεται μέχρις ότου όλοι οι εμπλεκόμενοι ικανοποιήσουν τις συνθήκες εφαρμογής των προδιαγραφθέντων θετικών εξουσιοδοτήσεών τους.

6.2.4 Κωδικοποίηση μηνυμάτων

Οι προαναφερθείσες κατηγορίες αλληλεπιδράσεων μεταξύ των οντοτήτων του συστήματος διαμορφώνονται ως μηνύματα ελέγχου που παράγονται και κωδικοποιούνται στη βάση του προτύπου JavaScript Object Notation (JSON) (117), ενσωματώνονται σε μηνύματα της μεθόδου POST του πρωτοκόλλου Hypertext Transfer Protocol (HTTP) (118) και μεταφέρονται σε ασφαλή κανάλια επικοινωνίας που προστατεύονται με χρήση του πρωτοκόλλου Hypertext Transfer Protocol Secure (HTTPS) (119). Ο τύπος κάθε μηνύματος υποδηλώνεται από την παρουσία συγκεκριμένων ζευγαριών JSON πεδίων και τιμών, ενώ όπου είναι απαραίτητο εσωκλείονται τα κατάλληλα ψηφιακά πιστοποιητικά ταυτότητας και ιδιοτήτων με την αξιοποίηση του προτύπου του IETF, Privacy Enhanced Mail (PEM) (120). Τέλος, προς σηματοδότηση της κατάστασης της διαδικασίας επεξεργασίας των μηνυμάτων, αξιοποιούνται οι κωδικοί κατάστασης απάντησης (response status codes) του πρωτοκόλλου HTTP: μια επιτυχημένη αλληλεπίδραση μεταξύ των οντοτήτων της Συνομοσπονδίας ισοδυναμεί με την παραγωγή ενός μηνύματος με κωδικό «*200 OK*» και «*202 Accepted*», μια ανεπιτυχής επιβεβαίωση της εγκυρότητας των εμπλεκόμενων πιστοποιητικών ή μια μη εξουσιοδοτημένη αίτηση πυροδοτεί ένα μήνυμα «*403 Forbidden*» και η αναγνώριση μη έγκυρου περιεχομένου στα εμπλεκόμενα μηνύματα ή άλλα παρεμφερή σφάλματα παράγουν μηνύματα με κωδικό κατάστασης «*500 Internal Server Error*». Πιο λεπτομερώς, τα διακριτά βήματα του πρωτοκόλλου κωδικοποιούνται με τα ακόλουθα JSON μηνύματα:

- requestACs([requestedDataType], [U-PKC], [U-AC]): Κατατίθεται από τον χρήστη στο ΚΔΕ του παρόχου ταυτοτήτων και εκκινεί το πρωτόκολλο εξουσιοδότησης. Τα πεδία [U-PKC] και [U-AC] φιλοξενούν τα αντίστοιχα πιστοποιητικά του χρήστη, ενώ το πεδίο [requestedDataType] υποδεικνύει τον τύπο των δεδομένων για τα οποία αιτείται πρόσβασης ο χρήστης. Σε περίπτωση διαδοχικών αιτημάτων, κι εφόσον ο χρήστης δεν αποσυνδεθεί από το ΚΔΕ, το μήνυμα μπορεί να παραλείψει την ενσωμάτωση των προσωπικών πιστοποιητικών του χρήστη που έχουν μεταφερθεί κατά την πρώτη εκτέλεση του μηνύματος.
- requestData([requestedData], [PDT-ACs]): Κατατίθεται από τον χρήστη στην ΚΔΕ του παρόχου υπηρεσίας και αναπαριστά το αίτημα του χρήστη για πρόσβαση σε δεδομένα του παρόχου. Το πεδίο [PDT-ACs] φιλοξενεί τα

αντίστοιχα πιστοποιητικά που έλαβε ο χρήστης μέσω ενός μηνύματος requestACs, ενώ το πεδίο [requestedData] υποδεικνύει τα δεδομένα για τα οποία αιτείται πρόσβασης ο χρήστης. Ο ίδιος τύπος μηνύματος αξιοποιείται για την αλληλεπίδραση μεταξύ παρόχων ταυτοτήτων και ιδιοτήτων.

- verifyPeer([publicKey], [serialNumber], [PDT-ACs]): Κατατίθεται από τις ΚΔΕ στην οντότητα ΕΣΙ και κωδικοποιεί την αναζήτηση πιθανών αρνητικών γνωματεύσεων της μονάδας σε σχέση με το υποκείμενο αίτημα, όπως μεταφράζεται από το πιστοποιητικό του πεδίου [PDT-ACs], καθώς και την απαίτηση της εξακρίβωσης της εγκυρότητας του πιστοποιητικού C-PKC που αντιστοιχεί στα πεδία [publicKey] και [serialNumber]. Για τη δεύτερη λειτουργικότητα η μονάδα ΕΣΙ εργάζεται ουσιαστικά ως ένας Online Certificate Status Protocol (OCSP) [121] εξυπηρετητής.

7 Ανάπτυξη Πλατφόρμας Εξουσιοδοτήσεων

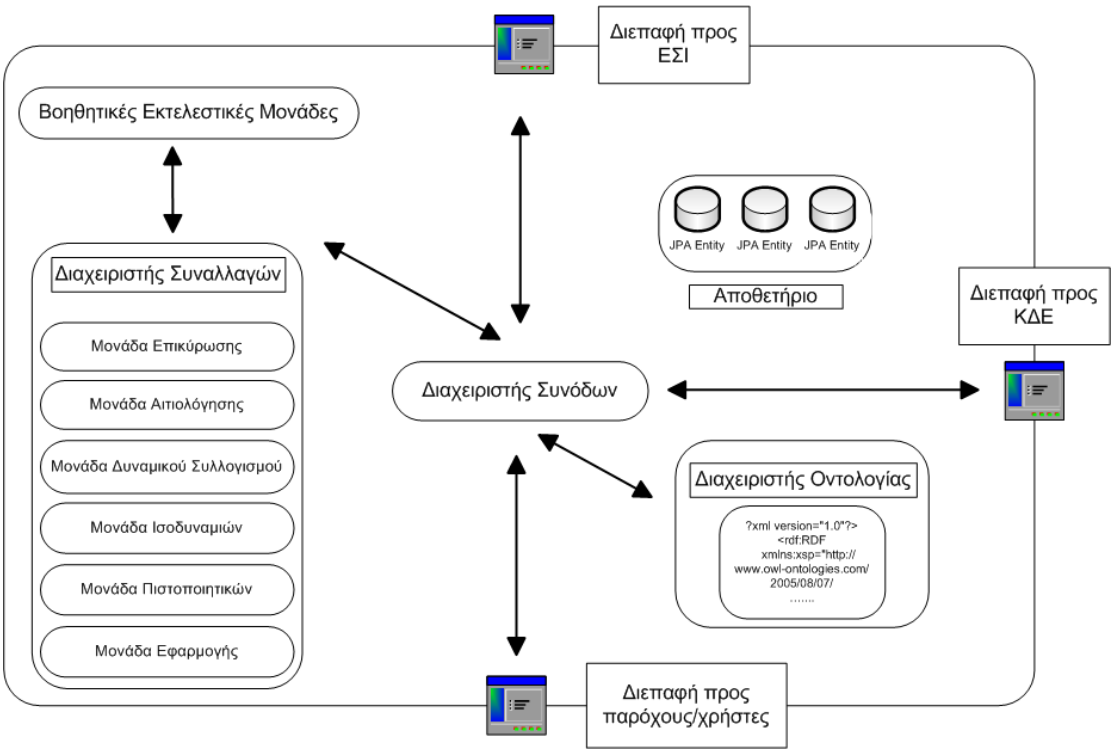
Το παρόν κεφάλαιο παρουσιάζει τις ενέργειες ανάπτυξης των διακριτών μονάδων της πλατφόρμας για την κατάλληλη ενσωμάτωση των λειτουργιών που παρουσιάστηκαν στα προηγούμενα κεφάλαια σε ένα ολοκληρωμένο σύστημα διαχείρισης εξουσιοδοτήσεων. Όπως έχει αναλυθεί, το σύνολο των λειτουργικοτήτων του συστήματος εντοπίζεται σε δύο θεμελιώδεις μονάδες επεξεργασίας, το Κέντρο Διαχείρισης Εξουσιοδοτήσεων και τον Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας.

7.1 Κέντρο Διαχείρισης Εξουσιοδοτήσεων

Όπως έχει αναλυθεί, οι μονάδες των Κέντρων Διαχείρισης Εξουσιοδοτήσεων αποτελούν τους προσωπικούς πράκτορες προστασίας των παρόχων και των χρηστών που συμμετέχουν στη Συνομοσπονδία, δρώντας ως μεσολαβητές μεταξύ των πόρων υπό προστασία και των πιθανών καταναλωτών πόρων. Σε αυτό το πλαίσιο και προς ικανοποίηση των λειτουργικών τους καθηκόντων (Ενότητα 4.2) τα ΚΔΕ χαρακτηρίζονται από μια εσωτερική δομή (Εικόνα 25) που συναπαρτίζεται από τις ακόλουθες λειτουργικές μονάδες:

- Διαχειριστής Συνόδων, που ενεργοποιείται για τη διαχείριση των διακριτών συνόδων (sessions) του ΚΔΕ, του συνόλου των ενεργοποιημένων Διαχειριστών Συναλλαγών και των αλληλεπιδράσεων του ΚΔΕ με τις λοιπές οντότητες του συστήματος.
- Διαχειριστής Συναλλαγών, που συνιστούν τον πυρήνα της επιχειρηματικής λογικής των ΚΔΕ και ενσωματώνουν τις κατάλληλες λειτουργίες για την εξυπηρέτηση των αιτήσεων προς εξουσιοδότηση.
- Διαχειριστής Οντολογίας Εξουσιοδοτήσεων, που επιτρέπει την αλληλεπίδραση του παρόχου και των χρηστών του ΚΔΕ με την Οντολογία Εξουσιοδοτήσεων.
- Αποθετήριο, που αναπαριστά την υποκείμενη υποδομή αποθήκευσης δεδομένων, συλλογισμών και πιστοποιητικών.
- Διεπαφές Επικοινωνίας, προς τις λοιπές οντότητες της πλατφόρμας.
- Βοηθητικές Εκτελεστικές Μονάδες (ΒΕΜ), που συνιστούν επιπρόσθετα εκτελεστικά εργαλεία της εξειδικευμένων στόχων κατά την εξυπηρέτηση

μονάδας ΚΔΕ προς τη διεκπεραίωση αιτήσεων για εξουσιοδότηση. Ειδικότερα, οι Βοηθητικές Εκτελεστικές Μονάδες, αξιοποιούνται για την τέλεση των απαιτούμενων ενεργειών που υποδεικνύουν οι συνθήκες εφαρμογής ενός κανόνα και κυρίως αυτές της ποιοτικοποίησης ποσοτήτων (greaterThan, atLeast κ.ο.κ.) ή της ανωνυμοποίησης δεδομένων. Ουσιαστικά, οι ΒΕΜ αποτελούν τους εκφραστές της στρατηγικής της μεταφοράς των διαδικασιών επεξεργασίας δεδομένων των παρόχων εντός της πλατφόρμας.



Εικόνα 25: Αρχιτεκτονική Κέντρου Διαχείρισης Εξουσιοδοτήσεων

Στη συνέχεια αναλύονται τα δύο βασικά εκτελεστικά εργαλεία των ΚΔΕ, ο Διαχειριστής Συναλλαγών και ο Διαχειριστής Συνόδων.

7.1.1 Διαχειριστής Συναλλαγών

Ο Διαχειριστής Συναλλαγών συνιστά τη μονάδα εκείνη του ΚΔΕ που συγκεντρώνει τις βασικές λειτουργίες για την εξυπηρέτηση των αιτήσεων για εξουσιοδότηση. Κάθε στιγμιότυπο του Διαχειριστή Συναλλαγών γίνεται αντιληπτό ως ο προσωπικός εκπρόσωπος των αιτούντων εντός των ΚΔΕ. Προς τούτο, καθ' όλη τη λειτουργία του συστήματος, κάθε στιγμιότυπο Διαχειριστή Συναλλαγών αντιστοιχίζεται αποκλειστικά στους διαφορετικούς χρήστες και τα τρίτα ΚΔΕ που αλληλεπιδρούν με

κάθε ΚΔΕ. Επομένως ο ίδιος χρήστης ή η ίδια οντότητα ΚΔΕ που αλληλεπιδρά με ένα ΚΔΕ μέσω των μηνυμάτων *requestACs* και *requestData* αντίστοιχα, αξιοποιεί το ίδιο αντικείμενο Διαχειριστή Συναλλαγών το οποίο εργάζεται ανεξάρτητα από τη λειτουργία των υπόλοιπων στιγμιότυπων. Με αυτόν τον τρόπο τα ΚΔΕ δύνανται να παρακολουθούν τα διαφορετικά στάδια επικοινωνίας τους με τις διακριτές οντότητες αλληλεπίδρασης. Σε αυτό το πλαίσιο, για την υλοποίηση των Διαχειριστών Συναλλαγών αξιοποιήθηκε η τεχνολογία των Enterprise JavaBeans 3 (EJB3) [122] της Java, ενώ πιο συγκεκριμένα κάθε Διαχειριστής Συναλλαγών αποτελεί ένα αντικείμενο παρακολούθησης καταστάσεων Stateful Enterprise Java Bean.

Για την εξυπηρέτηση των διαφορετικών λειτουργικών απαιτήσεων που απορρέουν από τις αρμοδιότητες του Διαχειριστή Συναλλαγών, ενεργοποιούνται οι παρακάτω μονάδες:

- Μονάδα Επικύρωσης, αρμόδια για τη διεξαγωγή των κατάλληλων ενεργειών για την επικύρωση της ορθότητας και ισχύος των πιστοποιητικών που διαχειρίζεται το ΚΔΕ στο πλαίσιο της εξυπηρέτησης συγκεκριμένων αιτήσεων. Η μονάδα κάνει εκτεταμένη χρήση της κρυπτογραφικής βιβλιοθήκης Bouncy Castle [123],
- Μονάδα Αιτιολόγησης, η οποία επιστρέφει μια δυαδική απάντηση στο ερώτημα της καταλληλότητας και της επάρκειας των παρουσιασθέντων ψηφιακών πιστοποιητικών για την εξυπηρέτηση του κατατιθεμένου αιτήματος. Ουσιαστικά, τα πιστοποιητικά ελέγχονται για την εύρεση στιγμιότυπων PDT που εξουσιοδοτούν το υποκείμενο αίτημα.
- Μονάδα Δυναμικού Συλλογισμού, που επιφορτίζεται με τη διεκπεραίωση όλων των διαδικασιών που περιγράφηκαν στην ενότητα 5.2.2 και αφορούν την περαιτέρω επιβολή περιορισμών στις εξουσιοδοτήσεις που υποδεικνύονται από τη Μονάδα Αιτιολόγησης.
- Μονάδα Ισοδυναμιών, που αξιοποιείται για τον έλεγχο σημασιολογικών ισοδυναμιών μεταξύ των ληφθέντων πιστοποιητικών και των τοπικών στιγμιότυπων της Οντολογίας Εξουσιοδοτήσεων, όπου αυτό κρίνεται απαραίτητο.
- Μονάδα Πιστοποιητικών, αρμόδια για τη διαχείριση των κατάλληλων πιστοποιητικών ταυτότητας και ιδιοτήτων που απαιτούνται τόσο για την

αναγνώριση των χρηστών του Κέντρου αλλά και την εξουσιοδότηση των αιτημάτων.

- Μονάδα Εφαρμογής, αποτελεί το Σημείο Εφαρμογής Πολιτικής του Κέντρου, όντας αρμόδιο τόσο για την υπόδειξη των απορρεόντων από την ισχύ των κανόνων εξουσιοδότησης υποχρεώσεων όσο και για την επιβολή της τελικής απόφασης εξουσιοδότησης.

7.1.2 Διαχειριστής Συνόδων

Ο Διαχειριστής Συνόδων αναπαριστά τη μονάδα εκείνη που ενορχηστρώνει τη λειτουργία των Διαχειριστών Συναλλαγών, ενώ ταυτόχρονα διαχειρίζεται το σύνολο των αλληλεπιδράσεων του ΚΔΕ με τις λοιπές οντότητες του συστήματος. Υπό αυτή τη σκοπιά, ο Διαχειριστής Συνόδων υλοποιεί τις αντίστοιχες διεπαφές επικοινωνίας με τους χρήστες του συστήματος και τα λοιπά ΚΔΕ και τον ΕΣΙ της Συνομοσπονδίας. Λειτουργώντας ως βασικός κόμβος επικοινωνίας, ο Διαχειριστής Συνόδων αναπτύχθηκε ως ένα αντικείμενο HTTP «μικροϋπηρεσιών» Java (HTTP Servlet). Επιπρόσθετα, με στόχο την υποστήριξη της κλιμακοθετησιμότητας του συστήματος, ο Διαχειριστής Συνόδων όπως και όλες οι μονάδες του ΚΔΕ αναπτύχθηκαν στο περιβάλλον υποστήριξης πολυνηματικής λειτουργίας (multithreading) κατά τη διαχείριση των Servlets και των Enterprise Java Beans του συστήματος, του Εξυπηρετητή Εφαρμογών JBoss Application Server [124]. Οι διεπαφές επικοινωνίας του Διαχειριστή Συνόδων σχεδιάστηκαν έτσι ώστε να υλοποιούν ασφαλή κανάλια επικοινωνίας με τις οντότητες της πλατφόρμας, στη βάση ασφαλών HTTP συνδέσεων και μέσω χρήσης του πρωτοκόλλου Transport Layer Security (TLS) [125]. Η υλοποίηση των εν λόγω καναλιών επικοινωνίας πραγματοποιήθηκε με χρήση των βιβλιοθηκών Java Secure Socket Extension (JSSE) [126].

Βασικό τμήμα των αρμοδιοτήτων του Διαχειριστή Συνόδων αναφέρεται στην οργάνωση του κύκλου ζωής των Διαχειριστών Συναλλαγών του ΚΔΕ. Πιο συγκεκριμένα, ο Διαχειριστής Συνόδων είναι υπεύθυνος για:

- την ενεργοποίηση ενός νέου στιγμιότυπου Διαχειριστή Συναλλαγών για κάθε αίτημα από χρήστη ή ΚΔΕ για τον οποίο δεν έχουν κρατηθεί στοιχεία προηγούμενης σύνδεσής του με το ΚΔΕ,

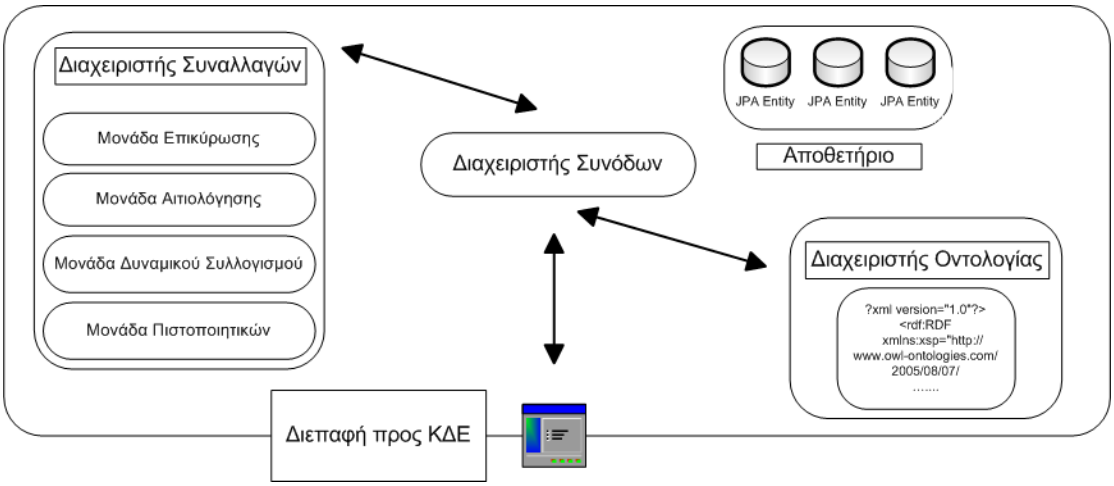
- την ενεργοποίηση του μοναδικού στιγμιότυπου Διαχειριστή Συναλλαγών που αντιστοιχεί σε κάθε χρήστη ή ΚΔΕ για τον οποίο προκύπτουν στοιχεία προηγούμενης σύνδεσής του με το ΚΔΕ,
- τη μεταφορά των ληφθέντων ψηφιακών πιστοποιητικών και των αιτημάτων στο κατάλληλο στιγμιότυπο Διαχειριστή Συναλλαγών προς αποσαφήνιση των εξουσιοδοτήσεων,
- την εφαρμογή των αποφάσεων του κατάλληλου στιγμιότυπου Διαχειριστή Συναλλαγών και
- την απενεργοποίηση του μοναδικού στιγμιότυπου Διαχειριστή Συναλλαγών που αντιστοιχεί σε κάθε χρήστη ή ΚΔΕ και τη διαγραφή των σχετικών πληροφοριών ιστορικού κινήσεων κατά την αποσύνδεση τους από την ΚΔΕ.

7.2 Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας

Ο σχεδιασμός της μονάδας του Επικεφαλής της Συνομοσπονδίας Ιδιωτικότητας είναι σαφώς επηρεασμένος από τις αρμοδιότητες της μονάδας στο πλαίσιο του υιοθετημένου μοντέλου εμπιστοσύνης και πιο συγκεκριμένα από τα καθήκοντα μιας τυπικής Αρχής Πιστοποίησης Γέφυρας σε μια Υποδομή Δημοσίου Κλειδιού. Επιπρόσθετα, η μονάδα ΕΣΙ είναι υπεύθυνη για την προδιαγραφή κοινών κανόνων εξουσιοδότησης που έχουν ως πεδίο εφαρμογής το σύνολο της Συνομοσπονδίας Ομότιμων Ιδιωτικότητας και για την παραγωγή των κατάλληλων γνωματεύσεων σε πραγματικό χρόνο. Πιο λεπτομερώς η εσωτερική αρχιτεκτονική της μονάδας (Εικόνα 26) περιλαμβάνει τις ακόλουθες λειτουργικές συνιστώσες:

- Διαχείρισης Συνόδων, που σε αντιστοιχία με τον Διαχειριστή Συνόδων των ΚΔΕ, ενεργοποιείται για τη διαχείριση των διακριτών συνόδων (sessions) της ΕΣΙ στα πλαίσια της αλληλεπίδρασής της με τις ΚΔΕ της Συνομοσπονδίας.
- Διαχειριστής Συναλλαγών, που επιτελούν το έργο της επιχειρηματικής λογικής του ΕΣΙ. Προς τούτο, συναπαρτίζονται από τις κατάλληλες υπό-μονάδες (Μονάδα Επικύρωσης, Μονάδα Αξιολόγησης, Μονάδα Δυναμικού Συλλογισμού και Μονάδα Πιστοποιητικών) καθεμία από τις οποίες είναι επιφορτισμένη με αρμοδιότητες πανομοιότυπες με αυτές των συγγενών υπό-μονάδων των ΚΔΕ.
- Διαχειριστής Οντολογίας Εξουσιοδοτήσεων, που επιτρέπει την αλληλεπίδραση του Επικεφαλής με την Οντολογία Εξουσιοδοτήσεων.

- Αποθετήριο, που αναπαριστά την υποκείμενη υποδομή αποθήκευσης συλλογισμών και πιστοποιητικών (και όχι δεδομένων καθώς ο ΕΣΙ διατηρεί καθαρά ρόλο επίβλεψης της πλατφόρμας)
- Διεπαφές Επικοινωνίας, προς τους ΚΔΕ της Συνομοσπονδίας.



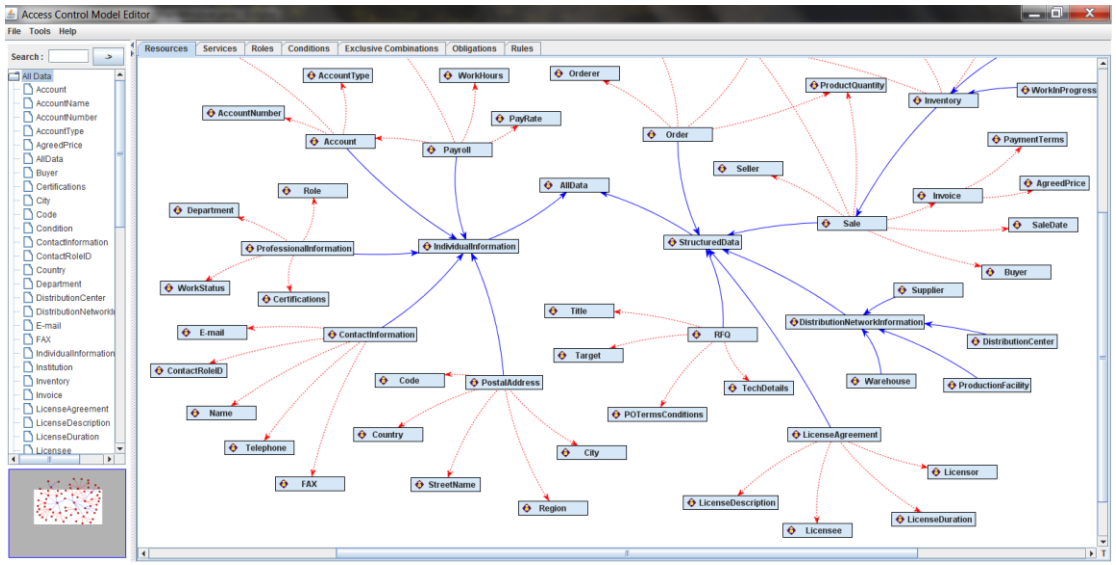
Εικόνα 26: Αρχιτεκτονική Επικεφαλής Συνομοσπονδίας Ιδιωτικότητας

Σημειώνεται ότι, σε αντιστοιχία με τις υπό-μονάδες των ΚΔΕ, ο Διαχειριστής Συνόδων του ΕΣΙ υλοποιήθηκε ως αντικείμενο Java Servlet και οι Διαχειριστές Συναλλαγών ως Stateful Enterprise Java Beans. Ομοίως, για την κατασκευή των ψηφιακών πιστοποιητικών εκμεταλλεύτηκαν οι δυνατότητες της κρυπτογραφικής βιβλιοθήκης Bouncy Castle, ενώ για τη δημιουργία των ασφαλών και κρυπτογραφημένων TLS καναλιών επικοινωνίας αξιοποιήθηκε το πακέτο βιβλιοθηκών Java Secure Socket Extension.

7.3 Λογισμικό Προδιαγραφής Οντολογίας Εξουσιοδοτήσεων

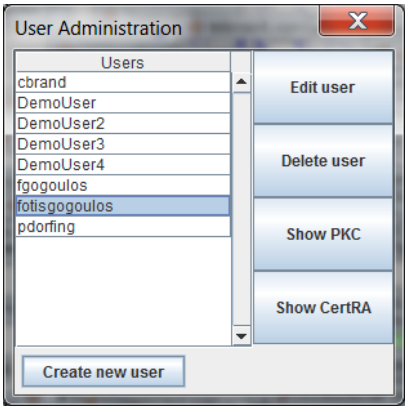
Η Οντολογία Εξουσιοδοτήσεων κατέχει κεντρικό ρόλο στις διαδικασίες και λειτουργίες που στοχεύουν στην παραγωγή σαφών αποφάσεων εξουσιοδότησης κι επομένως η διαχείρισή της αποκτά βαρύνουσα σημασία για την εύρυθμη λειτουργία της πλατφόρμας. Για την προδιαγραφή του σχήματος της Οντολογίας Εξουσιοδοτήσεων, τον σχεδιασμό των επιθυμητών στιγμιότυπών της και την οργάνωση των μεταξύ τους συσχετίσεων αξιοποιήθηκε εξειδικευμένο λογισμικό προδιαγραφής οντολογιών, κατάλληλα προσαρμοσμένο στις ανάγκες της προτεινόμενης πλατφόρμας. Το λογισμικό προδιαγραφής κανόνων ελέγχου πρόσβασης αποτελεί μια φιλική προς τον χρήστη εφαρμογή, που αναπτύχθηκε σε

Java για την απόκρυψη των εμπλεκόμενων τεχνικών λεπτομερειών από τους χρήστες κατά τη διαχείριση OWL οντολογιών. Η πλειοψηφία των υποστηριζόμενων λειτουργιών διαχείρισης οντολογιών και οπτικοποίησης των παραγόμενων ταξινομήσεων βασίζεται στις δυνατότητες των βιβλιοθηκών Jena και JUNG (Java Universal Network/Graph Framework) [127] αντίστοιχα, ενώ το λογισμικό περιλαμβάνει έναν αναλυτικό οδηγό προδιαγραφής κανόνων εξουσιοδότησης με ρυθμίσεις των απαραίτητων μεταβλητών βήμα-προς-βήμα.

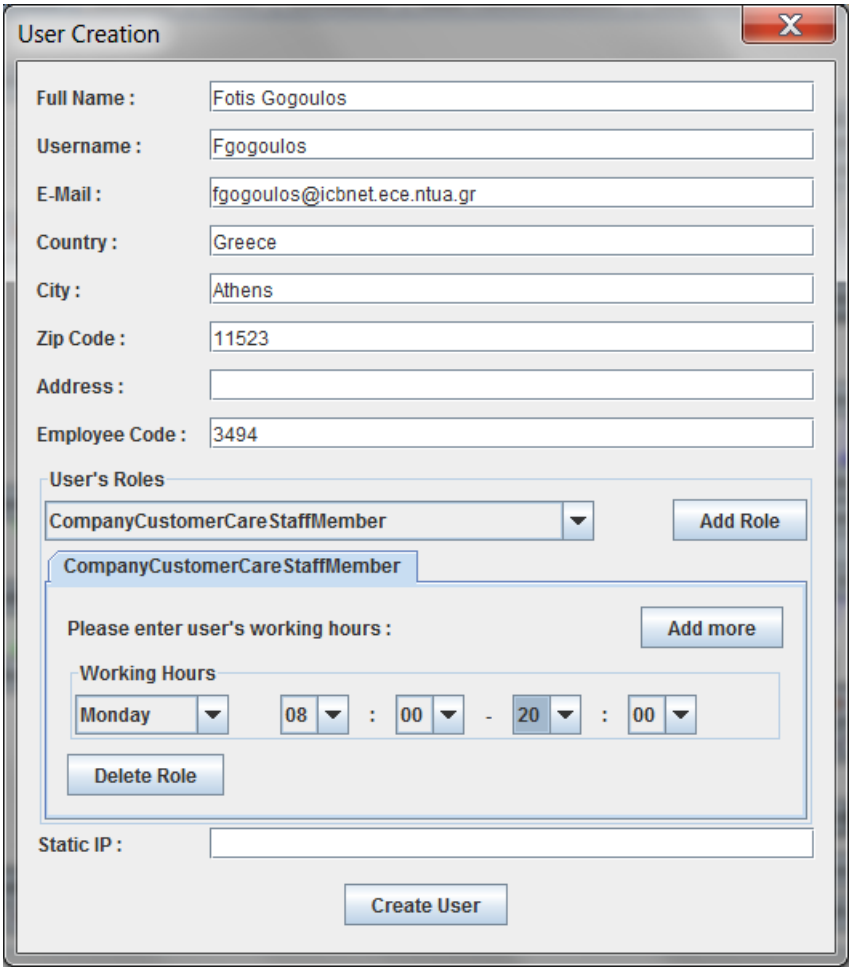


Εικόνα 27: Άποψη των στιγμιότυπων της κλάσης *Data*

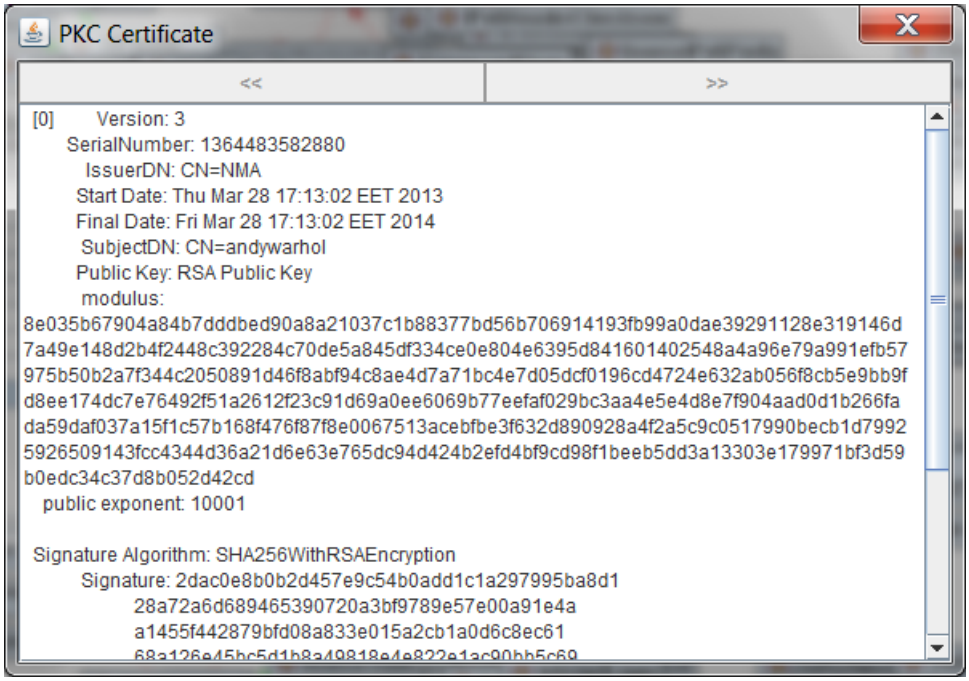
Βασικό τμήμα των λειτουργιών του λογισμικού αναφέρεται στη διαχείριση των χρηστών του συστήματος και ως επέκταση στη διαχείριση του κύκλου ζωής των εμπλεκόμενων πιστοποιητικών ταυτότητας και ιδιοτήτων. Προς τούτο, το λογισμικό παρέχει τη δυνατότητα καταγραφής των χρηστών και των ιδιοτήτων τους (Εικόνα 28 και Εικόνα 29), αναπαραγωγής των αντίστοιχων πιστοποιητικών U-PKC και U-AC (Εικόνα 30), αλλά και των πιστοποιητικών C-PKC καθώς και δημιουργίας λιστών ανάκλησης πιστοποιητικών (Certificate Revocation Lists – CRLs) (Εικόνα 31), τις οποίες τα ΚΔΕ και ο ΕΣΙ διατηρούν τοπικά και συμβουλεύονται κατά την επικύρωση των διαχειριζόμενων πιστοποιητικών από τις ενσωματωμένες Μονάδες Επικύρωσης.



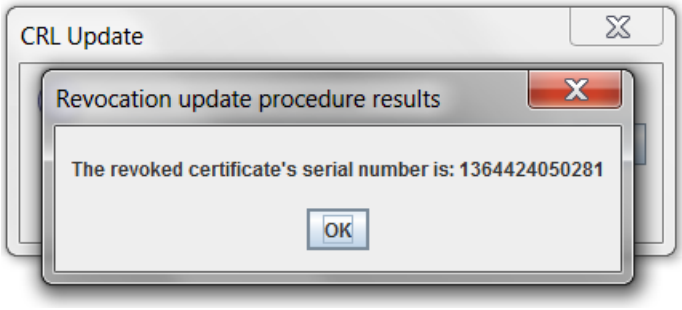
Εικόνα 28: Οθόνη διαχείρισης χρηστών και Πιστοποιητικών Ταυτότητας και Ιδιοτήτων



Εικόνα 29: Οθόνη καταχώρησης νέου χρήστη



Εικόνα 30: Πιστοποιητικό χρήστη U-PKC



Εικόνα 31: Οθόνη ενημέρωσης λίστας ανάκλησης πιστοποιητικών

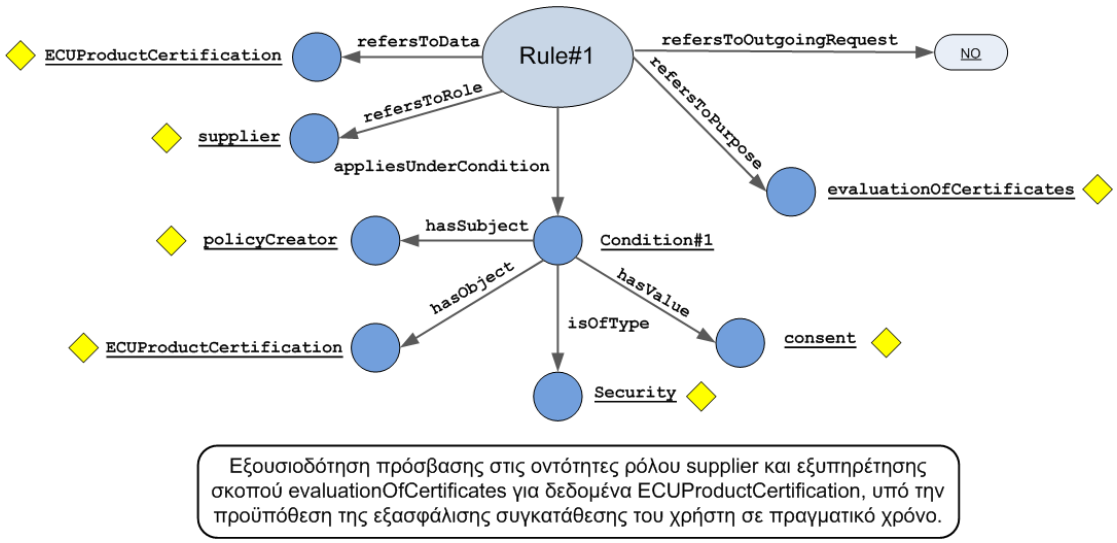
8 Παράδειγμα Χρήσης και Αξιολόγηση

Προκειμένου να γίνει κατανοητή η λειτουργία της προτεινόμενης πλατφόρμας διαχείρισης εξουσιοδοτήσεων, το παρόν κεφάλαιο παρουσιάζει την αξιοποίησή της σε ένα ρεαλιστικό σενάριο ροής δεδομένων μεταξύ απομακρυσμένων εταίρων σε επιχειρηματικό περιβάλλον, που είναι εμπνευσμένο από τα πρότυπα λειτουργίας του Enterprise 2.0. Το επιλεγμένο παράδειγμα αφορά τη ροή πληροφορίας σε ένα τυπικό σενάριο **δικτύων εφοδιαστικής αλυσίδας** (supply chain networks). Τα δίκτυα εφοδιαστικής αλυσίδας αναφέρονται σε εμπορικούς συνεταιρισμούς απομακρυσμένων και ανεξάρτητων οργανισμών που δημιουργούνται στη βάση του κοινού στόχου της παραγωγής κάποιου προϊόντος. Εντός των συνεταιρισμών, οι εταίροι της εφοδιαστικής αλυσίδας ενεργοποιούνται σε μια συνεχή συνεργασία, όπου η λήψη αποφάσεων για τον διαμοιρασμό πληροφοριών βρίσκεται στο επίκεντρο. Αν και τα παραδοσιακά δίκτυα εφοδιαστικής αλυσίδας είθισται να οργανώνονται σε ιεραρχικές δομές, ιδιαίτερο ενδιαφέρον παρουσιάζουν τα σύγχρονα μη ιεραρχικά συνεργατικά δίκτυα, στα οποία κάθε μέλος διατηρεί μεγαλύτερη αυτονομία και διαθέτει τους πόρους του σύμφωνα με ατομικές στρατηγικές και λιγότερο στη βάση του συλλογικού συμφέροντος των παραδοσιακών δικτύων εφοδιαστικής αλυσίδας.

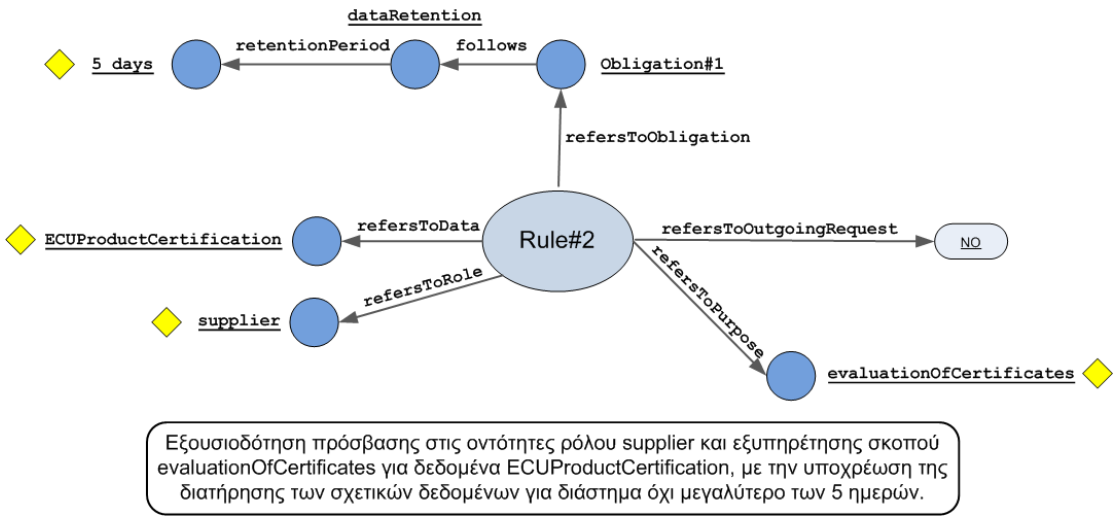
8.1 Βασικό Σενάριο Χρήσης

Η απλουστευμένη εφοδιαστική αλυσίδα του παραδείγματος αφορά το σχηματιζόμενο μη ιεραρχικό δίκτυο παραγωγής κινητήρων οχημάτων μεταξύ των εταιριών: α) *EngineComp* με αντικείμενο εργασίας την τελική συναρμολόγηση και παράδοση των κινητήρων στους πελάτες, β) *ECUComp* με αρμοδιότητες στο δίκτυο που σχετίζονται με την παραγωγή Μονάδων Ελέγχου Κινητήρα (Engine Control Unit – ECU) και γ) *RomECUComp* που εργάζεται για την παραγωγή μνημών ανάγνωσης (Read Only Memory – ROM) για μονάδες ECU. Πιο συγκεκριμένα το σενάριο χρήσης αφορά τον υπάλληλο *ECEmployee* του Τμήματος Προμηθειών (*PurchasingDepartmentEmployee*) της εταιρίας *EngineComp* ο οποίος απαιτεί πληροφορίες διαθεσιμότητας Μονάδων Ελέγχου Κινητήρα (*ECUAvailability*) από την εταιρία *ECUComp* κατά τη σύνταξη προσφοράς-απάντησης σε σχετική πρόσκληση (*RequestForQuotationReply*). Ταυτόχρονα, θεωρείται ότι ο οργανισμός

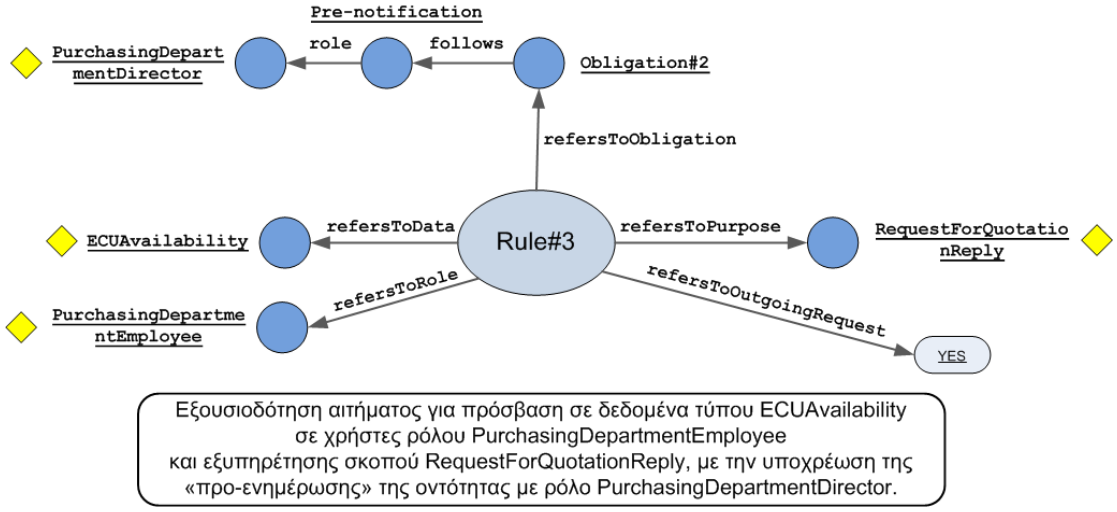
EngineComp, προς εξουσιοδότηση αιτήματος απαιτεί τη συγκατάθεση σε πραγματικό χρόνο του προϊσταμένου του τμήματος (*PurchasingDepartmentDirector*). Από την άλλη πλευρά, η εταιρία *ECUComp*, για την αποκάλυψη της σχετικής πληροφορίας απαιτεί από τους αιτούντες αφενός να αποδείξουν τον υποκείμενο ρόλο και σκοπό πρόσβασης που ταυτοποιούνται από ένα εταίρο του δικτύου ο οποίος χαρακτηρίζεται από υψηλό επίπεδο πολιτικών πιστοποίησης, αφετέρου να έχουν στην κατοχή τους τουλάχιστον μια πιστοποίηση προϊόντος σχετικά με τις μονάδες ECU (*ECUProductCertification*). Θεωρείται ότι η φάση της διαμόρφωσης της υποδομής έχει διεξαχθεί κι επομένως όλες οι οντότητες έχουν ήδη ορίσει τις προσωπικές τους προτιμήσεις εξουσιοδοτήσεων ενώ έχει εκδοθεί και το σύνολο των απαραίτητων πιστοποιητικών που διαμορφώνουν το υποκείμενο μοντέλο εμπιστοσύνης. Οι Εικόνες Εικόνα 32, Εικόνα 33, Εικόνα 34 και Εικόνα 35 αναπαριστούν το σύνολο των διαμορφωθέντων κανόνων από τις οντότητες του συστήματος, όπου χωρίς απώλεια της γενικότητας περιγράφονται κανόνες για δικαιώματα ανάγνωσης, ενώ τα εμπλεκόμενα στιγμιότυπα αξιοποιούν κοινές σημασιολογικές αποτυπώσεις. Επίσης, θεωρείται ότι τα δεδομένα τύπου *ECUProductCertification* αποτελούν τόσο ευαίσθητη επιχειρηματική πληροφορία των οργανισμών όσο και προσωπικό δεδομένο των χρηστών.



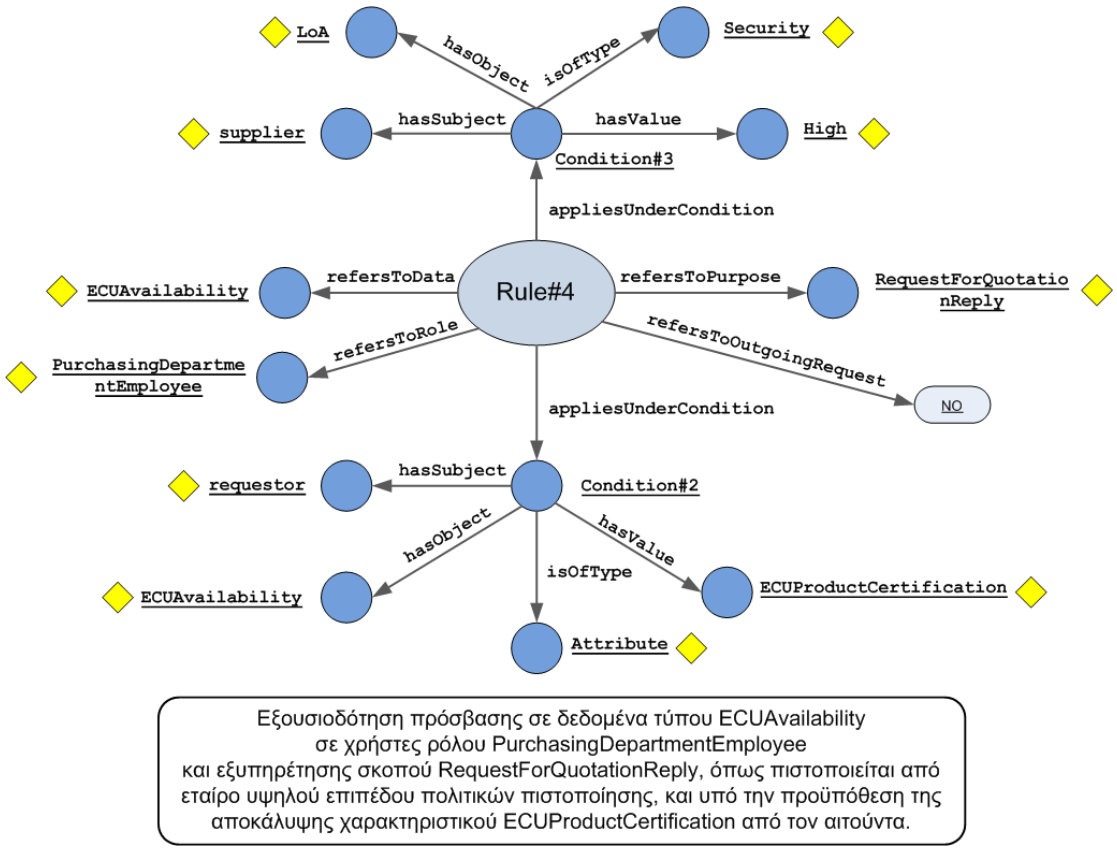
Εικόνα 32: Κανόνας χρήστη και υπαλλήλου της *EngineComp* για πρόσβαση στα δεδομένα τύπου *ECUProductCertification*



Εικόνα 33: Κανόνας οργανισμού *EngineComp* εφοδιαστικής αλυσίδας για πρόσβαση στα δεδομένα τύπου *ECUProductCertification*



Εικόνα 34: Κανόνας οργανισμού *EngineComp* εφοδιαστικής αλυσίδας για εξουσιοδότηση αιτήματος για πρόσβαση στα δεδομένα τύπου *ECUAvailability*



Εικόνα 35: Κανόνας οργανισμού *ECUComp* εφοδιαστικής αλυσίδας για εξουσιοδότηση πρόσβασης σε δεδομένα τύπου *ECUAvailability*

Αναλυτικά και στη βάση του σεναρίου χρήσης και των παραπάνω κανόνων εξουσιοδότησης, διεξάγονται τα ακόλουθα βήματα του πρωτοκόλλου εξουσιοδότησης (όπως απεικονίζονται στο διάγραμμα της Εικόνα 37):

Βήμα 1: Ο υπάλληλος *ECEmployee* αποδίδει μήνυμα τύπου **requestAC** στο ΚΔΕ του οργανισμού στον οποίο υπάγεται με στόχο την εξουσιοδότηση του αιτήματός του και με περιεχόμενα που προσδιορίζουν την ταυτότητα και τα χαρακτηριστικά του (μέσω πιστοποιητικών U-PKC και U-AC). Επιπρόσθετα, υποδεικνύει τον τύπο των δεδομένων για το οποίο προτίθεται να καταθέσει αίτημα στην πλευρά κάποιου μέλους της Συνομοσπονδίας (*ECUAvailability*), καθώς και τον εξυπηρετούμενο σκοπό πρόσβασης (*RequestForQuotationReply*). Μετά το πέρας του πρώτου βήματος, ο χρήστης-αιτών έχει αναγνωριστεί επιτυχώς από τον οργανισμό *EngineComp*.

Βήμα 2: Στο ΚΔΕ της εταιρίας *EngineComp* πραγματοποιείται έλεγχος για στιγμιότυπα PDT που να αφορούν το κατατιθέμενο αίτημα. Η ύπαρξη του κανόνα θετικής εξουσιοδότησης *Rule#3* (Εικόνα 34) ισοδυναμεί με την ύπαρξη ενός αντικειμένου PDT που συγκεκριμενοποιεί την εξουσιοδότηση του αιτήματος και την εμπλουτίζει με μεταδεδομένα συνθηκών και περιορισμών. Έτσι αφού εφαρμοστεί η

υποχρέωση της ενημέρωσης της οντότητας με ρόλο *PurchasingDepartmentDirector*, το αίτημα του χρήστη εξουσιοδοτείται τόσο «στατικά» όσο και «δυναμικά». Ως αποτέλεσμα, το ΚΔΕ παράγει ένα ψηφιακό πιστοποιητικό PDT-AC το οποίο αποτυπώνει την αντίστοιχη εξουσιοδότηση (Εικόνα 36) και το οποίο μεταφέρει στην πλευρά του χρήστη μαζί με το τοπικό C-PKC πιστοποιητικό, που αποδεικνύει τη συμμετοχή της εταιρίας *EngineComp* στη Συνομοσπονδία με επίπεδο εμπιστοσύνης των πολιτικών πιστοποίησής της ίσο με *High*. Θεωρώντας ότι το ΚΔΕ αξιοποιεί επακριβώς τα στιγμιότυπα της Οντολογίας Εξουσιοδοτήσεων που έχει ορίσει η οντότητα ΕΣΙ, το παραγόμενο πιστοποιητικό PDT-AC δεν υποδεικνύει συγκεκριμένες σημασιολογικές ισοδυναμίες.

```
Certificate:
  Data:

    Version: 2
    Serial Number: 01 3d b1 8f 2b a0
    Signature Algorithm: SHA512withRSA
    Issuer: CN= EngineComp
    Holder: PurchasingDepartmentEmployee
    Validity:
      Not Before: Tue Feb 17 16:23:40 EET 2013
      Not After: Tue Dec 19 16:47:00 EET 2013
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public Key (RSA 2048 bit):
30 82 01 0a 02 82 01 01 00 8e 03 5b 67 90 4a 84 b7 dd db ed 90 a8 a2 10 37
c1 b8 83 77 bd 56 b7 06 91 41 93 fb 99 a0 da e3 92 91 12 8e 31 91 46 d7 a4
9e 14 8d 2b 4f 24 48 c3 92 28 4c 70 de 5a 84 5d f3 34 ce 0e 80 4e 63 95 d8
41 60 14 02 54 8a 4a 96 e7 9a 99 1e fb 57 97 5b 50 b2 a7 f3 44 c2 05 08 91
d4 6f 8a bf 94 c8 ae 4d 7a 71 bc 4e 7d 05 dc f0 19 6c d4 72 4e 63 2a b0 56
f8 cb 5e 9b b9 fd 8e e1 74 dc 7e 76 49 2f 51 a2 61 2f 23 c9 1d 69 a0 ee 60
69 b7 7e ef af 02 9b c3 aa 4e 5e 4d 8e 7f 90 4a ad 0d 1b 26 6f ad a5 9d af
03 7a 15 f1 c5 7b 16 8f 47 6f 87 f8 e0 06 75 13 ac eb fb e3 f6 32 d8 90 92
8a 4f 2a 5c 9c 05 17 99 0b ec b1 d7 99 25 92 65 09 14 3f cc 43 44 d3 6a 21
d6 e6 3e 76 5d c9 4d 42 4b 2e fd 4b f9 cd 98 f1 be eb 5d d3 a1 33 03 e1 79
97 1b f3 d5 9b 0e dc 34 c3 7d 8b 05 2d 42 cd 02 03 01 00 01
    Attributes:{
                {Role: PurchasingDepartmentEmployee}
                {Purpose: RequestForQuotationReply}
                {DataType: ECUAvailability}
               }
    Extensions:
      X509v2AttCert Basic Constraints:
        CA: FALSE
```

Εικόνα 36: Πιστοποιητικό εξουσιοδότησης αιτήματος για πρόσβαση σε δεδομένα

Βήμα 3: Ο υπάλληλος *ECEmployee* αποδίδει μήνυμα τύπου **requestData** στο ΚΔΕ του οργανισμού που φιλοξενεί την πληροφορία που αναζητά (*ECUComp*) προωθώντας παράλληλα τα ανακτηθέντα πιστοποιητικά του ΚΔΕ του οργανισμού

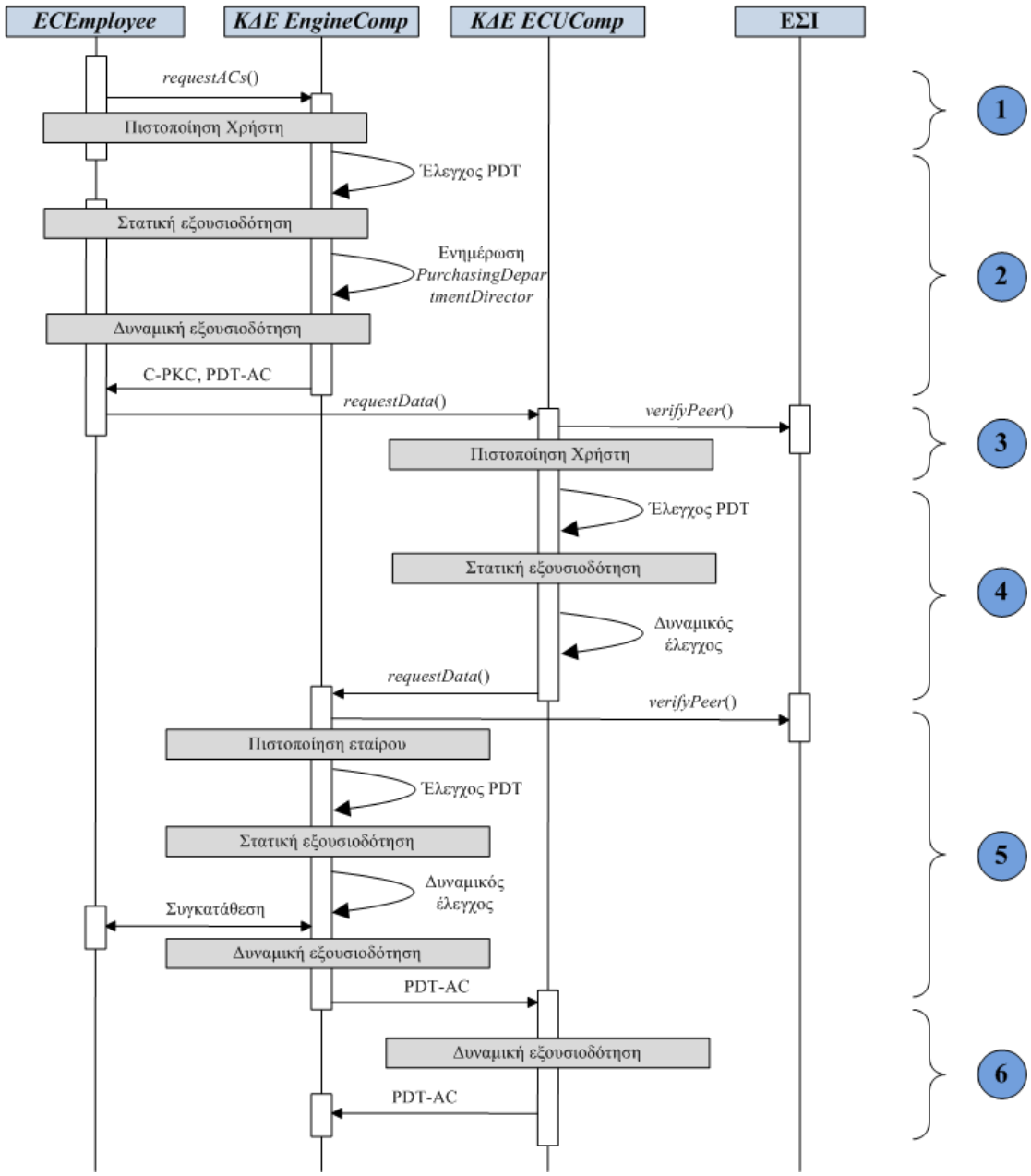
EngineComp και **κανένα** από τα προσωπικά του πιστοποιητικά. Προς εξακρίβωση της εγκυρότητας και ισχύος των πιστοποιητικών, το ΚΔΕ του *ECUComp* επικοινωνεί με την οντότητα ΕΣΙ (με μήνυμα **verifyPeer**) η οποία ανατρέχει στην τοπικά διατηρημένη Λίστα Ανάκλησης Πιστοποιητικών και βεβαιώνει ότι το πιστοποιητικό C-PKC της *EngineComp* δεν έχει ανακληθεί. Ταυτόχρονα, ενημερώνει για την απουσία κανόνα εξουσιοδότησης που να εφαρμόζει στην τρέχουσα περίπτωση. Σε αυτό το στάδιο, το ΚΔΕ του οργανισμού *ECUComp* έχει πιστοποιήσει το αίτημα του χρήστη, χωρίς να του έχει αποκαλυφθεί οποιοδήποτε είδος πληροφορίας πέραν της υπαγωγής του σε συγκεκριμένο οργανισμό της Συνομοσπονδίας.

Βήμα 4: Το ΚΔΕ της *ECUComp* εξετάζει τα αποτελέσματα των διαδικασιών στατικής και δυναμικής συλλογιστικής και διαπιστώνει την ύπαρξη του εφαρμόσιμου κανόνα *Rule#4* (Εικόνα 35). Ο κανόνας υποδεικνύει την προϋπόθεση της ικανοποίησης των συνθηκών της αποκάλυψης του χαρακτηριστικού *ECUProductCertification* από τον αιτούντα και της συνδιαλλαγής με εταίρο υψηλού επιπέδου πολιτικών πιστοποίησης. Επιβεβαιώνοντας την ισχύ της δεύτερης συνθήκης από το C-PKC που κατατέθηκε μαζί με το αίτημα του χρήστη, το ΚΔΕ κατασκευάζει ένα κατάλληλο PDT-AC για να κωδικοποιήσει το αίτημα του οργανισμού προς την εταιρία *EngineComp* με στόχο την ικανοποίηση της πρώτης συνθήκης. Το πιστοποιητικό εκτός από τον τύπο των ζητηθέντων δεδομένων (*ECUProductCertification*) περιλαμβάνει τον ρόλο που ενεργοποιεί ο οργανισμός (supplier), τον σκοπό πρόσβασης (*evaluationOfCertificates*) καθώς και τον σειριακό αριθμό του πιστοποιητικού PDT-AC (*01 3d b1 8f 2b a0*) που κατέθεσε ο χρήστης μαζί με το αίτημά του για πρόσβαση. Το δημιουργηθέν PDT-AC καθώς και το C-PKC της εταιρίας *ECUComp* μεταφέρονται στο ΚΔΕ της εταιρίας *EngineComp* μέσω ενός νέου αιτήματος **requestData**.

Βήμα 5: Μετά την επικοινωνία με την οντότητα ΕΣΙ (με μήνυμα **verifyPeer**) και τη μετέπειτα διαπίστωση της εγκυρότητας της *ECUComp* αλλά και της ανυπαρξίας κοινά ορισμένου κανόνα εξουσιοδότησης, το ΚΔΕ της *EngineComp* αναγνωρίζει τους κανόνες *Rule#1* (Εικόνα 32) και *Rule#2* (Εικόνα 33) ως εφαρμόσιμους για το υποκείμενο αίτημα. Σημειώνεται ότι για την αποσαφήνιση του συγκεκριμένου υπαλλήλου για τον οποίο ζητήθηκαν τα δεδομένα, το ΚΔΕ αξιοποιεί τον υποδειχθέντα σειριακό αριθμό που αντιστοιχεί στο PDT-AC του αρχικού αιτήματος του υπαλλήλου *ECEmployee*. Για την εφαρμογή των διατάξεων των εν λόγω κανόνων το ΚΔΕ εξασφαλίζει τη συγκατάθεση του υπαλλήλου και καταγράφει την υποχρέωση

διατήρησης της αποκαλυφθείσας πληροφορίας για διάστημα μικρότερο των 5 ημερών. Η εν λόγω υποχρέωση καταγράφεται σε πιστοποιητικό PDT-AC το οποίο συμπληρωματικά περιγράφει τα βασικά στοιχεία του αιτήματος αλλά και τη ζητηθείσα πληροφορία αυτή καθ' αυτή. Προς τούτο, ενσωματώνει σε συγκεκριμένο πεδίο-επέκταση του PDT-AC, το μοναδικό αναγνωριστικό της πιστοποίησης *ECUProductCertification* του υπαλλήλου *ECEmployee*. Το αναγνωριστικό μπορεί να αξιοποιηθεί στη συνέχεια από τα ενδιαφερόμενα μέλη για την αναζήτηση του σχετικού εγγράφου σε κάποιον εξειδικευμένο εξυπηρετητή περιεχομένου. Εναλλακτικά, προωθείται παράλληλα με το PDT-AC και το ηλεκτρονικό έγγραφο της πιστοποίησης. Στο τέλος του βήματος αλληλεπίδρασης, το πιστοποιητικό PDT-AC μεταφέρεται στο ΚΔΕ της *ECUComp*.

***Βήμα 6*:** Έχοντας εξασφαλίσει τα ζητηθέντα δεδομένα και ως εκ τούτου έχοντας βεβαιώσει την ικανοποίηση της συνθήκης αποκάλυψης των δεδομένων που αιτήθηκε ο χρήστης, το ΚΔΕ της *ECUComp* δημιουργεί ένα πιστοποιητικό PDT-AC, το οποίο καταγράφει τα βασικά στοιχεία του αιτήματος αλλά και την αρχικώς ζητηθείσα πληροφορία αυτή καθ' αυτή, αποκαλύπτοντας την τρέχουσα διαθεσιμότητα σε Μονάδες Ελέγχου Κινητήρα στο ΚΔΕ του αιτούντα, από όπου ο τελευταίος ενημερώνεται σχετικά. Σημειώνεται ότι, καθ' όλη τη διάρκεια του πρωτοκόλλου τα διαμοιραζόμενα δεδομένα (τόσο οι πιστοποιήσεις του χρήστη, όσο και η διαθεσιμότητα σε Μονάδες Ελέγχου Κινητήρα) περιορίζονται αποκλειστικά εντός των ορίων της Συνομοσπονδίας.

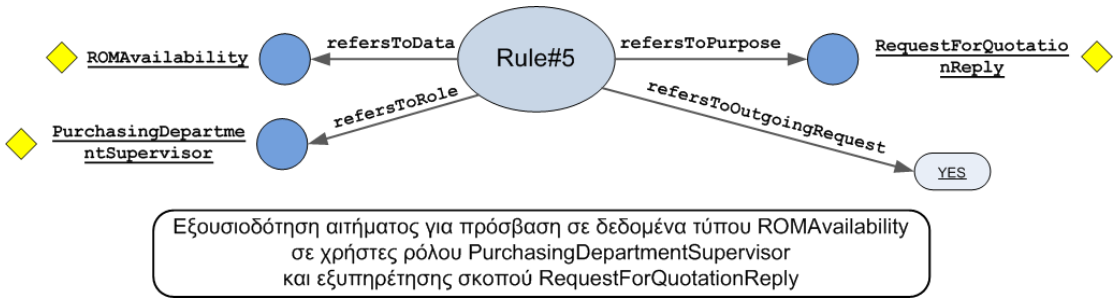


Εικόνα 37: Ροή εργασιών και δεδομένων κατά τη χρήση της πλατφόρμας

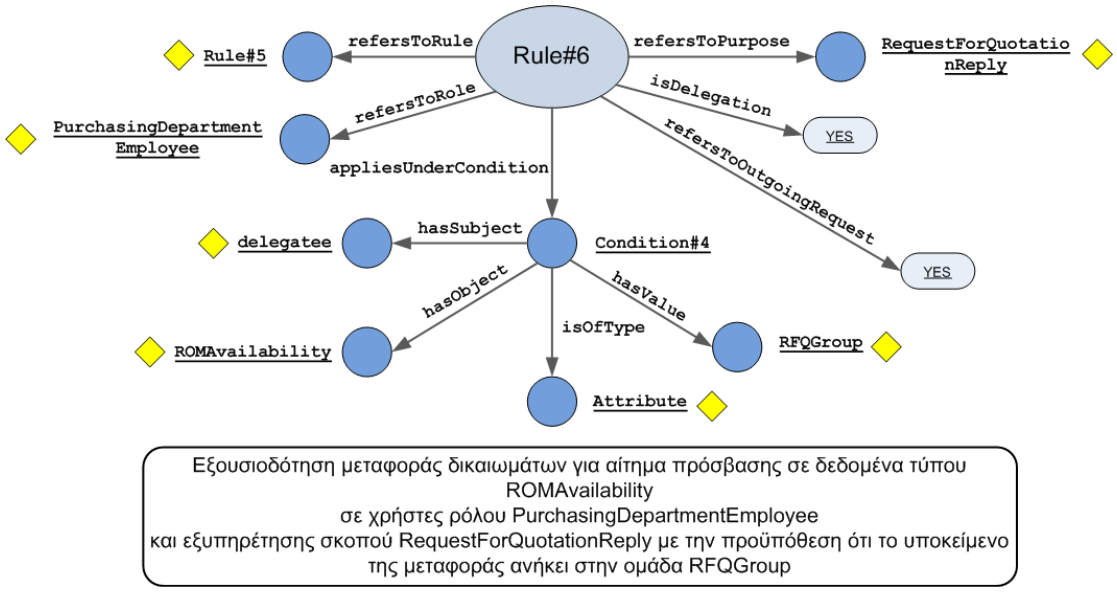
8.2 Επέκταση Βασικού Σεναρίου Χρήσης

Ως επέκταση του βασικού σεναρίου χρήσης, θεωρείται ότι πληροφορίες για τη διαθεσιμότητα μονάδων μνημών ανάγνωσης (*ROMAvailability*) είναι απαραίτητες για τον οργανισμό *ECUComp* προτού να είναι δυνατός ο υπολογισμός της άμεσης διαθεσιμότητας σε Μονάδες Ελέγχου Κινητήρα. Προς τούτο, επικοινωνεί με τον οργανισμό-τροφοδότη της εντός της εφοδιαστικής αλυσίδας, την εταιρία *RomECUComp* και αιτείται πρόσβασης στα σχετικά δεδομένα. Ωστόσο, θεωρείται ότι η εταιρία *RomECUComp*, δρώντας εντός μη ιεραρχικού δικτύου και άρα μην λειτουργώντας ως αποκλειστικός πάροχος μονάδων μνήμης της εταιρίας *ECUComp*,

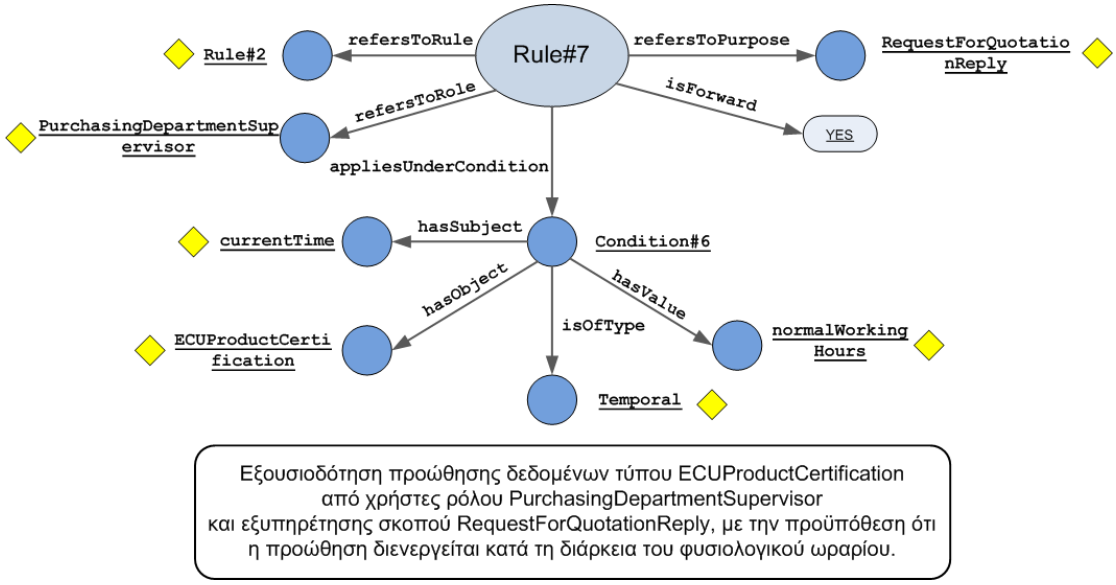
θέτει ατομικές προϋποθέσεις για την αποκάλυψη ευαίσθητων επιχειρηματικών πληροφοριών που φυσικά μπορεί να εμπλέκουν και άλλους εταίρους της Συνομοσπονδίας. Υπό αυτή τη σκοπιά, θεωρείται ότι για την αποκάλυψη της πληροφορίας της τρέχουσας διαθεσιμότητας σε μονάδες μνήμης, θέτει ως προϋπόθεση τον έλεγχο των πιστοποιήσεων προϊόντος σχετικά με τις μονάδες ECU (*ECUProductCertification*) του ατόμου που συντάσσει την πρόσφορά, στο πλαίσιο της οποίας πραγματοποιείται η συνεργασία των εταίρων. Για τη διαχείριση των επιμέρους εξουσιοδοτήσεων που προκύπτουν προδιαγράφονται επιπρόσθετα οι κανόνες *Rule#5* (Εικόνα 38) και *Rule#6* (Εικόνα 39) στο ΚΔΕ της *ECUComp* , *Rule#7* (Εικόνα 40) στο ΚΔΕ της *EngineComp* και *Rule#8* (Εικόνα 41) στο ΚΔΕ της *RomECUComp*.



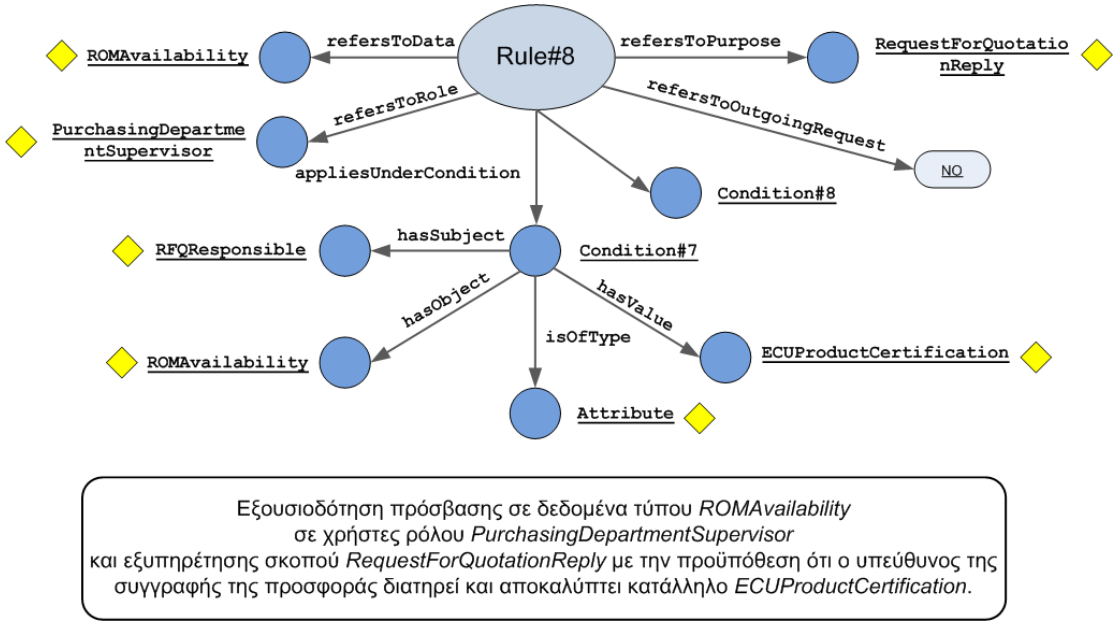
Εικόνα 38: Κανόνας οργανισμού *ECUComp* εφοδιαστικής αλυσίδας για εξουσιοδότηση αιτήματος για πρόσβαση στα δεδομένα τύπου *ROMAvailability*



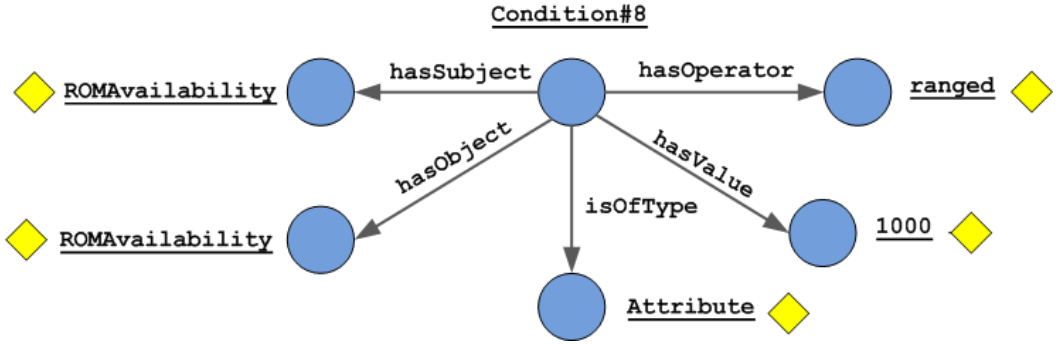
Εικόνα 39: Κανόνας οργανισμού *ECUComp* εφοδιαστικής αλυσίδας για μεταφορά δικαιωμάτων εξουσιοδότησης αιτήματος για πρόσβαση στα δεδομένα τύπου *ROMAvailability*



Εικόνα 40: Κανόνας οργανισμού *EngineComp* εφοδιαστικής αλυσίδας για εξουσιοδότηση προώθησης δεδομένων τύπου *ROMAvailability*



Εικόνα 41: Κανόνας οργανισμού *RomECUComp* εφοδιαστικής αλυσίδας για εξουσιοδότηση πρόσβασης σε δεδομένα τύπου *ROMAvailability*



Εικόνα 42: Συνθήκη περιορισμού της αποκάλυψης δεδομένων μέσω χρήσης εύρους τιμών στον οργανισμό *RomECUComp*

Οι διατάξεις του κανόνα *Rule#8* επιτρέπουν την πρόσβαση στις πληροφορίες διαθεσιμότητας μονάδων μνήμης της *RomECUComp* σε οντότητες που ενεργοποιούν τον ρόλο: Υπεύθυνος του Τμήματος Προμηθειών (*PurchasingDepartmentSupervisor*) και εξυπηρετούν τον σκοπό πρόσβασης: σύνταξη προσφοράς-απάντησης σε σχετική πρόσκληση (*RequestForQuotationReply*). Ωστόσο, για την εφαρμογή της θετικής εξουσιοδότησης του κανόνα προϋποθέτεται η αποκάλυψη της πιστοποίησης προϊόντος σχετικά με τις μονάδες ECU (*ECUProductCertification*) του συντάκτη της προσφοράς. Επίσης, ορίζεται η αποκάλυψη της διαθεσιμότητας μονάδων μνήμης να πραγματοποιηθεί όχι κατά απόλυτη τιμή αλλά μέσω εύρους τιμών, θεωρώντας πως για την εξυπηρέτηση του στόχου *RequestForQuotationReply* η σχετική πληροφορία είναι ικανή (Εικόνα 42). Η εν λόγω μετατροπή θα λάβει χώρα πριν την αποκάλυψη της πληροφορίας σχετικά με τη ζητηθείσα διαθεσιμότητα, μέσω της αξιοποίησης της κατάλληλης Βοηθητικής Εκτελεστικής Μονάδας.

Βάσει των διατάξεων του κανόνα *Rule#7* ο οργανισμός *EngineComp* εξουσιοδοτεί την περαιτέρω προώθηση της σχετικής πληροφορίας με μόνη προϋπόθεση ότι η προώθηση διενεργείται κατά τη διάρκεια του φυσιολογικού ωραρίου (Δευτέρα – Παρασκευή και 08:00 – 20:00). Υπενθυμίζεται ότι, ούτως ή άλλως ο κανόνας εξουσιοδότησης *Rule#2* προδιέγραφε την υποχρέωση διατήρησης των σχετικών δεδομένων για διάστημα μικρότερο των 5 ημερών. Τόσο η εν λόγω υποχρέωση όσο και η προϋποθέσεις προώθησης των δεδομένων, καταγράφονται εντός του PDT-AC αποκάλυψης της πληροφορίας *ECUProductCertification* κατά το βασικό σενάριο χρήσης.

Ο οργανισμός *ECUComp* έχοντας ήδη στη διάθεσή του τα δεδομένα *ECUProductCertification* μπορεί να τα αξιοποιήσει μέσα στα πλαίσια των προδιαγραφόμενων περιορισμών. Μάλιστα, ο κανόνας *Rule#5* επιτρέπει την κατάθεση αιτήματος από χρήστη με τον ρόλο του Υπεύθυνου του Τμήματος Προμηθειών (*PurchasingDepartmentSupervisor*) ενώ εξυπηρετεί τον σκοπό πρόσβασης *RequestForQuotationReply* για την αποκάλυψη της πληροφορίας *ROMAvailability*. Έτσι, σε συνδυασμό με τις διατάξεις του κανόνα *Rule#8* δημιουργείται εκείνη η ροή πληροφοριών που επιτρέπει την αποκάλυψη της διαθεσιμότητας μονάδων μνημών ανάγνωσης που κρίνεται απαραίτητη για τον υπολογισμό της άμεσης διαθεσιμότητας σε Μονάδες Ελέγχου Κινητήρα από τον οργανισμό *ECUComp*. Τέλος, ο κανόνας *Rule#6* επιτρέπει την κατάθεση αιτήματος από υπάλληλο της *ECUComp* στην πλευρά της *RomECUComp* ακόμα κι αν

ενεργοποιεί διαφορετικό ρόλο από αυτόν του *PurchasingDepartmentSupervisor*, αρκεί να ανήκει σε ομάδα εργασίας με συγκεκριμένο αναγνωριστικό (*RFQGroup*). Για την ορθή ολοκλήρωση της σχετικής μεταφοράς των δικαιωμάτων, ο υπάλληλος κατά την ταυτοποίησή του από την ΚΔΕ της *ECUComp* καταθέτει το πιστοποιητικό U-AC όπου πέραν των λοιπών στοιχείων, εμπεριέχονται πληροφορίες για τη συμμετοχή του σε συγκεκριμένες ομάδες εργασίας.

Σημειώνεται ότι, η παρουσίαση περιορίστηκε στην ανάλυση των διαμορφωθέντων κανόνων εξουσιοδότησης που καλύπτουν την επέκταση του βασικού σεναρίου χρήσης καθώς η εκ νέου παρουσίαση όλου του πρωτοκόλλου εξουσιοδότησης θεωρήθηκε περιττή.

9 Συμπεράσματα και Μελλοντική Εργασία

Βασικό έναυσμα για την εξέλιξη της διατριβής αποτέλεσε η ολοένα και αυξανόμενη τάση στις ηλεκτρονικές διαδικασίες, για ψηφιακή αλληλεπίδραση μεταξύ συνεργαζόμενων απομακρυσμένων οντοτήτων και τα προβλήματα εμπιστευτικότητας των διαμοιραζόμενων πληροφοριών που εγγενώς ανακύπτουν. Στο πλαίσιο της διατριβής προδιαγράφηκε και αναπτύχθηκε μια ολοκληρωμένη λύση κατανεμημένου συστήματος, όπου ο διαμοιρασμός πληροφοριών, που σχετίζονται με προσωπικά δεδομένα χρηστών και ευαίσθητα δεδομένα οργανισμών, είναι αντικείμενο διαχείρισης από κατάλληλα κατασκευασμένη μηχανή παραγωγής αποφάσεων εξουσιοδότησης. Πιο συγκεκριμένα, τα διακριτά μέρη που συναπαρτίζουν την προτεινόμενη λύση είναι τα εξής:

- Σημασιολογικό μοντέλο πληροφοριών, με την κατάλληλη εκφραστικότητα για την κάλυψη των αρχών ιδιωτικότητας όπως αυτές αναγνωρίστηκαν και καταγράφηκαν στα πλαίσια της παρούσας διατριβής. Βασικό αντικείμενο του μοντέλου αποτελεί ο ορισμός ρητών κανόνων ελέγχου πρόσβασης, μεταφοράς δικαιωμάτων και προώθησης δεδομένων από τις διακριτές οντότητες του συστήματος. Οι κανόνες μπορούν να αποτυπώνουν τόσο τις προτιμήσεις ιδιωτικότητας χρηστών όσο και τις επιλογές εμπιστευτικότητας ευαίσθητων πληροφοριών οργανισμών.
- Κατανεμημένη υποδομή εμπιστοσύνης, εντός της οποίας η εμπιστοσύνη μεταξύ των εταίρων θεωρείται εξασφαλισμένη και αδιαπραγμάτευτη. Οι οντότητες του συστήματος οργανώνονται σε ένα σχήμα Υποδομής Δημόσιου Κλειδιού και Υποδομής Διαχείρισης Δικαιωμάτων με ενσωμάτωση μιας Αρχής Πιστοποίησης Γέφυρας.
- Προηγμένη μηχανή παραγωγής αποφάσεων, που εργάζεται στη βάση πλαισίου ιδιωτικότητας που περιλαμβάνει τους δηλωθέντες κανόνες και προτιμήσεις των χρηστών του συστήματος, των οργανισμών-παρόχων της Συνομοσπονδίας και του Επικεφαλής της Συνομοσπονδίας καθώς και τις τρέχουσες τιμές δυναμικών, χωρικών, χρονικών και σχετικών με την υποκείμενη υποδομή μεταβλητών. Κύριο αντικείμενο της μηχανής είναι η εξομάλυνση και αποσαφήνιση των αποφάσεων εξουσιοδότησης της κάθε οντότητας του συστήματος σε χρόνο πριν την έναρξη του συστήματος αλλά

και ο συγκερασμός των διαφορετικών πολιτικών εξουσιοδότησης μεταξύ διακριτών πηγών κανόνων σε πραγματικό χρόνο. Προς τούτο, αναπτύχθηκε εξειδικευμένο λογισμικό παραγωγής συλλογισμών κατάλληλα προσαρμοσμένο στις απαιτήσεις του προτεινόμενου συστήματος.

- Οργάνωση των διαδικασιών εξουσιοδότησης και διαμοιρασμού πληροφοριών σε πρωτόκολλο εξουσιοδότησης και κωδικοποίηση σε κατάλληλα ψηφιακά πιστοποιητικά των διαφορετικών καταστάσεων του συστήματος και των σχέσεων των εμπλεκόμενων οντοτήτων.

Οι παραπάνω έννοιες και οι συνεπαγόμενες ενέργειες ανάπτυξης συστημάτων παρουσιάστηκαν αναλυτικά στα διακριτά κεφάλαια της διατριβής. Οι βασικές συνεισφορές της προτεινόμενης λύσης και συνεπώς της διατριβής στην τρέχουσα επιστημονική δραστηριότητα έγκεινται στα εξής:

- Η δυνατότητα ορισμού κανόνων ελέγχου πρόσβασης σε δεδομένα, μεταφοράς δικαιωμάτων πρόσβασης αλλά και περαιτέρω προώθησης δεδομένων σε τρίτες οντότητες στη βάση ενός σημασιολογικού μοντέλου πληροφοριών που ενσωματώνει τις θεμελιώδεις έννοιες που απορρέουν από τη νομοθεσία περί ιδιωτικότητας αλλά και διαδεδομένων προτύπων ασφάλειας.
- Η από κοινού διαχείριση των προτιμήσεων ιδιωτικότητας χρηστών και των προτιμήσεων εμπιστευτικότητας ευαίσθητων πληροφοριών οργανισμών, είτε οι τελευταίοι ενεργοποιούνται ως πάροχοι υπηρεσιών είτε ως πάροχοι υπηρεσιών, τόσο από την άποψη των σημασιολογικών μηχανισμών προδιαγραφής κανόνων εξουσιοδότησης όσο και από την άποψη των διαδικασιών επικοινωνίας μεταξύ των οντοτήτων. Με αυτόν τον τρόπο, επιτυγχάνεται μια συμμετρική αντιμετώπιση του προβλήματος που επιτρέπει τη μείωση της πολυπλοκότητας των διαδικασιών αλλά και του υπολογιστικού κόστους διαχείρισης των εξουσιοδοτήσεων.
- Η δυνατότητα κλιμακωτής προσαρμογής του επιπέδου της εμπιστοσύνης που επιτυγχάνεται μεταξύ των οντοτήτων βάσει της ποιότητας των πολιτικών πιστοποίησης που αξιοποιούν, ως αποτέλεσμα της ενεργοποίησης του σχήματος της Αρχής Πιστοποίησης Γέφυρας. Η εν λόγω επιλογή παρουσιάζει επίσης πλεονεκτήματα μεγαλύτερης κλιμακοθετησιμότητας έναντι παραδοσιακών σχημάτων Υποδομής Δημόσιου Κλειδιού, ενώ διευκολύνονται περιφερειακές ενέργειες των Αρχών Πιστοποίησης, όπως είναι η πιθανή άρση

της εμπιστοσύνης προς επιλεγμένους κόμβους, χωρίς αυτό να συνεπάγεται κάτι για τη λειτουργία της υποδομής.

- Η εξασφάλιση σημασιολογικής διαλειτουργικότητας κατά την προδιαγραφή κανόνων εξουσιοδότησης, καθώς για την εν λόγω ενέργεια οι οντότητες εργάζονται στη βάση τοπικών αντιγράφων μια κοινής οντολογίας. Επίσης, παρέχεται η δυνατότητα τροποποίησης επιμέρους αντικειμένων, υπό την προϋπόθεση της παραγωγής σημασιολογικών ισοδυναμιών αξιοποιώντας ως αναφορά τα αντικείμενα της κοινής οντολογίας.
- Η δυνατότητα εφαρμογής ελέγχου εξουσιοδότησης σε δύο διακριτές φάσεις (χωρίς η εν λόγω ενέργεια να είναι δεσμευτική), στην πλευρά του παρόχου ταυτοτήτων και στην πλευρά του παρόχου υπηρεσιών. Η δυνατότητα αυτή συνεπάγεται την κάλυψη περιπτώσεων, όπου η ίδια η κατάθεση αιτημάτων για πρόσβαση σε δεδομένα μπορεί να υπόκειται σε έλεγχο εξουσιοδότησης από τα εμπλεκόμενα μέλη.
- Η απόκρυψη ταυτοποιητικών στοιχείων κατά την παροχή υπηρεσιών στους αντίστοιχους παρόχους, καθώς αξιοποιώντας δομές ψηφιακών πιστοποιητικών οι οντότητες του συστήματος αποκτούν δικαιώματα πρόσβασης σε δεδομένα, αποκαλύπτοντας αναγνωριστικά στοιχεία που ταυτοποιούν αποκλειστικά τα αιτήματά τους και όχι τις ίδιες (untraceability). Επίσης, οι πάροχοι υπηρεσιών δεν μπορούν να συνδυάσουν τις κινήσεις των χρηστών (unlinkability) ενώ από την πλευρά τους οι χρήστες δεν μπορούν να επαναχρησιμοποιήσουν τα δικαιώματά πρόσβασης σε χρόνο μη επιτρεπτό (non-reusability) ή να μεταφέρουν τα δικαιώματα τους σε άλλες οντότητες (non-transferability). Ταυτόχρονα, η στρατηγική της μεταφοράς μέρους της επιχειρηματικής λογικής των παρόχων εντός της πλατφόρμας περιορίζει περαιτέρω την αποκάλυψη ευαίσθητων και προσωπικών δεδομένων στους παρόχους.
- Η υποστήριξη μεγαλύτερης κλιμακοθετησιμότητας κατά την προδιαγραφή των κανόνων εξουσιοδότησης που προκύπτει από την αξιοποίηση τεχνολογίας οντολογιών αλλά και κατά τη εξαγωγή συμπερασμάτων εξουσιοδότησης λόγω του σαφούς διαχωρισμού των εμπλεκόμενων διαδικασιών σε «στατικό» και «δυναμικό» μέρος. Το μεγαλύτερο και υπολογιστικά πιο χρονοβόρο τμήμα των διαδικασιών συλλογισμού διενεργείται σε χρόνο πριν την εκκίνηση του συστήματος, ενώ διατηρείται εκείνη η ευελιξία που επιτρέπει την προσαρμογή

του συστήματος σε μεταβολές του περιβάλλοντος χρήσης σε πραγματικό χρόνο.

Η τρέχουσα και μελλοντική ερευνητική εργασία για την επέκταση της διατριβής κινείται στους ακόλουθες άξονες:

- Αξιοποίηση τεχνικών αποδείξεων μηδενικής γνώσης (Zero Knowledge Proofs). Οι αποδείξεις μηδενικής γνώσης αξιοποιούνται σε κρυπτογραφικά πρωτόκολλα αλληλεπίδρασης, όπου μια οντότητα-διεκδικητής καλείται να επιβεβαιώσει σε μια οντότητα-επαληθευτή την ορθότητα και την ισχύ μιας πρότασης, με τρόπο τέτοιο που δεν φανερώνει καμία επιπρόσθετη πληροφορία εκτός της εγκυρότητας αυτής καθεαυτής [128]. Οι αποδείξεις μηδενικής γνώσης μπορούν να αξιοποιηθούν κατά τη φάση της προσκόμισης των προσωπικών πιστοποιητικών ταυτότητας και ιδιοτήτων από τους χρήστες στους παρόχους ταυτοτήτων με στόχο την ανώνυμη αυθεντικοποίησή τους και την παροχή ενός πλήρως ανώνυμου κρυπτογραφικού πρωτοκόλλου.
- Ενσωμάτωση προηγμένων στρατηγικών διαπραγματεύσεων εμπιστοσύνης (trust negotiations) [129] με στόχο την οργάνωση της ανταλλαγής πληροφοριών μεταξύ των παρόχων βάσει κανόνων αποκάλυψης των ίδιων των πολιτικών εξουσιοδότησης. Με αυτόν τον τρόπο η λήψη αποφάσεων αποκάλυψης δεδομένων δεν επηρεάζεται μόνο από τη σημαντικότητα των δεδομένων αλλά και από τη βαρύτητα των ίδιων των κανόνων που πραγματεύονται την αποκάλυψή τους, δημιουργώντας έτσι προηγμένες στρατηγικές διαπραγμάτευσης εμπιστοσύνης.
- Ενσωμάτωση προηγμένων στρατηγικών σημασιολογικής ισοδυναμίας, με στόχο τη διεύρυνση των δικαιωμάτων επεξεργασίας της κοινής οντολογικής βάσης προδιαγραφής κανόνων από τις οντότητες του συστήματος. Αν και η προτεινόμενη λύση εκμεταλλεύεται τις δυνατότητες καταγραφής σημασιολογικών ισοδυναμιών σε ψηφιακά πιστοποιητικά, σύμφωνα με τις οδηγίες του προτύπου X.509, η ενσωμάτωση περισσότερο προηγμένων τεχνικών ευθυγράμμισης οντολογιών [130] μπορεί να αναδείξει την ποιότητα του πρωτοκόλλου εξουσιοδότησης αλλά και να επιτρέψει τη λειτουργία της πλατφόρμας εκτός ενός αυστηρά ορισμένου περιβάλλοντος Υποδομών Δημοσίου Κλειδιού.

10 Αναφορές

[1] The Gallup Organization, «Data protection in the European Union: Citizens' perceptions – Analytical Report», Flash Eurobarometer 225, February 2008.

[2] TNS Opinion & Social, «Attitudes on Data Protection and Electronic Identity in the European Union», Special Eurobarometer 359, June 2011.

[3] W. Jianga, M. Baumgarten, Q. Dai and Y. Zhou, «The deployment and evaluation of a bioinformatics grid platform – The HUST_Bio_Grid», *Computers & Electrical Engineering*, May 2011.

[4] M. B. Geetha Manjusha, S. Jaganathan and A. Srinivasan, «gBeL: An Efficient Framework for e-Learning Using Grid Technology», in *Computer Networks and Information Technologies, Communications in Computer and Information Science*, Springer Berlin Heidelberg, pp. 63-83, 2011.

[5] S. Murugesan, «Cloud Computing Gives Emerging Markets a Lift», *IT Professional*, Volume 13, Issue 6, pp. 60-62 , November-December 2011.

[6] T. Hong-Linh and D. Schahram, «Cloud computing for small research groups in computational science and engineering: current status and outlook», *Computing*, Volume 91, Issue 1, pp. 75-91, January 2011.

[7] N. A. Sultan, «Reaching for the "cloud": How SMEs can manage», *International Journal of Information Management*, Volume 31, Issue 3, pp. 272-278, June 2011.

[8] T. Oreilly, «What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software», Available: http://oreilly.com/web2/archive/what-is-web-20.html, 30 September 2005 [1 January 2012].

[9] A. Mcafee, «Enterprise 2.0: the dawn of emergent collaboration», *Engineering Management Review, IEEE* , Volume 34, Issue 3, pp. 38-38, Third Quarter 2006.

[10] M. Sigala, «Preface: Special Issue on Web 2.0 in travel and tourism: Empowering and changing the role of travelers», *Computers in Human Behavior*, Volume 27, Issue 2, pp. 607-608, March 2011.

[11] Y. Wang, A. Greaseley and E. Thanassoulis, «Combining ERP systems with Enterprise 2.0», in *Enterprise Information Systems, Communications in Computer and Information Science*, Springer Berlin Heidelberg, pp. 198-207, 2011.

[12] S. Ba and P. Pavlou, «Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior», *MIS Quarterly*, Volume 26, Issue. 3, pp. 243-268, September 2002 .

[13] P. Beatty, I. Reay, S. Dick and J. Miller, «Consumer trust in e-commerce web sites: A meta-study», *ACM Computing Surveys*, Volume 43, Issue 3, pp. 14:1-14:46, April 2011.

[14] F. D. Schoorman, R. C. Mayer and J. H. Davis, «An integrative model of organizational trust: Past, present, and future», *Academy of Management Review*, Volume 32, Issue 2, pp. 344-354, 2007.

[15] P. Datta and S. Chatterjee, «Online consumer market inefficiencies and intermediation», *SIGMIS Database*, Volume 42, Issue 2, pp. 55-75, May 2011.

[16] S. D. Warren and L. D. Brandeis, «The Right to Privacy», *Harvard Law Review*, Volume IV, No. 5, pp. 193-220, December 1890.

[17] Ηνωμένα Έθνη, «Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα», Απόφαση 217 Α (III), 10 Δεκεμβρίου 1948.

[18] A. Acquisti, «The Economics of Personal Data and the Economics of Privacy», OECD Conference Centre. WPISP-WPIE Roundtable, 2010.

[19] Συμβούλιο της Ευρώπης, «Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου», 4 Νοεμβρίου 1950.

[20] Ηνωμένα Έθνη, «Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα», Απόφαση 2200 Α (XXI), 16 Δεκεμβρίου 1966.

[21] Ζ' Αναθεωρητική Βουλή των Ελλήνων, «Το Σύνταγμα της Ελλάδας», Αθήνα, 6 Απριλίου 2001.

[22] Βουλή των Ελλήνων, «Νόμος 2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 50, 10 Απριλίου 1997.

[23] Βουλή των Ελλήνων, «Νόμος 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των

ηλεκτρονικών επικοινωνιών και τροποποίηση του Νόμου 2472/1997», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 133, 28 Ιουνίου 2006.

[24] Βουλή των Ελλήνων, «Νόμος 3917/2011: Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 22, 21 Φεβρουαρίου 2011.

[25] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, «Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών», *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 281, σελ. 31-50, Νοέμβριος 1995.

[26] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, «Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)», *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 201, σελ. 37 – 47, Ιούλιος 2002.

[27] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, «Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ», *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 105, σελ. 54-63, Απρίλιος 2006.

[28] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Available: http://www.dpa.gr

[29] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, Available: http://www.adae.gr.

[30] Βουλή των Ελλήνων, «Νόμος 3115/2003: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Τεύχος Πρώτο, Αρ. Φύλλου 47, 27 Φεβρουαρίου 2003.

[31] Organisation for Economic Co-operation and Development, «Guidelines on the Protection of Privacy and Transborder Flows of Personal Data», September 1980.

[32] Organisation for Economic Co-operation and Development, Available: http://www.oecd.org/

[33] D. J. Solove, «A Brief History of Information Privacy Law», in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, Practising Law Institute, pp. 1-46, 2006

[34] Ομοσπονδιακή Συνέλευση, «Σύνταγμα των Ηνωμένων Πολιτειών», 17 Σεπτεμβρίου 1787.

[35] Act of Congress, «Privacy Act», *United States Code*, Title 5, Paragraph 552a, 31 December 1974.

[36] United States Congress, «Health Insurance Portability and Accountability Act of 1996», *Public Law 104-191*, 21 August 1996.

[37] Ευρωπαϊκή Επιτροπή, «Ψηφιακό θεματολόγιο για την Ευρώπη», Ανακοίνωση της Επιτροπής Προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Βρυξέλλες, 26 Αυγούστου 2010.

[38] Ευρωπαϊκή Επιτροπή, «Ευρώπη 2020: Στρατηγική για έξυπνη, διατηρήσιμη και χωρίς αποκλεισμούς ανάπτυξη», Ανακοίνωση της Επιτροπής, Βρυξέλλες, 3 Μαρτίου 2010.

[39] European Network and Information Security Agency, Available: http://www.enisa.europa.eu.

[40] International Organization for Standardization, Available: http://www.iso.org/iso/home.html.

[41] International Electrotechnical Commission, Available: http://www.iec.ch.

[42] International Organization for Standardization, «Information technology-Security techniques-Information security management systems-Requirements», ISO/IEC 27001:2005, October 2005.

[43] International Organization for Standardization, «Information technology-Security techniques-Code of practice for information security management», ISO/IEC 27002:2005, June 2005.

[44] International Organization for Standardization, «Information technology-Security techniques-Information security risk management», ISO/IEC 27005:2011, June 2011.

[45] National Institute of Standards and Technology, Available: http://www.nist.gov/index.html.

[46] National Institute of Standards and Technology, «Generally Accepted Principles and Practices for Securing Information Technology Systems», Special Publication 800-14, September 1996.

[47] National Institute of Standards and Technology, «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)», Special Publication 800-122, April 2010.

[48] National Institute of Standards and Technology, «Guidelines on Security and Privacy in Public Cloud Computing», Special Publication 800-144, December 2011.

[49] Information Security Forum, Available: https://www.securityforum.org

[50] Information Security Forum, «The Standard of Good Practice for Information Security», 2007.

[51] Information Security Forum, «The 2011 Standard of Good Practice for Information Security», 2011.

[52] Eurostat, «Information and Communication Technologies in the EU27», STAT/10/187, 9 December 2010.

[53] P. Ratnasingam, «Trust in Inter-Organizational Exchanges: A Case Study in Business to Business Electronic Commerce», *Decision Support Systems*, Volume 39, Issue 3, pp. 525-544, May 2005.

[54] W. Diffie and M. Hellman, «New Directions in Cryptography», *IEEE Transactions on Information Theory*, Volume 22, Issue 6, pp. 644-654, November 1976.

[55] P. R. Zimmermann, «The Official PGP User's Guide», Cambridge, MIT Press, May 1995, pp. 216.

[56] Telecommunication Standardization Sector of International Telecommunication Union, «Information technology – Open systems

interconnection – The Directory: Public-key and attribute certificate frameworks», ITU-T Recommendation X.509, November 2008.

[57] International Telecommunication Union, Available: http://www.itu.int/en/Pages/default.aspx.

[58] W. T. Polk, N. E. Hastings and A. Malpani, «Public Key Infrastructures that Satisfy Security Goals», *IEEE Internet Computing*, Volume7, Issue 4, pp. 60-67, July – August 2003.

[59] M. Shimaoka, N. Hastings and R. Nielsen, «Memorandum for Multi-Domain Public Key Infrastructure Interoperability», IETF RFC 5217 (Informational), July 2008.

[60] European Bridge CA, Available: https://www.ebca.de/en

[61] Federal Public Key Infrastructure, Available: http://www.idmanagement.gov/pages.cfm/page/Federal-PKI

[62] D.F. Ferraiolo, R. Sandhu, S. Gavrila, R.D. Kuhn and R. Chandramouli, «Proposed NIST Standard for Role-Based Access Control», *ACM Transactions on Information and System Security*, Volume 4, Issue 3, pp.224-274, August 2001.

[63] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, «Hippocratic databases», in *Proceedings of the 28th International Conference on Very Large Databases (VLDB' 2002)*, Hong Kong, China, August 20 – 23, 2002.

[64] J. Byun, E. Bertino and N. Li, «Purpose Based Access Control of Complex Data for Privacy Protection», in *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT 'O5)*, 2005, pp. 102-110.

[65] A. Masoumzadeh and J. B. D., «PuRBAC: Purpose-Aware Role-Based Access Control», in *On the Move to Meaningful Internet Systems: OTM 2008, Lecture Notes in Computer Science*, Berlin, Germany: Springer Berlin / Heidelberg, pp. 1104-1121, 2008.

[66] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. M. Karat, J. Karat and A. Trombetta, «Privacy-aware role based access control», in *Journal of ACM Transactions Information System Security*, Volume 13, Issue 3, pp. 1-31, 2010.

[67] E. Bertino, B. Catania, M. L. Damiani and P. Perlasca, «GEO-RBAC: A Spatially Aware RBAC», in *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT '06)*, 2006, pp. 29-37.

[68] J. B. D. Joshi, E. Bertino, U. Latif and A. Ghafoo, «A Generalized Temporal Role-Based Access Control Model», *Journal of IEEE Transactions on Knowledge and Data Engineering*, Volume 17, Issue 1, pp. 4-23, January 2005.

[69] A. N. Ravari, J. H Jafarian, M. Amini and R. Jalili, «GTHBAC: A Generalized Temporal History Based Access Control Model», *Journal of Telecommunication Systems*, Volume 45, Issue 2, pp. 111-125, 2010.

[70] A. N. Ravari, M. Amini, R. Jalili and J. H. Jafarian, «A History Based Semantic Aware Access Control Model using Logical Time», in *Proceedings of the 11th International Conference on Computer and Information Technology (ICCIT 2008)*, 2008, pp. 43-50.

[71] World Wide Web Consortium, OWL Web Ontology Language Overview, W3C Recommendation, 10 February 2004, Available: http://www.w3.org/TR/owl-features.

[72] F. Couppens and N. Cuppens-Boulahia, «Modeling Contextual Security Policies», *International Journal of Information Security*, Vol. 7, No. 4, pp. 285-305, July 2008.

[73] N. Ajam, N. Cuppens-Boulahia and F. Cuppens, «Contextual Privacy Management in Extended Role Based Access Control Model», in *Data Privacy Management and Autonomous Spontaneous Security*, Berlin, Germany: Springer Berlin/Heidelberg, pp. 121-135, 2010.

[74] F. Cuppens, N. Cuppens-Boulahia and M. B. Ghorbel, «High Level Conflict Management Strategies in Advanced Access Control Models», *Journal of Electronic Notes in Theoretical Computer Science*, Volume 186, pp. 3-26, July 2007.

[75] R. Bhatti, A. Ghafoor, E. Bertino and J. B. D. Joshi, «X-GTRBAC: An XML-Based Policy Specification Framework and Architecture for Enterprise-Wide Access Control», *Journal of ACM Transactions of Information and System Security*, Volume *8*, Issue 2, pp. 187-227, May 2005.

[76] World Wide Web Consortium, Extensible Markup Language (XML), W3C Recommendation, 26 November 2008.

[77] Organization for the Advancement of Structured Information Standards, Extensible Access Control Markup Language.

[78] Organization for the Advancement of Structured Information Standards, Available: http://www.oasis-open.org.

[79] Internet Engineering Task Force, Available: http://www.ietf.org.

[80] D. A. Haidar, N. Cuppens-Boulahia, F. Cuppens and H. Debar, «An Extended RBAC Profile of XACML», in *Proceedings of the 3rd ACM workshop on Secure web services (SWS '06)*, 2006, pp. 13-22.

[81] M. Blaze, J. Feigenbaum and J. Lacy, «Decentralized Trust Management», in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, 1996, pp. 164-173).

[82] S. Weeks, «Understanding Trust Management Systems», in *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, 2001, pp. 94-105.

[83] M. Blaze, J. Feigenbaum, J. Ioannidis and A. D. Keromytis, «The keyNote Trust Management System Version 2», IETF RFC 2704 (Informational), September 1999.

[84] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas and T. Ylonen, «SPKI certificate theory», IETF RFC 2693 (Experimental), September 1999.

[85] M.Y. Becker, and P. Sewell, «Cassandra: Distributed Access Control Policies with Tunable Expressiveness», in *Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks*, 2004, pp. 159-168.

[86] Middleware Architecture Committee for Education (MACE), Shibboleth System, Available: http://shibboleth.internet2.edu/.

[87] Organization for the Advancement of Structured Information Standards, «Security Assertion Markup Language (SAML) v2.0», *OASIS Standard*, March 2005, Available: http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip.

[88] T. Dierks and E. Rescorla, «The Transport Layer Security (TLS) Protocol Version 1.2», IETF RFC 5246 (Standards Track), August 2008.

[89] M. R. Thompson, A. Essiari and S. Mudumbai, «Certificate-based authorization policy in a PKI environment», *ACM Transactions on Information and System Security*, Volume 6, Issue 4, pp. 566-588, November 2003.

[90] D. Chadwick, G. Zhao, S. Otenko, R. Laborde, L. Su, Linying and T. A. Nguyen, «PERMIS: a modular authorization infrastructure», *Concurrency*

and Computation: Practice & Experience, Volume 20, Issue 11, pp. 1341-1357, August 2008.

[91] N. Zhang, L. Yao, A. Nenadic, J. Chin, C. Goble, A. Rector, D. Chadwick, S. Otenko and Q. Shi; «Achieving Fine-grained Access Control in Virtual Organisations», *Concurrency and Computation: Practice and Experience*, Volume 19, Issue 9, pp. 1333-1352, June 2007.

[92] K. Fatema, D. W. Chadwick and S. Lievens, «A Multi-privacy Policy Enforcement System», in *IFIP Advances in Information and Communication Technology, Privacy and Identity Management for Life*, Springer Boston, pp. 297-310, 2011.

[93] G. Karjoth, M. Schunter and M. Waidner, «Platform for enterprise privacy practices: privacy-enabled management of customer data», in *Proceedings of the 2nd international conference on Privacy enhancing technologies*, 2003, pp. 69-84.

[94] D. W. Chadwick and K. Fatema, «A privacy preserving authorisation system for the cloud», *Journal of Computer and System Sciences*, 2011.

[95] FP6 IST project PRIME (Privacy and Identity Management for Europe), Available: https://www.prime-project.eu.

[96] C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati and P. Samarati, «A privacy-aware access control system», *Journal of Computer Security*, Volume 16, Issue 4, pp. 369-397, September 2008.

[97] L. Bauer, M. A. Schneider, and E. W. Felten, «A proof-carrying authorization system», *Department of Computer Science, Princeton University*, Technical Report CS-TR-638-01, 2001.

[98] L. Bauer, M. A. Schneider, E. W. Felten, and A.W. Appel, «Access control on the Web using proof-carrying authorization», in *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, 2003, pp.117-119.

[99] M. Maffei and K. Pecina, «Privacy-aware proof-carrying authorization», in *Proceedings of the ACM SIGPLAN 6th Workshop on Programming Languages and Analysis for Security*. *ACM*, 2011.

[100] M.C. Mont, S. Pearson and P. Bramhall, «Towards accountable management of identity and privacy: sticky policies and enforceable tracing services», in

Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on, 2003, pp.377-382.

[101] European Opinion Research Group, «Attitudes on Data Protection and Electronic Identity in the European Union», Technical Report Special Eurobarometer 359, European Commission. Bruxelles, Belgium, 2011.

[102] H. Österle, E. Fleisch, and R. Alt, «Business networking: Shaping enterprise relationships on the internet», ISBN: 3- 540- 66612- 5, Springer, 1999.

[103] W.T. Polk, N.E. Hastings and A. Malpani, «Public key infrastructures that satisfy security goals», *IEEE Internet Computing*, Volume 7, pp. 60–67, July 2003.

[104] J.J. Borking, «Why adopting privacy enhancing technologies (pets) takes so much time», in *Computers, Privacy and Data Protection: an Element of Choice*, S. Gutwirth, Y. Poullet, P. De Hert, R. Leenes (eds.), Springer Netherlands, pp. 309–341, 2011.

[105] R. Dhamija and L. Dusseault, «The seven flaws of identity management: Usability and security challenges», *IEEE Security and Privacy*, Volume 6, pp. 24–29, March 2008.

[106] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zhao, R. Chilro, and L. Antunes, in «How to securely break into RBAC: the BTG-RBAC model», in *Annual Computer Security Applications Conference*, 2009, pp. 23-31.

[107] The World Wide Web Consortium (W3C), «Web Ontology Language (OWL)», W3C Recommendation 10 February 2004.

[108] The World Wide Web Consortium (W3C), homepage: http://www.w3.org/.

[109] The World Wide Web Consortium (W3C), «Resource Description Framework (RDF)», W3C Recommendation 10 February 2004.

[110] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, «Κανονισμός 2195/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Νοεμβρίου 2002 περί του κοινού λεξιλογίου για τις δημόσιες συμβάσεις», Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, Αρ. L. 340, σελ. 1-562, Δεκέμβριος 2006.

[111] North American Industry Classification System (NAICS), United States Census Bureau, 2012, Available: http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

[112] W. Samer, L. Romain, B. Francois and B. AbdelMalek, «A formal model of trust for calculating the quality of x.509 certificate», in *Security and Communication Networks*, Volume:4, pp. 651–665, 2011.

[113] E. Sirin, Evren, B. Parsia, B.C. Grau, A. Kalyanpur, and Y. Katz, «Pellet: A practical owl-dl reasoned», in *Web Semantics: science, services and agents on the World Wide Web* Volume:5, pp. 51-53, 2007.

[114] Jena – A Semantic Web Framework for Java, Available: http://jena.apache.org/

[115] International Telecommunication Union, «X.509: Information Technology-open systems interconnection-the directory: Public-key and attribute certificate frameworks» ITU-T Recommendation, 2008.

[116] D. Crockford, «RFC-4627: The application/json Media Type for JavaScript Object Notation (JSON)», Internet Engineering Task Force Request For Comments, 2006.

[117] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, «RFC-2616: Hypertext Transfer Protocol -- HTTP/1.1», Internet Engineering Task Force Request For Comments, 1999.

[118] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, «RFC-2616: Hypertext Transfer Protocol -- HTTP/1.1», Internet Engineering Task Force Request For Comments, 1999.

[119] E. Rescorla, "RFC-2818: HTTP Over TLS", Internet Engineering Task Force Request For Comments, 2000.

[120] J. Linn, «RFC-1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures», Internet Engineering Task Force Request For Comments, 1993.

[121] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "RFC-2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", Internet Engineering Task Force Request For Comments, 1999.

[122] Java Community Process, «JSR 220: Enterprise JavaBeans™ 3.0», Java Specification Requests, 2007.

[123] The Legion of the Bouncy Castle, Available: http://www.bouncycastle.org/

[124] JavaBeans Open Source Software Application Server, Available: http://www.jboss.org/

[125] T. Dierks and E. Rescorla, "RFC-5246: The Transport Layer Security (TLS) ProtocolVersion 1.2", Internet Engineering Task Force Request For Comments, 2008.

[126] Java Secure Socket Extension, Available: docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html

[127] Java Universal Network/Graph Framework, Available: http://jung.sourceforge.net/

[128] J. Camenisch, and A. Lysyanskaya, «An efficient system for non-transferable anonymous credentials with optional anonymity revocation», in *Advances in Cryptology—EUROCRYPT 2001*, Springer, Berlin, Heidelberg, 2001, pp. 93-118.

[129] A. Squicciarini, E. Bertino, E. Ferrari, F. Paci and B. Thuraisingham, «PP-trust-X: A system for privacy preserving trust negotiations», in *ACM Transactions on Information and System Security (TISSEC)*, Volume:10, 2007.

[130] J. Euzenat, and P. Shvaiko, «Ontology matching», ISBN: 978-3-540-49611-3, Springer, 2007.