ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Κρυπτογράφηση σε υποδομή καταλόγου LDAP και περιβάλλον GDPR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μιχάλης Η. Αθανασόπουλος

Επιβλέπων: Ευστάθιος Δ. Συκάς
Καθηγητής Ε.Μ.Π.

Αθήνα, Σεπτέμβριος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Κρυπτογράφηση σε υποδομή καταλόγου LDAP και περιβάλλον GDPR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μιχάλης Η. Αθανασόπουλος

Επιβλέπων: Ευστάθιος Δ. Συκάς
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 21η Σεπτεμβρίου 2020.

.....	.....	.....
Ε. Συκάς	Ι. Ρουσσάκη	Ν. Μήτρου
Καθηγητής Ε.Μ.Π.	Επ. Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Σεπτέμβριος 2020

.....

Μιχάλης Η. Αθανασόπουλος

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

Περίληψη

Η παρούσα εργασία μελετά την κρυπτογράφηση πεδίου σε υποδομή καταλόγου LDAP στο πλαίσιο της καλύτερης δυνατής συμμόρφωσης του Πανελλήνιου Σχολικού Δικτύου με το Γενικό Κανονισμό για την Προστασία των Δεδομένων. Στη σημερινή εποχή, η κρυπτογράφηση πεδίου καθίσταται εξαιρετικά χρήσιμη δεδομένου ότι ευαίσθητα δεδομένα είναι ασφαλή ακόμη και σε περίπτωση που ένας εισβολέας έχει ένα αντίγραφο των αρχείων της βάσης δεδομένων. Η μελέτη και εφαρμογή της κρυπτογράφησης πεδίου γίνεται με χρήση του λειτουργικού πακέτου Διακομιστή Καταλόγου 389, ο οποίος χρησιμοποιεί την υποδομή καταλόγου LDAP.

Αρχικά, επιχειρείται μία σύντομη επισκόπηση στην αναγκαιότητα και χρησιμότητα της κρυπτογράφησης πεδίου καθώς και στην υποδομή καταλόγου LDAP. Αναφέρονται, επίσης, κάποιες βασικές πληροφορίες για τον τύπο δεδομένων LDIF, ο οποίος χρησιμοποιείται κατά κόρον στον Διακομιστή Καταλόγου 389 για κάθε λειτουργία σχετική με το χειρισμό των δεδομένων, όπως προσθήκη, διόρθωση ή διαγραφή κάποιας καταχώρισης. Εξίσου σημαντική είναι και η αναφορά που γίνεται τόσο στο Γενικό Κανονισμό για την Προστασία των Δεδομένων όσο και στην υπηρεσία καταλόγου που χρησιμοποιεί το Πανελλήνιο Σχολικό Δίκτυο.

Εν συνεχεία, αναφέρονται βασικά γνωρίσματα του Διακομιστή Καταλόγου 389 και περιγράφεται αναλυτικά η εγκατάσταση, η παραμετροποίηση και ο σχεδιασμός του, ώστε να διασφαλιστεί η ορθή λειτουργία του για τη διαδικασία της κρυπτογράφησης πεδίου. Παράλληλα, παρουσιάζεται εκτενώς η διαδικασία της εισαγωγής των δεδομένων των σχολείων και των χρηστών, αντίστοιχα, καθώς και οι απαιτούμενες ρυθμίσεις για την ενεργοποίηση της κρυπτογράφησης ενός πεδίου.

Τέλος, παρατίθενται, σε μορφή διαγραμμάτων, τα αποτελέσματα των μετρικών απόδοσης, στα οποία αποτυπώνεται αφενός το αν υπάρχει επιπλέον κόστος στους πόρους του συστήματος και αφετέρου ο βαθμός του κόστους αυτού.

Λέξεις κλειδιά: Γενικός Κανονισμός Προστασίας Δεδομένων, διακομιστής καταλόγου 389, κρυπτογράφηση πεδίου, Πανελλήνιο Σχολικό Δίκτυο, υποδομή καταλόγου LDAP.

Abstract

This thesis analyzes attribute encryption in an LDAP directory service in the framework of compliance of the Greek School Network with the General Data Protection Regulation. Nowadays, attribute encryption has become extremely significant as it can certify that sensitive data are secure even if an intruder has a copy of the database files. The study and implementation of attribute encryption were conducted using the Directory Server 389 operating system package, which uses the LDAP directory service.

Initially, a brief overview of the necessity and usefulness of attribute encryption as well as the LDAP directory service is attempted. There are, also, provided some fundamental information about the LDIF data type, which is used extensively in Directory Server 389 for any function associated with data handling, such as add, modify or delete of an entry. Moreover, the reference of both the General Data Protection Regulation and the directory service used by the Greek School Network are extremely important, too.

Additionally, some key features of Directory Server 389 as well as its installation, configuration and design are listed, in order to ensure its proper function for the process of attribute encryption. Simultaneously, the process of importing the data of the schools and the users, respectively, is presented in detail, as well as the necessary settings for the activation of the encryption of an attribute.

Finally, the diagrammatical presentation of the results of the performance metrics indicates if there is an additional cost to the system resources and the degree of this cost.

Key words: attribute encryption, Directory Server 389, directory service LDAP, GDPR, Greek School Network.

Ευχαριστίες

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας θα ήθελα να ευχαριστήσω όλους όσους βοήθησαν κατά την εκπόνησή της.

Αρχικά, ευχαριστώ θερμά τον καθηγητή μου κ. Ευστάθιο Συκά για την εμπιστοσύνη που μου έδειξε με την ανάθεση της παρούσας εργασίας καθώς και για τη στήριξη του κατά τη διάρκεια της εκπόνησής της. Θα ήθελα, επίσης, να τον ευχαριστήσω για τις γνώσεις που μου μετέδωσε καθ' όλη τη διάρκεια φοίτησης μου στο Πολυτεχνείο.

Επιπλέον, θα ήθελα να ευχαριστήσω τον Ερευνητή του ΕΠΙΣΕΥ και Διδάκτορα κ. Δημήτρη Καλογερά για την άριστη συνεργασία που είχαμε, για την προθυμία του να με βοηθήσει και να με καθοδηγήσει σε κάθε βήμα της παρούσας εργασίας. Θα ήθελα, επίσης, να ευχαριστήσω τον κ. Αντώνη Λυμπέρη για τη συνδρομή του από τη μεριά του Σχολικού Δικτύου και τον κ. Κώστα Καλευρά για την πολύτιμη συνδρομή του σχετικά με την κατεύθυνση ορισμένων τμημάτων της εργασίας.

Τέλος, θα ήθελα να δώσω εγκάρδιες ευχαριστίες στην οικογένειά μου και στην Ειρήνη για τη στήριξη που μου προσέφεραν και την κατανόηση που έδειξαν καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας περιεχομένων

Κεφάλαιο 1

Εισαγωγή

1.1 Σκοπός εργασίας

Η παρούσα διπλωματική εργασία εκπονήθηκε σε ένα εικονικό μηχάνημα που μας παραχωρήθηκε από το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (ΕΑΙΤΥ). Σκοπός της είναι η εγκατάσταση, παραμετροποίηση και δοκιμή του Διακομιστή Καταλόγου 389, ο οποίος κάνει χρήση της υποδομής καταλόγου LDAP, και η λειτουργικότητα της κρυπτογράφησης πεδίου. Η κρυπτογράφηση ευαίσθητων πεδίων που αφορούν προσωπικά δεδομένα συμμορφώνεται πλήρως με το νέο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και κρίνεται απαραίτητη για την ασφαλή αποθήκευση και τον χειρισμό των δεδομένων.

Επιπλέον, στο πλαίσιο αυτής της διπλωματικής εργασίας, πραγματοποιούνται συγκριτικές δοκιμές λειτουργίας οι οποίες αποτυπώνουν το σχετικό φορτίο λόγω της κρυπτογράφησης πεδίου κατά τις λειτουργίες της εγγραφής, ανάγνωσης / αναζήτησης και διαγραφής. Η αποτύπωση του φορτίου είναι σημαντική καθώς μπορούν να εξαχθούν χρήσιμα συμπεράσματα σχετικά με το αν υπάρχει επιπλέον κόστος στις μετρικές απόδοσης, δηλαδή στο χρόνο, στη χρησιμοποίηση του επεξεργαστή, της μνήμης και του δίσκου.

1.2 Διάρθρωση εργασίας

Στο κεφάλαιο αυτό παρουσιάζονται ορισμένα εισαγωγικά στοιχεία έτσι, ώστε ο αναγνώστης να κατατοπιστεί σχετικά με το περιεχόμενο και τη δομή της παρούσας εργασίας.

Στο Κεφάλαιο 2 γίνεται μια εισαγωγή στη διαδικασία της κρυπτογράφησης πεδίου και στη χρησιμότητά της. Επίσης, αναφέρονται κάποιες πληροφορίες σχετικά με την υπηρεσία καταλόγου LDAP και τον τύπο αρχείου LDIF, ενώ, τέλος, γίνεται μία εισαγωγή στην υποδομή καταλόγου του Πανελλήνιου Σχολικού Δικτύου και στο Γενικό Κανονισμό Προστασίας Δεδομένων.

Στο Κεφάλαιο 3 περιγράφεται λεπτομερώς η εγκατάσταση και ο σχεδιασμός του Διακομιστή Καταλόγου 389. Αρχικά αναφέρονται κάποια βασικά χαρακτηριστικά για το λογισμικό του Διακομιστή Καταλόγου 389 και έπειτα παρουσιάζεται η εγκατάσταση του εικονικού μηχανήματος Centos 7 εντός χώρου Virtual Private Network (VPN) του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ). Τέλος, παρατίθενται τα βήματα για την αρχικοποίηση, την εκκίνηση και την

παραμετροποίηση που χρειάζεται ο Διακομιστής Καταλόγου 389 ώστε να διασφαλιστεί η ορθή λειτουργία του για την διαδικασία της κρυπτογράφησης πεδίου.

Στο Κεφάλαιο 4 παρουσιάζεται αναλυτικά η διαδικασία της εισαγωγής των δεδομένων των σχολείων και των χρηστών, αντίστοιχα. Αρχικά, αναλύεται η μέθοδος με την οποία το συντακτικό / αρχείο σχήματος μετατρέπεται σε κατάλληλη μορφή ώστε να εισαχθούν τα δεδομένα. Εν συνεχεία, δημιουργούνται και εισάγονται κάποια κλαδιά στη βάση δεδομένων, τα οποία είναι απαραίτητα για την εισαγωγή τόσο των χρηστών όσο και των εκπαιδευτικών ιδρυμάτων. Τέλος, υλοποιείται η παραγωγή των δεδομένων των χρηστών και παρουσιάζεται η διαδικασία της εισαγωγής των σχολείων και των χρηστών στη βάση δεδομένων.

Στο Κεφάλαιο 5 γίνεται μία εισαγωγή στον αλγόριθμο AES και παρουσιάζεται η σειρά των απαραίτητων βημάτων για την κρυπτογράφηση ενός πεδίου των εισαγόμενων δεδομένων, την επαλήθευση της διαδικασίας κρυπτογράφησης, ώστε να διαπιστωθεί η ορθότητά της, και τη μέθοδο της αφαίρεσης της κρυπτογράφησης ενός πεδίου, εφόσον αυτό κριθεί απαραίτητο.

Στο Κεφάλαιο 6 παρατίθενται τα αποτελέσματα των μετρήσεων χρόνου, χρησιμοποίησης επεξεργαστή, μνήμης και δίσκου σε μορφή διαγραμμάτων. Τέλος, συγκρίνονται τα παραπάνω αποτελέσματα με και χωρίς κρυπτογράφηση ενός πεδίου, ώστε να διαπιστωθεί αν υπάρχει επιπλέον κόστος από την εφαρμογή της.

Στο Κεφάλαιο 7 εξάγονται πολύ σημαντικά συμπεράσματα, από τη μελέτη που πραγματοποιήθηκε, τα οποία αναφέρονται αναλυτικά.

Κεφάλαιο 2

Εισαγωγή στην κρυπτογράφηση πεδίου, στην υποδομή καταλόγου LDAP και στο GDPR

2.1 Εισαγωγή στην κρυπτογράφηση πεδίου

Η κρυπτογράφηση πεδίου είναι ένα είδος κρυπτογράφησης δημοσίου κλειδιού κατά την οποία το μυστικό κλειδί του χρήστη και το κρυπτοκείμενο βασίζονται σε συγκεκριμένα χαρακτηριστικά, όπως η χώρα στην οποία διαμένει. Σε ένα τέτοιο σύστημα, η αποκρυπτογράφηση του κρυπτοκειμένου είναι δυνατή μόνο αν το σύνολο των χαρακτηριστικών του κλειδιού του χρήστη ταιριάζει με τα χαρακτηριστικά του κρυπτοκειμένου.

2.1.1 Αναγκαιότητα κρυπτογράφησης πεδίου

Ο Διακομιστής Καταλόγου 389 (Directory Server 389) προσφέρει μία ποικιλία μηχανισμών για την ασφαλή πρόσβαση σε ευαίσθητα δεδομένα. Τέτοιοι μηχανισμοί θεωρούνται τόσο οι λίστες ελέγχου πρόσβασης (Access Control Lists), οι οποίες αποτρέπουν τους μη εξουσιοδοτημένους χρήστες από το να διαβάσουν συγκεκριμένες καταχωρήσεις ή χαρακτηριστικά εντός κάποιων καταχωρήσεων, όσο και το πρωτόκολλο Transport Layer Security (TLS) μέσω του οποίου προστατεύονται τα δεδομένα από υποκλοπή σε μη ασφαλή δίκτυα. Ωστόσο, αν κάποια αρχεία της βάσης δεδομένων βρεθούν στην κατοχή ενός μη εξουσιοδοτημένου χρήστη, θα μπορούσε να υπάρξει πιθανότητα υποκλοπής ευαίσθητων δεδομένων, όπως κωδικών πρόσβασης και Αριθμών Φορολογικού Μητρώου (Α.Φ.Μ.). Κάτι τέτοιο δεν είναι απίθανο να συμβεί καθώς, ακόμα και αν χρησιμοποιούνται μέτρα ελέγχου πρόσβασης, το γεγονός ότι οι πληροφορίες εντός της βάσης δεδομένων αποθηκεύονται ως απλό κείμενο τις καθιστά ευάλωτες σε υποκλοπή.

Για εξαιρετικά ευαίσθητες πληροφορίες, αυτή η πιθανότητα απώλειας πληροφοριών θα μπορούσε να παρουσιάσει σημαντικό κίνδυνο ασφαλείας. Προκειμένου να εξαλειφθεί αυτός ο κίνδυνος, ο Directory Server 389 επιτρέπει την κρυπτογράφηση τμημάτων της βάσης δεδομένων του. Μόλις κρυπτογραφηθούν, τα δεδομένα αυτά είναι ασφαλή ακόμη και σε περίπτωση που ένας εισβολέας έχει ένα αντίγραφο των αρχείων της βάσης δεδομένων [1].

2.1.2 Βασικές πληροφορίες κρυπτογράφησης πεδίου στον Directory Server 389

Η κρυπτογράφηση της βάσης δεδομένων επιτρέπει στα χαρακτηριστικά να κρυπτογραφούνται μέσα στη βάση δεδομένων. Τόσο η κρυπτογράφηση όσο και ο αλγόριθμος κρυπτογράφησης μπορούν να διαμορφωθούν ανά χαρακτηριστικό. Όταν γίνει η απαραίτητη διαμόρφωση, κάθε εμφάνιση ενός συγκεκριμένου χαρακτηριστικού, ακόμη και αν αυτό είναι δεδομένο ευρετηρίου, κρυπτογραφείται για κάθε καταχώριση που είναι αποθηκευμένη σε αυτή τη βάση δεδομένων.

Σε αυτό το σημείο, αξίζει να σημειωθεί ότι υπάρχει μία εξαίρεση όσον αφορά τα κρυπτογραφημένα δεδομένα: οποιαδήποτε τιμή χρησιμοποιείται στο πεδίο του σχετικού διακεκριμένου ονόματος (Relative Distinguished Name) για μία καταχώριση δεν κρυπτογραφείται στο πεδίο του διακεκριμένου ονόματος. Για παράδειγμα, αν κρυπτογραφηθεί το χαρακτηριστικό uid, μπορεί η τιμή του να κρυπτογραφείται αλλά η πραγματική τιμή εμφανίζεται στο DN:

```
dn: uid=user1,ou=People,dc=example,dc=com
nsUniqueId: ee91ea82-1dd111b2-9f36e9bc-39fb8550
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
givenName: John
sn: Smith
uid:: Sf04P9nJWGU1qiW9JJCGRg==
```

Κάτι τέτοιο θα έδινε τη δυνατότητα σε κάποιον να ανακαλύψει την κρυπτογραφημένη τιμή. Ως εκ τούτου, οποιοδήποτε χαρακτηριστικό εντός του DN της καταχώρισης δεν μπορεί να κρυπτογραφηθεί αποτελεσματικά, δεδομένου ότι θα εμφανίζεται πάντα και στο πεδίο του διακεκριμένου ονόματος.

Τέλος, μπορούν να κρυπτογραφηθούν και χαρακτηριστικά ευρετηρίου (indexed attributes) τα οποία διευκολύνουν την αναζήτηση και ανάκτηση πληροφοριών ταξινομώντας και οργανώνοντας χαρακτηριστικά ή τιμές.

2.2 Εισαγωγή στην υποδομή καταλόγου LDAP

Το LDAP (Lightweight Directory Access Protocol) είναι ένα βιομηχανικό πρωτόκολλο εφαρμογών ανοικτού προτύπου για την πρόσβαση και τη συντήρηση κατανεμημένων υπηρεσιών πληροφοριών καταλόγου πάνω από το Internet Protocol (IP) δίκτυο [2]. Οι υπηρεσίες καταλόγου διαδραματίζουν σημαντικό ρόλο στην ανάπτυξη εφαρμογών intranet και internet επιτρέ-

ποντας την ανταλλαγή πληροφοριών που είναι σχετικές με χρήστες, συστήματα, δίκτυα, υπηρεσίες και εφαρμογές σε όλο το δίκτυο. Συνεπώς, οι υπηρεσίες καταλόγου ενδέχεται να παρέχουν ένα οποιοδήποτε οργανωμένο σύνολο εγγραφών (π.χ. έναν εταιρικό κατάλογο αλληλογραφίας), συχνά με μια ιεραρχική δομή.

Όσον αφορά την αρχιτεκτονική του, ένας κατάλογος LDAP έχει μία δομή δέντρου. Όλες οι καταχωρήσεις του καταλόγου έχουν καθορισμένη θέση σε αυτήν την ιεραρχία. Αυτή η ιεραρχία ονομάζεται δέντρο πληροφοριών καταλόγου (Directory Information Tree). Η πλήρης διαδρομή προς την επιθυμητή καταχώριση ονομάζεται διακεκριμένο όνομα (Distinguished Name) και κάθε αντικείμενο στο δέντρο αναγνωρίζεται από το σχετικό διακεκριμένο όνομά του (Relative Distinguished Name).

Το LDAP είναι καθορισμένο σε μια σειρά εκδόσεων του Internet Engineering Task Force (IETF) με την ονομασία Request for Comments (RFCs). Η τελευταία προδιαγραφή είναι η έκδοση 3 που δημοσιεύτηκε ως RFC 4511.

Μία συχνή χρήση του πρωτοκόλλου LDAP είναι να παρέχει ένα κεντρικό μέρος για την αποθήκευση ονομάτων χρηστών και κωδικών πρόσβασης. Αυτό επιτρέπει σε πολλές διαφορετικές εφαρμογές και υπηρεσίες να συνδέονται στον διακομιστή LDAP για την επικύρωση των χρηστών.

2.2.1 Τύπος δεδομένων LDIF

Η LDAP μορφή ανταλλαγής δεδομένων (LDAP Data Interchange Format ή LDIF) ορίζεται ως μία τυπική μορφή ανταλλαγής δεδομένων απλού κειμένου για την παρουσίαση του περιεχομένου του καταλόγου LDAP και των αιτήσεων ενημέρωσής του. Ένα αρχείο LDIF μεταφέρει το περιεχόμενο του καταλόγου ως ένα σύνολο εγγραφών, με μία εγγραφή για κάθε αντικείμενο (ή καταχώριση). Παρουσιάζει, επίσης, αιτήματα ενημέρωσης (π.χ. προσθήκη, τροποποίηση, διαγραφή και μετονομασία) ως ένα σύνολο από εγγραφές, μία για κάθε αίτηση ενημέρωσης.

Το LDIF σχεδιάστηκε στις αρχές της δεκαετίας του 1990 από τους Tim Howes, Mark C. Smith, και Gordon Good. Ενημερώθηκε και επεκτάθηκε για χρήση με την έκδοση 3 του LDAP στα τέλη της δεκαετίας του 1990 και ορίζεται επίσημα στο RFC 2849 [3].

Με την πάροδο των ετών έχουν προταθεί διάφορες επεκτάσεις για τον τύπο LDIF. Μία επέκταση, όμως, έχει καθοριστεί επίσημα από το IETF, η οποία δημοσιεύθηκε το 2006 στο RFC 4525 και επέκτεινε το LDIF για να υποστηρίζει την επέκταση LDAP Modify - Increment.

2.3 Εισαγωγή στην υπηρεσία καταλόγου του Πανελλήνιου Σχολικού Δικτύου και στο GDPR

Στόχος της υπηρεσίας καταλόγου είναι η δημιουργία και η λειτουργία ενός αποθετηρίου καταλόγου το οποίο θα συντηρεί τα στοιχεία ταυτοποίησης και παραμετροποίησης του κάθε χρήστη διαφόρων υπηρεσιών του Πανελλήνιου Σχολικού Δικτύου, όπως e-mail, προσωπικές σελίδες κλπ. Η παραμετροποίηση μπορεί να αφορά και πρόσβαση σε υπηρεσίες από οντότητες (π.χ. πρόσβαση με δρομολογητή ADSL ενός σχολείου) αντί για μεμονωμένα άτομα. Η υπηρεσία καταλόγου είναι μια προτυποποιημένη υπηρεσία (κατά ISO και IETF) και έχει ευρεία αποδοχή στο χώρο της δομημένης λειτουργίας υπηρεσιών διαδικτύου.

Ο Κανονισμός 2016/679 της Ευρωπαϊκής Ένωσης, ευρύτερα γνωστός ως Γενικός Κανονισμός για την Προστασία Δεδομένων (στα αγγλικά General Data Protection Regulation - GDPR), ψηφίστηκε στις 27 Απριλίου 2016 και τίθεται σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου 2018 [4].

Πρόκειται για ένα νέο, ενιαίο και άμεσα εφαρμόσιμο νομικό πλαίσιο, το οποίο ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα ατόμων που βρίσκονται στην Ευρωπαϊκή Ένωση, από άλλα άτομα, εταιρείες ή οργανισμούς.

Με το νέο Κανονισμό ενισχύονται τα δικαιώματα των υποκειμένων των δεδομένων, αυξάνονται, ποσοτικά και ποιοτικά, οι υποχρεώσεις των υπεύθυνων και εκτελούντων την επεξεργασία και γενικώς ενισχύεται σημαντικά η προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης.

Η υπηρεσία καταλόγου του ΠΣΔ διατηρεί ορισμένους αριθμούς μητρώου σχετικούς με τις οντότητες οι οποίες αποθηκεύονται σε αυτή. Τέτοια παραδείγματα αποτελούν ο αριθμός μητρώου εκπαιδευτικού, μονάδας καθώς και το ΑΦΜ εκπαιδευτικού / προσωπικού.

Στη νέα εποχή του GDPR ο πάροχος μιας υπηρεσίας που υλοποιείται σε απομακρυσμένες υποδομές (π.χ. σύννεφο) χρειάζεται να προστατεύεται. Στην παρούσα διπλωματική εργασία η προστασία που θα αξιολογηθεί είναι η κρυπτογράφηση πεδίου (attribute encryption). Με αυτό τον τρόπο προστασίας οι πρωτογενείς τιμές των τιμών κρυπτογραφούνται. Σε πολλές περιπτώσεις οι καταναλωτές της υπηρεσίας καταλόγου δε χρησιμοποιούν την υπηρεσία ως πρωταρχική πηγή δεδομένων αλλά για την επιβεβαίωση της ορθής αντιστοιχίας μιας τιμής με συγκεκριμένο χρήστη. Έτσι, λοιπόν, είναι πιθανό ο χρήστης να έχει εισαγάγει ο ίδιος τον αριθμό μητρώου του ως εκπαιδευτικός και η εφαρμογή να απαιτεί απλά την επιβεβαίωση ότι αυτός είναι ορθός. Εφόσον κάτι τέτοιο μπορεί να υλοποιηθεί χωρίς να απαιτείται πρόσβαση στον αριθμό μητρώου

που διατηρείται στην υπηρεσία καταλόγου, με αυτόν τον τρόπο αυξάνεται η ασφάλεια δεδομένων συνολικά. Αυτό συμβαίνει καθώς δεν είναι αναγκαίο για τις εφαρμογές να διαβάσουν το σύνολο των αριθμών μητρώου που διατηρεί η υπηρεσία μόνο και μόνο για να τους επιβεβαιώσουν με στοιχεία που εισάγουν οι χρήστες.

Κεφάλαιο 3

Εγκατάσταση και παραμετροποίηση Directory Server 389

3.1 Λογισμικό πακέτο Directory Server 389

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, πραγματοποιήθηκε πιλοτική εγκατάσταση και λειτουργία του DS 389, ενός εξυπηρετητή καταλόγου με δυνατότητα κρυπτογράφησης πεδίου. Σε ένα τέτοιο σενάριο τα ευαίσθητα πεδία κρυπτογραφούνται προτού αποθηκευτούν στο δίσκο και ως εκ τούτου δεν υπάρχει κίνδυνος απώλειας των δεδομένων του φυσικού μέσου αποθήκευσης. Επιπλέον, προς χάρη συμβατότητας προς τα πίσω με τις υφιστάμενες εφαρμογές:

- δεν απαιτείται τροποποίηση στο υφιστάμενο σχήμα (directory schema) για τις εφαρμογές χρήστη (παρά μόνο για τη διαχείριση του εξυπηρετητή καταλόγου).
- δεν απαιτείται αλλαγή στο API (LDAP API v3).

Το πακέτο λογισμικού Directory Server 389 (παλιότερα Fedora Directory Server) είναι ένα ανοιχτού τύπου λογισμικό για λειτουργία υπηρεσίας LDAP επιχειρησιακού επιπέδου (enterprise class). Αναπτύχθηκε από την δημόσια ομάδα του Fedora Project για την Red Hat. Το όνομα 389 προέρχεται από τον αριθμό θύρας του πρωτοκόλλου LDAP.

Μερικά βασικά χαρακτηριστικά του DS 389 είναι τα παρακάτω [5]:

- Εξυπηρετητής υψηλής απόδοσης που μπορεί να χειρίζεται χιλιάδες εργασίες κάθε δευτερόλεπτο και εκατοντάδες χιλιάδες λογαριασμούς.
- Ασύγχρονο Multi-Master Replication για αντοχή σε απώλεια server και υψηλή απόδοση για λειτουργία εγγραφών.
- Ο κώδικας αναπτύσσεται συνεχώς για περισσότερο από μία δεκαετία από ιστότοπους σε όλο τον κόσμο.
- Συγχρονισμός, μονόδρομης και αμφίδρομης κατεύθυνσης, με Active Directory για χρήστες και ομάδες.
- Υποστήριξη ασφαλούς καναλιού ταυτοποίησης και μετάδοσης (TLS 1/2 και SASL).
- Υποστήριξη της τρέχουσας έκδοσης του LDAP, δηλαδή της LDAPv3.
- Αλλαγές σε λειτουργία, μηδενικό downtime, διαχείριση με χρήση σχήματος LDAP, δυνατότητα για Access Control Information (ACI).

- Γραφική κονσόλα για διαχείριση χρήστη / ρόλου / ομάδας / λογαριασμού, αλλά και για διαχείριση εξυπηρετητή με λειτουργίες όπως η αποθήκευση αντιγράφων ασφαλείας, η αποκατάσταση του συστήματος, η εισαγωγή, η εξαγωγή, η αντιγραφή (replication) και η δημιουργία βάσης δεδομένων.
- Συνεχής παραγωγή και έλεγχος κώδικα με χρήση του Continuous Integration Testing Framework (lib389) το οποίο επιτρέπει την υψηλή σταθερότητα του κώδικα και μειώνει στις νέες εκδόσεις την πιθανότητα χρήσης ξεπερασμένου κώδικα.

3.2 Εγκατάσταση εικονικού μηχανήματος Centos εντός χώρου VPN ΠΣΔ

Για τη δοκιμαστική λειτουργία του DS 389 μάς παραχωρήθηκε από το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (ΕΑΙΤΥ) ένα εικονικό μηχάνημα στο ιδιωτικό Data Center με IP (10.2.241.15), στο οποίο έγινε εγκατάσταση του λειτουργικού συστήματος Centos (έκδοση 7.7). Στη συνέχεια, παρατίθενται οι απαραίτητες ρυθμίσεις και εγκαταστάσεις που έγιναν με τη σειρά που περιγράφονται και τον αντίστοιχο κώδικα.

1. Ρύθμιση του ονόματος στο αρχείο /etc/hosts:

```
vim /etc/hosts
[...]
10.2.241.15 openldap-gdpr.local openldap-gdpr   openldap-
gdpr.att.sch.gr
```

2. Ρύθμιση του τείχους προστασίας (firewall) και επανεκκίνησή του για να επιτρέπεται το πρωτόκολλο LDAP και LDAPS μέσω των ip tables:

```
firewall-cmd --permanent --add-port=389/tcp
firewall-cmd --permanent --add-port=636/tcp
firewall-cmd --permanent --add-port=9830/tcp
firewall-cmd --reload
```

3. Ρύθμιση στο τέλος του αρχείου /etc/sysctl.conf:

```
vim /etc/sysctl.conf
[...]
net.ipv4.tcp_keepalive_time = 300
net.ipv4.ip_local_port_range = 1024 65000
fs.file-max = 64000
```

4. Επανεκκίνηση του server:

```
shutdown -r now
```

5. Εγκατάσταση epel και remi repository:

```
sudo yum localinstall epel-release-latest-7.noarch.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-7.rpm
wget http://rpms.famillecollet.com/enterprise/remi-release-5.rpm
rpm -Uvh remi-release-5.rpm
rpm -Uvh remi-release-7.rpm
```

6. Δημιουργία χρήστη για διαχείριση του LDAP:

```
sudo useradd ldapadmin
sudo passwd ldapadmin
```

7. Εγκατάσταση λογισμικού DS 389:

```
sudo yum -y install 389-admin 389-admin-console 389-admin-console-doc
389-adminutil 389-console 389-ds 389-ds-base 389-ds-base-libs 389-ds-
console 389-ds-console-doc 389-dsgw
```

3.3 Αρχικοποίηση και εκκίνηση Directory Server 389

Ύστερα από την εγκατάσταση του λογισμικού απαιτείται η αρχικοποίηση με χρήση ενός προγράμματος αρχικών ρυθμίσεων που παρέχεται και είναι το setup-ds-admin.pl. Με την εκτέλεση αυτού του προγράμματος, παρουσιάζεται ο παρακάτω διάλογος:

```
[root@openldap-gdpr ~]# setup-ds-admin.pl
==============================================================
This program will set up the 389 Directory and Administration Servers.

It is recommended that you have "root" privilege to set up the software.
Tips for using this program:
  - Press "Enter" to choose the default and go to the next screen
  - Type "Control-B" then "Enter" to go back to the previous screen
  - Type "Control-C" to cancel the setup program

Would you like to continue with set up? [yes]:

==============================================================
Your system has been scanned for potential problems, missing patches,
etc.  The following output is a report of the items found that need to
be addressed before running this software in a production
environment.

389 Directory Server system tuning analysis version 14-JULY-2016.

NOTICE: System is x86_64-unknown-linux3.10.0-123.el7.x86_64 (1 processor).


Would you like to continue? [yes]:
 1. Express
     Allows you to quickly set up the servers using the most
     common options and pre-defined defaults. Useful for quick
```

```
    evaluation of the products.
  2. Typical
    Allows you to specify common defaults and options.
  3. Custom
    Allows you to specify more advanced options. This is
    recommended for experienced server administrators only.
To accept the default shown in brackets, press the Enter key.
Choose a setup type [2]: 2
Computer name [openldpap-gdpr.att.sch.gr]:
System User [dirsrv]:
System Group [dirsrv]:
Do you want to register this software with an existing
configuration directory server? [no]:
Configuration directory server
administrator ID [admin]:
Password:
Password (confirm):
Administration Domain [sch.lan]:
Directory server network port [389]:
Directory server identifier [openldpap-gdpr]:
Suffix [dc=sch,dc=gr]:
Directory Manager DN [cn=Directory Manager]:
Password:
Password (confirm):
Administration port [9830]:
Are you ready to set up your servers? [yes]:
Creating directory server . . .
Your new DS instance 'deploy' was successfully created.
Creating the configuration directory server . . .
Beginning Admin Server creation . . .
Creating Admin Server files and directories . . .
Updating adm.conf . . .
Updating admpw . . .
Registering admin server with the configuration directory server
Updating adm.conf with information from configuration directory server
Updating the configuration for the httpd engine . . .
..
..
Starting admin server . . .
The admin server was successfully started.
Admin server was successfully created, configured, and started.
```

Το dirsrv είναι το εκτελέσιμο πρόγραμμα του καταλόγου. Με τη χρήση του systemctl γίνεται η εκκίνηση, ο έλεγχος και ο τερματισμός του 389 Directory Server, όπως φαίνεται στη συνέχεια.

1. Εκκίνηση του Directory Server 389:

```
[root@openldap-gdpr ~]# systemctl start dirsrv.target
```

2. Έλεγχος λειτουργίας:

```
[root@openldap-gdpr ~]# systemctl status dirsrv.target
```

```
? dirsrv.target - 389 Directory Server
   Loaded: loaded (/usr/lib/systemd/system/dirsrv.target; disabled;
vendor preset: disabled)
   Active: active since Fri 2017-07-07 21:58:26 UTC; 2s ago


21:58:26 deploy systemd[1]: Reached target 389 Directory Server.
21:58:26 deploy systemd[1]: Starting 389 Directory Server.
```

3. Τερματισμός του DS 389:

```
[root@openldap-gdpr ~]# systemctl stop dirsrv.target
```

Εναλλακτικά, οι παραπάνω λειτουργίες μπορούν να πραγματοποιηθούν, αντίστοιχα, και με τις παρακάτω γραμμές κώδικα:

```
[root@openldap-gdpr ~]# start-dirsrv
Starting instance "deploy"


[root@openldap-gdpr ~]# status-dirsrv
? dirsrv.target - 389 Directory Server
   Loaded: loaded (/usr/lib/systemd/system/dirsrv.target; disabled; vendor
preset: disabled)
   Active: active since Fri 2017-07-07 21:58:26 UTC; 1min 39s ago


21:58:26 deploy systemd[1]: Reached target 389 Directory Server.
21:58:26 deploy systemd[1]: Starting 389 Directory Server.
Status of instance "deploy"
? dirsrv@deploy.service - 389 Directory Server deploy.
   Loaded: loaded (/usr/lib/systemd/system/dirsrv@.service; enabled; ven-
dor preset: disabled)
   Active: active (running) since Fri 2017-07-07 22:00:01 UTC; 4s ago
  Process:     4754     ExecStartPre=/usr/sbin/ds_systemd_ask_password_acl
/etc/dirsrv/slapd-%i/dse.ldif (code=exited, status=0/SUCCESS)
 Main PID: 4761 (ns-slapd)
   Status: "slapd started: Ready to process requests"
   CGroup: /system.slice/system-dirsrv.slice/dirsrv@deploy.service
           +-4761   /usr/sbin/ns-slapd   -D   /etc/dirsrv/slapd-deploy   -i
/var/run/dirsrv/slapd-deploy.pid


[root@openldap-gdpr ~]# stop-dirsrv
Stopping instance "deploy"
```

3.4 Ρυθμίσεις προετοιμασίας Directory Server 389

Η ενεργοποίηση της κρυπτογράφησης πεδίου στον DS 389 απαιτεί να έχει ενεργοποιηθεί πρώτα η λειτουργικότητα Transport Layer Security (TLS) στον εξυπηρετητή καταλόγου διότι η κρυπτογράφηση πεδίου χρησιμοποιεί το κλειδί κρυπτογράφησης TLS του διακομιστή και τις ίδιες μεθόδους εισαγωγής PIN με το TLS. Ο κωδικός PIN πρέπει να εισαχθεί χειροκίνητα κατά την εκκίνηση του διακομιστή ή πρέπει να χρησιμοποιηθεί ένα αρχείο PIN [6].

Τα τυχαία παραγόμενα συμμετρικά κλειδιά κρυπτογράφησης χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Αυτά τα κλειδιά διαμορφώνονται χρησιμοποιώντας το δημόσιο κλειδί από το πιστοποιητικό TLS του διακομιστή και το προκύπτον κλειδί αποθηκεύεται στα αρχεία διαμόρφωσης του διακομιστή. Η πραγματική ισχύς της κρυπτογράφησης πεδίου δεν είναι ποτέ μεγαλύτερη από την ισχύ του κλειδιού TLS του διακομιστή που χρησιμοποιείται για την παραπάνω διαδικασία. Χωρίς πρόσβαση στο ιδιωτικό κλειδί του διακομιστή, δεν είναι δυνατή η ανάκτηση των συμμετρικών κλειδιών από τα αντίγραφα που δημιουργούνται.

Οι κρυπτογραφικές υπηρεσίες στον DS 389 παρέχονται από τα Mozilla Network Security Services (NSS), οι οποίες αποτελούν ένα σύνολο βιβλιοθηκών που υποστηρίζουν μεταξύ άλλων τη λειτουργικότητα TLS και κάποιες βασικές κρυπτογραφικές λειτουργίες. Το NSS περιέχει μια υλοποίηση λογισμικού για κρυπτογραφικό δείγμα (cryptographic token) η οποία είναι πιστοποιημένη με το πρότυπο Federal Information Processing Standard (FIPS). Στη συνέχεια, παρατίθενται τα απαραίτητα βήματα σχετικά με τη δημιουργία και την εισαγωγή πιστοποιητικών στη βάση δεδομένων NSS καθώς και η διαδικασία της ενεργοποίησης του TLS [7].

1. Έλεγχος ότι υπάρχει NSS database για Directory Server:

```
[root@openldpap-gdpr ~]# ls -l /etc/dirsrv/slapd-openldpap-gdpr/*.db
-rw-rw----. 1 dirsrv dirsrv 65536 Apr  8 20:16 /etc/dirsrv/slapd-
openldpap-gdpr/cert8.db
-rw-rw----. 1 dirsrv dirsrv 16384 Apr  8 20:16 /etc/dirsrv/slapd-
openldpap-gdpr/key3.db
-rw-rw----. 1 dirsrv dirsrv 16384 Apr  8 22:25 /etc/dirsrv/slapd-
openldpap-gdpr/secmod.db
```

- Σε όλες τις περιπτώσεις που χρειάζεται η αναφορά στο εγκατεστημένο στιγμιότυπο του λογισμικού θα αναφερόμαστε στο /etc/dirsrv/slapd-openldpap-gdpr/ όπως προέκυψε κατά τη φάση της εγκατάστασης. Στη γενική περίπτωση θα είναι /etc/dirsrv/<slapd-instance_name>/.

Σε περίπτωση που δεν υπάρχει, δημιουργούμε νέα NSS:

```
[root@openldpap-gdpr ~]# certutil -d /etc/dirsrv/slapd-openldpap-
gdpr/ -N

Enter a password which will be used to encrypt your keys.
The password should be at least 8 characters long,
and should contain at least one non-alphabetic character.

Enter new password:
Re-enter password:
```

2. Δημιουργία Αιτήματος Υπογραφής Πιστοποιητικού (Certificate Signing Request - CSR):

```
[root@openldpap-gdpr ~]# certutil -d /etc/dirsrv/slapd-instance_name/
-R -g 4096 -a \
-o /root/openldap-gdpr.csr -8 openldap-gdpr.att.sch.gr \
-s "CN=openldap-gdpr.att.sch.gr,O=att,OU=SCH,C=GR"
```

Το αίτημα στάλθηκε στην DigiCert, εγκρίθηκε και έγινε λήψη του πιστοποιητικού του ε-ξυπηρετητή και της αρχής πιστοποίησης (CA), που έκανε την υπογραφή, σε ένα αρχείο zip το οποίο περιέχει δύο αρχεία.

3. Εισαγωγή πιστοποιητικών:

```
[root@openldpap-gdpr ~]# certutil -d /etc/dirsrv/slapd-instance_name/
-A –n “Digi” \
-t "C,," –i Digi.crt
[root@openldpap-gdpr ~]# certutil -d /etc/dirsrv/slapd-instance_name/
-A –n “server-cert”\  -t "u,u,u" –i server.crt
```

Ο έλεγχος των υπαρχόντων πιστοποιητικών στη βάση πιστοποιητικών NSS γίνεται με χρήση της παρακάτω εντολής:

```
[root@openldpap-gdpr ~]# certutil -K /etc/dirsrv/slapd-instance_name/
certutil: Checking token "NSS Certificate DB" in slot "NSS User Pri-
vate Key and Certificate Services"
Enter Password or Pin for "NSS Certificate DB":Enter Password or Pin
for "NSS Certificate DB":
< 0> rsa      296823034b807fddbed041ccb7acb34e476f29a6   NSS Certifi-
cate DB:server-cert
```

Σημείωση: Η εγγραφή «NSS Certificate DB:server-Cert» ορίζει το κλειδί (key) (εν είδει key-value) ή το ψευδώνυμο (nickname) που θα χρησιμοποιηθεί για πιστοποιητικό.

```
[root@openldpap-gdpr ~]# certutil -L -d /etc/dirsrv/slapd-openldpap-
gdpr/ -n server-cert
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:24:c1:a6:0c:8c:3c:65:5c:42:64:3e:e2:f2:d4:4b
        Signature Algorithm: PKCS #1 SHA-256 With RSA Encryption
        Issuer: "CN=TERENA SSL CA 3,O=TERENA,L=Amsterdam,ST=Noord-
Holland,C=N
            L"
        Validity:
            Not Before: Thu Dec 19 00:00:00 2019
            Not After: Wed Dec 23 12:00:00 2020
        Subject: "CN=openldap-gdpr.att.sch.gr,O=Greek School Net-
work,L=Rio,C=
            GR"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    d8:e7:24:2a:ea:c1:68:6f:28:2a:8d:1c:45:ef:a7:b2:
                    15:f9:81:a3:13:0a:bf:3d:3f:cc:f0:6e:a8:31:5a:90:
                    cb:04:c9:46:ea:54:8b:10:84:0f:18:8e:e3:2c:e5:5f:
                    53:1c:98:25:34:7a:c1:2d:11:41:81:f4:4c:f8:77:f0:
                    e3:1e:83:f5:c8:23:1f:39:78:5e:45:d7:b5:c8:50:ff:
                    48:d7:7a:70:79:b6:8a:28:5c:10:b8:85:5e:af:98:5e:
                    19:db:7c:67:27:7b:45:41:51:f2:6b:19:9a:fe:10:c6:
                    4c:cd:b2:35:86:6b:0f:24:aa:c1:e8:b9:08:65:9b:09:
                    cf:d5:6d:77:a1:6a:44:01:89:96:a7:b7:a2:30:18:e2:
                    c4:d1:da:3e:90:af:20:c9:30:23:99:44:b7:6a:cc:49:
                    16:70:64:82:58:8b:bd:b7:8b:68:96:2d:d4:2d:25:37:
                    a3:7d:49:b1:a1:1e:5f:de:d8:f7:7c:27:26:0a:a1:95:
                    2c:4c:66:55:9e:5d:cb:e0:e2:57:f1:ed:4b:05:34:6c:
                    8e:07:fb:a0:5b:14:33:67:22:83:3f:68:c0:fa:1e:af:
                    6d:dd:9a:74:92:cb:9a:63:57:24:e5:b0:df:49:36:21:
                    ea:8b:10:53:59:0d:05:d5:e5:29:26:7c:34:c7:c3:13
                Exponent: 65537 (0x10001)
        Signed Extensions:
            Name: Certificate Authority Key Identifier
            Key ID:
                67:fd:88:20:14:27:98:c7:09:d2:25:19:bb:e9:51:11:
                63:75:50:62

            Name: Certificate Subject Key ID
            Data:
                dd:37:c6:c0:34:80:27:b5:e2:d4:3c:5e:a4:59:c3:96:
                d1:4a:82:54

            Name: Certificate Subject Alt Name
            DNS name: "openldap-gdpr.att.sch.gr"
            DNS name: "www.openldap-gdpr.att.sch.gr"

            Name: Certificate Key Usage
            Critical: True
            Usages: Digital Signature
                    Key Encipherment

            Name: Extended Key Usage
                TLS Web Server Authentication Certificate
                TLS Web Client Authentication Certificate

            Name: CRL Distribution Points
```

```
            Distribution point:
                URI: "http://crl3.digicert.com/TERENASSLCA3.crl"
            Distribution point:
                URI: "http://crl4.digicert.com/TERENASSLCA3.crl"

            Name: Certificate Policies
            Data:
                Policy Name: OID.2.16.840.1.114412.1.1
                    Policy Qualifier Name: PKIX CPS Pointer Qualifier
                    Policy Qualifier Data:
"https://www.digicert.com/CPS"
                Policy Name: OID.2.23.140.1.2.2

            Name: Authority Information Access
            Method: PKIX Online Certificate Status Protocol
            Location:
                URI: "http://ocsp.digicert.com"
            Method: PKIX CA issuers access method
            Location:
                URI: "http://cacerts.digicert.com/TERENASSLCA3.crt"

            Name: Certificate Basic Constraints
            Critical: True
            Data: Is not a CA.

            Name: OID.1.3.6.1.4.1.11129.2.4.2
            Data:
                00:f1:00:77:00:a4:b9:09:90:b4:18:58:14:87:bb:13:
                a2:cc:67:70:0a:3c:35:98:04:f9:1b:df:b8:e3:77:cd:
                0e:c8:0d:dc:10:00:00:01:6f:1f:8d:79:ae:00:00:04:
                03:00:48:30:46:02:21:00:f5:d5:32:c5:4d:35:ca:26:
                23:3c:12:a6:fc:e9:9d:d1:c0:ea:81:fc:52:7f:b9:57:
                0a:71:89:e0:a6:20:f5:2f:02:21:00:9c:82:4e:79:3f:
                79:16:5a:9e:a3:58:51:b3:5b:f1:0a:96:89:d4:08:cf:
                24:c9:b8:cc:cb:61:d4:82:8a:d5:d2:00:76:00:5e:a7:
                73:f9:df:56:c0:e7:b5:36:48:7d:d0:49:e0:32:7a:91:
                9a:0c:84:a1:12:12:84:18:75:96:81:71:45:58:00:00:
                01:6f:1f:8d:79:5b:00:00:04:03:00:47:30:45:02:20:
                0e:83:11:4f:99:fd:ac:88:f2:d9:47:ae:93:7a:28:a5:
                e3:c1:71:d5:69:75:0c:fd:0b:c6:e2:8c:d2:35:e8:9f:
                02:21:00:d7:99:dc:a6:31:fd:09:85:4c:35:ee:2a:04:
                e9:40:e1:f7:9d:e4:69:8c:41:9f:57:1e:d5:26:3a:22:
                db:3d:a4

    Signature Algorithm: PKCS #1 SHA-256 With RSA Encryption
    Signature:
        87:bc:29:43:65:0a:2b:d6:b2:ee:ee:23:66:6f:63:0a:
        06:3b:83:01:bb:31:1a:3a:fa:fe:28:2c:71:e4:00:ee:
        6e:6c:39:10:45:9a:85:0e:72:47:ee:e2:32:6a:13:8e:
        45:54:61:79:9d:c6:6e:de:39:1b:14:5a:8c:7f:82:5f:
        90:91:e9:24:91:34:d5:54:2c:a2:36:ca:c1:0b:8e:f2:
        7b:b8:44:d9:bf:59:01:24:59:90:37:62:be:ef:74:66:
        30:18:fc:df:8c:6a:d0:80:46:b0:3f:54:45:85:a3:12:
        63:af:a3:5a:1d:15:4a:a4:e6:4f:2b:b3:7c:ee:53:a3:
        c1:0f:76:16:76:34:85:77:ca:47:14:2b:3f:f5:e9:19:
        71:9e:b0:d8:6d:4c:d1:6d:22:63:f5:d7:04:bf:5e:e7:
        0b:de:ba:4b:40:f3:43:99:dd:f3:a4:14:51:68:23:66:
        0e:a3:65:24:89:23:0a:9b:bb:6b:48:f0:80:5a:88:b3:
        08:18:f0:95:a5:8c:9b:ae:e0:8d:16:97:3d:82:8f:ef:
        cc:b8:ce:35:41:26:16:2b:84:a8:78:98:d8:dd:41:a3:
        3e:d9:60:ba:61:df:79:84:58:35:c6:e4:3b:f9:a6:90:
```

```
        25:d8:44:f2:fd:1b:33:85:25:0b:3e:2a:6e:94:07:01
    Fingerprint (SHA-256):

86:A5:9A:5B:72:EA:21:24:53:0C:A8:66:3C:A0:D4:97:0B:03:C5:76:FC:4D:A2:
86:24:E3:85:A9:EB:54:71:39
    Fingerprint (SHA1):
        96:04:F8:AE:C6:DE:0E:AB:D1:15:E7:0B:AA:CC:DE:08:96:5E:0D:FF
    Mozilla-CA-Policy: false (attribute missing)
    Certificate Trust Flags:
        SSL Flags:
            User
        Email Flags:
            User
        Object Signing Flags:
            User
```

Εάν υπάρχει σκοπός να προστατεύεται το αποθετήριο των NSS και ο Directory Server να ξεκινάει αυτόματα χωρίς την παρέμβαση διαχειριστή, τότε χρειάζεται να έχει αποθηκευτεί το PIN σε αρχείο και ειδικότερα στο /etc/dirsrv/slapd-openldpap-gdpr/pin.txt. Είναι φανερό, λοιπόν, ότι κάτι τέτοιο μειώνει κατά πολύ την ασφάλεια του περιβάλλοντος λειτουργίας και μπορεί να αποτελεί λύση μόνο σε περίπτωση με κρυπτογραφημένο αρχείο συστήματος (File System).

4. Ενεργοποίηση TLS και LDAPS:

Πλέον είναι δυνατό να γίνει ενεργοποίηση TLS στον κατάλογο με τη ρύθμιση - ενεργοποίηση της οικογένειας κρυπτογράφησης RSA (cipher family), τη ρύθμιση της χρήσης του NSS database security device από τον DS 389 και του συμβολικού ονόματος του πιστοποιητικού, όπως φαίνεται παρακάτω:

```
[root@openldpap-gdpr ~]# ldapadd -D "cn=Directory Manager" -W -p 389
-h openldap-gdpr.att.sch.gr –x \
dn: cn=config
changetype: modify
replace: nsslapd-securePort
nsslapd-securePort: 636
-
replace: nsslapd-security
nsslapd-security: on
```

```
[root@openldpap-gdpr ~]# ldapadd -D "cn=Directory Manager" -W -p 389
-h openldap-gdpr.att.sch.gr –x \
dn: cn=RSA,cn=encryption,cn=config
cn: RSA
objectClass: top
objectClass: nsEncryptionModule
nsSSLToken: internal (software)
nsSSLPersonalitySSL: server-cert
nsSSLActivation: on
```

Εάν για κάποιο λόγο έχουν γίνει στο παρελθόν ρυθμίσεις, κάνουμε τις παρακάτω τροποποιήσεις:

```
[root@openldpap-gdpr ~]# ldapadd -D "cn=Directory Manager" -W -p 389
-h openldap-gdpr.att.sch.gr –x \
dn: cn=RSA,cn=encryption,cn=config
changetype: modify
replace: nsSSLToken
nsSSLToken: internal (software)
-
replace: nsSSLPersonalitySSL
nsSSLPersonalitySSL: server-cert
-
replace: nsSSLActivation
nsSSLActivation: on
```

και επανεκκινούμε τον 389 Directory Server με την παρακάτω εντολή:

```
[root@openldpap-gdpr ~]# systemctl restart dirsrv.target
```

Μετά την εκτέλεση των παραπάνω, θα πρέπει η παρακάτω εντολή να επιστρέφει κάποιο αποτέλεσμα:

```
[root@openldpap-gdpr ~]# ldapsearch -H ldaps://openldap-
gdpr.att.sch.gr:636 -D "cn=Directory Manager" -LLL -w 'password' -b
"dc=sch, dc=gr"
dn: dc=sch,dc=gr
objectClass: top
objectClass: domain
dc: sch
```

Κεφάλαιο 4

Εισαγωγή δεδομένων

Για την επιτυχημένη εισαγωγή των δεδομένων στη βάση θα χρησιμοποιηθούν πραγματικά δεδομένα τα οποία δεν αναφέρονται σε πρόσωπα αλλά σε σχολεία, για να αποφευχθεί οποιαδήποτε επιπλοκή χειρισμού προσωπικών δεδομένων. Ωστόσο, προκειμένου να καλυφθεί ένα ευρύτερο φάσμα πραγματικών περιπτώσεων και λειτουργιών χρήσης, κρίθηκε απαραίτητο να παραχθούν -και κατ' επέκταση να εισαχθούν- 1.000.000 χρήστες βάσει ενός προτύπου που εξήχθη από αρχείο πραγματικών χρηστών. Σε αυτό το σημείο πρέπει να τονιστεί ότι τα αρχεία σχήματος, βάσει των οποίων χτίστηκε το τελικό σχήμα στο DS 389, παραχωρήθηκαν από το ΠΣΔ. Σε αυτό το κεφάλαιο παρουσιάζονται τα βήματα που ακολουθήθηκαν για την επιτυχή εισαγωγή των δεδομένων στη βάση.

4.1 Μετατροπή αρχείων σχήματος

Μετατρέπουμε τα αρχεία core.schema, dyngroup.schema, qmail.schema, radiusprofile.schema και sch.schema σε ldif κάνοντας χρήση του perl script schema-script.pl. Για την πλήρη μορφή του παραπάνω script βλ. «Κώδικας 1» σελ. 71 στο Παράρτημα. Κάποιες από τις συντακτικές διαφορές των τύπων αρχείων schema και ldif φαίνονται στον πίνακα 4.1:

	schema	**ldif**
Πρώτη γραμμή	-	dn: cn=schema
Μεταβλητή ορισμού χαρακτηριστικών	attributetype	attributeTypes:
Μεταβλητή ορισμού κλάσεων	objectclass	objectClasses:

Πίνακας 4.1

Τα νέα αρχεία ldif μετονομάστηκαν σε 60core.ldif, 60qmail.ldif, 60sch.ldif, 60dyngroup.ldif και 60radiusprofile.ldif, αντίστοιχα. Η παραπάνω μετονομασία είναι υποχρεωτική για τα αρχεία που χρησιμοποιούνται για την επέκταση του σχήματος, καθώς πρέπει να ακολουθούν την εξής μορφή: **[1-9][0-9]text.ldif**. Η εξήγηση για το παραπάνω έγκειται στο γεγονός ότι ο Διακομιστής Καταλόγου καταγράφει το νέο σχήμα στο αρχείο με το μεγαλύτερο αριθμητικό και αλφαβητικό όνομα και αναμένει αυτό το αρχείο να είναι το **99user.ldif** [9]. Σε διαφορετική περίπτωση, ο διακομιστής ενδέχεται να αντιμετωπίσει προβλήματα.

4.2 Μεταφορά αρχείων σχήματος

Εν συνεχεία, μεταφέρουμε τα πέντε παραπάνω αρχεία ldif στην τοποθεσία /etc/dirsrv/slapd-openldpap-gdpr/schema και επανεκκίνηση του Directory Server ή δυναμική ανανέωση του σχήματος.

- **Επανεκκίνηση του Διακομιστή Καταλόγου**:

```
[root@openldpap-gdpr ~]# systemctl stop dirsrv.target
[root@openldpap-gdpr ~]# systemctl start dirsrv.target
```

- **Δυναμική ανανέωση του σχήματος**:

```
[root@openldpap-gdpr ~]# schema-reload.pl -D "cn=Directory Manager"
-w 'password' -P LDAP
```

4.3 Διόρθωση αρχείων σχήματος

Επειδή κάποια από τα αρχεία σχήματος είχαν λάθη στον ορισμό μερικών χαρακτηριστικών τα οποία δεν επέτρεπαν στον Directory Server 389 να εκκινήσει, χρειάστηκε να διορθωθούν χειροκίνητα. Για παράδειγμα, το χαρακτηριστικό με όνομα «mailMessageStore» του αρχείου 60qmail.ldif χρειάστηκε αλλαγή του Αριθμού Αναγνωριστικού Αντικειμένου (Object Identifier Number, OID) από 1.3.6.1.4.1.7914.1.2.1.3 σε 2.16.840.1.113730.3.1.19 [8]. Στη σελ. 78 στο Παράρτημα παρατίθεται, ενδεικτικά, το αρχείο σχήματος 60core.ldif με την ονομασία «Κώδικας 2».

4.4 Επεξεργασία αρχείου δεδομένων προς εισαγωγή

Το αρχείο foo.ldif, αρχικά, περιείχε πληροφορίες για περίπου 19.000 σχολεία / εκπαιδευτικά ιδρύματα και κάποιες χιλιάδες χρήστες. Επειδή αυτή η διπλωματική εργασία αποσκοπεί στην προστασία και την κρυπτογράφηση των προσωπικών δεδομένων, κρίθηκε απαραίτητο να διαγραφεί κάθε πεδίο σχετικό με πρόσωπα / προσωπικά δεδομένα.

Ως εκ τούτου, κάνοντας χρήση της παρακάτω εντολής, λήφθηκε το τελικό αρχείο δεδομένων foo_final.ldif που περιέχει μόνο σχολεία και εκπαιδευτικά ιδρύματα:

```
[root@openldpap-gdpr ~]# sed '/dn: uid=/,/^$/d' /home/dkalo/foo.ldif >
foo_final.ldif
```

Η τελευταία τροποποίηση του αρχείου προς εισαγωγή είχε να κάνει με το παρακάτω πρόβλημα στα πεδία postalCode και postalAddress.

- Χειρισμός κενών ή μηδενικών πεδίων: Κάποια σχολεία δεν μπορούσαν να εισαχθούν στη βάση δεδομένων καθώς είτε είχαν postalCode: 0 ή το πεδίο postalAddress ήταν κενό. Έτσι, για την επίλυση αυτού του ζητήματος έγινε τροποποίηση του foo_final.ldif βάζοντας όπου postalCode: 0 → postalCode: 44444 και όπου postalAddress: κενό → postalAddress: aaaaa.

4.5 Δημιουργία κλαδιών για την εισαγωγή των σχολείων

Για την εισαγωγή των δεδομένων στην βάση, έπρεπε να δημιουργηθεί αρχικά ένα κλαδί με το όνομα ou = Units (ou: organizational unit) που θα περιέχει όλα τα δεδομένα προς εισαγωγή.

Ύστερα, έπρεπε να δημιουργηθούν τόσα κλαδιά όσα και τα διαφορετικά ou κάτω από το ou = Units. Για παράδειγμα, για την επιτυχημένη εισαγωγή του σχολείου με dn: ou=gym-astrous, ou=ark, ou=Units, dc=sch, dc=gr έπρεπε να δημιουργηθεί κάτω από το ou=Units το κλαδί ou=ark.

Το αρχείο 60add.ldif με τα παραπάνω κλαδιά βρίσκεται στο Παράρτημα στη σελ. 93 με την ονομασία «Κώδικας 3».

4.6 Παραγωγή 1.000.000 χρηστών

Αρχικά, σχεδιάστηκε ένα script που λειτουργεί ως πρότυπο με 28 πεδία για τους χρήστες. Τα 28 πεδία επιλέχθηκαν ως ελάχιστος αριθμός απαιτούμενων πεδίων, ώστε να συμπεριλαμβάνονται κάποιες βασικές πληροφορίες για τον κάθε χρήστη αλλά και τα απαραίτητα πεδία που απαιτούνται από το συντακτικό / σχήμα του DS 389:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/template28.sh

#!/bin/bash
exec >> $2
echo "#"
echo "dn: uid=user$1,ou=people,dc=sch,dc=gr"
echo "objectClass: top"
echo "userPassword::
e1NTSEF9aEs0SE53ZDEzQnkrVlhta3FPZjhMUkFrelBRZkZwNEZSeHc2QkE9PQ=
 ="
echo "umdValidatorsName: uid=uoa,ou=people,dc=sch,dc=gr"
echo "umdValidateTimestamp: 20180226081925Z"
echo "objectClass: radiusprofile"
echo "objectClass: organizationalPerson"
```

```
echo "objectClass: eduPerson"
echo "objectClass: qmailUser"
echo "objectClass: umdManagedObject"
echo "objectClass: gsnUser"
echo "objectClass: person"
echo "objectClass: inetOrgPerson"
echo "umdPasswordRecoveryHash;ts: 1519489000"
echo "ou;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "sn;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "cn;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "accountStatus: active"
echo "eduPersonOrgDN: dc=sch,dc=gr"
echo "eduPersonAffiliation;lang-en: staff"
echo "mail: mail@user$1-kk.voi.sch.gr"
echo "uid: user$1"
echo "umdObject: Account"
echo "gsnCreateTimeStamp: 20020326142639Z"
echo "gsnCreatorsName: uid=root,dc=sch,dc=gr"
echo "mailQuotaSize: 6000000000"
echo "mailQuotaCount: 15000"
echo "businessCategory;lang-en: PROTOVATHMIA"
echo ""
echo ""
```

Εν συνεχεία, σχεδιάστηκε ένα δεύτερο script το οποίο παράγει 1.000.000 χρήστες, σε 20 πακέτα των 50.000 χρηστών το καθένα, βάσει του προηγούμενου προτύπου:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/generate_us-
ers.sh

#!/bin/bash

for i in {1..50000}
do
       ./template$1.sh $i data1.ldif
done

for i in {50001..100000}
do
       ./template$1.sh $i data2.ldif
done
for i in {100001..150000}
do
       ./template$1.sh $i data3.ldif
done
for i in {150001..200000}
do
       ./template$1.sh $i data4.ldif
done
for i in {200001..250000}
do
       ./template$1.sh $i data5.ldif
done

for i in {250001..300000}
do
       ./template$1.sh $i data6.ldif
done
```

```
for i in {300001..350000}
do
       ./template$1.sh $i data7.ldif
done

for i in {350001..400000}
do
       ./template$1.sh $i data8.ldif
done

for i in {400001..450000}
do
       ./template$1.sh $i data9.ldif
done

for i in {450001..500000}
do
       ./template$1.sh $i data10.ldif
done

for i in {500001..550000}
do
       ./template$1.sh $i data11.ldif
done

for i in {550001..600000}
do
       ./template$1.sh $i data12.ldif
done

for i in {600001..650000}
do
       ./template$1.sh $i data13.ldif
done

for i in {650001..700000}
do
       ./template$1.sh $i data14.ldif
done

for i in {700001..750000}
do
       ./template$1.sh $i data15.ldif
done

for I in {750001..800000}
do
       ./template$1.sh $i data16.ldif
done

for I in {800001..850000}
do
       ./template$1.sh $i data17.ldif
done

for I in {850001..900000}
do
       ./template$1.sh $i data18.ldif
done
for I in {900001..950000}
do
```

```
        ./template$1.sh $i data19.ldif
done
for I in {950001..1000000}
do
        ./template$1.sh $i data20.ldif
done
```

Παράλληλα, κρίθηκε αναγκαίο να εξεταστεί και η περίπτωση στην οποία τα πεδία των χρηστών είναι περισσότερα, για να διαπιστωθεί αν παίζει κάποιο ρόλο στην απόδοση του συστήματος ο αριθμός των πεδίων. Με τη χρήση του παρακάτω προτύπου εξετάστηκε και η περίπτωση κατά την οποία ο αριθμός των πεδίων των χρηστών ανέρχεται στα 66, που είναι ο μέγιστος αριθμός πεδίων που εξήχθη από πραγματικά δεδομένα για τους χρήστες:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/template66.sh

#!/bin/bash

exec >> $2
echo "#"
echo "dn: uid=user$1,ou=people,dc=sch,dc=gr"
echo "objectClass: top"
echo "userPassword::
e1NTSEF9aEs0SE53ZDEzQnkrVlhta3FPZjhMUkFrelBRZkZwNEZSeHc2QkE9PQ=
 ="
echo "umdValidatorsName: uid=uoa,ou=people,dc=sch,dc=gr"
echo "umdValidateTimestamp: 20180226081925Z"
echo "objectClass: radiusprofile"
echo "objectClass: organizationalPerson"
echo "objectClass: eduPerson"
echo "objectClass: qmailUser"
echo "objectClass: umdManagedObject"
echo "objectClass: gsnUser"
echo "objectClass: person"
echo "objectClass: inetOrgPerson"
echo "umdPasswordRecoveryHash;ts: 1519400000"
echo "mailHost: msa6.att.sch.gr"
echo "mysqlPassword: %xb%jeq5;userdb1"
echo "ou;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "ou:: Oc6/IM6Uz-
pfOnM6fzqTOmc6azp8gzqPOp86fzpvOlc6Zzp8gzpvOmc6SzpHOlM6VzpnOkc6j"
echo "description;lang-en: 9o DIMOTIKO SCHOLEIO LIVADEIAS"
echo "description:: Oc6/IM6Uz-
pfOnM6fzqTOmc6azp8gzqPOp86fzpvOlc6Zzp8gzpvOmc6SzpHOlM6V
 zpnOkc6j"
echo "sn;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "cn;lang-en: 9o DIMOTIKO SCHOLEIO"
echo "sn:: Oc6/IM6Uz-
pfOnM6fzqTOmc6azp8gzqPOp86fzpvOlc6Zzp8gzpvOmc6SzpHOlM6VzpnOkc6j"
echo "cn:: Oc6/IM6Uz-
pfOnM6fzqTOmc6azp8gzqPOp86fzpvOlc6Zzp8gzpvOmc6SzpHOlM6VzpnOkc6j"
echo "physicalDeliveryOfficeName;lang-en: EPISIMOS LOGARIASMOS"
echo "physicalDeliveryOfficeName::
zpXOoM6ZzqPOl86czp/OoyDOm86fzpPOkc6hzpnOkc6jzpzOn
 86j"
echo "deliveryProgramPath: preline -f deliver -d user$1"
echo "accountStatus: active"
```

```
echo "eduPersonOrgDN: dc=sch,dc=gr"
echo "ftpQuota: false,hard,1.000.000000,-1,-1,0,0,0"
echo "eduPersonAffiliation;lang-en: staff"
echo "mailMessageStore: /users/voi/user$1-kk/user$1/Maildir/"
echo "mail: mail@user$1-kk.voi.sch.gr"
echo "uid: user$1"
echo "umdObject: Account"
echo "mailAlternateAddress: user$1@sch.gr"
echo "eduPersonOrgUnitDN: ou=user$1-kk,ou=voi,ou=units,dc=sch,dc=gr"
echo "eduPersonOrgUnitDN: ou=voi,ou=units,dc=sch,dc=gr"
echo "qmailGID: 1000"
echo "deliveryMode: nolocal"
echo "givenName:: IA=="
echo "homeDirectory: /users/voi/user$1-kk/user$1/"
echo "confirm: CONFIRMED"
echo "facsimileTelephoneNumber: 0260000000"
echo "l: ou=user$1-kk,ou=voi,ou=units,dc=sch,dc=gr"
echo "qmailUID: 10000"
echo "eduPersonAffiliation: staff"
echo "labeledURI: user$1-kk.voi.sch.gr"
echo "gsnCreateTimeStamp: 20020326142639Z"
echo "gsnCreatorsName: uid=root,dc=sch,dc=gr"
echo "mailQuotaSize: 6000000000"
echo "mailQuotaCount: 15000"
echo "businessCategory:: zqDOoc6pzqTOn86SzpHOmM6czpnOkQ=="
echo "businessCategory:: zpXOms6gzpHOmc6UzpX-
Opc6kzpnOms6XIM6czp/Onc6RzpTOkSAtIM6Vzpw
 ="
echo "businessCategory:: zpTOl86czp/Oo86ZzpE="
echo "businessCategory;lang-en: PROTOVATHMIA"
echo "businessCategory;lang-en: EKPAIDEFTIKI MONADA - EM"
echo "businessCategory;lang-en: DIMOSIA"
echo "mobile: 6970000000"
echo "umdPasswordRecoveryMail: user$1@gmail.com"
echo "telephoneNumber: 0260000000"
echo "title:: zpTOl86czp/OpM6ZzprOnyAtIM6UzpfOnA=="
echo "title:: zp/Om86fzpfOnM6VzqHOnw=="
echo "title;lang-en: DIMOTIKO - DIM"
echo "title;lang-en: OLOIMERO"
echo «»
echo «»
```

4.7 Δημιουργία κλαδιού για την εισαγωγή των χρηστών

Για την εισαγωγή των δεδομένων που αφορούν τους χρήστες στη βάση έπρεπε να δημιουργηθεί ένα κλαδί με το όνομα ou = People που θα περιέχει όλα τα δεδομένα προς εισαγωγή.

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/add_people.ldif

dn: ou=People,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: People
```

4.8 Εισαγωγή σχολείων και χρηστών

Μετά από τα παραπάνω βήματα είναι πλέον εφικτή η εισαγωγή των δεδομένων στη βάση. Για την εισαγωγή των σχολείων (με παράλληλη χρονομέτρηση της διαδικασίας της εισαγωγής) έγινε χρήση του παρακάτω script:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/im-
port_schools.sh

#!/bin/bash

time ldapadd -x -D "cn=Directory Manager" -w 'password' -f 60add.ldif
time ldapadd -x -D "cn=Directory Manager" -w 'password' -f foo_final.ldif
```

Για την εισαγωγή των χρηστών (με παράλληλη χρονομέτρηση της διαδικασίας της εισαγωγής) έγινε χρήση του παρακάτω script:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/import_users.sh

#!/bin/bash

time ldapadd -x -D "cn=Directory Manager" -w 'password' -f add_people.ldif

for I in {1..20}
do
       time ldapadd -x -D "cn=Directory Manager" -w 'password' -f
data$i.ldif > time$i.txt
       rm time$i.txt
done
```

Κεφάλαιο 5

Κρυπτογράφηση πεδίου

5.1 Αλγόριθμος κρυπτογράφησης AES

5.1.1 Ιστορική αναδρομή

Ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση πεδίου είναι ο AES (Advanced Encryption Standard). Ο αλγόριθμος AES είναι ένας από τους αλγόριθμους κρυπτογράφησης μπλοκ που δημοσιεύθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology) το 2000. Οι κύριοι στόχοι αυτού του αλγορίθμου ήταν να αντικαταστήσει τον αλγόριθμο DES αφού εμφανίστηκαν ορισμένες ευπαθείς πτυχές του. Το NIST κάλεσε ειδικούς που εργάζονται για την κρυπτογράφηση και την ασφάλεια δεδομένων σε όλο τον κόσμο για να εισαγάγουν έναν καινοτόμο αλγόριθμο κρυπτογράφησης μπλοκ για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων με ισχυρή και περίπλοκη δομή.

Το NIST δέχτηκε πέντε αλγόριθμους για αξιολόγηση και μετά την εφαρμογή διάφορων κριτηρίων και παραμέτρων ασφαλείας επέλεξαν έναν από τους πέντε αλγόριθμους κρυπτογράφησης που πρότειναν οι Βέλγοι κρυπτογράφοι Joan Daeman και Vincent Rijmen. Το αρχικό όνομα του αλγορίθμου AES ήταν αλγόριθμος Rijndel, ωστόσο, αυτό το όνομα δεν επικράτησε και έτσι αναγνωρίζεται ως αλγόριθμος Προηγμένου Προτύπου Κρυπτογράφησης (AES).

5.1.2 Χαρακτηριστικά αλγόριθμου AES

Ένα από τα σημαντικότερα κριτήρια για την επιλογή κατάλληλου αλγόριθμου από το NIST ήταν η ασφάλεια. Οι κύριοι λόγοι πίσω από αυτό είναι προφανείς καθώς ο στόχος του AES ήταν να βελτιώσει τα ζητήματα ασφαλείας του αλγόριθμου DES. Ο AES έχει την καλύτερη ικανότητα στο να προστατεύει ευαίσθητα δεδομένα από εισβολείς και δεν τους επιτρέπει να σπάσουν τα κρυπτογραφημένα δεδομένα σε αντίθεση με άλλους αλγόριθμους, όπως οι DES, 3DES, RC2, RC6.

Ένα άλλο κριτήριο στο οποίο δόθηκε έμφαση από το NIST για την αξιολόγηση των αλγορίθμων ήταν το κόστος. Οι λόγοι πίσω από αυτή την απόφαση είναι σαφείς και σχετικοί, ακόμη μία φορά, με τον αλγόριθμο DES και τη χαμηλή απόδοση του. Ο αλγόριθμος AES έχει, επίσης, επικρατήσει επειδή έχει υψηλή υπολογιστική απόδοση και μπορεί να χρησιμοποιηθεί σε ένα ευρύ φάσμα εφαρμογών, ιδίως σε ευρυζωνικές συνδέσεις με υψηλή ταχύτητα. Τέλος, πρέπει

να σημειωθούν σημαντικές πτυχές όπως η ευελιξία, η απλότητα και η καταλληλότητα του αλγορίθμου για μια μεγάλη ποικιλία υλικού και λογισμικού.

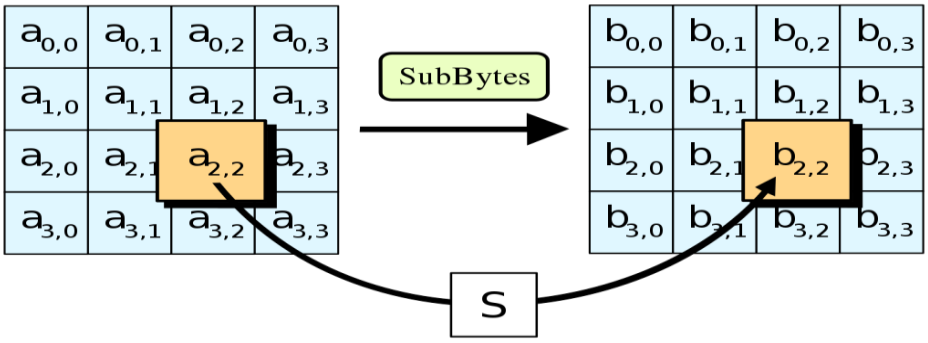
5.1.3 Βασική δομή και διαδικασία κρυπτογράφησης

Ο αλγόριθμος AES βασίζεται σε μία αρχή σχεδιασμού που είναι γνωστή ως δίκτυο αντικατάστασης – μετάθεσης και είναι αποτελεσματική τόσο στον τομέα του λογισμικού όσο και του υλικού. Σε αντίθεση με τον προκάτοχό του, DES, ο αλγόριθμος AES δεν χρησιμοποιεί το δίκτυο Feistel αλλά είναι μια παραλλαγή του Rijndael, με σταθερό μέγεθος μπλοκ 128 bit και μέγεθος κλειδιού 128, 192 ή 256 bit. Το μέγεθος κλειδιού που χρησιμοποιείται για τον αλγόριθμο κρυπτογράφησης AES καθορίζει τον αριθμό των γύρων μετασχηματισμού που μετατρέπουν την είσοδο, που ονομάζεται απλό κείμενο, στην τελική έξοδο, που ονομάζεται κρυπτοκείμενο. Για κλειδιά μεγέθους 128 bit έχουμε 10 γύρους, για κλειδιά μεγέθους 192 bit 12 γύρους και για κλειδιά 256 bit 14 γύρους. Κάθε γύρος αποτελείται από διάφορα στάδια επεξεργασίας, συμπεριλαμβανομένου ενός που εξαρτάται από το ίδιο το κλειδί κρυπτογράφησης. Ένα σύνολο αντίστροφων γύρων εφαρμόζεται για να μετατρέψει το κρυπτοκείμενο πίσω στο αρχικό απλό κείμενο χρησιμοποιώντας το ίδιο κλειδί κρυπτογράφησης.

Ο αλγόριθμος AES χρησιμοποιεί μια συγκεκριμένη δομή για την κρυπτογράφηση δεδομένων για την παροχή της καλύτερης δυνατής ασφάλειας. Για να το πετύχει αυτό βασίζεται σε έναν αριθμό γύρων όπου σε κάθε γύρο υλοποιούνται τέσσερα στάδια, για την κρυπτογράφηση μπλοκ μεγέθους 128 bit.

1. Μετασχηματισμός Αντικατάστασης Bytes

Το πρώτο στάδιο κάθε γύρου ξεκινά με τον μετασχηματισμό SubBytes (Substitute Bytes). Σε αυτό το στάδιο, κάθε byte του πίνακα κατάστασης αντικαθίσταται με ένα SubByte χρησιμοποιώντας το 8 bit S-box, πράγμα το οποίο αποδίδει μη γραμμικότητα στον αλγόριθμο κρυπτογράφησης, Προκειμένου να αποφευχθούν επιθέσεις που βασίζονται σε απλές αλγεβρικές ιδιότητες, το S-box κατασκευάζεται συνδυάζοντας την αντίστροφη λειτουργία με έναν αναστρέψιμο γραμμικό μετασχηματισμό. Παρακάτω παρατίθεται ένα παράδειγμα απεικόνισης της παραπάνω διαδικασίας:



Εικόνα 5.1: Στο βήμα SubBytes, κάθε byte στον πίνακα κατάστασης αντικαθίσταται με την καταχώριση του σε έναν σταθερό πίνακα αναζήτησης 8-bit [14]

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	FA	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	D6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Πίνακας 5.1: Πίνακας μετασχηματισμού **S-box**

Με τη βοήθεια του παραπάνω πίνακα S-box, μπορούμε να βρούμε την έξοδο του πίνακα κατάστασης μετά την εφαρμογή του μετασχηματισμού SubBytes. Αν το byte εισόδου είναι το “xy” σε δεκαεξαδική μορφή, αυτό αντικαθίσταται από το byte που βρίσκεται στη γραμμή “x” και τη στήλη “y” του **Πίνακα 5.**1.

Αν, για παράδειγμα, ο πίνακας εισόδου είναι ο **Πίνακας 5.2**, τότε μετά τον μετασχηματισμό προκύπτει ο **Πίνακας 5.3**, όπως φαίνεται παρακάτω:

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

Πίνακας 5.1

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Πίνακας 5.2

Το "ΕΑ" (σε δεκαεξαδική μορφή) byte αντικαθίσταται από το "87", όπως προκύπτει από τον **Πίνακα 5.1**. Αντίστοιχα, μπορούν να επαληθευτούν και τα υπόλοιπα bytes εξόδου.

2. Μετασχηματισμός ShiftRows

Το επόμενο στάδιο μετά τον μετασχηματισμό SubBytes είναι ο μετασχηματισμός ShiftRows κατά τον οποίο πραγματοποιείται κυκλική ολίσθηση των bytes προς τα αριστερά. Τα bytes της πρώτης γραμμής παραμένουν ως έχουν, της δεύτερης ολισθαίνουν μία θέση προς τα αριστερά, της τρίτης κατά δύο θέσεις, ενώ της τέταρτης κατά τρεις θέσεις.

3. Μετασχηματισμός MixColumns

Για τον μετασχηματισμό MixColumns ακολουθείται η εξής διαδικασία. Ο σταθερός **Πίνακας 5.3** πολλαπλασιάζεται κάθε φορά με μία στήλη του πίνακα που εξήχθη από το προηγούμενο στάδιο. Κατά τον πολλαπλασιασμός μιας γραμμής με την αντίστοιχη στήλη, αντί για τη συνήθη πράξη της πρόσθεσης, χρησιμοποιείται η πράξη XOR.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

Πίνακας 5.3

4. Μετασχηματισμός AddRoundKey

Το τελευταίο στάδιο κάθε γύρου είναι ο μετασχηματισμός AddRoundKey και αποτελεί το σημαντικότερο στάδιο του κρυπταλγόριθμου AES. Σε αυτό το στάδιο, κάθε byte του πίνακα κατάστασης συνδυάζεται με ένα byte του Round Key με μία πράξη XOR. Κάθε Round Key αποτελείται από Nb Ο πίνακας εξόδου του AddRoundKey

Σε συνδυασμό με τα παραπάνω 4 στάδια, αλγόριθμος AES βασίζεται στην επέκταση κλειδιού για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων και αποτελεί αναπόσπαστο κομμάτι του αλγόριθμου.

Επέκταση Κλειδιού

Ο αλγόριθμος AES παίρνει το κλειδί κρυπτογράφησης, K, και εκτελεί μία ρουτίνα επέκτασης κλειδιών για τη δημιουργία του προγράμματος κλειδιού (key schedule). Η επέκταση κλειδιού παράγει ένα σύνολο Nb (Nr + 1) λέξεις σύμφωνα με το γεγονός ότι ο αλγόριθμος απαιτεί ένα αρχικό σύνολο από Nb λέξεις και κάθε ένας από τους Nr γύρους απαιτεί Nb λέξεις από δεδομένα κλειδιού. Το κλειδί κρυπτογράφησης, δηλαδή το αρχικό κλειδί, χρησιμοποιείται για τη δημιουργία των πρώτων τεσσάρων λέξεων και εν τέλει το μέγεθος του κλειδιού αποτελείται από 16 bytes και αναπαρίσταται σε έναν πίνακα 4x4. Μπορούμε να υπολογίσουμε και να βρούμε τα κλειδιά κάθε γύρου κάνοντας χρήση του παρακάτω ψευδοκώδικα [15]:

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
        word temp
        i = 0
        while (i < Nk)
                w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
                i = i+1
        end while

        i = Nk

        while (i < Nb * (Nr+1)]
                temp = w[i-1]
                if (i mod Nk = 0)
                        temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
                else if (Nk > 6 and i mod Nk = 4)
                        temp = SubWord(temp)
                end if
                w[i] = w[i-Nk] xor temp
                i = i + 1
        end while
end
```

Τέλος, υπάρχει και η διαδικασία αποκρυπτογράφησης κατά την οποία γίνεται ανάκτηση των αρχικών δεδομένων που κρυπτογραφήθηκαν και βασίζεται στο κλειδί που ελήφθη από τον αποστολέα των δεδομένων Η διαδικασία αποκρυπτογράφησης του αλγόριθμου AES είναι παρόμοια με την διαδικασία κρυπτογράφησης με την αντίστροφη σειρά.

5.2 Ενεργοποίηση κρυπτογράφησης πεδίου

Προκειμένου να ενεργοποιήσουμε την κρυπτογράφηση πεδίου, πρέπει, αρχικά, να ελέγξουμε αν είναι ενεργοποιημένο το SSL/TLS στον εξυπηρετητή. Για αυτό το σκοπό, ανοίγουμε το αρχείο dse.ldif προς επεξεργασία με την παρακάτω εντολή:

```
[root@openldpap-gdpr ~]# vim /etc/dirsrv/slapd-openldpap-gdpr/dse.ldif
```

Ύστερα αναζητούμε το πεδίο nsslapd-security και ελέγχουμε αν είναι ενεργοποιημένο. Για την αναζήτηση πληκτρολογούμε το παρακάτω ακολουθούμενο από enter:

```
:/nsslapd-security
```

Το nsslapd-security, όταν είναι ενεργοποιημένο, επιτρέπει τη χρήση χαρακτηριστικών ασφαλείας SSL/TLS, καθώς και την κρυπτογράφηση πεδίου [10]. Αναζητώντας αυτό το πεδίο θα εμφανιστεί μία από τις παρακάτω τιμές:

```
:/nsslapd-security: off
```

```
:/nsslapd-security: on
```

Η default τιμή του πεδίου είναι off. Στην περίπτωση αυτή, θα πρέπει να σταματήσουμε τον server με την παρακάτω εντολή και ύστερα να αλλάξουμε την τιμή του πεδίου σε on.

```
[root@openldpap-gdpr ~]# systemctl stop dirsrv.target
```

Τέλος, εκκινούμε ξανά τον server:

```
[root@openldpap-gdpr ~]# systemctl start dirsrv.target
```

Αν το πεδίο έχει εξαρχής την τιμή on, τότε δε χρειάζεται να πραγματοποιήσουμε κάποια αλλαγή, καθώς η κρυπτογράφηση του πεδίου δύναται να εφαρμοστεί.

5.3 Δημιουργία και εισαγωγή αρχείων ρύθμισης κρυπτογράφησης

Ο αλγόριθμος κρυπτογράφησης μπορεί να διαμορφωθεί ανά χαρακτηριστικό και πρέπει να επιλεγεί από τον διαχειριστή κατά την κρυπτογράφηση ενός πεδίου.

Οι αλγόριθμοι κρυπτογράφησης που υποστηρίζονται είναι οι κάτωθι [11]:

- Advanced Encryption Standard (AES)

- Triple Data Encryption Standard (3DES)

Για πιο ισχυρή κρυπτογράφηση έγινε χρήση του αλγορίθμου AES καθώς είναι πιο ασφαλής και αποδοτικός από τον 3DES, όπως αναφέρθηκε και στο Κεφάλαιο 5.1.1.

Επιλέγουμε το πεδίο accountStatus προς κρυπτογράφηση για τους χρήστες και το πεδίο postalCode προς κρυπτογράφηση για τα σχολεία, κάνοντας χρήση του αλγόριθμου κρυπτογράφησης AES. Τα δύο ldif αρχεία φαίνονται παρακάτω:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/encr_accountSta-
tus.ldif
dn: cn=accountStatus,cn=encrypted attributes,cn=userRoot,cn=ldbm data-
base,cn=plugins,cn=config
objectClass: top
objectClass: nsAttributeEncryption
cn: accountStatus
nsEncryptionAlgorithm: AES
```

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/encr_post-
alCode.ldif

dn: cn=postalCode,cn=encrypted attributes,cn=userRoot,cn=ldbm data-
base,cn=plugins,cn=config
objectClass: top
objectClass: nsAttributeEncryption
cn: postalCode
nsEncryptionAlgorithm: AES
```

Η εισαγωγή των παραπάνω στη βάση δεδομένων γίνεται με τη χρήση του παρακάτω script:

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/import_encryp-
tion.sh

#!/bin/bash

ldapadd -x -c -D "cn=Directory Manager" -w 'password' -f encr_accountSta-
tus.ldif
ldapadd -x -c -D "cn=Directory Manager" -w 'password' -f encr_post-
alCode.ldif
```

και είναι απαραίτητο να τονιστεί ότι πρέπει να εισαχθεί στη βάση δεδομένων πριν από το αρχείο εισόδου final_foo.ldif.

5.4 Επαλήθευση της διαδικασίας κρυπτογράφησης πεδίου

Με την εντολή:

```
[root@openldpap-gdpr ~]# db2ldif -n userRoot -E
Exported ldif file: /var/lib/dirsrv/slapd-openldpap-gdpr/ldif/openldpap-
gdpr-userRoot-2020_05_07_142253.ldif
[07/May/2020:14:22:54.209250984 +0300] - INFO - slapd_extract_cert - CA
CERT NAME: Digi
[07/May/2020:14:22:54.243932042 +0300] - INFO - slapd_extract_cert -
SERVER CERT NAME: server-cert
ldiffile: /var/lib/dirsrv/slapd-openldpap-gdpr/ldif/openldpap-gdpr-
userRoot-2020_05_07_142253.ldif
```

δημιουργείται ένα αντίγραφο της κρυπτογραφημένης βάσης δεδομένων σε μορφή ldif στην τοποθεσία /var/lib/dirsrv/slapd-openldpap-gdpr/ldif [12].

Έτσι, μπορεί να ελεγχθεί εύκολα αν, για παράδειγμα, έχει πετύχει η κρυπτογράφηση στο πεδίο postalCode με μία απλή παρατήρηση στο εξαγόμενο αρχείο.

Αν το πεδίο postalCode περιέχει χαρακτήρες, τότε η κρυπτογράφηση πεδίου έχει πετύχει. Ειδάλλως, αν περιέχει έναν αριθμό 5 ψηφίων, σημαίνει πως έχει συμβεί κάποιο λάθος.

5.5 Διαγραφή κρυπτογράφησης πεδίου

Σε περίπτωση που κριθεί απαραίτητη η αφαίρεση της κρυπτογράφησης για κάποιο πεδίο, η διαδικασία που πρέπει να ακολουθηθεί είναι η εξής:

1. Τερματισμός του server:

```
[root@openldpap-gdpr ~]# systemctl stop dirsrv.target
```

2. Επεξεργασία του αρχείου dse.ldif:

```
[root@openldpap-gdpr ~]# vim /etc/dirsrv/slapd-openldpap-
gdpr/dse.ldif
```

Ύστερα, αν, για παράδειγμα, απαιτείται διαγραφή της κρυπτογράφησης του πεδίου postalCode, πληκτρολογούμε:

```
:/dn: cn=postalCode,cn=encrypted attributes
```

ακολουθούμενο από enter και ύστερα διαγράφουμε τις γραμμές

```
dn: cn=postalCode,cn=encrypted attributes,cn=userRoot,cn=ldbm data-
base,cn=plugins,cn=config
```

```
objectClass: top
objectClass: nsAttributeEncryption
cn: postalCode
nsEncryptionAlgorithm: AES
```

Αφού σώσουμε τις αλλαγές που έγιναν στο αρχείο dse.ldif, εκκινούμε τον server:

```
[root@openldpap-gdpr ~]# systemctl start dirsrv.target
```

Κεφάλαιο 6

Στοιχεία απόδοσης

6.1 Εισαγωγή

Η διαδικασία της καταγραφής στατιστικών απόδοσης / ταχύτητας χωρίστηκε σε τρεις κατηγορίες:

- στην εισαγωγή των δεδομένων στη βάση,
- στην αναζήτηση των δεδομένων με χρήση του ldapsearch και
- στη διαγραφή των δεδομένων από τη βάση.

Εν συνεχεία, αξίζει να σημειωθεί ότι τα δεδομένα χωρίστηκαν σε δύο κατηγορίες αρχείων:

- Σχολεία, μεγέθους 33 MB, που είναι 19.000 στο σύνολο και αποτελούν πραγματικά δεδομένα με τα οποία δεν υπήρχε πρόβλημα προσωπικών δεδομένων.
- Χρήστες, μεγέθους 854 MB και 2.38 GB, ανάλογα με τον αριθμό των πεδίων που επιλέγεται για τους χρήστες (28 και 66), όπως εξηγείται και στο κεφάλαιο 4.6.

Οι πόροι του εικονικού μηχανήματος, που χρησιμοποιήθηκε για τις μετρήσεις, αποτελούνται από:

- Τον επεξεργαστή Intel E5-2630 8 πυρήνων και 16 νημάτων στα 2.4 GHz,
- 16 GB DDR4 μνήμης RAM στα 1600 MHz και
- 70 GB χωρητικότητας σκληρού δίσκου.

Για την καταγραφή του χρόνου και των στατιστικών απόδοσης / ταχύτητας της κάθε λειτουργίας, χρησιμοποιήθηκαν οι εντολές time και sar [13], όπως φαίνεται, ενδεικτικά, στα παρακάτω scripts:

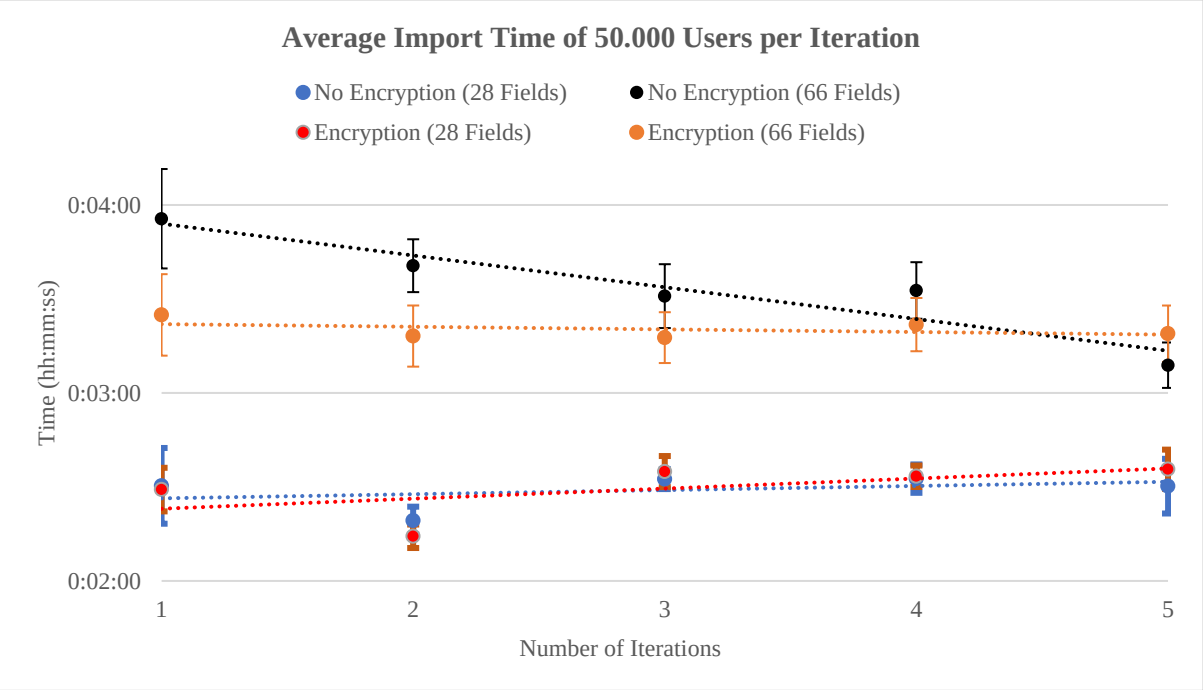
```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/import_users.sh

#!/bin/bash

time ldapadd -x -D "cn=Directory Manager" -w 'password' -f add_people.ldif

for I in {1..20}
do
       time ldapadd -x -D "cn=Directory Manager" -w 'password' -f
data$i.ldif > time$i.txt
       rm time$i.txt
done
```

```
[root@openldpap-gdpr ~]# cat /home/dkalo/statistics/users_import.sh

#!/bin/bash

for I in {1..5}
do

sar -u -b -r 1 1200 >> /home/dkalo/statistics//log$1_import_users_no.txt

done
```

```
[root@openldpap-gdpr ~]# cat /home/dkalo/populate_dataset/search_us-
ers1.000.000.sh
#!/bin/bash
for I in {1..10}
do
       time ldapsearch -x -z 1.000.000 -b 'ou=people,dc=sch,dc=gr' '(ob-
jectclass=*)' -D "cn=Directory Manager" -w 'password' > time1.txt
       rm time1.txt
done
```

6.2 Διαγράμματα μετρήσεων χρόνου

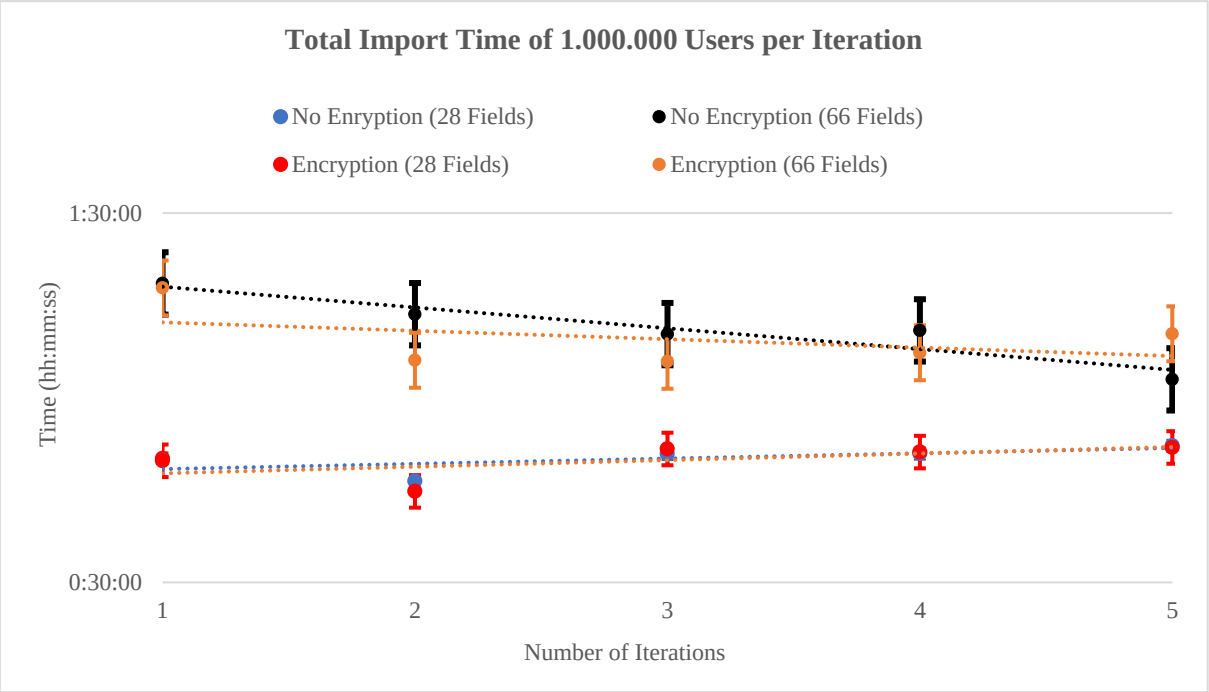
Παρακάτω παρατίθενται τα διαγράμματα που εξήχθησαν από τα στατιστικά του χρόνου των παραπάνω λειτουργιών, με και χωρίς κρυπτογράφηση πεδίου:



Σχήμα 1: Μέσος χρόνος εισαγωγής 50.000 χρηστών, με 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή μιας επανάληψης είναι ο μέσος όρος από 20 διαδοχικές μετρήσεις εισαγωγής 50.000 χρηστών και οι κατακόρυφες μπάρες είναι οι αντίστοιχες τυπικές αποκλίσεις. Με διακεκομμένες γραμμές απεικονίζονται οι γραμμές τάσης για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 1*** μπορούμε να διαπιστώσουμε τα εξής:

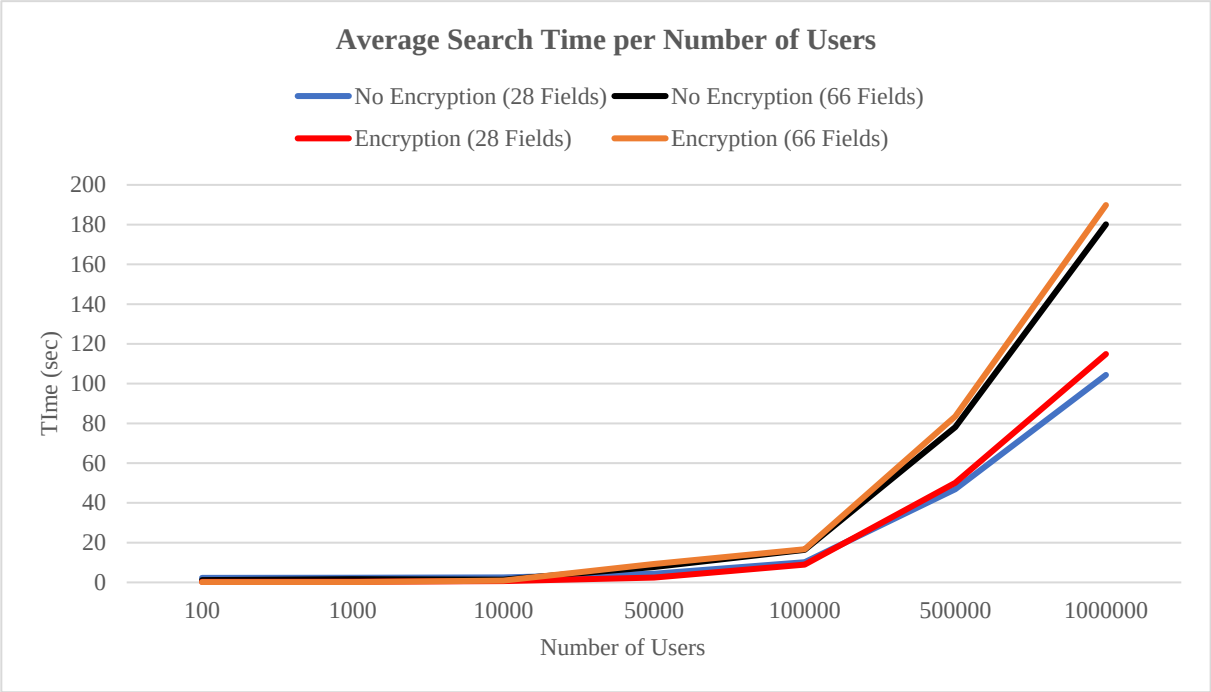
- Δεν υπάρχει επιπλέον κόστος στο χρόνο εισαγωγής των κρυπτογραφημένων δεδομένων για 50.000 χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων, για την περίπτωση 50.000 χρηστών, έχει επιπλέον κόστος της τάξης του 43% στο χρόνο εισαγωγής των μη κρυπτογραφημένων δεδομένων και επιπλέον κόστος της τάξης του 34% στο χρόνο εισαγωγής των κρυπτογραφημένων δεδομένων.



Σχήμα 2: Συνολικός χρόνος εισαγωγής 1.000.000 χρηστών, με 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Οι κατακόρυφες μπάρες απεικονίζουν τις τυπικές αποκλίσεις και με διακεκομμένες γραμμές απεικονίζονται οι γραμμές τάσης για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα*** διαπιστώνουμε τα εξής:

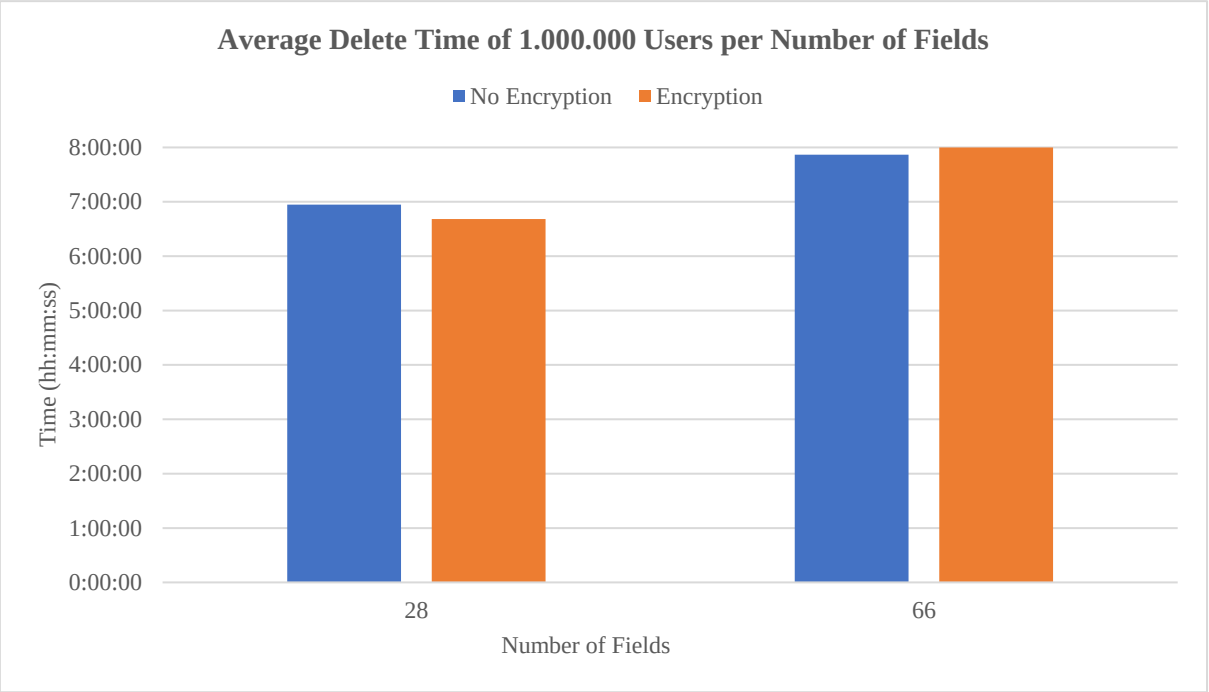
- Δεν υπάρχει επιπλέον κόστος στο χρόνο εισαγωγής των κρυπτογραφημένων δεδομένων για 1.000.000 χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων, για την περίπτωση 1.000.000 χρηστών, έχει επιπλέον κόστος της τάξης του 42% στο χρόνο εισαγωγής των μη κρυπτογραφημένων δεδομένων και επιπλέον κόστος της τάξης του 40% στο χρόνο εισαγωγής των κρυπτογραφημένων δεδομένων.



Σχήμα 3: Μέσος χρόνος αναζήτησης χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή χρόνου που απεικονίζεται είναι ο μέσος όρος από 10 διαδοχικές μετρήσεις αναζήτησης για κάθε αριθμό χρηστών.

Από το ***Σχήμα 3*** μπορούμε να διαπιστώσουμε τα εξής:

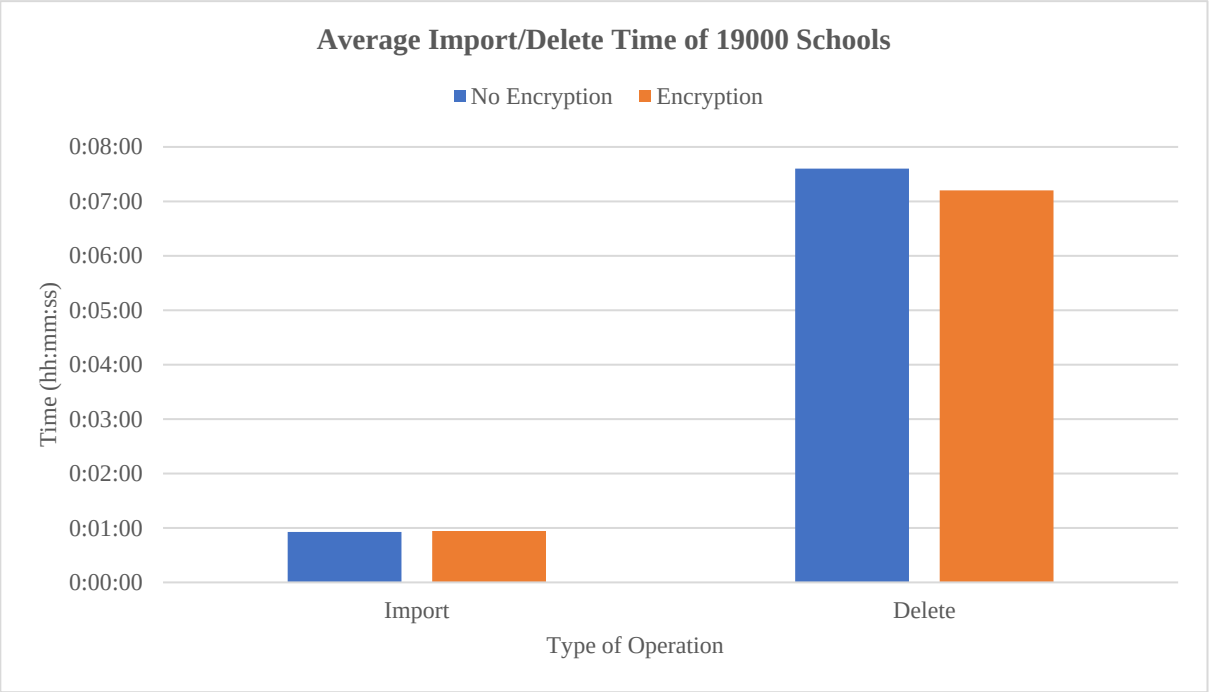
- Δεν υπάρχει επιπλέον κόστος στο χρόνο αναζήτησης των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων, για τις περιπτώσεις 100.000, 500.000 και 1.000.000 χρηστών, έχει επιπλέον κόστος της τάξης του 66% στο χρόνο αναζήτησης των μη κρυπτογραφημένων δεδομένων και επιπλέον κόστος της τάξης του 72% στο χρόνο αναζήτησης των κρυπτογραφημένων δεδομένων.



Σχήμα 4: Μέσος χρόνος διαγραφής 1.000.000 χρηστών ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή χρόνου που απεικονίζεται είναι ο μέσος όρος από 5 διαδοχικές μετρήσεις διαγραφής, για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 4*** μπορούμε να διαπιστώσουμε τα εξής:

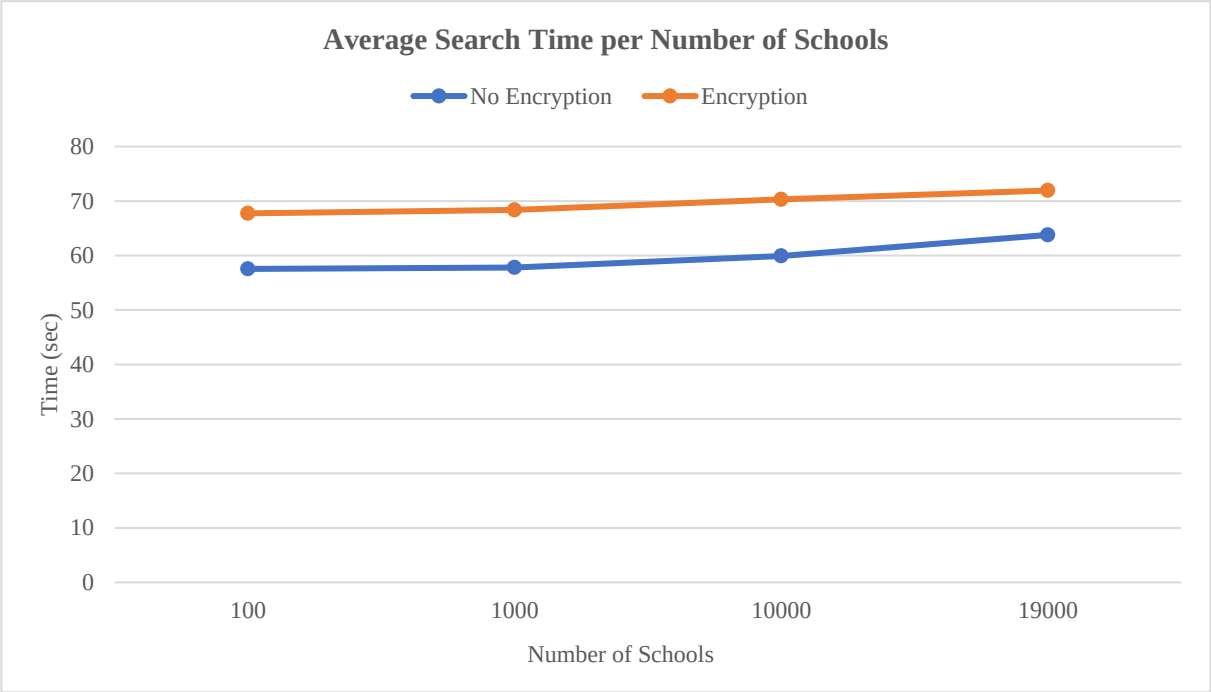
- Δεν υπάρχει επιπλέον κόστος στο χρόνο διαγραφής των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων, για 1.000.000 χρήστες, έχει επιπλέον κόστος της τάξης του 13% στο χρόνο διαγραφής των μη κρυπτογραφημένων δεδομένων και επιπλέον κόστος της τάξης του 19% στο χρόνο διαγραφής των κρυπτογραφημένων δεδομένων.



Σχήμα 5: Μέσος χρόνος εισαγωγής/διαγραφής 19.000 σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή χρόνου που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής, με και χωρίς κρυπτογράφηση πεδίου.

Από το ***Σχήμα 5*** μπορούμε να διαπιστώσουμε το εξής:

- Δεν υπάρχει επιπλέον κόστος στο χρόνο εισαγωγής / διαγραφής των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.



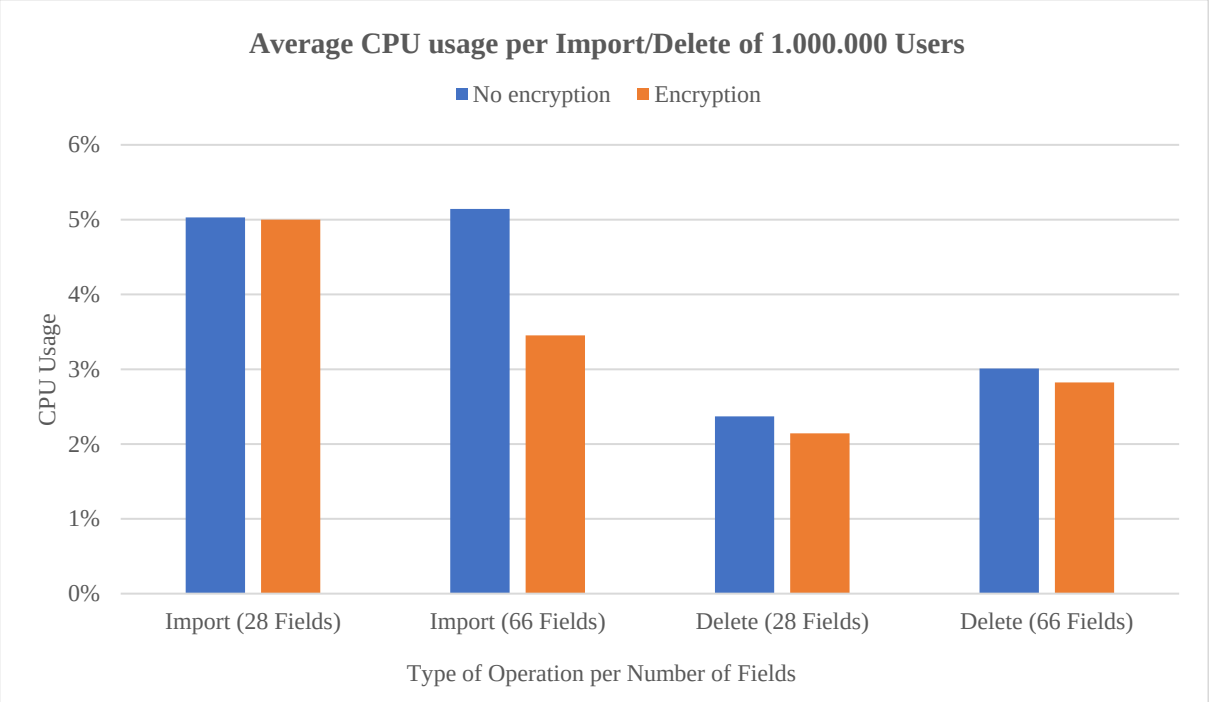
Σχήμα 6: Μέσος χρόνος αναζήτησης σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή χρόνου που απεικονίζεται είναι ο μέσος όρος από 10 διαδοχικές μετρήσεις αναζήτησης, με και χωρίς κρυπτογράφηση πεδίου.

Από το ***Σχήμα 6*** μπορούμε να διαπιστώσουμε το εξής:

- Υπάρχει επιπλέον κόστος της τάξης του 16% στο χρόνο αναζήτησης των κρυπτογραφημένων δεδομένων για τα σχολεία, σε σχέση με τα μη κρυπτογραφημένα δεδομένα.

6.3 Διαγράμματα μετρήσεων χρησιμοποίησης επεξεργαστή, μνήμης και δίσκου

Παρακάτω παρατίθενται τα διαγράμματα που εξήχθησαν από τα στατιστικά της απόδοσης / ταχύτητας των παραπάνω λειτουργιών, με και χωρίς κρυπτογράφηση πεδίου:

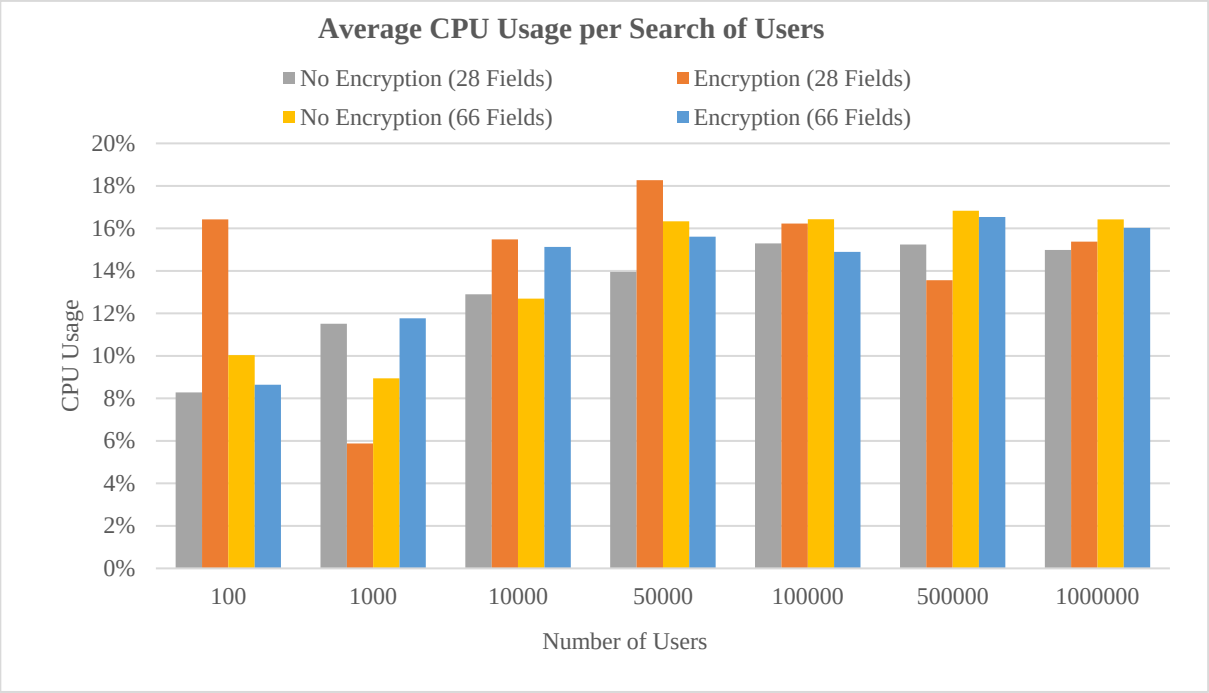


Σχήμα 7: Μέση χρησιμοποίηση CPU κατά την εισαγωγή / διαγραφή 1.000.000 χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή ποσοστού CPU που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής, για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 7*** μπορούμε να διαπιστώσουμε τα εξής:

- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την εισαγωγή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών, χωρίς κρυπτογράφηση, έχει κόστος της τάξης του 27% στη χρησιμοποίηση της CPU, κατά τη διαδικασία της διαγραφής 1.000.000 χρηστών.

- Η αύξηση των πεδίων των χρηστών, με κρυπτογράφηση, έχει κόστος της τάξης του 31% στη χρησιμοποίηση της CPU, κατά τη διαδικασία της διαγραφής 1.000.000 χρηστών.

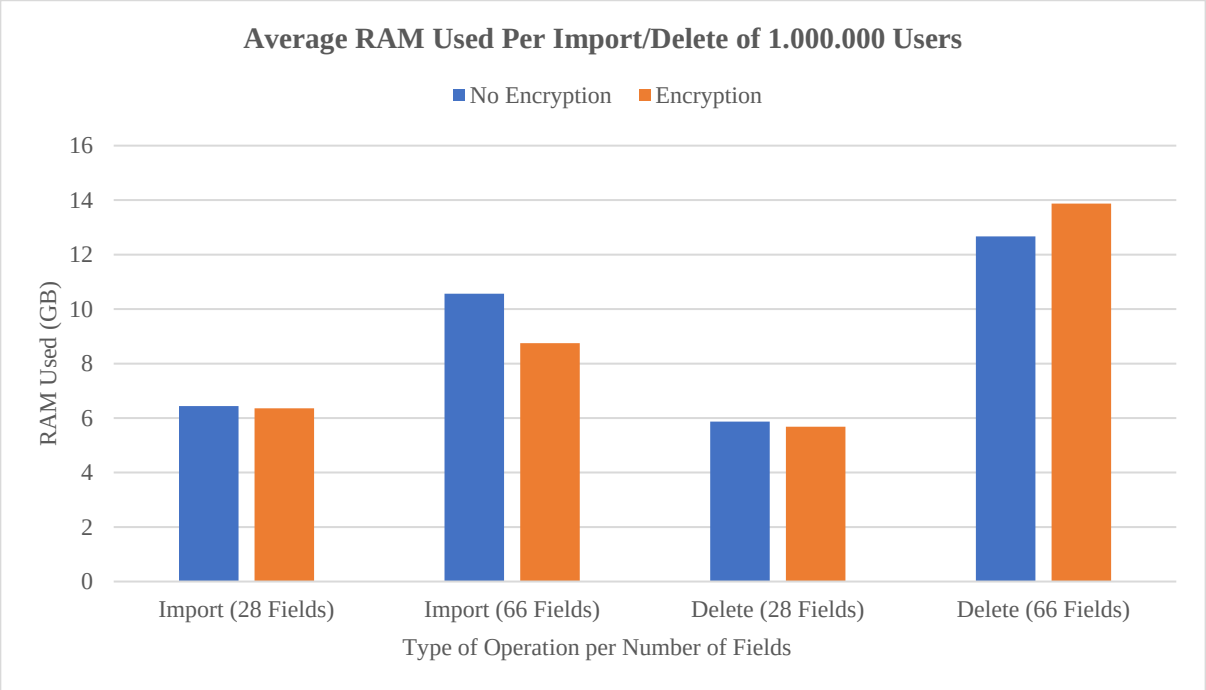


Σχήμα 8: Μέση χρησιμοποίηση CPU κατά την αναζήτηση χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή ποσοστού CPU που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς χρηστών.

Από το ***Σχήμα 8*** να διαπιστώνουμε τα εξής:

- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα, εκτός από την περίπτωση της αναζήτησης 100 χρηστών, όπου υπάρχει επιπλέον κόστος 98%, την περίπτωση της αναζήτησης 10.000 χρηστών, όπου υπάρχει επιπλέον κόστος 20% και την περίπτωση της αναζήτησης 50.000 χρηστών, όπου υπάρχει επιπλέον κόστος 30%.
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα, εκτός από την περίπτωση της αναζήτησης 1.000 χρηστών, όπου υπάρχει επιπλέον κόστος 31% και επιπλέον κόστος 19% κατά την αναζήτηση 10.000 χρηστών.

- Η αύξηση των πεδίων των χρηστών, χωρίς κρυπτογράφηση, έχει κόστος της τάξης του 21% στη χρησιμοποίηση της CPU κατά την αναζήτηση 100 χρηστών, κόστος 17% κατά την αναζήτηση 100.000 χρηστών, κόστος 10% κατά την αναζήτηση 500.000 χρηστών και κόστος 9% κατά την αναζήτηση 1.000.000 χρηστών.
- Η αύξηση των πεδίων των χρηστών, με κρυπτογράφηση, έχει κόστος της τάξης του 100% στη χρησιμοποίηση της CPU κατά την αναζήτηση 1.000 χρηστών και κόστος 17% κατά την αναζήτηση 500.000 χρηστών.

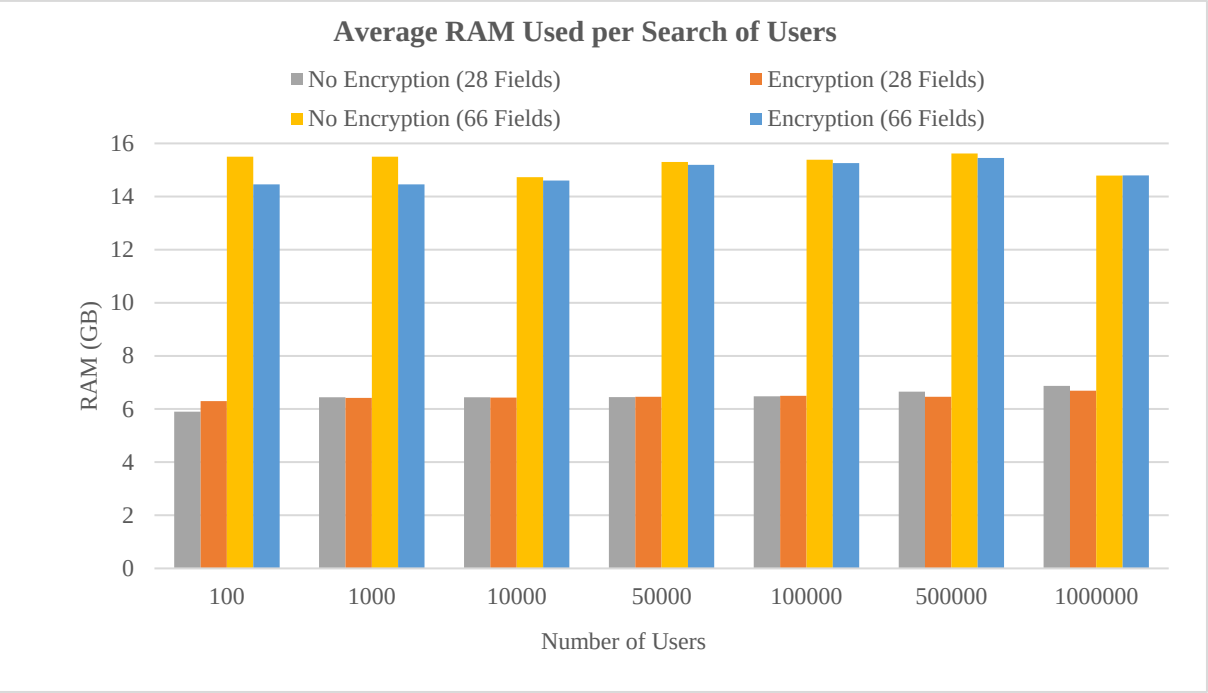


Σχήμα 9: Μέση τιμή της RAM που χρησιμοποιείται κατά την εισαγωγή / διαγραφή 1.000.000 χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή της RAM που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής 1.000.000 χρηστών, για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 9*** μπορούμε να διαπιστώσουμε τα εξής:

- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά την εισαγωγή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 63% στην χρησιμοποίηση της RAM, κατά τη διαδικασία της εισαγωγής χωρίς κρυπτογράφηση.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 37% στη χρησιμοποίηση της RAM, κατά τη διαδικασία της εισαγωγής με κρυπτογράφηση πεδίου.

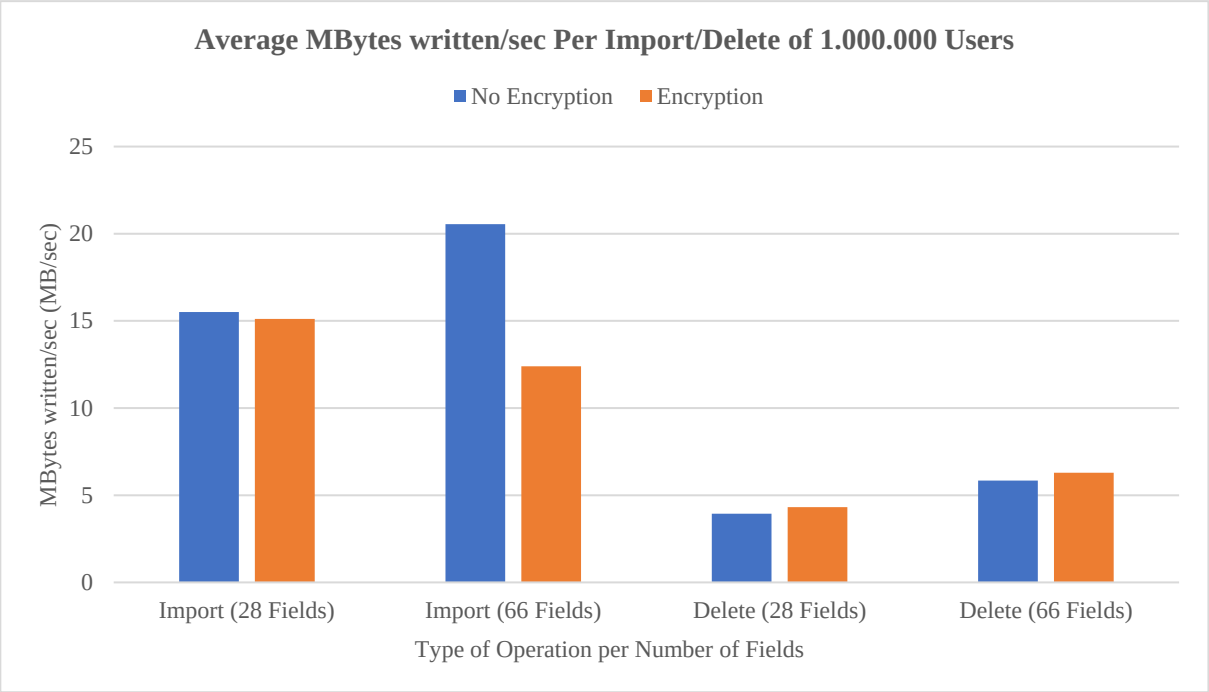
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά τη διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 πεδία, σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Υπάρχει επιπλέον κόστος 9% στη χρησιμοποίηση της RAM κατά τη διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 115% στη χρησιμοποίηση της RAM, κατά τη διαδικασία της διαγραφής χωρίς κρυπτογράφηση.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 144% στη χρησιμοποίηση της RAM, κατά τη διαδικασία της διαγραφής με κρυπτογράφηση πεδίου.



Σχήμα 10: Μέση τιμή της RAM που χρησιμοποιείται κατά την αναζήτηση χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή της RAM που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς χρηστών.

Από το ***Σχήμα 10*** διαπιστώνουμε τα εξής:

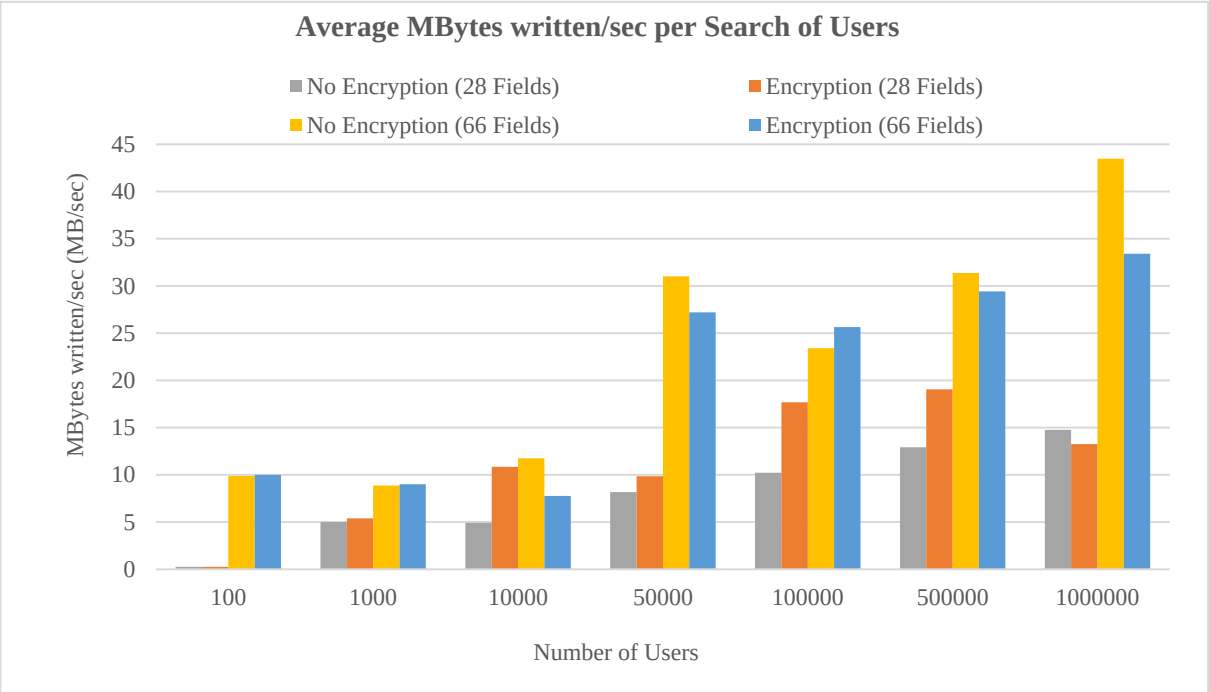
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες είτε με 28 είτε με 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών, με ή χωρίς κρυπτογράφηση, έχει κόστος της τάξης του 130% στη χρησιμοποίηση της RAM, κατά μέσο όρο.



Σχήμα 11: Μέση τιμή των MB / sec που γράφει ο δίσκος, κατά την εισαγωγή / διαγραφή 1.000.000 χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή των MB / sec εγγραφής που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής 1.000.000 χρηστών, για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 11*** διαπιστώνουμε τα εξής:

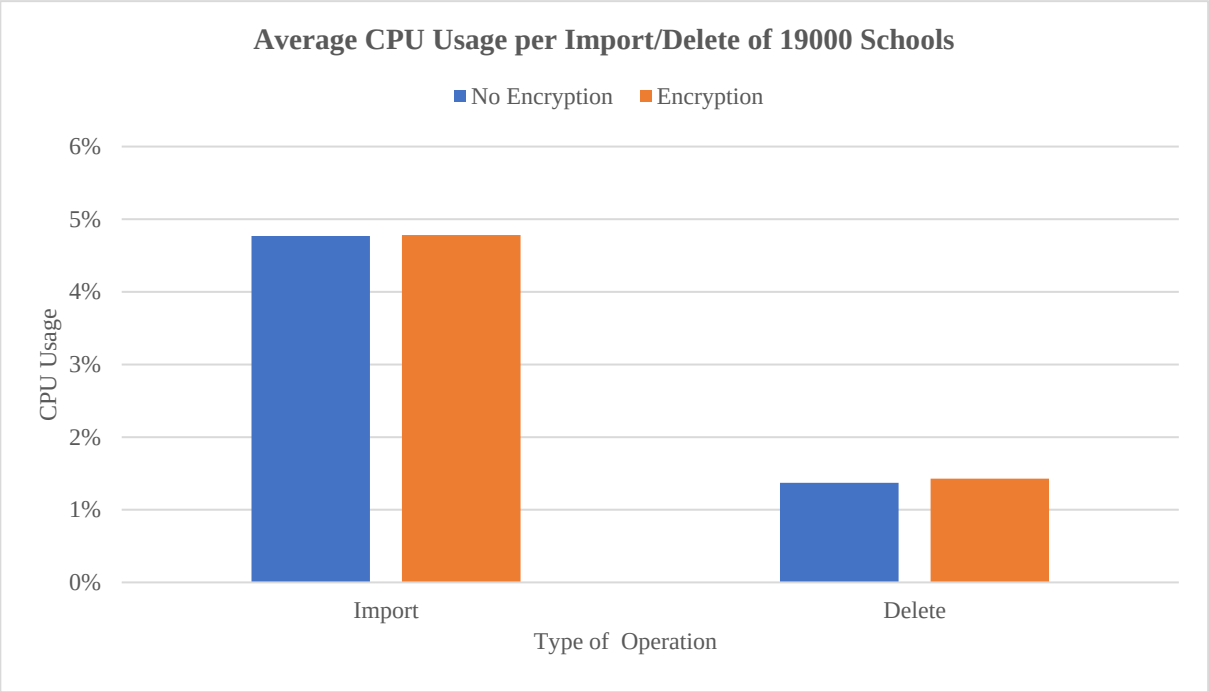
- Δεν υπάρχει επιπλέον κόστος στα MB / sec που γράφει ο δίσκος κατά την εισαγωγή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Υπάρχει επιπλέον κόστος της τάξης του 9% στα MB / sec που γράφει ο δίσκος κατά τη διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Υπάρχει επιπλέον κόστος 7% στα MB / sec που γράφει ο δίσκος κατά τη διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 48% στα MB / sec που γράφει ο δίσκος, κατά τη διαγραφή 1.000.000 χρηστών χωρίς κρυπτογράφηση πεδίου.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 45% στα MB / sec που γράφει ο δίσκος, κατά τη διαγραφή 1.000.000 χρηστών με κρυπτογράφηση πεδίου.



Σχήμα 12: Μέση τιμή των MB / sec που γράφει ο δίσκος, κατά την αναζήτηση χρηστών, ανά 28 και 66 πεδία δεδομένων, αντίστοιχα, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή των MB / sec εγγραφής που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς χρηστών.

Από το ***Σχήμα 12*** διαπιστώνουμε τα εξής:

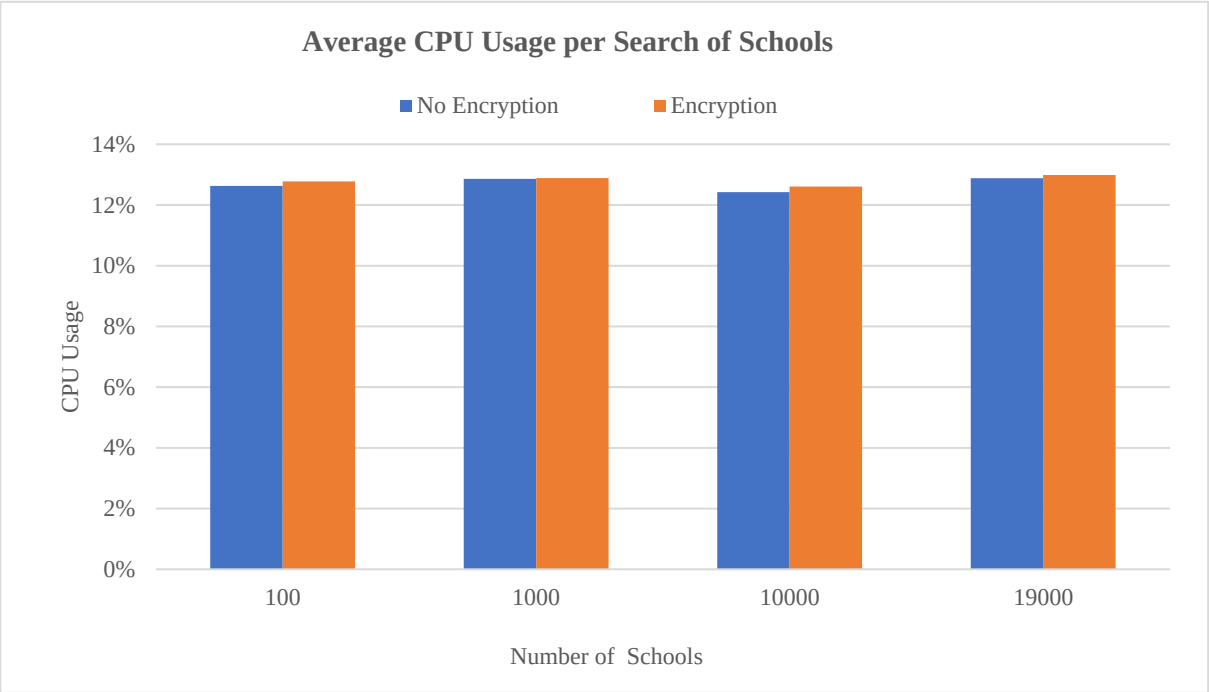
- Υπάρχει επιπλέον κόστος 37%, κατά μέσο όρο, στα MB / sec που γράφει ο δίσκος κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Δεν υπάρχει επιπλέον κόστος στα MB / sec που γράφει ο δίσκος, κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 680%, κατά μέσο όρο, στα MB / sec που γράφει ο δίσκος, κατά τη διαδικασία της αναζήτησης χρηστών χωρίς κρυπτογράφηση πεδίου.
- Η αύξηση των πεδίων των χρηστών έχει κόστος της τάξης του 591%, κατά μέσο όρο, στα MB / sec που γράφει ο δίσκος, κατά τη διαδικασία της αναζήτησης χρηστών με κρυπτογράφηση πεδίου



Σχήμα 13: Μέση χρησιμοποίηση CPU κατά την εισαγωγή / διαγραφή 19.000 σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή ποσοστού CPU που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής των 19000 σχολείων.

Από το ***Σχήμα 13*** διαπιστώνουμε το εξής:

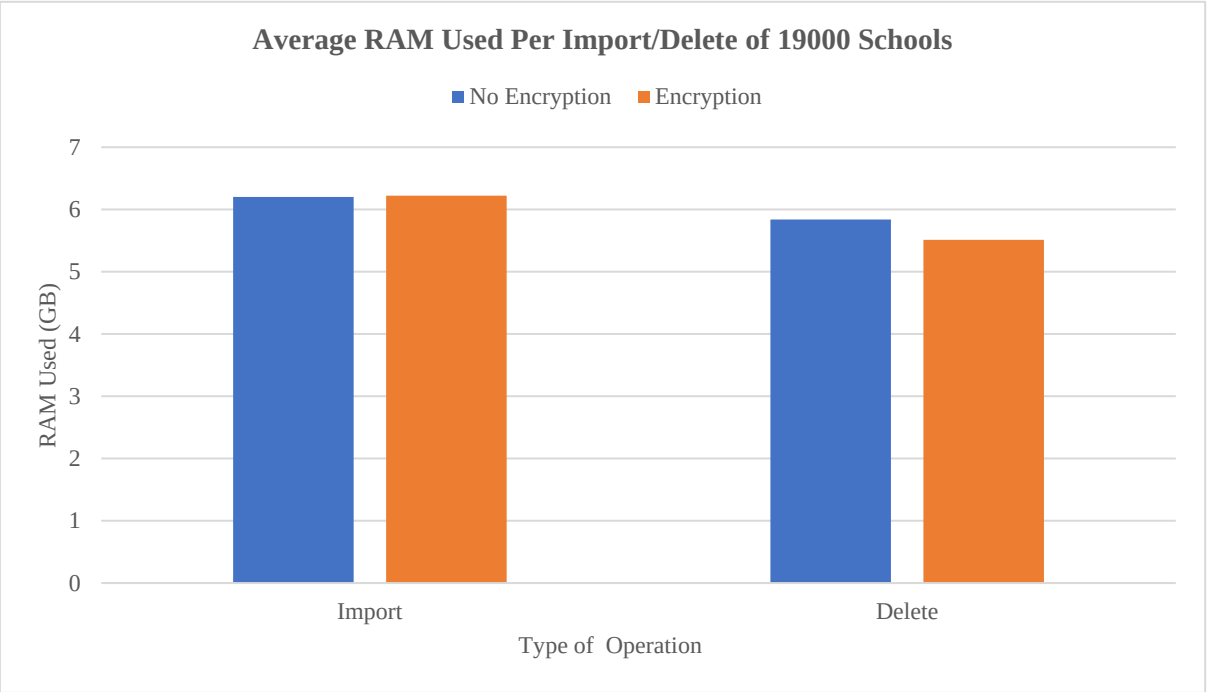
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την εισαγωγή / διαγραφή των κρυπτογραφημένων δεδομένων για τα 19.000 σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.



Σχήμα 14: Μέση χρησιμοποίηση CPU κατά την αναζήτηση σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή ποσοστού CPU που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς σχολείων.

Από το ***Σχήμα 14*** διαπιστώνουμε το εξής:

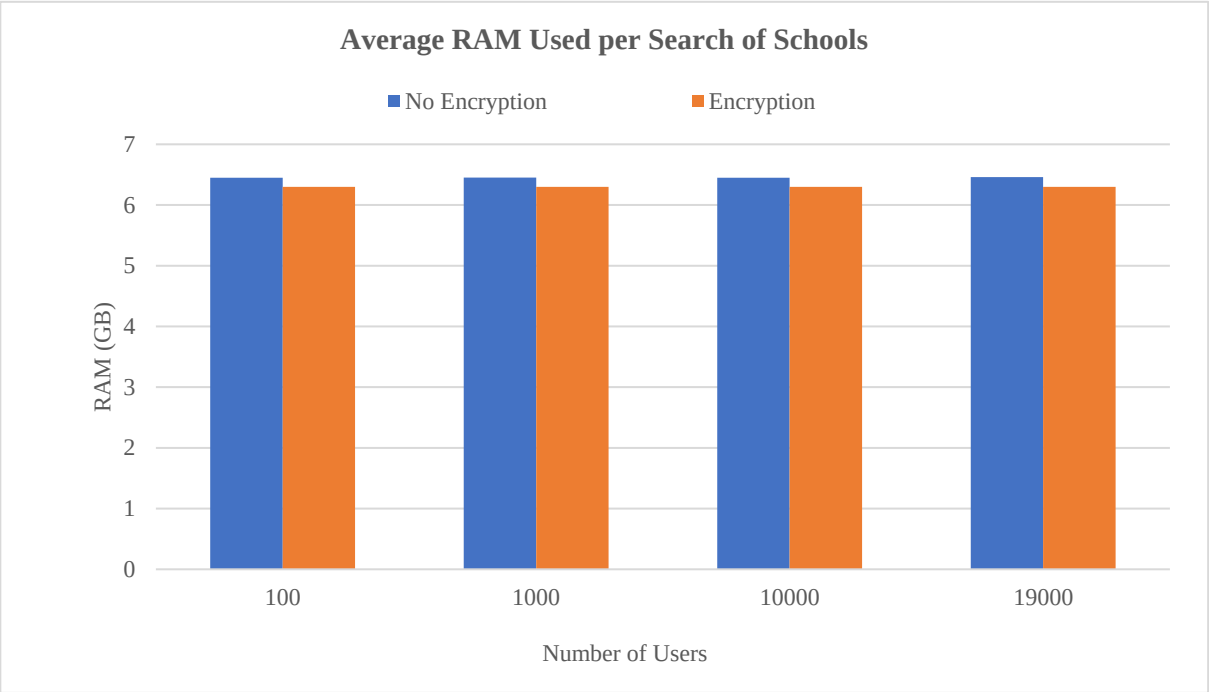
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.



Σχήμα 15: Μέση τιμή της RAM που χρησιμοποιείται κατά την εισαγωγή / διαγραφή 19.000 σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή της RAM που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής 19.000 σχολείων.

Από το ***Σχήμα 15*** διαπιστώνουμε το εξής:

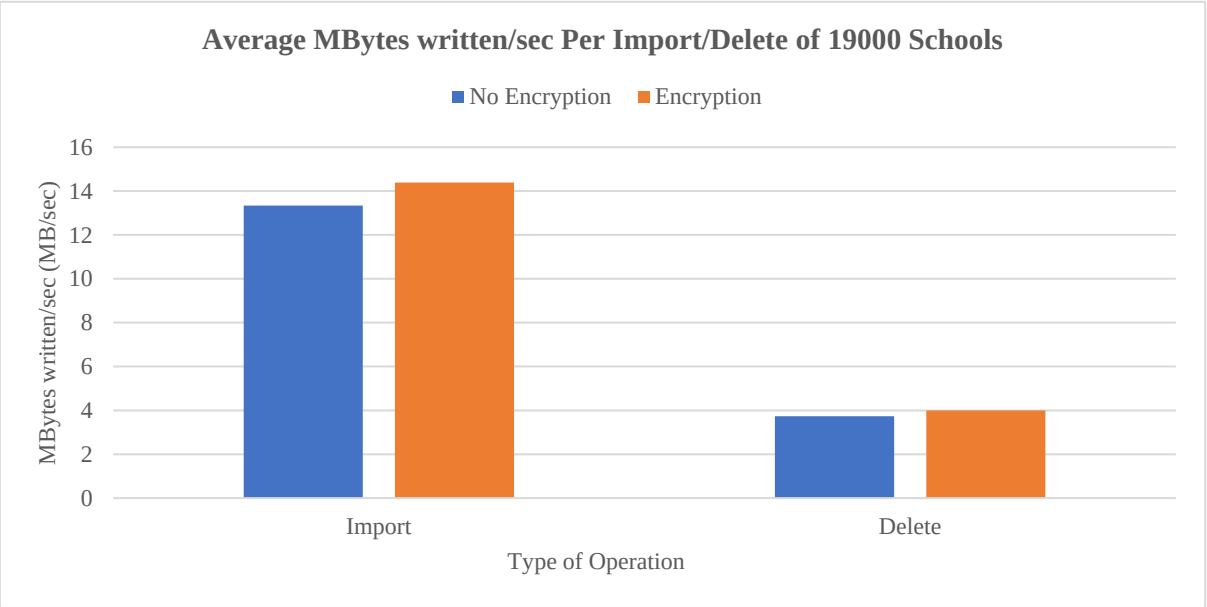
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά την εισαγωγή / διαγραφή των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα



Σχήμα 16: Μέση τιμή της RAM που χρησιμοποιείται κατά την αναζήτηση σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή της RAM που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς σχολείων.

Από το ***Σχήμα 16*** διαπιστώνουμε το εξής:

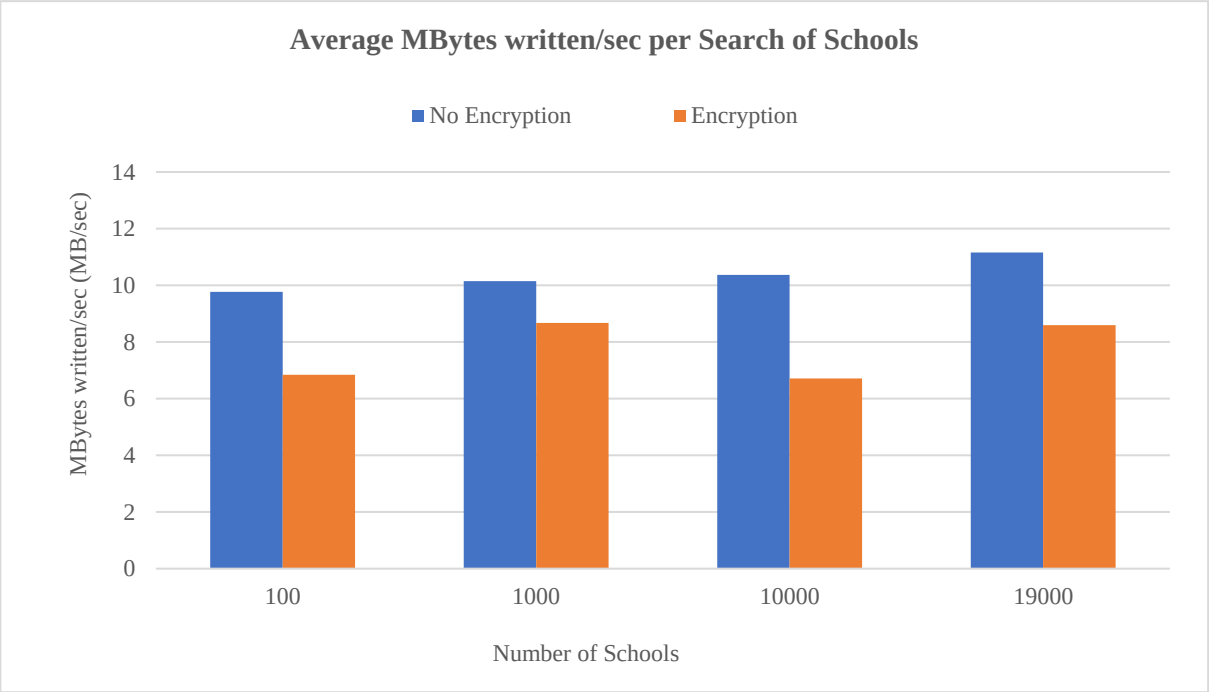
- Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.



Σχήμα 17: Μέση τιμή των MB / sec που γράφει ο δίσκος, κατά την εισαγωγή/διαγραφή 19.000 σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή των MB / sec εγγραφής που απεικονίζεται είναι ο μέσος όρος από 5 μετρήσεις εισαγωγής / διαγραφής 19.000 σχολείων, για κάθε μία από τις παραπάνω περιπτώσεις.

Από το ***Σχήμα 17*** διαπιστώνουμε το εξής:

- Δεν υπάρχει επιπλέον κόστος στα MB / sec που γράφει ο δίσκος κατά την εισαγωγή / διαγραφή των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.



Σχήμα 18: Μέση τιμή των MB / sec που γράφει ο δίσκος, κατά την αναζήτηση σχολείων, με και χωρίς κρυπτογράφηση ενός πεδίου. Κάθε τιμή των MB / sec εγγραφής που απεικονίζεται είναι ο μέσος όρος από 10 μετρήσεις αναζήτησης, για κάθε έναν από τους παραπάνω αριθμούς σχολείων.

Από το ***Σχήμα 18*** διαπιστώνουμε το εξής:

- Δεν υπάρχει επιπλέον κόστος στα MB / sec που γράφει ο δίσκος κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τα σχολεία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.

Κεφάλαιο 7

Συμπεράσματα

Η κρυπτογράφηση πεδίου στον Directory Server 389 και τα στοιχεία απόδοσης του πρώτου, μας οδήγησαν στις εξής παρατηρήσεις:

1. Η κρυπτογράφηση πεδίου είναι μία εύκολη διαδικασία η υλοποίηση της οποίας απαιτεί λιγοστό χρόνο.
2. Δεν υπάρχει επιπλέον κόστος στο χρόνο εισαγωγής, διαγραφής και αναζήτησης των κρυπτογραφημένων δεδομένων για τους 1.000.000 χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα.
3. Κατά την αύξηση των πεδίων των χρηστών από 28 σε 66 παρατηρήθηκε επιπλέον κόστος της τάξης του 40% στο χρόνο εισαγωγής, επιπλέον κόστος 72% στο χρόνο αναζήτησης και επιπλέον κόστος 19% στον χρόνο διαγραφής, αντίστοιχα.
4. Για την περίπτωση των σχολείων, δεν υπάρχει επιπλέον κόστος στο χρόνο εισαγωγής / διαγραφής των κρυπτογραφημένων δεδομένων σε σχέση με τα μη κρυπτογραφημένα δεδομένα, με εξαίρεση τη λειτουργία αναζήτησης κατά την οποία υπάρχει επιπλέον κόστος, στο χρόνο, της τάξης του 16%.
5. Όσον αφορά τις υπόλοιπες μετρικές απόδοσης, δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU κατά την εισαγωγή και διαγραφή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα. Εξαίρεση αποτελεί η λειτουργία αναζήτησης στην οποία παρατηρούμε επιπλέον κόστος στη χρησιμοποίηση της CPU, μόνο για τα κρυπτογραφημένα δεδομένα χρηστών με 28 πεδία, φαινόμενο το οποίο εξομαλύνεται όσο αυξάνεται ο αριθμός των χρηστών. Τέλος, η αύξηση των πεδίων των χρηστών, για κρυπτογραφημένα δεδομένα, οδηγεί σε μεγαλύτερη χρησιμοποίηση της CPU κατά την διαγραφή 1.000.000 χρηστών και κατά την αναζήτηση 1.000 και 500.000 χρηστών.
6. Δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της RAM κατά την εισαγωγή, διαγραφή και αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα, με εξαίρεση την περίπτωση της διαγραφής 66 πεδίων όπου υπάρχει επιπλέον χρησιμοποίηση 9%. Τέλος, η αύξηση των πεδίων των χρηστών, για κρυπτογραφημένα δεδομένα, οδηγεί σε επιπλέον χρησιμοποίηση της RAM σε ποσοστό 37% κατά την εισαγωγή, σε ποσοστό 144% κατά τη διαγραφή και σε ποσοστό 130% κατά την αναζήτηση.

7. Όσον αφορά τη λειτουργία εγγραφής του δίσκου (σε MB / sec), δεν υπάρχει επιπλέον κόστος κατά την εισαγωγή των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 ή 66 πεδία, σε σχέση με τα μη κρυπτογραφημένα δεδομένα. Σχετικά με τη διαγραφή, το επιπλέον κόστος που υπάρχει θεωρείται αμελητέο. Τέλος, υπάρχει επιπλέον κόστος 37%, κατά μέσο όρο, στα MB / sec που γράφει ο δίσκος κατά την αναζήτηση των κρυπτογραφημένων δεδομένων για τους χρήστες με 28 πεδία σε σχέση με τα μη κρυπτογραφημένα δεδομένα και δεν υπάρχει επιπλέον κόστος για τους χρήστες με 66 πεδία.
8. Σε συνέχεια με το παραπάνω, η αύξηση των πεδίων των χρηστών έχει περίσσιο κόστος της τάξης του 45% στα MB / sec που γράφει ο δίσκος κατά την διαγραφή 1.000.000 χρηστών με κρυπτογράφηση πεδίου και επιπλέον κόστος της τάξης του 591%, κατά μέσο όρο, στα MB / sec που γράφει ο δίσκος κατά τη διαδικασία της αναζήτησης χρηστών με κρυπτογράφηση πεδίου.
9. Αναφορικά με τις μετρικές απόδοσης που σχετίζονται με τα δεδομένα των σχολείων, δεν υπάρχει επιπλέον κόστος στη χρησιμοποίηση της CPU, της RAM ή στα MB / sec που γράφει ο δίσκος κατά την εισαγωγή, διαγραφή και αναζήτηση των κρυπτογραφημένων δεδομένων σε σχέση με τα μη κρυπτογραφημένα δεδομένα.

Βιβλιογραφία

[1] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/creating_and_maintaining_databases-database_encryption

[2] Brian Arkills, “LDAP Directories Explained”, 2003

[3] https://tools.ietf.org/html/rfc2849

[4] https://gdpr-info.eu/

[5] https://directory.fedoraproject.org/

[6] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/creating_and_maintaining_databases-database_encryption#Database_Encryption-Encryption_Keys

[7] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/enabling_tls

[8] https://github.com/leto/389-ds/blob/master/ldap/schema/50ns-mail.ldif

[9] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/custom-schema-files

[10] https://directory.fedoraproject.org/docs/389ds/howto/howto-ssl.html#turn-it-on

[11] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/database_encryption-encryption_ciphers

[12] https://access.redhat.com/documentation/en-us/red_hat_directory_server/10/html/administration_guide/database_encryption-exporting_and_importing_an_encrypted_database#exporting-encrypted-db

[13] https://www.thegeekstuff.com/2011/03/sar-examples/

[14] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#/media/File:AES-SubBytes.svg

[15] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Παράρτημα

Κώδικας 1: Παρακάτω παρατίθεται το script με το οποίο έγινε η μετατροπή των αρχείων σχήματος από .schema σε .ldif.

```
[root@openldpap-gdpr ~]# cat /home/dkalo/schema/schema-script.pl

#!/usr/bin/perl -w

my $optionCount = 0;
my $optionPrint = 0;
my $optionBadEntries = 0;
my $optionHelp = 0;
my $filename = "" ;

foreach (@ARGV) {
  $optionHelp = 1 if ( /^-h$/);
  $optionCount = 1 if ( /^-c$/);
  $optionPrint = 1 if ( /^-b$/);
  $optionBadEntries = 1 if ( /^-d$/);
  $filename = $_ if ( ! /^-b$/ && ! /^-c$/ && ! /^-d$/);
}

die "Usage: ol-schema-migrate-v2.pl [ -c ] [ -b ] [ -d ] schema\n" .
    "  -c\tcount attribute and object class\n" .
    "  -b\tconvert and beautify your schema\n" .
    "  -d\tdisplay unrecognized elements, find empty and duplicated
OID\n" .
    "  -h\tthis help\n" if ($filename eq "" || ($optionHelp || (!$op-
tionCount && !$optionPrint && !$optionBadEntries)));

if($optionCount) {
  print "Schema verification counters:\n";
  my $ldapdata = &getSourceFile($filename);
  print "".(defined($ldapdata->{attributes}) ? @{$ldapdata->{attrib-
utes}}: 0) . " attributes\n";
  print "".(defined($ldapdata->{objectclass}) ?  @{$ldapdata->{ob-
jectclass}}: 0) . " object classes\n\n"
}

if($optionPrint) {
  my $ldapdata = &getSourceFile($filename);
  &printit($ldapdata);
}

if($optionBadEntries) {
  print "Display unrecognized entries:\n";
  my $ldapdata = &getSourceFile($filename);
  my $errorsAttr = 0;
  my $errorsObjc = 0;
  my $errorsDup  = 0;
  my $emptyOid = 0;
  my %dup;

  foreach (@{$ldapdata->{attributes}}) {
    my $attr = $_;
```

```
    push @{$dup{$attr->{OID}}{attr}}, {NAME => $attr->{NAME}, LINENUMBER
=> $attr->{LINENUMBER}};

    $attr->{DATA} =~ s/\n/ /g;
    $attr->{DATA} =~ s/\r//g;
    $attr->{DATA} =~ s/attribute[t|T]ypes?:?\s*\(//;
    $attr->{DATA} =~ s/\Q$attr->{OID}//                  if(defined $attr-
>{OID});
    $attr->{DATA} =~ s/NAME\s*\Q$attr->{NAME}//          if(defined $attr-
>{NAME});
    $attr->{DATA} =~ s/DESC\s*'\Q$attr->{DESC}'//        if(defined $attr-
>{DESC});
    $attr->{DATA} =~ s/$attr->{OBSOLETE}//               if(defined $attr-
>{OBSOLETE});
    $attr->{DATA} =~ s/SUP\s*\Q$attr->{SUP}//            if(defined $attr-
>{SUP});
    $attr->{DATA} =~ s/EQUALITY\s*\Q$attr->{EQUALITY}// if(defined $attr-
>{EQUALITY});
    $attr->{DATA} =~ s/ORDERING\s*\Q$attr->{ORDERING}// if(defined $attr-
>{ORDERING});
    $attr->{DATA} =~ s/SUBSTR\s*\Q$attr->{SUBSTR}//      if(defined $attr-
>{SUBSTR});
    $attr->{DATA} =~ s/SYNTAX\s*\Q$attr->{SYNTAX}//      if(defined $attr-
>{SYNTAX});
    $attr->{DATA} =~ s/SINGLE-VALUE//                    if(defined $attr-
>{SINGLEVALUE});
    $attr->{DATA} =~ s/NO-USER-MODIFICATION//            if(defined $attr-
>{NOUSERMOD});
    $attr->{DATA} =~ s/COLLECTIVE//                      if(defined $attr-
>{COLLECTIVE});
    $attr->{DATA} =~ s/USAGE\s*\Q$attr->{USAGE}//        if(defined $attr-
>{USAGE});
    $attr->{DATA} =~ s/\)\s$//;
    $attr->{DATA} =~ s/^\s+(\S)/\n$1/  ;
    $attr->{DATA} =~ s/(\S)\s+$/$1\n/;
    do {
      $errorsAttr ++;
      do {  $emptyOid ++;
            print "Warning: no OID for attributes element at line $attr-
>{LINENUMBER} \n";
      } if( !defined($attr->{OID}));
      print "### Unknow element embedded in ATTRIBUTE at line $attr-
>{LINENUMBER}:\n$attr->{DATA}\n"
    } if($attr->{DATA} =~ /\w/);
  }

  foreach (@{$ldapdata->{objectclass}}) {
    my $objc = $_;
    push @{$dup{$objc->{OID}}{objc}} , {NAME => $objc->{NAME}, LINENUMBER
=> $objc->{LINENUMBER}};
    $objc->{DATA} =~ s/\n/ /g;
    $objc->{DATA} =~ s/\r//g;
    $objc->{DATA} =~ s/^object[c|C]lasse?s?:?\s*\(?//;
    $objc->{DATA} =~ s/\Q$objc->{OID}//                      if(defined
$objc->{OID});
    $objc->{DATA} =~ s/NAME\s*\Q$objc->{NAME}\E//            if(defined
$objc->{NAME});
    $objc->{DATA} =~ s/DESC\s*'\Q$objc->{DESC}\E'//          if(defined
$objc->{DESC});
    $objc->{DATA} =~ s/OBSOLETE//                            if(defined
$objc->{OBSOLETE});
```

```
    $objc->{DATA} =~ s/SUP\s*\Q$objc->{SUP}//                 if(defined
$objc->{SUP});
    $objc->{DATA} =~ s/\Q$objc->{TYPE}//                      if(defined
$objc->{TYPE});
    $objc->{DATA} =~ s/MUST\s*\Q$objc->{MUST}\E\s*//          if(defined
$objc->{MUST});
    $objc->{DATA} =~ s/MUST\s*\(?\s*\Q$objc->{MUST}\E\s*\)?// if(defined
$objc->{MUST});
    $objc->{DATA} =~ s/MAY\s*\Q$objc->{MAY}\E//               if(defined
$objc->{MAY});
    $objc->{DATA} =~ s/\)\s$//;
    $objc->{DATA} =~ s/^\s+(\S)/\n$1/  ;
    $objc->{DATA} =~ s/(\S)\s+$/$1\n/;

    do {
      print "#" x 80 ."\n";
      $errorsObjc ++;
      do { $emptyOid++ ;
           print "Warning: no OID for object class element at line $objc-
>{LINENUMBER} \n";
      } if( $objc->{OID} eq "");
      print "### Unknow element embedded in OBJECT CLASS at line $objc-
>{LINENUMBER}:\n$objc->{DATA}\n"
    } if($objc->{DATA} =~ /\w/);
  }

  my $nbDup = 0;
  foreach (keys %dup) {
    my $sumOid = 0;
    $sumOid += @{$dup{$_}{attr}} if(@{$dup{$_}{attr}});
    $sumOid += @{$dup{$_}{objc}} if(@{$dup{$_}{objc}});
    if( $sumOid > 1 && $_ ne "") {
      $nbDup ++;
      print "#" x 80 ."\n";
      print "Duplicate OID founds: $_\n";
      foreach (@{$dup{$_}{attr}}) {

        print "Attribute: $_->{NAME} (line: $_->{LINENUMBER})\n";
      }
      foreach (@{$dup{$_}{objc}}) {
        print "Object class: $_->{NAME} (line: $_->{LINENUMBER})\n";
      }

    }
  }

  print "\n$errorsAttr errors detected in ATTRIBUTES list\n";
  print "$errorsObjc errors detected in OBJECT CLASS list\n";
  print "$nbDup duplicate OID founds\n";
  print "$emptyOid empty OID fields founds\n\n";

}


sub printit {
  my $ldapdata = shift;
  &printSeparator;
  print "dn: cn=schema\n";
  &printSeparator;

foreach (@{$ldapdata->{attributes}}) {
```

```
    my $attr = $_;
    print "attributeTypes: (\n";
    print "  $attr->{OID}\n";
    print "  NAME $attr->{NAME}\n";
    print "  DESC '$attr->{DESC}'\n"         if(defined $attr->{DESC});
    print "  OBSOLETE\n"                     if(defined $attr->{OBSO-
LETE});
    print "  SUP $attr->{SUP}\n"             if(defined $attr->{SUP});
    print "  EQUALITY $attr->{EQUALITY}\n"   if(defined $attr->{EQUAL-
ITY});
    print "  ORDERING $attr->{ORDERING}\n"   if(defined $attr->{ORDER-
ING});
    print "  SUBSTR $attr->{SUBSTR}\n"       if(defined $attr->{SUBSTR});
    print "  SYNTAX $attr->{SYNTAX}\n"       if(defined $attr->{SYNTAX});
    print "  SINGLE-VALUE\n"                 if(defined $attr->{SIN-
GLEVALUE});
    print "  NO-USER-MODIFICATION\n"         if(defined $attr->{NOUSER-
MOD});
    print "  COLLECTIVE\n"                   if(defined $attr->{COLLEC-
TIVE});
    print "  USAGE $attr->{USAGE}\n"         if(defined $attr->{USAGE});
    print "  )\n";
    &printSeparator;
  }

  foreach (@{$ldapdata->{objectclass}}) {
    my $objc = $_;
    $objc->{SUP}         =~ s/^\(\s*(.*?)\s*\)$/\( $1 \)/  if (defined
$objc->{SUP});
    $objc->{MUST}        =~ s/^\(\s*(.*?)\s*\)$/\( $1 \)/  if (defined
$objc->{MUST});
    $objc->{MAY}         =~ s/^\(\s*(.*?)\s*\)$/\( $1 \)/  if (defined
$objc->{MAY});

    print "objectClasses: (\n";
    print "  $objc->{OID}\n";
    print "  NAME $objc->{NAME}\n";
    print "  DESC '$objc->{DESC}'\n"  if(defined $objc->{DESC});
    print "  OBSOLETE\n"              if(defined $objc->{OBSOLETE});
    print "  SUP $objc->{SUP}\n"      if(defined $objc->{SUP});
    print "  $objc->{TYPE}\n"         if(defined $objc->{TYPE});
    print "  MUST $objc->{MUST}\n"    if(defined $objc->{MUST});
    print "  MAY $objc->{MAY}\n"      if(defined $objc->{MAY});
    print "  )\n";
    &printSeparator;
  }
}

sub printSeparator {
  print "#\n";
  print "#" x 80 . "\n";
  print "#\n";
}

sub getSourceFile {
  my @data = &getFile(shift);
  my %result;
  my $result = \%result;
  my @allattrs;
  my @allattrsLineNumber;
  my @allobjc;
```

```
  my @allobjcLineNumber;
  my $at = 0;
  my $oc = 0;
  my $at_string;
  my $oc_string;
  my $idx = 0;
  my $beginParenthesis = 0;
  my $endParenthesis = 0;
  my $lineNumber = 0;
  for(@data) {
    $lineNumber++;
    next if (/^\s*\#/);

    if($at) {
      s/ +/ /;
      s/\t/ /;

       $at_string .= $_;
      $beginParenthesis = 0;
      $endParenthesis = 0;
      for(my $i=0;$ i < length($at_string); $i++) {
        $beginParenthesis++ if(substr ($at_string,$i,1) eq "(");
        $endParenthesis++ if(substr ($at_string,$i,1) eq ")");
      }
      if($beginParenthesis == $endParenthesis) {
        push @allattrs, $at_string;
        $at = 0;
        $at_string = "";
        $endParenthesis = 0;
        $beginParenthesis = 0;
      }
    }

    if (/^attribute[t|T]ype/) {
      my $line = $_;
       push @allattrsLineNumber, $lineNumber;
      for(my $i=0;$ i < length($line); $i++) {
        $beginParenthesis++ if(substr ($line, $i, 1) eq "(");
        $endParenthesis++ if(substr ($line, $i, 1) eq ")");
      }
      if($beginParenthesis == $endParenthesis && $beginParenthesis != 0)
{
        push @allattrs, $line;
        $endParenthesis = 0;
        $beginParenthesis = 0;
      } else {
        $at_string = $line;
        $at = 1;
      }
    }



    if($oc) {
      s/ +/ /;
      s/\t/ /;

      $oc_string .= $_;
      $endParenthesis = 0;
      $beginParenthesis = 0;
      for(my $i=0;$ i < length($oc_string); $i++) {
```

```
        $beginParenthesis++ if(substr ($oc_string, $i, 1) eq "(");
        $endParenthesis++ if(substr ($oc_string, $i, 1) eq ")");
      }
      if($beginParenthesis == $endParenthesis) {
        push @allobjc, $oc_string;
        $oc = 0;
        $oc_string = "";
        $endParenthesis = 0;
        $beginParenthesis = 0;
      }
    }

    if (/^object[c|C]lass/) {
      my $line = $_;
       push @allobjcLineNumber, $lineNumber;
      for(my $i=0;$ i < length($line); $i++) {
        $beginParenthesis++ if(substr ($line, $i, 1) eq "(");
        $endParenthesis++ if(substr ($line, $i, 1) eq ")");
      }
      if($beginParenthesis == $endParenthesis && $beginParenthesis != 0)
{
        push @allobjc, $line;
        $endParenthesis = 0;
        $beginParenthesis = 0;
      } else {
        $oc_string = $line;
        $oc = 1;
      }
    }
  }



  for(@allattrs) {
    s/\n/ /g;
    s/\r//g;
    s/ +/ /g;
    s/\t/ /g;
    $result->{attributes}->[$idx]->{DATA}        = $_
if($optionBadEntries);
    $result->{attributes}->[$idx]->{LINENUMBER}  = $allattrsLine-
Number[$idx];
    $result->{attributes}->[$idx]->{OID}         = $1              if
(m/^attribute[t|T]ypes?:?\s*\(?\s*([\.\d]*?)\s+/);
    $result->{attributes}->[$idx]->{NAME}        = $1              if
(m/NAME\s+('.*?')\s*/ || m/NAME\s+(\(.*?\))/);
    $result->{attributes}->[$idx]->{DESC}        = $1              if
(m/DESC\s+'(.*?)'\s*/);
    $result->{attributes}->[$idx]->{OBSOLETE}    = "OBSOLETE"      if
(m/OBSOLETE/);
    $result->{attributes}->[$idx]->{SUP}         = $1              if
(m/SUP\s+(.*?)\s/);
    $result->{attributes}->[$idx]->{EQUALITY}    = $1              if
(m/EQUALITY\s+(.*?)\s/);
    $result->{attributes}->[$idx]->{ORDERING}    = $1              if
(m/ORDERING\s+(.*?)\s/);
    $result->{attributes}->[$idx]->{SUBSTR}      = $1              if
(m/SUBSTR\s+(.*?)\s/);
    $result->{attributes}->[$idx]->{SYNTAX}      = $1              if
(m/SYNTAX\s+(.*?)(\s|\))/);
```

```
    $result->{attributes}->[$idx]->{SINGLEVALUE} = "SINGLE-VALUE"  if
(m/SINGLE-VALUE/);
    $result->{attributes}->[$idx]->{COLLECTIVE}  = "COLLECTIVE"    if
(m/COLLECTIVE/);
    $result->{attributes}->[$idx]->{USAGE}       = $1              if
(m/USAGE\s+(.*?)\s/);
    $result->{attributes}->[$idx]->{NOUSERMOD}   = "NO-USER-MODIFICATION"
if (m/NO-USER-MODIFICATION/);
    $idx ++;
  }

  $idx = 0;



  for(@allobjc) {
    s/\n/ /g;
    s/\r//g;
    s/ +/ /g;
    s/\t/ /g;
    $result->{objectclass}->[$idx]->{DATA}        = $_          if($op-
tionBadEntries);
    $result->{objectclass}->[$idx]->{LINENUMBER}  = $allobjcLine-
Number[$idx];
    $result->{objectclass}->[$idx]->{OID}         = $1          if
(m/^object[c|C]lasse?s?:?\s*\(?\s*([\.\d]*?)\s+/);
    $result->{objectclass}->[$idx]->{NAME}        = $1          if
(m/NAME\s+('.*?')\s*/ || m/NAME\s+(\(.*?\))/);
    $result->{objectclass}->[$idx]->{DESC}        =  $1         if
(m/DESC\s+'(.*?)'\s*/);
    $result->{objectclass}->[$idx]->{OBSOLETE}    = "OBSOLETE"  if (m/OB-
SOLETE/);
    $result->{objectclass}->[$idx]->{SUP}         = $1          if
(m/SUP\s+([^()]+?)\s/ || m/SUP\s+(\(.+?\))\s/);
    $result->{objectclass}->[$idx]->{TYPE}        = $1          if
(m/((?:STRUCTURAL)|(?:AUXILIARY)|(?:ABSTRACT))/);
    $result->{objectclass}->[$idx]->{MUST}        = $1          if
(m/MUST\s+(\w+)\)?/ || m/MUST\s+(\(.*?\))(\s|\))/s);
    $result->{objectclass}->[$idx]->{MAY}         = $1          if
(m/MAY\s+(\w+)\)?/ || m/MAY\s+(\(.*?\))(\s|\))/s);

    $idx++;
  }

  return $result;
}

sub getFile {
  my @data;
  my $file = shift;
  die "File not found: $file\n" if(! -e $file);
  open FH, $file;
  @data = <FH>;
  close FH;
  @data;
}
```

Κώδικας 2: Παρακάτω παρατίθεται το αρχείο σχήματος 60core.ldif , το οποίο είναι ένα από τα πέντε αρχεία σχήματος που χρειάζεται ο Διακομιστής Καταλόγου 389 ώστε να εισαχθούν επιτυχώς τα δεδομένα.

```
[root@openldpap-gdpr ~]# cat /etc/dirsrv/slapd-openldpap-
gdpr/schema/60core.ldif
#
########################################################################
######
#
dn: cn=schema
#
########################################################################
######
#
attributeTypes: (
  2.5.4.2
  NAME 'knowledgeInformation'
  DESC 'RFC2256: knowledge information'
  EQUALITY caseIgnoreMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.4
  NAME ( 'sn' 'surname' )
  DESC 'RFC2256: last (family) name(s) for which the entity is known by'
  SUP name
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.5
  NAME 'serialNumber'
  DESC 'RFC2256: serial number of the entity'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{64}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.6
  NAME ( 'c' 'countryName' )
  DESC 'RFC4519: two-letter ISO-3166 country code'
  SUP name
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.11
  SINGLE-VALUE
  )
#
```

```
#########################################################################
######
#
attributeTypes: (
  2.5.4.7
  NAME ( 'l' 'localityName' )
  DESC 'RFC2256: locality which this object resides in'
  SUP name
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.8
  NAME ( 'st' 'stateOrProvinceName' )
  DESC 'RFC2256: state or province which this object resides in'
  SUP name
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.9
  NAME ( 'street' 'streetAddress' )
  DESC 'RFC2256: street address of this object'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.10
  NAME ( 'o' 'organizationName' )
  DESC 'RFC2256: organization this object belongs to'
  SUP name
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.11
  NAME ( 'ou' 'organizationalUnitName' )
  DESC 'RFC2256: organizational unit this object belongs to'
  SUP name
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.12
  NAME 'title'
  DESC 'RFC2256: title associated with the entity'
  SUP name
  )
```

```
#
########################################################################
######
#
attributeTypes: (
  2.5.4.14
  NAME 'searchGuide'
  DESC 'RFC2256: search guide, deprecated by enhancedSearchGuide'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.25
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.15
  NAME 'businessCategory'
  DESC 'RFC2256: business category'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.16
  NAME 'postalAddress'
  DESC 'RFC2256: postal address'
  EQUALITY caseIgnoreListMatch
  SUBSTR caseIgnoreListSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.41
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.17
  NAME 'postalCode'
  DESC 'RFC2256: postal code'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{40}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.18
  NAME 'postOfficeBox'
  DESC 'RFC2256: Post Office Box'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{40}
  )
#
########################################################################
######
```

```
#
attributeTypes: (
  2.5.4.19
  NAME 'physicalDeliveryOfficeName'
  DESC 'RFC2256: Physical Delivery Office Name'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{128}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.20
  NAME 'telephoneNumber'
  DESC 'RFC2256: Telephone Number'
  EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.21
  NAME 'telexNumber'
  DESC 'RFC2256: Telex Number'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.52
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.22
  NAME 'teletexTerminalIdentifier'
  DESC 'RFC2256: Teletex Terminal Identifier'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.51
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.23
  NAME ( 'facsimileTelephoneNumber' 'fax' )
  DESC 'RFC2256: Facsimile (Fax) Telephone Number'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.22
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.24
  NAME 'x121Address'
  DESC 'RFC2256: X.121 Address'
  EQUALITY numericStringMatch
  SUBSTR numericStringSubstringsMatch
```

```
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{15}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.25
  NAME 'internationaliSDNNumber'
  DESC 'RFC2256: international ISDN number'
  EQUALITY numericStringMatch
  SUBSTR numericStringSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.36{16}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.26
  NAME 'registeredAddress'
  DESC 'RFC2256: registered postal address'
  SUP postalAddress
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.41
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.27
  NAME 'destinationIndicator'
  DESC 'RFC2256: destination indicator'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{128}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.28
  NAME 'preferredDeliveryMethod'
  DESC 'RFC2256: preferred delivery method'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.14
  SINGLE-VALUE
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.29
  NAME 'presentationAddress'
  DESC 'RFC2256: presentation address'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
  )
#
```

```
#########################################################################
######
#
attributeTypes: (
  2.5.4.30
  NAME 'supportedApplicationContext'
  DESC 'RFC2256: supported application context'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.31
  NAME 'member'
  DESC 'RFC2256: member of a group'
  SUP distinguishedName
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.32
  NAME 'owner'
  DESC 'RFC2256: owner (of the object)'
  SUP distinguishedName
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.33
  NAME 'roleOccupant'
  DESC 'RFC2256: occupant of role'
  SUP distinguishedName
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.42
  NAME ( 'givenName' 'gn' )
  DESC 'RFC2256: first name(s) for which the entity is known by'
  SUP name
  )
#
#########################################################################
######
#
attributeTypes: (
  2.5.4.43
  NAME 'initials'
  DESC 'RFC2256: initials of some or all of names, but not the sur-
name(s).'
  SUP name
  )
```

```
#
########################################################################
######
#
attributeTypes: (
  2.5.4.44
  NAME 'generationQualifier'
  DESC 'RFC2256: name qualifier indicating a generation'
  SUP name
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.45
  NAME 'x500UniqueIdentifier'
  DESC 'RFC2256: X.500 unique identifier'
  EQUALITY bitStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.6
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.46
  NAME 'dnQualifier'
  DESC 'RFC2256: DN qualifier'
  EQUALITY caseIgnoreMatch
  ORDERING caseIgnoreOrderingMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.44
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.47
  NAME 'enhancedSearchGuide'
  DESC 'RFC2256: enhanced search guide'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.21
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.50
  NAME 'uniqueMember'
  DESC 'RFC2256: unique member of a group'
  EQUALITY uniqueMemberMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.34
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.51
```

```
  NAME 'houseIdentifier'
  DESC 'RFC2256: house identifier'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.54
  NAME 'dmdName'
  DESC 'RFC2256: name of DMD'
  SUP name
  )
#
########################################################################
######
#
attributeTypes: (
  2.5.4.65
  NAME 'pseudonym'
  DESC 'X.520(4th): pseudonym for the object'
  SUP name
  )
#
########################################################################
######
#
attributeTypes: (
  0.9.2342.19200300.100.1.3
  NAME ( 'mail' 'rfc822Mailbox' )
  DESC 'RFC1274: RFC822 Mailbox'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256}
  )
#
########################################################################
######
#
attributeTypes: (
  0.9.2342.19200300.100.1.25
  NAME ( 'dc' 'domainComponent' )
  DESC 'RFC1274/2247: domain component'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  SINGLE-VALUE
  )
#
########################################################################
######
#
attributeTypes: (
  0.9.2342.19200300.100.1.37
  NAME 'associatedDomain'
  DESC 'RFC1274: domain associated with object'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
```

```
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
  )
#
##########################################################################
######
#
attributeTypes: (
  1.2.840.113549.1.9.1
  NAME ( 'email' 'emailAddress' 'pkcs9email' )
  DESC 'RFC3280: legacy attribute for email addresses in DNs'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128}
  )
#
##########################################################################
######
#
objectClasses: (
  2.5.6.2
  NAME 'country'
  DESC 'RFC2256: a country'
  SUP top
  STRUCTURAL
  MUST c
  MAY ( searchGuide $ description )
  )
#
##########################################################################
######
#
objectClasses: (
  2.5.6.3
  NAME 'locality'
  DESC 'RFC2256: a locality'
  SUP top
  STRUCTURAL
  MAY ( street $ seeAlso $ searchGuide $ st $ l $ description )
  )
#
##########################################################################
######
#
objectClasses: (
  2.5.6.4
  NAME 'organization'
  DESC 'RFC2256: an organization'
  SUP top
  STRUCTURAL
  MUST o
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $  x121Ad-
dress $ registeredAddress $ destinationIndicator $  preferredDelivery-
Method $ telexNumber $ teletexTerminalIdentifier $  telephoneNumber $ in-
ternationaliSDNNumber $  facsimileTelephoneNumber $ street $ postOfficeBox
$ postalCode $  postalAddress $ physicalDeliveryOfficeName $ st $ l $ de-
scription )
  )
#
##########################################################################
######
#
```

```
objectClasses: (
  2.5.6.5
  NAME 'organizationalUnit'
  DESC 'RFC2256: an organizational unit'
  SUP top
  STRUCTURAL
  MUST ou
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $  x121Ad-
dress $ registeredAddress $ destinationIndicator $  preferredDelivery-
Method $ telexNumber $ teletexTerminalIdentifier $  telephoneNumber $ in-
ternationaliSDNNumber $  facsimileTelephoneNumber $ street $ postOfficeBox
$ postalCode $  postalAddress $ physicalDeliveryOfficeName $ st $ l $ de-
scription )
  )
#
##############################################################################
######
#
objectClasses: (
  2.5.6.6
  NAME 'person'
  DESC 'RFC2256: a person'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( sn $ userPassword $ telephoneNumber $ seeAlso $ description )
  )
#
##############################################################################
######
#
objectClasses: (
  2.5.6.7
  NAME 'organizationalPerson'
  DESC 'RFC2256: an organizational person'
  SUP person
  STRUCTURAL
  MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $
preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $  tele-
phoneNumber $ internationaliSDNNumber $  facsimileTelephoneNumber $ street
$ postOfficeBox $ postalCode $  postalAddress $ physicalDeliveryOfficeName
$ ou $ st $ l )
  )
#
##############################################################################
######
#
objectClasses: (
  2.5.6.8
  NAME 'organizationalRole'
  DESC 'RFC2256: an organizational role'
  SUP top
  STRUCTURAL
  MUST cn
  MAY ( x121Address $ registeredAddress $ destinationIndicator $  pre-
ferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $  tele-
phoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $
seeAlso $ roleOccupant $ preferredDeliveryMethod $ street $  postOfficeBox
$ postalCode $ postalAddress $  physicalDeliveryOfficeName $ ou $ st $ l $
description )
  )
```

```
#
########################################################################
######
#
objectClasses: (
  2.5.6.9
  NAME 'groupOfNames'
  DESC 'RFC2256: a group of names (DNs)'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( businessCategory $ member $ seeAlso $ owner $ ou $ o $ description
)
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.10
  NAME 'residentialPerson'
  DESC 'RFC2256: an residential person'
  SUP person
  STRUCTURAL
  MUST l
  MAY ( businessCategory $ x121Address $ registeredAddress $  destination-
Indicator $ preferredDeliveryMethod $ telexNumber $  teletexTerminalI-
dentifier $ telephoneNumber $ internationaliSDNNumber $  facsimileTele-
phoneNumber $ preferredDeliveryMethod $ street $  postOfficeBox $ post-
alCode $ postalAddress $  physicalDeliveryOfficeName $ st $ l )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.11
  NAME 'applicationProcess'
  DESC 'RFC2256: an application process'
  SUP top
  STRUCTURAL
  MUST cn
  MAY ( seeAlso $ ou $ l $ description )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.12
  NAME 'applicationEntity'
  DESC 'RFC2256: an application entity'
  SUP top
  STRUCTURAL
  MUST ( presentationAddress $ cn )
  MAY ( supportedApplicationContext $ seeAlso $ ou $ o $ l $ description )
  )
#
########################################################################
######
#
```

```
objectClasses: (
  2.5.6.13
  NAME 'dSA'
  DESC 'RFC2256: a directory system agent (a server)'
  SUP applicationEntity
  STRUCTURAL
  MAY knowledgeInformation
  )
#
################################################################################
######
#
objectClasses: (
  2.5.6.14
  NAME 'device'
  DESC 'RFC2256: a device'
  SUP top
  STRUCTURAL
  MUST cn
  MAY ( serialNumber $ seeAlso $ owner $ ou $ o $ l $ description $ us-
ercertificate )
  )
#
################################################################################
######
#
objectClasses: (
  2.5.6.15
  NAME 'strongAuthenticationUser'
  DESC 'RFC2256: a strong authentication user'
  SUP top
  AUXILIARY
  MUST userCertificate
  )
#
################################################################################
######
#
objectClasses: (
  2.5.6.16
  NAME 'certificationAuthority'
  DESC 'RFC2256: a certificate authority'
  SUP top
  AUXILIARY
  MUST ( authorityRevocationList $ certificateRevocationList $  cACertifi-
cate )
  MAY crossCertificatePair
  )
#
################################################################################
######
#
objectClasses: (
  2.5.6.17
  NAME 'groupOfUniqueNames'
  DESC 'RFC2256: a group of unique names (DN and Unique Identifier)'
  SUP top
  STRUCTURAL
  MUST ( uniqueMember $ cn )
  MAY ( businessCategory $ seeAlso $ owner $ ou $ o $ description )
  )
```

```
#
########################################################################
######
#
objectClasses: (
  2.5.6.18
  NAME 'userSecurityInformation'
  DESC 'RFC2256: a user security information'
  SUP top
  AUXILIARY
  MAY ( supportedAlgorithms )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.16.2
  NAME 'certificationAuthority-V2'
  SUP certificationAuthority
  AUXILIARY
  MAY ( deltaRevocationList )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.19
  NAME 'cRLDistributionPoint'
  SUP top
  STRUCTURAL
  MUST ( cn )
  MAY ( certificateRevocationList $ authorityRevocationList $  deltaRevo-
cationList )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.20
  NAME 'dmd'
  SUP top
  STRUCTURAL
  MUST ( dmdName )
  MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $  x121Ad-
dress $ registeredAddress $ destinationIndicator $  preferredDelivery-
Method $ telexNumber $ teletexTerminalIdentifier $  telephoneNumber $ in-
ternationaliSDNNumber $ facsimileTelephoneNumber $  street $ postOfficeBox
$ postalCode $ postalAddress $  physicalDeliveryOfficeName $ st $ l $ de-
scription )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.21
  NAME 'pkiUser'
  DESC 'RFC2587: a PKI user'
```

```
  SUP top
  AUXILIARY
  MAY userCertificate
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.22
  NAME 'pkiCA'
  DESC 'RFC2587: PKI certificate authority'
  SUP top
  AUXILIARY
  MAY ( authorityRevocationList $ certificateRevocationList $  cACertifi-
cate $ crossCertificatePair $ uid )
  )
#
########################################################################
######
#
objectClasses: (
  2.5.6.23
  NAME 'deltaCRL'
  DESC 'RFC2587: PKI user'
  SUP top
  AUXILIARY
  MAY deltaRevocationList
  )
#
########################################################################
######
#
objectClasses: (
  1.3.6.1.4.1.250.3.15
  NAME 'labeledURIObject'
  DESC 'RFC2079: object that contains the URI attribute type'
  SUP top
  AUXILIARY
  MAY ( labeledURI )
  )
#
########################################################################
######
#
objectClasses: (
  0.9.2342.19200300.100.4.19
  NAME 'simpleSecurityObject'
  DESC 'RFC1274: simple security object'
  SUP top
  AUXILIARY
  MUST userPassword
  )
#
########################################################################
######
#
objectClasses: (
  1.3.6.1.4.1.1466.344
  NAME 'dcObject'
  DESC 'RFC2247: domain component object'
```

```
  SUP top
  AUXILIARY
  MUST dc
  )
#
########################################################################
######
#
objectClasses: (
  1.3.6.1.1.3.1
  NAME 'uidObject'
  DESC 'RFC2377: uid object'
  SUP top
  AUXILIARY
  MUST uid
  )
```

Κώδικας 3: Παρακάτω φαίνονται τα κλαδιά που έπρεπε να δημιουργηθούν ώστε να μπορούν να εισαχθούν επιτυχώς τα δεδομένα των σχολείων.

```
[root@openldpap-gdpr ~]# cat /home/dkalo/60add.ldif

dn: ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Units

dn: ou=Perif,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Perif

dn: ou=Aei,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Aei

dn: ou=Ypaideias,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Ypaideias

dn: ou=Gov,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Gov

dn: ou=thess-a,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: thess-a

dn: ou=thess-v,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: thess-v

dn: ou=noc,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: noc

dn: ou=cy,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: cy

dn: ou=Australia,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Australia

dn: ou=World,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: World
```

```
dn: ou=ao,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ao

dn: ou=Europe,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Europe

dn: ou=att-v,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-v

dn: ou=att-peiraia,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-peiraia

dn: ou=att-dytik,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-dytik

dn: ou=att-g,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-g

dn: ou=att-anatol,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-anatol

dn: ou=att-d,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-d

dn: ou=pde,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: pde

dn: ou=att-a,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att-a

dn: ou=Te,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Te

dn: ou=Ypepth,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Ypepth
```

```
dn: ou=Partners,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: Partners

dn: ou=ark,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ark

dn: ou=ach,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ach

dn: ou=ait,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ait

dn: ou=arg,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: arg

dn: ou=art,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: art

dn: ou=att,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: att

dn: ou=chal,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: chal

dn: ou=chan,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: chan

dn: ou=chi,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: chi

dn: ou=dod,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: dod

dn: ou=dra,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: dra

dn: ou=evr,ou=Units,dc=sch,dc=gr
```

```
objectClass: organizationalunit
objectClass: top
ou: evr

dn: ou=eyr,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: eyr

dn: ou=eyv,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: eyv

dn: ou=flo,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: flo

dn: ou=fok,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: fok

dn: ou=fth,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: fth

dn: ou=gre,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: gre

dn: ou=ilei,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ilei

dn: ou=ima,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ima

dn: ou=ioa,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ioa

dn: ou=ira,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ira

dn: ou=kar,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kar

dn: ou=kas,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
```

```
objectClass: top
ou: kas

dn: ou=kav,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kav

dn: ou=kef,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kef

dn: ou=ker,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ker

dn: ou=kil,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kil

dn: ou=kor,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kor

dn: ou=koz,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: koz

dn: ou=kyk,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: kyk

dn: ou=lak,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: lak

dn: ou=lar,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: lar

dn: ou=las,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: las

dn: ou=lef,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: lef

dn: ou=les,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
```

```
ou: les

dn: ou=mag,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: mag

dn: ou=mes,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: mes

dn: ou=pel,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: pel

dn: ou=pie,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: pie

dn: ou=pre,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: pre

dn: ou=reth,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: reth

dn: ou=rod,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: rod

dn: ou=ser,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: ser

dn: ou=sam,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: sam

dn: ou=tri,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: tri

dn: ou=thess,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: thess

dn: ou=thesp,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: thesp
```

```
dn: ou=voi,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: voi

dn: ou=xan,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: xan

dn: ou=zak,ou=Units,dc=sch,dc=gr
objectClass: organizationalunit
objectClass: top
ou: zak
```