VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

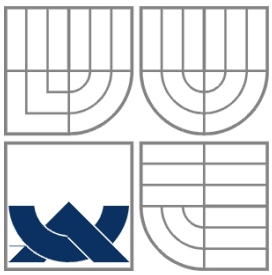
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

PLATEBNÍ SYSTÉMY A PROTOKOLY – ANALÝZA, SIMULACE, VERIFIKACE

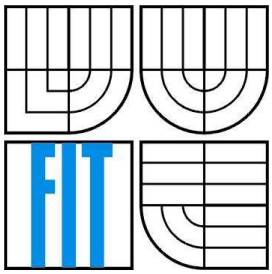
BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE PETRA KUČEROVÁ
AUTHOR

BRNO 2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

PLATEBNÍ SYSTÉMY A PROTOKOLY – ANALÝZA, SIMULACE, VERIFIKACE

PAYMENT SYSTEMS AND PROTOCOLS – ANALYSIS, SIMULATION, VERIFICATION

BAKALÁŘSKÁ PRÁCE

BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

PETRA KUČEROVÁ

VEDOUCÍ PRÁCE
SUPERVISOR

ING. PAVEL OČENÁŠEK

BRNO 2008

Abstrakt

Předmětem bakalářské práce „Platební systémy a protokoly – analýza, simulace, verifikace“ je přehled o platebních systémech v ČR, v EU, v USA a v Japonsku. První část se zabývá legislativou, druhá je věnována platebním systémům, třetí platebním protokolům, jejich charakteristice, použité technologii a bezpečnostním prvkům. Součástí práce je i srovnání jednotlivých platebních systémů a jednotlivých platebních protokolů. Práce se zabývá také bezpečnostními prvky.

Klíčová slova

Platební systém, platební protokol, platební karta, platební styk, zúčtovací centrum, CERTIS, TARGET, SET, VISA

Abstract

The aim of the thesis „Payment systems and protocols – analysis, simulation, verification“ is overview of payment systems in the Czech Republic, in EU, in USA and in Japan. The first part is concentrated on legislation, the second is dedicated to payment systems, the third is dedicated to payment protocols, their characteristics, used technology and security elements. Comparison of particular payment systems and of particular payment protocols is part of this work too. Thesis is also concentrated on security elements.

Keywords

Payment system, payment protocol, payment card, system of payment, clearing center, CERTIS, TARGET, SET, VISA

Citace

Kučerová Petra: Platební systémy a protokoly – analýza, simulace, verifikace. Brno, 2008, bakalářská práce, FIT VUT v Brně.

Platební systémy a protokoly – analýza, simulace, verifikace

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně pod vedením Ing. Pavla Očenáška. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

……
Petra Kučerová
12.5.2008

Poděkování

Děkuji vedoucímu bakalářské práce, panu Ing. Pavlovi Očenáškovi, za trpělivé vedení a pomoc při tvorbě této práce. Dále bych chtěla poděkovat své rodině za jejich podporu a praktické připomínky.

Obsah

1 Úvod

Jako téma své bakalářské práce jsem si zvolila téma Platební systémy a protokoly. Toto téma je s ohledem na rozvoj moderních technologií a jejich využití v bankovním sektoru velmi aktuální. Důležitost tématu podtrhuje také vývoj integrující se Evropy, což následně vyvolává tlak na sjednocení platebních systémů jednotlivých členských států Evropské unie. Zároveň se domnívám, že postupující globalizace vyvine tlak také na vývoj analogických platebních systémů, které umožní rozvoj trhu mezi jednotlivými kontinenty.

Cílem teoretické části práce je analýza jednotlivých platebních systémů a platebních protokolů. Nejdříve se zaměřím na legislativní stránku platebních systémů v ČR i v zahraničí. Další kapitolu věnuji technologii platebních systémů a jejich srovnání. Následující kapitolu věnuji platebním protokolům a jejich srovnání. Pozornost chci zaměřit také na bezpečnostní prvky, zneužití a slabá místa platebních protokolů. Pro názornost hodlám práci doplnit schématy, tabulkami či diagramy. Pro snadnější pochopení textu zařazuji i seznam použitých zkratek.

Praktickou část práce zaměřím na formalizaci protokolu Visa 3-D Secure. Cílem této části práce je vytvořit zjednodušený model protokolu a ověřit jeho bezpečnost v nástroji pro ověřování protokolů. Práci rozdělím na čtyři podkapitoly. První se věnuji nástroji Casper, druhá a třetí bude věnovaná samotné tvorbě skriptu a poslední se zabývá možnostmi napadení protokolu.

V závěru shrnu a zhodnotím výsledky této práce, zhodnotím dostupnou literaturu a nastíním případné potíže při vypracování tohoto tématu.

2 Právní úprava

Díky prudkému rozvoji elektronického (přímého) bankovnictví a díky tomu i rozvoji elektronického platebního styku je tato oblast předmětem úpravy na úrovni Evropské unie. Základní právní normou je Směrnice č. 2000/46/ES, o přístupu k činnosti institucí elektronických peněz, jejím výkonu a obezřetnostním dohledu nad touto činností. Tato směrnice se snaží o zamezení nekontrolovaných emisí elektronických peněz, o zvýšení právní jistoty klienta a o prohloubení důvěry veřejnosti k elektronickým platebním prostředkům.

Mezi další normy upravující tuto problematiku patří Směrnice č. 2002/65/ES, o uvádění finančních služeb pro spotřebitele na trh na dálku a Směrnice č. 97/7/ES, o ochraně spotřebitele v případě smluv uzavřených na dálku, ve kterých je upraven postup při zneužití platební karty. Úprava vztahů mezi vydavatelem a držitelem elektronických prostředků je zakotvena také v doporučení Komise ES č. 97/489/ES, o operacích prováděných elektronickými platebními

prostředky a zejména o vztahu mezi vydavatelem a držitelem, které je zaměřeno především na jasnou úpravu vztahů mezi vydavatelem a držitelem s akcentem na ochranu práv držitele.

Základní právní normou upravující elektronický platební styk v České republice je zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku).

Dle tohoto předpisu se elektronickým platebním prostředkem rozumí prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem a elektronický peněžní prostředek.

Elektronickým peněžním prostředkem je platební prostředek, který uchovává peněžní hodnotu v elektronické podobě.[1] Rozlišujeme dva typy elektronických peněžních prostředků, a to elektronické prostředky na samostatném nosiči a elektronické prostředky v paměti počítače. Elektronické prostředky na samostatném nosiči (např. platební karty) musí být při platbě předloženy. Při použití elektronických prostředků uložených v paměti počítače jsou data zpřístupněna za použití některé ze sítí pro přenos dat a informací.

Za elektronické peníze je považována peněžní hodnota, která představuje pohledávku za vydavatele, je uchovávána na elektronickém peněžním prostředku, je vydávána proti přijetí peněžních prostředků v hodnotě nižší než je hodnota vydávaných elektronických peněz a je přijímána jako platební prostředek jinými osobami než jejich vydavatelem.[2] Elektronické peníze můžeme podle jejich povahy rozdělit na:

- Token-based elektronické peníze – tyto peníze představují virtuální kopii opravdových peněz. Každá mince má svou jedinečnou číselnou hodnotu. Ta zajišťuje, aby nedocházelo k dvojímu utrácení (tzv. doublespending efektu), kdy je jedna mince použita pro dvojí placení. Příkladem těchto peněz je Ecash od firmy Digicash.
- Balance-based elektronické peníze – tyto představují kladný či záporný zůstatek na elektronickém účtu, např. platební systém I LIKE Q.

Úprava vzájemných práv a povinností vydavatelů a držitelů elektronických platebních prostředků je provedena ve vzorových podmínkách vydávaných Českou národní bankou a zveřejněných ve Věstníku České národní banky.

---

[1] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku)

[2] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku)

Elektronické peníze mohou vydávat pouze:

- Banky a pobočky zahraničních bank, mají-li v jim udělené licenci uvedenou činnost vydávání a správa platebních prostředků.
- Zahraniční banky, pokud je k vydávání platebních prostředků na území České republiky opravňuje jednotná licence podle zákona o bankách.
- Spořitelní a úvěrní družstva pro své členy, mají-li v jim uděleném povolení uvedenu činnost vydávání a správa platebních prostředků.
- Instituce elektronických peněz.
- Zahraniční instituce elektronických peněz, které vykonávají činnost podle tohoto zákona na území České republiky na základě jednotné licence.
- Česká národní banka.
- Jiné osoby na základě povolení České národní banky. [3]

Zákon upravuje také pojem platební systém. Platebním systémem se rozumí systém, který zajišťuje převody peněžních prostředků, jestliže

a) má alespoň

1. tři účastníky kromě účastníků uvedených v § 24 odst. 2 písm. a) až c), nebo

2. dva účastníky kromě účastníků uvedených v § 24 odst. 2 písm. a) až c), zajišťuje-li propojení systémů uvedených v seznamu podle § 29 odst. 1, vypořádacích systémů podle zvláštního právního předpisu, nebo vypořádacích systémů uvedených v seznamu Komise Evropských společenství a je-li jedním z nich systém provozovaný podle tohoto zákona,

b) je provozován na základě písemné smlouvy uzavřené mezi všemi účastníky systému nebo na základě písemných smluv uzavřených mezi provozovatelem systému a ostatními účastníky systému (dále jen „smlouva o platebním systému“),

c) provozovatel systému je držitelem licence k provozování platebního systému (§ 30),

d) provádí převody peněžních prostředků podle pravidel stanovených tímto zákonem a podle standardizovaných postupů dohodnutých mezi účastníky systému,

e) existenci systému a jeho název oznámí Česká národní banka Komisi Evropských společenství.[4]

---

[3] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku)

[4] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku)

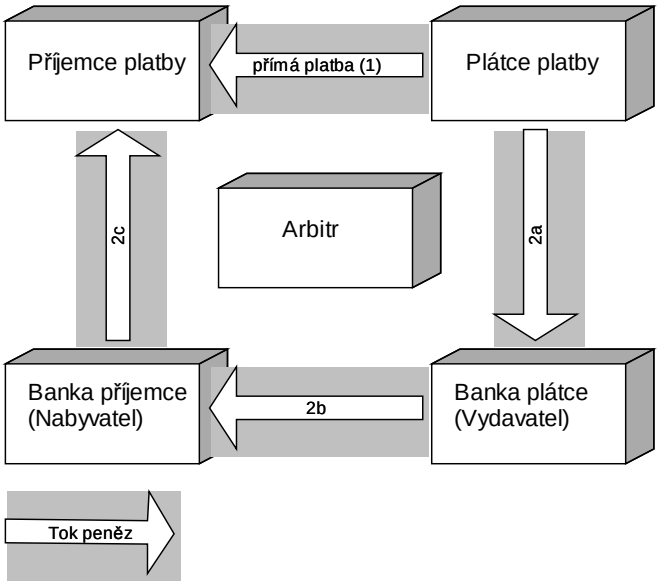
3 Elektronické platební systémy

Dnešní společnost se překotně vyvíjí a spěje k používání stále nových moderních technologií. Tyto změny se dotýkají každého z nás. Jednou z oblastí je i bankovnictví. Rapidní rozvoj moderních technologií jako je Internet a mobilní telefony vede k tomu, že dochází k přechodu od automatizovaného systému k počítači řízenému. Současná společnost se řídí heslem: „Čas jsou peníze.“ Proto většina bank přichází s novou technologií, která umožňuje svým klientům ovládat své účty přímo z domova nebo z kanceláře za použití dnes již zcela běžně dostupných komunikačních prostředků jako je právě Internet nebo mobilní telefon. Klienti tak ušetří čas i peníze, které by museli obětovat při cestě do bankovního ústavu. Elektronické bankovnictví je podporováno i bankami, které cenově zvýhodňují úkony prováděné elektronicky oproti klasickému bankovnictví.

Elektronickou platbou můžeme nazvat každou platbu, která se uskutečňuje prostřednictvím reprezentace platebních nástrojů. Zavedení elektronických plateb se ukázalo jako krok správným směrem. I tato cesta s sebou ale přináší řadu problémů. Jedním z nich je i zajištění bezpečnosti elektronických plateb. Relativně bezpečné jsou platby prováděné přes zabezpečené uzavřené finanční sítě, nebudeme-li brát v úvahu útoky zevnitř sítě. Většina plateb se ale provádí přes otevřenou síť, zejména přes Internet. Proto bylo nutné vytvořit takové platební systémy, které by odolaly všem možným útokům. Snaha o bezpečnost vedla k vytvoření různých bezpečnostních standardů a platebních protokolů, které se snaží nebezpečí útoku minimalizovat. Elektronické bankovnictví se vyvíjí rychlým tempem a současně s ním se sofistikují i útoky na něj, proto se požadavky na bezpečnost platebních systémů neustále mění a zvyšují. Proto nelze prohlásit žádný platební systém za zcela bezpečný.

3.1 Základní entity EPS

Základními entitami elektronického platebního systému je plátce, příjemce a minimálně jedna finanční instituce. Místo označení plátce a příjemce se můžeme setkat s pojmy zákazník a obchodník nebo nakupující a prodávající. Finanční institucí je většinou banka, jejíž funkcí je převést elektronickou podobu peněz na skutečnou. Finanční instituci můžeme dále rozdělit na banku příjemce (nabyvatel) a banku plátce (vydavatel). Už dle označení je zřejmá vydavatelova funkce. Vydavatel vydává peníze plátce bance příjemce nebo přímo příjemci. Naopak nabyvatel přijímá peníze od banky plátce nebo přímo od plátce a předává je příjemci. Nepovinným prvkem v systému může být arbitr, který řeší spory mezi účastníky. Některé platební systémy zahrnují navíc i roli certifikační a registrační autority. Elektronickou platbu lze pak znázornit jako tok peněz od plátce přes vydavatele a nabyvatele k příjemci nebo přímou cestou od plátce k příjemci.



Obr.1: Základní entity elektronického platebního systému a vztahy mezi nimi

3.2 Dělení EPS

Mezi základní dělení patří dělení dle toho, zda v sobě platební nástroj nese elektronickou hotovost, tzn. pracuje-li s přímým elektronickým modelem peněz. V tomto případě hovoříme o elektronickém platebním systému s elektronickými penězi. Nesplňuje-li systém výše uvedenou podmínku, jedná se o platební systém bez elektronických peněz.

Dalším dělením je dělení dle komunikace, a to na systémy s přímou komunikací a systémy s nepřímou komunikací. Za systémy s přímou komunikací označujeme systémy, kde dochází k přímé výměně elektronických peněz mezi plátcem a příjemcem. V případě systémů s nepřímou komunikací je operace vyvolána jen jednou stranou (iniciátorem platby). Banka plátce celou transakci provede a následně oznámí plátci.

Platební systémy rozlišujeme dále i z časového hlediska, a to podle vztahu mezi dobou, kdy iniciátor platby považuje transakci za uzavřenou a dobou, kdy dojde ke skutečnému převedení peněz od plátce k příjemci. Na základě tohoto rozlišujeme mezi předplacenými systémy (pre-paid payment systems), aktuálně placenými systémy (pay-now payment systems) a systémy s odloženou platbou (pay-later payment systems). Předplacené systémy můžeme také označit jako hotovostní (cash-like). Plátce si předem zakoupí platební instrument s již obsaženým kreditem, po zakoupení zboží či služby v budoucnu se hodnota kreditu z platebního instrumentu odečte. Typickým příkladem jsou předplacené telefonní karty. Následující dva modely vyžadují, aby zákazník měl zřízen účet v bance, proto jsou také někdy označovány jako tzv. účtové modely (account-based).

Podle způsobu realizace plateb dělíme systémy na on-line systémy a off-line systémy. Při placení v on-line systému si příjemce před poskytnutím zboží či služby ověřuje u banky plátce jeho platbu. Toto ověření se děje obvykle přes třetí stranu – autorizační autoritu. Na rozdíl od toho není při platbě v off-line systému nutné ověření transakce, tedy on-line spojení s bankou plátce. Aby se zamezilo dvojímu utrácení (duplikaci plateb) používá příjemce různá hardwarová a softwarová zařízení, např. smart karty.

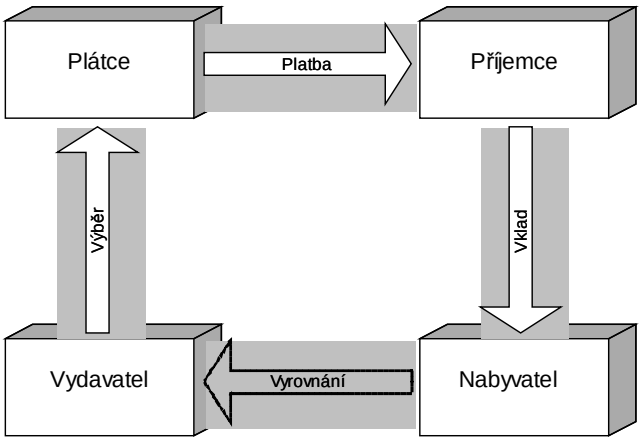
Elektronické platební systémy dále můžeme dělit podle velikosti přenášené částky. Potom hovoříme o systémech pracujících s mikroplatbami, o systémech s platbami s malou hodnotou a o systémech s velkou hodnotou.

Další dělení je založeno na možnosti přesně sledovat cestu elektronických peněz. Má-li vydavatel elektronických peněz možnost identifikovat účastníky každé transakce, hovoříme o identifikovatelných platebních systémech. Opakem jsou anonymní platební systémy, kdy vydavatel po emisi elektronických peněz nemá možnost dohledat jejich další cestu.

Z hlediska organizace platebního styku je důležité, jestli daná platební transakce probíhá v rámci jedné banky nebo mezi více bankami. Podle tohoto hlediska dělíme platební systémy na vnitrobankovní platební systémy a na mezibankovní platební systémy. U vnitrobankovních platebních systémů platba neopouští danou banku. Nutnou podmínku však je, aby plátce i příjemce byli klienti téže banky. V mezibankovním platebním systému jsou plátce i příjemce klienty různých bank. Převod platebních prostředků se v tomto případě sestává ze dvou operací, a to samotného převodu informací charakterizujících prováděnou platbu a zúčtování platby, kdy na jedné straně dochází k zatížení účtu plátce a na druhé straně k připsání částky ve prospěch účtu příjemce.

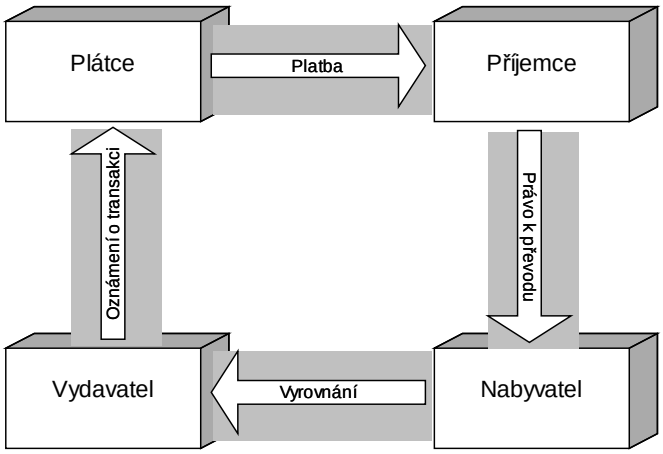
Platební systémy můžeme rozdělit také dle nezbytného toku informací mezi jednotlivými entitami na model s přímou komunikací, na model s odloženou platbou, na model s nepřímou komunikací a na model s nepřímou komunikací s vyloučením role plátce. Zde dochází k míšení jednotlivých výše uvedených kritérií dělení.

Na obr. 2 na následující straně vidíme model s přímou komunikací. Tento model je typický pro předplacené systémy. Plátce si u vydavatele předplatí kredit, pomocí něhož zaplatí platbu příjemci. Příjemce si pak u své banky elektronické peníze převede na reálné. Na konci musí dojít k zúčtování (vyrovnání) plateb.



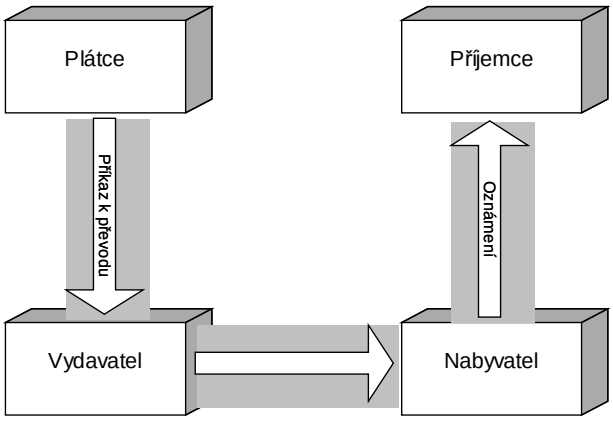
Obr.2: Model systému s přímou komunikací

Obr. 3 popisuje model s odloženou platbou. Jedná se opět o model s přímou komunikací. K převedení peněz však dochází později než v době koupě zboží či služby. Plátce dává příjemci právo převést peníze od vydavatele k nabyvateli s následným oznámením o provedené transakci plátci. Příkladem může být platba kreditní nebo debetní kartou.



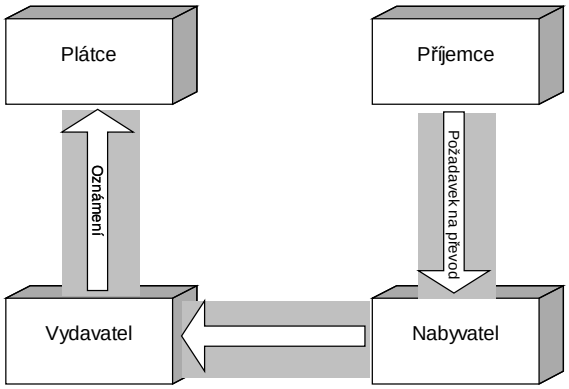
Obr.3: Model systému s odloženou platbou

Obr.4 popisuje model s nepřímou komunikací, kdy plátce zadá vydavateli příkaz k úhradě peněz nabyvateli. Příjemci je oznámeno provedení transakce. Příkladem může být běžný příkaz k převodu peněz.



Obr.4: Model systému s nepřímou komunikací

Obr.5: Posledním typem je platební systém založený na nepřímé komunikaci s vyloučením role plátce, např. trvalý příkaz, který umožňuje příjemci přes nabyvatele čerpat peněžní prostředky z účtu plátce u vydavatele.



Obr.5: Model systému s nepřímou komunikací s vyloučením role plátce

3.3 Elektronické platební systémy v ČR

V současné době je na území České republiky jediným aktivně fungujícím platebním systémem systém CERTIS (Czech Express Real Time Interbank Gross Settlement System). Provozovatelem systému je Česká národní banka. Provoz systému byl zahájen v rámci zúčtovacího centra SBČS 8.3.1992. Po rozdělení Československa zůstalo zúčtovací centrum v ČNB a na Slovensku byl vytvořen nový systém.

Všichni účastníci systému jsou jednoznačně identifikováni kódem své banky. Tento kód je povinným údajem každé bankovní transakce. Dále jsou používány další číselné údaje, které jednotlivé platby blíže identifikují.

Vznik, provozování systému, práva a povinnosti účastníků jsou upraveny Zákonem o platebním styku. Smlouvy o účtech jednotlivých účastníků systémů, které jsou vedeny v ČNB se řídí Obchodním zákoníkem.

CERTIS je založen na následujících principech:

- Zúčtování všech tuzemských mezibankovních plateb v českých korunách bez ohledu na výši částky.
- Všichni přímí účastníci systému mají v ČNB veden účet platebního styku.
- Na účtu platebního styku vedeném u ČNB není povolen debetní zůstatek – zůstatky jsou součástí povinných minimálních rezerv, které jsou stanovené jako určené procento z depozit (2% k 31.12.2007).
- Zúčtování pouze krytých plateb.
- Neodvolatelnost příkazů.

Mezi přímé účastníky systému patří banky, pobočky zahraničních bank, spořitelní a úvěrní družstva. Pro každou banku vede ČNB jeden účet mezibankovního platebního styku. Dalšími účastníky systému jsou tzv. třetí strany. Jedná se o účastníky se zvláštním statusem, kteří mají uzavřenou bilaterální smlouvu s ČNB. Většinou se jedná o významné finanční instituce, které hrají důležitou roli na trhu. Příkladem může být UNIVYC, a.s. (UNIverzální VYpořádací Centrum), které zajišťuje vypořádání obchodů na burze, RM-SYSTÉM, a.s. nebo clearingové středisko pro platební karty MasterCard a VISA. Tito účastníci nemají vedeny účty u ČNB, ale jsou oprávněni předávat se souhlasem přímého účastníka příkazy k převodu mezi účty přímých účastníků.

Systém zpracovává úhrady, inkasa, storna úhrad (opravné zúčtování), transakce třetích stran a informační a kontrolní položky. Účetní den začíná v 17 hodin předchozího pracovního dne a končí v 16 hodin následujícího pracovního dne. Data jsou do systému předávána v elektronické podobě, dle pravidel určených ČNB, prostřednictvím komunikační sítě. Platební příkaz je proveden po ověření všech kvalitativních požadavků dat. V průběhu celého procesu vypořádání je kontrolováno, zda je na účtu banky plátce dostatečný zůstatek. Pokud není na účtu potřebný zůstatek ke krytí platby, platba je umístěna do tzv. zadržené fronty. Banka plátce je o této situaci informována a má možnost platbu dodatečně pokrýt. Nepokryje-li ji, bude platba systémem odmítnuta a vrácena bance, která ji zaslala.

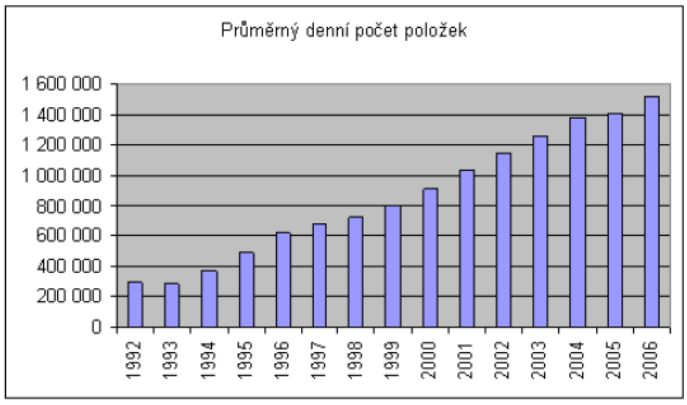
Aby byl dodržen harmonogram účetního dne a dodržen čas uzávěrky účetního dne, bylo nutné zajistit, aby byly jednotlivé žádosti o vypořádání rozloženy rovnoměrně v průběhu celého dne, nebo lépe, aby nejvíce žádostí o vypořádání přicházelo na začátku účetního dne. Proto ČNB stanovila poplatky za služby systému tak, že na začátku účetního dne jsou velmi nízké (0,22Kč) a na konci účetního dne velmi vysoké (100Kč). Při zpracovávání většího počtu transakcí jednou bankou jsou poskytovány slevy.

Pro bezpečnost celého systému byla prováděna řada ověřovacích testů. V říjnu 1996 byly úspěšně dokončeny testy projektu zálohování systému v reálném čase, který pracuje na principu on-line zálohy pomocí optických disků.

Začátkem roku 1999 byl uveden do provozu nový informační systém - CERTIS-IS. Tento informační systém poskytuje účastníkům informace o všech důležitých parametrech zpracování, včetně běžných zůstatků na účtech mezibankovního platebního styku, jednotlivých transakcích, platbách, které jsou seřazeny ve frontě příkazů, a jiných operačních aspektech. Informační systém je založen na extranetové technologii využívající šifrovací a rozlišovací znaky. [5]

Pro zvýšení bezpečnosti systému byly v roce 2001 spuštěny další dva podsystémy, které zajišťují bezpečnost dat (CERTIS-SZD) a bezpečnost přenosu zpráv (CERTIS-SPZ). Systém zabezpečení dat pracuje na principu veřejných klíčů. Funkci certifikační autority plní ČNB. Systém přenosu zpráv zajišťuje automatické předávání a zpracovávání dat.

1.11.2006 uvedla ČNB novou verzi systému CERTIS, která zvýšila rychlost zpracování položek. Nový systém zpracovává v průměru 1 500 000 transakcí za hodinu, oproti původním čtyř stům tisícům transakcí za hodinu.



Zdroj: www.cnb.cz

Obr.6: Průměrný denní počet položek zpracovávaný v systému CERTIS

[5] http://www.cnb.cz/cs/platebni_styk/certis/certis_popis.html

3.4 Elektronické platební systémy v EU

V současnosti se v Evropské unii používá řada významných platebních systémů. K nejdůležitějším patří TARGET2, systémy společnosti EBA (EURO1, STEP1, STEP2) a systém SEPA. Všechny tyto systémy využívají pro zasílání zpráv mezinárodní komunikační síť SWIFT. Považuji proto za důležité ji nejdříve osvětlit.

Realizace bezhotovostního platebního styku je založena na vzájemném předávání dat a informací týkajících se platebních transakcí mezi bankami, a to jak v národním, tak i v mezinárodním měřítku.[6] Dříve se k zasílání dat používal dálnopis. V současnosti je vybudována mezinárodní komunikační síť SWIFT (Society for Worldwide Interbank Financial Telecommunication). SWIFT je společnost pro celosvětovou mezibankovní finanční telekomunikaci. Její hlavní funkcí je propojení všech zúčastněných bank a jiných institucí pomocí počítačové sítě, která dovoluje rychlý, spolehlivý a hlavně bezpečný přenos informací o finančních transakcích. Je důležité zdůraznit, že SWIFT není žádný mezinárodní zúčtovací systém, ale pouze mezinárodní komunikační síť. Nerealizuje platby, pouze přenáší datové zprávy obsahující platební instrukce.

Společnost byla založena dle belgického práva roku 1973. U jejího vzniku stálo 239 velkých evropských a severoamerických bank z patnácti zemí. Právní forma této společnosti je akciová společnost a sídlí v Belgii. Síť začala fungovat v roce 1977 a počet jejích členů se neustále zvětšuje. Počet zpráv, které jsou přes síť za den odeslány, se pohybuje přes 10 milionů. Síť se skládá ze dvou operačních středisek, která slouží k zálohování dat. První středisko je v Evropě (Leiden) a druhé v USA (New York). Na tato střediska jsou napojeny tzv. národní koncentrátory, které slouží jako zpracovatelé informací pro jednotlivé země.

Technicky je systém zajištěn technologií telex. Přenos zpráv se realizuje pomocí vysoce standardizovaných swiftových zpráv. Společným jazykem těchto zpráv je angličtina. Bezpečnost přenášených zpráv je zajištěna kódováním a vzájemnou výměnou kódových klíčů.

Zprávy členíme dle jejich účelu a funkce do jednotlivých kategorií (0-9, poslední kategorie je označena jako x), skupin a typů. Každá zpráva je označena písmeny MT a třemi numerickými znaky po řadě znamenajícími kategorii zprávy, skupinu zprávy a typ zprávy. Kategorie zprávy vypovídá o účelu nebo předmětu obchodu, skupina zprávy popisuje funkci zprávy a typ správy definuje specifické detaily.

---

[6] MÁČE, M.: Platební styk klasický a elektronický. 1. vyd. Praha: Grada Publishing, a.s., 2006. s. 154. ISBN 80-247-1725-5

Obsah zprávy členíme do pěti bloků. Pro všechny zprávy je povinný pouze první blok. První tři bloky tvoří záhlaví zprávy, čtvrtý blok tvoří samotný text zprávy a poslední blok tvoří tzv. trailer. Záhlaví zprávy (header) obsahuje identifikaci odesílající banky nebo finanční instituce, vstupní pořadové číslo swiftové zprávy, typ zprávy, její prioritu a identifikaci adresáta swiftové zprávy.[7] Samotný text zprávy je tvořen cca 95ti textovými poli pevné nebo proměnné délky. Jednotlivá pole jsou seskupena do devíti skupin. Trailer je tvořen technickými informacemi o poslané zprávě.

Swiftová adresa (BIC – The Bank Idetifier Code) je stanovená normou ISO a slouží k identifikaci odesílatele a příjemce zprávy a k identifikaci swiftových bank. Identifikační kód banky je osmimístné nebo šestnáctimístné číslo, které se skládá z několika kódů. Počáteční čtyři znaky představují kód banky, za ním následuje kód země, ve které daná banka sídlí, dále pak kód místa (dvoumístný alfanumerický znak), který identifikuje město, ve kterém sídlí uživatel a nakonec kód pobočky. Kód pobočky je nepovinnou součástí swiftové adresy a skládá se ze tří alfanumerických znaků. Příklady swiftových adres: CSPOCZPP (Česká spořitelna), KOMBCZPP (Komerční banka).

3.4.1 TARGET

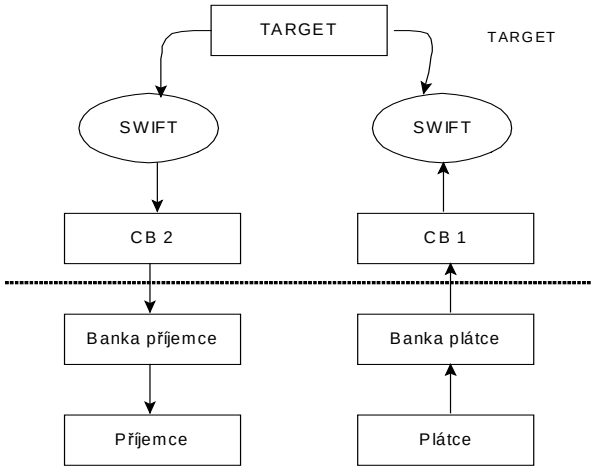
Trans-European Automated Real-Time Gross Settlement Express Transfer System (TARGET) je systém propojující národní platební systémy členů EU a platební systém Evropské centrální banky. TARGET byl uveden do provozu 4.1.1999. Je založen na brutto vypořádání systému v reálném čase (RTGS) a jedná se o systém plateb velkých objemů denominovaných v eurech. Cílem vytvoření tohoto systému bylo usnadnit bezpečný mechanismus pro brutto vypořádání v reálném čase, zvýšení efektivity zahraničních plateb v eurozóně a nabídnutí rychlého a bezpečného prostředku k provádění monetární politiky.

Pro národní platební systémy zapojené do systému TARGET musí platit, že pracují na stejném vypořádacím principu, tj. na principu brutto systému v reálném čase, systémy jsou provozovány centrálními bankami a musí pracovat v eurech.

Každá banka, která je součástí systému, je jednozačně identifikována pomocí BIN (Bank Identification Number – číslo přidělené karetní asociací dané bance). Účetní den začíná v 7 hodin a končí v 18 hodin středoevropského času. Stanovení jedenáctihodinové doby napomáhá snížit rizika vyrovnávání s devizovými operacemi. Otevírací doba se plně překrývá s provozní dobou zúčtovacího systému Fedwire v USA a platebního systému v Japonsku. Toto překrývání umožňuje souběžné vyrovnání.

[7] MÁČE, M.: Platební styk klasický a elektronický. 1. vyd. Praha: Grada Publishing, a.s., 2006. s. 156. ISBN 80-247-1725-5

Při zúčtování plateb v prvním kroku pošle banka plátce platební příkaz v místním formátu svému národnímu zúčtovacímu centru. Centrální banka tohoto státu zkontroluje, zda má banka na svém účtě dostatek finančních prostředků pro provedení platby. Pokud ano, přílušná částka je debetována z účtu a kreditována na účet banky příjemce, který je veden u centrální banky státu příjemce. Zpráva o platbě je potom poslána přes SWIFT do centrální banky ve státě příjemce. Tato banka předá platbu do národního zúčtovacího systému, který ji následně předá bance příjemce platby.



Obr.7: Průběh zúčtování v systému TARGET

Jistou nevýhodou systému jsou poměrně vysoké poplatky, které ECB účtuje za zpracování jednotlivých operací. Výše poplatků je závislá na počtu operací, nikoliv na převáděné částce, a poplatky se pohybují v rozmezí 0,8-1,75 EUR. Pro výši částky převodu neexistuje žádný minimální ani maximální limit, přesto je systém určen především pro zúčtování vyšších částek (LVTS – Large-value funds transfer system). Poplatky za vstup do systému neexistují.

S rozvojem procesu integrace a konsolidace evropského finančního systému byly na systém kladeny stále větší požadavky. Jednalo se zejména o požadavky na zlepšení kvality služeb a zavedení centralizovaného systému. Současný decentralizovaný systém se vyznačoval vysokými náklady na koordinaci systému. Při zachování současné struktury by přidružení dalších zemí do systému znamenalo existenci systému s velkým počtem základen, což by znesnadňovalo provoz systému.

3.4.2 TARGET2

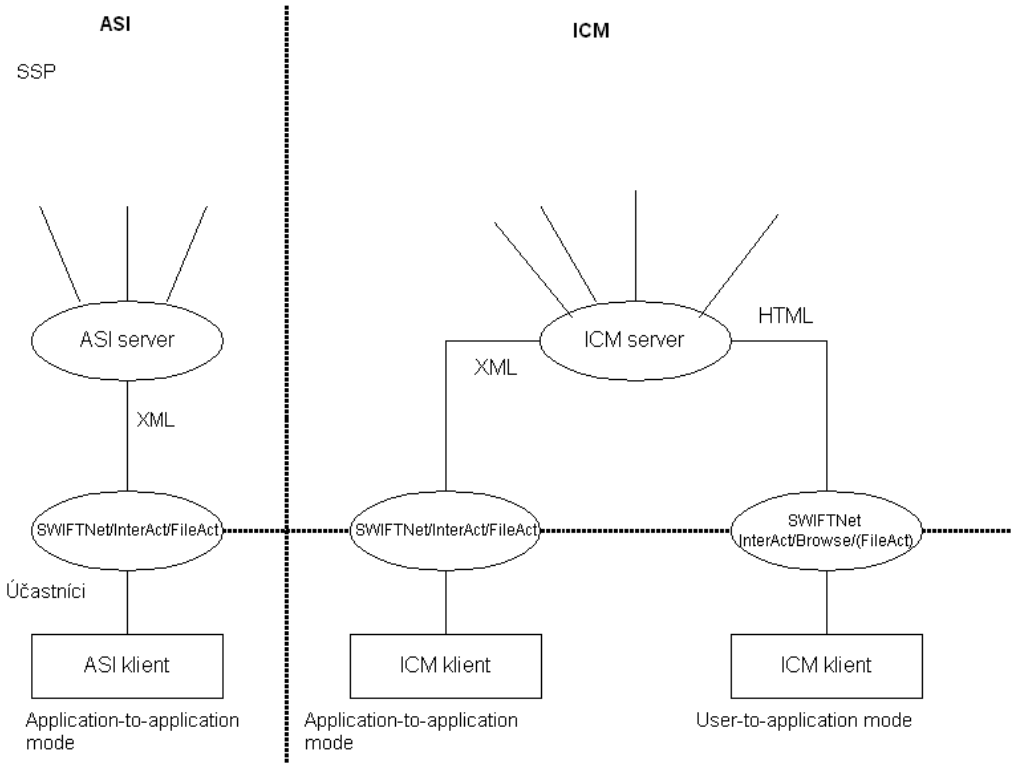
Důvody uváděné na konci předchozí kapitoly vedly k vývoji nástupce systému TARGET. Cílem projektu bylo vytvořit centralizovaný a plně harmonizovaný platební systém na základě jedné společné technické platformy (tzv. Single Shared Platform – SSP). Vlastníky systému jsou centrální banky členských států Evropské unie. Systém měl být schopný lépe uspokojit potřeby uživatelů svým zjednodušením, důraz se kladl i na snižování nákladů a především budoucí vývoj a rozšiřování EU.

Přechod na nový systém byl započat roku 2002 a můžeme jej rozdělit do tří základních fází – přípravná fáze, plánovací fáze a testovací fáze. Koordinátorem projektu byla Evropská centrální banka, která v říjnu roku 2002 odsouhlasila strategii nového systému.

V přípravné fázi došlo ke koordinaci úrovně služeb a k vývoji společné technické platformy. Ta vznikla ze spolupráce tří evropských centrálních bank, a to centrální banky Itálie (Banca d'Italia), centrální banky Francie (Banque de France) a německé centrální banky (Deutsche Bundesbank). Pro tyto banky se používá označení 3CB.

Pro komunikaci v systému se využívá mezinárodní sítě SWIFT. Podsítě SWIFTu jsou SWIFTNet a FIN Copy, poskytující své služby pro platby a vyrovnání. Pomocí další podsítě SWIFTNet InterAct je sledováno řízení peněz v reálném čase, pomocí další podsítě SWIFTNet FileAct je zajištěna distribuce souborů a zpráv. Pro prohlížení informací a kontrolu služeb slouží prohlížeč SWIFTNet Browse.

Systém se skládá ze dvou rozhraní, a to z pomocného systémového rozhraní (ASI – the Ancillary System Interface) a z modulu pro kontrolu informací (ICM – the Information and Control Module). Pro přístup k ICM jsou používány dva režimy. První z nich je režim Application-to-application, ve kterém je zasílání zpráv zcela automatizováno, a druhý je User-to-application, ve kterém jsou informace zobrazovány v internetovém prohlížeči.



Obr.8: Struktura systému TARGET2

Pro ukládání informací systém využívá dvou adresářů – TARGET2 Directory a SWIFT BIC Directory. Adresář TARGET2 obsahuje adresy institucí, které jsou v systému zapojeny, všechny přímé a nepřímé účastníky. Adresář SWIFT BIC obsahuje přesná identifikační čísla jednotlivých účastníků systému.

Bezpečnost systému je založena na PKI infrastruktuře (struktuře předávání veřejných klíčů).

3.4.3 Clearingové systémy EBA

Clearingová společnost EBA (Euro Banking Association) byla založena v červnu roku 1998 za účelem vlastnit a provozovat platební systém EURO1. Zakládajícími členy bylo 52 hlavních evropských a mezinárodních bank. Dnes EBA zahrnuje 71 bank (akcionářů). Přes systémy EURO1, STEP1 a STEP2 nabízí zúčtování a vyrovnání plateb velkých i malých objemů širokému množství bank Evropské unie.

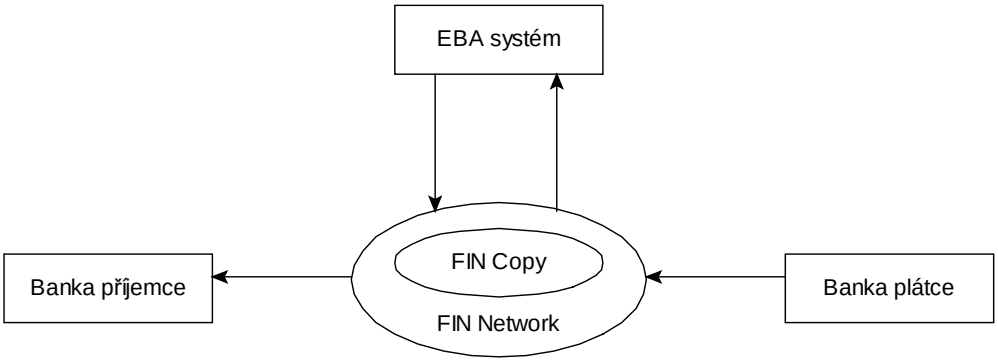
3.4.3.1 EURO1

Platební systém EURO1 byl uveden v roce 1998. Slouží jako platební systém pro přeshraniční a domácí platby v euroměně ve velkých objemech mezi bankami EU. Každý z členů tohoto systému musí splňovat kritéria pro vstup stanovená clearingovou společností EBA. Každý člen musí vlastnit prostředky ve výši nejméně 1,25 miliardy euro, krátkodobý úvěrový rating žadatele o vstup musí být nejméně P2 (dle Moodyho stupnice) nebo A2 (dle hodnoty stanovené společností S&P). Poslední podmínkou pro vstup do systému je přímý vstup k některému RTGS systému v Evropské unii, který je přímo napojený na systém TARGET. V současnosti má systém přes 130 přímých účastníků a zpracovává v průměru 185 000 transakcí v celkové hodnotě přes 195 bilionů euro. Pro komunikaci a přenos zpráv je využívána síť SWIFT. Hlavní odlišností od systému TARGET je, že EURO1 je nettingový platební systém – všechny příkazy jsou vypořádány prostřednictvím zúčtovací banky (ECB) na konci účetního dne.

3.4.3.2 STEP1

STEP1 je v prvé řadě platební systém pro komerční transakce a zpracovává jednoduché přeshraniční transakce v euroměně. Systém byl uveden v listopadu roku 2000 na podporu bank v době, kdy se legislativa EU, týkající se doby provádění a ceny za přeshraniční platby, stala účinnou. Účastníky systému jsou všichni členové systému EURO1 a přidruženým účastníkem se může stát i každá komerční banka EU. Členství není limitováno výší kapitálu banky. Systém zpracovává denně 22 000 transakcí v celkové hodnotě přesahující 400 milionů eur.

Systém pracuje na systému zasílání SWIFT zpráv přes síť FIN Copy. Banka plátce odešle zprávu s platebním příkazem. Zpráva obsahuje hlavičku s názvem „ERP“. FIN Copy tuto zprávu s příkazem zkopíruje do centrálního systému EBA, kde je předána STEP1 ke zpracování. Všechny zprávy předávané mezi bankou systému STEP1 a její vypořádací bankou jsou doručeny SWIFTu před druhou hodinou odpolední. V 7:30 začíná systém zpracovávat zprávu a probíhá zúčtování plateb za současného kontrolování limitu na účtu banky plátce. Ve 14:10 systém poskytne bance plátce tzv. potenciální čistý zůstatek (PNB – Potential Net Balance) pro denní transakce. V případě, že zúčtovací banka informuje EBA, že již nebude vyrovnávat za banku plátce, bude bance plátce PNB snížen. Po provedení transakcí v systému je bance příjemce zaslána přes síť SWIFT zpráva o provedení transakce a příslušná částka je zaúčtována.



Obr.9: Průběh zúčtování v systému STEP1

3.4.3.3 STEP2

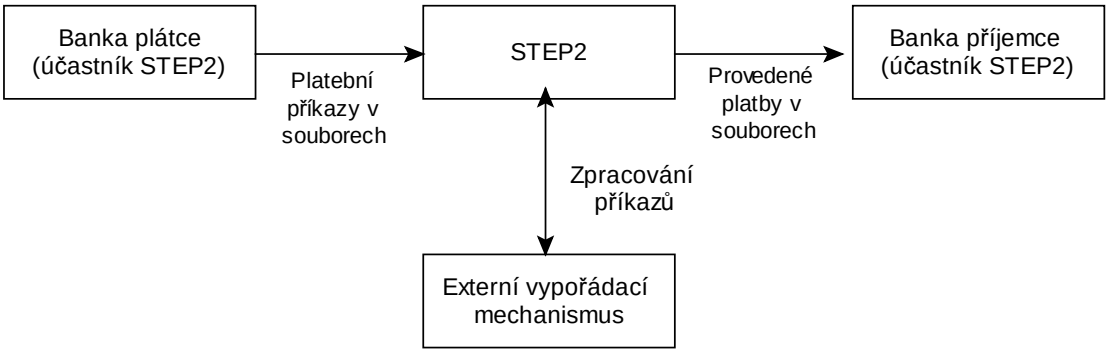
Činnost systému STEP2 byla zahájena v dubnu roku 2003. Jedná se o první panevropské automatické zúčtovací centrum (PE-ACH – Pan-European Automated Clearing House). Systém je určen převážně pro platby velkých objemů v eurech. Členy systému jsou všechny členské banky systémů EURO1 a STEP1. Přidruženým účastníkem se může stát každá aktivní komerční banka Evropské unie. Členství v systému není limitováno výší kapitálu banky. Systém je založen na standardu ISO 20022 Universal Financial Industry (UNIFI) a na zasílání zpráv ve formátu XML.

V systému jsou zpracovávány i maloobchodní platby až do 50 000 eur za jednu transakci. V systému je zapojeno 97 přímých účastníků a přes 1 500 nepřímých účastníků. Průměrný počet transakcí zpracovaných za den činí více než 200 000.

Systém se skládá ze tří služeb – XCT (Credeuro service), SCT (SEPA Credit Transfer service) a SDD (SEPA Direct Debit Service). Tyto služby jsou na sobě navzájem nezávislé, i když sdílí stejnou infrastrukturu a technologie a vyznačují se stejným stupněm odolnosti.

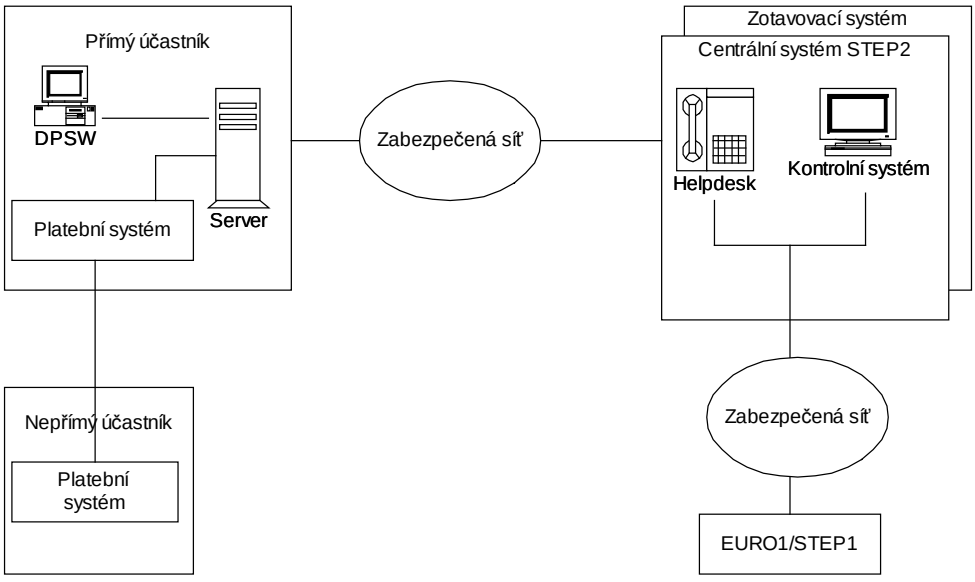
Systém je založen na externím vypořádacím mechanismu. Přímý účastník systému přenese své platby pomocí ICF (Input Credit Files) do centrálního systému STEP2. Centrální systém ověří podpis každého souboru a jako odpověď pošle CVF (Credit Validation File). Následuje přenos zúčtovací

instrukce do systému EURO1/STEP1 na zpracování a zaslání zpětné odpovědi od systému o úspěšném obdržení instrukce. Dalším krokem je přenos SCF (Settled Credit Files) k přímému účastníku. Po zpracování všech transakcí je všem přímým účastníkům zaslána CRR (Cycle Reconciliation Report) a DRR (Daily Reconciliation Report).



Obr.10: Průběh zúčtování v systému STEP2

Pro bezpečnou komunikaci účastníka se systémem se používá rozhraní DPSW (Direct Participant Webstation). Toto rozhraní využívá služeb mezinárodní organizace SWIFT a pomáhá přímému účastníku systému při každodenních operacích. Rozhraní slouží pro doplnění celkových informací a statistik, které jsou jinak běžně dostupné v denní smírčí zprávě (DRR) a měsíční statistické zprávě (MSR – Monthly Statistics Report). Přímý účastník má přístup pouze k informacím o operacích, ve kterých vystupuje jako plátce nebo příjemce, popřípadě k operacím jeho nepřímých účastníků. STEP2 dále obsahuje systém, který zajišťuje zotavení z chyb, detekuje ztrátu dat nebo jejich duplikaci.



Obr.11: Architektura systému STEP2

3.4.4 SEPA

S nástupem jednotné evropské měny vznikla potřeba jednotného platebního systému pro země EU. Proto bylo 4. května 2006 rozhodnuto o plánování nového platebního systému SEPA (Single Euro Payments Area). U jeho vzniku stálo 42 evropských bank a evropská bankovní sdružení EACB (European Association of Cooperative Banks), ESBG (European Savings Banks Group), FBE (European Banking Federation) a EBA. Byla vytvořena Evropská platební rada EPC (European Payment Council). Cílem této rady je vytvoření jednotné platební oblasti pro státy EU. Systém by měl zahrnovat tři podsystémy pro oblast kreditních plateb, přímého inkasa a platebních karet. V současné době má rada 64 členů z 27 evropských zemí.

Platební rada schválila tři fáze vývoje. V první fázi vývoje byl vytvořen návrh systému a jeho základní specifikace. První fáze zahrnovala i tvorbu nových platebních nástrojů (např. Panevropský přímý debet PEDD). Druhá fáze se zabývala samotnou implementací vytvořených nástrojů a infrastruktury systému. Poslední fáze vývoje byla započata v lednu tohoto roku a jejím cílem je nahrazení dosavadních platebních nástrojů jednotnými evropskými nástroji SEPA.

S jednotnou platební oblastí vyvstala i otázka její právní úpravy. Bylo nutné sladit právní normy všech zemí EU. Cílem právních úprav je komplexní ochrana spotřebitele, transparentnost a stejnorodost bankovních služeb.

Systém by měl být uveden do provozu v roce 2010. V České republice se projektem SEPA zabývá Česká bankovní asociace. Tento projekt se stane pro Českou republiku aktuální až po přistoupení na euro. Průzkumy ukázaly, že v dnešní době jsou na tento projekt nejvíce připraveny banky zemí severní Evropy, nejméně banky jižní Evropy.

3.5 Elektronické platební systémy USA a Japonska

3.5.1 Fedwire

Systém Fedwire je systém pro elektronický přenos plateb. Fedwire provozuje Federální rezervní systém Spojených států. Na systém jsou napojeny všechny federální rezervní banky, státní pokladna a přes 9000 nejvýznamnějších finančních institucí. Systém je využíván převážně k nočním převodům úvěrů bank, k vypořádání mezibankovních transakcí a k vypořádání obchodů s cennými papíry. Systém je založen na brutto vypořádání systému v reálném čase (RTGS). Počátky systému spadají až do roku 1918, kdy došlo k propojení dvanácti rezervních bank a státní pokladny. Tento systém pracoval na principu telegrafních spojů. S rozvojem moderních technologií došlo k přechodu na elektronickou formu komunikace.

Systém zpracovává denně okolo 528 000 příkazů v celkové hodnotě okolo 2,1 trilionů dolarů. Účetní den začíná v 00:30 a končí v 6:30 východního času. Tyto operační hodiny se překrývají jak s evropskými, tak s asijsko-pacifickými zúčtovacími systémy.

Účastníci systému zadávají platební příkazy rezervní bance online (zasláním elektronické zprávy) nebo offline (přes telefon). Platební příkazy musí být ve speciálním formátu a podléhají bezpečnostní kontrole.

Způsob vypořádání probíhá klasicky. Plátce zadá platební příkaz své bance. Banka plátce debituje plátcův účet a zahájí vypořádání. Obratem je v systému Fedwire snížen účet banky plátce a navýšen účet banky příjemce. Systém uvědomí banku příjemce o proběhlé transakci. Banka příjemce kredituje účet příjemce a uvědomí příjemce o připsání částky.

3.5.2 CHIPS

Systém mezibankovního zúčtování plateb CHIPS (Clearing House Interbank Payment System) patří k největším soukromým platebním systémům na světě. Systém byl uveden do provozu v roce 1970 a u jeho vzniku stála skupina komerčních bank města New York. Systém má 59 členů, mezi které patří významné banky USA a pobočky významných zahraničních bank. Většina členů systému CHIPS je zároveň členy systému Fedwire. Systém zpracovává přes 90 procent všech mezibankovních dolarových převodů. Systém je řízen desetičlenným představenstvem skládajícím se ze senior managerů největších amerických bank. CHIPS zpracovává denně okolo 240 000 transakcí v celkové výši přes 1,2 trilionů dolarů. Pro přenos zpráv ve formátu XML využívá systém síť SWIFT. Až do ledna roku 2001 CHIPS prováděl zúčtování transakcí na konci obchodního dne. Nyní provádí zúčtování během dne.

Malé platby, které mohou být kryty z kladných zůstatků na účtech bank, jsou prováděny okamžitě. Ostatní příkazy jsou řešeny bilaterálně (např. když banka A má zaplatit 500 milionů dolarů bance B a banka B má zaplatit stejnou částku bance A) bez pohybu na účtech obou účastníků. Další platby jsou vyrovnávány multilaterálně. Předpokládejme, že banka A musí zaplatit bance B 500 milionu dolarů a banka A současně předpokládá obdržení částky 500 milionů dolarů od banky C. Bez nettingu by banka A byla povinna zaplatit bance B danou částku, což by způsobilo pokles na účtu banky A. V systému CHIPS banka A zařadí požadavek banky B do pomyslné fronty a příkaz provede až po obdržení pohledávané částky od banky C. Platby, které nemohou být žádným podobným způsobem svázány, jsou provedeny na konci dne.

K usnadnění provádění příkazů během dne je každý účastník systému povinen mít na účtu minimální výši peněz (tzv. security deposit). Výše této částky je týdně přepočítávána a závisí na množství provedených transakcí daného účastníka. Tato částka je na konci dne využita k vypořádání transakcí, které nemohly být žádným způsobem svázány.

3.5.3 Platební systémy Japonska

V Japonsku existují čtyři hlavní platební systémy pro vypořádání mezibankovního platebního styku – tři zúčtovací systémy v soukromém sektoru a zúčtovací systém spravovaný centrální bankou (BOJ-NET). Třemi soukromými systémy jsou Zengin Data Telecommunication System (Zengin System), který vyrovnává maloobchodní obchody, Foreign Exchange Yen Clearing System (FXYCS), který se zaměřuje převážně na zúčtování přeshraničních obchodů s yeny a Bill and Cheque Clearing System (BCCSs), který vypořádává směnky a šeky.

3.5.3.1 BCCSs

První clearingový dům v Japonsku byl založen v Osace v roce 1879. Clearingový dům v Tokiu byl založen v roce 1887. Od prosince roku 2001 existovalo v celém Japonsku 540 clearingových domů, které se zabývaly vypořádáním šekových obchodů, ale jen 173 z nich bylo ustanoveno Ministerstvem spravedlnosti. Více než 70 procent všech šekových obchodů je vypořádáno v clearingovém domě v Tokiu, kde se denně vypořádávají obchody v částce 2,6 trilionů JPY. Většina clearingových domů je ve vlastnictví místních bankovních asociací. V případě tokijského bankovního domu se jedná o Tokyo Bankers Association (TBA). Systém má 421 účastníků, z toho 121 přímých účastníků. Příjemce šeku předloží vystavený šek své bance. Ta ho postoupí clearingovému domu, který si od banky plátce vyžádá požadovanou sumu.

3.5.3.2 Zengin System

Zengin System byl uveden do provozu již v roce 1973. Dnes zpracovává denně přes 5 milionů transakcí v celkové výši 10 trilionů JPY (82 bilionů USD). Provozovatelem systému je TBA. Z celkového počtu 2021 účastníků je 154 přímých účastníků. Koncovými uživateli systému jsou drobné firmy nebo jednotlivci.

Proces zahajuje plátce zadáním příkazu k převodu své bance. Banka plátce odešle platební příkaz do Zengin centra, které přepošle instrukci bance příjemce. Závazek mezi bankou plátce a bankou příjemce je nahrazen dvěma závazky. První je mezi bankou plátce a TBA a druhý je mezi bankou příjemce a TBA. Po obdržení instrukce banka příjemce navýší účet příjemce. Systém vypočítá výši závazku mezi jednotlivými bankami a TBA a odešle tuto informaci centrální bance Japonska přes svoji síť (Zengin System Network). V centrální bance potom dojde k debitu či kreditu jednotlivých účtů zúčastněných bank.

3.5.3.3 FXYCS

FXYCS byl uveden do provozu v roce 1980 jako systém sloužící k vyrovnání přeshraničních obchodů v domácí měně. Systém zpracovává 39 000 transakcí za den v celkové výši 28 trilionů JPY (230 bilionů USD). Systém je spravován TBA. Členy systému je 244 finančních institucí včetně 73 poboček zahraničních bank.

Plátce ze zahraničí instruuje svou banku k provedení platby v japonské měně. Banka plátce požádá o přenos přes síť SWIFT svou korespondenční banku. Ta pošle na síť BOJ-NET platební příkaz, který je následně odeslán bance příjemce. Ve stejném čase dochází k nahrazení závazku mezi bankou plátce a bankou příjemce za dva závazky, za závazek mezi bankou plátce a TBA a za závazek mezi bankou příjemce a TBA. Podle zadaného příkazu banka příjemce kredituje účet příjemce. Centrální banka Japonska vypočítá závazek mezi jednotlivými bankami a TBA a dojde k vyrovnání účtů.

3.5.3.4 BOJ-NET

Centrálním platebním systémem je BOJ-NET. Tento systém je RTGS systémem a byl uveden v roce 1988. V systému se denně zpracovává 21 000 transakcí v celkové výši okolo 77 trilionů JPY (634 bilionu USD). Systém se skládá ze dvou systémů: systému pro vyrovnání obchodů (BOJ-NET Funds Transfer System) a systému pro vyrovnání japonských vládních dluhopisů (BOJ-NET JGB Services). Systém je spravován centrální bankou Japonska a má 383 členů.

Účetní den trvá od 9ti do 17ti hodin. Příkazy jsou zadávány do systému přes síť BOJ-NET. Přístup do sítě je umožněn několika způsoby. Většina účastníků využívá speciálních BOJ-NET terminálů. Síť je založena na principu pronajatých linek a linek s výměnou digitálních datových paketů (tzv. digital data exchange – DDX). Tyto linky jsou poskytovány skupinou NTT, která je skupinou japonských dopravců. Oba dva typy linek se spojují v BOJ-NET Centru.

3.6 Srovnání platebních systémů

Vzhledem k tomu, že v podkapitolách zabývajících se jednotlivými platebními systémy uvádím charakteristické znaky daného systému, nebudu je v této kapitole znovu rozepisovat. Pro srovnání jsem raději zvolila tabulku, která se mi jeví přehlednější.

Oblast	**Název systému**		**Charakteristické znaky**
ČR	CERTIS		RTGS systém
EU	TARGET		RTGS systém
			Decentralizovaný -> vysoké náklady
	TARGET2		RTGS systém
			Centralizovaný (SSP)
	EBA	EURO1	Netto systém
			Vysoké objemy plateb v €
		STEP1	Komerční transakce
			Jednoduché transakce v €
		STEP2	Externí vypořádací mechanismus
			Vysoké objemy plateb v €
	SEPA		Snaha o jednotnou platební oblast
USA	Fedwire		RTGS systém
	CHIPS		Soukromý platební systém
			Bilaterální a multilaterální smlouvy
Japonsko	BOJ-NET		Státní platební systém
	BCCSs		Soukromý platební systém
			Vypořádání směnek a šeků
	Zengin		Soukromý platební systém
			Vypořádání maloobchodních transakcí
	FXYCS		Soukromý platební systém
			Přeshraniční platby v domácí měně

Tabulka č.1: Porovnání platebních systémů

Jen stěží lze provést srovnání jednotlivých platebních systémů z hlediska kvality. Některé systémy se již přežily. Takovým příkladem je platební systém TARGET, který se ukázal nevyhovující s postupem integrace v Evropě. Tento systém byl decentralizovaný a způsoboval tak vysoké finanční náklady na údržbu po přistoupení nových členských států. V současné době se v EU používá vypořádání plateb přes systémy TARGET2, EURO1, STEP1 a STEP2. Zároveň však vzniká potřeba vytvořit jednotný platební systém vyhovující všem členským státům a pracující na jednotném principu. Z toho důvodu byl započat vývoj nového platebního systému SEPA, který se nyní nachází ve stádiu projektu. Předpokládaným horizontem zavedení do provozu je rok 2010.

4 Platební protokoly

Protokolem rozumíme soubor syntaktických a sémantických pravidel, která zajišťují výměnu informací mezi minimálně dvěmi entitami. Každý protokol definuje způsob, jakým dojde k navázání spojení, definuje adresaci, specifikuje přenos dat, řízení komunikace a přidělování prostředků.

V následujících podkapitolách se budu zabývat jednotlivými platebními protokoly. První kapitola je věnována protokolům platebních karet. Vzhledem k tomu zařazuji do této podkapitoly také charakteristiku tohoto platebního nástroje, jeho dělení a informační toky při platbě platební kartou.

4.1 Standardy a protokoly platebních karet

Platební karty jsou nejstarším a v současné době i nejrozšířenějším produktem, jenž umožňuje vzdálený přístup k účtu elektronickou cestou, a to jak prostřednictvím pokladních terminálů, tak i jinými způsoby, zejména prostřednictvím Internetu.[8]

4.1.1 Platební karty

Platební karta je moderní nástroj bezhotovostního platebního styku. Využívá se zejména k úhradě spotřebních výdajů a výběru v hotovosti. Platební karta je považována za identifikační doklad, jehož rozměry (85,6 x 54 x 0,76 mm), obsahové náležitosti a fyzikální vlastnosti jsou mezinárodně standardizovány normou ISO3554. Mezi obsahové náležitosti platební karty patří:

- Označení vydavatele – název a logo příslušné banky.
- Číslo platební karty – 16 až 19 numerických znaků. První dva znaky označují druh karty, následujících 5 znaků je vyhrazeno pro identifikaci vydavatele karty a zbylé znaky pro identifikaci držitele karty.
- Část čísla BIN[9] – počáteční 4 znaky.
- Platnost platební karty – stanovení začátku a konce platnosti karty, popřípadě jen konce platnosti. Platební karta je majetkem vydavatele karty, tedy banky. Po konci platnosti karty proto banky vyžadují její navrácení.
- Jméno držitele karty – max. 27 znaků, u služebních karet i název podniku.
- Podpisový proužek – na zadní straně, vzor podpisu držitele karty.
- Záznam dat.

[8] MÁČE, M.: Platební styk klasický a elektronický. 1. vyd. Praha: Grada Publishing, a.s., 2006. s.170. ISBN 80-247-1725-5

[9] BIN – Bank Identification Number – číslo přidělené karetní asociací dané bance

Platební karty nejsou na území ČR podrobně regulovány zákonem. Dílčí úpravu obsahuje zákon č. 124/2002 Sb., o platebním styku, který upravuje vydávání a používání elektronických platebních prostředků, avšak z pohledu ochrany spotřebitele.[10]

4.1.1.1 Dělení platebních karet

Platební karty můžeme členit dle několika hledisek.

1. Dle způsobu zúčtování transakcí dělíme karty na:

- Kreditní úvěrové karty (Credit card) – jak již název napovídá, tento typ karet umožňuje držiteli čerpat spotřebitelský úvěr. K zúčtování dochází po době stanovené bankou, obvykle po jednom měsíci. Po splacení dlužné částky je možno úvěr poskytovat opakovaně (tzv. revolvingový úvěr). Velikost úvěru je stanovena tzv. úvěrovým limitem. Jeho velikost je dána bonitou klienta. Banky obvykle stanovují i minimální výši splátek, což obvykle činí 5-10% dlužné částky. Mezi tyto karty řadíme i karty vydávané leasingovými a úvěrovými společnostmi, které platí pouze v omezeném množství obchodů a většinou nedovolují bezúročné čerpání. Příkladem těchto karet může být Home Credit či OK karta.

- Debetní karty (Debit card) - tento typ karet je vydáván k běžnému účtu a slouží k hrazení plateb za zboží a služby a k výběrům hotovosti z bankomatu. Držitel nemá možnost čerpat úvěr. K zúčtování platby dochází okamžitě po zaregistrování platby bankou.

- Karty s odloženou platbou (Charge card) - tento typ karet je historicky nejstarší. Úhradu provedených plateb provádí držitel karty do sjednané doby po zaslání měsíčního výpisu od vydavatele karty. Nejedná se o nakupování na úvěr. V tomto případě držitel karty čerpá karetní úvěrový rámec. Tyto karty jsou vydávány pouze důvěryhodným klientům, které banka dobře zná a kteří mají odpovídající scoring.[11] Nejprestižnějším typem těchto karet jsou karty společnosti Dinners Club International – mezinárodní klubové karty vydávané od r. 1950. Tento produkt lze zakoupit i u nás v průměru za 5000 Kč ročně.

[10] MÁČE, M.: Platební styk klasický a elektronický. 1. vyd. Praha: Grada Publishing, a.s., 2006. s.55. ISBN 80-247-1725-5

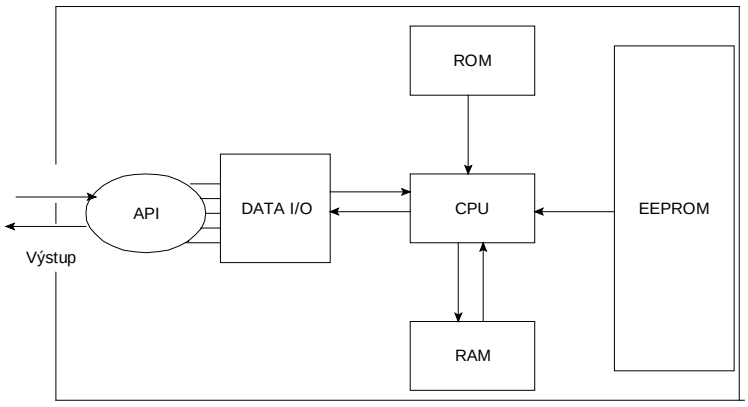
[11] scoring – metoda řízení rizika založená na statistickém odhadu pravděpodobnosti, že klient bude splácet úvěr

2. Podle záznamu dat dělíme karty na:

- Karty embosované – identifikační údaje držitele i vydavatele jsou na kartě vyraženy (embosovány). Údaje z karty jsou snímány obchodníkem na speciální formulář za použití kopírovacího mechanického snímače zvaného imprinter. Těmito kartami lze platit ve více obchodech, na rozdíl od elektronických platebních karet, kde je nutné, aby obchodník pomocí on-line platebního terminálu ověřil zůstatek účtu v bance. Cena těchto on-line terminálů totiž několikanásobně převyšuje cenu imprinterů. Daní za širší možnost uplatnění embosovaných karet je jejich dvakrát až třikrát vyšší cena než u elektronické karty. Mezi typické zástupce karet tohoto typu patří karty VISA Classic či Eurocard/MasteCard Standard.

- Karty s magnetickým pruhem – tento typ karet na sobě nese magnetický pruh se všemi potřebnými údaji. Nevýhodou tohoto typu karet je nízká ochrana proti zneužití a omezená kapacita magnetického proužku.

- Čipové karty (Smart cards) – u tohoto typu karet jsou informace uloženy v mikročipu, který se nachází na přední straně karty. Čipové karty se dále dělí na paměťové, které jsou použitelné pouze jednou (např. předplacené telefonní karty), a procesorové, kde je pomocí jednoduchého mikroprocesoru kontrolován přístup k informacím na kartě. Výhodou čipových karet je větší bezpečnost, větší množství zapsaných údajů na kartě (dle velikosti paměti čipu), levnější způsob místního ověření údajů držitele karty, např. pomocí PIN, více funkcí (zároveň lze použít jako telefonní kartu, zdravotní kartu,…). Postupně dochází k přechodu na tento typ karet.



Obr.12: Schéma čipové karty

- Karta s laserovým záznamem – data jsou zaznamenána do podkladové vrstvy laserem. Výhodou je vysoká kapacita záznamu, nevýhodou jednoduché kopírování.

- Virtuální karta – na rozdíl od předchozích typů karet nemá svou fyzickou podobu. Principem je 16ti-místné číslo a trojmístný kontrolní kód. V ČR virtuální karty poskytují zatím jen Citibank, eBanka, GE Capital Bank a KB.

3. Dle nutnosti kontaktu se čtecím zařízením karty dělíme na:

- Kontaktní – veškeré předcházející karty kromě virtuálních.
- Bezkontaktní – virtuální karty.

4. Podle vydavatele dělíme karty na:

- Karty bank a bankovních společností (VISA, EC/MC).
- Karty finančních společností (American Express).
- Karty obchodních společností.
- Karty telekomunikačních společností (předplacené telefonní karty).
- Karty leteckých společností.

5. Dle rozsahu služeb karty dělíme na:

- Základní (Mass Card) – většinou debetní karty, které jsou snadno dostupné většině klientů. Roční poplatek za vydání karty činí řádově stovky korun.
- Specializované (Business Card).
- Prestižní (Premier Card) – nároky na vydání těchto karet jsou daleko větší. U klientů se předpokládá velmi dobré finanční zajištění a vysoký scoring. Roční poplatek se pohybuje na hranici jednoho tisíce korun.
- Výběrové (Platinum Card) – tyto karty jsou nejprestižnější a roční poplatek se pohybuje v řádu tisíců korun.

6. Dle funkce a způsobu použití karty na:

- Univerzální karty určené k elektronickým a neelektronickým platebním transakcím.
- Bankomatové karty.
- Elektronické platební karty.
- Šekové záruční karty.

7. Dle teritoriálního hlediska karty dělíme na:

- Domácí, národní, tuzemské.
- Mezinárodní.

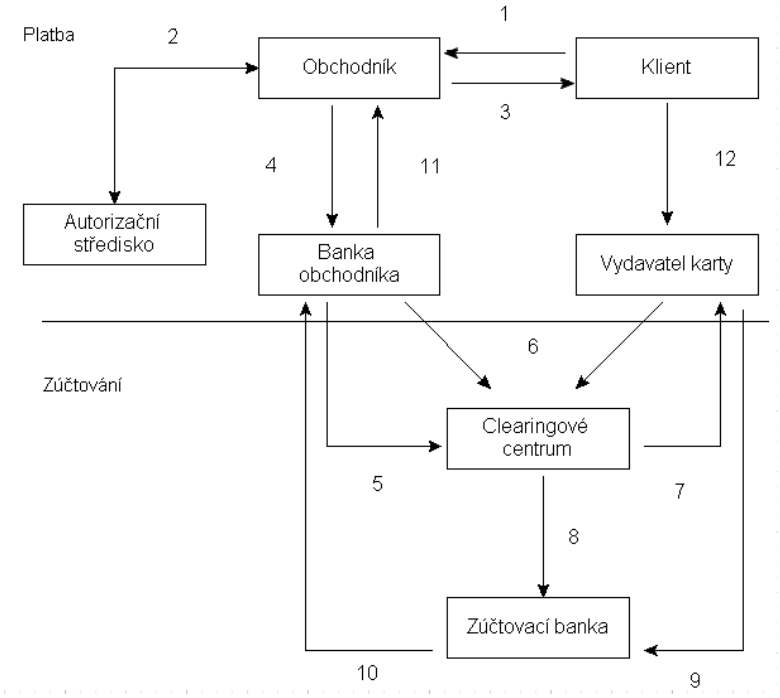
4.1.1.2 Informační toky dat při platbě platební kartou

Průběh placení kartou můžeme rozčlenit do tří základních fází. V první fázi se jedná o autorizaci požadované transakce, v další o zpracování v clearingovém centru a třetí fáze spočívá v zaúčtování probíhající transakce na účty zúčastněných stran. Autorizační centra jsou navzájem propojena přes centra karetních asociací. Společnost VISA užívá tzv. VAP, neboli Visa Access Point. Jde o spojení prostřednictvím satelitních technologií. MasterCard oproti tomu využívá komunikačního datového spojení mezi HW EM (Europay – Modul) a nově spojení skrze Network Interface Unit.[12]

Transakce probíhá následujícím způsobem. Po předložení karty obchodníkovi klientem ověří obchodník ochranné prvky na kartě (1 – viz.obr.13). Dalším krokem je autorizace (2). Autorizace slouží k ověření transakce. Spočívá jednak v kontrole ochranných prvků na kartě, kontrole platnosti karty a ověření, zda karta není na seznamu zakázaných karet. Autorizace se provádí rovněž tehdy, pokud výše transakce přesáhne autorizační limit přijímajícího místa. V tomto případě slouží autorizace jako ujištění finančního krytí transakce. Autorizaci lze provést prostřednictvím telefonu nebo Internetu dotazem na autorizační středisko, které se spojí s vydavatelem karty. Nejčastějším způsobem je transakce prováděná prostřednictvím zařízení napojeného on-line na síť propojující jednotlivé vydavatele karet. V tomto případě se autorizace provádí automaticky, klient pouze zadá pomocí klávesnice svůj PIN. Po skončení autorizace obchodník vystaví prodejní doklad (4) a banka obchodníka předá informace o platbě zúčtovacímu centru (5). Dalším krokem je clearingové zúčtování platby mezi bankou obchodníka a bankou klienta (6). Clearingové centrum předá informace o provedené platbě vydavateli karty (7) a vydá příkaz k vyrovnání sald mezi bankami (8). Dochází k zatížení nostro[13] účtu vydavatele karty (9) a převedení částky na nostro účet banky obchodníka (10). Banka obchodníka připíše částku sníženou o bankovní provize na účet obchodníka (11). Na druhé straně dochází naopak k zatížení účtu držitele karty danou částkou (12).

[12] SCHLOSSBERGER, O., HOZÁK, L.:Elektronické platební prostředky. 1. vyd. Praha: Bankovní institut, a.s., s. 91

[13] nostro účet – (náš) učet vedený korespondenční bankou tuzemské bance



Obr.13: Informační toky dat při placení kartou

4.1.1.3 Základní ochranné prvky

Ochranné prvky karet můžeme rozdělit na primární a sekundární. Mezi primární ochranné prvky řadíme snadno ověřitelné identifikační údaje jako je fotografie držitele karty, jeho podpis, popřípadě hologram na platební kartě. Existuje-li podezření, že je karta padělek, dochází ke kontrole sekundárních prvků jako je mikrotext či UV barvy. K ochraně dat na kartě slouží také řada verifikačních prvků. Nejdůležitějšími jsou PIN držitele karty, jeho podpis a biometrické prvky.

Nejstarším ochranným prvkem k ověření totožnosti klienta je PIN. Tento nástroj ovšem neposkytoval dostatečnou ochranu a byl spíše marketingovým nástrojem banky. Dnes se PIN používá jen jako doplňkový nástroj k ověření totožnosti a jeho hlavní úlohu převzala kryptologie.

Dnešní zabezpečení zajišťují také 2D, 3D hologramy a jejich kombinace. Hologramy pro karty MasterCard a VISA jsou tištěny v jedné tiskárně cenin a každý hologram má své identifikační číslo. Příkladem může být hologram u platebních karet MasterCard, který se vyznačuje:

- Dvourozměrnými kruhy vytvořenými opakovanými písmeny M C.
- Trojrozměrným globusem složeným z textu.
- Slovem MasterCard, které je vytištěno na pozadí ve dvou střídajících se barvách.
- Skrytým obrazem v rohu hologramu.

Nejmodernějším a také nejdražším ochranným prvkem jsou biometrické informace. Požadavky na biometrické prvky jsou definovány britskou asociací APACS. Prvek musí být snadno pořiditelný,

jeho pořiditelnost nesmí být klientovi nepříjemná, musí být levná, spolehlivá, rychlá, nenáročná na prostředí a zaškolení obsluhy. Vzorek musí být snadno ověřitelný. Dalšími požadavky jsou nepřenositelnost, nenapodobitelnost a stabilnost. Mezi nejznámější biometrické metody patří fotografie, otisk prstů, dynamický rozbor podpisu, rozbor hlasu a záznam sítnice oka.

Jednou z prvních společností, která v praxi aplikovala platební systém založený na identifikaci pomocí otisku prstu, byla společnost Pay by Touch. Autentizace se provádí přiložením prstu ke scanneru na platebním terminálu a zadáním vyhledávacího čísla. Poté zákazník pouze potvrdí částku a transakce je provedena. Aby mohla být autentizace provedena, klient musí být zaregistrován. Pay by Touch nepracuje přímo s otisky prstů, ale sbírá pouze určité unikátní znaky. Ze sebraných údajů nemůže být zpětně celý otisk prstu sestaven. Data jsou zašifrována a spravována v databázích IBM.

4.1.2 Jednotlivé standardy a protokoly platebních karet

V této kapitole se budu věnovat především standardům platebních karet, na které je v dnešní době zaměřena největší pozornost, tzn. na karty čipové, resp. smart karty. K nejznámějším bankovním asociacím, které se podílejí na vývoji těchto platebních systémů, patří VISA International a Europay/MasterCard. Europay a MasterCard jsou dvě nezávislé asociace, které spolu navzájem spolupracují. Europay zajišťuje vydávání platebních karet v Evropě a MasterCard mimo Evropu. K nebankovním asociacím podílejícím se na vývoji nových systémů patří American Express Company, Dinners Club International a Japan Credit Burea (JCB).

Systém	Počet karet (mil.)	Počet obchodníků (mil.)	Počet bankomatů (mil.)	Obrat (mld. USD)
VISA	1 079	21	783	1 854
Europay/MasterCard	1 700	21	604	857
American Express	51,7	5	500	296,7
JCB	36	7,3	n/a*	42
Dinners Club	8	5,9	331	35

** z anglického not acknowledge n/a - nepotvrzeno*

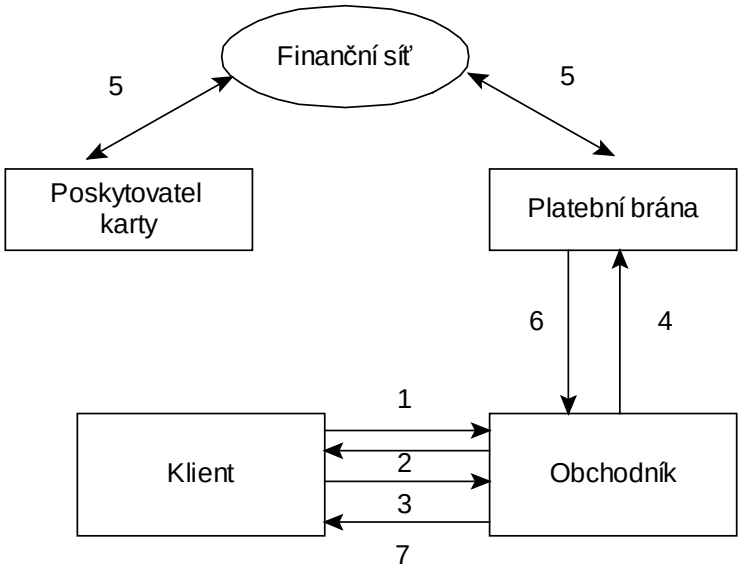
Tabulka č.2: Mezinárodní systémy v roce 2000 [14]

[14] JUŘÍK, P.: Svět platebních a identifikačních karet. 2.vyd. Praha: Grada Publishing, spol. s.r.o., 2001. s.19. ISBN 80-247-0195-2

4.1.2.1 SET, bezpečnostní prvky platebních protokolů

Secure Electronic Transaction byl uveden na trh roku 1996 společnostmi Visa a MasterCard a konsorciem jedenácti společností (např. IBM, Netscape, RSA atd.). Nový protokol se však příliš neprosadil z důvodu vysokých finančních nákladů na zavedení a z důvodu časové náročnosti.

Celá transakce začíná zasláním požadavku klienta obchodníkovi (1 – viz.obr.14). Obchodník požadavku přidělí unikátní identifikační číslo, které pošle spolu se svým certifikátem a certifikátem platební brány (X.509v3) zpět klientovi (2). Zaslané certifikáty jsou na straně klienta ověřeny a je vytvořena zpráva s informacemi o objednávce a o platbě spolu s přiděleným ID. Informace o platbě, dvojitý podpis a informace o objednávce jsou pomocí náhodně vygenerovaného symetrického klíče zašifrovány. Tento klíč je následně šifrován veřejným klíčem platební brány a vzniká digitální obálka, která se spolu s informacemi o objednávce a platbě, se dvojitým podpisem a certifikátem zákazníka odešle obchodníkovi (3). Obchodník informace pomocí digitálního podpisu překontroluje a přepošle zašifrované informace o platbě platební bráně (4). Platební brána si přes finanční síť ověří, zda má zákazník dostatečný zůstatek finančních prostředků na účtu (5). Po ověření krytí platby zašle platební brána potvrzení obchodníkovi (6), který objednávku uzavře a pošle oznámení zákazníkovi (7). Banka klienta následně převede peníze z účtu klienta na účet obchodníka.

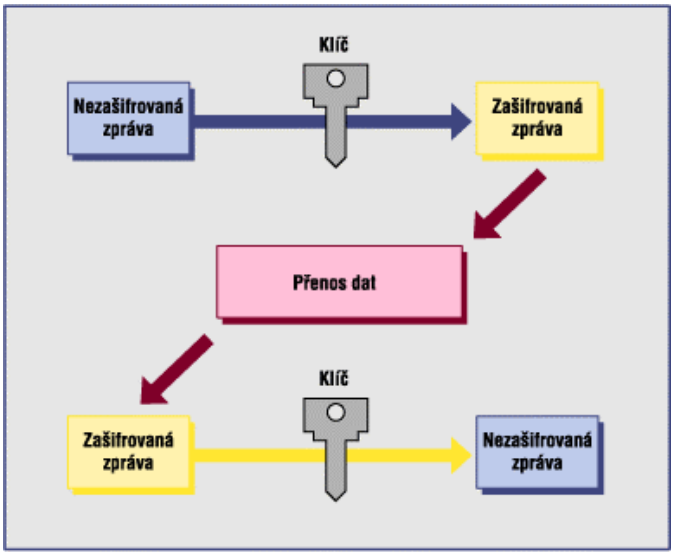


Obr.14: Průběh transakce za pomocí protokolu SET

SET využívá řadu zabezpečovacích mechanismů. Je to šifrování symetrickým klíčem, šifrování veřejným klíčem, dále hashovací funkce, digitální podpis a digitální obálka.

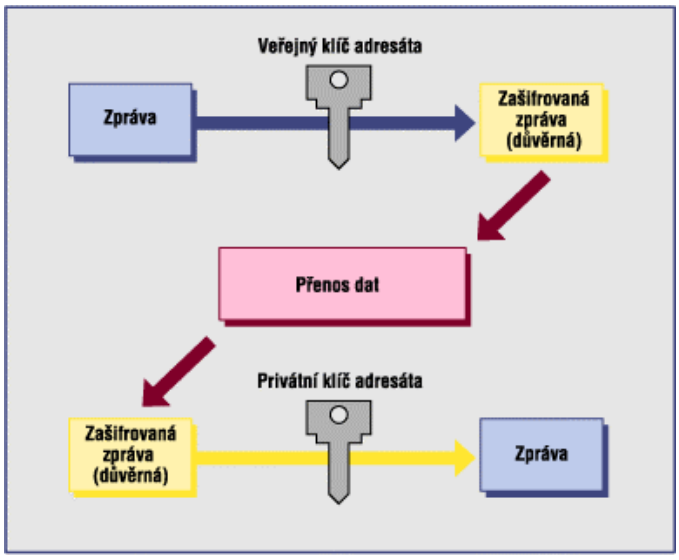
Při symetrickém šifrování je sdílen jeden stejný klíč, který je na jedné straně zašifrován a na druhé straně dešifrován. Jedná se o rychlý způsob, který ovšem přináší problém v podobě bezpečného předávání utajeného klíče. Mezi nejznámější šifrovací algoritmy patří DES, 3-DES a AES. Tento

způsob šifrování ovšem nesplňuje požadavek neodmítnutelnosti odpovědnosti. Nelze určit, která strana je odesílatelem a která příjemcem. V protokolu SET se využívá 56ti-bitového klíče šifrovaného algoritmem DES. Tento způsob se ovšem ukázal jako nedostatečný, když se zakrátko objevil moderní hardware, který dokázal tento klíč snadno rozšifrovat.



Obr.15: Symetrické šifrování [15]

Při šifrováním veřejným klíčem je použito dvou klíčů – veřejného a soukromého. Uživatel si vygeneruje oba dva klíče. Základní princip spočívá v tom, že zašifrovaná data nelze dešifrovat bez znalosti obou klíčů. Při šifrování je zpráva šifrována pomocí veřejného klíče příjemce. Příjemce zprávu dešifruje svým soukromým klíčem. K nejznámějším algoritmům patří RSA.

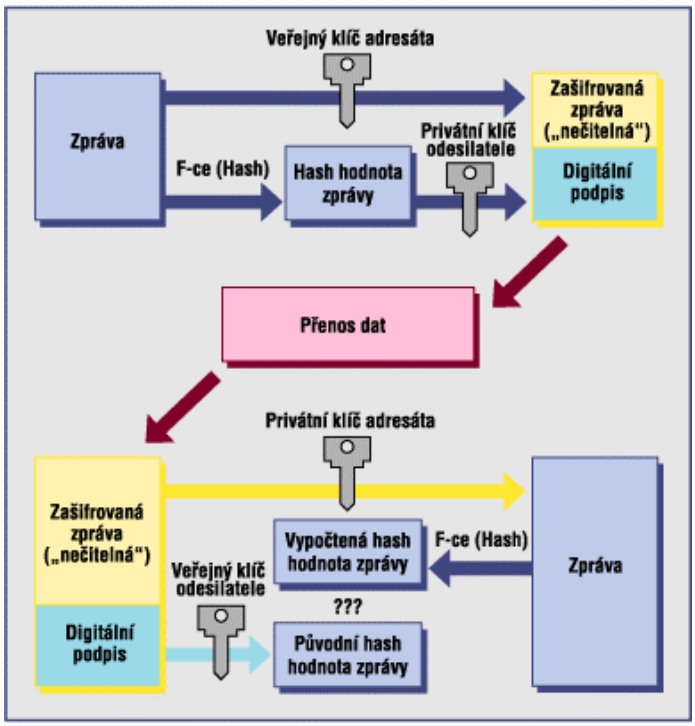


Obr.16: Asymetrické šifrování [16]

[15] Pramen: www.ica.cz
[16] Pramen: www.ica.cz

Hashovací funkce je používána jako doplňkový mechanismus. Zašifrovaná zpráva je jakýsi digitální otisk dat. Z vypočítaného hashe vstupních dat již není možné získat stejná data nazpět. K nejpoužívanějším algoritmům patří MD5 a SHA1.

Digitální podpis je implementován pomocí asymetrického šifrování a obsahuje dva algoritmy, pro podepisování a pro ověřování podpisu. Obvykle se s digitálním podpisem setkáváme pouze u hash zpráv. Hash je zašifrován pomocí privátního klíče odesílatele. Příjemce zprávy vygeneruje ze zprávy hash a porovná ho s hashem, který získá po dešifrování digitálního podpisu odesílatele.



Obr.17: Šifrování s digitálním podpisem [17]

Digitální obálka slouží k zajištění bezpečného přenosu symetrického klíče. Vygenerovaný symetrický klíč je zašifrován klíčem veřejným. Výsledný zašifrovaný klíč je odeslán. Příjemce klíč pomocí svého soukromého klíče dešifruje a pro další komunikaci používá symetrický klíč.

[17] Pramen: www.ica.cz

4.1.2.2 CSC, AVS

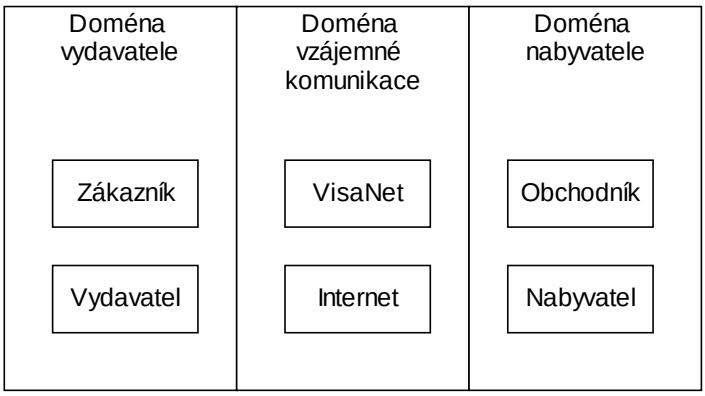
CSC (Card Security Code) je podpůrný bezpečnostní prostředek, který je vytištěn na zadní straně platební karty. Zasláním tohoto kódu vydavateli si může obchodník ověřit totožnost zákazníka. Na podobném principu pracuje i AVS (Address Verification Service). Tento prostředek slouží k ověření, zda se shoduje adresa držitele karty s adresou, která je uložena v databázi vydavatele karty. Tyto prostředky ovšem nezajišťují dostatečnou ochranu držitele karty.

4.1.2.3 Visa 3-D Secure

Visa 3-D Secure je tří-doménový zabezpečený protokol založený na principu XML. 3-D Secure je mechanismus autentizace držitele karty. Tento protokol je využíván asociací Visa i MasterCard. Hlavní rozdíl v implementaci u Visa a u MasterCard spočívá v metodě generování autentifikační hodnoty držitele karty (AAV – Accountholder Authentication Value). Společnost MasterCard používá UCAF (Universal Cardholder Authentication Field), zatímco společnost Visa používá CAVV (Cardholder Authentication Verification Value). Protokol byl přijat i nebankovní asociací JCB.

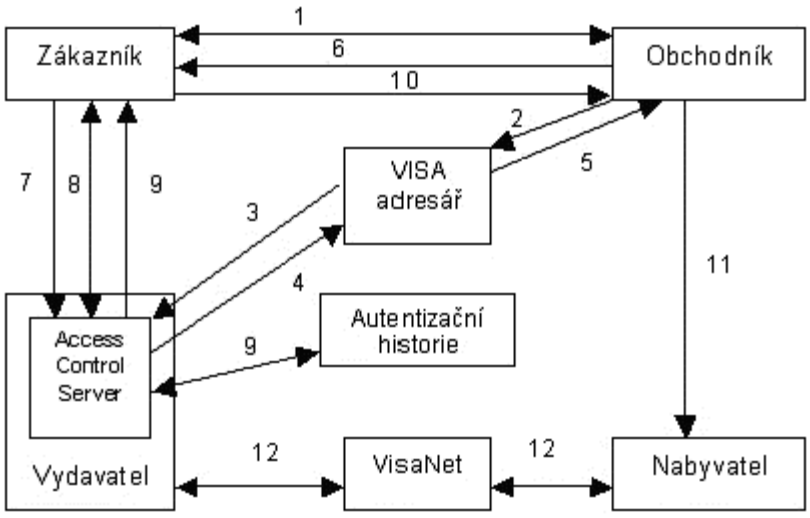
Mezi základní funkce protokolu patří přijímání a zasílání zpráv, které informují o stavu autentizace, zajištění autentizace držitele karty, vytvoření požadavku na autorizaci a požadavku na provedení transakce od obchodníka k nabyvateli. Další funkcí je provedení autorizace a transakce mezi vydavatelem a nabyvatelem přes doménu vzájemné komunikace (VisaNet).

Základními doménami systému jsou doména vydavatele (Issuer domain), doména nabyvatele (Acquirer domain) a doména vzájemné komunikace (Interoperability domain). Tyto tři domény spolu během transakce vzájemně komunikují pomocí zasílaných zpráv ve formátu XML přes TLS spojení. Aby mohla být transakce provedena, musí mít obchodník nainstalovanou Merchant plug-in komponentu (MPI) a vydavatel karty musí mít zpřístupněn Access control server (ACS), který zajišťuje autentizaci držitele karty. Informace o všech uživatelích, jejich platebních kartách a www adresách spojených s ACS jsou uloženy ve VISA adresáři – Visa Directory Server (VDS). Vydavatel karty komunikuje s držitelem přes Internetový prohlížeč, kde jsou sbírány autentizační informace. Ty jsou následně ověřeny a poslány zpět obchodníkovi jako autentizační odpověď. Do domény vzájemné komunikace můžeme zařadit také komerční certifikační autoritu a Visa certifikační autoritu.



Obr.18: Architektura Visa 3-D

Při platbě kartou se jako první zašle obchodníkovi číslo platební karty zákazníka, čímž se aktivuje obchodníkův plug-in (1 – viz.obr.19). Obchodníkův plug-in se spojí s VISA adresářem a ověří si, zda je zákazník zaregistrován (2). V případě, že ověření proběhlo v pořádku, VISA adresář instruuje plug-in, jak se spojit s ACS, kde je ověřováno, zda je karta řádně zaregistrována (3). Ten jako odpověď pošle adresáři údaje o zákazníkovi (4). Tyto informace jsou následně odeslány do obchodníkova plug-inu (5). Dalším krokem je odeslání obchodníkova požadavku na autentizaci plátce k ACS přes prohlížeč zákazníka (6,7). ACS pomocí hesla zadaného zákazníkem ověří zákazníka a odešle podepsanou odpověď MPI (8). V dalším kroku ACS odešle odpověď o autentizaci obchodníkovi přes prohlížeč zákazníka a současně odešle autentizační údaje na server autentizační historie (9,10). Obchodník vyšle požadavek na autorizaci své bance (11), která jej autorizuje bance zákazníka přes VisaNet (12). Mezi základní údaje, které se posílají při žádosti o autorizaci, patří CAVV (šifrovaná autentifikační hodnota generovaná ACS), ECI (Electronic Commerce Indicator) a XID – identifikátor transakce.



Obr.19: Průběh transakce v systému Visa 3-D

Pro zajištění bezpečnosti protokolu se používají následující technologie:

- Identifikační číslo a heslo.
- Veřejný klíč a certifikát.
- Bezpečnostní hardwarový modul.
- Digitální podpis.
- TLS

Protokol je snadno přenositelný i do zařízení jako jsou mobilní telefony, PDA a digitální televize.

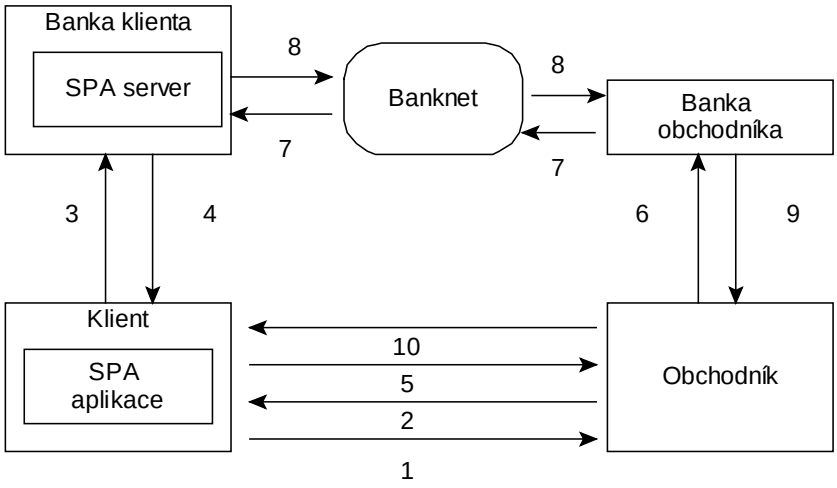
4.1.2.4 UCAF/SPA

Secure Payment Application byl představen v roce 2001 společností MasterCard. Systém je založen na UCAF (Universal Cardholder Authentication Field) s cílem minimalizovat náklady obchodníka. Systém UCAF poskytuje univerzální způsob, pomocí něhož jsou předávána autentizační data nezávisle na bezpečnostním schématu. Tento systém společnost MasterCard doplnila také o vlastní bezpečnostní schéma – SPA (Secure Payment Application).

Informace od zákazníka jsou zaslány vydavateli karty k autentizaci a autorizaci platby. Zákazník se autentizuje pomocí hesla nebo čipové karty. Vydavatel implementuje SPA server, který je zodpovědný za generování specifických bezpečnostních tokenů, nazývaných Accountholder Authentication Value (AAV), a zajišťuje distribuci SPA appletů k zákazníkům. Tokeny se zasílají obchodníkovi, jeho bance a nazpět vydavateli, který tímto transakci zkontroluje. Pro zasílání AAV byla zřízena vlastní bankovní síť Banknet.

Struktura UCAF se skládá ze dvou částí. První tvoří řada tajných, skrytých polí. Druhou částí je UCAF Authentication Data Field, tedy pole, které se nachází na obchodníkově straně. Jedná se o pole o třiceti dvou znacích, které sbírá a předává autentizační a autorizační údaje (autentizační token, čipové přihlášení, heslo a zpráva).

Pro zpracování transakcí pomocí SPA je uživatel nucen mít SPA aplikaci a musí být zaregistrován. Po výběru zboží a přistoupení k pokladně se aktivuje SPA aplikace, která začne komunikaci s obchodníkem (1 – viz.obr.20). SPA aplikace zajišťuje přenos informací od obchodníka ke klientovi (2). Klient zadává autentizační informace, které SPA aplikace přeposílá na SPA server umístěný v klientově bance (3). SPA server ověří, zda se shodují autentizační údaje poslané SPA aplikací s údaji, které jsou uloženy v databázi serveru, a vygeneruje autorizační token AAV, který odešle jako odpověď SPA aplikaci (4). Aplikace předá AAV obchodníkově straně (5). Obchodník pošle AAV a požadavek o autorizaci transakce své bance (6). Ta si krytí transakce ověří dotazem na banku klienta přes peněžní síť Banknet. Dotaz obsahuje autorizační požadavek a AAV (7). Banka klienta ověří shodu zaslané AAV s hodnotou uloženou ve své databázi a odpoví bance obchodníka (8). Ta přepošle odpověď obchodníkovi (9), který transakci potvrdí a pošle klientovi informace o proběhnuté transakci (10).



Obr.20: Průběh transakce v systému UCAF

4.1.2.5 CEPS

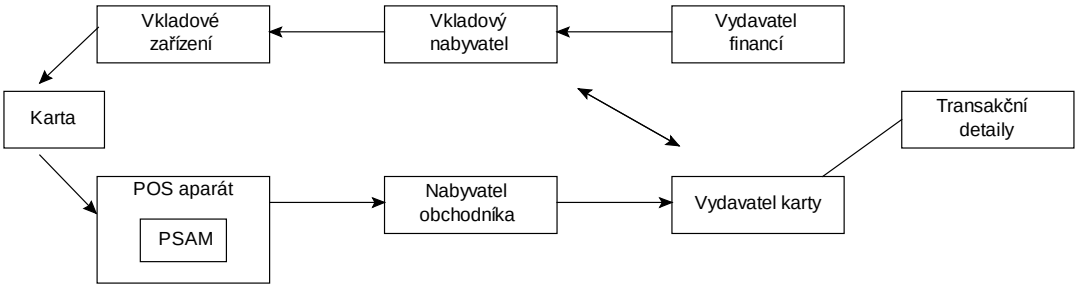
Common electronic purse specification byl vytvořen v březnu roku 1999 společností CEPSCO, LLC. Jedná se o celosvětový standard umožňující správu finančních prostředků. Pro CEPS je charakteristická kompatibilita se standardem Europay MasterCard Visa (EMV). Standard popisuje systémovou bezpečnost, specifikaci pro smart karty a požadavky pro komunikaci jednotlivých aplikací na kartě. Dále definuje rozhraní terminál – karta a specifikuje formát zasílaných zpráv pro zpracování transakcí. Pro zajištění bezpečného provedení transakce používá šifrování veřejným klíčem. Specifikace standardu je popsána ve třech dokumentech – Functional requirements, Business requirements a Technical specifications.

Mezi hlavní entity systému patří nabyvatel obchodníka, vkladový nabyvatel, vydavatel karty a vydavatel financí. Nabyvatel obchodníka umožňuje a finančně vyrovnává tzv. point-of-sale transakce (dále jen POS). Příkladem POS může být automat. Součástí POS aparátu je Purchase Secure Application Module (PSAM). PSAM zajišťuje bezpečnost uchovávaných a zpracovávaných dat, které se používají pro autentizaci transakce. Nabyvatel je odpovědný za správný chod tohoto POS zařízení. Nabyvatel musí zajistit, aby při zrušení transakce obdržel informaci o neprovedené transakci.

Vkladový nabyvatel odpovídá za autorizaci dané transakce. Vkladový nabyvatel spravuje vkladový aparát, který obsahuje informace o všech transakcích, které jsou zpracovávány. Příkladem vkladového zařízení může být i domácí počítač. Vydavatel karty poskytuje platební kartu a zároveň ručí za hotovost, která je na kartě uložena. Vydavatel musí být schopný ověřit platnost karty a ručí za všechny transakce, které obdrží.

Peníze se na kartu mohou dostat dvojím způsobem – spojeně a nespojeně. Při spojeném vkladu nedochází k přesunu peněz mezi finančními institucemi. V druhém případě se finanční prostředky přesunují od vydavatele financí do finančních rezerv vydavatele karty. Vydavatel financí autorizuje finanční prostředky, které jsou na kartu vkládány při nespojeném vkladu.

Autentizace může probíhat dvěma způsoby. Při on-line autentizaci dochází k přímé komunikaci mezi vydavatelem a platební kartou. Vydavatel karty spolu s kartou sdílí privátní klíč. Pomocí tohoto klíče jsou generovány MAC kódy (max. 8By). Při off-line autentizaci se komunikace uskutečňuje mezi PSAM a kartou. PSAM i karta užívají veřejný klíč a algoritmus RSA.



Obr.21: Hlavní entity CEPS

4.1.2.6 FINREAD

Počátek snah o vytvoření nového standardu FINREAD (akronym FINancial Transactional IC Card READer) spadá do roku 1998. Tento standard zajišťuje placení jak ve finančním sektoru, tak i v nefinančním sektoru.

FINREAD se skládá ze dvou prostředí. První prostředí je nezabezpečené a tvoří osobní prostředky uživatele. Jedná se například o počítač s připojením na Internet. Toto prostředí je spojeno se zabezpečeným prostředím, které tvoří čtečka smart karet a smart karta. Čtečka je schopna rozpoznat i karty bez smart appletů. V tomto případě pracuje v tzv. transparentním módu, který není zabezpečený.

Bezpečnost systému a odolnost proti napadení je zajištěna pomocí modulu FCR (FINREAD Card Reader), který pracuje se soukromým klíčem. FCR zajišťuje integritu přenášených dat a autenticitu uživatele. Data jsou přenášena v podepsaných paketech. Pro šifrování paketů se používá algoritmus SHA-1. Mezi další základní šifrovací algoritmy implementované v systému patří DES, 3DES, RSA a MD5. Veškeré přenosy citlivých informací jsou v souladu s AES (Advanced Electronic Signature).

4.1.2.7 EMV

Tento standard byl vyvinut v roce 1994 společnostmi Europay, MasterCard a Visa za účelem zjednodušit přechod od magnetických karet k čipovým. V roce 1999 byla založena společnost EMVCo LLC, která dohlíží nad úpravami tohoto standardu. Systém zajišťuje kompatibilitu všech čipových karet s jakýmikoliv EMV terminály.

Systém obsahuje funkce pro komunikaci karet s terminálem, definuje jakým způsobem spolu karta a terminál komunikují a jaké aplikace mají společné, dále specifikuje systém autentizace, minimální bezpečností požadavky a rizikový management terminálů.

Původní verze EMV'96 v. 3.1.1 byla v praxi používána až do roku 2002, kdy byla nahrazena novější verzí EMV 2000. Specifikace nynější verze se skládá ze čtyř dokumentů. První část (Application independent ICC to Terminal Interface requirements) obsahuje minimální požadavky na funkci integrovaných obvodů na kartě a v terminálu, popisuje rozhraní pro výměnu dat, částečně popisuje protokoly používané pro výměnu dat a strukturu souborů na kartě. Druhá část (Security and Key Management) je zaměřena na bezpečnost systému. Definuje základní bezpečnostní požadavky a správu šifrovacích klíčů. Třetí část (Application Specification) definuje nutné požadavky pro efektivní placení. Poslední část (Cardholder, Attendant, and Acquire Interface Requirements) se zaměřuje na podmínky, které musí splňovat terminály.

4.1.2.8 EEP

Standard European electronic purse byl vytvořen organizací European Committee for Banking Standards (ECBS) v roce 1999. Standard byl vytvořen pro platební karty, na kterých jsou uloženy peníze v různých měnách společně s euroměnou.

Specifikaci standardu tvoří čtyři zprávy. V první (Transaction Message Flow) jsou definovány toky dat a základní operace, které standard umožňuje, tj. placení, přírůstkovou platbu, změnu a zrušení platby, nabití, směnu peněz, sledování zůstatku a provedených operací. Druhá část (Detailed Functional Specification) popisuje detaily funkční specifikace. Vychází ze standardu CEN pro Inter-sector Electronic Purse a EMV'96 ICC specifikace pro platební systémy. V dalším dokumentu (Data Dictionary) je specifikován formát zasílaných zpráv. Poslední dokument (Minimum Technical Requirements) obsahuje technické požadavky na terminály, pracující s EEP transakcemi. Tyto dokumenty se staly základem pro vyvoření specifikace Identification card systems.

4.2 Další platební protokoly

4.2.1 BIPS, NPP

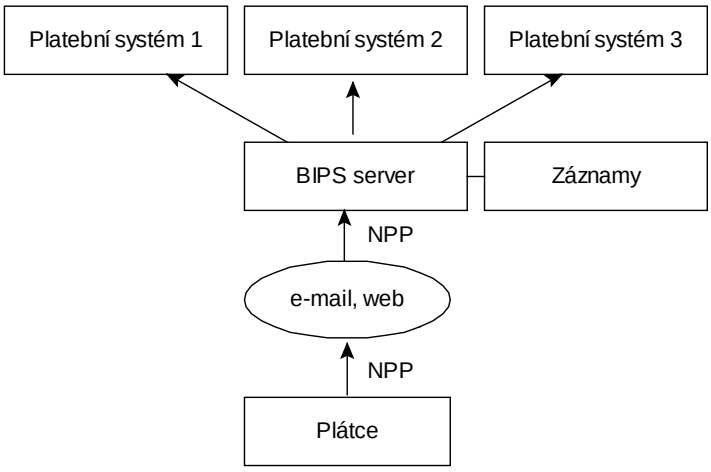
The Bank Internet Payment System byl uveden v roce 1998 díky požadavkům na vytvoření protokolu, který by umožňoval rozvoj B2B transakcí[19] přes volně dostupnou síť Internet. Systém je schopen zpracovávat transakce s vysokou i nízkou hodnotou. Obchodníci mohou zasílat platební příkazy do své banky přes síť Internet. Na straně banky je BIPS server, který instrukci přeloží a pošle danému platebnímu systému. BIPS server představuje mezistupeň mezi obchodníkem a ostatními platebními systémy, na které je napojen. Plátce komunikuje se svou bankou dvěma způsoby – e-mailem nebo přes internetový prohlížeč.

Protokol je založen na systému zasílání požadavků a odpovědí. Požadavky musí splňovat základní podmínky. Každý požadavek musí být proveditelný. Plátci musí být umožněno dohodnout se se svou bankou na daném platebním mechanismu. Požadavek musí splňovat podmínku úplnosti a aktuálnosti. Struktura požadavku musí obsahovat všechny potřebné údaje k provedení instrukce (částka, příjemce, plátce, den splatnosti atd.). Po zaslání tzv. stavového požadavku musí být plátci umožněno dozvědět se informace o stavu dřívějších instrukcí. Posledním typem požadavku je požadavek přerušení, který slouží k pozastavení nebo ukončení předchozích instrukcí.

Pro zajištění bezpečného přenosu informací a dat se používá infrastruktura veřejných klíčů (PKI) a digitální podpis (vytvářen na základě certifikátu X.509, který vlastní každý účastník systému). Digitální podpis je šifrován do ASCII znaků s kódováním Base64, kde je pro každý znak vyhrazeno 6 bitů. Všechny instrukce jsou opatřeny digitálním podpisem a certifikátem odesílatele spolu s unikátním identifikátorem transakce.

Na základech protokolu BIPS byl vytvořen Network Payment Protocol. Jádro protokolu tvoří jazyk XML (Extensible Markup Language). Protokol je podobně jako u BIPS založen na systému zasílání zpráv, které se skládají z několika polí. Každá NPP zpráva obsahuje informace o typu platby, plátci, příjemci, částce. Všechny zprávy jsou ukládány. Autentizace je založena na architektuře UCAF/SPA. Zprávy jsou symetricky šifrovány za použití algoritmu DES v ECB módu.

[19] B2B transakce – Business to Business – obchodování mezi obchodníky navzájem



Obr.22: Architektura systému BIPS

4.2.2 FSML

Financial Services Markup Language je značkovací jazyk, který byl vytvořen finančním konsorciem FSTC (Financial Services Technology Consortium) jako jazyk na podepisování finančních dokumentů a tvorbu elektronického šeku. Počátky tvorby FSML sahají do roku 1995. FSML byl implementován skupinou s názvem Electronic Check Project.

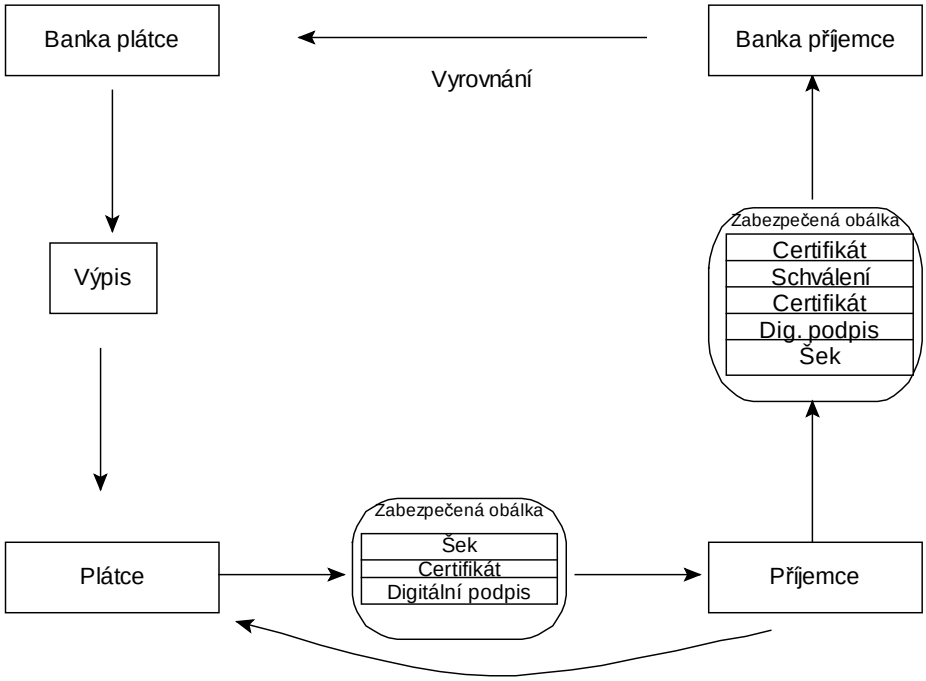
FSML specifikuje v jakém pořadí a jakým způsobem sestavit dokument do bloků. Dokument je následně podepsán. FSML umožňuje podepisovat i jednotlivé bloky dokumentu. FSML umožňuje přidávat a mazat jednotlivé bloky bez zneplatnění předchozího podpisu. Podpisy a připojené certifikáty (X.509) se stávají součástí FSML dokumentu a mohou být verifikovány dalšími příjemci dokumentu. FSML nedefinuje vlastní šifrování, ale využívá infrastrukturu PKI.

Každý blok se skládá z bloku popisujícího akce, které má příjemce provést, dále z tzv. podpisového bloku, který obsahuje podpisy a hashe všech podepsaných bloků, dále z certifikátu, z připojeného FSML dokumentu, ze zprávy informující například o chybách během přenosu. Posledním blokem je blok definovaný předchozím příjemcem.

Používá-li se protokol k definování struktury elektronického šeku, skládá se šek z následujících bloků:

- Blok akcí.
- Podpisový blok.
- Blok elektronického šeku.
- Blok obsahující stvrzenku.

- Indosament.[20]
- Certifikaci.
- Blok s informacemi o účtu.
- Veřejný klíč.
- Připojený FSML dokument.
- Faktura obsahující informace o platbě.
- Zpráva.
- Blok obsahující informace o stavu procesu.
- Blok s celkovým součtem.
- Blok definovaný uživatelem.



Obr.23: Elektronický šek

[20] indosament – rubopis – písemný projev vůle, kterým dosavadní majitel projevuje vůli převést šek na někoho jiného

4.2.3 HBCI

Homebanking Computer Interface je systém vytvořený konsorciem německých bank (Sparkasse, Volksbanken und Raiffeisenbanken a Bundesverband deutscher Banken). HBCI byl uveřejněn 1.10.1997. Zatímco protokoly OFX (Open Financial Exchange), IFX (Interactive Financial Exchange) nebo SET byly ušity na míru severoamerickému trhu, HBCI je protokol splňující požadavky trhu evropského.

Základními vlastnostmi protokolu jsou nezávislost na platformě a šifrování pomocí DES a RSA. Klíč je pro větší bezpečnost uložen na čipové kartě. HBCI definuje komunikaci mezi klientem a bankovními servery. Zasílané zprávy používají znakovou sadu ISO 8859. Každá zpráva obsahuje hlavičku, podpisové hlavičky, obchodní segmenty, podpisový trailer a trailer zprávy. Nepovinou součástí zprávy je tzv. šifrovací hlavička.

Pro zajištění bezpečného přenosu zpráv využívá protokol šifrování algoritmem RSA. Pro přístup klienta do bankovního systému je používáno heslo, které umožňuje jeho autorizaci. RSA algoritmus vytvoří unikátní digitální podpis. Ke kontrole integrity dat zprávy se používá hash kód, který je umístěn ve zprávě. Jedná se o jakýsi kontrolní součet. Server banky tento unikátní kód ověří a pokud došlo ke změně zprávy během přenosu, může zprávu odmítnout.

HBCI byl nahrazen svým nástupcem FinTS (Financial Transaction Services), ale většina bank v Německu stále používá protokol HBCI.

4.2.4 ECML

Electronic Commerce Modeling Language vznikl s cílem zjednodušit platby přes Internet. Neustálé vyplňování osobních klientských údajů zákazníky obtěžovalo, na základě čehož docházelo ke stornování započatých objednávek. Proto byl konsorciem Wallet/Merchant Standards Alliance vyvinut jazyk ECML, který pomáhá například elektronickým peněženkám efektivně vyplňovat údaje o zákazníkovi při zadávání objednávky. ECML je kompatibilní se všemi platebními systémy. Hlavním úkolem standardu je poskytovat obchodníkovi jednoduché jednotné formuláře. ECML je volně dostupný, k jeho používání není nutná licence. Pro bezpečný přenos informací se využívá SSL/TLS šifrování nebo IPSec.

4.2.5 OFX

Open Financial Exchange protokol byl představen 16.1.1997 společnostmi Microsoft, Intuit a CheckFree. Přínosem tohoto standardu je, že dovoluje přímou komunikaci mezi klienty a bankou. OFX vychází z jazykové rodiny SGML (Standard Generalized Markup Language). OFX byl původně vytvořen jako protokol nezávislý na jiném protokolu, ale už verze 1.0-1.6 využívaly skriptů rozhraní CGI (Common Gateway Interface) a komunikaci přes protokol TCP (Transmission Control Protocol).

Protokol je založen na principu dotaz-odpověď. Zasílané zprávy jsou ve formátu XML. Požadavky jsou zasílány na server ve formě http POST příkazu. Server požadavek zpracuje a odešle odpověď. K autentifikaci používá protokol certifikátů a k zabezpečení zpráv šifrovací algoritmus RSA.

4.3 Srovnání protokolů

Pro porovnání protokolů jsem zvolila následující kritéria: geografické hledisko, kritérium využitelnosti a bezpečnostní kritérium.

Dle geografického hlediska můžeme protokoly rozdělit na celosvětově používané protokoly, na ty, které byly vytvořeny pro severoamerický trh, a na protokoly ušité na míru podmínkám evropskému trhu. K celosvětově používaným protokolům patří protokoly vyvinuté společnostmi Visa a MasterCard. Ze spolupráce těchto společností vznikl protokol SET, který se však v oblasti elektronických plateb příliš neprosadil z důvodu vysokých finančních nákladů, časové náročnosti a složité implementovatelnosti. Dalším protokolem, který vznikl ze spolupráce těchto společností byl EMV. Spolupráce těchto společností postupně přešla do konkurence a každá společnost přichází se svým vlastním mezinárodně používaným standardem. U společnosti Visa hovoříme o standardu Visa 3-D Secure a v případě společnosti MasterCard se jedná o standard UCAF/SPA. Konkurence těchto významných společností přinesla řadu negativních dopadů. Nejvíce tuto skutečnost pocítili obchodníci, kteří byli nuceni investovat finanční prostředky do obou technologií, aby nepřišli o své zákazníky. Obchodníci, kteří tak neučinili, omezují zákazníky, protože ti potom musejí nakupovat pouze v obchodech, kde je možnost platit jejich platební kartou. K standardům vytvořeným speciálně pro oblast Ameriky patří protokoly OFX nebo již zmiňovaný SET. Pro oblast Evropy byly speciálně vytvořeny protokoly HBCI nebo FinTS.

Při pohledu na standardy dle jejich využitelnosti můžeme rozlišit několik základních skupin. První skupinu tvoří standardy věnované platebním kartám. K nejvýznamnějším patří opět Visa 3-D Secure a UCAF/SPA. Do této skupiny můžeme dále zařadit standard CEPS, orientovaný na smart karty, standard FINREAD, který zajišťuje platbu jak ve finančním, tak i nefinančním sektoru, a standard EMV, jehož cílem bylo usnadnit přechod od magnetických karet k čipovým. Další skupinu tvoří podpůrné bezpečnostní prostředky, které mohou být součástí jiných standardů nebo platebních systémů. Sem můžeme zařadit například mechanismy CSC, AVS nebo jazyk ECML, který zjednodušuje vyplňování objednávkových formulářů a je i součástí standardů od společnosti Visa. Poslední skupinu tvoří standardy orientované na speciální bankovní operace. Do této skupiny patří například standard FSML, který je využíván při tvorbě elektronického šeku.

Z hlediska bezpečnosti lze konstatovat, že všechny protokoly využívají pro zajištění svého systému před napadením řadu ochranných prvků. Mezi základní ochranné prvky patří šifrování

přenášených zpráv, digitální podpis, certifikáty, infrastruktura veřejných klíčů. Základním bezpečnostním mechanismem, který můžeme najít u většiny standardů, je SSL. Protokol SET využívá, mimo jiných bezpečnostních prvků, šifrování 56ti-bitového klíče algoritmem DES. Tento způsob se brzy ukázal jako nedostačující. Častým způsobem pro zajištění bezpečnosti je využívání certifikátů nebo podepisování odesílaných dat digitálním podpisem. Tento způsob ochrany můžeme nalézt u standardů SET, Visa 3-D Secure, CEPS, HBCI nebo BIPS. Častá je také implementace speciálních modulů, které se otázkou bezpečnosti zabývají. Se speciálními moduly se můžeme setkat u standardů FINREAD (modul FCR) nebo CEPS (PSAM).

Nabízí se otázka, který ze standardů je nejlepší. Dle mého názoru však nelze dát na tuto otázku jednoznačnou odpověď. Domnívám se, že výběr daného standardu závisí na lokální legislativě, na způsobu využití a na stupni zabezpečení.

5 Formalizace Visa 3-D Secure

Formalizací protokolu rozumíme vytvoření matematického modelu protokolu, nejčastěji za použití bezkontextových gramatik. Matematické vyjádření protokolu se využívá k ověření bezpečnosti protokolu a následné verifikaci.

Protokol Visa 3-D Secure jsem si vybrala proto, že je to v dnešní době nejpoužívanější platební protokol v oblasti platebních karet. V případě protokolu Visa 3-D hovoříme o tzv. víceúrovňovém protokolu. To znamená, že protokol využívá služeb bezpečných kanálů, které mohou být součástí implementace některého jiného protokolu.

V modelu jednoúrovňového protokolu (Dolev Yao) předpokládáme, že útočník monitoruje celou síť, opětovně přeposílá zachycené zprávy, ale není schopen rozluštit zašifrovaný text. Tato skutečnost naznačuje, že útočník je schopen manipulovat s transportním protokolem. Tento útok nebývá pro víceúrovňové protokoly typický. Víceúrovňový protokol předpokládá, že žádný útočník není stejného typu jako v modelu Dolev Yao, že útočník nemůže ovlivňovat spodní vrstvu protokolu, která je považována za bezpečnou. Rovněž se předpokládá, že útočník není schopen manipulovat s transportním protokolem.

Pro ověřování protokolu jsem si vybrala nástroj Casper, který zjednodušuje formální zápis protokolu a je založen na generování CSP[21] procesů. Výstup programu je následně vstupem pro kontrolor FDR, který ověří bezpečnost protokolu.

[21] CSP – Communicating Sequential Processes

5.1 Casper

Nástroj Casper vznikl na Oxford University a je zaměřen na automatickou tvorbu CSP popisu protokolů. Jedná se o kompilátor, který zjednodušuje složitý zápis protokolu a generuje CSP procesy a z jednoduchého zápisu protokolu následně generuje CSP kód. Zdrojový kód je s příponou `.spl` a skládá se ze dvou částí – první je definice protokolu, operátorů a druhá část je tvořena systémem, který má být kontrolován. Každá část se dále skládá z dalších podčástí – definice proměnných, procesů, popisu samotného protokolu, specifikace, aktuálních proměnných, funkcí, systému a narušitele. Zdrojový kód je převeden na CSP systém. Jednotliví agenti systému jsou reprezentováni procesy a komunikace mezi agenty je popsána v CSP notaci. Narušitel systému je rovněž modelován jako proces. Výstup kompilátoru je současně vstupem FDR[22] kontroloru, jehož úkolem je ověřit, zda protokol odpovídá všem bezpečnostním požadavkům. V případě, že protokol nesplňuje některý z bezpečnostních požadavků, informuje nás výstup FDR o tom, jakým způsobem je možné protokol napadnout. Tento zápis Casper zpětně přetransformuje do podoby, z níž zjistíme, která zpráva je v protokolu riziková.

5.2 Definice protokolu

První část skriptu se skládá z popisu protokolu, definice proměnných, definice procesů a požadavků na protokol. Jednotlivým částem budou věnovány následující podkapitoly.

5.2.1 Popis protokolu

Formální model protokolu představuje množinu událostí, které mohou v protokolu nastat. V našem případě se jedná o množinu zasílaných zpráv. Před začátkem psaní kódu je potřeba nadefinovat sekvenci zpráv protokolu. K tomuto použijeme hlavičku `#Protocol description`.

Abychom zaznamenali skutečnost, že je známo, mezi kým bude komunikace probíhat, je nutné na začátek přidat jedno pravidlo. Předpokládáme, že běh protokolu iniciuje klient, který obdrží nějakou zprávu od obchodníka nebo z okolního prostředí.

```
0. -> A : B
```

Absence pole odesílatele značí, že zpráva je poslána prostředím. Předpokládáme, že tento typ zprávy nemůže být odchycen narušitelem ani být podvrhnut.

---

[22] FDR – Failures – Divergence Refinement

Jakmile si klient vybere zboží, zašle požadavek na koupi zboží. Obchodníkovi zašle detaily o své platební kartě (číslo karty - `pan` a den vypršení platnosti - `exp`) zašifrované klíčem sezení. Expirační den nemůže nastat dříve než za měsíc. Všechny zprávy zasílané v protokolu jsou ve formátu XML. Zprávy se skládají z povinných, podmíněných a nepovinných polí. Pro bezpečný přenos zpráv je používáno SSL spojení. Každá zpráva je zašifrována SSL klíčem, který je sdílen oběma komunikujícími stranami. Pro vyjádření zaslané zprávy Casper využívá zápis *{m}{k}*. Zpráva *m* je zašifrována klíčem *k*.

```
--pozadavek na koupi
1. A -> B: {pan,exp}{KAB}
```

Plug-in na straně obchodníka se spojí s Visa directory serverem (VDS) – zašle zprávu `VEReq` (Verify Enrollment Request) . Obchodníkův plug-in zašle VDS číslo karty klienta (`pan`), nabyvatelův osobní kód (`acqBIN` – zpravidla šestimístné číslo přiřazené nabyvateli od společnosti VISA), identifikátor obchodníka (`merid` – 1-24 znaků) a heslo obchodníka, které získá od své banky (`merpass` – osmimístné, alfanumerické znaky).

```
--VERReq
2a. B -> VDS: {pan,acqbin,merid,merpass}{KVDSB}
```

VDS ověří platnost účtu, autentizuje obchodníka (na základě hesla nebo certifikátu) a přepošle získané informace ACS k ověření.

```
2b. VDS -> ACS: {pan,acqbin,merid,merpass}{KACSVDS}
```

Odpovědí ACS serveru, která je přes VDS poslána obchodníkovi, je zpráva `VERes` (Verify Enrollment Response), která ověří platnost karty zákazníka. Prvním polem zprávy je pole, které indikuje, zda identifikátor účtu byl autentizován – pole tvoří jeden znak (`Y` – ověření proběhlo v pořádku, `N` – klient není účastníkem, `U` – ověření nebylo možno provést). Další pole je tvořeno datovým řetězcem o délce 1 – 28 znaků (`acctid`), který identifikuje účet. Tento řetězec nesmí odkrývat číslo účtu a musí být generován algoritmem, který zaručuje unikátní hodnotu. Toto pole je vyžadováno pokud ověření proběhlo v pořádku. Následující pole zprávy `url` obsahuje URL adresu ACS, na který je následně posílána žádost o autorizaci platby. Posledním polem zprávy je označení platebního protokolu. Jedinou definovanou hodnotou je *„ThreeDSecure“*.

```
--VERes
3a. ACS -> VDS: {Y,acctid,url,protocol}{KACSVDS}
3b. VDS -> B: {Y,acctid,url,protocol}{KVDSB}
```

Po obdržení odpovědi plug-in obchodníka vygeneruje žádost o ověření plátce a odešle ji ACS přes prohlížeč držitele karty (`PAReq` – Payer authentication request). Zasílaná zpráva se skládá z nabyvatelova osobního kódu (`acqbin`), z identifikátoru obchodníka (`merid`), dále ze jména obchodníka (`mername`), z kódu země obchodníka (`mercnt` – 3 znaky), z URL adresy obchodníka (`merurl`), z identifikátoru transakce, který určí obchodník (`purxid`). Identifikátor transakce obsahuje 20ti-bytovou hodnotu, která je zakódovaná do 28 bytů. Dalším polem zprávy je datum a čas nákupu (`purdate` - ve světovém čase – YYYYMMDD HH:MM:SS = 17 znaků). Následující pole zprávy obsahuje cenu nákupu (`puramnt`) a skládá se z 1 –12 znaků. Následujícím nutným polem zprávy je identifikace účtu (`acctid`). Posledním nezbytným polem je pole obsahující expirační den (`exp` – 4 znaky: YYMM).

Skutečnost, že klient není schopen zaslanou zprávu rozšifrovat, ale pouze ji předat dál ACS, je zapsána pomocí %-notace. Využívá se zápisu *m%v*, který říká, že příjemce zprávy není schopen zprávu *m* dešifrovat, ale pouze ji vyzvednout v podobě proměnné *v*. Naopak zápis *v%m* říká, že odesílatel pošle zprávu uloženou v proměnné *v* a příjemce je schopen ji dešifrovat a získat uloženou zprávu *m*.

```
--PAReq
4a. B -> A:
{{acqbin,merid,mername,mercnt,merurl,purxid,purdate,puramnt,
acctid,exp}{SK(B)}% msg1}{KAB}
4b. A -> ACS:
{msg1 % {acqbin,merid,mername,mercnt,merurl,purxid,purdate,
puramnt,acctid,exp}{SK(B)} } {KACSA}
```

ACS následovně pošle zákazníkovi žádost o autorizaci platby. Žádost obsahuje zákazníkem definovanou zprávu a dotaz na ověřovací informace.

```
--ATReq
5. ACS -> A: {mername,puramnt,purdate,pansh,exp}{KACSA}
```

Klient zadá heslo a zpráva je odeslána zpět ACS.

```
--ATRes
6. A -> ACS: {pass}{KACSA}
```

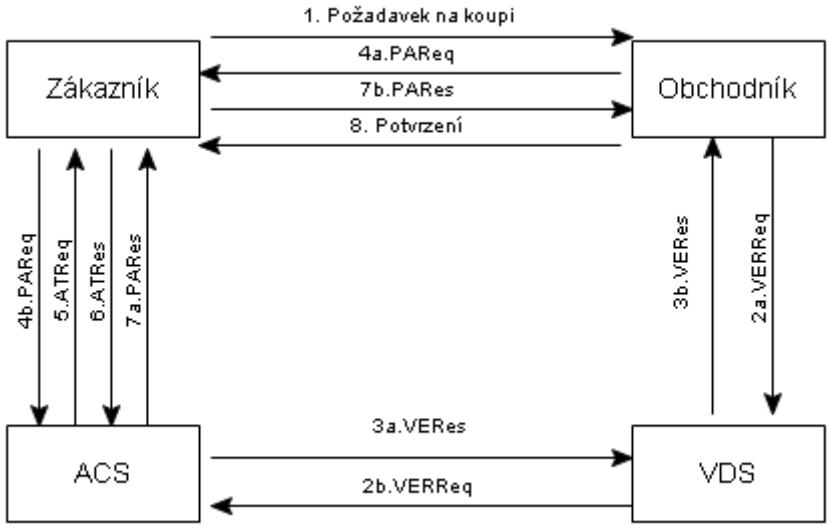
V případě, že ověření držitele karty proběhlo v pořádku, ACS odešle přes prohlížeč zákazníka odpověď obchodníkovi (`PARes`). Zpráva se skládá z osobního kódu nabyvatele (`acqbin`), identifikátoru obchodníka (`merid`), identifikátoru platby (`purxid`), data koupě (`purdate`), z ceny nákupu (`puramnt`), zkráceného čísla účtu (`pansh`). Dalším polem zprávy je datum a čas potvrzení zprávy ACS (`txtime`), pole indikující status transakce (`txstat`), pole obsahující CAVV (`cavv` – Cardholder Authentication Verification Value – ověřovací šifrovaná hodnota generovaná ACS), dále pole s ECI (`eci` – Electronic Commerce Indicator). Pole s hodnotou ECI znázorňuje stupeň zabezpečení a skládá se ze dvou číslic. Posledním nutným polem zprávy je pole `cavvalg`, které udává algoritmus použitý k vygenerování hodnoty CAVV.

```
--PARes
7a. ACS -> A:
{{acqbin,merid,purxid,purdate,puramnt,pansh,txtime,txstat,cavv,eci,
cavvalg}{SK(ACS)} % msg2} {KACSA}
7b. A -> B:
{msg2%{acqbin,merid,purxid,purdate,puramnt,pansh,txtime,txstat,cavv,
eci,cavvalg}{SK(ACS)}}{KAB}
```

Plug-in obchodníka následně vygeneruje potvrzení, které zašle zákazníkovi. Autorizační token bude zaslán nabyvateli pro následné vyrovnání platby.

```
--potvrzení
8. B -> A: {{txstat}{KAB}}{SK(B)}
```

Popis protokolu ve formě nákresu zasílaných zpráv znázorňuje následující obrázek.



Obr. č. 24: Zprávy protokolu Visa 3-D Secure

5.2.2 Definice proměnných

Za samotným popisem protokolu následuje definice používaných proměnných pod hlavičkou `#Free variables`.

```
#Free variables
A,B,VDS,ACS: Agent
pan, exp, acqbin, merid, merpass, acctid, url, protocol, Y, mername,
mercnt, merurl, purxid, purdate, puramnt, pansh, pass, txtime,
txstat, cavv, eci, cavvalg : Nonce
PK : Agent -> PublicKey
SK : Agent -> SecretKey
KAB,KVDSB,KACSVDS,KACSA : SessionKey
```

Název proměnné	Význam
A	Zákazník
acctid	Identifikace účtu
acqbin	Kód nabyvatele
ACS	Access Control Server
B	Obchodník
cavv	Ověřovací hodnota
cavvalg	Algoritmus generující CAVV
eci	Indikátor obchodní transakce
exp	Expirační den (den vypršení platnosti)
KAB, KVDSB, KACSVDS, KACSA	Session klíče
mercnt	Kód země obchodníka
merid	Identifikátor obchodníka
mername	Jméno obchodníka
merpass	Heslo obchodníka
merurl	URL adresa obchodníka
pan	Číslo účtu
pansh	Zkrácené číslo účtu
pass	Heslo klienta k ověření u ACS
protocol	Používaný platební protokol
puramnt	Cena nákupu
purdate	Datum a čas nákupu
purxid	Identifikátor transakce
txstat	Status transakce
txtime	Datum a čas potvrzení zprávy u ACS
url	URL adresa ACS
VDS	Visa Directory Server
Y	Znak indikující ověření účtu

Tabulka č.3: Přehled proměnných protokolu

Dále nadefinujeme, které klíče jsou mezi sebou vzájemně inverzní:

```
InverseKeys =
(PK,SK),(KAB,KAB),(KVDSB,KVDSB),(KACSVDS,KACSVDS),(KACSA,KACSA)
```

5.2.3 Definice procesů

Každý agent je v systému reprezentován jako CSP proces (Communicating Sequential Processes). Agenti jsou definováni následovně:

```
#Processes
INITIATOR (A,B,VDS,ACS,pan,exp,pansh,pass,KAB,KACSA) knows PK
RESPONDER(B,A,VDS,ACS,acqbin,merid,merurl,mername,merpass,mercnt,
purxid,purdate,puramnt,KAB,KVDSB) knows PK,SK(B)
SERVER (VDS,A,B,ACS,KVDSB,KACSVDS) knows PK,SK(VDS)
ACQ(ACS,VDS,A,B,pansh,txtime,acctid,protocol,url,Y,txstat,cavv,eci,
cavvalg,KACSVDS,KACSA) knows PK,SK(ACS)
```

Tyto definice dávají jednotlivým agentům jednoznačné role. Tato jména jsou také jména CSP procesů, které reprezentují jednotlivé agenty. Pomocí klíčového slova `knows` nadefinujeme, které klíče jednotliví agenti znají před začátkem běhu protokolu. Kdykoliv agent posílá zprávu, musí znát veškeré její složky, aby byl schopen ji sestavit.

5.2.4 Požadavky na protokol

Bezpečnostní požadavky, které klademe na protokol, definujeme pod hlavičkou `#Specification.` Požadavky, které začínají klíčovým slovem `Secret,` určují, že daná data jsou tajná. Například pravidlo *Secret(A,v,[*B_1 *,…,*B_n*])* říká, že agent *A* předpokládá, že hodnota proměnné *v* je utajená a je známa pouze agentům $B_1,\ldots,B_n$. Naproti tomu požadavky, které uvozuje klíčové slovo `Agreement,` značí specifikaci autentizace. Pravidlo *Agreement(A,B,[*$v_1,\ldots,v_n$*])* potom značí, že agent *A* se dohodl s agentem *B* na tom, že autentizace *A* u *B* bude probíhat zasláním proměnných $v_1,\ldots,v_n$.

Důležitým bezpečnostním požadavkem kladeným na protokol je, aby byla zachována bezpečnost přenášených dat. Zákazníkovo číslo účtu může v protokolu znát jen obchodník, kterému číslo účtu sdělí sám klient. Dále číslo účtu zná VDS, který ověřuje platnost účtu, a dále ACS, který se na ověřování rovněž podílí. Toto pravidlo zapíšeme následovně:

```
Secret(A,pan,[B,ACS,VDS])
```

Dalším údajem zákazníka, který musí být chráněn, je jeho heslo, kterým se přihlašuje k ACS. Toto heslo by nemělo být známo ostatním účastníkům komunikace. Heslo si musí zákazník před vstupem do systému dohodnout.

```
Secret(A,pass,[ACS])
Secret(ACS,pass,[A])
```

```
Agreement(A,ACS,[pass])
Agreement(ACS,A,[pass])
```

Stejně jako v případě zákazníka musí být zabezpečeno a předem dohodnuto i heslo obchodníka, které obchodník zasílá VDS :

```
Secret(B,merpass,[VDS])
Secret(VDS,merpass,[B])
Agreement(B,VDS,[merpass])
Agreement(VDS,B,[merpass])
```

Další požadavky na protokol se mohou týkat zabezpečení samotné transakce. Zákazník předpokládá, že výše částky nákupu bude známa jen obchodníkovi a ACS:

```
Secret(A,puramnt,[B,ACS])
```

Obchodník předpokládá, že identifikátor transakce bude znám jen ACS:

```
Secret(B,purxid,[ACS])
```

Ze strany ACS můžeme napsat pravidlo, které říká, že ACS předpokládá, že identifikátor účtu zná pouze zákazník, obchodník a VDS:

```
Secret(ACS,acctid,[A,B,VDS])
```

Pro přenos zpráv protokol využívá SSL protokolu. Každé zprávě je vytvořen relační klíč. Klíče relace musí být tajné a účastníci komunikace se na jeho hodnotě musí předem dohodnout. První klíč relace, který je v protokolu tvořen, je klíč mezi zákazníkem a obchodníkem (KAB). Zákazník předpokládá, že sdílený klíč je znám pouze obchodníkovi. Obráceně obchodník předpokládá, že klíč zná opět jen zákazník.

```
Secret(A,KAB,[B])
Secret(B,KAB,[A])
Agreement(A,B,[KAB])
Agreement(B,A,[KAB])
```

Podobně můžeme napsat pravidla pro komunikaci mezi zákazníkem a ACS:

```
Secret(A,KACSA,[ACS])
Secret(ACS,KACSA,[A])
Agreement(A,ACS,[KACSA])
Agreement(ACS,A,[KACSA])
```

Obdobná omezení platí i pro komunikaci mezi obchodníkem a VDS a pro komunikaci mezi servery:

```
Secret(B,KVDSB,[VDS])
Secret(VDS,KVDSB,[B])
Agreement(B,VDS,[KVDSB])
Secret(ACS,KACSVDS,[VDS])
Secret(VDS,KACSVDS,[ACS])
Agreement(ACS,VDS,[KACSVDS])
```

5.3 Definice systému

Druhou část skriptu tvoří definice konkrétního systému, který má být kontrolován. Skládá se z definice typů proměnných, z definice funkcí, z definice systému a z informací o narušiteli.

5.3.1 Definice typů

Definice typů proměnných používaných v testovaném systému je velmi podobná definici typu proměnných z první části skriptu. Liší se pouze v tom, že agentům jsou dána jakási zástupná jména. Dále je potřeba přidat nový proces, který bude reprezentovat narušitele systému, a vytvořit k němu příslušné klíče relace. Bývá zvykem proměnné systému, které korespondují s proměnnými uvedenými pod hlavičkou `#Free variables`, značit stejnými názvy. Proměnné se potom odlišují prvním velkým písmenem. Definice typů se děje pod hlavičkou `#Actual variables`.

```
#Actual variables
Zakaznik,Obchodnik,VisaServer,AccessCServer,Narusitel: Agent
Pan, Exp, Acqbin, Merid, Merpass, Acctid, Url, Protocol, y, Mername,
Mercnt, Merurl, Purxid, Purdate, Puramnt, Pansh, Pass, Txtime,
Txstat, Cavv, Eci, Cavvalg : Nonce
Kab,Kvdsb,Kacsvds,Kacsa,Kna,Knb,Knacs,Knvds : SessionKey
InverseKeys=(Kab,Kab),(Kvdsb,Kvdsb),(Kacsvds,Kacsvds),(Kacsa,Kacsa),
(Kna,Kna),(Knb,Knb),(Knacs,Knacs),(Knvds,Knvds)
```

5.3.2 Definice funkcí

Pod hlavičkou `#Functions` bývají definovány funkce, které jsou v systému používány. V programu jsme definovali používané klíče pomocí klíčového slova `symbolic`. Tento zápis značí, že program si vytvoří své vlastní hodnoty, aby reprezentoval výsledky funkce.

```
#Functions
symbolic PK,SK
```

5.3.3 Definice systému

Nejdůležitější částí definice celého systému je označení agentů, kteří mají být kontrolováni. Typy parametrů procesů musí odpovídat typům parametrů, které byly definovány pod hlavičkou `#Processes`. Definice systému probíhá pod hlavičkou `#System`. Abychom zaznamenali, že agenti mohou zrušit započatou akci a začít novou, je potřeba nastavit `WithdrawOption` na hodnotu `True`.

```
#System

INITIATOR(Zakaznik,Obchodnik,VisaServer,AccessCServer,Pan,Exp,Pansh,
Pass,Kab,Kacsa)
RESPONDER(Zakaznik,Obchodnik,VisaServer,AccessCServer,Acqbin,Merid,
Merurl,Mername,Merpass,Mercnt,Purxid,Purdate,Puramnt,Kab,Kvdsb)
SERVER(Zakaznik,Obchodnik,VisaServer,AccessCServer,Kvdsb,Kacsvds)
ACQ(Zakaznik,Obchodnik,VisaServer,AccessCServer,Pansh,Txtime,Acctid,
Protocol,Url,y,Txstat,Cavv,Eci,Cavvalg,Kacsvds,Kacsa)
WithdrawOption = True
```

5.3.4 Informace o narušiteli

Poslední částí skriptu jsou informace o narušiteli systému. Narušiteli je přidělen jeho identifikátor a množina dat, kterou na počátku běhu protokolu zná. Předpokládáme, že narušitel zná všechny agenty systému, některé z údajů obchodníka, svůj privátní klíč a dále, že si dokáže vytvořit relační klíče s jednotlivými agenty systému. Definice se děje pod hlavičkou `#Intruder Information`.

```
#Intruder Information
Intruder = Narusitel
IntruderKnowledge =
{Zakaznik,Obchodnik,VisaServer,AccessCServer,Mername,Merurl,Purdate,
Protocol,Acqbin,Cavvalg,PK,SK(Narusitel),Kna,Knb,Knacs,Knvds
```

5.4 Možnosti napadení

Protokol využívá k zasílání informací metodu POST. Tato metoda může způsobit napadení protokolu nedůvěryhodným obchodníkem, který může podvrhnout URL adresu ACS. Obchodníkovi je adresa ACS známa od VDS ze zprávy `VERes`. Pro provedení autorizace platby zasílá ACS klientovi zprávu `ATReq`. Klient se připojí na adresu ACS a zadá své heslo. Podvrhnutím URL adresy ACS přesměruje obchodník komunikaci na jím kontrolovaný kanál a získá tak heslo držitele karty. Útoku dále napomáhá, že spojení z webové stránky držitele karty na ACS iniciuje obchodník.

Doplňkovým bezpečnostním opatřením protokolu je osobní zpráva klienta (PAM – Personal Assurance Message), kterou si klient sám nastaví. Tato zpráva se zobrazí při každé autentizaci klienta. Toto bezpečnostní opatření by tak mělo klientovi zabezpečit, že zobrazená stránka není podvrhnuta a zamezit tak útokům typu spoofing. Toto opatření není ovšem příliš bezpečné, protože z výše uvedeného vyplývá, že obchodník je schopen duplikovat ověřovací dialog přesměrováním spojení na adresu ACS a obdržet tak tuto osobní zprávu.

Protokol tedy klade požadavky na ověření důvěryhodnosti obchodníka. Ve výhodě jsou větší firmy, které na formu elektronického obchodu přecházejí dříve než menší obchodníci. Velké firmy mají delší tradici a jsou tak pro zákazníka důvěryhodnější oproti menším firmám s kratší historií elektronického obchodu.

6 Závěr

Práci jsem rozdělila do šesti kapitol, první čtyři kapitoly se týkají teoretické části práce, pátou kapitolu tvoří praktická část, šestou kapitolou je závěr.

První kapitolu teoretické části jsem věnovala legislativní úpravě elektronických platebních systémů. Základní právní normou upravující elektronický platební styk v České republice je zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku). Na úrovni EU je daná problematika upravena směrnicemi č. 2000/46/ES, č. 2002/65/ES, č. 97/7/ES a doporučením Komise ES č. 97/489/ES. V této kapitole zároveň vymezuji základní pojmy jako je elektronický peněžní prostředek, elektronické peníze a elektronický platební systém.

Třetí kapitola práce je věnována elektronickým platebním systémům. V prvních dvou podkapitolách se zabývám vymezením základních entit platebního systému a dělením platebních systémů. Základní entity EPS tvoří plátce, příjemce a minimálně jedna finanční instituce. EPS dělíme na EPS nesoucí elektronickou hotovost, EPS bez elektronických peněz, systémy s přímou a nepřímou komunikací, systémy předplacené, aktuálně placené systémy, systémy s odloženou platbou, on-line systémy, off-line systémy, systémy pro mikroplatby, systémy pracující s malými a s velkými částkami a řada dalších. U systémů dělených dle informačních toků uvádím pro názornost také jejich modely. Další tři podkapitoly se týkají platebních systémů v ČR, v EU, v USA a v Japonsku. Jediným používaným platebním systémem v ČR je systém CERTIS. V dané podkapitole uvádím hlavní charakteristiku systému a rozvádím jeho technologii. Systém byl uveden do provozu v roce 1992 a je založen na brutto vyrovnání v reálném čase. Postupně se začleňováním do ekonomiky EU bude systém přecházet na jednotný platební systém SEPA. V podkapitole EPS v EU se nejprve věnuji mezinárodní komunikační síti SWIFT, kterou využívá pro zasílání zpráv většina evropských platebních systémů. Podstatou je předávání swiftových zpráv ve standardizovaném formátu. Pro identifikaci odesílatele a příjemce zprávy se využívá swiftových adres. Následující podkapitoly se zabývají jednotlivými platebními systémy v EU. V EU jsou nejčastěji používanými elektronickými platebními systémy TARGET, TARGET2, clearingové systémy EBA. Nově vyvíjený platební systém SEPA se zatím nachází ve stádiu projektu. Dále se zabývám platebními systémy v USA a v Japonsku. K nim patří EPS Fedwire, CHIPS, BOJ-NET, BCCSs, Zengin System a FXYCS. Těmito se zabývám jen okrajově. Hlavní důraz jsem kladla na EPS v Evropě. V podkapitole Srovnání platebních systémů jsem se rozhodla pro přehlednost uvést tabulku, která uvádí charakteristické rysy jednotlivých EPS a umožní tak snadnější srovnání.

Čtvrtou kapitolu tvoří platební protokoly. Nejdříve se věnuji platebním kartám, protože se k nim vztahují nejpoužívanější platební protokoly. Dále se zabývám charakteristikou a dělením platebních karet, informačními toky a základními bezpečnostními prvky platebních karet. Tuto část

práce jsem pro názornost doplnila také o obrázek schématu čipové karty a o obrázek informačních toků dat při placení kartou. Zabývám se také základními ochrannými prvky platebních karet, mezi něž patří PIN, hologramy, biometrické informace nebo kombinace ochranných prvků. Ve druhé podkapitole se věnuji jednotlivým protokolům platebních karet. Jsou to SET, CSC, AVS, Visa 3-D Secure, UCAF/SPA, CEPS, FINREAD, EMV, EEP. U každého protokolu se zaměřuji na jeho obecnou charakteristiku, technologii platby a na bezpečnostní prvky. Mám-li srovnat výše uvedené platební protokoly, mohu konstatovat, že nejpoužívanějšími protokoly jsou Visa 3-D Secure a UCAF/SPA, které postupně nahradily protokol SET. K podpůrným bezpečnostním mechanismům řadíme standardy CSC a AVS. Přechod od magnetických karet k dokonalejším čipovým kartám usnadňuje protokol EMV. Čipové karty jsou bezpečnější, umožňují ukládání většího množství dat a mají širší pole využitelnosti. V této části práce opět uvádím pro názornost schéma znázorňující průběh transakce v protokolu SET, schémata jednotlivých způsobů šifrování, schéma architektury systému Visa 3-D Secure, průběh transakce v protokolu Visa 3-D, průběh transakce v protokolu UCAF/SPA a schéma hlavních entit standardu CEPS. Poslední podkapitola se zabývá dalšími platebními protokoly. Jsou to BIPS, NPP, FSML, HBCI, ECML a OFX. Jsou to protokoly, které se méně využívají. Protokol OFX je ušit na míru severoamerickému trhu, protokol HBCI byl vytvořen pro podmínky evropského trhu. Pro snadnější vyplňování objednávkových formulářů byl vyvinut značkovací jazyk ECML, protokol FSML slouží jako jazyk k podepisování finančních dokumentů a k tvorbě elektronického šeku. Poslední část kapitoly Platební protokoly tvoří srovnání jednotlivých platebních protokolů. Geografickému kritériu a kritériu použitelnosti, podle kterých jsem protokoly srovnávala, jsem zde věnovala již dostatečný prostor.

Na tomto místě bych při srovnávání jednotlivých protokolů podtrhla spíše kritérium bezpečnosti. K zabezpečení slouží řada ochranných prvků. Mezi hlavní patří: šifrování, digitální podpis, certifikáty a infrastruktura veřejných klíčů. Pojednání o bezpečnostních prvcích jsem zařadila do podkapitoly č. 4.1.2.1 SET, a to z toho důvodu, že tento protokol využívá všech základních bezpečnostních prvků. Šifrování přenášených zpráv můžeme rozdělit na symetrické a asymetrické. K šifrování se používá řada algoritmů. Mezi nejznámější patří DES, 3-DES, AES, RSA, SHA-1 a MD5. Pro oba způsoby šifrování uvádím schémata znázorňující kódování, přenos a dekódování posílaných dat. Nejpoužívanějším bezpečnostním prvkem je použití digitálního podpisu. Tento způsob je založen na asymetrické kryptografii a obvykle bývá spojen s hashovací funkcí (viz. obr. 17). Použití certifikátů vyžaduje důvěryhodnou třetí stranu – tzv. certifikační autoritu, která potvrzuje pravost veřejných klíčů a zajišťuje jejich bezpečnou distribuci.

V teoretické části práce jsem se snažila přinést co nejucelenější přehled platebních systémů a protokolů, jejich důkladnou řešerši, analýzu a srovnání. Pro názornost a přehlednost jsem text práce průběžně doplňovala také schématy a tabulkami, některé jsem převzala, mnohé z nich jsem vytvořila sama. Snažila jsem se, aby práce byla ucelená a názorná a poskytla tak základní orientaci v dané problematice. O ucelený a názorný přehled jsem se snažila také z toho důvodu, že jsem doposud

v odborné literatuře nenašla žádnou práci, která by ho poskytovala. Spatřuji v tom jeden z přínosů své bakalářské práce.

Praktická část práce je zaměřena na formalizaci víceúrovňového platebního protokolu Visa 3-D Secure. Pro ověřování protokolu jsem si vybrala nástroj Casper, který zjednodušuje formální zápis protokolu a je založen na generování CSP procesů. Tomuto nástroji je věnována první podkapitola praktické části. V kapitole Definice protokolu se věnuji již přímo formalizaci protokolu a psaní první logické části skriptu. Tato kapitola se dále člení na podkapitoly týkající se jednotlivých hlaviček skriptu. Druhá část skriptu, popisující samotný testovaný systém, je popsána v kapitole Definice systému, opět se skládá z podkapitol věnovaných jednotlivým hlavičkám skriptu. Závěrečnou kapitolou praktické části je zhodnocení výsledků ověřování a popis možnosti napadení protokolu.

V praktické části jsem vytvořila zjednodušený model protokolu Visa 3-D Secure v nástroji Casper a po ověření jeho bezpečnosti v kontroloru FDR jsem nalezla způsob jeho napadení. Zjistila jsem, že slabinou protokolu je předpoklad důvěryhodnosti obchodníka. Obchodník může při autorizaci platby podvrhnout URL adresu ACS a získat tak osobní údaje klienta, čímž je ohrožena bezpečnost protokolu.

Práce je doplněna seznamem použitých zkratek. Přílohy jsou tvořeny seznamem použitých tabulek a schémat, logy systémů CHIPS, EBA, TARGET2 a logem společnosti SWIFT. Následujících osm příloh tvoří schémata zasílaných zpráv v protokolu Visa 3-D Secure. Poslední přílohou je zdrojový kód skriptu Visa3DSecure.spl.

Při zpracovávání tohoto tématu jsem narážela na řadu potíží. Byla jsem nucena se potýkat s odborným textem v anglickém jazyce. Podobně jako v českém jazyce, tak i v anglickém jazyce je k danému tématu literatury nedostatek. Z tohoto důvodu jsem byla nucena čerpat z internetových stránek centrálních bank, které jednotlivé platební systémy spravují a ze stránek společností, které vyvíjejí platební protokoly. Nejdůležitějším zdrojem informací pro mě byly specifikace protokolů, které jsem na těchto stránkách nalezla.

Tato práce byla podkladem pro odbornou publikaci, kterou jsem vytvořila spolu se svým vedoucím bakalářské práce Ing. Pavlem Očenáškem. S touto publikací plánuji vystoupit na Mezinárodní vědecké konferenci Management, economics and business development in the new european conditions, pořádané Fakultou podnikatelskou VUT ve dnech 23. – 24.5.2008 v Brně.

V budoucnu bych ráda navázala na získané zkušenosti a chtěla bych se zabývat možnostmi zabezpečení elektronických platebních systémů a protokolů.

7 Literatura

Monografie

[1] GIAMPAOLO, B.: *Formal Correctness od Security Protocols*. 2.vyd. Springer Berlin, 2007. ISBN 13 978-3-540-68134-2

[2] GRUBLOVÁ, E. a kol.: *Internetová ekonomika*. 1.vyd. Ostrava: Repronis, 2002. ISBN 80-7329-000-6

[3] HASHEM, M.S.: *Protocols for Secure Electronic Commerce*. 1.vyd. CRC Press LLC, 2004 ISBN 0-8493-1509-3

[4] JUŘÍK, P.: *Svět platebních a identifikačních karet*. 2.vyd. Praha: Grada Publishing, spol. s.r.o., 2001. ISBN 80-247-0195-2

[5] KIMBROUGH, S.: *Formal Modelling in Electronic Commerce*.1.vyd. Springer, 2005, ISBN 3-540-21431-3

[6] MÁČE, M.: *Platební styk klasický a elektronický*. 1. vyd. Praha: Grada Publishing, a.s., 2006. ISBN 80-247-1725-5

[7] PŘÁDKA, M., KALA, J.: *Elektronické bankovnictví: rady a tipy*. 1.vyd. Praha: Computer Press, 2000. ISBN 80-7226-328-5

[8] SCHLOSSBERGER, O., HOZÁK, L.: *Elektronické platební prostředky*. 1. vyd. Praha: Bankovní institut, a.s.

Internetové zdroje

[9] http://www.bis.org

[10] http://www.cnb.cz

[11] http://www.cl.cam.ac.uk/~lp15/Grants/SET.html

[12] https://www.chips.org/

[13] http://www.ebaclearing.eu/

[14] http://www.ecb.int/

[15] http://en.wikipedia.org/wiki/

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

[17] http://www.federalreserve.gov/paymentsystems/

[18] http://www.finread.com

[19] http://www.ica.cz/

[20] http://www.swift.com/

[21] http://www.unece.org/trade/

[22] http://www.visa.com/

Legislativní prameny

[23] Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku).

Seznam použitých zkratek

3-DES – Triple Data Ecryption Standard – datový kódovací standard

AAV – Accountholder Authentication Value – autentifikační hodnota držitele karty

ACS – Access control server – server zajišťující autentizaci držitele karty

AES – Advanced Electronic Signature– kódovací standardní postupy

ASI – the Ancillary System Interface – pomocné systémové rozhraní

AVS – Address Verification Service – podpůrný bezpečnostní prostředek pro ověření totožnosti zákazníka

B2B – Business to Business – obchodování mezi obchodníky navzájem

BCCSs – Bill and Cheque Clearing System – zúčtovací systém Japonska pro vypořádání směnek a šeků

BIC – The Bank Identifier Code – identifikační bankovní kód odesílatele a příjemce

BIN – Bank Identification Number – číslo přidělené karetní asociací dané bance

BIPS – The Bank Internet Payment System – protokol umožňující B2B transakce

BOJ-NET – platební systém Japonska spravovaný Bank of Japan

CAVV – Cardholder Authentication Verification Value – autentifikační ověřovací hodnota drřitele karty

CEPS – Common electronic purse specification – standard umožňující správu finančních prostředků

CERTIS – Czech Express Real Time Interbank Gross Settlement System – tuzemské mezibankovní platby v českých korunách

CGI – Common Gateway Interface – rozhraní

CHIPS – Clearing House Interbank Payment System – zúčtovací mezibankovní systém v USA

CRR – Cycle Reconciliation Report – zpráva zasílaná účastníkům STEP2 po proběhnutí každého cyklu

CSC – Card Security Code – podpůrný bezpečnostní prostředek

CSP – Communicating Sequential Processes

CVF – Credit Validation File – soubor poslaný jako odpověď účastníku systému STEP2 po ověření plateb

ČNB – Česká národní banka

DDX – digital data exchange – linky pro výměnu digitálních datových paketů

DES – Data Encryption Standard – datový kódovací standard

DPSW – Direct Participant Webstation – webové rozhraní systému STEP2

DRR – Daily Reconciliation Report – denní zpráva zasílaná účastníkům systému STEP2

EACB – European Association of Cooperative Banks – Evropská asociace kooperativních bank

EBA – the Euro Banking Association – Evropská bankovní asociace

ECB – European Central Bank – Evropská centrální banka

ECI – Electronic Commerce Indicator – indikátor elektronické transakce v protokolu Visa 3-D Secure

ECML – Electronic Commerce Modeling Language – jazyk usnadňující vyplňování objednávkových formulářů

EEP – European electronic purse – standard platebních karet, na nichž jsou uloženy peníze v různých měnách

EMV – Europay MasterCard Visa – standard pro přechod z magnetických karet na čipové

EPC – European Payment Council – Evropská platební rada

EPS – elektronický platební systém

ESBG – European Savings Banks Group – Evropská skupina spořitelních bank

FBE – European Banking Federation – Evropská bankovní federace

FCR – FINREAD Card Reader – modul zajišťující bezpečnost standardu FINREAD

FDR – Failures-Divergence Refinement

FINREAD – Financial Transactional IC Card Reader – standard pro placení ve finančním i nefinančním sektoru

FinTS – Financial Transaction Services – nástupce protokolu HBCI

FSML – Financial Services Markup Language – značkovací jazyk na podepisování finančních dokumentů a tvorbu elektronického šeku

FSTC – Financial Services Technology Consortium – finanční konsorcium, které vytvořilo jazyk FSML

FXYCS – Foreign Exchange Yen Clearing House – zúčtovací systém pro přeshraniční obchody v yenech

HBCI – Homebanking Computer Interface – systém vytvořený konsorciem německých bank

ICF – Input Credit File – soubor pro zasílané platby

ICM – the Information and Control Module – modul pro kontrolu informací

IFX – Interactive Financial Exchange – platební protokol vytvořený pro severoamerický trh

ISO – International Organization for Standardization – mezinárodní organizace pro standardizaci

JCB – Japan Credit Burea – nebankovní asociace podílející se na vývoji nových platebních systémů

LVTS – Large-value funds transfer system – systém pro zúčtování vyšších plateb

MD5 – šifrovací mechanismus

MPI – Merchant plug-in – plug-in na straně obchodníka, umožňující provedení transakce v protokolu Visa 3-D Secure

MSR – Monthly Statistics Report – měsíční statistická zpráva v systému STEP2

NPP – Network Payment Protocol – platební protokol vycházející z protokolu BIPS

NTT – skupina japonských dopravců

OFX – Open Financial Exchange – platební protokol vytvořený pro severoamerický trh

PAM – Personal Assurance Message – ověřovací zprávy klienta

PAReq – Payer Authentication Request – žádost o ověření držitele karty ve Visa 3-D Secure

PARes – Payer Authentication Response – odpověď s ověřením držitele karty ve Visa 3-D Secure

PDA – Personal Digital Assistant – malý kapesní počítač

PE-ACH – Pan-European Automated Clearing House – Panevropské automatické zúčtovací centrum

PEDD – Pan-European Direct Debet – Panevropský přímý debet – nový platební nástroj

PIN – Personal Identification Number – osobní identifikační číslo

PKI – Public Key Infrastructure – struktura předávání veřejných klíčů

PNB – Potential Net Balance – potenciální čistý zůstatek

POS – Point-of-sale – místo prodeje, např. automat

PSAM – Purchase Secure Application Module – modul zajišťující bezpečnost standardu CEPS

RSA – šifrovací algoritmus

RTGS – Real Time Gross Settlement – brutto vypořádání v reálném čase

SBČS – Státní banka Československá

SET – Secure Electronic Transaction – protokol pro zabezpečení elektronických plateb

SCF – Settled Credit Files – soubor zasílaný přímému účastníku systému STEP2

SCT – SEPA Credit Transfer service – služba poskytovaná systémem STEP2

SDD – SEPA Direct Debit Service – služba poskytovaná systémem STEP2

SEPA – Single Euro Payments Area – jednotná evropská platební oblast

SGML – Standard Generalized Markup Language – standardizovaný počítačový jazyk

SHA1 – šifrovací algoritmus

SPA – Secure Payment Application – vlastní bezpečnostní schéma společnosti MasterCard

SPP – Single Shared Platform – jednotná společná platforma

SPZ – systém přenosu zpráv

SSL – Secure Sockets Layer – protokol pro bezpečnou komunikaci

SWIFT – Society for Worldwide Interbank Financial Telecommunication – instituce pro zabezpečování mezibankovní komunikace – přenos dat

SZD – systém zabezpečení dat

TARGET, TARGET2 – Trans-European Automated Real-Time Gross-Settlement Express Transfer System – platební nadnárodní systémy organizované Evropským systémem centrálních bank

TBA – Tokyo Bankers Association – Tokijská asociace bankéřů

TCP – Transmission Control Protocol – přenosový řídící protokol orientovaný na virtuální spoje

UCAF – Universal Cardholder Authentification Fiels – univerzální autentifikační pole držitele karty

UNIVYC – Univerzální vypořádací centrum

URL – Uniform Resource Locator – internetová adresa

VAP – Visa Access Point – přístupové body společnosti Visa

VDS – Visa Directory Server – adresář společnosti Visa uchovávající informace o všech uživatelích

VEReq – Verify Enrollment Request – požadavek na ověření obchodníka ve Visa 3-D Secure

VERes – Verify Enrollment Response – odpověď žádost o ověření obchodníka ve Visa 3-D Secure

XCT – Credeuro Service – služba poskytovaná systémem STEP2

XID – identifikátor transakce v protokolu Visa 3-D Secure

XML – eXtensible Markup Language – otevřený jazykový systém (technologie přenosu dat)

Seznam příloh

Přílohy

Příloha č.1: Seznam použitých tabulek a schémat

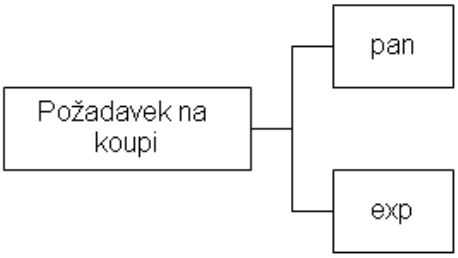
Příloha č.2: Logo EPS CHIPS

Příloha č.3: Logo společnosti EBA

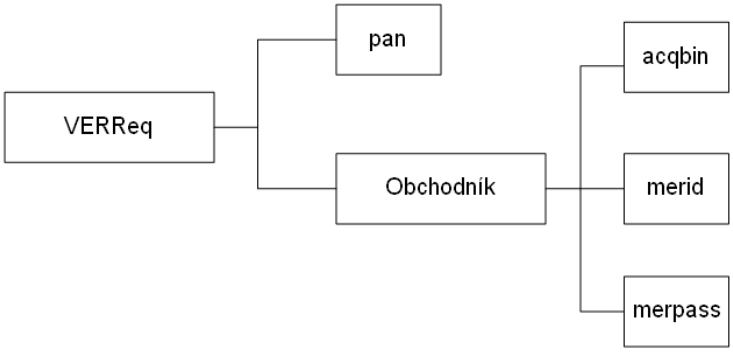
Příloha č.4: Logo mezinárodní sítě SWIFT

Příloha č.5: Logo EPS TARGET2

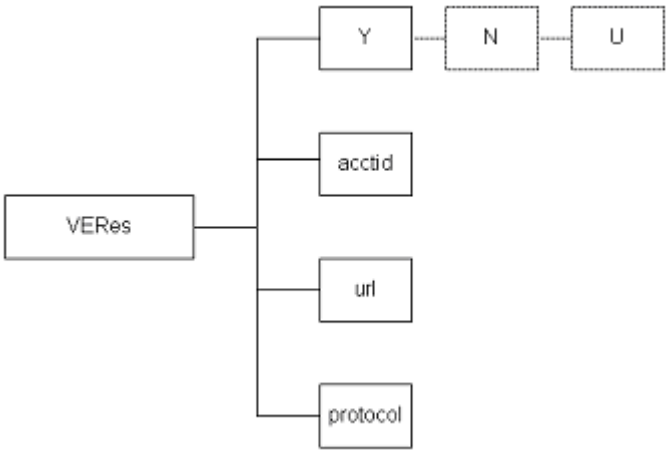
Příloha č.6: Struktura požadavku na koupi



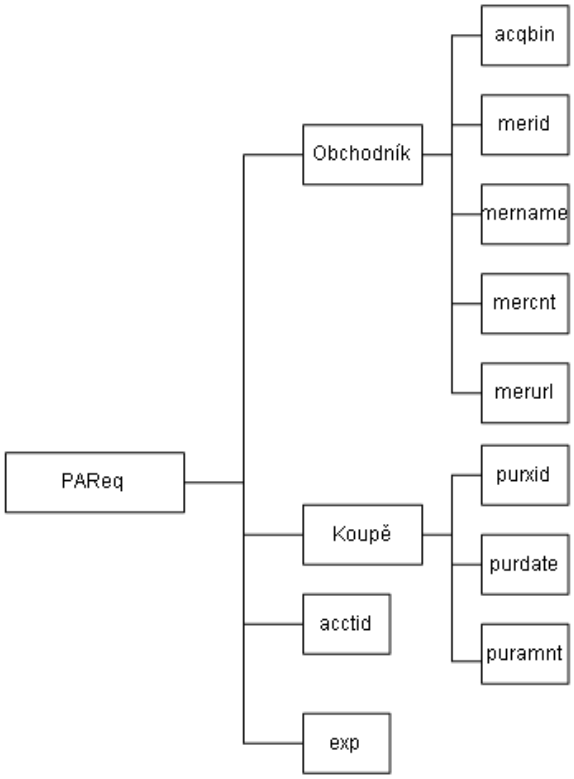
Příloha č.7: Struktura zprávy VERreq



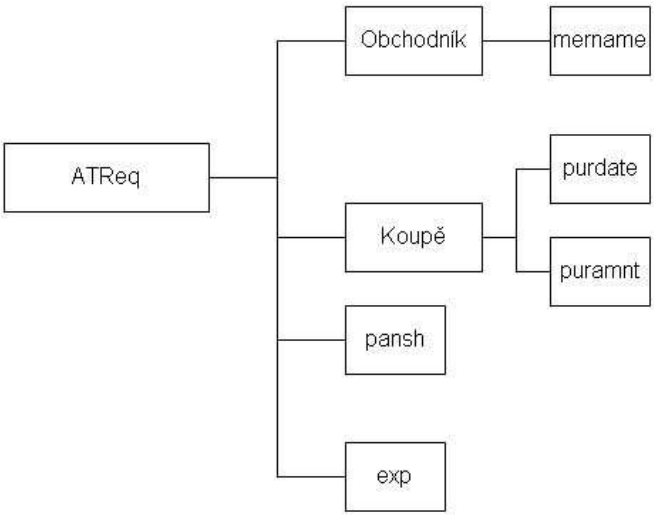
Příloha č.8: Struktura zprávy VERes



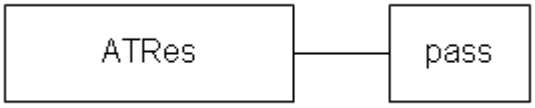
Příloha č.9: Struktura zprávy PAReq



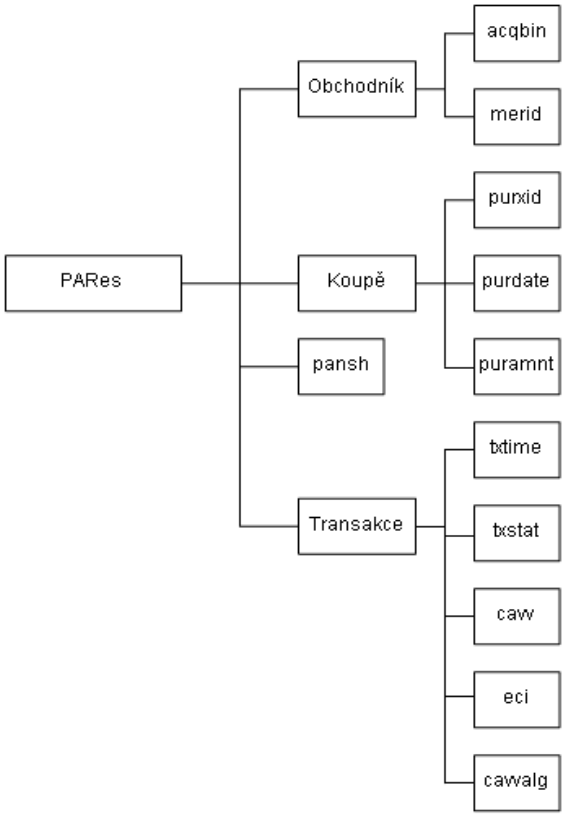
Příloha č.10: Struktura zprávy ATReq



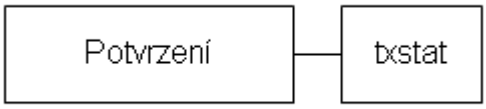
Příloha č.11: Struktura zprávy ATRes



Příloha č.12: Struktura zprávy PARes



Příloha č.13: Struktura potvrzení



Příloha č.14: Skript Visa3DSecure.spl

```
--Visa3DSecure
--Petra Kucerova

#Free variables
A,B,VDS,ACS: Agent
pan, exp, acqbin, merid, merpass, acctid, url, protocol, Y, mername,
mercnt, merurl, purxid, purdate, puramnt, pansh, pass, txtime,
txstat, cavv, eci, cavvalg : Nonce
PK : Agent -> PublicKey
SK : Agent -> SecretKey
KAB,KVDSB,KACSVDS,KACSA : SessionKey
InverseKeys=(PK,SK),(KAB,KAB),(KVDSB,KVDSB),(KACSVDS,KACSVDS),
(KACSA,KACSA)

#Processes
INITIATOR(A,B,VDS,ACS,pan,exp,pansh,pass,KAB,KACSA) knows PK
RESPONDER(B,A,VDS,ACS,acqbin,merid,merurl,mername,merpass,mercnt,
purxid,purdate,puramnt,KAB,KVDSB) knows PK,SK(B)
SERVER (VDS,A,B,ACS,KVDSB,KACSVDS) knows PK,SK(VDS)
ACQ(ACS,VDS,A,B,pansh,txtime,acctid,protocol,url,Y,txstat,cavv,eci,
cavvalg,KACSVDS,KACSA) knows PK,SK(ACS)

#Protocol description
0.->A:B
--pozadavek na koupi
1. A -> B: {pan,exp} {KAB}
--VERReq
2. B -> VDS: {pan,acqbin,merid,merpass} {KVDSB}
3. VDS -> ACS: {pan,acqbin,merid,merpass} {KACSVDS}
--VERes
4. ACS -> VDS: {Y,acctid,url,protocol} {KACSVDS}
5. VDS -> B: {Y,acctid,url,protocol} {KVDSB}
--PAReq
6.B->A:{{acqbin,merid,mername,mercnt,merurl,purxid,purdate,puramnt,
acctid,exp} {SK(B)}%msg1 } {KAB}
```

7.A -> ACS:{msg1%{acqbin,merid,mername,mercnt,merurl,purxid,purdate,puramnt,acctid,exp} {SK(B)} } {KACSA}
--ATReq
8. ACS -> A: {mername,puramnt,purdate,pansh,exp} {KACSA}
--ATRes
9. A -> ACS: {pass} {KACSA}
--PARes
10. ACS -> A: {{acqbin,merid,purxid,purdate,puramnt,pansh,txtime,txstat,cavv,eci,cavvalg} {SK(ACS)} % msg2 } {KACSA}
11. A -> B: {msg2 % {acqbin,merid,purxid,purdate,puramnt,pansh,txtime,txstat,cavv,eci,cavvalg} {SK(ACS)} } {KAB}
--potvrzení
12. B -> A: {{txstat} {KAB} } {SK(B)}

#Specification
Secret(A,pan,[B,ACS,VDS])
--Secret(A,pass,[ACS])
--Secret(ACS,pass,[A])
--Agreement(A,ACS,[pass])
--Agreement(ACS,A,[pass])
--Secret(B,merpass,[VDS])
--Secret(VDS,merpass,[B])
--Agreement(B,VDS,[merpass])
--Agreement(VDS,B,[merpass])
--Secret(A,puramnt,[B,ACS])
--Secret(B,purxid,[ACS])
--Secret(ACS,acctid,[A,B,VDS])
--Secret(A,KAB,[B])
--Secret(B,KAB,[A])
--Agreement(A,B,[KAB])
--Agreement(B,A,[KAB])
--Secret(A,KACSA,[ACS])
--Secret(ACS,KACSA,[A])
--Agreement(A,ACS,[KACSA])
--Agreement(ACS,A,[KACSA])
--Secret(B,KVDSB,[VDS])
--Secret(VDS,KVDSB,[B])

```
--Agreement(B,VDS,[KVDSB])
--Secret(ACS,KACSVDS,[VDS])
--Secret(VDS,KACSVDS,[ACS])
--Agreement(ACS,VDS,[KACSVDS])

#Actual variables
Zakaznik,Obchodnik,VisaServer,AccessCServer,Narusitel: Agent
Pan, Exp, Acqbin, Merid, Merpass, Acctid, Url, Protocol, y, Mername,
Mercnt, Merurl, Purxid, Purdate, Puramnt, Pansh, Pass, Txtime,
Txstat, Cavv, Eci, Cavvalg : Nonce
Kab,Kvdsb,Kacsvds,Kacsa,Kna,Knb,Knacs,Knvds : SessionKey
InverseKeys=(Kab,Kab),(Kvdsb,Kvdsb),(Kacsvds,Kacsvds),(Kacsa,Kacsa),
(Kna,Kna),(Knb,Knb),(Knacs,Knacs),(Knvds,Knvds)

#Functions
symbolic PK,SK

#System
INITIATOR(Zakaznik,Obchodnik,VisaServer,AccessCServer,Pan,Exp,Pansh,
Pass,Kab,Kacsa)
RESPONDER(Zakaznik,Obchodnik,VisaServer,AccessCServer,Acqbin,Merid,
Merurl,Mername,Merpass,Mercnt,Purxid,Purdate,Puramnt,Kab,Kvdsb)
SERVER(Zakaznik,Obchodnik,VisaServer,AccessCServer,Kvdsb,Kacsvds)
ACQ(Zakaznik,Obchodnik,VisaServer,AccessCServer,Pansh,Txtime,Acctid,
Protocol,Url,y,Txstat,Cavv,Eci,Cavvalg,Kacsvds,Kacsa)
WithdrawOption = True

#Intruder Information
Intruder=Narusitel
IntruderKnowledge={Zakaznik,Obchodnik,VisaServer,AccessCServer,
Mername,Merurl,Purdate,Protocol,Acqbin,Cavvalg,PK,SK(Narusitel),Kna,
Knb,Knacs,Knvds}
```