Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Bakalářská práce

2013 **Roman Valenta**

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta
Ústav aplikované informatiky

Bezpečnost platebních karet

Bakalářská práce

Roman Valenta

Školitel: Jan Doubek, MBA
Československá obchodní banka, a.s.

Garant: RNDr. Libor Dostálek

České Budějovice 2013

Bibliografické údaje

Valenta, R., 2013: Bezpečnost platebních karet. [Payment cards security. Bc. Thesis, in Czech.] – 60 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Abstrakt

Tato bakalářská práce se zabývá platebními kartami se zaměřením na jejich bezpečnost. V práci jsou rozděleny platební karty a popsány technologie, které zaručují jejich bezpečné používání. Je provedena analýza rizik a zranitelností, vysvětlující útoky na platební karty. Na základě provedené analýzy jsou navržena opatření, která zajistí obranu proti zneužití platební karty.

Abstract

This bachelor thesis deals with payment cards security. Different kinds of payment cards and technologies which make their usage secure are described in the work. There is an analysis of risks and vulnerabilities performed in the thesis explaining attacks on payment cards. Analysis-based measures that guarantee protection against of payment cards fraud are proposed.

Klíčová slova

platební karty, bezpečnost, zranitelnosti, zneužití, obrana

Key words

payment cards, security, vulnerabilities, fraud, protection

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátu.

V Českých Budějovicích, dne 26. 4. 2013.

Podpis: ……

Poděkování

Na tomto místě bych rád poděkoval panu Janu Doubkovi, MBA za poskytnutí literatury, cenných rad a připomínek, které přispěly k vypracování bakalářské práce. Dále bych rád poděkoval své rodině za její podporu při zpracovávání práce.

Obsah

1 Úvod

Platební karty, jakožto prostředek pro bezhotovostní platební styk, ovlivňují životy velké spousty lidí. Oblíbenost při jejich používání roste každým rokem již od dob jejich vzniku. Platební karty nám tak zjednodušují nakupování a v mnohých případech jsou i bezpečnější, než použití standardní hotovosti. Na druhou stranu jsou s nimi spojené značné sumy peněz, které častokrát převyšují hotovost v obsahu peněženky, a proto se tato práce zaměřuje především na zabezpečení platebních karet. Útoky na platební karty existovaly již od dob jejich prvopočátků, a tak celá problematika musela v rámci ochrany kapitálu klientů projít značným vývojem, přičemž vývoj bezpečnostních prvků se stále rozvíjí a do budoucna i rozvíjet bude. Vždy se totiž najde někdo, kdo i ty nejmodernější zábrany dříve nebo později pokoří a vystaví tím držitele karty do určitého rizika spojeného s použitím platební karty.

V práci budou představeny platební karty, jejich vývoj a rozdělení dle různých kritérií. Bude uveden způsob komunikace čipové karty se zařízením, jež ji přijímá na základě standardu EMV, který je v současnosti rozšířen nejvíce. Dále budou vysvětleny jednotlivé druhy použití platebních karet a popsány zabezpečovací prvky, které mají za úkol platbu kartou ochránit.

Cílem práce je představit platební karty, se zaměřením na současné řešení jejich zabezpečení. To zahrnuje popis bezpečnostních mechanizmů využívaných k ochraně prováděných transakcí a vytvoření analýzy rizik a zranitelností spojených s jejich používáním. V rámci systémové analýzy tak budou představeny a vysvětleny charakteristiky jednotlivých druhů známých i méně známých útoků, kterými lze zneužít platební kartu, a jejímu držiteli tím tak způsobit škodu. Dále budou navržena opatření, jakými by se měl držitel karty řídit a případné způsoby, kterými lze úroveň zabezpečení zvýšit tak, aby zneužití platební karty v nejlepším případě zabránil nebo alespoň snížil riziko provedení útoku. Na závěr práce budou navrženy technologie, které by zjištěné nedostatky, nebo alespoň jejich část, eliminovaly a tím by zneužití platebních karet zabránily a celkovou úroveň zabezpečení tak zlepšily.

2 Vznik platebních karet

Platební karty, ač se to nezdá, nejsou v platebním světě žádnou novinkou. Předchůdci těch současných je již téměř 150 let. Za první platební karty lze považovat karty z tvrdého papíru, které svým nejlepším zákazníkům nabízely některé americké telegrafní a dopravní společnosti a to již roku 1868. Zákazník nemusel disponovat hotovostí, stačilo, když podepsal stvrzenku a faktura mu byla následně zaslána poštou. Protože se 19. století neslo v duchu nových vynálezů, čerpala spousta domácností úvěry od obchodníků. Ti proto zákazníkům poskytovali úvěrové známky z papíru o určité peněžní hodnotě, které při použití proděravěli kleštěmi.

Za předchůdce karet, podobné těm dnešním, lze považovat i plechové kartičky z roku 1865, na kterých bylo vyraženo identifikační číslo zákazníka. Při placení klient pouze předložil kartičku a obchodník si do své evidence poznamenal potřebné údaje.

Náhradou za úvěrové známky se v USA kolem let 1911 – 1912 staly úvěrové karty (Credit Card). Rok 1914 se považuje za zrození první platební karty, která byla vydána telefonní společností Western Union. Na kartě se nacházelo číslo karty a podpisový vzor klienta. Cílem těchto karet bylo umožnit zákazníkům pohodlné bezhotovostní placení a zvýšit věrnost vůči obchodníkům. Western Union v budoucnu následovaly i jiné společnosti, jako byly obchodní domy nebo čerpací stanice.

Vznik prvních platebních karet, které umožňovaly splátkový prodej, se datuje do 30. let 20. století. Obchodníci nabídli zákazníkům možnost bezúročně splácet nákupy v několika měsíčních splátkách. Takovéto úvěry měly ovšem fatální následky pro obchodníky, když klienti nestíhali své závazky splácet.

Jako další se objevovaly tzv. Charge plates plechové karty, které na sobě měly vyraženo jméno klienta a číslo karty. Při placení kartou byl použit mechanický snímač – imprinter. Údaje otlačené na dokladu stvrdil zákazník svým podpisem. V následujících letech vznikaly věrnostní karty určené obchodním cestujícím u leteckých společností. Roku 1948 byla vydána první mezinárodně platná karta Air Travel Card.

Kolem roku 1950 začaly vznikat kartové společnosti, které sloužily jako prostředníci mezi obchodníky a jejich klienty. Mezi ty nejznámější se řadí, dnes již proslulá, společnost Diners Club. Cílem tohoto klubu bylo vydávat svým klientům úvěrové karty, kterými mohli zákazníci platit v síti restaurací. Klienti pak na konci měsíce dostali souhrnný účet k zaplacení. V roce 1953 se karty Diners Club staly celosvětově uznávané.

V 50. letech 20. století začaly své karty vydávat také americké banky. V Evropě byla první kreditní karta vydána v roce 1951 a první bankovní platební karta roku 1965, kterou vydala britská Westminster Bank.

Na konci 60. let 20. století ovlivnil vývoj platebních karet rozvoj výpočetní techniky. Roku 1968 se na platební karty dostal magnetický proužek, který slouží jako záznam dat. V 70. letech se díky rozvoji datových sítí rozšířila síť bankomatů a platebních terminálů. Od 80. let jsou magnetické proužky nahrazovány mikroprocesorovými kartami osazenými čipem, tzv. Smart Cards. Po vytvoření prvního internetového prohlížeče v roce 1995, rostl rozvoj e-commerce a internetových obchodů, kde lze platit kartou online, téměř exponenciálním tempem. V současné době je velkým trendem bezkontaktní placení, které zvyšuje pohodlí prováděných plateb (1).

O oblíbenosti platebních karet svědčí údaj o počtu vydaných platebních karet. Za rok 2012 jich bylo jen v České republice vydáno přes 10 miliónů (2).

3 Rozdělení platebních karet

3.1 Podle způsobu zúčtování na kartě

3.1.1 Debetní karty

Debetní platební karty vznikly v 70. letech 20. století a to díky rozvoji výpočetních a telekomunikačních prostředků. Po uvedení prvního bankomatu do provozu se od roku 1970 začaly po Spojených státech rozšiřovat karty s magnetickým proužkem (3). Debetní karta je platební kartou vydávanou k běžnému účtu klienta a slouží k nakládání s tímto účtem. Jejími hlavními funkcemi jsou platby u obchodníků a výběr hotovosti

z bankomatů. V dnešní době jsou debetní karty považovány za základní kartu vydávanou za účelem snadné manipulace s účtem a to i nezletilým osobám nebo klientům s nízkou bonitou (klientům, kteří nejsou příliš hmotně nebo nehmotně zajištěni).

3.1.2 Charge karty

Za vznikem charge karet stojí vydavatelé karet, kteří chtěli svým zákazníkům pomoci tím, že jim umožní odložit úhrady plateb jejich přesunutím k závěru měsíce, příp. i déle (3). Klientovi slouží karta převážně k platbám u obchodníků. Výběry z bankomatů jsou možné, avšak bývají pro klienta nevýhodně zpoplatněny. Po období čerpání následuje bezúročné období a datum splatnosti, do kterého musí být provedena plná splátka souhrnného výpisu od vydavatele. Charge karta je platební prostředek jednoduchý, bezpečný a pohodlný při použití na soukromých i služebních cestách (3). Vzhledem k vyšším úvěrovým limitům jsou tyto karty vydávány především bonitním klientům, protože je karta často zatížena vysokým poplatkem za její vydání, které je ovšem kompenzováno formou propracovaných věrnostních systémů, vstupů do speciálních letištních salónků, slev v hotelích a podobných doplňkových služeb. Mezi nejznámější vydavatele charge karet patří American Express nebo Diners Club.

3.1.3 Kreditní karty

Jde o platební kartu, která je spojena se spotřebním úvěrem čerpaným prostřednictvím revolvingového účtu. Získání kreditní karty je doprovázeno uzavřením úvěrové smlouvy. Klient využívá kartu, podobně jako charge kartu, především pro placení u obchodníků, a protože vstupuje do závazku vůči bance, je karta vydávána osobám zletilým a svéprávným. Stejně jako u charge karet je pro klienta nevýhodný výběr hotovosti z bankomatů. Na základě ohodnocení bonity klienta je stanoven úvěrový limit, který závisí na parametrech jako je věk klienta, roční příjem, již poskytnuté půjčky, vlastnictví majetku, vztah klienta k bance, apod. (3). Úvěrový limit se obnovuje splacením dlužné částky, která může být splacena po částech nebo najednou. Za platbu kartou odvádí obchodník poplatky bance za použití karty (tzv. merchant fee) a část tohoto poplatku je případně odváděna i vydavateli karty (tzv. interchange fee). Z hlediska banky se tak jedná o jeden z nejziskovějších produktů a to i přes vyšší úrokové riziko.

3.1.4 Elektronické peněženky

S nápadem elektronické peněženky přišly již v 80. letech 20. století francouzské banky. Díky rozšířenosti a oblibě platebních karet bylo jejich cílem zvětšit oblast použití karet i do jiných zařízení jako jsou parkovací a výdejní automaty nebo menší platby v obchodech. Elektronická peněženka má sloužit pro platby nižších částek a to zhruba do 30 amerických dolarů. Jedná se o čipové karty, které se dobíjejí na určitou peněžní částku a použitím peněženky při placení se tato částka snižuje. Zaplacené částky se zaznamenávají do platebních terminálů a v rámci úspor provozních nákladů jsou tyto transakce zasílány k zúčtování v souhrnné sumě. V současné době je zřejmě nejrozšířenějším systémem elektronických peněženek projekt Mondex, jehož většinový podíl vlastní společnost MasterCard. Mondex zahájil zkušební provoz již roku 1995 v anglickém městečku Swindon. Do této elektronické peněženky je možné dobít až 750 amerických dolarů, které mohou být rozděleny až do pěti různých měn. Mondex využívá bezpečnou platformu čipů s operačním systémem Multos (1).

3.2 Podle způsobu provedení

3.2.1 Elektronická

Elektronické platební karty mají veškeré informace na kartě uloženy v elektronické podobě a to na magnetickém proužku, ale v dnešní době především na elektronickém čipu, který se řídí standardem EMV. Některé volně dostupné informace jsou ale taktéž na kartě vytištěny (ne reliéfním písmem). Elektronické platební karty lze použít k výběru z bankomatů a platbám u obchodníků, kteří vlastní on-line platební terminál. Při každém použití vyžadují tyto karty ověření pomocí kódu PIN. Každá transakce provedená touto kartou je autentizována on-line jejím vydavatelem (4). Mezi nejrozšířenější elektronické platební karty v ČR patří Maestro a VISA Electron (2).

3.2.2 Embosovaná

Embosovaná karta neboli karta s reliéfním písmem má plasticky vytlačené údaje na kartě. Stejně jako elektronická karta nese informace uložené na magnetickém proužku nebo čipu. Oproti kartám elektronickým slouží ale i k použití v manuálních snímačích – tzv. imprinterech. Díky tomu mají embosované karty větší rozptyl použití (4). Embosované

karty nejsou příliš bezpečné a také manipulace s účtenkami a jejich následné typování do elektronické podoby je pro banky náročné na lidské zdroje (3). V případě ztráty nebo odcizení, a následné blokaci, musí být totiž karta zařazena na tzv. stoplist, tj. seznam blokovaných karet, který banka rozesílá obchodníkům, aby nebylo možné použít zablokovanou kartu. V ČR jsou nejrozšířenějšími embosovanými kartami MasterCard Standard a VISA Classic (2).

3.3 Podle způsobu záznamu dat

3.3.1 S magnetickým proužkem

Magnetický proužek se stal prvním elektronickým nosičem informací na platebních kartách. Princip magnetického záznamu byl znám již od roku 1878, ale až roku 1968 byla firmou IBM vyvinuta technologie záznamu dat na magnetický proužek, který mohl být umístěn na platební kartu, zvaná Hot Stamping – zažehlování (1). Pomocí magnetického proužku byl možný výběr hotovosti z bankomatu a později také elektronické placení. Použití karty je vázáno na znalost kódu PIN. Řešení záznamu dat na magnetický proužek sjednotily normy ISO 7811 a 17813. Na proužku se nacházejí 3 záznamové stopy, které jsou zakódovány (3).

Stopa 1 byla definována v roce 1969 Mezinárodní asociací leteckých dopravců IATA. Obsahuje 79 znaků, jež nesou informaci o číslu karty a jménu klienta.

Stopa 2 byla vyvinuta Asociací amerických bankéřů pro on-line transakce. Jejím obsahem je 40 číslic a to včetně čísla karty a v bankovnictví je využívána nejčastěji.

Stopa 3 může obsahovat až 170 číslic a dříve byla využívána pro off-line bankomaty. Byl zde zaznamenán parametr, podle kterého bylo možné ověřit kód PIN (1).

Magnetický proužek má ovšem omezenou kapacitu záznamu dat a mezi jeho další nevýhodu patří snadná duplikace. Již v době jeho vzniku měl spoustu odpůrců na straně některých bankovních společností a bylo též dokázáno, že zkopírovat data z jednoho magnetického proužku na druhý, šlo provést pouhým zahřátím žehličkou. Ostatní technická řešení záznamu dat na platební kartu, ač bezpečnější, se nakonec neprosadila, protože se jednalo o řešení technicky a finančně velice náročná (1). V dnešní době je

namísto magnetického proužku masově využíván čip, avšak magnetický proužek najedeme na kartách dodnes a to zejména z důvodu větší použitelnosti platební karty v případech, kdy obchodník nevlastní terminál, který umí přečíst kartu čipovou – tzv. hybridní karty (viz kapitola 3.3.3).

3.3.2 Čipové

Čipové platební karty jsou takové karty, které k uložení dat využívají paměťový čip nebo mikroprocesor. V dnešní době se jedná o nejbezpečnější druh záznamu na kartě, protože čipy poskytují vysokou ochranu zaznamenaných údajů proti jejich neoprávněnému čtení, záznamu či změně. K ověřování údajů slouží elektronické čtečky – terminály.

3.3.2.1 Vznik čipových karet

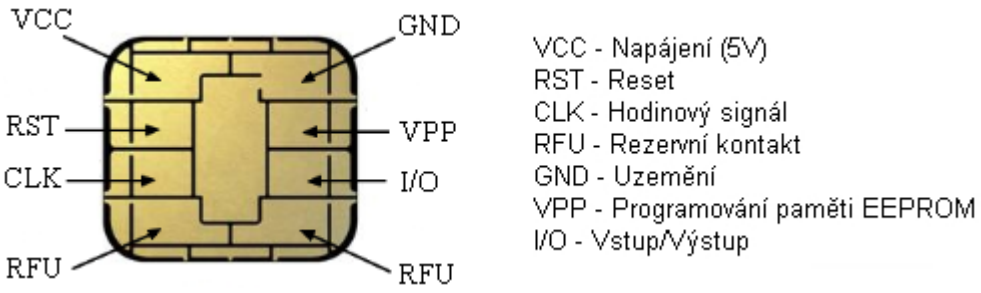
V 80. letech 20. století bylo z důvodu rostoucích požadavků na vyšší stupeň bezpečnosti identifikačních prostředků potřeba změnit dosud používanou technologii. V jednání byla dvě řešení a to čipové, nebo laserové karty. Laserové karty využívaly principu záznamu dat stejně jako kompaktní disky. Tyto karty vynikaly velmi vysokou pamětí (v době vzniku více než 4MB), avšak médium pro zápis zabíralo velkou plochu, a také provedené zápisy do paměti již nebylo možné smazat. I díky těmto důvodům se s laserovými kartami do budoucna nepočítalo a bankovní sféra investovala do karet čipových, jejichž možnosti jsou téměř nekonečné (3). Průkopníkem v oblasti používání čipových karet se staly francouzské banky, když se roku 1984 rozhodly využívat technologii Bull CP8 a čipy vyrobené firmami Motorola a Eurotechnique (1).

3.3.2.2 Druhy čipových karet

Existuje více typů čipových karet, a proto rozeznáváme zejména tři hlavní druhy – paměťové karty, paměťové karty s autentizací (vyžadují zadání PIN) a nejvyspělejší mikroprocesorové karty, které jsou v bankovnictví v současné době využívány nejvíce.

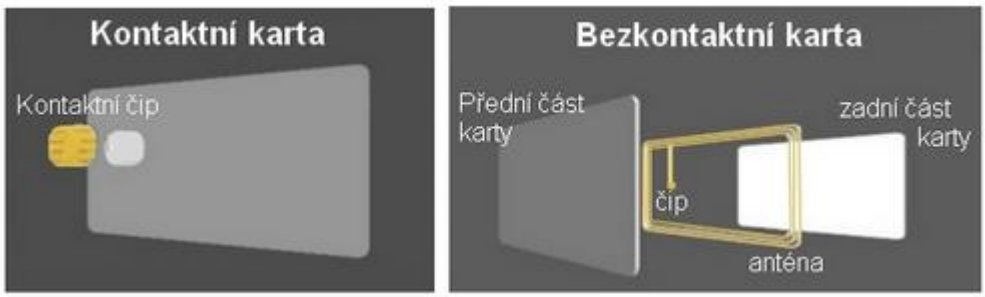
Mikroprocesorová karta má oproti kartám paměťovým tu výhodu, že disponuje tzv. aktivní inteligencí. Mikroprocesor dovolí přístup k datům uložených na čipu pouze subjektům, kteří se prokáží přístupovými kódy. Aplikace nahrané v čipu jsou schopny odhalit pokusy o neautorizovaný přístup a na základě toho kartu zablokovat nebo smazat data na ní uložená.

Na základě komunikace čipu karty s okolím rozeznáváme karty kontaktní a bezkontaktní. Kontaktní čipová karta musí byt vložena do čtečky čipových karet, aby došlo k přímému spojení kontaktů (viz Obrázek 1[1]). Přenos příkazů, dat a stavů karty probíhá přes tyto kontaktní místa (5). Standard kontaktních karet určuje mezinárodní norma ISO 7816 (viz kapitola 5.1).



Obrázek 1: Kontakty na čipu

Bezkontaktní karty využívají ke komunikaci s okolím anténu zapuštěnou po obvodu do struktury karty (viz Obrázek 2[2]). Takovou kartu stačí pouze přiložit do blízkosti čtečky a to přibližně na jednotky až desítky centimetrů. Jak karta, tak čtečka disponují anténou a komunikují pomocí rádiových vln. Většina bezkontaktních karet napájí čip pomocí tohoto elektromagnetického signálu (5). Standard bezkontaktních karet je určen především normami ISO 14443 a ISO 15693.



Obrázek 2: Struktura kontaktní a bezkontaktní karty

[1] Zdroj: https://www.conexus.ca/SharedContent/images/Banking/Actual%20Gold%20Chip.JPG
[2] Zdroj: http://www.smartcardalliance.org/pages/smart-cards-intro-primer

3.3.2.3 Struktura čipu

Čipové platební karty využívané v bankovnictví jsou poměrně složitá zařízení. Samotný čip mikroprocesorové karty se skládá z několika důležitých součástí (3):

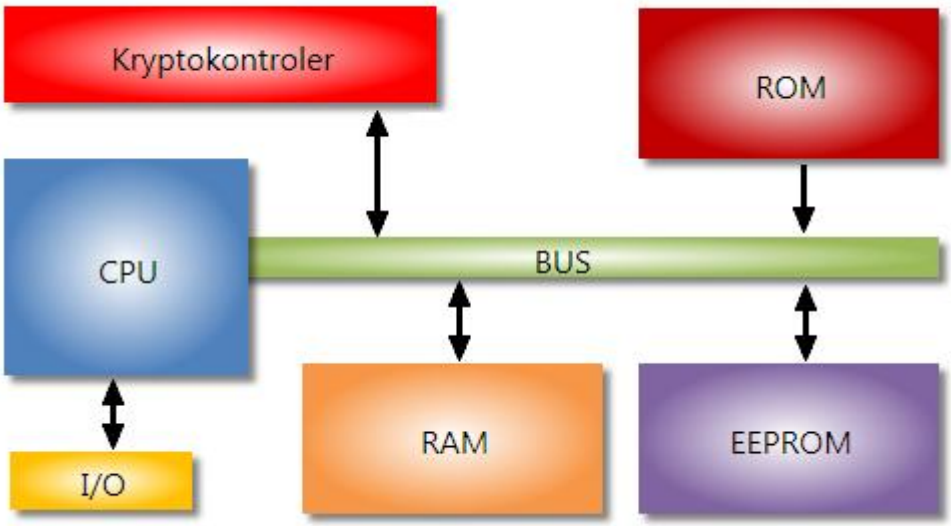
Vstup/Výstup – spojuje čip s vnějším okolím. Těmito kontakty prochází veškerá komunikace.

Paměť ROM – slouží k nahrání operačního systému, který je do ní zaznamenán při výrobě a nelze ji v budoucnu měnit. Mezi nejpoužívanější operační systémy čipových platebních karet patří například MULTOS nebo JavaCard. Paměť ROM se z bezpečnostních důvodů umísťuje do nejnižší vrstvy čipu, aby se zamezilo zkoumání její architektury za použití mikroskopů.

Paměť RAM – slouží k uchovávání dočasných výsledků výpočtů zajišťující ověřování vstupních kódů.

Paměť EEPROM – slouží pro uložení jednotlivých aplikací (platební aplikace, věrnostní programy, atd.) a je možné ji použít k záznamu nových programů nebo odstranění starých. Nacházejí se v ní informace volně dostupné (číslo karty, jméno držitele, apod.) a utajené (bezpečnostní klíče, digitální podpis, finanční limity klienta, PIN, aj.).

CPU (Central Processing Unit) – centrální řídící jednotka řídí a kontroluje veškeré operace a tok dat mezi čipem a jeho okolím. Vypočítává kontrolní výpočty a spolupracuje s bezpečnostními koprocesory, jakým je např. kryptokontroler. Používají se 8 až 32 bitové procesory.



Obrázek 3: Vnitřní struktura čipu

K ochraně dat uložených na čipové kartě je využíváno mnoho bezpečnostních opatření. Mezi ty, které výrobci netají, patří například detekce nízkého napětí, teplotní přesahy nebo detektory bránící ovlivnění hodinového signálu v čipu. Mikroprocesor bankovních karet využívá kryptokontroler, modulární aritmetický procesor a generátor náhodných čísel. Díky tomu jsou čipy schopné pracovat s digitálním podpisem RSA (3) (viz kapitola 6.2.1).

3.3.3 Hybridní

Hybridní karty jsou karty, které kombinují zápis uložení dat na různých typech záznamu. Nejčastěji se jedná o kombinaci magnetického proužku a čipu a to hlavně z důvodu přechodu terminálů u obchodníků, které provádí ověřování pouze pomocí magnetického proužku, k terminálům připravených pro čip.

Existují ovšem hybridní karty, které obsahují dva čipy (kontaktní a bezkontaktní). Může se jednat o čipy na sobě závislé (např. z důvodu navýšení paměti), nebo nezávislé (sloužící např. pro oddělení funkce platební karty a identifikační karty zaměstnance). Zároveň existují karty s jedním čipem a dvěma různými vstupně/výstupními rozhraními (tzv. duální čipové karty).

4 Náležitosti a ochranné prvky platební karty

Z fyzického hlediska obsahují platební karty určité povinné údaje a náležitosti a to nejen k využívání platebních funkcí, ale také ochranné prvky zabraňující výrobě padělků (viz Obrázek 4 a Obrázek 5[3]). Pro platební funkci karty je důležité číslo platební karty, jméno jejího držitele, platnost, CSC kód (pro transakce realizované přes internet) a podpisový vzor. Z bezpečnostního hlediska se na kartě nachází několik ochranných prvků pro znemožnění padělání karty a to zejména hologram, podpisový proužek, ultrafialové znaky nebo mikrotisk. Tyto prvky však hrají hlavní roli pouze při fyzickém padělání karty a při jejím běžném využívání pro platby již nejsou nadále ověřovány. Při nových způsobech použití platebních karet (bezkontaktní platby, platby mobilem) již ani obchodník nepřichází do očního kontaktu s kartou, protože tu má klient např. v peněžence nebo ve formě SIM karty ve svém chytrém telefonu.

Obrázek 4: Platební karta z přední strany

Obrázek 5: Platební karta ze zadní strany

[3] Zdroj: http://www.deutsche-card-services.com/en/service-area/risk-in-card-acquiring/card-fraud/fraud-protection-in-pos-selling.html

4.1 Hologram

Hologram byl zaveden v roce 1983 společností MasterCard jako ochranný prvek proti padělání, který v následujících letech zavedly i ostatní karetní asociace a společnosti (1). Používají se dvojrozměrné (2D) nebo třírozměrné (3D) lisované hologramy. Hologram se nejprve zaznamenává do fotocitlivého polymeru a následně je jako reliéf překopírován do kovové raznice. Z ní je v poslední fázi přetištěn do speciální fólie, která je umístěna na platební kartu (3).

4.2 Podpisový proužek

Pro zaznamenání podpisového vzoru držitele na kartě slouží zvláštní proužek papíru – podpisový proužek. Ten je proti padělání chráněn mnohobarevným tiskem a je citlivý na gumování a chemické látky. V případě gumování se na něm objeví nápis „VOID“ („neplatné“) (3).

4.3 Ultrafialové prvky

Většina platebních karet má skryté ultrafialové ochranné prvky, které jsou viditelné pouze pod UV lampou. Ochranné znaky by se pod UV lampu měly jasně objevit a neměly by být nijak pokřivené nebo zdeformované - to by značilo padělanou kartu. Každá karetní asociace si určuje vlastní znak, např. MasterCard používá písmena „MC“, VISA zase znak létajícího „V“.

4.4 Mikrotext

Jedná se o speciální mikroskopický tisk, který není pouhým okem rozeznatelný. Lze ho spatřit pod lupou, případně jinými specializovanými nástroji. Kopírovací stroje ho nedokáží zachytit a často bývá zanesen do textur, jako jsou vlnovky, proužky a podobné složitější obrazce. Kupříkladu platební karty MasterCard používají mikrotisk k lemování polokoulí v logu asociace.

5 Normy platebních karet

Protože se v prvopočátcích rozvoje čipových platebních karet vytvořilo hned několik různých způsobů provedení, bylo nutné zavést jednotné normy, které by tyto karty sjednotily. Dopomohlo k tomu i očekávané nasazení těchto technologií v jiných hospodářských oblastech, než bylo bankovnictví.

5.1 ISO

Mezinárodní organizace ISO v letech 1987 – 1989 vydala normy věnované kontaktním čipovým kartám. Norma ISO 7816 obsahuje následující části:

Označení	Význam
ISO 7816-1	Specifikuje fyzikální vlastnosti elektronických integrovaných obvodů kontaktních karet.
ISO 7816-2	Specifikuje rozměry a umístění jednotlivých kontaktů na čipu. Poskytuje také informaci o použití kontaktů.
ISO 7816-3	Specifikuje elektronické signály a napájení. Dále poskytuje informace o komunikaci mezi integrovaným obvodem a rozhraním (např. POS terminál).
ISO 7816-4	Definuje strukturu souborů a základní příkazy.
ISO 7816-5	Definuje registrační proceduru a identifikátory aplikací.
ISO 7816-6	Specifikuje datové prvky.
ISO 7816-7	Definuje příkazy pro SCQL (Structured Card Query Language).
ISO 7816-8	Specifikuje bezpečné příkazy pro karty s integrovanými obvody. Dále definuje bezpečné uložení dat na čip, prostřednictví ověřování přístupových práv.
ISO 7816-9	Specifikuje příkazy pro správu životního cyklu karty.
ISO 7816-10	Definuje elektronické signály a odpovědi na reset synchronních karet.
ISO 7816-11	Specifikuje osobní ověřování za pomoci biometrie.
ISO 7816-12	Specifikuje provozní podmínky karty s USB rozhraním, tzv. USB-ICC rozhraní.
ISO 7816-13	Specifikuje příkazy pro správu aplikací ve více-aplikačním prostředí.
ISO 7816-15	Struktura kryptografických aplikací (PKCS#15).

Tabulka 1: ISO 7816 - Popis jednotlivých složek (6)

Pro standard bezkontaktních karet byly vytvořeny normy ISO 10536 (pro karty s těsnou vazbou), ISO 14443 (pro karty s blízkou vazbou – cca do 10cm) a ISO 15693 (pro karty s vazbou na dálku – do vzdálenosti cca 1m) (6).

5.2 EMV standard

V roce 1994 založily karetní asociace Europay, MasterCard a VISA společnou skupinu nazvanou EMV Group. Jejich cílem bylo vytvoření nových norem, pro rozvíjející se generaci mikročipových platebních karet, založených na standardech ISO 7816 (3). V současné době je společnost EMV vlastněna asociacemi MasterCard, VISA, American Express a JCB.

Hlavním cílem společnosti EMV je pomoc usnadnit vzájemnou komunikaci čipových karet a zařízeních přijímající karty, jako jsou POS terminály nebo bankomaty, díky souhrnu specifikací určených pro platební sféru. Tento cíl se též vztahuje i na nové formy plateb, jako jsou bezkontaktní platby nebo mobilní platby. V polovině roku 2012 bylo celosvětově používáno 1,55 miliardy EMV platebních karet (7).

5.2.1 Průběh EMV transakce

Mezi čtením magnetického proužku a EMV čipu při průběhu transakce je zásadní rozdíl. V případě magnetického proužku se karta chová pouze jako úložiště dat, ze kterého terminál přečte data a karta již není nadále využívána. Terminál provede veškerá zpracování a na transakci aplikuje pravidla platby.

Během EMV transakce je čip schopen zpracovávat informace a stanovit mnoho parametrů platby. Terminál pomáhá určovat pravidla nastavená vydavatelem karty, která jsou uložena v paměti čipu. Tato pravidla mohou obsahovat služby jako off-line ověřování, ověření držitele karty pomocí kódu PIN nebo podpisu, on-line autorizace, atd.

EMV specifikace, z důvodu interakce mezi čipem a terminálem, definuje vlastní protokol, který obsahuje sérii několika kroků:

1. Výběr aplikace - V paměti čipu může být uloženo několik aplikací. Terminál i čip se musí shodnout na aplikaci určenou k provedení transakce.
2. Zahájení zpracování aplikace a čtení dat - Vybraná aplikace je inicializována a terminál čte potřebná data z čipu.
3. Off-line ověřování dat - Výběr statického, dynamického nebo kombinovaného ověřování dat.
4. Zpracování omezení - Provedení kontrol ke zjištění, zda čip dovoluje provedení požadované transakce.
5. Ověření držitele - Držitel karty je ověřen pomocí metody (podpis, on-line PIN, bez ověření, atd.) podporované terminálem a odsouhlasené čipem.
6. Řízení rizik terminálem - Terminál provede několik kontrol (jako je floor limit), aby zjistil, zda je potřebné on-line zpracování.
7. Analýza činnosti terminálu - Založená na předchozích čtyřech krocích, pravidlech terminálu a čipu. Aplikace v terminálu vyžaduje po čipu jeden z výsledků – zamítnout off-line ověření, schválit off-line ověření, nebo požadovat ověření on-line.
8. Analýza činnosti karty - Na základě pravidel a limitů, uložených na čipu vydavatelem karty, odpoví čip jednou ze tří odpovědí na předchozí dotaz terminálu.
9. Online zpracování - Nastane v případě, že čip odpověděl na dotaz terminálu „ověření on-line“. Terminál pak pro vydavatele karty vytvoří dotaz k autorizaci a on-line ověření karty. V případě, že odpověď obsahuje volitelné ověřování vydavatele, odesílá ještě terminál data čipu ke schválení.
10. Transakce je dokončena.

V případě transakce bezkontaktní technologií je postup odlišný pouze v tom, že komunikace mezi kartou a terminálem je mnohem rychlejší, a proto mohou být některé kroky (např. on-line ověření) provedeny až po odebrání čipu z blízkosti čtečky. Cílem je co nejkratší množství času, po které musí být čip přiložen k čtečce (8).

5.2.2 Prvky EMV

5.2.2.1 Aplikační kryptogram

Aplikační kryptogram je během EMV transakce vygenerován za použití dvou 3DES klíčů. Je to podpis generovaný z důležitých datových prvků obsažených v on-line žádosti o autorizaci u vydavatele karty, nebo pro poslední finanční transakci vyžadovanou pro clearing (zúčtování). Aplikační kryptogramy jsou používány ve zprávách zasílaných mezi kartou a jejím vydavatelem, on-line autorizacemi karty u vydavatele nebo pro ověřování integrity (neporušenosti) datových prvků transakce.

Kód generovaný pro žádost o on-line autorizaci se nazývá ARQC (Authorisation Request Cryptogram) a kód, který je generovaný podepisováním dat, kdy čip schvaluje platbu pro závěrečné zúčtování, se označuje jako TC (Transaction Certificate). Pokud je transakce odmítnuta, vygeneruje čip kryptogram zvaný AAC (Application Authentication Cryptogram).

Aplikační kryptogram má tedy dvojí význam (8):

a) Při on-line ověřování karty u vydavatele generuje čip ARQC kód, který je odesílán v žádosti o ověření. Vydavatelem potvrzený ARQC značí, že čip není padělaný.
   Vydavatel karty může vygenerovat zpětný kryptogram, nazývaný ARPC (Authorisation Response Cryptogram), který je čipu zasílán zpět v odpovědi. Verifikace ARPC umožní čipu zjistit, že schválení bylo provedeno od skutečného vydavatele.
b) Podepisování datových prvků pro ověření transakce a její integritu.
   Kryptogramy (ARQC, ARPC, TC a AAC) jsou generovány podepisováním důležitých datových prvků zpráv transakce. Ověření kryptogramů příjemcem pomáhá potvrzovat, že datové prvky nebyly změněny.

5.2.2.2 Řízení rizik a kontroly autorizace

EMV poskytuje vydavatelům kontroly u obchodníků, což pomáhá snížit úroveň vystavení se podvodům a úvěrovým rizikům při off-line transakcích a transakcích pod floor limitem. Vydavatelská banka může nastavit limity na čipu karty, čímž omezí počet po sobě jdoucích off-line transakcí, které mohou být zpracovány.

Dále EMV definuje příkazy (tzv. Scripts Commands), které mohou být vydavatelem odeslány na čip při odpovědi na on-line ověření (ty slouží např. pro snížení limitů karty). Vydavatelé mohou taktéž rozesílat příkazy pro blokaci ztracených či ukradených karet (8).

5.2.2.3 Zpracování při ověření držitele karty

EMV definuje dvě funkce, které umožňují vydavatelům karet ověřovat skutečného vlastníka platební karty. Ty pomáhají redukovat výskyt podvodů při ztrátě nebo odcizení karty. Jedná se o tzv. CVM List a Off-line PIN.

CVM (Cardholder Verification Method) list neboli seznam způsobů ověřování držitele karty je soupis všech možných metod ověření transakce, které může držitel provést. Tento seznam určuje vydavatel karty a je nahrán na čipu, v pořadí podle priority. Vydavatel tím může po držiteli karty vyžadovat zadání kódu PIN na každém teminálu, který PIN podporuje, ale při cestování na trhy, kde není PIN podporován, umožnit ověření transakce podpisem držitele.

Funkce Off-line PIN má při zasílání kódu k ověření z terminálu na kartu dvě varianty. Zašifrovaný off-line PIN, kde je využívána kryptografie veřejného klíče, a Plaintext off-line PIN, kdy je kód zasílán ve formě prostém textu (8).

5.2.2.4 Offline ověřování dat

EMV popisuje funkci offline ověřování dat pro boj proti padělatelským podvodům, které jsou prováděny v off-line platebních terminálech. Offline ověřování dat používá kryptografii veřejných klíčů pro provedení ověření údajů o platbě, bez nutnosti ověření transakce on-line u vydavatele.

Celkem jsou dostupné tři metody, které volí vydavatel v závislosti na možnostech karty. Během transakce může být vybrána pouze jedna metoda off-line ověření dat.

Statická autentizace dat

Značí, že podepsaná data na čipu nebyla změněna nebo že s nimi nebylo nijak manipulováno.

Každá karta je personalizována certifikátem veřejného klíče vydavatele a podepsanými statickými aplikačními daty, které se skládají z personalizovaných datových prvků na kartě, podepsaných privátním klíčem vydavatele.

Terminál provádí RSA šifrování pro ověření podepsaných statických dat za pomoci veřejného klíče vydavatele.

Statická autentizace neumožňuje odhalení padělku karty, protože nesvědčí o tom, zda je karta ověřována off-line.

Dynamická autentizace dat

Značí, že s kartou a jejími daty nebylo manipulováno a že karta není padělaná.

Každá taková karta je personalizována certifikátem veřejného klíče vydavatele, soukromým a veřejným klíčem karty.

Karta během transakce generuje unikátní dynamická aplikační data, podepisováním datových prvků jak od karty, tak od terminálu. Tyto data podepisuje svým soukromým klíčem. Terminál provádí RSA šifrování pro ověření podepsaných dynamických dat pomocí veřejného klíče karty.

Dynamická autentizace je bezpečnější než statická, protože značí, že karta byla ověřována off-line.

Kombinovaná autentizace dat

Jedná se o dynamickou autentizaci dat s generováním aplikačního kryptogramu. Vyžaduje stejné personalizační prvky jako dynamická autentizace a přidává dobrovolný krok během analýzy karty.

Karta za použití jejího soukromého klíče generuje tzv. dynamický podpis a to jako doplněk k aplikačnímu kryptogramu, aby dokázala, že karta ověřovaná během dynamické autentizace, byla ta stejná karta, která aplikační kryptogram poskytla.

Kombinovaná autentizace pomáhá při detekci útoku typu „man-in-the-middle“, kde podvodník mění data odesílaná mezi kartou a terminálem (8).

Plánem společnosti EMV do budoucna je snaha poskytovat bezpečnostní prvky pro jakékoliv druhy plateb. Do této činnosti lze zařadit tvorbu společného bezkontaktního jádra pro všechny platební systémy v jedné čtečce, rozšíření off-line procesu o kryptografii nad eliptickými křivkami a definice architektury pro EMV bezkontaktní a mobilní platby (7).

5.3 PKCS

Na vyšší komunikační úrovni, tzn. úroveň API, tedy komunikace s aplikačním rozhraním, se karty řídí bezpečnostními kryptografickými standardy PKCS#11 a PKCS#15.

Standard PKCS#11 specifikuje API rozhraní, zvané Cryptoki, pro zařízení, která uchovávají kryptografické údaje a provádí kryptografické operace. Cryptoki vykonává jednoduchý objektově založený přístup, nezávisle řeší cíle dané technologie (pro jakýkoliv druh zařízení), sdílí zdroje (více aplikací může přistupovat k více zařízením) a předává aplikacím společný pohled na zařízení, tzv. kryptografický token (9).

Standard PKCS#15 vychází z normy ISO 7816 a umožnuje uživatelům identifikovat se za použití kryptografických tokenů pro více aplikací, bez ohledu na Cryptoki aplikace poskytovatele.

6 Šifrování používaná v bankovnictví

6.1 Symetrické šifry

Symetrické šifry slouží k bezpečné komunikaci mezi účastníky za pomoci tajného klíče. Tento klíč si musí komunikující strany předem vyměnit a zajistit, aby se k němu nedostal útočník. Odesílatel tímto klíčem zprávu zašifruje a příjemce na příchozí zprávu aplikuje dešifrovací algoritmus za použití stejného klíče. Pokud byly dodrženy podmínky o utajení klíče, může symetrická šifra sloužit jako druh autorizace, protože účastníci komunikace ví, kdo daný klíč vlastní (10). Výhodou symetrické kryptografie je její rychlost. Naopak její nevýhodou jsou nároky na bezpečné předání klíčů komunikujících stran. Algoritmů založených na symetrických šifrách existuje několik. Mezi ty nejpoužívanější patří DES, 3DES nebo AES.

6.1.1 DES

Algoritmus DES (Data Encryption Standard) se skládá z bloku 64 binárních číslic, kde je 56 bitů náhodně generováno a zbylých 8 bitů je použito pro detekci chyb.

Algoritmus spočívá v opakování 16 cyklů pro vytvoření 16 klíčů o délce 48 bitů. V každém cyklu se vytvoří počáteční permutace, která se následně rozdělí na 2 poloviny (L_0 a R_0). Dojde k posunu bitů klíče. Pravá strana se rozšíří expanzivní permutací, následně jsou sčítačkou sečteny a jejich opětovná permutace je zkombinována s levou polovinou. Původní pravá strana se nemění a stává se novou levou polovinou pro další cyklus. Dešifrování probíhá v opačném směru ve správném pořadí posunu klíčů (11).

Složitost klíče DES byla již v minulosti překonána a dnes není považován za bezpečný. Vznikly proto modifikace DES algoritmu, např. 3DES, který provádí vícenásobnou (trojnásobnou) aplikaci DES za sebou. Díky této násobnosti je sice považovaný za bezpečný, výpočetně je ale pomalý a nehodí se pro každou aplikaci.

6.1.2 AES

Nový algoritmus byl standardizován v roce 2001 jako náhrada za již prolomený a nedostačující DES algoritmus. AES podporuje délky klíčů 128, 192 a 256 bitů v blocích po 128 bitech. Funguje tak, že před zašifrováním se odpovídající blok nezašifrovaného textu XORuje předcházejícím blokem zašifrovaného textu. To značí, že jednotlivé bloky na sobě závisí a aby se dešifroval konkrétní blok, musí se dešifrovat i ty předchozí. První blok se šifruje blokem náhodně vygenerovaným (12).

Postup AES algoritmu se skládá ze čtyř kroků:

1. SubBytes – prohodí jednotlivé bajty za jiné.
2. ShiftRows – transformace posledních třech ze čtyř řádků matice.
3. MixColumns – prohození sloupců a jejich roznásobení polynomem.
4. AddRoundKey – podklíč je zkombinován s každým bajtem za pomoci metody XOR.

6.2 Asymetrické šifry

Asymetrické šifry, oproti těm symetrickým, využívají dvojici klíčů. Jedná se o klíč šifrovací a dešifrovací, respektive soukromý a veřejný. Nejrozšířenějším asymetrickým algoritmem je RSA algoritmus. Mezi další asymetrické algoritmy lze zařadit i algoritmus eliptických křivek – ECC (Elliptic Curve Cryptography). Výpočetní náročnost ECC je stejná jako u RSA algoritmu, má ovšem výhodu v daleko menší délce klíče a to při zajištění stejné míry bezpečnosti (160 bitů dlouhý ECC klíč odpovídá klíči RSA o délce 1024 bitů) (10).

6.2.1 RSA

Algoritmus byl publikován v roce 1978. Zkratka RSA pochází z iniciálů jeho autorů Ronald Linn Rivest, Adi Shamir a Leonard Max Adleman. Algoritmus RSA pro šifrování a dešifrování zpráv těží z teorie zbytkových tříd a kongruencí.

Postup algoritmu je následující:

1. Zvolíme dvě prvočísla (p a q), která musí být dostatečně dlouhá.
2. Tyto prvočísla mezi sebou vynásobíme podle rovnice n = p*q.
3. Pro výsledek součinu n najdeme Eulerovu funkci.
4. Zvolíme číslo r, které je menší než výsledek Eulerovy funkce a je s ním nesoudělné.
5. Najdeme číslo s, které reprezentuje zbytkovou třídu inverzní ke zbytkové třídě r modulo výsledek Eulerovy funkce.

Tímto postupem získáme dvojice čísel, které slouží k vytvoření veřejného (n, r) a soukromého (n, s) klíče (13).

Pro zajištění bezpečného používání RSA algoritmu je nutné volit velká počáteční prvočísla. Obvyklé délky vygenerovaných klíčů se pohybují mezi 1024 – 2048 bitů (v některých případech až 4096 bitů), které se nedají žádnými prostředky faktorizovat (rozložit na součin prvočísel).

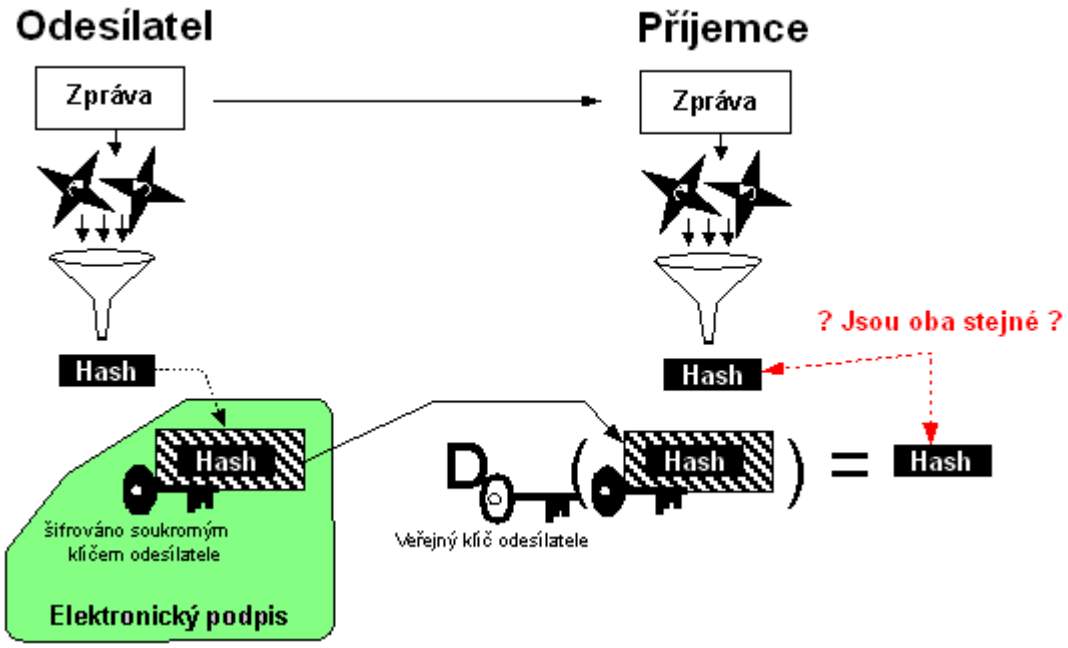
6.3 Elektronický podpis

Jak již bylo zmíněno v kapitole o EMV standardu, platební karta využívá v průběhu ověřování digitální podpis a podpis pomocí využití certifikátů. Elektronický podpis je založen na asymetrické kryptografii, využívá tudíž dvojici soukromého (je znám pouze vlastníkovi) a veřejného (je zveřejněn vlastníkem, např. v podobě certifikátu) klíče. Elektronický podpis v české legislativě řeší zákon „O elektronickém podpisu“ č. 227/2000 Sb., který byl později novelizován dalšími zákony.

6.3.1 Digitální podpis

Digitální podpis je postup, po kterém vznikne zašifrovaný dokument, zajišťující pravost a nepopiratelnost daného dokumentu. Z dokumentu se nejprve vypočte jeho otisk (tzv. hash), který je následně zašifrován soukromým klíčem odesílatele a nakonec přidán k odesílané zprávě.

Při ověřování si příjemce sám vypočte hash z doručené zprávy, veřejným klíčem odesílatele dešifruje digitální podpis a výsledný hash porovná s vypočteným. V případě rovnosti obou hashů má příjemce jistotu, že zpráva byla zašifrována vlastníkem odpovídajícího soukromého klíče, tedy odesílatelem (10).



Obrázek 6: Ověření digitálního podpisu (10)

6.3.2 Certifikát

Digitální podpis je při dodržení všech povinností relativně bezpečná funkce, avšak stále hrozí nebezpečí při distribuci veřejného klíče. Pokud do komunikace, při které si komunikující stany vyměňují veřejný klíč, vstoupí útočník, může si původní veřejný klíč uschovat a namísto toho podvrhnout svůj vlastní vygenerovaný. Odesílatel pak v domnění bezpečí šifruje zprávu útočníkovým podvrženým veřejným klíčem a ten následně může zprávu dešifrovat, přečíst, příp. změnit, zašifrovat originálním veřejným klíčem a poslat původnímu příjemci.

Proti tomuto problému se lze bránit certifikací veřejného klíče certifikační autoritou, která hraje roli nezávislé třetí strany. Certifikát je digitálně podepsaná datová struktura, jejíž hlavní složkou je veřejný klíč držitele certifikátu. Mezi další její složky patří verze certifikátu (odvozená od normy X.509), pořadové číslo certifikátu, algoritmus pro výpočet otisku a asymetrický algoritmus pro šifrování, platnost, vydavatel, předmět, jedinečné jméno a další možná rozšíření. Certifikát v konečné fázi slouží k vytváření elektronického podpisu, šifrování a autentizaci osob a objektů.

Postup vydání certifikátu je následující:

1. Vygenerování páru soukromého a veřejného klíče.
2. Sestavení struktury žádosti o certifikát (identifikační údaje žadatele, veřejný klíč, atd.)
3. Tuto strukturu žadatel digitálně podepíše svým vygenerovaným soukromým klíčem.
4. Žádost odešle certifikační autoritě.
5. Ověření údajů žadatele certifikační autoritou, která si též verifikuje elektronický podpis žadatele na základě přiloženého veřejného klíče – tím si ověří, že žadatel vlastní příslušný soukromý klíč.
6. Vydání certifikátu.

V tuto chvíli může být veřejný klíč šířen v podobě certifikátu, který si druhá strana ověří a v případě, že jsou všechny náležitosti v pořádku, šifruje zprávu za pomoci veřejného klíče z certifikátu. Původní žadatel o certifikát pak zprávu dešifruje svým, již vygenerovaným, soukromým klíčem (10).

6.4 Protokoly SSL, TLS

S rozvojem e-commerce, transakcí realizovaných platební kartou pomocí internetu, bylo nutné tyto transakce dostatečně zabezpečit. V počátcích vývoje tohoto druhu plateb našly banky a karetní asociace řešení v protokolech SSL a SET, nyní i v protokolu TLS (3).

SSL (Secure Socket Layer) je protokol vyvinutý v polovině 90. let 20. století firmou Netscape. Zajišťuje bezpečnou a důvěrnou komunikaci v síti internet za pomocí šifrování zpráv, volitelně může ověřovat oprávněnost klienta a obchodníka k transakci za využití certifikátů (3).

Roku 1995 vytvořily asociace Europay, MasterCard a VISA vlastní protokol, zvaný SET (Secure Electronic Transaction). Ten definuje komunikaci mezi zákazníkem, obchodníkem a bankou za využití certifikátů. Připojení bylo sice bezpečné, ale značně nepohodlné, protože každý uživatel SET protokolu musel disponovat vlastním certifikátem, a proto se tento protokol příliš nerozšířil (3).

TLS (Transport Layer Security) protokol je nástupcem protokolu SSL verze 3. TLS se stal oficiálním protokolem internetu (RFC-2246) a jedná se o otevřený protokol, který může využít libovolný aplikační protokol. TLS umožňuje autentizaci klienta a serveru (za pomoci certifikátů). Umožňuje komunikovat i zcela anonymně, ve většině případů ale autentizuje alespoň server. Počáteční výměna kryptografického materiálu proběhne za využití asymetrických šifer, následný přenos dat je pak šifrován symetricky. TLS zajišťuje integritu přenášených dat díky provádění kontrolního součtu. Neprovádí ovšem elektronické podepisování transakcí, tzn., že nezajišťuje důkaz o pravosti dat. To je volitelně zajišťováno aplikací na aplikační vrstvě. Na počátku komunikace se vytvoří tzv. TLS relace – dohoda serveru a klienta na použití kryptografických algoritmů, materiálu a provedení autentizace. Během navázané TLS relace již probíhá zabezpečené přenášení dat (10).

7 Způsoby použití platební karty a bezpečnostní prvky

7.1 Bankomat

ATM (Automated Teller Machine) neboli bankomat je zařízení, sloužící především k výběru hotovosti z účtu klienta za pomoci jeho platební karty.

Na myšlenku zařízení, které by bylo schopné vydávat hotovost 24 hodin denně, přišel již roku 1967 Skot John Shepard Baron. Otevírací doba bank nebyla v té době ke klientům příliš vstřícná, a on tak nechtěl být limitován v možnosti přístupu ke své hotovosti. Pro myšlenku bankomatu se nadchl generální ředitel Barclays Bank Harold Darvill. Jeho banka dne 27. června 1967 zprovoznila v Londýně vůbec první bankomat na světě. Klient do bankomatu vložil šek a byl požádán o zadání kódu PIN. Zařízení mu poté v přihrádce vystavilo svazek deseti jednolibrových bankovek (1).

Dnešní bankomaty jsou ovšem daleko sofistikovanější. Pomohl tomu hlavně přelom 20. a 21. století, kdy banky hledaly efektivnější distribuční modely. Dnešní víceúčelové bankomaty tak umožňují výběry hotovosti v domácí i cizí měně, možnost zvolit si požadovanou hodnotu, volbu skladby nominálů bankovek, vklady hotovosti (i mincí), zobrazení a tisk zůstatku na účtu, tisk peněžních poukázek, zadání příkazu k úhradě, prodej vstupenek, jízdenek a pojištění, změnu kódu PIN, důležité kontakty, nápovědu k obsluze a mnoho dalšího (1).

Z technického hlediska lze bankomat rozdělit na tři hlavní části:

Trezor – pro úschovu hotovosti.

Operátorská část – slouží k řízení bankomatu a obsahuje počítač, operátorskou klávesnici a tiskárnu.

Provozní část – obsahuje obslužnou obrazovku s klávesnicí, počítač bankovek, podávací a transportní systém, tiskárnu stvrzenek a snímač platební karty (3).

7.1.1 Bezpečnost bankomatů

Dnes najdeme v provozu výhradně on-line bankomaty, které jsou v reálném čase pomocí datové sítě napojeny na autorizační centrum banky, a ověření celé transakce je tak otázkou maximálně několika vteřin. Počítač uvnitř bankomatu dokáže šifrovat komunikaci a zajistit bezpečí posílaných dat jak mezi bankomatem a autorizačním centrem, tak mezi bankomatem a kartou. S jeho pomocí je možné připojit k bankomatu různá alarmová čidla pro detekci nežádoucích prvků umístěných na jeho důležitých částech nebo kameru zaznamenávající pohyb v okolí bankomatu. Speciální software pak má za úkol vyhodnocovat nestandardní chování (např. vložení karty, ale neprovedení žádné operace, apod.). V případě vyhodnocení kritického nebezpečí bankomat skutečnost ohlásí do centrály a vypne se. Ověřování držitele karty je nejčastěji prováděno zadáním kódu PIN na klávesnici bankomatu. Snížení rizika podvodů má na starosti i hardware ve formě zelených nástavců na slotu čtečky karet nebo trhavé pohyby zajíždějící karty pro znesnadnění zkopírování magnetického proužku.

Z fyzického hlediska jsou pak bankomaty chráněny nejen speciálním pláštěm, bezpečnostním a komunikačním modulem, kotvením konstrukce k zemi šrouby, demontovatelnými až po otevření trezorové části, ale i svou vahou (kolem 1000 kg) (3).

7.2 POS terminál

Platební terminál neboli POS (Point Of Sale) terminál je zařízení sloužící pro platby kartou u obchodníků. Klient vloží kartu do čtečky (terminálu) a v případě úspěšné autorizace je provedena transakce.

První terminály se objevily již v 60. letech minulého století, avšak k většímu rozšíření došlo až s rozvojem debetních karet po roce 1990 (1). Nahrazovaly mechanické snímače, tzv. imprintery, které otlačily reliéfní písmo embosované karty na účtenku. Ty však nepoužívaly autorizaci plateb pomocí kódu PIN. Autorizace byly prováděny telefonicky u transakcí o vyšší cenové hladině. Zavedení terminálů bylo vynuceno vzrůstajícím počtem papírových účtenek, které museli obchodníci zasílat bankám k úhradě a také nároky na časové odbavení klienta. On-line terminály zrychlily ověřování a zvýšili tím i bezpečnost. První terminály ověřovaly držitele na základě magnetického proužku.

Poslední generace terminálů umožnuje spouštění více aplikací najednou. To bylo vynuceno bankami i obchodníky, kteří chtěli na terminálech provozovat nejen operace platební, ale i věrnostní a jiné. Od roku 2005 se začaly rozvíjet terminály s moduly pro bezkontaktní placení a také pro bezkontaktní mobilní platby (1). Vzhledem k velkému počtu transakcí realizovaných skrze terminály jsou některé transakce ověřovány off-line, tzn., že se terminál při každé transakci nepřipojuje on-line na autorizační centrum, ale údaje o platbě si uloží do paměti a ty pak v určitých intervalech zasílá souhrnně ve větším množství. To prospívá k rychlejšímu odbavení zákazníků, ale současně částečně snižuje bezpečnost prováděné operace. Současné terminály umožňují při nákupu mj. i výběry hotovosti (Cash Back), dobití mobilních telefonů (Top Up), tisk vstupenek, poukázek, jízdenek nebo prodej a tisk virtuálních karet (1).

Čipová karta fyzicky komunikuje s terminálem za pomoci speciálních protokolů. Mezi ty nejpoužívanější patří:

T=0 – Znakově orientovaná asynchronní polo-duplexní sériová komunikace.

T=1 – Bloková asynchronní polo-duplexní sériová komunikace.

T=CL – Protokol pro bezkontaktní přenos (Contact Less).

T=USB – Protokol USB.

Kartě se zasílají instrukce pomocí tzv. APDU (Application Protocol Data Unit) a naopak karta vrací odpovědi v podobě tzv. ATR řetězce. Jedná se o řetězec s maximální délkou 33 B nastavený výrobcem karty, který by měl být předem registrovaný v operačním systému, aby bylo možné s kartou komunikovat (10).

7.2.1 Bezpečnost platebních terminálů

Z důvodu bezpečnosti obsahovaly již první terminály tzv. Black box, tj. dekódovací zařízení, které ověřovalo PIN. Tento dekodér byl chráněn proti neoprávněnému vniknutí sebedestrukcí, která v případě zásahu do zařízení smazala kódovací program (3). Dnešní kontaktní čipové karty vyžadují zadání kódu PIN. Ověření probíhá buď off-line (tzn., že čip porovná PIN zadaný na klávesnici terminálu s kódem PIN uloženým na čipu), nebo on-line u vydavatele, který je několikanásobně zašifrován a odeslán k ověření do autorizační centrály.

Platební terminály využívají k přenosu dat GSM, GPRS, Bluetooth nebo Wi-Fi sítě. Rostoucí míra bezpečnosti vyžaduje od roku 2002 šifrování pomocí 3DES algoritmu a od roku 2005 povinně RSA šifrování.

7.3 Bezkontaktní platby

Částečné představení bezkontaktní technologie již proběhlo v kapitole 3.3.2.2. Bezkontaktní platby vznikly zejména z důvodu usnadnění nákupů a pro platby o nižší cenové hladině, zpravidla do 25 amerických dolarů (v ČR 500 Kč), u kterých není vyžadováno zadání kódu PIN. Délka celé transakce tak zabere méně času. V případě překročení dané částky je držitel k zadání PIN standardně vyzván. V bankovnictví se pro bezkontaktní platby využívají především tři technologie – bezkontaktní platební karty, RFID nálepky a NFC technologie pro platby mobilním telefonem.

7.3.1 Bezkontaktní platební karty

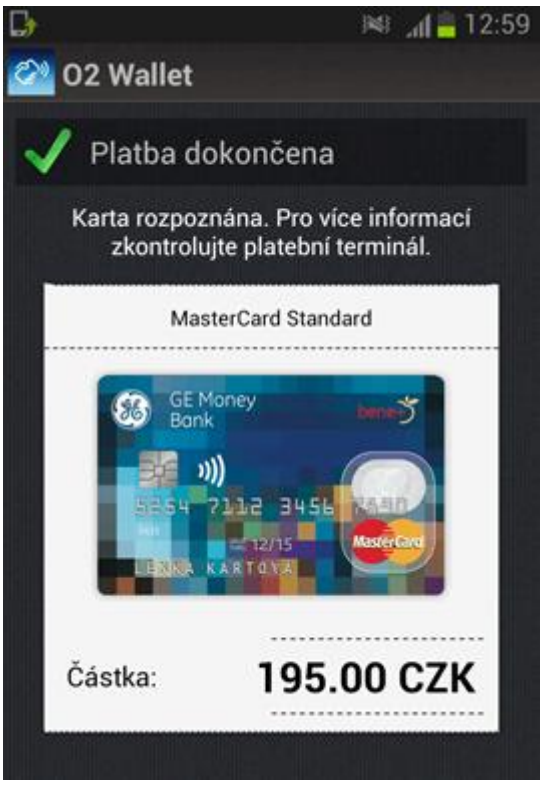
Již roku 2002 zahájila společnost MasterCard testovací provoz technologie zvané PayPass, u níž klient pouze přiloží bezkontaktní čipovou platební kartu do blízkosti terminálu (zhruba na 4cm) podporující bezkontaktní snímání a má zaplaceno. Komunikace mezi čipem a terminálem proběhne ve zlomku vteřiny (1). V ČR se kromě již zmíněné technologie MasterCard PayPass můžeme setkat s obdobnými technologie od společnosti VISA zvanou PayWave nebo expresspay od American Express.

7.3.2 Bezkontaktní RFID nálepky

Bezkontaktní platební karta může dále existovat ve formě tzv. RFID (Radio Frequency Identification) nálepky. Jedná se o samolepku, která obsahuje také čip s anténou a jsou na ní zaznamenány stejné údaje jako na platební kartě. Klient si tuto nálepku může díky menším rozměrům (oproti klasické platební kartě) nalepit např. na peněženku, klíče, zadní stranu telefonu apod. S těmito samolepkami lze platit pouze bezkontaktně, při překročení dané částky je klient vyzván k zadání PIN. Nálepky lze najít pod stejnými názvy jako bezkontaktní platební karty - v praxi nejvíce PayPass a PayWave. Jedná se spíše o řešení dočasné do té doby, dokud nedojde k většímu rozšíření chytrých telefonů s podporou NFC technologie pro bezkontaktní platby mobilem.

7.3.3 Platby mobilem

S velkým rozvojem mobilních telefonů došlo k vytvoření i zcela nového trhu, tzv. m-commerce (Mobile Commerce). To zahrnuje dva způsoby plateb – dálkové platby (prémiové SMS, mobilní platby přes WAP, apod.) a bezkontaktní platby mobilem. Ty slouží především pro placení za zboží a služby u obchodníků (1).



Obrázek 7: Platba mobilem (14)

Bezkontaktní platby pomocí mobilních telefonů využívají čipovou technologii NFC (Near Field Communication), tedy technologii pro bezkontaktní přenos mezi zařízeními. Ta se řídí standardem ISO/IEC schváleným v roce 2003. První nasazení této technologie proběhlo v letech 2007 – 2008, avšak s nepříliš velkým úspěchem. NFC ke své komunikaci používá elektromagnetickou indukci. Nejnovější chytré telefony již technologii NFC podporují, nicméně v současné chvíli je v bankovnictví zapotřebí, mít v telefonu ještě SIM kartu, která tuto technologii též podporuje, a nahradí tak bezkontaktní platební kartu. Na SIM kartu banka nahraje funkce platební karty spojené s účtem klienta. Dále banka poskytne klientovi speciální aplikaci pro jeho mobilní telefon, ve které najde informace o kartě, realizovaných transakcích a správu plateb.

Celá transakce probíhá tak, jako by klient používal bezkontaktní platební kartu. Odpovídající mobilní telefon s NFC podporou pouze přiloží k terminálu podporující NFC platby a transakce bude v případě úspěchu provedena. Do částek 500 Kč nebude vyžadován PIN, při každé vyšší částce bude klient vyzván aplikací k jeho zadání. Z aplikace pak dostane informaci o provedené transakci (14).

Současná implementace tohoto řešení je poněkud komplikovaná. Klient tak musí vlastnit odpovídající telefon schválený provozovatelem služby pro tento druh plateb. Zároveň musí být zákazníkem smluvního operátora banky a v posledním kroku mít nainstalovanou odpovídající aplikaci ve svém telefonu.

S náhradním řešením, které nevyžaduje NFC technologii, přichází společnost MasterCard. Jejich služba nese název MasterCard Mobile a jedná se o aplikaci, kterou si klient nainstaluje do svého chytrého telefonu. Klient v aplikaci zadá údaje o své platební kartě a zvolí si vlastní tzv. mPIN. Ten bude zadávat při každé transakci. Nevýhodou této aplikace je, že vyžaduje připojení k internetu (15).

Obdobnými řešeními se zabývají i jiné společnosti. Google nabízí mobilní peněženku zvanou Google Wallet, kterou lze propojit s platební kartou (zatím pouze pro karty vydané v USA). Google Wallet nepotřebuje připojení k internetu a využívá technologii PayPass. V ČR nabízí obdobnou službu společnost MOPET CZ. Jejich peněženka se jmenuje Mobito, ale zatím nenabízí platby pomocí technologie NFC.

7.3.4 Bezpečnost bezkontaktních plateb

Zabezpečení bezkontaktních platebních karet a bezkontaktních RFID samolepek se snaží výrobci řešit nasazováním bezpečnostních komunikačních kanálů na principech challenge-response (výzva-odpověď). V takovém případě terminál vyšle výzvu, čip odpoví a na základě dohody o použití šifrovacích mechanismů probíhá komunikace. Data tak nejsou vysílána na neautorizované zařízení a jsou šifrována. Využívá se symetrické i asymetrické kryptografie (16).

Při platbách pomocí mobilních telefonů je využívána funkce s názvem Secure element. Tato funkce je využívána pro operace s vyšším stupněm zabezpečení, kam mobilní platby spadají. Secure element je čip nezávislý na NFC technologii. Lze ho provozovat na SIM

kartě, integrovaný přímo v telefonu, nebo externě (např. microSD karta). Slouží jako uložiště veškerých důvěrných informací, které jsou zašifrovány a chráněny bezpečnostním kódem. Zakódovat lze také jen určité části Secure elementu – ty mohou být rozděleny z důvodu oddělení platební karty, věrnostní karty, ID zaměstnanecké karty apod. (17).

7.4 Platby přes internet

Se vznikem internetových stránek v 90. letech 20. století vznikly i nové možnosti nakupování a tím i další způsob využití platebních karet. Rozvoj internetu dovolil použití platebních karet v obchodech bez jejich fyzické návštěvy. V prvopočátcích byly využívány tzv. MO/TO (Mail Order, Telephone Order) transakce. Zákazník zasílal údaje o své platební kartě obchodníkovi za pomoci elektronické pošty, telefonu nebo faxem. S volným přenosem takovýchto informací byly ovšem spojeny problémy odchycení těchto důvěrných informací podvodníky, kteří zisku zcizených dat využívali ve svůj prospěch (1). Bankovní společnosti proto byly nuceny vyvinout technologie, za jejichž použití bude bezpečné platit kartou na internetu. V dnešní době se tak setkáme s celou řadou technologických řešení, které dělají platby kartou po internetu bezpečnými, avšak i zde mohou čekat nástrahy.

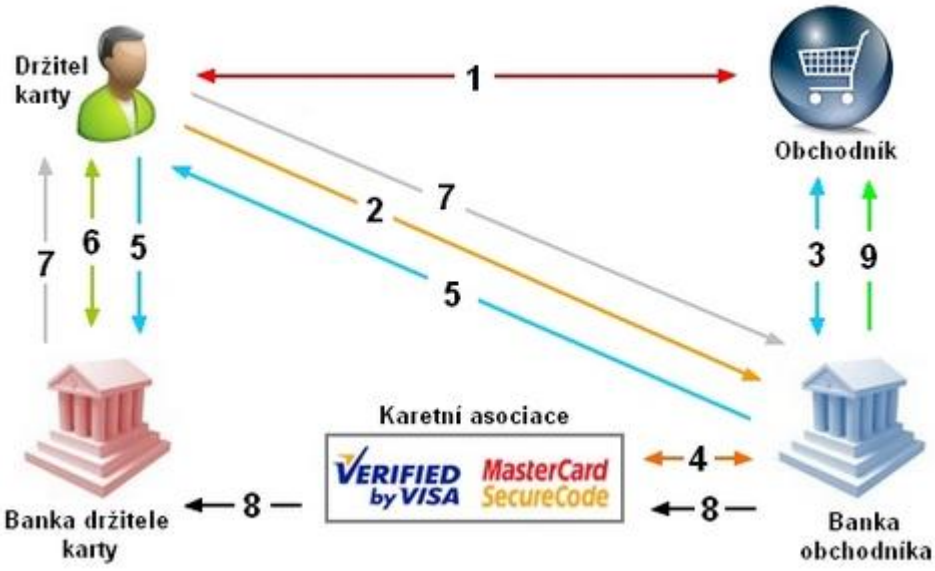
Pro samotný přenos dat v internetu je využíváno protokolů SSL a TLS, jejichž principy byly vysvětleny v kapitole 6.4. Karetní asociace přišly s řešeními nazvanými MasterCard SecureCode a Verified by VISA spolupracující s technologií 3D Secure. Dále se objevily i tzv. virtuální karty nebo technologie využívající zasílání jednorázových čísel pomocí SMS zpráv. Platební kartu lze také spojit s platebním systémem (PayPal, apod.).

Platba kartou na internetu vyžaduje zadání pouze několika údajů. Jedná se o číslo karty, její platnost a CSC kód (viz kapitola 7.4.3). V některých případech může být vyžadováno i jméno držitele karty. V případě metody 3D Secure je transakce doplněna o bezpečnostní SMS kód. Výhodou plateb kartou na internetu je pohodlí a nulové zatížení poplatkem, na rozdíl například od dobírky, za kterou musí zákazník zaplatit v důsledku manipulace dodavatele s hotovostí.

7.4.1 3D Secure

Služby technologie 3D Secure (MasterCard SecureCode a Verified by VISA) byly zavedeny v roce 2001 jako bezpečný způsob platby kartou v internetových obchodech společnostmi MasterCard a VISA. Obě společnosti stanovily pravidla pro odpovědnost vydavatele karty a zúčtovací banky obchodníka (acquier) u internetových transakcí. Využívá-li vydavatel karty technologii 3D Secure a acquier ne, odpovědnost za zneužití karty nese právě acquier (to platí i obráceně). Je tak v nejlepším zájmu bank, aby tuto technologii implementovaly (1).

Využití technologie 3D Secure v praxi je následující:



Obrázek 8: Schéma 3D Secure postupu

1. Zákazník (držitel karty) si vybere zboží v internetovém obchodě.
2. Po potvrzení objednávky je zákazník přesměrován na banku obchodníka, kde zadá platební údaje.
3. Mezi bankou obchodníka a obchodníkem proběhne odsouhlasení objednávky.
4. Banka obchodníka se dotazuje karetní asociace, zda je nebo není držitel zařazen do systému 3D Secure.
5. Banka obchodníka vyšle přes zákazníkův prohlížeč žádost o autentizaci karty do banky držitele.

6. Banka držitele karty požádá držitele karty o zadání jednorázového hesla. Ten ho vyplní a banka držitele karty toto následně potvrdí.
7. Banka držitele karty pošle přes www prohlížeč držitele karty odpověď zpět do banky obchodníka.
8. V případě úspěšné autentizace je internetová platba zpracována jako běžná transakce.
9. Banka obchodníka pošle obchodníkovi informaci o výsledku transakce.

Využitím technologie 3D Secure při internetových platbách se bezpečnost výrazně zvyšuje a pro útočníky je obtížné tuto metodu napadnout, protože by museli překonat vícefaktorovou autorizaci (zařízení připojené k internetu a mobilní telefon klienta, na který je zasílána SMS s bezpečnostním kódem).

7.4.2 Virtuální karty

Některé banky svým klientům poskytují pro platby přes internet tzv. virtuální karty. Nejedná se o fyzickou kartu, ale o důležitá čísla imaginární karty v tištěné podobě. Obsahuje šestnáctimístné číslo karty, platnost a CSC kód. Tyto údaje klient nenosí s sebou jako běžnou kartu, a tak nehrozí, že by někdo tyto údaje získal a zneužil. Virtuální kartou lze platit pouze po internetu a nelze ji používat k výběru hotovosti nebo k platbě u obchodníka.

Umožňuje nastavení důvěryhodných obchodníků tím, že bude vyžadovat pouze přenos realizovaný pomocí SSL šifrování. Klient ale může zvolit i možnost přístupu na internet bez omezení.

7.4.3 CSC kód

CSC (Card Secure Code) je bezpečnostní trojčíslí (někdy čtyřčíslí) uvedené vedle podpisového proužku na zadní straně karty (viz Obrázek 5). Společnost MasterCard označuje toto číslo jako CVC (Card Verification Code) nebo CVC2, společnost VISA pak CVV (Card Verification Value) respektive CVV2. Toto třímístné číslo slouží pro vyšší bezpečnost plateb prováděných po internetu a je doplňujícím údajem u internetové platby.

7.4.4 Platební systémy

Internetové platební systémy slouží jako elektronický platební prostředek, který je napojený na síť internetových obchodů. Účet zřízený v platebním systému je podobný běžnému účtu klienta v bance. Z běžného účtu si klient platební kartou převede peníze na účet platebního systému a z něho pak platí za zboží a služby v e-shopech.

Klient tak nesvěřuje své údaje o kartě přímo obchodníkům, ale pouze internetovému platebnímu systému, přes kterého bude obchodníkovi zaplaceno.

Mezi nejznámější internetový platební systém patří PayPal, který vznikl v roce 1998 v USA pro bezpečné placení na aukčním portálu eBay. V roce 2011 spravoval PayPal 103 miliónů účtů a za rok 2010 dosáhl obratu miliard dolarů, což tvořilo 18% světového trhu internetových plateb (1). Mezi další platební systémy užívané v ČR lze zařadit PaySec, Gopay, PayU aj., které fungují na podobných principech.

8 Analýza rizik a zranitelností

Protože jsou platební karty spojeny s penězi, není divu, že tak lákají zloděje a jiné útočníky, kteří se zabývají nelegálními činnostmi krádeží karet, údajů o nich a případně výrobou jejich padělků, jež mohou poté využít ve svůj prospěch. Útoky na platební karty se vyskytovaly již od dob jejich prvopočátků. Jednalo se o různá fyzická zcizení embosovaných karet, které v době svého rozvoje nevyužívaly kód PIN pro ověření transakce. Útočníkovi tak postačilo touto kartou zaplatit u obchodníka pomocí imprinteru a v nejhorším případě napodobit podpis původního držitele. Zneužití karet tehdy podporovala i absence ochranných prvků. S odcizenými kartami se také obchodovalo na černém trhu (1). S větším průnikem ochranných prvků a nových bezpečnostních technologií popsaných v předchozích kapitolách do oblasti platebních karet se začaly zdokonalovat i způsoby, jakými pachatelé postupují při zneužití platebních karet. Obecně lze tedy říci, že snahou pachatelů je získání údajů uložených na kartě za pomoci technických zařízení, případně zneužití nedostatků použitých technologií, skrze které je přenos a uložení dat prováděno. Dalším možným způsobem útoku je vylákat údaje z držitelů za pomoci sociálního inženýrství. V následujících kapitolách budou

představeny známé i méně známé druhy útoků, jejich charakteristické rysy a postupy. Dále budou navrženy způsoby, jakými se lze proti těmto útokům bránit nebo za jejíchž pomoci lze riziko zneužití snížit.

8.1 Typy útoků

8.1.1 Skimming

Skimmingem lze nazývat činnost výroby a přípravy zařízení, které pachatelé používají ke zneužití platebních karet. Taková zařízení pak nejčastěji montují na bankomaty a podobné výdejní nebo parkovací automaty, výjimkou nejsou ovšem ani platební terminály. Cílem této trestné činnosti je nezákonné odcizení důvěrných dat klienta z platební karty a v konečné fázi odčerpání jeho finančních prostředků. To může proběhnout díky vyrobenému padělku karty nebo použitím údajů z karty k platbám na internetu. Odčerpání prostředků klienta mohou pachatelé realizovat ihned po zcizení dat nebo i po delším časovém úseku (18). Pachatelé využívají nedokonalosti magnetického proužku a to zejména jeho snadnou duplikaci (viz kapitola 3.3.1). V některých zemích totiž ještě existují terminály nebo bankomaty, které nepodporují čipovou technologii, a právě zde lze padělky karet využít. Z tohoto důvodu se vyskytují hybridní karty, které obsahují jak novou čipovou technologii, tak zastaralý magnetický proužek (viz kapitola 3.3.3). Skimmingem se zabývají většinou specializované organizované skupiny pachatelů. Nejčastěji pak z Asie, Západní Evropy a v poslední době i ze zemí bývalého SSSR (1).

8.1.2 Phishing

Phishing je typ útoku sociálního inženýrství, při kterém se pachatelé vydávají za banku klienta s prosbou o potvrzení údajů. Může mít ale i formu informace o nepovedené platbě, výzvě k aktualizaci bezpečnostních údajů nebo jako průzkum klientské spokojenosti. Potvrzení znamená vylákání těchto údajů na základě klientovy důvěry, ať již se jedná o telefonickou, e-mailovou, příp. jinou komunikaci. Cílem těchto útoků je získání důvěrných informací o platební kartě, případně i její kód PIN a jejich následné zneužití. Tyto útoky mohou být náhodné nebo cílené na danou skupinu poškozených (v tomto případě na držitele platebních karet). Jejich znakem může být výzva napsaná v cizím jazyce nebo překlepy a nedostatky v překladu do daného jazyka.

8.1.3 Pharming

Pharming je nebezpečnější formou phishingu. Pharming spočívá v napadení DNS záznamů v počítači klienta, a ten je pak při požadavku o přístup na webové stránky banky přesměrován na stránky útočníků. Ty se však tváří jako původní web banky a na první pohled tak klient nerozezná rozdíl.

8.1.4 Ostatní typy útoků

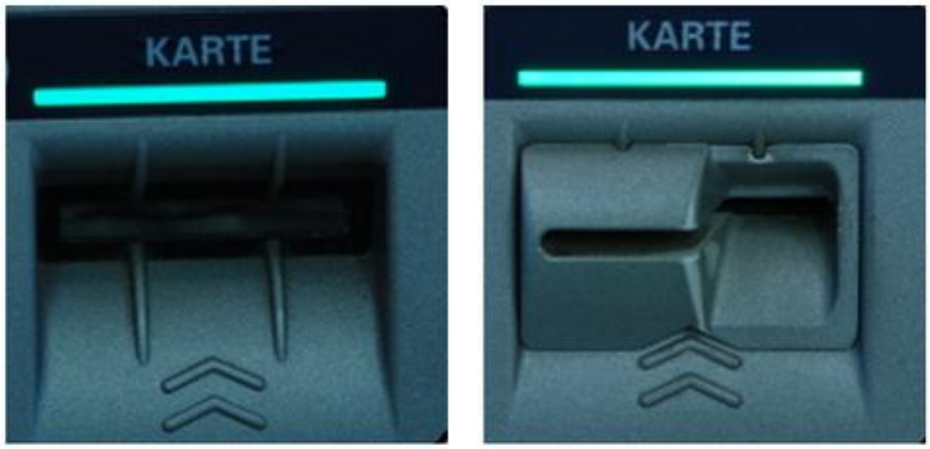
Jako další příklady útoků po síti lze uvést spoofing, jehož charakteristickým rysem je neoprávněné získávání dat přímo z počítačové sítě. Spoofingu existuje několik druhů, např. útoky man-in-the-middle nebo man-in-the-browser. V těch, jak jejich název napovídá, dochází k ovládnutí komunikace klienta mezi serverem nebo přímo internetového prohlížeče klienta, kde útočník získává všechna data vyslaná uživatelem z jeho internetového prohlížeče. Tyto útoky jsou většinou realizovány po napadení klientova počítače za pomoci různých virů, červů a podobných škodlivých kódů.

Mezi atypické útoky na platební karty lze zařadit napadení organizace, zabývající se zpracováním platebních transakcí na určitém spravovaném území. Pachatelé napadnou záznamy organizace, a ihned se tak dostanou k obrovskému množství zaznamenaných transakcí, které klienti provedli a nezáleží při tom, jaký způsob transakce byl zvolen, ať již se jednalo o použití karty v bankomatu nebo přes platební terminál u obchodníka. Odcizená data mohou pachatelé zneužít k neoprávněným transakcím, případně výrobě padělků karet. Tento nebezpečný typ útoku byl zaznamenán v roce 2009 ve Španělsku (18).

8.2 Zneužití bankomatů

8.2.1 Skimming bankomatů

Nejrozšířenějším druhem skimmingu je získávání dat z platební karty použité v bankomatu. Pachatelé v tomto případě nasazují na bankomat zařízení pro skimmování dat. Jeden nástavec je nasazen na vstupní zdířku čtečky karet a obsahuje elektroniku sloužící pro zaznamenávání dat z magnetického proužku. Další nástavec pak často obsahuje mobilní telefon, nebo videokameru, která snímá zadávaný kód PIN, a je nejčastěji umísťován na horní lištu bankomatu nebo např. do přihrádky s reklamními letáky v blízkosti automatu. Pokud je skimmovací zařízení vybaveno telefonem, mohou pachatelé zcizená data získávat pomocí bezdrátových sítí (např. Wi-Fi, Bluetooth). V opačném případě ponechají zařízení po vymezenou dobu na bankomatu a poté ho musí ručně odebrat a data získat drátovým spojením (18).



Obrázek 9: Bankomatová čtečka bez a se skimmovacím zařízením

Nic netušící klient si na takto napadeném bankomatu vybere peníze, současně jsou ale jeho údaje z karty zkopírovány. Obranou proti tomuto typu útoku je, aby klient před použitím pečlivě zkontroloval, zda bankomat nenese známky poškození, či jiných nápadných úprav. V každém případě je doporučeno zakrýt klávesnici při zadávání kódu PIN. Ovšem ani to není stoprocentní (viz Obrázek 10[4]), protože útočníci umísťují na

[4] Zdroj: http://www.puterea.ro/img/w560/http://www.puterea.ro/images/uploads/stiri/63199/card_skimming_europol.europa.eu.jpg

klávesnice svoje PIN Pady, tj. další klávesnici, za jejíž pomoci překryjí klávesnici originální. Tím je zachována funkčnost původní klávesnice, zatímco PIN Pad pachatelů zaznamenává veškerá data zadávaná držitelem platební karty při operacích u bankomatu.

Obrázek 10: Původní klávesnice překrytá PIN Padem pachatelů

Proti použití skimmovacích nástavců jsou na bankomaty instalovány speciální zelené bezpečnostní nástavce. Ovšem i to pachatele neodradilo, protože jejich nejnovější zařízení vypadají téměř shodně. Poslední případ skimmingu v ČR byl zaznamenán na bankomatu České spořitelny v Brně dne 2. února 2013, kdy se pachatelům podařilo v Kalifornii vybrat dvacet tisíc korun (19). Dalším možným způsobem obrany je pak mít s bankou sjednané pojištění proti zneužití karty.

8.2.2 Libanonská smyčka

Libanonská smyčka je nejstarším typem útoku na bankomaty. Zdířka pro vsunutí karty je překryta speciálním rámečkem pachatelů, který uvnitř obsahuje zadržovací pásku. Klient tedy do takto napadeného bankomatu vloží kartu, ta se ovšem přilepí k pásce. Klient tak nemá kartu ani své peníze. V tu chvíli přistupují pachatelé ve snaze pomoci, vždy ale pošlou klienta na reklamaci do banky (20). Po jeho odchodu odstraní rámeček a kartu použijí na základě znalosti kódu PIN odpozorovaného např. dalekohledem.

Obrázek 11: Libanonská smyčka (20)

Modifikace podobného útoku (pojmenovaného Hradecká lišta) se vyskytla i v roce 2009 a 2010 v ČR, kdy za pomoci lišty a lepicí pásky pachatelé zakryli otvor pro výdej hotovosti. Klient po provedení transakce získá svou kartu zpět, ale hotovost nikoli, protože ta je uvnitř přilepena k pásce. V případě odchodu klienta od bankomatu pachatelé lištu odstraní a peníze odeberou.

Doporučenou obranou při tomto typu útoků je zakrývat si zadávaný PIN a ten nikomu následně nesdělovat. V případě podobného zaseknutí karty nebo hotovosti by klient neměl bankomat opouštět a neprodleně telefonicky kontaktovat linku banky nebo policii.

8.3 Zneužití platebních terminálů

Využití skimmingu je možné i u platebních terminálů. Celý útok probíhá obdobným způsobem, jako bylo popsáno v kapitole (viz kapitola 8.2.1). Útočníci tak osazují terminály za své, vybavené skimmovacími zařízeními, umožňující klientům běžné platby kartou, ale zároveň zaznamenávání údajů z magnetických proužků a kódů PIN. Pachatelé se většinou vydávají za servisní techniky a v obchodním místě nahradí původní terminál napadeným, který po určitém časovém období opět odeberou a získaná data zneužijí. Tento typ útoků není příliš častý a v ČR se dosud neobjevil (18).

Jedinou obranou proti tomuto útoku je zvážení celého přístroje a porovnání s váhou udávanou výrobcem zařízení. Skimmovací zařízení pak lze odhalit po rozebrání terminálu. Tento typ útoků je tedy jen velmi těžko zpozorovatelný a obrana proti němu není jednoduchá ani praktická.

8.4 Zneužití bezkontaktní technologie

Bezpečnostní mechanismy bezkontaktních čipových karet a RFID samolepek, popisované v kapitole 7.3.4, umožňují však až čipy vyšší cenové kategorie. Nižší řady RFID čipů mají navíc značná omezení ve složitosti procesoru a jeho paměti pro uložení silných šifrovacích klíčů. Nebezpečím je právě ona bezkontaktní technologie – bezkontaktní čip totiž komunikuje pouze tehdy, pokud je ke komunikaci vyzván jakýmkoliv snímačem. Za použití vhodně citlivého a výkonného snímače lze přečíst data z bezkontaktní karty až na vzdálenost deseti metrů (16). Takový snímač pak nesmí mít příliš silný signál, aby nedošlo ke spálení obvodů čipu v závislosti na silném napájecím napětí. Útočník může tímto způsobem oskenovat údaje z platební karty, aniž by o tom poškozený věděl, a ty pak použít např. pro platbu přes internet.

Takovým problémům lze předcházet pomocí speciálně odstíněných pouzder pro platební karty, znemožňující její nechtěnou komunikaci. Ty jsou vyrobeny ze speciálních materiálů a tím zabrání vstupu elektromagnetického napětí k čipu karty. Pokud je karta zasunuta v pouzdru je nemožné s ní navázat komunikaci. To však platí pouze do doby, než klient kartu použije pro platbu u obchodníka, kde ji musí z pouzdra vyjmout.

Dalším způsobem, jak zcizit data uložená na platební kartě, lze pomocí chytrého telefonu. Na internetu se objevila aplikace, která pomocí technologie NFC na chytrém telefonu s operačním systémem Android dokáže přečíst data z platební karty. Konkrétně byl pokus dokázán na kartě MasterCard PayPass (21).

V oblasti plateb pomocí mobilních telefonů zatím nebylo nijak zneužito údajů o platebních kartách. Je to částečně tím, že celá technologie je stále ve vývoji a ani její rozšíření není příliš velké. Rizikem však může být ztráta mobilního telefonu a tím pádem i ztráta platební karty, čehož by potencionální útočník mohl zneužít k zaplacení transakcí nevyžadujících kód PIN, a způsobit tak držiteli škodu. Vzhledem ke ztrátě telefonu pak situaci komplikuje i nemožnost okamžitého zavolání na linku banky s požadavkem o blokaci platebních funkcí.

8.5 Zneužití platební karty na internetu

Jak již bylo vysvětleno v kapitole 7.4, k platbě platební kartou po internetu stačí znát pár údajů o kartě, které se na ní nacházejí i viditelně. V konkrétním případě ses tedy jedná o číslo karty, datum platnosti, třímístný CSC kód, ve výjimečných situacích pak i jméno držitele karty. V případě získání těchto údajů pachatelem může dojít k použití karty pro platbu na internetu bez vědomí jejího majitele. Karta ovšem musí být bankou aktivována pro platby přes internet.

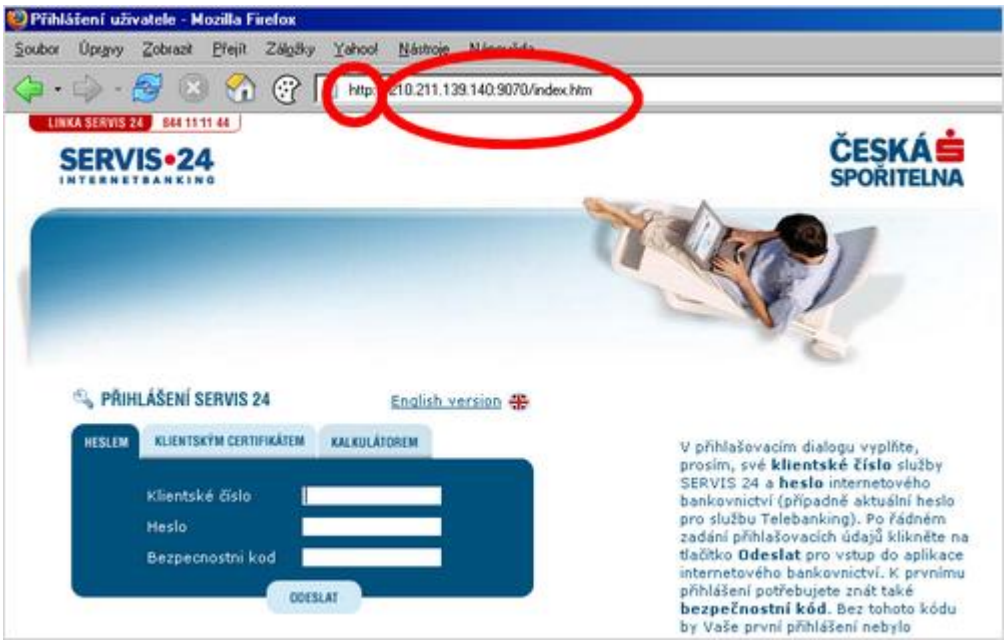
Z předchozích kapitol již víme, že údaje z platební karty lze zkopírovat pomocí skimmovacích zařízení. V případě přenášení údajů o platební kartě po internetu přes nešifrované spojení bez použití protokolu HTTPS (realizovaného za pomoci TSL nebo SSL protokolů) lze snadno tyto informace odposlechnout pomocí speciálních programů.

Rozšířenou formou získávání údajů o platební kartě jsou phishingové e-maily a falešná pharmingová přesměrování webových stránek banky na webové stránky útočníků. Ty se téměř shodují s oficiálními stránkami banky a vyžadují zadání stejných údajů, které pro ověřování klient běžně zadává. Zadáním však klient dané údaje odešle přímo do rukou pachatelů a ti je mohou ihned případně v dohledné době zneužít. Dalším možným útokem je rozesílání e-mailů s logem banky, tvářící se jakoby přišel od klientovy skutečné banky. E-mail je většinou propojen odkazem na již zmíněný falešný web útočníků a má navodit pocit formální komunikace klienta s bankou.

Obranou proti phishingu a pharmingu je důkladně kontrolovat zdroj dotazu a citlivé údaje o platební kartě po internetu v žádném případě nikomu v podobné komunikaci nesdělovat. V případě internetových stránek dbát na použití HTTPS protokolu a kontrolovat doménu a certifikát serveru.

U telefonických, e-mailových a jiných forem komunikace ověřovat, zda klient opravdu komunikuje se svojí bankou. Samozřejmostí by mělo být používání firewallu, antivirového programu a využívání pravidelných aktualizací všech důležitých software instalovaných v počítači.

Některé banky nabízejí možnost dočasné aktivace platby kartou po internetu. Klient si může nastavit časové rozmezí, kdy bude karta aktivována k tomuto druhu platby, příp. omezí i placenou částku. Tato funkce však může být bankou zpoplatněna. Pachateli se ale výrazně sníží možnost zneužití i přes to, že údaje o kartě zná.



Obrázek 12: Podvodné přesměrování klientů banky na web pachatelů (22)

Poslední útoky na držitele platebních karet v ČR byly zaznamenány v roce 2008 u klientů České spořitelny, kdy se jednalo o podvodné přesměrování www stránek banky na falešné stránky útočníků. Další formou pak byly podvodné e-maily rozesílané klientům do jejich e-mailových schránek, naposledy pak v únoru roku 2013 (22).

9 Vyhodnocení provedené analýzy

Na základě provedení systémové analýzy rizik a zranitelností, byla provedena vyhodnocení uspořádaná do výsledného tabulkového souhrnu. V první části vyhodnocení byla vytvořena komparace různých druhů záznamů dat na platebních kartách a byly porovnány jejich jednotlivé vlastnosti. Následuje výčet předností a slabin použití platebních karet v bankomatech, platebních terminálech, platbách přes internet

a bezkontaktních plateb se zaměřením na možné hrozby, které představují konkrétní typy útoků. V každé části jsou shrnuty jednotlivé útoky a navrhovaná opatření, kterými se proti nim lze bránit. V závěru souhrnu jsou vyjmenovány hrozby spojené s držením platební karty a manipulace s ní a je navrženo předcházení rizikům.

9.1 Komparace druhů záznamu dat

V této části byly zkoumány prvky analýzy pro jednotlivé druhy záznamu dat na platební kartě. Hodnoceny jsou dva, dnes výhradně používané, způsoby záznamu dat – magnetický proužek a mikroprocesorový čip. Do porovnání nejsou zahrnuty paměťové čipové karty, protože jejich využití v oblasti platebních karet není typické, ani laserový druh záznamu, který se v této oblasti vůbec neuplatnil. Tabulky obsahují tři pozorované vlastnosti – silné stránky, slabé stránky a hrozby daných technologií.

Magnetický proužek	
Silné stránky	**Slabé stránky**
Technicky jednoduché	Omezená kapacita záznamu
Finančně málo náročné	Snadná duplikace
Jednoduché na používání	Zastaralé řešení
Zašifrované informace	Umožňuje pouze čtení
Ověřování pomocí PIN	Nedisponuje aktivní logikou
	Možnost vytvoření kopie

Tabulka 2: Vlastnosti magnetického proužku

Mikroprocesorový čip	
Silné stránky	**Slabé stránky**
Ochrana zaznamenaných údajů	Finančně náročnější
Disponuje aktivní logikou	Nutnost držitele pamatovat si kód PIN
Povolení přístupu pouze subjektům s přístupovými klíči	Možnost zkoumání struktury čipu mikroskopem
Aplikace v čipu umožňující odhalení pokusu o neoprávněnou modifikaci dat	
Obsahuje kryptokontroler pro výpočty klíčů RSA	
Možnost uložení různých dat do paměti (aplikace, PIN, biometrické prvky, atd.)	
Použití čipu pro bankovní i nebankovní účely	
Možnost online ověřování	
Velmi složité vytvoření kopie čipu	
Ověřování pomocí PIN	

Tabulka 3: Vlastnosti mikroprocesorového čipu

Z vytvořených tabulek jasně vyplývá, že čipová technologie je o mnoho bezpečnější než zápis dat na magnetický proužek. Čipy jsou tak díky svým přednostem právoplatnými nástupci zastaralé technologie a k jejich rozšíření by mělo dojít co nejdříve, aby se snížilo riziko zneužívání záznamu dat na magnetickém proužku.

9.2 Vyhodnocení bezpečnosti použití platební karty

Vlastnosti jednotlivých způsobů použití platební karty, popsané v kapitole 7, byly shrnuty v následujících tabulkách. Srovnávána je stránka komfortu držitele při používání platební karty a ochranné prvky využívané při jejím použití. Bezpečnost je úměrná míře komfortu, a tak může při manipulaci s kartou docházet k oslabení zabezpečení vlivem preferováním pohodlí držitele. Porovnávány byly silné a slabé stránky jednotlivých způsobů použití. Dále byly shrnuty útoky na platební karty včetně navrhovaných opatření proti nim. Útoky se většinou odvíjí od slabých stránek.

V případě dostatečný dat ze statistik jsou tabulky s útoky doplněny o informace výskytu zjištěních trestných činů provedených na území České republiky a to textovou formou nebo v podobě obrázkové přílohy formou grafů.

9.2.1 Bankomaty

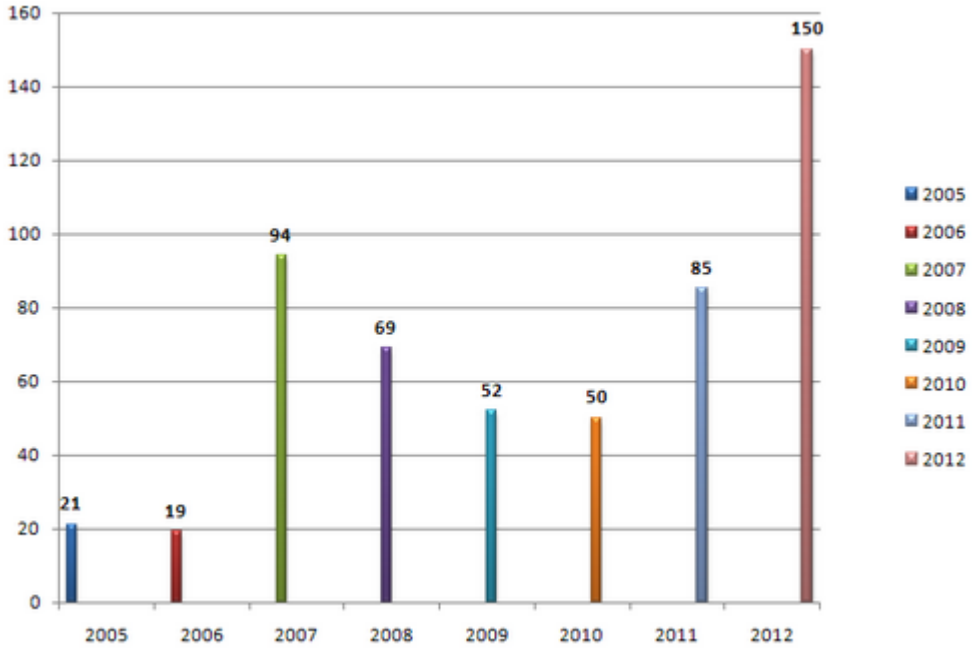
Použití platební karty v bankomatu	
Silné stránky	**Slabé stránky**
Víceúčelové funkce (vklady, výběry, zobrazení zůstatku, změna PIN, tisk poukázek, atd.)	Starší bankomaty v provozu nemusí být vybaveny nejmodernějšími čidly
Ověřování pomocí kódu PIN	Umístění některých bankomatů nahrává útočníkům
Online ověřování	
Rychlost ověřování	
Šifrování komunikace	
Zabudované PC	
Alarmová čidla	
Antiskimmovací zařízení	
Kamera	
Software pro rozpoznávání nestandardního chování	

Tabulka 4: Vlastnosti bankomatů

Z tabulky vyplývá, že bankomaty disponují velice silným zabezpečením a to hlavně díky zabudovanému PC, pomocí kterého je možné propojit více bezpečnostních prvků ve velice sofistikovaný celek. Ne každý bankomat má však stejné technické vybavení, a tak lze nalézt i stinné stránky, které mohou vést k útokům na ně vedených.

Útoky na bankomaty a obrana proti nim	
Útok	**Navrhovaná obrana**
Skimming bankomatů	Vizuální kontrola bankomatu
Libanonská smyčka	Udržení kódu PIN v tajnosti
Hradecká lišta	V případě problému zavolat na linku banky, příp. policii
	Nenechat se ovlivňovat cizí osobou při operaci s kartou u bankomatu
	Neuskutečňovat transakci v případě podezření
	Kontrolovat výpisy z účtu
	Mít sjednané pojištění proti zneužití karty

Tabulka 5: Útoky na bankomaty a obrana proti nim



Obrázek 13: Přehled skimmingu na území ČR v období let 2005 - 2012 (28)

Nejčastějším typem útoků na bankomaty v České republice je skimming. Ostatní útoky se vyskytly pouze v několika málo případech. Hlavní roli v obraně proti těmto útokům hraje dodržování zmíněných pravidel držitelem karty, ovšem vybavení pachatelů je mnohdy na velmi vysoké úrovni a ani tyto obranná opatření pak nemusí být stoprocentní.

V případě nečekaného zneužití platební karty a zároveň nejistoty držitele v dodržení všech bezpečnostních opatření může být řešením sjednané pojištění proti zneužití platební karty, které by mělo pokrýt zjištěné škody.

9.2.2 Platební terminály

Použití platební karty v POS terminálu	
Silné stránky	**Slabé stránky**
Zjednodušení plateb u obchodníků	Možnost odpozorování kódu PIN cizí osobou
Víceúčelové funkce (Cash Back, Top Up, atd.)	Možnost zaznamenání údajů o kartě nepoctivým obchodníkem
Přijímání kontaktních i bezkontaktních čipových karet	Delší doba trvání online ověření
Bonusy za platby kartou	Offline ověřování karet nahrává útočníkům
Pohodlí při bezkontaktních platbách	
Rychlost bezkontaktních plateb	
Online ověřování karty pro vyšší bezpečnost	
Offline ověřování pro rychlejší průběh	
Ověřování pomocí kódu PIN	
Blackbox	
Šifrovaná komunikace	

Tabulka 6: Vlastnosti platebních terminálů

Hlavní výhodou platebních terminálů je usnadnění plateb u obchodníků. Umožňují i vedení více aplikací než jsou platební funkce, zejména pak věrnostní programy pro sbírání bonusových bodů k obchodním produktům.

Útoky na POS terminály a obrana proti nim	
Útok	**Navrhovaná obrana**
Skimming terminálů	Zvážit zařízení
	Rozebrání terminálu

Tabulka 7: Útoky na platební terminály

Používání platebních terminálů je na vyšší úrovni zabezpečení. I když skimming terminálů existuje, je to útok velmi složitý na provedení, a proto se příliš nevyskytuje. To dokládá i fakt, že v České republice nebyl tento typ útoku nikdy zaznamenán.

9.2.3 Platby přes internet

Platby přes internet	
Silné stránky	**Slabé stránky**
Komfortní platba téměř odkudkoliv	Nešifrované spojení
Rychlost vybraných plateb	Servery bez certifikátu
Využití CSC kódů	Neustálé povolení karty pro platby přes internet
Metoda 3D Secure	Nepoctiví obchodníci
Virtuální platební karty	
Platební systémy	
Dočasná aktivace karty pro internetové platby	
Využití zabezpečených protokolů a využití certifikátů	

Tabulka 8: Vlastnosti plateb přes internet

Platby přes internet představují velice komfortní nástroj platby. Na druhé straně představují veliké riziko, které z velké části ovlivňuje držitel karty svým zacházením s kartou. Velkým problémem je vyobrazení údajů potřebných pro platbu přímo na platební kartě. Tu by tak měl její držitel pečlivě střežit a znemožnit, aby se nedostala z jeho dohledu. Za použití požadovaných zabezpečení (jakým je např. metoda 3D Secure) jsou platby přes internet bezpečné a pro útočníky těžko překonatelné.

Útoky na platby po internetu a obrana proti nim	
Útok	**Navrhovaná obrana**
Odposlech dat na síti	Antivirový program
Phishing	Pravidelné aktualizace instalovaného software
Pharming	Použití zabezpečených protokolů
Spoofing	Ověřování certifikátů serverů
	Kontrolovat adresu serveru
	Ověřovat komunikující protistranu

Tabulka 9: Útoky na platby kartou po internetu

Způsobů, jak z držitelů vylákat údaje o platební kartě existuje hned několik a jsou velmi nebezpečné. Vše ale závisí na chování držitele karty a na tom, jakým způsobem podporuje svoji bezpečnost. Tu lze zvýšit za pomoci různých antivirových programů a včasných aktualizací aplikací instalovaných v počítači. Důležité je používat zdravý rozum a pečlivě kontrolovat s kým je spojení navázáno, případně důkladně ověřovat a přesvědčit se o důvěryhodnosti komunikující protistrany.

9.2.4 Bezkontaktní technologie

Bezkontaktní platební karty	
Silné stránky	**Slabé stránky**
Komfort placení	Absence ověřování kódu PIN u transakcí do cca 500 Kč nahrává útočníkům
Rychlost transakce	Pasivní bezkontaktní technologie
Nevyžadují PIN do částek cca 500 Kč	Offline ověřování karty neodhalí odcizenou kartu
Lze nastavit limit, nad který proběhne ověřování pomocí kódu PIN	Vynechávání některých kroků ověřování karty v rámci úspory času
Ověřování pomocí PIN nad daný limit	
Šifrovaná komunikace	
Obsahují i kontaktní čip	
Challenge-response komunikace	

Tabulka 10: Vlastnosti bezkontaktních platebních karet

Bezkontaktní RFID nálepky	
Silné stránky	**Slabé stránky**
Lze umístit téměř na cokoliv	Samolepku lze použít pouze pro bezkontaktní platby u obchodníků
Malé rozměry	Náchylnější na ztrátu a odlepení
Komfort placení	Nedokonalost nižších řad RFID čipů
Rychlost transakce	Slabé stránky bezkontaktní platební karty
Nevyžadují PIN do částek cca 500 Kč	
Lze nastavit limit, nad který proběhne ověřování pomocí kódu PIN	
Ověřování pomocí PIN nad daný limit	
Šifrovaná komunikace	
Challenge-response komunikace	

Tabulka 11: Vlastnosti RFID bezkontaktních samolepek

Bezkontaktní platby mobilem s podporou NFC	
Silné stránky	**Slabé stránky**
Pohodlné řešení	Použití pouze pro bezkontaktní platby u obchodníků
Vyšší bezpečnost díky Secure element	Nároky na vlastnictví chytrého telefonu s podporou NFC
Přehled transakcí v aplikaci	Nutnost instalace speciální aplikace
Možnost zadat kód PIN bezpečně před platbou	Být klientem u smluvního telefonního operátora banky
Komfort placení	Slabé stránky bezkontaktní platební karty
Rychlost transakce	
Nevyžadují PIN do částek cca 500 Kč	
Lze nastavit limit, nad který proběhne ověřování pomocí kódu PIN	
Ověřování pomocí PIN nad daný limit	
Šifrovaná komunikace	

Tabulka 12: Vlatnosti plateb mobilem s podporou NFC

Bezkontaktní použití platební karty je v současnosti velmi oblíbené a to především pro její jednoduchost a rychlé odbavení při platbách o nižší cenové hladině. Jedná se novou technologii, jejíž první provoz byl spuštěn v roce 2012. Platby mobilem s podporou NFC technologie byly spuštěny v České republice začátkem roku 2013 a díky svému komfortu při placení začínají být také velice oblíbené.

Útoky na bezkontaktní technologii a obrana proti nim	
Útok	**Navrhovaná obrana**
Odposlech dat uložených na čipu karty	Odstíněné pouzdro pro kartu
Přečtení dat z čipu karty za pomoci aplikace na chytrém telefonu s podporou NFC	
Zneužití odcizené karty, RFID nálepky nebo chytrého telefonu pro platby do částek cca 500 Kč	

Tabulka 13: Útoky na bezkontaktní technologii

Z pohledu bezpečnosti však bezkontaktní platby nepřinášejí příliš nových prvků. Neexistuje tak ještě ani rozsáhlejší výčet realizovaných útoků. Specialisté na tuto oblast pouze demonstrovali jejich možné zneužití. Klienti využívající bezkontaktní platby tak preferují pohodlné placení oproti vyššímu bezpečí kontaktních čipových karet, u kterých nemůže dojít k odposlechu dat bez vědomí držitele. Celá technologie je ještě stále novinkou a případná zneužití budou záviset na pravděpodobnosti potencionálních útoků.

9.3 Vyhodnocení bezpečnosti držení platební karty

Rizika spojená s držením platební karty	
Hrozba	**Řízení rizik**
Ztráta platební karty	Neustále kontrolovat vlastnictví platební karty. V případě ztráty neprodleně zavolat vydavatelské bance s požadavkem na blokaci karty.
Výroba padělku odcizené karty	Ochranné prvky na platební kartě (hologram, mikrotisk, podpisový proužek, UV prvky).
Doručení nové platební karty klientovi	Oddělení zásilky platební karty a kódu PIN. Aktivace nové karty přes SMS či internetové bankovnictví. Novou kartu po převzetí podepsat.
Neoprávněná platba s odcizenou kartou	U kontaktní čipové karty je vyžadován kód PIN, příp. podpis. Obchodník může též požádat o identifikační doklad. Určitá transakce v pořadí provedená kartou musí být ověřená online u vydavatele karty.
Nepoctiví obchodníci	Nikdy nespouštět kartu z dohledu, v případě nepřenosných terminálů u obchodníků dojít k terminálu s obsluhou.
Kód PIN	Nikomu kód PIN nesdělovat, ani ho nemít poznačený v blízkosti platební karty. Vhodné PIN měnit.
Manipulace s platební kartou	Držitel karty má nárok na diskrétní zónu pro bezpečnou manipulaci s kartou.
Platby přes internet	Dbát zvýšených požadavků na zabezpečenou síť. Využívat metody 3D Secure.
Kontroly výpisů	Prověřovat provedené transakce. V případě nesrovnalostí kontaktovat vydavatelskou banku.

Tabulka 14: Rizika spojená s držením platební karty

Z tabulky plyne, že s používáním platební karty jsou spojeny nemalé povinnosti jejího držitele. Zvýšení míry zabezpečení tak přímo ovlivňuje právě on. Dodržování těchto základních pravidel vede k zamezení zneužití platební karty, případně snižuje riziko zneužití platební karty na minimum. Záleží tak hlavně na držiteli karty, jak bere bezpečnost používání platební karty vážně a upřednostňuje ji před pohodlím, protože bezpečné použití je vždy na úkor komfortu prováděných plateb.

10 Budoucnost platebních karet

Počty vydaných bankovních karet rostou každým rokem a stejně tak roste i jejich obliba. Do budoucna tak lze počítat s jejich dalším rozvojem a s tím spojenými novými technologiemi, které budou jejich zabezpečení zvyšovat.

Zajímavým případem je ověřování držitele pomocí kódu PIN, který existuje již od dob platebních šeků. Se svou jednoduchostí ho používáme dodnes, protože se jedná jak o metodu relativně bezpečnou, tak zároveň jednoduchou a pro klienty pochopitelnou. PIN kód se o svoji budoucnost jistě bát nemusí, avšak v následujících kapitolách bude představeno, že existují i jeho modernější formy.

Bezkontaktní placení je už teď velmi oblíbené a na oblíbenosti nabírají i platby za pomocí technologie NFC mobilních telefonů. Ty se budou rozšiřovat s větší penetrací chytrých telefonů mezi klienty a technologie mobilního placení ještě projde vývojem. Zajímavá je i myšlenka využití biometrie v oblasti platebních karet. Celá věc je ještě v začátcích a bude především záležet na ochotě klientů a jejich vůli svěřit své otisky prstů bankovním společnostem. Nicméně vzhledem k tomu, že nové občanské průkazy (eID) a pasy již využívají mikročipovou technologii, není tím pádem vyloučená ani možnost, že bychom se v budoucnu nedočkali propojení bankovního účtu klienta nebo funkcí platební karty právě s těmito osobními doklady.

Platební karty, takové jaké je dnes známe, ale jistě hned tak nevymizí do podoby mobilních telefonů a bezkontaktních samolepek. I v klientele totiž najdeme určitou část zákazníků, většinou velice bonitních, pro které jsou fyzické zlaté karty formou prestiže a jsou s nimi spojeny i nemalé výhody.

V následujících kapitolách se podíváme na několik technologických řešení, které jsou například ve fázi testování nebo nejsou prozatím tolik rozšířené, ale mají jistý potenciál stát se využívané v oblasti platebních karet a přispět ke zvýšení jejich zabezpečení.

10.1 MasterCard Display Card

Společnost MasterCard v roce 2010 představila novou generaci Display Cards debetních platebních karet obsahující displej a dotyková tlačítka (viz Obrázek 14[5]). První bankou v Evropě, nabízející tyto karty se stala turecká TBA banka. Displej je schopný zobrazovat písmena i číslice a držitel se z něho tak může dozvědět zůstatek na účtu, limit plateb nebo generovat dynamická hesla. Do budoucna by karty měly umožnit zobrazení i stavu věrnostních bodů, seznam posledních transakcí, aktuální částku transakce a mnoho dalšího.

Platební karta Display Card odpovídá normě ISO a je schválená i společností CSI. To znamená, že splňuje vysoké nároky na bezpečnost i na používání karty po celou dobu její platnosti.

Display Cards disponují také tzv. OTP (One Time Password) generátorem tedy generátorem jednorázových hesel. Při každé internetové transakci si tak držitel může vygenerovat jednorázové heslo a to zadat do údajů o platbě (23). Zamezí se tím tak nechtěnému zneužití karty na internetu. OTP generátor lze použít např. i pro přihlašování do internetového bankovnictví.

Obrázek 14: MasterCard Display Card

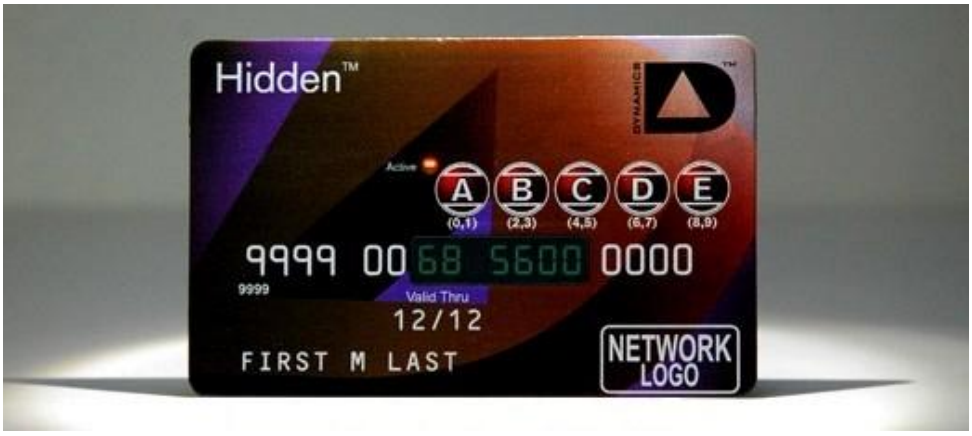
[5] Zdroj: http://www.nidsecurity.com/media/RSA2012/Images/526.jpg

10.2 Karta s dotykovou plochou

Společnost NXP představila na konci roku 2012 prototyp bezkontaktní platební karty s dotykovým displejem. Ten funguje podobně jako odemykání chytrého telefonu. Karta je po dobu nepoužívání uzamknutá a není možné s ní komunikovat. Při platbě kartou u terminálu je nutné zadat držitelovo gesto pro odemknutí karty, což umožní provedení transakce. Čip karty i samotný dotykový displej si vystačí s napájením poskytovaným terminálem. Tato technologie zamezuje nechtěnému odposlechu karty upravenými čtečkami na delší vzdálenosti a je pohodlnější než vytahovat kartu z odstíněného pouzdra, jak již bylo zmíněno v předchozích kapitolách. Gesto na dotykovém displeji zná pouze držitel a pouze on tak dokáže provést transakci. Společnost se do budoucna snaží rozšířit využití této technologie do chytrých telefonů s NFC podporou. Klient by tak mohl autorizovat platby zadáním gesta na displeji svého telefonu (24).

10.3 Systém Hidden

Proti zneužití čísla karty u internetových plateb přichází společnost Dynamics Inc. s řešením zvaným Hidden®. Jedná se o platební kartu, která obsahuje pět tlačítek a displej z části zakrývající číslo platební karty. Pro zobrazení čísla musí držitel zadat osobní kód na zmíněných tlačítkách. Po úspěšném ověření kódu se zbývající fragment čísla objeví na displeji. Ke zhasnutí displeje dojde po určitém časovém okamžiku. V případě ztráty platební karty z držitelova dohledu nebo v případě fyzické ztráty tak není možné zneužít její údaje pro internetovou transakci, a karta je tak v podstatě nepoužitelná (25).



Obrázek 15: Platební karta se skrytým číslem v displej (25)

10.4 Využití biometrie

Na konci roku 2012 začali někteří francouzští obchodníci testovat placení kartou za pomoci otisku prstu. Používají se bezkontaktní platební karty standardu EMV, které jsou snímány na vzdálenost až dvou metrů od snímače. Klient při ověřování přiloží prst do biometrické čtečky a ta následně sejme unikátní otisk žil nebo otisk prstu. Terminál porovná otisek uložený na čipu se vzorem sejmutým čtečkou a v případě rovnosti povolí provedení platby. Komunikace mezi terminálem a platební kartou je zabezpečena šifrováním. Klienti tak nevydávají kartu z ruky ani nezadávají kód PIN (26).

Biometrie však pronikla i do jiných oblastí použití platebních karet. V Japonsku jsou ve fázi testování provozovány bankomaty, které ověřují klienta za pomoci oskenování jeho dlaně. Klient v bance propojí svůj otisk dlaně se svým bankovním účtem a u bankomatu je autorizován pouze za pomoci sejmutí unikátního vzoru žil na dlani. Toto řešení tedy vůbec nevyžaduje použití platební karty, a tím tak zaniká i riziko zneužití karty formou skimmingu (27).

11 Závěr

V první části práce je čtenář seznámen s platebními kartami jako platebním prostředkem. Na úvod je popsán postupný historický vývoj platební karet od jejich prvopočátků, přes vývoj technologií až do dnešní současné podoby. Následuje rozdělení platební karet dle různých kritérií včetně vysvětlení jejich vzájemných odlišností. Větší část je věnována kartám čipovým. V další části jsou pak popsány náležitosti platebních karet a je vysvětlen význam jednotlivých ochranných prvků sloužících pro znesnadnění padělání karty.

V části věnované standardům a normám, dle kterých se platební karty řídí, je větší důraz kladen na představení standardu EMV. Popsány a vysvětleny jsou jeho základní funkce a prvky včetně postupů jednotlivých ověřovacích metod. Kapitola o šifrováních používaných v bankovnictví popisuje nejpoužívanější šifrovací algoritmy a vysvětluje jejich principy. Popsána je i struktura elektronického podpisu.

V druhé polovině práce následuje výčet jednotlivých způsobů použití platební karty se zaměření na technologie, zajišťující jejich bezpečné používání. Jedná se o použití platební karty v bankomatu, platebním terminálu nebo pro platbu přes internet. Zahrnuty jsou ale i nejmodernější způsoby plateb, jako je bezkontaktní placení nebo platby pomocí chytrého telefonu.

Hlavní částí práce je provedení analýzy rizik a zranitelností u jednotlivých způsobů použití platební karty. To zahrnuje popsání různých druhů známých i méně známých typů útoků, včetně vysvětlení jejich charakteristických rysů a postupů. Po provedení analýzy byly v kapitole nashromážděné informace shrnuty do tabulkového zobrazení a následně vyhodnoceny. Došlo k porovnání jednotlivých silných a slabých stránek druhů záznamu a způsobů použití platebních karet. V případě souhrnu útoků byly navrženy možné způsoby obrany, které by snížily nebo zamezily riziku zneužití platební karty. Jednotlivé typy hrozeb byly doplněny o textový nebo grafický přehled výskytu těchto útoků zjištěných na území České republiky.

Na závěr práce následuje kratší zamyšlení se nad možným budoucím vývojem platebních karet v oblasti bezpečnosti a jsou představeny některé technologické novinky, které by současnou úroveň zabezpečení mohly zvýšit.

Seznam použité literatury

1. **JUŘÍK, Pavel.** *Platební karty, ilustrovaná historie placení.* Praha : Libri, 2012. 978-80-7277-498-2.

2. **Sdružení pro bankovní karty.** [Online] 2012. [Citace: 6. 2. 2013.] http://statistiky.cardzone.cz/download/sbk_statistika_2012.pdf.

3. **JUŘÍK, Pavel.** *Svět platebních a identifikačních karet.* Praha : Grada Publishing, 1999. 80-7169-759-1.

4. **MasterCard®.** Typy karet MasterCard®. [Online] 2013. [Citace: 5. 3. 2013.] http://www.mastercard.com/cz/typy-karet-mastercard.html.

5. **Smart Card Alliance.** Smart Card Primer. [Online] [Citace: 26. 2. 2013.] http://www.smartcardalliance.org/pages/smart-cards-intro-primer.

6. **International Organization for Standardization.** [Online] [Citace: 12. 3. 2013.] http://www.iso.org/iso/home/search.htm?qt=7816&sort=rel&type=simple&published=on.

7. **EMVCo.** About EMV. [Online] 2013. [Citace: 16. 3. 2013.] http://www.emvco.com/.

8. **EMVCo**. A guide to EMV. [Online] [Citace: 16. 3. 2013.] http://www.emvco.com/download_agreement.aspx?id=599.

9. **EMC Corporation.** PKCS #11: Cryptographic Token Interface Standard. [Online] 2012. [Citace: 17. 3. 2013.] http://www.rsa.com/rsalabs/node.asp?id=2133.

10. **Dostálek, Libor, Vohnoutová, Marta a Knotek, Miroslav.** *Velký průvodce PKI a technologií elektronického podpisu.* Brno : Computer Press, a.s., 2009. 978-80-251-2619-6.

11. **National Institute of Standards and Technology.** DATA ENCRYPTION STANDARD (DES). [Online] 1993. [Citace: 19. 3. 2013.] http://www.itl.nist.gov/fipspubs/fip46-2.htm.

12. **National Institute of Standards and Technology.** ADVANCED ENCRYPTION STANDARD (AES). [Online] 2001. [Citace: 19. 3. 2013.] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

13. **Zalabová, Lenka.** UMB/567 Algebra. [Online] 2012. [Citace: 10. 12. 2012.] http://fix.prf.jcu.cz/~lzalabova/.

14. **GE Money.** Karta v mobilu. [Online] 2013. [Citace: 28. 3. 2013.] http://www.inovujeme.cz/karta-v-mobilu.

15. **Mastercard®.** MasterCard Mobile. [Online] 2012. [Citace: 28. 3. 2013.] http://www.mastercardmobile.cz/.

16. **Přibyl, Tomáš.** RFID z hlediska bezpečnosti. [Online] [Citace: 28. 3. 2013.] http://www.ictsecurity.cz/odborne-clanky/rfid-z-hlediska-bezpecnosti.html.

17. **Korb, Kryštof a Pultzner, Martin.** Secure element: klíč k mobilním platbám. [Online] 2012. [Citace: 28. 3. 2013.] http://nfc.mobilenet.cz/clanky/secure-element-klic-k-mobilnim-platbam-20.

18. **Padělání peněz a skimming.** [Online] [Citace: 26. 3. 2013.] http://www.karty-penize.webgarden.name/menu/skimming.

19. **Taušová, Zuzana.** Bankomat v Brně kopíroval platební karty, stopy vedou do Kalifornie. [Online] 2013. [Citace: 26. 3. 2013.] http://zpravy.idnes.cz/bankomat-v-centru-brna-kopiroval-na-zacatku-unora-platebni-karty-phm-/krimi.aspx?c=A130218_180154_brno-zpravy_taz.

20. **ATM - jiné útoky.** [Online] [Citace: 26. 3. 2013.] http://www.karty-penize.webgarden.name/menu/atm-jine-utoky.

21. **Sims, Gary.** Researcher develops Android app that can steal credit card information via NFC. [Online] 2012. [Citace: 28. 3. 2013.] http://www.androidauthority.com/android-app-steal-credit-card-info-nfc-96823/.

22. **Česká spořitelna, a. s.** Phishing. [Online] [Citace: 30. 3. 2013.] http://www.csas.cz/banka/nav/o-nas/phishing-d00014536.

23. **Herbert, Louise.** MasterCard Unveils 'Next Generation Debit Card'. [Online] MasterCard, 2013. [Citace: 2. 4. 2013.] http://www.mastercard.com/us/company/en/newsroom/next_generation.html.

24. **Edwards, Chris.** NXP's touch sensor for chipcards seals PIN inside. [Online] 2012. [Citace: 9. 4. 2013.] http://eandt.theiet.org/news/2012/oct/nxp-touchsensor.cfm?SaveToPDF.

25. **Dynamics Inc.** Hidden®. [Online] 2012. [Citace: 12. 4. 2013.] http://www.poweredcards.com/products_hidden.php.

26. **Planet Biometrics.** Biometric payment trial uses payment cards, biometrics and mid-range contactless technology. [Online] 2012. [Citace: 16. 4. 2013.] http://www.planetbiometrics.com/article-details/i/1318/.

27. **Muncaster, Phil.** Japanese bank palms off customers with biometric ATMs. [Online] 2012. [Citace: 18. 4. 2013.] http://www.theregister.co.uk/2012/04/12/ogaki_palm_scanning_cash/.

28. **Policie ČR.** SKIMMING 2012. [Online] [Citace: 20. 4. 2013.] http://www.policie.cz/clanek/skimming-2011.aspx.

Seznam obrázků

Seznam tabulek