ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Εγγενής Ενσωμάτωση Ιδιωτικότητας σε Τεχνολογίες Λογισμικού Προσανατολισμένου σε Υπηρεσίες

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μαρία Ν. Κουκοβίνη

Αθήνα, Δεκέμβριος 2013

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο --- ΕΚΤ) και από εθνικούς πόρους μέσω του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» του Εθνικού Στρατηγικού Πλαισίου Αναφο-ράς (ΕΣΠΑ) --- Ερευνητικό Χρηματοδοτούμενο Έργο: Ηράκλειτος ΙΙ. Επένδυση στην κοινωνία της γνώσης μέσω του Ευρωπαϊκού Κοινωνικού Ταμείου.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Εγγενής Ενσωμάτωση Ιδιωτικότητας σε Τεχνολογίες Λογισμικού Προσανατολισμένου σε Υπηρεσίες

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μαρία Ν. Κουκοβίνη

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

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 16η Δεκεμβρίου 2013

.....	.....	.....
Δ.-Θ. Ι. Κακλαμάνη	Ν. Κ. Ουζούνογλου	Ι. Στ. Βενιέρης
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
.....	.....	.....
Σ. Κ. Κάτσικας	Γ. Στασινόπουλος	Γ. Μεντζάς
Καθηγητής Παν. Πειραιά	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

.....
Δ. Φωτάκης
Λέκτορας Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2013

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο — ΕΚΤ) και από εθνικούς πόρους μέσω του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (ΕΣΠΑ) — Ερευνητικό Χρηματοδοτούμενο Έργο: *Ηράκλειτος ΙΙ. Επένδυση στην κοινωνία της γνώσης μέσω του Ευρωπαϊκού Κοινωνικού Ταμείου*.

.....
Μαρία Ν. Κουκοβίνη
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Τα συστήματα λογισμικού προσανατολισμένου σε υπηρεσίες συνιστούν κυρίαρχη αρχιτεκτονική προσέγγιση στα σύγχρονα κατανεμημένα, ετερογενή και δυναμικά περιβάλλοντα. Οι σχετικές τεχνολογίες, ωστόσο, θέτουν συχνά σε κίνδυνο την ιδιωτικότητα, καθώς από τη φύση τους βασίζονται σε μεγάλο βαθμό στην πρόσβαση σε και στην ανταλλαγή δεδομένων. Στο πλαίσιο αυτό, η διατριβή πραγματεύεται την προστασία της ιδιωτικότητας μέσω της εγγενούς ενσωμάτωσης των σχετικών μηχανισμών σε συστήματα λογισμικού βασισμένου σε υπηρεσίες, και ειδικότερα σε περιβάλλοντα ροών εργασιών. Ο στόχος αυτός, καθώς και η ακολουθούμενη προσέγγιση βρίσκονται σε συμφωνία με την αναδυόμενη τάση, τόσο νομική όσο και τεχνολογική, στον τομέα της ιδιωτικότητας που είθισται να αναφέρεται ως "ιδιωτικότητα εκ σχεδιασμού" (Privacy by Design).

Προκειμένου να πετύχει το στόχο, η διατριβή πραγματεύεται μια σειρά από θέματα και προδιαγράφει τις αντίστοιχες τεχνολογικές λύσεις. Δεδομένου ότι επιδιώκεται η εφαρμογή των απαιτήσεων της Νομοθεσίας αναφορικά με τη συλλογή και χρήση προσωπικών δεδομένων, αρχικά πραγματοποιείται επισκόπηση του σχετικού Ευρωπαϊκού και Εθνικού Νομικού και Κανονιστικού Πλαισίου, το οποίο αποτελεί την αφετηρία για τη σχεδίαση των προτεινόμενων λύσεων. Έτσι, στη βάση της Νομοθεσίας και των υφιστάμενων τεχνολογιών, πραγματοποιείται συστηματική τεκμηρίωση των ιδιαίτερων τεχνικών απαιτήσεων που διέπουν τις τεχνολογίες ροών εργασιών, λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά τους.

Η προτεινόμενη λύση αποτελείται από ένα σύνολο πρωτότυπων μηχανισμών, ο συνδυασμός των οποίων επιτυγχάνει την ικανοποίηση των εν λόγω απαιτήσεων. Κατ' αρχάς, δεδομένης της αδυναμίας των υφιστάμενων τεχνολογιών μοντελοποίησης ροών εργασιών να συμπεριλάβουν δομές για τον ορισμό πολιτικών ιδιωτικότητας, προτείνεται ένα καινοτόμο μοντέλο ροών εργασιών. Επιπρόσθετα, στη βάση του μοντέλου αυτού και σε συνδυασμό με τα κατάλληλα μοντέλα πληροφοριών και προδιαγραφής κανόνων ελέγχου πρόσβασης και χρήσης, αναπτύσσεται μεθοδολογία η οποία πραγματοποιεί έλεγχο των ροών εργασιών αναφορικά με τη συμμόρφωσή τους με τις αρχές της ιδιωτικότητας, καθώς και τις κατάλληλες τροποποιήσεις προκειμένου η συμμόρφωση να επιτευχθεί. Τέλος, σε ό,τι αφορά την εκτέλεση των ροών εργασιών, η διατριβή προδιαγράφει όλους τους απαραίτητους μηχανισμούς για τη συνακόλουθη εφαρμογή των ανωτέρω αποτελεσμάτων στο

περιβάλλον εκτέλεσης. Η διατριβή περιλαμβάνει ακόμα τεκμηριωμένη αξιολόγηση των προτάσεών της, και ολοκληρώνεται με τα σημαντικότερα συμπεράσματα που προκύπτουν καθώς και με την παρουσίαση των μελλοντικών επεκτάσεων των αποτελεσμάτων της.

Λέξεις κλειδιά: Ιδιωτικότητα, ιδιωτικότητα εκ σχεδιασμού, τεχνολογίες λογισμικού προσανατολισμένου σε υπηρεσίες, ροή εργασιών, Νομοθεσία προστασίας προσωπικών δεδομένων, απαιτήσεις ιδιωτικότητας, σχεδιασμός μοντέλου ροής εργασιών, επαλήθευση ροών εργασιών, εκτέλεση ροών εργασιών με επίγνωση ιδιωτικότητας, σημασιολογικό μοντέλο, οντολογία.

Abstract

Service-oriented architectures constitute a prominent technology in current distributed, heterogeneous and dynamic environments. However, they are in many cases characterised by serious privacy implications, since they natively rely to a large extent on access to and exchange of data. This thesis addresses in particular the realisation of the emerging trend of Privacy by Design in service-oriented workflow systems, ensuring that they are rendered inherently privacy-aware.

Towards achieving the above, a number of issues are investigated and the corresponding solutions are devised. Given that the ultimate goal is the enforcement of the regulatory provisions ruling on personal data collection and usage, an overview of the European and National Legal and Regulatory framework is provided, constituting the starting point for the proposed solution. Thus, with active legislation and current state-of-the-art as a baseline, the derived requirements in the context of workflow environments are elaborated upon, taking into account the particular needs and implications of the latter.

The proposed solution addresses said requirements through the combination of a number of innovative mechanisms. To begin with, in view of the inability of existing workflow modelling technologies to include structures for the specification of privacy policies as part of workflow definition, a novel comprehensive workflow modelling approach is proposed. On the basis of this approach, combined with the appropriate information model and an access and usage control model reflecting applicable privacy provisions, the thesis further presents a procedure for the automatic verification of workflow models and their subsequent transformation, if needed, so that they become inherently privacy-aware before being deployed for execution. Finally, the appropriate mechanisms for the consistent execution of workflows following their privacy-compliant specifications are also developed. The thesis additionally provides a thorough evaluation of its results from both a regulatory and technical viewpoint, and concludes by summarising the main features of the proposed approach and indicating possible future research directions.

Keywords: Privacy, privacy by design, service-oriented architectures, workflow, personal data protection legislation, privacy requirements, workflow model specification, workflow verification, privacy-aware workflow execution, semantic model, ontology.

Ευχαριστίες

Η διατριβή αποτελεί το προϊόν της ερευνητικής μου δραστηριότητας στο Εργαστήριο Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης του ΕΜΠ. Αναγνωρίζοντας ότι αυτή θα ήταν αδύνατον να πραγματοποιηθεί χωρίς την καθοδήγηση και τη συμπαράσταση κάποιων σημαντικών για εμένα ανθρώπων, θα ήθελα στο σημείο αυτό να ευχαριστήσω όλους όσους με στήριξαν.

Ξεκινώντας από τη συμβουλευτική μου επιτροπή, θα ήθελα ιδιαίτερα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου, κυρία Δήμητρα Κακλαμάνη, Καθηγήτρια ΕΜΠ, η οποία μου έδωσε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον ερευνητικό αντικείμενο, με εμπιστεύτηκε, με καθοδήγησε και ήταν διαθέσιμη να με βοηθήσει οποτεδήποτε τη χρειάστηκα. Συνεχίζοντας, θα ήθελα να ευχαριστήσω τον Καθηγητή ΕΜΠ κύριο Ιάκωβο Βενιέρη, που με την εμπειρία, τις πολύπλευρες γνώσεις του και την προθυμία του στάθηκε ουσιαστικά δεύτερος επιβλέπων για εμένα καθ' όλη την πορεία μου. Επίσης, θερμές ευχαριστίες στους Καθηγητές ΕΜΠ κύριο Νικόλαο Ουζούνογλου και κύριο Γεώργιο Στασινόπουλο και στον Καθηγητή Πανεπιστημίου Πειραιά κύριο Σωκράτη Κάτσικα, που πάντοτε ευγενικοί στήριξαν την προσπάθειά μου, και φυσικά στον Καθηγητή ΕΜΠ κύριο Γρηγόριο Μέντζα και στο Λέκτορα ΕΜΠ κύριο Δημήτρη Φωτάκη, που μου έκαναν την τιμή να συμπεριληφθούν στην επταμελή εξεταστική επιτροπή μου. Ευχαριστώ επίσης ολόψυχα όλα τα παιδιά στο εργαστήριο για την εποικοδομητική, όσο και διασκεδαστική, συνύπαρξη και συνεργασία μας όλα αυτά τα χρόνια, ιδιαιτέρως δε τους ερευνητές Γιώργο Λιουδάκη, Ευγενία Παπαγιαννακοπούλου και Νίκο Δέλλα, των οποίων η συμβολή στην ερευνητική μου εργασία υπήρξε κάτι παραπάνω από καθοριστική. Τέλος, θα ήθελα να πω ευχαριστώ στους φίλους που ήταν πάντα δίπλα μου και με ενθάρρυναν και στην οικογένειά μου, που χωρίς την αγάπη και την πίστη της σε εμένα θα είχα κάνει και θα ήμουν πολύ λιγότερα.

Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο - ΕΚΤ) και από εθνικούς πόρους μέσω του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (ΕΣΠΑ) – Ερευνητικό Χρηματοδοτούμενο Έργο: Ηράκλειτος ΙΙ . Επένδυση στην κοινωνία της γνώσης μέσω του Ευρωπαϊκού Κοινωνικού Ταμείου.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Σελ.

Κεφάλαιο 1

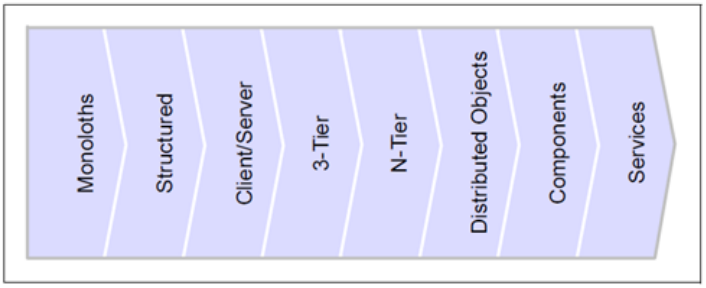
Εισαγωγή

Τα τελευταία χρόνια ένα πλήθος τεχνολογιών και προτύπων έχει αναπτυχθεί ως αποτέλεσμα της ανάγκης για την ενοποίηση και ολοκλήρωση ετερογενών συστημάτων εφαρμογών. Ανάμεσά τους, τα συστήματα λογισμικού προσανατολισμένου σε υπηρεσίες συνιστούν κυρίαρχη αρχιτεκτονική προσέγγιση και υπόσχονται την ανάπτυξη και παροχή ακόμα πιο προηγμένων ηλεκτρονικών υπηρεσιών.

Από την άλλη, η γενικότερη πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνίας προκαλεί την ολοένα αυξανόμενη ανησυχία των πολιτών σχετικά με τους κινδύνους που αυτή εγκυμονεί για την ιδιωτική τους ζωή. Στο πλαίσιο αυτό, τα σύγχρονα κατανεμημένα, ετερογενή και δυναμικά περιβάλλοντα εντείνουν το πρόβλημα, καθώς καθιστούν την όποια συλλογή, επεξεργασία και μετάδοση δεδομένων δύσκολα ελέγξιμη.

1.1 Αρχιτεκτονικές Προσανατολισμένες σε Υπηρεσίες

Οι *Αρχιτεκτονικές Προσανατολισμένες σε Υπηρεσίες (Service Oriented Architectures – SOA)* [1] αποτελούν ένα σύνολο ευέλικτων σχεδιαστικών αρχών που αφορούν στις φάσεις του σχεδιασμού και της ολοκλήρωσης υπολογιστικών συστημάτων και κατέχουν κεντρική θέση στις σύγχρονες τεχνολογίες πληροφορίας. Οι τελευταίες καλούνται σήμερα να αντιμετωπίσουν αφενός την ετερογενή φύση του Διαδικτύου, και συνακόλουθα σύνθετα θέματα όπως το κατανεμημένο λογισμικό, την ολοκλήρωση εφαρμογών, τις διαφορετικές πλατφόρμες και πρωτόκολλα και τις ποικίλες συσκευές, και αφετέρου την εξέλιξη των επιχειρησιακών οργανισμών από την κάθετη, διαχωρισμένη οργάνωση μέχρι και τη δεκαετία του 1980 στις από εκεί και μετά οριζόντιες δομές με επίκεντρο τις επιχειρησιακές διαδικασίες [2]. Οι αρχιτεκτονικές τύπου SOA εξελίσσονται ραγδαία ως η επικρατέστερη προσέγγιση ενοποίησης στα σημερινά πολύπλοκα ετερογενή υπολογιστικά περιβάλλοντα, τα οποία βασίζονται στη *χαλαρή συσχέτιση (loose-coupling)* συνιστωσών λογισμικού με σκοπό την παροχή υπηρεσιών.



Σχήμα 1: Η εξέλιξη των αρχιτεκτονικών λογισμικού [2].

Όπως φαίνεται στο Σχήμα 1, η έννοια της *υπηρεσίας* αποτελεί την τελευταία από τις τάσεις που εμφανίστηκαν μετά τις λεγόμενες μονολιθικές εφαρμογές με στόχο την εξάλειψη των προβλημάτων ετερογένειας, διαλειτουργικότητας, παγκόσμιας προσβασιμότητας και διαρκώς μεταβαλλόμενων απαιτήσεων. Οι πόροι λογισμικού σε μια SOA αρχιτεκτονική ομαδοποιούνται σε υπηρεσίες, με άλλα λόγια, καλά ορισμένες, αυτοπεριεκτικές (self-contained) δομικές μονάδες, καθεμιά από τις οποίες παρέχει συγκεκριμένη λειτουργικότητα και είναι ανεξάρτητη από την κατάσταση ή το πλαίσιο που χαρακτηρίζει άλλες υπηρεσίες. Αυτές με τη σειρά τους μπορούν να ενοποιηθούν και να αναχρησιμοποιηθούν για τη σύνθεση νέων υπηρεσιών, επιτρέποντας στους οργανισμούς να αναπτύσσουν, διασυνδέουν και συντηρούν εφαρμογές και υπηρεσίες αποδοτικά και με χαμηλό κόστος. Σε αυτό το πλαίσιο, οι *ροές εργασιών (workflows)* [3][4], οι καλώς ορισμένες, δηλαδή, ακολουθίες εργασιών οι οποίες συνδυάζονται και συντονίζονται με σκοπό την επίτευξη ποικίλων ευρύτερων επιχειρησιακών, επιστημονικών και άλλων στόχων, έχουν αναδειχθεί ως τεχνολογία αιχμής στα σύγχρονα κατανεμημένα και δυναμικά περιβάλλοντα, ενισχυόμενα ιδιαίτερα και από τη γρήγορη εξάπλωση των αρχιτεκτονικών τύπου SOA.

1.2 Ιδιωτικότητα

Η ιδιωτικότητα[1] χαρακτηρίζεται σαν ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, όπως έχει αναγνωριστεί από το Άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα [5] των Ηνωμένων Εθνών. Αποτελεί αναμφίβολα ένα από τα πιο σημαντικά ζητήματα αναφορικά με τα δικαιώματα του ανθρώπου που επηρεάζονται από την εξελισσόμενη "Εποχή της Πληροφορίας".

Είναι μάλλον δύσκολο να δοθεί ένας ενιαίος ορισμός για την ιδιωτικότητα, καθώς αποτελεί σε μεγάλο βαθμό υποκειμενική έννοια, ενώ διαφορετικές επιστήμες την εξετάζουν από διαφορετικές οπτικές γωνίες· στο πλαίσιο της διατριβής υιοθετείται ο ορισμός που διατυπώθηκε από τον Alan Westin το 1967 [6]:

Ιδιωτικότητα είναι η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το

[1]Ο όρος "Ιδιωτικότητα" αποτελεί μετάφραση του διεθνούς όρου "Privacy", σύμφωνα με τον Ελληνικό Οργανισμό Τυποποίησης.

χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων.

Πολύ συχνά, η προστασία της ιδιωτικότητας θεωρείται —λανθασμένα— συνώνυμη της ασφάλειας των πληροφοριακών συστημάτων και των ηλεκτρονικών επικοινωνιών. Η αλήθεια είναι ότι οι μηχανισμοί ασφάλειας, όπως η χρήση κρυπτογραφίας και ο έλεγχος πρόσβασης (access control) σε συστήματα και δεδομένα, αποτελούν τη στοιχειώδη βάση για την προστασία της ιδιωτικότητας (βλ. Ενότητες 3.4.1, 3.4.3), χωρίς ωστόσο να αποτελούν πανάκεια. Για παράδειγμα, οι μηχανισμοί ασφάλειας δεν είναι σε θέση να αποτρέψουν μια επιχείρηση από το να πουλήσει τα προσωπικά δεδομένα των πελατών της σε κάποια άλλη επιχείρηση που θα προβεί σε κατάχρησή τους. Επιπλέον, μερικές φορές οι έννοιες της ασφάλειας και της ιδιωτικότητας είναι αντιθετικές. Ενδεικτικά, η αυτόματη παρακολούθηση των συμβάντων σε ένα σύστημα για σκοπούς διατήρησης της ασφάλειας (π.χ., για την ανίχνευση εισβολών) μπορεί να αποτελέσει απειλή για την ιδιωτικότητα των χρηστών του, όπως καταδεικνύεται στο άρθρο [7]. Το γεγονός αυτό είναι γνωστό σαν το παράδοξο ασφάλειας – ιδιωτικότητας [8].

1.3 Προστασία της Ιδιωτικότητας σε Ροές Εργασιών

Οι ροές εργασιών διακρίνονται σε δύο βασικές κατηγορίες, τις επιχειρησιακές και τις επιστημονικές (βλ. Ενότητα 3.3). Οι πρώτες χρησιμοποιούνται πλέον κατά κόρον για την επιτέλεση καθημερινών λειτουργιών σε διάφορους τομείς που περιλαμβάνουν τη συλλογή και επεξεργασία προσωπικών δεδομένων, όπως είναι ο τραπεζικός, ο τομέας της υγείας, οι υπηρεσίες ηλεκτρονικής διακυβέρνησης, κ.ά. Από την άλλη, και το δεδομενοκεντρικό πρότυπο των επιστημονικών ροών εργασιών γίνεται συνεχώς ελκυστικότερο ως προς την καταλληλότητά του σε πολλά πεδία εφαρμογών ευάλωτα από πλευράς ιδιωτικότητας. Ως ενδεικτικά παραδείγματα μπορούν να αναφερθούν η επεξεργασία δεδομένων επικοινωνίας πραγματικού χρόνου από τηλεπικοινωνιακούς παρόχους με σκοπό τη διαχείριση και ασφάλεια των δικτυακών υποδομών, ή η ανάλυση συνεχούς ροής δεδομένων αισθητήρων, προερχόμενων από ένα ευρύ φάσμα πηγών, που μπορεί να περιλαμβάνουν από δορυφόρους μέχρι οικιακούς έξυπνους μετρητές ενέργειας. Προβάλλει, συνεπώς, ολοένα και πιο έντονη η ανάγκη για αποτελεσματική θωράκιση των ροών εργασιών, ανεξαρτήτως τύπου, απέναντι σε παραβιάσεις της ιδιωτικότητας, κάτι που θα αποτελέσει ένα σημαντικό βήμα προς την ενίσχυση της προστασίας των αντίστοιχων θεμελιωδών δικαιωμάτων των ατόμων, αλλά και της εμπιστοσύνης τους στις υπηρεσίες ΤΠΕ.

Τα συστήματα ροών εργασιών, ωστόσο, παρουσιάζουν διάφορες ιδιαιτερότητες αναφορικά με θέματα ιδιωτικότητας, θέτοντάς τη συχνά σε κίνδυνο, καθώς από τη φύση τους βασίζονται σε μεγάλο βαθμό στην πρόσβαση σε και στην ανταλλαγή δεδομένων. Εξάλλου, συχνά εξαρτώνται από, αλλά και καλλιεργούν, τη συνεργασία μέσα σε ετερογενή περιβάλλοντα και μεταξύ πολλών μετεχόντων μερών, κάτι που καθιστά ιδιαίτερα πολύ-

πλοκη την ευθεία και αποτελεσματική εφαρμογή ήδη υπαρχουσών λύσεων για την προστασία της ιδιωτικότητας. Πράγματι, η μεγαλύτερη πρόκληση που ανακύπτει σε ένα τέτοιο περιβάλλον είναι το γεγονός ότι οι διάφορες δραστηριότητες δε θα πρέπει πλέον να εξετάζονται μεμονωμένα αλλά, επιπλέον, και σε σχέση με τη *ροή* δεδομένων και ενεργειών, αποσκοπώντας σε μια ολιστική θεώρηση των αντίστοιχων διαδικασιών. Με άλλα λόγια, οι απαιτούμενοι μηχανισμοί (π.χ., έλεγχος πρόσβασης) θα πρέπει να επιβάλλονται αποτελεσματικά σε ό,τι αφορά όχι μόνο επιμέρους ενέργειες αλλά και τις σε μεγαλύτερη κλίμακα αλληλοσυσχετίσεις τους στο επίπεδο της ροής εργασιών.

Παράλληλα, όπως θα παρουσιαστεί λεπτομερώς στο Κεφάλαιο 2, η ιδιωτικότητα προστατεύεται νομοθετικά, και μάλιστα και σε υπερκρατικό/υπερεθνικό επίπεδο, κάτι που καθιστά ακόμα πιο έκδηλη τη σημασία που της αποδίδεται, ενώ πολυάριθμες μελέτες (π.χ., [9][10][11][12][13][14][7][15][16]) έχουν ως αντικείμενο τις αρχές και απαιτήσεις που συνεπάγονται τα σχετικά νομοθετήματα. Ιδιαίτερο ενδιαφέρον παρουσιάζει δε το γεγονός ότι πολλά συναφή νομικά κείμενα αφορούν συγκεκριμένους τομείς, διαδικασίες των οποίων, όπως προαναφέρθηκε, πολύ συχνά αυτοματοποιούνται μέσω συστημάτων ροών εργασιών, όπως οι επικοινωνίες (π.χ., [17][18]), η υγεία (π.χ., [19][20][21]) και η ηλεκτρονική διακυβέρνηση (π.χ., [22][23]). Σε αυτό το πλαίσιο, αναδυόμενη τάση αποτελεί πιο συγκεκριμένα η προστασία προσωπικών δεδομένων *ήδη από το σχεδιασμό και εξ ορισμού*, όπως προκύπτει εξάλλου και από από τον πρόσφατο προς ψήφιση "Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών" [24]. Όπως διαπιστώθηκε, κάτι τέτοιο δεν έχει μέχρι στιγμής πραγματοποιηθεί, τουλάχιστον όχι λαμβάνοντας υπόψη όλους τους κρίσιμους για την ιδιωτικότητα παράγοντες, καθώς η υφιστάμενη κατάσταση (βλ. Ενότητα 3.4.5) παρουσιάζει, πέρα από ενδιαφέρουσες λύσεις οι οποίες και θα αξιοποιηθούν, τις ακόλουθες ελλείψεις:

- Καμιά από τις υπάρχουσες τεχνολογίες μοντελοποίησης ροών εργασιών δεν είναι σε θέση αφεαυτής να αναπαραστήσει σε ικανοποιητικό βαθμό και τις τρεις βασικές όψεις που υπεισέρχονται στις ροές εργασιών, δηλαδή την όψη της ροής ελέγχου, την όψη των δεδομένων και την όψη των πόρων, οι οποίες είναι εξίσου σημαντικές για την προστασία προσωπικών δεδομένων. Γενικότερα, η εκφραστικότητα των λύσεων αυτών δεν επαρκεί για την αποτύπωση του συνόλου των χαρακτηριστικών που χρειάζεται να προδιαγραφούν και, κατόπιν, να ελεγχθούν, προκειμένου να μπορεί να εξασφαλιστεί η συμμόρφωση της εκτέλεσης μιας ροής εργασιών με τις αρχές ιδιωτικότητας που πιθανώς την αφορούν.
- Το μεγαλύτερο μέρος της έρευνας στο χώρο του ελέγχου πρόσβασης και συμμόρφωσης των ροών εργασιών είναι μέχρι τώρα προσανατολισμένο στη ροή ελέγχου και την ανάθεση σε πόρους, ενώ η όψη των δεδομένων έχει δευτερεύουσα θέση ή και αγνοείται. Έτσι, τα πιο δεδομενοκεντρικά συστήματα, όπως για παράδειγμα οι επιστημονικές ροές εργασιών, δεν υποστηρίζονται ικανοποιητικά αναφορικά με την επι-

βεβαίωση της συμμόρφωσής τους σε συγκεκριμένες αρχές. Κάτι τέτοιο ωστόσο είναι ανεπίτρεπτο για την ιδιωτικότητα, η οποία αφορά κατά κύριο λόγο στην προστασία των δεδομένων και κατά συνέπεια απαιτεί την τήρηση κανόνων που αφορούν ακριβώς σε αυτά.

- Ειδικά οι προσεγγίσεις στο ζήτημα του ελέγχου συμμόρφωσης θεωρούν συνήθως απλής μορφής κανόνες γενικού σκοπού, παραλείποντας έννοιες όπως είναι ο ρόλος ή ο σκοπός, που για την προστασία της ιδιωτικότητας θεωρούνται θεμελιώδεις. Άλλες πάλι πραγματεύονται μεν ζητήματα ιδιωτικότητας, εστιάζοντας ωστόσο σε συγκεκριμένες πλευρές της. Από την άλλη, η μέχρι τώρα εφαρμογή πιο πολύπλοκων μοντέλων που προβλέπουν παραμέτρους όπως οι παραπάνω περιορίζονται στην άσκηση ελέγχου πρόσβασης μόλις κατά τη φάση της εκτέλεσης ροών εργασιών και δεν αξιοποιούνται για την επαλήθευσή τους στη φάση του σχεδιασμού.

- Πέρα από το θέμα του ελέγχου, λίγες λύσεις έχουν προταθεί για την τροποποίηση /αναπροσαρμογή ενός μοντέλου διαδικασίας με σκοπό την απαλοιφή/αποφυγή των εκάστοτε παραβιάσεων. Ακόμα και αυτές, ωστόσο, αφορούν πρωτίστως τη βάσει απλών ως επί το πλείστον κανόνων δυναμική προσαρμογή ροών εργασιών κατά την εκτέλεσή τους, και όχι αλλαγές στην προδιαγραφή τους ήδη από τη φάση του σχεδιασμού.

Εν όψει των παραπάνω, η διδακτορική διατριβή υλοποιεί τις αρχές της λεγόμενης *"ιδιωτικότητας εκ σχεδιασμού" (Privacy by Design)* [25] σε συστήματα ροών εργασιών σε περιβάλλοντα SOA, μέσω της εξασφάλισης της συμμόρφωσής τους με τις απαιτήσεις της ιδιωτικότητας ήδη κατά τη φάση του σχεδιασμού τους και, εν συνεχεία, της συνεπούς εκτέλεσής τους. Στην κατεύθυνση αυτή, αρχικά καταγράφει και συστηματοποιεί τις τεχνικές απαιτήσεις που εισάγει η ανάγκη για προστασία της ιδιωτικότητας σε περιβάλλοντα ροών εργασιών. Με βάση αυτή την καταγραφή, προχωρά στην προδιαγραφή ενός νέου τρόπου μοντελοποίησης ροών εργασιών, που επιτυγχάνει τη φορμαλιστική απεικόνιση με έναν ενοποιημένο τρόπο όλων εκείνων των πληροφοριών που απαιτούνται για τον ενδελεχή έλεγχό τους ως προς τις αρχές ιδιωτικότητας και για τη συνεπή, λειτουργικά αλλά και από πλευράς προστασίας προσωπικών δεδομένων, εκτέλεσή τους. Επιπλέον προτείνει ένα μηχανισμό για την αυτόματη επαλήθευση μοντέλων ροών εργασιών και τη συνακόλουθη τροποποίησή τους, όπου αυτό χρειάζεται, προκειμένου αυτά να καθίστανται σύμμορφα με τις αρχές της ιδιωτικότητας. Τέλος, ορίζει μια νέα γλώσσα για την περιγραφή της συμπεριφοράς κάθε οντότητας που πρόκειται να εμπλακεί στην εκτέλεση μιας ροής εργασιών, ικανή για τη "μεταφορά" στο στρώμα εκτέλεσης του συνόλου της πληροφορίας που μπορεί να περικλείει η έγκυρη, από πλευράς ιδιωτικότητας, προδιαγραφή της.

1.4 Διάρθρωση της Διατριβής

Η διατριβή αποτελείται από συνολικά έντεκα κεφάλαια. Πέρα από το παρόν εισαγωγικό κεφάλαιο, το περιεχόμενο των υπολοίπων κεφαλαίων συνοψίζεται ως ακολούθως.

Στο δεύτερο κεφάλαιο συνοψίζεται το Νομικό και Κανονιστικό Πλαίσιο που διέπει την προστασία προσωπικών δεδομένων και που ουσιαστικά αντανακλά τις απαιτήσεις που πρέπει να ικανοποιεί ένα τεχνολογικό σύστημα που στοχεύει στην προστασία της ιδιωτικότητας. Έπειτα από μια σύντομη εισαγωγή και ιστορική αναδρομή, περιγράφονται οι βασικές αρχές προστασίας των προσωπικών δεδομένων όπως έχουν διαμορφωθεί και γίνει διεθνώς αποδεκτές. Στη συνέχεια, παρατίθεται η συνοπτική αλλά περιεκτική περιγραφή του Ευρωπαϊκού Δικαίου, που αποτελεί τη βάση για το Ελληνικό Εθνικό Δίκαιο, το οποίο επίσης επισκοπείται στη συνέχεια. Το κεφάλαιο κλείνει με τη σύνοψη των νομικών και κανονιστικών απαιτήσεων, όπως αυτές προκύπτουν από την προηγηθείσα ανάλυση.

Στη συνέχεια, πραγματοποιείται επισκόπηση των διαφόρων προτύπων καθώς και των ερευνητικών προσπαθειών που πραγματοποιήθηκαν μέχρι σήμερα όσον αφορά αφενός τις τεχνολογίες λογισμικού βασισμένου σε υπηρεσίες και, αφετέρου, τους μηχανισμούς προστασίας προσωπικών δεδομένων. Καλύπτονται θέματα όπως οι υπηρεσίες ιστού, οι σημασιολογικές υπηρεσίες ιστού, οι μηχανισμοί για τη σύνθεση υπηρεσιών, οι τεχνολογίες για τη μοντελοποίηση ροών εργασιών, καθώς και οι τεχνολογίες για την προστασία και διαχείριση της ιδιωτικότητας. Από την ανάλυση αναδεικνύονται οι περιορισμοί των τεχνολογιών λογισμικού σε ό,τι αφορά την ενσωμάτωση μηχανισμών προστασίας ιδιωτικότητας, καθώς και η χρησιμότητα των τελευταίων για τους σκοπούς της διατριβής.

Το τέταρτο κεφάλαιο περιγράφει τις γενικές αρχές της προτεινόμενης λύσης, παρέχοντας μια γενική επισκόπηση και παραθέτοντας κάποιες βασικές έννοιες. Στο πλαίσιο αυτό, εισάγεται η έννοια της ροής εργασιών με αφαιρετικό τρόπο και καταγράφονται οι βασικές αρχές που διέπουν τις ροές εργασίας αναφορικά με την προστασία της ιδιωτικότητας. Επιπλέον, προδιαγράφεται η γενική αρχιτεκτονική του συστήματος σχεδιασμού και εκτέλεσης ροών εργασιών, καλύπτοντας τον πλήρη κύκλο ζωής τους, και προσδιορίζονται τα επιμέρους συστήματα καθώς και τα σημασιολογικά μοντέλα που καθορίζουν τη συνολική λειτουργία. Τέλος, περιγράφονται το Σημασιολογικό Μοντέλο Πληροφοριών, το οποίο ορίζει σημασιολογικά τις έννοιες που αφορούν τις οντότητες του συστήματος, και το Σημασιολογικό Μοντέλο Πολιτικών, το οποίο παρέχει τους κανόνες ελέγχου πρόσβασης και χρήσης βάσει των οποίων πραγματοποιείται ο έλεγχος συμμόρφωσης των ροών εργασιών με τις αρχές τις ιδιωτικότητας.

Το πέμπτο κεφάλαιο, έχοντας ως αφετηρία τις νομικές και κανονιστικές απαιτήσεις που αφορούν την ιδιωτικότητα στα πληροφοριακά συστήματα όπως παρουσιάζονται στο Κεφάλαιο 2, εμβαθύνει στις εξ αυτών συναγόμενες τεχνικές απαιτήσεις που χαρακτηρίζουν τα περιβάλλοντα ροών εργασιών, λαμβάνοντας υπόψη τις συγκεκριμένες ανάγκες και ιδιαιτερότητές τους. Πιο συγκεκριμένα, οι απαιτήσεις αφορούν δύο άξονες: α) την

ανάγκη να συμπεριληφθούν στο επίπεδο της μοντελοποίησης των ροών εργασιών δομές ικανές να υποστηρίξουν τον ορισμό πολιτικών ιδιωτικότητας και μηχανισμών προστασίας ως μέρος του σχεδιασμού τους, και β) τα βασικά μοτίβα συμμόρφωσης που είναι πιθανό να ανακύψουν και, ως εκ τούτου, πρέπει να υποστηρίζονται, προκειμένου να καταστεί δυνατή η αυτόματη επαλήθευση μοντέλων ροών εργασιών ως προς όρους προστασίας της ιδιωτικότητας, αλλά και η αυτόματη τροποποίησή τους στην περίπτωση της ανίχνευσης παραβιάσεων αυτών.

Στο έκτο κεφάλαιο, παρουσιάζεται ένας καινοτόμος τρόπος προδιαγραφής ροών εργασιών, με τη χρήση σημασιολογικών οντολογιών. Ο προτεινόμενος τρόπος καλύπτει τα κενά των καθιερωμένων μεθόδων, εισάγοντας μια σειρά από καινοτόμα χαρακτηριστικά που τα σύγχρονα συστήματα δεν υποστηρίζουν. Μεταξύ αυτών περιλαμβάνονται η ενιαία μοντελοποίηση των ροών πληροφοριών και ελέγχου, η αναπαράσταση των εμπλεκομένων οντοτήτων μέσω καταλλήλων δομών που επιτρέπουν τον εμπλουτισμό του ορισμού τους με συνθήκες και περιορισμούς βάσει των ιδιαίτερων χαρακτηριστικών τους, και η εισαγωγή της έννοιας των "αντικειμένων επενέργειας" που εμφανίζεται για πρώτη φορά στη βιβλιογραφία.

Το έβδομο κεφάλαιο αναφέρεται στις "οδηγίες συμβατότητας", οι οποίες αποτελούν τη βάση για την πραγματοποίηση του ελέγχου και επαλήθευσης των ροών εργασιών αναφορικά με τη συμμόρφωσή τους με τις αρχές προστασίας της ιδιωτικότητας, και της συνακόλουθης τροποποίησής τους, εφόσον είναι αναγκαίο, προκειμένου να καταστούν συμβατές. Επιπλέον, στο δεύτερο μέρος του κεφαλαίου αναλύεται ο τρόπος αναπαράστασης των οδηγιών συμβατότητας μέσω σημασιολογικών οντολογιών.

Το όγδοο κεφάλαιο παρουσιάζει τη μεθοδολογία ελέγχου των ροών εργασιών ως προς τη συμμόρφωσή τους με τις απαιτήσεις ιδιωτικότητας, και της αυτόματης τροποποίησής τους, εφόσον απαιτείται, προκειμένου να εναρμονιστούν με αυτές. Εξηγείται το πώς οι οδηγίες συμβατότητας χρησιμοποιούνται για την εξαγωγή συμπεριφορικών νορμών και παρουσιάζεται η διαδικασία της αποσύνθεσης μιας ροής εργασιών, της εφαρμογής των νορμών και της ανασύνθεσης μιας έγκυρης τελικής ροής. Επιπλέον, τεκμηριώνονται οι υποκείμενες έννοιες, όπως οι "υπογράφοι–στιγμιότυπα" και οι "περιπτώσεις εκτέλεσης" μιας ροής εργασιών.

Το ένατο κεφάλαιο είναι αφιερωμένο σε θέματα που αφορούν την εκτέλεση μιας ροής εργασιών έπειτα από την επαλήθευσή της. Στο πλαίσιο αυτό, περιγράφεται η αρχιτεκτονική των βασικών συστημάτων που είναι επιφορτισμένα με την ενορχήστρωση της εκτέλεσης, αλλά και την εκτέλεση αυτή καθαυτή. Επιπλέον, αναλύονται ζητήματα που αφορούν τη διακίνηση, σε πραγματικό χρόνο, πληροφοριών πλαισίου και πληροφοριών δυνατοτήτων, καθώς και η πρωτότυπη περιγραφή τους. Τέλος, ιδιαίτερα σημαντικό ζήτημα αποτελεί η προδιαγραφή του ρόλου της κάθε οντότητας που συμμετέχει στην εκτέλεση της ροής εργασιών σε εκτελέσιμη γλώσσα οδηγιών· δεδομένου ότι οι υφιστάμενες γλώσσες αδυνατούν να περιγράψουν το σύνολο των χαρακτηριστικών που προδιαγράφονται

από τις ροές εργασιών και αναφέρονται στην ιδιωτικότητα, η διατριβή προτείνει μια νέα, πολύ περιγραφική γλώσσα που καλύπτει τα κενά των εν λόγω προσεγγίσεων.

Η αξιολόγηση της προτεινόμενης λύσης αποτελεί το αντικείμενο του δέκατου κεφαλαίου. Η αξιολόγηση αφορά διάφορους άξονες, όπως την εκφραστικότητα του μοντέλου ροής εργασιών, που αναδεικνύουν τα πλεονεκτήματα της προτεινόμενης από τη διατριβή λύσης. Ιδιαίτερης σημασίας είναι η αξιολόγηση της λύσης σε ό,τι αφορά τη συμμόρφωση με τις απαιτήσεις της Νομοθεσίας σχετικά με την προστασία προσωπικών δεδομένων.

Τέλος, το ενδέκατο κεφάλαιο αποτελεί τον επίλογο της διατριβής, υπογραμμίζοντας κάποια βασικά συμπεράσματα, αλλά και σκιαγραφώντας τις βασικές κατευθύνσεις που θα αποτελέσουν τους άξονες της συνέχισης της έρευνας έχοντας ως βάση τη λύση που προτείνεται από τη διατριβή.

Κεφάλαιο 2

Νομικό και Κανονιστικό Πλαίσιο για την Προστασία της Ιδιωτικότητας

Το Κεφάλαιο αυτό παρουσιάζει συνοπτικά τη Νομοθεσία που διέπει την προστασία των προσωπικών δεδομένων, η οποία ουσιαστικά αντανακλά τις απαιτήσεις που πρέπει να ικανοποιεί ένα τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων σε υπηρεσιοστραφή περιβάλλοντα. Έπειτα από μία σύντομη εισαγωγή και ιστορική αναδρομή, περιγράφονται οι βασικές αρχές προστασίας των προσωπικών δεδομένων όπως έχουν διαμορφωθεί και γίνει αποδεκτές. Στη συνέχεια, παρατίθεται η συνοπτική αλλά περιεκτική περιγραφή του Ευρωπαϊκού Δικαίου, το οποίο αποτελεί τη βάση για το Ελληνικό Εθνικό Δίκαιο, το οποίο επισκοπείται στην Ενότητα 2.4. Τέλος, γίνεται μια σύνοψη των νομικών και κανονιστικών απαιτήσεων, όπως αυτές προκύπτουν από την προηγηθείσα ανάλυση.

2.1 Εισαγωγή

Όπως προαναφέρθηκε, η πρώτη πραγματεία αναφορικά με το γεγονός ότι η ιδιωτική ζωή των πολιτών τίθεται σε κίνδυνο από την τεχνολογική πρόοδο [26] δημοσιεύτηκε ήδη το 19ο αιώνα, όταν δύο νομικοί στην πολιτεία της Βοστόνης των Ηνωμένων Πολιτειών επισήμαναν τον κίνδυνο για την ιδιωτική ζωή που εγκυμονούσε η – σχετικά νέα τότε – τεχνολογία της λήψης φωτογραφιών. Τα Ηνωμένα Έθνη αναγνώρισαν την ιδιωτικότητα σαν ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, με το Άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα [5]. Το ενδιαφέρον για την προστασία των προσωπικών δεδομένων αυξήθηκε ιδιαίτερα τις δεκαετίες του 1960 και 1970, με την έλευση των τεχνολογιών της πληροφορίας και τις προφανείς δυνατότητες παρακολούθησης και αρχειοθέτησης που αυτές έφερναν.

Το 1970, υιοθετήθηκε ο πρώτος σύγχρονος νόμος προστασίας προσωπικών δεδομέ-

νων από το Hesse, ένα από τα "κρατίδια" (Länder) της πρώην Δυτικής Γερμανίας. Ο νόμος αυτός [27] αποτέλεσε τη βάση για άλλες περιοχές της Δυτικής Γερμανίας, την ομοσπονδιακή της κυβέρνηση αλλά και χώρες πέρα από τη Γερμανία, όπως τη Σουηδία που το 1973 υιοθέτησε τον πρώτο παγκοσμίως εθνικό νόμο προστασίας προσωπικών δεδομένων. Αρκετές Ευρωπαϊκές χώρες υιοθέτησαν παρόμοιους νόμους πριν από το τέλος της δεκαετίας του 1970.

Στις Ηνωμένες Πολιτείες της Αμερικής, το Κογκρέσο υιοθέτησε το "Νόμο περί Ιδιωτικότητας" (Privacy Act) το 1974 [28], εκτιμώντας ότι τα πολύπλοκα υπολογιστικά συστήματα δημιουργούσαν απειλές για την προσωπική ιδιωτικότητα. Ο νόμος αυτός δέχτηκε αρκετές τροποποιήσεις μέχρι σήμερα με σημαντικότερες εκείνη του 1988 [29], η οποία λάμβανε υπόψη τις τεχνολογικές εξελίξεις στο χώρο της πληροφορικής, καθώς και εκείνη του 2001, στο πλαίσιο του "Πατριωτικού Νόμου" (Patriot Act) [30], ο οποίος ενεργοποιεί τη δυνατότητα για αυξημένη παρακολούθηση προσώπων υπερβαίνοντας κατά πολύ τις μέχρι τότε επιτρεπόμενες εισβολές στην προσωπική ιδιωτικότητα. Στο πλαίσιο αυτό ορίζονται ενδυναμωμένες διαδικασίες παρακολούθησης και γίνονται πιο χαλαροί οι κανόνες για την άρση του απορρήτου των τηλεπικοινωνιών και τη συλλογή προσωπικών δεδομένων.

Στις αρχές της δεκαετίας του 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development – OECD)[2], στον οποίο συμμετέχει και η Ελλάδα, εξέδωσε τις Κατευθυντήριες Οδηγίες 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 αναφορικά με την προστασία των προσωπικών δεδομένων. Οι κατευθυντήριες αυτές οδηγίες είχαν σαν σκοπό να βοηθήσουν στον εναρμονισμό των εθνικών νομοθεσιών των κρατών – μελών του Οργανισμού γύρω από μία κοινή βάση για την προστασία των προσωπικών δεδομένων. Παρόλο που οι κατευθυντήριες οδηγίες είχαν στη φύση τους συμβουλευτικό και όχι νομοθετικό χαρακτήρα, επέδρασαν σε πολύ μεγάλο βαθμό στη σχετική νομοθεσία που ακολούθησε σε παγκόσμιο επίπεδο, ενώ οι βασικές αρχές για την προστασία των προσωπικών δεδομένων που όρισαν αποτέλεσαν τη βάση των σύγχρονων νομοθετικών και κανονιστικών πλαισίων και παραμένουν διαχρονικές. Για το λόγο αυτό αναφέρονται σε αυτό το κεφάλαιο, ενώ οι βασικές αρχές παρουσιάζονται στην Ενότητα 2.2.

Τον Ιούλιο του 1990, η Ευρωπαϊκή Κοινότητα εξέδωσε την πρώτη πρόχειρη πρόταση για μία οδηγία περί της προστασίας των προσωπικών δεδομένων. Μετά από χρόνια διαβουλεύσεων, η τελική Οδηγία 95/46/ΕΚ [32] "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών" υιοθετήθηκε από το Ευρωπαϊκό Συμβούλιο το 1995 και τέθηκε σε εφαρμογή στα κράτη – μέλη από τον Οκτώβρη του 1998. Η Οδηγία αυτή αποτέλεσε ορόσημο και αποτέλεσε τη βάση για τη νομοθεσία όχι μόνο των κρατών – μελών της Ευρω-

[2]http://www.oecd.org/

παϊκής Κοινότητας αλλά σε παγκόσμιο επίπεδο, αποτελώντας σήμερα το πιο επιδραστικό νομικό κείμενο περί της προστασίας των προσωπικών δεδομένων στον πλανήτη.

Το Δεκέμβριο του 1997, η Ευρωπαϊκή Κοινότητα εξέδωσε την Οδηγία 97/66/ΕΚ [33], περί της "επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα", με σκοπό τη διασφάλιση του απορρήτου των τηλεπικοινωνιών των πολιτών Η Οδηγία αυτή ουσιαστικά εξειδίκευσε και συμπλήρωσε την Οδηγία 95/46/ΕΚ σε ό,τι αφορά τον τηλεπικοινωνιακό τομέα και γρήγορα αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ [17] καθώς δεν ήταν σε θέση να διευθετήσει ζητήματα που αφορούσαν τις τελευταίες τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ καλύπτει όλο το φάσμα των ηλεκτρονικών επικοινωνιακών και των υπηρεσιών που παρέχονται μέσω αυτών. Αργότερα εκδόθηκε η Οδηγία 2006/24/ΕΚ [18], η οποία τροποποιεί την Οδηγία 2002/58/ΕΚ, σε ό,τι αφορά τη διατήρηση ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Τέλος, η Οδηγία 2009/136 ΕΚ [34] τροποποίησε εκ νέου σε ορισμένα σημεία την Οδηγία 2002/58/ΕΚ.

2.2 Βασικές Αρχές Προστασίας Προσωπικών Δεδομένων

Οι βασικές αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων όπως ορίστηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης στις Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων [31] και που, περισσότερο ή λιγότερο, αντανακλώνται σε όλους τους σύγχρονους σχετικούς νόμους των δημοκρατικών κρατών παγκοσμίως, είναι οι παρακάτω:

- **Αρχή του περιορισμού της συλλογής** (collection limitation principle): Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και – όπου είναι δυνατό – με τη συναίνεση ή την ενημέρωση του χρήστη.
- **Αρχή της ποιότητας των δεδομένων** (data quality principle): Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ – στο βαθμό που είναι απαραίτητο για το σκοπό αυτό – θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.
- **Αρχή προσδιορισμού του σκοπού** (purpose specification principle): Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.

- **Αρχή περιορισμού της χρήσης** (use limitation principle): Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.

- **Αρχή της προστασίας της ασφάλειας** (security safeguards principle): Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.

- **Αρχή της διαφάνειας** (openness principle): Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και πρακτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.

- **Αρχή της συμμετοχής του ατόμου** (individual participation principle): Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:

  – Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.

  – Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή και εφόσον η ανακοίνωση προϋποθέτει κόστος, αυτό να μην είναι υπερβολικό.

  – Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης της απόρριψης και της περαιτέρω διεκδίκησης.

  – Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό και σε περίπτωση επιτυχημένης αμφισβήτησης να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση των δεδομένων αυτών.

- **Αρχή της ευθύνης** (accountability principle): Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων.

Στις παραπάνω βασικές αρχές για την προστασία των προσωπικών δεδομένων βασίστηκε, μεταξύ άλλων, και η ανάπτυξη της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ [32], η οποία παρουσιάζεται παρακάτω.

2.3 Ευρωπαϊκό Δίκαιο

Η Ενότητα αυτή περιγράφει συνοπτικά την Ευρωπαϊκή νομοθεσία αναφορικά με την προστασία των προσωπικών δεδομένων, κυρίως μέσω των δύο βασικών σχετικών οδηγιών. Έτσι, η Ενότητα 2.3.1 περιγράφει την Οδηγία 95/46/ΕΚ, ενώ η Ενότητα 2.3.2 περιγράφει την Οδηγία 2002/58/ΕΚ, καθώς και την τροποποίησή της από τις Οδηγίες 2006/24/ΕΚ και 2009/136 ΕΚ, με έμφαση στα θέματα εκείνα τα οποία μπορούν να ερμηνευτούν ως απαιτήσεις – τεχνικές ή διαχειριστικές – ενός συστήματος προστασίας προσωπικών δεδομένων. Τέλος, παρουσιάζεται ο τελευταίος προς ψήφιση Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που προορίζεται να αντικαταστήσει την Οδηγία 95/46/ΕΚ.

2.3.1 Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ [32] αποτελεί σήμερα το πιο επιδραστικό παγκοσμίως νομικό κείμενο αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, ορίζοντας ένα υψηλού επιπέδου πρότυπο. Υιοθετήθηκε επίσημα το Νοέμβριο του 1995 και τα κράτη – μέλη της Ευρωπαϊκής Ένωσης υποχρεώθηκαν να αναπροσαρμόσουν τις εθνικές τους νομοθεσίες τρία χρόνια αργότερα.

Ο βασικός στόχος της Οδηγίας είναι η προστασία της ιδιωτικότητας σαν θεμελιώδες δικαίωμα του ανθρώπου, αναφορικά προς τη συλλογή, επεξεργασία, αποθήκευση και μετάδοση των δεδομένων προσωπικού χαρακτήρα. Συμπληρωματικό στόχο της Οδηγίας αποτελεί η εφαρμογή ενός εναρμονισμένου νομικού πλαισίου σε όλα τα κράτη – μέλη της Ευρωπαϊκής Ένωσης, ούτως ώστε να προαχθεί η ελεύθερη διακίνηση προσωπικών δεδομένων μέσα στα σύνορα της Κοινότητας. Από την άλλη πλευρά, η Οδηγία εμποδίζει τη μετάδοση προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης οι οποίες δεν έχουν την κατάλληλη νομοθεσία που να πληροί τα ελάχιστα πρότυπα προστασίας των δεδομένων προσωπικού χαρακτήρα. Η Οδηγία διαρθρώνεται σε επτά κεφάλαια, μία σύντομη περιγραφή των οποίων παρουσιάζεται στη συνέχεια.

Το Κεφάλαιο Ι της Οδηγίας (”Γενικές Διατάξεις”) παρέχει τους απαραίτητους ορισμούς και ορίζει τους σκοπούς και το πεδίο εφαρμογής της Οδηγίας. Σύμφωνα με το Άρθρο 3 (1), οι διατάξεις της Οδηγίας ”εφαρμόζονται στην αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο[3]”. Ωστόσο (Άρθρο 3 (2)), εξαιρείται η επεξεργασία όταν ”πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου”, καθώς και όταν αφορά ”τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης και της οικονομικής ευημερίας του, εφόσον η επεξεργασία

[3]Ως αρχείο δεδομένων προσωπικού χαρακτήρα, ή απλά αρχείο, ορίζεται κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα προσιτών με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

αυτή συνδέεται με θέματα ασφάλειας του κράτους) και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου" ή όταν "πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων".

Το Κεφάλαιο ΙΙ της Οδηγίας ("Γενικές προϋποθέσεις σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα") παρουσιάζει τις βασικές αρχές για την προστασία των προσωπικών δεδομένων, σε γενική συμφωνία με αυτές που ορίζονται από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (βλ. Ενότητα 2.2) και αποτελεί τον κορμό της Οδηγίας. Οι "αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων" (Άρθρο 6) επιβάλλουν τη σύννομη και θεμιτή συλλογή και επεξεργασία των προσωπικών δεδομένων, την αρχή του αυστηρού προσδιορισμού του σκοπού για τον οποίο πραγματοποιούνται και το συμβιβασμό με το σκοπό αυτό κάθε περαιτέρω επεξεργασίας, καθώς και την αρχή της ακρίβειας. Υλοποιούν δηλαδή επί της ουσίας τις αρχές περιορισμού της συλλογής και της χρήσης, του προσδιορισμού του σκοπού και της ποιότητας των δεδομένων όπως ορίζονται στο [31]. Οι "βασικές αρχές της νόμιμης επεξεργασίας δεδομένων" (Άρθρο 7) αφορούν την αναγκαιότητα της επεξεργασίας των προσωπικών δεδομένων. Σύμφωνα με τις αρχές αυτές, τα προσωπικά δεδομένα μπορούν να υποστούν επεξεργασία μόνο εφόσον το πρόσωπο στο οποίο αναφέρονται έχει συναινέσει σχετικά ή εάν η επεξεργασία πραγματοποιείται στο πλαίσιο εκπλήρωσης ισχύοντος συμβολαίου στο οποίο εμπλέκεται το εν λόγω πρόσωπο ή είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντός του, καθώς και για λόγους συμμόρφωσης με νομικές υποχρεώσεις ή εκπλήρωσης γενικού συμφέροντος. Σύμφωνα με τις "ειδικές κατηγορίες επεξεργασίας" (Άρθρο 8), η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων τα οποία "παρέχουν πληροφορίες για τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις και την υγεία και τη σεξουαλική ζωή" απαγορεύεται. Ορίζονται ωστόσο και εξαιρέσεις. Τα Άρθρα 10 – 14 της Οδηγίας διατυπώνουν τα δικαιώματα του προσώπου στο οποίο αναφέρονται τα προσωπικά δεδομένα στην πρόσβασή του σε αυτά, καθώς και στην εκτενή ενημέρωσή του για τη συλλογή και την επεξεργασία τους συμπεριλαμβανομένων των σχετικών πληροφοριών, ορίζοντας παράλληλα και τις σχετικές εξαιρέσεις. Η εμπιστευτικότητα και η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων υπογραμμίζονται από τα Άρθρα 16 και 17, ενώ τα Άρθρα 18 και 19 ορίζουν την υποχρέωση που έχει ο υπεύθυνος για την επεξεργασία να ενημερώνει την εθνική ελεγκτική αρχή καθώς και το περιεχόμενο αυτής της ενημέρωσης και τις προϋποθέσεις κάτω από τις οποίες η υποχρέωση αυτή απλουστεύεται ή δεν ισχύει. Το Άρθρο 20 προβλέπει τον εκ των προτέρων έλεγχο από την αρχή ελέγχου των επεξεργασιών εκείνων που ενέχουν ειδικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ενδιαφερομένων. Επιπλέον, το Άρθρο 21 ορίζει ότι πρέπει να λαμβάνονται μέτρα ούτως ώστε να διασφαλίζεται η δημοσιότητα των ως άνω περιγραφόμενων επεξεργασιών για τις οποίες έχει πραγματοποιηθεί ενημέρωση της αρχής ελέγχου με τη χρήση σχετικού μητρώου, το οποίο μπορεί να συμβουλεύεται ο οποιοσδήποτε. Για εκείνες τις επεξεργασίες που δεν υπόκεινται σε κοινοποίηση στην αρχή ελέγχου, προβλέπεται η αντίστοιχη δημο-

σιοποίηση από τον υπεύθυνο τη επεξεργασίας ή άλλο οριζόμενο φορέα σε όποιο πρόσωπο το ζητήσει.

Το Κεφάλαιο III της Οδηγίας (″Ένδικα μέσα, ευθύνη και κυρώσεις″) προβλέπει ότι κάθε πρόσωπο έχει δικαίωμα να προσφύγει ενώπιον δικαστηρίου, εφόσον δεν μπορεί να επιληφθεί η ίδια η αρχή ελέγχου, σε περίπτωση παραβιάσεως δικαιωμάτων κατοχυρωμένων από την εθνική νομοθεσία που εφαρμόζεται στη σχετική επεξεργασία προσωπικών δεδομένων, ενώ προβλέπονται οι ευθύνες των υπευθύνων για την επεξεργασία και οι αντίστοιχες κυρώσεις.

Το ζήτημα της μεταφοράς προσωπικών δεδομένων σε χώρες εκτός Ευρωπαϊκής Ένωσης θίγεται από το Κεφάλαιο IV της Οδηγίας (″Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες″). Σύμφωνα με το Άρθρο 25, η διαβίβαση προς τρίτη χώρα δεδομένων προσωπικού χαρακτήρα, τα οποία έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται μόνον εάν η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Ωστόσο, το Άρθρο 26 υπογραμμίζει διάφορες παρεκκλίσεις από την αρχή αυτή, όπως για την περίπτωση κατά την οποία το πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα έχει συναινέσει σχετικά ή εάν η διαβίβαση πραγματοποιείται στο πλαίσιο εκπλήρωσης ισχύοντος συμβολαίου στο οποίο εμπλέκεται το εν λόγω πρόσωπο.

Στο Κεφάλαιο V της Οδηγίας (″Κώδικες δεοντολογίας″) ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας που αποσκοπούν στο να συμβάλουν, ανάλογα με τις κατά περίπτωση τομεακές ιδιομορφίες, στην ορθή εφαρμογή των εθνικών διατάξεων που θεσπίζουν τα κράτη μέλη κατ' εφαρμογή της Οδηγίας. Προβλέπεται επίσης ότι τα επαγγελματικά σωματεία και οι λοιπές οργανώσεις μπορούν να τους υποβάλουν προς εξέταση στην εθνική αρχή του κώδικες δεοντολογίας, προκειμένου να εξεταστεί η συμμόρφωσή τους με τη σχετική νομοθεσία.

Το Κεφάλαιο VI της Οδηγίας (″Αρχή ελέγχου και ομάδα για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα″) ορίζει δύο βασικούς θεσμικούς φορείς:

- Το Άρθρο 28 προβλέπει ότι, σε κάθε κράτος – μέλος, μία ή περισσότερες δημόσιες αρχές ελέγχου επιφορτίζονται, με πλήρη ανεξαρτησία, με τον έλεγχο της εφαρμογής, στο έδαφός του, των εθνικών διατάξεων που έχουν θεσπισθεί από τα κράτη μέλη, κατ' εφαρμογή της Οδηγίας. Οι αρχές ελέγχου διαθέτουν μέσα για τη διεξαγωγή έρευνας (όπως το δικαίωμα πρόσβασης στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας), αποτελεσματικές εξουσίες παρέμβασης, καθώς και την εξουσία παράστασης ενώπιον δικαστηρίου σε περίπτωση παράβασης των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της Οδηγίας, ή επισήμανσης των παραβάσεων αυτών στις δικαστικές αρχές. Κάθε πρόσωπο μπορεί να υποβάλει στην αρχή ελέγχου αίτηση σχετικά με την προστασία των δικαιωμάτων και ελευθεριών του έναντι της

επεξεργασίας προσωπικών δεδομένων. Σημειώνεται ότι τα μέλη και οι υπάλληλοι των αρχών ελέγχου δεσμεύονται ακόμα και μετά την παύση των δραστηριοτήτων τους από το επαγγελματικό απόρρητο, όσον αφορά τις εμπιστευτικές πληροφορίες στις οποίες έχουν πρόσβαση.

- Τα Άρθρα 29 και 30 ορίζουν την "Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα", η οποία έχει συμβουλευτικό χαρακτήρα, είναι ανεξάρτητη και απαρτίζεται από έναν αντιπρόσωπο της αρχής ή των αρχών ελέγχου που έχει ορίσει κάθε κράτος – μέλος, έναν αντιπρόσωπο της αρχής ή των αρχών που έχουν συσταθεί για τα όργανα και τους οργανισμούς της Ευρωπαϊκής Κοινότητας καθώς και έναν αντιπρόσωπο της Ευρωπαϊκής Επιτροπής. Στις αρμοδιότητές της περιλαμβάνονται η εξέταση οποιουδήποτε θέματος σχετικού με την εφαρμογή των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της Οδηγίας και η γνωμοδότηση προς την Ευρωπαϊκή Επιτροπή αναφορικά με σχέδια τροποποίησης της Οδηγίας και σχέδια συμπληρωματικών ή ειδικών μέτρων που πρέπει να ληφθούν για τη διασφάλιση των δικαιωμάτων και ελευθεριών των προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων.

Τέλος, το Κεφάλαιο VII της Οδηγίας ("Κοινοτικά μέτρα εκτέλεσης") συμπληρώνει τα Κεφάλαια III, V και VI αναφορικά με τις μεθόδους μέσω των οποίων οι διατάξεις του Κεφαλαίου II τίθενται σε εφαρμογή σε εθνικό και Κοινοτικό επίπεδο.

2.3.2 Οι Ευρωπαϊκές Οδηγίες 2002/58/ΕΚ, 2006/24/ΕΚ και 2009/136/ΕΚ

Η Ευρωπαϊκή Οδηγία 2002/58/ΕΚ [17] αναφερόμενη στην "επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών" αντικατέστησε την Οδηγία 97/66/ΕΚ [33]. Η τελευταία είχε επιληφθεί για πρώτη φορά τη μεταφορά των βασικών αρχών που όριζε η Οδηγία 95/46/ΕΚ [32] σε προβλέψεις και κανόνες που αφορούσαν συγκεκριμένα τον τομέα των τηλεπικοινωνιών. Ωστόσο, η ανάπτυξη των προηγμένων ψηφιακών τεχνολογιών και των Διαδικτυακών εφαρμογών και υπηρεσιών, καθώς και η ραγδαία εξάπλωση των κινητών ψηφιακών επικοινωνιών επέβαλλαν την αναθεώρηση της προηγούμενης Οδηγίας προκειμένου να καλυφθεί όλο το φάσμα των σύγχρονων ηλεκτρονικών επικοινωνιών.

Οι βασικές απαιτήσεις που θέτει η Οδηγία 2002/58/ΕΚ παρουσιάζονται στη συνέχεια. Στο Άρθρο 4 της Οδηγίας θίγεται το ζήτημα της ασφάλειας των προσωπικών δεδομένων, επιβάλλοντας την υποχρέωση του να λαμβάνονται από τους παρόχους υπηρεσιών και δικτύων όλα τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των παρεχόμενων υπηρεσιών.

Το Άρθρο 5 της Οδηγίας ασχολείται με το απόρρητο των επικοινωνιών, απαγορεύοντας "την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης

των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια". Το γεγονός αυτό ωστόσο δεν επηρεάζει, σύμφωνα με το ίδιο άρθρο, "οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα".

Το Άρθρο 6 της Οδηγίας αναφέρεται εκτενώς στα δεδομένα κίνησης, δηλαδή τα δεδομένα εκείνα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Σύμφωνα με το Άρθρο αυτό, τα δεδομένα κίνησης τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο του δικτύου ή κάποιας υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας ή για την εκπλήρωση κάποιου άλλου θεμιτού σκοπού. Ο συνδρομητής ή ο χρήστης πρέπει να ενημερώνονται από τον πάροχο δικτύου ή κάποιας υπηρεσίας ηλεκτρονικών επικοινωνιών σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της επεξεργασίας αυτής, ενώ θα πρέπει να ζητείται και παρέχεται η συναίνεσή του για ορισμένους τύπους και σκοπούς επεξεργασίας (π.χ. για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας).

Αναφορικά με τα δεδομένα θέσης εκτός εκείνων της κίνησης, δηλαδή όλα εκείνα τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας υπηρεσίας ηλεκτρονικών επικοινωνιών, το Άρθρο 9 της Οδηγίας ορίζει ότι είναι δυνατό να υποστούν επεξεργασία, η επεξεργασία αυτή επιτρέπεται μόνον όταν αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση των χρηστών ή συνδρομητών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών είναι υποχρεωμένος να ενημερώνει τους χρήστες ή συνδρομητές, προτού δώσουν τη συγκατάθεσή τους, σχετικά με τον τύπο των δεδομένων θέσης εκτός των δεδομένων κυκλοφορίας που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Στους χρήστες ή συνδρομητές πρέπει να δίνεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων θέσης, εκτός των δεδομένων κίνησης. Επιπλέον, ορίζεται ότι όταν ο χρήστης έχει δώσει τη συγκατάθεσή του για την επεξεργασία δεδομένων θέσης εκτός των δεδομένων κίνησης, θα πρέπει να εξακολουθεί να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να αρνείται προσωρινά την επεξεργασία των εν λόγω δεδομένων για κάθε σύνδεση με το δίκτυο ή για κάθε μετάδοση μιας επικοινωνίας.

Το Άρθρο 12 της Οδηγίας αναφέρεται στις συνθήκες εισαγωγής και περαιτέρω χρή-

σης των προσωπικών δεδομένων χρηστών ηλεκτρονικών επικοινωνιών σε τηλεφωνικούς καταλόγους συνδρομητών οι οποίοι είτε είναι ευθέως διαθέσιμοι στο κοινό είτε είναι δυνατή η εξαγωγή δεδομένων από αυτούς μέσω σχετικών ερωτήσεων. Σύμφωνα με το Άρθρο 12, οι συνδρομητές πρέπει να ενημερώνονται, ατελώς και πριν περιληφθούν στον κατάλογο, σχετικά με το σκοπό των καταλόγων στους οποίους μπορεί να περιλαμβάνονται τα προσωπικά τους δεδομένα, καθώς και σχετικά με τις περαιτέρω δυνατότητες χρήσης που βασίζονται σε λειτουργίες αναζήτησης. Επιπλέον, οι συνδρομητές πρέπει να έχουν την ευκαιρία να καθορίζουν εάν και ποια από τα προσωπικά τους δεδομένα θα περιλαμβάνονται καταλόγους και να επαληθεύουν, να διορθώνουν ή να αποσύρουν τα εν λόγω δεδομένα.

Η Οδηγία δίνει ιδιαίτερη σημασία στις αυτόκλητες κλήσεις. Σύμφωνα με το Άρθρο 13, η χρησιμοποίηση οποιουδήποτε μέσου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους. Έτσι, απαγορεύεται η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση, τα οποία συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, ή δίχως έγκυρη διεύθυνση στην οποία ο αποδέκτης να μπορεί να ζητεί τον τερματισμό της επικοινωνίας αυτής.

Το Άρθρο 15 της Οδηγίας, τιτλοφορούμενο "Εφαρμογή ορισμένων διατάξεων της Οδηγίας 95/46/ΕΚ", θέτει περιορισμούς σχετικά με τα δικαιώματα και τις υποχρεώσεις που ορίζονται από την Οδηγία, για εκείνες τις περιπτώσεις που αφορούν τη διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων. Για τους λόγους αυτούς, η Οδηγία προβλέπει τη φύλαξη προσωπικών δεδομένων για ορισμένο χρονικό διάστημα.

Η απαίτηση για φύλαξη προσωπικών δεδομένων γίνεται πιο συγκεκριμένη από την Οδηγία 2006/24/ΕΚ [18], η οποία τροποποιεί την Οδηγία 2002/58/ΕΚ σε ό,τι αφορά το συγκεκριμένο ζήτημα. Η Οδηγία 2006/24/ΕΚ ορίζει συγκεκριμένου τύπους δεδομένων που αφορούν τηλεφωνικές (σταθερές και κινητές) και Διαδικτυακές υπηρεσίες, για τους οποίους προβλέπεται υποχρεωτική διατήρηση για συγκεκριμένα χρονικά διαστήματα, με σκοπό τη διασφάλιση ότι τα δεδομένα αυτά θα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Σημειώνεται ότι η Οδηγία 2006/24/ΕΚ αναφέρει ρητά ότι δεν επιτρέπεται η διατήρηση δεδομένων που αποκαλύπτουν το περιεχόμενο των επικοινωνιών, ενώ πρόσβαση στα διατηρούμενα δεδομένα πρέπει να παρέχεται μόνο στις αρμόδιες εθνικές αρχές, σε ειδικές μόνο περιπτώσεις και σύμφωνα με τη νομοθεσία και τις απαιτήσεις της αναγκαιότητας και της αναλογικότητας.

Από την άλλη, η Οδηγία 2009/136/ΕΚ [34] τροποποιεί την Οδηγία 2002/58/ΕΚ σε διάφορα επιμέρους σημεία. Κατ' αρχάς θέτει πιο συγκεκριμένες απαιτήσεις αναφορικά με την ασφάλεια της επεξεργασίας, εισάγοντας, μεταξύ άλλων, το καθήκον του υπεύθυνου της επεξεργασίας να ενημερώνει τόσο την αρμόδια αρχή όσο και το υποκείμενο των δεδομένων σχετικά με παραβιάσεις ασφάλειας που ανακύπτουν κατά την επεξεργασία των δεδομέ-

νων. Επιπλέον, ορίζει ως απαραίτητη προϋπόθεση τη συγκατάθεση του υποκειμένου των δεδομένων στις περιπτώσεις άντλησης πληροφορίας που βρίσκεται αποθηκευμένη στον τερματικό εξοπλισμό του, ενώ αναφέρεται διεξοδικά και στους μηχανισμούς επιβολής κυρώσεων. Τέλος, επιβάλλει, ως πρόσθετη υποχρέωση για τον υπεύθυνο της επεξεργασίας, τις εγγυήσεις του τελευταίου ότι το υποκείμενο των δεδομένων έχει τη δυνατότητα να ασκήσει τα δικαιώματά του αναφορικά με την προστασία της ιδιωτικότητάς του με άμεσο και ακριβή τρόπο.

2.3.3 Προς Ψήφιση Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Τον Ιανουάριο του 2012 κατατέθηκε η πρόταση για τον "Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)" [24]. Η πρόταση βασίζεται στο άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), το οποίο είναι η νέα νομική βάση για τη θέσπιση κανόνων περί προστασίας των δεδομένων δυνάμει της συνθήκης της Λισαβόνας[4].

Ο προτεινόμενος Κανονισμός βασίζεται στις αρχές της Οδηγίας 95/46/ΕΚ, την οποία επεκτείνει και συμπληρώνει, ενώ με την ψήφισή του ουσιαστικά θα την καταργήσει. Επιπλέον, αποσαφηνίζει τη σχέση με, και τροποποιεί, την οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Όπως επισημαίνεται, κίνητρο για τη θέσπισή του συνιστά το γεγονός ότι "η κλίμακα της ανταλλαγής και της συλλογής δεδομένων έχει αυξηθεί σε μεγάλο βαθμό", ενώ "η ΕΕ χρειάζεται μια συνολικότερη και συνεκτικότερη πολιτική σχετικά με το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα", καθώς "το ισχύον πλαίσιο παραμένει προσφυές όσον αφορά τους στόχους και τις αρχές του, αλλά δεν κατάφερε να αποτρέψει τον κατακερματισμό του τρόπου εφαρμογής της προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ένωση, την ανασφάλεια δικαίου και μια διαδεδομένη αντίληψη του κοινού ότι υπάρχουν σημαντικοί κίνδυνοι, οι οποίοι σχετίζονται ειδικότερα με την επιγραμμική δραστηριότητα".

Τα κυριότερα νέα σημεία τα οποία εισάγονται από την εν λόγω πρόταση είναι τα εξής δύο:

- Αναπτύσσεται, προσδιορίζεται και ισχυροποιείται περαιτέρω το δικαίωμα του προσώπου στο οποίο αναφέρονται τα δεδομένα *"να λησμονηθεί"*, το δικαίωμα διαγραφής, μη περαιτέρω διάδοσης και περιορισμού της επεξεργασίας των δεδομένων του. Περιλαμβάνεται επιπλέον η υποχρέωση του υπευθύνου επεξεργασίας ο οποίος δημοσιοποίησε τα δεδομένα να ενημερώνει τους τρίτους για το αίτημα του προσώπου στο οποίο αναφέρονται τα δεδομένα για διαγραφή τυχόν συνδέσμων ή αντιγράφων

[4]http://europa.eu/lisbon_treaty/index_el.htm

ή αναπαραγωγής των εν λόγω δεδομένων προσωπικού χαρακτήρα. Σε παρόμοια κατεύθυνση, κατοχυρώνεται το δικαίωμα του προσώπου στο οποίο αναφέρονται τα δεδομένα να μην υπάγεται σε μέτρο βασισμένο στην κατάρτιση προφίλ.

- Καθορίζονται ρητά οι υποχρεώσεις του υπευθύνου επεξεργασίας οι οποίες απορρέουν από τις αρχές της προστασίας των δεδομένων ήδη *από τον σχεδιασμό* και *εξ ορισμού*. Αυτό σημαίνει ότι "ο υπεύθυνος επεξεργασίας οφείλει, τόσο *κατά τον καθορισμό των μέσων επεξεργασίας* όσο και *κατά την ίδια την επεξεργασία*, να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα και διαδικασίες κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα."

2.4 Ελληνικό Εθνικό Δίκαιο

Η Ελλάδα κατοχυρώνει συνταγματικά ως ατομικά και κοινωνικά δικαιώματα το δικαίωμα στην προστασία προσωπικών δεδομένων και στο απόρρητο της επικοινωνίας. Συγκεκριμένα, το Άρθρο 9Α του Συντάγματος της Ελλάδας [35] 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 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 δεν 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.

Σε ό,τι αφορά την εναρμόνιση με το Κοινοτικό Δίκαιο, όπως είναι επόμενο η Ελλάδα έχει ενσωματώσει στο Εθνικό της Δίκαιο τις Κοινοτικές Οδηγίες που περιγράφονται παραπάνω. Στο πλαίσιο αυτό, η Οδηγία 95/46/ΕΚ τέθηκε σε ισχύ τον Απρίλιο του 1997 με το Νόμο 2472/1997 [36], αντικείμενο του οποίου είναι η "η 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". Αναφορικά με την υλοποίηση του Άρθρου 28 της Οδηγίας καθώς και του Άρθρου 9Α του Συντάγματος, με το νόμο αυτό συγκροτήθηκε ως ανεξάρτητη δημόσια αρχή η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[5], με αποστολή την εποπτεία της εφαρμογής του νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των κατά περίπτωση αρμοδιοτήτων που της ανατίθενται.

Πέρα από την ΑΠΔΠΧ, ο Νόμος 3115/2003 [37] υλοποίησε το Άρθρο 19 του Συντάγ-

[5]http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL

ματος συγκροτώντας μία δεύτερη ανεξάρτητη αρχή, την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ)[6]. Ο σκοπός της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών είναι "η προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και η ασφάλεια των δικτύων και πληροφοριών". Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από το νόμο.

Αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, η αρχική Ευρωπαϊκή Οδηγία 97/66/ΕΚ [33] είχε ενσωματωθεί στο Ελληνικό δίκαιο με το Νόμο 2474/1999 [38], ο οποίος από τον Ιούλιο του 2006 αντικαταστάθηκε από το Νόμο 3471/2006 [39] που αποτελεί προσαρμογή της νεότερης σχετικής Οδηγίας 2002/58/ΕΚ [17]. Σκοπός του Νόμου 3471/2006 είναι "η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών". Επιπλέον, ο Νόμος 3471/2006 τροποποιεί το Νόμο 2472/97 ως προς ορισμένες διατάξεις του, ενώ ορίζει τις αντίστοιχες αρμοδιότητες της ΑΔΑΕ και της ΑΠΔΠΧ. Τέλος, ο Νόμος 3917/2011 [40] αποτελεί την υλοποίηση της Οδηγίας 2006/24/ΕΚ και πραγματεύεται 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 συναφή ζητήματα. Συγκεκριμένα ορίζει, μεταξύ άλλων, ως ανώτατο χρονικό όριο διατήρησης τους 12 μήνες από την ημερομηνία της επικοινωνίας, για δεδομένα που αποθηκεύονται από τους παρόχους σε φυσικά μέσα, τα οποία βρίσκονται αποκλειστικά μέσα στα όρια της Ελληνικής Επικράτειας.

Η ΑΔΑΕ εξέδωσε τον Ιανουάριο του 2005 ορισμένους Κανονισμούς που αφορούν άμεσα την προστασία των προσωπικών δεδομένων. Οι Κανονισμοί αυτοί αφορούν, από τη μία πλευρά, τη διασφάλιση του απορρήτου κατά την παροχή κινητών [41], σταθερών [42] και μέσω ασυρμάτων δικτύων [43] τηλεπικοινωνιακών υπηρεσιών, και από την άλλη, τη διασφάλιση του απορρήτου στις Διαδικτυακές υπηρεσίες και τις συναφείς υπηρεσίες και εφαρμογές [44], των διαδικτυακών υποδομών [45] και των εφαρμογών Διαδικτύου και των χρηστών τους [46]. Οι παραπάνω κανονισμοί αντικαταστάθηκαν το 2011 από τον "Κανονισμό για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών" [47], ενώ τον Ιούλιο του 2013 εκδόθηκε και ο "Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών" [48], ο οποίος καθορίζει τα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνουν οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό.

Στις διατάξεις των Κανονισμών της ΑΔΑΕ οφείλουν να συμμορφώνονται όλοι οι τη-

[6]http://www.adae.gr/

λεπικοινωνιακοί πάροχοι οι οποίοι παρέχουν τηλεπικοινωνιακές υπηρεσίες κινητές, σταθερές ή μέσω ασυρμάτων δικτύων, καθώς και όλοι οι τηλεπικοινωνιακοί φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα οι πάροχοι πρόσβασης στο Διαδίκτυο, οι πάροχοι διαδικτυακών υπηρεσιών και οι πάροχοι διαδικτυακών υπηρεσιών προστιθέμενης αξίας. Αναφορικά με τους φορείς αυτούς, οι Κανονισμοί προδιαγράφουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα τα οποία πρέπει να λαμβάνονται προκειμένου να διασφαλίζεται το απόρρητο των ηλεκτρονικών επικοινωνιών κάθε είδους και κατά συνέπεια των προσωπικών δεδομένων που μεταδίδονται στο πλαίσιο της διεξαγωγής των επικοινωνιών αυτών. Επιπλέον, οι Κανονισμοί θεσπίζουν τις υποχρεώσεις των εν λόγω φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών καθώς και απέναντι στην ανεξάρτητη αρχή, ενώ ορίζονται και τα σχετικά με τη διεξαγωγή ελέγχων στους φορείς αυτούς αναφορικά με τις υποχρεώσεις τους αυτές.

Σημειώνεται ότι οι Κανονισμοί της ΑΔΑΕ χαρακτηρίζονται από τέτοιο βαθμό πληρότητας που στην πράξη ωθούν τους φορείς που εμπίπτουν στις διατάξεις τους στην εφαρμογή των διεθνώς αναγνωρισμένων προτύπων ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων, όπως το ISO/IEC 17799 [49].

Τέλος, οι διαδικασίες καθώς και οι τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του ορίστηκαν με το Προεδρικό Διάταγμα 47/2005 [50] το Μάρτιο του 2005. Το Προεδρικό Διάταγμα 47/2005 ορίζει τα είδη της επικοινωνίας καθώς και τα στοιχεία εκείνα τα οποία, εφόσον τηρούνται οι νόμιμες προϋποθέσεις, είναι δυνατό να ζητούνται από τους παρόχους υπηρεσιών προστιθέμενης αξίας ή δικτύου. Από τις ειδικές περιπτώσεις που ορίζονται, ιδιαίτερο ενδιαφέρον παρουσιάζει η διάταξη που επιτρέπει στις αρμόδιες αρχές να αποκτούν πρόσβαση στα κλειδιά κρυπτογράφησης που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης (Certification Authorities), εφόσον φυσικά πληρούνται οι νόμιμες προϋποθέσεις και συντρέχουν οι νόμιμες αιτίες για αυτό. Επιπλέον, το Προεδρικό Διάταγμα 47/2005 ορίζει τα απαραίτητα μέσα και τον αναγκαίο εξοπλισμό για την άρση του απορρήτου, καθώς τη μέθοδο αλλά και τις αντίστοιχες υποχρεώσεις των παρόχων υπηρεσιών και δικτύων.

2.5 Σύνοψη Νομικών και Κανονιστικών Απαιτήσεων

Στις προηγούμενες ενότητες παρουσιάστηκε το Νομικό και Κανονιστικό Πλαίσιο που διέπει την προστασία των προσωπικών δεδομένων. Το πλαίσιο αυτό αντανακλά ουσιαστικά τις απαιτήσεις για το προτεινόμενο τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων σε υπηρεσιοστραφή περιβάλλοντα. Οι νομικές απαιτήσεις μπορούν να συνοψιστούν / κωδικοποιηθούν ως εξής:

- *Νομιμότητα της επεξεργασίας των δεδομένων*: Το σύστημα θα πρέπει να είναι σε θέση να εξετάζει εάν η συλλογή και επεξεργασία των δεδομένων βρίσκεται σε συμφωνία

με τους ισχύοντες νόμους και κανονισμούς.

- *Σκοπός της επεξεργασίας των δεδομένων*: Το σύστημα θα πρέπει να παρέχει τα μέσα για την ταυτοποίηση των σκοπών της συλλογής και επεξεργασίας δεδομένων, οι οποίοι θα πρέπει να είναι έννομοι και να κοινοποιούνται με σαφήνεια στο υποκείμενο των δεδομένων. Επιπλέον, θα πρέπει το σύστημα να είναι σε θέση να πραγματοποιεί έλεγχο των σκοπών συλλογής και επεξεργασίας, ούτως ώστε να αποφεύγεται η περαιτέρω επεξεργασία δεδομένων για σκοπούς άλλους από εκείνους για τους οποίους πραγματοποιήθηκε η συλλογή τους.

- *Αναγκαιότητα, καταλληλότητα και αναλογικότητα των δεδομένων υπό επεξεργασία*: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι υφίστανται επεξεργασία μόνο δεδομένα τα οποία είναι λειτουργικά, απαραίτητα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται.

- *Ποιότητα των δεδομένων υπό επεξεργασία*: Το σύστημα θα πρέπει να φροντίζει ότι τα δεδομένα υπό επεξεργασία είναι σωστά, ακριβή και ενημερωμένα. Σε αντίθετη περίπτωση, τα δεδομένα θα πρέπει διορθώνονται, ενημερώνονται ή διαγράφονται.

- *Ταυτοποιήσιμα δεδομένα*: Το σύστημα θα πρέπει να παρέχει τα μέσα ούτως ώστε τα δεδομένα που υφίστανται επεξεργασία να διατηρούνται σε μορφή που να ταυτοποιούν το υποκείμενο των δεδομένων μόνο για το χρονικό διάστημα το οποίο είναι απαραίτητο προκειμένου να επιτευχθούν οι σκοποί της επιδιωχθείσας επεξεργασίας.

- *Ειδικές κατηγορίες δεδομένων — ευαίσθητα δεδομένα*: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι η επεξεργασία ειδικών κατηγοριών δεδομένων θα πραγματοποιείται σε συμφωνία με τις συγκεκριμένες απαιτήσεις οι οποίες ορίζονται από την ισχύουσα νομοθεσία. Για παράδειγμα, ο Νόμος 2472/1997 ορίζει ως ευαίσθητα *"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"*, ενώ το Άρθρο 6 του Νόμου 3471/2006 θεσπίζει ειδικούς κανόνες για τα δεδομένα θέσης και κίνησης.

- *Πληροφόρηση, συγκατάθεση και λοιπά δικαιώματα των υποκειμένων των δεδομένων*: Το σύστημα θα πρέπει να έχει τη δυνατότητα να ενημερώνει τα υποκείμενα των δεδομένων αναφορικά με την επεξεργασία των δεδομένων τους. Επιπλέον, το σύστημα θα πρέπει να εγγυάται ότι η ρητή συγκατάθεση των υποκειμένων των δεδομένων θα απαιτείται προκειμένου να πραγματοποιηθεί επεξεργασία των δεδομένων, εφόσον η ισχύουσα νομοθεσία ορίζει σχετικά, ενώ η επεξεργασία οποιασδήποτε μορφής των δεδομένων θα λαμβάνει χώρα λαμβάνοντας υπόψη τις προτιμήσεις των υποκειμένων των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπροσθέτως, το σύστημα θα

πρέπει να παρέχει τη δυνατότητα στα υποκείμενα των δεδομένων να εξασκούν τα δικαιώματα πρόσβασης στα δεδομένα τους τα οποία προβλέπονται από την ισχύουσα νομοθεσία. Τέτοια δικαιώματα πρόσβασης αφορούν –για παράδειγμα– την ενημέρωση των δεδομένων τα οποία βρίσκονται αποθηκευμένα σε κάποια βάση δεδομένων, τη διαγραφή τους, το δικαίωμα αποτροπής της επεξεργασίας τους, κλπ.

- *Ειδοποιήσεις και λοιπές αρμοδιότητες / εξουσιοδοτήσεις των αρμοδίων Αρχών*: Το σύστημα θα πρέπει να έχει τη δυνατότητα να παρακολουθεί τη συμμόρφωση με την απαίτηση για την παροχή ειδοποιήσεων προς την αρμόδια Αρχή Προστασίας Δεδομένων, καθώς και την παροχή οποιασδήποτε άλλης αρμοδιότητας / εξουσιοδότησης διαθέτει η Αρχή. Επιπλέον, το σύστημα θα πρέπει να παρέχει τα μέσα επικοινωνίας μεταξύ της Αρχής και του συστήματος.

- *Εποπτεία και επιβολή προστίμων*[7]: Οι αρμόδιες Αρχές Προστασίας Δεδομένων θα πρέπει να διαθέτουν τη δυνατότητα εποπτείας και ελέγχου όλων των ενεργειών συλλογής και επεξεργασίας προσωπικών δεδομένων.

- *Διασύνδεση δεδομένων*: Η διασύνδεση δεδομένων μπορεί να λάβει χώρα μόνο υπό συγκεκριμένους όρους και σε κάθε περίπτωση κατόπιν ενημέρωσης προς την αρμόδια Αρχή. Επιπλέον, σύμφωνα με το Άρθρο 8 του Νόμου 3471/2006, *"εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων, ή εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνον με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης)"*.

- *Ασφάλεια και εμπιστευτικότητα*: Το σύστημα τα πρέπει να είναι ασφαλές, ούτως ώστε να είναι σε θέση να εγγυηθεί την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, προστατεύοντάς τα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, εξασφαλίζοντας επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Επιπλέον, το σύστημα θα πρέπει να είναι σε θέση να αποτρέπει την οποιαδήποτε υποκλοπή ή παρακολούθηση των δεδομένων εκτός εάν υπάρχει η ρητή συγκατάθεση του υποκειμένου των δεδομένων ή εφόσον προβλέπεται από την ισχύουσα νομοθεσία για λόγους που τεκμηριώνονται από το δημόσιο συμφέρον.

- *Περιορισμός πρόσβασης*: Το σύστημα τα πρέπει να παρέχει διαδικασίες εξουσιοδοτημένης πρόσβασης στα δεδομένα, το επίπεδο της οποίας θα πρέπει απαραιτήτως να διαφοροποιείται με βάση διάφορα κριτήρια, όπως το είδος των δεδομένων καθεαυτών, τους ρόλους και τους υποκείμενους σκοπούς. Επιπλέον, κάθε πρόσβαση σε δεδομένα θα πρέπει να καταγράφεται.

[7]Εξυπακούεται ότι η επιβολή προστίμων δεν είναι δυνατό να αποτελεί αντικείμενο ενός τεχνολογικού συστήματος· αναφέρεται ωστόσο εδώ για λόγους πληρότητας.

- *Αποθήκευση*: Το σύστημα θα πρέπει να διαγράφει ή καθιστά ανώνυμα με αυτόματο τρόπο εκείνα τα δεδομένα για τα οποία η αναγκαιότητά τους για την επίτευξη κάποιου σκοπού έχει λήξει ή για τα οποία έχει παρέλθει το οριζόμενο βάσει της νομοθεσίας χρονικό διάστημα διατήρησής τους.
- *Μεταφορά και διάδοση δεδομένων*: Όταν μέρος της επεξεργασίας ανατίθεται για εκτέλεση σε τρίτα μέρη, πρέπει να παρέχονται συγκεκριμένες εγγυήσεις ότι η συνακόλουθη επεξεργασία των δεδομένων είναι σύμφωνη με τους υποκείμενους κανονισμούς και συμβάσεις με το υποκείμενο των δεδομένων. Επιπλέον, ενώ η διαβίβαση δεδομένων προς χώρες – μέλη της Ευρωπαϊκής Ένωσης είναι ελεύθερη (σύμφωνα πάντα με τα παραπάνω), για τις υπόλοιπες χώρες ισχύουν ειδικοί κανόνες και συνθήκες. Γενικότερα, θα πρέπει να εξετάζονται τόσο ο τύπος των μεταφερόμενων δεδομένων όσο και οι συνθήκες υπό τις οποίες πραγματοποιείται η διατομεακή μεταφορά αυτών.

Οι παραπάνω απαιτήσεις θα αποτελέσουν τη βάση για το σχεδιασμό της προτεινόμενης λύσης, όπως θα περιγραφεί αναλυτικά στη συνέχεια της διατριβής.

Κεφάλαιο 3

Τεχνολογίες Υπηρεσιών, Ροών Εργασιών και Προστασίας Προσωπικών Δεδομένων

3.1 Τεχνολογίες Υπηρεσιών

3.1.1 Υπηρεσίες Ιστού

Οι *Υπηρεσίες Ιστού (Web Services)* παρέχουν ένα πλαίσιο για την ολοκλήρωση/ενοποίηση συστημάτων ανεξαρτήτως προγραμματιστικών γλωσσών και λειτουργικών συστημάτων και είναι συνεπώς κατάλληλες για την υποστήριξη διαλειτουργικών αλληλεπιδράσεων σε κατανεμημένα ετερογενή περιβάλλοντα. Επιπλέον, οι σχετικές τεχνολογίες προσφέρουν δυνατότητες συντονισμού πολλαπλών οντοτήτων που μπορεί να συμμετέχουν σε κάποιο δίκτυο συνεργασίας, με αποτέλεσμα να αποτελούν την επικρατέστερη επιλογή για την υλοποίηση αρχιτεκτονικών SOA. Στη συνέχεια παρουσιάζονται συνοπτικά αφενός η τριάδα των τεχνολογιών που συνιστούν κυριολεκτικά τα θεμέλια των Υπηρεσιών Ιστού (SOAP, WSDL, UDDI) και αφετέρου κάποιες επιπρόσθετες προδιαγραφές, χαρακτηριζόμενες από το πρόθεμα WS-* στο όνομά τους, οι οποίες επιλαμβάνονται κάποιων πιο εξειδικευμένων, εντούτοις όμως κρίσιμων, πλευρών των Υπηρεσιών Ιστού, όπως η αξιόπιστη παράδοση,η ασφάλεια, η δρομολόγηση και η προδιαγραφή πολιτικών.

Οι αλληλεπιδράσεις μεταξύ Υπηρεσιών Ιστού, δηλαδή αιτήματα από οντότητες–αιτούντες υπηρεσίες προς τις υπηρεσίες αυτές και οι αποκρίσεις των τελευταίων στους πρώτους βασίζονται στο *SOAP*[8] [51][52][53], μια προδιαγραφή του W3C[9], η οποία συνιστά ένα πρωτόκολλο επικοινωνίας βασισμένο σε XML για την ανταλλαγή πληροφοριών μεταξύ

[8]Η λέξη SOAP ήταν, κατά την πρώτη εμφάνιση του πρωτοκόλλου, τα αρχικά του Simple Object Access Protocol· ωστόσο από την έκδοση 1.2 και μετά δεν είναι πια ακρωνύμιο.

[9]`http://www.w3.org/`

υπολογιστών ανεξαρτήτως λειτουργικού συστήματος, προγραμματιστικού περιβάλλοντος ή πλαισίου μοντελοποίησης αντικειμένων, αντιμετωπίζοντας έτσι τα προβλήματα που δημιουργεί η συνύπαρξη συστημάτων τα οποία έχουν δημιουργηθεί μη ακολουθώντας καθολικά καθιερωμένα πρότυπα σε ετερογενείς υποδομές. Το SOAP αποτελεί, κατά συνέπεια, ένα εύχρηστο πρωτόκολλο, κατάλληλο για την ανταλλαγή δομημένης και τυποποιημένης πληροφορίας μεταξύ υπολογιστών και συστημάτων σε ένα αποκεντρωμένο και κατανεμημένο περιβάλλον, καθιστώντας επιπλέον δυνατή τη μετάδοση σύνθετων τύπων μηνυμάτων κατά μήκος ενός δικτύου, τον καλύτερο χειρισμό των πιθανών σφαλμάτων και την αυτοματοποίηση μεγάλου μέρους των διαδικασιών αναδιάταξης παραμέτρων μεθόδων και επιστρεφόμενων τιμών.

Η *Γλώσσα Περιγραφής Υπηρεσιών Ιστού (Web Services Description Language Version 2.0 – WSDL)* [54][55], πρότυπο του W3C, πραγματοποιεί τη λεπτομερή περιγραφή των διεπαφών που οι Υπηρεσίες Ιστού εκθέτουν στο εξωτερικό τους περιβάλλον, επιτρέποντας έτσι την πρόσβαση σε αυτές. Η WSDL αντιπροσωπεύει ένα είδος συμβολαίου ανάμεσα στον πάροχο και τον αιτούντα την υπηρεσία, ανεξάρτητου από πλατφόρμα και γλώσσα υλοποίησης, και χρησιμοποιείται κατά κύριο λόγο (αλλά όχι αποκλειστικά) για την περιγραφή υπηρεσιών που ακολουθούν το πρωτόκολλο SOAP. Η προδιαγραφή WSDL αποτελείται από δύο διακριτά μέρη, καθένα από τα οποία μπορεί να οριστεί ανεξάρτητα και να αναχρησιμοποιηθεί από το άλλο: τη *διεπαφή υπηρεσίας (service interface)*, η οποία περιγράφει όλες τις λειτουργίες που παρέχονται από την υπηρεσία, τις παραμέτρους τους και τους αντίστοιχους (αφηρημένους) τύπους δεδομένων, και την *υλοποίηση της υπηρεσίας (service implementation)*, η οποία παρέχει συγκεκριμένη πληροφορία για την πρόσβαση στην υπηρεσία. Και τα δύο αυτά τμήματα από κοινού προσφέρουν στον αιτούντα επαρκείς πληροφορίες για τον εντοπισμό της υπηρεσίας και την κλήση οποιασδήποτε από τις διαθέσιμες λειτουργίες της.

Το πρότυπο της *Καθολικής Περιγραφής, Ανακάλυψης και Ολοκλήρωσης (Universal Description, Discovery and Integration – UDDI)* του OASIS [56] βασίζεται σε ένα σύνολο κοινά αποδεκτών προτύπων, συμπεριλαμβανομένων των HTTP, XML, XML Schema και SOAP, και δημιουργήθηκε με σκοπό να παρέχει έναν ενιαίο τρόπο για την περιγραφή των επιχειρήσεων και των υπηρεσιών που αυτές προσφέρουν και την καταχώρησή τους σε κάποιο κατάλογο (μητρώο), ώστε οι εν λόγω υπηρεσίες να μπορούν να ανακαλυφθούν και εν συνεχεία να "καταναλωθούν". Το UDDI χρησιμοποιεί SOAP στο στρώμα μεταφοράς, συνεπώς οι εξωτερικές οντότητες μπορούν να αλληλεπιδράσουν με τα μητρώα UDDI μέσω κλήσεων SOAP και να αποκτήσουν πρόσβαση σε τεχνική πληροφορία αναφορικά με τις υπηρεσίες κάποιας επιχείρησης.

Περνώντας στην οικογένεια των WS-* προτύπων, το *WS-ReliableMessaging* [57] περιγράφει μια γενική υποδομή που επιτρέπει, μέσα από το συνδυασμό της με άλλες προδιαγραφές Υπηρεσιών Ιστού και διαφορετικά κατά περίπτωση εφαρμογής πρωτόκολλα, την αξιόπιστη διανομή μηνυμάτων SOAP μεταξύ κατανεμημένων εφαρμογών ακόμα και υπό την παρουσία βλαβών του συστήματος ή του δικτύου, προδιαγράφοντας έναν αριθμό *Εγ-*

γυήσεων Παράδοσης (Delivery Assurances). Το *WS-Addressing* [58], από την άλλη, προσφέρει έναν τρόπο για την αποτύπωση, με ενιαίο τρόπο και ανεξαρτήτως υποκείμενων τεχνολογιών, πληροφορίας που τυπικά παρέχεται από πρωτόκολλα μεταφοράς και ανάλογα συστήματα, ούτως ώστε αυτή να καθίσταται διαθέσιμη στο στρώμα των υπηρεσιών.

Περισσότερο συναφή με το αντικείμενο της διατριβής, ωστόσο, είναι πρότυπα που αφορούν στην ασφάλεια και τα διάφορα είδη πολιτικών σε περιβάλλοντα Υπηρεσιών. Το πρότυπο *Web Services Policy Framework (WS-Policy)* [59] προσφέρει ένα μοντέλο για τη διατύπωση πολιτικών, ικανό να εκφράσει όλους τους τύπους πολιτικών που μπορεί να αφορούν από την ασφάλεια σε επίπεδο μεταφοράς μέχρι περιορισμούς στη χρήση πόρων, QoS χαρακτηριστικά και από άκρο σε άκρο πολιτικές στο επίπεδο επιχειρησιακών διαδικασιών. Έτσι, τόσο πάροχοι όσο και καταναλωτές υπηρεσιών μπορούν να εκφράζουν τις απαιτήσεις και τις δυνατότητές τους αναφορικά με τις μεταξύ τους αλληλεπιδράσεις. Το πρότυπο αυτό συμπληρώνεται στις λειτουργίες από τέσσερα ακόμα: το *WS-PolicyAssertions*[10] ορίζει τη δομή κάποιων γενικών τύπων εγγυήσεων· το *WS-Policy Attachment* [60] επιτρέπει το συσχετισμό μιας πολιτικής με μια συγκεκριμένη Υπηρεσία· το *WS-MetadataExchange* [61] παρέχει έναν ενιαίο τρόπο ανταλλαγής μεταδεδομένων, συμπεριλαμβανομένων και πολιτικών· το *WS-SecurityPolicy* [62] προδιαγράφει ένα πρότυπο σύνολο συγκεκριμένα εγγυήσεων ασφάλειας, με βάση απαιτήσεις που αφορούν την προστασία των SOAP μηνυμάτων. Από την άλλη, το πρότυπο *WS-Security* [63] προσδιορίζει τους τρόπους εφαρμογής κατάλληλων κρυπτογραφικών μηχανισμών, συγκεκριμένα της XML Κρυπτογραφίας (XML Encryption) [64] και των XML Υπογραφών (XML Signature) [65] σε μηνύματα SOAP, με στόχο την ανά μήνυμα αυθεντικοποίηση και την από άκρο σε άκρο εμπιστευτικότητα και ακεραιότητα των μηνυμάτων, καθώς και της υποδομής XML Key Management Specification (XKMS) [66]. Η προδιαγραφή *WS-Trust* [67] βασίζεται σε και επεκτείνει τα παραπάνω πρότυπα, ορίζοντας μηχανισμούς για την αίτηση, έκδοση, ανανέωση, ακύρωση και επικύρωση τεκμηρίων ασφάλειας (security tokens), με σκοπό τη διαμεσολάβηση σε ό,τι αφορά σχέσεις εμπιστοσύνης και την αξιολόγησή τους. Τέλος, το *WS-SecureConversation* [68] συμπληρώνει τις παραπάνω προσεγγίσεις στην κατεύθυνση της ανταλλαγής πολλαπλών μηνυμάτων μέσω της δημιουργίας ενός γενικευμένου πλαισίου ασφάλειας (security context).

3.1.2 Σημασιολογικές Υπηρεσίες Ιστού

Οι Υπηρεσίες Ιστού είναι από τη φύση τους "συντακτικές", καθιστώντας αδύνατη ακόμα και την απλούστερη δυναμική σύνθεση ή άλλο αυτοματοποιημένο υπολογισμό. Συνεπώς, απαιτείται η συμπλήρωσή τους με τη σημασιολογική περιγραφή της λειτουργικότητάς τους, ώστε να υποστηρίζονται όχι μόνο κατανεμημένοι υπολογισμοί αλλά και η δυναμική ανακάλυψη, σύνθεση και εκτέλεση των υπηρεσιών, προσφέροντας παράλληλα άμεση ερμηνεία των υποκείμενων εννοιών τόσο στη φάση του σχεδιασμού όσο και της εκτέλεσης. Οι αντίστοιχες προσεγγίσεις, που προκύπτουν από το συνδυασμό των Υπηρε-

[10] `http://www.ibm.com/developerworks/library/specification/ws-polas/`

σιών Ιστού με τις τεχνολογίες του σημασιολογικού ιστού, αναφέρονται ως *Σημασιολογικές Υπηρεσίες Ιστού (Semantic Web Services – SWS)*. Οι τελευταίες συνίστανται ουσιαστικά στην επέκταση των Υπηρεσιών Ιστού με τη σαφή και λεπτομερή αντιστοίχισή τους σε συγκεκριμένα νοήματα και αποτελούν ένα ισχυρό εργαλείο για τη μετατροπή του σημερινού συντακτικού Ιστού σε ένα δυναμικό και σημασιολογικό σύστημα, βασισμένο στην έννοια του σκοπού. Σε αυτή την κατεύθυνση, οι οντολογίες παρέχουν τα μέσα για την επεξεργασία σημασιολογικά εμπλουτισμένης πληροφορίες και την επίλυση σύνθετων προβλημάτων διαλειτουργικότητας, καθώς διέπονται από δύο βασικές αρχές: την κοινή ερμηνεία των εννοιών και η τυπική σημασιολογία. Σε σύγκριση με τις συντακτικές γλώσσες που χρησιμοποιούνται για τον ορισμό ταξινομιών, όπως η XML, οι οντολογίες επιτρέπουν επιπλέον το συστηματικό ορισμό εννοιών και ιδιοτήτων, περιορισμών και κανόνων που τους αφορούν, καθώς επίσης και των σχέσεων και λειτουργικών που τους χαρακτηρίζουν.

Συγκεκριμένα, όταν δύο υπολογιστικά συστήματα επικοινωνούν, όλες οι εμπλεκόμενες όψεις της επικοινωνίας είναι εν δυνάμει μη συμβατές σημασιολογικά και ως εκ τούτου πιθανά πεδία αντινομιών· ωστόσο, η σημασιολογία διαδραματίζει σημαντικό ρόλο σε κυρίως δύο τομείς: στις ασυμφωνίες δεδομένων και συμπεριφοράς. Η σημασιολογία δεδομένων πραγματεύεται την περιγραφή δομών δεδομένων και λεξιλογίων, η οποία επιτρέπει ιδανικά την απόλυτη σε σημασιολογικό επίπεδο "συνεννόηση" μεταξύ δύο ή περισσότερων συστημάτων λογισμικού που ανταλλάσσουν δεδομένα. Από την άλλη, η σημασιολογία συμπεριφοράς επικεντρώνεται στην ορθή αλληλουχία ανταλλαγής μηνυμάτων ή στιγμιοτύπων δεδομένων μεταξύ των συστημάτων και αφορούν στο σημασιολογικό ταίριασμα της συμπεριφοράς ενός παρόχου υπηρεσιών με αυτή των καταναλωτών των υπηρεσιών του.

Η πρώτη σχετική προσέγγιση που εμφανίστηκε ήταν η *OWL-S* [69], μια οντολογία OWL που στοχεύει στην αυτόματη ανακάλυψη, κλήση, σύνθεση και παρακολούθηση πόρων Ιστού που προσφέρουν υπηρεσίες, μέσω της επισημείωσης των τελευταίων με σημασιολογική πληροφορία προερχόμενη από τις τρεις υπο-οντολογίες της [70].

Στη συνέχεια, το *Πλαίσιο Σημασιολογικών Υπηρεσιών Ιστού (Semantic Web Services Framework – SWSF)* [71] πρότεινε μια πιο περιεκτική και διεξοδική λύση, παρέχοντας ένα πλήρες εννοιολογικό μοντέλο διατυπωμένο με τη χρήση πρωτοβάθμιας λογικής (first-order logic), την *Οντολογία Σημασιολογικών Υπηρεσιών Ιστού (Semantic Web Services Ontology – SWSO)*, και μια γλώσσα αρκετά εκφραστική ώστε να περιγράφει το μοντέλο διαδικασιών Υπηρεσιών Ιστού, τη *Γλώσσα Σημασιολογικών Υπηρεσιών Ιστού (Semantic Web Services Language – SWSL)*. Οι βασικές καινοτομίες της SWSF έναντι της OWL-S είναι η χρήση πρωτοβάθμιας γλώσσας, η οποία διευκολύνει τον ορισμό της οντολογίας υπηρεσιών καθεαυτής και ενός πιο περιεκτικού μοντέλου διαδικασιών. Η SWSO διαθέτει ένα πλούσιο συμπεριφορικό μοντέλο διαδικασιών βασισμένο στην προϋπάρχουσα διεθνή πρότυπη οντολογία για κατασκευαστικές διαδικασίες PSL (Process Specification Language) [72], την οποία επεκτείνει με έννοιες απαραίτητες για εφαρμογές Υπηρεσιών Ιστού, όπως μηνύματα, κανάλια,

δεδομένα εισόδου και εξόδου.

Από την άλλη, η *Οντολογία Μοντελοποίησης Υπηρεσιών Ιστού (Web Service Modeling Ontology – WSMO)* [73] έχει ως υπόβαθρο το *Πλαίσιο Μοντελοποίησης Υπηρεσιών Ιστού (Web Service Modeling Framework – WSMF)*, το οποίο επεκτείνει και βελτιώνει με σκοπό την οντολογική προδιαγραφή των βασικών στοιχείων των SWS. Η WSMO είναι στην ουσία μια μεταοντολογία, η οποία καθορίζει το πώς μπορούν να κατασκευαστούν άλλες οντολογίες και αποτελείται σε υψηλό επίπεδο από τέσσερα στοιχεία: τις Οντολογίες (Ontologies), τους Σκοπούς (Goals), τις Υπηρεσίες Ιστού (Web Services) και τους Μεσάζοντες (Mediators). Η απαραίτητη συντακτική και τυπική σημασιολογία για το εννοιολογικό μοντέλο της WSMO παρέχεται από την οικογένεια γλωσσών *WSML (Web Services Modeling Language)* [74] [75], ενώ το *Περιβάλλον Μοντελοποίησης και Εκτέλεσης Υπηρεσιών Ιστού (Web Service Modeling Execution Environment – WSMX)* [76][77] προσφέρει λειτουργικότητα μεσισμικού για την αξιοποίηση των σημασιολογικών επισημειώσεων Υπηρεσιών Ιστού με χρήση του μοντέλου WSMO.

Τέλος, οι *WSDL-S* [78] και *Semantic Annotations for WSDL and XML Schema (SAWSDL)* [79] προτείνουν την εισαγωγή σημασιολογικών επισημειώσεων στις WSDL περιγραφές των Υπηρεσιών Ιστού, αξιοποιώντας τους μηχανισμού επεκτασιμότητας της WSDL. Σε αντίθεση με τις OWL-S, SWSO και WSMO, δεν ορίζουν κάποιο εννοιολογικό μοντέλο ούτε κάποια γλώσσα περιγραφής μοντέλων και μάλιστα είναι ανεξάρτητες των αντίστοιχων χρησιμοποιούμενων τεχνολογιών· αντ' αυτού παρέχουν μηχανισμούς με χρήση των οποίων έννοιες από το εκάστοτε σημασιολογικό μοντέλο μπορούν να προσπελαστούν από το εσωτερικό ενός εγγράφου WSDL μέσω επισημειώσεων.

3.1.3 Σύνθεση Υπηρεσιών

Οι τεχνολογίες Υπηρεσιών Ιστού δίνουν τη δυνατότητα ορισμού και κλήσης υπηρεσιών που χαρακτηρίζονται από σχέσεις χαλαρής συσχέτισης μεταξύ τους. Αυτό από μόνο του, ωστόσο, δεν επαρκεί για τις περιπτώσεις όπου μια ομάδα υπηρεσιών πρέπει να συντονιστεί, ώστε να επιτύχει ένα κοινό σκοπό. Έτσι, η πραγματική χρησιμότητά των αρχιτεκτονικών SOA έγκειται στις δυνατότητες που παρέχουν για ευέλικτη σύνθεση των συμμετεχόντων υπηρεσιών.

Σύνθεση είναι η έννοια εκείνη η οποία καθιστά δυνατό τον ορισμό και την εκτέλεση διαδικασιών που έχουν τη μορφή επί μακρόν επικοινωνίας και αλληλεπίδρασης μεταξύ των συμμετεχόντων μερών και περιλαμβάνουν πολλαπλές κλήσεις υπηρεσιών με σαφώς καθορισμένο τρόπο. Για το σκοπό αυτό, η διαδικασία σύνθεσης υπηρεσιών περιλαμβάνει λειτουργίες και μεθόδους για τη συνένωση πολλών υπηρεσιών σε μια νέα σύνθετη υπηρεσία, περιγράφοντας τις μεταξύ τους σχέσεις. Το αποτέλεσμα είναι ουσιαστικά μια δομή διαδικασίας αποτελούμενη από ένα σύνολο υπηρεσιών, καθεμιά από τις οποίες επιτελεί μια συγκεκριμένη λειτουργία στα πλαίσια της διαδικασίας. Η προκύπτουσα σύνθετη υπη-

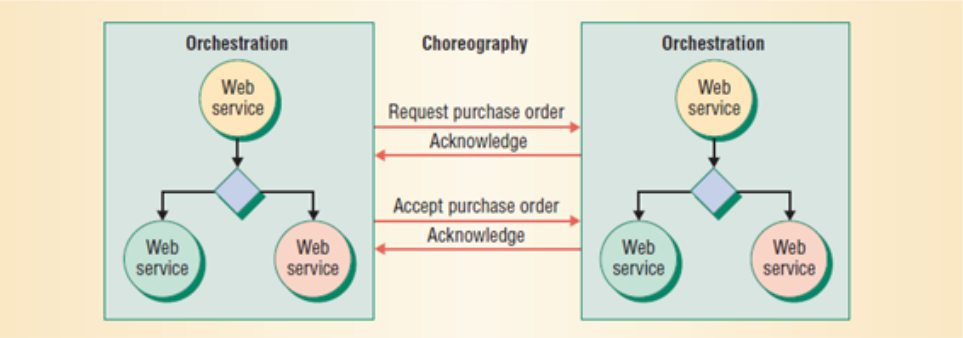
ρεσία μπορεί, από εκεί και πέρα, να χρησιμοποιηθεί ως δομική μονάδα σε περαιτέρω συνθέσεις υπηρεσιών ή να προσφερθεί ως ολοκληρωμένη τελική εφαρμογή σε κάποιο πελάτη.

Η σύνθεση υπηρεσιών μπορεί να περιγραφεί σε δύο μορφές, την *ενορχήστρωση* (orchestration) και τη *χορογραφία* (choreography). Οι όροι αυτοί χρησιμοποιούνται ευρέως για την περιγραφή πρωτοκόλλων αλληλεπιδράσεων που συντονίζουν και ελέγχουν συνεργαζόμενες υπηρεσίες, εκφράζοντας η καθεμιά διαφορετικές πλευρές μιας τέτοιας συνεργασίας [80]:

- Η ενορχήστρωση περιγράφει το πώς οι εμπλεκόμενες Υπηρεσίες Ιστού αλληλεπιδρούν μεταξύ τους σε επίπεδο μηνυμάτων, συμπεριλαμβανομένων της επιχειρησιακής λογικής και της σειράς εκτέλεσής τους από την οπτική γωνία και υπό τον έλεγχο μιας μοναδικής οντότητας, η οποία μπορεί από εκεί και πέρα να συμμετέχει ή όχι σε μια ευρύτερη συνεργασία με άλλη/άλλες οντότητες. Με την ενορχήστρωση, δηλαδή, οι επιχειρησιακές αλληλεπιδράσεις ελέγχονται πάντα από την (ιδιωτική) οπτική ενός εκ των συμμετεχόντων μερών που εμπλέκονται στη διαδικασία και συνεπώς αφορούν εσωτερικές του λειτουργίες μη ορατές στα μέρη με τα οποία μπορεί να βρίσκεται σε συνδιαλλαγή.

- Η χορογραφία, από την άλλη, είναι πιο συνεργατική στη φύση της, καθώς τυπικά σχετίζεται με τις δημόσιες (καθολικά ορατές) ανταλλαγές μηνυμάτων, τους κανόνες αλληλεπίδρασης και τις τυχόν συμφωνίες που λαμβάνουν χώρα μεταξύ πολλαπλών μερών συμμετεχόντων σε επιχειρησιακές διαδικασίες, και όχι, για παράδειγμα, με μια συγκεκριμένη διαδικασία εκτελούμενη από έναν συμμετέχοντα στα πλαίσια της εσωτερικής του λειτουργίας. Εκφράζει την οπτική όλων των μερών (κοινή άποψη) και ορίζει τη συμπληρωματική παρατηρούμενη συμπεριφορά μεταξύ των συμμετεχόντων σε μια επιχειρησιακή συνεργασία. Αυτή η κοινή άποψη ορίζει, στην ουσία, την από κοινού μοιραζόμενη κατάσταση των αλληλεπιδράσεων μεταξύ επιχειρησιακών οντοτήτων και μπορεί να χρησιμοποιηθεί ως βάση για τον καθορισμό συγκεκριμένων υλοποιήσεων για κάθε αυτόνομη οντότητα. Η χορογραφία προσφέρει τα μέσα με τα οποία μπορούν με σαφήνεια να οριστούν και συμφωνηθούν από κοινού οι κανόνες συμμετοχής σε μια συνεργασία, ενώ κάθε οντότητα μπορεί στη συνέχεια να υλοποιήσει το μέρος εκείνο της χορογραφίας που της αναλογεί. Η χορογραφία παρακολουθεί την αλληλουχία των μηνυμάτων, που μπορεί να περιλαμβάνει πολλαπλά μέρη και πηγές, όπως πελάτες, προμηθευτές και εταίρους, όπου κάθε εμπλεκόμενο μέρος περιγράφει το ρόλο που διαδραματίζει στην εν λόγω αλληλεπίδραση και κανένα από αυτά δεν ελέγχει τη συνδιαλλαγή συνολικά. Σε γενικές γραμμές, οι χορογραφίες διαδικασιών περιγράφουν την αλληλεπίδραση πολλαπλών αυτοπεριεκτικών επιχειρησιακών διαδικασιών και αποτελούν συνεπώς έννοια σημαντική για την υποστήριξη διεπιχειρησιακών (business-to-business) συνεργασιών.

Συμπερασματικά, οι όροι ενορχήστρωση και χορογραφία περιγράφουν δύο πλευ-



Σχήμα 2: Ενορχήστρωση και Χορογραφία. Η πρώτη αναφέρεται σε μια εκτελέσιμη διαδικασία· η δεύτερη αποτυπώνει την αλληλουχία μηνυμάτων μεταξύ των εμπλεκόμενων σε μια συνεργασία μερών [81].

ρές που σχετίζονται με τη δημιουργία επιχειρησιακών διαδικασιών με τη βοήθεια σύνθετων Υπηρεσιών Ιστού: κάθε σύνθεση υπηρεσιών έχει μια εσωτερική συμπεριφορά η οποία συνίσταται στην κλήση συνιστωσών με καθορισμένη σειρά (ενορχήστρωση) και μια εξωτερική που καθορίζει το πώς η σύνθεση αυτή αλληλεπιδρά με την οντότητα που την καλεί (χορογραφία). Η σχέση σε υψηλό επίπεδο μεταξύ των δύο όρων, οι οποίοι παρουσιάζουν κάποιο βαθμό επικάλυψης, απεικονίζεται στο Σχήμα 2.

Προκειμένου να πραγματοποιηθεί κάποια σύνθεση, θα πρέπει καταρχήν αυτή να σχεδιαστεί, καθορίζοντας την εσωτερική της συμπεριφορά. Τα βήματα που απαιτούνται είναι η αναγνώριση των συνιστωσών – Υπηρεσιών Ιστού που θα κληθούν, η κατανόηση των διεπαφών τους και ο ορισμός της σειράς κλήσης τους με βάση τις επιταγές των ροών ελέγχου και δεδομένων. Όταν αυτή η διαδικασία σχεδιασμού, η οποία θα οδηγήσει τελικά στην υλοποίηση της σύνθεσης, πραγματοποιείται με μη αυτόματο τρόπο, είναι ο μηχανικός λογισμικού εκείνος που πρέπει να εξασφαλίσει ότι η σύνθεση είναι σωστή όχι μόνο συντακτικά αλλά και σημασιολογικά, με την έννοια ότι η εκτέλεσή της "βγάζει νόημα", είναι με άλλα λόγια λειτουργικά αποδεκτή και οδηγεί στην επιθυμητή επιχειρησιακή κατάσταση. Αυτός ο μη αυτόματος προσδιορισμός οδηγεί σε *στατικές συνθέσεις*, των οποίων η εσωτερική συμπεριφορά οριστικοποιείται κατά τη φάση του σχεδιασμού. Στη φάση της εκτέλεσης δεν μπορεί να αλλάξει και μόνο στιγμιότυπα του αρχικού ορισμού μπορούν να δημιουργηθούν και εκτελεστούν. Οποιαδήποτε απαραίτητη αλλαγή θα πρέπει να πραγματοποιηθεί και πάλι στατικά και να διοχετευθεί στο περιβάλλον παραγωγής σύμφωνα με τον αντίστοιχο προγραμματισμό, ενώ ήδη υπό εκτέλεση στιγμιότυπα δεν επηρεάζονται από αυτή. Ακόμα και στην περίπτωση της διακλάδωσης υπό συνθήκη (conditional branching), όλες οι συνθήκες, καθώς και όλες οι ανά περίπτωση καλούμενες συνιστώσες, θα πρέπει να οριστούν κατά το σχεδιασμό, προκειμένου οι στατικές αυτές συνθέσεις να μπορούν να προσαρμοστούν σε συνθήκες πραγματικού χρόνου. Οι κυριότερες τεχνολογίες που υποστηρίζουν αυτή τη στατική προσέγγιση είναι οι WS-BPEL, WS-Choreography και WS-CDL.

Η *Γλώσσα Εκτέλεσης Επιχειρησιακών Διαδικασιών Υπηρεσιών Ιστού (Web Service Business Process Execution Language – WS-BPEL)* [82] αποτελεί πρότυπο του OASIS και την περισσότερο καθιερωμένη αυτή τη στιγμή γλώσσα σύνθεσης, προερχόμενη από τις προγενέστερες XLANG και WSFL [83]. Κατά βάση, η BPEL μοντελοποιεί τη συμπεριφορά Υπηρεσιών Ιστού σε αλληλεπιδράσεις υπηρεσιακών διαδικασιών. Παρέχει μια γραμματική βασισμένη σε XML για την περιγραφή της λογικής ελέγχου που απαιτείται για το συντονισμό υπηρεσιών που συμμετέχουν στη ροή μιας διαδικασίας και χρησιμοποιείται σε συνδυασμό με τη WSDL. Μια μηχανή ενορχήστρωσης μπορεί στη συνέχεια να εκτελέσει την προκύπτουσα περιγραφή, συντονίζοντας δραστηριότητες και αποκαθιστώντας τη συνολική διαδικασία στις περιπτώσεις σφαλμάτων. Μια διαδικασία ορισμένη σε BPEL συνιστά μια αναχρησιμοποιήσιμη οντότητα που μπορεί να χρησιμοποιηθεί ως υποδιαδικασία στα πλαίσια μιας άλλης πιο σύνθετης διαδικασίας. Η BPEL υποστηρίζει την προδιαγραφή αφενός *εκτελέσιμων* (ή ιδιωτικών) διαδικασιών, που μοντελοποιούν την ενορχήστρωση, και αφετέρου *αφηρημένων* (ή δημόσιων) διαδικασιών, που μοντελοποιούν τη χορογραφία υπηρεσιών. Επιπλέον, προβλέπει την ύπαρξη τόσο *βασικών* όσο και *δομημένων* δραστηριοτήτων, με τις πρώτες να αφορούν τη λήψη και αποστολή μηνυμάτων σε οντότητες εξωτερικές της διαδικασίας και την κλήση των υπηρεσιών καθεαυτών και τις δεύτερες να διαχειρίζονται τη συνολική ροή, ρυθμίζοντας την αλληλουχία των εν λόγω υπηρεσιών. Η BPEL διαθέτει επίσης δομές για τη μοντελοποίηση της ροής μηνυμάτων (*variable*) και των ρόλων που οι υπηρεσίες κατέχουν στα πλαίσια της διαδικασίας (*partnerLink*), ενώ διαθέτει εύρωστους μηχανισμούς διαχείρισης συναλλαγών και σφαλμάτων βασισμένους σε δύο άλλες προδιαγραφές, τις WS-Coordination [84] και WS-Transaction [11]. Η BPEL έχει καθιερωθεί ως το de-facto πρότυπο για την υλοποίηση επιχειρησιακών διαδικασιών βασισμένων σε Υπηρεσίες Ιστού. Πέραν τούτου και εξαιτίας της ωριμότητάς της, διάφορες επεκτάσεις της έχουν εμφανιστεί στη βιβλιογραφία, όπως η [85] στην κατεύθυνση της μοντελοποίησης πόρων ως μηχανών καταστάσεων αντί υπηρεσιών και η [86] που στοχεύει στο να υποστηρίζει εφαρμογές απαιτητικές ως προς τον όγκο δεδομένων προς επεξεργασία.

Από την άλλη, η *Χορογραφία Υπηρεσιών Ιστού (Web Service Choreography – WS-Choreography)* [87] είναι μια προδιαγραφή του W3C που ορίζει μια γλώσσα μοντελοποίησης επιχειρησιακών διαδικασιών βασισμένη σε XML, η οποία περιγράφει πρωτόκολλα συνεργασίας μεταξύ υπηρεσιών που δρουν ως ομότιμες οντότητες συμμετέχουσες σε καταστασιακές επί μακρών αλληλεπιδράσεις. Εξάλλου, το βασικότερο εγχείρημα στο θέμα της χορογραφίας προέρχεται από την ομάδα Web Services Choreography Working Group[12] του W3C, η οποία ολοκλήρωσε τις εργασίες της το 2009 με τη *Γλώσσα Περιγραφής Χορογραφίας Υπηρεσιών Ιστού (Web Service Choreography Description Language – WS-CDL)* [88] και αντικαθιστώντας με αυτή την προγενέστερη, αν και επιδραστική, *Διεπαφή Χορογραφίας Υπηρεσιών Ιστού (Web Service Choreography Interface – WSCI)* [89]. Η WS-CDL είναι μια γλώσσα βασισμένη σε XML για την περιγραφή του τρόπου με τον οποίο Υπηρεσίες Ιστού που συμμετέχουν σε μια

[11] `http://www.ibm.com/developerworks/library/specification/ws-tx/`
[12] `http://www.w3.org/2002/ws/chor/`

χορογραφία συνεργάζονται ως ομότιμες οντότητες. Η περιγραφή αυτή ορίζει την κοινή συμπεριφορά των υπηρεσιών και τη σειρά των ανταλλασσόμενων μηνυμάτων με σκοπό την επίτευξη ενός κοινού σκοπού. Στόχος των χορογραφιών Υπηρεσιών Ιστού είναι η σύνθεση ομότιμων αλληλεπιδράσεων μεταξύ οποιουδήποτε είδους υπηρεσιών, ανεξαρτήτως προγραμματιστικής γλώσσας ή του περιβάλλοντος στο οποίο ανήκει καθεμιά από αυτές. Συνακόλουθα, η WS-CDL περιγράφει τη συνολική και παρατηρήσιμη συμπεριφορά των εμπλεκόμενων μερών, άσχετα με το πώς αυτή η συμπεριφορά υλοποιείται εσωτερικά, κάτι που μπορεί να χρησιμοποιηθεί ως βάση για κάποιου είδους "συμβόλαιο" μεταξύ των μερών αυτών. Πράγματι, στην WS-CDL η συνεργασία μεταξύ Υπηρεσιών Ιστού λαμβάνει χώρα στα πλαίσια ενός συνόλου από συμφωνίες σχετικές με κανόνες αλληλουχίας και ανάλογους περιορισμούς.

Παρά τις προαναφερθείσες προσπάθειες, η σύνθεση Υπηρεσιών Ιστού παραμένει μια αρκετά πολύπλοκη εργασία και ο χειρισμός της όλης διαδικασίας δεν είναι πια δυνατός με μη αυτόματο τρόπο. Η πολυπλοκότητα συνίσταται σε γενικές γραμμές στα ακόλουθα [90]: πρώτα απ' όλα, ο αριθμός των διαθέσιμων στον Ιστό υπηρεσιών που θα πρέπει να αναζητηθούν αυξάνει δραματικά τα τελευταία χρόνια· κατά δεύτερον, οι Υπηρεσίες Ιστού δημιουργούνται και μεταβάλλονται δυναμικά, οπότε και το εκάστοτε σύστημα σύνθεσης οφείλει να ανιχνεύει τις αλλαγές που συμβαίνουν κατά τη φάση της εκτέλεσης και να λαμβάνει αποφάσεις με βάση την ανανεωμένη κάθε φορά πληροφορία· τρίτον, οι όποιες Υπηρεσίες μπορεί να αναπτύσσονται από διαφορετικούς οργανισμούς, οι οποίοι χρησιμοποιούν διαφορετικά εννοιολογικά μοντέλα για την περιγραφή τους, ενώ δεν υπάρχει κάποια μοναδική γλώσσα για τον ορισμό και την αποτίμηση των Υπηρεσιών Ιστού με πανομοιότυπο τρόπο. Συνεπώς, η δημιουργία σύνθετων Υπηρεσιών Ιστού με κάποιο αυτόματο ή ημιαυτόματο εργαλείο είναι καθοριστικής σημασίας. Οι περισσότερες προσεγγίσεις που έχουν εμφανιστεί σε αυτή την κατεύθυνση στηρίζονται είτε στις τεχνολογίες ροών εργασιών (βλ. πιο κάτω) είτε στην τεχνική του Σχεδιασμού Ενεργειών από την περιοχή της Τεχνητής Νοημοσύνης (AI Planning), σε συνδυασμό με Σημασιολογικές Υπηρεσίες Ιστού. Συγκεκριμένα, οι ροές εργασιών χρησιμοποιούνται κυρίως σε περιπτώσεις όπου ο αιτών τη σύνθεση έχει ήδη ορίσει το μοντέλο της διαδικασίας που επιθυμεί να εκτελεστεί σε υψηλό επίπεδο και από εκεί και πέρα απαιτείται κάποιος αυτοματισμός για τον εντοπισμό και δέσμευση των επί μέρους συγκεκριμένων υπηρεσιών που μπορούν να ικανοποιήσουν το αίτημα (ημιαυτόματη σύνθεση) [91][92][93][94][95] [96]. Οι μέθοδοι Σχεδιασμού Ενεργειών χρησιμοποιούνται όταν ο αιτών δεν έχει ορίσει κάποιο μοντέλο, παρά μόνο ένα σύνολο από περιορισμούς και προτιμήσεις, με βάση τα οποία το μοντέλο της διαδικασίας προκύπτει αυτόματα (αυτόματη σύνθεση). Οι προσεγγίσεις της τελευταίας κατηγορίας δεν έχουν φτάσει σε υψηλό επίπεδο ωριμότητας και κατά συνέπεια συναντώνται κυρίως σε ερευνητικό ακόμα επίπεδο, μολονότι έχουν δώσει κάποια αρκετά ενδιαφέροντα αποτελέσματα, όπως [97][98][99][100][101][102][103] και το CASCOM[13]. Από την άλλη, οι ροές εργα-

[13]FP6 IST-511632 project CASCOM (Context-Aware Business Application Service Coordination in Mobile Computing Environments), home page: http://www.ist-cascom.org/

σιών αποτελούν αρκετά ώριμη τεχνολογία και είναι αυτές που κυρίως χρησιμοποιούνται όταν πρόκειται για τη σύνθεση υπηρεσιών, καθώς εναρμονίζονται σε μεγάλο βαθμό με το υπόδειγμα των αρχιτεκτονικών τύπου SOA.

3.2 Μηχανισμοί και Πρότυπα στις Αρχιτεκτονικές Προσανατολισμένες σε Υπηρεσίες

Το θεμελιώδες συστατικό ολοκλήρωσης υπηρεσιών σε μια αρχιτεκτονική τύπου SOA είναι ο *Επιχειρησιακός Δίαυλος Υπηρεσιών (Enterprise Service Bus – ESB)* [1][104]. Ο ESB συνιστά ένα κορμό υλοποιημένο με βάση ανοιχτά πρότυπα για τη στήριξη χαλαρά συσχετισμένων SOA αρχιτεκτονικών, ο οποίος επιτρέπει την προσβασιμότητα σε άκρως κατανεμημένους προορισμούς κατά μήκος ενός διαύλου μηνυμάτων πολλαπλών πρωτοκόλλων, διασπώντας παράλληλα τη λογική ενοποίησης σε εύκολα διαχειρίσιμα μέρη. Επιτυγχάνει ορθό έλεγχο μηνυμάτων, με χρήση οποιουδήποτε αριθμού πιθανών πρωτοκόλλων, υποστηρίζει ποικίλα μοτίβα δρομολόγησης ([105]) και καλύπτει τις ανάγκες για ασφάλεια, μηχανισμούς πολιτικών, διαλειτουργικότητα, αξιοπιστία και κοστολόγηση/τιμολόγηση. Το μοντέλο αυτό καθιστά δυνατή μια πιο αποδοτική ενοποίηση πληθώρας διαφορετικών εφαρμογών προβάλλοντάς τες ως υπηρεσίες με χρήση Υπηρεσιών Ιστού (βλ. 3.1.1). Έτσι, ένας ESB συνδυάζει ουσιαστικά εφαρμογές και διακριτά συστατικά ολοκλήρωσης με σκοπό τη "συναρμολόγηση" υπηρεσιών και τη δημιουργία σύνθετων επιχειρησιακών διαδικασιών (βλ. Ενότητα 3.1.3), πράγμα που με τη σειρά του αυτοματοποιεί τις λειτουργίες μιας επιχείρησης.

Ιδιαίτερη μορφή αρχιτεκτονικών SOA συνιστούν μια σειρά από προσεγγίσεις που βασίζονται σε *συμβάντα (Event-driven SOA)*[106] και οι οποίες συνδυάζουν την ευφυΐα των αρχιτεκτονικών υπολογιστών βασισμένων σε συμβάντα με τις δυνατότητες ενός περιβάλλοντος υπηρεσιών. Πριν τις αντίστοιχες τεχνολογίες, η τυπική SOA πλατφόρμα ενορχήστρωνε τις υπηρεσίες κεντρικά, μέσω προκαθορισμένων διαδικασιών, θεωρώντας ότι οτιδήποτε θα πρέπει να εκτελεστεί έχει οριστεί ως μέρος της διαδικασίας (βλ. Ενότητα 3.1.3). Αυτή η πρώτη προσέγγιση δε λαμβάνει υπόψη συμβάντα τα οποία ανακύπτουν είτε μέσα στα πλαίσια μιας διαδικασίας είτε και έξω από αυτή. Συνεπώς, οι διαδικασίες δεν μπορούν να σχεδιάζονται θεωρώντας εκ των προτέρων ότι τα συμβάντα είναι προκαθορισμένα και ακολουθούν μια συγκεκριμένη ροή, αλλά πρέπει να ορίζονται δυναμικά, οδηγούμενες από εισερχόμενες, παράλληλες και ασύγχρονες ροές συμβάντων. Μια τέτοια αντιμετώπιση προσφέρει μεγαλύτερη ευελιξία, καθώς απαιτεί ότι οι δύο συμμετέχοντες σε κάποιο συμβάν (πελάτης και εξυπηρετητής) είναι πλήρως αποσυσχετισμένοι (και όχι απλά χαλαρά συσχετισμένοι), έτσι ώστε οι συμμετέχοντες να μη χρειάζεται να έχουν καμία γνώση ο ένας για τον άλλον προτού προχωρήσουν στην όποια συνδιαλλαγή. Η όποια σχέση είναι έμμεση και πραγματοποιείται μέσω του ESB, στον οποίο πελάτες και εξυπηρετητές καταχωρούνται ως πηγές συμβάντων ή/και συνδρομητές σε αυτά.

Στο πλαίσιο αυτό, και εναρμονισμένο με τις σχέσεις χαλαρής συσχέτισης που χαρακτηρίζουν τις κατανεμημένες αλληλεπιδράσεις σε εφαρμογές μεγάλης κλίμακας, το υπόδειγμα επικοινωνίας *Δημοσίευση/Συνδρομή* (Publish/Subscribe) δίνει τη δυνατότητα πλήρους αποσυσχέτισης σε τρεις διαστάσεις: χρόνο, χώρο και συγχρονισμό [107]. Στα συστήματα Δημοσίευσης/Συνδρομής, οι οντότητες–συνδρομητές υποβάλλουν προς καταχώρηση το ενδιαφέρον τους για κάποιο συμβάν ή μοτίβο συμβάντων και στη συνέχεια ενημερώνονται ασύγχρονα για συμβάντα προερχόμενα από οντότητες που τα δημοσιεύουν και τα οποία ταιριάζουν με το δηλωμένο ενδιαφέρον τους. Το συμβάν καθεαυτό ενθυλακώνει κάποια δραστηριότητα, η οποία αποτελεί πλήρη περιγραφή μιας συγκεκριμένης δράσης. Οι παραλήπτες συμβάντων απαιτούν μεταδεδομένα αναφορικά με αυτά, που οργανώνονται από τις οντότητες–πηγές συμβάντων στη βάση κάποια (τοπικής) ταξινομίας. Έτσι, ενώ οι διεπαφές υπηρεσιών είναι στατικές και προκαθορισμένες, μεταδεδομένα συσχετιζόμενα με συμβάντα δημιουργούνται δυναμικά και περιγράφουν τα ίδια τα δημοσιευμένα συμβάντα, στα οποία μπορούν να "εγγράφονται" οντότητες–συνδρομητές, τις διεπαφές πελατών και εξυπηρετητών υπηρεσιών, τα μηνύματα που ανταλλάσσουν, καθώς και το συμφωνημένο μορφότυπο και περιεχόμενο αυτών των μεταδεδομένων, χωρίς να υπάγονται τα ίδια στις τυπικές περιγραφές υπηρεσιών. Υπάρχουν διάφορες παραλλαγές για το σχεδιασμό συστημάτων Δημοσίευσης/Συνδρομής, με κυριότερες αυτές που βασίζονται στο θέμα (topic-based), στο περιεχόμενο (content-based) και στον τύπο (type-based), που προσφέρουν διαφορετικούς βαθμούς εκφραστικότητας η καθεμιά. Σε ό,τι αφορά τον ESB, η λειτουργικότητα Δημοσίευσης/Συνδρομής επιτυγχάνεται από τη μια μέσω των καθιερωμένων τεχνολογιών Υπηρεσιών Ιστού, συμπεριλαμβανομένων των SOAP, WSDL και BPEL, καθώς και ανερχόμενων προτύπων όπως WS-ReliableMessaging [57] and WS-Notification [108] (βλ. Ενότητα 3.1.1).

Όπως είναι αναμενόμενο, η έννοια των SOA έχει προσελκύσει σε μεγάλο βαθμό το ενδιαφέρον της κοινότητας σχεδίασης και ανάπτυξης λογισμικού. Το *Μοντέλο Αναφοράς για Αρχιτεκτονικές Προσανατολισμένες σε Υπηρεσίες (Service Oriented Architecture Reference Model – SOA RM)* [109] του οργανισμού OASIS [14], το οποίο παρουσιάστηκε το 2005, είναι μια αφηρημένη αρχιτεκτονική η οποία ορίζει και ενσωματώνει έννοιες και σχέσεις προορισμένες να αποτελέσουν τη βάση για την περιγραφή αρχιτεκτονικών και προτύπων αναφοράς με σκοπό τον ορισμό πιο ειδικών κατηγοριών SOA σχεδιασμών. Κεντρική έννοια αυτού του μοντέλου είναι αυτή της *Υπηρεσίας*, γύρω από την οποία ορίζονται επιπλέον οι ακόλουθες, είτε δυναμικές είτε στατικές, έννοιες: *Περιγραφή Υπηρεσιών (Service Description)*, *Ορατότητα (Visibility)*, *Αλληλεπίδραση (Interaction)*, *Επενέργεια στον Πραγματικό Κόσμο (Real World Effect)*, *Πλαίσιο Εκτέλεσης (Execution Context)*, *Συμβόλαιο και Πολιτική (Contract & Policy)*. Επιπρόσθετα, η *Αρχιτεκτονική Συνιστωσών Υπηρεσιών (Service Component Architecture – SCA)*[15] είναι ένα σύνολο προδιαγραφών, επίσης του OASIS, οι οποίες περιγράφουν ένα μοντέλο για τη δημιουργία εφαρμογών και συστημάτων με χρήση αρχιτεκτονι-

[14] http://www.oasis-open.org/

[15] `http://www.oasis-opencsa.org/sca`

κών SOA, επεκτείνοντας και συμπληρώνοντας προηγούμενες προσεγγίσεις και βασιζόμενο σε ανοιχτά πρότυπα, όπως είναι οι Υπηρεσίες Ιστού (βλ. Ενότητα 3.1.1). Το μοντέλο SCA υποστηρίζει τόσο τη σύνθεση υπηρεσιών όσο και τη δημιουργία συνιστωσών υπηρεσιών, ενώ στοχεύει στο να συμπεριλάβει μια ευρεία γκάμα τεχνολογιών συνιστωσών υπηρεσιών και μεθόδων πρόσβασης σε αυτές με σκοπό τη διασύνδεσή τους. Τέλος, λαμβάνει υπόψη και μη λειτουργικές απαιτήσεις, όπως αυτή της ασφάλειας, ενώ διαθέτει επιπλέον ένα *Πλαίσιο Πολιτικής (Policy Framework)* με σκοπό να υποστηρίξει την προδιαγραφή περιορισμών και προσδοκιών σχετικών με δυνατότητες (capabilities) και Ποιότητα Υπηρεσιών (Quality of Service – QoS), ξεκινώντας από το σχεδιασμό συνιστωσών και φτάνοντας μέχρι την υλοποίησή τους. Από τη σκοπιά της μοντελοποίησης, η *Οντολογία για Αρχιτεκτονικές SOA (SOA Ontology)* [110] του Open Group[16], βασισμένη στη χρήση της Γλώσσας Οντολογιών Ιστού (Web Ontology Language – OWL) [111], στοχεύει στο να προωθήσει την κατανόηση και τη μοντελοκεντρική υλοποίηση των σχετικών εννοιών. Η *Γλώσσα Μοντελοποίησης Αρχιτεκτονικών Προσανατολισμένων σε Υπηρεσίες (Service oriented architecture Modeling Language – SoaML)* [112] είναι ένα πρότυπο του Open Management Group (OMG)[17], το οποίο ορίζει επεκτάσεις της UML για τη μοντελοποίηση υπηρεσιών και άλλων σχετικών εννοιών. Ουσιαστικά μπορεί να θεωρηθεί ως η ενσάρκωση σε μια συγκεκριμένη πλατφόρμα του προαναφερθέντος SOA RM, η οποία ενσωματώνει τη UML και υποστηρίζει τη μοντελοποίηση υπηρεσιών με βάση την επίσης προερχόμενη από τον OMG Μοντελοκεντρική Αρχιτεκτονική (Model-Driven Architecture – MDA)[18]. Τέλος, άλλες αξιόλογες προδιαγραφές στην περιοχή είναι οι *Reference Architecture for SOA Foundation* [113] του OASIS, *SOA Governance Framework* [114], *SOA Reference Architecture* [115] και *Service Integration Maturity Model (OSIMM)* [116] του Open Group.

3.3 Ροές Εργασιών

Οι *ροές εργασιών (workflows)*, δηλαδή, οι καλώς ορισμένες ακολουθίες εργασιών απαραίτητων για τη διαχείριση μιας επιχειρησιακής ή υπολογιστικής (π.χ., επιστημονικής, μηχανικής, κλπ.) διαδικασίας, έχουν αναδειχθεί τα τελευταία χρόνια ως η κυρίαρχη προσέγγιση για το συντονισμό ομάδων κατανεμημένων εργασιών [4]. Σε περιβάλλοντα λογισμικού προσανατολισμένα σε υπηρεσίες, οι ροές εργασιών πραγματοποιούνται μέσω της σύνθεσης, και πιο συγκεκριμένα μέσω της ενορχήστρωσης, Υπηρεσιών Ιστού. Με άλλα λόγια, η σύνθεση υπηρεσιών αποτελεί τη γέφυρα ανάμεσα στις SOA αρχιτεκτονικές και τις τεχνολογίες ροών εργασιών. Οι τελευταίες, ανάλογα με το πεδίο εφαρμογής τους και τις ανάγκες τις οποίες καλύπτουν, χωρίζονται σε δύο ευρείες κατηγορίες: τις επιχειρησιακές (business workflows) και τις επιστημονικές ροές εργασιών (scientific workflows).

Αρχικά η ροή εργασιών ορίστηκε από τον Συνασπισμό Διαχείρισης Ροών Εργασιών

[16] `http://www.opengroup.org/`
[17] `http://www.omg.org/`
[18] `http://www.omg.org/mda/specs.htm`

(Workflow Management Coalition – WfMC) ως: *"η αυτοματοποίηση μιας επιχειρησιακής διαδικασίας, συνολικά ή εν μέρει, κατά τη διάρκεια της οποίας οι πληροφορίες ή εργασίες περνούν από τον ένα συμμετέχοντα στον άλλον προκειμένου να ενεργήσει ανάλογα, σύμφωνα με ένα σύνολο διαδικαστικών κανόνων"* [117]. Συνεπώς, οι ροές εργασιών, έχοντας τις καταβολές τους στα πρώτα συστήματα αυτοματισμών γραφείου, είχαν εξαρχής επιχειρησιακό προσανατολισμό και κίνητρα και αποτελούν έκτοτε τον κορμό αυτού που ονομάζουμε Διαχείριση Επιχειρησιακών Διαδικασιών (Business Process Management – BPM) (βλ. Ενότητα 1.1). Συγκεκριμένα, οι (επιχειρησιακές) ροές εργασιών έθεσαν τις βάσεις για τη *Μοντελοποίηση Επιχειρησιακών Διαδικασιών (Business Process Modeling – BPM)* [118], δηλαδή την ενορχήστρωση διαδικασιών μέσω του προσδιορισμού δραστηριοτήτων που εκτελούνται στα πλαίσια ενός οργανισμού και των σχέσεων μεταξύ τους, η οποία αποτελεί τελικά τη δημοφιλέστερη μέθοδο σύνθεσης Υπηρεσιών Ιστού. Από αυτή την άποψη, η Διαχείριση Επιχειρησιακών Ροών Εργασιών και η Μοντελοποίηση Επιχειρησιακών Διαδικασιών αποτελούν ώριμες ερευνητικές περιοχές, με μια ποικιλία από πρότυπα εργαλεία και γλώσσες να τα υποστηρίζουν [119][120]. Εκτός από τις βασισμένες σε XML γλώσσες εκτέλεσης σύνθεσης Υπηρεσιών Ιστού που προαναφέρθηκαν, ιδιαίτερα σημαντικές θεωρούνται και οι τεχνολογίες BPMN [121], που αποτελεί και πρότυπο, και YAWL [122][123][124][125][126], οι οποίες εστιάζουν και στη μοντελοποίηση διαδικασιών.

Σε αυτό το σημείο θα ήταν χρήσιμο να διασαφηνιστεί η έννοια της ροής εργασιών σε αντιδιαστολή με εκείνη της επιχειρησιακής διαδικασίας, με την οποία συχνά συγχέεται. Σύμφωνα με τον WfMC, μια επιχειρησιακή διαδικασία σχετίζεται με κάθε είδους δραστηριότητα, αυτοματοποιημένη ή μη, η οποία πραγματοποιεί έναν επιχειρησιακό στόχο. Μια ροή εργασιών, από την άλλη, αποτελεί τη (μερική) αυτοματοποίηση μιας επιχειρησιακής διαδικασίας. Με βάση αυτή τη διάκριση, και όπως επισημαίνεται στο [127], η Διαχείριση Ροών Εργασιών (Workflow Management – WFM) εστιάζει στη δημιουργία και εκτέλεση διαδικασιών, ενώ ο πιο πρόσφατος όρος Διαχείριση Επιχειρησιακών Διαδικασιών συνιστά υπερσύνολο της Διαχείρισης Ροών Εργασιών, επεκτείνοντάς τη μέσω της υποστήριξης και άλλων σημαντικών διαστάσεων, όπως η Ανάλυση Επιχειρησιακών Διαδικασιών (Business Process Analysis – BPA), καθώς και άλλων τρόπων αντιμετώπισης των διαδικασιών εν γένει.

Από την άλλη, η διαχείριση επιστημονικών ροών εργασιών αποτελεί ένα πολύ πιο πρόσφατο φαινόμενο, πυροδοτούμενο από i) μια μεταστροφή προς εφαρμογές απαιτητικές ως προς τον όγκο δεδομένων προς επεξεργασία και προς υπολογιστικές μεθόδους που συναντώνται κυρίως στις φυσικές επιστήμες, και ii) τη συνακόλουθη ανάγκη για εργαλεία που μπορούν να απλοποιήσουν και αυτοματοποιήσουν επαναλαμβανόμενες υπολογιστικές εργασίες. Στο [128] οι Επιστημονικές ροές εργασιών ορίζονται ως *"εκτελέσιμες περιγραφές αυτοματοποιήσιμων επιστημονικών διαδικασιών, όπως είναι οι υπολογιστικές επιστημονικές προσομοιώσεις και οι αναλύσεις δεδομένων"*. Αν και έχουν αναπτυχθεί διάφορα συστήματα επιστημονικών ροών εργασιών [129][130][131][132][133][134][135][136][137][138][128], δεν έχει ακόμα προκύψει κάποια προτυποποίηση, καθώς φαίνεται αναπόφευκτο κάθε

τέτοιο σύστημα να είναι τελικά προσαρμοσμένο στη βάση του στις ανάγκες ενός συγκεκριμένου επιστημονικού πεδίου.

Οι δύο αυτές κατηγορίες ροών εργασιών αναμφίβολα παρουσιάζουν ομοιότητες ως προς τα κίνητρα, τη γενική φιλοσοφία και τις απαιτήσεις, εμφανίζουν ωστόσο και διαφορές, που πηγάζουν από τους σκοπούς τους οποίους εξυπηρετούν. Συγκεκριμένα οι επιχειρησιακές ροές εργασιών επικεντρώνονται στη *ροή ελέγχου (control-flow)*, δηλαδή στις εξαρτήσεις προτεραιότητας και την αλληλουχία εκτέλεσης των εμπλεκόμενων εργασιών, και προβλέπουν/ υποστηρίζουν την επέμβαση του ανθρώπινου παράγοντα, ενώ η *ροή δεδομένων (data-flow)* συχνά υπονοείται ή μοντελοποιείται ξεχωριστά· οι επιστημονικές ροές εργασιών, αντίθετα, είναι σε μεγάλο βαθμό αυτοματοποιημένες και επικεντρωμένες στη ροή δεδομένων, με άλλα λόγια, η εκτέλεση οδηγείται από τις εξαρτήσεις δεδομένων μεταξύ των εργασιών, επιτρέποντας συγχρόνως την προδιαγραφή πιο πολύπλοκων διαδικασιών επεξεργασίας δεδομένων [139][140][141]. Από τις παραπάνω τεχνολογίες, μόνο η YAWL και η BPEL φαίνονται σε κάποιο βαθμό ικανές να αποτελέσουν μια κοινή λύση τόσο για το επιχειρησιακό όσο και για το επιστημονικό πεδίο [136][142].

Επιπρόσθετα, σημαντική συνεισφορά της επιστημονικής κοινότητας που δραστηριοποιείται στην περιοχή έχει αποτελέσει η αναγνώριση των εξής τριών βασικών όψεων σε κάθε ροή εργασιών:

- της *όψης ροής ελέγχου (control-flow perspective)*, η οποία αναφέρεται στις μορφές μου μπορούν να πάρουν οι σχέσεις διαδοχής και αλληλεπίδρασης (πλην της ανταλλαγής δεδομένων) μεταξύ των εργασιών, όπως επίσης και στα διάφορα είδη εξαρτήσεων που επηρεάζουν την εκτέλεσή τους.

- της *όψης δεδομένων (data perspective)*, η οποία αφορά στους τρόπους διάθεσης, κυκλοφορίας και μετάδοσης των δεδομένων στα πλαίσια των ροών εργασιών, καθώς και στην επίδραση της ροής δεδομένων στις άλλες όψεις και κυρίως σε αυτή της ροής ελέγχου.

- της *όψης πόρων (resource perspective)*, η οποία εστιάζει στη μοντελοποίηση των πόρων, ανθρώπινων (π.χ., κάποιος εργαζόμενος) ή μη (π.χ., οποιουδήποτε τύπου εξοπλισμός), που αναλαμβάνουν την εκτέλεση εργασιών, και της αλληλεπίδρασής τους με το εκάστοτε πληροφοριακό σύστημα με επίγνωση διαδικασιών.

Συνακόλουθα προέκυψαν, με προεξάρχουσες τις ομάδες των Πανεπιστημίων Τεχνολογίας του Eindhoven (Καθ. Wil van der Aalst) και του Queensland (Καθ. Arthur ter Hofstede), τα αντίστοιχα *μοτίβα* (workflow patterns)[19], με σκοπό την ανεξάρτητη από γλώσσα σχεδιασμού και υποκείμενη τεχνολογία φορμαλιστική περιγραφή των θεμελιωδών απαιτήσεων μοντελοποίησης των ροών εργασιών. Έτσι, τα μοτίβα ροής ελέγχου, δεδομένων και πόρων συνιστούν δομές οι οποίες συναντώνται και χρησιμοποιούνται συχνά κατά τη σχεδί-

[19]http://www.workflowpatterns.com/

αση και εκτέλεση ροών εργασιών σε σχέση με τις αντίστοιχες όψεις και κυρίως είτε είναι προσανατολισμένα στις Επιχειρησιακές ροές εργασιών είτε αφορούν εξαρτήσεις που εμπίπτουν και στις δύο κατηγορίες [143][144][145], αν και έχουν εμφανιστεί και προτάσεις που σχετίζονται ειδικά με επιστημονικές ροές εργασιών [146]. Τέτοια μοτίβα αποτελούν πλέον έναν καθιερωμένο τρόπο αξιολόγησης γλωσσών και συστημάτων διαχείρισης ροών εργασιών [147][148][149], καταδεικνύοντας το γεγονός ότι καμιά τεχνολογία δεν μπορεί από μόνη της να καλύψει επαρκώς όλες τις όψεις των ροών εργασιών και σίγουρα όχι κατά τον ίδιο τρόπο· επιπλέον, και όπως ήταν αναμενόμενο, οι επιχειρησιακές ροές εργασιών υποστηρίζουν ικανοποιητικά τις όψεις ελέγχου και πόρων, ενώ οι επιστημονικές άπτονται κυρίως της όψης των δεδομένων, προσφέροντας περιορισμένη ή και καθόλου υποστήριξη των περισσότερων μοτίβων πόρων και ελέγχου (π.χ., εκτέλεση υπό συνθήκη και χειρισμός εξαιρέσεων). Οι παραπάνω αποκλίσεις οδήγησαν σε έναν αριθμό προσπαθειών με σκοπό τη δημιουργία νέων (όπως συνέβη με τη YAWL) ή την ενίσχυση υπαρχόντων προσεγγίσεων στην κατεύθυνση της ενσωμάτωσης όσο το δυνατόν περισσότερων όψεων και μοτίβων [150][151][152], την ενοποίηση των ροών δεδομένων και ελέγχου [153][154][155][156], καθώς και την παροχή μιας κοινής τεχνολογικής λύσης για το σχεδιασμό και την εκτέλεση τόσο επιχειρησιακών όσο και επιστημονικών ροών εργασιών, προκειμένου να καταστεί δυνατός ο συνδυασμός των πλεονεκτημάτων και της χρησιμότητας και των δύο [157].

Παράλληλα, μια κοινή κατηγορία εφαρμογών που εμπίπτουν και στα δύο πεδία, επιχειρησιακό και επιστημονικό, και η οποία εξελίσσεται ταχύτατα, επωφελούμενη ιδιαίτερα και από την ανάπτυξη των τεχνολογιών Υπολογιστικού Νέφους (Cloud Computing) και Υπολογιστικού Πλέγματος (Grid Computing) [158][159], συνίσταται σε εφαρμογές παρακολούθησης (monitoring) και αντίδρασης (reactive), οι οποίες περιλαμβάνουν την επεξεργασία συνεχών ρευμάτων δεδομένων (data streams). Σχετικά παραδείγματα αποτελούν οι εφαρμογές οικονομικής ανάλυσης που παρακολουθούν ρεύματα δεδομένων τιμών μετοχών για την υποστήριξη της λήψης αποφάσεων σε χρηματιστηριακές εταιρίες και οι εφαρμογές περιβαλλοντικής ανάλυσης που συλλέγουν και αναλύουν δεδομένα αισθητήρων προερχόμενα από δορυφόρους, μετρητές στάθμης βροχής ή και έξυπνους μετρητές (smart meters) σε κατοικίες [160][161][162]. Παρ' όλα αυτά, τα παραδοσιακά συστήματα εκτέλεσης και οι σχετικές διαδικασίες σχεδιασμού ροών εργασιών αντιμετωπίζουν τις τελευταίες με τη λογική της αλληλεπίδρασης μία μόνο φορά με τις διάφορες πηγές δεδομένων και της εκτέλεσης μιας σειράς βημάτων από μία φορά το καθένα, σε κάθε περίσταση που ζητούνται τα αποτελέσματα της εκάστοτε ροής. Η θεμελιώδης υποκείμενη εικασία ήταν μέχρι τώρα ότι οι πηγές δεδομένων είναι στατικές και ότι όλες οι αλληλεπιδράσεις δομούνται γύρω από το μοντέλο αιτήματος/απόκρισης ("ερωτήματος")· αυτό συνεπάγεται τη θεώρηση ότι οι μεγάλες ποσότητες δεδομένων αποθηκεύονται και προσπελαύνονται περιοδικά, και όχι ότι υπόκεινται σε ανάλυση συνεχόμενα και άμεσα κατά την πρώτη εμφάνισή τους στο σύστημα. Συνεπώς, τα κλασικά συστήματα διαχείρισης ροών εργασιών δεν μπορούν να υποστηρίξουν αποτελεσματικά επιχειρησιακές ή επιστημονικές εφαρμογές παρακολούθησης που απαιτούν την επεξεργασία ρευμάτων δεδομένων. Αυτός ο νέος

τύπος κατανεμημένων εφαρμογών απαιτητικών ως προς τον όγκο δεδομένων προς επεξεργασία, που προσελκύει ολοένα και περισσότερο την προσοχή της σχετικής ερευνητικής δραστηριότητας, εισάγει την ανάγκη για την κατά κάποιο τρόπο ενσωμάτωση των φυσικών αντικειμένων στις ροές εργασιών [163] και για τη μετατόπιση από τις παραδοσιακές στις "συνεχείς" ροές εργασιών, οδηγώντας σε νέες απαιτήσεις, νέες δομές δεδομένων και νέα μοτίβα αλληλεπίδρασης [164][165][162]: η βασική διαφορά είναι ότι τέτοιες συνεχείς ροές εργασιών είναι μόνιμα εν ενεργεία αντιδρώντας διαρκώς είτε σε εσωτερικά ρεύματα συμβάντων είτε σε ρεύματα νέας πληροφορίας προερχόμενης από πολλαπλές εξωτερικές πηγές, την ίδια στιγμή και σε οποιοδήποτε σημείο του δικτύου της εκάστοτε ροής εργασιών.

Στη συνέχεια παρουσιάζονται συνοπτικά οι πιο επιδραστικές τεχνολογίες ροών εργασιών που αφορούν στο κομμάτι της μοντελοποίησής τους, καθώς ο συγκεκριμένος τομέας σχετίζεται άμεσα με τους στόχους της διατριβής.

3.3.1 Business Process Model and Notation (BPMN)

Η πρώτη έκδοση της γλώσσας BPMN [166] (τότε με πλήρη ονομασία "Business Process Modeling Notation") δημοσιεύτηκε το 2004 από τον Business Process Modeling Initiative (BPMI), προτού υιοθετηθεί δυο χρόνια αργότερα από τον Object Management Group (OMG). Η BPMN έχει εξελιχθεί σε μια πλούσια γλώσσα μοντελοποίησης και μέχρι στιγμής αποτελεί το πρότυπο αναφοράς στην περιοχή της μοντελοποίησης ροών εργασιών.

Η BPMN έχει ως επίκεντρο τα διαγράμματα επιχειρησιακών διαδικασιών (business process diagrams – BPDs) και βασίζεται σε μεγάλο βαθμό σε θεμελιακά στοιχεία της σημειογραφίας των διαγραμμάτων ροής (flowcharts). Τα διαγράμματα BPMN ενσωματώνουν πέντε κατηγορίες στοιχείων: α) τα σύμβολα ροής (flow objects), β) τα δεδομένα (data), γ) τα σύμβολα διασύνδεσης (connecting objects), δ) τα πλαίσια (swimlanes) και ε) τα αντικείμενα (artifacts). Τα σύμβολα ροής είναι τα κατεξοχήν γραφικά στοιχεία τα οποία ορίζουν τη συμπεριφορά μιας ροής εργασιών, εκπροσωπώντας Δραστηριότητες (Activities), Γεγονότα (Events) και ρυθμιστές ροής ή Πύλες (Gateways). Οι Πύλες εκφράζουν λογική εκτέλεσης, παρέχοντας τη δυνατότητα διαχωρισμού και ενοποίησης μονοπατιών ελέγχου μέσω δομών οι οποίες συμβολίζουν σημεία απόφασης/σύγκλισης, περιεκτικής (OR) ή αποκλειστικής διάζευξης (XOR), παράλληλης διακλάδωσης/ενοποίησης, κλπ.. Τα σύμβολα διασύνδεσης χρησιμοποιούνται για τη διασύνδεση συμβόλων ροής, με βασικότερα μεταξύ αυτών τη Ροή Αλληλουχίας (Sequence Flow), η οποία συνίσταται σε κατευθυνόμενες ακμές που σηματοδοτούν τη σειρά εκτέλεσης των Δραστηριοτήτων, και τη Ροή Μηνύματος (Message Flow), που σηματοδοτεί την ανταλλαγή Μηνυμάτων (Messages) μεταξύ συμμετεχόντων. Η διακινούμενη πληροφορία εκπροσωπείται από Αντικείμενα Δεδομένων (Data Objects), ενώ τα Αποθετήρια Δεδομένων (Data Stores) μοντελοποιούν την αλληλεπίδραση Δραστηριοτήτων με στοιχεία αποθήκευσης δεδομένων. Η έννοια του πλαισίου, από την άλλη, εξυπηρετεί τη διάκριση μεταξύ διαφορετικών συμμετεχόντων στη ροή εργασιών, τμηματο-

ποιώντας κατάλληλα το σχετικό διάγραμμα επιχειρησιακής διαδικασίας· υλοποιεί συνεπώς στην ουσία την όψη των πόρων μιας ροής εργασιών, συνεπικουρούμενη σε αυτό από τη χρήση κατάλληλων ιδιοτήτων στο επίπεδο κάθε μεμονωμένης Δραστηριότητας. Τέλος, τα αντικείμενα χρησιμοποιούνται για την ενσωμάτωση επιπλέον πληροφοριών που μπορεί να σχετίζονται με μια διαδικασία, παίρνοντας, για παράδειγμα, τη μορφή επισημειώσεων κειμένου.

Σε γενικές γραμμές, η BPMN χαρακτηρίζεται από σχετικά καλή ισορροπία σε ό,τι αφορά την κάλυψη των τριών προαναφερθεισών όψεων των ροών εργασιών: ελέγχου, δεδομένων και πόρων. Υποστηρίζει αρκετά μοτίβα αλληλεπίδρασης ελέγχου, μοντελοποιεί με σαφή τρόπο την πρόσβαση σε και τη ροή δεδομένων και σχηματοποιεί βασικές πλευρές της ανάθεσης Δραστηριοτήτων σε πόρους. Η BPMN 2.0 [121], μάλιστα, έχει ενσωματώσει διάφορες βελτιώσεις, συμπεριλαμβανομένης της εισαγωγής επεκτάσεων αναφορικά με γραφικά στοιχεία, αλλά και ευρύτερα με το τι μπορεί να μοντελοποιηθεί, νέα σύμβολα, ακριβέστερη σημασιολογική υπόσταση, ενώ, σε αντίθεση με την προκάτοχό της, είναι επιπλέον απευθείας εκτελέσιμη, απαλείφοντας έτσι την ανάγκη για σειριοποίησή της σε άλλο κατάλληλο μορφότυπο (π.χ., XPDL).

Παρ' όλα αυτά, η BPMN έχει δεχθεί σοβαρή κριτική (π.χ., [167]) σε σχέση με ζητήματα όπως η εκφραστικότητα, η σημασιολογική ακρίβεια, κάποιες αμφισημίες που παρουσιάζει η προδιαγραφή της, καθώς και η μερικές φορές περιττή πολυπλοκότητά της, τα οποία έχουν πρακτικά ως αποτέλεσμα τη σημαντική υποχρησιμοποίησή της [168]. Εξάλλου, η υποστήριξη της αναπαράστασης της ροής δεδομένων παραμένει περιορισμένη, καθώς απουσιάζουν, για παράδειγμα, μέσα για τη μοντελοποίηση εξεζητημένων συσχετίσεων μεταξύ των δεδομένων, ενώ τα Αντικείμενα Δεδομένων εξακολουθούν να παίζουν δευτερεύοντα ρόλο [169]. Επιπλέον, σύμφωνα με το [170], ούτε η όψη των πόρων καλύπτεται επαρκώς: τα πλαίσια και οι σχετικές ιδιότητες των δραστηριοτήτων δεν προσφέρουν τη δυνατότητα για λεπτομερή προδιαγραφή ανάθεσης εργασιών σε πόρους, ενώ περίπλοκοι ανάλογοι περιορισμοί, όπως ο Διαχωρισμός Καθηκόντων (Separation of Duties) επίσης δεν υποστηρίζονται.

Τα παραπάνω είχαν σαν αποτέλεσμα η BPMN να βρεθεί κατά καιρούς στο επίκεντρο διάφορων ερευνητικών προσπαθειών με στόχο την αντιμετώπιση των σχετικών ελλείψεων· έτσι, έχουν προταθεί διάφορες επεκτάσεις στην κατεύθυνση της ενίσχυσης των όψεων πόρων και δεδομένων (π.χ., [150] [151]), ενώ στο [171] εξετάζεται το ζήτημα της διατύπωσης εξουσιοδοτήσεων σχετικών με πιο σύνθετες μορφές ανάθεσης σε πόρους. Παρόμοια, εργασίες από την περιοχή της Μοντελοκεντρικής Ασφάλειας (Model Driven Security) (π.χ., Wolter2009) πραγματεύονται τον ορισμό απαιτήσεων ασφάλειας σε αφηρημένο επίπεδο ως μέρος των ίδιων των προδιαγραφών επιχειρησιακών διαδικασιών και τη συνακόλουθη μετάφρασή τους σε ρυθμίσεις ασφάλειας της εκάστοτε συγκεκριμένης πλατφόρμας (platform-specific).

3.3.2 Yet Another Workflow Language (YAWL)

Η YAWL [122] ξεχωρίζει πρωτίστως λόγω των ευρείας κλίμακας δυνατοτήτων μοντελοποίησης που διαθέτει και της με ακρίβεια ορισμένης τυπικής σημασιολογικής βάσης της· η τελευταία, προερχόμενη από τα Δίκτυα Petri (Petri Nets) [172], και για την ακρίβεια τα δίκτυα ροών εργασιών (WF-Nets) [3], καθιστούν τη YAWL κατάλληλη τόσο για τη μοντελοποίηση όσο και για την απευθείας εκτέλεση των επιχειρησιακών διαδικασιών.

Παρά το σχετικά περιορισμένο αριθμό γραφικών στοιχείων που περιλαμβάνει, η YAWL υποστηρίζει εκτενώς σχεδόν όλα τα μοτίβα ροής ελέγχου που καταγράφηκαν αρχικά [173], και σίγουρα περισσότερα από οποιαδήποτε άλλη γλώσσα, κάτι που εξάλλου αποτέλεσε και βασικό κίνητρο για την ανάπτυξή της. Μια προδιαγραφή YAWL είναι ένα ιεραρχικό, και με κάποιες επεκτάσεις, WF-Net (extended WF-Net – EWF-Net), αποτελούμενο από εργασίες (μεταβάσεις – transitions) και συνθήκες (μέρη – places). Μια εργασία μπορεί να είναι είτε απλή (atomic) είτε σύνθετη (composite), οπότε και αναλύεται σε μια υπο-ροή εργασιών (sub-workflow), δηλαδή ένα χαμηλότερου επιπέδου EWF-Net. Μπορεί, επίσης, να χαρακτηρίζεται ως "πολλαπλών στιγμιοτύπων", υποδεικνύοντας ότι επιτρέπει την παράλληλη εκτέλεση πολλαπλών στιγμιοτύπων της. Η YAWL υποστηρίζει επίσης την ακύρωση της εκτέλεσης εργασιών, περιπτώσεων (cases), κλπ. με χρήση ειδικής σημειολογίας που υποδηλώνει την απομάκρυνση της σκυτάλης εκτέλεσης. Διάφορα μοτίβα διακλάδωσης ροής υποστηρίζονται ευθέως μέσω ειδικών τύπων εργασιών που μοντελοποιούν διαίρεση και σύγκλιση AND/OR/XOR, ενώ η όψη των δεδομένων ενσωματώνεται με χρήση των τεχνολογιών XML Schema, XPath και XQuery. Επιπλέον η YAWL παρέχει τη δυνατότητα για διαχείριση σφαλμάτων [174], καθώς και για την προδιαγραφή δυναμικών ροών εργασιών μέσω της προσέγγισης των Worklets [123].

Εν όψει της αναθεώρησης του αρχικού συνόλου των μοτίβων ροής ελέγχου [145] αλλά και της εισαγωγής, στο μεταξύ, των μοτίβων δεδομένων [175] και πόρων [176], προτάθηκε μια επέκταση της YAWL, η επονομαζόμενη *new*YAWL [126], της οποίας η τυπική βάση έγκειται στα Coloured Petri Nets [177]. Η *new*YAWL επεκτείνει δραστικά το βαθμό στον οποίο η YAWL καλύπτει τις σχετικές όψεις, προσθέτοντας διάφορα επιπλέον χαρακτηριστικά στην αρχική προδιαγραφή. Ενδελεχείς στρατηγικές δρομολόγησης καθορίζουν τους συμμετέχοντες σε μια ροή εργασιών με βάση ποικίλα χαρακτηριστικά. Περαιτέρω προσδιορισμοί είναι δυνατοί μέσω της χρήσης περιορισμών (π.χ., retain familiar, four eyes principle, κλπ.), ενώ υποστηρίζονται επίσης διάφοροι μηχανισμοί ανάθεσης και στρατηγικές αλληλεπίδρασης. Αναφορικά με την όψη των δεδομένων, η *new*YAWL άπτεται ζητημάτων όπως η διατήρηση δεδομένων (persistence), η ταυτόχρονη πρόσβαση (concurrency) και άλλοι σύνθετοι τρόποι χειρισμού των δεδομένων, τα οποία αγνοούνται από πολλές γλώσσες ροών εργασιών.

Συνολικά, η YAWL είναι στην τωρινή της κατάσταση αρκετά ισχυρή και προφανώς πιο εκφραστική σε σύγκριση με το πρότυπο της BPMN σε ό,τι αφορά τη ροή ελέγχου και τη

διαχείριση πόρων. Ωστόσο, όπως παρατηρείται και στο [169], στερείται δομών ικανών να αποτυπώνουν με ακρίβεια οντότητες δεδομένων και εξαρτήσεις μεταξύ αυτών· η οποιαδήποτε επίγνωση δεδομένων περιορίζεται στο επίπεδο της μηχανής YAWL, όπου, και πάλι, μόνο κάποια βασικά στοιχεία προσφέρονται. Εξάλλου, τα ίδια τα θεμέλια της YAWL έχουν επίσης δεχτεί σημαντική κριτική. Ενδεικτικά, στο [167] υποστηρίζεται ότι ούτε τα Μοτίβα Ροών Εργασιών ούτε τα Δίκτυα Petri είναι επαρκώς κατάλληλα για να αποτελέσουν τη βάση ενός ευρέως αποδεκτού BPM συστήματος, ενώ, από την άλλη, αμφισβητούνται βασικά χαρακτηριστικά που υποτίθεται ότι αποτελούν αποκλειστικότητα της YAWL, όπως ο περιορισμένος αριθμός γραφικών δομών, η ευελιξία και η καλώς ορισμένη τυπική βάση.

3.3.3 Επιστημονικές Ροές Εργασιών

.

Οι επιστημονικές ροές εργασιών παρέχουν περιγραφές διαδικασιών που χρησιμοποιούνται για τη διεξαγωγή υπολογιστικών πειραμάτων και αναλύσεων προς επίτευξη επιστημονικών στόχων. Αναπαριστώνται κατά κύριο λόγο μέσω εργασιών, οι οποίες αντανακλούν υπολογιστικά βήματα, και των εξαρτήσεών τους· η συνήθης μορφή αφαίρεσης που χρησιμοποιείται είναι αυτή των κατευθυνόμενων γράφων, όπου οι κόμβοι αντιπροσωπεύουν εργασίες και οι ακμές υποδηλώνουν εξαρτήσεις δεδομένων.

Τα συστήματα επιστημονικών ροών εργασιών αναλαμβάνουν την εκτέλεση των επιστημονικών ροών εργασιών, προσφέροντας λειτουργικότητες που περιλαμβάνουν, μεταξύ άλλων, την ανακάλυψη και ανάθεση πόρων, την ενορχήστρωση, την παραλληλία σε ό,τι αφορά την εκτέλεση εργασιών αλλά και τον κύκλο ζωής των δεδομένων, καθώς και τη διαπίστωση της πορείας εκτέλεσης και της προέλευσης των δεδομένων. Επίσης, πολλά τέτοια συστήματα περιλαμβάνουν κατάλληλα περιβάλλοντα για το σχεδιασμό και τη σύνθεση ροών εργασιών. Μια ιδιομορφία των επιστημονικών ροών εργασιών είναι ότι οι υπάρχουσες τεχνολογίες απευθύνονται σε διαφορετικούς τομείς εφαρμογών η καθεμιά, με χαρακτηριστικά παραδείγματα τις φυσικές και περιβαλλοντικές επιστήμες, τη βιοπληροφορική, την ιατρική, την αστρονομία και τη μηχανική, που εμφανίζουν όπως είναι φυσικό διαφορετικές απαιτήσεις, με αποτέλεσμα τα αντίστοιχα συστήματα [132][131] να χαρακτηρίζονται από αποκλίσεις στην αρχιτεκτονική και τη λειτουργία τους. Ωστόσο, παρά τις διαφορές τους, κοινός παρονομαστής όλων των επιστημονικών ροών εργασιών είναι ο σαφής προσανατολισμός τους στη ροή δεδομένων και τα αντίστοιχα σημασιολογικά και υπολογιστικά μοντέλα που εφαρμόζουν.

Ένα αντιπροσωπευτικό και σχετικά καθιερωμένο σύστημα επιστημονικών ροών εργασιών είναι το Kepler [132]. Σε αυτό, κάθε μοντέλο ροής εργασιών είναι μια σύνθεση ανεξάρτητων μεταξύ τους οντοτήτων, των επονομαζόμενων δραστών (actors), που αντιπροσωπεύουν λειτουργίες ή πηγές δεδομένων και μπορούν να είναι απλοί ή σύνθετοι. Η ροή δεδομένων μοντελοποιείται μέσω καναλιών που συνδέουν τις θύρες εισόδου και εξό-

δου των δραστών, καθένα από τα οποία θεωρείται ότι μεταφέρει ένα μόνο ρεύμα δεδομένων. Το πρότυπο μοντελοποίησης που ακολουθείται βασίζεται στην έννοια του συμπεριφορικού πολυμορφισμού (behavioural polymorphism), σύμφωνα με τον οποίο, με δεδομένο ένα σχηματισμό δραστών μπορούν να οριστούν διαφορετικά μοτίβα εκτέλεσης, μέσω της επιλογής διαφορετικών συντονιστών (directors), όπως είναι ο συντονιστής Synchronous Data-Flow (SDF), ο Dynamic Data-Flow (DDF) ή ο Process Network (PN). Έτσι, υποστηρίζονται πολλαπλά ετερογενή υπολογιστικά μοντέλα (Models of Computation – MoC), επιτρέποντας την αναπαράσταση συστημάτων διαφορετικής φύσης. Με άλλα λόγια, ενώ κάθε δράστης υλοποιεί μια συγκεκριμένη λειτουργία, η συμπεριφορά του μπορεί να αλλάζει στη βάση του MoC που υιοθετείται κάθε φορά. Επιπρόσθετα, σημειώνεται ότι το Kepler υποστηρίζει την ιεραρχική ενσωμάτωση μιας ροής εργασιών σε άλλη, με προϋπόθεση τη συμβατότητα των συντονιστών τους, ώστε να μπορούν να σχηματιστούν ιεραρχικά πολύπλοκα μοντέλα συνδυάζοντας ακόμα και διαφορετικά MoC. Τέλος, διάφοροι ειδικοί δράστες δρομολόγησης μπορούν να χρησιμοποιηθούν για τη διάταξη των εργασιών πέρα από την απλή ακολουθιακή παράθεση βημάτων επεξεργασίας, όπως για να ορίσουν τη διακλάδωση και τη συγχώνευση της ροής δεδομένων, τη δρομολόγηση δεδομένων βάσει συνθήκης, βρόχους for, κλπ..

3.4 Τεχνολογίες για την προστασία της Ιδιωτικότητας

Στις ενότητες που ακολουθούν παρουσιάζονται συνοπτικά οι πιο σημαντικές τεχνολογίες που έχουν προταθεί ή εφαρμοστεί για την προστασία της ιδιωτικότητας (Privacy Enhancing Technologies – PETs), καθώς επίσης και οι κυριότεροι μηχανισμοί με τη βοήθεια των οποίων οι τεχνολογίες αυτές ενσωματώνονται μέχρι σήμερα στα συστήματα λογισμικού. Τέλος, γίνεται ιδιαίτερη αναφορά στους υπάρχοντες τρόπους διευθέτησης του ζητήματος της ιδιωτικότητας με εφαρμογή των PETs στα σύγχρονα κατανεμημένα περιβάλλοντα, στα οποία εξάλλου αφορά το αντικείμενο της διατριβής.

3.4.1 Συστήματα Κρυπτογραφίας, Ανωνυμίας και Ψευδωνυμίας

Ένα σημαντικό κομμάτι των τεχνολογιών για την προστασία της ιδιωτικότητας προέρχεται από την περιοχή της ασφάλειας, καθώς, όπως εξάλλου αναφέρθηκε στο Κεφάλαιο 2, η ασφάλεια των δεδομένων αποτελεί ρητή απαίτηση της νομοθεσίας και για την περίπτωση της ιδιωτικότητας (data security). Κοινό χαρακτηριστικό των αντίστοιχων μηχανισμών, ωστόσο, αποτελεί το γεγονός ότι είναι αναστρέψιμοι ή/και παρακάμψιμοι, με αποτέλεσμα από μόνοι τους να μην επαρκούν για την αποτελεσματική προστασία της· παρόλα αυτά, μπορούν να χρησιμοποιηθούν συμπληρωματικά και σε συνδυασμό με άλλες μεθόδους (βλ. Ενότητες 3.4.2, 3.4.3).

Όταν πραγματοποιείται μετάδοση προσωπικών δεδομένων, αυτά θα πρέπει να χα-

ρακτηρίζονται από επαρκή βαθμό προστασίας από τις εξωτερικές οντότητες οι οποίες ενδέχεται να επιθυμούν να υποκλέψουν τη σχετική πληροφορία και να την επιβουλευτούν. Η αποτροπή τρίτων οντοτήτων από το να υποκλέψουν προσωπικά δεδομένα κατά τη φάση της μετάδοσής τους καθίσταται δυνατή μέσα από τη χρήση *κρυπτογραφικών μεθόδων* [178] [179]. Επιπλέον, και η αποθήκευσή των δεδομένων πρέπει να χαρακτηρίζεται από υψηλό βαθμό ασφάλειας, ούτως ώστε να είναι δυνατό μόνο σε εξουσιοδοτημένες οντότητες να τα προσπελάσουν. Στην πράξη, αυτό μεταφράζεται σε δύο απαιτήσεις. Από τη μία, τα δεδομένα πρέπει να αποθηκεύονται κρυπτογραφημένα ούτως ώστε ακόμα και αν κάποιος αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα σχετικά αρχεία να μην είναι σε θέση να διαβάσει το περιεχόμενο. Από την άλλη, απαιτούνται ισχυροί μηχανισμοί ταυτοποίησης και εξουσιοδότησης χρηστών, ούτως ώστε να διασφαλίζεται ότι εξουσιοδοτημένες οντότητες και μόνο είναι δυνατό να αποκτήσουν πρόσβαση στα αποθηκευμένα δεδομένα. Συνεπώς, η χρήση κρυπτογραφικών μεθόδων βρίσκει και εδώ εφαρμογή. Τα συστήματα κρυπτογραφίας διακρίνονται σε δύο κατηγορίες, σε εκείνα που βασίζονται σε αλγόριθμους *Συμμετρικής Κρυπτογραφίας* [180][181][182][183][184][185][186][187] και σε εκείνα που κάνουν χρήση *Κρυπτογραφίας Δημόσιου Κλειδιού ή Ασύμμετρης Κρυπτογραφίας* [188][189][190] [191][192]. Αναφορικά με την εφαρμογή τους στην προστασία των δεδομένων, ο συνδυασμός των δύο ιδεών διασφαλίζει τόσο τη μυστικότητα, όσο και την αυθεντικότητα και ακεραιότητα της πληροφορίας μέσω της χρήσης των ψηφιακών υπογραφών. Εξάλλου, τα κρυπτογραφικά συστήματα δημοσίου κλειδιού βρίσκουν εφαρμογή σε διάφορα πρωτόκολλα ασφάλειας στο Διαδίκτυο. Ιδιαίτερα σημαντικά μεταξύ αυτών είναι το πρωτόκολλο Secure Sockets Layer (SSL) [193] καθώς και ο διάδοχός του, το πρωτόκολλο Transport Layer Security (TLS) [194][195]. Τα πρωτόκολλα SSL και TLS χρησιμοποιούνται συνήθως για τη διασφάλιση επικοινωνιακών καναλιών που ακολουθούν το πρωτόκολλο Hypertext Transfer Protocol (HTTP) [196], αλλά μπορούν να χρησιμοποιηθούν σε συνδυασμό και με άλλα πρωτόκολλα, όπως το Simple Mail Transfer Protocol (SMTP) [197] για τη διασφάλιση των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Επιπλέον, κρυπτογραφικοί μηχανισμοί χρησιμοποιούνται και για την προστασία σε περιβάλλοντα Υπηρεσιών Ιστού με βάση συγκεκριμένα πρότυπα (βλ. Ενότητα 3.1.1)

Μια ακόμα υποσχόμενη προσέγγιση συνιστά η χρήση *ανωνυμίας (anonymity)* ή *ψευδωνυμίας (pseudonymity)*, η οποία συχνά αποτελεί απαίτηση της νομοθεσίας [17] και επιτυγχάνει την ελαχιστοποίηση των δεδομένων (data minimisation) και την προστασία της ταυτότητας του χρήστη, στοχεύοντας στη διασφάλιση της ιδιωτικότητας σε διαφορετικά επίπεδα. Η ανωνυμία μπορεί να οριστεί σαν *"η κατάσταση κατά την οποία κάποιο υποκείμενο δεν είναι αναγνωρίσιμο μεταξύ των μελών ενός συνόλου υποκειμένων, του συνόλου ανωνυμίας"* [198]. Από την άλλη, η χρήση ψευδωνύμων επιτρέπει την προσωποποίηση των παρεχομένων υπηρεσιών χωρίς να κάνουν χρήση της πραγματικής ταυτότητας κάποιου χρήστη. Στο πεδίο των Επικοινωνιών, η προστασία της ανωνυμίας ανάγεται στην απόκρυψη των δικτυακών διευθύνσεων των εμπλεκόμενων χρηστών, κάτι που εφαρμόζεται σχετικά εύκολα και μπορεί να ενσωματωθεί σε οποιαδήποτε τεχνική λύση προστασίας προσωπι-

κών δεδομένων, καθώς υλοποιείται χωριστά σε σχέση από την εκάστοτε υποδομή ιδιωτικότητας. Θα πρέπει όμως να σημειωθεί, ότι η ανωνυμία στο επίπεδο δικτύου δεν μπορεί να αποτρέψει την αναγνώριση κάποιου χρήστη μέσω των προσωπικών του πληροφοριών που είναι αποθηκευμένες ή μεταδίδονται στο πλαίσιο της παροχής κάποιας υπηρεσίας. Τα τελευταία χρόνια έχουν προταθεί διάφορες τεχνολογίες ανωνυμίας, όπως Onion Routing [199][200], Crowds [201], FREENET [202][202], καθώς και τα συστήματα MIX [203],[204], τα οποία επηρέασαν σημαντικά την έρευνα στο συγκεκριμένο πεδίο.

3.4.2 Συστήματα Διαχείρισης Ταυτοτήτων

Η διαχείριση ταυτοτήτων αφορά την αναγνώριση ατόμων και τον μέσω αυτής έλεγχο της πρόσβασης σε ένα σύστημα. Σε τεχνολογικό επίπεδο, υφίστανται διάφορες προσεγγίσεις αναφορικά με τους μηχανισμούς διαχείρισης ηλεκτρονικών ταυτοτήτων [205], που ποικίλλουν αναφορικά με το εύρος και το πεδίο εφαρμογής τους, καθώς και την πολυπλοκότητα. Το πλέον καθιερωμένο πρότυπο είναι εκείνο της *Ομοσπονδιακής Διαχείρισης Ταυτοτήτων (Federated Identity Management)* [205][206][207]. Η ομοσπονδιακή διαχείριση ταυτοτήτων περιλαμβάνει μηχανισμούς που επιτρέπουν στα υπολογιστικά συστήματα να διανέμουν με δυναμικό τρόπο πληροφορίες ταυτότητας σε πολλαπλούς οργανισμούς και να μεταβιβάζουν την εκτέλεση σχετικών λειτουργιών επεξεργασίας, προσδίδοντας μεγάλη ευελιξία στις λειτουργίες. Ένα από τα πλέον αντιπροσωπευτικά πρότυπα ομοσπονδιακής διαχείρισης ταυτοτήτων αποτελούν οι προδιαγραφές του οργανισμού Liberty Alliance [20]. Το 2002, ο οργανισμός παρουσίασε την πρώτη οικογένεια προτύπων για την ομοσπονδιακή διαχείριση ταυτοτήτων (Identity Federation Framework – ID-FF) το οποίο στη συνέχεια εξελίχθηκε για να φτάσει στη σημερινή του έκδοση ID-FF 1.2 [208]. Η κεντρική ιδέα του προτύπου είναι η διασύνδεση σε μία ομοσπονδιακή ταυτότητα των προσωπικών πληροφοριών που αφορούν διαφορετικούς (και συμβατούς με το πρότυπο) παρόχους υπηρεσιών. Όπως γενικά τα συστήματα ομοσπονδιακής διαχείρισης ταυτοτήτων, το εν λόγω πρότυπο ορίζει διακριτά τους ρόλους του παρόχου ταυτότητας (identity provider) και παρόχου υπηρεσίας. Επιπλέον, ο οργανισμός έχει παρουσιάσει και άλλα συναφή πρότυπα, όπως είναι το Πλαίσιο Ταυτότητας Υπηρεσιών Ιστού (Identity Web Services Framework – ID-WSF) [209] και οι Προδιαγραφές Διεπαφής Υπηρεσίας Ταυτότητας (Identity Service Interface Specifications – ID-SIS) [210]. Εν τω μεταξύ, ο οργανισμός OASIS είχε προτυποποιήσει την πρώτη έκδοση της *Γλώσσας Σήμανσης Βεβαιώσεων Ασφάλειας (Security Assertion Markup Language – SAML)* [211]. Η σύγκλιση μεταξύ της SAML και του προτύπου Liberty Alliance αποτέλεσε τη βάση για την προδιαγραφή της SAML 2.0 [212], η οποία αποτελεί το κυρίαρχο πρότυπο για τη διαχείριση ομοσπονδιακών ταυτοτήτων.

Τεχνολογίες για την ομοσπονδιακή διαχείριση ταυτοτήτων υπάρχουν πολλές· μερικές από αυτές είναι το InfoCard [213] της εταιρείας Microsoft, καθώς και το Shibboleth [214], το οποίο αποτελεί μια λύση λογισμικού ανοικτού κώδικα που βασίζεται στη SAML 2.0. Η

[20]http://www.projectliberty.org/

ανερχόμενη όμως τεχνολογία είναι το OpenID [215][216], το οποίο συνιστά ένα ελεύθερο, αποκεντρωμένο και ανοικτό πρωτόκολλο. Το OpenID αίρει την ανάγκη για πολλαπλές ταυτότητες, καθώς βασίζεται στη λογική της σύνδεσης σε πολλές υπηρεσίες χρησιμοποιώντας μία και μοναδική ηλεκτρονική ταυτότητα· παρά το γεγονός ότι η δεύτερη έκδοσή του υποστηρίζει τη χρήση ψευδωνύμων, κρίνεται επισφαλές για κάποιες εφαρμογές. Ωστόσο, κάποιοι ερευνητές το θεωρούν ως ιδανική λύση για ανοικτές πλατφόρμες ηλεκτρονικής διακυβέρνησης [217].

Οι τεχνολογίες προστασίας ιδιωτικότητας που σχετίζονται με τη διαχείριση ταυτοτήτων στοχεύουν στην επαλήθευση της ταυτότητας των χρηστών με τον ελάχιστο όμως βαθμό αποκάλυψης της ταυτότητας καθεαυτής και στην προστασία ενάντια στην κλοπή ταυτοτήτων. Στα πλαίσια ενός οργανισμού, αυτό μεταφράζεται στην αποκάλυψη μόνο εκείνων των προσωπικών δεδομένων που είναι απαραίτητα για κάποιο επιχειρησιακό σκοπό, έτσι ώστε διαφορετικά τρίτα μέρη να έχουν πρόσβαση σε διαφορετική (μερική) πληροφορία για τον εκάστοτε χρήστη, διαδικασία που οδηγείται από τις επιλογές και τη συγκατάθεση του τελευταίου. Από αυτή τη σκοπιά, παρόλο που ένας από τους στόχους των προτύπων Liberty Alliance είναι η προστασία της ιδιωτικότητας των πληροφοριών ταυτότητας, πολλοί ερευνητές επεσήμαναν διαφαινόμενα προβλήματα και πρότειναν τροποποιήσεις, π.χ., [218][219][220]. Διάφορες προτάσεις στην κατεύθυνση της προστασίας και διαχείρισης ταυτοτήτων έχουν γενικά εμφανιστεί και αφορούν αρχιτεκτονικές υπηρεσιών σε κινητά περιβάλλοντα [221], διαδικασίες διαπραγμάτευσης εμπιστοσύνης [222], ανωνυμία δεδομένων θέσης των χρηστών [223][224] [225], κ.α..

Μια ενδιαφέρουσα προσέγγιση αντικατοπτρίζεται από ερευνητικές προτάσεις που συνιστούν τη χρήση κρυπτογραφικών μηχανισμών προκειμένου να καταστήσουν δυνατή την πιστοποίηση ταυτότητας με ανώνυμο τρόπο. Στο πλαίσιο αυτό, η ερευνητική τάση είναι η ενσωμάτωση στις τεχνολογίες διαχείρισης ταυτοτήτων των κατάλληλων λειτουργικοτήτων για διαχείριση πολλαπλών ταυτοτήτων και ψευδωνύμων πιστοποιητικών ταυτότητας. Μια τέτοια προσέγγιση είναι η ολοκλήρωση του συστήματος Idemix [226][227] της IBM στην ανοικτού κώδικα τεχνολογία για διαχείριση ταυτοτήτων Higgins [228], ερευνητική εργασία που έχει εν μέρει πραγματοποιηθεί στο πλαίσιο των χρηματοδοτούμενων από την Ευρωπαϊκή Ένωση προγραμμάτων PRIME [229] και PrimeLife [230]. Τέτοια συστήματα ανώνυμων διαπιστευτηρίων, όπως και το SPARTA [231], στηριζόμενα σε σχήματα ψηφιακής υπογραφής και κρυπτογραφικές αποδείξεις μηδενικής γνώσης (cryptographic zero-knowledge proofs) [232], μπορούν να επεκτείνουν τη λειτουργικότητα των συστημάτων ομοσπονδιακής διαχείρισης ταυτότητας, ούτως ώστε να καλύπτει ισχυρότερη προστασία της ιδιωτικότητας, έλεγχο του χρήστη και πολλαπλή χρήση διαπιστευτηρίων. Περαιτέρω, η ομάδα εργασίας Public-Key Infrastructure (PKIX) της Internet Engineering Task Force (IETF)[21] έχει παρουσίασει κάποια λύση στο θέμα της διαχείρισης διαπιστευτηρίων ιδιοτήτων (attributes) συνδεδεμένων με πιστοποιητικά ταυτοποίησης, η οποία ωστόσο είναι μάλ-

[21]http://www.ietf.org/html.charters/pkix-charter.html

λον πολύπλοκη από τη άποψη της εξάρτησης από πολλαπλά έμπιστα τρίτα μέρη (trusted third parties), χωρίς να αντιμετωπίζει πλήρως τα ζητήματα ιδιωτικότητας και ανωνυμίας. Άλλα σχήματα ανώνυμης πιστοποίησης αναφέρονται στα [233][234].

Τέλος, σχετική είναι και η περιοχή της διαχείρισης εμπιστοσύνης (trust management), όπου η παρεχόμενη πληροφορία εξαρτάται από την εκτίμηση της αξιοπιστίας του παραλήπτη, κάτι που στην περίπτωση των προσανατολισμένων σε Υπηρεσίες αρχιτεκτονικών ρυθμίζεται ήδη από συγκεκριμένα πρότυπα (βλ. Ενότητα 3.1.1). Τεχνολογίες προστασίας της ιδιωτικότητας που μπορούν να χρησιμοποιηθούν για το σκοπό αυτό περιλαμβάνουν τεχνικές διαχείριση φήμης [235][236][237], ελέγχου ακεραιότητας κάποιας απομακρυσμένης έμπιστης πλατφόρμας [238] και άλλες.

3.4.3 Συστήματα Ελέγχου Πρόσβασης

Κάθε παραβίαση της ιδιωτικότητας αφορά και περιλαμβάνει αθέμιτη πρόσβαση στα αντίστοιχα δεδομένα· για το λόγο αυτό, οι τεχνολογίες ελέγχου πρόσβασης αποτελούν μηχανισμούς ιδιαίτερης σημασίας για την προστασία των προσωπικών δεδομένων. Ωστόσο, οι παραδοσιακοί μηχανισμοί ελέγχου πρόσβασης, όπως ο *Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control – DAC)*, ο *Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC)* και ο πιο σύγχρονος *Έλεγχος Πρόσβασης Βάσει Ρόλων (Role-Based Access Control – RBAC)* [239], αδυνατούν να ανταποκριθούν στο σύνολο των ειδικών απαιτήσεων που διέπουν την προστασία της ιδιωτικότητας, καλύπτοντας ένα μόνο μέρος τους. Για παράδειγμα, δε λαμβάνουν υπόψη τη θεμελιώδη για την ιδιωτικότητα παράμετρο του σκοπού για τον οποίο πραγματοποιείται η συλλογή και επεξεργασία των δεδομένων και δεν προδιαγράφουν την εκτέλεση συμπληρωματικών ενεργειών, αυτών που στη διεθνή βιβλιογραφία αναφέρονται συχνά ως υποχρεώσεις (obligations) [240], όπως είναι η ενημέρωση του υποκειμένου των δεδομένων αναφορικά με τη συλλογή ή επεξεργασία των δεδομένων του. Έτσι, τα τελευταία χρόνια έχει προκύψει μια νέα οικογένεια μηχανισμών, κυρίως σε ερευνητικό επίπεδο, οι οποίοι κάνουν πράξη αυτό που ονομάζουμε *Έλεγχο Πρόσβασης για Προστασία της Ιδιωτικότητας* [241][242]. Κάποιοι από αυτούς επεκτείνουν μάλιστα τα μοντέλα RBAC, ενσωματώνοντάς τους επιπλέον κριτήρια για την παροχή πρόσβασης.

Ιδιαίτερη κατηγορία προσεγγίσεων ελέγχου πρόσβασης και απαρχή των αντίστοιχων τεχνολογιών αποτελεί η διαχείριση ιδιωτικότητας σε αποθετήρια δεδομένων (data repositories), η οποία αποσκοπεί στο να διασφαλίσει ότι τα αποθηκευμένα δεδομένα προσπελάζονται κατά τρόπο που να διασφαλίζεται η ιδιωτικότητα, έτσι ώστε να μη γίνεται συλλογή στοιχείων επικοινωνίας, μακροπρόθεσμων ατομικών χαρακτηριστικών και λοιπών ευαίσθητων προσωπικών στοιχείων. Στην κατεύθυνση αυτή έχουν προταθεί μηχανισμοί και λύσεις για την κρυπτογράφηση εμπιστευτικών δεδομένων κατά την αποθήκευσή τους σε αποθετήρια, για παράδειγμα με τη χρήση *Ημιδιαφανών Βάσεων Δεδομένων (Translucent Databases)* [243]. Οι περισσότερες τέτοιες λύσεις επικεντρώνονται στην εμπι-

στευτικότητα και τον έλεγχο πρόσβασης και έχουν μικρή ευελιξία ως προς την παροχή μηχανισμών βασισμένων σε πολιτικές σε ότι αφορά ζητήματα πέραν της αυθεντικοποίησης και εξουσιοδότησης. Στα [244][245] περιγράφονται μηχανισμοί κρυπτογράφησης βασισμένοι σε πολιτικές ελέγχου πρόσβασης για αρχεία XML. Επιπρόσθετα, αν και πλέον έχει αποσυρθεί από την παραγωγή, ο Tivoli Privacy Manager της IBM[22] παρείχε μηχανισμούς για τον ορισμό πολιτικών ιδιωτικότητας σε υψηλό βαθμό λεπτομέρειας και το συσχετισμό τους με δεδομένα. Μια εναλλακτική πρόταση βασίζεται σε ένα προσαρμόσιμο σύστημα διαχείρισης ιδιωτικότητας, όπου τα δεδομένα αντλούνται από συγκεκριμένα αποθετήρια και μέρη αυτών των δεδομένων είναι κρυπτογραφημένα και συσχετισμένα με πολιτικές ιδιωτικότητας [246].

Σε αυτό το πλαίσιο μια από τις πρώτες και πλέον επιδραστικές προσεγγίσεις για την ενσωμάτωση των βασικών αρχών περί προστασίας της ιδιωτικότητας στις διαδικασίες ελέγχου πρόσβασης σε δεδομένα αποτελούν οι *Ιπποκρατικές Βάσεις Δεδομένων (Hippocratic Databases)* [247], οι οποίες οφείλουν το όνομά τους στο ακόλουθο απόσπασμα από τον Όρκο του Ιπποκράτη: *"Και ό,τι δω ή ακούσω κατά την άσκηση του επαγγέλματός μου, ή κι εκτός, για τη ζωή των ανθρώπων, που δεν πρέπει ποτέ να κοινοποιηθεί, [ορκίζομαι] να σιωπήσω και να το τηρήσω μυστικό"*. Η ιδέα των Ιπποκρατικών Βάσεων Δεδομένων παρουσιάστηκε το 2002 από ομάδα ερευνητών της εταιρείας IBM, η οποία θέλησε να καταστήσει τα Σχεσιακά Συστήματα Βάσεων Δεδομένων (Relational Database Systems) συμβατά με τις βασικές αρχές προστασίας της ιδιωτικότητας, όπως εκείνες περιγράφονταν στις *"Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων"* [31], οι οποίες διατυπώθηκαν στις αρχές της δεκαετίας του 1980 από τον ΟΟΣΑ (βλ. Κεφάλαιο 2). Η βασικότερη συνεισφορά των Ιπποκρατικών Βάσεων Δεδομένων ήταν ότι εισήγαγαν την έννοια του σκοπού της συλλογής και επεξεργασίας, ενώ αποτέλεσαν το αντικείμενο διαφόρων επεκτάσεων (π.χ.,[248][249][250]).

Οι Ιπποκρατικές Βάσεις Δεδομένων αποτέλεσαν το πρώτο βήμα για την προδιαγραφή συστημάτων βάσεων δεδομένων τα οποία λαμβάνουν υπόψη την προστασία της ιδιωτικότητας και ενέπνευσαν αρκετές αντίστοιχες ερευνητικές προσπάθειες [251]. Μια από τις πιο σημαντικές και αντιπροσωπευτικές προσεγγίσεις αποτελεί το μοντέλο *Ελέγχου Πρόσβασης Βάσει Σκοπού (Purpose Based Access Control – PBAC)*, το οποίο πρωτοπαρουσιάστηκε το 2004 από ομάδα ερευνητών του Πανεπιστημίου Perdue των ΗΠΑ [252][253], ενώ στη συνέχεια εξελίχθηκε σε μεγάλο βαθμό [254]. Η βασική συνεισφορά του μοντέλου αυτού είναι ο αναλυτικός ορισμός της έννοιας του σκοπού. Καθώς η προσέγγιση στοχεύει στις βάσεις δεδομένων, βασίζεται σε ένα μηχανισμό μετασχηματισμού των τα ερωτημάτων (queries) μετά την υποβολή τους, με βάση τις παραμέτρους ιδιωτικότητας.

Η αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας μέσω ελέγχου πρόσβασης έχει αποτελέσει το αντικείμενο εκτενούς ακαδημαϊκής αλλά και βιομηχανικής έρευνας. Χαρακτηριστικά παραδείγματα αποτελούν οι προσεγγίσεις που έχουν προταθεί

[22]http://www-01.ibm.com/software/tivoli/products/privacy-mgr-e-bus/

από την IBM (π.χ., [255][256]), τη Hewlett Packard (π.χ., [240][257]) καθώς και τον OASIS, στον οποίο συμμετέχουν μερικές από τις σημαντικότερες βιομηχανίες, αλλά και πανεπιστήμια και μη κερδοσκοπικοί οργανισμοί. Ο οργανισμός OASIS προδιέγραψε και προτυποποίησε την *Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (eXtensible Access Control Markup Language – XACML)* καθώς και την αρχιτεκτονική για την εφαρμογή της [258]. Η XACML είναι μια γλώσσα γενικού σκοπού για την άσκηση ελέγχου πρόσβασης, ενώ είναι ανεξάρτητη των υποκείμενων συστημάτων. Η βασική της προδιαγραφή επεκτείνεται μέσω των λεγόμενων προφίλ (profiles) τα οποία την καθιστούν ένα πολύ δυνατό εργαλείο περιγραφής πολιτικών. Στο πλαίσιο αυτό, ορίζεται και το προφίλ πολιτικής ιδιωτικότητας (privacy policy profile) [259], το οποίο δίνει τη δυνατότητα διαχείρισης της έννοιας του σκοπού στο πλαίσιο μιας πολιτικής. Άλλη πολύ σημαντική προσέγγιση που στοχεύει στην ολοκλήρωση μεταξύ των μηχανισμών ελέγχου πρόσβασης και των πολιτικών ιδιωτικότητας επεκτείνοντας τα μοντέλα RBAC είναι και εκείνη του *RBAC για Ιδιωτικότητα (Privacy-Aware RBAC – P-RBAC)* [260].

Στον ευρωπαϊκό χώρο, ξεχωρίζει η ερευνητική δραστηριότητα του Πολυτεχνείου του Μιλάνο, το οποίο, μέσα από τη συμμετοχή του στο ερευνητικό πρόγραμμα PRIME [229] που χαρακτηρίζεται ως ορόσημο στο χώρο, ανέπτυξε ένα εξελιγμένο μοντέλο ελέγχου πρόσβασης για ιδιωτικότητα [261], καθώς και μια εκδοχή του η οποία λαμβάνει υπόψη τη θέση του χρήστη [262]. Η τελευταία εντάσσεται σε μια ερευνητική «οικογένεια» μοντέλων ελέγχου πρόσβασης, τα οποία χαρακτηρίζονται ως μοντέλα με επίγνωση πλαισίου (context-aware). Τα μοντέλα αυτά λαμβάνουν υπόψη χρονικές, χωρικές, ιστορικές και άλλες παραμέτρους για την απόδοση ή μη δικαιωμάτων πρόσβασης. Χαρακτηριστικά παραδείγματα τέτοιων μοντέλων είναι τα [263][264][265][266][267].

Τέλος, πρέπει να σημειωθεί ότι η ερευνητική ομάδα του ΕΜΠ στα πλαίσια της οποίας πραγματοποιείται η διατριβή δραστηριοποιείται στον έλεγχο πρόσβασης, έχοντας παρουσιάσει τα τελευταία χρόνια σημασιολογικά μοντέλα ελέγχου πρόσβασης τα οποία βασίζονται στη νομοθεσία περί προστασίας προσωπικών δεδομένων (π.χ., [7][268][269][270]). Ο σημασιολογικό έλεγχος πρόσβασης, ο οποίος εκμεταλλεύεται τη μεγάλη εκφραστικότητα των σημασιολογικών τεχνολογιών για την περιγραφή των υποκείμενων πολιτικών, αποτελεί μια ανερχόμενη τάση στην ερευνητική περιοχή, η οποία έχει ήδη παρουσιάσει αρκετές ενδιαφέρουσες εργασίες, όπως είναι οι [271][272][273].

3.4.4 Μηχανική Λογισμικού για Ασφάλεια και Ιδιωτικότητα

Στον τομέα της μηχανικής λογισμικού, έχουν προταθεί διάφορες προσεγγίσεις που ως στόχο τους έχουν την ασφάλεια και την προστασία της ιδιωτικότητας. Τέτοιες προσεγγίσεις αφορούν για παράδειγμα τις ενσωματωμένες λειτουργικότητες ελέγχου πρόσβασης της τεχνολογίας Enterprise JavaBeans (EJB) της Java [274], ή τη χρήση θεματοστραφούς ανάπτυξης [275] για την ενσωμάτωση χαρακτηριστικών προστασίας της ιδιωτικότητας είτε

σε εφαρμογές κατά τα τελευταία στάδια της ανάπτυξής τους, είτε σε υφιστάμενες εφαρμογές. Μια τέτοια προσέγγιση αποτυπώνεται στην προδιαγραφή του *Εργαλείου Έγχυσης Ιδιωτικότητας (Privacy Injector)* [276], που περιλαμβάνει διαδικασίες για τη δημιουργία, ενημέρωση, χρήση και διατήρηση μεταδεδομένων ιδιωτικότητας, καθώς και για την εφαρμογή τους σε συνδυασμό με την υποκείμενη πολιτική ιδιωτικότητας. Άλλες προσεγγίσεις αφορούν τον ορισμό ειδικών γλωσσών προδιαγραφής, οι οποίες χρησιμοποιούνται για την επισημείωση αφαιρετικών προδιαγραφών με χαρακτηριστικά ασφάλειας και ιδιωτικότητας. Τέτοιες είναι οι *UMLsec* [277] και *SecureUML* [278], οι οποίες έχουν ως βάση τους τη γλώσσα UML [279] και οι οποίες μπορούν να συνδυαστούν με διαφορετικές σχεδιαστικές γλώσσες σε επίπεδο μοντελοποίησης και να μετασχηματιστούν στη συνέχεια σε συγκεκριμένες υλοποιήσεις. Ιδιαίτερο ενδιαφέρον στην περιοχή παρουσιάζει και η έννοια της *Μοντελοκεντρικής Ασφάλειας (Model Driven Security – MDS)* [280], η οποία, έχοντας ως βάση τη μοντελοκεντρική ανάπτυξη [281][282], εστιάζει σε απαιτήσεις σχετικά με τον έλεγχο πρόσβασης και βασίζεται στο συνδυασμό της SecureUML με άλλες γλώσσες μοντελοποίησης, προκειμένου να επιτύχει μετασχηματισμό σε συγκεκριμένες υλοποιήσεις. Για παράδειγμα, στην εργασία [283] παρουσιάζεται η συνδυαστική χρήση της SecureUML με την ComponentUML, μια γλώσσα για την περιγραφή συστημάτων βασισμένων σε συστατικά (component-based systems).

Σημαντική ερευνητική δουλειά έχει πραγματοποιηθεί και στον τομέα της προδιαγραφής και ενσωμάτωσης των απαιτήσεων για ασφάλεια και ιδιωτικότητα στα υποκείμενα μοντέλα συστημάτων λογισμικού. Για το σκοπό αυτό, έχουν προταθεί διάφορες προσεγγίσεις, όπως οι μέθοδοι i* [284], NFR [285], Tropos [286], KAOS [287], GBRAM [288], Mofett-Nuseibeh [289][290], Bellotti-Sellen [291] και STRAP [292]. Εξέχουσα θέση μεταξύ των προσεγγίσεων αυτών καταλαμβάνει η μέθοδος PriS [293][294], η οποία έχει αναπτυχθεί από την ερευνητική ομάδα του Πανεπιστημίου Αιγαίου. Η μέθοδος PriS θεωρεί τις απαιτήσεις για ιδιωτικότητα ως στόχους οι οποίοι πρέπει να ικανοποιούνται και υιοθετεί τη χρήση υποδειγμάτων διεργασιών, ούτως ώστε να περιγράψει το αποτέλεσμα των απαιτήσεων στις επιχειρησιακές διεργασίες και να διευκολύνει τον ορισμό της αρχιτεκτονικής των συστημάτων για την υποστήριξη των διεργασιών.

3.4.5 Η Ιδιωτικότητα στα Κατανεμημένα Περιβάλλοντα

Κεντρική θέση στα σημερινά κατανεμημένα περιβάλλοντα κατέχει η έννοια της *συνεργασίας* (collaboration), καθώς η τελευταία αφενός ενισχύεται από και αφετέρου αποτελεί προϋπόθεση για την αξιοποίηση των δυνατοτήτων τεχνολογιών όπως οι αρχιτεκτονικές SOA, με απώτερο σκοπό την παροχή ακόμα πιο εξελιγμένων υπηρεσιών. Συγχρόνως όμως είναι και ο παράγοντας εκείνος ο οποίος περισσότερο δυσχεραίνει την ευθεία και αποτελεσματική εφαρμογή, μεταξύ άλλων, των ήδη υπαρχόντων λύσεων στο θέμα της προστασίας της ιδιωτικότητας που έχουν προηγουμένως αναφερθεί στο παρόν κεφάλαιο. Πράγματι, σε τέτοια συστήματα η εξισορρόπηση των αντικρουόμενων στόχων της συνερ-

γασίας αφενός και παραγόντων όπως η ασφάλεια και η προστασία προσωπικών δεδομένων αφετέρου συνιστά ένα δύσκολο, πολυδιάστατο πρόβλημα: από τη μια, η δημιουργία χρήσιμων συσχετισμών μεταξύ ανθρώπων, εργαλείων και πληροφοριών αποτελεί προαπαιτούμενο, ενώ από την άλλη απαιτείται συγχρόνως η διασφάλιση σε ακόμα μεγαλύτερο βαθμό χαρακτηριστικών όπως η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα των ίδιων αυτών στοιχείων. Στη συνέχεια παρουσιάζονται επιγραμματικά κάποιες αντιπροσωπευτικές προσεγγίσεις σχετικά με την αντιμετώπιση κάποιων καίριων πλευρών που άπτονται κυρίως ζητημάτων ελέγχου πρόσβασης σε κατανεμημένες συνεργασίες και μερικές εκ των οποίων έχουν προαναφερθεί, όπως η εμπιστοσύνη, η διαπραγμάτευση, η ενοποίηση πολιτικών, η εκχώρηση ρόλων και δικαιωμάτων, η εμπιστευτικότητα, η ασφαλής από κοινού χρήση πληροφοριών, ανάλογοι τρόποι διαχείρισης ροών υπηρεσιών κ.ά.

Στα ανοιχτά κατανεμημένα περιβάλλοντα, όπου οι κάτοχοι πόρων και οι αιτούντες τους πόρους αυτούς ανήκουν σε διαφορετικούς ως προς την ασφάλεια τομείς (domains), ελεγχόμενους από διαφορετικές αρχές και διαφορετικά πλαίσια ελέγχου πρόσβασης άγνωστα μεταξύ τους, μια απλή προσέγγιση είναι η επιβολή ελέγχου πρόσβασης βασισμένου σε συγκεκριμένα χαρακτηριστικά των αιτούντων, των λεγόμενων *ιδιοτήτων (attributes)*, κατά βάση εκπροσωπούμενα από ψηφιακά διαπιστευτήρια (credentials) [295][296][297]. Η διαλειτουργικότητα μπορεί να ενισχυθεί περαιτέρω με τη σημασιολογική συσχέτιση των ιδιοτήτων ανάμεσα σε διαφορετικούς τομείς, για παράδειγμα με τη χρήση οντολογιών [298].

Η *εμπιστοσύνη (trust)* αποτελεί απαίτηση–κλειδί στο πλαίσιο της συνεργατικής εργασίας, όπου κάθε οντότητα έχει μικρή ή καθόλου γνώση σχετικά με τις υπόλοιπες. Στη βιβλιογραφία η έννοια της εμπιστοσύνης αναλύεται ως μια σχέση εμπιστοσύνης (”ο Α εμπιστεύεται τον Β για τη διενέργεια της πράξης z”) και ένα σύνολο πεποιθήσεων συσχετισμένων με μια τέτοια σχέση (π.χ., η πεποίθηση του Α για την αξιοπιστία του Β, κλπ.). Η εμπιστοσύνη αντιμετωπίζεται κάποιες φορές απλά ως μια επιπλέον περίπτωση ιδιότητας [299][300][301][302], ενώ σε άλλες προσεγγίσεις υπολογίζεται στη βάση άλλων ιδιοτήτων των αιτούντων και/ή άλλων παραγόντων [303][304][305][306][307]. Σκοπός της διαχείρισης εμπιστοσύνης είναι όχι μόνο ο έλεγχος πρόσβασης αλλά σε κάποιες περιπτώσεις και ο περιορισμός της αποκάλυψης πολιτικών.

Η *διαχείριση ρόλων (role management)*, από την άλλη, επιχειρεί να αντιμετωπίσει το ζήτημα της ετερογένειας των ρόλων μεταξύ διαφορετικών τομέων που εφαρμόζουν έλεγχο πρόσβασης με βάση το ρόλο (π.χ., RBAC) και συνιστά προαπαιτούμενο για την ενοποίηση των πολιτικών μεταξύ τέτοιων επικρατειών. Κάποιες προσεγγίσεις, όπως οι [308][306][309], ορίζουν διατομεακές αντιστοιχίσεις ρόλων βασισμένες στις απαιτήσεις διαλειτουργικότητας της εκάστοτε συνεργασίας. Άλλες προσδίδουν ρόλους στους αιτούντες με βάση τα διαπιστευτήριά τους [301][302][310][311][312], ασκώντας έτσι κατά κάποιο τρόπο ένα συνδυασμό ελέγχου πρόσβασης με βάση το ρόλο (role-based) και ελέγχου πρόσβασης με βάση τις ιδιότητες (attribute-based).

Πρωταρχική απαίτηση της συνεργασίας σε ένα πολλαπλό (multi-domain) περιβάλ-

λον είναι η ενοποίηση του συνόλου των τοπικών πολιτικών με σκοπό τη σύνθεση μιας *καθολικής πολιτικής ελέγχου πρόσβασης* για τον έλεγχο της πληροφορίας και της κοινής χρήσης πόρων, λαμβάνοντας υπόψη και τους πιθανούς περιορισμούς όλων των συμμετεχόντων οντοτήτων. Κατά τη διαδικασία αυτή μπορεί να προκύψουν διάφορες συγκρούσεις (conflicts). Κάποιες από αυτές επιλύονται με βάση τις σχέσεις προτεραιότητας πολιτικών, με την έννοια ότι η πιο συγκεκριμένη εξουσιοδότηση υπερισχύει μιας πιο γενικής [313], ενώ άλλες μέσω της σταδιακής απαλοιφής σχέσεων αντιστοιχίας μεταξύ ρόλων και επανελέγχου των προκυπτουσών πολιτικών ως προς τη συνέπεια (consistency) [314]. Μια πιο εξελιγμένη προσέγγιση διατυπώνει τη σύνθεση αυτή σαν ένα πρόβλημα βελτιστοποίησης, όπου στόχος είναι η μεγιστοποίηση της διαλειτουργικότητας χωρίς να προκαλείται οποιαδήποτε παραβίαση της ασφάλειας των συνεργαζόμενων τομέων, και ενόσω οι απώλειες αυτονομίας παραμένουν μέσα σε αποδεκτά όρια [308].

Οντότητες που χρησιμοποιούν διαφορετικές πολιτικές μπορούν να συνεργαστούν βασιζόμενες στην έννοια του *Εικονικού Οργανισμού (Virtual Organisation – VO)*. Ένας Εικονικός Οργανισμός είναι κάποιου είδους συνασπισμός μεταξύ διαφόρων οργανισμών και σχηματίζεται από κάποιους χρήστες, υπηρεσίες ή πόρους των συμμετεχόντων αυτών οργανισμών. Για την ασφαλή αλληλεπίδραση στα πλαίσια ενός Εικονικού Οργανισμού, κάθε οργανισμός οφείλει να ορίσει την πολιτική ελέγχου πρόσβασής του και κάθε αλληλεπίδραση πρέπει να είναι συμβατή με τις πολιτικές των οργανισμών που εμπλέκονται σε αυτή. Πολλαπλές οντότητες μπορούν έτσι να ανήκουν σε έναν Εικονικό Οργανισμό, ο οποίος λειτουργεί σύμφωνα με μια μοναδική καθολική πολιτική που πρέπει να πληροί τις παραπάνω απαιτήσεις [315][316][317][318]. Στο [319] πραγματοποιείται επεξεργασία και ανάλυση πολιτικών, προκειμένου τέτοιες καθολικές πολιτικές να μετατραπούν σε συγκεκριμένους κανόνες κατάλληλους για την άσκηση ελέγχου πρόσβασης σε καθεμιά από τις διακριτές συνιστώσες που απαρτίζουν τον Εικονικό Οργανισμό. Από μια άλλη σκοπιά, κάθε οντότητα μπορεί να δημιουργήσει τοπικά έναν Εικονικό Οργανισμό για καθένα από τα υπόλοιπα μαζί της συνεργαζόμενα μέρη, ο οποίος θα αντιπροσωπεύει τις πολιτικές που ορίζουν τις μεταξύ τους αλληλεπιδράσεις [320].

Η *διαπραγμάτευση (negotiation)* συνιστά ένα μηχανισμό μέσω του οποίου δύο οντότητες που επιθυμούν να συνεργαστούν ανταλλάσσουν πληροφορίες με σκοπό να φτάσουν σε μια κοινή συμφωνία. Η διαπραγμάτευση μπορεί να χρησιμοποιηθεί για ποικίλους σκοπούς: την εδραίωση εμπιστοσύνης μεταξύ συνεργαζόμενων μερών (διαπραγμάτευση ιδιοτήτων, [303][307][304][321][305]), τη διαλειτουργικότητα (διαπραγμάτευση παραμέτρων, [297]), την ενοποίηση πολιτικών (διαπραγμάτευση πολιτικών, [318][322]).

Η *εμπιστευτικότητα (confidentiality)* είναι ένα ακόμα σημαντικό ζήτημα στις συνεργασίες, υπό την έννοια ότι τα συνεργαζόμενα μέρη μπορεί συχνά να είναι απρόθυμα να μοιραστούν συγκεκριμένες πληροφορίες. Αρκετές λύσεις επικεντρώνουν στην προστασία των διαπιστευτηρίων, με κάποιες από αυτές να προέρχονται από την περιοχή της διαπραγμάτευσης εμπιστοσύνης [323][324][304] [305][321]. Από την άλλη, μια σειρά προσεγγίσεων

στοχεύουν στην προστασία των πληροφοριών που αφορούν σε εσωτερικές πολιτικές, όπως η [303] που βασίζεται στην εμπιστοσύνη ή άλλες που χρησιμοποιούν μεθόδους αποσύνθεσης/ανάλυσης πολιτικών [325][326][323]. Τέλος, το σύστημα κρυφών διαπιστευτηρίων που συναντάται στα [327][328][329] προστατεύει τόσο ευαίσθητα διαπιστευτήρια όσο και ευαίσθητες πολιτικές: αφενός ο πάροχος δεν μαθαίνει τίποτα σχετικά με τα πιστοποιητικά του εκάστοτε αιτούντα, ούτε καν αν ο τελευταίος έχει αποκτήσει πρόσβαση, και αφετέρου ο αιτών δε μαθαίνει ούτε τη δομή πολιτικής του παρόχου, ούτε ποια από τα διαπιστευτήριά του τού επέτρεψαν την πρόσβαση.

Η *ασφαλής κοινή χρήση πόρων (safe resource sharing)* έχει αποτελέσει αντικείμενο μελέτης σε πολλές εργασίες, καθώς αποτελεί κρίσιμη πλευρά της όποιας συνεργασίας. Κάποιες προτεινόμενες λύσεις χρησιμοποιούν μεθόδους όπως η επιλεκτική κρυπτογράφηση και η κατάτμηση των δεδομένων [330][331][332]. Άλλες χρησιμοποιούν κανόνες βασισμένους σε ιδιότητες για τον έλεγχο της πρόσβασης σε πόρους που βρίσκονται σε κατανεμημένα συστήματα μεγάλης κλίμακας [333]. Μια εναλλακτική προσέγγιση προτείνει την επισύναψη ιδιοτήτων και πολιτικών σε αντικείμενα καθώς αυτό διανέμεται από τους παραγωγούς στους καταναλωτές σε ένα σύστημα [334], ακολουθώντας το υπόδειγμα των "προσκολλημένων πολιτικών" ("sticky policies" [335]). Αντίθετα, τα μοντέλα κοινής χρήσης πληροφοριών με βάση την ομάδα (group-centric) προτείνουν την κοινή χρήση αντικειμένων με βάση τις ιδιότητες χρηστών και αντικειμένων και τους κανόνες σύμφωνα με τους οποίους δημιουργήθηκε εξαρχής η αντίστοιχη ομάδα [336][337]. Επιπλέον, ανάλογες προκλήσεις έχουν ληφθεί υπόψη και στα πλαίσια του Προβλήματος Δυναμικών Συνασπισμών (Dynamic Coalition Problem), το οποίο, όπως φανερώνει και το όνομά του, αφορά τις περιπτώσεις κατά τις οποίες ένας συνασπισμός σχηματίζεται δυναμικά, για παράδειγμα ως απόκριση σε καταστάσεις κρίσης [338].

Ενώ το πλαίσιο (context) κάθε αυτόνομης οντότητας ξεχωριστά παίζει σημαντικό ρόλο στα συστήματα συνεργασίας, η συνολική συμπεριφορά τους καθορίζεται περισσότερο από το *πλαίσιο ομάδας (group context)*, εξαιτίας των σχέσεων και αλληλεπιδράσεων μεταξύ των οντοτήτων. Στο [339] παρουσιάζεται ένα ενδιαφέρον μοντέλο ελέγχου πρόσβασης βασισμένο στην κατάσταση ομάδας (group situation), μια έννοια που περιγράφει τη συνεργασία με όρους συνολικού πλαισίου σε συνδυασμό με μια αλληλουχία από λειτουργίες που πρέπει να εκτελεστούν προκειμένου να επιτευχθεί ένα κοινός σκοπός (Σχεδιασμός Ενεργειών – Planning).

Η ανάγκη για *εκχώρηση (delegation)* εμφανίζεται συχνά στα συστήματα ελέγχου πρόσβασης. Εκχώρηση είναι η διαδικασία εκείνη μέσω της οποίας κάποιος χρήστης χωρίς συγκεκριμένα διαχειριστικά προνόμια αποκτά την ικανότητα να χορηγήσει κάποιες εξουσιοδοτήσεις. Οι περισσότερες υπάρχουσες προσεγγίσεις αποτελούν πολύπλοκες επεκτάσεις μοντέλων RBAC [340] [267][341][342], ενώ κάποιες άλλες πιο ευέλικτες, όπως η [343], δεν καταφέρνουν να αντιμετωπίσουν το θέμα στην περίπτωση πολλαπλών οργανισμών. Σε αυτή την κατεύθυνση, μια ενδιαφέρουσα λύση είναι αυτή της δυναμικής εκχώρησης

ρόλων με τη χρήση διαπιστευτηρίων [344]: η εκχώρηση ρόλων, ή ιδιοτήτων στην πιο γενική περίπτωση, αντιπροσωπεύεται από διαπιστευτήρια, τα οποία απαιτούν κατάλληλη επικύρωση προτού αποδοθεί στο χρήστη η ιδιότητα την οποία ισχυρίζεται ότι κατέχει.

Επιπρόσθετα, μια σειρά από αξιοσημείωτες προτάσεις για αποκεντρωμένο έλεγχο πρόσβασης προέρχεται από την περιοχή των *Ηλεκτρονικών Κοινωνικών Δικτύων (Online Social Networks – OSNs)*. Σχεδόν όλες οι σχετικές προσεγγίσεις εφαρμόζουν έλεγχο πρόσβασης βασισμένο σε σχέσεις (relationship-based), σύμφωνα με τον οποίο οι απαιτήσεις ελέγχου πρόσβασης εκφράζονται μέσω των μονοπατιών σχέσεων που υφίστανται στο δίκτυο, του βάθους τους και της σχετιζόμενης με αυτά εμπιστοσύνης. Οι προτεινόμενες λύσεις περιλαμβάνουν την παροχή αποδείξεων από την πλευρά του πελάτη (client-side) βασισμένη σε "πιστοποιητικά σχέσεων" [345][346][347], κρυπτογραφικούς μηχανισμούς [348][349] και τεχνολογίες σημασιολογικού ιστού [350][351]. Στα πλαίσια αυτά, ένας αριθμός προσεγγίσεων υιοθετούν κρυπτογραφικές τεχνικές [352][353][354][355] και μηχανισμούς από το πεδίο του ασφαλούς υπολογισμού (secure computation), όπως τα πρωτόκολλα ιδιωτικής τομής συνόλων [356], προκειμένου να αποφευχθεί η διαρροή ιδιωτικής πληροφορίας αναφερόμενης σε σχέσεις και/ή στη σχετική εμπιστοσύνη και στις συναγόμενες πολιτικές.

Τέλος, καθώς οι ροές εργασιών αποτελούν την κύρια τεχνολογία υλοποίησης των αρχιτεκτονικών τύπου SOA και της αρχής της συνεργασίας μεταξύ ανθρώπων, υπηρεσιών αλλά και οργανισμών, πλήθος ανάλογων προσεγγίσεων με αυτές ως επίκεντρο έχουν εμφανιστεί στη βιβλιογραφία. Οι περισσότερες στοχεύουν στο να διασφαλίσουν ότι απαιτήσεις σε ασφάλεια και άλλων ειδών περιορισμοί που σχετίζονται με τον έλεγχο πρόσβασης τηρούνται κατά την εκτέλεση ροών εργασιών, ανάλογα με τις ειδικές ανάγκες που τέτοια περιβάλλοντα επιβάλλουν και ιδιαίτερα σε ό,τι αναφορά τον επιχειρησιακό τομέα (βλ. Ενότητα 3.1.3). Για παράδειγμα οι [310][357][358] αναδεικνύουν σχετικές απαιτήσεις και προτείνουν τρόπους ενοποίησης τεχνολογιών ελέγχου πρόσβασης με συστήματα διαχείρισης ροών εργασιών, ενώ τα [359][360] εισάγουν επεκτάσεις σε ένα ώριμο μοντέλο ελέγχου πρόσβασης, προκειμένου το τελευταίο να πραγματοποιεί έλεγχο πρόσβασης και ροής σε ροές εργασιών που αφορούν είτε έναν είτε περισσότερους οργανισμούς. Στα [361][362] προτείνεται η προδιαγραφή κανόνων συμβατότητας ανεξάρτητα από τα μοντέλα ροών εργασιών, ώστε να εφαρμοστούν κατόπιν κατά την εκτέλεσή τους. Οι [171][363] επιχειρούν τη φορμαλιστική μοντελοποίηση περιορισμών εξουσιοδότησης σαν μέρος της προδιαγραφής του μοντέλου μιας ροής εργασιών, ενώ προσεγγίσεις όπως οι [364][365][366][367][368][369][370] [371][372][373][374][375] προχωρούν ένα βήμα πιο πέρα μετατρέποντας με μοντελοκεντρικό τρόπο στόχους σχετικούς με ασφάλεια, που έχουν προηγουμένως μοντελοποιηθεί μέσω της επισημείωσης μοντέλων διαδικασιών, σε συγκεκριμένες υλοποιήσεις ασφάλειας, με άλλα λόγια στις αντίστοιχες πολιτικές ασφάλειας και ελέγχου πρόσβασης. Οι παραπάνω προτάσεις, ωστόσο, μολονότι σημαντικές, έχουν το μειονέκτημα ότι είτε τελικά εφαρμόζουν τις όποιες πολιτικές μόνο κατά τη φάση της εκτέλεσης και όχι κατά τη διάρκεια του σχεδιασμού μιας ροής εργασιών, είτε οι πολιτικές αυτές ορίζονται μεν ως μέρος του σχεδιασμού, δεν προκύπτουν ωστόσο αυτόματα από

κάποια φορμαλιστικά ορισμένη γνωσιακή βάση.

Από μια άλλη σκοπιά, ο έλεγχος και η επαλήθευση των ροών εργασιών καθεαυτών ως προς διάφορες επιθυμητές ιδιότητες έχει μελετηθεί αρκετά, και πάλι κυρίως στην περιοχή της διαχείρισης επιχειρησιακών διαδικασιών. Οι πρώτες προσεγγίσεις που εμφανίστηκαν αφορούσαν τη λεγόμενη *δομική επαλήθευση (structural verification)* των ροών εργασιών, είτε ως προς τη ροή ελέγχου είτε ως προς τη ροή δεδομένων, δηλαδή τον έλεγχό τους ως προς κριτήρια ανεξάρτητα του πεδίου εφαρμογής τους, που εξασφαλίζουν την ομαλή (συντακτικά) εκτέλεσή τους, ασχέτως οποιασδήποτε σημασιολογικής εγκυρότητας· κυριότερο τέτοιο κριτήριο είναι αυτό της *ορθότητας (soundness)*, το οποίο εγγυάται την απουσία συμπεριφορικών ανωμαλιών, όπως είναι τα διάφορα αδιέξοδα (deadlocks, livelocks) και η έλλειψη συγχρονισμού [376][377][3][378]. Για το σκοπό αυτό έχουν παρουσιαστεί ποικίλες λύσεις, οι οποίες συμπεριλαμβάνουν κυρίως αλγόριθμους μετασχηματισμού [379] και διάσχισης [380][381] γράφων και, τέλος, τη μετατροπή μιας ροής εργασιών σε Δίκτυο Petri (Petri Net), ένα φορμαλισμό για τη μοντελοποίηση και ανάλυση ασύγχρονων κατανεμημένων συστημάτων που έχει χρησιμοποιηθεί και για τη μοντελοποίηση ροών εργασιών, και τη μετέπειτα επεξεργασία της σε αυτή τη μορφή από ένα κατάλληλο εργαλείο ανάλυσης [382][376][377][383][384][385][386][387].

Σε αντίθεση με τη δομική επαλήθευση, ο *έλεγχος συμμόρφωσης (compliance checking)* εξετάζει το κατά πόσο μια ροή εργασιών είναι λειτουργικά σωστή, σύμφωνα με συγκεκριμένους κανόνες. Ο έλεγχος συμμόρφωσης μπορεί να λάβει χώρα είτε πριν είτε μετά την εκτέλεση. Η καταγραφή και εκ των υστέρων επιθεώρηση μιας εκτελεσθείσας ροής εργασιών είναι ένας τρόπος να επιτευχθεί το τελευταίο. Στο [388] παρουσιάζεται μια αυτοματοποιημένη προσέγγιση για την ανίχνευση παραβιάσεων από αρχεία καταγραφής ροών εργασιών με χρήση ελεγκτών μοντέλων (model checkers) LTL. Από την άλλη, οι μέθοδοι ελέγχου πριν την εκτέλεση μπορούν περαιτέρω να κατηγοριοποιηθούν σε μεθόδους *συμμόρφωσης εκ σχεδιασμού (compliance by design)* και *επαλήθευσης μετά το σχεδιασμό (post design verification)*. Στις προσεγγίσεις της πρώτης κατηγορίας, οι απαιτήσεις συμμόρφωσης επιβάλλονται κατά το σχεδιασμό νέων επιχειρησιακών διαδικασιών [389][390]. Αντίθετα, στη μετά το σχεδιασμό επαλήθευση ο έλεγχος συμμόρφωσης πραγματοποιείται ένα βήμα μετά το σχεδιασμό, διαχωρίζοντας έτσι τη φάση της μοντελοποίησης μιας διαδικασίας από τη φάση ελέγχου αυτής. Οι υπάρχουσες προτεινόμενες λύσεις επιστρατεύουν ποικίλα εργαλεία και μεθοδολογίες, προκειμένου να επιβεβαιώσουν την εκπλήρωση διαφόρων ειδών απαιτήσεων (επιχειρησιακών, ασφάλειας, κανονιστικών, σχετικών με την ανάθεση πόρων, κλπ.) [391][392][393][394][395][396][397][398][399][400][401][402][403], ενώ ένα σημαντικό μέρος τους εφαρμόζει έλεγχο μοντέλων (model checking) για την επαλήθευση του αν τα μοντέλα διαδικασιών ικανοποιούν τους κανόνες συμμόρφωσης [393][392][404] [405] [406][407][408][406]. Επιπλέον, κάποιες σχετικές προσεγγίσεις πραγματεύονται τη "μέτρηση" και ποσοτική εκτίμηση του βαθμού συμμόρφωσης ενός δεδομένου μοντέλου διαδικασίας [409]. Τέλος, κάποιες εργασίες, όπως η [410], ασχολούνται με ζητήματα επαλήθευσης και επικύρωσης που σχετίζονται συγκεκριμένα με συστήματα διαχείρισης ροών εργασιών πλέγ-

ματος, μια σχετικά νέα και όχι τόσο διερευνηθείσα περιοχή, η οποία παρουσιάζει έναν αριθμό επιπρόσθετων απαιτήσεων.

Συμπερασματικά, οι παραπάνω εργασίες, παρότι σημαντικές, αποτελούν λύσεις γενικού σκοπού και, ως εκ τούτου, δεν είναι σε θέση να καλύψουν συγκεκριμένες απαιτήσεις που σχετίζονται με την ιδιωτικότητα. Προς αυτή την κατεύθυνση, πρόσφατα παρουσιάστηκαν κάποιες ενδιαφέρουσες προσεγγίσεις [397][411][358], οι οποίες, εστιάζοντας σε σημαντικές πλευρές της ιδιωτικότητας, προτείνουν καλά τεκμηριωμένες λύσεις. Ωστόσο, τα εργαλεία ορισμού ροών εργασιών στα οποία βασίζονται δεν έχουν την απαιτούμενη εκφραστικότητα αναφορικά με όλους τους παράγοντες που αφορούν την προστασία προσωπικών δεδομένων, οπότε αρκετοί και σημαντικοί εξ αυτών δε λαμβάνονται υπόψη, τουλάχιστον όχι στον επιθυμητό βαθμό λεπτομέρειας. Τέλος, ακόμα και αυτές δεν προβαίνουν στο μετασχηματισμό των μοντέλων ροών εργασιών στην περίπτωση ανίχνευσης παραβιάσεων, με σκοπό τη μετατροπή τους σε εκτελέσιμες προδιαγραφές συμβατές με την ιδιωτικότητα. Γενικότερα, το ζήτημα της τροποποίησης ροών εργασιών έχει εξάλλου μελετηθεί κυρίως από τη σκοπιά της βάσει σχετικά απλών και γενικής φύσης κανόνων δυναμική προσαρμογής ροών εργασιών κατά την εκτέλεσή τους, και όχι της αλλαγής στην προδιαγραφή τους ήδη από τη φάση του σχεδιασμού [412][413][414][123][415].

Κεφάλαιο 4

Γενική Περιγραφή της Προτεινόμενης Λύσης

4.1 Ροές Εργασιών σε Υπηρεσιοστραφή Περιβάλλοντα

Σε γενικές γραμμές, μια ροή εργασιών είναι μια συλλογή από καλώς ορισμένα βήματα εργασίας που πρέπει να πραγματοποιηθούν από τους διαθέσιμους πόρους (resources) ενός συστήματος με τελικό σκοπό την ολοκλήρωση μιας πιο σύνθετης διαδικασίας, σε συνδυασμό με τις ποικίλες αλληλεξαρτήσεις μεταξύ τους, οι οποίες δηλώνουν τη σειρά εκτέλεσης των εργασιών αλλά και τη σειρά με την οποία αυτές επεξεργάζονται την όποια πληροφορία ανταλλάσσουν. Μια ροή εργασιών αναπαρίσταται σε αφηρημένο επίπεδο συνηθέστερα μέσω ενός κατευθυνόμενου γράφου <*T*, *E*>, του οποίου οι κόμβοι *T* εκπροσωπούν το σύνολο των εργασιών της ροής, ενώ οι ακμές του *E* αντιπροσωπεύουν τις σχέσεις μεταξύ εργασιών και τις αντίστοιχες παραμέτρους. Αφού αρχικά οριστεί μια ροή εργασιών στο κατάλληλο περιβάλλον σχεδιασμού, στη συνέχεια κάθε εργασία εκτελείται από τις οντότητες εκείνες που προσφέρουν την αντίστοιχη δυνατότητα (capability). Στο θεωρούμενο σύστημα, οι οντότητες αυτές προσφέρουν *υπηρεσίες*, οι οποίες εκπροσωπούν με ομοιογενή τρόπο κάθε είδος λειτουργίας που μπορεί να παρέχεται είτε εσωτερικά από τον οργανισμό που ελέγχει την εκτέλεση μιας ροής εργασιών είτε από άλλους οργανισμούς, υποστηρίζοντας έτσι οποιονδήποτε βαθμό κατανομής των διαδικασιών που λαμβάνουν χώρα.

Η παρούσα προσέγγιση, εκκινούμενη από τις γενικές αρχές που παρουσιάστηκαν στο Κεφάλαιο 2, αποσκοπεί στη συμμόρφωση των ροών εργασιών σε υπηρεσιοστραφή περιβάλλοντα με τους κανόνες ιδιωτικότητας και συνακόλουθα την αποτελεσματική προστασία της *"κατά τη στιγμή τόσο του σχεδιασμού των τεχνικών επεξεργασίας όσο και της εκτέλεσης της επεξεργασίας"* σύμφωνα με αντίστοιχη απαίτηση της Ευρωπαϊκής νομοθεσίας [32], υλοποιώντας έτσι την αρχή της *Ιδιωτικότητας εκ Σχεδιασμού (Privacy by Design)* [25].

4.2 Βασικές Αρχές Ιδιωτικότητας και Ροές Εργασιών

Όπως είδαμε λεπτομερώς στο Κεφάλαιο 2, η ιδιωτικότητα προστατεύεται νομοθετικά, και μάλιστα και σε υπερκρατικό/υπερεθνικό επίπεδο, κάτι που καθιστά ακόμα πιο έκδηλη τη σημασία που της αποδίδεται, ενώ πολυάριθμες μελέτες (π.χ., [9][10][11][12][13][14][7][15][16]) έχουν ως αντικείμενο τις αρχές και απαιτήσεις που συνεπάγονται τα σχετικά νομοθετήματα. Ιδιαίτερο ενδιαφέρον παρουσιάζει δε το γεγονός ότι πολλά συναφή νομικά κείμενα αφορούν συγκεκριμένους τομείς, διαδικασίες των οποίων πολύ συχνά αυτοματοποιούνται μέσω συστημάτων ροών εργασιών, όπως οι επικοινωνίες (π.χ., [17][18]), η υγεία (π.χ., [19][20][21]) και η ηλεκτρονική διακυβέρνηση (π.χ., [22][23]). Οι επιμέρους προκλήσεις οι οποίες απορρέουν από τις βασικές αρχές ιδιωτικότητας που πρέπει να διέπουν τα πληροφοριακά συστήματα (βλ. Ενότητα 2.5), ιδωμένες υπό το πρίσμα της διαχείρισης ροών εργασιών, συνοψίζονται στα παρακάτω:

- *Σκοπός (Purpose)*: Η λεγόμενη "αρχή του σκοπού" είναι ουσιώδης για την προστασία της ιδιωτικότητας, ως βασική συνιστώσα της νομιμότητας της συλλογής και επεξεργασίας δεδομένων [32]. Έτσι, μια ροή εργασιών θα πρέπει κατ' αρχάς να επιτρέπει τον προσδιορισμό του σκοπού που αυτή εξυπηρετεί. Παράλληλα, οφείλει να ικανοποιεί την απαίτηση της δέσμευσης σε αυτόν, συνεπώς όλες οι δραστηριότητες στα πλαίσια αυτής θα πρέπει να λαμβάνουν χώρα με ανάλογο τρόπο.

- *Επιβολή δικαιωμάτων πρόσβασης (Access rights enforcement)*: Το γεγονός ότι κάθε παραβίαση ιδιωτικότητας περιλαμβάνει αθέμιτη πρόσβαση σε προσωπικά δεδομένα έχει οδηγήσει στην ανάπτυξη ενός επιμέρους πεδίου των τεχνολογιών ελέγχου πρόσβασης, το οποίο αναφέρεται στη βιβλιογραφία ως έλεγχος πρόσβασης για την προστασία της ιδιωτικότητας (privacy-aware access control) [416][242][241]. Στις ροές εργασιών οι πολιτικές ελέγχου πρόσβασης και χρήσης θα πρέπει να ενσωματώνονται στα μοντέλα κατά τη φάση του σχεδιασμού. Αυτό συνεπάγεται την απαίτηση για ενδελεχή προδιαγραφή των προς εκτέλεση εργασιών, αλλά και ολιστικό έλεγχο της ροής εργασιών ως συνόλου αλληλεπιδρουσών εργασιών.

- *Ροή πληροφορίας σύμμορφη με τις αρχές ιδιωτικότητας (Privacy-aware information flow)*: Πέραν του ελέγχου πρόσβασης και χρήσης, ένα μοντέλο ροής εργασιών πρέπει να επιτρέπει τον εντοπισμό και την παρακολούθηση της διαδρομής των δεδομένων για πιθανές παραβιάσεις ιδιωτικότητας καθώς οι αντίστοιχες πληροφορίες "ρέουν" μεταξύ διαφορετικών υπολογιστικών μονάδων, μετεχόντων, ακόμα και (διοικητικών) τομέων που υπόκεινται σε διαφορετικούς κανονισμούς και πολιτικές.

- *Μη διασύνδεση (Unlinkability)*: Μια ροή εργασιών μπορεί να περιλαμβάνει πολλαπλά σημεία συλλογής και ανάκτησης δεδομένων, εντείνοντας τον κίνδυνο άμεσου ή έμμεσου συνδυασμού τους. Ως εκ τούτου, η δυνατότητα διασύνδεσης δεδομένων θα πρέπει

να ελέγχεται στο επίπεδο του μοντέλου μιας ροής εργασιών, σε ό,τι αφορά τόσο την αναγνώριση των επίμαχων σημείων όσο και την παρεμπόδισή της.

- *Επίγνωση πλαισίου (Context-awareness)*: Όπως έχει διαπιστωθεί και τεκμηριωθεί, οι παράμετροι πλαισίου (context) έχουν συχνά μεγάλη σημασία για τις πολιτικές ασφάλειας και ιδιωτικότητας [263]. Μια ροή εργασιών θα πρέπει να διαθέτει τη δυνατότητα αυτορύθμισης ανάλογα με υποκείμενες συνθήκες αλλά και συμβάντα που ανακύπτουν και επηρεάζουν τη συμπεριφορά της.

- *Διαχωρισμός και Σύνδεση Καθηκόντων (Separation and Binding of Duty – SoD/BoD)*: Πρόκειται για δύο είδη περιορισμών που κατέχουν σημαντική θέση μεταξύ των διαφόρων απαιτήσεων διαχείρισης εξουσιοδοτήσεων στις ροές εργασιών [417], διευκολύνοντας, μεταξύ άλλων, την αποφυγή συγκρούσεων. Η αποτελεσματική εφαρμογή τους χρησιμεύει, εξάλλου, και στην αποτροπή της διασύνδεσης δεδομένων.

- *Συμμετοχή του υποκειμένου των δεδομένων (Data subject participation)*: Ο ρόλος του υποκειμένου των δεδομένων εμφανίζεται ως ιδιαίτερα κρίσιμος στα πλαίσια της δυνατότητας ελέγχου που δικαιούται και πρέπει να έχει το άτομο πάνω στα δεδομένα που το αφορούν. Οι σχετικές απαιτήσεις περιλαμβάνουν τη διαφάνεια και την παροχή των ανάλογων δικαιωμάτων πρόσβασης, ενώ η ροή εργασιών θα πρέπει επιπλέον να προσφέρει μηχανισμούς για την πληροφόρηση του υποκειμένου των δεδομένων και τη λήψη συγκατάθεσης ή προτιμήσεων ιδιωτικότητας από αυτό.

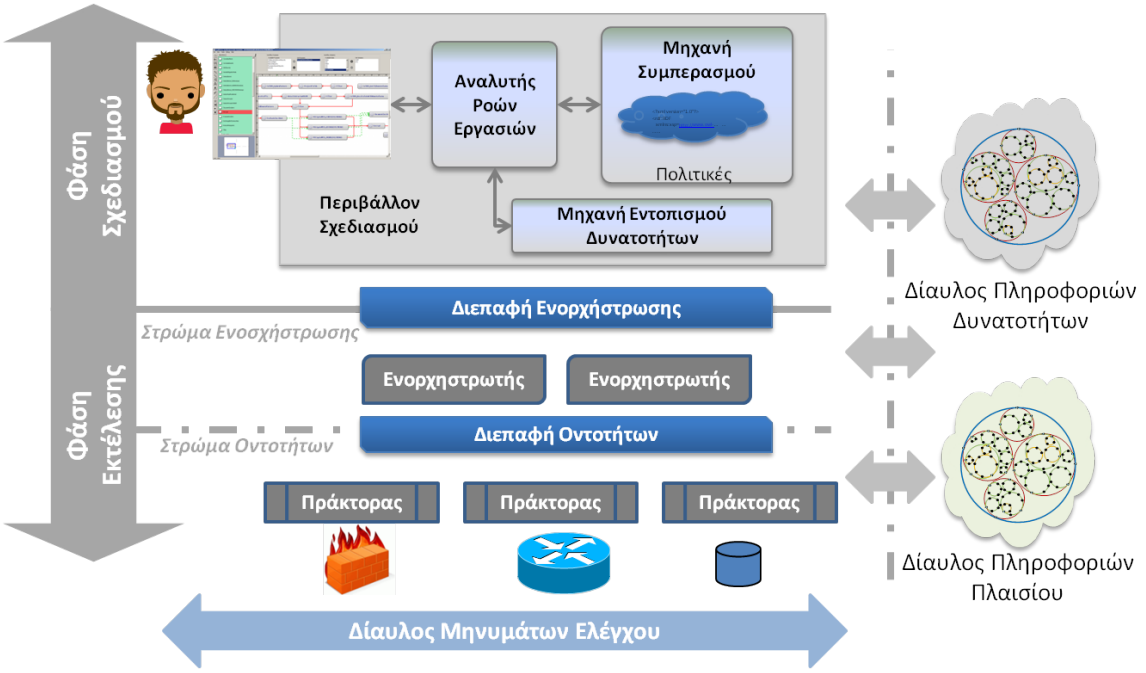
- *Ευθύνη (Accountability)*: Η δυνατότητα για απόδοση ευθύνης, η οποία αποκτά ιδιαίτερη βαρύτητα στους τομείς της ασφάλειας και της ιδιωτικότητας, στα πλαίσια των ροών εργασιών συνίσταται, για παράδειγμα, στην ενσωμάτωση των κατάλληλων μηχανισμών (κατά βάση, εξειδικευμένων εργασιών) για την καταγραφή των διαφόρων ενεργειών.

- *Σημασιολογική περιγραφή (Semantics)*: Οριζόντια με όλα τα παραπάνω είναι η ανάγκη για πλήρη σημασιολογικό ορισμό όλων των υποκείμενων εννοιών. Έτσι, τα δεδομένα, οι ενέργειες και τα υποκείμενά τους, το πλαίσιο και οι σκοποί, μεταξύ άλλων, πρέπει να ορίζονται σημασιολογικά, ενισχύοντας τη διαφάνεια στο επίπεδο της ενοποίησης, τη δυνατότητα απόδοσης ευθύνης και την ακρίβεια σε ό,τι αφορά την ιδιωτικότητα.

Η αρχιτεκτονική αναφοράς, η οποία προσφέρει τους απαραίτητους μηχανισμούς για την επίτευξη των παραπάνω, περιγράφεται στην ενότητα που ακολουθεί.

4.3 Αρχιτεκτονική

Όπως φαίνεται στο Σχήμα 3, ο κύκλος ζωής μιας ροής εργασιών αποτελείται στη γενική περίπτωση από δύο φάσεις: τη *Φάση Σχεδιασμού (Planning Phase)* και τη *Φάση Εκτέλεσης (Execution Phase)*. Η πρώτη αναφέρεται στην προδιαγραφή της ροής εργασιών και



Σχήμα 3: Αρχιτεκτονική συστήματος.

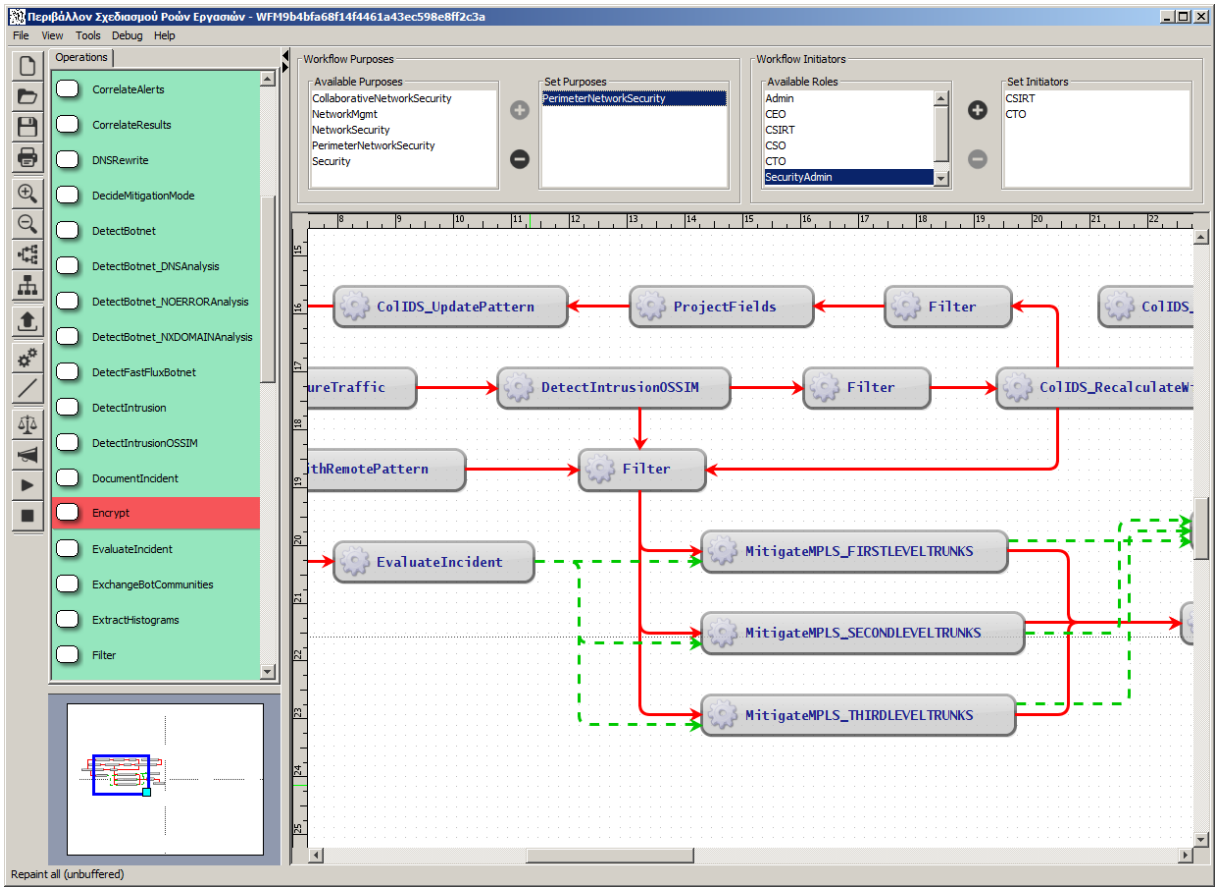
περιλαμβάνει όλα τα βήματα για το γραφικό ορισμό της, την αποσύνθεση των σύνθετων εργασιών (decomposition) σε στοιχειώδεις, τον έλεγχο συμμόρφωσης και τους απαραίτητους μετασχηματισμούς. Από την άλλη, η Φάση Εκτέλεσης βασίζεται στο προϊόν της Φάσης Σχεδιασμού και αναφέρεται σε διαδικασίες που αφορούν την εκτέλεση της έγκυρης πλέον ροής εργασιών από τις υποκείμενες οντότητες.

Το περιβάλλον σχεδιασμού περιλαμβάνει σε υψηλό επίπεδο, εκτός από το κατάλληλο γραφικό εργαλείο, στιγμιότυπο του οποίου απεικονίζεται στο Σχήμα 4, τα ακόλουθα δομικά μέρη:

- τον *Αναλυτή Ροών Εργασιών (Workflow Model Checker)*: είναι η οντότητα η υπεύθυνη για τη διενέργεια της επαλήθευσης και —αν χρειάζεται— τροποποίησης μιας ροής εργασιών, όπως αυτή έχει αρχικά προδιαγραφεί από το σχεδιαστή, ώστε να εξασφαλιστεί ότι υπακούει στους κανόνες ιδιωτικότητας και είναι λειτουργικά ορθή. Τελικά, διοχετεύει μια εκτελέσιμη έγκυρη ροή εργασιών στο Στρώμα Ενορχήστρωσης (βλ. πιο κάτω).

- τη *Μηχανή Συμπερασμού (Reasoner)*: προσφέρει στο σύστημα την απαιτούμενη γνώση για τους διάφορους ελέγχους και μετατροπές, με βάση το σημασιολογικό μοντέλο πολιτικών που ενσωματώνει και τη δυνατότητά της να διεξάγει μια σειρά από λογικούς υπολογισμούς πάνω σε αυτό.

- τη *Μηχανή Εντοπισμού Δυνατοτήτων (Capabilities Matching Component)*: επαληθεύει ότι οι λειτουργίες που ζητούνται στα πλαίσια μιας ροής εργασιών μπορούν πράγματι να παρασχεθούν από την υποκείμενη υποδομή.



Σχήμα 4: Η Γραφική Διεπαφή Χρήστη του Περιβάλλοντος Σχεδιασμού Ροών Εργασιών.

Από την άλλη, το περιβάλλον εκτέλεσης, το οποίο θα περιγραφεί αναλυτικότερα στο Κεφάλαιο 9, αποτελείται από δύο στρώματα:

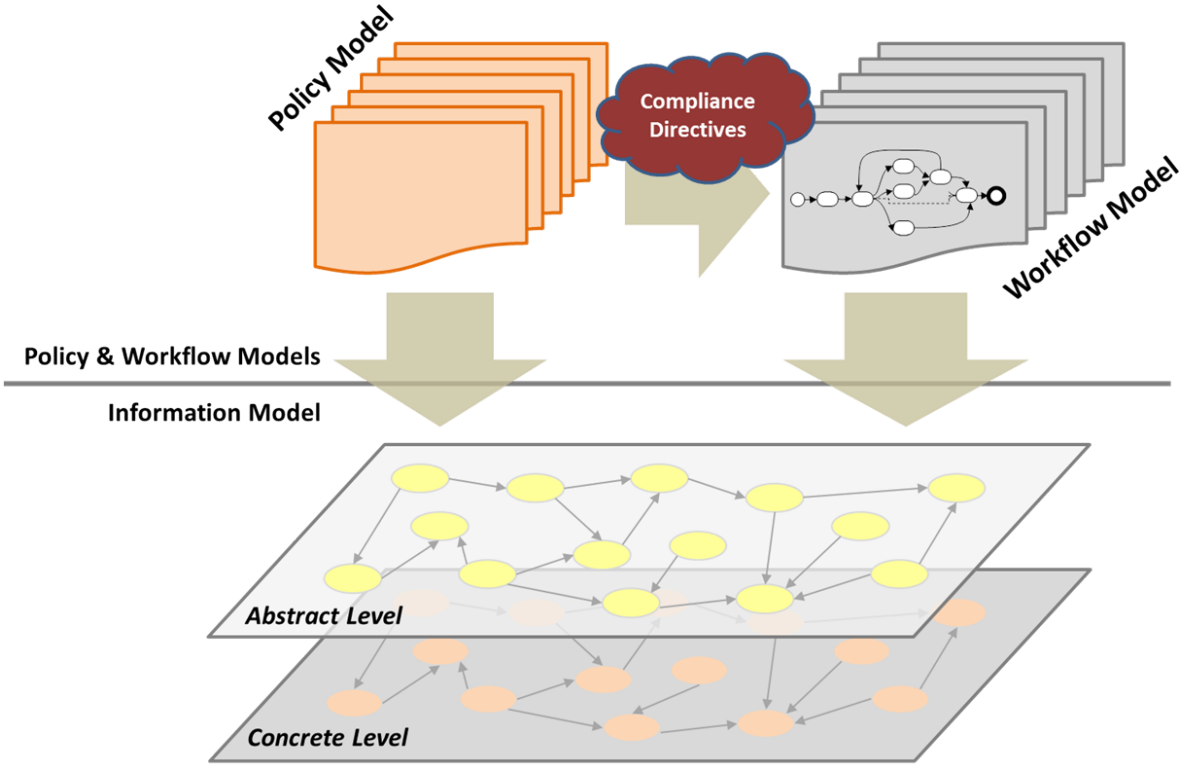
- το *Στρώμα Ενορχήστρωσης (Orchestration Layer)*: περιλαμβάνει ένα σύνολο *Ενορχηστρωτών (Orchestrators)*, καθένας από τους οποίους παίζει το ρόλο του συντονιστή μιας ροής εργασιών καθ' όλη τη διάρκεια εκτέλεσής της.
- το *Στρώμα Οντοτήτων (Components Layer)*: αποτελείται από *Πράκτορες (Agents)*, που παρέχουν την απαραίτητη αφαίρεση στο επίπεδο των υπηρεσιών των υποκείμενων οντοτήτων που θα εκτελέσουν τελικά τις διάφορες εργασίες. Οι Πράκτορες αναλαμβάνουν την επικοινωνία ελέγχου, τη μετατροπή της κλήσης κάθε υπηρεσίας από το Μοντέλο Ανεξαρτήτου Πλατφόρμας (Platform Independent Model – PIM) στο Μοντέλο Συγκεκριμένης Πλατφόρμας (Platform Specific Model – PSM) ανάλογα με τη φύση της υποκείμενης οντότητας, καθώς και καθήκοντα σχετικά με τη δημιουργία, δημοσίευση, κτήση και αποτίμηση πληροφοριών πλαισίου.

Τέλος, δύο βασικά στοιχεία της αρχιτεκτονικής είναι ο *Δίαυλος Πληροφοριών Πλαισίου (Context Bus)* και ο *Δίαυλος Πληροφοριών Δυνατοτήτων (Capabilities Bus)*. Ο πρώτος παρακολουθεί τις τιμές των παραμέτρων πλαισίου σε πραγματικό χρόνο και τις πληροφορίες

σχετικά με τα διάφορα συμβάντα και αναλαμβάνει την κυκλοφορία τους μεταξύ των ενδιαφερόμενων οντοτήτων. Ο Δίαυλος Πληροφοριών Δυνατοτήτων είναι υπεύθυνος για την παροχή πληροφόρησης σχετικά με τις διαθέσιμες "δυνατότητες" των υποκείμενων οντοτήτων, δηλαδή τις λειτουργίες που παρέχουν και άλλα σχετικά χαρακτηριστικά τους. Και τα δύο συστήματα συνιστούν υποδομές Δημοσίευσης/Συνδρομής [107] που καθιστούν δυνατή τη δημοσίευση και λήψη πληροφοριών με βάση τα σημασιολογικά τους χαρακτηριστικά.

Έτσι, στη βάση της παραπάνω υποδομής, αφού μια ροή εργασιών σχεδιαστεί, πραγματοποιείται η επαλήθευσή της ως προς τις απαιτήσεις ιδιωτικότητας που την αφορούν. Στη συνέχεια, προετοιμάζεται η εκτέλεσή της· αυτό προϋποθέτει ότι οι δυνατότητες που προσφέρει το σύστημα έχουν διαφημιστεί στο Δίαυλο Πληροφοριών Δυνατοτήτων, οπότε στο σημείο αυτό αρχικά εντοπίζονται μεταξύ αυτών εκείνες που είναι κατάλληλες για τη διεκπεραίωση των εργασιών της ροής. Κατόπιν, εξάγονται από την επαληθευμένη ροή εργασιών κατάλληλες καθοδηγητικές εντολές εκτέλεσης προς τους Πράκτορες, ορίζοντας επακριβώς τη συμπεριφορά τους τόσο από λειτουργικής άποψης όσο και αναφορικά με την τήρηση των προδιαγεγραμμένων όρων ιδιωτικότητας, όπως αυτές έχουν προηγουμένως ενσωματωθεί στον ορισμό της ροής εργασιών. Οι Πράκτορες αναλαμβάνουν την PIM-σε-PSM μετατροπή των εντολών αυτών και ρυθμίζουν τις υποκείμενες οντότητες, ώστε τελικά να ξεκινήσει η εκτέλεση της ροής εργασιών.

Βασικό συστατικό στοιχείο της παρούσας προσέγγισης αποτελεί η σημασιολογική αναπαράσταση της πληροφορίας που στηρίζει και οδηγεί τη λειτουργία του εν λόγω συστήματος. Στο Σχήμα 5 απεικονίζονται τα σημασιολογικά μοντέλα που χρησιμοποιούνται από τις οντότητες της αρχιτεκτονικής που περιγράφηκε παραπάνω προκειμένου να επιτευχθούν οι στόχοι της διατριβής. Συγκεκριμένα, η Μηχανή Συμπερασμού επεξεργάζεται ένα κατάλληλο *Σημασιολογικό Μοντέλο Πολιτικών (Policy Model)*, προκειμένου να εξάγει τη γνώση που είναι απαραίτητη για την επαλήθευση των ροών εργασιών πριν την εκτέλεσή τους, με τη μορφή *Οδηγιών Συμβατότητας (Compliance Directives)*. Οι τελευταίες περιγράφονται αναλυτικά στο Κεφάλαιο 7. Οι ροές εργασιών, με τη σειρά τους, ορίζονται μέσω των αντίστοιχων *Μοντέλων Ροών Εργασιών (Workflow Models)*, επί των οποίων εφαρμόζονται οι οδηγίες συμβατότητας· ο τρόπος προδιαγραφής των Μοντέλων Ροών Εργασιών παρουσιάζεται εκτενώς στο Κεφάλαιο 6. Όλα τα παραπάνω έχουν ως κοινή αναφορά το ίδιο *Σημασιολογικό Μοντέλο Πληροφοριών (Information Model)* που παρέχει τη φορμαλιστική μοντελοποίηση της εμπλεκόμενης πληροφορίας. Τα βασικά στοιχεία του τελευταίου παρουσιάζονται συνοπτικά στην ενότητα που ακολουθεί, ενώ η Ενότητα 4.5 επισημαίνει τα κύρια χαρακτηριστικά του χρησιμοποιούμενου Σημασιολογικού Μοντέλου Πολιτικών, που το καθιστούν κατάλληλο για τις ανάγκες της διατριβής.



Σχήμα 5: Τα σημασιολογικά μοντέλα του προτεινόμενου συστήματος.

4.4 Σημασιολογικό Μοντέλο Πληροφοριών

Στη λειτουργία ενός οργανισμού εμπλέκονται διάφορες ετερογενείς οντότητες, όπως είναι ο χρησιμοποιούμενος εξοπλισμός, οι χρήστες και τα πάσης φύσεως δεδομένα[23]. Θεωρούμε δύο επίπεδα αναπαράστασης: το *συγκεκριμένο (concrete) επίπεδο* αναφέρεται σε καλώς ορισμένες οντότητες, όπως, για παράδειγμα, προσδιορισμένους ανθρώπους, ενώ το *αφηρημένο (abstract) επίπεδο* καθιστά δυνατή την έμμεση αναφορά σε διάφορες οντότητες με χρήση αφαίρεσης, κυρίως μέσω του σημασιολογικού τους τύπου και των ιδιοτήτων που τις χαρακτηρίζουν.

Στο συγκεκριμένο επίπεδο, το σύνολο των *Χρηστών (Users – U)* αντιπροσωπεύει ανθρώπινες οντότητες, ενώ αυτό των *Οργανισμών (Organisations – Org)* περιγράφει συμμετέχοντα σε μια ροή εργασιών μέρη που έχουν τη μορφή είτε εξωτερικών ως προς το θεωρούμενο σύστημα οργανισμών είτε εσωτερικών υποδιαιρέσεών του (π.χ., τμήματα μιας εταιρείας). Ο υλικός εξοπλισμός εκφράζεται ως το σύνολο των *Μηχανών (Machines – M)*, στους οποίους είναι εγκατεστημένοι *Περιέκτες Λειτουργιών (Operation Containers – OpC)*, που προσφέρουν *Στιγμιότυπα Λειτουργιών (Operation Instances – OpI)*. Τα Στιγμιότυπα Λειτουργιών αντιστοιχούν σε συγκεκριμένες υλοποιήσεις που παρέχουν τις διάφορες λειτουργικότητες,

[23]Προφανώς το μοντέλο πληροφοριών μπορεί να μεταβάλλεται ανάλογα με το εκάστοτε πεδίο εφαρμογών. Ωστόσο, αρκετές έννοιες, όπως οι ρόλοι του οργανογράμματος, οι λειτουργίες, οι τύποι δεδομένων κλπ., εμφανίζονται πρακτικά σε όλα τα περιβάλλοντα και σε αυτά κυρίως εστιάζει η συγκεκριμένη ενότητα.

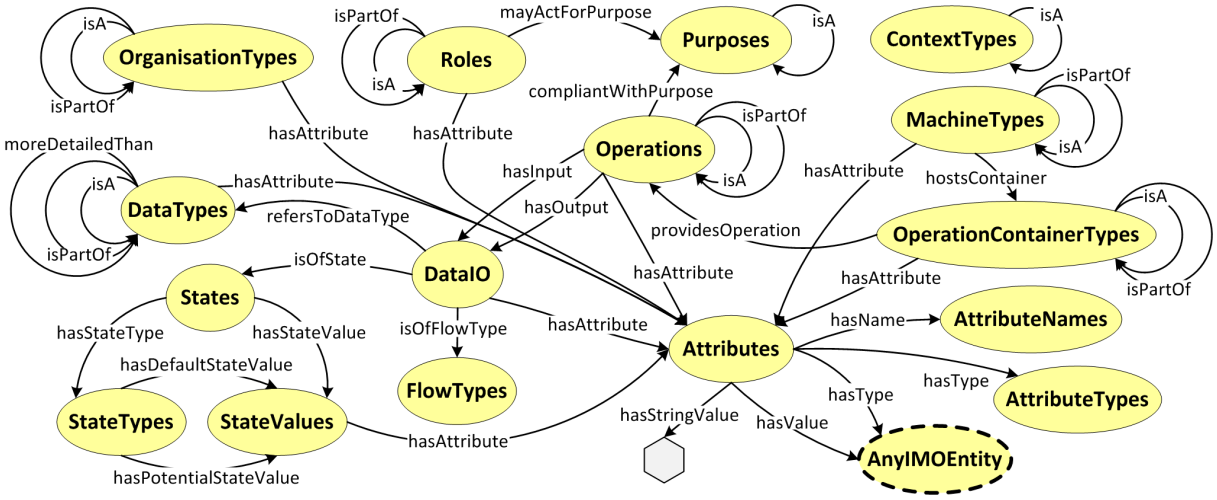
ενώ οι Περιέκτες Λειτουργιών αποτελούν ομάδες από Στιγμιότυπα Λειτουργιών τα οποία προσφέρονται από την ίδια λειτουργική μονάδα. Για παράδειγμα, ένα Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System – IDS) αποτελεί έναν Περιέκτη Λειτουργιών που περιλαμβάνει διάφορες λειτουργίες σχετικές με την ανίχνευση εισβολών[24]. Τέλος, τα διάφορα είδη πληροφορίας απαρτίζουν το σύνολο των *Δεδομένων (Data – D)*.

Όλα τα παραπάνω στοιχεία συνιστούν στιγμιότυπα των σημασιολογικών αναλόγων τους που περιγράφονται στο αφηρημένο επίπεδο. Στους χρήστες εκχωρούνται *Ρόλοι (Roles – R)*, τα Στιγμιότυπα Λειτουργιών παρέχουν υλοποιήσεις *Λειτουργιών (Operations – Op)*, ενώ για τα δεδομένα, τους οργανισμούς, τις μηχανές και τους περιέκτες λειτουργιών ορίζονται οι αντίστοιχοι τύποι, οι οποίοι αντανακλούν τις σημασιολογικές κατηγορίες στις οποίες οι οντότητες αυτές εντάσσονται. Έτσι, προκύπτουν τα σύνολα των *Τύπων Δεδομένων (Data Types – DT)*, των *Τύπων Οργανισμών (Organisation Types – OrgT)*, των *Τύπων Μηχανών (Machine Types – MT)* και των *Τύπων Περιεκτών Λειτουργιών (Operation Container Types – OpCT)*. Το σημασιολογικό μοντέλο περιλαμβάνει επίσης τους *Τύπους Πλαισίου (Context Types – ConT)*, οι οποίοι επιτρέπουν τον ορισμό παραμέτρων πλαισίου, τις *Ιδιότητες (Attributes – Att)*, που χρησιμοποιούνται για την περιγραφή ιδιοτήτων και χαρακτηριστικών άλλων στοιχείων, και τους *Σκοπούς (Purposes – Pu)* που είναι πιθανό να εξυπηρετούνται από την εκτέλεση της εκάστοτε ροής εργασιών.

Το Σημασιολογικό Μοντέλο Πληροφοριών υλοποιείται στην παρούσα προσέγγιση ως οντολογία με χρήση της γλώσσας OWL [111]· η Οντολογία Σημασιολογικού Μοντέλου Πληροφοριών (ΟΣΜΠ) απεικονίζεται Σχήμα 6. Όπως φαίνεται σε αυτό, όλες οι αφηρημένες έννοιες οργανώνονται σε κλάσεις, ενώ ορίζονται διάφορες σχέσεις τόσο μεταξύ μελών της ίδιας κλάσης όσο και μεταξύ μελών διαφορετικών κλάσεων. Οι μεν αφορούν ιεραρχικές σχέσεις σύζευξης (AND) και διάζευξης (OR), επιτρέποντας τον προσδιορισμών ανάλογων εξαρτήσεων και την κληρονομικότητα ιδιοτήτων. Πιο αναλυτικά, οι ιδιότητες αντικειμένου `isA` και `isPartOf` δηλώνουν, αντίστοιχα, την εξειδίκευση μιας έννοιας και τη συμπερίληψη μιας οντότητας σε μια άλλη, ενώ η ιδιότητα `moreDetailedThan` ορίζει μια μερική διάταξη μεταξύ μελών της κλάσης `DataTypes` ανάλογα με το βαθμό λεπτομέρειάς τους. Από την άλλη, οι σχέσεις μεταξύ μελών διαφορετικών κλάσεων περιγράφουν διαφόρων ειδών συσχετίσεις, όπως, για παράδειγμα, ρόλους που επιτρέπεται να δράσουν προς επίτευξη ενός ορισμένου σκοπού (`mayActForPurpose`), ή ιδιότητες που χαρακτηρίζουν κάποια έννοια (`hasAttribute`). Τα μέλη της κλάσης `Attributes`, με τη σειρά τους, συνδέονται με κάποιο κατάλληλο νοηματικά αναγνωριστικό (κλάση `AttributeNames`), με κάποιο τύπο, που μπορεί να παραπέμπει σε κάποιο κοινό τύπο (π.χ., "Integer") ή σε κάποια οντότητα της ΟΣΜΠ, και —προαιρετικά— με μια τιμή. Η τιμή αυτή μπορεί να είναι είτε ένα οντολογικό στοιχείο είτε μια αυθαίρετη συμβολοσειρά και υποδεικνύεται, αντίστοιχα, μέσω των ιδιοτήτων `hasValue` και `hasStringValue`. Μια ιδιότητα για την οποία ορίζεται κάποια τιμή

[24]Με όρους Υπηρεσιών Ιστού, κάθε Περιέκτης Λειτουργιών αντιστοιχεί στη *διεπαφή (interface)* μιας υπηρεσίας, ενώ τα Στιγμιότυπα Λειτουργιών εκπροσωπούν τις μέσω αυτής προσφερόμενες *λειτουργίες (operations)* [54].

από την ίδια την ΟΣΜΠ ονομάζεται *αμετάβλητη (immutable)*, σε αντιδιαστολή με τις *μεταβλητές (mutable)* ιδιότητες, οι τιμές των οποίων ορίζονται κατά το σχεδιασμό μιας ροής εργασιών ή, ανάλογα με την περίπτωση, ακόμα και κατά την εκτέλεσή της. Τέλος, ιδιαίτερα σημαντική για τον ακριβή ορισμό ροών εργασιών είναι η κλάση `DataIO`. Η κλάση αυτή αντιστοιχίζει κάθε λειτουργία με τους τύπους δεδομένων που δέχεται ως είσοδο και παράγει ως έξοδο (όπου υπάρχουν), υποδεικνύοντας, επιπλέον, τους αντίστοιχους τύπους ροής (βλ. Κεφάλαιο 6), καθώς και ιδιότητες που πιθανώς χαρακτηρίζουν περαιτέρω κάθε σχέση εισόδου/εξόδου.



Σχήμα 6: Η Οντολογία Σημασιολογικού Μοντέλου Πληροφοριών (ΟΣΜΠ)

4.5 Σημασιολογικό Μοντέλο Πολιτικών

Σε αναλογία με το συντακτικό σχήμα *υποκείμενο–ρήμα–αντικείμενο*, οτιδήποτε συμβαίνει στα πλαίσια ενός συστήματος μπορεί να θεωρηθεί ως μια *λειτουργία* που επιτελείται από κάποιο *δράστη* πάνω σε κάποιο *αντικείμενο επενέργειας*. Αυτό ισχύει σε κάθε επίπεδο ανάλυσης: σε χαμηλό επίπεδο, για παράδειγμα, ένας αναγνώστης RFID εκτελεί τη λειτουργία της ανάγνωσης (`read`) επί μιας ετικέτας RFID, ενώ στο υψηλότερο επίπεδο μιας επιχειρησιακής διαδικασίας ένα σύνολο δραστών επιτελούν στην ουσία μια συγκεντρωτική υπερ-λειτουργία, αποτελούμενη από πιο στοιχειώδεις λειτουργίες, επί ενός συνόλου αντικειμένων επενέργειας, τα οποία μπορεί εν προκειμένω να είναι προσωπικά δεδομένα. Έτσι, οι διάφοροι κανόνες πρόσβασης θα πρέπει να στρέφονται γύρω από τριάδες της μορφής {*δράστης, λειτουργία, αντικείμενο επενέργειας*}, οι οποίες μπορούν να ορίζονται είτε σε συγκεκριμένο είτε σε αφηρημένο επίπεδο, να αναφέρονται δηλαδή σε συγκεκριμένες αναγνωρίσιμες οντότητες ή αφηρημένες έννοιες που αντιστοιχούν σε κατηγορίες οντοτήτων και παρέχουν τις σχετικές γενικεύσεις.

Ωστόσο, προκειμένου να ρυθμίζεται αποτελεσματικά η λειτουργία ενός συστήματος ροών εργασιών, οι πολιτικές ιδιωτικότητας και οι συνακόλουθοι κανόνες ελέγχου πρό-

σβασης θα πρέπει να ενσωματώνουν κάποια επιπλέον χαρακτηριστικά. Κατ' αρχάς, πρέπει να παρέχεται πλήρης αφαίρεση, με αυτό εννοώντας την περιγραφή όλων των εννοιών σε αφηρημένο επίπεδο, κάτι που επιτρέπει την ενιαία μεταχείριση οντοτήτων που εμπίπτουν στην ίδια εννοιολογική ομάδα. Σε αυτή την κατεύθυνση, το μοντέλο RBAC [239] πρώτο εισήγαγε τη χρήση αφαίρεσης στο επίπεδο των χρηστών μέσω των ρόλων, και συνιστά το βασικό μοτίβο που ακολουθείται από τις περισσότερες προσεγγίσεις. Από την άλλη, λίγες μόνο προσεγγίσεις υποστηρίζουν την αναπαράσταση όλων των εμπλεκόμενων στοιχείων σε αφηρημένο επίπεδο [263][418], ενώ υβριδικές προσεγγίσεις έχουν μόλις πρόσφατα ξεκινήσει να ερευνώνται [419].

Επιπλέον, οι εκάστοτε πολιτικές θα πρέπει να είναι σε θέση να υποδεικνύουν τι θα πρέπει να έχει ήδη συμβεί πριν και τι θα πρέπει να συμβεί μετά από μια ενέργεια, καθώς και να λαμβάνουν υπόψη το ευρύτερο πλαίσιο (context) ή και συμβάντα που είναι πιθανό να ανακύπτουν. Κι ενώ το θέμα των πολιτικών ασφάλειας και ιδιωτικότητας με επίγνωση πλαισίου έχει ερευνηθεί αρκετά, τα περισσότερα σχετικά μοντέλα απλώς υποστηρίζουν μερικώς κάποιες βασικές περιπτώσεις πλαισίου, ιδιαίτερα σε σχέση με διάφορα είδη χρονισμών και ιστορικό εκτέλεσης. Ωστόσο, ένα σύνθετο σύστημα θα πρέπει όχι μόνο να συμπεριφέρεται λαμβάνοντας υπόψη παραμέτρους πλαισίου αλλά και να μπορεί να βασίζει τη λειτουργία του σε συμβάντα.

Με βάση τα παραπάνω, κάθε τριάδα της μορφής {*δράστης, λειτουργία, αντικείμενο επενέργειας*} μπορεί να χαρακτηριστεί ως μια *ενέργεια*. Οι ενέργειες είναι σε θέση να εκπροσωπούν οτιδήποτε λαμβάνει χώρα κατά τη διάρκεια της εξέλιξης μιας διαδικασίας και ως εκ τούτου μπορούν να χρησιμοποιηθούν για τη μοντελοποίηση πλαισίου που αφορά το παρελθόν, το παρόν και το μέλλον, καθώς και τα όποια συμβάντα. Συνεπώς, οι κανόνες που απαρτίζουν κάποια πολιτική ιδιωτικότητας θα πρέπει να ορίζονται στη βάση δομών της μορφής {*ενέργεια, σκοπός, προ-ενέργεια, μετά-ενέργεια, πλαίσιο*} και με τη βοήθεια των κατάλληλων κατηγορημάτων να σχηματίζουν τις προβλεπόμενες άδειες, απαγορεύσεις και υποχρεώσεις των εμπλεκόμενων οντοτήτων. Πιο αναλυτικά, στο εν λόγω μοτίβο:

- η *ενέργεια* εκφράζει το σημείο αναφοράς, το επίκεντρο του κανόνα, με άλλα λόγια, την ενέργεια που ο κανόνας, με τον τρόπο που ορίζεται, επιτρέπει, απαγορεύει ή επιβάλλει να εκτελεστεί.

- ο *σκοπός* αντανακλά τον απώτερο στόχο πίσω από τη συλλογή και επεξεργασία των δεδομένων. Σημειώνεται ότι κανενός είδους απόφαση δεν μπορεί να αγνοεί την παράμετρο αυτή, η οποία είναι ικανή να διαφοροποιεί σημαντικά τη συμπεριφορά μιας οντότητας.

- η *προ-ενέργεια* αντανακλά ενέργειες που θα πρέπει προηγουμένως να έχουν λάβει χώρα, έτσι ώστε ο κανόνας να ενεργοποιείται. Παράδειγμα αποτελεί η απαίτηση ο ασθενής να έχει παράσχει ρητή συγκατάθεση (προ-ενέργεια) προκειμένου ο ιατρικός του φάκελος να υποστεί επεξεργασία για ερευνητικούς σκοπούς.

- η *μετά-ενέργεια*, παρόμοια, υποδηλώνει οτιδήποτε πρέπει να συμβεί μετά την εφαρμογή ενός κανόνα. Για παράδειγμα, ένας κανόνας μπορεί να επιτρέπει την ανάγνωση κάποιων δεδομένων για την παροχή μιας υπηρεσίας, απαιτώντας όμως επιπλέον ότι τα δεδομένα θα διαγραφούν αμέσως μετά.
- το *πλαίσιο* περιγράφει συνθήκες που ορίζονται πάνω σε ιδιότητες και καταστάσεις του "περιβάλλοντος", όπως και συμβάντα.

Επιπρόσθετα, οι διάφορες ενέργειες, προ-ενέργειες και μετά-ενέργειες θα πρέπει να μπορούν να συνδυάζονται μέσω λογικών σχέσεων, σχηματίζοντας σύνθετες δομές ενεργειών, σε αναλογία με σχηματισμούς που στην ορολογία των ροών εργασιών αναφέρονται ως "worklets" [123]. Έτσι, κάποια αναμενόμενη συμπεριφορά εκφρασμένη ως ένα σύνθετο νέφος ενεργειών και συνοδευόμενο από την κατάλληλη σημασιολογική πληροφορία (π.χ., χρονισμοί), ή ακόμα εμφανίζοντας κάποιο βαθμό αοριστίας, μπορεί να συμπεριλαμβάνεται στη θεωρούμενη γνωσιακή βάση ως ένα worklet και ως τέτοιο να χρησιμεύει και αυτό στον έλεγχο και την επαλήθευση των ροών εργασιών.

Ένα σημασιολογικό μοντέλο πολιτικών το οποίο βασίζεται στις παραπάνω αρχές παρουσιάζεται στα [420][419][421][422]. Το μοντέλο αυτό προσφέρει πλήθος πλεονεκτημάτων σε σχέση με αντίστοιχες εργασίες που έχουν προταθεί, παρέχοντας μια ευφυή υποδομή για εξαγωγή γνώσης βασισμένη σε κανόνες, κατάλληλη να καθοδηγήσει τον έλεγχο μιας ροής εργασιών ως προς ποικίλες, πιο απλές αλλά και πιο σύνθετες, απαιτήσεις ιδιωτικότητας. Τα βασικά του στοιχεία είναι οι κανόνες ελέγχου πρόσβασης, οι οποίοι ορίζονται ακολουθώντας το μοτίβο που περιγράφηκε παραπάνω. Με άλλα λόγια, ένας κανόνας ελέγχου πρόσβασης έχει τη δομή:

$$\left.\begin{array}{l} Permission \\ Prohibition \\ Obligation \end{array}\right\} (pu, act, preAct, cont, postAct)$$

όπου *act* είναι η ενέργεια που αφορά ο κανόνας, $pu \in Pu$ είναι ο σκοπός για τον οποίο η ενέργεια *act* επιτρέπεται/απαγορεύεται/επιβάλλεται να εκτελεστεί, $cont \in \mathcal{P}(ConT)$ είναι μια δομή αποτελούμενη από παραμέτρους πλαισίου, *preAct* είναι μια δομή ενεργειών που πρέπει να έχουν προηγηθεί, και *postAct* είναι οι ενέργειες που πρέπει να εκτελεστούν ως συνέπεια της εφαρμογής ενός κανόνα, ακολουθώντας την κυρίως ενέργεια που αυτός αφορά.

Κεφάλαιο 5

Απαιτήσεις Ιδιωτικότητας στις Ροές Εργασιών

5.1 Εισαγωγή

Με αφετηρία τις νομικές και κανονιστικές απαιτήσεις που αφορούν την ιδιωτικότητα στα πληροφοριακά συστήματα, και οι οποίες παρουσιάστηκαν στο Κεφάλαιο 2, το παρόν Κεφάλαιο εμβαθύνει στις εξ αυτών συναγόμενες τεχνικές απαιτήσεις που χαρακτηρίζουν τα περιβάλλοντα ροών εργασιών, λαμβάνοντας υπόψη τις συγκεκριμένες ανάγκες και ιδιαιτερότητες αυτών. Σε αντίθεση με άλλες εργασίες που έχουν κατά καιρούς εμφανιστεί και άπτονται παρόμοιων ζητημάτων, όπως, για παράδειγμα οι [402] [411], και οι οποίες είτε αφορούν την εφαρμογή κανόνων γενικού σκοπού είτε, αντίθετα, επικεντρώνονται μόνο σε κάποιες συγκεκριμένες πλευρές της ιδιωτικότητας, η ανάλυση που ακολουθεί παρέχει μια σφαιρική θεώρηση της προστασίας της ιδιωτικότητας στις ροές εργασιών. Σε αυτή την κατεύθυνση, και εκκινώντας από τις σχετικές προκλήσεις και απαιτήσεις που περιγράφηκαν σε υψηλό επίπεδο στην Ενότητα 4.2, διερευνώνται οι τρόποι αντιμετώπισής τους ως προς δύο κεντρικούς άξονες: α) την ανάγκη να συμπεριληφθούν στο επίπεδο της μοντελοποίησης των ροών εργασιών δομές ικανές να υποστηρίξουν τον ορισμό πολιτικών ιδιωτικότητας ως μέρος του σχεδιασμού τους, οδηγώντας σε στοχευμένες προδιαγραφές ιδιωτικότητας προς επιβολή κατά τη φάση της εκτέλεσης· β) τα βασικά μοτίβα συμμόρφωσης που είναι πιθανό να ανακύψουν και, ως εκ τούτου, πρέπει να υποστηρίζονται, προκειμένου να καταστεί δυνατή η αυτόματη επαλήθευση μοντέλων ροών εργασιών ως προς όρους προστασίας της ιδιωτικότητας, αλλά και η αυτόματη τροποποίησή τους στην περίπτωση της ανίχνευσης παραβιάσεων αυτών [423][424].

5.2 Απαιτήσεις Μοντελοποίησης

Οι απαιτήσεις που παρουσιάστηκαν παραπάνω οδηγούν εν πρώτοις στην ανάγκη για υψηλή εκφραστικότητα αναφορικά με όλες τις διαστάσεις που υπεισέρχονται στη μοντελοποίηση των ροών εργασιών. Στο επίπεδο κάθε μεμονωμένης εργασίας, η σωστή και πλήρης εφαρμογή των δικαιωμάτων πρόσβασης μεταφράζεται σε αποτελεσματικό έλεγχο της *λειτουργίας* που ο *δράστης* ή οι δράστες που αναλαμβάνουν την εκτέλεσή της επιτελούν επί κάποιων *αντικειμένων επενέργειας*, των αντικειμένων, δηλαδή, εκείνων που υφίστανται το αποτέλεσμα της εν λόγω λειτουργίας. Υπό αυτή την έννοια, μια αποτελεσματική προσέγγιση στο θέμα της μοντελοποίησης εργασιών θα πρέπει να αποτυπώνει και τις τρεις αυτές παραμέτρους, επιτρέποντας τον ορισμό έγκυρων δομών της μορφής {δράστης/-ες, λειτουργία, αντικείμενο/-α επενέργειας}. Επιπλέον, δεδομένου ότι μια ροή εργασιών αποτελεί μια δυνητικά ιεραρχική δομή, όπου κάποιες εργασίες μπορούν να αναλύονται σε στοιχειωδέστερες υπο-εργασίες και, αντίστροφα, να συνθέτουν υψηλότερου επιπέδου λειτουργικές μονάδες, και τελικά τη συνολική ροή εργασιών, η εγκυρότητα αυτή πρέπει να εξασφαλίζεται σε όλα τα επίπεδα. Αυτό συνεπάγεται, μεταξύ άλλων, ότι οι (ανθρώπινες) οντότητες που πρόκειται να εκκινήσουν την εκτέλεση της ροής εργασιών πρέπει επίσης να ληφθούν υπόψη, ως δράστες οι οποίοι προκαλούν την εκτέλεση του συνόλου των εργασιών και των αλληλοσυσχετίσεών τους.

Παρόμοια, η ενδελεχής έκφραση της ροής πληροφορίας απαιτεί την κατάλληλη ενσωμάτωση πλήθους παραγόντων. Συγκεκριμένα, είναι καταρχήν απαραίτητη η λεπτομερής περιγραφή των διακινούμενων δεδομένων, εφόσον αυτά δηλώνουν ουσιαστικά τη φύση της πληροφορίας η οποία προσπελαύνεται από τις διάφορες εργασίες. Περαιτέρω, η διακριτή μοντελοποίηση των εισερχόμενων σε μια εργασία δεδομένων, ανεξάρτητα από τα αντικείμενα επενέργειας αυτής, αποτελεί επιπλέον βήμα για τον αποτελεσματικό έλεγχο του τι ακριβώς επιτελείται: παρόλο που τα εισερχόμενα δεδομένα μπορεί να συνιστούν, ως έχουν, και αντικείμενα επενέργειας, είναι πιθανό να χρησιμεύουν απλά ως είσοδος, χωρίς να επηρεάζονται από την αντίστοιχη λειτουργία. Από την άλλη, και μόνο η "ανάγνωση" κάποιου δεδομένου θεωρείται από την ίδια τη νομοθεσία ως είδος επεξεργασίας, ακόμα και στην περίπτωση που δεν υπεισέρχεται αποθήκευση ή άλλου είδους μεταχείρισή του, και συνεπώς θα πρέπει να ελέγχεται εξίσου. Επιπρόσθετα, η σαφής μοντελοποίηση των εισόδων και των αντικειμένων επενέργειας εξυπηρετεί τον έλεγχο διασύνδεσης των δεδομένων, υποβοηθούμενη και από την κατάλληλη σημειολογική επισημείωση των εργασιών, η οποία είναι απαραίτητη για τον προσδιορισμό του τρόπου χειρισμού πολλαπλών εισερχόμενων ροών ή άλλων πηγών πληροφορίας.

Εμβαθύνοντας, προκύπτει ότι επιπλέον έννοιες είναι αναγκαίο να αποτυπωθούν, συμπληρώνοντας την περιγραφή των εργασιών και της ροής πληροφοριών. Καταρχάς όλα τα στοιχεία που περιγράφηκαν παραπάνω θα πρέπει να μπορούν να εμπλουτιστούν με *ιδιότητες*, με τρόπο ανάλογο με αυτόν στον οποίο βασίζονται τα διάφορα μοντέλα ελέγχου πρόσβασης και χρήσης βάσει ιδιοτήτων (attribute-based), π.χ., [425]. Έτσι, ένα αρκού-

ντως περιγραφικό μοντέλο ροών εργασιών θα πρέπει να λαμβάνει υπόψη τις ιδιότητες που χαρακτηρίζουν τους δράστες, τις λειτουργίες ή τα δεδομένα που υφίστανται επεξεργασία ή/και ανταλλάσσονται, προωθώντας τη λεπτομερή προδιαγραφή των υποκείμενων εννοιών. Μεταξύ αυτών, εξάλλου, ιδιαίτερα σημαντική αναφορικά με την εκάστοτε υπό μετάδοση πληροφορία είναι η *κατάσταση των δεδομένων*, με άλλα λόγια η επίδραση πάνω σε αυτά των εργασιών που τα έχουν προηγουμένως επεξεργαστεί ή όχι, σε αντιδιαστολή με άλλες εγγενείς ιδιότητές που πιθανόν τα χαρακτηρίζουν. Η έννοια της κατάστασης δεδομένων είναι καίριας σημασίας για περιπτώσεις όπως είναι, για παράδειγμα, η ανάγκη να καθοριστεί το αν κάποια δεδομένα έχουν υποστεί διαδικασία που τα καθιστά ανώνυμα προτού κάποια άλλη εργασία τα προσπελάσει. Πράγματι, το αν κάποια δεδομένα βρίσκονται σε κατάσταση ανωνυμίας ή όχι είναι καθοριστικό για τον προσδιορισμό του βαθμού ταυτοποίησής τους, υποδεικνύοντας έτσι έμμεσα το είδος των περιορισμών που θα πρέπει να επιβληθούν στην όποια επεξεργασία τους.

Οι καταστάσεις δεδομένων και οι λοιπές ιδιότητες επιτρέπουν τον ορισμό περιορισμών επί των οντοτήτων που συμμετέχουν σε μια ροή εργασιών, οι οποίοι καθιστούν δυνατή τη διαφοροποίηση της συμπεριφοράς της τελευταίας ανάλογα με την ικανοποίηση ή μη αντίστοιχων συνθηκών. Ωστόσο, αυτές δεν είναι οι μόνες παράμετροι που δύνανται να επηρεάσουν την πορεία εκτέλεσης της ροής εργασιών. Σημαντικό ρόλο στη διαμόρφωση των γενικότερων συνθηκών διαδραματίζει επίσης το λεγόμενο πλαίσιο (context) και άλλες εξωγενείς ιδιότητες, ο σκοπός πίσω από κάθε ενέργεια, καθώς και σχέσεις και εξαρτήσεις μεταξύ οντοτήτων της ροής εργασιών. Ως εκ τούτου, η θεώρηση παραμέτρων πλαισίου είναι απαραίτητη για τη διεξοδική μοντελοποίηση ροών εργασιών και αφορά την εφαρμογή αντίστοιχων συνθηκών τόσο σε εργασίες, προδιαγράφοντας την υπο συνθήκη εκτέλεσή τους (π.χ., ορίζοντας παραλλαγές στον τρόπο εκτέλεσης), όσο και στη ροή, προδιαγράφοντας την υπό συνθήκη ”δρομολόγησή” της μέσω εναλλακτικών μονοπατιών ελέγχου και δεδομένων. Ειδικότερα σε ό,τι αφορά τις ροές, διάφορες επιπλέον ιδιότητες θα πρέπει κατά περίπτωση να μπορούν να οριστούν, όπως, για παράδειγμα, μηχανισμοί για την ασφαλή ανταλλαγή των δεδομένων (π.χ., μια έμπιστη VPN σύνδεση για τη μετάδοση πληροφορίας μεταξύ δυο επικοινωνουσών εργασιών).

Αναφορικά με την αρχή του σκοπού, η οποία συνιστά θεμελιώδη απαίτηση σε κάθε περιβάλλον που θέλει να χαρακτηρίζεται από επίγνωση ιδιωτικότητας, το σύστημα θα πρέπει να είναι σε θέση κατ’ αρχάς να αναγνωρίζει το σκοπό που η εκάστοτε επεξεργασία δεδομένων εξυπηρετεί και, σε δεύτερη φάση, να διασφαλίζει τη νομιμότητά του. Μια εγγενής εμπλοκή των ροών εργασιών είναι ότι και μόνο το σε ποιά ακριβώς επεξεργασία υπόκεινται τα δεδομένα δεν είναι ξεκάθαρο ούτε εύκολο να προσδιοριστεί, καθώς αφορά τόσο την επεξεργασία που πραγματοποιείται στα πλαίσια κάθε εργασίας ξεχωριστά αλλά και στη συνολική επεξεργασία την οποία υφίστανται τα δεδομένα αθροιστικά, κατά τη διέλευσή τους από μονοπάτια που περιλαμβάνουν περισσότερες της μιας εργασίες ή μετά την εκτέλεση ολόκληρης της ροής εργασιών. Σε αυτή την κατεύθυνση, μια ενδελεχής προσέγγιση για την εισαγωγή της επίγνωσης σκοπού σε κάθε επίπεδο αφαίρεσης μιας ροής

εργασιών κρίνεται απαραίτητη. Αυτό πρακτικά σημαίνει ότι ο σκοπός πρέπει να συσχετίζεται με κάθε μετέχουσα οντότητα (δράστες, λειτουργίες, δεδομένα, κλπ.) και να μπορεί να συμπεριλαμβάνεται στους περιορισμούς εκείνους που αφορούν τις λεγόμενες *ενδογενείς (intra-workflow) εξαρτήσεις*. Ο όρος αυτός χρησιμοποιείται για να περιγράψει διαφόρων ειδών αλληλοσυσχετίσεις μεταξύ στοιχείων της ροής εργασιών, αντιπροσωπευτικά παραδείγματα των οποίων είναι τα ακόλουθα: η εκτέλεση μιας εργασίας, και οι συνακόλουθες παράμετροι αυτής, εξαρτώνται από το σκοπό ή/και τον εκκινητή της ροής εργασιών· ο δράστης μιας εργασίας πρέπει να είναι η ίδια (φυσική) οντότητα με το δράστη μιας άλλης· σε δράστη ο οποίος έχει προσπελάσει κάποια δεδομένα (μέσω της αντίστοιχης εργασίας) δε θα πρέπει να επιτραπεί η πρόσβαση σε κάποια άλλα· μια εργασία δεν πρέπει να επεξεργάζεται συγκεκριμένα δεδομένα ταυτόχρονα με κάποια άλλα κ.ο.κ.

Επιπλέον, εφόσον οι ροές εργασιών ευνοούν τη συνεργασία και την ανταλλαγή δεδομένων μεταξύ πολλών οντοτήτων, περιλαμβάνοντας σε κάποιες περιπτώσεις διαφορετικούς Υπεύθυνους Επεξεργασίας (Controllers) και Εκτελούντες Επεξεργασία (Processors)[25], ακόμα και τομείς (domains) που υπόκεινται σε διαφορετικούς κανονισμούς ιδιωτικότητας, η όποια πληροφορία σχετική με τα παραπάνω θα πρέπει να αντικατοπτρίζεται με σαφήνεια σε μια προδιαγραφή ροής εργασιών, συνδεόμενη με τις αντίστοιχες κάθε φορά εργασίες. Τέλος, θα πρέπει να λαμβάνονται κατάλληλα μέτρα, ώστε να εξασφαλίζεται ο ενεργός ρόλος συγκεκριμένων κρίσιμων οντοτήτων, όπως είναι τα υποκείμενα των δεδομένων (data subjects) και οι αρμόδιες αρχές προστασίας των δεδομένων. Στα πλαίσια αυτά, θα πρέπει να υποστηρίζεται η, με διαφανή τρόπο, εναρμόνιση μιας ροής εργασιών με τις προτιμήσεις των υποκειμένων δεδομένων που αυτή αφορά και τους κατά περίπτωση ισχύοντες όρους ιδιωτικότητας.

5.3 Αξιολόγηση ως προς τη Συμμόρφωση

Πέρα από το λεπτομερή ορισμό των μοντέλων ροών εργασιών, μια πλήρης προσέγγιση στο ζήτημα της συμμόρφωσης με τις αρχές ιδιωτικότητας πρέπει να περιλαμβάνει τα μέσα για την αξιολόγηση μιας προδιαγραφής ροών εργασιών ως προς κάποιους *άξονες συμμόρφωσης*. Σκοπός των τελευταίων θα πρέπει να είναι α) ο έλεγχος της πρόσβαση σε και της ροής της πληροφορίας και η αποτροπή εν γένει παράτυπων ενεργειών, π.χ., παράνομη διατήρηση δεδομένων, και β) η διαπίστωση του αν ενέργειες αποφασιστικής σημασίας για την ιδιωτικότητα περιλαμβάνονται κατάλληλα και η επιβολή της εκτέλεσής τους σε αντίθετη περίπτωση, όπως, για παράδειγμα, στις περιπτώσεις που απαιτείται πληροφόρηση, συγκατάθεση ή άλλη παρέμβαση του υποκειμένου των δεδομένων, ενημέρωση των αρχών, αποθήκευση ή διαγραφή[26] δεδομένων, κλπ..

[25]Η απόδοση των εν λόγω όρων στα ελληνικά βασίστηκε στα σχετικά επίσημα μεταφρασμένα κείμενα που διατίθενται στο http://ec.europa.eu/justice/data-protection/law/index_en.htm.

[26]Ειδικά το ζήτημα της διαγραφής δεδομένων είναι ιδιαίτερα σύνθετο, καθώς θα πρέπει να εξετάζεται το αν και πώς αυτή επιδρά στη διαθεσιμότητα (availability) των δεδομένων, τόσο από τη σκοπιά της ιδιωτικότητας,

Στις ενότητες που ακολουθούν εξετάζονται διεξοδικά οι βασικοί άξονες συμμόρφωσης ως προς τους οποίους μια ροή εργασιών θα πρέπει να μπορεί να αποτιμηθεί. Εν συντομία, η εγκυρότητα εργασίας και η εγκυρότητα ροής αφορούν παράγοντες που υπεισέρχονται, αντίστοιχα, στην εκτέλεση μεμονωμένων εργασιών και σε απευθείας συσχετίσεις μεταξύ τους. Επιπρόσθετα, η παρουσία εργασιών πριν, μετά, παράλληλα και οπουδήποτε σε σχέση με κάποια εργασία αναφοράς σχετίζεται με απαιτήσεις για εκτέλεση συγκεκριμένων εργασιών στις κατάλληλες θέσεις. Καθεμιά από αυτές τις κατηγορίες απαιτήσεων διαφοροποιείται περαιτέρω ανάλογα με το αν αφορά απλά τη (χρονική) διαδοχή εργασιών, με βάση τις θεμελιώδεις σχέσεις χρονισμού, όπως αυτές κωδικοποιούνται με την άλγεβρα διαστημάτων του Allen [426], ή εστιάζει σε αλληλεξαρτήσεις που προκύπτουν από την επεξεργασία δεδομένων. Τέλος, η έννοια της απαγόρευσης χρησιμοποιείται για την αναφορά σε έμμεσα συσχετιζόμενες εργασίες και ροές, η συνύπαρξη των οποίων δεν επιτρέπεται στο ίδιο στιγμιότυπο της ροής εργασιών. Σημειώνεται ότι, παρόλο που δεν αναφέρεται ρητά για κάθε διαφορετική περίπτωση, κατά τη θεώρηση όλων των αξόνων συμμόρφωσης πρέπει να λαμβάνονται υπόψη και οι σκοποί που πρόκειται να εξυπηρετήσει η ροή εργασιών, αλλά και οι εκκινητές που αναμένεται να προκαλέσουν την εκτέλεσή της. Επίσης, κάθε είδους απαίτηση συμμόρφωσης μπορεί, κατά περίπτωση, να ισχύει με κάποιους περιορισμούς που αφορούν, λόγου χάρη, εξωτερικές συνθήκες, την παρουσία άλλων εργασιών στη ροή (ως προϋποθέσεις για την ανάγκη επιβολής των εν λόγω απαιτήσεων), ή τον τρόπο με τον οποίο κάποιες από αυτές πρόκειται να εκτελεστούν (π.χ., οι δράστες με τους οποίους έχουν οριστεί).

Στο σημείο αυτό τονίζεται ότι η παρακάτω απαρίθμηση δεν είναι εξαντλητική, καθώς σίγουρα μπορούν να προκύψουν επιπλέον περιπτώσεις, εμβαθύνοντας σε ή και συνδυάζοντας τα μοτίβα συμμόρφωσης που περιγράφονται στη συνέχεια.

5.3.1 Εγκυρότητα Εργασίας

Κάθε εργασία πρέπει να είναι σύμμορφη με τις απαιτήσεις ιδιωτικότητας ως αυτόνομη εκτελέσιμη μονάδα. Αυτό συνεπάγεται ότι η αντίστοιχη λειτουργία θα πρέπει να επιδρά πάνω στο σχετικό αντικείμενο επενέργειας, είτε πρόκειται για δεδομένα είτε όχι, με σύννομο τρόπο, και να επιτελείται από έναν εξουσιοδοτημένο δράστη, ο οποίος μπορεί να συνιστά ανθρώπινη οντότητα ή όχι (π.χ., κάποιο λογισμικό), ή να εκφράζει κάτι ευρύτερο που μπορεί να αναλάβει την ευθύνη για την εκτέλεση μιας εργασίας, όπως το τμήμα μιας εταιρείας, έναν οργανισμό, κλπ.. Επίσης, μια εργασία, μέσω του τρόπου που είναι ορισμένη, θεωρείται ότι αναπόφευκτα εξυπηρετεί κάποιους σκοπούς, τουλάχιστον ένας από τους οποίους θα πρέπει να είναι συμβατός με το σκοπό που εξυπηρετεί η ροή εργασιών συνολικά, αλλά και με τους σκοπούς που εξυπηρετούν και οι υπόλοιπες εργασίες της ροής εργασιών. Για παράδειγμα, σε μια ροή εργασιών που εκτελείται σε ένα νοσοκομείο για το σκοπό της "παροχής ιατρικής φροντίδας", κάθε "Ηλεκτρονικός Φάκελος Υγείας

όσο και λειτουργικά/δομικά [381].

(Electronic Health Record – EHR)" (αντικείμενο επενέργειας) μπορεί να "ανακτάται" (λειτουργία) μόνο από άτομα τα οποία κατέχουν το ρόλο "Ιατρός" (δράστης). Επιπλέον, ως ενδεικτικό παράδειγμα περιορισμών που αφορούν τις προαναφερθείσες ενδογενείς εξαρτήσεις, μπορεί να υπάρχει η απαίτηση ο εν λόγω γιατρός να είναι το ίδιο άτομο με το δράστη της εργασίας "φροντίζω ασθενή", οδηγώντας, έτσι, στην προδιαγραφή ενός περιορισμού Σύνδεσης Καθηκόντων (Binding of Duty – BoD) μεταξύ των δύο εργασιών.

5.3.2 Εγκυρότητα Ροής

Ο βασικός παράγοντας που καθιστά δυσκολότερο τον εντοπισμό παραβιάσεων της ιδιωτικότητας στις ροές εργασιών είναι ακριβώς η ροή πληροφορίας μεταξύ υπολογιστικών μονάδων, μετεχόντων, ακόμα και (διοικητικών) τομέων που υπόκεινται σε διαφορετικούς κανονισμούς. Λαμβάνοντας επιπλέον υπόψη το γεγονός ότι, όπως προαναφέρθηκε, ακόμα και η πρόσβαση σε δεδομένα μόνο για ανάγνωση αποτελεί νομικά μορφή επεξεργασίας αυτών, θα πρέπει να εξασφαλίζεται ότι, για κάθε ζεύγος εργασιών άμεσα συνδεόμενων μέσω ροής ελέγχου ή δεδομένων (η οποία συμβολίζεται μέσω της αντίστοιχης ακμής), η ανταλλαγή πληροφορίας μεταξύ τους, ή απλά η διαδοχή τους, είναι σύννομη. Αυτό αφορά τον τύπο της εκάστοτε επικοινωνούμενης πληροφορίας, ιδιότητες που μπορεί να τη χαρακτηρίζουν ή την κατάσταση στην οποία βρίσκεται, πιθανόν σε συνδυασμό με τις κρατούσες συνθήκες πλαισίου. Στην περίπτωση που οι σχετικές απαιτήσεις δεν ικανοποιούνται, πιθανόν να είναι εφικτή η παρεμβολή κατάλληλων επιπλέον εργασιών στην αντίστοιχη ροή, προκειμένου αυτές να επιτελέσουν τις απαραίτητες μετατροπές πάνω στα δεδομένα, που θα καταστήσουν τη ροή πληροφορίας συμβατή με τους αντίστοιχους κανονισμούς πρόσβασης. Τέλος, θα πρέπει επίσης να διασφαλίζεται ότι και ιδιότητες που αφορούν μηχανισμούς μεταφοράς δεδομένων χαμηλού επιπέδου, όπως, π.χ., μια συγκεκριμένη πλατφόρμα επικοινωνίας ή κάποιο πρωτόκολλο, επαρκούν για την ασφάλεια και εμπιστευτικότητα των δεδομένων.

5.3.3 Παρουσία Πριν

Θεωρώντας μια εργασία αναφοράς μέσα σε μια ροή εργασιών, πιθανόν να απαιτείται να έχουν προηγηθεί αυτής άλλες εργασίες στην πορεία της εκτέλεσης. Η απαίτηση αυτή μπορεί να λάβει διάφορες επιμέρους μορφές, ανάλογα με τους χρονικούς περιορισμούς και τις αλληλεξαρτήσεις στην επεξεργασία των δεδομένων που υποδηλώνει.

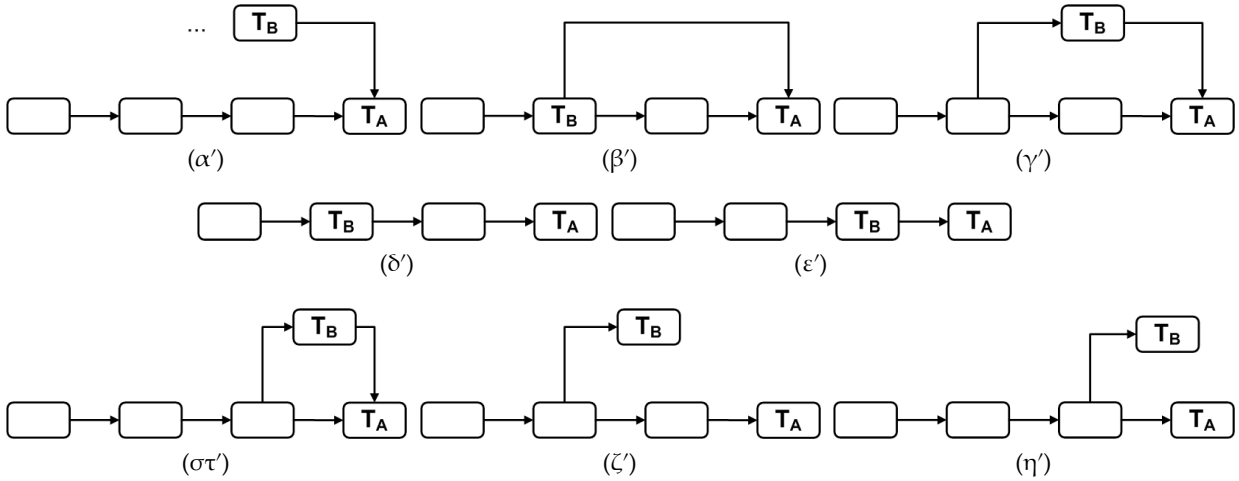
Αρχικά, μια εργασία αναφοράς T_A μπορεί να *απαιτεί κάποια δεδομένα εισόδου* προερχόμενα από την εργασία T_B. Αυτό συνεπάγεται κατά βάση ότι η T_B πρέπει να έχει ήδη ολοκληρώσει την εκτέλεσή της και στη συνέχεια να έχει παράσχει τα δεδομένα εξόδου της (ή κάποια από αυτά) στην T_A. Συνεπώς, ως προς την τοπολογία του γράφου της ροής εργασιών, η T_B πρέπει να ανήκει σε όλα τα πιθανά εναλλακτικά μονοπάτια που μπορεί κατά την εκτέλεση να οδηγήσουν στην T_A, ενώ θα πρέπει να υπάρχει και η αντίστοιχη

ακμή η οποία θα συνδέει τις δυο εργασίες και θα μεταφέρει την επιθυμητή (με όρους τύπων δεδομένων, ιδιοτήτων, κλπ.) είσοδο. Οι απαιτήσεις εισόδου μπορούν να εμφανιστούν σε τρεις παραλλαγές: *απλή*, *σύνδεσης μονοπατιού* και *άμεσης σύνδεσης*. Μια απαίτηση εισόδου απλού τύπου υποδεικνύει μόνο το είδος της εισόδου και την εργασία από την οποία αυτή πρέπει να προέρχεται (T_B), χωρίς να θέτει οποιουσδήποτε περιορισμούς ως προς τον τρόπο με τον οποίο η T_B συνδέεται με την υπόλοιπη ροή εργασιών, και μπορεί να ικανοποιηθεί από οποιαδήποτε τοπολογία διασφαλίζει μια τέτοια σχέση, όπως, π.χ., στα Σχήματα 7α′, 7β′, 7γ′, 7ε′, 7στ′[27]. Η σύνδεση μονοπατιού υποδηλώνει ότι η T_B πρέπει να ανήκει σε ή να συνδέεται (ως προς τα δεδομένα που λαμβάνει) με ένα ήδη εισερχόμενο στην T_A μονοπάτι, ακόμα και αν δεν αποτελεί μέρος αυτού, όπως στα 7β′, 7γ′, 7στ′. Για παράδειγμα, η T_A ίσως χρειάζεται να λάβει ως είσοδο το αποτέλεσμα μια συνάρτησης κατακερματισμού (hash) επί των δεδομένων που ήδη λαμβάνει, προκειμένου να επικυρωθεί η ακεραιότητά τους. Πιο αυστηρή ακόμα, η άμεση σύνδεση θέτει τον επιπλέον περιορισμό ότι η T_B πρέπει να εκτελεστεί επί δεδομένων που ήδη παρέχονται απευθείας στην T_A, ή, γενικότερα, να σχετίζεται ως προς τις εισόδους της με μια εργασία η οποία έτσι κι αλλιώς δίνει δεδομένα στην T_A (Σχήμα 7στ′).

Ένας διαφορετικός τύπος απαίτησης που αφορά παρελθούσες συσχετίσεις δεδομένων είναι αυτός της *προέλευσης των δεδομένων*, ο οποίος υποδηλώνει ότι κάποια δεδομένα εισόδου της T_A θα πρέπει να έχουν παραχθεί ή υποστεί κάποια (προ-)επεξεργασία από την T_B (Σχήματα 7β′, 7δ′, 7ε′). Από την άλλη, μπορεί να απαιτείται *συμπληρωματική προ-επεξεργασία* από την T_B, που σημαίνει ότι τα δεδομένα τα οποία παρέχονται ως είσοδος στην T_A, ή δεδομένα που απλά εμφανίζονται σε ένα εισερχόμενο μονοπάτι, πρέπει να υποστούν επεξεργασία από την T_B σε κάποιο (χρονικό) σημείο που να προηγείται της εκτέλεσης της T_A· τέτοιες απαιτήσεις ικανοποιούνται από όλα τα μοτίβα του Σχήματος 7. Σε αντίθεση με την απαίτηση προέλευσης, ωστόσο, εδώ τα δεδομένα δε χρειάζεται απαραίτητα να περνούν *διαμέσου* της T_B, η οποία μπορεί και να "κρέμεται" από την αντίστοιχη εισερχόμενη ροή, όπως δείχνουν τα Σχήματα 7γ′, 7στ′, 7ζ′, 7η′. Η συμπληρωματική προ-επεξεργασία εκ φύσεως υποδηλώνει *σύνδεση μονοπατιού*, με την έννοια ότι η T_B πρέπει να έχει επιδράσει σε όλα τα σχετικά δεδομένα που μεταφέρονται μέσω όλων των αντίστοιχων εισερχόμενων μονοπατιών, αδιάφορο σε ποιό ακριβώς χρονικό σημείο αυτό έχει συμβεί. Για παράδειγμα, πριν την αντιμετώπιση ενός συμβάντος που οδηγεί δυνητικά σε διαρροή προσωπικών δεδομένων, όλες οι σχετικές ειδοποιήσεις θα πρέπει να έχουν προηγουμένως αποθηκευτεί για το σκοπό της ανάλυσης σε μη πραγματικό χρόνο. Σε πιο αυστηρά πλαίσια, η *άμεση σύνδεση* μπορεί να χρησιμοποιηθεί και εδώ για να εκφράσει ότι η T_B πρέπει να επιδράσει στα δεδομένα κατά το τελευταίο βήμα, στην κατάσταση, δηλαδή, στην οποία βρίσκονται όταν μεταφέρονται στην T_A από κάποια αμέσως προηγούμενη εργασία (προκειμένου, λόγου χάρη, να διασφαλιστεί ότι λαμβάνεται υπόψη η τελική εκδοχή των

[27]Στα σχήματα που θα χρησιμοποιηθούν στο εξής (στο παρόν κεφάλαιο) δεν απεικονίζεται οποιαδήποτε πληροφορία σχετικά με τα μεταφερόμενα δεδομένα για λόγους απλότητας· σε ό,τι αφορά, ωστόσο, τις απαιτήσεις που αφορούν συσχετίσεις δεδομένων, θεωρούμε ότι οι αντίστοιχες ροές αφορούν κάθε φορά τα κατάλληλα δεδομένα.

δεδομένων), όπως στα Σχήματα 7ε′, 7στ′, 7η′.



Σχήμα 7: Ενδεικτικά τοπολογικά μοτίβα που ικανοποιούν απαιτήσεις "παρουσίας πριν".

Τέλος, η απαίτηση *κατάστασης δεδομένων* υποδηλώνει ότι κάποια δεδομένα που φτάνουν ως είσοδος στην T_A πρέπει να βρίσκονται σε μια συγκεκριμένη κατάσταση, προκληθείσα μέσω της επεξεργασίας τους από μια κατάλληλη εργασία T_B. Αν και μοιάζει αρκετά με την απαίτηση προέλευσης, η βασική της διαφορά είναι ότι θα πρέπει να εξασφαλιστεί η μη αναστροφή της κατάσταση αυτής μέχρι να έρθει η στιγμή να εκτελεστεί η T_A. Ως παράδειγμα, μπορούμε να θεωρήσουμε την περίπτωση κατά την οποία η T_A επιτρέπεται να εκτελεστεί πάνω σε κάποια δεδομένα, μόνο αν τα τελευταία γίνονται σε αυτή διαθέσιμα μέσω ψευδωνύμων. Εδώ, δεν αρκεί η εργασία T_B, που πραγματοποιεί τη δημιουργία των ψευδωνύμων με βάση τα αρχικά δεδομένα, να βρίσκεται σε κάθε μονοπάτι το οποίο μεταφέρει τα δεδομένα αυτά στην T_A, αλλά πρέπει επιπρόσθετα να μην υπάρχει μεταξύ των T_B και T_A εργασία τέτοια που να πραγματοποιεί ανάκτηση των αρχικών δεδομένων από τα αντίστοιχα ψευδώνυμα.

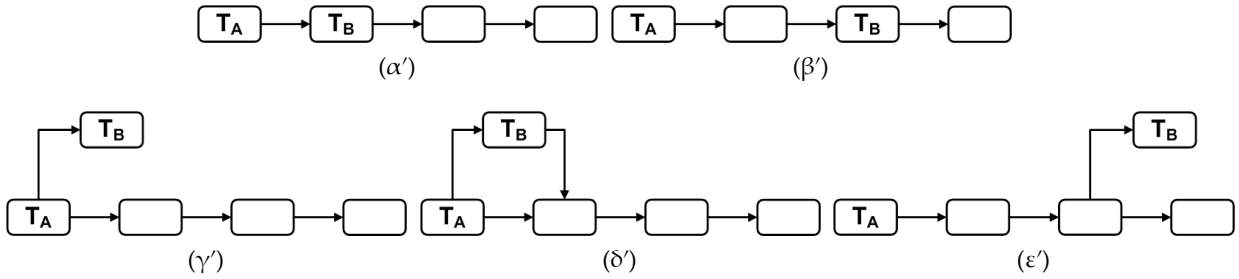
Από την οπτική γωνία της διαδοχής των εργασιών, μπορεί να απαιτείται η T_B να έχει εκτελεστεί *ακριβώς πριν* την T_A. Με άλλα λόγια, πριν η T_A ξεκινήσει την εκτέλεσή της, η T_B πρέπει να έχει μόλις ολοκληρωθεί, να είναι, δηλαδή, το τελευταίο πράγμα που θα έχει εκτελεστεί πριν την T_A (Σχήμα 7στ′). Για παράδειγμα, αμέσως πριν την επεξεργασία κάποιων δεδομένων, μπορεί να απαιτείται έλεγχος του αν η ανάλογη συγκατάθεση του υποκειμένου των δεδομένων υπάρχει και, επιπλέον, δεν έχει λήξει. Χαλαρώνοντας την παραπάνω απαίτηση, η *συμπληρωματική εκτέλεση* της T_B *πριν* την T_A επιτάσσει ότι η τελευταία θα πρέπει απλά να ακολουθεί την εκτέλεση της T_B. Αυτό δε σημαίνει ότι θα πρέπει να την ακολουθεί άμεσα, όπως παραπάνω, αλλά απλώς ότι η T_B θα πρέπει, σε κάθε περίπτωση, να έχει ήδη εκτελεστεί τουλάχιστον μία φορά. Στην *απλή* μορφή της απαίτησης αυτής, αρκεί η T_B να έχει ήδη ξεκινήσει, κάτι που ικανοποιείται από όλα τα μοτίβα του Σχήματος 7. Αν, αντίθετα, η απαίτηση οριστεί ως *αναστολτική*, η T_B θα πρέπει επιπλέον να έχει ολοκληρώσει την εκτέλεσή της πριν η T_A ξεκινήσει (Σχήματα 7α′, 7β′, 7γ′, 7δ′, 7ε′,

7στ′).

5.3.4 Παρουσία Μετά

Με παρόμοια λογική, κάποιες εργασίες μπορεί να χρειάζεται να εκτελεστούν μετά από μια εργασία αναφοράς T_A. Όταν απαιτείται *άμεση μετα-επεξεργασία* από την T_B πάνω σε κάποια δεδομένα, η T_B πρέπει να είναι η εργασία η αμέσως επόμενη της T_A επί του αντίστοιχου μονοπατιού δεδομένων, έτσι ώστε τα δεδομένα εξόδου της T_A που αφορά η απαίτηση να υποστούν την προσδιοριζόμενη τροποποίηση προτού προσπελαστούν και/ή υποστούν περαιτέρω επεξεργασία από οποιαδήποτε επόμενη εργασία της ροής (Σχήμα 8α′). Κάτι τέτοιο αντανακλά, για παράδειγμα, η απαίτηση ότι τα δεδομένα εξόδου (ή ορισμένα από αυτά) μιας συγκεκριμένης εργασίας θα πρέπει να κρυπτογραφούνται πριν την προσπέλασή τους από τις εργασίες που ακολουθούν. Από την άλλη, η *συμπληρωματική άμεση μετα-επεξεργασία* υπονοεί επιπλέον επεξεργασία, με την έννοια ότι η T_A πρέπει απλώς να τροφοδοτήσει με δεδομένα εξόδου της την T_B, συμπληρωματικά με τις συσχετίσεις δεδομένων στις οποίες πιθανώς ήδη συμμετέχει (Σχήματα 8α′, 8γ′, 8δ′). Για παράδειγμα, μπορεί να υπάρχει η ανάγκη, αμέσως μετά την εκτέλεση μιας εργασίας, κάποια εμπλεκόμενα δεδομένα να διαγράφονται άμεσα. Πέρα από την *απλή* αυτή μορφή, η αντίστοιχη απαίτηση μπορεί να εμφανιστεί και ως *συνδυαστική* ως προς τις ακόλουθες εργασίες της ροής, που σημαίνει ότι οι τελευταίες θα πρέπει να λάβουν υπόψη τους τα δεδομένα εξόδου της T_B, προκειμένου να συνεχιστεί η εκτέλεση της ροής εργασιών (Σχήματα 8α′, 8δ′). Τέλος, σύμφωνα με μια απαίτηση *συμπληρωματικής μετα-επεξεργασίας*, η οποία συνιστά τη λιγότερο αυστηρή μεταξύ των απαιτήσεων μελλοντικής παρουσίας που αφορούν αλληλεξαρτήσεις δεδομένων, η T_B πρέπει να εκτελεστεί επί δεδομένων που παράγονται/εξέρχονται από την T_A σε κάποιο σημείο κατά μήκος κάθε πιθανού εξερχόμενου μονοπατιού. Στην περίπτωση αυτή η άμεση γειτνίαση μεταξύ των δυο εργασιών δεν είναι απαραίτητη, αρκεί η T_B να επεξεργάζεται τα σωστά δεδομένα, ανεξάρτητα από τις εργασίες που έχουν στο μεταξύ εκτελεστεί· μια τέτοια απαίτηση ικανοποιείται από όλα τα μοτίβα του Σχήματος 8.

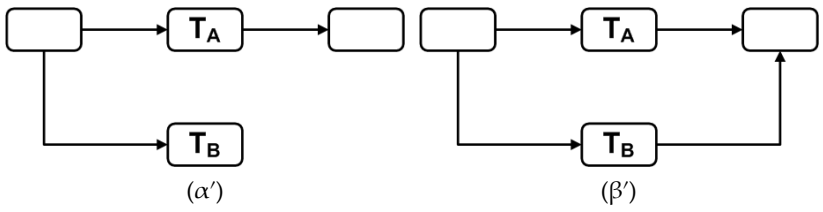
Σε ό,τι αφορά τη διαδοχή εργασιών, είναι πιθανό να απαιτείται η T_B να εκτελεστεί *αμέσως μετά* την ολοκλήρωση της T_A (Σχήματα 8α′, 8γ′, 8δ′). Ενδεικτικό παράδειγμα αποτελεί η περίσταση κατά την οποία, κάθε φορά που μια συγκεκριμένη ενέργεια έχει ως αποτέλεσμα την παραγωγή ειδοποιήσεων συμβάντων, θα πρέπει να ενημερώνεται άμεσα για το γεγονός αυτό το αρμόδιο για θέματα ιδιωτικότητας στέλεχος (Privacy Officer). Μια τέτοια απαίτηση μπορεί σε κάποιες περιπτώσεις να εμφανιστεί ως *αναστολτική*, με την έννοια ότι η T_B πρέπει επίσης να ολοκληρωθεί προκειμένου να προχωρήσει η εκτέλεση της ροής εργασιών (Σχήματα 8α′, 8δ′). Επιπλέον των παραπάνω, μπορεί να προκύψει η ανάγκη για *συμπληρωματική εκτέλεση* της T_B *μετά* την T_A ανεξαρτήτως εγκύτητας. Σε μια τέτοια περίπτωση δεν υπάρχουν άλλοι χρονικοί περιορισμοί πέραν του ότι αφού ολοκληρωθεί η T_A θα πρέπει κάποια στιγμή να εκτελεστεί και η T_B (ικανοποιείται από όλα τα μοτίβα του Σχήματος 8).



Σχήμα 8: Ενδεικτικά τοπολογικά μοτίβα που ικανοποιούν απαιτήσεις "παρουσίας μετά".

5.3.5 Παρουσία Παράλληλα

Μια ξεχωριστή κατηγορία απαιτήσεων αφορά την παραλληλία στην εκτέλεση των εργασιών. Από την οπτική γωνία της χρονικής αλληλουχίας, η *συμπληρωματική παράλληλη εκτέλεση* αναφέρεται στην περίπτωση που οι εργασίες T_A και T_B πρέπει να ξεκινήσουν ταυτόχρονα, με άλλα λόγια, μετά την ολοκλήρωση της αμέσως προηγούμενης εργασίας (ή εργασιών), η σκυτάλη εκτέλεσης πρέπει να περάσει ταυτόχρονα και στις δύο (Σχήματα 9α′, 9β′). Όταν μια τέτοια απαίτηση χαρακτηρίζεται επιπλέον ως *ανασταλτική*, αυτό σημαίνει ότι τόσο η T_A όσο και η T_Bπρέπει να έχουν ολοκληρωθεί προκειμένου να προχωρήσει η εκτέλεση της ροής εργασιών[28] (Σχήμα 9β′). Όταν δίνεται έμφαση στη ροή πληροφορίας, ωστόσο, η παραλληλία αποκτά άλλο νόημα, αγνοώντας αυστηρούς χρονικούς περιορισμούς όπως οι παραπάνω. Σε αυτή την κατεύθυνση, η *συμπληρωματική παράλληλη επεξεργασία* απαιτεί ότι οι T_A και T_B πρέπει να εκτελούνται με βάση τα ίδια ή σχετιζόμενα δεδομένα, τα δεδομένα εισόδου τους, δηλαδή, πρέπει να προέρχονται από ή να σχετίζονται με την ίδια προηγούμενη εργασία (Σχήματα 9α′, 9β′). Για παράδειγμα, όταν κάποια δεδομένα δρομολογούνται προς κάποια εργασία η οποία πραγματοποιεί τη διαγραφή τους, πρέπει όλα τα αντίγραφα αυτών στο σύστημα να διαγράφονται επίσης. Σε μια πιο αυστηρή εκδοχή, η συμπληρωματική παράλληλη επεξεργασία μπορεί να απαιτηθεί ως *συνδυαστική*, υποδηλώνοντας ότι οι εργασίες που ακολουθούν θα πρέπει να εκτελεστούν βασιζόμενες από κοινού στα δεδομένα εξόδου των T_A και T_B (Σχήμα 9β′).



Σχήμα 9: Ενδεικτικά τοπολογικά μοτίβα που ικανοποιούν απαιτήσεις "παρουσίας παράλληλα".

[28]Εδώ η ανάλυση σε περισσότερες υποπεριπτώσεις είναι δυνατή, θεωρώντας πιο εξεζητημένες σχέσεις χρονισμού, όπως αυτές που ορίζονται στο [426], ωστόσο στα πλαίσια της διατριβής το ζήτημα δεν εξετάζεται περαιτέρω.

5.3.6 Παρουσία Οπουδήποτε

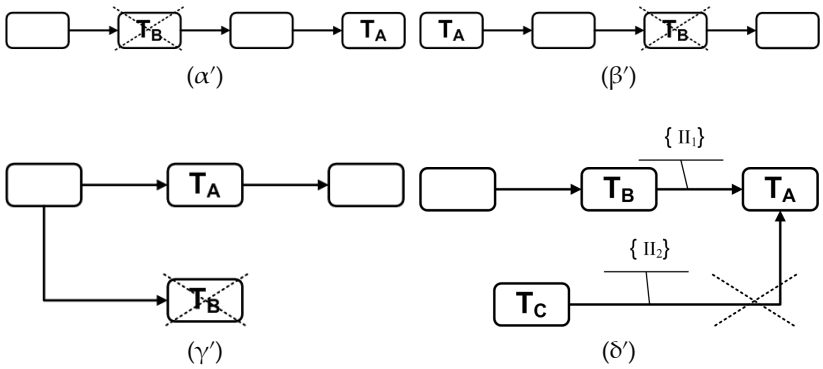
Εκτός από τα παραπάνω, μια εργασία μπορεί να πρέπει απλά να εκτελεστεί στα πλαίσια μιας ροής εργασιών, ανεξάρτητα από τη θέση της και τη σχετική διάταξή της ως προς οποιαδήποτε άλλη εργασία της ροής. Σε ό,τι αφορά τη διαδοχή εργασιών, μια τέτοια απαίτηση, η οποία αναφέρεται και ως *ύπαρξη εργασίας*, μπορεί να προκύπτει εξαιτίας της παρουσίας μιας άλλης εργασίας ή και όχι· μπορεί, για παράδειγμα, να εξαρτάται από το σκοπό ή/και τον εκκινητή που συνδέεται συνολικά με τη ροή εργασιών. Σε κάθε περίπτωση, αρκεί η απαιτούμενη εργασία να εμφανίζεται τουλάχιστον μία φορά σε κάθε εκτελέσιμο στιγμιότυπο του γράφου της ροής εργασιών. Σε μια περισσότερο περιοριστική εκδοχή, ωστόσο, μπορεί να απαιτείται η ύπαρξη της εν λόγω εργασίας επί συγκεκριμένων μονοπατιών δεδομένων, με σκοπό να διασφαλιστεί ότι τα αντίστοιχα δεδομένα υφίστανται τη συγκεκριμένη επεξεργασία κάποια στιγμή κατά τη διάρκεια ζωής τους εντός της ροής εργασιών, αδιάφορο σε ποιό ακριβώς στάδιο αυτό συμβαίνει.

5.3.7 Απαγόρευση

Στον αντίποδα των απαιτήσεων που υπαγορεύουν την παρουσία συγκεκριμένων εργασιών στη ροή, άλλες μπορεί να απαγορεύουν την εκτέλεση εργασιών ή κάποιες μορφές εξαρτήσεων μεταξύ τους. Στο επίπεδο των επιμέρους εργασιών και των απευθείας σχέσεων ροής, οι πιθανές απαγορεύσεις καλύπτονται από τις απαιτήσεις για εγκυρότητα εργασιών και ροής, που περιγράφηκαν στις Ενότητες 5.3.1 και 5.3.2, αντίστοιχα. Επεκτείνοντας την έννοια της απαγόρευσης σε μεγαλύτερη κλίμακα, δηλαδή, στις έμμεσες/απομακρυσμένες σχέσεις ροής, δυο εργασίες μπορεί να θεωρούνται αμοιβαία αποκλειόμενες σε συγκεκριμένες σχετικές θέσεις μεταξύ τους ή γενικά μέσα στην ίδια ροή εργασιών. Με όρους απλά ακολουθιακής διαδοχής, η εκτέλεση μιας εργασίας αναφοράς T_A μπορεί να συνεπάγεται την απαγόρευση της εκτέλεσης της T_B σε οποιοδήποτε σημείο πριν, μετά, παράλληλα ή και οπουδήποτε μέσα στη ροή εργασιών (π.χ., όπως στα Σχήματα 10α′, 10β′, 10γ′). Για παράδειγμα, προκειμένου να αποφευχθεί η διασύνδεση δεδομένων, μπορεί σε μια ροή εργασιών που αφορά τη διαχείριση παραγγελιών να απαγορεύεται το ίδιο άτομο που χειρίζεται την προετοιμασία μιας παραγγελίας να επιλαμβάνεται και της συνακόλουθης τιμολόγησης του πελάτη, προκειμένου κανένας εργαζόμενος να μην είναι σε θέση να γνωρίζει ποιός έχει αγοράσει τι (Διαχωρισμός Καθηκόντων – SoD). Όταν δίνεται έμφαση στη ροή δεδομένων μεταξύ λειτουργιών επεξεργασίας, η απαγόρευση μπορεί επιπλέον να εντοπίζεται πιο συγκεκριμένα στο μονοπάτι που τα δεδομένα ενδιαφέροντος διασχίζουν, υποδηλώνοντας ότι οι T_A και T_B δε θα πρέπει να προσπελαύνουν ή επηρεάζουν τα ίδια δεδομένα.

Τέλος, είναι πιθανό μια απαγόρευση να μην αφορά τις εργασίες καθεαυτές αλλά τις ροές που τις συνδέουν. Ένα ενδεικτικό παράδειγμα απεικονίζεται στο Σχήμα 10δ′: με δεδομένη τη ροή πληροφορίας μεταξύ των T_B και T_A, η οποία έχει σαν αποτέλεσμα την

πρόσβαση της T_A στη μονάδα πληροφορίας (information item) II_1, απαγορεύεται η εργασία T_C να παράσχει την πληροφορία II_2 στην T_A. Το αξιοσημείωτο εδώ είναι ότι μπορεί να επιτρέπεται η εκτέλεση αυτόνομα (ως προς την T_A) της T_C, ή ακόμα και η ίδια ακριβώς ροή μεταξύ των T_C και T_A αν απουσίαζε η ροή από την T_B προς την T_A.



Σχήμα 10: Ενδεικτικά τοπολογικά μοτίβα σχετικά με απαιτήσεις ”απαγόρευσης”.

Κεφάλαιο 6

Προδιαγραφή Ροών Εργασιών

6.1 Εισαγωγή

Όπως επισημάνθηκε στην Ενότητα 3.3, οι δύο βασικές και ως τώρα μη επικαλυπτόμενες κατηγορίες ροών εργασιών, επιχειρησιακές και επιστημονικές, εμφανίζουν θεμελιώδεις διαφορές, κυρίως ως προς το υπόδειγμα εκτέλεσης που ακολουθούν και το είδος και το βαθμό επέμβασης του ανθρώπινου παράγοντα. Οι επιχειρησιακές ροές εργασιών εστιάζουν στη ροή ελέγχου, με άλλα λόγια, στη διαδοχή των εργασιών και στις εξαρτήσεις αιτίου–αιτιατού μεταξύ τους, και προβλέπουν την ανάμιξη ανθρώπων–χρηστών, τη στιγμή που η ροή δεδομένων διαδραματίζει δευτερεύοντα ρόλο. Αντίθετα, οι επιστημονικές ροές εργασιών είναι σε μεγάλο ποσοστό αυτοματοποιημένες και επικεντρώνονται στη ροή δεδομένων, η εκτέλεσή τους, δηλαδή, οδηγείται από τις εξαρτήσεις δεδομένων μεταξύ των εργασιών. Τα παραπάνω έχουν σαν αποτέλεσμα αρκετά αποκλίνουσες προσεγγίσεις στη μοντελοποίηση και παρ' όλο που υπάρχει ένας ολοένα αυξανόμενος αριθμός εφαρμογών, οι απαιτήσεις των οποίων αδυνατούν να καλυφθούν από μία μόνο εκ των δύο κατηγοριών ροών εργασιών, καμία υπάρχουσα τεχνολογία δεν ενδείκνυται αφ' εαυτής για τη μοντελοποίηση τόσο επιχειρησιακών όσο και επιστημονικών ροών εργασιών. Παράλληλα, είναι αξιοσημείωτο το ότι καθεμιά από τις διαθέσιμες προσεγγίσεις στερείται επαρκούς εκφραστικότητας σε ό,τι αφορά τουλάχιστον μία από τις τρεις βασικές όψεις των ροών εργασιών (ροής ελέγχου, δεδομένων και πόρων) [4]. Ωστόσο, η σπουδαιότητα όλων των παραπάνω στοιχείων αναφορικά με την προστασία της ιδιωτικότητας δεν είναι ευκαταφρόνητη και, ως εκ τούτου, η εκπροσώπησή τους σε κάθε σχετική λύση κρίνεται απαραίτητη.

Έτσι, ένας από τους βασικούς άξονες της διατριβής συνίσταται στην προδιαγραφή ενός νέου τρόπου ορισμού ροών εργασιών, ο οποίος και αποτελεί το αντικείμενο του παρόντος κεφαλαίου [427]. Η προτεινόμενη μέθοδος επιτρέπει, μέσω ποικίλων δομών και μηχανισμών, τη λεπτομερή αναπαράσταση όλων των σημαντικών συστατικών στοιχείων μιας ροής εργασιών, συμπεριλαμβανομένων των εργασιών, των πόρων, των δεδομένων, αλλά και των εξωτερικών προς αυτή συνθηκών, βασιζόμενη όχι μόνο στο σημασιολογικό τους

χαρακτηρισμό αλλά και στον ακριβέστερο προσδιορισμό τους μέσω κατάλληλων περιορισμών πάνω σε ιδιότητες και σχέσεις. Περαιτέρω, εισάγει την έννοια του *αντικειμένου επενέργειας*, η οποία εμφανίζεται για πρώτη φορά στα πλαίσια της μοντελοποίησης ροών εργασιών και εξυπηρετεί τη ρητή αναπαράσταση των οντοτήτων που αποτελούν αποδέκτες των επιτελούμενων λειτουργιών. Τέλος, παρέχει έναν ενοποιημένο τρόπο μοντελοποίησης της ροής ελέγχου και της ροής δεδομένων, επιτρέποντας τον ορισμό ροών εργασιών που ακολουθούν οποιοδήποτε από τα δύο πρότυπα, ή και συνδυασμούς τους.

6.2 Βασικές Έννοιες

Σε γενικές γραμμές, μια *ροή εργασιών (workflow)* περιγράφει μια σειρά ενεργειών με καλά ορισμένες σχέσεις αλληλουχίας και εξαρτήσεις δεδομένων μεταξύ τους. Μια υπό εκτέλεση ροή εργασιών αναφέρεται ως *στιγμιότυπο ροής εργασιών (ΣΡΕ) (workflow instance)*, ενώ η προδιαγραφή της παρέχεται μέσω ενός *μοντέλου ροής εργασιών (ΜΡΕ) (workflow model)*, ενός "προσχεδίου", δηλαδή, από το οποίο προκύπτουν τα εκτελέσιμα στιγμιότυπα.

Το Σχήμα 11α' δείχνει ένα παράδειγμα ροής εργασιών, το οποίο θα χρησιμοποιηθεί στο παρόν Κεφάλαιο για την επεξήγηση των κύριων στοιχείων της ακολουθούμενης προσέγγισης. Η εν λόγω ροή εργασιών είναι εμπνευσμένη από διαδικασίες που σχετίζονται με τη λειτουργία τηλεπικοινωνιακών παρόχων. Η επιλογή του συγκεκριμένου πεδίου εφαρμογών βασίστηκε στο γεγονός ότι το τελευταίο συχνά περιλαμβάνει τη συνύπαρξη ροών ελέγχου και δεδομένων, κάτι που, όπως προαναφέρθηκε, αποτελεί σημαντική συνεισφορά της προτεινόμενης λύσης. Πράγματι, ένας τηλεπικοινωνιακός πάροχος είναι ένας επιχειρηματικός οργανισμός ο οποίος εκτελεί κατά κύριο λόγο επιχειρησιακές διαδικασίες (business processes), στα πλαίσια των οποίων, ωστόσο, τα τηλεπικοινωνιακά δεδομένα καθεαυτά συνιστούν ρεύματα δεδομένων (data streams) που υφίστανται επεξεργασία σε πραγματικό χρόνο, με σκοπό την επίτευξη αντίστοιχων εσωτερικών επιχειρησιακών στόχων (π.χ., διαχείριση δικτύου, ασφάλεια, κλπ.). Το παράδειγμα αφορά σε μια απλοποιημένη ροή εργασιών που αποσκοπεί στην αντιμετώπιση συμβάντων ασφάλειας (security incidents). Τα συμβάντα, αφού ανιχνευθούν μετά από λήψη και κατάλληλη επεξεργασία της δικτυακής κίνησης, αποτιμώνται, με στόχο τον καθορισμό της κατάλληλης στρατηγικής αντιμετώπισής τους. Αφού αντιμετωπιστεί, κάθε συμβάν καταγράφεται, ενώ περαιτέρω δεδομένα που σχετίζονται με την καταπολέμησή του, καθώς και οι αντίστοιχες ειδοποιήσεις που οδηγούν στην ανίχνευσή του (alerts), καταγράφονται επίσης για μελλοντική αναφορά. Για λόγους εμπιστευτικότητας, συγκεκριμένα πεδία των ειδοποιήσεων αυτών κρυπτογραφούνται πριν την καταγραφή.

Η προτεινόμενη μέθοδος προδιαγραφής ροών εργασιών είναι *σημασιολογική*, με την έννοια ότι βασίζεται στην ακριβή σημασιολογική ερμηνεία όλων των συστατικών στοιχείων τους, κάτι το οποίο έχει εξάλλου επισημανθεί ως έλλειψη των βασικών προσεγγίσεων στην περιοχή [167]. Επιπλέον, κάθε ΜΡΕ συμπληρώνεται από ένα *σημασιολογικό μο-*

ντέλο πληροφοριών, το οποίο ορίζει τις έννοιες που περιγράφουν τις οντότητες που συμμετέχουν στη ροή και τις αλληλοσυσχετίσεις τους. Στα πλαίσια της διατριβής, το θεωρούμενο Σημασιολογικό Μοντέλο Πληροφοριών είναι αυτό που περιγράφεται στην Ενότητα 4.4 και το οποίο, όπως είναι φυσικό, αποτελεί και τη βάση του Σημασιολογικού Μοντέλου Πολιτικών που οδηγεί την επαλήθευση των ροών εργασιών (βλ. Ενότητα 4.5). Τα MPE υλοποιούνται και αυτά οντολογικά με χρήση της γλώσσας OWL [111].

6.2.1 Μοντέλα Ροών Εργασιών

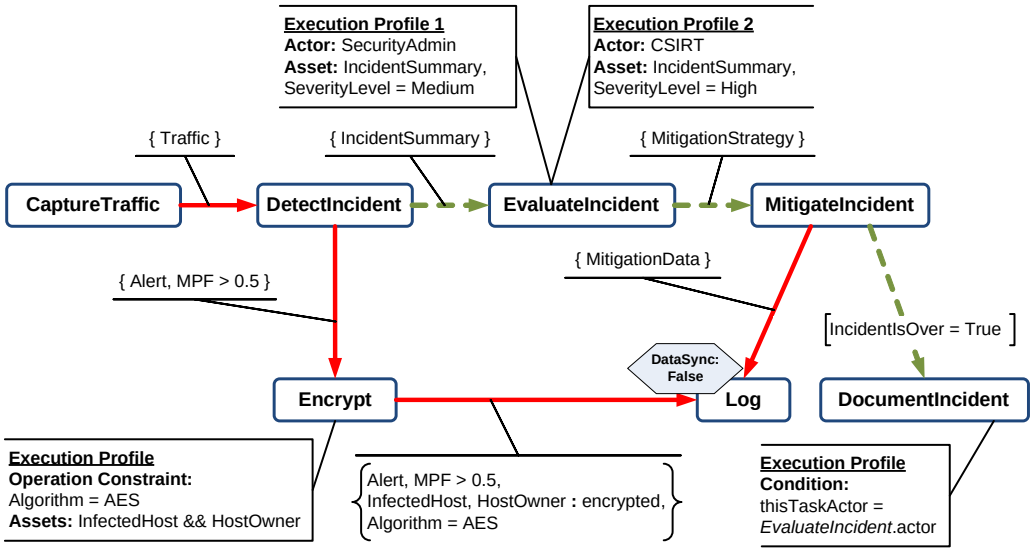
Τα θεμελιώδη στοιχεία που απαρτίζουν ένα MPE είναι οι *εργασίες (tasks)* και οι *ροές (flows)*. Οι πρώτες αντιπροσωπεύουν τις ενέργειες που πρέπει να εκτελεστούν στα πλαίσια της ροής εργασιών, καθεμιά από τις οποίες περιγράφει μια *λειτουργία (operation)* που εκτελείται από κάποιο *δράστη (actor)* πάνω σε κάποιο *αντικείμενο επενέργειας (asset)*. Οι ροές εκφράζουν εξαρτήσεις μεταξύ εργασιών, συμβολίζονται με κατευθυνόμενες ακμές και διακρίνονται σε δύο τύπους: *ελέγχου (control)* και *δεδομένων (data)*. Μια εξάρτηση ροής ελέγχου $t_A \xrightarrow{f_c} t_B$ μεταξύ δύο εργασιών t_A και t_B εκφράζει ότι η t_B εκτελείται μόνο αφού η εκτέλεση της t_A έχει ολοκληρωθεί· αυτό που "μεταφέρει" η ακμή σε αυτή την περίπτωση είναι το νήμα εκτέλεσης, πιθανώς συνοδευόμενο από απαραίτητες παραμέτρους ελέγχου. Αντίθετα, μια εξάρτηση ροής δεδομένων $t_A \xrightarrow{f_d} t_B$ υποδηλώνει ότι και οι δύο εργασίες βρίσκονται συνεχώς υπό εκτέλεση, με την t_B, ωστόσο, να εξαρτάται από το ρεύμα δεδομένων που παράγεται από την t_A. Εν συντομία, η ροή δεδομένων, σε αντίθεση με τη ροή ελέγχου, δεν πυροδοτεί την εκτέλεση μιας εργασίας· η εργασία ενεργοποιείται μόνο μια φορά (κατά την εκκίνηση της ροής εργασιών) και στη συνέχεια "γεννά" πολλαπλά στιγμιότυπα εκτέλεσης, βασιζόμενη στην άφιξη των δεδομένων και, πιθανώς, σε επιπρόσθετη σηματοδοσία ελέγχου [149].

Επιπλέον, ένα MPE συμπληρώνεται από τους επιχειρησιακούς *σκοπούς (purposes)* που προορίζεται να εξυπηρετήσει και τους υποψήφιους *εκκινητές (initiators)*, τις (ανθρώπινες) οντότητες, δηλαδή, που είναι εξουσιοδοτημένες να εκκινήσουν την εκτέλεση της ροής εργασιών συνολικά.

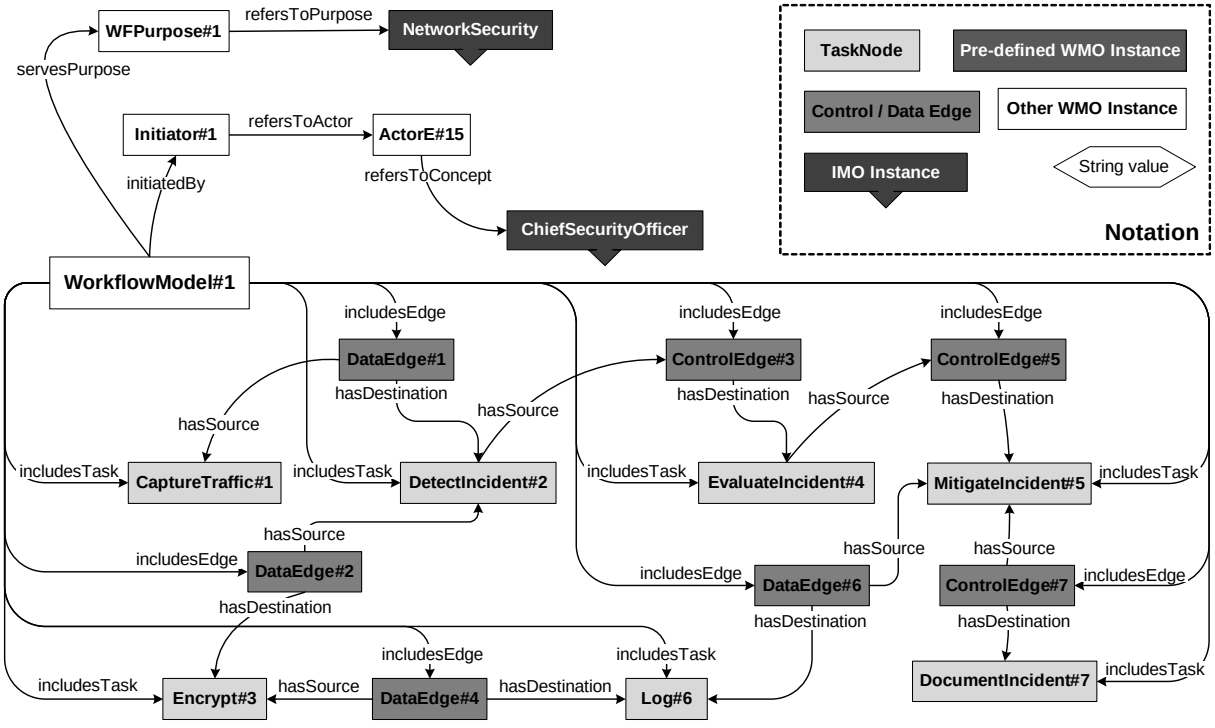
Συμπερασματικά, ένα MPE ορίζεται ως ακολούθως:

Ορισμός 1 Ενα *μοντέλο ροής εργασιών (MPE)* είναι μια πλειάδα $\langle T, F_C, F_D, Init, WFPu \rangle$, τέτοια ώστε: T είναι ένα πεπερασμένο σύνολο εργασιών $\langle t_1, t_2, ..., t_n \rangle$· F_C και F_D είναι σύνολα κατευθυνόμενων ακμών που εκφράζουν τις σχέσεις ροής ελέγχου και δεδομένων μεταξύ εργασιών· *Init* είναι το σύνολο των δραστών που, με βάση τη συγκεκριμένη προδιαγραφή, επιτρέπεται να εκκινήσουν την εκτέλεση της ροής εργασιών· $WFPu \subseteq Pu$ δηλώνει το σύνολο των σκοπών για την εξυπηρέτηση των οποίων η ροή εργασιών πρόκειται να εκτελεστεί.

Το κύριο τμήμα της *Οντολογίας Μοντέλων Ροών Εργασιών (OMPE)* φαίνεται στο Σχήμα 12α'. Όλες οι έννοιες που παίρνουν μέρος σε μια προδιαγραφή ροής εργασιών εκ-



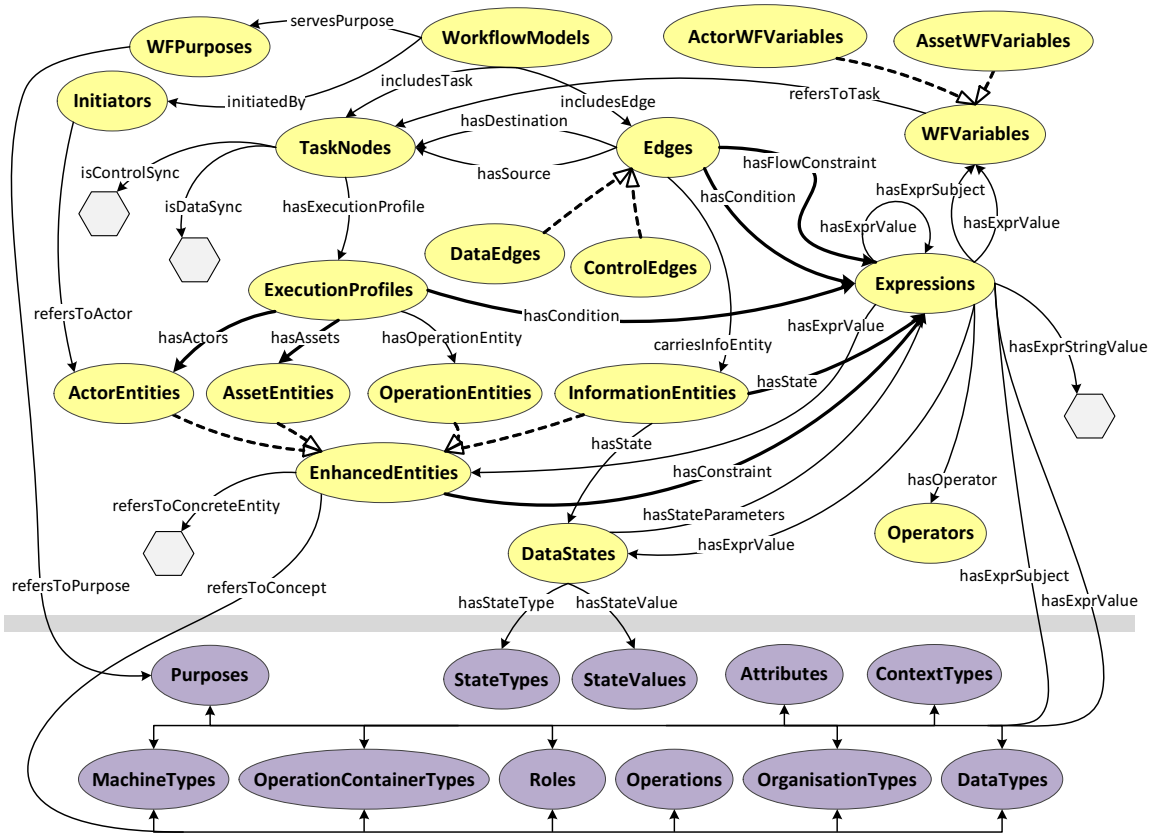
(α′) Απλοποιημένο παράδειγμα ροής εργασιών για τη διαχείριση συμβάντων ασφάλειας δικτύου. Τα ορθογώνια πλαίσια και οι κατευθυνόμενες ακμές αντιπροσωπεύουν εργασίες και ροές, αντίστοιχα· οι συνεχόμενες ακμές δηλώνουν ροή δεδομένων, ενώ οι διακεκομμένες ροή ελέγχου.



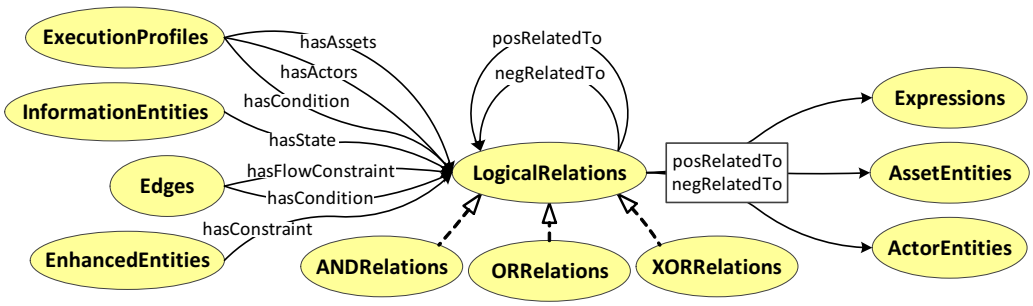
(β′) Οντολογική αναπαράσταση της παραπάνω ροής εργασιών, με έμφαση στα μέλη των κλάσεων `TaskNodes` και `ControlEdges/DataEdges`· τα ονόματα των πρώτων ακολουθούν εκείνα των λειτουργιών που υλοποιούν με βάση την ΟΣΜΠ (π.χ., `DetectIncident`) με την επιπλέον προσθήκη ενός ακεραίου, ενώ τα ονόματα των ακμών ακολουθούν το πρότυπο ControEdge/DataEdge με την προσθήκη επίσης ενός ακεραίου στο τέλος. Επιπρόσθετα απεικονίζεται ο τρόπος σύνδεσης ενός μέλους της `WorkflowModels` με έναν εξυπηρετούμενο σκοπό, καθώς και με έναν εκκινητή. Το πλαίσιο "Notation" επεξηγεί τη σημειογραφία που θα χρησιμοποιείται στα παραδείγματα του παρόντος Κεφαλαίου.

Σχήμα 11: Παράδειγμα ροής εργασιών

προσωπούνται από μέλη των αντίστοιχων κλάσεων, ενώ οι σχέσεις μεταξύ τους, καθώς και με στοιχεία της ΟΣΜΠ μοντελοποιούνται μέσω ιδιοτήτων αντικειμένου OWL.



(α′) Το κύριο μέρος της OMPE. Τα πιο σκουρόχρωμα στοιχεία αντιστοιχούν σε κλάσεις της ΟΣΜΠ.



(β′) Λογικές σχέσεις στην OMPE

Σχήμα 12: Η Οντολογία Μοντέλων Ροών Εργασιών (OMPE).

Πιο συγκεκριμένα, κάθε MPE εκπροσωπείται από ένα μέλος της κλάσης `WorkflowModels`, το οποίο συσχετίζεται με ένα σύνολο μελών της κλάσης `Initiators` και ένα σύνολο μελών της `WFPurposes`, μέσω των ιδιοτήτων `initiatedBy` και `servesPurpose`. Η κλάση `Initiators` δείχνει, μέσω της ιδιότητας `refersToActor`, σε εκείνα τα μέλη της `ActorEntities` (βλ. Ενότητα 6.3.1) που αποτελούν εκκινητές της ροής εργασιών, ενώ η `refersToPurpose` αντιστοιχίζει τα μέλη της `WFPurposes` με τα μέλη της `Purposes` της ΟΣΜΠ που ορίζουν σημασιολογικά τους εν λόγω σκοπούς.

Οι εργασίες και οι ακμές ορίζονται μέσω των κλάσεων `TaskNodes` και `Edges`, ενώ η τελευταία υποδιαιρείται περαιτέρω στις υποκλάσεις `DataEdges` και `ControlEdges`, σε αντιστοιχία με τους δύο τύπους ροής F_D and F_C. Από εκεί και πέρα, οι ιδιότητες `includesTask` και `includesEdge` συνδέουν κάθε μέλος της `WorkflowModels` με τις εργασίες και ακμές που αυτό περιλαμβάνει, δείχνοντας στα κατάλληλα μέλη της `TaskNodes` και των `DataEdges` ή `ControlEdges`, αντίστοιχα. Επιπρόσθετα, δεδομένου ότι οι ροές σχηματοποιούνται ως κατευθυνόμενες ακμές, καθεμιά χαρακτηρίζεται από ακριβώς μία εργασία–αφετηρία και μία εργασία–προορισμό· έτσι, μέλη των υποκλάσεων της `Edges` συνδέονται με μέλη της `TaskNodes` μέσω των ιδιοτήτων `hasSource` και `hasDestination`.

Στο Σχήμα 11β′ η ροή εργασιών του Σχήματος 11α′ αναπαράγεται ως οντολογία. Για λόγους ευκρίνειας, οι λεπτομέρειες εδώ παραλείπονται, δίνοντας έμφαση στα αντίστοιχα μέλη των κλάσεων `TaskNodes`, `DataEdges` και `ControlEdges` και στις μεταξύ τους σχέσεις. Ως σκοπός της ροής εργασιών ορίζεται η "Ασφάλεια Δικτύου" (Network Security) και ως εκκινητής ο ρόλος "Επικεφαλής Αξιωματούχος Ασφάλειας" (Chief Security Officer), με κατάλληλη αναφορά στα αντίστοιχα μέλη της ΟΣΜΠ.

6.2.2 Εκφράσεις και Λογικές Σχέσεις

Προς επίτευξη πλούσιας εκφραστικότητας, δυο χρήσιμα εργαλεία που χρησιμοποιούνται οριζόντια στην παρούσα προσέγγιση για τη λεπτομερή σημασιολογική περιγραφή των εμπλεκόμενων εννοιών είναι οι *εκφράσεις* και οι *λογικές σχέσεις*.

Οι λογικές σχέσεις επιτρέπουν τον ορισμό λογικών δομών μεταξύ ομοειδών εννοιών. Για παράδειγμα, μια εργασία μπορεί να μην ανατίθεται σε ένα μόνο τύπο δράστη· ο ορισμός της μπορεί να περιλαμβάνει ένα σύνολο ετερογενών οντοτήτων που πρέπει από κοινού να αναλάβουν την εκτέλεσή της (σχέση σύζευξης – AND), ένα σύνολο εναλλακτικών δραστών συνδεόμενων με σχέση περιεκτικής διάζευξης (OR) ή αποκλειστικής διάζευξης (XOR), ή συνδυασμούς των παραπάνω. Μια λογική σχέση ορίζεται ως εξής:

Ορισμός 2 Έστω $\mathcal{F}$ η κλάση όλων των μεθόδων επί ενός συνόλου S, τέτοιων ώστε κάθε $\phi_i(V) \in \mathcal{F}$ να αποτελεί έναν καλώς ορισμένο τύπο αποτελούμενο από τους ν-αδικούς τελεστές AND, OR και XOR, το μοναδιαίο τελεστή NOT, και ένα σύνολο μεταβλητών V· ως *λογική σχέση* ορίζεται μια λογική δομή $\phi(S')$, τέτοια ώστε $\phi \in \mathcal{F}$ και $S' \subseteq S$.

Οι έντονες γραμμές στο Σχήμα 12α′ υποδηλώνουν τη δυνατότητα χρήσης λογικών σχέσεων για το σχηματισμό δομών μεταξύ μελών των δεικνυόμενων κλάσεων, οι οποίες υλοποιούνται μέσω της κλάσης `LogicalRelations` (Σχήμα 12β′). Τα μέλη των υποκλάσεων της τελευταίας, `ANDRelations`, `ORRelations` και `XORRelations`, εκπροσωπούν τους τελεστές AND, OR και XOR. Τα οντολογικά μέλη που συμμετέχουν σε λογικές σχέσεις, συμπεριλαμβανομένων και άλλων λογικών σχέσεων, υποδεικνύονται μέσω των ιδιοτήτων `posRelatedTo` και `negRelatedTo`, με την τελευταία να μοντελοποιεί τη χρήση του αρνητι-

κού τελεστή (NOT).

Οι εκφράσεις, από την άλλη, καθιστούν δυνατό τον ορισμό συνθηκών (π.χ., πλαισίου) και ποικίλων περιορισμών πάνω σε έννοιες (π.χ., με βάση κάποιες ιδιότητές τους). Κάθε έκφραση είναι είτε μια τριαδική σχέση, η οποία θέτει μια τιμή σε μια οντότητα/έννοια μέσω ενός τελεστή, είτε μια λογική δομή αποτελούμενη από τέτοιες σχέσεις.

Ορισμός 3 Ως *ατομική έκφραση* ορίζεται μια τριάδα ⟨*exprSubject*, *operator*, *exprValue*⟩, τέτοια ώστε: το *exprSubject* αντανακλά την οντότητα/έννοια αναφοράς· *operator* ∈ *Operators*, όπου *Operators* είναι ένα σύνολο τελεστών, όπως είναι για παράδειγμα οι `equals`, `greaterThan`, `sameAs`, κλπ.· το *exprValue* αντιπροσωπεύει την τιμή που τίθεται στο *exprSubject*. Μια *έκφραση* είναι είτε μια ατομική έκφραση είτε μια λογική σχέση ατομικών εκφράσεων.

Οντολογικά, οι εκφράσεις μοντελοποιούνται με τη βοήθεια των κλάσεων `Expressions` και `LogicalRelations`· για την ακρίβεια, τα μέλη της πρώτης διατυπώνουν ατομικές εκφράσεις, ενώ η δεύτερη επιτρέπει το σχηματισμό σύνθετων εκφράσεων. Ακολουθώντας τον Ορισμό 3, για την κλάση `Expressions` ορίζονται οι κατάλληλες ιδιότητες για την υπόδειξη του υποκειμένου (`hasExprSubject`), του τελεστή (`hasOperator`) και της αποδιδόμενης τιμής (`hasExprValue`). Οι τελεστές ορίζονται σημασιολογικά ως μέλη της κλάσης `Operators`, ενώ το υποκείμενο και η τιμή κάθε έκφρασης μπορεί να είναι μέλη τόσο της ΟΜΡΕ όσο και της ΟΣΜΠ. Βέβαια, υπάρχει και η περίπτωση η τιμή μιας έκφρασης να μην ορίζεται οντολογικά, να έχει, δηλαδή, τη μορφή απλής συμβολοσειράς, οπότε για την ανάθεσή της χρησιμοποιείται αντί της `hasExprValue` η ιδιότητα τύπου δεδομένων `hasExprStringValue`.

6.2.3 Μεταβλητές Ροής Εργασιών

Η προτεινόμενη προσέγγιση εισάγει επιπρόσθετα τη χρήση των λεγόμενων *μεταβλητών ροής εργασιών*, οι οποίες προωθούν περαιτέρω τη διατύπωση σύνθετων περιορισμών. Οι μεταβλητές ροής εργασιών παρέχουν σημασιολογικούς "δείκτες" οι οποίοι λειτουργούν ως αφαιρετικές αναπαραστάσεις των υποκείμενων οντοτήτων, επιτρέποντας την περιγραφή δυναμικών σχέσεων και εξαρτήσεων. Ένα παράδειγμα τέτοιων περιορισμών που μπορεί να οριστεί με χρήση κατάλληλων μεταβλητών είναι ότι "ο δράστης της εργασίας t_B πρέπει να είναι ο ίδιος με το δράστη της t_A", οποιοιδήποτε και αν ορίζονται ως δράστες των δύο εργασιών κατά το σχεδιασμό της ροής εργασιών (βλ. το παράδειγμα στην Ενότητα 6.4.1), κάτι που μπορεί να διασφαλιστεί μόνο σε πραγματικό χρόνο, κατά την εκτέλεσης της ροής εργασιών.

Οι μεταβλητές ροής εργασιών ομαδοποιούνται από την κλάση `WFVariables`. Βασικά μέλη της είναι τα `thisInstanceInitiator` και `thisInstancePurpose`, τα οποία αναφέρονται στον τελικό εκκινητή και δηλωμένο σκοπό του εκάστοτε ΣΡΕ, τα `thisTaskActor` και `thisTaskAsset`, που χρησιμοποιούνται για να υποδείξουν το δράστη και το αντικείμενο

επενέργειας της υπό εξέταση εργασίας, και το `this`, που αποτελεί αναφορά στη συγκεκριμένη οντότητα που αφορά ο εν λόγω περιορισμός. Επιπλέον, οι υποκλάσεις `ActorWFVariables` και `AssetWFVariables` περιλαμβάνουν μεταβλητές για την αναφορά στους δράστες και τα αντικείμενα επενέργειας όλων των εργασιών μιας ροής. Έτσι, κάθε φορά που μια εργασία προστίθεται στο MPE, δημιουργούνται τα αντίστοιχα μέλη των `ActorWFVariables` και `AssetWFVariables`, ώστε οι δράστες και τα αντικείμενα επενέργειάς της να μπορούν να συμπεριληφθούν ως τέτοια σε εκφράσεις περιορισμών.

6.3 Οντότητες Ροής Εργασιών

Όπως έχει ήδη αναφερθεί στην Ενότητα 6.2.1, τα βασικά δομικά συστατικά κάθε εργασίας είναι ο δράστης (ή δράστες), η λειτουργία και το αντικείμενο (ή αντικείμενα) επενέργειας που τη χαρακτηρίζουν, ενώ, σε ό,τι αφορά τον ορισμό των ακμών, απαραίτητος είναι, μεταξύ άλλων, ο προσδιορισμός της πληροφορίας τη μεταφορά της οποίας υποδηλώνει η εκάστοτε ροή, είτε πρόκειται για παραμέτρους ελέγχου είτε για δεδομένα που καθίστανται διαθέσιμα με συνεχή τρόπο τροφοδοτώντας τις υπό εκτέλεση εργασίες. Προκειμένου να αποτυπωθούν επαρκώς οι βασικές όψεις των ροών εργασιών (βλ. Ενότητα 3.3), εισάγεται η έννοια της *οντότητας ροής εργασιών (ΟντΡΕ)*, η οποία χρησιμοποιείται για την ολιστική και ενδελεχή μοντελοποίηση των παραπάνω στοιχείων. Μια ΟντΡΕ δύναται να περιγράψει την υποκείμενη οντότητα είτε με συγκεκριμένο (concrete) τρόπο (π.χ., υποδεικνύοντας ένα συγκεκριμένο άτομο μέσω του ονόματός του) είτε σημασιολογικά (π.χ., μέσω κάποιου ρόλου οριζόμενου στο Σημασιολογικό Μοντέλο Πληροφοριών), στην τελευταία περίπτωση πιθανώς με τη συνοδεία περιορισμών.

Όπως θα φανεί παρακάτω, οι δράστες, τα αντικείμενα επενέργειας, οι λειτουργίες και οι οντότητες πληροφορίας αναπαρίστανται με σχεδόν πανομοιότυπο τρόπο, συνεπώς οι αντίστοιχες κλάσεις της OMPE (Σχήμα 12α′) είναι όλες υποκλάσεις της `EnhancedEntities`. Κάθε μέλος των υποκλάσεων αυτών υποδεικνύει το σημασιολογικό τύπο της ΟντΡΕ και τους τυχόν περιορισμούς που την περιγράφουν με περισσότερη λεπτομέρεια μέσω των ιδιοτήτων αντικειμένου `refersToConcept` και `hasConstraint`, αντίστοιχα, ενώ, αν η ΟντΡΕ ορίζεται σε συγκεκριμένο επίπεδο, χρησιμοποιείται αντ′ αυτών η ιδιότητα τύπου δεδομένου `refersToConcreteEntity`.

6.3.1 Οντότητες Δραστών και Αντικειμένων Επενέργειας

Οι οντότητες δραστών υλοποιούν στην ουσία την όψη των πόρων (resource perspective) σε ένα MPE, εκφράζουν, δηλαδή, κάθε είδους οντότητα "ικανή να προσφέρει έργο" [143], υπονοώντας με το τελευταίο τόσο την εκτέλεση επιμέρους εργασιών όσο και την εκκίνηση της ροής εργασιών συνολικά. Αντίστροφα, οι οντότητες αντικειμένων επενέργειας εκπροσωπούν τους αποδέκτες της εκτέλεσης των εργασιών, τις οντότητες, δηλαδή,

τις οποίες οι εργασίες προσπελαύνουν, επεξεργάζονται ή τροποποιούν προκειμένου να επιτευχθούν οι αντίστοιχες λειτουργικότητες.

Οι οντότητες δραστών και αντικειμένων επενέργειας ορίζονται με παρόμοιο τρόπο, είτε σε συγκεκριμένο (concrete) είτε σε αφηρημένο (abstract) επίπεδο αναπαράστασης. Στη δεύτερη περίπτωση, η χρήση περιορισμών μπορεί να επιστρατευθεί με σκοπό τον ακριβέστερο προσδιορισμό των αφηρημένων οντοτήτων, με βάση ποικίλα χαρακτηριστικά τους πέραν της σημασιολογικής ταξινόμησής τους στο Σημασιολογικό Μοντέλο Πληροφοριών, όπως είναι, για παράδειγμα, οι διάφορες ιδιότητες (attributes), ικανότητες, σχέσεις με άλλες οντότητες, ιστορικό εκτέλεσης, κλπ..

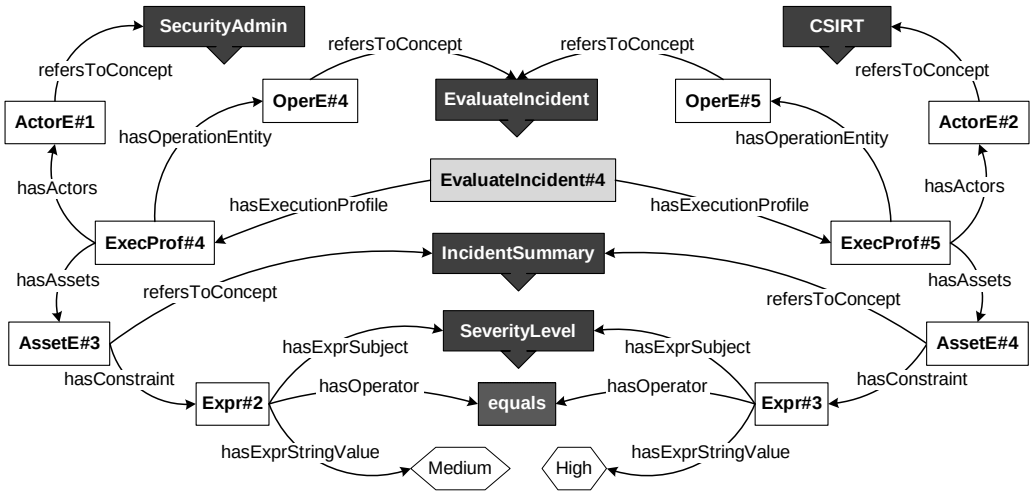
Ορισμός 4 Μια *οντότητα δράστη* ορίζεται ως $\langle conActor \mid abActor, actorConstr \rangle$, όπου: $conActor \in U \cup OpC \cup Org \cup M$ δηλώνει ένα δράστη ορισμένο σε συγκεκριμένο επίπεδο· $abActor \in R \cup OpCT \cup OrgT \cup MT$ δηλώνει ένα δράστη ορισμένο σε αφηρημένο επίπεδο· *actorConstr* είναι μια έκφραση η οποία διατυπώνει συγκεκριμένους περιορισμούς που ο (αφηρημένος) δράστης πρέπει να ικανοποιεί.

Ορισμός 5 Μια *οντότητα αντικειμένου επενέργειας* ορίζεται ως $\langle conAsset \mid abAsset, assetConstr \rangle$, όπου: $conAsset \in D \cup U \cup OpC \cup Org \cup M$ δηλώνει ένα αντικείμενο επενέργειας το οποίο περιγράφεται ως συγκεκριμένη οντότητα· $abAsset \in DT \cup R \cup OpCT \cup OrgT \cup MT$ δηλώνει ένα αντικείμενο επενέργειας εκπεφρασμένο σε αφηρημένο επίπεδο· *assetConstr* είναι μια έκφραση η οποία διατυπώνει συγκεκριμένους περιορισμούς που το (αφηρημένος) αντικείμενο επενέργειας πρέπει να ικανοποιεί.

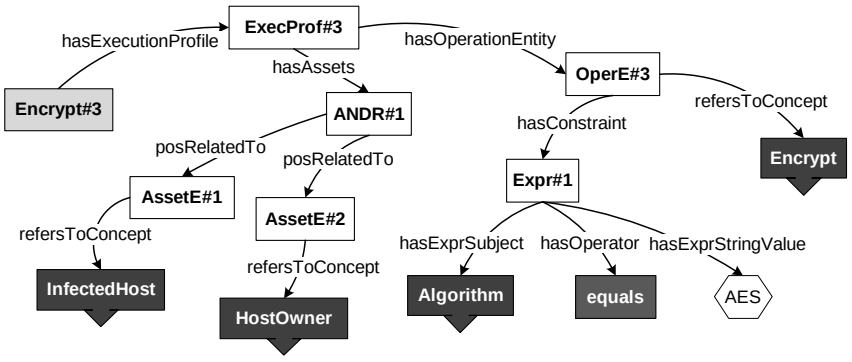
Όλες οι οντότητες δραστών και αντικειμένων επενέργειας σε ένα MPE *WM* συναπαρτίζουν, αντίστοιχα, τα σύνολα $Actors_{WM}$ και $Assets_{WM}$. Όπως προκύπτει από τα παραπάνω, οι εκκινητές μιας ροής εργασιών αποτελούν επίσης οντότητες δραστών, με άλλα λόγια, $Init_{WM} \subseteq Actors_{WM}$, οι οποίες, ωστόσο, αναφέρονται αποκλειστικά σε ανθρώπους. Αναφορικά με το παράδειγμα του παρόντος κεφαλαίου, αυτό απεικονίζεται στο Σχήμα 11β', όπου το μέλος της `ActorEntities` `ActorE#15` υποδεικνύει το ρόλο που ο εκκινητής της ροής εργασιών θα πρέπει να κατέχει.

Στις εκφράσεις που συμμετέχουν στη διατύπωση περιορισμών, το *exprSubject* μπορεί να αναφέρεται σε οποιοδήποτε στοιχείο χαρακτηρίζει την αντίστοιχη αφηρημένη οντότητα. Από οντολογική σκοπιά, τα στοιχεία αυτά μπορούν να περιλαμβάνουν μέλη διαφόρων κλάσεων της OMPE και της ΟΣΜΠ, ιδιαιτέρως δε των κλάσεων `Attributes`, `WFVariables`, καθώς και μέλη που ορίζουν επιμέρους τμήματα της αντίστοιχης αφηρημένης έννοιας, οριζόμενα ως σημασιολογικοί "απόγονοί" της μέσω της ιδιότητας `isPartOf`. Το *exprValue*, από την άλλη, μπορεί να αναφέρεται είτε σε αυθαίρετες τιμές (π.χ., έναν αριθμό) είτε σε οντολογικά ορισμένα στοιχεία, όπως, για παράδειγμα, σε ένα μέλος της `WFVariables`, ή σε μια οντολογική οντότητα η οποία αποτελεί την τιμή που αποδίδεται σε κάποιο μέλος της κλάσης `Attributes`, που λειτουργεί, στην περίπτωση αυτή, ως *exprSubject*.

Το Σχήμα 13α′ δείχνει τις οντότητες δραστών και αντικειμένων επενέργειας που σχετίζονται με την εργασία *EvaluateIncident* (βλ. Σχήμα 11α′) ορισμένες οντολογικά ως `ActorE#1`, `ActorE#2`, `AssetE#3` and `AssetE#4`. Τα δύο τελευταία μέλη αναφέρονται στον ίδιο τύπο δεδομένων, οπότε, και στις δύο περιπτώσεις, το αντικείμενο επενέργειας είναι μια σύνοψη συμβάντος (`IncidentSummary`). Ωστόσο, οι περιορισμοί που περιγράφονται από τα μέλη της `Expressions` `Expr#2` και `Expr#3` τα διαφοροποιούν με βάση την τιμή του πεδίου `Severity-Level` (το οποίο ορίζεται στο Σημασιολογικό Μοντέλο Πληροφοριών ως πεδίο του τύπου δεδομένου `IncidentSummary` μέσω σχέσης `isPartOf`), δηλώνοντας ότι η τιμή αυτή επηρεάζει τον τρόπο που η εργασία τελικά θα εκτελεστεί (δηλ., με διαφορετικό δράστη, βλ. Ενότητα 6.4).



(α′)



(β′)

Σχήμα 13: Οντολογική αναπαράσταση των εργασιών *EvaluateIncident* (a) και *Encrypt* (b).

6.3.2 Οντότητες Λειτουργιών

Το έργο που επιτελείται σε κάθε βήμα της ροής εργασιών περιγράφεται από την αντίστοιχη λειτουργία, η οποία ορίζεται σημασιολογικά με τη βοήθεια της κλάσης `Operations` της ΟΣΜΠ. Οι οντότητες λειτουργιών ουσιαστικά επεκτείνουν την περιγραφή των

λειτουργιών θέτοντας τιμές σε παραμέτρους (ρυθμίσεις εκτέλεσης) και άλλες ιδιότητές τους, προσφέροντας ακόμα περισσότερες δυνατότητες ελέγχου στο επίπεδο της λειτουργίας καθεαυτής. Στην OMPE ορίζονται ως μέλη της κλάσης `OperationEntities`.

Ορισμός 6 Μια οντότητα λειτουργίας ορίζεται ως $\langle op, operConstr \rangle$, όπου $op \in Op$ είναι η λειτουργία, όπως αυτή ορίζεται στην ΟΣΜΠ, και *operConstr* είναι μια έκφραση που θέτει τιμές στις παραμέτρους της *op* ή/και περιγράφει επιθυμητές ιδιότητες.

Για παράδειγμα, στο Σχήμα 13β′, το μέλος της `OperationEntities` `OperE#3`, που σχετίζεται με την εργασία *Encrypt*, υποδεικνύει, πέρα από την αντίστοιχη λειτουργία της ΟΣΜΠ, και τον αλγόριθμο κρυπτογράφησης "AES" ως την τιμή της ιδιότητας `Algorithm` της τελευταίας, με τη βοήθεια της έκφρασης `Expr#1`.

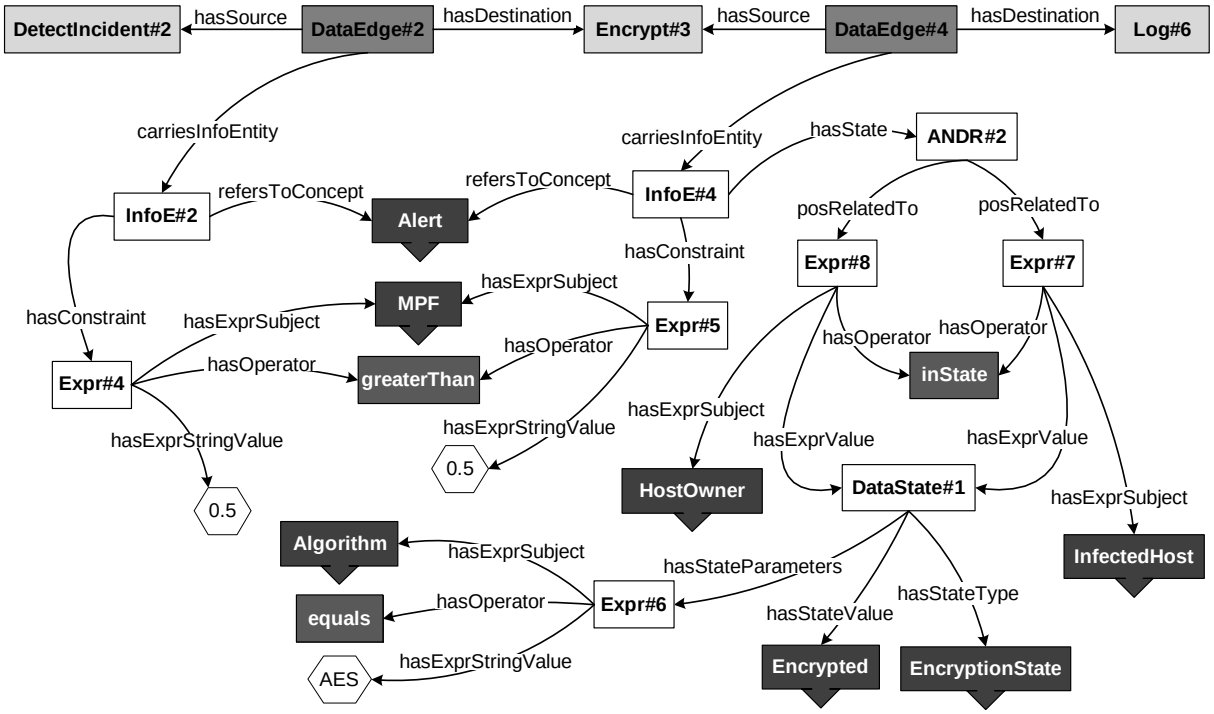
6.3.3 Οντότητες Πληροφοριών

Οι οντότητες πληροφοριών χρησιμοποιούνται στον ορισμό των ροών (βλ. Ενότητα 6.5), εμπλουτίζοντας την περιγραφή των μεταφερόμενων δεδομένων με περιορισμούς και ιδιότητες κατάστασης. Οι οντότητες πληροφοριών που εμφανίζονται σε ένα MPE *WM* συναποτελούν το σύνολο $Info_{WM}$ και εκπροσωπούνται από τα μέλη της κλάσης `Information-Entities` της OMPE, καθένα από τα οποία συνδέεται με ένα μέλος της κλάσης `DataTypes` της ΟΣΜΠ:

Ορισμός 7 Μια *οντότητα πληροφορίας* ορίζεται ως μια τριάδα $\langle dt, ds, dataConstr \rangle$, όπου: $dt \in DT$ είναι ο σχετικός τύπος δεδομένου· $ds \in DS_{WM}$, όπου DS_{WM} είναι το σύνολο όλων των καταστάσεων δεδομένων στο MPE· και *dataConstr* είναι μια έκφραση που ορίζει περιορισμούς στις τιμές των σχετικών ιδιοτήτων δεδομένων.

Η χρήση περιορισμών καθιστά δυνατή την υπό συνθήκη δρομολόγηση της εκάστοτε πληροφορίας με βάση τις ιδιότητές της. Για παράδειγμα, η έκφραση `Expr#4` στο Σχήμα 14 υποδηλώνει ότι οι ειδοποιήσεις που προέρχονται από την εργασία *DetectIncident* δε διοχετεύονται όλες στην εργασία *Encrypt*, παρά μόνο εκείνες στις οποίες το πεδίο Malware Probability Factor (MPF) λαμβάνει συγκεκριμένες τιμές (`MPF` $\xrightarrow{\texttt{isPartOf}}$ `Alert`, σύμφωνα με την ΟΣΜΠ).

Οι ιδιότητες κατάστασης δεδομένων, από την άλλη, χρησιμεύουν ως δείκτες της επίδρασης της εκτέλεσης προηγούμενων στο μονοπάτι εργασιών πάνω σε κάθε οντότητα πληροφορίας που ανταλλάσσεται, σε αντίθεση με τα εγγενή χαρακτηριστικά της, τα οποία προσδιορίζονται με τη χρήση περιορισμών επί των τιμών ιδιοτήτων της. Η κατάσταση των δεδομένων δεν καθορίζεται από το σχεδιαστή της ροής εργασιών, παρά εξάγεται από το σύστημα με βάση το μονοπάτι εκτέλεσης που τα εκάστοτε δεδομένα θα έχουν διασχίσει ευρισκόμενα σε μια συγκεκριμένη ακμή.



Σχήμα 14: Οι οντότητες πληροφορίας κατά μήκος του μονοπατιού *DetectIncident* ⟶ *Encrypt* ⟶ *Log*.

Κάθε ιδιότητα κατάστασης χαρακτηρίζεται από έναν *τύπο* και μια *τιμή* και, σε κάποιες περιπτώσεις, από επιπλέον παραμέτρους. Οι τύποι και οι τιμές κατάστασης περιλαμβάνονται στο Σημασιολογικό Μοντέλο Πληροφοριών ως τα σύνολα ST and SV και, αντίστοιχα, ως μέλη των οντολογικών κλάσεων της ΟΣΜΠ `StateTypes` and `StateValues`.

Ορισμός 8 Μια *κατάσταση δεδομένων* ορίζεται ως μια τριάδα $\langle st, sv, stateParameters \rangle$, όπου: $st \in ST$ είναι ένας τύπος κατάστασης, $sv \in SV$ είναι η τιμή που χαρακτηρίζει τα δεδομένα ως προς το συγκεκριμένο τύπο κατάστασης, και *stateParameters* είναι μια έκφραση που χρησιμοποιείται για την περιγραφή της εν λόγω κατάστασης με περισσότερη λεπτομέρεια, δίνοντας τιμές στις ιδιότητες που ορίζονται για δεδομένο τύπο και τιμή κατάστασης.

Οντολογικά, κάθε κατάσταση δεδομένων $ds \in DS_{WM}$ αναπαρίσταται ως μέλος της κλάσης `DataStates` της OMPE. Ο τύπος, η τιμή και οι παράμετροί της υποδεικνύονται από τις ιδιότητες `hasStateType`, `hasStateValue` and `hasStateParameters` (Σχήμα 12α'), ενώ η κατάσταση καθαυτή συνδέεται με το αντίστοιχο μέλος της `InformationEntities` μέσω της ιδιότητας `hasState`. Παρ' όλα αυτά, ενδέχεται κάποια κατάσταση να χαρακτηρίζει επιμέρους τμήματα της θεωρούμενης οντότητας πληροφορίας και όχι την οντότητα στο σύνολό της. Σε αυτή την περίπτωση, η ιδιότητα `hasState` δείχνει σε μια έκφραση, στην οποία το *exprSubject* αναφέρεται στον κατάλληλο τύπο δεδομένου που χαρακτηρίζει το αντίστοιχο τμήμα, το *exprValue* έχει τη μορφή που προδιαγράφεται από τον Ορισμό 8, ενώ ως τελεστής χρησιμοποιείται το μέλος της `Operators` `inState`. Παράδειγμα των παραπάνω απο-

τελεί η οντότητα πληροφορίας `InfoE#4` (Σχήμα 14), η οποία μεταφέρεται από την εργασία *Encrypt* στην εργασία *Log*. Οι εκφράσεις `Expr#7` και `Expr#8`, συνδυαζόμενες στο μέλος της `ANDRelation` `ANDR#2`, χρησιμοποιούνται για να δηλώσουν ότι μόνο τα πεδία με τύπο `InfectedHost` και `HostOwner` της ειδοποίησης είναι κρυπτογραφημένα (τιμή `Encrypted` για την κατάσταση `EncryptionState`).

6.4 Μοντελοποίηση Εργασιών

Μια εργασία αντιστοιχεί σε μια αυτοτελή μονάδα έργου παρεχόμενου στα πλαίσια της εκτέλεσης μιας ροής εργασιών. Θεωρώντας ένα MPE *WM*, οι εργασίες που αυτό περιλαμβάνει σχηματίζουν το σύνολο T_{WM} και ορίζονται οντολογικά ως μέλη της κλάσης `TaskNodes`. Κεντρικό στοιχείο κάθε εργασίας είναι η *λειτουργία* την οποία υλοποιεί, ενώ μπορεί να συμπληρώνεται και από τον ορισμό παραμέτρων, καθώς και από τους σχετικούς δράστες και αντικείμενα επενέργειας. Αντίθετα με άλλες προσεγγίσεις στις οποίες ο ορισμός των εργασιών είναι μάλλον μονοδιάστατος, η προτεινόμενη λύση εισάγει την έννοια του *προφίλ εκτέλεσης* (βλ. Ενότητα 6.4.1), επιτρέποντας, μεταξύ άλλων, την προδιαγραφή παραλλαγών στον τρόπο εκτέλεσης των εργασιών. Μια εργασία χαρακτηρίζεται επιπρόσθετα από μια συγκεκριμένη *συμπεριφορά συγχρονισμού* (βλ. Ενότητα 6.4.2). Συνολικά, ισχύει ο παρακάτω ορισμός:

Ορισμός 9 Μια εργασία $t_i \in T_{WM}$ ορίζεται ως μια πλειάδα $\langle op, EP_i, isDataSync_i, isControlSync_i \rangle$, τέτοια ώστε: $op \in Op$, EP_i είναι ένα σύνολο από προφίλ εκτέλεσης, και $isDataSync_i$, $isControlSync_i$ $\in \{true, false\}$ είναι boolean ιδιότητες οι τιμές των οποίων καθορίζουν τη συμπεριφορά συγχρονισμού της t_i.

6.4.1 Προφίλ Εκτέλεσης

Η εκτέλεσης μιας εργασίας συνεπάγεται ότι ένας ή περισσότεροι δράστες διενεργούν μια λειτουργία επί ενός ή περισσότερων αντικειμένων επενέργειας. Σε αυτή τη βάση, το προφίλ εκτέλεσης ως δομή καλύπτει την ενδεχόμενη ανάγκη για ορισμό εναλλακτικών τρόπων εκτέλεσης μιας εργασίας. Αυτό αφορά ειδικότερα τους εξής δύο άξονες: αφενός τη διαφοροποιημένη εκτέλεση της εργασίας αναλόγως κάποιων *συνθηκών* και, αφετέρου, την αποτύπωση εξαρτήσεων μεταξύ δραστών, αντικειμένων επενέργειας και παραμέτρων λειτουργίας, τον ακριβή, με άλλα λόγια, ορισμό έγκυρων συνδυασμών των παραπάνω στοιχείων. Στην περίπτωση του ορισμού πολλαπλών προφίλ, το ποιό μεταξύ αυτών θα εκτελεστεί τελικά καθορίζεται κατά την εκτέλεση της ροής εργασιών και εξαρτάται από τις συνθήκες πραγματικού χρόνου κάτω από τις οποίες οι συγκεκριμένοι δράστες, τα αντικείμενα επενέργειας και οι παράμετροι λειτουργίας μπορούν να συνδυαστούν για την εκτέλεση της τελευταίας, καθώς και από τη διαθεσιμότητα των εν λόγω οντοτήτων.

Κατά συνέπεια, και σε συνέχεια του Ορισμού 9, κάθε εργασία $t_i \in T_{WM}$ σε ένα MPE *WM* συσχετίζεται με ένα μη κενό σύνολο EP_i από προφίλ εκτέλεσης, καθένα από τα οποία ορίζεται ως εξής:

Ορισμός 10 Ένα *προφίλ εκτέλεσης* $ep_{i,j} \in EP_i$, που συνδέεται με μια εργασία $t_i \in T_{WM}$, είναι μια πλειάδα $\langle \phi(Actors_{WM}), \phi(Assets_{WM}), oe, taskConditions \rangle$, τέτοια ώστε: $\phi(Actors_{WM})$ και $\phi(Assets_{WM})$ είναι λογικές σχέσεις επί των συνόλων των δραστών και των εντικειμένων επενέργειας που ανήκουν στο MPE, *oe* είναι μια οντότητα λειτουργίας, και *taskConditions* είναι μια έκφραση η οποία ορίζει τις συνθήκες που πρέπει να ικανοποιούνται προκειμένου να εκτελεστεί το συγκεκριμένο προφίλ.

Εφόσον μια εργασία μπορεί να περιλαμβάνει πολλαπλούς δράστες, εναλλακτικούς ή συμπληρωματικούς μεταξύ τους, αλλά και περισσότερα του ενός αντικείμενα επενέργειας (επίσης εναλλακτικά ή συμπληρωματικά), κάθε προφίλ εκτέλεσης συνδέεται με λογικές σχέσεις αντίστοιχων οντοτήτων. Από την άλλη, η συσχέτιση με μια οντότητα λειτουργίας είναι, κατά κάποιο τρόπο, πλεονασμός, καθόσον η λειτουργία καθεαυτή ορίζεται μονοσήμαντα στο επίπεδο της εργασίας (βλ. Ορισμό 9) και μόνο οι τιμές των παραμέτρων και των ιδιοτήτων της χρήζουν προσδιορισμού στα πλαίσια του προφίλ εκτέλεσης. Ωστόσο, επελέγη η προσέγγιση αυτή για λόγους πληρότητας στην προδιαγραφή του προφίλ εκτέλεσης και συνοχής στην οντολογική υλοποίηση.

Ο ορισμός ενός προφίλ εκτέλεσης συμπληρώνεται από τις συνθήκες που θα πρέπει να ισχύουν προκειμένου να εκτελεστεί το προφίλ ως έχει. Οι συνθήκες αυτές συνίστανται σε περιορισμούς πραγματικού χρόνου που αφορούν παράγοντες που δεν αποτελούν μέρος της προδιαγραφής της ροής εργασιών (π.χ., εξωγενείς παράμετροι περιβάλλοντος) ή που εκτείνονται πέραν των ορίων της εργασίας και που, συνεπώς, δεν μπορούν να εκφραστούν αποκλειστικά στη βάση των ιδιοτήτων των εμπλεκόμενων οντοτήτων. Οι συνθήκες σε μια εργασία διατυπώνονται, όπως και οι υπόλοιποι τύποι περιορισμών, με χρηση εκφράσεων, οι οποίες μπορεί να αναφέρονται σε διάφορα ετερογενή στοιχεία, όπως τα δεδομένα εισόδου της εργασίας, παράμετροι πλαισίου (context), ή μεταβλητές ροής εργασιών, συμπεριλαμβανομένου του εκκινητή και του υποκείμενου σκοπού.

Όπως γίνεται φανερό από τα παραπάνω, τα προφίλ εκτέλεσης προσφέρουν έναν αποδοτικό μηχανισμό για την ενσωμάτωση πολιτικών ασφάλειας στα MPE. Στην ουσία αντανακλούν δηλώσεις εξουσιοδοτήσεων (authorisation statements), περιγράφοντας υπό συνθήκη παραλλαγές στην εκτέλεση των λειτουργιών, όπου δράστες, αντικείμενα επενέργειας και παράμετροι πραγματικού χρόνου βρίσκονται σε αλληλεξάρτηση. Ο ρόλος των ΟντΡΕ είναι εξίσου σημαντικός σε αυτό το πλαίσιο, καθώς επιτρέπουν την έκφραση περιορισμών βασισμένων στις ιδιότητες των δραστών, των αντικειμένων επενέργειας και της λειτουργίας, ενώ οι μεταβλητές ροής εργασιών και η ξεχωριστή θεώρηση του σκοπού καθιστούν δυνατή την επιβολή Διαχωρισμού Καθηκόντων (Separation of Duty – SoD) και Σύνδεσης Καθηκόντων (Binding of Duty – BoD) [417] και τη συμμόρφωση με τη βασική αρχή

ιδιωτικότητας που επιτάσσει τον προσδιορισμό του σκοπού και τη σε αυτόν δέσμευση [7].

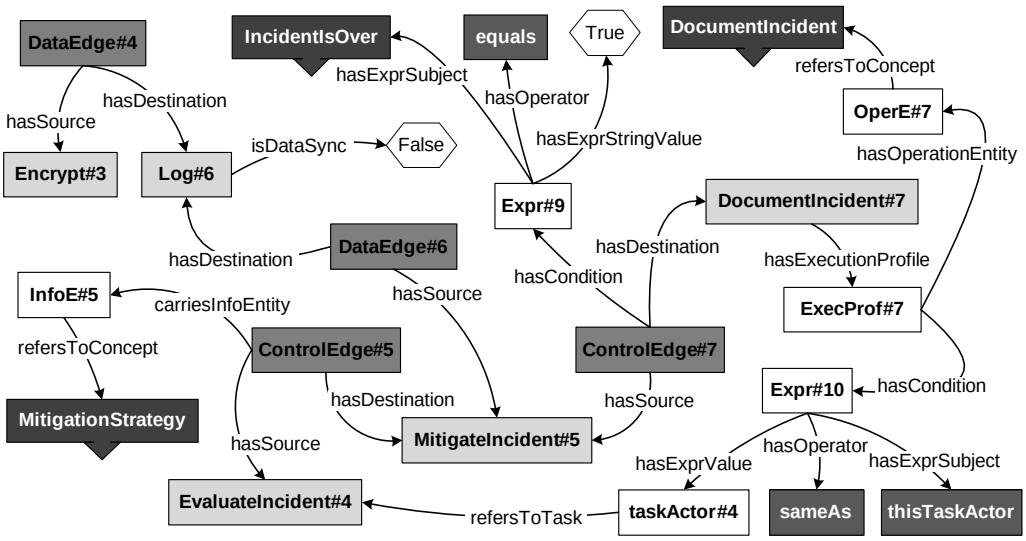
Τα προφίλ εκτέλεσης μοντελοποιούνται ως μέλη της κλάσης `ExecutionProfiles` της OMPE, τα οποία συνδέονται με τα κατάλληλα μέλη των `ActorEntities`, `AssetEntities` and `OperationEntities`, ή, στην περίπτωση δραστών και αντικειμένων επενέργειας, με λογικές σχέσεις αυτών (Σχήμα 12). Οι συνθήκες προσδιορίζονται με τη βοήθεια της ιδιότητας `hasCondition`, η οποία δείχνει σε ένα μέλος της `Expressions` ή της `LogicalRelations`, ενώ η ιδιότητα `hasExecutionProfile` συσχετίζει ένα μέλος της `TaskNodes` με τα μέλη της `ExecutionProfiles` που περιγράφουν τα οριζόμενα ως προφίλ εκτέλεσης αυτής.

Αναφορικά με το θεωρούμενο παράδειγμα ροής εργασιών, τα προφίλ εκτέλεσης `ExecProf#4` και `ExecProf#5` (Σχήμα 13α′) υποδεικνύουν δύο εναλλακτικούς επιτρεπόμενους συνδυασμούς σε σχέση με τους δράστες και τα αντικείμενα επενέργειας της εργασίας *EvaluateIncident*. Έτσι, αν το πεδίο `SeverityLevel` του αντικειμένου επενέργειας (`IncidentSummary`) έχει τιμή "Medium" (`Expr#2`), δράστης μπορεί να είναι οποιοσδήποτε κατέχει το ρόλο `SecurityAdmin`· αν, ωστόσο, το ίδιο πεδίο λάβει την τιμή "High" (`Expr#3`), ως δράστης ορίζεται ο σύνθετος ρόλος `CSIRT`[29]. Επιπρόσθετα, το `ExecProf#7` (Σχήμα 15) αποτελεί παράδειγμα χρήσης μεταβλητών ροής εργασιών για την έκφραση περιορισμών Σύνδεσης Καθηκόντων (BoD): σύμφωνα με τη συνθήκη `Expr#10`, η εργασία *DocumentIncident* πρέπει να εκτελεστεί από τον ίδιο δράστη που έχει προηγουμένως διεκπεραιώσει την εργασία *EvaluateIncident*. Τέλος, το προφίλ εκτέλεσης `ExecProf#3` της εργασίας *Encrypt* στο Σχήμα 13β′ αφορά μια περίπτωση συσχέτισης του ίδιου προφίλ εκτέλεσης με πολλαπλές οντότητες αντικειμένων επενέργειας. Πράγματι, μέσω της ιδιότητας `hasAssets` δείχνει σε ένα μέλος της `ANDRelations` που υποδεικνύει ότι η κρυπτογράφηση επιτελείται σε δύο συγκεκριμένα πεδία της πληροφορίας εισόδου (τύπου `Alert`, όπως φαίνεται από το `InfoE#2` στο Σχήμα 14)

6.4.2 Συμπεριφορά Συγχρονισμού

Σε αντίθεση με τις περισσότερες γλώσσες προδιαγραφής ροών εργασιών, η προτεινόμενη προσέγγιση δεν περιλαμβάνει ειδικούς κόμβους ή πύλες για την προδιαγραφή σύνθετων μοτίβων ροής της εκτέλεσης, όπως είναι, π.χ., ο διαχωρισμός (split) και η σύγκλιση (join) AND, OR ή XOR. Παρ' όλα αυτά, η συμπεριφορά που μπορεί να παρουσιάζει μια εργασία συγκεκριμένα ως προς το συγχρονισμό περιλαμβάνεται στον ορισμό της τελευταίας μέσω δύο ιδιοτήτων boolean (βλ. Ορισμό 9). Οι τιμές των ιδιοτήτων αυτών ενδέχεται είτε να ορίζονται ρητά από το σχεδιαστή της ροής εργασιών είτε να συνάγονται από το σύστημα στη βάση σημασιολογικής πληροφορίας που αφορά την εκάστοτε λειτουργία, και ειδικότερα αμετάβλητες ιδιότητες αυτής (βλ. Ενότητα 4.4). Οντολογικά υλοποιούνται με τη βοήθεια των ιδιοτήτων τύπου δεδομένων `isControlSynch` και `isDataSynch` (Σχήμα 12α′) και υποδεικνύουν το αν μια εργασία που αποτελεί σημείο σύγκλισης πολλαπλών εισερχό-

[29]Computer Security Incident Response Team [428].



Σχήμα 15: Οντολογική αναπαράσταση στοιχείων σχετικών με την εκτέλεση των εργασιών *DocumentIncident* και *Log*.

μενων ροών ελέγχου ή/και δεδομένων συγχρονίζει τις ροές αυτές.

Πιο συγκεκριμένα, στην περίπτωση πολλαπλών εισερχόμενων ροών ελέγχου, αν η τιμή της `isControlSync` είναι "True", η εργασία εκτελείται μόνο όταν όλες οι εργασίες στους ενεργούς εισερχόμενους κλάδους έχουν ολοκληρωθεί, ενώ η τιμή "False" δηλώνει την εκτέλεσή της εκ νέου κάθε φορά που οποιαδήποτε από τις αμέσως προηγούμενες εργασίες ολοκληρώνεται. Παρόμοια, όταν υπάρχουν πολλαπλές εισερχόμενες ροές δεδομένων, η τιμή "False" για την `isDataSync` σημαίνει ότι η εργασία επεξεργάζεται ξεχωριστά κάθε διακριτό εισερχόμενο ρεύμα δεδομένων και διοχετεύει απευθείας μετά το πέρας της επεξεργασίας το αποτέλεσμα στις εργασίες που ακολουθούν. Αντίθετα, η τιμή "True" έχει το νόημα ότι η εργασία περιμένει να λάβει είσοδο διαμέσου όλων των εισερχόμενων ακμών προκειμένου να προχωρήσει στην από κοινού επεξεργασία των αντίστοιχων δεδομένων. Όταν συγκλίνουν τόσο ροές ελέγχου όσο και δεδομένων, θεωρούμε ότι υφίσταται πάντα συγχρονισμός μεταξύ των δύο τύπων ροής, οι τιμές, ωστόσο, των δύο προαναφερθέντων ιδιοτήτων εξακολουθούν να εκφράζουν το κατά πόσο οι ροές του ίδιου τύπου συγχρονίζονται μεταξύ τους. Επιστρέφοντας στο παράδειγμα, η εργασία *Log* λαμβάνει δεδομένα από δύο διαφορετικές πηγές. Εντούτοις, τα δυο ρεύματα δεδομένων καταγράφονται ανεξάρτητα μόλις καταστούν διαθέσιμα και, συνεπώς, δεν απαιτείται συγχρονισμός. Το γεγονός αυτό αποτυπώνεται με τη βοήθεια της ιδιότητας `isDataSync` του μέλους της `TaskNodes Log#6` (Σχήμα 15).

Σημειώνεται ότι τα παραπάνω καλύπτουν κάποιες βασικές περιπτώσεις συγχρονισμού. Φυσικά, επεκτάσεις για την ικανοποίηση πιο σύνθετων απαιτήσεων είναι δυνατές ως μέρος μελλοντικής εργασίας.

6.5 Μοντελοποίηση Ροών

Η ροή ελέγχου και δεδομένων αναπαρίσταται σε ένα MPE μέσω κατευθυνόμενων *ακμών* του αντίστοιχου τύπου και, οντολογικά, ως μέλη των κλάσεων `ControlEdges` και `DataEdges` της OMPE. Οι ακμές ελέγχου και δεδομένων έχουν πανομοιότυπα χαρακτηριστικά: καθεμιά συνδέει δύο εργασίες και υποδηλώνει την κατεύθυνση της ροής, την ανταλλασσόμενη πληροφορία, τις συνθήκες κάτω από τις οποίες η εν λόγω μετάβαση λαμβάνει χώρα, και λοιπές ιδιότητες της ροής. Όπως επισημαίνεται στην Ενότητα 6.2.1, η διάκριση μεταξύ τους προέρχεται από τα σημασιολογικά χαρακτηριστικά των επικοινωνουσών λειτουργιών αναφορικά με τον τρόπο που αυτές λαμβάνουν και καταναλώνουν πληροφορία, οδηγώντας στο σχηματισμό των δύο ξένων μεταξύ τους συνόλων F_C and F_D των ακμών ελέγχου και δεδομένων.

Ορισμός 11 Σε ένα MPE *WM*, κάθε *ακμή* $e_i \in F_C \cup F_D$, με $F_C \cap F_D = \emptyset$, ορίζεται ως μια πλειάδα $\langle t_s, t_d, ie^k, flowCond_i, flowConstr_i \rangle$, όπου: $t_s, t_d \in T_{WM}$ είναι η εργασία–αφετηρία και η εργασία προορισμός, αντίστοιχα· $ie^k \subseteq \mathcal{P}(Info_{WM})$ είναι ένα σύνολο αποτελούμενο από k οντότητες πληροφορίας· τα $flowCond_i$ και $flowConstr_i$ είναι εκφράσεις που περιγράφουν τις συνθήκες και άλλων ειδών περιορισμούς της e_i. Μια ακμή e_i είναι είτε *ακμή ελέγχου* ($e_i \in F_C$) είτε *ακμή δεδομένων* ($e_i \in F_D$).

Οι συνθήκες και οι περιορισμοί ροής ορίζονται μέσω κατάλληλων εκφράσεων. Οι πρώτες είναι ανάλογες των συνθηκών που ορίζονται για τις εργασίες και πρέπει να ισχύουν προκειμένου να πραγματοποιηθεί η υποδηλούμενη μετάβαση μεταξύ των δύο εργασιών, υποστηρίζοντας έτσι, όταν είναι αναγκαίο, την υπό συνθήκη διακλάδωση της ροής ελέγχου ή δεδομένων. Οι περιορισμοί ροής προσδιορίζουν ιδιότητες των υποκείμενων λογικών "καναλιών" που χρησιμοποιούνται για τη σε πραγματικό χρόνο υλοποίηση της μετάβασης. Είναι συγγενείς εννοιολογικά με την ιδιότητα "implementation" που η BPMN ορίζει για τους τύπους εργασιών "Send" και "Receive" [121], με την έννοια ότι δεν περιγράφουν στοιχεία του MPE, αλλά χαμηλότερου επιπέδου χαρακτηριστικά που προσδιορίζουν τεχνικά τον τρόπο αλληλεπίδρασης αυτών. Το *exprSubject* εδώ αναφέρεται σε ιδιότητες που σχετίζονται με τα αντίστοιχα μέλη της κλάσης `DataIO` της ΟΣΜΠ (βλ. Ενότητα 4.4) και που ενδέχεται, συνεπώς, να διαφοροποιούνται ανάλογα με τις λειτουργίες, τον εκάστοτε τύπο δεδομένου και, πρωτευόντως, τον τύπο της ροής: ενώ ιδιότητες όπως το πρωτόκολλο και ο μορφότυπος (format) μπορούν να χαρακτηρίζουν αλληλεπιδράσεις είτε ελέγχου είτε δεδομένων, άλλες, όπως το μέγεθος ενταμιευτή εισόδου, οι ιδιότητες παραθύρου, κ.ά. που συχνά χρειάζεται να οριστούν για λειτουργίες συνεχούς ροής, αποκτούν νόημα μόνο όταν χρησιμοποιούνται για την περιγραφή ροών δεδομένων.

Οι συνθήκες και οι περιορισμοί υλοποιούνται οντολογικά ως εκφράσεις ή λογικές σχέσεις αυτών και συνδέονται με τις αντίστοιχες ακμές μέσω των ιδιοτήτων `hasCondition` και `hasFlowConstraint`. Επιπλέον, η ιδιότητα `carriesInfoEntity` συσχετίζει ένα μέλος της `ControlEdges` ή της `DataEdges` με ένα ή περισσότερα μέλη της `InformationEntities` τα

οποία δηλώνουν την πληροφορία που επικοινωνείται από την εργασία–αφετηρία στην εργασία–προορισμό.

Στα Σχήματα 14 και 15 περιγράφονται κάποιες από τις ροές που εμφανίζονται στη ροή εργασιών του παραδείγματος και οι σχέσεις τους με άλλες οντότητες. Ειδικότερα, αναφορικά με την ακμή ελέγχου `ControlEdge#7`, που συνδέει τις εργασίες *MitigateIncident* και *DocumentIncident* (Σχήμα 15), παρατηρούμε ότι δε σχετίζεται με καμία απολύτως οντότητα πληροφορίας, εκφράζοντας το ότι στη δεδομένη περίπτωση δε μεταφέρεται κάποια παράμετρος ελέγχου, παρά μόνο το νήμα εκτέλεσης. Η ακμή δείχνει, ωστόσο, στη συνθήκη `Expr#9`, δηλώνοντας ότι η εργασία *DocumentIncident* μπορεί να εκτελεστεί μόνο αν το συμβάν ασφάλειας που αφορά δεν υφίσταται πια.

Κεφάλαιο 7

Οδηγίες Συμβατότητας

Η διαδικασία ελέγχου μιας ροής εργασιών καθοδηγείται από ένα σύνολο *Οδηγιών Συμβατότητας*, οι οποίες, προερχόμενες από τη Μηχανή Συμπερασμού, υποδεικνύουν τους όρους υπό τους οποίους η εκάστοτε ροή εργασιών είναι αποδεκτή. Όπως θα περιγραφεί αναλυτικότερα στο Κεφάλαιο 8, προκειμένου να λάβει τις οδηγίες αυτές, ο Αναλυτής Ροών Εργασιών σε πρώτο στάδιο εξάγει από κάθε ροή εργασιών δύο είδη πληροφορίας: τα δυνατά ζεύγη σκοπών-εκκινητών, δηλαδή, όλους τους συνδυασμούς σκοπών και εκκινητών που έχουν προσδιοριστεί από το σχεδιαστή της ροής, και το σύνολο των διμερών συσχετισμών που η ροή εργασιών περιλαμβάνει. Με βάση τα παραπάνω, η Μηχανή Συμπερασμού συμπληρώνει την Οντολογία Μοντέλων Ροών Εργασιών (OMPE) με τις οδηγίες που θα κατευθύνουν την επαλήθευσή της από τον Αναλυτή Ροών Εργασιών.

Με τον όρο *Διμερής Συσχετισμός (ΔιΣ)(Bilateral Association - BA)* περιγράφεται κάθε ζεύγος άμεσα αλληλεπιδρουσών εργασιών της ροής, συμπεριλαμβανομένης της αλληλεπίδρασης καθεαυτής, δηλαδή της ακμής που τις ενώνει. Ο λόγος για τον οποίο η προκαταρκτική επεξεργασία στο επίπεδο της Μηχανή Συμπερασμού πραγματοποιείται λαμβάνοντας υπόψη τους διμερείς συσχετισμούς είναι ότι καθένας τους αποτελεί μια θεμελιώδη *μονάδα ροής*. Αυτό οδηγεί στην εξαγωγή πλουσιότερων σημασιολογικά οδηγιών, εφόσον αυτό που ενδιαφέρει δεν είναι μόνο οι εργασίες ως αυτόνομα εκτελέσιμες οντότητες, αλλά και οι μεταξύ τους σχέσεις. Εξάλλου, η θεώρηση των εργασιών ανά δύο και από κοινού με τους αντίστοιχους συγκεκριμένους συσχετισμούς, αντί, για παράδειγμα, της εξέτασης κάθε εργασίας ξεχωριστά, μειώνει σημαντικά τον αριθμό των προκυπτουσών οδηγιών και, ως εκ τούτου, τη συνολική πολυπλοκότητα.

Το πρώτο μέρος του παρόντος κεφαλαίου παρουσιάζει τις οδηγίες συμβατότητας, οι οποίες, βασισμένες στους κεντρικούς άξονες επαλήθευσης ροών εργασιών, όπως αυτοί καταγράφηκαν στην Ενότητα 5.3, κωδικοποιούν τις συγκεκριμένες απαιτήσεις ιδιωτικότητας που η ροή εργασιών πρέπει να ικανοποιεί. Στο δεύτερο μέρος περιγράφεται η οντολογική υλοποίηση των διαφόρων τύπων οδηγιών.

7.1 Οδηγίες Συμβατότητας

Οι διαφορετικοί τύποι οδηγιών συμβατότητας που θεωρήθηκαν στα πλαίσια της διατριβής περιγράφονται στις ενότητες που ακολουθούν, ενώ ο Πίνακας 16 δείχνει την αντιστοιχία μεταξύ των τύπων οδηγιών και των τεχνικών απαιτήσεων συμβατότητας που καλούνται να καλύψουν, όπως αυτές καταγράφηκαν στην Ενότητα 5.3.

		Οδηγία Εγκυρότητας Διμερούς Συσχετισμού	Οδηγία Απαίτησης εισόδου	Οδηγία Απαίτησης Εξόδου	Οδηγία Απαίτησης Εκτέλεσης	Οδηγία Απαγόρευσης Εκτέλεσης	Οδηγία Απαγόρευσης Ροής
R1	Εγκυρότητα εργασίας - ροής (συμπ. σκοπού & εκκινητή)	X					
R2	Απαίτηση εισόδου		X				
R3	Προέλευση δεδομένων				X		
R4	Συμπληρωματική προ-επεξεργασία				X		
R5	Απαίτηση κατάστασης δεδομένων	X					
R6	Εκτέλεση αμέσως πριν				X		
R7	Συμπληρωματική εκτέλεση πριν				X		
R8	Άμεση μετα-επεξεργασία	X					
R9	Συμπληρωματική άμεση μετα-επεξεργασία			X			
R10	Συμπληρωματική μετα-επεξεργασία				X		
R11	Εκτέλεση αμέσως μετά				X		
R12	Συμπληρωματική εκτέλεση μετά				X		
R13	Συμπληρωματική παράλληλη εκτέλεση				X		
R14	Συμπληρωματική παράλληλη επεξεργασία				X		
R15	Παρουσία οπουδήποτε				X		
R16	Απαγόρευση εκτέλεσης					X	
R17	Απαγόρευση ροής						X

Σχήμα 16: Αντιστοίχιση οδηγιών συμβατότητας και απαιτήσεων συμβατότητας.

7.1.1 Οδηγία Εγκυρότητας Διμερούς Συσχετισμού

Κάθε *Οδηγία Εγκυρότητας Διμερούς Συσχετισμού (ΟΕΔιΣ) (Bilateral Validity Directive – BVD)* αναφέρεται σε ένα ΔιΣ στο σύνολό του, υποδεικνύοντας αφενός έναν έγκυρο συνδυασμό δράστη–λειτουργίας–αντικειμένου επενέργειας για καθεμιά από τις εμπλεκόμενες εργασίες, και αφετέρου μια έγκυρη συσχέτιση μεταξύ τους. Η τελευταία, στην απλή περίπτωση, περιλαμβάνει τον ορισμό της ακμής που ενώνει τις δυο εργασίες (μεταφερόμενες οντότητες πληροφορίας, συνθήκες, κλπ.), ο οποίος μπορεί να συμπίπτει ή όχι με τον αρχικά προσδιορισμένο από το σχεδιαστή της ροής, ενώ σε κάποια πιο σύνθετη δύναται να προδιαγράφει επιπλέον την παρεμβολή ενός ή περισσότερων εργασιών, απαραίτητων για τη σύννομη ανταλλαγή δεδομένων μεταξύ των αρχικών εργασιών (π.χ., κάποια εργασία κρυπτογράφησης ή άλλου είδους μετασχηματισμού).

Για ένα δεδομένο ΔιΣ οι αντίστοιχες ΟΕΔιΣ είναι πρακτικά τόσες όσοι είναι οι διαφορετικοί επιτρεπτοί συνδυασμοί, αν υπάρχουν, που περιλαμβάνουν έννοιες–"φύλλα" (όπου

γίνεται αναφορά σε έννοιες) σε σχέση με τους οριζόμενους από το σχεδιαστή δράστες, λειτουργίες και αντικείμενα επενέργειας. Αν, από την άλλη, για οποιαδήποτε από τις δυο εργασίες δεν μπορεί να συναχθεί κάποιος έγκυρος συνδυασμός, δεν προκύπτει ΟΕΔιΣ για τον αντίστοιχο ΔιΣ.

Κάθε ΟΕΔιΣ, πέρα από την έγκυρη προδιαγραφή των εμπλεκόμενων εργασιών καθεαυτή, συνοδεύεται προαιρετικά από κάποια συνθήκη πλαισίου, υπό την οποία η αντίστοιχη προδιαγραφή θεωρείται αποδεκτή. Μπορεί, επίσης, να συμπληρώνεται από τον ορισμός προ-υποθέσεων ή/και μετα-υποθέσεων, υποδηλώνοντας ότι η συγκεκριμένη οδηγία είναι σε ισχύ μόνο αν κάποιες άλλες εργασίες προηγούνται ή έπονται, αντίστοιχα, του ΔιΣ[30].

Επιπρόσθετα, κάθε τέτοια οδηγία περιλαμβάνει αναφορά σε ένα ακριβώς ζεύγος εκκινητή–σκοπού, συνδέοντας την ισχύ της με τις συγκεκριμένες οντότητες. Φυσικά, οι ίδιες έγκυρες προδιαγραφές μπορούν να ισχύουν για περισσότερα από ένα τέτοια ζεύγη. Ο λόγος που επελέγη αυτή η προσέγγιση είναι η μεγαλύτερη ευελιξία αναφορικά και με τα υπόλοιπα είδη οδηγιών. Πράγματι, καθένα από αυτά σχετίζεται υποχρεωτικά με μία ή περισσότερες ΟΕΔιΣ, επιτρέποντας τη διαφοροποίηση λοιπών απαιτήσεων και απαγορεύσεων με βάση τον τρόπο εκτέλεσης κάθε εργασίας αλλά και, περαιτέρω, τους εκκινητές της ροής και τους σκοπούς που αυτή εξυπηρετεί. Έτσι, για παράδειγμα, η εργασία της αξιολόγησης κάποιων δεδομένων που αφορούν στην πιστοληπτική ικανότητα των πελατών μιας τράπεζας επιτρέπεται να εκτελεστεί από δύο διαφορετικούς ρόλους, τον επικεφαλής αλλά και τον απλό υπάλληλο του αντίστοιχου τμήματος, με την απαίτηση, ωστόσο, μόνο στη δεύτερη περίπτωση να έχει προηγηθεί έγκριση από τον πρώτο. Αντίστοιχα, η συλλογή κάποιων δεδομένων μπορεί μεν να επιτρέπεται να εκτελεστεί από τον ίδιο δράστη, μέσω της ίδιας λειτουργία και πάνω στα ίδια ακριβώς αντικείμενα επενέργειας, για τους σκοπούς είτε της προστασίας ενός τηλεπικοινωνιακού δικτύου παρόχου είτε της τιμολόγησης των υπηρεσιών, μόνο όμως στην πρώτη περίπτωση να απαιτείται η ρητή συναίνεση του πελάτη.

7.1.2 Οδηγία Απαίτησης Εισόδου

Μια *Οδηγία Απαίτησης Εισόδου (ΟΑΕισ) (Input Requirement Directive – IRD)* υποδεικνύει ότι κάποια εργασία, αν και έγκυρα ορισμένη αφεαυτής, χρειάζεται να λάβει κάποια επιπλέον δεδομένα ως είσοδο. Συνδέεται με μια ΟΕΔιΣ, δείχνοντας επιπλέον στη μέσα σε αυτή ορισμένη εργασία που πρέπει να λάβει τα δεδομένα, τα οποία δεν είναι ήδη παρόντα στον έγκυρο ΔιΣ στον οποίο αναφέρεται. Έτσι καθίσταται δυνατή, όπως προαναφέρθηκε, η διαφοροποίηση της ΟΑΕισ στη βάση της έγκυρης προδιαγραφής κάθε εργασίας.

Μια ΟΑΕισ εμπεριέχει τα δεδομένα εισόδου που πρέπει να παρασχεθούν, υποδει-

[30]Για την ακρίβεια, μια εργασία προηγείται ή έπεται ενός ΔιΣ συνολικά, αν προηγείται ή έπεται τουλάχιστον μιας εργασίας του ΔιΣ. Στα υπόλοιπα είδη οδηγιών μια τέτοια παραδοχή δεν είναι απαραίτητη, καθώς η καθεμιά από αυτές αναφέρεται σε συγκεκριμένη εργασία σε ένα ΔιΣ.

κνύοντας, αν χρειάζεται, και την εργασία ή δομή εργασιών από τις οποίες τα δεδομένα αυτά πρέπει να προέρχονται. Και εδώ είναι δυνατός ο ορισμός συνθηκών πλαισίου, προ-υποθέσεων και μετα-υποθέσεων. Επιπλέον ιδιότητες που εξυπηρετούν την ορθή εφαρμογή της οδηγίας, όπως το αν πρόκειται για περίπτωση *σύνδεσης μονοπατιού* ή *άμεσης σύνδεσης* (βλ. Ενότητα 5.3.3), προσδιορίζονται μέσω του κατάλληλου *προφίλ συμβατότητας*.

7.1.3 Οδηγία Απαίτησης Εξόδου

Παρόμοια, η *Οδηγία Απαίτησης Εξόδου (ΟΑΕξ) (Output Requirement Directive – ORD)* ορίζει, σχετιζόμενη με μια ΟΕΔιΣ, ότι κάποια από τις εμπλεκόμενες εργασίες πρέπει να παράσχει τα δεδομένα που παράγει ή μέρος τους σε κάποια άλλη εργασία. Έτσι, προσδιορίζει τα δεδομένα που πρέπει να διατεθούν και τη δομή εργασιών που πρέπει να τα λάβει (σε αντίθεση με μια ΟΑΕισ, το τελευταίο εδώ είναι υποχρεωτικό), ενώ μπορεί επίσης να συνοδεύεται από συνθήκες πλαισίου, προ-υποθέσεις και μετα-υποθέσεις. Και πάλι, η έννοια του προφίλ συμβατότητας χρησιμοποιείται για να δηλώσει τις υποπεριπτώσεις μιας ΟΑΕξ, που μπορεί επιπρόσθετα να είναι *ανασταλτική* ή *συνδυαστική* (βλ. Ενότητα 5.3.4).

7.1.4 Οδηγία Απαίτησης Εκτέλεσης

Μια *Οδηγία Απαίτησης Εκτέλεσης (ΟΑΕκ) (Task Presence Directive – TPD)* χρησιμοποιείται για να εκφράσει ότι μια έγκυρη εργασία, όπως προδιαγράφεται σε μια ΟΕΔιΣ, απαιτεί την ύπαρξη μια άλλης εργασίας ή δομής εργασιών στη ροή, πιθανώς υπό ορισμένες συνθήκες πλαισίου, προ-υποθέσεις ή μετα-υποθέσεις. Πέρα από τις απαιτούμενες αυτές εργασίες, η οδηγία υποδεικνύει επίσης τη σχετική θέση ή συσχέτιση σε επίπεδο ανταλλαγής δεδομένων που χαρακτηρίζουν τις πρώτες ως προς την εργασία αναφοράς. Οι πληροφορίες αυτές κωδικοποιούνται ως διαφορετικά προφίλ συμβατότητας, τα οποία για την περίπτωση αυτή είναι τα ακόλουθα (βλ. Ενότητες 5.3.3, 5.3.4,5.3.5, 5.3.6): *προέλευση δεδομένων*, *συμπληρωματική προηγούμενη επεξεργασία* (*σύνδεσης μονοπατιού* ή *άμεσης σύνδεσης*), *συμπληρωματική προηγούμενη εκτέλεση* (*απλή* ή *ανασταλτική*), *συμπληρωματική ακόλουθη επεξεργασία*, *συμπληρωματική ακόλουθη εκτέλεση*, *συμπληρωματική παράλληλη εκτέλεση* (*απλή* ή *ανασταλτική*), *συμπληρωματική παράλληλη επεξεργασία* (*απλή*, *συνδυαστική* ή *ανασταλτική*), *εκτέλεση αμέσως πριν*, *εκτέλεση αμέσως μετά*, *εκτέλεση οποτεδήποτε* (επί συγκεκριμένου μονοπατιού δεδομένων ή όχι) στα πλαίσια της ροής εργασιών.

Σημειώνεται ότι ειδικά η περίπτωση της ΟΑΕκ κάποιας εργασίας σε οποιαδήποτε θέση, ακριβώς λόγω της φύσης της, δεν είναι απαραίτητο να συνδέεται με μια άλλη συγκεκριμένη εργασία ή ΟΕΔιΣ, παρά μόνο ίσως με κάποιο σκοπό ή/και εκκινητή. Για παράδειγμα, σε μια ροή εργασιών με σκοπό την αντιμετώπιση συμβάντων ασφάλειας σε ένα δίκτυο, μπορεί να απαιτείται η αποθήκευση των ειδοποιήσεων που προκύπτουν, ανεξάρτητα από το σε ποιό σημείο του κύκλου ζωής τους αυτό συμβαίνει.

7.1.5 Οδηγία Απαγόρευσης Εκτέλεσης

Σε αντίθεση με τα παραπάνω είδη οδηγιών, οι *Οδηγίες Απαγόρευσης Εκτέλεσης (ΟΑπΕκ) (Task Forbiddance Directives – TFD)* απαγορεύουν την εκτέλεση κάποιων εργασιών, σε συγκεκριμένες ή μη θέσεις στη ροή, εν όψει της παρουσίας κάποιων άλλων εργασιών, όπως αυτές προκύπτουν από τις αντίστοιχες ΟΕΔιΣ. Έτσι, κάθε τέτοια οδηγία αναφέρεται σε μια ΟΕΔιΣ, καθώς και σε εκείνη την εργασία μέσα στην ΟΕΔιΣ που ενεργοποιεί την απαγόρευση, προσδιορίζοντας την εργασία ή εργασίες, με τις οποίες η υπό εξέταση εργασία δεν επιτρέπεται να συνυπάρχει, είτε γενικά στη ροή εργασιών είτε σε κάποια σχετική θέση. Το τελευταίο ορίζεται μέσω του προφίλ συμβατότητας, που μπορεί να έχει μια από τις παρακάτω τιμές: *πριν*, *μετά*, *παράλληλα*, *ακριβώς παράλληλα*, *οπουδήποτε*, ενώ επιπλέον υποδιαιρέσεις είναι δυνατές, ανάλογα με το αν η απαγόρευση αναφέρεται ή όχι σε συγκεκριμένο μονοπάτι δεδομένων (βλ. Ενότητα 5.3.7). Ομοίως, μια απαγόρευση μπορεί να ισχύει μόνο υπό συγκεκριμένες συνθήκες πλαισίου, προ-υποθέσεις ή μετα-υποθέσεις. Τέλος, και σε αυτή την περίπτωση, η απαγόρευση της εκτέλεσης μιας εργασίας σε οποιοδήποτε σημείο της ροής εργασιών μπορεί να είναι ανεξάρτητη άλλων εργασιών ή έγκυρων ΔιΣ.

7.1.6 Οδηγία Απαγόρευσης Ροής

Οι *Οδηγίες Απαγόρευσης Ροής (ΟΑπΡ) (Flow Forbiddance Directives – FFD)* αναφέρονται σε έναν έγκυρο ΔιΣ, απαγορεύοντας, δεδομένης της ήδη προσδιοριζόμενης ροής, δεδομένων ή ελέγχου, τη μεταφορά συγκεκριμένης επιπλέον πληροφορίας προς την εργασία προορισμού ή από την εργασία προέλευσης (βλ. Ενότητα 5.3.7). Η οδηγία δείχνει στη σχετική εργασία που λαμβάνει (αντ. αποστέλλει) δεδομένα, υποδεικνύοντας τα δεδομένα εισόδου (αντ. εξόδου) που η τελευταία απαγορεύεται να λάβει (αντ. δώσει), καθώς και, πιθανώς, την εργασία από την οποία αυτά δεν πρέπει να προέρχονται (αντ. στην οποία αυτά δεν πρέπει να καταλήγουν). Και εδώ είναι δυνατός ο ορισμός παραλλαγών, όπως *άμεσης σύνδεσης* ή *σύνδεσης μονοπατιού*, ενώ, ομοίως προς τις άλλες οδηγίες, υπάρχει δυνατότητα περιορισμού της απαγόρευσης από συνθήκες πλαισίου, προ-υποθέσεις ή μετα-υποθέσεις.

7.2 Οντολογική Αναπαράσταση Οδηγιών Συμβατότητας

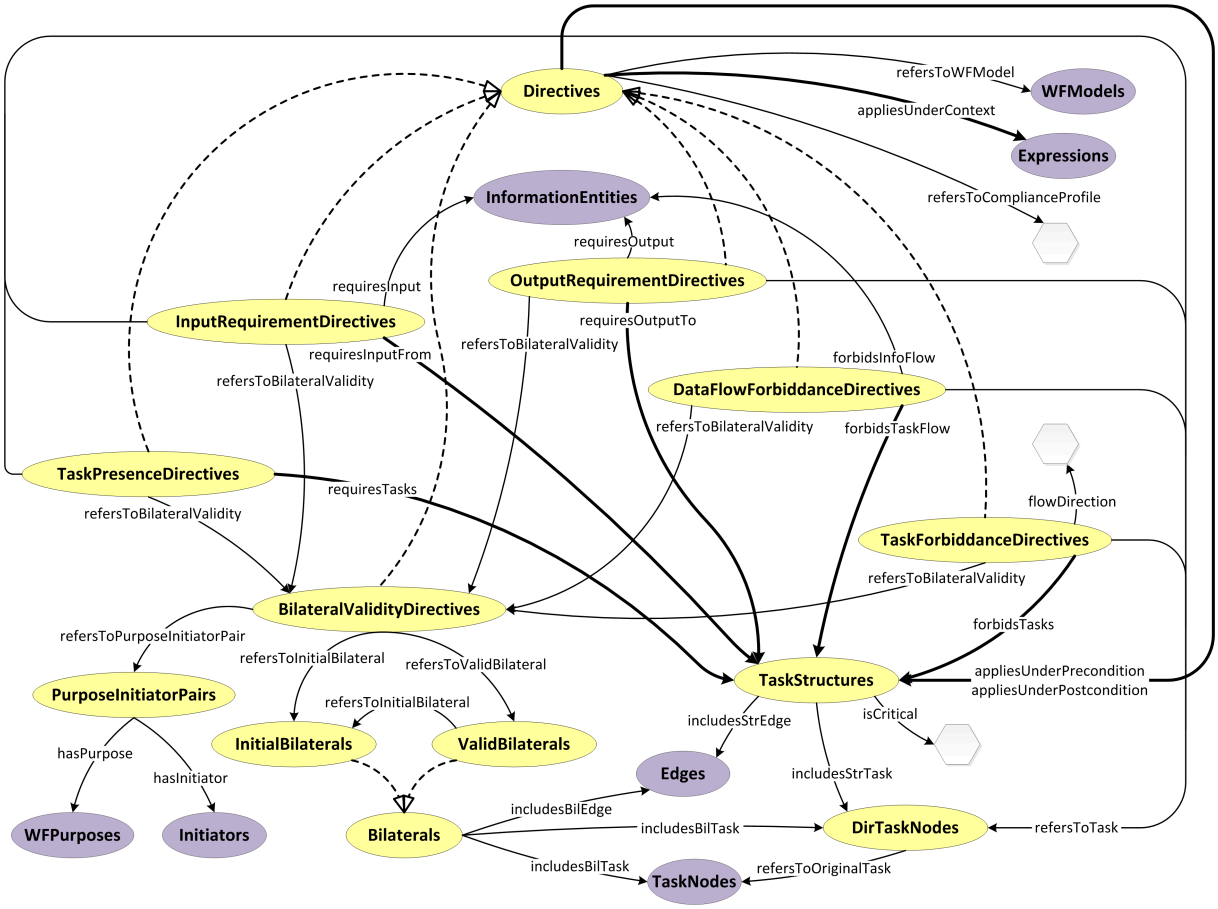
Ως τεχνικό μέσο για το φορμαλιστικό ορισμό των οδηγιών συμβατότητας επελέγη η χρήση οντολογίας στα πλαίσια μιας ενιαίας προσέγγισης στο επίπεδο της υλοποίησης, εφόσον οι οδηγίες αποτελούν στην ουσία το συνδετικό ιστό ανάμεσα στο Σημασιολογικό Μοντέλο Πολιτικών και το εκάστοτε Μοντέλο Ροής Εργασιών (ΜΡΕ). Σε αυτή την κατεύθυνση, η ΟΜΡΕ επεκτείνεται με επιπλέον κλάσεις, οι οποίες, βασιζόμενες στις οντότητες της ΟΜΡΕ, αποτυπώνουν τις οδηγίες συμβατότητας που αφορούν τα ΜΡΕ που η τελευταία περιλαμβάνει. Έτσι, οι προαναφερθέντες τύποι οδηγιών συνιστούν μέλη των αντίστοιχων

κλάσεων, ενώ οι διάφορες σχέσεις μεταξύ τους και μεταξύ αυτών και των δομών ενός μοντέλου ροής εργασιών εκπροσωπούνται από τις κατάλληλες ιδιότητες αντικειμένου. Συνοπτικά, οι νέες κλάσεις που εμφανίζονται είναι οι εξής:

- `Directives`, η οποία περικλείει όλες τις οδηγίες οι οποίες επιστρέφονται από τη Μηχανή Συμπερασμού για μια δεδομένη ροή εργασιών. Υποδιαιρείται περαιτέρω, με βάση τους διαφορετικούς τύπους οδηγιών που παρουσιάστηκαν παραπάνω, στις ακόλουθες υποκλάσεις: `BilateralValidityDirectives`, `InputRequirementDirectives`, `OutputRequirementDirectives`, `TaskPresenceDirectives`, `TaskForbiddanceDirectives`, `DataFlowForbiddanceDirectives`.
- `PurposeInitiatorPairs`, τα μέλη της οποίας ορίζουν τους συνδυασμούς σκοπού–εκκινητή για τους οποίους κάθε οδηγία ισχύει.
- `DirTaskNodes`, η οποία συμπεριλαμβάνει όλες τις έγκυρες προδιαγραφές εργασιών που ορίζονται από τις διάφορες οδηγίες.
- `Bilaterals`, η οποία χρησιμοποιείται για τη μοντελοποίηση των ΔιΣ στις οποίες αναφέρονται οι οδηγίες. Οι υποκλάσεις της `InitialBilaterals` και `ValidBilaterals` περιλαμβάνουν, αντίστοιχα, τους ΔιΣ όπως αυτοί εμφανίζονται στην αρχική ροή εργασιών και τις έγκυρες προδιαγραφές τους όπως ορίζονται από τη Μηχανή Συμπερασμού.
- `TaskStructures`, κάθε μέλος της οποίας αντιστοιχεί είτε σε μεμονωμένες εργασίες (μέλη της `DirTaskNodes`) είτε σε ροές/δομές αυτών.

Το Σχήμα 17 απεικονίζει τον οντολογικό ορισμό των οδηγιών συμβατότητας. Οι κλάσεις που στο σχήμα εμφανίζονται με πιο σκούρα σκίαση ταυτίζονται με τις ομώνυμές τους που περιλαμβάνονται ήδη στην αρχική (χωρίς οδηγίες) εκδοχή της OMPE (βλ. Κεφάλαιο 6). Η κλάση `DirTaskNodes` έχει πρακτικά τον ίδιο ορισμό με την `TaskNodes` στις ροές εργασιών, με τη μόνη διαφορά ότι συμπληρώνεται με τη λειτουργική ιδιότητα αντικειμένου `refersToTask`, η οποία δείχνει σε κάποιο μέλος της `TaskNodes` και χρησιμοποιείται στην περίπτωση που η εν λόγω εργασία ορίζεται από κάποια οδηγία προς "αντικατάσταση" κάποιας άλλης στην αρχική ροή εργασιών. Τέλος, οι τονισμένες γραμμές υπονοούν ότι οι αντίστοιχες ιδιότητες αντικειμένου μπορούν επιπλέον να συνδέονται και με λογικές σχέσεις μεταξύ μελών των κλάσεων που απεικονίζονται στο σχήμα ως μέρους του πεδίου τιμών τους.

Στις ενότητες που ακολουθούν περιγράφονται λεπτομερέστερα οι κεντρικές οντολογικές οντότητες που σχετίζονται με τις οδηγίες και οι μεταξύ τους σχέσεις.



Σχήμα 17: Οντολογική αναπαράσταση των οδηγιών συμβατότητας.

7.2.1 Η Κλάση `PurposeInitiatorPairs`

Για την κλάση αυτή ορίζονται δύο λειτουργικές ιδιότητες αντικειμένου, οι `hasPurpose` και `hasInitiator`, οι οποίες έχουν ως πεδία ορισμού τις κλάσεις `WFPurposes` και `Initiators`, αντίστοιχα. Χρησιμοποιούνται για τον προσδιορισμό ζευγών μεταξύ έγκυρων εκκινητών, δηλαδή δραστών εξουσιοδοτημένων για την εκκίνηση της ροής εργασιών, και των επιτρεπόμενων, σε κάθε περίπτωση, σκοπών. Όπως θα φανεί στη συνέχεια, κάθε οδηγία αναφέρεται, άμεσα ή έμμεσα, σε τέτοια ζεύγη, προκειμένου να υποδείξει τους συγκεκριμένους συνδυασμούς σκοπών–εκκινητών για τους οποίους έχει ισχύ.

7.2.2 Η Κλάση `TaskStructures`

Κάθε μέλος της κλάσης `TaskStructures` συνδέεται με ένα ή περισσότερα μέλη της `DirTaskNodes` μέσω της ιδιότητας αντικειμένου `includesStrTask` και, πιθανώς, με μέλη των κλάσεων `Edges`, `DataEdges`, `ControlEdges` μέσω της ιδιότητας `includesStrEdge`. Η κλάση αυτή χρησιμοποιείται για την αναπαράσταση είτε μεμονωμένων εργασιών είτε αλληλεπιδράσεων μεταξύ εργασιών, κατά τρόπο αντίστοιχο με αυτόν της περιγραφής ροών εργα-

σιών. Ωστόσο, οι αντίστοιχες δομές διαφοροποιούνται από τις τελευταίες σε διάφορα σημεία, όχι τόσο σε επίπεδο φορμαλιστικών ορισμών όσο αναφορικά με τον τρόπο χρήσης τους. Για παράδειγμα, γενικά στα πλαίσια των οδηγιών και σε αντίθεση με τον ορισμό των εργασιών που αποτελούν μέρος μιας ολοκληρωμένης ροής, κάθε μέλος της `DirTaskNodes` συνδέεται με ένα μόνο μέλος της `ExecutionProfiles` (βλ. Ενότητα 6). Επιπλέον, σε ό,τι αφορά τις ενδεχόμενες λογικές δομές δραστών και αντικειμένων επενέργειας που εμφανίζονται στα τελευταία, αυτές αφορούν μόνο σχέσεις σύζευξης (μέλη της `ANDRelations`), προκειμένου να σχηματοποιείται η απαίτηση ότι μια εργασία πρέπει να εκτελεστεί από κοινού από περισσότερους του ενός δράστες ή/και πάνω σε περισσότερα του ενός αντικείμενα επενέργειας. Από την άλλη, εναλλακτικές προδιαγραφές των παραπάνω μπορούν να οριστούν με χρήση λογικών σχέσεων μεταξύ ολόκληρων δομών εργασιών. Τέλος, τέτοιες δομές μπορεί να διαφοροποιούνται με βάση το αν θα πρέπει να αναζητούνται στη ροή εργασιών αυστηρά όπως ορίζονται, δηλαδή χωρίς να παρεμβάλλονται άλλες εργασίες, ή αν κάτι τέτοιο δεν είναι υποχρεωτικό. Αυτό δηλώνεται μέσω της ιδιότητας τύπου δεδομένου `isCritical`, η οποία λαμβάνει τιμή `true` όταν απαγορεύεται η παρεμβολή επιπλέον εργασιών και `false` στην αντίθετη περίπτωση.

7.2.3 Η Κλάση `Bilaterals`

Η κλάση αυτή είναι παρόμοια δομικά με την `TaskStructures`, καθώς και αυτή συνδέεται κατά βάση με εργασίες και ακμές μέσω των ιδιοτήτων `includesBilTask` και `includesBilEdge`, διαφέρει ωστόσο εννοιολογικά.

Η υποκλάση της `InitialBilaterals` περιλαμβάνει όλους τους ΔιΣ κάθε υπό επαλήθευση ροής εργασιών στην αρχική τους μορφή. Με άλλα λόγια, τα μέλη της `InitialBilaterals` είναι τόσα ακριβώς όσοι είναι οι ΔιΣ που έχουν προηγουμένως εξαχθεί από κάθε ροή εργασιών και υποβληθεί, σε αυτή τη μορφή, στη Μηχανή Συμπερασμού. Η τελευταία βασίζεται σε αυτά τα μέλη προκειμένου να δημιουργήσει τις αντίστοιχες οδηγίες προς εφαρμογή. Για κάθε μέλος της `InitialBilaterals` ορίζονται ακριβώς δύο τιμές της ιδιότητας `includesBilTask` και μια μοναδική τιμή της `includesBilEdge`, δείχνοντας στις αντίστοιχες δομές (`TaskNodes` και `Edges`) που συναποτελούν τον εν λόγω ΔιΣ.

Από την άλλη, ένα μέλος της υποκλάσης `ValidBilaterals` εκφράζει μια έγκυρη προδιαγραφή για ένα συγκεκριμένο μέλος της κλάσης `InitialBilaterals`, με την οποία το πρώτο σχετίζεται μέσω της λειτουργικής ιδιότητας αντικειμένου `refersToInitialBilateral`. Παρά την ονομασία της, η κλάση `ValidBilaterals` μπορεί να μην περιλαμβάνει μόνο διμερείς, με τη στενή έννοια, συσχετισμούς. Κάθε μέλος της συνδέεται με δύο τουλάχιστον μέλη της `DirTaskNodes` και ένα τουλάχιστον μέλος της `DataEdges` ή `ControlEdges`, το οποίο αντιστοιχεί στην περίπτωση κατά την οποία δεν απαιτείται η παρεμβολή επιπλέον εργασιών για τον πλήρη προσδιορισμό του έγκυρου ΔιΣ. Μπορεί, ωστόσο, να περιλαμβάνει και μεγαλύτερο αριθμό εργασιών και ακμών, αν βάσει κανόνων είναι απαραίτητη

η εισαγωγή ενδιάμεσων εργασιών και ροών δεδομένων. Σε κάθε περίπτωση, οι εργασίες `DirTaskNodes` που περιλαμβάνονται σε ένα μέλος της `ValidBilaterals` και προορίζονται για την "αντικατάσταση" εργασιών του αρχικού ΔιΣ (εργασιών οριζόμενων, δηλαδή, στο αντίστοιχο μέλος της `InitialBilaterals`) χαρακτηρίζονται η καθεμιά από την ιδιότητα αντικειμένου `refersToOriginalTask`, η οποία δείχνει, ανάλογα, στην εργασία–πηγή ή εργασία–προορισμό του αντίστοιχου αρχικού ΔιΣ. Για τις εργασίες που περιλαμβάνονται σε μέλη της `ValidBilaterals` ισχύουν οι ίδιες παρατηρήσεις ως προς το σχηματισμό με τις εργασίες που σχετίζονται με μέλη της κλάσης `TaskStructures`.

7.2.4 Η Κλάση `Directives`

Η κλάση `Directives` καθεαυτή δεν έχει μέλη· περιλαμβάνει το σύνολο των οδηγιών, καθεμιά από τις οποίες υλοποιείται, αναλόγως του τύπου της, ως μέλος μιας εκ των υποκλάσεων της `Directives`, οι οποίες θα παρουσιαστούν στη συνέχεια. Καθότι όλοι οι τύποι οδηγιών χαρακτηρίζονται από κάποιες κοινές παραμέτρους, στο επίπεδο της υπερκλάσης ορίζονται οι ακόλουθες ιδιότητες αντικειμένου:

- `refersToWFModel`, που δείχνει σε ένα μέλος της `WorkflowModels`, δηλώνοντας τη ροή εργασιών την οποία αφορά.
- `appliesUnderContext`, η οποία έχει ως πεδίο τιμών τις κλάσεις `Expressions` και `LogicalRelations` και χρησιμεύει για την περιγραφή των συνθηκών πλαισίου κάτω από τις οποίες η εκάστοτε οδηγία έχει ισχύ.
- `appliesUnderPrecondition`, που, με πεδίο τιμών τις `TaskStructures` και `LogicalRelations`, υποδεικνύει την εργασία ή εργασίες που πρέπει να προηγούνται της εργασίας αναφοράς μέσα στη ροή εργασιών, ώστε να ισχύει η οδηγία.
- `appliesUnderPostcondition`, η οποία, επίσης με πεδίο τιμών τις κλάσεις `TaskStructures` και `LogicalRelations`, υποδεικνύει την εργασία ή εργασίες που αυτή τη φορά πρέπει να έπονται της εργασίας αναφοράς μέσα στη ροή εργασιών, ώστε να ισχύει η οδηγία.

Επιπλέον, ορίζεται η ιδιότητα τύπου δεδομένου `refersToComplianceProfile`, που μπορεί να λάβει συγκεκριμένες τιμές ανάλογα με τον τύπο της οδηγίας που αφορά και προσδιορίζει με μεγαλύτερη ακρίβεια τον τρόπο εφαρμογής της, με άλλα λόγια, το ειδικότερο προφίλ συμβατότητας (βλ. Ενότητα 7.1).

Περνώντας στις επιμέρους υποκλάσεις, η κλάση `BilateralValidityDirectives` μοντελοποιεί τις ΟΕΔιΣ, παρέχοντας μέσω των μελών της έγκυρες προδιαγραφές για καθέναν από τους αρχικούς ΔιΣ της υπό εξέταση ροής εργασιών, με χρήση των ακόλουθων ιδιοτήτων αντικειμένου:

- `refersToInitialBilateral`, η οποία δείχνει στο ΔιΣ εργασιών που η οδηγία αφορά, δηλαδή σε ένα μέλος της `InitialBilaterals`.
- `refersToValidBilateral`, η οποία υποδεικνύει το μέλος της `ValidBilaterals` που εκφράζει τον έγκυρο ΔιΣ προς αντικατάσταση του αρχικού.
- `refersToPurposeInitiatorPair`, που, με πεδίο τιμών την κλάση `PurposeInitiatorPairs`, υποδεικνύει τους συγκεκριμένους συνδυασμούς εκκινητή–σκοπού που η εκάστοτε ΟΕΔιΣ αφορά.

Διαφορετικά μέλη της `BilateralValidityDirectives` συσχετισμένα με το ίδιο μέλος της `InitialBilaterals` υποδηλώνουν εναλλακτικές επιτρεπτές προδιαγραφές για ένα δεδομένο αρχικό ΔιΣ. Αν σε κάποιο αρχικό ΔιΣ δεν αντιστοιχεί κανένα μέλος της `BilateralValidityDirectives`, αυτό σημαίνει ότι δεν υπάρχει τρόπος ώστε ο συσχετισμός αυτός να καταστεί αποδεκτός μέσα στη συγκεκριμένη ροή εργασιών με βάση την προδιαγραφή του σχεδιαστή.

Σε αυτό το σημείο πρέπει να σημειωθεί ότι τα μέλη όλων των άλλων κλάσεων Οδηγιών συνδέονται υποχρεωτικά με μία ακριβώς οδηγία `BilateralValidityDirectives` μέσω της λειτουργικής ιδιότητας αντικειμένου `refersToBilateralValidity`, με αποτέλεσμα το συσχετισμό τους με τον αντίστοιχο αρχικό και έγκυρο ΔιΣ, αλλά και, έμμεσα, με συγκεκριμένους σκοπούς και εκκινητές. Με τον τρόπο αυτό μοντελοποιείται το γεγονός ότι οι απαιτήσεις ή απαγορεύσεις που εκφράζονται μέσω των Οδηγιών αυτών εξαρτώνται στην πράξη, όπως εξηγήθηκε παραπάνω, από την έγκυρη "εκδοχή" των εργασιών και των μεταξύ τους εξαρτήσεων που έχουν οριστεί από το χρήστη, καθώς και από τους εκκινητές και τους επιχειρησιακούς σκοπούς που η ροή εργασιών αφορά.

Η κλάση `InputRequirementDirectives` περιγράφει τις ΟΑΕισ μέσω των παρακάτω ιδιοτήτων:

- `refersToTask`, η οποία συνδέει την οδηγία με ένα μέλος της `DirTaskNodes` ενός έγκυρου ΔιΣ, προκειμένου να υποδείξει την εργασία μέσα σε αυτόν που χρειάζεται να λάβει τα επιπλέον δεδομένα εισόδου.
- `requiresInput`, η οποία, έχοντας ως πεδίο τιμών την κλάση `InformationEntities`, δηλώνει το είδος των δεδομένων που η εν λόγω εργασία πρέπει να λάβει ως είσοδο.
- `requiresInputFrom`, μια προαιρετική ιδιότητα, η οποία, με πεδίο τιμών τις κλάσεις `TaskStructures` και `LogicalRelations`, χρησιμοποιείται για τον ορισμό, όπου χρειάζεται, συγκεκριμένων εργασιών ή δομών από τις οποίες τα απαιτούμενα δεδομένα πρέπει να προέρχονται.

Όταν περισσότερες της μιας οδηγίες `InputRequirementDirectives` συνδέονται με την ίδια έγκυρη εργασία, τότε όλες πρέπει να ικανοποιηθούν προκειμένου να μπορεί να

θεωρηθεί έγκυρη η ροή εργασιών, με άλλα λόγια, η εργασία αναφοράς πρέπει να λάβει όλα τα δεδομένα που περιλαμβάνονται σε αυτές. Από την άλλη, είναι δυνατόν να οριστούν εναλλακτικές πηγές των απαιτούμενων δεδομένων με κατάλληλη χρήση, μέσα στην ίδια οδηγία, λογικών σχέσεων δομών εργασιών σε ό,τι αφορά τις τιμές της ιδιότητας `requiresInputFrom`.

Για την κλάση `OutputRequirementDirectives`, που χρησιμοποιείται για τη φορμαλιστική διατύπωση των ΟΑΕξ, ορίζονται επιπλέον οι εξής ιδιότητες:

- `refersToTask`, η οποία συνδέει την οδηγία με ένα μέλος της `DirTaskNodes` ενός έγκυρου ΔιΣ, προκειμένου να υποδείξει την εργασία μέσα σε αυτόν που πρέπει να παράσχει (κάποια από) τα δεδομένα που παράγει σε κάποια άλλη εργασία.
- `requiresOutput`, που δείχνει σε ένα ή περισσότερα στγμιότυπα `InformationEntities`, δηλώνοντας το είδος των δεδομένων που η εν λόγω εργασία πρέπει να παράσχει.
- `requiresOutputTo`, η οποία, μέσω του αντίστοιχου μέλους της `TaskStructures` ή της `LogicalRelations`, ορίζει τις εργασίες οι οποίες πρέπει να λάβουν τα παραγόμενα δεδομένα.

Και εδώ, η σύνδεση μιας εργασίας με πολλαπλές οδηγίες `OutputRequirementDirectives` υποδηλώνει ότι η πρώτη πρέπει να καταστήσει διαθέσιμα όλα τα σχετικά δεδομένα. Εναλλακτικές εργασίες προορισμού μπορούν να οριστούν με χρήση λογικών σχέσεων.

Η κλάση `TaskPresenceDirectives` ομαδοποιεί τις ΟΑΕκ, περιγράφοντάς τες με τη βοήθεια των ιδιοτήτων:

- `refersToTask`, η οποία συνδέει την οδηγία με ένα μέλος της `DirTaskNodes` ενός έγκυρου ΔιΣ, προκειμένου να υποδείξει μέσα σε αυτόν την εργασία που απαιτεί την εκτέλεση κάποιας άλλης εργασίας. Στην περίπτωση που κάποια εργασία απαιτείται να εκτελεστεί οπουδήποτε μέσα στη ροή ανεξαρτήτως υπαρχόντων εργασιών, η ιδιότητα αυτή δεν παίρνει καμία τιμή.
- `requiresTasks`, η οποία δείχνει σε μέλη των κλάσεων `TaskStructures` ή `LogicalRelations`, δηλώνοντας τις εργασίες που πρέπει να εκτελεστούν.

Όλες ανεξαιρέτως οι οδηγίες `TaskPresenceDirectives` πρέπει να ισχύουν σε μια ροή εργασιών. Αντίθετα, όταν μέσω λογικών σχέσεων ορίζονται στην ίδια οδηγία εναλλακτικές απαιτούμενες εργασίες ή δομές, τουλάχιστον μία από αυτές πρέπει να είναι παρούσα. Επιπλέον, πολλαπλές τιμές της ιδιότητας τύπου δεδομένου `refersToComplianceProfile` υποδηλώνουν ότι η ίδια εργασία πρέπει να συμμετέχει στη ροή με περισσότερους από έναν τρόπους, δηλαδή, να εκτελείται πιθανώς σε περισσότερα του ενός (χρονικά) σημεία.

Οι ΟΑπΕκ ορίζονται, σε συμμετρία με τις ΟΑΕκ, με τις ακόλουθες επιπλέον ιδιότητες:

- `refersToTask`, η οποία συνδέει την οδηγία με ένα μέλος της `DirTaskNodes` ενός έγκυρου ΔιΣ, προκειμένου να υποδείξει την εργασία μέσα σε αυτόν που απαγορεύει την εκτέλεση κάποιας άλλης εργασίας.
- `forbidsTasks`, η οποία δείχνει σε μέλη των κλάσεων `TaskStructures` ή `LogicalRelations`, δηλώνοντας τις εργασίες που απαγορεύεται να εκτελεστούν.

Τέλος, οι ΟΑπΡ περιγράφονται με βάση τις εξής ιδιότητες:

- `refersToTask`, η οποία συνδέει την οδηγία με ένα μέλος της `DirTaskNodes` ενός έγκυρου ΔιΣ, προκειμένου να υποδείξει την εργασία μέσα σε αυτόν που απαγορεύεται να λάβει ή να αποστείλει κάποια δεδομένα.
- `forbidsTaskFlow`, η οποία δείχνει σε μέλη των κλάσεων `TaskStructures` ή `LogicalRelations`, δηλώνοντας τις εργασίες που απαγορεύεται να αποστείλουν πληροφορία σε ή να λάβουν πληροφορία από την εργασία αναφοράς.
- `forbidsInfoFlow`, που δείχνει σε ένα ή περισσότερα στιγμιότυπα `InformationEntities`, δηλώνοντας το είδος των δεδομένων που η παραπάνω δομή εργασιών δεν πρέπει να αποστείλει σε ή να λάβει από την εργασία αναφοράς.
- `flowDirection`, μια ιδιότητα τύπου δεδομένου που μπορεί να πάρει μία από τις τιμές {*incoming*, *outgoing*}, δηλώνοντας την κατεύθυνση ροής που αφορά η απαγόρευση

Κεφάλαιο 8

Έλεγχος Ροών Εργασιών ως προς την Ιδιωτικότητα

Ο έλεγχος και η ενδεχόμενη τροποποίηση των ροών εργασιών με σκοπό την εξασφάλιση της συμβατότητάς τους με τις αρχές της ιδιωτικότητας πραγματοποιείται στο Περιβάλλον Σχεδιασμού και συγκεκριμένα από τον Αναλυτή Ροών Εργασιών. Στο κεφάλαιο αυτό περιγράφεται η διαδικασία που ακολουθείται για την επαλήθευση των ροών εργασιών στη βάση των οδηγιών που αφορούν καθεμιά [429].

8.1 Επισκόπηση Μεθοδολογίας Ελέγχου

Η διαδικασία ελέγχου ενός Μοντέλου Ροής Εργασιών (ΜΡΕ) ξεκινά μόλις το τελευταίο, αφού έχει οριστεί από το χρήστη μέσω της κατάλληλης Γραφικής Διεπαφής (βλ. Ενότητα 4.3), περνά στον Αναλυτή Ροών Εργασιών. Δομικά, οι υπό εξέταση ροές εργασιών θεωρούμε ότι έχουν τα παρακάτω χαρακτηριστικά:

- Δεν περιλαμβάνουν βρόχους (loops), έχουν, δηλαδή, τη μορφή Κατευθυνόμενων Ακυκλικών Γράφων (Directed Acyclic Graphs – DAGs), όπου οι κόμβοι εκπροσωπούν τις εργασίες της ροής και οι ακμές τις ροές ελέγχου ή δεδομένων (βλ. Κεφάλαιο 6).
- Είναι απαλλαγμένες από δομικά σφάλματα που αφορούν κυρίως στη ροή ελέγχου, όπως αδιέξοδα, έλλειψη συγχρονισμού κ.ά., αλλά και στη ροή δεδομένων (βλ. [430][3] [376][377][381][386][385])
- Κάθε εργασία ανήκει σε τουλάχιστον ένα κατευθυνόμενο μονοπάτι, το οποίο είτε ξεκινά από κάποια αρχική εργασία της ροής (μια εργασία, δηλαδή, που δεν έχει εισερχόμενες ακμές), είτε καταλήγει σε κάποια τελική εργασία της ροής (χωρίς εξερχόμενες ακμές), είτε και τα δύο. Με απλά λόγια, δεν εμφανίζονται εργασίες που δεν έχουν ούτε εισερχόμενες ούτε εξερχόμενες ακμές.

Η διαδικασία επαλήθευσης περιγράφεται σε υψηλό επίπεδο στον Αλγόριθμο 1. Σε πρώτη φάση, ο Αναλυτής Ροών Εργασιών πραγματοποιεί μια σειρά λειτουργιών απαραίτητων για τη λήψη των αρχικών οδηγιών συμβατότητας από τη Μηχανή Συμπερασμού. Σε αυτή την κατεύθυνση, ένα πρώτο βήμα περιλαμβάνει τη δημιουργία των διακριτών ζευγών σκοπών και εκκινητών, μέσω του υπολογισμού του καρτεσιανού γινομένου των μελών των κλάσεων `WFPurposes` και `Initiators` της Οντολογίας Μοντέλων Ροών Εργασιών (OMPE) που αντιστοιχούν στην υπό επαλήθευση ροή εργασιών *WM* (γρ. 1). Ο τελικός εκκινητής της ροής και ο σκοπός για τον οποίο ο πρώτος θα ξεκινήσει την εκτέλεσή της θα αντιστοιχούν σε κάποιο από αυτά τα ζεύγη και θα προσδιοριστούν κατά τη φάση της εκτέλεσης (για την ακρίβεια, αμέσως πριν). Καθώς όμως είναι πιθανό να επηρεάζουν το αν και με ποιό τρόπο είναι επιτρεπτή η εκτέλεση των δηλωμένων εργασιών, λαμβάνονται υπόψη ήδη κατά τα πρώτα στάδια του ελέγχου και ενσωματώνονται στην τελική προδιαγραφή της ροής εργασιών με τρόπο που θα φανεί στη συνέχεια.

Κατά την εκτέλεση μιας ροής εργασιών, η αλληλουχία των εργασιών που τελικά εκτελούνται μπορεί να ποικίλει. Αυτό αφορά στις περιπτώσεις που, μέσω της διατύπωσης συνθηκών και λοιπών περιορισμών, η ροή διαφοροποιείται σε κάποια σημεία ανάλογα με τις τιμές που λαμβάνουν κάποιες μεταβλητές πλαισίου (context) ή/και με ιδιότητες που χαρακτηρίζουν τα δεδομένα που λαμβάνουν μέρος ή δημιουργούνται κατά τη διάρκειά της (βλ. Κεφάλαιο 6). Έτσι κάθε φορά εκτελείται ένα υποσύνολο των εργασιών που περιλαμβάνονται στη ροή, με βάση τα διαφορετικά δεδομένα εκτέλεσης και τις εξαρτήσεις μεταξύ εργασιών. Κάθε τέτοιο υποσύνολο, μαζί με τις αλληλοσυσχετίσεις που συνδέουν τις αντίστοιχες εργασίες, συνιστούν έναν *υπογράφο–στιγμιότυπο (instance subgraph)* της ροής εργασιών.

Ορισμός 12 Για ένα μοντέλο ροής εργασιών (MPE) *WM* το σύνολο των *υπογράφων–στιγμιοτύπων* (*Instance Subgraphs*) *IS* αποτελείται από όλες τις διαφορετικές εναλλακτικές δυνατότητες εκτέλεσης του *WM*. Κάθε υπογράφος $is \subseteq IS$ είναι μια τριάδα $\langle T^{is}, F_C^{is}, F_D^{is} \rangle$, τέτοια ώστε: $T^{is} \subseteq T$ είναι ένα υποσύνολο των εργασιών του *WM*· τα F_C^{is} και F_D^{is} είναι σύνολα ακμών που εκφράζουν ροές ελέγχου και δεδομένων μεταξύ των εργασιών T^{is}, έτσι ώστε για κάθε συνδυασμό τιμών που ορίζεται από τις συνθήκες και τους περιορισμούς οντοτήτων πληροφορίας που συνδέονται με όλες τις ακμές $e_i \in F_C^{is} \cup F_D^{is}$, ο υπογράφος *is* είτε θα εκτελεστεί εξ ολοκλήρου είτε δε θα εκτελεστεί.

Με βάση τα παραπάνω, κατά το αρχικό αυτό στάδιο της επαλήθευσης, ο Αναλυτής Ροών Εργασιών προβαίνει επιπλέον στη δημιουργία όλων των υπογράφων–στιγμιοτύπων της ροής, ώστε στη συνέχεια κάθε υπογράφος να μελετηθεί αυτόνομα ως προς τις επιθυμητές ιδιότητες (γρ. 2). Η προσέγγιση αυτή τεκμηριώνεται από το γεγονός ότι οτιδήποτε τελικά συμβαίνει σχετίζεται πάντα με ένα συγκεκριμένο υπογράφο–στιγμιότυπο. Για παράδειγμα, η διαθεσιμότητα των δεδομένων που πρέπει να λάβει κάποια εργασία προκειμένου να εκτελεστεί με σύννομο τρόπο σχετίζεται με τις εργασίες που έχουν εκτελεστεί προηγουμένως και τις αντίστοιχες ροές πληροφοριών προς αυτή. Κάτι τέτοιο μπορεί να

Αλγόριθμος 1 VerifyWorkflowModel

Input: WM
Output: WM_V

$PIP \leftarrow$ CreatePurposeInitiatorPairs
$IS \leftarrow$ GenerateInstanceSubgraphs(WM)
$BA \leftarrow \emptyset$
for each is **in** IS **do**
  BA.add(ExtractInitialBA(is))
end for
$D \leftarrow$ VerifyInitialBA(BA, PIP)
$VPIP \leftarrow$ GetValidPIP(PIP, D)
$VIS \leftarrow \emptyset$
for each is **in** IS **do**
  $C_{is} \leftarrow$ GenerateCases(is, $VPIP$, D_{VB})
  $VC_{is} \leftarrow \emptyset$
  for each c **in** C_{is} **do**
    $D_c \leftarrow$ ExtractCaseDirectives(c, D)
    [FN, DN, $IPrN$, $IPoN$, ExN, StN] $\leftarrow$ GetNorms(D_c)
    $T \leftarrow$ TopologicalSort(c)
    $\overline{T} \leftarrow$ InverseTopologicalSort(T)
    $vc \leftarrow c$
    $vc \leftarrow$ ApplyForbiddanceNorms(vc, FN, T)
    $vc \leftarrow$ ApplyDirectNorms(vc, DN, T)
    $vc \leftarrow$ ApplyIndirectPreNorms(vc, $IPrN$, T)
    $vc \leftarrow$ ApplyIndirectPostNorms(vc, $IPoN$, $\overline{T}$)
    $vc \leftarrow$ ApplyExistenceNorms(vc, ExN, T)
    $vc \leftarrow$ ApplyConditionalDirectNorms(vc, DN, T)
    $vc \leftarrow$ ApplyConditionalIndirectPreNorms(vc, $IPrN$, T)
    $vc \leftarrow$ ApplyConditionalIndirectPostNorms(vc, $IPoN$, $\overline{T}$)
    $vc \leftarrow$ ApplyConditionalExistenceNorms(vc, ExN, T)
    $vc \leftarrow$ ApplyStateNorms(vc, StN, T)
    $vc \leftarrow$ ApplyForbiddanceNorms(vc, FN, T)
    if $vc \neq \emptyset$ **then**
      VC_{is}.add(vc)
    end if
  end for
  $vis \leftarrow$ MergeCases(VC_{is})
  if $vis \neq \emptyset$ **then**
    VIS.add(vis)
  end if
end for
if $VIS \neq \emptyset$ **then**
  $WM_V \leftarrow$ MergeInstanceSubgraphs(VIS)
else
  $WM_V \leftarrow \emptyset$
end if
return WM_V

θεωρηθεί καλά ορισμένο και προσδιορίσιμο μόνο για κάθε υπογράφο–στιγμιότυπο· δεδομένα που καθίστανται διαθέσιμα στην εργασία σε έναν υπογράφο μπορεί να απουσιάζουν σε έναν άλλο, λόγω των διαφορετικών εργασιών που ενδεχομένως οι δύο υπογράφοι περιλαμβάνουν. Πράγματι, η δημιουργία υπογράφων από έναν αρχικό γράφο ροής εργασιών αποτελεί συνήθη πρακτική σε προσεγγίσεις που αφορούν στον έλεγχο ροών εργασιών (π.χ., [381][431]), καθώς μειώνει την πολυπλοκότητα και διευκολύνει τον ακριβή εντοπισμό σφαλμάτων διασπώντας τη ροή εργασιών σε διαχειρίσιμα τμήματα. Σημειώνεται ότι στα πλαίσια της εδώ ακολουθούμενης μεθοδολογίας το όφελος σε πολυπλοκότητα είναι κατάτι μικρότερο, καθώς η εν λόγω λειτουργία δεν πραγματοποιείται κατ' ανάγκη εφάπαξ. Καθόλη τη διάρκεια ελέγχου οι ενδεχόμενες τροποποιήσεις της ροής εργασιών μπορεί να οδηγήσουν εκ νέου στην ανάγκη θεώρησης περαιτέρω υπογράφων, ωστόσο και πάλι η όλη διαδικασία καθίσταται με αυτό τον τρόπο περισσότερο ελέγξιμη.

Με δεδομένους τους υπογράφους–στιγμιότυπα, ο Αναλυτής Ροών Εργασιών εξάγει τους Διμερείς Συσχετισμούς (ΔιΣ) που τους απαρτίζουν, δηλαδή τα ζεύγη εργασιών μαζί με τις ακμές που τις ενώνουν (γρ. 3-6). Εν τω μεταξύ, έχουν ήδη σχηματιστεί τα δηλωμένα ζεύγη σκοπών–εκκινητών *PIP* ως το καρτεσιανό γινόμενο των αντίστοιχων συνόλων, όπως αυτά έχουν προσδιοριστεί από το σχεδιαστή της ροής εργασιών. Από τους ΔιΣ, σε συνδυασμό με τα ζεύγη σκοπών–εκκινητών, προκύπτουν κατόπιν οι οδηγίες συμβατότητας D που θα πρέπει να εφαρμοστούν, με βάση τα ισχύοντα Σημασιολογικά Μοντέλα Πολιτικών και Πληροφοριών (γρ. 7), και οι οποίες παρέχονται από τη Μηχανή Συμπερασμού (βλ. Κεφάλαιο 4). Ο λόγος που για την εξαγωγή των οδηγιών δε χρησιμοποιούνται οι ΔιΣ του αρχικού γράφου ροών εργασιών είναι ότι, όπως γίνεται φανερό από τα παραπάνω, οι πιθανές ροές ελέγχου και δεδομένων που θα προκύψουν κατά τη φάση της εκτέλεσης πρακτικά αντανακλώνται με ακρίβεια στους υπογράφους–στιγμιότυπα, στους οποίους οι ορισμοί των ακμών, κυρίως, ενδέχεται τελικά να διαφέρουν από αυτούς της αρχικής ροής εργασιών. Επιπλέον, από το αρχικό σύνολο *PIP* κρατούνται μόνο τα ζεύγη εκείνα τα οποία εμφανίζονται ως έγκυρα με βάση το σύνολο των οδηγιών D (σύνολο *VPIP*, γρ. 8).

Σε αυτό το σημείο ξεκινά η κυρίως φάση της επαλήθευσης, η οποία συνίσταται στον έλεγχο κάθε υπογράφου–στιγμιοτύπου $is \in IS$ χωριστά (γρ. 10-38). Το πρώτο βήμα της διαδικασίας αυτής είναι η δημιουργία των λεγόμενων *περιπτώσεων εκτέλεσης (workflow cases)* για καθέναν από τους υπογράφους που δημιουργήθηκαν προηγουμένως (γρ. 11). Ο όρος περίπτωση εκτέλεσης προέρχεται από τον όρο *περίπτωση (case)* όπως εισάγεται στο [3], ο οποίος χρησιμοποιείται για να υποδηλώσει ένα διακριτό υπόδειγμα εκτέλεσης μιας διαδικασίας, που έχει ένα μοναδικό αναγνωριστικό και αναφέρεται, για παράδειγμα, στο συγκεκριμένο ασθενή τον οποίο αφορά η εκτέλεση μιας ροής εργασιών σε ένα νοσοκομείο ή στη συγκεκριμένη παραγγελία που κάθε φορά πραγματεύεται μια διαδικασία χειρισμού παραγγελιών, αποτελώντας ουσιαστικά το αποτύπωμα σε πραγματικό χρόνο του εκάστοτε υπογράφου–στιγμιοτύπου, συσχετιζόμενου και με τα αντίστοιχα δεδομένα εκτέλεσης. Σε αυτή την κατεύθυνση, αλλά σε πιο αφηρημένο επίπεδο, οι περιπτώσεις εκτέλεσης χρησιμοποιούνται εδώ για να εκφράσουν τους διαφορετικούς τρόπους και συνθήκες υπό τις

οποίες οι εργασίες που απαρτίζουν κάθε αρχικό υπογράφο–στιγμιότυπο μπορούν να εκτελεστούν.

Έτσι, με βάση τις οδηγίες εγκυρότητας διμερούς συσχετισμού (ΟΕΔιΣ) D_{VB} που σχετίζονται με έναν υπογράφο–στιγμιότυπο is, κάθε περίπτωση εκτέλεσης $c \in C_{is}$ αντανακλά μια παραλλαγή στην εκτέλεση του *is*, κατά την οποία κάθε εργασία μπορεί να εκτελεστεί με μοναδικό τρόπο και όλες οι ακμές μεταξύ εργασιών είναι αυτές που προδιαγράφονται από τις αντίστοιχες ΟΕΔιΣ. Πράγματι, για κάθε ΔιΣ $\langle t_i, e_k, t_{i+1} \rangle$, κάθε προκύπτουσα ΟΕΔιΣ συνίσταται σε μια δομή $\langle t_i^*, e_k^*, t_{i+1}^* \rangle$, όπου καθεμιά από τις εργασίες t_i^* και t_{i+1}^* περιλαμβάνει ακριβώς ένα προφίλ εκτέλεσης (βλ. Ενότητα 6.4.1) και η e_k^* είναι η αντίστοιχη ακμή κατάλληλα προσαρμοσμένη. Είναι σημαντικό να τονιστεί ότι η e_k^* μπορεί να περιλαμβάνει επιπλέον εργασίες μεταξύ των t_i^* και t_{i+1}^*. Αυτή είναι, για παράδειγμα, η περίπτωση κατά την οποία παρεμβάλλονται εργασίες για την εφαρμογή ανωνυμίας ή κρυπτογράφησης των μεταφερόμενων δεδομένων. Τελικά, κάθε περίπτωση εκτέλεσης *c* αποτελεί προβολή του υπογράφου *is* με βάση έναν έγκυρο συνδυασμό δομών $\langle t_i^*, e_k^*, t_{i+1}^* \rangle$, προερχόμενων από τις ΟΕΔιΣ. Με άλλα λόγια, όλες οι περιπτώσεις εκτέλεσης ενός υπογράφου περιέχουν όλες τις αρχικές εργασίες του υπογράφου, ακριβέστερα, τις έγκυρες ισοδύναμές τους, δηλαδή πιθανόν με διαφοροποιημένες προδιαγραφές, και ίσως κάποιες επιπλέον εργασίες, η παρουσία των οποίων σε κάθε περίπτωση εκτέλεσης εξαρτάται από τις έγκυρες αυτές προδιαγραφές για τις ήδη υπάρχουσες εργασίες του υπογράφου. Αντίστροφα, ένας υπογράφος–στιγμιότυπο αντιστοιχίζεται σε ένα σύνολο περιπτώσεων εκτέλεσης, καθεμιά από τις οποίες εκτελεί τις ίδιες, με αναφορά στον αρχικό υπογράφο, εργασίες, πιθανώς με διαφορετικό τρόπο ή/και διαφορετικές επιπλέον απαιτήσεις. Όπως είναι φανερό, ένας υπογράφος δεν οδηγεί σε καμιά περίπτωση εκτέλεσης, οπότε και δεν μπορεί να εκτελεστεί, αν δεν υπάρχει τουλάχιστον ένα ζεύγος σκοπού–εκκινητή για το οποίο να υπάρχουν ΟΕΔιΣ προς όλους τους ΔιΣ, και μάλιστα συμβατές μεταξύ τους.

Στη συνέχεια, κάθε περίπτωση εκτέλεσης *c* που έχει δημιουργηθεί ελέγχεται ως προς τους υπόλοιπους τύπους οδηγιών, αν υπάρχουν (γρ. 13-33). Για το σκοπό αυτό, αρχικά δημιουργούνται για κάθε εργασία *t* της *c* συμπεριφορικές *νόρμες* με βάση το σύνολο των οδηγιών D_c που αντιστοιχούν στην περίπτωση εκτέλεσης (γρ. 14). Οι νόρμες αυτές προκύπτουν από την ομαδοποίηση οδηγιών που εμφανίζουν κοινά μοτίβα συμβατότητας (compliance patterns) και που, ως εκ τούτου, μπορούν να ελεγχθούν από κοινού για κάθε εργασία κατά την ίδια διάσχιση του γράφου της ροής.

Συγκεκριμένα, οι *Νόρμες Απαγόρευσης (NA)(Forbiddance Norms – FN)* συμπεριλαμβάνουν τις απαιτήσεις που προκύπτουν από τις σχετικές οδηγίες απαγόρευσης εκτέλεσης (ΟΑπΕκ) και οδηγίες απαγόρευσης ροής (ΟΑπΡ). Οι *Νόρμες Άμεσης Σύνδεσης (ΝΑΣ) (Direct Norms – NR)* αφορούν εργασίες που θα πρέπει να συνδέονται απευθείας με κάποια άλλη ήδη παρούσα στη ροή, με ακμές ροής ελέγχου ή δεδομένων, είτε εισερχόμενες είτε εξερχόμενες. Από την άλλη, οι *Νόρμες Έμμεσης Σύνδεσης Πριν (ΝΕΣΠ) (Indirect Pre-Norms – IPrN)* και *Έμμεσης Σύνδεσης Μετά (ΝΕΣΜ)(Indirect Post-Norms – IPoN)* υποδεικνύουν εργασίες που

θα πρέπει να προηγούνται, αντίστοιχα έπονται, της εκτέλεσης της *t*, χωρίς να απαιτείται η άμεση σύνδεση τους, ενώ οι *Νόρμες Εκτέλεσης (NE) (Existence Norms)* δηλώνουν την απαίτηση για την εκτέλεση επιπλέον εργασιών σε οποιοδήποτε σημείο της ροής. Οι *Νόρμες Κατάστασης (NK) (State Norms – SN)*, οι οποίες προκύπτουν έμμεσα ως αποτέλεσμα των ΟΕ-ΔιΣ, εκπροσωπούν απαιτήσεις σχετικές με την κατάσταση των δεδομένων (βλ. Ενότητα 6.3.3). Τέλος, όλες οι νόρμες μπορεί να χαρακτηρίζονται είτε ως *υπό συνθήκη (conditional)* είτε ως *απόλυτες (definite)*, ανάλογα με το αν οι αντίστοιχες οδηγίες σχετίζονται με προ-ή/και μετα-υποθέσεις ή όχι, αντίστοιχα. Με βάση την τοπολογική ταξινόμηση[31] των εργασιών, οι οποίες διατρέχονται είτε με αυτή είτε με την αντίστροφη σειρά, κατά περίπτωση, εφαρμόζονται οι αντίστοιχες νόρμες για κάθε εργασία, οδηγώντας πιθανώς στο σταδιακό μετασχηματισμό της περίπτωσης εκτέλεσης *c* και, κατ' επέκταση, στην επαληθευμένη εκδοχή της *vc* (ή σε απόρριψη αυτής).

Η διαδικασία ξεκινά και τελειώνει με εφαρμογή των απαγορεύσεων (γρ. 19, 29). Ο λόγος είναι ότι αφενός μπορεί ήδη κατά το αρχικό αυτό στάδιο η περίπτωση ροής να απορριφθεί λόγω της ανίχνευσης *συγκρούσεων (conflicts)*, όπως αυτές ορίζονται από τις αντίστοιχες ΝΑ, και αφετέρου, ο έλεγχος για τυχόν απαγορεύσεις είναι απαραίτητος ύστερα από όλες τις πιθανές τροποποιήσεις που μπορεί να έχει υποστεί η περίπτωση εκτέλεσης μέσω της εφαρμογής όλων των υπόλοιπων νορμών.

Το τελευταίο πραγματοποιείται σε τρεις φάσεις: αρχικά εφαρμόζονται οι απόλυτες απαιτήσεις (γρ. 20-23), ακολουθούμενες, σε δεύτερη φάση, από τις απαιτήσεις υπό συνθήκη (γρ. 24-27). Ο διαχωρισμός αυτός αποσκοπεί στο να πραγματοποιηθούν πρώτα οι έλεγχοι και αλλαγές που είναι ούτως ή άλλως απαραίτητοι και στη συνέχεια εκείνοι που εξαρτώνται από την ευρύτερη δομή της ροής εργασιών (προ-υποθέσεις, μετα-υποθέσεις), καθώς κάποιες από τις αντίστοιχες εξαρτήσεις μπορεί να υφίστανται ήδη στη ροή μετά την εφαρμογή των απόλυτων απαιτήσεων. Σε κάθε φάση, οι ΝΑΣ (γρ. 20, 24) εξετάζονται πριν από τις ΝΕΣΠ (γρ. 21, 25) και ΝΕΣΜ (γρ. 22, 26), λόγω του ότι οι απαιτήσεις άμεσης γειτνίασης θεωρούνται εν γένει πιο αυστηρές, ενώ, εφόσον ικανοποιούνται, ενδέχεται να καλύπτουν και κάποιες από τις έμμεσες. Επιπλέον, οι ΝΕΣΠ εφαρμόζονται ξεχωριστά από τις ΝΕΣΜ, καθώς οι τελευταίες προϋποθέτουν τη διάσχιση του γράφου εργασιών με αντίστροφη σειρά. Οι ΝΕ εφαρμόζονται στο τέλος, καθώς είναι πιθανό να έχουν στο μεταξύ καλυφθεί από τις προηγούμενες κατηγορίες (γρ. 23, 27). Η τρίτη φάση περιλαμβάνει την εφαρμογή των νορμών που σχετίζονται με την κατάσταση των δεδομένων, προκειμένου οι αντίστοιχοι έλεγχοι και τροποποιήσεις να γίνουν, αφού όλες οι υπόλοιπες νόρμες έχουν εξεταστεί και, κατά συνέπεια, όλες οι ενδεχόμενες προσθήκες εργασιών και τροποποιήσεις ροών δεδομένων και ελέγχου έχουν ολοκληρωθεί.

[31]Εφόσον θεωρούμε γράφους χωρίς βρόχους, παντού όπου χρειάζεται ταξινόμηση εργασιών χρησιμοποιείται ο κλασικός αλγόριθμος τοπολογικής ταξινόμησης (topological sort) για Κατευθυνόμενους Ακυκλικούς Γράφους που περιγράφεται στο [432]. Ως μέθοδος ταξινόμησης επιλέγεται η τοπολογική, λόγω του ότι ενδείκνυται για περιπτώσεις όπου, όπως στις ροές εργασιών, οι σχέσεις διαδοχής μεταξύ των κόμβων πρέπει να διατηρούνται.

Αφού η επαλήθευση, όπως περιγράφηκε παραπάνω, ολοκληρωθεί για όλες τις περιπτώσεις εκτέλεσης C_{is} του υπογράφου *is*, οι αντίστοιχες έγκυρες περιπτώσεις εκτέλεσης VC_{is} που προκύπτουν συνενώνονται, σχηματίζοντας τον έγκυρο υπογράφο–στιγμιότυπο *vis* (γρ. 34). Η συνένωση συνίσταται στην κατάλληλη ενοποίηση των προδιαγραφών των αντίστοιχων εργασιών και ακμών μεταξύ των διαφορετικών περιπτώσεων εκτέλεσης.

Κατά παρόμοιο τρόπο, αφού ολοκληρωθεί η δημιουργία όλων των έγκυρων υπογράφων της ροής εργασιών, οι τελευταίοι συνενώνονται επίσης, οδηγώντας στην τελική επαληθευμένη προδιαγραφή της ροής εργασιών WM_V (γρ. 39-42). Με άλλα λόγια, σε αντιστοιχία με τη διάσπαση της αρχικής ροής εργασιών σε υπογράφους–στιγμιότυπα και, στη συνέχεια, σε επιμέρους περιπτώσεις εκτέλεσης, η ανασύνθεση των περιπτώσεων εκτέλεσης και των επαληθευμένων υπογράφων οδηγεί στην ενοποιημένη επαληθευμένη προδιαγραφή της ροής εργασιών. Όπως είναι προφανές, προκειμένου η διαδικασία επαλήθευσης να είναι επιτυχής, με την έννοια ότι οδηγεί σε κάποια εκτελέσιμη μορφή της αρχικής ροής εργασιών, θα πρέπει να προκύπτει τουλάχιστον μία έγκυρη περίπτωση εκτέλεσης από την ανωτέρω διαδικασία.

Ο βασικός Αλγόριθμος 1 μπορεί να εκτελεστεί σε διαφορετικές παραλλαγές, οι οποίες κατά κύριο λόγο αφορούν την επαναληπτική εκτέλεση τμημάτων του κατά την επαλήθευση των περιπτώσεων εκτέλεσης, των υπογράφων ή και της ροής εργασιών συνολικά, μέχρι του σημείου επίτευξης σύγκλισης· το τελευταίο σημαίνει ότι ο έλεγχος σταματά όταν πλέον δεν εισάγεται καμία τροποποίηση. Αυτό οφείλεται στο ότι κατά τη μετατροπή της ροής εργασιών ενδέχεται να προκύπτουν νέες παραβιάσεις των αρχών ιδιωτικότητας οι οποίες δεν ήταν παρούσες στην αρχική μορφή της ροής. Αν, για παράδειγμα, δύο νέες εργασίες προστεθούν στη ροή εργασιών μέσω της διαδικασίας επαλήθευσης, οι οποίες όμως είναι αμοιβαία αποκλειόμενες, οι νεοδημιουργηθέντες ΔιΣ θα πρέπει να εξεταστούν εκ νέου προκειμένου να αποφευχθούν οι αντίστοιχες παραβιάσεις, καθώς κάτι τέτοιο δεν είναι ανιχνεύσιμο κατά την εξαγωγή των αρχικών οδηγιών.

Στη συνέχεια περιγράφονται με περισσότερη λεπτομέρεια οι βασικότερες από τις μεθόδους που καλεί ο παραπάνω αλγόριθμος.

8.2 Δημιουργία και Συνένωση Υπογράφων–Στιγμιοτύπων

Ο σχηματισμός υπογράφων έχει συχνά αποτελέσει αντικείμενο έρευνας καθαυτός (π.χ., [433]), οι προτεινόμενες λύσεις ωστόσο δεν είναι ευθέως εφαρμόσιμες στην παρούσα διατριβή, καθώς είτε βασίζονται σε συγκεκριμένα δομικά χαρακτηριστικά των κυριότερων υπαρχόντων γλωσσών περιγραφής ροών εργασιών που απουσιάζουν από τον τρόπο προδιαγραφής που παρουσιάστηκε στο Κεφάλαιο 6 (π.χ., χρήση ειδικών πυλών OR, XOR, AND, κλπ.), είτε αγνοούν ιδιότητες που η ακολουθούμενη προσέγγιση λαμβάνει υπόψη (π.χ., ο ορισμός ποικίλων και συνδεόμενων μεταξύ τους περιορισμών). Στην προτεινόμενη μεθο-

δολογία η δημιουργία των υπογράφων ενός γράφου ροής εργασιών βασίζεται στη λογική ότι αν ο τελευταίος περιλαμβάνει εργασίες από τις οποίες εξέρχονται περισσότερες της μίας ακμές που χαρακτηρίζονται από διαφορετικές συνθήκες πλαισίου ή ίδιου τύπου αλλά διαφοροποιημένη μεταφερόμενη πληροφορία, τότε οι διάφοροι υπογράφοι–στιγμιότυπα θα προκύπτουν από τους διαφορετικούς συνδυασμούς των μονοπατιών που εκκινούν από τις εργασίες αυτές. Κάθε υπογράφος εκπροσωπείται από μια δομή η οποία περιλαμβάνει τις ακμές που τον συναπαρτίζουν. Καθώς πραγματοποιείται διάσχιση του γράφου ακολουθώντας την τοπολογική ταξινόμηση των κόμβων–εργασιών, οι δομές αυτές τροποποιούνται κατάλληλα. Συγκεκριμένα, αν μια εργασία έχει είτε μία είτε περισσότερες εξερχόμενες ακμές που όμως δεν ορίζουν εναλλακτικά μονοπάτια, αλλά ενεργοποίηση όλων των εξερχόμενων κλάδων (AND-split), οι ακμές αυτές προστίθενται σε όλες τις δομές υπογράφων που περιλαμβάνουν τουλάχιστον μία ακμή με προορισμό τη θεωρούμενη εργασία. Η τοπολογική ταξινόμηση εξασφαλίζει επιπλέον ότι, κατά τη διαδικασία αυτή, όλες οι ακμές που έχουν ως προορισμό μια εργασία έχουν τοποθετηθεί κατάλληλα στις δομές υπογράφων, πριν η εν λόγω εργασία μελετηθεί, ώστε να μην προκύπτει απώλεια ακμών από τους αντίστοιχους υπογράφους. Αν, από την άλλη, οι εξερχόμενες ακμές ορίζουν, βάσει των περιορισμών που τις συνοδεύουν, διακριτές περιπτώσεις αναφορικά με τη μετέπειτα ροή (OR/XOR-split), υπολογίζονται καταρχήν οι περιπτώσεις αυτές κατά τέτοιο τρόπο ώστε να μην υπάρχει καμία μεταξύ τους επικάλυψη (XOR-split). Για το σκοπό αυτό γίνεται χρήση μιας απλής *άλγεβρας περιορισμών*, η οποία παρέχει κάποιες βασικές λειτουργίες που επιτρέπουν τον υπολογισμό όλων των αμοιβαία αποκλειόμενων *διαστημάτων περιορισμών* με βάση τις εκάστοτε εξερχόμενες ακμές. Στη συνέχεια, για κάθε τέτοιο διάστημα, επιλέγονται οι μεταβάσεις εκείνες που εμπίπτουν στους αντίστοιχους περιορισμούς και προκύπτουν νέες ακμές που συνδέονται με αυτούς, έτσι ώστε συνολικά οι προκύπτουσες ακμές ανά δύο μεταξύ τους να χαρακτηρίζονται είτε από ακριβώς ίδιους είτε από μη συμβατούς περιορισμούς. Κατ' αυτό τον τρόπο, για κάθε εργασία που ορίζει εναλλακτικούς εξερχόμενους κλάδους, δημιουργούνται τόσοι υπογράφοι όσα είναι τα διαφορετικά διαστήματα περιορισμών, καθένας από τους οποίους περικλείει τις εξερχόμενες ακμές που βάσει της αρχικής προδιαγραφής θα ενεργοποιηθούν αν οι αντίστοιχοι περιορισμοί ισχύσουν.

Τέλος, κεντρική ιδέα της διαδικασίας συνένωσης των επαληθευμένων υπογράφων–στιγμιοτύπων είναι ότι τα κοινά τμήματα μεταξύ των υπογράφων συγχωνεύονται, ενώ εκείνα στα οποία διαφοροποιούνται προστίθενται αυτούσια στην τελική έγκυρη προδιαγραφή της ροής εργασιών. Για το σκοπό αυτό, κάθε υπογράφος συγκρίνεται διαδοχικά με τους υπόλοιπους. Σε κάθε βήμα της σύγκρισης, τα θεωρούμενα τμήματα είτε προκύπτουν κοινά, οπότε προστίθενται στην τελική ροή μόνο αν δεν έχουν ήδη προστεθεί, είτε διαφοροποιούνται με τον υπογράφο αναφοράς, οπότε και προστίθενται ούτως ή άλλως. Με αυτό τον τρόπο "χτίζεται" διαδοχικά η επαληθευμένη ροή εργασιών. Αξίζει να σημειωθεί ότι οι διαδικασίες συνένωσης δεν είναι ιδιαίτερα κρίσιμες για τους σκοπούς της διατριβής, καθώς δεν αφορούν τον έλεγχο καθεαυτό, ο οποίος σε αυτό το σημείο έχει ήδη επιτευχθεί. Ωστόσο βελτιώνουν σημαντικά την αναγνωσιμότητα (readability) της προκύπτουσας επαληθευμέ-

νης ροής εργασιών, ενώ —το κυριότερο— καθιστούν δυνατή την εξαγωγή περισσότερο συμπαγών, περιεκτικών και διαχειρίσιμων εντολών εκτέλεσης προς τους υποκείμενους Πράκτορες κατά τα μετέπειτα φάση της εκτέλεσης, ώστε οι προδιαγεγραμμένες νόρμες τελικά να εφαρμοστούν. Η συνένωση ροών εργασιών είναι ένα σύνθετο πρόβλημα αφεαυτής, το οποίο έχει απασχολήσει τη βιβλιογραφία [434][435] και, ως εκ τούτου, δεν αναλύεται στα πλαίσια του παρόντος διεξοδικά.

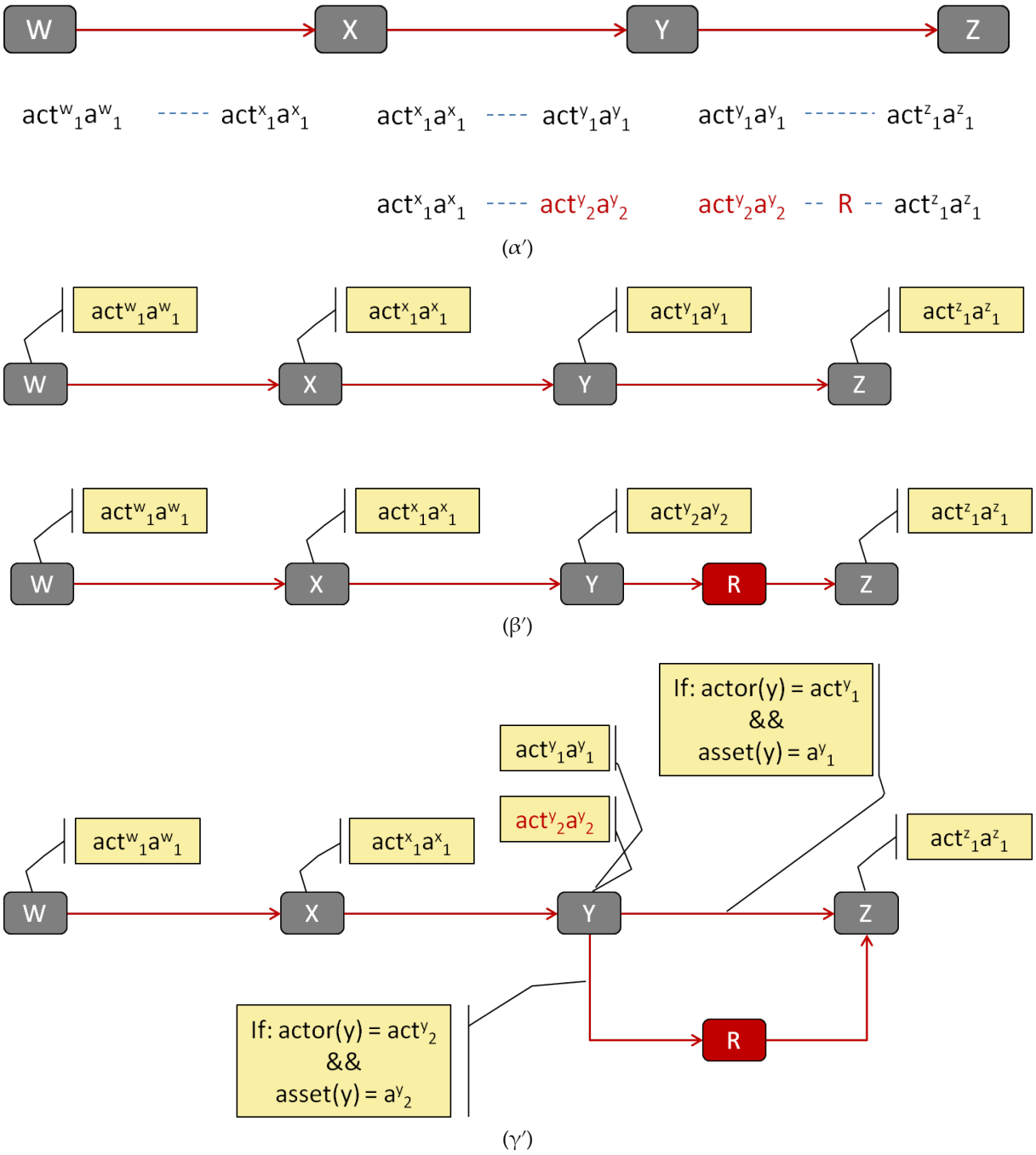
8.3 Δημιουργία και Συνένωση Περιπτώσεων Εκτέλεσης

Με αφετηρία τις εργασίες και ακμές, όπως αυτές έχουν αρχικά οριστεί από το χρήστη και ενδεχομένως μετασχηματιστεί, στη συνέχεια, κατά τη δημιουργία των υπογράφων, οι έγκυρες προδιαγραφές τους προκύπτουν μέσω του σχηματισμού των περιπτώσεων εκτέλεσης κάθε υπογράφου στη βάση των αντίστοιχων ΟΕΔιΣ. Για το σκοπό αυτό, αρχικά προσδιορίζονται τα έγκυρα ζεύγη σκοπών–εκκινητών *VPIP*, εκείνα, δηλαδή, στα οποία αναφέρεται τουλάχιστον μία ΟΕΔιΣ. Στη συνέχεια, για κάθε υπογράφο και για κάθε έγκυρο ζεύγος εντοπίζονται εκείνες οι ΟΕΔιΣ που αφορούν στο συγκεκριμένο ζεύγος σκοπού–εκκινητή και στους ΔιΣ που περιλαμβάνονται στον υπογράφο. Με βάση τις οδηγίες αυτές, οι παραγόμενες περιπτώσεις εκτέλεσης που αντιστοιχούν στον υπογράφο είναι τόσες όσοι είναι οι διαφορετικοί συνδυασμοί των έγκυρων προδιαγραφών εργασιών και ακμών για όλα τα έγκυρα ζεύγη σκοπών–εκκινητών[32].

Ως παράδειγμα των ανωτέρω, το Σχήμα 18 δείχνει τη δημιουργία των περιπτώσεων εκτέλεσης μιας απλής ροής εργασιών, αποτελούμενης από τις υποθετικές εργασίες W, X, Y, και Z, και τη συνένωσή τους μετέπειτα. Το Σχήμα 18α′ περιλαμβάνει την αρχική ροή και τις ΟΕΔιΣ κάτω από κάθε αντίστοιχο ΔιΣ, όπου, θεωρώντας το ίδιο έγκυρο ζεύγος σκοπού–εκκινητή, κάθε ζεύγος $\langle act_i^t, a_i^t \rangle$ συμβολίζει την προδιαγραφή της εργασίας t ως προς το δράστη (act) και το αντικείμενο επενέργειας (a), δεδομένου ότι η λειτουργία παραμένει ίδια με την αρχική, ενώ μεταξύ δύο γειτονικών προδιαγραφών μπορεί να ορίζεται και η εκτέλεση επιπλέον εργασιών (οι προδιαγραφές των αντίστοιχων ακμών δεν εμφανίζονται για λόγους απλότητας). Όπως παρατηρούμε, στη συγκεκριμένη περίπτωση, για την εργασία Y, και σε συνδυασμό με τις γειτονικές της, ορίζονται δύο επιτρεπτοί συνδυασμοί δραστών και αντικειμένων επενέργειας, ενώ για το δεύτερο απαιτείται η επιπρόσθετη εκτέλεση της εργασίας R μεταξύ των εργασιών Y και Z. Η προκύπτουσες περιπτώσεις εκτέλεσης απεικονίζονται στο σχήμα 18β′.

Επίσης, κατά τη δημιουργία των περιπτώσεων εκτέλεσης λαμβάνει χώρα και η *αποσύνθεση (decomposition)* σύνθετων εργασιών σε επιμέρους, η οποία μπορεί να λάβει δύο μορφές: α) την αντικατάσταση της εργασίας αναφοράς από ένα μέλος της `DirTaskNodes`

[32]Σημειώνεται ότι οι ακμές μπορεί αρχικά να είναι ουδέτερα ορισμένες από το χρήστη, δηλαδή να μην προσδιορίζονται ούτε ως ελέγχου ούτε ως δεδομένων, αλλά να αποτελούν μέλη της κλάσης `Edges`. Σε αυτή την περίπτωση οι τύποι των ακμών προκύπτουν από τις αντίστοιχες ΟΕΔιΣ, που πάντα τους προσδιορίζουν, και έτσι εμπερικλείονται στην επαληθευμένη μορφή της ροής εργασιών.



Σχήμα 18: Παράδειγμα δημιουργίας και συνένωσης περιπτώσεων εκτέλεσης.

(βλ. Ενότητα 7.2) ανά περίπτωση εκτέλεσης, με λειτουργία, όμως, διαφορετική από αυτήν της αρχικής εργασίας, με την οποία συνδέεται στην Οντολογία Σημασιολογικού Μοντέλου Πληροφοριών (ΟΣΜΠ) με σχέση *isA* (XOR-decomposition, αν η λειτουργία αλλάζει μεταξύ των περιπτώσεων εκτέλεσης), ή β) την αντικατάσταση της εργασίας αναφοράς από περισσότερα του ενός μέλη της `DirTaskNodes` ανά περίπτωση εκτέλεσης, οι λειτουργίες των οποίων συνδέονται με αυτήν της αρχικής εργασίας με σχέσεις *isPartOf* (AND-decomposition).

Η συνένωση των περιπτώσεων εκτέλεσης μετά το πέρας της επαλήθευσής τους, από την άλλη, συνίσταται στην ενοποίηση των εναλλακτικών προδιαγραφών, οδηγώντας σε διάφορα ενδιαφέροντα επιμέρους αποτελέσματα, όπως είναι τα ακόλουθα: α) η αποσύνθεση τύπου (αποκλειστικής) διάζευξης (XOR decomposition) σύνθετων λειτουργιών που συμμετέχουν σε εργασίες αναφοράς, δηλαδή ο ορισμός, για την ίδια εργασία, διαφορετικών υπολειτουργιών που μπορούν να την υλοποιήσουν, υπό συνθήκη ή όχι, μέσω της αντιστοίχισης διαφορετικών λειτουργιών στην ίδια εργασία αναφοράς ανά περίπτωση εκτέλεσης (βλ. παραπάνω)· β) ο ορισμός πολλαπλών προφίλ εκτέλεσης για την ίδια εργασία· γ) ο ορισμός εναλλακτικών διαδρομών μεταξύ των ίδιων εργασιών, σε εξάρτηση με την κατά τα άλλα δομή της ροής εργασιών ή άλλου είδους συνθήκες. Οι μεταβλητές ροής εργασιών καθίστανται ιδιαίτερα χρήσιμες κατά το στάδιο αυτό, ιδιαίτερα αν ληφθεί υπόψη το γεγονός ότι οι διαφοροποιήσεις μεταξύ των περιπτώσεων εκτέλεσης μπορεί να οφείλονται σε παράγοντες όπως ο σκοπός, ο εκκινητής ή οι προδιαγραφές των ΔιΣ καθεαυτές. Έτσι, αντίστοιχες εκφράσεις συνθηκών και περιορισμών θα πρέπει να δημιουργούνται σε σχέση, πρακτικά, με κάθε διαφοροποίηση, και να θεωρούνται κατάλληλα. Για παράδειγμα, στο Σχήμα 18γ′, το οποίο απεικονίζει τη συνένωση των περιπτώσεων εκτέλεσης του Σχήματος 18β′[33], προκύπτουν δύο προφίλ εκτέλεσης για την εργασία Y, ενώ ο κλάδος που περιλαμβάνει την εργασία R ακολουθείται μόνο αν ο δράστης και το αντικείμενο επενέργειας της Y είναι εκείνα που ορίζονται από την αντίστοιχη περίπτωση εκτέλεσης.

8.4 Εφαρμογή Νορμών Απαγόρευσης

Η εφαρμογή των εν λόγω Νορμών (μέθοδος ApplyForbiddanceNorms, Αλγόριθμος 1) περιλαμβάνει την εξέταση μιας περίπτωσης εκτέλεσης *c* ως προς τις ΟΑπΕκ και ΟΑπΡ που την αφορούν, θεωρώντας κάθε εργασία *t* που περιλαμβάνεται σε αυτή κατά σειρά τοπολογικής ταξινόμησης.

Αναφορικά με την εφαρμογή κάθε οδηγίας ΟΑπΕκ *tfd* που αφορά μια εργασία *t* (ιδιότητα `refersToTask`), η διαδικασία έχει, στη γενική περίπτωση, ως εξής (βλ. Αλγόριθμο 2): αρχικά εξάγονται από την *tfd* η εργασία που απαγορεύεται να εκτελεστεί $task_f$, οι σχετικές θέσεις $positions_f$ τις οποίες δεν πρέπει να καταλαμβάνει, και οι οποίες λαμβάνουν τιμές από το σύνολο {*before*, *after*, *parallel*, *tight_parallel*, *anywhere*, *on_data_path*}[34] (βλ. Ενότητα 7.1), και, τέλος, οι πιθανές συνθήκες πλαισίου $context_f$ υπό τις οποίες ισχύει η απαγόρευση. Έπειτα, αναζητείται η εργασία $task_f$ σε καθεμιά από τις θέσεις $positions_f$ (γρ. 6). Η αναζήτηση συνίσταται στον εντοπισμό μιας εργασίας η οποία χαρακτηρίζεται από λειτουργία (operation) και παραμέτρους (operation parameters) ταυτόσημες με της $task_f$ και από δράστες (actors) και αντικείμενα επενέργειας (assets) που είτε ταυτίζονται με είτε εμπερικλείουν στον ορισμό τους (π.χ., μέσω λογικών σχέσεων) τους δράστες και τα αντικεί-

[33]Θεωρώντας ότι δεν εισάγονται περαιτέρω τροποποιήσεις κατά τον έλεγχό τους.

[34]Η τιμή *on_data_path* νοείται μόνο σε συνδυασμό με κάποια άλλη και δεν αποτελεί μόνη της ξεχωριστή θέση.

μενα επενέργειας της $task_f$. Αν εντοπιστεί κάποια τέτοια εργασία (conflicting task) $task_c$ στη συγκεκριμένη θέση, το γεγονός αντιμετωπίζεται διαφορετικά ανάλογα με τα χαρακτηριστικά της. Έτσι, αν ο ορισμός της είναι ίδιος ακριβώς με εκείνον της $task_f$ και η οδηγία δεν περιορίζεται από κάποια συνθήκη πλαισίου, ισχύει, δηλαδή, σε κάθε περίπτωση, τότε η περίπτωση εκτέλεσης συνολικά πρέπει να απορριφθεί (γρ. 7-9). Αν, αντίθετα, ορίζεται συνθήκη πλαισίου, τότε απαιτείται κατάλληλη διευθέτηση της σύγκρουσης (γρ. 11), ώστε να μην επιτραπεί η εκτέλεση των μεταξύ τους ασύμβατων εργασιών, ωστόσο με όσο το δυνατόν λιγότερες "απώλειες" αναφορικά με την τελική εκτέλεση της ροής. Σε αυτή την κατεύθυνση, η προσέγγιση που επελέγη είναι να τροποποιηθεί το προφίλ εκτέλεσης της εργασίας *t*, ώστε η τελευταία να εκτελείται μόνο όταν δεν ισχύει το $context_f$. Με άλλα λόγια, αν $context_t$ είναι η συνθήκη πλαισίου του προφίλ εκτέλεσης $executionProfile_t$ της *t*, αυτό θα μετασχηματιστεί σε $context_t \cap \neg context_f$[35]. Από την άλλη, αν η εργασία $task_c$ εμπερικλείει δυνητικά κάποιους έγκυρους συνδυασμούς δραστών–αντικειμένων επενέργειας, το προφίλ εκτέλεσής της μετασχηματίζεται, ούτως ώστε να περιλαμβάνει μόνο τους έγκυρους αυτούς συνδυασμούς (γρ. 13-14). Για παράδειγμα, αν η εργασία $task_f$ ορίζει κάποιο αντικείμενο επενέργειας a_f το οποίο περιλαμβάνεται μεταξύ πολλαπλών αντικειμένων επενέργειας της $task_c$, οριζόμενων με τη βοήθεια μιας σχέσης σύζευξης (AND-relation), το εν λόγω αντικείμενο επενέργειας αφαιρείται από τη λογική σχέση. Όμοια, λαμβάνονται υπόψη και οι τυχόν περιορισμοί στους δράστες ή/και τα αντικείμενα επενέργειας της $task_f$ (actor constraints και asset constraints, αντίστοιχα, βλ. Ενότητα 6.3.1), ώστε τα τελικά προφίλ εκτέλεσης της $task_c$ να περιλαμβάνουν υποσύνολα των δραστών ή αντικειμένων επενέργειας που χαρακτηρίζονται από τις αρνήσεις (negations) των περιορισμών αυτών. Αν μετατροπές όπως οι παραπάνω δεν είναι δυνατές, η περίπτωση εκτέλεσης απορρίπτεται.

Μια απαγόρευση που αφορά συγκεκριμένο μονοπάτι δεδομένων (προφίλ συμβατότητας *on_data_path*) υποδηλώνει ότι η απαγορευμένη εργασία δε θα πρέπει να εκτελείται πάνω σε δεδομένα που σχετίζονται με κάποια είσοδο ή έξοδο (ανάλογα με άλλες τιμές του προφίλ συμβατότητας) της εργασίας αναφοράς. Για το σκοπό αυτό, αρχικά εντοπίζονται τα σχετικά μονοπάτια δεδομένων γύρω από την εργασία αναφοράς που περιλαμβάνουν, με συνεχή τρόπο (χωρίς, δηλαδή, να διακόπτεται η ροή της πληροφορίας), μεταξύ της μεταφερόμενης πληροφορία είδη δεδομένων (ως προς τον τύπο και άλλα χαρακτηριστικά) που περιέχονται στα δεδομένα τα οριζόμενα ως αντικείμενα επενέργειας της $task_f$. Αν η τελευταία περιλαμβάνεται σε κάποιο από αυτά τα μονοπάτια, θεωρούμε ότι υπάρχει σύγκρουση, η οποία αντιμετωπίζεται με τους παραπάνω τρόπους.

Κατά τον έλεγχο μιας ΟΑπΡ, η απαγορευμένη εργασία $task_f$ (ιδιότητα `forbidsTaskFlow`) αναζητείται μεταξύ εκείνων που στέλνουν σε ή λαμβάνουν από την εργασία *t* δεδομένα —αναλόγως της τιμής του προφίλ συμβατότητας, το οποίο σε σχέση με την κατεύθυνση της ροής μπορεί να πάρει μία από τις τιμές {*incoming*, *outgoing*}— ενώ λαμβάνεται υπόψη επιπρόσθετα το είδος της μεταφερόμενης πληροφορίας. Στην περίπτωση που υπάρ-

[35]Προφανώς, αν δεν ορίζεται εξαρχής κάποιο $context_t$, αυτό τελικά θα παίρνει απλά την τιμή $\neg context_f$.

Αλγόριθμος 2 Check forbiddance

Input: *c*, *t*, *tfd*
Output: *vc*

```
1:  vc ← c
2:  task_f ← tfd.forbidsTasks
3:  positions_f ← tfd.complianceProfile
4:  context_f ← tfd.appliesUnderContext
5:  for each position_f in positions_f do
6:     task_c ← LocateTask (task_f, position_f, t, vc)
7:     if ExactMatch(task_f, task_c) then
8:        if context_f == null then
9:           vc ← null /* case rejected */
10:       else
11:          vc ← HandleConflictExactMatch(context_f, t, vc)
12:       end if
13:    else if PartialMatch(task_f, task_c) then
14:       vc ← HandleConflictPartialMatch(task_f, task_c, vc)
15:    end if
16: end for
17: return vc
```

χει εξάρτηση από συνθήκες πλαισίου, αυτό δεν επηρεάζει το προφίλ εκτέλεσης της *t* αλλά την ακμή *e* που σηματοδοτεί την απαγορευμένη ροή, οπότε και οι συνθήκες $cond_e$ μετασχηματίζονται σε $cond_e \cap \neg context_f$ (ή, αν δεν προϋπάρχουν, $\neg context_f$). Επιπλέον, παρόμοια με τον έλεγχο των ΟΑπΕκ, μπορεί να προκύψουν έγκυρες προδιαγραφές–υποπεριπτώσεις της $task_c$. Και εδώ το αρχικό προφίλ εκτέλεσης της $task_c$ τροποποιείται ώστε να περιλαμβάνει μόνο τις έγκυρες αυτές υποπεριπτώσεις. Αν αυτό δεν είναι δυνατό, το επόμενο βήμα είναι να αναζητηθούν έγκυρες υποπεριπτώσεις των ανταλλασσόμενων δεδομένων μέσω του κατάλληλου ορισμού περιορισμών στις αντίστοιχες μονάδες πληροφορίας (βλ. Ενότητα 6.3.3), που συνίστανται ουσιαστικά στην άρνηση των περιορισμών που ορίζονται μέσω της ιδιότητας `forbidsInfoFlow`. Σε αυτή την περίπτωση, δημιουργείται επιπλέον ακμή *e′* που μεταφέρει τα επιτρεπτά (αν υπάρχουν) δεδομένα για $cond_e \cap context_f$, ενώ τροποποιούνται αντίστοιχα και οι συνθήκες της *e*.

Αν επιπλέον ορίζεται προφίλ συμβατότητας άμεσης σύνδεσης (*direct_binding*) ή σύνδεσης μονοπατιού (*path_binding*)[36], αυτό σημαίνει ότι η απαγόρευση αφορά την περίπτωση που η $task_c$ επεξεργάζεται δεδομένα τα οποία είτε προέρχονται από το πρώτο μέλος του υπό εξέταση ΔιΣ (άμεση σύνδεση) είτε από κάποια άλλη εργασία που ανήκει στο *μονοπάτι δεδομένων* (data path) που καταλήγει στην εργασία του ΔιΣ που ενεργοποιεί την απαγόρευση (σύνδεση μονοπατιού). Έτσι, προκειμένου να υπάρχει σύγκρουση, θα πρέπει η απαγορευμένη εργασία να συνδέεται με συγκεκριμένο τρόπο με την υπόλοιπη ροή εργασιών.

Σε αυτό το σημείο χρήζουν επεξήγησης κάποιες πτυχές του τρόπου χειρισμού των

[36]Ισχύουν μόνο για περιπτώσεις εισερχόμενης ροής.

συνθηκών πλαισίου (context), ο οποίος, παρότι δεν αποτελεί αντικείμενο της διατριβής καθεαυτός και ως εκ τούτου λόγω της πολυπλοκότητάς του δε διερευνάται σε βάθος, ωστόσο αντιμετωπίζεται με στοιχειώδη τρόπο ώστε να εξασφαλιστούν οι στόχοι του προτεινόμενου συστήματος. Γενικά, και αναφορικά με όλα τα είδη οδηγιών, θεωρούμε τα εξής:

1. Οι συνθήκες πλαισίου ενός προφίλ εκτέλεσης μιας εργασίας αποτιμώνται κατά την έναρξη της εκτέλεσης αυτής.
2. Οι συνθήκες πλαισίου μιας ακμής αποτιμώνται κατά την ολοκλήρωση της εκτέλεσης της εργασίας–αφετηρίας.
3. Οι συνθήκες πλαισίου μπορεί να μεταβάλλονται κατά τη διάρκεια της εκτέλεσης μιας εργασίας.
4. Οι συνθήκες πλαισίου διατηρούνται κατά μήκος μιας ακμής. Δηλαδή, οι συνθήκες που ισχύουν όταν η εργασία–αφετηρία στέλνει δεδομένα (ή απλά τη σκυτάλη εκτέλεσης) θεωρούμε ότι ισχύουν και όταν η εργασία–προορισμός τα λάβει.
5. Οι συνθήκες πλαισίου μπορεί να μεταβάλλονται από τη στιγμή που μια εργασία λάβει δεδομένα μέχρι τη στιγμή που τελικά θα εκτελεστεί.
6. Κάθε εργασία αποστέλλει ταυτόχρονα, με την ολοκλήρωσή της, όλα τα δεδομένα τα οποία παράγει.
7. Μια εργασία ξεκινάει να εκτελείται τη στιγμή που έχει διαθέσιμα όλα τα δεδομένα που πρέπει για το πλαίσιο που ισχύει όταν λαμβάνει το καθένα.

Έτσι, για τους παραπάνω λόγους, στις ΟΑπΕκ, που δεν αφορούν σχέσεις άμεσης γειτνίασης, δε λαμβάνουμε υπόψη τις συνθήκες πλαισίου παρά μόνο σε σχέση με την εργασία αναφοράς κάθε φορά, αφού ως προς αυτές ορίζεται η υπό συνθήκη απαγόρευση. Από την άλλη, κατά την εφαρμογή των ΟΑπΡ οι συνθήκες πλαισίου μπορούν να τροποποιούν τις εισερχόμενες ή εξερχόμενες ροές, καθώς αυτό που μας αφορά είναι η ροή συνολικά να μη λαμβάνει χώρα από τη στιγμή που οι συνθήκες πλαισίου αρχίζουν να ισχύουν και μετά (οπότε και οι αντίστοιχες εργασίες δε θα εκτελούνται επί δεδομένων που προέρχονται από μια απαγορευμένη ροή).

Όπως προαναφέρθηκε, και με βάση τον Αλγόριθμο 1, τόσο στην αρχή όσο και στο τέλος της επαλήθευσης μιας περίπτωσης εκτέλεσης (γρ. 19 και 29) ελέγχονται όλες οι ΟΑπΕκ και ΟΑπΡ. Ωστόσο κάποιες βελτιστοποιήσεις είναι δυνατές μέσω κάποιας κατανομής των οδηγιών μεταξύ των δύο φάσεων ελέγχου των απαγορεύσεων. Για παράδειγμα, θα μπορούσαν στην αρχή να ελέγχονται μόνο οι απόλυτες ΝΑ, αφήνοντας για το τέλος τις υπό συνθήκη (ώστε να ληφθούν υπόψη ενδεχόμενες τροποποιήσεις της ροής) καθώς και εκείνες μόνο μεταξύ των απόλυτων ΝΑ που η ισχύς τους δεν μπόρεσε να διαπιστωθεί —και, κατά συνέπεια, δε διευθετήθηκαν— κατά την πρώτη φάση.

Τέλος, σημειώνεται ότι η αναζήτηση μεμονωμένων εργασιών (μέθοδος LocateTask, Αλγόριθμος 2) επεκτείνεται με κατάλληλες προσαρμογές, όπως και σε όλες τις περιπτώσεις που ακολουθούν, ώστε να καλύπτει και την περίπτωση της αναζήτησης δομών εργασιών.

8.5 Εφαρμογή Νορμών Άμεσης Σύνδεσης

Οι ΝΑΣ περιλαμβάνουν τις οδηγίες απαίτησης εισόδου (ΟΑΕισ), απαίτησης εξόδου (ΟΑΕξ) και απαίτησης εκτέλεσης (ΟΑΕκ) με προφίλ συμβατότητας *αμέσως πριν* (*immediately_before*), *αμέσως μετά* (*immediately_after*), *συμπληρωματική παράλληλη εκτέλεση* (*complementary_parallel_execution*) και *συμπληρωματική παράλληλη επεξεργασία* (*complementary_parallel_processing*). Οι ΝΑΣ που αφορούν μια εργασία *t* ελέγχονται όλες μαζί κατά τη διάρκεια μιας διάσχισης της περίπτωσης εκτέλεσης *c* με βάση την τοπολογική ταξινόμηση των εργασιών (μέθοδος ApplyDirectNorms, Αλγόριθμος 1).

8.5.1 Εφαρμογή ΟΑΕισ

Μια ΟΑΕισ, στην απλή περίπτωση, προϋποθέτει ότι σε όλα τα πιθανά εναλλακτικά μονοπάτια που οδηγούν στην t (αν ορίζονται περισσότερα του ενός) περιλαμβάνεται η απαιτούμενη εργασία t_r (ιδιότητα `requiresInputFrom`) και παρέχει στην *t* δεδομένα d_r (ιδιότητα `requiresInput`). Έτσι, σε κάθε τέτοιο μονοπάτι, αν η t_r περιλαμβάνεται μεταξύ των αμέσως (δηλ. συνδεόμενων μέσω μιας ακμής) προηγούμενων εργασιών της t και η ακμή που τις ενώνει περιλαμβάνει όλα τα απαραίτητα δεδομένα, η οδηγία ικανοποιείται. Διαφορετικά, αν κάποια δεδομένα εκ των d_r απουσιάζουν, προστίθεται ακμή μεταξύ των δύο εργασιών που μεταφέρει τα επιπλέον δεδομένα. Αν η οδηγία συμπληρώνεται από συνθήκες πλαισίου $context_r$, το τελευταίο χαρακτηρίζει και την προστιθέμενη ακμή, είτε αυτόνομα είτε με την τομή του με το, αν υπάρχει, ήδη οριζόμενο *context* μεταξύ των δύο εργασιών[37]. Από τη άλλη, αν η t_r δε βρίσκεται σε άμεση προηγούμενη σύνδεση με την *t*, προστίθεται ως εξής: δημιουργείται νέα εργασία t_a με την προδιαγραφή της t_r και συνθήκη πλαισίου του προφίλ εκτέλεσης $context_r$, η οποία συνδέεται με την *t* με ακμή που μεταφέρει τα δεδομένα d_r και ισχύει επίσης για $context_r$. Από εκεί και πέρα πρέπει επίσης να εξεταστεί ο τρόπος σύνδεσης της t_a με τη ροή εργασιών. Για το σκοπό αυτό υποβάλλεται κατάλληλο ερώτημα στη Μηχανή Συμπερασμού, από την απάντηση στο οποίο προκύπτει το αν η t_a απαιτεί την προσθήκη επιπλέον εργασιών, αν μπορεί να λάβει δεδομένα απαραίτητα για την εκτέλεσή της από κάποια άλλη προηγούμενη εργασία, οπότε και προστίθεται η αντίστοιχη ακμή με τα εν λόγω δεδομένα, ή, τέλος, αν δεν απαιτεί επιπλέον πληροφορία, οπότε συνδέεται με ακμή ελέγχου με κάποια εργασία αμέσως προηγηθείσα της *t*. Οι ακμές αυ-

[37]Για το ίδιο μονοπάτι, θεωρούμε ότι αν συγκλίνουν στην *t* περισσότερες από μία εισερχόμενες ακμές, συνδέονται με την *t* με τις ίδιες συνθήκες πλαισίου *context*. Ωστόσο, αν η *t* έχει τιμή *false* στις ιδιότητες `isControlSync`, `isDataSync`, οι εισερχόμενες ακμές σηματοδοτούν στην ουσία ξεχωριστά μονοπάτια.

τές χαρακτηρίζονται από συνθήκες πλαισίου ίδιες με εκείνες που συνδέουν την εργασία που παρέχει την απαραίτητη είσοδο στην t_a με το μονοπάτι που οδηγεί στην t. Με αυτό τον τρόπο, τα απαραίτητα δεδομένα γίνονται διαθέσιμα συνεχώς στην t_a, η οποία όμως εκτελείται μόνο αν ισχύει $context_r$, και αν το τελευταίο εξακολουθεί να ισχύει όταν η t_a ολοκληρωθεί ή όταν συμβεί αυτό, τότε τα d_r δρομολογούνται στην t. Συνεπώς, κάθε φορά που η t είναι σε θέση να εκτελεστεί με βάση τις υπόλοιπες εισερχόμενες ροές και ισχύει το $context_r$, θα έχει λάβει και τα δεδομένα d_r.

Μια ΟΑΕισ με προφίλ συμβατότητας που υποδεικνύει άμεση σύνδεση (direct_binding) αναφέρεται κατά κανόνα στο δεύτερο (ή, γενικότερα, τελευταίο) μέλος ενός έγκυρου ΔιΣ για να δηλώσει ότι η t_r πρέπει συγκεκριμένα να συνδέεται με την αμέσως προηγούμενη εργασία t_b της t στον εν λόγω ΔιΣ, με άλλα λόγια η εκτέλεση της t_r να βασιστεί σε δεδομένα τα οποία έτσι κι αλλιώς καταλήγουν στην t. Έτσι, αν η t_b συνδέεται ήδη με κάποια εργασία που συμβαδίζει με τον ορισμό της t_r, πρέπει αρχικά να διασφαλιστεί ότι αυτό εμπερικλείει το τυχόν πλαίσιο *context* που οδηγεί στην t με βάση το θεωρούμενο ΔιΣ. Στη συνέχεια, αν τα d_r δε μεταφέρονται εξολοκλήρου στην t, και μάλιστα υπό κατάλληλες συνθήκες πλαισίου, προστίθεται και πάλι μία κατάλληλη ακμή με d_r ή το τμήμα τους που λείπει και $context_r$. Αν, από την άλλη, δεν υπάρχει η επιθυμητή εργασία στη θέση αυτή, προστίθενται μια νέα t_a και οι ακμές που τη συνδέουν με τις t_b και t, και οι οποίες πρέπει να περιλαμβάνουν, αντίστοιχα, τα δεδομένα που η t_b πρέπει να παράσχει στην t_a υπό συνθήκες πλαισίου *context* και τα δεδομένα d_r που η t_a πρέπει να παράσχει στην t υπό συνθήκες $context_r$. Και εδώ, το προφίλ εκτέλεσης της t_a θα πρέπει να ικανοποιεί το $context_r$.

Ένα προφίλ συμβατότητας σύνδεσης μονοπατιού (path_binding) υποδηλώνει ότι η t_r πρέπει να ανήκει σε ή να συνδέεται με σχέσεις δεδομένων εισόδου με το μονοπάτι που οδηγεί στην t. Στην πρώτη περίπτωση, αν δηλαδή βρεθεί μεταξύ προγενέστερων εργασιών μια εργασία t_b που ακολουθεί των ορισμό της t_r, χωρίς όμως ακμή που να μεταφέρει τα δεδομένα d_r στη t καλύπτοντας το $context_r$, θα πρέπει να προστεθεί ακμή μεταφέροντας τα κατάλληλα δεδομένα και με πλαίσιο $context_r$ ή $context_r \cap context$, όπου *context* το πλαίσιο που συνδέει την t_b με το υπόλοιπο μονοπάτι προς την t (αντίστοιχα, αν υπάρχει ακμή να τροποποιηθεί κατάλληλα). Έτσι εξασφαλίζεται ότι, από τη στιγμή που κάποιο πλαίσιο έχει ενεργοποιηθεί, τα απαιτούμενα δεδομένα θα καταστούν διαθέσιμα στην t. Αν τέτοια εργασία δε βρεθεί, προστίθεται η αντίστοιχη t_a, ενώ αναζητάται η εργασία εκείνη που θα της προσφέρει την απαιτούμενη είσοδο και που υποχρεωτικά πρέπει να ανήκει στο μονοπάτι το εισερχόμενο στην t, με προτεραιότητα στην εγγύτερη στην t. Σημειώνεται ότι στις περιπτώσεις σύνδεσης είτε άμεσης είτε μονοπατιού, ειδικά στις περιπτώσεις όπου έχουμε συνεχή ροή δεδομένων, απαιτούνται επιπλέον μηχανισμοί οι οποίοι να εγγυώνται τη σε πραγματικό χρόνο συσχέτιση των εμπλεκόμενων δεδομένων, για παράδειγμα μέσω της διατύπωσης επιπλέον περιορισμών ή συνθηκών πλαισίου. Οι μηχανισμοί αυτοί ξεφεύγουν από τους στόχους της παρούσας διατριβής και αποτελούν αντικείμενο μελλοντικής εργασίας.

Επιπλέον των ανωτέρω, είναι πιθανό μια ΟΑΕισ να μην ορίζει την εργασία από την οποία πρέπει να λαμβάνει τα απαιτούμενα δεδομένα, παρά μόνο τα δεδομένα καθεαυτά. Στην περίπτωση αυτή, με την υποβολή επιπλέον ερωτημάτων στη Μηχανή Συμπερασμού, προκύπτει η εργασία που πρέπει να παράσχει την απαιτούμενη πληροφορία καθώς και η ένταξή της στη ροή αν δεν υπάρχει ήδη, μέσω βημάτων που επίσης δεν αναλύονται εδώ διεξοδικά. Τέλος, σε όλες τις παραπάνω περιπτώσεις πραγματοποιείται, αν χρειάζεται, κατάλληλη ρύθμιση της ιδιότητας *isDataSync* (βλ. Ενότητα 6.4.2) της εργασίας αναφοράς *t*, ώστε να εξασφαλιστεί η εκτέλεση της τελευταίας με τη λήψη και των επιπλέον δεδομένων που απαιτούνται κάθε φορά.

8.5.2 Εφαρμογή ΟΑΕξ

Για να διαπιστωθεί η ισχύς μιας ΟΑΕξ ελέγχεται το αν υπάρχει ακμή εξερχόμενη από την εργασία αναφοράς *t* η οποία να μεταφέρει όλα τα απαιτούμενα δεδομένα d_r (ιδιότητα `requiresOutput`) στην εργασία t_r (ιδιότητα `requiresOutputTo`), ικανοποιώντας και τις ενδεχόμενες συνθήκες πλαισίου της οδηγίας. Έτσι, αν δεν υπάρχει εξερχόμενη σύνδεση ανάμεσα στην *t* και μια μεταγενέστερη εργασία t_b που ακολουθεί τον ορισμό της t_r, προστίθεται κατάλληλα η αντίστοιχη εργασία t_a με μια ακμή η οποία μεταφέρει σε αυτήν τα d_r από την *t*. Αν στην οδηγία ορίζεται επιπλέον συνθήκη πλαισίου $context_r$, αυτή αναφέρεται στη στιγμή που η *t*, αφού έχει ολοκληρώσει την εκτέλεσή της, είναι σε θέση να διαθέσει τα δεδομένα. Έτσι η προστιθέμενη ακμή θα χαρακτηρίζεται και από το $context_r$, αυτόνομα ή με την τομή του με ένα άλλο πλαίσιο *context*, το οποίο αναφέρεται κατά περίπτωση: α) στο συνδυασμό των συνθηκών πλαισίου που αφορά όλα τα πιθανά μονοπάτια τα εξερχόμενα από την *t*, αν η ΟΑΕξ αναφέρεται στο τελευταίο μέλος ενός έγκυρου ΔιΣ, ή β) το πλαίσιο που χαρακτηρίζει τη σύνδεση της *t* με το υπόλοιπο τμήμα του ΔιΣ, αν η *t* αφορά το πρώτο μέλος του έγκυρου ΔιΣ. Αν από την άλλη υπάρχει εξερχόμενη σύνδεση ανάμεσα στην *t* και μια μεταγενέστερη εργασία t_b που ακολουθεί τον ορισμό της t_r, η οποία σύνδεση όμως είτε δε μεταφέρει τα d_r ή μέρος αυτών είτε δεν ικανοποιεί τις συνθήκες πλαισίου που περιγράφηκαν παραπάνω, η αντίστοιχη ακμή τροποποιείται κατάλληλα, ενώ ίσως χρειαστεί και η προσθήκη επιπλέον ακμής στην περίπτωση της ελλειπούς μεταφοράς δεδομένων.

Αν η ΟΑΕξ χαρακτηρίζεται ως συνδυαστική (προφίλ συμβατότητας combinative) θα πρέπει όχι μόνο να ακολουθεί την *t* με τον τρόπο που περιγράφηκε παραπάνω, αλλά να συνδέεται και με την εργασία ή εργασίες που έπονται άμεσα της *t*. Αυτό, αν δεν ισχύει ήδη, πραγματοποιείται μέσω μιας ακμής η οποία θα εξασφαλίζει την παροχή στις επόμενες εργασίες των δεδομένων που παράγονται από την προστιθέμενη εργασία t_a. Αν ορίζεται ανασταλτικό προφίλ συμβατότητας (blocking) και δεν προϋπάρχει η αντίστοιχη εργασία κατάλληλα σε κάθε εξερχόμενο μονοπάτι, η t_a θα προστίθεται ομοίως και θα συνδέεται με ακμή ελέγχου με όλες τις αμέσως επόμενες εργασίες, ώστε να διασφαλιστεί ότι εκείνες δε θα εκτελεστούν αν πρώτα δεν έχει ολοκληρωθεί η εκτέλεση της t_a. Και στις δύο αυτές περιπτώσεις, οι ιδιότητες *isControlSync* και *isDataSync* των επόμενων εργασιών θα πρέπει

να τίθενται στην τιμή *true*.

8.5.3 Εφαρμογή ΟΑΕκ

Μια ΟΑΕκ με προφίλ εκτέλεσης αμέσως πριν (immediately_before) επιτάσσει ότι η απαιτούμενη εργασία t_r θα πρέπει να βρίσκεται μεταξύ των αμέσως προηγούμενων εργασιών της *t*. Αν αυτό ισχύει, ανεξαρτήτως των όποιων συνθηκών πλαισίου απαιτούνται, η οδηγία ικανοποιείται. Σε αντίθετη περίπτωση, προστίθεται η ανάλογη εργασία t_a ως εξής: στο αντίστοιχο εισερχόμενο μονοπάτι, όλες οι αμέσως προηγούμενες εργασίες συνδέονται με την t_a μέσω ακμών ελέγχου[38] με πλαίσιο ίδιο με εκείνο που συνδέει τις εν λόγω εργασίες με την *t*, ενώ και η t_a συνδέεται με την *t* μέσω ακμής ελέγχου. Αν ο ορισμός της οδηγίας συμπληρώνεται από συνθήκες πλαισίου $context_r$, οι τελευταίες πρέπει να χαρακτηρίζουν τόσο το προφίλ εκτέλεσης της t_a όσο και και την ακμή που την ενώνει με την *t*. Υπάρχει τέλος και το ενδεχόμενο οι απαιτούμενες συνδέσεις να υπάρχουν εν μέρει (π.χ. κάποια προηγούμενη εργασία να συνδέεται με t_r αλλά όχι σε πλήρη συμφωνία με το απαιτούμενο πλαίσιο, ή να μην υπάρχει ακμή σύνδεσης με την *t*) οπότε σε αυτή την περίπτωση συμπληρώνονται κατάλληλα.

Το προφίλ εκτέλεσης αμέσως μετά (immediately_after) υποδηλώνει ότι η *t* θα πρέπει να έχει, ανά εξερχόμενο μονοπάτι, μία τουλάχιστον εξερχόμενη ακμή η οποία να οδηγεί στην t_r (χωρίς να μεσολαβούν άλλες εργασίες) με συνθήκες που να καλύπτουν το ενδεχόμενο πλαίσιο $context_r$. Αν αυτό δεν ισχύει, είτε τροποποιείται το υπάρχον πλαίσιο είτε προστίθεται εξ ολοκλήρου η κατάλληλη t_a με ακμή η οποία σχετίζεται με τις απαιτούμενες συνθήκες πλαισίου $context_r$. Αν η οδηγία είναι επιπρόσθετα *ανασταλτική* (προφίλ συμβατότητας *blocking*), θα πρέπει να προστεθούν ακμές ελέγχου μεταξύ της t_a και όλων των υπόλοιπων εργασιών που ακολουθούν κατά άμεσο τρόπο την *t*.

Αναφορικά με τις σχέσεις άμεσης παραλληλίας, μια ΟΑΕκ με προφίλ συμβατότητας συμπληρωματικής παράλληλης εκτέλεσης (complementary_parallel_execution) απαιτεί ότι για κάθε ακμή που καταλήγει στην εργασία αναφοράς *t* θα πρέπει να υπάρχει ακμή η οποία θα ενώνει την αφετηρία της υπάρχουσας ακμής με μια άλλη εργασία με τα χαρακτηριστικά της t_r. Η ακμή αυτή θα πρέπει να ορίζεται, κατ' ελάχιστον, με τις ίδιες συνθήκες πλαισίου *context* που συνδέουν την πρώτη ακμή με την *t*, εκτός αν ορίζεται από την οδηγία πλαίσιο $context_r$, οπότε το πλαίσιο που θα πρέπει οπωσδήποτε να καλύπτεται περιορίζεται στο $context_r \cap context$. Αν τα παραπάνω δεν ικανοποιούνται, είτε τροποποιούνται τυχόν υπάρχουσες συνθήκες πλαισίου είτε προστίθενται κατάλληλα η απαιτούμενη εργασία και οι αντίστοιχες ακμές ελέγχου. Αν η οδηγία περιγράφεται ως ανασταλτική (blocking), θα πρέπει να υπάρχουν επιπλέον ακμές ελέγχου που να ενώνουν την t_r με όλες τις εργασίες

[38]Για να είναι επιτυχής η εφαρμογή της οδηγίας, και κατ' επέκταση αποδεκτή η περίπτωση εκτέλεσης, μεταφερόμενη πληροφορία που τυχόν απαιτείται θα πρέπει να παρέχεται από τις αμέσως προηγούμενες εργασίες ή τουλάχιστον μία εξ αυτών. Γενικά, το θέμα της σύνδεσης της t_a στην υπάρχουσα ροή αντιμετωπίζεται με τρόπο παρόμοιο με αυτόν που περιγράφηκε παραπάνω για τις ΟΑΕισ.

οι οποίες έπονται της *t*, ώστε να διασφαλιστεί ότι αυτές θα εκτελεστούν μόνο όταν η t_r θα έχει ολοκληρωθεί. Με παρόμοιο τρόπο αντιμετωπίζεται και η περίπτωση της συμπληρωματικής παράλληλης επεξεργασίας (complementary_parallel_processing), στην οποία όμως λαμβάνονται υπόψη και οι πληροφορίες οι οποίες θα πρέπει να μεταφέρονται στην παράλληλα τοποθετημένη εργασία μέσω ακμών ελέγχου ή δεδομένων και οι οποίες προσδιορίζονται με τη βοήθεια της ΟΣΜΠ στη βάση των αντίστοιχων λειτουργιών (operation) αφετηρίας και προορισμού.

8.6 Εφαρμογή Νορμών Έμμεσης Σύνδεσης Πριν

Οι ΝΕΣΠ περιλαμβάνουν τις οδηγίες ΟΑΕκ με προφίλ συμβατότητας *προέλευση δεδομένων (data_origin)*, *συμπληρωματική προηγούμενη επεξεργασία (complementary_pre-processing)* και *συμπληρωματική προηγούμενη εκτέλεση (complementary_execution_before)*, οι οποίες αποτιμώνται από κοινού για κάθε εργασία *t* κατά την ίδια διάσχιση της υπό εξέταση περίπτωσης εκτέλεσης με βάση την τοπολογική ταξινόμηση των εργασιών της (μέθοδος ApplyIndirectPreNorms, Αλγόριθμος 1).

Μια ΟΑΕκ προέλευσης δεδομένων αναφέρεται κατά κύριο λόγο σε μια εργασία t_r που πρέπει να έχει προηγηθεί και που είτε δίνει σαν έξοδο είτε επιδρά σε (μέσω αντίστοιχων αντικειμένων επενέργειας) πληροφορία η οποία σχετίζεται με κάποια από τις εισόδους της εργασίας αναφοράς. Έτσι η εργασία αυτή αναζητείται σε όλα τα μονοπάτια που καταλήγουν στην *t* και περιλαμβάνουν τα αντίστοιχα δεδομένα, λαμβάνοντας υπόψη και τη συνέχεια των μονοπατιών αυτών, το κατά πόσο, δηλαδή, ακόμα και αν εντοπιστούν δεδομένα που ως τύποι αφορούν την εργασία αναφοράς είναι τα ίδια που καταλήγουν σε αυτή μέσω της ακολουθούμενης ροής. Αν η απαιτούμενη εργασία δεν εντοπιστεί στο κατάλληλο μονοπάτι, η περίπτωση εκτέλεσης απορρίπτεται. Σημειώνεται ότι εξαίρεση σε αυτό θα μπορούσε να αποτελεί η περίπτωση που η οδηγία συνοδεύεται από συνθήκες πλαισίου $context_r$, μέρος των οποίων, έστω $context_{r-d}$, αφορά τιμές, χαρακτηριστικά ή καταστάσεις δεδομένων των οποίων η ισχύς μπορεί με βάση την υπάρχουσα μέχρι αυτό το σημείο ροή να αποκλειστεί. Τότε μπορεί να θεωρηθεί ότι η απαίτηση δεν ισχύει, οπότε η περίπτωση εκτέλεσης παραμένει αποδεκτή[39]. Αντικείμενο μελλοντικής εργασίας αποτελεί η αντιμετώπιση, στη βάση περισσότερης διαθέσιμης σημασιολογικής πληροφορίας, της μη ύπαρξης της t_r εφόσον η τελευταία όντως απαιτείται, μέσω, για παράδειγμα, της αντικατάστασης σχετικών υπαρχόντων εργασιών, της ανεύρεσης του κατάλληλου τρόπου σύνδεσης της t_r στην υπάρχουσα ροή ώστε αυτή να προστεθεί επιτυχώς χωρίς η ροή ως έχει

[39]Το ίδιο ισχύει και για τις υπόλοιπες ΝΕΣΠ που περιγράφονται στη συνέχεια, αλλά και για τις ΝΑΣ παραπάνω. Στην τελευταία περίπτωση, ωστόσο, δε χρειάζεται τέτοιος διαχωρισμός. Εκεί οι συνθήκες πλαισίου μπορούν να ελεγχθούν συνολικά κατά το τελευταίο βήμα πριν την εκτέλεση της εργασίας αναφοράς, πράγμα που δεν εφαρμόζεται στις ΝΕΣΠ λόγω της απόστασης από την εργασία αναφοράς, οπότε το πλαίσιο δεν μπορεί στην ουσία να αποτιμηθεί με ασφάλεια. Γενικά, οι συνθήκες πλαισίου στην παρούσα προσέγγιση αγνοούνται σε ό,τι αφορά τις ΝΕΣΠ. Αυτό σημαίνει ότι οι αντίστοιχες νόρμες πρέπει να ισχύουν για κάθε πλαίσιο, δεδομένου ότι ισχύει το κομμάτι $context_{r-d}$ που αφορά δεδομένα της ροής.

να διαταράσσεται ποιοτικά, κλπ..

Μια ΟΑΕκ με προφίλ συμβατότητας συμπληρωματικής προηγούμενης επεξεργασίας (complementary_pre-processing) εκφράζει την απαίτηση για την ύπαρξη μιας εργασίας t_r η οποία θα πρέπει να έχει προηγουμένως εκτελεστεί λαμβάνοντας ως είσοδο (με βάση τα οριζόμενα αντικείμενα επενέργειας) κάποια από τα δεδομένα που είναι διαθέσιμα ως έξοδοι προηγούμενων εργασιών στο γράφο της περίπτωσης εκτέλεσης. Αναζητείται σε όλα τα διαφορετικά μονοπάτια που περιέχουν τα δεδομένα αυτά και καταλήγουν στην t. Αν σε ένα τέτοιο μονοπάτι όλα τα δεδομένα ενδιαφέροντος περνούν μέσω της t_r η ΟΑΕκ ικανοποιείται. Αν η εργασία υπάρχει αλλά κατά τρόπο που "κρέμεται" από την υπόλοιπη ροή, ώστε τα αντίστοιχα δεδομένα να καταλήγουν στην t μέσω άλλης οδού, θα πρέπει να εξασφαλιστεί ότι η ακμή που οδηγεί στην t_r χαρακτηρίζεται από συνθήκη πλαισίου που να καλύπτει το πλαίσιο $context$ που οδηγεί από το ίδιο σημείο στην t, με την τομή του με $context_{r-d}$, αν υπάρχει. Αν η εργασία δε βρεθεί, προστίθεται κατάλληλα αντίστοιχη εργασία t_a, με βάση την τελευταία περίπτωση παραπάνω. Αν ορίζεται επιπλέον προφίλ συμβατότητας άμεσης σύνδεσης, θα πρέπει η t_r να αναζητείται και αντίστοιχα προστίθεται σε σύνδεση με την αμέσως προηγούμενη εργασία της t[40], όπου αυτό είναι εφικτό. Τέλος, η απαιτούμενη εργασία θα μπορούσε να συνδέεται και με μια ακμή ελέγχου με την t, ώστε να εξασφαλίζεται ότι η πρώτη θα έχει εκτελεστεί πριν ξεκινήσει η τελευταία να εκτελείται.

Τέλος, στην περίπτωση ΟΑΕκ με προφίλ συμπληρωματικής προηγούμενης εκτέλεσης (complementary_execution_before), η απαιτούμενη t_r αναζητείται σε κάθε εναλλακτικό προηγούμενο μονοπάτι, στο οποίο αρκεί να εντοπιστεί μία μόνο φορά. Αν αυτό δε συμβαίνει, προστίθεται η ανάλογη t_a σε σημείο το οποίο καθορίζεται από το τι είσοδο απαιτεί και ποιά υπάρχουσα προγενέστερη εργασία μπορεί να την παράσχει, όπως περιγράφηκε σε προηγούμενες περιπτώσεις (π.χ., ΟΑΕισ). Γενικά, αν υπάρχουν περισσότερες της μιας τέτοιες εργασίες, η προσέγγιση που ακολουθείται τώρα είναι να επιλέγεται η εγγύτερη στην t. Αντίστοιχα, αν δεν απαιτείται κάποια είσοδος, η t_a συνδέεται με ακμή ελέγχου με την εργασία την αμέσως προηγούμενη της t[41]. Και εδώ, θεωρούμε ότι η εργασία αυτή πρέπει να προηγείται κάτω από οποιεσδήποτε συνθήκες πλαισίου, δεδομένου ότι είναι πιθανό να ικανοποιούνται κατά την εκτέλεση οι τυχούσες συνθήκες $context_{r-d}$, ενώ η προσθήκη ακμής ελέγχου προς την t εξασφαλίζει ότι η εκτέλεση της t_r θα έχει ολοκληρωθεί (περίπτωση ανασταλτικού προφίλ συμβατότητας).

8.7 Εφαρμογή Νορμών Έμμεσης Σύνδεσης Μετά

Οι ΝΕΣΜ αφορούν στην ικανοποίηση ΟΑΕκ με προφίλ συμβατότητας *συμπληρωματικής ακόλουθης επεξεργασίας (complementary_post-processing)* και *συμπληρωματικής ακόλουθης εκτέλεσης (complementary_execution_before)*. Οι οδηγίες αυτές ελέγχονται από κοινού

[40]Εδώ το πλαίσιο θα θεωρηθεί εξ ολοκλήρου, όπως στις περιπτώσεις άμεσης σύνδεσης παραπάνω.
[41]Βλ. προηγούμενη υποσημείωση.

για κάθε εργασία αναφοράς, ακολουθώντας όμως αυτή τη φορά την αντίστροφη τοπολογική ταξινόμηση των εργασιών, προκειμένου σε κάθε βήμα να έχει κατά το δυνατόν οριστικοποιηθεί η "μελλοντική" δομή της περίπτωσης εκτέλεσης (μέθοδος ApplyIndirectPostNorms, Αλγόριθμος 1).

Μια ΟΑΕκ συμπληρωματικής ακόλουθης επεξεργασίας ικανοποιείται αν η απαιτούμενη εργασία t_r συναντάται σε όλα τα εναλλακτικά εξερχόμενα μονοπάτια της εργασίας αναφοράς t_r, τα οποία μεταφέρουν πληροφορία παραγόμενη από την t και η οποία κατά κανόνα αποτελεί αντικείμενο επενέργειας της t_r. Έτσι, αφού εντοπιστούν τα αντίστοιχα μονοπάτια, αναζητείται σε καθένα από αυτά η t_r, προσέχοντας ώστε να διατηρείται η συνέχεια του εκάστοτε μονοπατιού αναφορικά με τους τύπους των μεταφερόμενων δεδομένων. Αν βρεθεί και αποτελεί μέρος της κύριας ροής, με την έννοια ότι όλα τα δεδομένα του θεωρούμενου τύπου συνεχίζουν την πορεία τους μέσω της t_r, η απαίτηση πληρούται. Από την άλλη, αν ναι μεν υπάρχει, αλλά ως επιπλέον της κύριας ροής επεξεργασία, θα πρέπει να εξασφαλιστεί ότι εκτελείται υπό οποιεσδήποτε συνθήκες πλαισίου, δεδομένου ότι οι ενδεχόμενες συνθήκες $context_{r-d}$ είναι πιθανό να ικανοποιηθούν σε πραγματικό χρόνο. Αν η t_r δεν υπάρχει, προστίθεται αντίστοιχη t_a στο αντίστοιχο μονοπάτι αμέσως μετά την t, χωρίς όμως να διακόπτει τη ροή, με συνθήκες πλαισίου που συνίστανται στην τομή των συνθηκών των ήδη εξερχόμενων ακμών με τις συνθήκες πλαισίου που ορίζει η οδηγία. Μια ΟΑΕκ συμπληρωματικής ακόλουθης εκτέλεσης αντιμετωπίζεται με ακριβώς τον ίδιο τρόπο, χωρίς όμως να λαμβάνει υπόψη περιορισμούς σε σχέση με τη συνέχεια των μονοπατιών αναφορικά με τα μεταφερόμενα δεδομένα.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι, ειδικά για την περίπτωση των ΝΕΣΜ, οι συνθήκες πλαισίου θα μπορούσαν να έχουν ελαφρώς διαφορετική αντιμετώπιση. Συγκεκριμένα, αν η t_r εντοπιστεί σε κάποιο μεταγενέστερο σημείο της ροής κατά τρόπο που να "κρέμεται", δεν είναι απαραίτητο να εξασφαλιστεί η εκτέλεσή της υπό οποιεσδήποτε συνθήκες πλαισίου. Αντ' αυτού, οι πιθανές συνθήκες πλαισίου $context_r$ που συνοδεύουν την οδηγία, καθώς αφορούν τη στιγμή της εκτέλεσης της εργασίας αναφοράς t, θα μπορούσαν να ληφθούν υπόψη ως εξής: αν ισχύουν κατά την εκτέλεση της t, θα ενεργοποιούν κάποιο πλαίσιο $context'_r$, το οποίο και θα προστίθεται ως ένωση σε εκείνο της ακμής που οδηγεί στην ήδη υπάρχουσα t_r. Έτσι, εφόσον το πλαίσιο ενεργοποιηθεί, η εκτέλεση της απαιτούμενη εργασίας εξασφαλίζεται.

8.8 Εφαρμογή Νορμών Εκτέλεσης

Οι ΝΕ περιλαμβάνουν ΟΑΕκ με προφίλ συμβατότητας εκτέλεσης οποτεδήποτε (wherever) στα πλαίσια της ροής εργασιών, οι οποίες εξετάζονται με τυχαία σειρά (μέθοδος ApplyExistenceNorms, Αλγόριθμος 1). Σε αυτή τη φάση, αν η απαιτούμενη εργασία t_r δεν εντοπίζεται σε κάθε εναλλακτικό μονοπάτι της περίπτωσης εκτέλεσης, η τελευταία απορρίπτεται. Ως μέρος μελλοντικής εργασίας, κατάλληλα ερωτήματα προς τη Μηχανή Συ-

μπερασμού με βάση τις υπάρχουσες εργασίες στη ροή και επιπλέον διαχείριση του γράφου μπορούν να οδηγήσουν στην τοποθέτηση της αντίστοιχης t_a.

8.9 Εφαρμογή Νορμών Υπό Συνθήκη

Οι νόρμες υπό συνθήκη ελέγχονται με τον ίδιο τρόπο και με την ίδια σειρά με τις απόλυτες Νόρμες που περιγράφηκαν παραπάνω (μέθοδοι ApplyConditionalDirectNorms, ApplyConditionalIndirectPreNorms, ApplyConditionalIndirectPostNorms, ApplyConditionalExistenceNorms στον Αλγόριθμο 1). Η διαφορά εδώ έγκειται στο ότι το αν θα πρέπει να ικανοποιούνται ή όχι καθορίζεται από την παρουσία μιας ή περισσότερων εργασιών ή δομών εργασιών σε κάποιο σημείο πριν (preconditions) ή μετά (postconditions) της εργασίας αναφοράς, όπου και αναζητούνται. Αν δεν ορίζεται συγκεκριμένη εργασία αναφοράς, όπως μπορεί να συμβαίνει με κάποιες ΟΑΕκ με προφίλ συμβατότητας εκτέλεση οποτεδήποτε ή με κάποιες ΟΑπΕκ, οι προ-υποθέσεις και μετα-υποθέσεις ορίζουν σχετικές θέσεις ως προς τις αντίστοιχες εργασίες τις οποίες πρέπει (αντ. απαγορεύεται) να καταλαμβάνουν οι εργασίες που απαιτούνται (αντ. απαγορεύονται) από τις εν λόγω οδηγίες. Αν μια οδηγία ορίζει και προ-υποθέσεις και μετα-υποθέσεις, θα πρέπει να πληρούνται και οι δύο ώστε η οδηγία να έχει ισχύ. Από την άλλη, αν μέσω λογικών σχέσεων ορίζονται εναλλακτικές προ-υποθέσεις (ή μετα-υποθέσεις), αρκεί έστω μία από αυτές να ισχύει. Τέλος, ο αρνητικός λογικός τελεστής σηματοδοτεί την απουσία δεδομένων εργασιών ως συνθήκη υπό την οποία η οδηγία έχει ισχύ.

Σημειώνεται ότι, στην ίδια λογική που αφορά τον έλεγχο των ΝΕΣΜ, μια παραλλαγή του Αλγόριθμου 1 διαχωρίζει την εξέταση των οδηγιών που συνοδεύονται από προ-υποθέσεις από εκείνη των οδηγιών που χαρακτηρίζονται από μετα-υποθέσεις, και η οποία ακολουθεί την πρώτη με βάση την αντίστροφη τοπολογική ταξινόμηση των εργασιών. Επίσης, θέμα μελλοντικής εργασίας παραμένει ο χειρισμός των περιπτώσεων που εμφανίζουν εξάρτηση τόσο από προ-υποθέσεις όσο και από μετα-υποθέσεις. Γενικότερα, η σειρά ελέγχου και γενικότερα η αντιμετώπιση των νορμών υπό συνθήκη επιδέχεται βελτιώσεις λόγω της πολυπλοκότητας των περιπτώσεων αυτών.

Επιπλέον, αν η παρουσία μιας εργασίας ή ακμής, που προκύπτει είτε από τη διαδικασία επαλήθευσης είτε κατά τη δημιουργία των περιπτώσεων εκτέλεσης, οφείλεται σε προ-/μετα-υποθέσεις, προστίθενται οι κατάλληλες συνθήκες (όπως, εξάλλου, και στην περίπτωση τις εξάρτησης από συνθήκες πλαισίου), κάνοντας χρήση κυρίως μεταβλητών ροής εργασιών. Έτσι, αφενός προβλέπεται η εκτέλεση των αντίστοιχων εργασιών και αφετέρου διατηρείται η υπό συνθήκη φύση της, μετά και τη συνένωση των περιπτώσεων εκτέλεσης και των υπογράφων–στιγμιοτύπων.

8.10 Εφαρμογή Νορμών Κατάστασης

Ο έλεγχος των ΝΚ λαμβάνει χώρα στο τελευταίο βήμα της διαδικασίας, όταν όλες οι εργασίες που απαιτούνται ρητά και που ενδεχομένως επηρεάζουν καταστάσεις δεδομένων έχουν ήδη τοποθετηθεί στη ροή (μέθοδος ApplyStateNorms, Αλγόριθμος 1). Οι νόρμες αυτές δεν αντιστοιχούν σε συγκεκριμένες οδηγίες, αλλά προκύπτουν έμμεσα κατά τη δημιουργία των περιπτώσεων εκτέλεσης από τις τυχόν *εργασίες αλλαγής κατάστασης (state-changing tasks)* που παρεμβάλλουν μεταξύ εργασιών οι ΟΕΔιΣ, προκειμένου η πληροφορία η οποία μεταφέρεται στα πλαίσια ενός διμερούς συσχετισμού να βρίσκεται στην επιθυμητή κατάσταση. Με άλλα λόγια, ένας έγκυρος ΔιΣ μπορεί να περιλαμβάνει μία εργασία (ή και περισσότερες) που να αλλάζει την κατάσταση των δεδομένων (π.χ., κρυπτογράφηση), πράγμα που αποτυπώνεται στις ιδιότητες κατάστασης (βλ. Ενότητα 6.3.3) των αντίστοιχων εξερχόμενων πληροφοριών. Οι ιδιότητες αυτές συνιστούν στην ουσία τις ΝΚ (StN) που θα πρέπει τελικά να ικανοποιούνται. Έτσι, κατά το βήμα αυτό, κάθε εργασία (βάσει τοπολογικής ταξινόμησης) ελέγχεται ως προς το αν, κατ' αρχήν, επιφέρει την εκάστοτε κατάσταση που εξετάζεται και, στη συνέχεια, αν, και με ποιο τρόπο, είναι αναγκαίο να παραμείνει στη ροή, όπως υποδεικνύεται, στη βάση της κατάστασης που τα δεδομένα ενδιαφέροντος ήδη βρίσκονται (βλ. Αλγόριθμο 3). Για το σκοπό αυτό, αφού ανακτηθούν για μια δεδομένη εργασία αλλαγής κατάστασης (πληροφορία διαθέσιμη στο Σημασιολογικό Μοντέλο Πληροφοριών) οι εξερχόμενες ενότητες πληροφορίας (γρ.1) και προσδιοριστούν οι οριζόμενες (από τον έγκυρο ΔιΣ) καταστάσεις τους (γρ. 4), τότε, για κάθε κατάσταση, αν: α) αυτή είναι αποτέλεσμα της υπό εξέταση εργασίας (μέθοδος CreateState), και β) η συγκεκριμένη κατάσταση δεν ικανοποιείται από τις εργασίες που προϋπάρχουν της *t* σε κάθε εναλλακτικό μονοπάτι που οδηγεί στο παρόν σημείο (μέθοδος CheckState), τότε η αντίστοιχη ενότητα πληροφορίας προστίθεται στη λίστα *INV_OUT*, η οποία περιέχει όλες τις εξόδους της *t* οι οποίες δε βρίσκονται ήδη στην επιθυμητή κατάσταση (γρ. 5-9). Αφού η διαδικασία αυτή τελειώσει για όλες τις εξόδους της *t* και εφόσον η *INV_OUT* είναι άδεια, πράγμα που καθιστά στην ουσία περιττή την ύπαρξη της *t* σε αυτό το σημείο, καλείται η μέθοδος RemoveTaskAndMergeBranches (γρ. 11-12), η οποία και την απαλείφει. Αν, αντίθετα, η *INV_OUT* περιέχει στοιχεία, σημαίνει ότι για τα τελευταία η *t* πρέπει να εξακολουθεί να υπάρχει, οπότε και τίθενται ως τα —μοναδικά— αντικείμενα επενέργειας της *t* (γρ. 14).

Αναφορικά με την CheckState, ενδιαφέρον παρουσιάζει η πολυπλοκότητα του ζητήματος του προσδιορισμού της κατάστασης μιας οντότητας πληροφορίας, εν όψει κυρίως των σχέσεων *isPartOf* μεταξύ τύπων δεδομένων. Στο παρόν ακολουθείται η απλή προσέγγιση του να εντοπίζεται εκείνο το (προς τα πίσω) μονοπάτι το οποίο μεταφέρει με συνεχή τρόπο τον τύπο δεδομένων που εμφανίζεται στο συγκεκριμένο βήμα και να αναζητείται σε αυτό η εργασία *t*. Επίσης, αν υπάρχουν περισσότερα του ενός μονοπάτια που μεταφέρουν το δεδομένο αυτό, η *t* θα πρέπει να υπάρχει σε όλα, διαφορετικά δεν απαλείφεται από το δεδομένο σημείο. Επιπλέον όψεις που αξίζει να διερευνηθούν σχετίζονται με την προηγούμενη επίδραση μιας ίδιας εργασίας πάνω σε δεδομένα τα οποία είτε περιέχουν είτε συνα-

ποτελούν την οντότητα πληροφορίας που μελετάται στο εν λόγω βήμα, και τη γενικότερη πορεία τους. Σημειώνεται, τέλος, ότι δεν αρκεί ο εντοπισμός μιας εργασίας αντίστοιχης της *t*, αλλά πρέπει επιπλέον να διασφαλίζεται ότι, από την τελευταία εμφάνιση μιας τέτοιας εργασίας και μετά, δεν παρεμβάλλονται εργασίες που αντιστρέφουν τη δράση της. Σε αντίθετη περίπτωση, η *t* παραμένει.

Αλγόριθμος 3 Check state

Input: *c*, *t*
Output: *vc*

```
1: OUT ← RetrieveOutgoingInfoEntities(t)
2: INV_OUT ← ∅
3: for each out in OUT do
4:    STATES ← GetDataStates(out)
5:    for each state in STATES do
6:       if CreateState(t, state) && !CheckState(out, t, c) then
7:          INV_OUT.add(out)
8:       end if
9:    end for
10: end for
11: if INV_OUT is empty then
12:    vc ← RemoveTaskAndMergeBranches (c, t)
13: else
14:    vc.t.assets ← INV_OUT
15: end if
16: return vc
```

Κεφάλαιο 9

Εκτέλεση Ροών Εργασιών με Επίγνωση Ιδιωτικότητας σε Υπηρεσιοστραφές Περιβάλλον

9.1 Από το Σχεδιασμό στην Εκτέλεση

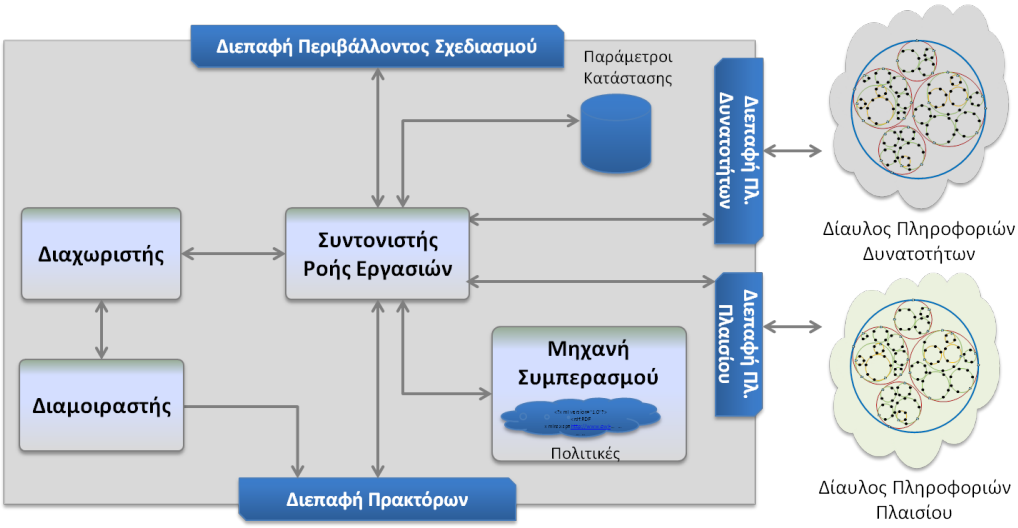
Όπως έχει ήδη αναφερθεί στο Κεφάλαιο 4, η Φάση Εκτέλεσης αναφέρεται στην πραγμάτωση μιας ροής εργασιών η οποία έχει προηγουμένως, και μέσα από το Περιβάλλον Σχεδιασμού, προδιαγεγραφεί, ελεγχθεί και, πιθανώς, μετασχηματιστεί, ώστε να ικανοποιεί διάφορες απαιτήσεις ιδιωτικότητας. Περιλαμβάνει δύο νοητά στρώματα: από τη μια, το *Στρώμα Ενορχήστρωσης (Orchestration Layer)* αναλαμβάνει το συντονισμό των ροών εργασιών, κάνοντας χρήση των λειτουργικοτήτων που προσφέρονται από τους *Ενορχηστρωτές (Orchestrators)* από τους οποίους αποτελείται· από την άλλη, το *Στρώμα Οντοτήτων (Components Layer)* παρέχει τον απαιτούμενο χαρακτήρα αφαίρεσης προκειμένου οι υποκείμενες λειτουργίες, είτε παθητικές (π.χ., μια βάση δεδομένων) είτε ενεργητικές (π.χ., κάποιος μηχανισμός ανίχνευσης συμβάντων ασφάλειας), να εκτίθενται και να αλληλεπιδρούν με το Στρώμα Ενορχήστρωσης αλλά και μεταξύ τους ως *υπηρεσίες*. Το τελευταίο αποτελεί βασικό χαρακτηριστικό κάθε συστήματος λογισμικού προσανατολισμένου σε υπηρεσίες (service orientation) και εξυπηρετεί στο να "κρύβει" την ετερογένεια των υποκείμενων τεχνολογιών υλοποίησης, καθιστώντας εφικτό το σε μεγάλη κλίμακα συντονισμό λειτουργιών σε κατανεμημένα περιβάλλοντα με ομοιογενή τρόπο. Έτσι, το Στρώμα Οντοτήτων απαρτίζεται από *Πράκτορες (Agents)*, καθένας από τους οποίους εκπροσωπεί μια υποκείμενη οντότητα που προσφέρει κάποια λειτουργία, παρέχοντάς της τις απαραίτητες λειτουργικότητες στο επίπεδο ελέγχου (control plane). Κατά συνέπεια, το Στρώμα Ενορχήστρωσης μπορεί να αλληλεπιδρά με την εκάστοτε οντότητα καλώντας την υπηρεσία που εκτίθεται από τον αντίστοιχο Πράκτορα. Στην ίδια κατεύθυνση, απαραίτητη είναι και η κατάλληλη ομοιογενής περιγραφή των υπηρεσιών, ώστε το μεσισμικό ενορχήστρωσης να

αντιλαμβάνεται ποιές λειτουργίες γίνονται διαθέσιμες και πού. Το θέμα της περιγραφής υπηρεσιών εξετάζεται στην Ενότητα 9.3.

Από τη στιγμή που ένα Μοντέλο Ροών Εργασιών (ΜΡΕ) θα περάσει από το Περιβάλλον Σχεδιασμού στο Περιβάλλον Εκτέλεσης, ανατίθεται σε έναν Ενορχηστρωτή, ο οποίος αναλαμβάνει εφεξής το συντονισμό της ροής εργασιών καθ' όλη τη διάρκεια της εκτέλεσής της, παίζοντας το ρόλο του διαμεσολαβητή ανάμεσα στο Περιβάλλον Σχεδιασμού και τις οντότητες που θα φέρουν τελικά εις πέρας τη ροή εργασιών και διατηρώντας συγχρόνως όλες τις πληροφορίες σχετικά με την πορεία εκτέλεσής της. Ο Ενορχηστρωτής, η εσωτερική δομή του οποίου απεικονίζεται στο Σχήμα 19, συνιστά μια οντότητα με χαρακτήρα διατήρησης κατάστασης (stateful), στην οποία ανατίθεται η εκτέλεση μιας μόνο ροής εργασιών κάθε φορά και η οποία απελευθερώνεται όταν αυτή ολοκληρωθεί. Το πρώτο βήμα είναι ο σε πραγματικό χρόνο εντοπισμός και η αναγνώριση των συγκεκριμένων οντοτήτων που είναι ικανές και διαθέσιμες να προσφέρουν τις λειτουργίες που εκπροσωπούν οι διάφορες εργασίες της ροής (capabilities matching), οπότε κάθε εργασία συνδέεται με τον Πράκτορα (μέσω αφηρημένης αναφοράς) που είναι υπεύθυνος για την εκτέλεσή της. Η διαδικασία αυτή πραγματοποιείται από το *Συντονιστή Ροής Εργασιών (Workflow Coordinator)* μέσω της επικοινωνίας του με το Δίαυλο Πληροφοριών Δυνατοτήτων (βλ. Ενότητα 9.3). Στη συνέχεια, το ληφθέν ΜΡΕ τμηματοποιείται από το *Διαχωριστή (Splitter)* κατά τέτοιο τρόπο ώστε να προκύπτουν περιγραφές της συμπεριφοράς αυτόνομων οντοτήτων. Για το σκοπό αυτό δημιουργείται ένα σύνολο *τεμαχίων ροών εργασιών (workflow fragments)*, τέτοια ώστε όλες οι εργασίες που περιλαμβάνονται σε κάθε τεμάχιο να εκτελούνται από τον ίδιο Πράκτορα, και συνεπώς την ίδια υποκείμενη οντότητα (σημασιολογική τεμαχιοποίηση), και σε κάθε Πράκτορα να αντιστοιχεί ένα ακριβώς τεμάχιο[42]. Ένα τεμάχιο μπορεί να αποτελείται από μία μόνο εργασία ή και ένα ευρύτερο τμήμα της ροής εργασιών, ενώ θα πρέπει να διατηρεί, πέρα από τις εργασίες και διαδρομές που μπορούν να εκτελούνται από τον ίδιο Πράκτορα, όλη την αρχική σημασιολογική πληροφορία εκτέλεσης που περιλαμβάνει το ΜΡΕ και που το αφορά. Έτσι, κάθε τεμάχιο εμπεριέχει τον προσδιορισμό της ακριβούς ροής ελέγχου και δεδομένων και όλες τις επιπλέον απαραίτητες πληροφορίες που αφορούν την εκτέλεσή του, όπως, για παράδειγμα, περιορισμούς σχετικούς με εξουσιοδοτήσεις ή εξαρτήσεις πλαισίου, αλλά και την κάθε είδους αλληλεπίδραση με άλλες οντότητες με τις οποίες μπορεί να σχετίζεται. Προς επίτευξη του τελευταίου, όλοι οι παράγοντες που αφορούν την εκτέλεση ενός τεμαχίου εξάγονται μέσω στατικής ανάλυσης του ΜΡΕ, υποδεικνύοντας τα μηνύματα συγχρονισμού που θα πρέπει να μεταδοθούν από και προς άλλες οντότητες κατά την εκτέλεση. Όλα τα παραπάνω διασφαλίζουν ότι, ενώ κάθε οντότητα/Πράκτορας έχει επίγνωση μόνο του δικού του ρόλου και της δικής του συμπεριφοράς στα πλαίσια της ροής εργασιών, λαμβάνει, ταυτόχρονα, οποιαδήποτε άλλη πληροφορία χρειάζεται ούτως ώστε να αλληλεπιδρά με τις υπόλοιπες εμπλεκόμενες οντότητες και γενικά να συμπεριφέρεται με συνέπεια ως προς τη συνολική προδιαγραφή της ροής εργασιών. Κάθε τεμάχιο

[42]Για την ακρίβεια, ένα ακριβώς τεμάχιο ανά υπό εκτέλεση ροή εργασιών. Αν ο Πράκτορας συμμετέχει συγχρόνως στην εκτέλεση περισσότερων της μιας ροής εργασιών, φτάνουν σε αυτόν ισάριθμα τεμάχια.

ροής εργασιών διατυπώνεται φορμαλιστικά με τη βοήθεια της Γλώσσα Περιγραφής Οδηγιών Εκτέλεσης (ΓΠΟΕ), η οποία επίσης προδιαγράφηκε στα πλαίσια της διατριβής και παρουσιάζεται στην Ενότητα 9.2.

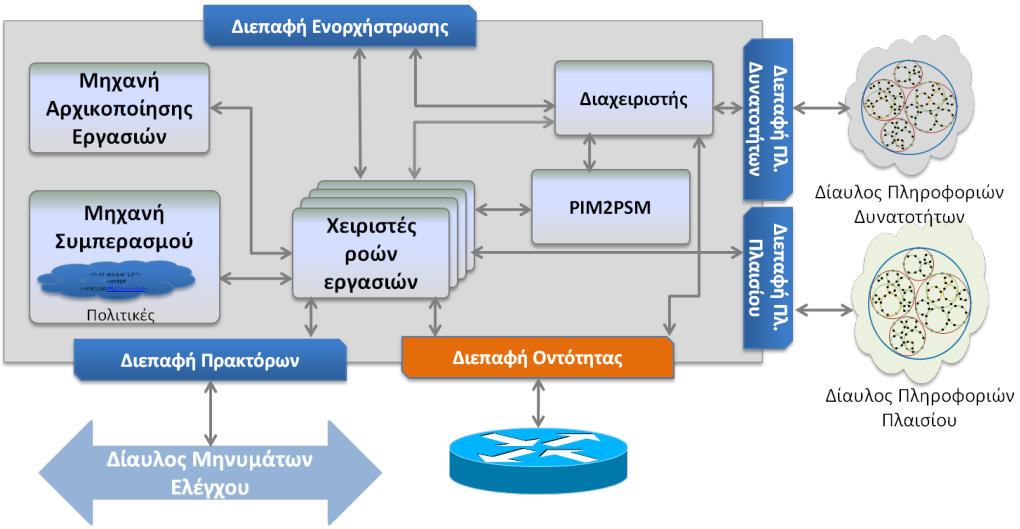


Σχήμα 19: Ενορχηστρωτής.

Αφού η ροή εργασιών διαιρεθεί κατάλληλα, η σε αφηρημένο επίπεδο αναφορά που σχετίζεται με κάθε τεμάχιο υποδεικνύοντας την οντότητα που καλείται να το εκτελέσει μετατρέπεται στο ακριβές αναγνωριστικό του αντίστοιχου Πράκτορα, έτσι ώστε τα τεμάχια να μπορέσουν να διανεμηθούν στους Πράκτορες μέσω του *Διαμοιραστή (Dispatcher)*. Όταν ένας Πράκτορας λάβει το τεμάχιο που καθορίζει το ρόλο και τα καθήκοντά του μέσα στη ροή εργασιών, δεσμεύει τους σχετικούς πόρους και είναι πλέον σε θέση να εκτελέσει το τμήμα της ροής εργασιών που του αναλογεί, μόλις λάβει τα κατάλληλα μηνύματα συγχρονισμού.

Η εσωτερική δομή ενός Πράκτορα φαίνεται στο Σχήμα 20. Από τις πρώτες ενέργειες που αυτός πραγματοποιεί εσωτερικά, μόλις του ανατεθεί η εκτέλεση ενός τεμαχίου, είναι η αρχικοποίηση των διαφόρων παραμέτρων εκτέλεσης των σχετικών εργασιών. Πράγματι, οι οδηγίες εκτέλεσης που λαμβάνει μέσω των τεμαχίων παραμένουν, στη γενική περίπτωση, διατυπωμένες σε αφηρημένο ή ημι-αφηρημένο επίπεδο, μέχρι τη στιγμή της εκτέλεσης των ορισμένων εργασιών· αυτό οφείλεται στο γεγονός ότι η ακριβής μορφή τους είναι πιθανό να εξαρτάται από όρους πραγματικού χρόνου. Έτσι, η *Μηχανή Αρχικοποίησης Εργασιών (Task Instantiation Engine)* κάθε Πράκτορα καθίσταται υπεύθυνη για τον προσδιορισμό των αντίστοιχων ενεργειών σε συγκεκριμένο επίπεδο μέσω της αντιστοίχισης μεταξύ αφηρημένων εννοιών (π.χ., κάποιο συμβολικό αναγνωριστικό) και των συγκεκριμένων οντοτήτων που τις εκπροσωπούν (π.χ., συγκεκριμένη IP διεύθυνση και θύρα) ή των τιμών που λαμβάνουν (π.χ., τιμές παραμέτρων πλαισίου) τη στιγμή της εκτέλεσης. Με λίγα λόγια, η Μηχανή Αρχικοποίησης Εργασιών μετατρέπει, με βάση τους διαθέσιμους πόρους και τις τιμές παραμέτρων πραγματικού χρόνου, την όποια αφηρημένη ή ημι-

αφηρημένη συμπεριφορά της υποκείμενης οντότητας σε συγκεκριμένες ενέργειες. Το επόμενο βήμα είναι η μετατροπή των συγκεκριμένων αυτών ενεργειών, που με βάση τη μοντελοκεντρική προσέγγιση αποτελούν ένα Μοντέλο Ανεξάρτητο Πλατφόρμας (Platform Independent Model – PIM) της λειτουργικής συμπεριφοράς της υποκείμενης οντότητας, στο Μοντέλο Συγκεκριμένης Πλατφόρμας (Platform-Specific Model – PSM), δηλαδή στην απευθείας εκτελέσιμη από τη οντότητα προδιαγραφή. Ο Πράκτορας, με άλλα λόγια, μέσω της δομικής υπομονάδας *PIM2PSM*, μεταφράζει κάθε κλήση μεθόδου στο συγκεκριμένο πρωτόκολλο που την υλοποιεί, όπως θα μπορούσε να είναι, για παράδειγμα, μια σειρά SQL εντολών που πραγματοποιούν τις λειτουργίες τις σχετικές με τους κανονισμούς διατήρησης των δεδομένων.



Σχήμα 20: Πράκτορας.

Επιπλέον, κάθε Πράκτορας, πέρα από το να φροντίζει για την υλοποίηση του τμήματος της ροής εργασιών που πρόκειται να εκτελεστεί τοπικά, επικοινωνεί μέσω των κατάλληλων διεπαφών με άλλες οντότητες που συμμετέχουν σε αυτή, όντας σε θέση να γνωρίζει τις εξαρτήσεις που εμφανίζει ως προς τους προκατόχους και τους διαδόχους του στη ροή της εκτέλεσης, όπως αυτές προσδιορίζονται στα αντίστοιχα τεμάχια. Ένας Πράκτορας ξέρει, δηλαδή, ποιόν άλλο Πράκτορα θα πρέπει να "καλέσει" μετά την εκτέλεση ενός τμήματος του τεμαχίου ή από ποιόν Πράκτορα θα πρέπει να λάβει μήνυμα ελέγχου προκειμένου να ξεκινήσει την εκτέλεση ενός άλλου. Αυτό είναι σημαντικό προκειμένου να διασφαλιστεί ότι η ροή ελέγχου της συνολικής ροής εργασιών διατηρείται, καθώς και ότι τα δεδομένα εισόδου και εξόδου των εργασιών μεταφέρονται σε συμφωνία με τις προδιαγεγραμμένες εξαρτήσεις δεδομένων, παρόλο που ο οποιοσδήποτε Πράκτορας δεν έχει καμία επίγνωση των εργασιών και λοιπών αλληλεπιδράσεων που δεν εμπίπτουν στη δικαιοδοσία του. Για το σκοπό αυτό, οι Πράκτορες ανταλλάσσουν μηνύματα συγχρονισμού μεταξύ τους και επικοινωνούν αυτόνομα χωρίς άλλη παρέμβαση του Ενορχηστρωτή, προωθώντας περαιτέρω την αποκεντροποιημένη εκτέλεση των ροών εργασιών. Έτσι, οι βασικοί τύποι ροής ελέγχου μπορούν πράγματι να συντονιστούν αποτελεσματικά, όπως θα

φανεί και από την περιγραφή της ΓΠΟΕ στην επόμενη ενότητα: για παράδειγμα, όταν μια οντότητα ολοκληρώνει την εκτέλεση ενός τεμαχίου της, στέλνει ένα μήνυμα συγχρονισμού στον Πράκτορα ο οποίος έχει οριστεί να εκτελέσει το επόμενο στη σειρά τεμάχιο· παρόμοια, στην περίπτωση της παράλληλης εκτέλεσης τεμαχίων από διαφορετικούς Πράκτορες, μπορεί, ανάλογα και με τη σχετική επισημείωση των εργασιών, να οριστεί ότι όλοι τους θα πρέπει να στείλουν μηνύματα συγχρονισμού στον ακριβώς επόμενο Πράκτορα, ώστε αυτός να εκκινήσει την εκτέλεση. Σημειώνεται ότι αναφορικά με την επικοινωνία στο επίπεδο δεδομένων, ο ίδιος ο Πράκτορας είναι αρμόδιος μόνο για τη δημιουργία και ρύθμιση των κατάλληλων διεπαφών μέσω μηνυμάτων συγχρονισμού και δεν έχει καμιά ενεργή ανάμειξη στην επικοινωνία καθεαυτή. Τέλος, ο Πράκτορας είναι σε θέση να ελέγχει, μέσω της διασύνδεσής του με την υποκείμενη οντότητα ή με άλλες κατάλληλες υποδομές, το αν οι περιορισμοί που έχουν προδιαγεγραφεί νωρίτερα κατά τη Φάση Σχεδιασμού εφαρμόζονται σωστά. Για παράδειγμα, θα πρέπει να εξασφαλίζει ότι ο χρήστης ο οποίος αναλαμβάνει τη διεκπεραίωση μιας λειτουργίας κατέχει τον απαιτούμενο ρόλο.

9.2 Γλώσσα Περιγραφής Οδηγιών Εκτέλεσης

Προκειμένου να καλυφθεί η ανάγκη της φορμαλιστικής περιγραφής των τεμαχίων μιας ροής εργασιών, κατά τρόπο ώστε αυτά να αποδίδουν όλη την απαραίτητη πληροφορία εκτέλεσης, όπως περιγράφηκε παραπάνω, στα πλαίσια της διατριβής προδιαγράφηκε μια πρωτότυπη γλώσσα για την περιγραφή των οδηγιών που πρέπει να λάβει κάθε Πράκτορας αναφορικά με τη συνεπή συμμετοχή του στη ροή εργασιών. Η Γλώσσα Περιγραφής Οδηγιών Εκτέλεσης (ΓΠΟΕ) είναι βασισμένη στη γλώσσα XML [436] και σχεδιάστηκε με γνώμονα την ακριβή μεταφορά όλων των εννοιών που ορίζονται σε ένα ΜΡΕ που ακολουθεί την προδιαγραφή του Κεφαλαίου 6, ώστε όλα τα χαρακτηριστικά ιδιωτικότητας που ενσωματώνονται σε αυτό να περνούν στο χαμηλότερο στρώμα εκτέλεσης, δηλαδή στο Στρώμα Οντοτήτων, εξασφαλίζοντας τη σύμμορφη λειτουργία τους.

Η ΓΠΟΕ χρησιμοποιείται εσωτερικά σε κάθε Ενορχηστρωτή. Συγκεκριμένα, ο Διαχωριστής επεξεργάζεται την Οντολογία Μοντέλων Ροών Εργασιών (ΟΜΡΕ) που του έχει ανατεθεί και, με βάση τις διαθέσιμες από το σύστημα οντότητες, όπως αυτές έχουν εντοπιστεί μέσω της αλληλεπίδρασης με το Δίαυλο Πληροφοριών Δυνατοτήτων, παράγει τα αντίστοιχα τεμάχια τα οποία προδιαγράφει με χρήση της ΓΠΟΕ και τα οποία διαβιβάζει στο Διαμοιραστή, απ' όπου τελικά καταλήγουν στους αρμόδιους Πράκτορες. Η ΓΠΟΕ αποτελεί, δηλαδή, στην ουσία τη γλώσσα για τη διαλειτουργικότητα μεταξύ του Στρώματος Οντοτήτων και του Περιβάλλοντος Σχεδιασμού και τον κοινό κώδικα που επιτρέπει το συντονισμό των υποκείμενων υπηρεσιών με συνέπεια ως προς τις απαιτήσεις ιδιωτικότητας. Στο σημείο αυτό θα πρέπει να σημειωθεί ότι η ΓΠΟΕ βασίζεται στο σημασιολογικό μοντέλο που ορίζεται στην Οντολογία Σημασιολογικού Μοντέλου Πληροφοριών (ΟΣΜΠ), προκειμένου να αναφερθεί σε τύπους λειτουργιών, δεδομένων, ρόλων, πληροφοριών πλαισίου,

κλπ..

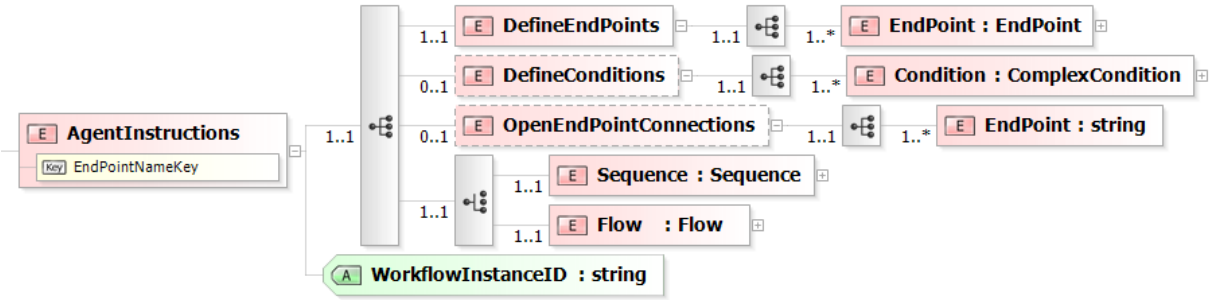
Στη συνέχεια παρουσιάζονται τα στοιχεία (elements) της γλώσσας ΓΠΟΕ, ενώ τα Σχήματα 21 έως 23 απεικονίζουν βασικά σημεία της αντίστοιχης XML δομής.

Στην αρχή κάθε τεμαχίου ορίζονται τα σημεία σύνδεσης (endpoints) μέσω των οποίων οι λειτουργίες που περιλαμβάνει το τεμάχιο επικοινωνούν μεταξύ τους αλλά και με τον "έξω κόσμο", δηλαδή, είτε με τις λειτουργίες με τις οποίες ο εν λόγω Πράκτορας συνορεύει αλλά που παρέχονται από άλλους Πράκτορες, είτε με το Δίαυλο Πληροφοριών Πλαισίου. Τα σημεία σύνδεσης ομαδοποιούνται κάτω από το στοιχείο `<DefineEndPoints>` και καθένα από αυτά εκφράζεται μέσω ενός στοιχείου `<EndPoint>`, το οποίο χαρακτηρίζεται από ένα όνομα, που αποτελεί το μοναδικό αναγνωριστικό του, (χαρακτηριστικό `Name`) και έναν τύπο (χαρακτηριστικό `Type`), με το τελευταίο να παίρνει μία από τις τιμές {`data`, `control`} προσδιορίζοντας το αν η σύνδεση αφορά ροή ελέγχου ή δεδομένων. Εσωτερικά, κάθε `EndPoint` περιέχει ένα από τα ακόλουθα υποστοιχεία, ανάλογα με τα χαρακτηριστικά του:

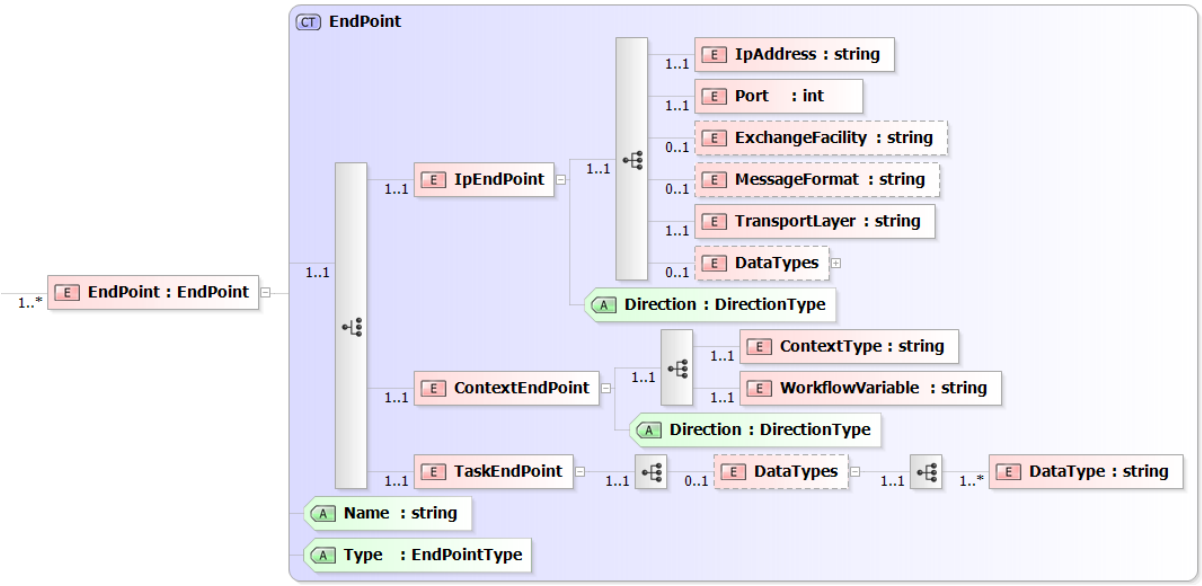
- `IpEndPoint`: Το στοιχείο `<IpEndPoint>` χρησιμοποιείται για να δηλώσει ένα σημείο σύνδεσης με κάποια εξωτερική οντότητα, με την οποία η θεωρούμενη λειτουργία θα πρέπει, κατά συνέπεια, να επικοινωνήσει μέσω δικτύου IP. Το χαρακτηριστικό `Direction`, παίρνοντας μία από τις τιμές {`input`, `output`} προσδιορίζει την κατεύθυνση της αντίστοιχης ροής ως προς το συγκεκριμένο Πράκτορα, έτσι ώστε αυτός να ξέρει αν πρόκειται να λάβει δεδομένα από ή να στείλει δεδομένα προς το συγκεκριμένο σημείο σύνδεσης, ενώ μια σειρά υποστοιχείων ορίζει περαιτέρω στοιχεία της σύνδεσης που θα πρέπει να ρυθμιστούν, δηλαδή την IP διεύθυνση (IpAddress), τη θύρα (Port), το πρωτόκολλο του στρώματος μεταφοράς (TransportLayer), το μορφότυπο των μηνυμάτων (MessageFormat) και λοιπά προσδιοριστικά του τρόπου επικοινωνίας (ExchangeFacility). Τέλος, το στοιχείο `<DataTypes>` μπορεί να χρησιμοποιηθεί για να δηλώσει τους τύπους δεδομένων που μεταφέρονται μέσω της εν λόγω σύνδεσης, καθένας από τους οποίους αποτελεί το περιεχόμενο ενός υποστοιχείου `<DataType>`.
- `ContextEndPoint`: Το στοιχείο `<ContextEndPoint>` χρησιμοποιείται για να σηματοδοτήσει την επικοινωνία του Πράκτορα με το Δίαυλο Πληροφοριών Πλαισίου. Αν το χαρακτηριστικό `Direction` λάβει την τιμή `input`, σημαίνει ότι ο Πράκτορας θα πρέπει να εγγραφεί στο Δίαυλο για ενημερώσεις πραγματικού χρόνου σχετικά με τον υποδεικνυόμενο τύπο πληροφορίας πλαισίου (υποστοιχείο `ContextType`) ή τη μεταβλητή ροής εργασιών που προσδιορίζεται (υποστοιχείο `WorkflowVariable`). Γενικά, η πληροφορία την οποία χρειάζεται να λάβει κάθε Πράκτορας από το Δίαυλο προκύπτει από τους περιορισμούς που σχετίζονται με τις εργασίες που αναλαμβάνει. Αν, από την άλλη, το χαρακτηριστικό `Direction` λάβει την τιμή `output`, ο Πράκτορας θα πρέπει, με την έναρξη της λειτουργίας της υποκείμενης οντότητας, να ξεκινήσει να δημοσιεύει την προσδιοριζόμενη πληροφορία στο δίαυλο, κάθε φορά που αυτή καθίσταται διαθέσιμη. Εδώ θεωρούμε ότι κάθε Πράκτορας δημοσιεύει εξ ορισμού τις τιμές

των βασικών μεταβλητών που αφορούν την εκτέλεση των εργασιών του (βλ. Ενότητα 6.2.3) και όποιο άλλο τύπο πληροφορίας παράγεται από αυτές και συγχρόνως αποτελεί παράμετρο πλαισίου.

- `TaskEndPoint`: Το <TaskEndPoint> αφορά τις συνδέσεις μεταξύ λειτουργιών που πραγματοποιούνται από τον ίδιο τον Πράκτορα που αφορούν οι οδηγίες. Οι συνδέσεις αυτές είναι νοητές και η μόνη παράμετρος που τις χαρακτηρίζει είναι οι τύποι των μεταφερόμενων δεδομένων (στοιχείο <DataTypes>).



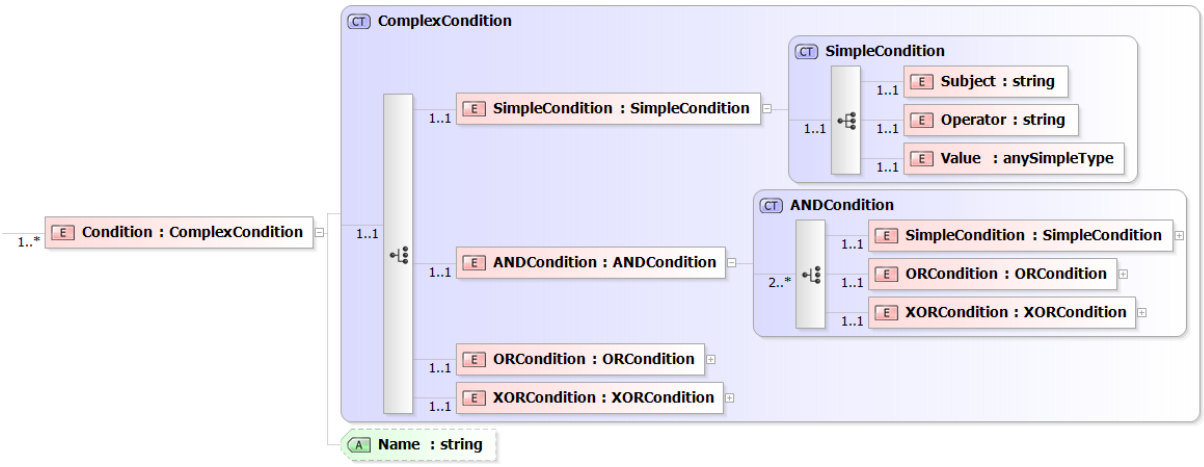
(α′) Βασική δομή.



(β′) Σημεία σύνδεσης.

Σχήμα 21: XML schema της ΓΠΟΕ.

Σε δεύτερη φάση, και εντός του στοιχείου <DefineConditions>, παρατίθενται όλες οι συνθήκες, αν υπάρχουν, που περιορίζουν με οποιοδήποτε τρόπο την εκτέλεση των εργασιών, αφορούν, δηλαδή είτε συνθήκες ροής οριζόμενες πάνω σε εισερχόμενες ή εξερχόμενες ακμές, είτε συνθήκες εργασιών που χαρακτηρίζουν τα αντίστοιχα προφίλ εκτέλεσης, είτε, τέλος, περιορισμούς επί οντοτήτων ροής εργασιών (ΟντΡΕ). Κάθε συνθήκη περιγράφεται από ένα στοιχείο <Condition> με μοναδικό χαρακτηριστικό το αναγνωριστικό του (`Name`), το οποίο εσωτερικά μπορεί να ορίζει ένα ακριβώς από τα ακόλουθα στοιχεία:



Σχήμα 22: XML schema της ΓΠΟΕ: συνθήκες.

- `SimpleCondition`: Το στοιχείο αυτό περιγράφει ουσιαστικά μια απλή έκφραση περιορισμού, οπότε, ακολουθώντας τον Ορισμό 3 του Κεφαλαίου 6, αποτελείται από τα υποστοιχεία <Subject>, <Operator>, <Value>.
- `ANDCondition` ή `ORCondition` ή `XORCondition`: καθένα από τα στοιχεία αυτά μοντελοποιεί την αντίστοιχη λογική σχέση και μπορεί εσωτερικά να περιλαμβάνει οποιοδήποτε συνδυασμό από στοιχεία απλών εκφράσεων (<SimpleCondition>) ή/και άλλες λογικές σχέσεις, οι οποίες αναλύονται περαιτέρω σε άλλες απλές εκφράσεις ή και λογικές σχέσεις, κ.ο.κ., με αποτέλεσμα μια εμφωλευμένη (nested) δομή ικανή να εκφράσει κάθε περιορισμό, όσο πολύπλοκος και αν είναι.

Στη συνέχεια, δίνεται η οδηγία στον Πράκτορα να εγκαταστήσει όλα τα κανάλια δεδομένων που απαιτούνται για την επικοινωνία με τις υπόλοιπες οντότητες. Για το σκοπό αυτό χρησιμοποιείται το στοιχείο <OpenEndPointConnections>, που με τη σειρά του περιλαμβάνει έναν αριθμό από στοιχεία <EndPoint>, καθένα από τα οποία έχει ως περιεχόμενο το αναγνωριστικό ενός σημείου σύνδεσης από αυτά που ορίστηκαν παραπάνω. Τα σημεία σύνδεσης τα οποία περιλαμβάνονται στο στοιχείο <OpenEndPointConnections> είναι όλα εκείνα των οποίων το χαρακτηριστικό Type λαμβάνει την τιμή data και τα οποία αντιστοιχίζονται συγκεκριμένα σε ένα στοιχείο <IpEndPoint>.

Το επόμενο βήμα είναι η περιγραφή της ροής εκτέλεσης που αφορά το συγκεκριμένο τεμάχιο καθεαυτής. Η ΓΠΟΕ χρησιμοποιεί δύο βασικά στοιχεία για να προσδιορίσει το συγχρονισμό των εργασιών, το <Sequence> και το <Flow>, εν μέρει εμπνευσμένα από άλλες γλώσσες περιγραφής ροής εργασιών, όπως είναι η δημοφιλής Γλώσσα Εκτέλεσης Επιχειρησιακών Διαδικασιών Υπηρεσιών Ιστού (Web Service Business Process Execution Language – WS-BPEL) [82]. Στο εσωτερικό ενός στοιχείου <Sequence>, όλες οι οριζόμενες ενέργειες εκτελούνται ακολουθιακά, με βάση τη σειρά με την οποία αναφέρονται. Αντίθετα, το στοιχείο <Flow> υποδηλώνει παραλληλία στην εκτέλεση, κατά συνέπεια όλες οι ενέργειες που ορίζονται στο εσωτερικό του είναι δυνατό να εκτελεστούν ταυτόχρονα ή

και με τυχαία σειρά. Έτσι, κάθε στοιχείο <Flow> περιλαμβάνει δύο ή περισσότερα στοιχεία <Sequence> προς παράλληλη εκτέλεση, καθένα από τα οποία μπορεί να αντιστοιχεί είτε σε μία μόνο εργασία είτε σε μια σειρά διαδοχικών βημάτων. Κάθε στοιχείο <Sequence>, από την άλλη, μπορεί να περιέχει έναν οποιοδήποτε αριθμό εργασιών και στοιχείων <Flow> τα οποία πρόκειται να εκτελεστούν ακολουθιακά. Όπως είναι προφανές, η δυνατότητα εμφώλευσης στοιχείων <Sequence> σε στοιχεία <Flow> και αντίστροφα καθιστά δυνατή την αναπαράσταση πολύπλοκων μορφών ροής ελέγχου. Μια εργασία, με τη σειρά της, περιγράφεται από τα ακόλουθα στοιχεία, τα οποία εμφανίζονται πάντα με αυτή τη σειρά σε ένα <Sequence>, καθώς η εργασία πραγματοποιείται ουσιαστικά μέσα από την ακολουθιακή εκτέλεση των αντίστοιχων βημάτων:

- Receive: Το στοιχείο αυτό δηλώνει εκείνο ή εκείνα από τα σημεία σύνδεσης που έχουν οριστεί παραπάνω από τα οποία η θεωρούμενη εργασία χρειάζεται να λάβει κάποια πληροφορία (υποστοιχείο <EndPoint>). Το χαρακτηριστικό Synch προσδιορίζει αν, στην περίπτωση πολλαπλών εισερχόμενων συνδέσεων, αυτές συγχρονίζονται ή όχι, με βάση τις προδιαγεγραμμένες τιμές των isControlSync και isDataSync της αντίστοιχης εργασίας στο MPE. Στην παρούσα υλοποίηση μπορεί να πάρει μόνο δύο τιμές (θεωρώντας μόνο έναν τύπο εισερχόμενης ροής), True ή False, παρ' όλα αυτά κατάλληλες επεκτάσεις θα επέτρεπαν την κάλυψη περισσότερο σύνθετων περιπτώσεων. Επίσης, στην περίπτωση που τα δεδομένα εισόδου που απαιτείται να λάβει η εργασία για να εκτελεστεί διαφέρουν ανάλογα με τις συνθήκες (κάτι που προκύπτει από τις εισερχόμενες ακμές σε συνδυασμό με την παράμετρο Synch), τα σημεία σύνδεσης χωρίζονται σε διαφορετικά στοιχεία <Receive>, ώστε καθένα από τα τελευταία τα περιλαμβάνει όλα τα σημεία σύνδεσης που ισχύουν υπό τις ίδιες συνθήκες. Έπειτα, κάθε τέτοιο στοιχείο <Receive> τοποθετείται μέσα σε ένα στοιχείο <EvaluateReceiveCondition>, το οποίο, μέσω του χαρακτηριστικού Condition, δείχνει σε εκείνο το στοιχείο <Condition> που περιγράφει τις σχετικές συνθήκες.

- WaitExecutionToken: Το στοιχείο <WaitExecutionToken> χρησιμοποιείται αντί του <Receive> όταν η εργασία που περιγράφεται είναι κάποια από τις αρχικές της ροής εργασιών, οπότε περιμένει την κατάλληλη σήμανση ελέγχου από τον Ενορχηστρωτή, και όχι από κάποιο άλλο Πράκτορα.

- Execute: Το στοιχείο <Execute> είναι αυτό που κατεξοχήν κατευθύνει την εκτέλεση της εργασίας. Το υποστοιχείο του <Operation> έχει ως περιεχόμενο το όνομα εκείνου του μέλους του γράφου των λειτουργιών στην ΟΣΜΠ που περιγράφει την ακριβή λειτουργία που επιτελείται στα πλαίσια της εργασίας, προκειμένου ο Πράκτορας να πραγματοποιήσει την κατάλληλη κλήση προς την υποκείμενη οντότητα. Από εκεί και πέρα, το στοιχείο <ExecutionModes> μπορεί να χρησιμοποιηθεί για να περιγράψει με περισσότερη λεπτομέρεια έναν ή περισσότερους τρόπους εκτέλεσης της υποκείμενης λειτουργίας, στη βάση των προφίλ εκτέλεσης του MPE. Στην κατεύθυνση αυτή, κάθε

υποστοιχείο <ExecutionMode> περιλαμβάνει τα ακόλουθα (ή όσα από αυτά προσδιορίζονται στο MPE):

- OperationParameters: Το στοιχείο αυτό χρησιμοποιείται για τη δήλωση των παραμέτρων εκτέλεσης που αφορούν τη λειτουργία. Κάθε παράμετρος ορίζεται με τη βοήθεια του στοιχείου <ParameterName> που περιέχει το όνομά της και του <ParameterValue> που τοποθετείται ακριβώς από κάτω και δείχνει την τιμή της συνοδευόμενη και από τον τελεστή της αντίστοιχης έκφρασης. Ο τελεστής είναι συνήθως ο equals, ωστόσο δεν αποκλείεται και η χρήση άλλων τελεστών, ενώ η τιμή καθεαυτή μπορεί να είναι και κάποια έκφραση ή κάποια πιο σύνθετη δομή. Σε κάθε περίπτωση, ολόκληρη η τιμή της παραμέτρου, όποια και αν είναι αυτή, μαζί με τον τελεστή αποτελούν με τη μορφή κειμένου το περιεχόμενο του στοιχείου <ParameterValue>, θεωρώντας ότι ο Πράκτορας θα είναι σε θέση να το επεξεργαστεί και αξιοποιήσει. Στο παρόν δε λαμβάνεται υπόψη το ενδεχόμενο χρήσης λογικών σχέσεων στον ορισμό παραμέτρων. Πράγματι, η συνήθης περίπτωση είναι αυτές να συνδέονται, ιδίως στο τελικό στάδιο της εκτέλεσης, με σχέση σύζευξης μεταξύ τους, οπότε και αρκεί να παρατίθενται απλά ως ζεύγη ονόματος–τιμής.
- Actors: Το στοιχείο <Actors> χρησιμοποιείται για τον ορισμό των δραστών που πρόκειται να αναλάβουν την εκτέλεση της εργασίας. Αν οι δράστες είναι περισσότεροι του ενός, το χαρακτηριστικό του ActorRelation δηλώνει τη λογική σχέση που τους συνδέει[43]. Κάθε δράστης ορίζεται εσωτερικά με τη βοήθεια είτε του στοιχείου <AbstractActor> είτε του <ConcreteActor>, ανάλογα με τον τύπο του. Κάθε <AbstractActor> μπορεί να χαρακτηρίζεται επιπλέον από το χαρακτηριστικό <ActorConstraint>, το οποίο δείχνει στο αναγνωριστικό ενός στοιχείου <Condition> που έχει οριστεί παραπάνω και διατυπώνει τυχόν περιορισμούς που αφορούν την εν λόγω αφηρημένη έννοια. Η τελευταία εμφανίζεται ως το περιεχόμενο του <AbstractActor> και προέρχεται από τους σχετικούς γράφους του Σημασιολογικού Μοντέλου Πληροφοριών. Ένα στοιχείο <ConcreteActor>, από την άλλη, συνοδεύεται από το χαρακτηριστικό Type, προκειμένου να υποδείξει στον Πράκτορα τη φύση της οντότητας που προσδιορίζεται μέσω του περιεχομένου του και, κατά συνέπεια, το πώς θα πρέπει αυτός να την αντιμετωπίσει. Αν η τιμή του χαρακτηριστικού αυτού είναι Constant, σημαίνει ότι το αντίστοιχο κείμενο αναφέρεται άμεσα σε μια συγκεκριμένη οντότητα με το καταχωρημένο αναγνωριστικό της (π.χ., στην περίπτωση ενός ανθρώπου, με το όνομά του), ενώ αν είναι ContextValue, το περιεχόμενο του στοιχείου αναφέρεται σε μια συγκεκριμένη μεν οντότητα, αλλά έμμεσα, μέσω, λόγου χάρη, κάποιας μεταβλητής ροής εργασιών ή της τιμής που λαμβάνει μια παράμετρος πλαισίου (μπορεί, π.χ., να δηλώνει τη συγκεκριμένη, κατά τη φάση της εκτέλεσης, οντότητα που συνι-

[43]Στην παρούσα υλοποίηση θεωρήθηκε η απλή περίπτωση όπου τυχόν λογικές σχέσεις μεταξύ δραστών και αντικειμένων επενέργειας ορίζονται το πολύ σε βάθος 1.

στά το δράστη μιας άλλης εργασίας της ροής).

– `Assets`: Με τη βοήθεια του στοιχείου αυτού ορίζονται, κατά πλήρη αντιστοιχία με τους δράστες, τα αντικείμενα επενέργειας της εργασίας. Οι σχετικές πληροφορίες παρέχονται μέσω των στοιχείων <AbstractAsset> και <ConcreteAsset> και των χαρακτηριστικών `AssetRelation`, `AssetConstraint` και `Type`.

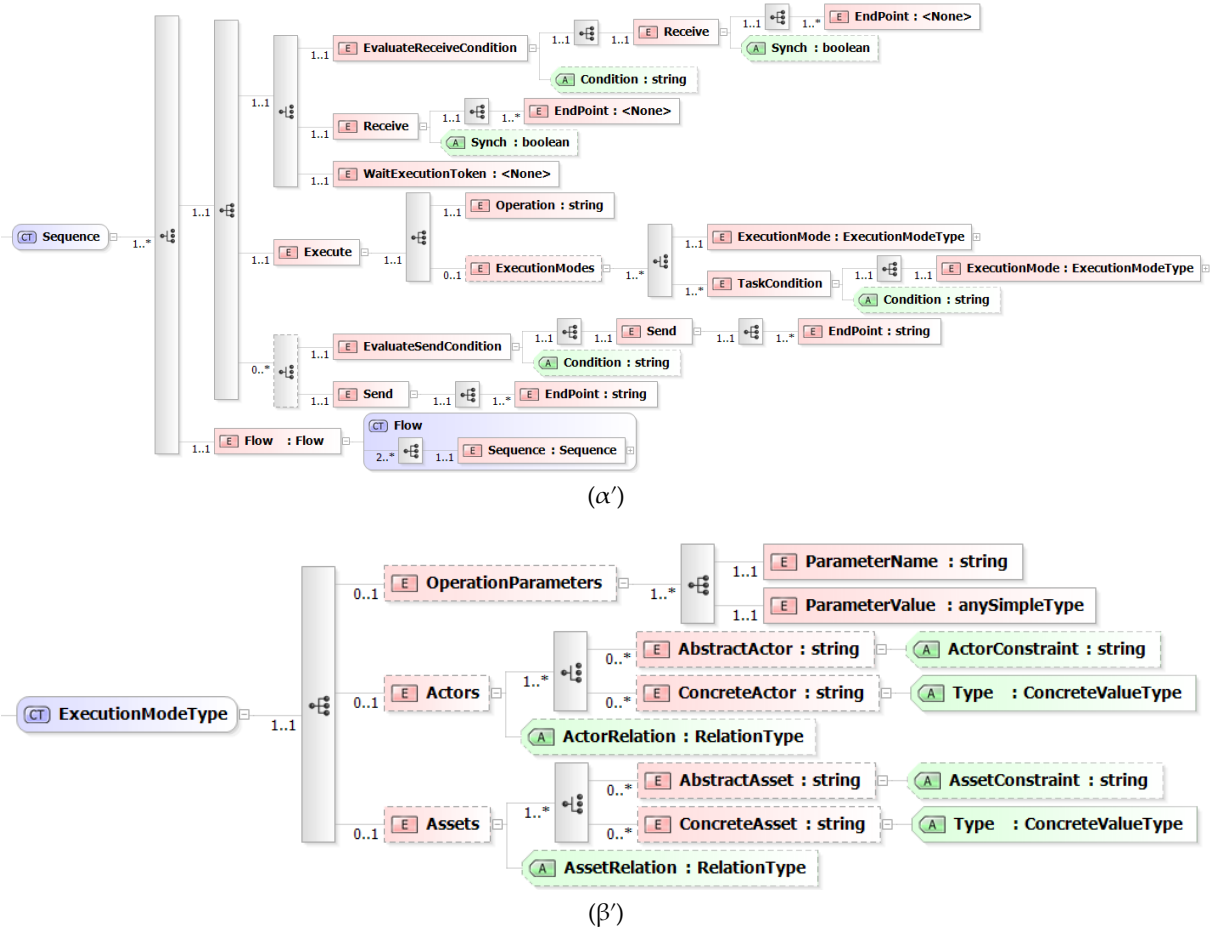
Αν το αντίστοιχο προφίλ εκτέλεσης περιλαμβάνει και κάποια συνθήκη, το <Execution-Mode> περικλείεται μέσα σε ένα στοιχείο <TaskCondition>, το χαρακτηριστικό `Condition` του οποίου παίρνει ως τιμή το αναγνωριστικό του κατάλληλου στοιχείου <Condition>.

- `Send`: Αυτό που ακολουθεί την εκτέλεση μιας εργασίας ή την επεξεργασία που αυτή πραγματοποιεί είναι η διοχέτευση των δεδομένων εξόδου προς τις αμέσως επόμενες εργασίες (εκτός και αν δεν ακολουθεί άλλη εργασία). Σε αυτή την κατεύθυνση, το στοιχείο <Execute> ακολουθούν ένα ή περισσότερα στοιχεία <Send>, το περιεχόμενο καθενός από τα οποία είναι το αναγνωριστικό ενός σημείου σύνδεσης. Κάθε στοιχείο <Send> που αντιστοιχεί σε ακμή συνοδευόμενη από περιορισμούς περικλείεται σε ένα στοιχείο `EvaluateSendCondition`, το χαρακτηριστικό `Condition` του οποίου δείχνει στο αναγνωριστικό του αντίστοιχου στοιχείου <Condition>.

9.3 Διακίνηση Πληροφοριών Πλαισίου και Διαθέσιμων Λειτουργιών

Δυο βασικές υποδομές της θεωρούμενης υπηρεσιοστραφούς αρχιτεκτονικής αποτελούν, όπως είδαμε συνοπτικά και στο Κεφάλαιο 4, ο Δίαυλος Πληροφοριών Δυνατοτήτων (Capabilities Bus) και ο Δίαυλος Πληροφοριών Πλαισίου (Context Bus). Ο πρώτος είναι υπεύθυνος για την παροχή πληροφοριών που αφορούν τις λειτουργίες που προσφέρει προς αξιοποίηση το σύστημα (συνιστώντας κατά κάποιο τρόπο ένα σημασιολογικό κατάλογο υπηρεσιών), ενώ ο δεύτερος παρακολουθεί τις πληροφορίες πλαισίου πραγματικού χρόνου και επιτρέπει τη διακίνησή τους.

Ο Δίαυλος Πληροφοριών Δυνατοτήτων καθιστά δυνατή την ανακάλυψη των απαιτούμενων λειτουργιών και το συνεπή, λειτουργικά αλλά και κανονιστικά, συνδυασμό τους για το σχηματισμό ροών εργασιών. Υλοποιείται ως υποδομή Δημοσίευσης/Συνδρομής (Publish/Subscribe) [107], η οποία επιτρέπει τη δημοσίευση και ανάκτηση πληροφοριών που αφορούν τις δυνατότητες των διάφορων υποκείμενων οντοτήτων με βάση τα ίδια τα σημασιολογικά χαρακτηριστικά των πληροφοριών αυτών και με ασύγχρονο τρόπο. Έτσι, σε πρώτη φάση, κάθε Πράκτορας δημοσιεύει στο Δίαυλο Πληροφοριών Δυνατοτήτων πληροφορίες απαραίτητες για την ανακάλυψη της οντότητας που εκπροσωπεί με τη μορφή σημασιολογικά επισημειωμένων περιγραφών υπηρεσιών. Η αλληλεπίδραση αυτή λαμβάνει χώρα μετά από κάθε προσθήκη ή ενημέρωση μιας λειτουργίας αλλά και μετά από



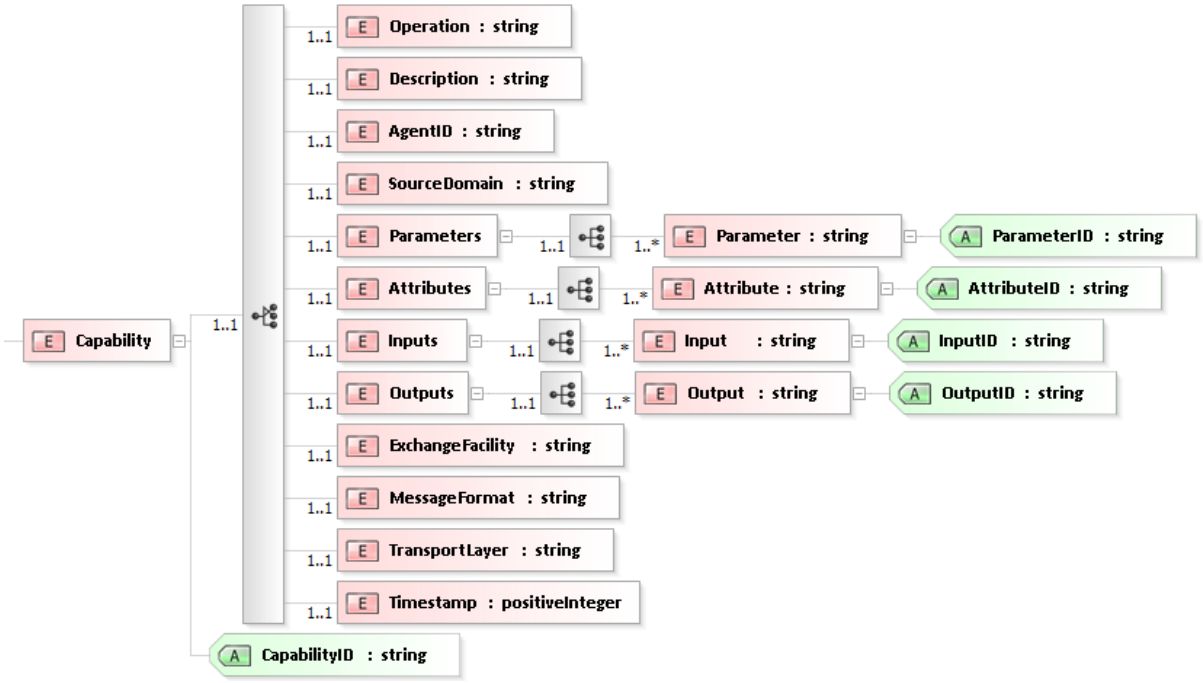
Σχήμα 23: XML schema της ΓΠΟΕ: ροή εκτέλεσης.

οποιαδήποτε ανιχνεύσιμη μεταβολή της ή διακύμανση της διαθεσιμότητάς της σε πραγματικό χρόνο. Σημειώνεται ότι, πέρα από τις δυνατότητες μεμονωμένων πρακτόρων, και σύμφωνα με το πνεύμα της αναχρησιμοποίησης και της τμηματικής σύνθεσης υπηρεσιών, μπορούν να διατίθενται ως υπηρεσίες και οι ίδιες οι ροές εργασιών που προκύπτουν κατά τη Φάση Σχεδιασμού. Σε μια τέτοια περίπτωση είναι το Περιβάλλον Σχεδιασμού που δημοσιεύει ενιαία και αυτόνομα μια ροή εργασιών ως την αντίστοιχη δυνατότητα–υπηρεσία. Από την άλλη, κατά τη Φάση Σχεδιασμού, η Μηχανή Εντοπισμού Δυνατοτήτων ενημερώνεται από το Δίαυλο Πληροφοριών Δυνατοτήτων σχετικά με την ικανότητα του συστήματος να προσφέρει τις επιθυμητές υπηρεσίες, ενώ κατά τη Φάση Εκτέλεσης ο Συντονιστής Ροής Εργασιών κάθε Ενορχηστρωτή εγγράφεται σε αυτόν για ενημερώσεις προκειμένου να εντοπίσει τις συγκεκριμένες οντότητες που προσφέρουν τις υπηρεσίες που απαιτούνται από το αντίστοιχο ΜΡΕ και στη συνέχεια να τις "καλέσει" αποστέλλοντάς τους τις σχετικές οδηγίες εκτέλεσης. Με άλλα λόγια, η πρώτη περίπτωση έχει να κάνει με τη διαβεβαίωση για τη διαθεσιμότητα των υπηρεσιών εντός του συστήματος, ενώ η δεύτερη αφορά τη σύνδεση με τις συγκεκριμένες οντότητες που προσφέρουν τις ζητούμενες υπηρεσίες.

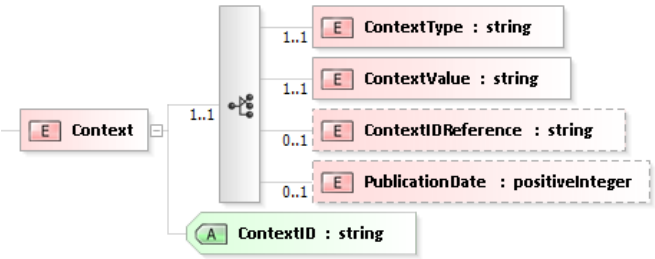
Ο Δίαυλος Πληροφοριών Πλαισίου ενισχύει περαιτέρω την ολοκλήρωση σε λογικό

επίπεδο μεταξύ ετερογενών οντοτήτων, επιτρέποντας τη διακίνηση πληροφοριών πλαισίου με ευέλικτο, κλιμακούμενο και ακριβή τρόπο, ώστε οι υποκείμενες οντότητες να μπορούν να διαλειτουργούν σε ό,τι αφορά συμβάντα, τιμές παραμέτρων πραγματικού χρόνου, κλπ.. Έχει και αυτός υλοποιηθεί ως σύστημα Δημοσίευσης/Συνδρομής, στο οποίο η δημοσίευση και ανάκτηση πληροφοριών πλαισίου βασίζονται στους σχετικούς σημασιολογικούς τύπους. Εξάλλου, το μοντέλο επικοινωνίας Δημοσίευσης/Συνδρομής θεωρείται ιδανικό για τη διάδοση συμβάντων σε όλη την έκταση ενός συστήματος, επιτυγχάνοντας πλήρως τη μη-συσχέτιση των επικοινωνουσών οντοτήτων σε τρεις διαστάσεις: χρόνο, χώρο και συγχρονισμό. Έτσι, με βάση αυτό το σχήμα αλληλεπίδρασης, κάθε Πράκτορας αφενός δημοσιεύει πληροφορίες πλαισίου που προέρχονται από την οντότητα την οποία εκπροσωπεί και αφετέρου εγγράφεται για ενημερώσεις σχετικά με πληροφορίες πλαισίου που η υποκείμενη οντότητα χρειάζεται και στις οποίες καλείται να προσαρμόσει κατάλληλα τη λειτουργία της, ακολουθώντας φυσικά τις οδηγίες του αντίστοιχου τεμαχίου.

Η αρχιτεκτονική και η βάση υλοποίησης των δυο Διαύλων είναι πανομοιότυπες, ωστόσο δεν εξετάζονται εδώ, καθώς ξεφεύγουν από τους στόχους της διατριβής. Αναφορικά με το μοντέλο δεδομένων που ακολουθείται, και στις δύο περιπτώσεις η προς δημοσίευση πληροφορία αναπαρίσταται σε XML και οργανώνεται με βάση το σημασιολογικό της τύπο. Για τις περιγραφές των δυνατοτήτων–υπηρεσιών που παρέχουν οι διάφορες οντότητες, η οργάνωση αυτή εδράζει στο γράφο των Λειτουργιών της ΟΣΜΠ (βλ. Ενότητα 4.4) και βάση αυτής ο Δίαυλος Δυνατοτήτων αποθηκεύει για καθεμιά οντότητα μια δομή από μετα-δεδομένα που περιγράφει τις δυνατότητές της. Από την άλλη, η οργάνωση των πληροφοριών πλαισίου είναι πιο σύνθετη υπόθεση, καθώς πλήθος παραγόντων μπορούν να θεωρηθούν ότι συνδιαμορφώνουν τις εκάστοτε συνθήκες πλαισίου. Οι δομές XML που χρησιμοποιούνται για την αναπαράσταση των υπηρεσιών και των πληροφοριών πλαισίου περιγράφονται, αντίστοιχα, από τα Σχήματα 24 και 25, ενώ οι Πίνακες 1 και 2 εξηγούν τη σημασία των χρησιμοποιούμενων XML στοιχείων. Το Σχήμα 26 απεικονίζει, ως παράδειγμα, την περιγραφή της δυνατότητας (capability) που παρέχεται από κάποιο απομακρυσμένο τομέα και μπορεί να χρησιμοποιηθεί στα πλαίσια μιας ροής εργασιών που αφορά την ανίχνευση εισβολών (intrusion detection). Τέλος, το Σχήμα 27 δείχνει το τμήμα εκείνο του γραφικού περιβάλλοντος το οποίο χρησιμοποιείται για τη δημοσίευση και διάθεση μιας ροής εργασιών που έχει προκύψει από το Περιβάλλον Σχεδιασμού ως ενιαίας υπηρεσίας.



Σχήμα 24: Το XML schema της περιγραφής δυνατοτήτων



Σχήμα 25: Το XML schema της περιγραφής πληροφοριών πλαισίου.

```
<Capability CapabilityID="AD10508">
    <Operation>CollaborativeIDS_ProvideFeedback</Operation>
    <Description>This capability represents a functionality offered by a remote
    domain, that provides a threat model based on local intrusion-related data
    and the alert it receives.</Description>
    <AgentID>BoundaryAgent</AgentID>
    <SourceDomain>ICBNET_NTUA</SourceDomain>
    <Inputs>
        <Input InputID="input1">IDMEFAlert</Input>
    </Inputs>
    <Outputs>
        <Output OutputID="output1">IntrusionDetectionThreatModel</Output>
    </Outputs>
    <ExchangeFacility>STANDARD</ExchangeFacility>
    <MessageFormat>IDMEF</MessageFormat>
    <TransportLayer>TCP_PLAIN2WAY</TransportLayer>
    <Timestamp>1368971563112</Timestamp>
</Capability>
```

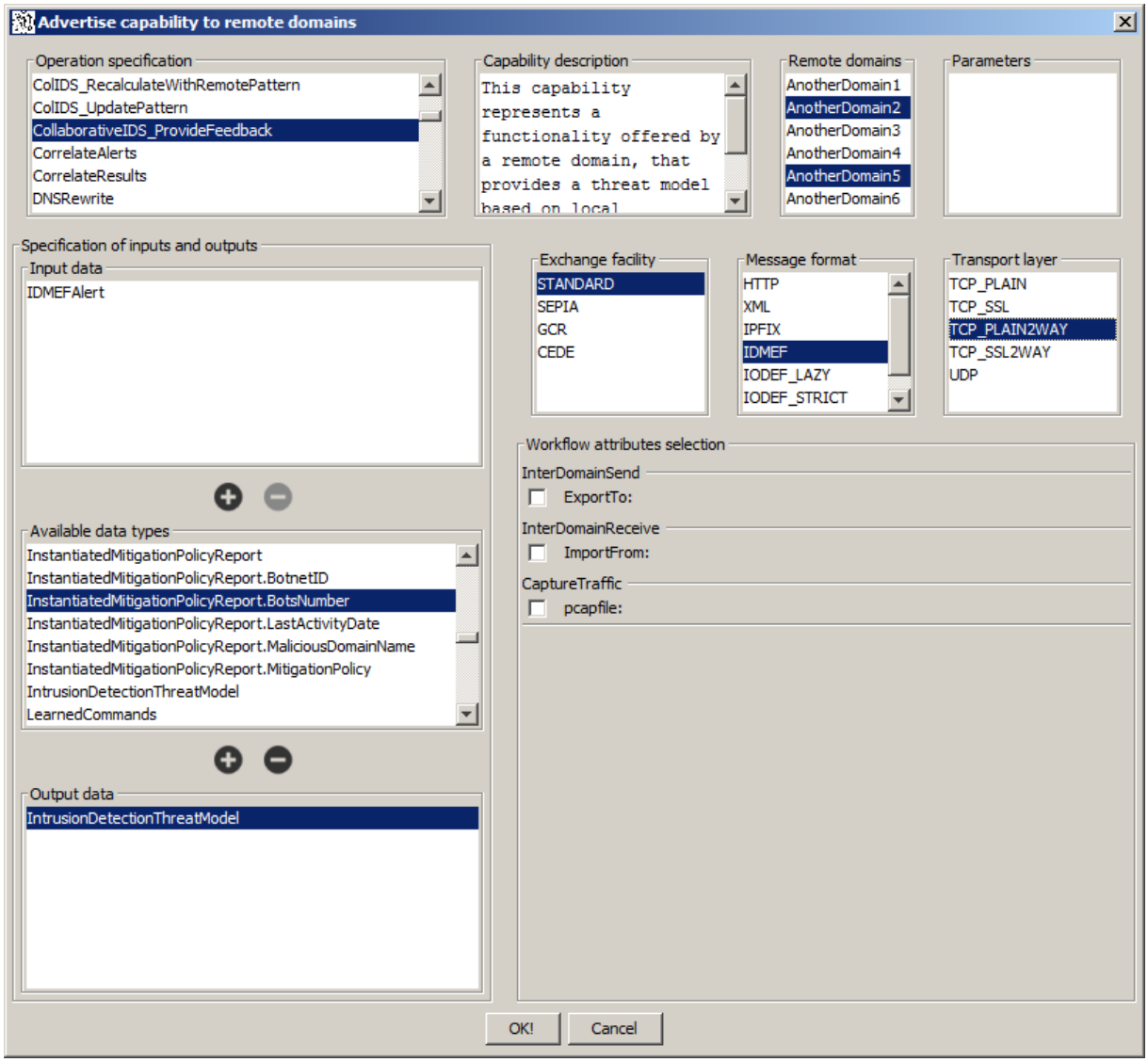
Σχήμα 26: Παράδειγμα περιγραφής δυνατότητας.

Πίνακας 1: Επεξήγηση των XML στοιχείων μιας περιγραφής δυνατότητας.

Στοιχείο XML	**Περιγραφή**
`Operation`	Η σημασιολογικά ορισμένη στην ΟΣΜΠ (βλ. Ενότητα 4.4) λειτουργία η οποία υλοποιείται από την εν λόγω παρεχόμενη υπηρεσία/δυνατότητα.
`Description`	Η περιγραφή, σε φυσική γλώσσα, της παρεχόμενης υπηρεσίας.
`AgentID`	Το αναγνωριστικό του Πράκτορα που έχει δημοσιοποιήσει τη συγκεκριμένη δυνατότητα.
`SourceDomain`	Ο τομέας ελέγχου ο οποίος διαθέτει την υπηρεσία (εφόσον πρόκειται για σύστημα που υποστηρίζει τη συνεργασία μεταξύ διαφορετικών τομέων στα πλαίσια της εκτέλεσης μιας ροής εργασιών).
`Parameters`	Οι (δυναμικές) παράμετροι προς ρύθμιση, προκειμένου να εκτελεστεί η λειτουργία.
`Attributes`	Ιδιότητες (στατικές) που χαρακτηρίζουν τη συγκεκριμένη υπηρεσία.
`Inputs`	Τα απαιτούμενα δεδομένα εισόδου.
`Outputs`	Οι τύποι δεδομένων που παράγονται από την εκτέλεση της υπηρεσίας.
`ExchangeFacility`	Το στοιχείο αυτό χρησιμεύει στον προσδιορισμό ποικίλων χαρακτηριστικών αναφορικά με τον τρόπο παροχής της υπηρεσίας (π.χ., τρόπος επικοινωνίας με τις αιτούσες οντότητες).
`MessageFormat`	Ο μορφότυπος των μηνυμάτων που ανταλλάσσονται· ενδεικτικές τιμές θα μπορούσαν να είναι, για παράδειγμα, οι `HTTP`, `SIP`, `IODEF`, `IDMEF`, `IPFIX`, κλπ..
`TransportLayer`	Το πρωτόκολλο του στρώματος μεταφοράς (TCP, UDP) που χρησιμοποιείται για την ανταλλαγή των δεδομένων.
`Timestamp`	Μια χρονοσφραγίδα (timestamp) (εκφρασμένη σε χιλιοστά του δευτερολέπτου από την 1η Ιανουαρίου 1970, 00:00:00 GMT), η οποία δηλώνει τη στιγμή που η δυνατότητα αυτή εγγράφηκε στο Δίαυλο· χρησιμοποιείται για σκοπούς καταγραφής και ελέγχου.

Πίνακας 2: Επεξήγηση των XML στοιχείων της αναπαράστασης πληροφοριών πλαισίου.

Στοιχείο XML	**Περιγραφή**
`ContextType`	Ο σημασιολογικός τύπος της εν λόγω πληροφορίας, όπως αυτός ορίζεται στην ΟΣΜΠ (βλ. Ενότητα 4.4).
`ContextValue`	Η τιμή που λαμβάνει η θεωρούμενη παράμετρος πλαισίου κατά τη στιγμή της δημοσίευσής της στο Δίαυλο.
`ContextIDReference`	Το αναγνωριστικό ενός αρχικού μηνύματος πλαισίου που δημοσιοποιήθηκε στο Δίαυλο. Η τιμή αυτή τίθεται σε όλα τα μετα-συμβάντα πλαισίου που δημιουργούνται αυτόματα από κάποιο τέτοιο αρχικό μήνυμα (με βάση τις σημασιολογικές σχέσεις μεταξύ τύπων πληροφοριών πλαισίου που ορίζει η ΟΣΜΠ).
`PublicationDate`	Μια χρονοσφραγίδα (timestamp) (εκφρασμένη σε χιλιοστά του δευτερολέπτου από την 1η Ιανουαρίου 1970, 00:00:00 GMT), η οποία εκφράζει τη χρονική στιγμή κατά την οποία η συγκεκριμένη πληροφορία πλαισίου ελήφθη από το Δίαυλο.



Σχήμα 27: Δημοσίευση ροής εργασιών ως ενιαίας υπηρεσίας/δυνατότητας.

Κεφάλαιο 10

Αξιολόγηση της Προτεινόμενης Λύσης

10.1 Αξιολόγηση σε Σχέση με τις Νομικές και Κανονιστικές Απαιτήσεις

Στην Ενότητα 2.5 κωδικοποιήθηκαν οι απαιτήσεις που απορρέουν από το Νομικό και Κανονιστικό Πλαίσιο αναφορικά με την ορθή χρήση των προσωπικών δεδομένων σε συγκεκριμένες αρχές. Η παρούσα ενότητα αναφέρεται στον τρόπο με τον οποίο η προτεινόμενη λύση ανταποκρίνεται αποτελεσματικά στις απαιτήσεις αυτές. Σημειώνεται ότι, εκτός από τα όσα αναφέρονται στο Κεφάλαιο 2, ελήφθησαν υπόψη και τα καθιερωμένα κριτήρια του EuroPriSe[44], τα οποία πρέπει να ικανοποιούνται προκειμένου οποιοδήποτε πληροφοριακό σύστημα, άρα και κάθε σύστημα ροής εργασιών, να θεωρείται συμβατό με τις αρχές προστασίας της ιδιωτικότητας.

10.1.1 Νομιμότητα της Επεξεργασίας των Δεδομένων

Η προτεινόμενη λύση παρέχει τα αναγκαία μέσα, τόσο σε επίπεδο σχεδιασμού όσο και σε επίπεδο εκτέλεσης, ώστε οι υφιστάμενες αρχές ιδιωτικότητας να μπορούν να επιβληθούν, οδηγώντας στην εξασφάλιση της νομιμότητας οποιασδήποτε επεξεργασίας δεδομένων λαμβάνει χώρα στα πλαίσια μιας ροής εργασιών. Κατ' αρχάς, για κάθε είδους ενέργεια που πραγματοποιείται λαμβάνεται υπόψη ο σκοπός που αυτή εξυπηρετεί, ενώ ο τρόπος προδιαγραφής των προς εκτέλεση εργασιών αλλά και η μεθοδολογία ελέγχου μιας ροής εργασιών συνολικά βασίζονται στην αρχή του ελέγχου πρόσβασης, η οποία οφείλει να διέπει τη λειτουργία κάθε συστήματος με επίγνωση ιδιωτικότητας. Επιπλέον, εξασφαλίζεται ο ενδελεχής και σε ευρεία κλίμακα έλεγχος της ροής της πληροφορίας μεταξύ των

[44]https://www.european-privacy-seal.eu/

εμπλεκόμενων οντοτήτων, με έμφαση, μεταξύ άλλων, στην παρεμπόδιση της διασύνδεσης δεδομένων που αθροιστικά θεωρούμενα μπορούν να οδηγήσουν σε παραβιάσεις της ιδιωτικότητας. Στο τελευταίο συμβάλλει και η χρήση μηχανισμών που επιτρέπουν την επιβολή Διαχωρισμού και Σύνδεσης Καθηκόντων, περιορισμών που αποκτούν ιδιαίτερη σημασία σε περιβάλλοντα ροών εργασιών στην κατεύθυνση της αποφυγής ποικίλων συγκρούσεων και διαρροών. Από την άλλη, συγκεκριμένα η δυνατότητα αυτόματης ενσωμάτωσης εργασιών είναι σε θέση να εξασφαλίσει την πραγματοποίηση ποικίλων ενεργειών που συχνά κρίνονται απαραίτητες από τη Νομοθεσία, προκειμένου να καθίσταται αποδεκτή η πρόσβαση σε δεδομένα και η συνακόλουθη επεξεργασία τους. Τέτοιες μπορεί να είναι, για παράδειγμα, οι λειτουργίες κρυπτογράφησης ή ψευδωνυμίας πάνω σε δεδομένα, ενέργειες που εκφράζουν τη με διάφορους τρόπους συμμετοχή του εκάστοτε υποκειμένου των δεδομένων ή την παρέμβαση των αρμόδιων αρχών, ή και λειτουργίες καταγραφής (logging) που καθιστούν δυνατή την απόδοση ευθύνης αναφορικά με οτιδήποτε λαμβάνει χώρα κατά την εκτέλεση μιας ροής εργασιών. Τέλος, το σύστημα βασίζεται αυστηρά στον ακριβή σημασιολογικό ορισμό των υποκείμενων εννοιών, εξυπηρετώντας τις απαιτούμενες διαφοροποιήσεις στην αντιμετώπιση των αντίστοιχων οντοτήτων, ενώ διαθέτει δομές, σε επίπεδο αρχιτεκτονικής αλλά και εννοιολογικής αναπαράστασης, που αποσκοπούν στην προσαρμογή της λειτουργίας του σε συνθήκες πλαισίου (context) και συμβάντα (events).

10.1.2 Σκοπός της Επεξεργασίας των Δεδομένων

Η παρουσία της έννοιας του σκοπού κυριαρχεί σε όλα τα επίπεδα της ακολουθούμενης προσέγγισης. Κατ' αρχάς ο σχεδιαστής μιας ροής εργασιών δηλώνει υποχρεωτικά το σκοπό ή τους σκοπούς τους οποίους η ροή αθροιστικά θα κληθεί να εξυπηρετήσει, ούτως ώστε να επαληθευτεί το κατά πόσο οι διάφορες εργασίες και ο τρόπος με τον οποίο σχετίζονται/συνδυάζονται είναι συμβατοί με τους σκοπούς αυτούς. Αυτό εξασφαλίζεται, σε ένα πρώτο επίπεδο, με τη συσχέτιση λειτουργιών (ιδιότητα `compliantWithPurpose`) και ρόλων (ιδιότητα `mayActForPurpose`) με συμβατούς σκοπούς, αλλά και τον ορισμό μιας ταξονομίας σκοπών (`isA`), ήδη στο θεωρούμενο Σημασιολογικό Μοντέλο Πληροφοριών, ενώ επιπρόσθετη ευελιξία και δυνατότητα για αυστηρότερες ρυθμίσεις παρέχεται μέσω της κεντρικής θέσης που κατέχει ο σκοπός στον ορισμό κάθε κανόνα του Σημασιολογικού Μοντέλου Πολιτικών. Ως εκ τούτου, το προκύπτον σύστημα δεν επιτρέπει πρόσβαση στα προσωπικά δεδομένα για σκοπούς άλλους εκτός από εκείνους που περιγράφει με αυστηρά καθορισμένο τρόπο εν είδει κανόνων ελέγχου πρόσβασης.

10.1.3 Αναγκαιότητα, Καταλληλότητα και Αναλογικότητα των Δεδομένων

Ο σημασιολογικός ορισμός των διαφόρων τύπων δεδομένων και των μεταξύ τους σχέσεων (`isA`, `isPartOf`, `moreDetailedThan`) στο Σημασιολογικό Μοντέλο Πληροφοριών, σε συνδυασμό με τον τρόπο ορισμού των εργασιών και των εξαρτήσεων δεδομένων στις

ροές εργασιών αλλά και στις οδηγίες συμβατότητας που τις αφορούν, καθιστούν δυνατό τον πλήρη έλεγχο της πρόσβασης στα δεδομένα. Εξάλλου, μέσω του μηχανισμού αυτόματης εισαγωγής εργασιών, μπορούν να παρεμβάλλονται πριν τα επίμαχα σημεία επεξεργασίας ειδικές εργασίες "φιλτραρίσματος" των διερχόμενων δεδομένων, ικανές να πραγματοποιούν την επιλογή (selection) ή προβολή (projection) αυτών ως προς συγκεκριμένα κριτήρια. Ως αποτέλεσμα των παραπάνω, τα προσωπικά δεδομένα τα οποία υφίστανται συλλογή ή/και επεξεργασία είναι τελικά πάντοτε τα αναγκαία, κατάλληλα και απολύτως απαραίτητα συναρτήσει της λειτουργίας που επιτελείται (και κατ' επέκταση του αντίστοιχου σκοπού).

10.1.4 Ποιότητα των Δεδομένων

Οποιαδήποτε ενέργεια πρόσβασης στα δεδομένα στα πλαίσια μιας ροής εργασιών ελέγχεται τόσο στο επίπεδο των μεμονωμένων εργασιών όσο και μακροσκοπικά στη ροή που αυτά ακολουθούν. Με τον τρόπο αυτό η κακόβουλη τροποποίηση αποτρέπεται. Επιπλέον, μέσω των μηχανισμών προσθήκης κατάλληλων πρόσθετων εργασιών, μπορεί να παρέχεται στο υποκείμενο των δεδομένων, όπου χρειάζεται, η δυνατότητα άμεσης πρόσβασης στα δεδομένα του, ούτως ώστε να διασφαλίζει τη συνέπειά τους, την ακρίβεια και την ενημερωμένη κατάστασή τους, ενώ καθίσταται δυνατή και η ενσωμάτωση εργασιών για την αυτόματη διαγραφή των δεδομένων κάθε φορά που ισχύουν οι συνθήκες που προβλέπονται από τη Νομοθεσία. Ασφαλώς, πολύ σημαντικό ρόλο για τη διασφάλιση της ποιότητας των δεδομένων παίζει το ζήτημα της ασφάλειάς τους, κάτι που επιτυγχάνεται και πάλι με την εισαγωγή στα κατάλληλα σημεία της διαδρομής τους αντίστοιχων εργασιών (π.χ., κρυπτογράφηση) αλλά και με τον έλεγχο ιδιοτήτων της ροής εργασιών που αφορούν τον τρόπο μετάδοσής τους (π.χ., ιδιότητες ακμών που υποδεικνύουν ασφαλή κανάλια επικοινωνίας μεταξύ των εμπλεκομένων οντοτήτων).

10.1.5 Ταυτοποιήσιμα Δεδομένα

Στην παρούσα προσέγγιση κάθε δεδομένο είναι σημασιολογικά αναγνωρίσιμο και αντιμετωπίζεται ανάλογα με το σημασιολογικό του τύπο. Με άλλα λόγια, σε ένα πρώτο επίπεδο, προκύπτει από το ίδιο το Σημασιολογικό Μοντέλο Πληροφοριών ποιά δεδομένα είναι (βάσει του τύπου τους) εξ ορισμού ταυτοποιήσιμα, είναι, δηλαδή, σε θέση να ταυτοποιούν το υποκείμενο των δεδομένων. Από εκεί και πέρα, με την εισαγωγή της έννοιας της κατάστασης δεδομένων, το σύστημα είναι σε θέση κατ' αρχάς να αναγνωρίζει το βαθμό στον οποίο τα εκάστοτε δεδομένα είναι ταυτοποιήσιμα, και συνεπώς, όπου χρειάζεται, να αποτρέπει την πρόσβαση σε αυτά για σκοπούς επεξεργασίας ή αποθήκευσης. Επιπλέον, και όταν υπάρχει περιθώριο για κάτι τέτοιο, μπορούν να εισάγονται οι απαραίτητοι μηχανισμοί με τη μορφή εμβόλιμων εργασιών, οι οποίοι θα τα καθιστούν μη ταυτοποιήσιμα σε αποδεκτά πλαίσια, μεταβάλλοντας την κατάστασή τους. Για παράδειγμα, το ονοματεπώ-

νυμο ενός ατόμου θεωρείται εξ ορισμού ταυτοποιήσιμο, εκτός —ίσως— και αν βρίσκεται σε κρυπτογραφημένη μορφή. Σε αυτή την περίπτωση, αν η ακολουθούμενη μεθοδολογία ελέγχου διαπιστώσει ότι δεν έχει στο μεταξύ κρυπτογραφηθεί, εισάγει αυτόματα την κατάλληλη εργασία κρυπτογράφησης, ώστε να επιτραπεί η αποθήκευσή του.

10.1.6 Ειδικές Κατηγορίες Δεδομένων — Ευαίσθητα Δεδομένα

Στο πλαίσιο της προτεινόμενης λύσης, κάθε προσωπικό δεδομένο χαρακτηρίζεται από το σημασιολογικό ορισμό του, βάσει του Σημασιολογικού Μοντέλου Πληροφοριών. Επιπλέον, ο σημασιολογικός τύπος του κάθε προσωπικού δεδομένου λαμβάνεται υπόψη σε κάθε ενέργεια συλλογής ή επεξεργασίας του. Κατά συνέπεια και βάσει των κανόνων που ορίζονται στο Σημασιολογικό Μοντέλο Πολιτικών και των συνεπαγόμενων κατευθύνσεων που υπαγορεύονται από τις οδηγίες συμβατότητας, το κάθε δεδομένο ειδικής κατηγορίας, όπως είναι τα δεδομένα κίνησης και θέσης στο πλαίσιο κάποιας επικοινωνίας, τα δικαστικά και άλλα ευαίσθητα δεδομένα, υφίσταται συλλογή και επεξεργασία που βασίζεται σε κάθε περίπτωση στον ιδιαίτερο τύπο του.

10.1.7 Πληροφόρηση, Συγκατάθεση και λοιπά Δικαιώματα των Υποκειμένων των Δεδομένων

Η απαίτηση αυτή καλύπτεται μέσω της δυνατότητας επιβολής της εκτέλεσης εργασιών που είτε πραγματοποιούν την "αποστολή" ενημερώσεων στα υποκείμενα των δεδομένων αναφορικά με τις πράξεις παραχώρησης και επεξεργασίας των προσωπικών τους δεδομένων είτε ζητούν τη ρητή συγκατάθεσή τους για τα παραπάνω, όντας σε θέση ακόμα και να αναστείλουν την κρίσιμη επεξεργασία όπου αυτό κρίνεται σκόπιμο. Γενικεύοντας, ακόμα και σε περιπτώσεις όπου κάτι τέτοιο δεν είναι ευθέως εφαρμόσιμο, παρόμοιες απαιτήσεις εισάγουν την ανάγκη για ενσωμάτωση συμπληρωματικών ενεργειών σε μια ροή εργασιών, οι οποίες αποτελούν στην ουσία υποχρεώσεις που πρέπει να ικανοποιηθούν προκειμένου η όποια επεξεργασία να είναι αποδεκτή.

10.1.8 Ειδοποιήσεις και λοιπές Αρμοδιότητες / Εξουσιοδοτήσεις των Αρμοδίων Αρχών

Και αυτή η απαίτηση ικανοποιείται από τη δυνατότητα που προσφέρει το σύστημα για αυτόματη ενσωμάτωση συμπληρωματικών εργασιών, οι οποίες στην περίπτωση αυτή αφορούν είτε την ενεργή παρέμβαση είτε απλά την ειδοποίηση των αρμοδίων αρχών σχετικά με την εξέλιξη μιας ροής εργασιών.

10.1.9 Εποπτεία και Επιβολή Προστίμων

Η εποπτεία επιτυγχάνεται με τους μηχανισμούς που περιγράφηκαν αμέσως παραπάνω. Αναφορικά με την επιβολή προστίμων, ασφαλώς δεν είναι δυνατό να αποτελεί εξ ολοκλήρου αντικείμενο ενός τεχνολογικού συστήματος. Ωστόσο, η προτεινόμενη λύση παρέχει τα μέσα τόσο για την ανίχνευση των γεγονότων που χρίζουν επιβολής προστίμου, όσο και για την τεκμηρίωση των προστίμων, μέσω της δυνατότητας απόδοσης ευθύνης που προσφέρει. Το τελευταίο μπορεί να επιτευχθεί μέσω της καταγραφής των ενεργειών πρόσβασης σε ευαίσθητα δεδομένα στα πλαίσια μιας ροής εργασιών (logging).

10.1.10 Διασύνδεση Δεδομένων

Η ακολουθούμενη προσέγγιση επιτυγχάνει τον αυστηρό έλεγχο της ροής και επεξεργασίας των δεδομένων, αφενός μέσω της ακριβούς μοντελοποίησής τους και αφετέρου σε επίπεδο επαλήθευσης. Πιο συγκεκριμένα, η μεταφερόμενη πληροφορία περιγράφεται λεπτομερώς στη βάση ποικίλων σημασιολογικών χαρακτηριστικών (τύπος, ιδιότητες, κατάσταση), ενώ παράλληλα το τμήμα αυτής που υφίσταται την οποιαδήποτε επεξεργασία αναπαρίσταται ρητά ως αντικείμενο επενέργειας της εκάστοτε εργασίας, οδηγώντας στη σαφή διάκριση μεταξύ πρόσβασης "μόνο για ανάγνωση" (read access) και "επεμβατικής" πρόσβασης (write access). Επιπλέον, η ιδιότητα `isDataSynch` που χαρακτηρίζει κάθε εργασία υποδηλώνει το κατά πόσο αυτή επεξεργάζεται συνδυαστικά τα εισερχόμενα δεδομένα. Με τη βοήθεια των μηχανισμών αυτών, η μεθοδολογία ελέγχου είναι κατόπιν σε θέση, βασιζόμενη κυρίως στις οδηγίες απαγόρευσης ροής και στις οδηγίες απαγόρευσης εκτέλεσης, να εντοπίσει και αποτρέψει τη διασύνδεση δεδομένων που προσπελαύνονται ή/και υφίστανται επεξεργασία από τις διάφορες εργασίες. Τέλος, η δυνατότητα μοντελοποίησης ενός ευρέως φάσματος περιορισμών που εκφράζουν Διαχωρισμό και Σύνδεση Καθηκόντων προωθεί περαιτέρω τον έλεγχο της συνδυαστικής πρόσβασης σε δεδομένα.

10.1.11 Ασφάλεια Δεδομένων και Εμπιστευτικότητα

Το σύστημα επιτρέπει την αυτόματη ενσωμάτωση σε μια ροή εργασιών των μηχανισμών εκείνων που επαρκούν ώστε να διασφαλίσουν τα επιθυμητά επίπεδα ασφάλειας και εμπιστευτικότητας των δεδομένων (π.χ., εργασίες κρυπτογράφησης). Επιπλέον, ελέγχοντας κάθε εργασία και κάθε ανταλλαγή δεδομένων, αποτρέπει οποιαδήποτε πρόσβαση σε δεδομένα από μη εξουσιοδοτημένες οντότητες. Τέλος, μέσω περιορισμών και λοιπών ιδιοτήτων που αφορούν τη μετάδοση της πληροφορίας, το εν λόγω σύστημα εξασφαλίζει ότι θα πληρούνται οι προϋποθέσεις για την ασφαλή μεταφορά της (π.χ., ασφαλή κανάλια επικοινωνίας, χρήση συγκεκριμένων πρωτοκόλλων, κλπ.).

10.1.12 Περιορισμός Πρόσβασης

Η προτεινόμενη λύση εφαρμόζει έλεγχο πρόσβασης σε υψηλό επίπεδο λεπτομέρειας και σε κάθε βήμα της επεξεργασίας. Κατ' αρχάς, κάθε εργασία, με τον τρόπο που ορίζεται, συνιστά στην ουσία μια πολιτική πρόσβασης: πράγματι, το ή τα προφίλ συμβατότητας που συνδέονται με αυτήν εκφράζουν το *ποιός* καλείται να πραγματοποιήσει *ποιά λειτουργία πάνω σε ποιό αντικείμενο επενέργειας*, προσδιορίζοντας πιθανώς και τις συνθήκες κάτω από τις οποίες αυτό επιτρέπεται να συμβεί. Η πληροφορία αυτή μεταφέρεται αμέσως πριν την εκτέλεση της ροής εργασιών στους Πράκτορες μέσω της XML δομής `<ExecutionMode>` της Γλώσσας Περιγραφής Οδηγιών Εκτέλεσης (ΓΠΟΕ), ενώ δηλώνεται επιπρόσθετα η πληροφορία την οποία θα πρέπει να λάβει ή/και αποστείλει κάθε οντότητα, και πιθανώς οι αντίστοιχες συνθήκες. Επιπλέον, οι οδηγίες συμβατότητας που κατευθύνουν τον έλεγχο και την τροποποίηση των ροών εργασιών προκύπτουν από ένα μοντέλο ελέγχου πρόσβασης και χρήσης, το οποίο περιλαμβάνει ένα σύνολο κανόνων που μπορούν να καλύπτουν όλους τους τύπους προσωπικών δεδομένων, λειτουργιών, ρόλων, κλπ. των εμπλεκομένων οντοτήτων. Με τον τρόπο αυτό, ο έλεγχος πρόσβασης αρχικά προδιαγράφεται κατά τη φάση του σχεδιασμού ως μέρος κάθε Μοντέλου Ροής Εργασιών (ΜΡΕ), ενώ η εφαρμογή/πραγμάτωσή του εξασφαλίζεται μέσω των οδηγιών εκτέλεσης, οι οποίες γνωστοποιούν επακριβώς τις προδιαγραφές αυτές στους Πράκτορες, ώστε οι τελευταίοι τελικά να τις υλοποιήσουν.

10.1.13 Αποθήκευση Δεδομένων

Ακόμα και αν σχετικά μέτρα δεν περιλαμβάνονται στην αρχική προδιαγραφή της ροής εργασιών, η προτεινόμενη προσέγγιση μπορεί να εξασφαλίσει ότι η οποιαδήποτε αποθήκευση των δεδομένων θα πραγματοποιείται μόνο όταν αυτό επιτρέπεται, και ακόμα και τότε μόνο υπό αποδεκτούς, για τη Νομοθεσία, όρους. Για παράδειγμα, αν κάποια δεδομένα απαγορεύεται να αποθηκευθούν σε ταυτοποιήσιμη μορφή, κατάλληλες εργασίες φιλτραρίσματος, κρυπτογράφησης ή διατήρησης ανωνυμίας, κλπ., μπορούν να παρεμβάλλονται αυτόματα πριν από την εργασία αποθήκευσης (όπου υπάρχει πρόβλεψη για κάτι τέτοιο). Περαιτέρω, και ο χρόνος αποθήκευσης είναι δυνατόν να ελέγχεται, εισάγοντας κατάλληλες εργασίες για την αυτόματη διαγραφή αποθηκευμένων δεδομένων μετά την παρέλευση ορισμένου χρόνου.

10.1.14 Μεταφορά και Διάδοση Δεδομένων

Σε μια ροή εργασιών, κάθε ακμή που συνδέει δυο εργασίες και συνοδεύεται από μία ή περισσότερες οντότητες πληροφορίας εκφράζει ακριβώς τη μεταφορά δεδομένων από την εργασία–αφετηρία στην εργασία–προορισμό, ο έλεγχος της οποίας καταλαμβάνει κεντρική θέση στη μεθοδολογία επαλήθευσης που ακολουθείται. Σημειώνεται ότι στην ει-

δική περίπτωση όπου ως δράστης μιας εργασίας ορίζεται κάποιος οργανισμός εξωτερικός ως προς τον οργανισμό εντός του οποίου εκκινείται η ροή εργασιών, καθιστώντας διαθέσιμες στον τελευταίο τις αντίστοιχες λειτουργικότητες, η ροή πληροφορίας από και προς την εργασία αυτή σηματοδοτεί ουσιαστικά διατομεακή (inter-domain) μεταφορά δεδομένων (διάχυση σε τρίτα μέρη, διασυνοριακή ροή δεδομένων, κλπ.), οπότε και οι αντίστοιχες οδηγίες αποφαίνονται αναφορικά με τους όρους υπό τους οποίους μια τέτοια μεταφορά είναι αποδεκτή.

10.2 Αξιολόγηση σε Σχέση με τις Δυνατότητες Μοντελοποίησης Ροών Εργασιών

Με βάση την κατηγοριοποίηση στο [169], οι γλώσσες μοντελοποίησης επιχειρησιακών ροών εργασιών χαρακτηρίζονται ως "βασισμένες στη ροή ελέγχου, με επίγνωση των εξαρτήσεων δεδομένων"[45]. Οι τεχνολογίες επιστημονικών ροών εργασιών, από την άλλη, είναι "βασισμένες στις εξαρτήσεις δεδομένων"[46], διαθέτοντας εκείνο το βαθμό επίγνωσης ροής ελέγχου που υπαγορεύεται από τα πεδία εφαρμογών στα οποία στοχεύουν. Η προσέγγιση που παρουσιάζεται στο παρόν είναι κατάλληλη για τη σε υψηλό επίπεδο, ωστόσο ενδελεχή, αναπαράσταση ροών εργασιών που βασίζονται τόσο στη ροή ελέγχου όσο και στη ροή δεδομένων. Αυτή όμως είναι μία μόνο πτυχή της εκφραστικής της δύναμης, καθώς όχι μόνο καταφέρνει να καλύψει εκτενώς ευρέως αναγνωρισμένες όψεις των ροών εργασιών, αλλά και αναδεικνύει νέα στοιχεία που υπεισέρχονται στην εκτέλεσή τους.

Κατ' αρχάς η προτεινόμενη μέθοδος μοντελοποίησης υποστηρίζει την πλειονότητα των Μοτίβων Ροών Εργασιών[47] [173][145][144][143], τα οποία συνιστούν ένα ευρέως χρησιμοποιούμενο και αποδεκτό πλαίσιο αναφοράς για την αξιολόγηση συστημάτων ροών εργασιών. Πράγματι, η εκφραστικότητά της έχει ως αποτέλεσμα την εγγενή κάλυψη όλων των βασικών μοτίβων αλληλεπίδρασης αναφορικά με τη ροή ελέγχου και δεδομένων, παρ' όλο που δε χρησιμοποιούνται ειδικές δομές, όπως λόγου χάρη στην BPMN [121] (π.χ., πύλες διάσπασης και συγχώνευσης ροής), κάτι που μειώνει τη συνολική πολυπλοκότητά της. Στον Πίνακα 3 η ακολουθούμενη προσέγγιση συγκρίνεται με τη BPMN, τη YAWL και το Kepler (βλ. Ενότητα 3.3) ως προς κάποια επιλεγμένα μοτίβα που αφορούν τις όψεις ελέγχου, δεδομένων και πόρων. Όπως καταδεικνύεται, η προτεινόμενη μέθοδος παρέχει ευρεία κάλυψη των μοτίβων ελέγχου, ενώ είναι η μοναδική διαθέσιμη λύση που είναι ικανή να μοντελοποιήσει όλα τα Μοτίβα Δημιουργίας (Creation Patterns) (σχετικά με την ανάθεση σε πόρους) και τα Μοτίβα Δρομολόγησης με Βάση τα Δεδομένα (Data-based Routing Patterns). Σε ό,τι αφορά τα τελευταία, ο ορισμός συνθηκών επί εργασιών και ακμών ροής επιτρέπει, σε αντίθεση με άλλες τεχνολογίες, την αποτύπωση οποιασδήποτε σχετικής εξάρτη-

[45] data-aware control-flow driven
[46] data-driven
[47] http://www.workflowpatterns.com/

σης. Παρόμοια, οι συνθήκες και οι περιορισμοί που μπορούν να οριστούν για τις διάφορες οντότητες, καθώς και η χρήση των μεταβλητών ροών εργασιών, μπορούν να υποστηρίξουν όλους τους καταγεγραμμένους τρόπους προσδιορισμού πόρων, συμπεριλαμβανομένης μιας ευρείας γκάμας απαιτήσεων που αφορούν την ανάθεση σε πόρους λαμβάνοντας πιθανώς υπόψη ευρύτερα τμήματα της ροής εργασιών και/ή ο τρόπος επιβολής των οποίων δεν μπορεί να προσδιοριστεί πλήρως παρά μόνο κατά τη φάση της εκτέλεσης. Τέτοιες είναι, για παράδειγμα, οι περιπτώσεις του Χειρισμού Περίπτωσης (Case Handling), του Διαχωρισμού Καθηκόντων (Separation of Duty) και της Σύνδεσης Καθηκόντων (Binding of Duty/Retain Familiar), που κατέχουν κεντρική θέση μεταξύ των απαιτήσεων διαχείρισης εξουσιοδοτήσεων σε ροές εργασιών [417], χωρίς, ωστόσο, να υποστηρίζονται εγγενώς από τις περισσότερες υπάρχουσες λύσεις μοντελοποίησης.

Επιπλέον η προτεινόμενη προσέγγιση διαθέτει διάφορα επιμέρους καινοτόμα χαρακτηριστικά. Ένα από αυτά είναι η εισαγωγή της έννοιας του *αντικειμένου επενέργειας*, η οποία καθιστά δυνατό τον ακόμα αυστηρότερο και λεπτομερή έλεγχο πάνω στην εκτέλεση των εργασιών. Σε συνδυασμό και με τα παραπάνω, αξίζει να σημειωθεί ότι ο ρητός και διακριτός ορισμός των αντικειμένων επενέργειας επιτρέπει, μεταξύ άλλων, την κατά κάποιο τρόπο επέκταση του Διαχωρισμού και της Σύνδεσης Καθηκόντων με σκοπό τον ακριβή και φορμαλιστικό ορισμό σχέσεων μεταξύ τόσο *δρώντων οντοτήτων* όσο και *οντοτήτων–αποδεκτών* της εκάστοτε ενέργειας. Έτσι, για παράδειγμα, μπορεί να εκφραστεί η απαίτηση ότι δυο εργασίες δεν πρέπει να εκτελεστούν επί του ίδιου αντικειμένου επενέργειας, ή ότι ο δράστης μιας εργασίας απαγορεύεται να είναι το αντικείμενο επενέργειας μιας άλλης. Περαιτέρω, καμιά άλλη προσέγγιση δεν ενσωματώνει σε τέτοιο βαθμό τη φορμαλιστική διατύπωση και χρήση εκφράσεων και λογικών σχέσεων, προκειμένου να περιγράψει κάθε είδους οντότητα μιας ροής εργασιών και την κατάσταση στην οποία βρίσκεται, τις εξωγενείς συνθήκες και τις ποικίλες ιδιότητες που μπορούν να χαρακτηρίζουν τη ροή της πληροφορίας. Όλα αυτά, σε συνδυασμό με τη χρήση των *προφίλ εκτέλεσης*, προωθούν τη λεγόμενη *ευελιξία εκ σχεδιασμού (flexibility by design)* [437] σε ό,τι αφορά τόσο την εκτέλεση των ίδιων των εργασιών όσο και τις αλληλεπιδράσεις τους. Εξάλλου, το όλο σύστημα στηρίζεται σε ένα πλούσιο Σημασιολογικό Μοντέλο Πληροφοριών, το οποίο υποστηρίζει τον ορισμό πλήθους σχέσεων μεταξύ αφηρημένων εννοιών, με αποτέλεσμα το λεπτομερή σημασιολογικό χαρακτηρισμό των στοιχείων μιας ροής εργασιών και των αλληλοσυσχετίσεών τους· ιδιαίτερα αξιοσημείωτες μεταξύ αυτών είναι οι σχέσεις *isA*, *isPartOf* και *moreDetailedThan*, η μοντελοποίηση των οποίων υποστηρίζεται για πρώτη φορά στα πλαίσια μιας ροής εργασιών. Έτσι, με τη βοήθεια όλων των παραπάνω μηχανισμών, η προτεινόμενη οντολογική μέθοδος σχεδιασμού θέτει τις βάσεις για την ενσωμάτωση, κατά την προδιαγραφή μιας ροής εργασιών, βασικών έως πιο σύνθετων πολιτικών ιδιωτικότητας προς επιβολή κατά την εκτέλεσή της.

Τέλος, από την άποψη της ποιότητας σχεδιασμού της Οντολογίας Μοντέλων Ροών Εργασιών (OMPE) και της Οντολογίας Σημασιολογικού Μοντέλου Πληροφοριών (ΟΣΜΠ), η συνολική εκφραστική δύναμη της προσέγγισης αντικατοπτρίζεται στις υψηλές τιμές των

Πίνακας 3: Σύγκριση της προτεινόμενης προσέγγισης με εξέχουσες τεχνολογίες ροών εργασιών ως προς Μοτίβα Ροών Εργασιών εφαρμόσιμα κατά τη φάση σχεδιασμού τους. Τα σύμβολα "+", "*", "-" υποδεικνύουν, αντίστοιχα, άμεση, μερική/έμμεση και μη υποστήριξη του σχετικού Μοτίβου.

Μοτίβο	**BPMN**	**YAWL**	**Kepler**	**Προτεινόμενη Λύση**
Μοτίβα ροής ελέγχου				
Sequence	+	+	+	+
Parallel Split	+	+	+	+
Synchronization	+	+	+	+
Exclusive Choice	+	+	+	+
Simple Merge	+	+	+	+
Multi-choice	+	+	-	+
Synchronizing Merge	*	+	-	+
Multi-merge	+	+	+	+
Discriminator	*	+	-	-
Arbitrary Cycles	+	+	+	+
Implicit Termination	+	-	+	*
Multiple Instances Without Synchronization	+	+	+	+
Multiple Instances With a Priori Design Time Knowledge	+	+	-	*
Multiple Instances With a Priori Runtime Knowledge	+	+	-	-
Multiple Instances Without a Priori Runtime Knowledge	-	+	-	-
Deferred Choice	+	+	-	-
Interleaved Parallel Routing	*	+	+	+
Milestone	-	+	-	+
Cancel Activity	+	+	-	-
Cancel Case	+	+	-	*
Μοτίβα δεδομένων: Δρομολόγηση με Βάση τα Δεδομένα				
Task Precondition - Data Existence	+	*	+	+
Task Precondition - Data Value	-	*	-	+
Task Postcondition -Data Existence	+	*	-	+
Task Postcondition - Data Value	-	*	-	+
Event-based Task Trigger	+	-	-	+
Data-based Task Trigger	+	-	-	+
Data-based Routing	+	+	+	+
Μοτίβα πόρων: Μοτίβα δημιουργίας				
Direct Allocation	+	+	-	+
Role-based Allocation	+	+	-	+
Deferred Allocation	-	+	-	+
Authorisation	-	+	-	+
Separation of Duties	-	+	-	+
Case Handling	-	-	-	+
Retain Familiar	-	+	-	+
Capability-based Allocation	-	+	-	+
History-based Allocation	-	+	-	+
Organisational Allocation	-	+	-	+
Automatic Execution	+	+	+	+

δεικτών που δηλώνουν τον πλούτο των οντολογιών αυτών σε σχέσεις μεταξύ κλάσεων (Relationship Richness – RR) και σε ιδιότητες που χαρακτηρίζουν τις τελευταίες (Attribute

Richness – AR) [438][439], οι οποίοι παρουσιάζονται στον Πίνακα 4[48]. Ο δείκτης RR εκφράζει το ποσοστό των σχέσεων που δεν εκφράζουν εξ ορισμού κληρονομικότητα (non-inheritance) επί του συνόλου των σχέσεων που ορίζονται σε μια οντολογία, με βάση τη λογική ότι μια οντολογία που περιλαμβάνει μόνο σχέσεις κληρονομικότητας συνήθως περικλείει λιγότερη πληροφορία από ότι μια οντολογία με ποικίλα είδη σχέσεων. Ο δείκτης AR, από την άλλη, εκφράζει το μέσο αριθμό ιδιοτήτων που ορίζονται ανά κλάση. Από τα στοιχεία του Πίνακα γίνεται επίσης εμφανής η αύξηση στην ποσότητα της πληροφορίας που περικλείεται στην ΟΜΡΕ ως συνέπεια της ενοποίησής της με την ΟΣΜΠ.

Πίνακας 4: Δείκτες ποιότητας σχεδιασμού και πολυπλοκότητας των εμπλεκόμενων οντολογιών.

			CID			COD		
Οντολογικό μοντέλο	**RR**	**AR**	**MIN**	**MAX**	**AVG**	**MIN**	**MAX**	**AVG**
ΟΜΡΕ	1	2.5	1	8	3.75	0	24	3.75
ΟΣΜΠ	0.79	1.39	0	12	2.26	0	8	2.26
ΟΜΡΕ + ΟΣΜΠ	0.92	1.85	0	12	3.49	0	24	3.49

10.3 Απαιτούμενοι Πόροι

Για τη διερεύνηση της επίδοσης ως προς την κατανάλωση πόρων της προτεινόμενης προσέγγισης προδιαγραφής ροών εργασιών, επαλήθευσής τους ως προς απαιτήσεις ιδιωτικότητας και συνεπούς εκτέλεσής τους χρησιμοποιήθηκαν 30 ΜΡΕ του πραγματικού κόσμου. Όλα τα στάδια από το σχεδιασμό μέχρι την εξαγωγή των οδηγιών εκτέλεσης που αφορούν κάθε Πράκτορα εκτελέστηκαν σε έναν προσωπικό υπολογιστή με τα ακόλουθα χαρακτηριστικά: επεξεργαστής Intel(R) Core(TM) i5-M430 2.27 GHz, RAM 4.00 GB, λειτουργικό σύστημα Windows 7 Professional, Service Pack 1, έκδοση Java 1.7.0_03. Κάθε ΜΡΕ αποτέλεσε μια αυτόνομη ΟΜΡΕ και περιελάμβανε από 3 έως 25 εργασίες και από 2 έως 32 ακμές, με διαβαθμισμένο βαθμό πολυπλοκότητας σε ό,τι αφορά τη συσχέτιση κάθε εργασίας/ακμής με οντότητες ροής εργασιών (ΟντΡΕ), προφίλ εκτέλεσης, εκφράσεις, λογικές σχέσεις, κ.ά..

Ο συνολικός χρόνος επαλήθευσης κάθε ροής εργασιών κυμάνθηκε από ∼0.3 έως ∼9 δευτερόλεπτα, χωρίς να συμπεριληφθεί ο χρόνος που απαιτήθηκε για την εξαγωγή των οδηγιών συμβατότητας. Για το τελευταίο, η Μηχανή Συμπερασμού που χρησιμοποιήθηκε παρουσίασε αρκετά μεγάλες αποκλίσεις, αφού χρειάστηκε κατά μέσο όρο ∼5.6 δευτερόλεπτα, φτάνοντας ωστόσο μέχρι και τα ∼25· σε κάθε περίπτωση πάντως η διαδικασία επαλήθευσης δεν ξεπέρασε τα ∼40 δευτερόλεπτα. Ως προς τα επιμέρους βήματα της ακολουθούμενης μεθοδολογίας, στη δημιουργία των υπογράφων–στιγμιοτύπων αφιερώθηκε

[48]Στους υπολογισμούς που αφορούν την ΟΜΡΕ δεν ελήφθησαν υπόψη οι κλάσεις που σχετίζονται με τις οδηγίες συμβατότητας, παρά μόνο οι οντολογικές οντότητες που χρησιμεύουν στο σχεδιασμό μιας ροής εργασιών.

κατά μέσο όρο το ∼8.17% του συνολικού χρόνου, στην εξαγωγή των διμερών συσχετισμών (ΔιΣ) και των ζευγών σκοπού–εκκινητή το ∼1.76% και ∼0.45%, αντίστοιχα, στην εφαρμογή των οδηγιών συμβατότητας (δημιουργία περιπτώσεων εκτέλεσης, περαιτέρω έλεγχο και συγχώνευσή τους) το ∼74.07% και στη συγχώνευση των υπογράφων–στιγμιοτύπων το ∼15.55%. Ως προς το τελευταίο, παρατηρήθηκε επιπλέον ότι ενώ ο χρόνος της επαλήθευσης καθεαυτής (εφαρμογής των οδηγιών συμβατότητας) γενικά υπερτερεί σημαντικά όλων των υπόλοιπων σταδίων, υπήρξαν περιπτώσεις στις οποίες η συγχώνευση των υπογράφων–στιγμιοτύπων λόγω αυξημένης πολυπλοκότητας ανήλθε χρονικά μέχρι και στο ∼76.98% της διαδικασίας. Τέλος, ο χρόνος εξαγωγής των οδηγιών εκτέλεσης ανά Πράκτορα κυμάνθηκε μεταξύ ∼0.1 και ∼0.2 δευτερολέπτων.

Αξίζει να σημειωθεί ότι οι σχετικά χαμηλοί χρόνοι που παρατηρήθηκαν οφείλονται και στον έλεγχο και την εξισορρόπηση που επιτυγχάνεται αναφορικά με την πολυπλοκότητα σχεδιασμού των ΟΜΡΕ και ΟΣΜΠ. Πιο συγκεκριμένα, ο Πίνακας 4 δείχνει τις τιμές των δεικτών που μετρούν το πλήθος των ακμών που καταλήγουν σε (Class In-Degree – CID) και ξεκινούν από (Class Out-Degree – COD) κάθε κόμβο κλάσης, αντίστοιχα [440], και οι οποίοι υπολογίστηκαν για τα αντίστοιχα οντολογικά σχήματα. Παρόμοια πληροφορία εκφράζει και ο λόγος του πλήθους ιδιοτήτων προς το πλήθος μελών (Property-Individual Ratio – PIR), ο οποίος μετρά την πυκνότητα διασύνδεσης μεταξύ μελών μιας οντολογίας (όχι πια, δηλαδή, σε επίπεδο σχήματος), η οποία στην εν λόγω περίπτωση αφορά την προδιαγραφή μιας συγκεκριμένης ροής εργασιών. Οι τιμές του PIR για τα χρησιμοποιούμενα ΜΡΕ κυμάνθηκαν από ∼3.38, για σχετικά απλές ροές εργασιών, μέχρι ∼4.96, για τις πιο σύνθετες μεταξύ αυτών, με μέση τιμή ∼4.09. Τέλος, υπολογίστηκε και η εντροπία γράφου (Entropy of Graph – EOG), η οποία ορίζεται, παρόμοια με το [440], ως:

$$EOG = -\sum_{i} p(i) log_2 p(i)$$

όπου *p(i)* είναι η πιθανότητα ενός μέλους να σχετίζεται με *i* το πλήθος ιδιότητες (αποτελώντας μέρος είτε του πεδίου ορισμού είτε του πεδίου τιμών τους). Οι τιμές της εντροπίας καταδεικνύουν ότι η "κανονικότητα" ενός οντολογικού ΜΡΕ δεν επηρεάζεται στην πράξη από το μέγεθος ή το βαθμό λεπτομέρειας της περιγραφής. Πράγματι, για τα ΜΡΕ αναφοράς, η τιμή της EOG περιορίστηκε στο διάστημα μεταξύ ∼2.07 και ∼2.58, με μέση τιμή ∼2.32.

Κεφάλαιο 11

Συμπεράσματα – Μελλοντική Εργασία

Βάση και κίνητρο για την πραγματοποίηση της παρούσας διατριβής αποτέλεσε η αναδυόμενη τάση, τόσο νομική όσο και τεχνολογική, στον τομέα της ιδιωτικότητας που είθισται να αναφέρεται ως *"ιδιωτικότητα εκ σχεδιασμού" (Privacy by Design)* [25], με στόχο την εφαρμογή της συγκεκριμένα στα συστήματα ροών εργασιών. Στη συνέχεια παρουσιάζονται οι βασικές συνεισφορές της προτεινόμενης λύσης προς αυτή την κατεύθυνση.

Σε πρώτη φάση καταγράφηκαν για πρώτη φορά συστηματικά οι τεχνικές απαιτήσεις που εισάγει η ανάγκη για προστασία της ιδιωτικότητας σε περιβάλλοντα ροών εργασιών. Οι απαιτήσεις αυτές, οι οποίες απορρέουν από την ανάλυση του νομικού και κανονιστικού πλαισίου που έχει θεσπιστεί για την προστασία της ιδιωτικότητας, διερευνήθηκαν ως προς δύο βασικούς άξονες, οι οποίοι και καθόρισαν τη μετέπειτα προσέγγιση στο πρόβλημα: α) την ανάγκη να συμπεριληφθούν στο επίπεδο της μοντελοποίησης των ροών εργασιών δομές ικανές να υποστηρίξουν τον ορισμό πολιτικών ιδιωτικότητας ως μέρος του σχεδιασμού τους, οδηγώντας σε στοχευμένες προδιαγραφές ιδιωτικότητας προς επιβολή κατά τη φάση της εκτέλεσης· β) τα βασικά μοτίβα συμμόρφωσης που είναι πιθανό να ανακύψουν και, ως εκ τούτου, πρέπει να υποστηρίζονται, προκειμένου να καταστεί δυνατή η αυτόματη επαλήθευση μοντέλων ροών εργασιών ως προς όρους προστασίας της ιδιωτικότητας, αλλά και η αυτόματη τροποποίησή τους στην περίπτωση της ανίχνευσης παραβιάσεων αυτών.

Στη βάση των παραπάνω, προδιαγράφηκε ένας νέος τρόπος ορισμού ροών εργασιών, μέσω οντολογιών, που επιτυγχάνει τη φορμαλιστική απεικόνιση με έναν ενοποιημένο τρόπο όλων εκείνων των πληροφοριών που απαιτούνται για τον ενδελεχή έλεγχό τους ως προς τις αρχές ιδιωτικότητας και για τη συνεπή, λειτουργικά αλλά και από πλευράς προστασίας προσωπικών δεδομένων, εκτέλεσή τους. Η συγκεκριμένη προσέγγιση είναι κατάλληλη για την ενδελεχή, αν και αφαιρετική, αναπαράσταση ροών εργασιών που βασίζονται τόσο στη ροή ελέγχου όσο και στη ροή δεδομένων, κάτι που αυτή τη στιγμή

απουσιάζει από τις διαθέσιμες λύσεις, παρ' όλο που αποτελεί ζητούμενο για διάφορα πεδία εφαρμογών. Περαιτέρω, τα δυο βασικά στοιχεία κάθε ροής εργασιών, οι εργασίες και οι ακμές ροής, περιγράφονται σε υψηλό βαθμό λεπτομέρειας ως προς όλες τις συνιστώσες τους, με αποτέλεσμα την εγγενή κάλυψη όλων των βασικών μοτίβων αλληλεπίδρασης αναφορικά με τις κύριες όψεις των ροών εργασιών (ελέγχου, δεδομένων και πόρων) (βλ. Ενότητα 10.2). Επιπλέον κάποιες επιμέρους έννοιες εμφανίζονται για πρώτη φορά, όπως, για παράδειγμα, το αντικείμενο επενέργειας, που μοντελοποιεί με διακριτό τρόπο την οντότητα–αποδέκτη κάθε λειτουργίας, και το προφίλ συμβατότητας, που προσφέρει έναν αποτελεσματικό μηχανισμό για την ενσωμάτωση πολιτικών ασφάλειας στα μοντέλα ροής εργασιών (MPE), προσφέροντας ταυτόχρονα τη δυνατότητα για την περιγραφή υπό συνθήκη παραλλαγών στην εκτέλεση των εργασιών. Τέλος, αξίζει να αναφερθεί η ρητή θεώρηση του σκοπού, καθώς και η έννοια της κατάστασης των δεδομένων, που επιτρέπει την παρακολούθηση και τον αποτελεσματικό έλεγχο της επεξεργασίας στην οποία αυτά υποβάλλονται.

Σημειώνεται ότι αρχικά διερευνήθηκε η δυνατότητα αξιοποίησης αξιόλογων υφιστάμενων τεχνολογιών περιγραφής ροών εργασιών, καθώς κατά κοινή ομολογία της επιστημονικής κοινότητας στη συγκεκριμένη περιοχή και όχι μόνο, η αναχρησιμοποίηση και επέκταση υπαρχόντων και ευρέως υιοθετημένων προτύπων κρίνεται πολυτιμότερη συγκριτικά με την προδιαγραφή ενός ακόμα νέου συστήματος. Ωστόσο, διαπιστώθηκε ότι καμιά τεχνολογία μοντελοποίησης από μόνη της δεν καλύπτει επαρκώς και/ή με τον τρόπο που απαιτείται (για τους σκοπούς της διατριβής) όλες τις όψεις και μοτίβα που υπεισέρχονται στις ροές εργασιών. Εξάλλου, η ανάγκη ενοποίησης, για παράδειγμα, των όψεων ροής ελέγχου και δεδομένων επισημαίνεται και στη βιβλιογραφία [144]. Από την άλλη, η εισαγωγή των κατάλληλων επεκτάσεων σε ήδη υπάρχοντα πρότυπα, όπως π.χ. αυτό της BPMN, θεωρήθηκε ότι θα εισήγαγε σημαντική πολυπλοκότητα στη λύση χωρίς κάποιο όφελος για τους στόχους της συγκεκριμένης ερευνητικής εργασίας, καθώς τέτοιες ώριμες προσεγγίσεις διαθέτουν ήδη σύνθετες δομές που θα έπρεπε να ληφθούν υπόψη, παρ' όλο που δε σχετίζονται με την ιδιωτικότητα.

Επιπρόσθετα, οι απαιτήσεις ως προς τις οποίες θα χρειαστεί να ελεγχθεί μια ροή εργασιών κωδικοποιήθηκαν σε κατάλληλες οδηγίες συμβατότητας και αναπτύχθηκε μεθοδολογία για την εφαρμογή τους σε MPE προδιαγεγραμμένα με τον προαναφερθέντα τρόπο. Οι οδηγίες συμβατότητας υλοποιούνται ως μέρος της οντολογίας μοντέλων ροών εργασιών (OMPE) και χρησιμοποιούνται για την εξαγωγή συμπεριφορικών νορμών, οι οποίες κατευθύνουν τον έλεγχο των αντίστοιχων MPE. Έτσι, στη βάση των παραπάνω, προτάθηκε ο μηχανισμός που καθιστά δυνατή την αυτόματη επαλήθευση ροών εργασιών και τη συνακόλουθη τροποποίησή τους, όπου αυτό χρειάζεται, προκειμένου να καθίστανται εγγενώς σύμμορφες με τις αρχές της ιδιωτικότητες ήδη πριν την εκτέλεσή τους.

Τέλος, προδιαγράφηκε μια νέα γλώσσα για την περιγραφή της συμπεριφοράς κάθε οντότητας που πρόκειται να εμπλακεί στην εκτέλεση μιας ροής εργασιών. Η γλώσσα αυτή

είναι σε θέση να αποτυπώσει τόσο τις λειτουργίες που θα πρέπει να λάβουν χώρα, την ανταλλαγή πληροφορίας που αυτό συνεπάγεται και την απαραίτητη επικοινωνία μεταξύ των υποκείμενων οντοτήτων, όσο και άλλα χαρακτηριστικά που περιλαμβάνονται στον οντολογικό ορισμό ενός MPE και αφορούν λιγότερο το λειτουργικό κομμάτι και περισσότερο το ζήτημα της τήρησης όρων ιδιωτικότητας. Το τελευταίο δεν είναι εφικτό μέσω υφιστάμενων γλωσσών εκτέλεσης ροών εργασιών (π.χ., BPEL), οι οποίες δε διαθέτουν τις απαραίτητες δομές για τη "μεταφορά" στο στρώμα εκτέλεσης του συνόλου της πληροφορίας που μπορεί να περικλείει μια OMPE.

Με τα παραπάνω εργαλεία, η προτεινόμενη λύση κατορθώνει να αντιμετωπίσει όλες τις επιμέρους προκλήσεις που ανακύπτουν σε περιβάλλοντα ροών εργασιών ως αποτέλεσμα της απαίτησης για τήρηση των βασικών αρχών ιδιωτικότητας (βλ. Ενότητα 4.2). Κατ' αρχάς, εφαρμόζεται επιβολή δικαιωμάτων πρόσβασης σε υψηλό επίπεδο λεπτομέρειας και σε κάθε βήμα της επεξεργασίας. Πράγματι, κάθε εργασία, με τον τρόπο που ορίζεται, συνιστά στην ουσία μια πολιτική πρόσβασης, καθώς τα προφίλ συμβατότητας που συνδέονται με αυτήν εκφράζουν το *ποιός* καλείται να πραγματοποιήσει *ποιά λειτουργία πάνω σε ποιό αντικείμενο επενέργειας*, προσδιορίζοντας πιθανώς και τις συνθήκες κάτω από τις οποίες αυτό επιτρέπεται να συμβεί. Η πληροφορία αυτή μεταφέρεται μετέπειτα στους Πράκτορες μέσω της Γλώσσας Περιγραφής Οδηγιών Εκτέλεσης (ΓΠΟΕ), ενώ δηλώνεται επιπρόσθετα η πληροφορία την οποία θα πρέπει να λάβει ή/και αποστείλει κάθε οντότητα, και πιθανώς οι αντίστοιχες συνθήκες. Επιπλέον, οι οδηγίες συμβατότητας που κατευθύνουν τον έλεγχο και την τροποποίηση των ροών εργασιών προκύπτουν από ένα μοντέλο ελέγχου πρόσβασης και χρήσης, το οποίο περιλαμβάνει ένα σύνολο κανόνων που μπορούν να καλύπτουν όλους τους τύπους προσωπικών δεδομένων, λειτουργιών, ρόλων, κλπ. των εμπλεκομένων οντοτήτων. Στο πλαίσιο αυτό λαμβάνεται σημαντικά υπόψη και η έννοια του σκοπού, ο οποίος αφενός δηλώνεται υποχρεωτικά ως μέρος της προδιαγραφής μιας ροής εργασιών συνολικά και αφετέρου κατέχει κεντρική θέση στο προαναφερθέν μοντέλο ελέγχου πρόσβασης, επηρεάζοντας κάθε σχετική απόφαση.

Επιπρόσθετα, ο τρόπος μοντελοποίησης και ελέγχου της ροής πληροφορίας μεταξύ εργασιών και μετεχόντων μερών, εν γένει, εξασφαλίζει τη συμμόρφωσή της με ποικίλες απαιτήσεις ιδιωτικότητας. Κάθε μονάδα πληροφορίας χαρακτηρίζεται λεπτομερώς σημασιολογικά μέσω του αντίστοιχου τύπου δεδομένου και, πιθανώς, άλλων ιδιοτήτων που συμπληρώνουν την περιγραφή της, ενώ η κατάσταση στην οποία βρίσκεται είναι δηλωτική της επεξεργασίας την οποία θα έχει ή δε θα έχει υποστεί (π.χ., κρυπτογράφηση) σε κάθε φάση του κύκλου ζωής της κατά την εκτέλεση της ροής εργασιών. Παράλληλα το τμήμα αυτής που υφίσταται την οποιαδήποτε επεξεργασία αναπαρίσταται ρητά ως αντικείμενο επενέργειας της εκάστοτε εργασίας, οδηγώντας στη σαφή διάκριση μεταξύ πρόσβασης "μόνο για ανάγνωση" (read access) και "επεμβατικής" πρόσβασης (write access). Επιπλέον, ο προσδιορισμός της συμπεριφοράς συγχρονισμού κάθε εργασίας υποδηλώνει το κατά πόσο αυτή επεξεργάζεται συνδυαστικά τα εισερχόμενα δεδομένα. Με τη βοήθεια των μηχανισμών αυτών, η μεθοδολογία ελέγχου είναι κατόπιν σε θέση να παρακολουθεί

στενά και να ρυθμίζει κάθε πρόσβαση και επεξεργασία δεδομένων που προδιαγράφεται σε μια ροή εργασιών, αλλά και, πιο συγκεκριμένα, να εντοπίζει και αποτρέπει τη διασύνδεση δεδομένων. Τέλος, η δυνατότητα μοντελοποίησης ενός ευρέως φάσματος περιορισμών που εκφράζουν Διαχωρισμό και Σύνδεση Καθηκόντων προωθεί περαιτέρω τον έλεγχο της συνδυαστικής πρόσβασης σε δεδομένα, και γενικότερα την αποφυγή ποικίλων συγκρούσεων και διαρροών.

Επιπλέον, μέσω της δυνατότητας αυτόματης εισαγωγής εργασιών κατά τη διαδικασία επαλήθευσης, εξασφαλίζεται η εκτέλεση ενεργειών που σε κάποιες περιπτώσεις θεωρούνται απαραίτητες από τη Νομοθεσία για την προστασία της ιδιωτικότητας. Έτσι, μπορούν να προστίθενται εργασίες που πραγματοποιούν την ενημέρωση του υποκειμένου των δεδομένων ή την παροχή της ρητής συγκατάθεσής του αναφορικά με τις πράξεις παραχώρησης και επεξεργασίας των προσωπικών του δεδομένων, πιθανώς και αναστέλλοντας, ανάλογα με την περίπτωση, τη συνέχιση της ροής εργασιών μέχρι την ολοκλήρωση των αντίστοιχων εργασιών. Το ίδιο ισχύει και για τις απαραίτητες ενημερώσεις προς τις αρμόδιες αρχές, καθώς και για λειτουργίες καταγραφής της όποιας δραστηριότητας (logging), οι οποίες εξυπηρετούν την απόδοση ευθυνών και, σε γενικότερο πλαίσιο, την παρακολούθηση κάθε επεξεργασίας που λαμβάνει χώρα σε πραγματικό χρόνο.

Από την άλλη, η επίγνωση πλαισίου (context) χαρακτηρίζει συνολικά τη λύση σε όλα τα επίπεδα. Η οντολογική μέθοδος μοντελοποίησης ροών εργασιών προβλέπει την ενσωμάτωση εξαρτήσεων από πληροφορίες πλαισίου μέσω του ορισμού συνθηκών σε εργασίες και ακμές και λοιπών περιορισμών. Οι συνθήκες αυτές και οι περιορισμοί λαμβάνονται υπόψη κατά των έλεγχο ροών εργασιών, αφενός στη φάση της δημιουργίας των υπογράφων–στιγμιοτύπων, η οποία προσδιορίζει με σαφήνεια τις πιθανές τροπές που μπορεί να πάρει η εκτέλεση, και αφετέρου στην εφαρμογή των οδηγιών συμβατότητας, στις οποίες προβλέπεται η δυνατότητα διαφοροποίησης ανάλογα με το υφιστάμενο πλαίσιο. Εξάλλου το τελευταίο κατέχει κεντρική θέση στο Σημασιολογικό Μοντέλο Πολιτικών που κατευθύνει την όλη διαδικασία. Τέλος, οι οδηγίες εκτέλεσης προς τους Πράκτορες διαθέτουν επίσης δομές για την αποτύπωση των σχετικών εξαρτήσεων, ενώ κρίσιμο στοιχείο της αρχιτεκτονικής του συστήματος συνιστά ο Δίαυλος Πληροφοριών Πλαισίου, επιτρέποντας τη διακίνηση σε πραγματικό χρόνο των πληροφοριών πλαισίου, όπως αυτές διαμορφώνονται κατά την εκτέλεση μιας ροής εργασιών.

Ο ακριβής σημασιολογικός ορισμός των εμπλεκόμενων εννοιών είναι άλλο ένα στοιχείο το οποίο χαρακτηρίζει οριζόντια την προτεινόμενη λύση. Το χρησιμοποιούμενο Σημασιολογικο Μοντέλο Πληροφοριών αποτελεί τη βάση για την περιγραφή κάθε οντότητας που συμμετέχει σε μια ροή εργασιών, σε ό,τι αφορά τόσο το σχεδιασμό όσο και την εκτέλεση. Επιπρόσθετα, στο ίδιο μοντέλο αναφέρεται και το Σημασιολογικό Μοντέλο Πολιτικών και οι εξ αυτού συναγόμενες οδηγίες συμβατότητας, με αποτέλεσμα την ολοκλήρωση της λύσης συνολικά σε σημασιολογικό επίπεδο. Περαιτέρω, η επιλογή της οντολογικής υλοποίησης ως κοινού μέσου φορμαλιστικής αναπαράστασης του Σημασιολογικού Μο-

ντέλου Πληροφοριών και των ΜΡΕ παρουσιάζει διάφορα επιπλέον πλεονεκτήματα, όπως είναι η απευθείας σύνδεσή τους, η δυνατότητα ακριβούς επεξεργασίας της τυπικά οριζόμενης πληροφορίας, συμπεριλαμβανομένης γνώσης που δεν περιέχεται ρητά στην ΟΜΡΕ, ενώ επιτρέπει σε κάθε ΜΡΕ να ακολουθεί αυτόματα και με διαφανή τρόπο την οποιαδήποτε εξέλιξη της γνωσιακής βάσης.

Η λύση που προτείνει η διατριβή επιδέχεται βελτιώσεις και στο πλαίσιο αυτό υπάρχουν διάφορες κατευθύνσεις στις οποίες μπορεί να κινηθεί η έρευνα με σκοπό την επέκταση των μηχανισμών που παρουσιάστηκαν. Δεδομένου ότι η εφαρμογή της παρούσας προσέγγισης εστιάζει σε ΜΡΕ που αναπαριστώνται ως κατευθυνόμενοι ακυκλικοί γράφοι, ένα πρώτο σημείο αφορά την κατάλληλη προσαρμογή της μεθοδολογίας ελέγχου ώστε αυτή να υποστηρίζει την επαλήθευση ροών εργασιών που περιέχουν βρόχους (loops). Επίσης, η διατριβή υιοθετεί για τους σκοπούς της μια σχετικά απλή άλγεβρα περιορισμών, ως εκ τούτου πιθανή μελλοντική εργασία αποτελεί η ανάπτυξη μιας πολύπλοκης και πολύ εκφραστικής άλγεβρας, ικανής να καλύπτει περισσότερο σύνθετες περιπτώσεις, ιδίως κατά τη διαδικασία δημιουργίας των υπογράφων–στιγμιοτύπων μιας ροής εργασιών. Επιπρόσθετα, ενδιαφέρον παρουσιάζει και η επέκταση της οντολογικής μεθόδου προδιαγραφής ροών εργασιών και οδηγιών συμβατότητας με σκοπό την υποστήριξη ακόμα περισσότερων Μοτίβων Ροών Εργασιών και την αναπαράσταση πιο εξειδικευμένων σχέσεων χρονισμού μεταξύ των προς εκτέλεση εργασιών. Ενδεικτικά παραδείγματα για το τελευταίο αποτελούν η εκκίνηση μιας εργασίας μετά την παρέλευση συγκεκριμένου χρονικού διαστήματος από την ολοκλήρωση μιας προηγούμενής της, η εκτέλεση μιας εργασίας ακριβώς για όσο χρόνο βρίσκεται σε εξέλιξη μια άλλη, κλπ..

Επιπλέον, βασικό ζητούμενο από τα συστήματα ροών εργασιών της επόμενης γενιάς είναι η ικανότητά τους να υποστηρίζουν τη δυναμική αναπροσαρμογή της ροής σε πραγματικό χρόνο, δηλαδή κατά τη διάρκεια της εκτέλεσης. Η παρούσα προσέγγιση, όπως και η πλειονότητα των σχετικών υφιστάμενων τεχνολογιών, βασίζεται στη λογική της ακριβούς προδιαγραφής κάθε δυνατού σεναρίου εκτέλεσης ήδη από το σχεδιασμό της ροής εργασιών, κάτι που όμως περιορίζει την ευελιξία του συστήματος, δεδομένου ότι η "αναγνωσιμότητα" (readability) και η "διατηρησιμότητα" (maintainability) ενός ΜΡΕ οφείλουν να παραμένουν σε αποδεκτά επίπεδα. Σε αυτό το πλαίσιο, πολλά στοιχεία της προτεινόμενης λύσης θα μπορούσαν να αξιοποιηθούν για τη σε πραγματικό χρόνο επαλήθευση και τροποποίηση των ροών εργασιών σύμφωνα με τις αρχές ιδιωτικότητας, με βάση τη λογική του σχετικά "ασαφούς" ορισμού μιας ροής εργασιών και της μετέπειτα συγκεκριμενοποίησής της στη φάση της εκτέλεσης, μεταξύ πληθώρας εναλλακτικών, ανάλογα με ανακύπτοντα συμβάντα, εξωγενείς συνθήκες, κλπ..

Αξίζει επίσης να σημειωθεί ότι το προτεινόμενο τεχνικό πλαίσιο εξυπηρετεί στην παρούσα διατριβή την προστασία της ιδιωτικότητας, ωστόσο οι βασικές αρχές σχεδιασμού του το καθιστούν κατάλληλο, πιθανώς με κάποιες προσαρμογές, για την εξασφάλιση της τήρησης κάθε είδους κανονιστικών απαιτήσεων συμβατότητας σε περιβάλλοντα ροών ερ-

γασιών. Έτσι, μπορεί να αξιοποιηθεί, για παράδειγμα, στην περιοχή της ασφάλειας συστημάτων ή για την επιβολή σύμμορφης συμπεριφοράς σύμφωνα με επιταγές που αφορούν συγκεκριμένα πεδία εφαρμογών (π.χ., στον οικονομικό/τραπεζικό τομέα απαιτήσεις που απορρέουν από τα [441][442]). Τέλος, ακόμα περισσότερο ενδιαφέρον παρουσιάζει η προοπτική της επέκτασης της προτεινόμενης λύσης σε τεχνολογικά πεδία που όχι μόνο υπόκεινται σε κανονιστικές ρυθμίσεις αλλά και απαιτούν ένα διευρυμένο βαθμό ενοποίησης, πέρα από τις παραδοσιακές όψεις της ροής ελέγχου, των δεδομένων και των πόρων. Παράδειγμα τέτοιου πεδίου αποτελούν οι τεχνολογίες ευφυούς ενεργειακού πλέγματος (smart grid) [443][444], στις οποίες τα αποτελέσματα της διατριβής μπορούν να αξιοποιηθούν με σκοπό την ενιαία αναπαράσταση και αντιμετώπιση μιας επιπλέον μορφής ροής, αυτής του ενεργειακού φορτίου, από κοινού με τις ροές ελέγχου και δεδομένων. Στο πλαίσιο αυτό ενδιαφέρον παρουσιάζει η μοντελοποίηση και διαχείριση των αλληλεπιδράσεων μεταξύ όλων των εμπλεκόμενων όψεων, όπως, λόγου χάρη, του πώς η ροή ελέγχου ή/και δεδομένων επηρεάζει τη ροή ενέργειας και αντίστροφα, προς επίτευξη πλήρως αυτοματοποιημένης διαχείρισης του πλέγματος.

Βιβλιογραφία

[1] M. P. Papazoglou and W.-J. Heuvel, "Service oriented architectures: approaches, technologies and research issues," *The VLDB Journal*, vol. 16, pp. 389–415, July 2007.

[2] M. Endrei, J. Ang, A. Arsanjani, S. Chua, P. Comte, P. Krogdahl, M. Luo, and T. Newling, *Patterns: Service-oriented Architecture and Web Services*. IBM, 2004.

[3] W. M. van der Aalst and K. van Hee, *Workflow Management: Models, Methods, and Systems*. Cambridge, Massachusetts London, England: The MIT Press, 1st ed., 2002.

[4] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Workflow Modeling Technologies," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

[5] Ηνωμένα Έθνη, "Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα." `http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=grk`, Δεκέμβριος 1948.

[6] A. F. Westin, *Privacy and Freedom*. Atheneum, 1967.

[7] G. V. Lioudakis, F. Gaudino, E. Boschi, G. Bianchi, D. I. Kaklamani, and I. S. Venieris, "Legislation-aware privacy protection in passive network monitoring," in *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues* (I. M. Portela and M. M. Cruz-Cunha, eds.), ch. 22, pp. 363–383, IGI Global, 2010.

[8] The Information and Privacy Commissioner - Ontario, Deloitte & Touche, "The Security-Privacy Paradox: Issues, Misconceptions, and Strategies," joint report, August 2003.

[9] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, and Σ. Κάτσικας, *Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα*. Αθήνα: Παπασωτηρίου, 2010.

[10] S. Gutwirth, R. Leenes, P. de Hert, and Y. Poullet, *European Data Protection: Coming of Age*. Springer, 2013.

[11] S. Gutwirth, R. Leenes, P. De Hert, and Y. Poullet, *European Data Protection: In Good Health?* Springer, 2012.

[12] S. Gutwirth, Y. Poullet, P. D. Hert, and R. Leenes, eds., *Computers, Privacy and Data Protection - an Element of Choice*. Springer, 2011.

[13] S. Gutwirth, Y. Poullet, and P. De Hert, *Data Protection in a Profiled World*. Springer, 2010.

[14] S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, and S. Nouwt, *Reinventing Data Protection?* Springer, 2009.

[15] I. M. Portela and M. M. Cruz-Cunha, *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*. IGI Global, 2010.

[16] D. J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven & London: Yale University Press, 2011.

[17] European Parliament and Council, "Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," *Official Journal of the European Communities*, vol. L 201, pp. 37–47, July 2002.

[18] European Parliament and Council, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," *Official Journal of the European Communities*, vol. L 105, pp. 54–63, April 2006.

[19] U.S. Congress, "Health Insurance Portability and Accountability Act," 1996. Public Law 104–191.

[20] Article 29 Data Protection Working Party, "Working Document on the processing of personal data relating to health in electronic health records (EHR)," April 2007. 00323/07/EN, WP 131.

[21] F. R. Gaudino, "Healthcare ICT and Personal Data Protection: The Applicable Legal Framework," in *of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, IEEE Press, 2010.

[22] Article 29 Data Protection Working Party, "Working Document on E-Government ," May 2003. 10593/02/EN, WP 73.

[23] R. Palanisamy and B. Mukerji, "Security and Privacy Issues in E-Government," in *E-Government Service Maturity and Development: Cultural, Organizational and Technological Perspectives* (M. Akhter Shareef and S. Dutta, eds.), pp. 236–248, IGI Global, 2012.

[24] Ευρωπαϊκή Επιτροπή, "Πρόταση: Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)," Βρυξέλλες, Ιανουάριος 2012.

[25] A. Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (G. Yee, ed.), IGI Global, 2012.

[26] S. D. Warren and L. D. Brandeis, "Ethical issues in the use of computers," ch. The Right to Privacy, pp. 172–183, Belmont, CA, USA: Wadsworth Publ. Co., 1985.

[27] "Gesetz- und Verordnungsblatt für das Land Hessen - Teil I - Nr. 4," 12 Oktober 1970. Wiesbaden. 625ff.

[28] "Public Law No. 93-579, 88 Stat. 1897 ," 31 December 1974. 5 U.S.C. 552a.

[29] "Public Law No. 100-503," 18 October 1988. 5 U.S.C. 552a.

[30] "Public Law No. 107-56, H. R. 3162, ," 21 October 2001.

[31] Organisation for Economic Co-operation and Development, "OECD guidelines on the protection of privacy and transborder flows of personal data." `http://dx.doi.org/10.1787/9789264196391-en`, 1980.

[32] European Parliament and Council, "Directive 95/46/EC of the European Parliament and of the Council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Communities*, vol. L 281, pp. 31–50, November 1995.

[33] European Parliament and Council, "Directive 97/66/ec of the European Parliament and of the Council of 15 december 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector," *Official Journal of the European Communities*, vol. L 24, pp. 1–8, December 1997.

[34] European Parliament and Council, "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," *Official Journal of the European Communities*, vol. L 337, pp. 11–36, December 2009.

[35] Η' Αναθεωρητική Βουλή των Ελλήνων, "Σύνταγμα της Ελλάδας." `http://www.hellenicparliament.gr/UserFiles/8c3e9046-78fb-48f4-bd82-bbba28ca1ef5/SYNTAGMA.pdf`, Μάιος 2008.

[36] Βουλή των Ελλήνων, "Νόμος 2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα," Απρίλιος 1997. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 50, Τεύχος Πρώτο.

[37] Βουλή των Ελλήνων, "Νόμος 3115/2003: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών," Φεβρουάριος 2003. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 47, Τεύχος Πρώτο.

[38] Βουλή των Ελλήνων, "Νόμος 2474/1999: Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα," 22 Δεκεμβρίου 1999. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 287, Τεύχος Πρώτο.

[39] 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," Ιούνιος 2006. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 133, Τεύχος Πρώτο.

[40] Βουλή των Ελλήνων, "Νόμος 3917/2011: Διατήρηση των δεδομένων που παράγονται ή υπόκεινται σε επεξεργασία στα πλαίσια της παροχής δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικής επικοινωνίας ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επικοινωνιών με λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και σχετικές διατάξεις.," Φεβρουάριος 2011. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 22.

[41] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 87, Τεύχος Δεύτερο.

[42] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 87, Τεύχος Δεύτερο.

[43] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 87, Τεύχος Δεύτερο.

[44] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 88, Τεύχος Δεύτερο.

[45] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 88, Τεύχος Δεύτερο.

[46] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου," Ιανουάριος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 88, Τεύχος Δεύτερο.

[47] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών," Νοέμβριος 2011. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 2715, Τεύχος Δεύτερο.

[48] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών," Ιούλιος 2013. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 1742, Τεύχος Δεύτερο.

[49] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Code of practice for information security management," December 2000. International Standard ISO/IEC 17799.

[50] Πρόεδρος της Ελληνικής Δημοκρατίας, "Προεδρικό Διάταγμα Υπ. Αριθ. 47: Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του," Μάρτιος 2005. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 64, Τεύχος Πρώτο.

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

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

[53] The World Wide Web Consortium (W3C), "SOAP Version 1.2 Part 0: Primer (Second Edition)." `http://www.w3.org/TR/soap12-part0/`, April 2007. W3C Recommendation.

[54] The World Wide Web Consortium (W3C), "Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language." `http://www.w3.org/TR/wsdl20/`, June 2007. W3C Recommendation.

[55] The World Wide Web Consortium (W3C), "Web Services Description Language (WSDL) Version 2.0 Part 2: Adjuncts." `http://www.w3.org/TR/wsdl20-adjuncts/`, June 2007. W3C Recommendation.

[56] Organization for the Advancement of Structured Information Standards (OASIS), "UDDI version 3.0.2." `http://www.uddi.org/pubs/uddi_v3.htm`, October 2004. UDDI Spec Technical Committee Draft.

[57] Organization for the Advancement of Structured Information Standards (OASIS), "Web Services Reliable Messaging (WS-ReliableMessaging)." `http://docs.oasis-open.org/ws-rx/wsrm/200702`, February 2009.

[58] The World Wide Web Consortium (W3C), "Web Services Addressing (WS-Addressing)." `http://www.w3.org/Submission/ws-addressing/`, August 2004. W3C Member Submission.

[59] The World Wide Web Consortium (W3C), "Web Services Policy 1.2 - Framework (WS-Policy)." `http://www.w3.org/Submission/WS-Policy/`, April 2006. W3C Member Submission.

[60] The World Wide Web Consortium (W3C), "Web Services Policy 1.2 - Attachment (WS-PolicyAttachment)." `http://www.w3.org/Submission/WS-PolicyAttachment/`, April 2006. W3C Member Submission.

[61] The World Wide Web Consortium (W3C), "Web Services Metadata Exchange (WS-MetadataExchange)." `http://www.w3.org/TR/2009/WD-ws-metadata-exchange-20090924/`, September 2009. W3C Working Draft.

[62] Organization for the Advancement of Structured Information Standards (OASIS), "WS-SecurityPolicy 1.3." `http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.html`, February 2009. OASIS Standard.

[63] Organization for the Advancement of Structured Information Standards (OASIS), "Web Services Security: SOAP Message Security 1.1." `http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf`, February 2006. OASIS Standard Specification.

[64] The World Wide Web Consortium (W3C), "XML Encryption Syntax and Processing." `http://www.w3.org/TR/xmlenc-core/`, December 2002. W3C Recommendation.

[65] The World Wide Web Consortium (W3C), "XML Signature Syntax and Processing (Second Edition)." http://www.w3.org/TR/xmldsig-core/, June 2008. W3C Recommendation.

[66] The World Wide Web Consortium (W3C), "XML Key Management Specification (XKMS 2.0)." http://www.w3.org/TR/xkms2/, June 2005. W3C Recommendation.

[67] Organization for the Advancement of Structured Information Standards (OASIS), "WS-Trust 1.3." http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf, March 2007. OASIS Standard.

[68] Organization for the Advancement of Structured Information Standards (OASIS), "WS-SecureConversation 1.3." http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.pdf, March 2007. OASIS Standard.

[69] The World Wide Web Consortium (W3C), "OWL-S: Semantic Markup for Web Services." http://www.w3.org/Submission/OWL-S/, November 2004. W3C Member Submission.

[70] D. Martin, M. Burstein, D. Mcdermott, S. Mcilraith, M. Paolucci, K. Sycara, D. L. Mcguinness, E. Sirin, and N. Srinivasan, "Bringing semantics to web services with owl-s," *World Wide Web*, vol. 10, pp. 243–277, September 2007.

[71] The World Wide Web Consortium (W3C), "Semantic Web Services Framework (SWSF) Overview." http://www.w3.org/Submission/SWSF/, September 2005. W3C Member Submission.

[72] International Organization for Standardization (ISO), "ISO 18629-11:2005: Industrial automation systems and integration – Process specification language – Part 11: PSL core," 2007. ISO Standard.

[73] D. Fensel, H. Lausen, A. Polleres, J. de Bruijn, M. Stollberg, D. Roman, and J. Domingue, *Enabling Semantic Web Services, The Web Service Modeling Ontology*. Berlin: Springer, 2006.

[74] WSML Working Group, "WSML Language Reference." http://www.wsmo.org/TR/d16/d16.1/v1.0/, 2008. WSML Final Draft.

[75] J. de Bruijn, H. Lausen, A. Polleres, and D. Fensel, "The Web Service Modeling Language WSML: An Overview," in *The Semantic Web: Research and Applications* (Y. Sure and J. Domingue, eds.), vol. 4011 of *Lecture Notes in Computer Science*, pp. 590–604, Springer Berlin / Heidelberg, 2006.

[76] A. Haller, E. Cimpian, A. Mocan, E. Oren, and C. Bussler, "Wsmx - a semantic service-oriented architecture," in *Proceedings of the IEEE International Conference on Web Services*, ICWS '05, (Washington, DC, USA), pp. 321–328, IEEE Computer Society, 2005.

[77] A. Mocan, M. Moran, E. Cimpian, and M. Zaremba, "Filling the gap - extending service oriented architectures with semantics," in *Proceedings of the IEEE International Conference on e-Business Engineering*, ICEBE '06, (Washington, DC, USA), pp. 594–601, IEEE Computer Society, 2006.

[78] The World Wide Web Consortium (W3C), "Web Service Semantics - WSDL-S." http://www.w3.org/Submission/WSDL-S/, November 2005. W3C Member Submission.

[79] The World Wide Web Consortium (W3C), "Semantic Annotations for WSDL and XML Schema." http://www.w3.org/TR/sawsdl/, August 2007. W3C Recommendation.

[80] M. P. Papazoglou and J. jacques Dubray, "A survey of web service technologies," Tech. Rep. DIT-04-058, University of Trento, Italy, June 2004.

[81] C. Peltz, "Web services orchestration and choreography," *Computer*, vol. 36, pp. 46–52, October 2003.

[82] Organization for the Advancement of Structured Information Standards (OASIS), "Web Services Business Process Execution Language Version 2.0." http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html, April 2007. OASIS Standard.

[83] IBM Software Group, "Web Services Flow Language (WSFL 1.0)." http://xml.coverpages.org/WSFL-Guide-200110.pdf, May 2001.

[84] Organization for the Advancement of Structured Information Standards (OASIS), "Web Services Coordination (WS-Coordination) Version 1.2." `http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.2-spec-cs-01.pdf`, October 2008. Public Review Draft 1.

[85] H. Overdick, "Towards resource-oriented bpel," in *Emerging Web Services Technology, Volume II* (M. Calisti, M. Walliser, S. Brantschen, M. Herbstritt, T. Gschwind, and C. Pautasso, eds.), Whitestein Series in Software Agent Technologies and Autonomic Computing, pp. 129–140, Birkhäuser Basel, 2008.

[86] D. Habich, S. Richly, S. Preissler, M. Grasselt, W. Lehner, and A. Maier, "BPEL^{DT} - data-aware extension for data-intensive service applications," in *Emerging Web Services Technology, Volume II* (M. Calisti, M. Walliser, S. Brantschen, M. Herbstritt, T. Gschwind, and C. Pautasso, eds.), Whitestein Series in Software Agent Technologies and Autonomic Computing, pp. 111–128, Birkhäuser Basel, 2008.

[87] The World Wide Web Consortium (W3C), "WS Choreography Model Overview." `http://www.w3.org/TR/ws-chor-model/`, March 2004. W3C Working Draft.

[88] The World Wide Web Consortium (W3C), "Web Services Choreography Description Language (WS-CDL) Version 1.0." `http://www.w3.org/TR/ws-cdl-10/`, November 2005. W3C Candidate Recommendation.

[89] The World Wide Web Consortium (W3C), "Web Service Choreography Interface (WSCI) 1.0." `http://www.w3.org/TR/wsci/`, August 2002. W3C Note.

[90] J. Rao and X. Su, "A survey of automated web service composition methods," in *Semantic Web Services and Web Process Composition* (J. Cardoso and A. Sheth, eds.), vol. 3387 of *Lecture Notes in Computer Science*, pp. 43–54, Springer Berlin / Heidelberg, 2005.

[91] T. Osman, D. Thakker, and D. Al-Dabass, "Bridging the gap between workflow and semantic-based web services composition," in *Proceedings of the WWW Service Composition with Semantic Web Services*, pp. 13–23, 2005.

[92] B. Norton and C. Pedrinaci, "3-level service composition and cashew: A model for orchestration and choreography in semantic web services," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (R. Meersman, Z. Tari, and P. Herrero, eds.), vol. 4277 of *Lecture Notes in Computer Science*, pp. 58–67, Springer Berlin / Heidelberg, 2006.

[93] J. Fiadeiro, A. Lopes, and L. Bocchi, "A Formal Approach to Service Component Architecture," in *Web Services and Formal Methods* (M. Bravetti, M. Núñez, and G. Zavattaro, eds.), vol. 4184 of *Lecture Notes in Computer Science*, pp. 193–213, Springer Berlin / Heidelberg, 2006.

[94] J. Abreu, L. Bocchi, J. Fiadeiro, and A. Lopes, "Specifying and composing interaction protocols for service-oriented system modelling," in *Formal Techniques for Networked and Distributed Systems – FORTE 2007* (J. Derrick and J. Vain, eds.), vol. 4574 of *Lecture Notes in Computer Science*, pp. 358–373, Springer Berlin / Heidelberg, 2007.

[95] S. Gorton, C. Montangero, S. Reiff-Marganiec, and L. Semini, "Stpowla: Soa, policies and workflows," in *Service-Oriented Computing - ICSOC 2007 Workshops* (E. Di Nitto and M. Ripeanu, eds.), vol. 4907 of *Lecture Notes in Computer Science*, pp. 351–362, Springer Berlin / Heidelberg, 2009.

[96] A. Brogi, R. Popescu, and M. Tanca, "Design and implementation of Sator: A web service aggregator," *ACM Trans. Softw. Eng. Methodol.*, vol. 19, pp. 10:1–10:21, February 2010.

[97] E. Sirin, B. Parsia, D. Wu, J. Hendler, and D. Nau, "Htn planning for web service composition using shop2," *Web Semant.*, vol. 1, pp. 377–396, October 2004.

[98] H. Meyer, H. Overdick, and M. Weske, "Plaengine: A system for automated service composition and process enactment," in *Proceedings of the WWW Service Composition with Semantic Web Services*, pp. 3–12, 2005.

[99] Y. Yan, Y. Liang, and H. Liang, "Composing business processes with partial observable problem space in web services environments," in *Proceedings of the IEEE International Conference on Web Services*, (Washington, DC, USA), pp. 541–548, IEEE Computer Society, 2006.

[100] Y. Li, X. Yu, L. Geng, and L. Wang, "Research on reasoning of the dynamic semantic web services composition," in *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence*, WI '06, (Washington, DC, USA), pp. 435–441, IEEE Computer Society, 2006.

[101] Y. Charif and N. Sabouret, "An Overview of Semantic Web Services Composition Approaches," *Electron. Notes Theor. Comput. Sci.*, vol. 146, pp. 33–41, January 2006.

[102] C. Ramos, J. C. Augusto, and D. Shapiro, "Ambient intelligence: the next step for artificial intelligence," *IEEE Intelligent Systems*, vol. 23, pp. 15–18, March 2008.

[103] K. Fujii and T. Suda, "Semantics-based context-aware dynamic service composition," *ACM Trans. Auton. Adapt. Syst.*, vol. 4, pp. 12:1–12:31, May 2009.

[104] D. Chappell, *Enterprise Service Bus*. Sebastopol: O'Reilly Media, Inc, 2004.

[105] G. Hohpe and B. Woolf, *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*. Addison-Wesley, 2004.

[106] S. Y. Ghalsasi, "Critical success factors for event driven service oriented architecture," in *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, ICIS '09, (New York, NY, USA), pp. 1441–1446, ACM, 2009.

[107] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, pp. 114–131, June 2003.

[108] Organization for the Advancement of Structured Information Standards (OASIS), "WS-Notification Version 1.3." `http://www.oasis-open.org/committees/documents.php?wg=wsn`, October 2006. OASIS Standard.

[109] Organization for the Advancement of Structured Information Standards (OASIS), "Reference Model for Service Oriented Architecture 1.0." `http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf`, October 2006. OASIS Standard.

[110] The Open Group, "Service-Oriented Architecture Ontology." `https://www.opengroup.org/projects/soa-ontology/uploads/40/22766/SOA_ontology_public_draft_3_2.pdf`, 2010. Technical Standard.

[111] The World Wide Web Consortium (W3C), "OWL Web Ontology Language Overview." `http://www.w3.org/TR/owl-features/`, February 2004. W3C Recommendation.

[112] The Object Management Group (OMG), "Service oriented architecture Modeling Language (SoaML) - Specification for the UML Profile and Metamodel for Services (UPMS)." `http://www.omg.org/spec/SoaML/1.0/Beta2/PDF`, 2009. OMG Adopted Specification.

[113] Organization for the Advancement of Structured Information Standards (OASIS), "Reference Architecture for Service Oriented Architecture Version 1.0." `http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf`, April 2008. Public Review Draft 1.

[114] The Open Group, "SOA Governance Framework." `https://www.opengroup.org/projects/soa-governance/uploads/40/19263/SOA_Governance_Architecture_v2.4.pdf`, 2009. Draft Technical Standard.

[115] The Open Group, "SOA Reference Architecture." `https://www.opengroup.org/projects/soa-ref-arch/uploads/40/19713/soa-ra-public-050609.pdf`, April 2009. Draft Technical Standard.

[116] The Open Group, "The Open Group Service Integration Maturity Model (OSIMM)." `https://www.opengroup.org/projects/osimm/uploads/40/17990/OSIMM_v0.3a.pdf`, 2006. Draft Technical Standard.

[117] P. Lawrence, ed., *Workflow handbook 1997*. New York, NY, USA: John Wiley & Sons, Inc., 1997.

[118] R. K. L. Ko, "A computer scientist's introductory guide to business process management (bpm)," *Crossroads*, vol. 15, pp. 4:11–4:18, June 2009.

[119] A. ter Hofstede, W. van der Aalst, A. ter Hofstede, and M. Weske, "Business process management: A survey," in *Business Process Management* (M. Weske, ed.), vol. 2678 of *Lecture Notes in Computer Science*, pp. 1019–1019, Springer Berlin / Heidelberg, 2003.

[120] M. Weske, W. M. P. van der Aalst, and H. M. W. Verbeek, "Advances in business process management," *Data Knowl. Eng.*, vol. 50, pp. 1–8, July 2004.

[121] The Object Management Group (OMG), "Business Process Model and Notation (BPMN), Version 2.0." `http://www.omg.org/spec/BPMN/2.0/PDF`, January 2011. OMG Specification.

[122] W. M. P. van der Aalst and A. H. M. ter Hofstede, "Yawl: yet another workflow language," *Information Systems*, vol. 30, pp. 245–275, June 2005.

[123] M. Adams, A. ter Hofstede, D. Edmond, and W. van der Aalst, "Worklets: A service-oriented implementation of dynamic flexibility in workflows," in *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE* (R. Meersman and Z. Tari, eds.), vol. 4275 of *Lecture Notes in Computer Science*, pp. 291–308, Springer Berlin / Heidelberg, 2006.

[124] J. Ye, S. Sun, W. Song, and L. Wen, "Formal semantics of bpmn process models using yawl," in *Intelligent Information Technology Application, 2008. IITA '08. Second International Symposium on*, vol. 2, pp. 70–74, dec. 2008.

[125] N. Russell and A. ter Hofstede, "Surmounting bpm challenges: the yawl story," *Computer Science - Research and Development*, vol. 23, pp. 67–79, 2009.

[126] N. Russell and A. ter Hofstede, "*new*YAWL: Towards Workflow 2.0," in *Transactions on Petri Nets and Other Models of Concurrency II* (K. Jensen and W. van der Aalst, eds.), vol. 5460 of *Lecture Notes in Computer Science*, pp. 79–97, Springer Berlin / Heidelberg, 2009.

[127] A. ter Hofstede, W. van der Aalst, and M. Weske, "Business Process Management: A Survey," in *Business Process Management* (M. Weske, ed.), vol. 2678 of *Lecture Notes in Computer Science*, pp. 1019–1019, Springer Berlin / Heidelberg, 2003.

[128] B. Ludäscher, I. Altintas, S. Bowers, J. Cummings, T. Critchlow, E. Deelman, D. D. Roure, J. Freire, C. Goble, M. Jones, S. Klasky, T. McPhillips, N. Podhorszki, C. Silva, I. Taylor, and M. Vouk, "Scientific process automation and workflow management," in *Scientific Data Management* (A. Shoshani and D. Rotem, eds.), Computational Science Series, ch. 13, Chapman & Hall, 2009.

[129] I. Altintas, C. Berkley, E. Jaeger, M. Jones, B. Ludascher, and S. Mock, "Kepler: an extensible system for design and execution of scientific workflows," in *Scientific and Statistical Database Management, 2004. Proceedings. 16th International Conference on*, pp. 423 – 424, june 2004.

[130] E. Deelman, G. Singh, M.-H. Su, J. Blythe, Y. Gil, C. Kesselman, G. Mehta, K. Vahi, G. B. Berriman, J. Good, A. Laity, J. C. Jacob, and D. S. Katz, "Pegasus: A framework for mapping complex scientific workflows onto distributed systems," *Scientific Programming*, vol. 13, pp. 219–237, July 2005.

[131] D. Churches, G. Gombas, A. Harrison, J. Maassen, C. Robinson, M. Shields, I. Taylor, and I. Wang, "Programming scientific and distributed workflow with triana services," *Concurrency and Computation: Practice and Experience*, vol. 18, no. 10, pp. 1021–1037, 2006.

[132] B. Ludäscher, I. Altintas, C. Berkley, D. Higgins, E. Jaeger, M. Jones, E. A. Lee, J. Tao, and Y. Zhao, "Scientific workflow management and the kepler system," *Concurr. Comput. : Pract. Exper.*, vol. 18, pp. 1039–1065, August 2006.

[133] Y. Gil, V. Ratnakar, E. Deelman, G. Mehta, and J. Kim, "Wings for pegasus: creating large-scale scientific applications using semantic representations of computational workflows," in *Proceedings of the 19th national conference on Innovative applications of artificial intelligence - Volume 2*, pp. 1767–1774, AAAI Press, 2007.

[134] Y. Gil, E. Deelman, M. Ellisman, T. Fahringer, G. Fox, D. Gannon, C. Goble, M. Livny, L. Moreau, and J. Myers, "Examining the challenges of scientific workflows," *Computer*, vol. 40, pp. 24–32, dec. 2007.

[135] Y. Zhao, I. Raicu, and I. Foster, "Scientific workflow systems for 21st century, new bottle or new wine?," in *Proceedings of the 2008 IEEE Congress on Services - Part I*, SERVICES '08, (Washington, DC, USA), pp. 467–471, IEEE Computer Society, 2008.

[136] V. Curcin and M. Ghanem, "Scientific workflow systems - can one size fit all?," in *Biomedical Engineering Conference, 2008. CIBEC 2008. Cairo International*, pp. 1–9, dec. 2008.

[137] A. Barker and J. van Hemert, "Scientific workflow: A survey and research directions," in *Parallel Processing and Applied Mathematics* (R. Wyrzykowski, J. Dongarra, K. Karczewski, and J. Wasniewski, eds.), vol. 4967 of *Lecture Notes in Computer Science*, pp. 746–753, Springer Berlin / Heidelberg, 2008.

[138] E. Deelman, D. Gannon, M. Shields, and I. Taylor, "Workflows and e-science: An overview of workflow system features and capabilities," *Future Gener. Comput. Syst.*, vol. 25, pp. 528–540, May 2009.

[139] B. Ludäscher, M. Weske, T. Mcphillips, and S. Bowers, "Scientific Workflows: Business as Usual?," in *Proceedings of the 7th International Conference on Business Process Management*, BPM '09, (Berlin, Heidelberg), pp. 31–47, Springer-Verlag, 2009.

[140] R. Barga and D. Gannon, "Scientific versus business workflows," in *Workflows for e-Science* (I. J. Taylor, E. Deelman, D. B. Gannon, and M. Shields, eds.), pp. 9–16, Springer London, 2007.

[141] U. Yildiz, A. Guabtni, and A. H. Ngu, "Business versus scientific workflows: A comparative study," *Services, IEEE Congress on*, vol. 0, pp. 340–343, 2009.

[142] W. Tan, P. Missier, R. Madduri, and I. Foster, "Service-oriented computing — icsoc 2008 workshops," ch. Building Scientific Workflow with Taverna and BPEL: A Comparative Study in caGrid, pp. 118–129, Berlin, Heidelberg: Springer-Verlag, 2009.

[143] N. Russell, A. ter Hofstede, D. Edmond, and W. van der Aalst, "Workflow Resource Patterns," 2004. BETA Working Paper Series, WP 127, Eindhoven University of Technology.

[144] N. Russell, A. ter Hofstede, D. Edmond, and W. van der Aalst, "Workflow Data Patterns," 2004. QUT Technical report, FIT-TR-2004-01, Queensland University of Technology, Brisbane.

[145] N. Russell, A. ter Hofstede, W. van der Aalst, and N. Mulyar, "Workflow Control-Flow Patterns : A Revised View," in *BPM Center Report BPM-06-22*, BPMcenter.org, 2006.

[146] U. Yildiz, A. Guabtni, and A. H. H. Ngu, "Towards scientific workflow patterns," in *Proceedings of the 4th Workshop on Workflows in Support of Large-Scale Science*, WORKS '09, (New York, NY, USA), pp. 13:1–13:10, ACM, 2009.

[147] S. White, "Process modeling notations and workflow patterns," in *Workflow Handbook 2004* (L. Fischer, ed.), Future Strategies Inc., 2004.

[148] P. Wohed, W. van der Aalst, M. Dumas, A. ter Hofstede, and N. Russell, "On the Suitability of BPMN for Business Process Modelling," in *Business Process Management* (S. Dustdar, J. Fiadeiro, and A. Sheth, eds.), vol. 4102 of *Lecture Notes in Computer Science*, pp. 161–176, Springer Berlin / Heidelberg, 2006.

[149] S. Migliorini, M. Gambini, and A. La Rosa, M.and ter Hofstede, "Pattern-Based Evaluation of Scientific Workflow Management Systems," in *BPM Center Report BPM-11-03*, BPMcenter.org, 2011.

[150] T. Schreiter, "xBPMN++, Towards Executability of BPMN: Data Perspective and Process Instantiation," Master's thesis, Hasso Platner Institute, 2008.

[151] A. Meyer, "Resource Perspective in BPMN: Extending BPMN to Support Resource Management and Planning," Master's thesis, Hasso Platner Institute, 2009.

[152] M. Magnani and D. Montesi, "BPDMN: A Conservative Extension of BPMN with Enhanced Data Representation Capabilities," *CoRR*, vol. abs/0907.1978, 2009.

[153] S. Fan, W. Dou, and J. Chen, "Dual workflow nets: Mixed control/data-flow representation for workflow modeling and verification," in *Advances in Web and Network Technologies, and Information Management* (K. Chang, W. Wang, L. Chen, C. Ellis, C.-H. Hsu, A. Tsoi, and H. Wang, eds.), vol. 4537 of *Lecture Notes in Computer Science*, pp. 433–444, Springer Berlin / Heidelberg, 2007.

[154] N. Trčka, W. M. Aalst, and N. Sidorova, "Analyzing control-flow and data-flow in workflow processes in a unified way," *Computer Science Report*, pp. 1–23, 2008.

[155] R. Hull, "Artifact-centric business process models: Brief survey of research results and challenges," in *On the Move to Meaningful Internet Systems: OTM 2008* (R. Meersman and Z. Tari, eds.), vol. 5332 of *Lecture Notes in Computer Science*, pp. 1152–1163, Springer Berlin / Heidelberg, 2008.

[156] S. Al-Fedaghi, "Integrating services: Control vs. flow," in *Information Reuse Integration, 2009. IRI '09. IEEE International Conference on*, pp. 68 –73, aug. 2009.

[157] M. Sonntag, D. Karastoyanova, and E. Deelman, "Bridging the gap between business and scientific workflows: Humans in the loop of scientific workflows," in *e-Science (e-Science), 2010 IEEE Sixth International Conference on*, pp. 206 –213, dec. 2010.

[158] J. Yu and R. Buyya, "A taxonomy of scientific workflow systems for grid computing," *SIGMOD Rec.*, vol. 34, pp. 44–49, September 2005.

[159] J. Yu and R. Buyya, "A taxonomy of workflow management systems for grid computing," tech. rep., JOURNAL OF GRID COMPUTING, 2005.

[160] D. J. Abadi, D. Carney, U. Çetintemel, M. Cherniack, C. Convey, S. Lee, M. Stonebraker, N. Tatbul, and S. Zdonik, "Aurora: a new model and architecture for data stream management," *The VLDB Journal*, vol. 12, pp. 120–139, August 2003.

[161] J. D. Blower, A. B. Harrison, and K. Haines, "Styx grid services: Lightweight middleware for efficient scientific workflows," *Sci. Program.*, vol. 14, pp. 209–216, December 2006.

[162] D. Zinn, Q. Hart, T. McPhillips, B. Luda® andscher, Y. Simmhan, M. Giakkoupis, and V. Prasanna, "Towards reliable, performant workflows for streaming-applications on cloud platforms," in *Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on*, pp. 235 –244, may 2011.

[163] A. Wombacher, "How physical objects and business workflows can be correlated," in *Services Computing (SCC), 2011 IEEE International Conference on*, pp. 226 –233, july 2011.

[164] P. Neophytou, P. K. Chrysanthis, and A. Labrinidis, "Towards continuous workflow enactment systems," in *Collaborative Computing: Networking, Applications and Worksharing* (E. Bertino, J. B. D. Joshi, O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari, M. Gerla, H. Kobayashi, S. Palazzo, S. Sahni, X. S. Shen, M. Stan, J. Xiaohua, A. Zomaya, and G. Coulson, eds.), vol. 10 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 162–178, Springer Berlin Heidelberg, 2009.

[165] L. Dou, D. Zinn, T. McPhillips, S. Kohler, S. Riddle, S. Bowers, and B. Ludascher, "Scientific workflow design 2.0: Demonstrating streaming data collections in kepler," in *Data Engineering (ICDE), 2011 IEEE 27th International Conference on*, pp. 1296 –1299, april 2011.

[166] Business Process Modeling Initiative (BPMI), "Business Process Modeling Notation (BPMN), Version 1.0." `http://www.omg.org/bpmn/Documents/BPMN_V1-0_May_3_2004.pdf`, May 2004.

[167] E. Börger, "Approaches to modeling business processes: a critical analysis of bpmn, workflow patterns and yawl," *Software & Systems Modeling*, vol. 11, no. 3, pp. 305–318, 2012.

[168] M. Muehlen and J. Recker, "How much language is enough? theoretical and practical use of the business process modeling notation," in *Advanced Information Systems Engineering* (Z. Bellahsène and M. Léonard, eds.), vol. 5074 of *Lecture Notes in Computer Science*, pp. 465–479, Springer Berlin Heidelberg, 2008.

[169] A. Meyer, S. Smirnov, and M. Weske, "Data in Business Processes," Tech. Rep. 50, Hasso Plattner Institute, University of Potsdam, 2011.

[170] A. Grosskopf, "An extended resource information layer for BPMN," 2007. BPTG seminar paper, Hasso Plattner Institute, University of Potsdam.

[171] C. Wolter, A. Schaad, and C. Meinel, "Task-based entailment constraints for basic workflow patterns," in *Proceedings of the 13th ACM symposium on Access control models and technologies*, SACMAT '08, (New York, NY, USA), pp. 51–60, ACM, 2008.

[172] C. A. Petri, *Kommunikation mit Automaten*. PhD thesis, Germany, 1962.

[173] W. M. P. Van Der Aalst, A. H. M. Ter Hofstede, B. Kiepuszewski, and A. P. Barros, "Workflow patterns," *Distrib. Parallel Databases*, vol. 14, pp. 5–51, July 2003.

[174] N. Russell, W. Aalst, and A. Hofstede, "Workflow exception patterns," in *Advanced Information Systems Engineering* (E. Dubois and K. Pohl, eds.), vol. 4001 of *Lecture Notes in Computer Science*, pp. 288–302, Springer Berlin Heidelberg, 2006.

[175] N. Russell, A. Hofstede, D. Edmond, and W. der Aalst, "Workflow data patterns: Identification, representation and tool support," in *Conceptual Modeling – ER 2005* (L. Delcambre, C. Kop, H. Mayr, J. Mylopoulos, and O. Pastor, eds.), vol. 3716 of *Lecture Notes in Computer Science*, pp. 353–368, Springer Berlin Heidelberg, 2005.

[176] N. Russell, W. Aalst, A. Hofstede, and D. Edmond, "Workflow resource patterns: Identification, representation and tool support," in *Advanced Information Systems Engineering* (O. Pastor and J. Falcão e Cunha, eds.), vol. 3520 of *Lecture Notes in Computer Science*, pp. 216–232, Springer Berlin Heidelberg, 2005.

[177] K. Jensen, *Coloured Petri Nets - Basic Concepts, Analysis Methods and Practical Use*. Berlin, Germany: Springer, 1996.

[178] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1996.

[179] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, NY, USA: John Wiley & Sons, Inc., 2nd ed., 1995.

[180] National Institute of Standards and Technology, "Data Encryption Standard (DES)," tech. rep., Federal Information Processing Standard Publication 46-3, October 1999.

[181] National Institute of Standards and Technology, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," tech. rep., Special Publication 800-67, May 2004.

[182] National Institute of Standards and Technology, "Advance Encryption Standard (AES)," tech. rep., Special Publication 800-67, May 2004.

[183] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," in *Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '90, (New York, NY, USA), pp. 389–404, Springer-Verlag New York, Inc., 1991.

[184] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *Fast Software Encryption, Cambridge Security Workshop*, (London, UK), pp. 191–204, Springer-Verlag, 1994.

[185] R. Rivest, "A Description of the RC2(r) Encryption Algorithm," March 1998.

[186] R. Rivest, "The RC4 encryption algorithm," tech. rep., RSA Data Security, Inc., March 1992.

[187] R. Baldwin and R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms," October 1996.

[188] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, pp. 644 – 654, nov 1976.

[189] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, February 1978.

[190] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, January 1987.

[191] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2nd ed., 2002.

[192] National Institute of Standards and Technology, "Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001.

[193] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL Protocol Version 3.0." draft-freier-ssl-version3-02.

[194] T. Dierks and E. Rescorla, "The TLS Protocol Version 1.1," April 2006.

[195] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," August 2008.

[196] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1," June 1999.

[197] J. Klensin, "Simple Mail Transfer Protocol," April 2001.

[198] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudeonymity — a proposal for terminology," in *International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, (New York, NY, USA), pp. 1–9, Springer-Verlag New York, Inc., 2001.

[199] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous connections and onion routing," in *IEEE Symposium on Security and Privacy*, pp. 44–54, IEEE Computer Society, 1997.

[200] R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, pp. 303–320, USENIX, 2004.

[201] M. K. Reiter and A. D. Rubin, "Crowds: anonymity for web transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998.

[202] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," in *International Workshop on Design Issues in Anonymity and Unobservability*, pp. 46–66, Springer, 2000.

[203] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[204] G. Danezis, C. Diaz, and P. Syverson, *Systems for Anonymous Communication*, ch. 13, pp. 341–389. CRC Cryptography and Network Security Series, Chapman & Hall, 2010.

[205] Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG), "Identity Management Systems (IMS): Identification and Comparison Study," September 2003.

[206] J. Camenisch and B. Pfitzmann, "Federated identity management," in *Security, Privacy, and Trust in Modern Data Management* (M. Petković and W. Jonker, eds.), Data-Centric Systems and Applications, pp. 213–238, Springer Berlin Heidelberg, 2007.

[207] S. S. Y. Shim, G. Bhalla, and V. Pendyala, "Federated identity management," *Computer*, vol. 38, pp. 120–122, December 2005.

[208] The Liberty Alliance Project, "Liberty Alliance Identity Federation 1.2 (ID-FF 1.2) Specifications." `http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications/`.

[209] The Liberty Alliance Project, "Liberty Alliance ID-WSF 2.0 Specifications including Errata v1.0 Updates." `http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates/`.

[210] The Liberty Alliance Project, "Liberty Alliance ID-SIS 1.0 Specifications." `http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_sis_1_0_specifications/`.

[211] Organization for the Advancement of Structured Information Standards, "OASIS Security Services (SAML) TC." http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[212] Organization for the Advancement of Structured Information Standards, "Security Assertion Markup Language (SAML) v2.0." http://saml.xml.org/saml-specifications.

[213] V. Bertocci, G. Serack, and C. Baker, *Understanding windows cardspace: an introduction to the concepts and challenges of digital identities*. Addison-Wesley Professional, first ed., 2007.

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

[215] OpenID Foundation. http://openid.net/.

[216] D. Recordon and D. Reed, "Openid 2.0: a platform for user-centric identity management," in *Proceedings of the second ACM workshop on Digital identity management*, DIM '06, (New York, NY, USA), pp. 11–16, ACM, 2006.

[217] Thibeau, D., "Open Trust Frameworks for Open Government: Enabling Citizen Involvement through Open Identity Technologies." A White Paper from the OpenID Foundation and Information Card Foundation, August 2009.

[218] B. Pfitzmann, "Privacy in enterprise identity federation," in *Privacy Enhancing Technologies* (R. Dingledine, ed.), vol. 2760 of *Lecture Notes in Computer Science*, pp. 189–204, Springer Berlin / Heidelberg, 2003.

[219] B. Pfitzmann and M. Waidner, "Analysis of liberty single-sign-on with enabled clients," *IEEE Internet Computing*, vol. 7, pp. 38–44, November 2003.

[220] M. Alsaleh and C. Adams, "Enhancing consumer privacy in the liberty alliance identity federation and web services frameworks," in *Privacy Enhancing Technologies* (G. Danezis and P. Golle, eds.), vol. 4258 of *Lecture Notes in Computer Science*, pp. 59–77, Springer Berlin / Heidelberg, 2006.

[221] T. Alamäki, M. Björksten, P. Dornbach, C. Gripenberg, N. Győrbíró, G. Márton, Z. Németh, T. Skyttä, and M. Tarkiainen, "Privacy enhancing service architectures," in *Privacy Enhancing Technologies* (R. Dingledine and P. Syverson, eds.), vol. 2482 of *Lecture Notes in Computer Science*, pp. 204–208, Springer Berlin / Heidelberg, 2003.

[222] K. Seamons, M. Winslett, T. Yu, L. Yu, and R. Jarvis, "Protecting privacy during on-line trust negotiation," in *Privacy Enhancing Technologies* (R. Dingledine and P. Syverson, eds.), vol. 2482 of *Lecture Notes in Computer Science*, pp. 249–253, Springer Berlin / Heidelberg, 2003.

[223] G. Gidofalvi, X. Huang, and T. B. Pedersen, "Privacy-preserving data mining on moving object trajectories," in *Proceedings of the 2007 International Conference on Mobile Data Management*, (Washington, DC, USA), pp. 60–68, IEEE Computer Society, 2007.

[224] A. Solanas, J. Domingo-Ferrer, and A. Mart´ınez-Ballest´, "Location privacy in location-based services: Beyond ttp-based schemes," in *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PiLBA)*, vol. 397, 2008.

[225] J. Domingo-Ferrer, "Location privacy via unlinkability: an alternative to cloaking and perturbation," in *Proceedings of the 2008 international workshop on Privacy and anonymity in information society*, PAIS '08, (New York, NY, USA), pp. 1–2, ACM, 2008.

[226] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '01, (London, UK), pp. 93–118, Springer-Verlag, 2001.

[227] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, (New York, NY, USA), pp. 21–30, ACM, 2002.

[228] "The Higgins Trust Framework Project." http://www.eclipse.org/higgins/.

[229] "FP6 IST project PRIME (Privacy and Identity Management for Europe)." `https://www.prime-project.eu/`.

[230] "FP7 IST project PrimeLife (Privacy and Identity Management in Europe for Life)." `http://www.primelife.eu/`.

[231] G. Bianchi, M. Bonola, V. Falletta, F. S. Proto, and S. Teofili, "The sparta pseudonym and authorization system," *Electron. Notes Theor. Comput. Sci.*, vol. 197, pp. 57–71, February 2008.

[232] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," in *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, STOC '87, (New York, NY, USA), pp. 210–217, ACM, 1987.

[233] D. Chaum, "Showing credentials without identification. signatures transferred between unconditionally unlinkable pseudonyms," in *Proc. of a workshop on the theory and application of cryptographic techniques on Advances in cryptology—EUROCRYPT '85*, (New York, NY, USA), pp. 241–244, Springer-Verlag New York, Inc., 1986.

[234] D. Chaum, "Achieving electronic privacy," *Scientific American*, pp. 91—101, 1992.

[235] S. Crane and M. C. Mont, "A customizable reputation-based privacy assurance system using active feedback," in *Securecomm and Workshops, 2006*, pp. 1 –8, 28 2006-sept. 1 2006.

[236] S. Pearson, "Trusted computing: Strengths, weaknesses and further opportunities for enhancing privacy," in *Trust Management* (P. Herrmann, V. Issarny, and S. Shiu, eds.), vol. 3477 of *Lecture Notes in Computer Science*, pp. 91–117, Springer Berlin / Heidelberg, 2005.

[237] A. Herzberg and Y. Mass, "Relying party credentials framework," vol. 4, pp. 23–39, January 2004.

[238] M. Mont and L. Tomasi, "A distributed system, adaptive to trust assessment, based on peer-to-peer e-records replication and storage," in *Proceedings of the 8th IEEE Workshop on Future Trends of Distributed Computing Systems*, (Washington, DC, USA), pp. 89–, IEEE Computer Society, 2001.

[239] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.

[240] M. Casassa Mont, "Dealing with privacy obligations: Important aspects and technical approache booktitle = Trust and Privacy in Digital Business, series = Lecture Notes in Computer Science, editor = Katsikas, Sokratis and Lopez, Javier and Pernul, Günther, publisher = Springer Berlin / Heidelberg, isbn = 978-3-540-22919-3, keyword = Computer Science, pages = 120-131, volume = 3184, year = 2004,"

[241] "Τεχνολογίες Ελέγχου Πρόσβασης για Προστασία της Ιδιωτικότητας," in *Προστασία της Ιδιωτικότητας στις Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα* (Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, and Σ. Κάτσικας, eds.), pp. 93 — 121, Αθήνα: Παπασωτηρίου, 2010.

[242] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Access Control," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

[243] P. Wayner, *Translucent Databases 2nd Edition: Confusion, misdirection, randomness, sharing, authentication and steganography to defend privacy*. Paramount, CA: CreateSpace, 2009.

[244] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in *Proceedings of the 29th international conference on Very large data bases - Volume 29*, VLDB '2003, pp. 898–909, VLDB Endowment, 2003.

[245] E. Bertino and E. Ferrari, "Secure and selective dissemination of xml documents," *ACM Trans. Inf. Syst. Secur.*, vol. 5, pp. 290–331, August 2002.

[246] M. Mont and S. Pearson, "An adaptive privacy management system for data repositories," in *Trust, Privacy, and Security in Digital Business* (S. Katsikas, J. López, and G. Pernul, eds.), vol. 3592 of *Lecture Notes in Computer Science*, pp. 236–245, Springer Berlin / Heidelberg, 2005.

[247] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic databases," in *VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases*, pp. 143–154, VLDB Endowment, 2002.

[248] K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. DeWitt, "Limiting disclosure in hippocratic databases," in *Proceedings of the Thirtieth international conference on Very large data bases - Volume 30*, VLDB '04, pp. 108–119, VLDB Endowment, 2004.

[249] F. Massacci, J. Mylopoulos, and N. Zannone, "Minimal disclosure in hierarchical hippocratic databases with delegation," in *Computer Security – ESORICS 2005* (S. di Vimercati, P. Syverson, and D. Gollmann, eds.), vol. 3679 of *Lecture Notes in Computer Science*, pp. 438–454, Springer Berlin / Heidelberg, 2005.

[250] F. Massacci, J. Mylopoulos, and N. Zannone, "Hierarchical hippocratic databases with minimal disclosure for virtual organizations," *The VLDB Journal*, vol. 15, pp. 370–387, November 2006.

[251] E. Bertino, J.-W. Byun, and N. Li, "Privacy-preserving database systems," in *Foundations of Security Analysis and Design III* (A. Aldini, R. Gorrieri, and F. Martinelli, eds.), vol. 3655 of *Lecture Notes in Computer Science*, pp. 178–206, Springer Berlin / Heidelberg, 2005.

[252] J.-W. Byun, E. Bertino, and N. Li, "Purpose based access control for privacy protection in relational database systems," Tech. Rep. TR 2004-52, CERIAS, Purdue University, 2004.

[253] J.-W. Byun, E. Bertino, and N. Li, "Purpose based access control of complex data for privacy protection," in *SACMAT '05: Proceedings of the 10th ACM symposium on Access control models and technologies*, pp. 102–110, ACM, 2005.

[254] J.-W. Byun and N. Li, "Purpose based access control for privacy protection in relational database systems," *The VLDB Journal*, vol. 17, no. 4, pp. 603–619, 2008.

[255] S. Ashley, P.and Hada, G. Karjoth, and M. Schunter, "Enterprise Privacy Authorisation Language (EPAL 1.2) Specification," tech. rep., IBM Research Report, June 2003.

[256] M. Backes, B. Pfitzmann, and M. Schunter, "A toolkit for managing enterprise privacy policies," in *Computer Security – ESORICS 2003* (E. Snekkenes and D. Gollmann, eds.), vol. 2808 of *Lecture Notes in Computer Science*, pp. 162–180, Springer Berlin / Heidelberg, 2003.

[257] M. Casassa Mont and R. Thyne, "A systemic approach to automate privacy policy enforcement in enterprises," in *Privacy Enhancing Technologies* (G. Danezis and P. Golle, eds.), vol. 4258 of *Lecture Notes in Computer Science*, pp. 118–134, Springer Berlin / Heidelberg, 2006.

[258] Organization for the Advancement of Structured Information Standards, "OASIS eXtensible Access Control Markup Language (XACML) TC." `http://www.oasis-open.org/committees/xacml/`.

[259] T. Moses, "OASIS Privacy Policy Profile of XACML v2.0," OASIS Standard, February 2005.

[260] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C.-M. Karat, J. Karat, and A. Trombetta, "Privacy-aware role-based access control," *ACM Transactions on Information and System Security*, vol. 13, no. 3, pp. 1–31, 2010.

[261] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "A privacy-aware access control system," *Journal of Computer Security*, vol. 16, pp. 369–392, September 2008.

[262] C. Ardagna, M. Cremonini, S. D. C. d. Vimercati, and P. Samarati, "Privacy-enhanced location-based access control," in *Handbook of Database Security* (M. Gertz and S. Jajodia, eds.), pp. 531–552, Springer US, 2008.

[263] F. Cuppens and N. Cuppens-Boulahia, "Modeling Contextual Security Policies," *International Journal of Information Security*, vol. 7, no. 4, pp. 285–305, 2008.

[264] J. B. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, pp. 4–23, 2005.

[265] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: A spatially aware RBAC," in *SACMAT '05: Proceedings of the 10th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 29–37, ACM, 2005.

[266] A. Ravari, J. Jafarian, M. Amini, and R. Jalili, "GTHBAC: A Generalized Temporal History Based Access Control Model," *Telecommunication Systems*, vol. 45, pp. 111–125, 2010.

[267] I. Ray and M. Toahchoodee, "A spatio-temporal access control model supporting delegation for pervasive computing applications," in *Trust, Privacy and Security in Digital Business* (S. Furnell, S. Katsikas, and A. Lioy, eds.), vol. 5185 of *Lecture Notes in Computer Science*, pp. 48–58, Springer Berlin / Heidelberg, 2008.

[268] G. V. Lioudakis, F. Gogoulos, A. Antonakopoulou, A. S. Mousas, I. S. Venieris, and D. I. Kaklamani, "An access control approach for privacy-preserving passive network monitoring," in *ICITST 2009: Proceedings of the 4th International Conference for Internet Technology and Secured Transactions*, November 2009.

[269] G. V. Lioudakis, F. Gogoulos, A. Antonakopoulou, D. I. Kaklamani, and I. S. Venieris, "Privacy protection in passive network monitoring: An access control approach," in *WAINA 2009: Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops*, pp. 109–116, IEEE Computer Society, 2009.

[270] G. Lioudakis, N. Dellas, E. Koutsoloukas, G. Kapitsaki, D. Kaklamani, and I. Venieris, "A semantic framework for privacy-aware access control," in *Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on*, pp. 813 –820, oct. 2008.

[271] R. Ferrini and E. Bertino, "Supporting rbac with xacml+owl," in *SACMAT '09: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, pp. 145–154, ACM, 2009.

[272] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham, "Rowlbac: representing role based access control in owl," in *Proceedings of the 13th ACM symposium on Access control models and technologies*, SACMAT '08, (New York, NY, USA), pp. 73–82, ACM, 2008.

[273] A. N. Ravari, M. Amini, and R. Jalili, "A semantic aware access control model with real time constraints on history of accesses," in *IMCSIT 2008: Proceedings of the International Multiconference on Computer Science and Information Technology*, pp. 827–836, IEEE Computer Society, 2008.

[274] Sun Microsystems, "Enterprise JavaBeans (EJB) Technology." `http://java.sun.com/products/ejb/`.

[275] R. Filman, L. Cranor, and A. Chowdhury, *Aspect-Oriented Software Development*. Addison-Wesley, 2004.

[276] C. Berghe and M. Schunter, "Privacy injector — automated privacy enforcement through aspects," in *Privacy Enhancing Technologies* (G. Danezis and P. Golle, eds.), vol. 4258 of *Lecture Notes in Computer Science*, pp. 99–117, Springer Berlin / Heidelberg, 2006.

[277] J. Jürjens, "Sound methods and effective tools for model-based security engineering with uml," in *Proceedings of the 27th international conference on Software engineering*, ICSE '05, (New York, NY, USA), pp. 322–331, ACM, 2005.

[278] T. Lodderstedt, D. A. Basin, and J. Doser, "Secureuml: A uml-based modeling language for model-driven security," in *Proceedings of the 5th International Conference on The Unified Modeling Language*, UML '02, (London, UK, UK), pp. 426–441, Springer-Verlag, 2002.

[279] Object Management Group (OMG), "Unified Modeling Language (UML) Version 2.2." `http://www.omg.org/technology/documents/formal/uml.htm`, February 2009. OMG Specification.

[280] D. Basin, J. Doser, and T. Lodderstedt, "Model driven security: From uml models to access control infrastructures," *ACM Trans. Softw. Eng. Methodol.*, vol. 15, pp. 39–91, January 2006.

[281] D. Frankel, *Model Driven Architecture: Applying MDA to Enterprise Computing*. New York, NY, USA: John Wiley & Sons, Inc., 2002.

[282] C. Atkinson and T. Kühne, "Model-driven development: A metamodeling foundation," *IEEE Software*, vol. 20, pp. 36–41, September 2003.

[283] M. Clavel, V. Silva, C. Braga, and M. Egea, "Model-driven security in practice: An industrial experience," in *Proceedings of the 4th European conference on Model Driven Architecture: Foundations and Applications*, ECMDA-FA '08, (Berlin, Heidelberg), pp. 326–337, Springer-Verlag, 2008.

[284] E. Yu, "Modeling organizations for information systems requirements engineering," in *Requirements Engineering, 1993., Proceedings of IEEE International Symposium on*, pp. 34 –41, jan 1993.

[285] L. Chung, "Dealing with security requirements during the development of information systems," in *Proceedings of Advanced Information Systems Engineering*, (London, UK), pp. 234–251, Springer-Verlag, 1993.

[286] H. Mouratidis, P. Giorgini, and G. Manson, "Integrating security and systems engineering: towards the modelling of secure information systems," in *Proceedings of the 15th international conference on Advanced information systems engineering*, CAiSE'03, (Berlin, Heidelberg), pp. 63–78, Springer-Verlag, 2003.

[287] E. Letier and A. van Lamsweerde, "Deriving operational software specifications from system goals," *SIGSOFT Softw. Eng. Notes*, vol. 27, pp. 119–128, November 2002.

[288] A. I. Anton and J. B. Earp, "Strategies for developing policies and requirements for secure electronic commerce systems," tech. rep., Raleigh, NC, USA, 2000.

[289] J. D. Moffett and B. A. Nuseibeh, "A Framework for Security Requirements Engineering," Report YCS 368, Department of Computer Science, University of York, 2003.

[290] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "A framework for security requirements engineering," in *Proceedings of the 2006 international workshop on Software engineering for secure systems*, SESS '06, (New York, NY, USA), pp. 35–42, ACM, 2006.

[291] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work*, (Norwell, MA, USA), pp. 77–92, Kluwer Academic Publishers, 1993.

[292] C. Jensen, *Designing for privacy in interactive systems*. PhD thesis, Atlanta, GA, USA, 2005. AAI3198554.

[293] E. Kavakli, C. Kalloniatis, P. Loucopoulos, and S. Gritzalis, "Incorporating privacy requirements into the system design process: The pris conceptual framework," *Internet Research*, vol. 16, pp. 140–158, 2006.

[294] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the pris method," *Requir. Eng.*, vol. 13, pp. 241–255, August 2008.

[295] R. Hebig, C. Meinel, M. Menzel, I. Thomas, and R. Warschofsky, "A web service architecture for decentralised identity- and attribute-based access control," in *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pp. 551–558, July 2009.

[296] Organization for the Advancement of Structured Information Standards (OASIS), "Web services profile of XACML (WS-XACML) version 1.0." `http://www.oasis-open.org/committees/download.php/24951/xacml-3.0-profile-webservices-spec-v1-wd-10-en.pdf`, August 2007. Working Draft 10.

[297] E. Bertino, L. Martino, F. Paci, A. Squicciarini, E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Access control for web services," in *Security for Web Services and Service-Oriented Architectures*, pp. 115–146, Springer Berlin Heidelberg, 2010.

[298] H. Shen, "A semantic-aware attribute-based access control model for web services," in *Algorithms and Architectures for Parallel Processing* (A. Hua and S.-L. Chang, eds.), vol. 5574 of *Lecture Notes in Computer Science*, pp. 693–703, Springer Berlin / Heidelberg, 2009.

[299] T. Dimitrakos, "A service-oriented trust management framework," in *Trust, Reputation, and Security: Theories and Practice* (R. Falcone, S. Barber, L. Korba, and M. Singh, eds.), vol. 2631 of *Lecture Notes in Computer Science*, pp. 53–72, Springer Berlin / Heidelberg, 2003.

[300] L. Olson, M. Winslett, G. Tonti, N. Seeley, A. Uszok, and J. Bradshaw, "Trust negotiation as an authorization service for web services," in *Data Engineering Workshops, 2006. Proceedings. 22nd International Conference on*, pp. 21–21, 2006.

[301] R. Bhatti, E. Bertino, and A. Ghafoor, "A trust-based context-aware access control model for web-services," in *Proceedings of the 2004 IEEE International Conference on Web Services*, pp. 184–191, July 2004.

[302] S. Chakraborty and I. Ray, "Trustbac: integrating trust relationships into the rbac model for access control in open systems," in *SACMAT '06: Proceedings of the 11th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 49–58, ACM, 2006.

[303] M. Mecella, M. Ouzzani, F. Paci, and E. Bertino, "Access control enforcement for conversation-based web services," in *Proceedings of the 15th international conference on World Wide Web*, WWW '06, (New York, NY, USA), pp. 257–266, ACM, 2006.

[304] W. Winsborough and N. Li, "Towards practical automated trust negotiation," in *Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on*, pp. 92 – 103, 2002.

[305] M. Winslett, T. Yu, K. Seamons, A. Hess, J. Jacobson, R. Jarvis, B. Smith, and L. Yu, "Negotiating trust in the web," *IEEE Internet Computing*, vol. 6, pp. 30 – 37, December 2002.

[306] R. Wonohoesodo and Z. Tari, "A role based access control for web services," in *Services Computing, 2004. (SCC 2004). Proceedings. 2004 IEEE International Conference on*, pp. 49 – 56, September 2004.

[307] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pp. 110 – 122, May 2003.

[308] B. Shafiq, J. Joshi, E. Bertino, and A. Ghafoor, "Secure interoperation in a multidomain environment employing rbac policies," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, pp. 1557 – 1577, November 2005.

[309] M. Srivatsa, A. Iyengar, T. Mikalsen, I. Rouvellou, and J. Yin, "An access control system for web service compositions," in *Web Services, 2007. ICWS 2007. IEEE International Conference on*, pp. 1–8, July 2007.

[310] F. Paci, E. Bertino, and J. Crampton, "An access-control framework for ws-bpel," *International Journal of Web Services Research*, vol. 5, pp. 20–43, July 2008.

[311] E. Cohen, R. K. Thomas, W. Winsborough, and D. Shands, "Models for coalition-based access control (cbac)," in *SACMAT '02: Proceedings of the 7th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 97–106, ACM, 2002.

[312] C. Emig, F. Brandt, S. Abeck, J. Biermann, and H. Klarl, "An access control metamodel for web service-oriented architecture," in *Software Engineering Advances, 2007. ICSEA 2007. International Conference on*, pp. 57–57, August 2007.

[313] P. Bonatti, S. De Capitani di Vimercati, and P. Samarati, "An algebra for composing access control policies," *ACM Transactions on Information and System Security*, vol. 5, pp. 1–35, February 2002.

[314] S. Dawson, S. Qian, and P. Samarati, "Providing security and interoperation of heterogeneous systems," *Distributed and Parallel Databases*, vol. 8, pp. 119–145, January 2000.

[315] L. Camarinha-Matos, I. Silveri, H. Afsarmanesh, and A. Oliveira, "Towards a framework for creation of dynamic virtual organizations," in *Collaborative Networks and Their Breeding Environments* (L. Camarinha-Matos, H. Afsarmanesh, and A. Ortiz, eds.), vol. 186 of *IFIP International Federation for Information Processing*, pp. 69–80, Springer Boston, 2005.

[316] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. Lorentey, and F. Spataro, "VOMS, an authorization system for virtual organizations," in *Grid Computing* (F. Fernandez Rivera, M. Bubak, A. Gomez Tato, and R. Doallo, eds.), vol. 2970 of *Lecture Notes in Computer Science*, pp. 33–40, Springer Berlin / Heidelberg, 2004.

[317] F. Kerschbaum and P. Robinson, "Security architecture for virtual organizations of business web services," *Journal of Systems Architecture*, vol. 55, no. 4, pp. 224 – 232, 2009. Secure Service-Oriented Architectures (Special Issue on Secure SOA).

[318] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Deploying security policy in intra and inter workflow management systems," in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, pp. 58–65, March 2009.

[319] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Managing access and flow control requirements in distributed workflows," in *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on*, pp. 702–710, 2008.

[320] F. Cuppens, N. Cuppens-Boulahia, and C. Coma, "O2o: Virtual private organizations to manage security policy interoperability," in *Information Systems Security* (A. Bagchi and V. Atluri, eds.), vol. 4332 of *Lecture Notes in Computer Science*, pp. 101–115, Springer Berlin / Heidelberg, 2006.

[321] W. Winsborough and N. Li, "Safety in automated trust negotiation," in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pp. 147 – 160, May 2004.

[322] A. El Kalam, Y. Deswarte, A. Baina, and M. Kaaniche, "Access control for collaborative systems: A web services based approach," in *Web Services, 2007. ICWS 2007. IEEE International Conference on*, pp. 1064–1071, July 2007.

[323] L. Su, D. Chadwick, A. Basden, and J. Cunningham, "Automated decomposition of access control policies," in *Policies for Distributed Systems and Networks, 2005. Sixth IEEE International Workshop on*, pp. 3 – 13, June 2005.

[324] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H.-C. Wong, "Secret handshakes from pairing-based key agreements," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pp. 180 – 196, May 2003.

[325] D. Lin, P. Rao, E. Bertino, N. Li, and J. Lobo, "Policy decomposition for collaborative access control," in *SACMAT '08: Proceedings of the 13th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 103–112, ACM, 2008.

[326] A. Bandara, E. Lupu, J. Moffett, and A. Russo, "A goal-based approach to policy refinement," in *Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE International Workshop on*, pp. 229 – 239, June 2004.

[327] J. E. Holt, R. W. Bradshaw, K. E. Seamons, and H. Orman, "Hidden credentials," in *Proceedings of the 2003 ACM workshop on Privacy in the electronic society*, WPES '03, (New York, NY, USA), pp. 1–8, ACM, 2003.

[328] R. W. Bradshaw, J. E. Holt, and K. E. Seamons, "Concealing complex policies with hidden credentials," in *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, (New York, NY, USA), pp. 146–157, ACM, 2004.

[329] K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," *IEEE Transactions on Computers*, vol. 55, pp. 1259–1270, October 2006.

[330] A. Bonifati, R. Liu, and H. Wang, "Distributed and secure access control in p2p databases," in *Data and Applications Security and Privacy XXIV* (S. Foresti and S. Jajodia, eds.), vol. 6166 of *Lecture Notes in Computer Science*, pp. 113–129, Springer Berlin / Heidelberg, 2010.

[331] S. Foresti, *Preserving Privacy in Data Outsourcing*. PhD thesis, Universita degli studi di Milano, Milano, 2008. PhD thesis.

[332] A. Singh, M. Srivatsa, and L. Liu, "Search-as-a-service: Outsourced search over outsourced storage," *ACM Transactions on the Web*, vol. 3, pp. 13:1–13:33, September 2009.

[333] P. Mazzoleni, B. Crispo, S. Sivasubramanian, and E. Bertino, "Xacml policy integration algorithms," *ACM Transactions on Information and System Security*, vol. 11, pp. 4:1–4:29, February 2008.

[334] D. W. Chadwick and S. F. Lievens, "Enforcing "sticky" security policies throughout a distributed application," in *Proceedings of the 2008 workshop on Middleware security*, MidSec '08, (New York, NY, USA), pp. 1–6, ACM, 2008.

[335] G. Karjoth, M. Schunter, and M. Waidner, "Platform for enterprise privacy practices: Privacy-enabled management of customer data," in *PET 2002: Proceedings of of the 2nd International Workshop on Privacy Enhancing Technologies* (R. Dingledine and P. Syverson, eds.), vol. 2482 of *Lecture Notes in Computer Science*, pp. 69–84, Springer Berlin / Heidelberg, 2003.

[336] R. Krishnan, R. Sandhu, J. Niu, and W. Winsborough, "Towards a framework for group-centric secure collaboration," in *Collaborative Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on*, pp. 1–10, November 2009.

[337] R. Krishnan, R. Sandhu, J. Niu, and W. H. Winsborough, "Foundations for group-centric secure information sharing models," in *SACMAT '09: Proceedings of the 14th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 115–124, ACM, 2009.

[338] J. Warner, V. Atluri, R. Mukkamala, and J. Vaidya, "Using semantics for automatic enforcement of access control policies among dynamic coalitions," in *SACMAT '07: Proceedings of the 12th ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 235–244, ACM, 2007.

[339] M. Kim, J. B. D. Joshi, and M. Kim, "Access control for cooperation systems based on group situation," in *Collaborative Computing: Networking, Applications and Worksharing* (O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari, M. Gerla, H. Kobayashi, S. Palazzo, S. Sahni, X. S. Shen, M. Stan, J. Xiaohua, A. Zomaya, G. Coulson, E. Bertino, and J. B. D. Joshi, eds.), vol. 10 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 11–23, Springer Berlin Heidelberg, 2009.

[340] J. Crampton and H. Khambhammettu, "Delegation in role-based access control," *International Journal of Information Security*, vol. 7, pp. 123–136, 2008.

[341] D.-G. Park and Y.-R. Lee, "A flexible role-based delegation model using characteristics of permissions," in *Database and Expert Systems Applications* (K. V. Andersen, J. Debenham, and R. Wagner, eds.), vol. 3588 of *Lecture Notes in Computer Science*, pp. 310–323, Springer Berlin / Heidelberg, 2005.

[342] W. Qiu and C. Adams, "Exploring user-to-role delegation in role-based access control," in *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the*, pp. 21–21, July 2007.

[343] M. Ben-Ghorbel-Talbi, F. Cuppens, N. Cuppens-Boulahia, and A. Bouhoula, "A delegation model for extended rbac," *International Journal of Information Security*, vol. 9, pp. 209–236, 2010.

[344] D. Chadwick, S. Otenko, and T. Nguyen, "Adding support to xacml for multi-domain user to user dynamic delegation of authority," *International Journal of Information Security*, vol. 8, pp. 137–152, 2009.

[345] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (R. Meersman, Z. Tari, and P. Herrero, eds.), vol. 4278 of *Lecture Notes in Computer Science*, pp. 1734–1744, Springer Berlin / Heidelberg, 2006.

[346] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," *ACM Transactions on Information and System Security*, vol. 13, pp. 6:1–6:38, November 2009.

[347] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: social access control for web 2.0," in *Proceedings of the first workshop on Online social networks*, WOSP '08, (New York, NY, USA), pp. 43–48, ACM, 2008.

[348] B. Ali, W. Villegas, and M. Maheswaran, "A trust based approach for protecting user data in social networks," in *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, CASCON '07, (New York, NY, USA), pp. 288–293, ACM, 2007.

[349] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP '07. IEEE Symposium on*, pp. 321–334, May 2007.

[350] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A semantic web based framework for social network access control," in *SACMAT '09: Proceedings of the 14th ACM symposium on Access control models and technologies*, pp. 177–186, ACM, 2009.

[351] N. Elahi, M. Chowdhury, and J. Noll, "Semantic access control in web based communities," in *ICCGI 2008: Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology*, pp. 131–136, IEEE Computer Society, August 2008.

[352] B. Carminati and E. Ferrari, "Privacy-aware collaborative access control in web-based social networks," in *Data and Applications Security XXII* (V. Atluri, ed.), vol. 5094 of *Lecture Notes in Computer Science*, pp. 81–96, Springer Berlin / Heidelberg, 2008.

[353] B. Carminati, E. Ferrari, and P. A., "A decentralized security framework for web-based social networks," *International Journal of Information Security and Privacy,*, vol. 2, no. 4, pp. 22 – 53, 2008.

[354] B. Carminati and E. Ferrari, "Enforcing relationships privacy through collaborative access control in web-based social networks," in *Collaborative Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on*, pp. 1–9, November 2009.

[355] J. Domingo-Ferrer, A. Viejo, F. Sebé, and ı. González-Nicolás, "Privacy homomorphisms for social networks with private relationships," *Computer Networks*, vol. 52, pp. 3007–3016, October 2008.

[356] G. Mezzour, A. Perrig, V. Gligor, and P. Papadimitratos, "Privacy-preserving relationship path discovery in social networks," in *Proceedings of the 8th International Conference on Cryptology and Network Security*, CANS '09, (Berlin, Heidelberg), pp. 189–208, Springer-Verlag, 2009.

[357] B. Alhaqbani and C. Fidge, "Access control requirements for processing electronic health records," in *Proceedings of the 2007 international conference on Business process management*, BPM'07, (Berlin, Heidelberg), pp. 371–382, Springer-Verlag, 2008.

[358] B. Alhaqbani, M. Adams, C. Fidge, and A. Hofstede, "Privacy-Aware Workflow Management," in *Business Process Management* (M. Glykas, ed.), vol. 444 of *Studies in Computational Intelligence*, pp. 111–128, Springer, 2013.

[359] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Managing access and flow control requirements in distributed workflows," in *Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on*, pp. 702–710, April 2008.

[360] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Deploying security policy in intra and inter workflow management systems," *Reliability and Security, International Conference on Availability*, pp. 58–65, 2009.

[361] K. Namiri and N. Stojanovic, "Pattern-based design and validation of business process compliance," in *Proceedings of the 2007 OTM Confederated international conference on On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA, and IS - Volume Part I*, OTM'07, (Berlin, Heidelberg), pp. 59–76, Springer-Verlag, 2007.

[362] S. Sadiq, G. Governatori, and K. Namiri, "Modeling control objectives for business process compliance," in *Proceedings of the 5th international conference on Business process management*, BPM'07, (Berlin, Heidelberg), pp. 149–164, Springer-Verlag, 2007.

[363] C. Wolter and A. Schaad, "Modeling of Task-Based Authorization Constraints in BPMN," in *Business Process Management* (G. Alonso, P. Dadam, and M. Rosemann, eds.), vol. 4714 of *Lecture Notes in Computer Science*, pp. 64–79, Springer Berlin / Heidelberg, 2007.

[364] M. Alam, M. Hafner, and R. Breu, "Constraint based role based access control in the sectet-framework: A model-driven approach," *Journal of Computer Security*, vol. 16, no. 2, pp. 223–260, 2008.

[365] C. Wolter, M. Menzel, and C. Meinel, "Modelling security goals in business processes," in *Modellierung*, pp. 197–212, 2008.

[366] M. Menzel, C. Wolter, and C. Meinel, "Towards the aggregation of security requirements in cross-organisational service compositions," in *Business Information Systems* (W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, C. Szyperski, W. Abramowicz, and D. Fensel, eds.), vol. 7 of *Lecture Notes in Business Information Processing*, pp. 297–308, Springer Berlin Heidelberg, 2008.

[367] C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel, "Model-driven business process security requirement specification," *J. Syst. Archit.*, vol. 55, pp. 211–223, April 2009.

[368] M. Schnjakin, M. Menzel, and C. Meinel, "A pattern-driven security advisor for service-oriented architectures," in *Proceedings of the 2009 ACM workshop on Secure web services*, SWS '09, pp. 13–20, ACM, 2009.

[369] M. Wolf, I. Thomas, M. Menzel, and C. Meinel, "A message meta model for federated authentication in service-oriented architectures," in *Service-Oriented Computing and Applications (SOCA), 2009 IEEE International Conference on*, pp. 1–8, January 2009.

[370] M. Menzel and C. Meinel, "A security meta-model for service-oriented architectures," *IEEE International Conference on Services Computing*, pp. 251–259, 2009.

[371] R. N. Hebig, C. Meinel, M. Menzel, I. Thomas, and R. Warschofsky, "A web service architecture for decentralised identity- and attribute-based access control," *IEEE International Conference on Web Services*, pp. 551–558, 2009.

[372] M. Menzel, I. Thomas, and C. Meinel, "Security requirements specification in service-oriented business process management," *International Conference on Availability, Reliability and Security*, pp. 41–48, 2009.

[373] M. Menzel, R. Warschofsky, I. Thomas, C. Willems, and C. Meinel, "The service security lab: A model-driven platform to compose and explore service security in the cloud," in *2010 6th World Congress on Services (SERVICES-1)*, pp. 115–122, July 2010.

[374] M. Menzel and C. Meinel, "SecureSOA," *IEEE International Conference on Services Computing*, pp. 146–153, 2010.

[375] M. Menzel, R. Warschofsky, and C. Meinel, "A pattern-driven generation of security policies for service-oriented architectures," *IEEE International Conference on Web Services*, pp. 243–250, 2010.

[376] W. M. P. v. d. Aalst, "Workflow verification: Finding control-flow errors using petri-net-based techniques," in *Business Process Management, Models, Techniques, and Empirical Studies*, (London, UK), pp. 161–183, Springer-Verlag, 2000.

[377] W. M. P. v. d. Aalst, A. Hirnschall, and H. M. W. E. Verbeek, "An alternative way to analyze workflow graphs," in *Proceedings of the 14th International Conference on Advanced Information Systems Engineering*, CAiSE '02, (London, UK, UK), pp. 535–552, Springer-Verlag, 2002.

[378] S. Sadiq, M. Orlowska, W. Sadiq, and C. Foulger, "Data flow and validation in workflow modelling," in *Proceedings of the 15th Australasian Database Conference - Volume 27*, ADC '04, (Darlinghurst, Australia, Australia), pp. 207–214, Australian Computer Society, Inc., 2004.

[379] W. Sadiq and M. E. Orlowska, "Applying graph reduction techniques for identifying structural conflicts in process models," in *Proceedings of the 11th International Conference on Advanced Information Systems Engineering*, CAiSE '99, (London, UK), pp. 195–209, Springer-Verlag, 1999.

[380] S. Perumal and A. Mahanti, "A graph-search based algorithm for verifying workflow graphs," *Database and Expert Systems Applications, International Workshop on*, vol. 0, pp. 992–996, 2005.

[381] H. S. Meda, A. K. Sen, and A. Bagchi, "On detecting data flow errors in workflows," *Journal of Data and Information Quality*, vol. 2, pp. 4:1–4:31, July 2010.

[382] E. Verbeek and W. M. P. van der Aalst, "Woflan 2.0: a petri-net-based workflow diagnosis tool," in *Proceedings of the 21st international conference on Application and theory of petri nets*, ICATPN'00, (Berlin, Heidelberg), pp. 475–484, Springer-Verlag, 2000.

[383] C. Ouyang, E. Verbeek, W. M. P. van der Aalst, S. Breutel, M. Dumas, and A. H. M. ter Hofstede, "Formal semantics and analysis of control flow in ws-bpel," *Sci. Comput. Program.*, vol. 67, pp. 162–198, July 2007.

[384] W. van der Aalst, K. van Hee, A. ter Hofstede, N. Sidorova, H. Verbeek, M. Voorhoeve, and M. Wynn, "Soundness of workflow nets:classification, decidability, and analysis," tech. rep., BPMcenter.org, 2008.

[385] N. Trčka, W. M. Aalst, and N. Sidorova, "Data-flow anti-patterns: Discovering data-flow errors in workflows," in *Proceedings of the 21st International Conference on Advanced Information Systems Engineering*, CAiSE '09, (Berlin, Heidelberg), pp. 425–439, Springer-Verlag, 2009.

[386] H. Zha, W. van der Aalst, J. Wang, L. Wen, and J. Sun, "Verifying workflow processes: a transformation-based approach," *Software and Systems Modeling*, vol. 10, pp. 253–264, 2011.

[387] C. Cabanillas, M. Resinas, A. Ruiz-Cortés, and A. Awad, "Automatic generation of a data-centered view of business processes," in *Proceedings of the 23rd international conference on Advanced information systems engineering*, CAiSE'11, (Berlin, Heidelberg), pp. 352–366, Springer-Verlag, 2011.

[388] W. van der Aalst, H. de Beer, and B. van Dongen, "Process mining and verification of properties: An approach based on temporal logic," in *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE* (R. Meersman and Z. Tari, eds.), vol. 3760 of *Lecture Notes in Computer Science*, pp. 130–147, Springer Berlin / Heidelberg, 2005.

[389] R. Lu, S. Sadiq, and G. Governatori, "Compliance aware business process design," in *Proceedings of the 2007 international conference on Business process management*, BPM'07, (Berlin, Heidelberg), pp. 120–131, Springer-Verlag, 2008.

[390] S. Goedertier and J. Vanthienen, "Designing compliant business processes with obligations and permissions," in *Business Process Management Workshops* (J. Eder and S. Dustdar, eds.), vol. 4103 of *Lecture Notes in Computer Science*, pp. 5–14, Springer Berlin / Heidelberg, 2006.

[391] G. Governatori, Z. Milosevic, and S. Sadiq, "Compliance checking between business processes and business contracts," in *Enterprise Distributed Object Computing Conference, 2006. EDOC '06. 10th IEEE International*, pp. 221–232, oct. 2006.

[392] Y. Liu, S. Müller, and K. Xu, "A static compliance-checking framework for business process models," *IBM Systems Journal*, vol. 46, pp. 335–361, April 2007.

[393] J. Yu, T. Manh, J. Han, Y. Jin, Y. Han, and J. Wang, "Pattern based property specification and verification for service composition," in *Web Information Systems – WISE 2006* (K. Aberer, Z. Peng, E. Rundensteiner, Y. Zhang, and X. Li, eds.), vol. 4255 of *Lecture Notes in Computer Science*, pp. 156–168, Springer Berlin / Heidelberg, 2006.

[394] R. Eshuis and R. Wieringa, "Tool support for verifying uml activity diagrams," *Software Engineering, IEEE Transactions on*, vol. 30, pp. 437 – 447, july 2004.

[395] R. Eshuis, "Symbolic model checking of uml activity diagrams," *ACM Trans. Softw. Eng. Methodol.*, vol. 15, pp. 1–38, January 2006.

[396] J. Zdravkovic and V. Kabilan, "Enabling business process interoperability using contract workflow models," in *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE* (R. Meersman and Z. Tari, eds.), vol. 3760 of *Lecture Notes in Computer Science*, pp. 77–93, Springer Berlin / Heidelberg, 2005.

[397] S. Short and S. P. Kaluvuri, "A data-centric approach for privacy-aware business process enablement," in *Enterprise Interoperability* (M. Sinderen, P. Johnson, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, C. Szyperski, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 76 of *Lecture Notes in Business Information Processing*, pp. 191–203, Springer Berlin Heidelberg, 2011.

[398] P. Senkul and I. H. Toroslu, "An architecture for workflow scheduling under resource allocation constraints," *Inf. Syst.*, vol. 30, pp. 399–422, July 2005.

[399] A. Awad and M. Weske, "Visualization of Compliance Violation in Business Process Models," in *Business Process Management Workshops* (S. Rinderle-Ma, S. Sadiq, F. Leymann, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 43 of *Lecture Notes in Business Information Processing*, pp. 182–193, Springer Berlin Heidelberg, 2010.

[400] A. Awad, G. Decker, and M. Weske, "Efficient compliance checking using bpmn-q and temporal logic," in *Proceedings of the 6th International Conference on Business Process Management*, BPM '08, (Berlin, Heidelberg), pp. 326–341, Springer-Verlag, 2008.

[401] A. Awad, M. Weidlich, and M. Weske, "Specification, Verification and Explanation of Violation for Data Aware Compliance Rules," in *Proceedings of the 7th International Joint Conference on Service-Oriented Computing*, ICSOC-ServiceWave '09, (Berlin, Heidelberg), pp. 500–515, Springer-Verlag, 2009.

[402] A. Awad, M. Weidlich, and M. Weske, "Visually specifying compliance rules and explaining their violations for business processes," *Journal ofVisualLanguagesandComputing*, vol. 22, pp. 30–55, February 2011.

[403] G. Governatori, J. Hoffmann, S. Sadiq, and I. Weber, "Detecting regulatory compliance for business process models through semantic annotations," in *Business Process Management Workshops* (D. Ardagna, M. Mecella, J. Yang, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 17 of *Lecture Notes in Business Information Processing*, pp. 5–17, Springer Berlin Heidelberg, 2009.

[404] F. Rabbi, H. Wang, and W. MacCaull, "Yawl2dve: An automated translator for workflow verification," in *Secure Software Integration and Reliability Improvement (SSIRI), 2010 Fourth International Conference on*, pp. 53 –59, june 2010.

[405] N. Leyla, A. S. Mashiyat, H. Wang, and W. MacCaull, "Towards workflow verification," in *Proceedings of the 2010 Conference of the Center for Advanced Studies on Collaborative Research*, CASCON '10, (Riverton, NJ, USA), pp. 253–267, IBM Corp., 2010.

[406] J. Dallien, W. MacCaull, and A. Tien, "Initial work in the design and development of verifiable workflow management systems and some applications to health care," in *Proceedings of the 2008 5th International Workshop on Model-based Methodologies for Pervasive and Embedded Software*, (Washington, DC, USA), pp. 78–91, IEEE Computer Society, 2008.

[407] A. Schaad, V. Lotz, and K. Sohr, "A model-checking approach to analysing organisational controls in a loan origination process," in *Proceedings of the eleventh ACM symposium on Access control models and technologies*, SACMAT '06, (New York, NY, USA), pp. 139–149, ACM, 2006.

[408] A. Dury, S. Boroday, A. Petrenko, and V. Lotz, "Formal verification of business workflows and role based access control systems," *Emerging Security Information, Systems, and Technologies, The International Conference on*, pp. 201–210, 2007.

[409] R. Lu, S. Sadiq, and G. Governatori, "Measurement of compliance distance in business processes," *Inf. Sys. Manag.*, vol. 25, pp. 344–355, October 2008.

[410] J. Chen and Y. Yang, "A taxonomy of grid workflow verification and validation," *Concurr. Comput. : Pract. Exper.*, vol. 20, pp. 347–360, March 2008.

[411] S. Witt, S. Feja, A. Speck, and C. Prietz, "Integrated privacy modeling and validation for business process models," in *Proceedings of the 2012 Joint EDBT/ICDT Workshops*, EDBT-ICDT '12, (New York, NY, USA), pp. 196–205, ACM, 2012.

[412] R. Müller, U. Greiner, and E. Rahm, "Agent work: a workflow system supporting rule-based workflow adaptation," *Data Knowl. Eng.*, vol. 51, pp. 223–256, November 2004.

[413] I. Vanderfeesten, H. A. Reijers, and W. M. P. Aalst, "Case handling systems as product based workflow design support," in *Enterprise Information Systems* (J. Filipe, J. Cordeiro, J. Cardoso, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 12 of *Lecture Notes in Business Information Processing*, pp. 187–198, Springer Berlin Heidelberg, 2009.

[414] W. M. P. van der Aalst and M. Weske, "Case handling: a new paradigm for business process support," *Data Knowl. Eng.*, vol. 53, pp. 129–162, May 2005.

[415] R. Lu, S. Sadiq, G. Governatori, and X. Yang, "Defining adaptation constraints for business process variants," in *Business Information Systems* (W. Abramowicz, W. Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 21 of *Lecture Notes in Business Information Processing*, pp. 145–156, Springer Berlin Heidelberg, 2009.

[416] A. Antonakopoulou, G. V. Lioudakis, F. Gogoulos, D. I. Kaklamani, and I. S. Venieris, "Leveraging access control for privacy protection: A survey," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (G. Yee, ed.), IGI Global, 2011.

[417] R. A. Botha and J. H. P. Eloff, "Separation of duties for access control enforcement in workflow environments," *IBM Systems Journal*, vol. 40, pp. 666–682, March 2001.

[418] F. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "Privacy-aware access control and authorization in passive network monitoring infrastructures," in *CIT 2010: Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, 2010.

[419] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, F. Cuppens, and N. Cuppens-Boulahia, "A Privacy-Aware Access Control Model for Distributed Network Monitoring," *Computers & Electrical Engineering*, vol. 39, pp. 2263–2281, October 2013.

[420] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, and I. S. Venieris, "A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress," in *Proceedings of the 4th MITACS Workshop on Foundations & Practice of Security (FPS 2011)* (J. Garcia-Alfaro and P. Lafourcade, eds.), vol. 6888 of *Lecture Notes in Computer Science*, pp. 208–217, Springer Berlin / Heidelberg, 2012.

[421] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, N. Cuppens-Boulahia, and F. Cuppens, "Leveraging Ontologies upon a Holistic Privacy-aware Access Control Model," in *Proceedings of the 6th International Symposium on Foundations & Practice of Security (FPS 2013)*, vol. 8352 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2013. (in press).

[422] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Leveraging Semantic Web Technologies for Access Control," in *Emerging Trends in Information and Communication Technologies Security* (B. Akhgar and H. Arabnia, eds.), pp. 493–506, Morgan Kaufmann, 2014.

[423] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Workflows: Challenges and Requirements," in *Proceedings of the 1st International Conference on Information and Communication Technologies and Law (ICT LAW 2013)* (I. Portela, P. Gonçalves, M. M. Cruz Cunha, and V. Carvalho, eds.), Cambridge Scholars, 2013.

[424] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy Compliance Requirements in Workflow Environments," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (M. M. Cruz Cunha, ed.), IGI Global, 2014.

[425] E. Yuan and J. Tong, "Attributed based access control (abac) for web services," in *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*, pp. –569, 2005.

[426] J. F. Allen, "Towards a general theory of action and time," *Artif. Intell.*, vol. 23, pp. 123–154, July 1984.

[427] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "An Ontology-Based Approach towards Comprehensive Workflow Modelling," *IET Software*, 2013. (to appear).

[428] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, "Handbook for computer security incident response teams (CSIRTs)," Tech. Rep. CMU/SEI-2003-HB-002, Carnegie Mellon University, Software Engineering Institute, 2003.

[429] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "A workflow checking approach for inherent privacy awareness in network monitoring," in *Proceedings of the 6th International Workshop on Data Privacy Management (DPM 2011)* (J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. De Capitani di Vimercati, eds.), vol. 7122 of *Lecture Notes in Computer Science*, pp. 295–302, Springer Berlin / Heidelberg, 2012.

[430] M. Weske, *Business Process Management: Concepts, Languages, Architectures*. Springer, Berlin Heidelberg, 2nd ed., 2012.

[431] F. Touré, K. Baïna, and K. Benali, "An efficient algorithm for workflow graph structural verification," in *On the Move to Meaningful Internet Systems: OTM 2008* (R. Meersman and Z. Tari, eds.), vol. 5331 of *Lecture Notes in Computer Science*, pp. 392–408, Springer Berlin Heidelberg, 2008.

[432] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. The MIT Press, third ed., 2009.

[433] S. Perumal and A. Mahanti, "Formal foundation of workflow hyperpaths and a graph search algorithm for workflow hyperpath generation," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, jan. 2008.

[434] M. Rosa, M. Dumas, R. Uba, and R. Dijkman, "Merging business process models," in *On the Move to Meaningful Internet Systems: OTM 2010* (R. Meersman, T. Dillon, and P. Herrero, eds.), vol. 6426 of *Lecture Notes in Computer Science*, pp. 96–113, Springer Berlin Heidelberg, 2010.

[435] M. La Rosa, M. Dumas, R. Uba, and R. Dijkman, "Business process model merging: An approach to business process consolidation," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 22, pp. 11:1–11:42, Mar. 2013.

[436] The World Wide Web Consortium (W3C), "Extensible Markup Language (XML) 1.0 (Fifth Edition)." `http://www.w3.org/TR/2008/REC-xml-20081126/`, November 2008. W3C Recommendation.

[437] H. Schonenberg, R. Mans, N. Russell, N. Mulyar, and W. M. P. van der Aalst, "Process Flexibility: A Survey of Contemporary Approaches," in *Advances in Enterprise Engineering I* (J. L. G. Dietz, A. Albani, J. Barjis, W. M. P. van der Aalst, J. Mylopoulos, M. Rosemann, M. J. Shaw, and C. Szyperski, eds.), vol. 10 of *Lecture Notes in Business Information Processing*, pp. 16–30, Springer Berlin / Heidelberg, 2008.

[438] S. Tartir, I. B. Arpinar, M. Moore, A. P. Sheth, and B. Aleman-meza, "OntoQA: Metric-based ontology quality analysis," in *Proceedings of the 2005 IEEE Workshop on Knowledge Acquisition from Distributed, Autonomous, Semantically Heterogeneous Data and Knowledge Sources (KADASH)*, pp. 45–53, IEEE Computer Society, November 2005.

[439] S. Tartir, I. Arpinar, and A. Sheth, "Ontological evaluation and validation," in *Theory and Applications of Ontology: Computer Applications* (R. Poli, M. Healy, and A. Kameas, eds.), pp. 115–130, Springer Netherlands, 2010.

[440] H. Zhang, Y.-F. Li, and H. B. K. Tan, "Measuring design complexity of semantic web ontologies," *Journal of Systems and Software*, vol. 83, pp. 803–814, May 2010.

[441] United States Senate and House of Representatives in Congress, "Sarbanes-Oxley Act of 2002," 2002. Public Law 107-204 (116 Statute 745).

[442] Basel Committee on Banking Supervision, "Basel III International regulatory framework for banks." `http://www.bis.org/bcbs/basel3.htm`.

[443] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*. The Fairmont Press, 2009.

[444] European Commission, "Smart Grids: from Innovation to Deployment," April 2011. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 202.

Δημοσιεύσεις

Διεθνή Επιστημονικά Περιοδικά

[1] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "An Ontology-Based Approach towards Comprehensive Workflow Modelling," *IET Software*, 2013. (to appear).

[2] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, F. Cuppens, and N. Cuppens-Boulahia, "A Privacy-Aware Access Control Model for Distributed Network Monitoring," *Computers & Electrical Engineering*, vol. 39, pp. 2263–2281, October 2013.

Κεφάλαια Βιβλίων

[3] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Leveraging Semantic Web Technologies for Access Control," in *Emerging Trends in Information and Communication Technologies Security* (B. Akhgar and H. Arabnia, eds.), pp. 493–506, Morgan Kaufmann, 2014.

[4] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy Compliance Requirements in Workflow Environments," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (M. M. Cruz Cunha, ed.), IGI Global, 2014.

Πρακτικά Διεθνών Επιστημονικών Συνεδρίων

[5] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Workflows: Challenges and Requirements," in *Proceedings of the 1st International Conference on Information and Communication Technologies and Law (ICT LAW 2013)* (I. Portela, P. Gonçalves, M. M. Cruz Cunha, and V. Carvalho, eds.), Cambridge Scholars, 2013.

[6] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, N. Cuppens-Boulahia, and F. Cuppens, "Leveraging Ontologies upon a Holistic Privacy-aware Access Control Model," in *Proceedings of the 6th International Symposium on Foundations & Practice of Security (FPS 2013)*, vol. 8352 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2013. (in press).

[7] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "A Workflow Checking Approach for Inherent Privacy Awareness in Network Monitoring," in *Proceedings of the 6th International Workshop on Data Privacy Management (DPM 2011)* (J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. De Capitani di Vimercati, eds.), vol. 7122 of *Lecture Notes in Computer Science*, pp. 295–302, Springer Berlin / Heidelberg, 2012.

[8] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, and I. S. Venieris, "A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress," in *Proceedings of the 4th MITACS Workshop on Foundations & Practice of Security (FPS 2011)* (J. Garcia-Alfaro and P. Lafourcade, eds.), vol. 6888 of *Lecture Notes in Computer Science*, pp. 208–217, Springer Berlin / Heidelberg, 2012.

[9] S. Rao, G. Bianchi, J. Garcia-Alfaro, F. Romero, B. Trammell, A. Berger, G. V. Lioudakis, E. I. Papagianakopoulou, M. N. Koukovini, and K. Mittig, "System Architecture for Collaborative Security and Privacy Monitoring in Multi-Domain Networks," in *Proceedings of the 3rd IEEE Workshop on Collaborative Security Technologies (CoSec 2011)*, IEEE Press, 2011.

Δημοσιεύσεις υπό Κρίση

[10] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Workflow Modeling Technologies," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

[11] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Access Control," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

Συνοπτικό Βιογραφικό Σημείωμα

Η κ. Μαρία Ν. Κουκοβίνη γεννήθηκε στην Αθήνα το 1984. Αποφοίτησε από το Ενιαίο Λύκειο Αμφιλοχίας το 2001, με βαθμό «Άριστα». Το ίδιο έτος εισήχθη πρώτη σε σειρά κατάταξης στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΕΜΠ, απ' όπου και αποφοίτησε το 2007 με γενικό βαθμό «Λίαν καλώς» (7,94/10). Το 2008 έγινε δεκτή ως υποψήφια διδάκτορας της ίδιας σχολής, ενώ το 2010 της χορηγήθηκε υποτροφία από το Υπουργείο Παιδείας και Θρησκευμάτων, στο πλαίσιο του Προγράμματος «Ηράκλειτος ΙΙ». Κατά την ερευνητική της εργασία μελέτησε, σχεδίασε και ανέπτυξε πρωτότυπο σύστημα για την εγγενή ενσωμάτωση μηχανισμών προστασίας της ιδιωτικότητας σε συστήματα λογισμικού προσανατολισμένου σε υπηρεσίες.

Η κ. Κουκοβίνη, κατά τη διάρκεια των μεταπτυχιακών της σπουδών, έλαβε μέρος σε διεθνή συνέδρια, στα οποία παρουσίασε το ερευνητικό της έργο και δημοσίευσε τις εργασίες της στα πρακτικά τους. Παράλληλα, έχει δημοσιεύσει εργασίες της σε συλλογικούς τόμους, καθώς και στα διεθνώς αναγνωρισμένα επιστημονικά περιοδικά Software (IET) και Computer & Electrical Engineering (Elsevier). Επιπλέον, έχει συνεισφέρει στις δραστηριότητες προτυποποίησης του οργανισμού European Telecommunications Standards Institute (ETSI), μέσω της συμμετοχής της στις ομάδες εργασίας Measurement Ontology for IP traffic (MOI) και Identity and access management for Networks and Services (INS).

Η κ. Κουκοβίνη έχει εργασθεί στον ιδιωτικό τομέα ως Μηχανικός Λογισμικού, συμμετέχοντας σε πληθώρα αναπτυξιακών έργων, και είναι μέλος του Τεχνικού Επιμελητηρίου Ελλάδος (Τ.Ε.Ε.).