ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Κρυπτογραφική διαχείριση ψηφιακών δικαιωμάτων

ΒΡΟΥΒΑΣ ΓΕΩΡΓΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος Διδάσκων

Λαμία, 13 Ιουλίου 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Κρυπτογραφική διαχείριση ψηφιακών δικαιωμάτων

ΒΡΟΥΒΑΣ ΓΕΩΡΓΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος Διδάσκων

Λαμία, 13 Ιουλίου 2023

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Cryptographic management of digital rights

VROUVAS GEORGIOS

FINAL THESIS

ADVISOR

Georgios Lioudakis
Adjunct Lecturer

Lamia, 13 July 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 13/07/2023

Ο Δηλ.
Βρούβας Γεώργιος

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία φιλοδοξεί στο να συνεισφέρει στο πρόβλημα εφαρμογής των αδειών που χρησιμοποιούνται στο πλαίσιο της διαχείρισης ψηφιακών δικαιωμάτων πάνω από τα ψηφιακά αρχεία. Τα τελευταία χρόνια, έχει παρατηρηθεί ένα αυξανόμενο ενδιαφέρον από τους χρήστες να θέλουν να προστατεύουν τα ψηφιακά τους τεκμήρια και η διαχείριση ψηφιακών δικαιωμάτων είναι ιδανική για κάτι τέτοιο. Στο πλαίσιο αυτό χρησιμοποιείται η γλώσσα έκφρασης δικαιωμάτων ODRL σε συνδυασμό με την τεχνική Κρυπτογράφησης βάσει Χαρακτηριστικών. Στην συγκεκριμένη πτυχιακή παρουσιάζονται αναλυτικά οι υποκείμενοι μηχανισμοί καθώς και το σύστημα που υλοποιήθηκε.

ABSTRACT

This thesis aspires to contribute to the problem of the application of licenses used in the context of digital rights management in digital archives. In recent years, there has been a growing interest from users to want to protect their digital assets, and digital rights management is ideal for this. In this context, the ODRL rights expression language is used in conjunction with the attribute-based encryption technique. In this specific thesis, the underlying mechanisms as well as the applied system are presented in detail.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Τα τελευταία χρόνια, έχει παρατηρηθεί ένα αυξανόμενο ενδιαφέρον από τους χρήστες να θέλουν να προστατεύουν τα ψηφιακά τους τεκμήρια και η διαχείριση ψηφιακών δικαιωμάτων είναι ιδανική για κάτι τέτοιο. Ωστόσο, οι τεχνολογίες αυτές έχουν ένα πολύ σημαντικό περιορισμό. Όταν τα ψηφιακά τεκμήρια φεύγουν από τον κάτοχο τους, τότε τίποτα δεν διασφαλίζει ότι θα τηρηθούν οι πολιτικές χρήσης που έχουν ορισθεί. Μια πιθανή λύση για το προαναφερθέν πρόβλημα είναι η Κρυπτογράφηση Βάσει Χαρακτηριστικών, όπου η αποκρυπτογράφηση ή μη των τεκμηρίων, εξετάζεται από τα χαρακτηριστικά που διαθέτει ο παραλήπτης.

Λαμβάνοντας υπόψη όλα τα παραπάνω, η πτυχιακή περιγράφει έναν μηχανισμό προστασίας χρήσης αρχείων. Πιο συγκεκριμένα, χρησιμοποιεί την γλώσσα έκφρασης δικαιωμάτων ODRL σε συνδυασμό με την τεχνική κρυπτογράφησης CP-ABE.

Η πτυχιακή εργασία διαρθρώνεται ως εξής: Στο κεφάλαιο δύο παρουσιάζεται η κρυπτογραφία και οι σύγχρονες τεχνολογίες της, με την μεγαλύτερη έμφαση να δίνεται στην Κρυπτογραφία βάσει Χαρακτηριστικών που χρησιμοποιούμε και στο σύστημα μας. Στο κεφάλαιο τρία γίνεται μια επισκόπηση στο ζήτημα της διαχείρισης ψηφιακών δικαιωμάτων, ενώ πιο αναλυτικά παρουσιάζεται η γλώσσα έκφρασης δικαιωμάτων ODRL. Επιπλέον, στο κεφάλαιο τέσσερα γίνεται αναφορά στις απαιτήσεις του συστήματος, στην αρχιτεκτονική του και στις τεχνολογίες που μας βοήθησαν στην υλοποίηση του. Τέλος, παρουσιάζεται ένα παράδειγμα χρήσης του συστήματος μας ώστε να γίνει κατανοητή η λειτουργία και ο τρόπος εφαρμογής του σε πραγματικές καταστάσεις.

ΚΕΦΑΛΑΙΟ 2 Κρυπτογραφία

2.1 Εισαγωγή στην κρυπτογραφία

2.1.α Βασικές έννοιες

Η κρυπτολογία είναι η μελέτη και η διαδικασία κωδικοποίησης και αποκωδικοποίησης απλών μηνυμάτων κειμένου έτσι ώστε να μην μπορούν να διαβαστούν από κανέναν χωρίς οδηγό ή κλειδί. Η κρυπτολογία χωρίζεται στους εξής δύο κλάδους:

1. Κρυπτογραφία: Ο κλάδος αυτός ασχολείται με την προστασία των πληροφοριών μετατρέποντάς τις σε μη αναγνώσιμη μορφή, έτσι ώστε μόνο εξουσιοδοτημένα πρόσωπα να μπορούν να τις διαβάσουν. Αυτό γίνεται με τη χρήση μαθηματικών αλγορίθμων και πλήκτρων που αναμειγνύουν και αποκωδικοποιούν δεδομένα με τρόπο που είναι δύσκολο να αντιστραφεί χωρίς το σωστό κλειδί.

2. Κρυπτανάλυση: Εν αντιθέση με την κρυπτογραφία, η κρυπτανάλυση στοχεύει στην διάσπαση ή την αποκρυπτογράφηση κρυπτογραφημένων πληροφοριών χωρίς τη γνώση του κλειδιού. Περιλαμβάνει ανάλυση και χειρισμό κρυπτογραφημένων δεδομένων για την αποκάλυψη του αρχικού μηνύματος ή κλειδιού.

Συνοπτικά, η κρυπτογραφία και η κρυπτανάλυση είναι δύο σημαντικά πεδία μελέτης στην ασφάλεια πληροφοριών. Η κρυπτογραφία παρέχει έναν τρόπο προστασίας ευαίσθητων πληροφοριών, ενώ η κρυπτανάλυση βοηθά στον εντοπισμό αδυναμιών στα κρυπτογραφικά συστήματα και στη βελτίωση της ασφάλειάς τους.

Το κύριο θέμα της συγκεκριμένης εργασίας είναι η κρυπτογραφία στην οποία και θα εστιάσουμε, παραθέτοντας κάποιες πληροφορίες σχετικά με αυτήν.

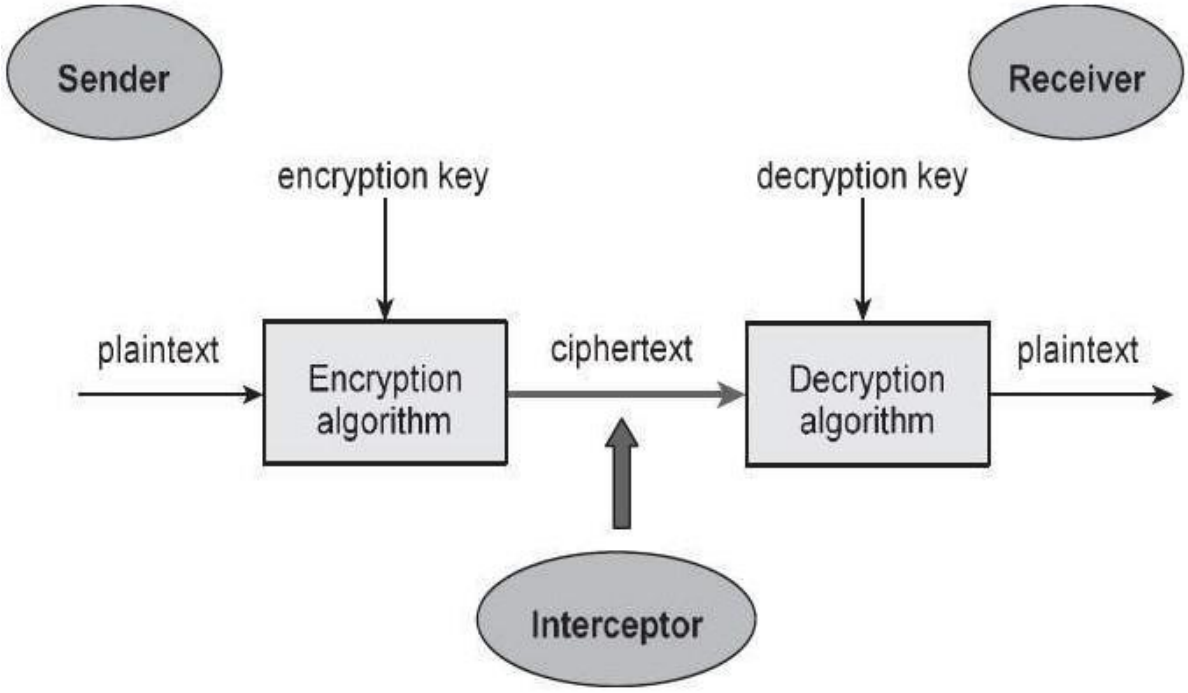
Η κρυπτογραφία είναι μια τεχνική για την επίτευξη εμπιστευτικότητας των μηνυμάτων. Ο όρος έχει συγκεκριμένη σημασία στα ελληνικά: «μυστική γραφή". Στις μέρες μας, ωστόσο, η ιδιωτικότητα των ατόμων και των οργανισμών παρέχεται μέσω κρυπτογραφίας σε υψηλό επίπεδο, διασφαλίζοντας ότι οι πληροφορίες που αποστέλλονται είναι ασφαλείς με τρόπο που ο εξουσιοδοτημένος δέκτης να μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες. Κοιτώντας πίσω στον χρόνο η κρυπτογραφία μπορεί να θεωρηθεί παλιά τεχνική που ακόμη αναπτύσσεται. Τα παραδείγματα φτάνουν πίσω στο 2000 π.Χ., όταν οι αρχαίοι Αιγύπτιοι χρησιμοποιούσαν «μυστικά» ιερογλυφικά, καθώς και άλλα στοιχεία με τη μορφή μυστικής γραφής στην αρχαία Ελλάδα ή τον περίφημο Κώδικα του Καίσαρα στην Αρχαία Ρώμη.

Δισεκατομμύρια άνθρωποι σε όλο τον κόσμο χρησιμοποιούν κρυπτογραφία σε καθημερινή βάση για την προστασία δεδομένων και πληροφοριών, αν και οι περισσότεροι δεν γνωρίζουν ότι το χρησιμοποιούν. Εκτός από εξαιρετικά χρήσιμο, θεωρείται επίσης και ιδιαίτερα εύθραυστο, καθώς τα κρυπτογραφικά συστήματα μπορούν να τεθούν σε κίνδυνο λόγω ενός σφάλματος προγραμματισμού ή προδιαγραφών.

Η κρυπτογραφία παρέχει 3 βασικές λειτουργίες («αντικειμενικοί σκοποί»):

- *Εμπιστευτικότητα*: Κατά τη μετάδοση δεδομένων, ο αποστολέας δεν θέλει κάποιον που κρυφακούει να καταλάβει το περιεχόμενο των μεταδιδόμενων μηνυμάτων. Το ίδιο ισχύει για τα αποθηκευμένα δεδομένα που πρέπει να προστατεύονται ενάντια σε μη εξουσιοδοτημένη πρόσβαση, για παράδειγμα από χάκερς.
- *Ακεραιότητα*: Αυτό σημαίνει ότι ο παραλήπτης ορισμένων δεδομένων έχει στοιχεία ότι δεν έχουν γίνει αλλαγές από κάποιον τρίτο.
- *Πιστοποίηση*: Αυτή η ιδιότητα ισοδυναμεί με υπογραφή. Ο παραλήπτης ενός μηνύματος θέλει απόδειξη ότι ένα μήνυμα προέρχεται από έναν συγκεκριμένο αποστολέα και όχι από κάποιον άλλον(ακόμα και αν ο αρχικός αποστολέας αργότερα θέλει να το αρνηθεί).

Στην κρυπτογραφία, οι κρυφές πληροφορίες ονομάζονται συνήθως «απλό κείμενο» και η διαδικασία συγκάλυψης του απλού κειμένου ορίζεται ως «κρυπτογράφηση»· το κρυπτογραφημένο απλό κείμενο είναι γνωστό ως «κρυπτογραφημένο κείμενο». Αυτή η διαδικασία επιτυγχάνεται με διάφορους κανόνες γνωστοί ως «αλγόριθμοι κρυπτογράφησης». Συνήθως, η διαδικασία της κρυπτογράφησης βασίζεται σε ένα «κλειδί κρυπτογράφησης», το οποίο στη συνέχεια δίνεται στο αλγόριθμο κρυπτογράφησης ως είσοδος μαζί με τις πληροφορίες. Χρησιμοποιώντας έναν «αλγόριθμο αποκρυπτογράφησης», η παραληφθείσα πλευρά μπορεί να ανακτήσει τις πληροφορίες χρησιμοποιώντας το κατάλληλο «κλειδί αποκρυπτογράφησης»



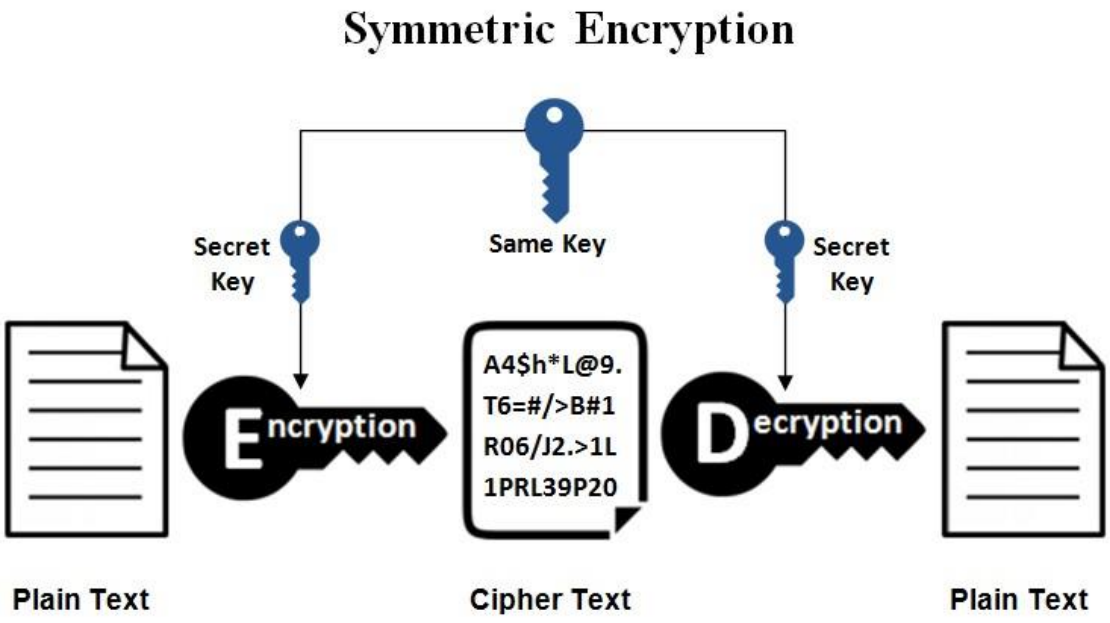
Σχήμα 2.1.1: Έννοια κρυπτογραφίας

2.1.β Τεχνικές κρυπτογράφησης

Οι τρόποι κατηγοριοποίησης των τύπων κρυπτογράφησης ποικίλουν. Στην συγκεκριμένη εργασία αυτή η κατηγοριοποίηση θα γίνει με βάση τα κλειδιά χρησιμοποιούνται για τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης. Με αυτόν τον τρόπο προκύπτουν οι εξής 3 τύποι κρυπτογράφησης:

1. Συμμετρική Κρυπτογράφηση

Η κρυπτογραφία συμμετρικού κλειδιού αναφέρεται σε μεθόδους κρυπτογράφησης, στην οποία ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί. Συμμετρικά κλειδιά κρυπτογράφησης είτε χρησιμοποιούνται ως μπλοκ κρυπτογράφησης ή ως κρυπτογράφηση ροής. Ένα κρυπτογραφικό μπλοκ κρυπτογραφεί τον τύπο εισόδου που χρησιμοποιείται από μια κρυπτογραφική ροή, σε μπλοκ απλού κειμένου σε αντίθεση με μεμονωμένους χαρακτήρες. Η συμμετρική κρυπτογραφία είναι πολύ πιο γρήγορη από την ασύμμετρη. Η συμμετρική κρυπτογράφηση φαίνεται στο Σχήμα 2.1.2.

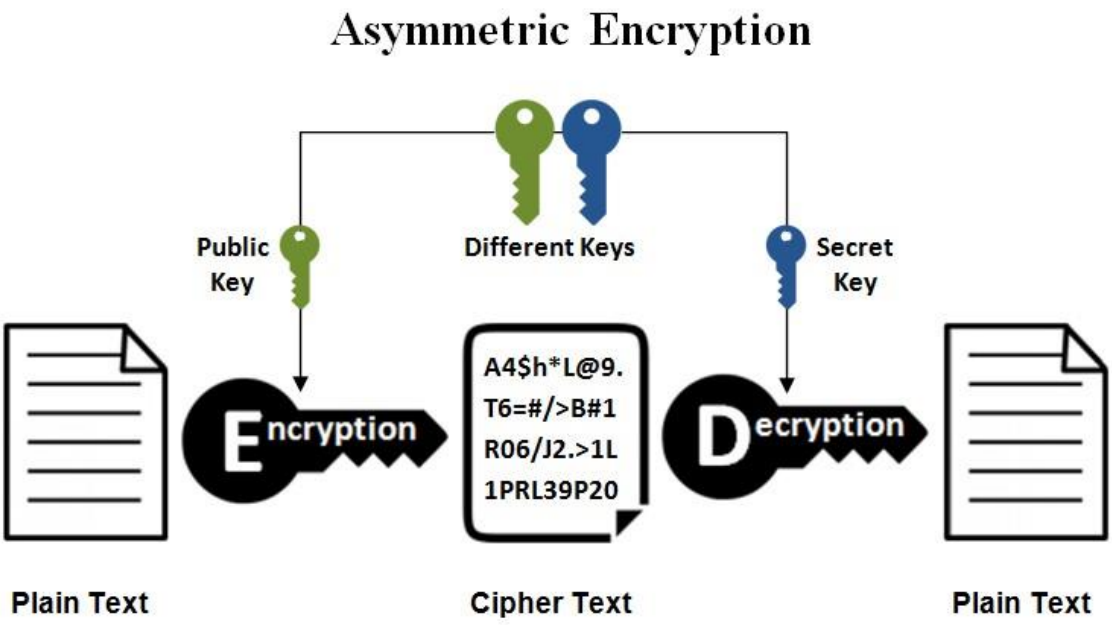


Σχήμα 2.1.2: Συμμετρική κρυπτογράφηση[14]

Αυτή είναι η απλούστερη μέθοδος κρυπτογράφησης, που απαιτεί μόνο ένα μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση πληροφοριών. Η συμμετρική κρυπτογράφηση είναι παλιά τεχνική και είναι πιο γνωστή. Χρησιμοποιεί ένα μυστικό κλειδί που μπορεί να είναι ένας αριθμός, μια φράση ή μια τυχαία συμβολοσειρά γραμμάτων. Για να τροποποιηθεί το υλικό με συγκεκριμένο τρόπο συνδυάζεται με το απλό κείμενο ενός εγγράφου. Ο αποστολέας και ο παραλήπτης θα γνώριζαν το μυστικό κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση και αποκρυπτογράφηση όλων των μηνυμάτων. Παραδείγματα συμμετρικής κρυπτογράφησης περιλαμβάνουν το DES, TDES, AES, Blowfish και RC4. Το AES-128, AES-192 και το AES-256 είναι οι πιο συχνά χρησιμοποιούμενοι συμμετρικοί αλγόριθμοι.

2. Ασύμμετρη κρυπτογράφηση

Η ασύμμετρη κρυπτογραφία κλειδιού αναφέρεται σε μεθόδους κρυπτογράφησης, στην οποία ο αποστολέας και ο παραλήπτης μοιράζονται το ίδιο κλειδί. Ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Δίνει μεγαλύτερη σταθερότητα από το συμμετρικά συστήματα. Η ασύμμετρη κρυπτογράφηση είναι σχετικά νέο και πολύπλοκο στυλ κρυπτογράφησης. Πολύπλοκο, γιατί χρησιμοποιεί δύο κρυπτογραφικά κλειδιά για την υλοποίηση της ασφάλειας δεδομένων. Αυτά τα κλειδιά αναφέρονται ως δημόσιο κλειδί και ιδιωτικό κλειδί. Όπως το όνομα προτείνει, το Δημόσιο Κλειδί είναι ανοιχτό σε όποιον επιθυμεί να στείλει ένα μήνυμα. Από την άλλη, ο ιδιοκτήτης του δημοσίου κλειδιού διατηρεί το ιδιωτικό κλειδί σε ασφαλές μέρος. Η ασύμμετρη κρυπτογράφηση φαίνεται στο Σχήμα 2.1.3.

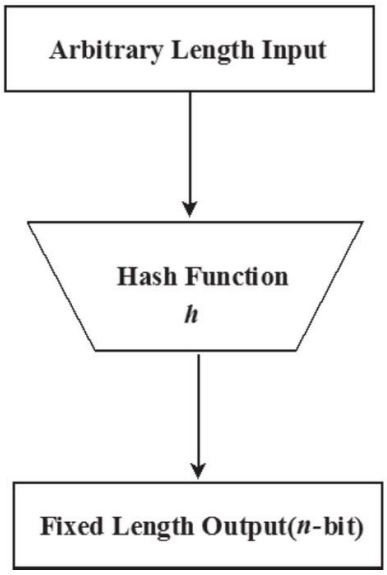


Σχήμα 2.1.3: Ασύμμετρη κρυπτογράφηση[14]

Η ασύμμετρη κρυπτογράφηση είναι επίσης γνωστή ως κρυπτογραφία δημοσίου κλειδιού, σε αντίθεση με τη συμμετρική κρυπτογράφηση, που είναι μια σχετικά νέα τεχνική. Για την ασύμμετρη κρυπτογράφηση, δύο κλειδιά χρησιμοποιούνται για την κρυπτογράφηση ενός απλού κειμένου. Τα κρυφά κλειδιά μοιράζονται σε ένα μεγάλο δίκτυο ή στο διαδίκτυο. Αυτό σημαίνει ότι δεν γίνεται ανεπιθύμητη χρήση των κλειδιών από κακόβουλους ανθρώπους. Είναι σημαντικό να σημειωθεί ότι οποιοσδήποτε με ένα μυστικό κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και αυτό είναι γιατί η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο συ σχετιζόμενα κλειδιά για την βελτίωση της ασφάλειας. Όποιος θέλει να σας στείλει ένα μήνυμα θα του δοθεί ένα δημόσιο κλειδί δωρεάν. Το δεύτερο ιδιωτικό κλειδί διατηρείται μυστικό για να το γνωρίζετε μόνο εσείς. Ένα μήνυμα κρυπτογραφημένο με χρήση δημόσιου κλειδιού μπορεί να αποκρυπτογραφηθεί μόνο με χρήση ιδιωτικού κλειδιού, ενώ με τη χρήση του δημοσίου κλειδιού μπορείτε επίσης να αποκρυπτογραφήσετε ένα μήνυμα που κρυπτογραφήθηκε με ιδιωτικό κλειδί. Η προστασία του δημόσιου κλειδιού δεν χρειάζεται αφού είναι διαθέσιμο στο κοινό και μπορεί να μεταδίδεται μέσω Διαδικτύου. Το ασύμμετρο κλειδί έχει πολύ μεγαλύτερη δύναμη για να διασφαλίσει ότι οι πληροφορίες που ανταλλάσσονται κατά την επικοινωνία είναι ασφαλείς.

3. Συναρτήσεις Κατακερματισμού

Στον συγκεκριμένο τύπο κρυπτογράφησης δεν έχουμε χρήση κλειδιού. Γίνεται η χρήση μιας τιμής κατακερματισμού, που έχει σταθερό μήκος και υπολογίζεται σύμφωνα με το αρχικό κείμενο, το οποίο καθιστά αδύνατη την δυνατότητα επαναφοράς του περιεχόμενου του απλού κειμένου. Πολλά λειτουργικά συστήματα χρησιμοποιούν αυτού του είδους κρυπτογράφησης έτσι ώστε να επιτύχουν την αποθήκευση διάφορων δεδομένων, όπως για παράδειγμα τους κωδικούς πρόσβασης.



Σχήμα 2.1.4: Κρυπτογραφία με συναρτήσεις κατακερματισμού

2.2 Κρυπτογραφία Βάσει Χαρακτηριστικών

2.2.α Εισαγωγή στην Κρυπτογραφία Βάσει Χαρακτηριστικών

Η Κρυπτογραφία Βάσει Χαρακτηριστικών (Attribute-based Encryption - ABE) ανήκει στην «οικογένεια>> των ασύμμετρων τεχνικών κρυπτογράφησης.

Σε ένα σχήμα ABE υπάρχουν τουλάχιστον τρεις διαφορετικοί τύποι κλειδιών. Σε ένα πρώτο βήμα, μια αυθεντία δημιουργεί ένα μυστικό κύριο κλειδί και ένα συσχετισμένο δημόσιο κλειδί. Η αυθεντία πρέπει να είναι μια αξιόπιστη οντότητα, καθώς έχει πρόσβαση στα μυστικά κύρια κλειδιά. Αυτά τα μυστικά κύρια κλειδιά μπορούν να χρησιμοποιηθούν για τη δημιουργία ιδιωτικών κλειδιών. Απαιτείται ιδιωτικό κλειδί για την αποκρυπτογράφηση των δεδομένων. Τα δημόσια κλειδιά κρυπτογραφούν δεδομένα και μπορούν να μοιραστούν με άλλους.

Με το ABE, είναι δυνατή η κρυπτογράφηση δεδομένων με μια λεπτομερή πολιτική ελέγχου πρόσβασης. Αυτό επιτυγχάνεται με τη χρήση συνόλων χαρακτηριστικών. Τα ιδιωτικά κλειδιά, τα οποία μπορούν να δημιουργηθούν μόνο χρησιμοποιώντας ένα μυστικό κύριο κλειδί, περιέχουν τέτοια σύνολα χαρακτηριστικών. Κατά την κρυπτογράφηση του αρχείου, ο χρήστης πρέπει να καθορίσει μια πολιτική, έναν τύπο Boolean που να περιγράφει ποια χαρακτηριστικά απαιτούνται για την αποκρυπτογράφηση,

π.χ., ((φοιτητής και εγγραφή < 2012) ή καθηγητής).

Αυτή η πολιτική περιγράφει ότι ένα αρχείο είναι προσβάσιμο μόνο από καθηγητές ή φοιτητές που έχουν εγγραφεί πριν από το 2012. Κατά την προσπάθεια αποκρυπτογράφησης του αρχείου, απαιτείται ιδιωτικό κλειδί. Εάν το σύνολο χαρακτηριστικών του ιδιωτικού κλειδιού ικανοποιεί αυτόν τον Boolean τύπο, τότε παρέχεται πρόσβαση στο απλό κείμενο.

Ένα πλεονέκτημα του ABE είναι ότι η δημιουργία ιδιωτικών κλειδιών και η αποκρυπτογράφηση είναι αποσυνδεδεμένες. Τα ιδιωτικά κλειδιά που δημιουργούνται με ορισμένα χαρακτηριστικά θα μπορούν πάντα να αποκρυπτογραφούν δεδομένα, για τα οποία πληρούν τους τύπους Boolean, χωρίς να επικοινωνούν ξανά με την αρχή κλειδιού. Αυτό δεν είναι πάντα μια επιθυμητή ιδιότητα, καθώς η ανάκληση κλειδιών δεν θα ήταν δυνατή χωρίς την εκ νέου κρυπτογράφηση των δεδομένων ή την αναδιανομή κάθε ιδιωτικού κλειδιού. Οι νεότερες προσεγγίσεις ABE μπορούν να εξηγήσουν αυτό το πρόβλημα με την ανάκληση μέσω διακομιστή μεσολάβησης ή μέσω εκχώρησης πολιτικής , η οποία επιτρέπει την ενημέρωση της πολιτικής ενός αρχείου σε μια πιο περιοριστική πολιτική που απαιτεί μόνο το δημόσιο κλειδί. Ωστόσο, λόγω της αποσυνδεδεμένης φύσης του ABE, τα χαρακτηριστικά είναι στατικά. Μπορούν να αλλάξουν μόνο με τη διανομή ενός νέου ιδιωτικού κλειδιού.

Ένα σημαντικό χαρακτηριστικό του ABE είναι η πρόληψη των επιθέσεων συμπαιγνίας. Για παράδειγμα, ένα αρχείο κρυπτογραφείται με την πολιτική (Χ και Υ) και αποστέλλεται σε δύο χρήστες. Ο πρώτος χρήστης έχει ιδιωτικό κλειδί με το χαρακτηριστικό Χ ενώ ο δεύτερος χρήστης έχει ιδιωτικό κλειδί με το χαρακτηριστικό Υ . Καθένα από αυτά δεν είναι σε θέση να αποκρυπτογραφήσει το αρχείο, καθώς και τα δύο χαρακτηριστικά που λαμβάνονται χωριστά δεν ικανοποιούν τον τύπο. Είναι λοιπόν επιθυμητή ιδιότητα του ABE ότι και οι δύο χρήστες δεν μπορούν να συνδυάσουν τα κλειδιά τους για να σχηματίσουν ένα ενιαίο κλειδί, το οποίο θα μπορεί να αποκρυπτογραφήσει το αρχείο. Στην πραγματικότητα, το ABE πληροί αυτή την ιδιότητα, που ονομάζεται αντίσταση συμπαιγνίας.

Υπάρχουν δύο κύριες παραλλαγές του ABE. Στο Ciphertext-Policy ABE (CP-ABE), ο τύπος Boole αποθηκεύεται στο κρυπτογραφημένο κείμενο, δηλαδή στο κρυπτογραφημένο αρχείο. Τα χαρακτηριστικά που απαιτούνται για την ικανοποίηση των πολιτικών αποθηκεύονται σε ένα ιδιωτικό κλειδί. Στο Key-Policy ABE (KP-ABE), αυτοί οι δύο ρόλοι αντιστρέφονται άμεσα: το ιδιωτικό κλειδί διατηρεί τον τύπο και το κρυπτογραφημένο κείμενο διαθέτει χαρακτηριστικά. Η τελευταία παραλλαγή θα μπορούσε να εφαρμοστεί σε περίπτωση χρήσης διαχείρισης ψηφιακών δικαιωμάτων (DRM), για παράδειγμα. Υπάρχουν τέσσερις βασικές λειτουργίες στο CP-ABE:

- **Ρύθμιση** - Δημιουργεί ένα δημόσιο κλειδί και ένα συσχετισμένο μυστικό κύριο κλειδί.

- **Κρυπτογράφηση** - Κρυπτογραφεί ένα αρχείο με δημόσιο κλειδί και βάση μιας πολιτικής.

- **Δημιουργία Κλειδιών** - Δημιουργεί ένα ιδιωτικό κλειδί με χαρακτηριστικά. Για να γίνει αυτό, χρειάζεται ένα μυστικό κύριο κλειδί. Αυτό το ιδιωτικό κλειδί συσχετίζεται με το μυστικό κύριο κλειδί και το δημόσιο κλειδί του.

- **Αποκρυπτογράφηση** - Χρειάζεται κρυπτογραφημένο κείμενο και ιδιωτικό κλειδί. Αποκρυπτογραφεί το κρυπτογραφημένο κείμενο μόνο εάν τα χαρακτηριστικά στο ιδιωτικό κλειδί πληρούν την πολιτική και το ιδιωτικό κλειδί σχετίζεται με το δημόσιο κλειδί που χρησιμοποιήθηκε αρχικά για κρυπτογράφηση.

Υπάρχουν δύο τύποι ατομικών τύπων: κανονικές και αριθμητικές ιδιότητες. Ένα κανονικό χαρακτηριστικό είναι απλώς μια συμβολοσειρά γραμμάτων και ψηφίων που ξεκινά με ένα γράμμα, π.χ. φοιτητής, καθηγητής, ομάδα εργασίας303, άνδρας ή γυναίκα. Τα αριθμητικά χαρακτηριστικά έχουν ένα όνομα και μια σχετική τιμή. Ως χαρακτηριστικό σε ένα ιδιωτικό κλειδί θα μοιάζει με αυτό:

hiringdate = 2014, yearofbirth = 1990.

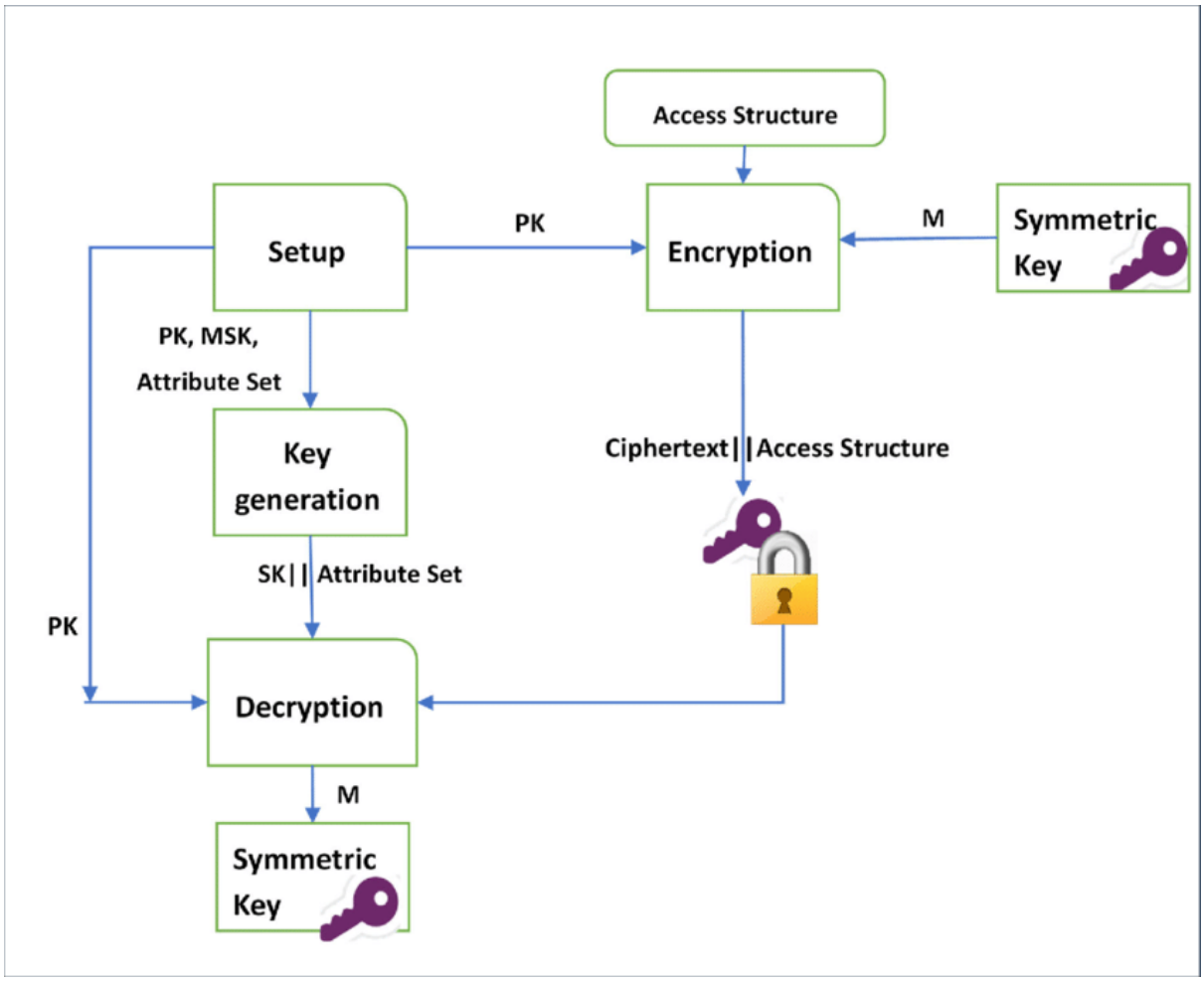
Στην υλοποίηση cpabe του Bethencourt υποστηρίζονται ακέραιοι αριθμοί στην περιοχή από 0 έως 264 − 1. Στις πολιτικές πρόσβασης, αυτά τα αριθμητικά χαρακτηριστικά μπορούν να συγκριθούν με αριθμούς με τους ακόλουθους τελεστές: =, <, >, ≥, ≤,

π.χ., ημερομηνία πρόσληψης ≤ 2014, έτος γέννησης = 2000, επίπεδο πρόσβασης ≥ 8.

Δεν είναι δυνατή η σύγκριση δύο διαφορετικών αριθμητικών χαρακτηριστικών ενός χρήστη, επομένως δεν είναι δυνατό τα εξής: καταμέτρηση μαθητών > μέτρηση εξετάσεων. Το δεύτερο όρισμα μιας αριθμητικής σύγκρισης πρέπει πάντα να είναι ένας αριθμός που είναι γνωστός τη στιγμή της κρυπτογράφησης. Για την ίδια την πολιτική πρόσβασης, υπάρχουν τρεις πιθανοί τελεστές: ή, και, και of. Αυτοί οι τελεστές μπορούν να συνδυαστούν για να σχηματίσουν σύνθετους τύπους. Ένα αρχείο μπορεί να είναι κρυπτογραφημένο με την ακόλουθη πολιτική πρόσβασης:

((φοιτητής και εγγραφή < 2014 και εξάμηνο σπουδών > 3) ή (φοιτητής και εξάμηνο σπουδών > 5) ή καθηγητής).

Όπως και σε άλλους αλγόριθμους ασύμμετρης κρυπτογράφησης, το ABE προορίζεται να αναπτυχθεί σε ένα σχήμα ενθυλάκωσης κλειδιού, δηλαδή σε σχήμα υβριδικής κρυπτογράφησης. Αυτός είναι ένας τυπικός τρόπος κατασκευής συστημάτων χρησιμοποιώντας ασύμμετρη κρυπτογράφηση, καθώς το ασύμμετρο μέρος είναι υπολογιστικά ακριβό. Αυτό είναι ιδιαίτερα απαραίτητο για το ABE, λόγω της πολυπλοκότητας και του χρόνου που απαιτείται για τη δημιουργία κλειδιών και την κρυπτογράφηση ή αποκρυπτογράφηση κρυπτογραφημένων κειμένων.



Σχήμα 2.2.1. Κύρια στοιχεία στην Κρυπτογράφηση βάσει χαρακτηριστικών (CP-ABE)

2.2.β Εφαρμογές της ABE

Οι Sahai και Waters πρότειναν μια νέα κατηγορία σχήματος κρυπτογράφησης, που ονομάζεται κρυπτογράφηση βάσει χαρακτηριστικών (ABE), όπου ο πάροχος των δεδομένων μπορεί να αποφασίσει την πολιτική πρόσβασης του κρυπτογραφημένου κειμένου, πράγμα που σημαίνει ότι μόνο οι χρήστες που ικανοποιούν τα καθορισμένα χαρακτηριστικά μπορούν να αποκρυπτογραφήσουν το κρυπτογραφημένο κείμενο. Οι πάροχοι πόρων χρειάζεται μόνο να κρυπτογραφούν τα μηνύματα σύμφωνα με τα χαρακτηριστικά των αποκρυπτογραφητών, χωρίς να ανησυχούν για την ταυτότητά τους και τον αριθμό των πιστοποιημένων αποκρυπτογραφητών. Αυτή η δυνατότητα μειώνει σημαντικά την επιβάρυνση της κρυπτογράφησης δεδομένων και επιτρέπει στους παρόχους πόρων να διαμορφώνουν ευέλικτες και επεκτάσιμες πολιτικές ελέγχου πρόσβασης για τη διαχείριση του εύρους κοινής χρήσης δεδομένων. Το πρώτο σχήμα ABE υποστηρίζει μόνο στρατηγικές ελέγχου πρόσβασης τύπου threshold. Η κοινότητα πρότεινε περαιτέρω το Key-Policy ABE και το CP-ABE για την υποστήριξη πιο ευέλικτων στρατηγικών ελέγχου πρόσβασης.

Τα τελευταία χρόνια, έχει προταθεί ένας αριθμός νέων σχημάτων ABE με ξεχωριστά χαρακτηριστικά ασφαλείας. Έχουν προταθεί εξειδικευμένα σχήματα ABE για διάφορα σενάρια εφαρμογών όπως το cloud computing, τα κοινωνικά δίκτυα, το Internet of things (IoT), τα blockchains και τα κινητά.

ΚΕΦΑΛΑΙΟ 3 Διαχείριση Ψηφιακών Δικαιωμάτων

3.1 Ψηφιακά Δικαιώματα

3.1.α Εισαγωγή στα ψηφιακά δικαιώματα

Τα τελευταία χρόνια, έχει παρατηρηθεί ένα αυξανόμενο ενδιαφέρον για νομικά ζητήματα, που αφορούν τη χρήση και την επαναχρησιμοποίηση διαδικτυακού δημοσιευμένου υλικού. Συγκεκριμένα, αρκετά ανοιχτά ζητήματα επηρεάζουν τους όρους και τις προϋποθέσεις υπό τους οποίους τα δεδομένα που δημοσιεύονται στο Διαδίκτυο γνωστοποιούνται στους χρήστες και τα δικαιώματα των χρηστών επί αυτών των δεδομένων. Αν και ο αριθμός του αδειοδοτημένου υλικού στον Ιστό αυξάνεται σημαντικά, το πρόβλημα της δημιουργίας πληροφοριών αδειών αναγνώσιμων από μηχανήματα παραμένει άλυτο.

Οι διαχειριστές ψηφιακών περιουσιακών στοιχείων πρέπει να παρακολουθούν και να ενεργούν σχετικά με τα δικαιώματα που συνδέονται με τα ψηφιακά στοιχεία. Οι γλώσσες έκφρασης δικαιωμάτων (RELs) μπορούν να βοηθήσουν στη διαχείριση δικαιωμάτων καταγράφοντας όρους σε μια μηχανικά αναγνώσιμη μορφή που μπορεί να ανταλλάσσεται μεταξύ συστημάτων πληροφοριών. Αν και τα RELs ποικίλλουν ευρέως ως προς τη σύνταξη και την πολυπλοκότητά τους, μοιράζονται κοινές έννοιες που παρέχουν ένα πλαίσιο για την κατανόηση και την αξιολόγηση κάθε γλώσσας.

Οι πληροφορίες για τα δικαιώματα πρέπει να είναι εύκολα διαθέσιμες για ανάλυση. Εάν οι πληροφορίες δικαιωμάτων αποθηκεύονται σε έντυπα συμβόλαια ή μέσα σε έγγραφα επεξεργασίας κειμένου, τότε δεν μπορούν να οδηγήσουν τις συμπεριφορές του συστήματος ή να αναλυθούν εύκολα για τη λήψη αποφάσεων. Για την επίλυση αυτού του προβλήματος υπάρχουν οι γλώσσες έκφρασης δικαιωμάτων (RELs). Τα RELs καταγράφουν πληροφορίες για τα δικαιώματα σε αναλυτική, αναγνώσιμη από μηχανή μορφή, καθιστώντας έτσι δυνατή τη δημιουργία αυτοματοποιημένων διαδικασιών που ενεργούν σε δεδομένα δικαιωμάτων και υποστηρίζουν τη λήψη επιχειρηματικών αποφάσεων.
Υπάρχει ένας μεγάλος αριθμός από RELs, όλα δημιουργημένα με διαφορετικές συντακτικές με στόχο την επίλυση διαφορετικών προβλημάτων.

3.1.β Βασικά Χαρακτηριστικά

Σε αυτή την ενότητα θα δούμε τα βασικότερα χαρακτηριστικά των ψηφιακών αδειών:

Άδειες

Οι άδειες είναι προνόμια που παραχωρούνται στους χρήστες από τους νόμιμους κατόχους δικαιωμάτων ενός ψηφιακού στοιχείου. Όπως εξήγησε ένας ερευνητής:

<<το δικαίωμα και η άδεια έχουν μερικές φορές διακριθεί ως η δύναμη ή το προνόμιο που παραχωρούνται από το νόμο στον δημιουργό ή κάτοχο δικαιωμάτων (δικαίωμα) έναντι της μεταβίβασης ή απονομή του δικαιώματος, συχνά μετά από ένα ή περισσότερα πληρωθέν κριτήρια, στον τελικό χρήστη (άδεια)>>.

Ενώ τα νόμιμα δικαιώματα κωδικοποιούνται από το νόμο, οι άδειες βασίζονται συχνά σε διαπραγματεύσεις μεταξύ των κατόχων δικαιωμάτων και των τελικών χρηστών. Για παράδειγμα, μια άδεια από έναν φωτογράφο μπορεί να παρέχει άδεια χρήσης μιας Εικόνας σε φυλλάδια που μπορούν να ληφθούν από τον παγκόσμιο ιστό, αλλά να μην επιτρέπεται η χρήση της Εικόνας εάν το φυλλάδιο είναι τυπωμένο.

Υποχρεώσεις

Μια υποχρέωση είναι μια προϋπόθεση που πρέπει να πληρούνται πριν επιτραπεί στον τελικό χρήστη να εκτελέσει μια συγκεκριμένη ενέργεια σε ένα περιουσιακό στοιχείο. Η πιο κοινή υποχρέωση σε μια εμπορική άδεια είναι η απαίτηση καταβολής τέλους. Στα έργα ανοιχτής πρόσβασης, οι υποχρεώσεις συχνά λαμβάνουν τη μορφή απαίτησης «όμοιου μεριδίου», όπου οι τελικοί χρήστες μπορούν να χρησιμοποιήσουν ένα περιουσιακό στοιχείο, αλλά οποιαδήποτε παράγωγα έργα που δημιουργούνται πρέπει να είναι διαθέσιμα υπό τους ίδιους όρους αδειοδότησης με το πρωτότυπο.

Ενέργειες

Μόλις οι τελικοί χρήστες έχουν εκπληρώσει οποιεσδήποτε υποχρεώσεις, έχουν το δικαίωμα να εκτελέσουν συγκεκριμένες ενέργειες σε ένα περιουσιακό στοιχείο. Στην πραγματικότητα, μια ενέργεια αντιπροσωπεύει την ικανότητα του τελικού χρήστη να ελέγχει ένα περιουσιακό στοιχείο για να αντλήσει όφελος από αυτό. Οι συνήθεις ενέργειες περιλαμβάνουν το δικαίωμα εκτύπωσης, αντιγραφής και δημιουργίας ενός παράγωγου έργου από ένα περιουσιακό στοιχείο. Οι τύποι των πιθανών ενεργειών εξαρτώνται από το εν λόγω ψηφιακό στοιχείο. Για παράδειγμα, ενώ η «εκτύπωση» είναι μια έγκυρη ενέργεια για μια Εικόνα, δεν ισχύει για μια εγγραφή ήχου. Ομοίως, ένα αρχείο ήχου μπορεί να «μεταγραφεί», αλλά αυτή η ενέργεια δεν θα μπορούσε να εφαρμοστεί άμεσα σε μια Εικόνα.

Περιορισμοί

Κατά την αδειοδότηση περιουσιακών στοιχείων, είναι σπάνιο να επιτρέπεται μια ενέργεια στο διηνεκές σε όλες τις περιπτώσεις. Αντίθετα, οι ενέργειες συνήθως περιορίζονται από συνθήκες. Ένας περιορισμός έχει δύο στοιχεία: (1) έναν τύπο και (2) μια τιμή. Ο τύπος καθορίζει τι περιορίζεται, ενώ η τιμή καθορίζει τις συνθήκες ή τις παραμέτρους του περιορισμού. Για παράδειγμα, μια άδεια βίντεο μπορεί να επιτρέπει στους χρήστες να προβάλλουν ένα βίντεο όταν αυτό προβάλλεται από έναν συγκεκριμένο τομέα ιστού. Σε αυτό το σενάριο, ο τύπος περιορισμού θα είναι «επιτρεπόμενος τομέας» και η επιτρεπόμενη τιμή θα είναι η συγκεκριμένη διεύθυνση ιστού. Οι τυπικοί περιορισμοί περιλαμβάνουν τις ημερομηνίες έναρξης και λήξης για μια άδεια, έναν περιορισμό καναλιού διανομής ή έναν γεωγραφικό περιορισμό. Αναμφισβήτητα, οι περιορισμοί είναι το πιο σημαντικό χαρακτηριστικό οποιασδήποτε άδειας, καθώς καθορίζουν τα όρια που καθορίζουν τον τρόπο χρήσης ενός περιουσιακού στοιχείου και είναι ζωτικής σημασίας για τον προσδιορισμό του εάν ένας τελικός χρήστης συμμορφώνεται με τους όρους μιας άδειας. Δεδομένης της σημασίας των περιορισμών, πολλά RELs παρέχουν πολύ αναλυτικούς όρους για να εκφράσουν περιορισμούς, ενώ οι ενέργειες μπορούν να υπονοούνται ή να αντιπροσωπεύονται μόνο με γενικούς όρους, όπως «χρήση», «αναπαραγωγή» ή «κατασκευή παραγώγου»

Λειτουργία REL

Προκειμένου να αποκτήσουν τα δικαιώματα που ισχύουν για τα ψηφιακά στοιχεία, τα RELs πρέπει να καταγράφουν τις λεπτομέρειες των νομικά καθορισμένων δικαιωμάτων, καθώς και τους όρους των αδειών που έχουν μεταβιβαστεί στους τελικούς χρήστες. Οι άδειες αποτελούνται από τουλάχιστον τρία συστατικά:
υποχρεώσεις, ενέργειες και περιορισμούς. Ο τομέας δικαιωμάτων περιλαμβάνει επίσης το ίδιο το περιουσιακό στοιχείο, καθώς και τα μέρη που εμπλέκονται ως δημιουργοί, κάτοχοι δικαιωμάτων και τελικοί χρήστες.

Οι πληροφορίες που συλλαμβάνει κάθε REL εξαρτάται από το σκοπό της μεμονωμένης γλώσσας. Ορισμένα RELs κατά κύριο λόγο μοντελοποιούν και εκφράζουν νόμιμα δικαιώματα, όπως τα πνευματικά δικαιώματα, ενώ άλλα επικεντρώνονται σε δικαιώματα που έχουν μεταβιβαστεί ως μέρος μιας εμπορικής συναλλαγής. Αυτή η επόμενη ενότητα της εργασίας συζητά τέσσερα γνωστά RELs για να διευκρινιστεί ο σκοπός τους και να εξεταστεί πότε μπορούν να χρησιμοποιηθούν καταλληλότερα.

3.1.γ Παραδείγματα RELs

ccREL

Η Creative Commons είναι ένας μη κερδοσκοπικός οργανισμός που επιδιώκει να προωθήσει τη χρήση έργων ανοιχτού κώδικα. Ο οργανισμός δημιούργησε το ccREL για να διευκολύνει τον προσδιορισμό του τρόπου με τον οποίο μπορούν να επαναχρησιμοποιηθούν τα στοιχεία ανοιχτού κώδικα. Οι δημιουργοί του ccREL ανέπτυξαν ειδικά τη γλώσσα για να απαντήσουν στις ακόλουθες ερωτήσεις, οι οποίες έχουν ληφθεί αυτολεξεί από την τεκμηρίωση του ccREL:

• Κάτω από ποια άδεια ο κάτοχος των πνευματικών δικαιωμάτων κυκλοφόρησε το έργο του, και

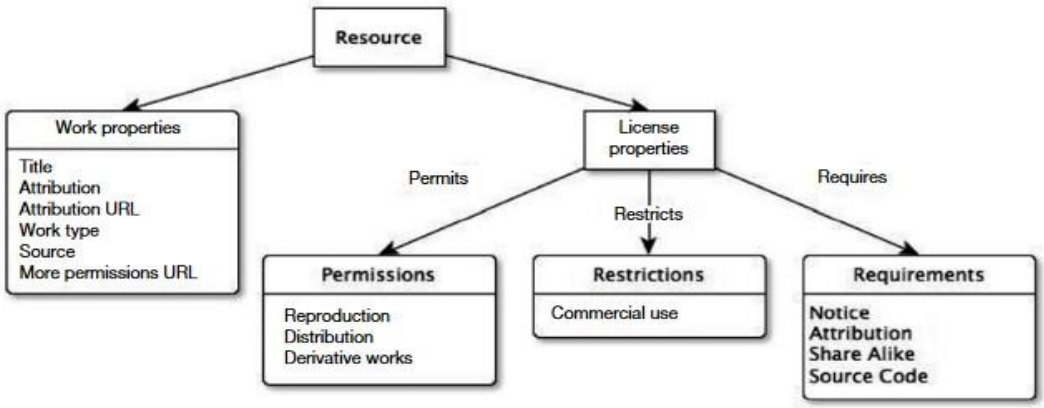
• ποιες είναι οι σχετικές άδειες και περιορισμοί;

• Μπορώ να αναδιανείμω αυτό το έργο για εμπορικούς σκοπούς;

• Μπορώ να διανείμω μια τροποποιημένη έκδοση αυτού του έργου;

• Πώς πρέπει να αποδώσω τα εύσημα στον αρχικό συγγραφέα;

Οι άδειες ccREL εκφράζονται χρησιμοποιώντας το μοντέλο πληροφοριών πλαισίου περιγραφής πόρων (RDF) και μπορούν να γραφτούν είτε ως επεκτάσιμη γλώσσα σήμανσης (XML) είτε σε μια μορφή που ονομάζεται πλαίσιο περιγραφής πόρων σε χαρακτηριστικά (RDFa), η οποία μπορεί να εισαχθεί σε ιστοσελίδες.



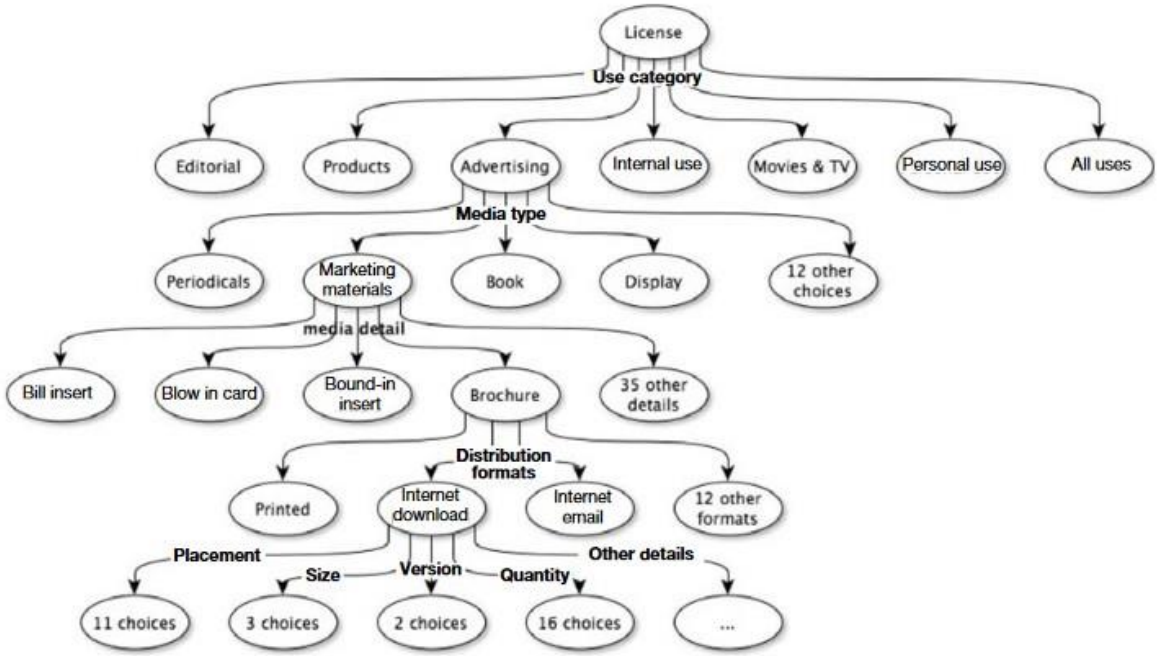
Σχήμα 3.1.1: Απλοποιημένη προβολή του μοντέλου δεδομένων ccREL[7]

PLUS

Η PLUS είναι μια γλώσσα δικαιωμάτων που αναπτύχθηκε από το PLUS Coalition προκειμένου να απλοποιήσει την αδειοδότηση εικόνων. Εκτός από το REL, το PLUS Coalition διατηρεί ένα λεξικό δεδομένων με τυπικούς

όρους καθώς και μια ταξινόμηση, που ονομάζεται PLUS Matrix, η οποία καθορίζει πώς μπορούν να χρησιμοποιηθούν οι εικόνες.

Οι άδειες χρήσης PLUS εκφράζονται σε RDF και σειριοποιούνται ως XML. Στο PLUS, όλες οι επιτρεπόμενες ενέργειες και περιορισμοί στην άδεια χρήσης αντιπροσωπεύονται από τυπικούς κωδικούς που ορίζονται στο λεξικό δεδομένων.

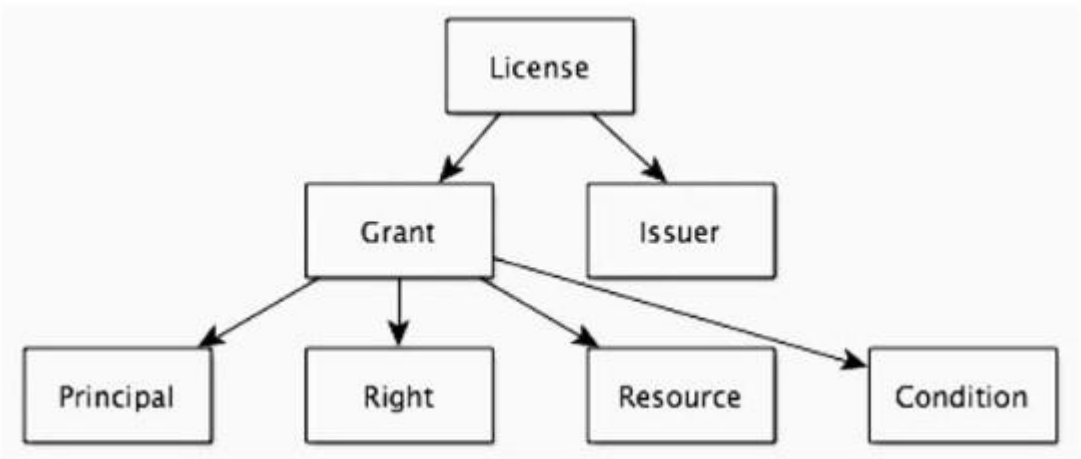


Σχήμα 3.1.2: Μερική απεικόνιση του πίνακα PLUS Matrix, που δείχνει διαθέσιμες επιλογές για την αδειοδότηση μιας Εικόνας για χρήση σε διαφημιστικό φυλλάδιο.[7]

MPEG-21/5

Το Motion Picture Experts Group έχει εκδώσει μια σειρά προτύπων για τη δημιουργία διανομής και κατανάλωσης ψηφιακών στοιχείων. Το μέρος 5 της σουίτας περιλαμβάνει ένα REL που συνήθως προσδιορίζεται ως «MPEG-21/5». Το πρότυπο περιλαμβάνει επίσης ένα λεξικό δεδομένων, το οποίο περιέχει περίπου 2.000 τυπικούς όρους που μπορούν να χρησιμοποιηθούν στο REL. Το MPEG-21/5 εκφράζεται σε μορφή XML και το Σχήμα 3.1.3 απεικονίζει το μοντέλο δεδομένων του. Κάθε άδεια δημιουργείται από έναν εκδότη και περιέχει μία ή περισσότερες επιχορηγήσεις που στοχεύουν πόρους. Κάθε παραχώρηση δίνει σε έναν τελικό χρήστη το δικαίωμα πρόσβασης στον συγκεκριμένο πόρο, αν και αυτό το δικαίωμα μπορεί να περιοριστεί από όρους. Στο μοντέλο MPEG-21/5, μια προϋπόθεση μπορεί να είναι είτε μια απαίτηση που πρέπει να πληροί ο χρήστης, όπως η πραγματοποίηση μιας πληρωμής, είτε μπορεί να είναι ένας περιορισμός, όπως η ημερομηνία λήξης. Το MPEG-21/5 προορίζεται για χρήση σε ροές εργασιών εμπορικής αδειοδότησης, όπου ένας χρήστης έχει αγοράσει ένα στοιχείο και ένα σύστημα ελέγχου πρέπει να αποφασίσει εάν επιτρέπεται στον χρήστη να έχει πρόσβαση σε αυτό. Με άλλα λόγια, η γλώσσα εστιάζει στην επιβολή κανόνων πρόσβασης και, ως εκ τούτου, το πρότυπο καθορίζει ένα σύνθετο σύνολο αλγορίθμων και απαιτήσεων για την

αναγνώριση των μερών, τη δημιουργία εμπιστοσύνης και τον υπολογισμό των αδειών.

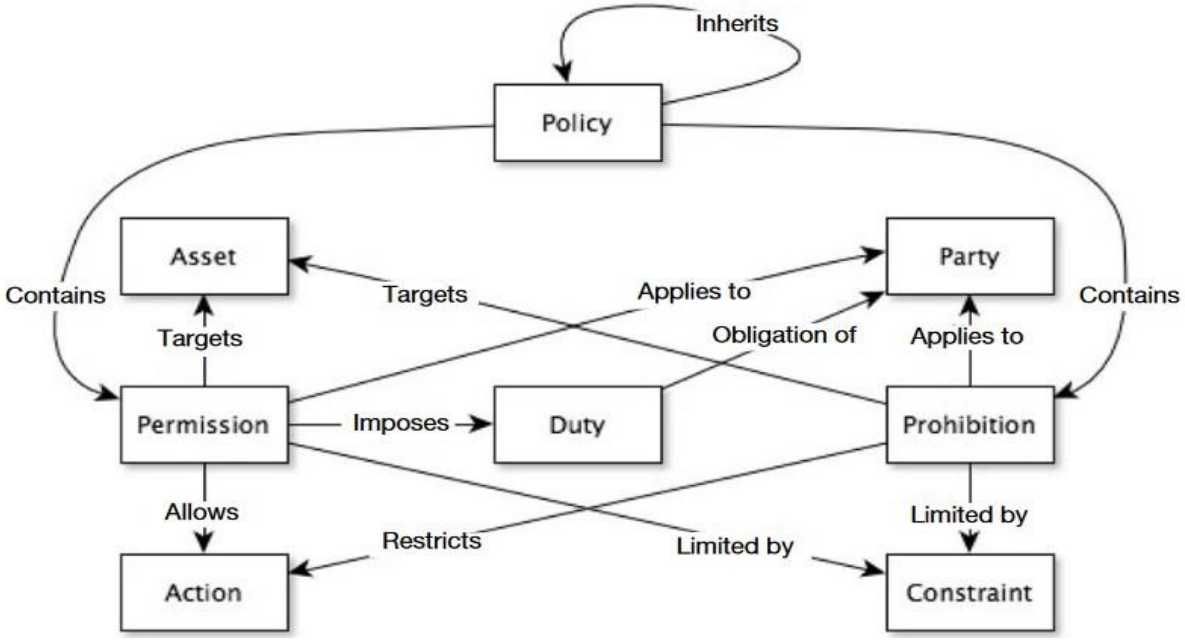


Σχήμα 3.1.3: Μοντέλο δεδομένων MPEG-21/5[7]

ODRL

Η ODRL αποσκοπεί στη διευκόλυνση της αδειοδότησης, διανομής και κατανάλωσης ψηφιακών μέσων. Σε αντίθεση με το PLUS, το ODRL δεν περιορίζεται σε εικόνες και δεν επιβάλλει ταξινόμηση σχετικά με τον συνδυασμό όρων που μπορεί να περιέχει μια άδεια. Το ODRL συχνά παρομοιάζεται με το MPEG-21/5 επειδή και τα δύο είναι RELs γενικής χρήσης κατάλληλα για την καταγραφή των όρων των εμπορικών αδειών. Η ODRL διατηρείται επί του παρόντος από το ODRL Community Group του World Wide Web Consortium, έναν οργανισμό προτύπων Ιστού. Η προδιαγραφή ODRL περιλαμβάνει ένα REL καθώς και ένα μικρό λεξικό δεδομένων που παραθέτει τυπικούς όρους για επιτρεπόμενες ενέργειες, υποχρεώσεις και περιορισμούς. Το βασικό μοντέλο για το ODRL βασίζεται σε όλες τις έννοιες που περιεγράφηκαν προηγουμένως σε αυτή την

ενότητα και απεικονίζεται στην Σχήμα 3.1.4.



Σχήμα 3.1.4: Μοντέλο δεδομένων ODRL[7]

Το μοντέλο ODRL ορίζεται με τρεις διαφορετικούς τρόπους: σε ένα σχήμα τεκμηρίωσης γλώσσας επεκτάσιμης σήμανσης (XSO), σε σχήμα σημειογραφίας αντικειμένου Javascript (JSON) και σε σημασιολογική οντολογία ιστού. Ανάλογα με το σχήμα που χρησιμοποιείται, είναι δυνατή η καταγραφή των όρων μιας άδειας ODRL σε XML, JSON ή σε οποιαδήποτε σύνταξη RDF, συμπεριλαμβανομένων των Turtle, N-Tuples και RDF XML.

```
{
   "policytype" : "http://www.w3.org/ns/odrl/2/Ticket",
   "policyid" : "http://example.com/policy:04311",
   "permissions" : [{
      "target" : "http://example.com/game:4589",
      "action" : "http://www.w3.org/ns/odrl/2/play",
      "constraints" : [{
         "name" : "http://www.w3.org/ns/odrl/2/dateTime",
         "operator" : "http://www.w3.org/ns/odrl/lteq",
         "rightoperand" : "2010-12-31"
      }]
   }]
}
```

Σχήμα 3.1.5: Άδεια ODRL εκφρασμένη σε μορφή JSON[7]

Μια άδεια ODRL, που ονομάζεται επίσης πολιτική, μπορεί να περιέχει τόσο άδειες όσο και απαγορεύσεις. Αυτές οι οντότητες είτε επιτρέπουν είτε απαγορεύουν στα μέρη να εκτελούν συγκεκριμένες ενέργειες σε στοχευμένα περιουσιακά στοιχεία. Οι ενέργειες μπορούν να περιορίζονται από περιορισμούς και οι άδειες μπορούν να επιβάλλουν καθήκοντα σε συγκεκριμένα μέρη προτού εκτελεστούν οι αντίστοιχες ενέργειές τους.

Από αυτά τα 4 παραδείγματα RELs που αναλύσαμε, εμείς στην παρούσα εργασία θα χρησιμοποιήσουμε την ODRL. Στο επόμενο υποκεφάλαιο θα αναλύσουμε εκτενέστερα την λειτουργεία της ODRL.

3.2 Open Digital Rights Language (ODRL)

3.2.α Περιγραφή της γλώσσας

Η ανοιχτή γλώσσα ψηφιακών δικαιωμάτων (ODRL) είναι μια γλώσσα έκφρασης πολιτικής που παρέχει ένα ευέλικτο και διαλειτουργικό μοντέλο πληροφοριών, λεξιλόγιο και μηχανισμούς κωδικοποίησης για την αναπαράσταση δηλώσεων σχετικά με τη χρήση περιεχομένου και υπηρεσιών. Το μοντέλο πληροφοριών ODRL περιγράφει τις υποκείμενες έννοιες, οντότητες και σχέσεις που αποτελούν τη θεμελιώδη βάση για τη σημασιολογία των πολιτικών ODRL.

Οι πολιτικές χρησιμοποιούνται για την αντιπροσώπευση επιτρεπόμενων και απαγορευμένων ενεργειών σχετικά με ένα συγκεκριμένο περιουσιακό στοιχείο, καθώς και τις υποχρεώσεις που απαιτούνται να εκπληρώσουν τα ενδιαφερόμενα μέρη. Επιπλέον, οι πολιτικές ενδέχεται να περιορίζονται από περιορισμούς (π.χ. χρονικούς ή χωρικούς περιορισμούς) και να επιβάλλονται υποχρεώσεις (π.χ. πληρωμές) στις άδειες.

3.2.β Εισαγωγή στην ODRL

Πολλά επιχειρηματικά σενάρια απαιτούν την έκφραση των επιτρεπόμενων και απαγορευμένων ενεργειών σε σχέση με τους πόρους. Αυτές οι επιτρεπόμενες/απαγορευμένες ενέργειες εκφράζονται συνήθως με τη μορφή πολιτικών, δηλαδή εκφράσεις που υποδεικνύουν εκείνες τις χρήσεις και επαναχρήσεις του περιεχομένου που είναι σύμφωνες με τους υπάρχοντες κανονισμούς ή με τους περιορισμούς που ορίζει ο κάτοχος. Οι πολιτικές μπορούν επίσης να εμπλουτιστούν με πρόσθετες πληροφορίες, π.χ. ποιοι είναι οι υπεύθυνοι για τον ορισμό αυτής της Πολιτικής και αυτοί που υποχρεούνται να συμμορφωθούν με αυτήν, ποιοι είναι οι πρόσθετοι περιορισμοί που πρέπει να σχετίζονται με τις Άδειες, τις Απαγορεύσεις και τις Υποχρεώσεις που εκφράζονται από την Πολιτική. Η ικανότητα έκφρασης αυτών των εννοιών και σχέσεων είναι σημαντική τόσο για τους παραγωγούς περιεχομένου, δηλαδή, μπορούν να δηλώσουν με σαφή τρόπο ποιες είναι οι επιτρεπόμενες και απαγορευμένες ενέργειες για την

αποφυγή κακής χρήσης, όσο και για τους καταναλωτές, δηλαδή, μπορεί να γνωρίζουν ακριβώς τι πόρους που επιτρέπεται να χρησιμοποιούν και να επαναχρησιμοποιούν για να αποφευχθεί η παραβίαση κανόνων, νόμων ή περιορισμών του ιδιοκτήτη. Αυτή η προδιαγραφή περιγράφει μια κοινή προσέγγιση για την έκφραση αυτών των εννοιών πολιτικής.

Το μοντέλο πληροφοριών ODRL ορίζει το υποκείμενο σημασιολογικό μοντέλο για δηλώσεις άδειας, απαγόρευσης και υποχρέωσης που περιγράφουν τη χρήση περιεχομένου. Το μοντέλο πληροφοριών καλύπτει τις βασικές έννοιες, οντότητες και σχέσεις που παρέχουν το θεμελιώδες μοντέλο για δηλώσεις χρήσης περιεχομένου. Αυτές οι αναγνώσιμες από μηχανές πολιτικές ενδέχεται να συνδέονται απευθείας με το περιεχόμενο με το οποίο σχετίζονται με στόχο να επιτραπεί στους καταναλωτές να ανακτήσουν εύκολα αυτές τις πληροφορίες.

3.2.γ Στόχος του μοντέλου

Ο πρωταρχικός στόχος του Μοντέλου Πληροφοριών ODRL είναι να παρέχει ένα τυπικό μοντέλο περιγραφής και μορφή που να εκφράζει δηλώσεις άδειας, απαγόρευσης και υποχρέωσης που θα συσχετίζονται με το περιεχόμενο γενικά. Αυτές οι δηλώσεις χρησιμοποιούνται για την περιγραφή των όρων χρήσης και επαναχρησιμοποίησης των πόρων. Το μοντέλο θα πρέπει να καλύπτει όσο το δυνατόν περισσότερες περιπτώσεις χρήσης άδειας, απαγόρευσης και υποχρέωσης, διατηρώντας παράλληλα τη μοντελοποίηση πολιτικής εύκολη, ακόμη και όταν αντιμετωπίζουμε περίπλοκες υποθέσεις.

Το μοντέλο πληροφοριών ODRL είναι ένα ενιαίο, συνεπές μοντέλο που μπορεί να χρησιμοποιηθεί από όλα τα ενδιαφερόμενα μέρη. Μια μεμονωμένη μέθοδος εκπλήρωσης μιας περίπτωσης χρήσης προτιμάται έντονα έναντι πολλαπλών μεθόδων, εκτός εάν υπάρχουν υπάρχοντα πρότυπα που πρέπει να τηρηθούν ή υπάρχει σημαντικό κόστος που σχετίζεται με τη χρήση μόνο μιας μεθόδου. Ενώ το μοντέλο πληροφοριών ODRL έχει δημιουργηθεί χρησιμοποιώντας αρχές Συνδεδεμένων Δεδομένων, η σχεδίαση προορίζεται να επιτρέψει υλοποιήσεις που δεν βασίζονται σε γραφήματα.

3.2.δ Ορολογία

Σε αυτή την ενότητα θα παρουσιάσουμε τις βασικές ορολογίες που χρησιμοποιεί η ODRL.

Policy
: Μια ομάδα ενός ή περισσότερων Κανόνων

Rule
: Μια αφηρημένη έννοια που αντιπροσωπεύει τα κοινά χαρακτηριστικά των *Αδειών*, των *Απαγορεύσεων* και των *Καθηκόντων*.

Action
: Μια Ενέργεια σε ένα Στοιχείο.

Permission
: Η δυνατότητα άσκησης μιας Ενέργειας σε ένα Στοιχείο.

Prohibition
: Η αδυναμία άσκησης μιας Ενέργειας σε ένα Στοιχείο.

Duty
: Η Υποχρέωση για να εξασκήσεις μια Ενέργεια.

Asset
: Ένας πόρος ή μια συλλογή πόρων που αποτελούν αντικείμενο ενός Κανόνα

Party
: Μια οντότητα ή μια συλλογή από οντότητες που αναλαμβάνουν Ρόλους σε έναν Κανόνα

Constraint
: Μια δυαδική/λογική έκφραση που βελτιώνει μια Ενέργεια και μια συλλογή Μέρους/Στοιχείων ή τις προϋποθέσεις που ισχύουν για έναν Κανόνα.

ODRL Validator
: Ένα σύστημα που ελέγχει τη συμμόρφωση των εκφράσεων πολιτικής ODRL, συμπεριλαμβανομένης της ταυτότητας των ιδιοτήτων και εάν σχετίζονται με τύπους τιμών όπως ορίζονται από το μοντέλο πληροφοριών ODRL, και τις απαιτήσεις επικύρωσης του μοντέλου πληροφοριών.

ODRL Evaluator
: Ένα σύστημα που καθορίζει εάν οι κανόνες μιας έκφρασης πολιτικής ODRL πληρούν την επιδιωκόμενη απόδοση Ενέργειας.

ODRL Core Vocabulary
: Το σύνολο των όρων που αντιπροσωπεύονται από το μοντέλο πληροφοριών ODRL.

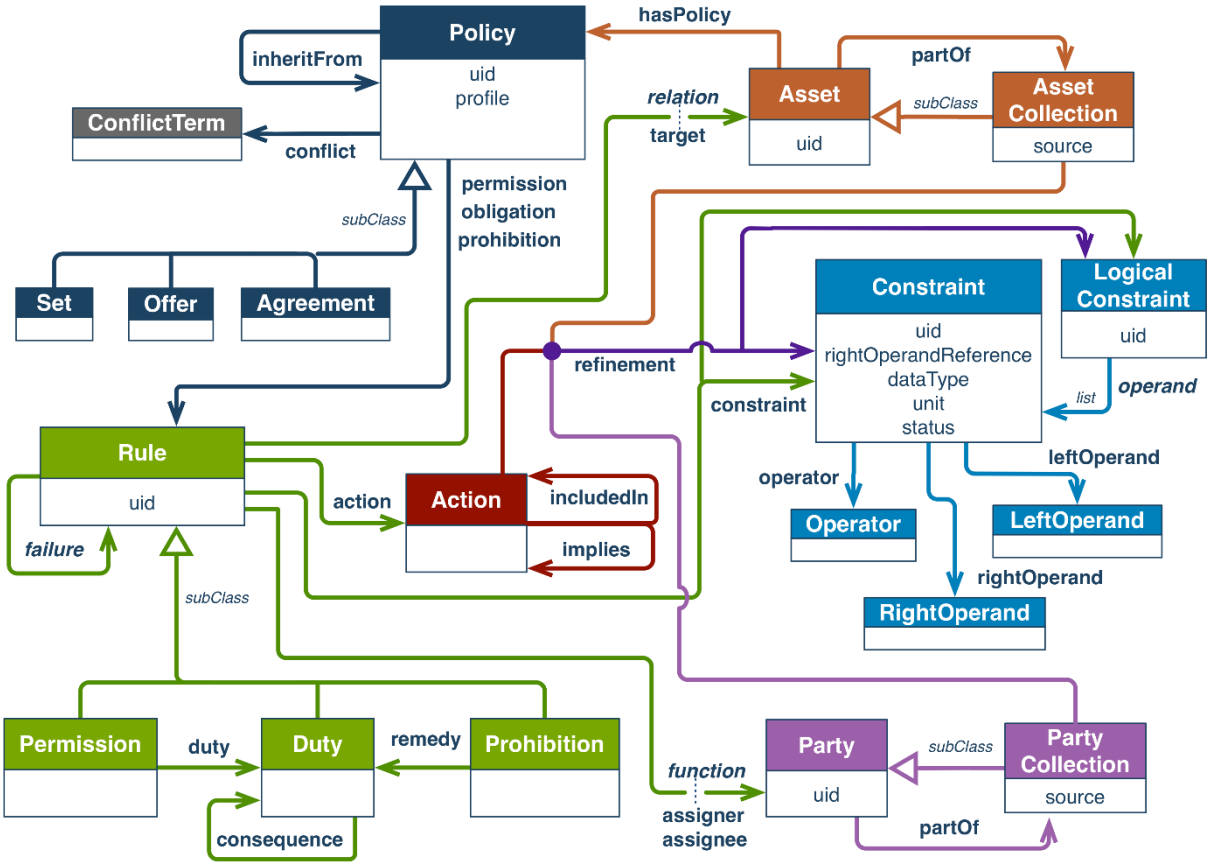
ODRL Profile
: Ένα συγκεκριμένο λεξιλόγιο κοινότητας ή τομέα που επεκτείνει το βασικό λεξιλόγιο ODRL με νέους όρους για την έκφραση Πολιτικών

ODRL Common Vocabulary
: Ένα σύνολο γενικών όρων που μπορούν να επαναχρησιμοποιηθούν από τα Προφίλ ODRL.

3.2.ε ODRL Σχεσιακό Μοντέλο

Το μοντέλο πληροφοριών ODRL αντιπροσωπεύει Πολιτικές που εκφράζουν Δικαιώματα, Απαγορεύσεις και Υποχρεώσεις που σχετίζονται με τη χρήση των πόρων του Στοιχείου. Το Μοντέλο Πληροφοριών εκφράζει ρητά τι επιτρέπεται και τι δεν επιτρέπεται από την Πολιτική, καθώς και άλλους όρους, απαιτήσεις και εμπλεκόμενα μέρη. Ο στόχος του Μοντέλου Πληροφοριών ODRL είναι να ενεργοποιήσει ευέλικτες εκφράσεις πολιτικής επιτρέποντας στον συντάκτη της πολιτικής να συμπεριλάβει τόσες ή λιγότερες λεπτομέρειες στις Πολιτικές.

Το παρακάτω σχήμα δείχνει το μοντέλο πληροφοριών ODRL.



Σχήμα 3.2.1: Μοντέλο πληροφοριών ODRL[10]

Το μοντέλο πληροφοριών ODRL έχει τις ακόλουθες κλάσεις:

- Policy - Μια μη κενή ομάδα Αδειών (μέσω της ιδιότητας άδειας) ή/και απαγορεύσεων (μέσω της ιδιότητας απαγόρευσης) και/ή Καθηκόντων (μέσω της ιδιότητας υποχρέωσης). Η κλάση Policy είναι η μητρική κλάση για τις υποκατηγορίες Set, Offer και Agreement:
  - Set - μια υποκατηγορία Πολιτικής που υποστηρίζει την έκφραση γενικών Κανόνων.
  - Offer - μια υποκατηγορία Πολιτικής που υποστηρίζει προσφορές κανόνων από τα συμβαλλόμενα Μέρη.
  - Agreement - μια υποκατηγορία Πολιτικής που υποστηρίζει τη χορήγηση Κανόνων από τον εκχωρούντα στον εκχωρηθέντα.
- Asset - Ένας πόρος ή μια συλλογή πόρων που αποτελούν αντικείμενο ενός Κανόνα (μέσω της ιδιότητας αφηρημένης σχέσης). Η κλάση Asset είναι η μητρική κλάση για:
  - AssetCollection - μια υποκατηγορία της Asset που προσδιορίζει μια συλλογή πόρων.
- Party - Μια οντότητα ή μια συλλογή οντοτήτων που αναλαμβάνουν ρόλους σε έναν Κανόνα (μέσω της ιδιότητας αφηρημένης συνάρτησης). Η κλάση Party είναι η γονική κλάση για:

    - PartyCollection - μια υποκατηγορία της Party που προσδιορίζει μια συλλογή οντοτήτων.
- Action – Μια Ενέργεια σε ένα Asset.
- Rule - Μια αφηρημένη έννοια που αντιπροσωπεύει τα κοινά χαρακτηριστικά των Αδειών, των Απαγορεύσεων και των Καθηκόντων.
    - Permission - Η δυνατότητα άσκησης μιας Ενέργειας σε ένα Asset. Η Άδεια ΜΠΟΡΕΙ να έχει και την ιδιότητα του καθήκοντος που εκφράζει μια συμφωνημένη Ενέργεια που ΠΡΕΠΕΙ να ασκηθεί (ως προϋπόθεση για τη χορήγηση της Άδειας).
    - Prohibition - Η αδυναμία άσκησης Ενέργειας σ' ένα Asset.
    - Duty – Η υποχρέωση να ασκήσεις μια Ενέργεια.
    - Constraint/LogicalConstraint - Μια δυαδική/λογική έκφραση που βελτιώνει μια Ενέργεια και μια συλλογή Party/Asset ή τις προϋποθέσεις που ισχύουν για έναν Κανόνα.

    Το μοντέλο πληροφοριών ODRL περιλαμβάνει σχέσεις ιδιοτήτων μεταξύ των κλάσεων. Οι περισσότερες ονομάζονται ρητά ιδιότητες και μερικές είναι αφηρημένες ιδιότητες (*specifically, relation, function, operand, and failure*). Οι αφηρημένες ιδιότητες είναι γενικές μητρικές ιδιότητες που έχουν σχεδιαστεί για να αντιπροσωπεύονται από θυγατρικές ιδιότητες (subtypes) με ρητή σημασιολογία.

Για παράδειγμα, οι δύο ιδιότητες *relation* και *function* έχουν σχεδιαστεί για να αντιπροσωπεύουν την εννοιολογική σχέση μεταξύ του Rule και των κλάσεων Asset και Party. Το σχήμα δείχνει την ιδιότητα *relation* με subtype target για να εκφράσει ότι το Asset είναι το κύριο θέμα του Rule. Η ιδιότητα *function* έχει subtype assigner για να εκφράσει το Party που εκδίδει τον Rule και τον subtype assignee για να εκφράσει το παραληφθέν Party του Rule.

ΚΕΦΑΛΑΙΟ 4 Ανάπτυξη συστήματος

Στο κεφάλαιο αυτό, παρουσιάζουμε το σύστημα που αναπτύξαμε. Θα προσπαθήσουμε να κατανοήσουμε τον τρόπο λειτουργίας του μέσα από την ανάλυση της αρχιτεκτονικής του, τις τεχνολογίες που χρησιμοποιήθηκαν για να αναπτυχθεί. Επιπλέον, θα δώσουμε ένα παράδειγμα χρήσης του, ώστε να παρουσιαστεί η εφαρμογή του στον πραγματικό κόσμο.

4.1 Απαιτήσεις–Περιπτώσεις χρήσης συστήματος

Για να κατανοήσουμε καλύτερα και να ολοκληρώσουμε με μεγαλύτερη ευκολία αυτό το σύστημα, προχωρήσαμε στην προσδιορισμό των περιπτώσεων χρήσεως (use-cases) και των απαιτήσεων του συστήματος (requirements).

4.1.α Περιπτώσεις χρήσης Συστήματος

Σύμφωνα με τον Βεσκούκη, ως περίπτωση χρήσης ορίζεται ως «η αλληλουχία ενεργειών που εκτελεί το λογισμικό αλληλοεπιδρώντας με τον χρήστη ή με εξωτερικά συστήματα, προκειμένου να ικανοποιήσει μία λειτουργική απαίτηση.» [Veskoukis, V. (2015)]. Οι περιπτώσεις χρήσης μας βοηθούν στο να προσδιορίσουμε, να ερμηνεύσουμε και οργανώσουμε της απαιτήσεις και τα χαρακτηριστικά σε ένα σύστημα και τον τρόπο χρήσης τους. Στο σύστημα μας, οι περιπτώσεις χρήσεις είναι οι εξής:

<u>Δημιουργία ODRL πολιτικών</u>
Για την υλοποίηση του συστήματος μας αρχικά προχωρούμε στην δημιουργία πολιτικών σε ODRL. Καθορίζουμε δηλαδή τα ψηφιακά δικαιώματα ενός αρχείου, προσδιορίζοντας τις άδειες, τις υποχρεώσεις σχετικά με τη χρήση του αλλά και τους περιορισμούς για το κοινό για το οποίο προορίζεται.

<u>Μετατροπή ODRL πολιτικής σε ABE</u>
Χρησιμοποιώντας την πολιτική που δημιουργήσαμε προηγουμένως, την μετατρέπουμε σε αναγνώσιμα δεδομένα από τον αλγόριθμο κρυπτογράφησης τα οποία θα χρησιμοποιήσουμε για την δημιουργία του κρυπτοκειμένου.

<u>Δημιουργία κλειδιών κρυπτογράφησης</u>
Το σύστημα μας δημιουργεί το δημόσιο κλειδί (Public Key) και το κύριο ιδιωτικό κλειδί (Master Secret Key). Ένας Key Generator (γεννήτρια κλειδιών) με βάσει το κύριο ιδιωτικό κλειδί που έχει δημιουργηθεί νωρίτερα και τα χαρακτηριστικά που ορίζουμε στο σύστημα, δημιουργεί το μοναδικό ιδιωτικό κλειδί (Secret Key).

Κρυπτογράφηση

Σε αυτήν την περίπτωση χρήσης το αρχείο που έχει εισαχθεί και αξιοποιώντας τα δεδομένα από την ODRL πολιτική που μας παρέχονται, προχωρούμε στην κρυπτογράφηση του, δημιουργώντας το κρυπτοκείμενο (ciphertext).

Αποκρυπτογράφηση

Στο τελευταίο μέρος του συστήματος γίνεται η αποκρυπτογράφηση της πληροφορίας. Για να υλοποιηθεί αυτή η διαδικασία παίρνουμε ως παραμέτρους το ιδιωτικό κλειδί (secret key), το οποίο είναι συνδεδεμένο με τα χαρακτηριστικά που ικανοποιούν τις πολιτικές και το αποτέλεσμα της διαδικασίας της κρυπτογράφησης, δηλαδή το κρυπτογραφημένο κείμενο αρχείο (ciphertext).

4.1.β Απαιτήσεις Συστήματος

Ως απαίτηση συστήματος ορίζεται «μια λειτουργία που αυτό θα πρέπει να επιτελεί ή μια συνθήκη που θα πρέπει να ικανοποιεί όταν θα έχει ολοκληρωθεί η κατασκευή του.» [Veskoukis, V. (2015)] Η ικανότητα του να μπορείς να διακρίνεις ποιες θα είναι οι λειτουργίες που θα εκτελεί του σύστημα σου είναι πολύ σημαντική, διότι αποφεύγεις την δημιουργία λογισμικού που δεν καλύπτει τις ανάγκες για τις οποίες αναπτύσσεται. Επομένως, οι απαιτήσεις που πρέπει να καλύπτει το δικό μας σύστημα είναι οι εξής:

- Δημιουργία πολιτικής (policy) σε ODRL για κάποιο αρχείο.
- Δημιουργία δημοσίου κλειδιού (Public Key)
- Δημιουργία κύριου κρυφού κλειδιού (Master Secret Key).
- Συνδυασμός των ABE χαρακτηριστικών (attributes) για την δημιουργία του κρυφού κλειδιού (secret key).
- Εισαγωγή του αρχείου που θέλουμε να κρυπτογραφήσουμε στο σύστημα.
- Μετατροπή της ODRL πολιτικής σε ABE.
- Κρυπτογράφηση του αρχείου.
- Εξαγωγή του κρυπτοκειμένου (ciphertext).
- Συνδυασμός κρυφού κλειδιού και κρυπτοκειμένου για την αποκρυπτογράφηση αυτού.

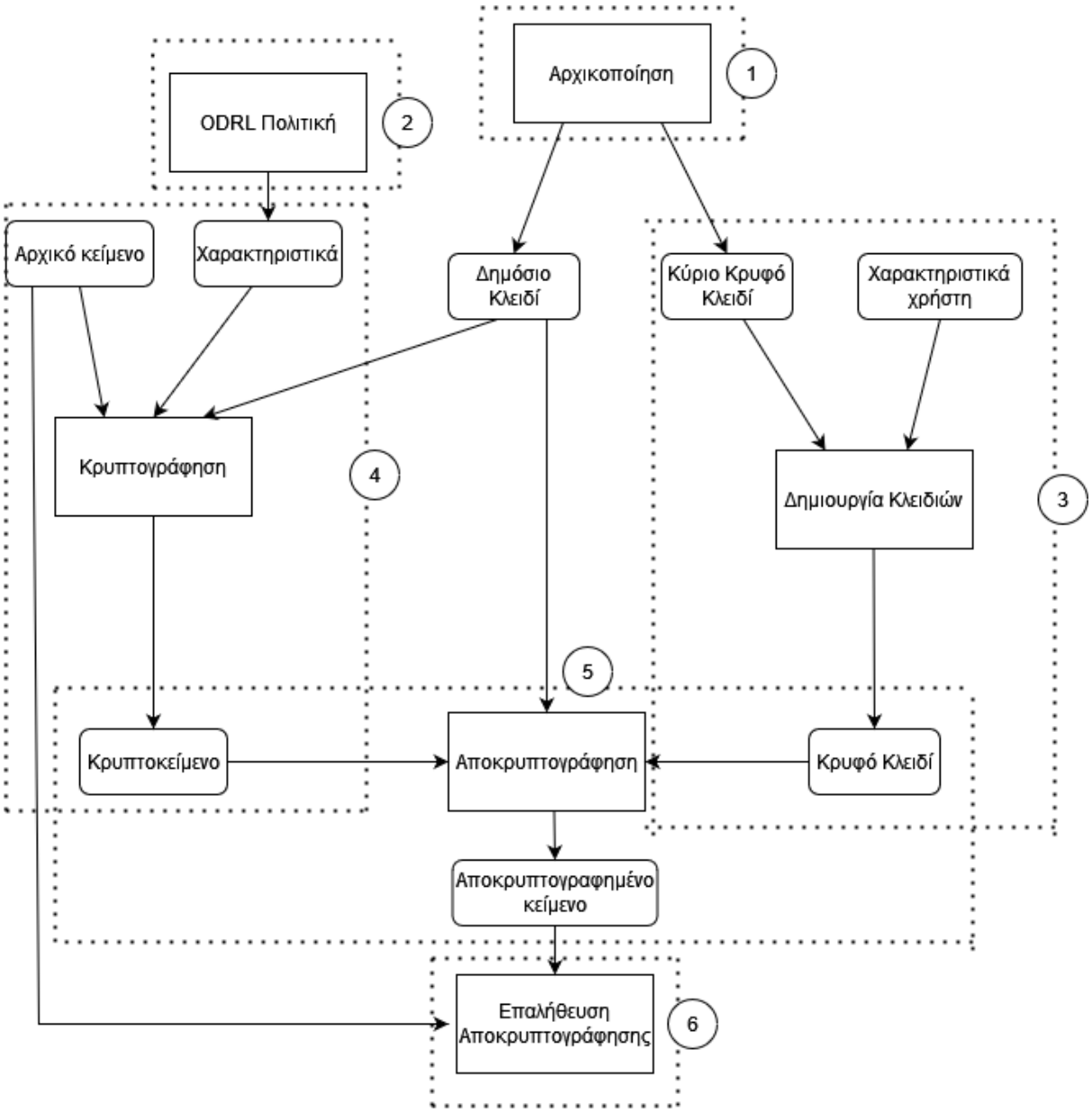
- Εμφάνιση μηνύματος επιτυχημένης ή αποτυχημένης αποκρυπτογράφησης.

4.2 Αρχιτεκτονική συστήματος

Ο στόχος της παρούσας πτυχιακής εργασίας είναι η ανάπτυξη ενός συστήματος το οποίο θα δέχεται ένα αρχείο ως είσοδο και θα κρυπτογραφείται βάσει της υποκείμενης πολιτικής χρήσης του. Στο πρώτο στάδιο δημιουργείται μια πολιτική τύπου ODRL, η οποία μέσω Αδειών και Απαγορεύσεων καθορίζει τις Ενέργειες που μπορεί να ασκήσει ο παραλήπτης της πληροφορίας. Θέτει ουσιαστικά περιορισμούς χρήσης του αρχείου βάσει χαρακτηριστικών του παραλήπτη. Στο δεύτερο στάδιο, με τα χαρακτηριστικά αυτά να παρέχονται από την ODRL πολιτική και μέσω της τεχνικής κρυπτογράφησης CP-ABE , προχωράμε στην κρυπτογράφηση του αρχείου. Στο τελικό στάδιο, αυτό της αποκρυπτογράφησης , γίνεται σύγκριση των χαρακτηριστικών που κατέχει ο χρήστης με αυτά που πρέπει να πληροί, όπως ορίζονται από την πολιτική. Εφόσον ικανοποιείται η πολιτική τότε η αποκρυπτογράφηση κρίνεται επιτυχής και ο χρήστης αποκτάει πρόσβαση στο αρχείο. Σε αντίθετη περίπτωση, η αποκρυπτογράφηση αποτυγχάνει.

Για να επιτευχθεί ο στόχος της υλοποίησης του παραπάνω συστήματος έχουμε τη δημιουργία έξι διαδικασιών.

Στο παρακάτω σχήμα παρουσιάζεται η σχέση μεταξύ των διαδικασιών και ακολούθως εξηγείται η κάθε μια από αυτές ξεχωριστά.



Εικόνα 4.2.1: Διαδικασίες Συστήματος

Η 1η διαδικασία (Setup) είναι η αρχικοποίηση του συστήματος. Εδώ, δημιουργείται το δημόσιο κλειδί (Public Key-pk) και το κύριο κρυφό κλειδί (Master Secret Key-msk). Χρησιμοποιώντας την σχετική λειτουργία της βιβλιοθήκης FAME προκύπτει η αρχικοποίηση με αυτόν τον τρόπο:

```
FAMEMasterKey msk = cpabe.setup();
```

Στην 2η διαδικασία (ODRL Policy) δημιουργείται η πολιτική χρήσης σε γλώσσα έκφρασης ODRL. Πιο συγκεκριμένα, ορίζονται τα χαρακτηριστικά που πρέπει να πληροί ο χρήστης, ώστε να μπορέσει να αποκτήσει πρόσβαση στο αρχείο που μας ενδιαφέρει να προστατεύσουμε. Αν καταφέρει τελικά να αποκτήσει πρόσβαση θα μπορέσει να ασκήσει τις Ενέργειες που έχει επιτρέψει ο κάτοχος του αρχείου μέσα από την δημιουργία της συγκεκριμένης πολιτικής, π.χ. ανάγνωση, εκτύπωση.

Η 3η διαδικασία αφορά την δημιουργία του κρυφού κλειδιού (Secret Key-skey) που θα χρησιμοποιηθεί από τον χρήστη στην αποκρυπτογράφηση του αρχείου. Για να επιτευχθεί η δημιουργία του κρυφού κλειδιού, γίνεται συνδυασμός του κύριου κρυφού κλειδιού και των σύνολο των χαρακτηριστικών που προσδιορίζουν τον χρήστη. Τα χαρακτηριστικά αυτά μπορούν να αντλούνται, π.χ. από ένα αρχείο ηλεκτρονικής ταυτότητας.

```
FAMESecretKey skey = cpabe.keygen(msk, new String[]{attr});
```

Η 4η διαδικασία είναι αυτή της κρυπτογράφησης. Το αρχικό κείμενο/αρχείο κρυπτογραφείται μέσω ενός αλγορίθμου κρυπτογράφησης με βάση τα χαρακτηριστικά που πρέπει να πληροί ο χρήστης και τα οποία εξάγουμε μέσω της μετατροπής της ODRL πολιτικής που δημιουργήσαμε στην 2η διαδικασία. Ως αποτέλεσμα από την διαδικασία της κρυπτογράφησης παίρνουμε το κρυπτοκείμενο (Ciphertext-cpt).
Λόγω κάποιων αδυναμιών της βιβλιοθήκης που χρησιμοποιήσαμε δεν ήταν δυνατή η εξαγωγή των constraints με την βοήθεια κάποιας συνάρτησης, για αυτό χρησιμοποιήσαμε τον παρακάτω τρόπο ώστε να προσπεραστεί το πρόβλημα.

```
String encryptionPolicy =
permission.getConstraints().get(0).labels.get(0);
```

Η διαδικασία της κρυπτογράφησης γίνεται με την χρήση της σχετικής βιβλιοθήκης FAME.

```
FAMECipherText cpt = cpabe.encrypt(String.join(delimiter:
" and ", encryptionPolicy), content.getBytes());
```

Η 5η διαδικασία είναι αυτή της αποκρυπτογράφησης. Σε αυτό το βήμα ο αλγόριθμος αποκρυπτογράφησης δέχεται ως είσοδο το κρυπτογραφημένο κείμενο/αρχείο, το μοναδικό κρυφό κλειδί αλλά και το δημόσιο κλειδί. Το αποτέλεσμα αυτής της διαδικασίας είναι ένα αποκρυπτογραφημένο κείμενο (decrypted). Μέσω της βιβλιοθήκης JPBC-FAME η αποκρυπτογράφηση γίνεται με την παρακάτω εντολή:

```
byte[] decrypted = cpabe.decrypt(skey, cpt);
```

Στην 6η και τελευταία διαδικασία του συστήματος μας γίνεται η επαλήθευση της αποκρυπτογράφησης. Εάν υπάρχει ταύτιση μεταξύ του decrypted text και του αρχικού κειμένου τότε η διαδικασία κρίνεται επιτυχημένη και έχουμε και την εμφάνιση του αντίστοιχου μηνύματος. Σε αντίθετη περίπτωση εμφανίζει το ανάλογο μήνυμα.

4.3 Παράδειγμα χρήσης

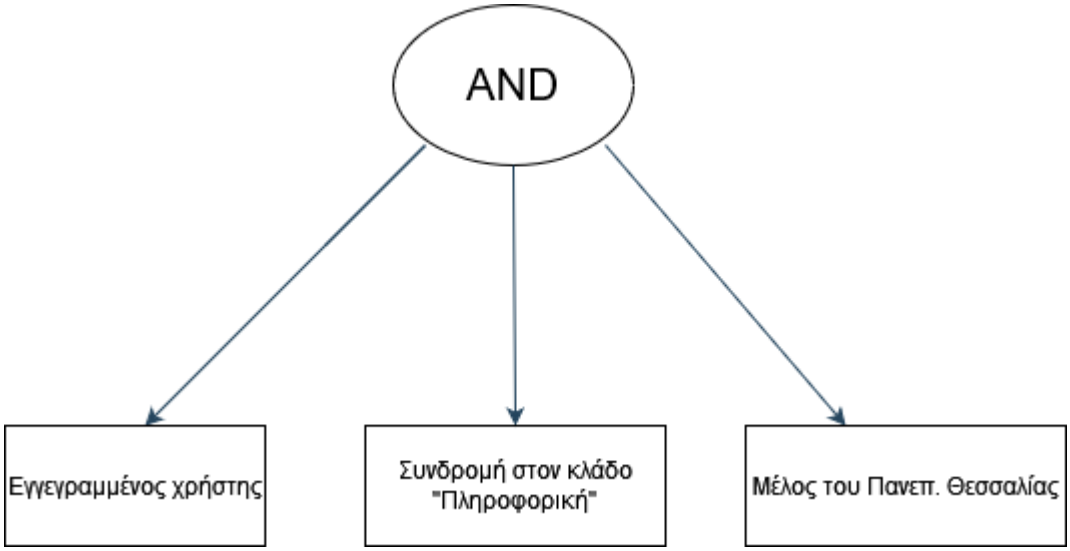
Το σύστημα που έχουμε αναπτύξει και παρουσιάσει σε αυτήν την πτυχιακή μπορεί να εφαρμοστεί σε περιπτώσεις διαμοιρασμού ενός ψηφιακού στοιχείου και να διασφαλίζει τόσο την χρήση του βάσει των επιθυμιών του κατόχου του όσο και της εμπιστευτικής μεταφορά του στις οντότητες για τις οποίες προορίζεται.

Για να κάνουμε κατανοητό το πως μπορεί να λειτουργήσει και να χρησιμοποιηθεί αυτό το σύστημα, παραθέτουμε το εξής παράδειγμα χρήσης.

Στην ιστοσελίδα κάποιου επιστημονικού εκδότη όπως για παράδειγμα του διεθνούς φήμης Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (**IEEE**) ανεβαίνει μια επιστημονική δημοσίευση που αφορά τον κλάδο της Πληροφορικής και προορίζεται συγκεκριμένα για τα μέλη του Πανεπιστημίου Θεσσαλίας. Ο δημιουργός αυτής, προστατεύει τα ψηφιακά δικαιώματα χρήσης της μέσω μιας πολιτικής ODRL. Προχωρώντας στην λήψη της συγκεκριμένης δημοσίευσης γίνεται άμεσα αντιληπτό ότι πρόκειται για ένα κρυπτογραφημένο αρχείο με βάσει μιας πολιτικής, δηλαδή ένα σύνολο χαρακτηριστικών που θα πρέπει να έχουν οι χρήστες, που θέλουν να έχουν πρόσβαση στην ανάγνωση και ανάλογα τις επιθυμίες του κατόχου της, στην εκτύπωση και στον διαμοιρασμό της δημοσίευσης. Αυτά τα χαρακτηριστικά είναι τα εξής:

1) Να είναι εγγεγραμμένος χρήστης της ιστοσελίδας.
2) Να έχει ενεργή συνδρομή για τον κλάδο της Πληροφορικής.
3) Να είναι μέλος του Πανεπιστημίου Θεσσαλίας (ανάγκη επαλήθευσης μέσω πανεπιστημιακού λογαριασμού).

Στην παρακάτω απεικόνιση δίνεται η λογική αναπαράσταση της αναφερόμενης πολιτικής (λογικό δένδρο).



Σχήμα 4.3.1: Πολιτική ABE

Επιπλέον, παρακάτω παρουσιάζεται η πολιτική εκφρασμένη σε ODRL.

```
<http://ieee.com/policy:Access_my_ Publication>
        a odrl:Policy , odrl:Agreement ;
        rdfs:label "policy:Access_my_ Publication" ;
        odrl:permission [ a odrl:Permission ;
                        odrl:action odrl:archive , odrl:read ;
                        odrl:assignee <http://ieee.com/publisher> ;
                        odrl:assigner <http://ieee.com/visitor> ;
                        odrl:constraint <http://ieee.com/visitorRequirements> ;
                        odrl:target "< http://ieee.com/My_Publication >"
                       ] .

<http://ieee.com/visitorRequirements>
        a odrl:Constraint ;
        odrl:registered "isRegistered" ;
        odrl:operator odrl:eq .

        a odrl:Constraint ;
        odrl:subscribed "toComputerScience" ;
        odrl:operator odrl:eq .

        a odrl:Constraint ;
        odrl:memberOf "UniversityOfThessaly" ;
        odrl:operator odrl:eq .
```

Σχήμα 4.3.2: ODRL πολιτική σε RDF

Σε αυτό το παράδειγμα έχουμε δύο χρήστες που έχουν κάνει λήψη της δημοσίευσης και προσπαθούν να αποκτήσουν πρόσβαση στο περιεχόμενο της. Σε πρώτη φάση και οι δύο είναι εγγεγραμμένοι χρήστες της ιστοσελίδας του εκδότη, άρα διαθέτουν το σχετικό attribute. Επιπλέον και οι δύο έχουν ενεργή συνδρομή για να έχουν πρόσβαση στις δημοσιεύσεις που σχετίζονται με τον κλάδο της Πληροφορικής. Τέλος, μόνο ο πρώτος χρήστης έχει συνδεθεί μέσω του πανεπιστημιακού λογαριασμού ώστε να γίνει η επαλήθευση πως είναι μέλος του Πανεπιστημίου Θεσσαλίας.
Ως εκ τούτου, τα attributes που έχουν χρησιμοποιηθεί για τον πρώτο είναι τα εξής:

- registered: "isRegistered"
- subscribed: "toComputerScience"
- memberOf: "UniversityOfThessaly"

Ενώ για τον δεύτερο τα εξης:

- registered: "isRegistered"
- subscribed: "toComputerScience"

Συνεπώς το αποτέλεσμα της πρώτης περίπτωσης είναι ο χρήστης να μπορέσει επιτυχημένα να αποκρυπτογραφήσει την δημοσίευση και να έχει την δυνατότητα να ασκήσει τις Ενέργειες που έχει ορίσει ο κάτοχος των ψηφιακών δικαιωμάτων της. Στην δεύτερη περίπτωση όπως γίνεται αντιληπτό, ενώ ο χρήστης ικανοποιεί τις δύο πρώτες συνθήκες της λογικής πολιτικής αλλά όχι και την τρίτη, δεν θα μπορέσει να αποκρυπτογραφήσει το αρχείο και να αποκτήσει πρόσβαση σε αυτό.

4.4 Τεχνολογίες συστήματος

Για την ανάπτυξη του παραπάνω συστήματος χρησιμοποιήθηκαν κάποια εργαλεία και βιβλιοθήκες που θα αναλυθούν παρακάτω. Η επιλογή αυτών έγινε με γνώμονα την μεταξύ τους συμβατότητα και την καταλληλότητα τους ώστε να στεφθεί επιτυχημένα η ανάπτυξη του ζητούμενου συστήματος.

Για την υλοποίηση της πτυχιακής επιλέξαμε να χρησιμοποιήσουμε την Java, ως γλώσσα προγραμματισμού και την βιβλιοθήκη jPBC-FAME, μιας βιβλιοθήκης που αναπτύχθηκε από τον C.Chow το 2020 και έχει βασιστεί πάνω στην DET-ABE των M. Morales-Sandoval και A. Diaz-Perez του 2015. Τέλος, για την δημιουργία πολιτικών σε γλώσσα αναγνώσιμης μορφής από μηχανή (RDF) επιλέξαμε να χρησιμοποιήσουμε το ODRL 2.0, ένα API δημιουργημένο από τον Víctor Rodríguez Doncel το 2014.

Java

Η Java είναι η γλώσσα προγραμματισμού που επιλέχθηκε για να αναπτυχθεί το σύστημα της παρούσας εργασίας. Είναι μια πολύ δημοφιλής γλώσσα προγραμματισμού που προτιμάται για την ευελιξία και τη

φορητότητά της. Μπορείς να μετακινήσεις γρήγορα κώδικα γραμμένο σε Java από ένα λάπτοπ σε ένα κινητό. Ο μηχανισμός Java Cryptography Extension προσφέρει ένα API κρυπτογράφησης για Java (JCE). Οι εφαρμογές μπορούν να επικοινωνούν μεταξύ τους χρησιμοποιώντας μια διεπαφή λογισμικού που ονομάζεται API (διεπαφή προγραμματισμού εφαρμογών). Το JCE παρέχει ένα πλαίσιο και υλοποίηση για κρυπτογράφηση, δημιουργία κλειδιού και συμφωνία κλειδιού και αλγόριθμους ελέγχου ταυτότητας μηνυμάτων (MAC). Το JCE δίνει τη δυνατότητα να κρυπτογραφείς και να αποκρυπτογραφείς δεδομένα, να επικυρώνεις δεδομένα που δίνονται από άλλους, να σχολιάζεις κώδικα και να εκτελείς διοικητικές εργασίες που σχετίζονται με κρυπτογραφία.

jPBC

Η βιβλιοθήκη Java Pairing-Based Cryptography Library (JPBC) παρέχει την δυνατότητα πρόσβασης στην Pairing-Based Cryptography Library (PBC), μιας βιβλιοθήκης που αναπτύχθηκε από τον Ben Lynn, για την εκτέλεση των μαθηματικών πράξεων στις οποίες βασίζονται τα κρυπτοσυστήματα που βασίζονται σε σύζευξη απευθείας στην Java. Για την ανάθεση του υπολογισμού σύζευξης στην PBC, η JPBC περιλαμβάνει μια συνάρτηση Wrapper ώστε να υπάρξει αύξηση της απόδοσης. Η διαφορά με την PBC είναι ότι περιέχει μια υλοποίηση Πολυγραμμικών Χαρτών που βασίζεται στο έγγραφο Practical Multilinear Maps over the Integers από τους Coron, Lepoint και Tibouchi [2013]. Η υλοποίηση υποστηρίζει τη λειτουργία πολλαπλών νημάτων και χρησιμοποιεί αρχεία με αντιστοίχιση μνήμης για αποθήκευση στις απαιτήσεις κύριας μνήμης.

FAME

Το 2017 οι S. Agrawal και M.Chase βασισμένοι στην έρευνα πάνω στην CP-ABE των Bethencourt,Sahai, and Waters του 2007, η οποία διακρίνεται για την απλή δομή και αξιέπαινη απόδοση της, προχώρησαν στην εξέλιξη της και την παροχή πλήρης ασφάλειας υπό μιας τυπικής υπόθεσης. Ενώ επίσης κρυπτογραφεί, αποκρυπτογραφεί και δημιουργεί γρηγορότερα κλειδιά χωρίς να θέτει κανέναν περιορισμό στο μέγεθος των πολιτικών ή των χαρακτηριστικών συνόλων που μπορούν να κωδικοποιηθούν.

ODRL2.0 API

Το API αυτό αναπτύχθηκε από τον Víctor Rodríguez Doncel το 2014 και βασίζεται πάνω στην γλώσσα έκφρασης πολιτικών ODRL 2.0. Η γλώσσα αυτή καθαυτή καθορίζεται από το ODRL W3C Community and Business Group. Αυτό το API είναι σε θέση να χειρίζεται (ανάγνωση/εγγραφή) εκφράσεις που συμμορφώνονται με ένα υποσύνολο της προδιαγραφής του βασικού μοντέλου και του κοινού λεξιλογίου της γλώσσας. Το ODRL2.0 μπορεί να σειριοποιηθεί ως XML, ως JSON ή ως RDF με βάση την πρόχειρη οντολογία ODRL2.0. Η μόνη σειριοποίηση που υποστηρίζει αυτό το Java API σε αυτήν την έκδοση είναι το RDF.

ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα

Στην παρούσα πτυχιακή παρουσιάσαμε και αναπτύξαμε ένα σύστημα με την βοήθεια της Κρυπτογράφησης Βάσει Χαρακτηριστικών, εξηγώντας πως η χρήση αυτής της μοντέρνας και συνεχώς αναπτυσσόμενης τεχνολογίας μπορεί να δώσει λύση στην προστασία ψηφιακών δικαιωμάτων πάνω σε ψηφιακά αρχεία. Σε συνδυασμό με μια γλώσσα έκφρασης δικαιωμάτων όπως η ODRL παρέχεται μεγαλύτερη ασφάλεια στους δημιουργούς και προστασία στο έργο τους.

Σε μελλοντική εργασία και με την περαιτέρω ανάπτυξη του συστήματος, θα στοχεύαμε στην διασφάλιση της προστασίας σε μεγαλύτερο βαθμό. Καθώς η τρέχουσα τεχνολογία της ODRL που χρησιμοποιήσαμε έχει κάποιους περιορισμούς, όπως η σειριοποίηση της μόνο σε RDF και όχι και XML, JSON. Επίσης η βιβλιοθήκη JPBC-FAME υποστηρίζει μόνο μέχρι 10 attributes. Ως εκ τούτου, με την εξάλειψη αυτών των μειονεκτημάτων θα συνεισφέραμε ακόμα περισσότερο στην ασφάλεια των ψηφιακών αρχείων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Agrawal S., Chase M., [2017]
FAME: Fast Attribute-based Message Encryption

[2] Akinyele J., Garman C., Miers I., Pagano M., Rushanan M., Green M., Rubin A., [2013]
Charm: a framework for rapidly prototyping cryptosystems

[3] Bethencourt J., Sahai A., Waters B., [2007] Ciphertext-Policy Attribute-Based Encryption

[4] Cabrio E., Aprosio A., Villata S., [2014]
These Are Your Rights: A Natural Language Processing Approach to Automated
RDF Licenses Generation

[5] Chow Chriz
JPBC-FAME
https://github.com/chrizchow/JPBC-FAME

[6] Cryptosystems
https://www.tutorialspoint.com/cryptography/cryptosystems.htm

[7] Hess D., [2015] Managing digital rights with rights
expression languages

[8] Krishna A., Dr. L. C. Manikandan, [2020]
A Study on Cryptographic Techniques
https://doi.org/10.32628/CSEIT206453

[9] Morales-Sandoval M., Diaz-Perez A., [2015]
DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute
Based Encryption

[10] ODRL Information Model 2.2
https://www.w3.org/TR/odrl-model/

[11] Pang L., Yang J., Jiang Z., [2014]
A Survey of Research Progress and Development Tendency of Attribute-Based Encryption
http://dx.doi.org/10.1155/2014/193426

[12] Rodríguez-Doncel Víctor
ODRL2.0 API
https://github.com/oeg-upm/licensius

[13] Simmons G. J., Cryptology
https://www.britannica.com/topic/cryptology

[14] Symmetric vs. Asymmetric Encryption – What are the differences?
https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[15] TechTarget, Cryptology
https://www.techtarget.com/searchsecurity/definition/cryptology

[16] The Java Pairing Based Cryptography Library (JPBC)
http://gas.dia.unisa.it/projects/jpbc/

[17] Veskoukis, V. (2015). Στοιχεία Τεχνολογίας Λογισμικού. Kallipos.gr.
https://repository.kallipos.gr/handle/11419/3160

[18] World Wide Web Consortium
https://www.w3.org/

[19] Zickau S., Thatmann D., Butyrtschik A., Denisow I., Kupper A., [2016] Applied Attribute-based Encryption Schemes

[20] Zimmermann P., An Introduction to Cryptography

[21] 7 Best Programming Languages for Cryptography
https://www.codecademy.com/resources/blog/programming-languages-for-cryptography/