АКАДЕМИЈА ТЕХНИЧКО-УМЕТНИЧКИХ СТРУКОТВНИХ СТУДИЈА БЕОГРАД

ОДСЕК ВИСОКА ШКОЛА ЕЛЕКТРОТЕХНИКЕ И РАЧУНАРСТВА

**Миленковић Ђорђе**

**ЈЕДНА ИМПЛЕМЕНТАЦИЈА СИСТЕМА ЗА ЧУВАЊЕ ЛОЗИНКИ НА ПАМЕТНИМ КАРТИЦАМА**

**- мастер рад -**



Београд, ххх 2021.

Кандидат: **Миленковић Ђорђе**

Број индекса: **РИН-65/17**

Студијски програм: **Рачунарско инжењерство**

Тема: **Једна имплементација система за чување лозинки на паметним картицама**

Основни задаци:

**1. Преглед у област истраживанја**

**2. Пројектовање система за чување лозинки**

**3. Имплементација система за чување лозинки**

Београд, ххх 2021. године. Ментор:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Др Немања Мачек, проф. ВИШЕР

**РЕЗИМЕ:**

ХХХХХХХХХХХХХХХххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххх

**Кључне речи:** ХХХХХХххххххххххххххххххх

**ABSTRACT:**

Ххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххххх

**Key words:** Хххххххххххххххххххххх

САДРЖАЈ

# Увод

Кроз целу историју човечанства, постојала је потреба за сигурном разменом информација. Проблемом сигурне комуникације бавили су се већ Египћани и Индијци пре више од 3000 година и од тада до данас основна идеја се није променила – пренети неку поруку са једног места на друго што је сигурније могуће, тј. направити алгоритам који би омогућио скривање оригиналне поруке тако да буде потпуно (у идеалном случају) неразумљива особама које би неовлашћено дошле у њен посед.

Главна предност смарт картица у односу на друге медијуме за чување података, као што су меморијске картице, је та што омогућавају сигурно чување поверљивих података. Да би се подаци из сигурне меморије на смарт картици прочитали, неопходно је успоставити сигуран канал комуникације између картице и терминала.

Циљ овог рада је приказати један систем за сигурно чување поверљивих података као што су кориснички налози и њихове лозинке на паметним картицама.

# Опис паметних картица

Паметне картице представљају једну од најмањих рачунарских платформи која се данас користи. Иако су веома малих димензија, памерне картице функционишу слично као персонални рачунари јер могу да складиште податке, манипулишу подацима и обављају функције као што су математичке операције, криптографске операције итд. Паметне картице се могу поделити у две форме: контактне и безконтактне. Контактне паметне картице захтевају уметање или дирактан контакт са читачем паметних картица док безконтактне функционишу на принципу магнетног поља и могу да се користе када су прислоњене близу безконтактног читача картица. Паметне картице су највише заступљене у следећим индустријама:

* Телекомуникације (78%)
* Банкарство (7%)
* Здравство (3%)
* Саобраћај и транспорт (2%)
* Остало (10%)

Паметне картице су израђене у потпуности од пластике, осим малог дела предвиђеног за чип картице. Интегрисана кола, или чипови, за паметне картице се производе од силицијумских плочица, баш као и други рачунарски чипови. Ови чипови су везани за алиминијумске површине (да би се обезбедила читљивост) и обложени су у епокси смолом пре уграђивања у пластику картице.

Пошто паметне картице садрже централну процесорску јединицу (ЦПУ), оперативни систем и различите типове меморије на њеном чипу, њихова анатомија је веома слична персоналним рачунарима. Чип једне паметне картице садржи следеће компоненте:

* **Централна процесорска јединица (ЦПУ) –** Централна процесорска јединица чипа паметне картице тумачи и извршава инструкције добијене од оперативног система.
* **Реад Онли Меморија (РОМ) –** Реад онлз меморија складишти податке који се, једним уписани, не могу променити или обрисати. Из тог разлога, произвођачи чипова паметних картица у РОМ меморији чувају оперативни систем картице, као и различите функције тестирања и дијагностике.
* **Рандом аццесс меморз (РАМ) –** РАМ меморија може да складишти и мења податке током једне сесије комуникације са читачем картица. Подаци могу да се уписују, мењају и бришу све док паметна картица има напајање тј. док је повезана са читачем картица. Када се напајање изгуби, сви подаци се трајно губе.
* **Меморија апликације (ЕЕПРОМ) –** За податке који требају бити измењени или обрисани, као што су подаци у апликацији, произвођачи чипова користе избрисиву програмабилну меморију само за читање (ЕЕПРОМ). ЕЕПРОМ меморија је веома слична хард диску персоналног рачунара јер подаци у њој могу остати и након губитка напајања и могу бити модификовани током сесије.

# Java Card платформа

Јава Цард платформа се састоји из два дела. Први део представља АПИ за приступ картици и укључује неке криптографске функције. Други део специфицира Јава Цард Виртуалну Машину (ЈЦВМ) која је дизајнирана као једноставна Јава виртуелна машина у коју је уграђен подскуп Јава програмског језика. Због свог малог меморијског простора, Јава Цард платформа подржава само пажљиво изабран, прилагођен подскуп карактеристика Јава језика. Овај подскуп садржи карактеристике које су прилагођене за писање апликација за паметне картице и друге мале уређаје уз очување објектно оријентисаних принципа Јава програмског језика.

Табела 1.1 приказује неке карактеристике Јава језика прилагођеног за паметне картице и Јава језика опште намене.

|  |  |  |
| --- | --- | --- |
| **Функција** | **Јава Цард** | **Јава** |
| Клонирање класа | Не | Да |
| Клонирање објеката | Не | Да |
| Целобројна вредност дужине 4 бајта | Опционо | Да |
| Податак типа boolean, byte, short | Да | Да |
| Податак типа long, float, double, character | Не | Да |
| Динамично преузимање класа | Не | Да |
| Динамично управљање меморијом | Не | Да |
| Динамично креирања објеката | Да | Да |
| Управљање изузецима | Да | Да |
| Поља објеката | Да | Да |
| Низови | Само једнодимензионални | Једнодимензионални и дводимензионални |
| Интерфејси | Да | Да |
| Оператори | Сви | Сви |
| Пакети | Да | Да |
| Нити | Не | Да |
| Виртуалне методе | Да | Да |

Табела 1.1. Ограничења ЈаваЦард платформе у односу на Јава језик опште намене

## Развој програма за ЈаваЦард платформу

Улога ЈаваЦард виртуелне машине се најбоље може објаснити у контексту процеса развоја софтвера за ЈаваЦард платформу. Постоји неколико компоненти које чине ЈаваЦард систем а то су ЈаваЦард виртуелна машина, Конвертер за ЈаваЦард платформу, инсталациони алат за инсталирање програма на картицу и сам програм који се покреће на паметној картици, као што је приказано на сликама 3.1 и 3.2.

  
Слика 3.1. ЈаваЦард Платформа

  
Слика 3.2. ЈаваЦард Платформа

Развој ЈаваЦард програма почиње као и било који други Јава програм: програмер пише једну или више Јава класа, компајлира изворни код стварајући једну или више .цласс датотека. Програм се развија, тестира и покреће на персоналном рачунару у развојном окружењу које представља симулацију за емулацију паметне картице. Затим кад је аплет спреман за инсталирање на паметну картицу, .цласс датотеке се конвертују у ЦАП (конвертовани аплет) датотеку помоћу ЈаваЦард конвертора.

ЈаваЦард конвертор прима .цласс датотеке, из једног или више Јава пакета, као улазне податке и креира ЈаваЦард ЦАП фајл. ЈаваЦард ЦАП фајл садржи само пакете аплета, само библиотеке пакета које се користе у пројекту или комбинацију пакета аплета или библиотека. Поред тога, пакети аплета или библиотека у ЈаваЦард ЦАП фајлу могу бити јавни или приватни.

Поред .цласс датотека, ЈаваЦард конвертор као улазне параметре прима и извозне фајлове (.exp фајлове). Један извозни фајл садржи информације о садржају других пакета које конвертоване класе импортују. Извозне датотеке се не учитавају на паметну картицу и интерпретер на паметним картицама их директно не користи. Оне се користе у сврхе верификације и повезивања. Садрже потписе метода и поља класа док не садрже бајткод.

Након конверзије, ЦАП фајл је спреман за инсталирање на паметну картицу. За инсталирање аплета на паметну картицу користи се посебан програм који се покреће на персоналном рачунару. Неопходно је да читач картица буде повезан са рачунаром и да картица буде конектована са читачем картица. Програм учитава ЦАП фајл и и шаље одговарајуће команде на паметну картицу. Паметна картица прима команде које између осталог представљају садржај ЦАП фајла припрема и инсталира аплет за покретања од стране ЈаваЦард виртуалне машине. Виртуелна машина не захтева прихватање и манимпулацију ЦАП фајлом. Она само извршава програм на паметној картици након што је аплет успешно инсталиран.

## ЈаваЦард аплети

ЈаваЦард аплете не треба мешати са Јава аплетима само зато што деле исто име. ЈаваЦард аплет је Јава програм.