ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Πρακτικές και Μεθοδολογίες Ελέγχου Διαλειτουργικότητας και Ιδιωτικότητας: Εφαρμογές σε Προηγμένες και Ασφαλείς Ηλεκτρονικές και Κινητές Υπηρεσίες»

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Υποβλήθηκε στο Τμήμα Πληροφορικής

του

Πανεπιστημίου Πειραιώς

Σπυρίδων Παπαστεργίου

ΠΕΙΡΑΙΑΣ, Ιούλιος 2009

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Πρακτικές και Μεθοδολογίες Ελέγχου Διαλειτουργικότητας και Ιδιωτικότητας: Εφαρμογές σε Προηγμένες και Ασφαλείς Ηλεκτρονικές και Κινητές Υπηρεσίες»

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Σπυρίδων Παπαστεργίου

Συμβουλευτική Επιτροπή : Δέσποινα Πολέμη
Χρήστος Δουληγέρης
Βασίλης Χρυσικόπουλος

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 13η Ιουλίου 2009.

..... Δέσποινα Πολέμη Επίκουρος Καθηγητής Πανεπιστημίου Πειραιά	..... Χρήστος Δουληγέρης Καθηγητής Πανεπιστημίου Πειραιά	..... Βασίλης Χρυσικόπουλος Καθηγητής Ιονίου Πανεπιστημίου
..... Νίκος Αλεξανδρής Καθηγητής Πανεπιστημίου Πειραιά	..... Μιλτιάδης Αναγνώστου Καθηγητής ΕΜΠ	..... Κώστας Λαμπρινουδάκης Επίκουρος Καθηγητής Πανεπιστημίου Πειραιά
	..... Άγγελος Πικράκης Λέκτορας Πανεπιστημίου Πειραιά	

Πειραιάς, Ιούλιος 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Αφιερώνεται στους γονείς μου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

.....
Σπυρίδων Παπαστεργίου

Διδάκτωρ Πανεπιστημίου Πειραιώς

Copyright © Σπυρίδων Παπαστεργίου, 2009
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

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

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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Ευχαριστίες

Αρχικά θα ήθελα να εκφράσω ένα μεγάλο ευχαριστώ στην επιβλέπουσα καθηγήτρια μου κ. Δέσποινα Πολέμη για την καθοδήγηση και το ενδιαφέρον της καθώς επίσης και για την τεράστια υπομονή και την υποστήριξή της. Επίσης ευχαριστώ τους καθηγητές κ. Χρήστο Δουληγέρη, Νικόλαο Αλεξανδρή και Βασίλη Χρυσικόπουλο για τις πολύτιμες συμβουλές τους καθ' όλη την διάρκεια της διατριβής. Οι παρατηρήσεις και τα σχόλια τους καθόρισαν σε πολύ μεγάλο βαθμό την αρτιότητα της διατριβής και με βοήθησαν να την βελτιώνω συνέχεια μέχρι την τελική μορφή της.

Θα ήθελα επίσης να ευχαριστήσω την Γενική Γραμματεία Έρευνας και Τεχνολογίας (ΓΓΕΤ) η οποία μέσω του προγράμματος ΠΕΝΕΔ 2003 χρηματοδότησε τη διδακτορική μου έρευνα συμβάλλοντας σε μεγάλο βαθμό στην επιτυχή ολοκλήρωση της.

Κατά την εκπόνηση της διατριβής υπήρξαν αρκετοί φίλοι και συνάδελφοι που με στήριξαν σε δύσκολες στιγμές. Ο Αλέξανδρος Καλιοντζόγλου και ο Αθανάσιος Καραντζιάς (και οι δύο διδάκτορες ΕΜΠ) ήταν από εκείνους τους ανθρώπους που βρίσκονταν από την αρχή στο πλευρό μου τόσο για να μου δώσουν συμβουλές για την διατριβή αλλά κυρίως ως φίλοι για να με βοηθήσουν με όποιο τρόπο μπορούσαν. Θα ήθελα να τους ευχαριστήσω ολόψυχα για τη συμπαράσταση και την υποστήριξή τους.

Επίσης, ένα μεγάλο ευχαριστώ θα ήθελα να εκφράσω και προς τους καλούς μου φίλους Παναγιώτη Πουλόγιαννη, Χαράλαμπο Σαββίδη και Κωνσταντίνο Λιντοβόη για την συμπαράσταση τους. Ήταν οι άνθρωποι με τους οποίους μπορούσα να μοιραστώ τις ανησυχίες, τις σκέψεις και τους προβληματισμούς μου.

Επίσης θέλω να ευχαριστήσω τους νέους φίλους και συνεργάτες Γιώργο Βάλβη, Βασίλη Μενεκλή, Γιώργο Πενταφρόνυμο και Θεωδωρή Ντούσκα για τις ιδέες και το ενδιαφέρον τους. Ελπίζω η φιλία μας να συνεχίσει και να βάλω και γω ένα λιθαράκι στην ολοκλήρωση των μεταπτυχιακών σπουδών τους.

Τέλος, ευχαριστώ την οικογένειά μου. Έχει παίξει ίσως τον σημαντικότερο ρόλο στο να μάθω να θέτω και να πραγματοποιώ στόχους στη ζωή μου και να προσπαθώ να βελτιώνομαι όσο μπορώ. Ελπίζω να τους έχω κάνει περήφανους.

Σπύρος Παπαστεργίου
Πειραιάς, Ιούλιος 2009

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Περιεχόμενα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

1 Εισαγωγή

Η επικρατούσα τάση της σύγχρονης ψηφιακής εποχής οδηγεί στη σχεδίαση και ανάπτυξη εφαρμογών, αρχιτεκτονικών και υπηρεσιών οι οποίες βασίζονται σε τεχνολογίες XML (Extensible Markup Language) [XML] και σε πρότυπα Υπηρεσιών Ιστού (Web Services). Η υιοθέτηση των συγκεκριμένων τεχνολογιών και προτύπων προσφέρει ένα συστηματικό και προτυποποιημένο τρόπο ευέλικτης αναπαράστασης των ψηφιακών δεδομένων και ανταλλαγής αυτών μεταξύ των πληροφοριακών και επικοινωνιακών συστημάτων.

Στην επιστημονική όσο και στην επιχειρηματική κοινότητα ο όρος *Υπηρεσίες Ιστού* χρησιμοποιείται για την περιγραφή δύο βασικών εννοιών [Kreger01, Booth04]. Η πρώτη αναφέρεται στα πρότυπα που χρησιμοποιούνται για την υλοποίηση ενός συνόλου επιχειρησιακών διαδικασιών, ενώ η δεύτερη συνδέεται με την αναπαράσταση των προσφερόμενων διαθέσιμων λειτουργιών στο πλαίσιο ενός δικτύου συστημάτων.

Τα τελευταία χρόνια το ερευνητικό ενδιαφέρον έχει εστιαστεί στην αναζήτηση αλλά και εφαρμογή των απαιτούμενων μηχανισμών που θα προσδώσουν στις Υπηρεσίες Ιστού τα απαραίτητα χαρακτηριστικά ασφάλειας, οδηγώντας παράλληλα στην ανάπτυξη και παροχή πιο κρίσιμων λειτουργιών. Ο συνδυασμός υποδομών όπως, είναι οι Υποδομές Δημοσίου Κλειδιού [Adams99], με τις Υπηρεσίες Ιστού λειτούργησε ως καταλύτης για την δημιουργία ενός ασφαλούς ηλεκτρονικού και κινητού περιβάλλοντος. Η υποστήριξη ενός ασφαλούς περιβάλλοντος επέβαλε την ανάπτυξη και τελικώς την υιοθέτηση προτύπων και προδιαγραφών όπως είναι η Κρυπτογράφηση XML [Naedele], οι Προηγμένες XML Ψηφιακές Υπογραφές (XAdES) [ETSI101733, XAdES02] και η Ασφάλεια Υπηρεσιών Ιστού [Hartman03] οι οποίες προσφέρουν το απαιτούμενο επίπεδο ασφάλειας στα σύγχρονα πληροφοριακά συστήματα.

Αξιοσημείωτα παραδείγματα τέτοιου είδους συστημάτων συναντώνται σε πολλούς τομείς του σύγχρονου ψηφιακού κόσμου όπως είναι στο ηλεκτρονικό/κινητό-εμπόριο [Polemi06a, Polemi06b], στην η/κ-διακυβέρνηση [Karantjias07a, Papastergiou08a, Kaliontzoglou06a, Kaliontzoglou06b] και στην η/κ-υγεία [Bourka03a, Bourka03b, Georgoulas03]. Η πολυπλοκότητα των συγκεκριμένων λύσεων ποικίλει και είναι άμεση συνάρτηση της πολυπλοκότητας των υιοθετημένων επιχειρησιακών διαδικασιών και της προσφερόμενης λειτουργικότητας.

Λαμβάνοντας υπόψη τα δομικά και επιχειρησιακά τους χαρακτηριστικά, οι λύσεις αυτές μπορεί να διακριθούν σε δύο κατηγορίες. Στην πρώτη κατηγορία περιλαμβάνονται εκείνες οι οποίες λειτουργούν ως αυτόνομες εφαρμογές προσφέροντας μια συγκεκριμένη ανεξάρτητη Υπηρεσία Ιστού. Αυτές μπορεί να είναι είτε εφαρμογές κινητών συσκευών που επιτρέπουν την κλήση μιας υπηρεσίας είτε ηλεκτρονικές εφαρμογές που έχουν τη δυνατότητα να προσφέρουν ή να καλέσουν μια συγκεκριμένη υπηρεσία. Τέτοιου τύπου λύσεις συνήθως έχουν περιορισμένη λειτουργικότητα χωρίς συχνά να διαθέτουν τη δυνατότητα υποστήριξης πολύπλοκων διαδικασιών.

Αντίθετα η δεύτερη κατηγορία συντίθεται από λύσεις οι οποίες επιτρέπουν την κάλυψη σύνθετων επιχειρησιακών αναγκών, υιοθετώντας τις αρχές των Αρχιτεκτονικών Προσανατολισμένων στις Υπηρεσίες - ΑΠΥ (Service Oriented Architecture) [High05, Papazoglou07] ως το καινοτόμο αρχιτεκτονικό ύφος για το σχεδιασμό και την ανάπτυξη ολοκληρωμένων πληροφοριακών συστημάτων και πλατφορμών. Οι προσφερόμενες διαδικασίες ουσιαστικά αποτελούν μια σύνθεση

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

“χαλαρά” συνδεδεμένων δομικών στοιχείων, η οποία πραγματοποιείται με τέτοιο τρόπο ώστε να αναπαρίσταται πλήρως η επιχειρησιακή λογική της αντίστοιχης διαδικασίας. Πρακτικά κάθε επιχειρησιακή διαδικασία αναπαριστάται από την εκτέλεση ενός συνόλου Υπηρεσιών Ιστού.

1.1 Πεδίο Ενδιαφέροντος

Στις μέρες μας κοινό τόπο αποτελεί το γεγονός ότι οι ανωτέρω λύσεις λειτουργούν στην πλειονότητά τους ανεξάρτητα η μία της άλλης. Η επίτευξη *διαλειτουργικότητας* είναι ένας δύσκολος στόχος, η πραγματοποίηση του οποίου θα επιτρέψει τη διεκπεραίωση πολύπλοκων ηλεκτρονικών συναλλαγών ανάμεσα σε διαφορετικούς επιχειρηματικούς φορείς επεκτείνοντας ταυτόχρονα τις επιχειρησιακές τους δραστηριότητες.
Η τάση για βελτίωση της αποτελεσματικότητας, της ευελιξίας και της διασύνδεσης των προσφερόμενων υπηρεσιών είχε ως αποτέλεσμα την εμφάνιση ενός συνόλου πρωτοβουλιών προτυποποίησης και πλαισίων διαλειτουργικότητας. Βασικός τους σκοπός [IDABC] αποτέλεσε ο καθορισμός των γενικότερων αρχών και της στρατηγικής που θα πρέπει να διέπουν την ανάπτυξη πληροφοριακών συστημάτων, καθώς επίσης και των τεχνολογικών προτύπων βάσει των οποίων πρέπει να αναπτύσσονται τα πληροφοριακά συστήματα, με στόχο την υποστήριξη τόσο της ανταλλαγής δεδομένων μεταξύ συστημάτων όσο και της παροχής ολοκληρωμένων υπηρεσιών ηλεκτρονικών συναλλαγών.
Σε πρακτικό όμως επίπεδο, απλά η υιοθέτηση κοινών προτύπων και τεχνολογιών παρά το γεγονός ότι ευνοεί την επίτευξη της διαλειτουργικότητας, δεν την εγγυάται. Απαιτείται η χρήση μηχανισμών που ελέγχουν την πιστή εφαρμογή των προτύπων και των οδηγιών και αποφαίνονται κατά πόσο καλύπτονται πλήρως το σύνολο των χαρακτηριστικών που προσδιορίζονται από αυτά.
Εύλογα, λοιπόν, εμφανίζεται η ανάγκη για δημιουργία μεθόδων ελέγχου της δυνατότητας επικοινωνίας των Υπηρεσιών Ιστού που να λαμβάνουν υπόψη τα ιδιαίτερα χαρακτηριστικά τους, να ακολουθούν συγκεκριμένη στρατηγική για την εκτέλεση των ελέγχων, να υιοθετούν συγκεκριμένους τύπους ελέγχων και να καθορίζουν συγκεκριμένα κριτήρια ως προς τα οποία αξιολογείται η δυνατότητα αλληλεπίδρασής τους. Υπάρχοντα πλαίσια ελέγχου μπορεί να χρησιμοποιηθούν στην περίπτωση των Υπηρεσιών Ιστού, αλλά συνήθως είτε είναι πολύ γενικά χωρίς να διατυπώνουν συγκεκριμένα και διακριτά βήματα που πρέπει να ακολουθηθούν και χωρίς να προσδιορίζουν με σαφήνεια τις διαδικασίες που πρέπει να εκτελεστούν για τον καθορισμό περιπτώσεων ελέγχου, είτε έχουν περιορισμένο πεδίο εφαρμογής όσον αφορά στα ιδιαίτερα χαρακτηριστικά των Υπηρεσιών Ιστού, ενώ σε ορισμένες περιπτώσεις αδυνατούν να κάνουν απόδοση ευθύνης στην Υπηρεσία Ιστού η οποία ευθύνεται για την αποτυχία επικοινωνίας.
Στο σημείο αυτό τίθεται ένα σύνολο ερωτημάτων, «ποια πρέπει είναι η βέλτιστη στρατηγική που πρέπει να ακολουθηθεί; Ποιοι είναι οι τύποι ελέγχων που πρέπει να υιοθετηθούν; Ποια είναι τα κριτήρια αξιολόγησης που πρέπει να εφαρμοστούν από μια μέθοδο ελέγχου, προκειμένου το αποτέλεσμα να εξασφαλίζει την διαλειτουργικότητα των Υπηρεσιών Ιστού;»
Η αυξανόμενη απαίτηση για διαλειτουργικότητα αποτελεί άμεση συνάρτηση της ραγδαίας αύξησης των προσφερόμενων Υπηρεσιών Ιστού καθώς επίσης και της πληθώρας των δεδομένων που ανταλλάσσονται μεταξύ των επιχειρησιακών φορέων. Το γεγονός αυτό εισάγει ένα σύνολο πρόσθετων ζητημάτων που αφορούν στη διαχείριση της ταυτότητας κυρίως των απλών χρηστών που μετέχουν στις

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συναλλαγές. Ο χρήστης απαιτείται, πλέον, να χρησιμοποιεί μόνο ένα υποσύνολο των πληροφοριών που συνθέτουν την *ταυτότητα* του για καθεμία από τις συναλλαγές του, έχοντας ως συνέπεια να καλείται να διαχειριστεί ένα σύνολο *μερικών ταυτοτήτων (partial identities)*, καθεμία από τις οποίες αναπαριστά ένα διακριτό υποσύνολο των δεδομένων που τον αφορούν.

Η ύπαρξη *Συστημάτων Διαχείρισης Ταυτότητας (ΣΔΤ)* [Haddad08] τα οποία αποτελούν έναν συνδυασμό τεχνολογιών και πρακτικών για την αναπαράσταση των χρηστών ως ψηφιακές ταυτότητες, επιτυγχάνουν την εκτέλεση ευέλικτων και εξελίξιμων συναλλαγών. Στο πλαίσιο των συστημάτων αυτών η μεταφορά και διάδοση πληροφοριών και γνώσης γίνεται με τρόπο ομαλό και αποτελεσματικό έτσι ώστε να εγγυάται τη συνέχεια και την ακρίβεια της ροής των δεδομένων. Παρά το γεγονός όμως του καθορισμού μιας σειράς ΣΔΤ τα οποία διακρίνονται κατά κύριο λόγο από ανομοιογένεια, βασικά ερωτήματα παραμένουν ανοικτά, όπως το ποιοι είναι οι βέλτιστοι τρόποι διαχείρισης της ταυτότητας των χρηστών που επιθυμούν να αποκτήσουν πρόσβαση στις Υπηρεσίες Ιστού και με ποιούς τρόπους μπορεί να διευκολυνθεί η πρόσβαση των χρηστών αυτών στις Υπηρεσίες Ιστού.

Παράλληλα, η ολοκλήρωση αξιόπιστων και έμπιστων συναλλαγών θέτει μια επιπλέον παράμετρο που σχετίζεται με την ύπαρξη μηχανισμών οι οποίοι διασφαλίζουν και εγγυώνται μια έμπρακτη *σχέση εμπιστοσύνης* μεταξύ των συμμετεχουσών οντοτήτων. Η διαμορφωμένη σχέση θα πρέπει να βασίζεται σε απτά στοιχεία ενώ θα πρέπει επίσης να αξιολογείται και να ανανεώνεται συχνά λαμβάνοντας υπόψη της την εν γένει συμπεριφορά των χρηστών. Τα ερωτήματα λοιπόν που ανακύπτουν είναι:

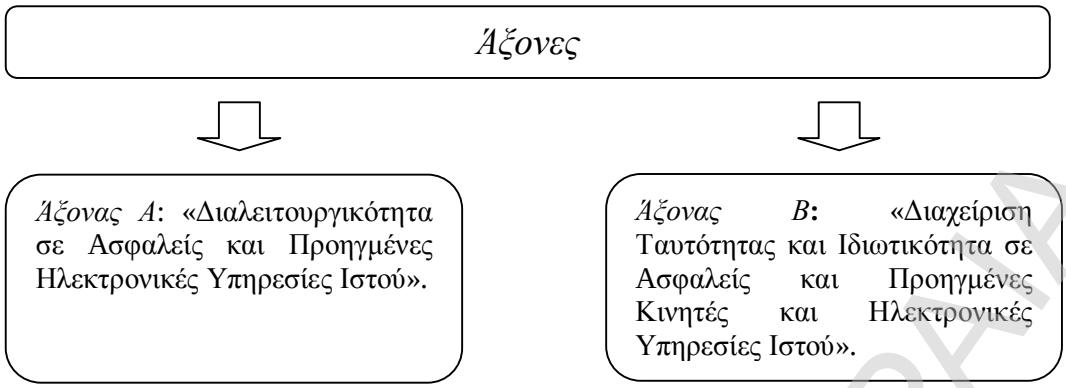
- «Πώς μπορεί να ενισχυθεί η εμπιστοσύνη μεταξύ των χρηστών και των παρόχων Υπηρεσιών Ιστού;»
- «Ποιο είναι το μέτρο που πρέπει να χρησιμοποιηθεί και το οποίο προσφέρει έναν αυτοματοποιημένο τρόπο αξιολόγησης της εμπιστοσύνης;»
- «Πώς μπορεί η προγενέστερη συμπεριφορά ενός χρήστη να επηρεάσει το επίπεδο πρόσβασης του στις παρεχόμενες Υπηρεσίες Ιστού;»

Αναμφισβήτητα, σημαντικό παράγοντα στην εδραίωση του απαιτούμενου επιπέδου επιστοσύνης διαδραματίζει, σε υψηλό μάλιστα βαθμό, και η προστασία της ιδιωτικότητας των εμπλεκόμενων οντοτήτων. Η υιοθέτηση διαδικασιών διαχείρισης και διανομής πληροφοριών ευαίσθητων ως προς το περιεχόμενό τους επιτάσσει την ικανοποίηση του συνόλου των πτυχών της ιδιωτικότητας (π.χ. ανωνυμία, ψευδωνυμία κ.τ.λ.). Οι εκτελούμενες, λοπόν, η/κ-συναλλαγές θα πρέπει να διέπονται από βασικές αρχές, όπως είναι συμφωνία ως προς το επίπεδο των δεδομένων που πρέπει να αποκαλυφθεί ή το επίπεδο ασφάλειας που πρέπει να εφαρμοστεί, οι οποίες θα καθορίζονται αποκλειστικά από τις οντότητες που μετέχουν σε αυτές. Επιπλέον, αποτελεί μια εξίσου σημαντική απαίτηση η διευθέτηση της *ανωνυμίας* σε *επίπεδο σύνδεσης*, όπου διασφαλίζεται ότι το σύνολο των δικτυακών πληροφοριών των εμπλεκόμενων οντοτήτων δεν θα αποκαλυφθούν. Επισημαίνεται, λοιπόν, η ανάγκη για εδραίωση επαρκών μηχανισμών που εγγυώνται την ανωνυμία σε ικανοποιητικό βαθμό.

1.2 Αντικείμενο, Προσφορά της Διατριβής

Βάσει της παραπάνω υπάρχουσας κατάστασης και αναγκών, το αντικείμενο μελέτης της παρούσας διατριβής χωρίζεται σε δύο άξονες, Σχήμα 1, σε καθένα από τους οποίους έχουν εντοπιστεί συγκεκριμένα προβλήματα και ελλείψεις:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 1. Βασικοί Άξονες Διατριβής

- *Άξονας Α*: «*Διαλειτουργικότητα σε Ασφαλείς και Προηγμένες Ηλεκτρονικές Υπηρεσίες Ιστού*». Ο πρώτος άξονας της διατριβής μελετά ζητήματα που αφορούν την διαλειτουργικότητα των Υπηρεσιών Ιστού. Πιο συγκεκριμένα, εστιάζεται στις μεθοδολογίες ελέγχου της διαλειτουργικότητας και συμμόρφωσης των ασφαλών και προηγμένων ηλεκτρονικών Υπηρεσιών Ιστού (ΥΙ) οι οποίες προσφέρονται είτε ως αυτόνομες Υπηρεσίες Ιστού είτε ενσωματωμένες σε μια Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ).
- *Άξονας Β*: «*Διαχείριση Ταυτότητας και Ιδιωτικότητα σε Ασφαλείς και Προηγμένες Κινητές και Ηλεκτρονικές Υπηρεσίες Ιστού*». Ο δεύτερος άξονας της διατριβής αναλύει ζητήματα που αφορούν στη διαχείριση της ταυτότητας των χρηστών, ερευνά τρόπους με τους οποίους μπορεί να ενισχυθεί η σχέση εμπιστοσύνης μεταξύ των οντοτήτων που εμπλέκονται σε μια συναλλαγή και επικεντρώνεται σε ζητήματα ιδιωτικότητας που σχετίζονται με τη ανωνυμία σε επίπεδο σύνδεσης στις ασφαλείς και προηγμένες κινητές και ηλεκτρονικές Υπηρεσίες Ιστού (ΥΙ).

Στο χώρο των παραπάνω ερευνητικών πεδίων, τα αποτελέσματα και η συνεισφορά της διατριβής παρουσιάζονται συνοπτικά στα επόμενα κεφάλαια.

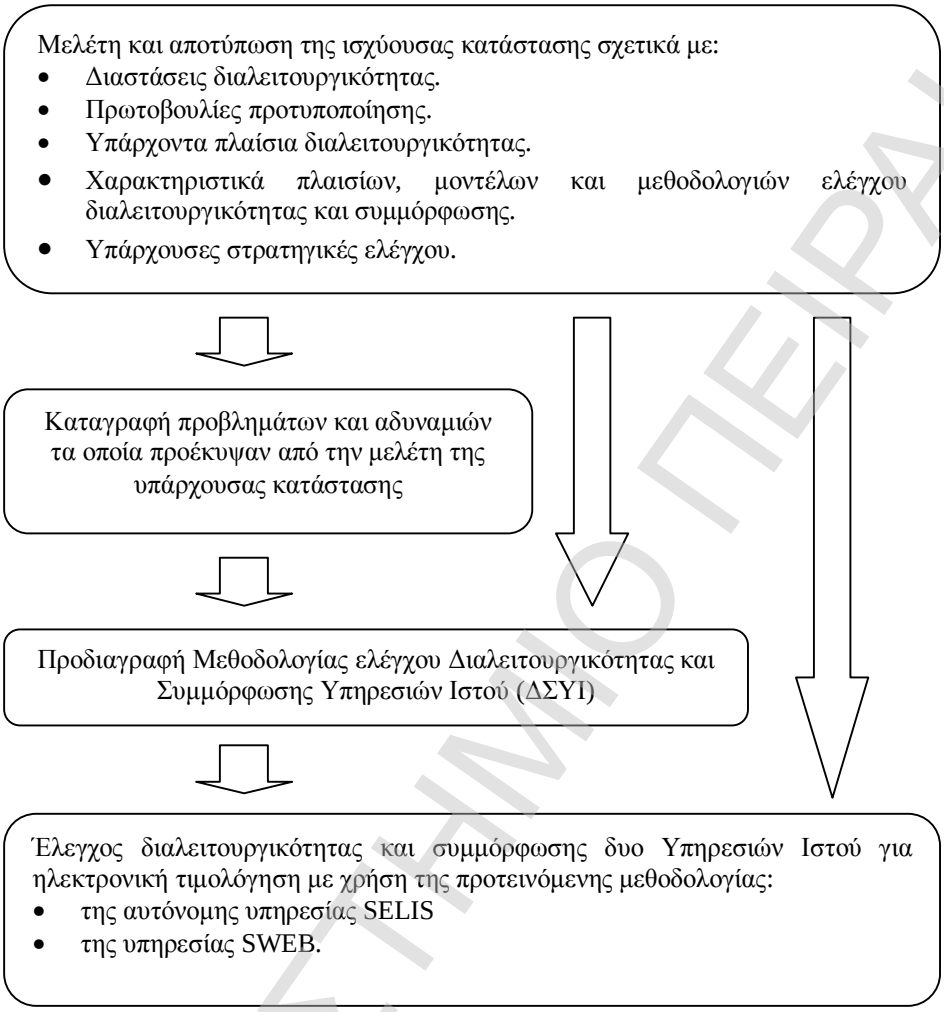
1.2.1 Άξονας Α: Διαλειτουργικότητα

Στα πλαίσια του πρώτου άξονα της διατριβής (Σχήμα 2) μελετήθηκαν και αποτιμήθηκαν ένα σύνολο ζητημάτων που αφορούν στη διαλειτουργικότητα των Υπηρεσιών Ιστού. Πιο συγκεκριμένα μελετήθηκαν τα ακόλουθα:

- Πρωτοβουλίες προτυποποίησης, που επικεντρώνονται στον καθορισμό συγκεκριμένων προτύπων και προδιαγραφών.
- Υπάρχοντα πλαίσια διαλειτουργικότητας, που εστιάζονται στον καθορισμό των γενικότερων αρχών και της στρατηγικής που θα πρέπει να διέπουν την ανάπτυξη πληροφοριακών συστημάτων, καθώς επίσης και στην καταγραφή των τεχνολογικών προτύπων βάσει των οποίων πρέπει να αναπτύσσονται τα πληροφοριακά συστήματα.
- Διαστάσεις διαλειτουργικότητας, οι οποίες θα πρέπει να ληφθούν υπόψη για τη δημιουργία ενός πλαισίου διαλειτουργικότητας.
- Υπάρχοντα πλαίσια και μεθοδολογίες ελέγχου διαλειτουργικότητας και συμμόρφωσης, που έχουν ως βασική επιδίωξη τον έλεγχο της αποτελεσματικής επικοινωνίας υπηρεσιών/εφαρμογών αλλά και σε πιο ευρεία έννοια προϊόντων τα οποία υλοποιούν συγκεκριμένες προδιαγραφές και πρότυπα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- Υπάρχουσες στρατηγικές ελέγχου, οι οποίες μπορούν να εφαρμοστούν για να ελέγξουν την δυνατότητα επικοινωνίας των υπηρεσιών/εφαρμογών και καθορίζουν τον βαθμό διεισδυσιμότητας των εκτελούμενων ελέγχων.



Σχήμα 2. Α Άξονας: «Διαλειτουργικότητα σε Ασφαλείς και Προηγμένες Ηλεκτρονικές Υπηρεσίες Ιστού»

Υπο το πρίσμα των Υπηρεσιών Ιστού, τα συμπεράσματα τα οποία προκύπτουν από τη μελέτη των παραπάνω ζητημάτων είναι τα ακόλουθα:

- Οι υπάρχουσες πρωτοβουλίες προτυποποίησης και τα πλαίσια διαλειτουργικότητας στο σύνολό τους εστιάζουν είτε στο να προτείνουν πρότυπα και προδιαγραφές είτε στο να καθορίσουν τις οδηγίες που θα πρέπει να διέπει ένα πλαίσιο διαλειτουργικότητας. Σε καμμιά περίπτωση όμως δεν μπορούν να εγγυηθούν ότι οι οργανισμοί οι οποίοι έχουν υιοθετήσει και υλοποιούν τα πρότυπα και τις οδηγίες ότι τα εφαρμόζουν και τα ακολουθούν πιστά καλύπτοντας πλήρως το σύνολο των πτυχών που προσδιορίζονται από αυτά. Επομένως οι πρωτοβουλίες αυτές παρά το γεγονός ότι συνδράμουν αποφασιστικά στην ενίσχυση της διαλειτουργικότητας αδυνατούν να την εγγυηθούν.
- Υπάρχει αδυναμία ολιστικής προσέγγισης του τρόπου με τον οποίο οι Υπηρεσίες Ιστού μπορούν να ελεχθούν ως προς τη διαλειτουργικότητα και τη συμμόρφωση τους προς τα αντίστοιχα πρότυπα και τις τεχνολογίες που έχουν

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

υιοθετήσει και υλοποιούν (π.χ. τεχνολογίες όπως η XML, οι Υπηρεσίες Ιστού και η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)).

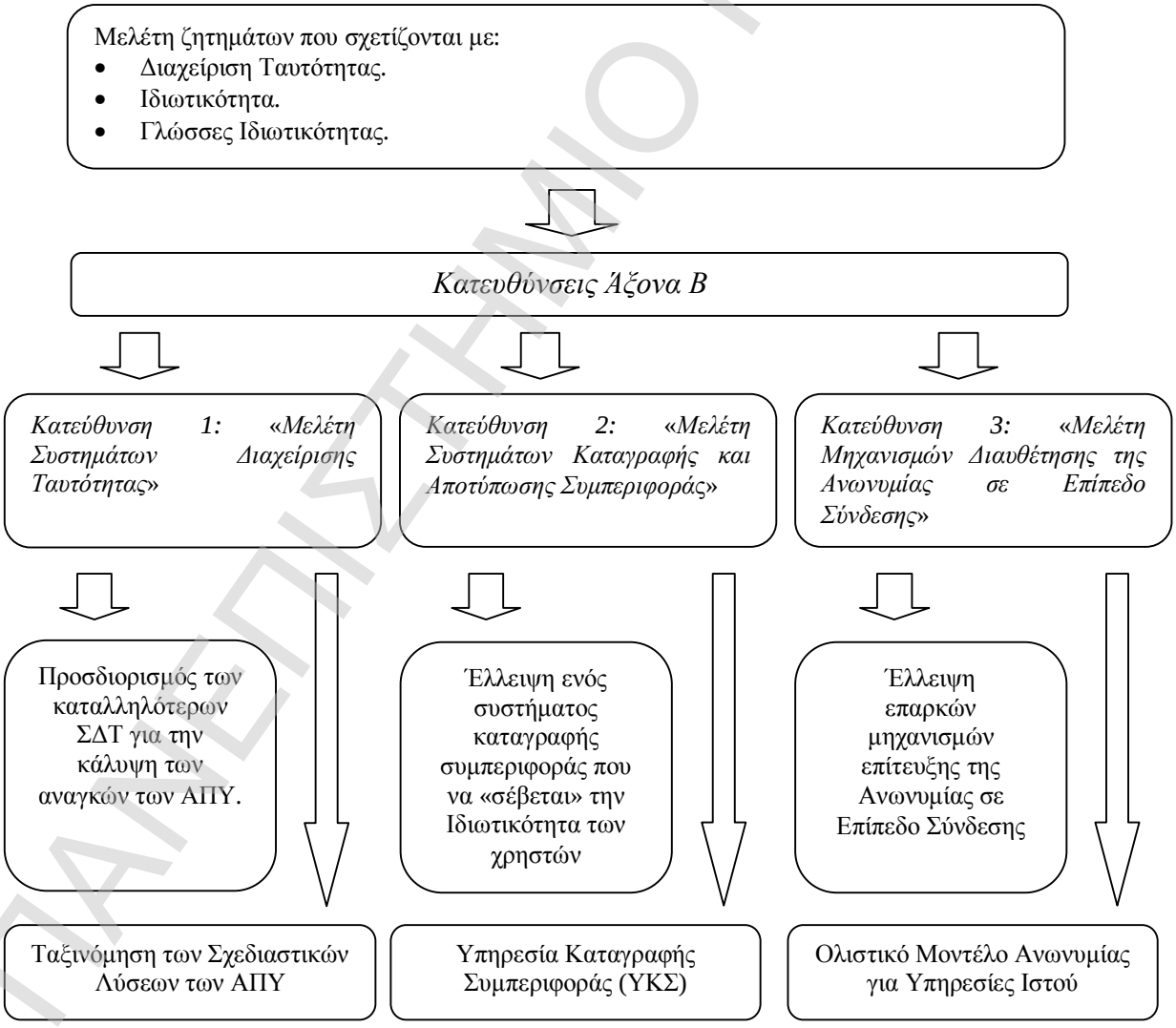
- Τα υπάρχοντα πλαίσια ελέγχου είναι πολύ γενικά χωρίς να διατυπώνουν συγκεκριμένα και διακριτά βήματα που πρέπει να ακολουθηθούν αλλά και δεν υπάρχει σαφής προσδιορισμός διαδικασιών που πρέπει να εκτελεστούν για τον καθορισμό περιπτώσεων ελέγχου.
- Τα υπάρχοντα πλαίσια ελέγχου έχουν περιορισμένο πεδίο εφαρμογής όσον αφορά στις πτυχές των Υπηρεσιών Ιστού που πρέπει να ελεχθούν, ενώ σε ορισμένες περιπτώσεις αδυνατούν να κάνουν απόδοση ευθύνης στην Υπηρεσία Ιστού η οποία είναι υπεύθυνη για την αποτυχία επικοινωνίας.
- Υπάρχουν διαφορετικές στρατηγικές ελέγχων που μπορεί να εφαρμοστούν για να ελέγξουν την δυνατότητα επικοινωνίας των εξεταζόμενων υπηρεσιών. Τέτοιου είδους στρατηγικές είναι ο έλεγχος "άσπρου" κουτιού στα πλαίσια του οποίου απαιτείται η πλήρης γνώση του λογισμικού της εφαρμογής, ο έλεγχος "μαύρου" κουτιού, κατά τον οποίο δεν είναι υποχρεωτική η καταννόηση της εσωτερικής συμπεριφοράς της εφαρμογής, και ο έλεγχος "γκρίζου" κουτιού, ο οποίος πραγματοποιείται με περιορισμένη γνώση της εσωτερικής αρχιτεκτονικής των υπηρεσιών. Η φύση των Υπηρεσιών Ιστού διαδραματίζει σημαντικό ρόλο στην υιοθέτηση της καταλληλότερης στρατηγικής ελέγχου καθώς εγείρει ένα σύνολο ζητημάτων και προκλήσεων τα οποία πρέπει να επισημανθούν και να ληφθούν υπόψη.

Η διατριβή λύνει τα παραπάνω προβλήματα προδιαγράφοντας μια *πρωτότυπη συστηματική και δομημένη μεθοδολογία ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ)*.
Τα πλεονεκτήματα της μεθοδολογίας σε σχέση με υπάρχουσες προσεγγίσεις και οι καινοτομίες της συνοψίζονται στα εξής:

- Λαμβάνει πλήρως υπ' όψη της τη φύση των Υπηρεσιών Ιστού και τις προκλήσεις που εγείρονται από αυτή υιοθετώντας τη βέλτιστη για τη συγκεκριμένη περίσταση στρατηγική που είναι ο έλεγχος "γκρίζου" κουτιού.
- Παρά το γεγονός ότι η ΔΣΥΙ είναι γενικευμένη, επιτρέποντας έτσι τον έλεγχο διαλειτουργικότητας και συμμόρφωσης ενός μεγάλου εύρους Υπηρεσιών Ιστού, είναι αναλυτικά δομημένη παρέχοντας συγκεκριμένα βήματα που πρέπει να ακολουθηθούν.
- Καθορίζει συγκεκριμένα κριτήρια ως προς τα οποία αξιολογούνται οι Υπηρεσίες Ιστού ενώ παράλληλα είναι επεκτάσιμη επιτρέποντας την υιοθέτηση νέων κριτηρίων χωρίς να επηρεάζεται ή να μεταβάλλεται σε κανέναν βαθμό η λογική συνέχεια, η πολυπλοκότητα και η ροή της μεθοδολογίας.
- Είναι παραμετροποιήσιμη υπό την έννοια ότι μπορούν να εφαρμοστούν κατάλληλα υποσύνολά της για την εφαρμογή ελέγχων.
- Παρέχει την δυνατότητα πλήρους ελέγχου πάνω στις εφαρμοζόμενες διαδικασίες εποπτεύοντας την εκτέλεσή τους.
- Επιτρέπει την απόδοση της ευθύνης στο σύστημα το οποίο ευθύνεται για την αποτυχία της επικοινωνίας καταγράφοντας στο σύνολο τους τα δεδομένα ελέγχου.
- Παρέχει υψηλό επίπεδο ανεξαρτησίας από τις τεχνολογίες με τις οποίες είναι υλοποιημένες οι εξεταζόμενες ΥΙ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η προτεινόμενη μεθοδολογία μπορεί να εφαρμοστεί για τον έλεγχο της διαλειτουργικότητας ηλεκτρονικών Υπηρεσιών Ιστού, όπως επίσης και υπηρεσιών οι οποίες εφαρμόζονται στα πλαίσια του ίδιου του πληροφοριακού συστήματος ή της ίδιας πλατφόμας. Επίσης, θα πρέπει να επισημανθεί ότι οι βασικές αρχές της μπορούν να εφαρμοστούν ακόμα και στην περίπτωση των κινητών Υπηρεσιών Ιστού.
Τέλος στα πλαίσια της διατριβής εξετάστηκε η ορθότητα και εφαρμοσιμότητα της προτεινόμενης μεθοδολογίας ελέγχου με την εφαρμογή της για τον έλεγχο της επικοινωνίας δυο υπαρχόντων και πλήρως λειτουργικών Υπηρεσιών Ιστού για ηλεκτρονική τιμολόγηση, της αυτόνομης υπηρεσίας ηλεκτρονικής τιμολόγησης SELIS (Secure Electronic Invoicing Service) [Kaliontzoglou06c, SELIS] και της υπηρεσίας ηλεκτρονικής και κινητής τιμολόγησης SWEB που είναι ενσωματωμένη σε μια ΑΠΥ [Meneklis07, Karantjias08a]. Η επιλογή των συγκεκριμένων προσεγγίσεων βασίστηκε στο γεγονός της υψηλής απαίτησης για διαλειτουργικότητα που παρουσιάζει η συγκεκριμένη υπηρεσία όπως και στο στοιχείο ότι οι αντίστοιχες υλοποιήσεις έχουν λειτουργήσει σε ένα πανευρωπαϊκό δίκτυο φορέων, λαμβάνοντας υπόψη το κοινοτικό πλαίσιο που διέπει τέτοιες διασυνοριακές συναλλαγές.



Σχήμα 3. Β Άξονας: «Διαχείριση Ταυτότητας και Ιδιωτικότητα σε Ασφαλείς και Προηγμένες Κινητές και Ηλεκτρονικές Υπηρεσίες Ιστού»

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

1.2.2 Άξονας Β: Διαχείριση Ταυτότητας και Ιδιωτικότητα

Ο δεύτερος άξονας της διατριβής (Σχήμα 3) πραγματεύεται μια σειρά ζητημάτων τα οποία σχετίζονται με τη διαχείριση ταυτότητας και την προστασία της ιδιωτικότητας των κινητών και ηλεκτρονικών Υπηρεσιών Ιστού. Πιο συγκεκριμένα, μελετώνται βασικές έννοιες (π.χ. μερικές ταυτότητες) που συνδέονται με τη διαχείριση της ταυτότητας των χρηστών και παρουσιάζεται η ανάγκη ύπαρξης Συστημάτων Διαχείρισης Ταυτότητας τα οποία θα αποτελούνται από διακριτές και αυστηρά ορισμένες υπηρεσίες. Στη συνέχεια επισημαίνεται η σημασία της προστασίας της ιδιωτικότητας των χρηστών για την ολοκλήρωση αξιόπιστων και έμπιστων η/κ-συναλλαγές και αναλύονται οι πτυχές της ιδιωτικότητας (ανωνυμία, ψευδωνυμία κτ.λ.), οι οποίες πρέπει να ληφθούν υπόψη για τον σχεδιασμό και υλοποίηση αποτελεσματικών, από επιχειρησιακή άποψη ΣΔΤ.
Τέλος, το ενδιαφέρον μεταφέρεται στη μελέτη των Γλωσσών Ιδιωτικότητας, οι οποίες μπορούν να χρησιμοποιηθούν ώστε να απεικονιστούν οι επιθυμίες των χρηστών και τα χαρακτηριστικά των Υπηρεσιών Ιστού. Η χρήση των γλωσσών αυτών αναγνωρίζεται ως ένας αποτελεσματικός και ευέλικτος τρόπος για την προστασία της ιδιωτικότητας των χρηστών.
Ο άξονας αυτός χωρίζεται σε τρεις κατευθύνσεις στα πλαίσια των οποίων εξετάστηκε ένα σύνολο επιμέρους ζητημάτων.

Κατεύθυνση 1: «Μελέτη Συστημάτων Διαχείρισης Ταυτότητας»

Οι σχεδιαστές των αρχιτεκτονικών προσανατολισμένων σε υπηρεσίων (ΑΠΥ) πλέον βρίσκονται αντιμέτωποι με ένα νέο πρόβλημα το οποίο σχετίζεται με τον προσδιορισμό των ΣΔΤ τα οποία είναι καταλληλότερα για να καλύψουν τις ανάγκες των ΑΠΥ που προτίθενται να αναπτύξουν ή έχουν ήδη αναπτύξει [Modinis06]. Η υιοθέτηση της καταλληλότερης λύσης θα πρέπει να γίνει με τρόπο που να μην εισάγει πρόσθετη πολυπλοκότητα στον σχεδιασμό και την υλοποίηση της ΑΠΥ ή να μην λαμβάνει υπόψη τις συγκεκριμένες πτυχές της ιδιωτικότητας.
Στα πλαίσια της πρώτης κατεύθυνσης για την επίλυση του συγκεκριμένου προβλήματος μελετήθηκαν και αναλύθηκαν οι σημαντικότερες και ευρέως διαδεδομένες προσεγγίσεις Συστημάτων Διαχείρισης Ταυτότητας καθώς και οι υπάρχουσες ταξινομήσεις τους παρέχοντας στον χρήστη μια ολοκληρωμένη εικόνα όσον αφορά τους στόχους που κάθε σύστημα επιχειρεί να καλύψει. Από τη μελέτη αυτή διαπιστώθηκε η ύπαρξη μιας πληθώρας λύσεων ΣΔΤ τα οποία παρουσιάζουν σημαντική έλλειψη ομοιογένειας.
Η διατριβή για το σκοπό αυτό προτείνει μια *ταξινόμηση των σχεδιαστικών λύσεων των Αρχιτεκτονικών Προσανατολισμένων στις Υπηρεσίες (ΑΠΥ) παρέχοντας συγκεκριμένες λύσεις διαχείρισης ταυτότητας και διαδικασιών* οι οποίες μπορούν να εφαρμοστούν για καθεμία από τις προσδιοριζόμενες κατηγορίες. Η ταξινόμηση με τον τρόπο αυτό μπορεί να λειτουργήσει ως «οδηγός» για τους σχεδιαστές ΑΠΥ που θα τους βοηθήσει να υιοθετήσουν την καταλληλότερη λύση που ικανοποιεί τις ανάγκες της συγκεκριμένης ΑΠΥ που υλοποιούν.

Κατεύθυνση 2 «Μελέτη Συστημάτων Καταγραφής και Αποτύπωσης Συμπεριφοράς»

Παρόλη τη ραγδαία αύξηση των προσφερόμενων ηλεκτρονικών και κινητών υπηρεσιών το επίπεδο της εμπιστοσύνης μεταξύ των εμπλεκομένων οντοτήτων παραμένει εξαιρετικά χαμηλό. Η χρήση Συστημάτων Διαχείρισης Ταυτότητας ως μια Έμπιστη Τρίτη Οντότητα η οποία παρακολουθεί και διασφαλίζει τη ροή των

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ανταλλασσόμενων πληροφοριών δεν μπορεί να διαμορφώσει και να εγγυηθεί μια σχέση εμπιστοσύνης μεταξύ των συμβαλλόμενων μερών σε ικανοποιητικό βαθμό.
Η ύπαρξη μιας γρήγορης και αυτοματοποιημένης διαδικασίας αξιολόγησης του βαθμού εμπιστοσύνης μπορεί να διαδραματίσει ουσιαστικό ρόλο στην ολοκλήρωση έμπιστων αλληλεπιδράσεων και τη μείωση των κινδύνων που εμπεριέχουν οι η/κ-συναλλαγές. Η χρήση Συστημάτων Καταγραφής Συμπεριφοράς τα οποία μπορούν αποτυπώσουν τη συμπεριφοράς που επιδεικνύεται από τους χρήστες στα πλαίσια των συναλλαγών που αυτοί εκτελούν με τις ΥΙ μπορεί να συμβάλλουν ουσιαστικά προς τη κατεύθυνση αυτή. Παρόλα αυτά ένα σημαντικό πρόβλημα το οποίο εντοπίζεται είναι η έλλειψη ενός συστήματος καταγραφής συμπεριφοράς που να «σέβεται» την ιδιωτικότητα των χρηστών.
Στα πλαίσια, λοιπόν, της δεύτερης κατεύθυνσης τα ζητήματα που εξετάστηκαν είναι τα ακόλουθα:

- Συστήματα Καταγραφής και Αποτύπωσης Συμπεριφοράς: υπάρχοντα συστήματα καταγραφής συμπεριφοράς τα οποία επικεντρώνονται κατά κύριο λόγο στη συλλογή, διανομή, και συγκέντρωση των στοιχείων που αφορούν στη συμπεριφορά των εμπλεκόμενων οντοτήτων.
- Συστήματα Διαχείρισης Ταυτότητας: συστήματα διαχείρισης ταυτότητας, με εστίαση στον τρόπο με τον οποίο αυτά επιτυγχάνουν να εγγυηθούν την εμπιστοσύνη μεταξύ των εμπλεκόμενων οντοτήτων και να διευθετήσουν την απαίτηση καταγραφής συμπεριφοράς.

Η διατριβή, λαμβάνοντας υπόψη την υφιστάμενη κατάσταση προτείνει μια *Υπηρεσία Καταγραφής Συμπεριφοράς (ΥΚΣ)* η οποία λειτουργεί στα πλαίσια ενός Συστήματος Διαχείρισης Ταυτότητας, προκειμένου να διαφυλάξει και να διασφαλίσει την αναπτυσσόμενη εμπιστοσύνη προσφέροντας έναν αυτοματοποιημένο τρόπο αξιολόγησης της. Η προτεινόμενη υπηρεσία αξιολογεί την αξιοπιστία των χρηστών παρέχοντας στους παρόχους αντικειμενικές και έμπιστες εκτιμήσεις οι οποίες αποκαλύπτουν τις προθέσεις τους, ως προς τον τρόπο με τον οποίο προτίθενται να συμπεριφερθούν στις μελλοντικές τους συναλλαγές. Οι εκτιμήσεις αυτές μπορούν επίσης να χρησιμοποιηθούν και ως επιπλέον κριτήριο από τους παρόχους επιτρέποντας τους να εκτελέσουν καλώς διαμορφωμένες αποφάσεις ελέγχου πρόσβασης.

Κατεύθυνση 3 «Μελέτη Μηχανισμών Διευθέτησης της Ανωνυμίας σε Επίπεδο Σύνδεσης»

Η τρίτη κατεύθυνση επικεντρώνεται στη έλλειψη επαρκών μηχανισμών διευθέτησης της Ανωνυμίας σε Επίπεδο Σύνδεσης οι οποίοι θα είναι εφαρμόσιμοι στην περίπτωση των ΥΙ. Η μελέτη των υπαρχουσών προσεγγίσεων Δικτύων Ανωνυμίας ανέδειξε ένα σύνολο αδυναμιών οι οποίες συνοψίζονται στις ακόλουθες:

- Δίκτυα Ανωνυμίας που είναι ευάλωτα σε χρονικούς περιορισμούς.
- Δίκτυα Ανωνυμίας που δεν μπορούν να προσφέρουν ουσιαστική προστασία των δικτυακών πληροφοριών των δύο τελικών σημείων της κίνησης (π.χ. με την παροχή κρυμμένων υπηρεσιών).

Η διατριβή για το σκοπό αυτό προτείνει ένα *Ολιστικό Μοντέλο Ανωνυμίας για Υπηρεσίες Ιστού***,** το οποίο αποτελεί μια λύση «υψηλής καθυστέρησης» (high latency)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

για Υπηρεσίες Ιστού, οι οποίες είναι ιδιαίτερα ανθεκτικές σε χρονικούς περιορισμούς. Το προτεινόμενο μοντέλο επιτυγχάνει απόκρυψη της δικτυακής θέση των εμπλεκόμενων οντοτήτων, τόσο του αρχικού χρήστη που επιθυμεί πρόσβαση σε μια Υπηρεσία Ιστού όσο και της ίδιας της Υπηρεσίας Ιστού μέσω της παροχής κρυμμένων Υπηρεσιών Ιστού, ενώ παράλληλα είναι ανθεκτικό σε ένα σύνολο (ενεργών και παθητικών) επιθέσεων οι οποίες βρίσκουν εφαρμογή στα δίκτυα ανωνυμίας.

1.3 Δομή της Διατριβής

Συνακόλουθα με τους παραπάνω άξονες, ο σκελετός του κειμένου της διατριβής διαρθρώνεται ως εξής:

- Το **1ο κεφάλαιο** αποτελεί την παρούσα εισαγωγή.
- Το **2ο κεφάλαιο** αποτυπώνει το σύνολο των πτυχών του Άξονα Α της διατριβής παρέχοντας μια επισκόπηση της προτεινόμενης Μεθοδολογίας Ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ) και διατυπώνοντας μελλοντικές ερευνητικές κατευθύνσεις.
- Το **3ο κεφάλαιο** παρουσιάζει την εφαρμογή της μεθοδολογίας ΔΣΥΙ με τον έλεγχο της επικοινωνίας δυο Υπηρεσιών Ιστού για ηλεκτρονική τιμολόγηση.
- Το **4ο κεφάλαιο** περιγράφονται μια σειρά ζητημάτων τα οποία σχετίζονται με τη διαχείριση ταυτότητας και την προστασία της ιδιωτικότητας των χρηστών ενώ παρουσιάζονται τα ανοιχτά προβλήματα του Άξονα Β της διατριβής.
- Το **5ο, 6ο** και **7ο κεφάλαιο** αντίστοιχα παρουσιάζει και παραθέτει τις τρεις κατευθύνσεις του Άξονα Β της διατριβής περιγράφοντας επίσης αντίστοιχες μελλοντικές ερευνητικές κατευθύνσεις.
- Το **8ο κεφάλαιο** ολοκληρώνει τη διατριβή διατυπώνοντας τα συνολικά συμπεράσματα και παρουσιάζοντας στο σύνολο τους τις μελλοντικές ερευνητικές κατευθύνσεις της διατριβής.
- Στο **Παράρτημα** παρέχει παραδείγματα δεδομένων ελέγχου που χρησιμοποιήθηκαν κατά την εφαρμογή της μεθοδολογίας ΔΣΥΙ του Άξονα Α και ορισμένα αποτελέσματα όπως αυτά προέκυψαν κατά την εκτέλεση της.

Κάθε κεφάλαιο ολοκληρώνεται με παραγράφους για συμπεράσματα και παράθεση βιβλιογραφικών αναφορών.

1.4 Αναφορές

[XML] T. Bray et al. (Editors). (2004). "*Extensible Markup Language (XML) 1.0 (Third Edition)*", W3C Recommendation 04 February 2004.

[Kreger01] H. Kreger. (2001). "*Web Services Conceptual Architecture – WSCA 1.0*", White paper, http://www-3.ibm.com/software/solutions/webservices/pdf/KREGER01.pdf.

[Booth04] D. Booth et al. (Editors). (2004). "*Web Services Architecture*", W3C Working Group Note 11 February 2004, http://www.w3.org/TR/2004/NOTE-ws-arch-20040211.

[Adams99] C. Adams, S. Lloyd. (1999). "*Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations*", 1st Edition, Macmillan Technical Publishing, 1999.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Naedele] G. M. Naedele. (2003). "*Standards for XML and Web Services Security*", IEEE Computer, pp.96-98, 2003.

[ETSI101733] ETSI Technical Specification. (2002). "*Electronic signature and infrastructures; Electronic signature formats*", ETSI TS 101 733 V1.4.0, http://portal.etsi.org.

[XAdES02] ETSI Technical Specification. (2002). "*ETSI TS 101 903 V1.1.1 - XML Advanced Electronic Signatures (XAdES)*".

[Hartman03] B. Hartman et al. (2003). "*Mastering Web Services Security*", Wiley Publishing.

[Polemi06a] D. Polemi, S. Papastergiou. (2006). "*A Secure e-Ordering Web Service*", Project E-Society: Building Bricks, Springer Boston, Volume 226/2006.

[Polemi06b] D. Polemi, S. Papastergiou. (2006). "*TOES: Trustful and Open e-Ordering Service for SMEs*", International Conference on Internet Surveillance and Protection, ICISP 2006, August 26 - 29, 2006, Cap Esterel, Côte d'Azur, France.

[Karantjias07a] A. Karantzias, S. Papastergiou, D. Polemi. (2007) "*Innovative, Secure And Interoperable e/m-Governmental Invoicing*", 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), 3-7 September 2007, Athens.

[Papastergiou08a] S. Papastergiou, A. Karantjias, D. Polemi, Markovic M. (2008). "*A Secure Mobile Framework for m-services*", The Third International Conference on Internet and Web Applications and Services (ICIW 2008), June 8-13, 2008 - Athens, Greece.

[Kaliontzoglou06a] A. Kaliontzoglou et al. (2006). "*A formalized design method for building e-government architectures*", Secure e-Government Web Services, Idea Group Publishing, Hershey, PA

[Kaliontzoglou06b] A. Kaliontzoglou, T. Karantjias, D. Polemi. (2006). "*Building innovative, secure and interoperable e-government services*", Secure e-Government Web Services, Idea Group Publishing, Hershey, PA.

[Bourka03a] A. Bourka et al. (2003). "*Enriching healthcare applications with cryptographic mechanisms and XML-based security services*", Technology and Healthcare, IOS Press, Issue 1, Vol. 11, pp. 61-76.

[Bourka03b] A. Bourka et al. (2003). "*PKI-based security of electronic healthcare documents*", SSGRR 2003 Winter Conference, L'Aquilla, Italy

[Georgoulas03] A. Georgoulas et al. (2003). "*RESHEN, a best practice approach for secure healthcare networks in Europe*", Advanced Health Telematics and Telemedicine - The Magdeburg Expert Summit Textbook, Vol. 96 in the "Studies in Health Technology and Informatics", IOS Press.

[High05] R. High, S. Kinder, S. Graham. (2005). "*IBM's SOA Foundation – An architectural Introduction and Overview*", http://www-128.ibm.com/developerworks/webservices/library/ws-soa-whitepaper/.

[Papazoglou07] M. Papazoglou, W. Heuvel. (2007). "*Service Oriented Architectures: Approaches, Technologies and Research Issues*", The VLDB Journal, Vol. 16, Issue 3, pp. 389-415, 2007.

[IDABC] The European Interoperability Framework for pan-European eGovernment Services (IDABC), ISBN 92-894-8389-X, 2004, http://europa.eu.int/idabc/servlets/Doc?id=19528.

[Haddad08] W. Haddad. (2008). "*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*", Network Working Group, IETF Trust.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Kaliontzoglou06c] A. Kaliontzoglou, P. Boutsi, D. Polemi. (2006). "*eInvoke: Secure e-Invoicing based on Web Services*", Electronic Commerce Research Journal, Springer.
[SELIS] Secure Electronic Invoicing Service, eTen, C517381, http://selis.unipi.gr
[Meneklis07] V. Meneklis, S. Papastergiou, C. Douligeris, D. Polemi. (2007). "*Towards advanced e/m-Government platforms*", International Conference on Information Society (i-Society 2007), October 7–11, 2007, Merrillville, Indiana, USA.
[Karantjias08a] A. Karantjias, S. Papastergiou, D. Polemi. (2008). "*Holistic Electronic & Mobile Government Platform Architecture*", 8th Joint Conference on Knowledge - Based Software Engineering 2008 (JCKBSE 08), IOS Press, August 25-28, 2008, Athens, Greece.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2 Διαλειτουργικότητα σε Ασφαλείς και Προηγμένες Ηλεκτρονικές Υπηρεσίες Ιστού

Οι δυνατότητες αλληλεπίδρασης των υπηρεσιών που βασίζονται σε τεχνολογίες XML και πρότυπα Υπηρεσιών Ιστού παραμένουν εξαιρετικά περιορισμένες παρά τη χρήση κοινών τεχνολογιών. Η υλοποίηση διαλειτουργικών υπηρεσιών αλλά και ο αποτελεσματικός έλεγχος της διαλειτουργικότητας των υπηρεσιών αυτών αποτελούν δυο στοιχεία η επίτευξη των οποίων επιτρέπει την αποτελεσματική ανταλλαγή δεδομένων και επιτυγχάνει το διαμοιρασμό πληροφοριών και γνώσης.
Το παρόν κεφάλαιο, λαμβάνοντας υπόψη του τη συγκεκριμένη διαπίστωση επισημαίνει, σε πρώτη φάση, την ανάγκη ύπαρξης διαλειτουργικότητας καθώς και τα οφέλη τα οποία δύναται να αποκομιστούν από την επίτευξη της, ενώ στην συνέχεια παρουσιάζει τις βασικές διαστάσεις οι οποίες πρέπει να ληφθούν υπόψη για την ικανοποίηση της. Ιδιαίτερη έμφαση δίνει επίσης στην μελέτη πρωτοβουλιών και πλαισίων διαλειτουργικότητας τα οποία θέτουν ως βασικό στόχο την προτυποποίηση.
Στη συνέχεια διαπιστώνοντας ότι οι πρωτοβουλίες αυτές δεν μπορούν να εγγυηθούν σε σημαντικό βαθμό τη δυνατότητα επικοινωνίας των υπηρεσιών εξετάζει ένα σύνολο μεθοδολογιών και πλαισίων διαλειτουργικότητας τα οποία ελέγχουν τη συγκεκριμένη δυνατότητα επισημαίνοντας και προσδιορίζοντας τις βασικές τους αδυναμίες, ενώ παράλληλα αναλύει και περιγράφει βασικούς τύπους ελέγχου (ελέγχοι συμμόρφωσης και διαλειτουργικότητας) αλλά και στρατηγικές οι οποίες μπορεί να εφαρμοστούν.
Τέλος το κεφάλαιο αυτό επικεντρώνεται στην παρουσίαση μιας πρωτότυπης, συστηματικής και δομημένης μεθοδολογίας ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ) παραθέτοντας αναλυτικά τις φάσεις και τα στάδια από τα οποία η προτεινόμενη μεθοδολογία αποτελείται.

2.1 Εισαγωγή

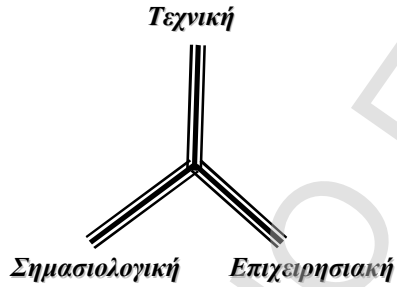
Τα τελευταία χρόνια έχει παρατηρηθεί μια εστίαση τόσο της επιστημονικής όσο και της επιχειρηματικής κοινότητας σε ζητήματα που αφορούν τη δυνατότητα επικοινωνίας μεταξύ οργανισμών οι οποίοι διαθέτουν διαφορετικά πληροφοριακά και επικοινωνιακά συστήματα. Η προσπάθεια αυτή έχει θέσει στο επίκεντρο του ενδιαφέροντός της την επίτευξη της διαλειτουργικότητας των συστημάτων αυτών. Βασική της επιδίωξη είναι η διερεύνηση και ο καθορισμό μεθόδων (προτύπων και προδιαγραφών) με τους οποίους μπορεί να επιτευχθεί η ασφαλής ανταλλαγή δεδομένων μεταξύ των οργανισμών εγκαθιστώντας ισχυρούς δεσμούς συνεργασίας και συνύπαρξης.
Με τον όρο διαλειτουργικότητα έχει οριστεί *"η δυνατότητα των πληροφοριακών και επικοινωνιακών συστημάτων καθώς επίσης και των υποστηριζόμενων επιχειρησιακών διαδικασιών να ανταλλάσουν δεδομένα επιτρέποντας τη διανομή τόσο των πληροφοριών όσο και της γνώσης"* [EIF]. Η αξία, λοιπόν, της επίτευξης της διαλειτουργικότητας είναι ιδιαίτερα σημαντική και τα οφέλη τα οποία δύναται να αποκομιστούν από αυτή σε παγκόσμιο επίπεδο μπορεί να συνοψιστούν στα ακόλουθα [Lueders]:

- Η διαλειτουργικότητα υποστηρίζει τη δημιουργία μιας παγκόσμιας αγοράς (Single Market) ευνοώντας την ελεύθερη μετακίνηση ανθρώπων, κεφαλαίων, αγαθών και υπηρεσιών παρέχοντας τη δυνατότητα διεκπεραίωσης πολύπλοκων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ηλεκτρονικών συναλλαγών ανάμεσα σε διαφορετικούς επιχειρηματικούς φορείς.

- Η διαλειτουργικότητα αποτελεί έναν σημαντικό οδηγό-παράγοντα που μπορεί να ωθήσει την παγκόσμια οικονομία επιφέροντας την ουσιαστική οικονομική ανάπτυξη και δίνοντας μια περαιτέρω ώθηση στην αύξηση της παραγωγικότητας.
- Η διαλειτουργικότητα μπορεί να αυξήσει την ποιότητα, την ευελιξία και την συνδεσιμότητα των παρεχόμενων υπηρεσιών μειώνοντας το κόστος διαχείρισης και ανάπτυξής τους. Επίσης επιτρέπει την ομαλή διανομή και επαναχρησιμοποίηση πληροφοριών με τέτοιο τρόπο ώστε να επιτυγχάνεται η εξάλειψη των χρονοβόρων διαδικασίων και να πραγματοποιείται η καταπολέμηση της γραφειοκρατίας που αποτελεί τη βασική μάστιγα του παλιού έντυπου κόσμου.



Σχήμα 4. Διαστάσεις Διαλειτουργικότητας

Επομένως, η ανάγκη ύπαρξης ενός κοινού πλαισίου διαλειτουργικότητας στα πλαίσια του οποίου οι οργανισμοί δύναται να αλληλεπιδρούν με επιτυχία είναι ιδιαίτερα έκδηλη και επιτακτική. Στο Σχήμα 4 απεικονίζονται οι τρεις βασικές διαστάσεις της διαλειτουργικότητας, οι οποίες θα πρέπει να ληφθούν υπόψη για τη δημιουργία ενός τέτοιου πλαισίου. Αναλυτικότερα, οι διαστάσεις αυτές είναι οι ακόλουθες [IDABC]:

- ***Τεχνική Διαλειτουργικότητα***: Η πτυχή αυτή καλύπτει τα τεχνικά ζητήματα που αφορούν την συνδεσιμότητα των υπολογιστικών συστημάτων και υπηρεσιών. Περιλαμβάνει τον καθορισμό των απαραίτητων διεπαφών, προτύπων και πρωτοκόλλων, αλλά και τον προσδιορισμό της απαιτούμενης αναπαράστασης των δεδομένων που θεωρούνται αναγκαίες για τη δημιουργία ασφαλών, αξιόπιστων, αποτελεσματικών, εύκολα προσβάσιμων και αποδοτικών πληροφοριακών συστημάτων και υπηρεσιών.
- ***Σημασιολογική Διαλειτουργικότητα:*** Η πτυχή αυτή εστιάζει στο να εξασφαλίσει ότι οι ανταλλασσόμενες πληροφορίες είναι νοηματικά κατανοητές από οποιαδήποτε υπηρεσία/εφαρμογή η οποία δεν αναπτύχθηκε αρχικά για το σκοπό αυτό. Η σημασιολογική διαλειτουργικότητα επιτρέπει στις υπηρεσίες/εφαρμογές αυτές να συνδυάσουν τις λαμβανόμενες πληροφορίες με άλλες πηγές πληροφοριών, επιτυγχάνοντας την περαιτέρω επεξεργασία τους. Επομένως, η πτυχή αυτή μπορεί να θεωρηθεί ως βασικό προαπαιτούμενο για την επιτυχή επικοινωνία υπηρεσιών που χρησιμοποιούν διαφορετικό λεξιλόγιο.
- ***Επιχειρησιακή Διαλειτουργικότητα:*** Η πτυχή αυτή επικεντρώνεται στον καθορισμό των επιχειρησιακών στόχων και τη διαμόρφωση των επιχειρησιακών διαδικασιών έτσι ώστε να επιτευχθεί η συνεργασία υπηρεσιών/εφαρμογών οι οποίες επιθυμούν την ανταλλαγή πληροφοριών και οι οποίες διαθέτουν διαφορετικές εσωτερικές δομές και διαδικασίες. Επιπλέον, η

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

επιχειρησιακή διαλειτουργικότητα θέτει ως βασικό στόχο της τη δημιουργία διαθέσιμων και εύκολα προσβάσιμων υπηρεσιών/εφαρμογών.

Ένα πλήρως ορισμένο πλαίσιο διαλειτουργικότητας για καθεμία από τις προαναφερθείσες διαστάσεις απαιτεί τον καθορισμό ενός συγκεκριμένου συνόλου προτύπων και οδηγιών στα οποία πρέπει να βασίζεται. Στο κεφάλαιο που ακολουθεί πραγματοποιείται μια παρουσίαση των πιο αντιπροσωπευτικών πρωτοβουλιών που στοχεύουν στην παραγωγή προτύπων αλλά και πλαισίων διαλειτουργικότητας. Η παρούσα διατριβή έχει εστιαστεί στις δύο διαστάσεις της διαλειτουργικότητας την τεχνική και την επιχειρησιακή.

2.2 Υπάρχουσα Κατάσταση – Ανοιχτά Προβλήματα

2.2.1 Πρότυπα και Εθνικά Πλαίσια Διαλειτουργικότητας

Το πρώτο και σημαντικότερο ίσως βήμα προς την επίτευξη της διαλειτουργικότητας και τη δημιουργία ενός κοινού πλαισίου είναι η προτυποποίηση. Η ύπαρξη ενός συνόλου οργανισμών προτυποποίησης ή ακόμα και η συνεργασία οργανισμών που δραστηριοποιούνται στον επιχειρηματικό κόσμο για τη δημιουργία τεχνικών επιτροπών με στόχο την πρόταση και δημιουργία νέων προτύπων και πλαισίων αναφοράς αναδεικνύουν το σημαντικό ρόλο της προτυποποίησης στη διαλειτουργικότητα.
Ένα σύνολο αντιπροσωπευτικών παραδειγμάτων αυτού του είδους είναι τα ακόλουθα:

- Η κοινοπραξία World Wide Web (W3C) [W3C] έχει αναπτύξει τεχνολογίες (πρότυπα, οδηγίες, λογισμικό, και εργαλεία) που προωθούν τη διαλειτουργικότητα και την ασφάλεια στο Διαδίκτυο. Η Extensible Markup Language (XML) [XML] και όλες οι τεχνολογίες οι οποίες βασίζονται σε αυτή, όπως είναι οι Υπηρεσίες Ιστού (Web Services) [Booth04], προσφέρουν μια προτυποποιημένη μέθοδο αναπαράστασης των δεδομένων στα πληροφοριακά συστήματα αλλά και ανταλλαγής αυτών με τη χρήση πρότυπων μηνυμάτων. Επίσης έχει ανακοινώσει πρότυπα για εφαρμογή XML ψηφιακών υπογραφών [XML-DSig] και κρυπτογράφησης [XML-Enc] (XML Signature and Encryption) τα οποία συνδυάζουν την XML με την εφαρμογή κρυπτογραφικών μεθόδων που βασίζονται στην Υποδομή Δημόσιας Κλείδας (ΥΔΚ) [Adams99].
- Ο οργανισμός OASIS [OASIS] αποτελεί μια μη-κερδοσκοπική κοινοπραξία που συμβάλλει στην ανάπτυξη, σύγκλιση και θέσπιση προτύπων (π.χ. WS-Security [Nadalin06, WSS]) για το ηλεκτρονικό εμπόριο.
- Η Electronic Business using eXtensible Markup Language (ebXML) [ebXML] συνθέτει ένα σύνολο προδιαγραφών που επιτρέπει στις επιχειρήσεις οποιουδήποτε μεγέθους και ανεξαρτήτως γεωγραφικής θέσης να δραστηριοποιηθούν στο Διαδίκτυο. Η ebXML παρέχει στις επιχειρήσεις έναν τυποποιημένο τρόπο ανταλλαγής επιχειρησιακών μηνυμάτων που βασίζονται σε τεχνολογίες της XML και των Υπηρεσιών Ιστού.
- Η RosettaNet [RosettaNet] αποτελείται από προδιαγραφές για το ηλεκτρονικό εμπόριο εστιάζοντας στη διαχείριση αλυσίδων εφοδιασμού.
- Οι xCBL [xCBL03], BASDA [eBIS-XML], UBL [UBL1.0] και OAGIS [Rowell] αποτελούν χαρακτηριστικά παραδείγματα οργανισμών που έχουν καθορίσει συγκεκριμένα XML σχήματα για την αναπαράσταση των δεδομένων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η ακαδημαϊκή και η επιχειρηματική κοινότητα έχουν να επιδείξουν μέχρι στιγμής ένα σύνολο προτύπων και πλαισίων αναφοράς που βοηθούν στη δημιουργία ασφαλών και διαλειτουργικών συστημάτων, τόσο σε επίπεδο προδιαγραφής συγκεκριμένων υπηρεσιών, μηχανισμών ή πρωτοκόλλων, όσο και σε ένα συνολικότερο επίπεδο σχεδιασμού ολοκληρωμένων υπολογιστικών συστημάτων.

Πέρα βέβαια από τον καθορισμό συγκεκριμένων προτύπων και προδιαγραφών, χαρακτηριστική είναι η προσπάθεια η οποία παρατηρείται σε πολλά κράτη για τη δημιουργία εθνικών πλαισίων διαλειτουργικότητας. Η βασική επιδίωξη αυτών των πλαισίων τα οποία βασίζονται σε ευρέως διαδεδομένα και αποδεκτά πρότυπα γνωστών οργανισμών προτυποποίησης είναι η βελτίωση της αποτελεσματικότητας και της ευελιξίας των προσφερόμενων υπηρεσιών. Ενδεικτικά παραδείγματα εθνικών πλαισίων διαλειτουργικότητας στο χώρο της ηλεκτρονικής διακυβέρνησης [EC03] είναι τα ακόλουθα:

- Το πλαίσιο διαλειτουργικότητας για την ηλεκτρονική Διακυβέρνηση του Ηνωμένου Βασιλείου (UK government's eGovernment Interoperability Framework (eGif)) [eGif] το οποίο ορίζει τις πολιτικές και τις τεχνικές προδιαγραφές που θα ενεργήσουν ως βάση της στρατηγικής για την η-Διακυβέρνηση.
- Το πλαίσιο διαλειτουργικότητας της Γαλλικής Κυβέρνησης (French government's 'Cadre commun d'interopérabilité (CCI)') [ADAE] που έχει ως σκοπό να υποστηρίξει τη συνεργασία μεταξύ της κεντρικής διοίκησης και των τοπικών αρχών, και ιδιαίτερα στον τομέα των η-υπηρεσιών που παρέχονται στους πολίτες και στις επιχειρήσεις.
- Το πλαίσιο διαλειτουργικότητας της Γερμανικής Κυβέρνησης (German government's SAGA framework) [SAGA] το οποίο διευκρινίζει τα πρότυπα και την αρχιτεκτονική που πρόκειται να υιοθετηθούν από τη Γερμανική Ομοσπονδιακή Κυβέρνηση για την η-διακυβέρνηση.
- Το υπουργείο Επιστημών, Τεχνολογίας και Καινοτομίας της Δανίας (Danish Ministry of Science, Technology and Innovation's national white paper on enterprise architecture) [Danish] το οποίο συστήνει την υιοθέτηση ενός προσανατολισμένου στις υπηρεσίες προτύπου αρχιτεκτονικής για το σχεδιασμό καλώς-ορισμένων υπηρεσιών.
- Η Συμβουλευτική Επιτροπή της Φινλανδίας για τη διαχείριση πληροφοριών στη δημόσια διοίκηση (Finland's Advisory Committee on Information Management in Public Administration, JUHTA) [JUHTA] η οποία εστιάζει στον εντοπισμό και την ταξινόμιση των προτύπων ανταλλαγής και αναπαράστασης της δομής και του περιεχομένου των δεδομένων.
- Ο Κατάλογος Προτυποποίησης και Ανοικτού Λογισμικού της Ολλανδικής Κυβέρνησης (Netherlands's government catalogue 'Open Standaarden en Open Source Software voor de overheid (OSOSS)') [OSOSS] ο οποίος παρουσιάζει τα πρότυπα που μπορούν να χρησιμοποιηθούν στις εφαρμογές η-διακυβέρνησης.
- Τα Κριτήρια που έχουν θεσπιστεί από την Ισπανική Κυβέρνηση (Spanish government's Criteria for security, standardization and preservation of information of applications) [ORDENPRE] τα οποία περιλαμβάνουν τις νομικές απαιτήσεις και τις αντίστοιχες τεχνικές και επιχειρησιακές προδιαγραφές που πρέπει να ληφθούν υπόψη από τη δημόσια διοίκηση.
- Το "Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας" [ΠΗΔ] καθορίζει τις γενικές αρχές και τη στρατηγική που θα πρέπει να διέπει την ανάπτυξη πληροφοριακών συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

από φορείς της Ελληνικής Δημόσιας Διοίκησης, καθώς επίσης και των τεχνολογικών προτύπων βάσει των οποίων πρέπει να αναπτύσσονται τα πληροφοριακά συστήματα, με στόχο την υποστήριξη τόσο της ανταλλαγής δεδομένων μεταξύ συστημάτων όσο και της παροχής ολοκληρωμένων υπηρεσιών Ηλεκτρονικών Συναλλαγών προς τους Πολίτες, τις Επιχειρήσεις ή άλλους Φορείς.

Αντίστοιχα, η Ευρωπαϊκή Ένωση αναγνωρίζοντας τη σημασία της διαλειτουργικότητας σε ευρωπαϊκό επίπεδο έχει αναπτύξει και υποστηρίζει ένα σύνολο από πρωτοβουλίες που επικεντρώνονται στην ενίσχυση της προτυποποίησης και ευννοούν τη δημιουργία πλαισίων διαλειτουργικότητας. Στην συνέχεια παρατίθενται ένα σύνολο αντιπροσωπευτικών πρωτοβουλιών:

- Οι ευρωπαϊκοί οργανισμοί προτυποποίησης, CEN [CEN] και ETSI [ETSI] έχουν αναπτύξει ένα Κυλιόμενο Σχέδιο Δράσης για την Προτυποποίηση (Rolling Standardisation Action Plan) [SAPE] ώστε να υποστηριχθούν οι πρωτοβουλίες που αναπτύσσονται σε ευρωπαϊκό επίπεδο. Στόχος του σχεδίου αυτού αποτελεί η βελτίωση και η επιτάχυνση των δρώμενων που αφορούν την προτυποποίηση σε ευρωπαϊκό επίπεδο και η εξασφάλιση της συμμετοχής όλων των κρατών μελών σε αυτή.
- Η Γενική Διεύθυνση της Κοινωνίας της Πληροφορίας (DG Information Society & Media) [DGISM] εξετάζει τη διαλειτουργικότητα μέσα στο ευρύτερο πλαίσιο της κοινωνίας των πληροφοριών. Εστιάζει σε ζητήματα που σχετίζονται με τη διαλειτουργικότητα υπηρεσιών και εφαρμογών τα οποία προσφέρονται μέσω πλατφόρμων της ψηφιακής τηλεόρασης και της τρίτης γενιάς κινητών τηλεπικοινωνιών, προτείνοντας και παρουσιάζοντας μια ολοκληρωμένη πλατφόρμα.
- Η Γενική Επιχειρησιακή Διεύθυνση (DG Enterprise) [DGE] υπό την επίβλεψη του προγράμματος "Ανταλλαγής Δεδομένων μεταξύ των Οργανισμών Δημόσιας Διοίκησης" ("Interchange of Data between Administrations (IDA)") [IDA] επιχειρεί τον καθορισμό συγκεκριμένων μέτρων και ενεργειών που εξασφαλίζουν τη διαλειτουργικότητα μεταξύ των υπηρεσιών της ηλεκτρονικής διακυβέρνησης σε ευρωπαϊκό επίπεδο. Απώτερο στόχο αποτελεί η επίτευξη της ομαλής και ευέλικτης ανταλλαγής πληροφοριών ανάμεσα στους δημόσιους οργανισμούς. Στα πλαίσια της πρωτοβουλίας αυτής έχει αναπτυχθεί και το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Interoperability Framework (EIF)) [EIF] που επικεντρώνεται στο να συμπληρώσει παρά να αντικαταστήσει τα εθνικά πλαίσια διαλειτουργικότητας μέρος των οποίων αναφέρθηκαν προηγουμένως προσδίδοντας την πανευρωπαϊκή διάσταση.
- Το CEN/ISSS "European eBusiness Interoperability Forum" (eBIF) [eBIF] αποτελεί ένα ευρωπαϊκό σημείο εστίασης για τα ζητήματα προτυποποίησης σχετικά με το ηλεκτρονικό εμπόριο υποβάλλοντας στρατηγικές συστάσεις. Προτείνοντας γενικές αρχές, το eBIF προωθεί τη διατομεακή διαλειτουργικότητα του ηλεκτρονικού εμπορίου με την παροχή μιας πλατφόρμας για την ανταλλαγή απόψεων και εμπειριών στο πεδίο της προτυποποίησης του ηλεκτρονικού εμπορίου.

Το στοιχείο το οποίο πρέπει να τονιστεί είναι ότι οι προαναφερθείσες πρωτοβουλίες στο σύνολο τους εστιάζονται είτε στο να προτείνουν πρότυπα και προδιαγραφές είτε στο να καθορίσουν τις οδηγίες που θα πρέπει να διέπει ένα πλαίσιο διαλειτουργικότητας. Σε καμμιά περίπτωση όμως δεν δύναται να εγγυηθούν ότι οι

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

οργανισμοί οι οποίοι έχουν υιοθετήσει και υλοποιούν τα πρότυπα και τις οδηγίες τα εφαρμόζουν και τα ακολουθούν πιστά καλύπτοντας πλήρως το σύνολο των πτυχών που προσδιορίζονται από αυτά. Το γεγονός αυτό αποτελεί ένα εμπόδιο στην επίτευξη της διαλειτουργικότητας, καθώς μόνο ο καθορισμός προτύπων και οδηγιών δεν μπορεί σε καμμία περίπτωση να εξασφαλίσει ότι οι οργανισμοί μπορούν τελικά να επικοινωνήσουν μεταξύ τους επιτυχώς, χωρίς την ακριβή μοντελοποίηση ή τη συγκεκριμένη αλγοριθμική αποτίμηση των βημάτων που πρέπει να ακολουθηθούν ώστε να ελεγχθεί η ορθή υλοποίηση του προτύπου.

2.2.2 Διαλειτουργικότητα Υπηρεσιών Ιστού

Ο πρώτος άξονας της διατριβής επικεντρώνεται κυρίως σε ζητήματα τα οποία αφορούν την διαλειτουργικότητα των ασφαλών και προηγμένων ηλεκτρονικών Υπηρεσιών Ιστού (ΥΙ) οι οποίες βασίζονται σε τεχνολογίες όπως είναι η Υποδομή Δημόσιας Κλείδας (Υ.Δ.Κ.) και σε πρότυπα της XML και των Υπηρεσιών Ιστού. Οι ΥΙ αυτές μπορούν να προσφέρονται είτε ως αυτόνομες Υπηρεσίες Ιστού είτε ενσωματωμένες σε μια Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ).

Εντούτοις, παρά την υιοθέτηση και χρήση κοινών προτύπων από τις ΥΙ το στοιχείο που κυριαρχεί είναι ότι οι δυνατότητες αλληλεπίδρασής τους παραμένουν εξαιρετικά περιορισμένες. Το γεγονός αυτό οφείλεται σημαντικά στον τρόπο με τον οποίο οι υπεύθυνοι για την ανάπτυξη των υπηρεσιών αντιλαμβάνονται, υλοποιούν και ενσωματώνουν τα υιοθετημένα πρότυπα στις υπηρεσίες τους.

Επομένως, η διευθέτηση των ζητημάτων της διαλειτουργικότητας μεταξύ των υπηρεσιών οι οποίες βασίζονται σε τεχνολογίες XML δεν επιτυγχάνεται αποκλειστικά με τον καθορισμό ενός συνόλου από χρησιμοποιούμενα πρότυπα και τον προσδιορισμό των οδηγιών που πρέπει να ακολουθηθούν. Πρέπει να επισημανθεί ότι τα στοιχεία αυτά κρίθηκαν ως πρωταρχικά για τον καθορισμό ενός πλαισίου διαλειτουργικότητας (βλ. § 2.1 και 2.2).

Έκδηλη, λοιπόν είναι η ανάγκη ύπαρξης και χρήσης μεθοδολογιών και πλαισίων τα οποία ελέγχουν και εγγυώνται τη δυνατότητα επικοινωνίας των ΥΙ. Αυτό μπορεί να πραγματοποιηθεί μέσω της εφαρμογής ελέγχων οι οποίοι εξετάζουν τη συμμόρφωση των υπηρεσιών αυτών ως προς τα πρότυπα τα οποία χρησιμοποιούν αλλά και άμεσων ελέγχων που διαπιστώνουν την απευθείας δυνατότητα επικοινωνίας των εμπλεκόμενων υπηρεσιών. Το στοιχείο που πρέπει να τονιστεί είναι ότι οι υπάρχουσες μεθοδολογίες στην πλειοψηφία τους παρουσιάζουν ουσιαστικές αδυναμίες αποτυγχάνοντας να καλύψουν το σύνολο των πτυχών που συνθέτουν ένα πλαίσιο διαλειτουργικότητας.

Κρίνεται λοιπόν επιτακτική η ανάγκη δημιουργίας μιας νέας τυπικής και δομημένης μεθοδολογίας ελέγχου Υπηρεσιών Ιστού. Για την επιτυχή επίτευξη του συγκεκριμένου στόχου κρίσιμη θεωρείται και η μελέτη των υπαρχόντων στρατηγικών ελέγχου ώστε να επιλεγεί και να υιοθετηθεί η βέλτιστη δυνατή. Ιδιαίτερη βαρύτητα για τη συγκεκριμένη επιλογή θα πρέπει να δοθεί στην ίδια τη φύση των ΥΙ αλλά και στις προκλήσεις οι οποίες προκύπτουν από αυτήν.

Στις παραγράφους που ακολουθούν πραγματοποιείται η παράθεση των υπαρχόντων μεθοδολογιών και πλαισίων ελέγχων παρουσιάζοντας τις αδυναμίες τους. Παράλληλα περιγράφονται οι πιο ευρέως χρησιμοποιούμενες στρατηγικές ελέγχου επισημαίνοντας την πιο κατάλληλη η οποία μπορεί να εφαρμοστεί στην περίπτωση των ΥΙ λαμβάνοντας υπόψη τα εγγενή χαρακτηριστικά τους.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.2.3 Μεθοδολογίες Ελέγχου και Αδυναμίες

Παραδοσιακά, οι μεθοδολογίες ελέγχου έχουν χρησιμοποιηθεί εκτενώς στη βιομηχανία των τηλεπικοινωνιών και στον κόσμο του Διαδικτύου. Βασικό τους στόχο αποτελεί ο έλεγχος της αποτελεσματικής επικοινωνίας υπηρεσιών/εφαρμογών αλλά και σε πιο ευρεία έννοια προϊόντων τα οποία υλοποιούν συγκεκριμένες προδιαγραφές και πρότυπα.

Για την ασφαλή επίτευξη του στόχου αυτού δύναται να χρησιμοποιηθεί μια μεγάλη ποικιλία ελέγχων όπως ποιότητας, απόδοσης, μηχανικής ανθεκτικότητας, ηλεκτρικής ασφάλειας, πίεσης, φορτίου και ηλεκτρομαγνητικών εκπομπών. Πρακτικά, όμως, δύο είναι οι τύποι ελέγχου οι οποίοι χρησιμοποιούνται ευρέως από τις μεθοδολογίες, ο *έλεγχος συμμόρφωσης* και ο *έλεγχος διαλειτουργικότητας*.

Οι δύο αυτοί τύποι παρά το γεγονός ότι είναι ανεξάρτητοι μεταξύ τους συνδέονται στενά επιτυγχάνοντας να καλύψουν σε μεγάλο βαθμό τις αδυναμίες ο ένας του άλλου [Kulvatunyou03, Dibuz03]. Ο έλεγχος συμμόρφωσης εξετάζει εάν μια υπηρεσία/εφαρμογή καλύπτει (και έως πιο σημείο) ή όχι όλες τις απαιτήσεις οι οποίες καθορίζονται από τα αντίστοιχα πρότυπα. Παραδείγματος χάριν, εξετάζει το περιεχόμενο και το σχήμα των ανταλλασσόμενων μηνυμάτων καθώς επίσης και την επιτρεπόμενη ακολουθία των μηνυμάτων αυτών. Με αυτόν τον τρόπο δύναται να ελεγχθεί η ορθή εφαρμογή ενός συγκεκριμένου προτύπου. Αντίστοιχα, ο έλεγχος διαλειτουργικότητας προσπαθεί να καταδείξει την ομαλή συνύπαρξη ομοειδών υπηρεσιών/εφαρμογών αξιολογώντας τη δυνατότητά τους να αλληλεπιδράσουν και να λειτουργήσουν επιτυχώς χρησιμοποιώντας τα πρότυπα και τις προδιαγραφές τις οποίες έχουν υιοθετήσει.

Το στοιχείο που πρέπει να σημειωθεί είναι ότι οι δύο τύποι ελέγχων παρουσιάζουν μια σειρά ευδιάκριτων διαφορών κυρίως ως προς τους στόχους που επιχειρούν να καλύψουν. Επομένως η χρησιμοποίηση ενός από αυτούς τους τύπους δεν μπορεί να εγγυηθεί σε καμία περίπτωση τη δυνατότητα επικοινωνίας των υπηρεσιών/εφαρμογών καθώς τα αποτελέσματα τα οποία λαμβάνονται από καθέναν από αυτούς δεν παρέχουν επαρκείς αποδείξεις.

Ως απόδειξη του στοιχείου αυτού μπορεί να θεωρηθεί το γεγονός κατά το οποίο ο έλεγχος διαλειτουργικότητας δύο ή περισσότερων υπηρεσιών/εφαμογών μπορεί να αποτύχει ακόμα και στην περίπτωση κατά την οποία οι τελευταίες περάσουν επιτυχώς τους ελέγχους συμμόρφωσης. Αυτό ενδέχεται να συμβεί λόγω της εφαρμογής μιας μη επαρκώς ορισμένης διαδικασίας ελέγχου συμμόρφωσης η οποία δεν μπορεί να εντοπίσει ότι οι υπηρεσίες/εφαρμογές δεν υποστηρίζουν κάποια προαιρετικά στοιχεία όπως αυτά επιβάλλονται από τα αντίστοιχα πρότυπα προκαλώντας με αυτόν τον τρόπο προβλήματα διαλειτουργικότητας.

Ομοίως, υπάρχει η πθανότητα δύο ή περισσότερες υπηρεσίες/εφαρμογές να αλληλεπιδρούν επιτυχώς παρά το γεγονός ότι μία από αυτές ή και όλες αποτυγχάνουν στον έλεγχο συμμόρφωσης. Το γεγονός αυτό οφείλεται στο ότι κατά την διάρκεια του ελέγχου διαλειτουργικότητας δεν δύναται να εξεταστεί το σύνολο των πτυχών των αντίστοιχων προτύπων. Οι πτυχές αυτές μπορεί να εξεταστούν μόνο μέσω του ελέγχου συμμόρφωσης. Επίσης υπάρχει και η πιθανότητα όλες οι υπηρεσίες/εφαρμογές να αντιλαμβάνονται και να υλοποιούν τα πρότυπα κατά τον ίδιο λανθασμένο τρόπο.

Ουσιαστικά, λοιπόν, η βέλτιστη πρακτική επιβάλλει την εφαρμογή και των δύο τύπων ελέγχου ως μοναδικό μέτρο για την παροχή μιας επιτυχούς διαλειτουργικής αξιολόγησης η οποία θα εξασφαλίσει σε βάθος την επιτυχή αλληλεπίδραση και λειτουργία των εξεταζόμενων υπηρεσιών/εφαρμογών. Στην πράξη, ο έλεγχος συμμόρφωσης προηγείται πάντοτε, παρέχοντας τις απαραίτητες αποδείξεις

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συμμόρφωσης και τις αναγκαίες εγγυήσεις αλληλεσύνδεσης, ενώ ο έλεγχος διαλειτουργικότητας έπεται προσφέροντας μια πιο ολοκληρωμένη εικόνα. Παρόλα αυτά πρέπει να επισημανθεί ότι συνήθης πρακτική είναι η χρησιμοποίηση ενός μόνο από τους δύο προαναφερθέντες ελέγχους.

Ένα σύνολο, λοιπόν, οργανισμών προτυποποίησης αναγνωρίζοντας τη σημασία της ύπαρξης και λειτουργίας μεθοδολογιών που στοχεύουν στον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης υπηρεσιών/εφαρμογών ως βασικό παράγοντα αρμονικής συνύπαρξης και ομαλής επικοινωνίας αυτών σε ένα κοινό πλαίσιο, προτείνουν και υιοθετούν μεθοδολογίες και πλαίσια ελέγχου. Οι πιο ευρέως διαδεδομένες μεθοδολογίες ελέγχου συνοψίζονται στις ακόλουθες:

- Η Open Systems Interconnection - Conformance Testing Methodology and Framework (ISO/IEC 9646) [OSI97] αποτελεί μια ευρέως και επιτυχώς εφαρμοσμένη μεθοδολογία ελέγχου συμμόρφωσης που έχει εξελιχθεί σε μεγάλο βαθμό στο πέρασμα των χρόνων. Έχει σχεδιαστεί κατά κύριο λόγο για τον έλεγχο της συμμόρφωσης των πρωτοκόλλων OSI. Εντούτοις, θεωρείται ως πολύ ανοικτό πλαίσιο προσφέροντας έναν ιδιαίτερα υψηλό βαθμό ελευθερίας στον αρμόδιο για την εφαρμογή της, ενώ παράλληλα παρέχει λίγες πρακτικές οδηγίες [ETSI96].
- Το European Telecommunications Standards Institute (ETSI) [ETSI] έχει προτείνει ένα ολοκληρωμένο πλαίσιο το οποίο αποτελείται από δύο τύπους ελέγχων, τον έλεγχο συμμόρφωσης και τον έλεγχο διαλειτουργικότητας.
  - Ο έλεγχος συμμόρφωσης του ETSI [Moseley03, ETSI95] βασίζεται στο ISO/IEC 9646 χρησιμοποιώντας τις αρχές του ως βάση, αλλά όχι ως ακριβείς οδηγίες. Εστιάζει στην παραγωγή ευκολότερων, πιό εφαρμόσιμων και πιό αναγνώσιμων ακολουθιών ελέγχου, ενώ μπορεί να εφαρμοστεί για τον έλεγχο συμμόρφωσης ενός μεγαλύτερου εύρους πρωτοκόλλων από ότι το ISO/IEC 9646. Γα το σκοπό αυτό το ETSI καθόρισε μια κεντρική γλώσσα, την Testing and Test Control Notation (TTCN-3) [ETSI02] που μπορεί να χρησιμοποιηθεί για τον καθορισμό ακολουθιών ελέγχου που είναι ανεξάρτητες από τις μεθόδους, τα στρώματα και τα πρωτόκολλα υπό εξέταση. Η TTCN-3 έχει χρησιμοποιηθεί [Dibuz03] ακόμα και για την αναπαράσταση και εκτέλεση ακολουθιών ελέγχου για YI. Οι περιπτώσεις ελέγχου οι οποίες καθορίστηκαν δεν πετυχαίνουν να καλύψουν το σύνολο των πτυχών ελέγχου. Παρέχουν μόνο μια περιγραφή των ανταλλασσόμενων πληροφοριών και της ακολουθίας των μηνυμάτων χωρίς να μπορούν να καλύψουν περιπτώσεις όπως είναι η συμβατότητα των μηνυμάτων αυτών ως προς τις αντίστοιχες περιγραφές των υπηρεσιών ή τη συμβατότητα των περιγραφών αυτών ως προς τα αντίστοιχα πρότυπα.
  - Ο έλεγχος διαλειτουργικότητας του ETSI [ETSI07] παρέχει μια γενική προσέγγιση που καθορίζει μόνο γενικές οδηγίες σχετικά με την προδιαγραφή και την εκτέλεση των ελέγχων διαλειτουργικότητας. Αυτές οι οδηγίες είναι υπό μορφή συστάσεων περισσότερο παρά σαφών κανόνων. Η TTCN-3 δύναται επίσης να χρησιμοποιηθεί και σε αυτό το είδος ελέγχου προσφέροντας ένα υψηλότερο επιπέδο ευελιξίας.

Το πιο σημαντικό μειονέκτημα και των ανωτέρω μεθοδολογιών είναι ότι αντιμετωπίζουν τον έλεγχο διαλειτουργικότητας και συμμόρφωσης των YI ως τμήμα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

μιας γενικής μεθόδου ελέγχου της δυνατότητας επικοινωνίας πρωτοκόλλων και γενικά εφαρμογών. Αδυνατούν να εστιάσουν στις ιδιαιτερότητες που έχουν οι YI και αποφεύγουν να επισημάνουν συγκεκριμένες πτυχές οι οποίες πρέπει να ελεγχθούν, γεγονός που αφήνεται στην διακριτική ευχέρεια των αρμόδιων που διεξάγουν τον έλεγχο. Παρέχουν μόνο γενικές οδηγίες και περιγράφουν υψηλού επιπέδου διαδικασίες ελέγχου που δύναται να εφαρμοστούν για τον έλεγχο της διαλειτουργικότητας διαφόρων τηλεπικοινωνιών και πληροφοριακών συστημάτων. Αναδεικνύεται λοιπόν η ανάγκη για μεθοδολογίες προσανατολισμένες στις YI οι οποίες υιοθετούν διαδικασίες και ελέγχους που επιχειρούν να καλύψουν ένα μεγάλο εύρος των πραγματικών διαστάσεων των υπηρεσιών αυτών.

Αυτή τη στιγμή, υφίστανται μόνο δύο ευρέως διαδεδομένες μεθοδολογίες οι οποίες εστιάζονται αποκλειστικά στον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης των YI. Οι μεθοδολογίες αυτές περιορίζονται στις ακόλουθες:

- Ο Οργανισμός Προτυποποίησης Διαλειτουργικότητας Υπηρεσιών Ιστού (Web Service Interoperability Standardization Organization (WS-I)) [Seely05, Ehnebuske03] αποτελεί μια επιχειρηματική κοιναπραξία που έχει θέσει ως βασικό της σκοπό την προώθηση της διαλειτουργικότητας των YI μεταξύ διαφορετικών λειτουργικών συστημάτων, πλατφορμών και γλωσσών προγραμματισμού. Βασικό του μέλημα αποτελεί να συμβάλλει αποφασιστικά στην ανάπτυξη διαλειτουργικών YI με την παροχή οδηγιών, προτεινόμενων πρακτικών πόρων αλλά και ενός συνόλου εργαλείων ελέγχου τα οποία την καθιστούν ένα ολοκληρωμένο και ευέλικτο περιβάλλον ελέγχου. Τα μειονεκτήματα της συγκεκριμένης μεθοδολογίας τα οποία εντοπίστηκαν είναι τα ακόλουθα:
    1. Δεν προσφέρεται η δυνατότητα καθορισμού και εκτέλεσης συγκεκριμένων ακολουθιών ελέγχου.
    2. Τα εργαλεία ελέγχου από τα οποία αποτελείται κρατούν μια πιο παθητική στάση παρατηρώντας απλά τη ροή των ανταλλασσόμενων μηνυμάτων.
    3. Δεν καλύπτεται ο έλεγχος της διαλειτουργικότητας και της συμμόρφωσης των εφαρμοζόμενων μηχανισμών ασφάλειας σε επίπεδο περιεχομένου των μηνυμάτων.
    4. Αποτελεί περισσότερο ένα πλαίσιο ελέγχου και όχι μια μεθοδολογία αλγοριθμική και κατασκευαστική.
- Η OASIS EBXML [ebXML01] αποτελεί ένα Business to Business (B2B) XML πλαίσιο το οποίο παρέχει συγκεκριμένες προδιαγραφές για δυναμικές συνεργασίες B2B. Έχει καθορίσει το πλαίσιο ελέγχου Εφαρμογής, Διαλειτουργικότητας και Συμμόρφωσης (Implementation, Interoperability, and Conformance (IIC)) [ebXML03, Lee05, Kim03] για το οποίο έχει προσδιοριστεί η υιοθετημένη αρχιτεκτονική ενώ έχουν προδιαγραφεί ακολουθίες ελέγχου όπως και γλώσσες για την αναπαράσταση των απαιτήσεων και ακολουθιών ελέγχου. Τα μειονεκτήματα τα οποία διαπιστώθηκαν είναι τα εξής επιμέρους:
    1. Υποστήριξη ελέγχων συμμόρφωσης και διαλειτουργικότητας μόνο για ebXML εφαρμογές.
    2. Αδυναμία εντοπισμού και απόδοσης ευθυνών στην εφαρμογή η οποία ευθύνεται για την αποτυχία της επικοινωνίας.
    3. Δεν καλύπτεται ο έλεγχος της διαλειτουργικότητας και της συμμόρφωσης των εφαρμοζόμενων μηχανισμών ασφάλειας σε επίπεδο περιεχομένου των μηνυμάτων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

4. Αποτελεί περισσότερο ένα πλαίσιο ελέγχου και όχι μια μεθοδολογία αλγοριθμική και κατασκευαστική.

Οι αδυναμίες και τα μειονεκτήματα όλων των μεθοδολογιών και των πλαισίων που παρουσιάστηκαν στον παρόν Κεφάλαιο και αφορούν τον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης των ΥΙ μπορούν να συνοψιστούν ως ακολούθως:

- Ø ***Γενικευμένες προσεγγίσεις***: χωρίς προσδιορισμό συγκεκριμένων και διακριτών βημάτων που πρέπει να ακολουθηθούν αλλά και διαδικασιών για τον καθορισμό περιπτώσεων ελέγχου.
- Ø ***Παθητικές προσεγγίσεις:*** έλεγχος μόνο της ροής των μηνυμάτων, χωρίς ελέγχο των εκτελέσιμων περιπτώσεων ελέγχου.
- Ø ***Προσεγγίσεις με περιορισμένο πεδίο εφαρμογής:*** που εφαρμόζουν ελέγχους σε περιορισμένες πτυχές των Υπηρεσιών Ιστού.
- Ø ***Προσεγγίσεις με αδυναμία απόδοσης ευθυνών*****:** αδυναμία απόδοσης ευθύνης στην αντίστοιχη ΥΙ στην περίπτωση ενδεχόμενης αποτυχίας μιας επικοινωνίας.

Τα παραπάνω συμπεράσματα λήφθηκαν υπόψη στη διατριβή, για τη δημιουργία μιας νέας τυπικής και δομημένης μεθοδολογίας που εστιάζει στον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης ηλεκτρονικών Υπηρεσίες Ιστού. Οι προαναφερθείσες μεθοδολογίες και πλαίσια θα χρησιμοποιηθούν ως βάση για την προσπάθεια αυτή.

2.2.4 Στρατηγικές Ελέγχων

Οι διαφορετικοί τύποι ελέγχων, όπως είναι ο έλεγχος διαλειτουργικότητας και συμμόρφωσης, οι οποίοι υιοθετούνται από τις μεθοδολογίες ελέγχου και εφαρμόζονται για να ελέγξουν την δυνατότητα επικοινωνίας των υπηρεσιών/εφαρμογών μπορεί να λάβουν χώρα σε διαφορετικά επίπεδα. Ο βαθμός διεισδυσιμότητας εξαρτάται πλήρως από το εύρος των τεχνικών στοιχείων που είναι γνωστά για τις συγκεκριμένες εφαρμογές. Στην βιβλιογραφία έχουν παρουσιαστεί τρεις βασικές στρατηγικές ελέγχου: ο έλεγχος “μαύρου” κουτιού, ο έλεγχος “άσπρου” κουτιού και ο έλεγχος “γκρίζου” κουτιού [Peyton08].

- Στον έλεγχο “μαύρου” κουτιού, οι υπηρεσίες/εφαρμογές οι οποίες ελέγχονται αντιμετωπίζονται ως μαύρα κουτιά για τα οποία δεν υπάρχει καμία γνώση της εσωτερικής τους δομής ή συμπεριφοράς ούτε και των προτύπων ή προδιαγραφών τα οποία υιοθετούν. Οι είσοδοι και οι αντίστοιχοι έξοδοι των συγκεκριμένων εφαρμογών αποτελούν τα μόνο γνωστά στοιχεία. Απώτερο στόχο τους αποτελεί η διαπίστωση ότι η παρεχόμενη λειτουργικότητα καλύπτει τις απαιτήσεις οι οποίες έχουν τεθεί από την εφαρμογή.
- Στον έλεγχο “άσπρου” κουτιού, ο πηγαίος κώδικας, οι δομές δεδομένων και οι αλγόριθμοι που υλοποιούνται από τις εφαρμογές είναι γνωστές και προσβάσιμες. Η ανάλυση των συγκεκριμένων στοιχείων μπορεί να οδηγήσει στην εκτέλεση ενός ευρέως φάσματος περιπτώσεων ελέγχου σε πολύ χαμηλό επίπεδο.
- Στον έλεγχο “γκρίζου” κουτιού, η γνώση της εσωτερικής αρχιτεκτονικής των εφαρμογών είναι περιορισμένη αλλά όχι μηδενική. Η πρόσβαση σε συγκεκριμένες πληροφορίες πέρα από τις απλές απαιτήσεις που πρέπει να καλύπτονται δίνει τη δυνατότητα διεξαγωγής αναλυτικότερων ελέγχων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Σε κάθε περίπτωση η επιλογή της καταλληλότερης στρατηγικής που πρέπει να ακολουθηθεί είναι άρρηκτα συνδεδεμένη με τη φύση της εφαρμογής η οποία ελέγχεται. Επομένως, η μελέτη και καταγραφή των βασικών χαρακτηριστικών των Υπηρεσιών Ιστού αποτελεί ένα στοιχείο το οποίο πρέπει να ληφθεί υποψη για την υιοθέτηση της καταλληλότερης στρατηγικής.
Οι Υπηρεσίες Ιστού αποτελούν μια σύνθεση από ολοκληρωμένες πρωτεύουσες υπηρεσίες [High05], κύρια χαρακτηριτικά των οποίων είναι τα ακόλουθα [Rizwan]:

- Είναι διανεμημένες υπό την έννοια ότι βρίσκονται σε διαφορετικές γεωγραφικές περιοχές, έχοντας ανεξάρτητες δυνατότητες ενώ είναι προσβάσιμες μέσω συγκεκριμένων διεπαφών οι οποίες περιγράφονται από αντίστοιχα έγγραφα WSDL [Christensen01].
- Είναι υλοιποιημένες σε διαφορετικές γλώσσες προγραμματισμού και "τρέχουν" σε διαφορετικά λειτουργικά συστήματα.
- Συνδέονται με στενές εξαρτήσεις με άλλες έμπιστες τρίτες οντότητες όπως είναι οι αρχές που προσφέρουν υπηρεσίες ΥΔΚ και χρονοσφράγισης.
- Η σύνδεση των υπηρεσιών αυτών επιτρέπει την κατάλληλη αναπαράσταση και διαμόρφωση της επιθυμητής επιχειρησιακής λογικής που εμπεριέχεται στις ΥΙ.

Τα συμπεράσματα τα οποία προκύπτουν από το σύνολο των προαναφερόμενων χαρακτηριστικών των ΥΙ είναι τα ακόλουθα. Ο έλεγχος "άσπρου" κουτιού σε ένα υπηρεσιοστρεφές περιβάλλον δεν είναι εφαρμόσιμος σε μεγάλο βαθμό εξαιτίας της δυασκολίας της πρόσβασης στον πηγαίο κώδικα των εξεταζόμενων ΥΙ. Παράλληλα, οι μεθοδολογίες οι οποίες εστιάζονται αποκλειστικά στον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης των ΥΙ (WS-I, ebXML IIC), όπως αυτές περιγράφηκαν στο προηγούμενο κεφάλαιο υιοθετώντας τον έλεγχο "μαύρου" κουτιού, οδηγούν σε ένα μη αποτελεσματικό και περιορισμένων δυνατοτήτων έλεγχο εξαιτίας της "τυφλής"φύσης των ελέγχων που εφαρμόζονται.
Η διανεμημένη φύση των ΥΙ καθιστά τον έλεγχο "γκρίζου" κουτιού ως την πιο ιδανική προσέγγιση για την ανίχνευση αδυναμιών διαλειτουργικότητας κατά την επικοινωνία των εξεταζόμενων ΥΙ. Αυτό πραγματοποιείται μέσω της εκμετάλλευσης της πληροφορίας η οποία περιέχεται στις περιγραφές των διεπαφών των υπηρεσιών (WSDL). Στην προκειμένη περίπτωση η εσωτερική δομή των ΥΙ μπορεί να προσδιοριστεί σε υψηλό επίπεδο, καθορίζοντας τις εμπλεκόμενες υπηρεσίες από τις οποίες αποτελείται καθώς και τις διεπαφές μέσω των οποίων είναι προσβάσιμες, έχοντας περιοσμένη ή μηδενική πρόσβαση στον πηγαίο κώδικα. Επομένως, ο έλεγχος "γκρίζου" κουτιού μπορεί να θεωρηθεί ως η πιο καταλληλότερη στρατηγική που μπορεί να ακολουθηθεί ώστε να ελεγχθεί η δυνατότητα επικοινωνίας των ΥΙ.

2.3 Επισκόπηση Μεθοδολογίας Ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ)

Στο κεφάλαιο αυτό εκτενώς παρουσιάζονται οι βασικές αρχές και πτυχές της προτεινόμενης μεθοδολογίας [Papastergiou09a]. Πρόκειται για μια μεθοδολογία που ακολουθεί τη στρατηγική του "γκρίζου" κουτιού και επιτυγχάνει να καλύψει ένα σύνολο απαιτήσεων.

2.3.1 Απαιτήσεις ΔΣΥΙ

Η ΔΣΥΙ θα πρέπει να ικανοποιεί ένα σύνολο απαιτήσεων ώστε να καθίσταται δυνατός ο αποτελεσματικός έλεγχος ενός μεγάλου εύρους υπηρεσιών οι οποίες

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

βασίζονται σε XML τεχνολογίες και Υπηρεσίες Ιστού ανεξάρτητα της πολυπλοκότητας η οποία εμπεριέχεται σε αυτές. Οι απαιτήσεις που πρέπει να καλύπτονται από τη ΔΣΥΙ είναι οι ακόλουθες:

- **Σαφήνεια**: η μεθοδολογία προσφέρει συγκεκριμένα και ευκρινώς ορισμένα κριτήρια αξιολόγησης για την εκτέλεση των ελέγχων διαλειτουργικότητας και συμμόρφωσης. Επιτρέπει, επίσης, τον ακριβή προσδιορισμό των εμπλεκομένων οντοτήτων καθώς επίσης και της διαδικασίας καθορισμού σαφών περιπτώσεων ελέγχου.
- **Πληρότητα**: η μεθοδολογία είναι καλώς δομημένη και περιλαμβάνει ένα καθορισμένο και ακριβές σύνολο βημάτων εφαρμογής.
- **Προσαρμοστικότητα & Επεκτασιμότητα**: η μεθοδολογία είναι ευπροσάρμοστη και επεκτάσιμη υπό την έννοια ότι νέα κριτήρια αξιολόγησης της διαλειτουργικότητας και της συμμόρφωσης δύναται να υποστηριχθούν και να ενσωματωθούν με ευκολία ενώ παρέχεται η δυνατότητα υιοθέτησης και χρησιμοποίησης καινούργιων εργαλείων και βιβλιοθηκών για την εκτέλεση των πραγματικών δοκιμών.
- **Ευελιξία**: η μεθοδολογία είναι παραμετροποιήσιμη υπό την έννοια ότι διακριτά τμήματα της μεθοδολογίας θα μπορούν να υιοθετηθούν για την πραγματοποίηση συγκεκριμένων ακολουθιών ελέγχου.
- **Απόδοση Ευθύνης**: η μεθοδολογία είναι σε θέση να καταγράφει όλα τα αποτελέσματα των εφαρμοζόμενων δοκιμών ελέγχου που παράγονται από τα κριτήρια αξιολόγησης έτσι ώστε να είναι σε θέση να εντοπίζει λανθασμένες συμπεριφορές και να αποδίδει την ευθύνη των αποτυχημένων ελέγχων στην αντίστοιχη ΥΙ.
- **Ανεξαρτησία & Εξελιξιμότητα**: η μεθοδολογία προσφέρει ένα υψηλό επίπεδο ανεξαρτησίας από τις εφαρμοζόμενες τεχνολογίες, τον αριθμό των εμπλεκομένων οντοτήτων καθώς επίσης και των πλατφορμών που οι ΥΙ υπό δοκιμή έχουν υιοθετήσει. Το γεγονός αυτό προσφέρει τη δυνατότητα ελέγχου της διαλειτουργικότητας και της συμμόρφωσης ενός μεγάλου πλήθους ΥΙ.

Συνοψίζοντας, θα πρέπει να επισημανθεί ότι οι απαιτήσεις αυτές προκύπτουν από την ανάγκη να ελεχθεί σε ικανοποιητικό βαθμό η δυνατότητα επικοινωνίας υπηρεσιών ανεξάρτητα από την προσφερόμενη λειτουργικότητα, τους επιχειρηματικούς στόχους και τις τεχνολογικές επιλογές των ίδιων των υπηρεσιών.

2.3.2 Επισκόπηση Φάσεων ΔΣΥΙ

Η προτεινόμενη μεθοδολογία αποτελείται από τέσσερις φάσεις (Σχήμα 5):

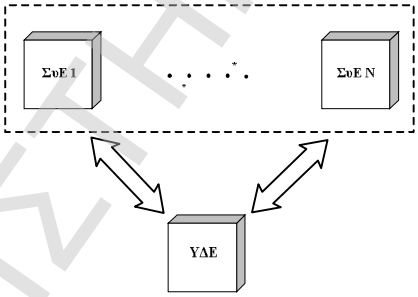
Σχήμα 5: Βασικές Φάσεις Μεθοδολογίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Φάση 1 «*Προσδιορισμός Οντοτήτων*»: περιλαμβάνει τον ακριβή προσδιορισμό των επλεκόμενων οντοτήτων και τον σαφή καθορισμό της διάταξής τους, στοιχείο που διαδραματίζει σημαντικό ρόλο για την εφαρμογή των απαιτούμενων ελέγχων. Οι εμπλεκόμενες οντότητες χωρίζονται σε δυο κατηγορίες: στα Συστήματα υπό Έλεγχο (ΣυΕ), των οποίων η προσφερόμενη ΥΙ ζητείται να εξεταστεί ως προς την διαλειτουργικότητά της και την Υποδομή Διαχείρισης Ελέγχου (ΥΔΕ). που αποτελεί την οντότητα η οποία εποπτεύει και συντονίζει την εκτέλεση των ελέγχων.
Φάση 2 «*Προσαρμογή Δομής Οντοτήτων*»: λαμβάνει χώρα ο καθορισμός της πραγματικής δομής των εμπλεκομένων οντοτήτων, δηλαδή των ΣυΕ και της ΥΔΕ, με την οποία οι οντότητες αυτές θα λάβουν μέρος στην εκτέλεση των ελέγχων.
Φάση 3 «*Έλεγχος Συμμόρφωσης*»: κάθε ΣυΕ εξετάζεται απέναντι σε προτυποποιημένες εφαρμογές ώστε να αξιολογηθεί ως προς την συμμόρφωσή του σε συγκεκριμένα πρότυπα.
Φάση 4 «*Έλεγχος Διαλειτουργικότητας*»: πραγματοποίηση ελέγχων διαλειτουργικότητας με συμμετοχή όλων των ΣυΕ ώστε να εξεταστεί η πραγματική δυνατότητα επικοινωνίας τους.
Τα κεφάλαια που ακολουθούν παραθέτουν μια λεπτομερή παρουσίαση των τεσσάρων φάσεων.

2.3.3 Φάση 1: Προσδιορισμός Οντοτήτων

Όπως γίνεται αντιληπτό από το σχήμα που ακολουθεί, ο βασικός στόχος της πρώτης φάσης της μεθοδολογίας είναι ο προσδιορισμός του αριθμού και της διάταξης όλων των οντοτήτων που μετέχουν στην ακολουθία ελέγχου. Η πλήρης εφαρμογή της προτεινόμενης μεθοδολογίας απαιτεί τον σαφή καθορισμό των κύριων εμπλεκομένων οντοτήτων οι οποίες συνοψίζονται στις ακόλουθες:



Σχήμα 6. Προσδιορισμός Ονοτήτων και Καθορισμός Διάταξής τους

Συστήματα υπό Έλεγχο (ΣυΕ): τα συστήματα ΣυΕ 1 … ΣυΕ N (Σχήμα 6) τα οποία βρίσκονται υπό αξιολόγηση και ελέγχονται τόσο ως προς τη συμμόρφωσή τους σε συγκεκριμένα πρότυπα όσο και ως προς την διαλειτουργικότητα τους. Ο στόχος των ελέγχων αυτών είναι να εξεταστεί ότι τα συστήματα αυτά είναι σε θέση να επικοινωνήσουν αλληλεπιδρώντας επιτυχώς. Ένα ΣυΕ εμπερικλείει μία και μόνο ΥΙ της οποίας στην πραγματικότητα ελέγχεται η διαλειτουργικότητα και η συμμόρφωση. Η ΥΙ αυτή θα πρέπει να είναι κοινή για όλα τα ΣυΕ τα οποία μετέχουν στον ίδιο έλεγχο. Ένα πρόσθετο στοχείο που πρέπει να σημειωθεί είναι ότι η εξεταζόμενη ΥΙ μπορεί να προσφέρεται είτε με τη μορφή μιας αυτόνομης ΥΙ είτε να είναι ενσωματωμένη σε μια ολοκληρωμένη αρχιτεκτονική προσανατολισμένη στις υπηρεσίες (ΑΠΥ).
Στην περίπτωση κατά την οποία μια ΑΠΥ προσφέρει ένα σύνολο από ΥΙ, τότε για καθεμία από τις ΥΙ αυτές θα πρέπει να οριστεί ένα αυτόνομο και ανεξάρτητο ΣυΕ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Καθένα από τα ΣυΕ αυτά θα πρέπει να λάβει μέρος στην εκτέλεση ανεξάρτητων ελέγχων εκτελώντας τα βήματα που προτείνονται από την μεθοδολογία.

Υποδομή Διαχείρισης Ελέγχου (ΥΔΕ): το βασικό συστατικό το οποίο παρατηρεί και εγγυάται τις ακολουθίες ελέγχου που εφαρμόζονται από τα ΣυΕ προκειμένου να εντοπίσει οποιαδήποτε λανθασμένη συμπεριφορά. Η λογική και οργανωτική δομή της ΥΔΕ είναι ανεξάρτητη από τη φύση των ΣυΕ. Από τεχνολογική άποψη η ΥΔΕ θα πρέπει να προσφέρει εξαιρετική ευελιξία και εξελιξιμότητα επιτρέποντας την αναβάθμιση των ήδη υιοθετημένων εργαλείων και βιβλιοθηκών ελέγχου και αξιολόγησης καθώς επίσης και την ενσωμάτωση νέων πιό προηγμένων. Η αναβάθμιση αυτή επιτρέπει τον έλεγχο ενός μεγάλου εύρους συστημάτων ως προς διαφορετικές πτυχές. Η ΥΔΕ λειτουργεί λοιπόν ως η οντότητα η οποία αρχικοποιεί τον έλεγχο, μετέχει σε αυτόν ως ενδιαμέση οντότητα και τελικώς αποφαίνεται για την δυνατότητα επικοινωνίας των ΣυΕ.

Τα βήματα που πρέπει να ακολουθηθούν για την ολοκλήρωση της συγκεκριμένης φάσης είναι τα ακόλουθα:

1. *Καθορισμός οντοτήτων* που μετέχουν στον έλεγχο.
2. *Δήλωση* εξεταζόμενης ΥΙ.
3. *Προσδιορισμός του ρόλου* των εμπλεκόμενων οντοτήτων μέσω του καθορισμού ενός εξεταζόμενου σεναρίου. Το σενάριο αυτό εξετάζει αν η επικοινωνία των οντοτήτων είναι εφικτή και σύμφωνη με τα εφαρμοζόμενα πρότυπα.
4. *Καθορισμός διάταξης οντοτήτων* λαμβάνοντας υπόψη τους ρόλους όπως αυτοί καθορίστηκαν στο προηγούμενο βήμα. Στο Σχήμα 6, ως ΣυΕ 1 ορίζεται το σύστημα το οποίο αρχικοποιεί την εκτέλεση των εφαρμοζόμενων ελέγχων, ενώ η διάταξη των υπολοίπων ΣυΕ (π.χ. ΣυΕ Ν) καθορίζεται με βάση το ρόλο τον οποίο διαδραματίζει κάθε οντότητα στο εξεταζόμενο σενάριο. Η ΥΔΕ ενεργεί ως γενικός συντονιστής της όλης διαδικασίας υποδεικνύοντας τις ακολουθίες ελέγχων που πρέπει να εφαρμοστούν και φέροντας την ευθύνη της εποπτείας της ορθής επικοινωνίας των ΣυΕ.

Στο πέρας του βήματος (4), έχει πραγματοποιηθεί τόσο ο καθορισμός των οντοτήτων όσο και η διάταξη με την οποία αυτές μετέχουν στον έλεγχο.

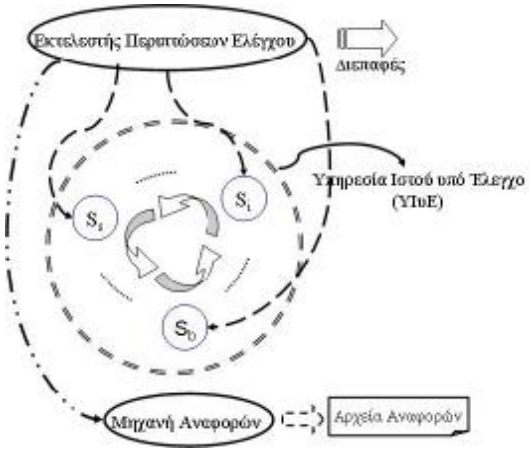
2.3.4 Φάση 2: Προσαρμογή Δομής Οντοτήτων

Κατά τη διάρκεια της δεύτερης φάσης της μεθοδολογίας, η πραγματική δομή των εμπλεκομένων οντοτήτων, ΥΔΕ και ΣυΕ, καθορίζεται πλήρως από τους αρμόδιους φορείς, υποδεικνύοντας και διαμορφώνοντας τα συστατικά από τα οποία αποτελείται κάθε οντότητα. Η τελική τους μορφή συνδέεται άρρηκτα με τους ελέγχους που θα εκτελεστούν και τις ακολουθίες που θα εφαρμοστούν.

2.3.4.1 Σύστημα υπό Έλεγχο (ΣυΕ)

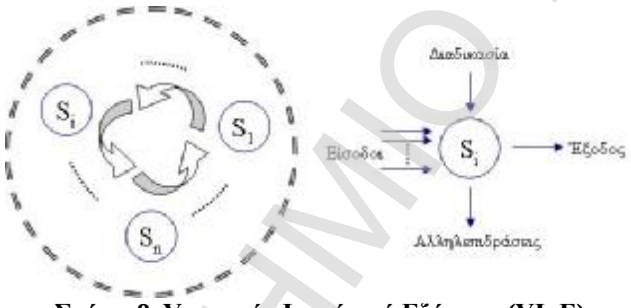
Κάθε ΣυΕ το οποίο εξετάζεται θα πρέπει αρχικά να εναρμονιστεί με τις αρχές που επιβάλλονται από την προτεινόμενη μεθοδολογία. Στην παρούσα φάση, κάθε ΣυΕ απαιτείται να αποκτήσει την κατάλληλη δομή. Η δομή αυτή συντίθεται από ένα σύνολο από συστατικά που επιτρέπουν την ολοκλήρωση των απαραίτητων βημάτων όπως είναι η επικοινωνία με την ΥΔΕ, η εκτέλεση των περιπτώσεων ελέγχου και η καταγραφή και υποβολή των αποτελεσμάτων ελέγχου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 7. Δομή Συστήματος υπό Έλεγχο

Το Σχήμα 7 απεικονίζει τα τρία κύρια συστατικά του ΣυΕ. Το πρώτο είναι η *Υπηρεσία Ιστού υπό Έλεγχο (ΥΙυΕ)* που αποτελεί το θεμελιώδες στοιχείο κάθε ΣυΕ. Το συστατικό αυτό αναπαριστά την προσφερθείσα λειτουργικότητα της πραγματικής ΥΙ η οποία και ελέγχεται.



Σχήμα 8. Υπηρεσία Ιστού υπό Εξέταση (ΥΙυΕ)

Μια ΥΙυΕ, όπως αποτυπώνεται στο Σχήμα 8, αποτελείται από ένα σύνολο από πρωτεύουσες υπηρεσίες $\{S_1,...,S_n\}$ ο συνδυασμός των οποίων διαμορφώνει και εκτελεί την επιχειρησιακή λογική της εξεταζόμενης ΥΙ. Κάθε πρωτεύουσα υπηρεσία αναπαριστά και υλοποιεί μια συγκεκριμένη λειτουργία, όπως είναι η υπηρεσία ασφάλειας για την παραγωγή και επαλήθευση ψηφιακών υπογραφών. Η ορθή λειτουργία καθεμίας υπηρεσίας προϋποθέτει τον καθορισμό ενός αυστηρού αριθμού παραμέτρων (*Εισόδων*) οι οποίες απαιτούνται για την παραγωγή του αντίστοιχου αποτελέσματος (*Εξόδου*).

Το σύνολο των υπηρεσιών αυτών, ακολουθώντας διακριτές διαδικασίες, διαχειρίζεται και παράγει μια σειρά δεδομένων τα οποία βασίζονται σε συγκεκριμένα πρότυπα. Η ουσιαστική συμμόρφωση των δεδομένων αυτών με τις απαιτήσεις όπως αυτές καθορίζονται από τα αντίστοιχα πρότυπα καθώς επίσης και η ικανότητα άλλων συστημάτων να διαχειρίζονται κατάλληλα τα παραγόμενα δεδομένα αποτελούν δυο παράγοντες οι οποίοι προσδιορίζουν και συμπεραίνουν τις δυνατότητες συμμόρφωσης και διαλειτουργικότητας της ΥΙυΕ.

Ας θεωρήσουμε την περίπτωση κατά την οποία μια υπηρεσία ασφάλειας για την παραγωγή και επαλήθευση ψηφιακών υπογραφών μιας "ΥΙυΕ Α" υπογράφει ένα έγγραφο XML σύμφωνα με το πρότυπο W3C XML Digital Signature. Σε πρώτη φάση, το υπογεγραμμένο έγγραφο θα πρέπει να εξεταστεί ως προς τη συμμόρφωσή του με τις αρχές του συγκεκριμένου προτύπου, ενώ στη συνέχεια θα πρέπει να ελεχθεί ότι μια "ΥΙυΕ Β" μπορεί να επαληθεύσει επιτυχώς την παραγόμενη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

υπογραφή. Τα συμπεράσματα τα οποία μπορούν να εξαχθούν από το συγκεκριμένο παράδειγμα είναι τα ακόλουθα:

1. Αν η "ΥΙυΕ Α" παράγει υπογεγραμμένα έγγραφα τα οποία είναι σύμφωνα με το πρότυπο W3C XML Digital Signature.
2. Αν η "ΥΙυΕ Α" μπορεί να αλληλεπιδράσει επιτυχώς με την "ΥΙυΕ Β" όσον αφορά την εφαρμογή ψηφιακών υπογραφών σε επιχειρησιακό επίπεδο.

Το γεγονός που πρέπει να επισημανθεί είναι ότι προκειμένου μια ΥΙυΕ να παράγει τα απαιτούμενα δεδομένα αξιολόγησης θα πρέπει να εκτελέσει μια σειρά από ενέργειες όπως αυτές υποδεικνύονται από συγκεκριμένες *περιπτώσεις ελέγχου*. Μια περίπτωση ελέγχου εκφράζει ένα σύνολο από συνθήκες και μεταβλητές οι οποίες αναπαριστούν και υποδηλώνουν τις ενέργειες που πρέπει να εκτελέσει κάθε ΥΙυΕ ώστε να ολοκληρωθεί μια ακολουθία ελέγχου. Ο καθορισμός των περιπτώσεων αυτών πραγματοποιείται σε συγκεκριμένο σημείο της προτεινόμενης μεθοδολογίας (βλ. § 2.3.5 και 2.3.6).

Η προτεινόμενη μεθοδολογία προκειμένου να επιτύχει την αυτοματοποιημένη εκτέλεση των περιπτώσεων ελέγχου καθώς επίσης και την συλλογή των παραγόμενων δεδομένων έχει καθορίσει δυο πρόσθετα δομικά συστατικά ως μέρος του ΣυΕ (Σχήμα 7). Τα συστατικά αυτά είναι ο *Εκτελεστής Περιπτώσεων Ελέγχου* και η *Μηχανή Αναφορών*.

Βασική ευθύνη του Εκτελεστή Περιπτώσεων Ελέγχου είναι η διαχείριση και εποπτεία της εκτέλεσης των περιπτώσεων ελέγχου στο ΣυΕ μέσω του συντονισμού της λειτουργίας των εμπλεκόμενων λειτουργιών της ΥΙυΕ ώστε να εκτελεστούν συγκεκριμένες ροές εργασιών. Κάθε ροή εργασίας αναπαρίσταται από μια προκαθορισμένη διαδικασία BPEL [WSBPEL] η οποία εμπεριέχει και αποτυπώνει τη λογική μιας εκτελούμενης περίπτωσης ελέγχου. Οι περιπτώσεις ελέγχου BPEL οι οποίες θα υιοθετηθούν και θα εκτελεστούν σχεδιάζονται κατά τη διάρκεια των φάσεων 3 και 4 της προτεινόμενης μεθοδολογίας όπου πρακτικά εκτελούνται οι ουσιαστικοί έλεγχοι συμμόρφωσης και διαλειτουργικότητας. Στις συγκεκριμένες φάσεις, ο Εκτελεστή Περιπτώσεων Ελέγχου υφίσταται μια κατάλληλη παραμετροποίηση προκειμένου να επιτευχθεί η εκτέλεση των καθορισμένων διαδικασιών BPEL. Η παραμετροποίηση περιλαμβάνει την δημιουργία και παροχή συγκεκριμένων διεπαφών οι οποίες καλούνται από την ΥΔΕ για την αρχικοποίηση της εκτέλεσης μιας περίπτωσης ελέγχου BPEL.

Επομένως, ο Εκτελεστής Περιπτώσεων Ελέγχου προσφέρει έναν ενδελεχή έλεγχο της διαδικασίας ελέγχου επιτρέποντας ταυτόχρονα την ευέλικτη συλλογή των δεδομένων αξιολόγησης που παράγονται από τις εκτελούμενες διαδικασίες BPEL. Η διαδικασία της συλλογής των δεδομένων μαζί με την εσωμάτωσή τους σε συγκεκριμένα αρχεία αναφορών (log files) αποτελεί την κύρια αρμοδιότητα της *Μηχανής Αναφορών* η οποία είναι το τελευταίο συστατικό του ΣυΕ. Τα παραγόμενα αρχεία θα χρησιμοποιηθούν από τα αρμόδια συστατικά της ΥΔΕ κατά τη εκτέλεση των φάσεων 3 και 4 της προτεινόμενης μεθοδολογίας ώστε να συμπεράνουν τη συμμόρφωση και τη διαλειτουργικότητα της ΥΙυΕ.

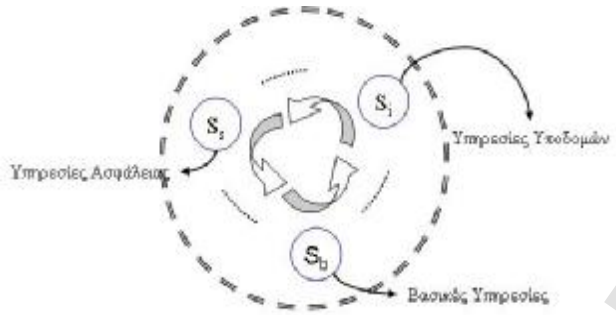
Στις παραγράφους που ακολουθούν πραγματοποείται μια αναλυτική παρουσίαση των δομικών στοιχείων από τα οποία αποτελείται κάθε ένα από τα παραπάνω συστατικά του ΣυΕ.

2.3.4.1.1 Υπηρεσία Ιστού υπό Έλεγχο (ΥΙυΕ)

Η Υπηρεσία Ιστού υπό Έλεγχο (ΥΙυΕ), Σχήμα 9, εμπερικλείει τις βασικές λειτουργίες κάθε ΥΙ, η οποία βρίσκεται υπό καθεστώς ελέγχου για να διαπιστωθεί η δυνατότητα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

επικοινωνίας με άλλες κοινές ΥΙ, όπως αυτές καθορίζονται σε μια Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ) [High05].



Σχήμα 9. Βασικές Λειτουργίες ΥΙυΕ

Χαρακτηριστικά είναι τα παραδείγματα ολοκληρωμένων πλατφορμών τόσο στο χώρο της ηλεκτρονικής διακυβέρνησης [Kaliontzoglou05], [Karantjias09a], [Papastergiou09b] όσο και του ηλεκτρονικού επιχειρείν που απαρτίζονται από ένα σύνολο υπηρεσιών οι οποίες προσφέρουν:

- επικοινωνία με τα συστήματα αποθετηρίων (π.χ. βάσεις δεδομένων, πληροφοριακά συστήματα Διαχείρισης Πληροφοριακών Πόρων) και την ολοκλήρωση του κατάλληλου μετασχηματισμού των δεδομένων.
- διαχείριση των ανταλλασσόμενων μεταξύ των ΥΙυΕ εγγράφων και την εφαρμογή των απαιτούμενων μηχανισμών ασφάλειας σε επιχειρησιακό επίπεδο, όπως είναι η εφαρμογή ψηφιακών υπογραφών ή/και η κρυπτογράφηση.
- διαχείριση των ανταλλασσόμενων μεταξύ των ΣυΕ μηνυμάτων και την εφαρμογή των απαιτούμενων μηχανισμών ασφάλειας σε επίπεδο μηνύματος.

Τέτοιου είδους κατηγορίες υπηρεσιών είναι οι ακόλουθες:

- *Υπηρεσίες μετασχηματισμού εγγράφων*: οι οποίες επιτρέπουν την μετατροπή εγγράφων προκειμένου να μεταφερθούν ανάμεσα σε διαφορετικές περιοχές διαχείρισης. Οι υπηρεσίες μετασχηματισμού πρέπει να σέβονται τη σημασιολογία του περιεχομένου των εγγράφων προκειμένου τα έγγραφα που ανταλλάσσονται να είναι αποδεκτά στο περιβάλλον κάθε περιοχής διαχείρισης.
- *Υπηρεσίες διαχείρισης αποθετηρίων:* οι οποίες ελέγχουν τις συναλλαγές με τα αποθετήρια (π.χ. βάσεις δεδομένων, πληροφοριακά συστήματα Διαχείρισης Πληροφοριακών Πόρων) που εμπεριέχονται σε κάθε σύστημα. Οι υπηρεσίες αυτές επιτρέπουν την απόθεση μετασχηματισμένων εγγράφων ή την εξαγωγή αυτών με σκοπό το μετασχηματισμό τους και την περαιτέρω επεξεργασία τους.
- Οι *μηχανισμοί διαχείρισης εγγράφων* επιτρέπουν τη δημιουργία, διαχείριση και κατάργηση ενός εγγράφου. Οι μηχανισμοί αυτοί θα πρέπει να σέβονται τη σημασιολογία του περιεχομένου των εγγράφων προκειμένου τα έγγραφα να γίνονται αποδεκτά στο περιβάλλον κάθε περιοχής διαχείρισης.
- Οι *μηχανισμοί ψηφιακών υπογραφών* χρησιμοποιούν κρυπτογραφία προκειμένου να ενσωματώσουν την ταυτότητα μιας οντότητας σε ένα έγγραφο και να εξασφαλίσουν την ακεραιότητα του εγγράφου αυτού. Οι απλές ψηφιακές υπογραφές ικανοποιούν τις απαιτήσεις για πιστοποίηση και ακεραιότητα.
- Οι *μηχανισμοί προηγμένων ηλεκτρονικών* υπογραφών αναβαθμίζουν τις απλές ψηφιακές υπογραφές συνδυάζοντάς τις με χρονοσφραγίδες καθώς και το κρυπτογραφικό «δέσιμο» της υπογραφής με μια πολιτική υπογραφής που εδραιώνει τη νομική της αξία στα πλαίσια ενός οργανισμού. Καλύπτουν την απαίτηση για μη-άρνηση συμμετοχής.

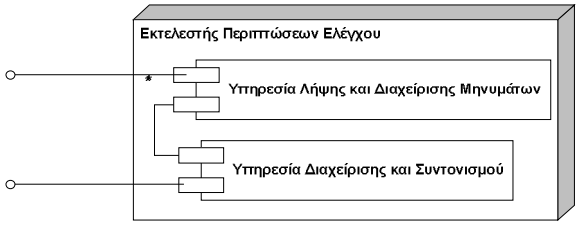
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- Οι *μηχανισμοί κρυπτογράφησης* χρησιμοποιούν αλγόριθμους κρυπτογράφησης για να κρυπτογραφήσουν και αποκρυπτογραφήσουν τα έγγραφα. Καλύπτουν την απαίτηση για μυστικότητα.
- Οι *Υπηρεσίες χρονοσφράγισης* επιτρέπουν την επικοινωνία με μια Έμπιστη Τρίτη Οντότητα προκειμένου να ληφθούν πιστοποιημένα δεδομένα χρόνου που είναι κρυπτογραφικά δεμένα με ένα έγγραφο. Σε συνδυασμό με τους μηχανισμούς προηγμένων ψηφιακών υπογραφών, καλύπτουν την απαίτηση για μη-άρνηση συμμετοχής.
- Οι *Υπηρεσίες διαχείρισης μηνυμάτων* έχουν ως βασική αρμοδιότητα την δημιουργία, κατάργηση και διατήρηση των μηνυμάτων που αποστέλλονται ή λαμβάνονται. Οι υπηρεσίες αυτές αναλαμβάνουν την δόμηση ή την αποδόμηση των μηνυμάτων εισάγοντας ή εξάγοντας αντίστοιχα τις απαιτούμενες πληροφορίες. Επομένως, θα πρέπει να σέβονται τη σημασιολογία του περιεχομένου των μηνυμάτων προκειμένου τα έγγραφα που ανταλλάσσονται να είναι αποδεκτά στο περιβάλλον κάθε περιοχής διαχείρισης.
- Οι *Υπηρεσίες ασφάλειας μηνυμάτων* επιτρέπουν την εφαρμογή και επικύρωση των απαραίτητων μηχανισμών ασφάλειας που πρέπει ή έχουν εφαρμοστεί αντίστοιχα στα μηνύματα που ανταλλάσσονται εφαρμόζοντας την κατάλληλη πολιτική μεταφοράς.
- Οι *Υπηρεσίες προώθησης μηνυμάτων* αναλαμβάνουν την μεταφορά μηνυμάτων στον σωστό παραλήπτη εφαρμόζοντας την κατάλληλη πολιτική μεταφοράς. Γι' αυτό το λόγο συνήθως κάνουν χρήση των Υπηρεσιών ασφάλειας μηνυμάτων.
- Οι *Υπηρεσίες διαχείρισης κλειδιών και πιστοποιητικών* αποτελούν τις υπηρεσίες που διαχειρίζονται κλειδιά και πιστοποιητικά των οντοτήτων που εμπλέκονται στο έλεγχο. Χρησιμοποιούνται για την λήψη κλειδιών και τον έλεγχο της εγκυρότητας των υπογεγραμμένων εγγράφων των και ανταλλασσόμενων μηνυμάτων.

Η αλληλεπίδραση των παραπάνω υπηρεσιών επιτρέπει την ολοκλήρωση των αντικειμενικών στόχων τόσο της ίδιας της ΥΙυΕ όσο και των εκτελούμενων περιπτώσεων ελέγχων.

2.3.4.1.2 Εκτελεστής Περιπτώσεων Ελέγχου

Ο Εκτελεστής Περιπτώσεων Ελέγχου αποτελεί το συστατικό του ΣυΕ το οποίο παρέχει τις απαιτούμενες διεπαφές οι οποίες καλούνται από την ΥΔΕ ώστε να αρχικοποιηθεί η εκτέλεση των περιπτώσεων ελέγχου. Όπως είναι εμφανές από το Σχήμα 10 ο Εκτελεστής Περιπτώσεων Ελέγχου απαρτίζεται από δυο βασικά δομικά στοιχεία, την *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* και την *Υπηρεσία Διαχείρισης και Συντονισμού*.



Σχήμα 10. ***Εκτελεστής Περιπτώσεων Ελέγχου***

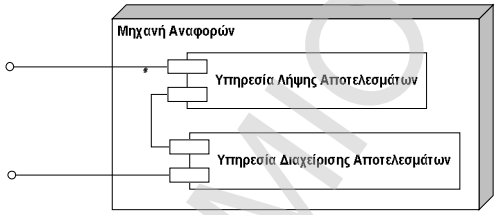
Η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* αναλαμβάνει την ευθύνη λήψης και διαχείρισης των μηνυμάτων που αποστέλλει η ΥΔΕ. Στην συνέχεια, τα αποδομεί

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

κατάλληλα εξάγοντας τα περικλειόμενα στοιχεία ελέγχου (που απαρτίζονται από τα πιθανά δεδομένα ελέγχου), τα οποία τα μεταβιβάζει στην *Υπηρεσία Διαχείρισης και Συντονισμού*.
Η *Υπηρεσία Διαχείρισης και Συντονισμού* ξεκινάει την εκτέλεση της κατάλληλης διαδικασίας BPEL η οποία καθορίζεται από την επίκληση της αντίστοιχης διεπαφής. Αυτό έχει ως αποτέλεσμα τη διαχείριση και τον συντονισμό ενός συνόλου λειτουργιών οι οποίες προσφέρονται από την ΥΙυΕ (βλ. § 2.3.4.1.1) προκειμένου να ολοκληρωθεί η εκτέλεση των περιπτώσεων ελέγχου και να παραχθούν τα δεδομένα προς αξιολόγηση.

2.3.4.1.3 Μηχανή Αναφορών

Η Μηχανή Αναφορών συνιστά το συστατικό του ΣυΕ που επικοινωνεί με τον Εκτελεστή Περιπτώσεων Ελέγχου για την επιτήρηση της εκτέλεσης των περιπτώσεων ελέγχου μέσω της καταγραφής των ενδιάμεσων καταστάσεων τις οποίες λαμβάνουν οι εμπλεκόμενες υπηρεσίες της ΥΙυΕ και της συλλογής των παραγόμενων δεδομένων. Η εκτέλεση των διαδικασιών αυτών πραγματοποιείται από τα δύο δομικά συστατικά από τα οποία και απαρτίζεται, όπως απεικονίζεται και στο Σχήμα 11, την *Υπηρεσία Λήψης Αποτελεσμάτων* και την *Υπηρεσία Διαχείρισης Αποτελεσμάτων*.



Σχήμα 11. ***Μηχανή Αναφορών***

Η Υπηρεσία Λήψης Αποτελεσμάτων έχει ως βασική αρμοδιότητα να εποπτεύει και να παρατηρεί την εκτέλεση των περιπτώσεων ελέγχου καταγράφοντας τη συμπεριφορά των εμπλεκόμενων υπηρεσιών και συγκεντρώνοντας τα παραγόμενα δεδομένα. Το γεγονός αυτό προϋποθέτει την ύπαρξη μιας άμεσης επικοινωνίας με τον Εκετελεστή Περιπτώσεων Ελέγχου και πιο συγκεκριμένα με την Υπηρεσία Διαχείρισης και Συντονισμού.
Ακολούθως, η Υπηρεσία Διαχείρισης Αποτελεσμάτων αναλαμβάνει τη σύνθεση των αποτελεσμάτων στην απαιτούμενη μορφή και την ενσωμάτωσή τους σε αρχεία αναφορών (log files). Η σύνθεση αυτή επιβάλλεται να πραγματοποιηθεί σε μια μορφή η οποία εξασφαλίζει τη σημασιολογία των δεδομένων έτσι ώστε οι πληροφορίες οι οποίες εμπεριέχονται να είναι απόλυτα αποδεκτές από τις εμπλεκόμενες οντότητες (ΣυΕ και ΥΔΕ).
Το σύνολο των δεδομένων τα οποία τελικώς συλλέγονται κατηγοριοποιούνται ως εξής:

- έγγραφα τα οποία εξάγονται από το αποθετήριο, καθώς επίσης και τα έγγραφα στα οποία αυτά μετασχηματίζονται ή αντίστροφα,
- πληροφορίες οι οποίες σχετίζονται με τις ίδιες τις διαδικασίες μετασχηματισμού και επικοινωνίας με τα αποθετήρια συγκρατώντας οποιαδήποτε εσφαλμένη αναφορά.
- έγγραφα τα οποία είτε παράγονται είτε εισάγονται ώστε να εφαρμοστούν σε αυτά οι αντίστοιχοι μηχανισμοί ασφάλειας καθώς επίσης και το τελικό έγγραφο το οποίο προκύπτει,

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- Ø πληροφορίες οι οποίες σχετίζονται με τις ίδιες τις διαδικασίες ασφάλειας και διαχείρισης του εγγράφου όπως είναι η επικοινωνία με την αρχή Χρονοσφράγισης, η ορθή δημιουργία και επικύρωση των μηχανισμών ασφάλειας και η ορθή διαχείριση των κλειδιών και των πιστοποιητικών.
- Ø μηνύματα τα οποία είτε παράγονται είτε λαμβάνονται και στα οποία δύναται να εφαρμοστούν μηχανισμοί ασφάλειας όπως είναι η δημιουργία και επικύρωση ψηφιακών υπογραφών και κρυπτογράφησης,
- Ø πληροφορίες οι οποίες σχετίζονται με τις ίδιες τις διαδικασίες διαχείρισης του μηνύματος όπως είναι πιστοποίηση των εφαρμοζόμενων στοιχείων ασφάλειας, η ορθή διαχείριση, λήψη ή αποστολή του μηνύματος και η διαχείριση των χρησιμοποιούμενων κλειδιών και πιστοποιητικών.

Τα δεδομένα αυτά θα χρησιμοποιηθούν στην $3^{η}$ και $4^{η}$ φάση της μεθοδολογίας για την ολοκλήρωση των ελέγχων συμμόρφωσης και διαλειτουργικότητας αντίστοιχα.

2.3.4.1.4 Επισκόπηση Βημάτων Καθορισμού ενός ΣυΕ

Στις παραγράφους που προηγήθηκαν έγινε μια παρουσίαση των βασικών δομικών στοιχείων όπως και των μηχανισμών και υπηρεσιών από τα οποία δύναται να απαρτίζεται ένα ΣυΕ. Στο κεφάλαιο αυτό πραγματοποιείται η παράθεση των επιμέρους βημάτων τα οποία πρέπει να εκτελεστούν ώστε να επιτευχθεί ο πλήρης καθορισμός ενός ΣυΕ. Η διαδικασία αυτή αποτελείται από τα εξής βήματα:

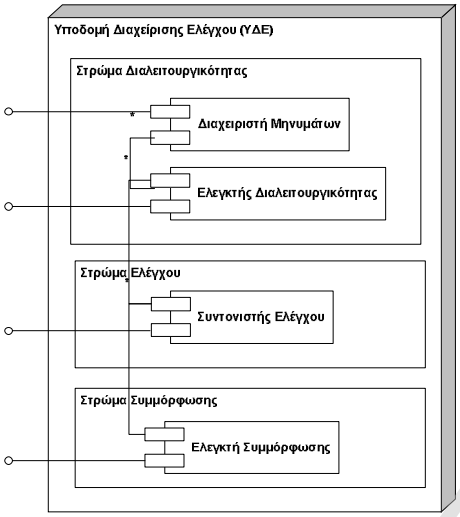
1. *Μελέτη και καταγραφή* των διαθέσιμων υπηρεσιών και μηχανισμών (λειτουργιών) που συνθέτουν την εξεταζόμενη ΥΙ.
2. *Ανάλυση Διεπαφών* των διαθέσιμων υπηρεσιών-λειτουργιών καθώς επίσης και των τύπων δεδομένων που χρησιμοποιείται ανά υπηρεσία, εξάγοντας τους τύπους των μηνυμάτων που απαιτείται να διαμορφωθούν όπως αυτά αναφέρονται στις αντίστοιχες περιγραφές των υπηρεσιών. Αυτό προϋποθέτει μια εκτενή ανάλυση ενός μεγάλου αριθμού περιγραφών υπηρεσιών.
3. *Καθορισμό των Προτύπων* που έχει υιοθετήσει και εφαρμόζει κάθε ΥΙυΕ.
4. *Ενσωμάτωση των Συστατικών Ελέγχου* που λειτουργούν ως πρόσθετα δομικά συστατικά για την εκτέλεση των ελέγχων. Τα απαιτούμενα συστατικά είναι ο Εκτελεστής Περιπτώσεων Ελέγχου και η Μηχανή Αναφορών.

Τα βήματα της μεθοδολογίας διατηρούν αυξημένη ανεξαρτησία από συγκεκριμένες τεχνολογικές λύσεις. Το συνολικό τεχνολογικό πλαίσιο που έχει υιοθετηθεί κατά την υλοποίηση της ΥΙ (για παράδειγμα αν έχει χρησιμοποιηθεί η αρχιτεκτονική Java Enterprise Architecture [J2EE] ή Microsoft .Net [dotNET] και τα δύο ή κάτι άλλο), δεν επηρεάζει τη συνολική εκτέλεση της διαδικασίας από την στιγμή που γίνονται σεβαστές οι βασικές αρχές της μεθοδολογίας.

2.3.4.2 Υποδομή Διαχείρισης Ελέγχου (ΥΔΕ)

Η γενική δομή και λειτουργικότητα της ΥΔΕ απεικονίζεται στο ακόλουθο σχήμα:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 12. Υποδομή Διαχείρισης Ελέγχου (ΥΔΕ)

Η ΥΔΕ αποτελείται από τρία θεμελιώδη στρώματα (Σχήμα 12): Το πρώτο είναι το *Στρώμα Ελέγχου* βασικό συστατικό του οποίου είναι ο *Συντονιστής Ελέγχου*. Πρωταρχική αρμοδιότητα του συστατικού αυτού είναι ο συντονισμός της εκτέλεσης των περιπτώσεων ελέγχου BPEL των ΣυΕ όπως αυτές αυτές καθορίζονται στις φάσεις 3 και 4 της προτεινόμενης μεθοδολογίας, μέσω ενός προκαθορισμένου προσχέδιου το οποίο διαμορφώνεται στις συγκεκριμένες φάσεις. Με βάση το προσχέδιο αυτό πραγματοποιείται διαδοχική κλήση των διεπαφών τα οποία παρέχονται από τον Εκτελεστή Περιπτώσεων Ελέγχου των ΣυΕ προκειμένου να αρχικοποιηθεί η εκτέλεση των αντίστοιχων BPEL διαδικασιών.
Η κλήση των διεπαφών μπορεί να απαιτεί ως είσοδο συγκεκριμένα δεδομένα ελέγχου. Τα δεδομένα αυτά εκφράζουν τα στοιχεία που ενδέχεται να απαιτηθούν για την εκτέλεση των περιπτώσεων ελέγχου. Το είδος των στοιχείων αυτών εξαρτάται από την φύση των ελέγχων, ενώ ποικίλουν από προκαθορισμένα μηνύματα μέχρι και έγγραφα. Τα στοιχεία αυτά ενδέχεται να περιλαμβάνουν ακόμη και δεδομένα τα οποία να μην συμμορφώνονται με τα αντίστοιχα πρότυπα δίνοντας την δυνατότητα να ελεγχθεί η συμπεριφορά ενός ΣυΕ απέναντι και σε μη έγκυρα δεδομένα. Τα απαιτούμενα δεδομένα ελέγχου βασίζονται αποκλειστικά στη φύση των εφαρμοζόμενων διαδικασιών BPEL και παράγονται παράλληλα με τον καθορισμό των περιπτώσεων ελέγχων.
Το επόμενο στρώμα της ΥΔΕ είναι το *Στρώμα Συμμόρφωσης* το οποίο συνίσταται μόνο από τον *Ελεγκτή Συμμόρφωσης*. Βασική αρμοδιότητα του συστατικού αυτού αποτελεί η ανάκτηση των αρχείων αναφορών τα οποία παράγονται από τη Μηχανή Αναφορών των ΣυΕ κατά την εκτέλεση των περιπτώσεων ελέγχου στην φάση 3 της μεθοδολογίας και η αξιολόγηση των δεδομένων που εμπεριέχονται σε αυτά ώστε να πραγματοποιηθούν οι απαιτούμενοι έλεγχοι συμμόρφωσης απέναντι στα πρότυπα τα οποία έχουν υιοθετηθεί.

Το *Στρώμα Διαλειτουργικότητας* αποτελεί το τελευταίο στρώμα της ΥΔΕ το οποίο κατέχει όμως ένα καίριο ρόλο. Απαρτίζεται από τα εξής συστατικά:

- Τον *Διαχειριστή Μηνυμάτων*, ο οποίος δρα μεταξύ των ΣυΕ λειτουργώντας ως ενδιάμεση οντότητα. Αναλαμβάνει την ευθύνη λήψης και μεταβίβασης των μηνυμάτων τα οποία ανταλλάσσονται μεταξύ των ΣυΕ κατά τη διάρκεια των ελέγχων διαλειτουργικότητας που λαμβάνει χώρα στη φάση 4 της μεθοδολογίας. Βασική ευθύνη του συστατικού είναι να ελέγχει αν τα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ανταλλασσόμενα μηνύματα είναι μέρος της επιχειρησιακής διαδικασίας όπως αυτή έχει ορισθεί στην περιγραφή των υπηρεσιών την οποία έχουν παράγει τα ΣυΕ.

- Τον *Ελεγκτή Διαλειτουργικότητας*, ο οποίος ανακτά και αξιολογεί τα αποτελέσματα των ελέγχων διαλειτουργικότητας τα οποία εκτελέστηκαν από τα ΣυΕ στη φάση 4 με σκοπό:
    - την υπόδειξη της δυνατότητας επικοινωνίας των εμπλεκόμενων ΣυΕ,
    - την ανίχνευση και εντοπισμό μη συμβατών σημείων επικοινωνίας και μη έγκυρων συμπεριφορών και
    - την απόδοση ευθύνης στο αντίστοιχο ΣυΕ στην περίπτωση μη επιτυχούς επικοινωνίας.

Τα παραπάνω συμπεράσματα προκύπτουν από την ολοκλήρωση μιας σαφώς ορισμένης διαδικασίας η οποία αποτελείται από τρία βασικά βήματα. Το πρώτο βήμα περιλαμβάνει τον έλεγχο ότι οι διαδικασίες των ΣυΕ κατέχουν και επεξεργάζονται τα δεδομένα προς αξιολόγηση επιτυχώς χωρίς τον εντοπισμό ενδείξεων που να υποδηλώνουν την ύπαρξη προβληματικής εκτέλεσης των επιμέρους διαδικασιών. Το γεγονός αυτό υποδεικνύει ότι τα δεδομένα αυτά είναι έγκυρα για όλα τα ΣυΕ. Το δεύτερο βήμα αποτελείται από μια διαδικασία σύγκρισης κατά τη διάρκεια της οποίας όλα τα δεδομένα τα οποία ανταλλάσσονται (π.χ. SOAP μηνύματα και έγγραφα) μεταξύ των ΣυΕ συγκρίνονται προκειμένου να επιβεβαιωθεί ότι τα ΣυΕ έχουν στην κατοχή τους και επεξεργάζονται τα ίδια δεδομένα. Στο τελευταίο βήμα ο Ελεγκτής Διαλειτουργικότητας ελέγχει και επαληθεύει ότι τα ανταλλασσόμενα μηνύματα είναι μέρος των επιχειρησιακών διαδικασιών όπως αυτές έχουν οριστεί από τα ΣυΕ στις αντίστοιχες περιγραφές των υπηρεσιών τους. Τα βήματα αυτά επιτρέπουν στον Ελεγκτή Διαλειτουργικότητας να διαπιστώσει τη δυνατότητα επικοινωνίας των ΣυΕ και το βαθμό στον οποίο αυτό επιτυγχάνεται κατά τη διάρκεια της τελευταίας φάσης της μεθοδολογίας.

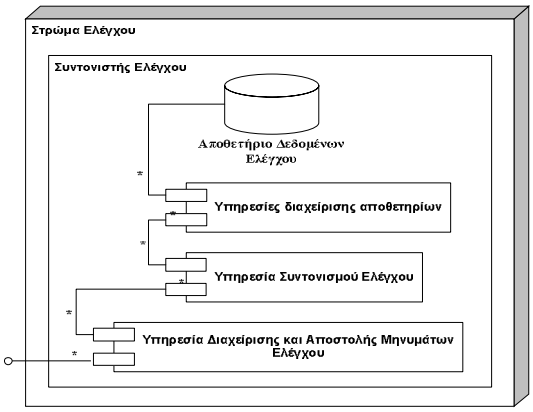
Οι πραγματικές διαδικασίες που πραγματοποιούνται με την συμμετοχή της ΥΔΕ περιγράφονται στις φάσεις 3 και 4. Η δομή της ΥΔΕ μπορεί να ποικίλει ανάλογα με το είδος αλλά και τις περιπτώσεις ελέγχου οι οποίες εφαρμόζονται. Η υιοθέτηση του συνόλου των ανωτέρω συστατικών συνθέτουν μια πλήρη και καλά ορισμένη ΥΔΕ η οποίο έχει την δυνατότητα να επιβλέψει και να εκτελέσει ένα μεγάλο πλήθος ελέγχων.

Στις παραγράφους που ακολουθούν θα παραρουσιαστούν τα ακριβή δομικά στοιχεία από τα οποία συντίθενται τα προαναφερθέντα, στρώματα καθώς επίσης και η προσφερόμενη λειτουργικότητάς τους.

2.3.4.2.1 Στρώμα Ελέγχου

Το βασικό συστατικό του Στρώματος Ελέγχου είναι ο Συντονιστής Ελέγχου (βλ. § 2.3.4.2) ο οποίος αποτελείται από ένα σύνολο από δομικά στοιχεία τα οποία απεικονίζονται στο Σχήμα 13. Τα στοιχεία αυτά είναι τα ακόλουθα:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



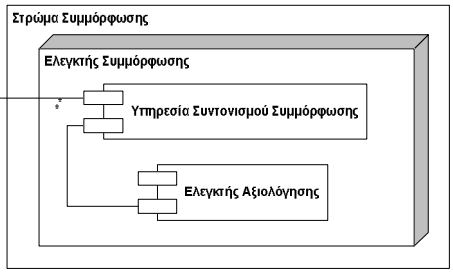
Σχήμα 13: Στρώμα Ελέγχου

- *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου*: αναλαμβάνει τη διαχείριση και αποστολή των μηνυμάτων που απαιτούνται για την κλήση των διεπαφών των ΣυΕ κατά την τρίτη και τέταρτη φάση της μεθοδολογίας. Πρωταρχική μέριμνα είναι η δόμηση των μηνυμάτων με την εισαγωγή των απαιτούμενων στοιχείων ελέγχου (δεδομένα ελέγχου) και η μεταφορά τους στα ΣυΕ.
- *Υπηρεσία Συντονισμού Ελέγχου*: συντονίζει το σύνολο των λειτουργιών οι οποίες προσφέρονται από το Στρώμα Ελέγχου προκειμένου να ολοκληρωθεί η κλήση των διεπαφών των ΣυΕ.
- *Υπηρεσίες διαχείρισης αποθετηρίων:* ελέγχουν τις συναλλαγές με τα αποθετήρια (π.χ. βάση δεδομένων) που εμπεριέχονται στο στρώμα ελέγχου. Οι υπηρεσίες αυτές επιτρέπουν την απόθεση και την ανάκτηση των δεδομένων ελέγχου.
- *Αποθετήριο Δεδομένων Ελέγχου:* το μέσο στο οποίο αποθηκεύονται και από το οποίο ανακτώνται τα δεδομένα ελέγχου που απαιτούνται για την εκτέλεση των περιπτώσεων ελέγχων.

Το Στρώμα Ελέγχου διαδραματίζει κυρίαρχο ρόλο στην τρίτη και τέταρτη φάση της μεθοδολογίας κατά την διάρκεια των οποίων λαμβάνουν χώρα αντίστοιχα οι Έλεγχοι Συμμόρφωσης και Διαλειτουργικότητας. Στις Παραγράφους 2.3.5 και 2.3.6 θα παρουσιαστούν διαγράμματα τα οποία περιγράφουν αναλυτικά την λειτουργία των προαναφερθέντων στοιχείων.

2.3.4.2.2 Στρώμα Συμμόρφωσης

Ο Ελεγκτής Συμμόρφωσης ως το βασικό συστατικό του Στρώματος Συμμόρφωσης (βλ. § 2.3.4.2) αποτελείται από την ακόλουθη σειρά δομικών στοιχείων (Σχήμα 14):



Σχήμα 14: Στρώμα Συμμόρφωσης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- *Ελεγκτής Αξιολόγησης*: αποτελείται από ένα σύνολο εργαλείων και βιβλιοθηκών ελέγχου τα οποία αξιολογούν την συμμόρφωση των δεδομένων που παράγονται από την εκτέλεση των περιπτώσεων ελέγχου στην 3η φάση της μεθοδολογίας έναντι των αντίστοιχων προτύπων. Τα εργαλεία και οι βιβλιοθήκες οι οποίες πρέπει να υιοθετηθούν και να ενσωματωθούν είναι άρρηκτα συνδεδεμένα με τα πρότυπα από τα οποία απαρτίζονται τα ΣυΕ, όπως αυτά καθορίστηκαν στο 3ο βήμα του καθορισμού ενός ΣυΕ (βλ. § 2.3.4.1.4). Τα εργαλεία αυτά κατηγοριοποιούνται ως εξής:
    - εργαλεία, βιβλιοθήκες ή ακόμα και ιστοχώροι που παρέχουν μηχανισμούς αξιολόγησης, οι οποίοι απαιτείται να χρησιμοποιηθούν για να ελέγξουν την συμμόρφωση των εφαρμοζόμενων μηχανισμών ασφάλειας των ανταλλασσόμενων εγγράφων σε σχέση με τα αντίστοιχα πρότυπα.
    - εργαλεία, βιβλιοθήκες ή ακόμα και ιστοχώροι που παρέχουν μηχανισμούς αξιολόγησης οι οποίοι απαιτείται να χρησιμοποιηθούν για να ελέγξουν την συμμόρφωση των ανταλλασσόμενων μηνυμάτων και των εφαρμοζόμενων σε αυτά μηχανισμών ασφάλειας καθώς, επίσης και την περιγραφή των υπηρεσιών ως προς τα αντίστοιχα πρότυπα των Υπηρεσιών Ιστού.
    - εργαλεία, βιβλιοθήκες ή ακόμα και ιστοχώροι που παρέχουν μηχανισμούς αξιολόγησης οι οποίοι απαιτείται να χρησιμοποιηθούν για να ελέγξουν την συμμόρφωση των παραγόμενων ή μετασχηματιζόμενων εγγράφων προς τα αντίστοιχα σχήματα ή ακόμα και την συμμόρφωση των ίδιων των μηχανισμών μετασχηματισμού που χρησιμοποιούνται.

  Τα ακριβή βήματα τα οποία πρέπει να ακολουθηθούν για την ολοκλήρωση του Ελεγκτή Αξιολόγησης είναι τα ακόλουθα:
    1. *Κατηγοριοποίηση των χρησιμοποιούμενων προτύπων* των ΣυΕ, όπως αυτά καταγράφηκαν στο 3ο βήμα του καθορισμού ενός ΣυΕ.
    2. *Καταγραφή των απαιτούμενων εργαλείων* που απαιτούνται για καθεμία από τις κατηγορίες που προκύπτουν από το πρώτο βήμα, ώστε να ελεγχθεί η συμμόρφωση μιας ΥΙυΕ ως προς τις αντίστοιχες προδιαγραφές. Οι βασικές λειτουργίες οι οποίες πρέπει να καλύπτουν τα εργαλεία είναι οι ακόλουθες:
        i. Εργαλεία που ελέγχουν την συμμόρφωση των παραγόμενων εγγράφων προς τα αντίστοιχα σχήματα.
        ii. Εργαλεία τα οποία ελέγχουν ότι οι μηχανισμοί ασφάλειας που εφαρμόζονται στα έγγραφα συμμορφώνονται στις αντίστοιχες προδιαγραφές.
        iii. Εργαλεία τα οποία ελέγχουν τη συμμόρφωση των ανταλλασσόμενων μηνυμάτων και των εφαρμοζόμενων σε αυτά μηχανισμών ασφάλειας καθώς επίσης και τη συμμόρφωση των περιγραφών των παρεχόμενων ΥΙ στις αντίστοιχες προδιαγραφές.
    3. *Αναζήτηση και συλλογή* υπαρχόντων εργαλείων, βιβλιοθηκών και ιστοχώρων που μπορεί να χρησιμοποιηθούν ως μηχανισμοί αξιολόγησης.
    4. *Επιλογή και ενσωμάτωση* των μηχανισμών που θα χρησιμοποιηθούν στην ΥΔΕ. Οι μηχανισμοί αυτοί ενσωματώνονται στον Ελεγκτή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

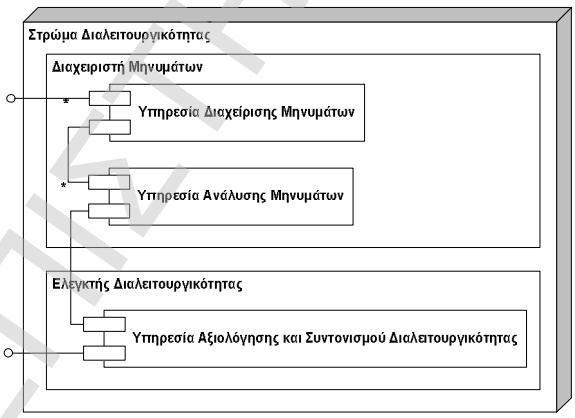
Αξιολόγησης και υφίσταται την απαιτούμενη διαμόρφωση μέσω της υλοποίησης κατάλληλων διεπαφών οι οποίες είναι απαραίτητες για την κλήση και χρήση των συγκεκριμένων εργαλείων. Στην περίπτωση κατά την οποία οι απαιτούμενες διεπαφές δεν μπορούν να υλοποιηθούν λόγω της φύσης των εργαλείων ελέγχου, θεωρείται επιβεβλημένη η χρήση μιας ημι-αυτοματοποιημένης διαδικασίας για την αξιολόγηση τη συμμόρφωσης των δεδομένων.

- *Υπηρεσία Συντονισμού Συμμόρφωσης*: λαμβάνει σαν είσοδο τα αρχεία αναφορών που παράγονται από τα ΣυΕ και καθορίζει τα εργαλεία του Ελεγκτή Αξιολόγησης τα οποία πρέπει να χρησιμοποιηθούν για να αξιολογηθεί η συμμόρφωση των περικλειόμενων δεδομένων μέσω της κλήσης των διεπαφών των αντίστοιχων εργαλείων του Ελεγκτή Αξιολόγησης. Η υπηρεσία αναλαμβάνει παράλληλα τη λήψη και την καταγραφή των αποτελεσμάτων της αξιολογήσης όπως αυτά παράγονται από τα εργαλεία του ελεγκτή.

Το Στρώμα Συμμόρφωσης διαδραματίζει κυρίαρχο ρόλο στην $3^{η}$ φάση της μεθοδολογίας όπου εκτελείται ο Έλεγχος Συμμόρφωσης. Στο Κεφάλαιο 2.3.5 παρατίθενται αναλυτικά η διαδικασία ολοκλήρωσης του Ελέγχου Συμμόρφωσης.

2.3.4.2.3 Στρώμα Διαλειτουργικότητας

Το Στρώμα Διαλειτουργικότητας αποτελείται από δύο βασικά συστατικά: τον Διαχειριστή Μηνυμάτων και τον Ελεγκτή Διαλειτουργικότητας (βλ. § 2.3.4.2). Τα συστατικά αυτά έχουν συγκεκριμένες και αυστηρά ορισμένες αρμοδιότητες καθιστώντας το ρόλο τους πλήρως διακριτό και ανεξάρτητο. Για την επιτυχή εκπλήρωση των κεντρικών τους στόχων κάθε ένα από τα συστατικά αυτά απαρτίζεται από ένα σύνολο από δομικά στοιχεία όπως φαίνεται από το Σχήμα 15.



Σχήμα 15. Στρώμα Διαλειτουργικότητας

Ο Διαχειριστής Μηνυμάτων συνίσταται από τα εξής επιμέρους στοιχεία:

- *Υπηρεσία Διαχείρισης Μηνυμάτων*: παρέχει δύο βασικές λειτουργίες. Παρεμβάλλεται μεταξύ των ΣυΕ, 'υποκλέπτοντας' τα ανταλλασσόμενα μηνύματα, λειτουργώντας ουσιαστικά σαν μια ενδιάμεση οντότητα η οποία λαμβάνει και στην συνέχεια προωθεί ένα μήνυμα στον παραλήπτη του. Η δεύτερη λειτουργία του αφορά τη καταγραφή των μηνυμάτων αυτών σε μια μορφή που επιτρέπει την περαιτέρω ανάλυσή τους από την Υπηρεσία Ανάλυσης Μηνυμάτων.
- *Υπηρεσία Ανάλυσης Μηνυμάτων*: δέχεται ως είσοδο τα μηνύματα που έχουν ληφθεί από την *Υπηρεσία Διαχείρισης Μηνυμάτων* και τα αναλύει με στόχο να

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

τα συσχετίσει με την περιγραφή της ΥΙ, όπως αυτή έχει παραχθεί από το αντίστοιχο ΣυΕ. Τα αποτελέσματα της ανάλυσης καταγράφονται τελικώς σε μια αναφορά η οποία θα χρησιμοποιηθεί για την τελική αξιολόγηση της επικοινωνίας των ΣυΕ που θα πραγματοποιηθεί από τις αντίστοιχες υπηρεσίες του στρώματος διαλειτουργικότητας οι οποίες θα αναλυθούν στην συνέχεια.

Το δεύτερο συστατικό του στρώματος διαλειτουργικότητας, ο Ελεγκτής Διαλειτουργικότητας, αναλάμβάνει την τελική ευθύνη της αξιολόγησης του συνόλου των αποτελεσμάτων τα οποία παράγονται από τον Έλεγχο Διαλειτουργικότητας (βλ. § 2.3.6). Τα βασικά δομικά στοιχεία από τα οποία αποτελείται το στοιχείο αυτό όπως και η προσφερόμενη λειτουργικότητα τους παρουσιάζονται στην συνέχεια:

- *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας*: λαμβάνει σαν είσοδο τα αρχεία αναφορών που παράγονται από τα ΣυΕ τα οποία περιέχουν τα δεδομένα προς αξιολόγηση. Βασική της αρμοδιότητα είναι η εκτέλεση ενός συνόλου διαδικασιών όπως είναι οι ακόλουθες:
  - αξιολογεί το σύνολο των διαδικασιών που αφορούν την διαχείριση των ανταλλασσόμενων εγγράφων καθώς επίσης και το επίπεδο της ασφάλειας που εφαρμαρμόστηκε σε αυτά από τα ΣυΕ κατά την διάρκεια του ελέγχου.
  - αξιολογεί το σύνολο των διαδικασιών που αφορούν την διαχείριση των ανταλλασσόμενων μηνυμάτων καθώς επίσης και το επίπεδο της ασφάλειας που εφαρμαρμόστηκε σε αυτά από τα ΣυΕ κατά την διάρκεια του ελέγχου. Επίσης επικοινωνεί με την *Υπηρεσία Ανάλυσης Μηνυμάτων* του Διαχειριστή Μηνυμάτων ώστε να λάβει τις αναφορές που σχετίζονται με τη συμμόρφωση των μηνυμάτων ως προς την περιγραφή των αντίστοιχων ΥΙ.
  - αξιολογεί το σύνολο των διαδικασιών που αφορούν τον μετασχηματισμό των ανταλλασσόμενων εγγράφων καθώς επίσης και την απόθεση τους στα συστήματα που διαθέτει το κάθε ΣυΕ κατά την διάρκεια του ελέγχου.

  Με βάση τα αποτελέσματα των παραπάνω διαδικασιών αξιολόγησης η υπηρεσία υποδεικνύει την δυνατότητα αλληλεπίδρασης των ΣυΕ, αναφέροντας μη έγκυρες συμπεριφορές και κάνοντας απόδοση ευθυνών στο ΣυΕ που κρίνεται ότι είναι υπαίτιο σε περίπτωση αποτυχίας της επικοινωνίας.

Το Στρώμα Διαλειτουργικότητας διαδραματίζει κυρίαρχο ρόλο στη 4^{η} φάση της μεθοδολογίας που αφορά τον Έλεγχο Διαλειτουργικότητας. Στο Κεφάλαιο 2.3.6 θα πραγματοποιηθεί μια αναλυτική παρουσίαση της ροής των πληροφοριών μεταξύ των προαναφερθέντων στοιχείων μέσω της χρήσης διαγραμμάτων, δίνοντας παράλληλα τη δυνατότητα καλύτερης κατανόησης της λειτουργίας των στοιχείων αυτών.

2.3.5 Φάση 3: Έλεγχος Συμμόρφωσης

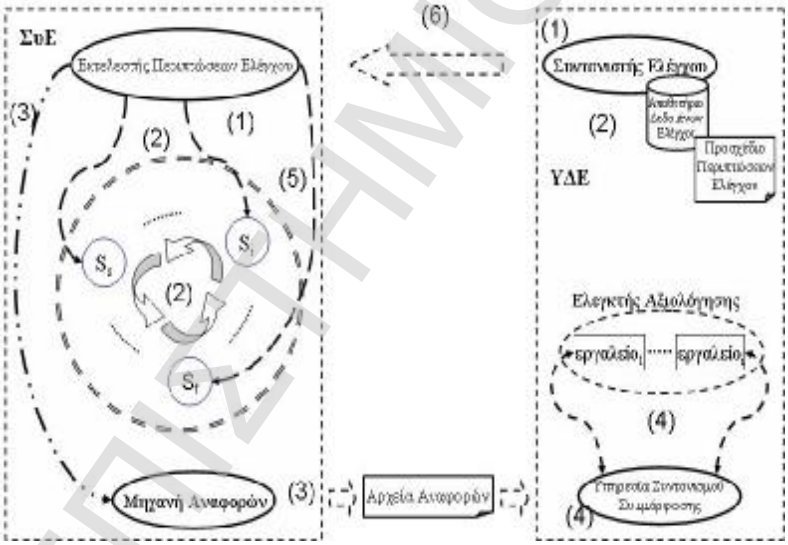
2.3.5.1 Επισκόπηση των Σταδίων Ελέγχου Συμμόρφωσης

Ο Έλεγχος Συμμόρφωσης θέτει ως πρωταρχικό στόχο την εξέταση της συμμόρφωσης κάθε ΣυΕ ως προς τα πρότυπα τα οποία έχει υιοθετήσει και υλοποιεί. Στο παρόν κεφάλαιο πραγματοποιείται η επισκόπηση των σταδίων ελέγχου συμμόρφωσης τα οποία πρέπει να εκτελεστούν. Η προτεινόμενη μεθοδολογία αποτελείται από έξι βασικά στάδια, τα οποία παρουσιάζονται στο Σχήμα 16:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Σχήμα 16: Τα έξι στάδια Ελέγχου Συμμόρφωσης

Στο Σχήμα 17 απεικονίζονται οι βασικές οντότητες που λαμβάνουν μέρος σε έναν έλεγχο συμμόρφωσης, ένα ΣυΕ και η ΥΔΕ, όπως επίσης και μια οπτική αναπαράσταση των εκτελέσιμων προτεινόμενων σταδίων. Η αναλυτική περιγραφή κάθε σταδίου περιλαμβάνεται στις παραγράφους που ακολουθούν.



Σχήμα 17: Οντότητες και Εκτελέσιμα Βήματα Ελέγχου Συμμόρφωσης

2.3.5.1.1 1ο στάδιο: Καθορισμός Περιπτώσεων Ελέγχου

2.3.5.1.1.1 Στόχοι

Το στάδιο αυτό είναι προπαρασκευαστικό προκειμένου να αρχικοποιηθεί ο έλεγχος συμμόρφωσης. Βασικός στόχος του σταδίου αποτελεί η αποτύπωση και δημιουργία των περιπτώσεων ελέγχου οι οποίες θα πρέπει να εκτελεστούν προκειμένου να διαπιστωθεί η συμμόρφωση του ΣυΕ απέναντι στα πρότυπα τα οποία έχει υιοθετήσει και υλοποιεί. Η ομαλή διεξαγωγή του σταδίου αυτού εξασφαλίζει την εφαρμογή ενός ολοκληρωμένου ελέγχου εξετάζοντας ένα ευρύ φάσμα πτυχών και παραμέτρων.

2.3.5.1.1.2 Μεθοδολογία Σταδίου για τον Καθορισμό Περιπτώσεων Ελέγχου

Το παρόν στάδιο περιλαμβάνει τα ακόλουθα βήματα:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

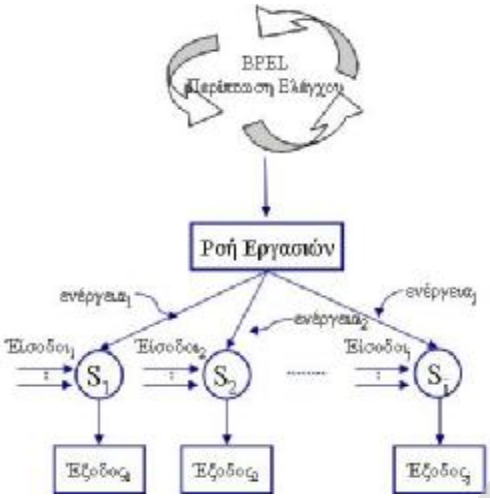
1. *Σχεδιασμός* των περιπτώσεων ελέγχου που πρέπει να εφαρμοστούν, λαμβάνοντας υπόψη τα πρότυπα τα οποία υλοποιεί μια ΥΙυΕ. Τα πρότυπα αυτά καταγράφηκαν στο 3ο βήμα του καθορισμού ενός ΣυΕ (βλ. § 2.3.4.1.4). Βασικός στόχος του συγκεκριμένου βήματος είναι ο καθορισμός και ο σχεδιασμός των περιπτώσεων ελέγχου που θα οδηγήσουν στην παραγωγή των απαιτούμενων δεδομένων αξιολόγησης. Στο Κεφάλαιο 2.3.5.1.1.3 παρουσιάζεται ο ακριβής ορισμός μιας σειράς περιπτώσεων ελέγχου συμμόρφωσης, ο τρόπος με τον οποίο αυτές μπορούν να απεικονιστούν καθώς επίσης και τα βήματα που πρέπει να εκτελεστούν για τη σχεδίασή τους.
2. *Διαμόρφωση και παραγωγή* των περιπτώσεων ελέγχου όπως αυτές σχεδιάστηκαν στο προηγούμενο βήμα. Στο Κεφάλαιο 2.3.5.1.1.4 αναφέρονται πρότυπα και μοντέλα που μπορεί να χρησιμοποιηθούν για την παραγωγή διαδικασιών που αναπαριστούν περιπτώσεις ελέγχου.
3. *Ενσωμάτωση* των παραγόμενων διαδικασιών περιπτώσεων ελέγχων, που παράγονται στο 2^{ο} βήμα στον Εκτελεστή Περιπτώσεων Ελέγχου με παράλληλη υλοποίηση των απαιτούμενων διεπαφών.
4. *Παραγωγή* των δεδομένων ελέγχου που απαιτούνται από τις περιπτώσεις ελέγχου (Προαιρετικό βήμα).
5. *Αποθήκευση* των παραγόμενων δεδομένων ελέγχου στο Αποθετήριο Δεδομένων Ελέγχου της ΥΔΕ (Προαιρετικό βήμα).
6. *Καθορισμός* της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου. Η αλληλουχία των ελέγχων θα πρέπει να πραγματοποιείται με λογικό τρόπο ώστε να εξασφαλίζεται η αποτελεσματικότητα τους. Πρωταρχικό κριτήριο για την επιλογή της σειράς είναι η πολυπλοκότητά των περιπτώσεων ελέγχου (έλεγχος αρχικά των βασικών λειτουργιών και συνέχιση με τις πιο πολύπλοκες).
7. *Αποτύπωση* της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου σε ένα προσχέδιο. Το προσχέδιο περιέχει τα URL των διαδικασιών BPEL που πρέπει να κληθούν από την ΥΔΕ όπως και τα δεδομένα ελέγχου που πιθανόν να απαιτούνται. Η αποθήκευση του προσχεδίου γίνεται στο Αποθετήριο Δεδομένων Ελέγχου της ΥΔΕ.

Στο πέρας του βήματος (7), έχει καταγραφεί και δημιουργηθεί το σύνολο των περιπτώσεων ελέγχου με βάση τις οποίες πρέπει να ελεγχθεί ένα ΣυΕ, καθώς επίσης και η σειρά εκτέλεσής τους. Παράλληλα, έχει ολοκληρωθεί η τελική μορφή και δομή των ΣυΕ με την οποία θα πάρουν μέρος στον Έλεγχο Συμμόρφωσης με την ενσωμάτωση των διαδικασιών των περιπτώσεων ελέγχων.

2.3.5.1.1.3 Περιπτώσεις Ελέγχου Συμμόρφωσης

Μια περίπτωση ελέγχου αποτελείται από μια μερικώς-διατεταγμένη λίστα βασικών ενεργειών οι οποίες πρέπει να εκτελεστούν ώστε να παραχθούν τα δεδομένα αξιολόγησης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



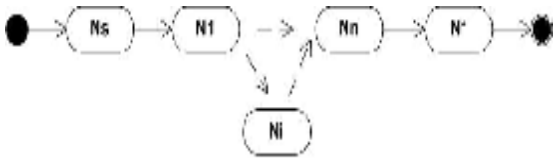
Σχήμα 18. BPEL Περίπτωση Ελέγχου

Όπως απεικονίζεται στο Σχήμα 18 μία περίπτωση ελέγχου ορίζεται ως εξής:

Περίπτωση ελέγχου = {Ενέργεια$_j$, Υπηρεσία$_j$, Είσοδος$_j$, Έξοδος$_j$}.

- Ενέργεια$_j$, ένα σύνολο από ενέργειες οι οποίες πρέπει να εκτελεστούν.
- Υπηρεσία$_j$, ένα σύνολο από πρωτεύουσες υπηρεσίες της ΥΙυΕ οι οποίες θα πρέπει να κληθούν και να συντονιστούν για την εκτέλεση της περίπτωσης ελέγχου. Κάθε υπηρεσία συνδέεται με την εκτέλεση μιας συγκεκριμένης ενέργειας.
- Έξοδος$_j$, ένα σύνολο από αποτελέσματα τα οποία παράγουν οι Υπηρεσίες$_j$. Τα αποτελέσματα αυτά αποτελούν τα δεδομένα αξιολόγησης των ΥΙυΕ.
- Είσοδος$_j$, ένα σύνολο από παραμέτρους τις οποίες κάθε Υπηρεσία$_j$ απαιτεί ώστε να ολοκληρωθεί η εκτέλεση μιας προκαθορισμένης διαδικασίας. Ως είσοδοι μπορούν να θεωρηθούν:
  - δεδομένα ελέγχου τα οποία τροφοδοτούνται από την ΥΔΕ κατά την διάρκεια αρχικοποίησης μια διαδικασίας ελέγχου,
  - έξοδοι άλλων πρωτεύουσων υπηρεσιών,
  - παράμετροι οι οποίες έχουν καθοριστεί και περιλαμβάνονται στις ίδιες τις διαδικασίες.

Στην περίπτωση του ελέγχου συμμόρφωσης, οι περιπτώσεις ελέγχου που πρέπει να καθοριστούν αποτελούνται μόνο από *εσωτερικές ενέργειες*. Αυτό σημαίνει ότι για την εκτέλεση των συγκεκριμένων περιπτώσεων ελέγχου χρειάζεται να αλληλεπιδράσουν μόνο οι πρωτεύουσες υπηρεσίες που περιέχονται στην ΥΙυΕ προκειμένου να παραχθούν τα απαιτούμενα δεδομένα αξιολόγησης.



Σχήμα 19. Διάγραμμα Ενεργειών Περιπτώσεως Ελέγχου

Ένα διάγραμμα ενεργειών (activity graph diagram), όπως φαίνεται στο Σχήμα 19 μπορεί επίσης να χρησιμοποιηθεί σαν μια οπτική αναπαράσταση των χρησιμοποιούμενων περιπτώσεων ελέγχου. Το διάγραμμα ενεργειών έχει τη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

δυνατότητα να απεικονίσει τη ροή των ενεργειών που πρέπει να εκτελεστούν με τρόπο αποτελεσματικό. Ένα τέτοιο διάγραμμα συντίθεται από τα εξής στοιχεία:

$\{N, E, N_s, N_f\}$,

όπου N είνα ένα σύνολο από κόμβους $\{N_1,...,N_n\}$, οι οποίοι αντιστοιχούν σε εφαρμοζόμενες ενέργειες,
Ε είνα ένα σύνολο από ακμές $\{E_1,...,E_n\}$ οι οποίες αποτελούν αυστηρές ακολουθίες καθοριζόμενες από την εκτελούμενη ροή εργασιών, και
N_s είναι ο Αρχικός Κόμβος και N_f ο Τελικός Κόμβος μιας ροής εργασίας.

Το στοιχείο που πρέπει να σημειωθεί είναι ότι τα δεδομένα προς αξιολόγηση προκύπτουν συνήθως από τον Τελικό Κόμβο (N_f) μιας ροής εργασίας.
Συνοψίζοντας, λοιπόν, παρατίθενται μια σειρά υποβημάτων τα οποία πρέπει να ακολουθηθούν προκειμένου να σχεδιαστούν οι περιπτώσεις ελέγχου συμμόρφωσης. Τα υποβήματα αυτά είναι τα ακόλουθα:

1. *Επισήμανση* του υπό εξέταση προτύπου.
2. *Ορισμός* περίπτωσης ελέγχου με βάση τον ορισμό που δόθηκε παραπάνω.
3. *Απεικόνιση* της περίπτωσης ελέγχου με χρήση ενός διαγράμματος ενεργειών.

Η ολοκλήρωση των ανωτέρω υποβημάτων επιτρέπει το σαφή προσδιορισμό του συνόλου των εξεταζόμενων περιπτώσεων ελέγχου.

2.3.5.1.1.4 Παραγωγή Περιπτώσεων Ελέγχου Συμμόρφωσης

Στο Κεφάλαιο 2.3.4.1 καθορίστηκε ότι η προτεινόμενη μεθοδολογία υιοθετεί μια αναπαράσταση BPEL των εφαρμοζόμενων περιπτώσεων ελέγχων. Η απόφαση αυτή βασίστηκε στον εντοπισμό μιας σειράς μειονεκτημάτων και περιορισμών [Pentafronimos08] που παρουσιάζουν ένα σύνολο γλωσσών που έχουν χρησιμοποιηθεί για την αναπαράσταση και υλοποίηση των περιπτώσεων ελέγχων καθώς επίσης έλαβε υπόψη της και τη φύση και τα χαρακτηριστικά γνωρίσματα της ίδιας της γλώσσας BPEL.
Σε γενικές γραμμές, η BPEL επιτρέπει τον καθορισμό και την αναπαράσταση μιας συγκεκριμένης επιχειρησιακής ροής σε μια μορφή XML. Η BPEL εμπεριέχει μοναδικά στοιχεία σε συντακτικό (π.χ. ροές με συγχρονισμό ενεργειών, τελετές σύνδεσης) και σημασιολογικό επίπεδο που την καθιστά μια υψηλής εκφραστικότητας συμπαγή γλώσσα. Στη βιβλιογραφία, εκτενής έρευνα έχει πραγματοποιηθεί όσον αφορά τον ακριβή σημασιολογικό καθορισμό της BPEL καθώς επίσης και την παρουσίαση μοντέλων επικύρωσης BPEL [Fostre06, Xu06]. Επιπρόσθετα, έχει περιγραφεί ένα σύνολο από πλαίσια και μοντέλα [Zheng07, Sinha06, Yuan06, Yan06] τα οποία επιτρέπουν τον αυτοματοποιημένο καθορισμό και παραγωγή την περιπτώσεων ελέγχων βασισμένων στην BPEL.
Μέχρι σήμερα, οι περιπτώσεις ελέγχου BPEL στο σύνολο τους έχουν χρησιμοποιηθεί για να ελέγξουν εάν η συμπεριφορά της διαδικασίας BPEL μιας ΥΙ είναι σύμφωνη με τους στόχους και τις αρχές που έχουν καθοριστεί από την ίδια την ΥΙ. Στην προτεινόμενη μεθοδολογία, οι διαδικασίες BPEL που καθορίζονται και υιοθετούνται αναπαριστούν ροές ενεργειών που απεικονίζουν τον τρόπο με τον οποίο οι πρωτεύουσες υπηρεσίες των ΥΙυΕ πρέπει να συγχρονιστούν για την παραγωγή των

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

απαιτούμενων δεδομένων αξιολόγησης με βάση τα οποία θα ελεγχθεί η δυνατότητα συμμόρφωσης και διαλειτουργικότητας των ΥΙυΕ.
Για την παραγωγή συγκεκριμένων διαδικασιών BPEL μπορεί να χρησιμοποιηθούν υπάρχοντα πλαίσια παραγωγής περιπτώσεων ελέγχου BPEL ή άλλοι μηχανισμοί δημιουργίας διαδικασιών BPEL [ActiveBPEL].

2.3.5.1.2 2ο στάδιο: Εκτέλεση Περιπτώσεων Ελέγχου

2.3.5.1.2.1 Στόχοι

Στο παρόν στάδιο πραγματοποιείται η εκτέλεση των περιπτώσεων ελέγχων όπως αυτές ορίστηκαν στο 1ο στάδιο της μεθοδολογίας. Πρέπει να σημειωθεί ότι στον έλεγχο συμμόρφωσης συμμετέχουν μόνο ένα ΣυΕ και η ΥΔΕ.

2.3.5.1.2.2 Μεθοδολογία Σταδίου για την Εκτέλεση των Περιπτώσεων Ελέγχου

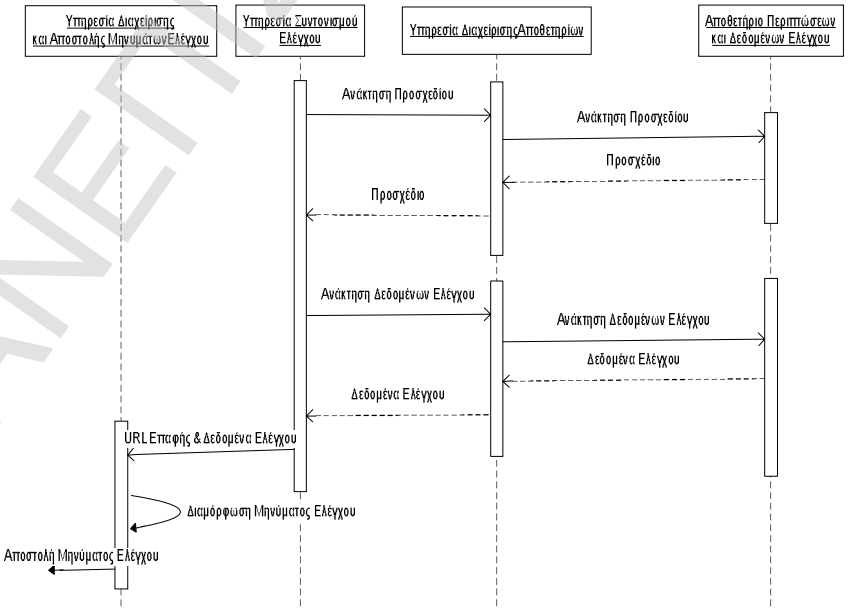
Το παρόν στάδιο αποτελείται από τα εξής επιμέρους βήματα:

1. Η *ΥΔΕ* αρχικοποιεί και συντονίζει την εκτέλεση των περιπτώσεων ελέγχων με την κλήση των αντίστοιχων διεπαφών ακολουθώντας το προσχέδιο που καθορίστηκε στο 1ο στάδιο της συγκεκριμένης φάσης. Στο Κεφάλαιο 2.3.5.1.2.3 αναλύεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.
2. Το *ΣυΕ* αναλαμβάνει την εκτέλεση των περιπτώσεων ελέγχων συντονίζοντας τα απαραίτητα συστατικά της ΥΙυΕ. Στο Κεφάλαιο 2.3.5.1.2.4 παρατίθεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.

Στο πέρας του βήματος (2), έχουν παραχθεί τα δεδομένα προς αξιολόγηση τα οποία απαιτούνται για να ελεγχθεί η συμμόρφωση της ΥΙυΕ ως προς τις αντίστοιχες προδιαγραφές.

2.3.5.1.2.3 ΥΔΕ: Αρχικοποίηση και Συντονισμός Εκτέλεσης των Περιπτώσεων Ελέγχου

Στο Σχήμα 20 παρέχεται το διάγραμμα ακολουθίας που παρουσιάζει τη διαδικασία που εκτελείται από τον *Συντονιστή Ελέγχου* της ΥΔΕ (βλ. § 2.3.4.2.1) και αποσκοπεί στην αρχικοποίηση και στο συντονισμό της εκτέλεσης των περιπτώσων ελέγχου.



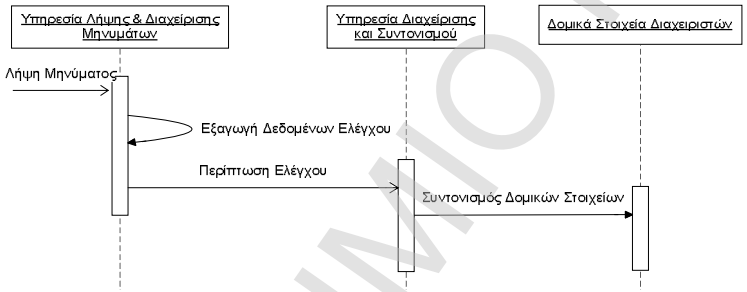
Σχήμα 20: ΥΔΕ: Αρχικοποίηση και Συντονισμός Εκτέλεσης των Περιπτώσεως Ελέγχου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η διαδικασία αρχικοποιείται από την *Υπηρεσία Συντονισμού Ελέγχου* η οποία φέρει την ευθύνη του συντονισμού όλων των απαιτούμενων λειτουργιών. Αρχικά αναθέτει στην *Υπηρεσία Διαχείρισης Αποθετηρίων* την ανάκτηση του προσχεδίου από το *Αποθετήριο Δεδομένων Ελέγχου* με βάση το οποίο θα πραγματοποιηθεί η εκτέλεση των περιπτώσεων ελέγχου. Στην συνέχεια αναλαμβάνει το συντονισμό της εκτέλεσής τους ανακτώντας τα δεδομένα ελέγχου που ενδέχεται να απαιτούνται από το αποθετήριο και αναθέτοντας στην *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου* να διαμορφώσει τα απαραίτητα μήνυμα ελέγχου μέσω των οποίων θα γίνει η κλήση των αντίστοιχων διεπαφών του ΣυΕ.

2.3.5.1.2.4 ΣυΕ: Εκτέλεση Περιπτώσεως Ελέγχου

Το διάγραμμα ακολουθίας του Σχήμα 21 περιγράφει τη διαδικασία λήψης και διαχείρισης του μηνύματος που περιέχει τα στοιχεία που απαιτούνται για την εκτέλεση του ελέγχου συμμόρφωσης από το ΣυΕ. Ο *Εκτελεστής Περιπτώσεων Ελέγχου* αποτελεί το συστατικό του ΣυΕ (βλ. § 2.3.4.1.2) που αναλαμβάνει τη διαδικασία αυτή.



Σχήμα 21: Εκτέλεση Περιπτώσεως Ελέγχου

Αναλυτικότερα τα ακριβή βήματα τα οποία εκτελούνται είναι τα ακόλουθα: η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* λαμβάνει το μήνυμα και το αποδομεί εξάγοντας τα περικλειόμενα δεδομένα ελέγχου. Ακολούθως, ενημερώνει την *Υπηρεσία Διαχείρισης και Συντονισμού* σχετικά με την διαδικασία BPEL η οποία πρέπει να εκτελεστεί, η οποία με τη σειρά της προβαίνει στο συντονισμό των πρωτεύουσων υπηρεσιών από τα οποία απαρτίζεται η ΥΙυΕ για την ολοκλήρωση της περιπτώσεως ελέγχου.

2.3.5.1.3 3ο στάδιο: Συλλογή των Δεδομένων Αξιολόγησης

2.3.5.1.3.1 Στόχοι

Ο βασικός στόχος του σταδίου είναι η συλλογή των δεδομένων τα οποία παράγονται από την εκτέλεση των περιπτώσεων ελέγχου.

2.3.5.1.3.2 Μεθοδολογία Σταδίου για τη Συλλογή των Δεδομένων Αξιολόγησης

Τα βήματα από τα οποία αποτελείται το παρόν 3ο στάδιο είναι τα ακόλουθα:

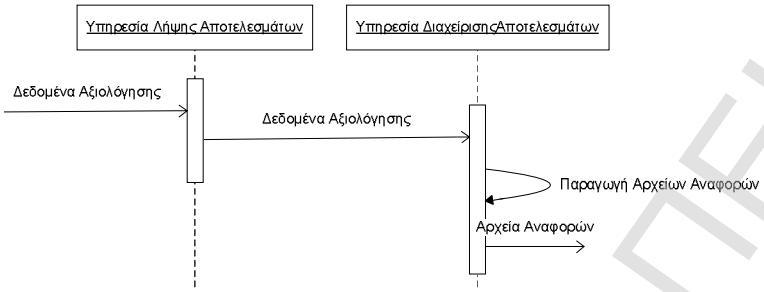
1. Η *Μηχανή Αναφορών* (βλ. § 2.3.4.1.3) εποπτεύει την εκτέλεση των περιπτώσεων ελέγχου και συλλέγει τα δεδομένα που παράγονται από το συντονισμό των υπηρεσιών της ΥΙυΕ.
2. Η *Μηχανή Αναφορών* συνθέτει τα συλλεγόμενα δεδομένα στην απαιτούμενη μορφή και τα ενσωματώνει σε αρχεία αναφορών (log files).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Στο πέρας του βήματος (2), τα δεδομένα είναι έτοιμα να ανακτηθούν από την ΥΔΕ ώστε να ελεγχθεί η συμμόρφωσή τους ως προς τις αντίστοιχες προδιαγραφές. Στο Κεφάλαιο 2.3.5.1.3.3 αναλύεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.

2.3.5.1.3.3 Λήψη Δεδομένων Αξιολόγησης από Μηχανή Αναφορών

Το διάγραμμα ακολουθίας του Σχήμα 22 περιγράφει τη διαδικασία καταγραφής των δεδομένων που έχουν συλλεγεί προς αξιολόγηση και την ενσωμάτωσή τους σε αρχεία αναφορών (log files). Η *Μηχανή Αναφορών* αποτελεί το συστατικό του ΣυΕ που αναλαμβάνει τη διαδικασία αυτή.



Σχήμα 22: Διαδικασία Λήψης Δεδομένων Αξιολόγησης από Μηχανή Αναφορών

Πιο συγκεκριμένα εκτελούνται τα εξής επιμέρους βήματα: η *Υπηρεσία Λήψης Αποτελεσμάτων* επικοινωνεί με τον *Εκτελεστή Περιπτώσεων Ελέγχου* και ανακτά τα δεδομένα προς αξιολόγηση. Στη συνέχεια, η *Υπηρεσία Διαχείρισης Αποτελεσμάτων* τα συνθέτει σε μια μορφή η οποία είναι σημασιολογικά αποδεκτή από την ΥΔΕ και τα ενσωματώνει σε αρχεία αναφορών (log files).

2.3.5.1.4 4ο στάδιο: Ανάλυση Αποτελεσμάτων

2.3.5.1.4.1 Στόχοι

Στο στάδιο αυτό λαμβάνει χώρα η ανάκτηση των αποτελεσμάτων προς αξιολόγηση από την ΥΔΕ και ο πραγματικός έλεγχος συμμόρφωσης των δεδομένων αυτών από τους υιοθετημένους μηχανισμούς αξιολόγησης.

2.3.5.1.4.2 Μεθοδολογία Σταδίου για την Ανάλυση των Αποτελεσμάτων

Το παρόν στάδιο περιλαμβάνει τα ακόλουθα βήματα:

1. *Ανάκτηση* των δεδομένων προς αξιολόγηση και ανάλυσή τους ώστε να διευκρινιστούν οι μηχανισμοί αξιολόγησης οι οποίοι πρέπει να χρησιμοποιηθούν.
2. *Ανάλυση* των δεδομένων και έλεγχος συμμόρφωσής τους ως προς τις αντίστοιχες προδιαγραφές με την είσοδο τους στους αντίστοιχους μηχανισμούς αξιολόγησης που είναι ενσωματωμένοι στην ΥΔΕ. Πιθανοί έλεγχοι οι οποίοι μπορεί να εκτελεστούν (βλ. § 2.3.4.2.2) είναι οι ακόλουθοι:
    i. έλεγχος της συμμόρφωσης των εφαρμοζόμενων μηχανισμών ασφάλειας των ανταλλασσόμενων εγγράφων προς τα αντίστοιχα πρότυπα.
    ii. έλεγχος της συμμόρφωσης των ανταλλασσόμενων μηνυμάτων και των εφαρμοζόμενων σε αυτά μηχανισμών ασφάλειας καθώς επίσης και την περιγραφή των ΥΙ προς τα αντίστοιχα πρότυπα.
    iii. έλεγχος της συμμόρφωσης των παραγόμενων εγγράφων προς τα αντίστοιχα σχήματα.

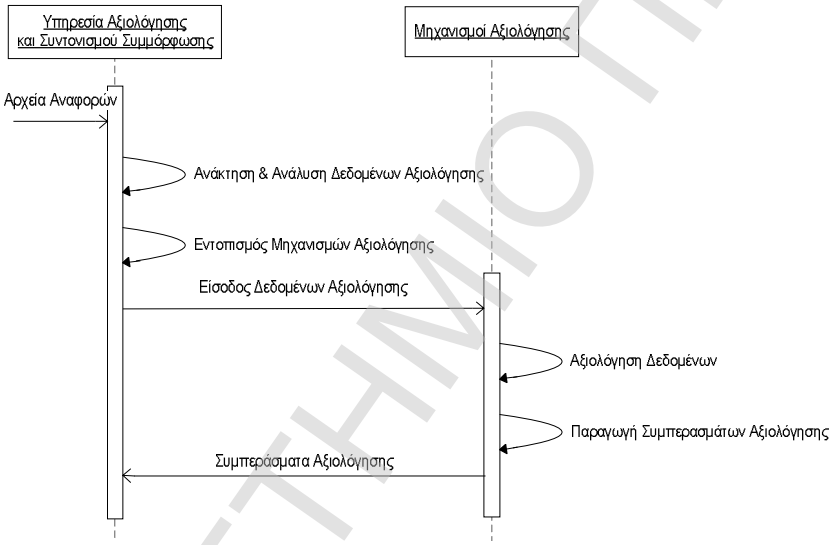
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3. *Παραγωγή* συμπερασμάτων ελέγχου συμμόρφωσης από τους μηχανισμούς αξιολόγησης. Τα συμπεράσματα αυτά περιέχουν τα αποτελέσματα της ανάλυσης όπως αυτά προέκυψαν από την εκτέλεση του 1^{ου} βήματος.
4. *Καταγραφή* των παραγόμενων αποτελεσμάτων.

Στις Παραγράφους που ακολουθούν παρατίθενται οι ακριβείς διαδικασίες οι οποίες πραγματοποιούνται. Στο πέρας του βήματος (4), έχει ολοκληρωθεί η ανάλυση των δεδομένων και έχουν παραχθεί τα αποτελέσματα της αξιολόγησης. Επομένως στην παρούσα φάση το ΣυΕ πρέπει να ενημερωθεί για τα συγκεκριμένα αποτελέσματα.

2.3.5.1.4.3 Ανάκτηση Δεδομένων Αξιολόγησης από Στρώμα Συμμόρφωσης

Στο Σχήμα 23 απεικονίζεται το διάγραμμα ακολουθίας που παρουσιάζει την διαδικασία η οποία λαμβάνει χώρα για την ανάκτηση των δεδομένων αξιολόγησης από την ΥΔΕ. Το *Στρώμα Συμμόρφωσης* αποτελεί το συστατικό της ΥΔΕ που αναλαμβάνει τη διαδικασία αυτή.



Σχήμα 23: Διαδικασία Ανάκτησης Δεδομένων Αξιολόγησης από Στρώμα Συμμόρφωσης

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Συμμόρφωσης* αναλαμβάνει να επεξεργαστεί τα αρχεία αναφοράς τα οποία παράγονται από τα ΣυΕ και εξάγει τα δεδομένα που περιέχονται σε αυτά. Ακολούθως, προχωράει σε ανάλυση των δεδομένων ώστε να διαπιστώσει τους μηχανισμούς αξιολόγησης (βλ. § 2.3.4.2.2) τους οποίους πρέπει να χρησιμοποιήσει για τα συγκεκριμένα δεδομένα.
Με την ολοκλήρωση των διαπιστώσεων αυτών τα δεδομένα τροφοδοτούνται στους αντίστοιχους μηχανισμούς αξιολόγησης.

2.3.5.1.4.4 Διαδικασία Ανάλυσης Δεδομένων Αξιολόγησης

Η διαδικασία ανάλυσης των αποτελεσμάτων παρουσιάζεται στο διάγραμμα ακολουθίας του Σχήμα 23.
Οι υιοθετημένοι μηχανισμοί αξιολόγησης αναλύουν και ελέγχουν την συμμόρφωση των δεδομένων προς τις αντίστοιχες προδιαγραφές. Στη συνέχεια παράγουν τα συμπεράσματα τα οποία μεταβιβάζονται στην *Υπηρεσία Αξιολόγησης και Συντονισμού Συμμόρφωσης* η οποία αναλαμβάνει την καταγραφή των συγκεκριμένων αποτελεσμάτων.

2.3.5.1.5 5^{ο} στάδιο: Διόρθωση ΥΙυΕ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.3.5.1.5.1 Στόχοι

Στον παρόν στάδιο τα αποτελέσματα της ανάλυσης των ελέγχων συμμόρφωσης που παράγονται στο 4ο στάδιο της μεθοδολογίας τίθενται υπόψη των αρμοδίων της ΥΙυΕ οι οποίοι φέρουν την ευθύνη του σχεδιασμού και της υλοποίησης της πραγματικής ΥΙ η οποία και ελέγχεται.. Ο στόχος είναι να γίνουν οι απαραίτητες διορθωτικές ενέργειες που θα οδηγήσουν σε συμμόρφωση της ΥΙ ως προς τις αντίστοιχες προδιαγραφές.

2.3.5.1.5.2 Μεθοδολογία Σταδίου για τη Διόρθωση της ΥΙυΕ

Τα συγκεκριμένα βήματα που ακολουθούνται στο παρόν 5ο στάδιο είναι τα ακόλουθα:

1. *Ενημέρωση* των αρμοδίων της ΥΙυΕ για τα αποτελέσματα της ανάλυσης των ελέγχων συμμόρφωσης.
2. *Αξιολόγηση* των αποτελεσμάτων από τους αρμόδιους. Με την διαδικασία αυτή πραγματοποιείται ο εντοπισμός των προδιαγραφών και κατ' επέκταση των σημείων της υλοποίησης (δομικά στοιχεία (βλ. § 2.3.4.1.1)) στα οποία έχει εντοπιστεί από την ανάλυση ότι δεν παρατηρείται συμμόρφωση.
3. *Ενημέρωση των προδιαγραφών και διόρθωση της υλοποίησης* με στόχο τη συμμόρφωση της ΥΙυΕ με τις υιοθετημένες προδιαγραφές. Πρέπει να επισημανθεί ότι το βήμα αυτό εκτελείται μόνο στην περίπτωση κατά την οποία έχουν εντοπιστεί σημεία της υλοποίησης στα οποία δεν παρατηρείται συμμόρφωση.

Το βήμα 3 αποτελεί το βασικό βήμα του συγκεκριμένου σταδίου καθώς περιλαμβάνει τη διαδικασία διόρθωσης της υλοποίησης των στοιχείων της ΥΙυΕ όπου αυτό θεωρείται επιβεβλημένο. Μόνο η ορθή ολοκλήρωσή του μπορεί να οδηγήσει σε επιτυχή επίτευξη του ελέγχου συμμόρφωσης.
Η παρούσα μεθοδολογία, δεν προδιαγράφει συγκεκριμένη μέθοδο τεχνολογίας λογισμικού ή εργαλεία υλοποίησης τα οποία θα χρησιμοποιηθούν για τη διόρθωση της υλοποίησης και τον προγραμματισμό. Η επιλογή για κάποια μέθοδο ή μεθόδους αφήνεται στον σχεδιαστή της ΥΙυΕ.
Κατά την διάρκεια της διόρθωσης της υλοποίησης, ενδέχεται ορισμένες αποφάσεις που είχαν ληφθεί στον σχεδιασμό να οδηγούν σε αδιέξοδο, να εντοπίζονται πιο συμφέρουσες λύσεις ή να χρησιμοποιηθούν νέες βιβλιοθήκες που δεν ήταν ξεκάθαρες ή ορατές στην αρχή (κάτι το οποίο είναι ο κανόνας και όχι η εξαίρεση στον σχεδιασμό και την υλοποίηση σύνθετων συστημάτων). Οι αλλαγές των προδιαγραφών που χρειάζονται, συλλέγονται και τεκμηριώνονται.
Στο πέρας του βήματος (3), η ΥΙυΕ έχει διορθωθεί και μπορεί να επαναληφθεί η διαδικασία ελέγχου συμμόρφωσης με την εκτέλεση των απαιτούμενων ελέγχων για τις προδιαγραφές για τις οποίες δεν παρατηρήθηκε συμμόφωση.

2.3.5.1.6 6ο στάδιο: Επανεκτέλεση Απαιτούμενων Ελέγχων

2.3.5.1.6.1 Στόχοι

Στόχος του παρόντος σταδίου είναι η επανεκτέλεση ενός συνόλου περιπτώσεων ελέγχου οι οποίες θα ελέγξουν την συμμόρφωση της ΥΙυΕ. Από τη στιγμή λοιπόν που έχουν οριστεί οι ανεπιτυχείς περιπτώσεις ελέγχου και οι απαιτούμενες διορθωτικές ενέργειες έχουν ολοκληρωθεί ένας καινούργιος κύκλος ελέγχου συμμόρφωσης ξεκινάει. Όπως είναι ευκρινές το στάδιο αυτό είναι προαιρετικό και εκτελείται μόνο στην περίπτωση κατά την οποία έχουν εντοπιστεί ανωμαλίες ως προς την συμμόρφωση της ΥΙυΕ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.3.5.1.6.2 Μεθοδολογία Σταδίου για την Επανεκτέλεση των Απαιτούμενων Ελέγχων

Το 6ο στάδιο περιλαμβάνει τα εξής βήματα:

1. *Εντοπισμός* των περιπτώσεων ελέγχου που πρέπει να επανεκτελεστούν. Οι περιπτώσεις αυτές δεν περιορίζονται μόνο στις περιπτώσεις ελέγχου οι οποίες κρίθηκαν ως ανεπιτυχείς στο 4ο βήμα της μεθοδολογίας αλλά περιλαμβάνουν και αυτές των οποίων τα αποτελέσματα ενδέχεται να επηρεαστούν από τις διορθωτικές ενέργειες οι οποίες εφαρμόστηκαν στην υλοποίηση (τα δομικά στοιχεία) της ΥΙυΕ που πραγματοποιήθηκε στο 5ο βήμα.
2. *Επανεκτέλεση* της μεθοδολογίας ξεκινώντας από το 6ο βήμα του 1ου σταδίου στο πλαίσιο του οποίου γίνεται καθορισμός της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου.

Με την εκτέλεση του 2ου βήματος ο έλεγχος συμμόρφωσης εισέρχεται σε μια επαναλαμβανόμενη διαδικασία η οποία ολοκληρώνεται με την επιτυχή εκτέλεση όλων των περιπτώσεων ελέγχου. Η διαπίστωση ως προς τη συμμόρφωση της ΥΙυΕ λαμβάνεται κατά το 4ο στάδιο όπου γίνεται και η αξιολόγηση των αποτελεσμάτων ελέγχου και η παραγωγή των αποτελεσμάτων της ανάλυσης.

2.3.6 Φάση 4: Έλεγχος Διαλειτουργικότητας

2.3.6.1 Επισκόπηση των Σταδίων Ελέγχου Διαλειτουργικότητας

Ο Έλεγχος Διαλειτουργικότητας αποτελεί μια πιο πολύπλοκη διαδικασία σε σχέση με τον Έλεγχο Συμμόρφωσης (βλ. § 2.3.5) καθώς εμπλέκονται σε αυτόν περισσότερα του ενός ΣυΕ. Η αρχικοποίηση του ελέγχου αυτού έπεται συνήθως της επιτυχούς ολοκλήρωσης του ελέγχου συμμόρφωσης των ΣυΕ, γεγονός το οποίο δεν είναι περιοριστικό καθώς οι συγκεκριμένοι τύποι ελέγχων μπορεί να πραγματοποιηθούν ανεξάρτητα ο ένας του άλλου.

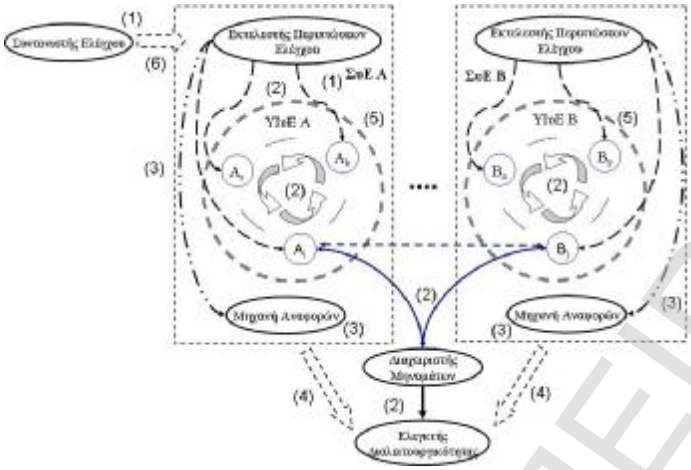
Κύριος στόχος του αποτελεί η εξέταση της δυνατότητας επικοινωνίας των εμπλεκομένων ΣυΕ. Στο Κεφάλαιο αυτό πραγματοποιείται η επισκόπηση των βασικών σταδίων τα οποία πρέπει να εκτελεστούν. Η προτεινόμενη μεθοδολογία αποτελείται από έξι βασικά στάδια, τα οποία παρουσιάζονται στο Σχήμα 24:

Σχήμα 24: Τα έξι στάδια Ελέγχου Διαλειτουργικότητας

Το Σχήμα 25 παραθέτει μια απεικόνιση των βασικών οντοτήτων που μετέχουν στον έλεγχο, τουλάχιστον δυο ΣυΕ (π.χ. "ΣυΕ Α" και "ΣυΕ Β") και η ΥΔΕ, όπως επίσης και μια οπτική αναπαράσταση των εκτελέσιμων προτεινόμενων σταδίων. Η

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

αναλυτική περιγραφή κάθε σταδίου περιλαμβάνεται στις παραγράφους που ακολουθούν.



Σχήμα 25: Οντότητες και Εκτελέσιμα Βήματα Ελέγχου Διαλειτουργικότητας

2.3.6.1.1 1ο στάδιο: Καθορισμός Περιπτώσεων Ελέγχου

2.3.6.1.1.1 Στόχοι

Το στάδιο αυτό βρίσκεται σε πλήρη αντιστοίχιση με το πρώτο στάδιο (βλ. § 2.3.5.1.1) του ελέγχου συμμόρφωσης. Ο στόχος του συνοψίζεται στην αποτύπωση, ολοκλήρωση και ενσωμάτωση των περιπτώσεων ελέγχου οι οποίες θα πρέπει να εκτελεστούν προκειμένου να διαπιστωθεί η δυνατότητα αλληλεπίδρασης των εξεταζόμενων ΣυΕ. Η ολοκλήρωση του σταδίου αυτού με ακρίβεια εξασφαλίζει σε σημαντικό βαθμό την εφαρμογή ενός ολοκληρωμένου ελέγχου εξετάζοντας ένα ευρύ φάσμα πτυχών και παραμέτρων.

2.3.6.1.1.2 Μεθοδολογία Σταδίου για τον Καθορισμό Περιπτώσεων Ελέγχου

Το παρόν στάδιο περιλαμβάνει τα ακόλουθα βήματα:

1. *Σχεδιασμός* των περιπτώσεων ελέγχου που πρέπει να εφαρμοστούν στην περίπτωση του ελέγχου διαλειτουργικότητας. Στο Κεφάλαιο 2.3.6.1.1.3 παρουσιάζεται ο ορισμός μιας περίπτωσης ελέγχου διαλειτουργικότητας καθώς και τα βήματα που πρέπει να εκτελεστούν για τη σχεδίασή τους.
2. *Διαμόρφωση και παραγωγή* των διαδικασιών των περιπτώσεων ελέγχου, όπως αυτές σχεδιάστηκαν στο προηγούμενο βήμα. Η παραγωγή των διαδικασιών αυτών γίνεται όμοια με τις αντίστοιχες του ελέγχου συμμόρφωσης χρησιμοποιώντας πρότυπα και πλαίσια που περιγράφηκαν στο Κεφάλαιο 2.3.5.1.1.4.
3. *Ενσωμάτωση* των παραγόμενων διαδικασιών των περιπτώσεων ελέγχου στους Εκτελεστές Περιπτώσεων Ελέγχου των ΣυΕ με παράλληλη υλοποίηση των απαιτούμενων διεπαφών.
4. *Παραγωγή* των δεδομένων ελέγχου που απαιτούνται από τις περιπτώσεις ελέγχου (Προαιρετικό βήμα).
5. *Αποθήκευση* των παραγόμενων δεδομένων ελέγχου στο Αποθετήριο Δεδομένων Ελέγχου της ΥΔΕ (Προαιρετικό βήμα).
6. *Καθορισμός* της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου. Η αλληλουχία των ελέγχων θα πρέπει να πραγματοποιείται με λογικό τρόπο ώστε να εξασφαλίζεται η αποτελεσματικότητα τους. Πρωταρχικό κριτήριο για την επιλογή της σειράς είναι η πολυπλοκότητα των περιπτώσεων ελέγχου (έλεγχος αρχικά των βασικών λειτουργιών και συνέχιση με τις πιο πολύπλοκες).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

7. *Αποτύπωση* της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου σε ένα προσχέδιο. Το προσχέδιο περιέχει τα URL των διαδικασιών BPEL που πρέπει να κληθούν από την ΥΔΕ όπως και τα δεδομένα ελέγχου που πιθανόν να απαιτούνται. Η αποθήκευση του προσχεδίου γίνεται στο Αποθετήριο Δεδομένων Ελέγχου της ΥΔΕ.

Στο πέρας του βήματος (7), το σύνολο των εξεταζόμενων περιπτώσεων ελέγχου όπως και η σειρά εξέτασης τους καταγράφονται και αποθηκεύονται.

2.3.6.1.1.3 Περιπτώσεις Ελέγχου Διαλειτουργικότητας

Η φύση και η δομή των περιπτώσεων ελέγχου διαλειτουργικότητας οι οποίες σχεδιάζονται και χρησιμοποιούνται σε αυτήν τη φάση της μεθοδολογίας είναι όμοιες με τις αντίστοιχες περιπτώσεις ελέγχου συμμόρφωσης που παρουσιάστηκαν στο Κεφάλαιο 2.3.5.1.1.3. Μια σημαντική διαφορά αποτελεί το γεγονός ότι οι περιπτώσεις ελέγχου διαλειτουργικότητας περιλαμβάνουν και *εξωτερικές ενέργειες* πέρα από *εσωτερικές*. Αυτό σημαίνει ότι για την εκτέλεση των περιπτώσεων ελέγχου δεν απαιτείται ο συγχρονισμός μόνο των πρωτευουσών υπηρεσιών μιας ΥΙυΕ αλλά και η αλληλεπίδραση πρωτευουσών υπηρεσιών διαφορετικών ΥΙυΕ. Το γεγονός αυτό έχει ως άμεση συνέπεια την αύξηση της πολυπλοκότητας των διαδικασιών BPEL οι οποίες πρέπει να σχεδιαστούν για να αναπαραστήσουν την λογική μιας περιπτώσεως ελέγχου.

Δυο βασικοί παράμετροι οι οποίες πρέπει να ληφθούν υπόψη για το σχεδιασμό μιας περιπτώσης ελέγχου είναι ο ρόλος που διαδραματίζουν τα εμπλεκόμενα ΣυΕ μέσω του σενάριου ελέγχου το οποίο καθορίστηκε στην $1^{η}$ φάση της μεθοδολογίας και τα πρότυπα τα οποία οι ΥΙυΕ έχουν υιοθετήσει. Στην πραγματικότητα οι προσδιοριζόμενες περιπτώσεις ελέγχου θα πρέπει να αποτελούν υποπεριπτώσεις του εξεταζόμενου σεναρίου καλύπτοντας το σύνολο των διαφορετικών εκδοχών του και λαμβάνοντας υπόψη τα υιοθετημένα πρότυπα.

Επίσης, το στοιχείο που πρέπει να τονιστεί είναι ότι οι περιπτώσεις ελέγχου σχεδιάζονται μόνο για τα ΣυΕ που αρχικοποιούν μια διαδικασία ελέγχου. Ας λάβουμε για παράδειγμα το σενάριο που απεικονίζεται στο Σχήμα 25 όπου το "ΣυΕ Α" αλληλεπιδρά με το "ΣυΕ Β" λαμβάνοντας μια απόκριση. Με βάση το σενάριο αυτό, η "ΥΙυΕ Α" συντονίζει κατάλληλα τις υπηρεσίες της (π.χ. A_s και A_k) προκειμένου να εκτελεστεί μια συγκεκριμένη διαδικασία η οποία επιτρέπει σε μια υπηρεσία Ai να επικοινωνήσει με την υπηρεσία Bj της "ΥΙυΕ Β" περιμένοντας μια απάντηση την οποία θα διαχειριστεί κατάλληλα. Η "ΥΙυΕ Β" αντιδρά σε αυτήν την αλληλεπίδραση δημιουργώντας μια απάντηση σύμφωνα με τη λογική η οποία περιλαμβάνεται στην εφαρμογή της. Στο παραπάνω παράδειγμα η περίπτωση ελέγχου διαλειτουργικότητας περιγράφει τις ενέργειες οι οποίες πρέπει να εκτελεστούν μόνο από το "ΣυΕ Α".

Πιο συγκεκριμένα, τα ακριβή υποβήματα που πρέπει να ακολουθηθούν για τον σχεδιασμό μιας περίπτωσης ελέγχου διαλειτουργικότητας είναι τα εξής:

1. *Προσδιορισμός* μιας εκδοχής η οποία αποτελεί τμήμα του σεναρίου που καθορίστηκε στην $1^{η}$ φάση της μεθοδολογίας. Για την εκδοχή αυτή προσδιορίζεται το ΣυΕ που αρχικοποιεί τη συγκεκριμένη διαδικασία.
2. *Ανάλυση* της επιχειρησιακής λογικής της διαδικασίας η οποία εμπεριέχεται στο ΣυΕ που λειτουργεί ως αρχικοποιητής και με βάση την οποία μετέχει στη διαδικασία ελέγχου.
3. *Καταγραφή* όλων των υποσυνόλων των διαδικασιών που καλύπτουν τη συνολική επιχειρησιακή λογική της υπηρεσίας βάσηει των επιχειρησιακών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

απαιτήσεων που προκύπτουν από την εκδοχή του σεναρίου που προσδιορίστηκε στο υποβήμα 1.

4. *Καθορισμός* της περίπτωσης ελέγχου για το ΣυΕ που αρχικοποιεί τη διαδικασία ελέγχου με βάση τον ορισμό που δόθηκε στο Κεφάλαιο 2.3.5.1.1.3 δηλαδή:

   Περίπτωση ελέγχου = {Ενέργεια$_j$, Υπηρεσία$_j$, Είσοδος$_j$, Έξοδος$_j$}

5. *Απεικόνιση* της περίπτωσης ελέγχου με χρήση ενός διαγράμματος ενεργειών.

Τα βήματα αυτά επιτρέπουν το σαφή προσδιορισμό ενός συνόλου εξεταζόμενων περιπτώσεων ελέγχου διαλειτουργικότητας.

2.3.6.1.2 2^ο στάδιο: Εκτέλεση Περιπτώσεων Ελέγχου

2.3.6.1.2.1 Στόχοι

Βασικός στόχος του παρόντος σταδίου αποτελεί η εκτέλεση των περιπτώσεων ελέγχων οι οποίες ορίστηκαν στο 1^ο στάδιο της μεθοδολογίας. Οι εμπλεκόμενες οντότητες στον έλεγχο διαλειτουργικότητας είναι όλα τα ΣυΕ και η ΥΔΕ.

2.3.6.1.2.2 Μεθοδολογία Σταδίου για την Εκτέλεση Περιπτώσεων Ελέγχου

Τα επιμέρους βήματα του σταδίου είναι τα ακόλουθα:

1. Η *ΥΔΕ* δίνει το έναυσμα για την εκτέλεση των περιπτώσεων ελέγχων με την κλήση των αντίστοιχων διεπαφών ακολουθώντας το προσχέδιο που καθορίστηκε στο 1^ο στάδιο της συγκεκριμένης φάσης. Στο Κεφάλαιο 2.3.5.1.2.3 αναλύεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.
2. Τα *ΣυΕ* εκτελούν τις περιπτώσεις ελέγχου συντονίζοντας τα απαραίτητα συστατικά των ΥΙυΕ. Στο Κεφάλαιο 2.3.6.1.2.4 παρατίθεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.

Στο πέρας του βήματος (2), έχουν παραχθεί τα δεδομένα προς αξιολόγηση τα οποία απαιτούνται για να ελεχθεί η διαλειτουργικότητα των εμπλεκόμενων ΥΙυΕ.

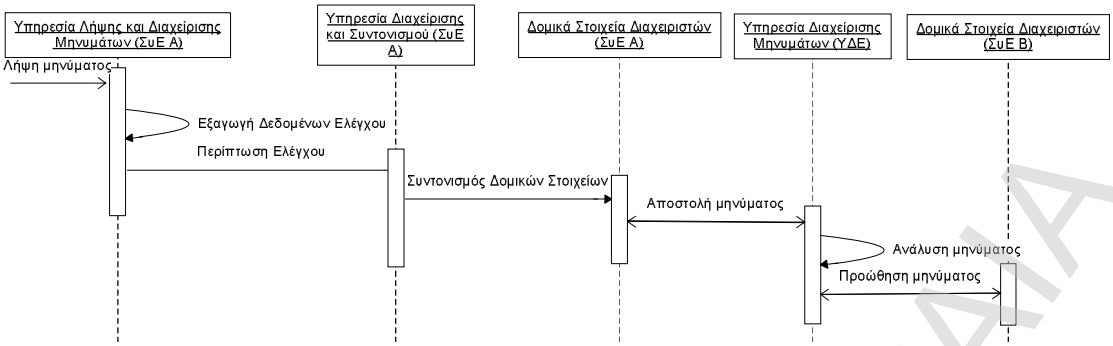
2.3.6.1.2.3 ΥΔΕ: Αρχικοποίηση και Συντονισμός των Περιπτώσεων Ελέγχου Διαλειτουργικότητας

Η διαδικασία η οποία λαμβάνει χώρα είναι ταυτόσημη με αυτή που εκτελείται και στην περίπτωση του ελέγχου συμμόρφωσης (βλ. § 2.3.5.1.2.3) και παρατίθεται στο διάγραμμα ακολουθίας του Σχήμα 20. Η ΥΔΕ καλεί την αντίστοιχη διεπαφή του ΣυΕ (π.χ. "ΣυΕ Α" (Σχήμα 25)) που αρχικοποιεί την διαδικασία ελέγχου η οποία έχει οριστεί στο προσχέδιο που έχει διαμορφωθεί στο 1^ο βήμα της συγκεκριμένης φάσης.

2.3.6.1.2.4 ΣυΕ: Εκτέλεση Περιπτώσεως Ελέγχου Διαλειτουργικότητας

Το ΣυΕ (π.χ. "ΣυΕ Α") που αρχικοποιεί τη διαδικασία ελέγχου λαμβάνει το μήνυμα που στέλνεται από τη ΥΔΕ και ξεκινάει τη διαδικασία εκτέλεσης της περιπτώσεως ελέγχου. Η διαδικασία αυτή βρίσκεται σε πλήρη αντιστοιχία με αυτή που περιγράφηκε στο Κεφάλαιο 2.3.5.1.2.4.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 26: Εκτέλεση Περιπτώσεως Ελέγχου Διαλειτουργικότητας

Πιο συγκεκριμένα, όπως απεικονίζεται στο Σχήμα 26, η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* του "ΣυΕ Α" λαμβάνει το μήνυμα και το αποδομεί εξάγοντας τα περικλειόμενα δεδομένα ελέγχου. Ακολούθως, ενημερώνει την *Υπηρεσία Διαχείρισης και Συντονισμού* σχετικά με την διαδικασία BPEL η οποία πρέπει να εκτελεστεί, η οποία με τη σειρά της προβαίνει στο συντονισμό των πρωτευουσών υπηρεσιών από τις οποίες απαρτίζεται η ΥΙυΕ για την ολοκλήρωση της περιπτώσης ελέγχου.

Στην προκειμένη περίπτωση η ΥΙυΕ του ΣυΕ (ΣυΕ Α) που αρχικοποιεί τη διαδικασία ελέγχου απαιτείται να επικοινωνήσει και με την ΥΙυΕ ενός άλλου ΣυΕ (ΣυΕ Β) των οποίων εξετάζεται η διαλειτουργικότητα. Η επικοινωνία αυτή πραγματοποιείται μέσω της δημιουργίας και αποστολής μηνυμάτων. Τα ανταλλασσόμενα αυτά μηνύματα "υποκλέπτονται" αρχικά από την *Υπηρεσία Διαχείρισης Μηνυμάτων* (βλ. § 2.3.4.2.3) της ΥΔΕ η οποία αναθέτει στην *Υπηρεσία Ανάλυσης Μηνυμάτων* να τα αναλύσει με στόχο τη συσχέτιση τους με τις περιγραφές των ΥΙ όπως αυτές έχουν παραχθεί από τα ΣυΕ που λειτουργούν ως παραλήπτες των μηνυμάτων. Τα αποτελέσματα της ανάλυσης καταγράφονται τελικώς σε μια αναφορά. Στη συνέχεια, η *Υπηρεσία Διαχείρισης Μηνυμάτων* αναλαμβάνει την προώθηση των μηνυμάτων στα ΣυΕ (ΣυΕ Β) που λειτουργούν ως τελικοί παραλήπτες και τα οποία εκτελούν τις ενέργειες που αντιστοιχούν στη λογική η οποία περιλαμβάνεται στην εφαρμογή τους.

2.3.6.1.3 3ο στάδιο: Συλλογή των Δεδομένων Αξιολόγησης

2.3.6.1.3.1 Στόχοι

Το παρόν στάδιο εστιάζεται στη συλλογή των αποτελεσμάτων τα οποία παράγονται από την εκτέλεση της περιπτώσεως ελέγχου από τα ΣυΕ.

2.3.6.1.3.2 Μεθοδολογία Σταδίου για τη Συλλογή των Δεδομένων Αξιολόγησης

Τα βήματα από τα οποία αποτελείται το παρόν 3ο στάδιο είναι τα ακόλουθα:

1. Οι *Μηχανές Αναφορών* (βλ. § 2.3.4.1.3) των ΣυΕ που εμπλέκονται στον έλεγχο διαλειτουργικότητας είτε αρχικοποιώντας την εκτέλεση των διαδικασιών ελέγχου είτε απλά μετέχοντας σε αυτές εποπτεύουν την εκτέλεση των περιπτώσεων ελέγχου και συλλέγουν τα δεδομένα που παράγονται από το συντονισμό των υπηρεσιών των ΥΙυΕ.
2. Οι *Μηχανές Αναφορών* συνθέτουν τα συλλεγόμενα δεδομένα στην απαιτούμενη μορφή και τα ενσωματώνουν σε αρχεία αναφορών (log files).

Στο πέρας του βήματος (2), τα δεδομένα προ αξιολόγηση είναι έτοιμα να ανακτηθούν από την ΥΔΕ ώστε να ελεγχθεί η δυνατότητα διαλειτουργικότητας των ΣυΕ. Στο Κεφάλαιο 2.3.6.1.3.3 αναλύεται η ακριβής διαδικασία η οποία λαμβάνει χώρα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

2.3.6.1.3.3 ΣυΕ: Λήψη Δεδομένων Αξιολόγησης από Μηχανή Αναφορών

Η διαδικασία η οποία ολοκληρώνεται για τη λήψη των δεδομένων αξιολόγησης από τις Μηχανές Αναφορών των ΣυΕ που μετέχουν στην εκτέλεση των περιπτώσεων ελέγχων είναι ίδια με αυτή που περιγράφεται στο Κεφάλαιο 2.3.5.1.3.3.

2.3.6.1.4 4ο στάδιο: Ανάλυση Δεδομένων Αξιολόγησης

2.3.6.1.4.1 Στόχοι

Στο στάδιο αυτό λαμβάνει χώρα η ανάκτηση των αποτελεσμάτων προς αξιολόγησης από την ΥΔΕ και ο ουσιαστικός έλεγχος της δυνατότητας επικοινωνίας των ΣυΕ.

2.3.6.1.4.2 Μεθοδολογία Σταδίου για την Ανάλυση των Δεδομένων Αξιολόγησης

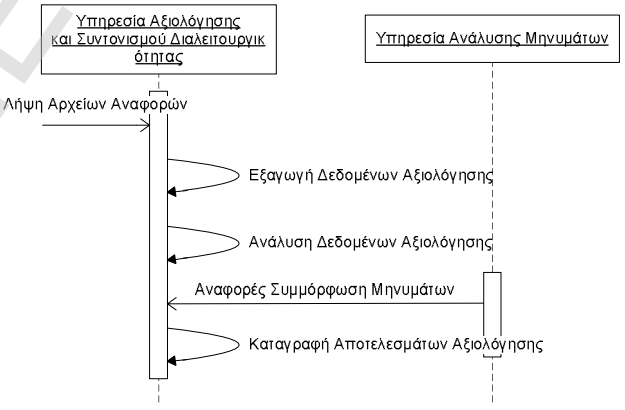
Το παρόν στάδιο περιλαμβάνει τα ακόλουθα βήματα:

1. *Ανάκτηση* των δεδομένων προς αξιολόγηση.
2. *Ανάλυση* των δεδομένων αξιολόγησης και έλεγχος δυνατότητας αλληλεπίδρασης των ΣυΕ. Στο Κεφάλαιο 2.3.4.2 παρουσιάστηκε η διαδικασία ανάλυσης των αποτελεσμάτων και η έλεγχοι οι οποίοι πραγματοποιούνται.
3. *Παραγωγή* συμπερασμάτων ελέγχου διαλειτουργικότητας Τα συμπεράσματα αυτά περιέχουν τα αποτελέσματα της ανάλυσης όπως αυτά προέκυψαν από την εκτέλεση του 2ου βήματος.
4. *Καταγραφή* των παραγόμενων αποτελεσμάτων.

Στο Κεφάλαιο που ακολουθεί παρατίθεται η ακριβλης διαδικασία η οποία λαμβάνει χώρα στο παρόν στάδιο. Στο πέρας του βήματος (4), έχει διαπιστωθεί αν δύναται να αλληλεπιδράσουν επιτυχώς οι ΥΙυΕ ενώ σε περίπτωση αδυναμίας γίνεται ακριβής εντοπισμός των δυσλειτουργιών και πραγματοποιείται απόδοση ευθύνης στις αντίστοιχες ΥΙυΕ.
Επομένως στην παρούσα φάση τα ΣυΕ πρέπει να ενημερωθούν για τα συγκεκριμένα αποτελέσματα.

2.3.6.1.4.3 ΥΔΕ: Λήψη και Ανάλυση Δεδομένων Αξιολόγησης από το Στρώμα Διαλειτουργικότητας

Το στρώμα Διαλειτουργικότητας της ΥΔΕ είναι το αρμόδιο συστατικό της ΥΔΕ το οποίο αναλαμβάνει την ανάκτηση των δεδομένων αξιολόγησης που παράγονται από τα ΣυΕ. Στο Σχήμα 27 απεικονίζεται το διάγραμμα ακολουθίας που παρουσιάζει την διαδικασία η οποία λαμβάνει χώρα στη ΥΔΕ.



Σχήμα 27: Διαδικασία Λήψης και Ανάλυσης Δεδομένων Αξιολόγησης από το Στρώμα Διαλειτουργικότητας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας* αναλαμβάνει να επεξεργαστεί τα αρχεία αναφοράς τα οποία παράγονται από τα ΣυΕ και εξάγει τα δεδομένα που περιέχονται σε αυτά. Ακολούθως, η υπηρεσία αυτή προχωράει σε ανάλυση των δεδομένων εκτελώντας τις ακόλουθες διαδικασίες:

- ü συγκρίνει τα έγγραφα τα οποία διαθέτουν στην κατοχή τους τα ΣυΕ ώστε να διαπιστώσει ότι είναι ταυτόσημα. Επιπλέον, ελέγχει ότι οι μηχανισμοί ασφάλειας που έχουν εφαρμοστεί (π.χ. δημιουργία και πιστοποίηση ψηφιακών υπογραφών) σε επίπεδο εγγράφων έχουν ολοκληρωθεί με επιτυχία.
- ü συγκρίνει τα μηνύματα τα οποία ανταλλάχθηκαν κα τελικώς παραλήφθηκαν από τα ΣυΕ ώστε να διαπιστώσει ότι είναι ταυτόσημα, ενώ ελέγχει και την επιτυχή εφαρμογή και πιστοποίηση των εφαρμοζόμενων σε αυτά μηχανισμών ασφάλειας. Επίσης επικοινωνεί με την *Υπηρεσία Ανάλυσης Μηνυμάτων* του Διαχειριστή Μηνυμάτων (βλ. § 2.3.4.2.3) ώστε να λάβει τις αναφορές που σχετίζονται με τη συμμόρφωση των μηνυμάτων ως προς την περιγραφή των αντίστοιχων ΥΙ.
- ü αξιολογεί ότι η μετατροπή των εγγράφων από ένα σχήμα σε ένα άλλο έχει πραγματοποιηθεί χωρίς την εμφάνιση οποιουδήποτε προβλήματος.

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας* με βάση τις ανωτέρω διαδικασίες ανάλυσης παράγει τα συμπεράσματα ελέγχου διαλειτουργικότητας τα οποία και καταγράφει. Λαμβάνοντας υπόψη τα καταγεγραμμένα αποτελέσματα είναι δυνατός ο προσδιορισμός της δυνατότητας επικοινωνίας των ΣυΕ επισημαίνοντας μη έγκυρες συμπεριφορές και αποδίδοντας ευθύνες στο ΣυΕ που κρίνεται ότι είναι υπαίτιο σε περίπτωση αποτυχίας της επικοινωνίας.

2.3.6.1.5 5ο στάδιο: Ενημέρωση και Διορθωτικές Ενέργειες

2.3.6.1.5.1 Στόχοι

Το παρόν στάδιο βρίσκεται σε πλήρη εναρμόνιση με το 5ο στάδιο του ελέγχου συμμόρφωσης (βλ. § 2.3.5.1.5). Στη συγκεκριμένη φάση τα αποτελέσματα τα οποία έχουν παραχθεί από την ανάλυση του ελέγχου διαλειτουργικότητας στο προηγούμενο στάδιο (4ο στάδιο) της μεθοδολογίας γνωστοποιούνται στους αρμόδιους των ΥΙυΕ με στόχο την εκτέλεση των απαιτούμενων διορθωτικών ενεργειών που θα επιτρέψουν την επιτυχή αλληλεπίδρασή τους.

2.3.6.1.5.2 Μεθοδολογία Σταδίου για την Ενημέρωση και την Εφαρμογή Διορθωτικών Ενεργειών

Τα συγκεκριμένα βήματα που θα πρέπει να ακολουθηθούν είναι τα ακόλουθα:

1. *Ενημέρωση* των αρμοδίων των ΥΙυΕ για τα αποτελέσματα της ανάλυσης των ελέγχων διαλειτουργικότητας. Από την ανάλυση δημιουργείται μια σαφής εικόνα της ευθύνης που φέρει η κάθε ΥΙυΕ.
2. *Αξιολόγηση* των αποτελεσμάτων από τους αρμόδιους. Με την διαδικασία αυτή πραγματοποιείται η αποτίμηση της ευθύνης για κάθε ΥΙυΕ και προσδιορίζονται επακριβώς οι προδιαγραφές και τα σημεία της υλοποίησης (δομικά στοιχεία (βλ. § 2.3.4.1.1)) που παρουσιάζουν δυσλειτουργία.
3. *Ενημέρωση των προδιαγραφών και διόρθωση της υλοποίησης* ώστε να ξεπεραστούν οι δυσλειτουργίες που εντοπίστηκαν στο προηγούμενο βήμα. Πρέπει να σημειωθεί ότι το συγκεκριμένο βήμα είναι προαιρετικό και εκτελείται μόνο στην περίπτωση κατά την οποία έχει εντοπιστεί αδυναμία επικοινωνίας και αφορά

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

μόνο τις ΥΙυΕ στις οποίες έχει αποδοθεί ένας συγκεκριμένος βαθμός ευθύνης. (Προαιρετικό)

Όπως έχει ήδη διευκρινιστεί (βλ. § 2.3.5.1.5.2), στόχος της προτεινόμενης μεθοδολογίας δεν αποτελεί ο καθορισμός μιας συγκεκριμένης μεθόδου τεχνολογίας λογισμικού ή η πρόταση εργαλείων υλοποίησης τα οποία θα χρησιμοποιηθούν για τη διόρθωση της υλοποίησης και τον προγραμματισμό. Η επιλογή για κάποια μέθοδο ή μεθόδους αφήνεται αποκλειστικά στους σχεδιαστές των εμπλεκομένων ΥΙυΕ.
Στο παρόν στάδιο είναι πιθανόν αποφάσεις που είχαν ληφθεί στον σχεδιασμό να αναπροσδιοριστούν. Οι εκτελούμενες αλλαγές θα πρέπει να καταγράφονται και να τεκμηριώνονται.
Στο πέρας του βήματος (3), οι ΥΙυΕ έχουν πλέον διορθωθεί και οι απαιτούμενοι έλεγχοι πρέπει να επαναληφθούν.

2.3.6.1.6 6ο στάδιο: Επανεκτέλεση Απαιτούμενων Ελέγχων

2.3.6.1.6.1 Στόχοι

Το παρόν στάδιο θέτει ως στόχο την επανεκτέλεση του συνόλου των περιπτώσεων ελέγχου που απαιτούνται για τον έλεγχο της διαλειτουργικότητας των ΣυΕ. Ο καθορισμός των ανεπιτυχών ελέγχων και η ολοκλήρωση των απαραίτητων διορθωτικών ενεργειών έχει ως αποτέλεσμα την αρχικοποίηση ενός νέου κύκλου ελέγχου διαλειτουργικότητας. Το στάδιο αυτό όπως και το αντίστοιχο στάδιο του ελέγχου συμμόρφωσης (βλ. § 2.3.5.1.6) εκτελείται μόνο στην περίπτωση κατά την οποία έχουν εντοπιστεί ανωμαλίες και αδυναμία επικοινωνίας των ΥΙυΕ.

2.3.6.1.6.2 Μεθοδολογία Σταδίου για την Επανεκτέλεση των Απαιτούμενων Ελέγχων

Το 6ο στάδιο περιλαμβάνει τα εξής βήματα:

1. *Εντοπισμός* των περιπτώσεων ελέγχου που πρέπει να επανεκτελεστούν. Οι περιπτώσεις αυτές δεν περιορίζονται μόνο στις περιπτώσεις ελέγχου οι οποίες κρίθηκαν ως ανεπιτυχείς στο 4ο βήμα της μεθοδολογίας αλλά περιλαμβάνουν και αυτές των οποίων τα αποτελέσματα ενδέχεται να επηρεαστούν από τις διορθωτικές ενέργειες οι οποίες εφαρμόστηκαν στην υλοποίηση (τα δομικά στοιχεία) της ΥΙυΕ που πραγματοποιήθηκε στο 5ο βήμα.
2. *Επανεκτέλεση* της μεθοδολογίας ξεκινώντας από το 6ο βήμα του 1ου σταδίου στα πλαίσια του οποίου γίνεται καθορισμός της ακολουθίας εκτέλεσης των περιπτώσεων ελέγχου.

Η είσοδος στο 2ο βήμα του ελέγχου διαλειτουργικότητας υποδηλώνει την έναρξη μιας επαναλαμβανόμενης διαδικασίας η οποία ολοκληρώνεται με την επιτυχή εκτέλεση όλων των περιπτώσεων ελέγχου. Η διαπίστωση της επιτυχούς δυνατότητας επικοινωνίας των ΥΙυΕ λαμβάνεται κατά το 4ο στάδιο όπου γίνεται και η αξιολόγηση των αποτελεσμάτων ελέγχου και η παραγωγή των αποτελεσμάτων της ανάλυσης.

2.3.7 Πλεονεκτήματα ΔΣΥΙ

Τα κύρια πλεονεκτήματα της μεθοδολογίας συνοψίζονται στα ακόλουθα:

- Είναι γενικευμένη και μπορεί να χρησιμοποιηθεί για τον έλεγχο της διαλειτουργικότητας και της συμμόρφωσης ενός μεγάλου εύρους ΥΙ. Κατά την εφαρμογή της μεθοδολογίας στο Κεφάλαιο 3 εξετάζεται η συμμόρφωση και η διαλειτουργικότητα δυο υπαρχόντων και πλήρως λειτουργικών Υπηρεσιών Ιστού

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

για ηλεκτρονική τιμολόγηση. Η πρώτη είνα η αυτόνομη υπηρεσίας ηλεκτρονικής τιμολόγησης SELIS η οποία προσφέρεται στο χώρο του η-επιχειρείν και η δεύτερη είναι η υπηρεσία ηλεκτρονικής και κινητής τιμολόγησης SWEB που είναι ενσωματωμένη σε μια πλατφόρμα η-διακυβέρνησης.

- Είναι δομημένη και παρέχει συγκεκριμένα βήματα που πρέπει να ακολουθηθούν σε κάθε στάδιο. Η μεθοδολογία αποτελείται από καλώς ορισμένες φάσεις (βλ. § 2.3.2) κάθε μία από τις οποίες έχει διακριτά στάδια.
- Είναι επεκτάσιμη επιτρέποντας την υιοθέτηση νέων κριτηρίων χωρίς να επηρεάζεται ούτε να μεταβάλλεται σε κανέναν βαθμό η λογική συνέχεια, η πολυπλοκότητα και η ροή της μεθοδολογίας. Αντίθετα αποδεικνύει την πλήρη ανεξαρτησία της από τα κριτήρια αξιολόγησης ως προς τα οποία αξιολογείται μια ΥΙ. Αυτό επιτυγχάνεται με την υιοθέτηση νέων εργαλείων αξιολόγησης της συμμόρφωσης των ΥΙυΕ (βλ. § 2.3.4.2.2 και 3.3.1.2.2.2) από την ΥΔΕ.
- Είναι ευπροσάρμοστη επιτρέποντας την υιοθέτηση και χρησιμοποίηση καινούργιων εργαλείων και βιβλιοθηκών για την εκτέλεση των ελέγχων. Στο στρώμα συμμόρφωσης της ΥΔΕ (βλ. § 2.3.4.2.2 και 3.3.1.2.2.2) μπορεί να ενσωματωθούν ένα σύνολο εργαλείων τα οποία θα ελέγχουν τη συμμόρφωση μιας ΥΙυΕ ως προς τις αντίστοιχες προδιαγραφές.
- Είναι παραμετροποιήσιμη υπό την έννοια ότι μπορούν να εφαρμοστούν κατάλληλα υποσύνολά της για την εφαρμογή ελέγχων. Η μεθοδολογία αποτελείται από διακριτές φάσεις (βλ. § 2.3.2), όπως είναι η «Φάση 3: *Έλεγχος Συμμόρφωσης*» και η «Φάση 4: *Έλεγχος Διαλειτουργικότητας*» οι οποίες είναι ανεξάρτητες μεταξύ τους. Η εκτέλεση των συγκεκριμένων φάσεων εξαρτάται αποκλειστικά από τους στόχους που έχει τεθεί κατά την αρχικοποίηση του ελέγχου.
- Παρέχει τη δυνατότητα πλήρους ελέγχου πάνω στις εφαρμοζόμενες διαδικασίες εποπτεύοντας την εκτέλεση τους. Η Μηχανή Αναφορών (βλ. § 2.3.4.1.3) αποτελεί το συστατικό του ΣυΕ που φέρει την ευθύνη καταγραφής των δεδομένων που έχουν παραχθεί κατά τη εκτέλεση των ελέγχων συμμόρφωσης και διαλειτουργικότητας.
- Επιτρέπει την απόδοση της ευθύνης στο σύστημα το οποίο ευθύνεται για την αποτυχία της επικοινωνίας καταγράφοντας στο σύνολο τους τα δεδομένα ελέγχου. Η Μηχανή Αναφορών (βλ. § 2.3.4.1.3) καταγράφει τα δεδομένα που παράγονται από την εκτέλεση των ελέγχων συμμόρφωσης και διαλειτουργικότητας με βάση τα οποία αποδίδεται η ευθύνη σε περίπτωση αδυναμίας επικοινωνίας των ΣυΕ.
- Παρέχει υψηλό επίπεδο ανεξαρτησίας από τεχνολογίες με το οποίες είναι υλοποιημένες οι εξεταζόμενες ΥΙ. Αυτό επιτυγχάνεται από την ίδια τη φύση των ΥΙ οι οποίες και εξετάζονται.

2.4 Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Αντικείμενο μελέτης του πρώτου άξονα της διατριβής αποτέλεσαν τα ζητήματα που αφορούν τη διαλειτουργικότητα μεταξύ διαφορετικών πληροφοριακών και επικοινωνιακών συστημάτων/υπηρεσιών τα οποία έχουν υιοθετηθεί και προσφέρονται από ένα σύνολο οργανισμών. Στα πλαίσια του άξονα αυτού επισημάνθηκε η ανάγκη ύπαρξης διαλειτουργικότητας καθώς και τα οφέλη τα οποία δύναται να αποκομιστούν από την επίτευξη της σε παγκόσμια κλίμακα, ενώ στην συνέχεια παρουσιάστηκαν οι βασικές διαστάσεις οι οποίες πρέπει να ληφθούν υπόψη για την ικανοποίηση της. Ιδιαίτερη έμφαση δόθηκε επίσης και στη μελέτη

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

πρωτοβουλιών και πλαισίων διαλειτουργικότητας τα οποία θέτουν ως βασικό στόχο την προτυποποίηση μέσω της πρότασης και δημιουργίας νέων προδιαγραφών και τον καθορισμό σαφών κανόνων και οδηγιών οι οποίες πρέπει να ακολουθηθούν για την ενίσχυση της διαλειτουργικότητας μεταξύ των συστημάτων/υπηρεσιών.

Ο παρών άξονας της διατριβής επικεντρώθηκε στον έλεγχο της διαλειτουργικότητας ηλεκτρονικών Υπηρεσιών Ιστού οι οποίες βασίζονται σε τεχνολογίες της XML και οι οποίες προσφέρονται είτε με τη μορφή αυτόνομων Υπηρεσιών Ιστού είτε ενσωματωμένες σε μια ολοκληρωμένη αρχιτεκτονική προσανατολισμένη στις υπηρεσίες. Η διαπίστωση η οποία προέκυψε από τη μελέτη των υπηρεσιών αυτών είναι ότι παρά το γεγονός ότι έχουν υιοθετηθεί και χρησιμοποιούνται κοινές XML προδιαγραφές οι δυνατότητες αλληλεπίδρασης των υπαρχόντων ΥΙ παραμένουν εξαιρετικά περιορισμένες. Το γεγονός αυτό οφείλεται σημαντικά στον τρόπο με τον οποίο οι υπεύθυνοι για την ανάπτυξη των υπηρεσιών αντιλαμβάνονται, υλοποιούν και ενσωματώνουν τα υιοθετημένα πρότυπα στις υπηρεσίες τους χωρίς πολλές φορές να δίνουν την δυνατότητα να καλύπτονται στο έπακρο το σύνολο των πτυχών που προσδιορίζονται από αυτά.

Έκδηλη, λοιπόν είναι η ανάγκη ύπαρξης και χρήσης μεθοδολογιών και πλαισίων διαλειτουργικότητας τα οποία ελέγχουν και εγγυώνται τη δυνατότητα επικοινωνίας των Υπηρεσιών Ιστού. Στα πλαίσια της διαπίστωσης αυτής εξετάστηκαν οι υπάρχουσες μεθοδολογίες και τα ευρέως διαδεδομένα πλαίσια καθώς επίσης και οι τύποι ελέγχου (ελέγχοι συμμόρφωσης και διαλειτουργικότητας) οι οποίοι έχουν υιοθετηθεί και εφαρμόζονται από αυτά, ενώ παράλληλα επισημάνθηκαν και προσδιορίστηκαν οι βασικές τους αδυναμίες. Σε γενικές γραμμές συναντήθηκαν προσεγγίσεις οι οποίες είτε είναι πολύ γενικές χωρίς να διατυπώνουν συγκεκριμένα και διακριτά βήματα που πρέπει να ακολουθηθούν και χωρίς να προσδιορίζουν με σαφήνεια τις διαδικασίες που πρέπει να εκτελεστούν για τον καθορισμό περιπτώσεων ελέγχου, είτε έχουν περιορισμένο πεδίο εφαρμογής όσον αφορά τις πτυχές των Υπηρεσιών Ιστού που πρέπει να ελέγχουν, ενώ σε ορισμένες περιπτώσεις αδυνατούν να κάνουν απόδοση ευθύνης στην Υπηρεσία Ιστού η οποία φέρει την ευθύνη για την αποτυχία επικοινωνίας.

Βάσει των παραπάνω διαπιστώσεων, στον πρώτο άξονα της διατριβής επιχειρήθηκε να δοθεί λύση στην περιορισμένη δυνατότητα επικοινωνίας των Υπηρεσιών Ιστού προτείνοντας μια πρωτότυπη μεθοδολογία η οποία δύναται να ελέγξει τη διαλειτουργικότητα και τη συμμόρφωση κοινών ηλεκτρονικών Υπηρεσιών Ιστού εγγυώντας τη δυνατότητα αλληλεσύνδεση τους. Η προτεινόμενη μεθοδολογία επιτυγχάνει να καλύψει σε σημαντικό βαθμό το σύνολο των αδυναμιών όπως αυτές εντοπίστηκαν από τις υπάρχουσες μεθοδολογίες και πλαίσια διαλειτουργικότητας τα οποία μελετήθηκαν. Το στοιχείο το οποίο πρέπει να επισημανθεί είναι ότι η μεθοδολογία μπορεί να εφαρμοστεί για τον έλεγχο της διαλειτουργικότητας ηλεκτρονικών Υπηρεσιών Ιστού, όπως επίσης και υπηρεσιών οι οποίες εφαρμόζονται στα πλαίσια του ίδιου του πληροφοριακού συστήματος ή της ίδιας πλατφόμας, ενώ επίσης, οι βασικές αρχές της μπορούν να εφαρμοστούν ακόμα και στην περίπτωση των κινητών Υπηρεσιών Ιστού.

Προκειμένου να επαληθευτεί η αξία, η ορθότητα και η εφαρμοσιμότητα της μεθοδολογίας, οι αρχές της εφαρμόστηκαν ώστε να ελεχθεί η διαλειτουργικότητα και η συμμόρφωση δυο υπηρεσιών ηλεκτρονικής τιμολογήσης οι οποίες προσφέρονται αντίστοιχα από μια εφαρμογή του η-επιχειρείν, τη SELIS, και από μια πλατφόρμα της η-διακυβέρνησης, τη SWEB. Η εφαρμογή της προτεινόμενης μεθοδολογίας παρουσιάζεται στο Κεφάλαιο 3.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που μπορούν να βασιστούν και να επεκτείνουν την προτεινόμενη μεθοδολογία είναι οι ακόλουθες:

- Μια επέκταση της μεθοδολογίας θα μπορούσε να είναι η ενσωμάτωση νέων τύπων ελέγχων όπως είναι οι έλεγχοι απόδοσης και ποιότητας οι οποίοι θα παρέχουν πιο ολοκληρωμένα και με μεγαλύτερη ακρίβεια αποτελέσματα σχετικά με την δυνατότητα επικοινωνίας των εξεταζόμενων Υπηρεσιών Ιστού.
- Η εμπειρία δείχνει ότι τα αποτελέσματα της σημασιολογικής διαλειτουργικότητας στην προτεινόμενη μεθοδολογία μπορούν να βελτιωθούν σημαντικά με τη χρήση μεταδεδομένων και οντολογιών τα οποία δίνουν τη δυνατότητα αλληλεπίδρασης Υπηρεσιών Ιστού οι οποίες χρησιμοποιούν διαφορετικά XML σχήματα και διαφορετικά λεξιλόγια.
- Εμπλουτισμό των κριτηρίων αξιολόγησης των εξεταζόμενων Υπηρεσιών Ιστού με νέα κριτήρια όπως είναι η αυτοματοποιημένη σύγκριση των Πολιτικών Ιδιωτικότητας. Μια Πολιτική Ιδιωτικότητας η οποία αντιστοιχεί σε μια Υπηρεσία Ιστού χρησιμοποιείται για να εκφράσει το σύνολο των μη λειτουργικών χαρακτηριστικών της υπηρεσίας τα οποία δεν εμπεριέχονται στην περιγραφή που παρέχεται από το WSDL έγγραφο. Τα χαρακτηριστικά αυτά σχετίζονται με πτυχές ή στοιχεία που αφορούν ζητήματα όπως είναι ο καθορισμός των απαιτούμενων μηχανισμών εμπιστευτικότητας, των απαραίτητων χαρακτηριστικών πιστοποίησης, ποιότητας υπηρεσιών και ιδιωτικότητας.

Το σημείο το οποίο πρέπει να τονιστεί είναι ότι οι παραπάνω επεκτάσεις μπορούν να ενσωματωθούν στην προτεινόμενη μεθοδολογία χωρίς να επηρεάζεται ή να μεταβάλλεται σε κανέναν βαθμό η λογική συνέχεια, η πολυπλοκότητα και η ροή της.

2.5 Αναφορές

[EIF] European Interoperability Framework (EIF), http://ec.europa.eu/idabc/en/document/3473/5585.

[Lueders] H. Lueders. (2005). "*Interoperability and Open Standards for eGovernment Services*", January 2005, http://xml.coverpages.org/Comptia-ISC-OpenStandards.pdf.

[IDABC] The European Interoperability Framework for pan-European eGovernment Services (IDABC), ISBN 92-894-8389-X, 2004, http://europa.eu.int/idabc/servlets/Doc?id=19528.

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

[XML] T. Bray et al. (Editors). (2004). "*Extensible Markup Language (XML) 1.0 (Third Edition)*", W3C Recommendation 04 February 2004.

[Booth04] D. Booth et al. (Editors). (2004). "*Web Services Architecture*", W3C Working Group Note 11 February 2004, http://www.w3.org/TR/2004/NOTE-ws-arch-20040211.

[XML-DSig] XML Signature Recommendation (XML-Dsig), http://www.w3.org/TR/xmldsig-core/.

[XML-Enc] XML Encryption (XML-Enc), http://www.w3.org/Encryption/2001/

[Adams99] C. Adams, S. Lloyd, "*Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations*", 1st Edition, Macmillan Technical Publishing, 1999.

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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Nadalin06] A. Nadalin et al. (Editors). (2006). "*Web Services Security: SOAP Message Security 1.1*", OASIS Standard Specification, http://docs.oasis-open.org/wss/v1.1/.
[WSS] OASIS Web Services Security (WSS), November 28th 2006 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.
[ebXML] Electronic Business using eXtensible Markup Language (ebXML), http://www.ebxml.org/.
[RosettaNet] RosettaNet, (2003), http://www.rosettanet.org/.
[xCBL03] xCBL.org, (2003), XML Common Business Library version 4.00 (xCBL v4.00). www.xcbl.org/xcbl40/xcbl40.html.
[eBIS-XML] Specifications, Business Application Software Developers Association (BASDA), basda.net/twiki/pub/Core/DownloadTheSuite/eBIS-XML-3.05.zip.
[UBL1.0] OASIS, "Universal Business Language UBL 1.0", ver. 1.0, Official OASIS Standard, http://docs.oasis-open.org/ubl/cd-UBL-1.0.zip.
[Rowell] M. Rowell, (Editor). (2002). "*OAGIS - A "Canonical" Business Language*", Open Applications Group white paper, version 1.0, www.openapplications.org/downloads/whitepapers/whitepaperdocs/20020429_OAGIS_A_Canonical_Business_Langugage-PDF.zip
[EC03]. Linking up Europe: the Importance of Interoperability for eGovernment Services. The European Commission (EC), 2003, http://ec.europa.eu/idabc/servlets/Doc?id=1675.
[eGif] UK government's eGovernment Interoperability Framework (eGif), http://www.govtalk.gov.uk/interoperability/egif.asp.
[ADAE] l'Agence pour le développement de l'administration électronique (ADAE): Cadre commun d'interopérabilité des systèmes d'information publics à l'usage des administrations et de leurs partenaires, 2003, http://globalservices.bt.com/static/assets/pdf/case_studies/adae_en.pdf.
[SAGA] German Federal Ministry of Interior. (2003). "SAGA - Standards and Architectures for e-government Applications, version 2.0".
[Danish] Danish Ministry of Science, Technology and Innovation: National white paper on enterprise architecture, http://en.itst.dk/architecture-and-standards/publications/whitepaper-on-it-architecture.
[JUHTA] Finland's Advisory Committee on Information Management in Public Administration, JUHTA, http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/05_it_toiminta/03_juhta/index.jsp
[OSOSS] Open Standaarden en Open Source Software voor de overheid (OSOSS), http://www.ictu.nl/download/OSOSS_English.pdf.
[ORDENPRE] ORDENPRE/1551/2003, June 10th 2003, http://www.csi.map.es/csi/pg5c10.htm.
[ΠΗΔ] Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας (Πλαίσιο Ηλεκτρονικής Διακυβέρνησης (ΠΗΔ)), http://www.e-gif.gov.gr/.
[CEN] European Committee for Standardization, http://www.cenorm.be/isss/.
[ETSI] European Telecommunications Standards Institute (ETSI), http://www.etsi.org/.
[SAPE] Standardisation Action Plan in support of eEurope, http://ec.europa.eu/information_society/programmes/others/index_en.htm#Standard.
[DGISM] DG Information Society & Media, http://ec.europa.eu/dgs/information_society/index_en.htm.
[DGE] DG Enterprise,

ΠΑΡΑΤΗΜΑ ΙΕΡΑΙΑ

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/02/281&format=HTML&aged=0&language=EN&guiLanguage=en.
[IDA] Electronic interchange of data between administrations: IDA programme, http://europa.eu/scadplus/leg/en/lvb/l24147a.htm.
[eBIF] CEN European e-Business Interoperability Forum (eBIF), http://www.cen.eu/CENORM/BusinessDomains/businessdomains/isss/activity/ebif.asp.
[Kulvatunyou03] B. Kulvatunyou, N. Ivezic, M. Martin, A.T. Jones. (2003). "*A Business-to-Business Interoperability Testbed: An Overview*", Fifth International Conference on Electronic Commerence, Pittsburg, PA October 2003.
[Dibuz03] S. Dibuz and P. Kremer. (2003). "*Framework and Model for Automated Interoperability Test and its Application to ROHC*", TestCom-03, pages 243--257, 2003.
[OSI97] Open System Interconnection (OSI), Conformance testing methodology and framework, ISO/IEC 9646, 1997.
[ETSI96] ETSI Technical Report 266 (August 1996): Methods for testing and Specification (MTS); Test Purpose style guide.
[ETSI] European Telecommunications Standards Institute (ETSI), http://portal.etsi.org/mbs/Testing/testing.htm.
[Moseley03] S. Moseley, S. Randall, A. Wiles. (2003). "*Experience within ETSI of the combined roles of conformance testing and interoperability testing*", Standardization and Innovation in Information Technology, pp 177- 189, IEEE Press, 2003.
[ETSI95] ETSI 300 406 (January 1995): Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology.
[ETSI02] ETSI ES 201 873 (May 2002): The Testing and Test Control Notation version 3, v2.2.0.
[ETSI07] ETSI EG 202 237 V1.1.2 (2007-04): Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); Generic approach to interoperability testing.
[Seely05] S. Seely, D. Lauzon, (2005), WS-I monitor tool functional specification, ver. 1.1. Technical report, WS-I, NY (2005).
[Ehnebuske03] D. Ehnebuske et al., (2003), "*WS-I Overview*", www.ws-i.org/docs/20021003.wsi.introduction.pdf.
[ebXML01] ebXML Technical Architecture Project Team: ebXML Technical Architecture Specification v1.0.4, February 16, 2001.
[ebXML03] OASIS ebXML Implementation, Interoperability and Conformance Technical Committee: ebXML Test Framework v0.3, 07 March, 2003.
[Lee05] Y. Lee. (2005). "*ebXML Test Framework on Dually Coupled Asynchronous MSH*", Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05), pp. 198-203, IEEE Press, 2005.
[Kim03] D. Kim, J.H. Yun. (2003). "*Development -of an ebXML Conformance Test System for e-Business Solutions*", EC-Web 2003, LNCS, vol 2738, pp. 145-154, 2003 Springer-Verlag Berlin Heidelberg (2003).
[Peyton08] L. Peyton, B. Stepien, P. Seguin. (2008). "*Integration Testing of Composite Applications*", HICSS '08: Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences, IEEE Computer Society, January 2008.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[High05] R. High, S. Kinder, S. Graham. (2005). "*IBM's SOA Foundation – An architectural Introduction and Overview*", http://www-128.ibm.com/developerworks/webservices/library/ws-soa-whitepaper/.
[Rizwan] M. Rizwan, Y. Mamoon. "*SOA Testing using Black, White and Gray Box Techniques*", White paper Crosscheck Networks, available at http://www.crosschecknet.com/resources/articles/soatesting-v2.htm.
[Christensen01] E. Christensen et al. (2001). "*Web Services Description Language (WSDL) 1.1*", W3C Note, http://www.w3.org/TR/wsdl.
[Papastergiou09a] S. Papastergiou, D. Polemi, "*A testing process for Interoperability and Conformance of secure Web Services*", Radio Communications, published by IN-TECH, ISBN 978-953-7619-X-X, 2009.
[WSBPEL] OASIS Web Services Business Process Execution Language Version 2.0, WSBPEL 2.0, www.oasis-open.org/committees/wsbpel/
[Kaliontzoglou05] A. Kaliontzoglou et al. (2005). "*A secure e-Government platform architecture for small to medium sized public organizations*", Electronic Commerce Research & Applications, Elsevier, Volume 4, No. 2, pp. 174-186.
[Karantjias09a] T. Karantjias, S. Papastergiou, D. Polemi. (2009). "Design Principles of Secure Federated e/m - Government Framework", International Journal of Electronic Governance, Special Issue on "Users and uses of electronic governance", 2009.
[Papastergiou09b] S. Papastergiou, D. Polemi, C. Douligeris. (2009). "*SWEB: An advanced mobile Residence Certificate Service*", 3rd International Conference on e-Democracy "Next Generation Society: Technological and Legal Issues", 23 - 25 September 2009, Athens, Greece.
[J2EE] SUN Microsystems. Java 2 Platform, Enterprise Edition (J2EE). Specification, SUN Microsystems.
[dotNet] Microsoft. (2006). Microsoft .NET. http://www.microsoft.com/net/.
[Pentafronimos08] G. Pentafronimos, S. Papastergiou, D. Polemi. (2008). "*Definition and representation of test cases for e-government Web Services*", 2nd International Conference on Theory and Practice of Electronic Governance (ICEGOV2008), 1 - 4 December, 2008, Cairo, Egypt.
[Fostre06] H. Fostre, S. Uchitel, J. Magee, J. Kramer. (2006). "*Model based analysis of obligations in web service choreography*", AICT-ICIW, IEEE Computer Society, 2006, p. 149.
[Xu06] K. Xu, Y. Liu, G. Pu. (2006). "*Formalization, verification and restructuring of bpel models with pi calculus and model checking*", IBM, Tech. Rep., 2006.
[Zheng07] Y. Zheng, J. Zhou, P. Krause. (2007). "*An Automatic Test Case Generation Framework for Web Services*", Journal of Software, vol. 2(3), pp. 64-77 (2007).
[Sinha06] A. Sinha, A. Paradkar. (2006). "*Model based functional conformance testing of web services operating on persistent data*", TAV-WEB. ACM Press, 2006, pp. 17–22.
[Yuan06] Y. Yuan, Z. Li, W. Sun. (2006). "*A graph-search based approach to bpel4ws test generation*", ICSEA, IEEE Computer Society, 2006, p. 14.
[Yan06] J. Yan, Z. Li, Y. Yuan, W. Sun, J. Zhang. (2006). "*Bpel4ws unit testing: Test case generation using a concurrent path analysis approach*", ISSRE. IEEE Computer Society, 2006, pp. 75–84.
[ActiveBPEL] ActiveBPEL Engine Architecture, July 2006, available at http://www.activebpel.org/docs/architecture.html.

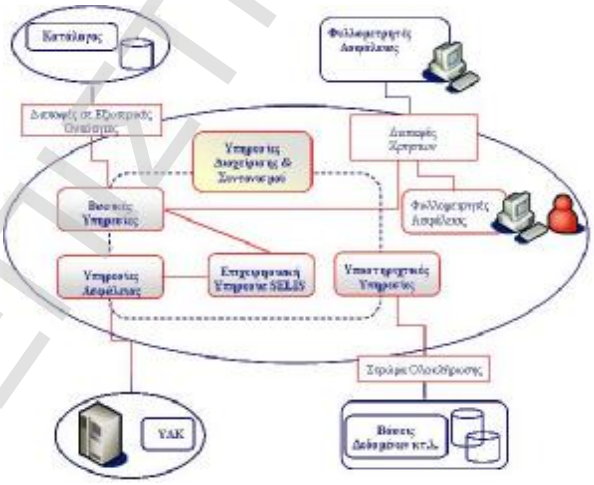
PANEPISTIMIO PIRAIA

3 Εφαρμογή ΔΣΥΙ σε Ηλεκτρονικές Υπηρεσίες

Το παρόν κεφάλαιο στοχεύει στο να επαληθεύσει την ορθότητα και εφαρμοσιμότητα της Μεθοδολογίας Ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ) που παρουσιάστηκε στο κεφάλαιο 2.3, με την εφαρμογή της για τον έλεγχο της επικοινωνίας δυο υπαρχόντων και πλήρως λειτουργικών Υπηρεσιών Ιστού για ηλεκτρονική τιμολόγηση, της αυτόνομης υπηρεσίας ηλεκτρονικής τιμολόγησης SELIS (Secure Electronic Invoicing Service) και της υπηρεσίας ηλεκτρονικής και κινητής τιμολόγησης SWEB.
Αρχικά θα πραγματοποιηθεί μια σύντομη παρουσίαση των δυο εξεταζόμενων υπηρεσιών τιμολόγησης και στη συνέχεια θα εφαρμοστούν μία προς μία οι φάσεις αλλά και τα αντίστοιχα στάδια που έχουν περιγραφεί για τη διεκπεραίωση των απαιτούμενων ελέγχων.

3.1 Αυτόνομη Υπηρεσία Ηλεκτρονικής Τιμολόγησης SELIS

Η SELIS [Kaliontzoglou06c, Kaliontzoglou06d] αποτελεί μια αυτόνομη διασυνοριακή υπηρεσία για την ασφαλή ανταλλαγή ηλεκτρονικών τιμολογίων, προσφέροντας μια εύκολα υλοποιήσιμη λύση. Βασίζεται σε μια καινοτόμο, εναλλακτική του EDI (Electronic Data Interchange) [EDI], αρχιτεκτονική ηλεκτρονικής τιμολόγησης, η οποία υιοθετεί τα πιο εξελιγμένα και ευρέως αποδεκτά πρότυπα (Υπηρεσίες Ιστού, XML, ΥΔΚ), που είναι διαθέσιμα στη σημερινή εποχή, για την ασφαλή και διαλειτουργική παροχή υπηρεσιών, ενώ παράλληλα ικανοποιεί όλες τις απαιτήσεις που προβάλλονται από τις πολιτικές της Ευρωπαϊκής Ένωσης.
Μια υψηλού επιπέδου παρουσίαση της γενικής αρχιτεκτονικής του SELIS απεικονίζεται στο Σχήμα 28:



Σχήμα 28: Αρχιτεκτονική της υπηρεσίας SELIS

Όπως γίνεται εμφανές, η αρχιτεκτονική διαιρείται σε συγκεκριμένους τομείς υπηρεσιών με ευδιάκριτες λειτουργίες. Οι τομείς αυτοί είναι: οι Βασικές Υπηρεσίες, οι Υπηρεσίες Διαχείρισης και Συντονισμού, οι Υπηρεσίες Ασφάλειας, οι Υποστηριχτικές Υπηρεσίες και η Επιχειρησιακή Υπηρεσία SELIS. Μια σύντομη περιγραφή των ομαδοποιημένων αυτών υπηρεσιών είναι η ακόλουθη:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- *Υπηρεσίες Διαχείρισης και Συντονισμού:* επιτελούν μια πολύ σημαντική λειτουργία μέσα στο αρχιτεκτονικό πλαίσιο: τη διαχείριση και ενορχήστρωση όλων των υπηρεσιών. Διαιρούνται σε: υπηρεσίες πρόσβασης, υπηρεσίες συντονισμού διαδικασιών, υπηρεσίες πολιτικών και υπηρεσίες διαχείρισης χρηστών. Στο SELIS ο συντονισμός των υπηρεσιών αποτελεί μια διαφανή διαδικασία.
- *Βασικές Υπηρεσίες*: παρέχουν βασικές λειτουργίες που χρησιμοποιούνται από την αρχιτεκτονική συνολικά για την εκτέλεση απλών διεργασιών. Οι βασικές υπηρεσίες περιλαμβάνουν τις υπηρεσίες διεπαφής με τον χρήστη, τις υπηρεσίες μετασχηματισμού μηνυμάτων, τις υπηρεσίες μεταβίβασης μηνυμάτων, τις υπηρεσίες κοινοποίησης και ανάκτησης και τις υπηρεσίες γνωστοποίησης.
- *Υπηρεσίες Ασφάλειας:* διευθετούν τις απαιτήσεις ασφάλειας της αρχιτεκτονικής. Οι μηχανισμοί ασφάλειας που υποστηρίζονται είναι οι ακόλουθοι: ψηφιακές υπογραφές, προηγμένες ηλεκτρονικές υπογραφές και κρυπτογράφηση. Οι μηχανισμοί ασφάλειας είναι ενσωματωμένοι σε συγκεκριμένα συστατικά και είναι διαθέσιμοι σε οποιοδήποτε άλλο συστατικό της αρχιτεκτονικής τους χρειάζεται, λαμβάνοντας υπόψη τις πολιτικές που διέπουν τις υπηρεσίες. Οι υπηρεσίες ασφάλειας περιλαμβάνουν επίσης μηχανισμούς που σχετίζονται με τη χρονοσφράγιση και τη διαχείριση κλειδιών και πιστοποιητικών.
- *Επιχειρησιακή Υπηρεσία SELIS:* συντονίζει την εκτέλεση των απαιτούμενων υπηρεσιών της αρχιτεκτονικής έτσι ώστε η επιχειρησιακή διαδικασία της υπηρεσίας η-τιμολόγησης να ολοκληρωθεί επιτυχώς.
- *Υποστηριχτικές Υπηρεσίες:* διαχειρίζονται το ενδιάμεσο στρώμα ολοκλήρωσης της αρχιτεκτονικής που αναλαμβάνει τη σύνδεση με τα συστήματα αποθετηρίων όπως είναι οι βάσεις δεδομένων, τα πληροφοριακά συστήματα Διαχείρισης Πληροφοριακών Πόρων κ.λπ..

Η υπηρεσία SELIS χρησιμοποιεί όλες τις ανωτέρω υπηρεσίες της αρχιτεκτονικής προκειμένου να πραγματοποιηθεί ο απαιτούμενος επιχειρησιακός σκοπός της.

3.1.1 Υποστηριζόμενα Πρότυπα

Η αρχιτεκτονική SELIS προκειμένου να καλύψει τους επιχειρηματικούς της στόχους έχει υιοθετήσει τα πιο εξελιγμένα και ευρέως χρησιμοποιούμενα πρότυπα για την παροχή ασφαλών και διαλειτουργικών υπηρεσιών, ικανοποιώντας παράλληλα όλες τις απαιτήσεις που καθορίζουν την ανταλλαγή και διαχείριση των ηλεκτρονικών τιμολογίων. Η υπηρεσία βασίζεται στις τεχνολογίες της XML και των Υπηρεσιών Ιστού, ένα γεγονός που επιτρέπει την ομαλή ολοκλήρωση με τα υπάρχοντα οικονομικά και λογιστικά πακέτα λογισμικού που οι διάφοροι οργανισμοί μπορεί να χρησιμοποιούν. Επίσης η υπηρεσία αυτή είναι αυτόνομη, γεγονός που ικανοποιεί και τις μικρότερες επιχειρήσεις. Αυτό επιτυγχάνεται με την κοινοποίηση της παρεχόμενης υπηρεσίας σε μια διεύθυνση Universal Description, Discovery and Integration Protocol (UDDI) [Clement04], στην οποία η περιγραφή της υπηρεσίας, διατυπώνεται όπως διευκρινίζεται από τη Web Services Description Language (WSDL). Η υπηρεσία αυτή μπορεί να ανακτηθεί και επομένως να χρησιμοποιηθεί από άλλες Υπηρεσίες Ιστού μέσω της χρήσης των κατάλληλων, ως προς το σχήμα τους, μηνυμάτων.
Η χρήση της XML για τη μορφοποίηση των εγγράφων των ηλεκτρονικών τιμολογίων, επιτρέπει τη χρήση XML ψηφιακών υπογραφών και την εφαρμογή χρονοσφραγίδων στο έγγραφο XML. Το σχήμα που υιοθετείται για το έγγραφο ηλεκτρονικού τιμολογίου είναι ένα υποσύνολο της προαναφερθείσας XML Common

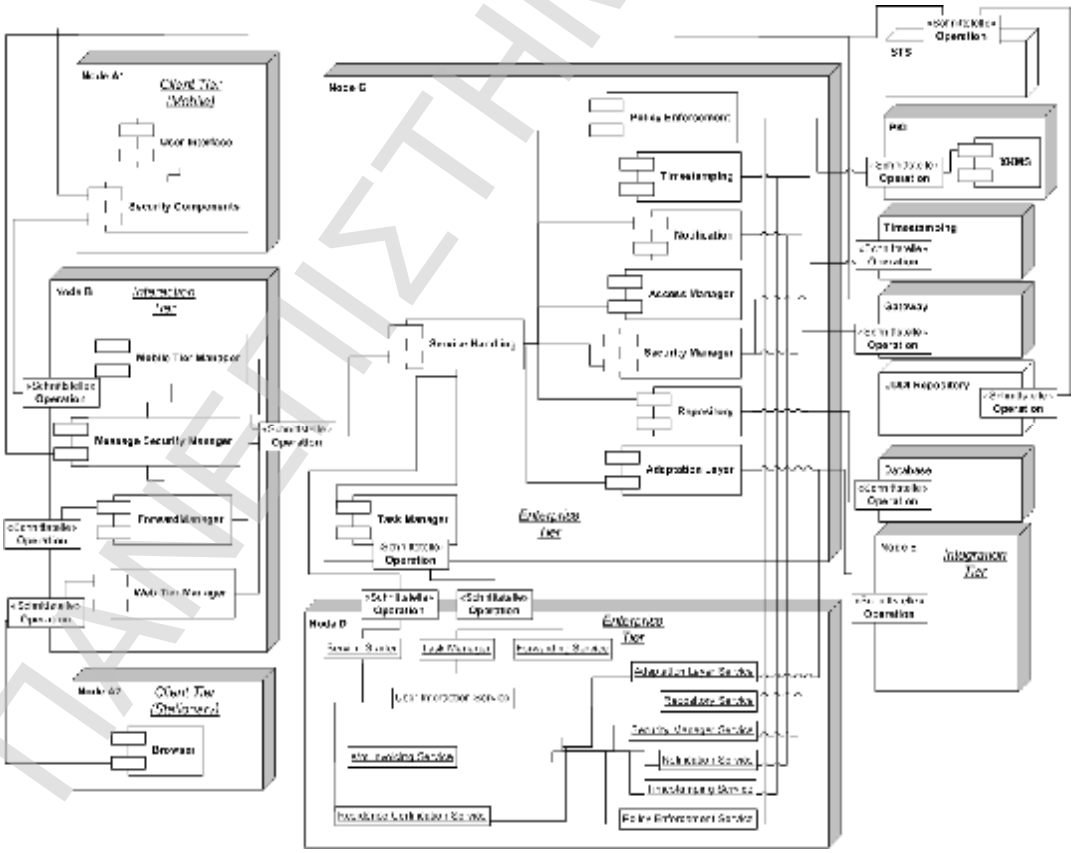
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Business Library, version 4.0 (xCBL 4.0), η οποία καλύπτει όλους τους υποχρεωτικούς τομείς που καθορίζονται στην οδηγία 2001/115/EC [European Parliament01]. Η αρχιτεκτονική SELIS υποστηρίζει επίσης την Extensible Stylesheet Language Transformation (XSLT) [XSLT] για τον μετασχηματισμό μεταξύ διαφορετικών τύπων XML εγγράφων.

Ο υποστηριζόμενος μηχανισμός ανταλλαγής για τα ηλεκτρονικά τιμολόγια στηρίζεται στο Simple Object Access Protocol (SOAP) [Mitra03] χρησιμοποιώντας και τις επεκτάσεις ασφάλειας των υπηρεσιών Ιστού [WSS06]. Η αποθήκευση αντιμετωπίζεται με την υιοθέτηση μιας βάσης δεδομένων XML με στόχο την ικανοποίηση της απαίτησης για ασφαλή αποθήκευση των ανταλλαγμένων ηλεκτρονικών τιμολογίων στη μορφή στην οποία αυτά στάλθηκαν και παραλήφθηκαν. Η ακεραιότητα και η μη-άρνηση αποποίησης ευθύνης για τα έγγραφα ηλεκτρονικών τιμολογίων εξασφαλίζονται με την χρήση των XML ψηφιακών υπογραφών έτσι ώστε οι πληροφορίες προέλευσης και ακεραιότητας να ενσωματώνονται στο ηλεκτρονικό τιμολόγιο.

3.2 Υπηρεσία Ηλεκτρονικής και Κινητής Τιμολόγησης SWEB

Η SWEB [Meneklis07] αποτελεί μια ασφαλή, ανοικτή, προσιτή πλατφόρμα ηλεκτρονικής διακυβέρνησης η οποία προσφέρει ένα σύνολο από καινοτόμες, ασφαλείς και ευέλικτες ηλεκτρονικές και κινητές υπηρεσίες, όπως η η/κ-τιμολόγηση. Οι υπηρεσίες αυτές είναι προσιτές από διάφορους οργανισμούς αλλά και από τους πολίτες που έχουν υιοθετήσει και χρησιμοποιούν ηλεκτρονικές και κινητές λύσεις οι οποίες βασίζονται σε πρότυπα των Υπηρεσιών Ιστού.



Σχήμα 29: Αρχιτεκτονική της Πλατφόρμας SWEB

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η αρχιτεκτονική της πλατφόρμας SWEB, όπως απεικονίζεται στο Σχήμα 29, αποτελείται από πέντε κόμβους με διακριτές λειτουργίες. Οι κόμβοι αυτοί είναι οι ακόλουθοι:

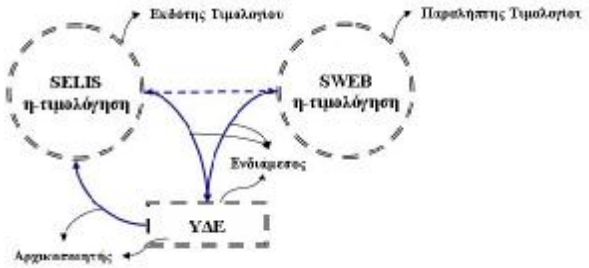
- *Κόμβος Α* στο επίπεδο πελάτη. Στον κόμβο βρίσκεται η *Εφαρμογή πελάτη (Client)* με την οποία αλληλεπιδρούν οι οργανισμοί και οι πολίτες με την κύρια πλατφόρμα και αποτελεί το ένα μέρος της υπηρεσίας διεπαφής χρηστών. Σε αυτή περιλαμβάνονται ηλεκτρονικές και κινητές εφαρμογές οι οποίες υποστηρίζουν πρότυπα και τεχνολογίες όπως είναι η XML, οι Υπηρεσίες Ιστού, XML προηγμένες και απλές ψηφιακές υπογραφές, XML κρυπτογράφηση κτλ.
- *Κόμβος Β* στο επίπεδο αλληλεπίδρασης. Ο κόμβος περιέχει τον *Διαχειριστή Αιτήσεων* που δέχεται τις αιτήσεις πρόσβασης από τις εφαρμογές πελάτες, τις αποδομεί κατάλληλα και τις αποστέλλει στο πρώτο επιχειρησιακό επίπεδο στον κόμβο C, προκειμένου να λάβει τις απαραίτητες απαντήσεις. Η εποικοινωνία βασίζεται σε μηνύματα SOAP.
- *Κόμβος C* στο πρώτο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών Β (App Server B)*. Ο κόμβος αυτός αποτελεί την καρδιά της συγκεκριμένης αρχιτεκτονικής όπου φιλοξενείται το μεγαλύτερο μέρος των υπηρεσιών διαχείρισης καθώς και οι βασικές υπηρεσίες, οι υπηρεσίες υποστήριξης υπαρχουσών υποδομών και οι υπηρεσίες ασφάλειας.
- *Κόμβος D* στο δεύτερο επιχειρησιακό επίπεδο, ο οποίος περιέχει τον *Εξυπηρετητή εφαρμογών C (App Server C)*. Αυτός ο κόμβος περιλαμβάνει το αντικείμενο *Διαχειριστής επιχειρησιακών διεργασιών (Enterprise Task Manager)*, ο οποίος επιτελεί τις διαχειριστικές εργασίες τις σχετικές με τον σχεδιασμό, συντονισμό, εγκατάσταση και απεγκατάσταση των επιχειρησιακών υπηρεσιών και υπο-υπηρεσιών. Στον κόμβο αυτό βρίσκεται η επιχειρησιακή λογική της Υπηρεσίας ηλεκτρονικής και κινητής τιμολόγησης.
- *Κόμβος Ε* στο επίπεδο ολοκλήρωσης. Στον κόμβο Ε περιλαμβάνεται το κομμάτι της υπηρεσίας υποστήριξης υπαρχουσών υποδομών που ολοκληρώνει το υπάρχον σύστημα του οργανισμού (Βάση δεδομένων, Πληροφοριακά Συστήματα Διαχείρισης Πληροφοριακών Πόρων).

Η πλατφόρμα είναι ιδιαίτερα ευπροσάρμοστη έχοντας τη δυνατότητα να υποστηρίξει και να ενσωματώσει ένα σύνολο νέων υπηρεσιών.

3.3 1η Φάση ΔΣΥΙ: Προσδιορισμός Οντοτήτων

Κατά την πρώτη φάση της μεθοδολογίας προσδιορίζεται ο ακριβής αριθμός και η διάταξη των οντοτήτων που μετέχουν στην ακολουθία ελέγχου. Η ολοκλήρωση της διαδικασίας αυτής γίνεται ακολουθώντας τα βήματα που παρουσιάστηκαν στο Κεφάλαιο 2.3.3.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 30. Προσδιορισμός Οντοτήτων και Καθορισμός Διάταξης τους

Στην προκειμένη περίπτωση τα συστήματα τα οποία ελέγχονται είναι δύο, η υπηρεσία ηλεκτρονικής τιμολόγησης SELIS (SELIS η-τιμολόγηση) και η υπηρεσία τιμολόγησης της πλατφόρμας SWEB (SWEB η-τιμολόγηση). Η διάταξη των δύο συστημάτων υπό έλεγχο εμφανίζεται στο Σχήμα 30, σύμφωνα με το οποίο η SELIS η-τιμολόγηση ενεργεί ως το ΣυΕ 1 το οποίο δημιουργεί ένα ηλεκτρονικό τιμολόγιο και το αποστέλλει (ρόλος-Εκδότης), ενώ η SWEB η-τιμολόγηση ενεργεί ως το ΣυΕ 2 το οποίο λαμβάνει το απεσταλμένο τιμολόγιο το επεξεργάζεται (ρόλος-Παραλήπτης) επιστρέφοντας μια επιβεβαίωση.
Η ΥΔΕ δρα ως ο γενικός συντονιστής της όλης διαδικασίας φέροντας την ευθύνη της εποπτείας της ορθής επικοινωνίας μεταξύ των δύο ΣυΕ και επιδεικνύοντας σε αυτά τις εξεταζόμενες περιπτώσεις ελέγχου.

3.3.1 2η Φάση ΔΣΥΙ: Προσαρμογή Δομής Οντοτήτων

Στα πλαίσια της δεύτερης φάσης της μεθοδολογίας πραγματοποιείται ο καθορισμός της δομής των εμπλεκομένων οντοτήτων, της ΥΔΕ και των δύο ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης, με την μορφή με την οποία θα λάβουν μέρος στους εκτελέσιμους ελέγχους.

3.3.1.1 Καθορισμός Συστημάτων υπό Έλεγχο (ΣυΕ)

Στην παρούσα φάση θα πραγματοποιηθεί η εκτέλεση των βημάτων καθορισμού των δύο ΣυΕ (βλ. § 2.3.4.1.4) τα οποία αντιστοιχούν στα δύο συστήματα τα οποία ελέγχονται, τη SELIS η-τιμολόγηση και τη SWEB η-τιμολόγηση. Στις παραγράφους που ακολουθούν θα γίνει παρουσίαση των βημάτων αυτών για κάθε ένα από τα εξεταζόμενα συστήματα.

3.3.1.1.1 SELIS η-τιμολόγηση

3.3.1.1.1.1 Βήμα 1 & 2: Μελέτη και Καταγραφή Διαθέσιμων Υπηρεσιών & Ανάλυση Διεπαφών

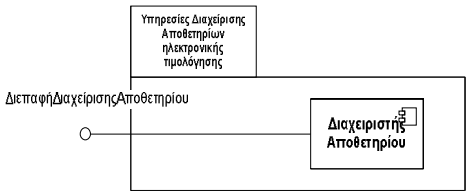
Στο Κεφάλαιο αυτό θα ολοκληρωθούν από κοινού τα δύο πρώτα βήματα του καθορισμού του ΣυΕ της SELIS η-τιμολόγησης. Το πρώτο βήμα αφορά τη "Μελέτη και καταγραφή των διαθέσιμων υπηρεσιών και μηχανισμών" της SELIS η-τιμολόγησης και το δεύτερο την "Ανάλυση Διεπαφών των διαθέσιμων υπηρεσιών-λειτουργιών" της. Το σύνολο αυτών των στοιχείων συνθέτουν την SELIS YIυE.
Στις παραγράφους που ακολουθούν περιγράφονται οι υποστηριζόμενοι μηχανισμοί και υπηρεσίες.

3.3.1.1.1.1.1 Υπηρεσία διαχείρισης αποθετηρίων ηλεκτρονικής τιμολόγησης

Μια *Υπηρεσία διαχείρισης αποθετηρίου ηλεκτρονικής τιμολόγησης* είναι υπεύθυνη για την εισαγωγή και εξαγωγή εγγράφων ηλεκτρονικής τιμολόγησης από ένα αποθετήριο

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

(π.χ. βάσεις δεδομένων, πληροφοριακά συστήματα Διαχείρισης Πληροφοριακών Πόρων). Το βασικό δομικό στοιχείο της είναι ο *Διαχειριστής Αποθετηρίου (Repository Manager)*, όπως φαίνεται στο Σχήμα 31.

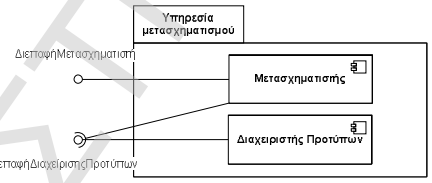


Σχήμα 31: Βασικό Στοιχείο Υπηρεσίας Διαχείρισης Αποθετηρίου

Ο Διαχειριστής Αποθετηρίου υλοποιεί την *διεπαφή διαχείρισης αποθετηρίου (repository manager interface)*, η οποία είναι διαθέσιμη σε άλλες υπηρεσίες που θέλουν να εισάγουν ή να εξάγουν κάποιο έγγραφο από το αποθετήριο, ή να κάνουν μια *ερώτηση (query)* για την λήψη πληροφοριών βάσει των ήδη υπαρχόντων εγγράφων.

3.3.1.1.1.1.2 Υπηρεσία μετασχηματισμού ηλεκτρονικών τιμολογίων

Η *Υπηρεσία μετασχηματισμού ηλεκτρονικών τιμολογίων* αποτελείται από δύο βασικούς μηχανισμούς. Μια «μηχανή» μετασχηματισμών που χρησιμοποιεί πρότυπα μετασχηματισμών προκειμένου να μετατρέψει έγγραφα ηλεκτρονικής τιμολόγησης XML από μια μορφή σε μια άλλη, και από έναν διαχειριστή των προτύπων αυτών. Ο διαχειριστής των προτύπων είναι προσβάσιμος από έναν διαχειριστή του συστήματος προκειμένου να προσθέσει, να αφαιρέσει ή να παραμετροποιήσει πρότυπα, αλλά και από την ίδια την μηχανή μετασχηματισμών για την ανάκτηση προτύπων κατά την διαδικασία μετασχηματισμού.
Το βασικό στοιχείο της όψης φαίνεται στο ακόλουθο γενικό διάγραμμα δομικών στοιχείων:



Σχήμα 32: Βασικό Στοιχείο Υπηρεσίας Μετασχηματισμού

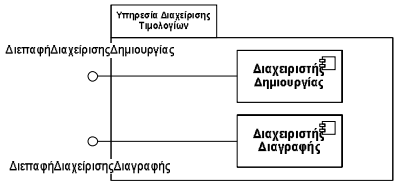
Η λειτουργία της μηχανής μετασχηματισμών αποτελείται από το δομικό στοιχείο *Μετασχηματιστής (Transformer)* και η διαχείριση των προτύπων από τον *Διαχειριστή Προτύπων (Template Manager)*. Τα δομικά στοιχεία υλοποιούν δύο διεπαφές, την `διεπαφή μετασχηματιστή (transformer interface)` και την `διεπαφή διαχείρισης προτύπων (template manager interface)`. Όπως φαίνεται στο σχήμα Σχήμα 32, η διεπαφή διαχείρισης προτύπων είναι διαθέσιμη προς χρήση τόσο από εξωτερικές οντότητες / υπηρεσίες όσο και από την ίδια την μηχανή μετασχηματισμών. Επίσης, ο *Διαχειριστής Προτύπων* επικοινωνεί με μια *Υπηρεσία Διαχείρισης Αποθετηρίων* προκειμένου να φυλάξει, να μεταβάλλει και να ανακτήσει τα πρότυπα μετασχηματισμού.

3.3.1.1.1.1.3 Υπηρεσία Διαχείρισης Τιμολογίων

Η *Υπηρεσία διαχείρισης τιμολογίων* αναλαμβάνει να διαχειριστεί όλο τον κύκλο ζωής ενός τιμολογίου από την δημιουργία μέχρι και την πιθανή διαγραφή ενός προσχέδιου ηλεκτρονικής τιμολόγησης. Το βασικά δομικά στοιχεία της είναι ο *Διαχειριστής*

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Δημιουργίας (Creation Manager) και ο *Διαχειριστής Διαγραφής (Deletion Manager)* όπως φαίνεται στο Σχήμα 33.

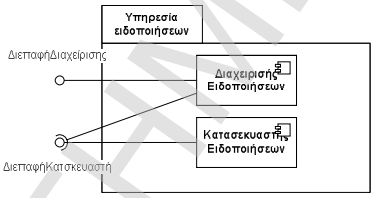


Σχήμα 33: Βασικό Στοιχείο Υπηρεσίας Διαχείρισης Αποθετηρίου

Οι διεπαφές οι οποίες υλοποιούνται είναι η `διεπαφή διαχείρισης δημιουργίας (creation manager interface)` και η `διεπαφή διαχείρισης διαγραφής (deletion manager interface)`.

3.3.1.1.1.1.4 Υπηρεσία ειδοποιήσεων ηλεκτρονικής τιμολόγησης

Η *Υπηρεσία ειδοποιήσεων ηλεκτρονικής τιμολόγησης* αποτελείται από δύο στοιχεία που επιτελούν βασικές λειτουργίες, τον *Διαχειριστή Ειδοποιήσεων (Notification Manager)*, ο οποίος είναι υπεύθυνος για την λήψη αιτήσεων για αποστολή της ειδοποίησης και την δημιουργία των κατάλληλων *Κατασκευαστών Ειδοποιήσεων (Notification Producer)*. Ο *Κατασκευαστής Ειδοποιήσεων* αναλαμβάνει να κατασκευάσει ένα αντικείμενο πληροφορίας το οποίο αποτελεί ένα έγγραφο XML που στέλνεται σαν απόκριση για την λήψη του απεσταλμένου εγγράφου ηλεκτρονικής τιμολόγησης.

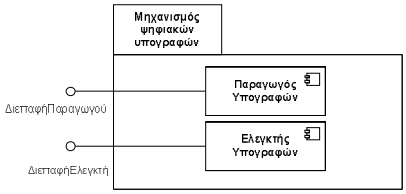


Σχήμα 34: Βασικό Στοιχείο Υπηρεσίας Ειδοποιήσεων

Ο *Διαχειριστής Ειδοποιήσεων* υλοποιεί την `διεπαφή διαχείρισης (ManagerInterface)`, και ο `Κατασκευαστής την Διεπαφή Κατασκευαστή (ProducerInterface)`. Όπως φαίνεται στο Σχήμα 34, ο *Διαχειριστής* επίσης επικοινωνεί με έναν *Κατασκευαστή* μέσω της ίδιας `διεπαφής Κατασκευαστή`.

3.3.1.1.1.1.5 Μηχανισμός ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση

Ο *Μηχανισμός ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση* χρησιμοποιεί το πρότυπο ψηφιακών υπογραφών XML για να παράγει και να επαληθεύσει ψηφιακές υπογραφές εγγράφων ηλεκτρονικής τιμολόγησης βάσει συγκεκριμένων κλειδιών και πιστοποιητικών που είναι αποθηκευμένα σε μια έξυπνη κάρτα ή έναν αποθηκευτικό χώρο στον δίσκο της μονάδας.



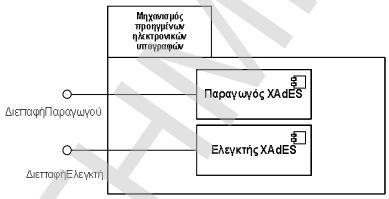
Σχήμα 35: Βασικό Στοιχείο Μηχανισμού Ψηφιακών Υπογραφών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η δομή του βασικού στοιχείου είναι απλή. Αποτελείται από τον *Παραγωγό Υπογραφών (SignatureGenerator)* ο οποίος δέχεται το έγγραφο προς υπογραφή και μια αναφορά στο χώρο αποθήκευσης του κρυπτογραφικού υλικού που θα χρησιμοποιηθεί (π.χ. ιδιωτικό κλειδί σε έξυπνη κάρτα) και παράγει το υπογεγραμμένο έγγραφο. Ο μηχανισμός μπορεί να παραμετροποιηθεί με κατάλληλα πρότυπα προκειμένου να παράγεται κάποιο από τα τρία είδη υπογραφών (περικλείουσες, περικλειόμενες ή αποσπασμένες). Ο *Ελεγκτής Υπογραφών (SignatureValidator)* δέχεται ένα υπογεγραμμένο έγγραφο και κάνει όλους τους απαραίτητους ελέγχους προκειμένου να αποφανθεί εάν η υπογραφή είναι έγκυρη (π.χ. έλεγχο των χρησιμοποιούμενων πιστοποιητικών, κρυπτογραφική συνοχή των δεδομένων κ.λ.π) όπως προδιαγράφεται από το πρότυπο. Γι' αυτό το λόγο ενδέχεται να επικοινωνεί με την αντίστοιχη υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών. Από αρχιτεκτονικής άποψης, τα δύο στοιχεία θα μπορούσαν να ενοποιηθούν σε ένα που να περιλαμβάνει και τις δύο λειτουργίες.
Τα στοιχεία υλοποιούν τις αντίστοιχες *διεπαφές Παραγωγού (GeneratorInterface)* και *Ελεγκτή (ValidatorInterface)*.

3.3.1.1.1.1.6 Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών για ηλεκτρονική τιμολόγηση

Ο *Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών για ηλεκτρονική τιμολόγηση* βασίζεται στο πρότυπο XAdES, για την παραγωγή και επαλήθευση υπογραφών XML σε έγγραφα ηλεκτρονικής τιμολόγησης που περιέχουν ένα ευρύτερο σύνολο πληροφοριών το οποίο τις καθιστά κατάλληλες για ηλεκτρονικές συναλλαγές.



Σχήμα 36: Βασικό Στοιχείο Προηγμένων Ηλεκτρονικών Υπογραφών

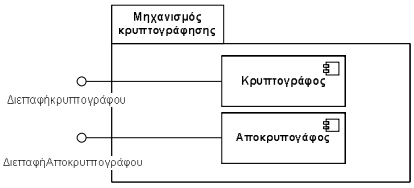
Το βασικό στοιχείο του μηχανισμού αρχικά αποτελείται από τον *Παραγωγό XAdES (XAdESGenerator)* ο οποίος συλλέγει τις κατάλληλες πληροφορίες για την παραγωγή της υπογραφής. Σύμφωνα με το πρότυπο οι πληροφορίες αυτές είναι το έγγραφο ηλεκτρονικής τιμολόγησης XML προς υπογραφή, η πολιτική υπογραφής που ακολουθείται σε ηλεκτρονική μορφή, ένα σύνολο χαρακτηριστικών της υπογραφής (κάποια από τα οποία υπογράφονται και κάποια όχι), η χρονοσφραγίδα και τα δεδομένα ανάκλησης πιστοποιητικών. Προκειμένου να ενσωματώσει όλες αυτές τις πληροφορίες σε μια υπογραφή XAdES ο παραγωγός πρέπει να επικοινωνήσει τουλάχιστον με την υπηρεσία χρονοσφράγισης και την αντίστοιχη υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών. επίσης, κάνει χρήση του μηχανισμού απλών ψηφιακών υπογραφών της προηγούμενης παραγράφου.
Ο *Ελεγκτής XAdES (XAdESValidator)* ελέγχει την εγκυρότητα της υπογραφής XAdES στο σύνολό της. Δηλαδή ελέγχει όλα τα επιμέρους συστατικά που την αποτελούν καθώς και την ίδια την απλή XML υπογραφή που περιέχει, κάνοντας χρήση του Μηχανισμού ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση (βλ. § 3.3.1.1.1.1.5).

3.3.1.1.1.1.7 Μηχανισμός κρυπτογράφησης για ηλεκτρονική τιμολόγηση

Ο *Μηχανισμός κρυπτογράφησης για ηλεκτρονική τιμολόγηση* υλοποιεί την κρυπτογράφηση και αποκρυπτογράφηση ολόκληρων ή μέρους XML εγγράφων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ηλεκτρονικής τιμολόγησης σύμφωνα με το αντίστοιχο πρότυπο. Χρησιμοποιεί την αντίστοιχη υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών προκειμένου να εντοπίσει το κατάλληλο δημόσιο κλειδί που θα χρησιμοποιηθεί κάθε φορά για την κρυπτογράφηση.

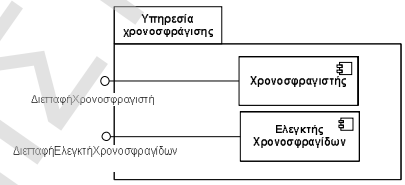


Σχήμα 37: Βασικό Στοιχείο Μηχανισμού Κρυπτογράφησης

Ο μηχανισμός αποτελείται από έναν *Κρυπτογράφο (Encryptor)* και έναν *Αποκρυπτογράφο (Decryptor)*. Ο *Κρυπτογράφος* δέχεται το απλό έγγραφο, μια αναφορά σε ένα δημόσιο κλειδί και τις παραμέτρους κρυπτογράφησης (π.χ. αλγόριθμοι που θα χρησιμοποιηθούν). Εντοπίζει το κλειδί και υλοποιεί την διαδικασία κρυπτογράφησης σύμφωνα με το πρότυπο (χρησιμοποιώντας υβριδική κρυπτογραφία). Ο *Αποκρυπτογράφος* έχει πρόσβαση στον αποθηκευτικό χώρο που περιέχει το ιδιωτικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση.
Τα στοιχεία υλοποιούν τις αντίστοιχες διεπαφές *Κρυπτογράφου* `(EncryptorInterface)` και *Αποκρυπτογράφου* `(DecryptorInterface)`.

3.3.1.1.1.1.8 Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση

Η *Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση* αποτελεί επί της ουσίας μια υπηρεσία για την πραγματική υπηρεσία που βρίσκεται εκτός του ΣυΕ και παρέχεται από μια Υποδομή Δημοσίου Κλειδιού. Η υπηρεσία αυτή έχει ως στόχο να λαμβάνει αιτήσεις για χρονοσφραγίδες σε έγγραφα ηλεκτρονικής τιμολόγησης από τις υπηρεσίες που βρίσκονται εντός του ΣυΕ και να τις προωθεί στην πραγματική υπηρεσία για λήψη χρονοσφραγίδων.



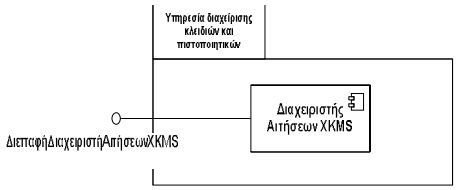
Σχήμα 38: Βασικό Στοιχείο Υπηρεσίας Χρονοσφράγισης

Γι' αυτό το λόγο η αρχιτεκτονική του βασικού στοιχείου της υπηρεσίας είναι απλή. Ο *Χρονοσφραγιστής (TimeStamper)* λαμβάνει το έγγραφο προς χρονοσφράγιση και αναλαμβάνει να αποστείλει το hash του στην Αρχή Χρονοσφράγισης σύμφωνα με το πρότυπο χρονοσφράγισης RFC 3161. Επιστρέφει το δυαδικό αντικείμενο χρονοσφράγισης που του αποστέλλει η Αρχή Χρονοσφράγησης (χρονοσφραγίδα). Όταν μια υπηρεσία ζητά την επαλήθευση μιας τέτοιας χρονοσφραγίδας, επικαλείται τον *Ελεγκτή Χρονοσφραγίδων (StampValidator)*, ο οποίος ελέγχει την κρυπτογραφική υπόσταση της σφραγίδας και επικοινωνεί με την υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για να ελέγξει αν είναι έγκυρο το πιστοποιητικό που χρησιμοποιήθηκε για την συγκεκριμένη χρονοσφραγίδα.
Ο *Χρονοσφραγιστής* και ο *Ελεγκτής Χρονοσφραγίδων* υλοποιούν αντίστοιχα τις διεπαφές *Χρονοσφραγιστή* `(StamperInterface)` και *Ελεγκτή Χρονοσφραγίδων* `(ValidatorInterface)`.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.3.1.1.1.1.9 Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης

Η υπηρεσία αυτή αποτελεί έναν εξυπηρετητή που υλοποιεί το πρότυπο XML Key Management System (XKMS), η οποία επικοινωνεί με την Αρχή Πιστοποίησης.



Σχήμα 39: Βασικό Στοιχείο Υπηρεσίας Διαχείρισης Κλειδιών και Πιστοποιητικών

Αποτελείται από μια μονάδα *Διαχείρισης Αιτήσεων XKMS (XKMSRequestManager)* που αναλαμβάνει να δέχεται τις αιτήσεις για οποιαδήποτε εργασία διαχείρισης, είτε σε μια μορφή που είναι ήδη συμβατή με το XKMS είτε σε κάποια άλλη μορφή, να τις μετατρέπει σε μορφή XKMS αν απαιτείται, και να τις αποστέλλει στον εξυπηρετητή XKMS της Αρχής Πιστοποίησης με την οποία επικοινωνεί.
Η υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών ενδέχεται να χρησιμοποιεί τους *μηχανισμούς ψηφιακών υπογραφών και κρυπτογραφίας* στα μηνύματα που συνθέτει προς την Αρχή Πιστοποίησης.

3.3.1.1.1.1.10 Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης

Η *Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης* αποτελείται από στοιχεία που αναγνωρίζουν το πλαίσιο μεταφοράς ενός μηνύματος που περιέχει ένα ηλεκτρονικό τιμολόγιο και δημιουργούν τα κατάλληλα μηνύματα SOAP προκειμένου να το αποστείλουν στη σωστή διεύθυνση, εφαρμόζοντας στην πορεία τους απαιτούμενους μηχανισμούς ασφάλειας, σύμφωνα με την πολιτική που έχει καθοριστεί.

Σχήμα 40: Βασικό Στοιχείο Υπηρεσίας Προώθησης Μηνυμάτων

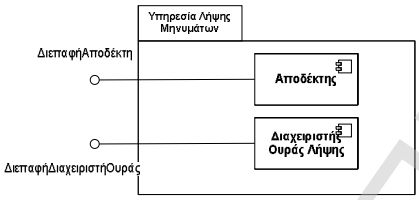
Το διάγραμμα δομικών στοιχείων του Σχήμα 40 επιδεικνύει τα δύο στοιχεία που αποτελούν την υπηρεσία, τον *Διακομιστή (Forwarder)* και τον *Διαχειριστή της Ουράς Προώθησης (Forwarding Queue Manager)*.
Ο *Διακομιστής* αναλαμβάνει να ανακτά κάθε φορά ένα μήνυμα που έχει αποθηκευτεί στην ουρά προώθησης, να φτιάχνει τον απαραίτητο μήνυμα που το περιέχει, να ενσωματώνει όποια πληροφορία ασφάλειας απαιτείται και να το αποστέλλει στον παραλήπτη του. Για την περαίωση των παραπάνω διαδικασιών, ενδέχεται να επικοινωνεί με διάφορες υπηρεσίες ασφάλειας (ή να χρησιμοποιεί μηχανισμούς ασφάλειας) ανάλογα με την πολιτική που ακολουθείται και με την Υπηρεσία Δημοσίευσης και αναζήτησης σε καταλόγους Υπηρεσιών Ιστού, όταν πρόκειται να αναζητηθεί η διεύθυνση ενός παραλήπτη, εάν δεν είναι γνωστή με άλλο τρόπο.
Ο *Διαχειριστής της Ουράς Προώθησης* δέχεται τα μηνύματα που πρόκειται να προωθηθούν, καθορίζει το πλαίσιο προώθησης κάθε μηνύματος και το αποθηκεύει

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

στην ουρά. Η πρόσβαση στα δύο στοιχεία γίνεται μέσω των αντίστοιχων διεπαφών *Διεπαφή Διακομιστή* (`ForwardInterface`) και *Διεπαφή Διαχειριστή Ουράς* (`QueueManagerInterface`).

3.3.1.1.1.1.11 Υπηρεσία λήψης μηνυμάτων ηλεκτρονικής τιμολόγησης

Η *Υπηρεσία Λήψης Μηνυμάτων ηλεκτρονικής τιμολόγησης* αποτελείται από στοιχεία που αναγνωρίζουν το πλαίσιο μεταφοράς ενός μηνύματος λαμβάνοντας τα και αποδομώντας τους «φακέλους» SOAP. Η πληροφορία η οποία εξάγεται από τους «φακέλους» είναι είτε τα ανταλλασσόμενα ηλεκτρονικά τιμολόγια είτε οι ειδοποιήσεις.



Σχήμα 41: Στοιχεία Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων

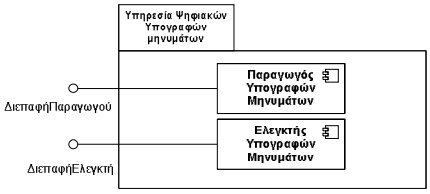
Το διάγραμμα δομικών στοιχείων του Σχήμα 41 επιδεικνύει τα δύο στοιχεία που αποτελούν την υπηρεσία, τον *Αποδέκτη (Receiver)* και τον *Διαχειριστή της Ουράς Λήψης (Receiving Queue Manager)*.

Ο *Αποδέκτης* λαμβάνει τα μηνύματα που προορίζονται για το ΣυΕ και τα αποθηκεύει στην ουρά λήψης χρησιμοποιώντας τον *Διαχειριστή της Ουράς Λήψης*. Επιπλέον αναλαμβάνει να ανακτά κάθε φορά ένα μήνυμα που έχει αποθηκευτεί στην ουρά λήψης και να το αποδομεί εξάγοντας το περιεχόμενο του.

Η πρόσβαση στα δύο στοιχεία γίνεται μέσω των αντίστοιχων *διεπαφών* *ΔιεπαφήΑποδέκτη* (`ReceiveInterface`) και *ΔιεπαφήΔιαχειριστήΟυράς* (`QueueManagerInterface`).

3.3.1.1.1.1.12 Υπηρεσία ψηφιακών υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης

Η *Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης* χρησιμοποιεί το πρότυπο ασφάλειας υπηρεσιών ιστού για να παράγει και να επαληθεύσει ψηφιακές υπογραφές σε μηνύματα τα οποία βασίζονται στις υπηρεσίες ιστού βάσει συγκεκριμένων κλειδιών και πιστοποιητικών που είναι αποθηκευμένα σε έναν αποθηκευτικό χώρο στον δίσκο της μονάδας.



Σχήμα 42: Βασικό Στοιχείο Μηχανισμού Ψηφιακών Υπογραφών

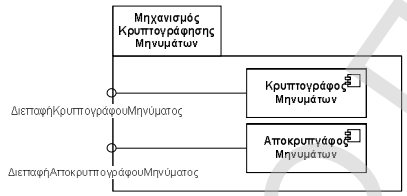
Η δομή του βασικού στοιχείου είναι απλή. Αποτελείται από τον *Παραγωγό Υπογραφών Μηνυμάτων (SignatureGeneratorMessage)* ο οποίος δέχεται το μήνυμα προς υπογραφή καθώς και μια αναφορά στο χώρο αποθήκευσης του κρυπτογραφικού υλικού που θα χρησιμοποιηθεί (π.χ. ιδιωτικό κλειδί) και παράγει το υπογεγραμμένο μήνυμα. Ο *Ελεγκτής Υπογραφών Μηνυμάτων (SignatureValidatorMessage)* δέχεται ένα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

υπογεγραμμένο μήνυμα και κάνει όλους τους απαραίτητους ελέγχους προκειμένου να αποφανθεί εάν η υπογραφή είναι έγκυρη (π.χ. έλεγχο των χρησιμοποιούμενων πιστοποιητικών, κρυπτογραφική συνοχή των δεδομένων κ.λ.π) όπως προδιαγράφεται από το πρότυπο. Γι' αυτό το λόγο ενδέχεται να επικοινωνεί με την αντίστοιχη υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών.
Τα στοιχεία υλοποιούν τις αντίστοιχες *διεπαφές Παραγωγού (GeneratorMesInterface)* και *Ελεγκτή (ValidatorMesInterface)*.

3.3.1.1.1.1.13 Υπηρεσία κρυπτογράφησης μηνυμάτων ηλεκτρονικής τιμολόγησης

Η *Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης* υλοποιεί την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων των υπηρεσιών ιστού σύμφωνα με το αντίστοιχο πρότυπο. Χρησιμοποιεί την αντίστοιχη υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών προκειμένου να εντοπίσει το κατάλληλο δημόσιο κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση κάθε φορά.

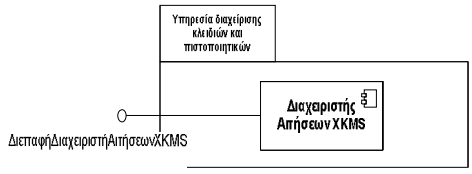


Σχήμα 43: Βασικό Στοιχείο Μηχανισμού Κρυπτογράφησης

Ο μηχανισμός αποτελείται από έναν *Κρυπτογράφο Μηνυμάτων (EncryptorMessage)* και έναν *Αποκρυπτογράφο Μηνυμάτων (DecryptorMessage)*. Ο *Κρυπτογράφος* δέχεται ένα μήνυμα, μια αναφορά σε ένα δημόσιο κλειδί και τις παραμέτρους κρυπτογράφησης (π.χ. αλγόριθμοι που θα χρησιμοποιηθούν). Εντοπίζει το κλειδί και υλοποιεί την διαδικασία κρυπτογράφησης σύμφωνα με το πρότυπο (χρησιμοποιώντας υβριδική κρυπτογραφία). Ο *Αποκρυπτογράφος* έχει πρόσβαση στον αποθηκευτικό χώρο που περιέχει το ιδιωτικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση.
Τα στοιχεία υλοποιούν τις αντίστοιχες διεπαφές *Κρυπτογράφου Μηνύματος (EncryptorMesInterface)* και *Αποκρυπτογράφου Μηνύματος (DecryptorMesInterface)*.

3.3.1.1.1.1.14 Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων

Η υπηρεσία αυτή αποτελεί έναν εξυπηρετητή που υλοποιεί το πρότυπο XKMS, η οποία επικοινωνεί με την Αρχή Πιστοποίησης.



Σχήμα 44: Βασικό Στοιχείο Υπηρεσίας Διαχείρισης Κλειδιών και Πιστοποιητικών

Η ύπαρξη της υπηρεσίας (Σχήμα 44) επιτυγχάνει έναν κεντρικό έλεγχο της διαχείρισης των κλειδιών και των πιστοποιητικών που θα χρησιμοποιηθούν για την εφαρμογή και επαλήθευση των μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων. Αποτελείται από μια μονάδα *Διαχείρισης Αιτήσεων XKMS (XKMSRequestManager)* που αναλαμβάνει να δέχεται τις αιτήσεις για οποιαδήποτε εργασία διαχείρισης, είτε σε μια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

μορφή που είναι ήδη συμβατή με το XKMS είτε σε κάποια άλλη μορφή, να τις μετατρέπει σε μορφή XKMS, αν απαιτείται, και να τις αποστέλλει στον εξυπηρετητή XKMS της Αρχής Πιστοποίησης με την οποία επικοινωνεί.
Η *υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών* ενδέχεται να χρησιμοποιεί τους *μηχανισμούς ψηφιακών υπογραφών και κρυπτογραφίας* στα μηνύματα που συνθέτει προς την Αρχή Πιστοποίησης.

3.3.1.1.1.2 Βήμα 3: Καθορισμός των Προτύπων

Το 3ο βήμα του συγκεκριμένου σταδίου αποτελεί η καταγραφή των προτύπων που έχει υιοθετήσει και εφαρμόζει η SELIS η-τιμολόγηση. Η αρχιτεκτονική SELIS προκείμενου να καλύψει τους επιχειρηματικούς της στόχους έχει υιοθετήσει τα πιο εξελιγμένα και ευρέως χρησιμοποιούμενα πρότυπα για την παροχή ασφαλών και διαλειτουργικών υπηρεσιών, ικανοποιώντας παράλληλα όλες τις απαιτήσεις που καθορίζουν την ανταλλαγή και διαχείριση των ηλεκτρονικών τιμολογίων.

ΣυΕ	**Πρότυπα/Προδιαγραφές**		**Σκοπός**
SELIS η-τιμολόγηση	XML common business library version 4.0 (xCBL 4.0)		SELIS XML έγγραφα ηλεκτρονικής τιμολόγησης
	XML σχήμα που υποστηρίζεται από το Exact ERP		Έγγραφα ηλεκτρονικής τιμολόγησης υποστηριζόμενα από το πληροφοριακό σύστημα διαχείρισης επιχειρησιακών πόρων
	Extensible Stylesheet Language (XSL) Transformations		Μετασχηματισμό XML εγγράφων ηλεκτρονικής τιμολόγησης
	W3C XML Encryption		Κρυπτογράφηση XML εγγράφων ηλεκτρονικής τιμολόγησης
	W3C XML Digital Signature		Ψηφιακή υπογραφή XML εγγράφων ηλεκτρονικής τιμολόγησης
	XML Advanced Electronic Signature (XAdES)	XAdES Basic Electronic Signature (XAdES-BES)	Προηγμένη ψηφιακή υπογραφή XML εγγράφων ηλεκτρονικής τιμολόγησης
		XAdES with Complete validation data (XAdES-C)	
		XAdES Explicit Policy based Electronic Signature (XAdES-EPES)	
		XAdES with Time-Stamp (XAdES-T)	
		XML Advanced Electronic Signature with eXtended validation data (XAdES-X)	
	Simple Object Access Protocol (SOAP)		Μηχανισμός ανταλλαγής ηλεκτρονικών τιμολογίων
	WS-Security Mechanisms		Μηχανισμοί ασφάλειας για τη μεταφορά ηλεκτρονικών τιμολογίων
	Web Services Description Language (WSDL)		Μηχανισμός περιγραφής της SELIS υπηρεσίας η-τιμολόγησης

Πίνακας 1. Πρότυπα SELIS η-τιμολόγησης

Η υπηρεσία βασίζεται κατά κύριο λόγο στις τεχνολογίες της XML και των Υπηρεσιών Ιστού. Πιο συγκεκριμένα, χρησιμοποιεί την XML για τη μορφοποίηση των εγγράφων των ηλεκτρονικών τιμολογίων ενώ επίσης κάνει χρήση XML ψηφιακών υπογραφών και χρονοσφραγίδων σε αυτά. Το σχήμα που υιοθετείται για το έγγραφο ηλεκτρονικού τιμολογίου είναι ένα υποσύνολο της XML Common Business

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Library, version 4.0 (xCBL 4.0), η οποία καλύπτει όλους τους υποχρεωτικούς τομείς που καθορίζονται στην οδηγία 2001/115/EC. Η αρχιτεκτονική SELIS συνδέεται με ένα λογιστικό πακέτο λογισμικού που προσφέρεται από την Exact [Exact] (το Exact ERP) υποστηρίζοντας ταυτόχρονα και το σχήμα XML το οποίο υποστηρίζεται από το συγκεκριμένο πακέτο. Επίσης χρησιμοποιεί την Extensible Stylesheet Language Transformation (XSLT) για τον μετασχηματισμό μεταξύ διαφορετιών τύπων εγγράφων XML.

Ο υποστηριζόμενος μηχανισμός ανταλλαγής για τα ηλεκτρονικά τιμολόγια στηρίζεται στο Simple Object Access Protocol (SOAP) χρησιμοποιώντας και τις επεκτάσεις ασφάλειας των υπηρεσιών Ιστού ενώ η περιγραφή των παρεχόμενων υπηρεσιών, διατυπώνεται όπως διευκρινίζεται από τη Web Services Description Language (WSDL). Η αποθήκευση αντιμετωπίζεται με την υιοθέτηση μιας βάσης δεδομένων XML με στόχο την ικανοποίηση της απαίτησης για ασφαλή αποθήκευση των ανταλλαγμένων ηλεκτρονικών τιμολογίων στη μορφή στην οποία αυτά στάλθηκαν και παραλήφθηκαν. Η ακεραιότητα και η μη-άρνηση αποποίησης ευθύνης για τα έγγραφα ηλεκτρονικών τιμολογίων εξασφαλίζονται με την χρήση των ψηφιακών υπογραφών XML έτσι ώστε οι πληροφορίες προέλευσης και ακεραιότητας να ενσωματώνονται στο ηλεκτρονικό τιμολόγιο.

Ο Πίνακας 1 παραθέτει συνοπτικά το σύνολο των προτύπων που υποστηρίζονται από την SELIS η-τιμολόγηση.

3.3.1.1.1.3 Βήμα 4: Ενσωμάτωση των Συστατικών Ελέγχου

Στο τελευταίο βήμα (4^{ο} βήμα) του καθορισμού ενός ΣυΕ απαιτείται να γίνει η ενσωμάτωση των δύο συστατικών ελέγχου. Επομένως, στην SELIS ΥΙυΕ προσαρμόζονται τα δυο πρόσθετα συστατικά όπως αυτά καθορίστηκαν στο Κεφάλαιο 2.3.4.1, ο *Εκτελεστής Περιπτώσεων Ελέγχου* και η *Μηχανή Αναφορών*.

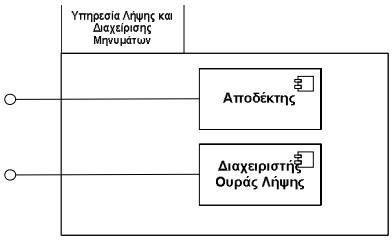
Στις παραγράφους που ακολουθούν θα πραγματοποιηθεί η παρουσίαση της δομής των συστατικών αυτών.

3.3.1.1.1.3.1 Δομή SELIS Εκτελεστή Περιπτώσεων Ελέγχου

Ο Εκτελεστής Περιπτώσεων Ελέγχου αποτελείται από δύο δομικά στοιχεία: την *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* και την *Υπηρεσία Διαχείρισης και Συντονισμού* (βλ. § 2.3.4.1.2), τα οποία απαρτίζονται από ένα σύνολο από λογικά και λειτουργικά στοιχεία τα οποία παρουσιάζονται στη συνέχεια.

3.3.1.1.1.3.1.1 Υπηρεσία λήψης και διαχείρισης μηνυμάτων

Η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* αποτελείται από στοιχεία που αναγνωρίζουν το πλαίσιο μεταφοράς ενός μηνύματος λαμβάνοντας τα και αποδομώντας τα μηνύματα SOAP. Η πληροφορία η οποία εξάγεται από τα μηνύματα είναι οι εκτελέσιμες περιπτώσεις και τα πιθανά δεδομένα ελέγχου.



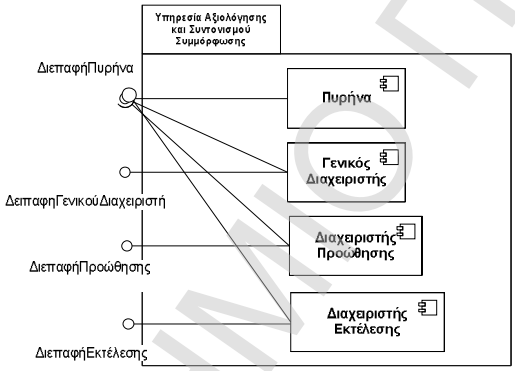
Σχήμα 45: Στοιχεία Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Το διάγραμμα δομικών στοιχείων του Σχήμα 45 παρουσιάζει τα δύο στοιχεία που αποτελούν την υπηρεσία, τον *Αποδέκτη (Receiver)* και τον *Διαχειριστή της Ουράς Λήψης (Receiving Queue Manager)*:
Ο *Αποδέκτης* λαμβάνει τα μηνύματα που προορίζονται για το ΣυΕ και τα αποθηκεύει στην ουρά λήψης χρησιμοποιώντας τον *Διαχειριστή της Ουράς Λήψης*. Επιπλέον αναλαμβάνει να ανακτά κάθε φορά ένα μήνυμα που έχει αποθηκευτεί στην ουρά λήψης και να το αποδομεί εξάγοντας το περιεχόμενό του.
Η πρόσβαση στα δύο στοιχεία γίνεται μέσω κατάλληλων διεπαφών που καθορίζονται και υλοποιούνται στις φάσεις 3 και 4 της μεθοδολογίας.

3.3.1.1.1.3.1.2 Υπηρεσία διαχείρισης και συντονισμού

Η *Υπηρεσία Διαχείρισης και Συντονισμού*, όπως φαίνεται στο Σχήμα 46, αποτελείται από τέσσερα στοιχεία: τον *Πυρήνα (Kernel)*, το *Γενικό Διαχειριστή (AdminManager)*, τον *Διαχειριστή Προώθησης (ForwardManager)* και τον *Διαχειριστή Εκτέλεσης (ExecutorManager)*.



Σχήμα 46: Στοιχεία Υπηρεσία Διαχείρισης και Συντονισμού

Ο *Πυρήνας* επιτελεί τις βασικές λειτουργίες δημιουργίας και διαγραφής συνόδων υπηρεσιών, την εγκατάσταση και απεγκατάσταση υπηρεσιών και την λήψη πληροφοριών για συνόδους και υπηρεσίες. Ο *Γενικός Διαχειριστής* χρησιμοποιεί τον πυρήνα για την εποπτεία ορισμένων από τις λειτουργίες του. Οι δραστηριότητες που αναλαμβάνει περιέχουν την παράθεση των ενεργών συνόδων, την ρύθμισή τους, την εγκατάσταση νέων και την απεγκατάσταση υπαρχουσών υπηρεσιών και την φόρτωση αρχείων διαμόρφωσης. Ο *Διαχειριστής Προωθήσεων* λειτουργεί βοηθητικά για την προώθηση μηνυμάτων ή αντικειμένων εντός του ΣυΕ, όπου αυτό είναι απαραίτητο. Τέλος ο *Διαχειριστή Εκτέλεσης* εκτελεί τις διαδικασίες των περιπτώσεων ελέγχου συντονίζοντας τις αναγκαίες υπηρεσίες της ΥΙυΕ που πρέπει να αλληλεπιδράσουν για την ολοκλήρωση του αντίστοιχου ελέγχου και συλλέγει τα παραγόμενα δεδομένα αξιολόγησης. Το στοιχείο που πρέπει να επισημανθεί είναι το γεγονός ότι οι διαδικασίες των περιπτώσεων ελέγχου που τελικά θα χρησιμοποιηθούν καθορίζονται και ενσωματώνονται στα αντίστοιχα στάδια των φάσεων 3 και 4 της προτεινόμενης μεθοδολογίας.
Οι διεπαφές που υλοποιούνται αποτελούνται από την `Διεπαφή Πυρήνα (KernelInterface)`, την `Διεπαφή Γενικού Διαχειριστή (AdminManagerInterface)`, την `Διεπαφή Προώθησης (ForwardInterface)` και την `Διεπαφή Εκτέλεσης (ExecutorInterface)`. Η `Διεπαφή Πυρήνα` όπως φαίνεται χρησιμοποιείται από τον *Γενικό Διαχειριστή*, τον *Διαχειριστή Προωθήσεων* και τον *Διαχειριστή Εκτέλεσης*.

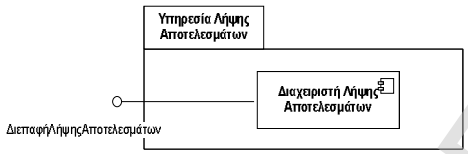
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.3.1.1.1.3.2 Δομή Μηχανής Αναφορών SELIS

Η Μηχανή Αναφορών αποτελείται από δύο δομικά στοιχεία: την *Υπηρεσία Λήψης Αποτελεσμάτων* και την *Υπηρεσία Διαχείρισης Αποτελεσμάτων* (βλ. § 2.3.4.1.3). Καθένα από τα στοιχεία αυτά αποτελείται από ένα σύνολο από λογικά και λειτουργικά στοιχεία όπως αυτά περιγράφονται στις παραγράφους που ακολουθούν.

3.3.1.1.1.3.2.1 Υπηρεσία λήψης αποτελεσμάτων

Η *Υπηρεσία Λήψης Αποτελεσμάτων* όπως φαίνεται στο Σχήμα 47, περιλαμβάνει τον *Διαχειριστή Λήψης Αποτελεσμάτων (Result Manager)*.

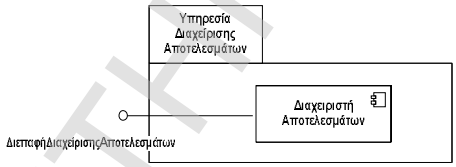


Σχήμα 47: Στοιχεία Υπηρεσίας Λήψης Αποτελεσμάτων

Ο *Διαχειριστής Λήψης Αποτελεσμάτων* αναλαμβάνει αποκλειστικά τη συλλογή του συνόλου των αποτελεσμάτων από τον Εκτελεστή Περιπτώσεων Ελέγχου.
Η διεπαφή η οποία υλοποιείται είναι η *Διεπαφή Λήψης Αποτελεσμάτων (ReceiveResultInterface)*.

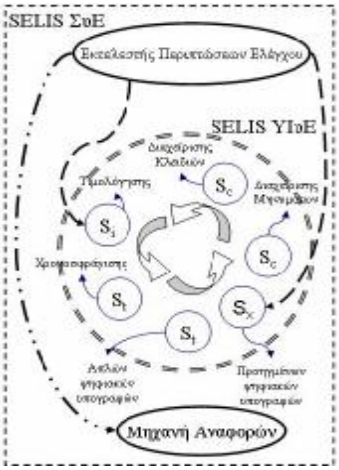
3.3.1.1.1.3.2.2 Υπηρεσία διαχείρισης αποτελεσμάτων

Η *Υπηρεσία Διαχείρισης Αποτελεσμάτων* (Σχήμα 48) αποτελείται από τον *Διαχειριστή Αποτελεσμάτων (Result Manager)*.



Σχήμα 48: Στοιχεία Υπηρεσίας Διαχείρισης Αποτελεσμάτων

Ο *Διαχειριστής Αποτελεσμάτων* αναλαμβάνει τη σύνθεση των αποτελεσμάτων στην απαιτούμενη μορφή και την ενσωμάτωσή τους σε αρχεία αναφορών (log files).
Η διεπαφή η οποία υλοποιείται είναι η `Διεπαφή Διαχείρισης Αποτελεσμάτων (ManagerResultInterface)`.



Σχήμα 49. ΣυΕ SELIS η-τιμολόγηση

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.3.1.1.2 ΣυΕ SELIS η-τιμολόγηση

Στο Σχήμα 49 παρουσιάζεται η δομή του ΣυΕ SELIS η-τιμολόγησης, όπως αυτή προέκυψε από την εκτέλεση των τεσσάρων βημάτων που απαιτούνται για τον καθορισμό ενός ΣυΕ. Το ΣυΕ SELIS η-τιμολόγησης θα μετάσχει στους ελέγχους συμμόρφωσης και διαλειτουργικότητας της $3^{η}$ και $4^{η}$ φάσης της προτεινόμενης μεθοδολογίας .

3.3.1.1.3 SWEB η-τιμολόγηση

Η διαδικασία η οποία λαμβάνει χώρα είναι πανομοιότυπη με αυτήν που ολοκληρώθηκε στην περίπτωση της SELIS η-τιμολόγησης και παρουσιάστηκε στο Κεφάλαιο 3.3.1.1.1.

ΣυΕ	**Πρότυπα/Προδιαγραφές**		**Σκοπός**
SWEB η-τιμολόγηση	XML common business library version 4.0 (xCBL 4.0)		SWEB XML έγγραφα ηλεκτρονικής τιμολόγησης
	Σχήμα που υποστηρίζεται από το SAP ERP [SAP]		Έγγραφα ηλεκτρονικής τιμολόγησης υποστηριζόμενα από το πληροφοριακό σύστημα διαχείρισης επιχειρησιακών πόρων
	Extensible Stylesheet Language (XSL) Transformations		Μετασχηματισμό XML εγγράφων ηλεκτρονικής τιμολόγησης
	W3C XML Encryption		Κρυπτογράφηση XML εγγράφων ηλεκτρονικής τιμολόγησης
	W3C XML Digital Signature		Ψηφιακή υπογραφή XML εγγράφων ηλεκτρονικής τιμολόγησης
	XML Advanced Electronic Signature (XAdES)	XAdES Basic Electronic Signature (XAdES-BES)	Προηγμένη ψηφιακή υπογραφή XML εγγράφων ηλεκτρονικής τιμολόγησης
		XAdES with Complete validation data (XAdES-C)	
		XAdES Explicit Policy based Electronic Signature (XAdES-EPES)	
		XAdES with Time-Stamp (XAdES-T)	
		XML Advanced Electronic Signature with eXtended validation data (XAdES-X)	
	Simple Object Access Protocol (SOAP)		Μηχανισμός ανταλλαγής ηλεκτρονικών τιμολογίων
	WS-Security Mechanisms		Μηχανισμοί ασφάλειας για τη μεταφορά ηλεκτρονικών τιμολογίων
	Web Services Description Language (WSDL)		Μηχανισμός περιγραφής της SWEB υπηρεσίας η-τιμολόγησης

Πίνακας 2. Πρότυπα SWEB η-τιμολόγησης

Στον Πίνακας 2 γίνεται παράθεση των προτύπων από τα οποία απαρτίζεται η SWEB η-τιμολόγηση όπως αυτό απαιτείται στο $3^{ο}$ βήμα του καθορισμού ενός ΣυΕ.

3.3.1.2 Δομή Υποδομής Διαχείρισης Ελέγχου (ΥΔΕ)

Η λογική και οργανωτική δομή της ΥΔΕ παραμένει αναλλοίωτη ανεξάρτητα από τη φύση της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης. Αντίθετα, από

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

τεχνολογική άποψης υιοθετεί και ενσωματώνει εργαλεία και βιβλιοθήκες ελέγχου λαμβάνοντας υπόψη τα πρότυπα και τις προδιαγραφές που υποστηρίζουν τα ΣυΕ.
Όπως έχει αναφερθεί στο Κεφάλαιο 2.3.4.2 η ΥΔΕ αποτελείται από τα ακόλουθα τρία στρώματα:

- Στρώμα Ελέγχου.
- Στρώμα Συμμόρφωσης.
- Στρώμα Διαλειτουργικότητας.

Η δομής της ΥΔΕ με την μορφή με την οποία μετέχει στους ελέγχους συμμόρφωσης και διαλειτουργικότητας των ΣυΕ είναι αυτή που απεικονίζεται στο Σχήμα 12, ενώ στις επόμενες παραγράφους παρουσιάζεται η δομή των επιμέρους στρωμάτων.

3.3.1.2.1 Δομή Στρώματος Ελέγχου

Το στρώμα ελέγχου αποτελείται από τα συστατικά και τα δομικά στοιχεία που παρουσιάζονται στον Πίνακας 3 (βλ. § 2.3.4.2.1).

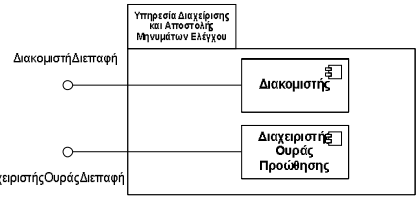
Στρώμα Ελέγχου	
Συστατικά	*Δομικά Στοιχεία*
Συντονιστής Ελέγχου	Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου
	Υπηρεσία Συντονισμού Ελέγχου
	Υπηρεσίες Διαχείρισης Αποθετηρίων
	Αποθετήριο Δεδομένων Ελέγχου

Πίνακας 3. Συστατικά & Δομικά Στοιχεία Στρώματος Ελέγχου

Καθένα από τα δομικά στοιχεία συνίσταται από συγκεκριμένα λογικά και λειτουργικά στοιχεία τα οποία παρουσιάζονται στις παραγράφους που ακολουθούν.

3.3.1.2.1.1 Υπηρεσία διαχείρισης και αποστολής μηνυμάτων ελέγχου

Η *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου* αποτελείται από στοιχεία που αναγνωρίζουν το πλαίσιο μεταφοράς ενός μηνύματος και δημιουργούν τους κατάλληλους «φακέλους» SOAP προκειμένου να τα αποστείλουν στα αντίστοιχα ΣυΕ.
Το ακόλουθο διάγραμμα δομικών στοιχείων επιδεικνύει τα δύο στοιχεία που αποτελούν την υπηρεσία, τον *Διακομιστή (Forwarder)* και τον *Διαχειριστή της Ουράς Προώθησης (Forwarding Queue Manager)*.



Σχήμα 50: Στοιχεία Υπηρεσίας Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου

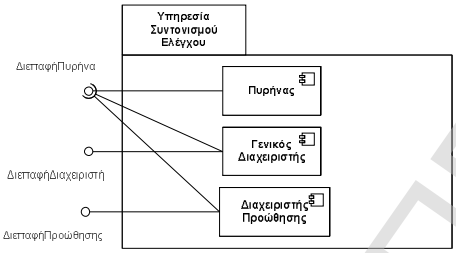
Ο *Διακομιστής* αναλαμβάνει να ανακτά κάθε φορά ένα μήνυμα που έχει αποθηκευτεί στην ουρά προώθησης, να φτιάχνει τον απαραίτητο μήνυμα που το περιέχει και να το αποστέλλει στον παραλήπτη του. Ο *Διαχειριστής της Ουράς Προώθησης* δέχεται τα μηνύματα που πρόκειται να προωθηθούν, καθορίζει το πλαίσιο προώθησης κάθε μηνύματος και τα αποθηκεύει στην ουρά.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η πρόσβαση στα δύο στοιχεία γίνεται μέσω των αντίστοιχων διεπαφών Διακομιστή Διεπαφή (ForwardInterface) και Διαχειριστής Ουράς Διεπαφή (QueueManagerInterface).

3.3.1.2.1.2 Υπηρεσία συντονισμού ελέγχου

Η *Υπηρεσία Συντονισμού Ελέγχου* αποτελεί μια από τις σημαντικότερες υπηρεσίες του στρώματος ελέγχου. Όπως φαίνεται στο Σχήμα 51, αποτελείται από τρία στοιχεία: τον *Πυρήνα (Kernel)*, τον *Γενικό Διαχειριστή (AdminManager)* και τον *Διαχειριστή Προώθησης (ForwardManager)*.

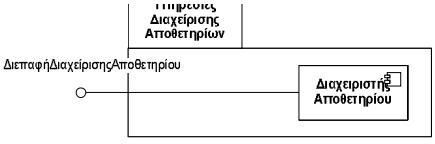


Σχήμα 51: Στοιχεία Υπηρεσίας Συντονισμού Ελέγχου

Ο *Πυρήνας* επιτελεί τις βασικές λειτουργίες δημιουργίας και διαγραφής συνόδων υπηρεσιών, την εγκατάσταση και απεγκατάσταση υπηρεσιών και την λήψη πληροφοριών για συνόδους και υπηρεσίες. Ο *Γενικός Διαχειριστής* χρησιμοποιεί τον πυρήνα για την εποπτεία ορισμένων από τις λειτουργίες του. Οι δραστηριότητες που αναλαμβάνει περιέχουν την παράθεση των ενεργών συνόδων, την ρύθμισή τους, την εγκατάσταση νέων και την απεγκατάσταση υπαρχουσών υπηρεσιών και την φόρτωση αρχείων διαμόρφωσης. Ο *Διαχειριστής Προωθήσεων* λειτουργεί βοηθητικά για την προώθηση μηνυμάτων ή αντικειμένων εντός της ΥΔΕ, όπου αυτό είναι απαραίτητο (σε αντίθεση με την *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου* που ακολουθεί και προωθεί μηνύματα εκτός της ΥΔΕ).
Οι διεπαφές που υλοποιούνται αποτελούνται από την *ΔιεπαφήΠυρήνα (KernelInterface)*, την *ΔιεπαφήΔιαχειριστή (AdminManagerInterface)* και την *ΔιεπαφήΠροώθησης (ForwardInterface)*. Η Διεπαφή Πυρήνα όπως φαίνεται χρησιμοποιείται από τον *Γενικό Διαχειριστή και τον Διαχειριστή Προωθήσεων*.

3.3.1.2.1.3 Υπηρεσίες διαχείρισης αποθετηρίων

Μια *Υπηρεσία Διαχείρισης Αποθετηρίων* είναι υπεύθυνη για την εισαγωγή και εξαγωγή εγγράφων και πληροφορίας από ένα αποθετήριο. Το βασικό δομικό στοιχείο της είναι ο *Διαχειριστής Αποθετηρίου (Repository Manager)* όπως φαίνεται στο Σχήμα 52.



Σχήμα 52: Στοιχείο Υπηρεσίας Διαχείρισης Αποθετηρίων

Ο *Διαχειριστής Αποθετηρίου* υλοποιεί την *Διεπαφή Διαχείρισης Αποθετηρίου (repository manager interface)*, η οποία είναι διαθέσιμη σε άλλες υπηρεσίες που θέλουν να εισάγουν ή να εξάγουν κάποιο έγγραφο από το αποθετήριο, ή να κάνουν μια *ερώτηση (query)* για την λήψη πληροφοριών βάσει των ήδη υπαρχόντων εγγράφων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.3.1.2.1.4 Αποθετήριο δεδομένων ελέγχου

Το *Αποθετήριο Περιπτώσεων και Δεδομένων Ελέγχου* αποτελείται από μια βάση δεδομένων στην οποία αποθηκεύονται αλλά και ανακτώνται οι περιπτώσεις ελέγχου οι οποίες θα εκτελεστούν κατά τη διάρκεια των ελέγχων αλλά και τα δεδομένα ελέγχου που ενδέχεται να απαιτούνται από αυτές. Η χρησιμοποίηση της eXist [Meier02] ως μια εγγενής βάση δεδομένων XML αποτελεί μια επιλογή που επιτρέπει την αποθήκευση δεδομένων ελέγχου σε μορφή XML.

3.3.1.2.2 Δομή Στρώματος Συμμόρφωσης

Το στρώμα συμμόρφωσης αποτελείται από τα συστατικά και τα δομικά στοιχεία που παρουσιάζονται στον Πίνακας 4 (βλ. § 2.3.4.2.2).

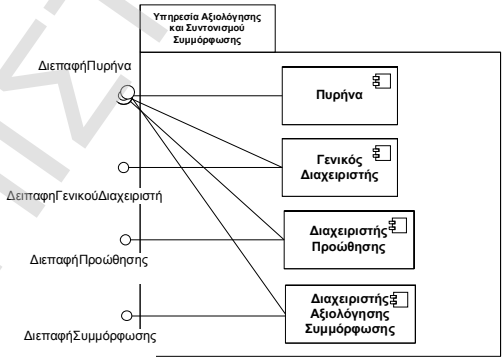
Στρώμα Συμμόρφωσης	
Συστατικά	*Δομικά Στοιχεία*
Ελεγκτής Συμμόρφωσης	Υπηρεσία Συντονισμού Συμμόρφωσης
	Ελεγκτής Αξιολόγησης

Πίνακας 4. Συστατικά & Δομικά Στοιχεία Στρώματος Συμμόρφωσης

Στις παραγράφους που ακολουθούν παρουσιάζονται στο σύνολό τους τα στοιχεία αυτά.

3.3.1.2.2.1 Υπηρεσία αξιολόγησης και συντονισμού συμμόρφωσης

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Συμμόρφωσης* αποτελεί μία από τις σημαντικότερες υπηρεσίες του στρώματος συμμόρφωσης. Όπως φαίνεται στο Σχήμα 53, αποτελείται από τέσσερα στοιχεία: τον *Πυρήνα (Kernel)*, τον *Γενικό Διαχειριστή (AdminManager)*, τον *Διαχειριστή Προώθησης (ForwardManager)* και τον *Διαχειριστή Αξιολόγησης Συμμόρφωσης (EvaluatorConformanceManager)*.



Σχήμα 53: Στοιχεία Υπηρεσίας Συντονισμού Ελέγχου

Ο *Πυρήνας* επιτελεί τις βασικές λειτουργίες δημιουργίας και διαγραφής συνόδων υπηρεσιών, την εγκατάσταση και απεγκατάσταση υπηρεσιών και την λήψη πληροφοριών για συνόδους και υπηρεσίες. Ο *Γενικός Διαχειριστής* χρησιμοποιεί τον πυρήνα για την εποπτεία ορισμένων από τις λειτουργίες του. Οι δραστηριότητες που αναλαμβάνει περιέχουν την παράθεση των ενεργών συνόδων, την ρύθμισή τους, την εγκατάσταση νέων και την απεγκατάσταση υπαρχουσών υπηρεσιών και την φόρτωση αρχείων διαμόρφωσης. Ο *Διαχειριστής Προωθήσεων* λειτουργεί βοηθητικά για την προώθηση μηνυμάτων ή αντικειμένων εντός της ΥΔΕ, όπου αυτό είναι απαραίτητο. Τέλος ο *Διαχειριστής Αξιολόγησης Συμμόρφωσης* λαμβάνει σαν είσοδο τα αρχεία

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

αναφορών που παράγονται από τα ΣυΕ και καθορίζει τα εργαλεία του Ελεγκτή Αξιολόγησης τα οποία πρέπει να χρησιμοποιηθούν, ενώ παράλληλα συγκεντρώνει και καταγράφει τα αποτελέσματα της αξιολόγησης.
Οι διεπαφές που υλοποιούνται αποτελούνται από την *Διεπαφή Πυρήνα (KernelInterface)*, την *Διεπαφή Γενικού Διαχειριστή (AdminManagerInterface)*, την *Διεπαφή Προώθησης (ForwardInterface)* και την *Διεπαφή Συμμόρφωσης (ConformInterface)*. Η Διεπαφή Πυρήνα όπως φαίνεται χρησιμοποιείται από τον *Γενικό Διαχειριστή*, τον *Διαχειριστή Προωθήσεων* και τον *Διαχειριστή Αξιολόγησης* Συμμόρφωσης.

Βήμα 1: Κατηγοριοποίηση χρησιμοποιούμενων προτύπων		**Βήμα 2: Καταγραφή των απαιτούμενων εργαλείων**	**Βήμα 3: Αναζήτηση και συλλογή υπαρχόντων εργαλείων**	**Βήμα 4: Επιλογή και ενσωμάτωση των μηχανισμών**
Πρότυπα	*Κατηγορίες*			
XML common business library version 4.0 (xCBL 4.0)	Διαχείριση Εγγράφων & Μετασχηματισμού	Εργαλεία ελέγχου συμμόρφωσης εγγράφων ως προς τα αντίστοιχα σχήματα	Altova XMLSpy [Altova]	Altova XMLSpy
XML σχήμα που υποστηρίζεται από το Exact ERP				
Extensible Stylesheet Language (XSL) Transformations				
W3C XML Encryption	Ασφάλεια Εγγράφων	Εργαλεία και ιστοχώροι επαλήθευσης και εφαρμογής XML ψηφιακών υπογραφών, προηγμένων XML ψηφιακών υπογραφών και κρυπτογράφησης	IBM XML security suite [IBM]	IAIK XML signature library
			IAIK XML signature library [IAIK]	
W3C XML Digital Signature			Apache XML security [Apache]	
			Microsoft .Net security library tools [Microsoft]	IAIK XAdES toolkit
			Online XML Digital Signature Verifier [OnlineVer]	
XML Advanced Electronic Signature (XAdES)			IAIK XAdES toolkit [IAIKXAdES]	
Simple Object Access Protocol (SOAP)	Διαχείριση Μηνυμάτων & Ασφάλειας	Εργαλεία και οδηγίες ελέγχου συμμόρφωσης των προτύπων των Υπηρεσιών Ιστού με αντίστοιχα πρότυπα	WS-I (Web Services Interoperability) standardization organization testing tools [Ehnebuske03]	WS-I (Web Services Interoperability) standardization organization testing tools
WS-Security Mechanisms			WS-I profiles (Basic Profile, Attachments Profile and Simple SOAP Binding Profile, and Basic Security Profile)	WS-I profiles (Basic Profile, Attachments Profile and Simple SOAP Binding Profile, and Basic Security Profile)
Web Services Description Language (WSDL)				

Πίνακας 5. Βήματα ολοκλήρωσης του Ελεγκτή Αξιολόγησης

3.3.1.2.2.2 Ελεγκτής Αξιολόγησης

Ο Ελεγκτής Αξιολόγησης αποτελείται από ένα σύνολο εργαλείων και βιβλιοθηκών ελέγχου τα οποία ουσιαστικά αξιολογούν την συμμόρφωση των δεδομένων που

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

παράγονται από την εκτέλεση των περιπτώσεων ελέγχου στην 3η φάση της μεθοδολογίας έναντι των αντίστοιχων προτύπων. Για τον προσδιορισμό της δομής του Ελεγκτή Αξιολόγησης θα πρέπει να ακολουθηθούν τα βήματα που καθορίστηκαν στο Κεφάλαιο 2.3.4.2.2. Η εκτέλεση των βημάτων αυτών παρουσιάζεται στον Πίνακας 5.

3.3.1.2.3 Δομή Στρώματος Διαλειτουργικότητας

Το στρώμα διαλειτουργικότητας αποτελείται από τα συστατικά και τα δομικά στοιχεία που παρουσιάζονται στον Πίνακας 6 (βλ. § 2.3.4.2.3).

Στρώμα Διαλειτουργικότητας	
Συστατικά	*Δομικά Στοιχεία*
Διαχειριστής Μηνυμάτων	Υπηρεσία Διαχείρισης Μηνυμάτων
	Υπηρεσία Ανάλυσης Μηνυμάτων
Ελεγκτής Διαλειτουργικότητας	Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας

Πίνακας 6. Συστατικά & Δομικά Στοιχεία του Στρώματος Διαλειτουργικότητας

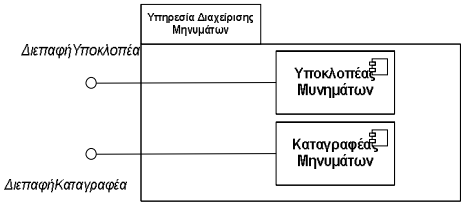
Στις ακόλουθες παραγράφους παρατίθενται τα αντίστοιχα λογικά και λειτουργικά στοιχεία.

3.3.1.2.3.1 Διαχειριστής Μηνυμάτων

Ο Διαχειριστής Μηνυμάτων στην περίπτωση του ελέγχου των δύο ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολογήσης, για να αποδώσει την λειτουργικότητα των δύο δομικών στοιχείων από τα οποία απαρτίζεται, ήτοι *Υπηρεσίας Διαχείρισης Μηνυμάτων* και της *Υπηρεσίας Ανάλυσης Μηνυμάτων*, υιοθετεί τα εργαλεία ελέγχου τα οποία προσφέρονται από τον Οργανισμό WS-I [Brittenham]. Στις παραγράφους που ακολουθούν παρατίθεται η αντιστοίχιση η οποία πραγματοποιήθηκε ανάμεσα στα εργαλεία και στα δομικά στοιχεία του Διαχειριστή Μηνυμάτων.

3.3.1.2.3.1.1 Υπηρεσία διαχείρισης μηνυμάτων

Για να καλυφθεί η λειτουργικότητα της Υπηρεσίας Διαχείρισης Μηνυμάτων χρησιμοποιήθηκε το εργαλείο ‘Σύστημα Ελέγχου’ (Monitor) το οποίο προσφέρεται από τον Οργανισμό WS-I [Brittenham05a]. Το εργαλείο αυτό αποτελείται από δύο στοιχεία, τον *Υποκλοπέα Μηνυμάτων (Message Interceptor)* και τον *Καταγραφέα Μηνυμάτων (Message Logger)*, όπως απεικονίζεται στο Σχήμα 54.



Σχήμα 54: Στοιχεία Υπηρεσίας Διαχείρισης Μηνυμάτων

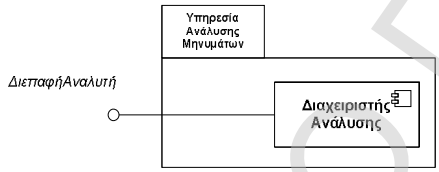
Ο *Υποκλοπέας Μηνυμάτων* ‘υποκλέπτει’ τα ανταλλασσόμενα μεταξύ των ΣυΕ μηνύματα, λειτουργώντας ουσιαστικά σαν μια ενδιάμεση οντότητα η οποία λαμβάνει και στην συνέχεια προωθεί ένα μήνυμα στον παραλήπτη του. Ο Καταγραφέας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Μηνυμάτων καταγράφει τα μηνύματα αυτά σε μια μορφή που επιτρέπει την περαιτέρω ανάλυσή τους. Οι λειτουργίες και των δύο στοιχείων ρυθμίζονται από ένα αρχείο διαμόρφωσης το οποίο καθορίζει τη σχέση μεταξύ των θυρών τις οποίες ο Υποκλοπέας Μηνυμάτων πρέπει να ακούει ώστε να λάβει τα εισερχόμενα μηνύματα, της διεύθυνσης του παραλήπτη στον οποίο τα μηνύματα αυτά πρέπει να προωθηθούν και της διεύθυνσης του αρχείου στο οποίο τα μηνύματα πρέπει να καταγραφούν από τον Καταγραφέα Μηνυμάτων.
Οι διεπαφές που υλοποιούνται αποτελούνται από την `Διεπαφή Υποκλοπέα (InterceptorInterface)` και την `Διεπαφή Καταγραφέα (LoggerInterface)`.

3.3.1.2.3.1.2 Υπηρεσία ανάλυσης μηνυμάτων

Για να καλυφθεί η λειτουργικότητα της *Υπηρεσίας Ανάλυσης Μηνυμάτων* χρησιμοποιήθηκε το εργαλείο 'Αναλυτής' (Analyzer) [Brittenham05b]. Το βασικό του στοιχείο είναι ο *Διαχειριστής Ανάλυσης (AnalyzerManager)* (Σχήμα 55).



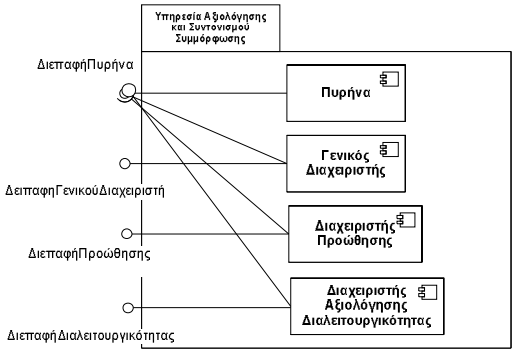
Σχήμα 55: Στοιχεία Υπηρεσίας Ανάλυσης Μηνυμάτων

Ο *Διαχειριστής Ανάλυσης* δέχεται ως είσοδο τα μηνύματα που έχουν ληφθεί από την Υπηρεσία Διαχείρισης Μηνυμάτων και τα αναλύει με στόχο να τα συσχετίσει με την περιγραφή της ΥΙ όπως αυτή έχει παραχθεί από το αντίστοιχο ΣυΕ. Τα αποτελέσματα της ανάλυσης καταγράφονται τελικώς σε μια αναφορά. Οι λειτουργίες που επιτελούνται ρυθμίζονται από ένα αρχείο διαμόρφωσης το οποίο περιέχει όλες τις απαιτούμενες πληροφορίες.
Ο *Διαχειριστής Ανάλυσης* υλοποιεί την `Διεπαφή Αναλυτή (AnalyzerInterface)`.

3.3.1.2.3.2 Δομή Ελεγκτή Διαλειτουργικότητας

3.3.1.2.3.2.1 Υπηρεσία αξιολόγησης και συντονισμού διαλειτουργικότητας

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας* αποτελεί μια από τις σημαντικότερες υπηρεσίες του στρώματος διαλειτουργικότητας. Όπως φαίνεται στο Σχήμα 56, αποτελείται στο ελάχιστο από τέσσερα στοιχεία: τον *Πυρήνα (Kernel)*, το *Γενικό Διαχειριστή (AdminManager)*, τον *Διαχειριστή Προώθησης (ForwardManager)* και τον *Διαχειριστή Αξιολόγησης Διαλειτουργικότητας (EvaluatorInterManager)*.



Σχήμα 56: Στοιχεία Υπηρεσίας Συντονισμού Ελέγχου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Ο *Πυρήνας* επιτελεί τις βασικές λειτουργίες δημιουργίας και διαγραφής συνόδων υπηρεσιών, την εγκατάσταση και απεγκατάσταση υπηρεσιών και την λήψη πληροφοριών για συνόδους και υπηρεσίες. Ο *Γενικός Διαχειριστής* χρησιμοποιεί τον πυρήνα για την εποπτεία ορισμένων από τις λειτουργίες του. Οι δραστηριότητες που αναλαμβάνει περιέχουν την παράθεση των ενεργών συνόδων, την ρύθμισή τους, την εγκατάσταση νέων και την απεγκατάσταση υπαρχουσών υπηρεσιών καθώς και την φόρτωση αρχείων διαμόρφωσης. Ο *Διαχειριστής Προωθήσεων* λειτουργεί βοηθητικά για την προώθηση μηνυμάτων ή αντικειμένων εντός της ΥΔΕ, όπου αυτό είναι απαραίτητο. Τέλος ο *Διαχειριστής Αξιολόγησης Διαλειτουργικότητας* φέρει την ευθύνη της ανάκτησης των δεδομένων αξιολόγησης και της εκτέλεσης των απαιτούμενων ελέγχων για την εκτίμηση της δυνατότητας επικοινωνίας των ΣυΕ. Οι έλεγχοι συνοψίζονται στους ακόλουθους:

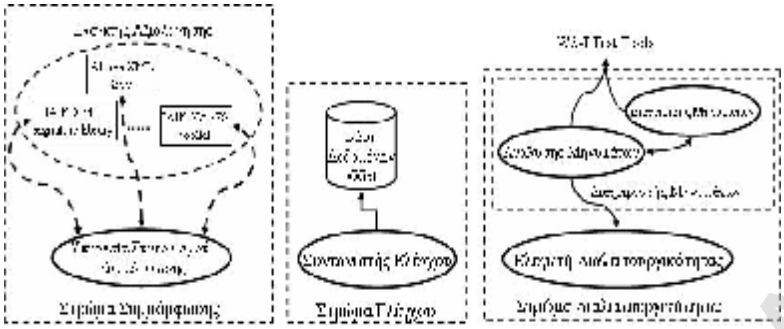
- αναλαμβάνει να ελέγξει ότι τα ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης, έχουν στην κατοχή τους τα ίδια έγγραφα (ηλεκτρονικό τιμολόγιο και επιβεβαίωση) και ότι οι εφαρμοζόμενοι μηχανισμοί ασφάλειας και οι αντίστοιχοι της επικύρωσης έχουν ολοκληρωθεί επιτυχώς και από τα δύο μέρη.
- πιστοποιεί ότι τα δύο ΣυΕ έχουν ολοκληρώσει τη διαδικασία αποστολής, λήψης αλλά και εφαρμογής και πιστοποίησης των μηχανισμών ασφάλειας με ορθό τρόπο.
- λαμβάνει από την *Υπηρεσία Ανάλυσης Μηνυμάτων του Διαχειριστή Μηνυμάτων* την αναφορά που έχει παραχθεί και αναφέρει αν τα ανταλλασσόμενα μηνύματα συμμορφώνονται με τις περιγραφές των αντίστοιχων Υπηρεσιών Ιστού.
- διαπιστώνει ότι κατά το μετασχηματισμό των ανταλλασσόμενων εγγράφων (ηλεκτρονικό τιμολόγιο) και την απόθεσή τους στα συστήματα (π.χ. βάσεις δεδομένων) που διαθέτουν τα ΣυΕ, δεν έχει εντοπιστεί οποιαδήποτε δυσλειτουργία.

Επιπλέον βασική του αρμοδιότητα αποτελεί και η καταγραφή των αποτελεσμάτων της αξιολόγησης τα οποία προκύπτουν από την εκτέλεση των ανωτέρω ελέγχων.
Οι διεπαφές που υλοποιούνται αποτελούνται από την *Διεπαφή Πυρήνα* `(KernelInterface)`, την *Διεπαφή Γενικού Διαχειριστή* `(AdminManagerInterface)`, την *Διεπαφή Προώθησης* `(ForwardInterface)` και την *Διεπαφή Διαλειτουργικότητας* `(InteroperabilityInterface)`. Η *Διεπαφή Πυρήνα* όπως φαίνεται χρησιμοποιείται από τον *Γενικό Διαχειριστή*, τον *Διαχειριστή Προωθήσεων* και τον *Διαχειριστή Αξιολόγησης Διαλειτουργικότητας*.

3.3.1.2.4 Δομή Στρωμάτων ΥΔΕ

Στο Σχήμα 57 παρουσιάζεται η δομή των τριών στρωμάτων της Υποδομής Διαχείρισης Ελέγχου (ΥΔΕ). Η ΥΔΕ με τη συγκεκριμένη δομή θα μετέχει στους ελέγχους συμμόρφωσης και διαλειτουργικότητας της $3^{η}$ και $4^{η}$ φάσης της προτεινόμενης μεθοδολογίας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 57. Δομή Στρωμάτων ΥΔΕ

3.3.2 3η Φάση ΔΣΥΙ: Έλεγχος Συμμόρφωσης

Με το πέρας τη δεύτερης φάσης έχουν καθοριστεί με ακρίβεια η δομή των εμπλεκόμενων στον έλεγχο οντοτήτων, της ΥΔΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης. Ακολουθώντας, λοιπόν τα βήματα που ορίζει η μεθοδολογία στην παρούσα φάση θα πραγματοποιηθούν οι έλεγχοι συμμόρφωσης των δύο ΣυΕ ως προς τα πρότυπα που έχουν υιοθετήσει και υλοποιούν.

3.3.2.1 Έλεγχος Συμμόρφωσης SELIS η-τιμολόγησης

3.3.2.1.1 Στάδιο 1ο: Καθορισμός Περιπτώσεων Ελέγχου

Ως πρώτο βήμα στο παρόν στάδιο έχει τεθεί ο *Σχεδιασμός* των εφαρμοζόμενων περιπτώσεων ελέγχου (βλ. § 2.3.5.1.1.2). Στο Κεφάλαιο 2.3.5.1.1.3 παρουσιάστηκαν τα τρία υποβήματα τα οποία πρέπει να εκτελεστούν για την ολοκλήρωση του συγκεκριμένου στόχου.

Στην παρούσα φάση θα παρουσιαστεί ενδεικτικά ο σχεδιασμός μίας μόνο περίπτωσης ελέγχου η οποία θα χρησιμοποιηθεί ως υπόδειγμα για τον σχεδιασμό όλων των υπολοίπων. Η περίπτωση ελέγχου η οποία θα χρησιμοποιηθεί αφορά τον *"Έλεγχος συμμόρφωσης της XAdES-X ψηφιακής υπογραφής που εφαρμόζεται σε ένα XML έγγραφο ηλεκτρονικής τιμολόγησης όπως αυτό παράγεται από τη SELIS η-τιμολόγηση"*.

Ακολουθώντας, λοιπόν τα υποβήματα που έχουν οριστεί για το σχεδιασμό περιπτώσεων ελέγχου έχουμε τα ακόλουθα:

1 υποβήμα. Πρότυπο υπό εξέταση

Το υπό εξέταση πρότυπο είναι το *XAdES-X*.

2 υποβήμα. Ορισμός περίπτωσης ελέγχου

Ο Πίνακας 7 περιγράφει την περίπτωση ελέγχου συμμόρφωσης που πρέπει να διαμορφωθεί με βάση τον ορισμό που δόθηκε στο Κεφάλαιο 2.3.5.1.1.3 ώστε να εξεταστεί η συμμόρφωση της SELIS απέναντι στο εξεταζόμενο πρότυπο.

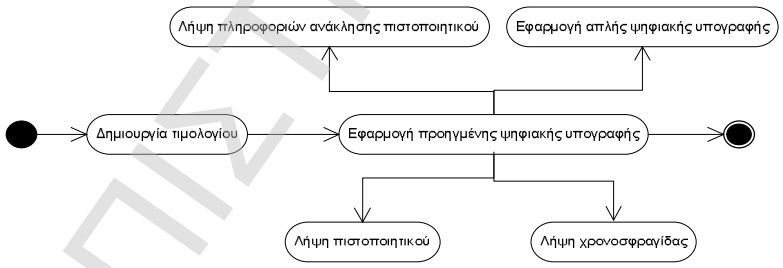
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Ορισμός Περιπτώσεως Ελέγχου Συμμόρφωσης ως το πρότυπο XAdES-X			
Ενέργεια$_i$	*Υπηρεσία*$_i$	*Είσοδος*$_i$	*Έξοδος*$_i$
Δημιουργία εγγράφου ηλεκτρονικής τιμολόγησης XML (xCBL)	Υπηρεσία Διαχείρισης Τιμολογίων	Στοιχεία ηλεκτρονικού τιμολογίου (π.χ. ημερομηνία έκδοσης, στοιχεία εκδότη)	έγγραφο ηλεκτρονικής τιμολόγησης XML
Εφαρμογή προηγμένης ψηφιακής υπογραφής	Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών για ηλεκτρονική τιμολόγηση	έγγραφο ηλεκτρονικής τιμολόγησης XML - Πληροφορίες ανάκλησης πιστοποιητικού - Χρονοσφραγίδα	XAdES-X υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης
Λήψη πιστοποιητικού για τη διαδικασία υπογραφής εγγράφου	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης	Πληροφορίες ανάκτησης πιστοποιητικού (π.χ. ψευδώνυμο, κωδικούς πρόσβασης)	Ιδιωτικό κλειδί πιστοποιητικού
Λήψη πληροφοριών ανάκλησης πιστοποιητικού	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης	Στοιχεία πιστοποιητικού	Πληροφορίες ανάκλησης πιστοποιητικού
Υπογραφή εγγράφου με βάση το πρότυπο W3C XML Digital Signature	Μηχανισμός ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση	έγγραφο ηλεκτρονικής τιμολόγησης XML	Υπογεγραμμένο XML έγγραφο ηλεκτρονικής τιμολόγησης (W3C XML Digital Signature)
Λήψη χρονοσφραγίδας	Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση	Σύνοψη υπογεγραμμένου εγγράφου ηλεκτρονικής τιμολόγησης XML	Χρονοσφραγίδα

Πίνακας 7. Ορισμός Περιπτώσεως Ελέγχου Συμμόρφωσης ως το πρότυπο XAdES-X

3 υποβήμα. Απεικόνιση περίπτωσης ελέγχου

Η απεικόνιση της περίπτώσης ελέγχου που εξετάζεται ω υπόδειγμα γίνεται με τη χρήση ενός διαγράμματος ενεργειών (activity graph diagram) (βλ. § 2.3.5.1.1.3). Το διάγραμμα που αναπαριστά τη συγκεκριμένη περίπτωση ελέγχου εμφανίζεται στο Σχήμα 58.



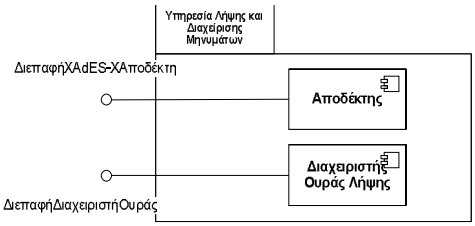
Σχήμα 58. Διάγραμμα Ενεργειών Περιπτώσεως Ελέγχου Συμμόρφωσης ως το πρότυπο XAdES-X

Στο παραπάνω διάγραμμα οι κόμβοι αντιστοιχούν στις ενέργειες που πρέπει να εκτελεστούν για την ολοκλήρωση της περίπτωσης ελέγχου, όπως αυτές περιγράφονται στον Πίνακας 7, ενώ οι ακμές καθορίζουν τη ροή που πρέπει να ακολουθηθεί για την επίτευξη του τελικού στόχου που είναι η παραγωγή των δεδομένων αξιολόγησης που στη συγεκριμένη περίπτωση είναι ένα XML έγγραφο ηλεκτρονικής τιμολόγησης υπογεγραμμένο με βάση το πρότυπο XAdES-X.

Στο επόμενο βήμα του παρόντος σταδίου και από τη στιγμή που έχει ολοκληρωθεί ο σχεδιασμός της εξεταζόμενης περιπτώσεως ελέγχου πραγματοποιείται η παραγωγή της αντίστοιχης διαδικασίας BPEL. Η δημιουργία της διαδικασίας αυτής γίνεται με τη χρήση πλαισίων και μοντέλων [Zheng07, Sinha06, Yuan06, Yan06] τα οποία

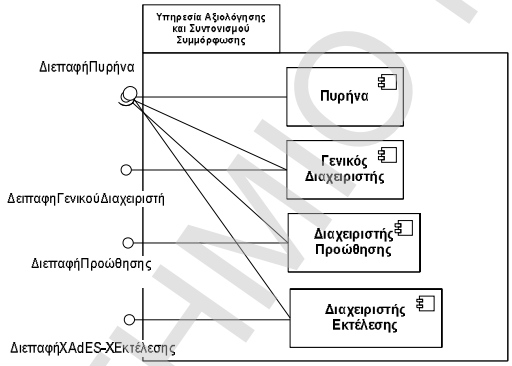
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

επιτρέπουν την αυτοματοποιημένη δημιουργία περιπτώσεων ελέγχου βασισμένων στην BPEL.
Στο τρίτο βήμα η παραγόμενη διαδικασία BPEL ενσωματώνεται στον *Διαχειριστή Εκτέλεσης* της *Υπηρεσία Διαχείρισης και Συντονισμού του Εκτελεστή Περιπτώσεων Ελέγχου* του SELIS ΣυΕ υλοποιώντας τις απαιτούμενες διεπαφές.



Σχήμα 59: Στοιχεία Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων

Στον *Αποδέκτη* της *Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων* του Εκτελεστή Περιπτώσεων Ελέγχου δημιουργείται η επαφή *ΔιεπαφήXAdES-Xαποδέκτη* (Σχήμα 59) η οποία καλείται από την ΥΔΕ κατά την αρχικοποίηση της διαδικασίας ελέγχου.



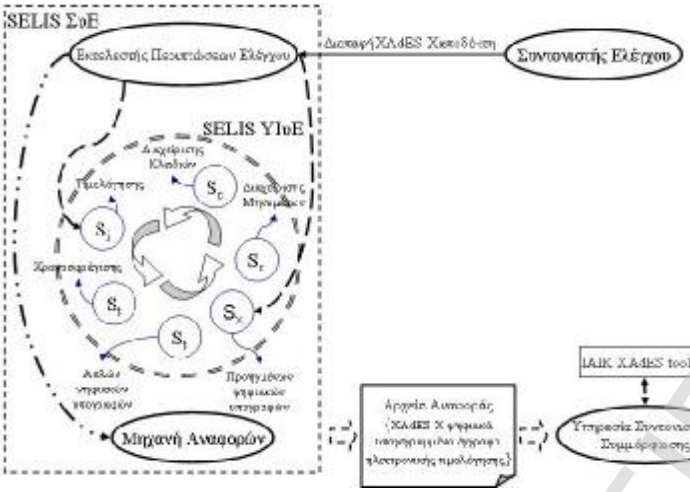
Σχήμα 60: Στοιχεία Υπηρεσίας Διαχείρισης και Συντονισμού

Στον *Διαχειριστή Εκτέλεσης* της *Υπηρεσίας Διαχείρισης και Συντονισμού* δημιουργείται η διεπαφή *ΔιεπαφήXAdES-XΕκτέλεσης* (Σχήμα 60) η οποία καλείται από τον *Διαχειριστή Ουράς Λήψης* της *Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων* για την εκτέλεση της καθοριζόμενης διαδικασίας BPEL.
Στο τέταρτο και πέμπτο βήμα του σταδίου τα οποία είναι προαιρετικά δεν απαιτείται η παραγωγή και αποθήκευση κάποιων δεδομένων ελέγχου.
Τέλος, στο έκτο και έβδομο βήμα διαμορφώνεται το προσχέδιο με βάση το οποίο πραγματοποιείται η αλληλουχία των ελέγχων και η αποθήκευση του στο *Αποθετήριο Δεδομένων Ελέγχου* της ΥΔΕ. Στο παράδειγμα που εξετάζουμε υπάρχει μόνο μία περίπτωση ελέγχου, επομένως στο προσχέδιο εισάγεται μόνο το URL της διεπαφής *ΔιεπαφήXAdES-Xαποδέκτη* που υλοποιήθηκε στον *Αποδέκτη* της *Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων του Εκτελεστή Περιπτώσεων Ελέγχου.*

3.3.2.1.2 Στάδιο 2ο: Εκτέλεση Περιπτώσεων Ελέγχου

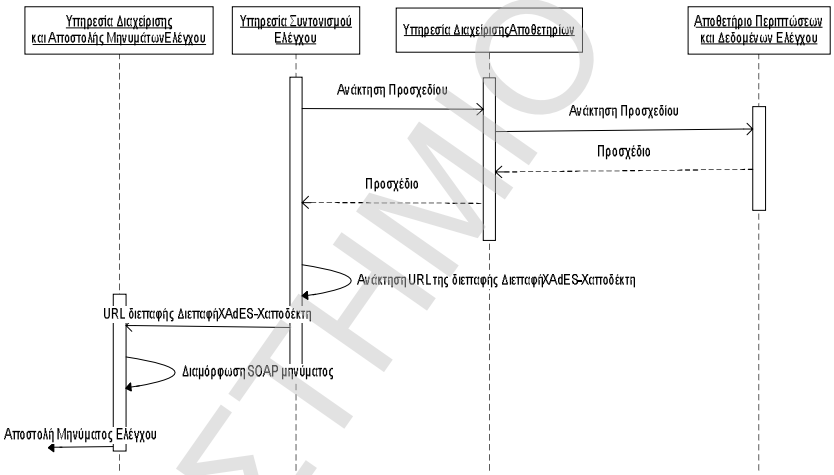
Στο στάδιο αυτό ξεκινάει η εκτέλεση των περιπτώσεων ελέγχου με βάση την σειρά με την οποία καθορίστηκαν στο προσχέδιο το οποίο διαμορφώθηκε στο 1ο στάδιο, όπως φαίνεται στο Σχήμα 61. Στην παρούσα φάση το προσχέδιο περιέχει μία μόνο περίπτωση ελέγχου που αφορά τον *"Έλεγχο συμμόρφωσης της XAdES-X ψηφιακής υπογραφής που εφαρμόζεται σε ένα XML έγγραφο ηλεκτρονικής τιμολόγησης"*.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 61. Έλεγχος Συμμόρφωσης SELIS ΣυΕ

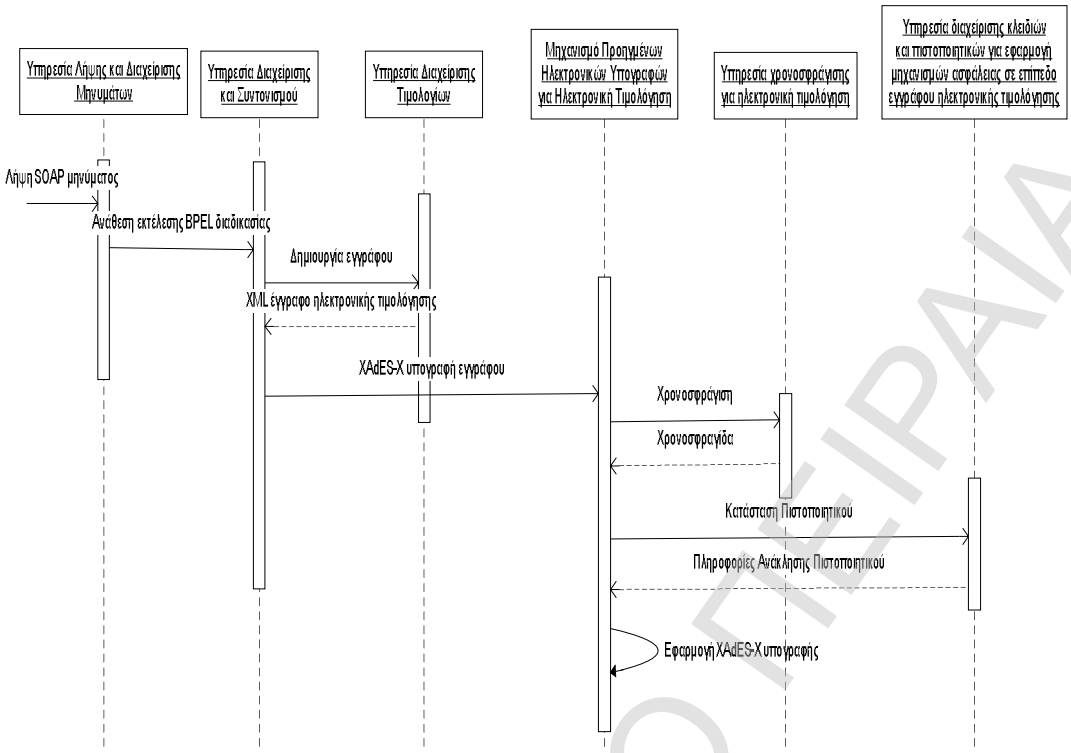
Στο Κεφάλαιο 2.3.5.1.2.3 παρουσιάστηκε η διαδικασία αρχικοποίησης της εκτέλεσης των περιπτώσεων ελέγχου η οποία πραγματοποιείται από την ΥΔΕ. Συνοπτικά η διαδικασία αυτή απεικονίζεται στο διάγραμμα ακολουθίας του Σχήμα 62.



Σχήμα 62. ΥΔΕ Ανάκτηση Περιπτώσεως Ελέγχου

Σύμφωνα λοιπόν με το Σχήμα 62 η *Υπηρεσία Συντονισμού Ελέγχου* αναθέτει στην *Υπηρεσία Διαχείρισης Αποθετηρίων* την ανάκτηση του προσχεδίου από το *Αποθετήριο Δεδομένων Ελέγχου*. Από το προσχέδιο λαμβάνεται το URL της διεπαφής *ΔιεπαφήXAdES-Χαποδέκτη* το οποίο απαιτείται να κληθεί για την εκτέλεση της περίπτωσης ελέγχου που αφορά τον *"Έλεγχο συμμόρφωσης της XAdES-X ψηφιακής υπογραφής"*. Στην συνέχεια η υπηρεσία αναθέτει στην *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου* να πραγματοποιήσει τη συγκεκριμένη κλήση με τη διαμόρφωση και αποστολή του απαραίτητου μηνύματος ελέγχου SOAP στο ΣυΕ της SELIS η-τιμολόγησης.

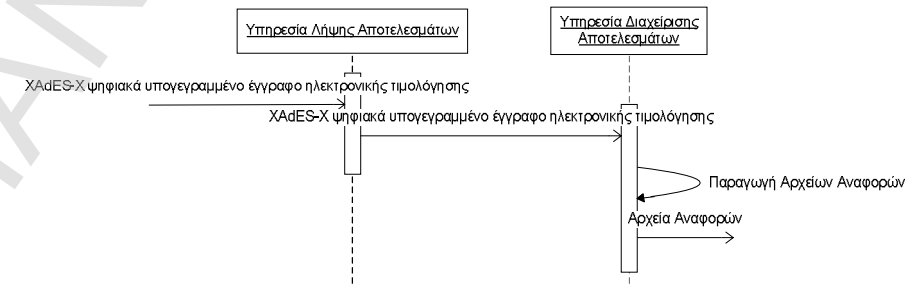
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 63: Εκτέλεση 14ης Περιπτώσεως Ελέγχου στη SELIS η-τιμολόγηση

Η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* του Εκτελεστή Περιπτώσεων Ελέγχου του SELIS ΣυΕ έχει την ευθύνη της λήψης και αποδόμησης του μηνύματος αναθέτοντας στην *Υπηρεσία Διαχείρισης και Συντονισμού* την εκτέλεση της αντίστοιχης διαδικασίας BPEL όπως αυτή ορίστηκε στην 3.3.2.1.1. Με βάση τη διαδικασία αυτή πραγματοποιείται ο συντονισμός των υπηρεσιών από τα οποία απαρτίζεται η SELIS ΥΙυΕ τα οποία απαιτούνται για την εκτέλεση της περίπτωσης ελέγχου.

Σύμφωνα λοιπόν με την προσδιοριζόμενη διαδικασία BPEL, η οποία απεικονίζεται στο διάγραμμα ακολουθίας του Σχήμα 58, αρχικά γίνεται ενεργοποίηση της *Υπηρεσίας Διαχείρισης Τιμολογίων* για τη δημιουργία ενός xCBL XML εγγράφου ηλεκτρονικής τιμολόγησης. Στην συνέχεια, ο *Μηχανισμό Προηγμένων Ηλεκτρονικών Υπογραφών για Ηλεκτρονική Τιμολόγηση* χρησιμοποιώντας τρεις υπηρεσίες, την *Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση*, την *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης* και τον *Μηχανισμός ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση* παράγει την XAdES-X υπογραφή του παραγόμενου XML εγγράφου τιμολόγησης.

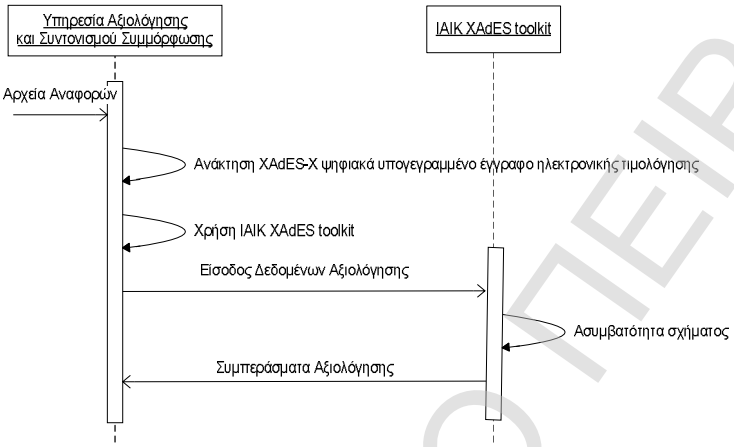


Σχήμα 64: Αποστολή XAdES-X Ψηφιακά Υπογεγραμμένου εγγράφου στη ΥΔΕ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.3.2.1.3 Στάδιο 3ο: Συλλογή των Δεδομένων Αξιολόγησης

Στόχο του σταδίου αποτελεί η συλλογή των δεδομένων αξιολόγησης της εξεταζόμενης περιπτώσεως ελέγχου. Σε πρώτη φάση η *Υπηρεσία Λήψης Αποτελεσμάτων* επικοινωνεί με τον Εκτελεστή Περιπτώσεων Ελέγχου και ανακτά το XAdES-X ψηφιακά υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης (Σχήμα 65). Στη συνέχεια, η *Υπηρεσία Διαχείρισης Αποτελεσμάτων* εισάγει το αρχείο αυτό σε ένα αρχείο αναφορών (log file).



Σχήμα 65: Διαδικασία Αξιολόγησης Υπογεγραμμένου Εγγράφου

3.3.2.1.4 Στάδιο 4ο: Ανάλυση Δεδομένων Αξιολόγησης

Στο παρόν στάδιο η *Υπηρεσία Αξιολόγησης και Συντονισμού Συμμόρφωσης* του στρώματος συμμόρφωσης της ΥΔΕ λαμβάνει το αρχείο αναφορών που έχει παραχθεί από το SELIS ΣυΕ εξάγοντας το XAdES-X ψηφιακά υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης (Σχήμα 65). Η υπηρεσία από την ανάλυση του εγγράφου διαπιστώνει ότι ο μηχανισμός αξιολόγησης που πρέπει να χρησιμοποιηθεί είναι το εργαλείο/βιβλιοθήκη IAIK XAdES toolkit. Στο σημείο αυτό το παραγόμενο υπογεγραμμένο έγγραφο εισέρχεται στο εργαλείο/βιβλιοθήκη (IAIK XAdES toolkit) το οποίο ελέγχει τη συμμόρφωση της εφαρμοζόμενης υπογραφής ως προς το XAdES-X πρότυπο.

Το αποτέλεσμα της αξιολόγησης διαπίστωσε μια ασυμβατότητα του σχήματος της παραγόμενης υπογραφής ως προς το αντίστοιχο πρότυπο υποδεικνύοντας την εξεταζόμενη περίπτωση ελέγχου ως ανεπιτυχής.

3.3.2.1.5 Στάδιο 5ο: Διόρθωση ΥΙυΕ

Με το πέρας της εκτέλεσης της περιπτώσεως ελέγχου οι αρμόδιοι της SELIS η-τιμολόγησης ενημερώθηκαν σχετικά με τα αποτελέσματα της αξιολόγησης. Σύμφωνα, λοιπόν με την περίπτωση ελέγχου η οποία εξετάστηκε στις προηγούμενες παραγράφους δημιουργείται η ανάγκη για διόρθωση της χρησιμοποιούμενης εφαρμογής XAdES.

Η SELIS η-τιμολόγηση [Papastergiou07a] δημιουργεί και επαληθεύει προηγμένες ηλεκτρονικές υπογραφές με τη χρησιμοποίηση μιας αναβαθμισμένης έκδοσης της βιβλιοθήκης ανοικτού κώδικα XAdES που είχε αναπτυχθεί στο πρόγραμμα OpenXAdES [OpenXAdES] στην Εσθονία, ως μέρος της πρακτικής πιστοποίησης που έχει υιοθετηθεί στην ηλεκτρονική διακυβέρνηση [Esthonian06]. Η βιβλιοθήκη αυτή έχει τροποποιηθεί ώστε να υποστηρίζει το μεγαλύτερο μέρος των μορφών των

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

προηγμένων ψηφιακών υπογραφών όπως αυτές καθορίζονται από το πρότυπο XAdES (XAdES-BES, XAdES-EPES, XAdES-T, XAdES-C και XAdES-X). Στο παράρτημα (βλ. § 9.1) παρατίθεται το XAdES-X υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης που παράγει η υπηρεσία SELIS κατά την πρώτη φάση του ελέγχου συμμόρφωσης.
Τα αποτελέσματα όμως της αξιολόγησης δηλώνουν ότι απαιτείται μια περαιτέρω βελτίωση της εφαρμογής ώστε να υπάρχει πλήρης συμμόρφωση. Οι βελτιώσεις αυτές αφορούν αποκλίσεις ως προς το αντίστοιχο σχήμα.
Η εφαρμογή XAdES, λοιπόν, διορθώνεται και τροποποιείται κατάλληλα ώστε να επαναλάβει τον αποτυχημένο έλεγχο συμμόρφωσης. Στο παράρτημα (βλ. § 9.2) παρατίθεται το XAdES-X-L υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης που παράγει η υπηρεσία SELIS μετά την υλοποίηση των διορθώσεων.

3.3.2.1.6 Στάδιο 6ο: Επανεκτέλεση Απαιτούμενων Ελέγχων

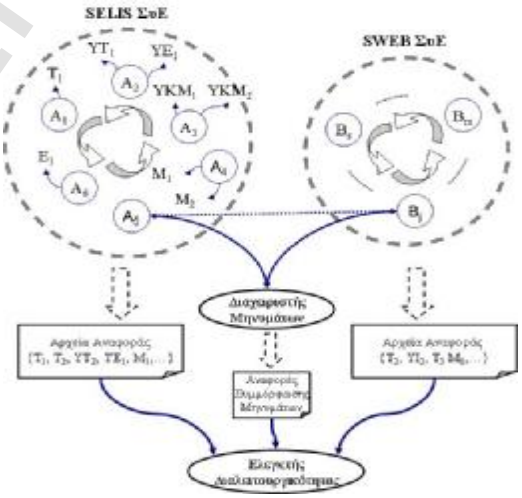
Στο στάδιο αυτό πραγματοποιείται η επανεκτέλεση τη εξεταζόμενης περίπτωσης ελέγχου που αφορά τον "*Έλεγχο συμμόρφωσης της XAdES-X ψηφιακής υπογραφής που εφαρμόζεται σε ένα XML έγγραφο ηλεκτρονικής τιμολόγησης*". Αυτή εκτελείται ξεκινώντας από το 6ο βήμα του 1ου σταδίου της μεθοδολογίας ελέγχου συμμόρφωσης. Τα αποτελέσματα αξιολόγησης τα οποία τελικώς προέκυψαν από το 4ο στάδιο υποδεικνύουν πλήρη συμμόρφωση της SELIS η-τιμολόγησης ως προς το πρότυπο XAdES.

3.3.2.2 Έλεγχος Συμμόρφωσης SWEB η-τιμολόγησης

Η SWEB η-τιμολόγηση εκτελεί και αυτή με τη σειρά της μια ανάλογη διαδικασία ελέγχου συμμόρφωσης όμοια με αυτή που παρουσιάστηκε για την περίπτωση της SELIS η-τιμολόγηση στο Κεφάλαιο 3.3.2.1.

3.3.3 4η Φάση ΔΣΥΙ: Έλεγχος Διαλειτουργικότητας

Τα δύο ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης, στην παρούσα φάση εξετάζονται ως προς τη δυνατότητα να επικοινωνήσουν μεταξύ τους επιτυχώς. Η διάταξη με την οποία μετέχουν τα συστήματα στον έλεγχο έχει καθοριστεί από την πρώτη φάση της μεθοδολογίας και απεικονίζεται στο Σχήμα 66. Στις παραγράφους που ακολοθούν παρουσιάζεται η εκτέλεση των βημάτων που καθορίζονται από την προτεινόμενη μεθοδολογία για τον έλεγχο διαλειτουργικότητας.



Σχήμα 66. Διάταξη ΣυΕ για συμμετοχή στον Έλεγχο Διαλειτουργικότητας

3.3.3.1 Στάδιο 1ο: Καθορισμός Περιπτώσεων Ελέγχου

Στο Κεφάλαιο 2.3.6.1.1 παρουσιάστηκε ένα σύνολο βημάτων τα οποία πρέπει να ακολουθηθούν για τον καθορισμό των περιπτώσεων ελέγχου διαλειτουργικότητας. Σαν 1ο βήμα τέθηκε ο σχεδιασμός των εξεταζόμενων περιπτώσεων ελέγχου. Στο σημείο αυτό θα ολοκληρωθεί η διαδικασία σχεδιασμού μίας μόνο περιπτώσεως ελέγχου η οποία θα χρησιμοποιηθεί ως παράδειγμα για τον σχεδιασμό των υπολοίπων.
Τα απαιτούμενα υποβήματα τα οποία πρέπει να εκτελεστούν παρουσιάστηκαν στην 2.3.6.1.1.3 και είναι τα ακόλουθα:

1 υποβήμα. Προσδιορισμός μιας εκδοχής του σεναρίου

Η εκδοχή η οποία επιλέγεται να εξεταστεί αποτελεί το σύνολο του σεναρίου όπως αυτό ορίστηκε κατά την 1η φάση της μεθοδολογίας (βλ. § 3.3). Πιο συγκεκριμένα, η SELIS η-τιμολόγηση λειτουργεί ως ο εκδότης ενός ηλεκτρονικού τιμολογίου ενώ η SWEB η-τιμολόγηση δρά ως ο αποδέκτης του τιμολογίου ο οποίος επιστρέφει μια ειδοποίηση στη SELIS η-τιμολόγηση. Στην εξεταζόμενη διαδικασία, η SELIS αποτελεί το ΣυΕ που ενεργεί ως αρχικοποιητής.

2 υποβήμα. Ανάλυση της επιχειρησιακής λογικής

Η επιχειρησιακή λογική η οποία εμπεριέχεται στο SELIS ΣυΕ και με βάση την οποία μετέχει στη διαδικασία ελέγχου είναι η ακόλουθη:

1. Εξαγωγή ενός εγγράφου ηλεκτρονικής τιμολόγησης από το υποστηριζόμενο σύστημα Διαχείρισης Πληροφοριακών Πόρων.
2. Μετασχηματισμός του εξαγόμενου εγγράφου ηλεκτρονικής τιμολόγησης σε μια μορφή με την οποία θα αποσταλεί στον παραλήπτη.
3. Εφαρμογή προηγμένης ψηφιακής υπογραφής στο έγγραφο ηλεκτρονικής τιμολόγησης που προκύπτει από τον μετασχηματισμό.
4. Αποστολή του υπογεγραμμένου εγγράφου ηλεκτρονικής τιμολόγησης με χρήση κατάλληλων δικλείδων ασφαλείας (κρυπτογράφησης και ψηφιακής υπογραφής).
5. Λήψη ενός μηνύματος επιβεβαίωσης και επικύρωση των εφαρμοσμένων μηχανισμών ασφάλειας (κρυπτογράφησης και ψηφιακής υπογραφής).
6. Εξαγωγή της ειδοποίησης που εμπεριέχεται στο μήνυμα και επαλήθευση της ορθότητας των εφαρμοσμένων μηχανισμών ασφάλειας (απλή ψηφιακή υπογραφή).
7. Αποθήκευση του υπογεγραμμένου εγγράφου ηλεκτρονικής τιμολόγησης και της ληφθείσας υπογεγραμμένης ειδοποίησης.

3 υποβήμα. Καταγραφή υποσυνόλων

Στον Πίνακας 8 παρουσιάζονται τα βήματα τα οποία περιλαμβάνονται στην διαδικασία η οποία αποτελεί ένα υποσύνολο της συνολικής διαδικασίας που περιγράφηκε στο υποβήμα 2. Για την περιγραφή των βημάτων λήφθηκαν υπόψη και τα χρησιμοποιούμενα πρότυπα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΣυΕ	Ακολουθία	Εκτελέσιμα Βήματα
SELIS η-τιμολόγηση	1.	Εξαγωγή εγγράφου XML από το Exact ERP
	2.	Μετασχηματισμός σε ένα έγγραφο xCBL
	3.	Εφαρμογής ψηφιακής υπογραφής XAdES-X
	4.	Δημιουργία μήνυματος SOAP
	5.	Ψηφιακή υπογραφή και κρυπτογραφηση μηνύματος
	6.	Αποστολή μηνύματος SOAP
	7.	Λήψη μηνύματος SOAP
	8.	Αποκρυπτογράφηση μηνύματος SOAP
	9.	Επαλήθευση Ψηφιακής Υπογραφής μηνύματος SOAP
	10.	Εξαγωγή υπογεγραμμένης ειδοποίησης XML (YE1)
	11.	Επαλήθευση ψηφιακής υπογραφής ειδοποίησης XML
	12.	Αποθήκευση των υπογεγραμμένων εγγράφων

Πίνακας 8. Βήματα Εξεταζόμενης Διαδικασίας

4 υποβήμα. Ορισμός περίπτωσης ελέγχου

Ο Πίνακας 9 περιγράφει την περίπτωση ελέγχου διαλειτουργικότητας που αντιστοιχεί στην εκδοχή του σεναρίου που καθορίστηκε στο 1^{ο} υποβήμα με βάση τον ορισμό που δόθηκε στην 2.3.5.1.1.3.

Ορισμός Περιπτώσεως Ελέγχου Διαλειτουργικότητα			
Ενέργεια$_i$	Υπηρεσία$_i$	Είσοδος$_i$	Έξοδος$_i$
Εξαγωγή XML εγγράφου τιμολόγησης από το Exact ERP	Υπηρεσία διαχείρισης αποθετηρίων ηλεκτρονικής τιμολόγησης	Πληροφορίες πρόσβασης στο σύστημα και εξαγωγής του ζητούμενου εγγράφου	(Exact ERP) έγγραφο ηλεκτρονικής τιμολόγησης XML
Μετασχηματισμός του (Exact ERP) εγγράφου XML σε ένα έγγραφο xCBL	Υπηρεσία μετασχηματισμού ηλεκτρονικών τιμολογίων	(Exact ERP) έγγραφο ηλεκτρονικής τιμολόγησης XML, έγγραφο μετασχηματισμού XSLT	xCBL έγγραφο ηλεκτρονικής τιμολόγησης XML
Εφαρμογή προηγμένης ψηφιακής υπογραφής	Μηχανισμός προηγμένων ηλεκτρονικών υπογραφών για ηλεκτρονική τιμολόγηση	έγγραφο ηλεκτρονικής τιμολόγησης XML - Πληροφορίες ανάκλησης πιστοποιητικού - Χρονοσφραγίδα	XAdES-X υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης XML
Λήψη πιστοποιητικού	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης	Πληροφορίες ανάκτησης πιστοποιητικού (π.χ. ψευδώνυμο, κωδικούς πρόσβασης)	Ιδιωτικό κλειδί πιστοποιητικού
Λήψη πληροφοριών ανάκλησης πιστοποιητικού	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης	Στοιχεία πιστοποιητικού	Πληροφορίες ανάκλησης πιστοποιητικού
Υπογραφή εγγράφου με βάση το πρότυπο W3C XML Digital Signature	Μηχανισμός ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση	εγγράφου ηλεκτρονικής XML	υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης XML (W3C XML Digital Signature)
Λήψη χρονοσφραγίδας	Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση	Σύνοψη υπογεγραμμένου εγγράφου ηλεκτρονικής τιμολόγησης XML	Χρονοσφραγίδα
Δημιουργία μηνύματος	Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης	XAdES-X υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης XML	μήνυμα SOAP του εγγράφου τιμολόγησης
Λήψη πιστοποιητικού	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων	Πληροφορίες ανάκτησης του πιστοποιητικού (π.χ. ψευδώνυμο, κωδικούς πρόσβασης)	Ιδιωτικό κλειδί
Υπογραφή μηνύματος	Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης	Πληροφορίες ανάκτησης πιστοποιητικού (π.χ. ψευδώνυμο, κωδικούς πρόσβασης)	Υπογεγραμμένο μήνυμα SOAP

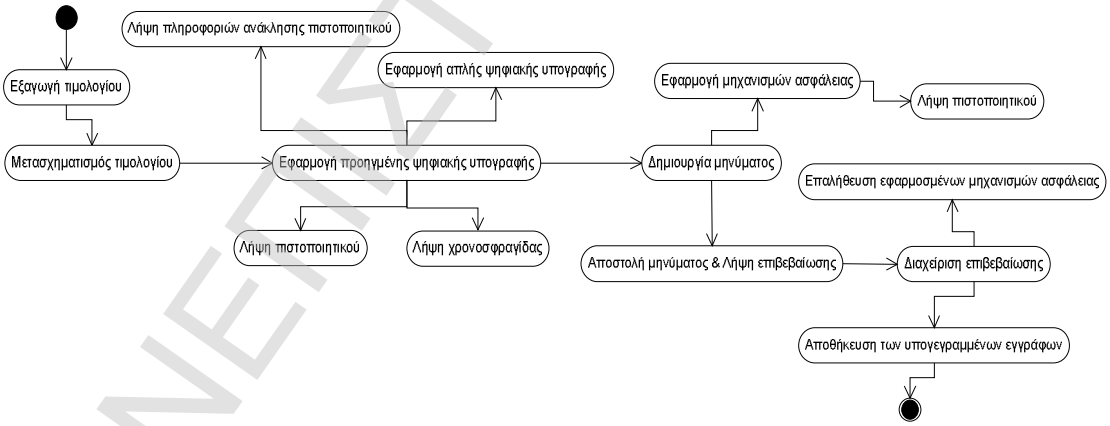
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Λήψη πιστοποιητικού	Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων	Πληροφορίες ανάκτησης πιστοποιητικού (π.χ. ψευδώνυμο, κωδικούς πρόσβασης)	Χρησιμοποιούμενο πιστοποιητικό
Κρυπτογράφηση μηνύματος	Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης	Χρησιμοποιούμενο πιστοποιητικό, μήνυμα SOAP	Κρυπτογραφημένο μήνυμα SOAP
Αποστολή μηνύματος	Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης	Κρυπτογραφημένο μήνυμα SOAP	Κρυπτογραφημένο μήνυμα SOAP
Αποκρυπτογράφηση μηνύματος	Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης	Κρυπτογραφημένο μήνυμα SOAP	Αποκρυπτογραφημένο μήνυμα SOAP
Επαλήθευση Ψηφιακής Υπογραφής μηνύματος	Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης	Αποκρυπτογραφημένο μήνυμα SOAP	μήνυμα SOAP
Εξαγωγή υπογεγραμμένης XML ειδοποίησης	Υπηρεσία ειδοποιήσεων ηλεκτρονικής τιμολόγησης	μήνυμα SOAP	Υπογεγραμμένο έγγραφο ειδοποίησης XML (W3C XML Digital Signature)
Επαλήθευση ψηφιακής υπογραφής ειδοποίησης XML	Υπογραφή εγγράφου με βάση το πρότυπο W3C XML Digital Signature	Υπογεγραμμένο έγγραφο ειδοποίησης XML (W3C XML Digital Signature)	Υπογεγραμμένο έγγραφο ειδοποίησης XML (W3C XML Digital Signature)
Αποθήκευση των υπογεγραμμένων εγγράφων	Υπηρεσία διαχείρισης αποθετηρίων ηλεκτρονικής τιμολόγησης	Πληροφορίες πρόσβασης βάσης δεδομένων, υπογεγραμμένο έγγραφο ειδοποίησης XML (W3C XML Digital Signature), XAdES-X υπογεγραμμένο XML έγγραφο ηλεκτρονικής τιμολόγησης	

Πίνακας 9. Ορισμός Περιπτώσεως Ελέγχου Διαλειτουργικότητας

5 υποβήμα. Απεικόνιση περίπτωσης ελέγχου

Οι περιπτώσεις ελέγχου διαλειτουργικότητας, ομοίως με τις αντίστοιχες του ελέγχου συμμόρφωσης, μπορεί να απεικονιστούν με τη χρήση ενός διαγράμματος ενεργειών (activity graph diagram) (βλ. § 2.3.6.1.1.3). Το διάγραμμα που αναπαριστά στην εξεταζόμενη περίπτωση ελέγχου εμφανίζεται στο Σχήμα 67.



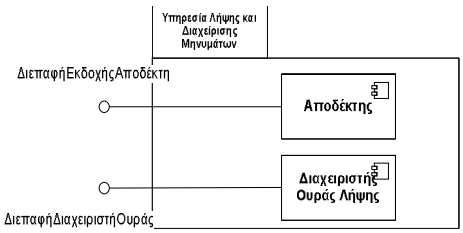
Σχήμα 67. Διάγραμμα Ενεργειών Εξεταζόμενης Περίπτωσης Ελέγχου Διαλειτουργικότητας

Το στοιχείο που πρέπει να τονιστεί είναι ότι η περίπτωση ελέγχου η οποία προσδιορίστηκε καθορίζει μόνο τις ενέργειες οι οποίες πρέπει να εκτελεστούν από το SELIS ΣυΕ που αρχικοποιεί τη διαδικασία ελέγχου. Το SWEB ΣυΕ ανταποκρίνεται με βάση τη λογική που περιέχεται στην ΥΙυΕ που περιλαμβάνεται σε αυτό.

Το δεύτερο βήμα του παρόντος σταδίου επικεντρώνεται στην παραγωγή της διαδικασίας BPEL που αντιστοιχεί στην περίπτωση ελέγχου που ορίστηκε στο 1^{ο} βήμα. Η δημιουργία της διαδικασίας αυτής γίνεται με τη χρήση πλαισίων και

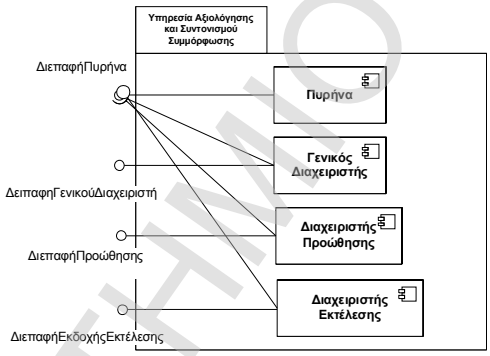
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

μοντέλων [Zheng07, Sinha06, Yuan06, Yan06] τα οποία επιτρέπουν την αυτοματοποιημένη δημιουργία περιπτώσεων ελέγχου βασισμένων στην BPEL.
Στο πλαίσιο του τρίτου βήματος η παραγόμενη διαδικασία BPEL ενσωματώνεται στον *Διαχειριστή Εκτέλεσης* της *Υπηρεσίας Διαχείρισης και Συντονισμού του Εκτελεστή Περιπτώσεων Ελέγχου* του SELIS ΣυΕ. Η ενσωμάτωση ολοκληρώνεται με την υλοποίηση των διεπαφών που φαίνονται στο Σχήμα 69.



Σχήμα 68: Στοιχεία Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων

Στον *Αποδέκτη της Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων* του *Εκτελεστή Περιπτώσεων Ελέγχου* δημιουργείται η επαφή `ΔιεπαφήΕκδοχήςαποδέκτη` (Σχήμα 68) η οποία καλείται από την ΥΔΕ κατά την αρχικοποίηση της διαδικασίας ελέγχου.



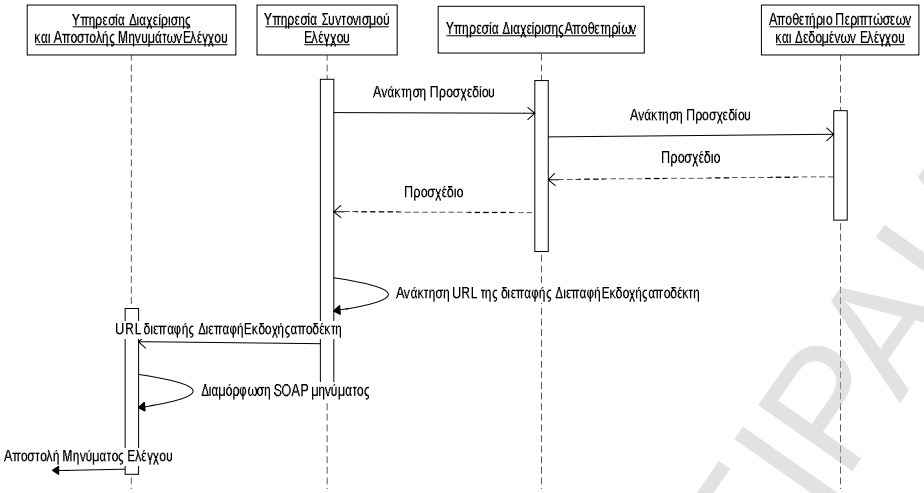
Σχήμα 69: Στοιχεία Υπηρεσίας Διαχείρισης και Συντονισμού

Στην συνέχεια στον *Διαχειριστή Εκτέλεσης της Υπηρεσίας Διαχείρισης και Συντονισμού* δημιουργείται η διεπαφή `ΔιεπαφήΕκδοχήςΕκτέλεσης` (Σχήμα 69) η οποία καλείται από τον *Διαχειριστή Ουράς Λήψης* της *Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων* για την εκτέλεση της καθοριζόμενης διαδικασίας BPEL.
Το τέταρτο και το πέμπτο βήμα του σταδίου δεν εκτελούνται από τη στιγμή που δεν απαιτείται η παραγωγή και αποθήκευση κάποιων δεδομένων ελέγχου.
Τέλος, στο έκτο και το έβδομο βήμα διαμορφώνεται το προσχέδιο με βάση το οποίο πραγματοποιείται η αλληλουχία των ελέγχων και η αποθήκευσή του στο *Αποθετήριο Δεδομένων Ελέγχου* της ΥΔΕ. Στο παράδειγμα που εξετάζουμε υπάρχει μόνο μία περίπτωση ελέγχου, επομένως στο προσχέδιο εισάγεται μόνο το URL της διεπαφής `ΔιεπαφήΕκδοχήςαποδέκτη` που υλοποιήθηκε στον *Αποδέκτη* της *Υπηρεσίας Λήψης και Διαχείρισης Μηνυμάτων του Εκτελεστή Περιπτώσεων Ελέγχου*.

3.3.3.2 Στάδιο 2ο: Εκτέλεση Περιπτώσεων Ελέγχου

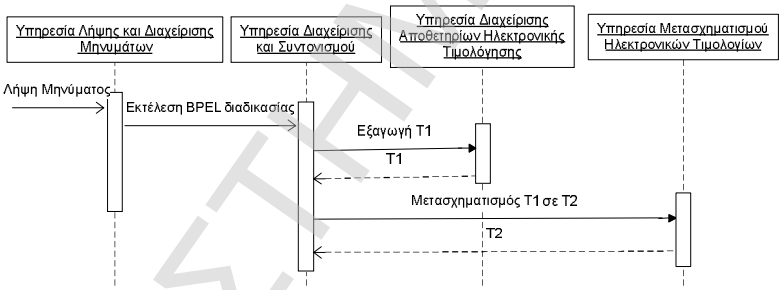
Στο παρόν στάδιο θα πραγματοποιηθεί η εκτέλεση της περίπτωσης ελέγχου που καθορίστηκε στο 1ο στάδιο. Η διαδικασία εκτέλεσης ξεκινάει από την ΥΔΕ με την κλήση της διεπαφής που ορίστηκε για τη συγκεκριμένη περίπτωση ελέγχου. Στο διάγραμμα ακολουθίας του Σχήμα 70 παρουσιάζεται η διαδικασία αυτή.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 70: ΥΔΕ: Ανάκτηση Περιπτώσεως Ελέγχου Διαλειτουργικότητας

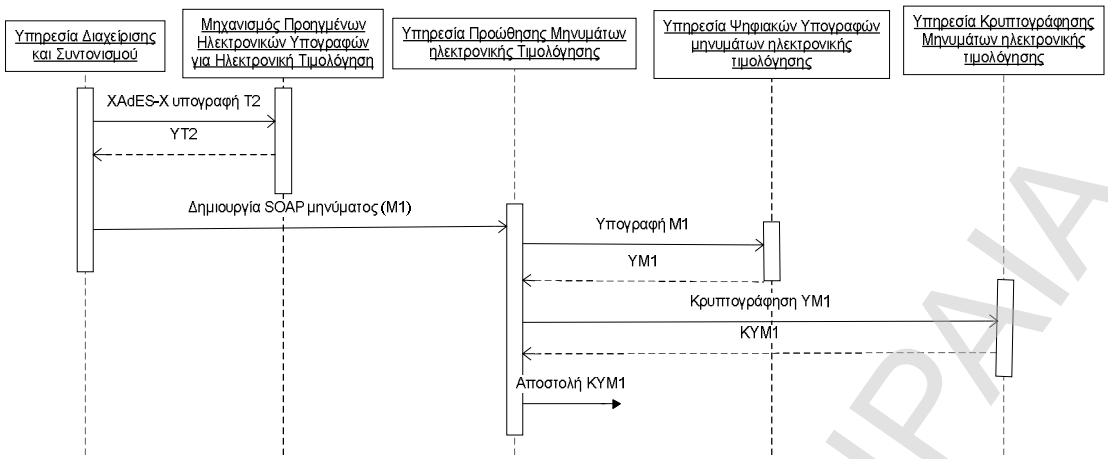
Συγκεκριμένα, η *Υπηρεσία Συντονισμού Ελέγχου* αναθέτει στην *Υπηρεσία Διαχείρισης Αποθετηρίων* την ανάκτηση του προσχεδίου από το *Αποθετήριο Δεδομένων Ελέγχου*. Από το προσχέδιο λαμβάνεται το URL της διεπαφής `ΔιεπαφήΕκδοχήςαποδέκτη` το οποίο απαιτείται να κληθεί για την εκτέλεση της εξεταζόμενης περίπτωσης ελέγχου. Στην συνέχεια η υπηρεσία αναθέτει στην *Υπηρεσία Διαχείρισης και Αποστολής Μηνυμάτων Ελέγχου* να πραγματοποιήσει τη συγκεκριμένη κλήση με τη διαμόρφωση και αποστολή του απαραίτητου μήνυμα ελέγχου SOAP στο ΣυΕ της SELIS η-τιμολόγησης.



Σχήμα 71: SELIS η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (α)

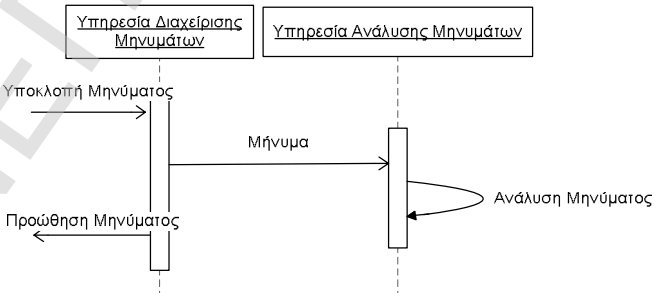
Η *Υπηρεσία Λήψης και Διαχείρισης Μηνυμάτων* του Εκτελεστή Περιπτώσεων Ελέγχου του SELIS ΣυΕ έχει την ευθύνη της λήψης και αποδόμησης του μηνύματος αναθέτοντας στην *Υπηρεσία Διαχείρισης και Συντονισμού* την εκτέλεση της αντίστοιχης διαδικασίας BPEL όπως αυτή ορίστηκε στην 3.3.3.1. Με βάση τη διαδικασία αυτή πραγματοποιείται ο συντονισμός των υπηρεσιών από τα οποία απαρτίζεται η SELIS ΥΙυΕ τα οποία απαιτούνται για την εκτέλεσης της περίπτωσης ελέγχου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 72: SELIS η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (β)

Η διαδικασία (Σχήμα 71 και Σχήμα 72) ξεκινάει από τη SELIS η-τιμολόγηση και από την *Υπηρεσία Διαχείρισης και Συντονισμού* η οποία ενεργοποιεί την *Υπηρεσία διαχείρισης αποθετηρίων ηλεκτρονικής τιμολόγησης* η οποία εξάγει από το Exact ERP ένα έγγραφο ηλεκτρονικής τιμολόγησης (T1). Το έγγραφο αυτό μετασχηματίζεται με την χρήση της *Υπηρεσία μετασχηματισμού ηλεκτρονικών τιμολογίων* σε ένα xCBL έγγραφο ηλεκτρονικής τιμολόγησης (T2) και υπογράφεται (YT2). Για τη δημιουργία της υπογραφής χρησιμοποείται ο *Μηχανισμός Προηγμένων Ηλεκτρονικών Υπογραφών για Ηλεκτρονική Τιμολόγηση* ο οποίος χρησιμοποιεί δύο υπηρεσίες, την *Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση* και την *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης* για την εφαρμογή της XAdES-X υπογραφής στο παραγόμενο έγγραφο τιμολόγησης XML.
Η *Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης* λαμβάνει το έγγραφο αυτό και το εισάγει σε ένα μήνυμα SOAP (M1) στο οποίο εφαρμόζει ψηφιακή υπογραφή (YM1) και κρυπτογράφηση (YKM1) κάνοντας χρήση της *Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης*, της *Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης* και της *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων*. Τέλος, το μήνυμα SOAP (YKM1) αποστέλλεται στη SWEB η-τιμολόγηση.

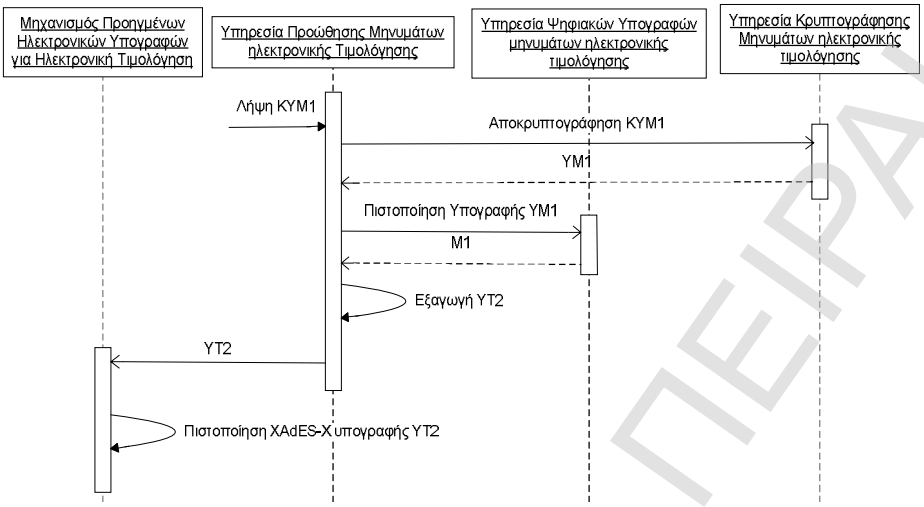


Σχήμα 73: Ανάλυση Μηνύματος από την ΥΔΕ

Η *Υπηρεσία Διαχείρισης Μηνυμάτων* της ΥΔΕ η οποία παρακολουθεί τα δεδομένα τα οποία ανταλλάσσονται μεταξύ των δύο συστημάτων υποκλέπτει (Σχήμα 73) το μήνυμα και το καταγράφει σε μια μορφή η οποία επιτρέπει την περαιτέρω ανάλυση του από την *Υπηρεσία Ανάλυσης Μηνυμάτων*. Η υπηρεσία αυτή ελέγχει τη συμμόρφωση του μηνύματος (βλέπε § 9.3) με την περιγραφή της υπηρεσία της

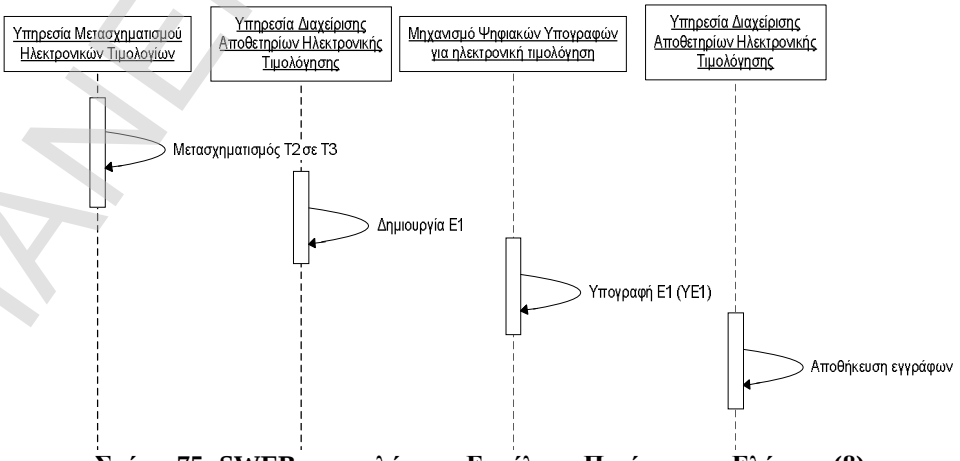
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

SWEB ηλεκτρονικής τιμολόγησης που περιέχεται στο WSDL αρχείο (βλέπε § 9.3). Στη συνέχεια, η *Υπηρεσία Διαχείρισης Μηνυμάτων* αναλαμβάνει την προώθηση του μηνύματος στη SWEB η-τιμολόγηση η οποία εκτελεί τις ενέργειες που της αναλογούν.



Σχήμα 74: SWEB η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (α)

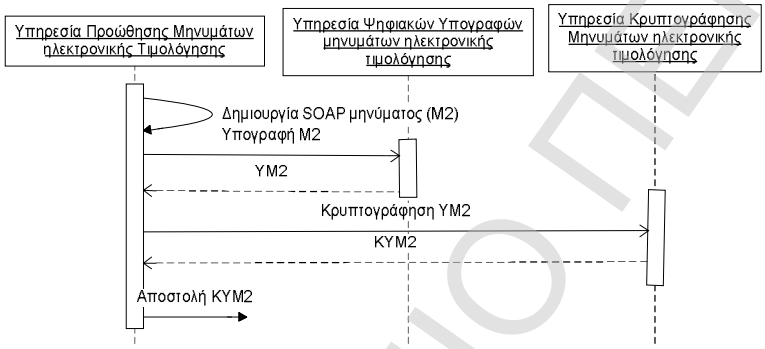
Η SWEB η-τιμολόγηση με τη λήψη του μηνύματος SOAP (YKM1) το διαχειρίζεται σύμφωνα με τη λογική η οποία έχει ενσωματωθεί στην ίδια την εφαρμογή (Σχήμα 74) Η *Υπηρεσία Λήψης Μηνυμάτων ηλεκτρονικής τιμολόγησης* λαμβάνει το μήνυμα και αναθέτει την αποκρυπτογράφηση και επαλήθευση της ψηφιακής υπογραφής του στις ακόλουθες υπηρεσίες: *Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης*, *Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης* και *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων*.
Στη συνέχεια το υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης xCBL (YT2) εξάγεται από το μήνυμα και γίνεται επαλήθευση της εφαρμοζόμενης υπογραφής. Η επαλήθευση πραγματοποιείται μέσω του *Μηχανισμού Προηγμένων Ηλεκτρονικών Υπογραφών για Ηλεκτρονική Τιμολόγηση* ο οποίος χρησιμοποιεί δύο υπηρεσίες, την *Υπηρεσία χρονοσφράγισης για ηλεκτρονική τιμολόγηση* και την *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης*.



Σχήμα 75: SWEB η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (β)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Το απεσταλμένο τιμολόγιο (Τ2) μετασχηματίζεται (Σχήμα 75) σε έγγραφο SAP ERP ηλεκτρονικής τιμολόγησης (Τ3) μέσω της *Υπηρεσίας μετασχηματισμού ηλεκτρονικών τιμολογίων* και εισέρχεται στο SAP ERP με χρήση της *Υπηρεσίας διαχείρισης αποθετηρίων ηλεκτρονικής τιμολόγησης*. Με την ολοκλήρωση της διαδικασίας αυτής η *Υπηρεσία ειδοποιήσεων ηλεκτρονικής τιμολόγησης* δημιουργεί μια xCBL XML ειδοποίηση παραλαβής εγγράφου ηλεκτρονικής τιμολόγησης (Ε1) η οποία υπογράφεται ψηφιακά (ΥΕ1) χρησιμοποιώντας το *Μηχανισμό ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση* και την *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης*. Τα υπογεγραμμένα έγγραφα της ειδοποίησης XML και ηλεκτρονικής τιμολόγησης xCBL XML αποθηκεύονται σε μια βάση δεδομένων μέσω της *Διαχείριση Αποθετηρίων ηλεκτρονικής τιμολόγησης*.

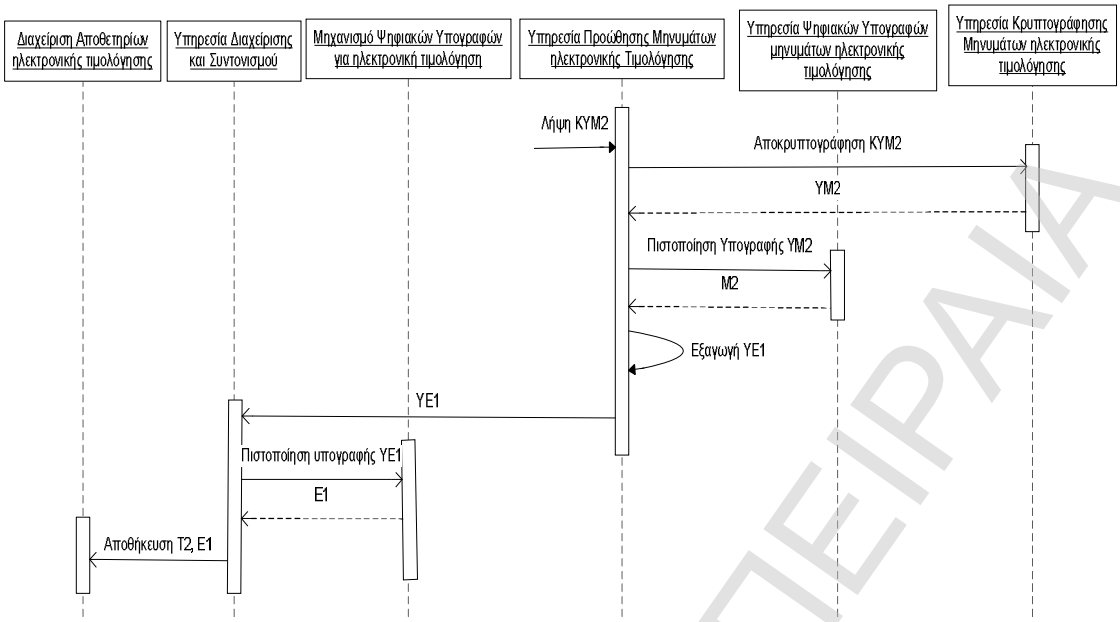


Σχήμα 76: SWEB η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (γ)

Τελικά, η *Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης* δημιουργεί ένα μήνυμα SOAP (M2) (Σχήμα 76) το οποίο περιέχει την υπογεγραμμένη ειδοποίηση και στο οποίο εφαρμόζει ψηφιακή υπογραφή (YM2) και κρυπτογράφηση (YKM2) κάνοντας χρήση της *Υπηρεσίας Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης*, της *Υπηρεσίας Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης* και της *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων*. Το μήνυμα SOAP (YKM2) στέλνεται στη SELIS η-τιμολόγηση.

Ομοίως, η *Υπηρεσία Διαχείρισης Μηνυμάτων* της ΥΔΕ υποκλέπτει το μήνυμα και το καταγράφει (Σχήμα 73) ενώ αναθέτει στην *Υπηρεσία Ανάλυσης Μηνυμάτων* να ελέγξει τη συμμόρφωση του μηνύματος με την περιγραφή της υπηρεσία της SELIS ηλεκτρονικής τιμολόγησης που περιέχεται στο αντίστοιχο αρχείο WSDL. Στη συνέχεια, η Υπηρεσία Διαχείρισης Μηνυμάτων αναλαμβάνει την προώθηση του μηνύματος στη SELIS η-τιμολόγηση η οποία εκτελεί τις ενέργειες που υπολοίπουνται και οι οποίες έχουν οριστεί στην διαδικασία BPEL της εξεταζόμενης περιπτώσεως ελέγχου.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 77: SELIS η-τιμολόγηση Εκτέλεση Περίπτωσης Ελέγχου (γ)

Η *Υπηρεσία προώθησης μηνυμάτων ηλεκτρονικής τιμολόγησης* της SELIS η-τιμολόγησης λαμβάνοντας το μήνυμα SOAP (ΥΚΜ2) (Σχήμα 78) που αποτελεί την απάντηση στο μήνυμα το οποίο είχε στείλει να αποκρυπτογραφεί και επαληθεύει την ψηφιακή υπογραφή του μέσω των ακόλουθων υπηρεσιών: *Υπηρεσία Ψηφιακών Υπογραφών μηνυμάτων ηλεκτρονικής τιμολόγησης, Υπηρεσία Κρυπτογράφησης Μηνυμάτων ηλεκτρονικής τιμολόγησης* και *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο μηνυμάτων*. Ακολούθως εξάγει την υπογεγραμμένη ειδοποίηση (ΥΕ1) και επαληθεύει την υπογραφή (με το *Μηχανισμό ψηφιακών υπογραφών για ηλεκτρονική τιμολόγηση* και την *Υπηρεσία διαχείρισης κλειδιών και πιστοποιητικών για εφαρμογή μηχανισμών ασφάλειας σε επίπεδο εγγράφου ηλεκτρονικής τιμολόγησης*).
Τελικά, αποθηκεύει τα δύο ανταλλασσόμενα υπογεγραμμένα έγγραφα (υπογεγραμμένη ειδοποίηση XML (ΥΕ1) και υπογεγραμμένο ηλεκτρονικό τιμολόγιο xCBL XML (ΥΤ2)) σε μια βάση δεδομένων χρησιμοποιώντας την *Διαχείριση Αποθετηρίων ηλεκτρονικής τιμολόγησης*.

3.3.3.3 Στάδιο 3ο: Συλλογή των Δεδομένων

Τα αποτελέσματα αξιολόγησης τα οποία παράγονται από τα ΣυΕ κατά την εκτέλεση των περιπτώσεων ελέγχου συλλέγονται από τις αντίστοιχες Μηχανές Αναφορών τους. Πιο συγκεκριμένα οι *Υπηρεσίες Λήψης Αποτελεσμάτων* εποπτεύοντας τις πρωτεύουσες υπηρεσίες των ΥΙυΕ ανακτούν τα δεδομένα τα οποία στη συνέχεια προωθούνται στις *Υπηρεσίες Διαχείρισης Αποτελεσμάτων* οι οποίες τα εισάγουν σε αρχεία αναφορών (log files).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΣυΕ	*Συστατικά*	**Αποτελέσματα**
SELIS η-τιμολόγησης	*Μηχανή Αναφορών*	Πληροφορίες εξαγωγής εγγράφου (T1) από το Exact ERP
		Πληροφορίες μετασχηματισμού του T1 σε T2
		έγγραφο T2
		XAdES-X ψηφιακά υπογεγραμμένο έγγραφο YT2
		Πληροφορίες δημιουργίας XadES-X υπογραφής
		ψηφιακά υπογεγραμμένη ειδοποίηση YE1
		Πληροφορίες επαλήθευσης ψηφιακής υπογραφής της ειδοποίησης YE1
		μήνυμα SOAP (M1)
		Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM1)
		Κρυπτογραφημένο Μήνυμα SOAP (YKM1)
		Πληροφορίες δημιουργίας, ψηφιακή υπογραφή και κρυπτογράφηση του Μηνύματος SOAP M1
		μήνυμα SOAP (M2)
		Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM2)
		Κρυπτογραφημένο Μήνυμα SOAP (YKM2)
		Πληροφορίες επαλήθευσης ψηφιακής υπογραφής και την κρυπτογράφηση του Μηνύματος SOAP M2
SWEB η-τιμολόγησης	*Μηχανή Αναφορών*	Πληροφορίες μετασχηματισμού T2 σε T3
		Πληροφορίες εισαγωγής T3
		Το ψηφιακά υπογεγραμμένο έγγραφο ειδοποίηση (YE1)
		Πληροφορίες σχετικά με την ορθή επαλήθευση της XAdES-X υπογραφής
		Το έγγραφο ηλεκτρονικής τιμολόγησης xCBL (T2)
		Το έγγραφο ειδοποίησης xCBL (E1)
		ψηφιακά υπογεγραμμένο έγγραφο ειδοποίηση xCBL (YE1)
		Πληροφορίες δημιουργίας ψηφιακής υπογραφής στην ειδοποίηση YE1
		μήνυμα SOAP (M2)
		Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM2)
		Κρυπτογραφημένο Μήνυμα SOAP (YKM2)
		Πληροφορίες δημιουργίας, ψηφιακής υπογραφής και κρυπτογράφησης του Μηνύματος SOAP M2
		μήνυμα SOAP (M1)
		Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM1)
		Κρυπτογραφημένο Μήνυμα SOAP (YKM1)
		Πληροφορίες επαλήθευσης της ψηφιακής υπογραφής και της κρυπτογράφησης του Μηνύματος SOAP M1

Πίνακας 10. Συλλεγόμενα Δεδομένα Αξιολόγησης

Στον Πίνακας 10 εμφανίζονται τα αποτελέσματα που συλλέγει καθεμία από τις Μηχανές Αναφορών των αντίστοιχων ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης.

3.3.3.4 Στάδιο 4ο: Ανάλυση Δεδομένων Αξιολόγησης

Η *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας* του στρώματος διαλειτουργικότητας της ΥΔΕ στο συγκεκριμένο στάδιο φέρει την ευθύνη της ανάκτησης των αρχείων αναφορών που έχουν παραχθεί από τα ΣυΕ και της εξαγωγής των δεδομένων αξιολόγησης από αυτά.

Στη συνέχεια τα δεδομένα αυτά αναλύονται ώστε να διαπιστωθεί η δυνατότητα επικοινωνίας των δύο ΣυΕ. Στους Πίνακας 11, Πίνακας **12** και Πίνακας **13** εμφανίζονται οι έλεγχοι οι οποίοι πραγματοποιήθηκαν για την περίπτωση ελέγχου που εξετάζεται.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Έλέγχος	Έλεγχος	Αποτέλεσμα Ελέγχου
Αξιολόγηση μετατροπής εγγράφων από ένα σχήμα σε ένα άλλο	Πληροφορίες εξαγωγής του εγγράφου T1 από το Exact ERP	Επιτυχής
	Πληροφορίες μετασχηματισμού του T1 σε T2	Επιτυχής
	Πληροφορίες μετασχηματισμού του T2 σε T3	Επιτυχής
	Πληροφορίες εισαγωγής του εγγράφου T3 στο SAP ERP	Επιτυχής
Συνολικό Αποτέλεσμα		Επιτυχής μετασχηματισμός εγγράφων

Πίνακας 11. Εκτελούμενοι Έλεγχοι στον Ελεγκτή Μετασχηματισμού

Ελεγκτής Διαλειτουργικότητας	Έλεγχος		Αποτέλεσμα Ελέγχου
	SELIS η-τιμολόγησης	*SWEB η-τιμολόγησης*	
Σύγκριση ανταλλασσόμενων εγγράφων & έλεγχος εφαρμοζόμενων μηχανισμών ασφάλειας	Έγγραφο T2	Έγγραφο T2	Όμοια
	XAdES-X ψηφιακά υπογεγραμμένο έγγραφο YT2	XAdES-X ψηφιακά υπογεγραμμένο έγγραφο YT2	Όμοια
	Πληροφορίες δημιουργίας της XAdES-X υπογραφής	Πληροφορίες επαλήθευσης της XAdES-X υπογραφής	Επιτυχής
	ψηφιακά υπογεγραμμένη ειδοποίηση YE1	ψηφιακά υπογεγραμμένο έγγραφο ειδοποίηση xCBL (YE1)	Όμοια
	Πληροφορίες σχετικά με την ορθή επαλήθευση της ψηφιακής υπογραφής της ειδοποίησης (YE1)	Πληροφορίες δημιουργίας ψηφιακής υπογραφής στην ειδοποίηση YE1	Επιτυχής
		Ειδοποίησης (E1)	
Συνολικό Αποτέλεσμα			Κατοχή όμοιων εγγράφων – επιτυχής εφαρμογή και επαλήθευση μηχανισμών

Πίνακας 12. Εκτελούμενοι Έλεγχοι στον Ελεγκτή Εγγράφου

Ελεγκτής Διαλειτουργικότητας	Έλεγχος		Αποτέλεσμα Ελέγχου
	SELIS η-τιμολόγησης	*SWEB η-τιμολόγησης*	
Σύγκριση ανταλλασσόμενων μηνυμάτων & έλεγχος εφαρμοζόμενων μηχανισμών ασφάλειας	μήνυμα SOAP (M1)	μήνυμα SOAP (M1)	Όμοια
	Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM1)	Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM1)	Όμοια
	Κρυπτογραφημένο Μήνυμα SOAP (YKM1)	Κρυπτογραφημένο Μήνυμα SOAP (YKM1)	Όμοια
	Πληροφορίες δημιουργίας, ψηφιακής υπογραφής και κρυπτογράφησης του Μηνύματος SOAP M1	Πληροφορίες επαλήθευση της ψηφιακής υπογραφής και την κρυπτογράφηση του Μηνύματος SOAP M1	Επιτυχής
	μήνυμα SOAP (M2)	μήνυμα SOAP (M2)	Όμοια
	Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP	Ψηφιακά Υπογεγραμμένο Μήνυμα SOAP (YM2)	Όμοια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

	(ΥΜ2)		
	Κρυπτογραφημένο Μήνυμα SOAP (ΥΚΜ2)	Κρυπτογραφημένο Μήνυμα SOAP (ΥΚΜ2)	Όμοια
	Πληροφορίες επαλήθευσης της ψηφιακής υπογραφής και της κρυπτογράφησης του Μηνύματος SOAP Μ2	Πληροφορίες δημιουργίας, ψηφιακής υπογραφής και κρυπτογράφησης του Μηνύματος SOAP Μ2	Επιτυχής
Συνολικό Αποτέλεσμα			Κατοχή όμοιων μηνυμάτων – επιτυχής εφαρμογή και επαλήθευση μηχανισμών μηνυμάτων

Πίνακας 13. Εκτελούμενοι Έλεγχοι στον Ελεγκτή Μηνυμάτων

Επίσης, επικοινωνεί με την Υπηρεσία Ανάλυσης Μηνυμάτων του Διαχειριστή Μηνυμάτων (βλ. § 2.3.4.2.3) ώστε να λάβει τις αναφορές που σχετίζονται με τη συμμόρφωση των μηνυμάτων ως προς την περιγραφή των αντίστοιχων ΥΙ.
Τα αποτελέσματα των ελέγχων καταγράφονται από την *Υπηρεσία Αξιολόγησης και Συντονισμού Διαλειτουργικότητας* και αποτελούν κριτήρια αξιολόγησης της διαλειτουργικότητας των ΣυΕ.

3.3.3.5 Στάδιο 5ο: Ενημέρωση και Διορθωτικές Ενέργειες

Με το πέρας της εκτέλεσης του συνόλου των περιπτώσεων ελέγχου οι αρμόδιοι των δύο ΣυΕ, της SELIS η-τιμολόγησης και της SWEB η-τιμολόγησης ενημερώθηκαν σχετικά με τα αποτελέσματα της αξιολόγησης, τα οποία υποδηλώνουν ότι τα δύο ΣυΕ μπορούν να επικοινωνήσουν επιτυχώς μεταξύ τους.

3.4 Συμπεράσματα

Το παρόν κεφάλαιο παρουσίασε την εφαρμογή της προτεινόμενης Μεθοδολογίας Ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ) για τον έλεγχο της επικοινωνίας δυο υπαρχόντων και πλήρως λειτουργικών Υπηρεσιών Ιστού για ηλεκτρονική τιμολόγηση, της αυτόνομης υπηρεσίας ηλεκτρονικής τιμολόγησης SELIS (Secure Electronic Invoicing Service) και της υπηρεσίας ηλεκτρονικής και κινητής τιμολόγησης SWEB. Οι βασικές αρχές της προτεινόμενης μεθοδολογίας έχουν ήδη χρησιμοποιηθεί στα πλαίσια δύο Ευρωπαϊκών ερευνητικών έργων.
Το γεγονός το οποίο πρέπει να σημειωθεί είναι ότι η χρήση μεθοδολογιών ελέγχου διαλειτουργικότητας θέτουν ως βασικό στόχο να εξετάσουν και να εξασφαλίσουν την ομαλή και αποτελεσματική ανταλλαγή ευαίσθητων πολλές φορές ως προς τη φύση τους και το περιεχόμενό τους δεδομένων. Το στοιχείο αυτό όμως εγείρει ένα σύνολο πρόσθετων ζητημάτων που αφορούν τη διαχείριση της ταυτότητας και ειδικότερα την προστασία της ιδιωτικότητας τόσο των απλών χρηστών που επιζητούν πρόσβαση στις προσφερόμενες υπηρεσίες όσο και των παρόχων των υπηρεσιών αυτών. Ο δεύτερος άξονας της διατριβής, που παρουσιάζεται στα κεφάλαια που ακολουθούν, θέτει στο επίκεντρο του ενδιαφέροντος ζητήματα που αφορούν την διαχείριση της ταυτότητας και της ιδιωτικότητας στις ασφαλείς και προηγμένες κινητές και ηλεκτρονικές Υπηρεσίες Ιστού (ΥΙ).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

3.5 Αναφορές

[Kaliontzoglou06c] A. Kaliontzoglou, P. Boutsi, D. Polemi. (2006). "*eInvoke: Secure e-Invoicing based on Web Services*", Electronic Commerce Research Journal, Springer.

[Kaliontzoglou06d] A. Kaliontzoglou et al. (2006). "*Secure electronic eInvoicing with the SELIS architecture: technical overview, market trends and deployment models*", Proceedings of 2nd Conference on Electronic Democracy, Athens, 2006.

[EDI] Electronic Data Interchange (EDI), Federal Information Processing Standards Publication 161-2, 1996 April 29, http://www.itl.nist.gov/fipspubs/fip161-2.htm

[Clement04] L. Clement et al. (Editors). (2004). "*UDDI Version 3.0.2*", OASIS UDDI Spec Technical Committee Draft http://uddi.org/pubs/uddi-v3.0.2-20041019.htm

[European Parliament01] The European Parliament. (2001). Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax.

[XSLT] Extensible Stylesheet Language Transformations (XSLT), Version 2.0, W3C Recommendation 23 January 2007.

[Mitra03] N. Mitra. (Editor). (2003). "*SOAP version 1.2 Part0: Primer*", W3C Recommendation, http://www.w3.org/TR/soap12-part0/.

[WSS06] Web Services-Security (WSS) Core Specification 1.1 - OASIS Standard 1.1, (2006), http://www.oasis-open.org.

[Meneklis07] V. Meneklis, S. Papastergiou, C. Douligeris, D. Polemi. (2007). "*Towards advanced e/m-Government platforms*", International Conference on Information Society (i-Society 2007), October 7–11, 2007, Merrillville, Indiana, USA.

[Exact] Exact ERP Solution, http://www.exactamerica.com/.

[SAP] SAP ERP, Invoice Management, http://www50.sap.com/businessmaps/C725391FA85E44D7B90F7C0BC8ACBD07.htm.

[Meier02] W. Meier, (2002), "*eXist: An Open Source Native XML Database*", Lecture Notes In Computer Science, Revised Papers from the NODe 2002 Web and Database-Related Workshops on Web, Web-Services, and Database Systems, Springer-Verlag, 169-183.

[Altova] Altova XMLSpy, http://www.altova.com/.

[IBM] IBM XML Security Suite, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite.

[IAIK] IAIK XML signature library, http://jce.iaik.tugraz.at/sic/products/xml_security

[Apache] Apache XML security, http://xml.apache.org/security/index.html

[Microsoft] Microsoft .Net security library tools, http://msdn.microsoft.com/netframework/

[OnlineVer] Online XML Digital Signature Verifier, http://www.aleksey.com/xmlsec/xmldsig-verifier.html

[IAIKXAdES] IAIK XAdES library. (2006). http://jce.iaik.tugraz.at/sic/products/xml_security/xades.

[Ehnebuske03] D. Ehnebuske, et al.. (2003). "*WS-I Overview*", www.ws-i.org/docs/20021003.wsi.introduction.pdf.

[Brittenham] P. Brittenham. "*Understanding the WS-I Test Tool*", http://www-128.ibm.com/developerworks/webservices/library/ws-wsitest/.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Brittenham05a] P. Brittenham et al. (Contributors). (2005). "*WS-I Monitor Tool Functional Specification*", WS-I Testing Work Group, 13/06/2005. Version 1.1.
[Brittenham05b] P. Brittenham et al. (Editors). (2005). "*WS-I Analyzer Tool Functional Specification*", WS-I Testing Work Group, 13/06/2005. Version 1.1.
[Zheng07] Y. Zheng, J. Zhou, P. Krause. (2007). "*An Automatic Test Case Generation Framework for Web Services*", Journal of Software, vol. 2(3), pp. 64-77 (2007).
[Sinha06] A. Sinha, A. Paradkar. (2006). "*Model based functional conformance testing of web services operating on persistent data*", TAV-WEB. ACM Press, 2006, pp. 17–22.
[Yuan06] Y. Yuan, Z. Li, W. Sun. (2006). "*A graph-search based approach to bpel4ws test generation*", ICSEA. IEEE Computer Society, 2006, p. 14.
[Yan06] J. Yan, Z. Li, Y. Yuan, W. Sun, J. Zhang. (2006). "*Bpel4ws unit testing: Test case generation using a concurrent path analysis approach*", ISSRE. IEEE Computer Society, 2006, pp. 75–84.
[Papastergiou07a] S. Papastergiou, A. Kaliontzoglou, D. Polemi. (2007). "*Interoperability issues of a Secure Electronic Invoicing Service*", 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), 3-7 September 2007, Athens.
[OpenXAdES] The OpenXAdES project, (2003), http://www.openxades.org
[Esthonian06] The Esthonian ID-card e-government project, (2006), http://www.id.ee/pages.php/0303.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

4 Διαχείριση Ταυτότητας και Ιδιωτικότητα σε Ασφαλείς και Προηγμένες Κινητές και Ηλεκτρονικές Υπηρεσίες Ιστού

Στο παρόν κεφάλαιο, σε πρώτη φάση, μελετώνται και παρουσιάζονται βασικές έννοιες (π.χ. μερικές ταυτότητες) που συνδέονται με τη διαχείριση της ταυτότητας των χρηστών και αναδεικνύεται η ανάγκη ύπαρξης Συστημάτων Διαχείρισης Ταυτότητας τα οποία θα αποτελούνται από διακριτές και αυστηρά ορισμένες υπηρεσίες. Στη συνέχεια επισημαίνεται η σημασία της προστασίας της ιδιωτικότητας των χρηστών για την ολοκλήρωση αξιόπιστων και έμπιστων η/κ-συναλλαγές και γίνεται παράθεση του συνόλου των πτυχών της ιδιωτικότητας οι οποίες πρέπει να ληφθούν υπόψη για τον σχεδιασμό και υλοποίηση αποτελεσματικών, από επιχειρησιακή άποψη ΣΔΤ.
Επιπλέον, η χρήση των Πολιτικών Ιδιωτικότητας αναγνωρίζεται ως ένας αποτελεσματικός και ευέλικτος τρόπος για την προστασία της ιδιωτικότητας και πραγματοποιείται και παρουσιάζεται μια ταξινόμηση των Γλωσσών Πολιτικών Ιδιωτικότητας με βάση το σκοπό υλοποίησης αλλά και χρήσης κάθε γλώσσας. Τέλος, το κεφάλαιο αυτό περιγράφει τα πραγματικά προβλήματα με τα οποία έρχεται αντιμέτωπη η διατριβή στα πλαίσια του δεύτερου άξονα.

4.1 Εισαγωγή

Η Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ) θεωρήθηκε ως το πιο καινοτόμο αρχιτεκτονικό ύφος για το σχεδιασμό και την ανάπτυξη ενός συνόλου από πλατφόρμες και πληροφοριακά συστήματα. Χαρακτηριστικά παραδείγματα μπορούν να εντοπιστούν σε πολλές περιοχές του ψηφιακού κόσμου, όπως η η-διακυβέρνηση και το η-επιχειρείν.
Οι αρχιτεκτονικές αυτού του τύπου επιτρέπουν την παροχή ενός συνόλου ηλεκτρονικών και κινητών Υπηρεσιών Ιστού (η/κ-ΥΙ). Οι ΥΙ αυτές είναι προσβάσιμες από μια μεγάλη ποικιλία οντοτήτων όπως είναι οι επιχειρήσεις, αλλά και από ένα μεγάλο πλήθος απλών χρηστών. Η Ασφάλεια των συναλλαγών με τις ΥΙ αποτέλεσε ένα θεμελιώδες ζήτημα το οποίο απασχόλησε τόσο την επιστημονική όσο και την επιχειρηματική κοινότητα τα τελευταία χρόνια. Η ικανοποίηση των τεσσάρων διαστάσεων της ασφάλειας (*πιστοποίηση*, *εμπιστευτικότητα*, *ακεραιότητα* και *μη-αποποίηση ευθύνης*) διαδραματίζει σημαντικό ρόλο για την επιτυχία των η/κ-συναλλαγών. Η υιοθέτηση προτύπων και προδιαγραφών όπως είναι η Κρυπτογράφηση XML, η Υποδομή Δημόσιας Κλείδας (ΥΔΚ), οι Προηγμένες XML Ψηφιακές Υπογραφές (XAdES) και η Ασφάλεια Υπηρεσιών Ιστού παρέχει επαρκείς λύσεις για την δημιουργία ενός ασφαλούς περιβάλλοντος.

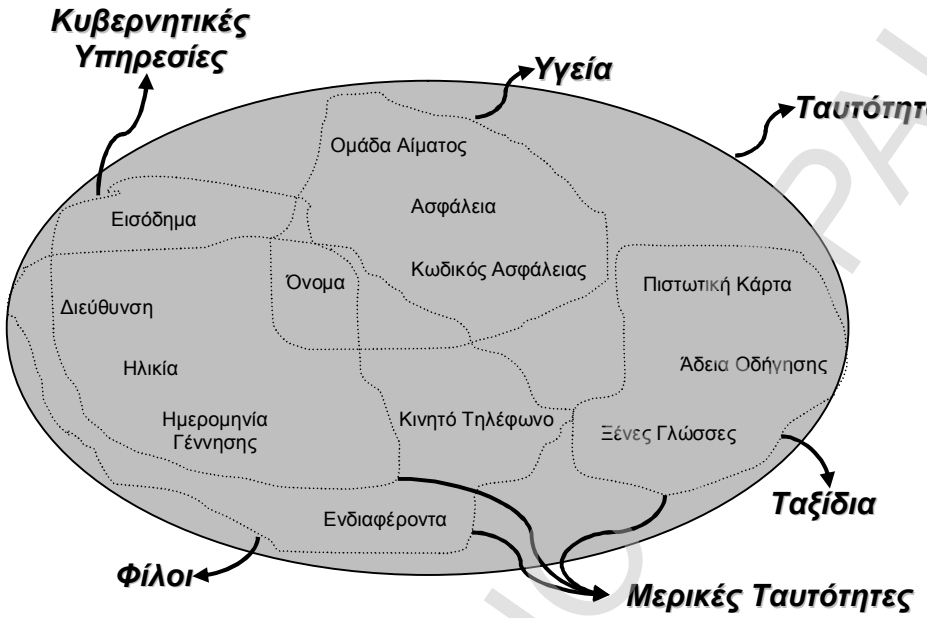
4.2 Υπάρχουσα Κατάσταση – Ανοιχτά Προβλήματα

4.2.1 Διαχείριση Ταυτότητας

Στις μέρες μας, η αύξηση των προσφερόμενων η/κ-ΥΙ από τους οργανισμούς έχει φέρει στο προσκήνιο ένα σύνολο από ζητήματα. Τα ζητήματα αυτά σχετίζονται με το γεγονός ότι οι χρήστες απαιτείται πλέον να παρέχουν ένα σύνολο προσωπικών δεδομένων κάθε φορά που χρησιμοποιούν τις υπηρεσίες αυτές [Yee06]. Σύνηθες

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

είναι το φαινόμενο, οι οργανισμοί να αποτελούν κομιστές και συλλέκτες ενός μεγάλου όγκου προσωπικών και έμπιστων πολλές φορές πληροφοριών, καθιστώντας τους χρήστες ανήμπορους να αντιδράσουν στην ανεξέλεκτη αυτή συλλογή των ευαίσθητων δεδομένων που συνθέτουν την *Ταυτότητά* τους.



Σχήμα 78: Ταυτότητα - Μερικές Ταυτότητες Χρήστη

Η *Ταυτότητα* ενός χρήστη αποτελείται από μια μεγάλη ποικιλία χαρακτηριστικών γνωρισμάτων τα οποία τον προσδιορίζουν μοναδικά [Buell03]. Καθένα από αυτά τα χαρακτηριστικά αντιπροσωπεύουν τον χρήστη, εντούτοις, διαφορετικοί συνδυασμοί αυτών είναι σε θέση να τον ταυτοποιήσουν μοναδικά. Στη σύγχρονη ψηφιακή κοινωνία, ένας χρήστης υιοθετεί και υποδύεται μια σειρά διαφορετικών ρόλων, όπως είναι δημότης, μαθητής, εργαζόμενος, ασφαλιζόμενος, ταξιδιώτης, πελάτης κ.τ.λ.. Με βάση λοιπόν τον ρόλο του ο χρήστης έχει πρόσβαση σε ένα σύνολο η/κ-ΥΙ εκτελώντας μια σειρά η/κ-συναλλαγών. Για καθεμία από τις συναλλαγές αυτές ο χρήστης δεν απαιτείται να χρησιμοποιεί το σύνολο της ταυτότητάς του αλλά μόνο ένα υποσύνολο αυτής το οποίο αποτελεί μια *μερική ταυτοτήτα* [Claub, Clauss05]. Για παράδειγμα ένας χρήστης χρησιμοποιεί διαφορετική μερική ταυτότητα για την εργασία του και άλλη για τις επαφές του με διάφορους οργανισμούς όπως είναι μια τράπεζα. Επομένως η ταυτότητα κάθε χρήστη χωρίζεται σε μεγάλο αριθμό μερικών ταυτοτήτων, όπως απεικονίζεται στο Σχήμα 78, η καθεμία από τις οποίες χρησιμοποιείται ανάλογα με την εκάστοτε περίπτωση.

Η *Διαχείριση Ταυτότητας* των οντοτήτων που μετέχουν σε μια η/κ-συναλλαγή αποτελεί πλέον ένα μείζον ζήτημα του σύγχρονου ψηφιακού κόσμου. Η Διαχείριση Ταυτότητας αποτελείται από το σύνολο των επιχειρησιακών διαδικασιών, εργαλείων, πολιτικών και τεχνολογιών που προσδιορίζουν την δημιουργία, διατήρηση και κατάργηση των μερικών ταυτοτήτων ενός χρήστη για την ασφαλή πρόσβαση σ' ένα διευρυμένο σύνολο συστημάτων και εφαρμογών [Pato03].

Πιο συγκεκριμένα, η διαχείριση ταυτότητας εστιάζει κυρίως στα εξής ζητήματα:

- Στον προσδιορισμό των επιχειρηματικών διαδικασιών που απαιτούν ταυτοποίηση των χρηστών.

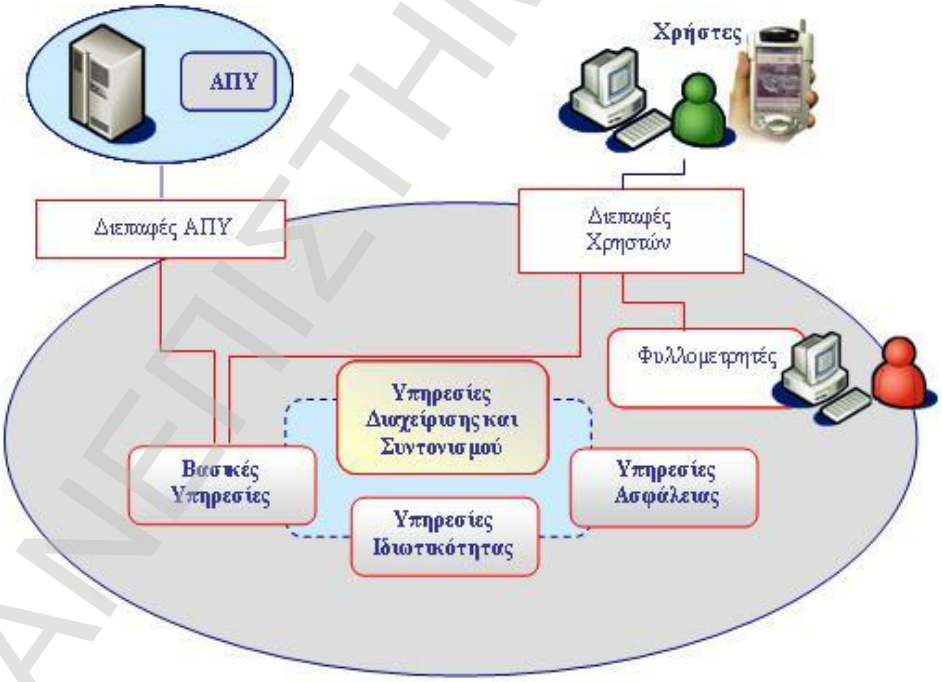
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- ü Στο βαθμό ταυτοποίησης των χρηστών στο σύστημα, δηλαδή στο πόσο ισχυρή είναι η ταυτότητα που δημιουργείται από το σύστημα και αν είναι ανθεκτική σε αντιγραφή ή κακή χρήση της.
- ü Στην διακριτική προσπέλαση των χρηστών σε διάφορες υπηρεσίες που προσφέρει το σύστημα.
- ü Στην επιλογή εκείνων των εργαλείων που θα διαχειρίζονται αποτελεσματικά τις ταυτότητες των χρηστών και θα δημιουργούν ένα ασφαλές περιβάλλον χωρίς προβλήματα.

Επομένως έκδηλη είναι η ανάγκη ύπαρξης *Συστημάτων Διαχείρισης Ταυτότητας* [Haddad08] τα οποία θα υποστηρίζουν και θα ολοκληρώνουν το σύνολο των διαδικασιών και των στοιχείων που αποτελούν μέρη της Διαχείρισης Ταυτότητας. Τα συστήματα αυτά επιτρέπουν την προστασία των χρηστών από την χωρίς έλεγχο αποκάλυψη των προσωπικών τους δεδομένων η οποία πραγματοποιείται από την συχνή χρήση η/κ-ΥΙ.

4.2.2 Συστήματα Διαχείρισης Ταυτότητας (ΣΔΤ)

Στο παρόν κεφάλαιο παρουσιάζονται οι απαιτούμενες υπηρεσίες από τις οποίες πρέπει να αποτελείται ένα Σύστημα Διαχειρίσης Ταυτότητας (ΣΔΤ), όπως αυτές έχουν προταθεί και περιγραφεί στο [Papastergiou07b], προκειμένου να ανταποκριθεί στις επιχειρησιακές του ανάγκες. Οι υπηρεσίες αυτές χωρίζονται σε τέσσερις κατηγορίες, όπως απεικονίζεται στο Σχήμα 79, καθεμία από τις οποίες εκτελεί μια σειρά ανεξάρτητων αλλά πλήρως αλληλένδετων λειτουργιών. Οι κατηγορίες είναι οι ακόλουθες:



Σχήμα 79: Υπηρεσίες ΣΔΤ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- *Υπηρεσίες Ιδιωτικότητας*, παρέχουν τις απαιτούμενες λειτουργίες, διαδικασίες και εργαλεία για την προστασία της ιδιωτικότητας των χρηστών.
- *Υπηρεσίες Ασφάλειας*, προσφέρουν τους αναγκαίους μηχανισμούς ασφάλειας για την εξασφάλιση των ασφαλών συναλλαγών.
- *Βασικές Υπηρεσίες*, προσφέρουν τις απαραίτητες βασικές λειτουργίες για την εγκατάσταση της επικοινωνίας με όλες τις εξωτερικές προς αυτήν οντότητες (π.χ. τους χρήστες).
- *Υπηρεσίες Διαχείρισης και Συντονισμού*, αναλαμβάνουν την διαχείριση όλων των λειτουργιών και μηχανισμών, αλλά και τον συντονισμό των ανωτέρω υπηρεσιών για την επιτυχή ολοκλήρωση των απαιτούμενων διαδικασίων.

Το σύνολο των κατηγοριών αυτών θα περιγραφεί στις παραγράφους που ακολουθούν αναλυτικά παραθέτοντας των σύνολο των πτυχών τους.

4.2.2.1 Υπηρεσίες Ιδιωτικότητας

Οι Υπηρεσίες Ιδιωτικότητας περιλαμβάνουν μια σειρά εργαλείων και υπηρεσιών οι οποίες στοχεύουν στη δημιουργία ενός περιβάλλοντος το οποίο θέτει στο επίκεντρο του ενδιαφέροντός του την προστασία της ιδιωτικότητας των χρηστών. Ειδικότερα, οι υπηρεσίες αυτές είναι οι εξής:

- **Υπηρεσίες Καταγραφής**: επιτρέπουν την καταγραφή των χρηστών οι οποίοι αιτούνται δικαίωμα πρόσβασης σε ένα σύνολο από προσφερόμενες ΥΙ. Μέσω της χρήσης της συγκεκριμένης υπηρεσίας οι χρήστες έχουν την δυνατότητα να επικοινωνούν με το ΣΔΤ για την παροχή των προσωπικών τους πληροφοριών και προτιμήσεων. Επιπλέον, μέσω της συγκεκριμένης υπηρεσίας δίνεται και η δυνατότητα στους οργανισμούς να καθορίσουν τις αρχές οι οποίες πρέπει να διέπουν την πρόσβαση στις ΥΙ τις οποίες προσφέρουν όπως είναι το σύνολο των προσφερόμενων πληροφοριών και το επίπεδο της ασφάλειας που πρέπει να εφαρμοστεί, ενώ επίσης μπορούν κα προσδιορίσουν και τους ρόλους που αποδίδονται στους χρήστες.
- **Υπηρεσίες Διαπραγμάτευσης**: παρέχουν ασφαλείς, αξιόπιστους και ευέλικτους μηχανισμούς διαπραγμάτευσης των δεδομένων τα οποία ανταλλάσσονται κατά την διάρκεια μιας συναλλαγής αλλά και το επίπεδο ασφάλειας που πρέπει να εφαρμοστεί. Με βάση την υπηρεσία αυτή καθορίζεται και ο ρόλος ο οποίος πρέπει να αποδοθεί στον χρήστη.
- **Υπηρεσίες Πιστοποίησης**: προσφέρουν επαρκείς μηχανισμούς πιστοποίησης και ταυτοποίησης των χρηστών οι οποίοι μετέχουν στις συναλλαγές.
- **Υπηρεσίες Έκδοσης Διαπιστευτηρίων**: εκτελούν διαδικασίες οι οποίες σχετίζονται με την δημιουργία, έκδοση και διανομή των απαιτούμενων διαπιστευτηρίων (π.χ. διαπιστευτήρια πιστοποίησης ή εξουσιοδότησης) στους εμπλεκόμενους χρήστες και οργανισμούς.
- **Υπηρεσίες Μετασχηματισμού**: παρέχουν μηχανισμούς οι οποίοι αναλαμβάνουν τον μετασχηματισμό των προτιμήσεων των χρηστών και των οργανισμών διαμορφώνοντας τις αντίστοιχες Πολιτικές Ιδιωτικότητας.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Οι προαναφερθέντες μηχανισμοί ιδιωτικότητας θέτουν ως κύριο μέλημά τους να διασφαλίσουν και να εγγυηθούν την προστασία της ιδιωτικότητας των εμπλεκομένων οντοτήτων.

4.2.2.2 Υπηρεσίες Ασφάλειας

Με την χρήση των υπηρεσιών ιδιωτικότητας, παρά το γεγονός ότι προστατεύεται η ταυτότητα των οντοτήτων, δεν μπορεί να επιτευχθεί η ασφαλής μεταφοράς τους. Για το λόγο αυτό απαιτείται η ολοκλήρωση των αναγκαίων μηχανισμών ασφάλειας οι οποίοι είναι οι ακόλουθοι:

- ***Υπηρεσίες Ασφάλειας Διαπιστευτηρίων,*** οι οποίες διαχειρίζονται τους διαφόρους τύπους των πιστοποιητικών πιστοποίησης που χρησιμοποιούν οι οντότητες.
- ***Μηχανισμοί Ψηφιακών Υπογραφών,*** χρησιμοποιούν κρυπτογραφία προκειμένου να επιτύχουν την ενσωμάτωση της ταυτότητας μιας οντότητας σε ένα διαπιστευτήριο και την εξασφάλιση της ακεραιότητάς του.
- **Μηχανισμοί κρυπτογράφησης**, χρησιμοποιούν αλγόριθμους κρυπτογράφησης για την κρυπτογράφηση και αποκρυπτογράφηση των διαπιστευτηρίων.

Ιδιαίτερη έμφαση θα πρέπει να δοθεί στην περίπτωση των κινητών εφαρμογών οι οποίες υπόκεινται σε συγκεκριμένους περιορισμούς, η διευθέτηση των οποίων επιβάλλει την υιοθέτηση των απαιτούμενων μηχανισμών ασφάλειας.

4.2.2.3 Βασικές Υπηρεσίες

Το ΣΔΤ, προκειμένου να εκτελέσει μια σειρά βασικών λειτουργιών, πρέπει να υιοθετήσει ένα σύνολο εργαλείων, υπηρεσιών οι οποίες διακρίνονται στις ακόλουθες:

Υπηρεσιές Διεπαφής

Οι *Υπηρεσίες διεπαφής* αναλαμβάνουν την επικοινωνία με τις εξωτερικές οντότητες (π.χ. χρήστες) μέσω της παροχής προηγμένων διεπαφών. Οι υπηρεσίες αυτές έχουν τις εξής δυνατότητες:

- Επιτρέπουν την επικοινωνία με τα διάφορα είδη φυλλομετρητών που χρησιμοποιούν οι χρήστες είτε εκτός είτε εντός του ΣΔΤ. Οι υπηρεσίες αυτές λαμβάνουν και επεξεργάζονται τα μηνύματα από τους ασφαλείς φυλλομετρητές και κάνουν χρήση των υπηρεσιών ασφάλειας όπου αυτό χρειάζεται, προκειμένου να επαληθεύσουν τις παραμέτρους ασφάλειας που ενδέχεται να συνοδεύουν τα μηνύματα.
- Αναλαμβάνουν την μεταφορά διαφόρων τύπων μηνυμάτων στον αντίστοιχο παραλήπτη εφαρμόζοντας την κατάλληλη πολιτική μεταφοράς. Για το σκοπό αυτό γίνεται χρήση των Υπηρεσιών Ασφάλειας.
- Αναλαμβάνουν την λήψη μηνυμάτων με στόχο την επεξεργασία τους επικυρώνοντας τους εφαρμοζόμενους μηχανισμούς ασφάλειας. Για το λόγο αυτό κάνουν χρήση των Υπηρεσιών Ασφάλειας.

Υπηρεσίες Διαχείρισης Αποθετηρίων

Οι *Υπηρεσίες διαχείρισης αποθετηρίων* ελέγχουν τις συναλλαγές με τα αποθετήρια (π.χ. βάσεις δεδομένων) που εμπεριέχονται στο ΣΔΤ παρέχοντας τις απαραίτητες διαδικασίες για την ασφαλή αποθήκευση και ανάκτηση ευαίσθητων δεδομένων, πολιτικών, κανόνων και ρόλων.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Υπηρεσίες Μετασχηματισμού και Διαχείρισης

Οι *Υπηρεσίες μετασχηματισμού μηνυμάτων* επιτρέπουν την μετατροπή μηνυμάτων προκειμένου να μεταφερθούν ανάμεσα σε διαφορετικές περιοχές διαχείρισης, όπως για παράδειγμα ανάμεσα σε οργανισμούς διαφορετικών χωρών. Οι υπηρεσίες μετασχηματισμού πρέπει να σέβονται τη σημασιολογία του περιεχομένου των μηνυμάτων προκειμένου τα έγγραφα που ανταλλάσσονται να είναι αποδεκτά στο περιβάλλον κάθε περιοχής διαχείρισης.

4.2.2.4 Υπηρεσίες Διαχείρισης και Συντονισμού

Η βασική αρμοδιότητα των Υπηρεσιών Διαχείρισης και Συντονισμού εστιάζεται στη διαχείριση και στον συντονισμό όλων των προαναφερθέντων εργαλείων/υπηρεσιών του ΣΔΤ. Βασική επιδίωξη αποτελεί η διασφάληση της ροής μεταξύ των υπηρεσιών για την επιτυχή ολοκλήρωση των απαιτούμενων διαδικασιών.

4.2.3 Ιδιωτικότητα

Η ραγδαία αύξηση των προσφερόμενων η/κ-ΥΙ έχει αναδείξει σε σημαντικό βαθμό τη σημασία της ιδιωτικότητας στις η/κ-συναλλαγές. Με τον όρο ιδιωτικότητα εννοούμε *το δικαίωμα μιας οντότητας να καθορίζει το χρόνο, τον τρόπο και το επίπεδο των πληροφοριών που προτίθεται να παραχωρήσει κατά την διάρκεια της επικοινωνίας της με μια άλλη άγνωστη πολλές φορές οντότητα. Επίσης έχει την δυνατότητα να θέσει περιορισμούς που αφορούν την επεξεργασία και την προσβασιμότητα των παρεχόμενων πληροφοριών"* [Westin67].

Γίνεται, λοιπόν, εύκολα κατανοητό το γεγονός ότι η ιδιωτικότητα συνδέεται άρρηκτα με την διαχείριση ταυτότητας των χρηστών διαδραματίζοντας έναν αποφασιστικό ρόλο στις διαδικασίες της. Επομένως, βασική απαίτηση για τον σχεδιασμό και υλοποίηση των συστημάτων διαχείρισης ταυτότητας αποτελεί η δημιουργία αποτελεσματικών, από επιχειρησιακή άποψη, συστημάτων που παράλληλα θα διασφαλίζουν και θα προστατεύουν την ιδιωτικότητα των χρηστών λαμβάνοντας υπόψη τους το σύνολο των πτυχών της, όπως είναι:

- *Ανωνυμία*, η οποία διασφαλίζει ότι ένας χρήστης έχει την δυνατότητα να χρησιμοποιεί μια ΥΙ χωρίς να απαιτείται να αποκαλύψει την ταυτότητά του.
- *Μη Συνδεσιμότητα*, η οποία διασφαλίζει ότι ένας χρήστης έχει την δυνατότητα να χρησιμοποιεί μια ΥΙ πολλές φορές χωρίς να είναι δυνατή η σύνδεση των συναλλαγών του.
- *Ψευδωνυμία*, η οποία διασφαλίζει ότι ένας χρήστης έχει την δυνατότητα να χρησιμοποιεί μια ΥΙ χωρίς να απαιτείται να αποκαλύψει την ταυτότητά του, αλλά συγχρόνως να είναι υπόλογος των πράξεων του.
- *Μοναδική Αυθεντικοποίηση (Single Sign-On (SSO))*, η οποία επιτρέπει στον χρήστη να χρησιμοποιεί πολλαπλές ΥΙ οι οποίες προσφέρονται από διαφορετικούς οργανισμούς πραγματοποιώντας τη διαδιακασία πιστοποίησης μόνο μία φορά.
- *Μοναδική Έξοδο* (Single Logout (SLO)), η οποία επιτρέπει στον χρήστη να τερματίζει την πρόσβασή του σε ΥΙ οι οποίες προσφέρονται από διαφορετικούς οργανισμούς πραγματοποιώντας την διαδικασία εξόδου μόνο μία φορά.

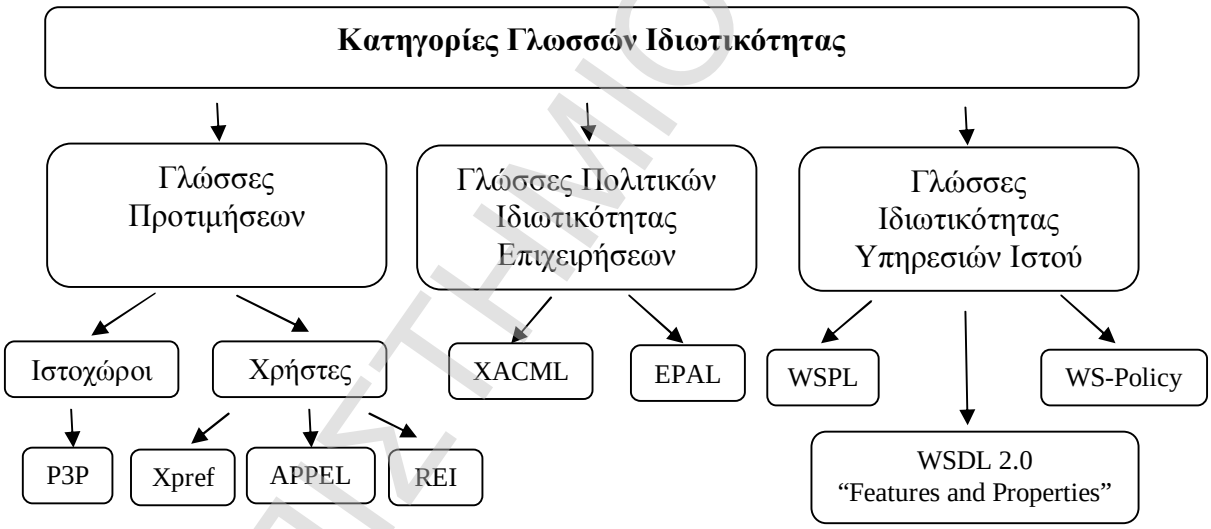
Ένας αποτελεσματικός και ευέλικτος τρόπος για την προστασία της ιδιωτικότητας είναι η διαχείρισή της μέσω της χρήσης *Πολιτικών Ιδιωτικότητας* [Polemi06c]. Η ερευνητική και επιχειρηματική κοινότητα σε παγκόσμια κλίμακα έχει προτείνει μια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

σειρά προτύπων (γλωσσών) τα οποία μπορούν να χρησιμοποιηθούν για να εκφράσουν τις πολιτικές αυτές.
Στα πλαίσια της διατριβής πραγματοποιήθηκε η ταξινόμηση των *Γλωσσών Πολιτικών Ιδιωτικότητας* σε τρεις βασικές κατηγορίες. Η κατηγοριοποίηση που λαμβάνει χώρα γίνεται με βάση το σκοπό υλοποίησης αλλά και χρήσης κάθε γλώσσας. Στην πρώτη κατηγορία περιλαμβάνονται γλώσσες που δίνουν την δυνατότητα έκφρασης συγκεκριμένων προτιμήσεων από μέρους των συμβαλλόμενων μερών. Στην δεύτερη κατηγορία περιλαμβάνονται γλώσσες που χρησιμοποιούνται για τον καθορισμό των Πολιτικών Ιδιωτικότητας μιας επιχείρησης. Τα τελευταία χρόνια έχουν προταθεί ορισμένες γλώσσες για Υπηρεσίες Ιστού. Οι γλώσσες αυτές αποτελούν την τρίτη κατηγορία και παρουσιάζουν ποικίλους βαθμούς εκφραστικότητας και πολυπλοκότητας.

4.2.3.1 Ταξινόμηση Γλωσσών Ιδιωτικότητας

Στο παρόν κεφάλαιο παρουσιάζεται η προτεινόμενη κατηγοριοποίηση, όπως απεικονίζεται στο Σχήμα 80, με βάση τον σκοπό υλοποίησης αλλά και χρήσης κάθε γλώσσας παραθέτοντας τις πιο αντιπροσωπευτικές γλώσσες που ανήκουν σε καθεμία από τις προτεινόμενες κατηγορίες.



Σχήμα 80: Κατηγοριοποίηση Γλωσσών Ιδιωτικότητας

4.2.3.1.1 Γλώσσες Προτιμήσεων

Η πιο αντιπροσωπευτική γλώσσα της κατηγορίας αυτής αποτελεί η P3P (Platform for Privacy Preferences 1.0) [Cranor02]. Η P3P έχει καθιερωθεί ως το πρότυπο για την έκφραση του είδους των δεδομένων αλλά και του σκοπού συλλογής των δεδομένων από μέρους των Ιστοχώρων. Η μέθοδος κωδικοποίησης των πρακτικών συλλογής και χρήσης των δεδομένων που παρέχεται είναι σε μορφή XML, στοιχείο που την καθιστά αυτόματα ανεξάρτητη πλατφόρμας και υπολογιστικού συστήματος.
Στα πλαίσια της προδιαγραφής P3P μέσω του καθορισμού της γλώσσας προτιμήσεων P3P Preference Exchange Language (APPEL) [Marchiori02] παρέχεται η δυνατότητα και στον χρήστη να εκφράσει τις προτιμήσεις ιδιωτικότητάς του. Ο στόχος είναι οι προτιμήσεις που εκφράζονται σε APPEL να συγκριθούν με τις προτιμήσεις που εκφράζονται σε P3P προκειμένου ένας χρήστης να αποφασίσει αν είναι διατεθειμένος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

να αποκαλύψει τα δεδομένα που του ζητούνται από τον Ιστοχώρο ώστε να ανακτήσει πρόσβαση σε αυτόν.
Παρά το γεγονός όμως ότι η προδιαγραφή P3P επιτρέπει τόσο στον χρήστη όσο και στους Ιστοχώρους να εκφράσουν τις προτιμήσεις τους, το μοντέλο αυτό δεν έχει βρει ακόμα ευρεία αποδοχή. Οι βασικοί λόγοι [Kolari05] στους οποίους οφείλεται το γεγονός αυτό συνοψίζονται στους ακόλουθους:

i. οι διαθέσιμες γλώσσες ώστε να περιγραφούν οι προτιμήσεις ιδιωτικότητας των χρηστών δεν είναι αρκετά εκφραστικές,
ii. οι χρήστες δεν εμπιστεύονται τις πολιτικές P3P που ανακοινώνονται από τους Ιστοχώρους. Το στοιχείο αυτό πηγάζει από το γεγονός ότι η P3P δεν παρέχει κάποιον ενσωματωμένο μηχανισμό που να εξασφαλίζει ότι οι Ιστοχώροι ενεργούν σύμφωνα με τις πολιτικές που ανακοινώνουν, και
iii. η προδιαγραφή P3P δεν παρέχει μια ολοκληρωμένη άποψη των διαθέσιμων μηχανισμών προστασίας της ιδιωτικότητας στο χρήστη.

Στα στοιχεία αυτά έρχονται να προστεθούν και τα προβλήματα που δημιουργούνται από την διαλειτουργικότητα μεταξύ της P3P και της APPEL. Τα προβλήματα αυτά πηγάζουν από τους περιορισμούς που παρουσιάζει η APPEL, οι οποίοι οφείλονται:

- στην έλλειψη λογικών συνδέσμων,
- στην δυνατότητα καθορισμού κανόνων που δεν επιτρέπουν την περιγραφή του τι δεν είναι αποδεκτό αλλά μόνο του τι είναι αποδεκτό, και
- στην ταύτιση των κριτηρίων που χρησιμοποιούνται.

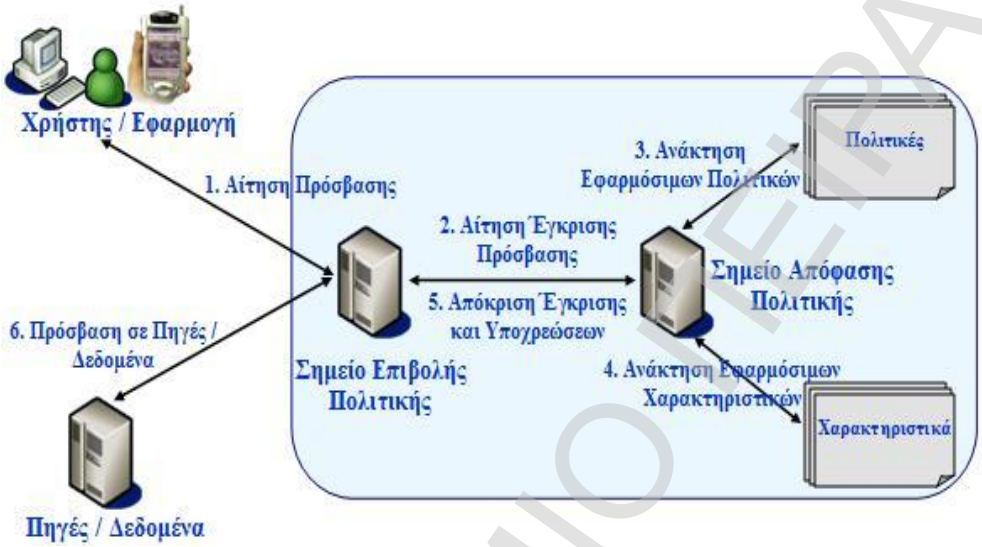
Προκειμένου λοιπόν να καλυφθεί ένα μέρος ή το σύνολο των αδυναμιών που προκύπτουν από την χρήση της APPEL, έχουν προταθεί ορισμένες νέες γλώσσες. Μια προτεινόμενη γλώσσα είναι η Xpref [Agrawal03] η οποία βασίζεται στην XPath [Clark99]. Η Xpref έχει επιτύχει να υιοθετήσει την πλήρη λειτουργικότητα της APPEL, αποφεύγοντας παράλληλα κάποια από τα μειονεκτήματά της. Ένα βασικό πλεονέκτημά της σε σχέση με την APPEL αποτελεί το γεγονός της χρήσης λογικών συνδέσμων (AND, OR) και τελεστών ισότητας (=, !=) ώστε να καθοριστούν οι απαιτήσεις ταύτισης.
Παρόλα αυτά όμως η Xpref, όπως και η APPEL, παρουσιάζει περιορισμένη εκφραστικότητα. Πιο συγκεκριμένα, δεν υποστηρίζει την έκφραση τυχόν «υποχρεώσεων» που πρέπει να διέπουν μια συναλλαγή ή τον δυναμικό καθορισμό και την αυτοματοποιημένη διαπραγμάτευση των κοινοποιημένων πολιτικών. Για την διευθέτηση των ζητημάτων αυτών έχουν προταθεί άλλες γλώσσες όπως η REI [Kagal03, Moses05].

4.2.3.1.2 Γλώσσες Πολιτικών Ιδιωτικότητας Επιχειρήσεων

Οι δυο πιο διαδεδομένες γλώσσες που περιλαμβάνονται στην κατηγορία αυτή είναι η Enterprise Privacy Authorization Language (EPAL) [Ashley03] της IBM και η eXtensible Access Control Markup Language (XACML) [Moses05] του OASIS. Βασικό χαρακτηριστικό γνώρισμα και των δύο γλωσσών αποτελεί το γεγονός ότι είναι ανεξάρτητες πλατφόρμας, στοιχείο που οφείλεται στην XML αναπαράσταση τους.
Η XACML αποτελεί ένα πρότυπο του OASIS και η χρήση της συνοψίζεται σε δύο βασικές κατευθύνσεις ως μια Γλώσσα Πολιτικών και ως μιας γλώσσα ελέγχου πρόσβασης αίτησης/απόκρισης. Στην πρώτη περίπτωση στόχος της είναι η περιγραφή των γενικών απαιτήσεων ελέγχου πρόσβασης, ενώ στην δεύτερη περίπτωση, η χρήση της αποσκοπεί στην δημιουργία αιτήσεων λαμβάνοντας υπόψη ορισμένα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

χαρακτηριστικά ώστε να ελεγχθεί αν πρέπει να επιτραπεί ή όχι μια ενέργεια πάνω σε ένα σύνολο δεδομένων ή πηγών. Την αίτηση αυτή ακολουθεί μια απόκριση που ενημερώνει το αποτέλεσμα της αιτήσεως.
Η EPAL αποτελεί μια γλώσσα που αναπτύχθηκε από την IBM και έχει προταθεί στον W3C από τον Νοέμβριο του 2003 για προτυποποίηση. Οι αντικειμενικοί της στόχοι είναι δυο. Η παροχή της δυνατότητας κωδικοποίησης των Πολιτικών και η εισαγωγή μιας γλώσσας επιβολής των επιλεγμένων Πολιτικών.



Σχήμα 81: Μοντέλο Επιβολής Πολιτικής

Τόσο η XACML όσο και η EPAL [Anderson05] χρησιμοποιούν το ίδιο μοντέλο επιβολής Πολιτικών, το οποίο απεικονίζεται στο Σχήμα 81. Στο μοντέλο αυτό ένας χρήστης/εφαρμογή επιδιώκει να αποκτήσει πρόσβαση σε ένα σύνολο πηγών/δεδομένων, υποβάλλοντας ένα αίτημα στο *Σημείο Επιβολής Πολιτικής* (Policy Enforcement Point (PEP)) (ενέργεια 1). Το συστατικό αυτό διαμορφώνει μια αίτηση που περιέχει τα χαρακτηριστικά της αίτησης του χρήστη/εφαρμογής. Τα χαρακτηριστικά που περιέχονται στην νέα αίτηση είναι η ταυτότητα του αιτούντος, η πηγή για την οποία ζητείται η πρόσβαση, η ενέργεια που θα εκτελεστεί στην πηγή και ο σκοπός πρόσβασης. Η αίτηση έγκρισης της πρόσβασης υποβάλλεται στο *Σημείο Απόφασης Πολιτικής* (Policy Decision Point (PDP)) (ενέργεια 2). Το συστατικό αυτό μόλις λάβει την αίτηση, ανακτά τις εφαρμόσιμες πολιτικές (ενέργεια 3), μαζί με τα πρόσθετα στοιχεία που απαιτούνται για την αξιολόγηση των πολιτικών (ενέργεια 4) και αξιολογεί τις πολιτικές ώστε να καθορίσει την απόφαση έγκρισης. Η ληφθείσα απόφαση επιστρέφεται στο Σημείο Επιβολής Πολιτικής (ενέργεια 5) το οποίο επιτρέπει ή απαγορεύει την πρόσβαση στον χρήστη/εφαρμογή (ενέργεια 6).
Οι δύο γλώσσες παρουσιάζουν μια σειρά από ομοιότητες και διαφορές (Anderson, 2005), όμως σε γενικές γραμμές μπορεί να θεωρηθεί ότι η EPAL προσφέρει ένα υποσύνολο της λειτουργικότητας της XACML. Η XACML στην ουσία αναπτύχθηκε για να προσφέρει έλεγχο επιχειρηματικής πρόσβασης διευθετώντας ζητήματα τα οποία προέκυπταν στα διανεμημένα συστήματα. Επίσης περιέχει ένα σύνολο από στοιχεία τα οποία δεν περιέχονται στην EPAL, περιορίζοντας την δυνατότητα της να εκφράσει ευέλικτες και εξελικτικές Πολιτικές.
Ένας σημαντικός περιορισμός της EPAL αποτελεί το γεγονός ότι δεν πρόκειται για μια γλώσσα ελέγχου πρόσβασης γενικού σκοπού. Κάθε αίτημα πρόσβασης πρέπει να περιέχει τον σκοπό της πρόσβασης, στοιχείο το οποίο δεν είναι απαιτούμενο στην

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

περίπτωση της XACML, καθιστώντας την μη ικανή να ανταποκριθεί στο σύνολο των περιπτώσεων.
Ορισμένες από τις αδυναμίες της EPAL σε σχέση με την XACML μπορούν να συνοψιστούν στις ακόλουθες:

- αδυναμία να υποστηρίξει πρόσθετους τύπους δεδομένων,
- αδυναμία περιγραφής επιχειρηματικών πολιτικών από την στιγμή που δεν μπορούν να υποστηριχτούν διανεμημένες πολιτικές.

Αντίστοιχα, η EPAL πλεονεκτεί της XACML στην χρήση μη συγκεκριμένου λεξιλογίου από μέρους των χαρακτηριστικών των πολιτικών και των κανόνων και στην χρήση ιεραρχίας κατηγοριών. Το γεγονός όμως αυτό δεν προσφέρει καμία πρόσθετη λειτουργικότητα σε σχέση με την XACML καθιστώντας την προτυποποίησή της έναν δύσκολο στόχο.

4.2.3.1.3 Γλώσσες Ιδιωτικότητας Υπηρεσιών Ιστού

Οι Υπηρεσίες Ιστού προκειμένου να επικοινωνήσουν μεταξύ τους απαιτούν επιμέρους πληροφορίες που δεν περιγράφονται σε ένα έγγραφο WSDL [Christensen01]. Οι πληροφορίες αυτές σχετίζονται με πτυχές ή στοιχεία που αφορούν ζητήματα όπως είναι ο καθορισμός των απαιτούμενων μηχανισμών εμπιστευτικότητας και των απαραίτητων στοιχείων πιστοποίησης, ποιότητας υπηρεσιών και ιδιωτικότητας. Οι *Γλώσσες Ιδιωτικότητας των Υπηρεσιών Ιστού* αποτελούν την τρίτη κατηγορία των γλωσσών και έχουν ως απώτερο στόχο την περιγραφή του συνόλου των στοιχείων των Υπηρεσιών Ιστού που απαρτίζουν τα μη – λειτουργικά χαρακτηριστικά μιας υπηρεσίας, διευκολύνοντας με αυτόν τον τρόπο την διαλειτουργικότητα, την προσβασιμότητα και την αξιοπιστία των Υπηρεσιών.
Μέχρι σήμερα [Anderson05] δεν υπάρχει μια πρότυπη γλώσσα η οποία μπορεί να χρησιμοποιηθεί για την έκφραση των Πολιτικών Υπηρεσιών Ιστού. Οι πιο ευρέως γνωστές και χρησιμοποιούμενες γλώσσες ακολουθούν την ακόλουθη δομή: μια Πολιτική αποτελεί έναν συνδυασμό κατηγορημάτων ή ισχυρισμών, οι οποίοι διευκρινίζουν τις αποδεκτές τιμές για ένα ή περισσότερα χαρακτηριστικά. Οι πιο αντιπροσωπευτικές γλώσσες της κατηγορίας αυτής ποικίλουν ως προς την εκφραστικότητα και την πολυπλοκότητα και μπορούν να συνοψιστούν στην Web Service Policy Language (WSPL) [Moses03, Anderson04], στην πρόταση της Oracle για προσθήκη “συνθετικών” (Λογικών Συνδέσμων) στην WSDL 2.0 “Features and Properties” [Yalcinalp04] και, τέλος, στο Web Services Policy Framework (WS-Policy) [Schlimmer04].
Η Web Services Policy Language (WSPL) [Anderson04] αναπτύχθηκε από την Τεχνική Επιτροπή OASIS XACML και το συντακτικό της αποτελεί ένα υποσύνολο του προτύπου XACML. Η χρήση της εστιάζεται στον καθορισμό των Πολιτικών των Υπηρεσιών Ιστού, χρησιμοποιώντας πρότυπους τύπους δεδομένων και τελεστών για την έκφραση των παραμέτρων. Ιδιαίτερα σημαντικό είναι το γεγονός ότι επιτρέπει την συγχώνευση δυο Πολιτικών, δημιουργώντας μια τρίτη Πολιτική η οποία ικανοποιεί τις απαιτήσεις των δυο αρχικών, υποθέτοντας βέβαια ότι μια τέτοια Πολιτική υφίσταται.
Η πρόταση της Oracle για προσθήκη “συνθετικών” (Λογικών Συνδέσμων) στην WSDL 2.0 “Features and Properties (F & P)” [Yalcinalp04] έχει ως στόχο να ενισχύσει το τμήμα των χαρακτηριστικών γνωρισμάτων που είναι διαθέσιμα στην WSDL 2.0 ώστε να διευθετηθούν πλήρως οι ανάγκες των Υπηρεσιών Ιστού για γνωστοποίηση των απαιτήσεών τους. Η F & P με την ενίσχυση αυτή επιτρέπει στις Υπηρεσίες Ιστού να κοινοποιήσουν τα χαρακτηριστικά τους χωρίς όμως να παρέχεται

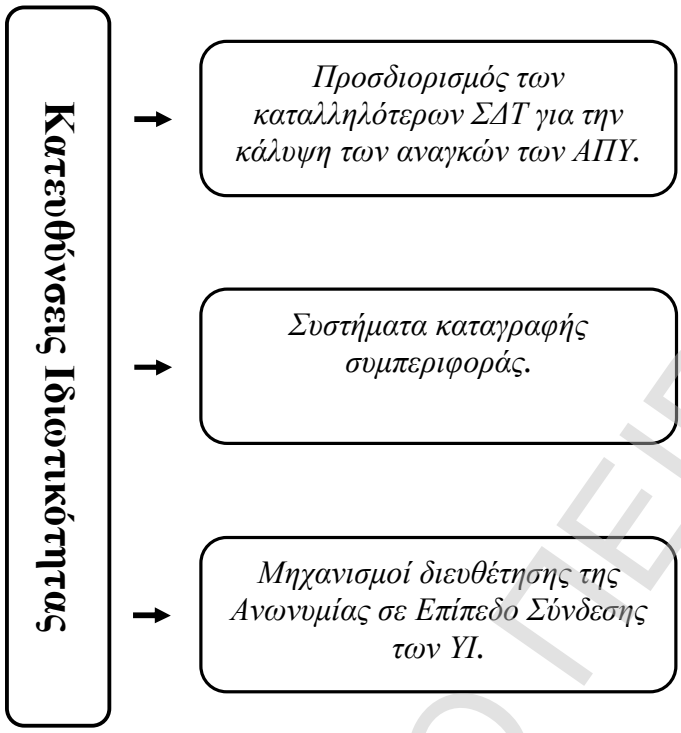
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

σημαντική εκφραστικότητα εξαιτίας της έλλειψης τελεστών για τον συνδυασμό των ισχυρισμών.
Το Web Services Policy Framework (WS-Policy) [Schlimmer04] παρέχει μια εύκαμπτη και εκτενής γραμματική για την έκφραση των ικανοτήτων, των απαιτήσεων, και των γενικών χαρακτηριστικών των οντοτήτων ενός XML Υπηρεσιο-στρεφούς συστήματος. Η WS-Policy καθορίζει το πλαίσιο για την έκφραση αυτών των ιδιοτήτων ως πολιτικές. Κάθε πολιτική αποτελεί μια συλλογή εναλλακτικών πολιτικών, ενώ κάθε εναλλακτική πολιτική αποτελεί μια συλλογή πολιτικών ισχυρισμών.
Η WS-Policy προκειμένου να δηλώσει τους ισχυρισμούς αυτούς χρησιμοποιεί λεξιλόγιο το οποίο το δανείζεται από γλώσσες όπως είναι η WS-SecurityPolicy [Nadalin04], η WS-ReliableMessaging Policy [Bilorusets05] και η WS-Trust [Bohren05] ώστε να περιγράψει τους ισχυρισμούς που αντιστοιχούν σε κάθε ένα από τα πεδία που περιγράφουν οι συγκεκριμένες γλώσσες. Παρά το γεγονός όμως ότι η WS-Policy παρέχει την απαιτούμενη γραμματική δεν καθορίζει τον τρόπο με τον οποίο μπορούν εκφραστούν οι ισχυρισμοί αυτοί.
Η WS-PolicyConstraints [Devaraj05] παρέχει το συντακτικό και την σημασιολογία μιας γλώσσας για τον καθορισμό, την επαλήθευση, τον συνδυασμό και την εφαρμογή των περιορισμών αυτών. Η δημιουργία της βασίστηκε κυρίως στην OASIS Standard eXtensible Access Control Markup Language, ενώ το βασικό της χαρακτηριστικό είναι το γεγονός ότι δεν εξαρτάται από την γλώσσα (όπως η WS-SecurityPolicy) η οποία δανείζει το λεξιλόγιο.
Για την έκφραση των περιορισμών των πολιτικών έχουν προταθεί ένα σύνολο από σημασιολογικές γλώσσες όπως η Ontology Web Language (OWL) [Schreiber04, Verma05] και η Resource Description Framework (RDF) [Beckett, Prudhommeaux04]. Οι γλώσσες [Devaraj05] αυτές παρά το γεγονός ότι έχουν την δυνατότητα να εκφράσουν την σημασιολογία του χρησιμοποιούμενου λεξιλογίου, έχουν ως μειονέκτημα την αδυναμία να υποστηρίξουν αριθμητικούς τελεστές σύγκρισης.

4.3 Ανοικτά Προβλήματα

Ο δεύτερος άξονας της διατριβής πραγματεύεται μια σειρά ζητημάτων τα οποία σχετίζονται με την διαχείριση ταυτότητας και την προστασία της ιδιωτικότητας των οντοτήτων που μετέχουν στις η/κ-συναλλαγές. Πιο συγκεκριμένα, ο άξονας αυτός κινείται σε τρεις ανεξάρτητες αλλά πλήρως αλληλένδετες κατευθύνσεις, όπως απεικονίζονται στο Σχήμα 82. Κάθε μία από τις κατευθύνσεις αυτές εστιάζεται στην επίλυση ενός συγκεκριμένου προβλήματος.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 82: Κατευθύνσεις Άξονα Ιδιωτικότητας

Στις μέρες μας, οι σχεδιαστές των αρχιτεκτονικών προσανατολισμένων σε υπηρεσίων (ΑΠΥ) πλέον βρίσκονται αντιμέτωποι με ένα νέο πρόβλημα το οποίο σχετίζεται με τον προσδιορισμό των ΣΔΤ τα οποία είναι καταλληλότερα για να καλύψουν τις ανάγκες των ΑΠΥ που προτίθενται να αναπτύξουν ή έχουν ήδη αναπτύξει [Modinis06]. Η υιοθέτηση της καταλληλότερης λύσης θα πρέπει να γίνει με τρόπο που να μην εισάγει πρόσθετη πολυπλοκότητα στον σχεδιασμό και την υλοποίηση της ΑΠΥ ή να μην λαμβάνει υπόψη τις συγκεκριμένες πτυχές της ιδιωτικότητας. Στα πλαίσια της πρώτης κατεύθυνσης για την επίλυση του συγκεκριμένου προβλήματος μελετήθηκαν και αναλύθηκαν ένα σύνολο Συστημάτων Διαχείρισης Ταυτότητας (ΣΔΤ). Από τη μελέτη αυτή διαπιστώθηκε η ύπαρξη μιας πληθώρας λύσεων ΣΔΤ τα οποία παρουσιάζουν σημαντική έλλειψη ομοιογένειας.

Επιπρόσθετα, με την αύξηση των η/κ-συναλλαγών στον σύγχρονο ψηφιακό κόσμο ένα βασικό πρόβλημα το οποίο εντοπίστηκε είναι η έλλειψη ενός συστήματος καταγραφής συμπεριφοράς που να «σέβεται» την ιδιωτικότητα των χρηστών και να λειτουργεί σε συνδυασμό με τα ΣΔΤ [Carrara07]. Το πρόβλημα αυτό εξετάστηκε στα πλαίσια της δεύτερης κατεύθυνσης του παρόντος άξονα, όπου έγινε μελέτη ενός συνόλου συστημάτων καταγραφής συμπεριφοράς και ΣΔΤ. Το βασικό στοιχείο που διαπιστώθηκε είναι η σημασία που έχει η καταγραφή και αποτύπωση της συμπεριφοράς που επιδεικνύεται από τους χρήστες στα πλαίσια των συναλλαγών που αυτοί εκτελούν με τις ΥΙ και του ρόλου που αυτή μπορεί να διαδραματίσει για την ενίσχυση της ιδιωτικότητας

Παράλληλα με τις προαναφερόμενες κατευθύνσεις, ένα σημαντικό πρόβλημα είναι και η έλλειψη επαρκών μηχανισμών διευθέτησης της Ανωνυμίας σε Επίπεδο Σύνδεσης οι οποίοι θα είναι εφαρμόσιμοι στην περίπτωση των ΥΙ. Η τρίτη κατεύθυνση πραγματεύεται το συγκεκριμένο ζήτημα, αναδεικνύοντας την σημασία ύπαρξης και υιοθέτηση των μηχανισμών αυτών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

4.4 Συμπεράσματα

Το παρόν κεφάλαιο αποτέλεσε μια εισαγωγή για τον δεύτερο άξονα της διατριβής μελετώντας και αναλύοντας ένα σύνολο έννοιες που συνδέονται άρρηκτα με τη διαχείριση της ταυτότητας και την προστασία της ιδιωτικότητας των χρηστών. Παράλληλα, παρουσιάστηκε ο κεντρικός ρόλος που διαδραματίζουν τα ΣΔΤ για την επίτευξη των δύο προαναφερόμενων στόχων.
Τέλος, το κεφάλαιο αυτό εστιάστηκε στην περιγραφή των πραγματικών προβλημάτων με τα οποία έρχεται αντιμέτωπη η διατριβή στα πλαίσια του δεύτερου άξονα. Στις παραγράφους που ακολουθούν, γίνεται μια αναλυτικότερη παρουσίαση των προβλημάτων που έχουν εντοπιστεί και παραθέτονται οι λύσεις οι οποίες έχουν προταθεί για την διευθέτηση τους.

4.5 Αναφορές

[Yee06] G. Yee (editor). (2006). "*Privacy Protection for E-Services*", IDEA Group Publishing, book, 2006.
[Buell03] D. A. Buell, R. Sandhu. (2003). "*Identity management*", IEEE Internet Computing, v. 7, no. 6, November/December 2003, pp. 26-28.
[Claub] S. Claub, M. Kohntopp. (2001). "*Identity management and its support of multilateral security*", Computer Networks, 37(2), 205-219.
[Clauss05] S. Clauss, D. Kesdogan, T. Kölsch. (2005). "*Privacy enhancing identity management: protection against re-identification and profiling*", Proceedings of the 2005 workshop on Digital identity management, November 11-11, 2005, Fairfax, VA, USA.
[Pato03] J. Pato, J. Rouault. (2003). "*Identity management: The drive to federation*", April, 05, 2004,
http://devresource.hp.com/drc/technical_white_papers/IdentityMgmt_Federation.pdf
[Haddad08] W. Haddad. (2008). "*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*", Network Working Group, IETF Trust.
[Papastergiou07b] S. Papastergiou, A. Karantjias, D. Polemi. (2007), "*A Federated Privacy-Enhancing Identity Management System (FPE-IMS)*". 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), 3-7 September 2007, Athens.
[Westin67] A. Westin. (1967). "*Privacy and Freedom*", Atheneum Press, NY, USA, 1967.
[Polemi06c] D. Polemi, S. Papastergiou. (2006). "*Achievements and future direction in security policies*", Electronic Democracy Challenges of the digital era, 2nd National Conference with International Participation, Athens, March, 16-17, 2006, ACCI.
[Cranor02] L. Cranor et Al. (2002). "*The Platform for Privacy Preferences 1.0 (P3P1.0)*", Specification, W3C Recommendation, 16 April 2002. http://www.w3.org/TR/P3P/.
[Marchiori02] M. Marchiori, L. Cranor, M. Langheinrich. (2002). "*A P3P Preference Exchange Language 1.0 (APPEL1.0)*", W3C Working Draft.
[Kolari05] P. Kolari et Al. (2005). "*Enhancing Web Privacy Protection through Declarative Policies*", Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Agrawal03] R. Agrawal et Al. (2003). "*An XPath-based Preference Language for P3P*", Copyright is held by the author/owner(s). *WWW2003*, May 20–24, 2003, Budapest, Hungary. ACM 1581136803/03/0005.
[Clark99] J. Clark et Al. (1999). "*XML Path Language (XPath) Version 1.0*", W3C Recommendation, November 1999.
[Kagal03] L. Kagal, T. Finin, A. Joshi. (2003). "*A policy based approach to security for the semantic web*", 2nd International Semantic Web Conference (ISWC2003), September 2003.
[Moses05] T. Moses. (2005). "*eXtensible Access Control Markup Language (XACML)*", Version 2.0, OASIS Standard.
[Ashley03] P. Ashley et Al. (2003). "*Enterprise Privacy Authorization Language (EPAL)*", Version 1.2, the version submitted to the W3C. http://www.w3.org/Submission/2003/SUBMEPAL-20031110/.
[Anderson05] A. Anderson. (2005). "*A Comparison of Two Privacy Policy Languages: EPAL and XACML*", SMLI TR-2005-147 September 2005.
[Christensen01] E. Christensen et Al. (2001). "*Web Services Description Language (WSDL) 1.1*", W3C Note. 15 March 2001, http://www.w3.org/TR/wsdl.
[Anderson05] A. Anderson. (2005). "*WS-PolicyConstraints: A Domain-Independent Web Services Policy Assertion Language*", Sun Microsystems Laboratories 3 November 2005.
[Moses03] T. Moses, ed.. (2003). "*XACML profile for Web-services, also known as the Web Services Policy Language(WSPL)*", Working Draft 04, 29 September 2003.
[Anderson04] A. Anderson. (2004). "*An Introduction to the Web Services Policy Language*", Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04). 8 June 2004. Available http://research.sun.com/projects/xacml/Policy2004.pdf
[Yalcinalp04] U. Yalcinalp. (2004). "*Proposal for adding Compositors to WSDL 2.0*", 26 January 2004, http://lists.w3.org/Archives/Public/www-ws-desc/2004Jan/0153.html
[Schlimmer04] J. Schlimmer, ed.. (2004). "*Web Services Policy Framework (WS-Policy)*", September 2004, http://www-128.ibm.com/developerworks/webservices/library/specification/ws-polfram/
[Nadalin04] A. Nadalin, et al. (2004). "*Web Services Security: SOAP Message Security 1.0*", WS-Security 2004, March 2004.
[Bilorusets05] R. Bilorusets, et al. (2005). "*Web Services Reliable Messaging Protocol (WS-ReliableMessaging)*", February 2005.
[Bohren05] J. Bohren, et al. (2005). "*Web Services Trust Language (WS-Trust)*", February 2005.
[Devaraj05] B. Devaraj, A. Anderson. (2005). "*XACML-Based Web Services Policy Constraint Language (WS-PolicyConstraints)*", Working Draft 06, 24 October 2005.
[Schreiber04] G. Schreiber, et al. (2004). "*Web Ontology Language*", W3C Recommendation 10 February 2004. Available http://www.w3.org/TR/owl-ref/
[Verma05] K. Verma, R. Akkiraju, R. Goodwin. (2005). "*Semantic Matching of Web Service Policies*", 2005 IEEE International Conference on Web Services (ICWS 2005).
[Beckett] D. Beckett, et al. "*Resource Description Framework (RDF)*", http://www.w3.org/RDF/

ENEA-TRIO-FIPA

[Prudhommeaux04] E. Prud'hommeaux. (2004). "*RDF For Web Service Policy Assertions Workshop on Constraints and Capabilities for Web Services*", 20 August 2004, http://www.w3.org/2004/08/20-ws-pol-pos/
[Modinis06] Modinis study on identity management. Identity management issue report, (2006).
[Carrara07] E. Carrara, G. Hogben (Editors). (2007). "*Reputation-based Systems: a security analysis*", ENISA Position Paper No. 2, October 2007.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

5 Προσδιορισμός των καταλληλότερων ΣΔΤ για την κάλυψη των αναγκών των ΑΠΥ

Στο πλαίσιο του παρόντος κεφαλαίου διαπιστώνεται η ύπαρξη μιας μεγάλης ποικιλίας λύσεων διαχείρισης ταυτότητας τα οποία χαρακτηρίζονται κατά κύριο λόγο από ανομοιογένεια. Το κεφάλαιο αυτό παραθέτει υπάρχουσες ταξινομήσεις των Συστημάτων Διαχείρισης Ταυτότητας (ΣΔΤ) παρουσιάζοντας χαρακτηριστικά παραδείγματα για κάθε μία κατηγορία.
Το πρόβλημα, όμως που προκύπτει αφορά τον προσδιορισμό του καταλληλότερου πλαισίου ή λύσης ΣΔΤ που θα μπορεί να καλύψει αποτελεσματικά τις ανάγκες κάθε Αρχιτεκτονικής Προσανατολισμένης στις Υπηρεσίες (ΑΠΥ). Για το σκοπό αυτό στο παρόν κεφάλαιο προτείνεται και παρουσιάζεται μια ταξινόμηση των σχεδιαστικών λύσεων των ΑΠΥ με σεβασμό στον τρόπο με τον οποίο η σχέση εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων, χρηστών και ΑΠΥ, διαμορφώνεται επιτρέποντας στον χρήστη την πρόσβαση στις προσφερόμενες υπηρεσίες. Η ταξινόμηση διευκρινίζει ποιές ακριβώς σχεδιαστικές λύσεις διαχείρισης ταυτότητας πρέπει να υιοθετηθούν για καθεμία από τις προσδιορισμένες κατηγορίες.

5.1 Εισαγωγή

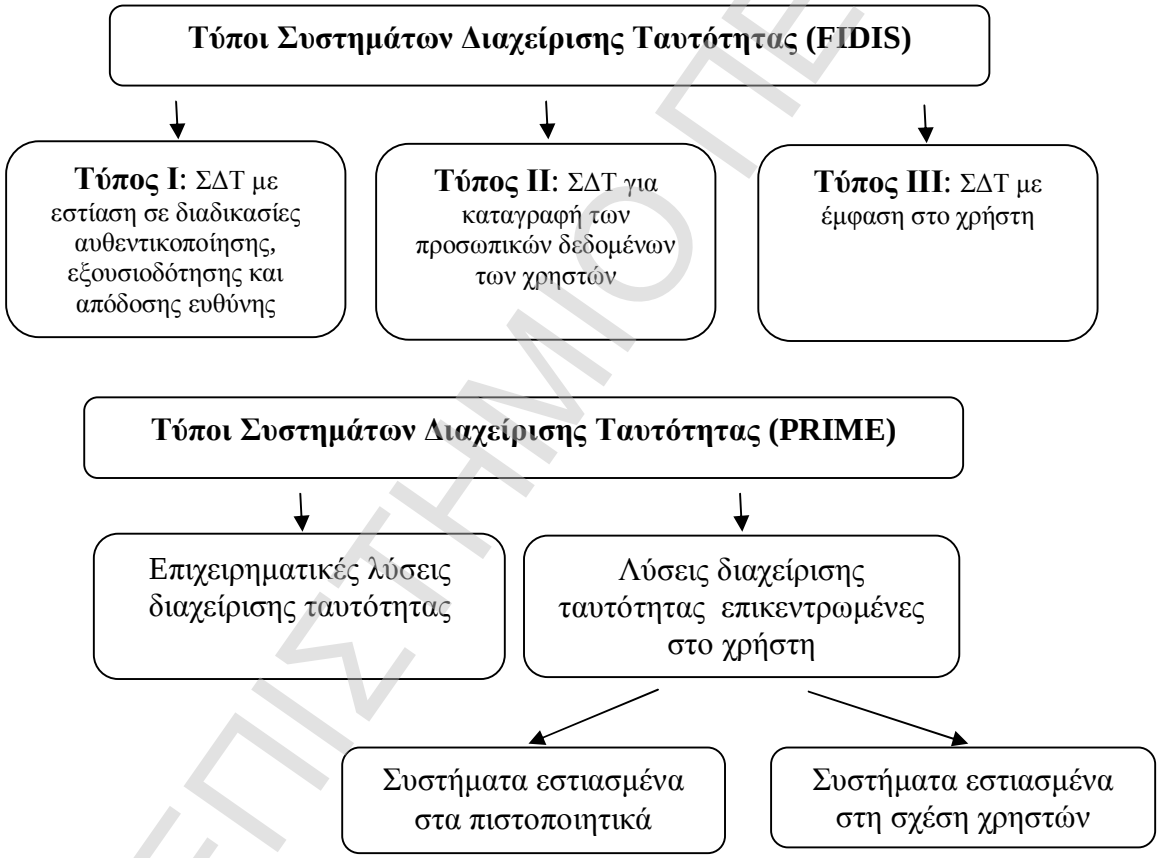
Στις μέρες μας, η ανάγκη για η/κ-συναλλαγές οι οποίες δίνουν ιδιαίτερη έμφαση στην ιδιωτικότητα εγείρει σημαντικά ζητήματα, όπως είναι η διαχείριση της ταυτότητας τα οποία οι Αρχιτεκτονικές Προσανατολισμένες στις Υπηρεσίες (ΑΠΥ) πρέπει να λάβουν υπόψη τους και να διευθετήσουν. Κοινή πρακτική αποτελεί η υιοθέτηση πολιτικών ιδιωτικότητας ως μέσο για την αποτύπωση των δυνατοτήτων και των απαιτήσεων του συνόλου των οντοτήτων που μετέχουν στις συναλλαγές. Εντούτοις, οι πολιτικές ιδιωτικότητας δεν αποτελούν μια πλήρη λύση διαχείρισης ταυτότητας από μόνες τους, από την στιγμή που δεν υλοποιούν αλλά ούτε και εγγυώνται τις επιχειρησιακές διαδικασίες που απαιτεί ένα τέτοιο σύστημα.
Η ερευνητική και επιχειρηματική κοινότητα έχει προσδιορίσει μια μεγάλη ποικιλία λύσεων διαχείρισης ταυτότητας τα οποία χαρακτηρίζονται από ανομοιομορφία και διαφορετικές προσεγγίσεις μιας κοινής διαδικασίας. Χαρατηριστικά παραδείγματα τέτοιων λύσεων αποτελούν το Liberty Alliance [LibertyAlliance], το WS-Federation [Lockhart06], το SAML [SAML05] και το Open Mobile Alliance (OMA) [OMA06]. Σε αυτήν την ποικιλομορφία των λύσεων, ένας σχεδιαστής μιας ΑΠΥ αντιμετωπίζει πλέον το πρόβλημα του προσδιορισμού του καταλληλότερου πλαισίου ή λύσης που θα μπορεί να καλύψει τις ανάγκες της ΑΠΥ που σχεδιάζει, χωρίς να εισάγεται πρόσθετη πολυπλοκότητα τόσο στο σχεδιασμό όσο και στην υλοποίησή της αλλά και λαμβάνοντας παράλληλα υπόψη συγκεκριμένες πτυχές της ιδιωτικότητας.
Για την κάλυψη του συγκεκριμένου προβλήματος έχει προταθεί μια ταξινόμηση των σχεδιαστικών λύσεων των ΑΠΥ με σεβασμό στον τρόπο με τον οποίο η σχέση εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων, χρηστών και ΑΠΥ, διαμορφώνεται επιτρέποντας στον χρήστη την πρόσβαση στις προσφερόμενες υπηρεσίες. Η ταξινόμηση διευκρινίζει ποιές ακριβώς σχεδιαστικές λύσεις διαχείρισης ταυτότητας πρέπει να υιοθετηθούν για καθεμία από τις προσδιορισμένες κατηγορίες. Η ταξινόμηση με τον τρόπο αυτό μπορεί να λειτουργήσει ως «οδηγός» για τους σχεδιαστές ΑΠΥ που θα τους βοηθήσει να υιοθετήσουν την καταλληλότερη λύση που ικανοποιεί τις ανάγκες της συγκεκριμένης ΑΠΥ που υλοποιούν.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Στις παραγράφους που ακολουθούν παρατίθενται οι υπάρχουσες ταξινομήσεις των Συστημάτων Διαχείρισης Ταυτότητας αλλά και η περιγραφή της προτεινόμενης ταξινόμησης των ΑΠΥ.

5.2 Υπάρχουσες Ταξινομήσεις των ΣΔΤ

Γενικές λύσεις για τη διαχείριση και τον έλεγχο της πρόσβασης στις υπηρεσίες έχουν προταθεί από διάφορα ερευνητικά προγράμματα και πρωτοβουλίες. Το πρόγραμμα FIDIS [Meints] ολοκλήρωσε μια σαφή ταξινόμηση των υπαρχουσών ΣΔΤ, η οποία παρατίθεται στο Σχήμα 83, λαμβάνοντας υπόψη τις υιοθετημένες επιχειρησιακές διαδικασίες. Στο πλαίσιο του συγκεκριμένου προγράμματος τρείς είναι οι βασικοί τύποι ΣΔΤ που προτάθηκαν.



Σχήμα 83: Ταξινομήσεις των Συστημάτων Διαχείρισης Ταυτότητας (ΣΔΤ)

Ο πρώτος τύπος δίνει έμφαση στην υλοποίηση μιας υποδομής η οποία επικεντρώνεται σε διαδικασίες όπως είναι η πιστοποίηση, η εξουσιοδότηση και η απόδοση ευθύνης. Αντιπροσωπευτικά παραδείγματα αποτελούν το Liberty Alliance (LA) [LibertyAlliance03] και το WS-Federation [Goodner07]. Το LA έχει αναπτύξει και υλοποιεί ανοιχτά πρότυπα που βασικός τους στόχος είναι η δημιουργία μιας δικτυακής υποδομής διαχείρισης ταυτότητας η οποία θα υποστηρίζει όλες τις υπάρχουσες και αναδυόμενες δικτυακές συσκευές πρόσβασης. Σε μια τέτοια υποδομή δίνεται η δυνατότητα να προστατεύεται η ιδιωτικότητα και η ασφάλεια των ευαίσθητων δεδομένων των εμπλεκομένων οντοτήτων, παρέχοντάς τους επίσης την δυνατότητα να διαχειριστούν τις επιχειρησιακές τους σχέσεις. Το WS-Federation, ακολουθώντας μια διαφορετική προσέγγιση, επιτρέπει τη δημιουργία ενός

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ομοσπονδιακού πλαισίου το οποίο είναι ικανό να ενσωματώσει τις υπάρχουσες υποδομές σε μια ομοσπονδία.

Ο δεύτερος τύπος αφορά την καταγραφή των προσωπικών δεδομένων των χρηστών από ένα σύστημα, μέσω της χρήσης λεπτομερών αρχείων καταγραφής ή βάσεων δεδομένων οι οποίες υποστηρίζουν εξατομικευμένες υπηρεσίες ή μέσω της ανάλυσης της συμπεριφοράς των χρηστών. Το ίδιο το πρόγραμμα FIDIS αποτελεί ένα παράδειγμα του συγκεκριμένου τύπου. Ο τελευταίος τύπος ΣΔΤ περιλαμβάνει λύσεις οι οποίες παρέχουν στον απλό χρήστη τη δυνατότητα να διαχειριστεί ο ίδιος πλήρως τις προσωπικές του πληροφορίες καθορίζοντας το ρόλο του και το ψευδώνυμο το οποίο θα χρησιμοποιήσει στις συναλλαγές του και με το οποίο θα αναγνωρίζεται από τα άλλα συστήματα.

Το πρόγραμμα PRIME [PRIME05, Ardagna06] προτείνει και υλοποιεί μια αρχιτεκτονική ενός συστήματος το οποίο δίνει πλήρη έλεγχο στο χρήστη να διαχειριστεί τα ευαίσθητα δεδομένα του ενώ παράλληλα διευθετεί σε σημαντικό βαθμό ζητήματα που αφορούν την ιδιωτικότητα και την απόδοση ευθύνης (accountability) των χρηστών στις ηλεκτρονικές συναλλαγές. Το πρόγραμμα αυτό παρουσιάζει μια νέα κατηγοριοποίηση των ΣΔΤ, όπως εμφανίζται στο Σχήμα 83, σε δύο επιμέρους κατηγορίες:

- Τις *επιχειρηματικές λύσεις διαχείρισης ταυτότητας*: Ο έλεγχος των δεδομένων ασκείται από την επιχείρηση αντί του μεμονωμένου χρήστη. Αυτές οι λύσεις εξυπηρετούν πρώτιστα τις επιχειρηματικές ανάγκες.
- Τις *επικεντρωμένες στο χρήστη λύσεις διαχείρισης ταυτότητας*: Η διαχείριση και ο έλεγχος των δεδομένων της ταυτότητας των χρηστών τοποθετούνται άμεσα στα χέρια τους, επιτρέποντάς τους να έχουν τον συνολικό έλεγχο των προσωπικών πληροφοριών τους και των προτιμήσεών τους.

  Η συγκεκριμένη κατηγορία έχει ταξινομηθεί περαιτέρω στις ακόλουθες προσεγγίσεις [BhargavSpantzel06]:
  - Στα *συστήματα εστιασμένα στα πιστοποιητικά* (credential-focused systems), τα οποία υποστηρίζουν τους σε μη απευθείας σύνδεσης διαχειριστές ταυτότητας και τη χρήση μακράς διάρκειας πιστοποιητικών από την μεριά του χρήστη.
  - Στα *συστήματα εστιασμένα στη σχέση χρηστών* (relationship-focused), τα οποία βασίζονται στην άμεση σχέση μεταξύ των χρηστών και των απευθείας σύνδεσης διαχειριστών ταυτότητας οι οποίοι εκδίδουν και διανέμουν μικρής διάρκειας πιστοποιητικά τα οποία μπορούν να χρησιμοποιηθούν για τις συναλλαγές.

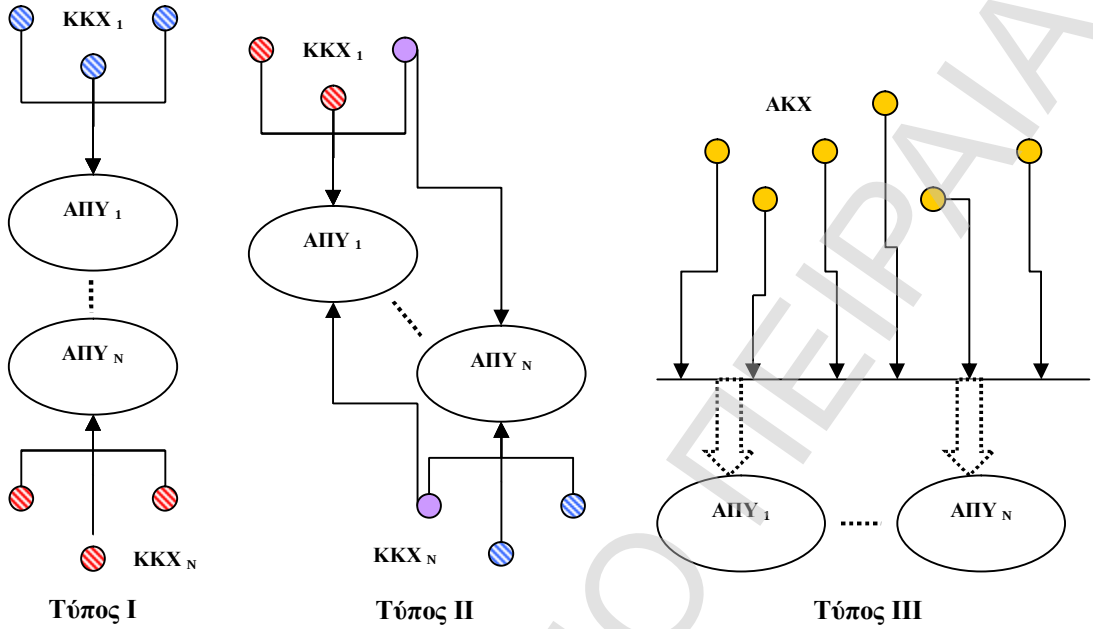
Ένα χαρακτηριστικό όλων των προαναφερόμενων λύσεων αποτελεί το γεγονός ότι χαρακτηρίζονται από ανομοιομορφία και διαφορετικές προσεγγίσεις μιας κοινής διαδικασίας. Επομένως είναι επιτακτική η ανάγκη αυστηρού καθορισμού των αρχών που θα πρέπει να διέπουν τις λύσεις διαχείρισης ταυτότητας οι οποίες θα πρέπει να υιοθετηθούν από καθεμία από τις κατηγορίες ΑΠΥ όπως αυτές παρουσιάζονται στο επόμενο κεφάλαιο.

5.3 Τοπολογίες ΑΠΥ για Διαχείριση Ταυτότητας

Οι σχεδιαστικές λύσεις των ΑΠΥ μπορεί να διακριθούν σε τρεις βασικούς τύπους με βάση τον τρόπο με τον οποίο οι χρήστες (π.χ, φυσικά πρόσωπα, ιδιωτικοί/δημόσιοι οργανισμοί, υπηρεσίες) αποκτούν πρόσβαση στις η/κ-ΥΙ αναδεικύοντας την

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

απαίτηση ύπαρξης διαφορετικών μεθόδων διαχείρισης της ταυτότητας των χρηστών. Οι προτεινόμενοι τύποι, όπως απεικονίζονται στο Σχήμα 84, είναι οι ακόλουθοι:



Σχήμα 84: Ταξινόμηση των Αρχιτεκτονικών Προσανατολισμένων στις Υπηρεσίες (ΑΠΥ)

Τύπος I: Κάθε ΑΠΥ παρέχει μια σειρά από η/κ-ΥΙ οι οποίες είναι προσιτές από ένα σύνολο χρηστών που ανήκουν σε μια *Κλειστή Κοινότητα Χρηστών (ΚΚΧ)*. Κάθε ΑΠΥ διαχειρίζεται τις ταυτότητες της ΚΚΧ της και θετεί συγκεκριμένους ελέγχους ιδιωτικότητας επιτρέποντας την πρόσβαση μόνο στην συγκεκριμένη ΚΚΧ. Για παράδειγμα, ένας οργανισμός μπορεί να παρέχει μια αυτόνομη Υπηρεσία Ιστού ηλεκτρονικής τιμολόγησης (π.χ. SELIS [Polemi07a], TOES [Papastergiou07c]) επιτρέποντας την ανταλλαγή η-τιμολογίων μόνο με άλλες συγκεκριμένες Υπηρεσίες Ιστού (που λειτουργούν ως χρήστες).

Τύπος II: Κάθε ΑΠΥ δεν παρέχει τις υπηρεσίες μόνο στη δική του ΚΚΧ (όπως στον τύπο Ι) αλλά και σε οποιοδήποτε άλλο χρήστη ο οποίος ανήκει σε μια έμπιστη ΚΚΧ. Η η-διακυβέρνηση είναι ένας χαρακτηριστικός τομέας αυτού του τύπου, όπου παραδείγματος χάριν διάφοροι έμπιστοι ευρωπαϊκοί δήμοι, οι οποίοι έχουν υιοθετήσει ΑΠΥ, παρέχουν πρόσβαση στις ΥΙ τους σε ένα σαφώς προσδιορισμένο σύνολο χρηστών.

Τύπος III: Αυτός ο τύπος περιλαμβάνει διάφορες ΑΠΥ που συμπεριφέρονται ως ανοικτές αρχιτεκτονικές με *Ανοικτές Κοινότητες Χρηστών (ΑΚΧ)*. Σε αυτήν την περίπτωση, οποιοσδήποτε χρήστης μπορεί να έχει πρόσβαση σε οποιαδήποτε υπηρεσία η οποία προσφέρεται από οποιαδήποτε ΑΠΥ. Το κύριο χαρακτηριστικό του τύπου ΙΙΙ είναι ότι οι χρήστες διαχειρίζονται την ταυτότητά τους είτε άμεσα είτε μέσω ενός συνόλου διαχειριστών ταυτότητας που φιλοξενούν τα προσωπικά τους δεδομένα καθώς και τις προσωπικές τους προτιμήσεις, επιλέγοντας οι ίδιοι τις ΥΙ με τις οποίες επιθυμούν να αλληλεπιδράσουν. Ένα αντιπροσωπευτικό παράδειγμα είναι ένα ανοικτό περιβάλλον όπου οι χρήστες αλληλεπιδρούν με πολλαπλά ΑΠΥ για την αγορά αγαθών, την υποβολή αιτημάτων ή την κοινοποίηση πληροφοριών, αλληλεπιδρώντας ενδεχομένως με άλλους χρήστες της ΑΚΧ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

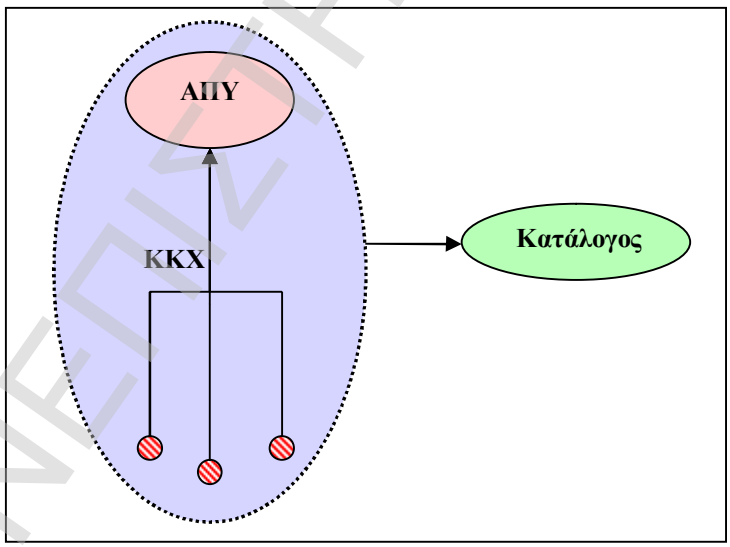
Η προτεινόμενη ταξινόμηση υπονοεί την ανάγκη για υιοθέτηση διαφορετικών λύσεων διαχείρισης ταυτότητας για καθεμία προτεινόμενη κατηγορία. Ένας σχεδιαστής ΑΠΥ θα πρέπει να λάβει υπόψη τα διαφορετικά επίπεδα πολυπλοκότητας ενσωματώνοντας τις διαδικασίες διαχείρισης ταυτότητας στις αρχιτεκτονικές του. Το κεφάλαιο που ακολουθεί παρουσιάζει τις καταλληλότερες λύσεις για κάθε τύπο.

5.4 Προτενόμενες Λύσεις Συστημάτων Διαχείρισης Ταυτότητας (ΣΔΤ)

Η εφαρμογή γενικών ή ειδικών λύσεων διαχείρισης ταυτότητας δεν μπορεί να προσφέρει ικανοποιητική λύση στα ζητήματα εξελιξιμότητας και κλιμάκωσης που εισάγονται λόγω των περίπλοκων μορφών και των συγκεκριμένων χαρακτηριστικών που παρουσιάζουν οι ΑΠΥ. Το παρόν κεφάλαιο παραθέτει συγκεκριμένες και ακριβείς λύσεις διαχείρισης ταυτότητας για κάθε ένα από τους προτεινόμενους τύπους ΑΠΥ.

5.4.1 ΣΔΤ –Τύπος Ι

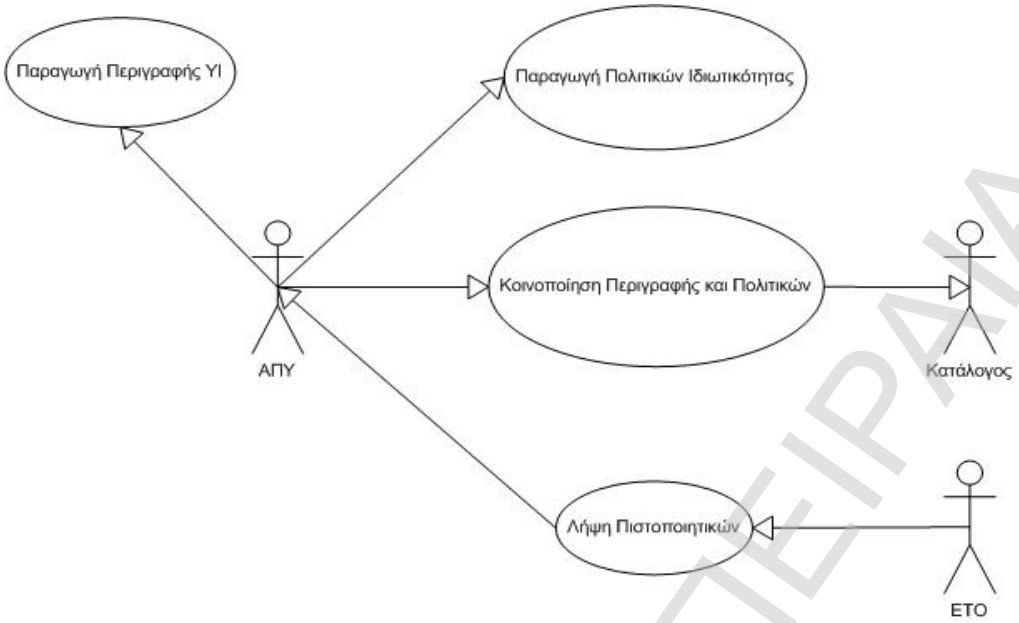
Η πρώτη κατηγορία (Τύπος Ι) απαρτίζεται από ΑΠΥ που λειτουργούν εντελώς αυτόνομα. Αλληλεπιδρούν με μια συγκεκριμένη *Κλειστή Κοινότητα Χρηστών (ΚΚΧ)* η οποία αποτελείται από μέλη τα οποία καθορίζονται από τις ίδιες τις ΑΠΥ. Η επιλογή των χρηστών βασίζεται σε καθαρά υποκειμενικά κριτήρια χωρίς να λαμβάνονται υπόψη τυχόν συστάσεις από άλλες οντότητες σχετικά με τις προθέσεις και τον ρόλο των χρηστών. Οι χρήστες επικοινωνούν απευθείας με τις ΑΠΥ, παρέχοντας τα απαιτούμενα προσωπικά δεδομένα χωρίς να απαιτείται η παρέμβαση οποιασδήποτε άλλης οντότητας.



Σχήμα 85: ΣΔΤ –Τύπος Ι

Το Σχήμα 85 αποτυπώνει τη λύση διαχείρισης ταυτότητας για τον τύπο Ι των ΑΠΥ. Στο απεικονιζόμενο παράδειγμα μια ΑΠΥ παρέχει μια σειρά από ΥΙ οι οποίες είναι προσβάσιμες από ένα συγκεκριμένο ΚΚΧ. Οι βασικές αρμοδιότητες της ΑΠΥ εστιάζονται στην ολοκλήρωση των ακόλουθων διαδικασιών (Σχήμα 86):

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 86. Βασικές Αρμοδίοτητες ΑΠΥ

Παραγωγή Περιγραφών ΥΙ
Η ΑΠΥ θα πρέπει να παράγει τις περιγραφές των ΥΙ και των αντίστοιχων Πολιτικών Ιδιωτικότητας. Οι περιγραφές των υπηρεσιών απεικονίζουν τα λειτουργικά χαρακτηριστικά τους ενώ ο κεντρικός στόχος των Πολιτικών Ιδιωτιότητας είναι η παρουσίαση των όρων αλληλεπίδρασης των δύο σημείων των υπηρεσιών. Όλες οι πληροφορίες που παρέχονται στην Πολιτική Ιδιωτικότητας στοχεύουν στην περιγραφή των δυνατοτήτων και των απαιτήσεων των υπηρεσιών.

Κοινοποίηση Περιγραφών ΥΙ
Η ΑΠΥ θα πρέπει να κοινοποιήσει τις περιγραφές των ΥΙ και των αντίστοιχων Πολιτικών Ιδιωτικότητας σε έναν κατάλογο ο οποίος είναι προσβάσιμος από τους χρήστες. Για την προστασία της ιδιωτικότητας των κοινοποιημένων πληροφοριών μπορεί να γίνει χρήση μιας προτυποποιημένης συνάρτησης κατακερματισμού η οποία να εφαρμοστεί σε ένα υποσύνολο των δεδομένων τα οποία περιγράφουν τα χαρακτηριστικά των ΥΙ.

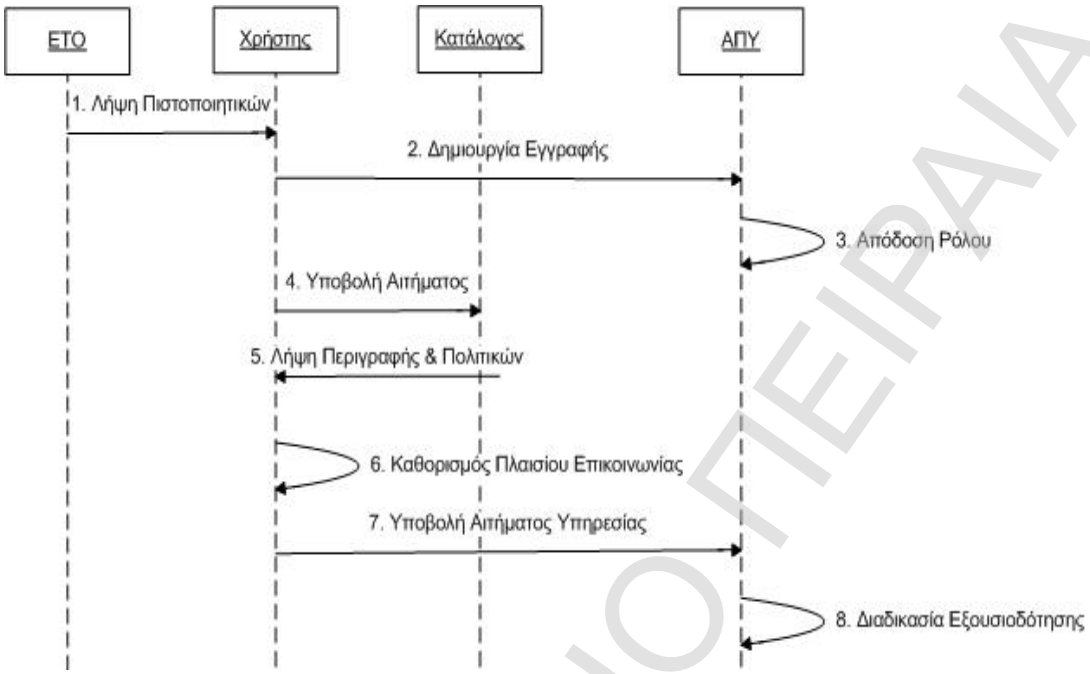
Λήψη των απαιτούμενων Πιστοποιητικών
Η ΑΠΥ θα πρέπει να επικοινωνήσει με μια Έμπιστη Τρίτη Οντότητα και πιο συγκεκριμένα με την Αρχή Πιστοποίησης και την Αρχή Εγγραφής από τις οποίες αποτελείται κάνοντας χρήση των υπηρεσιών εγγραφής και πιστοποίησης που αυτές προσφέρουν προκειμένου να ανακτήσει τα απαιτούμενα πιστοποιητικά.

Οι παραπάνω διαδικασίες αποτελούν μέρος μιας αρχικής φάσης η οποία εκτελείται από τις ΑΠΥ με σκοπό την ενίσχυση της προσβασιμότητας των προσφερόμενων ΥΙ. Στο κεφάλαιο που ακολουθεί παρατίθενται μια σειρά βημάτων τα οποία αποτελούν μέρος των διαδικασιών της λύσης διαχείρισης ταυτότητας που προτείνεται για τους συγκεκριμένους τύπους ΑΠΥ.

5.4.1.1 Διαδικασίες ΣΔΤ – Τύπος Ι

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Η προτεινόμενη διαδικασία, όπως απεικονίζεται στο Σχήμα 87, αρχικοποιείται από έναν χρήστη ο οποίος έχει υιοθετήσει και χρησιμοποιεί μια εφαρμογή η οποία βασίζεται σε τεχνολογίες όπως είναι η XML και οι Υπηρεσίες Ιστού.



Σχήμα 87: Ακολουθία βημάτων για το ΣΔΤ –Τύπος Ι

Ο χρήστης αρχικά επικοινωνεί με μια Έμπιστη Τρίτη Οντότητα (ΕΤΟ) για ανάκτηση των απαιτούμενων πιστοποιητικών. Στην συνέχεια, επικοινωνεί με την ΑΠΥ και χρησιμοποιώντας την υπηρεσία εγγραφής που αυτή προσφέρει παρέχει ένα σύνολο προσωπικών του δεδομένων. Με αυτόν τον τρόπο ο χρήστης καταχωρείται από την ΑΠΥ η οποία τον πιστοποιεί με βάση ένα συγκεκριμένο σύνολο πληροφοριών πιστοποίησης όπως είναι αυτά τα οποία ο χρήστης λαμβάνει από την Έμπιστη Τρίτη Οντότητα. Ο ρόλος ο οποίος αποδίδεται στον χρήστη καθορίζεται με βάση τα στοιχεία τα οποία παρέχει αλλά και με βάση την ισχύ των πληροφοριών πιστοποίησης.

Ο χρήστης, ακολούθως, επικοινωνεί με τον Κατάλογο στον οποίο έχουν κοινοποιηθεί οι περιγραφές των ΥΙ αλλά και οι αντίστοιχες Πολιτικές Ιδιωτικότητας δημιουργώντας και υποβάλλοντας ένα αίτημα. Στις πληροφορίες οι οποίες εμπεριέχονται στο αίτημα για την προστασία της ιδιωτικότητάς τους έχει εφαρμοστεί μια συνάρτηση κατακερματισμού. Με βάση τις ληφθείσες περιγραφές και τις Πολιτικές Ιδιωτικότητας ο χρήστης διαμορφώνει το σύστημα του ώστε να μπορεί να ανταλλάξει τα απαιτούμενα μηνύματα.

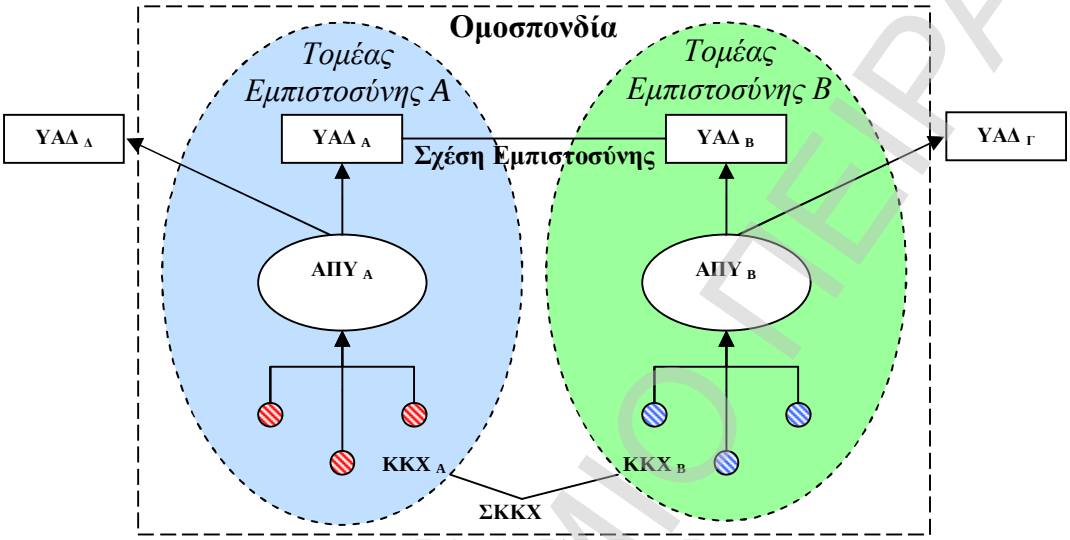
Ο χρήστης στην παρούσα φάση έχει την δυνατότητα χρησιμοποιώντας την εφαρμογή του να αλληλεπιδράσει με μια ΥΙ. Αυτό πραγματοποιείται με τη δημιουργία του αντίστοιχου αιτήματος συμπληρώνοντας τις απαραίτητες πληροφορίες και την υποβολή του στην ΑΠΥ. Η τελευταία με την λήψη του αιτήματος πιστοποιεί τον χρήστη λαμβάνοντας υπόψη τις παρεχόμενες πληροφορίες πιστοποίησης και επιτρέπει την πρόσβαση στην αιτούμενη ΥΙ με βάση τον καθοριζόμενο ρόλο.

5.4.2 ΣΔΤ –Τύπος ΙΙ

Οι χρήστες, ακολουθώντας την λύση η οποία προτείνεται για τον πρώτο τύπο ΑΠΥ απαιτείται να μετέχουν σε μια σειρά ΚΚΧ προκειμένου να έχουν πρόσβαση στις ΥΙ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

που ποσφέρονται από τις ΑΠΥ. Επιπλέον, οι ίδιες οι ΑΠΥ πρέπει να διαχειρίζονται τα προσωπικά δεδομένα ενός μεγάλου όγκου χρηστών αυξάνοντας σημαντικά το απαιτούμενο διαχειριστικό κόστος.
Επομένως, η ανάγκη για μια ευέλικτη και κλιμακωτή λύση διαχείρισης ταυτότητας η οποία διευθετεί το παραπάνω πρόβλημα ενώ παράλληλα εξασφαλίζει την προστασία της ιδιωτικότητας των χρηστών είναι επιτακτική. Η υιοθετημένη λύση θα πρέπει να επιτρέπει στους χρήστες διαφορετικών ΚΚΧ να αποκτούν πρόσβαση σε ένα διακριτό πλήθος ΑΠΥ με ομαλό και αποτελεσματικό τρόπο.



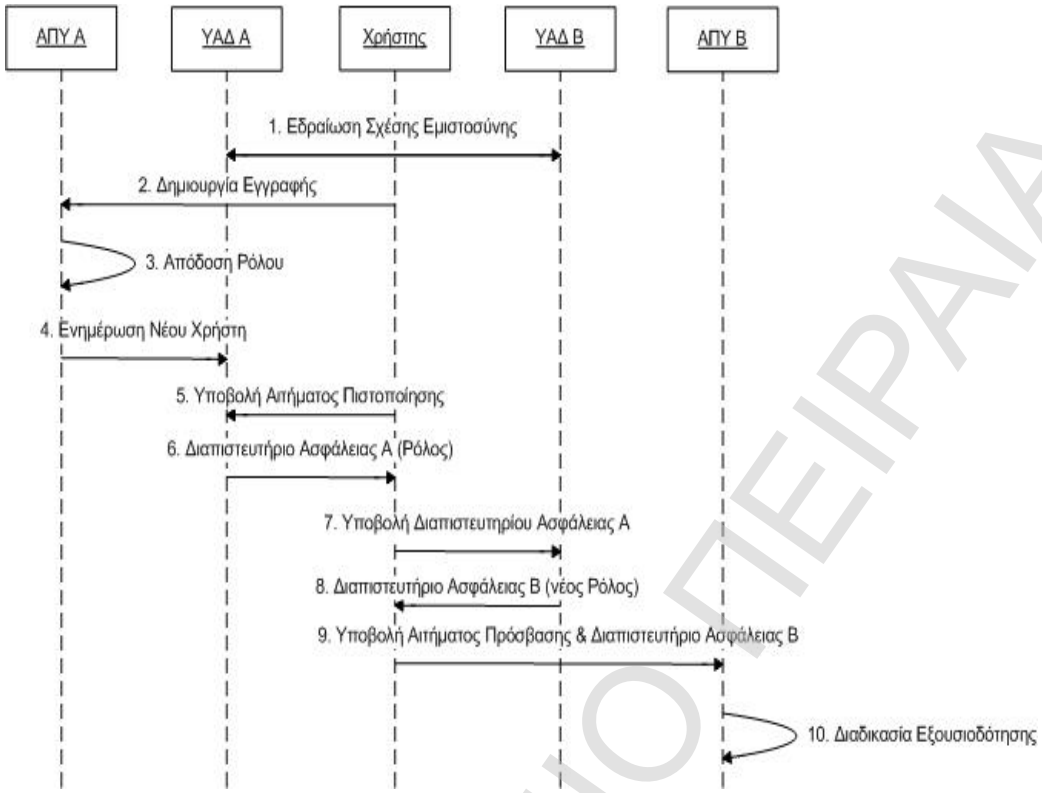
Σχήμα 88: ΣΔΤ –Τύπος ΙΙ

Το Σχήμα 88 απεικονίζει την προτεινόμενη λύση για τον δεύτερο τύπο ΑΠΥ. Στα πλαίσια της λύσης αυτής κάθε ΑΠΥ εμπιστεύεται ένα ανεξάρτητο σύνολο έμπιστων οντοτήτων οι οποίες φέρουν το όνομα *Υπηρεσίες Ασφάλειας Διαπιστευτηρίων (ΥΑΔ)* δημιουργώντας πολλαπλούς *τομείς εμπιστοσύνης*. Βασική αρμοδιότητα των ΥΑΔ αποτελεί η εγγύηση και ο έλεγχος της πρόσβασης στις προσφερόμενες ΥΙ. Η δημιουργία και η εδραίωση μιας σχέσης εμπιστοσύνης μεταξύ των τομέων εμπιστοσύνης οδηγεί στην δημιουργία συλλογών γνωστών και ως ομοσπονδίες. Στα όρια των ομοσπονδιών αυτών οι ΑΠΥ παρέχουν εξουσιοδοτημένη πρόσβαση στις ΥΙ μόνο στους χρήστες οι οποίοι φέρουν διαπιστευτήρια τα οποία έχουν εκδοθεί από μιά ΥΑΔ ενός έμπιστου τομέα εμπιστοσύνης.
Η λύση αυτή συμφωνεί πλήρως με το γενικό μοντέλο ομοσπονδίας όπως αυτό έχει καθοριστεί από το WS-Federation, το WS-Trust, το WS-SecurityPolicy και το WS-Security. Ένα χαρακτηριστικό παράδειγμα του συγκεκριμένου τύπου αποτυπώνεται στο Σχήμα 88 στο οποίο εμφανίζεται ο τομέας εμπιστοσύνης Α ο οποίος αποτελείται από την ΑΠΥ Α, την ΥΑΔ Α και την ΚΚΧ Α και ο τομέας εμπιστοσύνης Β που αποτελείται αντίστοιχα από την ΑΠΥ Β, την ΥΑΔ Β και την ΚΚΧ Β. Η εδραίωση μιας σχέσης εμιστοσύνης μεταξύ της ΥΑΔ Α και Β έχει σαν αποτέλεσμα την δημιουργία μιας ομοσπονδίας στα πλαίσια της οποίας προσφέρονται ένα σύνολο υπηρεσιών οι οποίες είναι προσβάσιμες από μια *Σφαιρική Κλειστή Κοινότητα Χρηστών (ΣΚΚΧ)*.

5.4.2.1 Διαδικασίες ΣΔΤ –Τύπος ΙΙ

Η διαδικασία η οποία λαμβάνει χώρα στη λύση διαχείρισης ταυτότητας για τον δεύτερο τύπο ΑΠΥ παρουσιάζεται στο διάγραμμα ακολουθίας του Σχήμα 89.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 89: Ακολουθία βημάτων για το ΣΔΤ –Τύπος ΙΙ

Ένας χρήστης ο οποίος θέλει να συμμετέχει στην ΚΚΧ της ΑΠΥ Α θα πρέπει να επικοινωνήσει πρώτα με την συγκεκριμένη ΑΠΥ ώστε να πραγματοποιήσει την διαδικασία εγγραφής του παρέχοντας ένα σύνολο προσωπικών δεδομένων. Η ΑΠΥ Α πιστοποιεί τον χρήστη με βάση κάποιες συγκεκριμένες πληροφορίες πιστοποίησης όπως είναι τα πιστοποιητικά τα οποία λαμβάνονται από μια Έμπιστη Τρίτη Οντότητα. Οι παρεχόμενες πληροφορίες αποθηκεύονται τοπικά στην ΑΠΥ Α και συνδέονται με ένα συγκεκριμένο ψευδώνυμο το οποίο παρέχεται είτε από την ΑΠΥ είτε από τον ίδιο τον χρήστη. Το ψευδώνυμο αυτό χρησιμοποιείται ως ένα μοναδικό προσδιοριστικό του χρήστη. Στην συνέχεια η ΑΠΥ Α ενημερώνει την ΥΑΔ Α σχετικά με την είσοδο του νέου μέλους καθώς επίσης και για τον ρόλο ο οποίος του αποδίδεται.

Η ολοκλήρωση της παραπάνω διαδικασίας δίνει την δυνατότητα στον χρήστη να αλληλεπιδράσει με τις ΥΙ οι οποίες παρέχονται από τις ΑΠΥ Α και Β. Κατά την περίπτωση κατά την οποία ο χρήστης επιθυμεί να χρησιμοποιήσει μια ΥΙ του ΑΠΥ Β τότε θα πρέπει να εκτελεστούν τα ακόλουθα βήματα.

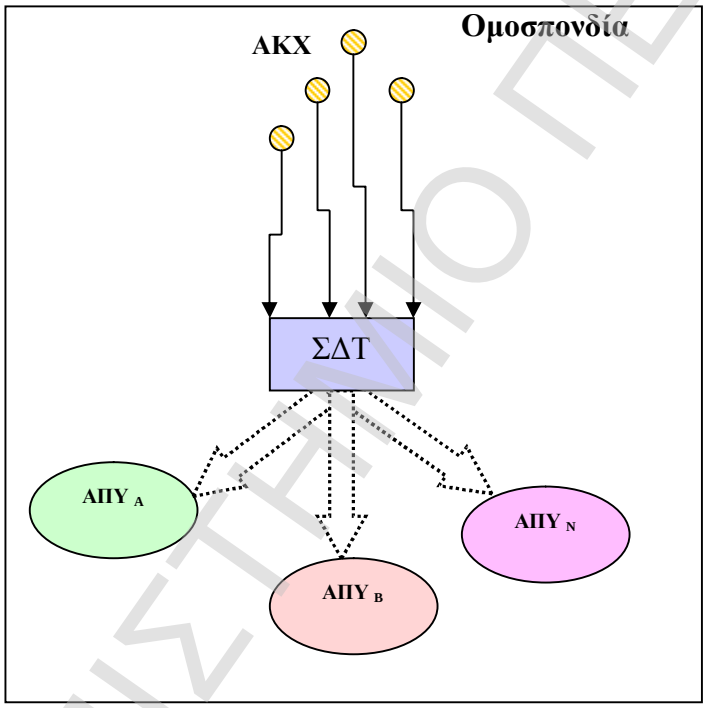
Ο χρήστης δημιουργεί ένα αίτημα πιστοποίησης το οποίο περιέχει τις πληροφορίες πιστοποίησης του και το οποίο το υποβάλει στην ΥΑΔ Α. Η τελευταία εκτελεί την διαδικασία πιστοποίησης του χρήστη εκδίδοντας ένα Διαπιστευτήριο Ασφάλειας Α το οποίο περιέχει τον ρόλο του. Το Διαπιστευτήριο αυτό επιστρέφεται στον χρήστη ο οποίος το υποβάλει στην ΥΑΔ Β από την οποία λαμβάνει το Διαπιστευτήριο Ασφάλειας Β το οποίο περιέχει το νέο του ρόλο. Το Διαπιστευτήριο Β ο χρήστης το υποβάλει στην ΑΠΥ Β μαζί με το αίτημα του για πρόσβαση σε μια ΥΙ. Η ΑΠΥ λαμβάνοντας υπόψη το ρόλο του χρήστη επιτρέπει ή απαγορεύει την πρόβαση στην αιτούμενη ΥΙ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

5.4.3 ΣΔΤ –Τύπος III

Η ανάγκη για ευρύτερα περιβάλλοντα ηλεκτρονικού επιχειρείν όπου οι χρήστες δεν θα συνδέονται με μια συγκεκριμένη ΑΠΥ μετέχοντας σε κάποια ΚΚΧ ενώ παράλληλα οι ΑΠΥ θα είναι σε θέση να αλληλεπιδράσουν με μια ΑΚΧ (βλ. § 5.3), οδηγεί στην απαίτηση για μια πιο προηγμένη και περιεκτική λύση διαχείρισης ταυτότητας. Στα περιβάλλοντα αυτά, η ταυτότητα των χρηστών θα μπορεί να διαχειρίζεται είτε από τους ίδιους τους χρήστες [Higgins06] είτε από ένα σύνολο διαχειριστών ταυτότητας.

Το πλεονέκτημα της συγκεκριμένης λύσης είναι ότι οι χρήστες μπορούν να έχουν υψηλό έλεγχο των αλληλεπιδράσεων τις οποίες μπορούν να εκτελέσουν όντας σε θέση να αποφασίσουν οι ίδιοι με ποια ΑΠΥ θέλουν να συνδιαλλαγούν αλλά και υπό ποιους όρους. Το Σχήμα 90 παρουσιάζει την προτεινόμενη λύση διαχείρισης ταυτότητας για τον συγκεκριμένο τύπο ΑΠΥ.



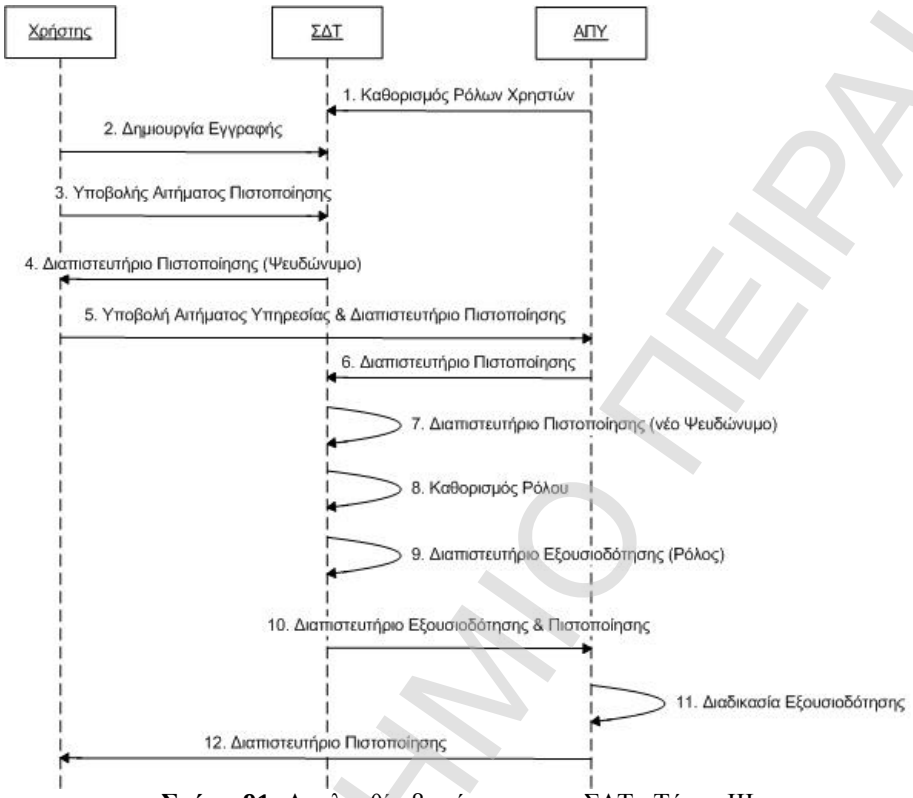
Σχήμα 90: ΣΔΤ –Τύπος III

Η έννοια της ομοσπονδίας όπως αυτή παρουσιάστηκε στο Κεφάλαιο 5.4.2 θα πρέπει να επεκταθεί δημιουργώντας ευρύτερα πλαίσια. Σε αυτό το πλαίσιο, θα πρέπει να εγκαθιστάται μια σχέση μεταξύ χρήστη-ΑΠΥ η οποία θα εγγυάται και θα ελέγχεται από μια Εμπιστευμένη Τρίτη Οντότητα. Η απαιτούμενη τρίτη οντότητα είναι το Σύστημα Διαχείρισης Ταυτότητας (ΣΔΤ) το οποίο θα είναι αρμόδιο για τη διαχείριση των μερικών ταυτοτήτων και των ψευδωνύμων των διαφόρων χρηστών ενώ επίσης θα αναλαμβάνει την έκδοση των απαιτούμενων διαπιστευτηρίων που θα διευκολύνουν την πρόσβαση των χρηστών στις προσφερόμενες ΥΙ.

Η λύση αυτή είναι βασισμένη σε μια προσέγγιση ενός ΣΔΤ [Papastergiou07b] το οποίο υιοθετεί το σύνολο των υπηρεσιών που περιγράφηκαν στο Κεφάλαιο 4.2.2. Το προτεινόμενο ΣΔΤ παρέχει την δυνατότητα στους χρήστες να έχουν αυξημένο έλεγχο της ταυτότητάς τους. Αρχικά, μια ΑΠΥ η οποία επιθυμεί να συμμετέχει στην ομοσπονδία πρέπει να εκτελέσει κάποιες συγκεκριμένες διαδικασίες. Μια νεοεισερχόμενη ΑΠΥ πρέπει πρώτα να επικοινωνήσει με το ΣΔΤ και να καθορίσει τους ρόλους που μπορούν να αποδοθούν στους χρήστες. Ο ρόλος που θα αποκτηθεί

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

από έναν χρήστη εξαρτάται από τις πληροφορίες που σκοπεύει να αποκαλύψει, την ισχύ των πληροφοριών πιστοποίησης που παρέχει και τους μηχανισμούς ασφάλειας που προτίθεται να εφαρμόσει. Επιπλέον, η ΑΠΥ πρέπει να εμπιστεύεται τα διαπιστευτήρια-ισχυρισμούς τα οποία παρέχονται από το ΣΔΤ και αφορούν έναν συγκεκριμένο χρήστη.



Σχήμα 91: Ακολουθία βημάτων για το ΣΔΤ –Τύπος ΙΙΙ

5.4.3.1 Διαδικασίες ΣΔΤ –Τύπος ΙΙΙ

Το Σχήμα 91 παραθέτει την ακολουθία των βημάτων που θα πρέπει να εκτελεστούν για τον τρίτο τύπο ΑΠΥ. Αρχικά ο χρήστης πρέπει να επικοινωνήσει με το ΣΔΤ πραγματοποιώντας την διαδικασία εγγραφής. Η διαδικασία αυτή ολοκληρώνεται με την παροχή των προτιμήσεων του χρήστη όσον αφορά τις πληροφορίες που ο χρήστης προτίθεται να αποκαλύψει κατά την διάρκεια των συναλλαγών του. Προαιρετικά ο χρήστης μπορεί να παραχωρήσει ένα υποσύνολο των πληροφοριών αυτών. Επίσης, συγκεκριμένες πληροφορίες πιστοποίησης και ένα ψευδώνυμο συνδέονται με την καταχώρηση αυτή.

Με την ολοκλήρωση της παραπάνω διαδικασίας ο χρήστης έχει την δυνατότητα να αποκτήσει πρόσβαση στις ομοσποδιακές ΥΙ. Επομένως, δημιουργεί ένα αίτημα πιστοποίησης το οποίο περιέχει τις πληροφορίες πιστοποίησης του και το οποίο το υποβάλει στο ΣΔΤ. Το ΣΔΤ εκτελεί την διαδικασία πιστοποίησης του χρήστη και εκδίδει ένα διαπιστευτήριο πιστοποίησης το οποίο περιέχει το ψευδώνυμο του και μια περίοδο ισχύος κατά την διάρκεια της οποίας το διαπιστευτήριο είναι έγκυρο και μπορεί να χρησιμοποιηθεί, ενώ παράλληλα υπογράφεται χρησιμοποιώντας το πιστοποιητικό του ΣΔΤ. Το διαπιστευτήριο στην συνέχεια επιστρέφεται στον χρήστη το οποίο υποβάλεται μαζί με το αίτημα για πρόσβαση στην ΥΙ μιας ΑΠΥ.

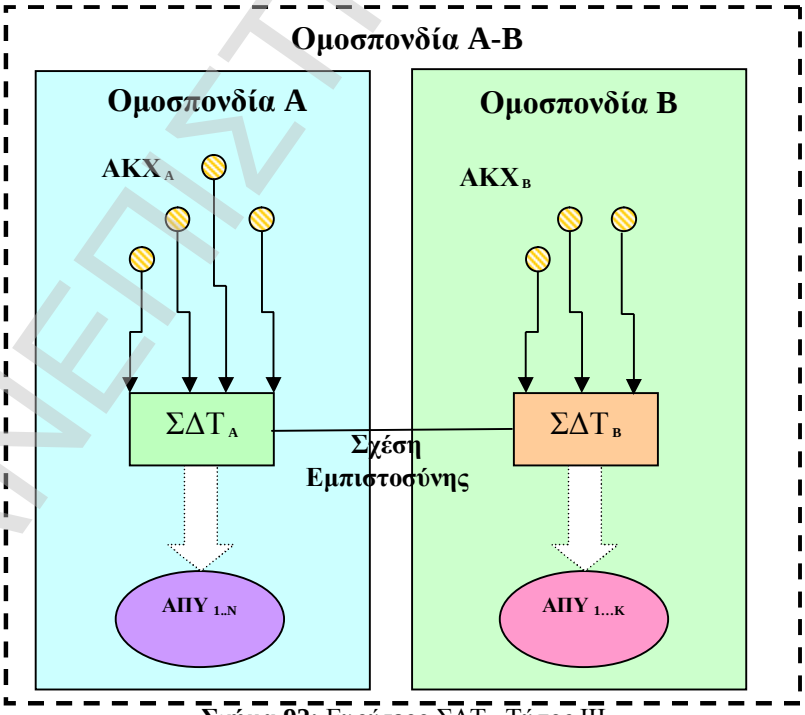
Η ΑΠΥ λαμβάνει το διαπιστευτήριο και το στέλνει στο ΣΔΤ το οποίο το επικυρώνει και το ανανεώνει εκδίδοντας ένα νέο που έχει μια πιο εκτεταμένη περίοδο ισχύος και

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ένα νέο ψευδώνυμο. Το νέο διαπιστευτήριο υπογράφεται με το πιστοποιητικό του ΣΔΤ και κρυπτογραφείται χρησιμοποιώντας το πιστοποιητικό του χρήστη. Επίσης το ΣΔΤ εκδίδει και ένα διαπιστευτήριο εξουσιοδότησης το οποίο περιέχει τα αποτελέσματα της διαδικασίας επικύρωσης του διαπιστευτηρίου πιστοποίησης καθώς επίσης τις απαιτούμενες πληροφορίες για την ολοκλήρωση της διαδικασίας ελέγχου πρόσβασης από την ΑΠΥ, όπως είναι ο ρόλος.
Τέλος, και τα δύο διαπιστευτήρια επιστρέφονται στην ΑΠΥ η οποία τα εξάγει και εκτελεί την διαδικασία ελέγχου πρόσβασης στην αιτούμενη ΥΙ. Στην περίπτωση που ο χρήστης στο αίτημα του δεν έχει δώσει όλα τα απαιτούμενα δεδομένα τότε η ΑΠΥ επικοινωνεί με το ΣΔΤ για να τα πάρει. Αν το ΣΔΤ δεν διαθέτει τις πληροφορίες αυτές τότε το αίτημα κρίνεται ως μη έγκυρο και απορρίπτεται.
Τελικά το νέο διαπιστευτήριο πιστοποίησης επιστρέφεται στο χρήστη για να χρησιμοποιηθεί στην επόμενη συναλλαγή του.

5.4.4 Ευρύτερο ΣΔΤ –Τύπος III

Το μοντέλο της ομοσπονδίας που προτάθηκε ως λύση ΣΔΤ για τον τρίτο τύπο ΑΠΥ μπορεί να επεκταθεί δημιουργώντας σφαιρικές ομοσπονδίες και διευκολύνοντας την πρόσβαση του χρήστη στις ΥΙ. Ένα αντιπροσωπευτικό παράδειγμα αποτελεί το ευρύτερο μοντέλο που απεικονίζεται στο Σχήμα 92 με το όνομα Ομοσπονδία Α-Β. Το μοντέλο αυτό αποτελείται από την Ομοσπονδία Α η οποία συντίθεται από ένα σύνολο ΑΠΥ 1...N, το ΣΔΤ Α και την ΑΚΧ Α και την Ομοσπονδία Β η οποία με τη σειρά της απαρτίζεται από ένα σύνολο ΑΠΥ 1...K, το ΣΔΤ Β και την ΑΚΧ Β. Μια σχέση εμπιστοσύνης μεταξύ των ΣΔΤ Α και Β έχει αναπτυχθεί και αποτελεί το κυρίαρχο στοιχείο πάνω στο οποίο βασίζεται η Ομοσποδίας Α-Β.
Πρέπει να σημειωθεί, ότι ευρύτερα μοντέλα μπορεί δημιουργηθούν με την συμμετοχή περισσότερων των δύο Ομοσπονδιών δίνοντας την δυνατότητα στους χρήστες να αποκτούν πρόσβαση σε ακόμη περισσότερες ΥΙ.

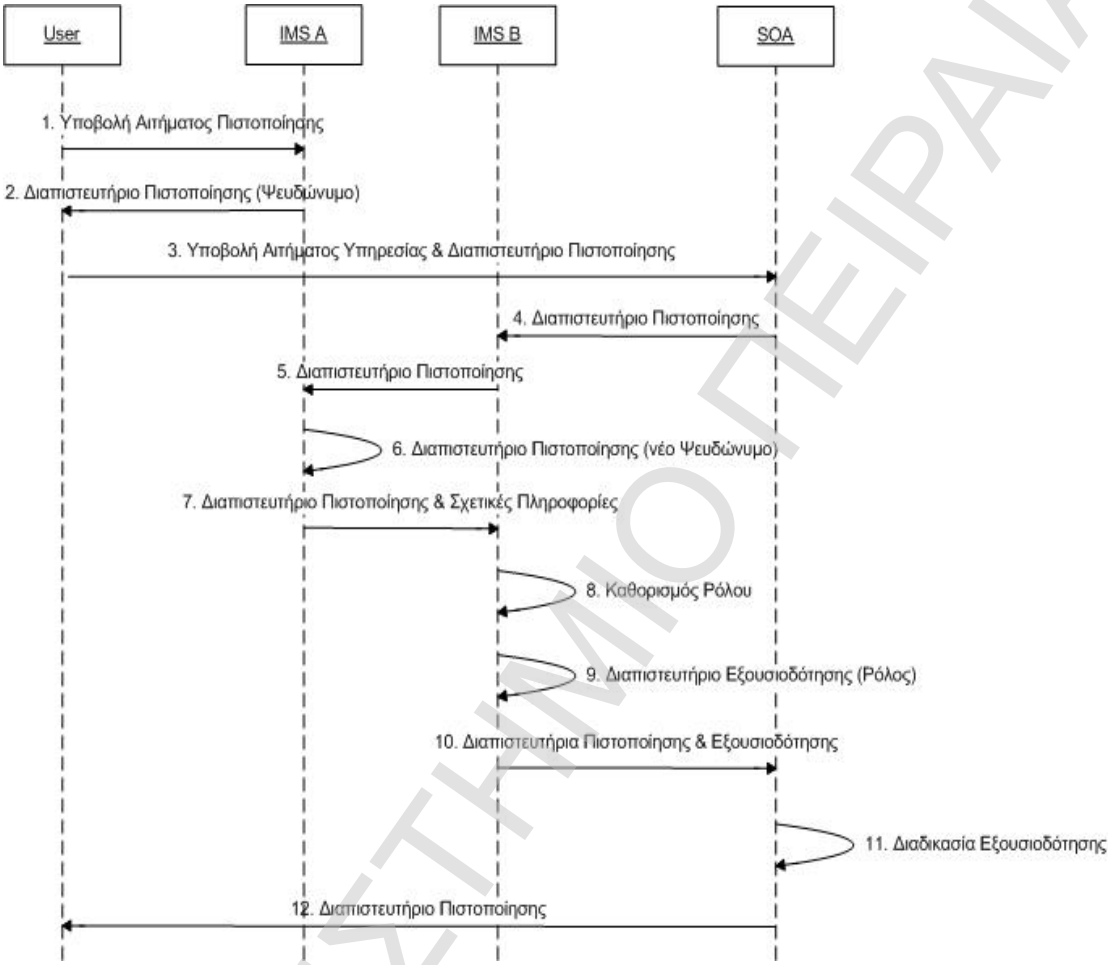


Σχήμα 92: Ευρύτερο ΣΔΤ –Τύπος III

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

5.4.4.1 Διαδικασίες Ευρύτερο ΣΔΤ –Τύπος ΙΙΙ

Στο ευρύτερο μοντέλο ένας χρήστης Α ο οποίος ανήκει στην ΑΚΧ Α έχει την δυνατότητα να χρησιμοποιήσει τις ΥΙ που προσφέρονται από τις ΑΠΥ 1...Κ. Τα βήματα τα οποία πρέπει να εκτελεστούν παρουσιάζονται στο διάγραμμα ακολουθίας του Σχήμα 93.



Σχήμα 93: Ακολουθία βημάτων για το Ευρύτερο ΣΔΤ –Τύπος ΙΙΙ

Ο χρήστης Α δημιουργεί ένα αίτημα πιστοποίησης που περιέχει τις πληροφορίες πιστοποίησης του το οποίο το υποβάλει στο ΣΔΤ Α. Το τελευταίο πιστοποιεί τον χρήστη και εκδίδει ένα διαπιστευτήριο πιστοποίησης το οποίο περιλαμβάνει το ψευδώνυμο του χρήστη και την περίοδο ισχύος του, ενώ επιστρέφεται στο χρήστη Α αφού υπογραφεί με το πιστοποιητικό του ΣΔΤ Α. Στην συνέχεια ο χρήστης Α υποβάλει στην ΑΠΥ (της Ομοσπονδίας Β) το διαπιστευτήριο μαζί με το αίτημα πρόσβασης στην ΥΙ.

Η ΑΠΥ μόλις λάβει το διαπιστευτήριο το στέλνει στο ΣΔΤ Β το οποίο αναγνωρίζει ότι έχει εκδοθεί από ένα έμπιστο ΣΔΤ. Το ΣΔΤ Β στη συνέχεια το στέλνει με τη σειρά του στο ΣΔΤ Α το οποίο το επικυρώνει επανεκδίδοντας ένα νέο, επεκτείνοντας την περίοδο ισχύος του και αποδίδοντας ένα νέο ψευδώνυμο. Το νέο διαπιστευτήριο πιστοποίησης υπογράφεται με το πιστοποιητικό του ΣΔΤ Α και κρυπτογραφείται με το πιστοποιητικό του χρήστη ενώ τελικά στέλνεται στο ΣΔΤ Β μαζί με μία δήλωση που περιλαμβάνει τις πληροφορίες που ο χρήστης προτίθεται να παρέχει (όχι το ίδιο το περιεχόμενο) αλλά και το επίπεδο ασφάλειας που επιθυμεί να εφαρμόσει.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Το ΣΔΤ Β πιστοποιεί ότι ο χρήστης είναι πιστοποιημένος με βάση τους παρεχόμενους ισχυρισμούς και αποδίδει στο χρήστη το ρόλο που του αναλογεί. Το ΣΔΤ Β εκδίδει ένα διαπιστευτήριο εξουσιοδότησης το οποίο περιέχει τα αποτελέσματα της διαδικασίας πιστοποίησης και τις πληροφορίες (π.χ. ο ρόλος) που απαιτούνται για την ολοκλήρωση της διαδικασίας εξουσιοδότησης από την ΑΠΥ. Τελικά, τα διαπιστευτήρια πιστοποίησης και εξουσιοδότησης που έχουν εκδοθεί από το ΣΔΤ Α και Β, αντίστοιχα, στέλνονται στην ΑΠΥ για να εκτελέσει τη διαδικασία ελέγχου πρόσβασης στην αιτούμενη ΥΙ.
Η ΑΠΥ με τη σειρά της επιστρέφει το νέο διαπιστευτήριο πιστοποίησης στο χρήστη Α για να το χρησιμοποιήσει για την επόμενη συναλλαγή του.

5.5 Συμπεράσματα – Μελλοντικές Επεκτάσεις

Η Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ) έχει θεωρηθεί ως ο πιο ενδεδειγμένος τρόπος για τη σχεδίαση πληροφοριακών συστημάτων και πλατφόρμων που επιτρέπουν την ολοκλήρωση πολύπλοκων ηλεκτρονικών συναλλαγών ανάμεσα σε διαφορετικούς επιχειρηματικούς φορείς. Στις μέρες μας, τα συστήματα αυτά έρχονται πλέον αντιμέτωπα με ένα σύνολο ζητημάτων που σχετίζονται με τη διαχείριση της ταυτότητας και την προστασία της ιδιωτικότητας των ψηφιακών ταυτοτήτων των χρηστών.
Στο πλαίσιο του παρόντος κεφαλαίου εντοπίστηκε η ανάγκη κατηγοριοποίησης των σχεδιαστικών λύσεων των ΑΠΥ με σεβασμό στον τρόπο με τον οποίο η σχέση εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων, χρηστών και ΑΠΥ, διαμορφώνεται επιτρέποντας στον χρήστη την πρόσβαση στις προσφερόμενες υπηρεσίες. Το γεγονός αυτό επέτρεψε τον προσδιορισμό συγκεκριμένων σχεδιαστικών λύσεων αλλά και διαδικασιών διαχείρισης ταυτότητας για καθεμία από τις προτεινόμενες κατηγορίες. Ο καθορισμός των σχεδιαστικών λύσεων έγινε θέτοντας ως βασικό στόχο την κάλυψη όλων των πιθανών περιπτώσεων ανεξαρτήτως πολυπλοκότητας διασφαλίζοντας παράλληλα την ιδιωτικότητα των εμπλεκόμενων οντοτήτων.
Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που μπορούν να βασιστούν στην παρούσα κατεύθυνση είναι οι ακόλουθες:

- Ανάγκη ύπαρξης μεθόδων και πλαισίων Αυτοματοποιημένης Σύγκρισης Πολιτικών Ιδιωτικότητας, οι οποίες θα επιτρέπουν τον έλεγχο της συμβατότητας των πολιτικών διαπιστώνοντας τη δυνατότητα επικοινωνίας των οντοτήτων. Στις μέρες μας, η ανωτέρω δραστηριότητα απαιτεί την ανθρώπινη συμμετοχή η οποία είναι αποδεδειγμένα χρονοβόρα, καθιστώντας εντονότερη την ανάγκη υιοθέτησης μιας αυτοματοποιημένης διαδικασίας.
- Πέραν βέβαια από τη σύγκριση των πολιτικών δημιουργείται και η απαίτηση για μεθόδους και διαδικασίες που επιτρέπουν την διαπραγμάτευση των όρων των πολιτικών ιδιωτικότητας ώστε να καθοριστούν οι αρχές με βάση τις οποίες θα πραγματοποιηθεί μια συναλλαγή.
- Τέλος επιτακτική κρίνεται η ανάγκη μεθόδων που θα εγγυώνται την εκτέλεση των Πολιτικών Ιδιωτικότητας με βάση των οποίων πραγματοποιήθηκε μια συγκεκριμένη συναλλαγή. Η ανάπτυξη τέτοιων μεθόδων θα πρέπει να πραγματοποιηθεί ακολουθώντας, από τη μία, το υπάρχον νομικό πλαίσιο προστασίας των δεδομένων και, από την άλλη, τα αποδεδειγμένα πρότυπα ασφάλειας στον τομέα της ιδιωτικότητας των δικτυοκεντρικών συστημάτων και

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

υπηρεσιών (όπως το ISO17999 (ISO17999, 2000), Common Criteria (Common Criteria)).

Η ολοκλήρωση των παραπάνω στόχων θα επιτρέψει την εκτέλεση πιο αξιόπιστων συναλλαγών συμβάλλοντας δραστικά στην δημιουργία ενός ολοένα πιο ασφαλούς ηλεκτρονικού και κινητού περιβάλλοντος στα πλαίσια του οποίου η εμπιστοσύνη μεταξύ των εμπλεκόμενων οντοτήτων θα παίζει αποφασιστικό ρόλο.

5.6 Αναφορές

[LibertyAlliance] Liberty Alliance. "Liberty ID-WSF Web Services Framework Overview", version 2.0 specifications, http://www.projectliberty.org.

[Lockhart06] H. Lockhart et al.. (2006). "*Web Services Federation Language (WS-Federation)*", Version 1.1 December 2006.

[SAML05] Oasis Standard. Security assertion markup language (SAML) V2.0, 2005.

[OMA06] International Telecommunication Union, Draft of Guideline on Single Sign-On and Access Control Methods for Mobile Web Environments. Jeju, Korea, 19-28 April 2006.

[Meints] M. Meints et al. "*D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*", http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

[LibertyAlliance03] Liberty Alliance Project White Paper: Liberty Alliance & WS-Federation: A Comparative Overview, October 2003, http://www.projectliberty.org/resources/whitepapers/.

[Goodner07] M. Goodner et al.. (2007). "*Understanding WS-Federation*", version 1.0, May 28, 2007.

[PRIME05] PRIME Project, "*Privacy and Identity Management for Europe*", European RTD Integrated Project under the FP6/IST Programme, http://www.prime-project.eu.org/, 2005.

[Ardagna06] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, F. Frati, P. Samarati. (2006). "*Privacy-Enhanced Identity Management for e-Services*". In book on Secure eGovernment Web Services, Idea Group INC., 2006.

[BhargavSpantzel06] A. Bhargav-Spantzel, J. Camenisch, T. Gross, D. Sommer. (2006). "*User centricity: a taxonomy and open issues*". Digital Identity Management 2006: 1-10.

[Polemi07a] D. Polemi, A. Mitrakas. (2007). "*Trustworthy e-Invoicing services*" Chapter in the book "E-Taxation: State & Perspectives: E-Government in the field of Taxation: Scientific Basis, Implementation Strategies Good Practice Examples" Editors: Josef Makolm, Gerti Orthofer, Verlag, 2007.

[Papastergiou07c] Papastergiou S., Polemi D.. (2007). "*A Secure and Trustful e-Ordering Architecture (TOES) for Small and Medium size Enterprises (SMEs)*". International Journal of Information Security and Privacy, IdeaGroup Inc., 2007.

[Higgins06] Higgins Trust Framework, 2006, http://www.eclipse.org/higgins/.

[Papastergiou07b] S. Papastergiou, A. Karantjias, D. Polemi. (2007). "*A Federated Privacy-Enhancing Identity Management System (FPE-IMS)*", 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), 3-7 September 2007, Athens.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

6 Σύστημα Καταγραφής Συμπεριφοράς (ΣΚΣ)

Το κεφάλαιο αυτό επισημαίνει τη σημασία που έχει η καταγραφή και αποτύπωση της συμπεριφοράς που επιδεικνύεται από τους χρήστες στα πλαίσια των συναλλαγών που αυτοί εκτελούν με τις ΥΙ και του ρόλου που αυτή μπορεί να διαδραματίσει για την ενίσχυση της ιδιωτικότητας. Για το λόγο αυτό εξετάζονται ένα σύνολο από συστήματα καταγραφής και αποτύπωσης συμπεριφοράς και παραθέτονται οι αδυναμίες τους. Στη συνέχεια προτείνεται η ενσωμάτωση μιας Υπηρεσίας Καταγραφής Συμπεριφοράς στα Συστήματα Διαχείρισης Ταυτότητας τα οποία αποτελούν τις κεντρικές οντότητες των ομοσπονδιών επιτρέποντας με αυτόν τον τρόπο την ενίσχυση των πλαισίων αυτών μέσω της υιοθέτησης μιας αυτοματοποιημένης διαδικασίας αξιολόγησης της εμπιστοσύνης των εμπλεκόμενων οντοτήτων. Στο πλαίσιο του κεφαλαίο γίνεται εκτενής περιγραφή της προτεινόμενης υπηρεσίας παραθέτοντας το σύνολο των πτυχών της.

6.1 Εισαγωγή

Μια αναμφισβήτητη διαπίστωση της σύγχρονης ψηφιακής εποχής αποτελεί το γεγονός ότι παρ' όλη τη ραγδαία αύξηση των προσφερόμενων ηλεκτρονικών και κινητών υπηρεσιών το επίπεδο της εμπιστοσύνης μεταξύ των εμπλεκομένων οντοτήτων παραμένει εξαιρετικά χαμηλό. Το στοιχείο αυτό έχει ως αποτέλεσμα οι υπηρεσίες αυτές να μην βρίσκουν μεγάλη απήχηση στο ευρύ κοινό εμποδίζοντας ταυτόχρονα τους απλούς χρήστες να ευνοηθούν από τα οφέλη που αυτές προσφέρουν.

Η επιστημονική και επιχειρηματική κοινότητα για την αντιμετώπιση του προβλήματος αυτού έχει στραφεί προς τη δημιουργία Ομοσπονδιών όπως αυτές παρουσιάστηκαν στις Παραγράφους 5.4.2.1 και 5.4.3.1. Στα πλαίσια των ομοσπονδιών αυτών δημιουργείται μια σχέση εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων η οποία εξασφαλίζει την ομαλή και έμπιστη αλληλεπίδραση τους. Η σχέση αυτή συνήθως εγγυάται και ελέγχεται από ένα Σύστημα Διαχείρισης Ταυτότητας (ΣΔΤ) [Haddad08], το οποίο αποτελεί την Έμπιστη Τρίτη Οντότητα (ΕΤΟ) η οποία διαχειρίζεται όλες τις πληροφορίες και τις προτιμήσεις των οντοτήτων ενώ παράλληλα παρέχει τα απαραίτητα διαπιστευτήρια που διασφαλίζουν τη ροή των ανταλλασσόμενων πληροφοριών.

Ουσιαστικά, όμως, στα ομοσπονδιακά πλαίσια παρά το γεγονός της έμπιστης σχέσης η οποία πρακτικά υφίσταται, η έννοια της εμπιστοσύνης παραμένει αρκετά ασαφής και απροσδιόριστη. Η ανάγκη υιοθέτησης ενός ποσοτικού μεγέθους το οποίο θα προσφέρει το πλεονέκτημα μιας γρήγορης και αυτοματοποιημένης διαδικασίας αξιολόγησης του βαθμού εμπιστοσύνης η οποία αποδίδεται σε μια οντότητα κρίνεται επιτακτική. Η καταγραφή της συμπεριφοράς η οποία επιδεικνύεται από έναν χρήστη κατά την διάρκεια των συναλλαγών του καλύπτει την ανάγκη αυτή στοχεύοντας στην παραγωγή της απαραίτητης αντίληψης που μια οντότητα δημιουργεί μέσω των προηγούμενων ενεργειών της για τις μελλοντικές της προθέσεις και φιλοδοξίες [Mui02].

Διάφορες η-αγορές, όπως είναι το Amazon [Amazon], το eBay [Resnick02] και το BizRate [BizRate] αντιλαμβανόμενες τη σημασία της καταγραφής αυτής για την ολοκλήρωση έμπιστων αλληλεπιδράσεων καθώς επίσης και τη μείωση των κινδύνων που οι η/κ-συναλλαγές εσωκλείουν έχουν υιοθετήσει ένα *Σύστημα Καταγραφής Συμπεριφοράς (ΣΚΣ)* [Traupman06]. Το σύστημα αυτό επικεντρώνεται κατά κύριο

λόγο στη συλλογή, διανομή και συγκέντρωση των στοιχείων που αφορούν τη συμπεριφορά των εμπλεκόμενων οντοτήτων επιδιώκοντας να αποκαλύψουν τις προθέσεις τους σχετικά με τον τρόπο που αναμένεται να ενεργήσουν στις μελλοντικές αλληλεπιδράσεις τους.
Η ENISA [Carrara07] αναγνωρίζοντας και αυτή με τη σειρά της το σπουδαίο ρόλο και τα οφέλη που μπορούν να προκύψουν από τα ΣΚΣ επισημαίνει την ανάγκη για σχεδιασμό τέτοιου είδους συστημάτων με έμφαση στην ιδιωτικότητα των χρηστών. Η παρούσα κατεύθυνση στοχεύοντας στο να συμβάλει προς την ενίσχυση των ΣΔΤ προτείνει μια *Υπηρεσία Καταγραφής Συμπεριφοράς (ΥΚΣ)* η οποία λειτουργεί σε ένα ΣΔΤ προκειμένου να διαφυλάξει και να διασφαλίσει την αναπτυσσόμενη εμπιστοσύνη στο πλαίσιο των Ομοσπονδιών προσφέροντας έναν αυτοματοποιημένο τρόπο αξιολόγησής της. Η προτεινόμενη υπηρεσία, επιτρέπει τη συσσώρευση των πληροφοριών συμπεριφοράς των χρηστών που επιθυμούν να αποκτήσουν πρόσβαση σε ένα σύνολο υπηρεσιών οι οποίες προσφέρονται από παρόχους που εμπιστεύονται το ΣΔΤ λειτουργώντας με τρόπο που να σέβεται την ιδιωτικότητα των χρηστών. Η υπηρεσία επιτρέπει επίσης την αξιολόγηση της αξιοπιστίας των χρηστών προσφέροντας στους παρόχους την δυνατότητα να λάβουν καλώς διαμορφωμένες αποφάσεις ελέγχου πρόσβασης λαμβάνοντας υπόψη την προγενέστερη συμπεριφορά τους.
Στις παραγράφους που ακολουθούν αρχικά γίνεται μια παρουσίαση και αξιολόγηση των υπαρχόντων συστημάτων καταγραφής συμπεριφοράς περιγράφοντας επίσης τον τρόπο με τον οποίο η εμπιστοσύνη και η καταγραφή συμπεριφοράς διευθετείται από τα υπάρχοντα ΣΔΤ. Στη συνέχεια πραγματοποιείται μια περιγραφή της προτεινόμενης υπηρεσίας παραθέτοντας το σύνολο των πτυχών της.

6.2 Υπάρχοντα ΣΚΣ

Στο παρόν κεφάλαιο πραγματοποιείται η κατηγοριοποίηση των υπαρχόντων ΣΚΣ και η παρουσίαση των πιο σημαντικών απειλών που αυτά αντιμετωπίζουν. Παράλληλα ευρέως διαδεδομένα ΣΔΤ αξιολογούνται ως προς τον τρόπο με τον οποίο προσεγγίζουν την έννοια της εμπιστοσύνης και της καταγραφής συμπεριφοράς.

6.2.1 Συστήματα Καταγραφής Συμπεριφοράς

Τα τελευταία χρόνια έχει παρουσιαστεί ένα μεγάλο σύνολο ΣΚΣ υιοθετώντας και προτείνοντας σχήματα και μεθόδους που επικεντρώνονται στη συλλογή και συσσώρευση εκτιμήσεων σχετικά με την συμπεριφορά που επιδεικνύεται από μια οντότητα. Τα συστήματα αυτά διαιρούνται σε δυο βασικές κατηγορίες [Jøsang07] με βάση τη σχεδίαση και τα οργανωτικά τους χαρακτηριστικά:
Τα *Κεντροποιημένα ΣΚΣ*: όπου μια κεντρική οντότητα αναλαμβάνει την ευθύνη συλλογής των εκτιμήσεων και υπολογισμού της τιμής συμπεριφοράς για καθεμία από τις εμπλεκόμενες οντότητες. Το Amazon, το eBay και το BizRate αποτελούν αντιπροσωπευτικά παραδείγματα αυτού του τύπου συστημάτων τα οποία έχουν υιοθετήσει πρώιμους μηχανισμούς ανάκτησης των εκτιμήσεων και καταγραφής της συμπεριφοράς. Σε αυτά τα συστήματα, οι εκτιμήσεις οι οποίες παρέχονται από τους χρήστες κυμαίνονται σε μια ορισμένη κλίμακα τιμών, π.χ. από 1 έως 10, ενώ η τελική τιμή της συμπεριφοράς τους προκύπτει από τον υπολογισμό του μέσου όρου των παρεχόμενων εκτιμήσεων.
Τα *Διανεμημένα ΣΚΣ*: όπου οι εκτιμήσεις της συμπεριφοράς για μια συγκεκριμένη οντότητα βρίσκονται διανεμημένες σε διαφορετικά σημεία του πλαισίου. Πιο

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συγκεκριμένα, έχει προταθεί μια σειρά μοντέλων [Lin05, Park05] τα οποία επιτρέπουν στους χρήστες, προκειμένου να διαπιστώσουν τη συμπεριφορά ενός παρόχου υπηρεσιών, να λαμβάνουν και να καταγράφουν πληροφορίες σχετικές με τη συμπεριφορά του παρόχου από άλλους χρήστες οι οποίοι κατά το παρελθόν έχουν εκτελέσει συναλλαγές μαζί του. Σε αυτόν τον τύπο ανήκει επίσης και ένα σύνολο ΣΚΣ για διανεμημένα P2P δίκτυα [Kamvar03, Damiani02] επιτρέποντας στους κόμβους να ανταλλάσσουν μεταξύ τους πληροφορίες συμπεριφοράς προκειμένου να προωθήσουν την κίνηση τους στον πιο αξιόπιστο κόμβο.

Η ανάγκη για υιοθέτηση πιο αποτελεσματικών συστημάτων που θα επιτρέπουν την αύξηση της αξιοπιστίας ως προς την αξιολόγηση της εμπιστοσύνης και της συμπεριφοράς παρέχοντας ακριβέστερα αποτελέσματα έχει οδηγήσει στην πρόταση μια σειράς μοντέλων [Zou07] για τον υπολογισμό της συμπεριφοράς. Τα μοντέλα αυτά ποικίλουν από Διακριτής Εμπιστοσύνης (Discrete Trust) [Cahill03, Carbone03] και Πεποιθήσεων (Belief) [Jøsang01] μέχρι μοντέλα που βασίζονται σε Ασαφή Λογική (Fuzzy) [Sabater02a, Sabater02b] και σε Ροές (Flow) [Levien04, Ziegler04], παρέχοντας ένα μεγάλο εύρως επιλογών.

Οι παραπάνω λύσεις στο σύνολο τους δεν συνδέονται με μια συγκεκριμένη μέθοδο λήψης και συλλογής πληροφοριών συμπεριφοράς ή διαθέτουν έναν ιδιαίτερα απλό μηχανισμό που δεν εγγυάται την ακεραιότητα της συνολικής διαδικασίας. Επιπλέον, δεν επιτυγχάνουν την διευθέτηση των απαιτήσεων ιδιωτικότητας όπως είναι η ψευδωνυμία των εμπλεκόμενων οντοτήτων αποτυγχάνοντας να διασφαλίσουν και να εγγυηθούν την δημιουργία του απαιτούμενου επιπέδου εμπιστοσύνης. Επομένως σε πολλές περιπτώσεις η γνώση η οποία παράγεται δεν μπορεί να προσφέρει ασφαλή αποτελέσματα.

Έχουν καταγραφεί ένα σύνολο από απειλές τις οποίες αντιμετωπίζουν τα ΣΚΣ και οι οποίες συνοψίζονται στις ακόλουθες:

- *Άδικες Εκτιμήσεις (Unfair rating)*: οι λανθασμένες εκτιμήσεις (θετικές ή αρνητικές) οι οποίες παρέχονται από μία οντότητα προκειμένου να επηρεάσουν θετικά ή αρνητικά τη συμπεριφορά η οποία καταγράφεται για μια άλλη οντότητα. Για το σκοπό αυτό έχουν προταθεί μοντέλα [Withby05, Sen02, Dellarocas00] ανίχνευσης και αποκλεισμού εκτιμήσεων που πιθανολογούνται να είναι άδικες τα οποία βασίζονται σε στατιστικές αναλύσεις.
- *Ανακριβείς Εκτιμήσεις (Inaccurate rating)*: λανθασμένες εκτιμήσεις οι οποίες παρέχονται από οντότητες εξαιτίας της μειωμένης γνώσης που έχουν για άλλες οντότητες. Έχουν παρουσιαστεί αλγόριθμοι [Miller03] που επιτρέπουν τη διόρθωση των επιβλαβών εκτιμήσεων οι οποίες παρέχονται.
- *Περιορισμένος αριθμός Εκτιμήσεων (Limited number of rating)*: η αδιαφορία των οντοτήτων να παρέχουν τις εκτιμήσεις τους. Πρόταση σχημάτων [Jurca03] για την εκμαίευση έντιμων εκτιμήσεων με βάση κάποια ανταμοιβή.
- Θα πρέπει να υπάρχει εγγύηση για την ιδιωτικότητα των οντοτήτων των οποίων συλλέγεται και καταγράφεται η συμπεριφορά. Η χρήση ψευδωνύμων στα οποία συνδέονται οι αντίστοιχες τιμές συμπεριφοράς επιτρέπει την ενίσχυση της ιδιωτικότητας ως ένα βαθμό. Η λύση όμως αυτή υποφέρει από τη συνδεσιμότητα των εκτελέσιμων συναλλαγών με άμεση συνέπεια τη μείωση της ανωνυμίας των αντίστοιχων οντοτήτων, γεγονός που μπορεί να οδηγήσει σε δηλώσεις προκατειλημμένων εκτιμήσεων σχετικά με τη συμπεριφορά συγκεκριμένων οντοτήτων. Ένα σύνολο λύσεων είναι διαθέσιμες για την άμβλυνση του συγκεκριμένου προβλήματος [Carrara07, Steinbrecher07].
- *Αρχικοποίηση Συμπεριφοράς*: η αρχική τιμή συμπεριφοράς που λαμβάνει μια οντότητα μόλις εισέλθει σε ένα σύστημα αποτελεί ένα μείζον ζήτημα. Το

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

γεγονός αυτό μπορεί να ενθαρρύνει την οντότητα να συμπεριφερθεί έντιμα ή όχι με βάση το αντίκτυπο που θα επιφέρει η επανασύνδεσή της στο σύστημα με μια άλλη ταυτότητα [Friedman01].

Το στοιχείο που πρέπει να επισημανθεί είναι η έλλειψη μιας ολοκληρωμένης προσέγγισης η οποία έχει τη δυνατότητα να αντιμετωπίσει αποτελεσματικά το σύνολο των παραπάνω απειλών παρέχοντας μια αξιόπιστη και ευρέως αποδεκτή λύση ΣΚΣ. Ένα τέτοιο σύστημα θα επέτρεπε την ενίσχυση της αξιοπιστίας των συναλλαγών ενισχύοντας το αίσθημα εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων.

6.2.2 Συστήματα Διαχείρισης Ταυτότητας

Έχει προταθεί μια σειρά από διαφορετικά ΣΔΤ την τελευταία δεκαετία σε μια προσπάθεια να ικανοποιηθεί ένα πλήθος απαιτήσεων και πτυχών της διαχείρισης ταυτότητας και να διαμορφωθεί το απαιτούμενο επίπεδο εμπιστοσύνης μεταξύ των συμβαλλόμενων οντοτήτων. Πρωτοβουλίες όπως το Liberty Alliances [LibertyAlliance], WS-Federation [Lockhart06] και το PRIME (Privacy and Identity Management for Europe) [Andersson05] αποτελούν αντιπροσωπευτικά παραδείγματα ΣΔΤ.
Στο Κεφάλαιο 5.2 πραγματοποιήθηκε η παρουσίαση των συστημάτων αυτών περιγράφοντας τις βασικές τους πτυχές. Η παράθεση υπαρχόντων κατηγοριοποιήσεων επιτρέπει τη δημιουργία μιας πιο ολοκληρωμένης εικόνας ως προς τους στόχους του οποίους καθένα από τα ΣΔΤ επιχειρεί να καλύψει.
Το στοιχείο που πρέπει να σημειωθεί είναι το γεγονός ότι καθένα από τα ανωτέρω συστήματα προσεγγίζει την έννοια της εμπιστοσύνης από διαφορετική σκοπιά. Το Liberty Alliance και το WS-Federation θεωρούν την διαμόρφωση της εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων ως ένα προαπαιτούμενο το οποίο επιτυγχάνεται μέσω συμφωνηθέντων συμβάσεων οι οποίες ρυθμίζουν τις αλληλεπιδράσεις των οντοτήτων. Για το λόγο αυτό χρησιμοποιείται ο όρος *επιχειρηματική εμπιστοσύνη* (business trust) ώστε να αποδοθεί με σαφήνεια η σωστή διάσταση της σχέσης μεταξύ των συμμετεχόντων. Η απουσία ενός μηχανισμού ο οποίος εγγυάται και διασφαλίζει την εφαρμογή των συμφωνιών και η έλλειψη μιας υπηρεσίας η οποία θα ελέγχει και θα καταγράφει τη συμπεριφορά των χρηστών κατά την διάρκεια των συναλλαγών τους έχουν αναγνωριστεί ως σημαντικές αδυναμίες των συγκεκριμένων μοντέλων.
Αντίθετα το PRIME [Crane06] προσφέρει μια ολοκληρωμένη λύση επιτρέποντας στις οντότητες οι οποίες ενεργούν ως πάροχοι υπηρεσιών να παρέχουν τα απαραίτητα πειστήρια και αποδείξεις, στους χρήστες τους σχετικά με το γεγονός ότι τα προσωπικά τους στοιχεία τα οποία έχουν παραχωρηθεί θα επεξεργαστούν σύμφωνα με τις πολιτικές ιδιωτικότητας που έχουν ανακοινωθεί. Οι χρήστες λοιπόν, με βάση τις αποδείξεις αυτές καταγράφουν τη συμπεριφορά των συγκεκριμένων παρόχων. Η καταγραφή αυτή τους δίνει την δυνατότητα να δηλώσουν το βαθμό εμπιστοσύνης που αποδίδουν σε κάθε πάροχο επιτρέποντάς τους να εκτελούν συναλλαγές μόνο με πάροχους που συμπεριφέρονται με εντιμότητα.

6.3 Προτεινόμενη ΥΚΣ

Στην παρούσα κατεύθυνση αναγνωρίζοντας τον πρωταρχικό ρόλο που διαδραματίζει η καταγραφή της συμπεριφοράς στην ανάπτυξη ενός έμπιστου πλαισίου, προτείνεται μια Υπηρεσία Καταγραφής Συμπεριφοράς (ΥΚΣ) η οποία θα λειτουργεί σε ένα ΣΔΤ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

σε πλήρη αρμονία με όλες τις διαδικασίες και τις υπηρεσίες που προσφέρονται από αυτό (π.χ. υπηρεσίες έκδοσης διαπιστευτηρίων (βλ. § 4.2.2)). Η προτεινόμενη υπηρεσία εστιάζεται στη συγκέντρωση δεδομένων που σχετίζονται με την συμπεριφορά που επιδεικνύεται από τους χρήστες οι οποίοι επιθυμούν να αποκτήσουν πρόσβαση σε υπηρεσίες παρόχων που εμπιστεύονται το ΣΔΤ.
Η ΥΚΣ δίνει την δυνατότητα στους παρόχους να επιτρέπουν ή να απαγορεύουν την πρόσβαση των χρηστών στις υπηρεσίες τους λαμβάνοντας υπόψη μια επιπλέον παράμετρο, τη συμπεριφορά τους. Η συμπεριφορά του χρήστη επηρεάζεται θετικά ή αρνητικά ανάλογα με τον αριθμό και το είδος των επιτυχημένων ή αποτυχημένων συναλλαγών που έχει εκτελέσει. Οι αποτυχημένες συναλλαγές οφείλονται στην αδυναμία του παρόχου να διαχειριστεί και τελικώς να εκτελέσει το αίτημα του χρήστη. Η διατριβή έχει καθορίσει ένα σύνολο περιπτώσεων στις οποίες οφείλεται η συγκεκριμένη αδυναμία οι οποίες συνοψίζονται στις ακόλουθες:

- *Αποτυχία Πιστοποίησης*: Οι παρεχόμενες πληροφορίες πιστοποίησης από τον χρήστη δεν είναι έγκυρες.
- *Αποτυχία Εξουσιοδότησης*: Ο χρήστης δεν έχει τα απαιτούμενα διακαιώματα για να αποκτήσει πρόσβαση στην υπηρεσία.
- *Αποτυχία Προσωποποίησης και Κλοπής Ταυτότητας*: Η συναλλαγή χαρακτηρίζεται από προσπάθεια προσωποποίησης ή κλοπής ταυτότητας.
- *Αποτυχία Απαιτούμενων Υποχρεώσεων*: Η συναλλαγή χαρακτηρίζεται ως αποτυχημένη λόγω της αδυναμίας του χρήστη να ανταπεξέλθει στις απαιτήσεις της συναλλαγής όπως είναι η παροχή των απαιτούμενων πληροφοριών ή ακόμα και η αποπληρωμή του κόστους που προκύπτει από την χρήση της υπηρεσίας. Το γεγονός αυτό επηρεάζει τον οργανισμό αρνητικά όσον αφορά τον χρόνο αλλά και την υπολογιστική δύναμη που απαιτείται για την εκτέλεση της συναλλαγής.

Οι ανωτέρω περιπτώσεις δημιουργούν τέσσερις κατηγορίες αποτυχημένων συναλλαγών οι οποίες συναντιούνται στις αλληλεπιδράσεις μεταξύ των οντοτήτων. Καθεμία από τις κατηγορίες αυτές έχει διαφορετική βαρύτητα και επηρεάζει σε διαφορετικό βαθμό την τελική διαμόρφωση της συμπεριφοράς ενός χρήστη. Ο *βαθμός βαρύτητας* $a_i, i = 1...4$ κάθε κατηγορίας αποτελεί μια ποσότητα που καθορίζεται από τον ίδιο τον πάροχο, σύμφωνα με την πολιτική ασφάλειας και την επιχειρηματική πολιτική του παρόχου.
Στις παραγράφους που ακολουθούν παρατίθενται οι απαιτήσεις τις οποίες πρέπει να καλύπτει η ΥΚΣ και περιγράφεται η γενική αρχιτεκτονική ενός ΣΔΤ που έχει υιοθετήσει αυτήν την υπηρεσία.

6.3.1 Απαιτήσεις ΥΚΣ

Οι βασικές απαιτήσεις οι οποίες πρέπει να ικανοποιούνται από την Υπηρεσία Καταγραφής Συμπεριφοράς και οι οποίες εμπερικλείουν τα βασικά προβλήματα που αντιμετωπίζουν τα υπάρχοντα ΣΚΣ είναι οι ακόλουθες:

- *Αυτοκαθορισμός*. Καταγραφή των δεδομένων που σχετίζονται με την συμπεριφορά των χρηστών και υπολογισμός των αντίστοιχων τιμών μέσω της εκτέλεσης ενός αλγορίθμου και με τρόπο που δεν επιτρέπεται καμμία εξωτερική παρέμβαση.
- *Ανεξαρτησία*. Καθορισμός των απαιτούμενων κατωφλίων από τους παρόχους υπηρεσιών τα οποία είναι απαραίτητα για τον υπολογισμό της συμπεριφοράς των χρηστών. Ο καθορισμός θα πρέπει να γίνεται με τρόπο που να απεικονίζει

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

πλήρως την πολιτική πρόσβασης και ασφάλειας που ακολουθείται από τον αντίστοιχο πάροχο, από τη στιγμή που οι τιμές των κατωφλίων καθορίζουν το βαθμό πρόσβασης που οι χρήστες αποκτούν στις προσφερόμενες υπηρεσίες.

- *Ανωνυμία/Ψευδωνυμία/Μη-Συνδεσιμότητα.* Αποσύνδεση των τιμών συμπεριφοράς με ένα συγκεκριμένο ψευδώνυμο το οποίο προσδιορίζει μοναδικά ένα χρήστη και οδηγεί σε συσχέτιση των συναλλαγών του και μείωση της ανωνυμίας του. Επομένως, μια συμπεριφορά θα πρέπει να συνδέεται με ένα μοναδικό ψευδώνυμο το οποίο χρησιμοποιείται ανά συναλλαγή.
- *Δικαιοσύνη.* Η ΥΚΣ θα πρέπει να αποδίδει μια συγκεκριμένη τιμή συμπεριφοράς σε κάθε καινούργιο χρήστη. Κάθε πάροχος θα πρέπει να προσδιορίσει την αρχική τιμή που αποδίδεται με βάση υποκειμενικά κριτήρια τα οποία προκύπτουν από την πολιτική ασφάλειας και πρόσβασης που έχει καθορίσει.
- *Εξελιξιμότητα.* Καθορισμός πολλαπλών επιπέδων λανθαμένων συναλλαγών που επηρεάζουν την συμπεριφορά των χρηστών σε διαφορετικό βαθμό.
- *Επιβράβευση.* Η ΥΚΣ θα πρέπει να ανταμείβει τους χρήστες που αλληλεπιδρούν με τους παρόχους, αυξάνοντας ή μειώνοντας τις αντίστοιχες τιμές συμπεριφοράς τους.
- *Ευελιξία.* Η ΥΚΣ θα πρέπει να είναι ευπροσάρμοστη και επαναπροσδιορίσιμη κατά την περίπτωση που οι πάροχοι επιθυμούν να επανακαθορίσουν τις τιμές κατωφλίων που απαιτούνται για τον υπολογισμό της συμπεριφοράς των χρηστών. Η διαδικασία θε πρέπει να εκτελεστεί με τρόπο που να είναι εντελώς διαφανής στις εμπλεκόμενες οντότητες.
- *Απόδοση.* Η ΥΚΣ δεν θα πρέπει να αυξάνει την πολυπλοκότητα της λειτουργίας του ΣΔΤ στο οποίο εφαρμόζεται. Θα πρέπει να έχει ελάχιστες απαιτήσεις όσον αφορά την αναγκαία υπολογιστική δύναμη και την πολυπλοκότητα των ανταλλασσόμενων μηνυμάτων.
- *Δυσδιάστατη.* Η συμπεριφορά ενός χρήστη διαιρείται σε δύο επίπεδα, στη συμπεριφορά η οποία επιδεικνύεται απέναντι σε ένα συγκεκριμένο πάροχο και στη συμπεριφορά απέναντι στο σύνολο των παρόχων που εμπιστεύονται το ΣΔΤ.
- *Επιεικής.* Η ΥΚΣ θα πρέπει να δίνει λιγότερο βάρος σε παλιότερες συναλλαγές που έχει εκτελέσει ένας χρήστης και να μην επιτρέπει τις απότομες αλλαγές στην τιμή συμπεριφοράς του. Οι αλλαγές της συμπεριφοράς των χρηστών θα πρέπει να γίνεται μετά από προσεκτική παρατήρηση της στάσης που επιδεικνύεται μετά από ένα σύνολο εκτελέσιμων αλληλεπιδράσεων.

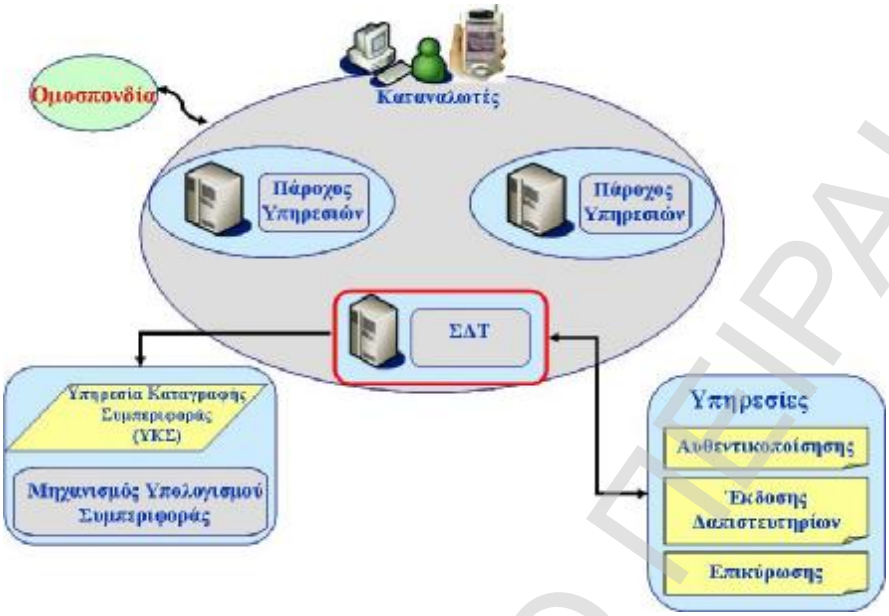
Η ικανοποίηση των ανωτέρω απαιτήσεων αποτελεί ένας δύσκολο αλλά παρόλα αυτά ουσιώδη στόχο που πρέπει να επιτυχθεί από την προτεινόμενη ΥΚΣ.

6.3.2 Εισαγωγή ΥΚΣ σε ένα ΣΔΤ

Η προτεινόμενη ΥΚΣ μπρορεί να λειτουργήσει ως μιας προστιθέμενης αξίας υπηρεσία ενός ΣΔΤ το οποίο ενεργεί ως Έμπιστη Τρίτη Οντότητα η οποία εξασφαλίζει και ελέγχει την εμπιστοσύνη στα πλαίσια μιας Ομοσπονδίας (βλ. § 5.4.2.1 και 5.4.3.1). Η ΥΚΣ επιτρέπει την ενίσχυση της προτεινόμενης αρχιτεκτονικής του ΣΔΤ προσφέροντας έναν αυτοματοποιημένο τρόπο με τον οποίο επιτυγχάνεται η αξιολόγηση της εμπιστοσύνης των εμπλεκόμενων οντοτήτων. Το Σχήμα 94 απεικονίζει σε υψηλό επίπεδο την ενισχυμένη αρχιτεκτονική ενός ΣΔΤ,

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

παρουσιάζοντας τις βασικές οντότητες που μετέχουν σε αυτό όπως επίσης και τις πτυχές της ΥΚΣ. Οι εμπλεκόμενες αυτές οντότητες είναι οι ακόλουθες:



Σχήμα 94: Ενισχυμένη Αρχιτεκτονική ΣΔΤ

α) *Καταναλωτές*: Οι χρήστες οι οποίοι μετέχουν στην ομοσπονδία και επιθυμούν να αποκτήσουν πρόσβαση στις η/κ-υπηρεσίες οι οποίες προσφέρονται από τους παρόχους. Η βασική τους ευθύνη επικεντρώνεται στην απόκτηση μιας καλής τιμής συμπεριφοράς προκειμένου να έχουν την δυνατότητα να αυξήσουν την προσβασιμότητά τους σε περισσότερες υπηρεσίες.
β) *Σύστημα Διαχείρισης Ταυτότητας (ΣΔΤ)*: η Έμπιστη Τρίτη Οντότητα (ΕΤΟ) η οποία διαχειρίζεται όλες τις πληροφορίες και τις προτιμήσεις των οντοτήτων ενώ παράλληλα παρέχει τα απαραίτητα διαπιστευτήρια που διασφαλίζουν τη ροή των ανταλλασσόμενων πληροφοριών. Επίσης, έχει υιοθετήσει την ΥΚΣ η οποία αποτελείται από το *Μηχανισμό Υπολογισμού Συμπεριφοράς (ΜΥΣ)* ο βασικός στόχος του οποίου είναι η παραγωγή και αποθήκευση των απαιτούμενων τιμών συμπεριφοράς των χρηστών με βάση τις υποδείξεις των παρόχων, μέσω της χρήσης ενός αλγόριθμου υπολογισμού συμπεριφοράς. Η ΥΚΣ θα πρέπει να λειτουργεί σε αρμονία με τις υπόλοιπες υπηρεσίες και διαδικασίες του ΣΔΤ ενισχύοντάς τες. Βασική της επιδίωξη είναι να δίνεται η δυνατότητα συγκέντρωσης όλων των έγκυρων θετικών/αρνητικών εκιμήσεων από τους παρόχους για τους χρήστες καθώς επίσης και η παροχή των απαραίτητων τιμών συμπεριφοράς που απαιτούνται για την διαδικασία εξουσιοδότησης από τους παρόχους. Η καταγραφή της συμπεριφοράς από την ΥΚΣ θέτει ως βασικό προαπαιτούμενο για την εκτέλεση της συγκεκριμένης διαδικασίας την ύπαρξη προγενέστερης έγκρισης από μέρους των χρηστών.
γ) *Πάροχοι Υπηρεσιών*: Οργανισμοί οι οποίοι προσφέρουν ένα σύνολο η/κ-υπηρεσιών. Λαμβάνουν αποφάσεις ελέγχου πρόσβασης με βάση δεδομένα εξουσιοδότησης (π.χ. τιμές συμπεριφοράς, ρόλος χρηστών) τα οποία εκδίδονται από το ΣΔΤ. Η συμπεριφορά των χρηστών όπως αυτή υπολογίζεται από τον ΜΥΣ της ΥΚΣ αποτελεί έναν πρόσθετο παράγοντα που πρέπει να ληφθεί υπόψη κατά την διάρκεια της διαδικασίας εξουσιοδότησης. Οι Πάροχοι χρησιμοποιούν τις διαδικασίες επικοινωνίας που προσφέρονται από το ΣΔΤ ώστε να δηλώσουν και να λάβουν τις εκτιμήσεις σχετικά με την συμπεριφορά των χρηστών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

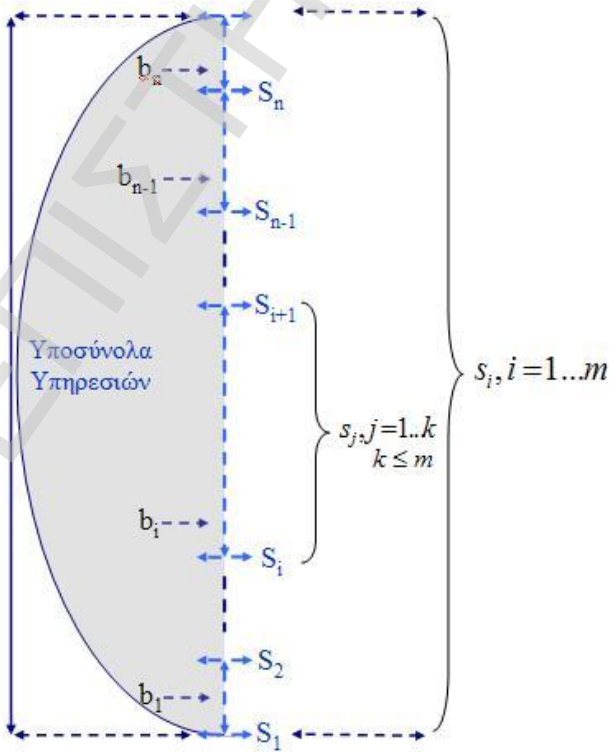
Στις παραγράφους που ακολουθούν περιγράφεται η λειτουργία του ΜΥΣ της ΥΚΣ και η παρουσίαση των ενισχυμένων μηχανισμών επικοινωνίας που θα επιτρέπουν την λήψη και διανομή των τιμών συμπεριφοράς μέσω της παρουσίασης ενός πλήρως εφαρμοζόμενου σενάριου.

6.3.3 Μηχανισμός Υπολογισμού Συμπεριφοράς (ΜΥΣ)

Ο ΜΥΣ είναι υπεύθυνος για τον υπολογισμό της συμπεριφοράς των καταναλωτών. Η συμπεριφορά του καταναλωτή χωρίζεται σε δύο επίπεδα, στη *Συμπεριφορά Καταναλωτή* (C_R) η οποία αποτυπώνει τη στάση που επιδεικνύει ένας καταναλωτής απέναντι σε έναν συγκεκριμένο Πάροχο Υπηρεσιών και στην *Συνολική Συμπεριφορά* (G_R) η οποία απεικονίζει τη συμπεριφορά του απέναντι σε όλους τους παρόχους που μετέχουν στην ομοσπονδία και εμπιστεύονται το ΣΔΤ.

Η ορθή λειτουργία του Μηχανισμού Υπολογισμού Συμπεριφοράς απαιτεί από τους παρόχους να εκτελέσουν μια σειρά βημάτων που θα επιτρέψουν στην ΥΚΣ την ορθή καταγραφή και υπολογισμό της συμπεριφοράς των χρηστών. Τα βήματα που πρέπει να ολοκληρωθούν είναι τα ακόλουθα:

α) *Προσδιορισμός Επιπέδου Ασφάλειας*
Σε πρώτη φάση κάθε πάροχος θα πρέπει να καθορίσει συγκεκριμένα επίπεδα ασφάλειας $b_i, i=1...n$ καθένα από τα οποία αναπαριστά και απεικονίζει τον βαθμό ευαισθησίας των πληροφοριών τις οποίες ο πάροχος διαχειρίζεται. Για παράδειγμα η διαχείριση μη ευαίσθητων πληροφοριών μπορεί να τεθεί στο επίπεδο $b_1=1$ ενώ η διαχείριση άκρως ευαίσθητων δεδομένων μπορεί να οριστεί στο επίπεδο $b_n=n$.



Σχήμα 95. Υποσύνολα Υπηρεσιών

β) Ιεραρχική *Κατηγοριοποίηση*

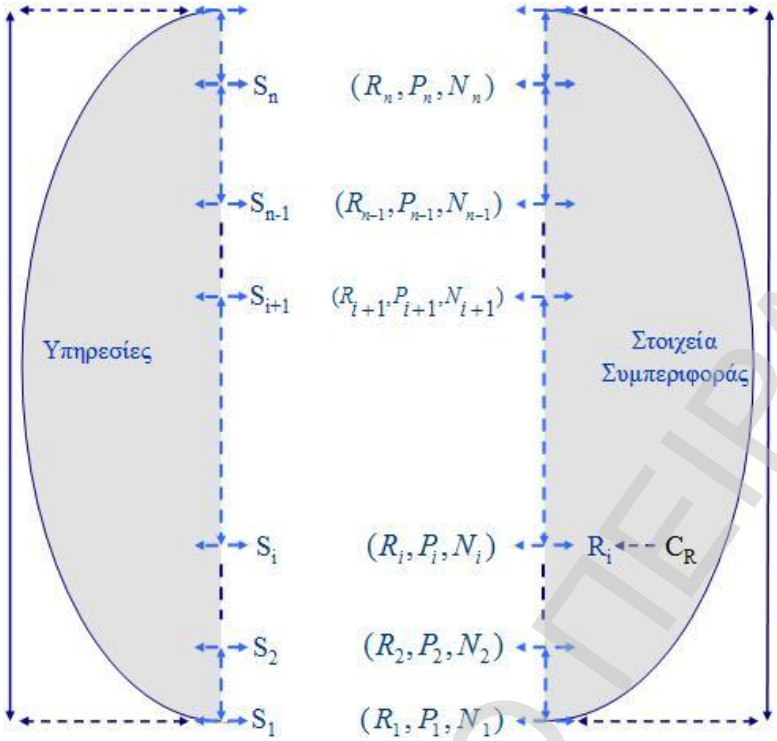
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Στη δεύτερη φάση ολοκληρώνεται η ιεραρχική κατηγοριοποίηση των προσφερόμενων η/κ-υπηρεσιών $s_i, i=1...m$ με βάση τα προσδιοριζόμενα επίπεδα ασφάλειας που ορίστηκαν στο πρώτο βήμα. Επομένως κάθε πάροχος αρχικά κατηγοριοποιεί όλες τις υπηρεσίες του σε σαφώς ορισμένα διατεταγμένα υποσύνολα $\{S_1,...,S_n\}$ με βάση το επίπεδο των ευαίσθητων πληροφοριών που κάθε υπηρεσία διαχειρίζεται, όπως απεικονίζεται στο Σχήμα 95. Για παράδειγμα $S_i < S_{i+1}$ στην περίπτωση που το υποσύνολο S_i περιλαμβάνει υπηρεσίες $s_j, j=1...k$ με $k \le m$ που διαχειρίζονται λιγότερο ευαίσθητα δεδομένα από τις υπηρεσίες του υποσυνόλου S_{i+1}, δηλαδή με $b_i < b_{i+1}$.

Ένα αντιπροσωπευτικό παράδειγμα κατηγοριοποίησης μπορεί να συναντηθεί στον τομέα της ηλεκτρονικής Διακυβέρνησης όπου ένας κυβερνητικός οργανισμός ενεργώντας ως πάροχος προσφέρει ένα σύνολο η/κ-υπηρεσιών. Στις προσφερόμενες υπηρεσίες περιλαμβάνονται οι ακόλουθες:

- μη κρίσιμες υπηρεσίες πληροφοριών ή παραπόνων οι οποίες ανήκουν σε μία κατηγορία S_l η οποία έχει συνδεθεί με ένα χαμηλό επίπεδο ασφάλειας b_l λόγω των μη ευαίσθητων πληροφοριών που αυτές διαχειρίζονται,
- περισσότερο κρίσιμες υπηρεσίες, όσον αφορά στο επίπεδο των διαχειριζόμενων πληροφοριών, όπως είναι η υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής οι οποίες ανήκουν σε μια κατηγορίας S_m στην οποία έχει αποδοθεί ένα μεσαίο επίπεδο ασφάλειας b_m, όπου $m > l$,
- υψηλής κρισιμότητας υπηρεσίες που εμπερικλείουν ιδιαίτερα ευαίσθητες πληροφορίες και οι οποίες εμπεριέχονται σε μια υψηλού επιπέδου ασφάλειας b_h κατηγορία S_h, όπου $h > m > l$. Παραδείγματα υπηρεσιών της τελευταίας κατηγορίας είναι οι υπηρεσίες έκδοσης ταυτοτήτων ή διαβατηρίων οι οποίες στον έντυπο κόσμο απαιτούν την παρουσία ενός έμπιστου μάρτυρα για να εγγυηθεί τη σύνδεση των ευαίσθητων εμπλεκόμενων πληροφοριών, όπως είναι η φωτογραφία του χρήστη, με τον αντίστοιχο χρήστη της υπηρεσίας. Στον ηλεκτρονικό κόσμο, η κατοχή μιας υψηλής τιμής συμπεριφοράς επιτρέπει την δημιουργία του έμπιστου πλαισίου που απαιτείται για τη χρήση της συγκεκριμένης υπηρεσίας, γεγονός που επιτρέπει την αυτοματοποίηση και ασφάλεια ιδιαίτερα κρίσιμων διαδικασιών.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 96. Καθορισμός Κατωφλίων

γ) *Καθορισμός Κατωφλίων*

Σε κάθε μία από τις κατηγορίες $S_i, i = 1...n$ που προέκυψαν από το δεύτερο βήμα, ο πάροχος ορίζει την ακόλουθη τριάδα κατωφλίων, όπως απεικονίζεται στο Σχήμα 96, δημιουργώντας αντίστοιχα ιεραρχικά υποσύνολα συμπεριφορών:

$$(R_i, P_i, N_i),\ i = 1,...,n \text{ όπου}$$

- R_i είναι η τιμή Συμπεριφοράς Καταναλωτή (C_R) που αποδίδεται σε έναν καταναλωτή προκειμένου να έχει πρόσβαση στις υπηρεσίες της συγκεκριμένης κατηγορίας αλλά και σε όλες τις υπηρεσίες οι οποίες ανήκουν σε υποσύνολα υπηρεσιών στα οποία έχει αποδοθεί μικρότερη τιμή συμπεριφοράς από αυτήν που έχει στην κατοχή του,
- P_i εκφράζει το ελάχιστο ποσοστό επιτυχών συναλλαγών που ένας καταναλωτής πρέπει να εκτελέσει από τη στιγμή που εισέρχεται και αποκτά πρόσβαση σε μια νέα κατηγορία υπηρεσιών S_i έτσι ώστε η συμπεριφορά του να αυξηθεί από R_i σε R_{i+1}.
- N_i απεικονίζει το μέγιστο ποσοστό ανεπιτυχών συναλλαγών που ένας καταναλωτής πρέπει να εκτελέσει από τη στιγμή που εισέρχεται και αποκτά πρόσβαση σε μια νέα κατηγορία υπηρεσιών S_i έτσι ώστε η συμπεριφορά του να μειωθεί από R_i σε R_{i-1}.

δ) *Οριοθέτηση Αρχικής Συμπεριφοράς*

Στην περίπτωση κατά την οποία ένας καταναλωτής επιχειρήσει να αποκτήσει πρόσβαση στις υπηρεσίες ενός παρόχου για πρώτη φορά ορίζεται σε αυτόν μια αρχική τιμή συμπεριφοράς $C_R = R_i$. Η τιμή αυτή είναι ανεξάρτητη για κάθε πάροχο και βασίζεται αποκλειστικά στην πολιτική πρόσβασης και ασφάλειας που έχει

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

καθορίσει. Επομένως ο καταναλωτής έχει τη δυνατότητα να αποκτήσει πρόσβαση στις υπηρεσίες του παρόχου που ανήκουν στο υποσύνολο S_i αλλά και σε αυτές που ανήκουν στα υποσύνολα $\{S_1,...,S_{i-1}\}$ στα οποία έχει αποδοθεί μικρότερη τιμή συμπεριφοράς από την R_i.

Η εκτέλεση των παραπάνω βημάτων από τους παρόχους αποτελούν προαπαιτούμενα για την ορθή λειτουργία του ΜΥΣ της ΥΚΣ. Η καταγραφή και ο υπολογισμός της συμπεριφοράς των χρηστών αποτελεί μια διαδικασία η οποία πραγματοποιείται από το ΜΥΣ σε δύο επίπεδα. Στο πρώτο επίπεδο πργματοποιείται ο *Υπολογισμός Συμπεριφοράς Καταναλωτή* (C_R) και στο δεύτερο ο *Υπολογισμός Συνολικής Συμπεριφοράς* (G_R). Η διαδικασία η οποία λαμβάνει χώρα σε κάθε επίπεδο είναι η ακόλουθη:

Συναλλαγές	**Τιμή Συμπεριγοράς**	
Από 1 μέχρι K_i	$C_R = R_i$	p_N, n_N υπολογισμός
Μετά από K_i	Περιπτώσεις	
	$C_R = R_{i+1}$	$s, f = 0$, $p_N = 0$, K_{i+1} $n_N = 0$
	$C_R = R_{i-1}$	$s, f = 0$, $p_N = 0$, K_{i-1} $n_N = 0$
	$C_R = R_i$	p_N, n_N υπολογισμός
		$K_i + 1$

Πίνακας 14. Κανόνες καθορισμού της Συμπεριφοράς Καταναλωτή (C_R)

α) *Υπολογισμός Συμπεριφοράς Καταναλωτή* (C_R)

Η C_R αποτυπώνει τη συμπεριφορά που επιδεικνύει ένας καταναλωτής απέναντι σε έναν συγκεκριμένο πάροχο. Από τη στιγμή, λοιπόν, που ο καταναλωτής εισέρχεται και του επιτρέπεται η είσοδος σε μια νέα κατηγορία υπηρεσιών S_i ορίζεται σε αυτόν η τιμή συμπεριφοράς R_i της συγκεκριμένης κατηγορίας ($C_R = R_i$).

Όπως παρουσιάζεται στον Πίνακας 14, για τις πρώτες K_i συναλλαγές που ο συγκεκριμένος καταναλωτής εκτελεί από την στιγμή που του ορίστηκε η νέα τιμή συμπεριφοράς μόνο προς τον συγκεκριμένο πάροχο, ο ΜΥΣ υπολογίζει τις ακόλουθες παραμέτρους:

το ποσοστό επιτυχών συναλλαγών: $p_N = \dfrac{\sum_{i=1}^{s} b_i}{\sum_{i=1}^{s} b_i + \sum_{i=1}^{f} a_i b_i}$,

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

το ποσοστό ανεπιτυχών συναλλαγών: $n_N = \frac{\sum_{i=1}^{f} a_i b_i}{\sum_{i=1}^{s} b_i + \sum_{i=1}^{f} a_i b_i}$,

όπου, s και f οι επιτυχημένες και αποτυχημένες συναλλαγές αντίστοιχα από τις K_i εκτελέσιμες συναλλαγές, b_i το επίπεδο ασφάλειας της κατηγορίας (βλ. § 6.3.3) στην οποία ανήκει η υπηρεσία για την οποία πραγματοποιήθηκε η συναλλαγή και a_i ο βαθμός βαρύτητας της αντίστοιχης κατηγορίας αποτυχημένων συναλλαγών (βλ. § 6.3).

Μετά από την εκτέλεση των K_i συναλλαγών από τον καταναλωτή προς τον συγκεκριμένο πάροχο και με βάση τη φύση των εκτελούμενων συναλλαγών, ο ΜΥΣ εκτελώντας τους κανόνες που ορίζονται στον Όπως παρουσιάζεται στον Πίνακας 14, γ διαμορφώνει την μελλοντική τιμή της Συμπεριφοράς Καταναλωτή (C_R). Σύμφωνα λοιπόν με τους κανόνες αυτούς διακρίνονται τρεις περιπτώσεις.

- *Περίπτωση 1.* Αν $p_N > P_i$ και $n_N < N_i$, όπου P_i και N_i το ελάχιστο ποσοστό επιτυχών και το μέγιστο ποσοστό ανεπιτυχών συναλλαγών αντίστοιχα που εχουν οριστεί για τη συγκεκριμένη κατηγορία, τότε η τιμή *Συμπεριφοράς Καταναλωτή* (C_R) αυξάνεται σε R_{i+1} ($C_R = R_{i+1}$).
- *Περίπτωση 2.* Αν $n_N > N_i$ η τιμή *Συμπεριφοράς Καταναλωτή* (C_R) μειώνεται σε R_{i-1} ($C_R = R_{i-1}$).
- *Περίπτωση 3.* Αν $p_N < P_i$ και $n_N > N_i$, η τιμή *Συμπεριφοράς Καταναλωτή* (C_R) παραμένει στα ίδια επίπεδα ($C_R = R_i$).

β) *Υπολογισμός Σφαιρικής Συμπεριφοράς* (G_R)

Η Υπηρεσία Καταγραφής Συμπεριφοράς, προκειμένου να έχει την δυνατότητα να προσφέρει στους παρόχους μια πιο ολοκληρωμένη εικόνα των προθέσεων του καταναλωτή όσον αφορά στον τρόπο με τον οποίο προτίθεται να αντιδράσει στις μελλοντικές του συναλλαγές υπολογίζει και τη *Σφαιρική Συμπεριφορά* (G_R) του. Η τιμή αυτή απεικονίζει τη συμπεριφορά του καταναλωτή απέναντι σε όλους τους παρόχους που μετέχουν στην ομοσπονδία και εμπιστεύονται το ΣΔΤ. Επομένως, ένας πάροχος έχει τη δυνατότητα να αντιληφθεί τον τρόπο με τον οποίο ο καταναλωτής συνήθως συμπεριφέρεται κατά τη διάρκεια των συναλλαγών του, προσφέροντάς του το ανάλογο επίπεδο πρόσβασης στις υπηρεσίες του.

Σε μια δεδομένη λοιπόν χρονική στιγμή κατά την οποία ένας καταναλωτής έχει εκτελέσει ένα σύνολο T συναλλαγών προς όλους τους παρόχους που μετέχουν στην ομοσπονδία από τις οποίες οι επιτυχημένες συναλλαγές είναι s_g και οι αποτυχημένες είναι f_g με $0 \le s_g, f_g \le T$ και $s_g + f_g = T$, η Σφαιρική Συμπεριφορά του καταναλωτή είναι η ακόλουθη:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

$$G_R = \frac{\sum_{i=1}^{s_g} b_i}{\sum_{i=1}^{s_g} b_i + \sum_{i=1}^{f_g} a_i}.$$

όπου, b_i το επίπεδο ασφάλειας της κατηγορίας (βλ. § 6.3.3) στην οποία ανήκει η υπηρεσία για την οποία πραγματοποιήθηκε η συναλλαγή και a_i ο βαθμός βαρύτητας της αντίστοιχης κατηγορίας αποτυχημένων συναλλαγών (βλ. § 6.3).

6.3.3.1 Επαναπροσδιορισμός Μηχανισμού Υπολογισμού Συμπεριφοράς

Κάθε πάροχος θα πρέπει να έχει την δυνατότητα να τροποποιήσει την υπάρχουσα παραμετροποίηση του ΜΥΣ, μεταβάλλοντας τις τιμές που έχουν δηλωθεί για τα κατώφλια χωρίς να επηρεάζεται η συνολική λειτουργία της ΥΚΣ και με τρόπο που να είναι εντελώς διαφανής στις εμπλεκόμενες οντότητες. Οι μεταβολές αυτές ενδέχεται να συμβούν εξαιτίας της αναπροσαρμογής της πολιτικής πρόσβασης και ασφάλειας που ακολουθείται από τους παρόχους. Οι πιθανές περιπτώσεις οι οποίες πρέπει να καλύπτονται είναι οι ακόλουθες:

- *Διαγραφή/Προσθήκη Υπηρεσίας*: Ο πάροχος επιλέγει το υποσύνολο στο οποίο η υπηρεσία θα προστεθεί ή από το οποίο θα διαγραφεί εκτελώντας την αντίστοιχη λειτουργία χωρίς την τροποποίηση των τιμών των κατωφλίων.
- *Συγχώνευση Υποσυνόλων Υπηρεσιών*: Δύο ή περισσότερα γειτονικά υποσύνολα υπηρεσιών (π.χ. S_{i-1}, S_i, S_{i+1} με R_{i-1}, R_i, R_{i+1}) συγχωνεύονται δημιουργώντας ένα νέο υποσύνολο (π.χ. S'_i με R'_i), το οποίο περιέχει όλες τις υπηρεσίες των συγχωνευθέντων υποσυνόλων. Ο πάροχος θα πρέπει σε πρώτη φάση να καθορίσει ένα νέο επίπεδο ασφάλειας b'_i που θα αναπαριστά το επίπεδο ευαισθησίας των πληροφοριών οι οποίες θα διαχειρίζονται από τις υπηρεσίες που θα ανήκουν στη νέα κατηγορία, ενώ στη συνέχεια απαιτείται ο καθορισμός των απαιτούμενων κατωφλίων (R'_i, P'_i, N'_i) για τη συγκεκριμένη κατηγορία. Η διαδικασία ολοκληρώνεται με τον ΜΥΣ να ενημερώνει τη τιμή της Συμπεριφοράς Καταναλωτή (C_R) για όλους τους καταναλωτές που ανήκαν στα συγχωνευμένα υποσύνολα ώστε να πάρουν την τιμή R'_i.
- *Προσθήκη ενός Νέου Υποσυνόλου Υπηρεσιών*: Ένας πάροχος δημιουργεί ένα νέο υποσύνολο S'_i καθορίζοντας ένα νέο επίπεδο ασφάλειας b'_i και ορίζοντας τα αντίστοιχα κατώφλια (R'_i, P'_i, N'_i).
- *Διαγραφή ενός Υποσυνόλου Υπηρεσιών*: Ένας πάροχος για να διαγράψει ένα υποσύνολο υπηρεσιών S_i με (R_i, P_i, N_i) θα πρέπει να μεταφέρει όλες τις υπηρεσίες σε άλλα υποσύνολα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Περιπτώσεις	Τιμή Συμπεριφοράς	
$p_N > P_i$ & $n_N < N_i$	$C_R = R_{i+1}$	$s, f = 0$, $p_N = 0$, $K = K_{i+1}$ $n_N = 0$
Διαφορετικά	$C_R = R_{i-1}$	$s, f = 0$, $p_N = 0$, $K = K_{i-1}$ $n_N = 0$

Πίνακας 15. Κανόνες για Διαγραφή Υποσυνόλου Υπηρεσιών

Η τιμή της Συμπεριφοράς Καταναλωτή (C_R) για όλους τους καταναλωτές που ανήκαν στο προς διαγραφή υποσύνολο ανανεώνεται με βάση τους κανόνες του Πίνακας 15 λαμβάνοντας υπόψη τις συναλλαγές που κάθε χρήστης έχει εκτελέσει μέχρι τη συγκεκριμένη στιγμή.
Σύμφωνα, λοιπόν με τους κανόνες αυτούς διακρίνονται οι ακόλουθες δύο περιπτώσεις.

- *Περίπτωση 1*. Αν $p_N > P_i$ και $n_N < N_i$, όπου P_i και N_i το ελάχιστο ποσοστό επιτυχών και το μέγιστο ποσοστό ανεπιτυχών συναλλαγών αντίστοιχα που έχουν οριστεί για τη διαγραφόμενη κατηγορία και p_N και n_N το ποσοστό των επιτυχών και ανεπιτυχών συναλαγών που έχει εκτελέσει ο κάθε χρήστης μέχρι εκείνη τη χρονική στιγμή τότε η τιμή *Συμπεριφοράς Καταναλωτή* (C_R) του αντίστοιχου χρήστη αυξάνεται σε R_{i+1} ($C_R = R_{i+1}$).
- *Περίπτωση 2*. Σε κάθε άλλη περίπτωση η τιμή *Συμπεριφοράς Καταναλωτή* (C_R) των αντίστοιχων χρηστών μειώνεται σε R_{i-1} ($C_R = R_{i-1}$).

Το στοιχείο που πρέπει να τονιστεί είναι ότι ο επαναπροσδιορισμός του ΜΥΣ αποτελεί μια ιδιαίτερα σημαντική διαδικασία η οποία θα πρέπει να εκτελεστεί με τη συμβολή ατόμων τα οποία διαθέτουν βαθιά γνώση της πολιτικής πρόσβασης και ασφάλειας του παρόχου, προκειμένου να αποφευχθεί οποιαδήποτε πιθανότητα μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες υπηρεσίες και δεδομένα.

6.3.4 Διαδικασίες ΥΚΣ

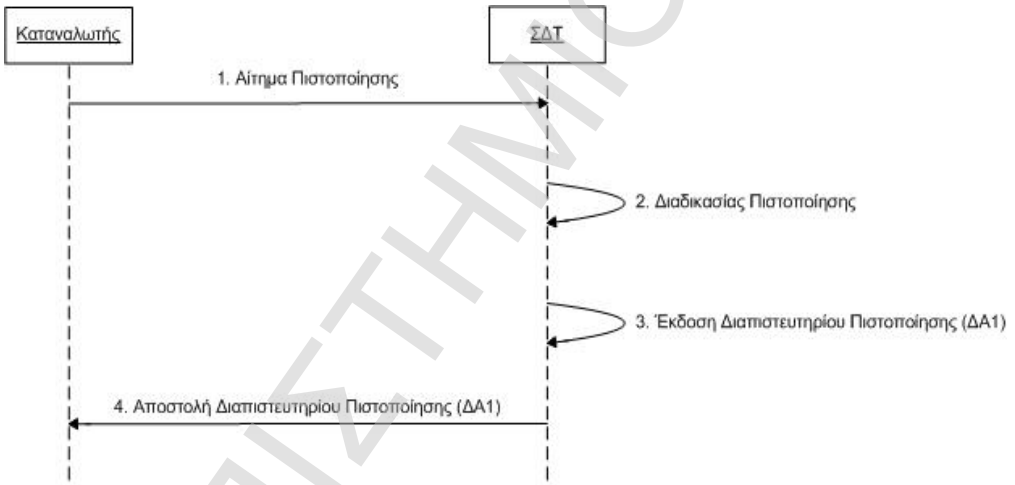
Στο παρόν κεφάλαιο περιγράφεται η λειτουργία της προτεινόμενης ΥΚΣ μέσω της παρουσίασης ενός πλήρους σεναρίου το οποίο εφαρμόζεται σε ένα ομοσπονδιακό πλαίσιο. Θεωρούμε λοιπόν την περίπτωση κατά την οποία ένα σύνολο κυβερνητικών οργανισμών όπως είναι οι δήμοι σε συνεργασία με τους δημότες τους και τους επιχειρησιακούς τους εταίρους δημιουργούν ένα πλαίσιο ομοσπονδίας [SWEB]. Η διαμορφώμενη σχέση εμπιστοσύνης μεταξύ των εμπλεκόμενων οντοτήτων μπορεί να εγγυηθεί από ένα ΣΔΤ το οποίο επιβλέπει και ελέγχει τη ροή των ανταλλασσόμενων πληροφοριών.
Το ΣΔΤ στοχεύοντας στην ενίσχυση της σχέσης εμπιστοσύνης μεταξύ των οντοτήτων έχει υιοθετήσει την προτεινόμενη ΥΚΣ. Οι εμπλεκόμενοι λοιπόν δήμοι καθένας από

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

τους οποίους προσφέρει ένα διακριτό σύνολο η/κ-υπηρεσιών, όπως είναι η κ-υπηρεσία έκδοσης εγγράφων πιστοποίησης μητρώου διαμονής και η/κ-υπηρεσία τιμολόγησης, θα πρέπει σε πρώτη φάση να προχωρήσει στην εκτέλεση των απαιτούμενων βημάτων, όπως αυτά ορίστηκαν στο Κεφάλαιο 6.3.3, ώστε να επιτραπεί η ορθή λειτουργία του ΜΥΣ της προτεινόμενης ΥΚΣ.
Στο πλαίσιο, λοιπόν, του περιγραφόμενου σεναρίου ένας δημότης επιθυμεί να χρησιμοποιήσει την κ-υπηρεσία έκδοσης εγγράφων μητρώου διαμονής η οποία προσφέρεται από τον «Δήμο Α» στον οποίο ανήκει. Κατά την παρουσίαση του σεναρίου θα περιγραφεί ο τρόπος λειτουργίας της ΥΚΣ σε συνδυασμό με τις άλλες υπηρεσίες του ΣΔΤ έτσι ώστε να διασφαλίζεται η ιδιωτικότητα του δημότη, ενώ ιδιαίτερη έμφαση θα δοθεί επίσης και στην περιγραφή των διαδικασιών οι οποίες σχετίζονται:

- με τη συλλογή των εκτιμήσεων με βάση τις οποίες πραγματοποιείται ο υπολογισμός της συμπεριφοράς των χρηστών, και
- με τον έλεγχο πρόσβασης ο οποίος πραγματοποιείται από τον δήμο επιτρέποντας ή απαγορεύοντας την πρόσβαση στις προσφερόμενες υπηρεσίες λαμβάνοντας υπόψη παράγοντες όπως είναι η συμπεριφορά του αιτούμενου.

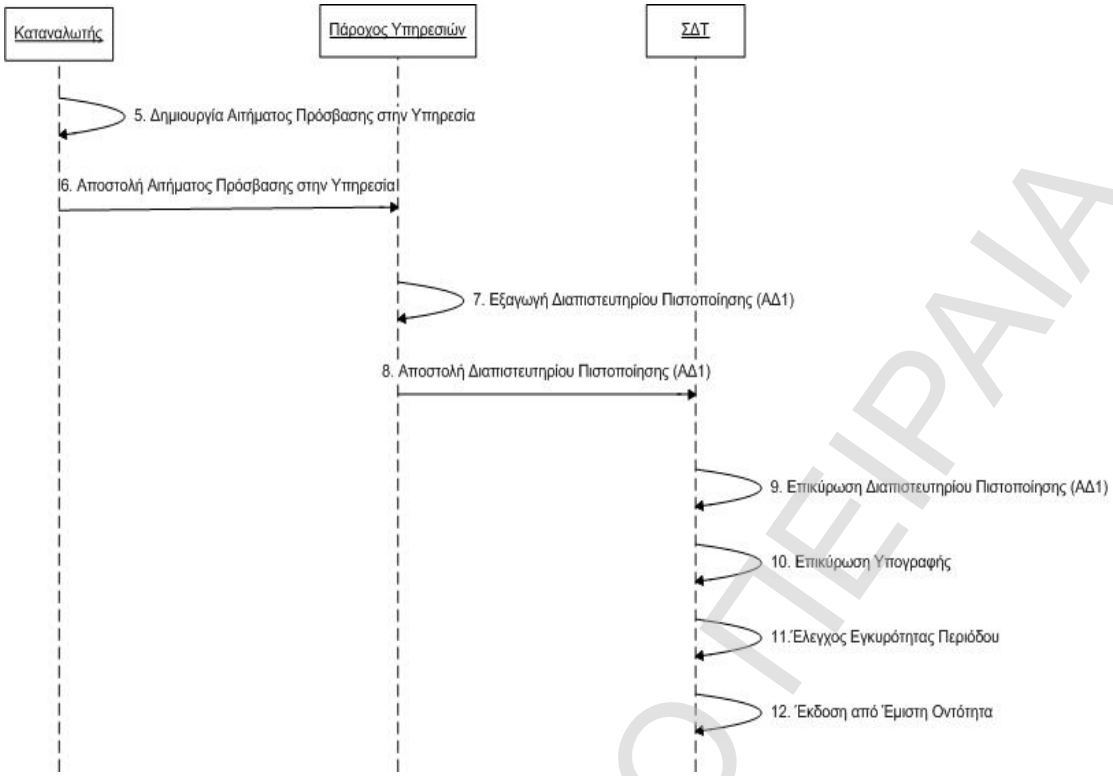
Τα ακριβή βήματα τα οποία πρέπει να εκτελεστούν προκειμένου ο δημότης να αποκτήσει πρόσβαση στην αιτούμενη υπηρεσία παρουσιάζονται ακολούθως.



Σχήμα 97. Διαδιακασίας Πιστοποίησης

Βήμα 1: *Διαδικασία Πιστοποίησης* (Σχήμα 97)
Ο δημότης θα πρέπει να επικοινωνήσει με το ΣΔΤ εκτελώντας τη διαδικασία πιστοποίησης. Για το λόγο αυτό δημιουργεί ένα αίτημα πιστοποίησης το οποίο περιέχει τις πληροφορίες πιστοποίησής του. Το αίτημα υποβάλλεται στο ΣΔΤ το οποίο τον αυθεντικοποιεί εκδίδοντάς του ένα Διαπιστευτήριο Πιστοποίησης (ΔΑ1). Το διαπιστευτήριο περιλαμβάνει πληροφορίες όπως είναι το ψευδώνυμο του δημότη, την περίοδο εγκυρότητας του διαπιστευτηρίου και πληροφορίες του ΣΔΤ που το εξέδωσε. Στη συνέχεια το διαπιστευτήριο υπογράφεται χρησιμοποιώντας τα πιστοποιητικά του ΣΔΤ και αποστέλλεται στον δημότη.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 98. Υποβολή Αιτήματος Πρόσβασης και Επικύρωσης Διαπιστευτηρίου

Βήμα 2: *Υποβολή Αίτησης Πρόσβασης της Υπηρεσίας* (Σχήμα 98)
Ο δημότης ανακτά το Διαπιστευτήριο Πιστοποίησης (ΔΑ1), και δημιουργεί το αίτημα πρόσβασης στην υπηρεσία το οποίο αποτελείται από το ΔΑ1 και από το αίτημα έκδοσης εγγράφου μητρώου διαμονής. Το αίτημα αποστέλλεται στον Δήμο Α ο οποίος εξάγει το ΔΑ1 και το στέλνει στο ΣΔΤ για να ελέγξει την εγκυρότητά του.

Βήμα 3: *Διαδικασία επικύρωσης του Διαπιστευτηρίου Πιστοποίησης* (Σχήμα 98)
Το ΣΔΤ μόλις λάβει το ΔΑ1 από τον δήμο ελέγχει αν ο δημότης για τον οποίο εκδόθηκε το διαπιστευτήριο έχει εκτελέσει κάποια άλλη συναλλαγή με τον συγκεκριμένο δήμο. Στην περίπτωση κατά την οποία ο δημότης δεν έχει χρησιμοποιήσει ξανά κάποια η/κ-υπηρεσία του δήμου ορίζεται σε αυτόν η τιμή συμπεριφοράς $C_R = R_i$, όπως αυτή έχει καθοριστεί από τον δήμο στην διάρκεια της δήλωσης των κατωφλίων.
Στην συνέχεια το ΣΔΤ επικυρώνει το ΔΑ1 ελέγχοντας τα ακόλουθα στοιχεία:

i. επικύρωση υπογραφής,
ii. έλεγχος ότι η περίοδος εγκυρότητας δεν έχει εκπνεύσει, και
iii. αν το διαπιστευτήριο έχει εκδοθεί από μια έμπιστη οντότητα.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Σύστημα Διαχείρισης Ταυτότητας	Ενέργειες Υπηρεσίας Καταγραφής Συμπεριφοράς	
Διαδικασίας Επικύρωσης		
Αποτυχημένη	Εκτέλεση Κανόνων Καθορισμού Συμπεριφοράς (Πίνακας 14)	
	Αποθήκευση	ΔΑ1
		κ-υπηρεσία έκδοσης εγγράφων μητρώου διαμονής
		Δήμος Α
		Αποτυχία Πιστοποίησης
Επιτυχημένη	Συνέχεια της διαδικασίας στο βήμα 4	

Πίνακας 16. Περιπτώσεις Διαδιακασίας επικύρωσης

Ο Πίνακας 16 παρουσιάζει όλες τις πιθανές περιπτώσεις της διαδικασίας επικύρωσης του διαπιστευτηρίου πιστοποίησης που εκτελείται από το ΣΔΤ.
Στην περίπτωση κατά την οποία η διαδικασία είναι αποτυχημένη η Υπηρεσία Καταγραφής Συπεριφοράς εκτελεί τους κανόνες καθορισμού συμπεριφοράς που παρουσιάζονται στον Πίνακας 14 και αποθηκεύει τοπικά το Διαπιστευτήριο Πιστοποίησης, την Αιτούμενη Υπηρεσία και τον Πάροχο Υπηρεσιών δηλώνοντας ότι η αντίστοιχη συναλλαγή χαρακτηρίζεται από «Αποτυχημένη Πιστοποίηση». Με τον τρόπο αυτό η ΥΚΣ διατηρεί όλα τις απαραίτητες πληροφορίες με βάση τις οποίες υπολογίζεται η συμπεριφορά του αντίστοιχου δημότη.
Σε περίπτωση που η διαδικασία επικύρωσης του διαπιστευτηρίου πιστοποίησης είναι επιτυχής, η διαδικασία για την απόκτηση πρόσβασης στην αιτούμενη υπηρεσία συνεχίζεται με την εκτέλεση του βήματος 4.

Σχήμα 99. Έκδοση Διαπιστευτηρίου Εξουσιοδότησης και Διαδικασία Ελέγχου Πρόσβασης

Βήμα 4: *Διαδικασία Έκδοσης Διαπιστευτηρίου Εξουσιοδότησης* (Σχήμα 99)
Το ΣΔΤ επανεκδίδει ένα νέο Διαπιστευτήριο Πιστοποίησης (ΔΑ2) το οποίο έχει μια πιο εκτεταμένη περίοδο ισχύος και ένα νέο ψευδώνυμο. Το νέο διαπιστευτήριο

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

υπογράφεται με το πιστοποιητικό του ΣΔΤ και κρυπτογραφείται χρησιμοποιώντας το πιστοποιητικό του δημότη. Επίσης το ΣΔΤ εκδίδει και ένα Διαπιστευτήριο Εξουσιοδότησης (ΔΕ1) το οποίο περιέχει τις ακόλουθες πληροφορίες:

- τα αποτελέσματα της διαδικασίας επικύρωσης του διαπιστευτηρίου πιστοποίησης,
- τις απαιτούμενες πληροφορίες για την ολοκλήρωση της διαδικασίας ελέγχου πρόσβασης από την ΑΠΥ οι οποίες αποτελούνται από τον ρόλο και τις αντίστοιχες τιμές συμπεριφοράς του δημότη (τη Συμπεριφορά Καταναλωτή (C_R) και τη Σφαιρική Συμπεριφορά (G_R)).

Τέλος, και τα δύο διαπιστευτήρια (ΔΑ2 και ΔΕ1) επιστρέφονται στον Δήμο Α ο οποίος τα εξάγει για να εκτελέσει την διαδικασία ελέγχου πρόσβασης στην αιτούμενη υπηρεσία.

Βήμα 5: *Διαδικασία Ελέγχου Πρόσβασης* (Σχήμα 99)
Το Διαπιστευτήριο Εξουσιοδότησης (ΔΕ1) χρησιμοποιείται από τον δήμο προκειμένου να εκτελέσει την απαραίτητη διαδικασία ελέγχου πρόσβασης. Με βάση τη διαδικασία αυτή επιτρέπει ή αρνείται την πρόσβαση στον δημότη στην αιτούμενη υπηρεσία. Οι πιθανές περιπτώσεις οι οποίες προκύπτουν είναι οι ακόλουθες, όπως παρουσιάζονται στον Πίνακας 17:

<table>
<tr><th colspan="4">Διαδιακασία Ελέγχου Πρόσβασης Παρόχου Υπηρεσιών</th><th colspan="2">Ενέργειες Υπηρεσίας Καταγραφής Συμπεριφοράς</th></tr>
<tr><td colspan="6"></td></tr>
<tr><td>Περιπτώσεις</td><td>Απόφαση Ελέγχου Πρόσβασης</td><td>Διαχείριση Αιτήματος</td><td>Απόφαση</td><td colspan="2"></td></tr>
<tr><td rowspan="5">Α</td><td>Μη-κατάλληλος ρόλος</td><td rowspan="5"></td><td rowspan="5">Άρνηση Πρόσβασης</td><td colspan="2">Εκτέλεση Κανόνων Καθορισμού Συμπεριφοράς (Πίνακας 14)</td></tr>
<tr><td rowspan="4">Τιμές Συμπεριφοράς C_R, G_R χαμηλές</td><td rowspan="4">Αποθήκευση</td><td>ΔΑ1</td></tr>
<tr><td>κ-υπηρεσία έκδοσης εγγράφων μητρώου διαμονής</td></tr>
<tr><td>Δήμος Α</td></tr>
<tr><td>Αποτυχία Εξουσιοδότησης</td></tr>
<tr><td rowspan="5">Β</td><td>ρόλος κατάλληλος</td><td rowspan="5">Αποτυχία ικανοποίησης των υποχρεώσεων που επιβάλλονται από τη υπηρεσία</td><td rowspan="5">Άρνηση Πρόσβασης</td><td colspan="2">Εκτέλεση Κανόνων Καθορισμού Συμπεριφοράς (Πίνακας 14)</td></tr>
<tr><td rowspan="4">Τιμές Συμπεριφοράς C_R, G_R επαρκείς</td><td rowspan="4">Αποθήκευση</td><td>ΔΑ1</td></tr>
<tr><td>κ-υπηρεσία έκδοσης εγγράφων μητρώου διαμονής</td></tr>
<tr><td>Πάροχος Υπηρεσιών</td></tr>
<tr><td>Αποτυχία Ικανοποίησης Απαιτούμενων Υποχρεώσεων</td></tr>
<tr><td rowspan="5">Γ</td><td>ρόλος κατάλληλος</td><td rowspan="5">Ικανοποίηση των υποχρεώσεων που επιβάλλονται από τη υπηρεσία</td><td rowspan="5">Παροχή Πρόσβασης</td><td colspan="2">Εκτέλεση Κανόνων Καθορισμού Συμπεριφοράς (Πίνακας 14)</td></tr>
<tr><td rowspan="4">Τιμές Συμπεριφοράς C_R, G_R επαρκείς</td><td rowspan="4">Αποθήκευση</td><td>ΔΑ1</td></tr>
<tr><td>κ-υπηρεσία έκδοσης εγγράφων μητρώου διαμονής</td></tr>
<tr><td>Πάροχος Υπηρεσιών</td></tr>
<tr><td>Έγκυρη Παροχή Πρόσβασης</td></tr>
</table>

Πίνακας 17. Καθορισμός Περιπτώσεων Ελέγχου Πρόσβασης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Περίπτωση Α: η πρόσβαση στην αιτούμενη υπηρεσία δεν επιτρέπεται εξαιτίας του γεγονότος ότι ο δημότης δεν κατέχει τα απαραίτητα δικαιώματα πρόσβασης, π.χ. ο ρόλος του δεν είναι κατάλληλος ή/και οι τιμές συμπεριφοράς του δεν είναι επαρκείς. Στην προκειμένη περίπτωση το αίτημα δεν ικανοποιείται και ο δήμος ενημερώνει την ΥΚΣ ότι η πρόσβαση στην υπηρεσία με χρήση του ΔΑ1 δεν έγινε αποδεκτή. Η ΥΚΣ με τη σειρά της προβαίνει στην εκτέλεση των κανόνων καθορισμού συμπεριφοράς που παρουσιάζονται στον Πίνακας 14. Παράλληλα αποθηκεύει τοπικά το Διαπιστευτήριο Πιστοποίησης ΔΑ1, την Αιτούμενη Υπηρεσία και τον Πάροχο Υπηρεσιών δηλώνοντας ότι η αντίστοιχη συναλλαγή χαρακτηρίζεται από «Αποτυχημένη Εξουσιοδότηση».

Περίπτωση Β: ο Δήμος ελέγχει ότι ο δημότης κατέχει τα απαιτούμενα διαπιστευτήρια εξουσιοδότησης και συνεχίζει με την διαχείριση του ίδιου του αιτήματος. Στο σημείο αυτό διαπιστώνει ότι οι υποχρεώσεις όπως αυτές τίθενται από την υπηρεσία δεν ικανοποιούνται, π.χ. ασυνέπεια στην αποκάλυψη των απαιτούμενων πληροφοριών. Ο Πάροχος ενημερώνει την Υπηρεσία Καταγραφής Συμπεριφοράς ότι η πρόσβαση στην υπηρεσία με χρήση του ΔΑ1 δεν έγινε αποδεκτή. Η ΥΚΣ εκτελεί τους κανόνες καθορισμού συμπεριφοράς που παρουσιάζονται στον Πίνακας 14 και αποθηκεύει τοπικά το Διαπιστευτήριο Πιστοποίησης ΔΑ1, την Αιτούμενη Υπηρεσία και τον Πάροχο Υπηρεσιών δηλώνοντας ότι η αντίστοιχη συναλλαγή χαρακτηρίζεται από «Αποτυχημένη Ικανοποίηση Απαιτούμενων Υποχρεώσεων».

Περίπτωση Γ: ο Δήμος επιτρέπει την πρόσβαση στην υπηρεσία και διαχειρίζεται επιτυχώς το αίτημα. Στη συνέχεια ενημερώνει την Υπηρεσία Καταγραφής Συμπεριφοράς ότι η πρόσβαση στην υπηρεσία με χρήση του ΔΑ1 ήταν επιτυχής. Η ΥΚΣ εκτελεί τους κανόνες καθορισμού συμπεριφοράς που παρουσιάζονται στον Πίνακας 14 και αποθηκεύει τοπικά το Διαπιστευτήριο Πιστοποίησης ΔΑ1, την Αιτούμενη Υπηρεσία και τον Πάροχο Υπηρεσιών δηλώνοντας ότι η αντίστοιχη συναλλαγή χαρακτηρίζεται από «Έγκυρη Παροχή Πρόσβασης».

Τέλος ο δήμος διαμορφώνει μια απάντηση με την οποία ενημερώνει τον δημότη σχετικά με την κατάσταση τους αιτήματος του. Η απάντηση αυτή περιέχει και το νέο Διαπιστευτήριο Πιστοποίησης (ΔΑ2) το οποίο εκδόθηκε από το ΣΔΤ με το νέο ψευδώνυμό του, το οποίο θα χρησιμοποιήσει στην επόμενη συναλλαγή του.

6.4 Αξιολόγηση Προτεινόμενης ΥΚΣ

Η προτεινόμενη Υπηρεσία Καταγραφής Συμπεριφοράς επιτυγχάνει να καλύψει ένα σύνολο αδυναμιών:
Αυτονομία/Ακρίβεια: Η ΥΚΣ καταγράφει το σύνολο των στοιχείων (διαπιστευτήρια, αιτούμενη υπηρεσία, πάροχος υπηρεσιών) τα οποία σχετίζονται με τις συναλλαγές που εκτελούν οι καταναλωτές. Επομένως, ο υπολογισμός της συμπεριφοράς των καταναλωτών γίνεται με βάση απτά στοιχεία και όχι τυχόν αβάσιμες πολλές φορές υποδείξεις κακόβουλων οντοτήτων.
Ανεξαρτησία: Η ευθύνη των Παρόχων Υπηρεσιών περιορίζεται στην εκτέλεση της απαιτούμενης κατηγοριοποίησης των προσφερόμενων υπηρεσιών και του καθορισμού των αναγκαίων για τον υπολογισμό της συμπεριφοράς κατωφλίων. Η ΥΚΣ αναλαμβάνει τον υπολογισμό, την αποθήκευση και την διανομή των τιμών

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συμπεριφοράς χωρίς να επιτρέπει κάποια εξωτερική παρέμβαση να επηρεάζει τη λειτουργία της.
Άδικες και Ανακριβείς Εκτιμήσεις: Στο Κεφάλαιο 6.3.2 παρουσιάστηκαν οι τύποι αποτυχημένων συναλλαγών με βάση τους οποίους οι πάροχοι δηλώνουν ακριβείς και δίκαιες εκτιμήσεις σχετικά με τη συμπεριφορά των καταναλωτών. Επιπλέον, η χρησιμοποίηση διαφορετικού διαπιστευτηρίου πιστοποίησης και επομένως και ψευδωνύμου για κάθε συναλλαγή από μέρους του καταναλωτή αποτρέπει τον πάροχο να ευννοήσει ή να αδικήσει συγκεκριμένους καταναλωτές.
Περιορισμένος αριθμός Εκτιμήσεων: Οι πάροχοι για κάθε διαπιστευτήριο πιστοποίησης το οποίο προσκομίζουν στο ΣΔΤ για να το επικυρώσει θα πρέπει να δηλώσουν αν η αντίστοιχη συναλλαγή ήταν επιτυχής ή όχι. Επιπλέον, ο καθορισμός μιας αρχικής τιμή *Συμπεριφοράς Καταναλωτή* (C_R) για έναν νεο-εισερχόμενο καταναλωτή μπορεί να αντισταθμίζει τον περιορισμένο αριθμό εκτιμήσεων.
Ιδιωτικότητα: Οι διαδικασίες με τον τρόπο με τον οποίο περιγράφηκαν στο Κεφάλαιο 6.3.4 δίνουν την δυνατότητα στον καταναλωτή να αποκτά πρόσβαση σε υπηρεσίες χρησιμοποιώντας κάθε φορά διαφορετικό διαπιστευτήριο πιστοποίησης άρα και διαφορετικό ψευδώνυμο. Το γεγονός αυτό επιτρέπει την αποσύνδεση των τιμών συμπεριφοράς του καταναλωτή με ένα συγκεκριμένο ψευδώνυμο το οποίο τον προσδιορίζει μοναδικά και οδηγεί σε συσχέτιση και σύνδεση των συναλλαγών του άρα και μείωση της ανωνυμίας του.

Η προτεινόμενη υπηρεσία μέσω της διευθέτησης των παραπάνω αδυναμιών επιτυγχάνει να ενισχύσει την αξιοπιστία και την ακρίβειας της.

6.5 Συμπεράσματα – Μελλοντικές Επεκτάσεις

Με το πέρασμα του χρόνου, οι καταναλωτές και οι πάροχοι υπηρεσιών συνειδητοποίησαν ότι η επίτευξη της εμπιστοσύνης αποτελεί μια κρίσιμη παράμετρο για την ολοκλήρωση αξιόπιστων συναλλαγών. Η ικανοποίηση της απαίτησης για εμπιστοσύνη αποτελεί έναν δύσκολο μα απαραίτητο στόχο. Στις μέρες μας, η επικρατούσα τάση είναι η δημιουργία ομοσπονδιών στα πλαίσια των οποίων όλοι οι συμμετέχοντες θεωρούνται ως έμπιστες οντότητες.
Η ενσωμάτωση μιας Υπηρεσίας Καταγραφής Συμπεριφοράς στα Συστήματα Διαχείρισης Ταυτότητας τα οποία αποτελούν τις κεντρικές οντότητες των ομοσπονδιών επιτρέπει την ενίσχυση των πλαισίων αυτών μέσω της υιοθέτησης μιας αυτοματοποιημένης διαδικασίας αξιολόγησης της εμπιστοσύνης των εμπλεκόμενων οντοτήτων. Η προτεινόμενη υπηρεσία αξιολογεί την αξιοπιστία των καταναλωτών παρέχοντας στους παρόχους αντικειμενικές και έμπιστες εκτιμήσεις οι οποίες αποκαλύπτουν τις προθέσεις τους όσον αφορά τον τρόπο με τον οποίο προτίθενται να συμπεριφερθούν στις μελλοντικές τους συναλλαγές. Οι εκτιμήσεις αυτές μπορούν επίσης να χρησιμοποιηθούν και ως επιπλέον κριτήριο από τους παρόχους επιτρέποντας τους να εκτελέσουν καλώς διαμορφωμένες αποφάσεις ελέγχου πρόσβασης.
Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που αφορούν την προτεινόμενη ΥΚΣ είναι οι ακόλουθες:

- Επέκταση της προσφερόμενης λειτουργικότητας, επιτρέποντας στην ΥΚΣ τη συσσώρευση γνώσης σχετικά με τους παρόχους υπηρεσιών υπολογίζοντας και καταγράφοντας και τη συμπεριφορά που επιδεικνύουν και αυτοί με τη σειρά τους. Η γνώση αυτή μπορεί να χρησιμοποιηθεί από τους καταναλωτές ως

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

κριτήριο επιλογής του πιο αξιόπιστου παρόχου. Επιπλέον έρευνα θα πρέπει να εκτελεστεί προκειμένου να διερευνηθεί η ομαλή ολοκλήρωση και αυτής της διαδικασίας στο ομοσπονδιακό πλαίσιο χωρίς να αυξηθεί η υποκείμενη πολυπλοκότητα.

- Ο αυτόματος συνδυασμός δεδομένων συμπεριφοράς από ένα δεδομένο πλαίσιο αναφοράς σε ένα άλλο αποτελεί μία δύσκολη πρόκληση η οποία δυσχεραίνεται ακόμα περισσότερο εάν οι αντίστοιχοι χρήστες έχουν απαιτήσεις ιδιωτικότητας. Οι γλώσσες οντολογίας όπως η OWL αποτελούν αυτή τη στιγμή τον καλύτερο τρόπο για την εξασφάλιση της διαλειτουργικότητας μεταξύ της σημασιολογίας διαφορετικών κρίσεων συμπεριφοράς, ώστε να είναι δυνατή η λήψη μιας συνδυασμένης τιμής συμπεριφοράς από ετερογενής πηγές.
- Η δημιουργία ενός προτυποποιημένου τρόπου αναπαράστασης δεδομένων συμπεριφοράς και ενσωμάτωσής τους σε πρωτόκολλα μεταφοράς πληροφοριών όπως είναι το SAML.

Η καταγραφή της συμπεριφοράς από μια υπηρεσία ή ένα σύστημα καταγραφής συμπεριφοράς μπορεί αναμφισβήτητα να προσφέρει οφέλη τα οποία να ενισχύσουν σε σημαντικό βαθμό την αξιοπιστία των η/κ-συναλλαγών και να δημιουργήσουν ένα έμπιστο και ασφαλή περιβάλλον στα πλαίσια του οποίου ευννοείται η συνεργασία μεταξύ των οντοτήτων.

6.6 Αναφορές

[Haddad08] W. Haddad. (2008). "*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*", Network Working Group, IETF Trust.

[Mui02] L. Mui, M. Mohtashemi, A. Halberstadt. (2002). "*A Computational Model of Trust and Reputation*", Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.

[Amazon], Amazon, at http://www.amazon.com/.

[Resnick02] P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood. (2002). "*The value of reputation on eBay: A controlled experiment*", Working paper originally presented at the ESA conference, June 2002.

[BizRate] BizRate, at www.bizrate.com/.

[Traupman06] J. Traupman and R. Wilensky. (2006). "*Robust Reputations for Peer-to-Peer Markets*", Proc. International Conference on Trust Management (iTrust), 2006.

[Carrara07] E. Carrara, G. Hogben (Editors). (2007). "*Reputation-based Systems: A security analysis*", ENISA position paper, October 2007.

[Jøsang07] A. Jøsang, R. Ismail, and C. Boyd. (2007). "*A survey of trust and reputation systems for online service provision*", Decision Support Systems 43(2):pp. 618-644.

[Lin05] K. J. Lin et al.. (2005). "*A Reputation and Trust Management Broker Framework for Web Applications*", Proc. IEEE International Conference on e-Technology, e-Commerce, and e-Services, IEEE CS Press, 2005, pp. 262–269.

[Park05] S. Park, L. Liu, C. Pu, M. Srivatsa, and J. Zhang. (2005). "*Resilient Trust Management for Web Service Integration*", Proc. IEEE Int'l Conf. Web Services (ICWS '05), pp. 499-506, 2005.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Kamvar03] S. Kamvar, M. Scholsser, and H. Garcia-Molina. (2003). "*The EigenTrust Algorithm for Reputation Management in P2P Networks*", Proceedings of the 12th international conference on World Wide Web, 2003.
[Damiani02] E. Damiani, S. D. C. Vimercati, S. Paraboschi, P. Samarati, and F. Violante. (2002). "*A reputation-based approach for choosing reliable resources in peer-to-peer networks*", 9th ACM Conference on Computer and Communications Security, Washington, DC, USA.
[Zou07] Y. Zou, L. Gu, G. Li, B. Xie, H. Mei. (2007). "*Rectifying Prejudicial Feedback Ratings in Reputation based Trust Management*", IEEE International Conference on Services Computing (SCC 2007), pp.530-535, 2007.
[Cahill03] V. Cahill, B. Shand, E. Gray, et al.. (2003). "*Using Trust for Secure Collaboration in Uncertain Environments*", Pervasive Computing, 2(3):52.61, July-September 2003.
[Carbone03] M. Carbone, M. Nielsen, and V. Sassone. (2003). "*A Formal Model for Trust in Dynamic Networks*", International Conference on Software Engineering and Formal Methods (SEFM'03), Brisbane, September 2003.
[Jøsang01] A. Jøsang. "*A Logic for Uncertain Probabilities*", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279.311, June 2001.
[Sabater02a] J. Sabater, C. Sierra. (2002). "*Reputation and Social Network Analysis in Multi-Agent Systems*", In Proceedings of the First Int. Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS), July 2002.
[Sabater02b] J. Sabater, C. Sierra. (2002). "*Social ReGreT, a reputation model based on social relations*", SIGecom Exchanges, 3.1:44.56, 2002.
[Levien04] R. Levien. (2004). "*Attack Resistant Trust Metrics*", PhD thesis, University of California at Berkeley, 2004.
[Ziegler04] C.-N. Ziegler, G. Lausen. (2004). "*Spreading Activation Models for Trust Propagation*", IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE '04), Taipei, March 2004.
[Withby05] A. Withby, A. Jøsang, and J. Indulska. (2005). "*Filtering Out Unfair Ratings in Bayesian Reputation Systems*", The Icfain Journal of Management Research, 4(2):48.64, 2005.
[Sen02] S. Sen and N. Sajja. (2002). "*Robustness of Reputation-based Trust: Boolean Case*", First Int. Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS). ACM, July 2002.
[Dellarocas00] C. Dellarocas. (2000). "*Immunizing online reputation reporting systems against unfair ratings and discriminatory behaviour*", 2nd ACM Conference on Electronic Commerce, Minneapolis, MN, USA.
[Miller03] N. Miller, P. Resnick, and R. Zeckhauser. (2003). "*Eliciting Honest Feedback in Electronic Markets*", Working paper originally prepared for the SITE'02 workshop, February 11 2003.
[Jurca03] R. Jurca and B. Faltings. (2003). "*An Incentive Compatible Reputation Mechanism*", 6th Int. Workshop on Deception Fraud and Trust in Agent Societies (at AAMAS'03).
[Steinbrecher07] S. Steinbrecher. (2007). "*Privacy-respecting Reputation System for Future Internet Communities*", ENISA eID Workshop, May 2007.
[Friedman01] E. Friedman, P. Resnick. (2001). *"The Social Cost of Cheap Pseudonyms*", Journal of Economics and Management Strategy 10(2): 173-199.
[LibertyAlliance] Liberty Alliance. "*Liberty ID-WSF Web Services Framework Overview*", version 2.0 specifications, http://www.projectliberty.org.

PARENTHESIS MONTERAY

[Lockhart06] H. Lockhart et al.. (2006). "*Web Services Federation Language (WS-Federation)*", Version 1.1 December 2006.
[Andersson05] C. Andersson, J. Camenisch, S. Crane, S. Fischer-Hubner, R. Leenes, S. Pearsorr, J.S. Pettersson, D. Sommer. "*Trust in PRIME*", Fifth IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp.552-559, 2005.
[Crane06] S. Crane, M. C. Mont. (2006). "*A Customizable Reputation-based Privacy Assurance System using Active Feedback*", Securecomm and Workshops, 2006.
[SWEB] Sixth Framework Programme, Priority 2, Information Society Technologies, (2007), "Secure, interoperable, cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries – SWEB", IST-2006-2.6.5, Available at www.sweb-project.org.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

7 Μηχανισμοί διευθέτησης της Ανωνυμίας σε Επίπεδο Σύνδεσης

Το παρόν κεφάλαιο εστιάζει στη διερεύνηση μηχανισμών οι οποίοι μπορούν να διευθετήσουν την Ανωνυμία σε Επίπεδο Σύνδεσης των ΥΙ. Μελετώνται υπάρχουσες προσεγγίσεις που στρέφονται προς την κατεύθυνση αυτή και καταγράφονται συγκεκριμένες αδυναμίες τους. Βασικός στόχος του κεφαλαίου αποτελεί η πρόταση ενός Ολιστικού Μοντέλου Ανωνυμίας για Υπηρεσίες Ιστού. Το προτεινόμενο μοντέλο είναι εφαρμόσιμο σε η/κ-Υπηρεσίες Ιστού οι οποίες είναι ανθεκτικές σε μεγάλες χρονικές καθυστερήσεις.

7.1 Εισαγωγή

Η σύγχρονη ψηφιακή εποχή όπως αναφέρθηκε στο Κεφάλαιο 4.2.3 χαρακτηρίζεται από την απαίτηση για ιδιωτικότητα. Ιδιαίτερα έντονη είναι η ανάγκη για ανώνυμη πρόσβαση σε πολλές η/κ-Υπηρεσίες Ιστού όπως είναι η η/κ-παραγγελιοδοσία επιτρέποντας την εκτέλεση μη-ανιχνεύσιμων, μη-συνδέσιμων και μη-παρατηρήσιμων συναλλαγών [Haddad08] με την συμμετοχή μη ευπροσδιόριστων οντοτήτων.
Η ανωνυμία έχει δύο ανεξάρτητες μα στενά συνδεόμενες πτυχές, την *ανωνυμία δεδομένων* και την *ανωνυμία σύνδεσης* [Gabber99, Tillwick06]. Η ανωνυμία δεδομένων σχετίζεται με την γνωστοποίηση πληροφοριών οι οποίες δεν αποκαλύπτουν την πραγματική ταυτότητα μιας οντότητας. Η διευθέτηση της πτυχής αυτής πραγματοποιείται στο επίπεδο της εφαρμογής με την χρήση συνήθως Συστημάτων Διαχείρισης Ταυτότητας (όπως αυτά παρουσιάστηκαν στο Κεφάλαιο 5).
Αντίθετα η ανωνυμία σύνδεσης αφορά την προστασία του διαύλου επικοινωνίας ανάμεσα στα σημεία τα οποία αποτελούν την αρχική πηγή και τον τελικό αποδέκτη της κίνησης. Βασικός της στόχος αποτελεί η συγκάλυψη της σχέσης μεταξύ του ανταλλασσόμενου μηνύματος και του αποστολέα και του παραλήπτη του συγκεκριμένου μηνύματος. Οι λύσεις οι οποίες έχουν προταθεί για την ικανοποίηση της ανωνυμίας σε επίπεδο σύνδεσης εφαρμόζονται στην πλειοψηφία τους στο επίπεδο της μεταφοράς. Πρόκειται στην πραγματικότητα για *δίκτυα ανωνυμίας* τα οποία εξασφαλίζουν την απόκρυψη της διαδρομής που ακολουθεί η ανταλλασσόμενη κίνηση ενώ παράλληλα επιτρέπουν την παροχή κρυμμένων υπηρεσιών.
Οι προτεινόμενες λύσεις οι οποίες μπορούν να εφαρμοστούν στην περίπτωση των η/κ-Υπηρεσιών Ιστού παρουσιάζουν σημαντικές αδυναμίες, καθώς είναι ευάλωτες από ισχυρούς επιτιθέμενους οι οποίοι κατέχουν μεγάλη υπολογιστική δύναμη και είναι ικανοί παρατηρώντας τα μηνύματα τα οποία ανταλλάσσονται να εκτελέσουν χρονικούς συσχετισμούς.
Στο πλαίσιο του συγκεκριμένου κεφαλαίου αναγνωρίζεται η σημασία της ανωνυμίας σύνδεσης και διαπιστώνεται η έλλειψη επαρκών μηχανισμών με τους οποίους μπορεί αυτή να διευθετηθεί σε ικανοποιητικό βαθμό. Τα στοιχεία αυτά οδήγησαν στην πρόταση ενός Ολιστικού Μοντέλου Ανωνυμίας για Υπηρεσίες Ιστού [Papastergiou08b]. Το προτεινόμενο μοντέλο είναι εφαρμόσιμο σε η/κ-Υπηρεσίες Ιστού οι οποίες είναι ανθεκτικές σε μεγάλες χρονικές καθυστερήσεις κατά την διάρκεια της ανταλλαγής των μηνυμάτων. Οι δυνατότητες που προσφέρει το μοντέλο είναι οι ακόλουθες:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- **ü** Ικανοποίηση της απαίτησης για ανωνυμία δεδομένων μέσω της υιοθέτησης ενός ΣΔΤ και την εφαρμογή διαδικασιών οι οποίες παρουσιάστηκαν στο Κεφάλαιο 5.
- **ü** Ικανοποίηση της ανωνυμίας σύνδεσης με τη υιοθέτηση προτύπων και τεχνολογιών βασισμένων στις Υπηρεσίες Ιστού όπως το WS-Addressing [WebAddressing06] καθώς επίσης και τη χρήση ενός ευρέως διαδεδομένου δικτύου ανωνυμίας, του Tor [Dingledine04], εκμεταλλευόμενο τα οφέλη τα οποία αυτό προσφέρει. Το γεγονός που πρέπει να σημειωθεί είναι ότι σε αντίθεση με τα υπόλοιπα δίκτυα ανωνυμίας η προτεινόμενη λύση διευθετεί την συγκεκριμένη πτυχή παρέχοντας δύο επίπεδα ανωνυμίας σε επίπεδο σύνδεσης και σε επίπεδο μεταφοράς.

Στις παραγράφους που ακολουθούν αρχικά γίνεται μια παρουσίαση των υπαρχόντων δικτύων ανωνυμίας παραθέτοντας της αδυναμίες τους ενώ στην συνέχεια πραγματοποιείται μια περιγραφή του προτεινόμενου μοντέλου και διερευνάται η ανθεκτικότητά του απέναντι σε ένα σύνολο γνωστών επιθέσεων.

7.2 Υπάρχοντες Μηχανισμοί Ανωνυμίας σε Επίπεδο Σύνδεσης

Ένα μείζον ζήτημα για την ανωνυμία της επικοινωνίας είναι η ανάλυση της κίνησης [Raymond00]. Η ανάλυση της κίνησης περιλαμβάνει τη λήψη και εξέταση της ανταλλασσόμενης κίνησης με στόχο να εκμαιευτούν ευαίσθητα προσωπικά δεδομένα επιδιώκοντας τη μείωση της ιδιωτικότητας των οντοτήτων που μετέχουν στη συναλλαγή. Η διαδικασία αυτή μπορεί να πραγματοποιηθεί ακόμα και στην περίπτωση κατά την οποία η κίνηση είναι κρυπτογραφημένη και δεν μπορεί να αποκρυπτογραφηθεί.

Το πρώτο βήμα για την ανωνυμία της επικοινωνίας έγινε από το D. Chaum [Chaum81] με την παρουσίαση των *"δικτύων ανάμειξης"*. Ένας *"αναμίκτης"* αποτελεί έναν κόμβο αποθήκευσης-και-προώθησης σε ένα δίκτυο το οποίο τροποποιεί τα λαμβανόμενα μηνύματα χρησιμοποιώντας κάποιον κρυπτογραφικό μετασχηματισμό και τα προωθεί σε μια επαναπροσδιοριζόμενη σειρά με έναν τέτοιο τρόπο που να δυσκολεύει την συσχέτιση των εισερχόμενων και εξερχόμενων μηνυμάτων, ειδικά στην περίπτωση κατά την οποία ένα σύνολο μηνυμάτων αναμεταδίδονται ταυτόχρονα. Υπάρχει βέβαια η δυνατότητα αντί να χρησιμοποιηθεί ένας μοναδικός έμπιστος αναμίκτης να χρησιμοποιηθούν μια αλυσίδα από αναμίκτες προκειμένου να προωθηθούν τα μηνύματα.

Μια προσέγγιση κατασκευής δικτύων ανάμειξης περιλαμβάνει την διαδικασία *"ελεύθερης επιλογής διαδρομής"* η οποία εκτελείται από την οντότητα η οποία αρχικοποιεί την επικοινωνία. Οι επιλεγμένοι κόμβοι προώθησης αλληλοσυνδέονται εγκαθιδρύοντας την διαδρομή επικοινωνίας εκμέρους του αρχικοποιητή. Ο συγκεκριμένος τύπος δικτύου ανάμειξης ονομάζεται δίκτυο*"ελεύθερης διαδρομής"*. Ένας άλλος τύπος είναι τα δίκτυα *"σύζευξης"* στα οποία οι κόμβοι προώθησης ομαδοποιούνται σε ένα σύνολο σταθερών διαδρομών και ο αρχικοποιητής επιλέγει μόνο από αυτό το σύνολο μια συγκεκριμένη διαδρομή προκειμένου να αναμεταδόσει τη κίνηση του.

Μια πρώτη εφαρμογή μιας αρχιτεκτονικής βασισμένης σε δίκτυα ανάμειξης βασίζεται στην παροχή ανώνυμων υπηρεσιών ηλεκτρονικού ταχυδρομίου. Η αρχιτεκτονική αυτή αποτελεί τον τύπο Ι εφαρμογών ηλεκτρονικού ταχυδρομίου. Προκειμένου να ενισχυθεί η ανωνυμία των υπηρεσιών αυτών, μηχανισμοί όπως είναι η εισαγωγή εσκεμμένων μεταβλητών καθυστέρησης και ο επαναπροσδιορισμός της

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

σειράς αναμετάδοσης των μηνυμάτων ενσωματώθηκαν στο σχεδιασμό του Mixmaster [Moeller04] ή αλλιώς τύπου ΙΙ υπηρεσιών ηλεκτρονικού ταχυδρομίου. Η έρευνα της ανωνυμίας στο επίπεδο των συγκεκριμένων υπηρεσιών συνεχίστηκε με το Mixminion [Danezis03] το οποίο εξασφαλίζει την μυστική προώθηση και υποστηρίζει ποικίλλα σχήματα εικονικής κίνησης και παραγεμίσματος.
Τεχνικές όπως ο επαναπροσδιορισμός της σειράς των μηνυμάτων και η εικονική κίνηση αυξάνει την ανωνυμία στην περίπτωση της κίνησης η οποία είναι ανθεκτική στις καθυστερήσεις, αλλά παραμένει ακατάλληλη για κίνηση η οποία υπόκειται σε αυστηρούς χρονικούς περιορισμούς. Με την ανάπτυξη των τεχνολογιών του Διαδικτύου, υπήρχε μιας σαφής ανάγκη νέων σχεδιαστικών λύσεων για την επίτευξη της ανωνυμίας στην περίπτωση των επικοινωνιών οι οποίες δεν είναι ανθεκτικές στις καθυστερήσεις.
Το Crowds [Reiter] είναι ένα χαμηλής καθυστέρησης δίκτυο σύζευξης για ανώνυμες συνδέσεις Διαδικτύου. Αποτελεί μια προσέγγιση όπου το σύνολο των δυνατών διαδρομών δημιουργείται δυναμικά και κάθε διαδρομή συνιστά μια ακολουθία κόμβων προώθησης. Μια άλλη δυνατότητα αποτελεί η χρησιμοποίηση ενός μοναδικού εξυπηρετητή ανωνυμίας (anonymizing proxy server) [SixFour, Anonymizer]. Σε αυτήν την περίπτωση όλες οι επικοινωνίες μιας οντότητας δρομολογούνται μέσω του συγκεκριμένου εξυπηρετητή ενώ ο παραλήπτης της κίνησης συνδέεται μόνο με τον εξυπηρετητή και όχι με τον πραγματικό αποστολέα.
Τέλος, ένα αξιοσημείωτο παράδειγμα ενός χαμηλής καυθυστέρησης ελεύθερης διαδρομής δικτύου αποτελεί το δίκτυο δρομολόγησης κρόμμυον (onion routing network) [Reed96], το οποίο συντίθεται από ένα σύνολο κόμβων προώθησης με το όνομα κρόμμυον δρομολογητές (onion routers). Το δίκτυο αυτό τρέχει πάνω από την υπάρχουσα υποδομή Διαδικτύου. Η εγκατάσταση της επικοινωνίας στα πλαίσια του συγκεκριμένου δικτύου λαμβάνει χώρα με την διαχείριση και αποστολή μιας πολυ-επίπεδης δομής δεδομένων, με το όνομα κρόμμυον το οποίο περιέχει τα συμμετρικά κλειδιά και τις αναγκαίες πληροφορίες δρομολόγησης. Η σχεδιαστική λύση αυτή εξελίχθηκε στο δίκτυο Tor [Dingledine04] το οποίο εισήγαγε ένα σύνολο βελτιώσεων δημιουργώντας ένα ευέλικτο δίκτυο ανωνυμίας.
Το δίκτυο Tor επιτυγχάνει να διευθετήσει ένα σύνολο ζητημάτων όπως είναι η μυστική προώθηση, η έλλειψη της οποίας ήταν ένα κενό ασφαλείας στην προηγούμενη έκδοση του δικτύου δρομολόγησης κρόμμυον. Το Tor δεν δημιουργεί απευθείας ένα κρόμμυον με όλα τα κλειδιά των κόμβων, αντίθετα διαπραγματεύεται τα συμμετρικά κλειδιά με κάθε επιλεγμένο κόμβο κατασκευάζοντας το κύκλωμα σταδιακά. Μια άλλη βελτίωση του Tor είναι η παροχή διαφορετικών τμημάτων και επιπέδων. Προσπαθεί να προστατεύσει το επίπεδο μεταφοράς επιτρέποντας να χρησιμοποιηθεί από ένα ευρύ σύνολο εφαρμογών, που βρίσκεται πάνω από το συγκεκριμένο επίπεδο, ενώ επίσης επιχειρεί να βελτιώσει τη φιλικότητα προς τον τελικό χρήστη.
Το στοιχείο, το οποίο πρέπει να σημειωθεί είναι το γεγονός ότι το Tor είναι το μόνο χαμηλής καθυστέρησης δίκτυο το οποίο προάγει την πρόσβαση σε κρυμμένες υπηρεσίες [Dingledine06] με την εφαρμογή σημείων ραντεβού (rendezvous points). Τα σημεία αυτά λειτουργούν ως προκαθορισμένα σημεία συνάντησης για τους ανώνυμους παροχείς υπηρεσιών και τους απλούς χρήστες μέσα στο δίκτυο ενισχύοντας σημαντικά την ανωνυμία τους.
Εντούτοις, εξαιτίας του περιορισμού που παρουσιάζει το Tor να υποστηρίξει υψηλής καθυστέρησης κίνηση εμφανίζει σημαντικές αδυναμίες, ειδικά απέναντι σε ισχυρούς επιτιθέμενους οι οποίοι κατέχουν μεγάλη υπολογιστική δύναμη και οι οποίοι μπορούν να διαπιστώσουν και να συνδέσουν δυο οντότητες οι οποίες επικοινώνησαν μεταξύ

τους εκτελώντας χρονικούς συσχετισμούς. Αυτό είναι εφικτό είτε με την παρατήρηση και την διαχείριση (π.χ. δημιουργία, τροποποίηση, διαγραφή, ή αναμετάδοση) της ανταλλασσόμενης κίνησης [Wright04, Murdoch05], είτε με κατοχή και λειτουργία ενός τμήματος του δικτύου [Øverlier06].
Λαμβάνοντας, λοιπόν, υπόψη τις αδυναμίες των χαμηλής καθυστέρησης δικτύων, όπως είναι το δίκτυο Tor, να διευθετήσουν πλήρως την ανωνυμία σύνδεσης στην περίπτωση των η/κ-Υπηρεσιών Ιστού και την έλλειψη μιας υψηλής καθυστέρησης λύσης για το σκοπό αυτό, στο κεφάλαιο που ακολουθεί γίνεται η παρουσίαση ενός Ολιστικού Μοντέλο Ανωνυμίας.

7.3 Ολιστικό Μοντέλο Ανωνυμίας για Υπηρεσίες Ιστού

Στο παρόν κεφάλαιο παρουσιάζεται το προτεινόμενο Ολιστικό Μοντέλο παραθέτοντας τις τεχνολογίες πάνω στις οποίες στηρίχθηκε, τους στόχους που επιτυγχάνει καλύψει, τις οντότητες που μετέχουν και περιγράφεται η υιοθετημένη αρχιτεκτονική και οι διαδικασίες που εφαρμόζονται.

7.3.1 Υιοθετημένες Τεχνολογίες και Πρότυπα

Η χρησιμοποίηση τεχνολογιών XML και προτύπων που βασίζονται σε Υπηρεσίες Ιστού παρέχουν την κατάλληλη υποδομή και αποτελούν την βάση για την υλοποίηση του προτεινόμενου μοντέλου. Το Simple Object Access Protocol (SOAP) αποτελεί ένα "ελαφρύ" πρωτόκολλο που επιτρέπει την ανταλλαγή καλώς δομημένων πληροφοριών σε ένα πλήρως αποκεντροποιημένο και διανεμημένο περιβάλλον. Στο συγκεκριμένο περιβάλλον οι διαδικασίες πιστοποίησης και εξουσιοδότησης πραγματοποιούνται με την υιοθέτηση του WS-Trust [Bohren05] το οποίο προσφέρει ένα γενικού σκοπού πρωτόκολλο ανταλλαγής διαπιστευτηρίων παρέχοντας επίσης την δυνατότητα έκδοσης, ανανέωσης και επικύρωσης των διαπιστευτηρίων αυτών.
Το Web Services Security [Nadalin04] σε συνδυασμό με την χρήση "*τυφλών*" πιστοποιητικών (blind certificates) [Mao96] επιτρέπουν την εφαρμογή των μηχανισμών ασφάλειας που απαιτούνται για την ολοκλήρωση μιας αξιόπιστη συναλλαγής διασφαλίζοντας ότι η ταυτότητα των συμμετοχόντων δεν θα αποκαλυφθεί. Το Web Services Description Language (WSDL) και το WS-Policy περιγράφουν αντίστοιχα το σύνολο των λειτουργικών και μη χαρακτηριστικών μιας η/κ-Υπηρεσίας Ιστού, ακολουθώντας μια καινοτόμο προσέγγιση. Επιπλέον, η υιοθέτηση καταλόγων τα οποία βασίζονται στο Universal Description, Discovery and Integration Protocol (UDDI) ενισχύει την αίσθηση της διαλειτουργικότητας καθιστώντας τις ανωτέρω περιγραφές διαθέσιμες και προσβάσιμες από τους ενδιαφερόμενους.

Χαρακτηριστικά	**Περιγραφή**
Προορισμός	Διεύθυνση προοριζόμενου παραλήπτη.
Σημείο Πηγής	Πηγή (Αρχικός Αποστολέας) του μηνύματος.
Σημείο Απόκρισης	Σημείο αναφοράς που προσδιορίζει τον παραλήπτη της απάντησης.
Σημείο Σφάλματος	Σημείο αναφοράς που προσδιορίζει τον παραλήπτη του σφάλματος.
Ενέργεια	Μοναδικό προσδιοριστικό (URI) που καθορίζει τη σημασιολογία του μηνύματος.
Κωδικός Μηνύματος	Υποδεικνύει τη σχέση των μηνυμάτων.

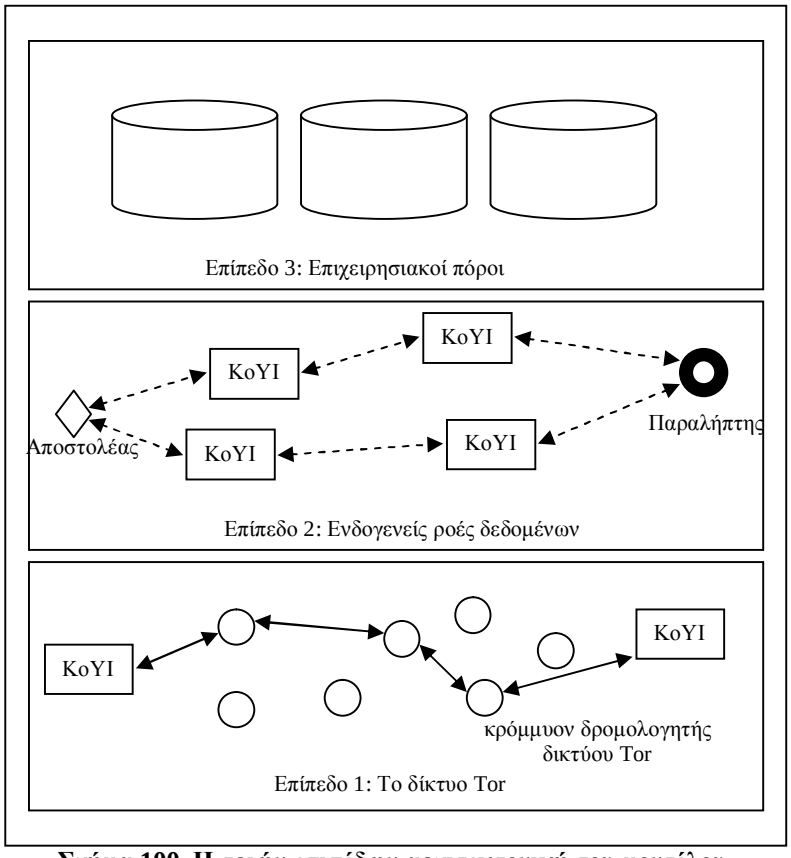
Πίνακας 18. Χαρακτηριστικά Διευθυνσιοδότησης Μηνύματος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Ιστορικά, η μεταβίβαση ενός μηνύματος SOAP στον παραλήπτη ήταν ένα ζήτημα που αποτελούσε αρμοδιότητα του επιπέδου μεταφοράς. Τα πρότυπα Υπηρεσιών Ιστού μέσω του WS-Addressing [WebAddressing06] καθορίζουν ένα πρότυπο τρόπο δρομολόγησης των συγκεκριμένων μηνυμάτων πάνω από πολλαπλά επίπεδα ενώ παράλληλα επιτρέπουν την καθοδήγηση της απάντησης προς μια τρίτη οντότητα. Αυτό επιτυγχάνεται μέσω του καθορισμού συγκεκριμένων πληροφοριών διευθυνσιοδότησης οι οποίες είναι ανεξάρτητες του επιπέδου μεταφοράς. Το WS-Addressing ουσιαστικά αποτελείται από τα ακόλουθα τμήματα:

- *Αναφορά τελικού σημείου Υπηρεσίας Ιστού* (Web service Endpoint reference): παρέχει τις απαιτούμενες πληροφορίες για τον προσδιορισμό/αναφορά ενός τελικού σημείου μιας Υπηρεσίας Ιστού.
- *Χαρακτηριστικά Διευθυνσιοδότησης Μηνύματος* (Message Addressing Properties): καθορίζει ένα σύνολο πρόσθετων προτυποποιημένων επικεφαλίδων του SOAP μηνύματος, όπως αυτές παραθέτονται στον Πίνακας 18, οι οποίες χρησιμοποιούνται για την μεταφορά πληροφοριών σχετικών με ένα μήνυμα.

Το σύνολο των ανωτέρω προτύπων και τεχνολογιών αποτελούν την βάση του μοντέλου επιτρέποντας την κάλυψη του συνόλου των απαιτήσεων που τίθενται από αυτό.



Σχήμα 100. Η τριών επιπέδων αρχιτεκτονική του μοντέλου.

7.3.2 Αρχιτεκτονική και Σχεδιαστικοί Στόχοι Ολιστικού Μοντέλου Ανωνυμίας

Όπως απεικονίζεται στο Σχήμα 100 το προτεινόμενο μοντέλο βασίζεται σε μια τριών επιπέδων διανεμημένη αρχιτεκτονική η οποία επιτρέπει την εφαρμογή των απαιτούμενων μηχανισμών ιδιωτικότητας που είναι απαραίτητοι για τον ασφαλή και έμπιστο διαμοιρασμό επιχειρησιακών πληροφοριών. Ο ρόλος και οι αρμοδιότητες κάθε επιπέδου είναι απόλυτα διακριτές και συνοψίζονται στα ακόλουθα.

- *Επίπεδο 3*: αποτελεί το ανώτερο επίπεδο της αρχιτεκτονικής το οποίο περιλαμβάνει το σύνολο των επιχειρησιακών πόρων που απαιτούνται για την παραγωγή των πληροφοριών οι οποίες ανταλλάσσονται μέσω των κατώτερων επιπέδων. Σε αυτούς συμπεριλαμβάνονται όλοι οι επιχειρησιακοί πόροι των οντοτήτων που διαδραματίζουν πρωταρχικό ή ακόμα και συμπληρωματικό επιχειρησιακό ρόλο στην εκτέλεση των διαδικασιών.
- *Επίπεδο 2*: φιλοξενεί μια σειρά ενδογενών ροών δεδομένων οι οποίες επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ των διαφορετικών επιχειρησιακών εταίρων που βρίσκονται σε διαφορετικές διαχειριστικές περιοχές. Η ανταλλαγή των πληροφοριών αυτών πραγματοποιείται μέσω ενός συνόλου βοηθητικών Κόμβων Υπηρεσιών Ιστού (KoYI).

  Οι κόμβοι αυτοί λειτουργούν ως κόμβοι αποθήκευσης-και-προώθησης (αναμετάδοσης) των ανταλλασσόμενων πληροφοριών και πιο συγκεκριμένα των μηνυμάτων που περιέχουν τις πληροφορίες αυτές. Αυτό επιτυγχάνεται με υιοθέτηση κατάλληλων στρατηγικών μαζικής αποστολής (batching strategy) [Serjantov02], με την εισαγωγή μιας τυχαίας καθυστέρησης στα μηνύματα που αναμεταδίδονται. Βασική επιδίωξη αποτελεί η απόκρυψη των δικτυακών πληροφοριών των εμπλεκόμενων οντοτήτων εμποδίζοντας παράλληλα έναν επιτιθέμενο από το να συσχετίσει τα ανταλλασσόμενα μηνύματα συνδέοντας τον αρχικό αποστολέα με τον τελικό παραλήπτη των μηνυμάτων.

  Στις παραγράφους που ακολουθούν περιγράφονται εκτενώς οι απαιτούμενοι KoYI αλλά και οι διαδικασίες οι οποίες εκτελούνται.
- *Επίπεδο 1*: αποτελεί το χαμηλότερο επίπεδο της αρχιτεκτονικής το οποίο έχει ενσωματωμένο το δίκτυο ανωνυμίας Tor. Μέσα του επιπέδου αυτού και πιο συγκεκριμένα μέσω του δικτύου Tor μεταφέρονται τα μηνύματα τα οποία ανταλλάσσονται μεταξύ των KoYI που έχουν οριστεί στο επίπεδο 2. Με τον τρόπο αυτό επιτυγχάνεται μεγαλύτερος βαθμός ανωνυμίας επιτρέποντας την απόκρυψη της σχέσης μεταξύ των χρησιμοποιούμενων KoYI.

Το προτεινόμενο Ολιστικό Μοντέλο Ανωνυμίας που περιγράφηκε παραπάνω αποτελεί στην πραγματικότητα μια υψηλής καθυστέρησης λύση για Υπηρεσίες Ιστού οι οποίες είναι ιδιαίτερα ανθεκτικές σε χρονικούς περιορισμούς και οι οποίες βασίζονται κατά κύριο λόγο στη χρήση ασύγχρονης επικοινωνίας. Οι βασικοί σχεδιαστικοί στόχοι του μοντέλου είναι οι ακόλουθοι:

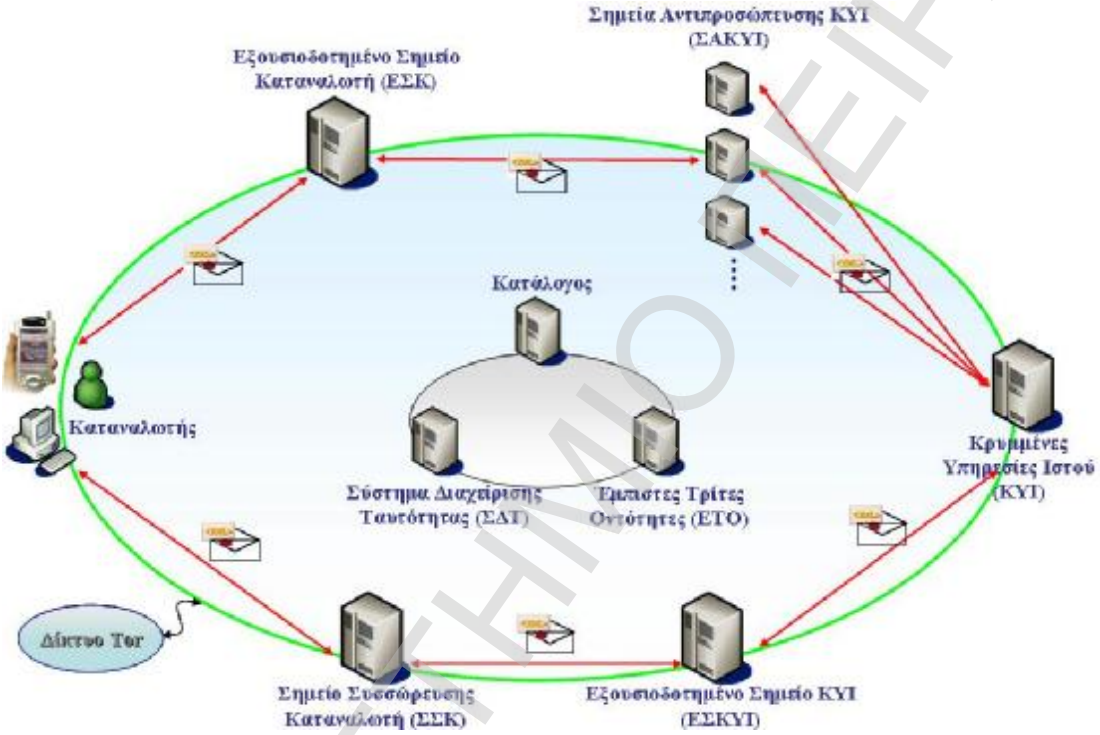
- **ü** η απόκρυψη της δικτυακής θέσης των εμπλεκόμενων οντοτήτων, τόσο του αρχικοποιητή της επικοινωνίας που επιθυμεί πρόσβαση σε μια YI όσο και της ίδιας της YI μέσω της παροχής κρυμμένων Υπηρεσιών Ιστού,
- **ü** η παροχή υψηλής αντίστασης απέναντι σε επιτιθέμενους οι οποίοι παρατηρούν το δίκτυο και ανιχνεύουν την κίνηση.

Οι στόχοι αυτοί επιτυγχάνονται με την χρήση δύο επιπέδων ανωνυμίας:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

- *Ανωνυμία σε Επίπεδο Μεταφοράς*: μέσω της χρήσης του δικτύου Tor το οποίο συγκαλύπτει τη σχέση επικοινωνίας μεταξύ των εμπλεκόμενων οντοτήτων αποκρύπτοντας τις δικτυακές τους πληροφορίες.
- *Ανωνυμία σε Επίπεδο Εφαρμογής*: μέσω της υιοθέτησης ευρέως χρησιμοποιούμενων XML τεχνολογιών για την παροχή κρυμμένων η/κ-Υπηρεσιών Ιστού, καθώς επίσης και την καθυστέρηση-και-αναμετάδοση των μηνυμάτων αποτρέποντας την εφαρμογή χρονικών συσχετισμών.

Τα ανωτέρω επίπεδα ανωνυμίας λειτουργούν συμπληρωματικά το ένα προς το άλλο προσφέροντας μια ολοκληρωμένη υψηλής καθυστέρησης λύση.



Σχήμα 101: Ολιστικό Μοντέλο Ανωνυμίας για Υπηρεσίες Ιστού

7.3.3 Εμπλεκόμενες Οντότητες

Το προτεινόμενο μοντέλο, όπως αυτό απεικονίζεται στο Σχήμα 101, περιλαμβάνει το σύνολο των κεντρικών οντοτήτων οι οποίες παίρνουν μέρος σε μια συνήθη συναλλαγή με μια η/κ-Υπηρεσία Ιστού. Οι οντότητες αυτές είναι οι ακόλουθες:

Κατάλογος: Ένα δημόσιο ευρετήριο όπου κοινοποιούνται οι περιγραφές (WSDL έγγραφα και Πολιτικές Ιδιωτικότητας) των προσφερόμενων Υπηρεσιών Ιστού καθιστώντας τες διαθέσιμες και προσβάσιμες από τις ενδιαφερόμενες οντότητες.
Σύστημα Διαχείρισης Ταυτότητας (ΣΔΤ) [Papastergiou07b]: Μια έμπιστη οντότητα η οποία, όπως αναφέρεται στο Κεφάλαιο 5.4.3, έχει την ευθύνη της διαμορφώσης μιας σχέσης εμπιστοσύνης μεταξύ των Καταναλωτών και των Παρόχων Υπηρεσιών. Αυτό επιτυγχάνεται με την διαχείριση των μερικών ταυτοτήτων και των προτιμήσεων των καταναλωτών και την έκδοση, διανομή και επικύρωση εμπιστευμένων από τους παρόχους υπηρεσιών διαπιστευτηρίων διευκολύνοντας την πρόσβαση στις παρεχόμενες Υπηρεσίες Ιστού. Βασικός στόχος είναι η διευθέτηση της ανωνυμίας σε

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

επίπεδο δεδομένων υιοθετώντας διαδικασίες όπως αυτές παρουσιάστηκαν στο Κεφάλαιο 5.4.3.

Έμπιστες Τρίτες Οντότητες (ΕΤΟ): Οι απαιτούμενες ΕΤΟ είναι μια Αρχή Πιστοποίησης (Certificate Authority, CA) και μια Αρχή Εγγραφών (Registration Authority, RA) η οποία προσφέρει τις απαιτούμενες υπηρεσίες ΥΔΚ (εγγραφής, πιστοποίησης και ανάκλησης) [Adams99], καθώς επίσης και μια Αρχή Έκδοσης Χρονοσφραγίδων (Time Stamping Authority, TSA) η οποία παρέχει υπηρεσίες χρονοσφράγισης.

Κρυμμένες Υπηρεσίες Ιστού (ΚΥΙ): Ένας πάροχος υπηρεσιών ο οποίος προσφέρει η/κ-Υπηρεσίες Ιστού όπως είναι η η/κ-Παραγγελιοδοσία [Polemi06d] επιτρέποντας στους καταναλωτές να αποκτούν πρόσβαση στις υπηρεσίες του χωρίς όμως η ταυτότητά του να αποκαλύπτεται.

Καταναλωτής: Η οντότητα η οποία αποκτά πρόσβαση σε μια ΚΥΙ χωρίς η ταυτότητά της να αποκαλύπτεται.

Το προτεινόμενο μοντέλο προκειμένου να προστατεύσει τη διαδρομή μεταξύ της ΚΥΙ και του Καταναλωτή, εισάγει ένα σύνολο από Κόμβους Υπηρεσιών Ιστού (ΚοΥΙ) (βλ. § 7.3.2). Οι κόμβοι αυτοί έχουν ως στόχο να αποτρέψουν την αποκάλυψη των δικτυακών πληροφοριών του Καταναλωτή και της ΚΥΙ και να εμποδίσουν έναν επιτιθέμενο από το να συσχετίσει τα ανταλλασσόμενα SOAP μηνύματα με τον αρχικό αποστολέα και τον τελικό παραλήπτη των μηνυμάτων.

Τόσο ο Καταναλωτής όσο και η ΚΥΙ, λοιπόν ορίζουν δικά τους σύνολα ΚοΥΙ. Πιο συγκεκριμένα, ο Καταναλωτής ορίζει τα ακόλουθα δικτυακά σημεία:

- *Το Εξουσιοδοτημένο Σημείο Καταναλωτή (ΕΣΚ)* το οποίο είναι ένας ΚοΥΙ, ο οποίος λειτουργεί για λογαριασμό του Καταναλωτή με σκοπό να αναμεταδίδει τα μηνύματα SOAP που αποστέλλονται από αυτόν.
- Το *Σημείο Συσσώρευσης Καταναλωτή (ΣΣΚ)* το οποίο είναι ένας ΚοΥΙ με σημαντικές υπολογιστικές και αποθηκευτικές δυνατότητες ο οποίος λαμβάνει και αποθηκεύει τα μηνύματα SOAP τα οποία προορίζονται για τον Καταναλωτή.

Αντίστοιχα, η ΚΥΙ θα πρέπει να επιλέξει τα ακόλουθα σημεία:

- Τα *Σημεία Αντιπροσώπευσης ΚΥΙ (ΣΑΚΥΙ)* τα οποία λειτουργούν ως αποδέκτες των μηνυμάτων SOAP τα οποία προορίζονται για την ΚΥΙ, ενεργώντας ως τα κοινοποιημένα τελικά σημεία της ΚΥΙ. Πρόκειται για ΚοΥΙ οι οποίοι λαμβάνουν τα μηνύματα και τα αναμεταδίδουν στην ΚΥΙ.
- *Το Εξουσιοδοτημένο Σημείο ΚΥΙ (ΕΣΚΥΙ)* το οποίο προσφέρει αντίστοιχη λειτουργία με το ΕΣΚ ενεργώντας ως ένας ΚοΥΙ στην προκειμένη περίπτωση για λογαριασμό της ΚΥΙ.

Ενέργειες	*Αναμετάδοση*	*Καθυστέρηση*	*Αποστολή*	*Επεξεργασία*	*Αποθήκευση*
Καταναλωτής			**ü**	**ü**	
ΕΣΚ	**ü**	**ü**			
ΣΑΚΥΙ	**ü**	**ü**			
ΚΥΙ			**ü**	**ü**	
ΕΣΚΥΙ	**ü**	**ü**			
ΣΣΚ	**ü**	**ü**			**ü**

Πίνακας 19. Ενέργειες Εμπλεκόμενων Οντοτήτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

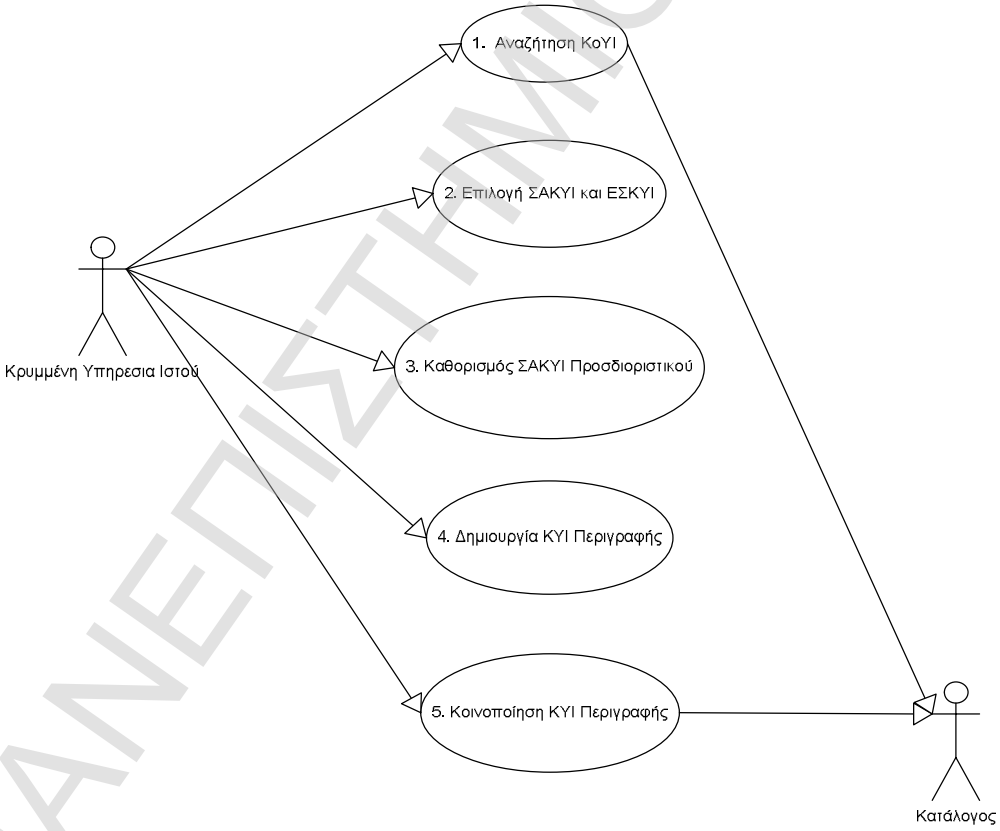
Το σημείο το οποίο πρέπει να σημειωθεί είναι ότι όλες οι ανωτέρω οντότητες θα πρέπει να είναι μέρος του Tor δικτύου. Ο Πίνακας 19 παρουσιάζει τις ενέργειες που εκτελεί καθεμία από τις οντότητες αυτές όσον αφορά τη διαχείριση των ανταλλασσόμενων SOAP μηνυμάτων.

7.3.4 Διαδικασίες Ανωνυμίας

Στο παρόν κεφάλαιο θα παρουσιαστούν οι διαδικασίες οι οποίες πρέπει να ακολουθηθούν για την εκτέλεση μιας συναλλαγής μέσω του προτεινόμενου μοντέλου. Οι διαδικασίες αυτές διακρίνονται στις ακόλουθες φάσεις:

Κοινοποίηση KoYI
Όλες οι οντότητες οι οποίες μπορούν να λειτουργήσουν ως KoYI κοινοποιούν την δυνατότητά τους αυτή στον Κατάλογο.

Λήψη των απαιτούμενων Πιστοποιητικών
Όλες οι οντότητες που μετέχουν στην διαδικασία θα πρέπει να επικοινωνήσουν με μια Έμπιστη Τρίτη Οντότητα και πιο συγκεκριμένα με την Αρχή Πιστοποίησης και την Αρχή Εγγραφής από τις οποίες αποτελείται κάνοντας χρήση των υπηρεσιών εγγραφής και πιστοποίησης που αυτές προσφέρουν προκειμένου να ανακτήσουν τα απαιτούμενα πιστοποιητικά (*τυφλά πιστοποιητικά*).

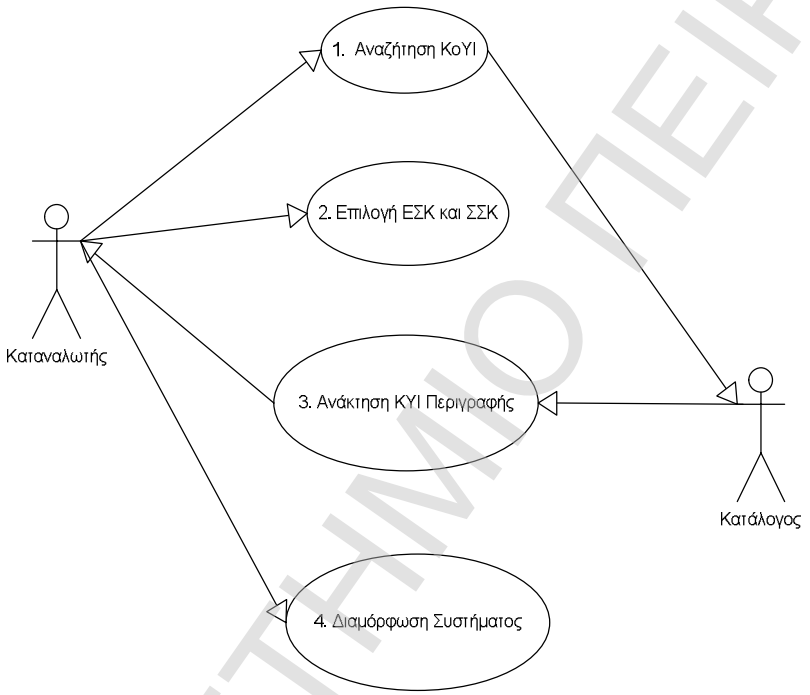


Σχήμα 102: Κοινοποίηση ΚΥΙ

Κοινοποίηση ΚΥΙ
Οι ενέργειες οι οποίες πρέπει να εκτελεστούν από την ΚΥΙ αποτυπώνονται στο Σχήμα 102 και είναι οι εξής:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

1. Αναζήτηση στον Κατάλογο για την ανάκτηση των οντοτήτων που μπορούν να ενεργήσουν ως ΚοΥΙ.
2. Επιλογή των χρησιμοποιούμενων ΣΑΚΥΙ και ΕΣΚΥΙ.
3. Σύνδεση κάθε ΣΑΚΥΙ με ένα μοναδικό προσδιοριστικό το οποίο συνδέει το ΣΑΚΥΙ με την ΚΥΙ.
4. Δημιουργία τη περιγραφής της ΚΥΙ (του εγγράφου WSDL και των Πολιτικών Ιδιωτικότητας), υποδεικνύοντας τα ΣΑΚΥΙ ως τα τελικά σημεία της ΚΥΙ και δηλώνοντας το προσδιοριστικό που έχει αποδοθεί στε κάθε ΣΑΚΥΙ.
5. Κοινοποίηση της περιγραφής της ΚΥΙ στον Κατάλογο.



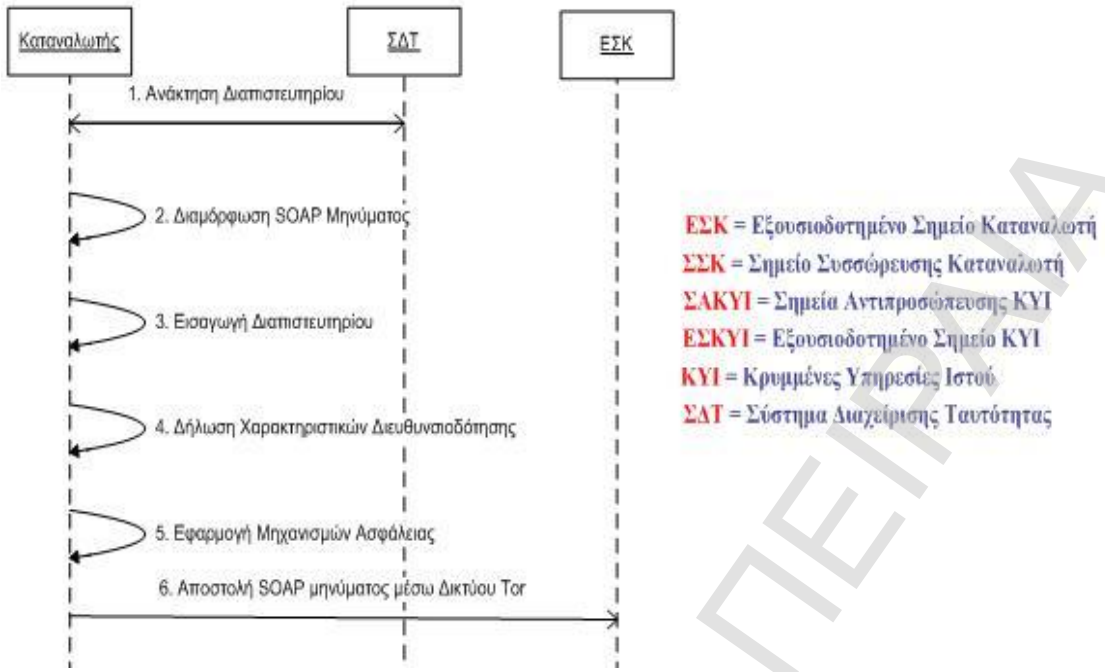
Σχήμα 103: Διαμόρφωση Καταναλωτή

Διαμόρφωση Καταναλωτή
Οι ενέργειες οι οποίες πρέπει να εκτελεστούν από τον Καταναλωτή απεικονίζονται στο Σχήμα 103 και είναι οι ακόλουθες:

1. Αναζήτηση στον Κατάλογο για την ανάκτηση των οντοτήτων που μορούν να ενεργήσουν ως ΚοΥΙ.
2. Επιλογή των χρησιμοποιούμενων ΕΣΚ και ΣΣΚ.
3. Ανάκτηση της κοινοποιημένης περιγραφής της ΚΥΙ.
4. Διαμόρφωση του συστήματος του για την ανταλλαγή των απαιτούμενων μηνυμάτων.

Η ολοκλήρωση των προαναφερθέντων φάσεων επιτρέπει την αρχικοποίηση της διαδικασίας πρόσβασης μιας ΚΥΙ από έναν καταναλωτή μέσου του προτεινόμενου μοντέλου. Τα απαιτούμενα βήματα τα οποία πρέπει να εκτελεστούν είναι τα ακόλουθα:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ



Σχήμα 104. Δημιουργία και Αποστολή SOAP μηνύματος στο ΕΣΚ

Βήμα 1: *Δημιουργία και Αποστολή μηνύματος SOAP στο ΕΣΚ* (Σχήμα 104: Ενέργειες 1-6)
Ο Καταναλωτής επικοινωνεί με το ΣΔΤ και λαμβάνει ένα διαπιστευτήριο (SAML Assertion). Στη συνέχεια, δημιουργεί ένα μήνυμα SOAP στις επικεφαλίδες του οποίου εισάγει το διαπιστευτήριο και δηλώνει τα χαρακτηριστικά διευθυνσιοδότησης του Μηνύματος που παρουσιάζονται στον Πίνακας 20. Τέλος, εφαρμόζει στο μήνυμα τους μηχανισμούς ασφάλειας Υπηρεσιών Ιστού (WS-Security features) χρησιμοποιώντας το τυφλό πιστοποιητικό της ΚΥΙ και το αποστέλλει στο ΕΣΚ μέσω του Tor δικτύου.

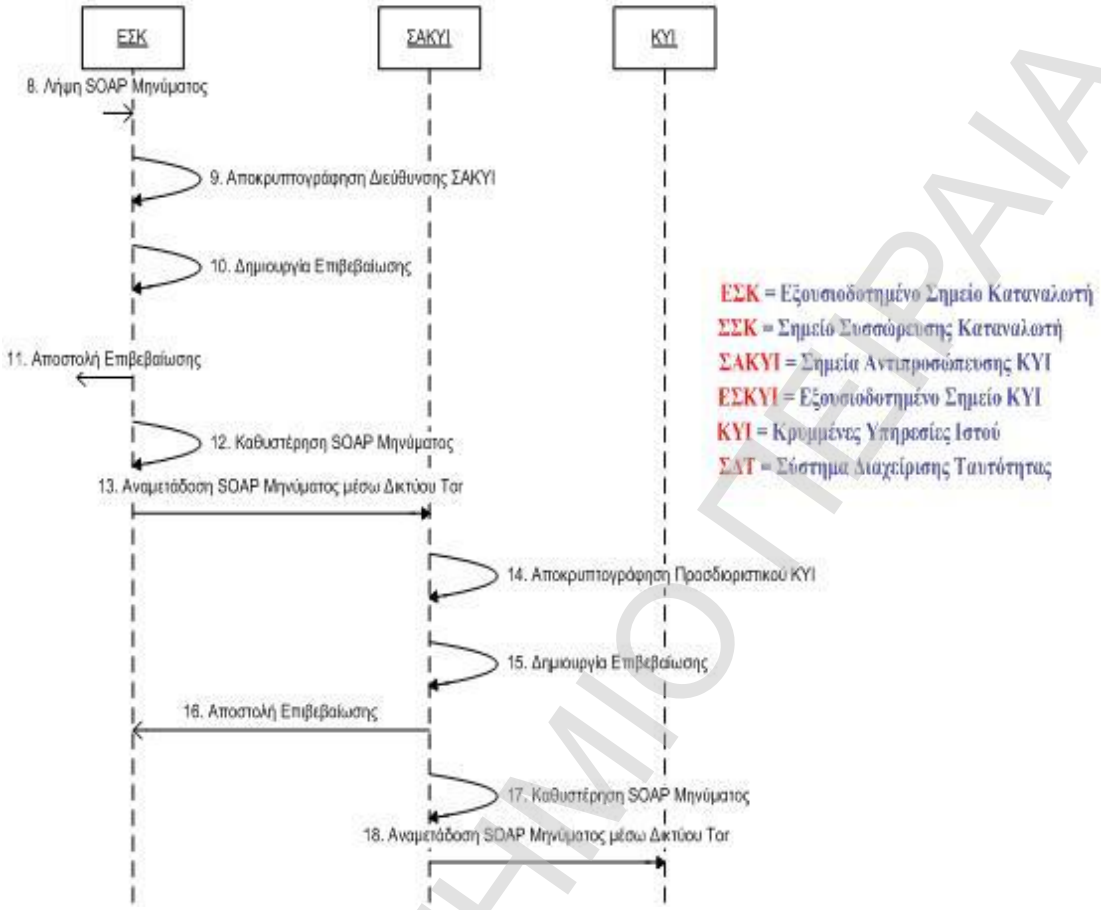
Χαρακτηριστικά	Τιμή
Προορισμός	Η διεύθυνση του ΣΑΚΥΙ κρυπτογραφημένη με το δημόσιο κλειδί του ΕΣΚ.
Σημείο Πηγής	http://www.w3.org/2005/08/addressing/anonymous.
Σημείο Απόκρισης	Η διεύθυνση του ΣΣΚ κρυπτογραφημένη με το δημόσιο κλειδί του ΚΥΙ.
Σημείο Σφάλματος	Η διεύθυνση του ΣΣΚ κρυπτογραφημένη με το δημόσιο κλειδί του ΚΥΙ.
Ενέργεια	Το μοναδικό προσδιοριστικό (URI) που συνδέει το ΣΑΚΥΙ με την ΚΥΙ, κρυπτογραφημένο με το δημόσιο κλειδί του ΣΑΚΥΙ.
Κωδικός Μηνύματος	Ο κωδικός του μηνύματος που χρησιμοποιείται για να προσδιορίσει μοναδικά ένα μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί του ΚΥΙ.

Πίνακας 20. Χαρακτηριστικά Διευθυνσιοδότησης Μηνύματος

Με την εκτέλεση του συγκεκριμένου βήματος επιτυγχάνεται αρχικά ο προσδιορισμός των «μονοπατιών» μέσω των οποίων τόσο το αρχικό μήνυμα SOAP όσο και η αντίστοιχη απάντηση θα φτάσουν στον τελικό προορισμό τους. Αυτό πραγματοποιείται με τον καθορισμό των απαιτούμενων τιμών των χαρακτηριστικών διευθυνσιοδότησης. Στην συνέχεια μέσω της προώθησης του μηνύματος SOAP στον

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΕΣΚ, της χρήσης “τυφλών” πιστοποιητικών και του δικτύου Tor επιτρέπεται η απόκρυψη της δικτυακής ταυτότητας του χρήστη και η επίτευξη της ανωνυμίας του.



Σχήμα 105: Λήψη SOAP μηνύματος από την ΚΥΙ

Βήμα 2: *Προώθηση του μηνύματος SOAP στο ΣΑΚΥΙ* (Σχήμα 105: Ενέργειες 8-13)
Ο ΕΣΚ λαμβάνει το μήνυμα SOAP, αποκρυπτογραφεί το χαρακτηριστικό Προορισμός από τα Χαρακτηριστικά Διευθυνσιοδότησης Μηνύματος και εξάγει την διεύθυνση προορισμού του μηνύματος (διεύθυνση ΣΑΚΥΙ). Ένα μήνυμα επιβεβαίωσης δημιουργείται και στέλνεται πίσω στον καταναλωτή ενημερώνοντάς τον ότι το μήνυμα του θα προωθηθεί στον προορισμό που έχει δηλώσει. Το κρυπτογραφημένο μήνυμα αποθηκεύεται για ένα ορισμένο χρονικό διάστημα το οποίο εξαρτάται από την στρατηγική μαζικής αποστολής που έχει υιοθετήσει και στην συνέχεια στέλνεται στο ΣΑΚΥΙ μέσω του Tor δικτύου.
Ο ΕΣΚ στον παρόν στάδιο λειτουργώντας ως ένας κόμβος αναμεταδότης επιτρέπει να αποκρύψει την ταυτότητα του αρχικού καταναλωτή, ενώ παράλληλα καθυστερώντας την αποστολή του μηνύματος επιτρέπει την αποφυγή χρονικών συσχετισμών οι οποίοι ενδέχεται να πραγματοποιηθούν από έναν επιτιθέμενο. Η χρήση του δικτύου Tor για την αναμετάδοση επιτυγχάνει επίσης της απόκρυψη της ταυτότητας του από τον ΣΑΚΥΙ στον οποίο το μήνυμα αποστέλλεται.

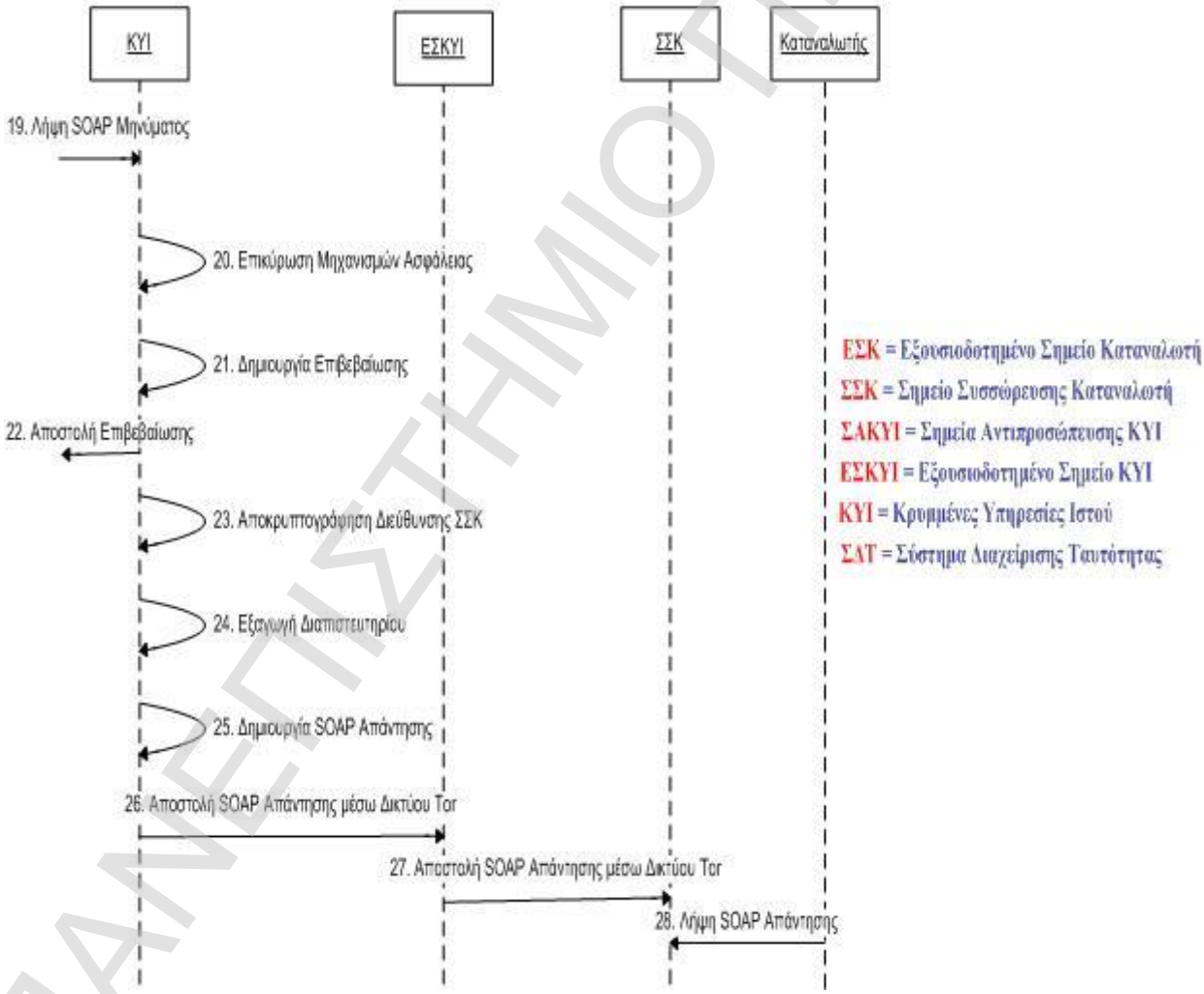
Βήμα 3: *Παραλαβή του μηνύματος SOAP από την ΚΥΙ* (Σχήμα 105: Ενέργειες 14-18)
Ο ΣΑΚΥΙ ακολουθώντας μια παρόμοια διαδικασία με τον ΕΣΚ λαμβάνει το μήνυμα και εξάγει τον τελικό αποδέκτη από το κρυπτογραφημένο προσδιοριστικό του χαρακτηριστικού Ενέργεια που βρίσκεται στα Χαρακτηριστικά Διευθυνσιοδότησης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Μηνύματος. Το προσδιοριστικό έχει επιλεγεί κατά τη διάρκεια της φάσης *Κοινοποίησης ΚΥΙ* στο πλαίσιο της οποίας ένα προσδιοριστικό συνδέει την ΚΥΙ με κάθε ένα ΣΑΚΥΙ. Τέλος, δημιουργείται μια επιβεβαίωση η οποία στέλνεται στο ΕΣΚ, ενώ το μήνυμα SOAP (αφού αποθηκευτεί για ένα ορισμένο χρονικό διάστημα ανάλογα με την υιοθετημένη στρατηγική δέσμης) στέλνεται στην ΚΥΙ μέσω του δικτύου Tor.

Πρέπει να σημειωθεί ότι ο ΣΑΚΥΙ έχει θεωρηθεί από τον καταναλωτή ως ο τελικός αποδέκτης του μηνύματος, επιτυγχάνοντας με αυτόν τον τρόπο την απόκρυψη της δικυακής ταυτότητας της αιτούμενης υπηρεσίας και την προσφορά κρυμμένων ΥΙ. Η διαπίστωση για το πού πρέπει να προωθηθεί το μήνυμα γίνεται μέσω του μοναδικού κρυπτογραφημένου προσδιοριστικού που έχει θέσει στις επικεφαλίδες διευθυνσιοδότησης ο καταναλωτής.

Οι χρονικοί συσχετισμοί κατά την αναμετάδοση και στην προκειμένη περίπτωση αποφεύγονται με την χρήση μια κατάλληλης στρατηγική μαζικής αποστολής από μέρους του ΣΑΚΥΙ.



Σχήμα 106. Επεξεργασία SOAP μηνύματος και Αποστολή Απάντησης στο ΣΣΚ

Βήμα 4: *Επεξεργασία του μηνύματος SOAP από την ΚΥΙ* (Σχήμα 106: Ενέργειες 19-25)

Το μήνυμα SOAP λαμβάνεται από την ΚΥΙ η οποία επαληθεύει τους εφαρμοζόμενους μηχανισμούς ασφάλειας και στη συνέχεια δημιουργεί και στέλνει μια επιβεβαίωση στο ΣΑΚΥΙ. Η ΚΥΙ εξάγει το ενσωματωμένο διαπιστευτήριο που

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

εκδόθηκε από το ΣΔΤ εκτελώντας τις απαιτούμενες διαδικασίες πιστοποίησης και εξουσιοδότησης και επεξεργάζεται την αίτηση.
Στη συνέχεια, η ΚΥΙ δημιουργεί την απάντηση η οποία στέλνεται στην διεύθυνση που είχε δηλωθεί από τον Καταναλωτή στο χαρακτηριστικό Σημείο Απόκρισης που βρίσκεται στα Χαρακτηριστικά Διευθυνσιοδότησης Μηνύματος. Στη συνέχεια, η ΚΥΙ εισάγει το διαπιστευτήριο στις επικεφαλίδες του νέου μηνύματος στο οποίο τελικά εφαρμόζει τους αντίστοιχους μηχανισμούς ασφάλειας χρησιμοποιώντας το τυφλό πιστοποιητικό του καταναλωτή.

Βήμα 5 *Αποστολή του μηνύματος SOAP στον Καταναλωτή* (Σχήμα 106: Ενέργειες 26-28)
Η ΚΥΙ στο παρόν βήμα ξεκινάει την αποστολή της απάντησης στον καταναλωτή. Η διαδικασία η οποία ακολουθείται είναι σε γενικές γραμμές ταυτόσημη με αυτήν που ακολουθήθηκε κατά την αποστολή του αρχικού μηνύματος. Η απάντηση αναμεταδίδεται μέσω του κόμβου ΕΣΚΥΙ και πάνω από το δίκτυο Tor ώστε να επιτευχθεί η απόκρυψη της διαδικτυακής ταυτότητας της ΚΥΙ.
Η ΚΥΙ γνωρίζει ως τελικό αποδέκτη του μηνύματος όχι τον ίδιο τον καταναλωτή αλλό το ΣΣΚ το οποίο έχει οριστεί από αυτόν. Επομένως, μετά τη λήψη της απάντησης από τον ΣΣΚ, ο καταναλωτής λαμβάνει το SOAP μήνυμα από το ΣΣΚ υποδεικνύοντας το διαπιστευτήριο με το οποίο έκανε πρόσβαση στην ΚΥΙ.

Ορατότητα	*Καταναλωτής*	*ΕΣΚ*	*ΣΑΚΥΙ*	*ΚΥΙ*	*ΕΣΚΥΙ*	*ΣΣΚ*
Καταναλωτής		**ü**	**ü**			**ü**
ΕΣΚ			**ü**			
ΣΑΚΥΙ				**ü**		
ΚΥΙ			**ü**		**ü**	**ü**
ΕΣΚΥΙ						**ü**
ΣΣΚ	**ü**					

Πίνακας 21. Ορατότητα των Εμπλεκόμενων Οντοτήτων

Ο Πίνακας 21 εμφανίζει την ορατότητα του προτεινόμενου μοντέλου, υποδεικνύοντας τα δικτυακά σημεία τα οποία είναι ορατά από καθεμία από τις εμπλεκόμενες οντότητες.

7.4 Επιθέσεις

Στο κεφάλαιο αυτό θα παρουσιαστούν ορισμένες γνωστές επιθέσεις και θα εξεταστεί ο τρόπος με τον οποίο η προτεινόμενη αρχιτεκτονική τις αντιμετωπίζει. Στην βιβλιογραφία, υπάρχει μια σαφής διάκριση μεταξύ ενός *ενεργού* και ενός *παθητικού* επιτιθέμενου. Ένας ενεργός επιτιθέμενος έχει τη δυνατότητα να τροποποιήσει αυθαίρετα την αρχική κίνηση με την εισαγωγή, καθυστέρηση ή και διαγραφή κάποιων μηνυμάτων. Αντίθετα, ένας παθητικός επιτιθέμενος είναι ικανός να καταγράψει τα απαιτούμενα σημεία επικοινωνίας μόνο μέσω της παρακολούθησης και της συσχέτισης της κίνησης.

7.4.1 Παθητικές Επιθέσεις

Ένα σύνολο από παθητικές επιθέσεις οι οποίες μπορούν να εκτελεστούν είναι οι ακόλουθες:

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Χρονικός συσχετισμός.
Η ύπαρξη μιας στενής σχέσης μεταξύ των εισερχόμενων και των εξερχόμενων μηνυμάτων αποτελεί ένα στοιχείο το οποίο μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Ο επιτιθέμενος αυτός παρατηρώντας κάποια τμήματα της κίνησης στον αποστολέα και στον παραλήπτη έχει σοβαρές πιθανότητες να διαπιστώσει τη μεταξύ τους επικοινωνία.
Ένας τρόπος με τον οποίο η προτεινόμενη αρχιτεκτονική αποτρέπει αυτήν την επίθεση είναι η εισαγωγή μιας τυχαίας καθυστέρησης στην αναμετάδοση κάθε SOAP μηνύματος το οποίο στέλνεται μέσω του μοντέλου αυτού. Πιο συγκεκριμένα κάθε KoYI ο οποίος λαμβάνει ένα μήνυμα SOAP πρωτού το αναμεταδώσει το αποθηκεύει για συγκεκριμένο χρονικό διάστημα. Το χρονικό διάστημα που μεσολαβεί εξαρτάται από την στρατηγική μαζικής αποστολής (batching strategy) μηνυμάτων που έχει υιοθετήσει ο συγκεκριμένος κόμβος. Ένα παράδειγμα τέτοιου είδους στρατηγικής είναι η συλλογή τουλάχιστον n μηνυμάτων προτού προχωρήσει στην αναμετάδοση τους σε δέσμες με τυχαία σειρά.
Ένα πρόσθετο βήμα για την αντιμετώπιση αυτών των επιθέσεων είναι επίσης και η απόκρυψη της σχέσης μεταξύ των KoYI που έχουν επιλεγεί λειτουργώντας οι ίδιοι οι κόμβοι αυτοί και ως κρόμμυων δρομολογητές του δικτύου Tor. Στην περίπτωση αυτή τα μηνύματα SOAP τα οποία μεταδίδονται από τους KoYI συνενώνονται και με την δικτυακή κίνηση η οποία μεταφέρεται μέσω του δικτύου Tor. Με τον τρόπο αυτό δυσχεραίνεται ακόμη περισσότερο το έργο του επιτιθέμενου ο οποίος επιπλέον χρειάζεται να κάνει διάκριση της αρχικής κίνησης που αντιστοιχεί στα SOAP μηνύματα από την κίνηση η οποία απλά διέρχεται από το δίκτυο Tor, αυξάνοντας το κόστος της παρατήρησης.

Ανάλυση ωφέλιμου φορτίου
Η επίθεση αυτή μπορεί να πραγματοποιηθεί με την συλλογή και ανάλυση των SOAP μηνυμάτων τα οποία στέλνονται προς ή από τους KoYI με σκοπό την ανάκτηση χρήσιμων πληροφοριών. Το προτεινόμενο μοντέλο διευθετεί τη συγκεκριμένη επίθεση με την εφαρμογή κατάλληλων μηχανισμών ασφάλειας. Τα ίδια τα SOAP μηνύματα δεν μπορούν να αποκαλύψουν οποιαδήποτε πληροφορία σε κάποιον αναρμόδιο χρήστη εξαιτίας των πολλαπλών επιπέδων κρυπτογράφησης τα οποία χρησιμοποιειούνται, μέσω της χρήσης του προτύπου WS-Security και μηχανισμών κρυπτογράφησης που έχουν υιοθετήσει από το ίδιο το δίκτυο Tor.

Επίθεση διατομής (Intersection attack).
Ένας επιτιθέμενος παρακολουθώντας την κίνηση έχει τη δυνατότητα να καταλήξει σε πολλά σύνολα από διαφορετικούς κόμβους στα οποία έχει την υποψία ότι περιέχονται τόσο ο αποστολέας όσο και ο παραλήπτης της κίνησης. Εφαρμόζοντας την τομή των συνόλων αυτών μπορεί να επιτύχει την απόρριψη ορισμένων από αυτούς τους κόμβους μειώνοντας με αυτόν τον τρόπο τον αριθμό των πιθανών κόμβων.
Ένα μέτρο αντιμετώπισης του συγκεκριμένου κινδύνου είναι η υιοθέτηση μιας κατάλληλης στρατηγικής μαζικής αποστολής μηνυμάτων από τους KoYI. Μια τέτοια λύση επιτρέπει ταυτόχρονα τη μαζική αναμετάδοση ενός συνόλου μηνυμάτων με αποτέλεσμα την αύξηση του συνόλου των πιθανών αποστολέων ενός συγκεκριμένου μηνύματος. Ένα σημαντικό ζήτημα προκύπτει με την υιοθέτηση στρατηγικών μαζικής αποστολής μηνυμάτων σε περιπτώσεις κατά τις οποίες τα μηνύματα SOAP τα οποία λαμβάνονται από έναν KoYI είναι τόσο λίγα ώστε να μην είναι εφικτή η συλλογή του απαιτούμενου αριθμού μηνυμάτων για την αναμετάδοσή τους σε ένα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

εύλογο χρονικό διάστημα. Με αυτόν τον τρόπο ένας KoYI μπορεί να παραμείνει ανενεργός για μεγάλο χρονικό διάστημα με αποτέλεσμα να είναι πιο ευάλωτος στην εφαρμογή χρονικών επιθέσεων.
Ο κίνδυνος αυτός μπορεί να μειωθεί ως έναν βαθμό λαμβάνοντας υπόψη το γεγονός ότι ο KoYI λειτουργεί και ως δρομολογητής του δικτύου Tor έχοντας με αυτόν τον τρόπο τη δυνατότητα να λαμβάνει και να αναμεταδίδει κίνηση σε τυχαίες χρονικές στιγμές.

7.4.2 Ενεργές Επιθέσεις

Ένα σύνολο από ενεργές επιθέσεις οι οποίες μπορούν να εκτελεστούν είναι οι ακόλουθες:

Επίθεση μηνυμάτων αναμετάδοσης.
Ένας επιτιθέμενος έχει τη δυνατότητα να υπερκεράσει τους εφαρμοζόμενους μηχανισμούς ιδιωτικότητας με την καταγραφή και αναμετάδοση του ίδιου μηνύματος. Όπως περιγράφηκε σε προηγούμενες παραγράφους η προτεινόμενη αρχιτεκτονική χρησιμοποιεί το δίκτυο Tor για την μεταφορά των SOAP μηνυμάτων τα οποία ενθυλακώνονται σε μικρότερα κελιά για να αποσταλλούν. Το δίκτυο Tor χρησιμοποιεί το TLS πάνω από το TCP για τη μεταφορά των παραγόμενων κελιών με τη χρήση κλειδιών κρυπτογράφησης τα οποία είναι έγκυρα μόνο για ένα μικρό χρονικό διάστημα. Επομένως, τα κελιά αυτά δεν μπορούν να χρησιμοποιηθούν για αναμετάδοση.
Υπάρχει όμως η περίπτωση ένας KoYI να καταληφθεί από έναν επιτιθέμενο ο οποίος έχει τη δυνατότητα να αναμεταδίδει ολόκληρα τα μηνύματα SOAP. Ένας τρόπος αποφυγής τέτοιου είδους επιθέσεων είναι να κρατιέται κάποιο ίχνος των εισερχομένων μηνυμάτων για ορισμένο χρονικό έστω διάστημα αποτρέποντας την αναμετάδοση ύποπτων μηνυμάτων. Η ανίχνευση αναμεταδόσεων είναι ένα ζήτημα το οποίο έχει μελετηθεί σημαντικά [Denning82]. Βασικές τεχνικές αντιμετώπισης του κινδύνου αυτού είναι η χρήση αύξοντα αριθμού ή ακόμα και χρονοσφραγίδων.

*Επιθέσεις παραγεμίσματος (**Tagging attacks**).*
Ένας επιτιθέμενος ο οποίος ελέγχει έναν κόμβο σε κάποιο σημείο του κυκλώματος μπορεί να αλλοιώσει ένα κελί τροποποιώντας το περιεχόμενό του και ανιχνεύοντάς το σε κάποιο άλλο σημείο του κυκλώματος επιβεβαιώνοντας τη σχέση μεταξύ των δύο κόμβων. Η χρήση του δικτύου Tor αποτρέπει τον κίνδυνο αυτόν με τη χρήση κατάλληλων μηχανισμών επιβεβαίωσης της ακεραιότητας των κελιών που μεταβιβάζονται.

Επιθέσεις Ανάμειξης.
Ένας ενεργός επιτιθέμενος έχει τη δυνατότητα στέλνοντας συγκεκριμένα μηνύματα και καθυστερώντας άλλα να ελέγχει τα μηνύματα τα οποία εισέρχονται σε έναν KoYI. Με αυτόν τον τρόπο ο επιτιθέμενος διαμορφώνει τα μηνύματα τα οποία αναμεταδίδει ο KoYI με τέτοιο τρόπο ώστε το μόνο απροσδιόριστο μήνυμα το οποίο αναμεταδίδεται είναι αυτό το οποίο αρχικά παρατηρεί. Παρατηρώντας λοιπόν την έξοδο που δίνει ο τελευταίος κόμβος του κυκλώματος επικοινωνίας ο οποίος έχει διαμορφωθεί μπορεί να συνδέσει το αρχικό μήνυμα με τον παραλήπτη του. Εφαρμόζοντας την τακτική αυτή σε κάθε KoYI μπορεί να επιτευχθεί η σύνδεση μεταξύ του αποστολέα και του τελικού παραλήπτη του μηνύματος. Η επιλογή μιας τυχαίας στρατηγικής μαζικής αποστολής μηνυμάτων έχει τη δυνατότητα να μειώσει τον κίνδυνο μιας τέτοιου είδους επίθεσης.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Προσωποποίηση κρυμμένης υπηρεσίας
Ένας επιτιθέμενος μπορεί να προσωποποιηθεί ότι αποτελεί την κρυμμένη υπηρεσία επεξεργάζοντας με αυτόν τον τρόπο το μήνυμα που στέλνεται από τον αποστολέα και επιστρέφοντας μια απάντηση. Στο προτεινόμενο μοντέλο ένας επιτιθέμενος ο οποίος ελέγχει έναν ΚοΥΙ όπως ο ΣΑΚΥΙ δεν έχει τη δυνατότητα να εκτελέσει μια τέτοιου είδους επίθεση. Αυτό οφείλεται στο γεγονός ότι το σημείο το οποίο αποτελεί αποδέκτη της απάντησης (ΣΣΚ) βρίσκεται στο χαρακτηριστικό Σημείο Απόκρισης που βρίσκεται στα Χαρακτηριστικά Διευθυνσιοδότησης του αρχικού Μηνύματος και είναι κρυπτογραφημένο με το δημόσιο κλειδί της κρυμμένης υπηρεσίας ιστού, επομένως είναι δύσκολο να ανακτηθεί.

Επίθεση ενδιάμεσου
Μια επίθεση αυτού του είδους μπορεί να εφαρμοστεί με την εξής μορφή, ένας επιτιθέμενος επικοινωνεί ανεξάρτητα με τον καταναλωτή και την ΚΥΙ και αναμεταδίδει μηνύματα SOAP. Στην προκειμένη περίπτωση, ενώ ο επιτιθέμενος ελέγχει όλη τη συναλλαγή τα τελικά σημεία έχουν πεποίθηση ότι επικοινωνούν με ασφάλεια. Στον μοντέλο που περιγράφηκε στις προηγούμενες παραγράφους η επίθεση ενδιαμέσου είναι δύσκολο να επιτευχθεί εξαιτίας του γεγονότος ότι η αρχιτεκτονική παρέχει ισχυρή αυθεντικοποίηση η οποία μπορεί να μετριάσει την επιτυχία μιας τέτοιας επίθεσης. Ένα τροποποιημένο μήνυμα SOAP μπορεί να εντοπιστεί πολύ εύκολα εξαιτίας της προστασίας η οποία προσφέρεται από την εφαρμογή μηχανισμών όπως το WS-security. Επιπλέον, η διεύθυνση του ΣΣΚ βρίσκεται κρυπτογραφημένη στο χαρακτηριστικό Σημείο Απόκρισης που βρίσκεται στα Χαρακτηριστικά Διευθυνσιοδότησης του αρχικού Μηνύματος γεγονός που καθιστά την απόκτηση της εξαιρετικά δύσκολη.

Επίθεση διαθεσιμότητας
Ο μεγάλος κίνδυνος της διαθεσιμότητας βασίζεται στο γεγονός ότι όλες οι πληροφορίες των εμπλεκόμενων κόμβων βρίσκονται διαθέσιμες και προσβάσιμες σε καταλόγους UDDI. Το γεγονός αυτό δίνει τη δυνατότητα σε έναν επιτιθέμενο να λάβει τις πληροφορίες του ΣΑΚΥΙ και να εκτελέσει άμεσες ή έμμεσες επιθέσεις εναντίον του. Άμεσες επιθέσεις στους ΚοΥΙ μπορούν επίσης να πραγματοποιηθούν στέλνοντας έναν μεγάλο αριθμό μηνυμάτων στο ΣΑΚΥΙ μιας ΚΥΙ εξαντλώντας το σύνολο της υπολογιστικής του δύναμης και καθιστώντας τον ανενεργό.

7.4.3 Επιθέσεις στον Κατάλογο UDDI

Η βασική αρμοδιότητα ενός καταλόγου UDDI [Clement02] εστιάζεται στο να παρέχει στους καταναλωτές τις επιχειρησιακές περιγραφές των υπηρεσιών που έχουν κοινοποιηθεί, μαζί με τις τεχνικές πληροφορίες οι οποίες απαιτούνται για να κληθεί μια υπηρεσία. Πλέον, η παροχή κρίσιμων και ευαίσθητων ως προς το περιεχόμενό τους υπηρεσιών εγείρουν ένα σύνολο ζητημάτων που σχετίζονται με το επίπεδο της ασφάλειας που εφαρμόζεται στου καταλόγους αυτούς. Ζητήματα πιστοποίησης είναι ιδιαίτερα κρίσιμα κυρίως σε περιπτώσεις που οι κατάλογοι UDDI διαχειρίζονται από ανεξάρτητες μη έμπιστες πολλές φορές αρχές. Επομένως κάτω από αυτές τις συνθήκες η διασφάλιση της ακεραιότητας και της αξιοπιστίας των κοινοποιημένων πληροφοριών έγγειται σε μεγάλο βαθμό στην αξιοπιστία του ίδιου του καταλόγου. Στην πράξη ένας επιτιθέμενος έχει τη δυνατότητα να κατακλύσει έναν κατάλογο με κατευθυνόμενες εγγραφές προκειμένου να οδηγήσει τους χρήστες στην επιλογή ΚοΥΙ οι οποίοι ελέγχονται από αυτούς. Επιπλέον, ένας επιτιθέμενος εκμεταλλευόμενος τα

κενά ασφαλείας του ίδου του καταλόγου έχει τη δυνατότητα να παραποιήσει και τις υπάρχουσες εγγραφές.
Στη βιβιογραφία έχουν προταθεί διάφορες μεθόδοι με τις οποίες είναι δυνατόν να ενισχυθεί η ασφάλεια των δεδομένων και των υπηρεσιών αντίστοιχα που κοινοποιούνται σε μη έμπιστους καταλόγους UDDI. Για παράδειγμα στη θέση των κοινοποιημένων δεδομένων μπορεί να δημοσιευτούν οι συνόψεις των δεδομένων αυτών με τη χρήση κατάλληλων συναρτήσεων σύνοψης [Carminati05]. Αντίστοιχα, η αναζήτηση των υπηρεσιών μπορεί να γίνει με τη χρήση ερωτημάτων που περιέχουν τη σύνοψη των κριτηρίων εύρεσης. Το γεγονός αυτό μπορεί να εμποδίσει έναν επιτιθέμενο ο οποίος είτε ελέγχει τον κατάλογο είτε όχι από το να εντοπίσει ποιές είναι οι πραγματικές υπηρεσίες οι οποίες προσφέρονται από μια οντότητα.

7.5 Συμπεράσματα – Μελλοντικές Επεκτάσεις

Η ιδιωτικότητα των οντοτήτων οι οποίες μετέχουν σε η/κ-συναλαγές απειλείται σε σημαντικό βαθμό από την παρατήρηση της δικτυακής κίνησης η οποία ανταλλάσσεται μεταξύ τους. Η παρατήρηση αυτή επιτρέπει το συσχετισμό μεταξύ των ανταλλασσόμενων μηνυμάτων και του αποστολέα και του παραλήπτη των μηνυμάτων αυτών, επιφέροντας τον προσδιορισμό των εμπλεκόμενων οντοτήτων και μειώνοντας με αυτόν τον τρόπο την ανωνυμία τους.
Απάντηση στην πρόκληση αυτή αποτελεί η προστασία του διαύλου επικοινωνίας ανάμεσα στα σημεία τα οποία αποτελούν την αρχική πηγή και τον τελικό αποδέκτη της κίνησης με την συγκάλυψη της διαδρομής η οποία ακολουθεί η κίνηση αυτή. Παραδοσιακά, η ικανοποίηση της απαίτησης αυτής είχε αφεθεί στο στρώμα μεταφοράς με την χρήση δικτύων ανωνυμίας, όπως είναι το δίκτυο Tor. Εντούτοις, τα δίκτυα αυτά παρουσιάζουν σημαντικές αδυναμίες καθώς είτε είναι ευάλωτα σε χρονικούς περιορισμούς είτε δεν μπορούν να προσφέρουν ουσιαστική προστασία των δικτυακών πληροφοριών των δύο τελικών σημείων της κίνησης (π.χ. με την παροχή κρυμμένων υπηρεσιών).
Η υιοθέτηση, όμως, τεχνολογιών και προτύπων που βασίζονται στην XML για την ανάπτυξη Υπηρεσιών Ιστού έχει επιτρέψει την εισαγωγή ευέλικτων και επεκτάσιμων μηχανισμών. Οι μηχανισμοί αυτοί επιτρέπουν να ξεπεραστούν ένα σύνολο αδυναμιών των υπαρχόντων δικτύων ανωνυμίας, επιτρέποντας τη δημιουργία ενός Ολιστικού Μοντέλου Ανωνυμίας για Υπηρεσίες Ιστού οι οποίες είναι ιδιαίτερα ανθεκτικές σε χρονικούς περιορισμούς. Το μοντέλο αυτό αποτελεί μια υψηλής καθυστέρησης λύση για Υπηρεσίες Ιστού οι βασικοί στόχοι του οποίου είναι οι ακόλουθοι:

- να αποκρύψει τη δικτυακή θέση των εμπλεκόμενων οντοτήτων, τόσο του αρχικού χρήστη που επιθυμεί πρόσβαση σε μια ΥΙ όσο και της ίδιας της ΥΙ μέσω της παροχής κρυμμένων Υπηρεσιών Ιστού,
- να παρέχει υψηλή αντίσταση απέναντι σε επιτιθέμενους οι οποίοι παρατηρούν το δίκτυο και ανιχνεύουν την κίνηση εκτελώντας χρονικούς συσχετισμούς.

Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που αφορούν το προτεινόμενο μοντέλο ανωνυμίας είναι οι ακόλουθες:

- Η χρησιμοποίηση διαπιστευτηρίων ανωνυμίας τα οποία εκδίδονται από τα Συστήματα Διαχείρισης Ταυτότητας και χρησιμοποιούνται για την πιστοποίηση και την εξουσιοδότηση των χρηστών για την εφαρμογή των απαιτούμενων μηχανισμών ασφάλειας στην περίπτωση των Υπηρεσιών Ιστού. Το προτεινόμενο μοντέλο στην παρούσα φάση για την επίτευξη αξιόπιστων συναλλαγών στα πλαίσια των οποίων θα διασφαλίζεται ότι η ταυτότητα των

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συμμετοχόντων δεν θα αποκαλυφθεί υιοθετεί "τυφλά" πιστοποιητικά η χρήση όμως των οποίων ενδέχεται να οδηγεί σε συνδεσιμότητα των εκτελέσιμων συναλλαγών.

Το γεγονός που πρέπει να σημειωθεί είναι ότι το προτεινόμενο μοντέλο επιτυγχάνει να καλύψει την απαίτηση της ανωνυμίας των οντοτήτων που μετέχουν σε αυτό σε σημαντικό βαθμό επιτρέποντας την προστασία της ιδιωτικότητάς τους.

7.6 Αναφορές

[Haddad08] W. Haddad. (2008). "*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*". Network Working Group, IETF Trust.

[Gabber99] E. Gabber, P. Gibbons, D. Kristol, Y. Matias, A. Mayer. (1999). "*Consistent, yet anonymous, Web access with LPWA*", Communication ACM, vol.42, no.2, pp.42–47, Feb. 1999.

[Tillwick06] H. Tillwick, M. Olivier. (2005). "*Towards a framework for connection anonymity*", Annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries. ACM International Conference Proceeding Series, vol.150, pp113 – 122, 2005.

[Papastergiou08b] Papastergiou S., Valvis G., Polemi D.. (2008). "*A Holistic Anonymity Framework for Web Services*". The 1st International Conference on Pervasive Technologies Related to Assistive Environments (PETRA 2008), July 15-19, 2008- Athens.

[WebAddressing06] Web Services Addressing 1.0 – Core, W3C Recommendation 9 May 2006, http://www.w3.org/TR/ws-addr-core/.

[Dingledine04] R. Dingledine, N. Mathewson, P. Syverson. (2004). "*Tor: The Second-Generation Onion Router*", 13th Usenix Security Symp., Usenix Assoc., 2004, pp. 303–319; http://tor.eff.orgtor-design.pdf.

[Raymond00] J.F. Raymond .(2000). "*Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems*", Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pages 10–29. Springer-Verlag, LNCS 2009, July 2000.

[Chaum81] D. Chaum. (1981). "*Untraceable electronic mail, return addresses, and digital pseudonyms*", in Communications of the ACM v 24 no 2 (Feb 1981).

[Moeller04] U. Moeller et al.. (2004). "*Mixmaster protocol version 2*", Technical report, Network Working Group, 2004, Internet-Draft.

[Danezis03] G. Danezis, R. Dingledine, N. Mathewson. (2003). "*Mixminion: Design of a type III anonymous remailer protocol*", in IEEE Symposium on Security and Privacy, IEEE, Berkeley, CA, 2003.

[Reiter] M.K. Reiter, A.D. Rubin. (1998). "*Crowds: Anonymity for web transactions*", ACM Transactions on Information System Security, April 1998.

[SixFour] The Six/Four System. http://sourceforge.net/projects/sixfour/.

[Anonymizer] Anonymizer, Inc. http://www.anonymizer.com/.

[Reed96] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. (1996). "*Proxies for anonymous routing*", 12th Annual Computer Security Applications Conference, 1996. http://www.onion-router.net/Publications.html.

[Dingledine06] R. Dingledine and N. Mathewson. (2006). "*Tor rendezvous specification*", Technical report, The Free Haven Project, February 2006, http://tor.eff.org/cvs/doc/rend-spec.txt.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

[Wright04] M.K. Wright, M. Adler, B.N. Levine, C. Shields. (2004). "*The predecessor attack: An analysis of a threat to anonymous communications systems*", ACM Trans. Inf. Syst. Secur. 7 (2004) 489–522.
[Murdoch05] S.J. Murdoch, G. Danezis. (2005). "*Low-cost traffic analysis of Tor*", 2005 IEEE Symposium on Security and Privacy, IEEE CS (2005).
[Øverlier06] L. Øverlier, P. Syverson. (2006). "*Locating hidden servers*", 2006 IEEE Symposium on Security and Privacy, IEEE CS.
[Bohren05] J. Bohren. et al.. 2005. "*Web Services Trust Language (WS-Trust)*" February 2005.
[Nadalin04] A. Nadalin. et al. 2004, "*Web Services Security: SOAP Message Security 1.0*", WS-Security 2004, March 2004.
[Mao96] W. Mao. (1996). "*Blind Certification of Public Keys*", HP Labs Technical Reports, HPL-96-71, May 16, 1996.
[Serjantov02] A. Serjantov, R. Dingledine, P. Syverson. (2002). "*From a trickle to a flood: Active attacks on several mix types*", Information Hiding (IH 2002). Springer-Verlag, LNCS, 2002.
[Papastergiou07b] S. Papastergiou, A. Karantjias, D. Polemi. (2007), "*A Federated Privacy-Enhancing Identity Management System (FPE-IMS)*", 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), 3-7 September 2007, Athens.
[Adams99] C. Adams, S. Lloyd, "*Understanding Public-Key Infrastructure – Concepts, Standards and Deployment Considerations*", 1st Edition, Macmillan Technical Publishing, 1999.
[Polemi06d] Polemi, D., Papastergiou, S.. (2006). "*A Secure, Open and Interoperable e-Ordering Service*", 2nd International Conference on Web Information Systems and Technologies, Webist 2006 INSTICC Press (ISBN: 978-972-8865-46-7), p57-62 (2006), Setubal, Portugal.
[Denning82] D.E.R. Denning. (1982). "*Cryptography and Data Security*", Addison Wesley, 1982.
[Clement02] L. Clement, A. Hately, C. Von Riegen, T. Rogers. (2002). "*Universal description, discovery and integration (UDDI)*", Version 3.0 (UDDI Spec Technical Committee specification). http://uddi.org/pubs/uddi-v3.00-published-20020719.htm.
[Carminati05] B. Carminati, E. Ferrari, P.C.K. Hung. (2005). "*Exploring Privacy Issues in Web Services Discovery Agencies*", IEEE Security & Privacy Magazine. 3(5):14-21, 2005.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

8 Συμπεράσματα – Μελλοντικές Κατευθύνσεις

Η παρούσα διατριβή κινήθηκε σε δυο παράλληλους αλλά αλληλένδετους άξονες μελετώντας και επισημαίνοντας σε πρώτη φάση προβλήματα τα οποία αντιμετωπίζουν οι υπηρεσίες οι οποίες βασίζονται σε τεχνολογίες της XML και σε πρότυπα των Υπηρεσιών Ιστού και προχωρώντας στη συνέχεια στην πρόταση συγκεκριμένων λύσεων για την αντιμετώπιση τους. Ως εξεταζόμενες υπηρεσίες τέθηκαν υπηρεσίες οι οποίες λειτουργούν είτε ως αυτόνομες κινητές ή ηλεκτρονικές εφαρμογές είτε ενσωματωμένες σε μια Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες (ΑΠΥ).

Στα πλαίσια του πρώτου άξονα, η διαλειτουργικότητα των Υπηρεσιών Ιστού (ΥΙ) τέθηκε στο επίκεντρο του ενδιαφέροντος διαπιστώνοντας τις περιορισμένες δυνατότητες αλληλεπίδρασης των υπηρεσιών αυτών παρά το γεγονός ότι χρησιμοποιούν κοινές τεχνολογίες και μελετώντας μεθόδους οι οποίες μπορούν να τις εγγυηθούν. Για το λόγο αυτό εξετάστηκαν μεθοδολογίες διαλειτουργικότητας και συμμόρφωσης οι οποίες έχουν προταθεί και εφαρμόζονται σε ένα ευρύ σύνολο συστημάτων και προδιαγραφών τόσο στο τομέα των τηλεπικοινωνιών όσο και των πληροφοριακών συστημάτων και αρχιτεκτονικών με βασική επιδίωξη την αποτύπωση των αδυναμιών και μειονεκτημάτων τους. Διαπιστώθηκε μια αδυναμία ολιστικής προσέγγισης του τρόπου με τον οποίο δύο ή περισσότερες Υπηρεσίες Ιστού μπορούν ελεχθούν ως προς τη δυνατότητα επικοινωνίας τους

Η διατριβή στον πρώτο άξονα λύνει το πρόβλημα αυτό προδιαγράφοντας μια πρωτότυπη συστηματική και δομημένη μεθοδολογία ελέγχου Διαλειτουργικότητας και Συμμόρφωσης Υπηρεσιών Ιστού (ΔΣΥΙ). Ο κύριος στόχος ο οποίος τέθηκε ήταν οι αρχές σχεδιασμού που θα προταθούν να μπορούν να είναι εφαρμόσιμες ανεξαρτήτως δομής, φύσης και υποκείμενης πολυπλοκότητας των εξεταζόμενων Υπηρεσιών Ιστού. Η ορθότητα και εφαρμοσιμότητα της προτεινόμενης μεθοδολογίας ελέγχου διαπιστώθηκε με την εφαρμογή της για τον έλεγχο της επικοινωνίας δύο υπαρχόντων και πλήρως λειτουργικών Υπηρεσιών Ιστού για ηλεκτρονική τιμολόγηση, της αυτόνομης υπηρεσίας ηλεκτρονικής τιμολόγησης SELIS και της SWEB υπηρεσίας ηλεκτρονικής και κινητής τιμολόγησης.

Οι μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις οι οποίες επισημάνθηκαν στα πλαίσια του πρώτου άξονα είναι οι ακόλουθες:

- Η επέκταση της προτεινόμενης μεθοδολογίας με την ενσωμάτωση νέων τύπων ελέγχων όπως είναι οι έλεγχοι απόδοσης και ποιότητας οι οποίοι θα παρέχουν πιο ολοκληρωμένα, πλήρης και με μεγαλύτερη ακρίβεια αποτελέσματα σχετικά με την δυνατότητα επικοινωνίας των εξεταζόμενων Υπηρεσιών Ιστού.
- Η επίτευξη της σημασιολογικής διαλειτουργικότητας στην προτεινόμενη μεθοδολογία με τη χρήση μεταδεδομένων και οντολογιών δίνοντας τη δυνατότητα επιτυχούς αλληλεπίδρασης Υπηρεσιών Ιστού οι οποίες χρησιμοποιούν διαφορετικά XML σχήματα και διαφορετικά λεξιλόγια.
- Ο εμπλουτισμός των κριτηρίων αξιολόγησης των εξεταζόμενων Υπηρεσιών Ιστού με νέα κριτήρια όπως είναι η αυτοματοποιημένη σύγκριση των Πολιτικών Ιδιωτικότητας.

Ο δεύτερος άξονας της διατριβής θέτει στο επίκεντρο του ενδιαφέροντος ζητήματα που αφορούν την διαχείριση της ταυτότητας και της ιδιωτικότητας στις ασφαλείς και προηγμένες κινητές και ηλεκτρονικές Υπηρεσίες Ιστού (ΥΙ). Σε πρώτη φάση μελετήθηκαν ζητήματα που αφορούν τη διαχείριση ταυτότητας και παρουσιάστηκαν

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

και κατηγοριοποιήθηκαν οι υπάρχουσες γλώσσες ιδιωτικότητας οι οποίες μπορούν να χρησιμοποιηθούν ώστε να αποτυπωθούν οι πολιτικές ιδιωτικότητας των οντοτήτων που μετέχουν σε μια συναλλαγή απεικονίζοντας με αυτόν τον τρόπο τα χαρακτηριστικά στοιχεία τόσο των χρηστών όσο και των ΥΙ.
Στη συνέχεια μελετήθηκαν σε βάθος τα υπάρχοντα συστήματα διαχείρισης ταυτότητας και οι προτεινόμενες κατηγοριοποιήσεις τους. Βασική επιδίωξη ήταν η πρόταση μιας ταξινόμησης των σχεδιαστικών λύσεων των Αρχιτεκτονικών Προσανατολισμένων στις Υπηρεσίες (ΑΠΥ) παρέχοντας συγκεκριμένες λύσεις διαχείρισης ταυτότητας και διαδικασιών οι οποίες μπορούν να εφαρμοστούν για καθεμία από τις προσδιοριζόμενες κατηγορίες.
Οι περαιτέρω ανάγκες οι οποίες εντοπίστηκαν από τη συγκεκριμένη μελέτη συνοψίζονται στις ακόλουθες:

- Η ύπαρξη μεθόδων και πλαισίων Αυτοματοποιημένης Σύγκρισης Πολιτικών Ιδιωτικότητας, οι οποίες θα επιτρέπουν τον έλεγχο της συμβατότητας των Πολιτικών διαπιστώνοντας τη δυνατότητα επικοινωνίας των οντοτήτων.
- Η απαίτηση για μεθόδους και διαδικασίες που επιτρέπουν την διαπραγμάτευση των Όρων των Πολιτικών Ιδιωτικότητας ώστε να καθοριστούν οι αρχές με βάση τις οποίες θα πραγματοποιηθεί μια συναλλαγή.
- Μέθοδοι οι οποίοι εγγυώνται την εκτέλεση των Πολιτικών Ιδιωτικότητας με βάση των οποίων πραγματοποιήθηκε μια συγκεκριμένη συναλλαγή. Η ανάπτυξη τέτοιων μεθόδων θα πρέπει να πραγματοποιηθεί ακολουθώντας, από τη μία πλευρά, το υπάρχον νομικό πλαίσιο προστασίας των δεδομένων και, από την άλλη πλευρά, τα αποδεδειγμένα πρότυπα ασφάλειας στον τομέα της ιδιωτικότητας των δικτυοκεντρικών συστημάτων και υπηρεσιών (όπως το ISO17999 (ISO17999, 2000), Common Criteria (Common Criteria)).

Κατά την διάρκεια της έρευνας στο δεύτερο άξονα διαπιστώθηκε επίσης και η σημασία που έχει η καταγραφή και αποτύπωση της συμπεριφοράς που επιδεικνύεται από τους χρήστες στα πλαίσια των συναλλαγών που αυτοί εκτελούν με τις ΥΙ και του ρόλου που αυτή μπορεί να διαδραματίσει για την ενίσχυση της ιδιωτικότητας. Για το λόγο αυτό εξετάστηκαν ένα σύνολο από συστήματα καταγραφής και αποτύπωσης συμπεριφοράς παραθέτοντας τις αδυναμίες που αυτά παρουσιάζουν. Επιδίωξη αποτέλεσε η πρόταση μιας υπηρεσίας καταγραφής συμπεριφοράς (ΥΚΣ) περιγράφοντας τον τρόπο που αυτό λειτουργεί σε συνδυασμό με ένα σύστημα διαχείρισης ταυτότητας.
Μελλοντικές ερευνητικές δραστηριότητες και κατευθύνσεις που αφορούν την προτεινόμενη ΥΚΣ είναι οι ακόλουθες:

- Επέκταση της προσφερόμενης λειτουργικότητας, επιτρέποντας στην ΥΚΣ τη συσσώρευση γνώσης σχετικά με του παρόχους υπηρεσιών υπολογίζοντας και καταγράφοντας και τη συμπεριφορά που επιδεικνύουν και αυτοί με τη σειρά τους. Η γνώση αυτή μπορεί να χρησιμοποιηθεί από τους καταναλωτές ως κριτήριο επιλογής του πιο αξιόπιστου παρόχου. Επιπλέον έρευνα θα πρέπει να διεξαχθεί προκειμένου να διερευνηθεί η ομαλή ολοκλήρωση και αυτής της διαδικασίας στο ομοσπονδιακό πλαίσιο χωρίς να αυξηθεί η υποκείμενη πολυπλοκότητα.
- Η πρόκληση του αυτόματου συνδυασμού δεδομένων συμπεριφοράς από ένα δεδομένο πλαίσιο αναφοράς. Οι γλώσσες οντολογίας όπως η OWL αποτελούν αυτή τη στιγμή τον καλύτερο τρόπο για την εξασφάλιση της διαλειτουργικότητας μεταξύ της σημασιολογίας διαφορετικών κρίσεων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

συμπεριφοράς, ώστε να είναι δυνατή η λήψη μιας συνδυασμένης τιμής συμπεριφοράς από ετερογενής πηγές.

- Η έλλειψη ενός προτυποποιημένου τρόπου αναπαράστασης δεδομένων συμπεριφοράς και ενσωμάτωσης τους σε πρωτόκολλα μεταφοράς πληροφοριών όπως είναι το SAML.

Τέλος ο δεύτερος άξονας της διατριβής εστίασε στη διερεύνηση μηχανισμών οι οποίοι μπορούν να διευθετήσουν την Ανωνυμία σε Επίπεδο Σύνδεσης των ΥΙ. Μελετήθηκαν υπάρχουσες προσεγγίσεις που στρέφονται προς την κατεύθυνση αυτή και καταγράφηκαν συγκεκριμένες αδυναμίες τους. Στόχος ήταν η πρόταση ενός ολοκληρωμένου πλαισίου στο οποίο η Ανωνυμία δύναται να διευθετηθεί ικανοποιητικά. Ένα σημαντικό ζήτημα το οποίο αφορά το προτεινόμενο μοντέλο ανωνυμίας και η διευθέτηση του οποίου διαδραματίζει σημαντικό ρόλο στην ενίσχυση του σχετίζεται με τη χρησιμοποίηση διαπιστευτηρίων ανωνυμίας τα οποία εκδίδονται από τα Συστήματα Διαχείρισης Ταυτότητας και τα οποία στην παρούσα φάση χρησιμοποιούνται για την πιστοποίηση και την εξουσιοδότηση των χρηστών για την εφαρμογή των απαιτούμενων μηχανισμών ασφάλειας στην περίπτωση των Υπηρεσιών Ιστού.

Στο σύνολο τους οι μελλοντικές κατευθύνσεις μορεί να θεωρηθούν ως επεκτάσεις της προτεινόμενης διατριβής ενώ η πρόταση σαφώς ορισμένων και τεκμηριωμένων λύσεων επιτρέπουν την ενίσχυση και τη διασφάλιση των αποτελεσμάτων της.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

9 Παράστημα

9.1 XAdES-X Υπογεγραμμένο Έγγραφο Ηλεκτρονικής Τιμολόγησης

Στο παρόν Κεφάλαιο παρατίθεται το XAdES-X υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης που παράγει η υπηρεσία SELIS κατά την πρώτη φάση του ελέγχου συμμόρφωσης.

XAdES-X-Invoice.xml

9.2 XAdES-X-L Υπογεγραμμένο Έγγραφο Ηλεκτρονικής Τιμολόγησης

Στο παρόν Κεφάλαιο παρατίθεται το XAdES-X-L υπογεγραμμένο έγγραφο ηλεκτρονικής τιμολόγησης που παράγει η υπηρεσία SELIS μετά την υλοποίηση των διορθώσεων.

XAdES-X-L-Invoice.xml

9.3 Περιγραφή της Υπηρεσία της SWEB Ηλεκτρονικής Τιμολόγησης

Στο παρόν κεφάλαιο παρατίθεται η περιγραφή της υπηρεσία της SWEB ηλεκτρονικής τιμολόγησης.

eInvoice_WSDL_Description.xml

9.4 Αποτελέσματα Συμμόρφωσης

Στο παρόν κεφάλαιο παρατίθενται τα αποτελέσματα (Πίνακας 22, Πίνακας 23, Πίνακας 24, Πίνακας 25 και Πίνακας 26) του ελέγχου συμμόρφωσης του μηνύματος που στέλνει η υπηρεσία ηλεκτρονικής τιμολόγησης SELIS στην υπηρεσία ηλεκτρονικής τιμολόγησης SWEB όπως αυτά παράγονται από το εργαλείο ‘Αναλυτής’ (Analyzer) του WS-I που έχει ενσωματωθεί στην Υπηρεσίας Ανάλυσης Μηνυμάτων της ΥΔΕ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Summary	
Result	Passed

Πίνακας 22. Συνολικό αποτέλεσμα συμμόρφωσης

Artifact: description						
Assertion Result Summary:						
Assertion ID	Passed	Failed	Prerequsite Failed	Warning	Not Applicable	Missing Input
BP2010	1	0	0	0	0	
BP2011	1	0	0	0	0	
BP2012	1	0	0	0	0	
BP2013	0	0	0	0	1	
BP2014	0	0	0	0	1	
BP2017	1	0	0	0	0	
BP2018	1	0	0	0	0	
BP2019	1	0	0	0	0	
BP2020	0	0	0	0	1	
BP2021	1	0	0	0	0	
BP2022	0	0	0	0	1	
BP2032	1	0	0	0	0	
BP2034	1	0	0	0	0	
BP2098	0	0	0	0	0	X
BP2101	0	0	0	0	1	
BP2102	1	0	0	0	0	
BP2103	1	0	0	0	0	
BP2104	0	0	0	0	1	
BP2105	0	0	0	0	1	
BP2107	1	0	0	0	0	
BP2108	1	0	0	0	0	
BP2110	1	0	0	0	0	
BP2111	1	0	0	0	0	
BP2112	0	0	0	0	1	
BP2113	1	0	0	0	0	
BP2114	1	0	0	0	0	
BP2115	3	0	0	0	0	
BP2116	3	0	0	0	0	

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

BP2117	0	0	0	0	**1**	
BP2118	**1**	0	0	0	0	
BP2119	**1**	0	0	0	0	
BP2120	**1**	0	0	0	0	
BP2122	**1**	0	0	0	0	
BP2123	0	0	0	0	**1**	
BP2201	**1**	0	0	0	0	
BP2202	**1**	0	0	0	0	
BP2208	**1**	0	0	0	0	
BP2402	**1**	0	0	0	0	
BP2404	**1**	0	0	0	0	
BP2406	**1**	0	0	0	0	
BP2416	**1**	0	0	0	0	
BP2417	**1**	0	0	0	0	
BP2700	**1**	0	0	0	0	
BP2701	**1**	0	0	0	0	
BP2703	**1**	0	0	0	0	
BP2803	0	0	0	0	0	**X**
BP4200	0	0	0	0	**1**	
BP4201	0	0	0	0	**1**	
BP4202	**1**	0	0	0	0	
SSBP2209	**1**	0	0	0	0	
SSBP2403	**1**	0	0	0	0	

Πίνακας 23. Αναφορά συμμόρφωσης για τα χαρακτηριστικά περιγραφής (description artifacts) του SOAP μηνύματος

Artifact: Discovery						
Assertion Result Summary:						
Assertion ID	**Passed**	**Failed**	**Prerequsite Failed**	**Warning**	**Not Applicable**	**Missing Input**
BP3001	0	0	0	0	0	**X**
BP3002	0	0	0	0	0	**X**
BP3003	0	0	0	0	0	**X**

Πίνακας 24. Αναφορά συμμόρφωσης για τα χαρακτηριστικά ανακάλυψης (discovery artifacts) του SOAP μηνύματος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Artifact: Message						
Assertion Result Summary:						
Assertion ID	Passed	Failed	Prerequsite Failed	Warning	Not Applicable	Missing Input
BP1001	2	0	0	0	0	
BP1002	2	0	0	0	0	
BP1004	1	0	0	0	0	
BP1006	1	0	0	0	0	
BP1010	0	0	0	0	1	
BP1101	0	0	0	0	1	
BP1103	0	0	0	0	1	
BP1116	1	0	0	0	0	
BP4103	0	0	0	0	2	
BP4104	2	0	0	0	0	
BP4105	0	0	0	0	2	
BP4106	0	0	0	0	1	
BP4107	0	0	0	0	1	
SSBP1003	2	0	0	0	0	
SSBP5100	2	0	0	0	0	
SSBP5101	2	0	0	0	0	

Πίνακας 25. Αναφορά συμμόρφωσης για τα χαρακτηριστικά μηνύματος (message artifacts) του SOAP μηνύματος

Artifact: Envelope						
Assertion Result Summary:						
Assertion ID	Passed	Failed	Prerequsite Failed	Warning	Not Applicable	Missing Input
BP1005	0	0	0	0	1	
BP1007	2	0	0	0	0	
BP1008	0	0	0	0	2	
BP1009	2	0	0	0	0	
BP1011	1	0	0	0	0	
BP1012	0	0	0	0	1	
BP1013	1	0	0	0	0	
BP1031	0	0	0	0	1	
BP1032	2	0	0	0	0	
BP1033	2	0	0	0	0	
BP1100	1	0	0	0	0	

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

BP1107	0	0	0	0	**1**	
BP1201	**2**	0	0	0	0	
BP1202	**2**	0	0	0	0	
BP1203	0	0	0	0	**1**	
BP1204	**2**	0	0	0	0	
BP1208	**2**	0	0	0	0	
BP1211	0	0	0	0	**2**	
BP1212	0	0	0	0	**2**	
BP1213	**2**	0	0	0	0	
BP1214	0	0	0	0	**2**	
BP1301	**2**	0	0	0	0	
BP1302	0	0	0	0	**1**	
BP1305	0	0	0	0	**1**	
BP1306	0	0	0	0	**1**	
BP1307	**2**	0	0	0	0	
BP1308	**2**	0	0	0	0	
BP1309	**2**	0	0	0	0	
BP1316	0	0	0	0	**1**	
BP1318	0	0	0	0	**2**	
BP1600	**2**	0	0	0	0	
BP1601	**2**	0	0	0	0	
BP1701	**2**	0	0	0	0	
BP1755	0	0	0	0	**2**	
BP4100	**2**	0	0	0	0	
BP4101	0	0	0	0	**2**	
BP4102	0	0	0	0	**2**	
BP4109	**2**	0	0	0	0	
SSBP1601	**2**	0	0	0	0	
SSBP9704	**2**	0	0	0	0	

Πίνακας 26 Αναφορά συμμόρφωσης για τα χαρακτηριστικά φακέλου (envelope artifacts) του SOAP μηνύματος