Универзитет у Крагујевцу

Факултет инжењерских наука у Крагујевцу

Назив студијског програма: Машинско инжењерство
Ниво студија: Основне академске студије
Модул: Информатика у инжењерству
Предмет: Архитектура рачунарских система
Број индекса: 742/2010

Дарко Ж. Браковић

Смарт картице

завршни рад

Комисија за преглед и одбрану:

1. **Др. Јасна Радуловић - ментор**
2. _____ Датум одбране:_____
3. _____ Оцена:_____

У оквиру овог завршног рада кандидат треба да проучи препоручену и ширу литературу која се односи на системе смарт картица. На бази усвојеног знања кандидат треба да обради типове картица, њихове карактеристике преко физичких и електричних својстава као и да напомене оперативне системе смарт картица и протоколе за пренос података.

Препоручена литература:

[1] U.S. General Services Administration (2004) “Government smart card handbook” Smart Card Alliance 191 Clarksville Road, Princeton Junction, New Jersey 08550 (USA)

[2] Yahya Haghiri., Thomas Tarantino (2002). ”Smart Card Manufacturing”, John Wiley & Sons, Ltd Baffins Lane, Chichester West Sussex, PO 19 1 UD, England

[3] Wolfgang R., Wolfgang E (2002). ”Smart card handbook, third edition”, John Wiley & Sons, Ltd Baffins Lane, Chichester West Sussex, PO 19 1 UD, England

Крагујевац, новембар 2011

ментор:
Др. Јасна Радуловић

_____

Резиме рада:

У овом раду приказан је развој картица од најосновнијих до смарт картица. Разматране су области примене као и типови картица које су у употреби. Јединствени контакт смарт картице може да се програмира са више банкарских акредитива, правом на медицинску заштиту, возачку дозволу, право на јавни превоз, програм безбедности, чланство у клубу и сл.

Посебна пажња је посвећена физичким и електричним својствима картице, те информатичким основама, самом оперативном систему смарт картице и систему датотека као и комуникацијским протоколима између терминала и смарт картица.

У овом раду су објашњене карактеристике смарт картица и будући и садашњи разлози за њихову све већу примену. Смарт картице побољшавају удобност употрбе on line трансакција и њихову сигурност.

Рад представља садашње стање техничког знања, у областима које тренутно пролазе кроз брзе промене.

Кључне речи: оперативни систем, протоколи, меморија, чипови, микроконтролери, датотеке, кодирање

Summary of work:

This paper presents the development of the basic cards to smart cards. Discussed are the application areas and types of cards in use. Unique contact smart card can be programmed with several banking credentials, the right to medical care, driver's license, the right to public transportation, safety program, club membership and so on.

Special attention was paid to the physical and electrical properties of the card, and IT basics, the smart card operating system and file system as well as the communication protocol between the terminal and the card.

In this paper are presented the characteristics of smart cards and future and present reasons for their growing use. Smart cards enhance the benefits upotrbe on-line transactions and their safety.

Work represents a current state of technical knowledge in areas that are currently going through rapid changes.

Keywords: operating systems, protocols, memory chips, microcontrollers, data files, coding

Садржај

Резиме рада …….. 3
Summary of work 3

Садржај ……. 4
Увод ……... 6

Део 1
1. Увод у смарт картице 7
1.1 Историјат смарт картица …….. 7
1.2 Стандрдизација …….. 8
Део 2
2. Типови картица и области примене ……. 9
2.1 Рељефне картице ……..... 9
2.2 Картице са магнетном-траком ……. 10
2.3 Смарт (паметне) картице …….. 11
2.3.1 Контактне картице ……... 12
2.3.1.1 Меморијске картице …….. 13
2.3.2 Микропроцесорске картице ……. 14
2.3.2.1 Микроконтролери смарт картица …… 15
2.3.2.2 Типови процесора ……. 16
2.3.2.3 Врсте меморија …….. 16
2.3.3 Бесконтактне смарт картице …… 17
2.3.4 Оптичке меморијске картице …….. 21
Део 3
3. Физичке и електричне особине 22
3.1 Физичке особине 22
3.1.1 Формати картица 23
3.1.2 Компоненте картица и безбедносне функције ... 25
3.2 Тело картице …….. 27
3.2.1 Материјали картица 28
3.2.2 Кућишта чипова 29
3.2.2.1 Електрична веза између чипа и кућишта 29
3.2.2.2 TAB кућишта ……. 29
3.2.2.3 Кућиште савитљивог чипа …… 30
3.2.2.4 Кућиште са оловним рамом 31
3.2.2.5 Процес површинског чипа 31
3.3 Електрична својства 32
3.3.1 Електричне везе 32
3.3.2 Напајање 33
3.3.3 Снабдевање струјом …….. 33
3.3.4 Спољашњи генератор такта ……. 34
3.3.5 Секвенце активације и деактивације ……... 34

Део 4

4. Информатичке основе ……. 35
4.1 Структуирање података …… 35
4.1.1 Кодирање алфанумеричких података 36
4.2 Детекција грешака и кодови корекције 37
4.2.1 Исправљање грешке 39
4.3 Компресија података 40
4.4 Криптографске могућности 41
4.4.1 Дигитални потпис и дигитални сертификат ….. 42
4.5 Оперативни системи смарт картица 43
4.5.1 Организација меморије 45
4.5.2 Датотеке смарт картица …… 45
4.5.2.1 Типови датотека 46
4.5.2.2 Имена датотека 47
4.6 Пренос података смарт картица 48
4.6.1 Одговор на ресет (ATR) 48
4.6.2 Селекција параметра протокола (PPS) 49
4.6.3 Протоколи за пренос података …… 50
4.6.3.1 T = 0 преносни протокол 50
4.6.3.2 T = 1 преносни протокол 52
4.6.3.3 T = 14 преносни протокол и USB протокол 53
4.6.3.4 Структура поруке APDU 53
Закључак …….. 55
Литература 56

Увод

У овом раду ће кроз четири поглавља бити приказан развој смарт картица и разлози за њихову све већу примену, као и области у којима се примењују. У трећем делу се разматрају физичке и електричне особине смарт картица, док четврто поглавље говори о информатичким основама смарт картица.

Смарт картице побољшавају удобност и сигурност сваке трансакције. Оне пружају складиштење корисничких налога и идентитета. Системи смарт картица показали су се као поузданији од других машински читљивих картица, као што је магнетна трака или баркод. Смарт картице такође пружају виталне компоненте система безбедности за размену података кроз практично било који тип мреже. Оне су заштита од безбедносних претњи, као и од непажљивог складиштења лозинки корисника на хакерске системе. Трошкови управљања лозинкама за организације или предузећа су веома високи, што чине смарт картице исплативим решењем у овим срединама. Мултифункционалне картице се такође могу користити за управљање приступом мрежним системима и чување вредности и других података. Широм света, људи користе смарт картице за широк спектар свакодневних задатака. Предност смарт картица је директно повезана са количином информација и апликација који су програмирани за коришћење.

Смарт картица неумољиво продире у нове области нашег свакодневног живота. Најновије увођење картица осигурања и приступних картица за мобилне телефоне значи да је смарт картица постала природни саставни део модерног живота. Смарт картица се сматра погодним средствима, која могу послужити за заштиту појединца у данашњим веома сложеним системима.

Могућности примене смарт картица су широко распрострањене. Оне покривају велике различите апликације, нпр безбедносни услов приступа областима, рачунарима и приступ овлашћеним за трансакцијама и заштита података у јавној комуникацији (Интернет) и приватној (интранет) мрежи.

Различите примене смарт картица за одређене области захтевају стално напредовање. Ово је посебно случај за повећање интелигенције и перформанси смарт картица за бољу заштиту података власника у мрежама јавне комуникације.

Овај рад је покушај да се затвори јаз водећи читаоца корак по корак кроз развој смарт картица од идеје до пластике. Желим да истакнем да је већина решења заступљена у овом раду заштићена патентима. За комерцијалну употребу ових решења треба узети у обзир правну ситуацију.

1. Увод у смарт картице

Данашње друштво еволуира у информатичко друштво. Технологија постаје алат у служби информације, а информација знање, моћ и новац. У данашњем свету технологија је све више присутна у свакодневном раду и јављају се многе нове услуге са циљем да нам се „олакша“ живот. Типичан пример је спајање рачунара и мобилних телефона у један уређај. Какве то везе има са паметним картицама? Принцип је исти! Разни пружаоци финансијских, туристичких, и других услуга могу увелико профитирати обједињавањем система аутентификације. У пракси то значи да корисник са једном паметном картицом користи различите услуге. Иста картица може се користити као електронски новчаник за плаћање на разним аутоматима, наплату јавног превоза, аутентикацију приликом приступа свом банковном рачуну или некој зони где је приступ ограничен, [3].

Највеће светске финансијске организације су удружиле своје знање и ресурсе у циљу примене картица у системима плаћања. Мобилна телефонија преко GSM-а створила је велико подручје примене картица. Па ипак иако телекомуникациона и финансијска индустрија представљају највеће системе картица, они не одређују есенцијална својства картица већ их само користе, [2].

Од свог оснивања, смарт картице су показале да су веома корисне као трансакционо, ауторизацијско и идентификационо средство у европским земљама. Са повећањем способности, оне могу постати ултимативни "танки клијент" који замењује све ствари које смо до сада носили у нашем новчанику, укључујући готовину, па чак и породичне фотографије. Како користе разне идентификацијске сертификате, смарт картице се могу користити за добровољну идентификују, без обзира на то где смо и на којој рачунарској мрежи, [12].

1.1 Историјат смарт картица

Ширење пластичних картица је започело почетком 1950-их. Ниска цена синтетичких материјала од PVC-а је омогућила производњу робусних, издржљивих пластичних картица које су много погодније за свакодневну употребу од папирнатих и картонских картица које су се раније користиле, и које нису могле на адекватан начин да издрже механичка напрезања и климатске ефекте.

Прва пластична платна картица за општу употребу је издата од стране Diners club 1950. Била је намењена за високу класу појединаца, омогућавајући власнику да плати његовим "добрим именом" уместо кешом. У почетку, само одређени ресторани и хотели су прихватили ове картице, тако да је овај тип картице постао познат као картица за "путовања и забаве", [3].

Данас, кредитне картице омогућавају путницима да купују без новца свуда у свету. Употреба кредитних картица такође елиминише досадан задатак размене валуте, када смо у иностранству. Ове јединствене предности помогле су кредитним картицама да се наметну. Стотине милиона картица су произведене и издају се годишње.

У почетку, функције ових картица су биле прилично једноставне. Служиле су за складиштење података. Опште информације, су штампане на површини, док су лични подаци, утискивани. Многе картице су такође имале панел за потпис, где је корисник картице могао оставити своје име. У картицама прве генерације, заштита од

фалсификовања била је омогућена визуелним карактеристикама, као што су сигурносна штампа и панел за потпис. Са повећањем ширења коришћења картица, ове прилично основне функције више нису биле довољн, [13].

Са општим ширењем електронске обраде података, дисциплина криптографија доживела је неку врсту квантног скока. Модеран хардвер и софтвер омогућили су спровођење сложених, софистицираних математичких алгоритама који су омогућили неупоредиво већи ниво безбедности.

Смарт картица се показала као идеални медиј. Висок ниво безбедности (на основу криптографије) доступан је свима, јер се могао безбедно сачути тајни кључ и извршити криптографски алгоритам. Поред тога, смарт картице су толико мале и лаке за руковање да су се могле преносити и користи свуда, свако у свакодневном животу. То је била природна идеја да покушај да се користе ове нове безбедносне функције за банкарске картице, са циљем да се суоче са безбедносним ризицима који произилазе из повећања употребе картице са магнетном траком.

Француске банке су прве увеле ову технологију 1984, након пробе са 60.000 картица у 1982-83. Било је потребно још 10 година пре него што су све француске банкарске картице имале чипове. У Немачкој, прва проба на терену одржана је 1984-85, користећи мултифункционалне платне картице које садрже чип.

Електронски новчаник показао се као још један велики фактор у промовисању међународне употребе паметних картица за финансијске трансакције. Плаћања путем интернета понудила су нове и перспективне области примене за електронски новчаник. Смарт картице могу да играју одлучујућу улогу у обезбеђивању одговора на ове проблеме.

. Тренутно, смарт картице се користе у здравственим секторима у многим земљама. Висок степен функционалне флексибилности смарт картице, који чак дозвољава програме за нове апликације, је отворио потпуно нову примену у областима које се протежу изван граница традиционалних картица. Смарт картице се такође користе као "електронске карте" за локални јавни превоз у многим градовима широм света. Бесконтактне смарт картице се обично користе за такве апликације, јер су посебно погодне и кориснички пријатне, [5].

1.2 Стандрдизација

Предуслов за светски продор смарт картица у свакодневном животу, у облику телефонске картице, картице здравственог осигурања и банковних картица, је био стварање националних и међународних стандарда. Смарт картица је обично једна компонента комплексног система. То значи да интерфејс између картице и остатка система мора бити прецизно специфициран. Наравно, ово би могло да се уради за сваки систем од случаја до случаја, без обзира на друге системе. Међутим, то би значило да ће други тип смарт картице бити потребан за сваки систем. Корисници би тако морали да носе посебне картице за сваку апликацију. Да би се ово избегло, генерисани су стандарди који омогућавају мултифункционалним картицама да се развију

ISO/IEC стандарди су посебно значајни за смарт картице, јер су дефинисали основне особине смарт картица. ISO је Међународна Организација за Стандардизацију, док IEC означава Међународну Комисију за Електротехнику. Такође је значајан и Европски Национални Комитет CEN, [5].

Међународна стандардизација смарт картица

Међународни стандарди за смарт картице су развијене под покровитељством ISO/ IEC, као и на европском нивоу од стране CEN-а. Слика показује преглед структуре релевантних радних група и стандарде за које су одговорни. Ови стандарди заснивају се на претходним ISO стандардима у 7810, 7811, 7812 и 7813 породици, који дефинишу својства идентификационе картице у ID-1 формату. Ови стандарди укључују рељефне картице и картице са магнетним тракама, које сви знамо у форми кредитних картица.

Компатибилност са овим постојећим стандардима је критеријум од самог почетка у развоју стандарда за паметне картице, у циљу обезбеђивања глатке транзиције из рељефних картица и картица са магнетном траком у смарт картице. Таква транзиција је могућа зато што све функционалне компоненте, као што су утискивање, магнетне траке, контакти и компоненте за бесконтактне интерфејсе, могу бити интегрисани у једну картицу.

У последњих неколико година, све већи број спецификација је припремљено и објављено од стране привредних организација и других не јавних група, без покушаја да се укључе у активности стандардизације ISO. Аргументи за овај начин рада је начин на који функционише ISO који је сувише спор да одржи корак са иновационим циклусима информатике и телекомуникацијске индустрије, [1].

2. Типови картица и области примене

Ово поглавље даје преглед различитих типова картица, јер је комбинација различитих функција од посебног интереса за многе примене, а посебно када се картице које се користе у постојећим системима (као што су картице са магнетном траком) требају заменити смарт картицама. У таквим случајевима, обично није могуће заменити постојеће инфраструктуре (као што су терминали картица са магнетном траком) од стране нове технологије преко ноћи.

Решење овог проблема углавном се састоји од издавања картице са магнетним тракама и чиповима, за употребу у току прелазног периода. Такве картице се могу користити за обе врсте терминала (стари и нови). Наравно, нове функције које су могуће само са чипом, не могу се користити на терминалу који подржава само картице са магнетном траком, [3].

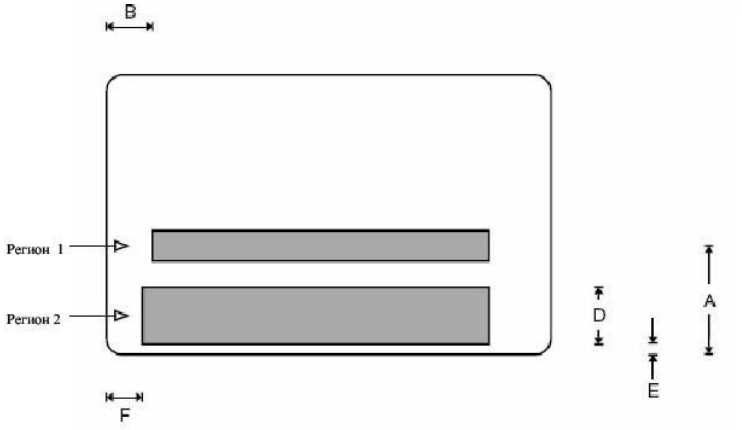
2.1 Рељефне картице

Утискивање је најстарија техника за додавање машински читљиве функције. Рељефни карактери на картици се могу пренети на папир користећи једноставан, јефтин уређај, и они се такође могу лако визуелно прочитати (од стране људи). Место утискивања је наведено у ISO 7811 стандарду. Овај стандард, који је подељен на пет делова, бави са магнетним тракама, као и утискивањем.

ISO 7811 део 1 прецизира услове за рељефне карактере, укључујући и њихов облик, величину и висину утискивања. Део 3 дефинише прецизно позиционирање знакова на картици и дефинише два одвојена региона. Регион 1 је резервисан за идентификациони

број картице, који идентификује картицу издаваоца, као и власника картице,. регион 2 је резервисан за додатне податке који се односе на власника картице, као што су његово име и адреса, [11].

На први поглед, пренос информација помоћу форме за штампу са рељефним карактерима може да изгледа прилично примитивно. Међутим, једноставност ове технике је допринела ширењу кредитне картице широм света, чак и у земљама у развоју. Ова технологија не захтева коришћење електричне енергије, ни везу са телефонском мрежом.



Слика 2.1 Рељефна локација.
Регион 1 је резервисан за ID број (19 карактера), регион 2 је резервисан за име власника картице и адресу (4×27 карактера). A = 21.42 ± 0.12 mm, B = 10.18 ± 0.25 mm, D = 14.53 mm, E = 2.41−3.30 mm, F = 7.65 ± 0.25 mm [16]

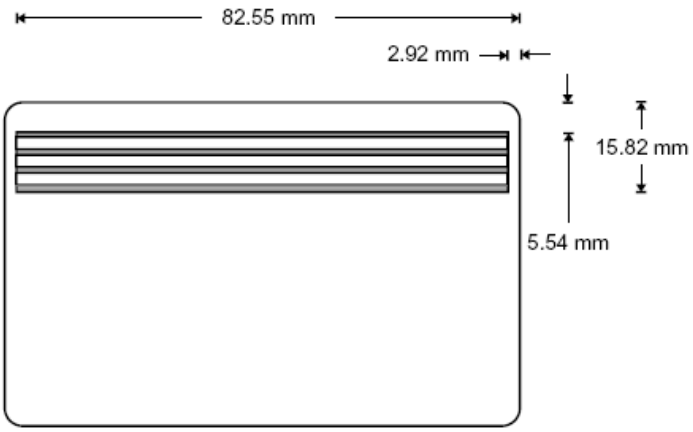
2.2 Картице са магнетном-траком

Основни недостатак рељефних картица је у томе што њихова употреба ствара поприличан број признаница, које су скупе. Једно од решења за овај проблем је дигитално кодирање података са картице на магнетну траку која се налази на полеђини картице. Магнетна трака се чита провлачењем преко главе за читање, било ручно или аутоматски, за податке који се читају и чувају електронским путем, [16].

Делови 2, 4 и 5 ISO стандарда 7811 одређују својства магнетне траке, технике кодирања и локације магнетних трака. Магнетна трака може да садржи до три стазе. Стазе 1 и 2 су предвиђене да буду само за читање, док стаза 3 може бити и за писање.

Иако је капацитет магнетне траке око 1000 бита, што није много, ипак је више него довољно за складиштење информација садржаних у рељефу. Додатни подаци се могу читати и бити написани на стази 3, као што је то случај са кредитним картицама.

Главни недостатак технологије магнетних трака је тај што се подаци могу веома лако да се мењају. Манипулација рељефним карактерима захтева најмање одређену количину спретности.. Насупрот томе, подаци забележени на магнетну траку могу се мењати релативно лако коришћењем стандардних уређаја, а тешко је касније доказати да су подаци измењени. Поред тога, картице са магнетном траком се често користе у аутоматској опреми у којој визуелна инспекција није могућа, као што су банкомати. Потенцијални криминалац, са прибављеним важећим личним подацима, може лако да користи дуплирану картицу у таквим машинама без надзора, без потребе да се фалсификују визуелне безбедносне функције, [12].



Слика 2.2 Локација магнетне траке на ID-1 картици [16]

2.3 Смарт (паметне) картице

Термин смарт картица везује се за картицу која садржи полупроводнички уређај (чип) и линк за пренос података између смарт картица и читача смарт картице. Ова веза може бити успостављена путем спољашњих контакта. Осим тога, веза може и да се одвија без видљивих контакта такозване бесконтактне смарт картице. Бесконтактни пренос података може бити индуктивно реализовати преко антене, капацитивно са кондензаторима, оптички са опто спојницом или другим физичким ефектом, [3].

Смарт картице нуде неколико предности у односу на картице са магнетном траком. На пример, максимални капацитет смарт картице је много већи од картице са магнетном траком.

Једна од најважнијих предности смарт картица је да се подаци чувају од неовлашћеног приступа и манипулације. Пошто се подацима може приступити само преко серијског интерфејса који контролише оперативни систем и безбедносна логика, поверљиви подаци се могу чувати и бити написани на картицу на начин који спречава читање изван картице. Таквим поверљивим подацима може приступити само процесорска јединица чипа. У принципу, и хардвер и софтвер механизми могу да се користе да се ограничи коришћење складиштења функција писања, брисања и читања података и везати их специфичним условима. Ово омогућава да се конструишу разни безбедносни механизми, који могу такође бити прилагођени специфичним захтевима одређене апликације. Неке додатне предности смарт картица су висок степен поузданости и дуг живот у поређењу са картицама са магнетном траком, чији је корисни век трајања генерално ограничен на једну или две године, [12].

Смарт картице се могу поделити у две групе, које се разликују у функционалност и цени на:

- контактне картице
- безконтактне картице

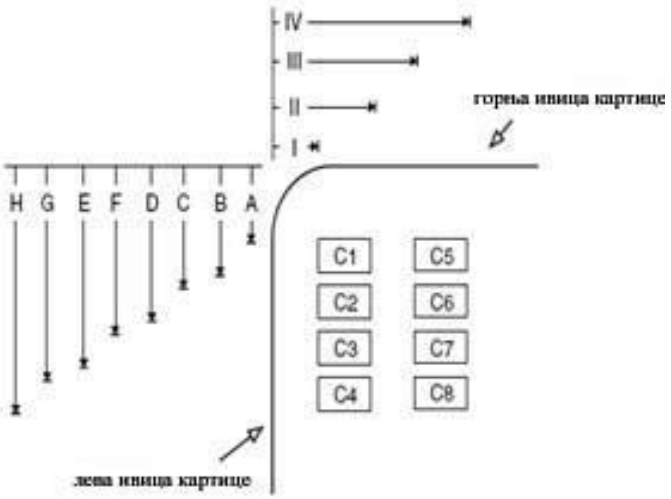
Постоји и подела међу контактним картицама на:

- меморијске картице
- микропроцесорске картице

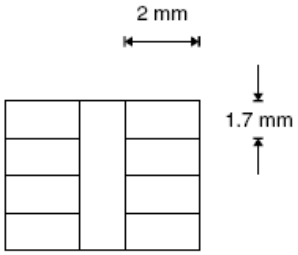
2.3.1 Контактне картице

Значајна компонента контактне смарт картице је тело картице, чип и спољашњи контакати. Слика шематски приказује заједничку верзију контактне смарт картице. Шупљина се производи у телу картице, на пример, глодањем. У ову шупљину се чип везује лепком. Ако се контакти користе за напајање и функције преноса података, електричне везе су обавезне. Састоје се од шест или осам позлаћених контакта, што се може видети на свакој стандардној смарт картици. Локација ових контаката је у складу са телом картице и интернационалним стандардима, [2].

Слика 2.3 Шематска структура контактне смарт картице [2]



Слика 2.4 Позиција контаката у односу на нацрт тела картице [16]

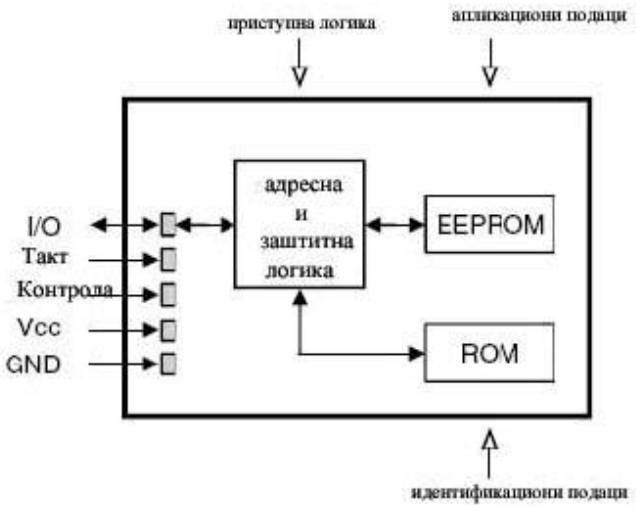


Слика 2.5 Минимална димензија контакта [16]

2.3.1.1 Меморијске картице

Подаци који су потребни од стране апликације се чувају у меморији, која је обично EEPROM. Приступ меморији контролише безбедносна логика, која се у најједноставнијем случају састоји само од заштите писања и брисања у меморију или неке од региона меморије. Међутим, ту су и меморијски чипови са сложенијим безбедносним логикама који могу да обављају једноставна шифровања. Подаци се преносе до и од картице преко U/I порта. Део 3 ISO 7816 стандарда дефинише посебне синхроне протоколе преноса који омогућавају да имплементација чипова буде посебно једноставна и јефтина.

Функционалност меморијске картице је обично оптимизована за одређену апликацију. мада ово озбиљно ограничава флексибилност картице, што их чини прилично јефтиним, [3].



Слика 2.6 Типична архитектура контактне меморијске картице са безбедносном логиком [16]

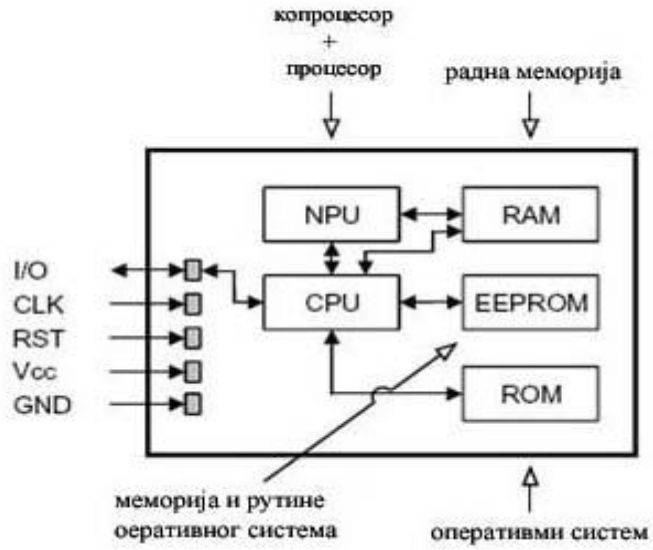
Ове картице су припејд, са вредностима које се чувају електронским путем на чипу, које би се смањиле за износ накнаде позива сваки пут када се картица користи. Све што ће корисник морати да уради је да сними те податке који се налазе у време куповине и препише их на магнету траку након коришћења картице. Картица би онда имала своју првобитну вредност и могла би се користити више пута. Ова врста манипулације, позната као "бафероване", је онемогућена у паметним телефонским картицама у склопу безбедносне логике,

Овај тип смарт картице може природно да се користи не само за телефонске позиве, већ кад год је потребно платити робу или услуге без употребе новца. Примери могућих употреба обухватају локални јавни превоз, аутомате свих врста, базена, паркинга и тако даље. Предност ове врсте картице лежи у једноставној технологији (површина чипа је обично само неколико квадратних милиметара), а самим тим и ниске цене. Недостатак је да картица не може бити рециклирана након што се испразани, али мора бити одбачена као отпад, уколико не заврши као нечија колекција. Још једна типична примена меморијске картице је картица за здравствено осигурање, за сва лица уписана у национални план здравственог осигурања. Информације које су претходно написане на картицу пацијента су смештене у чип уштампавањем или ласерским гравирањем. Коришћење чипа за складиштење података чини картице машински читљивим користећи једноставну опрему, [16].

Укратко, смарт картица меморијског типа има ограничену функционалност. Њихова интегрисана безбедносна логика омогућава заштиту чувања податке од манипулације. Оне су погодне за употребу као припејд картице или идентификационе картице у системима где је ниска цена од првенственог значаја.

2.3.2 Микропроцесорске картице

Срце чипа у микропроцесорким картицама, је процесор, који је обично окружен са четири додатна функционална блока: маска ROM-а, EEPROM, RAM, U/I порт.



Слика 2.7 Типична архитектура микропроцесора контактне картице са копроцесором[16]

Маск ROM садржи оперативни систем чипа, који је утиснут при производњи чипа. Садржај је, идентичан за све чипове, и не може се мењати током животног века чипа. Подаци и програмски код могу да се упишу и да се прочитају из EEPROM -а уз контролу оперативног система. RAM је радна меморија процесора. Ова меморија је нестабилна, тако да се сви подаци који се чувају у њој губе када је чип искључен. U/I интерфејс се обично састоји само од једног регистра, преко којег се подаци преносе бит по бит.

Микропроцесорске картице су веома флексибилне у употреби. У најједноставнијем случају, она садржи програм оптимизован за једну примену, тако да се може користити само за конкретну апликацију. Међутим, оперативни систем савремене смарт картице омогућава да неколико различитих апликација буде интегрисано у једну картицу. У овом случају, ROM садржи само основне компоненте оперативног система, уз примену специфичног дела оперативног система који се учитава у EEPROM тек након што је картица произведена. Специјалне хардверске и софтверске мере се користе за спречавање безбедносних услова за појединачне апликације, [16].

Њихова способност да безбедно складишти приватне кључеве и извршавање савремених криптографских алгоритама чини их пожељним у систему плаћања. Будући да је микропроцесор уграђен у картицу чини је програмабилном, а функционалност микропроцесорских картица је ограничена само на доступни простор за складиштење и капацитет процесора.

Могућа примена за микропроцесорске картице укључује идентификацију, контролу приступа системима у рестриктивним зонама и компјутерима, сигурно складиштење података, електронског потписа, као и мултифункционалност јер садржи неколико апликација. Модерни оперативни системи смарт картица такође омогућавају да нове апликације буду учитане у картице након што је већ издата кориснику, без угрожавања безбедности различитих апликација. Такви безбедоносни модули могу безбедно чувати личне кључеве и извршавати криптографске алгоритме високих перформанси. Ови задаци могу се обављати на елегантан начин од стране микропроцесора са криптографским копроцесором. Спецификације за безбедне интернет апликације помоћу смарт картице се тренутно развијају у целом свету, [3].

Укратко, основне предности микропроцесорских картица су велики капацитет, способност за безбедно чување поверљивих података и способност за извршавање криптографских алгоритама. Ове предности чине широк спектар могућности за нове апликације, поред традиционалних банковних апликација. Потенцијал смарт картица никако није још исцрпљен, и штавише, он се стално проширује напретком у технологији полупроводника.

2.3.2.1 Микроконтролери смарт картица

Из информатичке перспективе, централна компонента паметних картица је микроконтролер уграђен испод контакта. Он контролише, иницира и прати све активности картице. Микроконтролери који су специјално дизајнирани и развијени за ову намену су комплетни рачунари у правом смислу те речи. То значи да они садрже процесор, меморију и интерфејс за спољашњи свет.

Најважније функционалне компоненте типичног микроконтролера смарт картице су процесор, адреса и магистрала података и три врсте меморије. Чип има јединицу интерфејса која пружа серијску комуникацију са спољним светом. Овај интерфејс не треба замишљати као комплексну функционалну јединицу која може независно преносити и примати податке. У најједноставнијем случају, серијски интерфејс је само локација које може бити адресирана од стране CPU-а и која је повезана са U/I контактима. [11]

Поред тога, неки произвођачи обезбеђују посебне процесоре на чипу који делују као нека врста математичких копроцесора, иако су функције које обезбеђују ове компоненте ограничене на експоненцијалне и на операције са целим бројевима. Обе ове операције су неопходни елементи јавног кључа за процедуру шифровања, као што је RSA алгоритам.

Микроконтролери који се користе у смарт картицама нису стандардне, широко доступне компоненте. Уместо њих, развијени су други посебно за ту сврху, и они се не користе у другим апликацијама. Безбедносна политика многих произвођача картица је да микроконтролери који се користе нису доступни на отвореном тржишту. То га чини знатно тежим за анализу, јер потенцијални нападач обично му неможе приступити. Међутим, ова позиција је озбиљно ослабљена општом доступношћу програмабилних смарт картица, као што су Јава картице, што углавном доводи до тога да су стандардне апликације небрањиве, [3].

2.3.2.2 Типови процесора

Процесори смарт картица морају бити изузетно поуздани. Због тога је боље ослонити се на старији тип процесора који је доказан у пракси, уместо да се експериментише са протопитом произвођача полупроводника.

Процесори користе углавном CISC архитектуру, што значи да они захтевају више циклуса извршавања инструкција и обично имају веома велики скуп инструкција. Опсег адреса 8-битних процесора је најчешће 16 бита, што омогућава и до 65.536 бајтова које треба адресирати. Приступ меморији контролише се преко посебних регистара. Међутим, ова врста нелинеарног адресирања меморије има значајне недостатке. На пример, релативно сложену дистрибуцију програмског кода преко више меморијских банки значајно компликује софтвер, чиме се повећава вероватноћа грешака. X8 је само 16-битни процесор за микроконтролер смарт картице са RISC архитектуром и одговарајућим сетом инструкција Међу 32-битним процесорима, основна су два процесорска језгра, а која су такође ушла у област смарт картица. Они су MIPS и ARM процесори. Иако 32-битни процесори заузимају знатно више простора од 8-битних процесора користећи исту технологију, због шире магистрале и сложеније унутрашња структуре, они се користе у све већем броју, [13].

2.3.2.3 Врсте меморија

Осим процесора, најважније компоненте микроконтролера су различите врсте меморије, које служе за чување кода програма и података. Од када микроконтролери смарт картица морају бити комплетни рачунари, они користе карактеристичне поделе меморије на RAM, ROM-а EEPROM. Тачна подела зависи од крајње примене области чипа.

Интегрисање три различите врсте полупроводничке меморије у једно силиконско кућиште је технички тежак задатак који захтева велики број производних корака и изложеност маске. Различити типови меморије, такође заузимају различите области, због различитих структура и оперативних принципа.

Нови тип меморијске технологије за смарт картице постао је доступан релативно недавно. Он се зове Flash EEPROM, а времена писања и брисања је много краћа него са претходно доступним типовима EEPROM-а. Величина ћелија је приближно половина конвенционалне EEPROM меморије, у зависности од дизајна, [11].

ROM

ROM смарт картице садржи већину оперативних система, као и разне тестове и дијагностичке функције. Ови програми су уграђене у чип од стране произвођача, када је направљен. То се ради при припреми ROM маске, а затим коришћењем ове маске да "утисне" програм у чип користећи литографски процес.

PROM

PROM се не користи у микроконтролерима смарт картице, мада може да понуди неколико предности. за разлику од ROM-а, PROM не треба да буде програмиран у току производње, али може да се напише непосредно пре него што је чип уграђен. PROM не

користи никакав напон напајања да задржи податке. Главни разлог за некоришћење PROM-а је да програмирање захтева адресни приступ, податке и контролу магистрале.

EEPROM

EEPROM меморија се користи у смарт картицама за све податке и програме који треба да се измене или избришу у неком тренутку.

Flash EEPROM

Постоји неколико микроконтролера смарт картица са Flash EEPROM-ом, који се пре свега користи у микроконтролерима смарт картица као замена за PROM. Користећи микроконтролер са Flash EEPROM-ом може се смањити време развоја смарт картице неколико месеци, јер се елиминише потреба за генерисањем маске ROM-а.

RAM

У смарт картицама, RAM меморија се користи за држање података који су ускладиштени или измењени током израде. Број приступа је неограничен. RAM који се користи у смарт картицама је статички, што значи да његов садржај не мора да буде периодично освежен. Стога не зависи од спољнег такта, за разлику од динамичког. Важно је да RAM буде статички, јер мора да се заустави такт сигнала паметане картице. Са динамичким RAM-ом, то би проузроковало губитак ускладиштених информација.

FRAM

FRAM је потенцијално идеалан за смарт картице, јер има веома пожељна својства за складиштење података. Само 5V је потребно за програмирање, чије је време око 100 ns и максималан број циклуса програмирања је око један трилион. FRAM има два недостатка. Први је ограничен број циклуса читања, што захтева освежавање циклуса, оно што је више значајно, јесте да производња FRAM-а која укључује кораке обраде које је тешко савладати.

2.3.3 Безконтактне смарт картице

Поузданост контактних смарт картица је стално била побољшавана током последњих неколико година, као резултат акумулираног искуства у производњи таквих картица. Контакти су један од најчешћих извора неуспеха у електромеханичким системима. Сметње могу бити проузроковане факторима као што су загађење и истрошеност контаката. У мобилној опреми, вибрације могу да изазову кратак спој. Од тренутка када се контакти на површини картице директно повежу на улазе интегрисаног кола постоји ризик да чип може бити оштећен или уништен услед електростатичког пражњења. Статичка пражњења од неколико хиљада волти нису реткост, [2].

Ови технички проблеми се елегантно избегавају бесконтактним смарт картицама. Поред своје техничке предности, технологија бесконтактне картице нуди издаваоцу и власнику картица опсег нових и атрактивних могућности примене. Бесконтактна технологија је такође предност у системима који захтевају намерно убацивање картице у читач, јер није битно колико је картица убачена у читач. Ово је у супротности са

магнетним картицама или картицама са контактима, које раде само са одређеним оријентацијама картица. Слобода оријентације поједностављује коришћење и на тај начин повећава прихватање корисника.

Да би лакше разумели различите технике које се користе, бесконтактне картице се могу класификовати у складу са различитим параметрима. Једна могућност је да се класификују по методи која се користи за пренос енергије и података. Најчешће коришћена метода је пренос радио таласа или микроталаса, оптички пренос, капацитивне спојнице и индуктивне спојнице. Капацитивне и индуктивне спојнице најбоље одговарају равном облику смарт картице без интерног извора енергије, [3].

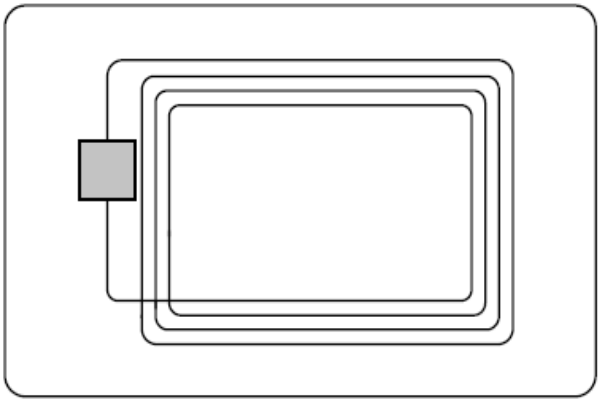
Баш као и код контактне смарт картице, систем бесконтактне картице се састоји од најмање две компоненте, односно картице и компатибилног терминала. Следеће четири функције су потребне да се омогући бесконтактним картицама комуникација са терминалом:

- пренос енергије на картицу за напајање интегрисаног кола
- пренос такт сигнала
- пренос података на смарт картицу
- пренос података са смарт картице

Много различитих концепата су развијени да задовоље ове услове. Већина њих је специјално дизајнирана за одређену примену. На пример, постоји знатна разлика између система у којима се картице далеко само неколико милиметара од терминала у нормалној употреби и системи у којима картице могу бити удаљене и до метар од терминала. Наравно, када је много различитих решења дизајнирано и оптимизовано за посебне апликације, она су неизбежно међусобно некомпатибилна, [12].

Индуктивна спојница

Индуктивна спојница је тренутно најраспрострањенија техника за бесконтактне смарт картице. Она може да се користи за пренос енергије и података различитих захтева и ограничења, као што су прописи радио лиценци.



Слика 2.8 Основна конструкција бесконтактне смарт картице са индуктивном спојницом [3]

Код неких апликација, као што је контрола приступа, довољна је само могућност да чита податке који се чувају у картици, што чини могућим једноставна техничка решења. Због своје мале снаге потрошње (неколико микровати), употребљиви распон тих картица се простире на око један метар. Њихов капацитет меморије је обично само неколико стотина бита. Ако подаци морају бити уписани, потрошња електричне енергије расте за

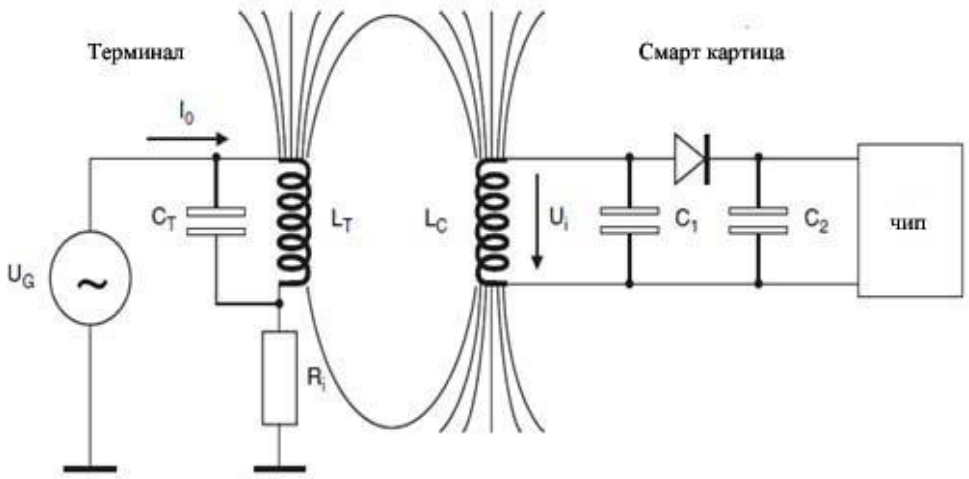
више од 100 μV. Последица тога, је ограничен опсег на око 10 cm у режиму писане форме, Потрошња енергије у микропроцесору картице је још већа и обично је 100 mV. Удаљеност од терминала је, дакле, још ограниченија.

Независно од њиховог асортимана и потрошње, све картице које користе индуктивне спојнице раде на истом принципу. Један или више намотаја (обично са великим затвореним областима) је уграђено у тело картице, који се понашају као спојница компоненте за пренос енергије и података, дуж једног или више чипова, [3].

Пренос енергије

Готово без изузетка, бесконтактне смарт картице се пасивно користе. То значи да се сва енергије потребна за рад у чипу смарт картице мора пренети из читача на картицу.

Овај трансфер енергије је заснован на принципу лабаво повезаног трансформатора. Јака висока фреквенција магнетног поља генерише калем у терминалу у циљу преноса енергије. Најчешће коришћене фреквенције 135 kHz и 13.56 MHz, који одговарају таласној дужини од 2400 m и 22 m, респективно. Таласна дужина електромагнетног поља је, дакле, неколико пута већа од удаљености картице до терминала, што значи да се картица налази у близини области терминала. Ако се бесконтактне картице доведу близу терминала, део магнетног поља терминала пролази кроз калем у картицу и индукује напон Ui у овом калему. Овај напон се исправља да обезбеди напајање чипа. Како је спојница између намотаја у терминалу и картице врло слаба, ефикасност овог аранжмана је веома низак. Висок ниво је потребан у калему терминала да постигне потребну снагу поља. Ово се постиже повезивањем кондензатора Ct паралелно са калемом Lt са вредношћу кондензатора таквим да калем и кондензатор оформе паралелно-резонантну мрежу чија резонантна фреквенција одговара фреквенцији за пренос сигнала, [3].



Слика 2.9 Пример кола илуструје принцип оптерећења модулације, која се користи у бесконтактним смарт картицама за пренос података [3]

Због ниског степена спреге између калемова у терминалу и картице, варијације напона индуковане у терминалу због оптерећења модулације су веома мале. У пракси, амплитуда корисног сигнала је само неколико миливолти. То се једино може детектовати помоћу софистицираних кола, јер се знатно већи сигнал (око 80 dB) преноси терминалом.

Капацитивна спојница

Ако је растојање између картице и терминала веома мало, могуће је да се за пренос података користе капацитивне спојнице. Са овом врстом спојница, проводне површине су укључене у тело картице и терминал тако да оне делују као плоче кондензатора када је картица убачена у терминал или постављена на терминал. Капацитивност која се може добити у суштини зависи од величине површина спојница и њиховог растојања. Максимално растојање је тако ограничено димензијама картице, а минимално растојање се утврђује од изолације која је потребна између површине спојница. Прихватљив ниво трошкова и напора, употребљиви капацитет од неколико десетина пикофарада се може добити. Ово је недовољно за пренос енергије неопходне за напајање микропроцесора. Сходно томе, овај метод се користи само за пренос података.

Избегавање судара (колизије)

Када се користе безконтактне картице, увек постоји могућност да се две или више картица налазе се у опсегу терминала у исто време. То нарочито важи за системе са великим ефикасним дометима, али то чак може да се деси и код система са релативно малим опсезима . Све картице у домету одређеног терминала ће покушати да одговоре на команде из терминала. Међутим, истовремени пренос података ће неминовно да проузрокује сметње и губитак података ако одређене противмере нису предузете. Техничке методе које се користе да се обезбеди несметана размена података више картица у оквиру ефикасног спектра терминала се називају методе за избегавање колизије или антиколизиона метода.

Размена података између више мобилних јединица и базне станице се често среће у области комуникација, и то се назива "вишеструки приступ". Типичан пример је мобилна мрежа, у којој се сви корисници налазе у одређеној радио ћелији истовременог приступа једној базној станици. Бројне методе развијене су да би се сигнали појединих корисника разликовати једни од других. Ове методе антиколизије се могу поделити на четири врсте.

Вишеприступна подела простора (SDMA) покушава да ограничи или скенира оперативне области терминала на такав начин да се само једна картица може појавити у одређено време. Пошто је овај метод захтева веома компликован и скуп, он се не користи за бесконтактне картице.

Мере вишеприступне поделе времена (TDMA), су предузете како би се осигурало да поједине картице имају различита времнска понашања, тако да се могу одвојено идентификовати и појединачно обратити терминалу. Ово је најчешће коришћен метод, а има много варијанти.

Вишеприступна подела фреквенције (FDMA), пружа истовремено различите носиоце фреквенције за трансмисију. Међутим, ова метода је технички компликована и тиме скупа. Сходно томе, она се не користи за бесконтактне картице. Иста разматрања односе се и на вишеприступну поделу шифри (CDMA).

Даље интересантна варијанта у коришћењу бесконтактних картица подразумева "површински терминал". У овом случају, картица није убачена у лежиште, већ се једноставно ставља на обележене локације на површини читача картица. Поред једноставности коришћења, ово решење је атрактивно, јер значајно смањује ризик од вандализма (убацивање жваке или супер лепка у слот за картицу).

Технологија за масовну производњу бесконтактних картица је сазрела до тачке где су производи високог квалитета доступни по ценама које се незнатно разликују од оних за контактне картице. До сада, бесконтактне картице се пре свега користе у локалним јавним транспортним системима, у којима служе као електронска карта..

Међутим, постоји растући захтев за увођење додатне услуге у системима електронских карата. Мултифункционалне картице са интегрисаним микропроцесорима се, дакле, користе све чешће, плаћања се најчешће се реализују коришћењем конвенционалних техника заснованих на контактима у циљу да се искористе постојеће инфраструктуре, као што је систем електронског новчаника. Нове мултифункцијске картице имају и контактне и бесконтактне спојне елементе и називају се дуал интерфејс картице, [16].

Безконтактне картице не морају да се убацују у читач картица, јер су доступни системи које раде у опсегу до једног метра. То је велика предност у контроли система приступа где врата или баријере морају да буду отворене, пошто ауторизација приступа може да се провери без потребе да се картица извади из торбе или џепа и убаци у читач. Један од главних примена ове технологије је локални јавни превоз, који захтева да велики број људи буде идентификован у најкраћем могућем року. Бесконтактне картице, у којима се подаци преносе без икаквог електричног контакта између картице и терминала, постигле су статус комерцијалних производа у последњих неколико година. Тренутно, су меморијске картице и микропроцесорске картице доступне као бесконтактне картице. Бесконтактне картице са микропроцесором обично раде на удаљености од само неколико центиметра од терминала, бесконтактне меморијске картице могу се користити и до метар од терминала. То значи да се такве картице не морају држати у руци током употребе, али могу остати у ташни корисника или новчанику. Бесконтактне картице су посебно погодне за примене у којој би лица или предмети требало бити брзо идентификовани. Неке од апликације су:

- контрола приступа
- локални јавни превоз
- ски пролази
- авио карте
- идентификација пртљага

Међутим, постоје примене где рад преко даљине може да проузрокује проблеме и то треба спречити. Типичан пример је електронски новчаник. Декларација о намерама од стране картице се обично захтева да би завршили финансијску трансакцију. Ово потврђује износ уплате и потврда власника картице да плати. Код бесконтактне картице, ова потврда се остварује убацивањем картице у терминал и потврђивањем наведених средстава преко тастатуре. Да би бесконтактно плаћање преко релативно велике раздаљине било могуће, "преварант" може уклонити новац из електронског новчаника без знања власника картице. Дуал интерфејс картице (понекад се назива "combicard") нуди могуће решење за овај проблем. Ове картице комбинују контакти и бесконтактни интерфејс у једној картици. Таква картица може да комуницира са терминалом преко, или његовог контакт интерфејса или бесконтактним интерфејсом, према ономе што се жели, [3].

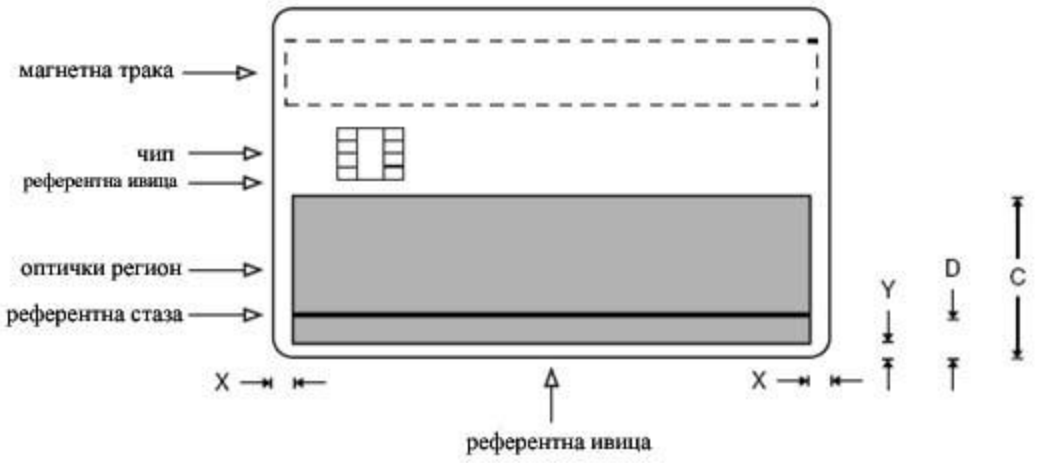
2.3.4 Оптичке меморијске картице

За примене где је капацитет смарт картица недовољан, оптичке картице које могу похранити неколико мегабајта података су на располагању. Међутим, са тренутном технологијом ових картица подаци се могу уписати само једном и не могу се избрисати.

ISO/IEC 11 693 и 11 694 стандарди дефинишу физичке карактеристике оптичких меморијских картица и линеарне технике снимања података које се користе са таквим картицама.

Комбинација великог складишног капацитета оптичких меморијских картица и интелигенције паметних картица доводи до интересантне нове могућности. На пример, подаци могу бити написани у шифрованој форми у оптичку меморију, да кључ буде безбедно ускладиштен у приватну меморију чипа. Овако се штити ускладиштен податак од неовлашћеног приступа.

Слика 2.10 показује типичан распоред оптичке смарт картице са контактима, магнетном траком и регионом за оптичко складиштење. Може се видети да је простор који је на располагању за оптичко складиштење ограничен контактима чипа, који природно смањује укупан капацитет. Магнетна трака се налази на задњем делу картице, [16].



Слика 2.10 Локација оптичког складишног простора на ID-1 картици у складу са ISO / IEC 11 694-2. C = 9.5-49.2 mm, D = 5,8 ± 0,7 mm, X = 3 mm, Y = 1 mm [16]

До сада, коришћење оптичких меморијских картица је озбиљно ограничено високим трошковима опреме за читање и писање ове врсте картица. Једна апликација за оптичке меморијске картице бележи податкео пацијентима у медицинском сектору, јер њихов велики капацитет омогућава чак да се и рендгенске слике чувају на картици.

3 Физичке и електричне особине

Тело смарт картице наслеђује основна својства од свог претходника, рељефне картице. Такве картице су једноставне пластичне структуре које су персонализоване утискивањем различитих функција, као што су име и број картице. Касније верзије ове картице су добиле магнетну траку да омогуће једноставану обраду. Када је идеја имплантирања чипа у картицу, настала, постојећи тип картице је коришћен као основ и микроконтролер је уграђен у тело картице. Многи стандарди који се односе на физичке особине картице нису специфични само за смарт картице, али се у истој мери односе и на картице са магнетном траком и рељефне картице.

3.1 Физичке особине

Већина физичких карактеристика у ствари је чисто механичке природе, као што су формат картице и отпорност на савијање и увијање. Ове карактеристике су познате сваком кориснику из личног искуства. У пракси, међутим, физичке особине као што су осетљивост на температуру или светлост и отпорност на влагу су такође важне. Веза између тела картице и чипа такође се мора узети у обзир, јер само комбинација ове две компоненте чини функционалну картицу. На пример, тело картице дизајнирано за употребу на високим температурама од мале је користи ако уграђен микроконтролер не дели ово својство. Ове две компоненте морају појединачно и колективно испунити све релевантне захтеве, јер у супротном високе стопе неуспеха могу да се очекују током употребе.

3.1.1 Формати картица

Различите картице које су данас на располагању користе се за све могуће намене и имају широк спектар димензија, па је често тешко одредити да ли су одређене картице заправо ID-1 смарт картице. Поред уграђеног чипа, једна од најбољих идентификационих карактеристика је дебљина картице. Ако је мера 0,76 mm и картица садржи микроконтролер, она се може сматрати смарт картицом. Конвенционални ID-1 формат има предност јер је веома лак за руковање.

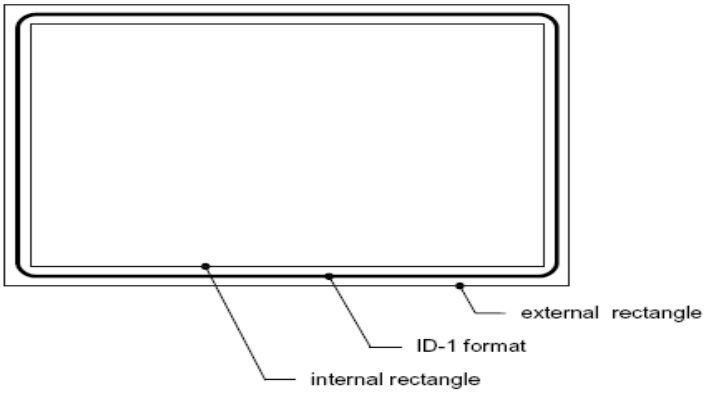
Ипак, овај формат увек не испуњава захтеве модерне минијатуризације. Неки мобилни телефони тешки су само 200 g и не много већи од пакета папирних марамица. Требало је дефинисати мањи формат поред ID-1 формата, због потреба малих терминала. У ову сврху је дефинисан ID-000 формат. Овај формат се тренутно користи само уз GSM мобилне телефоне, који имају врло мало простора за картицу и не захтевају да се картица често размењује, [16].

Међутим, чињеница је да су картице у ID-000 формату незгодне за руковање, како у производњи и тако и код крајњег корисника, што је довело до развоја додатних формата. Овај формат је одредио ID-00. Њене димензије су упола од оних за ID-1 и ID-000 картице.

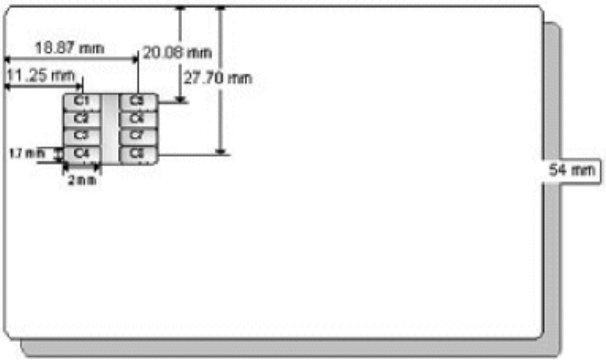
Формати су дефинисани у релевантним стандардима на начин који поједностављује мерење димензије картица. На пример, висина и ширина ID 1 картица мора да буде таква да одговара димензијма два концентрична правоугаоника као што је приказано на слици 3.1 (игноришући заобљене углове), који имају следеће димензије:

- спољашњи правоугаоник: ширина: 85,72 mm**,** висина: 54.03 mm
- унутрашњи правоугаоник: ширина: 85.46 mm **,** висина: 53.92 mm

Дебљина мора да буде 0,76 mm, са толеранцијом од ± 0,08 mm, угао радијуса и дебљина картице су конвенционално дефинисани, [5].



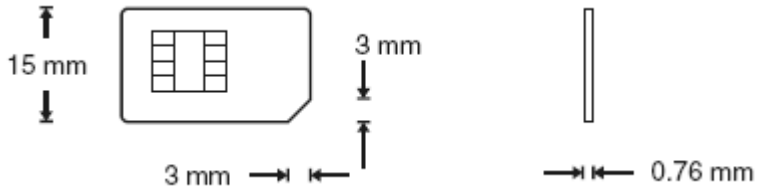
Слика 3.1 Дефинисање димензија картице ID-1 формата [16]



Слика 3.2 ID-1 формат [8]

ID-000 формат је такође дефинисан помоћу два концентрична правоугаоника. У доњем десном углу картица је одсечена под углом од 45 ˚, у циљу олакшавања исправног убацивања картице у читач. Димензије два правоугаоника за ID-000 формата су:

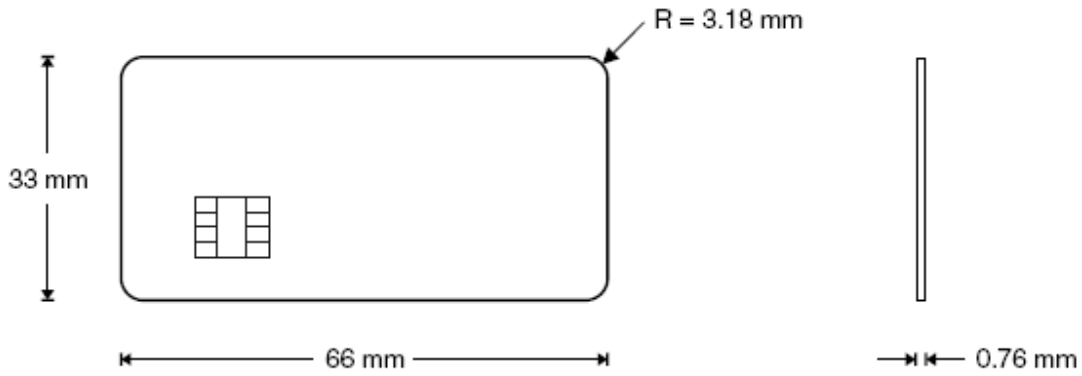
- спољни правоугаоник: ширина: 25,10 mm , висина: 15.10 mm
- унутрашњи правоугаоник: ширина: 24.90 mm , висина: 14.90 mm



Слика 3.3 ID-000 формат [3]

ID-00 формат дефинисан је помоћу два концентрична правоугаоника са следећим димензијама: су:

- спољни правоугаоник: ширина: 66,10 mm , висина: 33.10 mm
- унутрашњи правоугаоник: ширина: 65.90 mm , висина: 32.90 mm



Слика 3.4 ID-00 формат [16]

Међутим, уобичајени формат картице још увек има неке недостатке за неке апликације. У таквим ситуацијама, неки друге варијанте могу да се користе, као што је USB прикључак са интегрисаним микроконтролером, [8].

3.1.2 Компоненте картица и безбедносне функције

Пошто се смарт картице примарно користе да пруже ауторизацију за поједине акције или за идентификују, безбедносне функције на телу картице су често потребне као додатак поред уграђеног чипа. Неке безбедносне функције упошљавају модификовани микроконтролер и на тај начин могу бити верификовани само од стране рачунара. За разлику од безбедносне функције са микроконтролерима, карактеристике уобичајене људске верификације аутентичности картица се не заснивају на криптографским процедурама.Уместо тога, она се примарно заснива на коришћењу тајног материјала и процеса производње или на коришћење процеса чије владање захтева велику количину напора или значајну стручност, [3].

Панели за потпис

Веома једноставан начин да се идентификују власници картица је коришћење панела за потпис, што је уобичајено за кредитне картице. Када је такав панел потписан, не може се мењати, тако да је то неизбрисив доказ. Врло фини обојени образац одштампан на панелу чини сваки покушај да се покрије панел очигледним. Панел за потпис је трајно везан за тело картице користећи процес топлог лепљења да би се приложила штампана папирна трака на картицу. Алтернативно, панел за потпис може бити део горњи слој картице, који је залепљен на картицу током процеса састављења.

Гијош обрасци

Нешто компликованија техника је да се фолија са одштампаним обрасцима стави под гијош транспарентан спољни слој картице. Гијош обрасци су обрасци који се састоје од веома финих испреплетаних декоративних линија, обично округлих или овалних, као оне које се налазе на неким новчаницама и сертификатима. Ови обрасци су тако фине структуре који могу бити производи само процесом штампања, а као такви тешки за копирање.

Микротекст

Друга техника безбедности заснива се на структури финих штампаних која користи линије микротекста. Појављују се јасне линије видљиве голим оком, али се оне могу препознати као текст користећи лупу. Као и гијош образац, микротекст се не може фотокопирати.

Ултраљубичасти текст

Да се не би утицало на видљиви изглед картице, контрола карактера или контрола бројева може да буде одштампана на картици користећи мастило које је видљиво само под ултраљубичастим светлом. Међутим, ова техника обезбеђује само релативно ограничену заштиту од фалсификовања.

Баркод

За чување мале количине података, баркод може да се одштампа на површини картице коришћењем ласерског гравирања или термо-трансферне штампе. Предност баркодова је што се они могу аутоматски читати из непосредне близине користећи оптичку опрему. Баркодов исписан на смарт картици укључују не само коришћење једнодимензионалног типа, већ и дводимензионалне баркодове у облику матрице баркодова.

Холограми

Холограми за смарт картице зову се "рељефни" холограми. Додатне заштитне функције које се могу видети само са ласерском светлошћу понекад су интегрисане у холограме. Да би се произвели рељефни холограми, неопходно је да се прво генеришу мастер холограми користећи уобичајене холограмске технике. Гравирање отиска се припрема од стране мастер холограмског процеса преноса. Гравирани отисак садржи микроструктуру која ће касније производити уграviране холограме.

Холограм је трајно везан за тело картице, тако да не може бити уклоњен а да се не уништи. Ово се може урадити користећи процес пластификације. У каснијем процесу, холограм се налази на носачу филма који се утисне на картицу грејањем ваљка. Носилац филма се потом скине и холограм остаје трајно заварен за тело пластичне картице. Трећи процес који се користи је процес топлог печаћења.

Ласерско гравирање

Затамњивања специјалног слоја пластике грејањем ласерским зраком се зове ласерско гравирање, или једноставно ласеровање. Ово је сигуран начин да се подаци напишу на појединачну картицу, као што су име власника картице и број картице. То је сигуран начин зато што је потребно имати опрему и знање како да се користити а која није доступна Две различите методе користе се за ласерско гравирање: вектор и растер гравирање. Код методе вектора, ласерски сноп се усмерава дуж пута без прекида. Веома је погодна за писање карактера и има предност јер је брза. Код технике растера, с друге стране, велики број суседних тачака поцрни да би произвео слику, слично раду инк-џет или матричном штампачу. Ова метода се углавном користи да постави слику на картицу.

Утискивање

Још један начин да се додају подаци корисника на картицу је утискивање карактера на картицу. То се ради ударањем металних слова о картицу. У принципу, овај процес функционише на исти начин као и што функционишу и механичке писаће машине. Данас, једина корист од утискивања је да се рељефни карактери лако могу пренети на одштампани образац коришћењем индиго папира.

3.2 Тело картице

Материјал, изградa и производња тела картице је ефикасно одређен на основу функционалне компоненте картице. Типичне функционалне компоненте укључују:

- магнетне траке
- панел за потпис
- утискивање личних података ласерским снопом (текст, слика ...)
- холограм
- сигурносна штампа
- невидљиве аутентификацијске функције (флуоросцентне)
- чип са контактима или неким другим спојним елементима

Јасно је, да чак и релативно мала картица, од само 0,76 mm дебљине, мора понекад да садржи велики број функционалних компоненти. Ово поставља екстремне захтеве у погледу квалитета материјала који се користи у процесу производње. Минимални захтеви који се односе на робусност картице су наведени у свим ISO стандардима .Захтеви се у суштини односе се на следеће области:

- ултраљубичасто зрачење
- рентгенско зрачење
- профилске површине картице
- механичка робусност картице и контаката
- електромагнетна осетљивост
- електростатичко пражњење
- отпорност на температуру

Тестови на савијање и увијање су посебно важни за смарт картице, јер чип, који је ломљив и крт као стакло, је деликатно страно тело у еластичној картици. Посебне структурне особине су у обавези да га штите од механичких оптерећења које производи савијање и увијање картице, [5].

3.2.1 Материјали картица

PVC

Први материјал који се користио за картице, који је још увек у широкој употреби, је поливинил хлорид (PVC), аморфни термопластични материјал. Он је најјефтинији од свих доступних материјала, лак за обраду и погодан за широк спектар примене. Користи се широм света за кредитне картице. Његове мане су ограничени животни век, због физичког пропадања и ограничена отпорност на топлоту и хладноћу. PVC се сматра штетним за околину, јер је сировина, винил хлорид, канцерогена. Ипак, PVC је још увек далеко најраспрострањенији материјал за картице. То је пре свега због своје ниске цене и добрих карактеристика обраде.

ABS

Да би се избегли недостаци PVC-а, акрилонитрил бутаиен стирен (ABS) је коришћен неко време за производњу картица. То је такође аморфна термопластика која се одликује стабилношћу и отпорношћу на екстремне температуре. Сходно томе, често се користи за израду картица за мобилне телефоне, који из очигледних разлога не могу бити изложени релативно високим температурама. Главни недостаци су ограничење у прихватању мастила и ниска отпорност на атмосферске утицаје.

PC

За апликације у којима су потребни екстремна стабилност и издржљивост, користи се поликарбонат (PC). Обично се користи за личне карте, и случајно је основни материјал за израду компакт дискова и DVD-ова. Због своје високе термичке стабилности, потребно је применити релативно високе температуре за остављање холограма или магнетних трака путем процеса врућег печата. Главни недостаци поликарбоната су низак степен отпора на гребање и веома високе цене у поређењу са другим материјалима.

PET

Еколошки материјал који се углавном користи као замена PVC-а је полиетилен терефталата (PET), који се релативно дуго користи за паковање материјала. Обично је познат као полиестер. Овај термопластични материјал се користи код смарт картица, у оба аморфна облика (A-PET) и његов кристални облик (P-ETP). Међутим, PETP је тежак за премазивање, што захтева додатне кораке обраде.

Учињени су бројни покушаји да се пронађу нови или бољи материјали за тело картице, поред уобичајених материјала. Један од примера је целулозни ацетат, који иако има добре еколошке особине, до сада није показао да одговара маси за производњу картица. Заиста различити материјали, као што су папир, су често помињани, али до сада они никада нису били коришћени у значајним количинама. Захтеве које имају картице, у смислу трошкова, трајности и квалитета који су на крају крајева веома високи, тренутно може испунити само пластика, [3].

3.2.2 Кућиште чипа

Најважнији саставни део смарт картице је, наравно, чип. Наравно, ова веома слаба компонента се не може једноставно залепити на површину картице као магнетна трака. Уместо тога, потребна је нека врста кућишта како би га заштитила од грубог свакодневног живота картице. Ово кућиште се зове чип модул. Поред заштите од услова околине, чиповима за контактне смарт картице потребно је шест или осам контакта, који ефективно обезбеђују напајање чипа и омогућавају комуникацију са терминала. Део површине модула служи да омогући електрични контакт спољном свету. Наравно, чип модул треба да буде што је могуће јефтинији, [16].

Велики број дизајна модула осмишљен је у току израде смарт картице, у циљу задовољавања техничких услова за заштиту крхког полупроводничког чипа и омогућавање контактне површине. Најважнији од њих су:

- TAB кућиште
- оловни рам
- површински чип
- савитљиви чип

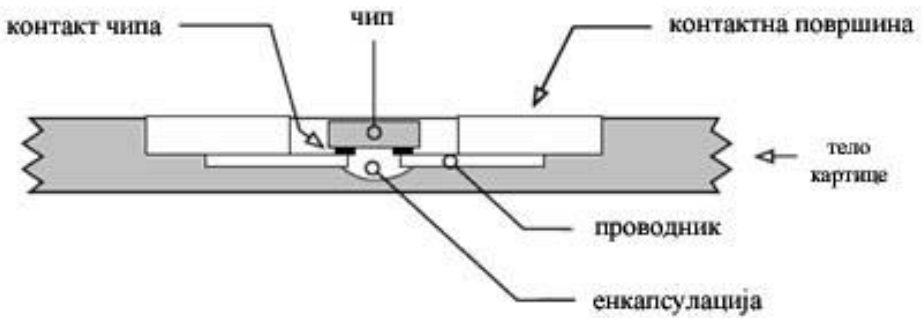
3.2.2.1 Електрична веза између чипа и кућишта

Електричне везе су потребне између чипова унутар модула и контаката изван модула. Тренутно, два процеса се примарно користе за то. У процесу лемљења жицом, при аутоматском лемљењу од стране машине додаје се златна жица пречника од само неколико микрометара, између чипа и задње површине контаката. Жице су електрично везане за чип и модул користећи ултразвучно заваривање. Ово је био стандардан процес у индустрији полупроводника неко време, и може се лако користи за масовну производњу кућишта чипа. Међутим, сваки чип мора бити електрично повезан са модулом са пет жица, што наравно изискује доста новца и времена, [3].

Други је процес везивања. У овом процесу, електричне везе између чипа и кућишта се не врше жицама. Уместо тога, везе се остварују механички, постављањем чипа на полеђини кућишта.

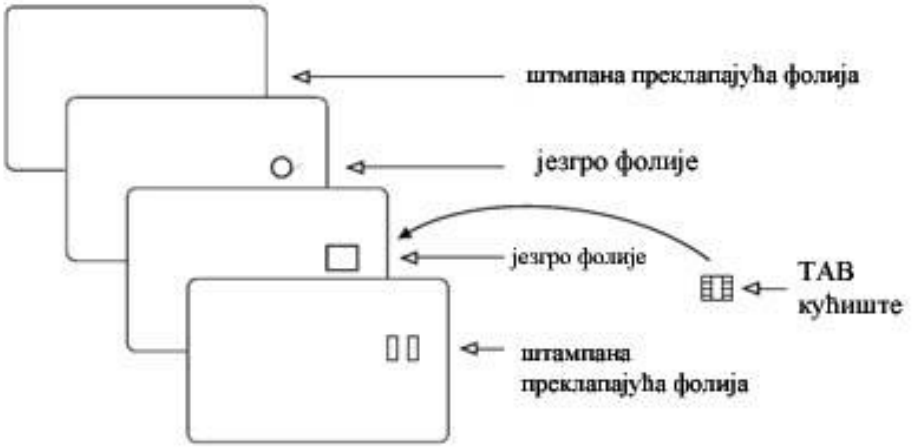
3.2.2.2 TAB кућишта

Посебна одлика овог процеса је та што су метална испупчења прво електрично вежу за чип, а онда се носач залеми на ова испупчења. Лем везе су толико снажне да ниједна додатна подршка није потребна за чип. Активна површина чипа је заштићена од амбијенталних услова енкапсулирајућим материјалима. Предности TAB процеса су механичка чврстоћа конектора и низак профил модула. Међутим, ове предности доносе веће трошкове у поређењу са другим процесима припреме модула.



Слика 3.5 Пресек модула чипа коришћењем TAB процеса [16]

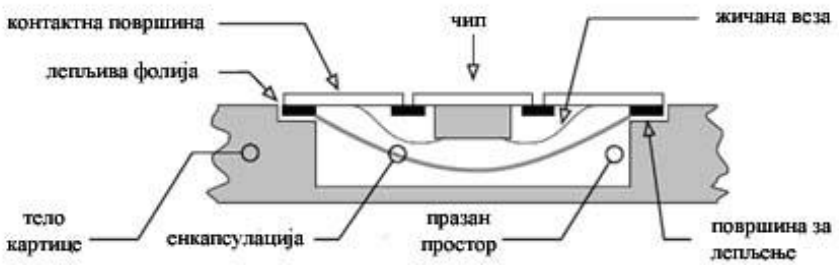
Уклапање TAB модула у смарт картицу није лако, јер се кућиште мора узети током припреме пластификације фолије за картицу. Пре него што су слојеви залепљени, погодни отвори ударе у њих, а затим се чип убацује у кућиште. Кућиште је накнадно заварено за тело картице у току процеса пластификације. Овај процес обезбеђује веома поуздану везу између чипа и тела картице. Готово је немогуће уклонити чип са картице без уништавања картице, [16].



Слика 3.6 Убацивање TAB модула за време процеса пластификације [3]

3.2.2.3 Кућиште савитљивог чипа

Кућиште савитљивог чипа са жичаном везом контаката је најраспрострањенији тип кућишта. Овим процесом, отвара се могућност да чип може бити залемљен у кућиште готовог тела картице. Носећи материјал је флексибилна плоча направљена од фибергласа која је ојачана епоксидном смолом. Контакти су формирани од слоја бакра. Контактне површине су позлаћене у каснијим корацима да би их заштитили од процеса који могу утицати негативно на електричну проводљивост, као што је оксидација. Чипови, који су ефективно око 200 микрона дебели, узети су из тестерастих плочица од стране робота и уклопљени у отворе у плочи. Затим, су контакти чипа повезани са задње стране контакта везивањем помоћу жица. На крају, чип и жице за лемљење су затворене у грудвице синтетичких смола као заштита од спољашњих услова. Укупна дебљина готовог модула се обично креће око 600 микрона.



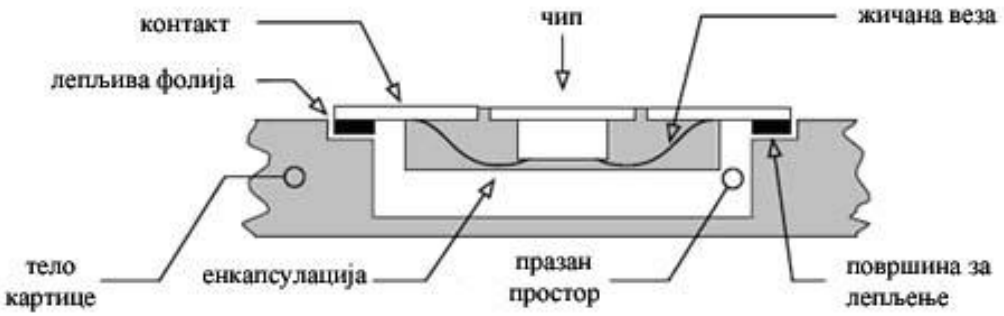
Слика 3.7 Пресек модула чипа на савијање [3]

.

Предност овог процеса се у великој мери заснива на коришћењу стандарда у индустрији полупроводника за уградњу чипа у стандардне пакете. Не захтева толико специјализовано искуство као TAB процес, па је стога мање скуп. Такође, сам овај процес доводи до производње врло сложених тела картица са много активних компоненти. Недостатак овог процеса је што је дебљина површине кућишта чипа знатно већа од оних димензија TAB модула, јер жице морају бити покривене заштитним слојем. Ово је посебно неповољно, у смислу стандардне дебљине смарт картице од 0,76 mm која не оставља пуно простора за претерано дебеле модуле, [3].

3.2.2.4 Кућиште са оловним рамом

Структура кућишта са оловним рамом је једноставна. Чип је смештен на рам и онда повезан на полеђину контаката коришћењем жица за везивање. Даље, чип је покривен заштитном непрозирном грудвицом од епоксидне смоле, Овај процес је тренутно један од јефтинијих процеса за израду кућишта чипа.



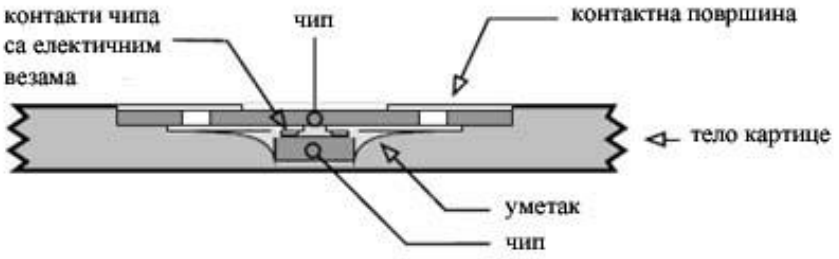
Слика 3.8 Пресек модула чипа са оловним рамом [16]

3.2.2.5 Процес површинског чипа

Мозаик процес је погодан за чипове чија је површина око 1 mm. Овај процес тренутно ограничава његова примена за меморијске чипове, пошто су микроконтролери и даље превелики за овај процес. Процес функционише на следећи начин: прво се користи ласер за уклањање материјала са локације на којој чип треба да буде постављен, а затим се чип залепи у направљено удубљење. У следећем кораку, проводна сребрна паста се нанесе на површину чипа и тело картице, формирајући на тај начин контактне површине и у исто време повезује чип. У последњем кораку, чип и доводи до контакта се прекривају

непроводним лаком. Ово пружа електричну изолацију и штити их од спољашњих климатских услова.

Процес површинског чипа је веома погодан за масовну производњу великог броја картица, јер се у суштини састоји само од ласерког глодања тела картице и два процеса штампања. Међутим, овај процес захтева изузетно прецизну штампу да би се осигурало да су контакти за чип постављени правилно. За овај процес погоно је да тело картице буде од поликарбоната. Други процес је флип (окрени) чип процес, у којем је чип окренут лицем супротно од задње површине кућишта и електрично спојен.



Слика 3.9 Пресек модула чипа направљеног помоћу флип-чип процеса [3]

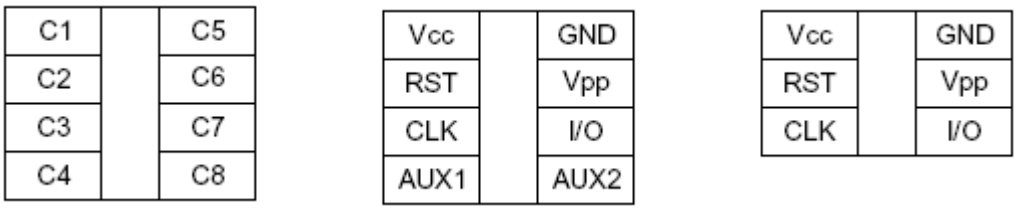
3.3 Електрична својства

Електрична својства смарт картица зависе само од уграђених микроконтролера, јер је то једина компонента картице са електричним колом. Апикација која од самог почетка има много круте услове електричних својстава је GSM систем. Овај систем, ефективно има изузетно велики избор технички различитих типова уређаја. Због великог броја смарт картица које се користе, електричне карактеристике за одређене картице су постале опште смернице за све произвођаче микроконтролера смарт картица.

Разлика између смарт картица које се користе за финансијске трансакције и смарт картица које се користе за телекомуникацију су одређене различите примене. На пример, у подручју финансијских трансакција текућа потрошња и параметри напона су потпуно некритични, јер су терминали који се користе за такве апликације повезани на јавну мрежу напајања. Ситуација у области телекомуникација је сасвим другачија, јер се сваки миливат рачуна када је циљ да се постигне најдуже могуће време рада батерије. Сходно томе, захтеви за најмању могућу потрошњу и ниско снабдевање напоном су веома важни у овој области примене, [13].

3.3.1 Електричне везе

Смарт картице имају шест или осам контакта на предњој страни, који чине електрични интерфејс између терминала и микроконтролера у картици. Сви електрични сигнали се преносе преко тих контакта. Два од осам контакта (C4 и C8) резервисани су за помоћне контакате AUX1 и AUX2. Неки модули смарт картица имају само шест контакта, јер то смањује производне трошкове, и они имају исту функционалност као и модули са осам контакта. Контакти су секвенцијално нумерисани од горње левог до доње десног.



Слика 3.10 Електрични задаци и нумерација контаката смарт картице, према ISO 7816-2 [5]

Дакле, свака паметна картица има контакт који нема стварну функцију, али који мора увек бити присутан, пошто се контакт напона за програмирање налази између друга два која су неопходна за рад картице, не могу једноставно да се уклоне.

Контакт	*Назив*	*Функција*
C1	*Vcc*	*Напон напајања*
C2	*RST*	*Ресет*
C3	*CLK*	*Такт*
C4	*AUX1*	*Допунски контакт*
C5	*GND*	*Уземљење*
C6	*Vpp*	*Напон програмирања*
C7	*I/O*	*Улаз/Излаз*
C8	*AUX2*	*Додатни контакт*

Табела 3.1 Ознаке контакта и функције у складу са ISO 7816-2 [5]

3.3.2 Напајање

Напон напајања за смарт картице првобитно је био 5V, са максималном толеранцијом од ± 10%. Као и код других полупроводничких компоненти, све мања структура и потреба за смањењем текуће потрошње је довела до тога да је неопходно да се значајно смањује опсег напона.

EEPROM-и су такође интегрисани у микроконтролер смарт картице. Ови EEPROM-и су највећа препрека нисконапонских смарт картица. Ипак, уз одређену количину техничке генијалности сигурно је могуће да се EEPROM-и и њихово пуњење интегришу у микроконтролер који може да ради преко напона напајања у распону од 1.62 до 5.5 V.

Стандард и његове измене и допуне дефинишу три класе за карактеристичне опсеге напона смарт картица. Класа А обухвата напон од 5 V ± 10%, класа Б покрива опсег од 3 V ± 10%, а класа Ц покрива опсег од 1,8 V ± 10%. Све три класе се могу користити појединачно или у било којој жељеној комбинацији. Стандард намеће још један једнако важан услов, а то је да се ни под којим условима микроконтролери за смарт картице не могу оштетити ако се картица напаја из напона који не подржава микроконтролер. То је основни предуслов за обезбеђивање компатибилност нових типова смарт картица са старијим типовима терминала, [5].

3.3.3 Снабдевање струјом

Микроконтролер картице добија своје напајање, а самим тим и снабдевање струјом, путем контакта C1. Ова тренутна струја не може бити већа од 10 mA и мора да се налази испод одређене вредности да дозволи хардверу у терминалу да се снабде одговарајућом максималном струјом.

Сви микроконтролери смарт картица имају један или више посебних режима рада за уштеду енергије Принцип оваквог режима је заснован на онемогућавању функционалних компоненти чипа које се не користе. У принципу, само прекидна логика, регистри процесора и RAM меморија треба да остану под напоном, како би се сачувало тренутно стање пословања. У пракси, процесор често остаје под напоном, али су ROM и EEPROM искључени. Када је микроконтролер у овом режиму мировања, или стању мировања, потрошња струје опадне, јер је већина делова чипа изолована од напона напајања. Поред овог режима мировања, многи микроконтролери паметних картица подржавају још један режим који се примењује где генератор такта може да се искључи, а то је режим заустављања такта .Основна намена овог режима је да се дозволи компонентама хардвера у терминалу који генеришу такт да могу бити искључене, што овај режим чини посебно атрактивним за батерије терминала.

Сви микроконтролери користе CMOS технологију. Под одређеним условима, велика струја кратког споја може се појавити током процеса пребацивања транзистора. Ово проузрокује тренутне скокове који су много пута већи од номиналне оперативне струје, уз трајање у опсегу наносекунде. Уколико терминали не могу да ускладиште велику струју током ових кратких временских интервала, напон напајања ће пасти испод дозвољене вредности. Ово може да произведе грешку приликом писања у EEPROM меморију чипа, [3].

3.3.4 Спољашњи генератор такта

Процесор смарт картице обично нема унутрашњи генератор такта. Стога је неопходан спољашњи генератор такта. Овај генератор такође обезбеђује референцу за брзину преноса података. Тактни сигнал који се примењује на контакте није нужно да буде исти као и унутрашњи који даје процесор. Неки микроконтролери имају множилац такта или разделник који може опционо да се убаци између спољних и унутрашњих тактова. Често делилац такта дели фактор, тако да је унутрашњи стопа сата само половина спољнег такта. Ово је делом због хардверских карактеристика, а делом зато што дозвољава осцилатору који је већ присутан у терминалима да буде извор сигнала такта за чип.

Већина микроконтролера смарт картице дозвољава сигналу такта да буде искључен када је процесор у режиму мировања. У овом случају, искључивање такта значи држати такт на дефинисаном нивоу. У зависности од предности произвођача чипова, искључен ниво може бити или висок или низак, [15].

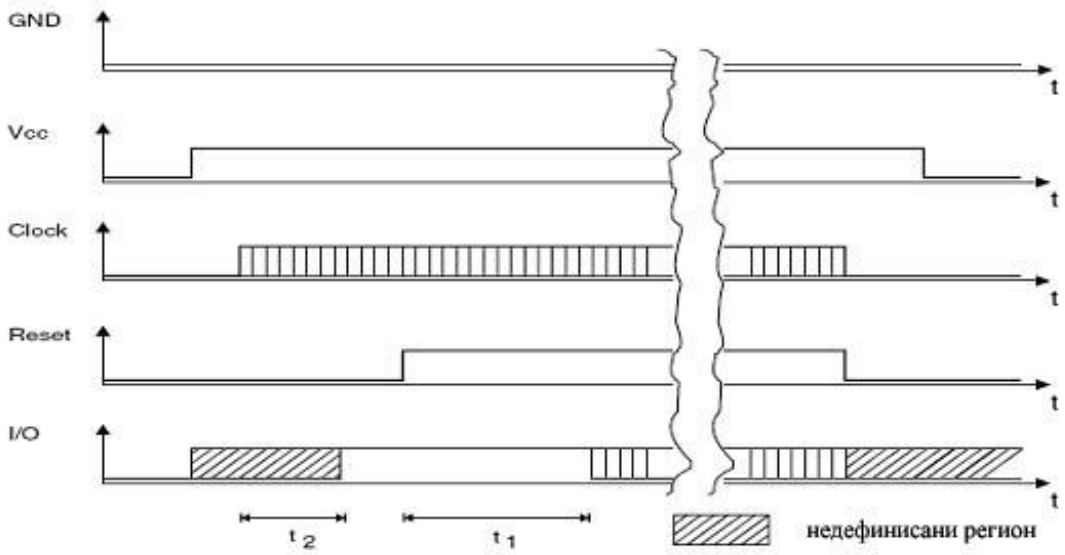
3.3.5 Секвенце активације и деактивације

Сви микроконтролери смарт картица су заштићени од електростатичког набоја и потенцијала на контактима. Да би се избеглп недефинисано стање, тачно одређене секвенце активације и деактивације су прописане и морају бити стриктно поштоване. Ове секвенце дефинишу електричне аспекте активирања и деактивирања картице и немају никакве везе са редоследом успостављања механичког контакта са картицом.. Ипак, механички контакт је први са контактом уземљења на картици као предострожност како би се обезбедио добро дефинисан систем електричног укључивања и искључивања.

Прво се мора активирати контакт за електрично уземљење, а потом контакт за прикључење напона напајања. После овога долази конектор за такт. Уколико се покуша

повезивање такта пре него што се прикључи напон напајања, микроконтролер ће покушати да привуче тренутно напајање преко такт линије. Ово би могло неповратно оштетити чип, изазвати потпуни функционални неуспех. Неисправна деактивација такође има сличне ефекте на микроконтролеру, [3].

Када микроконтролер ради, он може бити ресетован преко ресет линије. Најпре се на овој линији примени низак ниво, а стварни ресет се покреће након наиласка растуће ивице. Овакав ресет у току операције се зове топли ресет. Насупрот томе, хладни ресет је онај који се јавља када су све линије снабдевања укључене.



Слика 3.11 Секвенце активације и деактивације смарт картице [3]

4. Информатичке основе

"Смарт картица је мали рачунар у формату кредитних картица без интерфејса човек-машина". Ова изјава изражава суштинске ствари, а то је да за разлику од свих осталих врста картица, специфична особина смарт картица су микроконтролери интегрисани у картицу.

Основна функција пластичног тела картице је да носи микроконтролер. Наравно, остале компоненте могу бити присутне поред микроконтролера, али оне нису од суштинског значаја.

4.1 Структуирање података

Складиштење или преношење података неминовно захтева тачну дефиницију података по питању њихове структуре. Тек тада је могуће да се накнадно препознају и интерпретирају елементи података. Подаци непроменљиве дужине са немодификованом секвенцом редовно изазивају колапс.

Проблем структурирања података је присутан већ дуго времена, и постоји адекватан избор метода које се могу користити за решавање проблема. Један од метода који је врло популаран, долази из области преноса података и зове се Апстрактна Синтакса Нотације 1 или ASN.1. Ово је независан опис кодирања објеката података, првобитно развијен за пренос података између различитих рачунарских система. Алтернатива би био XML за структуру података, али до сада овај метод није добио упориште у реалним апликацијама.

У принципу, ASN.1 је нека врста вештачког језика који је погодан за описивање података и структуре података, а не програма. ASN.1 има више елементарних типова података и композитне типове података. Такође је могуће да се прошири синтакса коришћењем макроа у циљу добијања било којег жељеног побољшања.

Накнадна проширења структуре података се могу обавити веома лако, све што је неопходно јесте да се убаце додатни кодирани подаци у постојећу структуру података. Потпуна компатибилност са претходном верзијом задржава се све док се претходни објекати не обришу. Исто важи и за нове верзије структуре података у којој су промене учињене у односу на претходно кодирање. То је једноставан процес који захтева само измене ознака, [11].

Главни недостатак ASN.1 је да су административни подаци прилично високи ако је обим корисничких података мали. На пример, ако је корисник података само један бајт, два додатна бајта (ознака и дужина) су и даље потребни за административне податке.

Приликом процене ове структуре података, рачунар упоређује први таг са свим познатим ознакама. Ако пронађе подударање, препознаје га као први објекат. Каснији бајтови су стварни објекти, односно лично име. Ово је праћено следећим објектом, чији је први бајт ознака за презиме. Уколико је неопходно да се продужи структура података, на пример, додавањем наслова, нови тип података може једноставно бити уметнут у постојећу структуру. Проширена структура остаје у потпуности компатибилна са претходном верзијом, јер нови тип података добија своју ознаку и стога је недвосмислено идентификован.

4.1.1 Кодирање алфанумеричких података

Алфанумерички подаци у датотекама и објектима података смарт картица се могу складиштити у широким различитим форматима. Делом, то је резултат мере интензивне оптимизације меморијског простора и недостатка општег слагања између различитих апликација и спецификација, а делом то је због тријумфалног напретка смарт картица у земљама изван западне Европе, који имају своје писмо. У таквим ситуацијама, оригинални 7- и 8-битни сет карактера мора бити замењен моћнијом шемом кодирања за алфанумеричке податке.

7-битни код

Укупно 128 карактера може се представити коришћењем 7-битног кода. Најраспрострањенији међународни 7-битни код, је ASCII код (Амерички Стандардни Код за размену информација). Значај ASCII кода стално опада већ дужи низ година, јер је број карактера који се може представити превише мали.

8-битни код

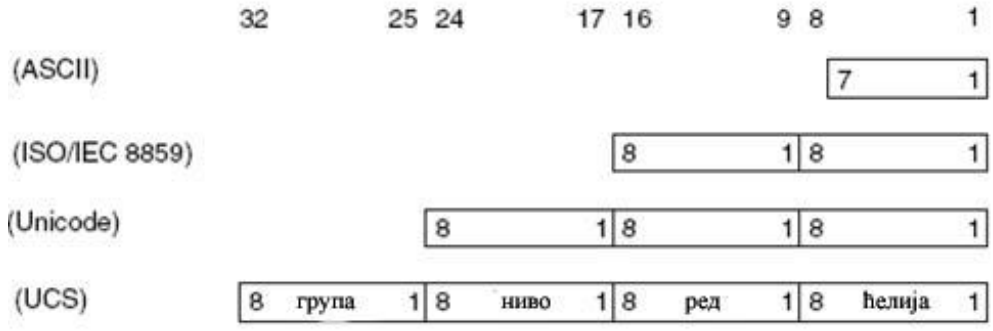
Најчешће се користи 8-битни код који се добија из 7-битног ASCII кода. Састоји се од две 7-битне кодне табеле која садржи контролу карактера и штампање карактера. Нижи ред табеле је идентичан 7-битној ASCII табели и увек је исти. Виши ред може да варира и да прими одређени скуп знакова земље. Вероватно најпознатији виши ред кода је Latin 1, који садржи знакове специфичне за земље Западне Европе. Latin 2, насупрот томе, садржи посебне знакове за источноевропске земље.

16-битни код (Unicode)

Кодови са ширином од 16 бита омогућавају 65,546 (2^{16}) карактера. Једини пример таквог кода је Unicod. Првих 256 карактера су идентични са Latin 1, тако да је постигнута компатибилност у овом делу карактера кодирања. Иако је број карактера који се може представити са 16-битним кодом довољан да представља карактере већине живих језика, нажалост није довољан да представља све постојеће знакове.

32-битни код (UCS)

Unicod је првобитно ограничен на 65.536 карактера. Иако ово ограничење не проузрокује проблеме у свакодневној употреби, може се избећи коришћењем проширене шеме кодирања карактера. 32-битни код назван "универзални карактер сет (UCS)", омогућава 2^{32} каратера за коришћење, иако се користи само половина карактера. Четири бајта UCS се зову група, ниво, ред и ћелија. UCS се састоји од 256 група са 256 нивоа, од којих сваки има 256 редова са 256 ћелија. Најнижи ниво, који је група 0, ниво 0, носи назив "Основна Вишејезична Раван" (BMP) и идентичан је Unicode. Најнижи ред, који је група 0, ниво 0, ред 0, одговара скупу знакова Latin 1, и првих 128 карактера је на тај начин идентичан ASCII коду, [3].



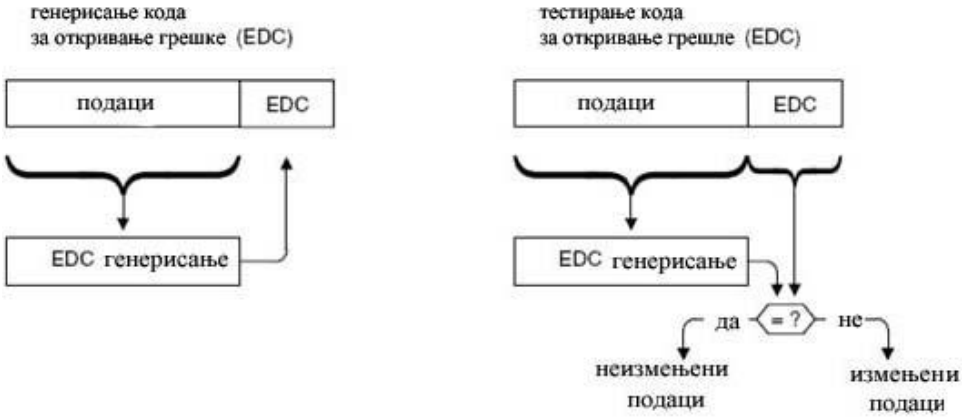
Слика 4.1 Веза између најчешће коришћених 7 -, 8 -, 16 - и 32-битних кодова [3]

4.2 Детекција грешака и кодови корекције

Кад год се подаци преносе или складиште, требало би омогућити откривање било какве промене података. Конкретно, смештени програми морају бити заштићени против корупције, јер само један измењени бит програмског кода може упропастити програм или

модификовати његово извршење до те мере да он више не пружа потребне функције. EEPROM меморије које се користе у смарт картицама су посебно осетљиве на спољне утицаје, као што су топлота и варирање напона. Као последица тога, делови који обављају безбедносне функције морају бити заштићени, тако да нежељене промене открије оперативни систем и избегне њихове негативне ефекате.

Веома осетљиви садржај фајла, као што је програмски код, кључеви, услови приступа, показивач структуре и слично, морају бити заштићени од мењања. Кодови откривања грешака (EDC) се користе за ову сврху. Вероватноћа откривања промена у региону меморије која је заштићена EDC-ом зависи од врсте кода који се користи. Кодови за исправљање грешке (ECC) су наставак детекције грешке. Они омогућавају да се, не само детектују грешке у заштићеним подацима, већ и да исправимо грешке у ограниченој мери.



Слика 4.2 Основни процеси за генерисање и откривање грешке код (EDC) [3]

Сви ови кодови раде на принципу додавања контролне суме на заштићене податке. Контролна сума се обично чува заједно са заштићеним подацима. Она се израчунава коришћењем углавном познатог алгоритма, а не тајног. Посебан аспект детекције грешке и корекције је да се користи велики број математичких процедура. У већини случајева, коришћење таквих алгоритама енормно повећава комплексност и величину програмског кода. Много чешће се користе процедуре у којима откривање грешке не разликује горњи и доњи део бајта, већ функционише на бајт, као целину, [3].

Најпознатији тип детекције кода грешке је несумњиво бит парности, који се додаје у сваки бајт у многим протоколима за пренос података и неким врстама модула меморије. Бит парности се бира тако да је укупан број '1' битова у бајту података плус бит парности паран број. Са непарним паритетом, овај тотал је непаран број.

XOR контролна сума

XOR контролна сума, која је такође позната као лонгитудинални вишак провере због начина на који се обрачунава, може се добити врло једноставно и врло брзо. Ово су важни критеријуми за откривање кодова грешака који се користе у смарт картицама. Поред тога, алгоритам може да се имплементира веома лако. Поред заштите података који се налазе у меморији, XOR контролна сума се типично користи за пренос података. XOR контролна сума се израчунава обављањем узастопне логичке XOR операције на свим бајтовима података..

Ако је контролна сума постављена директно после податка и нова контролна сума се обрачунава на основу податка и прве контролне суме, резултат је '00'. Ово је

најједноставнији начин провере да ли податак и контролна сума још увек имају своје првобитне вредности.

На жалост, XOR контролна сума такође пати од неколико озбиљних недостатака, што значајно ограничава њихову практичну примену. Она у принципу није баш сигурна. Последица свега овога је да се XOR контролна сума углавном користи за пренос података, али се користи само у врло ограниченој мери да провери доследност садржаја меморије.

CRC контролна сума

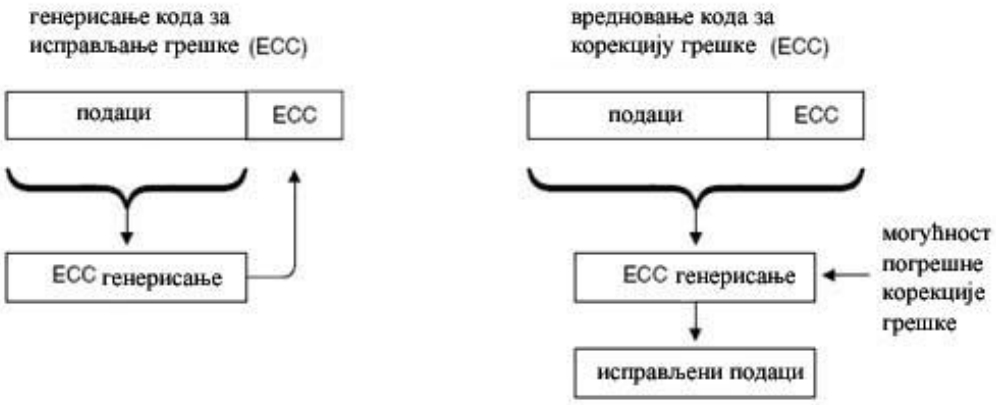
CRC метод (провера цикличног вишка) такође долази из области преноса података, али је знатно боља од XOR методе. Ипак, ова контролна сума је само код за детекцију грешке, тако да се не може користи за исправљање грешке.

CRC-16 контролна сума генерише 16-битни циклични померачки регистар и она се најчешће користи за смарт картице. Повратне информације у померачком регистру утврђују се стварањем полинома. CRC треба користити само уз количине података до 4kB, пошто вероватноћа откривања грешака оштро опада изнад ове тачке.

Главна предност CRC контролне суме је да обезбеђује поуздано откривање грешке, чак и са више грешака.. Поред тога, за разлику од XOR методе, CRC омогућава смењење бајтова података који се детектују. Међутим, веома је тешко одредити тачну вероватноћу детекције такве грешке, јер они веома зависе од локације грешке, [3].

4.2.1 Исправљање грешке

Технички најједноставније решење је да се складиштење података врши у вишеструке, физички одвојене меморије странице и користе приликом читања података. Као алтернатива за заштиту вишеструког складиштења података, могуће је користити алгоритам за корекцију грешке, као што је Рид-Соломон алгоритам. Ово је посебно погодно за употребу са кластерима грешке, које се могу јавити у смарт картици, због квара. Алгоритам заузима неколико стотина бајтова меморије када је програмиран у асемблерском језику, а величина ECC података првенствено зависи од вероватноће са којом грешка мора да буде откривена и / или правилно исправљена.



Слика 4.3 Основни принцип коришћења кода за исправљање грешке (ECC) [3]

По правилу, када се проблеми са садржајем података јаве, виши ниво система који омогућава људску интервенцију мора да одлучи шта да ради. На пример, ако се грешке се

јављају у смарт картици, власник картице ће је највероватније ручно отклонити. Ако се грешка понавља више пута, систем ће реаговати, јер постоји могућност да је EEPROM корумпиран. јер не може да обавља корекцију грешке у картици, већ систем администратор мора да интервенише, [3].

4.3 Компресија података

Као што је познато, количина доступне меморије у паметној картици озбиљно је ограничена. Постоје неке препреке које треба превазићи пре него што компресија података може да се користити. Алгоритми не смеју да заузимају превише простора у меморији, а морају да захтевају веома мало RAM-а. Поред тога, прихватљива брзина компресије би требало да буде остварена. Фактор компресије није толико важан, јер је обим података увек само пар стотина бајтова. Методе које се често користе за смарт картице су покретна дужина кодирања и променљива дужина кодирања.

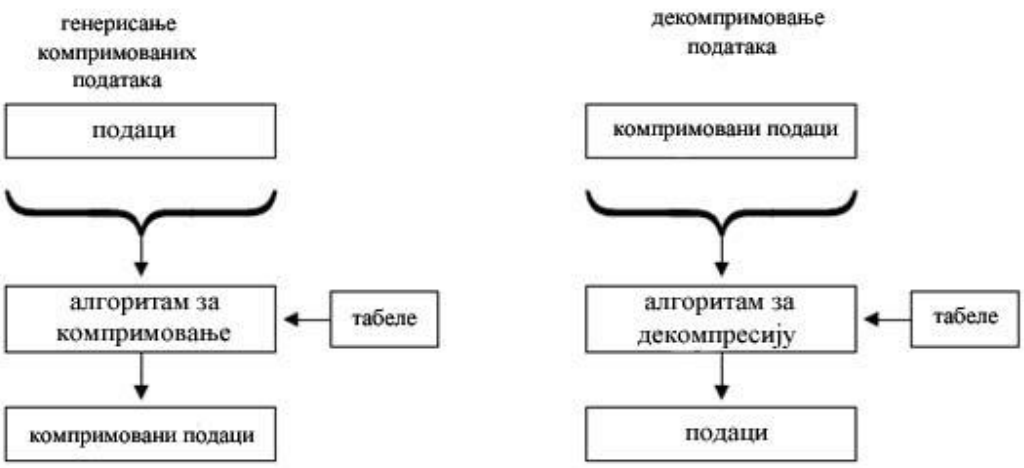
Код покретне дужине кодирања, гранични низ идентичних објеката података је замењен комбинацијом понављања рачуна и објекта (као што је карактер) која се понавља. Са променљивом дужином кодирања, учесталост појављивања карактера који је фиксне дужине (нпр., један бајт) се анализира, а карактери који се најчешће јављају су замењени знакови са краћим дужинама. Ређе се јављају знакови који су кодирани коришћењем више кодова.

Са променљивом дужином кодирања, замена је направљена коришћењем претходно дефинисаних табела. Динамичка верзија променљиве дужине кодирања прво анализира расподелу фреквенција знакова у оригиналном податку и потом конструише табелу замене на основу резултата ове анализе. Трећа варијација је адаптивна променљива дужина кодирања, у којој се табела редовно ажурира током процеса компресије да би се постигла оптимална компресија.

Динамичка и адаптивна променљива дужина кодирања не долазе у обзир за смарт картице, због комплексности њихових алгоритама и њиховог великог захтева меморије. Покретна дужина кодирања и статичка променљива дужина кодирања су, дакле, једине праве алтернативе за употребу у смарт картицама. Алгоритам за покретну дужину кодирања не захтева много кода програма, али је недостатак јер може да се користи само са понављаним подацима. Кључеви за симетричне криптографске алгоритме би били потпуно неодговарајући за компресију са овим алгоритмом, јер имају особине случајних бројева.

Статичка променљива дужина кодирања је други метод компресије који се користи за смарт картице. Сасвим је погодан за датотеке које садрже информације телефонског именика, на пример, када је структура сачуваних података позната и табела замене може бити трајно уграђена у алгоритам.

Међутим, неке ствари морају се узети у обзир у вези са компресијом података за смарт картице. У идеалном случају, компресија података треба да буде изведена у оквиру оперативног система на начин који је у потпуности транспарентан према спољном свету, тако да се некомпресовани подаци могу читати и писати на уобичајени начин користећи стандардне команде, [3].



Слика 4.4 Основни принцип компресије података за складиштење података [3]

.

4.4 Криптографске могућности

Тренутно стање је да смарт картице имају довољно криптографских могућности да подрже популарне безбедносне апликације и протоколе. RSA потпис и верификација су подржани са избором 512, 768, или 1024-битне дужине кључа. Чак и на 1024-битној дужини кључа, време потребно за обављање потписа је обично испод 1 секунде. Обично, је EEPROM фајл који садржи приватни кључ дизајниран тако да осетљиви кључни материјал никада не напушта чип. У овом случају, чак и картица не може да приступи кључном материјалу. Поред тога, коришћење приватног кључа је заштићено личним бројем корисника (PIN), тако да поседовање картице не значи способност да се потпише са картицом. Неке картице такође имплементирају пуњење које је дефинисано путем јавног RSA кључа криптографског стандардна број 1.

Иако смарт картице имају могућност да генеришу RSA пар кључева, то може бити веома споро. Типично време потребно за 1024-битни RSA пар кључева се креће од 8 секунди до 3 минута. Такође, квалитет парова кључева не може бити изузетно висок. Недостатак рачунарске снаге подразумева релативно слаб случајни број извора, као и релативно слаб алгоритам за избор великих простих бројева.

Алгоритам за дигитални потпис (DSA) је мање имплементиран од RSA. Када је имплементиран, може се обично наћи само са 512-битном дужином кључа. Смарт картице подржавају могућност да се конфигуришете више PIN-ова који могу имати различите намене, [1].

Стандард за енкрипцију података (DES) и Triple DES се најчешће налази у водећим смарт картицама. Да би се избегло клонирање картица, непроменљив серијски број је често утиснут у меморију. Картице су дизајниране да се саме ресетују ако постоји флуктуација напона, температуре или фреквенције. Читање или писање ROM-а је обично онемогућено. Сваки произвођач има своје (обично власничке) планове за ове мере, и увек је добро да се пита и / или захтева извештај независних лабораторија за испитивање.

Функционалност електронског новчаника је често присутна, али они су типично базирани на технологији симетричних кључева као што су DES и Triple DES. Дакле, заједнички тајни кључ спроводи безбедност многих од ових програма. Заједнички хеш алгоритами су SHA-1 и MD-5, али опет, низак пропусни опсег серијског прикључка омета ефикасно коришћење највећег хеша на картици.

Генерисање случајних бројева (RNG) варира између картица продаваца. Неки спроводе псеудо генератор случајних бројева, за које свака картица има јединствено семе. Неке картице имају прави, хардверски генератор случајних бројева, који се користи неке физичке аспекте силицијума. Најбоље је да се провери са продавцем за детаље RNG-а да ли ће се користити у криптографски осетљивом контексту.

Комуникацијски протоколи смарт картице на командном нивоу, често имају уграђен безбедносни протокол. Они су типично базирани на технологији симетричних кључева и омогућавају смарт картици аутентикацију читања и писања терминала или обратно. Међутим, криптограми и алгоритми за ове протоколе су обично специфични за дату примену и сету терминала, [2].

4.4.1 Дигитални потпис и дигитални сертификат

Дигитални потпис је 51-битни број који се добија применом RSA алгоритма на HASH вредност генерисану из блока података који се штити. Он се додаје на крај блока података који се шаље. Под блоком података мисли се на читав DER (Датотека за електронску размену података) осим његовог последњег дела. Дигитални потпис осигурава интегритет електронске информације, непорецивости и идентификацију потписника, али не и тајност. Провером потписа доказује се интегритет информације и идентификује се потписник. Ако је информација измењена након што је била потписана то ће се утврдити провером потписа.

Да би потписао документ, потписник мора јасно назначити границе документа који потписује. За означену поруку (податак) који треба сигурно пренети, HASH функција софтвера потписника израчунава јединствени отисак, додељен једино тој поруци. Софтвер затим трансформише отисак у дигитални потпис користећи се потписниковим тајним (приватним) кључем. Тако настали дигитални потпис је стога јединствен и за поруку и за приватни кључ који га је креирао. Уобичајено је да се дигитални потпис придодаје поруци, складишти и шаље заједно са њом. Међутим, он се може послати и као одвојени податак, докле год задржава поуздану везу са оригиналном поруком. Како је сваки потпис јединствено додељени оригинал, бесмислено га је у потпуности одвојити од извора на основу којег је настао.

Поступци креирања и верификације дигиталног потписа пролазе кроз поступке модификације већ читаву деценију, и могу се аутоматизовати до те мере да је људска интеракција потребна само у изузетним случајевима. Вероватноћа отказа или проблем безбедности у системима криптографије који су дизајнирани и имплементирани према развијеним индустријским стандардима је безначајан, и пуно је мањи од ризика непримећеног фалсификата или измене документа на папиру.

Дигитални сертификат је дигитално потписани документ који повезује јавни кључ са особом којој припада. Можемо га назвати и дигиталном личном картом, јер он то заиста и јесте - дигитална лична карта у "сајбер простору", односно средство којим доказујемо идентитет на Интернету. Уведен је из тог разлога што учесници у комуникацији, да би уопште могли да комуницирају, морају на неки начин сазнати кључеве својих партнера. Осим тога, морају бити уверени да партнери нису уљези који се лажно представљају. Сертификат се дигитално потписује из тог разлога што се обезбеђује његов интегритет, који гарантује потписник. Потписник дигиталног сертификата назива се сертификацијски центар.

Све ове безбедносне механизме овде наведене обједињује сложени систем у којем се одвија сигурна комуникација, а који се назива инфраструктура јавног кључа, [17].

4.5 Оперативни системи смарт картица

Термин оперативни систем, дакле, није аутоматски ограничен на огромне програме и количине података. Уместо тога, он је потпуно независан од величине, јер се односи само на функционалност. Чињеница да оперативни систем омогућава интерфејс између хардвера и стварног апликативног софтвера је такође важна, јер онемогућава апликативни софтвер да се директно обрати хардверу. Ово је значајна предност, јер омогућава примену софтвера са одређеном количином преносивости, иако је то често веома ограничено.

Чип Оперативни Систем смарт картица (COS) је трајни низ инструкција уграђен у ROM смарт картице. COS инструкције не зависе од одређене апликације али се најчешће користе у већини апликација, [14].

Чип оперативни системи се деле на две породице:

- опште намене који поседује генерички командни сет у којем различите секвенце покривају већину примена
- посвећен OS са командама дизајнираним за специфичне примене које могу чак и да садрже само апликације

Основне функције COS који су заједничке за све смарт картице укључују:

- Управљање разменом података између картице и спољног света, тј протоколе за управљање
- Управљање датотекама и меморијом
- Контрола приступа информацијама и функцијама картице
- Управљање безбедношћу картице
- Заштита података
- Управљање различитим фазама животног циклуса картице

Основни однос између смарт картице и терминала је по принципу слуге и господара. Терминал шаље команду смарт картици, смарт картица извршава команду, враћа резултат терминалу ако их има и чека другу команду.

Већина смарт картица данас користи сопствени оперативни систем за комуникацију и основне функције. Дакле, нови тренд у систему смарт картица је JavaCard оперативни систем који је развијен од стране Сун Микросистема и потом унапређен у JavaCard Форум. Оперативни систем Јава картица је популаран јер даје независност програмерима. Java OS може користити било који произвођач смарт картица. Предност JavaCard OS омогућава концепт накнадне измене, омогућавајући надоградњу апликација на паметној картици након предаје картице крајњем кориснику, [9].

Архитектура Java OS

Типичан уређај Јава картица има 8 - или 16-битни процесор који ради на 3.7 MHz, са 1k RAM и више од 16k за меморије типа EEPROM-а или флеш. Високоперформансне паметне картице долазе са одвојеним процесором и криптографским чипом и меморијом за енкрипцију, а неки долазе са 32-битним процесорима.

Java Card технологија се састоји из три дела:

- Java Card виртуелна машина дефинише подскуп Јава програмских језика и VM за смарт картице
- Јави картица са временом извршења понашања за Јава смарт картице
- Java Card API спецификација картица, којим се дефинишу основни оквири и проширења Јава пакета и класа за апликације смарт картица

MULTOS (Вишеоперативни систем)

MULTOS је оперативни систем који омогућава да се више апликација и програма инсталира и борави одвојено и безбедно на смарт картици. Сваки програм је изолован од оперативног систем тако да не може ометати примену оног другог. Ранији системи смарт картице нису дозвољавали новим апликацијама да се инсталирају а да се не обрише старе, MULTOS ово омогућава. Исправке или закрпе могу такође бити инсталиране по потреби. Свака апликација је независна од платформе, због примене виртуелне машине. Програмери пишу апликације за смарт картице MULTOS користећи MULTOS Извршни Језик (MEL).

Безбедност за MULTOS смарт картице обезбеђује MULTOS сертификационо тело (CA), које издаје криптографске кључеве за сваку MULTOS смарт картицу и све MULTOS апликације. Ови тастери спречавају да неовлашћене апликације буду учитане у картицу или обрисане без дозволе издаваоца. MULTOS је подражан од стране свих водећи компанија из ове области MasterCard, Europay, [3].

Windowsc за смарт картице (WFSC)

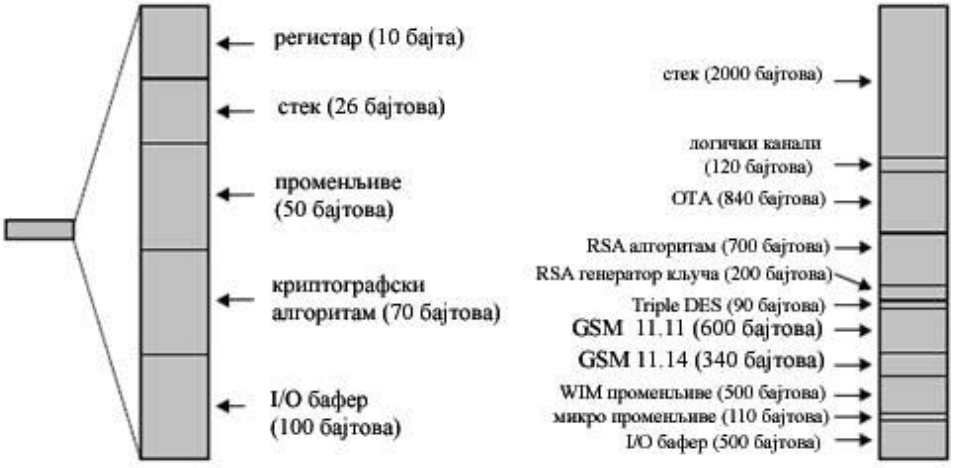
Windows за смарт картице је развијен и затражен од стране Мајкрософт-а. То је микрорачунар без Графичког корисничког интерфејса (GUI). Повећава постојећу корпоративну мрежу засновану на Windows OS фамилији. Може се прилагодити сваком кориснику и може се програмирати за више тастера. Овакве картице се могу користити за пријаву на рачунар или за једну или више мрежа и извођење удаљеног пријављивања, тако што ће се ускладиштити све аутентификацијске информације корисника, [18].

Отворена платформа

Отворена платформа представља скуп међуиндустријске техничке спецификације, која може да се користи за развој безбедних и флексибилних система цмарт картице. Компоненте као што су картице и терминали, дефинишу платформу смарт картице која је лака за коришћење на којој су стандардизоване апликације, као што су плаћање кредитним и дебитним картицама, електронски новчаник. Отворена платформа функционише са различитим картицама и оперативним системима. Она омогућава емитенатима смарт картица да бирају између оперативних система и апликација уз обезбеђивање основне безбедности. Термин "отворена платформа" је првобитно сковала Visa. Сада је спецификација, стандардизована од стране GlobalPlatform организације, која је преименована у "GlobalPlatform спецификација", [4].

4.5.1 Организација меморије

Уобичајена организација меморије 256 бајта RAM-а подељена је на регионе за регистре, стек меморију, променљиве, радни простор за криптографске алгоритме и U/I бафер. Ако је U/I бафер од 256 бајтова потребан, на пример, или ако додатна променљива мора да се чува у RAM-у, до граница расположиве меморије се може доћи веома брзо. Овај проблем је решен тако што постоји радни простор у EEPROM меморији, која се на тај начин користи као RAM. Недостатак овог решења је да је потребно око 10.000 пута више времена да се упишу подаци у EEPROM, него када се подаци уписују у RAM. Додатна мана је ограничен век EEPROM ћелија, јер за разлику од RAM ћелије, не могу бити уписивани неограничен број пута. Међутим, померање садржаја из RAM-а у EEPROM је често једино решење, на пример када је U/I бафер већи од целокупног износа расположивог RAM -а. За поређење, слика показује типичну организацију 6 kB RAM -а високих перформанси телекомуникацијској смарт картици, [16].



Слика 4.5 Дијаграм са леве стране приказује типичну поделу 256 бајтова RAM-а за једноставну смарт картицу. Дијаграм на десној страни показује организацију меморије 6MB RAM-а смарт картица за високе перформансе у телекомуникацији [3]

Организација података који се налазе у EEPROM-у је много компликованија и замршенија него код друга два типа меморије.

4.5.2 Датотеке смарт картица

Прве смарт картице имале су мање или више директно адресабилни регион меморије, које може да се користи за упис или читање података. Подацима се приступа тако што се наводи физичка меморијска адреса. Данас, све паметне картице имају потпуно хијерархијско управљање системима датотека са симболичним, хардверски независним адресирањем.

Наравно, ови системи за управљање датотекама имају одређене карактеристике које су специфичне за смарт картице. Најочигледнија особина је да не постоји интерфејс човек-машина. Све датотеке су адресиране коришћењем хексадецималних кодова, а све команде су стриктно на основу овог адресирања, јер се комуникација одвија само између два

рачунара. Исто тако за системе за управљање датотекама типично је то што су дизајнирани да користе малу количину меморије.

Савремени системи за управљање датотекама смарт картице имају објектно оријентисану структуру. То значи да се све информације о датотекама чувају у самој датотеци. Фајлови у таквом објектно-оријентисаном систему су увек подељени на два дела. Први део, је заглавље датотеке, који садржи информације о изгледу и структури датотека и условима приступа. Кориснички подаци који се модификују чувају се у другом делу, који је повезан са заглављем датотеке показивачем, [3].

Поред тога што пружа веће структурирање података, ова шема такође има предност обезбеђујући бољу физичку безбедност података. Заглавље датотека и тело датотеке увек се налазе на посебним страницама меморије. Заглавље, које се обично ретко мења, чува све услове приступа. Писање или брисање грешке које укључује тело датотеке не може утицати на ове услове.

Неки оперативни системи смарт картица нуде могућност адресирања тела датотеке из два различита заглавља. Ова два заглавља се обично налазе у директоријуму фајла и припадају двема различитим апликацијама. Ово омогућава да се подаци размењују између две апликације на технички елегантан начин. У овом случају, важно је услови приступа у два заглавља биду идентична.

4.5.2.1 Типови датотека

У основи постоје две категорије фајлова за смарт картице. Прва категорија је директоријум фајлова, које се зову посвећени фајлови DF. Друга категорија се састоји од датотека које садрже стварне податке корисника, која се зове основни фајлови EF, [3].

MF

Рут (корен) директоријум се зове главна датотека. Имплицитно се бира након што се смарт картица ресетује и садржи све друге директоријуме и све датотеке.

DF

Датотеке директоријума могу постојати хијерархијски испод мастер датотека према потреби. Оне могу да садрже друге датотеке директоријума. Број нивоа није ограничен иако због ограничене меморије на картици ретко постоји више од два поднивоа.

EF

Кориснички подаци потребни за примену налазе се у основном фајлу, који може да се налази директно испод MF-а или испод DF-а. Да би се омогућило да се подаци чувају у минималном износу меморије и логично оптимизованим структурама података, EF увек има унутрашњу структуру датотеке. EF је класификован на радни EF и унутрашњи EF. Сви подаци који морају бити прочитани или написани од стране терминала, налазе се у радном EF-у. Подаци садржани у тим датотекама се не користе од стране оперативног система. Поред EF-а за апликације, постоји и интерни систем датотека који складишти податке за сам оперативни систем, податке за извршење пријаве, тајне кључеве и програмски код. Приступ овим подацима је специјално заштићен оперативним системом.

4.5.2.2 Имена датотека

У модерним оперативним системима смарт картица, фајлови се без изузетка адресирају логичким именима, уместо да им се приступа коришћењем директне физичке адресе. Све шеме које користе логичка имена датотека су значајно боље, а изнад свега много лакше се проширују.

Идентификатор датотека (FID)

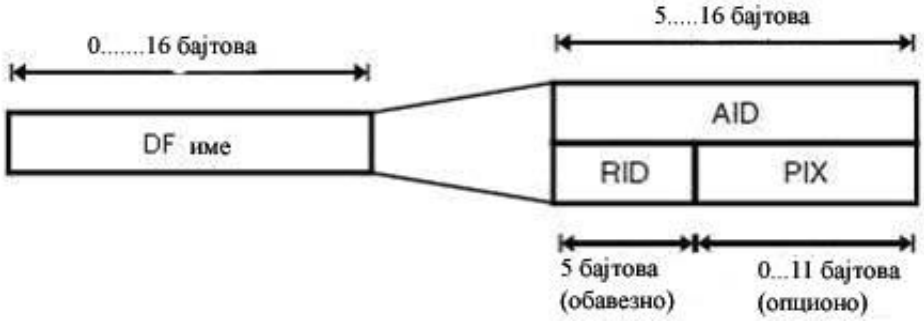
Сваки фајл, укључујући и директоријум датотека, има 2 бајта за идентификатор фајла (FID), који се може користити да би се изабрала датотека. FID-ове у стаблу датотека треба одабрати тако да су фајлови недвосмислено изабрани. Забрањено је да два различита фајла у истом DF-у имају исти FID.

Кратак идентификатор датотека (SFI)

Кратак идентификатор датотека може се користити за имплицитни избор датотека у непосредном контексту команде. SFI се преноси као параметар команде за имплицитни избор датотека и дуг је само 5 бита.

DF име

DF је нека врста директоријума, и може да садржи и EF и друге DF-ове. DF име има дужину од 1 до 16 бајта, и обезбеђује довољно адресног простора да омогући свакој апликацији смарт картице недвосмислену идентификацију. Како су имена слободно изабрана, могуће је да два различита DF-а понекад имају исто име. Као последица тога, име се обично користи само заједно са AID-ом (апликациони идентификатори). AID може имати дужину између 5 и 16 бајта и састоји се из два елемента.



Слика 4.6 DF име у односу на AID [3]

Апликациони идентификатор (AID) се састоји од два елемента података. Први елемент је регистровани идентификатор (RID), који је фиксне дужине од 5 бајта. Ако је потребно, добављач апликације може да стави власнички апликациони идентификатор продужетка (PIX) после RID-а, і може бити до 11 бајтова дуг, [3].

4.6 Пренос података смарт картица

Могућност двосмерне комуникације је предуслов за све интеракције између смарт картице и терминала. Међутим, само једна линија је на располагању. Дигитални подаци се размењују између картице и терминала преко ове електричне везе. Како постоји само једна линија, картице и терминали морају да се смењују током преноса података,где једна страна делује као прималац. Овај алтернативни пренос и примање података се назива полу-дуплекс поступак.

После убацивања картице у терминал, њени контакти се прво механички повезују са контактима терминала. Пет активних контакта потом је електрично омогућено у исправној секуенци. Након тога, картица аутоматски извршава напајање и онда терминалу шаље одговор на ресет (ATR). Терминал оцењује ATR, који садржи разне параметаре који се односе на картицу и пренос података, а затим шаље прве команде. Картица генерише одговор, који се поново шаље терминалу. Овакав процес се наставља све док се картица не деактивира.

Између ATR-а и прве команде послате картици, терминал може да шаље параметарки протокол селекција (PPS). Терминал може да користи ову команду, која је независна од протокола преноса.

4.6.1 Одговор на ресет (ATR)

Након напона напајања, примењују се сигнали такта и ресета, Смарт картица шаље одговор на ресет преко U/I порта. Овај низ података, који садржи највише 33 бајта, увек се шаље са разделником вредности. Он садржи разне параметре који се односе на протоколе за пренос и картицу. Овај разделник вредности треба да се користи чак и ако се протоколи за пренос користе након што ATR запосли различите разделнике вредности (нпр. 64). Овим се обезбеђује да се ATR из било које картице увек може примити, без обзира на параметре протокола преноса.

Веома је ретко да ATR има максимално дозвољену дужину. Најчешће се састоји само од неколико бајтова. Посебно у апликацијама где би картица требало да буде употребљива веома брзо након секвенце активирања, ATR треба да буде кратак. Типичан пример је плаћање путарине коришћењем смарт картица.

Прва два бајта, TC и T0, дефинишу неколико основних параметара за пренос и указују на присуство наредних бајтова. Интерфејс одређује специјалне трансмисионе параметаре за протокол, који су важни за следећи пренос података. Знак за проверу, је контролна сума претходних бајтова.

Почетни карактер

Помоћу овог знака се одређује брзина преноса података, и конвенција о редоследу битова као и њихова интерпретација. Постоје две конвенције директна и инверзна. Код инверзне конвенције је нисконапонски ниво интерпретиран као логичка јединица а први послати бит има највећу тежину. Сви терминали и многе смарт картице подржавају обе конвенције.

Формат карактера

Други бајт, T0 садржи бит поље које указује на то који карактери следе у ATR-у. Он такође указује на број историјских карактера. Као што је TC, и овај бајт мора бити присутан у сваком ATR-у.

Интерфејс карактери

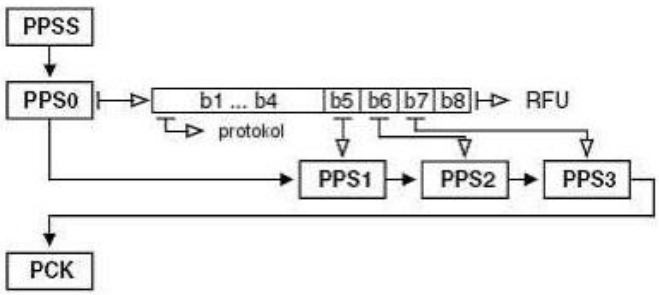
Интерфејс карактери прецизирају све параметре преноса за текући протокол. Они се састоје од TA, TB, TC и TD бајтова. Међутим, ови бајтови су опциони у ATR-у, и могу се изоставити на одговарајући начин. Могу се поделити на глобалне параметре који се односе на све могуће протоколе и на специфичне параметре који се односе само на неки одређени протокол. Неки од глобалних параметара односе се само на T = 0 протокол, и може се изоставити ако се тај протокол не користи.

Глобални интерфејс карактер TA1 дефинише глобалне параметре FI и DI. FI је делилац такта а DI је фактор подешавања брзине преноса. Глобални интерфејс карактер TB1 се користи како би се одредио напонски ниво који је потребан за програмирање меморије картице. Глобални интерфејс карактер TC1 се такође сврстава у групу глобалних. Он кодира евентуално додатно "чувано време". То време се додаје на трајање стоп бита. Историјски знакови нису обухваћени стандардом и из тог разога могу да обухватају широк опсег информација зависно од произвођача паметних картица. Неки произвођачи су их користили за идентификацију оперативног система и верзију меморије.

Знак за проверу је последњи бајт у ATR-у је знак провере (TCK). Вредност овог знака мора бити таква да операцијом XOR над свим знаковима од T0 до TCK добијемо нулу. TCK бајт мора бити присутан у T= 1 протоколу, [5].

4.6.2 Селекција параметра протокола (PPS)

Током одговора на ресет паметна картица специфицира разне параметре преноса података. Ако терминал жели да промени неке параметре мора да спроведе селекцију параметара протокола PPS пре него што почне размена података. Ова процедура може да се спроведе на два начина. Према једном (режим по договору) стандардне вредности F и D остају непромињењене док се PPS успешно не заврши, а према другом (специфични режим) PPS се извршава користећи вредности F и D наведене у ATR-у. PPS се мора спровести одмах након одговора на ресет. Ако картица прихвата захтеве из PPS-а онда мора вратити примљене PPS бајтове назад терминалу. Стандард забрањује поновно слање PPS података. У пракси PPS се ретко користи јер се обично параметри картица и терминала унапред утврђују, [3].



Слика 4.7 Основна структура и елементи података из PPS-а [16]

Елемент	Намена
PPSS	Иницијални знак
PPS0	Знак формата
PPS1, PPS2, PPS3	Знакови параметара
PCK	Знак за проверу

Табела 4.1 PPS елементи података и њихове ознаке [3]

4.6.3 Протоколи за пренос података

Постоје разни начини којима се успоставља комуникација смарт картицом. Такође постоји различити број метода за ресинхронизацију комуникације ако се деси поремећај. Тачна имплементација команди, одговарајући одговори и поступци који се користе у случају грешке преноса је дефинисана у облику протокола преноса.

Протоколи се обележавају са 'T =' (протокол за пренос) и редним бројем. Тај број је управо онај који је кодиран у знаку TD1.

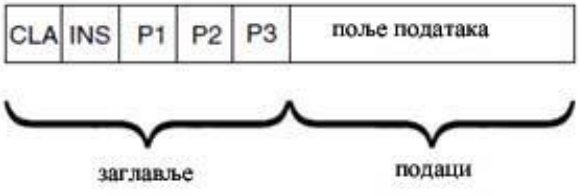
Протокол	Значење
T=0	Асинхрони, полудуплексни, пренос података у бајтовима
T=1	Асинхрони, полудуплексни, пренос података у блоковима
T=2	Асинхрони, дуплексни, пренос података у блоковима
T=3	Дуплексни, још није специфициран
T=4	Асинхрони, полудуплексни, пренос података у бајтовима, екстензија T = 0 протокола, још није специфициран
T=5 ... T=13	Резервисано за будућу употребу, још није специфицирано
T=14	За националну употребу, није ИСО стандардизован
T=15	Резервисан за будућу употребу, још није специфициран

Табела 4.2 Протоколи за пренос података [8]

Два од ових протокола доминирају у међународној употреби. Први је T=0 протокол а други је T=1.

4.6.3.1 T = 0 преносни протокол

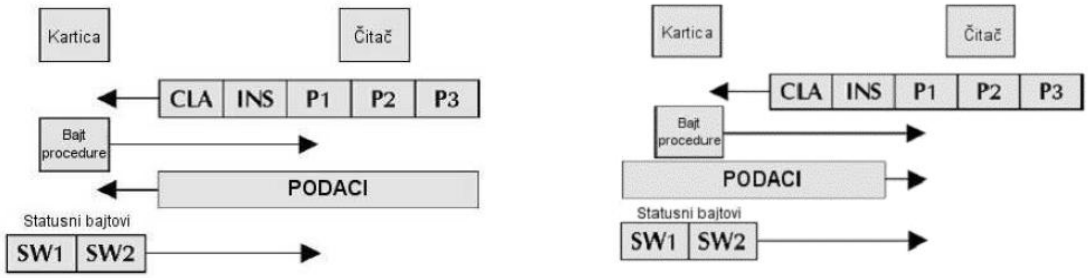
T=0 је био једини протокол иницијално специфициран у ISO 7816-3 стандарду 1989 године. С обзиром на снагу хардвера којом се тада располагало дизајниран је како би користио што мање меморије и био максимално једноставан. Користи се и у GSM картицама те га то цини најшире коришћеним од свих картичних протокола. Овај протокол је бајтно орјентисан што значи да је најмања преносива јединица управо један бајт. Наредба која се преноси састоји се од заглавља (хедер) и опционог поља података. Заглавље се се састоји од бајта класе, бајта команде и три бајта параметара, [3].



Слика 4.8 Структура команде код T = 0 протокола [11]

Уколико се догоди грешка при преносу података мора се одмах поновити нетачан бајт, док се код протокола оријентисаних на пренос блока података поново преноси цео блок. Откривање грешке се базира искључиво на провери паритетног бита који је део сваког послатог бајта.

Како бисмо приказали ток комуникације између картице и терминала претпоставимо да терминал шаље картици команду са пољем података. Терминал ће прво послати заглавље, и чекати да оно буде потврђено бајтом процедуре. Кад се то догоди терминал шаље податке дужине онолико бајтова колико је било назначено у бајту P3. Сад је картица примила целу команду, може је извршити и генерисати одговор. Одговор се састоји од два статусна бајта SW1 и SW2 и евентуално од неких додатних података што је назначено у бајту SW2. Након што терминал прими статусне бајтове он "зна" да ли жели да му картица пошаље још података. Тиме се затвара циклус једне наредбе, [11].



Слика 4.9 Пренос података између а) терминала и картице б) картице и терминала [11]

T=0 протокол омогућава картици примање података један по један бајт након примања заглавља. То се остварује слањем инвертног бајта команде терминалу, после којег терминал шаље један бајт податка. Следећи бајт податка ће бити послат након следећег бајта процедуре. То се наставља све док картица не прими све податке или док не пошаље неинвертни бајт команде терминалу као бајт процедуре.

Механизам за откривање грешака T=0 протокола састоји се само од провере паритета на крају сваког бајта. Ово омогућава поуздано препознавање једнобитне грешаке, али двобитне грешке се не могу детектовати. Ако је бајт изгубљен током преноса, долази у бесконачне петље (застоја) у картици, јер се очекује одређени број бајтова. Једини практичан начин за терминал да побегне из ове ситуације је да ресетује картицу и успостави комуникацију поново од почетка. Главне предности T=0 протокола су добре просечне брзине преноса, минимална имплементација и широка употреба.

4.6.3.2 T = 1 преносни протокол

T=1 протокол је тренутно једини међународни протокол за паметне картице који без компромиса може омогућити сигуран пренос података. Он такође уклања ограничење протокола T=0 према којем је терминал увек био тај који би иницирао команду а картица би одговарала. Сада и картица и терминал, у оквирима протокола, могу иницирати команду, [11].

Структура блока

Послати блокови се користе у две различите сврхе. Једна је транспарентно слање апликационих података док је друга слање контролних знакова протокола или баратање грешкама у преносу. Блок за слање података се састоји од пролог поља, информационог поља и епилог поља. Пролог и епилог поља су обавезна и морају увек бити послата. Информационо поље је опционо и садржи податке за апликациони слој, који је или APDU команда послата картици или APDU одговор картице.

Постоје три типа блокова у T=1: информациони блок, блок за потврду пријема и системски блок. Информациони блокови служе за транспарентну размену података апликационог нивоа. Блокови за потврду пријема који не садрже поља података служе за потврђивање или негирање пријема. Системски блокови служе за контролу информација везаних за сам протокол. Могу садржати информационо поље.

Пролог поље

Састоји се од три поља: адресе чвора (NAD), контролног бајта протокола (PCB) и дужине (LEN). Дугачко је три бајта и садржи основне контролне податке и показиваче за актуелни блок. Адреса чвора садржи адресу одредишта и изворишта блока. Сваки је кодиран користећи три бита. Контролни бајт протокола служи за контролу и надгледање протокола. Он повећава количину потребног кодирања. Поље дужине садржи дужину информационог поља у хексадецималној форми, [3].

Информационо поље

У I блоку ово поље служи као резервоар за податке апликационог слоја. Садржај овог поља се шаље потпуно транспарентно, тј. протокол га не оцењује ни интерпретира. S блок садржи податке за протокол. Једино се у овом случају садржај овог поља користи у преносном слоју.

Епилог поље

Ово поље се налази на крају блока. Садржи код за детекцију грешака који је израчунат на основу свих претходних бајтова у блоку. Употребљава се или LRC (лонгитудинална провера редундантности) или CRC (циклична провера редундантности). Будући да је та операција брза и једноставна може се изводити у лету и стандардни је део свих T=1 имплементација.

Бројач редоследа слање / пријем

Сваки информациони блок у T=1 протоколу има секвенцу слања броја који се састоји од само једног бита који се налази у PCB бајту. Овај број је увећан по модулу 2. Основна сврха бројача послатог низа је да подржи захтеве за поновно слање блокова који су са грешком.

Време чекања

Дефинисано је неколико времена чекања како би се пошиљаоцима и примаоцима назначили интервали за разне акције током преноса података. Оно такође представља начин избегавања комплетног застоја.

Време чекања на знак (CWT) дефинисано је као максимални интервал између два знака унутар блока. Прималац активира бројач на сваку узлазну ивицу користећи CWT као иницијалну вредност. Ако бројач дође до нуле пре него што се региструје нова узлазна ивица прималац претпоставља да је блок у целости примљен.

Сврха времена чекања на блок (BWT) је да се омогући прекид комуникације ако картица не одговара. Оно је дефинисано као временски интервал између узлазне ивице последњег бајта у послатом блоку и узлазне ивице првог бајта којег картица враћа. Уколико тај интервал истекне терминал може претпоставити да са картицом нешто није у реду, и предузме одговарајућу акцију, нпр ресетује картицу.

Чувано време блока (BGT) дефинисано је као најмањи интервал између узлазне ивице последњег бајта и узлазне ивице првог бајта у супротном смеру. Сврха овог времена је да осигура пошиљаоцу временски интервал у којем се пребацује из слања у пријем, [3].

4.6.3.3 T = 14 преносни протокол и USB протокол

ISO/IEC 7816-3 стандард у одговору на ресет предвиђа ознаку за националне комуникационе протоколе. Такав протокол је T=14. Створен кад се указала потреба за протоколом који би служио за комуникацију између мобилних телефона и паметних картица. Оставио је дубок утицај на развој свог наследника протокола T=1. Управо га је он и заменио те се T=14 више не користи.

USB протокол, који је превагнуо над сличнима кад је реч о примени на паметним картицама. Он захтева посебну компоненту на процесору картице. Он такође доноси веће брзине преноса од T=0 и T=1 протокола. Чини се да ће за комуникацију са картицама бити коришћена верзија 1.1, са могућношћу спорог и брзог преноса. Наведене брзине се смањују кад се узму у обзир подаци протокола који се такође преносе, [11].

4.6.3.4 Структура поруке APDU

Овај део стандарда се наставља на дефиницију протокола T=1 из стандарда ISO 7816-3 и дефинише структуру APDU. APDU се користи за размену свих података између картице и терминала и он је стандардизован за апликациони слој. Његов садржај и структура морају бити независни од комуникационог протокола. Постоје два типа APDU-а, APDU наредбе и APDU одговора.

Слика 4.10 Структура APDU поруке [11]

APDU наредбе

Састоји се од заглавља и тела. Тело може имати промењљиву дужину, или може бити потпуно одсутно уколико је поље податка празно. Заглавље се састоји од четири елемента, који су бајт класа (CLA), бајт инструкција (INS) и два бајта параметра (P1 и P2). Класа се такође користи за идентификацију апликације и специфичне скупове команди. Следећи бајт у командном APDU је инструкција, која кодира стварну команду. Скоро цео адресни простор овог бајта може бити искоришћен. Два параметра се примарно користе да пруже више информација о изабраној командни од стране инструкције. LE и LC поља су обично један бајт, али могу да се конвертују у поља која су три бајта дуга.

APDU одговора

Састоји се од опционог тела и обавезног наставка. Тело се састоји од дела података, чија је дужина одређена Ле пољем из APDU-а команде. Уколико се догоди грешка приликом извођења команде APDU не мора да садржи део података. У том случају се информација о грешци види из статусних знакова, [11].

Закључак

У овом раду је кроз четири поглавља описано тренутно стање у области смарт картица. У другом делу је било речи о развоју самих картица и разлозима за њихово увођење, као и о областима у којима се користе. Треће поглавље даје преглед физичких и електричних карактеристика смарт картица. Информатичке основе које су неизоставни део сваке смарт картице су описане у четвртом делу овог рада. Приказани су оперативни системи који се јављају, као и сама структура датотека и организација меморије. Криптографске основе које су неизоставни део смарт картице су дате само кроз један осврт, јер су исувише комплексне и преобимне и свакако би биле тема за неки други рад.

Употреба картица у данашње време постаје све учесталија. Као што су рачунари постали део свакидашњице, картице су постале нешто што се подразумева и омогућује активно присуство у дигиталном свету. Могућности картица из дана у дан постају све веће, тако да једна картица постаје све универзалнија. Као пример могу се узети развијеније земље које користе смарт картице у систему здравства и на тај начин комплетан здравствени картон и сву евиденцију пацијената су сместиле на једну картицу.

Развој смарт картица отворио је многе нове визије будућности, стварајући потрошачки живот завидно једноставнијим. Свеједно, пред технологијом смарт картица се налази још доста проблема које треба решити, а то су пре свега питања приватности и безбедности података. Ову технологију не треба посматрати као замену за остале начине идентификације и обележавања већ као комплементарну технологију.

Уколико се узме у обзир убрзани развој супер смарт картица долази се до закључка да ће употреба картица а пре свега њихова мобилност у многоме олакшати свакодневни живот, поред већ приступне личне карте са чипом, маркица за превоз, контроле приступа и сл. У наредним годинама, може се очекивати да ова технологија надмаши све остале, поготово што је још увек у повоју и нема јој краја, а ни консолидација није на видику. Технологија смарт картица напредује огромном брзином.

На крају би требало истаћи да је смарт картица уколико се испоштују сви стандарди приликом њене производње изузетно сигуран уређај, те као таква може послужити за смештање изузетно поверљивих информација почевши од биометријских информација па све до финансијских.

Литература

[1] U.S. General Services Administration (2004) "Government smart card handbook" Smart Card Alliance 191 Clarksville Road, Princeton Junction, New Jersey 08550 (USA)

[2] Yahya Haghiri., Thomas Tarantino (2002). "Smart Card Manufacturing", John Wiley & Sons, Ltd Baffins Lane, Chichester West Sussex, PO 19 1 UD, England

[3] Wolfgang R., Wolfgang E (2002). "Smart card handbook, third edition", John Wiley & Sons, Ltd Baffins Lane, Chichester West Sussex, PO 19 1 UD, England

[4] http://www.visa.com/openplatform. ,октобар 2011

[5] www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

[6] http://www.smartcardclub.co.uk/ , септембар 2011

[7] http://www.smartcardforum.org/ , октобар-новембар 2011

[8] http://www.cherrycorp.com/english/keyboards/faqs/index.htm новембар 2011

[9] http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev.html

[10] http://www.chipcard.ibm.com/ , новембар 2011

[11] http://www.smartcard.co.uk/tutorials/sct-itsc.pdf, октобар 2011

[12] http://www.smartcardbasics.com/smart-card-types.html , новембар 2011

[13] http://www.smart-card.com/category/chip-card , новембар 2011

[14] http://www.javacard.org/others/, новембар 2011

[15] www.cardsweek.com, новембар 2011

[16] http://www.gorferay.com/types-of-cards/, новембар 2011

[17] http://www.itsecurity.com/dictionary/tamper.htm, новембар 2011

[18] http://developers.sun.com/techtopics/mobility/javacard/articles, новембар 2011

[19] http://www.cyantechnology.com/public/manuals ,октобар 2011