Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: ΜΑΡΙΑ ΚΑΡΥΔΑ

Εργαστηριακοί Συνεργάτες: ΔΟΥΜΑ ΑΝΑΣΤΑΣΙΑ

ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

3212017206 Τσότρας Χρήστος

Σάμος, Δευτέρα, 2020

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Κατάλογος Περιεχομένων

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Συντομη περιγραφη της εφαρμογης

Σκοπός της εφαρμογής είναι να παρέχει εναν ασφαλή και εύχρηστο χωρο αποθήκευσης πιστωτικών καρτών, στον οποίο οι χρήστες θα μπορούν να βασίζονται οτι τα δεδομένα τους είναι ασφαλή καθώς:

Το password του χρήστη αφου παραχθει συνοψη αυτου με τυχαιο salt μοναδικο για καθε χρήστη υποκειται κρυπτογράφηση με δήμοσιο κλειδί της εφαρμογής και αποθηκεύεται.

Κατα την διαρκεια της αυθεντικοποιησης του χρηστη(sign in) αποκρυπτογραφειται το password του username που εχει εισαγει ο χρηστης και γινεται η συγκριση των δυο συνοψεων.

Κατα την εγγραφη του χρηστη εκτος απο το μοναδικο salt παραγεται και ενα μοναδικο συμμετρικο κλειδι το οποιο χρησιμοποιουμαι για να κρυπτογραφησουμε/αποκρυπτογραφησουμε οποιαδηποτε πληροφορια εισάγει ο χρηστης

Αφου ο χρηστης συνδεθει στην εφαρμογη επιτυχως του παρουσιαζεται το main menu της εφαρμογης στο οποιο μπορει να περιηγηθει και να διαλεξει λειτουργιες οπως δημιουργια νεας καρτας, εμφανιση ολων των καρτων ενος τυπου καρτας (πχ. VISA).

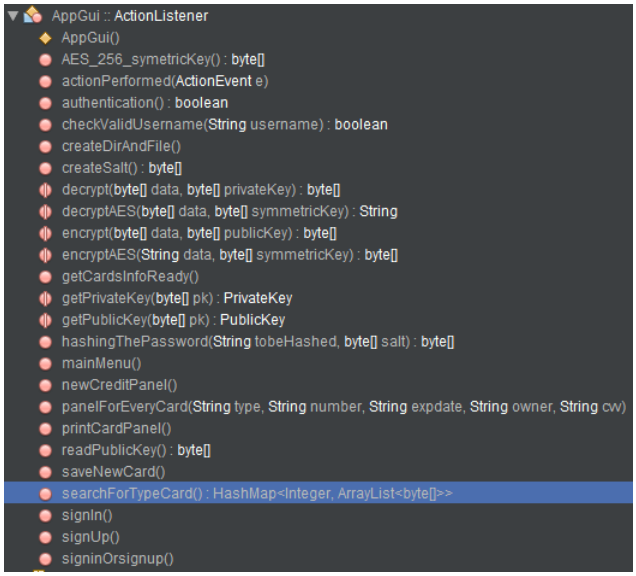
Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Αναφορά των συναρτησεων οπου υλοποιηθηκαν

Το σύνολο των συναρτησεων που υλοποιηθηκαν ειναι 24, και μπορουμε να τις χωρισουμε σε δυο κατηγοριες

- Αυτες που υλοποιουν γραφικα
- Αυτες που υλοποιουν διαδικασιες-λειτουργιες



<u>Υλοποιουν Γραφικά :</u>

1. signinOrsignup()
2. signIn()
3. signUp()
4. mainMenu()
5. newCreditPanel()
6. printCardPanel()
7. panelForEveryCard()

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Υλοποιουν διαδικασίες :

1. checkValidUsername
2. getCardsInfoReady
3. searchForTypeCard
4. saveNewCard
5. createDirAndFile
6. decryptAES
7. encryptAES
8. encrypt
9. decrypt
10. getPrivateKey
11. getPublicKey
12. readPublicKey
13. createSalt
14. hashingThePassword
15. AES_256_symetricKey
16. authentication

Υπαρχει εκτεταμενος σχολιασμος για την καθε λειτουργια καθε συναρτησης στον πηγαιο κωδικα του προτζεκτ σε μορφη σχολιασμου.

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Απαντηση ερωτησεων

1. **Ποιος ο λόγος της χρήσης του salt για την παραγωγή της σύνοψης ενός συνθηματικού;**

   Η ουσιαστική χρήση του salt είναι για την τυχαιοποιηση της παραγωγής της συνοψης

2. **Ποιες είναι κατά την γνώμη σας οι αδυναμίες της συγκεκριμένης εφαρμογής; Περιγράψτε σύντομα τι ευπάθειες μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Προτείνετε μηχανισμούς που κατά την γνώμη σας μπορούν να βελτιώσουν την ασφάλεια που παρέχει η εφαρμογή.**

   Μια απο τις αδυναμιες της εφαρμογης που υλοποιηθηκε ειναι οι χωροι αποθηκευσης οι οποιοι ειναι .txt αρχεια.

   Ενας επιτιθεμενος κατα πασα πιθανοτητα θα μπορουσε να εκμεταλευτει οτι το ονομα του φακελου της καθε καρτας φτιαχνεται με βαση τον αριθμο της καρτας για ευκολοτερη ευρεση, μπορει να το εκμεταλευτει αντλοντας αυτη τη πληροφορια.

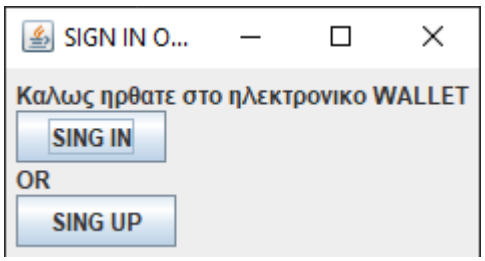
   Κατα τη γνωμη η υλοποιηση της εφαρμογης με τη βοηθεια μιας βάσης δεδομενων για την αποθηκευση θα την καθιστουσε αποδοτικοτερη και σαφως ασφαλεστερη.

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

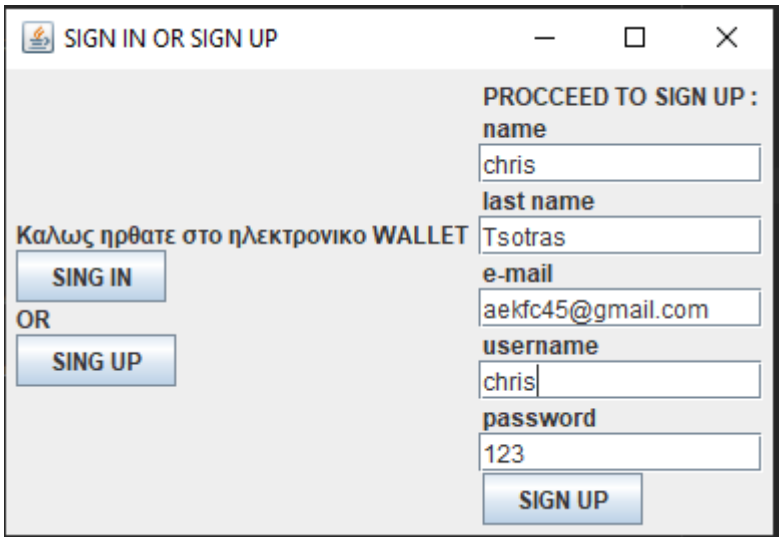
ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Στιγμιοτυπα Οθονης

Αρχικα το πρωτο παραθυρο της εφαρμογης καθοριζει αν εισαι εγγεγραμενος χρηστης η οχι



Αν δεν εισαι εγγεγραμενος χρηστης προχωρας πατωντας signUp

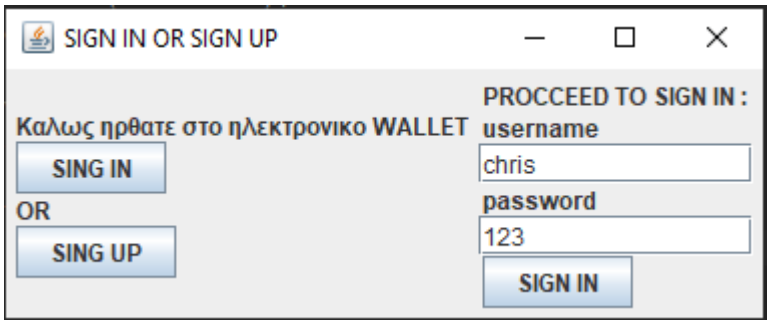


Αφου συμπληρωσεις τα στοιχεια σου πατας το κουμπι sign up

Τίτλος Μελέτης: ΥΛΟΠΟΙΗΣΗ ΜΕ ΧΡΗΣΗ ΚΑΤΑΛΛΗΛΩΝ ΚΛΑΣΕΩΝ ΤΟΥ JAVA API, ΜΗΧΑΝΙΣΜΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ, ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ, ΣΥΝΟΨΗΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

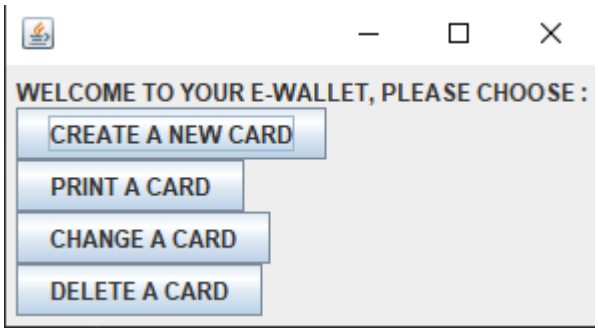
ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

Στη συνεχεια προχωρας στο log in- αυθεντικοποιηση

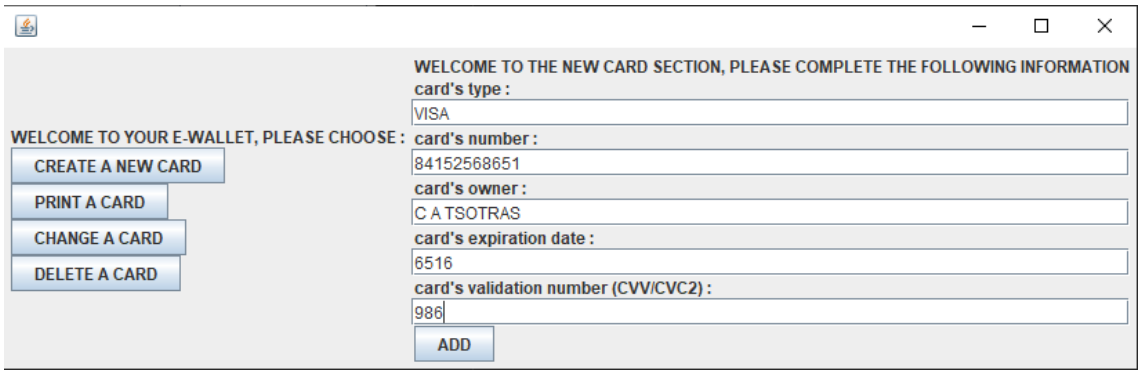


Προσθετεις τα στοιχεια σου και πατας sign in

Και εμφανιζεται το δευτερο παραθυρο της εφαρμογης, το Main Menu

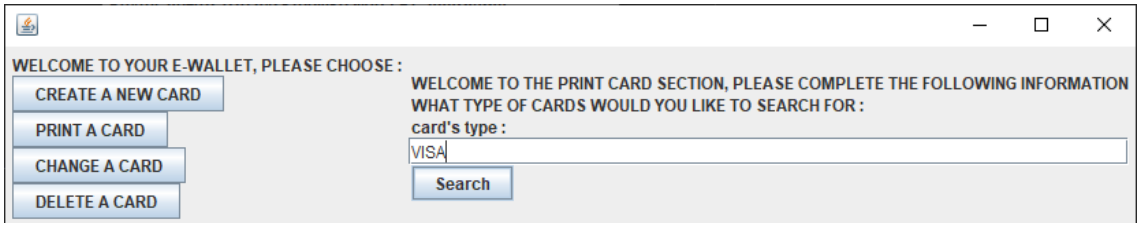


Σε περιπτωση που θες να δημιουργησεις καινουργια καρτα επιλεγεις το CreateNewCard

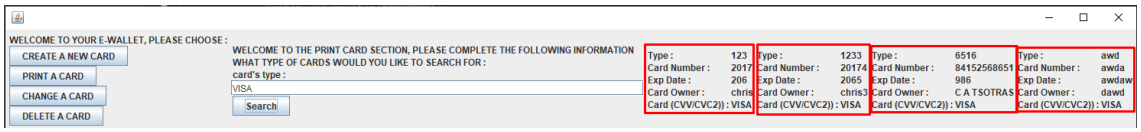


Και αφου συμπληρωσεις ολα τα στοιχεια κανεις ADD την καρτα

Στη συνεχεια υπαρχει η δυνατοτητα να εμφανισεις ολες τις καρτες ενος συγκεκριμενου τυπου καρτας για παραδειγμα VISA



Εαν υπαρχει τετοιος τυπος καρτας καταγεγραμμενος θα εμφανιστουν οι καρτες



Οι λειτουργιες αλλαγη καρτας, και διαγραφη καρτας δεν υλοποιηθηκαν.

ΠΗΓΕΣ

RSA encryption https://www.devglan.com/java8/rsa-encryption-decryption-java

AES 256 encryption https://howtodoinjava.com/security/aes-256-encryption-decryption/