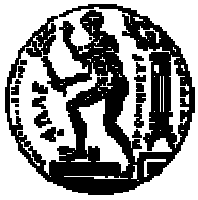


ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Σχεδίαση και Υλοποίηση Συστήματος Διαδικτυακής Τηλεφωνίας, το οποίο παρέχει Εγγυήσεις για τη Διασφάλιση της Ιδιωτικότητας των Χρηστών του

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΝΔΡΕΑΣ ΝΟΜΙΚΟΣ
ΕΡΡΙΚΟΣ ΟΥΖΙΕΛ

Επιβλέπων : Ιάκωβος Βενιέρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2008

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

Σχεδίαση και Υλοποίηση Συστήματος Διαδικτυακής Τηλεφωνίας, το οποίο παρέχει Εγγυήσεις για τη Διασφάλιση της Ιδιωτικότητας των Χρηστών του

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΝΔΡΕΑΣ ΝΟΜΙΚΟΣ
ΕΡΡΙΚΟΣ ΟΥΖΙΕΛ

Επιβλέπων : Ιάκωβος Βενιέρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή τη 16η Οκτωβρίου 2008.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Ιάκωβος Βενιέρης Καθηγητής Ε.Μ.Π.	Δήμητρα-Θεοδώρα Κακλαμάνη Αν. Καθηγήτρια Ε.Μ.Π.	Νικόλαος Ουζούνογλου Καθηγητής Ε.Μ.Π

Αθήνα, Οκτώβριος 2008

(Υπογραφή)

.....

ΑΝΔΡΕΑΣ ΝΟΜΙΚΟΣ

(Υπογραφή)

.....

ΕΡΡΙΚΟΣ ΟΥΖΙΕΛ

Διπλωματούχοι Ηλεκτρολόγοι Μηχανικοί και Μηχανικοί Υπολογιστών Ε.Μ.Π.

Περίληψη

Σκοπός της διπλωματικής εργασίας είναι η ανάπτυξη ενός συστήματος προστασίας των προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας. Για την επίτευξη του στόχου αυτού αναλύθηκε το σύστημα μιας υποθετικής εταιρείας, η οποία προσφέρει τέτοιου είδους διαδικτυακές υπηρεσίες, βασισμένες στο γνωστό πρωτόκολλο SIP. Το επιχειρηματικό μοντέλο της εταιρείας δεν βασίζεται μόνο σε υπηρεσίες τηλεφωνίας, αλλά επεκτείνεται και σε άλλες γνωστές υπηρεσίες, όπως της αποστολής άμεσων μηνυμάτων, της παροχής υπηρεσιών παρουσίας και της πώλησης στατιστικών στοιχείων πελατολογίου σε τρίτους. Στη συνέχεια, σχεδιάστηκε η αρχιτεκτονική ενός συστήματος διαδικτυακής τηλεφωνίας, που θα παρέχει εγγυήσεις στους συνδρομητές της εταιρείας για την προστασία των προσωπικών τους δεδομένων, ενώ ταυτόχρονα θα διατηρεί, όσο το δυνατόν, αναλλοίωτο το επιχειρηματικό μοντέλο της εταιρείας. Στη σχεδίαση λήφθηκαν σοβαρά υπόψη οι υπάρχουσες προτάσεις της διεθνούς βιβλιογραφίας για το συγκεκριμένο ζήτημα και προτάθηκαν επεκτάσεις, όπου κρίθηκε απαραίτητο.

Συγκεκριμένα, υιοθετήθηκε και επεκτάθηκε ο μηχανισμός προστασίας των προσωπικών δεδομένων που προτείνεται από την IETF για χρήση στο πρωτόκολλο SIP. Οι επεκτάσεις περιλαμβάνουν την υποστήριξη της ανωνυμίας της διεύθυνσης IP και τη χρήση προσωρινών ψευδωνύμων χρήστη για την υλοποίηση ανωνυμίας στο SIP.
Ταυτόχρονα, προτείνεται η υλοποίηση ενός συστήματος ελεγχόμενης πρόσβασης της εταιρείας στα προσωπικά δεδομένα, που περιέχονται στη βάση δεδομένων. Το σύστημα αυτό εκμεταλλεύεται τις εξελίξεις στο χώρο της σημασιολογικής απεικόνισης και βασίζεται σε μια οντολογία, η οποία μοντελοποιεί τους κανόνες της σχετικής νομοθεσίας, για να ελέγξει και πιθανόν να μετατρέψει εισερχόμενα προς τη βάση ερωτήματα σε αντίστοιχα, των οποίων τα αποτελέσματα δεν θα παραβιάζουν την ιδιωτικότητα των συνδρομητών.

Εκτός από τη σχεδίαση της αρχιτεκτονικής του συστήματος σε θεωρητικό επίπεδο, επιλέχθηκαν συγκεκριμένα ελεύθερα προγράμματα ανοικτού κώδικα (Tor, JAIN-SIP proxy, SIP-Communicator), τα οποία μπορούν να αποτελέσουν βάση για την υλοποίηση της προτεινόμενης αρχιτεκτονικής, και σχεδιάστηκε η επέκταση τους, ή η ενοποίηση τους ώστε να υλοποιούν την προτεινόμενη λειτουργικότητα. Τέλος, υλοποιήθηκε ένα πειραματικό σύστημα, που υποστηρίζει ένα υποσύνολο της προτεινόμενης λειτουργικότητας.

Η συγκεκριμένη διπλωματική εργασία μπορεί να γίνει οδηγός για την υλοποίηση ενός πλήρους συστήματος προστασίας προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας, στο οποίο θα μπορέσουν να γίνουν μετρήσεις για να διαπιστωθεί η αποτελεσματικότητα της αρχιτεκτονικής σε πραγματικές συνθήκες.

Λέξεις Κλειδιά: ιδιωτικότητα, διαδικτυακή τηλεφωνία, προστασία προσωπικών δεδομένων, προστασία ιδιωτικότητας στο SIP, προστασία διευθύνσεων IP στο SIP , Tor στο SIP, σημασιολογική ανάλυση ερωτημάτων SQL, οντολογία προστασίας ιδιωτικότητας, προστατευμένη πρόσβαση σε βάση προσωπικών δεδομένων

Abstract

The scope of this thesis was the development of a VoIP system that would provide guaranteed privacy to its users. The system of a VoIP Service Provider that deploys the SIP architecture was analyzed in order to specify the privacy issues, whereas the company's business model also includes providing presence services and selling statistical data to third parties. The primary objective was to design an architecture that would provide guarantees to the customers about the protection of their private data, whilst preserving the company's business model. Modern solutions addressing this issue were taken into consideration during design and new suggestions were made where necessary.

More specifically the suggested Privacy Mechanism for SIP (RFC 3323) was adopted and implemented, and new additions were defined in order to support IP and SIP URI anonymization. The latter is achieved through the use of temporary routable pseudonyms valid only inside a specific domain. Moreover a privacy-aware mechanism for accessing private data in a secure database was suggested to provide the company with extended flexibility. This mechanism takes advantage of the latest achievements in the area of semantics and uses an ontology in order to model the related laws and forbid or reform SQL queries to the database, that would violate the user's privacy.

In addition to the theoretical system analysis and design, certain open source programs were chosen (Tor, JAIN-SIP proxy, SIP-Communicator) to provide a base working platform and their integration or expansion according to the suggested architecture was designed. In the end a subset of the proposed functionality was implemented in an experimental system.

This particular thesis provides guidance for the implementation of a full scale privacy-aware VoIP system, that can be used to evaluate the proposed architecture under real life circumstances.

Keywords: Privacy, VoIP, SIP, IP anonymization, Tor network, semantic processing of SQL queries, Privacy Ontology, privacy-aware access of database

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή της διπλωματικής μας κ. Ιάκωβο Βενιέρη, για την ευκαιρία που μας έδωσε να ασχοληθούμε με το παρόν ερευνητικό αντικείμενο. Επίσης ευχαριστούμε τον κ. Γεώργιο Λιουδάκη, για την καθοδήγησή του και την πολύτιμη βοήθειά του στην εκπόνηση της παρούσας διπλωματικής εργασίας. Θέλουμε να εκφράσουμε την ευγνωμοσύνη μας στους γονείς μας για την διαρκή τους υποστήριξη.

Νομικός Ανδρέας

Ουζιέλ Ερρίκος,

Αθήνα, 9η Οκτωβρίου 2008

Πίνακας περιεχομένων

Πίνακας Εικόνων

1

Εισαγωγή

1.1 Το πρόβλημα της προστασίας της Ιδιωτικότητας

Η ιδιωτικότητα αποτελεί ένα καίριο θέμα συζήτησης για κοινωνιολόγους, φιλόσοφους και νομικούς. Σύμφωνα με τη Διακήρυξη των Ανθρωπίνων Δικαιωμάτων του Ο.Η.Ε. αποτελεί ένα από τα θεμελιώδη ανθρώπινα δικαιώματα και η προστασία της πρέπει να αποτελεί διαρκή επιδίωξη για μια δημοκρατική κοινωνία [1]. Παρ' όλα αυτά, με την αλματώδη ανάπτυξη των υπολογιστών και των διασυνδεμένων δικτύων, η ύπαρξη προσωπικής ελευθερίας τίθεται διαρκώς υπό αμφισβήτηση. Οι απεριόριστες δυνατότητες που προσφέρει το παγκόσμιο διαδίκτυο, η κορωνίδα των πληροφοριακών συστημάτων, για την συλλογή, αποθήκευση και επεξεργασία πληροφοριών, αλλάζουν άρδην τον τρόπο με τον οποίο αντιλαμβανόμαστε τον κόσμο. Στην πραγματικότητα, η διεθνής κοινότητα μόλις τώρα αρχίζει να αντιλαμβάνεται το εύρος των δυνατοτήτων και τους κινδύνους που παρουσιάζονται.

Πώς ορίζεται, όμως, αυτή η τόσο σημαντική, αλλά άυλη έννοια;

„Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [Westin 1967].

„Ιδιωτικότητα είναι το θεμελιώδες δικαίωμα των ατόμων, των ομάδων και των ιδρυμάτων να καθορίζουν οι ίδιοι, τον χρόνο, τον τρόπο και το εύρος της δημοσιοποίησης πληροφοριών που αφορούν τους ίδιους σε τρίτους." [Westin 1967].

Σύμφωνα με τον ορισμό που δίνει ο Alan Westin [1], τόσο τα φυσικά, όσο και τα νομικά πρόσωπα έχουν δικαίωμα στην ιδιωτικότητα. Στον ορισμό αυτό δίνεται έμφαση στο δικαίωμα του ανθρώπου στον αυτοπροσδιορισμό και την αυτοδιαχείριση των δεδομένων, που τον

zαφορούν. Ως προσωπικά δεδομένα θεωρούνται όλα αυτά που αφορούν την προσωρινή, ή μόνιμη κατάσταση ενός ατόμου και τις προσωπικές απόψεις του, ενώ η προστασία της ιδιωτικότητας ορίζεται ως εξής: οι ενέργειες που λαμβάνονται για την προστασία των προσωπικών δεδομένων με στόχο την εγγυημένη διασφάλιση της ιδιωτικότητας του ατόμου. Η έννοια της προστασίας της ιδιωτικότητας όμως, αποτελεί μόνο ένα μέρος της ευρύτερης έννοιας της ιδιωτικότητας, αφού η τελευταία, στις σύγχρονες κοινωνίες, δεν εξασφαλίζει μόνο την προστασία του ατόμου, αλλά πρέπει να συνδέεται και με άλλα δικαιώματα και νομικές αξίες που πηγάζουν από την κοινωνία, στην οποία εφαρμόζεται. Εξάλλου κανένα άτομο δεν μπορεί να είναι μέλος μιας κοινωνίας χωρίς να αποκαλύπτει ποτέ προσωπική του πληροφορία, αφού η επικοινωνία στα πλαίσια μιας κοινωνίας είναι πολύ σημαντική για την ανάπτυξη και ευημερία της. Εδώ θα πρέπει να επισημανθεί και να διασαφηνισθεί μια συνηθισμένη σύγχυση που συμβαίνει συχνά στον χώρο των διαδικτυακών υπηρεσιών. Η σύγχυση των όρων ασφάλεια (security) και ιδιωτικότητα (privacy). Παρ' όλο που οι όροι εμφανίζονται στο ίδιο περιβάλλον και επικρατεί η αντίληψη ότι αναφέρονται στην ίδια έννοια, η ασφάλεια είναι κάτι διαφορετικό από την ιδιωτικότητα.

Η έννοια ασφάλεια (security) αναφέρεται σε τεχνικές λύσεις και τεχνολογίες, οι οποίες εξασφαλίζουν ότι θα έχουν πρόσβαση στα δεδομένα που ανταλλάζονται σε ένα κανάλι επικοινωνίας ή βρίσκονται αποθηκευμένα στους υπολογιστές χρηστών και εταιρειών, μόνο όσοι έχει προβλεφθεί ότι θα έχουν. Έτσι ο όρος «ασφάλεια» αναφέρεται στην προστασία από μη εξουσιοδοτημένη πρόσβαση, προστασία από τις υποκλοπές, προστασία κατά τη μετάδοση κωδικών πρόσβασης και πιστωτικών καρτών και αντίστοιχες τεχνολογίες. Για την εξασφάλιση της ασφάλειας μιας διαδικτυακής υπηρεσίας υπάρχουν ευρέως εφαρμοζόμενες τεχνολογίες κρυπτογράφησης και ελέγχου πρόσβασης, οι οποίες θεωρούνται απαραβίαστες, ή τουλάχιστον τόσο δύσκολα παραβιάσιμες, που μόνο κυβερνητικοί οργανισμοί με τρία γράμματα μπορούν να παραβιάσουν. Αν και σ' όλα τα πληροφοριακά συστήματα υπάρχουν κενά ασφαλείας, τα οποία συνήθως οφείλονται στον ανθρώπινο παράγοντα, οι τεχνολογίες ασφαλείας που υπάρχουν είναι τόσο αξιόπιστες ώστε να αποτελούν θεμέλιο της εκρηκτικής οικονομικής δραστηριότητας, που έχει αναπτυχθεί στο διαδίκτυο. Αλγόριθμοι κρυπτογράφησης των οποίων η κρυπτανάλυση θα απαιτούσε χιλιάδες χρόνια υπολογιστικού χρόνου μπορούν να εξασφαλίσουν ότι τα δεδομένα είναι προσβάσιμα μόνο από όσους έχουν το κλειδί να ξεκλειδώσουν την κλειδαριά. Όπως περιγράψαμε παραπάνω, η ιδιωτικότητα περιλαμβάνει την έννοια της αυτοδιαχείρισης της προσωπικής πληροφορίας. Άρα η έννοια της δεν περιλαμβάνει μόνο προστασία κάποιων δεδομένων από παράνομη πρόσβαση, αλλά γενικότερα προστασία δεδομένων προσωπικού χαρακτήρα από οποιονδήποτε δεν επιθυμεί ο χρήστης. Σε σχέση για παράδειγμα με τα προφίλ των χρηστών σε μια υπηρεσία στα οποία αποθηκεύονται προσωπικά δεδομένα, προτιμήσεις και συνήθειες τους, παρά το γεγονός ότι μπορεί να είναι αποθηκευμένα σε ασφαλείς βάσεις δεδομένων, δεν υπάρχει εξασφάλιση ότι κάποιος εξουσιοδοτημένος υπάλληλος, από μια εταιρεία παροχής υπηρεσιών ή ακόμα και κάποιο αυτοματοποιημένο ηλεκτρονικό σύστημα συλλογής και επεξεργασίας δεδομένων, δεν θα έχει πρόσβαση σε δεδομένα που ο ιδιόκτητης τους ποτέ δεν θα ήθελε να αποκαλυφτούν. Άρα η ασφάλεια, ενώ είναι αναγκαία συνθήκη για την ιδιωτικότητα, δεν είναι ικανή για την εξασφάλιση της.

Το πρόβλημα της προστασίας της ιδιωτικότητας είναι πολύπλοκο λόγω των αντικρουόμενων συμφερόντων των εμπλεκόμενων πλευρών. Όπως για παράδειγμα, η νέα μόδα παροχής υπηρεσιών στο διαδίκτυο, οι προσωπικές υπηρεσίες. Όλοι επιθυμούν να διατηρούν την ιδιωτικότητα τους, αλλά κανένας δεν λέει «όχι» στις εξαιρετικές προτάσεις του Amazon σε τίτλους βιβλίων, ούτε στα ακριβή αποτελέσματα, που προσφέρει η μηχανή

αναζήτησης της Google, υπηρεσίες που έχουν τόσο μεγάλη επιτυχία, ακριβώς λόγω της διαρκούς επεξεργασίας προσωπικών πληροφοριών των προηγούμενων χρηστών της υπηρεσίας. Η κατάσταση περιπλέκεται ακόμα περισσότερο αν αναλογιστούμε ότι εταιρίες-κολοσσοί έχουν βασίσει ολόκληρο το επιχειρηματικό τους μοντέλο στην επεξεργασία πληροφοριών και σίγουρα δεν θα ήθελαν να χάσουν τα κεκτημένα τους. Στον 21^{ο} αιώνα η πληροφορία είναι δύναμη και είναι η δύναμη που οδηγεί τις εξελίξεις. Σ' αυτό το ευμετάβλητο περιβάλλον η προστασία των προσωπικών δεδομένων τίθεται διαρκώς υπό αμφισβήτηση. Πληροφορίες, ασήμαντες μέχρι χτες, μπορεί να έχουν τεράστια αξία αύριο. Η εγκαθίδρυση ενός σταθερού νομοθετικού πλαισίου κρίνεται απαραίτητη [1], ενώ απαιτείται και ευελιξία από τους θεσμούς για την προσαρμογή στις νέες ανάγκες που θα προκύψουν. Ταυτόχρονα, η παγκοσμιοποίηση του διαδικτύου περιπλέκει τα πράγματα, αφού δεδομένα που θεωρούνται προσωπικά στην Ε.Ε. μπορεί να μην προστατεύονται στις Η.Π.Α., ενώ το νομικό πλαίσιο ευθυνών σε περίπτωση παραβιάσεων παραμένει νεφελώδες. Το γεγονός αυτό έχει οδηγήσει τα τελευταία χρόνια στην ανάπτυξη ενός μοντέλου προστασίας της ιδιωτικότητας, στις εταιρικές πολιτικές προστασίας ιδιωτικότητας (Privacy Policies), το οποίο είναι αμφιλεγόμενο, ενώ η αποδοτικότητα του τίθεται καθημερινά υπό αμφισβήτηση.

Στις υπάρχουσες αρχιτεκτονικές, ο χρήστης θα πρέπει να εμπιστεύεται την εταιρεία ότι θα τηρήσει τις δεσμεύσεις της όσον αφορά την προστασία της ιδιωτικότητας του, ενώ οι δεσμεύσεις αυτές εκφράζονται μέσω ενός νομικού εγγράφου (δήλωση ιδιωτικότητας) [2]-[4], που περιγράφει την πολιτική της σχετικά με την ιδιωτικότητα. Σ' αυτό το κείμενο περιγράφονται τα προσωπικά δεδομένα που συγκεντρώνει μια εταιρεία, το πώς τα χρησιμοποιεί και τη χρονική διάρκεια κατά την οποία τα διατηρεί αποθηκευμένα. Επίσης, δηλώνει με ποιους τα μοιράζεται και για ποιους σκοπούς. Η κάθε εταιρεία έχει τον απόλυτο έλεγχο πάνω στην πολιτική προστασίας της ιδιωτικότητας, που θα ακολουθήσει, αρκεί αυτή να μην έρχεται σε σύγκρουση με την υπάρχουσα νομοθεσία. Η συνήθης πρακτική είναι η εταιρεία να ζητά από το χρήστη να αποδεχτεί τη δήλωση ιδιωτικότητάς της για να μπορέσει να εγγραφεί σε μια υπηρεσία. Ωστόσο, επειδή συνήθως η δήλωση ιδιωτικότητας αποτελεί ένα δυσνόητο νομικό κείμενο, οι χρήστες της υπηρεσίας δεν δίνουν την πρέπουσα σημασία, (πολλές φορές δεν δίνουν καμία σημασία), στην ανάγνωσή της, συναινώντας μ' αυτόν τον τρόπο σε διαδικασίες αποκάλυψης των προσωπικών δεδομένων τους που δεν θα γίνονταν αποδεκτές αν ήταν πιο σαφώς διατυπωμένες. Ταυτόχρονα, η εταιρεία θέτει στους χρήστες ένα εκβιαστικό δίλημμα, αφού η υπηρεσία προσφέρεται, μόνο σύμφωνα με την συγκεκριμένη δήλωση ιδιωτικότητας, κάτι που αποκλείει πολλούς χρήστες από τη χρήση της. Αυτό για σημαντικές υπηρεσίες, όπως η τηλεφωνία δεν είναι αποδεκτό.

Αν κάποιος διαβάσει τις δηλώσεις προστασίας ιδιωτικότητας των δημοφιλέστερων διαδικτυακών υπηρεσιών θα δει ότι ουσιαστικά οι πολιτικές ιδιωτικότητας έχουν τον αντίθετο ρόλο απ' αυτόν, που κάποιος θα περίμενε να έχουν [2]-[4]. Αντί να περιγράφουν τις διαδικασίες, που εφαρμόζει η εταιρεία για να προστατέψει την ιδιωτικότητα των χρηστών και τις εγγυήσεις που παρέχει αυτή απέναντί τους, περιγράφουν το ότι για να παρασχεθεί η υπηρεσία είναι απαραίτητο να διαμοιραστούν πάσης φύσεως δεδομένα, σχετικά με το χρήστη, σε τρίτους και ζητείται από το χρήστη με τη συναίνεσή του να νομιμοποιήσει αυτές τις πρακτικές. Υπάρχουν πολλές χαρακτηριστικές περιπτώσεις που εφαρμόζεται η συγκεκριμένη λογική, με πιο διαδεδομένη την περίπτωση των ιστοσελίδων κοινωνικής δικτύωσης [2]. Η συντριπτική πλειοψηφία αυτών των διαδικτυακών τόπων προσφέρουν δωρεάν τις υπηρεσίες τους στους χρήστες και αξιοποιούν τις προσωπικές πληροφορίες που συγκεντρώνουν για να κάνουν στοχευμένη διαφήμιση. Μάλιστα, σε ορισμένες περιπτώσεις επιτρέπουν και σε εταιρείες με τις οποίες συνεργάζονται, να έχουν πρόσβαση στα προσωπικά

δεδομένα και μάλιστα τις εξουσιοδοτούν να τα χρησιμοποιήσουν για δικούς τους σκοπούς (third party applications). Αν και ο χρήστης της υπηρεσίας θεωρητικά κατά την εγγραφή του ενημερώνεται γι' αυτές τις διαδικασίες, τελικά χάνει κάθε έλεγχο για το ποίος έχει την κατοχή του και επεξεργάζεται τα προσωπικά του δεδομένα.

Υπάρχουν όμως και περιπτώσεις που έχει γίνει αποκάλυψη πληροφορίας, η οποία θεωρείται προσωπική, χωρίς τη συγκατάθεση του χρήστη, περιπτώσεις που καταδεικνύουν την ανεπάρκεια του υπάρχοντος μοντέλου να παρέχει εγγυήσεις στους χρήστες για την προστασία των προσωπικών τους δεδομένων. Στο σκάνδαλο αποκάλυψης δεδομένων αναζήτησης της AOL (AOL search data scandal, 2006) [5], η αναφερόμενη εταιρεία παροχής υπηρεσιών αναζήτησης στο διαδίκτυο αποκάλυψε δώδεκα εκατομμύρια κλειδιά αναζήτησης από ερωτήματα που είχαν εκτελέσει πάνω από 650.000 χρήστες εντός μιας περιόδου τριών μηνών. Αν και στο αρχείο που δημοσιεύτηκε είχε αντικατασταθεί το όνομα του κάθε χρήστη με κάποιον ανώνυμο μοναδικό αριθμό, πολλά από τα κλειδιά αναζήτησης αποκάλυπταν επακριβώς την ταυτότητα του χρήστη, που εκτέλεσε το ερώτημα, τη διεύθυνσή του, αλλά και άλλα προσωπικά του δεδομένα. Μέσω του αρχείου αποκαλύφτηκαν ακόμα και ευαίσθητα προσωπικά δεδομένα χρηστών, όπως ιατρικό ιστορικό και πολιτικές απόψεις, καθώς είναι σύνηθες κάποιος χρήστης να αναζητά πληροφορίες σχετικά με αυτά τα ζητήματα. Το σκάνδαλο πήρε τόσο μεγάλες διαστάσεις που δημιουργήθηκαν ειδικές σελίδες [6] στο διαδίκτυο, ελεγχόμενες από τρίτους, στις οποίες γινόταν η αναζήτηση και η ταυτοποίηση χρηστών, καθώς και η κατηγοριοποίησή τους με βάση τις συνήθειες τους. Η AOL παραδέχτηκε ότι η δημοσιοποίηση των δεδομένων ήταν λάθος και αμέσως απέσυρε το αρχείο από τη σελίδα της, ωστόσο μετά τη δημοσιοποίησή του άμεσα αντιγράφτηκε σε άλλες σελίδες και διατηρείται ακόμα στη δημοσιότητα. Το παραπάνω περιστατικό παρουσιάζει τη διάσταση που μπορεί να έχει η αποκάλυψη προσωπικής πληροφορίας στο σύγχρονο δικτυωμένο κόσμο, όπου τα δεδομένα ανταλλάσσονται και αποθηκεύονται ακαριαία και αβίαστα. Η βλάβη που μπορεί να προκληθεί στο άτομο και την υπόληψή του από την αποκάλυψη προσωπικών δεδομένων είναι μη αναστρέψιμη, καθώς, όταν χαθεί η ιδιωτικότητα, δεν υπάρχει τρόπος να επανακτηθεί.

Υπάρχουν ακόμα περιπτώσεις, που εταιρείες παραβιάζουν κατάφορα τη νομοθεσία, σχετικά με την προστασία των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών, εκμεταλλευόμενες το γεγονός ότι παρέχουν οι ίδιες τέτοιου είδους υπηρεσίες. Χαρακτηριστικότερη περίπτωση αποτελεί το σκάνδαλο που αποκαλύφθηκε πρόσφατα [7], σχετικά με τον κυρίαρχο πάροχο επικοινωνιών της Γερμανίας, την Deutsche Telekom. Ο όμιλος είχε επιφορτίσει ιδιωτική εταιρεία ασφάλειας με την αξιολόγηση συνομιλιών, που είχαν υποκλαπεί με στόχο τον εντοπισμό των προσώπων, που διοχέτευαν απόρρητα στοιχεία της εταιρείας σε δημοσιογράφους. Χρησιμοποιώντας τα αρχεία της εταιρείας με τους αριθμούς, τη διάρκεια και τις ημερομηνίες των τηλεφωνημάτων, η εταιρεία ασφάλειας αναζητούσε επαφές, ανάμεσα σε διευθυντικά στελέχη του γερμανικού κολοσσού τηλεπικοινωνιών και δημοσιογράφους, αξιολογώντας εκατοντάδες χιλιάδων συνδιαλέξεων κινητής και σταθερής τηλεφωνίας, που γίνονταν από συσκευές που ανήκαν σε δημοσιογράφους, οι οποίοι κάλυπταν το ρεπορτάζ των δραστηριοτήτων της. Αυτό το περιστατικό αποδεικνύει ότι ακόμα και η Κοινοτική νομοθεσία από μόνη της δεν μπορεί να αποτρέψει τη διαρροή προσωπικών πληροφοριών από οργανισμούς που παρέχουν τις υπηρεσίες τηλεπικοινωνιών και καταδεικνύει την αναγκαιότητα να αναζητηθούν λύσεις, που θα εξασφαλίζουν την ιδιωτικότητα των χρηστών από κάθε πιθανή διαρροή. Το πρόβλημα οξύνεται από το γεγονός ότι δεν υπάρχει κοινά αποδεκτή τεχνολογία και τεχνογνωσία, που να επιτρέπει τη διασφάλιση της ιδιωτικότητας του χρήστη. Η ιδιωτικότητα είναι κάτι που για να

εξασφαλιστεί απαιτεί αλλαγή στην αρχιτεκτονική και τη λειτουργία των πληροφοριακών συστημάτων.

1.2 Αντικείμενο διπλωματικής

Στην παρούσα διπλωματική εργασία ασχοληθήκαμε με το πρόβλημα της προστασίας των προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας (VoIP). Βασική επιδίωξη αποτελεί η παροχή εγγυήσεων διασφάλισης της ιδιωτικότητας στους συνδρομητές ενός παρόχου σχετικών υπηρεσιών, ακόμα και στην περίπτωση που ο ίδιος ο πάροχος δεν είναι έμπιστος. Για την επίτευξη του συγκεκριμένου στόχου αξιοποιήθηκε το θεωρητικό υπόβαθρο της διεθνούς βιβλιογραφίας στο συγκεκριμένο πεδίο και εφαρμόστηκαν γνωστές τεχνικές επίτευξης ανωνυμίας σε υπάρχουσες αρχιτεκτονικές, ενώ, όπου χρειάστηκε, προτάθηκαν συμπληρωματικές λειτουργίες και τεχνικές για την υποστήριξη της επιθυμητής λειτουργικότητας.

1.2.1 Συνεισφορά της παρούσας διπλωματικής

Η συνεισφορά της διπλωματικής στην επίλυση του προβλήματος της προστασίας των προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας συνοψίζεται στα εξής:

a. Μελέτη και ορισμός περιβάλλοντος λειτουργίας συστήματος
b. Σχεδιασμός της αρχιτεκτονικής προστασίας των προσωπικών δεδομένων και κατανομή λειτουργιών στις εμπλεκόμενες οντότητες
c. Σχεδιασμός έξυπνου συστήματος προστατευμένης πρόσβασης σε προσωπικά δεδομένα, το οποίο αξιοποιεί μοντελοποίηση των κανόνων της σχετικής νομοθεσίας
d. Περιγραφή των προδιαγραφών απαιτήσεων ενός πραγματικού συστήματος, βασισμένου στην προτεινόμενη αρχιτεκτονική
e. Σχεδιασμός υλοποίησης της προτεινόμενης αρχιτεκτονικής, βασισμένος σε διαδεδομένα υπάρχοντα προγράμματα-λύσεις.
f. Υλοποίηση πειραματικού συστήματος, που υποστηρίζει υποσύνολο της λειτουργικότητας του συστήματος προστασίας των προσωπικών δεδομένων

1.3 Οργάνωση κειμένου

Στο κεφάλαιο 2 περιγράφεται το υπάρχον περιβάλλον λειτουργίας των συστημάτων παροχής υπηρεσιών διαδικτυακής τηλεφωνίας με αναφορές στη σχετική νομοθεσία, που διέπει τη λειτουργία τους. Ταυτόχρονα, επισημαίνονται και αναλύονται τα κενά που παρουσιάζουν τα συγκεκριμένα συστήματα, σε σχέση με την προστασία της ιδιωτικότητας των πελατών τους. Η προτεινόμενη αρχιτεκτονική, για την επίλυση του προβλήματος, περιγράφεται στο κεφάλαιο 3 με ιδιαίτερη έμφαση στους σχεδιαστικούς άξονες, που τέθηκαν

και στη λειτουργικότητα που πρέπει να επιτευχθεί από το τελικό σύστημα. Το κεφάλαιο 4 περιέχει τις προδιαγραφές απαιτήσεων του συστήματος εκφρασμένες με τη βοήθεια της γλώσσας UML σε μια πρότυπη μορφή, ενώ το κεφάλαιο 5 αναφέρεται στο σχεδιασμό της υλοποίησης της προτεινόμενης αρχιτεκτονικής, βασιζόμενο σε υπάρχοντες πλατφόρμες. Ταυτόχρονα υποσυστήματα απαραίτητα για την επίτευξη των βασικών στόχων για τα οποία δεν υπάρχουν γνωστές λύσεις μοντελοποιούνται και σχεδιάζονται εξ αρχής. Στο κεφάλαιο 6 παρουσιάζεται η υλοποίηση ενός πειραματικού συστήματος που υποστηρίζει υποσύνολο της λειτουργικότητας του συστήματος προστασίας των προσωπικών δεδομένων και στο κεφ.7 παρουσιάζονται τα αποτελέσματα της λειτουργίας του με βάση κάποια παραδείγματα. Τέλος, στο κεφάλαιο 8 συνοψίζονται τα αποτελέσματα της διπλωματικής, παρουσιάζονται τα συμπεράσματα και προτείνονται επεκτάσεις του προτεινομένου συστήματος για μελλοντική ερευνητική δραστηριότητα, ενώ στο κεφάλαιο 9 παρουσιάζεται η λίστα βιβλιογραφικών αναφορών της παρούσας διπλωματικής εργασίας.

2

Το περιβάλλον της διαδικτυακής τηλεφωνίας

Η διασφάλιση των προσωπικών δεδομένων και της ιδιωτικότητας των χρηστών είναι επιτακτικότερη από ποτέ στο περιβάλλον της διαδικτυακής τηλεφωνίας, καθώς από τη φύση της η συγκεκριμένη υπηρεσία αξιοποιεί και συλλέγει μεγαλύτερο αριθμό προσωπικών δεδομένων ακόμα και σε σχέση με την παραδοσιακή τηλεφωνία. Στην παραδοσιακή τηλεφωνία ο κάθε συνδρομητής ύστερα από αίτηση στον τηλεπικοινωνιακό οργανισμό αποκτά μια σταθερή γραμμή από το τηλεφωνικό κέντρο προς το σπίτι του, μέσω της οποίας προσφέρεται η υπηρεσία. Η γραμμή αυτή συνδέεται μ' έναν τηλεφωνικό αριθμό, μέσω του οποίου γίνονται οι τηλεφωνικές κλήσεις και ο οποίος αντιστοιχεί τις περισσότερες φορές σ' ένα συγκεκριμένο τερματικό (εκτός από περιπτώσεις ISDN και ειδικών τηλεφωνικών κέντρων). Η αλλαγή τόσο του καταχωρημένου ιδιοκτήτη της γραμμής, όσο και του τηλεφωνικού αριθμού δεν μπορεί να γίνει άμεσα, χωρίς χρονοβόρες διαδικασίες και αρκετά πιστοποιητικά. Έτσι, η υπηρεσία είναι απόλυτα συνδεδεμένη με τη γραμμή, τον τηλεφωνικό αριθμό και τελικά το χώρο στον οποίο παρέχεται η υπηρεσία. Αντίθετα, στη διαδικτυακή τηλεφωνία η παρεχόμενη υπηρεσία δεν συνδέεται με την τοποθεσία ή το τερματικό, αλλά υποστηρίζεται η κινητικότητα χρήστη. Αυτό σημαίνει τόσο ότι ο χρήστης μπορεί να χρησιμοποιήσει τα στοιχεία ταυτοποίησής του σε οποιοδήποτε τερματικό θέλει και να λάβει εκεί την παρεχόμενη υπηρεσία, όσο και το ότι πολλοί χρήστες μπορούν να χρησιμοποιούν το ίδιο τερματικό την ίδια στιγμή. Στην παραδοσιακή τηλεφωνία μπορεί κάποιος να έχει ένα επίπεδο ανωνυμίας, χρησιμοποιώντας κάποιο από τα δημόσια τηλέφωνα, κάτι όμως που δεν είναι δυνατόν για την τηλεφωνία VoIP. Από τα παραπάνω καταλαβαίνουμε ότι η υπηρεσία της διαδικτυακής τηλεφωνίας είναι συνδεδεμένη με το χρήστη σαν άτομο και όχι με την τοποθεσία στην οποία βρίσκεται (π.χ. σπίτι ή εργασία) και καθιστά σημαντικότερη την προστασία της ιδιωτικότητας του. Η λίστα τηλεφωνικών κλήσεων VoIP δεν αποκαλύπτει πια επικοινωνία μεταξύ δύο αριθμών, αλλά ταυτοποιεί απόλυτα τους ανθρώπους που συνδιαλέγονται. Μ' αυτό τον τρόπο ένας κακόβουλος χρήστης ή η εταιρεία παροχής της υπηρεσίας και οι υπάλληλοι της θα μπορούσαν να εξάγουν σίγουρα συμπεράσματα για τις

συνήθειες των χρηστών και τις κοινωνικές τους συναναστροφές, που στην παραδοσιακή τηλεφωνία θα είχαν σημαντικό βαθμό αβεβαιότητας.

Η πιο στενή σύνδεση της υπηρεσίας της διαδικτυακής τηλεφωνίας με το χρήστη σαν άτομο γίνεται πιο αντιληπτή, αν λάβουμε υπόψη ότι ο χρήστης κατά τη συνδρομή του στην υπηρεσία δημιουργεί ένα προσωπικό προφίλ με τα στοιχεία του. Τα στοιχεία, που θα αποθηκεύσει στο προφίλ του, εξαρτώνται τόσο από την παρεχόμενη από την εταιρεία υπηρεσία, όσο και από τις προτιμήσεις του χρήστη. Είναι πολύ πιθανό η εταιρεία να συνδυάζει την υπηρεσία της διαδικτυακής τηλεφωνίας μ' αυτήν της κοινωνικής δικτύωσης, αξιοποιώντας και επεκτείνοντας τα προφίλ χρηστών, που έχει στη διάθεσή της, για να προσφέρει μια πιο ολοκληρωμένη υπηρεσία. Σ' αυτήν την περίπτωση στο προφίλ του χρήστη μπορεί να αποθηκευτεί οτιδήποτε επιλέξει ο ίδιος από τη λίστα φραγμένων εισερχομένων κλήσεων, μέχρι φωτογραφίες από τις διακοπές του. Αν δεν υπάρχει πρόβλεψη για προστασία της ιδιωτικότητας του χρήστη τόσο σε επίπεδο privacy policy, όσο και σε τεχνικό σχεδιασμό, αρκεί κάποιος να γνωρίζει το όνομα του χρήστη για να μπορέσει να έχει πρόσβαση σ' όλα αυτά τα προσωπικά δεδομένα. Ένας κακόβουλος χρήστης μπορεί πολύ εύκολα με μια αναζήτηση να μάθει ένα πλήθος προσωπικών στοιχείων που δεν εξαντλούνται απλά στο φύλο, την ηλικία και την οικογενειακή κατάσταση.

Το VoIP παρέχει σε τεχνικοοικονομικό επίπεδο πολλά πλεονεκτήματα κάτι που αντικατοπτρίζεται στη δημιουργία νέων εταιρειών και στην ταχύτατη ανάπτυξη του κλάδου. Η υλοποίηση ενός δικτύου διαδικτυακής τηλεφωνίας απαιτεί σημαντικά λιγότερους πόρους και επένδυση σε υποδομή, σε σχέση με την εγκατάσταση ενός νέου δικτύου παραδοσιακής τηλεφωνίας. Επίσης, όπως περιγράψαμε, μπορεί να συνδυασθεί με την παροχή άλλων υπηρεσιών και εν γένει παρέχει υψηλότερο επίπεδο ασφαλείας στους χρήστες απέναντι σε πιθανές υποκλοπές, λόγω της διαδεδομένης χρήσης ισχυρών μεθόδων κρυπτογράφησης. Το αυξημένο κόστος τερματικού εξοπλισμού είναι παράγοντας ήσσονος σημασίας καθώς με τη μαζική παραγωγή συρρικνώνεται.

Εξάγεται λοιπόν το συμπέρασμα ότι στο κοντινό μέλλον οι υπηρεσίες διαδικτυακής τηλεφωνίας θα εκτοπίσουν σε μεγάλο βαθμό, αν δεν αντικαταστήσουν πλήρως, τις υπηρεσίες παραδοσιακής τηλεφωνίας. Το γεγονός αυτό σε συνδυασμό με την ψευδαίσθηση που έχουν οι χρήστες ότι η υψηλή ασφάλεια, που προσφέρεται, προστατεύει και την ιδιωτικότητα τους, αναδεικνύει την ανάγκη η προστασία της ιδιωτικότητας του χρήστη υπηρεσιών διαδικτυακής τηλεφωνίας να είναι κρίσιμη παράμετρος στη σχεδίαση τόσο της αρχιτεκτονικής του συστήματος, όσο και του μοντέλου λειτουργίας της εταιρείας παροχής της υπηρεσίας.

2.1 Νομοθεσία

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ [8] υιοθετήθηκε τον Οκτώβριο του 1995 και αποτέλεσε την πρώτη προσπάθεια για την εγκαθίδρυση ενός κοινού νομοθετικού πλαισίου με στόχο την αναγνώριση της προστασίας της ιδιωτικότητας στα ανερχόμενα τότε νέα μέσα επικοινωνιών. Ταυτόχρονα, η ευρωπαϊκή οδηγία προσπάθησε να καθιερώσει ένα ελάχιστο κοινό πρότυπο για την προστασία της ιδιωτικότητας, αποσκοπώντας στην αποτροπή τυχόν προβλημάτων στην ελεύθερη ροή πληροφοριών μεταξύ των μελών της, λόγω της διαφορετικής αντιμετώπισης της εννοίας της ιδιωτικότητας από τα κράτη-μέλη. Διαφορές στην υλοποίηση της προστασίας της ιδιωτικότητας μεταξύ των μελών μπορεί να αποτελέσουν τροχοπέδη στην υλοποίηση της ενοποιημένης ευρωπαϊκής αγοράς, αφού η διασυνοριακή μεταφορά συγκεκριμένων πληροφοριών μπορεί να απαγορευτεί. Παρ' όλα αυτά η Ευρώπη, ως

παραδοσιακός προμαχώνας του αγώνα για τα ανθρώπινα δικαιώματα, έθεσε τον πήχη ψηλά, όσον αφορά στο παρεχόμενο επίπεδο προστασίας. Η Οδηγία χρησιμοποιεί επιμέρους διαδικασίες και νομοθεσίες όλων των κρατών-μελών για να ορίσει ένα αυστηρό πλαίσιο στο οποίο θα πρέπει να κινούνται όλες οι νομοθεσίες των μελών. Στα επιμέρους κεφάλαια της Οδηγίας αναλύεται το πλαίσιο αρχών, θεωρήσεων, κανόνων, λειτουργιών, διαδικασιών, ευθυνών, αλλά και των ποινών που θα πρέπει να διέπουν την «ολική ή μερική επεξεργασία των προσωπικών δεδομένων με αυτοματοποιημένο, ή με οποιοιδήποτε άλλο τρόπο και τα οποία πρόκειται να συμπεριληφθούν σε κάποιο αρχείο». Ταυτόχρονα, προβλέπεται η εξαίρεση από την Οδηγία των διαδικασιών που εμπίπτουν στην κατηγορία των «διαδικασιών επεξεργασίας προσωπικών δεδομένων, που αφορούν στους τομείς δημόσιας ασφάλειας, άμυνας, κρατικής ασφάλειας και των ενεργειών της πολιτείας στον τομέα της εφαρμογής της ποινικής νομοθεσίας», ενώ καθορίζεται και το πλαίσιο κάτω από το οποίο επιτρέπεται η μεταφορά ευαίσθητων δεδομένων σε τρίτες χώρες. Σύμφωνα πάντα με τη συγκεκριμένη Οδηγία ορίζονται τα παρακάτω ατομικά δικαιώματα σε σχέση με τα προσωπικά δεδομένα, που τον αφορούν:

- Δικαίωμα ενημέρωσης: Καλύπτει την περίπτωση συλλογής δεδομένων τόσο από το ίδιο το πρόσωπο στο οποίο αναφέρονται, όσο και την περίπτωση που τα συγκεκριμένα δεδομένα συλλέγονται από τρίτο.
- Δικαίωμα πρόσβασης: Θεμελιώνει το δικαίωμα του ατόμου να έρθει σε επαφή με τον υπεύθυνο επεξεργασίας των δεδομένων και να ενημερωθεί για τον τρόπο επεξεργασίας και τη χρήση των πληροφοριών.
- Δικαίωμα αντίταξης: Θεμελιώνει το δικαίωμα του ατόμου να αρνηθεί την επεξεργασία των δεδομένων που τον αφορούν.

Τέλος, οι επεξεργασία, μεταφορά και αποθήκευση της πληροφορίας από τους αποδέκτες της θα πρέπει να γίνεται με τέτοιο τρόπο, ώστε να αποφευχθεί πιθανή απώλεια, αλλοίωση, απαγορευμένη πρόσβαση ή καταστροφή της.

Δύο χρόνια αργότερα (1997) η Ευρωπαϊκή Οδηγία για τις Τηλεπικοινωνίες [9] έθεσε το πλαίσιο λειτουργίας των παρόχων τηλεπικοινωνιακών υπηρεσιών, καθώς και τις υποχρεώσεις τους απέναντι στην προστασία των προσωπικών δεδομένων των πελατών τους. Οι νέοι κανόνες περιόρισαν σημαντικά τις επιχειρηματικές ενέργειες προώθησης προϊόντων που παραβίαζαν την ιδιωτικότητα των πελατών, την πρόσβαση σε πληροφορίες χρώσεων, ενώ δηλώθηκε ρητά ότι πληροφορία, που συλλέγεται κατά την διάρκεια της επικοινωνίας, θα πρέπει να καταστρέφεται με το πέρας της κλήσης. Οι παραπάνω οδηγίες έθεσαν το πλαίσιο λειτουργίας σε γενικό επίπεδο, όμως η ραγδαία ανάπτυξη των σχετικών κλάδων έκανε επιτακτική την ανάγκη για συμπληρωματικές οδηγίες με πιο συγκεκριμένα πλαίσια.

Η Οδηγία 2002/58/ΕΚ αναφέρεται στην προστασία της ιδιωτικότητας στο χώρο των ηλεκτρονικών επικοινωνιών και έχει ως στόχο την εφαρμογή του πλαισίου της Ε.Ε. στο συγκεκριμένο νευραλγικό χώρο ώστε, ταυτόχρονα με την προστασία της ιδιωτικότητας, να επιτυγχάνεται η ελεύθερη κυκλοφορία των πληροφοριών στα νέα δημόσια δίκτυα επικοινωνιών της Ένωσης προς όφελος της ενοποιημένης αγοράς. Επίσης, για πρώτη φορά θεσμοθετείται η προστασία των έννομων συμφερόντων των προσώπων νομικού δικαίου. Η συγκεκριμένη οδηγία είναι πολύ σημαντική, αφού αφορά κυρίως στις υπηρεσίες τηλεφωνίας, μιας από τις πιο διαδεδομένες υπηρεσίες και σημείο σημαντικών παραβιάσεων της ιδιωτικότητας των πελατών. Στη συγκεκριμένη Οδηγία απαγορεύεται ρητά η ακρόαση, υποκλοπή, αποθήκευση και γενικά οι τρόποι παρακολούθησης χωρίς τη συγκατάθεση των χρηστών, ενώ ορίζονται ειδικές περιπτώσεις, όπου παρέχεται από την ανεξάρτητη δικαστική

εξουσία της κάθε χώρας άδεια για την εκτέλεση των παραπάνω ενεργειών. Σε άλλα άρθρα της Οδηγίας ορίζονται οι υποχρεώσεις των παρόχων υπηρεσιών σε σχέση με το χειρισμό των δεδομένων σηματοδοσίας μιας κλήσης και των συμπερασμάτων που απορρέουν από αυτή. (Για παράδειγμα επεξεργασία δεδομένων προώθησης κλήσης, φραγής κλήσης, αναγνώρισης κλήσης, καθώς και επεξεργασία δεδομένων θέσης).

Η τελευταία αναφορά στην ευρωπαϊκή νομοθεσία είναι η Οδηγία 2006/24/ΕΚ [10], η οποία αφορά στην διατήρηση των δεδομένων που παράγονται κατά τη διάρκεια παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών και δημοσίων δικτύων επικοινωνιών. Η συγκεκριμένη Οδηγία συμπληρώνει τη 2002/58/ΕΚ και εξασφαλίζει ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης και δίωξης ποινικών αδικημάτων. Σημαντικό στοιχείο της συγκεκριμένης Οδηγίας είναι ότι η εφαρμογή της επεκτείνεται σε δεδομένα κίνησης και θέσης και στα σχετικά δεδομένα που απαιτούνται για την αναγνώριση της πηγής, του προορισμού, του είδους, της ακριβής ώρας και της διάρκειας της επικοινωνίας καθώς και της θέσης και του εξοπλισμού που χρησιμοποιήθηκε από τα δύο μέλη. Η Οδηγία όμως δεν εφαρμόζεται με κανέναν τρόπο στο περιεχόμενο της επικοινωνίας αφού το κανάλι δεδομένων δεν πρέπει να αποθηκεύεται σε κανένα σημείο της επικοινωνίας. Τέλος, ορίζεται η διάρκεια διατήρησης των συγκεκριμένων δεδομένων κατ' ελάχιστο για ένα εξάμηνο και κατά το μέγιστο για δύο χρόνια από την ημερομηνία τέλεσης της επικοινωνίας. Τα κράτη-μέλη της Ε.Ε. είναι υποχρεωμένα να δημιουργήσουν ανεξάρτητες αρχές που θα ασχολούνται με τη διασφάλιση των συγκεκριμένων πληροφοριών.

Η Ελλάδα ως κράτος-μέλος της ΕΕ οφείλει να εφαρμόζει τους νόμους που ορίζει η ΕΕ, αλλά έχει υιοθετήσει επιπλέον κάποιες νομοθεσίες περί προστασίας δεδομένων προσωπικού χαρακτήρα. Οι νόμοι 2472/1997 [11] και 3471/2006 [12] διέπουν την ελληνική επικράτεια και υλοποιούν τις σχετικές οδηγίες της Ε.Ε. Οι νόμοι αυτοί, μεταξύ άλλων ορίζουν ότι για να θεωρείται νόμιμη η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να συλλέγονται με θεμιτό τρόπο και για προκαθορισμένους, σαφείς και νόμιμους σκοπούς. Θα πρέπει η επεξεργασία, στην οποία υποβάλλονται τα δεδομένα να είναι ακριβής, και να μην οδηγεί σε συμπεράσματα πέραν του αρχικού σκοπού, ενώ η διατήρηση τους πέραν της προβλεπόμενης διάρκειας θα πρέπει να εγκρίνεται από ανεξάρτητη αρχή και μόνο για επιστημονικούς, ιστορικούς και στατιστικούς λόγους εφόσον δεν θίγονται τα δικαιώματα των αναφερόμενων ατόμων. Γενικά, η επεξεργασία επιτρέπεται μόνο όταν το άτομο έχει δώσει τη ρητή συγκατάθεση του, εκτός από τις ειδικές περιπτώσεις που προβλέπει και η ευρωπαϊκή Οδηγία, ενώ σε κάθε περίπτωση για την εκτέλεση οποιασδήποτε επεξεργασίας θα πρέπει να υπάρχει σχετική άδεια από την ανεξάρτητη αρχή και να ακολουθούνται αυστηρές διαδικασίες, που θα διασφαλίζουν το αδιάβλητο και θα προστατεύουν τα ευαίσθητα δεδομένα. Η ελληνική νομοθεσία ορίζει και προστατεύει τα τρία ατομικά δικαιώματα που ορίζονται στην ευρωπαϊκή νομοθεσία και προσθέτει σ' αυτά το δικαίωμα της προσωρινής δικαστικής προστασίας, σύμφωνα με το οποίο κάθε άτομο έχει το δικαίωμα να αναστείλει την εφαρμογή μιας πράξης επεξεργασίας προσωπικών δεδομένων που τον θίγει.

Τέλος ο νόμος 3471/2006 υλοποιεί τις αντίστοιχες διατάξεις της ευρωπαϊκής Οδηγίας 2006/24/ΕΚ για την εγκαθίδρυση και διασφάλιση του απορρήτου των επικοινωνιών. Η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης επιτρέπεται μόνο κατά τη διάρκεια νόμιμων επαγγελματικών συναλλαγών με σκοπό την παροχή αποδεικτικών στοιχείων για την πραγματοποίηση αυτών και μόνο υπό την προϋπόθεση ότι και τα δύο μέρη συναινούν σ' αυτή. Τα δεδομένα κίνησης, που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από το φορέα παροχής δικτύου, θα πρέπει

να καταστρέφονται ή να καθίστανται ανώνυμα με τη λήξη της επικοινωνίας χρησιμοποιώντας κατάλληλη κωδικοποίηση. Επίσης, αξίζει να αναφερθεί το παρακάτω τμήμα τη νομοθεσίας: οι πάροχοι ηλεκτρονικών υπηρεσιών είναι υποχρεωμένοι να λάβουν όλα τα απαραίτητα τεχνικά μέτρα για την προστασία της ασφάλειας του δικτύου τους και των προσωπικών δεδομένων των πελατών τους. Σύμφωνα όμως με τη νομοθεσία οι διαδικασίες ασφαλείας πρέπει να παρέχουν προστασία ανάλογου επιπέδου με τον κίνδυνο και εγκαθιδρύονται λαμβάνοντας υπόψη τις πιο πρόσφατες τεχνολογικές δυνατότητες καθώς και το κόστος εφαρμογής τους.

2.2 Επιχειρηματικό μοντέλο λειτουργίας εταιρείας παροχής υπηρεσιών VoIP

΄ Στην παρούσα εργασία θα εξεταστούν τα ζητήματα προστασίας προσωπικών δεδομένων που εγείρονται στο περιβάλλον της διαδικτυακής τηλεφωνίας μέσω της μελέτης της λειτουργίας μιας υποθετικής εταιρείας παροχής τέτοιων υπηρεσιών. Η εταιρεία παροχής υπηρεσιών στην παρούσα φάση βασίζεται στο παρακάτω επιχειρηματικό μοντέλο:

I. Υλοποίηση της αρχιτεκτονικής του πρωτοκόλλου SIP για τη διεκπεραίωση τηλεφωνικών κλήσεων VoIP με δυνατότητα χρέωσης ανά λεπτό ή με χρήση πακέτων ομιλίας.
II. Χρήση της υποδομής SIP για υλοποίηση επιπλέον υπηρεσιών με τους ίδιους όρους χρέωσης, όπως είναι η ανταλλαγή σύντομων μηνυμάτων και οι υπηρεσίες κινητικότητας και παρουσίας
III. Ύπαρξη διαδικτυακής πύλης (Portal) για την υλοποίηση συμπληρωματικών υπηρεσιών, όπως εγγραφή στις υπηρεσίες της εταιρείας, διαχείριση προσωπικού, προφίλ χρήστη και προβολή διαφημίσεων.
IV. Πώληση χρήσιμων στατιστικών στοιχείων πελατολογίου σε ενδιαφερόμενες τρίτες εταιρίες.

Το παραπάνω επιχειρηματικό μοντέλο παραβιάζει τα προσωπικά στοιχεία των πελατών της εταιρείας σε πολλές περιπτώσεις. Συγκεκριμένα:

A. Η διεκπεραίωση των τηλεφωνικών κλήσεων στην παραδοσιακή αρχιτεκτονική ενός συστήματος SIP εκθέτει πληροφορίες για τα πρόσωπα που επικοινωνούν και τη διάρκεια της επικοινωνίας τους τόσο στην εταιρεία, όσο και σε τρίτους. Οι τελευταίοι έχουν τη δυνατότητα να παρακολουθούν τη μεταφερόμενη κίνηση στο δίκτυο, αφού τα μηνύματα σηματοδοσίας του SIP είναι γραμμένα σε απλό κείμενο (στα πρότυπα του HTTP) και το ίδιο το πρωτόκολλο δεν παρέχει καμία εγγύηση για το κανάλι σηματοδοσίας του. Για το κανάλι δεδομένων υπάρχει κίνδυνος για τα προσωπικά δεδομένα μόνο από παρεμβολή τρίτων καθώς αυτό εγκαθιδρύεται απευθείας μεταξύ των δύο χρηστών και δεν παρεμβάλλεται σ' αυτό η εταιρεία παροχής της υπηρεσίας.
B. Για την κατηγορία των συμπληρωματικών υπηρεσιών SIP ισχύουν αντίστοιχες συνθήκες με τη διαφορά ότι και το περιεχόμενο των συντόμων μηνυμάτων, αλλά και οι πληροφορίες παρουσίας εκτίθενται στην εταιρεία, λόγω της φύσης της υλοποίησης του SIP για μεταφορά αυτών των πληροφοριών. (Περισσότερες λεπτομέρειες για την αρχιτεκτονική του SIP, που χρησιμοποιεί η εταιρεία και για τις παραβιάσεις της ιδιωτικότητας στη αρχιτεκτονική αυτή, ακολουθούν σε επόμενες παραγράφους).

C. Τα προσωπικά προφίλ των χρηστών περιέχουν πληροφορίες ταυτοποίησης του χρήστη και χρησιμοποιούνται εκτός από την παροχή υπηρεσιών και για τις απαραίτητες λειτουργίες της εταιρείας όπως η χρέωση. Η διαχείριση αυτών των στοιχείων, μέσω της διαδικτυακής πύλης της εταιρείας, της επιτρέπει πλήρη πρόσβαση σ' αυτά.
D. Η συλλογή όλων των πληροφοριών στους διακομιστές της εταιρείας της δίνει τη δυνατότητα να τις επεξεργάζεται, να δημοσιεύει και να εμπορεύεται τα αποτελέσματα κατά το συμφέρον της, ανεξάρτητα από τις επιθυμίες των χρηστών.

2.3 Το Πρωτόκολλο SIP

Στο σημείο αυτό κρίνεται σκόπιμη μια συνοπτική παρουσίαση του πρωτοκόλλου SIP, της αρχιτεκτονικής του και των δομικών μονάδων του [13].

2.3.1 Γενικά

Το πρωτόκολλο SIP, το οποίο στην ανανεωμένη έκδοση του ορίζεται πλήρως στο RFC 3261 [14], αποτελεί ένα πρωτόκολλο σηματοδοσίας, το οποίο μπορεί να χρησιμοποιηθεί για την εγκαθίδρυση συνόδων πολυμέσων στο περιβάλλον των δικτύων υπολογιστών, όπως αυτό ορίζεται με τη χρήση του πρωτοκόλλου IP. Σε αντίθεση, η παραδοσιακή τηλεφωνία χρησιμοποιεί άλλα πρωτόκολλα σηματοδοσίας, όπως τα SS7 και H.32x. Το SIP αποτελεί ένα πρωτόκολλο επιπέδου εφαρμογής στη στοίβα πρωτοκόλλων, αφού χρησιμοποιεί τις υπηρεσίες των πρωτοκόλλων μεταφοράς UDP ή TCP για να μεταφέρει τα μηνύματα του και διαχειρίζεται έννοιες υψηλότερου επιπέδου από το επίπεδο μεταφοράς, όπως αναζήτηση χρηστών, κωδικοποίηση ήχου κ.τ.λ.

Οι κύριες λειτουργίες σηματοδοσίας που επιτελεί το SIP είναι οι παρακάτω:

- Δημιουργία αιτημάτων εγκαθίδρυσης συνόδου πολυμέσων.
- Εύρεση τελικού αποδέκτη αιτήματος
- Επικοινωνία με τελικό αποδέκτη για την αποδοχή ή απόρριψη του αιτήματος συνόδου
- Ανταλλαγή πληροφοριών για το είδος της συνόδου πολυμέσων
- Τροποποίηση εγκατεστημένων συνόδων
- Τερματισμός εγκατεστημένων συνόδων

Ταυτόχρονα σε άλλα RFC [15]-[19] έχουν προταθεί επεκτάσεις του για την ενσωμάτωση περαιτέρω λειτουργιών όπως:

- Δημοσιοποίηση πληροφορίας παρουσίας (presence information) [18]
- Διακίνηση πληροφορίας παρουσίας
- Ενημέρωση από την πλευρά του δικτύου για σημαντικά γεγονότα (Events notification) [15]
- Μεταφορά σύντομων μηνυμάτων [16]

Το SIP είναι ένα πρωτόκολλο που βασίζεται σε μηνύματα κειμένου με συγκεκριμένη δομή, η οποία περιλαμβάνει: επικεφαλίδα επιλογών (header) και κυρίως σώμα μηνύματος (body) στα πρότυπα του HTTP, ενώ δανείζεται και στοιχεία από το SMTP , όπως τις επικεφαλίδες: To, From, Date, Subject. Επίσης ως προς την ονοματολογία που χρησιμοποίει δανείζεται τη χρήση των ενοποιημένων δεικτών πόρων (uniform resource identifier URI) και των ενοποιημένων δεικτών θέσεων πόρων (uniform resource locators URL) από το HTTP, ενώ δανείζεται από το SMTP τη χρήση των διευθύνσεων ταχυδρομείου (username@domain) για την ανεύρεση των χρηστών.

Οι διευθύνσεις SIP ονομάζονται SIP URI (με μορφή <sip: username@domain>) και τελικά μετατρέπονται στις τελικές διευθύνσεις IP των παραληπτών μέσω χρησιμοποίησης ενδιάμεσων διακομιστών(proxy servers) και DNS αναζητήσεων, όπου γίνεται χρήση των εγγραφών SRV του DNS. Τα SIP URI χωρίζονται σε δύο κατηγορίες:

- User URI ή (Address of Record AOR): Αποτελούν το αποκλειστικό όνομα χρήστη στα πρότυπα των διευθύνσεων ηλεκτρονικού ταχυδρομείου.
- Device URI: Αποτελούν αποκλειστικό όνομα μιας συσκευής SIP (User Agent UA). Οι συσκευές αυτές συνδέονται με κάποιο User URI για περιορισμένο χρονικό διάστημα σε ειδικούς διακομιστές του συστήματος.

Εκτός από τις παραπάνω κατηγορίες, που αφορούν τις διευθύνσεις SIP για δίκτυα IP, υπάρχουν τυποποιήσεις του SIP για υποστήριξη τηλεφωνικών αριθμών (με μορφή <tel: number>), που χρησιμοποιούνται για επικοινωνία του SIP μέσω ειδικών πυλών με το παραδοσιακό σύστημα τηλεφωνίας. Επίσης, ορίζονται URI που καθορίζουν στο DNS μηχανήματα, τα οποία χρησιμοποιούνται για την υλοποίηση υπηρεσιών παρουσίας (με μορφή <pres: username@domain>) και μεταφοράς άμεσων μηνυμάτων (με μορφή <im: username@domain>)

Για το SIP το διαδίκτυο χωρίζεται σε διαχειριστικές οντότητες (domains), οι οποίες έχουν την ευθύνη για ένα συγκεκριμένο domain και για όλους τους χρήστες που λαμβάνουν υπηρεσίες απ' αυτό. Οι χρήστες χρησιμοποιούν μοναδικά username ανά πάροχο, με αποτέλεσμα να δημιουργούνται παγκοσμίως μοναδικά User URI ενώ για τη λήψη υπηρεσιών εισέρχονται σ' αυτές τις διαχειριστικές οντότητες. Η δρομολόγηση των μηνυμάτων βασίζεται στο δέντρο διευθύνσεων του DNS (γίνεται χρήση των εγγραφών του DNS SRV) για να φθάσει το μήνυμα στην τελική διαχειριστική οντότητα, η οποία είναι αυτή που θα το προωθήσει στον παραλήπτη ή θα απαντήσει κατάλληλα στον αποστολέα.

2.3.2 Μηνύματα SIP

Στο SIP ορίζονται δύο γενικές κατηγορίες μηνυμάτων:

- Μηνύματα-αιτήσεις (Request messages): Είναι μηνύματα που παράγονται για να επιτελέσουν μια συγκεκριμένη λειτουργία.
- Μηνύματα-απαντήσεις (Response messages): Είναι μηνύματα που παράγονται ως απάντηση σε κάποιο μήνυμα-αίτηση .

Στο RFC 3261 ορίζονται τα παρακάτω βασικά μηνύματα-αιτήσεις, οι παρακάτω κατηγορίες μηνυμάτων-απαντήσεων, ενώ περιέχεται και η αναλυτική περιγραφή της χρήσης των μηνυμάτων αυτών από τις δομικές μονάδες του SIP ανάλογα με τις συνθήκες και τις επιθυμητές λειτουργίες.

Μηνύματα-αιτήσεις :

- INVITE : Μήνυμα-αίτηση εγκαθίδρυσης συνόδου
- REGISTER: Μήνυμα-αίτηση εισόδου στο σύστημα
- BYE: Μήνυμα-αίτηση τερματισμού συνόδου
- ACK: Μήνυμα-αίτηση τελικής γνωστοποίησης παραλαβής μηνύματος-απάντησης σε αίτηση εγκαθίδρυσης συνόδου, το οποίο και ολοκληρώνει την τριπλή χειραψία. Όλα τα υπόλοιπα μηνύματα-απαντήσεις δεν επιβεβαιώνονται εκτός αν χρησιμοποιηθεί το PRACK, όπως θα δούμε παρακάτω
- CANCEL: Μήνυμα-αίτηση ακύρωσης του προηγούμενου μηνύματος-αίτησης
- OPTIONS: Μήνυμα μεταφοράς πληροφοριών στο δίκτυο

Μηνύματα-αιτήσεις για συμπληρωματικές υπηρεσίες εκτός RFC 3261:

- SUBSCRIBE: Μήνυμα-αίτηση εγγραφής σε κάποιον διακομιστή παρουσίας (Presence Agent PA), έτσι ώστε ο αποστολέας να ειδοποιηθεί για συγκεκριμένα γεγονότα (Events). Χρησιμοποιείται από διακομιστές και χρήστες για την υλοποίηση υπηρεσιών παρουσίας [15].
- NOTIFY: Μήνυμα μεταφοράς πληροφορίας στο δίκτυο ως αποτέλεσμα ενός γεγονότος. Χρησιμοποιείται ως απάντηση σε κάποιο μήνυμα SUBSCRIBE [15].
- MESSAGE: Μήνυμα αίτηση μεταφοράς σύντομου μηνύματος (instant message IM) στο δίκτυο. Μπορούν να σταλούν ανεξάρτητα ή ως μέρος μιας εγκατεστημένης συνόδου [16].
- PUBLISH: Μήνυμα-αίτηση γνωστοποίησης πληροφοριών παρουσίας σε κάποιον διακομιστή παρουσίας [18]
- PRACK: Μήνυμα-αίτηση γνωστοποίησης παραλαβής μηνύματος-απάντησης. Χρησιμοποιείται για την υλοποίηση αξιόπιστης μεταφοράς μηνυμάτων στο επίπεδο του SIP, όταν χρησιμοποιείται αναξιόπιστο πρωτόκολλο μεταφοράς [17].
- INFO: Μήνυμα-αίτηση αλλαγής παραμέτρων του καναλιού σηματοδοσίας σε μια εγκατεστημένη σύνοδο. (Οι παράμετροι του καναλιού δεδομένων αλλάζουν μόνο με ένα INVITE (re-INVITE) μήνυμα).
- UPDATE: Μήνυμα-αίτηση αλλαγής παραμέτρων σε μια σύνοδο που εκκρεμεί. (Δηλαδή έχει σταλεί το μήνυμα INVITE αλλά όχι το μήνυμα ACK) [19].

Μηνύματα-απάντησεις:

- 1xx Informational : Κατηγορία που περιέχει τα μηνύματα πληροφόρησης χρήστη για την κατάσταση ενός αιτήματος του πριν την ολοκλήρωση του.
- 2xx Success : Κατηγορία που περιέχει τα μηνύματα πληροφόρησης για την επιτυχία ενός αιτήματος.
- 3xx Redirection: Κατηγορία που περιέχει τα μηνύματα ανακατεύθυνσης ενός αιτήματος.
- 4xx Client Error: Κατηγορία που περιέχει τα μηνύματα πληροφόρησης σφάλματος στην πλευρά του πελάτη.
- 5xx Server Error: Κατηγορία που περιέχει τα μηνύματα πληροφόρησης σφάλματος στην πλευρά του διακομιστή.
- 6xx Global Error: Κατηγορία που περιέχει τα μηνύματα πληροφόρησης σφάλματος στο δίκτυο.

Η δομή ενός τυπικού μηνύματος SIP με τις επικεφαλίδες και το σώμα του μηνύματος φαίνεται παρακάτω :

```
INVITE sip:marconi@radio.org SIP/2.0
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
Max-Forwards: 70
To: G. Marconi <sip:Marconi@radio.org>
From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
Call-ID: 123456789@lab.high-voltage.org
CSeq: 1 INVITE
Subject: About That Power Outage...
Contact: <sip:n.tesla@lab.high-voltage.org>
Content-Type: application/sdp
Content-Length: 158

v=0
o=Tesla 2890844526 2890844526 IN IP4 lab.high-voltage.org
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Όπως παρατηρούμε ένα μήνυμα SIP ξεκινάει μ' ένα χαρακτηριστικό του είδους του μηνύματος (INVITE σ' αυτή την περίπτωση που έχουμε ένα μήνυμα-αίτηση) ή με κάποιον από τους κωδικούς μηνυμάτων, που ορίστηκαν παραπάνω (όταν έχουμε μήνυμα-απάντηση). Στη συνέχεια, ανάλογα με το είδος του μηνύματος ακολουθεί ένα URI που προσδιορίζει τον προορισμό ή το επόμενο βήμα προώθησης και στο τέλος υπάρχει το αναγνωριστικό της έκδοσης του SIP που χρησιμοποιείται. Ακολουθούν οι επικεφαλίδες επιλογών του μηνύματος με τις σημαντικότερες, οι οποίες είναι και υποχρεωτικές σε κάθε μήνυμα να είναι οι εξής:

i. Via: Περιέχει πληροφορίες για τις δομικές μονάδες SIP από τις οποίες διέρχεται το μήνυμα μέχρι να φτάσει στον προορισμό του και χρησιμοποιείται ώστε η απάντηση σε κάθε αίτημα να διέλθει από τις ίδιες δομικές μονάδες, οι οποίες πιθανότατα να κρατάνε κάποια πληροφορία για τη σύνοδο. Γι αυτό το λόγο εξάλλου κάθε δομική μονάδα εισάγει μια νέα γραμμή στην συγκεκριμένη επικεφαλίδα και χρησιμοποιεί την ετικέτα «branch», η οποία έχει μόνο τοπική σημασία, για να αναγνωρίζει τις απαντήσεις (responses) για κάθε συγκεκριμένο αίτημα (request) (γενικά προσδιορίζει τοπικά τις συναλλαγές) . Εκτός όμως από την ετικέτα και το όνομα(hostname)(ή διεύθυνση IP) της δομικής μονάδας SIP, περιλαμβάνεται και η πληροφορία της έκδοσης του SIP και του πρωτοκόλλου μεταφοράς, που χρησιμοποιεί η συγκεκριμένη δομική μονάδα.
ii. Max-Forwards: Το μέγιστο πλήθος αλμάτων που μπορεί να κάνει το μήνυμα μέχρι να φτάσει στον προορισμό του. Αποτρέπει ένα μήνυμα από το να περιφέρεται συνέχεια στο δίκτυο λόγο σφαλμάτων στη δρομολόγηση.
iii. To: Περιέχει το όνομα παραλήπτη και το SIP URI (αναγνωριστικό χρήστη) του σε παρενθέσεις, ενώ ταυτόχρονα περιέχει μια ετικέτα «tag», η οποία δημιουργείται στο πρώτο μήνυμα-απάντηση από τον παραλήπτη και χρησιμοποιείται μαζί με το Call-ID για το μοναδικό προσδιορισμό της συνόδου. Το SIP URI αυτής της επικεφαλίδας χρησιμοποιείται για τη δρομολόγηση του αιτήματος στον προορισμό.
iv. From: Περιέχει το όνομα αποστολέα και το SIP URI (αναγνωριστικό χρήστη) του σε παρενθέσεις. Επίσης περιέχει μια ετικέτα tag η οποία δημιουργείται από τον

αποστολέα στο αίτημα εγκαθίδρυσης της συνόδου και χρησιμοποιείται μαζί με το Call-ID για το μοναδικό προσδιορισμό της συνόδου

v. Call-ID: Είναι ένα αλφαριθμητικό που χρησιμοποιείται για τον προσδιορισμό μιας κλήσης, το οποίο παράγεται στο χρήστη που δημιουργεί την αίτηση και χρησιμοποιείται στη συνέχεια σε όλα τα SIP μηνύματα της συγκεκριμένης συνόδου. Συνήθως, χρησιμοποιείται η εξής μορφή: <Τυχαίο αλφ/τικό@όνομα-υπολογιστή> για να καταστήσει το συγκεκριμένο πεδίο παγκοσμίως μοναδικό. Μαζί με τις δύο ετικέτες «tag» στις επικεφαλίδες «From» και «To» αποτελούν το προσδιοριστικό της συνόδου.

vi. Cseq: Περιγράφει την αλληλουχία των μηνυμάτων για τη συγκεκριμένη σύνοδο

vii. Contact: Περιέχει το SIP URI (αναγνωριστικό μηχανήματος) του μηχανήματος επικοινωνίας του αποστολέα και μπορεί να χρησιμοποιηθεί για απευθείας επικοινωνία, όπως για παράδειγμα στο τρίτο βήμα της τριπλής χειραψίας της εγκαθίδρυσης συνόδου. Επίσης, χρησιμοποιείται σε περιπτώσεις που θέλουμε να παρακάμψουμε κάποιο τείχος προστασίας, δηλώνοντας ως διεύθυνση επιστροφής αυτή του proxy server ώστε να δρομολογηθεί σωστά η απάντηση.

viii. Content-Length: Προσδιορίζει τον αριθμό των οκτάδων στο σώμα του μηνύματος.

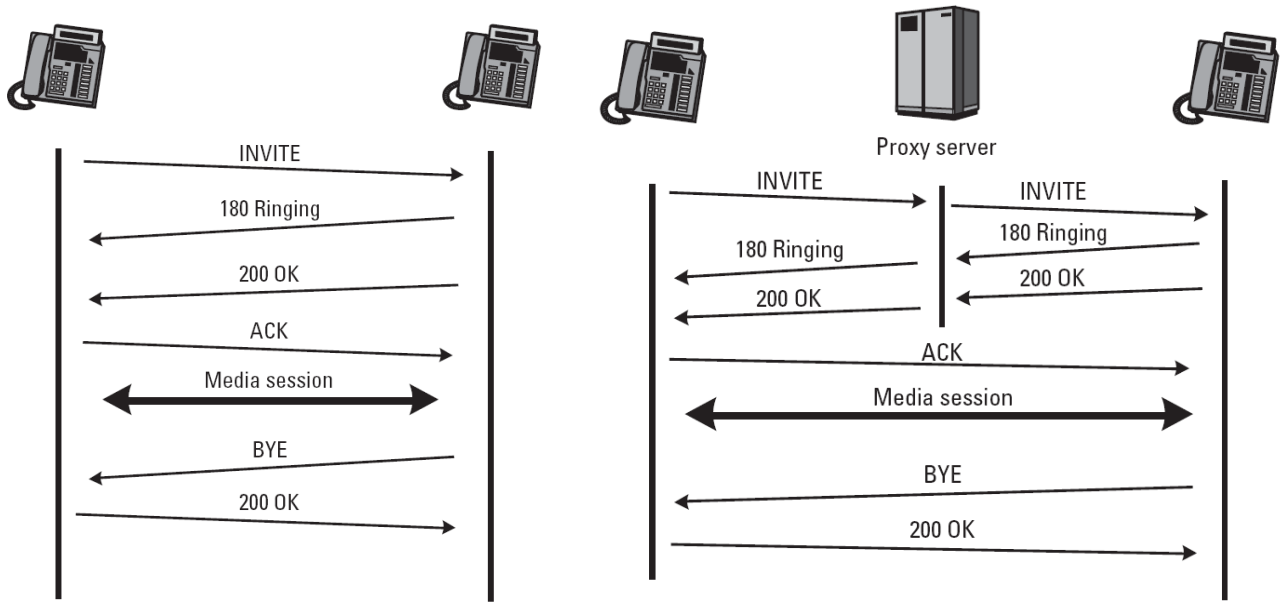
Εκτός από τις παραπάνω επικεφαλίδες, μπορούν να προστεθούν και άλλες, οι οποίες περιέχουν απαραίτητες πληροφορίες για άλλους τύπους μηνύματος ή γενικά χρήσιμες πρόσθετες πληροφορίες. Αυτές που μας απασχολούν, λόγω της παραβίασης των προσωπικών δεδομένων, είναι οι παρακάτω:

- Call – Info : Περιέχει ένα γενικό URI, το οποίο περιλαμβάνει πληροφορίες για την εγκαθίδρυση της συνόδου
- Event: Χρησιμοποιείται από τα μηνύματα-αιτήσεις SUBSCRIBE για την ειδοποίηση του αποστολέα μετά από συγκεκριμένα γεγονότα στην πλευρά του παραλήπτη και από τα NOTIFY και PUBLISH για να υποδείξει το γεγονός, το οποίο οδήγησε στην αποστολή του μηνύματος
- In –Reply – to: Χρησιμοποιείται για να συνδέσει μια τρέχουσα αίτηση εγκαθίδρυσης συνόδου με κάποια παλιότερη σύνοδο, η οποία μπορεί να διακόπηκε απότομα ή να μην παρελήφθη.
- Record-Route: Χρησιμοποιείται από ενδιάμεσους διακομιστές για να εξαναγκάσουν μελλοντικά μηνύματα στο κανάλι σηματοδοσίας να δρομολογηθούν μέσω αυτών. Χρησιμοποιείται και από ενδιάμεσους διακομιστές για την παράκαμψη ενός τείχους προστασίας.
- Reply-to: Χρησιμοποιείται όταν για κάποιο λόγο δεν μπορεί να συμπληρωθεί η επικεφαλίδα «From».
- Organization: Περιέχει το όνομα του οργανισμού από τον οποίο προέρχεται το μήνυμα και είτε χρησιμοποιείται για αποφάσεις δρομολόγησης, είτε χρησιμοποιείται από ενδιάμεσους διακομιστές κατά τη μεταφορά μηνυμάτων από το δίκτυο μιας διαχειριστικής οντότητας σε δίκτυο άλλης.
- Server: Περιέχει πληροφορίες για το μηχάνημα παραλήπτη, όπως πληροφορίες κατασκευαστή και έκδοση λογισμικού.
- Subject: Περιέχει το θέμα επικοινωνίας
- User- Agent: Περιέχει πληροφορίες για το μηχάνημα του αποστολέα μηνύματος, όπως πληροφορίες κατασκευαστή και έκδοση λογισμικού.
- Warning: Περιέχει επιπλέον πληροφορίες ανάλογα με τον κωδικό 1xx, 2xx, 3xx.

Τέλος, σε πολλά από τα μηνύματα-αιτήσεις και απαντήσεις, όπως και στο συγκεκριμένο μήνυμα-αίτηση εγκαθίδρυσης συνόδου του παραδείγματος, ακολουθούν επικεφαλίδες με πληροφορίες για το είδος των δεδομένων, που περιέχεται στο σώμα του μηνύματος, ενώ στο ίδιο το σώμα υπάρχουν περισσότερες λεπτομέρειες ανάλογα με τον τύπο του μηνύματος. Για παράδειγμα κατά τη διαπραγμάτευση του είδους της συνόδου πολυμέσων περιέχονται πληροφορίες, όπως η διεύθυνση IP στην οποία θα εγκαθιδρυθεί η σύνοδος, η κωδικοποίηση και το πρωτόκολλο πολυμέσων που θα χρησιμοποιηθεί.

2.3.3 Διεκπεραίωση κλήσεων

Το πρωτόκολλο SIP ακολουθεί μια αποκεντρωμένη αρχιτεκτονική με αποτέλεσμα να μην είναι απαραίτητη η ύπαρξη διακομιστών ή άλλων υποδομών δικτύου για την εγκαθίδρυση μιας κλήσης, αρκεί ο χρήστης που επιθυμεί να επικοινωνήσει με κάποιον άλλο να γνωρίζει τη διεύθυνση IP του παραλήπτη. Σ' αυτή την περίπτωση η αλληλουχία μηνυμάτων για μια σύνοδο φαίνεται στο παρακάτω σχήμα.



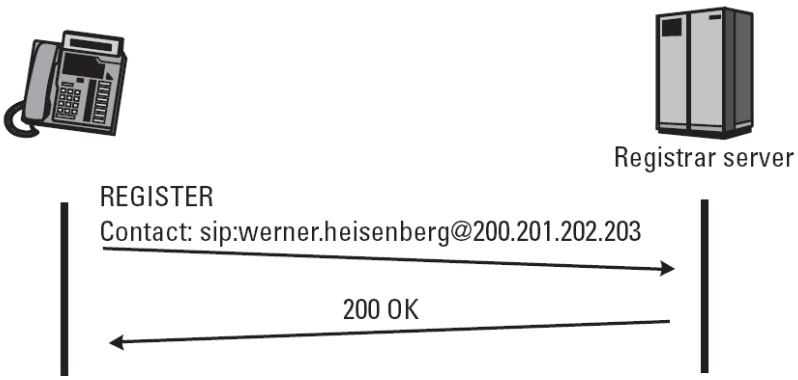
Εικόνα 1: Επικοινωνία δύο τερματικών SIP

Τις περισσότερες φορές όμως η διεύθυνση IP του παραλήπτη δεν είναι γνωστή και μάλιστα η δύναμη του SIP έγκειται στην ικανότητα του να βρίσκει τους χρήστες του, ενώ αυτοί μετακινούνται από μηχάνημα σε μηχάνημα και από δίκτυο σε δίκτυο και να προωθεί περισσότερες αιτήσεις σε πολλούς παραλήπτες, ανάλογα με την κατάσταση και τις επιλογές του κάθε χρήστη. Για να επιτευχθούν αυτές οι δυνατότητες είναι απαραίτητη η παρουσία ενδιάμεσων διακομιστών SIP, οι οποίοι θα λαμβάνουν τις αιτήσεις από τους χρήστες και θα εκτελούν όλους τους ελέγχους, τις επιλογές, τις αναζητήσεις και τελικά τις δρομολογήσεις των αιτημάτων στο δίκτυο. Οι διακομιστές αυτοί ονομάζονται Ενδιάμεσοι Διακομιστές SIP (SIP Proxy servers) και γενικά χρησιμοποιείται ένας τέτοιος διακομιστής ανά διαχειριστική οντότητα, ο οποίος είναι υπεύθυνος για τους χρήστες που ανήκουν σ' αυτήν. Φυσικά, για λόγους επεκτασιμότητας μπορεί να υπάρχουν περισσότεροι τέτοιοι διακομιστές σε κάθε διαχειριστική οντότητα, οι οποίοι να είναι γεωγραφικά κατανεμημένοι ανάλογα με τις τυπικές θέσεις των χρηστών ή σε οποιαδήποτε άλλη διάταξη

Η αλληλουχία των μηνυμάτων για την εγκαθίδρυση συνόδων με χρήση ενδιάμεσου διακομιστή φαίνεται στο παραπάνω σχήμα, όπου και οι δύο χρήστες ανήκουν στην ίδια διαχειριστική οντότητα. Στη γενική περίπτωση τα μηνύματα εγκαθίδρυσης προωθούνται από ενδιάμεσο διακομιστή σε ενδιάμεσο διακομιστή (με την επικεφαλίδα «Via» να αποθηκεύει την αλληλουχία) μέχρι να φτάσουν στο διακομιστή, ο οποίος είναι υπεύθυνος για τον παραλήπτη. Όπως παρατηρούμε από την αλληλουχία μηνυμάτων στο σχήμα, ο ενδιάμεσος διακομιστής έχει ρόλο μόνο κατά την αρχική διαπραγμάτευση και την εγκατάσταση της επικοινωνίας των δύο πλευρών. Στη συνέχεια, τα μηνύματα δεν χρειάζεται να δρομολογούνται μέσω αυτού, εκτός αν το ζητήσει ρητά εισάγοντας μια επικεφαλίδα «Record-Route». Η δρομολόγηση των μηνυμάτων-αιτήσεων μετά τη φάση εγκαθίδρυσης συνόδου βασίζεται στις επικεφαλίδες «Route», ενώ τα μηνύματα-απαντήσεις δρομολογούνται πάντα μέσω των επικεφαλίδων «Via» που σχηματίστηκαν στο μήνυμα κατά την αποστολή του αντίστοιχου μηνύματος-αίτησης.

2.3.4 Είσοδος στο σύστημα

Η διαδικασία με την οποία δημιουργείται η αντιστοίχιση ενός χρήστη με το μηχάνημα, στο οποίο θα λαμβάνει τα αιτήματα που προορίζονται γι' αυτόν, βασίζεται στο μήνυμα REGISTER ενώ τη διεκπεραίωση του αιτήματος μαζί με τους συνεπαγόμενους ελέγχους πιστοποίησης αναλαμβάνει ένας ειδικός διακομιστής, ο οποίος ονομάζεται Διακομιστής Καταχώρισης Χρηστών SIP (SIP Registrar Server). Σημαντικά στοιχεία που πρέπει να λάβουμε υπόψη είναι το γεγονός ότι ένας χρήστης μπορεί να εισέλθει στο σύστημα (register) από πολλά μηχανήματα ταυτόχρονα, οπότε και οι ενδιάμεσοι διακομιστές που λαμβάνουν μια αίτηση γι αυτόν, την προωθούν είτε παράλληλα, είτε σειριακά προς όλα αυτά τα μηχανήματα. Επιπλέον, η διάρκεια εγκυρότητας της εγγραφής, μετά το πέρας της οποίας απαιτείται επανάληψη της διαδικασίας, καθορίζεται κατά τη διεκπεραίωση της αίτησης εισόδου στο σύστημα.



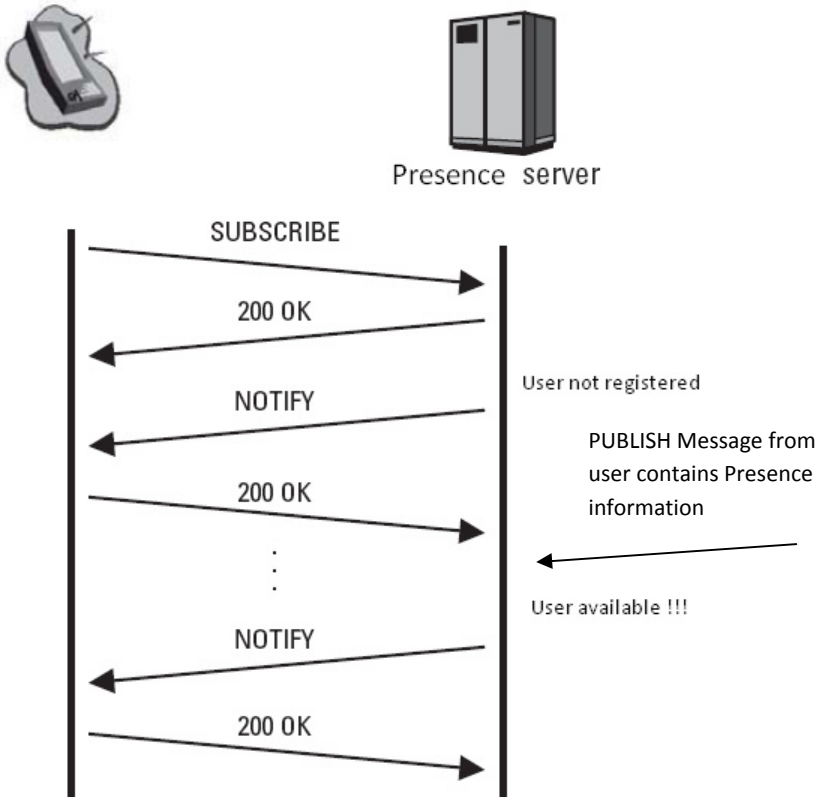
Εικόνα 2: Διαδικασία εγγραφής σε σύστημα SIP

2.3.5 Υπηρεσίες παρουσίας και μηνυμάτων

Μια από τις πιο διαδεδομένες επεκτάσεις του πρωτοκόλλου SIP περιλαμβάνει υποστήριξη για την παροχή υπηρεσιών παρουσίας και μεταφορά άμεσων μηνυμάτων. Ο κάθε χρήστης έχει ένα συγκεκριμένο διακομιστή παρουσίας, που λαμβάνει μηνύματα-αιτήσεις σε σχέση με την πληροφορία παρουσίας του, ο οποίος ορίζεται με το αντίστοιχο SIP URI <pres: username@domain> . Ο διακομιστής αυτός είναι υπεύθυνος να μεταδίδει στους ενδιαφερόμενους, δηλαδή στους χρήστες που αποστέλλουν κάποιο SUBSCRIBE,

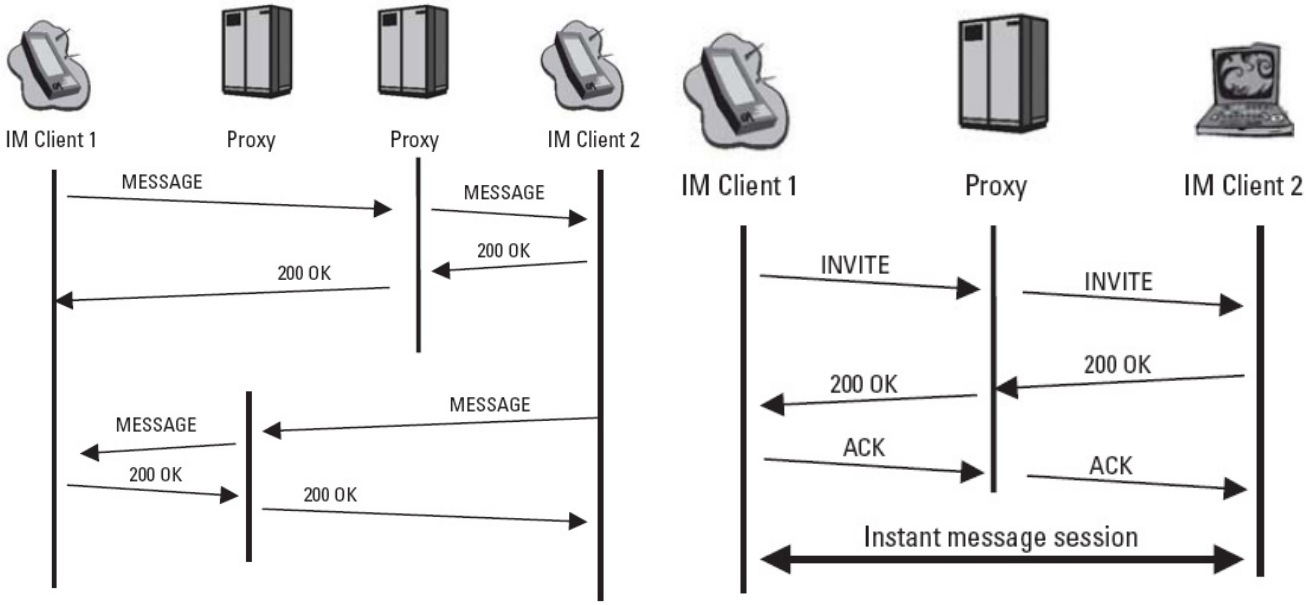
πληροφορίες για την παρουσία του χρήστη μέσω μηνυμάτων NOTIFY. Επίσης, είναι υπεύθυνος για να παρακολουθεί τα τρέχοντα UA, στα οποία βρίσκεται ο χρήστης (όπως καθορίζονται από τα μηνύματα REGISTER) και να λαμβάνει μηνύματα PUBLISH απ' αυτά ώστε να μπορεί στη συνέχεια να ειδοποιεί τους χρήστες, που ενδιαφέρονται για την πληροφορία παρουσίας.

Ένα παράδειγμα, όπου φαίνεται η επικοινωνία ενός ενδιαφερόμενου χρήστη με τον διακομιστή παρουσίας ενός άλλου χρήστη, παρουσιάζεται παρακάτω.



Εικόνα 3: Διαδικασία λήψης πληροφοριών παρουσίας σε σύστημα SIP

Ο κάθε χρήστης μπορεί φυσικά να υλοποιεί έναν PA ως ένα module σ' ένα UA, αλλά τότε αυτό το μηχάνημα θα πρέπει να είναι συνεχώς σε λειτουργία για τη λειτουργία της υπηρεσίας, οπότε η συνήθης πρακτική είναι να υπάρχει ένας PA για κάθε διαχειριστική οντότητα. Αντίστοιχα, ο κάθε χρήστης έχει ένα συγκεκριμένο UA, το οποίο λαμβάνει τα σύντομα μηνύματα που απευθύνονται σ' αυτόν και ορίζεται με το αντίστοιχο SIP URI <im: username@domain>. Αν ο χρήστης είναι ενεργός τότε τα μηνύματα προωθούνται προς τον UA που αυτός χρησιμοποιεί, αλλιώς ένας ειδικός διακομιστής μηνυμάτων τα αποθηκεύει μέχρι ο χρήστης να εισέλθει στο σύστημα, ή τα προωθεί σ' έναν διακομιστή ηλεκτρονικού ταχυδρομείου (e-mail server) αν γίνει χρήση ενός <mailto:> URI. Αν ο χρήστης είναι ενεργός τότε μπορεί αυτά τα άμεσα μηνύματα να στέλνονται είτε ανεξάρτητα με μηνύματα SIP MESSAGE, είτε να εγκαθιδρυθεί μια σύνοδος δεομένων, όπου θα στέλνεται περιεχόμενο κειμένου αντί για πολυμέσων.



Εικόνα 4: Αποστολή σύντομων μηνυμάτων σε σύστημα SIP

2.3.6 Δομικές μονάδες SIP

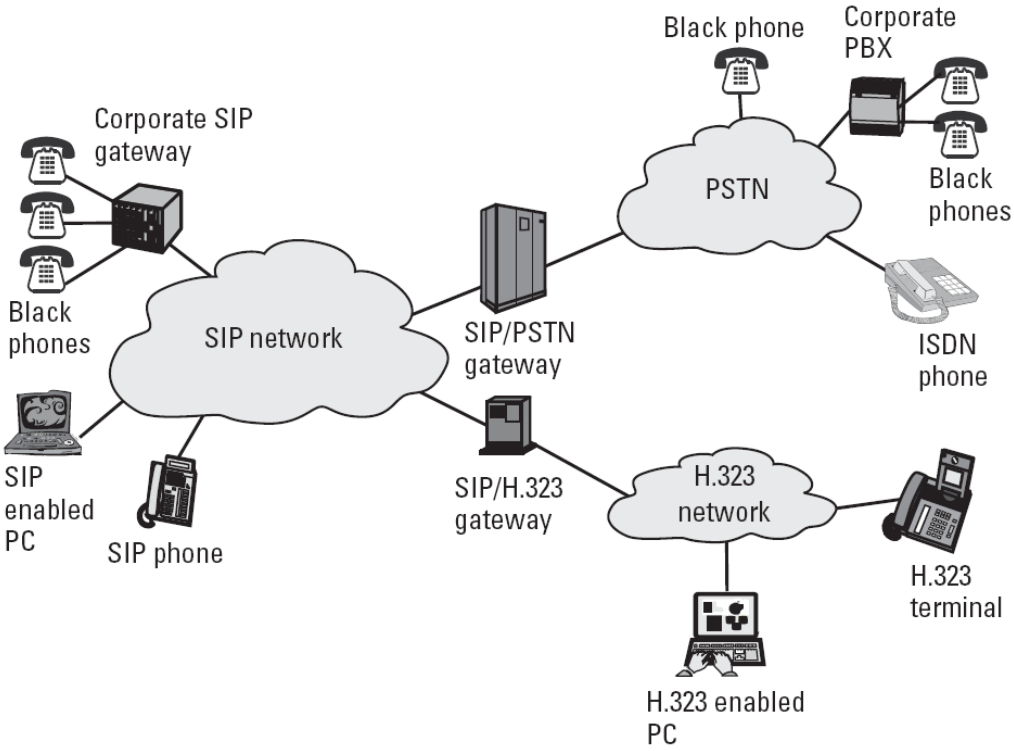
Οι δομικές μονάδες της αρχιτεκτονικής του SIP είναι οι παρακάτω:

- *Πράκτορας χρήστη (User Agent):* Είναι η δομική μονάδα που χρησιμοποιεί ο χρήστης για να αξιοποιήσει το πρωτόκολλο SIP και αποτελείται από τις επιμέρους μονάδες:
    a. Πράκτορας Χρήστη-Πελάτης (User agent-client UAC): Η εφαρμογή του καλούντα χρήστη, η οποία παράγει και στέλνει αιτήσεις SIP.
    b. Πράκτορας Χρήστη-Εξυπηρετητής (User agent-server UAS): Η εφαρμογή, η οποία λαμβάνει αιτήσεις SIP και απαντάει αποστέλλοντας απαντήσεις SIP για λογαριασμό των χρηστών.
    c. Τερματικό SIP (SIP Terminal): Το σύστημα πρόσβασης του χρήστη στην υπηρεσία. Υποστηρίζει επικοινωνία πραγματικού χρόνου και προς τις δύο κατευθύνσεις με μιαν άλλη οντότητα SIP καθώς και πρωτόκολλα πολυμέσων, όμοια με ένα τερματικό H.323. Η ελάχιστη απαίτηση είναι να υποστηρίζει στοίβα πρωτοκόλλων TCP-UDP/IP καθώς και το SDP (Session Description Protocol)
    d. Πράκτορας παρουσίας (Presence Agent PA): Η εφαρμογή, η οποία λαμβάνει αιτήματα παρουσίας και αποστέλλει πληροφορίες κατάστασης.

    Ο Πράκτορας χρήστη πρέπει να διατηρεί την κατάσταση όλων των συνόδων στις οποίες συμμετέχει, για να μπορεί να ξεχωρίζει τα μηνύματα που λαμβάνει , να παράγει τα σωστά μηνύματα-απαντήσεις και να εκτελεί τις σωστές ενέργειας ανάλογα με το μήνυμα, κάτι το οποίο σημαίνει αποθήκευση των πληροφοριών της επικεφαλίδας «Call-ID», των ετικετών «tag», της επικεφαλίδας «CSeq», καθώς και των απαραίτητων πληροφοριών δρομολόγησης. Στο RFC 3261 ορίζεται ένας ελάχιστος αριθμός μηνυμάτων και λειτουργιών, τις οποίες θα πρέπει να υποστηρίζει ο πράκτορας χρήστη. Όλα τα υπόλοιπα μηνύματα μπορούν να αντιμετωπίζονται με τον ίδιο τρόπο ανάλογα με την κατηγορία στην οποία ανήκουν. (Για παράδειγμα, αν δεν υπάρχει διαφορετική υλοποίηση, ένα μήνυμα 498 αντιμετωπίζεται σαν μήνυμα 400).

Επίσης, για την υποστήριξη συμπληρωματικών υπηρεσιών θα πρέπει ο πράκτορας χρήστη να υλοποιεί όλες τις συμπληρωματικές λειτουργίες και να υποστηρίζει τα κατάλληλα μηνύματα και τις κατάλληλες επικεφαλίδες. Οι λειτουργίες, τις οποίες μπορεί να επιτελέσει ένας πράκτορας, θα πρέπει να περιλαμβάνονται σε κάθε αίτηση, την οποία αποστέλλει ο χρήστης, στις επικεφαλίδες «Allow» και «Supported», ώστε η πλευρά του παραλήπτη να μη χρειάζεται να ρωτάει ειδικά τον αποστολέα γι' αυτές.

- *Back to Back User agent (B2BUA):* Είναι δομικές μονάδες που δρουν ως ενδιάμεσοι τόσο στο κανάλι δεδομένων, όσο και στο κανάλι ελέγχου και μετασχηματίζουν μηνύματα SIP από μια μορφή σε μία διαφορετική. Ουσιαστικά πρόκειται για ενδιάμεσους διακομιστές με αποθήκευση κατάστασης (Stateful Proxies), οι οποίοι επιτελούν λειτουργίες πέρα απ' αυτές, τις οποίες ορίζει αυστηρά το RFC 3261 για τους ενδιάμεσους διακομιστές. Η λειτουργία ενός B2B2A έχει συνήθως έναν πολύ συγκεκριμένο σκοπό, όπως είναι η παροχή μιας συγκεκριμένης υπηρεσίας . Οι σύνοδοι SIP τερματίζουν και αναδημιουργούνται σ' αυτόν οπότε η συνολική σύνοδος από άκρη σε άκρη χωρίζεται σε δύο ανεξάρτητες συνόδους, οι οποίες γεφυρώνονται μόνο μέσω του B2BUA.
- *Πύλες SIP (SIP Gateways):* Είναι δομικές μονάδες, οι οποίες μετατρέπουν συνόδους SIP τόσο στο κανάλι σηματοδοσίας, όσο και στο κανάλι δεδομένων σε διαφορετικά πρωτόκολλα σηματοδοσίας και μεταφοράς πολυμέσων. Κάθε πύλη εκτελεί συγκεκριμένες ενέργειες ανάλογα με το σύστημα με το οποίο επικοινωνεί (π.χ. PSTN, H.323) και προσφέρει τη δυνατότητα διασύνδεσης του SIP με την παραδοσιακή τηλεφωνία.



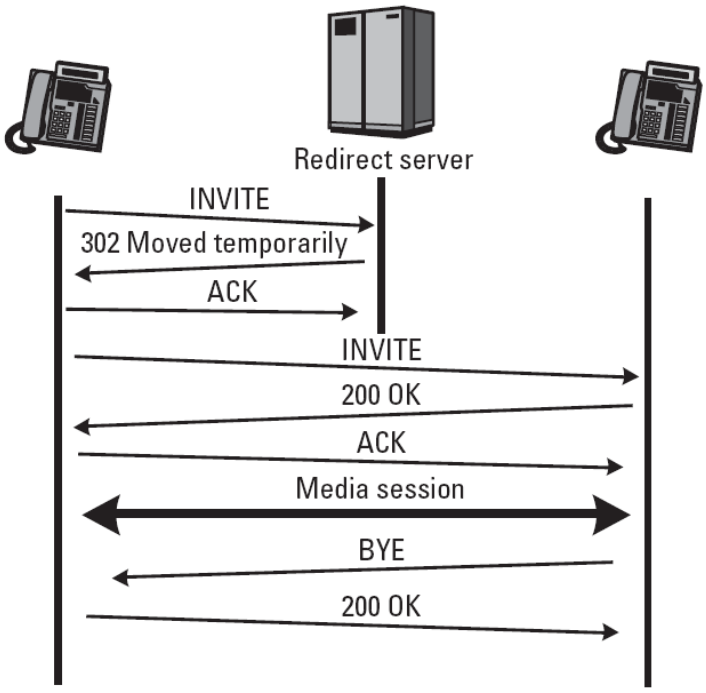
Εικόνα 5: Επικοινωνία συστήματος SIP με παραδοσιακά δίκτυα τηλεφωνίας

- *Ενδιάμεσος Διακομιστής SIP (SIP Proxy Server):* Είναι υπεύθυνος για την αναζήτηση της θέσης των παραληπτών και για την κατάλληλη δρομολόγηση των αιτημάτων. Σ' αυτό το διακομιστή εκτελούνται πρώτα όλοι οι απαραίτητοι έλεγχοι για την αποδοχή του αιτήματος του πράκτορα χρήστη, όπως είναι η πιστοποίηση χρήστη και η επιλογή της παρεχομένης υπηρεσίας. Επίσης, σ' αυτόν υλοποιούνται τυχόν ειδικές πολιτικές σε σχέση με τις αιτήσεις, όπως για παράδειγμα μια υπηρεσία προώθησης

κλήσεων. Σε περίπτωση που δεν μπορεί να εντοπιστεί ο χρήστης το αίτημα προωθείται σε άλλους διακομιστές, ενώ ανάλογα με την πολιτική που χρησιμοποιείται ο διακομιστής παρακολουθεί την εξέλιξη της κλήσης και εκτελεί τις απαραίτητες λειτουργίες σε περίπτωση αποτυχίας.

Ο Ενδιάμεσος Διακομιστής χρησιμοποιεί πληροφορία σ' άλλους διακομιστές ή υπηρεσίες για να επιτελέσει τη λειτουργία του, ενώ ανάλογα με το αν αποθηκεύει πληροφορίες για τις τρέχουσες συνόδους τοπικά, χωρίζεται: σε διακομιστή με αποθήκευση κατάστασης ή χωρίς αποθήκευση κατάστασης (Stateful vs Stateless Proxies). Ένας Ενδιάμεσος Διακομιστής με αποθήκευση κατάστασης αναλαμβάνει και την αναμετάδοση μηνυμάτων σε περίπτωση αποτυχίας, ενώ μπορεί να επιτελέσει περισσότερες λειτουργίες, συμπεριλαμβανομένης της πολλαπλής προώθησης αιτημάτων, σε περίπτωση που ο χρήστης έχει κάνει είσοδο από περισσότερα του ενός μηχανήματα. Ο Ενδιάμεσος Διακομιστής δεν εξετάζει σε καμία περίπτωση το σώμα του μηνύματος SIP και βασίζεται αποκλειστικά στην πληροφορία των επικεφαλίδων για την εκτέλεση των λειτουργιών του ενώ και οι αλλαγές τις οποίες μπορεί να κάνει σ' αυτές ορίζονται αυστηρά στο RFC 3261.

- *Διακομιστής Θέσης SIP (SIP Location Server):* Είναι υπεύθυνος για την παρακολούθηση της παρουσίας των χρηστών στο σύστημα και τη διατήρηση της πληροφορίας θέσης τους (Διεύθυνση IP) ή SIP URI (κατηγορία Device URI) ώστε να μπορεί το σύστημα να προωθήσει τις αιτήσεις στους παραλήπτες.
- *Διακομιστής Καταχώρισης Χρηστών SIP (SIP Registrar Server) :* Είναι υπεύθυνος για την ταυτοποίηση και την είσοδο των χρηστών στο σύστημα ώστε να μπορούν να λαμβάνουν τις υπηρεσίες καθώς και για την τροποποίηση των πληροφοριών εισόδου από τους χρήστες. Δέχεται μόνο μηνύματα τύπου REGISTER και αποθηκεύει την πληροφορία θέσης στο Διακομιστή Θέσης της συγκεκριμένης διαχειριστικής οντότητας ώστε ο χρήστης να είναι προσβάσιμος από το σύστημα.
- *Διακομιστής Ανακατεύθυνσης SIP (SIP Redirect Server) :* Λαμβάνει αιτήσεις SIP και εκτελεί παρόμοιες λειτουργίες μ' εκείνες του Ενδιάμεσου Διακομιστή, αλλά, αντί να προωθήσει τα αιτήματα, επιστρέφει μια απάντηση τύπου 3xx, η οποία υποδεικνύει στον αποστολέα πού θα πρέπει να απευθύνει το αίτημα του. Χρησιμοποιείται και για την υποστήριξη κινητικότητας χρήστη στο δίκτυο.



Εικόνα 6: Λειτουργία του SIP Redirect Server

- *Διακομιστής Παρουσίας SIP (SIP Presence Server or Presence Agent) :* Είναι διακομιστής, ο οποίος διαχειρίζεται τα μηνύματα SUBCRIBE και εκδίδει μηνύματα NOTIFY. Λαμβάνει αιτήσεις από χρήστες για την παρακολούθηση της παρουσίας χρηστών της διαχειριστικής οντότητας, στην οποία ανήκει. Οι χρήστες, που θέλουν να δημοσιοποιήσουν την πληροφορία παρουσίας τους στέλνουν, μηνύματα PUBLISH προς αυτόν.

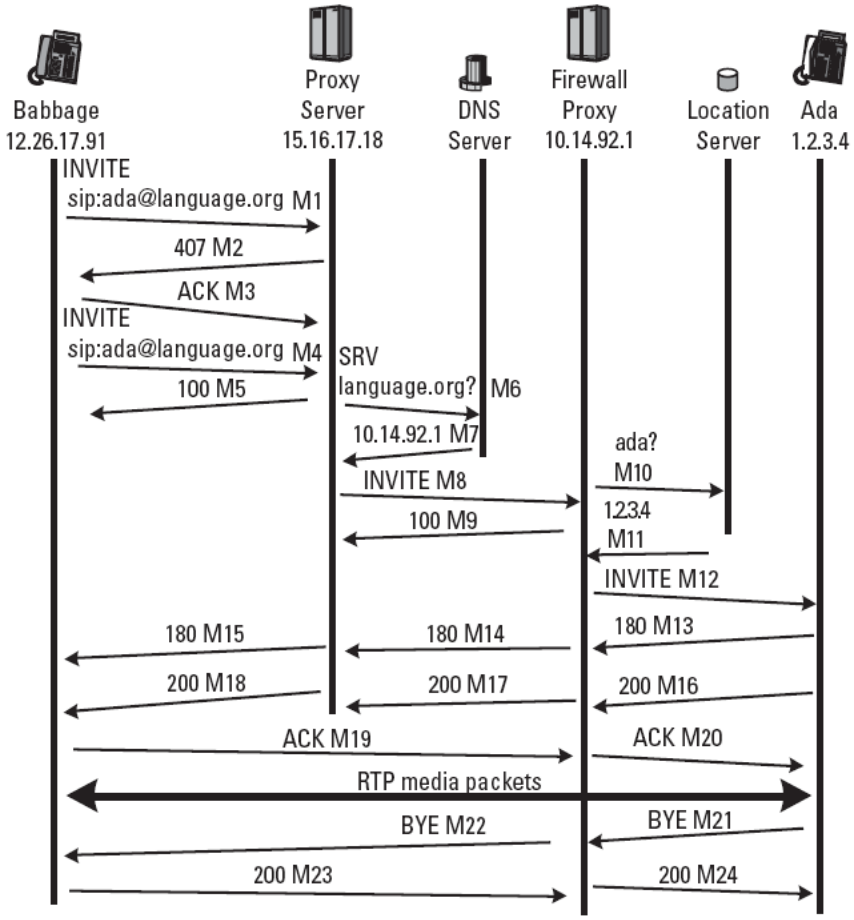
2.4 Παραβιάσεις της ιδιωτικότητας στο SIP

Στην προηγούμενη ενότητα έγινε μια παρουσίαση της αρχιτεκτονικής του SIP και παρατέθηκαν διαγράμματα με την αλληλουχία μηνυμάτων για τις βασικές λειτουργίες του, που είναι η αίτηση έναρξης συνόδου, η είσοδος στο σύστημα, καθώς και οι πιο διαδεδομένες συμπληρωματικές υπηρεσίες, όπως οι υπηρεσίες παρουσίας και σύντομων μηνυμάτων. Η υπάρχουσα αρχιτεκτονική του SIP σχεδιάστηκε με βασική προτεραιότητα να προσφέρει αποδοτική και ευέλικτη υπηρεσία επικοινωνίας πάνω από το διαδίκτυο, αλλά η προστασία της ιδιωτικότητας δεν συμπεριλήφθηκε στις αρχικές προδιαγραφές του πρωτοκόλλου. Αυτό σημαίνει ότι τα προσωπικά στοιχεία των χρηστών είναι διαθέσιμα στις δομικές μονάδες που προβλέπονται. Ως προσωπικά δεδομένα σε μια σύνοδο SIP θεωρούνται: οι ταυτότητες των εμπλεκομένων μελών, ή οποιαδήποτε άλλα στοιχεία θα μπορούσαν να οδηγήσουν στην αποκάλυψη της ταυτότητας των εμπλεκομένων μελών, όπως οι IP διευθύνσεις τους.

Στο πρωτόκολλο SIP η ταυτότητα είναι στις περισσότερες περιπτώσεις στη μορφή ενός SIP URI AOR (δες 2.3.1), τα οποία εμφανίζονται συνήθως στις επικεφαλίδες «From» ή «Reply-to» και «To», τόσο των μηνυμάτων-αιτήσεων, όσο και των μηνυμάτων-απαντήσεων. Ταυτόχρονα, χρησιμοποιείται συνήθως και ένα όνομα εμφάνισης (display name), το οποίο είναι ακόμα πιο κατανοητό από ανθρώπους και εμφανίζεται στις οθόνες των τερματικών κατά τη διάρκεια της επικοινωνίας. Άλλες επικεφαλίδες που περιέχουν SIP URI με δεδομένα ταυτότητας είναι: η επικεφαλίδα «Contact», η «Call –ID», καθώς και η «In-reply-to» που αναφέρεται σ' αυτήν, αφού η πιο συχνά χρησιμοποιούμενη σύμβαση για την παραγωγή της προτρέπει τη χρήση της IP διεύθυνσης ή του hostname του αποστολέα. Οι επικεφαλίδες «Via», «Record-route» και «Warning», που χρησιμοποιούνται από τους ενδιάμεσους διακομιστές, δεν αποκαλύπτουν άμεσα την ταυτότητα ενός αποστολέα, αλλά αποκαλύπτουν πληροφορίες, όπως η διαχειριστική οντότητα στην οποία ανήκει και οι οποίες μπορεί να οδηγήσουν σε αποκάλυψη της ταυτότητας του. Τέλος, υπάρχουν επικεφαλίδες που δεν περιέχουν πληροφορίες ταυτότητας, αλλά άλλου είδους προσωπικά δεδομένα, όπως οι επικεφαλίδες: «Subject», «Organization», «User – Agent», «Call – Info».

2.4.1 Μια τυπική αλληλουχία μηνυμάτων

Σ' αυτό το σημείο θα παρουσιασθούν τα κενά στην προστασία της ιδιωτικότητας στο περιβάλλον του SIP, αναλύοντας την παρακάτω τυπική αλληλουχία μηνυμάτων για την εγκαθίδρυση μιας συνόδου.



Εικόνα 7: Σηματοδοσία κατά την εγκαθίδρυση συνόδου SIP

Παραβιάσεις ιδιωτικότητας ανά μήνυμα.

M1:
Ο χρήστης Babbage αποκαλύπτει την ταυτότητα του στον Ενδιάμεσο Διακομιστή της διαχειριστικής του οντότητας καθώς και την ταυτότητα του παραλήπτη με τον οποίον θέλει να επικοινωνήσει. Τέλος, αποκαλύπτει τη διεύθυνση IP του τρέχοντος μηχανήματος, το οποίο χρησιμοποιεί τόσο στο επίπεδο δικτύου μέσω του πεδίου Source IP Address της επικεφαλίδας IP, όσο και σε επίπεδο SIP, μέσω της επικεφαλίδας Contact. Ταυτόχρονα, αποκαλύπτονται ευαίσθητες πληροφορίες, που περιέχονται σε κάποια από τις υπόλοιπες προαιρετικές επικεφαλίδες.
Επίσης, τυχόν τρίτοι που παρακολουθούν το κανάλι επικοινωνίας μπορούν να εξάγουν τις ίδιες πληροφορίες μέσω μιας επίθεσης ενδιάμεσου (man-in-the middle attack) ή παρακολούθησης (eavesdropping). Ο τελευταίος κίνδυνος υπάρχει σε όλες τις μεταδόσεις μηνυμάτων στο δίκτυο, αλλά θα τον αναφέρουμε μόνο εδώ.

M8:
Ο χρήστης Babbage αποκαλύπτει την ταυτότητα του στον Ενδιάμεσο Διακομιστή της τελικής, ή οποιασδήποτε άλλης ενδιάμεσης διαχειριστικής οντότητας καθώς και την ταυτότητα του παραλήπτη με τον οποίον θέλει να επικοινωνήσει. Επίσης αποκαλύπτεται η διεύθυνση IP του αποστολέα μέσω του SIP URI της επικεφαλίδας «Contact», ενώ η επικεφαλίδα «Via» αποκαλύπτει πληροφορίες, που μπορούν να οδηγήσουν κατά προσέγγιση στο γεωγραφικό προσδιορισμό του αποστολέα .

M11:
Αποκαλύπτεται η διεύθυνση IP που χρησιμοποιεί ο παραλήπτης στον τελικό Ενδιάμεσο Διακομιστή.

M12:
Αποκαλύπτονται όλες οι παραπάνω πληροφορίες στον τελικό παραλήπτη Ada.

M17:
Αποκαλύπτεται η διεύθυνση IP που χρησιμοποιεί ο χρήστης Ada στον Ενδιάμεσο Διακομιστή της αρχικής, ή οποιασδήποτε άλλης ενδιάμεσης, διαχειριστικής οντότητας.

M18:
Αποκαλύπτεται η διεύθυνση IP που χρησιμοποιεί ο χρήστης Ada στο χρήστη Babbage.

Παρόμοιες παραβιάσεις έχουμε και κατά την εκτέλεση των υπολοίπων λειτουργιών του SIP, ενώ οι υπηρεσίες παρουσίας αποκαλύπτουν ακόμα περισσότερα προσωπικά στοιχεία, αφού υποστηρίζουν κινητικότητα χρήστη και αποκαλύπτουν πληροφορίες για την τρέχουσα τοποθεσία και κατάσταση του .
Ταυτόχρονα, οι υπηρεσίες αυτές χρησιμοποιούνται από τους χρήστες για την κατάρτιση και ενημέρωση της λίστας φίλων (buddy list), η οποία αποκαλύπτει πληροφορίες για κοινωνικές συναναστροφές αν δεν υπάρξει μηχανισμός για την προστασία της. Ταυτόχρονα, η λίστα αυτή καθιστά ευκολότερη την εξαγωγή προσωπικών πληροφοριών, αφού η διαρκής ενημέρωσή της απαιτεί μεγάλη διακίνηση μηνυμάτων στο δίκτυο.

2.5 Απαιτήσεις προστασίας ιδιωτικότητας από την διαδικτυακή τηλεφωνία

Λαμβάνοντας υπόψη τις παραβιάσεις ιδιωτικότητας του πρωτοκόλλου SIP, που αναφέρθηκαν σε προηγούμενη παράγραφο, ένα σύστημα διαδικτυακής τηλεφωνίας με προστασία της ιδιωτικότητας βασισμένο σ' αυτό θα πρέπει να έχει τις παρακάτω ιδιότητες:

1. Κάθε χρήστης του συστήματος, ο οποίος επιθυμεί για προσωπικούς του λόγους να αποστείλει ένα ανώνυμο μήνυμα, θα πρέπει να λαμβάνει εγγυήσεις για την ιδιωτικότητά του. Η ανωνυμία μπορεί να μην υλοποιείται μόνο απέναντι στον τελικό παραλήπτη, αλλά σε διαφορετικά επίπεδα, όπως φαίνεται και στις ακόλουθες περιπτώσεις:

    - Κατά την διάρκεια της παρουσίας του στο σύστημα ο χρήστης επιθυμεί να προστατεύονται τα μηνύματα του από παρεμβάσεις τρίτων.
    - Κατά την αποστολή ενός μηνύματος ο χρήστης θέλει να αποκρύψει την ταυτότητα του από τον τελικό παραλήπτη ενώ αυτή μπορεί να είναι εμφανής σε ενδιάμεσες μονάδες κατά τη δρομολόγηση. Αυτό μπορεί να είναι επιθυμητό εφόσον ο χρήστης επιθυμεί κατά την επικοινωνία του να αποκαλύψει στον παραλήπτη πληροφορίες με τις οποίες δεν θα ήθελε να συσχετιστεί (για παράδειγμα κατά την λειτουργία ανώνυμων συμβουλευτικών τηλεφωνικών κέντρων).
    - Κατά την αποστολή ενός μηνύματος ο χρήστης θέλει να αποκρύψει την ταυτότητα του από ενδιάμεσες μονάδες, αλλά αυτή να είναι εμφανής στον τελικό παραλήπτη.
    - Κατά την αποστολή ενός μηνύματος ο χρήστης θέλει να αποκρύψει την ταυτότητα του τόσο από τον τελικό παραλήπτη, όσο και από τους ενδιάμεσους.

- Κατά την αποστολή ενός μηνύματος ο χρήστης θέλει να αποκρύψει την ταυτότητα του από ένα σύνολο μη έμπιστων δομικών μονάδων SIP ή διαχειριστικών οντοτήτων, αλλά αυτή να είναι εμφανής σ' ένα άλλο σύνολο που εμπιστεύεται.
- Ο χρήστης έχει τη δυνατότητα να επιλέξει να αρνηθεί το σύστημα να παρέχει συγκεκριμένες ή γενικά πληροφορίες παρουσίας σε άλλους χρήστες, που τις ζητούν, εκτός από κάποιες συγκριμένες έμπιστες επαφές.

Ανάλογα με τις επιθυμίες των χρηστών οι μη έμπιστοι παραλήπτες ή ενδιάμεσοι δεν θα πρέπει να έχουν τη δυνατότητα να εκκινήσουν μια νέα σύνοδο με τον ανώνυμο αποστολέα. Παρ' όλα αυτά ο ανώνυμος αποστολέας θα πρέπει να είναι σε θέση να λαμβάνει μηνύματα-απαντήσεις και μηνύματα-αιτήσεις ως μέρος της συγκεκριμένης συνόδου. Ταυτόχρονα, μόνο οι έμπιστοι ενδιάμεσοι διακομιστές θα γνωρίζουν την ταυτότητα του αποστολέα του μηνύματος και μόνο οι έμπιστες επαφές του χρήστη θα μπορούν να λαμβάνουν πληροφορίες σε σχέση με την παρουσία του στο σύστημα.

2. Ο χρήστης-παραλήπτης μπορεί να έχει παρόμοιες απαιτήσεις, αν και για να είναι δυνατή η επικοινωνία η ταυτότητα του θα πρέπει να είναι γνωστή στον αποστολέα. Μπορεί όμως να μην επιθυμεί ο αποστολέας να μάθει το σημείο στο οποίο αυτός λαμβάνει τις τρέχουσες κλήσεις του, όπως αυτό εκφράζεται από το SIP-URI στην επικεφαλίδα «Contact», ενώ διατηρεί το δικαίωμα να μην μαθαίνουν, ενδιάμεσες διαχειριστικές οντότητες, ότι δέχεται κλήσεις.

Γενικά οι χρήστες δεν πρέπει να βασίζουν την προστασία των προσωπικών τους δεδομένων στην εκτίμηση για τη διαδρομή, που θα ακολουθήσει το μήνυμα τους αφού στην πραγματικότητα μπορεί το μήνυμα να καταλήξει σε διαφορετικούς προορισμούς και μέσω διαφορετικών διαδρομών. Για παράδειγμα, μπορεί ο αποστολέας bob@ntua.gr να αποστείλει ένα μήνυμα στην alice@ntua.gr και θεωρώντας ότι η alice ανήκει στην ίδια διαχειριστική οντότητα, που ο ίδιος εμπιστεύεται, να μην προβεί σε περαιτέρω ενέργειες για προστασία της ταυτότητας του. Υπάρχει όμως περίπτωση το αίτημα να δρομολογηθεί σε άλλη διαχειριστική οντότητα, στην οποία θα έχει βρεθεί προσωρινά η alice με αποτέλεσμα την αποκάλυψη της ταυτότητας του bob σε μη έμπιστους φορείς.

2.6 Παρεχόμενες υπηρεσίες προστασίας στο υπάρχον σύστημα διαδικτυακής τηλεφωνίας

2.6.1 Παρεχόμενες υπηρεσίες από το SIP

Το πρωτόκολλο SIP στη βασική του μορφή προσφέρει υπηρεσίες ασφάλειας και πιστοποίησης, οι οποίες ως ένα βαθμό προστατεύουν τους χρήστες, κυρίως απέναντι σε επιθέσεις τρίτων με τις παρακάτω λειτουργίες:

a. Για την επίλυση των προβλημάτων παρέμβασης τρίτων στο κανάλι σηματοδοσίας του πρωτόκολλου SIP μεταξύ των πελατών και της εταιρείας, καθώς και μεταξύ των διακομιστών των εταιριών παροχής υπηρεσιών, υπάρχει ήδη πλούσια βιβλιογραφία. Ειδικά, στο RFC 3261 προτείνεται η χρήση του πρωτοκόλλου Secure SIP, η οποία αποτελεί μια υλοποίηση του SIP πάνω από το πρωτόκολλο TLS (Transport Layer Security) και περιλαμβάνει μηχανισμούς πιστοποίησης και κρυπτογράφησης με

γνωστές μεθόδους ψηφιακών πιστοποιητικών, συμμετρικής και ασύμμετρης κρυπτογράφησης και χρήσης αριθμών nonce ώστε να αποφευχθούν οι περισσότερες από τις κακόβουλες επιθέσεις, όπως επιθέσεις ενδιαμέσου (man in the middle attacks), υποκλοπή μηνυμάτων και αναπαραγωγή μηνυμάτων. Το πρωτόκολλο αυτό χρησιμοποιείται σε μια λογική βήμα προς βήμα (hop by hop) και όχι από άκρη σε άκρη (end to end) ώστε το περιεχόμενο των μηνυμάτων να είναι διαθέσιμο στις δομικές μονάδες του SIP, αφού στις επικεφαλίδες περιέχονται απαραίτητα στοιχεία για τη δρομολόγηση των κλήσεων, τα οποία πρέπει και να επεξεργάζονται από τους ενδιάμεσους διακομιστές.

b. Για την πιστοποίηση των χρηστών χρησιμοποιούνται δύο λύσεις:
   i. Μια μορφή ελαφριάς πιστοποίησης με username και password (digest authentication method) στα πρότυπα της αντίστοιχης πιστοποίησης που χρησιμοποιείται στο http και η οποία συμπληρώνεται με τη χρήση ασφαλών πρωτοκόλλων μεταφοράς.
   ii. Χρήση ψηφιακών πιστοποιητικών τόσο από την πλευρά του χρήστη, όσο και από την πλευρά των διακομιστών.

c. Για την παροχή υπηρεσιών κρυπτογράφησης και πιστοποίησης από άκρη σε άκρη υποστηρίζεται ο τύπος μηνύματος S/MIME που ορίζεται στο RFC 2633 [20] και εφαρμόζει αλγόριθμους κρυπτογράφησης ασύμμετρου κλειδιού με το δημόσιο κλειδί του παραλήπτη σ' ένα μήνυμα για την επίτευξη ασφάλειας. Σ' αυτό το μήνυμα συμπεριλαμβάνεται μεταξύ άλλων το ψηφιακό πιστοποιητικό του αποστολέα και η κρυπτογραφική σύνοψη MD5 του μηνύματος για την επίτευξη ταυτοποίησης και ακεραιότητας αντίστοιχα. Με χρήση κρυπτογράφησης από άκρο σε άκρο των επικεφαλίδων SIP που πρέπει να μένουν αμετάβλητές από το δίκτυο (δηλαδή όχι των «Via», «Route» κ.τ.λ.), ο τελικός χρήστης μπορεί να κρίνει, αν το μήνυμα έχει αλλοιωθεί από κάποιον ενδιάμεσο πριν φθάσει σ' αυτόν.

Οι παραπάνω λειτουργίες δίνουν τη δυνατότητα προστασίας των προσωπικών δεδομένων των πελατών από τις επιθέσεις τρίτων με τις γνωστές τεχνολογίες κρυπτογράφησης και πιστοποίησης, αλλά παραμένει το πρόβλημα προστασίας των δεδομένων απέναντι στην ίδια την εταιρεία παροχής της υπηρεσίας. Η εταιρεία μπορεί να μην υιοθετεί κάποια πολιτική προστασίας των προσωπικών δεδομένων, ή, ακόμα και αν υιοθετεί, μπορεί στην πράξη να μην την υλοποιεί. Σε κάθε περίπτωση δεν υπάρχει τρόπος να ελεγχθεί και γι' αυτόν το λόγο απαιτείται μια διαφορετική προσέγγιση για την επίλυση του προβλήματος.

2.6.2 Παρεχόμενες υπηρεσίες από τις εταιρίες διαδικτυακής τηλεφωνίας

Οι υπάρχουσες λύσεις στο χώρο της διαδικτυακής τηλεφωνίας δεν δίνουν την πρέπουσα σημασία στην προστασία της ιδιωτικότητας του χρήστη. Τόσο σε επίπεδο επιχειρηματικού μοντέλου, όσο και σε επίπεδο τεχνικών λύσεων, που παρέχονται, η προστασία των προσωπικών δεδομένων των πελατών είναι κάτι που δεν έχει προβλεφθεί, παρόλο που επιβάλλεται από την υπάρχουσα κοινοτική και εθνική νομοθεσία. Αν και οι εταιρείες δεσμεύονται από τη νομοθεσία σχετικά με το απόρρητο των ηλεκτρονικών υπηρεσιών και συγκεκριμένα των επικοινωνιών, υπάρχουν συγκεκριμένες παράμετροι που κάνουν την εφαρμογή της δύσκολη και τελικά αναξιόπιστη. Οι εταιρείες παροχής υπηρεσιών τηλεφωνίας, οποιασδήποτε μορφής, είναι συνήθως μεγάλοι οργανισμοί που απασχολούν

χιλιάδες άτομα ως προσωπικό. Η εκτεταμένη γεωγραφική κάλυψη που επιβάλλεται από τη φύση της παρεχόμενης υπηρεσίας καθώς και το μεγάλο πλήθος των συνδρομητών, κάνει αναγκαία τη χρήση σύνθετων πληροφοριακών συστημάτων. Για να μπορούν οι υπάλληλοι να εξυπηρετούν τους πελάτες σε κάθε γεωγραφική περιοχή απαιτείται η πρόσβαση σ' αυτά τα πληροφοριακά συστήματα ώστε να γίνεται η τροποποίηση των προφίλ των συνδρομητών, σύμφωνα με τις επιλογές τους. Στα συγκεκριμένα προφίλ, εκτός από πληροφορίες άμεσα συσχετισμένες με την εταιρεία, όπως επιλεγμένο πρόγραμμα χρέωσης, πολύ συχνά είναι αποθηκευμένα και προσωπικά δεδομένα συνδρομητών με πιο συνηθισμένο τη λίστα κλήσεων τους.

Είναι εύκολο να γίνει αντιληπτό ότι η υψηλή κλιμάκωση αυτών των πληροφοριακών συστημάτων σε συνδυασμό με την παροχή δικαιωμάτων πρόσβασης σε πολλά άτομα του προσωπικού από διαφορετικά κλιμάκια ιεραρχίας, κάθε άλλο παρά προστατεύει την ιδιωτικότητα του χρήστη. Όταν δεν έχει ενεργή παρουσία κάποια αρχή υπεύθυνη για την προστασία των προσωπικών δεδομένων, μπορεί εύκολα κάποιος τρίτος με χρήση social engineering, ή ακόμα πιο απλά με κάποιον γνωστό υπάλληλο της εταιρείας, να έχει πρόσβαση στα αρχεία λίστας κλήσεων και τα προσωπικά δεδομένα πελατών. Αυτές οι παραβιάσεις ιδιωτικότητας, παρά το γεγονός ότι γίνονται εύκολα και συχνά, ούτε καταγράφονται ούτε τιμωρούνται τις περισσότερες φορές, καθώς εμφανίζονται σαν συναλλαγές ρουτίνας με το πληροφοριακό σύστημα και δεν υπάρχει πουθενά καταγεγραμμένη κάποια μη εξουσιοδοτημένη πρόσβαση. Ακόμα και αν η εταιρεία εφαρμόζει αυστηρή πολιτική πρόσβασης στα συστήματά της, το πρόβλημα παραμένει, αφού πηγάζει από το γεγονός ότι όλη η πληροφορία αποθηκεύεται κεντρικά και είναι ευάλωτη σε επιθέσεις ασφαλείας. Για να προστατευθεί η ιδιωτικότητα των χρηστών είναι απαραίτητο να αναπτυχθούν τεχνικές λύσεις, οι οποίες θα κάνουν δυνατή την προστασία των προσωπικών δεδομένων, κατανέμοντας κατάλληλα την πληροφορία ώστε οι πιθανοί επιτιθέμενοι να μην μπορούν να την συγκεντρώσουν ολόκληρη στην περίπτωση εύρεσης ενός κενού ασφαλείας.

Στις υπάρχουσες λύσεις το θέμα της ιδιωτικότητας δεν αντιμετωπίζεται ως τεχνικό ζήτημα, αλλά ως ζήτημα της επιχειρηματικής πολιτικής (business policy). Οι πελάτες τις περισσότερες φορές απλά βασίζονται σε πολιτικές βέλτιστης προσπάθειας και καταλήγουν να εμπιστεύονται την εταιρεία χωρίς εγγυήσεις, γιατί δεν μπορούν να πράξουν διαφορετικά. Οι εταιρείες από την πλευρά τους υποστηρίζουν ότι τα δίκτυα τους είναι απόλυτα ασφαλή και ότι οι συνομιλίες των πελατών τους είναι σχεδόν αδύνατο να υποκλαπούν. Τονίζουν δηλαδή θέματα ασφαλείας (security) για τα οποία υπάρχουν έτοιμες διαδεδομένες λύσεις και προσπαθούν να δημιουργήσουν στους χρήστες την ψευδαίσθηση ότι η ασφάλεια εξασφαλίζει την ιδιωτικότητά τους. Είναι πλέον σύνηθες οι τηλεφωνικές κλήσεις στο διαδίκτυο να κρυπτογραφούνται ώστε να υπάρχει σχεδόν απόλυτη προστασία από τρίτους, που θα προσπαθήσουν να υποκλέψουν την τηλεφωνική συνομιλία. Αυτό που πριν μια δεκαετία απλά απαιτούσε δύο κομμάτια καλώδιο και ένα μαγνητοφωνάκι, απαιτεί πλέον πανίσχυρους υπολογιστές και ουσιαστικά άπειρο υπολογιστικό χρόνο. Οι εταιρείες παροχής διαδικτυακών υπηρεσιών τηλεφωνίας φυσικά το γνωρίζουν αυτό, οπότε δεν αμελούν να διαφημίζουν και να στηρίζουν τη φήμη τους στο πόσο ασφαλείς είναι οι υπηρεσίες τους, αφήνοντας να εννοηθεί ότι με τους ισχυρότατους αλγορίθμους κρυπτογράφησης μπορεί να εξασφαλισθεί η ασφάλεια και ιδιωτικότητα του χρήστη. Άλλωστε, αφού είναι τόσο δύσκολο κάποιος να υποκλέψει τις τηλεφωνικές κλήσεις η «ιδιωτικότητα είναι» εξασφαλισμένη. Αυτό είναι μια μεγάλη σύγχυση που ίσως και εσκεμμένα τροφοδοτείται από τις εταιρείες παροχής διαδικτυακής τηλεφωνίας, καθώς η έννοια ιδιωτικότητα είναι κάτι πολύ ευρύτερο από την ασφάλεια και δεν μπορεί να

εξασφαλισθεί απλά με την εφαρμογή υπαρχόντων τεχνολογιών ασφαλείας χωρίς σημαντικές αλλαγές στην αρχιτεκτονική του πληροφοριακού συστήματος μιας εταιρείας. Μόνο μια τεχνική λύση, η οποία θα έχει σχεδιασθεί εξ αρχής με σκοπό την προστασία της ιδιωτικότητας στο περιβάλλον της διαδικτυακής τηλεφωνίας, μπορεί να δώσει τις απαραίτητες εγγυήσεις στον τελικό χρήστη για τον τρόπο με τον οποίο θα αποθηκεύονται και θα επεξεργάζονται τα προσωπικά του δεδομένα. Η νομοθεσία [8]-[12] επιβάλλει ότι ο χρήστης είναι αυτός που έχει τον τελευταίο λόγο πάνω στα προσωπικά του στοιχεία και εκτός ιδιαζόντων περιπτώσεων τίποτα δεν μπορεί να γίνει χωρίς τη συγκατάθεσή του.

3

Αρχιτεκτονική του συστήματος

Η βασική ιδέα [21], στην οποία θα βασιστεί η αρχιτεκτονική του συστήματος για την επίλυση του προβλήματος της προστασίας προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας, είναι η έννοια της Ανεξάρτητης Αρχής (Α.Α.). Η έννοια αυτή εμφανίζεται στη θεωρία της ηλεκτρονικής ταυτοποίησης με τη χρήση ψηφιακών πιστοποιητικών και μάλιστα εφαρμόζεται ήδη με μεγάλη επιτυχία. Η Α.Α. είναι ένας οργανισμός τον οποίο εμπιστεύονται τόσο οι πελάτες, όσο και η εταιρεία παροχής της υπηρεσίας. Η αμοιβαία εμπιστοσύνη είναι ένα σημαντικό στοιχείο, το οποίο δίνει τη δυνατότητα να εκτελούνται οι κρίσιμες λειτουργίες του συστήματος, οι οποίες περιλαμβάνουν ανταλλαγή και επεξεργασία προσωπικών δεδομένων σ' έναν οργανισμό που έχει καθολική αποδοχή. Επίσης μας δίνει ένα σταθερό σημείο από το οποίο μπορεί να ξεκινήσει ο σχεδιασμός, αφού όλες οι άλλες προτεινόμενες αρχιτεκτονικές καταλήγουν τελικά σε περίπλοκες συσχετίσεις εμπιστοσύνης, περιβάλλον στο οποίο τις περισσότερες φορές δεν είναι δυνατή η εύρεση κάποιας λύσης για την παροχή της υπηρεσίας. Ακόμα και όταν επιτυγχάνεται λύση, αυτή περιλαμβάνει πολύπλοκα συστήματα αλλεπάλληλων κρυπτογραφήσεων και πιστοποιήσεων με καταστρεπτικές επιπτώσεις στην απόδοση του συστήματος. Η ιδέα της κεντρικής διαχείρισης των τομέων ασφάλειας και προστασίας εφαρμόζεται ήδη σ' όλα τα επίπεδα παροχής υπηρεσιών (από τα firewall μέχρι τις αρχές έκδοσης πιστοποιητικών).

Η Α.Α. συνεργάζεται με την εταιρεία παροχής υπηρεσιών τόσο σε επιχειρηματικό, όσο και σε τεχνικό επίπεδο και μ' αυτόν τον τρόπο δίνεται η δυνατότητα να ενταχθεί στο σύστημα μια δομική μονάδα, η οποία θα επιβάλλει τη νομοθεσία και θα παρέχει τις επιθυμητές εγγυήσεις για την προστασία των προσωπικών δεδομένων των πελατών. Αυτή η δομική μονάδα θα εγκατασταθεί στο χώρο και στο δίκτυο της εταιρείας , αλλά θα βρίσκεται υπό την αποκλειστική διαχειριστική ευθύνη της Α.Α [22]. Μ' αυτόν τον τρόπο μπορεί να αναπτυχθεί μια αρχιτεκτονική που θα διασφαλίζει και την προστασία των πελατών, αλλά και θα επιτρέψει στην εταιρεία να συνεχίσει τη λειτουργία του επιχειρηματικού της μοντέλου με

τα απαραίτητα γι' αυτό δεδομένα να είναι διαθέσιμα και προσβάσιμα με κάποιον αποδοτικό τρόπο.

Στην αρχιτεκτονική, που προτείνεται, η Α.Α. αναλαμβάνει μέρος των λειτουργιών της εταιρείας παροχής υπηρεσίας και συγκεκριμένα το τμήμα εκείνο το οποίο σχετίζεται με την ανταλλαγή προσωπικών δεδομένων. Η βασική δομική μονάδα της Α.Α. είναι ένας διακομιστής (τον οποίο ονομάζουμε Διακομιστή Προστασίας Ιδιωτικότητας (Δ.Π.Ι.) (Privacy Server)), ο οποίος παρεμβάλλεται μεταξύ των πελατών και της εταιρείας παροχής υπηρεσίας και εκτελεί όλες τις απαραίτητες ενέργειες για να διασφαλίσει την προστασία των προσωπικών δεδομένων των πελατών, αλλά ταυτόχρονα παρέχει αρκετά δεδομένα στην εταιρεία ώστε αυτή να μπορεί να εκτελέσει τις λειτουργίες των υπηρεσιών της. Οι ενέργειες αυτές περιλαμβάνουν όλες τις γνωστές τεχνικές που συναντούμε σε αντίστοιχα προβλήματα, όπως: κρυπτογράφηση, δημιουργία μοναδικών αναγνωριστικών και χρήση ψηφιακών πιστοποιητικών.

Ως προς την υπηρεσία VoIP μέσω SIP, η οποία αποτελεί και το βασικό στοιχείο του επιχειρηματικού μοντέλου, η Α.Α. παρεμβάλλεται πάντα μεταξύ των διακομιστών της εταιρείας και των πελατών καθώς και μεταξύ των διακομιστών και του υπολοίπου διαδικτύου, εκτελώντας λειτουργίες μετασχηματισμών και κρυπτογράφησης για να προστατέψει τα προσωπικά δεδομένα που αποκαλύπτει η λειτουργία του SIP (δες 2.4). Ο Δ.Π.Ι. αποκρύπτει μ' αυτόν τον τρόπο τη δράση των χρηστών της υπηρεσίας, προσφέροντας ο ίδιος υπηρεσίες ανωνυμίας. Επομένως, το μόνο που έχουν να κάνουν οι χρήστες, οι οποίοι θέλουν να λάβουν μια τέτοια υπηρεσία είναι να τη ζητήσουν από το συγκεκριμένο διακομιστή. Όσον αφορά στο υπόλοιπο επιχειρηματικό μοντέλο, ο Δ.Π.Ι. θα πρέπει να αναλάβει να δρα ως ενδιάμεσος σε όλες τις λειτουργίες που αφορούν τη μεταφορά προσωπικών δεδομένων, μετατρέποντας κατάλληλα την κίνηση που μεταφέρεται, ώστε να αποτρέπει την αποκάλυψη προσωπικών δεδομένων , ενώ θα πρέπει να αναλάβει όλες εκείνες τις βασικές λειτουργίες, που αφορούν την διαχείριση του όλου συστήματος παροχής προστασίας ιδιωτικότητας. Περισσότερες λεπτομέρειες για τη λειτουργία των υπολοίπων υποσυστημάτων του Δ.Π.Ι. θα δοθούν σε επόμενες παραγράφους, σε σχέση με τις συγκεκριμένες παραβιάσεις της ιδιωτικότητας του επιχειρηματικού μοντέλου που καλούνται να αποσοβήσουν.

3.1 Ο μηχανισμός προστασίας προσωπικών δεδομένων στο SIP που περιγράφεται στο RFC 3323

Το RFC 3323 [23] ορίζει έναν μηχανισμό με τον οποίο μπορεί να παρασχεθεί η υπηρεσία ανωνυμίας στο πρωτόκολλο SIP, ενώ υποδεικνύει και τις ενέργειες, στις οποίες μπορούν να προβούν οι ίδιοι οι χρήστες για την προστασία της ιδιωτικότητας τους και οι οποίες θα εξεταστούν παρακάτω. Συγκεκριμένα, ορίζεται μια ακόμα οντότητα στην αρχιτεκτονική του SIP, η οποία προσφέρει υπηρεσίες ανωνυμίας, εξετάζοντας απαιτήσεις προστασίας ιδιωτικότητας που εκφράζονται σε μια καινούργια επικεφαλίδα «Privacy». Η συγκεκριμένη επικεφαλίδα μπορεί να πάρει μία από τις παρακάτω επιλογές, οι οποίες εκφράζουν και ένα επίπεδο ανωνυμίας, το οποίο απαιτεί ο χρήστης από το σύστημα: (Οι

αναλυτικές λειτουργίες που επιτελούνται ανάλογα με την κάθε επιλογή, αναλύονται σε επόμενες παραγράφους.)

- user: Ο χρήστης αιτείται να του παρασχεθεί υπηρεσία ανωνυμίας αντίστοιχης με αυτή που θα μπορούσε να επιτελέσει και ο ίδιος, αλλά για κάποιο λόγο δεν μπορεί.
- header: Ο χρήστης αιτείται να του παρασχεθεί υπηρεσία απόκρυψης όλων των πληροφοριών επικεφαλίδας που μπορεί να αποκαλύπτουν έμμεσα προσωπικά του στοιχεία, όπως αυτά των επικεφαλίδων Via και Contact.
- session: Ο χρήστης αιτείται να του παρασχεθεί υπηρεσία ανωνυμίας των συνόδων δεδομένων που ξεκινάνε μ' αυτό το μήνυμα.
- none: Ο χρήστης αιτείται ρητά να μην του παρασχεθεί καμία υπηρεσία ιδιωτικότητας ανεξάρτητα από άλλες υπάρχουσες πολιτικές.
- critical: Ο χρήστης αιτείται οι υπηρεσίες προστασίας ιδιωτικότητας, για αυτό το μήνυμα να εφαρμοστούν σε κάθε περίπτωση, αλλιώς το μήνυμα θα πρέπει να απορριφθεί από το δίκτυο.

Η επικεφαλίδα μπορεί να περιλαμβάνει την επιλογή «none» ή οποιοδήποτε συνδυασμό των πρώτων τριών επιλογών ακολουθουμένων προαιρετικά από την επιλογή «critical».

Οι χρήστες που θέλουν να λάβουν υπηρεσίες ιδιωτικότητας πρέπει να κατευθύνουν τα μηνύματα-αιτήσεις τους στο Δ.Π.Ι. της Α.Α. που συνεργάζεται με την εταιρεία παροχής υπηρεσιών, έχοντας συμπληρώσει το κατάλληλο πεδίο στην επικεφαλίδα Privacy, ανάλογα με το επίπεδο υπηρεσίας που επιθυμούν να λάβουν. Καθώς θεωρούμε ότι όλες οι εταιρίες παροχής υπηρεσίας που θέλουν να παρέχουν εγγυημένες υπηρεσίες στους πελάτες τους, θα συνεργάζονται με μια Α.Α., είναι βέβαιη η παρουσία τουλάχιστον ενός διακομιστή στη διαχειριστική οντότητα της εταιρείας με τη διεύθυνση IP, ή το hostname του να είναι γνωστό στους πελάτες της, ενώ η ταυτότητα του κατά την επικοινωνία θα πιστοποιείται από ένα ψηφιακό πιστοποιητικό της Α.Α. Για την περαιτέρω διασφάλιση των χρηστών κατά την επικοινωνία με τον διακομιστή της Α.Α. προτείνεται η χρήση ενός ασφαλούς πρωτοκόλλου επιπέδου μεταφοράς, όπως το TLS. Μ' αυτόν τον τρόπο ο χρήστης θα μπορεί να επιβεβαιώσει το ψηφιακό πιστοποιητικό του διακομιστή, ενώ τα προσωπικά του στοιχεία θα προστατεύονται τόσο από παρακολούθηση, όσο και από παραποίηση πριν την επεξεργασία τους από το διακομιστή.

Σύμφωνα με το RFC 3323 η λειτουργία του διακομιστή ιδιωτικότητας, ο οποίος γενικά δρα σαν ένας ακόμα Ενδιάμεσος Διακομιστής SIP, έχει ως εξής:

a. Λαμβάνει όλα τα μηνύματα-αιτήσεις από τους χρήστες και εξετάζει την επικεφαλίδα «Privacy» για να προσδιορίσει το επίπεδο προστασίας της ιδιωτικότητας που επιθυμεί ο χρήστης. Αν το μήνυμα δεν περιέχει επικεφαλίδα «Privacy» ο διακομιστής θα εφαρμόζει κάποιες προεπιλεγμένες επιλογές της εταιρείας παροχής υπηρεσίας ή του ίδιου του χρήστη.
b. Εφαρμόζει τις λειτουργίες για κάθε επίπεδο ιδιωτικότητας που αιτείται, όπως ορίζονται παραπάνω, ενώ δεν εφαρμόζει καμία στην περίπτωση της επιλογής none. Επιπλέον, αν υπάρχει η επιλογή «critical» και δεν μπορέσει να εφαρμόσει όλες τις λειτουργίες για κάποιο λόγο, τότε ο διακομιστής πρέπει να απορρίψει την αίτηση και να επιστρέψει το κατάλληλο μήνυμα (500 Server Error) στο χρήστη παρέχοντας πληροφορίες για το λόγο της αποτυχίας.

c. Μετά την υλοποίηση των λειτουργιών ο διακομιστής θα πρέπει να αφαιρέσει την επικεφαλίδα «Privacy» αφού ο σκοπός της επιτελέστηκε, διότι περαιτέρω παρουσία της στο μήνυμα αποκαλύπτει ανεπιθύμητες πληροφορίες.

Γενικά οι χρήστες θα πρέπει να περιλαμβάνουν σε κάθε μήνυμα-αίτηση την επικεφαλίδα «Privacy» για να δηλώσουν ρητά τις προτιμήσεις τους έτσι ώστε η υπηρεσία ανωνυμίας να εφαρμόζεται ρητά και να μη βασίζονται σε προκαθορισμένες πολιτικές της Α.Α.. Από την άλλη πλευρά οι χρήστες θα μπορούν να έχουν προεπιλέξει συγκεκριμένα επίπεδα ανωνυμίας ανάλογα με τις παραμέτρους της κάθε κλήσης (π.χ. το όνομα του παραλήπτη) κάτι που βοηθάει σε περιπτώσεις που το τερματικό του χρήστη (UA) δεν υποστηρίζει τη χρήση της επικεφαλίδας «Privacy».

3.2 Άξονες Σχεδίασης της Αρχιτεκτονικής

Σε αυτή την παράγραφο παρουσιάζονται οι βασικές σχεδιαστικές απαιτήσεις που πρέπει να ικανοποιεί το προτεινόμενο σύστημα και οι οποίες παρουσιάζονται με σειρά προτεραιότητας. Σχεδιαστικές επιλογές για την ικανοποίησης μιας εξ' αυτών γίνονται δεκτές μόνο εφόσον δεν επηρεάζουν την υλοποίηση ανώτερης απαίτησης στην ιεραρχία:

- Εφαρμογή της νομοθεσίας και συνυπολογισμός των απαιτήσεων του κράτους

Βασική προτεραιότητα στη σχεδίαση της αρχιτεκτονικής του τροποποιημένου συστήματος τηλεφωνίας, μέσω διαδικτύου, είναι η εφαρμογή της νομοθεσίας προστασίας προσωπικών δεδομένων, η οποία αποτελεί τον κύριο λόγο, που θα πρέπει να γίνουν τροποποιήσεις στην υπάρχουσα αρχιτεκτονική ώστε να ικανοποιούνται οι αυξημένες λειτουργικές απαιτήσεις. Η νομοθεσία για το απόρρητο των τηλεπικοινωνιών επιβάλλει να προστατεύονται ανά πάσα στιγμή οι ταυτότητες των μελών μιας τηλεφωνικής κλήσης, αλλά ταυτόχρονα να διατηρείται η πληροφορία για ένα συγκεκριμένο χρονικό διάστημα ώστε η δικαστική εξουσία να έχει πρόσβαση σ αυτήν για αρκετό καιρό. Η απαίτηση για παροχή εγγυήσεων προς όλες τις πλευρές για τη λειτουργία του συστήματος σημαίνει ότι η εφαρμογή της νομοθεσίας δεν μπορεί να βασίζεται σε πρακτικές καλής θέλησης των εταιρειών παροχής υπηρεσιών ούτε μπορεί να αρκεστεί στην απλή εφαρμογή business policies, αλλά σε μια τεχνική υποδομή, η οποία θα εξασφαλίζει την εφαρμογή της και θα παρέχει εγγυήσεις για τη λειτουργία. Μ' αυτόν τον τρόπο θα είναι σαφής ο καταμερισμός ευθυνών στα εμπλεκόμενα μέλη, οπότε σε περιπτώσεις παραβίασης θα διευκολύνεται η δικαιοσύνη στην ανεύρεση των υπεύθυνων.

Για τους παραπάνω λόγους υψίστη προτεραιότητα κατά τη σχεδίαση του συστήματος είναι η οργάνωση των επιμέρους τμημάτων του συστήματος VoIP και η ανάθεση σαφών ρόλων και λειτουργιών στις εμπλεκόμενες πλευρές (χρήστες, εταιρίες παροχής υπηρεσιών VoIP και Α.Α.) ώστε να εξασφαλίζεται η προστασία της ιδιωτικότητας του χρήστη, όπως επιβάλλεται από τις διατάξεις της νομοθεσίας. Σύμφωνα με τη βασική αρχιτεκτονική, που προτείνεται, γίνεται αντιληπτή η αναγκαιότητα ελέγχου της ροής μηνυμάτων SIP από τον αρμόδιο Δ.Π.Ι.. Το γεγονός αυτό επηρεάζει καθοριστικά την αρχιτεκτονική του συστήματος και απαιτείται προσεκτικός περαιτέρω σχεδιασμός ώστε τόσο η παρεχόμενη λύση να είναι, κατά το δυνατόν, εφαρμόσιμη, όσο και να μην εμφανίζονται κενά στη λειτουργία του συστήματος και παραβιάσεις των εγγυήσεων, που αυτό παρέχει. Η αποθήκευση των

κρίσιμων πληροφοριών του συστήματος θα πρέπει να κατανέμεται κατάλληλα μεταξύ των εμπλεκόμενων μελών, ώστε να μην είναι δυνατόν κάποιος μη εγκεκριμένος φορέας να την συγκεντρώσει και να βγάλει αξιόλογα συμπεράσματα.

Χαρακτηριστικό παράδειγμα της παραπάνω απαίτησης είναι η λίστα τηλεφωνικών κλήσεων κάθε χρήστη, η οποία αφενός θα πρέπει να διατηρείται για τις περιπτώσεις που αίρεται το απόρρητο των τηλεπικοινωνιών για λόγους εθνικής ασφάλειας ή εγκλημάτων κατά της ζωής, όπως επιβάλλει η νομοθεσία και αφετέρου θα πρέπει να είναι απόρρητη, έτσι ώστε ούτε η ίδια η εταιρεία, που παρέχει την υπηρεσία, να έχει πρόσβαση σ' αυτήν. Ταυτόχρονα, το μοντέλο λειτουργίας της εταιρείας, που προβλέπει η χρέωση να γίνεται ανά κλήση, επιβάλλει την παρακολούθηση της εξέλιξης της κλήσης από ενδιάμεσο διακομιστή της εταιρείας, αυξάνοντας μ' αυτόν τον τρόπο την πολυπλοκότητα της λύσης . Για να ικανοποιηθούν αυτές οινα λληλοαντικρουόμενες απαιτήσεις επιλέχτηκε ένας μηχανισμός που βασίζεται σε ψευδώνυμα και θα αναλυθεί στη συνέχεια του κεφαλαίου. Αυτό σημαίνει ότι η εταιρεία θα διατηρεί τη συνολική λίστα κλήσεων, αλλά τα συμβαλλόμενα μέλη κάθε κλήσης θα εμφανίζονται με τυχαία ψευδώνυμα, ενώ η Α.Α. θα διατηρεί τη συσχέτιση ψευδωνύμων και πραγματικών ονομάτων. Μ' αυτόν τον τρόπο μόνο ο συνδυασμός των δύο πληροφοριών, που προέρχονται από διαφορετικές πηγές, θα αποκαλύψει χρήσιμες πληροφορίες.

- Παροχή εγγυήσεων στους χρήστες για την προστασία των προσωπικών τους δεομένων, ακόμα και στις πιο ακραίες περιπτώσεις με τους πελάτες να μην εμπιστεύονται την εταιρεία παροχής της υπηρεσίας, αλλά και κατά περίπτωση ούτε τους άλλους πελάτες με τους οποίους επικοινωνούν.

Η συγκεκριμένη απαίτηση αποτελεί και τη διαφοροποίηση της συγκεκριμένης λύσης σε σχέση με τις ήδη υπάρχουσες. Ενώ στα υπάρχοντα συστήματα η προστασία της ιδιωτικότητας ανήκει κυρίως στο επιχειρηματικό μοντέλο, όπου ζητείται από τους χρήστες να εμπιστευθούν ότι η εταιρεία παροχής υπηρεσίας δεν θα δημοσιοποιήσει τα προσωπικά τους στοιχεία, στη σχεδιαζόμενη αρχιτεκτονική η προστασία της ιδιωτικότητας του χρήστη διασφαλίζεται με τεχνικές λύσεις. Οποιοσδήποτε προσπαθήσει να έχει πρόσβαση στα προσωπικά δεδομένα ελέγχεται από τη νομοθεσία και από τον ίδιο το χρήστη. Οι μόνοι που είναι εξουσιοδοτημένοι να έχουν πρόσβαση είναι ο ίδιος ο χρήστης και οι ανεξάρτητες αρχές που προβλέπονται από τη νομοθεσία για τις περιπτώσεις που αίρεται το απόρρητο των επικοινωνιών (lawful interception) [8]-[12]. Ταυτόχρονα, θα παρέχεται πολύ συγκεκριμένη διεπαφή και τρόπος πρόσβασης των παραπάνω στα δεδομένα ώστε να εξασφαλιστεί ο μηδενισμός των παραβιάσεων της ιδιωτικότητας.

Η προστασία που παρέχει το σύστημα δεν θα πρέπει να αναφέρεται μόνο απέναντι στις εταιρίες παροχής υπηρεσιών, αλλά και απέναντι σε τρίτους χρήστες της υπηρεσίας. Εξασφαλίζουμε έτσι την ιδιωτικότητα των χρηστών απέναντι σε κακόβουλους τρίτους ή κάποιον οργανισμό που θα μπορούσε, δημιουργώντας πλαστούς χρήστες, να έχει πρόσβαση σε προσωπικά δεδομένα. Αυτό σημαίνει ότι μόνο τα απολύτως απαραίτητα προσωπικά δεδομένα θα αποκαλύπτονται σε έμπιστους τρίτους χρήστες και αυτό μόνο μετά από ρητή εντολή-επιλογή του χρήστη. Στις υπόλοιπες περιπτώσεις ο χρήστης θα έχει πλήρη ανωνυμία απέναντι στα μέλη με τα οποία επικοινωνεί.

Συνοψίζοντας: οι απαιτήσεις προστασίας που θα παρέχει το σύστημα είναι όσο το δυνατόν πιο αυστηρές, αφού αναμένεται ότι, αν κάποιος μπορεί να έχει πρόσβαση σε προσωπικά δεδομένα κάποιου τρίτου, θα το εκμεταλλευτεί κακόβουλα. Θεωρούμε, λοιπόν,

ότι τα μόνα ασφαλή σημεία για την προσωπική πληροφορία είναι το τερματικό του ίδιου του χρήστη, οι διακομιστές της Α.Α. και κατά περίπτωση τρίτοι χρήστες, που δηλώνονται ρητά από τον κάτοχο της προσωπικής πληροφορίας. Όλα τα υπόλοιπα σημεία του συστήματος αποτελούν πιθανά σημεία παραβίασης της ιδιωτικότητας.

- Διατήρηση αναλλοίωτου του επιχειρηματικού μοντέλου της εταιρείας.

Μ' αυτή την απαίτηση θέλουμε να τονίσουμε την προσπάθεια για όσο το δυνατόν μικρότερη παρέμβαση στη λειτουργία της εταιρείας παροχής της υπηρεσίας. Αν το προτεινόμενο σύστημα απαιτούσε για την επίτευξη προστασίας της ιδιωτικότητας εκτεταμένες αλλαγές στο επιχειρηματικό μοντέλο της εταιρείας, που θα το εφαρμόσει, η υιοθέτηση του θα ήταν πολύ δύσκολη αν όχι αδύνατη. Σίγουρα η προστασία της ιδιωτικότητας σ' όλα τα επίπεδα είναι μια πολύπλοκη διαδικασία και απαιτεί ορισμένες αλλαγές και στο επιχειρηματικό μοντέλο ωστόσο έγινε κάθε δυνατή προσπάθεια οι αλλαγές αυτές να είναι οι ελάχιστες δυνατές.

Η συγκεκριμένη απαίτηση επηρεάζει σημαντικά την τελική σχεδίαση του συστήματος καθώς η προστασία της ιδιωτικότητας του χρήστη θα πρέπει να επιτυγχάνεται με ταυτόχρονη διατήρηση του ρόλου, που έχει η εταιρεία παροχής υπηρεσιών στο σύστημα. Η ανάθεση πολλών λειτουργιών στην Α.Α., αν και θα καθιστούσε πιο εύκολο το σχεδιασμό, δεν αποτελεί πραγματική λύση, καθώς τελικά η υπηρεσία θα παρεχόταν σχεδόν εξ ολοκλήρου από αυτή και η εταιρεία θα είχε απλά ένα τυπικό ρόλο, κάτι που δεν είναι ούτε επιθυμητό ούτε υλοποιήσιμο. Γίνεται λοιπόν αντιληπτό ότι η επιτυχία σ' αυτόν το σχεδιαστικό άξονα επιτρέπει την ευρεία εφαρμογή της λύσης, καθώς και την οικονομική βιωσιμότητα της εταιρείας, η οποία την παρέχει.

- Ελαχιστοποίηση των λειτουργιών και του υλικού που βρίσκεται υπό τη διαχειριστική ευθύνη της Α.Α.

Όπως αναφέρθηκε παραπάνω η εξασφάλιση της ιδιωτικότητας του χρήστη υλοποιείται με την παρεμβολή στην επικοινωνία ενός κόμβου υπό τη διαχειριστική ευθύνη της Α.Α. Επειδή κάθε πάροχος θα πρέπει να ενσωματώσει στο σύστημά του έναν τέτοιο κόμβο και μάλιστα αυτός θα πρέπει να ελέγχει όλη τη ροή μηνυμάτων SIP προς την εταιρεία, η Α.Α θα έχει ένα σεβαστό διαχειριστικό φορτίο. Οι απαιτήσεις σε επιπλέον υποδομή και προσωπικό, που μεταφράζονται σε αυξημένα λειτουργικά κόστη, θα επιβαρύνουν την εταιρεία παροχής της υπηρεσίας και γι' αυτόν το λόγο θα πρέπει να είναι τα ελάχιστα δυνατά. Επίσης, για να μπορέσει να λειτουργεί αποδοτικά το σύστημα και να μην παρουσιάζεται στενωπός επίδοσης στον κόμβο της Α.Α., θα πρέπει οι λειτουργίες, που αυτός επιτελεί, να είναι όσο το δυνατόν λιγότερες. Άλλωστε, η Α.Α θα είναι υπεύθυνη μόνο για την εξασφάλιση της προστασίας των χρηστών και δεν θα πρέπει να απασχολείται με λειτουργικά καθήκοντα που αφορούν την παροχή της υπηρεσίας. Σύμφωνα με αυτές τις παραμέτρους, κατά τον σχεδιασμό του συστήματος λαμβάνεται μέριμνα ώστε οι λειτουργίες και το υλικό που βρίσκονται υπό τη διαχειριστική ευθύνη της Α.Α να είναι οι ελάχιστες που επιτρέπουν την εξασφάλιση των επιθυμητών εγγυήσεων.

- Ελαχιστοποίηση των αλλαγών στην υπάρχουσα αρχιτεκτονική του SIP, ώστε το υλικό και το λογισμικό που ήδη υπάρχει στην αγορά να μπορεί να προσαρμοστεί γρήγορα και αποδοτικά σ' αυτές.

Είναι γεγονός ότι η χρήση του πρωτόκολλου SIP είναι ευρύτατα διαδεδομένη. Οι εταιρείες παροχής υπηρεσιών διαδικτυακής τηλεφωνίας έχουν κάνει σημαντικότατες επενδύσεις σε υποδομή, που υποστηρίζει την αρχιτεκτονική SIP, μια υποδομή που δεν μπορεί εύκολα να καταστεί άχρηστη σε περίπτωση που πρέπει να υλοποιηθεί προστασία της ιδιωτικότητας του χρήστη. Ταυτόχρονα, από την πλευρά των χρηστών υπάρχει πολύ μεγάλη εγκατεστημένη βάση σε λογισμικό, αλλά και υλικό τερματικών ,τα οποία κάνουν χρήση της υπάρχουσας τεχνολογίας. Ο σχεδιασμός της νέας αρχιτεκτονικής γίνεται με γνώμονα τη δυνατότητα πρακτικής εφαρμογής, κάτι που δεν θα ήταν δυνατόν, αν η εφαρμογή της απαιτούσε εκτεταμένες αλλαγές στην υπάρχουσα υποδομή υλικού και λογισμικού. Για τον παραπάνω λόγο επιλέγεται η επέκταση της υπάρχουσας υποδομής για την κάλυψη των νέων απαιτήσεων και όχι η ανάπτυξη ενός νέου πρωτοκόλλου.

Η συγκεκριμένη απαίτηση επηρεάζει το σχεδιασμό του συστήματος καθώς καθιστά υποχρεωτική την επιλογή λύσεων που βασίζονται στην υπάρχουσα τεχνολογία, ακόμα και αν αυτές οι λύσεις δεν είναι οι καλύτερες δυνατές τόσο σε ευκολία ανάπτυξης, όσο και σε αποδοτικότητα. Το πρωτόκολλο SIP δεν σχεδιάστηκε με γνώμονα την προστασία της ιδιωτικότητας και γι αυτό το λόγο οι πιθανές επεκτάσεις του θα είναι λιγότερο αποδοτικές σε σχέση με τη σχεδίαση μιας νέας αρχιτεκτονικής . Ωστόσο η εκτεταμένη υπάρχουσα υποδομή στις εταιρείες παροχής υπηρεσιών και τους χρήστες καθιστά αυτήν τη λύση μονόδρομο.

- Ευελιξία κατά την επιλογή προτιμήσεων προστασίας ιδιωτικότητας από τους χρήστες στο εξεταζόμενο περιβάλλον.

Για να παρασχεθεί η υπηρεσία της διαδικτυακής τηλεφωνίας ο χρήστης θα πρέπει να δημιουργήσει ένα προφίλ, ώστε να μπορεί να διαχειρίζεται το λογαριασμό του και να έχει πρόσβαση σε στοιχεία χρέωσης, στη λίστα κλήσεών του και γενικά σε στοιχεία που αφορούν τον ίδιο. Όπως περιγράψαμε και σε προηγούμενη παράγραφο, ανάλογα με τις υπηρεσίες που έχει επιλέξει η εταιρεία να συνδυάσει με τη διαδικτυακή τηλεφωνία (π.χ. κοινωνική δικτύωση), στο προφίλ του πελάτη μπορούν να αποθηκευτούν περισσότερα προσωπικά δεδομένα πέρα από τα ελάχιστα δυνατά που απαιτούνται για τη χρέωση του. Όπως επιβάλλει η νομοθεσία ο χρήστης θα πρέπει να έχει τον απόλυτο έλεγχο: στο ποιος έχει πρόσβαση στα προσωπικά δεδομένα του, τι επεξεργασία θα γίνεται σ' αυτά, ενώ θα πρέπει να έχει την δυνατότητα να τα αποσύρει άμεσα αν το επιθυμήσει. Ταυτόχρονα, κατά την πραγματοποίηση κλήσεων θα πρέπει να δίνεται η δυνατότητα στους χρήστες να επιλέγουν το επίπεδο ανωνυμίας, που θα τους παρέχεται ανά κλήση. Οι παραπάνω επιλογές θα πρέπει να πραγματοποιούνται με κάποιον ευέλικτο και αποδοτικό τρόπο ώστε και η εταιρεία να μπορεί να εφαρμόζει το επιχειρηματικό της μοντέλο, αλλά και να εξασφαλίζονται τα νομικά δικαιώματα των χρηστών.

Τέλος, θα πρέπει να αναφέρουμε κάποιες απαιτήσεις, που προκύπτουν γενικά από την εφαρμογή της προστασίας της ιδιωτικότητας στην τηλεφωνία VoIP:

- Οι χρήστες μπορεί να έχουν το δικαίωμα να απαιτήσουν την προστασία της ανωνυμίας τους και των συνεπαγόμενων προσωπικών πληροφοριών κατά την παροχή της υπηρεσίας καθώς και να απαιτήσουν εγγυήσεις για την υλοποίηση αυτής, αλλά το σύστημα και οι τελικοί παραλήπτες διατηρούν το δικαίωμα να απορρίψουν μηνύματα για τα οποία δεν μπορεί να ταυτοποιηθεί ο αποστολέας. Αυτό σημαίνει ότι ο χρήστης επιλέγοντας την παροχή ανωνυμίας αποδέχεται το γεγονός ότι σε ορισμένες περιπτώσεις η παροχή της υπηρεσίας θα είναι αδύνατη λόγω αυτής της επιλογής του και η εταιρεία δεν φέρει καμία ευθύνη για αυτό.
- Οι χρήστες μπορεί να μην είναι πάντα οι καλύτεροι κριτές για το πότε χρειάζονται μια υπηρεσία ανωνυμίας ακόμα και κάτω από ιδανικές συνθήκες και για αυτό το λόγο πρέπει να εφαρμόζονται κάποιες προκαθορισμένες πολιτικές προστασίας από τις εταιρίες και τις συνεργαζόμενες Α.Α. ώστε ακόμα και όταν ο χρήστης δεν ζητά ρητά την παροχή ανωνυμίας, ή το τερματικό του δεν υποστηρίζει τη συγκεκριμένη λειτουργία, να παρέχεται ένα ελάχιστο επίπεδο προστασίας ιδιωτικότητας.

Λόγω της πολυπλοκότητας που εισάγει η προστασία της ιδιωτικότητας στο σύστημα, αλλά και της πιθανότητας απόρριψης ανωνύμων μηνυμάτων από ενδιάμεσους διακομιστές ή παραλήπτες, λόγω ανωνυμίας, ο χρήστης θα πρέπει κάθε φορά να αιτείται ακριβώς το επίπεδο ανωνυμίας, που χρειάζεται, από το σύστημα για τη συγκεκριμένη αίτηση και όχι το μέγιστο δυνατό. Αν ο χρήστης δεν χρειάζεται καμία υπηρεσία ανωνυμίας τότε μπορεί να χρησιμοποιήσει και την πραγματική IP του για την κλήση, αποφεύγοντας την καθυστέρηση που επιφέρει μια υπηρεσία ανώνυμης διεύθυνσης IP.

3.3 Ζητήματα προστασίας προσωπικών δεδομένων και μεθοδολογίες επίλυσης

Στη συνέχεια του παρόντος κεφαλαίου αναλύονται τα επιμέρους ζητήματα που ανακύπτουν από την εφαρμογή της προστασίας της ιδιωτικότητας σ’ ένα σύστημα VoIP βασισμένο στο SIP. Σ’ αυτή την ανάλυση έχουν γίνει οι παρακάτω παραδοχές:

- Ο κάθε χρήστης του συστήματος, καθώς και οι διαχειριστικές οντότητες που εμπλέκονται στη λειτουργία του, κατέχουν ένα ζεύγος ιδιωτικού και δημοσίου κλειδιού καθώς και ένα ψηφιακό πιστοποιητικό, το οποίο πιστοποιεί την ταυτότητα και το δημόσιο κλειδί τους.
- Οι δομικές μονάδες του συστήματος μπορούν να έχουν πρόσβαση στο δημόσιο κλειδί οποιουδήποτε χρήστη, μέσω κάποιου καταλόγου ώστε να μπορεί να χρησιμοποιηθεί για επίτευξη ασφαλούς επικοινωνίας μ’ αυτόν.
- Υπάρχει τηλεφωνικός κατάλογος στον οποίο αντιστοιχίζονται τα φυσικά πρόσωπα με τα SIP URI AOR τους.

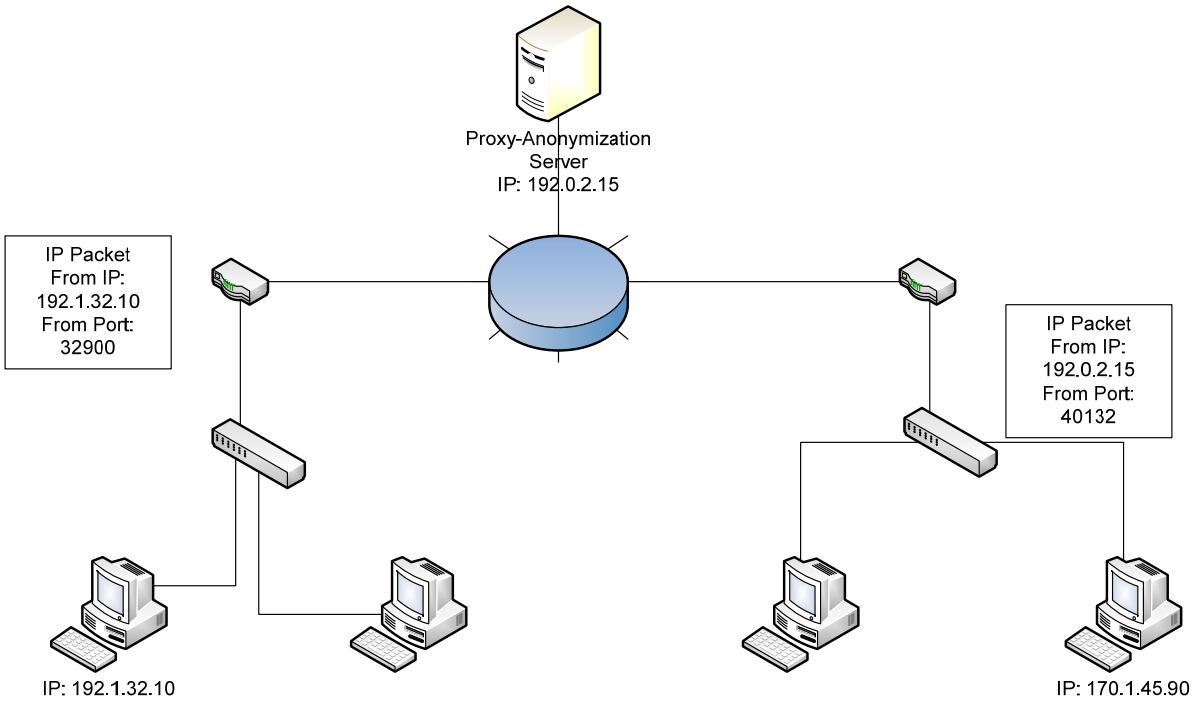
- Οι δομικές μονάδες χρησιμοποιούν πρωτόκολλα ασφαλούς επικοινωνίας (SIPS, TLS) και γενικά λαμβάνουν τις απαραίτητες ενέργειες διασφάλισης της κίνησης στο δίκτυο.
- Στις επικεφαλίδες των μηνυμάτων SIP και όπου αυτό προβλέπεται γίνεται χρήση διευθύνσεων IP και όχι hostnames, αφού η χρήση των τελευταίων θα περιέπλεκε την προστασία της ιδιωτικότητας, λόγω της εμπλοκής του συστήματος DNS στη διαδικασία. Σ' αυτή την περίπτωση θα έπρεπε να πραγματοποιηθούν εκτεταμένες αλλαγές στο σύστηνα ώστε και το DNS να υποστηρίζει ονόματα που υλοποιούν προστασία της ιδιωτικότητας (privacy-aware hostnames).

3.3.1 Προστασία Διεύθυνσης IP

Οι πρωτοπόροι του διαδικτύου πίστευαν ότι αυτό θα ήταν το απόλυτο ανώνυμο και ελεύθερο μέσο επικοινωνίας. Αρκετά χρόνια αργότερα η πείρα έχει δείξει ότι τελικά η ιδέα της ανωνυμίας, αλλά και της ελευθερίας, απέχει πολύ από την πραγματικότητα. Το πρωτόκολλο IP που χρησιμοποιείται γα τη δρομολόγηση των πακέτων στο διαδίκτυο πέτυχε λόγω της απλότητας του, με αποτέλεσμα όμως να μην παρέχεται καμιά επιπλέον υπηρεσία στο επίπεδο δικτύου. Ακόμα και η υποστήριξη μιας υπηρεσίας ασφάλειας θα εφαρμόζεται μόνο στο IPv6. Ως εκ τούτου η διεύθυνση IP που χρησιμοποιείται από κάποιο χρήστη για τη λήψη μιας υπηρεσίας και αποτελεί προσωπικό του δεδομένο, αφού αποκαλύπτει πολλές φορές στοιχεία, όπως γεωγραφική τοποθεσία, πάροχο ISP κ.α., δεν προστατεύεται εγγενώς με κανένα τρόπο. Η κατάσταση είναι χειρότερη για τους οικιακούς χρήστες, οι οποίοι λαμβάνουν διευθύνσεις IP και σύνδεση με το διαδίκτυο ένα συγκεκριμένο ISP, καθώς ο ISP κρατάει πληροφορίες για τη διεύθυνση IP που παρέχει στους χρήστες ανά πάσα στιγμή, μαζί με τα πλήρη στοιχεία τους. Παρ' όλο που αυτά τα στοιχεία προστατεύονται από το απόρρητο των τηλεπικοινωνιών, η πληροφορία είναι πολύ σημαντική για να βρίσκεται όλη αποθηκευμένη στον ISP, αφού σε συνδυασμό με το είδος της πληροφορίας, που μεταφέρεται, αποκαλύπτεται το είδος υπηρεσιών που χρησιμοποιεί ο χρήστης. Ειδικά στο πρωτόκολλο SIP οι διευθύνσεις IP μεταφέρονται αυτούσιες στο εσωτερικό των μηνυμάτων και μπορούν να χρησιμοποιηθούν για την ταυτοποίηση των χρηστών. Για τον παραπάνω λόγο η παροχή ανωνυμίας στο πρωτόκολλο SIP θα επιτυγχάνεται μόνο σε συνδυασμό με την ύπαρξη ανωνυμίας στο επίπεδο δικτύου. Τα τελευταία χρόνια έχουν προταθεί αρχιτεκτονικές και υπηρεσίες ανωνυμίας της διεύθυνσης IP στο διαδίκτυο με τις δύο πιο χαρακτηριστικές να περιγράφονται στη συνέχεια.

3.3.1.1 Χρήση ενδιάμεσων διακομιστών (Proxy servers)

Η πρώτη αρχιτεκτονική που προσέφερε ανωνυμία IP ήταν η χρήση ενδιάμεσων διακομιστών που μετατρέπουν τις διευθύνσεις IP και τις TCP/UDP πόρτες του αποστολέα σε διαφορετικές, ενώ διατηρούν μια αντιστοίχιση ώστε να προωθήσουν τις απαντήσεις πίσω στον αποστολέα.



Εικόνα 8: Χρήση ενδιάμεσου διακομιστή για παροχή ανωνυμίας IP

Συγκεκριμένα, η αρχιτεκτονική αυτή αξιοποιεί την ίδια ιδέα με τα συστήματα NAT, εκμεταλλεύεται δηλαδή την ύπαρξη δεδομενογραφημάτων TCP ή UDP στο φορτίο των πακέτων, ώστε να αντικαταστήσει τη διεύθυνση IP και την πόρτα αποστολέα με τη διεύθυνση IP του διακομιστή και μια τυχαία επιλεγμένη μη χρησιμοποιούμενη πόρτα, όπως φαίνεται στο σχήμα (αντικατάσταση 192.1.32.10:32900 με 192.0.2.15:40132). Στη συνέχεια, το μήνυμα προωθείται στον τελικό παραλήπτη. Αντίστοιχα, όταν φτάσει η απάντηση στην επιλεγμένη πόρτα, ο διακομιστής αντικαθιστά τα πεδία και προωθεί το μήνυμα στον αρχικό αποστολέα.

Στο διαδίκτυο υπάρχει αυτή τη στιγμή μια πληθώρα τέτοιων διακομιστών [24], οι οποίοι χρησιμοποιούνται κυρίως για την επίτευξη ανωνυμίας στο http, ενώ για την επίτευξη μεγαλύτερης ανωνυμίας δίνεται η δυνατότητα ένα μήνυμα να περάσει από περισσότερους του ενός διακομιστές για την καλύτερη προστασία της IP. Η διεθνής βιβλιογραφία περιέχει πολλά πρωτόκολλα με τα οποία οι χρήστες μπορούν να ζητήσουν την παροχή υπηρεσίας από έναν τέτοιο διακομιστή. Επίσης, εκτός από την περίπτωση ενός μηνύματος και της απόκρισης σ' αυτό, παρέχεται η δυνατότητα εγκαθίδρυσης ημιμόνιμων αντιστοιχίσεων ώστε οι χρήστες να μπορούν να είναι προσβάσιμοι από το υπόλοιπο διαδίκτυο. Για παράδειγμα: στις απλές περιπτώσεις αίτησης-απάντησης, όπως στο http, χρησιμοποιείται το πρωτόκολλο SOCKS [25], ενώ αν απαιτείται μια ημιμόνιμη σύνδεση, χρησιμοποιείται το STUN [26] και η επέκταση του το TURN [27], το οποίο προτείνεται [28] από την IETF για την παροχή προστασίας ιδιωτικότητας IP στο SIP. Το τελευταίο παρέχει πολλές δυνατότητες παραμετροποίησης για την αίτηση αντιστοίχισης, ανάλογα με την κίνηση που αναμένεται να μεταφερθεί μέσω του διακομιστή, καθώς και την δυνατότητα δημιουργίας ετικετών για μια συγκεκριμένη ροή δεδομένων ώστε να γίνεται γρηγορότερα η επεξεργασία των πακέτων, αν απαιτείται χαμηλή καθυστέρηση από τις εφαρμογές.

3.3.1.1.1 Υλοποίηση στο περιβάλλον διαδικτυακής τηλεφωνίας

Η συγκεκριμένη αρχιτεκτονική εμφανίζει σημαντικά μειονεκτήματα, τα οποία δεν την καθιστούν αποτελεσματική στην περίπτωση του SIP. Η Α.Α. είναι ο μοναδικός οργανισμός που μπορεί να αναλάβει τη διαχείριση και λειτουργία ενός τέτοιου διακομιστή, αφού αυτός περιέχει την πολύ κρίσιμη πληροφορία των αντιστοιχίσεων παλιών και νέων IP-port.

Στην περίπτωση όμως αυτή ανακύπτουν τα παρακάτω ζητήματα:

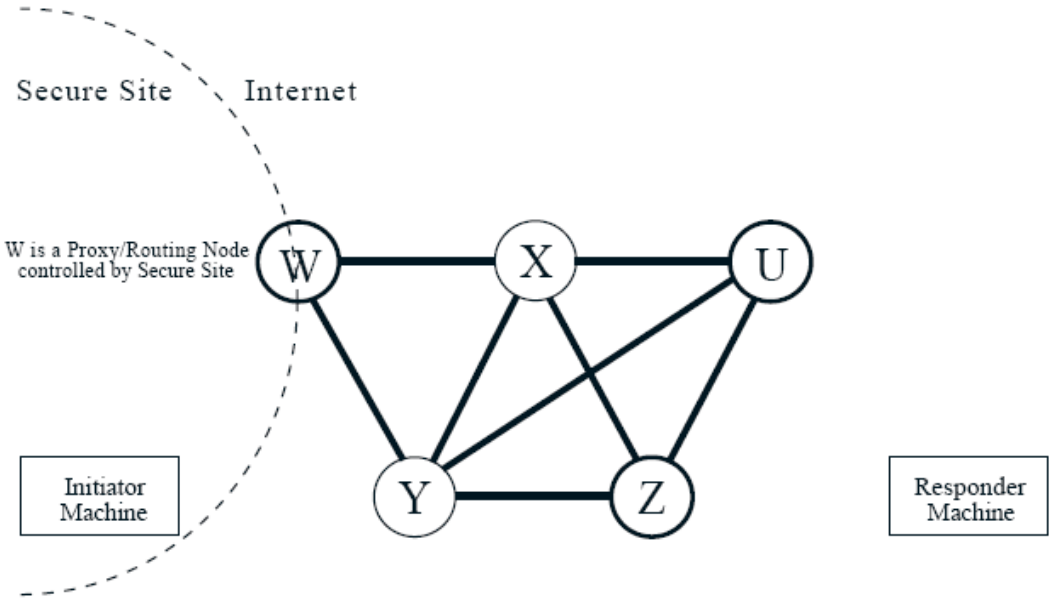
- Ο διακομιστής προστασίας IP αποτελεί σαφέστατα στενωπό του συστήματος αφού όλη η κίνηση πρέπει να δρομολογείται σ' αυτόν, και μοναδικό σημείο αποτυχίας του συστήματος καθώς, αν αποτύχει, δεν μπορεί να εκτελεσθεί η λειτουργία της προστασίας IP και θα παραβιαστούν τα προσωπικά δεδομένα των χρηστών ενώ και όλες οι εγκαθιδρυμένες σύνοδοι θα διακοπούν.
- Τα SIP UA τα οποία χρειάζονται την προστασία της διεύθυνσης IP τους δεν δρουν μόνο ως clients (UAC), αλλά και ως servers (UAS), αφού δεν ξεκινούν μόνο νέες αιτήσεις, αλλά αναμένουν και αιτήσεις προερχόμενες από το διαδίκτυο. Αυτό σημαίνει ότι δεν μπορεί να χρησιμοποιηθεί η τεχνική του NAT, η οποία δημιουργεί μια αντιστοιχία για κάθε απεσταλμένο πακέτο, αναμένοντας την απάντηση σ' αυτό. Εδώ οι αντιστοιχίσεις πρέπει να είναι μόνιμες ή ημιμόνιμες, ανάλογα με το πόσο συχνά εκτελεί SIP REGISTER ο χρήστης. Αυτό σημαίνει ότι ο κάθε ενδιάμεσος διακομιστής προστασίας IP θα μπορεί να υποστηρίζει μόνο 65000 περίπου χρήστες ταυτόχρονα σε κάθε interface για το οποίο έχει IP, δηλαδή όσος είναι και ο αριθμός πορτών εξόδου στο TCP/UDP. Φυσικά, η χρήση πολλαπλών interface μπορεί να αυξήσει αυτόν τον αριθμό, αλλά προφανώς η αρχιτεκτονική αυτή έχει πρόβλημα επέκτασης.
- Επιβάλλεται στην Α.Α. η διαχείριση ενός ακόμα πολύπλοκου κόμβου, κάτι που αντιβαίνει στους άξονες σχεδίασης μας.
- Η Α.Α. δεν μπορεί να υλοποιήσει έναν τέτοιο διακομιστή στο εσωτερικό δίκτυο της εταιρείας παροχής υπηρεσίας, αφού η εταιρεία μπορεί με ανάλυση της κίνησης (traffic analysis attack) να παραβιάσει το σύστημα και να μάθει τη διεύθυνση IP των χρηστών. Ακόμα και αν ο διακομιστής βρίσκεται εκτός του δικτύου της εταιρείας, η στατική θέση και η σταθερή IP του τον καθιστούν ευάλωτο στο συγκεκριμένο είδος επίθεσης.

  Η επίθεση με ανάλυση της κίνησης υλοποιείται με τον επιτιθέμενο να παρατηρεί τα πακέτα IP, που μεταφέρονται στο δίκτυο και να χρησιμοποιεί πληροφορίες, όπως το μέγεθος των πακέτων και οι χρονικές συσχετίσεις τους για να ανακαλύπτει ποιοι υπολογιστές επικοινωνούν μεταξύ τους. Θεωρείται από τις σημαντικότερες επιθέσεις στα θέματα ανωνυμίας, αφού ο επιτιθέμενος δεν χρειάζεται να δει καν το περιεχόμενο των μηνυμάτων για να εξάγει χρήσιμα συμπεράσματα.

3.3.1.2 Χρήση onion routing

Η ιδέα του onion routing [29] αποτελεί επέκταση της χρήσης μιας αλυσίδας ενδιάμεσων διακομιστών για την απόκρυψη της IP διεύθυνσης του αποστολέα ενός μηνύματος, παρέχοντας πρόσθετες λειτουργίες που διασφαλίζουν τον αποστολέα ακόμα και αν κάποιος ή κάποιοι από τους κόμβους δεν είναι έμπιστοι. Ταυτόχρονα, επειδή ως

πρωτόκολλο τοποθετείται μεταξύ του επιπέδου δικτύου και του επιπέδου μεταφοράς, μπορεί να εφαρμοστεί σε όλα τα πρωτόκολλα εφαρμογών, τα οποία χρησιμοποιούν ή μπορούν να χρησιμοποιήσουν έναν ενδιάμεσο διακομιστή.

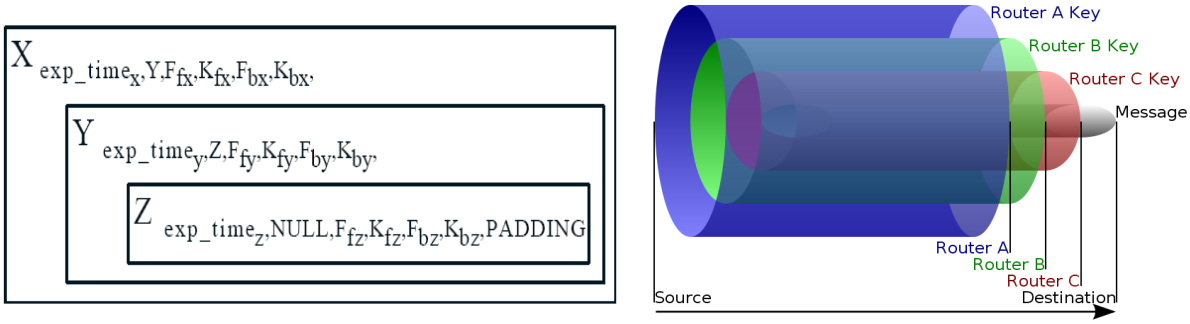


Εικόνα 9: Τοπολογία δικτύου βασισμένου στο onion routing

Οι κόμβοι οι οποίοι εφαρμόζουν το onion routing σχηματίζουν μεταξύ τους ένα επικαλύπτον δίκτυο (overlaid network) μεταγωγής ετικέτας (label switching) πάνω από το IP με τους χρήστες που θέλουν να το χρησιμοποιήσουν να συνδέονται με κάποιον από αυτούς και να ζητούν την εγκαθίδρυση ενός ασφαλούς κυκλώματος μέσω του δικτύου. Ο πρώτος κόμβος, ο οποίος ονομάζεται και κόμβος εισόδου, είναι κρίσιμος για τη λειτουργία του συστήματος καθώς αποφασίζει για όλα τα θέματα που αφορούν το onion routing και είναι ο πιο ευάλωτος σε επιθέσεις. Οι επόμενοι κόμβοι εκτελούν απλώς μια λειτουργία προώθησης με χρήση ετικετών, κρυπτογραφώντας ταυτόχρονα με τον κατάλληλο τρόπο τα δεδομένα.

Η βασική μεταφορική μονάδα στο onion routing είναι μια μορφή κρυπτογραφημένου πακέτου με πολλά επίπεδα κρυπτογράφησης (onion) . Βασική προϋπόθεση για τη λειτουργία του συστήματος είναι κάθε κόμβος του δικτύου να έχει ένα γνωστό δημόσιο και ένα ιδιωτικό κλειδί , τα οποία θα μπορούν να χρησιμοποιούνται κατά τη φάση εγκαθίδρυσης του κυκλώματος. Ο πρώτος κόμβος που λαμβάνει ένα μήνυμα, επιλέγει μια τυχαία διαδρομή στο onion δίκτυο και δημιουργεί κατάλληλα συμμετρικά κλειδιά για καθέναν από τους κόμβους που θα αποτελούν το κύκλωμα. Στη συνέχεια ανάλογα με τους κόμβους που θα επιλέξει κρυπτογραφεί το αρχικό μήνυμα διαδοχικά με τα αντίστοιχα δημόσια κλειδιά των κόμβων από τον τελευταίο προς τον πρώτο κόμβο της διαδρομής, προσθέτοντας σε κάθε επίπεδο του μηνύματος πληροφορίες που αφορούν το συγκεκριμένο κόμβο και προσδιορίζουν την ταυτότητα του επόμενου κόμβου, τη διάρκεια εγκαθίδρυσης του κυκλώματος, καθώς και τους αλγορίθμους και τα συμμετρικά κλειδιά, που θα χρησιμοποιηθούν για την επικοινωνία των δεδομένων. Ο κάθε κόμβος «ξεφλουδίζει» ένα επίπεδο κρυπτογράφησης από το εισερχόμενο μήνυμα και ανάλογα με τις πληροφορίες, που περιέχονται σ' αυτό αποθηκεύει τις τοπικές αντιστοιχίσεις του κυκλώματος και τα κατάλληλα συμμετρικά κλειδιά, που αφορούν στην επικοινωνία δεδομένων. Η κρυπτογράφηση της κίνησης με ισχυρότερα συμμετρικά κλειδιά επιλέγεται για μεγαλύτερη ασφάλεια και για να αποφευχθούν αδυναμίες του αλγορίθμου

δημοσίου RSA [29], που μπορούν να εκμεταλλευτούν επιτιθέμενοι. Τέλος, για τη διατήρηση του onion σε σταθερό μέγεθος με σκοπό την καλύτερη προστασία απέναντι στην ανάλυση κίνησης ο αρχικός χρήστης χρησιμοποιεί ένα padding, ενώ όλοι οι υπόλοιποι κόμβοι προσθέτουν στο τέλος του μηνύματος ένα τυχαίο αλφαριθμητικό ίσο με το μέγεθος της κεφαλίδας που αφαίρεσαν. Η εντολή που δημιουργεί ένα onion κύκλωμα είναι η «create».



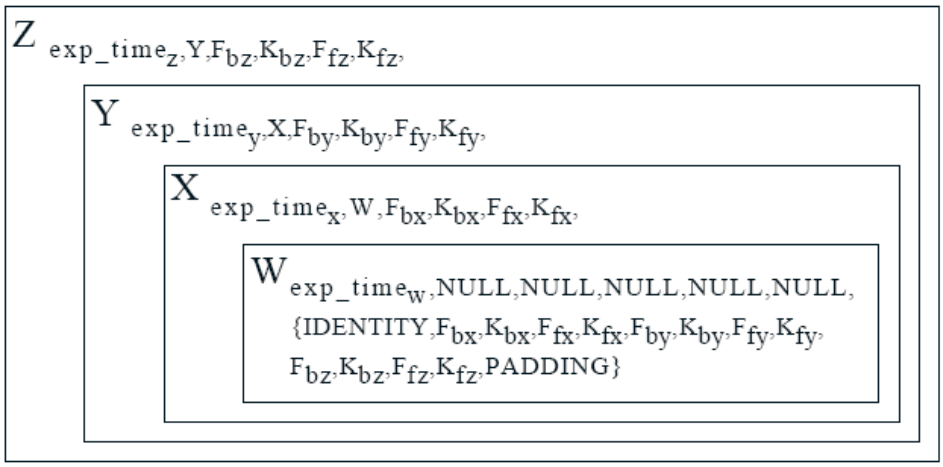
Εικόνα 10: Ένα πακέτο σε δίκτυο onion routing (onion)

Η μεταγωγή των πακέτων δεδομένων στο εγκατεστημένο κύκλωμα ακολουθεί τη θεωρία των δικτύων μεταφοράς με μεταγωγή ετικέτας, αφού κάθε κόμβος κρατάει μία τοπική αντιστοιχία μεταξύ της εισόδου και εξόδου για το κάθε κύκλωμα, καθώς και τα κλειδιά και τους αλγόριθμους κρυπτογράφησης που χρησιμοποιούνται σε κάθε ζεύξη. Όπως συμβαίνει στα δίκτυα μεταγωγής ετικέτας, ο κάθε κόμβος δεν γνωρίζει τίποτα για το υπόλοιπο δίκτυο εκτός από τον προηγούμενο και τον επόμενο κόμβο για κάθε κύκλωμα. Κάθε μήνυμα, που λαμβάνεται από έναν κόμβο αποκρυπτογραφείται (κρυπτογραφείται για την αντίστροφη διαδρομή) με το κλειδί που καθορίστηκε κατά την εγκατάσταση του κυκλώματος και στέλνεται στον επόμενο κόμβο. Ο αρχικός κόμβος ο οποίος είναι και ο μόνος που γνωρίζει όλα τα κλειδιά κρυπτογραφεί όλα τα επίπεδα για τα μηνύματα που εισάγει στο δίκτυο και αποκρυπτογραφεί όλα τα επίπεδα για τα μηνύματα που λαμβάνει ώστε να στείλει πίσω στο χρήστη το τελικό μήνυμα. Τα δεδομένα μεταφέρονται στο onion δίκτυο με την εντολή «data».

Τέλος, για την αποδέσμευση των κυκλωμάτων υπάρχει η εντολή «destroy». Εναλλακτικά το πεδίο exp_time που χρησιμοποιείται για την ανίχνευση επαναλήψεων και την προστασία απέναντι σε κάποιες επιθέσεις [29] καταδεικνύει τη διάρκεια που πρέπει να έχει το κύκλωμα. Οι επικεφαλίδες του onion που περιέχουν την ετικέτα κυκλώματος και την εντολή πρέπει να κρυπτογραφούνται ανά σύνδεση διαδοχικών δρομολογητών onion για την επίτευξη μέγιστης ασφάλειας έναντι τρίτων, αλλά ακόμα και αν το κλειδί της σύνδεσης παραβιαστεί ο εισβολέας μαθαίνει μόνο στοιχεία για το συγκεκριμένο κόμβο και απέχει πολύ από την αποκάλυψη της ταυτότητας του αποστολέα. Φυσικά, πρέπει να αναφέρουμε ότι η σύνδεση στο επίπεδο μεταφοράς από τον αποστολέα στον παραλήπτη πρέπει να κρυπτογραφείται, ανεξάρτητα από τη χρήση του onion routing, αφού σε αντίθετη περίπτωση τα δεδομένα από τον κόμβο εξόδου στον παραλήπτη θα μεταφέρονταν ως καθαρό κείμενο (plain text).

Μια επέκταση στο παραπάνω σύστημα ορίζει τα reply-onions, όπου ο ενδιαφερόμενος χρήστης μέσω του κόμβου εισόδου δημιουργεί ένα onion σαν αυτό που θα είχε δημιουργήσει ένας κόμβος εξόδου για να φτιάξει ένα κύκλωμα προς αυτόν. Η λογική που χρησιμοποιείται είναι ακριβώς η ίδια και μάλιστα οι ενδιάμεσοι κόμβοι δεν

αντιλαμβάνονται καμία διαφορά. Η μόνη διαφορά είναι ότι η εγκατάσταση του κυκλώματος θα γίνει από τον κόμβο εξόδου προς τον κόμβο εισόδου, επομένως το μόνο που έχει να κάνει ένας χρήστης, που θέλει να διαφημίσει μια ανώνυμη υπηρεσία, είναι να κατασκευάσει ένα reply-onion και να το τοποθετήσει κάπου, που οι ενδιαφερόμενοι θα μπορούν να το χρησιμοποιήσουν για να τον βρουν.



Εικόνα 11: Reply onion

Η χρησιμότητα των reply-onions στο SIP είναι εμφανής, αφού ο χρήστης μπορεί να δημιουργεί ένα reply onion κατά τη διαδικασία του REGISTER και ο Διακομιστής Θέσης SIP να αποθηκεύει την IP του κόμβου εξόδου μαζί με το reply-onion ώστε όταν υπάρχει κάποια εισερχόμενη κλήση για το χρήστη να εγκαθιδρύεται το ασφαλές κύκλωμα onion routing και να προωθείται η αίτηση σ' αυτόν. Φυσικά, πρέπει να εξασφαλιστεί ότι οι χρήστες, μέσω των οποίων υπολογίζεται να εγκαθιδρυθεί το ανώνυμο κύκλωμα, θα παραμείνουν σε λειτουργία, αλλά αυτές οι περιπτώσεις διαχείρισης του συστήματος, σε περίπτωση ιδιαζόντων καταστάσεων, ξεφεύγουν από τα πλαίσια της παρούσας διπλωματικής.

Η μέθοδος προστασίας IP μέσω onion routing εμφανίζει μεγάλα πλεονεκτήματα και ανθεκτικότητα σε γνωστές επιθέσεις, ενώ αποτελεί ένα πλήρως κατανεμημένο σύστημα με όλα τα πλεονεκτήματα απόδοσης και επεκτασιμότητας που αυτό συνεπάγεται. Φυσικά δεν είναι απόλυτα ασφαλές απέναντι σε επιθέσεις ανάλυσης κίνησης [29],[30], κυρίως λόγο του χρονικού συσχετισμού των πακέτων , αλλά και σε επιθέσεις κατάληψης ενδιάμεσων κόμβων του δικτύου onion, όπου η πιθανότητα να αποκαλυφθεί ένα κύκλωμα είναι μια συνάρτηση του κλάσματος c/n των κατειλημμένων κόμβων έναντι του συνόλου των κόμβων στο σύστημα. Πάντως, στις περισσότερες περιπτώσεις η κατάληψη ενός ενδιάμεσου κόμβου μπορεί να οδηγήσει σε επίθεση άρνησης υπηρεσίας (Denial of Service DoS). Είναι σαφές ότι η ύπαρξη πολλών διαφορετικών και γεωγραφικά απομακρυσμένων κόμβων στο σύστημα, αλλά και η ύπαρξη συνεχούς και σταθερής ροής δεδομένων προς όλους του κόμβους, βελτιώνει την απόδοση απέναντι σε επιθέσεις ανάλυσης κίνησης και προς αυτήν την κατεύθυνση κινείται η έρευνα στο συγκεκριμένο τομέα [30].

3.3.1.2.1 Υλοποίηση στο περιβάλλον διαδικτυακής τηλεφωνίας

Μια αρχιτεκτονική υλοποίησης του onion routing, στην περίπτωση του περιβάλλοντος της διαδικτυακής τηλεφωνίας, προτείνεται να είναι η δημιουργία ενός onion δικτύου με χρήση των UA όλων των χρηστών, ως κόμβους του και το Δ.Π.Ι. να αναλαμβάνει

το διαχειριστικό ρόλο. Μ' αυτόν τον τρόπο τα διαδικτυακά τηλέφωνα, που έτσι και αλλιώς τον περισσότερο χρόνο είναι σε κατάσταση αναμονής, περιμένοντας εισερχόμενες κλήσεις, θα αξιοποιούνται για την προστασία της ανωνυμίας όλων των χρηστών. Αυτό σημαίνει ότι ο κάθε χρήστης που επιθυμεί να λάβει υπηρεσία ανώνυμης IP θα ρωτάει το Δ.Π.Ι. για την ύπαρξη κόμβων στο σύστημα, που θα μπορούσε να χρησιμοποιήσει ως ενδιάμεσους κόμβους για τη δρομολόγηση των μηνυμάτων του. Αν υποθέσουμε ότι ο Δ.Π.Ι. βρίσκεται στο δίκτυο της εταιρείας παροχής υπηρεσίας και υπάρχει ανάγκη προστασίας ακόμα και της πληροφορίας αίτησης ανωνυμίας IP από ένα συγκεκριμένο χρήστη, τότε το ερώτημα αυτό θα γίνεται μέσω ενός δημόσιου ανώνυμου δικτύου για την προστασία της IP του αποστολέα ή μέσω κάποιων προεπιλεγμένων κόμβων. Ο Δ.Π.Ι. παρέχει μια λίστα ενεργών κόμβων στο χρήστη, ο οποίος στη συνέχεια επιλέγει τυχαία έναν αριθμό εξ αυτών και υπολογίζει τα κλειδιά για την επικοινωνία. Στη συνέχεια, εγκαθιστά το ανώνυμο κύκλωμα στο onion δίκτυο και τέλος στέλνει το μήνυμα REGISTER στο Διακομιστή Καταχώρισης Χρηστών SIP για να δημιουργήσει την αντιστοίχιση μεταξύ του URI του και της διεύθυνσης του κόμβου εξόδου που επέλεξε.

Εδώ υπάρχουν δύο δυνατότητες: είτε ο κόμβος εξόδου θα δεσμεύει μια πόρτα εξόδου για το κύκλωμα του χρήστη, οπότε δεν χρειάζεται να γίνει άλλη ενέργεια και όλο το υπόλοιπο σύστημα του SIP θα δουλεύει με τον ίδιο τρόπο, είτε θα στέλνεται ένα reply onion στο Διακομιστή Θέσης για χρήση στις περιπτώσεις αιτημάτων SIP προς το χρήστη. Η τελευταία όμως περίπτωση επιβάλλει κάποιες αλλαγές στο υπάρχον υλικό του SIP καθώς οι διακομιστές θα πρέπει να επεκταθούν για να υποστηρίζουν τη χρήση onions. Η Α.Α. θα πληροφορείται πάντα από το χρήστη για την επιλογή κόμβων, που έκανε και συγκεκριμένα για την επιλογή τελικού κόμβου ώστε να δημιουργείται η αντιστοίχιση των IP στο σύστημα και να υλοποιείται το τμήμα της νομοθεσίας, που επιβάλλει το κράτος να υπάρχει δυνατότητα πρόσβασης στα πλήρη στοιχεία μιας κλήσης για λόγους ασφαλείας. Η κοινοποίηση αυτή θα μπορεί να λαμβάνει χώρα κατά τη διάρκεια της πιστοποίησης του χρήστη από το Δ.Π.Ι.

3.3.1.3 Συμπεράσματα

Και οι δύο λύσεις, που αναφέραμε, είναι συμβατές με τη λειτουργία του SIP, αφού το UA του χρήστη γνωρίζει σε κάθε περίπτωση τον κόμβο εξόδου και μπορεί να βάλει την IP του στα αναγκαία πεδία του μηνύματος SIP ώστε να υλοποιείται η διαδικασία προώθησης των μηνυμάτων στους χρήστες.

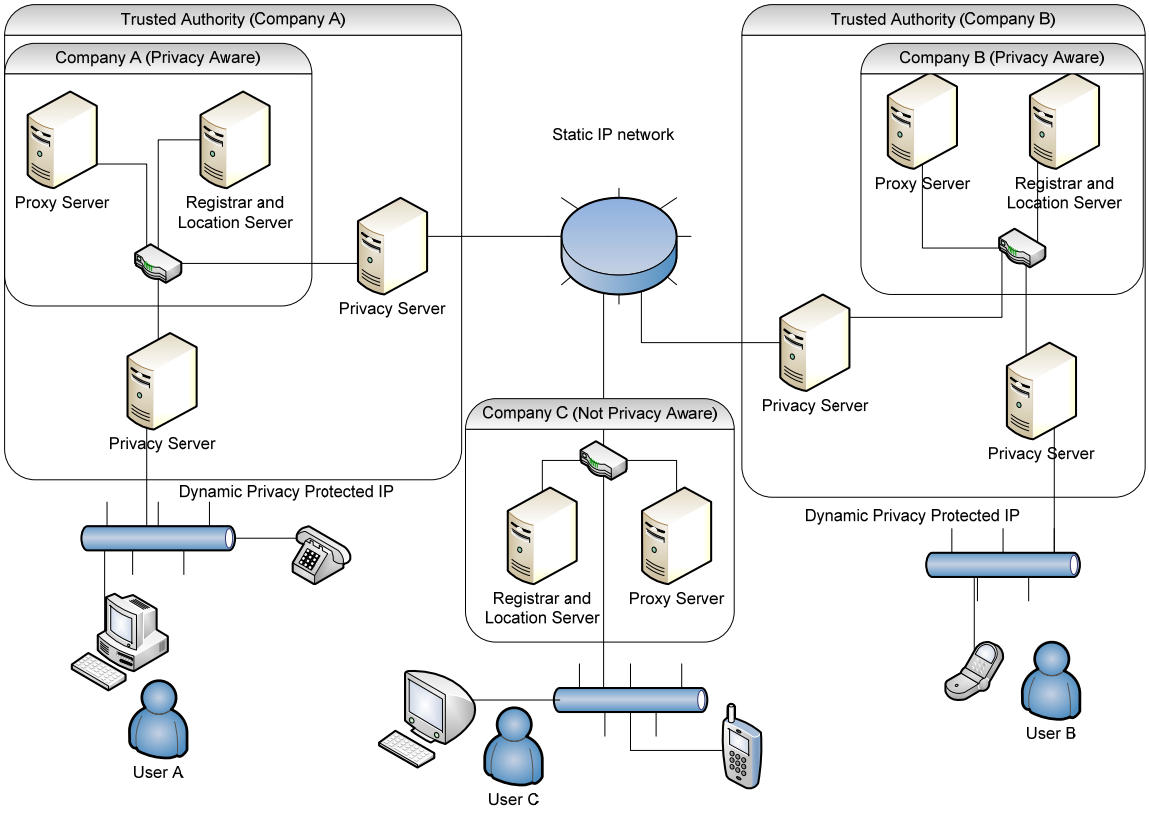
Το κανάλι ελέγχου του πρωτόκολλου SIP αποτελεί ιδανική περίπτωση για τη χρήση του onion routing, αφού δεν μεταφέρει δεδομένα πραγματικού χρόνου και χρονικές καθυστερήσεις, ακόμα και λίγων δευτερολέπτων, θεωρούνται αποδεκτές ενώ το φορτίο του είναι σχετικά μικρό. Αυτό σημαίνει ότι μπορούν να χρησιμοποιηθούν διάφορες τεχνικές της βιβλιογραφίας [30], που εισάγουν τεχνητές καθυστερήσεις στους κόμβους και χρήση αυξομειούμενου padding για την καλύτερη προστασία των χρηστών απέναντι σε επιθέσεις ανάλυσης κίνησης.

Αντίθετα, για το κανάλι δεδομένων είναι καλύτερα να χρησιμοποιηθεί ένας ειδικός ενδιάμεσος διακομιστής της Α.Α. (πιθανότατα μέσω χρήσης TURN), εκτός δικτύου της εταιρείας παροχής υπηρεσίας για την παροχή ανωνυμίας, αφού προσφέρει τη μικρότερη καθυστέρηση για δεδομένα πραγματικού χρόνου. Παρ' όλα αυτά η έρευνα προχωράει για την υλοποίηση δικτύων ανωνυμίας χαμηλής καθυστέρησης και πιθανότατα στο μέλλον θα μπορεί να χρησιμοποιηθεί ασφαλές onion routing και για το κανάλι δεδομένων.

3.3.2 Ζητήματα Προστασίας Ονομάτων στο SIP

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο ένα σημαντικό σημείο παραβίασης της ιδιωτικότητας στο SIP είναι η αποκάλυψη των SIP URI και άλλων πληροφοριών, που περιέχονται στις επικεφαλίδες ενός μηνύματος SIP, σε μη έμπιστες δομικές μονάδες, συμπεριλαμβανομένων των διακομιστών των εταιρειών παροχής υπηρεσίας του αποστολέα και του παραλήπτη, αλλά και του ίδιου του τερματικού του παραλήπτη. Για την περαιτέρω ανάλυση της προτεινόμενης αρχιτεκτονικής κρίνεται απαραίτητη η υιοθέτηση κάποιων παραδοχών για τη δικτυακή τοπολογία του συστήματος, οι οποίες προτείνεται να υιοθετούνται στην περίπτωση υλοποίησης ενός συστήματος βασισμένου σε αυτή την αρχιτεκτονική.

Οι εταιρείες παροχής υπηρεσιών SIP έχουν κατοχυρωμένο ένα συγκεκριμένο αναγνωριστικό για το σύστημα DNS (DNS domain) και διατηρούν, για λόγους ευκολίας στη διαχείριση και ελαχιστοποίηση των λειτουργικών εξόδων, όλους τους διακομιστές τους σε ένα υποδίκτυο IP. Ανεξάρτητα από την παροχή υπηρεσιών SIP, οι εταιρείες αυτές μπορεί να αποτελούν ταυτόχρονα και παρόχους υπηρεσιών διαδικτύου (ISP). Σύμφωνα με την κεντρική ιδέα της αρχιτεκτονικής του συστήματος, ο Δ.Π.Ι. θα πρέπει να ελέγχει τουλάχιστον την εισερχόμενη ροή μηνυμάτων SIP προς τους διακομιστές της εταιρείας και γι’ αυτό το λόγο επιβάλλεται η υιοθέτηση μιας τοπολογίας ανάλογης μ’ αυτήν που παρουσιάζεται στο παρακάτω σχήμα. Σ’ αυτό παρατηρούμε ένα δίκτυο υπολογιστών από την πλευρά του SIP όπου δύο πάροχοι υπηρεσιών (A και B) προσφέρουν εγγυημένες υπηρεσίες προστασίας ιδιωτικότητας στους πελάτες τους και υλοποιούν την προτεινόμενη αρχιτεκτονική, ενώ ο τρίτος (C) δεν προβαίνει σε καμία αντίστοιχη ενέργεια . Οι πάροχοι A και B εφαρμόζουν πολιτικές προστασίας της IP των χρηστών τους και γι’ αυτό παρατηρείται η σχετική διαφοροποίηση στο σχήμα.



Εικόνα 12: Τοπολογία δικτύου παροχής υπηρεσιών SIP

3.3.2.1 Προστασία ιδιωτικότητας αποστολέα.

Η προστασία της ιδιωτικότητας του αποστολέα είναι πιο εύκολο να εξασφαλιστεί καθώς στην αρχιτεκτονική που προτείνουμε η πρόσβαση σε μια υπηρεσία ιδιωτικότητας είναι εξασφαλισμένη πριν οποιοσδήποτε τρίτος έχει την ευκαιρία να έρθει σε επαφή με τα δεδομένα ενός μηνύματος. Θα χρησιμοποιήσουμε, λοιπόν, την υπηρεσία ιδιωτικότητας, την οποία μπορεί να παρέχει ο Δ.Π.Ι. με τον τρόπο που ορίζεται στο RFC 3323, προτείνοντας κάποιες επεκτάσεις, όπου είναι απαραίτητο, με βάση τις απαιτήσεις και τους στόχους της σχεδίασης που θέσαμε νωρίτερα. Για την προστασία των προσωπικών του στοιχείων ο ίδιος ο αποστολέας είναι σε θέση να παρέχει στον εαυτό του ένα επίπεδο ιδιωτικότητας. Παρ' όλα αυτά υπάρχει πρόβλεψη να αναθέσει στο Δ.Π.Ι. τη συγκεκριμένη λειτουργία αν δεν έχει αυτή τη δυνατότητα (για παράδειγμα αν είναι ένα τερματικό περιορισμένων δυνατοτήτων ή έχει περιορισμούς απόδοσης και πολυπλοκότητας, όπως ένα κινητό τηλέφωνο στην περίπτωση του χρήστη B), θέτοντας την επιλογή user στην επικεφαλίδα «Privacy».

Το επίπεδο αυτό περιλαμβάνει τις παρακάτω λειτουργίες:

- Αφαίρεση όλων των προαιρετικών επικεφαλίδων του SIP συμπεριλαμβανομένων των «Subject», «Call-Info», «Organization», «User –Agent», «Reply-to», «in-Reply-to», οι οποίες περιέχουν προσωπικά δεδομένα των χρηστών.

- Αλλαγή του SIP URI AOR της επικεφαλίδας «From» σε μια ανώνυμη τιμή με τη χρήση γνωστών συμβάσεων της βιβλιογραφίας [23], οι οποίες προτείνουν τη χρήση του URI **From: "Anonymous" <sip:anonymous@anonymous.invalid>**
- Χρήση ενός κατάλληλα μεγάλου αλφαριθμητικού ως τιμή στην επικεφαλίδα «Call-Id» σε αντίθεση με τις υπάρχουσες συμβάσεις, που προτείνουν τη χρήση της διεύθυνσης IP ή του hostname του χρήστη. Για παράδειγμα: μπορεί να χρησιμοποιηθεί ο αύξων αριθμός του μηχανήματος (ο οποίος έτσι και αλλιώς είναι μοναδικός) κρυπτογραφημένος με κάποιο τυχαίο κλειδί γνωστό μόνο στο χρήστη.
  Αυτή είναι και η μοναδική λειτουργική απαίτηση της αρχιτεκτονικής για το μηχάνημα του χρήστη, αφού αν την επιτελούσε ο Δ.Π.Ι., θα έπρεπε να δράσει ως μια μονάδα B2BUA και τα μηνύματα-απαντήσεις θα έπρεπε να δρομολογηθούν μέσω αυτού κάτι που δεν είναι αποδεκτό από τη σχεδιαστική απαίτηση για ελαχιστοποίηση του φόρτου εργασίας του Δ.Π.Ι .

Σ’ αυτό το σημείο θα κάνουμε διαχωρισμό μεταξύ δύο περιπτώσεων:

1. Αν ο αποστολέας εμπιστεύεται τον τελικό χρήστη, τότε προφανώς θα επιθυμεί ο χρήστης αυτός να παραλάβει ένα μήνυμα το οποίο θα περιέχει όλες τις προαναφερθείσες πληροφορίες, οι οποίες αφαιρέθηκαν. Γι αυτό το λόγο μπορεί να χρησιμοποιήσει στο σώμα του μηνύματος ένα υποστηριζόμενο από το SIP τύπο φορτίου S/MIME, ο οποίος προσφέρει δυνατότητες πιστοποίησης, ακεραιότητας και ασφάλειας και να εισάγει σ’ αυτό όλες εκείνες τις επικεφαλίδες, που περιέχουν προσωπικά δεδομένα με τις πραγματικές τιμές τους.

   Σε περίπτωση που ο αποστολέας είναι ένα μηχάνημα με περιορισμένες δυνατότητες μπορεί να ζητήσει αυτή την υπηρεσία από τον Δ.Π.Ι., χρησιμοποιώντας μια επιπλέον προαιρετική επιλογή στην επικεφαλίδα Privacy (στα πρότυπα της επιλογής critical). Προτείνεται η επιλογή αυτή να ονομάζεται **end-user-trusted** και σε περίπτωση που την αντιμετωπίσει ένας διακομιστής, ο οποίος προσφέρει υπηρεσίες ιδιωτικότητας, θα πρέπει να αναζητά με βάση το SIP URI, που περιέχεται στην επικεφαλίδα «Το», το ψηφιακό πιστοποιητικό του παραλήπτη από μια βάση δεδομένων. Μ’ αυτόν τον τρόπο θα μπορέσει να σχηματίσει με το δημόσιο κλειδί του το κατάλληλο S/MIME, το οποίο και θα προσθέσει στο σώμα του μηνύματος SIP. Στην τελευταία περίπτωση ο παραλήπτης θα πρέπει να εμπιστεύεται την Α.Α. που παρέχει υπηρεσίες στον αποστολέα για να αποδεχθεί, ως έγκυρες και προερχόμενες απ’ αυτόν, τις επικεφαλίδες του μηνύματος, αφού ο τρόπος κατασκευής του S/MIME επιβάλλει την χρήση του πιστοποιητικού της Α.Α..

   Προφανώς, αν η υπηρεσία αυτή παρασχεθεί από το Δ.Π.Ι., τότε παραβιάζονται μέθοδοι ακεραιότητας και κρυπτογράφησης που εφαρμόζονται από άκρο σε άκρο της επικοινωνίας και ορίζονται στο RFC 3261 οπότε οι χρήστες θα πρέπει να μην εφαρμόζουν αυτές τις μεθόδους, αλλά να αφήνουν την εφαρμογή τους στο Δ.Π.Ι.
2. Αν ο αποστολέας δεν εμπιστεύεται τον τελικό παραλήπτη ή αν δεν μπορεί να εξασφαλίσει την ακεραιότητα των προσωπικών του δεδομένων μέχρι να φθάσουν σ’ αυτόν, τότε το μήνυμα θα πρέπει να αποκρύπτει εντελώς τα προσωπικά στοιχεία του με εφαρμογή των λειτουργιών που αναφέρθηκαν παραπάνω είτε από τον ίδιο, είτε από το Δ.Π.Ι..

Αν υπάρχει μόνο η παραπάνω επιλογή ιδιωτικότητας στο μήνυμα, η οποία αποτελεί και το χαμηλότερο επίπεδο προστασίας, ο Δ.Π.Ι. δεν χρειάζεται να εισάγει εγγραφή στην επικεφαλίδα «Via» που να αναπαριστά τον ίδιο, αλλά ούτε και κάποια εγγραφή «Record-route». Μ' αυτόν τον τρόπο ο Δ.Π.Ι. αποφεύγει να βρίσκεται στο μονοπάτι δρομολόγησης των απαντήσεων και των υπολοίπων μηνυμάτων της συνόδου, ελαχιστοποιώντας το φορτίο που καλείται να αντιμετωπίσει. Η περαιτέρω παρουσία του Δ.Π.Ι. στο κανάλι σηματοδοσίας δεν κρίνεται σκόπιμη, αφού ο αποστολέας θα μπορεί στη συνέχεια της συνόδου να διατηρήσει το ίδιο επίπεδο προστασίας, ανάλογα με το μήνυμα-απάντηση, το οποίο θα λάβει. Αν το μήνυμα-απάντηση περιέχει στην επικεφαλίδα «From» διαφορετικό SIP URI AOR από αυτό που έστειλε, θα απαντήσει εισάγοντας αυτό το τροποποιημένο URI στα μελλοντικά μηνύματα της συνόδου.

Το επόμενο επίπεδο προστασίας ιδιωτικότητας, το οποίο ορίζεται στο RFC 3323, είναι η επιλογή header με την οποία δηλώνεται η επιθυμία του αποστολέα να αποκρύπτονται πληροφορίες, οι οποίες δεν αποκαλύπτουν άμεσα την ταυτότητα του, αλλά μπορεί να οδηγήσουν σε χρήσιμα στοιχεία για αυτόν, όπως αυτές που περιέχονται στις επικεφαλίδες Via και Contact. Σε περίπτωση που υπάρχει αυτή η επιλογή ο Δ.Π.Ι. πρέπει να προβεί στις παρακάτω λειτουργίες:

- Αφαίρεση της επικεφαλίδας «Via» (Via stripping), που υπάρχει στο μήνυμα και περιέχει μεταξύ άλλων στην τελευταία γραμμή της τη διεύθυνση IP ή το hostname στο οποίο ο χρήστης αναμένει την απάντηση στην αίτηση του. Στη συνέχεια, ο Δ.Π.Ι. προσθέτει μια επικεφαλίδα «Via», η οποία περιέχει μόνο μια εγγραφή με τη δική του IP και μ' αυτόν τον τρόπο για όλο το υπόλοιπο δίκτυο το μήνυμα φαίνεται σαν να προέρχεται απ' αυτόν. Ο διακομιστής δρα σ' αυτή την περίπτωση σαν μια δομική μονάδα B2BUA, διατηρώντας μια σύνοδο προς τον αποστολέα και μια προς τον παραλήπτη (με διαφορετικά Call-ID). Είναι ο μόνος στον οποίο αποθηκεύεται η αντιστοίχιση των επικεφαλίδων και η κίνηση πρέπει να δρομολογείται αναγκαστικά μέσω αυτού. Όταν φτάσει η απάντηση για το αίτημα από τον παραλήπτη, τότε ο διακομιστής επαναφέρει την προηγούμενη επικεφαλίδα «Via» και επιστρέφει την απάντηση στον αποστολέα.
- Ομοίως ο διακομιστής οφείλει να πράξει και για την περίπτωση της επικεφαλίδας «Contact» και να την αντικαταστήσει με μία που θα αναπαριστά τον ίδιο ώστε τα επόμενα μηνύματα SIP να δρομολογηθούν σ' αυτόν. Ουσιαστικά μ' αυτόν τον τρόπο ο Δ.Π.Ι. παρεμβάλλεται στο κανάλι σηματοδοσίας της συνόδου σαν να είχε θέσει μια επικεφαλίδα «Record-Route» (μόνο που εδώ αλλάζει και το μοναδικό αναγνωριστικό της συνόδου) και αποκρύπτει τον πραγματικό αποστολέα από το υπόλοιπο δίκτυο.

Η παροχή της παραπάνω υπηρεσίας σημαίνει ότι ο Δ.Π.Ι. θα πρέπει να διατηρεί ένα μεγάλο αριθμό από δεδομένα για κάθε σύνοδο που έχει περάσει απ' αυτόν, κάτι που προφανώς οδηγεί σε πρόβλημα κλιμάκωσης του συστήματος. Μια λύση σ' αυτό το πρόβλημα θα μπορούσε να είναι η προσθήκη ενός ακόμα S/MIME στο σώμα του μηνύματος ή κάποιας, παρόμοιας λογικής και σκοπού, επικεφαλίδας. Οι πληροφορίες σ' αυτήν την περίπτωση θα κρυπτογραφούνται μ' ένα γνωστό συμμετρικό κλειδί από τον ίδιο το διακομιστή, οπότε το μήνυμα θα μεταφέρει τη συγκεκριμένη πληροφορία μαζί του, απαλλάσσοντας το διακομιστή από την ανάγκη διατήρησης μεγάλου αριθμού πληροφοριών. Ταυτόχρονα, το σύστημα γίνεται πιο εύρωστο με αυτόν τον τρόπο, αφού όλη η πληροφορία συνδέσεων μεταφέρεται στο μήνυμα και ακόμα και αν αποτύχει ένας διακομιστής, ένας άμεσος αντικαταστάτης (hot swap)

μπορεί να αρχίσει να λειτουργεί αμέσως χωρίς οι εγκαθιδρυμένες συνδέσεις να χαθούν. Φυσικά, η ίδια η διαδικασία δημιουργίας του S/MIME, η οποία απαιτεί κρυπτογράφηση, είναι χρονοβόρα οπότε ανάλογα με την κλίμακα και τις απαιτήσεις του συστήματος πρέπει να επιλεγεί η κατάλληλη λύση. Η παραπάνω επιλογή προστασίας ιδιωτικότητας πρέπει να επιλέγεται από τους χρήστες μόνο εφόσον δεν υλοποιούν κάποια μέθοδο προστασίας της IP τους. Αν υλοποιούν κάποια τέτοια λειτουργία, τότε θα πρέπει να επιλέγουν το προηγούμενο επίπεδο προστασίας ιδιωτικότητας user ώστε να ελαχιστοποιηθεί το φορτίο του Δ.Π.Ι. και να μη χρειάζεται να προβαίνει σε Via stripping. Η τελευταία ενέργεια εκτός του ότι αυξάνει το υπολογιστικό φορτίο του Δ.Π.Ι., όπως θα δούμε παρακάτω, μπορεί να οδηγήσει και σε απόρριψη της κλήσης στο Δ.Π.Ι. του παραλήπτη, λόγω δικών του επιλογών προστασίας ιδιωτικότητας.

Το τελευταίο επίπεδο προστασίας ιδιωτικότητας που προτείνεται στο RFC 3323 παρέχεται με χρήση της επιλογής session, η οποία δηλώνει ότι ο χρήστης χρειάζεται προστασία των προσωπικών του δεδομένων και για το κανάλι δεδομένων, κάτι που προφανώς υποδεικνύει ότι δεν εμπιστεύεται τον τελικό παραλήπτη. Σ' αυτήν την περίπτωση η σύνοδος που ξεκινά ο αποστολέας θα πρέπει να τερματίσει στο Δ.Π.Ι. , ο οποίος θα δημιουργήσει μια νέα σύνοδο προς τον παραλήπτη (αφού το RFC 3261 υποδεικνύει ότι οι ενδιάμεσοι δεν πρέπει να μεταβάλλουν τα σώματα των μηνυμάτων και προσφέρει μεθόδους από άκρης σε άκρη για τη διασφάλιση του), δρώντας ακριβώς, όπως στην περίπτωση της επιλογής header για το κανάλι σηματοδοσίας (χρήση Via stripping και αλλαγής Call-ID). Ταυτόχρονα, πρέπει να μεταβάλει την πληροφορία που περιέχεται στο σώμα του μηνύματος SDP [31] ώστε ο παραλήπτης να κατευθύνει την αίτηση για την έναρξη του καναλιού δεδομένων σ' ένα ενδιάμεσο κουτί (middlebox) [32], τη λειτουργία του οποίου θα ελέγχει η Α.Α. Ταυτόχρονα, η ύπαρξη ενός ενδιάμεσου στο κανάλι δεδομένων κάνει επιτακτική τη χρήση ενός πρωτοκόλλου, που παρέχει ασφάλεια από άκρου σε άκρο, όπως το SRTP [33].

3.3.2.2 Προστασία ιδιωτικότητας παραλήπτη.

Ενώ η προστασία της ιδιωτικότητας του αποστολέα μπορεί να υλοποιηθεί με τις λειτουργίες που αναφέραμε παραπάνω, η προστασία της ιδιωτικότητας του παραλήπτη παρουσιάζει μεγαλύτερες δυσκολίες και δεν επιλύεται συνολικά στη διεθνή βιβλιογραφία. Το βασικό πρόβλημα προκύπτει από το γεγονός ότι ο παραλήπτης δεν μπορεί να ελέγξει από ποιες διαχειριστικές οντότητες θα περάσει ένα μήνυμα, το οποίο απευθύνεται σ' αυτόν. Το πρώτο σημείο στο οποίο ο χρήστης θα μπορέσει εγγυημένα να εφαρμόσει πολιτικές προστασίας του είναι κατά την είσοδο του μηνύματος στη διαχειριστική οντότητα του παρόχου υπηρεσιών του, όπου ο Δ.Π.Ι. ελέγχει την εισερχόμενη κίνηση. Αυτό σημαίνει ότι αν απαντήσει σε μια εισερχόμενη κλήση ο παραλήπτης, είναι πιθανό ο ενδιάμεσος διακομιστής μιας διαχειριστικής οντότητας σαν την εταιρεία C (δες Εικόνα 12) να έχει την πλήρη πληροφορία της κλήσης. Ταυτόχρονα και σε αντίθεση με το όνομα αποστολέα, που δεν χρησιμοποιείται ουσιαστικά πουθενά στο SIP, εκτός από πιθανές λειτουργίες πιστοποίησης, το όνομα του παραλήπτη πρέπει να είναι μια έγκυρη τιμή, η οποία θα κατευθύνει τη δρομολόγηση των μηνυμάτων σ' αυτόν.

Πριν εξετάσουμε, όμως, το παραπάνω πρόβλημα, θα ασχοληθούμε με την προστασία της ιδιωτικότητας του παραλήπτη, όταν δέχεται κλήσεις από αποστολείς, που ανήκουν στην ίδια διαχειριστική οντότητα. Η απαίτηση για χρήση ενός URI, η οποία θα οδηγεί στη σωστή

παράδοση των μηνυμάτων στους παραλήπτες, επηρεάζει τη διαδικασία εισόδου του χρήστη στο σύστημα, όπου στη διαχειριστική οντότητα του χρήστη δημιουργείται η αντιστοίχιση μεταξύ του ονόματος του και των διευθύνσεων στις οποίες αυτός θα δέχεται τα μηνύματα SIP. Στη διεθνή βιβλιογραφία προτείνεται μια λύση για τη δημιουργία ανώνυμων URI, τα οποία διατηρούν την ιδιότητα της δρομολόγησης με χρήση του συστήματος GRUU [34]. Το σύστημα αυτό χρησιμοποιεί συμβάσεις για τη δημιουργία προσωρινών ψευδωνύμων URI καθώς και συμπληρωματικές επικεφαλίδες κοινοποίησης στο χρήστη του ψευδωνύμου που επιλέχτηκε.

Η παραπάνω λύση παρόλο που μας δίνει κάποια πολύ χρήσιμα στοιχεία και ιδέες δεν είναι αποδεκτή σύμφωνα με τις απαιτήσεις μας, αφού στη βιβλιογραφία χρησιμοποιείται κυρίως για να αποκρύψει στοιχεία της επικεφαλίδας «Contact» ενός αποστολέα, αναγκάζοντας το κανάλι σηματοδοσίας να περνάει πάντα από ένα διακομιστή της διαχειριστικής οντότητας, λόγω του τρόπου δρομολόγησης των μηνυμάτων του SIP μέσω του DNS (καθώς μόνο αυτός θα μπορεί να μετατρέψει το GRUU στην πραγματική επαφή (IP η hostname) του χρήστη). Μ' αυτόν τον τρόπο προστατεύονται τα δεδομένα της επικεφαλίδας «Contact» από το υπόλοιπο δίκτυο, αλλά όχι και από την ίδια την εταιρεία παροχής υπηρεσίας, η οποία έχει την αντιστοίχιση του ανώνυμου URI με την πραγματική διεύθυνση IP. Και σ' αυτήν την περίπτωση, σύμφωνα με τις απαιτήσεις μας, θα χρειαζόταν κάποιος άλλος μηχανισμός προστασίας της IP. Ταυτόχρονα, σύμφωνα με το GRUU, υπεύθυνος για την δημιουργία των URI είναι ο Διακομιστής Καταχώρισης Χρηστών SIP, κάτι που σημαίνει ότι οι λειτουργίες του θα έπρεπε να συμπεριληφθούν στο Δ.Π.Ι., αντιβαίνοντας στην απαίτηση για ελαχιστοποίηση των λειτουργιών του και διατήρηση κατά το δυνατόν αναλλοίωτης της λειτουργίας των βασικών δομικών μονάδων του SIP, που ήδη υπάρχουν.

Θα χρησιμοποιήσουμε, όμως, την παραπάνω ιδέα της δημιουργίας ανώνυμων και προσωρινών URI μ' έναν παρόμοιο τρόπο προς όφελος της ανωνυμίας των παραληπτών. Ο χρήστης, ο οποίος θέλει να λάβει υπηρεσία ανωνυμίας ως παραλήπτης, θα πρέπει να ζητήσει από το Δ.Π.Ι. τη δημιουργία ενός προσωρινού και ανώνυμου URI για τη συγκεκριμένη διαχειριστική οντότητα. Αυτό μπορεί να γίνει ως μέρος του SIP REGISTER ή με όποιον άλλο τρόπο επιθυμεί να το υλοποιήσει η Α.Α.. Σε κάθε περίπτωση, ως αποτέλεσμα της αίτησης ο χρήστης θα παραλάβει ένα προσωρινό ανώνυμο URI για τη συγκεκριμένη διαχειριστική οντότητα καθώς και ένα τρόπο πιστοποίησης (username/password ή άλλου είδους πιστοποίηση), τον οποίο θα χρησιμοποιήσει για μελλοντικές εισόδους του στο σύστημα μ' αυτό το ψευδώνυμο. Ο Δ.Π.Ι. θα θέσει ένα χρονικό σημείο μέχρι του οποίου η αντιστοίχιση του ψευδωνύμου με το χρήστη θα θεωρείται έγκυρη μετά το πέρας της οποίας θα πρέπει να πραγματοποιείται επανεγγραφή, όπως θα αναλυθεί στη συνέχεια. Ταυτόχρονα, ο Δ.Π.Ι. θα κάνει μια εγγραφή στο σύστημα πιστοποίησης της εταιρείας παροχής υπηρεσίας για το συγκεκριμένο URI με τα στοιχεία πιστοποίησης, που έστειλε και στο χρήστη. Σε μελλοντικές διαδικασίες εισόδου ο χρήστης θα χρησιμοποιήσει τα στοιχεία αυτά για να εισέλθει στο σύστημα, πραγματοποιώντας ένα κανονικό REGISTER στο Διακομιστή Καταχώρισης Χρηστών SIP της εταιρείας παροχής υπηρεσιών. Προφανώς, θεωρείται ότι ο χρήστης χρησιμοποίει κάποιον τρόπο προστασίας της IP. Από τη στιγμή που οι παραλήπτες έχουν εισέλθει στο σύστημα, χρησιμοποιώντας κάποιο προσωρινό ανώνυμο URI, το μόνο που απαιτείται να γίνει από το Δ.Π.Ι. για την προστασία της ανωνυμίας των παραληπτών είναι η μετατροπή του SIP URI AOR, που υπάρχει στην επικεφαλίδα «To», ενός μηνύματος που απευθύνεται στον εν λόγω χρήστη και προέρχεται από το ασφαλές δίκτυο της διαχειριστικής οντότητας, στο αντίστοιχο ανώνυμο URI, το οποίο χρησιμοποιεί εκείνη τη στιγμή. Προφανώς,

η συχνή ανανέωση των προσωρινών URI, όπως και όλων των άλλων μηχανισμών προστασίας ιδιωτικότητας, καθώς και των μεθόδων προστασίας της IP, συμβάλλει στην καλύτερη προστασία των χρηστών. Επειδή οι μηχανισμοί ανανέωσης της εισόδου των χρηστών στο σύστημα παρέχονται ήδη από το SIP, η λύση αυτή φαίνεται να έχει πολλά πλεονεκτήματα.

Επεκτείνοντας την παραπάνω ιδέα μπορούμε πάντα να προστατεύσουμε το όνομα του παραλήπτη από τον πάροχο υπηρεσίας του, πραγματοποιώντας μια αντίστοιχη μετατροπή στο Δ.Π.Ι., ο οποίος ελέγχει τη ροή εισόδου των μηνυμάτων SIP που προέρχονται από άλλες διαχειριστικές οντότητες, (δες Εικόνα 12) στο δίκτυο της εταιρείας. Η μόνη διαφορά που υπάρχει, σε σχέση με την παραπάνω περίπτωση, είναι ότι ο Δ.Π.Ι. πρέπει αναγκαστικά να δράσει σ' αυτό το σημείο ως B2BUA, τερματίζοντας τη σύνοδο εισόδου και επανεκκινώντας την μ' ένα νέο αναγνωριστικό συνόδου (επικεφαλίδα Call –ID και ετικέτα tag στην επικεφαλίδα From). Η συγκεκριμένη ενέργεια είναι απαραίτητη, αφού υπάρχει περίπτωση ένας μη έμπιστος ενδιάμεσος διακομιστής άλλης διαχειριστικής οντότητας να έχει καταχώριση που θα περιέχει το αναγνωριστικό συνόδου και την επικεφαλίδα «Το» με το πραγματικό όνομα παραλήπτη. Ακόμα και σ' αυτή την περίπτωση η εταιρεία μπορεί να χρησιμοποιήσει επίθεση με ανάλυση κίνησης για να βρει τον προηγούμενο κόμβο και να συνεργαστεί μαζί του για την αποκάλυψη της πληροφορίας, οπότε τελικά το συμπέρασμα είναι ότι η Α.Α. δυσκολεύεται να δώσει εγγυήσεις στους παραλήπτες για την προστασία τους στη γενική περίπτωση, λόγω αδυναμίας ελέγχου της δρομολόγησης του μηνύματος πριν την άφιξη του σ' αυτήν. Αυτό σημαίνει ότι, σε περίπτωση που ο παραλήπτης επιλέξει να αποδεχτεί τελικά την κλήση, κάποιος μη έμπιστος ενδιάμεσος διακομιστής θα ενημερωθεί για το γεγονός της κλήσης, της αποδοχής της και πιθανών της διάρκειάς της με συμμετέχοντα ως παραλήπτη ένα συγκεκριμένο SIP URI AOR, το οποίο θα μπορεί εύκολα να αντιστοιχίσει στον άνθρωπο από μια υπηρεσία καταλόγου.

Μια πιθανή αντιμετώπιση είναι να απορρίπτονται τα μηνύματα στο Δ.Π.Ι. και να επιστρέφεται μήνυμα λάθους στον αποστολέα ή να ειδοποιείται ο παραλήπτης ότι η αποδοχή του συγκεκριμένου μηνύματος θα αποκαλύψει προσωπικά του δεδομένα σε μη έμπιστες οντότητες. Φυσικά, μπορεί να ενταχθεί στο σύστημα ένα σύστημα επιλογών του χρήστη, ο οποίος θα μπορεί να δηλώσει ρητά την εμπιστοσύνη του σε συγκεκριμένες διαχειριστικές οντότητες ή χρήστες, οπότε ο Δ.Π.Ι. μπορεί να εξετάζει την επικεφαλίδα «Via» για να πιστοποιήσει ότι όλοι οι ενδιάμεσοι είναι έμπιστοι πριν προωθήσει ή απορρίψει τελικά την κλήση. Εδώ πρέπει να αναφερθεί ότι, αν το εισερχόμενο μήνυμα είναι αποτέλεσμα ενός «Via stripping», πρέπει να αντιμετωπίζεται με απόρριψη εκτός και αν ο Δ.Π.Ι. εμπιστεύεται αυτόν που το πραγματοποίησε, ή/και υπάρχει ρητή επιλογή από το χρήστη, οπότε ο Δ.Π.Ι. αντιμετωπίζει το μήνυμα σαν να προήλθε από τη διαχειριστική οντότητά του.

Τέλος, οφείλουμε να εξετάσουμε την περίπτωση που το μήνυμα προέρχεται από τη διαχειριστική οντότητα μιας εταιρείας, η οποία υλοποιεί την προτεινόμενη αρχιτεκτονική για την προστασία δεδομένων (περίπτωση κλήσης μεταξύ χρήστη Α και Β δες Εικόνα 12). Αν υπάρχει αμοιβαία συμφωνία συνεργασίας και εμπιστοσύνης μεταξύ των Α.Α., που συνεργάζονται με τις εταιρίες Α και Β, υπάρχει η δυνατότητα να δημοσιοποιεί η μία στην άλλη τις τρέχουσες αντιστοιχίσεις των προσωρινών ανώνυμων URI με τα SIP URI AOR των χρηστών, οπότε η πολιτική προστασίας ιδιωτικότητας του παραλήπτη στην εταιρεία Α εφαρμόζεται απευθείας από την Α.Α. της εταιρείας Β στον Δ.Π.Ι. που δέχεται τα αιτήματα από τους πελάτες της. Σ' αυτή την περίπτωση, δηλαδή, αν ο Δ.Π.Ι. της εταιρείας Α αντιμετωπίσει ένα μήνυμα με επικεφαλίδα «Το», η οποία περιέχει ένα έγκυρο προσωρινό

ανώνυμο URI, ο Δ.Π.Ι. θα προωθήσει απλά το μήνυμα στο εσωτερικό της διαχειριστικής οντότητας της εταιρείας Α. Φυσικά το μήνυμα θα πρέπει να συνοδεύεται από πιστοποιητικό της εταιρείας Β για να αποφευχθούν επιθέσεις επανάληψης.

3.3.2.3 Προστασία ιδιωτικότητας domain.

Όλες οι παραπάνω λύσεις που προτείναμε εξασφαλίζουν την ανωνυμία των χρηστών, εκτός από την αποκάλυψη του domain στο οποίο είναι γραμμένος, δηλαδή ουσιαστικά το όνομα της εταιρείας που του παρέχει υπηρεσίες SIP.

Όσον αφορά σ' έναν αποστολέα μηνύματος η πληροφορία αυτή αποκαλύπτεται κυρίως μέσω της επικεφαλίδας «Via» που θα καταδεικνύει τον πρώτο ενδιάμεσο διακομιστή που επεξεργάστηκε το μήνυμα. Η χρήση Via stripping από τον Δ.Π.Ι. στη ροή εξόδου μηνυμάτων από το δίκτυο της εταιρείας θα μπορούσε να αποτελέσει μια λύση, αλλά αυτό θα αύξανε σημαντικά το φορτίο του, αφού θα έπρεπε να επεξεργάζεται και τη ροή εξόδου κάτι για το οποίο δεν έχει υπάρξει ανάγκη ως τώρα. Ταυτόχρονα, ο πάροχος υπηρεσίας τελικά θα μπορούσε να αποκαλυφθεί και από την IP του Δ.Π.Ι. σε περίπτωση που δεν χρησιμοποιεί και αυτός κάποια μέθοδο ανωνυμίας IP. Γενικά προστίθεται στο σύστημα μεγάλη πολυπλοκότητα για μια πληροφορία που έτσι και αλλιώς θα είναι γνωστή στον πάροχο της υπηρεσίας και σύμφωνα με τη θεώρηση μας θα μπορεί να δοθεί σε οποιαδήποτε ενδιαφερόμενο. Για την περίπτωση του παραλήπτη η πληροφορία αυτή είναι απολύτως απαραίτητη για τη δρομολόγηση των μηνυμάτων SIP, ενώ συνδέεται και με το σύστημα του DNS, αφού ο κάθε ενδιάμεσος διακομιστής εκτελεί ένα ερώτημα DNS για να βρει τον υπολογιστή στον οποίο πρέπει να προωθήσει ένα αίτημα. Για τον παραπάνω λόγο δεν είναι εφικτή η χρήση ψευδωνύμων για την κάλυψη της διαχειριστικής οντότητας προορισμού ενός μηνύματος ακόμα και αν όλες οι εταιρείες συνεργάζονταν με την ίδια Α.Α. (κάτι που δεν θα πρέπει να θεωρείται σίγουρο, αφού οι εταιρείες προέρχονται από διαφορετικές χώρες), αφού και σ' αυτή την περίπτωση η Α.Α. θα έπρεπε να αναλάβει τη λειτουργία του διακομιστή DNS στον οποίο θα απευθύνουν μηνύματα όλες οι εταιρείες, κάτι προφανώς ανέφικτο

3.3.3 Ζητήματα Υπηρεσιών Παρουσίας

Οι υπηρεσίες παρουσίας παρουσιάζουν μεγαλύτερη πολυπλοκότητα σε σχέση με τις άλλες υπηρεσίες, που προσφέρονται από το SIP,αφού συνεχίζονται ακόμα και αν ο χρήστης δεν έχει εισέλθει στο σύστημα. Παρ' όλα αυτά η προστασία της ιδιωτικότητας των χρηστών κατά την παροχή της συγκεκριμένης υπηρεσίας δεν διαφέρει πολύ σε σχέση με την υπηρεσία εγκαθίδρυσης συνόδου που αναλύθηκε προηγουμένως. Η κυριότερη διαφορά έγκειται στο γεγονός ότι τα κριτήρια αποδοχής (και προώθησης) ενός αιτήματος SUBSCRIBE από το Δ.Π.Ι. σε αντίθεση με ένα μήνυμα INVITE ή MESSAGE, θα πρέπει είναι αυστηρότερα. Η πληροφορία παρουσίας αποτελεί πολύ σημαντικό προσωπικό δεδομένο και ειδικά από τη στιγμή που το πρότυπο [35] ορίζει γενικές δομές XML που μπορούν να μεταφέρουν πολλών ειδών πληροφορίες ως μέρος ενός PUBLISH ή NOTIFY (Κατάσταση χρήστη, Διάθεση χρήστη κτλ.). Γι' αυτό το λόγο η συγκεκριμένη υπηρεσία θα πρέπει να παρέχεται μόνο μεταξύ πιστοποιημένων χρηστών, οι οποίοι εμπιστεύονται ο ένας τον άλλον. Αυτό σημαίνει ότι η δομή, που περιέχει την πληροφορία παρουσίας και η οποία μεταφέρεται στο σώμα των

μηνυμάτων PUBLISH και NOTIFY, θα πρέπει να είναι κρυπτογραφημένη με γνωστά συμμετρικά κλειδιά και ο Διακομιστής Παρουσίας (PA) θα πρέπει να την μεταφέρει αυτούσια. Αυτό δεν είναι κάτι παράδοξο, αφού έτσι και αλλιώς η πληροφορία παρουσίας χρησιμοποιείται κυρίως για τη διατήρηση και την ανανέωση της λίστας φίλων (Buddy List), οπότε είναι αναμενόμενο να μοιράζεται μεταξύ χρηστών, που εμπιστεύονται ο ένας τον άλλον.

Για την προστασία της προσωπικής πληροφορίας, που μεταφέρεται στις επικεφαλίδες των μηνυμάτων, θα χρησιμοποιήσουμε τις ιδέες που αναπτύχθηκαν παραπάνω. Επεκτείνοντας την ιδέα της χρήσης GRUU, οι χρήστες που θέλουν να δημοσιοποιούν την πληροφορία παρουσίας τους μπορούν να λαμβάνουν ένα αντίστοιχο ψευδώνυμο για χρήση αποκλειστικά στην υπηρεσία παρουσίας με τον Δ.Π.Ι. ή γενικά την Α.Α. να διατηρεί την αντιστοιχία. Τα εισερχόμενα στο δίκτυο μηνύματα SUBSCRIBE, τα οποία σύμφωνα με την προτεινόμενη αρχιτεκτονική του συστήματος περνάνε πρώτα από τον Δ.Π.Ι., μετασχηματίζονται κατάλληλα ώστε να χρησιμοποιείται το τρέχον ψευδώνυμο, αντί του SIP URI AOR. Φυσικά, για να γίνει αποδεκτό το μήνυμα SUBSCRIBE και να το προωθήσει ο Δ.Π.Ι. θα πρέπει να ταυτοποιήσει τον αποστολέα ακόμα και αν αυτός έχει κάνει χρήση ανωνυμίας, πιθανόν επιστρέφοντας ένα μήνυμα 404 Authentication Required, ή με κάποια άλλη μέθοδο. Αν ο αποστολέας είναι έμπιστος του χρήστη στον οποίο αναφέρεται το SUBSCRIBE τότε αυτό προωθείται με ανωνυμία αποστολέα προς τον PA της διαχειριστικής οντότητας με τον Δ.Π.Ι. να δρα ως ένας B2BUA για να αποκρύψει την ευαίσθητη πληροφορία του αναγνωριστικού συνόδου μεταξύ του εσωτερικού και του εξωτερικού της εταιρείας παροχής υπηρεσίας. Όταν ένας χρήστης επιθυμεί να δημοσιοποιήσει την πληροφορία παρουσίας του, τότε αποστέλλει ένα μήνυμα PUBLISH, το οποίο μετά την επεξεργασία του από τον Δ.Π.Ι. θα προωθείται στο διακομιστή παρουσίας. Αυτός εν συνεχεία θα στείλει τα κατάλληλα μηνύματα NOTIFY στους εγγεγραμμένους σ' αυτόν ενδιαφερόμενους χρήστες. Αν οι χρήστες αυτοί προέρχονται από το εξωτερικό της διαχειριστικής οντότητας, τα μηνύματα δρομολογούνται μέσω του Δ.Π.Ι. ώστε να γίνει η κατάλληλη αντίστροφη μετατροπή και να καταλήξουν στους σωστούς παραλήπτες. Για λόγους ασφαλείας συνίσταται ο Δ.Π.Ι. να αφαιρεί την επικεφαλίδα «Event» στα εξερχόμενα μηνύματα NOTIFY, αφού αυτή αποκαλύπτει ως ένα βαθμό προσωπικές πληροφορίες και να αφήνει τον παραλήπτη να αντιληφθεί το είδος του γεγονότος από την ειδική δομή μεταφοράς πληροφορίας παρουσίας, που περιέχεται στο σώμα του μηνύματος.

3.3.4 Ζητήματα Διαχείρισης Ψευδωνύμων

Τα προσωρινά ψευδώνυμα δίνουν τη δυνατότητα στους χρήστες του συστήματος να λαμβάνουν υπηρεσίες που εξασφαλίζουν την ιδιωτικότητα. Για την ενίσχυση των εγγυήσεων προστασίας των χρηστών τα ψευδώνυμα αυτά θα πρέπει να ανανεώνονται ανά τακτά χρονικά διαστήματα, ώστε να διασφαλίζεται ότι η εταιρεία δεν θα μπορεί να ταυτοποιήσει κάποιον χρήστη με μια ή πολλές κλήσεις. Η χρήση των ψευδωνύμων, όμως, προσθέτει πολυπλοκότητα στο σύστημα, ενώ ταυτόχρονα ανακύπτουν και κάποιες περιπτώσεις που θα πρέπει να αποσαφηνιστούν.

Συγκεκριμένα:

- Στο SIP ο κάθε χρήστης έχει τη δυνατότητα να εισέρχεται στο σύστημα από διαφορετικά μηχανήματα και ο ενδιάμεσος διακομιστής της διαχειριστικής

οντότητας έχει τη δυνατότητα να προωθεί πολλαπλές αιτήσεις στην περίπτωση λήψης ενός μηνύματος-αίτησης προς το χρήστη. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να μπορεί να χρησιμοποιεί το ίδιο ψευδώνυμο διαφανώς από διαφορετικά μηχανήματα.

- Στο σύστημα παροχής ψευδωνύμων που προτείνεται, ο Δ.Π.Ι. θεωρεί ότι το ψευδώνυμο που παρέχεται είναι έγκυρο για ένα χρονικό διάστημα με σκοπό να επιβάλλεται η τακτική ανανέωση τους ώστε να προστατεύεται καλύτερα η ιδιωτικότητα των χρηστών. Αυτό σημαίνει, όμως, ότι θα πρέπει να καθοριστεί ο τρόπος με τον οποίο θα γίνεται μετάβαση από το ένα ψευδώνυμο στο επόμενο χωρίς να αποκαλύπτεται αυτή η πληροφορία σε μη έμπιστες οντότητες.
- Οι συμπληρωματικές υπηρεσίες παρουσίας και σύντομων μηνυμάτων δημιουργούν ακόμα περισσότερα προβλήματα, αφού θα πρέπει να συνεχίσουν να παρέχονται ακόμα και αν ο χρήστης αλλάξει ψευδώνυμο ή δεν έχει εισέλθει καν στο σύστημα και δεν διαθέτει κανένα έγκυρο ψευδώνυμο

Για την κάλυψη των παραπάνω περιπτώσεων θα πρέπει να υλοποιούνται οι παρακάτω λειτουργίες κατά αντιστοιχία.

1. Όταν ο κάθε χρήστης παραλαμβάνει ένα νέο ψευδώνυμο θα του παρέχεται από το Δ.Π.Ι. ο χρόνος λήψης της ισχύος του ψευδωνύμου αυτού. Το μηχάνημα του χρήστη είναι υποχρεωμένο να ξεκινήσει μια διαδικασία επανεισόδου (re-register) στο σύστημα μετά το πέρας του χρόνου αυτού ώστε να λάβει το νέο ψευδώνυμο. Φυσικά, ο χρήστης θα πρέπει να αλλάξει και τη διεύθυνση IP του πριν από τη διαδικασία για να μην μπορεί να χρησιμοποιηθεί η διεύθυνση IP για την ταυτοποίηση παλιού και νέου ψευδωνύμου. Αν ο ίδιος χρήστης εκκινήσει διαδικασία εισόδου πριν το πέρας αυτού του χρονικού διαστήματος από διαφορετικό μηχάνημα, τότε ο Δ.Π.Ι. θα επιστρέφει το ίδιο ψευδώνυμο και τον ίδιο χρόνο ανανέωσης. Μ' αυτόν τον τρόπο όλα τα μηχανήματα, τα οποία χρησιμοποίει ο χρήστης, θα είναι συγχρονισμένα ως προς τη χρήση του ψευδωνύμου και θα επιτυγχάνεται η επιθυμητή συμπεριφορά από το σύστημα.
2. Ο Δ.Π.Ι. θα θεωρεί έγκυρο ένα ψευδώνυμο (και θα προωθεί στο σύστημα αιτήσεις προς αυτό) μέχρι τη στιγμή που ο χρήστης θα εκκινήσει μια νέα διαδικασία εισόδου στο σύστημα. Μετά το πέρας της διαδικασίας εισόδου του χρήστη στο σύστημα τα μηνύματα-αιτήσεις προς το χρήστη θα προωθούνται με το νέο ψευδώνυμο. Για να μην μπορεί να προσδιοριστεί ο χρόνος αλλαγής ψευδωνύμου από την εταιρεία παροχής της υπηρεσίας, η χρονική διάρκεια για την οποία θα γίνεται το SIP REGISTER θα πρέπει να είναι εντελώς διαφορετική και να μη συσχετίζεται με τη χρονική διάρκεια εγκυρότητας του ψευδωνύμου. Μ' αυτόν τον τρόπο απλά από κάποιο σημείο και πέρα ο Ενδιάμεσος Διακομιστής δεν θα λαμβάνει πια αιτήσεις για το ψευδώνυμο του χρήστη, αλλά δεν θα γνωρίζει αν αυτό θα οφείλεται σε έλλειψη κίνησης ή αλλαγή ψευδωνύμου. Όταν θα λήξει και το χρονικό διάστημα εγγραφής του ψευδωνύμου στο Διακομιστή Θέσης η μετάβαση θα έχει ολοκληρωθεί πλήρως.
3. Για την επίτευξη των υπηρεσιών παρουσίας ο χρήστης θα πρέπει αρχικά να αποστείλει ένα μήνυμα PUBLISH με το παλιό ψευδώνυμο, το οποίο στο σώμα του θα ειδοποιεί τους έμπιστους παραλήπτες να διενεργήσουν μια νέα διαδικασία εκδήλωσης ενδιαφέροντος (SUBSCRIBE), αφού το συγκεκριμένο ψευδώνυμο δεν θα ξαναχρησιμοποιηθεί.

Για τις υπηρεσίες μηνυμάτων ανακύπτει πρόβλημα μόνο εφόσον ο χρήστης δεν έχει εισέλθει στο σύστημα από κανένα μηχάνημα, αφού τότε τα μηνύματα αποθηκεύονται στο ειδικό Διακομιστή Μηνυμάτων της διαχειριστικής οντότητας και παραδίδονται στο χρήστη μετά την επανείσοδο του στο σύστημα. Αυτό σημαίνει ότι για να λειτουργήσει η υπηρεσία ο χρήστης θα πρέπει πρώτα να κάνει μια «εικονική» είσοδο στο σύστημα με το προηγούμενο έγκυρο ψευδώνυμο του, ώστε να λάβουν τα μηνύματα κατά τη διαδικασία εισόδου και μετά να εκτελέσει μια διαδικασία επανεγγραφής ώστε να λάβει το νέο ψευδώνυμο.
Φυσικά, ο Δ.Π.Ι. θα πρέπει να επιστρέφει το παλιό ψευδώνυμο στο χρήστη σε περίπτωση επανεγγραφής μετά από απουσία του από το σύστημα, ώστε να εξασφαλιστεί η ακεραιότητα της λειτουργίας του συστήματος σε όλες τις περιπτώσεις.

3.3.5 Ζητήματα Αποθήκευσης Προσωπικών Δεδομένων

Ένα σημαντικό ζήτημα που πρέπει να επιλυθεί σε μια αρχιτεκτονική που παρέχει κάποιες υπηρεσίες, προστατεύοντας ταυτόχρονα την ιδιωτικότητα του χρήστη, είναι το μέρος που θα αποθηκευτούν τελικά τα προσωπικά του δεδομένα. Στη συμβατική αρχιτεκτονική ενός συστήματος διαδικτυακής τηλεφωνίας όλα τα δεδομένα που είναι απαραίτητα για την παροχή της υπηρεσίας (προσωπικά δεδομένα του χρήστη), όπως και αυτά που δημιουργούνται κατά τη λειτουργία της (λίστα κλήσεων και στοιχεία χρέωσης), αποθηκεύονται στην κεντρική βάση δεδομένων της εταιρείας. Από τη στιγμή, όμως, που η εταιρεία παροχής υπηρεσιών διαδικτυακής τηλεφωνίας έχει άμεση πρόσβαση σε αυτά τα δεδομένα, δεν υπάρχει τεχνικά εφικτός τρόπος να ελεγχθεί η χρήση τους και να επιβληθεί η σχετική νομοθεσία. Ο πάροχος έχει τον απόλυτο έλεγχο πάνω στα δεδομένα και μπορεί να τα αξιοποιήσει με τρόπους που ο χρήστης δεν θα επέτρεπε, (αποστολή στοχευόμενης διαφήμισης, κατηγοριοποίηση χρηστών (profiling)). Ακόμα και αν η ίδια η εταιρεία παροχής της υπηρεσίας εφαρμόζει πολιτικές προστασίας της ιδιωτικότητας, η διαρροή προσωπικών δεδομένων μπορεί να γίνει με τρόπους που δεν μπορούν να ελεγχθούν από εξουσιοδοτημένους ή μη υπαλλήλους, οι οποίοι έχουν πρόσβαση σ' αυτά τα δεδομένα.

Λαμβάνοντας υπόψη τα παραπάνω καταλαβαίνουμε ότι ο μόνος τρόπος να προστατευθούν τα προσωπικά δεδομένα του χρήστη είναι η εταιρεία παροχής υπηρεσιών διαδικτυακής τηλεφωνίας να μην έχει άμεση πρόσβαση σ' αυτά. Η πληροφορία πρέπει να είναι κατανεμημένη ώστε να ελαχιστοποιείται η πιθανότητα να συγκεντρωθεί μεγάλο μέρος της σε περίπτωση παραβίασης των ασφαλιστικών δικλείδων, αλλά θα πρέπει ταυτόχρονα να μπορεί να επεξεργαστεί με αποδοτικό τρόπο.

Με βάση αυτές τις απαιτήσεις προκύπτουν οι παρακάτω πιθανές λύσεις:

- Αποθήκευση των δεδομένων στο τερματικό του χρήστη.

  Η συγκεκριμένη λύση δεν είναι πρακτική καθώς απαιτεί την εκτέλεση πολλών λειτουργιών της υπηρεσίας στο τερματικό του χρήστη, το οποίο πολλές φορές δεν μπορεί να αντέξει το υπολογιστικό και διαχειριστικό φορτίο, ιδιαίτερα αν είναι μια αυτόνομη ή φορητή συσκευή. Εξάλλου υπάρχουν δεδομένα τα οποία δεν δημιουργούνται από το τερματικό του χρήστη, αλλά από την ίδια τη χρήση της υπηρεσίας, όπως για παράδειγμα η λίστα κλήσεων. Για τους παραπάνω λογούς η

αρχιτεκτονική αυτή κρίνεται ακατάλληλη για εφαρμογή στο περιβάλλον της διαδικτυακής τηλεφωνίας.

- Πλήρως κατανεμημένη αποθήκευση των δεδομένων.

  Σ' αυτή τη λύση το σύνολο της πληροφορίας για τα προσωπικά δεδομένα κατανέμεται στα τερματικά των χρηστών της υπηρεσίας, ενώ χρησιμοποιείται μια λύση δικτύων ομότιμων κόμβων (P2P) για την ανάκτηση των πληροφοριών, όταν αυτές είναι απαραίτητες. Η Α.Α. διαδραματίζει διαχειριστικό ρόλο διατηρώντας τη θέση της κάθε αποθηκευμένης πληροφορίας και ανακτώντας την από τους κόμβους, όταν αυτό κρίνεται απαραίτητο. Για λόγους εξασφάλισης των αποθηκευμένων δεδομένων, σε περίπτωση αποτυχίας κάποιων κόμβων, η πληροφορία αποθηκεύεται σε κατάλληλο αριθμό αντιτύπων και ανακατανέμεται ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο ομότιμων κόμβων. Το πακέτο πληροφορίας, που αποθηκεύεται στον κάθε ομότιμο κόμβο, θα πρέπει να είναι κρυπτογραφημένο με κατάλληλη μέθοδο από την Α.Α. ώστε να μην μπορεί να ανακτηθεί το περιεχόμενο από μη εγκεκριμένους χρήστες. Η συγκεκριμένη αρχιτεκτονική έχει την ιδιότητα της πλήρους αποκέντρωσης του συστήματος με τα γνωστά πλεονεκτήματα σε απόδοση και ευρωστία, καθώς δεν υπάρχουν διακομιστές οι οποίοι επωμίζονται μεγάλο υπολογιστικό βάρος και αποτελούν προφανή σημεία επιθέσεως στο σύστημα. Από την άλλη πλευρά είναι ευπαθή σε μια διαφορετικού είδους επίθεση αφού, χωρίς κάποιο κεντρικό σημείο πιστοποίησης, ένας κακόβουλος χρήστης θα μπορούσε να δημιουργήσει εικονικούς χρήστες με σκοπό να μαζέψει σ' αυτούς αρκετά πακέτα πληροφορίας και να δοκιμάσει μελλοντικά μια επίθεση κρυπτανάλυσης με μεγαλύτερη πιθανότητα επιτυχίας. Επιπλέον, λόγω της απουσίας κεντρικής βάσης δεδομένων, η επεξεργασία των πληροφοριών δεν θα γίνεται με αποδοτικό τρόπο, ενώ θα πρέπει και να αναπτυχθεί μεθοδολογία ώστε η εταιρεία παροχής υπηρεσίας να έχει ελεγχόμενη πρόσβαση σ' αυτά.

- Αποθήκευση των δεδομένων σε κεντρική βάση δεδομένων.

  Σε σχέση με τις προηγούμενες λύσεις μια κεντρική βάση δεδομένων έχει το πλεονέκτημα της χρήσης μιας διαδεδομένης τεχνολογίας με γνωστά πλεονεκτήματα σε απόδοση και ακεραιότητα δεδομένων. Παρ' όλα αυτά είναι προφανές ότι μια κεντρική βάση δεδομένων προσωπικού χαρακτήρα θα πρέπει να βρίσκεται υπό το διαχειριστικό έλεγχο της Α.Α. κάτι που αντιβαίνει στην απαίτηση για χαμηλό διαχειριστικό φορτίο σ' αυτήν. Γι' αυτό και η λύση που τελικά επιλέγουμε είναι να χρησιμοποιήσουμε μια βάση δεδομένων, η οποία βρίσκεται υπό μεικτή διαχειριστική ευθύνη της εταιρείας και της Α.Α. Η Α.Α έχει την ευθύνη του τμήματος της βάσης, στο οποίο αποθηκεύονται τα προσωπικά δεδομένα, ενώ η εταιρεία παροχής υπηρεσίας είναι υπεύθυνη για όλα τα υπόλοιπα στοιχεία που είναι απαραίτητα για τη λειτουργία της. Η φυσική θέση της βάσης δεδομένων δεν επηρεάζει την λειτουργία του συστήματος, αρκεί να μπορεί να εξασφαλιστεί η αποκλειστική πρόσβαση της εξουσιοδοτημένης Α.Α στα αρχεία των προσωπικών δεδομένων, ενώ η υιοθέτηση ενός σχήματος κρυπτογράφησης της βάσης θα εξασφαλίζει την προστασία των δεδομένων σε φυσικό επίπεδο από επιθέσεις. Οι κρυπτογραφημένες βάσεις δεδομένων αποτελούν μια διαδεδομένη τεχνολογία κάτι που καθιστά ρεαλιστική την υιοθέτηση της συγκεκριμένης λύσης. Για τη διατήρηση του επιχειρηματικού της μοντέλου η εταιρεία παροχής υπηρεσίας θα πρέπει να έχει πρόσβαση σε ανώνυμα στατιστικά δεδομένα. Η πρόσβαση αυτή θα πρέπει να γίνεται έμμεσα μέσω της Α.Α., κάτι που κρίνεται απαραίτητο, ώστε η Α.Α να

επεξεργαστεί τα δεδομένα και να τα καταστήσει ανώνυμα, προστατεύοντας την ιδιωτικότητα των χρηστών.

Η επιλογή της αρχιτεκτονικής αποθήκευσης δεδομένων σε κεντρική βάση με μεικτή διαχείριση έχει επίδραση σε διαδικασίες, οι οποίες σε μια παραδοσιακή αρχιτεκτονική θεωρούνταν τετριμμένες. Συγκεκριμένα: θα πρέπει να αναπτυχθούν κατάλληλες μέθοδοι ώστε να εξασφαλίζεται η ιδιωτικότητα του χρήστη στις περιπτώσεις που αυτός ή η εταιρεία επιθυμούν να έχουν πρόσβαση στα δεδομένα. Αυτό συμβαίνει στις ακόλουθες περιπτώσεις, οι οποίες θα αναλυθούν παρακάτω:

3.3.5.1 Πρόσβαση χρήστη στο προσωπικό του προφίλ

Το επιχειρηματικό μοντέλο της εταιρείας παροχής της υπηρεσίας προβλέπει ότι αυτή θα έχει τη διαχειριστική ευθύνη ενός διαδικτυακού τόπου, ο οποίος έχει τη μορφή μιας διαδικτυακής πύλης (portal). Στη διαδικτυακή πύλη οι χρήστες μπορούν να έχουν ανώνυμη πρόσβαση στο δημοσιευμένο περιεχόμενο, ενώ μπορεί να γίνεται και προβολή διαφημίσεων. Σε περίπτωση που ο χρήστης κατά την περιήγησή του στο διαδικτυακό τρόπο της εταιρείας επιλέξει να επισκεφτεί το προσωπικό του προφίλ για να επεξεργαστεί τις προσωπικές του πληροφορίες ή να εξετάσει τη λίστα κλήσεών του, θα πρέπει να ταυτοποιηθεί με το κατάλληλο username/password. Η ταυτοποίηση του χρήστη και η ακόλουθη είσοδος στο προφίλ του αποκαλύπτει τα προσωπικά δεδομένα του στην εταιρεία, καθώς ο διακομιστής διαδικτύου είναι υπό τη διαχειριστική ευθύνη της εταιρείας. Συνεπώς, θα πρέπει να ληφθεί μέριμνα για να διασφαλιστεί η ιδιωτικότητα του χρήστη.

Η λύση που προτείνεται είναι να υλοποιηθεί στον κόμβο που βρίσκεται υπό την διαχειριστική ευθύνη της Α.Α., ένας διακομιστής διαδικτύου που θα διαχειρίζεται τις συναλλαγές, που σχετίζονται με επεξεργασία και ανταλλαγή των προσωπικών δεδομένων (τον ονομάζουμε Δ.Δ.Π.Δ Διακομιστής Διαδικτύου Προσωπικών Δεδομένων). Συγκεκριμένα: αφού ένας χρήστης συμπληρώσει τα στοιχεία ταυτοποίησής του στην κατάλληλη φόρμα στη διαδικτυακή πύλη της εταιρείας, η καταχώρισή τους θα γίνει στο Δ.Δ.Π.Δ, ενώ παράλληλα ο χρήστης θα ανακατευθυνθεί (redirect) στις σελίδες επεξεργασίας του προσωπικού του προφίλ. Οι σελίδες αυτές θα κατασκευάζονται δυναμικά από το Δ.Δ.Π.Δ και θα έχουν υβριδικό περιεχόμενο. Συγκεκριμένα: ο Δ.Δ.Π.Δ θα επικοινωνεί με το διακομιστή διαδικτύου της εταιρείας από τον οποίο θα παίρνει στατικές σελίδες χωρίς προσωπικά δεδομένα (φόρμες προς συμπλήρωση, μενού πλοήγησης στη διαδικτυακή πύλη κ.α) και θα τις επεξεργάζεται σε δεύτερη φάση συμπληρώνοντας τα κενά πεδία με τα προσωπικά δεδομένα του συγκεκριμένου χρήστη. Ο Δ.Δ.Π.Δ μ' αυτόν τον τρόπο θα δρα σαν ενδιάμεσος στην επικοινωνία του χρήστη με την πύλη της εταιρείας, εισάγοντας την προσωπική πληροφορία στην οποία δεν έχει πρόσβαση η εταιρεία. Με τον μηχανισμό που περιγράφεται παραπάνω καταφέρνουμε να δίνουμε μεγαλύτερη ευελιξία στην εταιρεία παροχής υπηρεσιών στο σχεδιασμό της διαδικτυακής πύλης, ενώ προστατεύεται η ιδιωτικότητα του χρήστη. Ταυτόχρονα, αποφορτίζεται η Α.Α από τον ανασχεδιασμό των σελίδων του προσωπικού προφίλ χρηστών κάθε φορά που επιλέγει η εταιρεία να κάνει ανασχεδιασμό της σελίδας της ή οπτικές παρεμβάσεις σ' αυτήν. Μπορεί βέβαια να φαίνεται πολύπλοκη η διαδικασία τροποποίησης της σελίδας για να συμπληρωθούν τα προσωπικά στοιχεία, η υλοποίηση όμως του μηχανισμού αυτού είναι αρκετά εύκολη. Αρκεί να υπάρχουν κάποιες προκαθορισμένες ετικέτες (tags) στο σώμα των σελίδων HTML, τις οποίες θα ανιχνεύει ο Δ.Δ.Π.Δ και θα παρεμβάλλει τα κατάλληλα δεδομένα στις αντίστοιχες θέσεις.

Πέρα από τις προκαθορισμένες ετικέτες, όλο το υπόλοιπο περιεχόμενο της σελίδας μπορεί να τροποποιηθεί κατά τη βούληση της εταιρείας.

Εκτός από την παραπάνω μέθοδο μπορεί να χρησιμοποιηθεί και μια απλούστερη, αν θεωρήσουμε ότι η διαδικτυακή πύλη της εταιρείας βασίζεται σε κάποιο σύστημα διαχείρισης περιεχομένου (CMS) που χρησιμοποιεί portlets, κάτι που αποτελεί τον κανόνα των περιπτώσεων. Τα portlets είναι μικρές διαδικτυακές εφαρμογές κάθε μία από τις οποίες εμφανίζεται σ' ένα ορισμένο τμήμα της σελίδας και επιτελεί μια αυτόνομη λειτουργία. Η διαδεδομένη αυτή τεχνολογία επιτρέπει στους περιηγητές ιστού να λαμβάνουν τμήματα μιας σελίδας HTML από διαφορετικούς διακομιστές ιστού. Αξιοποιώντας αυτήν την τεχνολογία μπορεί να γίνει κατάλληλος σχεδιασμός της ιστοσελίδας, ώστε το τμήμα της σελίδας που χρησιμοποιείται για την επεξεργασία των προσωπικών δεδομένων να ενσωματωθεί σ' ένα portlet, το οποίο λαμβάνει το περιεχόμενό του από το Δ.Δ.Π.Δ, ενώ η υπόλοιπη σελίδα θα φορτώνεται από το διακομιστή διαδικτύου της εταιρείας. Οι ανεξάρτητες σύνοδοι που δημιουργούνται κατά την φόρτωση των σελίδων δίνουν τη δυνατότητα για χρήση του πρωτοκόλλου HTTPS, οπότε οι λειτουργίες πιστοποίησης και ασφάλειας στην επικοινωνία με το Δ.Δ.Π.Δ. είναι εξασφαλισμένες. Η συγκεκριμένη λύση προσφέρει περισσότερη ευελιξία και ευκολία υλοποίησης, ενώ υποστηρίζεται από όλες τις διαδεδομένες τεχνολογίες ανάπτυξης διαδικτυακών τόπων.

3.3.5.2 Πρόσβαση της εταιρείας σε στατιστικά στοιχεία πελατολογίου

Μια άλλη λειτουργία, που προβλέπεται από το επιχειρηματικό μοντέλο της εταιρείας παροχής της υπηρεσίας, είναι η επεξεργασία των προσωπικών δεδομένων των χρηστών με σκοπό την εξαγωγή ανώνυμης στατιστικής πληροφορίας, απαραίτητης για τη λειτουργία της (σχεδιασμός δικτύου, τμήμα διαφήμισης και προώθησης προϊόντων). Η εταιρεία μπορεί εναλλακτικά να εμπορευτεί στατιστικά στοιχεία του πελατολογίου της σε ενδιαφερόμενες τρίτες εταιρείες. Ένα κρίσιμο σημείο της λειτουργίας του συστήματος είναι ο τρόπος με τον οποίο θα γίνεται η επεξεργασία των προσωπικών δεδομένων των χρηστών ώστε να μπορεί να προκύψει στατιστική πληροφορία, ενώ ταυτόχρονα να εξασφαλίζεται ότι αυτή η πληροφορία δεν μπορεί να συνδεθεί με συγκεκριμένους συνδρομητές.

Η πιο ασφαλής λύση σε αυτό το πρόβλημα είναι η Α.Α να δίνει στην εταιρεία πρόσβαση στη βάση μέσω μιας συγκεκριμένης διεπαφής (interface), η οποία να μπορεί να εκτελέσει προκαθορισμένα ερωτήματα, που είναι εξασφαλισμένο ότι δεν μπορούν να αποκαλύψουν τα προσωπικά δεδομένα του χρήστη. Η Α.Α σε συνεργασία με την εταιρεία παροχής υπηρεσιών διαδικτυακής τηλεφωνίας θα διαμορφώνουν τα ερωτήματα αυτά, έτσι ώστε και η εταιρεία να μπορεί να επεξεργάζεται ανώνυμα στατιστικά στοιχεία (aggregate data) και να εξασφαλίζεται η προστασία των προσωπικών δεδομένων. Η λύση αυτή είναι η πιο ασφαλής και η απλούστερη στην υλοποίηση, αλλά δεν παρέχει ευελιξία. Η υλοποίηση ενός νέου ερωτήματος θα πρέπει να περνάει από χρονοβόρες διαδικασίες ελέγχου από την Α.Α. και τελικής εφαρμογής στη διεπαφή επικοινωνίας.

Μια πιο ευέλικτη λύση στο συγκεκριμένο πρόβλημα, η οποία διατηρεί μέρος της εκφραστικής δύναμης της γλώσσας SQL και της αποδοτικότητας μιας βάσης δεδομένων, είναι η διατήρηση μιας διεπαφής, η οποία θα χρησιμοποιεί ερωτήματα SQL για την εξαγωγή των πληροφοριών. Το ζητούμενο είναι να γίνεται αυτοματοποιημένα ο έλεγχος και η τροποποίηση των ερωτημάτων, που εκτελεί η εταιρεία, με κατάλληλο τρόπο ώστε να προστατεύεται η ιδιωτικότητα των χρηστών. Τα ερωτήματα, που εκτελεί η εταιρεία στη

βάση, θα εξετάζονται και αν δεν πληρούν κάποιες προϋποθέσεις είτε θα απορρίπτονται, είτε θα τροποποιούνται ώστε τα αποτελέσματα να μην αποκαλύπτουν προσωπικά δεδομένα συγκεκριμένων χρηστών. Ο τρόπος που μπορεί να υλοποιηθεί αυτό είναι με τη μοντελοποίηση των προσωπικών δεδομένων των χρηστών σε μια οντολογία, η οποία θα περιέχει επίσης τις προϋποθέσεις και τη μορφή των δεδομένων που μπορούν να αποκαλυφθούν. Στην ίδια οντολογία μοντελοποιούνται πιθανές μορφές ερωτημάτων προς τη βάση δεδομένων (range queries με ομαδοποίηση, ακριβές ερώτημα πάνω σε μία στήλη καθώς και άλλα πιθανά). Στις κλάσεις, που αντιπροσωπεύουν τα προσωπικά δεδομένα, υπάρχουν ιδιότητες, οι οποίες περιγράφουν σε ποια ερωτήματα μπορεί να χρησιμοποιηθεί κάθε προσωπικό δεδομένο. Επίσης, υπάρχουν προσωπικά δεδομένα, τα οποία μπορούν να εκφρασθούν με διαφορετικά επίπεδα ακρίβειας. Για παράδειγμα, η διεύθυνση του χρήστη μπορεί να εκφρασθεί ως πόλη, περιοχή, δρόμος ή ακριβής διεύθυνση. Η οντολογία χρησιμοποιώντας κατάλληλους κανόνες μπορεί να ελέγχει αν ένα ερώτημα αποκαλύπτει στην εταιρεία σημαντική προσωπική πληροφορία για τους χρήστες. Σε περίπτωση που συμβαίνει αυτό, αν είναι δυνατόν, θα μετασχηματίζει το ερώτημα σ' ένα που επιστρέφει πιο ασαφή πληροφορία, αλλιώς απλά θα το απορρίπτει.

Για να γίνει πιο σαφής η συγκεκριμένη ιδέα παρατίθεται τα παρακάτω παραδείγματα: Έστω ότι η εταιρεία εκτελεί ένα ερώτημα σχετικά με τον αριθμό των πελατών σε κάθε περιοχή της Αθήνας. Η οντολογία θα ελέγξει το ερώτημα και θα το επιτρέψει καθώς αποτελεί ένα ερώτημα με ομαδοποίηση πάνω σ' ένα αρκετά γενικό χαρακτηριστικό (Περιοχή). Αντίθετα, ένα ερώτημα του αριθμού των πελατών σε κάθε δρόμο της Αθήνας θα απορριφθεί καθώς αποτελεί ένα ερώτημα με ομαδοποίηση πάνω σ' ένα πολύ ειδικό χαρακτηριστικό (Δρόμος). Επίσης, ένα ερώτημα που θα παρουσιάζει την ακριβή ημερομηνία γέννησης των συνδρομητών σε μια περιοχή της Αθήνας θα πρέπει είτε να απορριφθεί, είτε να τροποποιηθεί σ' ένα ερώτημα, που θα παρουσιάζει τον αριθμό συνδρομητών μιας περιοχής σε κάθε ηλικιακή ομάδα. Η συγκεκριμένη ιδέα αποτελεί επέκταση του ερευνητικού τομέα που μελετάει την τροποποίηση ερωτημάτων σε βάσεις δεδομένων με βάση τη σημασιολογία αυτών (Semantic Query Optimisation, Sematic Query Reformulation) [36],[37]. Υπάρχουσες εφαρμογές του συγκεκριμένου τομέα είναι η μετατροπή ενός ερωτήματος με βάση τη σημασιολογία των εμπλεκόμενων πληροφοριών για την παραγωγή πληρέστερων αποτελεσμάτων, ή τη βελτίωση της απόδοσης του ερωτήματος. Η συγκεκριμένη διπλωματική προτείνει τη χρήση σημασιολογικών μοντέλων για τη μετατροπή ερωτημάτων με σκοπό την προστασία προσωπικών δεδομένων, που βρίσκονται στη βάση δεδομένων.

Το γεγονός ότι το 87% του πληθυσμού των Ηνωμένων Πολιτειών της Αμερικής μπορεί να προσδιορισθεί μοναδικά από τον ταχυδρομικό του κώδικα, το φύλο και την ημερομηνία γέννησης κάνει φανερό το πόσο δύσκολο είναι να προστατευθούν τα προσωπικά δεδομένα ακόμα και όταν υπάρχει μερική πρόσβαση σ' αυτά. Γι' αυτόν το λόγο και για να εξασφαλισθούν ακόμα περισσότερο τα προσωπικά δεδομένα των χρηστών, μπορούμε να χρησιμοποιήσουμε εκτός από την οντολογία και άλλες τεχνολογίες προστασίας της ιδιωτικότητας, που βασίζονται στη μετά-επεξεργασία των δεδομένων προς δημοσίευση ώστε να καταστεί στατιστικά απίθανη η εξαγωγή πληροφοριών για ένα χρήστη. Ενδεικτικά οι πιο διαδεδομένες μέθοδοι είναι: το k-Anonymity, το l-diversity και το m-Invariance [38]-[40]. Αυτό που εξασφαλίζεται με την εφαρμογή αυτών των μεθόδων είναι η αδυναμία ενός εξωτερικού δράστη (επιτιθέμενος) να εξάγει ακριβή πληροφορία για κάποια συγκεκριμένη εγγραφή στη βάση δεδομένων, χρησιμοποιώντας ήδη υπάρχοντες πίνακες ή προηγούμενες δημοσιευμένες εκδόσεις των ίδιων δεδομένων. Αυτό επιτυγχάνεται με συγκεκριμένους

αλγορίθμους, οι οποίοι ομαδοποιούν τα δεδομένα με τέτοιο τρόπο ώστε, έπειτα από συνένωση του δημοσιευμένου πίνακα με κάποιον ήδη υπάρχοντα, να μην αποκαλύπτονται συγκεκριμένες πληροφορίες για κάποια εγγραφή. Το αποτέλεσμα εφαρμογής των αλγορίθμων είναι ο διαχωρισμός των αποτελεσμάτων σε ομοιογενείς κλάσεις κάθε μία από τις οποίες περιέχει πολλές εγγραφές με παρόμοιες, αλλά όχι ίδιες τιμές. Με κατάλληλη ομαδοποίηση των δεδομένων είναι αδύνατο κάποιος να αποδώσει συγκεκριμένη τιμή σε κάποια εγγραφή. Φυσικό επακόλουθο αυτής της διαδικασίας είναι η απώλεια πληροφορίας, παρά το ότι οι αλγόριθμοι μπορούν να βελτιστοποιηθούν, ώστε να επιτευχθεί η ελάχιστη απώλεια δεδομένων για ένα δεδομένο επίπεδο προστασίας. Αυτό δεν επηρεάζει την αποτελεσματικότητα των συγκεκριμένων τεχνικών καθώς στατιστικά δεδομένα μπορούν να εξαχθούν και από τις ομαδοποιημένες εγγραφές. Οι διαφορετικές τεχνικές διαφοροποιούνται στο ποια δεδομένα επιδιώκουν να προστατεύσουν. Πρακτικά, η τεχνική k-Anonymity εξασφαλίζει ότι ο επιτιθέμενος το πολύ με πιθανότητα 1/k θα ανακαλύψει σε ποιον αναφέρεται μια εγγραφή, η τεχνική l-diversity εξασφαλίζει ότι ο επιτιθέμενος το πολύ με πιθανότητα 1/l θα ανακαλύψει τα ευαίσθητα δεδομένα ενός ατόμου, ανεξάρτητα σε ποια εγγραφή ανήκει αυτό το άτομο και η τεχνική m-Invariance επεκτείνει την προηγούμενη ώστε να μπορεί να εφαρμοσθεί σε δυναμικά δεδομένα (δεδομένα που τροποποιούνται και αναδημοσιεύονται).

Συμπερασματικά: με χρήση των παραπάνω τεχνικών σε συνδυασμό με την οντολογία μπορούμε να εξασφαλίσουμε τόσο την πρόσβαση της εταιρείας σε ανώνυμα στατιστικά δεδομένα, όσο και την προστασία των προσωπικών δεδομένων κάθε πελάτη.

3.3.6 Ζητήματα Πιστοποίησης

Ένα ακόμα ζήτημα που ανακύπτει κατά τη λειτουργία του συστήματος είναι η ταυτοποίηση των χρηστών και η εξουσιοδότηση τους για τη λήψη των υπηρεσιών. Όπως ήδη αναφέρθηκε, το πρωτόκολλο SIP παρέχει ενσωματωμένους μηχανισμούς για την ταυτοποίηση των χρηστών με χρήση ειδικών απαντήσεων (407 Authentication required) και αυτή πραγματοποιείται μέσω χρήσης username και password, αλλά και με χρήση ψηφιακών πιστοποιητικών. Για τις υπηρεσίες που βασίζονται στο SIP η λειτουργία αυτή επιτελείται στο Διακομιστή Καταχώρισης Χρηστών SIP για τις υπηρεσίες, που ο πελάτης λειτουργεί ως παραλήπτης και στον Ενδιάμεσο Διακομιστή SIP γι' αυτές που λειτουργεί ως αποστολέας. Για τις υπόλοιπες υπηρεσίες, που παρέχονται στο επιχειρηματικό μοντέλο, όπως η επεξεργασία του προφίλ του χρήστη και η παρακολούθηση της λίστας κλήσεων τους, η ταυτοποίηση πραγματοποιείται στο Διακομιστή Διαδικτύου με κάποιες από τις μεθόδους που παρέχει το πρωτόκολλο HTTP. Παρ' όλα αυτά η ταυτοποίηση των χρηστών επιβάλει την επεξεργασία ευαίσθητων προσωπικών δεδομένων και προφανώς μπορεί να αποκαλύψει τις ταυτότητες των χρηστών, που λαμβάνουν ή αιτούν μια υπηρεσία. Γι αυτό το λόγο η διαδικασία ταυτοποίησης των χρηστών πρέπει απαραιτήτως να γίνεται στο Δ.Π.Ι. ώστε να προστατεύονται οι ταυτότητες των χρηστών.

- Κατά την είσοδο ενός χρήστη στο σύστημα, περίπτωση η οποία αναλύθηκε σε προηγούμενη παράγραφο, ο χρήστης σε συνδυασμό με την παραλαβή ενός προσωρινού ανώνυμου SIP URI λαμβάνει από το Δ.Π.Ι. και ένα έγκυρο username και password, που μπορεί να χρησιμοποιήσει για την είσοδο του στο σύστημα.

- Κατά την αποστολή ενός μηνύματος-αίτησης SIP, ο Δ.Π.Ι. παρεμβάλλεται έτσι και αλλιώς στη διαδρομή του μηνύματος με σκοπό την προστασία της ιδιωτικότητας του αποστολέα, οπότε μπορεί ταυτόχρονα να υλοποιήσει και την πολιτική ταυτοποίησης της εταιρείας παροχής υπηρεσίας με χρήση των παρεχομένων μεθόδων του SIP για ταυτοποίηση.
- Κατά την είσοδο ενός χρήστη στο προσωπικό του προφίλ στην ιστοσελίδα της εταιρείας η πιστοποίηση παρέχεται από τους μηχανισμούς του πρωτόκολλου HTTPS, το οποίο και χρησιμοποιείται για την επικοινωνία με το Δ.Δ.Π.Δ..

Στον παρακάτω πίνακα παρουσιάζονται συνοπτικά οι λειτουργίες που επιτελεί η κάθε διαχειριστική οντότητα

Διαχειριστική Οντότητα	Λειτουργίες
Ανεξάρτητη Αρχή	• Υλοποίηση μηχανισμού προστασίας της διεύθυνσης IP των χρηστών με διαχείριση ενός κατανεμημένου δικτύου ανωνυμίας βασισμένο στο onion routing. • Υλοποίηση μηχανισμού προστασίας των προσωπικών δεδομένων που περιέχονται στα εξερχόμενα μηνύματα-αιτήσεις των χρηστών. Ο μηχανισμός αυτός βασίζεται στο πρότυπο του διακομιστή Ιδιωτικότητας (Privacy Server), ο οποίος προτείνεται στο RFC 3323 και η μετατροπή των μηνυμάτων SIP από την Α.Α σε αποδεχτές μορφές κατά την εισαγωγή τους στο σύστημα πρέπει να υλοποιείται εφόσον τα τερματικά συστήματα δεν παρέχουν εξαρχής αυτήν την λειτουργία. • Δημιουργία και διαχείριση προσωρινών SIP URI ψευδωνύμων, ώστε κάθε φορά που κάποιος χρήστης εισέρχεται στο σύστημα να απολαμβάνει προστασία της Ιδιωτικότητας του στα εισερχόμενα προς αυτόν αιτήματα, Η προστασία αυτή πρέπει να επεκτείνεται και στις υπηρεσίες που συνεχίζουν να παρέχονται ακόμα και όταν ο χρήστης είναι εκτός συστήματος (offline). Για την υλοποίηση της προστασίας Ιδιωτικότητας η Α.Α. θα πρέπει να παρεμβάλλεται στο κανάλι σηματοδοσίας και να μετατρέπει όλη την κίνηση που διέρχεται από τους χρήστες και από άλλες διαχειριστικές οντότητες προς την εταιρία με βάση ένα πίνακα αντιστοίχησης ψευδωνύμων. • Πιστοποίηση χρηστών, ώστε η εταιρία παροχής υπηρεσίας να μην χρειάζεται να διαχειριστεί τα προσωπικά δεδομένα που είναι απαραίτητα για την λειτουργία της πιστοποίησης. • Αποθήκευση όλων των προσωπικών δεδομένων των χρηστών που διαχειρίζεται το συστήμα συμπεριλαμβανομένων των προσωπικών προφίλ των χρηστών και του ιστορικού αντιστοίχησης ψευδωνύμων - ονομάτων SIP, ώστε να είναι δυνατή η ανακατασκευή της λίστας κλήσεων σε συνδυασμό με τα στοιχεία που κρατάει η εταιρία παροχής υπηρεσίας. • Υλοποίηση συμπληρωματικής Διαδικτυακής υπηρεσίας διαχείρισης των προφίλ των χρηστών. • Υλοποίηση μηχανισμού πρόσβασης στα προσωπικά δεδομένα, ώστε η εταιρία παροχής υπηρεσίας να μπορεί να συνεχίσει το επιχειρηματικό της μοντέλο ως προς την πώληση χρήσιμων στοιχείων πελατολογίου. • Διατήρηση λογαριασμών χρέωσης για κάθε χρήστη του συστήματος σε τρίτη εταιρία παροχής υπηρεσιών ασφαλούς χρέωσης.
Πράκτορας Χρήστη	• Υλοποίηση λειτουργιών του SIP που αφορούν τους πελάτες του συστήματος. • Υλοποίηση λειτουργιών κόμβων του κατανεμημένου δικτύου ανωνυμίας βασισμένο στο onion routing. • Προαιρετική υλοποίηση μηχανισμού προστασίας Ιδιωτικότητας σε τοπικό επίπεδο για εξερχόμενα μηνύματα αιτήσεις, όπως αυτός καθορίζεται από το RFC 3323. Σε κάθε περίπτωση θα πρέπει ο πελάτης να υλοποιεί μηχανισμό αιτήσεων προς την Α.Α. για παροχή υπηρεσιών προστασίας Ιδιωτικότητας. • Διαχείριση κλειδιών κρυπτογραφημένης επικοινωνίας, όπως για παράδειγμα στην περίπτωση της λίστας φίλων.
Εταιρία παροχής υπηρεσίας	• Υλοποίηση αρχιτεκτονικής SIP για παροχή υπηρεσιών εγκατάστασης συνόδου, αποστολής σύντομων μηνυμάτων, παροχής υπηρεσιών παρουσίας. • Υλοποίηση διαδικτυακής πύλης για την πρόσβαση στην διαδικασία εγγραφής στο σύστημα και των συμπληρωματικών υπηρεσιών. • Αποθήκευση των πληροφοριών που σχετίζονται με την διεκπεραίωση των κλήσεων.

4

Ανάλυση Απαιτήσεων Συστήματος

Στο παρόν κεφάλαιο παρουσιάζεται η προτεινόμενη αρχιτεκτονική του συστήματος με τη βοήθεια σεναρίων λειτουργίας και με χρήση της γλώσσας UML για την εκπόνηση διαγραμμάτων χρήσης και ακολουθιακών διαγραμμάτων. Ειδικά στα ακολουθιακά διαγράμματα παρουσιάζονται τόσο τα μηνύματα SIP, που διαβιβάζονται στο σύστημα, όσο και τα ερωτήματα στις βάσεις δεδομένων και οι κλήσεις διαδικασιών του συστήματος.

4.1 Δράστες Συστήματος

4.1.1 Σύνοψη

Αρχικά θα παρουσιαστούν οι Δράστες του συστήματος με βάση τις τρεις διαφορετικές οντότητες που δρουν στο σύστημα.

1. *Ο Πελάτης του συστήματος τηλεφωνίας διαδικτύου (VoIP):* αλλιώς Χρήστης της υπηρεσίας, χρησιμοποιεί ένα ή περισσότερα προγράμματα και υλικό για να λάβει τις υπηρεσίες, που παρέχονται από το σύστημα. Είναι ενεργός χρήστης αφού μπορεί να δημιουργήσει νέες διαδικασίες στο σύστημα. (Αιτήσεις κλήσεων και παροχής υπηρεσιών SIP, Αποστολή σύντομων μηνυμάτων, Αιτήσεις τροποποίησης προσωπικού προφίλ, Εγγραφή και Είσοδος στο σύστημα). Σ' αυτόν το χρήστη συμπεριλαμβάνουμε τις λειτουργίες και τα χαρακτηριστικά των δομικών στοιχείων UAC, UAS και Τερματικό πελάτη, όπως αυτά περιγράφτηκαν στις προηγούμενες παραγράφους. Τέλος, ο συγκεκριμένος δράστης επιτελεί όλες της λειτουργίες προστασίας της ιδιωτικότητας που απασχολούν τη διαχειριστική οντότητα του πελάτη της υπηρεσίας, όπως αναφέρονται στο τέλος του Κεφαλαίου 3.

2. *Εταιρεία παροχής υπηρεσιών VoIP:* Είναι υπεύθυνη για τη διεκπεραίωση των κλήσεων, την αποθήκευση των στοιχείων αυτών και γενικά την παροχή της υπηρεσίας VoIP καθώς και των συμπληρωματικών υπηρεσιών. Η εταιρεία εκπροσωπείται από τους παρακάτω δράστες:
    a. *Ενδιάμεσος Διακομιστής:* Επιτελεί τις λειτουργίες που αντιστοιχούν στον Ενδιάμεσο Διακομιστή SIP, όπως περιγράφεται στην ενότητα 2.3.6
    b. *Διακομιστής Θέσης:* Επιτελεί τις λειτουργίες που αντιστοιχούν στο Διακομιστή Θέσης SIP, όπως περιγράφεται στην ενότητα 2.3.6
    c. *Διακομιστής Καταχώρισης Χρηστών:* Επιτελεί τις λειτουργίες που αντιστοιχούν στο Διακομιστή Καταχώρισης Χρηστών SIP, όπως περιγράφεται στην ενότητα 2.3.6
    d. *Διακομιστής Διαδικτύου:* Είναι υπεύθυνος για τη διαχείριση του ιστοτόπου της εταιρείας παροχής υπηρεσίας.
    e. *Διακομιστής Μηνυμάτων:* Είναι υπεύθυνος για την αποθήκευση των σύντομων μηνυμάτων, όταν ο παραλήπτης τους δεν έχει εισέλθει στο σύστημα. Επίσης, αναλαμβάνει την επαναποστολή τους με την εγγραφή του παραλήπτη στο σύστημα
    f. *Διακομιστής Παρουσίας:* Επιτελεί τις λειτουργίες που αντιστοιχούν στο Διακομιστή Παρουσίας SIP, όπως αυτός περιγράφεται στην ενότητα 2.3.6
    g. *Βάση Δεδομένων:* Δες Βάση Δεδομένων 3c

3. *Ανεξάρτητη Αρχή:* Είναι ο οργανισμός διασφάλισης του απορρήτου των προσωπικών δεδομένων και χαίρει της εμπιστοσύνης τόσο των χρηστών, όσο και της ίδιας της εταιρείας παροχής υπηρεσίας. Οι δράστες της Α.Α. επιτελούν όλες τις λειτουργίες προστασίας της ιδιωτικότητας, που απασχολούν τη διαχειριστική οντότητα της Α.Α. , όπως αναφέρονται στο τέλος του Κεφαλαίου 3 και είναι οι παρακάτω:
    a. *Διακομιστής Προστασίας Ιδιωτικότητας:* Είναι ο βασικός διακομιστής της Α.Α. και ασχολείται με την τροποποίηση (κρυπτογράφηση, δημιουργία ψευδώνυμων κ.τ.λ.) των ευαίσθητων στοιχείων που περνάνε στην εταιρεία παροχής υπηρεσίας ώστε να προστατεύονται τα προσωπικά δεδομένα των χρηστών. Η λειτουργία του και διαχείρισή του είναι αποκλειστική ευθύνη της Α.Α.
    b. *Διακομιστής Διαδικτύου Προσωπικών Δεδομένων:* Είναι συμπληρωματικός διακομιστής του Διακομιστή Διαδικτύου της εταιρείας παροχής υπηρεσίας για να διαχειρίζεται τις ιστοσελίδες αυτές, οι οποίες περιλαμβάνουν ανταλλαγή προσωπικών δεδομένων.
    c. *Βάση Δεδομένων:* Η Βάση Δεδομένων του συστήματος είναι υπό τη διαχειριστική ευθύνη και των δύο πλευρών. Η Ανεξάρτητη Αρχή είναι υπεύθυνη για τη διαχείριση του κομματιού που αφορά τα προσωπικά δεδομένα, ενώ η εταιρεία παροχής υπηρεσίας είναι υπεύθυνη για όλα τα υπόλοιπα στοιχεία που είναι απαραίτητα. Η πρόσβαση της εταιρείας παροχής υπηρεσίας στα προσωπικά δεδομένα πρέπει να περνάει από ένα μηχανισμό, ο οποίος θα περιορίζει την ανάκτηση πληροφοριών σύμφωνα με τη νομοθεσία.

Εκτός από τις τρείς παραπάνω διαχειριστικές οντότητες που συμμετέχουν στο σύστημα, θα εισάγουμε στο μοντέλο λειτουργίας και τις παρακάτω, οι οποίες εμφανίζονται σε συγκεκριμένα σενάρια λειτουργίας του συστήματος

4. *Εταιρεία παροχής υπηρεσίας ασφαλούς χρέωσης:* Είναι υπεύθυνη για τη διεκπεραίωση της χρέωσης των υπηρεσιών, που παρέχονται στους χρήστες.
5. *Τρίτη Ανεξάρτητη Αρχή:* Σύμφωνα με τη νομοθεσία έχει πρόσβαση υπό προϋποθέσεις στα αρχεία τηλεφωνικών κλήσεων των εταιρειών παροχής υπηρεσιών τηλεφωνίας.
6. *Τρίτη εταιρεία:* Είναι ένας φορέας, ο οποίος ενδιαφέρεται για στατιστικά στοιχεία του πελατολογίου της εταιρείας παροχής υπηρεσιών και έχει σύμβαση μ' αυτή για την παροχή τέτοιων υπηρεσιών.

4.1.2 Ορισμοί Δραστών

4.1.2.1 Πελάτης συστήματος

Περιγραφή	Πελάτης του συστήματος είναι σε κάθε περίπτωση το κατάλληλο πρόγραμμα, το οποίο υλοποιεί όλες τις απαιτούμενες λειτουργίες που χρειάζεται ο Χρήστης της υπηρεσίας. Αυτές περιλαμβάνουν την εγγραφή και την είσοδο στο σύστημα, τη διαχείριση του προσωπικού προφίλ του Χρήστη, την πραγματοποίηση κλήσεων, την αποστολή σύντομων μηνυμάτων και γενικά την αίτηση υπηρεσιών SIP. Περιλαμβάνει τις λειτουργίες των UAC, UAS και τερματικό χρήστη, ενώ για την επίτευξη της προστασίας ιδιωτικότητας επιτελεί τις λειτουργίες που αντιστοιχούν στη διαχειριστική οντότητα των πελατών του συστήματος, όπως αυτές περιγράφονται στο τέλος του Κεφαλαίου 3
Συνώνυμα	Καλών, Καλούμενος, Αποστολέας, Παραλήπτης, Ενδιαφερόμενος, Προτιμώμενος, Πελάτης
Τύπος Δράστη	Ενεργός, υποχρεωτικός
Διαχειριστική οντότητα	Πελάτης συστήματος

4.1.2.2 Ενδιάμεσος Διακομιστής

Περιγραφή	Ο διακομιστής αυτός χρησιμοποιείται για την επίτευξη των κλήσεων και τη σύνδεση των χρηστών. Επίσης, παρακολουθεί την εξέλιξη της κλήσης έτσι ώστε, όταν τελειώσει, να κάνει την κατάλληλη εγγραφή στο αρχείο κλήσεων. Σ' αυτόν υλοποιούνται οι πολιτικές της εταιρείας καθώς και τυχόν έλεγχοι που αφορούν τις κλήσεις, όπως μια υπηρεσία προώθησης ή φραγής.
Συνώνυμα	Ε.Δ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.3 Διακομιστής Θέσης

Περιγραφή	Είναι υπεύθυνος για την παρακολούθηση των χρηστών που είναι συνδεδεμένοι στο σύστημα και διατηρεί την πληροφορία τοποθεσίας τους (IP διεύθυνση) ώστε να πραγματοποιούνται οι κλήσεις.
Συνώνυμα	Δ.Θ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.4 Διακομιστής Καταχώρισης Χρηστών

Περιγραφή	Ο διακομιστής χρησιμοποιείται για την είσοδο των χρηστών στο σύστημα σύμφωνα με τις επιταγές της αρχιτεκτονικής του SIP και σ' αυτόν εκτελείται η πιστοποίηση των στοιχείων του χρήστη και διαπιστώνεται το πλήθος και το είδος των υπηρεσιών που θα λάβει από το σύστημα.
Συνώνυμα	Δ.Κ.Χ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.5 Διακομιστής Διαδικτύου

Περιγραφή	Διαχειρίζεται τον ιστότοπο της εταιρείας και είναι το σημείο όπου εγγράφονται οι νέοι πελάτες. Επίσης, προσφέρει και άλλες υπηρεσίες που ορίζει το επιχειρηματικό μοντέλο της εταιρείας. Επειδή βρίσκεται υπό τη διαχείριση της εταιρείας παροχής υπηρεσίας δεν επιτρέπεται να διαχειρίζεται σελίδες, που αφορούν την ανταλλαγή προσωπικών δεδομένων.
Συνώνυμα	Δ.Δ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.6 Διακομιστής Μηνυμάτων

Περιγραφή	Αποθηκεύει τα σύντομα μηνύματα, όταν ο παραλήπτης δεν έχει εισέλθει στο σύστημα. Όταν ο παραλήπτης εισέλθει στο σύστημα, προωθεί τα μηνύματα σ' αυτόν.
Συνώνυμα	Δ.Μ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.7 Διακομιστής Παρουσίας

Περιγραφή	Παρακολουθεί την παρουσία των χρηστών στο σύστημα και ειδοποιεί τους ενδιαφερόμενους τρίτους χρήστες για την πληροφορία παρουσίας τους.
Συνώνυμα	Δ.Π.
Τύπος Δράστη	Ενεργός, υποχρεωτικός
Διαχειριστική οντότητα	Εταιρεία Παροχής Υπηρεσίας

4.1.2.8 Διακομιστής Προστασίας Ιδιωτικότητας

Περιγραφή	Είναι υπεύθυνος για την προστασία των προσωπικών δεδομένων των πελατών της εταιρείας παροχής υπηρεσίας διαδικτυακής τηλεφωνίας. Εκτελεί όλες τις κατάλληλες λειτουργίες και μετατροπές ενώ υλοποιεί και το μηχανισμό, ο οποίος θα περιορίζει την πρόσβαση στο κομμάτι της Βάσης Δεδομένων, που περιέχει τα προσωπικά στοιχεία των χρηστών.
Συνώνυμα	Δ.Π.Ι.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Ανεξάρτητη Αρχή

4.1.2.9 Διακομιστής Διαδικτύου Προσωπικών Δεδομένων

Περιγραφή	Αποτελεί συμπλήρωμα του Διακομιστή Διαδικτύου και διαχειρίζεται τις ιστοσελίδες, που αφορούν την ανταλλαγή προσωπικών δεδομένων.
Συνώνυμα	Δ.Δ.Π.Δ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Ανεξάρτητη Αρχή

4.1.2.10 Βάση Δεδομένων

Περιγραφή	Αποθηκεύει όλα τα δεδομένα που είναι απαραίτητα για την λειτουργία του συστήματος. Χωρίζεται σε δύο μέρη ανάλογα με τη διαχειριστική ευθύνη. Η Ανεξάρτητη Αρχή είναι υπεύθυνη για τη διαχείριση του κομματιού που αποθηκεύονται τα προσωπικά δεδομένα, ενώ η Εταιρεία Παροχής Υπηρεσίας για το υπόλοιπο κομμάτι
Συνώνυμα	Βάση Προσωπικών Δεδομένων Β.Π.Δ. (Διαχείριση Α.Α.) Βάση Δεδομένων Β.Δ. (Διαχείριση Εταιρείας Παροχής Υπηρεσίας)
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Ανεξάρτητη Αρχή, Εταιρεία Παροχής Υπηρεσίας

4.1.2.11 Διακομιστής Ασφαλούς Χρέωσης

Περιγραφή	Η χρέωση των υπηρεσιών μπορεί να γίνεται από τρίτη εταιρεία, η οποία ειδικεύεται στις υπηρεσίες ασφαλούς χρέωσης.
Συνώνυμα	Δ.Α.Χ.
Τύπος Δράστη	Παθητικός, υποχρεωτικός
Διαχειριστική οντότητα	Τρίτη Εταιρεία Παροχής Υπηρεσίας Ασφαλούς Χρέωσης

4.1.2.12 Τρίτη Ανεξάρτητη Αρχή

Περιγραφή	Στα πλαίσια της πιστοποιημένης πρόσβασης στα προσωπικά δεδομένα, λόγω άρσης του απορρήτου των τηλεπικοινωνιών (lawful interception) , δίνεται η δυνατότητα σε τρίτη Ανεξάρτητη Αρχή να έχει πρόσβαση στη λίστα κλήσεων και στα προσωπικά δεδομένα.
Συνώνυμα	Ανεξάρτητος Φορέας
Τύπος Δράστη	Ενεργητικός, προαιρετικός
Διαχειριστική οντότητα	Τρίτη Ανεξάρτητη Αρχή

4.1.2.13 Τρίτη εταιρεία πελάτης

Περιγραφή	Μια τρίτη εταιρεία μπορεί να ενδιαφέρεται για στοιχεία του πελατολογίου της εταιρείας παροχής υπηρεσίας διαδικτυακής τηλεφωνίας.
Συνώνυμα	Όχι
Τύπος Δράστη	Ενεργητικός, προαιρετικός
Διαχειριστική οντότητα	Τρίτη Εταιρεία Πελάτης

4.2 Περιγραφές Σεναρίων Λειτουργίας

4.2.1 Εγγραφή στο σύστημα

Περιγραφή:

Για να παρέχονται υπηρεσίες VoIP σε κάποιον πελάτη, αυτός θα πρέπει πρώτα να έχει εγγραφεί στο σύστημα, δίνοντας τα προσωπικά του στοιχειά και τις προτιμήσεις του για τη δημιουργία του προφίλ του, καθώς και τα στοιχεία χρέωσης του για τις παρεχόμενες υπηρεσίες. Ο χρήστης λαμβάνει ένα όνομα χρήστη και ένα κωδικό πρόσβασης, τα οποία μπορεί να χρησιμοποιήσει για μελλοντική είσοδο στο σύστημα.

Δράστες:

Πελάτης συστήματος

Διακομιστής Διαδικτύου

Διακομιστής Διαδικτύου Προσωπικών Δεδομένων

Βάση Προσωπικών Δεδομένων

Διακομιστής Ασφαλούς Χρέωσης

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Ο Χρήστης μπαίνει στην ιστοσελίδα της εταιρείας και αιτείται την εγγραφή του στην υπηρεσία. Ο Διακομιστής Διαδικτύου επιστρέφει μια ηλεκτρονική φόρμα στην οποία ο χρήστης συμπληρώνει όλα τα απαραίτητα στοιχεία για τη λειτουργία της υπηρεσίας και την υποβάλλει στο σύστημα και συγκεκριμένα στο Διακομιστή Διαδικτύου Προσωπικών Δεδομένων. Από τα στοιχεία αυτά θα δημιουργηθεί ένα προσωπικό προφίλ χρήστη, το οποίο θα αποθηκευθεί στη Βάση Προσωπικών Δεδομένων. Ταυτόχρονα, δημιουργείται και ένας λογαριασμός χρέωσης του χρήστη στην εταιρεία παροχής υπηρεσίας ασφαλούς χρέωσης. Αν όλα τα στοιχεία εγκριθούν, τότε η εγγραφή επικυρώνεται και ο χρήστης διαθέτει πια το όνομα χρήστη και τον κωδικό πρόσβασης του.

Εναλλακτικές Πορείες Σεναρίου:

Εάν ο χρήστης παραλείψει να συμπληρώσει κάποιο απαραίτητο για την υπηρεσία πεδίο της φόρμας, τότε η εγγραφή δεν επικυρώνεται και ζητείται από το χρήστη η εισαγωγή του στοιχείου αυτού, ενώ ο χρήστης μπορεί ανά πάσα στιγμή να διακόψει τη διαδικασία εγγραφής χωρίς να κρατηθεί κανένα στοιχείο του από την εταιρεία.

Επεκτείνει:

Όχι.

4.2.2 Είσοδος στο Σύστημα

Περιγραφή:

Όταν ένας χρήστης επιθυμεί να χρησιμοποιήσει τις υπηρεσίες του συστήματος, πρέπει να εισέλθει σ' αυτό, δίνοντας το όνομα χρήστη και τον κωδικό πρόσβασής του. Μ' αυτόν τον τρόπο δημιουργείται στο σύστημα μια εγγραφή για την τρέχουσα θέση (διεύθυνση IP) του χρήστη ώστε να προωθούνται σωστά οι κλήσεις και τα μηνύματα. Η εγγραφή στο σύστημα γίνεται με χρήση προσωρινών ψευδωνύμων για την προστασία της ιδιωτικότητας των πελατών.

Δράστες:

Πελάτης συστήματος

Διακομιστής Προστασίας Ιδιωτικότητας

Διακομιστής Θέσης

Διακομιστής Καταχώρισης Χρηστών

Βάση Προσωπικών Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Ο Χρήστης αιτείται αρχικά από το Δ.Π.Ι. τη χορήγηση προσωρινού ψευδωνύμου για να εισέλθει στο σύστημα. Ο Δ.Π.Ι. ελέγχει αν θα πρέπει να δημιουργήσει ένα νέο ψευδώνυμο για το χρήστη ή έχει ήδη κάποια έγκυρη εγγραφή στη βάση του. Αν πρόκειται για είσοδο με νέο ψευδώνυμο, ο Δ.Π.Ι. παράγει το ψευδώνυμο, το οποίο συνοδεύεται και από ένα κατάλληλο κωδικό για πιστοποίηση του μηνύματος REGISTER. Τα παραπάνω στοιχεία επιστρέφονται στο Χρήστη μαζί με τη διάρκεια εγκυρότητας του νέου ψευδωνύμου και το αμέσως προηγούμενο έγκυρο ψευδώνυμο, αφού πρώτα γίνει η κατάλληλη εγγραφή γι' αυτά στο σύστημα πιστοποίησης του Δ.Κ.Χ. ώστε μελλοντικές αιτήσεις εισόδου να γίνουν αποδεκτές. Εν συνεχεία ο Δ.Π.Ι. πραγματοποιεί μια αίτηση εισόδου στο σύστημα και μ' αυτόν τον τρόπο ο Δ.Κ.Χ. μπορεί να εκτελέσει τον απαραίτητο έλεγχο πιστοποίησης και τελικά να δημιουργήσει την αντιστοίχιση μεταξύ Διεύθυνσης IP και ψευδωνύμου χρήστη, η οποία και αποθηκεύεται στο Διακομιστή Θέσης. Αν η είσοδος είναι επιτυχής, ο Δ.Π.Ι. αποθηκεύει στη Β.Π.Δ. την αντιστοίχιση του χρήστη με το ψευδώνυμο, που του δόθηκε καθώς και το χρόνο παραχώρησης και τη διάρκεια της.

Εναλλακτικές Πορείες Σεναρίου:

Αν ο χρήστης διαθέτει έγκυρο ψευδώνυμο από προηγούμενη εγγραφή μπορεί να εκτελέσει απευθείας αίτηση εισόδου στο Δ.Κ.Χ.

Επεκτείνει:

Όχι

4.2.3 Ανανέωση Προφίλ

Περιγραφή:

Ο χρήστης έχει τη δυνατότητα να δει προσωπικά του στοιχεία, που σχετίζονται με τη χρήση του συστήματος, όπως η λίστα κλήσεων, να διαχειρισθεί τα στοιχεία του προφίλ του καθώς και να αλλάξει κάποιες από τις επιλογές του. Αυτές οι δυνατότητες παρέχονται από τον ιστότοπο της εταιρείας, ενώ στο σενάριο αυτό η υλοποίηση του ιστοτόπου έχει γίνει με τη χρήση portlets.

Δράστες:

Πελάτης συστήματος

Διακομιστής Διαδικτύου

Διακομιστής Διαδικτύου Προσωπικών Δεδομένων

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Ο Χρήστης περιηγείται τον ιστότοπο της εταιρείας παροχής υπηρεσίας και αποφασίζει να δει ή να τροποποιήσει στοιχεία του προφίλ του. Χρησιμοποιώντας το κατάλληλο link ή το κατάλληλο portlet πιστοποιεί την ταυτότητά του στο Διακομιστή Διαδικτύου Προσωπικών Δεδομένων με τον κωδικό πρόσβασης του και αιτείται την τροποποιήση του προφίλ του. Ο Διακομιστής Διαδικτύου Προσωπικών Δεδομένων επιστρέφει μια ηλεκτρονική φόρμα στην οποία ο χρήστης ελέγχει και τροποποιεί τα προσωπικά του στοιχεία και τις επιλογές του και στη συνέχεια τυχόν τροποποιήσεις του προφίλ του χρήστη αποθηκεύονται στη Βάση Προσωπικών Δεδομένων. Τέλος, ο χρήστης έχει επίσης τη δυνατότητα σε άλλη σελίδα να δει αναλυτικά τα στοιχεία των κλήσεών του (ώρα, διάρκεια κλήσης και καλούμενος / καλών χρήστης).

Εναλλακτικές Πορείες Σεναρίου:

Εάν ο χρήστης εισάγει μη έγκυρα δεδομένα κατά την τροποποίηση του προφίλ του τότε η τροποποίηση δεν επικυρώνεται και ζητείται από το χρήστη η σωστή εισαγωγή των στοιχείων του.

Ο χρήστης μπορεί ανά πάσα στιγμή να διακόψει τη διαδικασία τροποποίησης χωρίς να αποθηκευθεί κανένα στοιχείο που έχει τροποποιηθεί.

Επεκτείνει:

Όχι.

4.2.4 Εγκαθίδρυση Συνόδου (απλή περίπτωση Καλών-Καλούμενος ανήκουν στην ίδια διαχειριστική οντότητα)

Περιγραφή:

Ο Καλών επιθυμεί να εγκαθιδρύσει μια σύνοδο επικοινωνίας SIP με τον Καλούμενο. Αποστέλλει την αίτηση του στο σύστημα και αυτό εγκαθιδρύει με τη βοήθεια της δρομολόγησης από τον Ενδιάμεσο Διακομιστή της διαχειριστικής οντότητας ένα απευθείας κανάλι επικοινωνίας μεταξύ των δύο πλευρών.

Δράστες:

Καλών

Καλούμενος

Διακομιστής Προστασίας Ιδιωτικότητας

Διακομιστής Θέσης

Ενδιάμεσος Διακομιστής

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών
- Καλών και Καλούμενος ανήκουν στην ίδια διαχειριστική οντότητα.

Κείμενο Σεναρίου:

Ο Καλών αιτείται την συνδεσή του με τον Καλούμενο, χρησιμοποιώντας το όνομα χρήστη αυτού και αιτείται την παροχή συγκεκριμένων υπηρεσιών προστασίας ιδιωτικότητας, θέτοντας την κατάλληλη επιλογή στην επικεφαλίδα «Privacy» του μηνύματος-αίτησης. Ταυτόχρονα, εφαρμόζει ο ίδιος, αν το επιθυμεί και μπορεί, το επίπεδο προστασίας ιδιωτικότητας user, κρυπτογραφεί τις επικεφαλίδες, που θέλει να εμφανιστούν στον τελικό χρήστη σ' ένα μήνυμα S/MIME και εισάγει στο μήνυμα κάποια πιστοποίηση της ταυτότητας του. Ο Διακομιστής Προστασίας Ιδιωτικότητας εκτελεί έναν έλεγχο πιστοποίησης στην ταυτότητα του Καλούντα και εφόσον αυτός είναι επιτυχής, ασχολείται με την υλοποίηση της προστασίας ιδιωτικότητας. Αρχικά, εκτελεί τις λειτουργίες που προβλέπονται από την επιλογή που υπάρχει στην επικεφαλίδα «Privacy» του μηνύματος και στη συνέχεια την αφαιρεί. Αν αυτή δεν υπάρχει, εφαρμόζει προεπιλεγμένες πολιτικές ανά χρήστη ή πολιτικές της Α.Α.. Έπειτα ερευνά, αν γνωρίζει, κάποια τρέχουσα αντιστοίχιση του ονόματος Καλούμενου με κάποιο προσωρινό τυχαίο ψευδώνυμο και αλλάζει το μήνυμα-αίτηση ώστε, αντί για το όνομα καλούμενου χρήστη, να περιέχει τυχαίο ψευδώνυμο και προωθεί την αίτηση στον Ενδιάμεσο Διακομιστή. Αν δεν γνωρίζει κάποια τέτοια αντιστοίχιση, αλλά η διαχειριστική οντότητα του Καλούμενου(όπως αυτή καθορίζεται από το SIP URI AOR Καλούμενου) είναι η αυτή για την οποία είναι υπεύθυνος, εφαρμόζει κάποια προεπιλεγμένη πολιτική της Α.Α., αλλιώς προωθεί απλά το μήνυμα στον Ενδιάμεσο Διακομιστή. Ο

Ενδιάμεσος Διακομιστής εφαρμόζει την πολιτική δρομολόγησης της εταιρείας ανάλογα με τη διαχειριστική οντότητα του Καλούμενου. Στην απλή περίπτωση που Καλών και Καλούμενος ανήκουν στην ίδια διαχειριστική οντότητα αναζητά, αν υπάρχει, εγγραφή στο Διακομιστή Θέσης για το συγκεκριμένο αναγνωριστικό και ανάλογα με τη διεύθυνση IP προωθεί το μήνυμα αίτησης στον Καλούμενο. Με την εισαγωγή μιας επικεφαλίδας «Record-Route» ο Ενδιάμεσος Διακομιστής εξασφαλίζει την παρουσία του στο κανάλι σηματοδοσίας, που θα εγκαθιδρυθεί ώστε να εφαρμόσει την πολιτική χρέωσης της εταιρείας αφού διαπιστώσει τη διάρκεια της συνόδου.

Ο Καλούμενος λαμβάνει την αίτηση κλήσης και την αποδέχεται.

Το μήνυμα αποδοχής επιστρέφει μέσω του Ενδιάμεσου Διακομιστή στον Καλούντα.

Ο Καλών στέλνει μήνυμα αποδοχής σύνδεσης και εγκαθίδρυσης παραμέτρων επικοινωνίας στον Καλούμενο, όπως προβλέπει η αρχιτεκτονική του SIP

Εναλλακτικές Πορείες Σεναρίου:

Αν ο χρήστης δεν παρέχει κάποιο τρόπο ταυτοποίησης, τότε ο Δ.Π.Ι του επιστρέφει μήνυμα 407 Authentication Required.

Αν ο χρήστης έχει εντάξει στις επιλογές της επικεφαλίδας «Privacy» την προαιρετική επιλογή «critical» και δεν μπορεί να εφαρμοσθεί το επίπεδο προστασίας, που αιτείται, τότε το μήνυμα απορρίπτεται και επιστρέφεται μήνυμα λάθους στον Καλούντα.

Αν ο Διακομιστής Θέσης δεν περιέχει εγγραφή για την τρέχουσα διεύθυνση IP του Καλούμενου, τότε επιστρέφεται μήνυμα λάθους στον Καλούντα.

Αν ο Καλούμενος απορρίψει την κλήση, τότε επιστρέφεται μήνυμα «Κατειλημμένο» στον Καλούντα.

Επεκτείνει:

Όχι.

4.2.5 Εγκαθίδρυση Συνόδου (περίπτωση Καλών-Καλούμενος ανήκουν σε διαφορετικές διαχειριστικές οντότητες)

Περιγραφή:

Σε επέκταση του σεναρίου 1.2.4 ο Καλών και ο Καλούμενος ανήκουν σε διαφορετικές οντότητες, οπότε πραγματοποιείται δρομολόγηση μεταξύ των ενδιάμεσων διακομιστών, μέχρι το μήνυμα να καταλήξει στη διαχειριστική οντότητα του Καλούμενου.

Δράστες:

Καλών

Καλούμενος

Διακομιστής Προστασίας Ιδιωτικότητας Α

Διακομιστής Προστασίας Ιδιωτικότητας Β

Διακομιστής DNS Α

Διακομιστής Θέσης Β

Ενδιάμεσος Διακομιστής Α

Ενδιάμεσος Διακομιστής Β

Βάση Προσωπικών Δεδομένων Α

Βάση Προσωπικών Δεδομένων Β

Βάση Δεδομένων Α

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.
- Καλών και Καλούμενος ανήκουν σε διαφορετικές διαχειριστικές οντότητες.

Κείμενο Σεναρίου:

Οι ενέργειες και οι λειτουργίες που επιτελούνται σ’ αυτό το σενάριο είναι παρόμοιες με το σενάριο 1.2.4. μέχρι την άφιξη του μηνύματος στον Ενδιάμεσο Διακομιστή Α, όπου και εφαρμόζεται η πολιτική δρομολόγησης της εταιρείας. Σ’ αυτή την περίπτωση πραγματοποιείται ερώτημα DNS με στόχο την εξεύρεση του υπεύθυνου διακομιστή για τη διαχειριστική οντότητα προορισμού. Αυτός ο διακομιστής είναι ο Δ.Π.Ι. Β, ο οποίος μετά την παραλαβή του μηνύματος εφαρμόζει τις επιλογές προστασίας ιδιωτικότητας του παραλήπτη. Στη συνηθέστερη περίπτωση αυτό σημαίνει τερματισμό της συνόδου στο Δ.Π.Ι. Β και αναδημιουργία της για τη συνέχεια, όπως έχει περιγραφεί σε προηγούμενο κεφάλαιο. Στη συνέχεια, το μήνυμα προωθείται στον Ε.Δ. Β, όπου και πραγματοποιείται η αναζήτηση για την τρέχουσα θέση του Καλούμενου ώστε να προωθηθεί το μήνυμα προς αυτόν.

Η συνέχεια του σεναρίου περιλαμβάνει ενέργειες και λειτουργίες παρόμοιες μ' αυτές του σεναρίου 1.2.4, εκτός από την επιβεβλημένη παρουσία του Δ.Π.Ι. Β στο κανάλι σηματοδοσίας.

Εναλλακτικές Πορείες Σεναρίου:

Αν ο Καλούμενος έχει κατάλληλες επιλογές ιδιωτικότητας, το μήνυμα μπορεί να απορριφθεί από το Δ.Π.Ι. Β με επιστροφή μηνύματος λάθους.

Αν οι επιλογές προστασίας του καλούμενου έχουν εφαρμοσθεί ήδη από συμβαλλόμενη Ανεξάρτητη Αρχή, πριν την άφιξη του μηνύματος στο Δ.Π.Ι. Β, το μήνυμα προωθείται όπως λαμβάνεται.

Επεκτείνει:

1.2.4. Εγκαθίδρυση Συνόδου (Ίδια Διαχειριστική Οντότητα)

4.2.6 Αποστολή Σύντομου Μηνύματος

Περιγραφή:

Ο Αποστολέας επιθυμεί να αποστείλει ένα σύντομο μήνυμα στον Παραλήπτη.

Δράστες:

Αποστολέας

Παραλήπτης

Διακομιστής Προστασίας Ιδιωτικότητας

Διακομιστής Θέσης

Ενδιάμεσος Διακομιστής

Διακομιστής Μηνυμάτων

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Ο Αποστολέας αιτείται την αποστολή σύντομου μηνύματος στον Παραλήπτη, εκτελώντας από την πλευρά του τις ίδιες λειτουργίες μ' αυτές που θα εκτελούσε στην περίπτωση αίτησης εγκαθίδρυσης Συνόδου. Ο Διακομιστής Προστασίας Ιδιωτικότητας εκτελεί τις ίδιες λειτουργίες με την περίπτωση εγκαθίδρυσης συνόδου και το μήνυμα στη συνέχεια προωθείται στον Ενδιάμεσο Διακομιστή. Εκεί εφαρμόζεται η πολιτική δρομολόγησης της εταιρείας ανάλογα με τη διαχειριστική οντότητα του Καλούμενου. Όταν φθάσει στον Ενδιάμεσο Διακομιστή της διαχειριστικής οντότητας του Παραλήπτη αναζητείται μια τρέχουσα εγγραφή του χρήστη. Αν αυτή βρεθεί, τότε το μήνυμα προωθείται στον παραλήπτη. Αν δεν βρεθεί τρέχουσα εγγραφή ή το μήνυμα δεν μπορέσει να παραδοθεί επιτυχώς στον Παραλήπτη, τότε αυτό προωθείται στο Διακομιστή Μηνυμάτων και επιστρέφεται μήνυμα 202 Accepted στον Αποστολέα. Τα αποθηκευμένα μηνύματα θα παραδοθούν στον Παραλήπτη, όταν αυτός εισέλθει στο σύστημα, όπως θα παρουσιασθεί στο επόμενο σενάριο λειτουργίας.

Εναλλακτικές Πορείες Σεναρίου:

Όχι

Επεκτείνει:

1.2.4. Εγκαθίδρυση Συνόδου (Ίδια Διαχειριστική Οντότητα)

1.2.5. Εγκαθίδρυση Συνόδου (Διαφορετικές Διαχειριστικές Οντότητες)

4.2.7 Παραλαβή Σύντομων Μηνυμάτων

Περιγραφή:

Αν ο χρήστης επανέλθει στο σύστημα μετά από μια περίοδο απουσίας του, ο Διακομιστής Καταχώρισης Χρηστών ειδοποιεί το Διακομιστή Μηνυμάτων, ώστε να παραδοθούν στο χρήστη τα σύντομα μηνύματα που απευθύνθηκαν σ' αυτόν κατά τη διάρκεια της απουσίας του.

Δράστες:

Πελάτης

Διακομιστής Καταχώρισης Χρηστών

Διακομιστής Μηνυμάτων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.
- Ο χρήστης επανεισέρχεται στο σύστημα μετά από μια περίοδο απουσίας.

Κείμενο Σεναρίου:

Ο Πελάτης εφαρμόζει τις διαδικασίες εισόδου στο σύστημα, όπως αυτές αναφέρονται στο σενάριο 1.2.2 και κάνει χρήση είτε ενός τρέχοντος έγκυρου ψευδωνύμου, αν δεν έχει παρέλθει το διάστημα παραχώρησης του, είτε του τελευταίου έγκυρου ψευδωνύμου, που του παραχωρήθηκε πριν από την έξοδο του από το σύστημα. Ο Διακομιστής Καταχώρισης Χρηστών εκτός από την ενεργοποίηση του χρήστη στο Διακομιστή Θέσης, ειδοποιεί το Διακομιστή Μηνυμάτων για την είσοδο του χρήστη, ο οποίος αποστέλλει όλα τα μηνύματα που προορίζονται για το χρήστη στο σύστημα, δρώντας ως Αποστολέας του σεναρίου 1.2.6

Εναλλακτικές Πορείες Σεναρίου:

Όχι

Επεκτείνει:

1.2.2. Είσοδος

1.2.6 Αποστολή Σύντομου Μηνύματος

4.2.8 Υπηρεσίες Παρουσίας

Περιγραφή:

Ο Ενδιαφερόμενος αιτείται την προώθηση μηνυμάτων πληροφοριών παρουσίας του Προτιμώμενου σ' αυτόν.

Δράστες:

Ενδιαφερόμενος

Προτιμώμενος

Διακομιστής Προστασίας Ιδιωτικότητας

Διακομιστής Παρουσίας

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.
- Ο Ενδιαφερόμενος ανήκει στην ομάδα φίλων του Προτιμώμενου

Κείμενο Σεναρίου:

Το αίτημα του Ενδιαφερόμενου αντιμετωπίζεται αρχικά σαν όλα τα μηνύματα-αιτήσεις SIP με εφαρμογή ελέγχου πιστοποίησης και λειτουργιών προστασίας ιδιωτικότητας του Ενδιαφερόμενου. Εφόσον ο χρήστης είναι πιστοποιημένος (εφαρμόζοντας πιο αυστηρά κριτήρια αυτή τη φόρα, αφού θα πρέπει να ανήκει σ' ένα πολύ κλειστό σύνολο έμπιστων χρηστών (buddies)) και μετά τη μετατροπή του αιτήματος, ώστε να χρησιμοποιείται το τρέχον ψευδώνυμο του Προτιμώμενου, το αίτημα προωθείται στο Διακομιστή Παρουσίας, όπου γίνεται η κατάλληλη εγγραφή, σύμφωνα με την αρχιτεκτονική του SIP. Όταν ο Προτιμώμενος στείλει πληροφορίες παρουσίας του στο Διακομιστή Παρουσίας με χρήση του κατάλληλου ψευδωνύμου, ο διακομιστής προωθεί τις κρυπτογραφημένες πληροφορίες παρουσίας με κατάλληλα μηνύματα στους κατάλληλους Ενδιαφερόμενους.

Εναλλακτικές Πορείες Σεναρίου:

Όχι

Επεκτείνει:

1.2.4. Εγκαθίδρυση Συνόδου (Ίδια Διαχειριστική Οντότητα)

1.2.5. Εγκαθίδρυση Συνόδου (Διαφορετικές Διαχειριστικές Οντότητες)

4.2.9 Ανεξάρτητη αρχή ελέγχει τα στοιχεία του χρήστη (lawful interception)

Περιγραφή:

Όπως επιβάλλει η ευρωπαϊκή νομοθεσία μια πιστοποιημένη Ανεξάρτητη Αρχή θα πρέπει να έχει πρόσβαση στα προσωπικά δεδομένα του χρήστη και στην πλήρη λίστα κλήσεών του στις περιπτώσεις που αίρεται το απόρρητο των τηλεπικοινωνιών. Η εταιρεία παροχής υπηρεσιών VoIP θα πρέπει να παρέχει αυτήν τη δυνατότητα στους κατάλληλους φορείς.

Δράστες:

Ανεξάρτητος Φορέας

Διακομιστής Διαδικτύου Προσωπικών Δεδομένων

Διακομιστής Προστασίας Ιδιωτικότητας

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Ο Ανεξάρτητος Φορέας πιστοποιεί την ταυτότητά του στο Διακομιστή Διαδικτύου Προσωπικών Δεδομένων, ο οποίος επιστρέφει μια ηλεκτρονική φόρμα, στην οποία ο κρατικός φορέας μπορεί να κάνει ερωτήματα πάνω στο αρχείο κλήσεων καθώς και μέσα στα προσωπικά προφίλ των χρηστών. Αν πρόκειται για ερώτημα πάνω στην λίστα κλήσεων, ο Δ.Δ.Π.Δ. ελέγχει, αν η πιστοποίηση που παρέχεται, δίνει δικαιώματα για την εκτέλεση του συγκεκριμένου ερωτήματος και στη συνέχεια το εκτελεί. Αν πρόκειται για ερώτημα σε πληροφορίες προφίλ, αυτό προωθείται στο Διακομιστή Προστασίας Ιδιωτικότητας, ο οποίος ελέγχει το ερώτημα σε σχέση με το επίπεδο πρόσβασης του Φορέα, έτσι ώστε στα αποτελέσματα να εμφανίζονται μόνο τα δεδομένα που ο συγκεκριμένος φορέας επιτρέπεται να δει. Τέλος, ο Δ.Π.Ι. εκτελεί το ερώτημα και επιστρέφει τα αποτελέσματα.

Εναλλακτικές Πορείες Σεναρίου:

Όχι

Επεκτείνει:

Όχι.

4.2.10 Τρίτη εταιρεία βλέπει στοιχεία χρηστών

Περιγραφή:

Μια Τρίτη Εταιρεία, η οποία έχει κάνει σύμβαση με την Εταιρεία Παροχής Υπηρεσιών VoIP μπορεί να έχει ελεγχόμενη πρόσβαση σε συγκεντρωτικά και/ή ανώνυμα δεδομένα των προφίλ των χρηστών.

Δράστες:

Τρίτη Εταιρεία Πελάτης

Διακομιστής Διαδικτύου

Διακομιστής Προστασίας Ιδιωτικότητας

Βάση Προσωπικών Δεδομένων

Βάση Δεδομένων

Προαπαιτούμενα:

- Κανονική λειτουργία των εμπλεκομένων δραστών.

Κείμενο Σεναρίου:

Η Τρίτη Εταιρεία Πελάτης πιστοποιεί την ταυτότητά της στη σελίδα της εταιρείας VoIP ώστε να της δοθεί ελεγχόμενη πρόσβαση. Ο Διακομιστής Διαδικτύου επιστρέφει μια ηλεκτρονική φόρμα, στην οποία η Τρίτη Εταιρεία Πελάτης μπορεί να κάνει ερωτήματα μέσα στα προσωπικά προφίλ των χρηστών. Αυτά τα ερωτήματα μπορεί να είναι προεπιλεγμένα, αλλά αυτό δεν είναι απαραίτητο, αφού το σύστημα της Α.Α. που θα κάνει την πιστοποίηση του ερωτήματος μπορεί να επεξεργασθεί οποιοδήποτε ερώτημα. Στη συνέχεια, η εταιρεία VoIP ελέγχει αν τα ερωτήματα που κάνει η Τρίτη Εταιρεία είναι επιτρεπτά με βάση τη σύμβαση μεταξύ τους και αν είναι, τα προωθεί στο Διακομιστή Προστασίας Ιδιωτικότητας, ο οποίος ελέγχει αν το ερώτημα είναι επιτρεπτό με βάση τη νομοθεσία και τις προσωπικές επιλογές των χρηστών, το πλαίσιο των οποίων καθορίζεται από τη νομοθεσία και αν είναι το εκτελεί και επιστρέφει τα αποτελέσματα από τη Βάση Προσωπικών Δεδομένων.

Με την παραπάνω ακολουθία μηνυμάτων είναι δυνατή η επεξεργασία αποκλειστικά των δεδομένων που επιτρέπονται από τη νομοθεσία, τους χρήστες και το επίπεδο πρόσβασης της τρίτης εταιρείας.

Εναλλακτικές Πορείες Σεναρίου:

Στην περίπτωση που η Τρίτη Εταιρεία δεν έχει το απαιτούμενο επίπεδο πρόσβασης για να εκτελέσει το ερώτημα, που επιθυμεί, ανακατευθύνεται σε μια σελίδα στην οποία της προτείνονται εναλλακτικά προγράμματα-συμβάσεις με την εταιρεία VoIP, τα οποία της παρέχουν ευρύτερη πρόσβαση.

Σε περίπτωση που το αρχικό ερώτημα δεν πληροί τις προϋποθέσεις προστασίας της ιδιωτικότητας των πελατών του συστήματος, ο Δ.Π.Ι. το μετασχηματίζει σε μια επιτρεπτή

μορφή, η οποία να είναι όσο το δυνατόν πιο κοντά στην εννοιολογική σημασία του αρχικού, το εκτελεί και επιστρέφει τα αποτελέσματα.

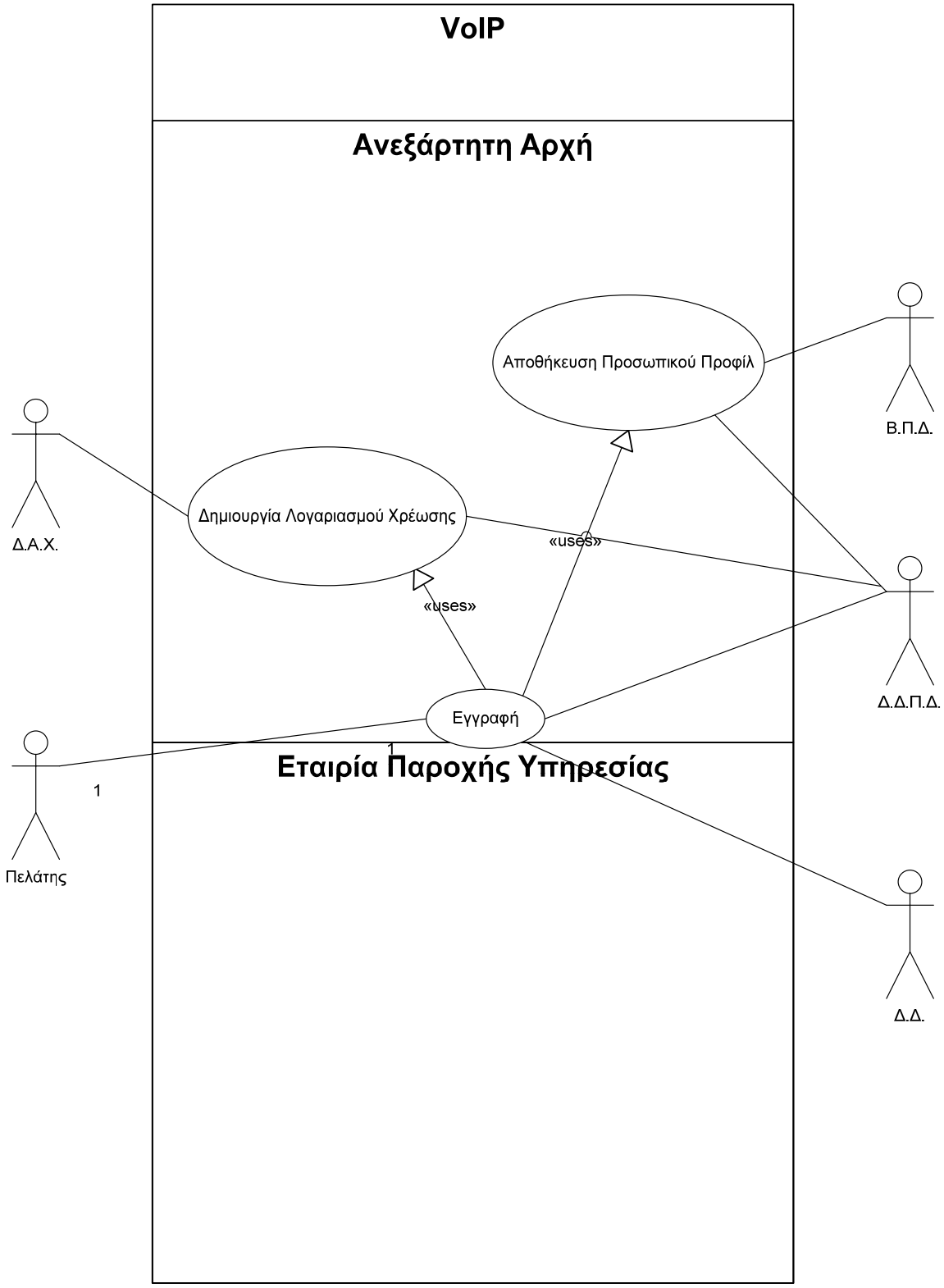
Σε περίπτωση που το αρχικό ερώτημα, αλλά και όλοι οι πιθανοί μετασχηματισμοί του, δεν πληρούν τις επιθυμητές προϋποθέσεις επιστρέφεται μήνυμα λάθους.

Επεκτείνει:

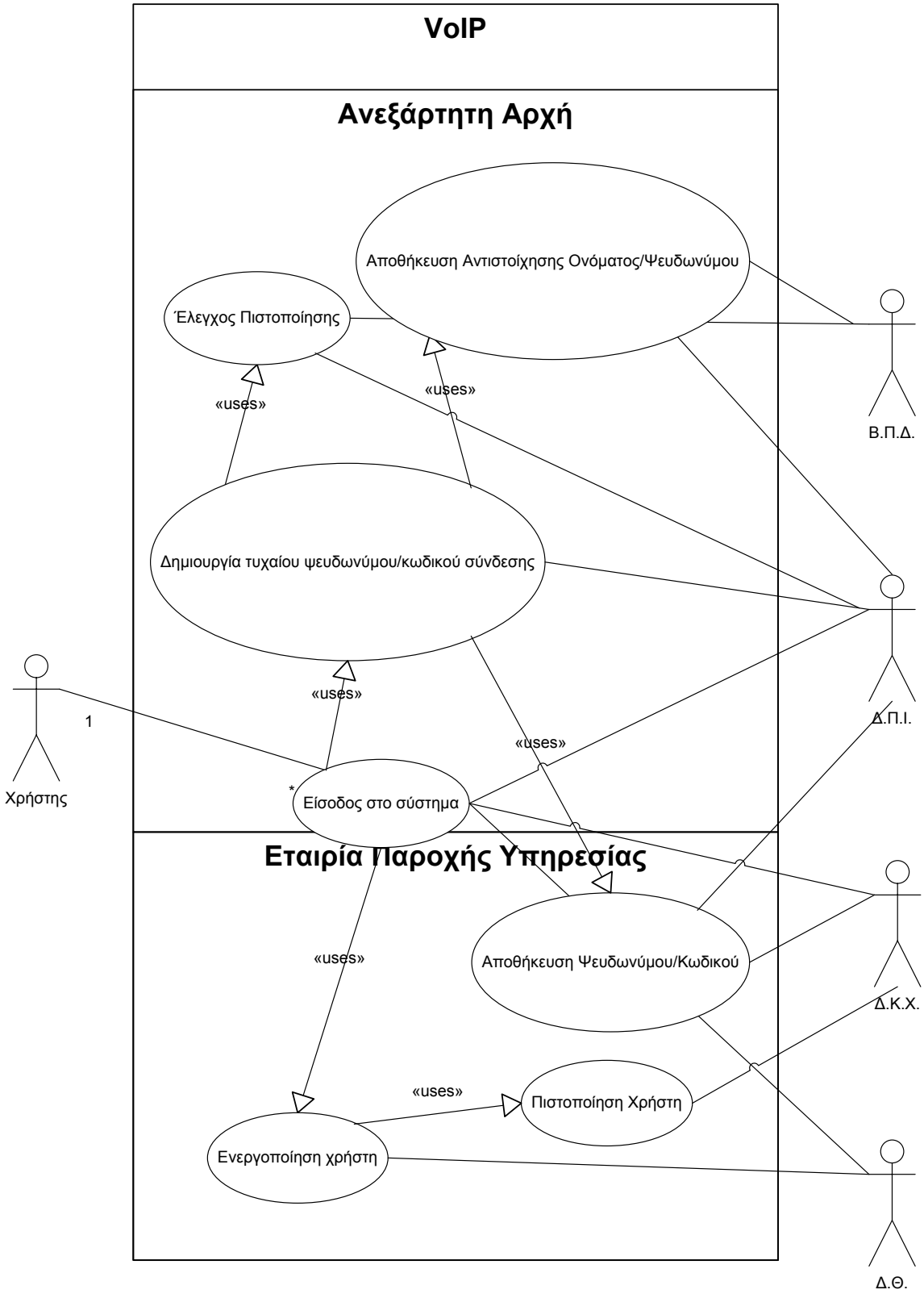
Όχι.

4.3 Διαγράμματα Χρήσης

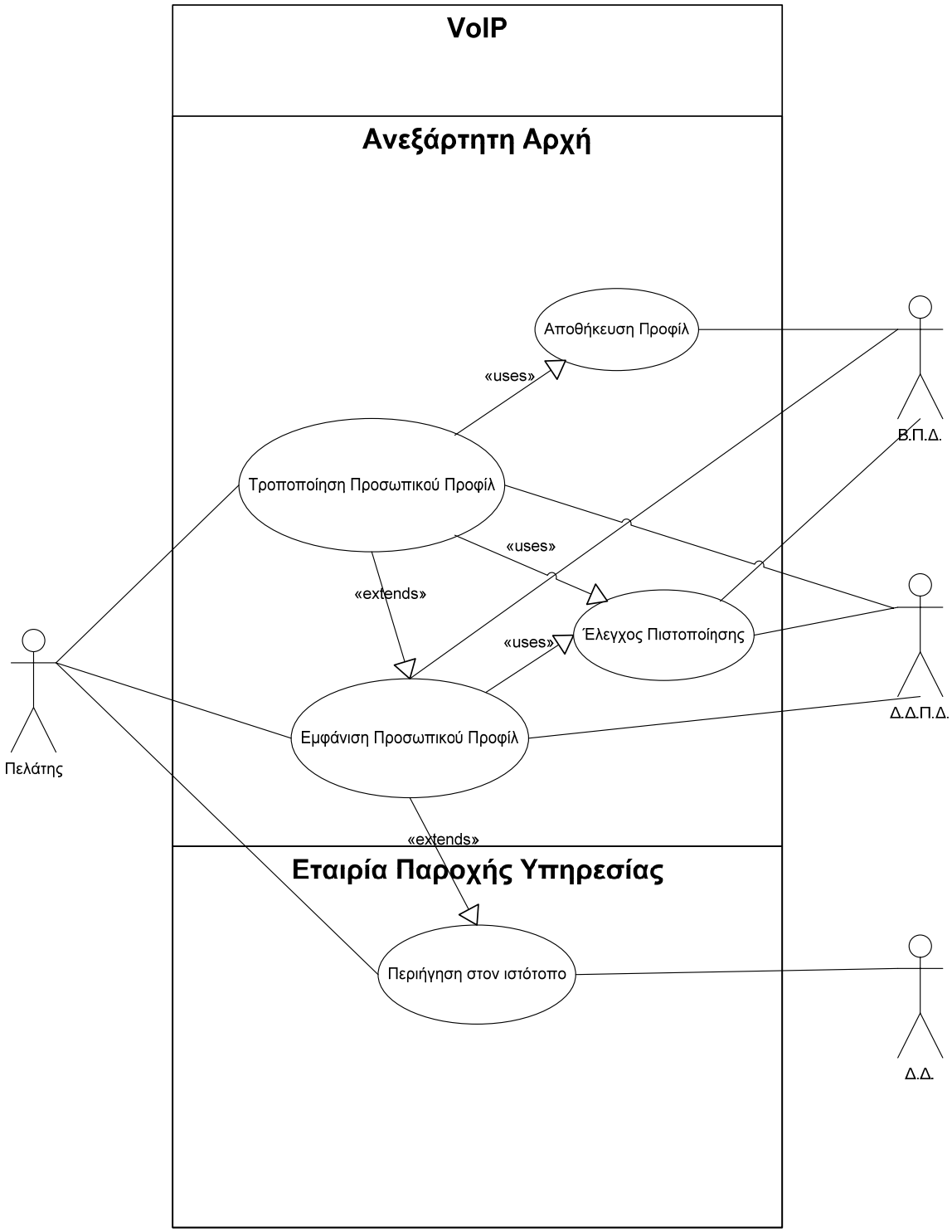
4.3.1 Εγγραφή στο σύστημα



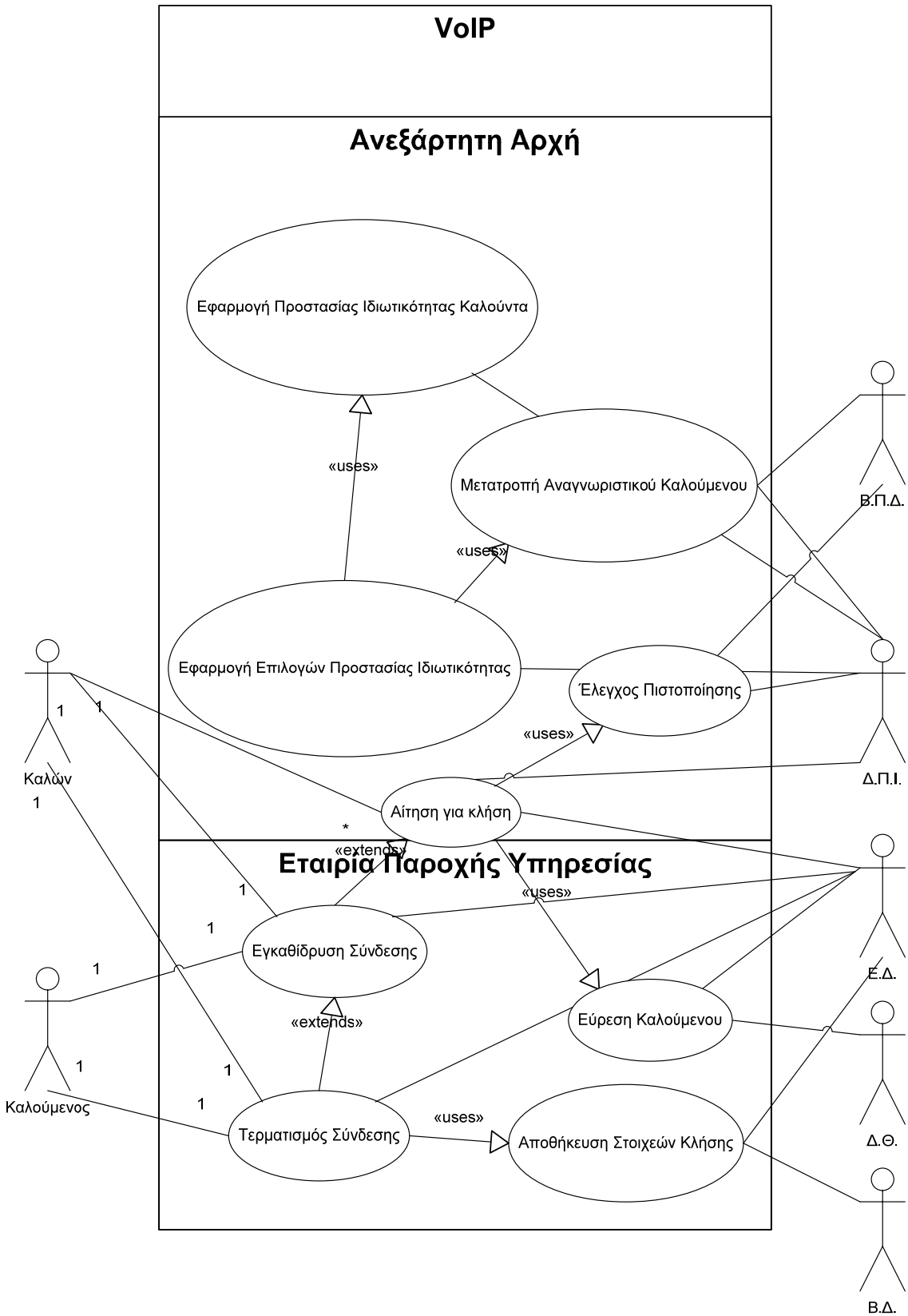
4.3.2 Είσοδος στο σύστημα



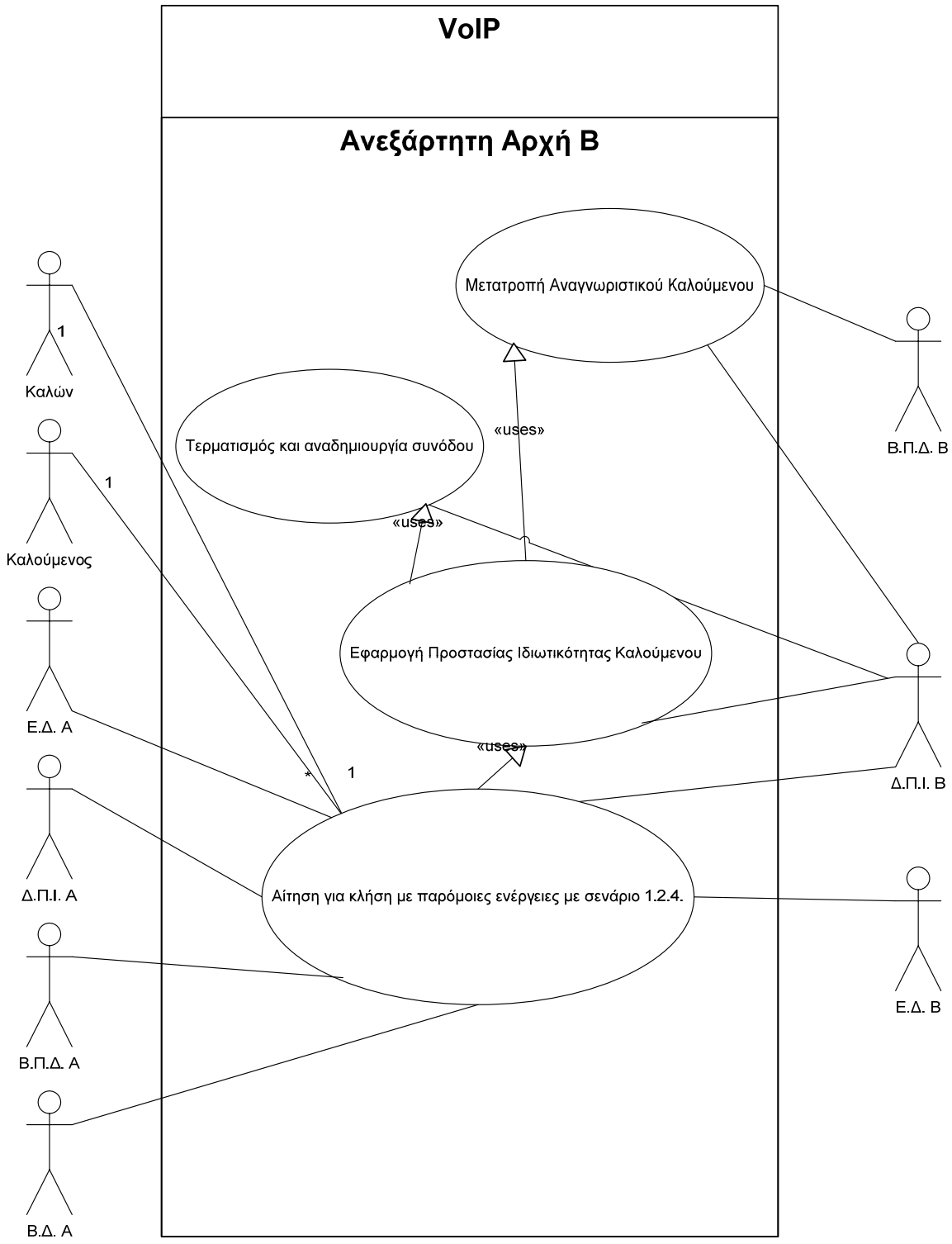
4.3.3 Ανανέωση Προφίλ



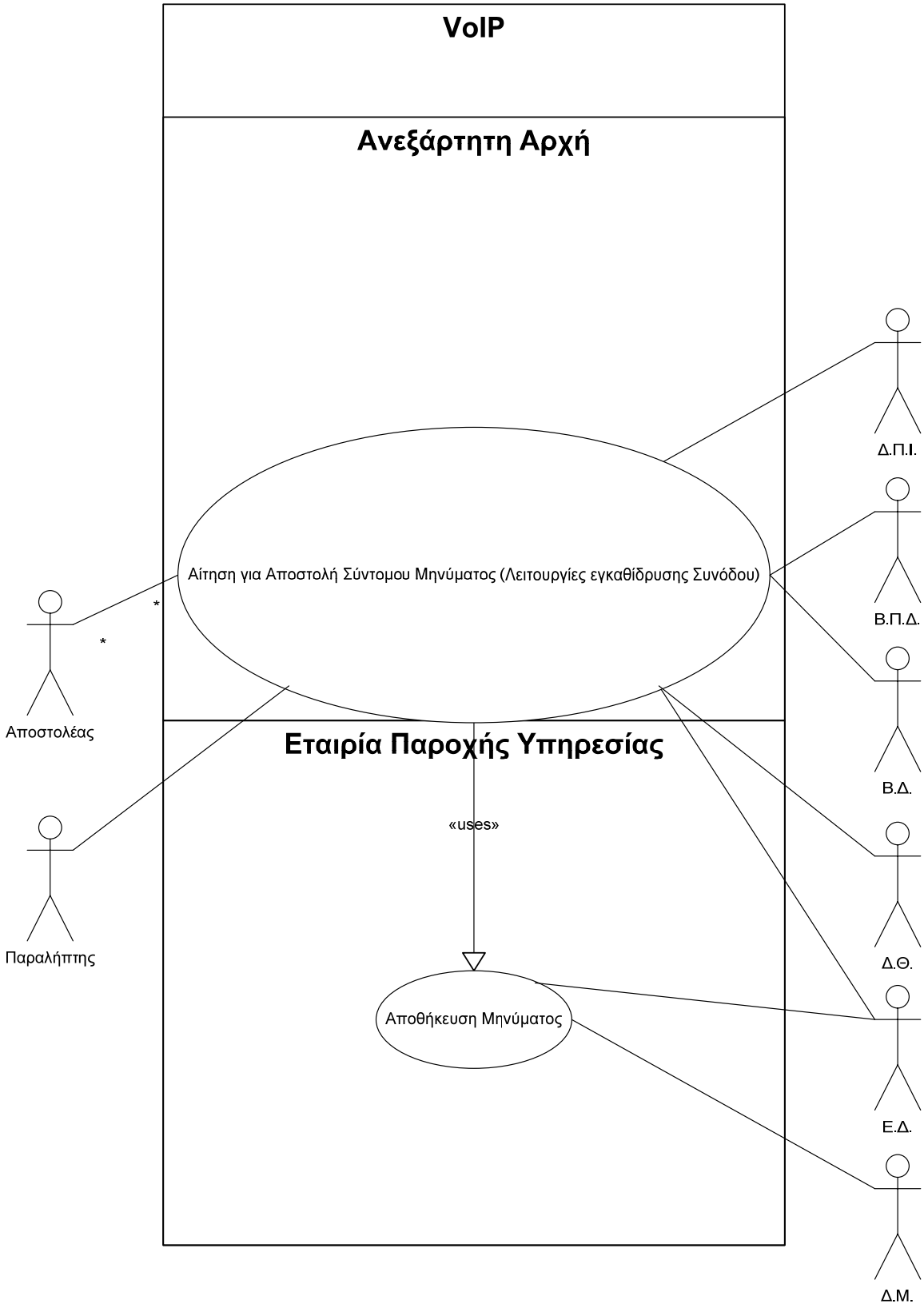
4.3.4 Εγκαθίδρυση Συνόδου (απλή περίπτωση Καλών-Καλούμενος ανήκουν στην ίδια διαχειριστική οντότητα)



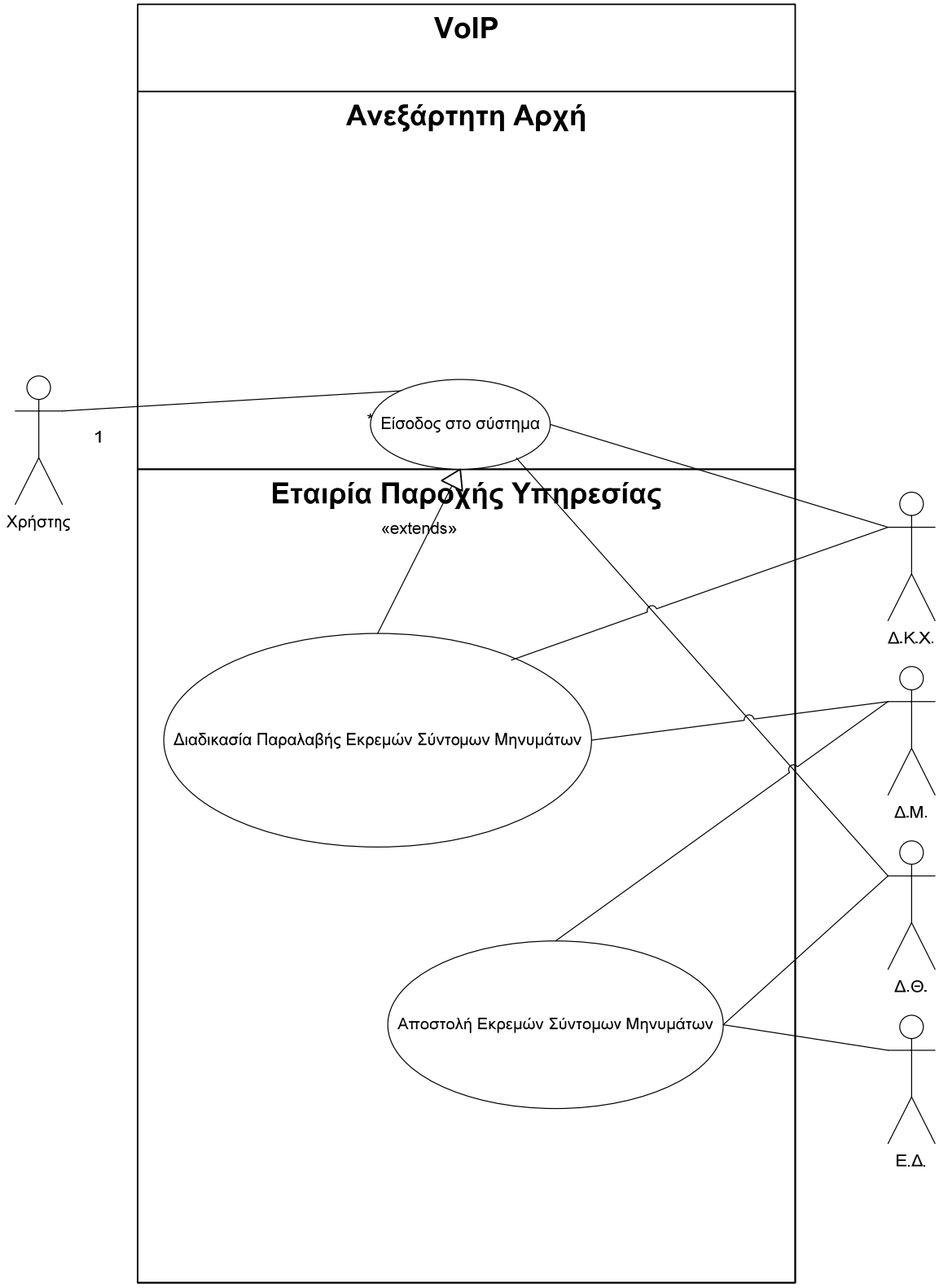
4.3.5 Εγκαθίδρυση Συνόδου (περίπτωση Καλών-Καλούμενος ανήκουν σε διαφορετικές διαχειριστικές οντότητες)



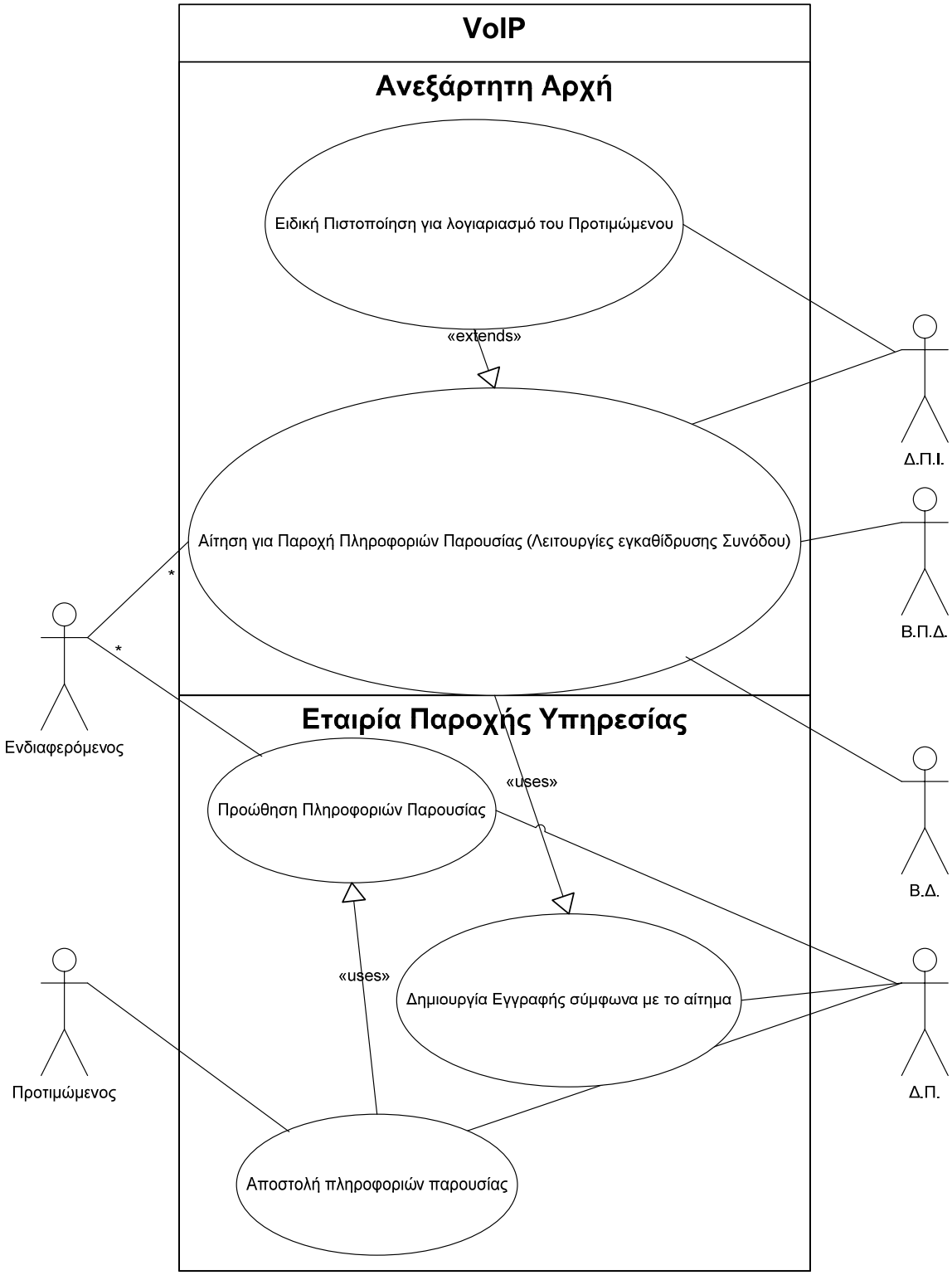
4.3.6 Αποστολή Σύντομου Μηνύματος



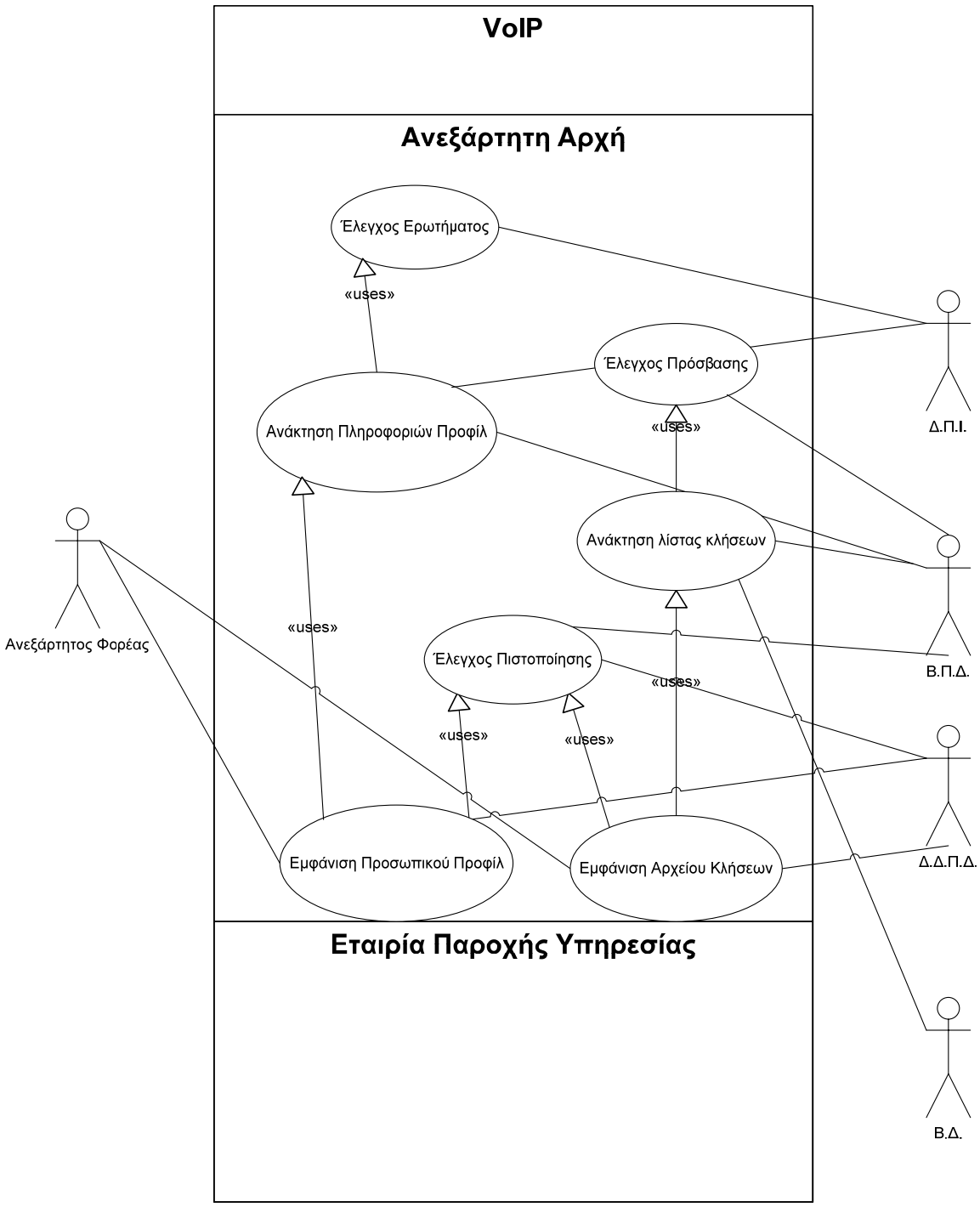
4.3.7 Παραλαβή Σύντομων Μηνυμάτων



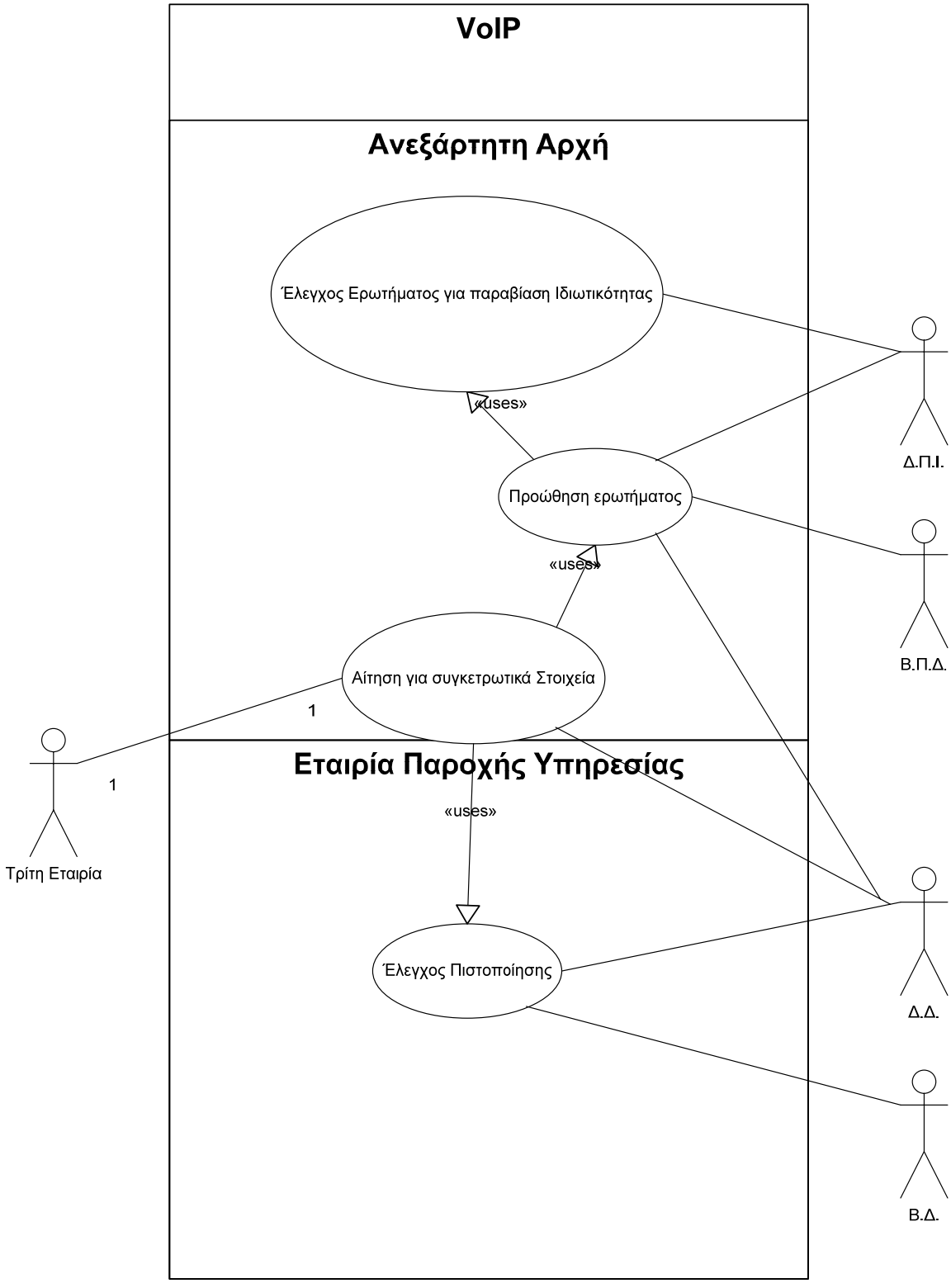
4.3.8 Υπηρεσίες Παρουσίας



4.3.9 Ανεξάρτητη αρχή ελέγχει τα στοιχεία του χρήστη (lawful interception)

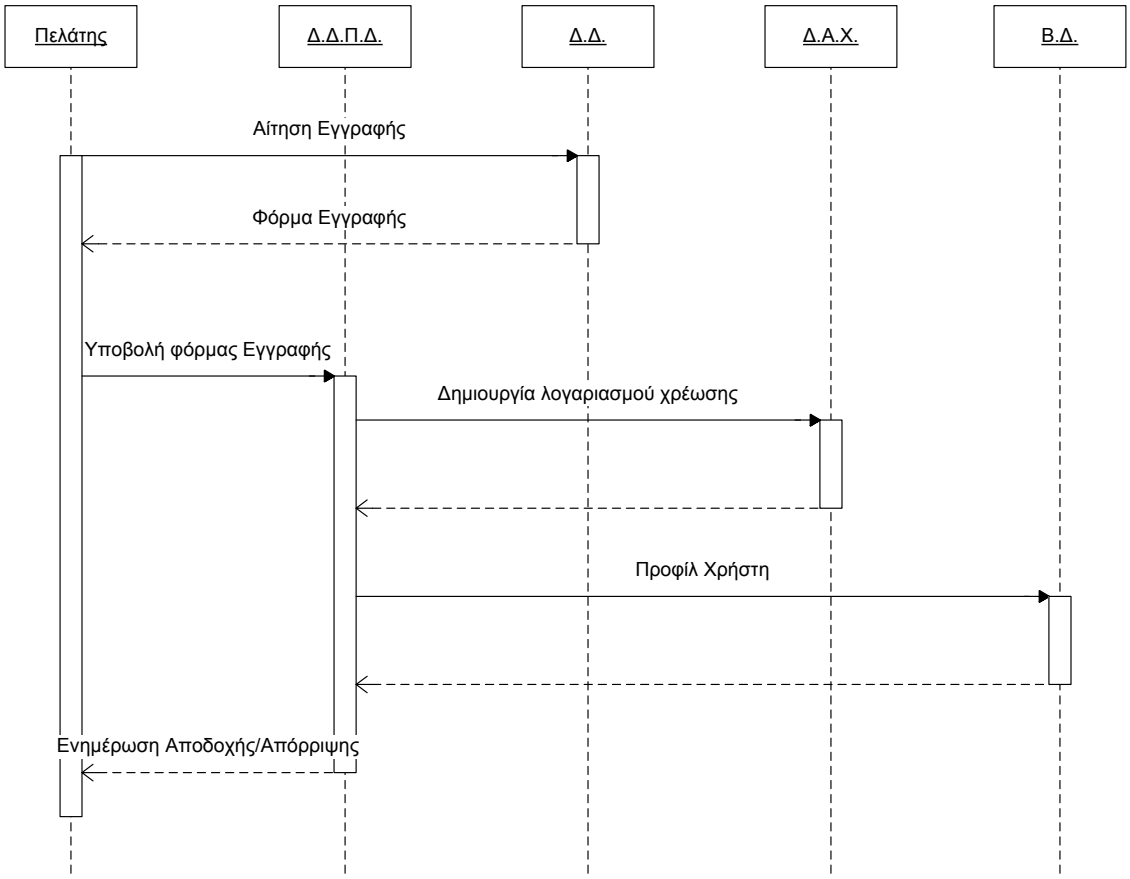


4.3.10 Τρίτη εταιρεία βλέπει στοιχεία χρηστών

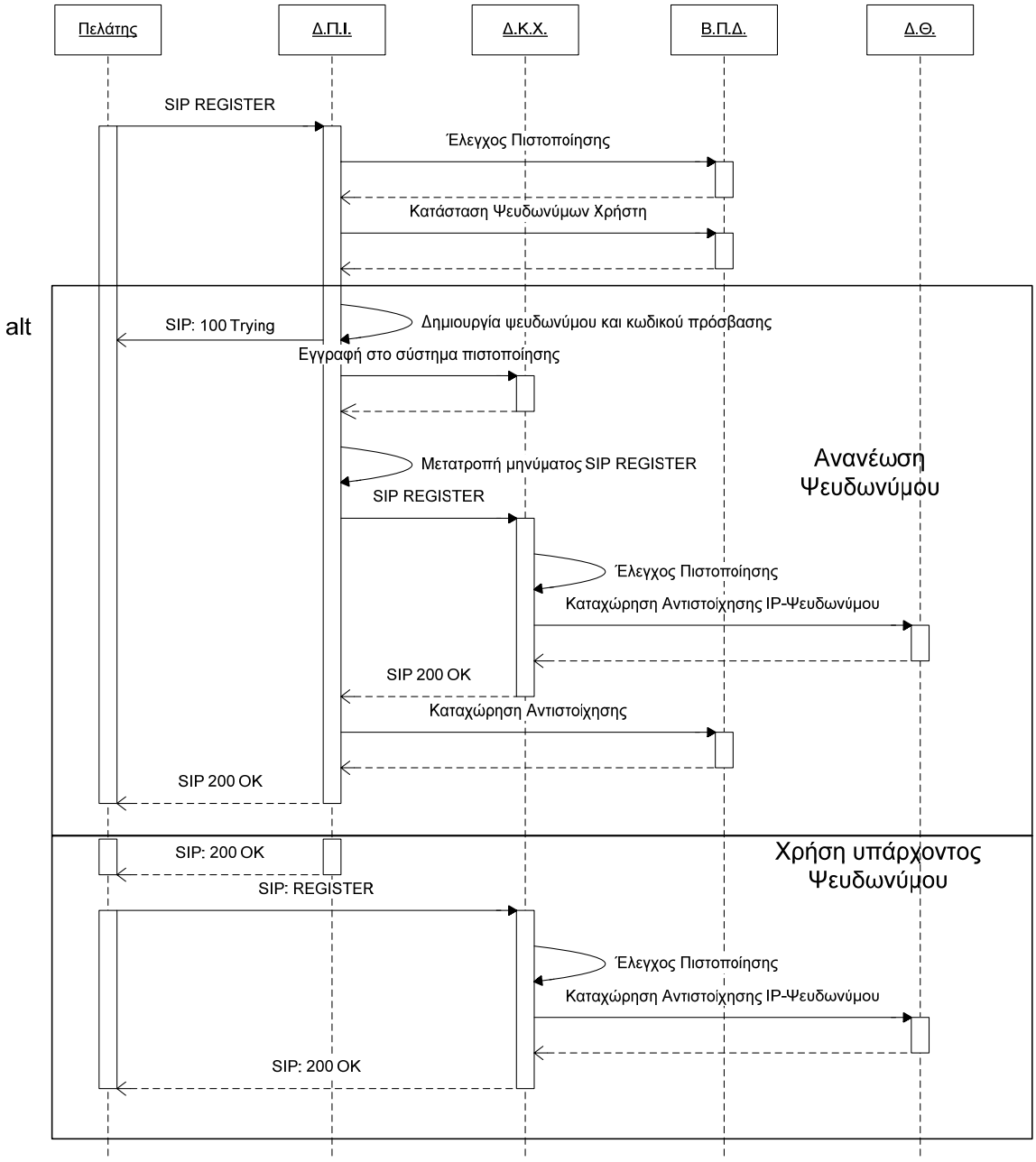


4.4 Ακολουθιακά Διαγράμματα

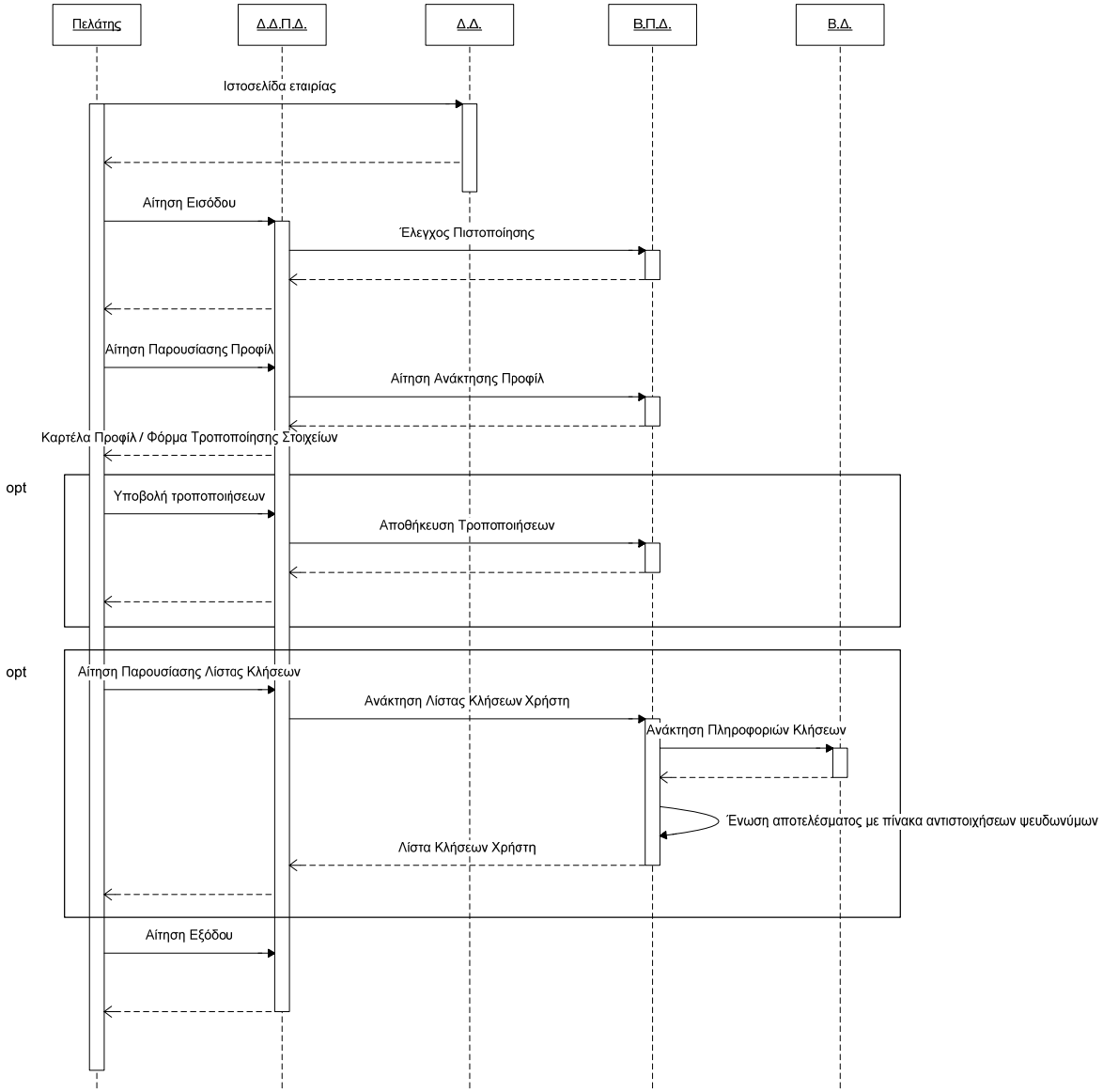
4.4.1 Εγγραφή στο σύστημα



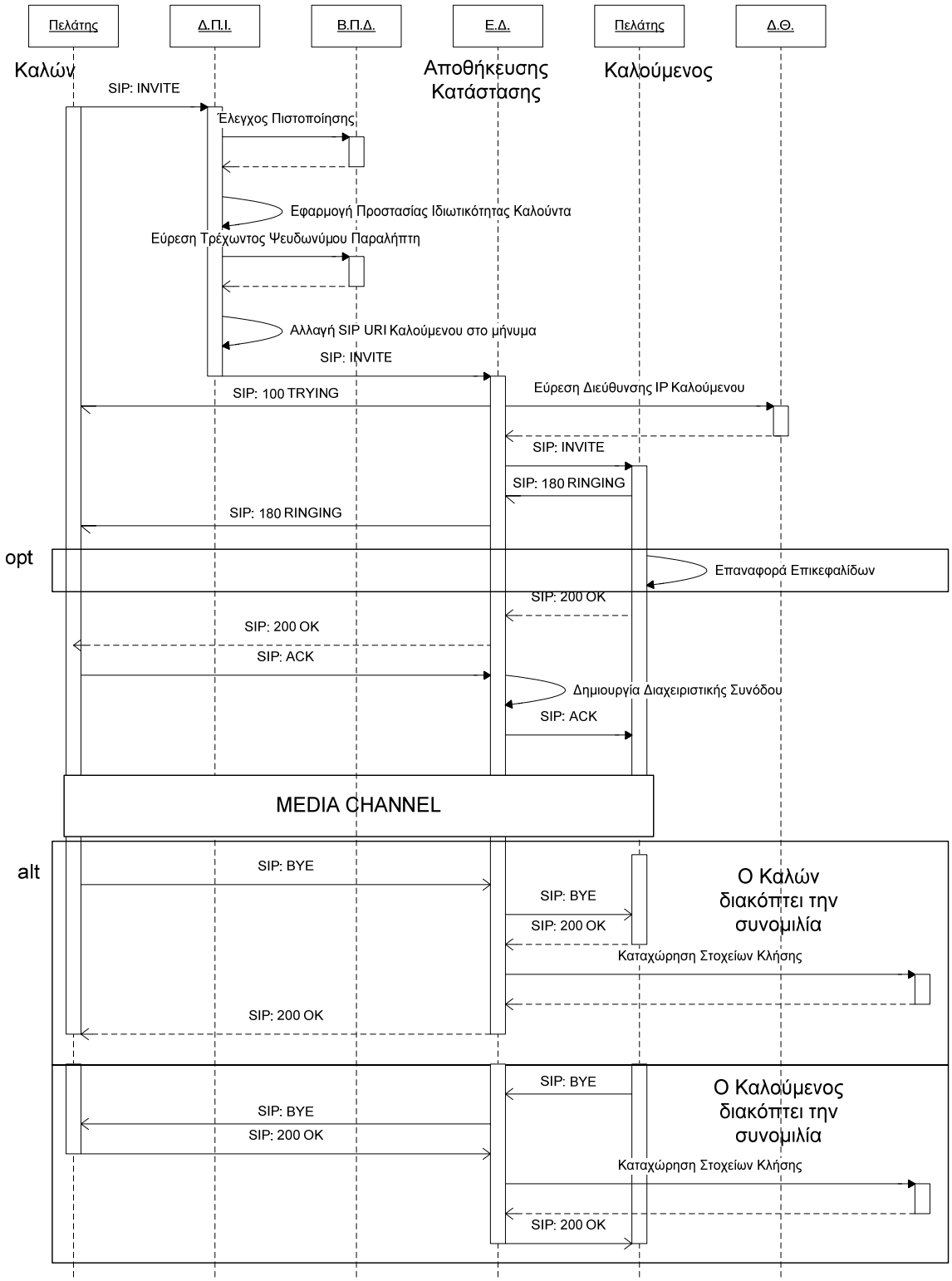
4.4.2 Είσοδος στο σύστημα



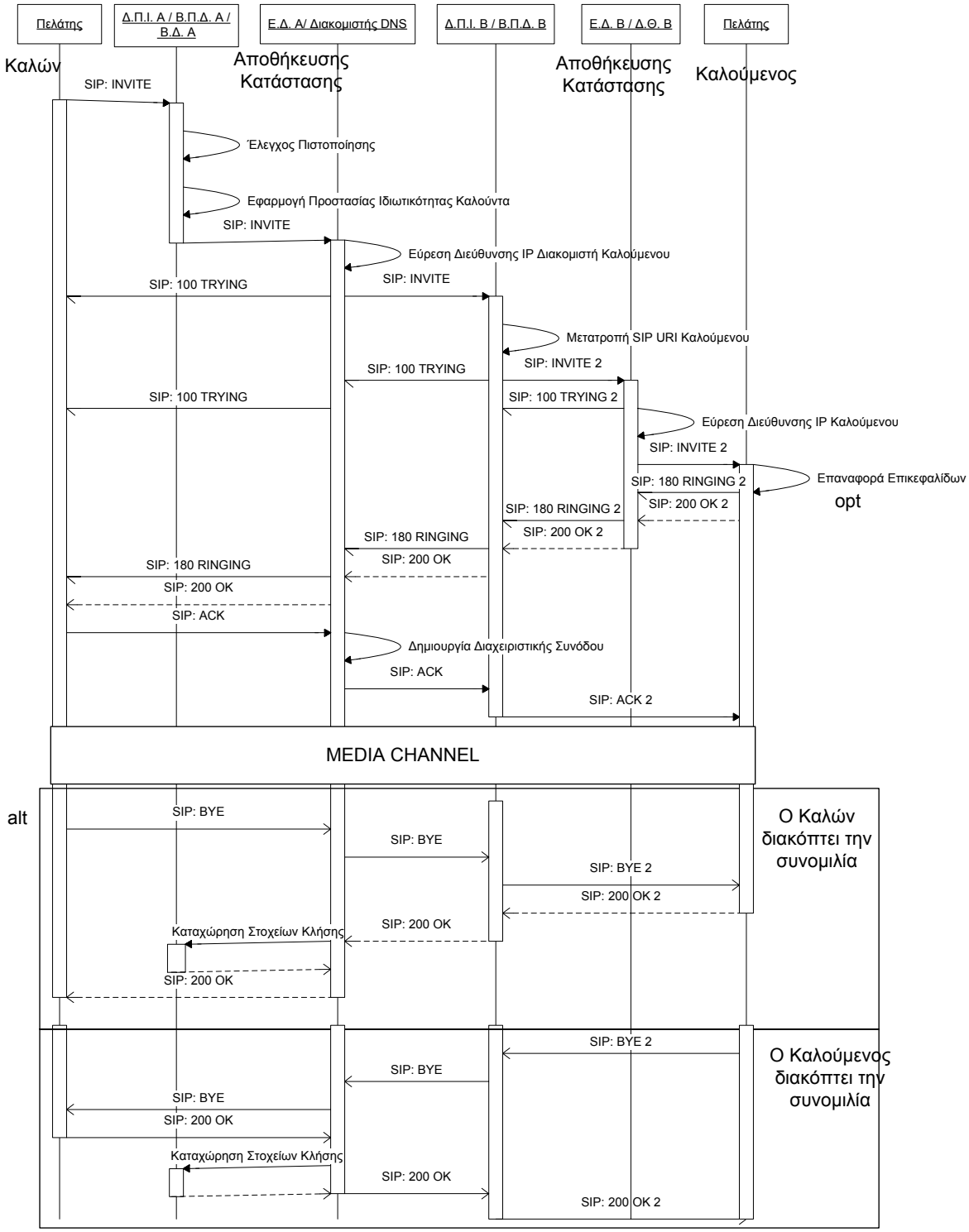
4.4.3 Ανανέωση Προφίλ



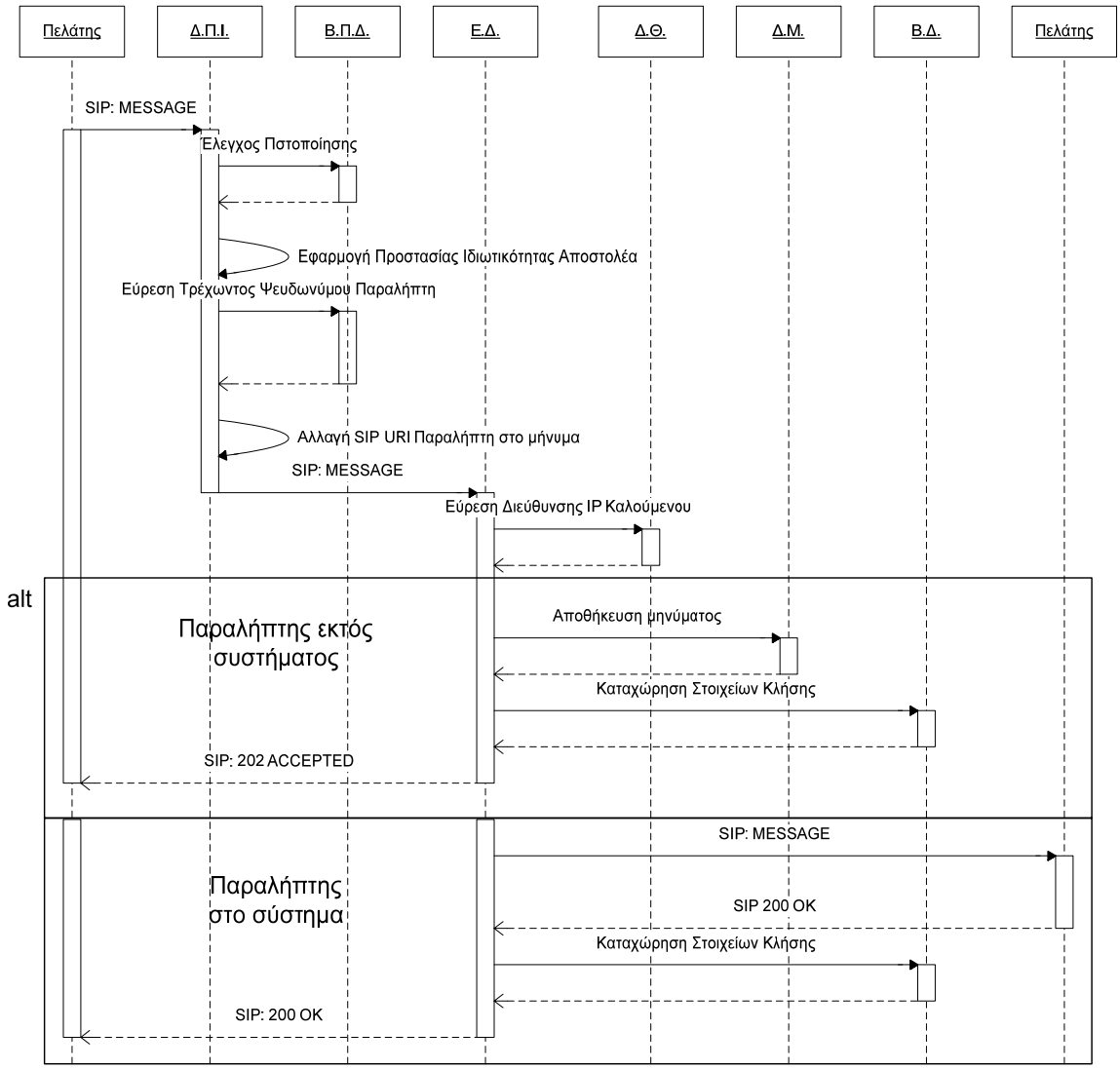
4.4.4 Εγκαθίδρυση Συνόδου (απλή περίπτωση Καλών-Καλούμενος ανήκουν στην ίδια διαχειριστική οντότητα)



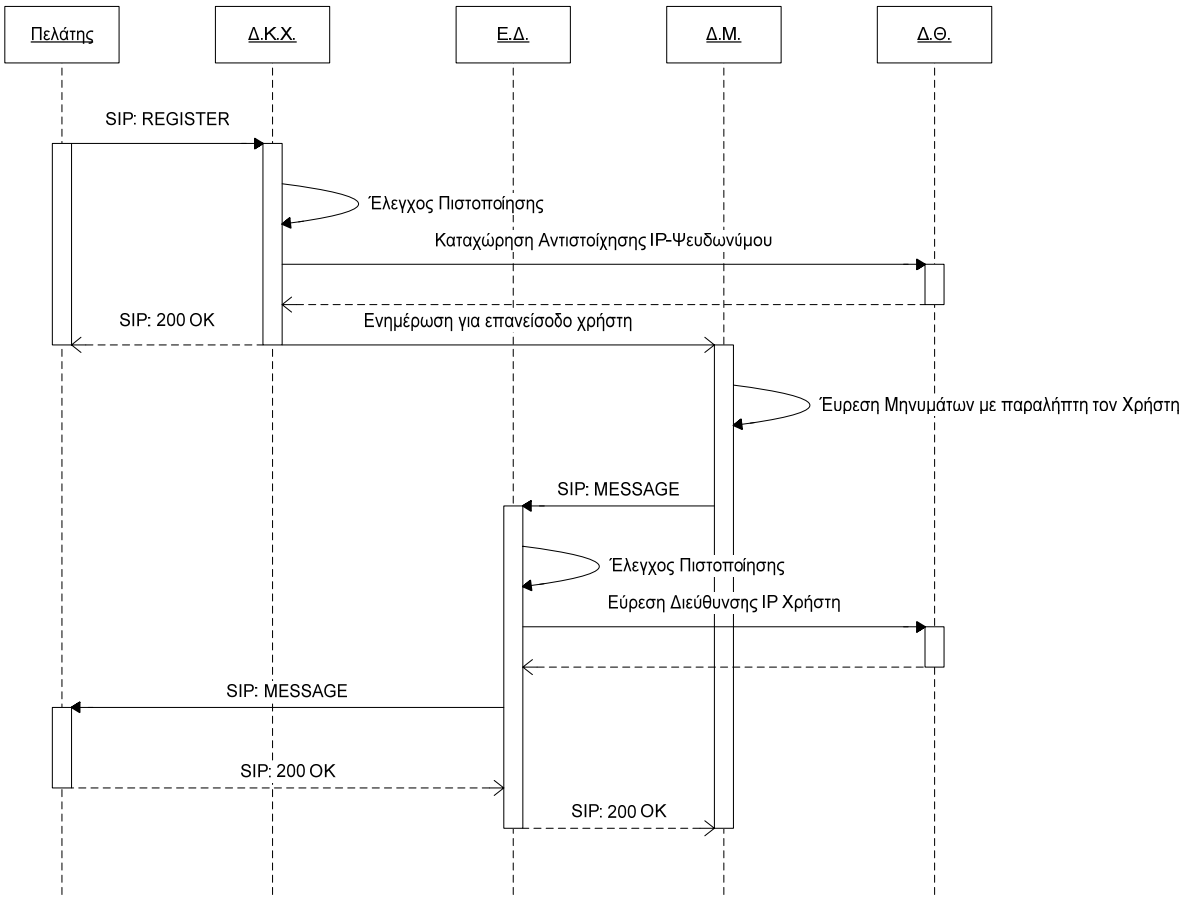
4.4.5 Εγκαθίδρυση Συνόδου (περίπτωση Καλών-Καλούμενος ανήκουν σε διαφορετικές διαχειριστικές οντότητες)



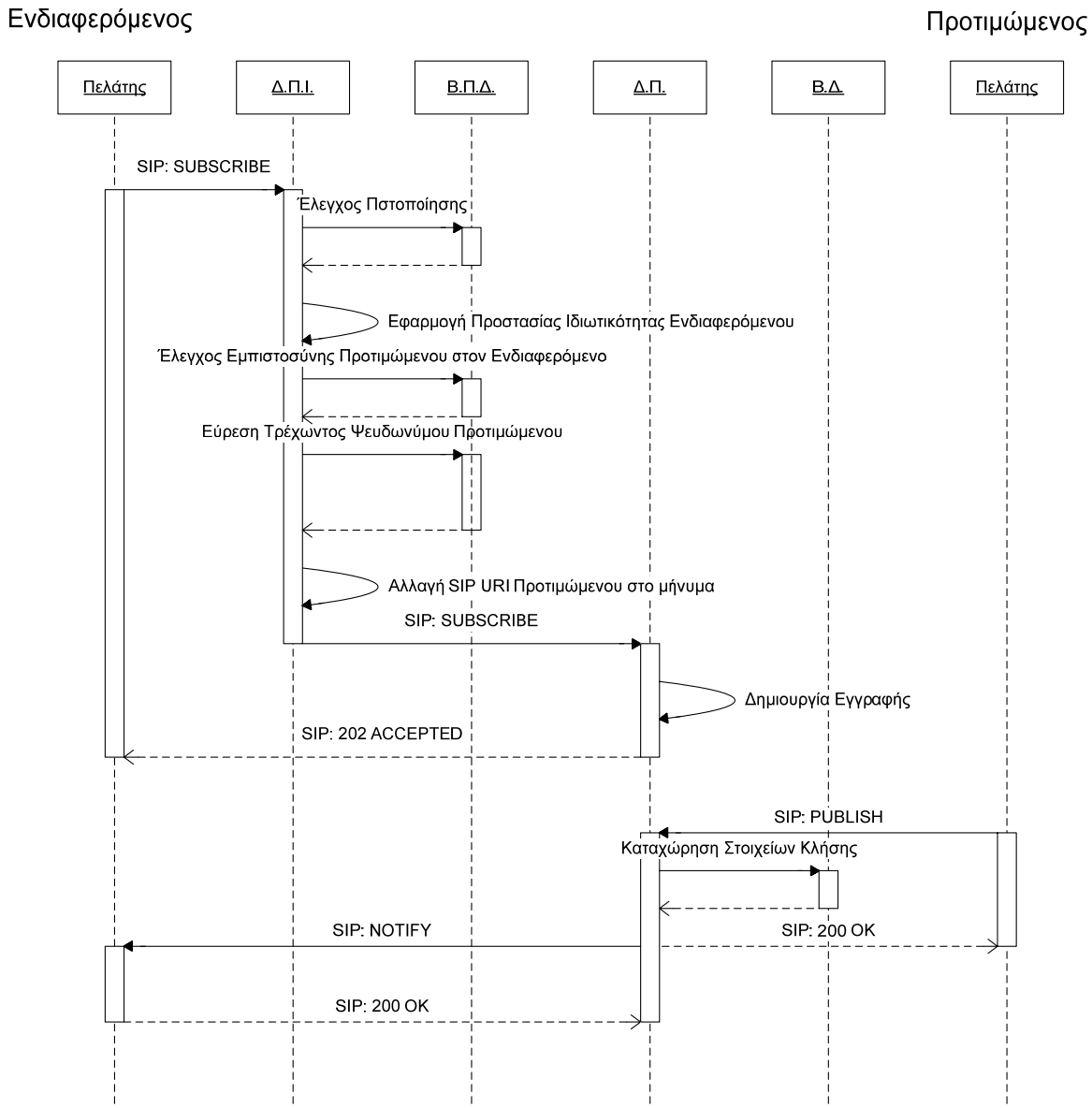
4.4.6 Αποστολή Σύντομου Μηνύματος



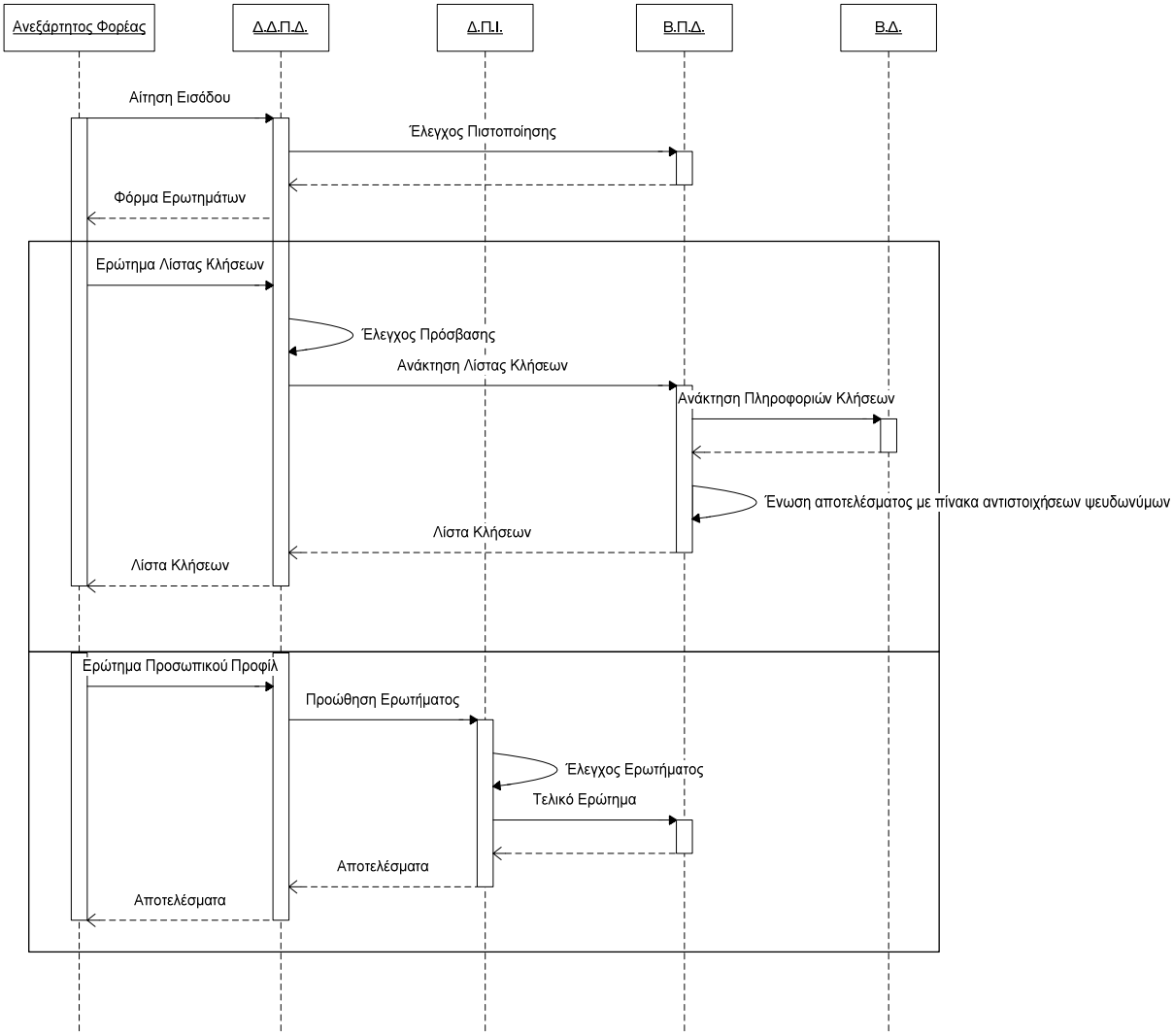
4.4.7 Παραλαβή Σύντομων Μηνυμάτων



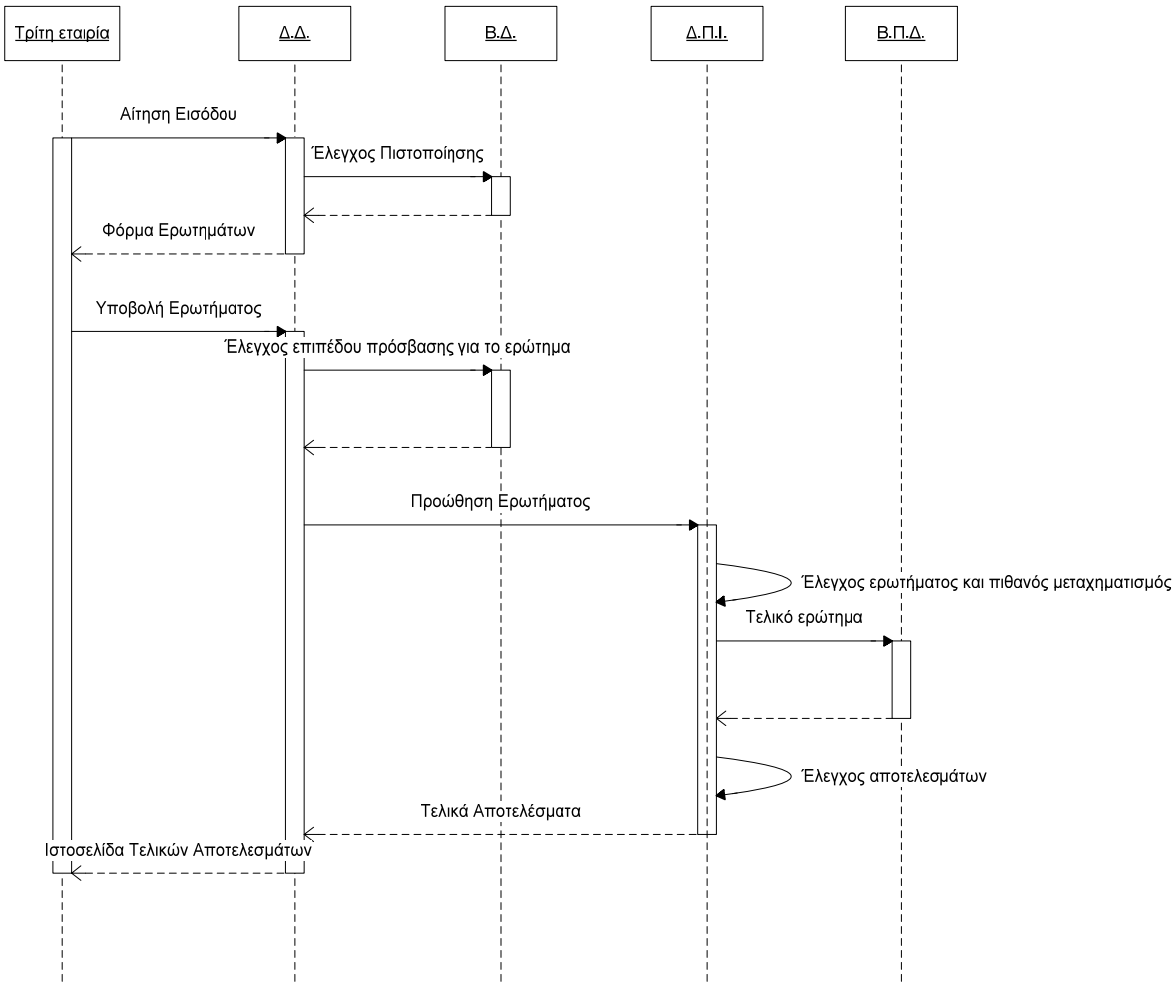
4.4.8 Υπηρεσίες Παρουσίας



4.4.9 Ανεξάρτητη αρχή ελέγχει τα στοιχεία του χρήστη (lawful interception)



4.4.10 Τρίτη εταιρεία βλέπει στοιχεία χρηστών



5

Σχεδίαση Συστήματος

Το σύστημα που περιγράφτηκε στα προηγούμενα κεφάλαια παρουσιάζει εκτεταμένη πολυπλοκότητα με αποτέλεσμα να μην είναι δυνατή η πλήρης υλοποίησή του στο πλαίσιο της συγκεκριμένης διπλωματικής εργασίας. Στο παρόν κεφάλαιο θα παρουσιάσουμε τη σχεδίαση της υλοποίησης των σημαντικότερων υποσυστημάτων με τη βοήθεια των σύγχρονων εργαλείων, που υπάρχουν στο συγκεκριμένο τομέα. Ως πλατφόρμα υλοποίησης του λογισμικού του συστήματος επιλέχτηκε η Java για τους παρακάτω λόγους:

- Το αντικειμενοστραφές μοντέλο ανάπτυξης και συγγραφής κώδικα ταιριάζει στη φύση του συστήματος μας, αφού παρουσιάζεται ανάγκη για διαχωρισμό των λειτουργιών σε κάθε υποσύστημα. Οι δυνατότητες που παρέχει η πλατφόρμα για κληρονομικότητα, πολυμορφισμό και αφαιρετικότητα επιτρέπουν τον ευκολότερο σχεδιασμό των υποσυστημάτων, αφού το επίπεδο υλοποίησης αποκρύπτεται από καλά ορισμένες διεπαφές.
- Η ύπαρξη ενός εικονικού μηχανήματος (VM) σημαίνει ότι η υλοποίηση του συστήματος θα είναι θεωρητικά ανεξάρτητη από το σύστημα ανάπτυξης και θα μπορεί πολύ εύκολα να μεταφερθεί σε διαφορετικές αρχιτεκτονικές και λειτουργικά συστήματα.
- Ύπαρξη πολλών έτοιμων βιβλιοθηκών που παρέχουν αυξημένες δυνατότητες στο χειρισμό πολύπλοκων δομών, αλλά και στην εκτέλεση τυπικών λειτουργιών. Μεταξύ αυτών υπάρχει βιβλιοθήκη διαδικτυακής επικοινωνίας και υλοποίησης υπηρεσιών ασφαλείας στο διαδίκτυο.
- Ύπαρξη ανοικτών API για χρήση των βασικών υποσυστημάτων της προτεινόμενης αρχιτεκτονικής.
    - JAIN-SIP για τη χρήση του πρωτοκόλλου SIP [41]
    - Jena για την αξιοποίηση των οντολογιών. [42]

- Ύπαρξη ελεύθερων προγραμμάτων ανοιχτού κώδικα, που υλοποιούν πολλές από τις βασικές λειτουργίες που απαιτούνται από το σύστημα. Επιλέχτηκαν βασικές εκδόσεις δύο προγραμμάτων με πολύ συγκεκριμένη λειτουργικότητα για λόγους απλότητας και για να επικεντρωθεί η σχεδίαση και ανάπτυξη στην προσθήκη των απαραίτητων λειτουργιών, που απαιτούνται για την επίτευξη της προστασίας της ιδιωτικότητας. Συγκεκριμένα: επιλέχτηκε ένα πρόγραμμα διαδικτυακής τηλεφωνίας (softphone), το οποίο υλοποιεί τις λειτουργίες που απαιτεί η αρχιτεκτονική του SIP από την πλευρά του πελάτη και ένα πρόγραμμα διακομιστή, το οποίο υλοποιεί τις λειτουργίες του ενδιάμεσου διακομιστή, του διακομιστή καταχώρισης χρηστών, του διακομιστή θέσης και του διακομιστή παρουσίας. Τα προγράμματα αυτά χρησιμοποιούνται και για εκπαιδευτικούς σκοπούς στο μάθημα «Τεχνολογία λογισμικού» της Σχολής ΗΜΜΥ του ΕΜΠ [43], οπότε υπήρχε μια βασική εξοικείωση μ' αυτά, που διευκόλυνε τη σχεδίαση του λογισμικού προστασίας ιδιωτικότητας.
    - Jain-Sip Video Phone Application (Sip Communicator) [44]:
    - Jain-sip Proxy Server [45]:
- Η ύπαρξη του IDE Eclipse και όλων των συμπληρωματικών εργαλείων του, όπως το subclipse, το οποίο συνδέεται με ένα SVN Server για υλοποίηση ελέγχου εκδόσεων κώδικα (versioning), διευκολύνουν σε μεγάλο βαθμό την ανάπτυξη λογισμικού και βελτιώνουν την αποδοτικότητα των ομάδων ανάπτυξης λογισμικού.

Η σημαντικότερη δομική μονάδα, η οποία θα πρέπει να υλοποιηθεί, είναι ο Δ.Π.Ι.. Εξάλλου μια από τις βασικές απαιτήσεις σχεδίασης επιβάλλει την ελαχιστοποίηση των παρεμβάσεων στο λογισμικό τόσο της εφαρμογής πελάτη, όσο και των υπολοίπων δομικών μονάδων του συστήματος. Οι λειτουργίες του Δ.Π.Ι., όπως φαίνεται και στο σχήμα στο τέλος του Κεφ. 3, χωρίζονται στις παρακάτω τρεις κατηγορίες.

- Προστασία διευθύνσεων IP
- Προστασία περιεχομένου μηνυμάτων SIP
- Μηχανισμός πρόσβασης στα προσωπικά δεδομένα των χρηστών.

5.1 Προστασία διευθύνσεων IP

Πριν προχωρήσουμε στην ανάλυση του σχεδιασμού του συστήματος κρίνεται σκόπιμη μια σύντομη παρουσίαση του API JAIN-SIP, καθώς χρησιμοποιείται εκτενώς στη συνέχεια του κεφαλαίου και αποτελεί τη βάση των δύο προγραμμάτων εφαρμογής, που επιλέχτηκαν..

5.1.1 JAIN-SIP

Το JAIN-SIP τη συγκεκριμένη χρονική περίοδο βρίσκεται στην πειραματική έκδοση 2.0 [41],[45]. Η τελευταία σταθερή έκδοση του πακέτου είναι η 1.2 , ενώ πολλές από τις υπάρχουσες εφαρμογές χρησιμοποιούν ακόμα την έκδοση 1.1. Το JAIN-SIP εκμεταλλεύεται τις δυνατότητες που παρέχει ο αντικειμενοστραφής προγραμματισμός, καθώς και διάφορα σχεδιαστικά μορφήματα, για να επιτύχει την εύκολη επεξεργασία και μεταφορά των μηνυμάτων SIP από τις εφαρμογές.

5.1.1.1 Τα πακέτα και οι επιμέρους λειτουργίες

Τα επιμέρους πακέτα του JAIN-SIP και οι λειτουργίες που αυτά επιτελούν [45] είναι τα παρακάτω:

- javax.sip.address:
- javax.sip.header:
- javax.sip.message:

Τα τρία αυτά πακέτα περιέχουν τις διεπαφές που περιγράφουν τη δομή και τις μεθόδους δημιουργίας και επεξεργασίας, των διευθύνσεων που χρησιμοποιούνται στο SIP (SIP URI), των επικεφαλίδων των μηνυμάτων SIP (SIP Headers) και των ίδιων των μηνυμάτων SIP.

- gov.nist.javax.sip.address:
- gov.nist.javax.sip.header:
- gov.nist.javax.sip.header.extensions:
- gov.nist.javax.sip.header.ims:
- gov.nist.javax.sip.message:

Τα παραπάνω πακέτα περιέχουν τις κλάσεις υλοποίησης των αντίστοιχων διεπαφών και για τη λειτουργία τους χρησιμοποιούνε κλάσεις από τα πακέτα gov.nist.javax.sip.parser, gov.nist.javax.sip.parser.extensions, gov.nist.javax.sip.parser.ims ώστε να επιτύχουν τη μετατροπή κατάλληλων αλφαριθμητικών σειρών σε αντικείμενα.

- gov.nist.core.net:

Πακέτο που ασχολείται με την επικοινωνία με το επίπεδο δικτύου και συγκεκριμένα υλοποιεί μια μέθοδο επίλυσης διευθύνσεων και τη δημιουργία, διαχείριση και χρησιμοποίηση των πορτών (sockets) επικοινωνίας.

- javax.sdp:
- gov.nist.javax.sdp:
- gov.nist.javax.sdp.fields:
- gov.nist.javax.sdp.parser:

Το πρώτο πακέτο περιέχει τις διεπαφές (interfaces), οι οποίες αναπαριστούν τις δομές περιγραφής συνόδων SDP, ενώ τα υπόλοιπα πακέτα περιέχουν κλάσεις που διαχειρίζονται, ορίζουν και μετατρέπουν αντίστοιχα τις δομές περιγραφής συνόδων SDP.

- javax.sip:

Το συγκεκριμένο πακέτο περιέχει τις διεπαφές (interfaces), οι οποίες περιγράφουν την αρχιτεκτονική υλοποίησης μιας μηχανής ικανής για τη λήψη και την επεξεργασία μηνυμάτων SIP. Ταυτόχρονα, περιγράφονται τα γεγονότα (events), τα οποία διέπουν τη λειτουργία του συστήματος καθώς και οι εξαιρέσεις (exceptions), οι οποίες μπορούν να προκληθούν κατά τη λειτουργία του.

- gov.nist.javax.sip:
- gov.nist.javax.sip.stack:

Το πακέτο αυτό περιέχει τις κλάσεις υλοποίησης των διεπαφών του πακέτου javax.sip. Αυτές χρησιμοποιούνται για την υλοποίηση του παρόχου SIP (SipProvider) , της στοίβας SIP (SipStack) και του ακροατή SIP (SipListener), οι οποίοι είναι και αυτοί που αναλαμβάνουν την επεξεργασία των μηνυμάτων SIP, τη μετάδοση τους (εγγυημένη ή όχι) και την επικοινωνία της στοίβας SIP με το δίκτυο αντίστοιχα. Οι κλάσεις αυτού του πακέτου χρησιμοποιούν αυτές, που ορίζονται σε όλα τα υπόλοιπα πακέτα, για να εκτελέσουν την επικοινωνία με χρήση του πρωτοκόλλου SIP και όλες τις λειτουργίες, που αυτή συνεπάγεται.

5.1.1.2 Η αρχιτεκτονική

Η αρχιτεκτονική του API βασίζεται στα εξής.

Αρχικά δημιουργείται η SipStack, η οποία παρέχει το βασικό API στην εφαρμογή που θέλει να χρησιμοποιήσει το πρωτόκολλο SIP. Σε όρους δικτύου η SipStack αποτελεί την υλοποίηση των λειτουργιών του επιπέδου εφαρμογής ώστε να μπορούν εφαρμογές να χρησιμοποιήσουν διαφανώς το δίκτυο για να επικοινωνήσουν με άλλες αντίστοιχες εφαρμογές μέσω του δικτύου. Κάθε SipStack υλοποιείται θεωρητικά μία φορά σε κάθε μηχάνημα, ή υλοποιείται μία φορά τουλάχιστον για κάθε διεύθυνση IP , αφού διατηρεί συγκεκριμένη διεύθυνση IP, μοναδικό όνομα και χρησιμοποιεί ένα συγκεκριμένο ενδιάμεσο διακομιστή (outbound proxy), στον οποίο προωθεί τις καινούργιες αιτήσεις που παράγει. Η διεύθυνση IP της SipStack είναι αυτή που χρησιμοποιείται στο εσωτερικό των μηνυμάτων SIP και γι αυτό είναι πολύ σημαντική, αφού αν υποθέσουμε ότι χρησιμοποιείται ένα δίκτυο ανωνυμίας IP, η συγκεκριμένη διεύθυνση θα πρέπει να ταυτίζεται με τη διεύθυνση IP του κόμβου εξόδου.

Κάθε SipStack συνδέεται με ένα Router, ο οποίος παρέχει τις λειτουργίες δρομολόγησης δοθέντος ενός μηνύματος SIP, δηλαδή αποφασίζεται σε ποιον υπολογιστή θα σταλεί ένα μήνυμα SIP, εφαρμόζοντας τις πολιτικές δρομολόγησης ανά μήνυμα (πχ απευθείας δρομολόγηση στον προεπιλεγμένο ενδιάμεσο διακομιστή, δρομολόγηση ανάλογα με τον τύπο του μηνύματος, δρομολόγηση ανάλογα με τις επικεφαλίδες Route).

Για την υλοποίηση ασφαλούς μεταφοράς των μηνυμάτων πάνω από αναξιόπιστα πρωτόκολλα μεταφοράς, η SipStack επεκτείνει την κλάση SipTransactionStack, η οποία υλοποιεί μηχανισμούς συναλλαγών με καταστάσεις (statefull transactions) και παρέχει τις κατάλληλες μεθόδους για τη διαχείριση των συναλλαγών αυτών συνολικά. Ταυτόχρονα, υποστηρίζει τη διαχείριση διαλόγων (Dialogs), τα οποία αποτελούν την αναπαράσταση μιας εγκαθιδρυμένης SIP συνόδου. Οι διάλογοι χρησιμοποιούνται από τη SIP Stack για να αποστέλλονται μηνύματα-αιτήσεις σε μια ήδη εγκαθιδρυμένη σύνοδο SIP μεταξύ δύο μελών.

Για την επικοινωνία με το επίπεδο μεταφοράς, η SipStack δημιουργεί SipProviders και Listening Points. Κάθε Listening Point αναπαριστά ένα συγκεκριμένο socket, το οποίο χρησιμοποιεί ένα καθορισμένο πρωτόκολλο μεταφοράς για να στείλει τα μηνύματα στο δίκτυο. Κάθε SipProvider συνδέεται με κάποια Listening Points, τα οποία χρησιμοποιεί για να στείλει τα μηνύματα. Σε παλιότερες εκδόσεις επιτρεπόταν μονάχα ένας SipProvider ανά Listening Point, αλλά αυτό άλλαξε ώστε να μπορεί κάθε SipProvider να στέλνει μηνύματα με διαφορετικά πρωτόκολλα μεταφοράς. Παρ' όλα αυτά κάθε SipProvider δεν επιτρέπεται να χρησιμοποιεί Listening Points με ίδιο επίπεδο μεταφοράς. Αν μια εφαρμογή επιθυμεί να στέλνει μηνύματα από διαφορετικά sockets με το ίδιο επίπεδο μεταφοράς, θα πρέπει να ζητήσει τη δημιουργία περισσότερων SipProviders από τη SipStack. Κάθε καινούργιο

μήνυμα-αίτηση SIP, το οποίο θέλουμε να σταλεί με εγγυημένο τρόπο, δημιουργεί και μία συναλλαγή πελάτη (ClientTransaction) πριν σταλεί. Η αντίστοιχη συναλλαγή στην άλλη πλευρά του καναλιού επικοινωνίας είναι η συναλλαγή διακομιστή (ServerTransaction) και χρησιμοποιείται για την αποστολή του μηνύματος-απάντησης πίσω στον αποστολέα. Μόνο όταν φτάσει η απάντηση θεωρείται ολοκληρωμένη μια συναλλαγή πελάτη, αφού αν η απάντηση καθυστερήσει στέλνεται ξανά το μήνυμα. Υλοποιείται, δηλαδή, εν μέρει ο μηχανισμός αξιόπιστης μετάδοσης του TCP με χρήση χρονομέτρων, γεγονότων λήξης χρονομέτρου (TimeoutEvents) και με τα μηνύματα-απαντήσεις να παίζουν το ρόλο των επιβεβαιώσεων ACK. Παρόμοιος μηχανισμός προβλέπεται για τις συναλλαγές διακομιστή μόνο αν χρησιμοποιηθούν μηνύματα PRACK, αφού γενικά τα μηνύματα-απαντήσεις δεν επιβεβαιώνονται στο SIP. Ο SipProvider παρέχει μεθόδους για τη δημιουργία νέων συναλλαγών, για τη διαχείριση των Listening Points, τα οποία χρησιμοποιεί και για τη μετάδοση (αξιόπιστη η όχι) των μηνυμάτων, που του παραδίδονται από τη SipStack. Τέλος, θα πρέπει να αναφέρουμε ότι η SipStack είναι υπεύθυνη για την παρακολούθηση όλων των συνδέσεων SIP (SIP Transactions), που χειρίζεται και εξασκεί έλεγχο στο πλήθος τους για την αποφυγή της υπερφόρτωσης του διακομιστή. Τα μηνύματα που φτάνουν σε κάποιο από τα Listening Points αναγνωρίζονται από τον υπεύθυνο SipProvider, αντιστοιχίζονται στην κατάλληλη συναλλαγή, αν υπάρχει και στη συνέχεια δημιουργείται το γεγονός, το οποίο και χειρίζεται από τον κατάλληλο SIP Listener, ανάλογα με το αν το μήνυμα είναι αίτηση ή απάντηση.

Ακολουθούν τα διαγράμματα καταστάσεων των συναλλαγών πελάτη και διακομιστή καθώς και το ψηφιδικό διάγραμμα της αρχιτεκτονικής του JAIN-SIP.

Συναλλαγές πελάτη

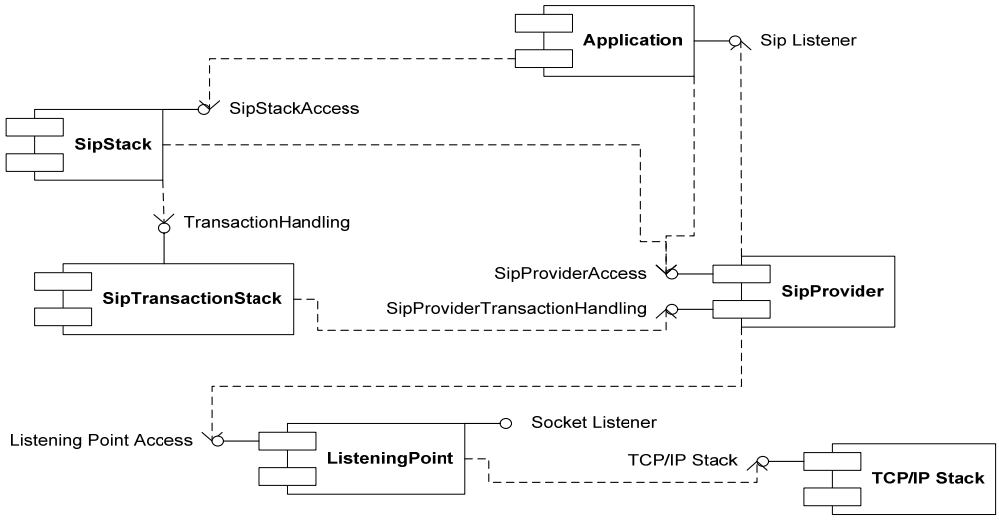
Invite Transaction:
Calling → Proceeding → Completed → Terminated

Non-Invite Transaction:
Trying → Proceeding → Completed → Terminated

Συναλλαγές διακομιστή

Invite Transaction:
Proceeding → Completed → Confirmed → Terminated

Non-Invite Transaction:
Trying → Proceeding → Completed → Terminated



Εικόνα 13: Η αρχιτεκτονική της διαπροσωπίας JAIN-SIP

5.1.2 Υλοποίηση προστασίας διευθύνσεων IP – Το δίκτυο Tor

Ο λόγος για τον οποίο αναλύθηκε εκτενώς το API του Jain-Sip είναι για να καταδειχθούν τα σημεία, στα οποία θα πρέπει να γίνουν τροποποιήσεις ώστε να μπορεί να ενταχθεί ένα διαφανές σύστημα ανωνυμίας IP.

Στο κεφάλαιο 3 αναλύθηκαν δύο συστήματα παροχής ανωνυμίας σε επίπεδο IP και από τη σύγκριση των δύο επιλέχθηκε η χρήση του onion routing για την παροχή της συγκεκριμένης υπηρεσίας στο κανάλι σηματοδοσίας του πρωτοκόλλου SIP. Η τελευταία έκδοση της τεχνολογίας του onion routing είναι το δίκτυο Tor [47]. Το δίκτυο αυτό αποτελεί ένα δίκτυο ανωνυμίας χαμηλής καθυστέρησης (low latency anonymity network), υλοποιεί τις αρχές του onion routing για την προστασία της διεύθυνσης IP και θεωρείται [48] η δεύτερη γενιά δικτύων ανωνυμίας βασισμένων σ' αυτή τη θεωρία. Το Tor ξεκίνησε ως ερευνητική πλατφόρμα [47],[48] της συγκεκριμένης θεωρίας με σκοπό να μελετηθεί η απόδοση ενός onion δικτύου σε πραγματική κλίμακα, αλλά οι πολύ καλές επιδόσεις του το οδήγησαν σύντομα σε μια πραγματική πλατφόρμα επίτευξης ανωνυμίας IP, η οποία χρησιμοποιείται τόσο από απλούς χρήστες σε όλο τον κόσμο, όσο και από επίσημες κρατικές υπηρεσίες. Ταυτόχρονα, πολλοί ερευνητές εργάζονται για την ανάλυση του σε θεωρητικό επίπεδο [48], αλλά και μηχανικοί δουλεύουν πάνω στη επέκταση του και τη βελτίωση των υπηρεσιών, που προσφέρει [47].

Από τεχνικής άποψης το Tor υλοποιεί τη βασική θεωρία του onion routing και εισάγει κάποια νέα στοιχεία με σκοπό τη βελτίωση της απόδοσης του συστήματος. Το Tor λειτουργεί αποκλειστικά με φορτίο συνδέσεις TCP και οι κόμβοι του χρησιμοποιούν το γνωστό πρωτόκολλο SOCKS για να μπορούν οι εφαρμογές να αιτούνται την αποστολή μηνυμάτων με χρήση του δικτύου. Για λόγους απόδοσης και ασφάλειας τα εικονικά κυκλώματα που δημιουργούνται στο δίκτυο, διατηρούνται για 10 λεπτά, οπότε μελλοντικές αιτήσεις από τον ίδιο υπολογιστή θα δρομολογούνται από το ίδιο κύκλωμα, ενώ δεν υποστηρίζεται μεταφορά συνδέσεων, κάτι που σημαίνει ότι μετά το πέρας των 10 λεπτών το σύστημα θα περιμένει να λήξει η τελευταία ενεργή TCP σύνδεση πριν αποδεσμεύσει το εικονικό κύκλωμα. Το Tor χρησιμοποιεί ένα διακομιστή καταλόγου (directory server), ο οποίος διατηρεί την κατάσταση των ενεργών κόμβων του δικτύου, τις δυνατότητες τους σε εύρος ζώνης και παράλληλες συνδέσεις, ενώ απαντάει σε αιτήματα από τους κόμβους κατά

τη φάση εγκαθίδρυσης του κυκλώματος για την υπόδειξη άλλων ενεργών κόμβων, που μπορούν να χρησιμοποιηθούν στο εικονικό κύκλωμα.

Το νέο στοιχείο, που εισάγεται στο Tor, είναι οι κρυμμένες υπηρεσίες (hidden services) [47], λειτουργία που επιτρέπει σε πελάτες να μπορούν να συνδέονται σε μια ανώνυμη υπηρεσία. Αρχικά ο διακομιστής της υπηρεσίας επιλέγει κάποιους Tor κόμβους, που θα χρησιμοποιήσει ως κόμβους γνωστοποίησης (introduction points), δημιουργεί εικονικά κυκλώματα προς αυτούς και τους γνωστοποιεί ένα δημόσιο κλειδί που έχει δημιουργήσει. Στη συνέχεια, ο διακομιστής δημιουργεί μια περιγραφή της υπηρεσίας, η οποία περιλαμβάνει το δημόσιο κλειδί της και το σύνολο των κόμβων γνωστοποίησης και την δημοσιεύει σ' ένα διακομιστή καταλόγου, χρησιμοποιώντας και πάλι ένα εικονικό κύκλωμα. Η υπηρεσία λαμβάνει τότε ένα όνομα της μορφής XYZ.onion. Το XYZ είναι ένα αναγνωριστικό 16 χαρακτήρων, που προκύπτει μοναδικά από το δημόσιο κλειδί της υπηρεσίας. Το σύνολο ονομάτων «.onion» δεν αναγνωρίζεται από το παραδοσιακό σύστημα DNS και οι εφαρμογές, που το συναντούν, θα πρέπει να γνωρίζουν ένα διακομιστή καταλόγου για να οδηγηθούν στην υπηρεσία. Ένας χρήστης που θέλει να συνδεθεί στην υπηρεσία και μαθαίνει το όνομά της με κάποιο τρόπο, επικοινωνεί ανώνυμα με το διακομιστή καταλόγου και παίρνει τη λίστα των κόμβων γνωστοποίησης. Ταυτόχρονα, επικοινωνεί μ' έναν ειδικό κόμβο Tor και του ζητά να δράσει ως σημείο συνάντησης (rendezvous point) παρέχοντας του έναν αριθμό nonce. Ακολούθως, δημιουργεί ένα μήνυμα εγκαθίδρυσης, που περιλαμβάνει την τοποθεσία του σημείου συνάντησης και τον αριθμό nonce κρυπτογραφημένα με το δημόσιο κλειδί της υπηρεσίας και ζητά από έναν από τους κόμβους γνωστοποίησης να το προωθήσουν στο διακομιστή της υπηρεσίας. Αυτό μπορεί να υλοποιηθεί είτε διατηρώντας ένα ημιμόνιμο εικονικό κύκλωμα από κάθε κόμβο γνωστοποίησης προς το διακομιστή, είτε χρησιμοποιώντας ένα reply onion. Ο διακομιστής της υπηρεσίας αποκρυπτογραφεί το μήνυμα και βρίσκει τη διεύθυνση του σημείου συνάντησης και τον αριθμό nonce. Τέλος, ο διακομιστής της υπηρεσίας δημιουργεί ένα εικονικό κύκλωμα προς το σημείο συνάντησης, παραδίδει σ' αυτό τον αριθμό nonce, πιστοποιώντας ότι είναι πράγματι η υπηρεσία, που ζήτησε ο πελάτης και το σημείο συνάντησης συνενώνει τα δύο κυκλώματα για να δημιουργηθεί μια διαδρομή από τον πελάτη στο διακομιστή.

Το δίκτυο Tor, αν και προς το παρόν χρησιμοποιείται κυρίως για περιήγηση στον ιστό, μπορεί να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή, υποστηρίζει χρήση επικοινωνίας με ενδιάμεσους διακομιστές μέσω του SOCKS. Συγκεκριμένα, με τα υπάρχοντα εργαλεία που είδαμε η υλοποίηση του συστήματος θα έχει ως εξής:

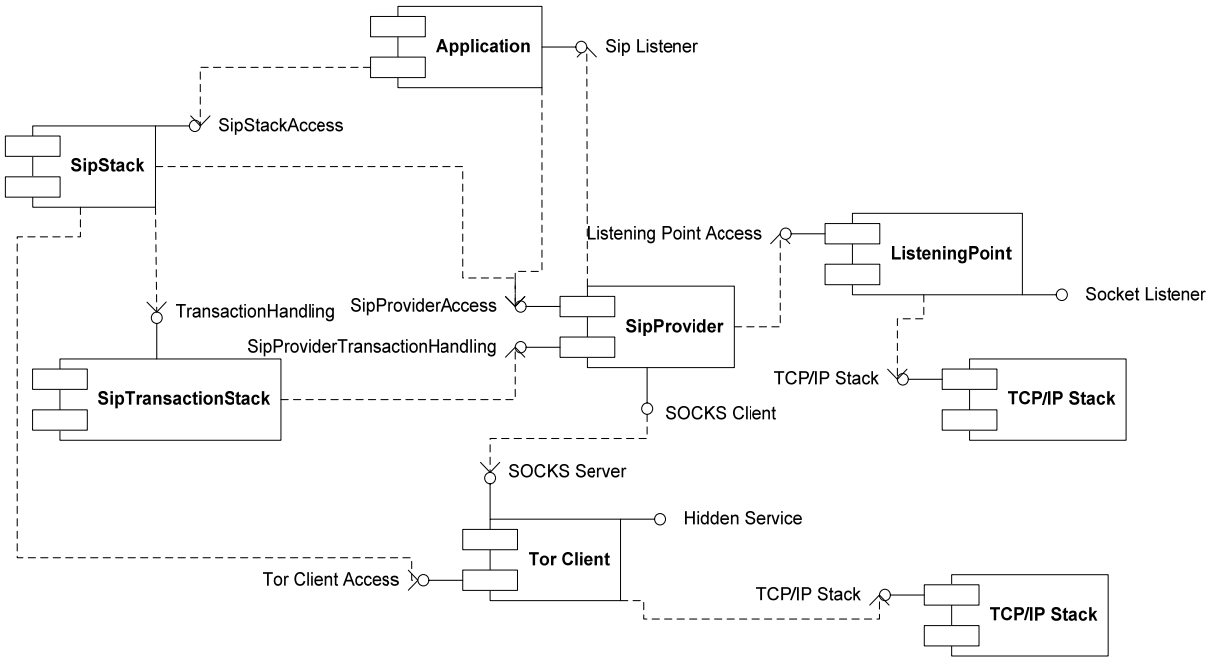
- Αρχικά θα πρέπει να αναφέρουμε ότι όλες οι λειτουργίες του διακομιστή καταλόγου θα πρέπει να ενσωματωθούν στο Δ.Π.Ι., κάτι που προβλέπεται και από την αρχιτεκτονική μας. Σε σχέση μ' αυτά που αναφέρθηκαν στο κεφάλαιο 3, ο Δ.Π.Ι. θα πρέπει να υλοποιεί και τις λειτουργίες εγκαθίδρυσης κρυφών υπηρεσιών.
- Ο πελάτης του συστήματος θα πρέπει να τρέχει σε δικό του μηχάνημα τον Tor client για τη χρήση του δικτύου Tor. Σε περίπτωση που το UA του πελάτη είναι περιορισμένων δυνατοτήτων (π.χ. φορητή συσκευή), ο πελάτης μπορεί να συνδεθεί με κάποιο ασφαλές πρωτόκολλο μεταφοράς στον οικιακό του υπολογιστή, ο οποίος θα δρα ως διακομιστής εισόδου στο δίκτυο Tor.
- Η SipStack του πελάτη θα δημιουργήσει έναν ειδικό SipProvider, ο οποίος θα πρέπει να υλοποιεί και τις λειτουργίες ενός SOCKS client για να μπορεί να επικοινωνεί με

τον Tor client. Ο SipProvider θα πρέπει με τη σειρά του να δημιουργήσει ένα Listening Point σε κάποια πόρτα, η οποία θα χρησιμοποιεί το πρωτόκολλο TLS, αφού παράλληλα με τη χρήση του Tor απαιτείται κρυπτογράφηση από άκρο σε άκρο. Όταν ο χρήστης επιθυμεί να στείλει ένα μήνυμα-αίτηση SIP θα αποστέλλει το μήνυμα στο SIP provider και αυτός θα χρησιμοποίει τον Tor client για να εισάγει το μήνυμα στο δίκτυο Tor και να λάβει το μήνυμα-απάντηση απ' αυτό. Στην περίπτωση εγκαθίδρυσης κλήσεων από το χρήστη θα πρέπει να φροντίζει να κρατάει ενεργή την TCP σύνδεση από την οποία θα στείλει το SIP ACK ώστε ο ενδιάμεσος διακομιστής SIP να μπορεί να την χρησιμοποιήσει για να του στείλει μελλοντικά μηνύματα ως μέρος του συγκεκριμένου διαλόγου SIP.

- Από την πλευρά του παραλήπτη η SipStack θα πρέπει να υλοποιεί κάποια κρυμμένη υπηρεσία, αφού ο παραλήπτης δεν μπορεί να γνωρίζει πότε θα λάβει κάποια νέα αίτηση. Το ζητούμενο είναι να προστεθεί μια εγγραφή στο αρχείο Torrc που ελέγχει τη λειτουργία του Tor Client στο μηχάνημα, που έχει επιλέξει ο χρήστης. Οι εγγραφές αυτές έχουν την παρακάτω μορφή:

```
HiddenServiceDir /Library/Tor/var/lib/Tor/hidden_service/
HiddenServicePort 80 127.0.0.1:5222
```

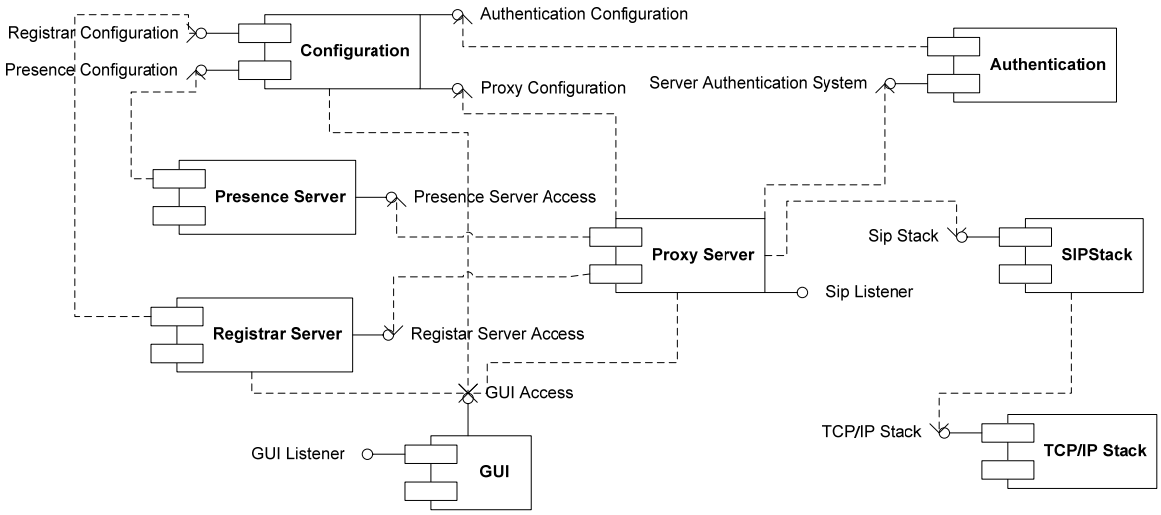
Η δεύτερη εγγραφή καθορίζει την πραγματική διεύθυνση IP και πόρτα του ListeningPoint, που χρησιμοποιεί εκείνη την ώρα η SipStack καθώς και την πόρτα από την οποία θα νομίζουν οι υπόλοιποι χρήστες ότι προέρχεται η κίνηση. Η πρώτη εγγραφή καθορίζει ένα φάκελο του συστήματος, στο οποίο τρέχει ο Tor Client και σ' αυτόν εισάγονται δύο αρχεία με ονόματα «private_key» και «hostname», τα οποία περιέχουν το ζεύγος δημοσίου/ιδιωτικού κλειδιού και το δημόσιο όνομα «.onion» της υπηρεσίας. Ο Tor Client είναι υπεύθυνος για τη δημοσιοποίηση του συγκεκριμένου ονόματος στο διακομιστή καταλόγου/Δ.Π.Ι. με τη χρησιμοποίηση ενός ανώνυμου εικονικού κυκλώματος. Η SipStack θα πρέπει να ειδοποιηθεί με κάποιο τρόπο από τον Tor Client για την επιτυχία της εγγραφής και να αποθηκεύσει σε μια τοπική μεταβλητή το όνομα της υπηρεσίας. Το όνομα αυτό θα πρέπει να χρησιμοποιείται από τη SipStack στην επικεφαλίδα «Contact» και την επικεφαλίδα «Via» κάθε εξερχόμενου μηνύματος του πελάτη και να χρησιμοποιείται από τον κατάλληλο ενδιάμεσο διακομιστή SIP για την εγκαθίδρυση ενός ανώνυμου εικονικού κυκλώματος μεταξύ των δύο. Αυτό σημαίνει ότι ο ενδιάμεσος διακομιστής SIP θα πρέπει να υλοποιεί τις λειτουργίες, που αναφέρθηκαν παραπάνω ως προς την επιλογή σημείου συνάντησης, αλλά από τη στιγμή που δεν μας ενδιαφέρει η προστασία της IP του διακομιστή, το σημείο συνάντησης μπορεί να είναι ο ίδιος ο ενδιάμεσος διακομιστής SIP. Μ' αυτόν τον τρόπο, ακόμα και αν ο πελάτης του συστήματος χρειάζεται να λάβει ένα μήνυμα, η εγκαθίδρυση των εικονικών κυκλωμάτων θα λαμβάνει χώρα πάντα με κατεύθυνση από τον πελάτη στον ενδιάμεσο διακομιστή SIP.



Εικόνα 14: Η αρχιτεκτονική ενσωμάτωσης του Tor στο JAIN-SIP

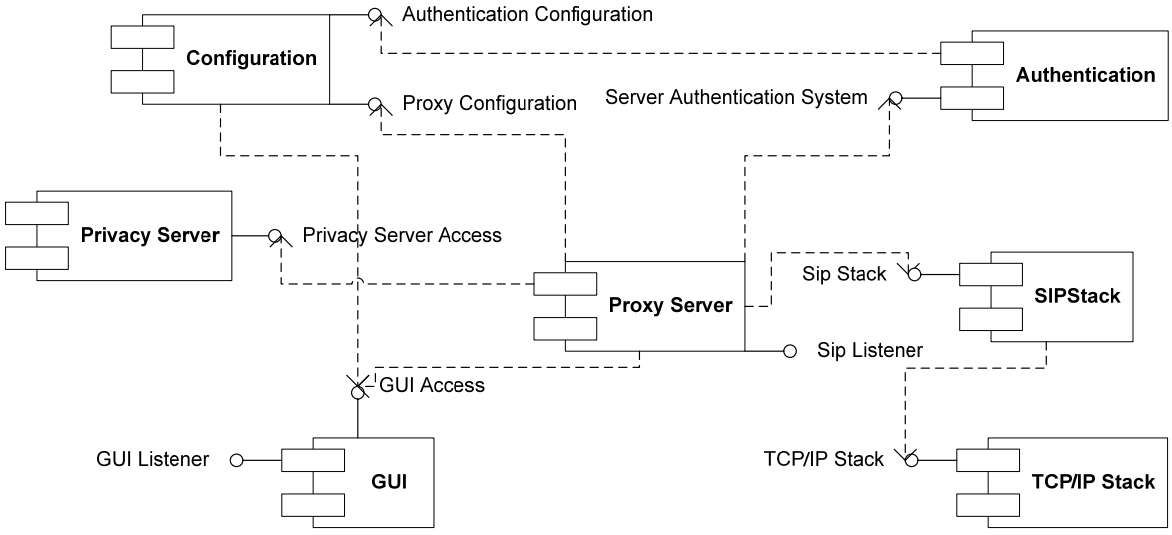
5.2 Προστασία περιεχομένου μηνυμάτων SIP

Η σχεδίαση του Δ.Π.Ι. όσον αφορά στην υλοποίηση της προστασίας των περιεχομένων των μηνυμάτων SIP, θα βασισθεί στη σχεδίαση ενός ήδη υπάρχοντος συστήματος δομικής μονάδας SIP ώστε να είναι δυνατή η επαναχρησιμοποίηση του κώδικα των λειτουργιών, που είναι κοινές και αφορούν κυρίως τη λήψη και μετάδοση μηνυμάτων SIP. Άλλωστε, ο Δ.Π.Ι. περιέχει στη βάση του μια δομική μονάδα SIP, η οποία λαμβάνει και προωθεί μηνύματα. Ακολουθεί το ψηφιδικό διάγραμμα του Jain-sip Proxy Server, όπου είναι σαφής η διάρθρωση των υποσυστημάτων του και τα σημεία επικοινωνίας μεταξύ τους.



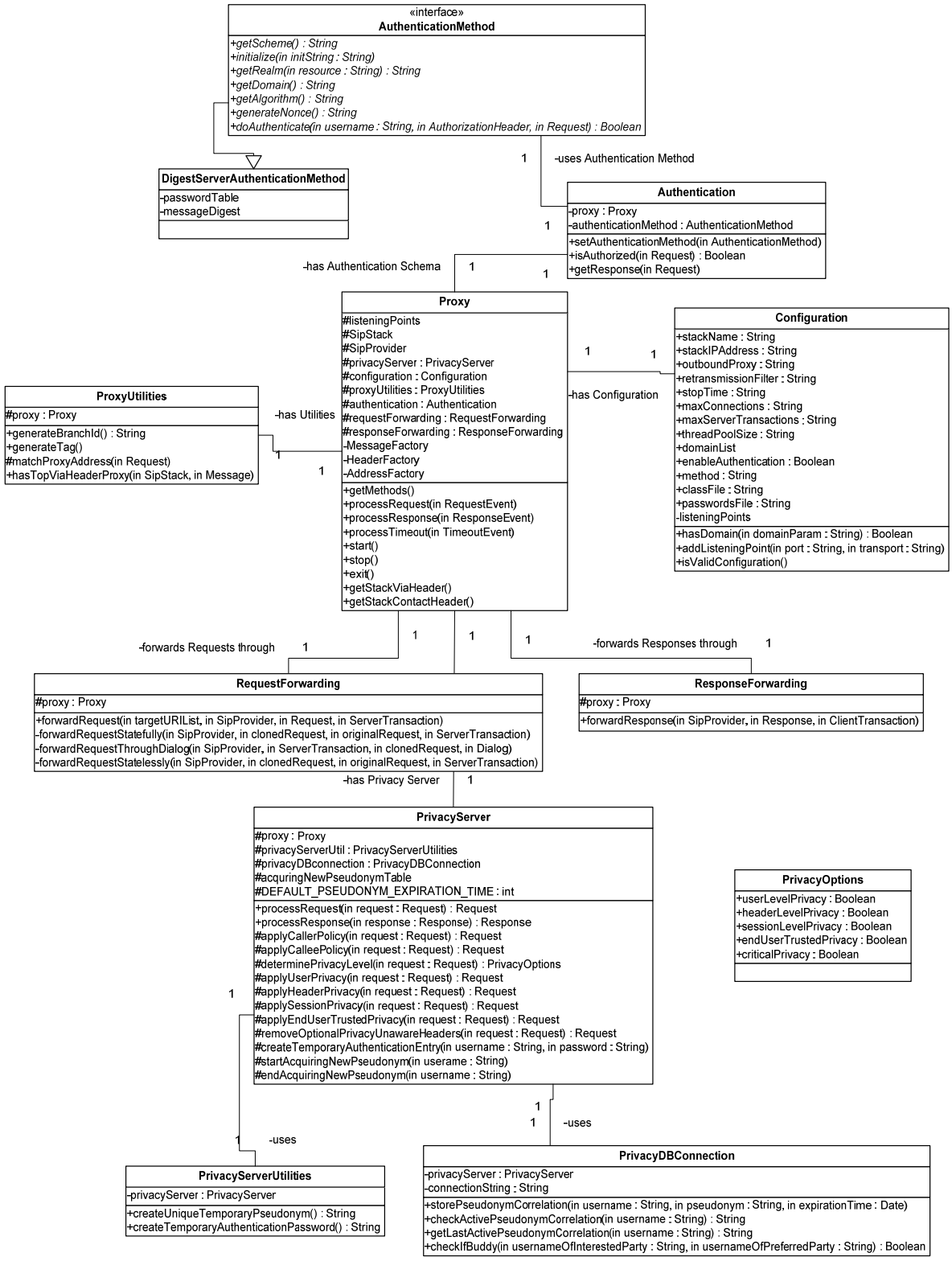
Εικόνα 15: Ψηφιδικό διάγραμμα υποσυστημάτων JAIN-SIP-PROXY SERVER

Με βάση την παραπάνω σχεδίαση και αξιοποιώντας τα υποσυστήματα, τα οποία χρησιμοποιούνται για τη δρομολόγηση των μηνυμάτων SIP, το ψηφιδικό διάγραμμα της δομικής μονάδας SIP Δ.Π.Ι. θα έχει ως εξής:



Εικόνα 16: Ψηφιδικό διάγραμμα υποσυστημάτων Δ.Π.Ι.

Οι λειτουργίες της δομικής μονάδας περιλαμβάνουν την υλοποίηση των λειτουργιών, που αναφέρθηκαν κατά τη σχεδίαση της αρχιτεκτονικής του συστήματος.



Εικόνα 17: Διάγραμμα κλάσεων Δ.Π.Ι.

Αναλυτικά οι μέθοδοι των κλάσεων του PrivacyServer και οι λειτουργίες, που αυτές επιτελούν έχουν ως εξής:

5.2.1 PrivacyServer:

Κλάση που υλοποιεί τις λειτουργίες προστασίας ιδιωτικότητας των μηνυμάτων SIP, εφαρμόζοντας το μηχανισμό, που περιγράφηκε στο Κεφ. 3.

Ιδιότητες:

a. *Proxy proxy:* Αποτελεί την αναφορά (java reference) στο υποκείμενο σύστημα Proxy, το οποίο είναι υπεύθυνο για τη δρομολόγηση και μετάδοση των μηνυμάτων.
b. *PrivacyServerUtil privacyServerUtil:* Αποτελεί την αναφορά στο αντικείμενο, που υλοποιεί αυτόνομες διαδικασίες απαραίτητες για τη λειτουργία του Δ.Π.Ι.
c. *PrivacyDBConnection privacyDBConnection:* Αποτελεί την αναφορά στο αντικείμενο, που υλοποιεί τη διαπροσωπία επικοινωνίας με τη Βάση Προσωπικών Δεδομένων.
d. *HashTable acquiringNewPseudonymTable:* Αποτελεί μια συλλογή, η οποία υποδεικνύει τους χρήστες του συστήματος, οι οποίοι βρίσκονται σε διαδικασία ανανέωσης ψευδωνύμου και απαγορεύεται να τους προωθηθεί κάποιο μήνυμα.

Μέθοδοι:

a. *Request processRequest(Request):* Η συγκεκριμένη μέθοδος δέχεται ένα αντικείμενο που αναπαριστά ένα μήνυμα-αίτηση και αφού εφαρμόσει τις πολιτικές προστασίας της ιδιωτικότητας, που ορίζονται στην επικεφαλίδα «Privacy» αυτού καθώς και τις πολιτικές προστασίας της ιδιωτικότητας του παραλήπτη, επιστρέφει στον Proxy Server το αντικείμενο που αναπαριστά το μήνυμα-αίτηση, που θα πρέπει να προωθηθεί στον Ενδιάμεσο Διακομιστή SIP της εταιρείας παροχής υπηρεσιών.
b. *Response processResponse(Response):* Η μέθοδος που εφαρμόζει λειτουργίες προστασίας της ιδιωτικότητας στα μηνύματα απαντήσεις.
c. *Request applyCallerPolicy(Request):* Η μέθοδος αυτή εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας Αποστολέα και επιστρέφει το μήνυμα προς αποστολή.
d. *Request applyCallePolicy(Request):* Μέθοδος, η οποία εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας Παραλήπτη και επιστρέφει το μήνυμα προς αποστολή.
e. *PrivacyOptions determinePrivacyLevel(Request):* Η μέθοδος αυτή μετατρέπει (parsing) την επικεφαλίδα «Privacy» ενός μηνύματος-αίτησης στο αντικείμενο επιλογών προστασίας ιδιωτικότητας.
f. *Request applyUserPrivacy(Request):* Η μέθοδος αυτή εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας, που περιλαμβάνονται στο επίπεδο user και ορίζονται στο RFC 3323.
g. *Request applyHeaderPrivacy(Request):* Η μέθοδος αυτή εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας, που περιλαμβάνονται στο επίπεδο header και ορίζονται στο RFC 3323.
h. *Request applySessionPrivacy(Request):* Μέθοδος, η οποία εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας, που περιλαμβάνονται στο επίπεδο Session και ορίζονται στο RFC 3323.

i. *Request applyEndUserTrustedPrivacy(Request):* Η μέθοδος αυτή εφαρμόζει τις λειτουργίες προστασίας ιδιωτικότητας, που περιλαμβάνονται στο επίπεδο End-User-Trusted και ορίζονται στο Κεφ.3 της παρούσας διπλωματικής εργασίας.
j. *Request removeOptionalPrivacyUnawareHeaders(Request):* Μέθοδος, η οποία αφαιρεί από το μήνυμα-αίτηση όλες τις προαιρετικές επικεφαλίδες SIP, οι οποίες μπορεί να αποκαλύψουν προσωπικά στοιχεία του Αποστολέα.
k. *createTemporaryAuthenticationEntry(String, String):* Η μέθοδος αυτή δημιουργεί στο σύστημα πιστοποίησης της εταιρείας κατάλληλη εγγραφή για το προσωρινό ψευδώνυμο χρήστη, ώστε ο χρήστης να μπορεί να στέλνει για λόγους απόδοσης απευθείας μηνύματα στην εταιρεία παροχής υπηρεσίας, χρησιμοποιώντας το προσωπικό του ψευδώνυμο.
l. *startAcquiringNewPseudonym(String):* Η μέθοδος αυτή καταδεικνύει ότι ένας χρήστης ξεκινάει τη διαδικασία ανανέωσης ψευδωνύμου και δεν μπορεί να δέχεται μηνύματα.
m. *stopAcquiringNewPseudonym(String):* Η μέθοδος αυτή καταδεικνύει ότι ένας χρήστης ολοκλήρωσε τη διαδικασία ανανέωσης ψευδωνύμου και μπορεί να δεχθεί ξανά μηνύματα.

5.2.2 PrivacyDBConnection:

Κλάση, που προσφέρει συγκεκριμένη διεπαφή για την επικοινωνία με τη Βάση Προσωπικών Δεδομένων.

Ιδιότητες:

a. *PrivacyServer privacyServer:* Αποτελεί την αναφορά στο αντικείμενο PrivacyServer στο οποίο προσφέρονται οι υπηρεσίες.
b. *String connectionString:* Περιγράφει τον τρόπο επικοινωνίας με τη Βάση.

Μέθοδοι:

a. *storePseudonymCorrelation(String,String,Date):* Η μέθοδος αυτή αποθηκεύει στη Βάση τη συσχέτιση χρήστη – προσωρινού ψευδωνύμου και το χρόνο μέχρι τον οποίο είναι έγκυρη.
b. *String checkActivePseudonymCorrelation(String):* Η μέθοδος αυτή επιστρέφει το τρέχον ενεργό ψευδώνυμο του χρήστη, ή «κενό» αν έχει περάσει ο χρόνος αντιστοίχισης του.
c. *String getLastActivePseudonymCorrelation(String):* Η μέθοδος αυτή επιστρέφει το τελευταίο ενεργό ψευδώνυμο του χρήστη για χρήση του μετά από μελλοντική επανείσοδο στο σύστημα, όπως περιγράφεται στο κεφ. 3
d. *Boolean checkIfBuddy(String, String):* Η μέθοδος αυτή υποδεικνύει αν ένας χρήστης είναι έμπιστος κάποιου άλλου και χρησιμοποιείται στην παροχή υπηρεσιών παρουσίας.

5.2.3 PrivacyServerUtilities:

Κλάση, που παρέχει συμπληρωματικές ανεξάρτητες υπηρεσίες στην κύρια κλάση.

Ιδιότητες:

a. *PrivacyServer privacyServer:* Αποτελεί την αναφορά στο αντικείμενο PrivacyServer, στο οποίο προσφέρονται οι υπηρεσίες.

Μέθοδοι:

a. *String createUniqueTemporaryPseudonym():* Η μέθοδος αυτή επιστρέφει ένα μοναδικό προσωρινό ψευδώνυμο για χρήση σε προστασία ιδιωτικότητας Παραλήπτη.
b. *String createTemporaryAuthenticationPassword():* Η μέθοδος αυτή επιστρέφει ένα τυχαίο μοναδικό κωδικό πρόσβασης.

5.2.4 PrivacyOptions:

Κλάση, που αναπαριστά τις επιλογές προστασίας ιδιωτικότητας ενός μηνύματος.

Ιδιότητες:

a. *Boolean userLevelPrivacy:* Αν το μήνυμα χρειάζεται εφαρμογή προστασίας ιδιωτικότητας επιπέδου user.
b. *Boolean headerLevelPrivacy:* Αν το μήνυμα χρειάζεται εφαρμογή προστασίας ιδιωτικότητας επιπέδου header.
c. *Boolean sessionLevelPrivacy:* Αν το μήνυμα χρειάζεται εφαρμογή προστασίας ιδιωτικότητας επιπέδου session.
d. *Boolean endUserTrustedPrivacy:* Αν το μήνυμα χρειάζεται εφαρμογή της υπηρεσίας end-user-trusted
e. *Boolean criticalPrivacy:* Αν η εφαρμογή προστασίας ιδιωτικότητας στο μήνυμα θεωρείται απολύτως απαραίτητη.

5.3 Μηχανισμός πρόσβασης στα προσωπικά δεδομένα των χρηστών

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο για την εξασφάλιση της προστασίας των προσωπικών δεδομένων των χρηστών κατά την προσπέλαση της βάσης δεδομένων από την εταιρεία παροχής υπηρεσιών διαδικτυακής τηλεφωνίας θα χρησιμοποιηθεί ένα υποσύστημα βασισμένο σε μια σημασιολογική οντολογία, το οποίο θα ελέγχει και θα μετασχηματίζει τα ερωτήματα που εκτελούνται στη Βάση, ώστε τα επιστρεφόμενα αποτελέσματα να μην αποκαλύπτουν προσωπική πληροφορία. Σ' αυτό το σημείο κρίνεται σκόπιμο να γίνει μια σύντομη περιγραφή της έννοιας της οντολογίας και στη συνέχεια να παρουσιασθεί ο μηχανισμός με τον οποίο μπορεί να υλοποιηθεί η επιθυμητή λειτουργικότητα στο σύστημα.

5.3.1 Η έννοια της οντολογίας

Ο όρος «οντολογία» στην περιοχή της επιστήμης υπολογιστών και του σημασιολογικού δικτύου χρησιμοποιείται για να περιγράψει μία τεχνική που επιτρέπει τη μοντελοποίηση και τη φορμαλιστική αναπαράσταση ενός συνόλου εννοιών, που ανήκουν σ' ένα συγκεκριμένο πεδίο και τις συσχετίσεις, που υπάρχουν μεταξύ τους [49]. Μέσω της οντολογίας δίνεται η δυνατότητα να περιγραφούν ιδέες, γεγονότα και αντικείμενα, ο τρόπος με τον οποίο αλληλεπιδρούν και σχετίζονται μεταξύ τους, καθώς και το πώς κατηγοριοποιούνται. Μια ορθώς σχεδιασμένη οντολογία που αναπαριστά έννοιες από ένα πεδίο μπορεί να χρησιμοποιηθεί για την εξαγωγή συμπερασμάτων με αυτόματο τρόπο, χρησιμοποιώντας ειδικό λογισμικό (reasoner) και μια γλώσσα ερωτημάτων πάνω σ' αυτήν καθώς είναι διαμορφωμένη με σαφείς κανόνες και αυστηρό φορμαλισμό.

Στη συγκεκριμένη διπλωματική η οντολογία, που θα χρησιμοποιηθεί για τη μοντελοποίηση των προσωπικών δεδομένων και των κανόνων που καθορίζουν την πρόσβαση της εταιρείας σ' αυτά, θα αναπτυχθεί στη πιο διαδεδομένη γλώσσα ανάπτυξης οντολογιών: την OWL (Web Ontology Language), η οποία προτείνεται [50] από τη W3C για εφαρμογές σχετικές με το σημασιολογικό ιστό. Τα δομικά στοιχεία που χρησιμοποιούνται στην OWL, αλλά και γενικότερα για να αναπτυχθεί μια οντολογία είναι: οι κλάσεις, τα άτομα και οι ιδιότητες [51],[52].

Οι κλάσεις (Classes) αποτελούν σύνολα ατόμων που έχουν κάποιες κοινές ιδιότητες. Κάθε κλάση έχει ορισμένες ιδιότητες (αλλιώς πεδία, slots ή properties), οι οποίες αυτόματα ενσωματώνονται στα άτομα που ανήκουν σ' αυτή. Μια κλάση μπορεί, επίσης, να έχει υποκλάσεις, οι οποίες κάνουν πιο συγκεκριμένη την έννοια της και κληρονομούν τις ιδιότητές της. Ένα άτομο (Instance), που ανήκει σε κάποια υποκλάση, ανήκει επίσης και στις κλάσεις, οι οποίες περιέχουν την κλάση αυτή. Ταυτόχρονα, υποστηρίζεται πολλαπλή κληρονομικότητα, δηλαδή ένα άτομο μπορεί να ανήκει σε πολλές κλάσεις και να διαθέτει την ένωση των ιδιοτήτων τους. Επίσης, υποστηρίζονται δύο βασικά ειδή ιδιοτήτων: οι ιδιότητες με τύπο δεδομένων (Datatype properties) και οι ιδιότητες αντικειμένων (Object properties). Οι ιδιότητες με τύπο δεδομένων είναι πεδία, τα οποία μπορούν να πάρουν τιμές ενός συγκεκριμένου τύπου δεδομένων και αποτελούν χαρακτηριστικό των ατόμων (συμβολοσειρές, αριθμούς, αληθοτιμές κτλ.). Αντίθετα, οι ιδιότητες αντικειμένων μπορούν να συμπληρωθούν με άτομα από συγκεκριμένες κλάσεις, που ορίζονται κατά τη δημιουργία της ιδιότητας. Με τις ιδιότητες αντικειμένων μπορούμε να εκφράσουμε σχέσεις μεταξύ ατόμων και μεταξύ κλάσεων.

Οι ιδιότητες, που συνδέουν άτομα και εκφράζουν συσχετίσεις μεταξύ τους, μπορούν να υπάρχουν σε ζεύγη με τις αντίστροφες (inverse) τους. Για παράδειγμα, η ιδιότητα «έχει-Παιδί» μπορεί να έχει σαν αντίστροφη την «έχει-Γονέα». Επίσης, οι ιδιότητες μπορούν να έχουν κάποια χαρακτηριστικά, τα οποία ρυθμίζουν τη σημασιολογία και τη λειτουργικότητά τους. Συγκεκριμένα, μια ιδιότητα μπορεί να είναι μεταβατική (transitive), συμμετρική (symmetric) συναρτησιακή (functional), ή αντίστροφα συναρτησιακή (inverse functional). Αν μια ιδιότητα prop είναι μεταβατική, τότε, αν ισχύει ότι A prop B και B prop Γ, εξάγεται το συμπέρασμα ότι ισχύει και A prop Γ. Αν είναι συμμετρική, τότε A prop B ισοδυναμεί με B prop A. Αν μια ιδιότητα είναι συναρτησιακή, τότε για ένα συγκεκριμένο άτομο υπάρχει μοναδικό άλλο άτομο, το οποίο σχετίζεται μ' αυτό μέσω αυτής της ιδιότητας. Αντίστοιχα, το ότι μια ιδιότητα είναι αντίστροφα συναρτησιακή, σημαίνει ότι η αντίστροφη της είναι

συναρτησιακή, δηλαδή ότι για ένα συγκεκριμένο άτομο μπορεί να υπάρχει μόνο ένα άλλο άτομο, το οποίο να σχετίζεται μ' αυτό μέσω της ιδιότητας. Αν μια ιδιότητα είναι συναρτησιακή και αντίστροφα συναρτησιακή, τότε διαμορφώνει σχέσεις ένα-προς-ένα στα άτομα που συνδέει.

Οι κλάσεις μπορούν να ορίζονται ρητά ή με χρήση πράξεων σε σύνολα ατόμων, που διαμορφώνονται από άλλες κλάσεις στην ιεραρχία. Για παράδειγμα: μια κλάση μπορεί να ορισθεί σαν την τομή των ατόμων δύο άλλων κλάσεων, ή το υποσύνολο των ατόμων μιας κλάσης, που έχουν μια συγκεκριμένη τιμή σε κάποια ιδιότητα. Αυτό επιτρέπει μεγάλη εκφραστικότητα στην οντολογία, κάνοντας δυνατή τη μοντελοποίηση συσχετίσεων και ομαδοποιήσεων, που ορίζονται με πολύπλοκους κανόνες. Ωστόσο, μπορεί να οδηγήσει σε ασυνέπειες, οι οποίες καθιστούν αδύνατη την εκτέλεση ερωτημάτων στη σχεδιαζόμενη οντολογία. Για να ανιχνευθούν οι ασυνέπειες στην οντολογία, να υπολογιστούν συμπεράσματα, τα οποία προκύπτουν από τον ορισμό της οντολογίας έμμεσα (για παράδειγμα το αν ένα άτομο ανήκει σε μία κλάση που έχει οριστεί, χρησιμοποιώντας πράξεις συνόλων μεταξύ υπαρχόντων κλάσεων), καθώς και για την εκτέλεση ερωτημάτων στην οντολογία, χρησιμοποιείται ειδικό λογισμικό (μηχανή λογισμού, reasoner), το οποίο εκτελεί σημασιολογική ανάλυση πάνω στην οντολογία και ελέγχει για ασυνέπειες στον ορισμό της. Μια σημαντική διαφορά, που θα πρέπει να επισημανθεί, είναι ότι η εξαγωγή συμπερασμάτων στις οντολογίες βασίζεται στη θεώρηση ανοιχτού κόσμου. Δηλαδή μια πρόταση που δεν μπορεί να επαληθευτεί με βάση την πληροφορία, που υπάρχει στην οντολογία, δεν μπορεί να θεωρηθεί ψευδής, απλά θεωρείται ότι πληροφορία που αναφέρεται σ' αυτήν δεν έχει προστεθεί ακόμα στη γνωσιακή βάση. Μόνο κάτι που αναφέρεται ρητά, ή προκύπτει με εφαρμογή κανόνων της λογικής πρώτης τάξης στην υπάρχουσα γνωσιακή βάση, μπορεί να θεωρηθεί αληθές. Αυτή η θεώρηση έρχεται σε αντίθεση με τη θεώρηση κλειστού κόσμου που εφαρμόζεται στην SQL και τις σχεσιακές βάσεις δεδομένων, στις οποίες μια πρόταση, που δεν μπορεί να επαληθευθεί με βάση την υπάρχουσα γνωστή πληροφορία, θεωρείται ψευδής.

Όπως αναφέρθηκε προηγουμένως, είναι δυνατόν να γίνουν ερωτήματα σε μια οντολογία για να εξαχθούν συμπεράσματα απ' αυτήν, ή να ελεγχθεί η αληθοτιμή μιας πρότασης, που αναφέρεται σε στοιχεία και συσχετισμούς που ανήκουν σ' αυτήν. Τα ερωτήματα αυτά, αφού γραφτούν σε κάποια ειδική γλώσσα, τροφοδοτούνται σε μια μηχανή ερωτημάτων, η οποία, χρησιμοποιώντας μια μηχανή συλλογισμού, εξάγει τα αποτελέσματα του ερωτήματος. Υπάρχουν πολλές διαφορετικές γλώσσες ερωτημάτων σε οντολογίες, οι οποίες διαφοροποιούνται στις δυνατότητες, την εκφραστικότητα και τη σύνταξη. Στην παρούσα διπλωματική εργασία επιλέχθηκε η γλώσσα SPARQL (**S**imple **P**rotocol **a**nd **R**DF **Q**uery **L**anguage), η οποία επισήμως συνιστάται [53] από τη W3C από τον Ιανουάριο του 2008. Η γλώσσα SPARQL [53] δανείζεται τη σύνταξή της από τη γλώσσα ερωτημάτων σε σχεσιακές βάσεις δεδομένων SQL, ωστόσο η διαφορετική λογική, με την οποία γίνεται η μοντελοποίηση στις οντολογίες, περιορίζει εκεί τις ομοιότητες των δύο γλωσσών. Τα ερωτήματα στη SPARQL εκφράζονται με τη μορφή τριπλετών, οι οποίες σε κάποιες ή σε όλες τις θέσεις τους έχουν μεταβλητές. Ένα ερώτημα μπορεί να αποτελείται από περισσότερες από μια τριπλέτες. Κατά την εκτέλεση του ερωτήματος η μηχανή λογισμού προσπαθεί να ταιριάζει τα μοτίβα, που εμφανίζονται στις τριπλέτες με αντίστοιχα μοτίβα που υπάρχουν στο γράφο, που αναπαριστά την οντολογία (pattern matching). Κάθε φορά που ανιχνεύεται στην οντολογία ένα μοτίβο, που ταιριάζει με το μοτίβο που σχηματίζουν οι τριπλέτες του ερωτήματος, οι αντίστοιχες τιμές των μεταβλητών αποτελούν ένα αποδεκτό αποτέλεσμα. Η αναζήτηση αποδεκτών αναθέσεων των μεταβλητών συνεχίζεται μέχρι να μην

ανιχνεύονται ταιριαστά μοτίβα. Η λογική με την οποία εκτελούνται τα ερωτήματα θυμίζει μηχανισμούς, που εμφανίζονται και σ' άλλες γλώσσες που κάνουν χρήση της λογικής πρώτης τάξης, όπως η prolog, ωστόσο η πιο αυστηρή και περιορισμένη σύνταξη των ερωτημάτων SPARQL καθιστούν πιο εύκολη τόσο τη συγγραφή, όσο και την αποτίμηση των ερωτημάτων χωρίς σημαντικούς περιορισμούς στην εκφραστικότητα.

5.3.2 Σχεδιασμός Οντολογίας συστήματος

Για την ανάπτυξη της οντολογίας, που χρησιμοποιήθηκε στα πλαίσια της διπλωματικής εργασίας, χρησιμοποιήθηκε ένα από τα πιο διαδεδομένα περιβάλλοντα ανάπτυξης οντολογιών, το Protégé [54]. Το συγκεκριμένο περιβάλλον ανάπτυξης δίνει στο χρήστη τη δυνατότητα να έχει πλήρη επισκόπηση της οντολογίας με γραφικό τρόπο, διευκολύνοντας την ανάπτυξη και την εύρεση λαθών σ' αυτήν. Επιπλέον, ενσωματώνει λειτουργίες μηχανής λογισμού (reasoner) για την εκτέλεση ερωτημάτων, ενώ μπορεί εύκολα να συνδεθεί και με εξωτερικές μηχανές λογισμού για να εκτελέσει ελέγχους συνέπειας και υπολογισμού παραγόμενων τύπων (inferred types). Όπως περιγράφτηκε και σε προηγούμενο κεφάλαιο, η επιθυμητή λειτουργικότητα που πρέπει να επιτελεί η προτεινόμενη οντολογία, είναι να λαμβάνει ερωτήματα που απευθύνονται σε μία βάση, όπου αποθηκεύονται προσωπικά δεδομένα, να εξετάζει σημασιολογικά το ρόλο που παίζουν τα πεδία μέσα στο ερώτημα και στη συνέχεια να ελέγχει, με βάση τους κανόνες, αν θα επιτρέψει την εκτέλεση του ερωτήματος, αν θα το τροποποιήσει, ή αν θα το απορρίψει. Με βάση την επιθυμητή λειτουργικότητα σχεδιάστηκε μια οντολογία, η οποία να είναι όσο το δυνατόν πιο επεκτάσιμη και ευέλικτη ώστε να μπορεί εύκολα να ικανοποιήσει νέες απαιτήσεις, όταν εμφανισθούν. Επιλέχθηκε να μοντελοποιηθούν μόνο οι βασικές έννοιες, που συμμετέχουν στη λειτουργία της οντολογίας με κλάσεις, ενώ οι οντότητες που ανήκουν στις βασικές κλάσεις, μοντελοποιήθηκαν με άτομα. Δηλαδή, επιλέχθηκε ένας όσο το δυνατόν επίπεδος σχεδιασμός στις κλάσεις καθώς δεν γίνεται χρήση υποκλάσεων. Η ιεραρχία και η ομαδοποίηση των διαφόρων οντοτήτων έγινε με τη χρήση ειδικών ιδιοτήτων, που ορίζονται ανάμεσα τους (containsType , isContainedBy) . Αν και η δομή αυτή δεν συναντάται συχνά κατά την ανάπτυξη οντολογιών, στη συγκεκριμένη περίπτωση επιτρέπει μεγαλύτερη ευελιξία καθώς οι οντότητες που συμμετέχουν ιεραρχούνται με διαφορετικά κριτήρια, τα οποία μπορεί να οδηγούν σε αντικρουόμενες ομαδοποιήσεις. Ενώ η διαμόρφωση μιας ιεραρχίας κλάσεων μπορεί να εκφράσει μόνο μια σχέση ιεραρχίας μεταξύ των αντικειμένων, η διαμόρφωση ιεραρχών με ιδιότητες δεν έχει αυτόν τον περιορισμό. Μπορούν να ορισθούν όσο περίπλοκες σχέσεις ιεραρχίας χρειάζεται για να επιτευχθεί η επιθυμητή λειτουργικότητα. Η ευελιξία, που μας δίνει αυτή η σχεδιαστική επιλογή, φαίνεται παρακάτω, όπου περιγράφεται η οντολογία που αναπτύχθηκε.

5.3.2.1 Οι κλάσεις της οντολογίας

Η οντολογία περιέχει τις παρακάτω κλάσεις, οι οποίες αντιστοιχούν στις βασικές έννοιες που θέλουμε να μοντελοποιήσουμε:

- **PersonalData** : Η κλάση αυτή μοντελοποιεί τα προσωπικά δεδομένα πάνω στα οποία μπορούν να εκτελεσθούν ερωτήματα. Τα άτομα, που ανήκουν σ' αυτήν την κλάση, θα πρέπει να αντιστοιχούν με τα πεδία στη Βάση Προσωπικών Δεδομένων ώστε οι κανόνες που εκφράζονται στην οντολογία να έχουν άμεση εφαρμογή.
  Παραδείγματα ατόμων: SSID (ΑΦΜ) , Name (όνομα), AdressCity (πόλη) κ.τ.λ.

- **QueryFunctionality :** Η κλάση αυτή μοντελοποιεί τη λειτουργικότητα, που μπορεί να έχει ένα προσωπικό δεδομένο μέσα σε ένα SQL ερώτημα προς τη Βάση. Για παράδειγμα: αν εμφανίζεται στα αποτελέσματα, αν χρησιμοποιείται σαν παράμετρος για να γίνει επιλογή των κατάλληλων εγγραφών, ή αν χρησιμοποιείται για ομαδοποίηση των αποτελεσμάτων.
  Παραδείγματα ατόμων: ExactValue (χρήση σαν ακριβής τιμή επιλογής εγγραφών), ResultOfQuery (επιστρεφόμενο αποτέλεσμα) κ.τ.λ.
- **Rules :** Η κλάση αυτή μοντελοποιεί τους κανόνες, που ορίζονται μεταξύ των προσωπικών δεδομένων και της λειτουργικότητας αυτών μέσα στο ερώτημα. Οι κανόνες αυτοί καθορίζουν, αν είναι επιτρεπτό, ένα συγκεκριμένο ερώτημα.
  Παραδείγματα ατόμων: NonDisclosureOfName (κανόνας που απαγορεύει την εμφάνιση του ονόματος), DisclosureOfLessDetailedData (κανόνας που καθιστά επιτρεπτή την εμφάνιση των λιγότερο αναλυτικών στοιχείων) κ.τ.λ.
- **Action :** Η κλάση αυτή μοντελοποιεί το αποτέλεσμα του ελέγχου ενός κανόνα
  Παραδείγματα ατόμων: Allow (επιτρέπεται), Deny (απαγορεύεται), CheckForLessDetailedLevel (μετασχηματισμός σε λιγότερο αναλυτικά δεδομένα)

5.3.2.2 Οι ιδιότητες μεταξύ των κλάσεων

Στην οντολογία υλοποιούνται οι παρακάτω ιδιότητες αντικειμένων, οι οποίες εκφράζουν συσχετίσεις μεταξύ διαφορετικών ατόμων από την ίδια ή από διαφορετικές κλάσεις:

- **containsType ↔ isContainedBy :** Η ιδιότητα containsType κα η αντίστροφή της isContainedBy συνδέει άτομα, που ανήκουν στην κλάση PersonalData και χρησιμοποιείται για να διαμορφωθεί μια ιεραρχική ομαδοποίηση των επιμέρους προσωπικών δεδομένων. Όπως αναφέρθηκε και παραπάνω, αυτή η ομαδοποίηση θα μπορούσε να γίνει με τη χρήση κλάσεων και υποκλάσεων, ωστόσο επιλέχθηκε η συγκεκριμένη υλοποίηση γιατί θεωρείται πιο ευέλικτη και εύκολα επεκτάσιμη.
  Αντίστροφη: isContainedBy
  Χαρακτηριστικά: Μεταβατική
  Παράδειγμα : Το άτομο Age στην ιδιότητα containsType περιέχει τα άτομα BirthDate, BirthYear, BirthRange. Το αντίστροφο συμβαίνει στα άτομα BirthDate, BirthYear, BirthRange, όπου στην ιδιότητά τους isContainedBy περιέχουν το άτομο Age.

- **hasLessDetailLevel ↔ hasMoreDetailLevel :** Η ιδιότητα hasLessDetailLevel και η αντίστροφή της hasMoreDetailLevel συνδέει άτομα, που ανήκουν στην κλάση PersonalData και χρησιμοποιείται για να ιεραρχήσει ομοειδή προσωπικά δεδομένα (δεδομένα που αναφέρονται στην ίδια έννοια), ανάλογα με το επίπεδο λεπτομέρειας με το οποίο προσδιορίζουν την έννοια αυτή.
  Αντίστροφη: hasMoreDetailLevel
  Χαρακτηριστικά: Μεταβατική
  Παράδειγμα : Τα άτομα Country, Prefecture, City, Municipality, StreetAndNumber αναφέρονται με διαφορετικά επίπεδα ακρίβειας στη διεύθυνση ενός συνδρομητή. Ισχύει η παρακάτω αλυσίδα:
  Country → Prefecture→ City → Municipality → StreetAndNumber

Όπου → σημαίνει ότι το άτομο στα αριστερά έχει στην ιδιότητά hasLessDetailLevel το άτομο δεξιά. Το αντίστροφο θα γινόταν στην περίπτωση που → αντιστοιχεί στη σχέση hasMoreDetailLevel:
StreetAndNumber → Municipality → City → Prefecture → Country

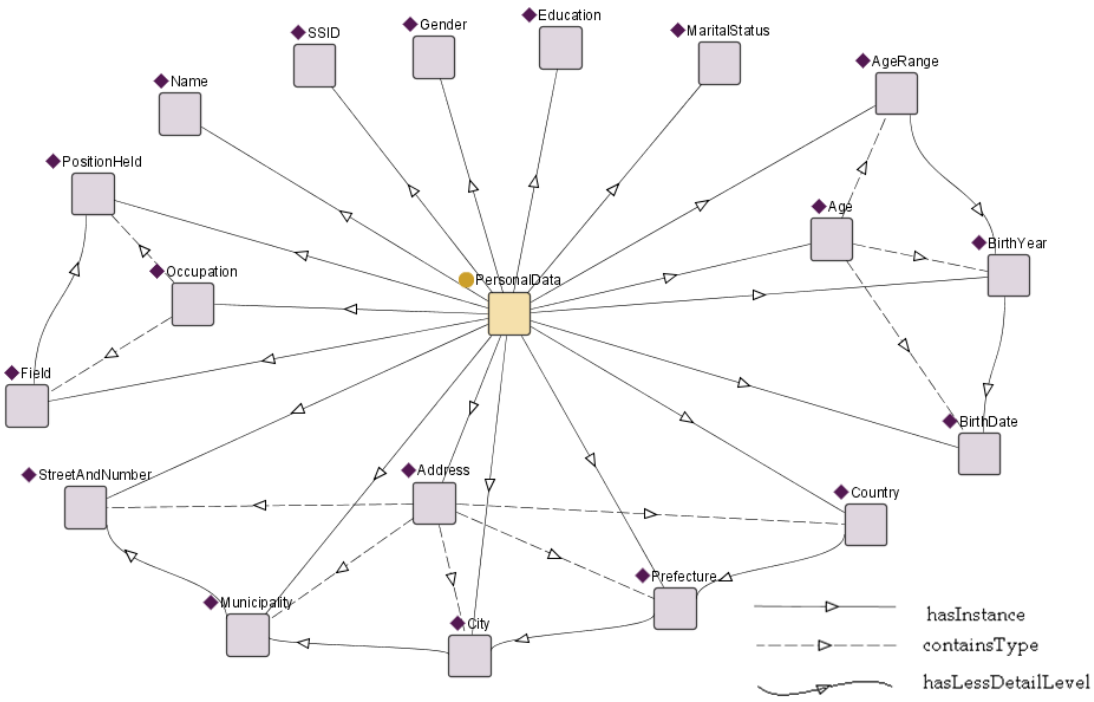
- **refersToData ↔ isRegardedByRule :** Η ιδιότητα refersToData συνδέει άτομα που ανήκουν στην κλάση Rules με άτομα που ανήκουν στην κλάση PersonalData και χρησιμοποιείται για να εκφράσει σε ποια προσωπικά δεδομένα αναφέρεται ένας συγκεκριμένος κανόνας.
  Αντίστροφη: isRegardedByRule
  Χαρακτηριστικά: Κανένα
  Παράδειγμα: Ο κανόνας που αναπαριστάται από το άτομο NonDisclosureOfName στην ιδιότητα refersToData περιέχει το άτομο Name.

- **dataUsedAs :** Η ιδιότητα dataUsedAs συνδέει άτομα που ανήκουν στην κλάση Rules με άτομα που ανήκουν στην κλάση QueryFunctionality και χρησιμοποιείται για να εκφράσει τη λειτουργικότητα μέσα στο ερώτημα, που έχει το άτομο από την κλάση προσωπικών δεδομένων, στο οποίο αναφέρεται ο κανόνας (refersToData)
  Χαρακτηριστικά: Κανένα
  Παράδειγμα: Ο κανόνας που αναπαριστάται από το άτομο DisclosureOfAverageAge στην ιδιότητα dataUsedAs περιέχει το άτομο Average.

- **hasAction:** Η ιδιότητα hasAction συνδέει άτομα που ανήκουν στην κλάση Rules με άτομα που ανήκουν στην κλάση Action και χρησιμοποιείται για να εκφράσει το αποτέλεσμα, που επιφέρει η ικανοποίηση ενός κανόνα, δηλαδή, το αν επιτρέπεται να εκτελεσθεί ένα ερώτημα, στην περίπτωση που ένα προσωπικό δεδομένο χρησιμοποιείται με συγκεκριμένο τρόπο, όπως περιγράφεται στον κανόνα.
  Χαρακτηριστικά: Συναρτησιακή (Functional)
  Παράδειγμα: Ο κανόνας που αναπαριστάται από το άτομο NonDisclosureOfSSID στην ιδιότητα hasAction περιέχει το άτομο Deny.

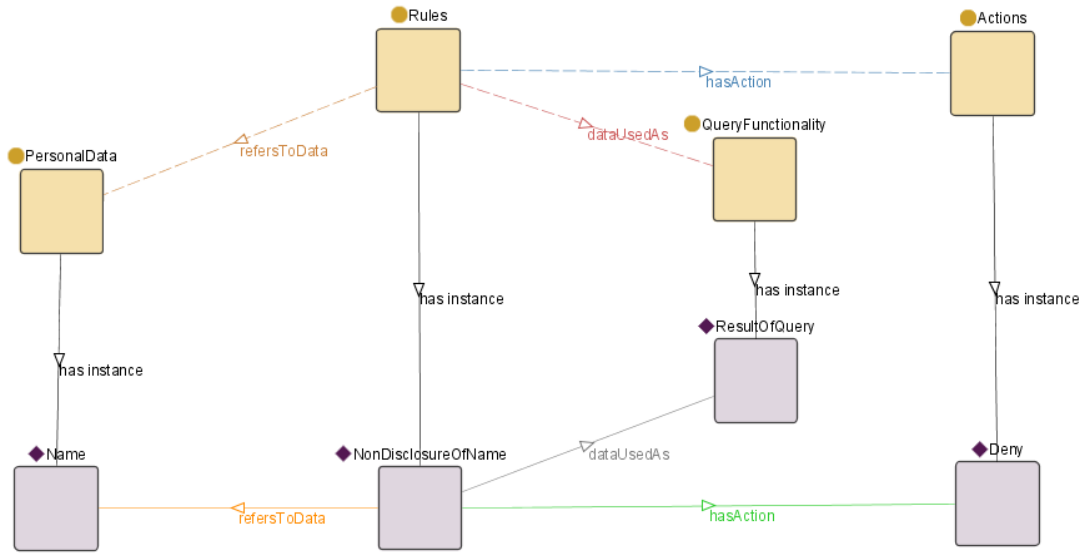
5.3.2.3 Σχηματική αναπαράσταση οντολογίας

Στην παρακάτω εικόνα παρουσιάζεται η βασική κλάση PersonalData που μοντελοποιεί τα προσωπικά δεδομένα, την ιεραρχία (σχέση containsType) τους και τη συσχέτισή τους όσον αφορά στη λεπτομέρεια των δεδομένων, που αποκαλύπτουν (hasLessDetailLevel)



Εικόνα 18: Οντολογια: Κατηγοριοποίηση Προσωπικών Δεδομένων

Στην παρακάτω εικόνα παρουσιάζεται η συσχέτιση μεταξύ των κλάσεων και των αντίστοιχων ατόμων σ' αυτές με τη χρήση ενός κανόνα ως παράδειγμα.



Εικόνα 19: Οντολογία: Μοντελοποίηση ενός κανόνα

Μέσω του παραπάνω κανόνα γίνεται η απόρριψη των ερωτημάτων, που έχουν σαν αποτέλεσμα συγκεκριμένα ονόματα συνδρομητών. Όπως βλέπουμε και στο σχήμα, ο κανόνας NonDisclosureOfName αναφέρεται (referesToData) στο προσωπικό δεδομένο όνομα (Name), όταν αυτό χρησιμοποιείται (dataUsedAs) σαν αποτέλεσμα ενός ερωτήματος (ResultOfQuery). Με αντίστοιχους κανόνες μπορούν να ορισθούν συγκεκριμένες συνθήκες

υπό τις οποίες επιτρέπεται ή αποτρέπεται η εκτέλεση ερωτημάτων. Η πλήρης απαρίθμηση περιπτώσεων λειτουργικότητας των προσωπικών δεδομένων στα ερωτήματα προς τη Βάση και κανόνων εμφάνισης αυτών είναι έξω από τα πλαίσια της παρούσας διπλωματικής, καθώς απαιτείται ανάλυση της νομοθεσίας και συνεργασία με ειδικούς στον τομέα αυτόν. Παρακάτω παρατίθενται, ενδεικτικά, πιθανοί κανόνες που θα μπορούσαν να εφαρμοσθούν, αφού ελεγχθούν με βάση τη νομοθεσία:

- NonDisclosureOfName:
  refersToData: Name
  dataUsedAs: ResultOfQuery
  hasAction: Deny

Περιγραφή: Αποτρέπει την εμφάνιση ονομάτων στα αποτελέσματα ενός ερωτήματος

- DisclosureOfLessDetailedData:
  refersToData: AgeRange, Occupation Field, City, Gender
  dataUsedAs: ResultOfQuery
  hasAction: Allow

Περιγραφή: Επιτρέπει την εμφάνιση των προσωπικών δεδομένων με το μικρότερο βαθμό λεπτομέρειας στα αποτελέσματα ενός ερωτήματος. Κανόνες σ' αυτήν τη μορφή μπορούν με κατάλληλα ερωτήματα SPARQL να συνδυασθούν με τις ιδιότητες hasLessDetailLevel και hasMoreDetailLevel και να εφαρμοσθούν σε προσωπικά δεδομένα, που δεν αναφέρονται ρητά στο πεδίο refersToData, αλλά συνδέονται με δεδομένα απ'αυτό, μέσω των προαναφερθέντων σχέσεων. Όπως παρουσιάζεται στο επόμενο κεφάλαιο της υλοποίησης, δίνεται η δυνατότητα, μέσω ενός κατάλληλου SPARQL ερωτήματος, να εκτελεσθεί έλεγχος για το αν κάποιο δεδομένο (π.χ Prefecture) παρέχει λιγότερη λεπτομέρεια (hasLessDetailLevel) από κάποιο δεδομένο στο πεδίο refersToData του κανόνα. Σ' αυτήν την περίπτωση η εμφάνιση του δεδομένου αυτού θα είναι επιτρεπτή, ακόμα και αν δεν υπάρχει κανόνας που ρητά το επιτρέπει αυτό. Μ' αυτό το παράδειγμα γίνεται αντιληπτή η ευελιξία που παρέχει η χρήση της οντολογίας για σημασιολογική ερμηνεία εννοιών, που σε άλλη περίπτωση θα αντιμετωπίζονταν ως απλοί τύποι δεδομένων (συμβολοσειρές).

- DisclosureGroupByMunicipality:
  refersToData: Municipality
  dataUsedAs: GroupBy
  hasAction: Allow

Περιγραφή: Επιτρέπει την εμφάνιση ερωτημάτων που χρησιμοποιούν ομαδοποίηση με βάση το δήμο. Τέτοιας μορφής ερωτήματα μπορούν να εμφανίσουν χρήσιμα στατιστικά δεδομένα, χωρίς να αποκαλύπτονται προσωπικά στοιχεία συγκεκριμένων χρηστών.

5.3.3 Το υποσύστημα πρόσβασης στα προσωπικά δεδομένα

Με βάση την οντολογία και το μηχανισμό κανόνων που περιγράφτηκε παραπάνω, θα παρουσιασθεί η διαδικασία που επιτελείται στο υποσύστημα πρόσβασης στα προσωπικά

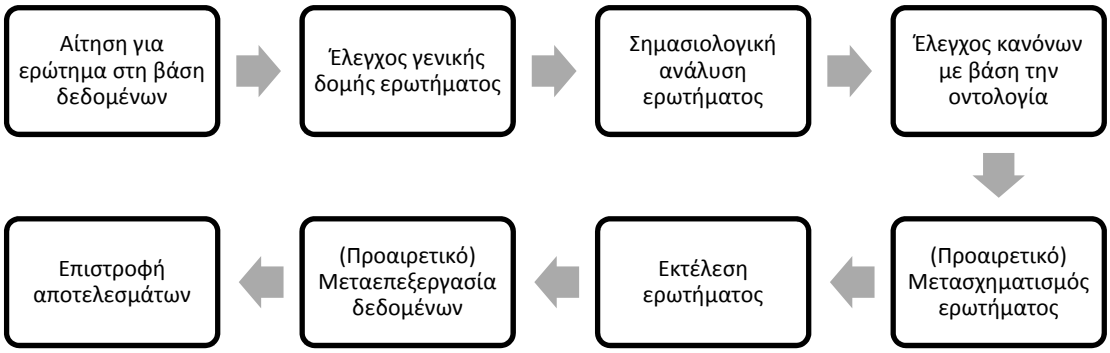
δεδομένα μετά την αίτηση προς το Δ.Π.Ι. για την εκτέλεση ενός ερωτήματος SQL στη Βάση Προσωπικών Δεδομένων.

Αρχικά το εισερχόμενο ερώτημα ελέγχεται για το αν πληροί ορισμένους γενικούς κανόνες, που αφορούν τη μορφή του. Τέτοιοι κανόνες, για παράδειγμα, μπορεί να απαγορεύουν την αποκάλυψη μεγάλου αριθμού προσωπικών δεδομένων σ' ένα ερώτημα. (Πέντε π.χ. διαφορετικά πεδία, τα οποία μπορούν σε ορισμένες περιπτώσεις να ταυτοποιήσουν πλήρως κάποιον χρήστη ή την εκτέλεση ερωτημάτων με δομή που δεν έχει προβλεφθεί κατά τη σχεδίαση της οντολογίας). Αυτός ο πρωτοβάθμιος έλεγχος κάνει το επόμενο βήμα της σημασιολογικής ανάλυσης του ερωτήματος ευκολότερα υλοποιήσιμο, ενώ ταυτόχρονα περιορίζει τον κίνδυνο διαρροής προσωπικών δεδομένων από ερωτήματα με περίπλοκη δομή, που δεν έχουν προβλεφθεί κατά το σχεδιασμό.

Το επόμενο στάδιο είναι η ανάλυση της μορφής του ερωτήματος και η εξαγωγή των προσωπικών δεδομένων που συμμετέχουν σ' αυτό μαζί με τη λειτουργία τους στο ερώτημα. Σ' αυτό το στάδιο αρχικά εκτελείται συντακτική ανάλυση (parsing) ώστε να εξαχθεί η γενική μορφή και λειτουργία του ερωτήματος. Στη συνέχεια, εξάγονται τα προσωπικά δεδομένα που συμμετέχουν και ο ρόλος τους στο ερώτημα, δηλαδή το ερώτημα «διασπάται» στα επιμέρους δεδομένα από το οποίο «δομείται». Μ' αυτόν τον τρόπο εκτελείται μια μορφή σημασιολογικής ανάλυσης στο ερώτημα, τα αποτελέσματα της οποίας, (ζεύγη προσωπικών δεδομένων με την αντίστοιχη λειτουργικότητά τους), τροφοδοτούνται στο επόμενο στάδιο. Σ' αυτό το σημείο σημειώνεται ότι η υλοποίηση των παραπάνω μηχανισμών είναι εκτός των πλαισίων της παρούσας διπλωματικής και ανήκει στον ερευνητικό τομέα της σημασιολογικής επεξεργασίας και βελτιστοποίησης ερωτημάτων (Semantic query processing and optimisation). Αυτό ωστόσο δεν επηρεάζει τη λειτουργικότητα της σχεδιαζόμενης οντολογίας και των επόμενων σταδίων της διαδικασίας.

Τα αποτελέσματα της σημασιολογικής ανάλυσης του προηγούμενου σταδίου, δηλαδή τα ζεύγη τιμών (προσωπικό δεδομένο, λειτουργία στο ερώτημα) εφαρμόζονται σε κατάλληλα ερωτήματα SPARQL, τα οποία εκτελούνται πάνω στην οντολογία και ελέγχουν αν το αρχικό ερώτημα SQL, με βάση τους υπάρχοντες κανόνες, μπορεί να εκτελεσθεί. Το ερώτημα τελικά εκτελείται χωρίς τροποποίηση, μόνο στην περίπτωση που οι κανόνες το επιτρέπουν για όλα τα ζεύγη που αναφέρονται σ' αυτό. Σε περίπτωση που κάποιος κανόνας δεν επιτρέπει την εκτέλεση του ερωτήματος, γίνεται έλεγχος για το αν το δεδομένο, το οποίο προκαλεί το πρόβλημα, έχει συσχετιζόμενα άτομα που αποκαλύπτουν λιγότερη πληροφορία. Ο έλεγχος αυτός υλοποιείται μέσω της σχέσης hasLessDetailLevel μ' ένα κατάλληλο SPARQL ερώτημα. Αν βρεθούν τέτοια άτομα-προσωπικά δεδομένα, ο Δ.Π.Ι δίνει τη δυνατότητα στο δράστη, που εκτέλεσε το αρχικό SQL ερώτημα, να αποδεχθεί πιθανή τροποποίησή του, η οποία είναι επιτρεπτή σύμφωνα με τους κανόνες της νομοθεσίας. Αν η τροποποίηση δεν γίνει αποδεκτή, το ερώτημα απορρίπτεται. Το ίδιο συμβαίνει σε περίπτωση που δεδομένο, που προκαλεί την απόρριψη του ερωτήματος, δεν έχει συσχετιζόμενα μ' αυτό άτομα, που αποκαλύπτουν λιγότερη πληροφορία. Σε περίπτωση που το ερώτημα είναι επιτρεπτό, μετά την εκτέλεσή του, προαιρετικά μπορεί να υπάρχει ένα ακόμα στάδιο, το οποίο εκτελεί άλλες μεθόδους προστασίας των προσωπικών δεδομένων, που βασίζονται στη μετα-επεξεργασία των δεδομένων προς δημοσίευση (k-Anonymity, l-diversity, m-Invariance). Το στάδιο αυτό αποτελεί μια επιπλέον δικλείδα ασφαλείας για την προστασία της ταυτότητας του χρήστη, αν και στις περισσότερες περιπτώσεις ο μηχανισμός της οντολογίας κρίνεται από μονός του επαρκής.

Στο παρακάτω σχήμα παρουσιάζεται συνοπτικά η διαδικασία που περιγράφτηκε παραπάνω.



Εικόνα 20: Διάγραμμα Ροής υποσυστήματος προστατευμένης πρόσβασης στα προσωπικά δεδομένα

6

Υλοποίηση

Στα πλαίσια της παρούσας διπλωματικής εργασίας υλοποιήθηκαν δύο υποσυστήματα του συστήματος τηλεφωνίας με παροχή εγγυήσεων για την προστασία της ιδιωτικότητας. Συγκεκριμένα:

- Με βάση τη σχεδίαση του λογισμικού, που προτάθηκε στο προηγούμενο κεφάλαιο, υλοποιήθηκε ένας Δ.Π.Ι., ο οποίος εφαρμόζει την προτεινόμενη αρχιτεκτονική και τις απαιτήσεις συστήματος στην περίπτωση των υπηρεσιών εγκαθίδρυσης συνόδων SIP για την προστασία των ονομάτων SIP,
- Για να δειχθεί η λειτουργία της οντολογίας, που σχεδιάστηκε στο προηγούμενο κεφάλαιο για τον έλεγχο των ερωτημάτων προς τη Βάση Προσωπικών Δεδομένων και να παρουσιασθεί η λειτουργία του αντίστοιχου σταδίου της διαδικασίας επεξεργασίας των ερωτημάτων, υλοποιήθηκε ένα απλό πρόγραμμα σε JAVA, το οποίο αξιοποιεί τη βιβλιοθήκη Jena, μια βιβλιοθήκη εξαγωγής συμπερασμάτων και σημασιολογικής επεξεργασίας, που υποστηρίζει τη γλώσσα περιγραφής οντολογιών OWL.

6.1 Λεπτομέρειες υλοποίησης

6.1.1 Υλοποίηση Διακομιστή Προστασίας Ιδιωτικότητας

Ο Διακομιστής Προστασίας Ιδιωτικότητας, ως μια δομική μονάδα SIP, επιλέχθηκε να βασισθεί σε μια ήδη υπάρχουσα λύση ανοικτού κώδικα και να μην αναπτυχθεί εκ νέου, αφού ο στόχος της παρούσας διπλωματικής ήταν η υλοποίηση της λειτουργικότητας προστασίας της ιδιωτικότητας και όχι η εκ νέου ανάπτυξη ενός διακομιστή SIP. Η αναζήτηση στο διαδίκτυο κατέδειξε ότι οι περισσότερες λύσεις ανοικτού κώδικα είναι υλοποιημένες στη

γλώσσα C κάτι που δεν ικανοποιεί τις απαιτήσεις του συστήματος για υλοποίηση στην πλατφόρμα της Java. Το μόνο κατάλληλο έργο που βρέθηκε είναι το JAIN-SIP Proxy Server, το οποίο χρησιμοποιείται και για εκπαιδευτικούς σκοπούς στο μάθημα της «Τεχνολογίας Λογισμικού» της Σχολής Η.Μ.Μ.Υ. Ε.Μ.Π. [43]. Παράλληλα μ' αυτό επιλέχθηκε και ως πρόγραμμα πελάτη το Sip-Communicator σε παλιότερη έκδοση, που επίσης χρησιμοποιείται στο μάθημα της «Τεχνολογίας Λογισμικού». Και τα δύο προγράμματα χρησιμοποιούν το JAIN-SIP API για την υλοποίηση λειτουργιών του SIP με αποτέλεσμα να έχουν κοινά σημεία που βοήθησαν στην επέκταση του συστήματος. Δεν επιλέχθηκε η χρήση νεώτερης και πιο σύγχρονης έκδοσης του Sip-Communicator, παρ' όλο που αυτή είναι η κυρίαρχη εφαρμογή πελάτη διαδικτυακής τηλεφωνίας [55], λόγω ασυμβατότητας στην έκδοση του χρησιμοποιούμενου JAIN-SIP API σε σχέση με το πρόγραμμα διακομιστή (1.2, 1.1 αντίστοιχα) και λόγω του γεγονότος ότι το Sip-Communicator υποστηρίζει στην παρούσα μορφή και άλλα πρωτόκολλα, όπως το Jabber και το Microsoft MSN, κάτι που έχει αυξήσει την πολυπλοκότητα του κώδικα, καθιστώντας την επέκταση του αδύνατη στα στενά χρονικά περιθώρια μιας διπλωματικής εργασίας.

Μετά την απαραίτητη χρονική περίοδο που απαιτήθηκε για την κατανόηση της δομής των δύο εφαρμογών, ο κώδικας του προγράμματος JAIN-SIP-PROXY SERVER αναθεωρήθηκε ριζικά με αποτέλεσμα να παραμείνουν μόνο οι λειτουργίες που τον καθιστούσαν απλά μια δομική μονάδα λήψης και επαναπροώθησης πακέτων SIP. Στη συνέχεια, προστέθηκε το πακέτο «privacyserver», το οποίο και περιέχει τις κλάσεις που υλοποιούν την επιθυμητή λειτουργικότητα, που περιγράφτηκε σε προηγούμενα κεφάλαια και σχεδιάστηκε στο κεφάλαιο 5. Λόγω των περιορισμένων δυνατοτήτων των δύο προγραμμάτων βάσης [44],[45], που χρησιμοποιήθηκαν, στάθηκε αδύνατη η υλοποίηση στο Δ.Π.Ι. των λειτουργιών για την κάλυψη των απαιτήσεων του συστήματος, όσον αφορά στις υπηρεσίες παρουσίας και άμεσων μηνυμάτων, αφού η βασική λειτουργικότητα τους δεν υποστηριζόταν τόσο από το πρόγραμμα διακομιστή, όσο και από το πρόγραμμα πελάτη. Επίσης, στάθηκε αδύνατη η υλοποίηση του σχεδιασμού χρήσης του δικτύου TOR στα πλαίσια της παρούσας διπλωματικής, αφού στάθηκε αδύνατος ο εντοπισμός του κώδικα του JAIN-SIP API v1.1. Επίσης, λόγω της αδυναμίας του JAIN-SIP να υποστηρίξει την επικεφαλίδα «Privacy», ο Δ.Π.Ι. υλοποιεί μια προεπιλεγμένη πολιτική προστασίας ιδιωτικότητας, προστατεύοντας τόσο την ταυτότητα του αποστολέα, όσο και αυτή του παραλήπτη από το ενδιάμεσο δίκτυο, δηλαδή από την εταιρεία παροχής υπηρεσίας. Επίσης, θεωρήθηκε ότι ο κάθε χρήστης του συστήματος εμπιστεύεται τον άλλο, οπότε δεν υπάρχει ανάγκη για υλοποίηση του Δ.Π.Ι. ως B2BUA. Τέλος, στα πλαίσια της παρούσας διπλωματικής δεν θεωρήθηκε σκόπιμη η χρήση μιας βάσης δεδομένων για την αποθήκευση των πληροφοριών, που ορίσθηκαν κατά τη σχεδίαση του συστήματος. Έτσι δημιουργήθηκε απλά μια συλλογή (HashTable) κατάλληλων αντικειμένων ώστε να υλοποιηθεί η κατάλληλη λειτουργικότητα.

Συγκεκριμένα υλοποιήθηκαν οι παρακάτω λειτουργίες:

- processRequest: Διαχωρισμός λειτουργιών επεξεργασίας μηνύματος-αίτησης ανάλογα με την μέθοδο του μηνύματος και κλήση κατάλληλων μεθόδων.
- processResponse: Στην προτεινόμενη αρχιτεκτονική δεν χρειάζεται ο διακομιστής να επεξεργαστεί το μήνυμα-απάντηση.
- applyCalleePolicy: Αντικατάσταση SIP URI AOR παραλήπτη με το τρέχον ψευδώνυμο του.

- applyCallerPolicy: Αφαίρεση προαιρετικών κεφαλίδων μηνύματος, που μπορεί να αποκαλύψουν προσωπικά δεδομένα και εφαρμογή προστασίας ιδιωτικότητας επιπέδου user.
- applyUserPrivacy: Εφαρμογή προστασίας επιπέδου user, όπως αυτή ορίζεται στο REF 3323.
- removeOptionalPrivacyUnawareHeaders: Αφαίρεση προαιρετικών κεφαλίδων μηνύματος, που μπορεί να αποκαλύψουν προσωπικά δεδομένα
- createUniqueTemporaryPseydonym: Χρήση της γεννήτριας τυχαίων αλφαριθμητικών, που παρέχει το JAIN-SIP API για δημιουργία τυχαίων επικεφαλίδων «Call-Id»

Ένα τελευταίο πρόβλημα, που ανέκυψε, είναι η αδυναμία του JAIN-SIP να μετατρέψει τα στοιχεία ενός εγκαθιδρυμένου διαλόγου σε κάποιο χρονικό σημείο μετά την εγκαθίδρυση του. Αυτό σημαίνει ότι ο Αποστολέας θα έχει εσφαλμένη αντίληψη για τα δύο πρόσωπα, που πραγματικά συνομιλούν στο διάλογο, (θα νομίζει ότι επικοινωνούν «andreas»-«errikos», ενώ για το σύστημα θα είναι «anonymous»–«021as0421fdsad21ws123»), αφού για λόγους απόδοσης μπορεί η προστασία της ιδιωτικότητας να εφαρμόζεται απευθείας στο μηχάνημα του πελάτη μετά την εγκαθίδρυση της συνόδου. Γι αυτό το λόγο θα πρέπει να υπάρξει υποστήριξη από το API για την αλλαγή των στοιχείων ενός διαλόγου. Στην παρούσα υλοποίηση το πρόβλημα παρακάμφθηκε αποθηκεύοντας στο μηχάνημα του χρήστη ακριβώς τις επικεφαλίδες «From» και «To», οι οποίες θα πρέπει να χρησιμοποιούνται σε μελλοντικά μηνύματα στα πλαίσια του ίδιου διαλόγου.

6.1.2 Υλοποίηση Οντολογίας

Για να αξιοποιηθεί η οντολογία, που σχεδιάστηκε στο προηγούμενο κεφάλαιο, για τον έλεγχο των ερωτημάτων προς τη Βάση Προσωπικών Δεδομένων και να παρουσιασθεί η λειτουργία του αντίστοιχου σταδίου της διαδικασίας επεξεργασίας των ερωτημάτων, υλοποιήθηκε ένα πρόγραμμα σε JAVA, το οποίο αξιοποιεί τη βιβλιοθήκη Jena, μια βιβλιοθήκη εξαγωγής συμπερασμάτων και σημασιολογικής επεξεργασίας, που υποστηρίζει τη γλώσσα περιγραφής οντολογιών OWL. Η συγκεκριμένη βιβλιοθήκη δίνει τη δυνατότητα να εκτελεσθούν ερωτήματα SPARQL στην οντολογία, που σχεδιάστηκε, καθώς ενσωματώνει δικιά της μηχανή λογισμού.

Όπως αναφέρθηκε και παραπάνω θα θεωρηθεί δεδομένη η σημασιολογική ανάλυση του ερωτήματος SQL, ότι δηλαδή έχουν εξαχθεί τα προσωπικά δεδομένα και η λειτουργία τους σ' αυτό. Η διαδικασία του ελέγχου, για το αν ένα ερώτημα είναι επιτρεπτό και η εύρεση πιθανών μετασχηματισμών του, γίνεται με τη χρήση SPARQL ερωτημάτων πάνω στην οντολογία. Τα ερωτήματα SPARQL εκτελούνται με τη βοήθεια του προγράμματος JAVA-Jena, που αναφέρθηκε. Το συγκεκριμένο πρόγραμμα εφαρμόζει και τις διαφορετικές ροές εκτέλεσης ερωτημάτων, ανάλογα με τα διαφορετικά αποτελέσματα των ερωτημάτων στην οντολογία και τις επιλογές του χρήστη. Σε περίπτωση που το πρόγραμμα εφαρμοσθεί σε πραγματικό σύστημα, η μέθοδος που υλοποιεί την επιθυμητή λειτουργικότητα θα δημοσιευθεί με τη μορφή ενός web service σε JAVA, μέσω του οποίου θα υλοποιηθεί η υπηρεσία ασφαλούς πρόσβασης στην προστατευμένη βάση προσωπικών δεδομένων. Η ροή εκτέλεσης, που αναφέρθηκε, παρουσιάζεται στο επόμενο κεφάλαιο ώστε να γίνει αντιληπτή η λογική της λειτουργίας του μηχανισμού προστατευμένης πρόσβασης. Τα εισερχόμενα

ερωτήματα SQL, που επιλέχθηκαν για τα παραδείγματα, είναι στοιχειώδη και έχουν σαν σκοπό να βοηθήσουν ακριβώς την περιγραφή της λογικής και γι αυτό το λόγο στερούνται πρακτικής χρησιμότητας. Ωστόσο με τη συμπλήρωση διαφορετικών ρόλων στο SQL ερώτημα στην οντολογία (στην κλάση QueryFunctonality) και τη συγγραφή κατάλληλων κανόνων, η ίδια διαδικασία μπορεί να γενικευθεί σε όσο περίπλοκα ερωτήματα χρειάζεται η εφαρμογή. Η ευελιξία της οντολογίας έγκειται στο γεγονός ότι οι μόνες τροποποιήσεις, που απαιτούνται να γίνουν, είναι στο σημασιολογικό αναλυτή και την οντολογία. Το πρόγραμμα JAVA με τα SPARQL ερωτήματα, που αποτελούν και τον πυρήνα της διαδικασίας, μπορούν να μείνουν αμετάβλητα.

6.2 Πλατφόρμες και προγραμματιστικά εργαλεία

6.2.1 Υλοποίηση Διακομιστή Προστασίας Ιδιωτικότητας

Για την ανάπτυξη του συστήματος του Δ.Π.Ι. χρησιμοποιήθηκε το προγραμματιστικό περιβάλλον του Eclipse με χρήση του Subeclipse για την ενσωμάτωση των λειτουργιών του Subversion, το οποίο αποτελεί ένα σύστημα ελέγχου εκδόσεων κώδικα (versioning system), σ' αυτό. Τα προγράμματα βάσης, που επιλέχθηκαν προήλθαν, από την ιστοσελίδα του μαθήματος της «Τεχνολογίας Λογισμικού» της περιόδου 2007-2008 και αποτελούν παλιότερες εκδόσεις σύγχρονων προγραμμάτων υλοποίησης διαδικτυακής τηλεφωνίας. Τα προγράμματα εγκαταστάθηκαν με βάση τις οδηγίες εγκατάστασης που αναφέρονταν στο συνοδευτικό φυλλάδιο του μαθήματος της «Τεχνολογίας Λογισμικού» σε διαφορετικά μηχανήματα, ώστε να είναι δυνατή η δημιουργία ενός περιβάλλοντος ανάπτυξης που να ικανοποιεί τις απαιτήσεις δικτύωσης, που επιβάλει η προτεινόμενη αρχιτεκτονική.

6.2.2 Υλοποίηση Οντολογίας

Για την ανάπτυξη της οντολογίας χρησιμοποιήθηκε το περιβάλλον Protégé, το οποίο είναι το πιο διαδεδομένο περιβάλλον ανάπτυξης οντολογιών ανοιχτού κώδικα. Πέρα από τις ενσωματωμένες λειτουργίες επισκόπησης και επεξεργασίας της οντολογίας, μπορούν να ενσωματωθούν επιπλέον πρόσθετα (plugins), που επεκτείνουν τη λειτουργικότητά του (π.χ. το πρόσθετο jambalaya, το οποίο κάνει αναλυτική απεικόνιση των οντοτήτων και των σχέσεων της οντολογίας σε διαδραστικά γραφικά). Το Protégé ενσωματώνει επίσης και μηχανή λογισμού, ικανή να εκτελέσει SPARQL ερωτήματα απευθείας μέσα από το περιβάλλον ανάπτυξης. Ωστόσο η συγκεκριμένη μηχανή λογισμού δεν έδινε σωστά αποτελέσματα, καθώς αντιμετώπιζε προβλήματα με τις μεταβατικές (transitive) ιδιότητες. Για αυτόν το λόγο επιλέξαμε να χρησιμοποιήσουμε εξωτερικές μηχανές λογισμού.

Για τον έλεγχο της σημασιολογικής ακεραιότητας και του υπολογισμού παραγόμενων τύπων (inferred types) το Protégé συνδέθηκε με την εξωτερική μηχανή λογισμού FaCT++, η οποία, όπως ήταν αναμενόμενο, δεν βρήκε κάποια ασυνέπεια στον ορισμό της οντολογίας. Για την εκτέλεση των SPARQL ερωτημάτων χρησιμοποιήθηκε η μηχανή λογισμού που ενσωμάτωνε η βιβλιοθήκη υποστήριξης οντολογιών, που χρησιμοποιήθηκε, η βιβλιοθήκη Jena. Η συγκεκριμένη μηχανή λογισμού ήταν η μόνη που

βρέθηκε να επιστρέφει σωστά αποτελέσματα σε SPARQL ερωτήματα που κάνουν χρήση μεταβατικών ιδιοτήτων, και για αυτό επιλέχθηκε από τις υπόλοιπες για τη συγκεκριμένη εφαρμογή. Το πρόγραμμα σε JAVA, που αναπτύχθηκε για την παρουσίαση της λειτουργίας της οντολογίας, αξιοποιούσε τους μηχανισμούς, που προσφέρει η βιβλιοθήκη Jena για τη φόρτωση της οντολογίας, την εκτέλεση SPARQL ερωτημάτων και τον έλεγχο των αποτελεσμάτων στο αυτοματοποιημένο περιβάλλον ενός ολοκληρωμένου προγράμματος. Όπως και με τα υπόλοιπα τμήματα του συστήματος διαδικτυακής τηλεφωνίας που αναπτύχθηκαν σε JAVA, η δημιουργία του προγράμματος έγινε στο περιβάλλον Eclipse.

7

Έλεγχος

Για να παρουσιάσουμε την λειτουργία των δύο υλοποιημένων υποσυστημάτων επιλέχθηκαν οι τοπολογίες και τα παραδείγματα που ακολουθούν.

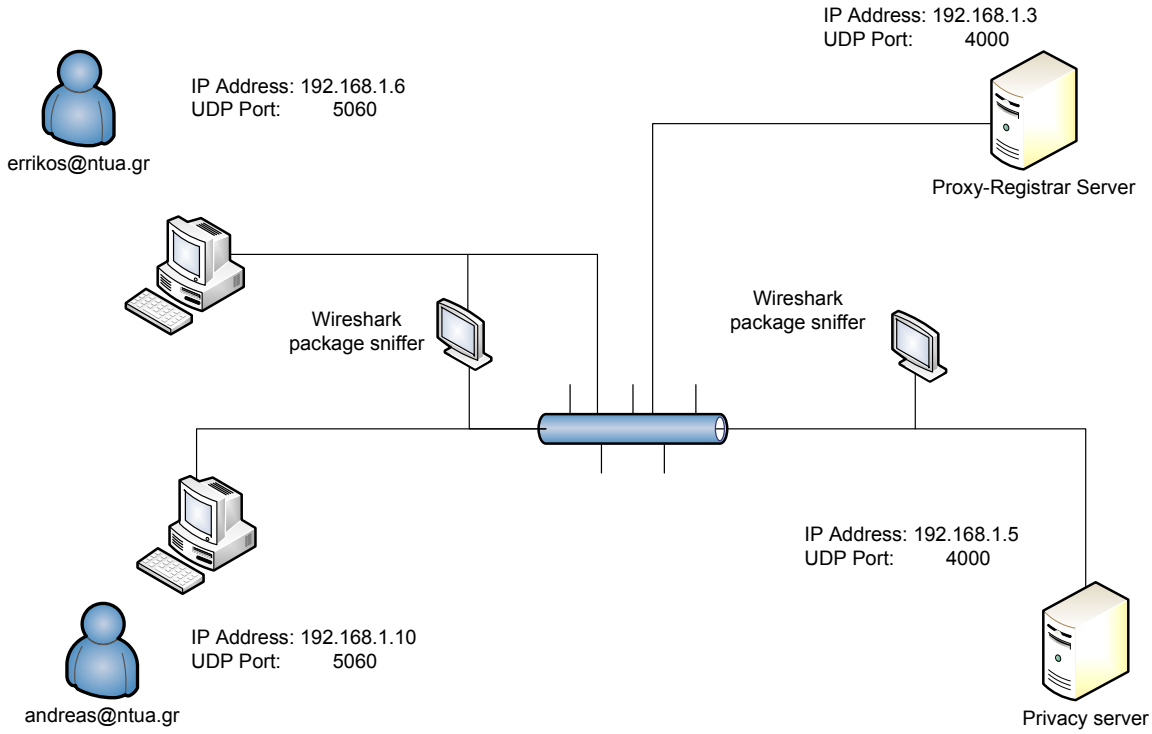
7.1 Έλεγχος λειτουργίας Δ.Π.Ι.

7.1.1 Μεθοδολογία ελέγχου

Για να παρουσιασθεί η υλοποίηση του συστήματος θα χρησιμοποιηθεί ένα τυπικό σενάριο λειτουργίας του συστήματος με εγκαθίδρυση μια τηλεφωνικής συνόδου μεταξύ δύο χρηστών «andreas» - «errikos». Το σενάριο λειτουργίας του συστήματος, που θα παρουσιαστεί, έχει ως εξής:

- Ο χρήστης «andreas» εγγράφεται στο σύστημα.
- Ο χρήστης «andreas» ζητά επικοινωνία με το χρήστη «errikos»
- Ο χρήστης «errikos» εγγράφεται στο σύστημα.
- Ο χρήστης «andreas» ζητά επικοινωνία με το χρήστη «errikos».
- Εγκαθίδρυση συνόδου.
- Ο χρήστης «errikos» τερματίζει την επικοινωνία.

Η δικτυακή τοπολογία του συστήματος έχει ως εξής:



Εικόνα 21: Δικτυακή τοπολογία σεναρίου λειτουργίας πειραματικού συστήματος

Όπως παρατηρούμε και οι δύο χρήστες του συστήματος ανήκουν στην ίδια διαχειριστική οντότητα, αφού έχουν κοινό πάροχο υπηρεσιών SIP. Για να δούμε τα μηνύματα, που μεταφέρονται στο δίκτυο, εγκαταστήσαμε δύο ανιχνευτές πακέτων (packet sniffers) . Το παράδειγμα υλοποιήθηκε με τη χρήση πρωτοκόλλου μεταφοράς UDP ώστε να μπορούμε να δούμε το περιεχόμενο των μηνυμάτων που μεταφέρονται στο δίκτυο, αν και στο κανονικό σύστημα θα έπρεπε όλες οι συνδέσεις να χρησιμοποιούν το πρωτόκολλο TLS. Επίσης δεν έγινε χρήση συστήματος πιστοποίησης, αφού δεν υπήρχε η δυνατότητα για τη χρήση ψηφιακών πιστοποιητικών. Το σύστημα digest θεωρείται πολύ αδύναμο για ένα πραγματικό σύστημα, οπότε δεν θεωρήθηκε σκόπιμη η χρήση του και η ενσωμάτωση του στο πειραματικό σύστημα. Επίσης, στο σενάριο λειτουργίας, που παρουσιάζεται παρακάτω, θεωρείται δεδομένη η προστασία των διευθύνσεων IP.

7.1.1.1 Παραμετροποίηση των προγραμμάτων

Τα προγράμματα που χρησιμοποιούνται επιτρέπουν την παραμετροποίηση τους για τη σωστή λειτουργία τους. Αυτό επιτυγχάνεται με τη συγγραφή ενός configuration XML, το οποίο περιέχει όλες τις απαραίτητες πληροφορίες και κατά τη φάση της αρχικοποίησης του προγράμματος μετατρέπεται (μέσω parsing) στο κατάλληλο αντικείμενο παραμέτρων. Περισσότερες πληροφορίες για την παραμετροποίηση και τη λειτουργία των προγραμμάτων μπορούν να βρεθούν στο συμπληρωματικό υλικό, που συνοδεύει τα προγράμματα και υπάρχει στις αναφορές [43].

Για τις τέσσερις λοιπόν δομικές μονάδες, που χρησιμοποιούνται, έχουμε την παρακάτω παραμετροποίηση:

- **Ενδιάμεσος Διακομιστής-Διακομιστής καταχώρισης Χρηστών και Δ.Π.Ι.**

```
<!--local IP address of server and server parameters -->
<SIP_STACK
stack_name="nist-proxy"
stack_IP_address="192.168.1.3" - "192.168.1.5"
router_path="gov.nist.sip.proxy.router.ProxyRouter"
max_connections="20"
max_server_transactions="20"
thread_pool_size="20"
    >

<LISTENING_POINT port="4000" transport="udp" /> <!--listening port
proxy for udp -->
<LISTENING_POINT port="4000" transport="tcp" /> <!--listening port
proxy for tcp -->
<DOMAIN domain="anonymous.invalid" />
<DOMAIN domain="ntua.gr" />
</SIP_STACK>
```

Ορίσθηκε η διεύθυνση 192.168.1.3 (192.168.1.5 για το Δ.Π.Ι.) για την SipStack και η δημιουργία δύο ListeningPoints στην πόρτα 4000, ένα για χρήση του πρωτοκόλλου UDP και ένα για χρήση του TCP. Ταυτόχρονα, ορίσθηκε η διαχειριστική οντότητα που διαχειρίζεται ο συγκεκριμένος διακομιστής να είναι η ntua.gr, ενώ και τα ονόματα που περιέχουν την εικονική διαχειριστική οντότητα anonymous.invalid δεν θα πρέπει να απορρίπτονται, αφού μπορεί να προέρχονται από μια υπηρεσία προστασίας ιδιωτικότητας.

- **Προγράμματα Πελάτη**

```
      <communicator>
          <FIRST_LAUNCH value="false"/>
          <ENABLE_SIMPLE value="false"/>
          <media>
              <PREFERRED_AUDIO_ENCODING value="0"/>
              <PREFERRED_VIDEO_ENCODING value="26"/>
            <MEDIA_SOURCE value=""/>
            <MEDIA_BUFFER_LENGTH value="100"/>
            <IP_ADDRESS value=""/>
<!-- IP used for rtf channel -->
            <AUDIO_PORT value="22224"/>
<!-- Media Port used for video rtf -->
            <VIDEO_PORT value="22222"/>
<!-- Media Port used for audio rtf -->
        </media>
        <sip>
  <PUBLIC_ADDRESS value="sip:andreas@ntua.gr"-"sip:errikos@ntua.gr"/>
<!-- The SIP URI AOR used for others to call me -->
            <TRANSPORT value=""/>
            <REGISTRAR_ADDRESS value="192.168.1.3:5000"/>
<!-- IP and port of registrar server to be used-->
            <USER_NAME value="andreas"-"errikos" />
<!-- USERNAME of user -->
            <STACK_PATH value="gov.nist"/>
            <PREFERRED_LOCAL_PORT value=""/>
```

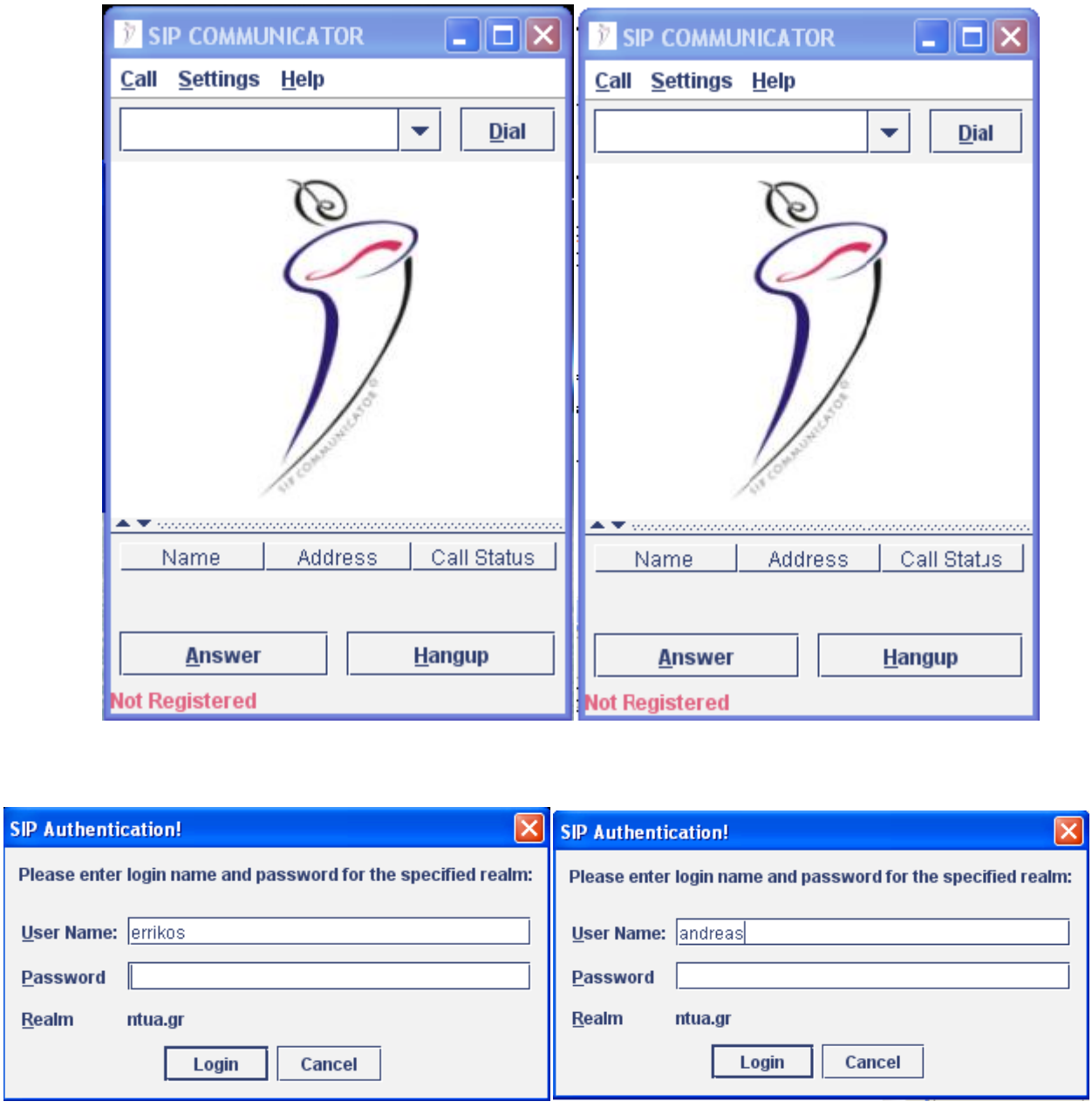
```
            <DISPLAY_NAME value="Andreas"-"Errikos" />
<!-- display name of user -->
            <REGISTRAR_TRANSPORT value="UDP"/>
            <REGISTRATIONS_EXPIRATION value="3600"/>
            <REGISTRAR_PORT value="5060"/>
<!--port on local machine for UAS-->

            <DEFAULT_DOMAIN_NAME value="ntua.gr"/>
<!--domain of user-->
            <DEFAULT_AUTHENTICATION_REALM value="ntua.gr"/>
<!--domain for authentication-->
            <WAIT_UNREGISTGRATION_FOR value="1100"/>
            <SAME_USER_EVERYWHERE value="true"/>
            <simple>
                <CONTACT_LIST_FILE value="contact-list.xml"/>
                <SUBSCRIPTION_EXP_TIME value="600"/>
                <MIN_EXP_TIME value="120"/>
                <LAST_SELECTED_OPEN_STATUS value="online"/>
            </simple>
        </sip>
```

Στα προγράμματα πελάτη ορίσθηκε η διεύθυνση 192.168.1.6 (192.168.1.10) για τη SipStack και η δημιουργία ενός ListeningPoint στην πόρτα 5060, το οποίο χρησιμοποιείται και για την αποστολή και για τη λήψη μηνυμάτων. Ορίσθηκαν οι πόρτες, που θα χρησιμοποιούν τα RTP πακέτα μεταφοράς της φωνής και δόθηκαν πληροφορίες, που αφορούν τα SIP URI AOR των χρηστών, τα ονόματα χρήστη τους και τα ονόματα εμφάνισης, που θα χρησιμοποιούνται. Ταυτόχρονα, ορίσθηκε το ntua.gr ως διαχειριστική οντότητα, στην οποία ανήκουν οι χρήστες και ο πάροχος υπηρεσίας. Τέλος, όπως βλέπουμε παρακάτω, ορίσθηκε η διεύθυνση του Δ.Π.Ι. ως προεπιλεγμένος διακομιστής προώθησης, ώστε να εξασφαλισθεί η επεξεργασία των καινούργιων αιτήσεων για προστασία της ιδιωτικότητας.

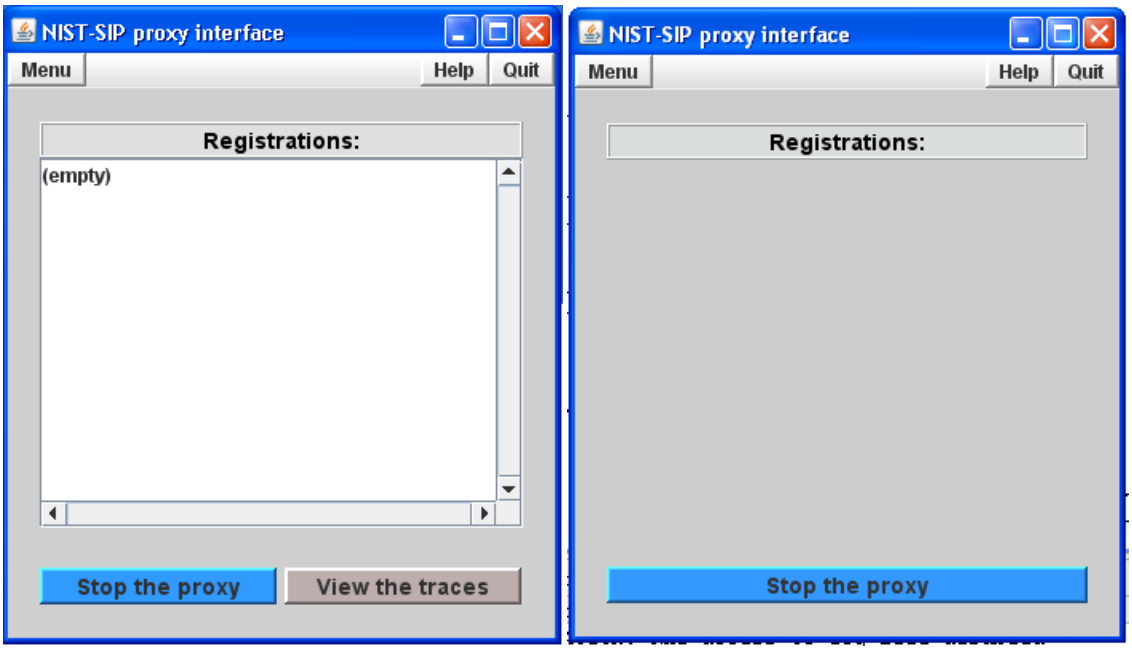
```
<javax>
    <sip>
        <IP_ADDRESS value="192.168.1.6" - "192.168.1.10" />
<!--local IP address of sip communicator-->
        <STACK_NAME value="sip-communicator"/>
        <ROUTER_PATH
value="net.java.sip.communicator.sip.SipCommRouter"/>
        <OUTBOUND_PROXY value="192.168.1.5:4000/udp"/>
<!--IP port and protocol of outbound proxy-->
        <RETRANSMISSON_FILTER value=""/>
        <EXTENSION_METHODS value=""/>
        <RETRANSMISSION_FILTER value="true"/>
    </sip>
</javax>
```

7.1.2 Αναλυτική παρουσίαση ελέγχου

Εκκινώντας τα τέσσερα προγράμματα έχουμε την παρακάτω εικόνα:

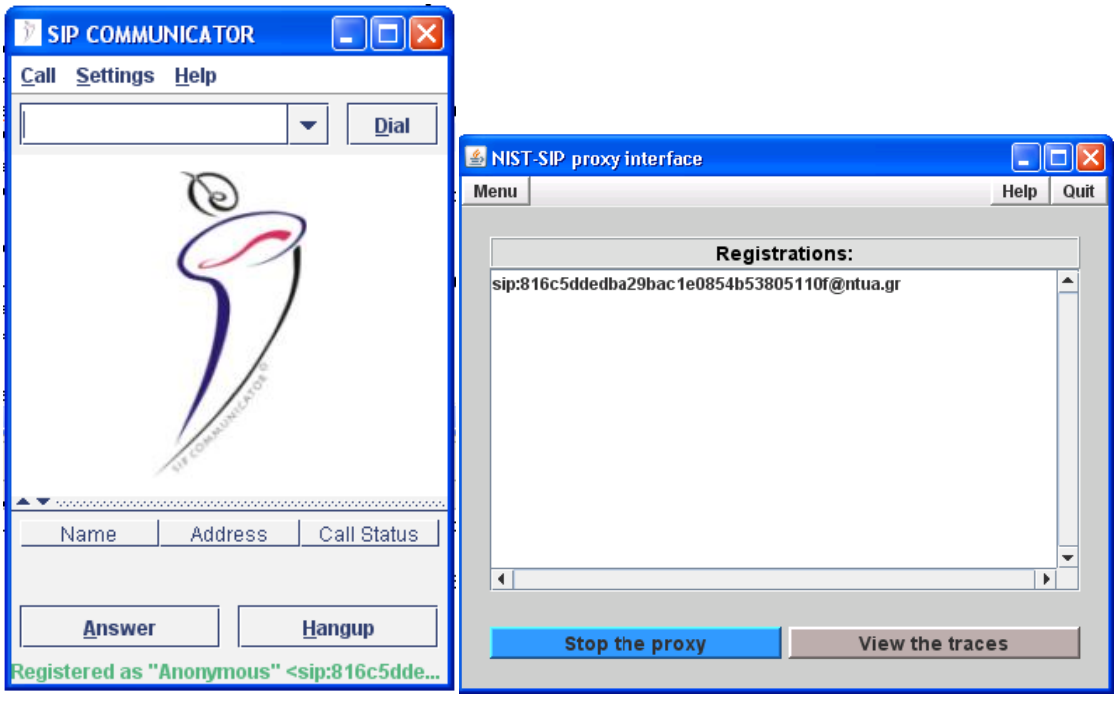


Εικόνα 22: Εκκίνηση προγραμμάτων πελάτη των δύο χρηστών του συστήματος



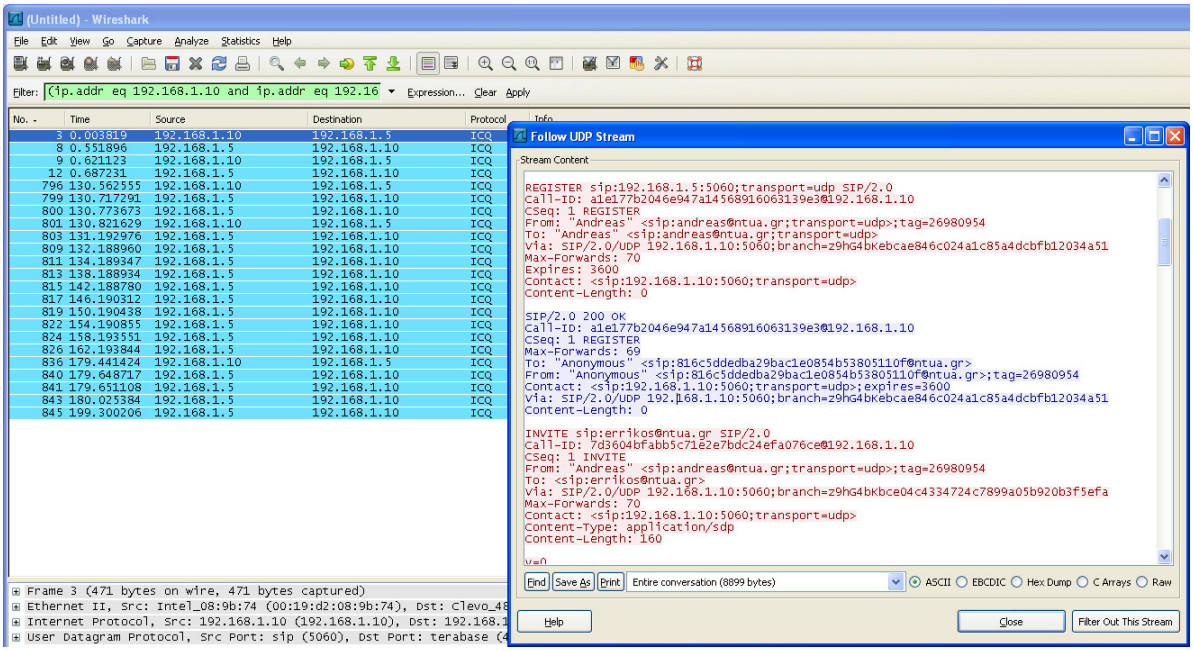
Εικόνα 23: Εκκίνηση των δύο διακομιστών του συστήματος

Η διαδικασία εισόδου ενεργοποιείται με το πλήκτρο Login και για το χρήστη «andreas» οδηγεί στη εξής εικόνα:



Εικόνα 24: Εγγραφή του χρήστη «andreas» στο σύστημα

Τώρα η ταυτότητα του χρήστη προστατεύεται για τις κλήσεις στις οποίες δρα ως παραλήπτης



Εικόνα 25: Παρακολούθηση περιεχομένου πακέτων εγγραφής στο Wireshark

M1: REGISTER from 192.168.1.10 (andreas@ntua.gr) to 192.168.1.5 (Privacy Server)

```
REGISTER sip:192.168.1.5:5060;transport=udp SIP/2.0
Call-ID: a1e177b2046e947a14568916063139e3@192.168.1.10
CSeq: 1 REGISTER
From: "Andreas" <sip:andreas@ntua.gr;transport=udp>;tag=26980954
To: "Andreas" <sip:andreas@ntua.gr;transport=udp>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bKebcae846c024a1c85a4dcbfb12034a51
Max-Forwards: 70
Expires: 3600
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Length: 0
```

M2: REGISTER from 192.168.1.5 (Privacy Server) to 192.168.1.3 (Proxy-Registrar Server)

```
REGISTER sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: a1e177b2046e947a14568916063139e3@192.168.1.10
CSeq: 1 REGISTER
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bka50b0a2b8ab1dfed545611fa0c67f1f6,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bKebcae846c024a1c85a4dcbfb12034a51
Max-Forwards: 69
Expires: 3600
Contact: <sip:192.168.1.10:5060;transport=udp>
To: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>
From: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>;tag=26980954
Content-Length: 0
```

M3: 200 OK Response from 192.168.1.3(Proxy-Registrar Server) to 192.168.1.5 (Privacy Server)

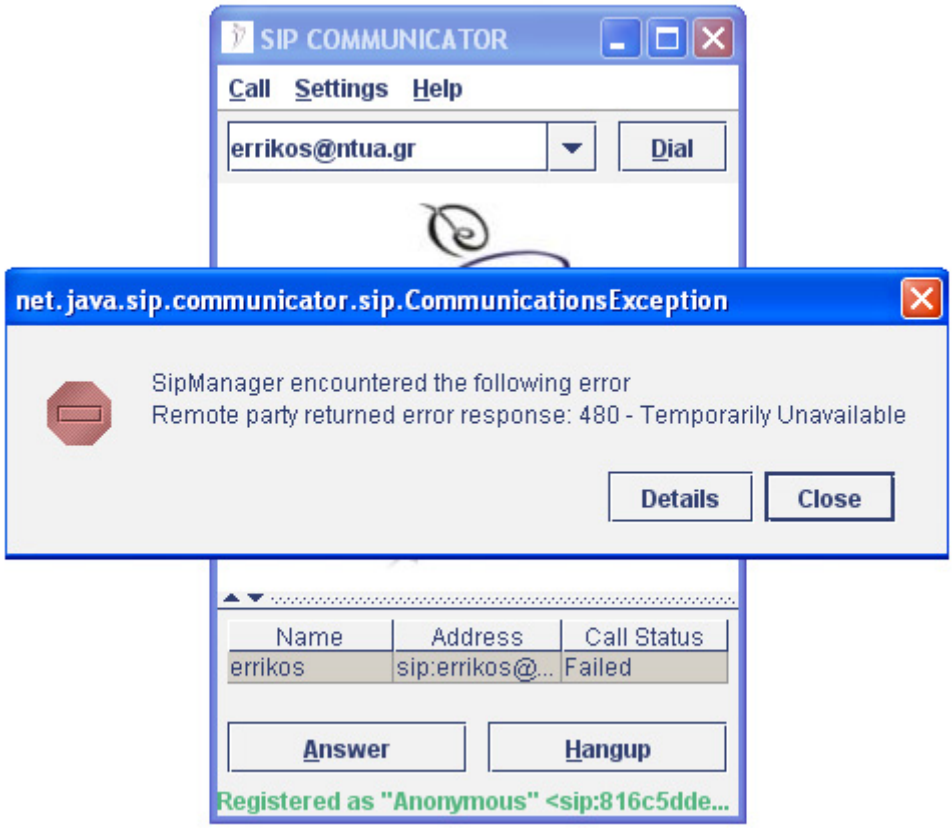
```
SIP/2.0 200 OK
Call-ID: a1e177b2046e947a14568916063139e3@192.168.1.10
CSeq: 1 REGISTER
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bka50b0a2b8ab1dfed545611fa0c67f1f6,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bKebcae846c024a1c85a4dcbfb12034a51
```

```
Max-Forwards: 69
To: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>
From: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>;tag=26980954
Contact: <sip:192.168.1.10:5060;transport=udp>;expires=3600
Content-Length
```

M4: 200 OK Response from 192.168.1.5(Privacy Server)to 192.168.1.10 (andreas@ntua.gr)

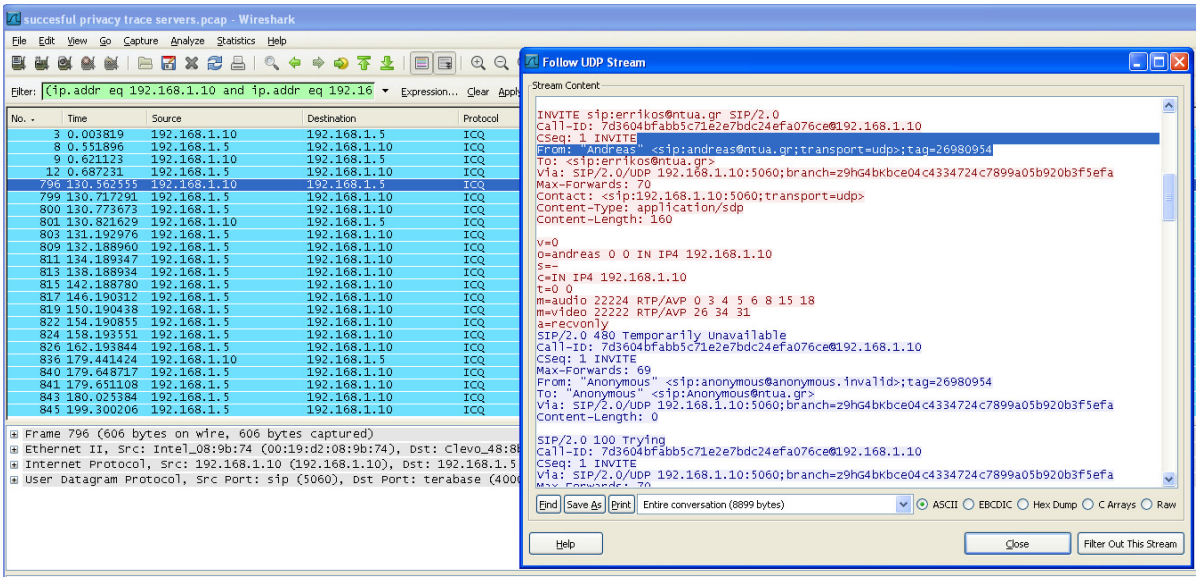
```
SIP/2.0 200 OK
Call-ID: a1e177b2046e947a14568916063139e3@192.168.1.10
CSeq: 1 REGISTER
Max-Forwards: 69
To: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>
From: "Anonymous" <sip:816c5ddedba29bac1e0854b53805110f@ntua.gr>;tag=26980954
Contact: <sip:192.168.1.10:5060;transport=udp>;expires=3600
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bKebcae846c024a1c85a4dcbfb12034a51
Content-Length: 0
```

Για την αποτυχημένη προσπάθεια κλήσης βλέπουμε την παρακάτω εικόνα στο πρόγραμμα πελάτη:



Εικόνα 26: Αποτυχημένη προσπάθεια κλήσης χρήστη «errikos» από χρήστη «andreas»

Στο Wireshark παρατηρούμε τα παρακάτω μηνύματα:



Εικόνα 27: Παρακολούθηση περιεχομένου μηνυμάτων αποτυχημένης κλήσης στο Wireshark

M5: INVITE from 192.168.1.10 (andreas@ntua.gr) to 192.168.1.5 (Privacy Server)

```
INVITE sip:errikos@ntua.gr SIP/2.0
Call-ID: 7d3604bfabb5c71e2e7bdc24efa076ce@192.168.1.10
CSeq: 1 INVITE
From: "Andreas" <sip:andreas@ntua.gr;transport=udp>;tag=26980954
To: <sip:errikos@ntua.gr>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bKbce04c4334724c7899a05b920b3f5efa
Max-Forwards: 70
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 160

v=0
o=andreas 0 0 IN IP4 192.168.1.10
s=-
c=IN IP4 192.168.1.10
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonlyWith Privacy Server Disabled:
```

M6: INVITE from 192.168.1.5 (Privacy Server) to 192.168.1.3 (Proxy-Registrar Server)

```
INVITE sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: 7d3604bfabb5c71e2e7bdc24efa076ce@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bkc560734f2437da53e7f68da6966fe235,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bKbce04c4334724c7899a05b920b3f5efa
Max-Forwards: 69
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Type: application/sdp
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:Anonymous@ntua.gr>
```

```
Content-Length: 160


v=0
o=andreas 0 0 IN IP4 192.168.1.10
s=-
c=IN IP4 192.168.1.10
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

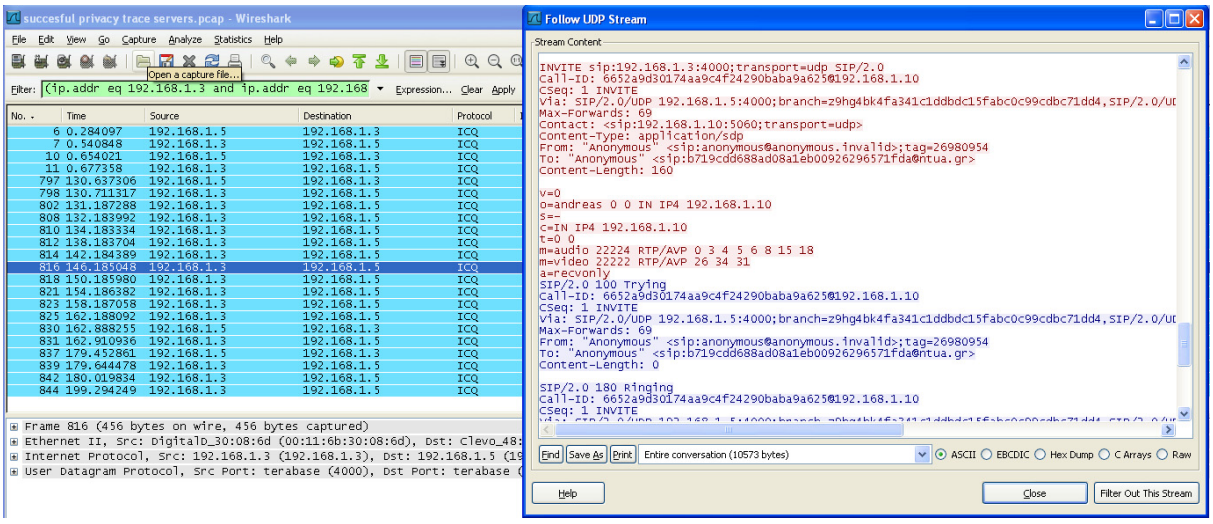
M7: 480 Response from 192.168.1.3(Proxy-Registrar Server) to 192.168.1.5 (Privacy Server)

```
SIP/2.0 480 Temporarily Unavailable
Call-ID: 7d3604bfabb5c71e2e7bdc24efa076ce@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bkc560734f2437da53e7f68da6966fe235,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bKbce04c4334724c7899a05b920b3f5efa
Max-Forwards: 69
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:Anonymous@ntua.gr>
Content-Length: 0 With Privacy Server Disabled:
```

M8: 480 Response from 192.168.1.3(Privacy Server)to 192.168.1.10 (andreas@ntua.gr)

```
SIP/2.0 480 Temporarily Unavailable
Call-ID: 7d3604bfabb5c71e2e7bdc24efa076ce@192.168.1.10
CSeq: 1 INVITE
Max-Forwards: 69
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:Anonymous@ntua.gr>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bKbce04c4334724c7899a05b920b3f5efa
Content-Length: 0
```

Τέλος, μετά την είσοδο στο σύστημα και του χρήστη «errikos» η διαδικασία κλήσης επαναλαμβάνεται και λαμβάνουμε τα παρακάτω αποτελέσματα:



Εικόνα 28: Παρακολούθηση περιεχομένου μηνυμάτων εγκαθίδρυσης κλήσης στο Wireshark

M9: INVITE from 192.168.1.10 (andreas@ntua.gr) to 192.168.1.5 (Privacy Server)

```
INVITE sip:errikos@ntua.gr SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
From: "Andreas" <sip:andreas@ntua.gr;transport=udp>;tag=26980954
To: <sip:errikos@ntua.gr>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 70
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 160


v=0
o=andreas 0 0 IN IP4 192.168.1.10
s=-
c=IN IP4 192.168.1.10
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

M10: INVITE from 192.168.1.5 (Privacy Server) to 192.168.1.3 (Proxy-Registrar Server)

```
INVITE sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 69
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Type: application/sdp
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
Content-Length: 160


v=0
o=andreas 0 0 IN IP4 192.168.1.10
s=-
c=IN IP4 192.168.1.10
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

M11: INVITE from 192.168.1.3(Proxy-Registrar Server)to 192.168.1.6(errikos@ntua.gr)

```
INVITE sip:192.168.1.6:5060 SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.3:4000;branch=z9hG4bKc09cd4175d4f5c30a07d1d9c6ea28060,SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
Contact: <sip:192.168.1.10:5060;transport=udp>
Content-Type: application/sdp
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
Record-Route: <sip:192.168.1.3:4000>
Content-Length: 160


v=0
o=andreas 0 0 IN IP4 192.168.1.10
s=-
```

```
c=IN IP4 192.168.1.10
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

M12+: 100-180-200 Trying-Ringing-OK Response from 192.168.1.6(errikos@ntua.gr) to 192.168.1.3(Proxy-Registrar Server)

```
SIP/2.0 100 Trying
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.3:4000;branch=z9hG4bKc09cd4175d4f5c30a07d1d9c6ea28060,SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
Record-Route: <sip:192.168.1.3:4000>
Content-Length: 0


SIP/2.0 180 Ringing
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.3:4000;branch=z9hG4bKc09cd4175d4f5c30a07d1d9c6ea28060,SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Content-Length: 0


SIP/2.0 200 OK
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.3:4000;branch=z9hG4bKc09cd4175d4f5c30a07d1d9c6ea28060,SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Content-Type: application/sdp
Contact: <sip:192.168.1.6:5060;transport=udp>
Content-Length: 158

v=0
o=andreas 0 0 IN IP4 192.168.1.6
s=-
c=IN IP4 192.168.1.6
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

M13+: 100-180-200 Trying-Ringing-OK Response from 192.168.1.3(Proxy-Registrar Server) to 192.168.1.5 (Privacy Server)

```
SIP/2.0 100 Trying
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
```

```
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 69
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
Content-Length: 0


SIP/2.0 180 Ringing
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Content-Length: 0


SIP/2.0 200 OK
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP
192.168.1.5:4000;branch=z9hg4bk4fa341c1ddbdc15fabc0c99cdbc71dd4,SIP/2.0/UDP
192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Content-Type: application/sdp
Contact: <sip:192.168.1.6:5060;transport=udp>
Content-Length: 158


v=0
o=andreas 0 0 IN IP4 192.168.1.6
s=-
c=IN IP4 192.168.1.6
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

M14+: 100-180-200 Trying-Ringing-OK Response from 192.168.1.3(Privacy Server)to 192.168.1.10 (andreas@ntua.gr)

```
SIP/2.0 100 Trying
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Max-Forwards: 69
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Content-Length: 0


SIP/2.0 100 Trying
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Max-Forwards: 70
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>
```

```
Content-Length: 0


SIP/2.0 180 Ringing
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Content-Length: 0

SIP/2.0 200 OK
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 INVITE
Max-Forwards: 68
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Record-Route: <sip:192.168.1.3:4000>
Content-Type: application/sdp
Contact: <sip:192.168.1.6:5060;transport=udp>
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=z9hG4bK7afb1018229f348ff57d151aeba48e09
Content-Length: 158


v=0
o=andreas 0 0 IN IP4 192.168.1.6
s=-
c=IN IP4 192.168.1.6
t=0 0
m=audio 22224 RTP/AVP 0 3 4 5 6 8 15 18
m=video 22222 RTP/AVP 26 34 31
a=recvonly
```

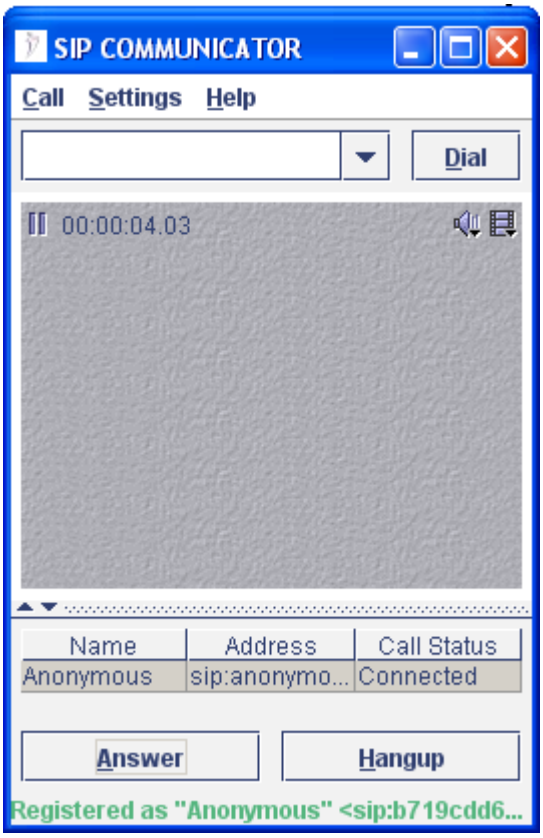
M15: ACK from 192.168.1.10 (andreas@ntua.gr) to 192.168.1.3(Proxy-Registrar Server)

```
ACK sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 ACK
Via: SIP/2.0/UDP 192.168.1.10:5060;branch=39322e3136382e312e31303a3530363
Max-Forwards: 70
Route: <sip:192.168.1.6:5060;transport=udp>
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
Content-Length: 0
```

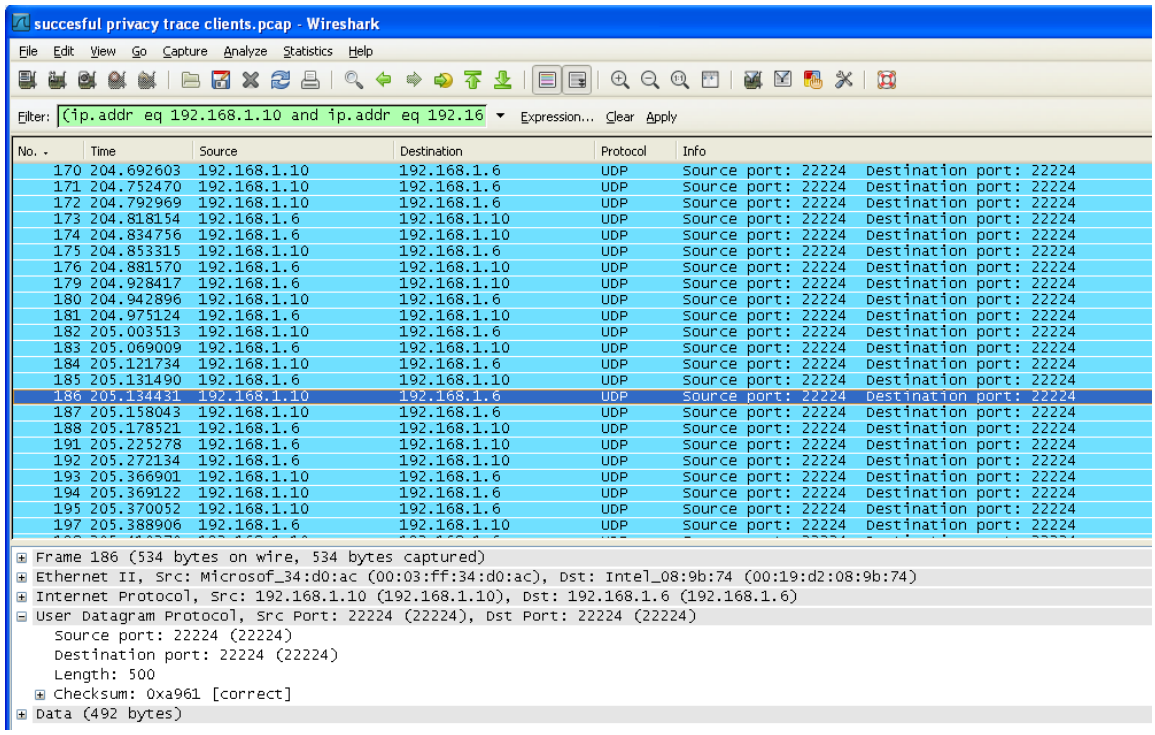
M16: ACK from 192.168.1.3(Proxy-Registrar Server) to 192.168.1.6(errikos@ntua.gr)

```
ACK sip:192.168.1.6:5060 SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 ACK
Via: SIP/2.0/UDP
192.168.1.3:4000;branch=z9hG4bK3f3ec23611207795009bc6c7a5f38c51,SIP/2.0/UDP
192.168.1.10:5060;branch=39322e3136382e312e31303a3530363
Max-Forwards: 69
Route: <sip:192.168.1.6:5060;transport=udp>
To: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
Record-Route: <sip:192.168.1.3:4000>
Content-Length: 0
```

Όταν η σύνοδος εγκαθιδρυθεί στο πρόγραμμα πελάτη, παρατηρούμε την παρακάτω εικόνα, ενώ και στο Wireshark παρατηρούμε τη μεταφορά των RTP πακέτων φωνής:



Εικόνα 29: Πρόγραμμα χρήστη κατά την συνομιλία



Εικόνα 30: Παρακολούθηση RTP πακέτων στο Wireshark

Τελικά, ο χρήστης «errikos» θα τερματίσει τη σύνδεση με την παρακάτω αλληλουχία μηνυμάτων:

M17: BYE from 192.168.1.6 (errikos@ntua.gr) to 192.168.1.3 (Proxy-Registrar Server)

```
BYE sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 BYE
Max-Forwards: 68
Via: SIP/2.0/UDP 192.168.1.6:5060;branch=z9hG4bK2477c2d0432a18e52d6bef0ab9b94a79
Route: <sip:192.168.1.10:5060;transport=udp>
To: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
From: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Content-Length: 0
```

M18: BYE from 192.168.1.3 (Proxy-Registrar Server)to 192.168.1.10 (andreas@ntua.gr)

```
BYE sip:192.168.1.3:4000;transport=udp SIP/2.0
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 BYE
Max-Forwards: 68
Via: SIP/2.0/UDP
192.168.1.3:4000;branch=z9hG4bK7e84f74ecaf5161022c36ca7da5d7639,SIP/2.0/UDP
192.168.1.6:5060;branch=z9hG4bK2477c2d0432a18e52d6bef0ab9b94a79
Route: <sip:192.168.1.10:5060;transport=udp>
To: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
From: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Content-Length: 0
```

M19: 200 OK Response from 192.168.1.10 (andreas@ntua.gr)to 192.168.1.3 (Proxy-Registrar Server)

```
SIP/2.0 200 OK
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 BYE
Max-Forwards: 68
Via: SIP/2.0/UDP
192.168.1.3:4000;branch=z9hG4bK7e84f74ecaf5161022c36ca7da5d7639,SIP/2.0/UDP
192.168.1.6:5060;branch=z9hG4bK2477c2d0432a18e52d6bef0ab9b94a79
To: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
From: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Content-Length: 0
```

M20: 200 OK Response from 192.168.1.3 (Proxy-Registrar Server)to 192.168.1.6 (errikos@ntua.gr)

```
SIP/2.0 200 OK
Call-ID: 6652a9d30174aa9c4f24290baba9a625@192.168.1.10
CSeq: 1 BYE
Max-Forwards: 68
Via: SIP/2.0/UDP 192.168.1.6:5060;branch=z9hG4bK2477c2d0432a18e52d6bef0ab9b94a79
To: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=26980954
From: "Anonymous" <sip:b719cdd688ad08a1eb00926296571fda@ntua.gr>;tag=2545159
Content-Length: 0
```

7.2 Έλεγχος λειτουργίας οντολογίας

7.2.1 Μεθοδολογία ελέγχου

Για τον έλεγχο της λειτουργίας της προτεινόμενης οντολογίας δόθηκαν συγκεκριμένα παραδείγματα SQL ερωτημάτων στο δοκιμαστικό πρόγραμμα και ελήφθησαν τα αποτελέσματα, που επιστρέφει η οντολογία, τα οποία και παρουσιάζονται στη συνέχεια. Όπως αναφέρθηκε, τα εισερχόμενα ερωτήματα είναι στοιχειώδη και στερούνται ουσιαστικής πρακτικής σημασίας, αφού έχουν σαν σκοπό αποκλειστικό να παρουσιάσουν τη ροή εκτέλεσης και την αλληλουχία ερωτημάτων SPARQL, που θα πρέπει να εκτελεσθούν σε αντίστοιχες πραγματικές περιπτώσεις.

7.2.2 Αναλυτική παρουσίαση ελέγχου

7.2.2.1 Παράδειγμα 1

Εισερχόμενο ερώτημα SQL:

```
SELECT name
FROM users
WHERE Field='telecomunications'
```

Το παραπάνω ερώτημα παρουσιάζει το όνομα των συνδρομητών που απασχολούνται στο πεδίο των τηλεπικοινωνιών.

Έξοδος σημασιολογικού αναλυτή ερωτήματος :

Ο σημασιολογικός αναλυτής θα εξάγει τα ακόλουθα ζεύγη τιμών (προσωπικό δεδομένο, λειτουργία στο ερώτημα): (Name, ResultOfQuery), (Field, ExactValue)

Ερώτημα SPARQL που θα εκτελεσθεί:

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Action
WHERE
{
        ?Rule ontology:refersToData  ontology:Name.
        ?Rule ontology:dataUsedAs  ontology:ResultOfQuery .
        ?Rule ontology:hasAction ?Action.
}
```

Το παραπάνω ερώτημα SPARQL επιστρέφει τους κανόνες που αναφέρονται σ' ένα προσωπικό δεδομένο, που έχει ένα συγκεκριμένο ρόλο σ' ένα ερώτημα καθώς και το αποτέλεσμα εφαρμογής αυτού. Τα υπογραμμισμένα στοιχεία στη δεύτερη περίπτωση αντικαθιστώνται από τις αντίστοιχες τιμές (Field, ExactValue)

Αποτελέσματα:
(Name, ResultOfQuery)

Κανόνας	Αποτέλεσμα κανόνα
ontology:NonDisclosureOfName	ontology:Deny

Άρα, το συγκριμένο ερώτημα απορρίπτεται

Αποτελέσματα:
(Field, ExactValue)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfLessDetailedData	ontology:Allow

Ο κανόνας αυτός δεν απαγορεύει το ερώτημα, ωστόσο, αφού ο προηγούμενος το απαγορεύει, τελικά το ερώτημα απορρίπτεται.

7.2.2.2 Παράδειγμα 2

Εισερχόμενο ερώτημα SQL:

```
SELECT prefecture
FROM users
WHERE occupationField='Software Engineering' AND gender='Female'
```

Το παραπάνω ερώτημα παρουσιάζει το νομό των συνδρομητών, που απασχολούνται στο πεδίο της ανάπτυξης λογισμικού και είναι θηλυκού γένους.

Έξοδος σημασιολογικού αναλυτή ερωτήματος :
Ο σημασιολογικός αναλυτής θα εξάγει τα ακόλουθα ζεύγη τιμών (προσωπικό δεδομένο, λειτουργία στο ερώτημα): (Prefecture, ResultOfQuery), (Field, ExactValue), (Gender, ExactValue)

Ερώτημα SPARQL, που θα εκτελεσθεί:

Έχει την ίδια μορφή με το προηγούμενο παράδειγμα

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Action
WHERE
{
        ?Rule ontology:refersToData  ontology:Gender.
        ?Rule ontology:dataUsedAs  ontology:ExactValue.
        ?Rule ontology:hasAction ?Action.
}
```

Αποτελέσματα:
(Field, ExactValue)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfLessDetailedData	ontology:Allow

Ο κανόνας αυτός επιτρέπει την εκτέλεση του ερωτήματος.

Αποτελέσματα:
(Gender, ExactValue)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfGender	ontology: Allow

Ο κανόνας αυτός επιτρέπει την εκτέλεση του ερωτήματος.

Αποτελέσματα:
(Prefecture, ResultOfQuery)

Κανόνας	Αποτέλεσμα κανόνα
-	–

Βλέπουμε ότι δεν έχουμε καταγεγραμμένη πληροφορία στην οντολογία για τη συγκεκριμένη περίπτωση. Σ' αυτήν την περίπτωση το πρόγραμμα θα εκτελέσει διαφορετικά ερωτήματα SPARQL για να εξετάσει, αν υπάρχουν κανόνες, που αφορούν κάποιο προσωπικό δεδομένο, που σχετίζεται με το Prefecture, μέσω των σχέσεων hasLessDetailLevel ή hasMoreDetailLevel. Τα ερωτήματα SPARQL, που θα εκτελεσθούν μαζί με τα αποτελέσματά τους, είναι τα ακόλουθα:

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Persdata
WHERE
{       ?Persdata ontol:hasMoreDetailLevel ontology:Prefecture .
        ?Rule ontology:refersToData ?Persdata.
        ?Rule ontology:dataUsedAs  ontology:ResultOfQuery.
        ?Rule ontology:hasAction ontology:Allow.
}
```

Το παραπάνω ερώτημα ελέγχει, αν υπάρχει κάποιος κανόνας που να επιτρέπει την εμφάνιση ενός προσωπικού δεδομένου, που αποκαλύπτει με μεγαλύτερη ακρίβεια την έννοια στην οποία αναφέρεται ο νομός, κάτι που συμβαίνει αν το εν λόγω προσωπικό δεδομένο συνδέεται με το Prefecture, μέσω της σχέσης hasMoreDetailLevel.
Στην περίπτωση αυτή, αφού επιτρέπεται η αποκάλυψη περισσότερο αναλυτικής πληροφορίας θέσης, θα επιτρέπεται και η αποκάλυψη του νομού.

Αποτελέσματα:
(Prefecture, ResultOfQuery)

Κανόνας	Προσωπικό δεδομένο Persdata
ontology: DisclosureOfLessDetailedData	ontology: City

Άρα, σύμφωνα με το παραπάνω αποτέλεσμα και την προηγούμενη συλλογιστική το ερώτημα είναι επιτρεπτό.

Θα πρέπει για λόγους πληρότητας να γίνει και ο αντίστροφος έλεγχος, δηλαδή αν υπάρχει κάποιος κανόνας που να απαγορεύει την εμφάνιση ενός προσωπικού δεδομένου, που αποκαλύπτει με μικρότερη ακρίβεια την έννοια στην οποία αναφέρεται ο νομός, κάτι που συμβαίνει αν το εν λόγω προσωπικό δεδομένο συνδέεται με το Prefecture μέσω της σχέσης hasLessDetailLevel. Το αντίστοιχο ερώτημα είναι το εξής:

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Persdata
WHERE
{       ?Persdata ontol:hasLessDetailLevel ontology:Prefecture .
        ?Rule ontology:refersToData ?Persdata.
        ?Rule ontology:dataUsedAs  ontology:ResultOfQuery.
        ?Rule ontology:hasAction ontology:Deny.
}
```

Αποτελέσματα:
(Prefecture, ResultOfQuery)

Κανόνας	Προσωπικό δεδομένο Persdata
-	-

Το ερώτημα επιστρέφει κενό αποτέλεσμα, άρα το αρχικό SQL ερώτημα είναι επιτρεπτό και μπορεί να εκτελεσθεί.

7.2.2.3 Παράδειγμα 3

Εισερχόμενο ερώτημα SQL:

```
SELECT PositionHeld, AVG(BirthYear)
FROM users
WHERE city='Athens'
GROUP BY municipality, PositionHeld
```

Το παραπάνω ερώτημα παρουσιάζει το μέσο όρο ηλικίας (που μπορεί να εξαχθεί από το χρόνο γέννησης) των συνδρομητών σε κάθε δήμο που ανήκει στην Αθήνα, ανάλογα με τη θέση εργασίας.

Έξοδος σημασιολογικού αναλυτή ερωτήματος :
Ο σημασιολογικός αναλυτής θα εξάγει τα ακόλουθα ζεύγη τιμών
(προσωπικό δεδομένο, λειτουργία στο ερώτημα):
(PositionHeld, ResultOfQuery), (BirthYear, Average), (City, ExactValue), (Municipality, GroupBy), (PositionHeld, GroupBy)

Το ερώτημα SPARQL, που θα εκτελεσθεί:

Για κάθε ζευγάρι τιμών έχει την ίδια μορφή με το πρώτο παράδειγμα

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Action
WHERE
{
        ?Rule ontology:refersToData  ontology:Gender.
        ?Rule ontology:dataUsedAs  ontology:ExactValue.
        ?Rule ontology:hasAction ?Action.
}
```

Αποτελέσματα:

(BirthYear, Average)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfAverageAge	ontology: Allow

Άρα, σύμφωνα με το παραπάνω αποτέλεσμα, το ερώτημα επίσης δεν απορρίπτεται.

Αποτελέσματα:

(Municipality, GroupBy)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfGroupByMunicipality	ontology: Allow

Άρα, σύμφωνα με το παραπάνω αποτέλεσμα, το ερώτημα επίσης δεν απορρίπτεται.

Αποτελέσματα:

(City, ExactValue)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfLessDetailedData	ontology: Allow

Άρα, σύμφωνα με το παραπάνω αποτέλεσμα, το ερώτημα επίσης δεν απορρίπτεται.

Αποτελέσματα:

(PositionHeld, GroupBy)

Κανόνας	Αποτέλεσμα κανόνα
ontology: DisclosureOfLessDetailedData	ontology: Allow

Αποτελέσματα:

(PositionHeld, ResultOfQuery)

Κανόνας	Αποτέλεσμα κανόνα
ontology: NonDisclosureOfPositionHeld	ontology: Deny

Σύμφωνα με τα παραπάνω αποτελέσματα , το ερώτημα δεν θα πρέπει να γίνει αποδεκτό, ωστόσο το πρόγραμμα μπορεί αυτόματα να ανιχνεύσει, χρησιμοποιώντας ένα τετριμμένο ερώτημα SPARQL, ότι το προσωπικό δεδομένο PositionHeld είναι συνδεδεμένο μέσω της σχέσης hasMoreDetailLevel με άλλα προσωπικά δεδομένα, τα οποία αποκαλύπτουν λιγότερη πληροφορία. Σ' αυτήν την περίπτωση δίνει στο χρήστη τη δυνατότητα να επιλέξει, αν επιθυμεί, να γίνει έλεγχος για το αν υπάρχουν πιθανές τροποποιήσεις στο ερώτημα SQL που να το καθιστούν επιτρεπτό. Αν ο χρήστης απαντήσει καταφατικά, το πρόγραμμα εκτελεί το παρακάτω SPARQL ερώτημα, που αναζητά πιθανούς μετασχηματισμούς του πεδίου, που προκαλεί την απαγόρευση της εκτέλεσης του ερωτήματος:

```
PREFIX ontology:  <http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Persdata
WHERE
{       ?Persdata ontol:hasLessDetailLevel ontology:PositionHeld .
        ?Rule ontology:refersToData ?Persdata .
        ?Rule ontology:dataUsedAs  ontology:ResultOfQuery.
        ?Rule ontology:hasAction ontology:Allow.
}
```

Αποτελέσματα:
(PositionHeld, ResultOfQuery)

Κανόνας	Προσωπικό δεδομένο Persdata
ontology: DisclosureOfLessDetailedData	ontology:Field

Αποτελέσματα:
(PositionHeld,GroupBy)

Κανόνας	Προσωπικό δεδομένο Persdata
ontology: DisclosureOfLessDetailedData	ontology:Field

Σύμφωνα με τα παραπάνω αποτελέσματα, αν το πεδίο PositionHeld αντικατασταθεί με το Field, το ερώτημα θα καταστεί επιτρεπτό. Σε άλλες περιπτώσεις προσωπικών δεδομένων μπορούν να επιστραφούν πολλές διαφορετικές εναλλακτικές λύσεις. Οι λύσεις αυτές επιστρέφονται σ' αυτόν που εκτέλεσε το αρχικό SQL ερώτημα για να επιλέξει αυτή, που καλύπτει καλύτερα τις ανάγκες του. Τελικά, το τροποποιημένο SQL ερώτημα εκτελείται στη Βάση Προσωπικών Δεδομένων:

Τροποποιημένο ερώτημα SQL:

```
SELECT Field, AVG(BirthYear)
FROM users
WHERE city='Athens'
GROUP BY municipality, Field
```

7.2.2.4 Παράδειγμα 4

Τα παραπάνω παραδείγματα παρουσιάζουν τα SPARQL ερωτήματα, μέσω των οποίων γίνεται ο έλεγχος και η τροποποίηση των SQL ερωτημάτων με τη χρήση της οντολογίας. Πάνω στην οντολογία ωστόσο μπορούν να εκτελεστούν οποιασδήποτε μορφής SPARQL ερωτήματα για διαχειριστικούς ή πληροφοριακούς σκοπούς. Για παράδειγμα, παραθέτουμε ένα χρήσιμο ερώτημα SPARQL που επιστρέφει όλα τα προσωπικά δεδομένα που επιτρέπεται να εμφανιστούν σε ένα ερώτημα, τη λειτουργία αυτών καθώς και τον κανόνα που τα καθιστά αποκαλύψιμα:

Το ερώτημα SPARQL είναι το παρακάτω:

```
PREFIX ontology:<http://www.owl-ontologies.com/Ontology1220700347.owl#>
SELECT ?Rule ?Persdata ?QueryFunctionality
WHERE {
        {
                ?Rule ontology:refersToData?Persdata .
                ?Rule ontology:dataUsedAs?QueryFunctionality .
                ?Rule ontology:hasAction ontology:Allow .
        } UNION {
                ?Persdata ontology:hasLessDetailLevel ?SeekPersData .
                ?Rule ontology:refersToData ?SeekPersData .
                ?Rule ontology:dataUsedAs ?QueryFunctionality.
                ?Rule ontology:hasAction ontology:Allow.
        }
}
```

Αποτελέσματα:

Προσωπικό δεδομένο	Λειτουργικότητα	Κανόνας
ontology:AgeRange	ontology:Average	ontology:DisclosureOfAge
ontology:AgeRange	ontology:ExactValue	ontology:DisclosureOfAge
ontology:AgeRange	ontology:ResultOfQuery	ontology:DisclosureOfAge
ontology:AgeRange	ontology:GroupBy	ontology:DisclosureOfAge
ontology:City	ontology:Average	ontology:DisclosureOfLessDetailedData
ontology:City	ontology:ExactValue	ontology:DisclosureOfLessDetailedData
ontology:City	ontology:ResultOfQuery	ontology:DisclosureOfLessDetailedData
ontology:City	ontology:GroupBy	ontology:DisclosureOfLessDetailedData
ontology:AgeRange	ontology:Average	ontology:DisclosureOfLessDetailedData
ontology:AgeRange	ontology:ExactValue	ontology:DisclosureOfLessDetailedData
ontology:AgeRange	ontology:ResultOfQuery	ontology:DisclosureOfLessDetailedData
ontology:AgeRange	ontology:GroupBy	ontology:DisclosureOfLessDetailedData
ontology:Field	ontology:Average	ontology:DisclosureOfLessDetailedData
ontology:Field	ontology:ExactValue	ontology:DisclosureOfLessDetailedData
ontology:Field	ontology:ResultOfQuery	ontology:DisclosureOfLessDetailedData
ontology:Field	ontology:GroupBy	ontology:DisclosureOfLessDetailedData
ontology:BirthYear	ontology:Average	ontology:DisclosureOfAverageAge
ontology:Gender	ontology:ExactValue	ontology:DisclosureOfGender
ontology:Gender	ontology:ResultOfQuery	ontology:DisclosureOfGender
ontology:AgeRange	ontology:Average	ontology:DisclosureOfAverageAge
ontology:Prefecture	ontology:Average	ontology:DisclosureOfLessDetailedData
ontology:Prefecture	ontology:ExactValue	ontology:DisclosureOfLessDetailedData
ontology:Prefecture	ontology:ResultOfQuery	ontology:DisclosureOfLessDetailedData
ontology:Prefecture	ontology:GroupBy	ontology:DisclosureOfLessDetailedData
ontology:Country	ontology:Average	ontology:DisclosureOfLessDetailedData
ontology:Country	ontology:ExactValue	ontology:DisclosureOfLessDetailedData
ontology:Country	ontology:ResultOfQuery	ontology:DisclosureOfLessDetailedData
ontology:Country	ontology:GroupBy	ontology:DisclosureOfLessDetailedData
ontology:Municipality	ontology: GroupBy	ontology:DisclosureOfGroupByMunicipality

Οι παραπάνω εφαρμογές της οντολογίας, που αναπτύχθηκε, καθιστούν αντιληπτές τις δυνατότητες που ξετυλίγονται, όταν χρησιμοποιηθεί η σημασιολογία των προσωπικών δεδομένων για την επεξεργασία τους. Αξιοποιώντας την ευελιξία και την εκφραστικότητα των οντολογιών στην περιοχή της προστασίας των προσωπικών δεδομένων, μπορούν εύκολα να υλοποιηθούν διαδικασίες, οι οποίες θα ήταν αδύνατο να μοντελοποιηθούν με τη χρήση κάποιας απλής διαδικαστικής γλώσσας προγραμματισμού. Επιπλέον, γίνεται επιτρεπτή η χρήση της σημασιολογίας των προσωπικών δεδομένων κατά την επεξεργασία τους. Τα διαφορετικά προσωπικά δεδομένα δεν αντιμετωπίζονται πλέον σαν απλοί τύποι δεδομένων από τη μεριά των πληροφοριακών συστημάτων, αλλά αποκτούν την πραγματική τους διάσταση, στην οποία στις παραδοσιακές αρχιτεκτονικές είχε πρόσβαση μόνο ο άνθρωπος.

8

Επίλογος

Κλείνοντας την παρούσα διπλωματική εργασία θα γίνει μια συνοπτική παρουσίαση της συνεισφοράς της στην επίλυση των προβλημάτων, που τέθηκαν και θα προταθούν ζητήματα τα οποία χρίζουν περαιτέρω επιστημονικής διερεύνησης.

8.1 Σύνοψη και συμπεράσματα

Στην παρούσα εργασία παρουσιάσθηκε μια αρχιτεκτονική επίλυσης του προβλήματος προστασίας των προσωπικών δεδομένων στο περιβάλλον της διαδικτυακής τηλεφωνίας. Το πρόβλημα προσεγγίσθηκε ορίζοντας μια υποθετική εταιρεία παροχής υπηρεσιών με σαφές επιχειρηματικό μοντέλο και τεχνική υποδομή και αναλύθηκαν τα κενά του συστήματος ως προς την προστασία της ιδιωτικότητας. Στο παραπάνω περιβάλλον ορίσθηκαν οι εμπλεκόμενες οντότητες και οι ρόλοι που θα επιτελούν αυτές μέσα στο σύστημα σύμφωνα με την επιθυμητή λειτουργικότητα. Τελικά, η αρχιτεκτονική, που προτάθηκε, εξασφαλίζει την επιθυμητή παροχή εγγυήσεων στους πελάτες της υπηρεσίας διαδικτυακής τηλεφωνίας, διαχωρίζοντας σαφώς τις ευθύνες και τις λειτουργίες που θα πρέπει να επιτελεί η κάθε εμπλεκόμενη οντότητα. Η αρμόδια ανεξάρτητη αρχή διασφάλισης της προστασίας των προσωπικών δεδομένων, που προβλέπεται από τη νομοθεσία, εμπλέκεται στη διαδικασία μετάδοσης της πληροφορίας στο σύστημα, αναλαμβάνοντας κρίσιμες λειτουργίες και δρώντας ως ενδιάμεσος στην επικοινωνία των πελατών με το σύστημα του παρόχου της υπηρεσίας. Ταυτόχρονα, λήφθηκε μέριμνα για την εξασφάλιση της βιωσιμότητας της προτεινόμενης λύσης, διατηρώντας όσο το δυνατόν αναλλοίωτο το επιχειρηματικό μοντέλο της εταιρείας παροχής υπηρεσίας. Για το λόγο αυτό ελαχιστοποιήθηκαν οι παρεμβάσεις στις υπάρχουσες υποδομές και παρουσιάσθηκαν τεχνικές λύσεις, οι οποίες αντιμετωπίζουν τα σημαντικότερα προβλημάτων που ανακύπτουν, λαμβάνοντας υπόψη τις τελευταίες τεχνολογικές εξελίξεις στο χώρο και ακολουθώντας τα καθιερωμένα διεθνή πρότυπα. Ταυτόχρονα, προτάθηκε ένα σύστημα ελεγχόμενης πρόσβασης σε βάσεις προσωπικών

δεδομένων, το οποίο εκμεταλλεύεται τις εξελίξεις στη σημασιολογική αναπαράσταση γνώσης για τον έλεγχο και την αναδιαμόρφωση ερωτημάτων SQL με σκοπό την προστασία της προσωπικής πληροφορίας.

Η εκρηκτική ανάπτυξη των υπηρεσιών διαδικτυακής τηλεφωνίας, αλλά και ευρύτερα της επικοινωνίας μέσω της χρήσης του διαδικτύου, προβλέπεται να προκαλέσει αυξημένο ενδιαφέρον στην κοινή γνώμη για ζητήματα προστασίας προσωπικών δεδομένων, κάτι που θα φέρει αυτού του είδους τις εργασίες σε πρώτο πλάνο. Στην παρούσα εργασία αποδεικνύεται ότι η εφαρμογή της προστασίας της ιδιωτικότητας είναι εφικτή με τεχνικά μέσα και μάλιστα με μικρές τροποποιήσεις των υπαρχόντων υποδομών. Ενώ υπάρχουν έτοιμες τεχνικές λύσεις, που αντιμετωπίζουν μεμονωμένα ζητήματα (ανωνυμία IP, ανωνυμία URI, πρωτόκολλα επικοινωνίας με ενδιάμεσους διακομιστές, αλγόριθμοι διασφάλισης ιδιωτικότητας σε βάσεις δεδομένων π.χ. k-anonymity), δεν υπάρχει συγκεντρωτική αρχιτεκτονική, που να τις αξιοποιεί για να επιλύσει το πρόβλημα της προστασίας της ιδιωτικότητας σ' όλα τα επίπεδα σ' ένα συγκεκριμένο περιβάλλον. Ενώ ο παραδοσιακός ρόλος της ανεξάρτητης αρχής ήταν καθαρά ελεγκτικός και συμβουλευτικός, παρουσιάζεται η ανάγκη να επεκταθεί με την ανάληψη λειτουργιών σε τεχνικό επίπεδο. Συγκεκριμένα η ανεξάρτητη αρχή καθίσταται υπεύθυνη για τη διαχείριση ενός συστήματος πραγματικού χρόνου, κάτι που οδηγεί σε αναγκαία αναδιάρθρωση της.

8.2 Μελλοντικές επεκτάσεις

- Επέκταση της υλοποίησης του Δ.Π.Ι. και των εξαρτώμενων πακέτων για την πλήρη υλοποίηση της προτεινόμενης αρχιτεκτονικής.
- Υλοποίηση σημασιολογικού αναλυτή ερωτημάτων SQL, που θα έχει τη δυνατότητα επεξεργασίας περίπλοκων ερωτημάτων και εξαγωγής της σημασιολογίας αυτών.
- Επέκταση οντολογίας σε συνεργασία με νομικούς με στόχο την πλήρη υλοποίηση της σχετικής νομοθεσίας.
- Υλοποίηση μηχανισμού lawful interception για την πρόσβαση στα προσωπικά δεδομένα με αξιοποίηση τεχνολογιών trusted computing και trusted platforms (αξιοποίηση καρτών, πιστοποιητικών και ηλεκτρονικών ενταλμάτων)
- Ενσωμάτωση μηχανισμού εξισορρόπησης φορτίου (load balancing) στο Δ.Π.Ι, για βελτιστοποίηση της παρεχόμενης ασφάλειας και επίδοσης του δικτυού Tor στο περιβάλλον της προτεινόμενης αρχιτεκτονικής εκμεταλλευόμενοι το γεγονός της πλήρους εικόνας του δικτύου από το διακομιστή καταλόγου στον Δ.Π.Ι..
- Έλεγχος επίδοσης της προτεινόμενης αρχιτεκτονικής είτε θεωρητικά μέσω εξομοίωσης, είτε με μετρήσεις σε πραγματικό περιβάλλον.

9

Βιβλιογραφία

[1] S. Fisher- Hübner, " Privacy in the Global Information Society, " in *IT-Security and Privacy*, Vol. 1958, LNCS, Ed. Heidelberg: Springer-Verlag Berlin, 2001, pp. 5−33.

[2] Facebook Privacy Policy, Dec. 6, 2007. [Online]. Available: http://www.facebook.com/policy.php. [Accessed: Sep. 7, 2008]

[3] Skype Privacy Statement, [Online]. Available: http://www.skype.com/legal/privacy/general/. [Accessed: Sep. 7, 2008]

[4] voip.com Privacy Policy. [Online]. Available: http://www.voip.com/privacy_policy.asp [Accessed: Sep. 7, 2008]

[5] AOL search data scandal. Aug. 25, 2006. [Online]. Available: http://en.wikipedia.org/wiki/AOL_search_data_scandal [Accessed: Sep. 7, 2008]

[6] AOL Stalker - The leading resource in anti-privacy, 2006. [Online]. Available: http://www.aolstalker.com [Accessed: Sep. 7, 2008]

[7] "Για παραβίαση του απορρήτου τηλεπικοινωνιών κατηγορούνται εργαζόμενοι της DT", May. 25, 2008. [Online]. Available: http://www.in.gr/NEWS/article.asp?lngEntityID=903563. [Accessed: Sep. 7, 2008]

[8] "Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών", Oct. 24, 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:HTML. [Accessed: May. 7, 2008]

[9] " Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)", Jul. 12, 2002. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EL:HTML [Accessed: May. 7, 2008]

[10] "Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ", Mar. 15, 2006. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:HTML. [Accessed: May. 7, 2008]

[11] " Νόμος 2472 του 1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις". [Online]. Available: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/2472_1997.PDF. [Accessed: May. 7, 2008]

[12] " Νόμος 3471, 28 Ιουνίου 2006, Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ". [Online]. Available: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/3471_2006.PDF. [Accessed: May. 7, 2008]

[13] A. Johnston, *SIP, Understanding the Session Initiation Protocol,* 2nd ed. Boston: Artech House, 2004.

[14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, *SIP: Session Initiation Protocol,* IETF RFC 3261, June, 2002.

[15] J. Rosenberg, *A Presence Event Package for the Session Initiation Protocol (SIP),* IETF RFC 3856, August, 2004.

[16] J. Rosenberg, H. Schulzrinne, C. Huitema and D. Gurle, *Session Initiation Protocol (SIP) Extension for Instant Messaging,* Ed. B. Campbell, IETF RFC 3428, December, 2002.

[17] J. Rosenberg, H. Schulzrinne, *Reliability of Provisional Responses in the Session Initiation Protocol (SIP),* IETF RFC 3262, June, 2002.

[18] A. Niemi, *Session Initiation Protocol (SIP) Extension for Event State Publication,* IETF RFC 3903, October, 2004.

[19] J. Rosenberg, *The Session Initiation Protocol (SIP) UPDATE Method,* IETF RFC 3311, September, 2002.

[20] B. Ramsdell, *S/MIME Version 3 Message Specification,* IETF RFC 2633, June, 1999.

[21] G. V. Lioudakis, E. A. Koutsoloukas, N. L. Dellas, F. Gaudino, D. I. Kaklamani and I. S. Venieris, " Technical Enforcement of Privacy Legislation," The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens, Greece, September 2007.

[22] G. V. Lioudakis, E. Koutsoloukas, N. Dellas, S. Kapellaki, G. N. Prezerakos, D. I. Kaklamani, I. S. Venieris, "A Proxy for Privacy: the Discreet Box," IEEE Eurocon 2007, Warsaw (Poland), 9-12 September, 2007.

[23] J. Peterson, *A Privacy Mechanism for the Session Initiation Protocol (SIP),* IETF RFC 3323, August, 2004.

[24] Public Proxy Servers. [Online]. Available: http://www.publicproxyservers.com/ [Accessed: Sep. 10, 2008]

[25] M. Leech, M. Ganis, Y. Lee, R. Kuris , D. Koblas, L. Jones, *SOCKS Protocol Version 5,* IETF RFC 1928, March, 1996.

[26] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),* IETF RFC 3489, March, 2003.

[27] J. Rosenberg, R. Mahy, P. Matthews, *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),* IETF Internet-Draft draft-ietf-behave-turn-09, Expires: January 13, 2009, July 12, 2008.

[28] M. Munakata, S. Schubert, T. Ohba, *UA-Driven Privacy Mechanism for SIP,* IETF Internet-Draft draft-ietf-sip-ua-privacy-02, Expires: January 13, 2009, July 14, 2008.

[29] D. M. Goldschlag, M. G.Reed and Paul F. Syverson, " Hiding Routing

Information," Workshop on Information Hiding, Cambridge, UK, May 1996.

[30] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Challenges in deploying low-latency anonymity", NRL CHACS Report 5540-625, 2005

[31] M. Handley, V. Jacobson and C. Perkins, *SDP: Session Description Protocol,* IETF RFC 4566, July, 2006.

[32] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor and A. Rayhan, *Middlebox communication architecture and framework*, IETF RFC 3303, August, 2002.

[33] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, *The Secure Real-time Transport Protocol (SRTP)*, IETF RFC 3711, March, 2004.

[34] J. Rosenberg, *Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP),* IETF Internet-Draft draft-ietf-sip-gruu-12, Expires: September 7, 2007, March 5, 2007.

[35] H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, W. Carr and J. Peterson, *Presence Information Data Format (PIDF)*, IETF RFC 3863, August, 2004.

[36] Chokri Ben Necib and Johann-Christoph Freytag, " Using Ontologies for Database Query Reformulation,"

[37] U. Chakravarthy, J. Grant and Jack Minker" Logic-Based Approach to Semantic Query Optimization," ACM Transactions on Database Systems, Vol. 15, No. 2, June 1990.

[38] Kristen LeFerve, David J. DeWitt, Raghu Ramakrishnan, " Incognito: Ecient Full-Domain K-Anonymity," University of Wisconsin-Madison, in ACM SIGMOD 2005.

[39] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer l-Diversity: Privacy Beyond k-Anonymity. Department of Computer Science, Cornell University, in ICDE 2006.

[40] X. Xiao, Y. Tao m-Invariance: Towards Privacy Preserving Re-publication of Dynamic Datasets. Department of Computer Science and Engineering, Chinese University of Hong Kong, in SIGMOD 2007.

[41] jain-sip: JAVA API for SIP Signaling. [Online]. Available: https://jain-sip.dev.java.net/ [Accessed: June -Aug, 2008]

[42] Jena – A Semantic Web Framework for Java. [Online]. Available: http://www.ece.uwaterloo.ca/~ece355/project/references/sip_communicator_doc.html [Accessed: Aug-Sep, 2008]

[43] ΤΕΧΝΟΛΟΓΙΑ ΛΟΓΙΣΜΙΚΟΥ, ΗΜΜΥ (ΡΟΗ Λ) Κωδικός 3.4.56.9, Άσκηση 1 (Επέκταση Πρωτοκόλλου SIP). [Online]. Available: http://courses.softlab.ntua.gr/softeng/project-sip.html [Accessed: Mar, 2008]

[44] SIP COMMUNICATOR - a JAIN-SIP Video Phone for the People!. [Online]. Available: http://jena.sourceforge.net/ [Accessed: June -Aug, 2008]

[45] jain-sip-presence-proxy: JAIN-SIP-PRESENCE-PROXY. [Online]. Available: https://jain-sip-presence-proxy.dev.java.net/ [Accessed: June -Aug, 2008]

[45] NIST-SIP: The Reference Implementation for JAIN-SIP 1.2. [Online]. Available: http://snad.ncsl.nist.gov/proj/iptel/jain-sip-1.2/javadoc/overview-summary.html [Accessed: June -Aug, 2008]

[47] Tor: anonymity online. [Online]. Available: http://www.torproject.org/ [Accessed: Aug-Sep, 2008]

[48] Roger Dingledine, Nick Mathewson and Paul Syverson, " Tor: The Second-Generation Onion Router,"

[49] Ontology (information science). [Online]. Available: http://en.wikipedia.org/wiki/Ontology_(information_science) [Accessed: Aug, 2008]

[50] World Wide Web Consortium - Web Standards. [Online]. Available: http://www.w3.org/ [Accessed: Aug-Sep, 2008]

[51] Natalya F. Noy and Deborah L. McGuinness, " Ontology Development 101: A Guide to Creating Your First Ontology," Stanford University, Stanford, CA, 94305

[52] Matthew Horridge, Holger Knublauch, Alan Rector, Robert Stevens and Chris Wroe, " A Practical Guide To Building OWL Ontologies Using The Protégé-OWL Plugin and CO-ODE Tools," edition 1, The University Of Manchester, August 27, 2004

[53] SPARQL Query Language for RDF. [Online]. Available: http://www.w3.org/TR/rdf-sparql-query/ [Accessed: Aug-Sep, 2008]

[54] The Protégé Ontology Editor and Knowledge Acquisition System. [Online]. Available: http://protege.stanford.edu/ [Accessed: June -Sep, 2008]

[55] Sip-Communicator. [Online]. Available: http://sip-communicator.org/ [Accessed: May-Jun, 2008]