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 | Једнодимензионални | Мултидимензионални |
| Интерфејси | Да | Да |
| Оператори | Сви | Сви |
| Пакети | Да | Да |
| Нити | Не | Да |
| Виртуалне методе | Да | Да |

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

## Развој програма за JavaCard платформу

Улога JavaCard виртуелне машине се најбоље може објаснити у контексту процеса развоја софтвера за JavaCard платформу. Постоји неколико компоненти које чине JavaCard систем а то су JavaCard виртуелна машина, Конвертер за JavaCard 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. JavaCard Платформа

  
Слика 3.2. JavaCard Платформа

Развој JavaCard 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 CAP (конвертовани аплет) датотеку помоћу JavaCard конвертора.

JavaCard конвертор прима .цласс датотеке, из једног или више Јава пакета, као улазне податке и креира JavaCard CAP фајл. JavaCard CAP 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 JavaCard CAP фајлу могу бити јавни или приватни.

Поред .цласс датотека, JavaCard 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, CAP 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 CAP фајл и и шаље одговарајуће команде на паметну картицу. Паметна картица прима команде које између осталог представљају садржај CAP фајла припрема и инсталира аплет за покретања од стране JavaCard виртуалне машине. Виртуелна машина не захтева прихватање и манимпулацију CAP фајлом. Она само извршава програм на паметној картици након што је аплет успешно инсталиран.

## JavaCard аплети

JavaCard аплете не треба мешати са Јава аплетима само зато што деле исто име. JavaCard аплет је Јава програм који се покреће и извршава на паметној картици. Он није намењен за покретање у интернет прегледачу као што су за то намњени обични Јава аплети. За разлику од многих ембеддед система, ЈаваЦард аплети не морају да се учитавају у РОМ меморију.

Главна класа аплета мора наследити класу javacard.framework.Applet класу. Основна класа Апплет је супер класа за све инсталиране аплете који се налазе на паметној картици. Аплет који ради на картици је заправо инстанца главне класе аплета. Сваки аплет садржи свој идентификациони број и његов пакет садржи свој идентификациони број. Помоћу ових идентификационих бројева, програм који комуницира са картицом зна који аплет треба да покрене.

ЈаваЦард окружење подржава рад са више аплета на паметној картици. На једној паметној картици може постојати више аплета, а један аплет може имати више инстанци. На пример једна инстанца аплета за новчаник може да креира објекат за амерички долар, а други за британску фунту.

# Комуникација са паметном картицом

Предуслов за све интеракције између паметне картице и рачунара је комуникација између две стране. Са конвенционалним протоколима ИСО/ИЕЦ Т = 0 и Т = 1, само једна комуникациона линија је доступна за то. Ова веза чини основу за размену података између паметне картице и рачунара. Будући да постоји само једна линија, терминал и паметна картица морају да комуницирају наизменично, при чему супротна страна делује као пројемник. Овај процес наитменичног преноса и пројема назива се полу-дуплекс комуникација. Потпуна дуплекс комуникација, у којој обе стране могу истовремено да преносе и примају податке, тренутни није имплементирана у свету паметних картица.

Комуникацију са картицом увек иницира терминал. Картица увек реагује на команде примљене са терминала, што значи да картица никад не шаље податке без спољног иницирања. Ово резултира чистим односом мастер – слејв, са терминалом као мастер и картицом као слејв. Након што је паметна картица обрадила команду која јој је послата и одговор послала терминалу, враћа се у стање мировања. У овом стању је може пробудити само друга наредба послата са терминала. Овакав тип комуникације је приказан на слици 4.1.

  
Слика 4.1. Стање паметне картице током активирања и комуникације са терминалом

## АПДУ протокол

АПДУ протокол се користи за размену свих података између паметне картице и терминала. АПДУ је акроним од Application Protocol Data Unit, који означава међународно стандардизовану јединицу података слоја апликације. Постоји разлика између АПДу команде (Ц-АПДУ) које представљају наредбе послате на картицу и АПДУ одговора (Р-АПДУ) које представљају одговоре на наредбе које картица враћа. АПДУ команда се протоколом преноса транспарентно преноси, што значи без модификације. АПДУ команде су у складу са ИСО/ИЕЦ 7816-4 стандардом дизајниране тако да буду независне од преносног протокола. Сходно тома, садржај и формат АПДУ команде може остати непромењен када се користи другачији протокол преноса.

Као што је приказано на слици 4.2. АПДУ команда се састоји од заглавља и тела. Тело може имате променљиву дужину или може бити потпуно одсутно ако је поље за податке празно. Заглавље се састоји од 4 елемента: бајта класе (ЦЛА), бајта инструкције (ИНС) и два бајта параметра (П1 и П2). Бајт класе се такође користи за идентификацију апликација. Бајт класе се може користити и као идентификатор да су подаци који се шаљу АПДУ командом шифровани.



Слика 4.2. Структура АПДУ команде

Други бајт у заглављу АПДУ команде је бајт инструкције (ИНС). Тај бајт означава функцију коју аплет треба да изврши. Два бајта параметра (П1 и П2) примарно се користе за пружање више информација за функцију изабрану бајтом инструкције. На пример једна функција може у зависности од прослеђених параметара П1 и П2 уради једну или другу ствар. Након заглавља следи тело АПДУ команде које може бити празно изузев параметра за дужину тела поруке и параметра за дужину података који се враћају са картице. Параметар за дужину (ЛЦ поље) одређује дужину података који ће бити послати АПДУ командом. Параметар за дужину (ЛЕ поље) одређује очекивану дужину података који се враћају са картице. Поред параметара за дужину, тело се састоји од поља за податке који се шаљу на картицу. Ако је вредност ЛЕ поља „00“, терминал не очекује да ће картица вратити податке.

Поља ЛЦ и ЛЕ обично имају дужину од једног бајта, али се могу претворити у поља дужине три бајта у зависности од потребе. Ово омогућава да се одреде дужине до 65536 бајтова. Стандард дефинише ову спецификацију дужине три бајта као резервисану за будућу употребу. Међутим, већ постоје неки оперативни системи паметних картица са великим простором меморије који подржавају спецификације дужине три бајта. Претходно описани елементи АПДУ команде се могу комбиновати са 4 случаја који су приказани на слици 4.3.

  
Слика 4.3. Четири могуће варијанте АПДУ команде

АПДУ одговор који картица шаље као одговор на АПДУ наредбу се састоји од обавезног заглавља и опционог тела, као што је приказано на слици 4.4.

  
Слика 4.4. Структура АПДУ команде као одговор са паметне картице

Тело одговора се састиоји од поља података чија је дужина одређена ЛЕ пољем претходне АПДУ команде.