Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής – Ανάπτυξη Λογισμικού και Τεχνητής Νοημοσύνης»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Εξατομικευμένο Λογισμικό Ασφαλούς Διαμοίρασης Αρχείων με Ελλειπτική Κρυπτογράφηση** **Personalized Secure File Sharing using Elliptic Curves**
Ονοματεπώνυμο Φοιτητή	**Βαρκάς Χρήστος - Στυλιανός**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 18004**
Επιβλέπων	**Ευάγγελος Σακκόπουλος, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2021**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Ευάγγελος Σακκόπουλος Επίκουρος Καθηγητής	Ευθύμιος Αλέπης Αναπληρωτής Καθηγητής	Μαρία Βίρβου Καθηγήτρια

Περιεχόμενα

Περίληψη

Η παρούσα διατριβή αφορά την ανάπτυξη μιας διαδικτυακής εφαρμογής, όπου σκοπός της είναι, η διαμοίραση αρχείων σε τρίτο άτομο, εκ των οποίων αυτών των αρχείων θα είναι Digitally Signed με χρήση Digital Certificate Authority που είναι εγκαταστημένη στον Server.

Τα κρυπτογραφικά συστήματα που βασίζονται στις ελλειπτικές καμπύλες αποτελούν ένα πολύ σημαντικό κομμάτι της κρυπτογραφίας δημόσιου κλειδιού και τα τελευταία χρόνια όλο και περισσότεροι επιστήμονες ασχολούνται με τη μελέτη τους. Τα πλεονεκτήματα των συστημάτων αυτών σε σχέση με τα συμβατικά κρυπτογραφικά συστήματα είναι ότι χρησιμοποιούν μικρότερες παραμέτρους και κλειδιά προσφέροντας τα ίδια επίπεδα ασφαλείας.

Κύριος στόχος της ασφάλειας γενικότερα στα πληροφοριακά συστήματα, αλλά και ειδικότερα στα βασισμένα στον Παγκόσμιο Ιστό (Web-based) περιβάλλοντα, είναι η διαφύλαξη της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας όλων των συστατικών τους μερών. Κάθε εξέλιξη της τεχνολογίας μοιάζει να δημιουργεί νέα προβλήματα ασφάλειας, έτσι η μεγαλύτερη πρόκληση στον χώρο της ασφάλειας οφείλεται ακριβώς στο ότι απαιτεί την άμεση εκμετάλλευση τεχνολογιών αιχμής για την αντιμετώπιση των νέων προβλημάτων που συνεχώς αναδύονται.

Χρειάζεται να γίνει περισσότερο σαφής η εικόνα των «επικίνδυνων καταστάσεων» ή «ζημιών». Τι ακριβώς διακυβεύεται; Οι επικρατούσες απόψεις διακρίνουν τις τρεις ακόλουθες βασικές έννοιες σε σχέση με τη διαχείριση ενός ασφαλούς συστήματος (Cherdantseva & Hilton, 2013):

- **Εμπιστευτικότητα (confidentiality):** Είναι έννοια στενά συνδεμένη με την ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Αφορά τη μη αποκάλυψη των ευαίσθητων πληροφοριών σε χρήστες που δεν έχουν την κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (integrity):** Αφορά τη δυνατότητα τροποποιήσεων (προσθήκες, διαγραφές και μεταβολές) των πληροφοριών. Μόνο σε κατάλληλα εξουσιοδοτημένους χρήστες πρέπει το σύστημα να επιτρέπει τέτοιου είδους ενέργειες. Έτσι διαφυλάσσεται η ακρίβεια και η πληρότητα των περιεχομένων ενός πληροφοριακού συστήματος.
- **Διαθεσιμότητα (availability):** Αφορά τη δυνατότητα άμεσης πρόσβασης στις πληροφορίες, στις υπηρεσίες και γενικότερα σε όλους τους πόρους πληροφορικής τεχνολογίας (IT resources) όταν ζητούνται, χωρίς αδικαιολόγητες καθυστερήσεις.

Όπως θα αναφέρουμε στη συνέχεια της εργασίας υπάρχουν διάφοροι τύποι αλγορίθμων για πιστοποιητικά, με διάφορους αλγόριθμους. Εμείς στη παρούσα εργασία θα χρησιμοποιήσουμε Elliptic Curve και συγκεκριμένα τον αλγόριθμο secp256k1 ο οποίος όπως υποδηλώνει και ο αριθμός του αλγορίθμου καθορίζει το μήκος του κλειδιού σε 256-bit), ισχύ ασφαλείας. Επίσης θα αναφερθούμε περιεκτικότερα για τον σκοπό της εργασίας καθώς και της χρήσης Elliptic Curve,τι επιλύει και τα πλεονεκτήματα της χρήσης αυτής.

Abstract

This dissertation concerns the development of an online application, the purpose of which is to share files to a third party, of which these files will be Digitally Signed using a Digital Certificate Authority installed on the Server. As we will mention later in the work there are different types of algorithms for certificates, with different algorithms.

Cryptographic systems based on elliptic curves are a very important part of public key cryptography and in recent years more and more scientists are studying them. The advantages of these systems over conventional cryptographic systems are that they use smaller parameters and keys while offering the same levels of security.

The main goal of security in information systems in general, but also in web-based environments in particular, is to preserve the confidentiality, integrity and availability of all their components. Every technological development seems to create new security problems, so the biggest challenge in the field of security is precisely because it requires the immediate use of cutting-edge technologies to deal with new problems that are constantly emerging.

The picture of "dangerous situations" or "damages" needs to be made clearer. What exactly is at stake? The prevailing views distinguish the following three basic concepts in relation to the management of a secure system (Cherdantseva & Hilton, 2013):

- **Confidentiality:** It is a concept closely related to privacy and secrecy. It concerns the non-disclosure of sensitive information to users who do not have the appropriate authorization.
- **Integrity:** It concerns the possibility of modifications (additions, deletions and changes) of information. Only properly authorized users should the system allow such actions. This preserves the accuracy and completeness of the contents of an information system.
- **Availability:** Refers to the possibility of direct access to information, services and in general to all information technology resources (IT resources) when requested, without undue delay.

In this work we will use the Elliptic Curve and specifically the algorithm secp256k1 which as the number of the algorithm indicates determines the key length in 256-bit), security power. We will also report more comprehensively on the purpose of the work as well as the use of the Elliptic Curve, what slves the advantages of this use.

Εισαγωγή

Αντικείμενο της παρούσας διατριβής είναι η δημιουργία μιας εφαρμογής διαμοίρασης αρχείων μεταξύ χρηστών τα οποία θα είναι Digitally Signed με τη χρήση Digital Certificate Authority που είναι εγκατεστημένη στον Server.

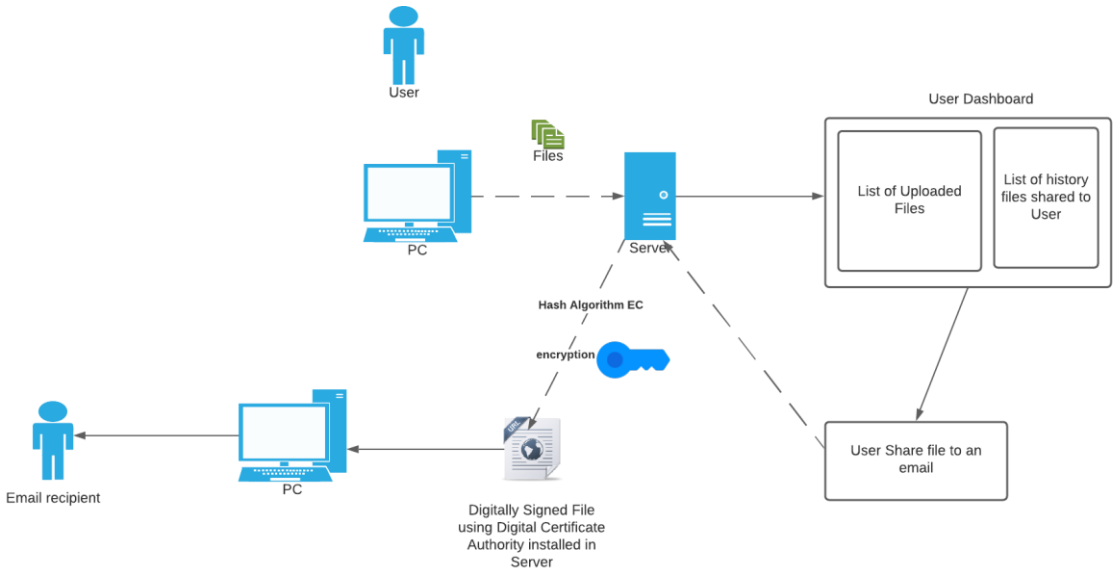
Πιο συγκεκριμένα η εφαρμογή με το που στέλνει ένα Generated Temporary URL σε κάποιο e-mail θα είναι ενεργό για 1 ώρα που θα έχει πρόσβαση το άτομο που έχει γίνει η διαμοίραση. Το αρχείο περνάει από τον Server το οποίο με τη χρήση του open_ssl μετατρέπεται με παράμετρο Elliptic Curve αλγορίθμου για να υπάρχει ασφάλεια κατά τη διαμοίραση του. Όταν ο παραλήπτης του διαμοιρασμένου αρχείου επιστρέψει στο Site που ανοίγει το αρχείο γίνεται έλεγχος αν συμβαδίζει με το πρωτότυπο αρχείο και αφού γίνει Verified μπορεί να δει και να κατεβάσει το αρχείο τοπικά στον Υπολογιστή του.

Η εργασία χωρίζεται σε πέντε κεφάλαια, Το πρώτο κεφάλαιο αφορά την ιστορική αναδρομή πίσω από το SSL. Το δεύτερο κεφάλαιο αναφέρονται κάποια από τα δημοφιλέστερα συστήματα διαχείρισης αρχείων με ψηφιακή υπογραφή, και στο τέλος του κεφαλαίου θα υπάρξει ένας αναλυτικός πίνακας σύγκρισης μεταξύ αυτών των εφαρμογών αλλά και της εφαρμογής που δημιουργήθηκε. Το τρίτο κεφάλαιο αναφέρει σχετικά για την κρυπτογραφία και SSL/TLS καθώς και υποστήριξη για την κρυπτογράφηση δεδομένων καθώς και μηχανισμούς για την ανταλλαγή των κλειδιών, αλλά και τα χαρακτηριστικά και που λαμβάνει χώρα στο Μοντέλο OSI. Επίσης, εμβαθύνουμε συγκεκριμένα για την κρυπτογραφία Ελλειπτικής καμπύλης (Elliptic Curve) και τα πλεονεκτήματα της. Στο τέταρτο κεφάλαιο αναλύουμε το σκοπό της υλοποίησης με Elliptic curve και την εφαρμογή της στην παρούσα εργασία, καθώς θα αναπαραστήσουμε και με σχήματα Use Case, Activity Diagram, Sequence Diagram και την εφαρμογή μας. Επίσης στις τελευταίες ενότητες του τέταρτου κεφαλαίου θα αναφερθούν και τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής. Στο τέλος του κεφαλαίου θα αναφέρουμε λίγα λόγια της PHP καθώς και τα πλεονεκτήματα χρήσης PHP Framework στην περίπτωση μας Laravel.

Στο πέμπτο κεφάλαιο θα μιλήσουμε για την υλοποίηση εφαρμογής, που θα αφορά τη δημιουργία κλειδιών στο Server, και θα γίνει η παρουσίαση της εφαρμογής.

Τέλος στο έκτο και τελευταίο κεφάλαιο παρουσιάζει τα τελικά συμπεράσματα αλλά και πιθανές μελλοντικές επεκτάσεις.

Παρακάτω γίνετε αναπαράσταση της αρχιτεκτονικής του συστήματος.



Σκοπός της παρούσας εργασίας είναι ναι μεν η διαμοίραση αρχείων μεταξύ χρηστών τόσο του συστήματος όσο και σε χρήστες που δεν είναι εγγεγραμμένοι στο σύστημα. Επίσης στη

περίπτωση που εγγραφτούν αργότερα και έχει γίνει νωρίτερα διαμοίραση αρχείων προς αυτούς να υπάρχει ένα ιστορικό από αρχεία που έχουν λάβει καθώς και την κατάσταση τους, αν δηλαδή τα Temporary URLs αυτών είναι ακόμα ενεργά ή ανενεργά. Ωστόσο όμως ο κύριος σκοπός της δεν είναι η απλή διαμοίραση αρχείων, αλλά και η ασφάλεια – κρυπτογράφηση αυτών για την αποφυγή λήψης από τρίτους και από κακόβουλους. Όπως αναφέρθηκε και στην περίληψη υπάρχουν διάφοροι τύποι κρυπτογραφήσεων, ωστόσο σκοπός μας ήταν να την κάνουμε με μεγαλύτερη ασφάλεια χρησιμοποιώντας Ελλειπτική Καμπύλη για κρυπτογράφηση.

Τα πλεονεκτήματα χρήσης Ελλειπτικής καμπύλης είναι η ασφάλεια των ψηφιακών υπογραφών, των αλγόριθμων ασφαλούς ανταλλαγής κλειδιών και τα κρυπτοσυστήματα δημόσιου κλειδιού μέσω ελλειπτικών καμπυλών βασίζονται στην δυσκολία εύρεσης του διακριτού λογάριθμου, που είναι εκτελέσιμος σε υποεκθετικό χρόνο. Συνεπώς μπορούν να επιλεχθούν αρκετά μικρότεροι παράμετροι για τα κρυπτοσυστήματα ελλειπτικών καμπυλών από ότι στα συνήθη κρυπτοσυστήματα διακριτού λογαρίθμου ή για το RSA, πετυχαίνοντας το ίδιο επίπεδο ασφάλειας. Μικρότερες παράμετροι μπορούν ενδεχομένως να οδηγήσουν σε σημαντικά οφέλη, ειδικά για υψηλότερα επίπεδα ασφάλειας. Στο κεφάλαιο 3.1 , 3.3, 3.4 αναγράφεται αναλυτικά για την ελλειπτική καμπύλη καθώς και τους αλγορίθμους δημιουργίας.

Κεφάλαιο 1. Ιστορική αναδρομή

Η Netscape Communications ανέπτυξε την αρχική έκδοση των πρωτοκόλλων SSL. Η έκδοση 1.0 δεν δημοσιεύτηκε ποτέ λόγω πολύ μεγάλων κενών ασφαλείας στο πρωτόκολλο. Η έκδοση 2.0 όμως, δημοσιεύτηκε τον Φεβρουάριο του 1995, και "περιείχε πληθώρα κενών ασφαλείας που εν τέλη οδήγησαν στον σχεδιασμό του SSL 3.0. Δημοσιευμένο το 1996, το SSLv3 ήταν το επανασχεδιασμένο πρωτόκολλο του μηχανικού Paul Kocher, ο οποίος δούλεψε μαζί με του μηχανικούς της Netscape Communications Phil Karlton και Alan Freier, και είχε μια πρότυπη υλοποίηση από τον Christopher Allen και τον Tim Dierks της Consensus Development. Οι νεότερες εκδόσεις του SSL/TLS είναι βασισμένες στο SSL v3.0. Το πρόχειρο προσδιοριστικό έγγραφο του 1996, δημοσιεύτηκε από το IETF σαν ιστορικό ντοκουμέντο στο RFC 6101.

Ο Δρ. Taher Elgamal, επικεφαλής επιστήμονας στην Netscape Communications από το 1995 μέχρι το 1998, είναι γνωστός ως ο "πατέρας του SSL".

Από το 2014, η έκδοση 3.0 του SSL δεν θεωρείται ασφαλής καθώς είναι ευπαθής στην επίθεση POODLE που επηρεάζει όλους τους Κρυπτογραφικούς Αλγόριθμους Δέσμης στο SSL, και το RC4, τον μόνο μη κρυπτογραφικό αλγόριθμο δέσμης που υποστηρίζει το SSL 3.0.

Το SSL 2.0 απαγορεύτηκε και θεωρήθηκε μη-ασφαλές το 2011, στο RFC 6176.

Το SSL 3.0 θεωρήθηκε μη-ασφαλές τον Ιούνιο του 2015, με το RFC 7568.

Κεφάλαιο 2. Δημοφιλή συστήματα διαχείρισης αρχείων με ψηφιακή υπογραφή

Σε αυτό το κεφάλαιο θα αναφερθεί μια λίστα από δημοφιλή συστήματα διαχείρισης αρχείων με ψηφιακή υπογραφή. Θα γίνει μια αναφορά σε αυτά τα συστήματα και στην συνέχεια θα υπάρξει μια ανάλυση για το καθένα. Πριν αναφερθούμε σε αυτά να αναφερθεί η γενική ιδέα αυτών των συστημάτων.

Το γενικό χαρακτηριστικό αυτών των εφαρμογών είναι η χρήση ψηφιακής υπογραφής ή γνωστή και ως ηλεκτρονική υπογραφή. Χρησιμοποιούν κρυπτογραφία για την προστασία εγγράφων και ενσωματώνουν λεπτομέρειες όπως τη διεύθυνση email, πότε και που υπογράφετε οποιοδήποτε έγγραφο και ποια συσκευή έγινε χρήση για να γίνει η διαδικασία της υπογραφής. Αυτό δημιουργεί το «δακτυλικό αποτύπωμα» που κάνει το έγγραφο μοναδικό και μπορεί να επαληθευτεί η αυθεντικότητα του. Αυτό το κάνει πολύ ασφαλές και αναγνωρίζεται νομικά παγκοσμίως.

Παρακάτω θα αναφερθούν τέσσερις εφαρμογές που χρησιμοποιούν ηλεκτρονική υπογραφή και είναι κάποιες από τις οποίες χρησιμοποιούν κάποιες επιχειρήσεις για την ασφάλεια που προσφέρουν. Αυτές είναι :

- DocuSign (για επιχειρήσεις που υπογράφουν πολλά έγγραφα)
- HelloSign (για ενσωμάτωση σε cloud Storage)
- PandaDoc (για τη συλλογή πληρωμών όταν υπογράφουν άτομα)
- SignNow (για μικρές ομάδες)

Στις παρακάτω ενότητες θα αναφερθούμε σε αυτές τις εφαρμογές / πλατφόρμες.

2.1 DocuSign

Το DocuSign είναι μια πλατφόρμα συμβολαίου, ηλεκτρονικής υπογραφής και λύσης πληρωμής από άκρο σε άκρο. Ωστόσο, η εστιασμένη πλατφόρμα ψηφιακής υπογραφής της, που ονομάζεται eSignature, μπορεί να αγοραστεί ως αυτόνομο προϊόν. Μπορείτε να εισαγάγετε έγγραφα, να μετατρέψετε αρχεία, να στείλετε μαζικές συμφωνίες, ακόμη και να διαχειριστείτε ροές υπογραφών με διάφορους τρόπους.

Το εξειδικευμένο λογισμικό περιλαμβάνει άλλες δυνατότητες όπως:

- Μετατροπές αρχείων
- Ενσωμάτωση στο cloud storage
- Αυτόματες ετικέτες
- Υπογραφή κινητής τηλεφωνίας
- Δρομολόγηση υπογραφής

- Μαζική αποστολή
- Υπενθυμίσεις
- Παρακολούθηση σε πραγματικό χρόνο
- Ενσωμάτωση τρίτων εφαρμογών
- Υπογραφή κινητής τηλεφωνίας

Το λογισμικό περιλαμβάνει διάφορα μέτρα ελέγχου ταυτότητας, από κλειδιά που βασίζονται σε email έως τηλέφωνο και έλεγχο ταυτότητας Federated Identity. Μπορείτε επίσης να λάβετε πολλά πρόσθετα, όπως επεξεργασία πληρωμών, αναλυτικά στοιχεία βάσει τεχνητής νοημοσύνης και συγκέντρωση εγγράφων.

2.2 HelloSign

Το HelloSign είναι ένα διαδικτυακό εργαλείο που επιτρέπει στους χρήστες να ανεβάζουν έγγραφα και να ζητούν νομικά δεσμευτικές ηλεκτρονικές υπογραφές. Διαθέτει ένα απλό, εύχρηστο εργαλείο μεταφοράς και απόθεσης, που σας επιτρέπει να προσαρμόσετε τις φόρμες και τα πρότυπά σας. Μπορείτε να εισαγάγετε τα αρχεία σας από σχεδόν οποιοδήποτε σύστημα, συμπεριλαμβανομένων των DropBox και του Google Drive, ή να ενσωματώσετε το λογισμικό με τις προϋπάρχουσες εφαρμογές και το περιβάλλον σας.

Παρόλο που είναι μια πιο απλή, εστιασμένη πλατφόρμα ψηφιακής υπογραφής, το HelloSign προσφέρει επίσης πολλές επιπλέον δυνατότητες:

- Εργαλεία διαχείρισης ομάδας
- Προσαρμόσιμα πρότυπα
- Επιλογές επωνυμίας
- Ενσωμάτωση API
- Ευέλικτες ροές εργασίας
- Συμβατότητα με κινητά
- Ειδοποιήσεις
- Κρυπτογράφηση και ασφάλεια
- Διαδρομές ελέγχου

Επιπλέον, η πλατφόρμα υποστηρίζει 17 τύπους αρχείων, έλεγχο ταυτότητας δύο παραγόντων και κρυπτογράφηση σε επίπεδο τράπεζας. Ενώ ορισμένες από τις δυνατότητες συμμόρφωσης και ασφάλειας περιορίζονται σε προγράμματα πληρωμένων υψηλότερου επιπέδου, όλες οι συνδρομές περιλαμβάνουν ίχνη ελέγχου και επικύρωση δεδομένων.

2.3 PandaDoc

Το PandaDoc ενώ περιλαμβάνει ηλεκτρονικές υπογραφές στην προσφορά του, αυτό είναι ένα μέρος του τι είναι ικανό να κάνει σαν σύστημα. Περιλαμβάνει πολλές πρόσθετες υπηρεσίες όπως δημιουργία προσφορών, κοινή χρήση εγγράφων, διαχείριση συμβολαίων και υποστήριξη πληρωμής. Ενσωματώνεται επίσης με λογιστικές και CRM πλατφόρμες, καθιστώντας την μία από τις καλύτερες επιλογές λογισμικού ψηφιακής υπογραφής για επιχειρήσεις που χρειάζονται μια ολοκληρωμένη λύση.

Μερικά από τα κορυφαία χαρακτηριστικά του περιλαμβάνουν:

- Ασφαλής κρυπτογράφηση
- Αυθεντικοποίηση
- Παρακολούθηση διαδικασίας
- Διαδρομές ελέγχου
- Διαχείριση αρχείων
- Συμβατότητα με κινητά
- Ενσωμάτωση Τρίτων Εφαρμογών
- Ενεργές πληροφορίες

Το PandaDoc περιλαμβάνει ισχυρά αναλυτικά στοιχεία και αναφορές. Είναι ικανό να στέλνει ειδοποίηση όταν κάποιος ανοίξει το έγγραφο σας, πόσο καιρό το βλέπει, αν προσθέσει σχόλια κ.α. Επιπλέον, το σύστημα ενημερώνει εάν ο πελάτης υπογράψει μια συμφωνία, φροντίζοντας να μη ξεχάσει καμία συμφωνία.

2.4 signNow

Με το signNow βελτιώνονται οι διαδικασίες. Θεωρείτε μία από τις καλύτερες πλατφόρμες λογισμικού ψηφιακής υπογραφής. Το σύστημα επιτρέπει να στείλει κάποιος ή και να ζητήσει έγγραφα και συμβόλαια, επιτρέποντας στους πελάτες να τα υπογράφουν ηλεκτρονικά. Όλες οι ηλεκτρονικές υπογραφές είναι πιστοποιημένες και νομικά δεσμευμένες.

Το λογισμικό βρίσκεται στο cloud, αλλά διαθέτει επίσης εφαρμογές για Android και iOS, ώστε να μπορεί κάποιος να στέλνει συμβόλαια σε πελάτες για υπογραφή με τα smartphones. Άλλα χαρακτηριστικά είναι:

- Ομαδική συνεργασία
- Πρότυπα επωνυμίας
- Προσαρμοσμένες παραγγελίες υπογραφής
- Ενσωμάτωση τρίτων εφαρμογών
- Ασφάλεια εγγράφων
- Έλεγχος ταυτότητας υπογραφής
- Κινητές εφαρμογές

Το signNow έχει αρκετές επιπλέον δυνατότητες που συνοδεύουν το airSlate Business Cloud. Οι λειτουργίες περιλαμβάνουν αυτοματοποίηση διεργασιών, λογισμικό e-signature εταιρικού επιπέδου, πληρωμές, διαχείριση συμβολαίων και διαπραγματεύσεις και ενσωμάτωση φόρμας ιστού.

2.5 Αναλυτική σύγκριση Εφαρμογών με ψηφιακή υπογραφή

Οι παρακάτω συγκρίσεις προήλθαν από την ιστοσελίδα:

	DocuSign	*HelloSign*	*PandaDoc*	*SignNow*	*My Application*
Notify Sender if file / Url Opened					✓
Temporary URL of shared File for specific time					✓
Platforms supported					
Web-based	✓	✓	✓	✓	✓
iPhone app	✓			✓	
Android app	✓	✓	✓	✓	
Typical customers					
Freelancers	✓	✓	✓	✓	✓
Small businesses	✓	✓	✓	✓	
Mid size businesses	✓	✓	✓	✓	
Large enterprises	✓	✓	✓	✓	
Total features					
API	✓	✓	✓	✓	
Access Controls/Permissions		✓	✓	✓	
Activity Dashboard			✓	✓	✓
Alerts/Notifications			✓	✓	✓
Audit Management			✓	✓	
Audit Trail	✓	✓	✓	✓	
Authentication	✓	✓	✓	✓	✓
CRM			✓	✓	
Configurable Workflow	✓		✓	✓	
Customizable Branding	✓	✓		✓	
Customizable Fields	✓		✓	✓	

Customizable Forms	✓		✓	✓	
Customizable Templates	✓	✓	✓	✓	
Data Security		✓	✓	✓	✓
Digital Signature	✓		✓		✓
Document Analytics	✓	✓	✓	✓	
Document Automation			✓	✓	✓
Document Management	✓		✓	✓	
Document Review	✓		✓		✓
Document Storage	✓	✓	✓	✓	
Document Templates			✓	✓	
Drag & Drop			✓	✓	
Electronic Signature	✓	✓	✓	✓	
File Sharing		✓	✓	✓	✓
Forms Management			✓	✓	
HIPAA Compliant			✓	✓	
Mobile Access	✓		✓		
Mobile Signature Capture	✓	✓	✓	✓	
Multi-Party Signing	✓	✓	✓	✓	
Progress Tracking			✓	✓	✓
Projections	✓		✓		
Reminders	✓	✓	✓	✓	
Single Sign On			✓	✓	
Task Progress Tracking	✓	✓	✓	✓	
Team Collaboration		✓	✓	✓	
Template Management	✓		✓	✓	
Workflow Management	✓		✓	✓	
Integrations					
Dropbox Business	✓	✓	✓	✓	
Google Drive	✓	✓	✓	✓	
Magento Commerce				✓	
Microsoft 365				✓	
NetSuite	✓			✓	
PayPal			✓		
Salesforce Sales Cloud		✓	✓	✓	
Slack		✓	✓		
Stripe	✓		✓		
Xero			✓		
Zapier			✓	✓	
Security					
Encryption of sensitive data at rest	?	?	?	✓	
HTTPS for all pages (web-based apps)	?	✓	?	✓	
Reports/alerts for security breaches	?	✓	?	✓	
Multifactor authentication options	?	✓	?	✓	
Customer data removed upon service cancellation	?	✓	?	?	
ECDSA	?	?	?	?	✓

Κεφάλαιο 3. Κρυπτογραφία και SSL / TLS

Το SSL/TLS είναι ένα υβριδικό πρωτόκολλο. Χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού για την αυθεντικοποίηση και την δημιουργία των κλειδιών ενώ για να εγγυηθεί την εμπιστευτικότητα του κύριου όγκου της μεταδιδόμενης πληροφορίας χρησιμοποιεί συμμετρικούς αλγορίθμους.

Για την ακεραιότητα των μηνυμάτων χρησιμοποιούνται κώδικες MAC (Message Authentication Code).

Για την κρυπτογράφηση των δεδομένων υποστηρίζονταν οι παρακάτω:

- DES
- 3DES
- DES 40
- IDEA
- RC2 40
- RC4 128
- RC4 40
- Fortezza

Οι εκδόσεις του TLS επεκτείνουν την συμβατότητα του πρωτοκόλλου με αρκετούς ακόμη αλγορίθμους, πιο σύγχρονους και ασφαλείς (π.χ. AES, Camellia, SEED).

Για τα MAC που χρησιμοποιούνται στο πρωτόκολλο είχε επιλεγεί η χρήση SHA-256

Τέλος, ενημερωτικά αναφέρεται ότι για την ανταλλαγή των κλειδιών υποστηρίζονται διάφοροι μηχανισμοί όπως:

- DHE_DSS
- DHE_RSA
- DH_DSS
- DH_RSA
- RSA
- RSA_SHA

Αξίζει να σημειωθεί ότι για όλα τα παραπάνω μπορεί το SSL/TLS να ρυθμιστεί ώστε να χρησιμοποιεί τις αντίστοιχες “EXPORT” εκδόσεις που είναι λιγότερο ασφαλείς (κλειδιά περιορισμένου μήκους bits) ώστε να πληρεί τους παλαιότερους αυστηρούς νόμους περί εξαγωγής κρυπτογραφίας από τις ΗΠΑ σε τρίτες χώρες.

3.1 Κρυπτογραφία Elliptic Curve

Ο αλγόριθμος ψηφιακής υπογραφής Elliptic Curve ή αλλιώς ECDSA είναι ένας κρυπτογραφικός αλγόριθμος που χρησιμοποιείτε κυρίως από το Bitcoin και από κρυπτονομίσματα για να διασφαλίσει ότι τα χρήματα μπορούν να δαπανηθούν μόνο από τους νόμιμους κατόχους τους.

Το Elliptic curve έχει διάφορες παραμέτρους κρυπτογράφησης και κάποιες από τις ποιο γνωστές είναι το :

- Secp256k1
- c2pnb272w1
- c2tnb359v1
- prime256v1
- c2pnb304w1
- c2pnb368w1
- c2tnb431r1
- sect283r1
- sect283k1
- secp256r1
- sect571r1
- sect571k1
- sect409r1
- sect409k1
- secp521r1
- secp384r1
- P-256
- P-384
- b-409
- b-283
- k-409
- k-283
- k-571
- brainpoolp512r1
- brainpoolp384t1
- brainpoolp256r1
- brainpoolp512t1
- brainpoolp256t1
- brainpoolp320r1
- brainpoolp384r1
- brainpoolp320t1
- FRP256v1

- P-521
- sm2p256v

Το secp256k1 αναφέρεται στις παραμέτρους του Elliptic Curve που χρησιμοποιείται στην κρυπτογράφηση δημόσιου κλειδιού του Bitcoin και ορίζεται στα Πρότυπα για αποτελεσματική κρυπτογραφία (SEC)

Μερικές έννοιες που σχετίζονται με το ECDSA:

- **ιδιωτικό κλειδί:** Ένας μυστικός αριθμός, γνωστός μόνο στο άτομο που το δημιούργησε. Ένα ιδιωτικό κλειδί είναι ουσιαστικά ένας τυχαία αριθμός. Στο Bitcoin, ένα ιδιωτικό κλειδί είναι ένας ακέραιος 256 bit χωρίς υπογραφή (32 bytes).
- **δημόσιο κλειδί:** Ένας αριθμός που αντιστοιχεί σε ένα ιδιωτικό κλειδί, αλλά δεν χρειάζεται να παραμείνει μυστικός. Ένα δημόσιο κλειδί μπορεί να υπολογιστεί από ένα ιδιωτικό κλειδί, αλλά όχι το αντίστροφο. Ένα δημόσιο κλειδί μπορεί να χρησιμοποιηθεί για να προσδιορίσει εάν μια υπογραφή είναι γνήσια (με άλλα λόγια, που παράγεται με το κατάλληλο κλειδί) χωρίς να απαιτείται η αποκάλυψη του ιδιωτικού κλειδιού.
- **υπογραφή**: Ένας αριθμός που αποδεικνύει ότι πραγματοποιήθηκε μια λειτουργία υπογραφής.

3.2 OpenSSL

Το OpenSSL είναι μια βιβλιοθήκη κρυπτογράφησης για την υλοποίηση των πρωτοκόλλων SSL (Secure Sockets Layer) και TLS (Transport Layer Security). Το πρόγραμμα openssl χρησιμοποιεί συναρτήσεις της βιβλιοθήκης OpenSSL για τη δημιουργία κλειδιών τόσο συμμετρικής όσο και ασύμμετρης κρυπτογράφησης, για την υλοποίηση διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης καθώς και για τις διαδικασίες υπογραφής και επαλήθευσης.

Γενική μορφή σύνταξης:

openssl command <command_options> <command_args>

3.3 Κλειδί και μέγεθος υπογραφής

Όπως με την κρυπτογραφία ελλειπτικής καμπύλης (Elliptic Curve) γενικά, το μέγεθος bit του δημόσιου κλειδιού που απαιτείται για το ECDSA είναι περίπου το διπλάσιο μέγεθος του επιπέδου ασφαλείας σε bits. Για παράδειγμα, σε επίπεδο ασφαλείας 80-bit (που σημαίνει ότι ένας εισβολέας απαιτεί έως και περίπου 2^{80} λειτουργίες για την εύρεση του ιδιωτικού κλειδιού), το μέγεθος ενός ιδιωτικού κλειδιού ECDSA θα είναι 160 bits, ενώ το μέγεθος του ιδιωτικού κλειδιού DSA είναι τουλάχιστον 1024 bit.

Από την άλλη, το μέγεθος της υπογραφής είναι το ίδιο και για τα DSA και για το ECDSA: περίπου 4t bits όπου t είναι το επίπεδο ασφάλειας που μετράτε σε bits, δηλαδή περίπου 320 bit για μια ασφάλεια επιπέδου 80 bit.

3.4 Αλγόριθμος δημιουργίας υπογραφών

Ας υποθέσουμε ότι κάποιος θέλει να στείλει ένα υπογεγραμμένο μήνυμα σε κάποιον. Αρχικά, πρέπει να συμφωνήσουν για τις παραμέτρους της καμπύλης (CURVE, G, n). Επιπρόσθετα, εκτός από το πεδίο και την εξίσωση της καμπύλης χρειαζόμαστε το G, ένα βασικό σημείο πρώτης τάξης στην καμπύλη. n είναι η πολλαπλασιαστική σειρά του σημείου G.

Παρακάτω ακολουθεί ένας πίνακας με παραμέτρους και επεξηγήσεις.

Parameter	
CURVE	το ελλειπτικό πεδίο καμπύλης και την εξίσωση που χρησιμοποιούνται

G	ελλειπτικό σημείο βάσης καμπύλης, ένα σημείο στην καμπύλη που δημιουργεί μια υποομάδα μεγάλης πρώτης τάξης n
n	Ακέραια σειρά του G, σημαίνει ότι n X G = O, όπου O είναι το στοιχείο ταυτότητας
d_A	ιδιωτικό κλειδί (επιλέγεται τυχαία)
Q_A	δημόσιο κλειδί (υπολογίζεται με ελλειπτική καμπύλη)
m	μήνυμα για αποστολή

Η σειρά n, του σημείου βάσης G, πρέπει να είναι πρωταρχική. Πράγματι υποθέτουμε ότι κάθε μη μηδενικό στοιχείο του δακτυλίου Z/nZ είναι αναστρέψιμο, έτσι ώστε Z/nZ πρέπει να είναι το πεδίο. Αυτό σημαίνει ότι το n πρέπει να είναι πρωταρχικό.

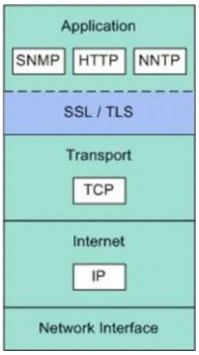
Ο πρώτος δημιουργεί ένα ζεύγος κλειδιών, που αποτελείται από έναν ακέραιο αριθμό ιδιωτικού κλειδιού d_A , όπου επιλέγεται τυχαία στο διάστημα [l,n – 1], και ένα σημείο καμπύλης δημόσιου κλειδιού $Q_A = d_A$ X G. Χρησιμοποιούμε το X για να υποδηλώσουμε τον ελλειπτικό πολλαπλασιασμό σημείων καμπύλης με μια βαθμίδα.

Για να υπογράψει ο πρώτος ένα μήνυμα m, ακολουθεί τα παρακάτω βήματα:

- Υπολογίζει e = HASH(m). (Το Hash είναι μια κρυπτογραφική συνάρτηση, όπως για παράδειγμα SHA-2, με έξοδο να μετατρέπεται σε ακέραιο).
- Το z είναι το L_n , αριστερότερα bits του e, είναι το μήκος bit της ομάδας προτεραιότητας n. (Σημείωση ότι το z μπορεί ναι είναι μεγαλύτερο από το n αλλά όχι μεγαλύτερο σε μήκος.
- Επιλέγει έναν κρυπτογραφικά ασφαλή τυχαίο ακέραιο k από [l, n – 1].
- Υπολογίζει το σημείο καμπύλης (x1,y1) = k X G.
- Υπολογίζει r = x1 mod n. Αν r = 0, επιστρέφει στο 3ο βήμα.
- Υπολογίζει $s = k^{-1} (z + rd_A) \bmod n$, αν το s = 0 επιστρέφει στο 3ο βήμα.
- Η υπογραφή είναι ζευγάρι (r,s). Και (r, -s mod n) είναι επίσης ένα έγκυρο ζευγάρι.

3.5 Χαρακτηριστικά – Μοντέλο OSI

Το SSL/TLS λειτουργεί επάνω από το επίπεδο Μεταφοράς (Transport Layer – Επίπεδο 5 στο μοντέλο OSI). Παρακάτω στο σχήμα φαίνεται η αντίστοιχη θέση στο μοντέλο TCP/IP.

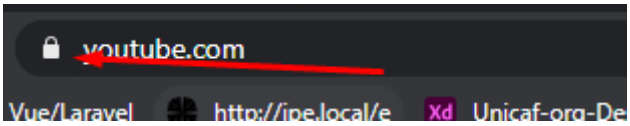


Εικόνα 1 Transport Layer of OSI Model

Από τα κατώτερα στρώματα απαιτεί συνήθως αξιόπιστη σύνδεση (π.χ. TCP,DTLS), παρόλο που υπάρχουν και υλοποιήσεις με χρήση UDP, ενώ δεν θέτει περιορισμό στα ανώτερα στρώματα.

Λόγω της θέσης του, το SSL μπορεί να αξιοποιηθεί από ένα πλήθος εφαρμογών με αόρατο στον χρήστη τρόπο. Χαρακτηριστικά παραδείγματα τέτοιων εφαρμογών είναι τα: HTTP, FTP, Telnet, VPNs κ.α.

Στο επόμενο σχήμα φαίνεται ένα παράδειγμα ασφαλούς επικοινωνίας HTTP με χρήση του SSL. Στο URL η διεύθυνση ξεκινάει με “https” αντί του τυπικού “http”. Και συνήθως στα αριστερά του URL Bar δείχνει ένα Λουκέτο ή το όνομα του Certification.



Εικόνα 2 Ασφαλής επικοινωνία HTTPS με χρήση SSL

Κεφάλαιο 4. Εφαρμογή υλοποίησης Ελλειπτικής καμπύλης

Σύμφωνα με τις προδιαγραφές της παρούσας εργασίας, θα υλοποιηθεί μια εφαρμογή (διαδικτυακή), η οποία θα επέτρεπε σε κάποιον να ανεβάζει στον Server αρχεία , είτε εικόνες είτε pdf. Ο χρήστης μετά την εγγραφή του στη πλατφόρμα θα έχει ένα διαχειριστικό για το ανέβασμα αρχείων καθώς και να τα βάλει σε λίστα διαγραμμένων. Από εκεί έχει την επιλογή την μόνιμη διαγραφή του αρχείου ή την επαναφορά αυτού. Στην οθόνη του διαχειριστικού που δείχνει όλα τα ανεβασμένα αρχεία του χρήστη έχει στα δεξιά ένα πάνελ που του επιτρέπει να βλέπει αν του έχουν διαμοιραστεί αρχεία από κάποιον άλλον χρήστη, με δικαίωμα να τα κατεβάσει, αλλά για περιορισμένο χρονικό όριο (1 ώρας). Στην περίπτωση που έχει περάσει 1 ώρα από την διαμοίραση του αρχείου, αναγράφεται ότι έχει λήξει και δεν ισχύει το url για το αρχείο καθώς και αν το πατήσει θα τον ανακατευθύνει σε μια σελίδα που δεν του επιτρέπει να το δει. Ο χρήστης από την άλλη στην σελίδα διαχειριστικού που βλέπει όλα τα αρχεία που έχει ανεβάσει, έχει το δικαίωμα σε κάθε αρχείο να βάλει, σε ένα πεδίο δίπλα από το αρχείο, το e-mail κάποιου φίλου που θέλει να το διαμοιράσει και να πατήσει το κουμπί share. Σε αυτήν τη περίπτωση στέλνετε ένα e-mail, στον χρήστη που έχει το e-mail (είτε είναι εγγεγραμμένος στο σύστημα , είτε όχι) και έχει το δικαίωμα από το e-mail να πατήσει πάνω στο λινκ του αρχείου που του έχει διαμοιραστεί). Στην περίπτωση που ο χρήστης πατήσει αυτόν τον σύνδεσμο από το email του, στέλνεται αναφορά στον πρώτο ότι το αρχείο έχει ανοιχθεί. Επίσης αν κάποιος δεν έχει λογαριασμό στην πλατφόρμα αλλά του έχουν διαμοιραστεί αρχεία στο e-mail του, ανά πάσα ώρα και στιγμή αποφασίσει να φτιάξει λογαριασμό, θα έχει ένα ιστορικό στο δεξί πάνελ με τα αρχεία που του έχουν διαμοιραστεί ακόμα και πριν δημιουργήσει τον λογαριασμό του.

Όλη όμως η ασφάλεια και η πιστοποίηση γίνεται με το που ένας χρήστης βάλει στο πεδίο κάποιο e-mail και πατήσει Share file. Με το που πατηθεί το κουμπί περνάει το αρχείο από τον Server και το Certificate του, δημιουργεί κλειδί για το συγκεκριμένο αρχείο σε base64 και αποθηκεύετε το αρχείο κρυπτογραφημένο σε αρχείο με το όνομα του αρχείου (πριν την κρυπτογράφηση) και με κατάληξη 64. Με το που ανοίξει ο χρήστης το αρχείο τότε περνάει από τον Server, γίνεται αντιστοίχιση των κλειδιών και της κρυπτογραφίας και αν είναι έγκυρο ανοίγεται το αρχικό αρχείο (σε περίπτωση που είναι εικόνα). Σε περίπτωση που είναι PDF το αρχείο γίνεται Self – Signed και ακόμα και να το κατεβάσει τοπικά ο χρήστης μπορεί να δει την υπογραφή και τον Server που το έχει λάβει μαζί με το certification.

Παρακάτω θα αναλυθεί σε ενότητες όλο το Flow της εφαρμογής καθώς θα υπάρχουν και Use Case, Activity και Sequence Diagram, αλλά και η εγκατάσταση της εφαρμογής σε κάποιον Server, οι τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση της εφαρμογής και εικόνες με επεξηγήσεις και τα βήματα όλης της εφαρμογής.

4.1 Use Case Diagram

Στα παρακάτω διαγράμματα που έχουν υλοποιηθεί με την χρήση Use Case βλέπουμε τρεις καταστάσεις. Στην πρώτη είναι ο επισκέπτης που έχει την επιλογή να κάνει σύνδεση ή εγγραφή

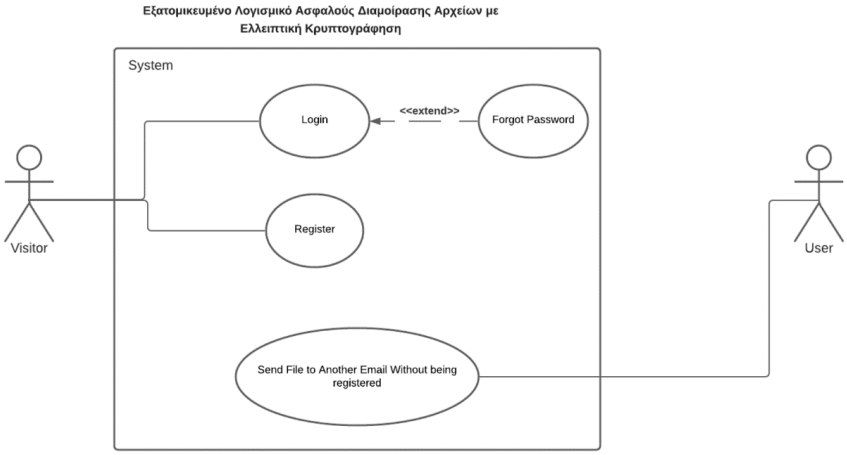
ή να λάβει το αρχείο που του έχει στείλει κάποιος άλλος χρήστης χωρίς απαραίτητα να είναι εγγεγραμμένος. Επίσης έχει την επιλογή από την σύνδεση χρήστη να ανακτήσει τον κωδικό του σε περίπτωση που τον έχει ξεχάσει. Στο δεύτερο στάδιο βλέπουμε τον χρήστη του συστήματος και τις επιλογές που έχει προς αυτό. Μέσα από το διαχειριστικό μπορεί να δει τη λίστα αρχείων του καθώς και τα διαμοιρασμένα αρχεία (το ιστορικό) που του έχει στείλει άλλος χρήστης καθώς και την κατάσταση τους αν είναι ενεργά ή όχι. Στη λίστα αρχείων του μπορεί να κάνει διαμοίραση του αρχείου του καθώς δημιουργείτε ένας προσωρινός σύνδεσμος και στέλνετε με την εισαγωγή στο πεδίο το email και πατώντας το κουμπί share. Άλλη επιλογή είναι να βάλει τα αρχεία στον κάδο (προσωρινή διαγραφή). Στην πρώτη περίπτωση της διαμοίρασης Ο Server παίρνει το αρχείο και το κάνει Self Sign με το αρχείο του Certificate.

Άλλες επιλογές του χρήστη είναι η προβολή των αρχείων που βρίσκονται στον κάδο και από εκεί έχει την επιλογή επαναφοράς ή την μόνιμη διαγραφή τους.

Τέλος έχει την επιλογή να ανεβάσει ένα νέο αρχείο στο διαχειριστικό του.

Στο τελευταίο σχέδιο γίνεται μια αναπαράσταση που όταν ο παραλήπτης του διαμοιρασμένου αρχείου πατήσει το προσωρινό σύνδεσμο τότε ο πρώτος, δηλαδή αυτός που είχε διαμοιράσει εξ αρχής το αρχείο, λαμβάνει Ειδοποιήσεις μέσω email ότι ο χρήστης με το ανάλογο email έχει ανοίξει το αρχείο του που είχε αποσταλεί σε αυτόν.

Σύμφωνα με τις περιπτώσεις χρήσης που ακολουθούν της εφαρμογής θα αναφέρουμε την συστηματική περιγραφή τους:



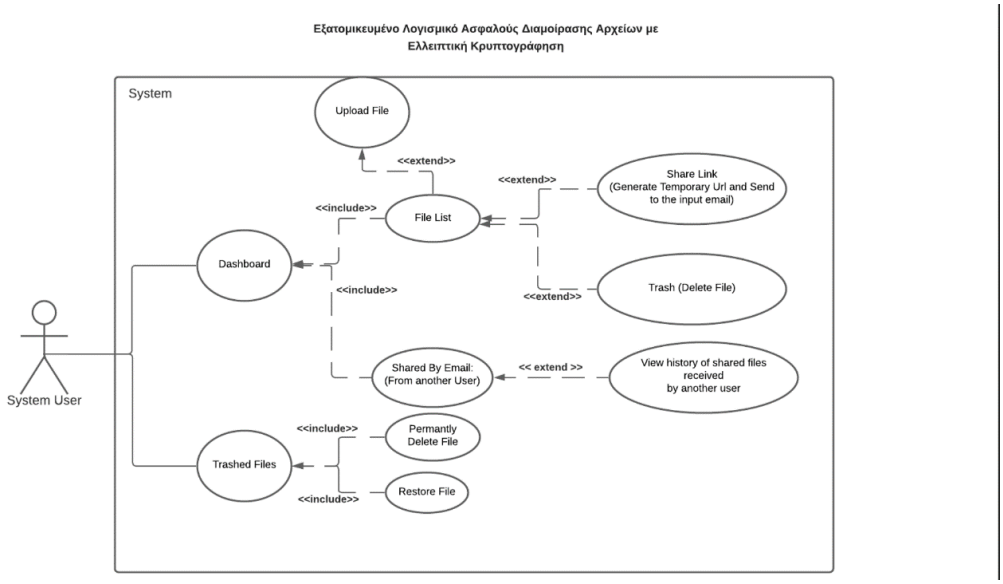
Εικόνα 4 Use Case Diagram Εφαρμογής – Σύστημα Χρηστών

Πρωτεύον μονοπάτι:

1. Ο επισκέπτης κάνει σύνδεση ή εγγραφή στο σύστημα. Σε περίπτωση που έχει ξεχάσει τον κωδικό του έχει την επιλογή για ανάκτηση του.
2. Με την επιτυχή σύνδεση ή εγγραφή του επισκέπτη, πλέον σαν χρήστης συνδέετε στο διαχειριστικό του σύστημα της εφαρμογής.
3. Η περίπτωση χρήσης τελειώνει με επιτυχία

Εναλλακτικά μονοπάτια:

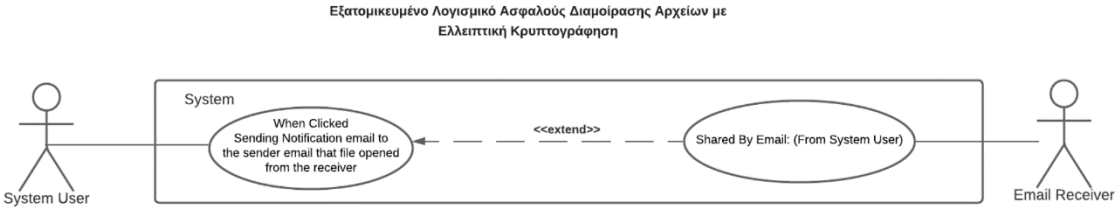
1. **Αποτυχία σύνδεσης στο σύστημα**
   a. Ο επισκέπτης προσπαθεί να κάνει σύνδεση με αποτυχημένα στοιχεία σύνδεσης.
   b. Τον επιστρέφει στη σελίδα σύνδεσης με μηνύματα σφάλματος.
   c. Η περίπτωση χρήσης τελειώνει με αποτυχία



Εικόνα 5 Use Case Diagram Εφαρμογής – Δυνατότητες χρήστη στο Σύστημα

Πρωτεύον μονοπάτι:

1. Με την επιτυχή σύνδεση ή εγγραφή του, πλέον σαν χρήστης ανακατευθύνεται στο διαχειριστικό του, όπου μπορεί να δει τα μεταφορτωμένα αρχεία του, καθώς και το ιστορικό των αρχείων που έχουν γίνει διαμοίραση προς αυτόν.
2. Από την Λίστα αρχείων έχει την επιλογή να κάνει Share Link σε ένα e-mail που εισάγει σε πεδίο και να γίνει η διαμοίραση του στέλνοντας e-mail. Επίσης έχει την επιλογή να κάνει Delete το αρχείο που θα το πάει στα Trashed Files.
3. Επίσης υπάρχει η επιλογή Upload File που με την επιτυχημένη μεταφόρτωση του θα το δείχνει στο File List.
4. Από την άλλη έχει την επιλογή ο χρήστης να δει τα Trashed Files. Σε αυτήν την σελίδα μπορεί είτε να διαγράψει μόνιμα το αρχείο είτε να κάνει Restore το αρχείο.
5. Η περίπτωση χρήσης τελειώνει με επιτυχία.



Εικόνα 6 Use Case Diagram Εφαρμογής – Ενημέρωση Χρήστη μέσω email όταν κάποιος τρίτος ανοίγει το αρχείο

Πρωτεύον μονοπάτι:

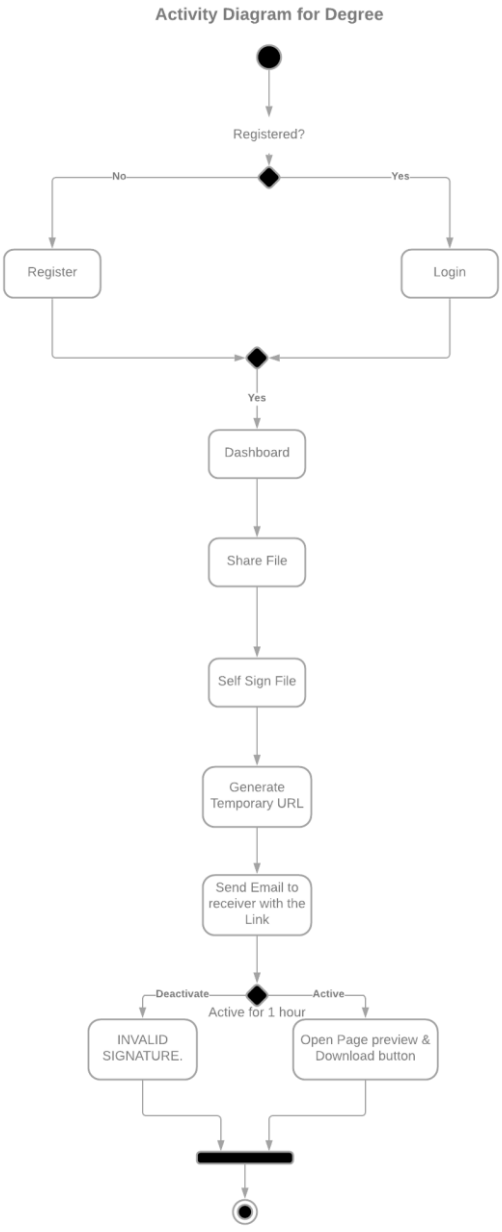
1. Ο επισκέπτης – χρήστης που έλαβε e-mail από διαμοιρασμένο αρχείο από χρήστη του συστήματος λαμβάνει ένα Temporary URL.
2. Το σύστημα στέλνει μήνυμα στον χρήστη που αρχικά είχε διαμοιράσει αυτό το αρχείο e-mail με το email που άνοιξε τον σύνδεσμο.
3. Η περίπτωση χρήσης τελειώνει με επιτυχία

Εναλλακτικά μονοπάτια:

1. **Ο προσωρινός σύνδεσμος έχει λήξει (1 ώρας)**
   a. Ο χρήστης που έχει λάβει ένα διαμοιρασμένο αρχείο και έχει περάσει η μία ώρα από την ώρα διαμοίρασης του, αν πατήσει τον σύνδεσμο επιστρέφει στο σύστημα σε μια σελίδα 403 – Invalid Signature.
   b. Η περίπτωση χρήσης τελειώνει με αποτυχία.

4.2 Activity Diagram

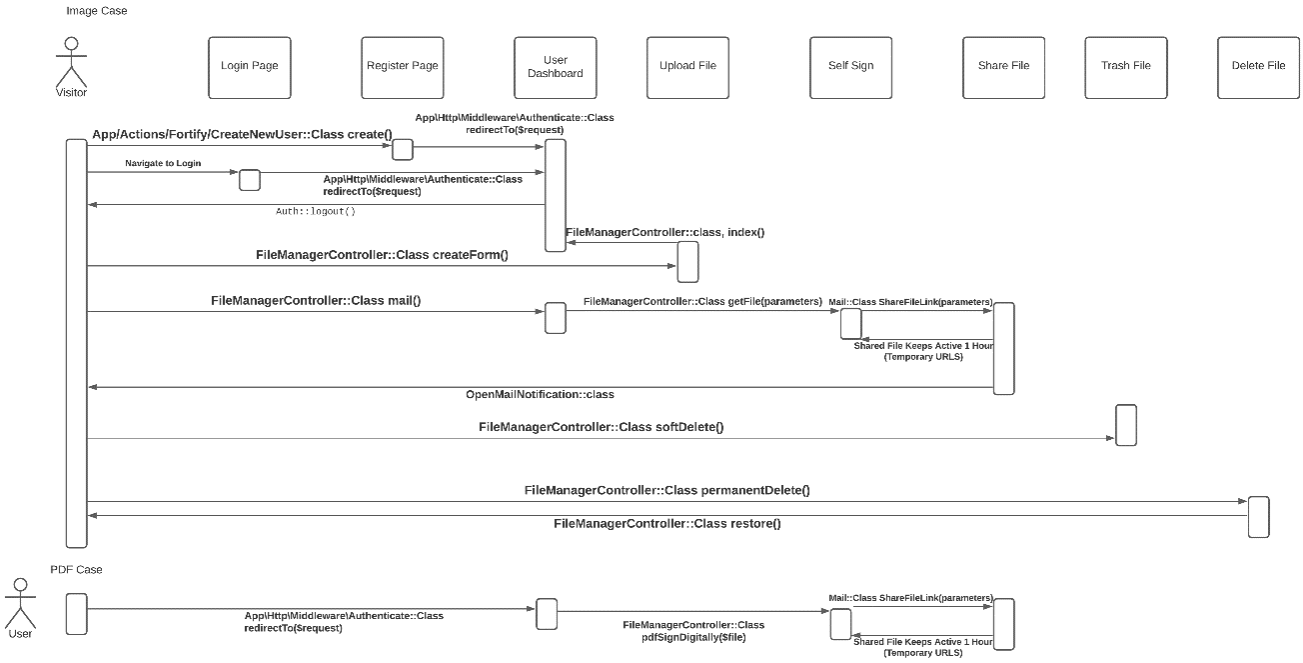
Όπως βλέπουμε παρακάτω στην εικόνα είναι το Activity Diagram της εφαρμογής. Ουσιαστικά αναπαριστά την διαδικασία που ακολουθεί η εφαρμογή. Με το που κάποιος επισκεφτεί την εφαρμογή θα πρέπει να κάνει σύνδεση χρήστη. Αν δεν έχει λογαριασμό πρέπει να κάνει εγγραφή για νέο χρήστη. Σε κάθε περίπτωση μετά την επιτυχή εγγραφή ή σύνδεση του θα μεταφερθεί στο διαχειριστικό του. Από το διαχειριστικό μπορεί να κάνει διαμοίραση του αρχείου που έχει ήδη ανεβάσει σε ένα άλλο e-mail. Με το που γίνει ο διαμοιρασμός του αρχείου γίνεται Digitally Signed το αρχείο με χρήση Digital Certificate Authority, γίνετε η δημιουργία ενός προσωρινού συνδέσμου με ζωή μίας ώρας και στέλνεται αυτός ο σύνδεσμος στο email που είχε μπει πριν δύο βήματα. Ο παραλήπτης λαμβάνει το e-mail με το προσωρινό σύνδεσμο και έχει μία ώρα για να μπορεί να επισκεφτεί το αρχείο. Αν είναι ανενεργό τον οδηγεί σε σελίδα που του βγάζει μήνυμα Invalid Signature ή αν είναι ενεργός ο σύνδεσμος τον οδηγεί σε σελίδα με preview του αρχείου και ένα κουμπί για λήψη καθώς του δείχνει και το TXT Certification Key που έχει γίνει Verified από τον Server σε μορφή base64().



Εικόνα 7 Activity Diagram Εφαρμογής

4.3 Sequence Diagram

Στο σχήμα βλέπουμε όλη τη διαδικασία. Ο Visitor αρχικά πρέπει να φτιάξει ένα account. Οπότε πλοηγείτε στο Registration Page. Στη συνέχει βάζει τα στοιχεία του όπως Όνομα, Email, και τον κωδικό του με επαλήθευση. Αφού κάνει επιτυχή εγγραφή γίνεται χρήστης και ανακατευθύνετε στο User Dashboard του. Από το User Dashboard ο χρήστης (πλέον) μπορεί να ανεβάσει αρχείο. Με το που το ανεβάσει το βλέπει σε μια λίστα στο αριστερό Panel στην αρχική του Dashboard ανεβασμένο. Από εκεί μπορεί να κάνει το αρχείο share βάζοντας σε ένα πεδίο το e-mail που θέλει να το στείλει. Με το που πατήσει το κουμπί Share, ο Server αναλαμβάνει τη παραγωγή Elliptic Curve Certificate για τις εικόνες μέσα από εντολές openSSL, ενώ για PDF αρχεία (που γίνεται αναπαράσταση στο τέλος του διαγράμματος) τα κάνει Self – Signed με τη βοήθεια της βιβλιοθήκης TCPDF.Με το που παράξει τα νέα αρχεία και τα κλειδιά στέλνετε το email με το λινκ του αρχείου που μπορεί ο παραλήπτης να ανοίξει. Το URL αυτό είναι προσωρινό και έχει περιορισμένη ζωή 1 ώρας. Με το που ανοίξει ο παραλήπτης αυτό το URL γίνεται έλεγχος του κρυπτογραφημένου αρχείου με το αρχικό και του δίνει την επιλογή να το κατεβάσει καθώς του αναφέρει και την υπογραφή του αρχείου signature digest με Base64.



Εικόνα 8 Sequence Diagram Εφαρμογής

4.4 Λίγα λόγια για την PHP

Η PHP (PHP: Hypertext Preprocessor) είναι μια γλώσσα προγραμματισμού για τη δημιουργία σελίδων web με δυναμικό περιεχόμενο. Μια σελίδα PHP περνά από επεξεργασία από ένα συμβατό διακομιστή του Παγκόσμιου Ιστού (π.χ. Apache), ώστε να παραχθεί σε πραγματικό χρόνο το τελικό περιεχόμενο, που είτε θα σταλεί στο πρόγραμμα περιήγησης των επισκεπτών σε μορφή κώδικα HTML ή θα επεξεργασθεί τις εισόδους δίχως να προβάλλει την έξοδο στο χρήστη, αλλά θα τις μεταβιβάσει σε κάποιο άλλο PHP script.

Η PHP αποτελεί μια από τις πιο διαδεδομένες τεχνολογίες στο Παγκόσμιο Ιστό, καθώς χρησιμοποιείται από πληθώρα εφαρμογών και ιστότοπων. Διάσημες εφαρμογές που κάνουν εκτενή χρήση της PHP είναι το γνωστό Σύστημα Διαχείρισης Περιεχομένου (Content Management System, WordPress και το Drupal).

Ο συνδυασμός Linux/Apache/MySQL/PHP, που είναι η πιο δημοφιλής πλατφόρμα εκτέλεσης ιστοσελίδων είναι γνωστός και με το ακρωνύμιο LAMP. Παρόμοια, ο συνδυασμός */Apache/MySQL/PHP ονομάζεται *AMP, όπου το πρώτο αρχικό αντιστοιχεί στην πλατφόρμα, στην οποία εγκαθίστανται ο Apache, η MySQL και η PHP

Η ιστορία της PHP ξεκινά από το 1994, όταν ένας φοιτητής, ο Rasmus Lerdorf δημιούργησε χρησιμοποιώντας τη γλώσσα προγραμματισμού C ένα απλό script με όνομα php.cgi, για προσωπική χρήση. Το script αυτό είχε σαν σκοπό να διατηρεί μια λίστα στατιστικών για τα άτομα που έβλεπαν το online βιογραφικό του σημείωμα. Αργότερα αυτό το script το διέθεσε και σε φίλους του, οι οποίοι άρχισαν να του ζητούν να προσθέσει περισσότερες δυνατότητες. Η γλώσσα τότε ονομαζόταν PHP/FI από τα αρχικά Personal Home Page/Form Interpreter. Το 1997 η PHP/FI έφθασε στην έκδοση 2.0 αριθμώντας περισσότερους από 50.000 ιστότοπους που τη χρησιμοποιούσαν, ενώ αργότερα την ίδια χρονιά οι Andi Gutmans και Zeev Suraski ξαναέγραψαν τη γλώσσα από την αρχή, βασιζόμενοι όμως αρκετά στην PHP/FI 2.0. Έτσι η PHP έφθασε στην έκδοση 3.0 η οποία θύμιζε περισσότερο τη σημερινή μορφή της. Στη συνέχεια, οι Zeev και Andi δημιούργησαν την εταιρεία Zend (από τα αρχικά των ονομάτων τους), η οποία συνεχίζει μέχρι και σήμερα την ανάπτυξη και εξέλιξη της γλώσσας PHP. Ακολούθησε το 1998 η έκδοση 4 της PHP, τον Ιούλιο του 2004 διατέθηκε η έκδοση 5, ενώ αυτή τη στιγμή έχουν ήδη διατεθεί και οι πρώτες δοκιμαστικές εκδόσεις της επερχόμενης PHP 6, για οποιονδήποτε προγραμματιστή θέλει να τη χρησιμοποιήσει. Οι περισσότεροι ιστότοποι επί του παρόντος χρησιμοποιούν κυρίως τις εκδόσεις 5, 6 και 7 της PHP.

4.5 Πλεονεκτήματα PHP Framework – Laravel

Η ανάπτυξη σύνθετων έργων χρειάζεται ακρίβεια και όσο το δυνατόν πιο απλοποιημένη προσέγγιση. Οι περισσότερες web εφαρμογές αναπτύσσονται σε PHP Frameworks. Αυτά τα Frameworks προσφέρουν μεγαλύτερη ασφάλεια, ακεραιότητα και φυσικά ευκολία, άρα μικρότερο κόστος ανάπτυξης.

Το Laravel θεωρείται το καλύτερο PHP Framework αυτή τη στιγμή, από την κοινότητα των προγραμματιστών. Προσθέτει εγκυρότητα και υπεροχή στο σύνολο του έργου ενώ διευκολύνει την ανάπτυξη με τα ενσωματωμένα εργαλεία προγραμματιστών που διαθέτει καθώς και με την ευκολία εγκατάστασης σε σχέση με άλλα frameworks.

Παρακάτω αναφέρονται τα βασικά πλεονεκτήματα της χρήσης του Laravel.

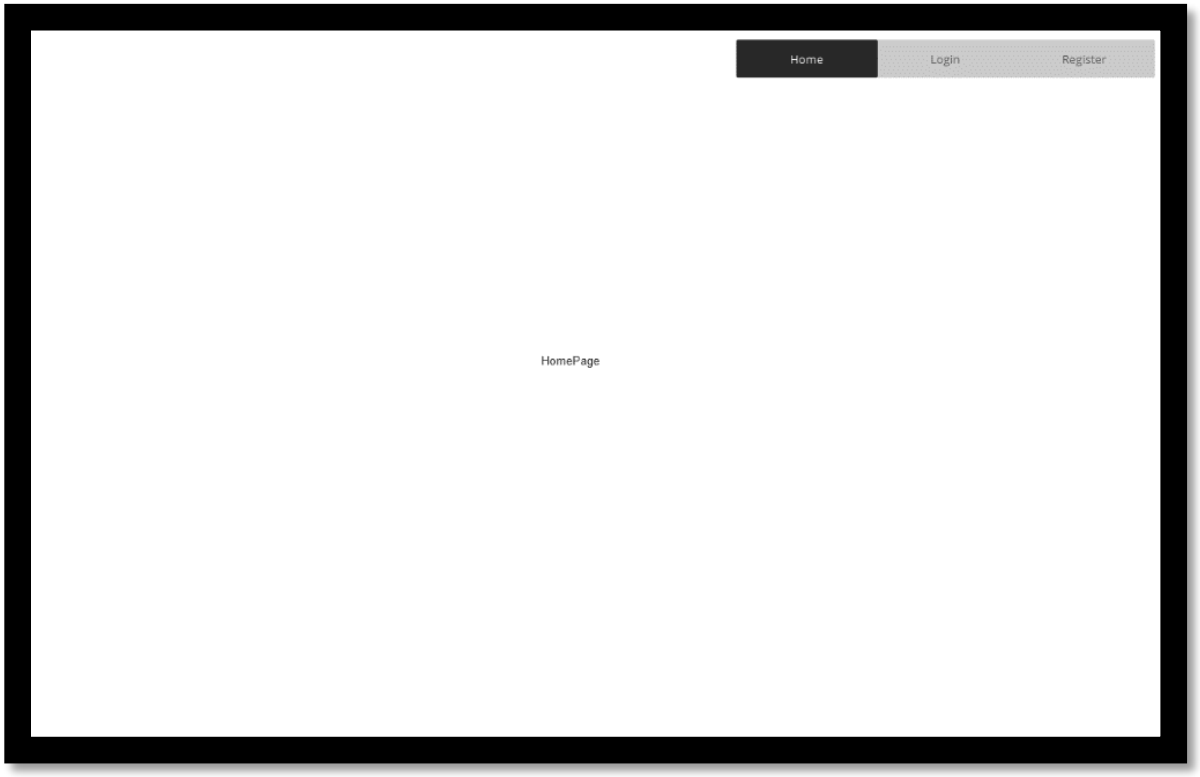
1. Αρχιτεκτονική MVC
2. Εργαλείο templating
3. Από και γρήγορο σύστημα ORM
4. Γραμμη εντολών – Artisan Command Line
5. Σύστημα Modular Packaging
6. Σύστημα Migration
7. Ενσωματωμένες βιβλιοθήκες
8. Μοναδικό Micro – Framework
9. Εξαιρετικές λειτουργίες ασφάλειας

Απλοποιημένη διαδικασία Unit Testing

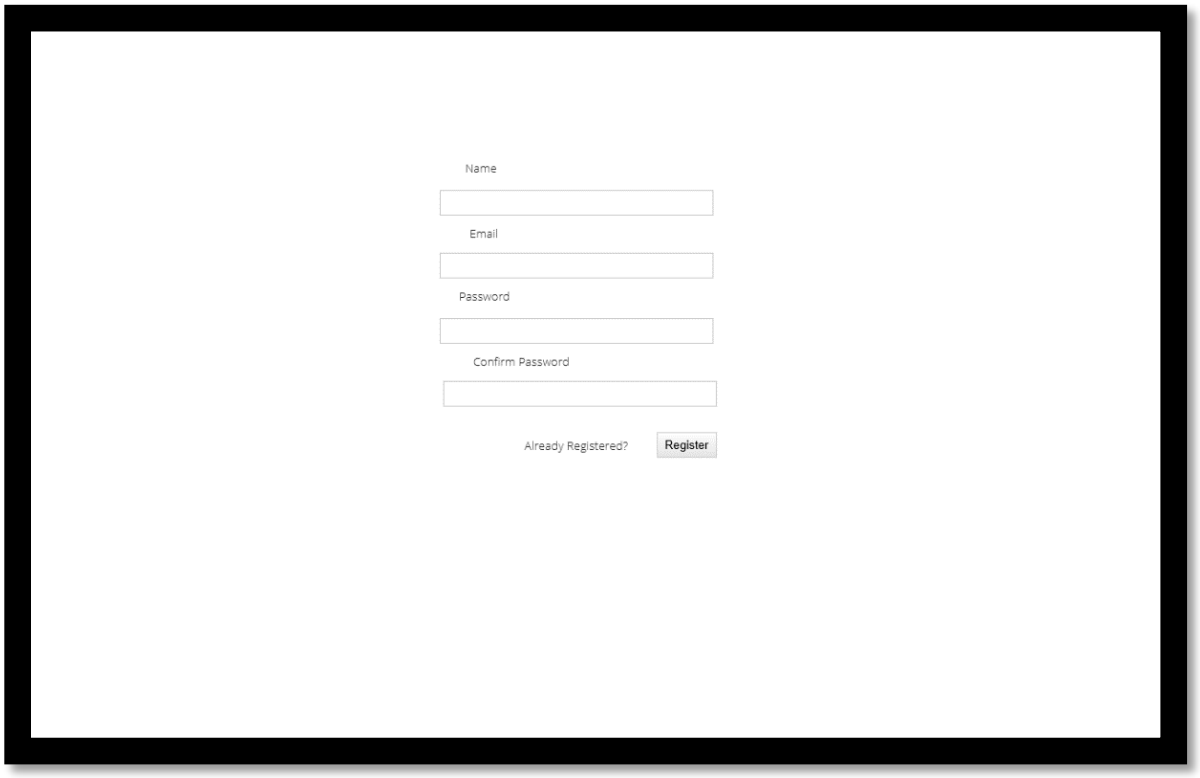
4.6 Προσχεδιασμός εφαρμογής με χρήση justinmind Mockup

Παρακάτω παρουσιάζεται ένας αρχικός σχεδιασμός που έγινε πριν την υλοποίηση της εφαρμογής με την χρήση του Justinmind Mockup. Σκοπός ήταν να γίνει μια αναπαράσταση πριν την υλοποίηση της, καθώς και να αναπαρασταθούν οι λειτουργίες που θα προσφέρονται στην εφαρμογή και τον σκοπό της.

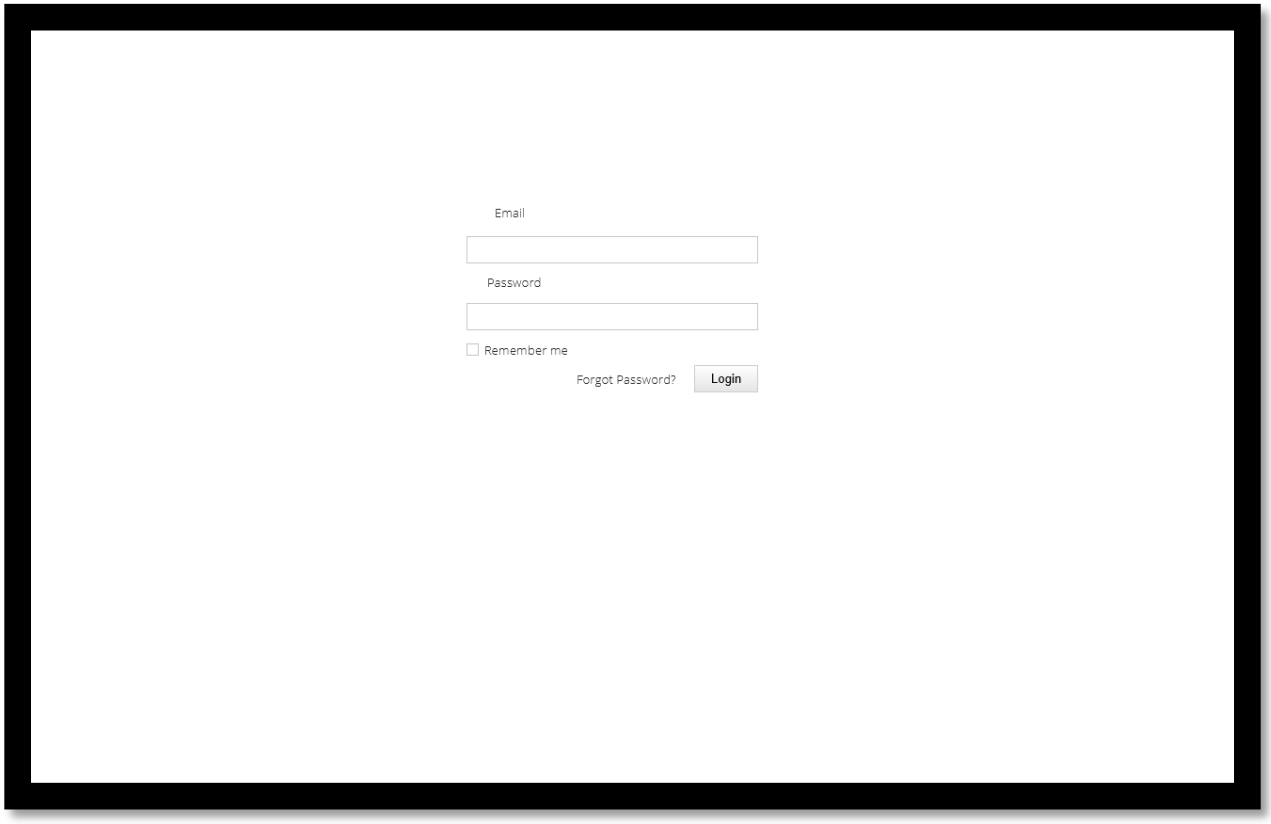
HomeScreen



RegisterScreen

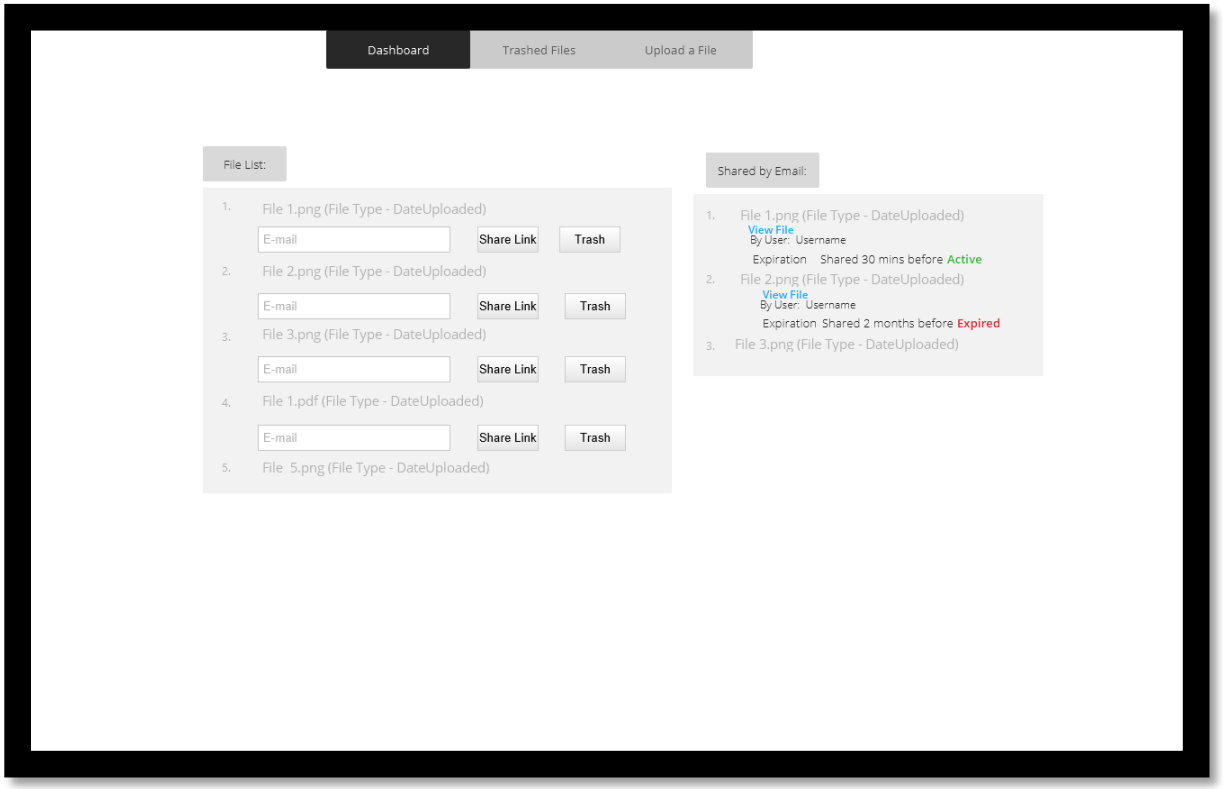


LoginScreen

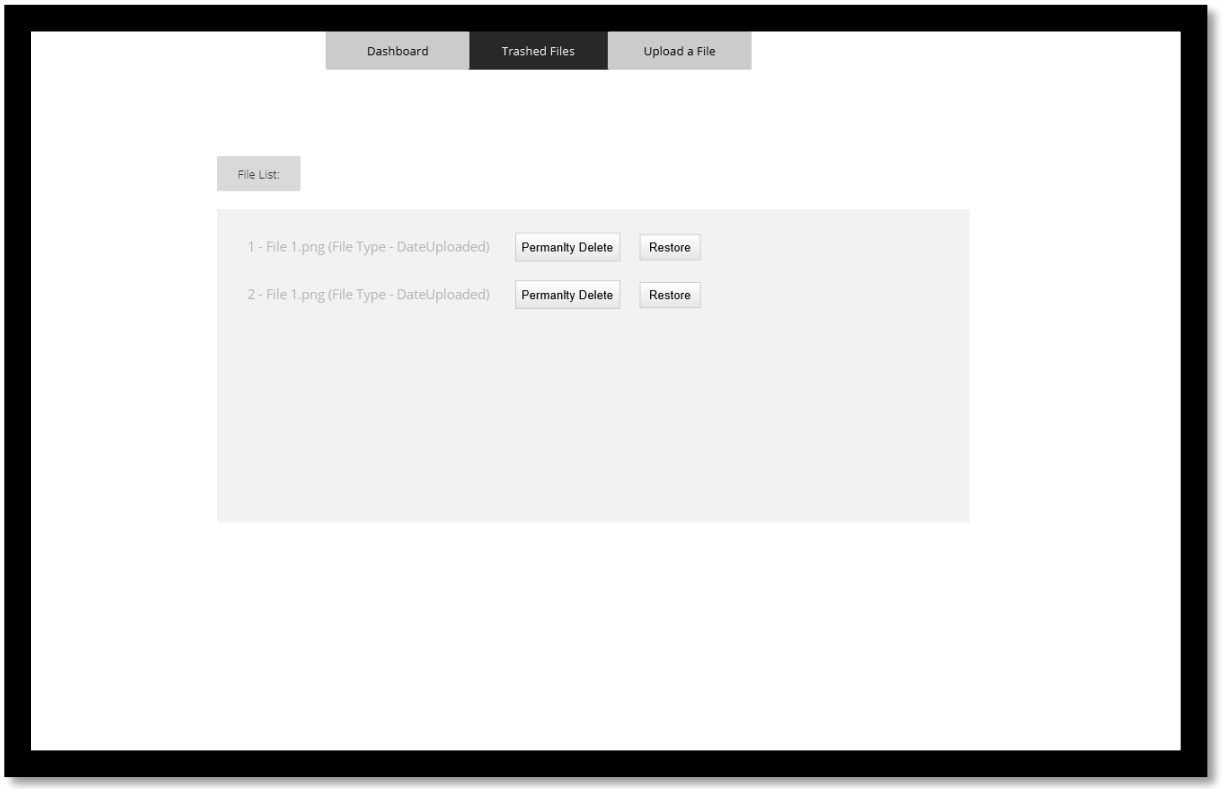


ForgotPasswordScreen

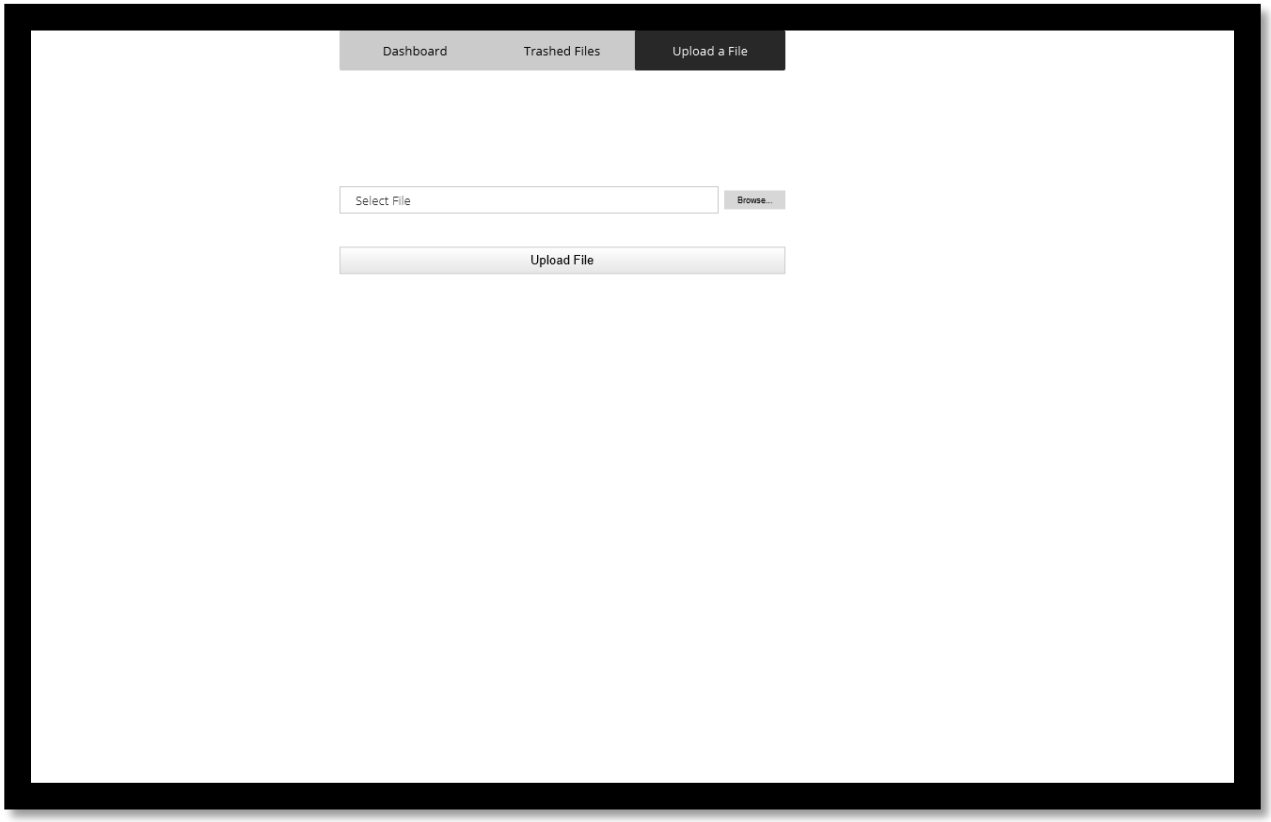
UserDashboardScreen



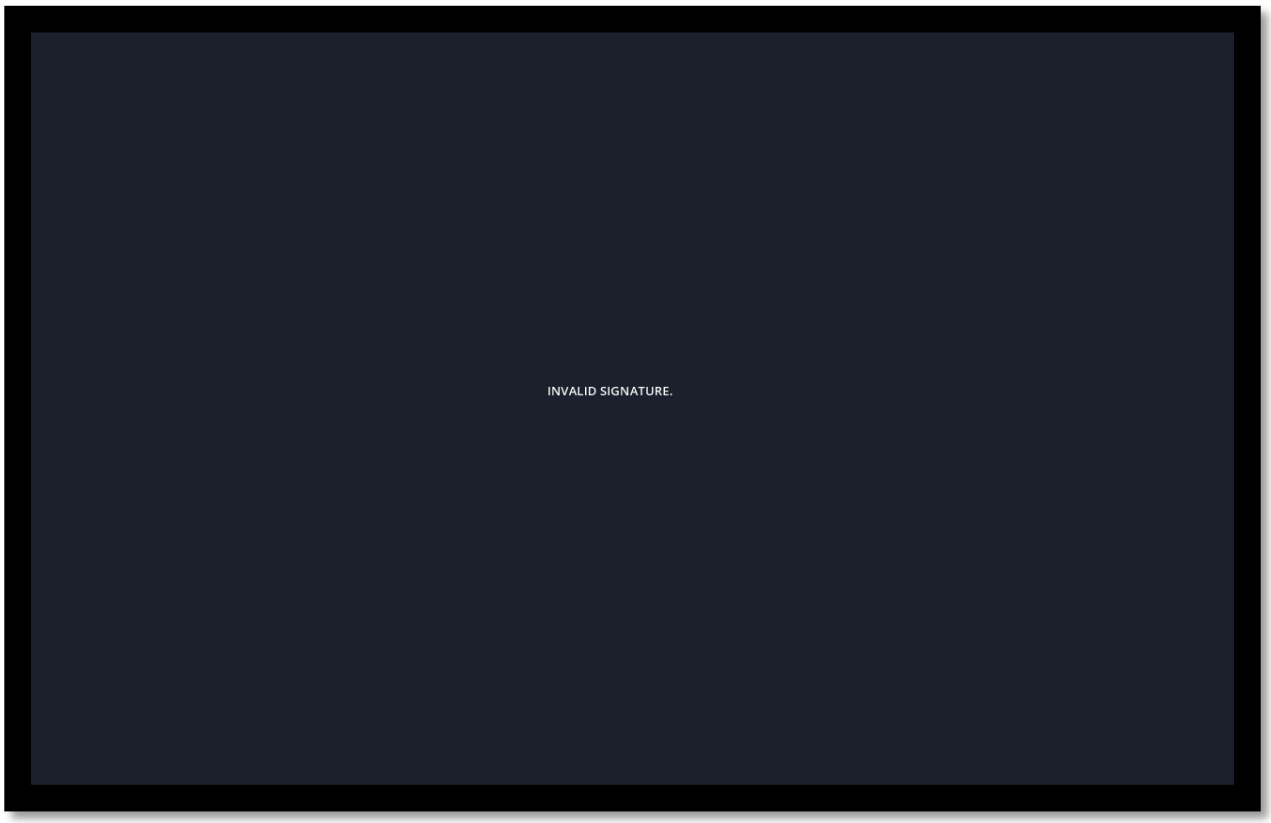
TrashedFilesScreen



UploadFileScreen



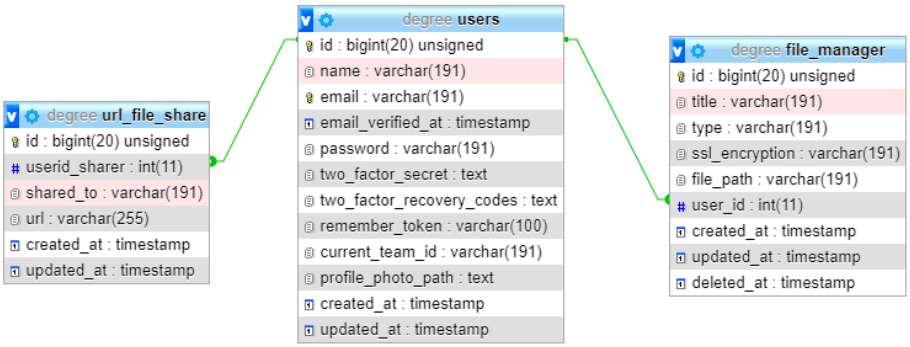
ExpiredUrlScreen



FileVerificationScreen

4.7 Σχεδιασμός Βάσης Δεδομένων

Για την αποθήκευση των δεδομένων της, η εφαρμογή χρησιμοποιεί μια σχεσιακή βάση MySQL. Οι πίνακες που υποστηρίζουν την αποθήκευση των δεδομένων καθώς και οι σχέσεις μεταξύ τους εμφανίζονται στο παρακάτω διάγραμμα



Εικόνα 9 Σχήμα Βάσης δεδομένων για το Self Sign αρχείων

- Ο πίνακας users περιέχει όλες τις πληροφορίες των χρηστών καθώς και τα credentials για την σύνδεση τους στην εφαρμογή. Έχει χρησιμοποιηθεί το υπάρχον Migration του

Laravel 8, ωστόσο έχουν γίνει custom συσχετίσεις με custom Migrations για την επιτυχή δημιουργία της εφαρμογής.

- Ο πίνακας file_manager είναι υπεύθυνος να κρατάει τις πληροφορίες των αρχείων που γίνεται μεταφόρτωση από τους χρήστες. Όπως βλέπουμε και από το παραπάνω σχήμα υπάρχει συσχετισμός του αρχείου κάθε εγγραφής με τον ID του user που το έκανε μεταφόρτωση. Αυτό σημαίνει ότι οι υπόλοιποι χρήστες του συστήματος δεν μπορούν να δουν τα μεταφορτωμένα αρχεία ο ένας του άλλου. Επίσης στη βάση αποθηκεύετε και το path που βρίσκεται το αρχείο.
- Ο πίνακας url_file_share είναι υπεύθυνος να κρατάει πληροφορίες και προστίθεται νέα εγγραφή όταν κάποιος χρήστης κάνει share ένα αρχείο με κάποιον άλλον βάση του e-mail του. Πάλι υπάρχει συσχετισμός με το user ID του πίνακα users και το column userid_sharer. Αυτός ο συσχετισμός υπάρχει λόγω του μηχανισμού που θα αναφερθεί παρακάτω όταν πατιέται ο σύνδεσμος από τον χρήστη που του έγινε η διαμοίραση του URL να στέλνεται ενημερωτικό email στον διαμοιραστή ότι το αρχείο του ανοίχτηκε από το συγκεκριμένο e-mail. Επίσης στο column URL αυτού του πίνακα αποθηκεύεται το temporary URL που έχει δημιουργηθεί από τον Controller με χρόνο χρήσης 1 ώρας.

Κεφάλαιο 5. Υλοποίηση εφαρμογής

5.1 Δημιουργία κλειδιών στο Server

Οι παράμετροι για Elliptic Curve δημιουργία κλειδιού. Για τη δημιουργία κλειδιού elliptic Curve με αλγόριθμο 256k1 χρησιμοποιούμε την παρακάτω εντολή.

- openssl ecparam -name secp256k1 -out secp256k1.pem

Για την δημιουργία ιδιωτικού κλειδιού χρησιμοποιούμε την εντολή.

- openssl ecparam -in secp256k1.pem -genkey -noout -out key1.pem

Για να κάνουμε Generate το αντίστοιχο δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό χρησιμοποιούμε την εντολή.

- openssl ec -in key1.pem -pubout > pubkey1.pem

Όλα αυτά σύμφωνα με το παρών Project έχουμε φτιάξει ένα φάκελο certificates στο root path και τα έχουμε βάλει μέσα.

Στην συνέχεια κάνουμε Generate η δυαδική υπογραφή και μετατροπή με τον αλγόριθμο base64 χρησιμοποιούμε την εντολή.

- openssl dgst -sha256 -sign key1.pem file_name.file_type > sig1 base64 sig1 > sig1b64

Για να επιβεβαιώσουμε την υπογραφή του αρχείου από base64 χρησιμοποιούμε την εντολή

- base64 -d sig1b64 > sig1d
- openssl dgst -sha256 -verify (__FOLDER_PATH__)/certificates/pubkey1.pem -signature sig1d file_name.file_path

Αν όλα γίνουν σωστά πρέπει να μας επιστρέψει στο τερματικό

Verified OK

Για την μετατροπή PEM αρχείου σε CRT χρησιμοποιούμε την παρακάτω εντολή.

- openssl x509 -outform der -in certificate.pem -out certificate.crt

Όπως επίσης για την μετατροπή PKCS#12 αρχείου (δηλαδή με κατάληξη .pfx .p12), που συμπεριλαμβάνει ένα ιδιωτικό κλειδί και το certificate to PEM χρησιμοποιούμε την εντολή.

- openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes

Σε αυτήν την περίπτωση μπορεί κάποιος να βάλει σαν παράμετρο το

-nocerts για να βγάλει στο output μόνο το ιδιωτικό κλειδί ή να προσθέσει τη παράμετρο -nokeys για να βγάλει στο output μόνο το certificate.

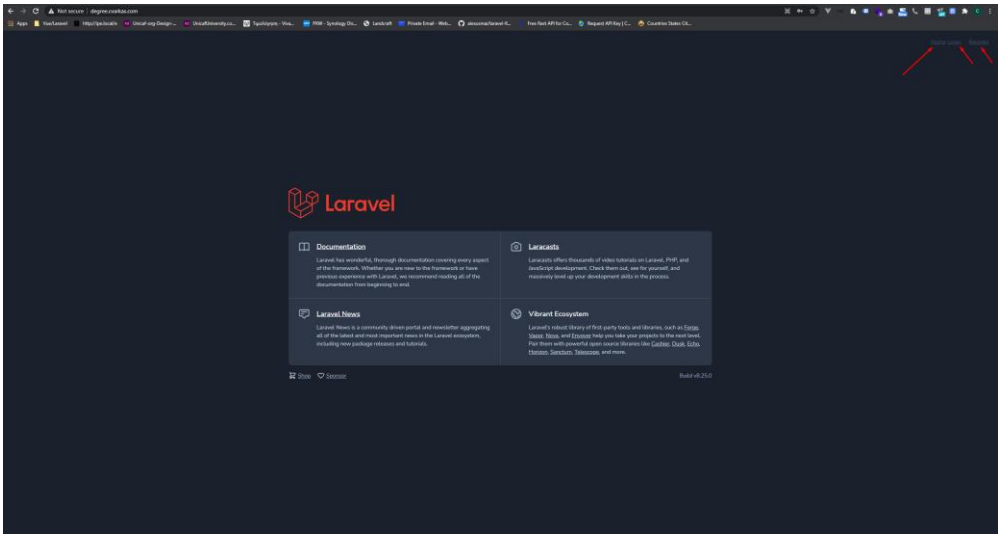
Όλες οι εντολές ωστόσο που χρησιμοποιήθηκαν έχουν μπει στους Controllers με μεθόδους με την βοήθεια της PHP μεθόδου shell_exec() περνώντας μέσα στη παρένθεση αυτές τις εντολές και

κάνοντας δυναμικά τα ονόματα αρχείων κάθε φορά που εκτελούνται για το κάθε αρχείο. Για την δημιουργία κλειδιών έγινε ωστόσο μία φορά η εκτέλεση τους και μπήκαν στο φάκελο με όνομα certificates.

5.2 Παρουσίαση εφαρμογής

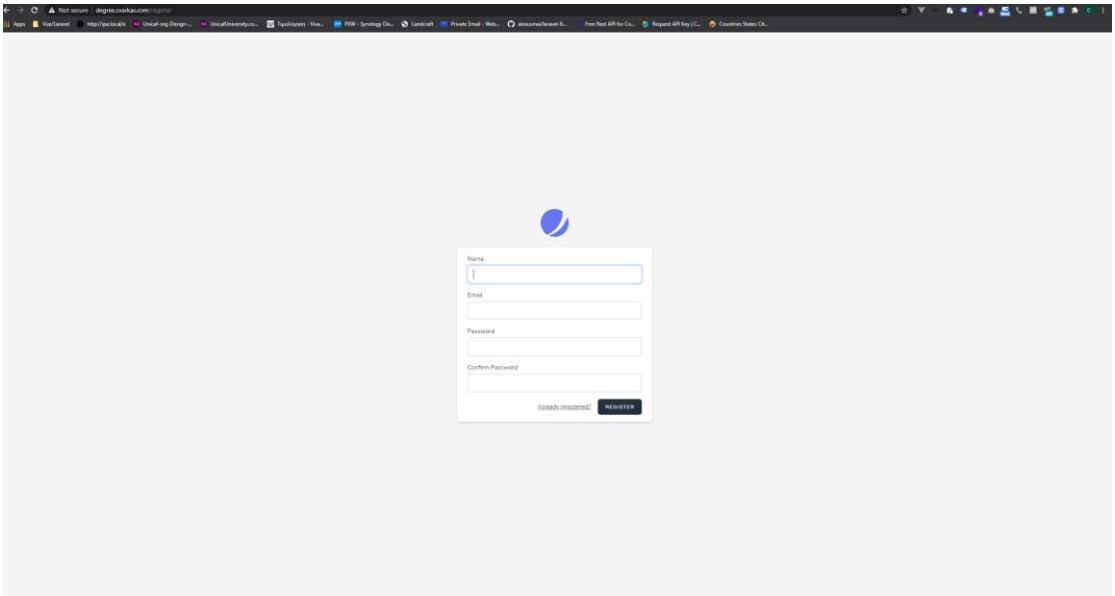
Παρακάτω θα αναλύσουμε και με εικόνες και με περιγραφές την εφαρμογή. Μπορείτε να έχετε πρόσβαση για να την δείτε στο παρακάτω URL. Το συγκεκριμένο URL θα μείνει ενεργό καθ' όλη τη διάρκεια παράδοσης της εργασίας. Μετά το πέρας αυτής της περιόδου το URL θα απενεργοποιηθεί. http://degree.cvarkas.com/

Με το που πατήσουμε το URL θα μας εμφανίσει την default σελίδα της Laravel, μιας και όλος ο μηχανισμός είναι μετά την εγγραφή και τη σύνδεση του χρήστη δεν υπήρχε κάποιος λόγος να επεξεργαστώ το default view. Αυτά που μας ενδιαφέρουν είναι στο header το μενού.



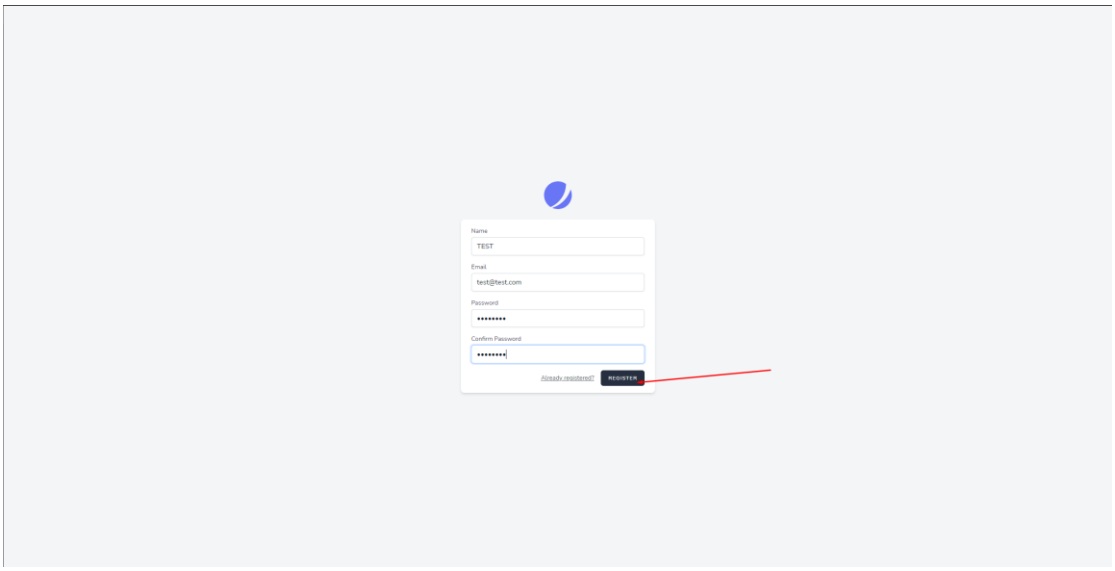
Εικόνα 10 Αρχική Σελίδα Ανοίγματος Εφαρμογής

Με το που πατήσουμε Register θα μας εμφανιστεί η σελίδα εγγραφής και μια φόρμα για τη δημιουργία ενός νέου χρήστη στο σύστημα.

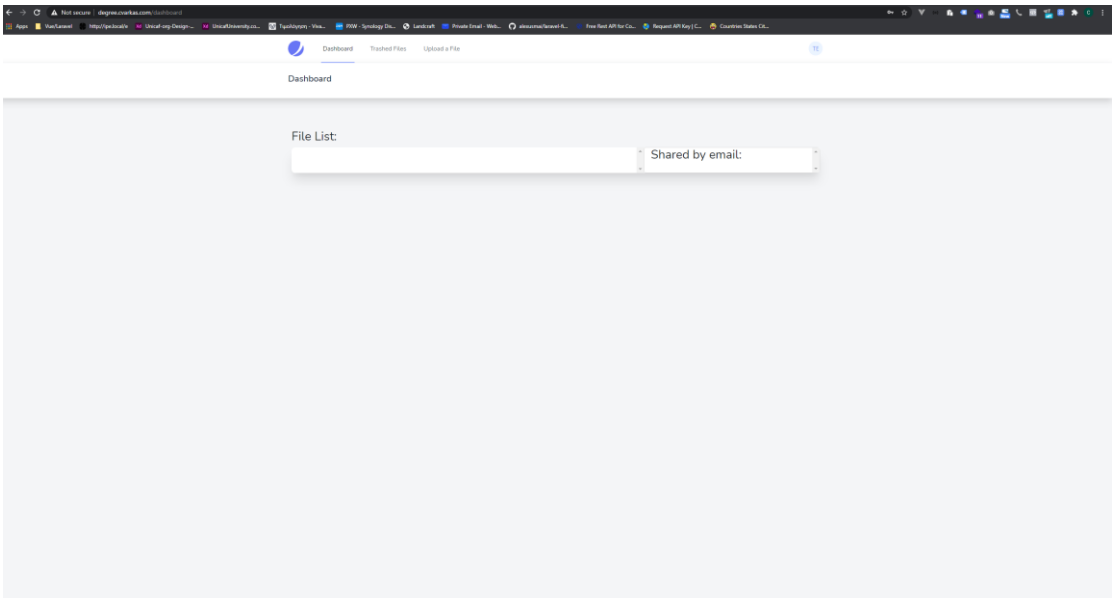


Εικόνα 11 Σελίδα Εγγραφής νέου χρήστη

Με το που συμπληρώσουμε τα πεδία και πατήσουμε το κουμπί Register θα μας ανακατευθύνει στο διαχειριστικό του χρήστη

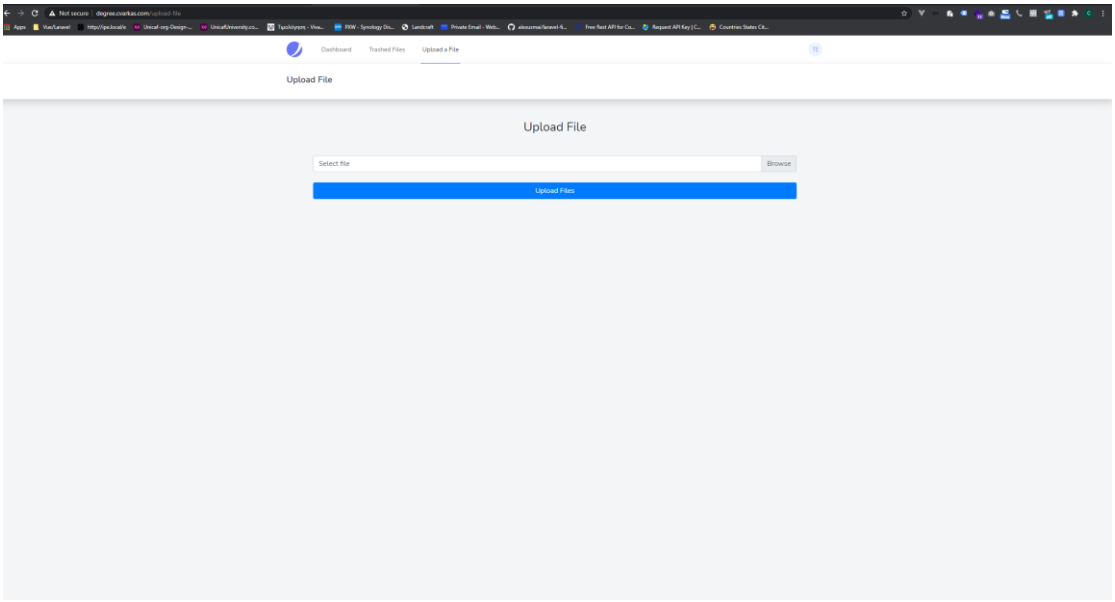


Εικόνα 12 Εγγραφή Χρήστη μετά τη συμπλήρωση φόρμας



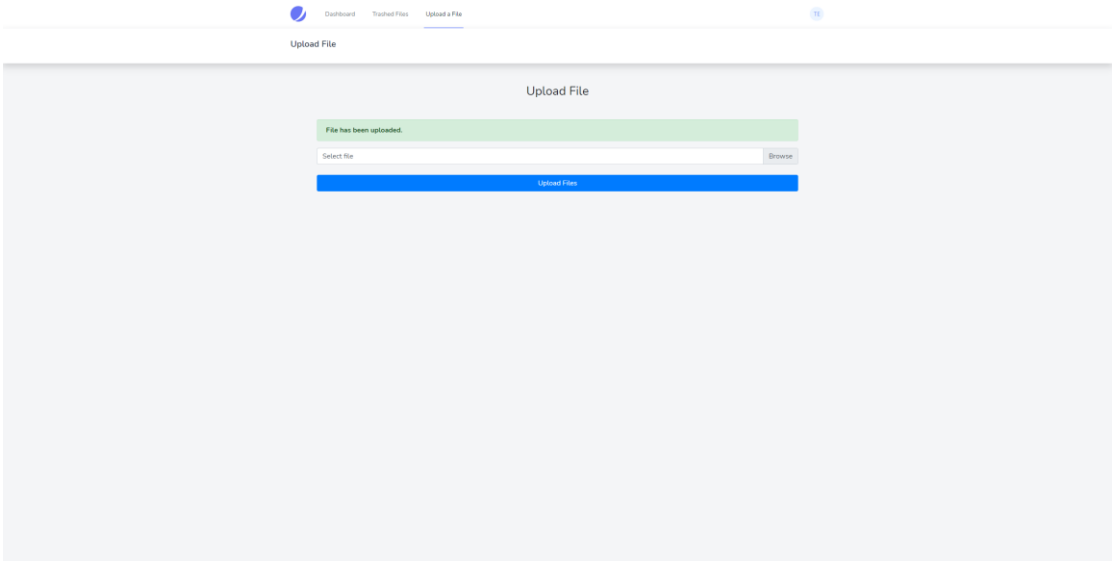
Εικόνα 13 Διαχειριστικό χρήστη Πρώτη σελίδα μετά την επιτυχή σύνδεση

Στα αριστερά μας βλέπουμε το File List Panel το οποίο εκεί θα εμφανίζονται τα αρχεία που θα ανεβάζουμε στον Server. Στα δεξιά μας βλέπουμε το Shared By Email Panel το οποίο είναι τα αρχεία που λαμβάνουμε από άλλους χρήστες. Πάνω στο Header Βλέπουμε 3 Links, το Dashboard που είναι η παραπάνω εικόνα, το Trashed Files που πηγαίνουν τα αρχεία που έχουμε ανεβάσει και θέλουμε να διαγράψουμε και από κει μπορούμε είτε να τα διαγράψουμε ολικώς, είτε να τα επαναφέρουμε στην File List. Τέλος είναι το Upload a File το οποίο από εκεί μπορούμε να ανεβάσουμε τα αρχεία μας.



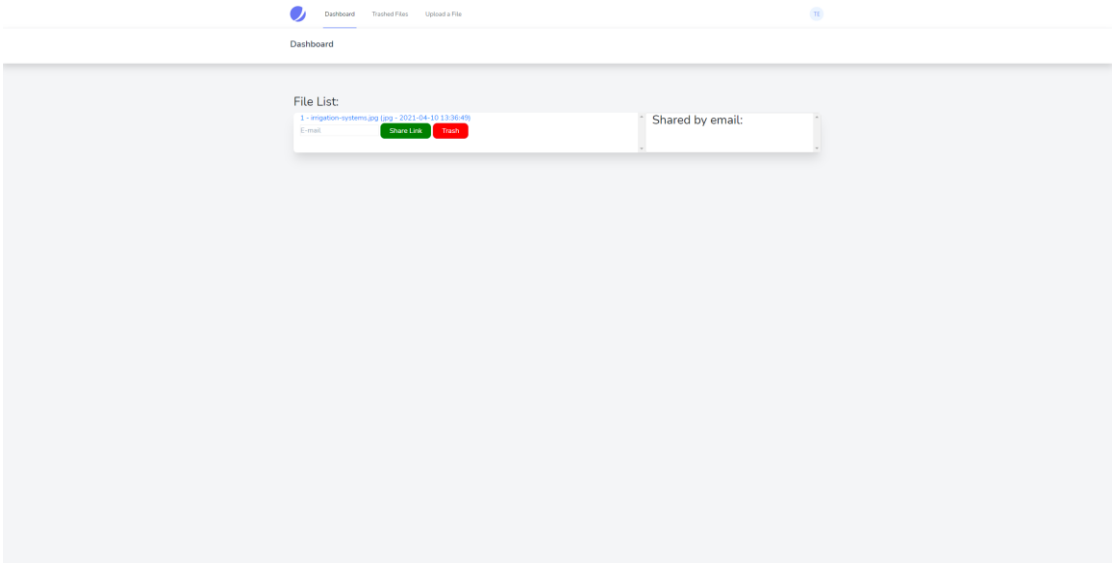
Εικόνα 14 Σελίδα που ο χρήστης έχει τη δυνατότητα να ανεβάσει αρχεία

Με το που ανεβάσουμε κάποιο αρχείο και είναι επιτυχής το ανέβασμα μας γυρνάει στο ίδιο View με μήνυμα επιτυχίας.



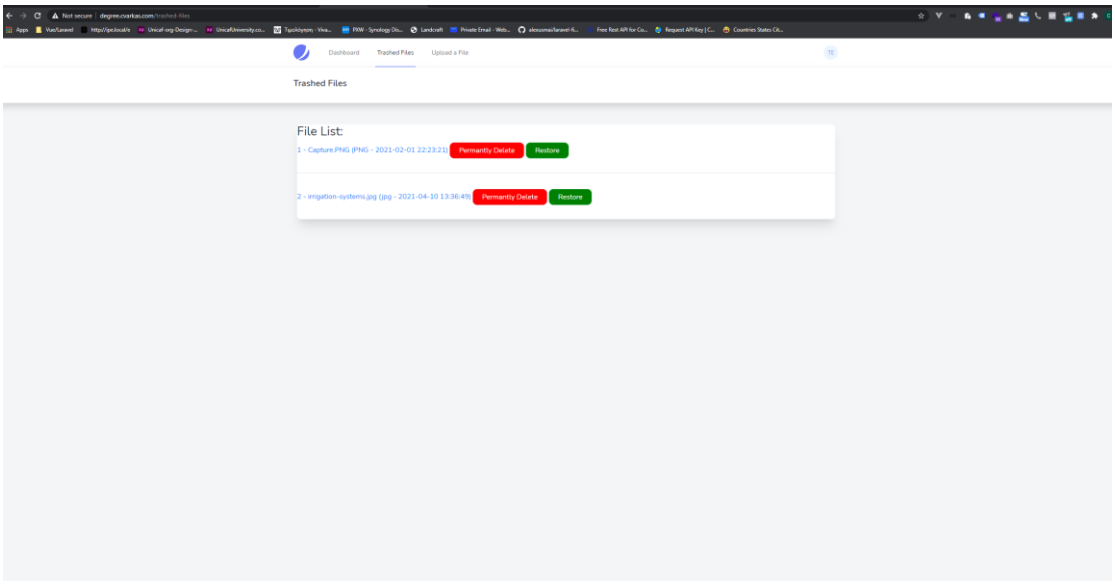
Εικόνα 15 Επιτυχής μεταφόρτωσης αρχείου

Αν επιστρέψουμε πίσω στο dashboard θα δούμε το αρχείο που μόλις έχει ανέβει. Από εκεί βλέπουμε 2 επιλογές και ένα input. Μπορούμε είτε να το βάλουμε στα Trash που σημαίνει ότι θα πάει στα Trashed files, είτε θα συμπληρώσουμε το e-mail που θέλουμε να κάνουμε share το αρχείο με κάποιον.



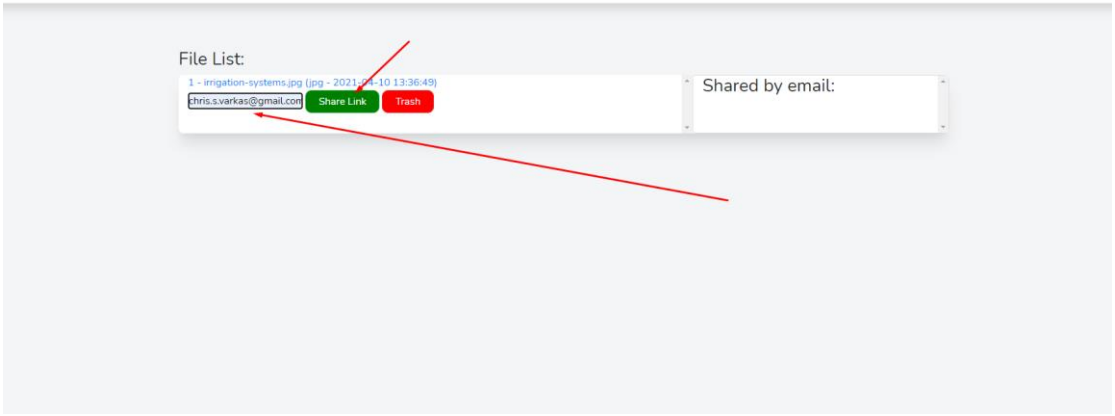
Εικόνα 3 Διαχειριστικό περιέχοντας τη Λίστα αρχείων που έχουν μεταφορτωθεί

Στην πρώτη περίπτωση που το διαγράψουμε και πάμε στα Trashed Files θα δούμε μια λίστα με διαγραμμένα.

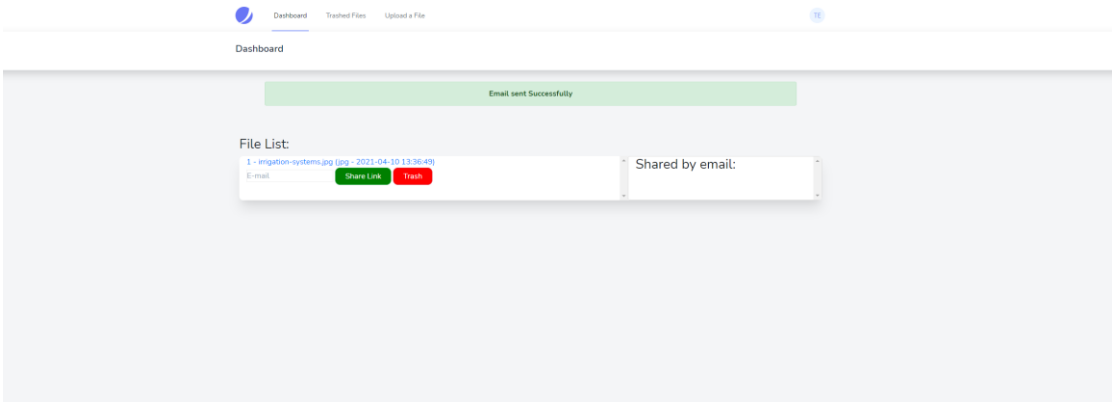


Εικόνα 17 Σελίδα με όλα τα διαγραμμένα αρχεία έχοντας την επιλογή επαναφοράς ή οριστικής διαγραφής

Από εκεί μπορούμε να το κάνουμε μόνιμα διαγραφή είτε να το επαναφέρουμε. Στην δεύτερη επιλογή μπορούμε να το στείλουμε σε κάποιον. Οπότε συμπληρώνοντας το όνομα του και πατήσουμε share Link



Εικόνα 18 Σελίδα Διαχειριστικού που ο χρήστης συμπληρώνει το email που θέλει να διαμοιράσει το αρχείο

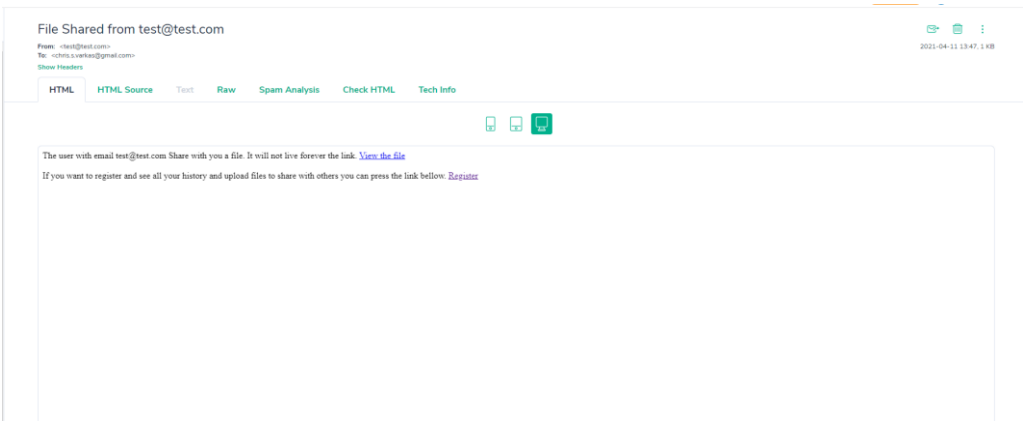


Εικόνα 4 Επιτυχής αποστολή email με το URL που έγινε Generate

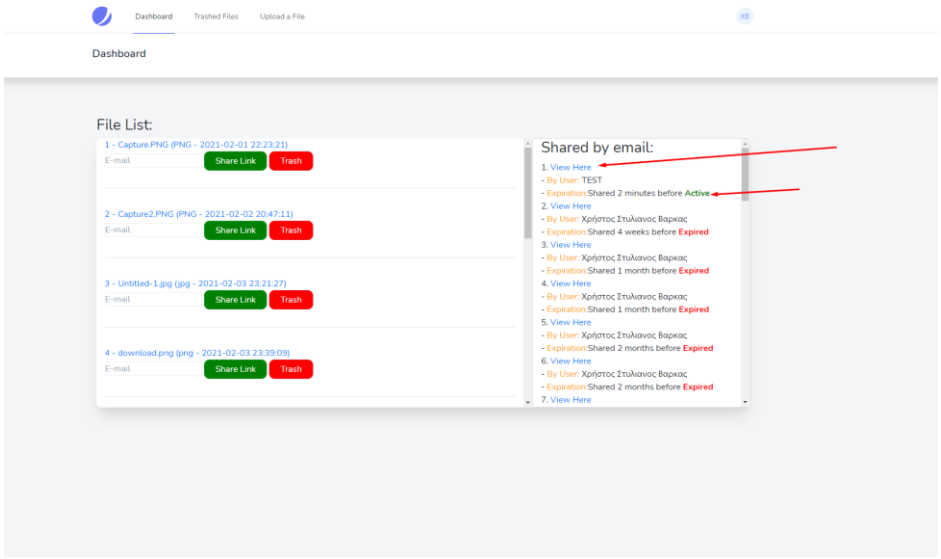
Παρακάτω Βλέπουμε το κώδικα που υλοποιήθηκε στην μέθοδο η οποία ονομάστηκε mail με παράμετρο το email που θέλουμε να κάνουμε διαμοίραση του αρχείου και είναι υπεύθυνο για τη μετατροπή σε δυαδικό του αρχείου και μετατροπή με base 64 Elliptic Curve sha256.

```
$basePath = base_path();

    $output = shell_exec('ls ' . $basePath . '/storage/app/public/uploads -lart');


    // Genering binary of the file and convert it to Base64
    shell_exec('openssl dgst -sha256 -sign ' . $basePath . '/certificates/key1.pem ' . $basePath .
    '/storage/app/public/uploads/' . $filename . ' > ' . $basePath . '/storage/app/public/uploads/' .
    $filename . '-sha ');
    shell_exec('base64 ' . $basePath . '/storage/app/public/uploads/' . $filename . '-sha > ' .
    $basePath . '/storage/app/public/uploads/' . $filename . '-sha64 ');
    shell_exec('base64 -d ' . $basePath . '/storage/app/public/uploads/' . $filename . '-sha64  > ' .
    $basePath . '/storage/app/public/uploads/' . $filename . '-sha');
    $verification = shell_exec('openssl dgst -sha256 -verify ' . $basePath .
    '/certificates/pubkey1.pem -signature ' . $basePath . '/storage/app/public/uploads/' . $filename .
    '-sha ' . $basePath . '/storage/app/public/uploads/' . $filename . '');
```

Με το που σταλεί το share URL ο χρήστης λαμβάνει e-mail για το αρχείο που μπορεί να δει το αρχείο για 1 ώρα. Επίσης αν ο χρήστης φτιάξει λογαριασμό θα δει τη λίστα με το αρχείο πριν πόση ώρα του έχει σταλεί και αν είναι ενεργός ο σύνδεσμος.

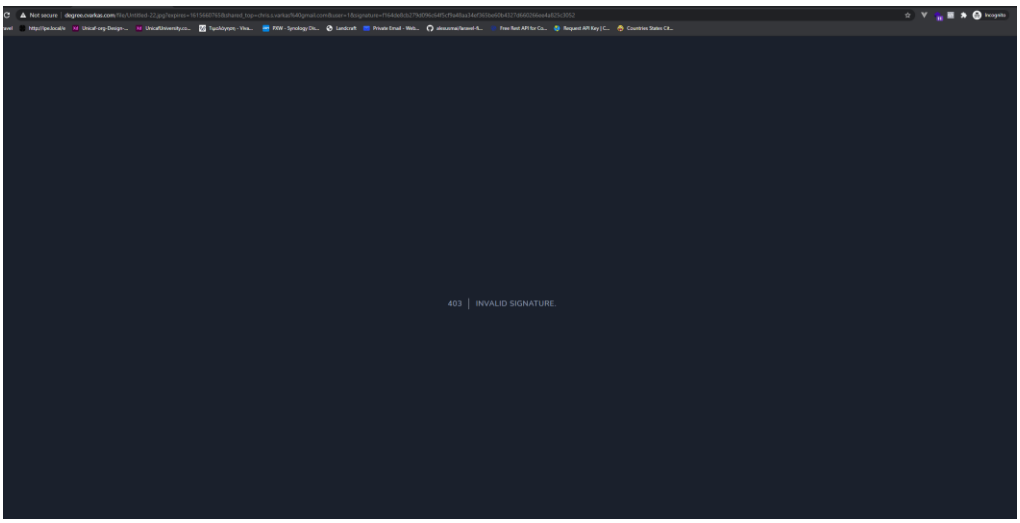


Εικόνα 19 Το email που λαμβάνει ο παραλήπτης όταν έγινε η διαμοίραση



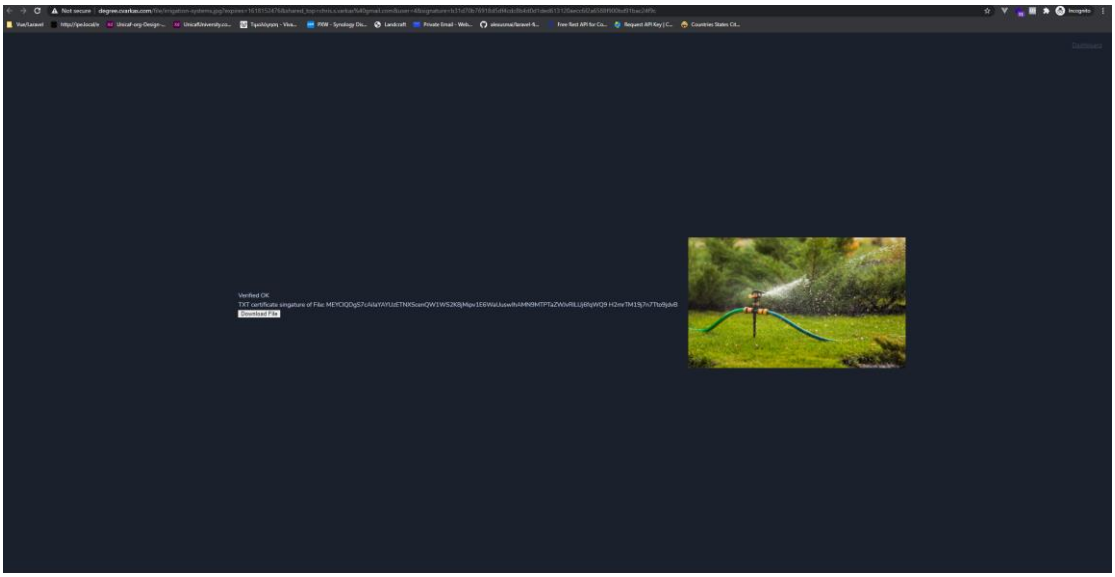
Εικόνα 20 Δεξί πάνελ με όλα τα μοιρασμένα αρχεία που έχει λάβει ο χρήστης από άλλον χρήστη

Στην αντίθετη περίπτωση αν έχει λήξει ο χρόνος του αρχείου αναγράφεται ότι είναι Expired και δεν έχει πρόσβαση στο να δει το αρχείο όταν πατήσει το Link αναγράφοντας Error 403 | Invalid Signature.



Εικόνα 21 Σελίδα ανακατεύθυνσης μετά από λήξη URL

Στην περίπτωση που το αρχείο είναι ενεργό θα του εμφανίσει μια σελίδα με προεπισκόπηση καθώς και κουμπί να κάνει λήψη το αρχείο αλλά ωστόσο του βγάζει και μήνυμα αν το αρχείο είναι Verified μαζί με το Certificate Signature key.



Εικόνα 22 Σελίδα ανακατεύθυνσης με έγκυρο αρχείο

Εδώ έχει υλοποιηθεί ο κώδικας στον Controller που κάνει έλεγχο και verify αν το certification που έχει γίνει πριν τη διαμοίραση του αρχείου είναι το ίδιο. Παρακάτω βλέπουμε απόσπασμα κώδικα στην μέθοδο getFile στην οποία γίνεται ο έλεγχος αυτός και μας επιστρέφει το original αρχείο και διαθέσιμο προς λήψη τοπικά στον Υπολογιστή μας.

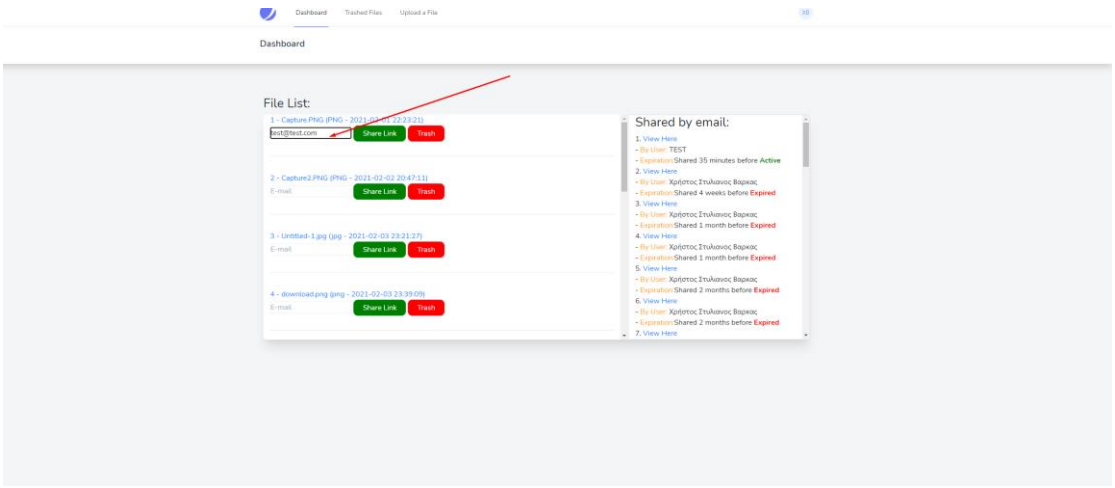
```
public function getFile($filename, Request $res)
    {

        $file = Storage::disk('public')->getDriver()->getAdapter()->applyPathPrefix('/uploads/' .
    $filename);

        $extension = pathinfo($file, PATHINFO_EXTENSION);

        $user_email = User::findOrFail($res->user);


        $basePath = base_path();
        $verification = shell_exec('openssl dgst -sha256 -verify ' . $basePath .
    '/certificates/pubkey1.pem -signature ' . $basePath . '/storage/app/public/uploads/' . $filename .
    '-sha ' . $basePath . '/storage/app/public/uploads/' . $filename . '');
        $base64Txt = shell_exec('cat ' . $basePath . '/storage/app/public/uploads/' . $filename . '-
    sha64');


        Mail::to($user_email->email)->send(new OpenMailNotification(['user' => auth()->user(),
    'email' => $res->shared_top, 'file_url' => $res->fullUrl()]));


        if ($extension == 'pdf') {
            $this->pdfSignDigitally($file);
        }

        return view('file-validation')->with(['data' => $filename, 'verification' => $verification,
    'base64Txt' => $base64Txt]);
```

```
}
```

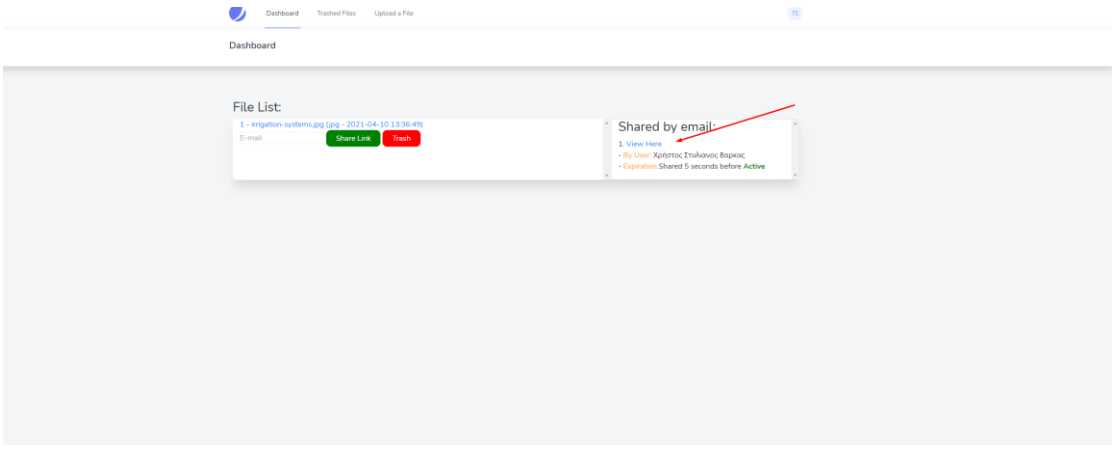
Στον κώδικα μπορούμε να παρατηρήσουμε και άλλα πράγματα. Πρώτο με το που γίνει εκτέλεση της μεθόδου στέλνεται ένα άλλο email στον χρήστη ο οποίος είχε κάνει τη διαμοίραση του αρχείου αναφέροντας πώς ο χρήστης με το παρών e-mail άνοιξε το αρχείο που του έστειλε. Δεύτερον βλέπουμε ότι αν το extension του αρχείου είναι pdf εκτελείται μια άλλη μέθοδος η οποία γίνεται χρήση του TCPDF και το pdf γίνεται self-signed μέσα στο ίδιο pdf. Αλλιώς συνεχίζεται το Validation (στη περίπτωση που είναι τύπος εικόνας και βρίσκει το αρχικό αρχείο της εικόνας που γίνεται Verified. Παρακάτω θα δούμε και τον κώδικα της μεθόδου pdfSignDigitally, όταν αναφερθούμε στη λήψη pdf.

Εικόνα 23 Επιτυχής λήψη τοπικά του αρχείου

Στην περίπτωση που το αρχείο που ανέβει είναι pdf Κατεβάζει το αρχείο pdf με Self Singed το pdf αρχείο



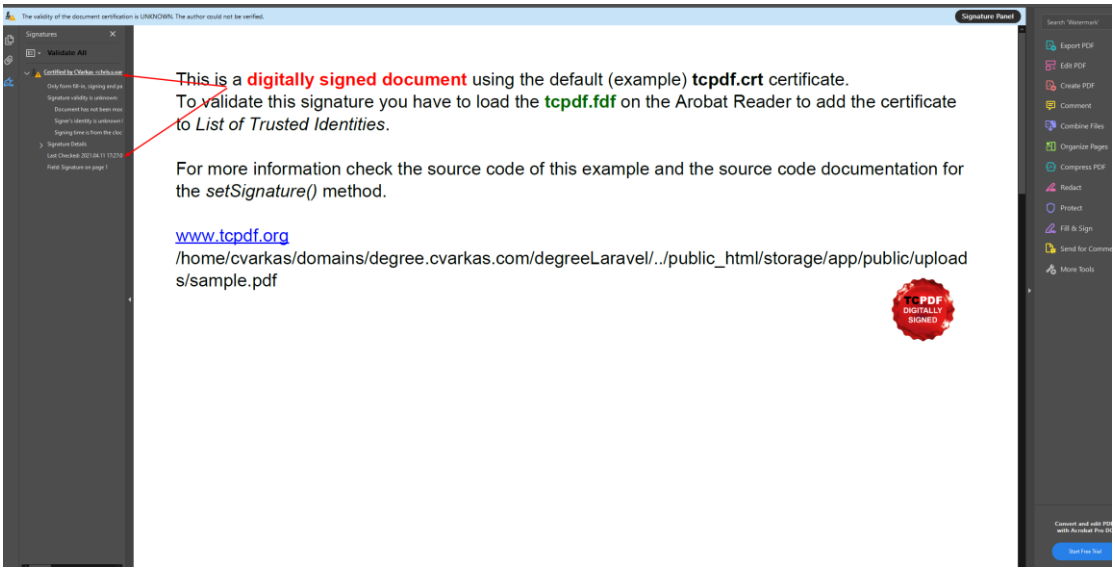
Εικόνα 24 Ανέβασμα PDF αρχείου



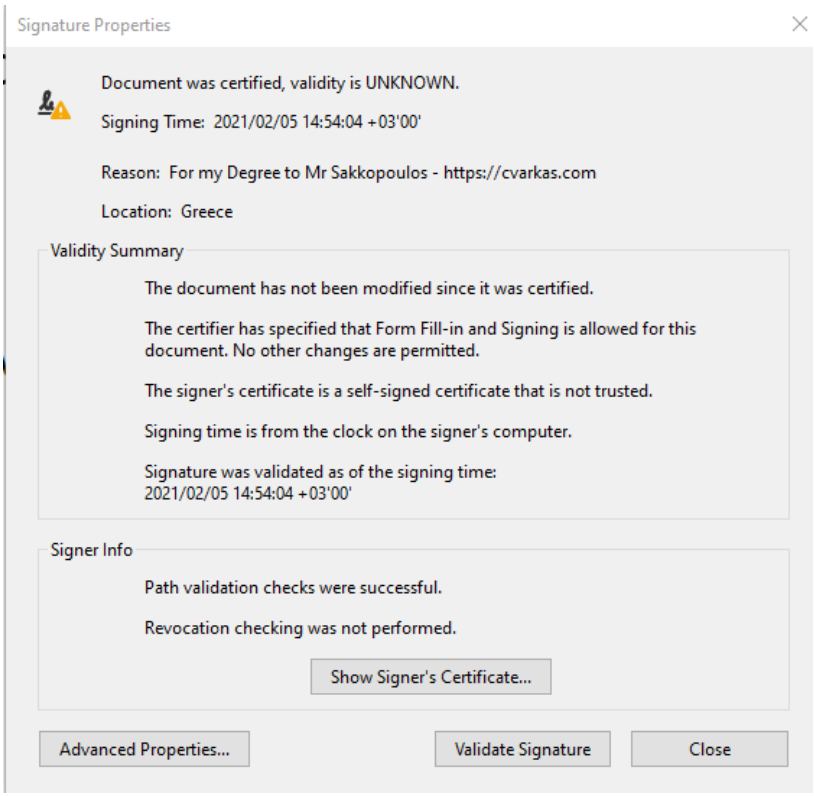
Εικόνα 5Αναφορά ότι το συγκεκριμένο αρχείο είναι ακόμα ενεργό

Παραπάνω είχαμε αναφερθεί σε μια μέθοδο με όνομα pdfSignDigitally. Εδώ θα δείξουμε το κώδικα που υλοποιήθηκε για να μπορεί το pdf να γίνεται digital signed με τη χρήση Digital Certificate Authority που είναι εγκαταστημένη στον Server.

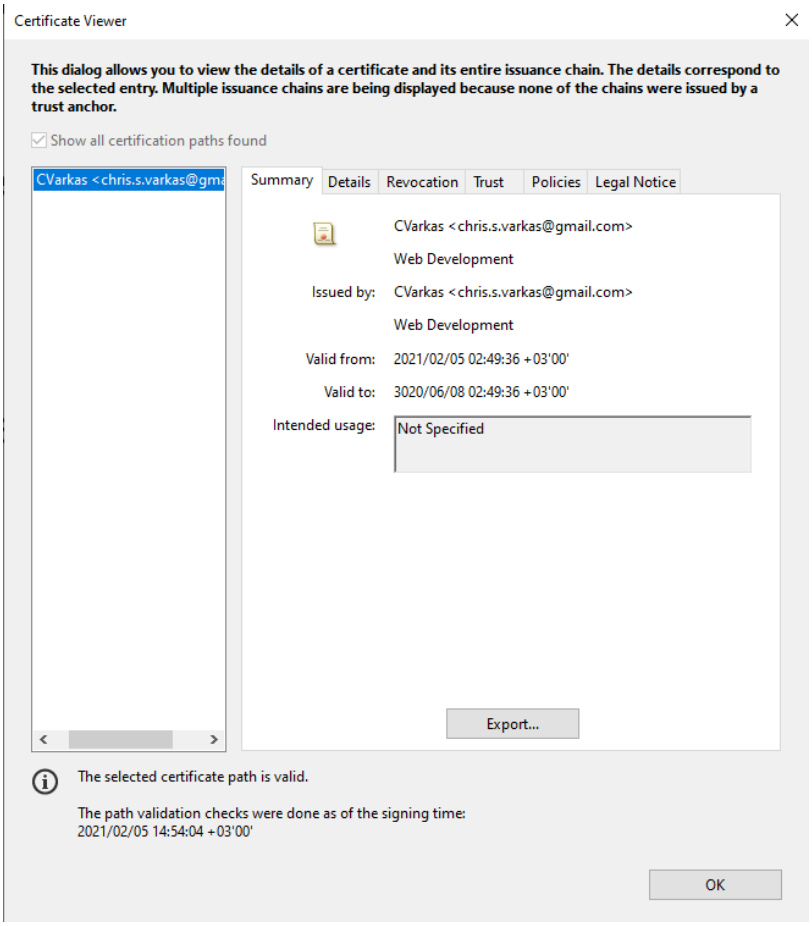
```
public function pdfSignDigitally($file)
    {
        $basePath = base_path();

        $certificate = 'file:///../certificates/tcpdf.crt';

        // set additional information in the signature
        $info = array(
            'Name' => 'Chris S. Varkas',
            'Location' => 'Greece',
            'Reason' => 'For my Degree',
            'ContactInfo' => 'https://cvarkas.com',
        );

        // set document signature
        PDF::setSignature($certificate, $certificate, 'tcpdfdemo', '', 2, $info);

        PDF::SetFont('helvetica', '', 12);
        PDF::SetTitle('Signed File PDF from degree.cvarkas.com');
        PDF::AddPage();

        // print a line of text
         $text = 'This is a <b color="#FF0000">digitally signed document</b> using the default
    (example) <b>tcpdf.crt</b> certificate.<br />To validate this signature you have to load the <b
    color="#006600">tcpdf.fdf</b> on the Arobat Reader to add the certificate to <i>List of Trusted
    Identities</i>.<br /><br />For more information check the source code of this example and the
    source code documentation for the <i>setSignature()</i> method.<br /><br /><a
    href="http://www.tcpdf.org">www.tcpdf.org</a>';

        // add view content
        PDF::writeHTML($text, true, 0, true, 0);

        // add image for signature
        PDF::Image($basePath.'/../public_html/storage/app/public/uploads/site/tcpdf_signature.png',
    180, 60, 15, 15, 'PNG');

        // define active area for signature appearance
        PDF::setSignatureAppearance(180, 60, 15, 15);

        PDF::importPDF($basePath.'/../public_html/storage/app/public/uploads/sample.pdf');

        // save pdf file
        PDF::Output($file, 'F');

        PDF::reset();

    }
```



Εικόνα 26 Digitally Signed PDF με χρήση Digital Certificate Authority που είναι εγκαταστημένη στον Server

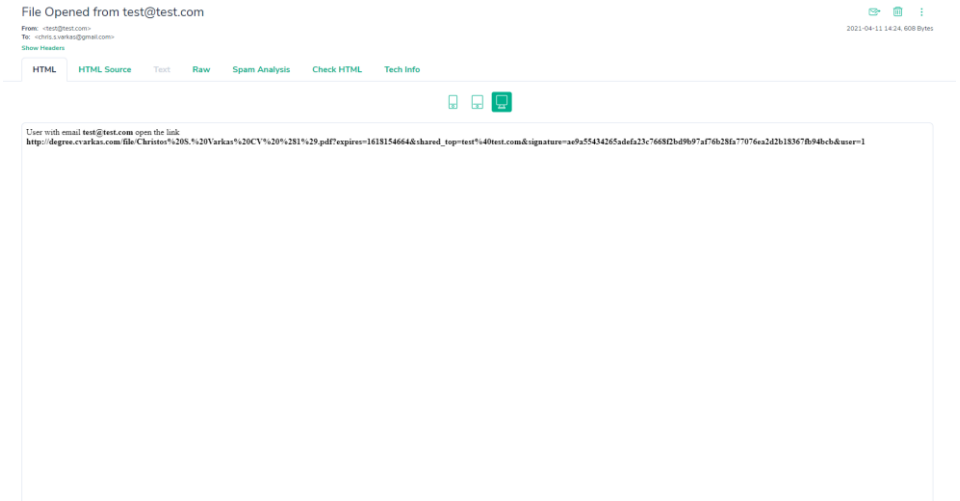


Εικόνα 27 Λεπτομέρειες του Server και του Certificate που έγινε Signed το PDF



Εικόνα 28 Περισσότερες λεπτομέρειες Certificate

Τέλος, όταν κάποιος χρήστης πατήσει το Generated Link που του έχει στείλει (το έχει κάνει share) ένας άλλος χρήστης, τότε ο άλλος χρήστης λαμβάνει email notification που αναγράφει ότι ο χρήστης με το e-mail xxxx@xxx.com έχει ανοίξει το αρχείο xxxx.xxx.



Εικόνα 6 Email που λαμβάνει χρήστης όταν ανοίγει κάποιος που έχει διαμοιραστεί ένα αρχείο μαζί του αναγράφοντας το e-mail του

Κεφάλαιο 6. Συμπεράσματα και μελλοντικές επεκτάσεις εφαρμογής

Η παρούσα διατριβή είχε σαν στόχο να προτείνει ένα σύστημα ασφαλής διαμοίρασης αρχείων από έναν χρήστη σε άλλον το οποίο ακολουθεί τις σύγχρονες απαιτήσεις ασφαλείας των certifications. Συμπερασματικά δίνει απάντηση σε δύο ζητήματα:

1. Διαμοιρασμός αρχείων για συγκεκριμένη χρονική περίοδο σε συγκεκριμένο άτομο
2. Digitally Signed αρχεία με χρήση Digital Certificate Authority για να μη γίνετε από τρίτους κακόβουλη διαμοίραση αρχείων από το πρωτότυπο αρχείο

Θα μπορούσε να είχε κάποιες επιπλέον επεκτάσεις για να γίνει πλήρως λειτουργική εφαρμογή με σκοπό τη χρήση από διάφορες εταιρείες. Μερικές από αυτές τις επεκτάσεις είναι:

- Περισσότερες επιλογές διαμοίρασης και permissions πάνω στο αρχείο που θα έχει το άτομο που του έχει γίνει η διαμοίραση
- Βελτίωση του User Interface καθώς και περισσότερες επιλογές με το τι να κάνουν με αυτά τα αρχεία.
- Ταυτοποίηση στο σύστημα ότι ο εν λόγω χρήστης που επιστρέφει στον Server από το Temporary URL έχει κάποιο Password Protected για την προβολή των αρχείων.

Βιβλιογραφία

Digital.Com Staff. (2021, Οκτώβριος 10). *digital.com*. Ανάκτηση από The Best Digital Signature Software of 2021: https://digital.com/digital-signature-software/

8gwifi.org. (χ.χ.). Ανάκτηση από EC Signature Generate & Verification: https://8gwifi.org/ecsignverify.jsp

Firebit.gr. (2017, Οκτωβρίου 23). *Firebit*. Ανάκτηση από Laravel – 10 σημαντικά πλεονεκτήματα: https://www.firebit.gr/2017/10/23/laravel-%CF%80%CE%BB%CE%B5%CE%BF%CE%BD%CE%B5%CE%BA%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1-%CE%B1%CE%BD%CE%AC%CF%80%CF%84%CF%85%CE%BE%CE%B7-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CF%8E%CE%BD/

GetApp. (χ.χ.). *getapp.com*. Ανάκτηση από PandaDoc vs DocuSign vs signNow vs HelloSign Comparison: https://www.getapp.com/operations-management-software/a/pandadoc/compare/docusign-standard-electronic-signature-vs-signnow-vs-hellosign/

Greene, T. (2014, Μάϊος 30). *networkworld*. Ανάκτηση από Αρχειοθετήθηκε από το πρωτότυπο «Father of SSL says despite attacks, the security linchpin has lots of life left»: https://web.archive.org/web/20140531105257/http://www.networkworld.com/news/2011/101111-elgamal-251806.html

Information Technology Laboratory. (2013, Ιούλιος). *National Institute of Standards and Technology*. Ανάκτηση από Digital Signature Standard (DSS): https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Lerdorf, R. (2012, Ιουλίου 20). *Βικιπαίδεια*. Ανάκτηση από Βικιπαίδεια PHP - «I wonder why people keep writing that PHP was ever written in Perl. It never was. #php»: https://el.wikipedia.org/wiki/PHP#cite_ref-1

Loesch, S. (2019, Απρίλιος 27). *medium.com*. Ανάκτηση από OpenSSL and ECDSA Signatures: https://medium.com/@skloesch/openssl-and-ecdsa-signatures-db60c005b1f4

Messmer, E. (2014, Μάϊος 31). *networkworld*. Ανάκτηση από Father of SSL, Dr. Taher Elgamal, finds fast-moving IT projects in the Middle East: https://web.archive.org/web/20140531105537/http://www.networkworld.com/news/2012/120412-elgamal-264739.html

Netscape. (1997, Ιουνίου 14). *web.archive.org*. Ανάκτηση από Αρχειοθετήθηκε από το πρωτότυπο http://home.netscape.com/: https://web.archive.org/web/19970614020952/http://home.netscape.com/newsref/std/SSL.html

Red Hat. (2014, Οκτωβρίου 21). *https://access.redhat.com/articles/1232123*. Ανάκτηση από «POODLE: SSLv3 vulnerability (CVE-2014-3566)»: https://access.redhat.com/articles/1232123

Wikipedia.org. (2021, Μάϊος 26). *Wikipedia*. Ανάκτηση από Elliptic Curve Digital Signature Algorithm: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

Γεωργιάδης, Χ. Κ. (2015, Οκτώβριος). *ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΠΑΓΚΟΣΜΙΟ ΙΣΤΟ*. Ανάκτηση από repfiles.kallipos.gr: http://repfiles.kallipos.gr/html_books/9536/Chapter%202/Chapter02.html

Ελληνικό Μεσογειακό Πανεπιστήμιο - eClass. (2020, Νοέμβριος 15). *Ασφάλεια Πληροφοριακών Συστημάτων - Διαφάνεια Εργαστηρίου*. Ανάκτηση από SSL / TLS: https://eclass.hmu.gr/modules/document/file.php/TP122/03.%CE%95%CF%81%CE%B

3%CE%B1%CF%83%CF%84%CE%AE%CF%81%CE%B9%CE%B1/Lab%206%20-%20SSL%20%26%20VPN/Lab%206%20-%20SSL.pdf

ΧΡΙΣΤΟΠΟΥΛΟΥ, Ρ.-Ν. (2012, Οκτώβριος 04). *Σχεδίαση και υλοποίηση ασφαλούς υπηρεσίας με χρήση*. Ανάκτηση από Τεχνολογίας Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/6396/1/ECC_Cryptograpfy_v1%203.pdf