Zaščita negotovinskih oblik plačevanja

Aleš Zelenik, Zdenko Mezgec
Margento R&D, d. o. o., Gosposvetska cesta 84, 2000 Maribor
ales.zelenik@margento.com, zdenko.mezgec@margento.com

Izvleček

Negotovinske oblike plačevanja se vse bolj uveljavljajo. Pri tem je treba zagotoviti visoko raven varnosti, saj skozi negotovinske sisteme prehajajo velike količine denarja. Pomemben korak pri tem so naredili glavni izdajatelji plačilnih kartic s specifikacijami EMV, ki naj bi stopile v veljavo leta 2011. Članek podrobneje predstavi postopke, ki jih zahtevajo specifikacije EMV, kot tudi druge zahteve, ki jih morajo izpolniti udeleženci negotovinskih sistemov. Poleg kartičnega poslovanja je predstavljeno tudi alternativno negotovinsko plačevanje z uporabo mobilnega telefona. Pri tem so opisane zaščite in njihova podobnost z zaščitami pri kartičnem poslovanju.

Ključne besede: negotovinsko plačevanje, plačilne kartice, EMV, zaščita, mobilno plačevanje, Margento, zaščita.

Abstract

CASHLESS PAYMENT SECURITY

Nowadays, more and more people use systems that provide cashless payments. With cashless payment, it is necessary to ensure a high level of security, because through these systems huge amounts of money are transferred every day. Main payment card issuers had made a huge step ahead, with EMV specifications, which should come into force in 2011. The article presents in detail the procedures required by the EMV specifications, as well as other requirements that providers of cashless systems must meet. In addition, an alternative cashless system is presented, that is, payments with user's mobile phone. It describes the level of protection and its similarity with the security features of card payments.

Keywords: cashless payment, payment cards, EMV, security, mobile payment, Margento, security.

1 UVOD

Danes smo priča velikemu razmahu negotovinskih oblik plačevanja, ki z vsakim dnem privabijo nove uporabnike. Nekateri izmed njih so odločeni, da bodo iz gole radovednosti le preizkusili novi način plačevanja in nato še naprej uporabljali stari preverjeni način plačevanja z denarjem, vendar jih po prvi uporabi preprosta uporaba negotovinskih oblik plačevanja velikokrat pritegne in postanejo redni uporabniki. S takšnim načinom se število uporabnikov nezadržno veča, s tem pa se povečuje tudi skupni tok denarja, ki prehaja skozi negotovinske sisteme.

Velike vsote denarja pa vedno privabijo nepridiprave, ki želijo delež tega denarja zase. Tega se proizvajalci in razvijalci negotovinskih plačilnih sistemov dobro zavedajo, zato poskušajo storiti vse, kar je v njihovi moči, da bi raznim nepridipravom onemogočili delovanje. Žal ni popolne varnosti, zato je vzdrževanje visoke ravni varnosti tekmovanje med tistimi, ki razvijajo varnostne mehanizme, in tistimi, ki hočejo zaobiti te mehanizme.

S pojavom računalnikov in naprednejših šifrirnih postopkov se je tekmovanje zaostrilo, saj morajo na trg zaradi vse višje procesorske moči[1] prihajati nove oblike zaščite ter novi predvsem procesorsko zahtevnejši algoritmi. Problem v zagotavljanju varnosti se dodatno povečuje zaradi odprte politike finančnih ustanov, ki dovoljujejo neposreden dostop do posameznih finančnih storitev. Rezultat tega predstavlja neskončno iskanje novih oz. izboljšanih varnostnih sistemov s čim višjimi ravnmi zaščite.

2 PLAČILNE KARTICE

Najbolj pogost in uveljavljen način negotovinskega plačevanja so plačilne kartice. Prve so se pojavile v začetku dvajsetega stoletja v Ameriki. Za njihovo uporabo so zaslužne velike naftne družbe, verige hotelov in velikih trgovin, ki so jih začele izdajati svojim večjim potrošnikom [10]. Podjetje Diners Club je leta 1950 izdalo prvo pravo plačilno kartico, s katero je bilo sprva mogoče plačevati hrano v štirinajstih restavracijah v New Yorku. Zaradi velikega uspeha kartic Diners Cluba so se finančne ustanove kmalu odločile, da ustvarijo svoje plačilne kartice. Tako je Bank of America leta 1958 izdala svojo plačilno kartico BankAmericard, leta 1966 pa je konkurenčna Interbank Card Assosiation začela izdajati svoje plačilne kartice Master Charge: The Interbank Card. Ti dve organizaciji sta predhodnici izdajateljev današ-

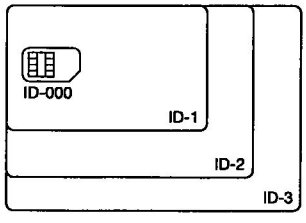
[1] Moorov zakon: procesorska moč se podvoji vsakih 18 mesecev.

njih najbolj razširjenih plačilnih kartic VISA in MasterCard [12].

Prve kartice so bile natisnjene na papirju, kar je zadoščalo le za najnižjo stopnjo varnosti, zato so jih hitro zamenjale plastične kartice. Številko računa na plastičnih karticah so kmalu začeli izpisovati reliefno, kar je omogočilo prvi korak k avtomatizaciji plačevanja [11]. Leta 1970 so karticam zaradi varnosti in možnosti strojnega obdelovanja podatkov na zadnjo stran dodali magnetni trak. Tako so kartice z odobritvijo standardov postale del informacijske dobe. Ker so podatki znotraj magnetnega zapisa prosto dostopni, se je uvedla osebna identifikacijska številka, imenovana PIN, poleg nje pa se je na zadnji strani kartice nahajal tudi podpis imetnika kartice.

Kartice, opremljene z magnetnim zapisom, danes ne zagotavljajo več dovolj visoke ravni varnosti, saj je magnetni zapis relativno preprosto kopirati in si narediti dvojnike kartic, imetniki kartic žal na številko PIN ne pazijo dovolj, medtem ko lahko podpis z nekaj vaje dokaj zadovoljivo ponaredimo. Zaradi omenjenih razlogov je predvideno, da bodo kartice z magnetnim zapisom v obtoku le še do leta 2011, ko jih bodo zamenjale pametne kartice [7]. S tem pojmom označujemo kartice z integriranim vezjem, ki so lahko le pomnilniške, lahko pa vsebujejo tudi mikroprocesor in druge potrebne komponente, s čimer sestavljajo samostojno računalniško vezje.

Fizične dimenzije vseh identifikacijskih kartic spadajo pod format ID-1, ki ga določa mednarodni standard ISO[2] 7810. Poleg plačilnih kartic uporabljajo ta format še kartice raznih programov zvestobe, poslovne vizitke ter celo kartična vozniška dovoljenja, ki se uporabljajo v nekaterih državah. Velikost formata ID-1 je 85,60 mm x 53,98 mm. Razmerja med različnimi dimenzijami kartic prikazuje slika 1. Standard ISO 7813 pa za plačilne kartice dodatno določa še debelino[3] ter polmer[4] zaobljenih robov kartice [14].



Slika 1: **Relativna primerjava velikosti formatov**

[2] International Organization for Standardization.
[3] 0,76 mm.
[4] 3,18 mm.

2.1 Današnji trendi zaščite

Zaradi problema varnosti plačevanja s plačilnimi karticami so glavna podjetja že leta 1994 začela oblikovati določila, ki bi zvišala raven varnosti. Posledica skupnih moči teh podjetij so specifikacije EMV,[5] ki obljubljajo drastično zmanjšanje možnosti goljufij. Te specifikacije se stalno dopolnjujejo, s čimer se odpravljajo ali zmanjšujejo možnosti pridobitve občutljivih podatkov [7].

Kot primarno metodo plačevanja določajo specifikacije EMV pametno kartico, ki bo v prihodnjih nekaj letih popolnoma zamenjala vse plačilne kartice, opremljene z magnetnim trakom. Posledično bo treba skladno s specifikacijami EMV prilagoditi tudi vse plačilne (POS[6]) terminale, da bodo lahko sprejeli katero koli pametno kartico EMV, ki jo bo izdal kateri koli izdajatelj. Za doseganje popolne združljivosti morajo vse kartice in vsi terminali prestati več ravni certificiranja, ki jih lahko v grobem razdelimo v štiri večje sklope:

- PCI PED,[7]
- 1. raven EMV,
- 2. raven EMV,
- izdajateljevo certificiranje.

Certificiranje PCI PED se osredinja na odkrivanje možnosti pridobitve zaupnih podatkov, ki se prenašajo med komponentami oz. hranijo v terminalu. Specifikacije določajo serijo specifičnih priporočil o dizajnu plačilnih terminalov. 1. raven certificiranja EMV se osredinja predvsem na strojno opremo, ki se uporablja za branje podatkov s kartice, medtem ko 2. raven certificiranja preveri delovanje programske opreme, ki je zadolžena za pravilno procesiranje podatkov, pridobljenih s kartice ter nadaljnjo komunikacijo z bankami in uporabnikom. Poleg tega morajo plačilni terminali prestati še certificiranje pri izdajateljih kartic. Izdajatelji namreč še dodatno preverijo, ali aplikacijska raven na terminalu nameščene programske opreme podpira specifičnosti njihovih kartic.

2.2 PCI PED

Specifikacije PCI PED so nastale z namenom zmanjšanja tveganja plačevanja s plačilnimi karticami na minimum. Specifikacije se osredinjajo predvsem na visoko raven zaščite uporabnikove številke PIN. Poleg tega specifikacije določajo raven zaščite podatkov

[5] Kratica EMV izhaja iz začetnic imen podjetij Europay, MasterCard in Visa.
[6] Point of Sale.
[7] Card Industry Pin Entry Device.

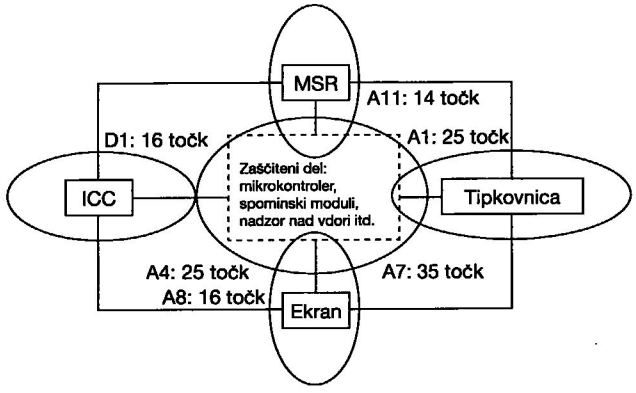
na magnetnem zapisu na kartici.[8] Večina današnjih napadov je namreč izvedena s kopiranjem podatkov magnetnega zapisa in pridobitvijo številke PIN z opazovanjem ali snemanjem uporabnika med vnosom številke PIN. Specifikacije poskrbijo tudi za zaščito zaupnih podatkov, med katere spadajo javni in zasebni ključi, posamezna gesla, načini vzdrževalnih postopkov itn. [13].

Za zaščito plačilnih terminalov specifikacije PCI PED določajo tri fizične načine zaščite, ki so izpeljani iz standarda ISO 13491-1:

- odpornost na vdor,
- razvidnost vdora,
- odkritje vdora in aktivno reagiranje nanj.

Odpornost na vdor predstavlja način, kako napadalcu otežimo njegovo delo. Pri tej ravni ne onemogočimo napadalca, temveč podaljšamo čas in povečamo trud, ki ga le-ta potrebuje za pridobitev uporabnih podatkov. Napadalec za uspešen preboj zaščite potrebuje tudi več znanja in razna specializirana orodja. Proizvajalci povečajo odpornost terminalov pred vdori z uporabo ključavnic, kovinskih preprek in unikatno oblikovanih glav vijakov. Učinkovit način zaščite na tej ravni je zalitje celotnega elektronskega vezja s homogeno trdno snovjo, ki je ni mogoče preprosto prerezati, odstraniti, prevrtati ali raztopiti, kljub temu pa mora ta prevajati oz. odvajati toploto, ki jo ustvari vezje med delovanjem. S pravilno namestitvijo zaščitnih elementov poskrbimo, da napadalec za pridobitev uporabnih podatkov pri vsakem terminalu porabi približno enako časa. Višja raven zaščite je raven razvidnosti vdorov. Ta poskrbi, da so v primeru vdora na zunanjem ohišju razvidne očitne poškodbe, ki jih lahko hitro opazita tako lastnik kartice kot prodajalec. Med načine zagotavljanja razvidnosti vdorov spadajo enosmerni vijaki, spojke za enkratno uporabo, ultrazvočno varjenje, močna lepila itn. Specifikacije 2.0 zahtevajo zaščitne mehanizme, ki aktivno odkrivajo vdore in nanje tudi aktivno reagirajo. Ob odkritju vdora je prvi korak kar brisanje vseh vrst v terminalu shranjenih ključev, kar povzroči, da terminal preneha delovati. Sprva se mogoče zdi, da je takšna logika prestroga, vendar edino tako lahko učinkovito dosežemo zaščito ključev. Na tej ravni zaščite uporabljamo razne senzorje za odkrivanje vdorov in pridružene mehanizme za brisanje podatkov. Senzorji nadzirajo okoljske in električne karakteristike, kot so napetost, pritisk, temperatura, sevanje, gibanje, prevodnost, hitrost urinega takta itn. [13]

Specifikacije PCI PED določajo skupek zahtev, ki jih lahko v grobem razdelimo v štiri skupine. Vsaka od teh skupin je razdeljena na več podskupin, ki vsaka posebej določajo posamezne vidike določenih delov oz. postopkov plačilnega terminala. Posamezne podskupine morajo za pridobitev certifikata na testiranju doseči določeno raven varnosti, ki je merljiva s postopki, ki jih bomo opisali v nadaljevanju. Slika 2 predstavlja najpomembnejše dele plačilnih terminalov, njihove ravni varnosti, potrebne za uspešno certifikacijo, in oznake podskupin, ki podrobneje določajo zahteve.



Slika 2: **Deli terminala, opremljeni z ravnmi varnosti**

S slike 2 je razvidno, da zahteve določajo največjo stopnjo varnosti za zaščiteni del terminala, v katerem so spravljeni vsi ključi in se izvajajo vse operacije, povezane z zaščito terminala. Visoka raven varnosti je potrebna tudi za zaščito tipkovnice terminala, kar seveda ni presenečenje, saj prek nje uporabnik vnese svojo skrivno številko PIN [16].

2.3 Izpolnjevanje zahtev

Fizična zahteva A1 v aktualnih specifikacijah kot osnovna raven zaščite zahteva aktivno odkrivanje vdorov, pri katerih je primarni namen odkritje uporabnikove številke PIN ter reagiranje na te vdore s takojšnjim avtomatiziranim brisanjem vseh skrivnih in občutljivih informacij, ki se nahajajo v terminalu. S tem postopkom postane plačilni terminal neuporaben za plačevanje, kar onemogoči napadalčeve namene. Napadalci poskušajo pridobiti uporabnikovo

[8] Do popolne uveljavitve pametnih kartic, ki ne bodo več vsebovale magnetnega zapisa na zadnji strani.

številko PIN predvsem s postavitvijo majhne naprave v bližino tipkovnice, ki bo prestregla vnos številke. Mehanizmi zaščite morajo tako odkrivati vdore v zunanje ohišje, npr. vrtanje, lasersko topljenje, kemijske reagente, odpiranje ohišja, vstope skozi ventilacijske odprtine itn. Fizična zahteva A4 določa ravnanje z občutljivimi podatki znotraj zaščitenega dela terminala. Ti podatki morajo biti zaščiteni z ravnjo varnosti 25 točk, kar velja tudi za vse funkcije, ki kakor koli operirajo s temi podatki. Ustrezna raven zaščite je tako lahko dosežena le ob strogi ločitvi strojno-programske opreme, ki se nahaja v zaščitenem delu, od ostalih ravni. S strogo ločitvijo teh dveh ravni lahko kasneje izboljšamo ter zamenjamo aplikacijsko raven brez potrebe po ponovnem certificiranju, saj nismo vplivali na samo strojno-programsko opremo. Najvišjo raven zaščite – 35 točk – določa fizična zahteva A7. V tem delu se poskuša z vsemi možnimi postopki pridobiti PIN oz. šifrirne ključe, uporabljene za njegovo šifriranje. A8 zahteva raven varnosti šestnajstih točk in se nanaša na terminale, pri katerih uporabnik prek tipkovnice poleg vnosa svoje številke PIN vnese tudi druge podatke. Namen specifikacije je preprečitev vnosa uporabnikove številke PIN v primeru, ko terminal ne deluje v zaščitenem načinu. Zahteva A11 se navezuje na združljivost s karticami, opremljenimi z magnetnim zapisom. Z ravnjo štirinajstih točk je namreč zaščitena magnetna bralna glava in prostor okrog nje, tako da ni mogoče dodajati, zamenjati ali modificirati delov bralnega sistema z namenom pridobitve podatkov iz magnetnega zapisa.

Logične zahteve so razdeljene v petnajst podskupin. Te zahteve določajo predvsem programsko logiko, ki se izvaja znotraj terminala. Programska oprema, ki je nameščena znotraj terminala, ne sme biti na kakršen koli način spremenjena, zato mora terminal vsaj vsakih 24 ur preveriti integriteto strojno-programske opreme. Največkrat uporabljeni metodi za preverjanje integritete sta preverjanje ciklične redundance – CRC – in rezultata zgoščevalne funkcije – SHA-1. Poleg preverjanja integritete vsakih 24 ur so priporočena tudi dodatna preverjanja, ki se lahko izvedejo pred vsako transakcijo. V primeru odkritja napake mora terminal preiti v nedelujoče stanje, tako da med tem prehodom ni nezaščitenih stanj. Če terminal podpira oddaljeno posodabljanje strojno-programske opreme, mora biti tudi na tem mestu izvedeno preverjanje integritete in v primeru, da je odkrita napaka pri preverjanju, se mora posodobitev zavreči brez vpliva na delovanje terminala. V realnem svetu[9] je mogoče opraviti le omejeno število transakcij na določeno časovno enoto. V primeru napada na plačilni terminal s fiksnim ključem za zaščito številke PIN bo napadalec poskušal izvesti čim več vnosov številke PIN naenkrat, saj bo s tem hitreje preizkusil vseh 10.000 kombinacij in tako hitro prišel do prave številke PIN. Tako mora biti v terminalu zgornja meja števila opravljenih transakcij nastavljena na 120 transakcij na uro, kar znese natančno dve transakciji vsako minuto [13].

Če pri tvorjenju ključev, preverjanju pristnosti itn. uporabljamo generator naključnih števil (RNG), je treba preveriti njegovo pravilno implementacijo. S tem ugotovimo, ali so števila res dovolj naključna. Preverjanje opravi neodvisni laboratorij, ki oceni izhod RNG-ja v velikosti 2^30 bitov podatkov. Dostop do občutljivih podatkov in funkcij mora biti minimalen, torej mora biti dostopov le toliko, kolikor jih je minimalno potrebno. Vsi tako dobljeni podatki se morajo takoj, ko jih ne uporabljamo več, zbrisati iz notranjih medpomnilnikov že med samo transakcijo, obenem pa se morajo ob koncu transakcije pobrisati tudi prav vse začasne lokacije hranjenja podatkov. Brisanje se mora izvesti tudi ob poteku časovnega obdobja, namenjenega za izvedbo transakcije, saj s tem dodatno zbrišemo podatke ob morebitnem napadu. Vsak dostop do občutljivih funkcij zahteva preverjanje pristnosti. Poleg preverjanja pristnosti mora terminal podpirati časovno omejitev nahajanja v občutljivem stanju, prav tako pa mora omejiti tudi največje število klicanih občutljivih funkcij. Upravljanje s ključi podrobneje določata ISO 11568 in ANSI[10] X9.24. Implementacijo tehnike šifriranja ključev določa ISO 9564. Posamezni ključi morajo biti uporabljeni le za natančno določen namen. Iz tega sledi, da enakega ključa ne smemo in ne moremo uporabiti za šifriranje števila PIN in drugih podatkov, temveč sta za to namenjena dva različna ključa. Vsi ključi morajo vedno biti varno spravljeni, poleg tega ne sme obstajati mehanizem, s katerim bi bilo mogoče na zaslonu prikazati vrednosti ključev. Pravzaprav v terminalu ne sme obstajati način, ki bi nešifriran ključ prenesel med strožje varovanim območjem v manj varovano območje [13].

Offline zahteve se nanašajo predvsem na bralnik pametnih kartic – ICC, saj pri offline transakcijah terminal pošlje plačilni kartici število PIN v preverjanje.

[9] Plačilo s plačilno kartico.
[10] American National Standards Institute.

Omenjeni bralnik mora biti zavarovan z ravnjo varnosti 16 točk. S tem dosežemo zaščito nad bralnikom, tako da je težko dodati oz. modificirati strojno ali celo programsko opremo bralnika z namenom pridobitve zaupnih podatkov. Bralnik mora biti takšen, da je vanj nemogoče vstaviti dve plačilni kartici. Druga, ki bi bila manjša, bi se namreč lahko namestila med pravo kartico in med kontakte bralnika, ki služijo za komunikacijo s kartico. Napadalec bi lahko tako prestregel vso komunikacijo in si pridobil zaupne podatke. Prav tako mora biti zaščiteno, da ni mogoče v notranji prostor namestiti žic tako, da jih uporabnik ne bi videl, ko bi bile te povezane na neki zunanji vmesnik. Po specifikacijah mora biti namreč bralnik na terminalu nameščen tako, da je celoten v vidnem polju uporabnika [13].

2.4 Računanje ravni zaščite

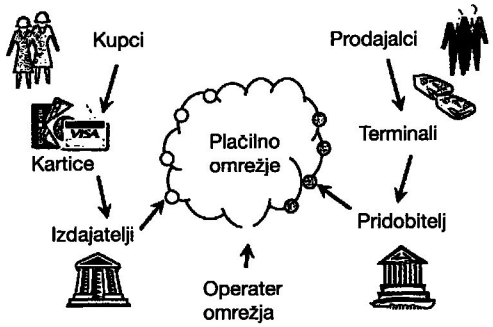
Računanje ravni zaščite poteka v dveh fazah. Prva predstavlja odkrivanje pomanjkljivosti in možnosti izkoriščanja le-teh. Če ocenjevalec odkrije več ranljivosti, se upošteva tista, ki prinese najmanjše število točk, kar v praksi predstavlja ranljivost, ki jo je najlaže izkoristiti za napad. Po koncu prve faze je navadno terminal uničen, saj se mora ocenjevalec do podrobnosti spoznati z delovanjem terminala in vsemi zaščitami. V realnem svetu bi prva faza predstavljala pridobitev terminala in izdelavo dodatnega vezja, ki bi prebral podatke z magnetnega zapisa kartice.

V drugi fazi imamo to prednost, da smo oboroženi z znanjem iz prve faze in imamo že narejeno taktiko izkoriščanja ranljivosti ter tudi morebitna dodatna vezja. Druga faza v realnem scenariju predstavlja pridobitev aktivnega terminala iz trgovine, namestitev vezja ter vrnitev v trgovino, ne da bi kdor koli izvedel, da je bil terminal kakor koli modificiran. V tej fazi po navadi potrebujemo veliko manj časa za izvedbo napada, prav tako je potrebno dosti manj znanja, saj oseba deluje po napotkih ocenjevalca/napadalca iz prve faze.

Skupna ocena ravni varnosti je seštevek vsot obeh faz in mora za uspešno certificiranje zadoščati minimalnim pogojem, določenim s specifikacijami PCI PED [15][16].

2.5 Udeleženci v plačilnih sistemih

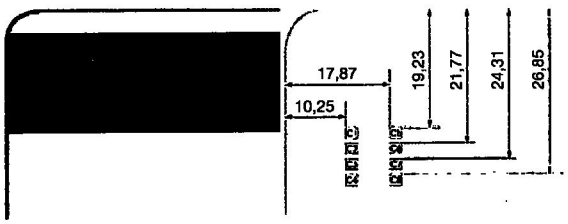
Temelj vseh plačilnih sistemov sestavlja pet udeležencev. Poleg kupcev in prodajalcev, brez katerih kartični plačilni sistemi ne bi obstajali, so za pravilno delovanje nujni še trije udeleženci. To so izdajatelji kartic, pridobitelji in ustrezno plačilno omrežje, kar prikazuje slika 3.



Slika 3: **Shema plačilnega omrežja**

Glavno gonilo prehajanja na tehnologijo pametnih kartic je zagotavljanje višje stopnje varnosti. Prednosti, ki jih prinaša čip proti magnetnemu traku, seveda niso zanemarljive. Čip precej teže kopirati, kar je pri magnetnem traku relativno preprosto, saj je na trgu mogoče dobiti opremo že za nekaj sto evrov. Druga pomembna izboljšava je možnost hranjenja večjega števila podatkov. Poleg tega imamo pri tehnologiji pametnih kartic možnost dodatka logike v kartico, saj veliko število pametnih kartic vsebuje tudi mikroprocesor. Ta mikroprocesor lahko uporabimo za tvorjenje dinamičnih podatkov, šifrirnih ključev in pri uporabi drugih povezanih algoritmov, predvsem v smislu varnosti,. Poleg teh mikroprocesor omogoča tudi izvajanje skript, s katerimi lahko spremenimo obnašanje kartic na daljavo.

Pametne kartice se od kartic z magnetnim trakom razlikujejo tudi fizično. Tako lahko pri karticah z magnetnim zapisom na zadnji strani opazimo 1,2 cm širok črn trak, ki sega prek vse dolžine kartice. Pri pametnih karticah ni tega traku,[11] namesto njega je na sprednji strani čip z osmimi kontakti [1], kar prikazuje slika 4.

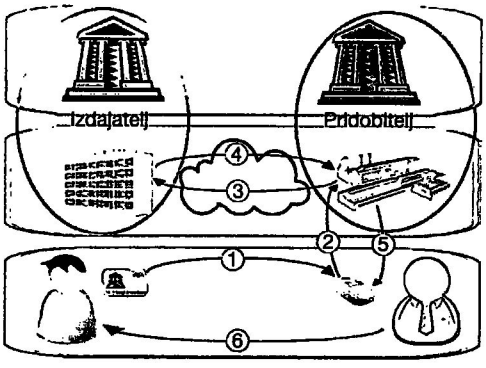


Slika 4: **Fizične razlike pri karticah (mere v mm)**

[11] V vmesnem obdobju sta pri karticah uporabljeni obe tehnologiji.

2.6 Postopek plačila

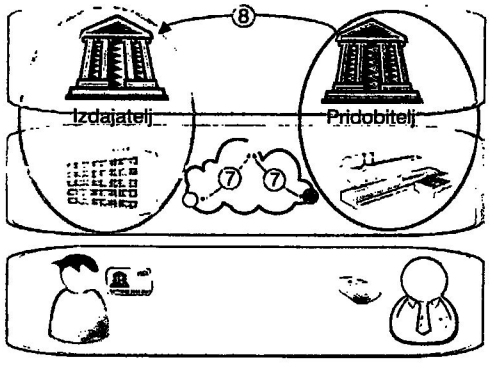
Kartice z magnetnim trakom počasi prehajajo v zgodovino, saj naj bi jih do leta 2011 povsem zamenjale pametne kartice [9]. Za lažje razumevanje prednosti pametne kartice si najprej oglejmo potek transakcije s kartico, ki vsebuje podatke, zapisane v magnetnem zapisu. Glavne korake prikazuje slika 5.



Slika 5: **Plačilo s kartico z magnetnim trakom**

Vso transakcijo smo zaradi večje preglednosti razdelili v tri logično povezane sloje. Spodnji je fizični sloj; v njem se opravi vse potrebno rokovanje s kartico. Drugi sloj predstavlja tehnično stran transakcije in se imenuje funkcionalni sloj. V njem se nahajata pridobitelj in izdajatelj kartic. Poleg njiju v tem sloju najdemo tudi plačilno omrežje. V tretjem sloju se nahajajo finančne ustanove, ki so v večini primerov banke, ki skrbijo za kritje stroškov transakcije.

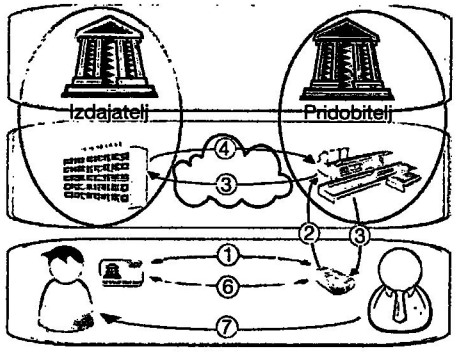
Plačilo z magnetno kartico lahko razdelimo v šest korakov, ki so označeni na sliki 5. V prvem koraku – ko prodajalec potegne plačilno kartico skozi bralnik, nameščen v plačilnem terminalu – dobi plačilni terminal podatke, zapisane na plačilni kartici. Po tem dogodku sledi še opcijski vnos osebne kode, poimenovane število PIN imetnika kartice. Ti podatki se potem pošljejo naprej pridobitelju, kar vidimo v drugem koraku. Zahtevo po avtorizaciji pridobitelj prek plačilnega omrežja posreduje izdajatelju – 3. korak. Izdajatelj preveri veljavnost kartice in ustreznost števila PIN ter primerja identifikacijsko številko kartice s seznamom, ki ga imenujemo črna lista. Na tej listi se nahajajo vse do sedaj odkrite ukradene oz. ponarejene kartice. Glede na rezultat omenjenih preverjanj izdajatelj pošlje pridobitelju pozitiven ali negativen odgovor. Pridobitelj nato ta odgovor pošlje proti terminalu. V primeru odobrenega plačila preda prodajalec blago kupcu – 6. korak, v nasprotnem primeru prodajalec ravna v skladu z napotki pridobitelja. Praviloma ob koncu dneva potekajo še drugi koraki, ki jih prikazuje slika 6.



Slika 6: **Izmenjava informacij ob koncu dneva – kartica z magnetnim zapisom**

Ob koncu dneva skrbnik plačilnega omrežja najprej pridobi podatke o vseh opravljenih transakcijah od pridobitelja in izdajatelja – 7. korak. Nato skladno s temi informacijami poskrbi za ustrezno izmenjavo denarja med sodelujočimi bankami.

Za lažjo primerjavo poteka transakcije pri pametni kartici s potekom transakcije pri kartici z magnetnim trakom smo za prikaz korakov plačila uporabili enako sliko kot prej. Ob pogledu na sliko 7 lahko ugotovimo, da pri plačilu s pametno kartico obstaja več korakov.

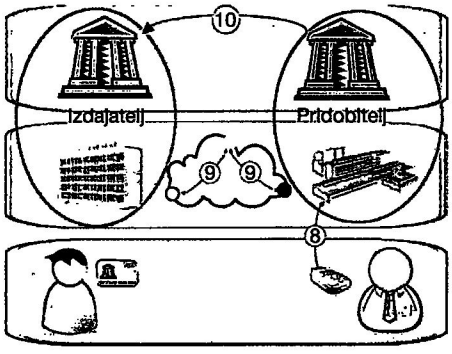


Slika 7: **Plačilo s pametno kartico**

Ob bolj podrobnem pogledu lahko opazimo, da komunikacija med pametno kartico in plačilnim terminalom poteka v obe smeri in celo dvakrat. To je storjeno v prvem in šestem koraku, ki predstavljata prvo in drugo polovico transakcijskega protokola EMV. Ostali koraki ostajajo podobni kot pri plačilu s kartico z magnetnim trakom. Tako ugotavljamo, da

pri transakciji EMV obstajata dve izmenjavi podatkov med plačilno kartico in terminalom, ki obakrat potekata v obe smeri. Ti izmenjavi bosta podrobneje opisani v nadaljevanju.

Tako kot pri kartici z magnetnim trakom tudi pri tehnologiji pametnih kartic pridobitelj in izdajatelj ob koncu dneva operaterju omrežja sporočita podatke o opravljenih transakcijah. Shemo prikazuje slika 8.

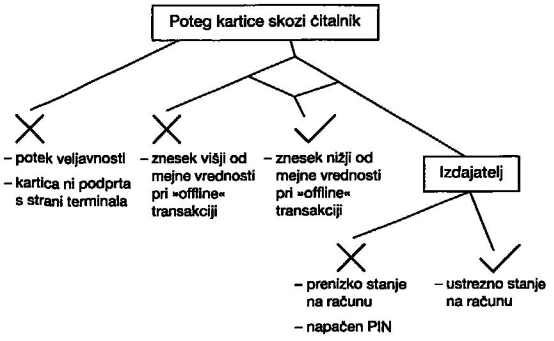


Slika 8: **Izmenjava informacij ob koncu dneva – pametna kartica**

Iz slike 8 hitro opazimo dodatno točko (8. korak), v kateri terminal ob koncu dneva pošlje dodatne podatke pridobitelju. Ti podatki se lahko glede na uporabljeni protokol pošljejo tudi ob koncu vsake transakcije. Podatki predstavljajo certifikat transakcije, ki ga mora pridobitelj hraniti 18 mesecev. V certifikatu transakcije so vsebovani vsi podatki o transakciji, kar preprečuje možnost zanikanja transakcije s strani kupca ali prodajalca. Certifikat torej predstavlja napredno potrdilo o opravljeni transakciji.

2.7 Transakcijski protokol

V primeru plačila s kartico z magnetnim trakom je odločitev glede sprejetja oz. zavrnitve transakcije preprosta. Ali bo transakcija potrjena, je odvisno od pogojev, ki jih prikazuje slika9.



Slika 9: **Odločitveno drevo kartice z magnetnim zapisom**

Po potegu kartice se najprej preveri, ali terminal podpira to vrsto plačilnih kartic. Če jo, terminal preveri še datum veljavnosti kartice. Če izmed pogojev ne ustreza, transakcije ni mogoče nadaljevati. Nato terminal preveri znesek. Če je ta pod določeno vrednostjo,[12] terminalu ni treba preveriti online, ali je kupec pravi in zmožen plačila, marveč se transakcija odobri samodejno. Če je znesek višji od mejne vrednosti in terminal nima možnosti preveriti plačilno zmožnost kupca online, se transakcija zavrne, v nasprotnem primeru pa terminal pošlje pridobitelju zahtevo po avtorizaciji plačila. Pridobitelj nato pošlje zahtevo naprej izdajatelju, ki najprej preveri ustreznost števila PIN. Če je PIN veljaven, izdajatelj primerja še višino sredstev na računu z višino zneska transakcije in skladno s tema preverbama pošlje odgovor.

Kot smo že omenili, obstaja pri transakcijah EMV med plačilno kartico in plačilnim terminalom več izmenjav podatkov. Te vedno potekajo v obe smeri. S tem se del odločitve odobritve prenese tudi na plačilno kartico. Korake transakcije EMV lahko razdelimo na 11 delov [3][4][5]:

- izbira aplikacije,
- branje podatkov s kartice,
- preverjanje pristnosti podatkov offline,
- omejitve procesiranja,
- verifikacija lastnika kartice,
- terminalovo upravljanje tveganja,
- analiza rezultatov postopkov – plačilni terminal,
- analiza rezultatov postopkov – plačilna kartica,
- procesiranje online,
- procesiranje skript izdajatelja,
- končanje transakcije.

Plačilna kartica vedno deluje v pasivnem načinu. To pomeni, da kartica v nobenem primeru ne ustvarja zahtev, temveč le podaja odgovore na zahteve, ki jih pošlje terminal. Na terminalski strani je treba pazljivo ravnati s pošiljanjem zahtev proti kartici, saj se mora terminal najprej prepričati, s kakšno kartico ima opravka, šele nato ji lahko začne pošiljati zahteve, toda le tiste, za katere se je terminal prepričal, da jih podpira kartica.

2.7.1 Izbor aplikacije

Po vstavitvi pametne kartice v čitalnik se najprej izvede izbor ustrezne aplikacije na pametni kartici.

[12] Mejna vrednost je v večini primerov okrog 20 evrov.

Terminal lahko to stori na dva načina. V prvem sprašuje kartico, ali podpira enake aplikacije, ki jih podpira sam. Ta način se imenuje način eksplicitne izbire. Če terminal podpira večje število aplikacij, postane tak postopek zamuden, zato EMV omogoča tudi drugi način, v katerem terminal prebere vse podprte aplikacije na kartici naenkrat in jih potem primerja z aplikacijami, ki jih podpira sam. Aplikacije, ki jih lahko uporabimo za plačilo, morajo biti navzoče tako na kartici kot na terminalu, zato predstavljajo presek obeh seznamov. Če se v preseku znajde več kot ena aplikacija, se za plačilo uporabi aplikacija z višjo prioriteto. Kadar v preseku ni nobene aplikacije, postane plačilo s to kartico v kombinaciji s tem terminalom nemogoče.

Aplikacije na plačilnih karticah predstavljajo posamezne možnosti plačila. Tako med aplikacije spadajo: Maestro (debetna), MasterCard (kreditna), bonusni programi itn.

2.7.2 Branje podatkov s kartice

V drugem koraku začne terminal s pametne kartice brati podatke, kar lahko primerjamo z branjem podatkov s kartice z magnetnim trakom. Razlika je predvsem v obsegu podatkov, ki znaša pri karticah z magnetnim trakom približno 130 zlogov, pri pametnih karticah pa okrog 2500 zlogov. Prebrani podatki so nato na voljo terminalu ali/in izdajatelju. Poleg osnovnih podatkov o kartici izvemo v tem koraku tudi, katere varnostne mehanizme podpira kartica. Te podatke dobi terminal v paketu AIP,[13] ki predstavlja profil aplikacije. Drugi pomemben dobljeni paket se imenuje AFL,[14] v katerem so zbrane lokacije posameznih podatkov na kartici. Te lokacije so vsebovane v skupinah s po štirimi zlogi, pri čemer lahko posamezna skupina vsebuje več zapisov podatkov.

2.7.3 Offline preverjanje pristnosti podatkov

Iz podatkov, prejetih v prejšnjem koraku, lahko terminal ugotovi, ali je vstavljena pametna kartica pristna. To ugotovi z uporabo šifriranja RSA[15], pri čemer morajo biti v terminalu na varnem mestu shranjeni izdajateljevi (Visa, MasterCard, JCB,[16] Amex idr.) javni ključi.[17] Velikost oz. dolžino ter datume poteka veljavnosti ključev določa organizacija EMVCo.

Za preverjanje podatkov imamo na voljo tri načine:

- statično preverjanje podatkov – SDA,
- dinamično preverjanje podatkov – DDA,
- kombinirano preverjanje podatkov – CDA.

SDA omogoča statično tvorjenje podpisa, s katerim podpišemo pristnost izmenjanih podatkov. Zaradi statično ustvarjenega podpisa je ta enak pri vsaki transakciji, opravljeni z določeno kartico. DDA in CDA na drugi strani dinamično tvorita podpis, saj pri računanju podpisa dodatno upoštevata naključno število, ki ga je ustvaril terminal. Zaradi tega je podpis pri vsaki transakciji drugačen.

2.7.4 Omejitve procesiranja

Iz prejetih podatkov terminal najprej preveri datumsko veljavnost kartice. Kartica je lahko neveljavna v dveh primerih: imetnik je kartico pravkar dobil, zato še ni bila aktivirana, ali – kar je bolj pogosto – je kartica presegla rok veljavnosti. Poleg preverjanja datuma terminal primerja še verzijo izbrane aplikacije na pametni kartici z verzijo, ki jo podpira sam. Nazadnje terminal preveri še zmožnost uporabe kartice v okolju terminala. Zadnje preverjanje onemogoči plačevanje v tujini karticam, ki so namenjene le za domačo rabo.

Rezultati vseh treh preverjanj se shranijo za kasnejše procesiranje znotraj terminala v podatkovnem elementu TVR.[18] Potreba po kasnejšem procesiranju izhaja iz tega, da terminalu korake 3–6 ni potrebno izvajati zaporedno, temveč jih lahko izvaja vzporedno v smislu krajših časov transakcije.

2.7.5 Verifikacija lastnika kartice

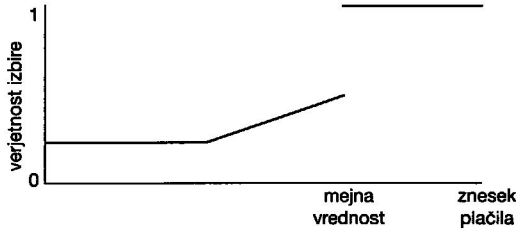
Specifikacije EMV omogočajo več vrst verifikacije lastnika kartice. Poleg podpisa obstaja še možnost preverjanja števila PIN, ki je mogoča na tri načine: online, offline in šifrirani offline. Uporaba posamezne metode je lahko odvisna od višine zneska ali od okolja, v katerem poteka plačilo. Specifikacije EMV imajo predvidene tudi druge metode verifikacije lastnika, kot je recimo identifikacija s pomočjo biometrije. Pri posamezni transakciji se lahko uporabi tudi več metod za preverjanje lastnika (npr. PIN in podpis).

[13] Application Interchange Profile.
[14] Application File Locator.
[15] Kratica izhaja iz začetnic priimkov avtorjev algoritma: Rivest, Shamir, Adleman.
[16] Japan Credit Bureau.
[17] Sistem PKI – infrastruktura javnih ključev.
[18] Terminal Verification Results.

Poleg višine zneska in okolja je metoda preverjanja odvisna tudi od možnosti plačilnega terminala[19] ter od odločitve plačilne kartice. Plačilna kartica vsebuje dva seznama kod, prek katerih določi svoje zahteve po preverjanju imetnika kartice.

2.7.6 Terminalovo upravljanje tveganja

V tej točki terminal preveri višino zneska plačila in jo primerja z mejno vrednostjo. Če višina zneska preseže mejno vrednost, ki jo določi izdajatelj, se zahteva po odobritvi transakcije pošlje izdajatelju. Terminal poleg višine zneska preveri še pogostost uporabe kartice. Visoka dejavnost kartice namreč takoj poraja sum o ukradeni kartici, zato lahko terminal določi, da se tudi takšna transakcija izvede online. Poleg obeh primerov vsiljenja transakcij online se v terminalu izvaja algoritem, ki naključno izbira transakcije, katere bodo – čeprav v prejšnjih dveh primerih ni potrebe po preverjanju online – vseeno poslane v preverjanje online kot dodaten ukrep. Primer algoritma za naključno izbiranje transakcij glede na znesek plačila prikazuje slika 10.



Slika 10: **Primer algoritma**

2.7.7 Analiza rezultatov postopkov – terminal

V sedmem koraku terminal ovrednoti rezultate korakov 3, 4, 5 in 6 in poda svojo končno odločitev glede nadaljnjega procesiranja transakcije. Odločitev temelji na primerjanju rezultatov zgornjih operacij, s kodami, shranjenimi v terminalu. Obstajajo tri možnosti odločitve:

- zavrnitev transakcije,
- nadaljevanje s transakcijo online,
- nadaljevanje s transakcijo offline.

Ob koncu sedmega koraka terminal svojo odločitev sporoči plačilni kartici.

2.7.8 Analiza rezultatov postopkov – kartica

Plačilna kartica najprej prejme odločitev plačilnega terminala o nadaljnjem poteku transakcije. Glede na odločitev terminala lahko kartica določi le še bolj strogo omejitev, saj ne more odobriti transakcije, če je terminal ni odobril (ker je ugotovil določene nepravilnosti). Tako lahko kartica v primeru, da je terminal odobril transakcijo offline, zahteva izvedbo transakcije online oz. ne odobri transakcije; v primeru, ko je terminal odobril transakcijo online pa zahteva onemogočitev nadaljnjega izvajanja transakcije. Te primere prikazuje slika 11.

KARTICA

TERMINAL	Zavrni	Pojdi online	Dovoli offline
Zavrni	✔	N/A	N/A
Pojdi online	✔	✔	N/A
Dovoli offline	✔	✔	✔

Slika 11: **Odločitev plačilne kartice (glede na terminal)**

Strožje ukrepe uporabi kartica glede na logiko, ki jo vsebuje. Tako ima lahko vsaka kartica pravilo, da v primeru prve transakcije izvede preverjanje online.

2.7.9 Procesiranje online

Pri transakciji online se izvedeta še koraka 9 in 10, ki se pri transakciji offline ne izvedeta. Pri korakih 9 in 10 izdajatelj prejme še številko računa, višino zneska transakcije in šifrirano število PIN. Na podlagi teh podatkov nato izdajatelj odobri ali zavrne transakcijo. Pomembna značilnost procesiranja online je obojestransko preverjanje pristnosti. S tem se plačilna kartica prepriča, da je na drugem koncu pravi izdajatelj, izdajatelj pa, da je na drugi strani njegova kartica. Preverjanje pristnosti temelji na trojnem DES[20] (TDES) šifriranju.

2.7.10 Procesiranje skript izdajatelja

Pri vsaki transakciji online lahko izdajatelj dodatno pošlje del programske kode, imenovane skripta. Ta poskrbi za vnos nove logike oz. parametrov v kartico. S skriptami lahko izdajatelj spremeni več stvari. Med glavne spremembe spadajo spreminjanje števila PIN, blokiranje kartice, sprostitev blokiranih aplikacij, spreminjanje mejne vrednosti kartice itn. Skripte se lahko pošljejo pred odobritvijo transakcije ali po njej. Zaradi varnosti so skripte podpisane s kodo in opcijsko še dodatno zaščitene s šifriranjem TDES[21] [2].

[19] Podpis se ne more uporabiti, če plačilni terminal nima tiskalnika.

[20] Data Encryption Standard.

[21] V primeru menjave številke PIN je šifriranje skripte obvezno.

2.7.11 Konec transakcije

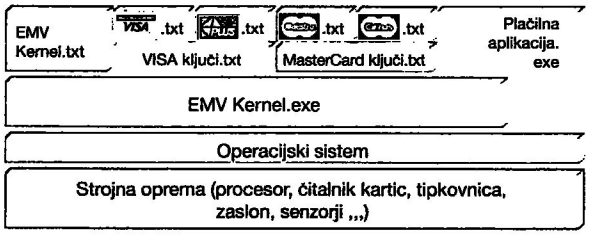
Ob koncu transakcije se v terminalu shrani elektronsko potrdilo o opravljeni transakciji. Poleg tega se na terminalovem zaslonu izpiše rezultat transakcije in natisne potrdilo za imetnika kartice.

2.8 Izdajateljevo certificiranje

Specifikacije EMV so pravzaprav specifikacije, ki določajo vse vidike terminala; iz njih lahko implicitno dobimo tudi specifikacije, ki določajo vidike pametne kartice. V teoriji to sicer drži, vendar se je žal v praksi pokazalo, da si različni ljudje in organizacije enake specifikacije različno razlagajo. Tako so izdajatelji razvili vsak svoje funkcionalne specifikacije, ki določajo delovanje njihovih pametnih kartic:

- VISA: VIS 1.4.0,
- MasterCard: M/Chip 4,
- JCB:[22] J/Smart 1.2.

Posledica tega je dodatno certificiranje, katerega opravi izdajatelj, da se prepriča, ali terminal ustreza njegovim pametnim karticam. Slika 12 predstavlja arhitekturo plačilnega terminala, iz katere so razvidni vsi cilji certificiranj [4].



Slika 12: **Arhitektura plačilnega terminala**

Certificiranje strojne opreme določa predvsem certificiranje PCI PED in seveda 1. raven EMV. EMV Kernel.exe in EMV Kernel.txt sta certificirana prek 2. ravni EMV. S popolno ločitvijo plačilne aplikacije od EMV Kernela imamo možnost spreminjati npr. izpise, račune itn. brez zahteve po ponovnem certificiranju, saj sprememba same aplikacija nima vpliva na EMV Kernel [4].

Certificiranje pri izdajatelju poteka z namestitvijo izdajateljevih ključev in parametrov v terminal ter testiranjem komunikacije med terminalom in vsemi udeleženci pri transakciji. MasterCard in VISA imata za ta postopek na voljo testna orodja in testne skripte:

- MasterCard: TIP[23] – testiranje s testnim orodjem ETEC,[24]
- VISA: testiranje z ADVT.[25]

Šele ko terminal prestane vsa testiranja, ga je mogoče uporabljati tudi za prave transakcije. Žal pa je ta postopek zelo dolgotrajen, saj je težko prestati teste vseh izdajateljev, poleg tega pa imajo pridobitelji po navadi pred lansiranjem terminalov na trg še svoje specifične zahteve, zato je izvedba univerzalnega plačilnega terminala, ki bi omogočal plačevanje z vsemi karticami, izredno težavna.

3 MOBILNI TELEFONI

Zanimiva alternativa uporabi plačilnih kartic je ideja plačevanja z mobilnim telefonom. Proizvajalci mobilnih telefonov poskušajo pri razvoju novih modelov ustreči čim večjemu številu uporabnikov, zato v svoje produkte vgrajujejo funkcionalnosti drugih naprav, kot so digitalni fotoaparati, radii, dlančniki, glasbeni ter video predvajalniki in celo navigacijske naprave. Zakaj torej ne bi prevzeli tudi vloge plačilnega sredstva, če jih imamo vedno pri sebi?

S tem vprašanjem se je spoprijelo že več podjetij, zato je nastalo več sistemov, ki so omogočali razne oblike plačevanja z mobilnim telefonom. Med najbolj pogoste uvrščamo: plačevanje prek kratkih sporočil – SMS, USSD,[26] prek brezžične komunikacije (NFC,-[27] RFID[28]), prek obiska določene strani, locirane na medmrežju (GPRS,[29] UMTS[30]), prek klica IVR[31] idr. Vsaka od teh oblik je imela kakšno pomanjkljivost, predvsem v podpori vseh obstoječih telefonov,[32] in/ali pa je bila njihova uporaba zapletena.

Za razliko od vseh teh tehnologij si je podjetje Margento R&D, d. o. o., zadalo nalogo izvesti novo tehnologijo, ki bi bila preprosta za uporabo in bi podpirala prav vse mobilne telefone na trgu. Novi sistem za plačevanje, imenovan sistem Margento, tako temelji na osnovni funkcionalnosti, ki jo podpirajo prav vsi telefoni, to je prenos zvoka po govornem kanalu različnih omrežij, zato bomo v nadaljevanju opisali

[22] JCB se pridruži EMVCo konec leta 2004.

[23] Terminal Integration Process.
[24] Easy Test Cards.
[25] Acquirer Device Validation Toolkit.
[26] Unstructured Supplementary Service Data.
[27] Near Field Communication.
[28] Radio Frequency Identification.
[29] General Packet Radio Service.
[30] Universal Mobile Telecommunications System.
[31] Interactive Voice Response.
[32] NFC ne moremo uporabiti, če telefon ne vsebuje čipa NFC.

vrste zaščitnih elementov, ki so bili implementirani pri sistemu Margento.

Za prenos podatkov in identifikacijo uporabnika ter plačilnega mesta, sistem uporablja uporabnikov mobilni telefon. Sistem deluje podobno kot sistemi, pri katerih se kupec predstavi s svojo plačilno ali bančno kartico. Razlika nastane v identifikaciji in v prenosu podatkov, saj se oseba predstavi terminalu s svojim mobilnim telefonom, drugi podatki transakcije pa se delno ali popolno prenašajo po govornem kanalu mobilnega telefona osebe, ki opravlja transakcijo [17].

Ob tem se nam poraja vprašanje varnosti takšnega početja oz. primerjava z ravnjo zaščite pri plačilnih karticah, ki jim v splošnem ljudje kar dobro zaupamo. Prenos podatkov namreč ne poteka le po fizičnih linijah in ustaljenih protokolih, temveč ta poteka tudi prek prenosa zvoka med terminalom in mobilnim telefonom uporabnika [18]. Ta del prenosa lahko uporabnik oz. napadalec sliši in preprosto posname ter kasneje analizira. Zaradi tega je bilo treba poskrbeti za varnost na več ravneh z uporabo najnaprednejših šifrirnih algoritmov, postopkov in procedur.

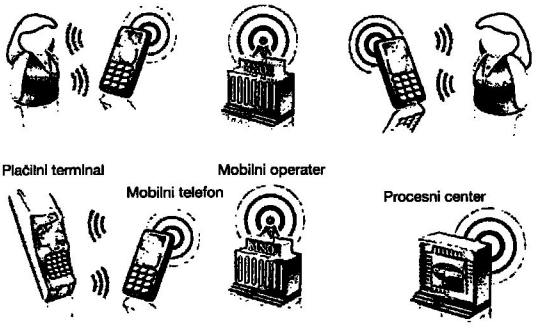
3.1 Identifikacija uporabnika in plačilnega mesta

Sistem Margento pridobi identiteto uporabnika prek telefonske številke njegovega mobilnega telefona. To številko določa kartica SIM,[33] ki je nameščena znotraj uporabnikovega mobilnega telefona. Vsako kartico SIM je treba pred prvo uporabo prijaviti v mobilno omrežje ponudnika mobilnih storitev, drugače je ne moremo uporabljati. Dobra stran tega ukrepa je, da mobilni ponudniki ne dovoljujejo obstoja dveh kartic SIM z enako številko, kar takoj zagotovi unikatno identiteto uporabnika. Če se ozremo na primerjavo s plačilnimi karticami, ki so opremljene z magnetnim zapisom, takoj uvidimo, da tam ni tako, saj je znanih veliko primerov, ko so nepridipravi kopirali kartice, si naredili dvojnike in jih nato uporabljali, s čimer so oškodovali lastnika kartice. Poleg tega da v mobilnih omrežjih ni mogoče uporabljati dveh enakih kartic SIM, je te tudi zelo težko kopirati, saj sama kartica SIM vsebuje določeno logiko, zaradi katere jo lahko uvrščamo med samostojne zaščitne elemente. Podobno kot kartice SIM je težko kopirati tudi pametne kartice, ki jih zahtevajo specifikacije EMV.

Pri identifikaciji uporabnika smo v sistemu Margento uvedli, podobno kot je to storjeno pri plačilnih karticah, vnos osebne identifikacijske številke PIN. Glede na delovanje pametnih kartic, kjer se vnos številke PIN pri nizkih zneskih po navadi preveri s številom zapisanim znotraj pametne kartice,[34] smo se pri sistemu Margento odločili za izboljšano rešitev. Veliko prednost sistema namreč predstavlja preverjanje vseh transakcij online. Vneseno število PIN se tako takoj po vnosu zašifrira in pošlje skupaj z drugimi transakcijskimi podatki po zaščiteni povezavi do procesnega centra,[35] kjer se število PIN primerja s shranjenim številom določenega uporabnika.

Med opravljanjem plačila se uporabnikova identiteta nikoli ne razkrije ne terminalu ne prodajalcu, saj je znana le procesnemu centru. Tako uspešno ločimo število PIN in uporabnikovo identiteto,[36] kar nam zagotovi višjo stopnjo varnosti.

Plačilo prek mobilnega telefona v sistemu Margento, poteka enako kot opravljanje preprostega telefonskega klica, pri čemer zamenjamo določene elemente klica. Vlogo govorca tako prevzame plačilni terminal, medtem ko vlogo sogovornika in njegovega mobilnega telefona prevzame procesni center, kar prikazuje slika 13. Uporabnik pokliče številko procesnega centra, s čimer procesni center dobi uporabnikovo identifikacijsko (MSISDN) številko.



Slika 13: **Primerjava plačila s telefonskim klicem**

V tem trenutku procesni center ve, kdo hoče plačati določeno storitev, ne ve pa še, kaj, koliko in kje želi to opraviti. Ti podatki se prenesejo po vzpostavitvi zaščitene seje med terminalom in procesnim centrom. Pri tem je treba omeniti, da je identifikacija

[33] Subscriber Identity Module.

[34] Glej razdelek 2.7.5.

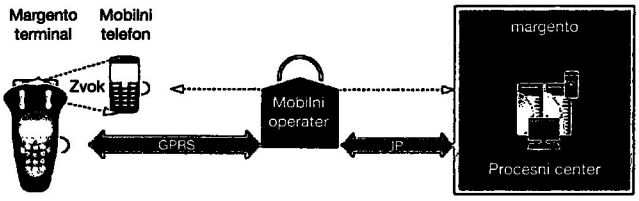
[35] V nekaterih primerih se podatki pošljejo naprej do bančnih ustanov.

[36] Uporabnikovi podatki, številka računa itd.

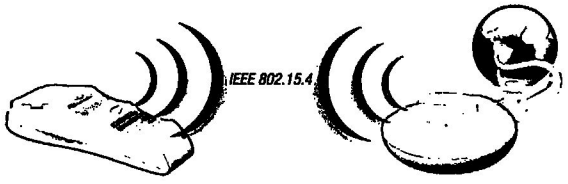
plačilnega mesta samodejna, saj terminal med potekom izmenjave informacij samodejno pošlje svojo identifikacijsko številko. To je velika prednost, saj se s tem izognemo možnosti človeške napake, pri čemer bi se lahko zgodilo, da bi uporabnik sporočil napačno številko prodajnega mesta, kar predstavlja velik problem pri plačevanju prek SMS, saj se uporabniki velikokrat zatipkajo.

3.2 Zaščitena povezava

Za vzpostavitev povezave, prek katere se prenesejo transakcijski podatki, so lahko uporabljeni različni komunikacijski kanali. Prenos podatkov se lahko nadaljuje prek govornega kanala omrežja GSM, lahko pa se po identifikaciji uporabnika in plačilnega mesta klic prekine, za prenos transakcijskih podatkov pa terminal vzpostavi GPRS [19] (slika 14) ali povezavo ZigBee/IP [20][21], kar prikazuje slika 15.

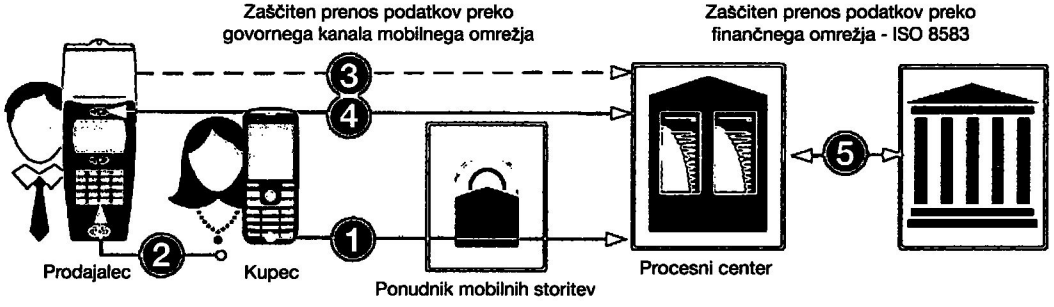


Slika 14: **Navzočnost dveh komunikacijskih kanalov**



Slika 15: **Povezava IP kot drugi komunikacijski kanal**

Po vzpostavitvi povezave med plačilnim terminalom in procesnim centrom se začne postopek vzpostavitve zaščitene povezave. Ta faza je sestavljena iz določitve in izmenjave šifrirnih ključev ter obojestranskega preverjanja pristnosti udeležencev.



Slika 16: **Prikaz plačila**

Sistem Margento za upravljanje s ključi uporablja sistem PKI, ki temelji na eliptičnih krivuljah – ECC oz. na postopkih asimetričnega šifriranja. Asimetrično šifriranje uporabljamo tudi za obojestransko preverjanje pristnosti. Na ta način terminal preveri procesni center in na drugi strani procesni center preveri terminal.

S tem se izognemo možnosti, da bi nepridipravi poskušali opraviti transakcijo z lažnim terminalom oz. lažnim centrom. Uporaba ECC je bila izbrana zaradi več razlogov. V primerjavi z bolj znanim RSA, ki je uporabljen pri plačilnih karticah, nam ECC zagotavlja enako stopnjo zaščite pri dosti krajših ključih, kar nam omogoča hitrejše prenose, manjšo porabo procesorske moči in pasovne širine. Za lažjo primerjavo nam tabela 1[37] predstavlja dolžine ključev ECC in dolžine njihov alternativ –ključev RSA ter stopnjo varnosti, ki jo določa čas, potreben za ugotovitev ključa. Ta čas je podan kot čas, ki bi ga potreboval računalnik, ki lahko izvede en milijon inštrukcij na sekundo.

Tabela 1: **Primerjava zaščite ECC proti RSA**

Velikost ključa ECC	Velikost ključa RSA	Razbitje zaščite (v MIPS letih)
113	512+	10^5
131	768	10^8
163	1024	10^{12}
233	2048+	$>10^{22}$

Po določitvi šifrirnih ključev, ki so drugačni za vsako transakcijo, se ti ključi uporabijo za šifriranje transakcijskih podatkov, pri čemer je uporabljeno

[37] Rezultati so povzeti na podlagi ocen iz članka [22].

simetrično šifriranje. Glede na želje bank in drugih ustanov na posameznem območju smo podprli več različnih šifriranj, med katerimi sta najbolj znana DES ter trojni DES – 3DES.

Uporabniki pogosto želijo, da se za plačilo uporabi kar denar, ki se nahaja na njihovih bančnih računih. Zaradi tega smo morali dodati možnost povezave do finančnih ustanov, v katerih imajo uporabniki svoje račune, kar prikazuje slika 16. Te povezave temeljijo na specifikacijah ISO 8583. Za zaščito prenosa podatkov med procesnim centrom in finančnimi ustanovami, smo poleg zgoraj omenjenih zaščit uporabili standardne pristope:

- SSL – protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem,
- VPN – navidezno zasebno omrežje.

3.3 Mobilno plačevanje

Prednosti sistema Margento so vsekakor v zagotavljanju visoke ravni varnosti. Tu pride do izraza predvsem izvajanje vseh transakcij in preverjanje pristnosti online v realnem času. S tem imamo na voljo centraliziran sistem, ki ga upravljamo prek procesnega centra. Tu imamo dodatno implementirane črne in bele liste, prek katerih preverimo vsako zahtevo po plačilu. V slučaju ukradenega telefona se ta takoj doda na črno listo, kar onemogoči kakršno koli plačevanje z njim. V procesni center smo vgradili tudi logiko, ki odkriva značilnosti, ki lahko namigujejo na razne možne kršitve in nelegalno početje, kot so:

- več zaporednih neuspešnih vzpostavitev zaščitene seje na istem terminalu,
- neveljavni digitalni podpis,
- več neuspešnih poskusov transakcij istega uporabnika,
- prekomerna uporaba določenega terminala.

Ob odkritju takšnega početja se sproži alarm, pri čemer se preverita aktivnost in uporaba in glede na odkritje se nato ukrepa. Za lažjo sledljivost in preverjanje plačil se še dodatno hranijo:

- zapisi o opravljenih klicih pri ponudniku mobilnih storitev,
- informacije o vsaki transakcijski zahtevi in odgovoru ter poteku, ki se hranijo na procesnem centru,
- zapisi pri finančnih ustanovah,
- natisnjena potrdila o opravljenih plačilih pri prodajalcu,
- potrdila o opravljenih plačilih, ki so zapisana znotraj vsakega terminala.

4 SKLEP

Kartična industrija je z zavedanjem o pomanjkljivosti kartic, opremljenih z magnetnim trakom, naredila velik in pravočasen korak že v devetdesetih letih prejšnjega stoletja. Z nadaljevanjem njihovega prizadevanja in intenzivnim delom se nam vsem obeta popoln prehod na tehnologijo pametnih kartic do leta 2011.

Ali to pomeni konec vseh goljufij in mogočih nepravilnosti? Žal ne, vendar bo verjetnost, da pride do goljufije, občutna manjša. Specifikacije EMV namreč so že od prvih verzij usmerjene k temu, da se nepridipravom ne bi splačalo izrabiti sistema, tudi če bi jim to uspelo. Za izkoriščanje katere koli varnostne luknje certificiranega terminala naj bi po predvidevanjih imeli za najmanj 25.000 dolarjev stroškov, česar si nikakor ne bi mogli pokriti z informacijami, dobljenimi prek te varnostne luknje [7]. Torej se nepridipravom ne splača niti poskusiti z napadom, saj bodo tudi v primeru, da jim uspe, v izgubi ter seveda v prekršku.

Tehnologija EMV nam torej obljublja dosti manj goljufij. Verjetno pa zaradi nje nepridipravi ne bodo nehali delovati, marveč se bodo preusmerili na področja, ki še ne uporabljajo oz. nočejo uporabljati tehnologije EMV. S tem se bodo vse goljufije začele pojavljati na manjšem območju, kar bo povzročilo, da bodo izdajatelji in lokalni pridobitelji kljub svojemu začetnemu negodovanju nad tehnologijo EMV začeli prehajati na EMV. Zato je predvideno, da se bo slej ko prej tehnologija EMV začela uporabljati po vsem svetu. Ali se bo to res zgodilo ali pa bo kdo izdal kakšne svoje specifikacije, bo pokazal šele čas.

Plačevanje z mobilnimi telefoni vsekakor predstavlja zanimivo alternativo plačilu s karticami. Mobilne telefone imamo namreč vedno s seboj in jih uporabljamo za različne namene, medtem ko plačilne kartice nosimo s seboj predvsem za plačevanje storitev. Če bi torej za plačila storitev in dvige gotovine lahko vedno uporabljali mobilni telefon, bi odpadla potreba po dodatnih plačilnih instrumentih, kot so plačilne, bonusne, kreditne in predplačniške kartice.

Glavni namen uporabe mobilnih telefonov seveda ni bil plačevanje storitev na tak način, zato se je bilo treba pri razvoju spopasti s številnimi problemi. Od dejstva, da govorni kanal ni prilagojen prenosu podatkov, do dejstva, da je bilo potrebno zaradi opravka z denarjem in nezaupljivostjo finančnih ustanov, implementirati visoke ravni zaščite.

5 LITERATURA*

[1] EMV Integrated Circuit Card Specifications for Payment Systems – Book 1: Application Independent ICC to Terminal Interface Requirements, verzija 4.1, maj 2004, 201 strani.

[2] EMV Integrated Circuit Card Specifications for Payment Systems – Book 2: Security and Key Management, verzija 4.1, maj 2004, 187 strani.

[3] EMV Integrated Circuit Card Specifications for Payment Systems – Book 3: Application Specification, verzija 4.1, maj 2004, 237 strani.

[4] EMV Integrated Circuit Card Specifications for Payment Systems – Book 4: Cardholder, Attendant, and Acquirer Interface Requirements, verzija 4.1, maj 2004, 161 strani.

[5] EMV Integrated Circuit Card Specifications for Payment Systems: Common Payment Application Specification, verzija 1.0, december 2005, 770 strani.

[6] http://www.europeanpaymentscouncil.eu/.

[7] http://www.emvco.com/.

[8] http://www.corporate.visa.com/av/about_visa/corp_history.jsp.

[9] http://www.europeanpaymentscouncil.org/documents/Roadmap%20public%20version%204th%20April.pdf.

[10] http://en.wikipedia.org/wiki/Credit_card.

[11] http://www.creditcards.com/history-of-credit-cards.php.

[12] http://money.howstuffworks.com/credit-card.htm.

[13] https://www.pcisecuritystandards.org/.

[14] http://en.wikipedia.org/wiki/ISO_7810.

[15] PED Program Guide v1-0, december 2007.

[16] PCI POS PED Security Requirements v2.0, julij 2007.

[17] www.margento.com.

[18] Z. Mezgec, M. Pec, R. Svečko, A. Chowdhury, Prenos podatkov po govornem kanalu GSM sistema, ERK 2005.

[19] F. Horvat, D. Slavinec, Z. Mezgec, A. Chowdhury, Nadgradnja osnovne M-Pay komunikacije, ERK 2007.

[20] A. Zelenik, A. Medved, Z. Mezgec, A. Chowdhury, Izbor brezžične podatkovne komunikacije za mobilni transakcijski terminal, ERK 2007.

[21] A. Zelenik, A. Koštomaj, Z. Mezgec, A. Chowdhury, Postopki oddaljenega posodabljanja mobilnih plačilnih terminalov, ERK 2008.

[22] A. Odlyzko: "The Future of Integer Factorization", Cryptobytes Vol. 1(2), 1995.

■

Aleš Zelenik je leta 2007 diplomiral na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru na smeri telekomunikacije z diplomsko nalogo Oddaljeno brezžično varovanje prenosa vrednostnih predmetov. Svoje izobraževanje nadaljuje na enovitem doktorskem študiju elektrotehnike. Teoretične izkušnje, pridobljene med študijem, preliva v prakso pri delu v razvojnem centru podjetja Margento R&D. V teku svojega dela je razvil več sistemov za brezžični prenos podatkov med napravami, temelječih na standardu IEEE 802.15.4. Njegovo delo je med drugim obsegalo tudi implementacijo več orodij za podporo in programiranje mikroprocesorjev TI DSP, vpeljavo postopkov za obdelavo signalov, definiranje novih prenosnih protokolov med napravami itn. Njegova predvidena doktorska disertacija bo obsegala nove postopke pri odkrivanju in razpoznavanju čustev v govoru.

■

Zdenko Mezgec ima več kot osem let izkušenj v razvojnoraziskovalnem delu na področju naprednih regulacijskih sistemov in komunikacij ter komunikacijskih sistemov. Leta 2004 je diplomiral na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru z diplomsko nalogo Optimizacija prenosa podatkov po govornem kanalu GSM. Leta 2009 je na isti fakulteti doktoriral z disertacijo Indirektne segmentacijske metode za adaptivno robustno kontrolo prenosa podatkov po govornem kanalu GSM.

* Viri povezav temeljijo na datumu 1. 3. 2009.