Diplomová práce

Implementace technologie SET

Petr Slabý
740326/0073

1. Úvod

1.1 Úvod diplomové práce

Práce popisuje technologii SET (Secure Electronic Transaction) - protokolu vytvořeného k elektronickému obchodování na Internetu. Zadání této práce vzniklo současně s rozjetím pilotního projektu SET v České republice. Protokol SET je otevřený projekt, který se stále vyvíjí a dynamicky mění. A zvláště obchodování na Internetu dostává čím dál více dominantní roli. Když jsem si vybral tuto diplomovou práci, netušil jsem, jak je problematika elektronického obchodování rozsáhlá a co musí obsahovat a splňovat platební systém. Během vývoje experimentálního platebního systému jsem si uvědomoval jak složitý je vývoj platebního systému, jaké technické nedostatky může mít a co se musí udělat pro to, aby byl spolehlivý a relativně bezpečný.

Cílem této práce je zmapovat vývoj SET technologie v České republice a ve světě a vytvořit vlastní experimentální platební systém, který vychází z platebního protokolu SET.

V úvodní části je popsán platební styk zákazníka s bankou (bezhotovostní platby z účtu, používané typy platebních karet). V této kapitole jsou také popsány algoritmy používané k zabezpečení dat, jako např. Symetrické a asymetrické šifrování, funkce digitálního podpisu a funkce certifikátu.

Ve druhé části je popsán samotný protokol SET, tzn. jeho funkce a subjekty, které zahrnuje. Je zde uveden popis platby ve Virtuálním Obchodním Domě a detailní (teoretický) popis platby pomocí SETu (registrace, získání certifikátu).

Ve třetí části je popsán vývoj technologie SET v České republice. Je zde uveden seznam obchodníků přijímajících platby pomocí SETu a detailní popis historie vývoje v ČR. Dále je popsán vývoj technologie SET ve světě. V této kapitole je návod co má udělat zákazník pro to, aby získal možnost platit SETem nebo obchodník, aby mohl poskytovat služby spojené s technologií SET.

Ve čtvrté části je popsán návrh mého vlastního experimentálního systému, který je z větší části odvozen z protokolu SET. Zahrnuje obchodní a technické požadavky na platební systém a popisuje teoretické a programové řešení experimentálního platebního systému.

V závěrečné části je popis některých platebních systémů, které jsou používány v ČR nebo ve světě. Jsou to např. mikroplatby (systém Millicent), elektronická hotovost (systém ECASH), elektronické šeky (projekt FSTC) nebo přímé bankovnictví (Expandia banka).

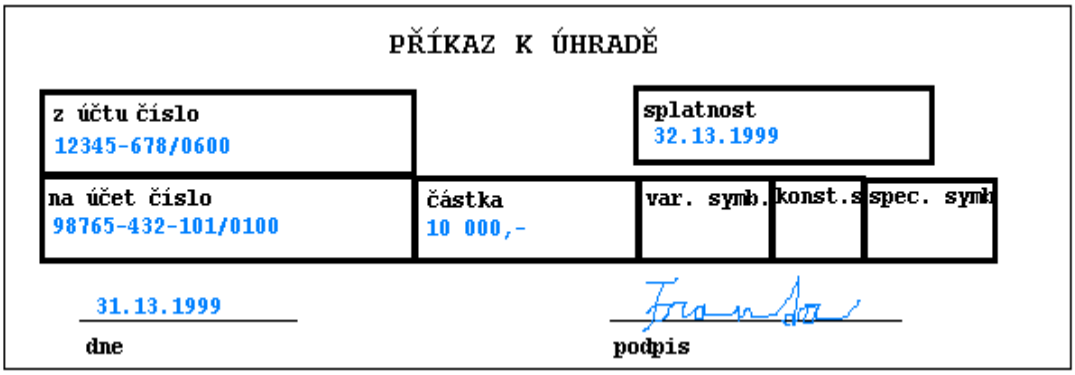
1.2 Platební styk

1.2.1 Co jsou bezhotovostní platby z účtu

Mít hotové peníze doma zašité ve slamníku není bezpečné, protože zloději je mohou sebrat a proto je lepší uložit je do banky na bankovní účet. Bankovní účet je pomyslná přihrádka v bance, ve které moje peníze jakoby leží. Ve skutečnosti si banka jen poznamená, kolik peněz jsem si k ní uložil a hodí peníze na jednu velkou hromadu. Je to ale jedno, protože když přijdu a chci peníze vybrat, zase je z té velké hromady vezme a dá mi je.

Každý účet v rámci jedné banky má své číslo (např. 12345-678), každá banka má své číslo (např. 0600), proto je každý účet jedinečný svým číslem spojeným s číslem banky (např. 12345-678/0600).

Pokud mám svůj účet a chci zaplatit někomu peníze, kdo má také svůj účet, i když třeba v jiné bance, nemusím peníze ze svého účtu vybrat v hotovosti a dotyčnému člověkovi je zanést, stačí, když své bance přikáži, aby převedla peníze z mého účtu na účet onoho člověka. Příkaz k tomuto převodu se většinou podává písemně, kde je uvedeno, ze kterého účtu, na jaký účet a kolik peněz chci převést:



obrázek 1 - Příkaz k úhradě

Příkaz k převodu musí být ověřený, většinou podpisem, aby banka věděla, že jí příkaz podává skutečně ten, komu účet patří (nebo někdo jiný, kdo byl majitelem pověřen).

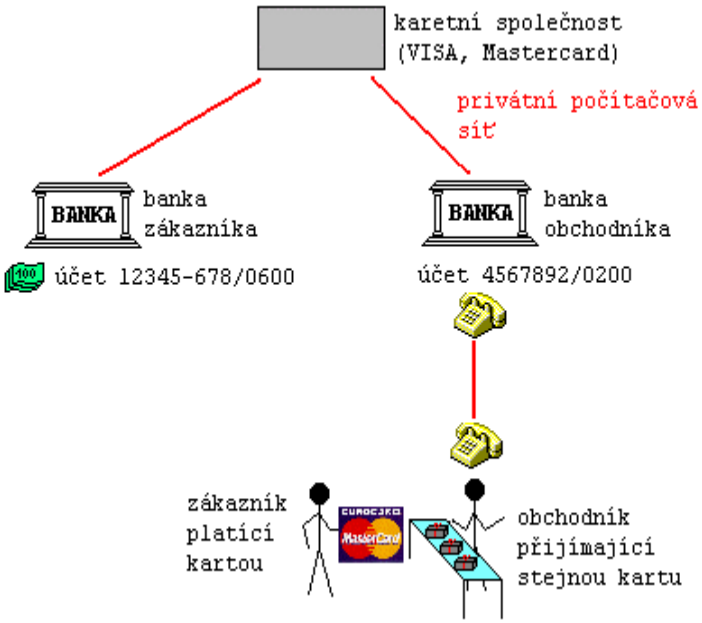
Platby provedené tímto způsobem se nazývají bezhotovostní, protože při nich hotové peníze nejsou vůbec potřeba, stačí podpis majitele účtu.

O tom, co se na mém účtu děje, se dozvím z výpisu z účtu, který mi banka pravidelně posílá, většinou měsíčně. Výpis z účtu je prostě seznam událostí, které se s účtem staly od minulého výpisu, tedy seznam plateb přišlých na účet a plateb odešlých z účtu.

Mít peníze na účtu je mnohem bezpečnější a pohodlnější než mít hotové peníze, zvláště pak pokud používám homebanking (podávání příkazů k úhradě a jiných operací pomocí počítače) a nemusím docházet do banky osobně.

1.2.2 Co je platební karta

Stručně řečeno: pokud mám své peníze na účtu v bance, vím to já, ví to banka, ale ostatní mi to nemusí věřit. Platební karta k účtu znamená, že obchodník, který moji kartu přijímá, si může ověřit, jestli peníze skutečně mám.



obrázek 2 - Schéma platby v kamenném obchodě

Zákazník má peníze na účtu 12345-678/0600. K tomuto účtu má vydanou platební kartu. Přišel do obchodu, kde přijímají platby jeho kartou, což se pozná podle toho, že na dveřích obchodu je vylepené stejné logo, jaké má zákazník na kartě. Zákazník si vybral zboží a chce zaplatit.

Obchodník má svůj účet č. 4567892/0200 v jiné bance a má s ní smlouvu na přijímání platebních karet. Na kartě zákazníka si přečte číslo karty a zatelefonuje do své banky, kam nahlásí číslo karty a placenou částku.

V obchodníkově bance se přes společnost, která daný druh karty vydává, zeptají v bance zákazníka, jestli je karta platná a lze s ní požadovanou částku zaplatit. Výsledek sdělí obchodníkovi, který zboží buď vydá (při kladné odpovědi), nebo nevydá. Dotazu obchodníka na solventnost zákazníkova účtu se říká autorizace. Peníze jsou z účtu zákazníka na účet obchodníka převedeny později při zvláštní operaci capture.

To, jestli karta zákazníkovi skutečně patří, se ověřuje podpisem nebo číslem PIN, které zná jen majitel karty. (Obchodník nemusí do banky zrovna telefonovat, může mít on-line pokladnu, která si přečte z karty číslo sama a sama se zeptá v bance přes datový spoj. Nicméně podstata zůstává, obchodník se přes svou banku a karetní společnost zeptá v bance zákazníka. Dále se u malých částek může prostě předpokládat, že zákazník peníze na účtu má a autorizace se provádět nemusí.)

Platebních karet jsou dva druhy:

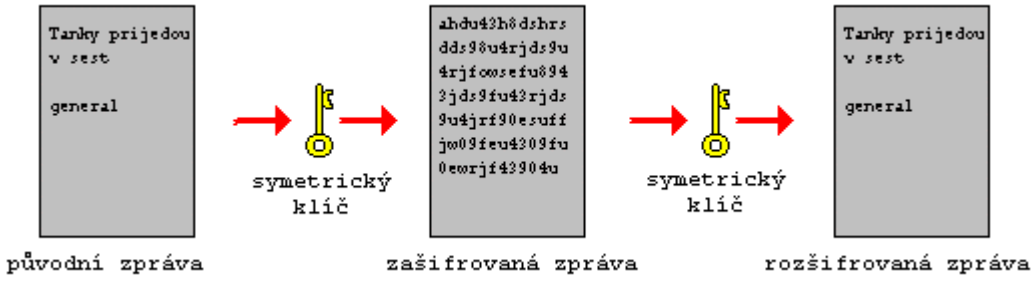
- **debetní** - peníze jsou z účtu zákazníka strženy v okamžiku, kdy je platba provedena. Tento typ karet je u nás nejrozšířenější.
- **kreditní** - peníze banka obchodníkovi zaplatí ihned, ale po zákazníkovi je chce až na konci měsíce. Po tuto dobu vlastně banka zákazníka úvěruje.

Placení kartou má své obrovské výhody. Pro zákazníka tu, že nemusí s sebou nosit hotové peníze, takže mu nemohou být zcizeny, a přesto je má stále po ruce. Pro obchodníka tu, že lidé platící kartou více utrácejí. Proto je ve světě placení kartou zcela běžné, a i u nás má už kartu přes dva miliony lidí. Pokud si necháváte posílat výplatu na sporožiro, postžiro, o-konto nebo jiný účet, můžete si k němu nechat vystavit platební kartu.

1.3 Bezpečnost dat

1.3.1 Symetrické šifrování

Ze špionážních filmů a válečných románů je známé tzv. symetrické šifrování, kdy odesílatel i příjemce nějaké důležité zprávy mají dohodnutý způsob šifrování, například použití nacistického šifrovacího stroje Enigma, a nějaký klíč, což je údaj, nejčastěji krátké heslo, použitý pro zašifrování konkrétní zprávy. Při posílání více zpráv se používá stále stejný způsob šifrování, ale pokaždé jiný klíč, takže prozrazení jednoho klíče umožní nepříteli dešifrovat jen jednu zprávu. Tento způsob šifrování se nazývá symetrický právě proto, že obě strany mají stejný klíč, používaný pro zašifrování i dešifrování. Slabinou tohoto způsobu šifrování je právě nutnost dohodnout si předem společný klíč, nebo klíč dopravit bezpečným kanálem příjemci před odesláním zprávy.

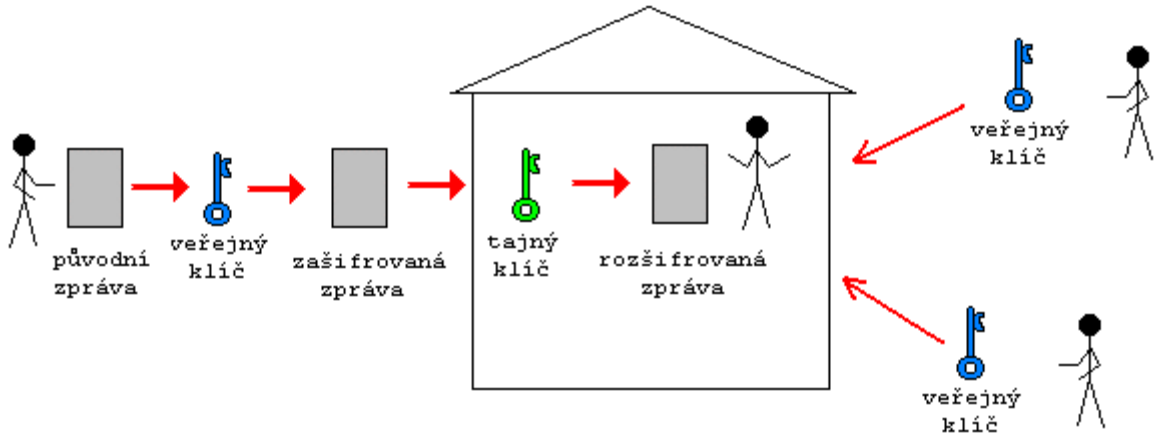


obrázek 3 - Symetrické šifrování

1.3.2 Asymetrické šifrování

Proto bylo vyvinuto tzv. asymetrické šifrování, kdy se používají klíče dva. Tyto klíče mají tu zajímavou vlastnost, že co se jedním zašifruje, lze odšifrovat jen druhým, a naopak. Při použití asymetrického šifrování si příjemce zpráv vyrobí dvojici klíčů, jeden si nechá a střeží ho jako oko v hlavě, to je tzv. tajný klíč, a druhý vylepí na všech nárožích a rozdá potenciálním odesílatelům, to je tzv. veřejný klíč. Pokud chce někdo poslat zprávu takovémuto příjemci, zašifruje ji jeho veřejným klíčem a pošle mu ji. Má jistotu, že nikdo, kdo nemá příslušný tajný klíč, ji nedokáže rozšifrovat. Příjemce si pak zprávu svým tajným klíčem rozšifruje.

Při asymetrickém způsobu šifrování se všechny zprávy šifrují stále stejným veřejným klíčem, který všichni znají. Ještě jednou zdůrazňuji nutnost naprostého utajení tajného klíče, protože s ním stojí a padá celá bezpečnost asymetrického šifrování. Ten, kdo má tajný klíč, má možnost rozšifrovávat všechny zprávy došlé jednomu příjemci, protože veřejný klíč má jeden příjemce pouze jeden !

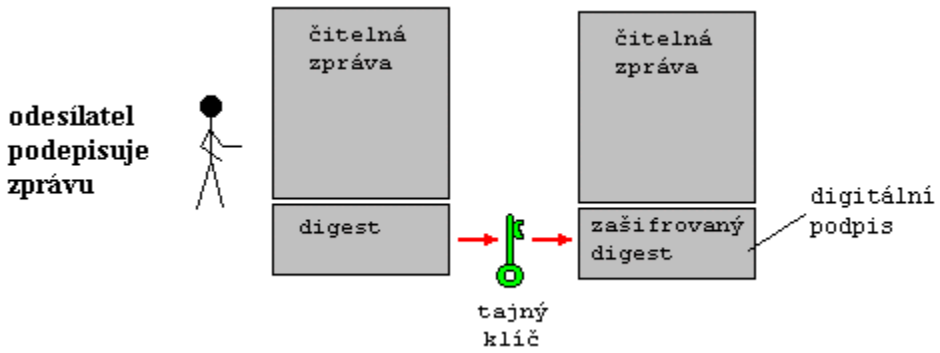


obrázek 4 - Asymetrické šifrování

1.3.3 Digitální podpis

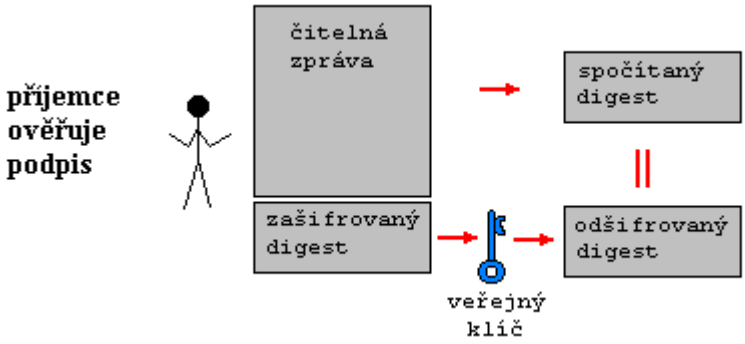
V opačném směru se dá stejný pár klíčů použít k digitálnímu podepisování, tedy vytvoření zprávy, kterou si sice každý může přečíst, ale je jisté, že ji nevytvořil nikdo jiný než odesílatel a že nebyla po cestě změněna.

Funkce je jednoduchá, k podepisované zprávě se připojí něco, co závisí na textu zprávy a co nemohl vytvořit nikdo jiný, než odesílatel. Konkrétně se spočítá jakýsi součet znaků ve zprávě (písmena jsou v počítači reprezentována jako čísla), tzv. message digest, ten odesílatel zašifruje svým tajným klíčem a připojí ho ke zprávě.



obrázek 5 - Message digest - odesílatel

Pokud chce někdo ověřit digitální podpis zprávy, sežene si veřejný klíč odesílatele, rozšifruje message digest připojený ke zprávě a porovná ho s message digestem, který si sám spočítá. Pokud se shodují, je jisté, že zprávu odeslal majitel tajného klíče patřícího k veřejnému klíči použitého pro ověření, tedy odesílatel, a že zpráva nebyla po cestě změněna.



obrázek 6 - Message digest - příjemce

Podepisování zpráv se dnes běžně používá v elektronické poště, z volně dostupných e-mailových programů umí digitální podepisování (i šifrování) Netscape Communicator a Microsoft Outlook Express. Zde jsou pro větší názornost příklady e-mailových zpráv podepsaných digitálním podpisem:

e-mail podepsaný podle standardu PGP

```
Content-Type: application/pgp; format=text; x-action=sign
Content-Transfer-Encoding: 7bit
Content-Length:   329

-----BEGIN PGP SIGNED MESSAGE-----

Tanky prijedou v sest.

General

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: noconv

IQB1AwUBNSHocfNAlnXZYBHhAQHSTQL/XtuUdG36R9ZVgX0b/MuE6SyqHRvmi+Qy
Iq1FzYCCLeVHxwwQu4kz3SnyeXqKd/CxPAfPrujICeDhbrmvBy9m3jxb3uzXLoDg
LC4zQRrgscBt2RDbA2pfo+CSWBhXN6cx
=AkUc
-----END PGP SIGNATURE-----
```

e-mail podepsaný podle standardu S/MIME

```
Content-Type: multipart/signed;
              protocol="application/x-pkcs7-signature";
              micalg=sha1; boundary="------------msAEFE8CC4BBD6CDB2637B5646"

This is a cryptographically signed message in MIME format.

--------------msAEFE8CC4BBD6CDB2637B5646
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

Tanky prijedou v sest.

General

--------------msAEFE8CC4BBD6CDB2637B5646
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIFmQYJKoZIhvcNAQcCoIIFijCCBYYCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC
BBswggHsMIIBVQICANYwDQYJKoZIhvcNAQEEBQAwXDELMAkGA1UEBhMCQ1oxETAPBgNVBAoT
CFBWVCBhLnMuMRAwDgYDVQQDEwdDQS1QVlQxMSgwJgYJKoZIhvcNAQkBFhljYS1vcGVyQHA3
MHgwMy5icm4ucHZ0LmN6MB4XDTk3MTEwNjE5NTg1M1oXDTk3MTEyMDE5NTg1M1owZDELMAkG
```

```
A1UEBhMCQ1oxEjAQBgNVBAgTCVZvZG92YSA0MzENMAsGA1UEBxMEQnJubzEUMBIGA1UEAxML
+5Z/Q0img9iU3N42zdSfbn0Xl0qtMwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAF3otOnrJghy
beZIEcrheHdBux4RC+umSae5rmDwaYNy9FgZOXhnztWh9bx7CftSDI58h0ePTN1teMcVay+v
jTJj3f8nE+jfAxxvD2N8qEX5aY6Qzw/ZoeJ6wLv4hSGGkVEYNmQzURprw6DG9JyRcbbsDZgD
doMPWc1lsxTC/nDaMIICJzCCAZACAQEwDQYJKoZIhvcNAQEEBQAwXDELMAkGA1UEBhMCQ1ox
ETAPBgNVBAoTCFBWVCBhLnMuMRAwDgYDVQQDEwdDQS1QVlQxMSgwJgYJKoZIhvcNAQkBFhlj
--------------msAEFE8CC4BBD6CDB2637B5646--
```

Pokud mají odesílatel i příjemce zprávy svůj pár klíčů, je možné zprávu zašifrovat (veřejným klíčem příjemce) i digitálně podepsat (tajným klíčem odesílatele), takže je pak dokonale chráněna, protože příjemce ví, že

- zprávu si po cestě nikdo třetí nepřečetl (šifrování)
- zprávu odeslal skutečně ten, kdo je pod ní podepsán (podpis)
- zpráva nebyla po cestě změněna (digest)

To je mnohem lepší zabezpečení než u klasických papírových dokumentů, které nejsou proti změně po cestě nijak chráněny.

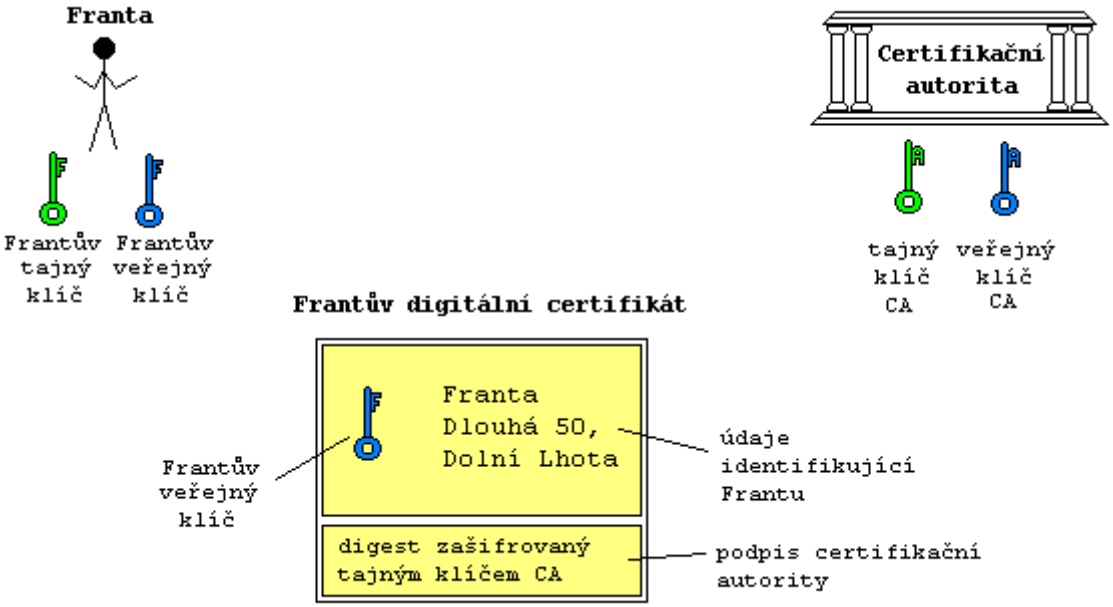
1.3.4 Digitální certifikát

S asymetrickým šifrováním je jedna potíž. Je sice dokonale bezpečné pro daný pár klíčů (veřejný-tajný), ale jak můžeme vědět, že veřejný klíč patří skutečně tomu, komu myslíme ?!?

Představme si, že si chci dopisovat, dejme tomu, s Frantou. Pokud mi svůj veřejný klíč přinese osobně, mám jistotu, že je skutečně jeho. Ale co když Franta žije v Austrálii a nemůžeme se osobně setkat ? Pokud by mi poslal svůj veřejný klíč jen tak nezabezpečeně elektronickou poštou, mohl by nepřítel po cestě podvrhnout svůj veřejný klíč místo Frantova klíče, a pak by si mohl číst všechnu poštu, kterou Frantovi pošlu. Dokonce by ji pak mohl zašifrovat skutečným Frantovým veřejným klíčem a poslat mu ji, takže by si Franta ničeho nevšiml. V opačném směru bych pak zprávy podepsané nepřítelem považoval za zprávy podepsané Frantou. To se v žádném případě nesmí stát. Je tedy nutné jednoznačně svázat veřejný klíč s osobou, které patří. To se řeší zavedením tzv. digitálních certifikátů. Digitální certifikát je něčí veřejný klíč (což je, konec konců, jen informace zapsatelná jako text), spojený s údaji o jeho osobě, a obojí je digitálně podepsané nějakou třetí důvěryhodnou stranou, jejíž veřejný klíč znám. Tato důvěryhodná třetí strana se nazývá certifikační autorita, a je to obvykle všeobecně známá instituce, která digitální certifikát vydává, ale až po ověření totožnosti certifikovaného, například předložením občanského průkazu a rodného listu.

V našem příkladě se tedy s Frantou dohodneme na nějaké certifikační autoritě, kterou oba známe, Franta navštíví její australskou pobočku, předloží svůj veřejný klíč a doklady, načež mu bude vydán jeho digitální certifikát, který mi klidně pošle e-mailem. Nepřítel nebude moci nic udělat, protože nemá tajný klíč certifikační autority, tudíž nemůže vyrobit falešný certifikát. Máme to vyřešeno.

Pro e-mailovou poštu zabezpečovanou systémem S/MIME a pro bezpečný přístup na WWW je známou certifikační autoritou americká firma Verisign, Inc., jejíž veřejný klíč je zakompilován v Netscape Communicatoru i Microsoft Exploreru.



obrázek 7 - Certifikační autorita

Můj digitální certifikát je můj veřejný klíč, spojený s údaji o mé osobě, obojí podepsané certifikační autoritou (spojené dohromady s message digestem zašifrovaným tajným klíčem certifikační autority).

Digitální certifikát nemusím nijak utajovat, protože neobsahuje můj tajný klíč, naopak já ho musím všude šířit.

Certifikační autorita je někdo, obvykle instituce, jejíž veřejný klíč znám, a jíž důvěřuji, že digitální certifikáty vydává až po ověření skutečné totožnosti certifikovaného.

1.3.5 Kombinace symetrické a asymetrické šifry

Asymetrická šifra má tu nevýhodu, že šifrování je značně náročné na výpočetní výkon počítače a proto je pomalé. V praxi se proto používá kombinace se symetrickou šifrou, jejíž používání je rychlé. Pro každou zprávu se vygeneruje náhodný symetrický klíč, který se zašifruje asymetrickou šifrou a pošle adresátovi. Tak se vlastně vytvoří onen bezpečný kanál pro přenos klíče, který symetrické šifře chybí k dokonalosti. Pak se zpráva zašifruje symetrickou šifrou s tímto náhodným symetrickým klíčem a odešle se.

Tuto techniku používají ve velkém všechny používané šifrovací systémy na Internetu - SSL pro zabezpečený přístup na WWW, S/MIME a PGP pro bezpečnou elektronickou poštu i SET pro bezpečné placení.

1.3.6 Poznámka k existenci asymetrické šifry

Pro existenci asymetrické šifry je třeba existence matematické funkce, která je "jednosměrná", tedy lze ze zadání vypočítat výsledek, ale z výsledku nelze zpětně odvodit zadání. Není známo, zda taková funkce existuje. Byly

však nalezeny funkce, které jsou "jednosměrné v dostatečné době", tedy výpočet jedním směrem trvá počítači zlomek vteřiny, ale opačný postup by trval stejnému počítači miliony let. Nejpoužívanější asymetrická šifra RSA využívá toho, že vynásobit dvě stomístná prvočísla je pro počítač hračka, kdežto rozložit vzniklé dvěstěmístné číslo na součin prvočísel znamená vyzkoušet postupně dělitelnost 2, 3, 5, 7 ... atd. až do odmocniny onoho velkého čísla. Tak obrovský počet kroků by trval i mnoha současně pracujícím superpočítačům stovky let. Nicméně, počítá se s pokrokem ve výkonu počítačů, a proto se životnost reálně používaných klíčů omezuje na nejvýše několik let, po jejichž uplynutí je nutné vygenerovat klíče nové.

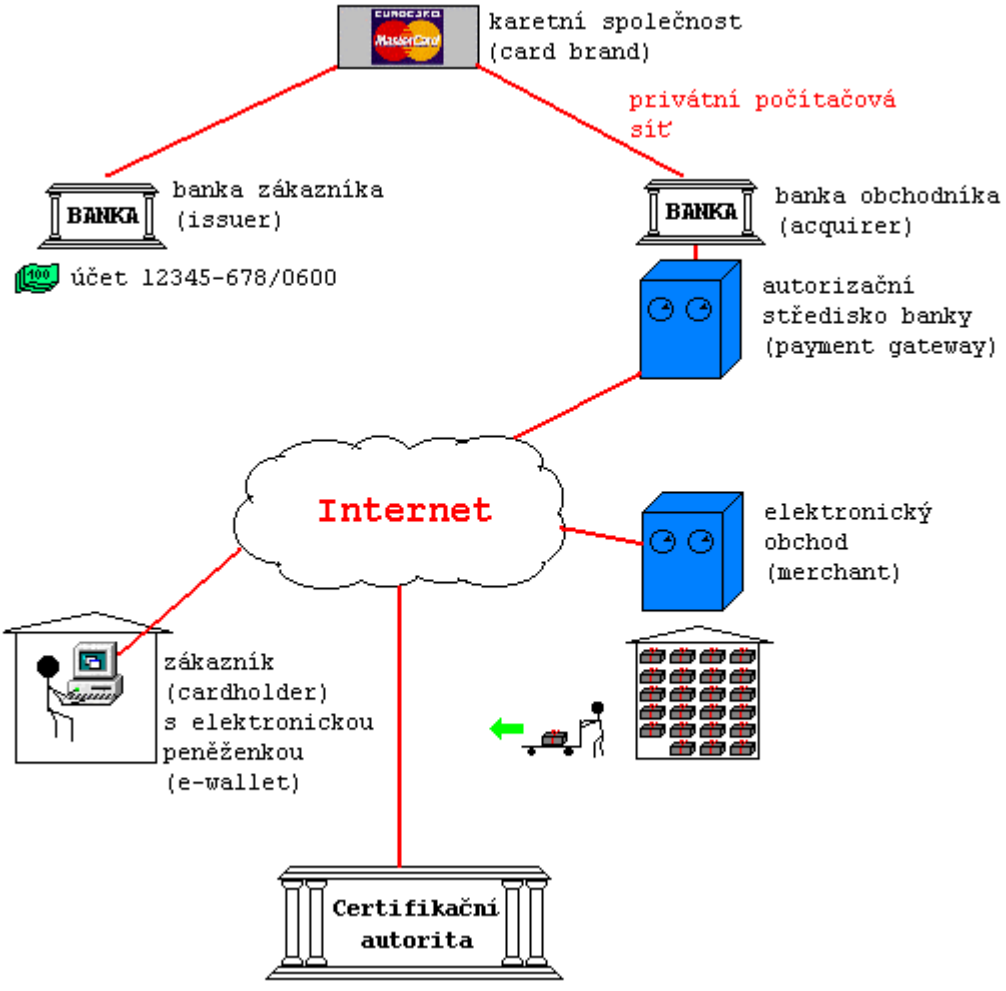
2. SET

SET je komunikační protokol pro provedení bezpečné platby mezi držitelem platební karty a obchodníkem v prostředí nezabezpečené komunikační sítě.

2.1 Úvod do SETu

V Internetových obchodech je největším problémem placení. Zatím jsou reálně používané dvě metody:

- **zaslání na dobírku** - zákazník platí při převzetí zboží na poště. Nevýhody - zákazník musí osobně dojít na poštu. Obchodník tratí na nevyzvednutých zásilkách.
- **nahlášení čísla platební karty** - zákazník zaplatí sdělením osobních údajů a čísla platební karty, stejně jako při placení přes telefon (tzv. MOTO - Mail Order/Telephone Order). Nevýhody: Existuje nebezpečí zneužití čísla karty, proto banky nechtějí uzavírat smlouvy o přijímání karet s Internetovými obchodníky. Obchodník musí vyčlenit pracovní



obrázek 8 - Platební systém se SETem

sílu, která volá na autorizační centrum banky a ověřuje platnost karet, což ho stojí peníze.

Proto hlavní firmy vydávající platební karty - VISA a MASTERCARD - společně s velkými firmami zabývajícími se bezpečností - RSA, Verisign, IBM - vyvinuly SET jakožto protokol, který používáním šifrování, digitálních podpisů a digitálních certifikátů umožňuje provést platbu z bankovního účtu, ke kterému je vydána platební karta (dá se ověřit solventnost majitele účtu), i v prostředí Internetu, tedy sítě, kde procházející data může kdokoliv po cestě odposlouchávat nebo modifikovat.

SET protokol zahrnuje tyto účastníky:

- zákazník (cardholder)
- banka, ve které má zákazník účet s platební kartou (issuer)
- obchodník (merchant)
- banka, se kterou má obchodník smlouvu o přijímání platebních karet (acquirer)
- platební brána (payment gateway) - počítač se speciálním programem umístěný v autorizačním středisku banky obchodníka
- společnost vydávající karty (card brand) - společnost, která je napojena na obě banky, zákazníkovu i obchodníkovu, a umožňuje autorizaci a provedení plateb platebními kartami
- certifikační autorita (certification authority) - instituce, která vydává digitální certifikáty pro všechny zúčastněné po ověření jejich totožnosti

Obě banky a společnost vydávající karty vůbec nemusí být připojeny k Internetu. Certifikační autorita je zapotřebí jen na začátku pro ověření identity zákazníka, obchodníka a platební brány.

Platba probíhá podobně jako u platby platební kartou v kamenném obchodě, až na to, že kromě zákazníka se jí nemusí zúčastnit žádný živý člověk, což šetří náklady. Zákazník, obchodník i platební brána používají speciální program, každý svůj.

Při platbě se zákazníkův program, nazvaný elektronická peněženka, spojí s programem obchodníka, navzájem si předloží své digitální certifikáty, aby věděly, s kým komunikují. Pak elektronická peněženka vyrobí platební příkaz, podepíše ho a zašifruje tak, že si jej může přečíst platební brána banky, ale ne obchodník. Tento platební příkaz pošle programu obchodníka, který ho předá platební bráně banky se žádostí o autorizaci. Platební brána se přes karetní společnost spojí s bankou zákazníka, která platbu buď povolí, nebo zamítne. Výsledek platební brána oznámí obchodníkovi. V kladném případě obchodník odešle zboží a zašle platební bráně žádost o převedení peněz. Tím je celá transakce hotova.

SET přísně odděluje informace určené pro obchodníka od informací pro banku. Obchodník se nikdy nedozví nic o zákazníkově kontu, a naopak banka se nedozví, co zákazník nakoupil.

2.2 Bezpečnost SETu

SET používá 56-bitový DES (Data Encryption Standard) jako symetrickou šifru a 1024-bitový RSA (Rivest-Shamir-Adleman algoritmus) jako asymetrickou šifru. Podle údajů firmy RSA, by ke zlomení 1024-bitového RSA silou, bylo třeba 1.5×10^{11} MIPS roků, tedy práce milionu počítačů o výkonu 1000 MIPS po dobu 150 let. I pak by však útočník získal přístup jen k jednomu páru klíčů. Ke zlomení 56-bitového DES za několik dní je třeba počítač v ceně jednoho milionu dolarů. DESem jsou však šifrovány jen méně důležité údaje, kdežto číslo platební karty a ostatní důležité údaje jsou šifrovány pomocí RSA.

Softwarový systém SET zajišťuje:

- privátnost platebních instrukcí
- důvěrnost informací přenášených společně s platebními instrukcemi
- identifikaci a ověření držitele platební karty
- ověření obchodníkova souhlasu s prováděnou transakcí
- ochranu integrity platebních instrukcí
- certifikaci pro specifické účely

2.3 Postup při placení SETem v obchodním domě

Vlastní placení SETem je velice rychlé a jednoduché. Předpokládejme, že už máte nainstalovánu elektronickou peněženku a v ní zavedenu kreditní kartu, ke které máte vystavený platný certifikát od banky.

Ve Virtuálním Obchodním Domě si vyberete zboží, hodíte ho do košíku a v pokladně vyplníte svoji adresu, na kterou bude zboží zasláno. Jako platební metodu si vyberete SET. Objeví se stránka s tlačítkem "Platím SETem":

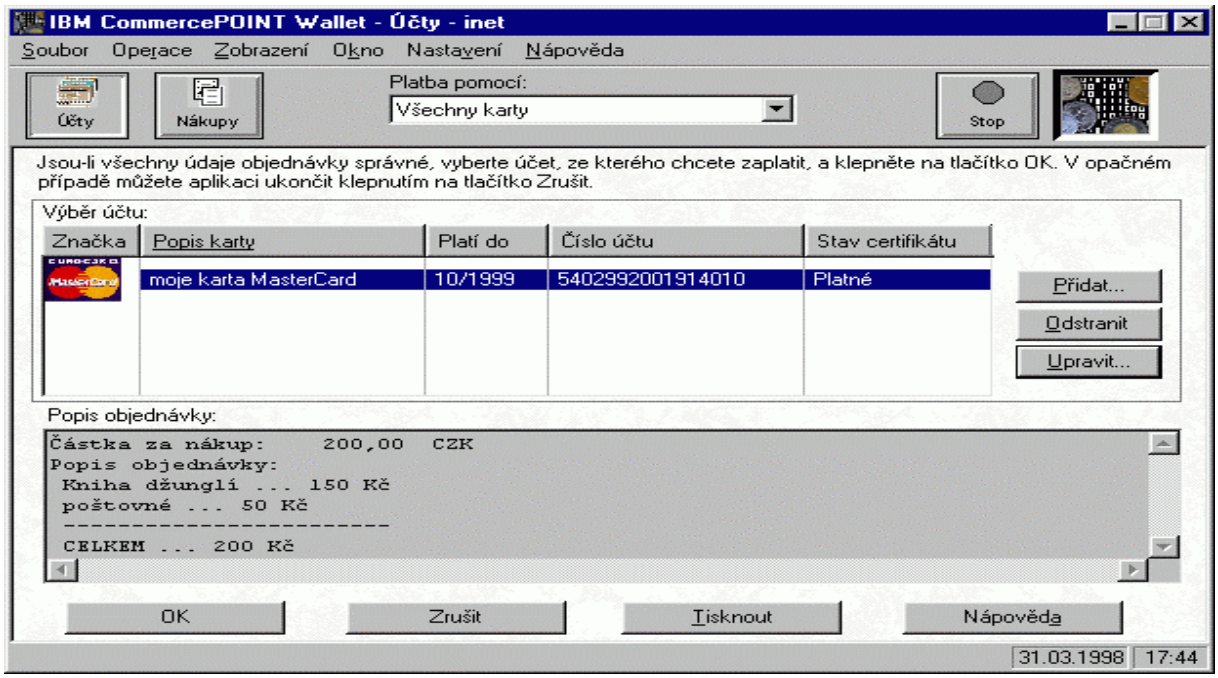
obrázek 9 - Platba SETem

Po zmáčknutí tlačítka „Platím SETem“ se vzbudí elektronická peněženka. Je chráněna heslem, aby jí nemohl použít někdo nepovolaný.

obrázek 10 - Inicializace peněženky

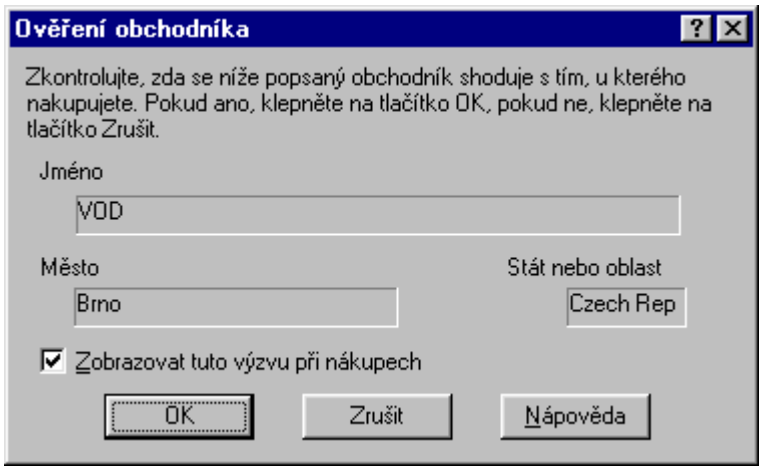
Po zadání správného hesla se peněženka otevře. Pokud máte v peněžence více platných platebních karet, vyberete si, kterou z nich zaplatíte. Pokud máte kartu jen jednu, je vybrána automaticky.

V popisu objednávky je uvedeno, kolik a za co přesně platíte:



obrázek 11 - Peněženka účty

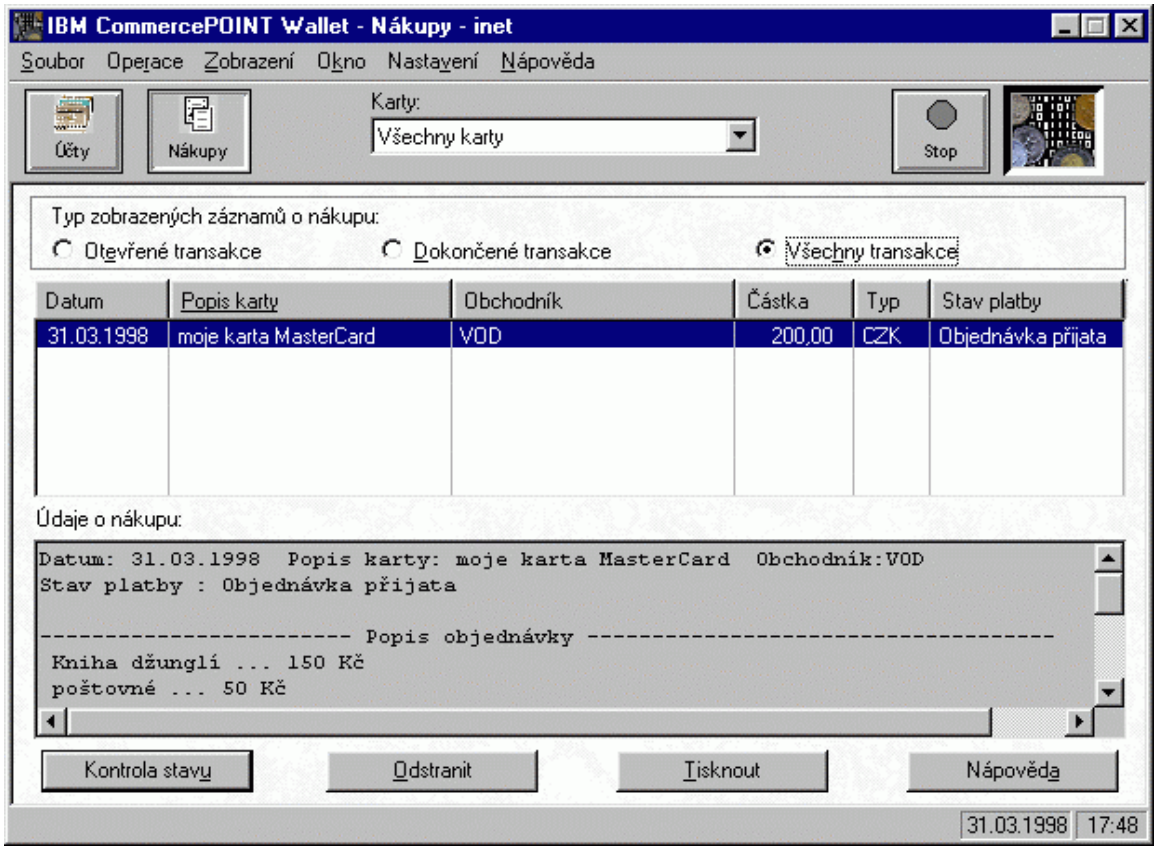
Zmáčknete "OK", načež se objeví certifikát obchodníka. Obsahem certifikátu je skutečná identita obchodníka, jak ji ověřila banka. Na tuto informaci se můžete spolehnout:



obrázek 12 - Ověření obchodníka

Po zmáčknutí "OK" se platba provede, peněženka se sama zavře a prohlížeč zobrazí děkovnou stránku. Tím je nakoupeno.

Pokud si elektronickou peněženku později spustíte sami, máte možnost nechat si vypsat všechny provedené platby:



obrázek 13 - Peněženka - účty

2.4 Detailní popis procesu platby SETem

2.4.1 Úvod k popisu

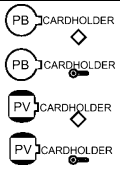
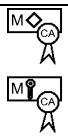
Set definuje různé druhy transakčních protokolů, které využívají kryptografické koncepty již zmíněné v odstavci 1.2, pro zajištění bezpečnosti elektronického obchodu. Dále budou popsány následující transakce:

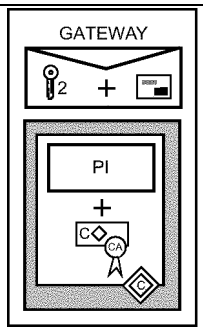
- Registrace zákazníka (Cardholder registration)
- Registrace Obchodníka (Merchant registration)
- Požadavek nákupu (Purchase request)
- Autorizace platby (Payment authorization)
- Uskutečnění platby – předložení transakce k zúčtování bance (Payment capture)

Legenda k následujícím odstavcům:

Iniciála	*Český výraz*	*Anglický výraz*
C	Zákazník	Cardholder
M	Obchodník	Merchant
P	Platební brána	Payment Gateway
CA	Certifikační autorita	Certificate Authority
OI	Objednávkové informace	Order informations
PI	Platební instrukce	Payment instructions

Tabulka symbolů použitých v diagramech:

Symbol	*Popis*
	Toto jsou kryptografické klíče. • „Zuby“ klíče označují vlastníka klíče. • Klíče s PB na držadle jsou veřejné klíče, a klíče s PV jsou privátní klíče. Privátní klíče jsou vždy známy jejim vlastníkům. • Klíče s diamantem (◇) jsou podpisové klíče a s malým klíčem (⊶) jsou klíče na výměnu.
	Toto je digitální podpis. Iniciála označuje čí privátní klíč byl použit k vytvoření podpisu. Např. tento podpis byl vytvořen privátním klíčem obchodníka (merchant).
	Toto je dvojitý podpis. Iniciála označuje čí privátní klíč byl použit k vytvoření podpisu. Např. tento podpis byl vytvořen privátním klíčem zákazníka (cardholder).
	Toto jsou certifikáty. • Iniciála na pečeti označuje čí privátní klíč byl použit k vytvoření certifikátu. • Písmeno na certifikátu označuje veřejný klíč,

	který je certifikován. • Symboly diamantu a klíče rozlišují podpisové certifikáty od certifikátů klíčů na výměnu. „CA“ na těchto symbolech značí, že tyto certifikáty byly vytvořeny certifikační autoritou a „M“ určuje, že je certifikoval obchodník.
	Toto je symetrický klíč použitý na zakódování dat. Vždy bude poslán se zakódovanými daty v digitální obálce. Číslo rozlišuje různé symetrické klíče používané v transakcích.
	Toto je platební karta a je používaná k oznámení, že číslo konta zákazníka je vysíláno v digitální obálce se symetrickým kódovacím klíčem.
	Toto jsou zabezpečená data. Jejich použití reprezentuje poslané informace o kontu v digitální obálce registrační žádosti pro obchodníka a platební bránu.
	Toto je zakódovaná zpráva obsahující digitální obálku. Data v šedém obdélníku byla zakódována použitím náhodně generovaného symetrického klíče (zde jako druhý klíč generovaný pro tuto transakci). Nad obálkou je název entity jejíž klíč byl použit na zakódování obálky (v tomto případě platební brána (payment gateway)). Pozn.: V tomto případě digitální obálka obsahuje symetrický klíč a číslo konta zákazníka. V části zprávy zakódované symetrickým klíčem je obsažen certifikát podpisu zákazníka a byl dvojitě podepsán zákazníkem.

tabulka 1 - Symboly použité v diagramech

2.4.2 Funkce certifikační autority

Základní funkce certifikační autority jsou:

- příjem registračních žádostí
- zpracování a schválení nebo odmítnutí žádosti
- vydání certifikátu

Popis zpracování jejích funkcí je takový, jako by byly vykonávány jedinou entitou, ale příležitostně mohou být vykonávány jednou až třemi entitami. Společnosti vydávající platební karty a individuální platební instituce budou prohlížet jejich obchodní požadavky pro tyto funkce, aby bylo vybráno řešení pro jejich implementaci. Vybrané řešení může být implementováno jako zařízení single-server, které poskytuje certifikační autorita nebo jako násobné zařízení, které je distribuováno zpracováním.

V následujícím seznamu je navrženo několik možných úprav s možnostmi distribuce:

- Společnost vydávající vlastní platební karty může pro svoje zákazníky vykonat všechny tři kroky.
- Finanční instituce může přijmout, zpracovat a schválit žádost certifikace pro svoje zákazníky nebo obchodníky a vrátí informace společnosti vydávající platební karty, která poté vydá certifikát.
- Nezávislá registrační autorita, která zpracovává aplikace certifikátu platebních karet pro několik společností vydávající platební karty, může přijmout žádost o certifikát a poslat jej vhodné finanční instituci (Issuer nebo Acquirer) na zpracování. Finanční instituce vrátí vydanou žádost společnosti vydávající platební karty, která pak vydá certifikát.

2.4.3 Získání certifikátu

2.4.3.1 Certifikace zákazníka

Funkce certifikace zákazníka je elektronická reprezentace platební karty. Protože jsou digitálně podepsány finanční institucí, nemohou být změněny třetí stranou a mohou být generovány pouze finanční institucí. Certifikát zákazníka neobsahuje číslo konta ani datum ukončení platnosti. Místo informací o kontu a tajné hodnoty známé pouze zákazníkovu programu jsou zakódovány použitím jednosměrného hashovacího algoritmu. Jestliže číslo konta, datum ukončení platnosti a tajná hodnota jsou známy, potom odkaz k certifikátu může být vyzkoušen, ale informace nemohou být odvozeny prohlížením certifikátu. V SET protokolu zákazník doplňuje informace o kontu a tajnou hodnotu platební bráně, kde je odkaz ověřen.

Zákazník získá certifikát, jestliže to schválí finanční instituce zákazníka. Žádostí o certifikát zákazník indikuje, že chce uskutečnit obchod elektronickou cestou. Tento certifikát je vyslán obchodníkům se žádostí o koupi a zakódovanými platebními instrukcemi. Po přijmutí zákazníkova certifikátu může být obchodník ujištěn, že číslo konta zákazníka bylo ověřeno finanční institucí vydávající platební karty nebo jejím agentem.

2.4.3.2 Certifikace obchodníka

Funkce certifikace obchodníka je elektronické zastoupení pro značku platební společnosti vydávající platební karty. Protože jsou digitálně podepsány finanční institucí obchodníka, nemohou být změněny třetí stranou a mohou být generovány pouze finanční institucí.

Tyto certifikáty jsou schválené finanční institucí obchodníka a opatřeny ujištěním, že obchodník dodržuje platnou dohodu s bankou obchodníka. Obchodník musí mít nejméně jeden pár certifikátů zúčastněných v SET prostředí, ale může mít také několik párů certifikátů. Obchodník má pár certifikátů pro každou společnost vydávající platební karty, která je akceptuje.

2.4.3.3 Certifikace platební brány

Certifikáty platební brány jsou získány od banky obchodníka nebo od jeho zpracovatelů pro systémy, které zpracovávají autorizaci a přijímají zprávy. Kódovací klíč brány, který zákazník získá z tohoto certifikátu, je použit na zajištění informací o kontu zákazníka.

Certifikáty platební brány jsou vydány bance obchodníka platební společností.

2.4.3.4 Certifikace banky obchodníka

Banka obchodníka musí mít certifikáty v pořádku, aby certifikační autorita mohla přijmout a zpracovat certifikační požadavky přímo od obchodníků přes veřejné a privátní sítě. Tyto banky obchodníků, které vybraly společnosti vydávající platební karty ke zpracování certifikačních žádostí, na ně nebudou potřebovat certifikáty, protože nezpracovávají SET zprávy. Banky obchodníků přijímají jejich certifikáty ze společnosti vydávající platební karty.

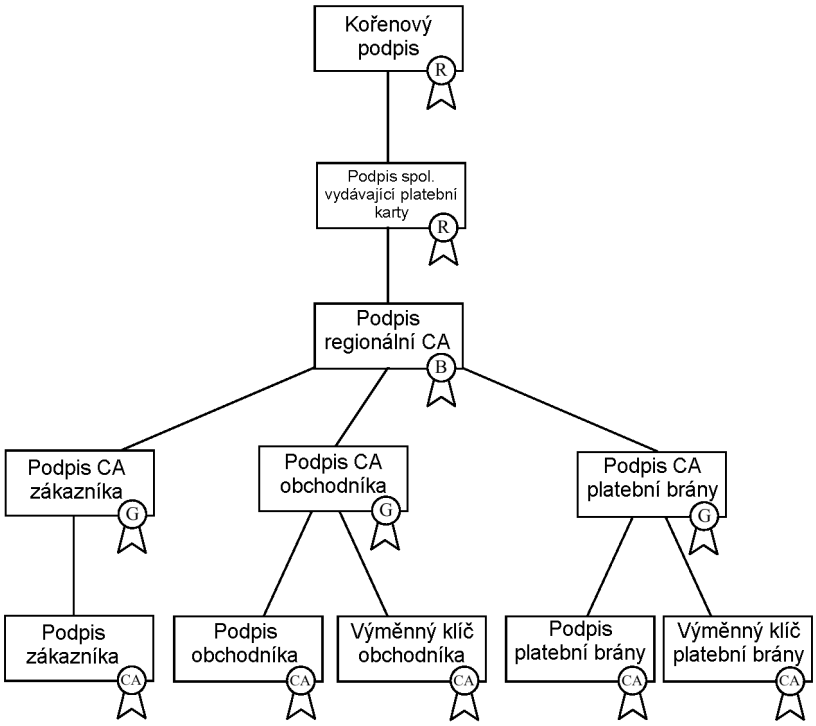
2.4.3.5 Certifikace banky zákazníka

Banka zákazníka musí mít certifikáty v pořádku, aby certifikační autorita mohla přijmout a zpracovat certifikační požadavky přímo od zákazníků přes veřejné a privátní sítě. Tyto banky zákazníků, které vybraly společnosti vydávající platební karty ke zpracování certifikačních žádostí, na ně nebudou potřebovat certifikáty, protože nezpracovávají SET zprávy. Banky zákazníků přijímají jejich certifikáty ze společnosti vydávající platební karty.

2.4.3.6 Hierarchie zabezpečení

SETové certifikáty jsou ověřeny přes hierarchii zabezpečení. Každý certifikát je propojen k podpisovému certifikátu entity, která jej podepsala. Např. certifikát zákazníka je propojen na certifikát banky zákazníka. Certifikát banky zákazníka je zpět propojen ke kořenovému klíči přes certifikát společnosti vydávající platební karty. Veřejný kořenový podpisový klíč je znám všem SET programům a může být použit pro ověření každého certifikátu. Následující diagram zobrazuje hierarchii zabezpečení.

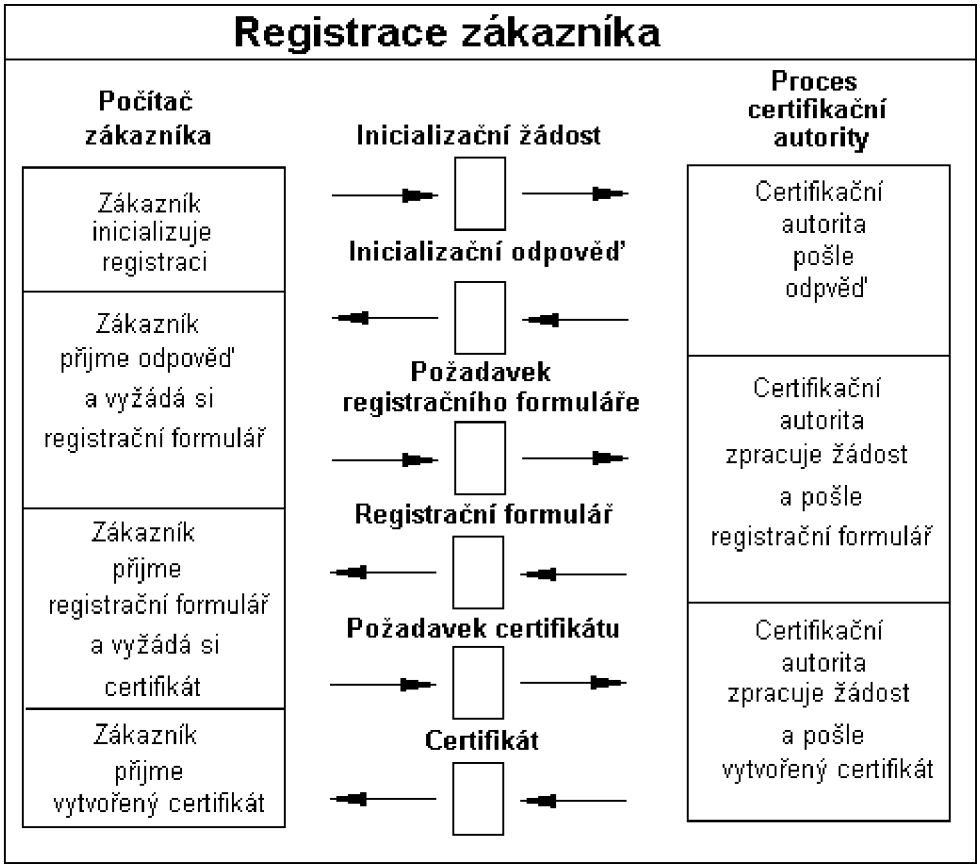
Počet zobrazených stupňů v tomto diagramu je ilustrativní. Společnost vydávající platební karty nemusí vždy pracovat mezi regionální certifikační autoritou a finančními institucemi.



obrázek 14 - Hierarchie zabezpečení

2.4.4 Registrace zákazníka

Na následujícím obrázku je znázorněn proces registrace zákazníka, ukazující sedm základních kroků. Detailní sekce, které následují, popisují jednotlivé kroky.



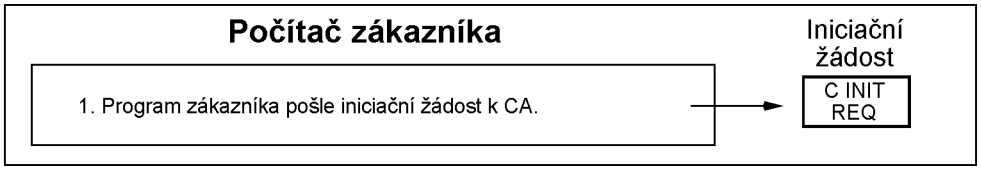
obrázek 15 - Registrace zákazníka

2.4.4.1 Krok č. 1

Zákazník se musí registrovat u CA ještě před tím, než pošle SET zprávy obchodníkovi. Aby mohl poslat SET zprávy CA, musí zákazník mít kopii veřejného výměnného klíče CA, který je v certifikátu výměnného klíče CA.

Zákazník dále potřebuje kopii registračního formuláře ze svého finančního institutu. Aby od CA získal řádný registrační formulář, musí program zákazníka identifikovat vydávající finanční instituci CA. K získání registračního formuláře je zapotřebí dvou výměn mezi programem zákazníka a CA.

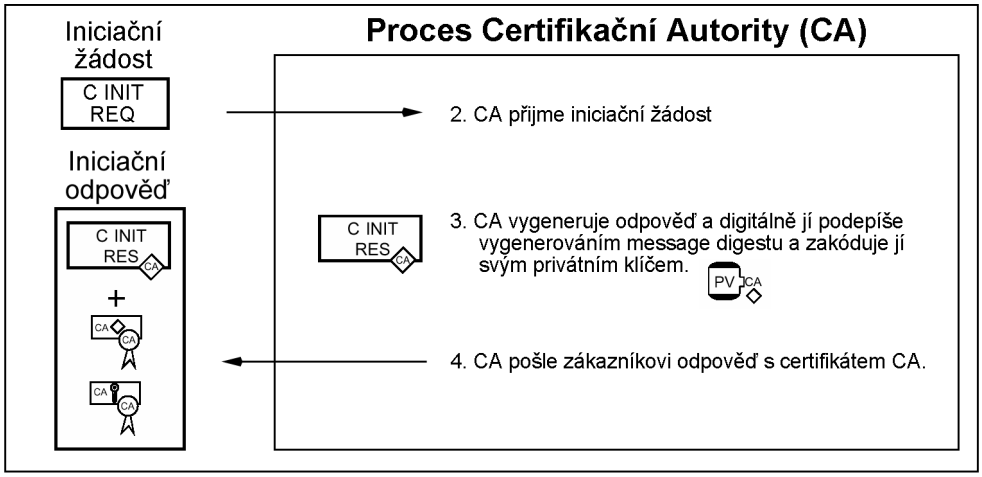
Registrační proces je spuštěn, když si program zákazníka vyžádá kopii certifikátu výměnného klíče CA.



obrázek 16 - Registrace zákazníka - krok č. 1

2.4.4.2 Krok č. 2

Když CA přijme žádost, vyšle její certifikáty k zákazníkovi. Certifikát kódovacího klíče CA opatří program zákazníka s nutnými informacemi k zabezpečení čísla platební karty v žádosti o registrační formulář.



obrázek 17 - Registrace zákazníka - krok č. 2

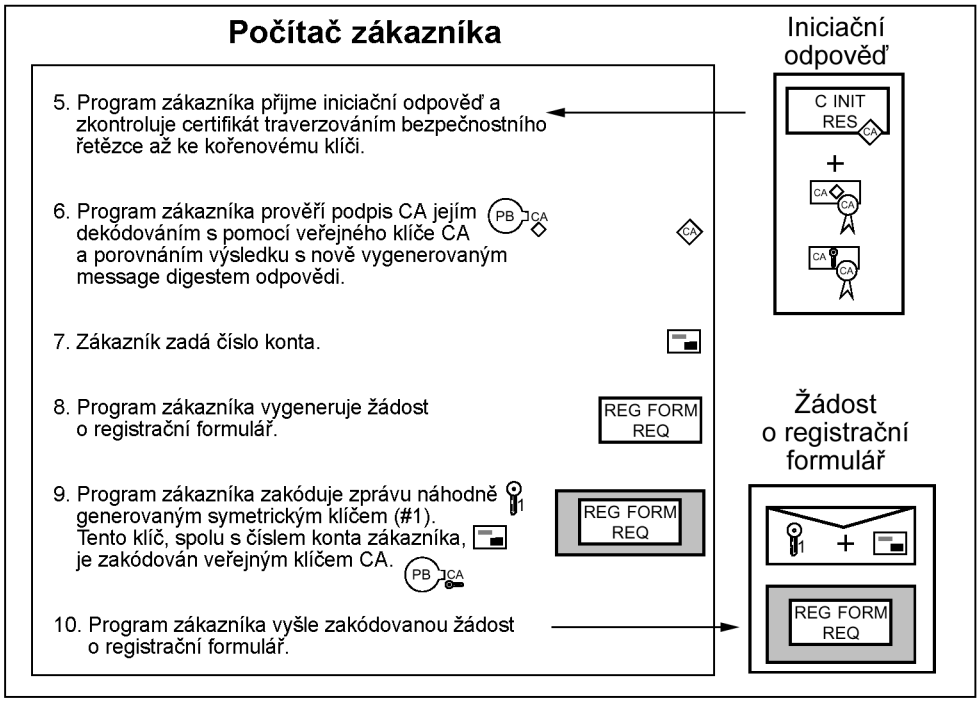
2.4.4.3 Krok č. 3

Program zákazníka ověří certifikát CA traverzováním bezpečnostního řetězce až ke kořenovému klíči. (popsáno v odstavci 2.4.3.6). Program zákazníka musí uchovat certifikáty CA pro pozdější použití během registračního procesu. Má-li jednou program zákazníka kopii certifikátu výměnného klíče CA, může zákazník poslat žádost o registrační formulář.

Program zákazníka vytvoří zprávu žádosti o registrační formulář. Dále program vygeneruje náhodný symetrický kódovací klíč. Tento klíč se použije k zakódování zprávy žádosti o registrační formulář. Náhodný klíč je zakódován spolu s číslem konta do digitální obálky s použitím veřejného výměnného klíče CA. Na závěr program vyšle tyto tři komponenty k CA.

Program zákazníka:

- ověří certifikát CA traverzováním bezpečnostního řetězce až ke kořenovému klíči,
- uchová certifikáty CA k pozdějšímu použití během registračního procesu,
- vytvoří zprávu žádosti o registrační formulář,
- generuje náhodný symetrický kódovací klíč,
- použije náhodný klíč k zakódování zprávy žádosti o registrační formulář,
- zakóduje náhodný klíč spolu s číslem konta do digitální obálky s použitím veřejného výměnného klíče CA,
- vyšle všechny tři komponenty k CA.

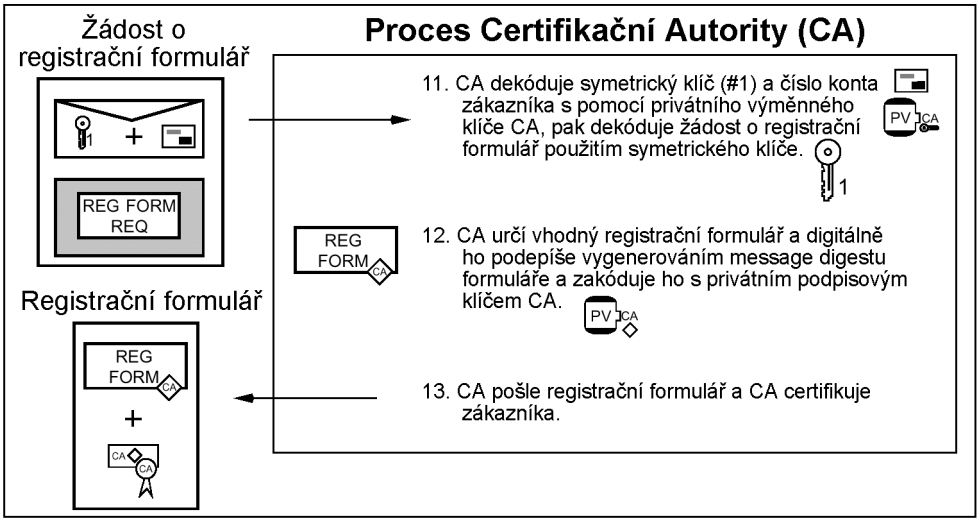


obrázek 18 - Registrace zákazníka – krok č. 3

2.4.4.4 Krok č. 4

CA identifikuje finanční instituci zákazníka (použitím prvních 6-ti z 11-ti číslic čísla konta) a vybere odpovídající registrační formulář pro zákazníka. Digitálně ho podepíše a pak vrátí tento registrační formulář zákazníkovi.

V některých případech, když CA nemá k dispozici kopii registračního formuláře, může informovat program zákazníka, kde může být formulář získán. Např. zákazníkova finanční instituce může pracovat s její vlastní CA. Při této události vrací CA referenční odpověď místo registračního formuláře. (Tato referenční odpověď není zobrazena v těchto diagramech.)



obrázek 19 - Registrace zákazníka – krok č. 4

2.4.4.5 Krok č. 5

Program zákazníka ověří certifikát CA traverzováním bezpečnostního řetězce až ke kořenovému klíči.

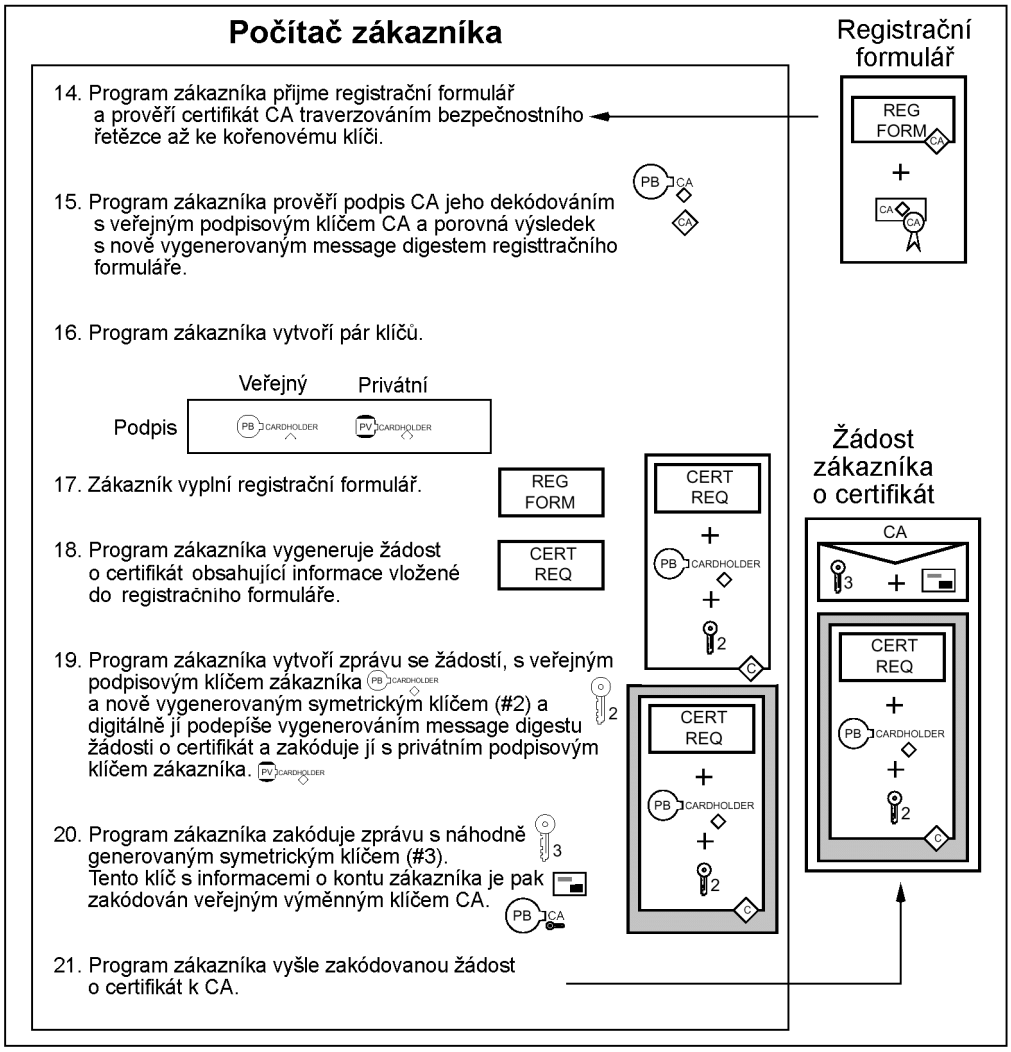
Zákazník potřebuje pár podpisových klíčů (veřejný a privátní) pro použití v SETu. Program zákazníka generuje tento pár klíčů pokud ještě nebyly vytvořeny.

K registraci konta zákazník vyplní registrační formulář, který byl vrácen CA s informacemi (jako jméno zákazníka, datum ukončení platnosti, adresa účetního konta a jiné další informace vydávající finanční instituce nezbytné k identifikaci žadatele o certifikát jako platného zákazníka).

Program zákazníka vygeneruje náhodné číslo, které bude použito CA ke generování certifikátu. Použití tohoto náhodného čísla je popsáno ve zpracování vykonávaném CA.

Program zákazníka vezme tuto registrační informaci a zkombinuje jí s veřejným klíčem v registrační zprávě. Program digitálně podepíše registrační zprávu. Dále program vygeneruje dva náhodné symetrické klíče. Program vloží jeden náhodný symetrický klíč do zprávy (CA použije tento klíč k zakódování odpovědi). Druhý náhodný klíč použije k zakódování registrační zprávy. Tento náhodný klíč je zakódován spolu s číslem konta, datem ukončení platnosti a náhodným číslem do digitální obálky s použitím veřejného výměnného klíče CA. Nakonec program vyšle všechny tyto komponenty k CA.

Pozn.: Jestliže CA vrátí referenční odpověď, popsanou dříve ve zpracování CA, tak se program zákazníka vrátí na začátek registračního procesu, který komunikuje s referenční CA, aby přijal tyto certifikáty CA a vhodný registrační formulář.



obrázek 20 - Registrace zákazníka - krok č. 5

2.4.4.6 Krok č. 6

Když CA přijme žádost zákazníka, dekóduje digitální obálku, aby získala symetrický kódovací klíč, informace o kontu zákazníka a náhodné číslo generované programem zákazníka. Použije symetrický klíč k dekódování registrační žádosti. Pak použije podpisový klíč ve zprávě k ochraně žádosti podepsané použitím odpovídajícího privátního podpisového klíče. Je-li podpis ověřen, zpracovávání zprávy pokračuje, jinak je zpráva zamítnuta a odpovídající odpovědní zpráva je zaslána zákazníkovi.

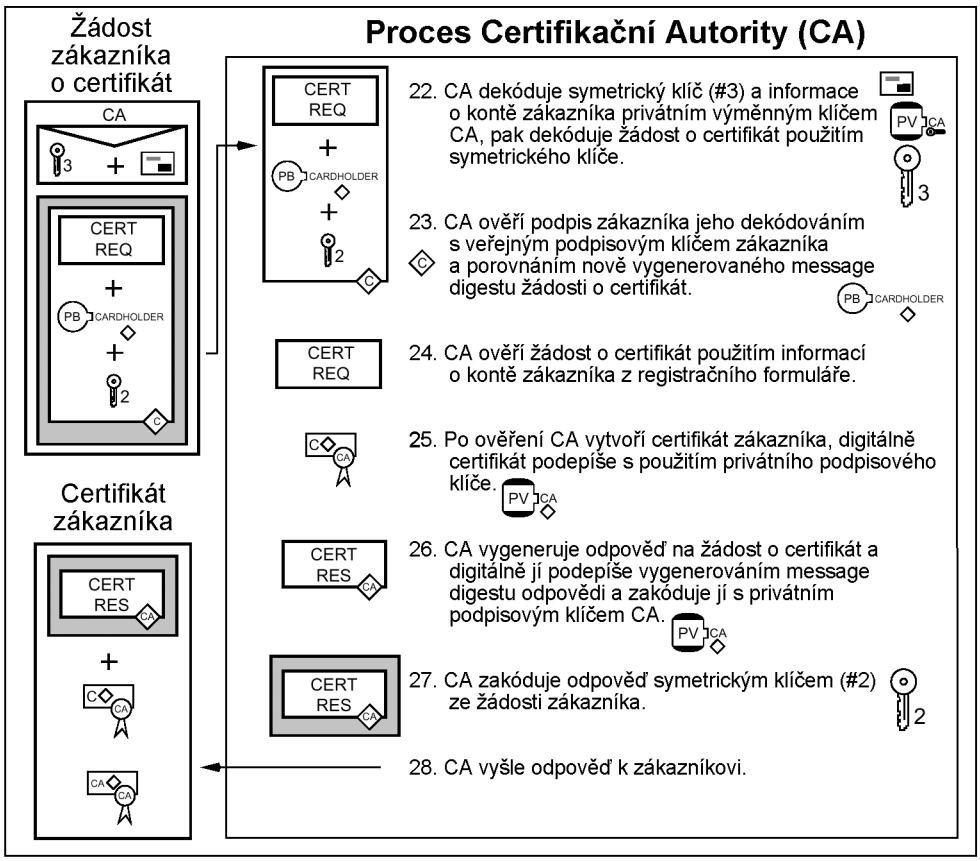
Dále CA musí ověřit informace z registrační žádosti použitím informací o kontu zákazníka. Tak jak bylo popsáno v odstavci 2.4.2, je zde několik cest ke konfiguraci zpracování vykonávajícího CA a banky zákazníka, jako je společnost vydávající platební karty zajišťující všechny nebo pouze některé funkce ve prospěch banky zákazníka nebo si banka zákazníka zajišťuje všechny nebo pouze nějaké funkce sama.

V případě, že informace obsažené v registrační žádosti jsou ověřeny, tak může být vydán certifikát. Nejdříve CA generuje náhodné číslo, které je kombinováno s náhodným číslem vytvořeným programem zákazníka

k vygenerování tajné hodnoty. Tato tajná hodnota je použita k ochraně informací o kontě v certifikátu zákazníka. Číslo konta, datum ukončení platnosti a tajná hodnota jsou zakódovány použitím jednocestného hashovacího algoritmu. Výsledek hashovacího algoritmu je vložen do certifikátu zákazníka. Jestliže číslo konta, datum ukončení platnosti a tajná hodnota jsou známy, propojení certifikátu může být vyzkoušeno, ale informace nemohou být odvozeny prohlížením certifikátu.

Dále CA vytvoří a digitálně podepíše certifikát zákazníka. Doba platnosti tohoto certifikátu bude dána politikou CA, často bude odpovídat datu ukončení platnosti platební karty, ale může být ukončena i dříve.

Odpovědní zpráva obsahuje náhodné číslo generované CA a další informace (jako je logo společnosti vydávající platební karty) jsou pak generovány a zakódovány symetrickým klíčem, který byl poslán zákazníkem v registrační zprávě. Odpověď je pak vyslána k zákazníkovi.



obrázek 21 - Registrace zákazníka - krok č. 6

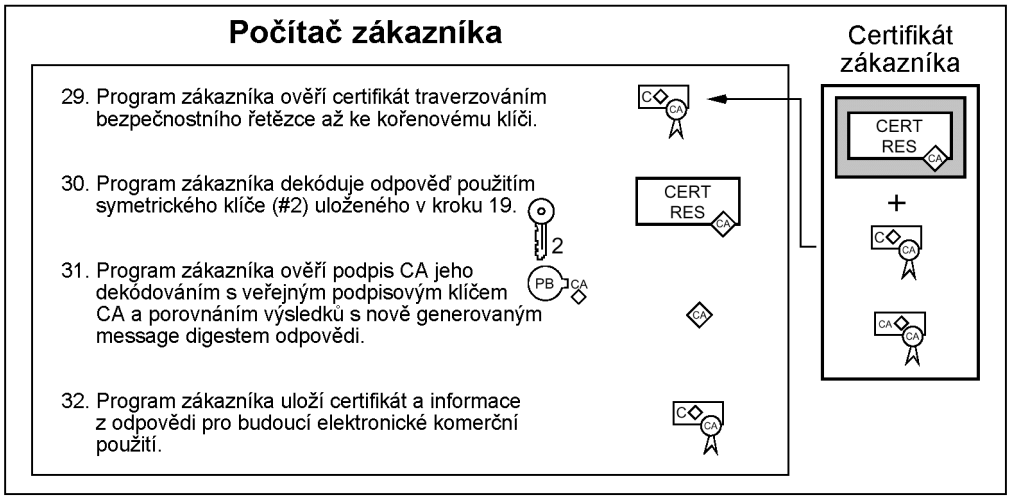
2.4.4.7 Krok č. 7

Když program zákazníka přijme odpověď od CA, tak ověří certifikát traverzováním bezpečnostního řetězce až ke kořenovému klíči. Uloží certifikát v počítači zákazníka pro budoucí použití v obchodních elektronických transakcích.

Dále program zákazníka dekóduje registrační odpověď použitím symetrického kódovacího klíče, který byl poslán CA v registrační odpovědi.

Kombinuje náhodné číslo vrácené CA s hodnotou, kterou poslal v registrační zprávě, aby určil tajnou hodnotu. Poté uloží tajnou hodnotu, aby byla k použití s certifikátem.

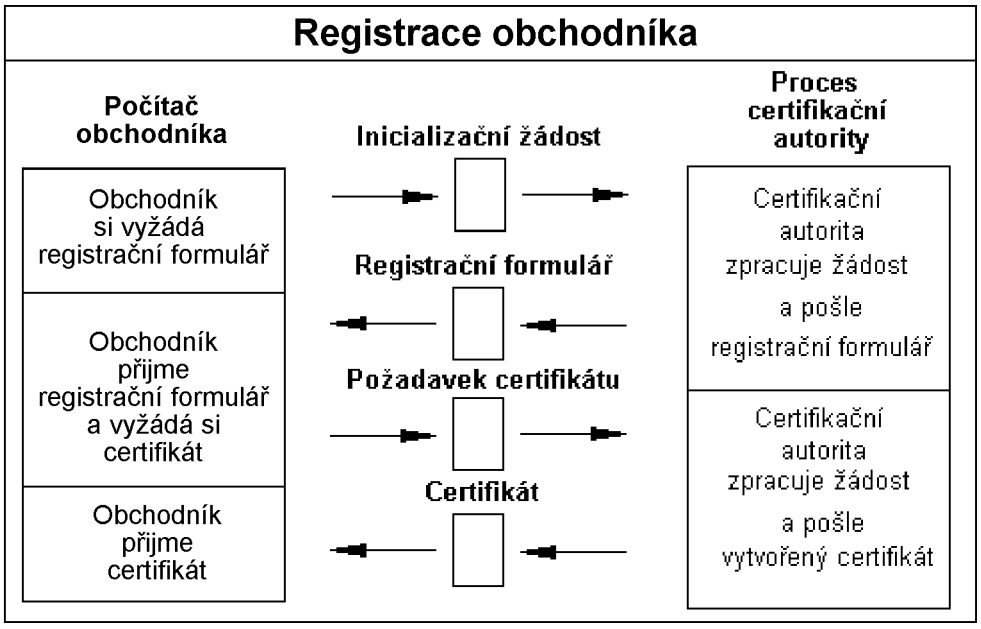
Program zákazníka bude obchodníkům poskytovat tento certifikát a vztažné informace budou uloženy jako prevence proti neautorizovanému přístupu.



obrázek 22 - Registrace zákazníka - krok č. 7

2.4.5 Registrace obchodníka

Na následujícím obrázku je znázorněn proces registrace obchodníka, ukazující pět základních kroků. Detailní sekce, které následují, popisují jednotlivé kroky.



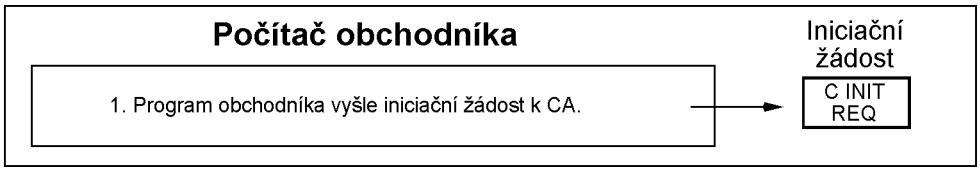
obrázek 23 - Registrace obchodníka

2.4.5.1 Krok č. 1

Obchodníci se musí registrovat u Certifikační autority (CA) ještě před tím, než přijmou platební instrukce SETu od zákazníků nebo budou zpracovávat transakce SETu přes platební bránu. Aby poslali SET zprávy CA, tak musí mít kopii veřejného výměnného klíče CA, který je v certifikátu výměnného klíče.

Obchodník také potřebuje kopii registračního formuláře ze svojí finanční instituce. Program obchodníka musí identifikovat banku obchodníka CA.

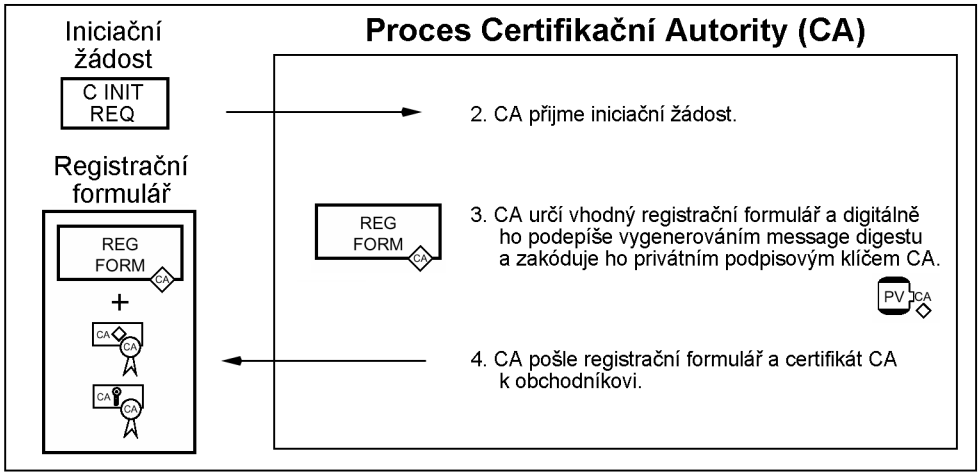
Registrační proces začne, když si program obchodníka vyžádá kopii certifikátu výměnného klíče CA a odpovídajícího registračního formuláře.



obrázek 24 - Registrace obchodníka - krok č. 1

2.4.5.2 Krok č. 2

CA identifikuje finanční instituci obchodníka a vybere odpovídající registrační formulář. Pak vrátí registrační formulář s kopií vlastního certifikátu výměnného klíče obchodníkovi.



obrázek 25 - Registrace obchodníka - krok č. 2

2.4.5.3 Krok č. 3

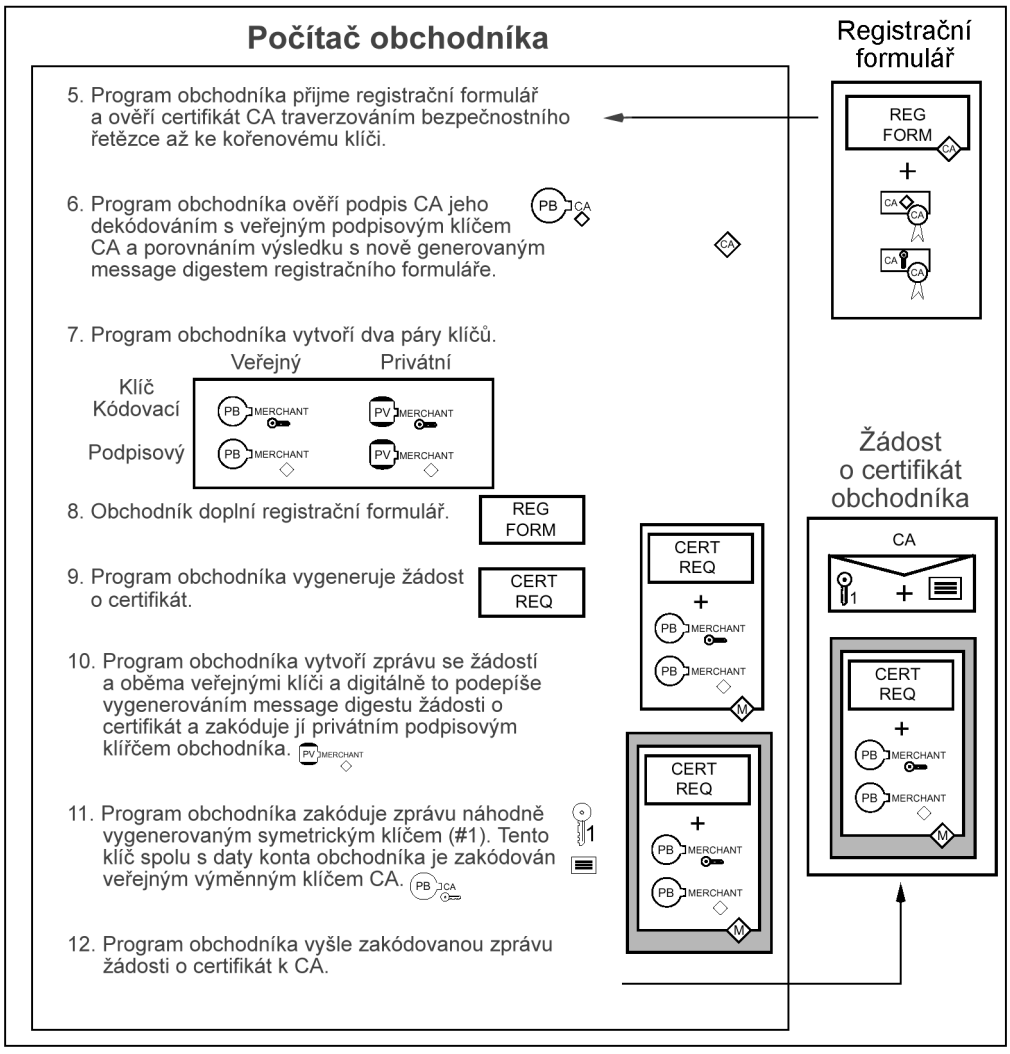
Program obchodníka ověří certifikát CA traverzováním bezpečnostního řetězce až ke kořenovému klíči, pak uchová certifikát CA pro pozdější použití během registračního procesu. Jestliže program jednou dostane kopii certifikátu výměnného klíče CA, pak obchodník může přijímat platební

instrukce SETu a zpracovávat transakce SETu. Ještě dříve než certifikační žádost bude zpracována, tak obchodník musí mít vztah k bance obchodníka.

Obchodník potřebuje dva páry klíčů (veřejné a privátní) pro použití v SETu: výměnný a podpisový klíč. Obchodník si tyto klíče vygeneruje, jestliže tyto klíče ještě neexistují.

Pro registraci obchodník vyplní registrační formulář informacemi jako jsou jméno obchodníka, adresa, obchodní identifikace.

Program obchodníka vezme tyto registrační informace a zkombinuje je s veřejným klíčem do registrační zprávy. Program digitálně podepíše registrační zprávu. Dále program vygeneruje náhodný symetrický kódovací klíč. Ten je použit k zakódování zprávy. Náhodný klíč je zakódován do digitální obálky veřejným výměnným klíčem CA. Nakonec program vyšle všechny komponenty k CA.



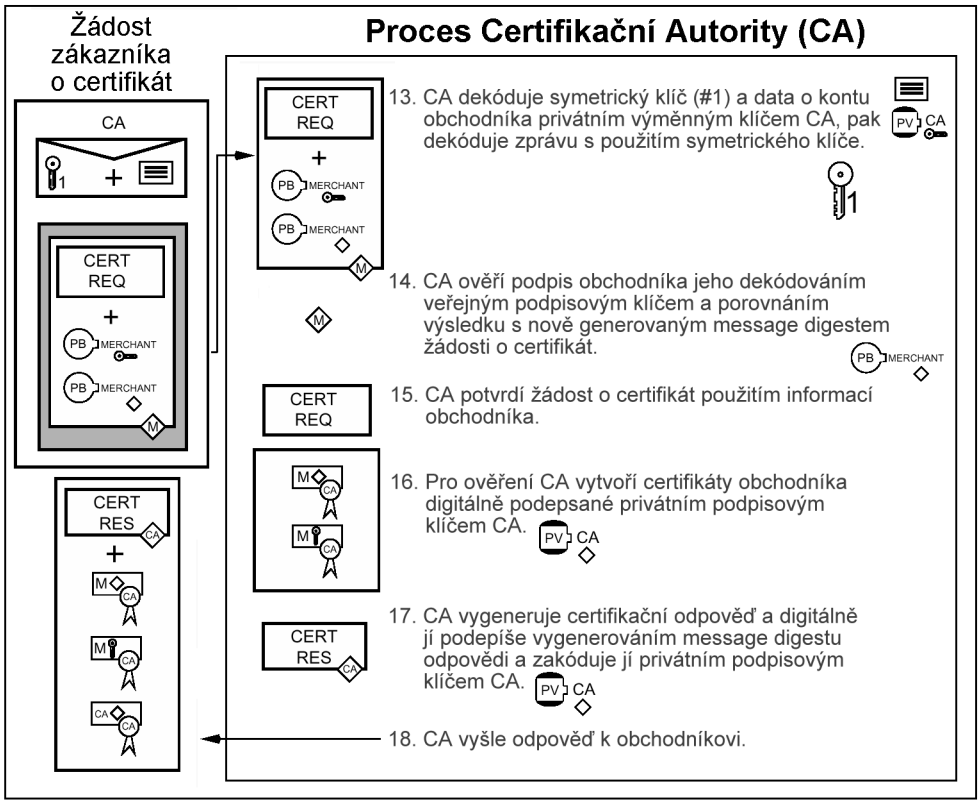
obrázek 26 - Registrace obchodníka - krok č. 3

2.4.5.4 Krok č. 4

Když CA přijme žádost obchodníka, tak dekóduje digitální obálku, aby získala symetrický kódovací klíč, který je použit pro dekódování registrační žádosti. Pak použije podpisový klíč ze zprávy ke zjištění jestli žádost byla podepsána odpovídajícím privátním podpisovým klíčem. Jestliže je podpis ověřen, tak zpracování zprávy pokračuje, jinak je zpráva odmítnuta a odpovídající odpovědní zpráva je zaslána obchodníkovi.

Dále CA musí ověřit informace z registrační žádosti použitím známých informací o obchodníkovi. Tak jak bylo popsáno dříve v úvodu, existuje několik cest ke konfiguraci zpracování vykonávajícího CA a banky obchodníka, jako je společnost vydávající platební karty zajišťující několik nebo všechny funkce ve prospěch banky obchodníka nebo banka obchodníka zajišťuje několik nebo všechny tyto funkce.

Po ověření informací z registrační žádosti CA vytvoří a digitálně podepíše certifikát obchodníka. Doba platnosti tohoto certifikátu bude určena politikou CA, často bude odpovídat datu ukončení platnosti smlouvy s obchodníkem a s bankou obchodníka, ale může být ukončena i dříve. Certifikát je zakódován náhodně generovaným symetrickým klíčem, který je momentálně zakódován veřejným výměnným klíčem obchodníka. Odpověď je vyslána k obchodníkovi.

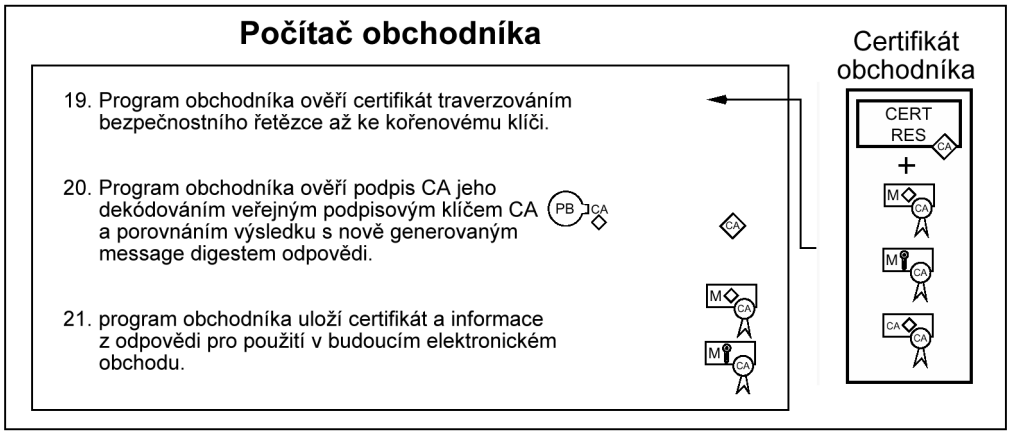


obrázek 27 - Registrace obchodníka - krok č. 4

2.4.5.5 Krok č. 5

Když program obchodníka přijme odpověď od CA, tak dekóduje digitální obálku, aby získal symetrický kódovací klíč. Použije symetrický klíč k dekódování registrační odpovědi obsahující certifikát obchodníka.

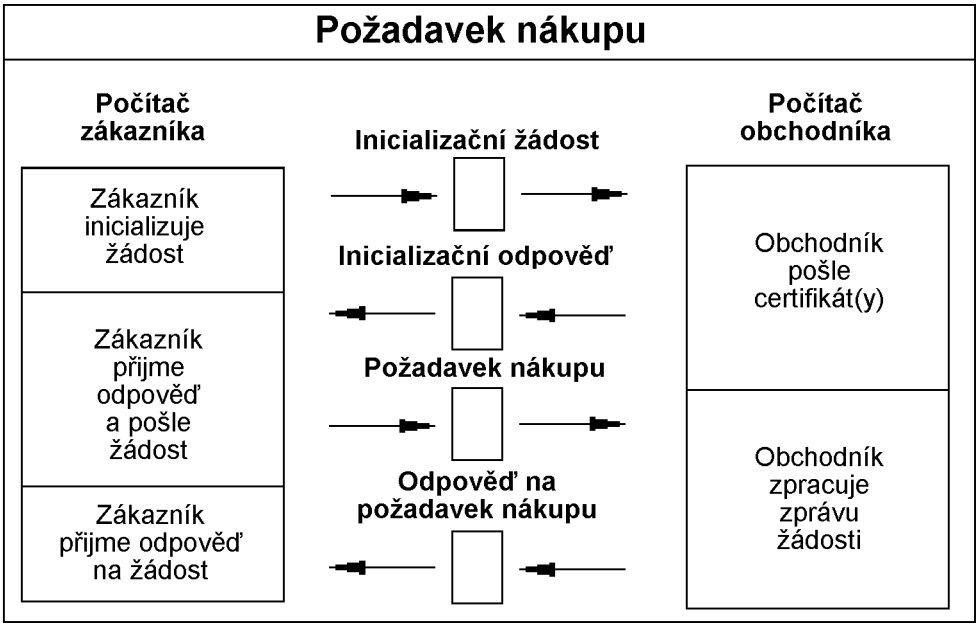
Poté program obchodníka ověří certifikát traverzováním bezpečnostního řetězce až ke kořenovému klíči, dále uloží certifikát v počítači obchodníka, který pak bude v budoucnu použit pro elektronické obchodní transakce.



obrázek 28 - Registrace obchodníka - krok č. 5

2.4.6 Nákupní žádost

Na následujícím obrázku je znázorněn proces nákupní žádosti, ukazující pět základních kroků. Detailní sekce, které následují, popisují jednotlivé kroky.

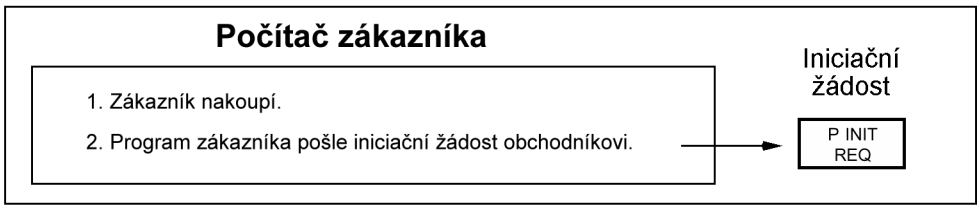


obrázek 29 - Nákupní žádost

2.4.6.1 Krok č. 1

Set protokol je zavolán poté, co zákazník ukončí prohlídku a výběr zboží. Zákazník bude reprezentován úplným nákupním formulářem s odpovídajícím obsahem a podmínkami, jako je číslo splátkové platby, jestliže obchodník je oprávněn pro transakce se splátkami. Dodatečně bude vybrána platební karta zákazníka jako druh platby.

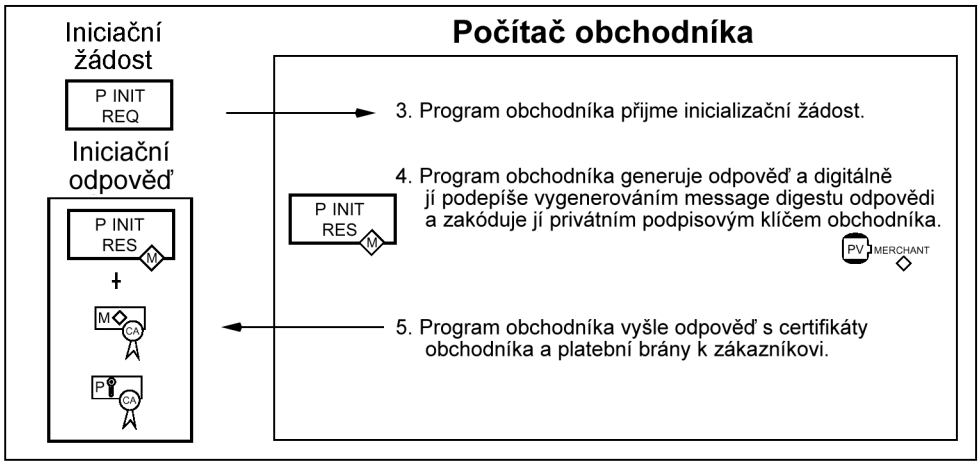
Aby bylo možné poslat SET zprávu obchodníkovi, musí mít zákazník kopii výměnného klíče platební brány. Proces SET objednávky je odstartován, když program zákazníka si vyžádá kopii certifikátu platební brány. Zpráva od zákazníka určuje, která společnost vydávající platební karty bude použita pro transakci.



obrázek 30 - Nákupní žádost - krok č. 1

2.4.6.2 Krok č. 2

Když obchodník přijme žádost, je přiřazen jednotný identifikátor transakce ke zprávě. Ten pak vyšle certifikáty obchodníka a platební brány, které odpovídají společnosti vydávající platební karty určené zákazníkem, spolu s identifikátorem transakce k zákazníkovi.



obrázek 31 - Nákupní žádost - krok č. 2

2.4.6.3 Krok č. 3

Program zákazníka ověří certifikáty obchodníka a platební brány traverzováním bezpečnostního řetězce až ke kořenovému klíči, pak uloží certifikáty pro pozdější použití během objednávkového procesu.

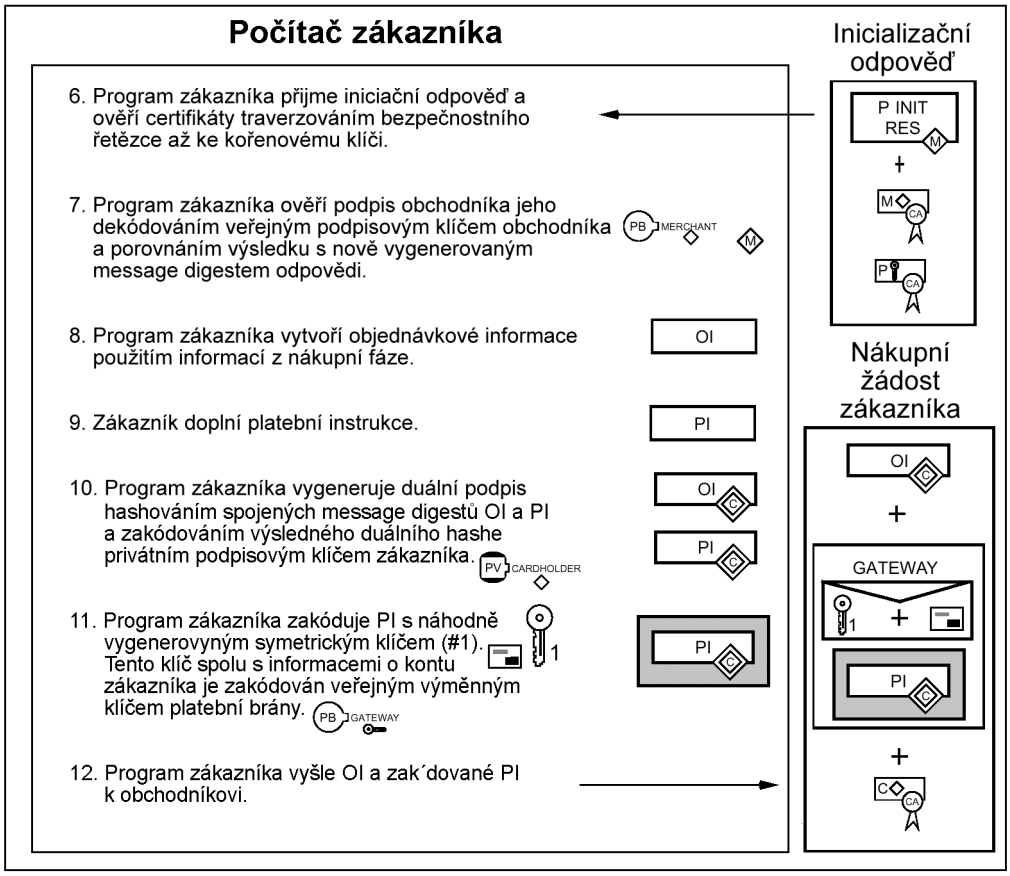
Program zákazníka vytvoří Objednávkové informace (OI) a Platební instrukce (PI). Program vloží identifikátor transakce přiřazený obchodníkem v OI a PI. Tento identifikátor bude použit platební bránou na spojení OI spolu s PI, když si obchodník vyžádá autorizaci.

Pozn.: OI neobsahuje objednávková data jako je popis zboží (položky a počet) nebo podmínky objednání (jako je číslo splátkové platby). Tyto informace jsou vyměněny mezi programy zákazníka a obchodníka během nákupní fáze ještě před první SET zprávou.

Program zákazníka vygeneruje duální podpis pro OI a PI vypočítáním message digestů pro OI a PI, spojením obou digestů, vypočítáním message digestu výsledku a zakódováním privátním podpisovým klíčem zákazníka. Message digesty OI a PI jsou poslány spolu s duálním podpisem.

Dále program vygeneruje náhodný symetrický kódovací klíč a použije ho k zakódování duálního podpisu PI. Program pak zakóduje číslo konta zákazníka právě tak, jako byl použit náhodný symetrický klíč k zakódování PI do digitální obálky, s použitím výměnného klíče platební brány.

Nakonec program vyšle zprávu sestávající se z OI a PI k obchodníkovi.



obrázek 32 – Nákupní žádost – krok č. 3

2.4.6.4 Krok č. 4

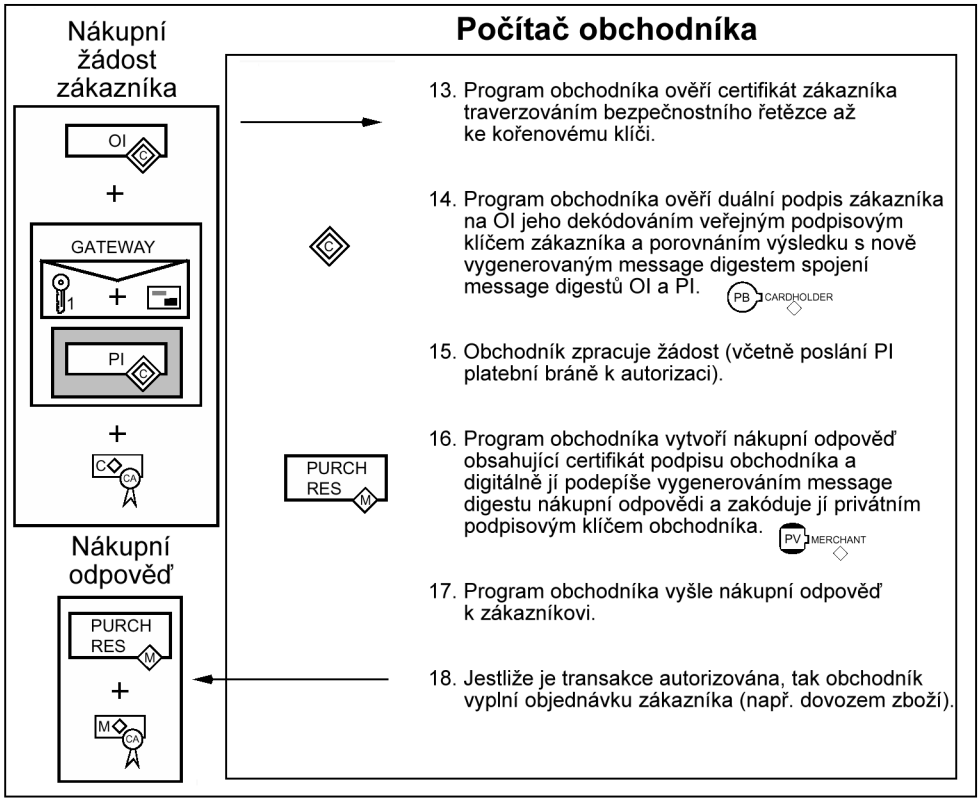
Když program obchodníka přijme objednávku, tak zkontroluje certifikát podpisu zákazníka traverzováním bezpečnostního řetězce až ke kořenovému klíči. Dále použije veřejný podpisový klíč zákazníka a message digest PI (obsažený s OI) ke kontrole digitálního podpisu jestli objednávka nebyla cestou změněna a jestli opravdu byla podepsána privátním podpisovým klíčem zákazníka.

Program obchodníka pak zpracuje objednávku vložením platební autorizace, která je popsána v odstavci 2.4.7.

Pozn.: Pro zákazníka není nezbytné vykonat autorizační fázi dříve než pošle odpověď zákazníkovi. Zákazník může určit jestli autorizace byla vykonána posláním zprávy objednávkového dotazu.

Po zpracování OI program obchodníka vygeneruje a digitálně podepíše zprávu odpovědi, která obsahuje certifikát podpisu obchodníka a určení, jestli objednávka zákazníka byla přijata obchodníkem. Odpověď je vyslána k zákazníkovi.

Jestliže autorizační odpověď indikuje, že transakce byla schválena, tak obchodník dodá zboží nebo vykoná služby určené objednávkou.

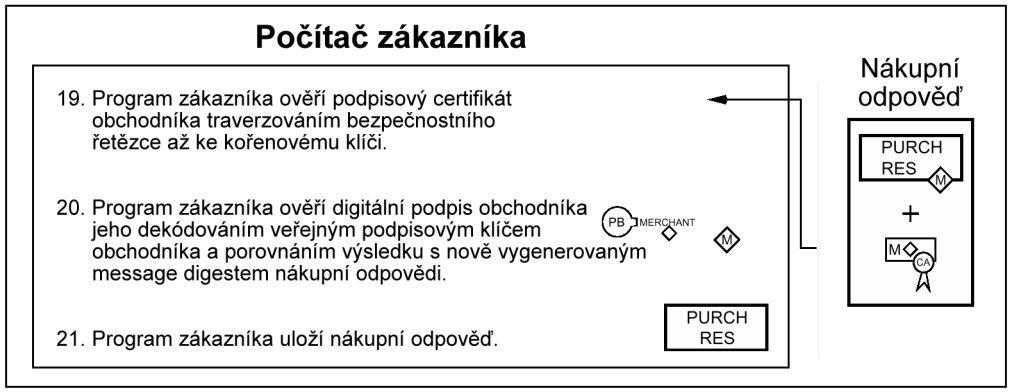


obrázek 33 - Nákupní žádost - krok č. 4

2.4.6.5 Krok č. 5

Když program zákazníka přijme zprávu odpovědi od obchodníka ověří certifikát podpisu obchodníka traverzováním bezpečnostního řetězce až ke kořenovému klíči. Použije veřejný podpisový klíč obchodníka ke kontrole digitálního podpisu obchodníka. Na závěr vykoná několik akcí založených na obsahu zprávy odpovědi, jako je zobrazení zprávy zákazníkovi nebo aktualizace databáze se statusem odpovědi.

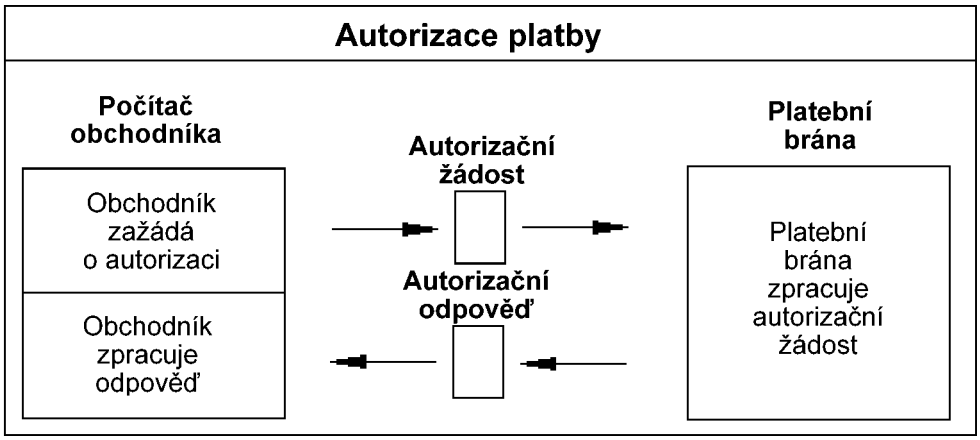
Zákazník může určit status odpovědi (např. zdali byl autorizován nebo odeslán k platbě) posláním zprávy objednávkové informace.



obrázek 34 - Nákupní žádost - krok č. 5

2.4.7 Autorizace platby

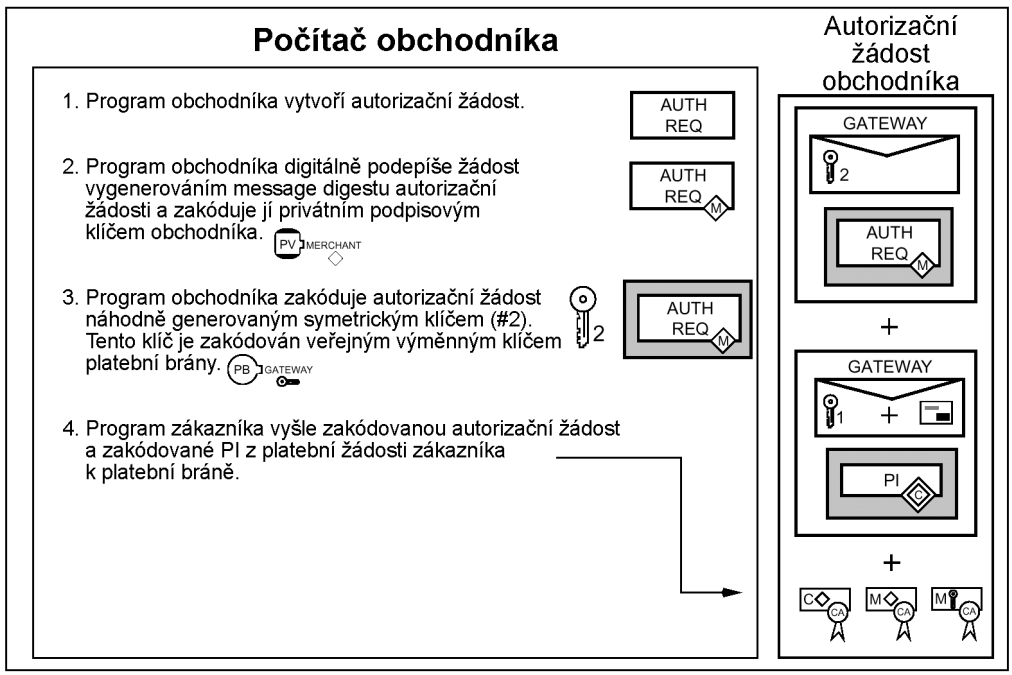
Na následujícím obrázku je znázorněn proces autorizace platby, ukazující tři základní kroky. Detailní sekce, které následují, popisují jednotlivé kroky.



obrázek 35 - Autorizace platby

2.4.7.1 Krok č. 1

Během zpracování objednávky zákazníka (odstavec 2.4.6) obchodník bude autorizovat transakci. Program obchodníka vygeneruje a digitálně podepíše autorizační žádost, která obsahuje částku pro autorizaci, identifikátor transakce z OI a další informace o transakci. Žádost je zakódována náhodně generovaným symetrickým klíčem, který je momentálně zakódován veřejným výměnným klíčem platební brány. (Je to



obrázek 36 - Autorizace platby – krok č. 1

ten samý klíč, který zákazník použil k zakódování digitální obálky platebních instrukcí.) Autorizační žádost a platební instrukce jsou vyslány k platební bráně.

Pozn.: SET protokol také obsahuje prodejní transakce, které dovolují obchodníkovi autorizovat transakci a platební žádost v jediné zprávě.

2.4.7.2 Krok č. 2

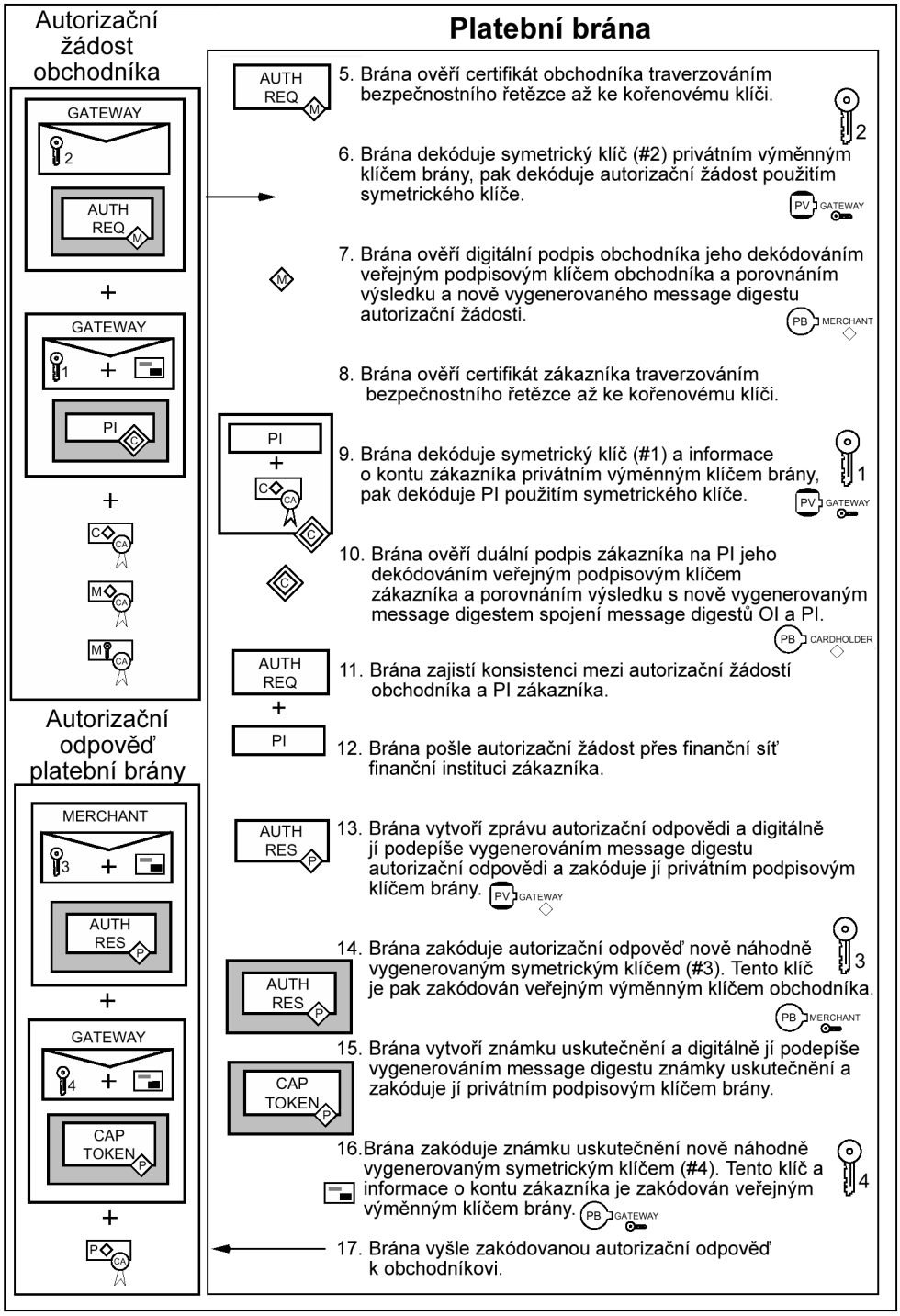
Když platební brána přijme autorizační žádost, tak dekóduje digitální obálku autorizační žádosti, aby získala symetrický kódovací klíč. Použije symetrický klíč k dekódování žádosti. Pak ověří certifikát podpisu obchodníka traverzováním bezpečnostního řetězce až ke kořenovému klíči, dále pak ověří jestli doba platnosti certifikátu nevypršela. Použije veřejný podpisový klíč obchodníka jestli opravdu byla podepsána privátním podpisovým klíčem obchodníka.

Dále platební brána dekóduje digitální obálku Platebních instrukcí, aby získala symetrický kódovací klíč a informace o kontu. Symetrický klíč použije k dekódování PI. Ověří certifikát podpisu zákazníka traverzováním bezpečnostního řetězce až ke kořenovému klíči, dále ještě ověří jestli doba platnosti certifikátu nevypršela. Dále použije veřejný podpisový klíč zákazníka a message digest OI (obsaženého v PI) ke kontrole digitálního podpisu jestli PI nebyly cestou změněny a jestli opravdu byly podepsány privátním podpisovým klíčem zákazníka.

Platební brána ověří identifikátor transakce přijatý od obchodníka odpovídající jedné z platebních instrukcí zákazníka. Platební brána poté zformuluje a pošle platební žádost bance zákazníka přes platební systém.

Po obdržení autorizační odpovědi od banky zákazníka, platební brána vygeneruje a digitálně podepíše zprávu autorizační odpovědi, která obsahuje odpověď banky zákazníka a kopii certifikátu podpisu platební brány. Odpověď také obsahuje volitelné označení platby s informacemi platební brány potřebné pro zpracování žádosti o uskutečnění platby (viz. odstavec 2.4.8). Označení platby je vloženo pouze tehdy, vyžaduje-li to banka obchodníka.

Odpověď je zakódována použitím nového náhodně generovaného symetrického klíče, který je momentálně zakódován veřejným výměnným klíčem obchodníka. Odpověď je poté zaslána obchodníkovi.



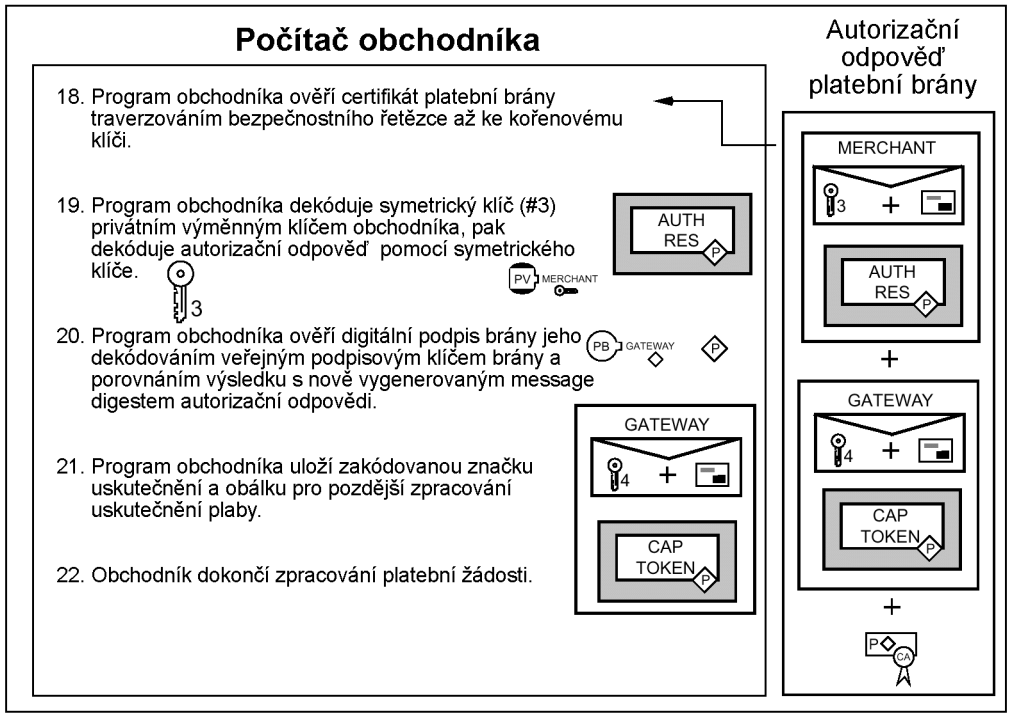
obrázek 37 - Autorizace platby – krok č. 2

2.4.7.3 Krok č. 3

Když program obchodníka přijme zprávu autorizační odpovědi od platební brány, tak dekóduje digitální obálku, aby získal symetrický kódovací klíč. Symetrický klíč použije k dekódování zprávy odpovědi. Poté ověří certifikát podpisu platební brány traverzováním bezpečnostního řetězce až

ke kořenovému klíči. Použije veřejný podpisový klíč platební brány ke kontrole digitálního podpisu platební brány.

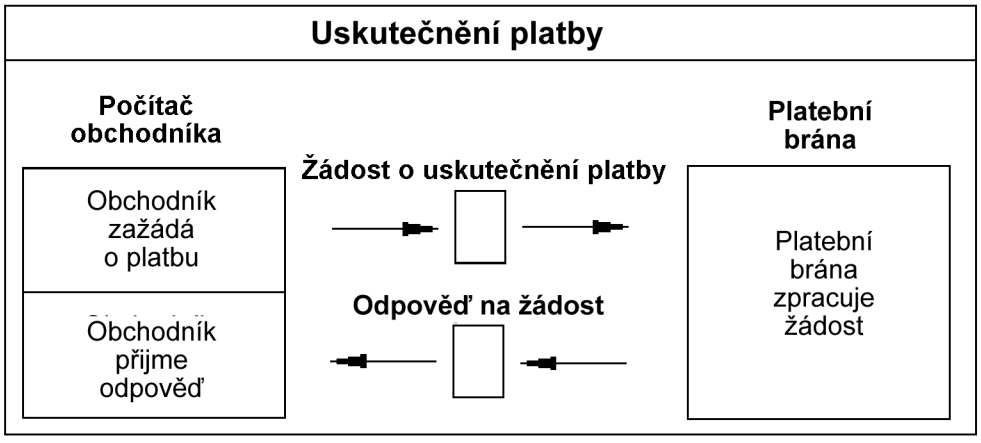
Program obchodníka uloží autorizační odpověď a označení platby bude použito až při žádosti platby přes žádost o uskutečnění platby (viz. odstavec 2.4.8). Obchodník poté ukončí zpracování objednávky zákazníka (viz. odstavec 2.4.6) dodávkou zboží nebo provedením služeb určených v objednávce.



obrázek 38 - Autorizace platby – krok č. 3

2.4.8 Uskutečnění platby

Na následujícím obrázku je znázorněn proces uskutečnění platby, ukazující tři základní kroky. Detailní sekce, které následují, popisují jednotlivé kroky.



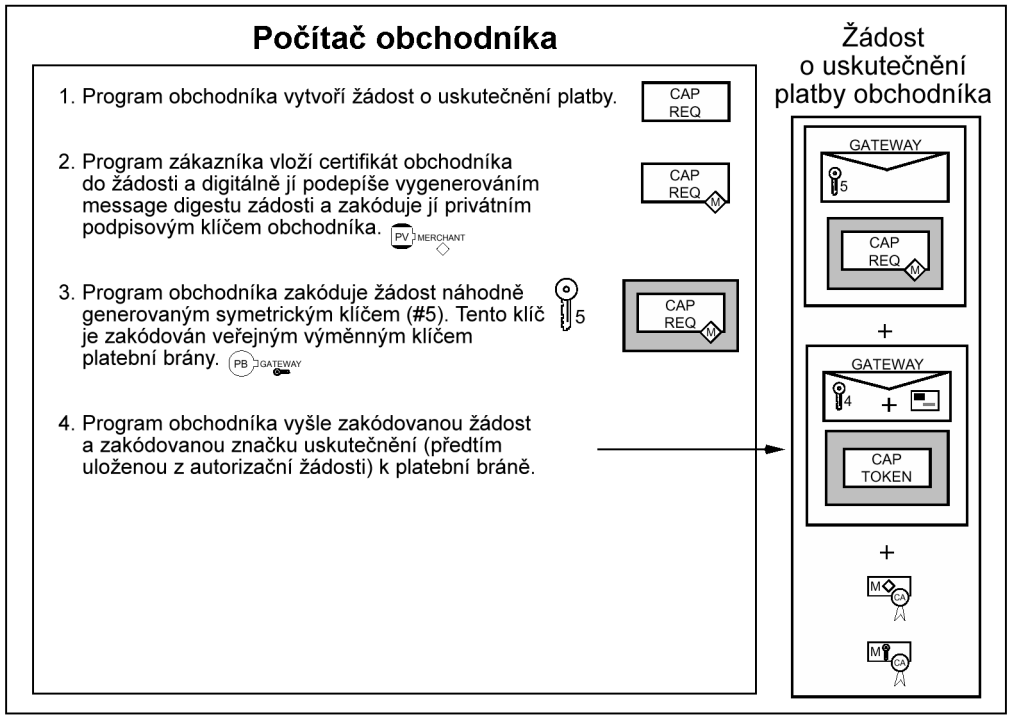
obrázek 39 - Uskutečnění platby

2.4.8.1 Krok č. 1

Po ukončení zpracování objednávky bude obchodník od zákazníka (viz. odstavec 2.4.6) vyžadovat platbu.

Program obchodníka vygeneruje a digitálně podepíše žádost o uskutečnění platby, která obsahuje koncovou částku transakce, identifikátor transakce z OI a další informace o transakci. Žádost je zakódována nově náhodně vygenerovaným symetrickým klíčem, který je momentálně zakódován veřejným výměnným klíčem platební brány. Žádost o uskutečnění platby a volitelné označení platby, jestliže bylo vloženo do autorizační odpovědi (viz. odstavec 2.4.7), jsou vyslány k platební bráně.

Pozn.: Průběh zde popsaný obsahuje pouze jednoduchou žádost o uskutečnění platby, ale program obchodníka dovoluje více žádostí v jedné zprávě.



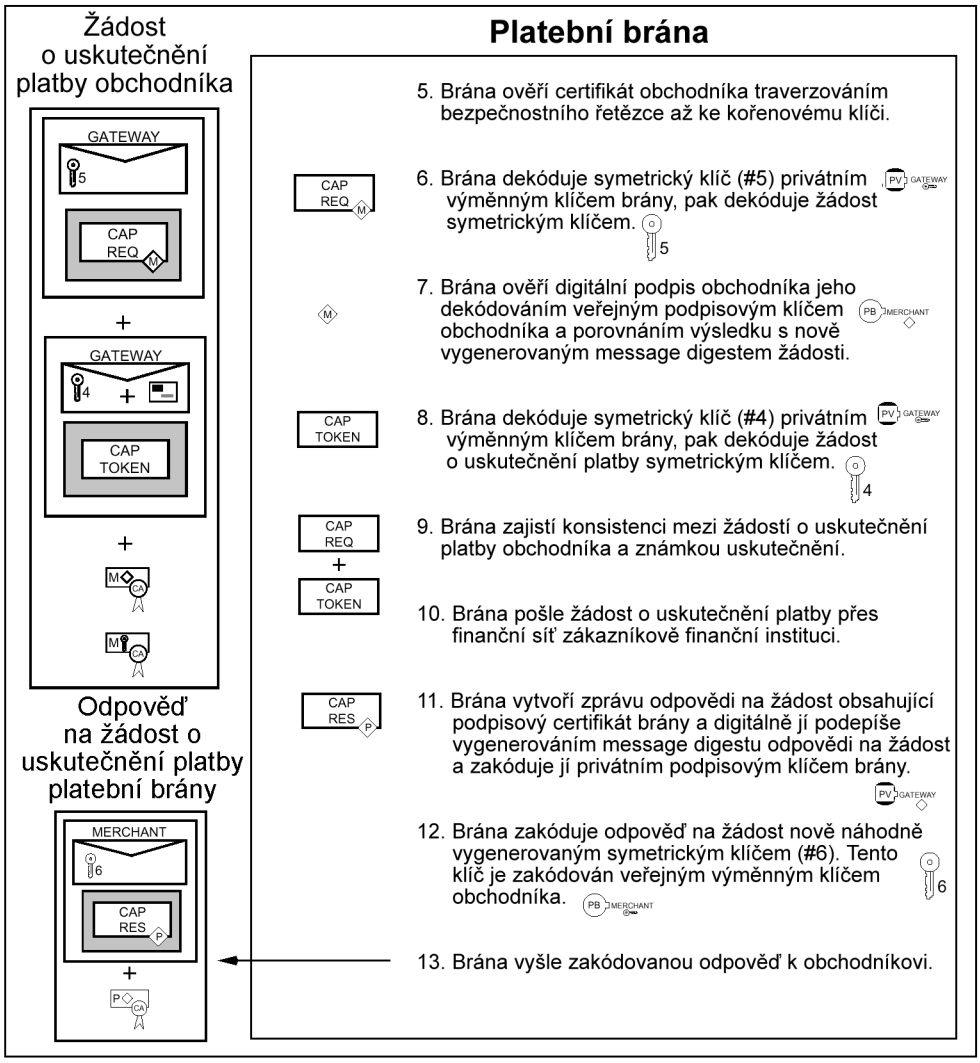
obrázek 40 - Uskutečnění platby - krok č. 1

2.4.8.2 Krok č. 2

Když platební brána přijme žádost o uskutečnění platby, tak dekóduje digitální obálku žádosti, aby získala symetrický kódovací klíč.Tímto symetrickým klíčem dekóduje žádost. Použitím veřejného podpisového klíče obchodníka zkontroluje, jestli žádost byla podepsána privátním podpisovým klíčem obchodníka.

Platební brána dekóduje označení platby, jestliže je přítomno, a použije informace ze žádosti o uskutečnění platby a označení platby k formulování čistící žádosti, která je poslána bance zákazníka přes systém platby platebních karet.

Platební brána vygeneruje a digitálně podepíše zprávu odpovědi, která obsahuje kopii certifikátu podpisu platební brány. Odpověď je zakódována nově náhodně vygenerovaným symetrickým klíčem, který je momentálně zakódován veřejným výměnným klíčem obchodníka. Poté je odpověď poslána obchodníkovi.

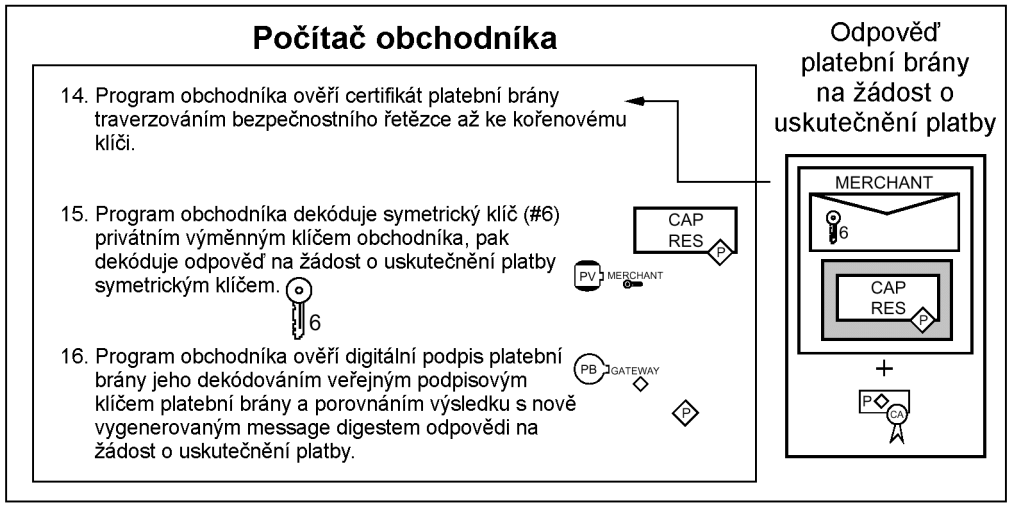


obrázek 41 - Uskutečnění platby - krok č. 2

2.4.8.3 Krok č. 3

Když program obchodníka přijme zprávu odpovědi od platební brány, dekóduje digitální obálku, aby získal symetrický kódovací klíč. Symetrický klíč použije k dekódování zprávy odpovědi. Ověří certifikát podpisu platební brány traverzováním bezpečnostního řetězce až ke kořenovému klíči. Použitím veřejného podpisového klíče platební brány ověří digitální podpis platební brány.

Program obchodníka uloží odpověď na žádost o uskutečnění platby, aby byla použita pro spárování s platbou z banky obchodníka.



obrázek 42 - Uskutečnění platby - krok č. 3

3. Vývoj SETu

3.1 Vývoj v České Republice

Začátkem roku 1997 byl zahájen pilotní projekt implementace SETu v České republice. Dne 29. dubna 1998 byla provedena první platba SETem a tím odstartovala testovací fáze projektu. Této fáze se mohli zúčastnit všichni držitelé karet MasterCard Komerční banky, ale provoz byl technicky omezen na Českou republiku.

Účastníky pilotního projektu jsou:

- **Komerční banka** (issuer i acquirer)
- **I.S.C. MUZO** (cardholder CA, merchant CA, payment gateway)
- **INET** (merchant)
- **IBM** (dodavatel technologie)

Platby SETem přijímají tito obchodníci:

- **Virtuální obchodní dům** – http://www.shop.cz
- **Česká pojišťovna** – http://ruceni.cpoj.cz
- **VLTAVA** – http://www.vltava.cz
- **HLAVA** – http://hlava.vogel.cz
- **CYBEX On-Line** – http://www.cybex.cz

3.1.1 Historie

- ***březen 1997***
  Byl odstartován pilotní projekt jako čtvrtý na světě. V té době nebyla ještě zveřejněna konečná specifikace protokolu verze 1.0, začalo se tedy s verzí 0.9.

- ***1. červen 1997***
  Byla zveřejněna konečná specifikace protokolu verze 1.0.

- ***prosinec 1997***
  IBM uvedla na trh software implementující SET verze 1.0 pod názvem IBM CommercePOINT

- ***únor 1998***
  Software CommercePOINT dorazil do České republiky

- ***29. dubna 1998***
  Byla provedena první transakce SETem přes Internet v České republice. Provedl ji Dr. Salzman ve Virtuálním Obchodním Domě SHOP.CZ. Od toho okamžiku mohli vybraní klienti Komerční banky platit "naostro" v SHOP.CZ.

- ***Invex 1998 (říjen)***
  Do projektu přistupují další držitelé karet. Zájemci vlastnící kartu EC/MC Komerční banky si mohli nechat vydat SET peněženku s digitálním certifikátem na počkání přímo na výstavě.

- ***únor 1999***
  Objevilo se druhé místo na českém Internetu, kde je možné platit SETem. Povinné ručení za motorová vozidla je od toho okamžiku možné zaplatit v České pojišťovně přes Internet.

- ***12. květen 1999***
  Poslední ze čtveřice softwarových modulů, používaných v pilotním projektu, získal oficiální certifikaci o kompatibilitě se specifikací protokolu SET. Od tohoto okamžiku je možné používat oficiální logo SETu.
  Časový průběh byl následující:
  - 7.10.1998 prošla úspěšně testy elektronická peněženka,
  - 17.11.1998 certifikační autorita,
  - 25.2.1999 platební brána,
  - 12.5.1999 software pro obchodníky. IBM mezitím tuto řadu produktů přejmenovala na **IBM Payment Suite**

- ***květen 1999***
  INET, a.s. začíná nabízet pronájem SET pokladny ve službě SET PROXY.

- ***2. září 1999***
  V pořadí třetí obchodní místo na českém Internetu začalo přijímat platby SETem. Je to www.VLTAVA.cz. Využívá pronájmu služby SET PROXY.

- ***24. září 1999***
  Čtvrté obchodní místo na českém Internetu začalo přijímat platby SETem. Je to www.HLAVA.cz. Používá vlastní platební modul.

- ***14. říjen 1999***
  Páté obchodní místo na českém Internetu začalo přijímat platby SETem. Je to www.CYBEX.cz. Využívá pronájmu služby SET PROXY.

- ***15. říjen 1999***
  Končí pilotní provoz omezený na Českou republiku a klienty Komerční banky.

- ***1. listopad 1999***
  Přechod na mezinárodní provoz s kartami MasterCard. Z obchodů zúčastněných v pilotním projektu od začátku funguje jen www.SHOP.cz.

- ***4. listopad 1999***
  CYBEX přešel na plný provoz.

3.2 Vývoj ve světě

3.2.1 Historie

- ***1. únor 1996***
  VISA a Mastercard oznámili zahájení vývoje nového standardu pro bezpečné placení.

- ***1. červen 1997***
  Zveřejněna specifikace SET v1.0.

- ***19. prosinec 1997***
  Založena SETCo, organizace dohlížející na standard.

- ***29. květen 1998***
  První software prošel testy na kompatibilitu se specifikací. Jsou to **SET peněženky** firem GlobeSet, Terisa, Trintech a Verifone.

- ***15. červen 1998***
  První software pro **obchodníky** prošel testy kompatibility, je to POS firmy GlobeSet.

- ***21. červenec 1998***
  První software pro **certifikační autoritu** prošel testy kompatibility od CA firmy GlobeSet.

- ***28. srpen 1998***
  První software pro **platební bránu** prošel testy kompatibility od Gateway firmy GlobeSet.

- ***7. říjen 1998***
  Další **peněženka**, tentokrát od IBM, prošla testy kompatibility.

- ***17. listopad 1998***
  Další **certifikační autorita** od IBM, prošla testy kompatibility.

- ***11. leden 1999***
  Další software pro **obchodníky** od firmy Trintech, prošel testy kompatibility.

- ***20. leden 1999***
  Další software pro **obchodníky** od firmy VeriFone, prošel testy kompatibility.

- ***16. únor 1999***
  Další **platební brána** od VeriFone, prošla testy kompatibility.

- ***25. únor 1999***
  Další **platební brána** od IBM, prošla testy kompatibility.

- ***26. únor 1999***
  Další **certifikační autorita** od firmy Verisign, prošla testy kompatibility.

- ***19. duben 1999***
  Další **platební brána** od firmy Trintech, prošla testy kompatibility.

- ***12. květen 1999***
  Další software pro **obchodníky** od firmy IBM, prošel testy kompatibility.

- ***19. květen 1999***
  Další dva softwary prošly testy kompatibility. Je to **peněženka** od firmy Brokat a software pro **obchodníky** od firmy CyberCash.

- ***20. květen 1999***
  Další **peněženka** od firmy CyberCash, prošla testy kompatibility.

- ***26. květen 1999***
  Další **peněženka** od firmy Fujitsu, prošla testy kompatibility.

- ***6. červen 1999***
  Další **certifikační autorita** od firmy Fujitsu, prošla testy kompatibility.

- ***8. červen 1999***
  První **serverová peněženka**, od firmy GlobeSet, prošla testy kompatibility.

- ***8. červen 1999***
  První **serverový software pro obchodníky**, od firmy GlobeSet, prošel testy kompatibility.

- ***10. srpen 1999***
  Další **peněženka**, tentokrát od firmy Samsung, prošla testy kompatibility.

- ***10. srpen 1999***
  Další **platební brána** od firmy Fujitsu, prošla testy kompatibility.

- ***10. srpen 1999***
  Další software pro **obchodníky** od firmy Fujitsu, prošel testy kompatibility.

3.3 Jak získat SET jako zákazník

3.3.1 Konkrétně v České republice

Držitelé platebních karet Eurocard/MasterCard vydaných Komerční bankou, a.s. (produkty Interkarta, Gold Card, Business Silver Card, Fischer Card plus, Unikarta) se mohou v případě zájmu obrátit na e-mail: Martin_Zurek@KOBA.CZ. Obratem budou zaslány bližší pokyny a podmínky.
Pokud nemáte kartu EC/MC od Komerční banky, nezbývá než si ji buď pořídit, nebo přesvědčit svou banku, aby taky podporovala SET.

3.3.2 Obecně kdekoliv

Založíte si konto v bance, která podporuje SET. Na toto konto si dáte tolik peněz, aby k němu banka vydala mezinárodně uznávanou kreditní kartu. Touto kreditní kartou můžete vybírat z bankomatů a platit v obchodech. Navíc požádáte banku o vydání SET peněženky. Postup bude vypadat zhruba takto:

- Navštívíte banku osobně, podepíšete smlouvu, banka Vám předá **CD-ROM s instalačními soubory SET peněženky**, dále Vám sdělí **URL stránky certifikační autority** a tzv. **hash kód**, a dohodnete si spolu **heslo** pro prokázání totožnosti u certifikační autority. Tato cesta je jediná, kterou musíte fyzicky podstoupit. Další se již děje prostřednictvím Internetu.
- Přijdete ke svému počítači, který má připojení na Internet a WWW prohlížeč. Z CD-ROMu **nainstalujete peněženku**, ta automaticky nastaví prohlížeč, aby ji spouštěl v okamžiku placení.
- U certifikační autority si **vyžádáte certifikát**. Po jeho obdržení můžete platit SETem.

3.3.3 Obdržení certifikátu

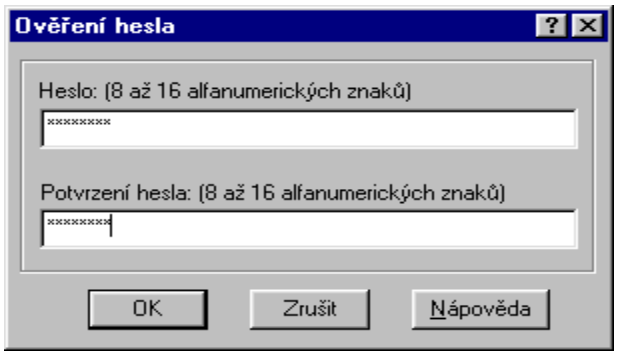
Procedura vydání platného certifikátu vypadá sice složitě, ale je nutné ji absolvovat jen jednou a komplikovaná je kvůli zajištění vysoké bezpečnosti.

Procedura vydání certifikátu:

1. Spustíte prohlížeč WWW a zadáte **URL stránky certifikační autority**. Na této stránce bude odkaz, na který klepnete a spustí se peněženka.

2. Peněženku je možné sdílet mezi více lidmi a je chráněna heslem. Proto při startu peněženky zadáte **uživatele** a **heslo** (pozor, jiné heslo, než které máte dohodnuté s bankou).

obrázek 43 - Inicializace peněženky

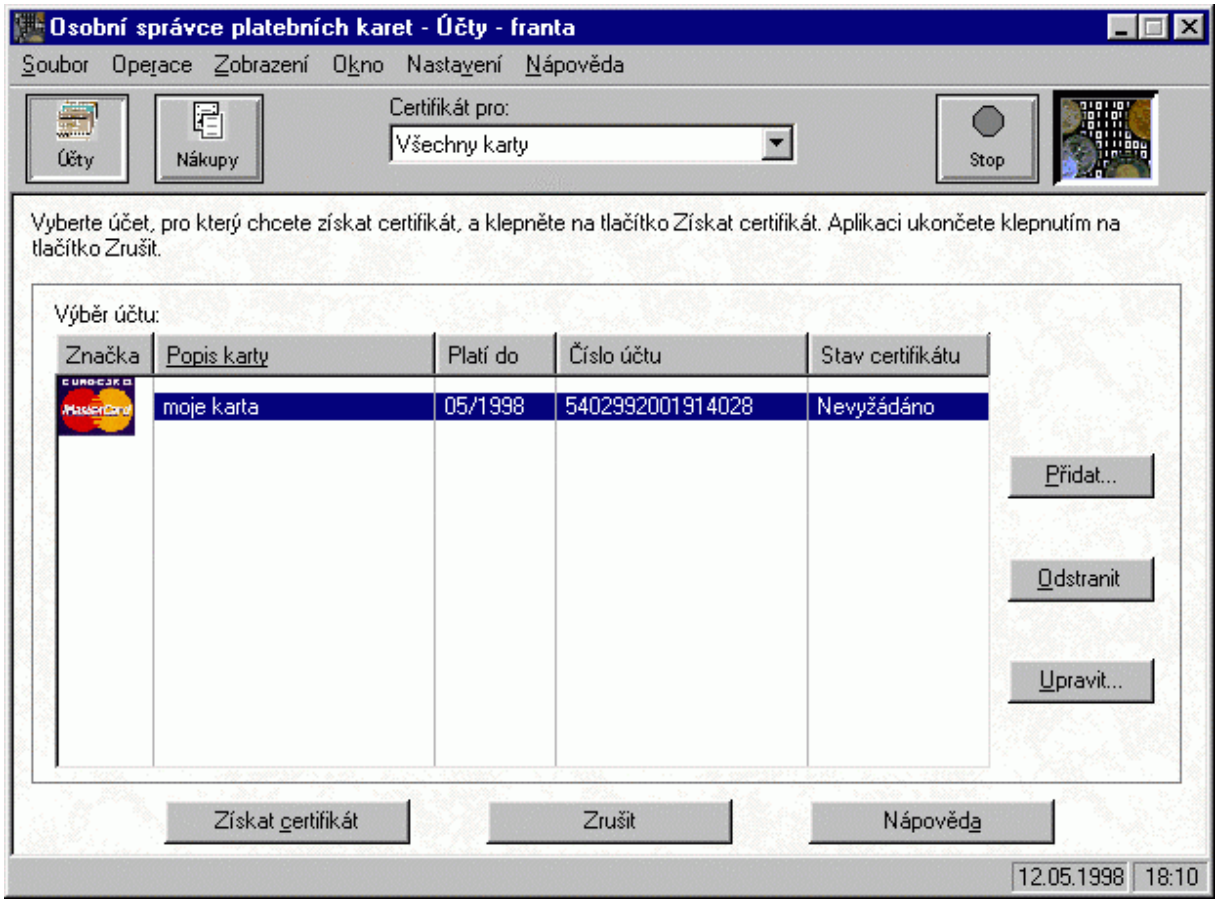


obrázek 44 - Zadání hesla

3. Nová peněženka je prázdná, musíte nejdřív přidat alespoň jednu kartu. Do připraveného formuláře zadáte informace o svém kontu.

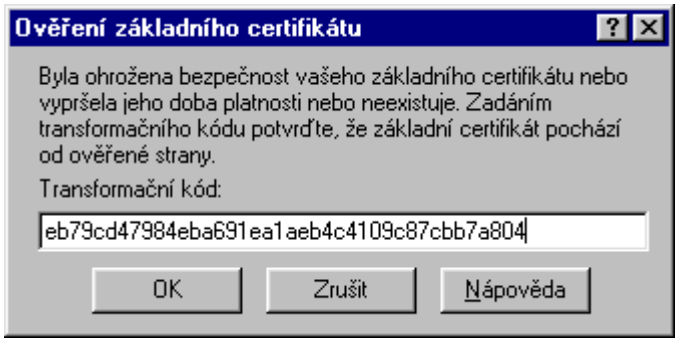
obrázek 45 – Přidání nové karty

Tím se zavede karta do peněženky, ale zatím bez certifikátu.



obrázek 46 - Peněženka účty

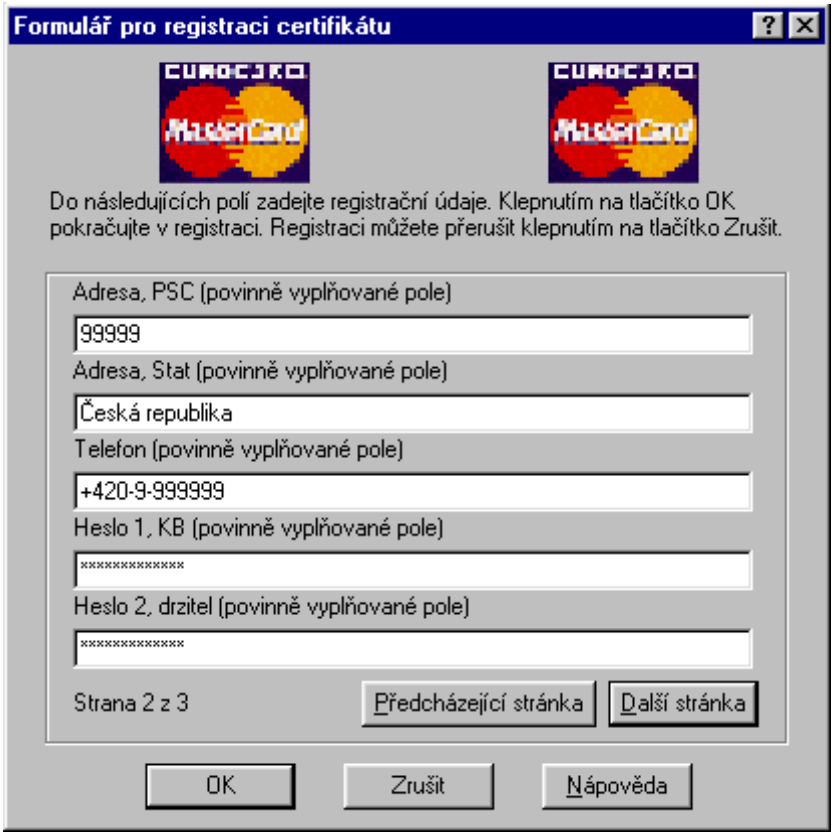
4. Klepnutím na "Získat certifikát" vyšlete certifikační autoritě žádost o zahájení certifikace. Autorita jako odpověď zašle formulář, který musíte vyplnit. Protože ve formuláři uvedete velice důležité údaje, musí mít peněženka jistotu, že komunikuje skutečně s certifikační autoritou a ne s nějakým hackerem, který se za ni jen vydává. Proto musíte vložit tzv. hash kód.



obrázek 47 - Zadání hash kódu

5. Formulář pravdivě vyplníte. Jeho součástí je i předem dohodnuté heslo, podle kterého banka pozná, že o certifikát žádá správný člověk a ne někdo jiný.

obrázek 48 - Registrace certifikátu – krok č. 1



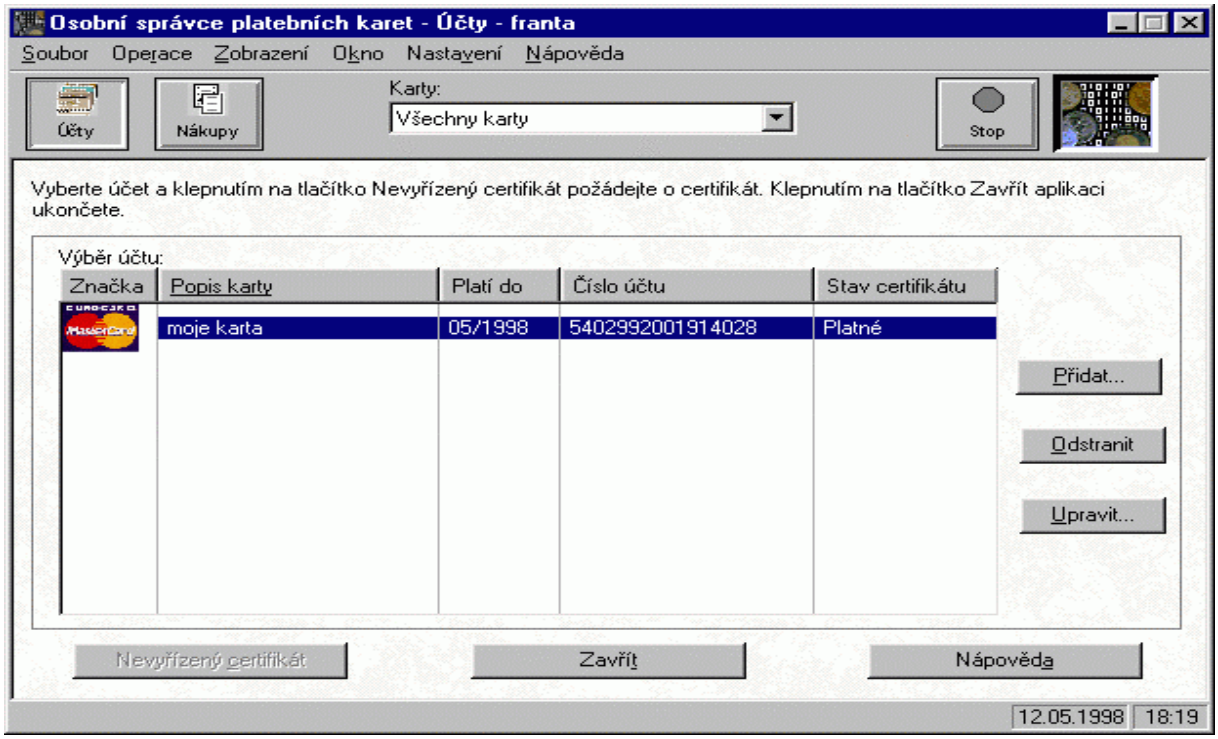
obrázek 49 - Registrace certifikátu – krok č. 2

6. Po odeslání vyplněného formuláře se peněženka zavře. V bance mezi tím ověří pravdivost údajů ve formuláři a uvolní certifikát. Pokud tuto činnost provádí člověk, bude to nějakou dobu trvat. U strojového ověření bude certifikát uvolněn ihned.

7. Po uvolnění certifikátu si jej můžete vyzvednout. Otevřete peněženku. Je nutné zadat uživatele a heslo.

obrázek 50 - Inicializace peněženky

Po vyzvednutí certifikátu je peněženka připravena k placení.



obrázek 51 - Peněženka účty

3.4 Jak získat SET jako obchodník

Obchodník, který chce přijímat platby SETem, se musí dostavit na pobočku Komerční banky a.s. (smluvním partnerem KB se může stát pouze organizace, která je k provozování činnosti registrována v ČR). Tam obchodník vyplní „Dotazník pro přijímání platebních karet prostřednictvím Komerční banky“ a předloží výpis z obchodního rejstříku nebo živnostenský list, případně jiný doklad opravňující k podnikání podle zvláštních předpisů. Před vyhotovením smlouvy Komerční banka ověří, zda je obchodník technicky připraven k zúčtování. Banka zároveň zhodnotí webovské stránky obchodníka, zda jsou vedeny formou zaručující důvěryhodnost obchodu (doporučení Asociace pro elektronickou komerci). Obchodník uzavře s Komerční bankou smlouvu, obdrží pokyny a specifikaci parametrů pro virtuální platební terminál. Poté si obchodník vygeneruje v certifikační autoritě jedinečný certifikát.

Obchodník si sám vybere a pořídí virtuální platební terminál, který musí být schválen organizací SETCo (označen příslušným logem a textem). Technickou implementaci virtuálního platebního terminálu do prostředí vlastního elektronického obchodu si zajišťuje obchodník samostatně.

4. Návrh experimentálního systému

4.1 Požadavky na platební systém

Elektronický platební systém by měl splňovat tyto funkce:

- Bezpečnost
  - Bezpečná komunikace mezi subjekty
  - Ověření protistrany
  - Prokazatelnost původu zpráv
  - Integrita dat

- Přístupnost
  - 24 hodin denně
  - Z jakéhokoliv počítače připojeného k Internetu
  - Pro jakéhokoliv zákazníka, obchodníka či banku
  - Žádné speciální hardwarové nároky (speciální čtecí a ověřovací zařízení)
  - Použití systému není vázáno na platební kartu, ale na číslo účtu v bance

- Použitelnost
  - Nákup a prodej
  - Převody peněz z účtu na účet

Platební systém musí obsahovat kompletní sadu protokolů pro jednotlivé peněžní transakce. Součástí systému by mělo být i ošetření některých dalších jevů, ke kterým může docházet. Těmito jevy míním např. různé snahy o oklamání systému, apod..

Při konstrukci jednotlivých protokolů jsou vznášeny různé požadavky, které je možno obecně rozdělit na obchodní (marketingové) a technické. Přičemž samozřejmě obojí spolu úzce souvisí.

Jestliže chci provozovat nějaký platební systém, tak mě kromě samotných protokolů musí zajímat mnohem větší okruh otázek. Tyto otázky se týkají např. přenosového média, které chci používat ke komunikaci, hardwarového vybavení (počítače, modemy a další) a jejich předpokládaného zatížení, ale třeba také ceny za napojení jednoho zákazníka a obchodníka, množství potenciálních uživatelů, vlastnosti použitelné pro propagaci, atd.

4.1.1 Obchodní požadavky

Jedním ze základních požadavků je to, aby byl systém akceptovatelný pro trh. Trhem zde myslím obchodníky a uživatele (zákazníky).

Při vzniku protokolu SET byly vzneseny tyto požadavky:

- dosáhnutí celkové přijatelnosti snadnou realizovatelností a co nejmenším vlivem na obchodníky a koncové uživatele .

- umožnit modulovou implementaci platebního protokolu do existujících zákaznických aplikací
- minimalizovat změny ve vztazích zákazníci - poskytovatelé a nabyvatelé - obchodník
- požadovat co nejmenší vliv na existující aplikace a infrastrukturu obchodníků, banky a platebního systému
- poskytovat efektivní protokol z pohledu finanční instituce

Původ většiny požadavků je zřejmý a vychází z předpokladu (do značné míry oprávněného), že pokud chcete po lidech, aby se naučili používat něco nového a zároveň do toho měli sami investovat, tak se velkého vděku nedočkáte.

Druhým z cílů uvedených požadavků je jediné - přesvědčit zákazníky (uživatele a obchodníky), že novou věc prostě potřebují a hlavně, že na tom vydělají. Jestliže se toto nepodaří, tak ani sebelépe technicky navržený platební systém v konkurenci neuspěje.

Máme dva základní požadavky, které jdou do jisté míry proti sobě. Je otázkou, na který z nich dáme větší důraz.

4.1.2 Technické požadavky

Technické požadavky směřují k zajištění funkčnosti a bezpečnosti platebního systému. Hlavní požadavky na platební protokoly by mohly znít takto:

- poskytovat důvěrnost platebních informací a zajistit důvěrnost informací z objednávek
- zajistit integritu všech přenášených dat
- poskytovat autentizaci uživatele (držitele karty), jak ve vztahu k bance (vlastnictví účtu), tak ve vztahu k obchodníkovi (peníze jsou v pořádku)
- umožnit autentizaci obchodníka ve vztahu k uživateli (prodávám zboží, které nabízím), aby mohl přijímat elektronické peníze
- dostatečné použití bezpečnostních postupů a technik při návrhu systému k ochraně všech legitimních účastníků platebního protokolu
- zajistit, aby byl protokol nezávislý na bezpečnosti přenosových mechanismů
- při pokusu o obelstění systému je možné jednoznačně určit viníka a na základě této identifikace ho příslušným způsobem postihnout

Tyto požadavky jsou zajištěny implementací čtyř základních principů. Všechny tyto principy jsou v navrženém systému použity. Jmenovitě jsou to:

- **důvěrnost** - označuje vlastnost zprávy, kdy její obsah je znám pouze odesílateli a zjistit ho může pouze příjemce. Jakákoliv jiná strana, která zprávu získá není schopna obsah v rozumné době zjistit

- **integrita** - zajištění integrity označuje stav, kdy obsah zprávy je při příjmu shodný s obsahem odeslaným. Porušení integrity musí být rozpoznatelné.
- **autentizace** - je proces, kdy jedna strana dokazuje svou totožnost druhé straně. To platí jak o osobě, tak například o instituci, nebo počítači.
- **neodmítnutelnost odpovědnosti** - úzce souvisí s autentizací, zajišťuje, že se nemohu zbavit odpovědnosti za akce, jichž jsem původcem.

4.1.2.1 Důvěrnost informací

Pro usnadnění a podporu elektronického obchodu je nutné ujistit uživatele, že citlivé informace, které používají při činnosti v rámci platebního systému jsou bezpečně uloženy a přístupné pouze tomu, komu jsou určeny. Proto musí být informace o platbách, objednávaném zboží, čísla účtů uživatelů zajištěny nejen při přenosu, ale i při archivaci. V opačném případě by samozřejmě mohlo dojít ke zneužití těchto citlivých informací neautorizovanou stranou. V současné době, kdy drtivá většina informací je přenášena přes otevřené sítě bez jakéhokoliv zabezpečení, je nutné používání kryptografie. Příkladem může být např. placení zadáním čísla kreditní karty. Je jen otázkou času, kdy se tyto důvěrné informace pokusí někdo zneužít.

S pomocí počítačů je možno nadělat mnohem větší škody v mnohem kratší době. Jestliže se tato činnost zautomatizuje vytvořením speciálních programů, tak výsledná škoda bude nesrovnatelná s klasickými podvody bez použití výpočetní techniky.

4.1.2.2 Integrita dat

Specifikace musí zajistit zachování obsahu zpráv při přenosu mezi jednotlivými stranami protokolu, a případnou detekci neautorizovaných změn. Je jasné, že ve chvíli kdy tato vlastnost nebude zajištěna, je otevřena brána pro různá individua, která poté mohou s malou námahou páchat vysoké škody.

Jestliže se změní některá z položek objednávky, osobní data, nebo platební instrukce (a nejen úmyslně, ale i chybou při přenosu), tak to může vést k chybám, nebo (a to je mnohem pravděpodobnější) k podvodům. Proto je nutné použít mechanismy, které zajistí, že obsah přenesené zprávy je přesný a že nedošlo k jeho změně. Jestliže bude zjištěn opak, musí být zpráva odmítnuta a případně vyžádat opakování zaslání zprávy.

4.1.2.3 Autentizace

Třetí princip v pořadí. Při použití algoritmu RSA má každý účastník systému dva klíče: veřejný a soukromý. Soukromý používá on sám a nikomu ho nesděluje. Veřejný klíč je naopak rozšiřován mezi

všemi, kteří chtějí s tímto účastníkem komunikovat.V této fázi je nutno zajistit, že veřejný klíč účastníka XY skutečně patří účastníku XY a ne někomu, kdo se za něj vydává. Pro splnění tohoto požadavku se používají jiné mechanismy, jež budou popsány dále. Teprve takto zajištěný klíč už může sloužit k autorizaci tohoto účastníka kdykoliv dále.

4.1.2.4 Neodmítnutelnost odpovědnosti

Princip neodmítnutelnosti odpovědnosti slouží k jednoznačnému určení totožnosti původce ať už nějaké zprávy, nebo činnosti. Zásadní odlišnost od autentizace je v tom, že určení totožnosti původce se v tomto případě provádí až po uskutečnění sledované činnosti. Nemohu tedy zabránit provedení nežádoucích akcí, mohu pouze následně určit jejich původce.

V platebním protokolu je tento princip nutný k tomu, aby bylo možné zjistit a následně postihovat účastníky systému, kteří se nechovají podle pravidel.

4.2 Teoretické řešení

4.2.1 Bezpečnostní požadavky

Autentizace spočívá v ověření totožnosti protistrany. Zákazník zadá svoje iniciály (jméno, příjmení, rodné číslo, atd..) a heslo. Z bezpečnostních důvodů není dobré posílat tyto privátní údaje přes veřejnou síť jakou Internet je. A proto se z těchto údajů vypočte hashovacím algoritmem kód, který je posílán přes Internet k protistraně. Hashovací algoritmus je samozřejmě jednocestná funkce, takže z výsledného kódu nelze zpětně určit vstupní data.

Pro zabezpečení přenášených dat je použita metoda šifrování a digitálního podpisu. Je použita kombinace symetrického a asymetrického šifrování.

4.2.1.1 Vstupní hashovací algoritmus

Jako vstupní hashovací algoritmus je použit Secure Hash Algorithm (SHA). Výstupem tohoto algoritmu je 160-ti bitový digest.

4.2.1.2 Symetrické kódování

Pro symetrické kódování je použit algoritmus TRIPLE DES (3DES) s délkou symetrického klíče 192 bitů. Tento klíč je vždy náhodně generovaný. Při aktivaci spojení mezi dvěma subjekty se vygeneruje pokaždé jiný náhodný klíč.

4.2.1.3 Asymetrické kódování

Pro asymetrické kódování je použita metoda RSA, tj. metoda privátního a veřejného klíče. Délka klíče je 512 bitů. Metoda RSA spočívá v tom, že co se zakóduje pomocí veřejného klíče, to se musí dekódovat pomocí privátního a veřejného klíče.

Pozn.: Možné modifikování vzhledem k bezpečnosti:
Délka klíče může být až 2048 bitů. Na počátku spojení, mezi dvěma subjekty, mohou být privátní a veřejné klíče nově vygenerovány a tím by se značně zvýšila bezpečnost platebního systému.

4.2.1.4 Digitální podpis

Digitální podpis je výstupní kód z hashovacího algoritmu, který je zakódován veřejným klíčem protější strany. Zde je, jako hashovací algoritmus, použit standardní Message Digest 5 (MD5).

4.3 Programové řešení

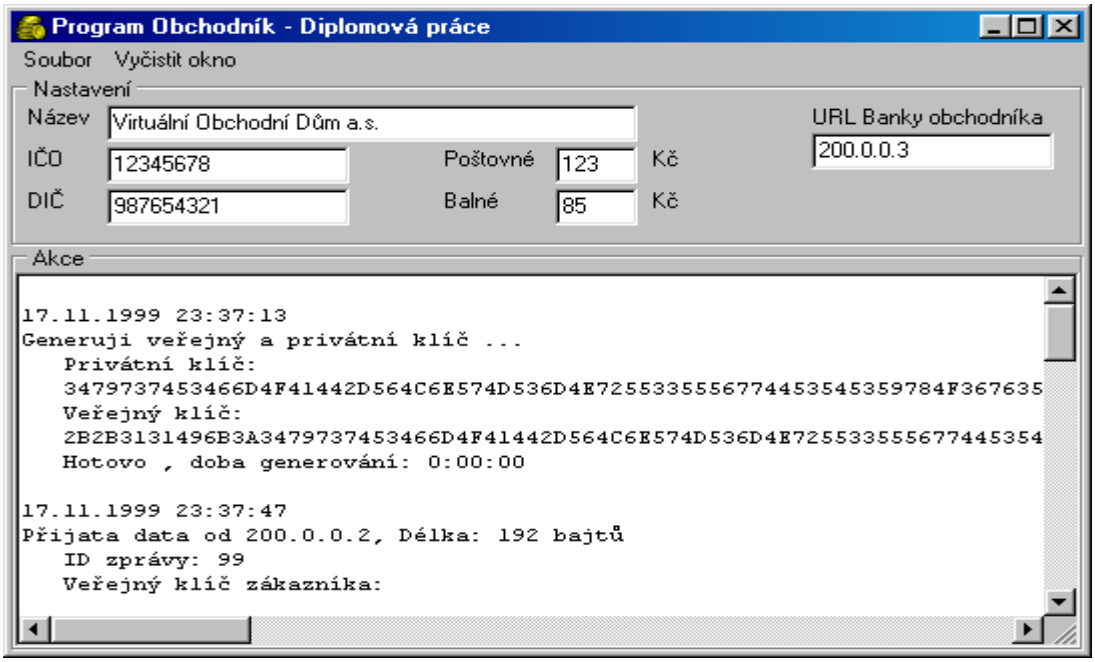
Platební systém jsem naprogramoval v DELPHI 4.0 pro Windows 95/98. Skládá se ze čtyř samostatných programů – Peněženka, Obchodník, Banka a CGI. Každý z těchto programů je samostatně spustitelný na jakémkoli počítači s operačním systémem Windows 95 nebo vyšší a samozřejmě připojených na Internet.

Pro symetrické kódování a hashovací algoritmy jsem použil komponenty TCipherManager a THashManager. Pro asymetrické kódování jsem použil komponentu TRSA.

4.3.1.1 Peněženka

Program je navržen tak, aby byl přístupný pro jakéhokoliv uživatele, tzn. může být nainstalován na veřejně přístupných počítačích. Na počítač, kde je tato peněženka nainstalována, se neukládají žádné privátní údaje o uživatelích, takže nemůže dojít k jejich zneužití. Funkci peněženky by mohl obstarávat i web server banky, ale z hlediska větší bezpečnosti a rychlosti zpracování je lepší mít program na lokálním disku. Program má dvě funkce. První je, že peněženka je použita k vyvolání platební transakce (program je spuštěn automaticky WWW prohlížečem) a druhá, že peněženka si vyžádá od banky zákazníka výpis všech provedených plateb (program si spustí uživatel sám z příkazové řádky).

4.3.1.2 Obchodník

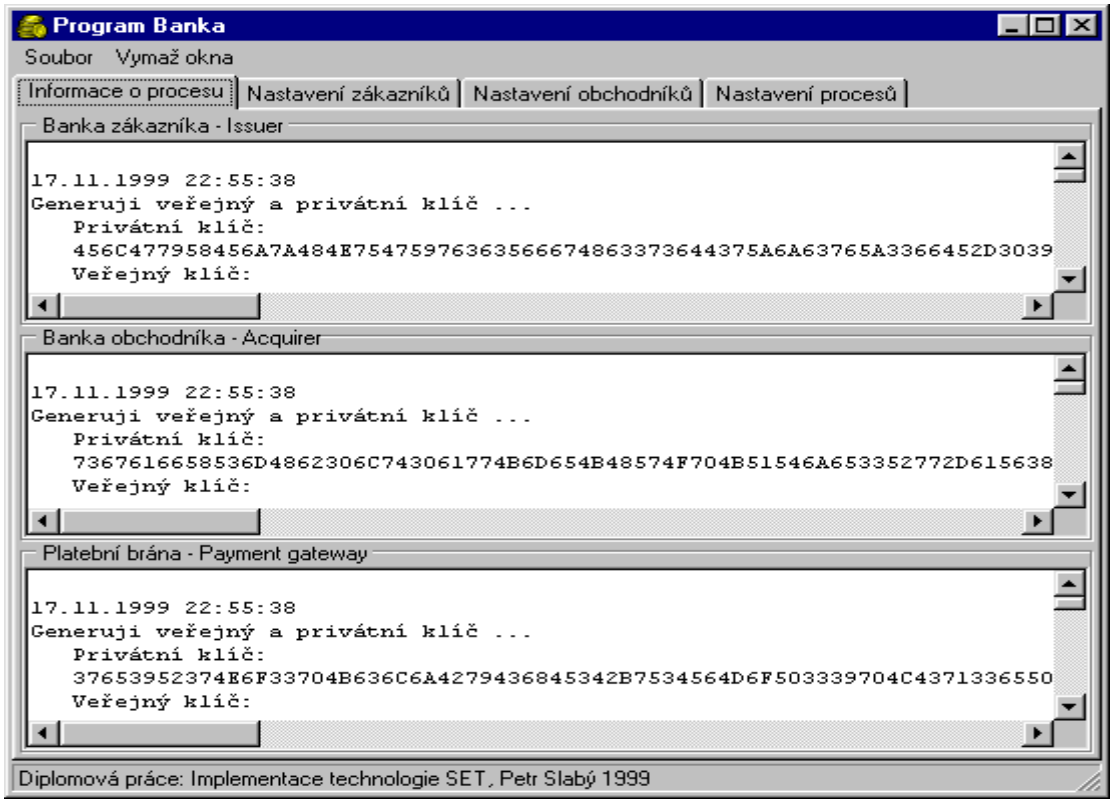


obrázek 52 - Program Obchodník

Je to program, který vlastně spolu s programem CGI zajišťuje zázemí obchodníka.

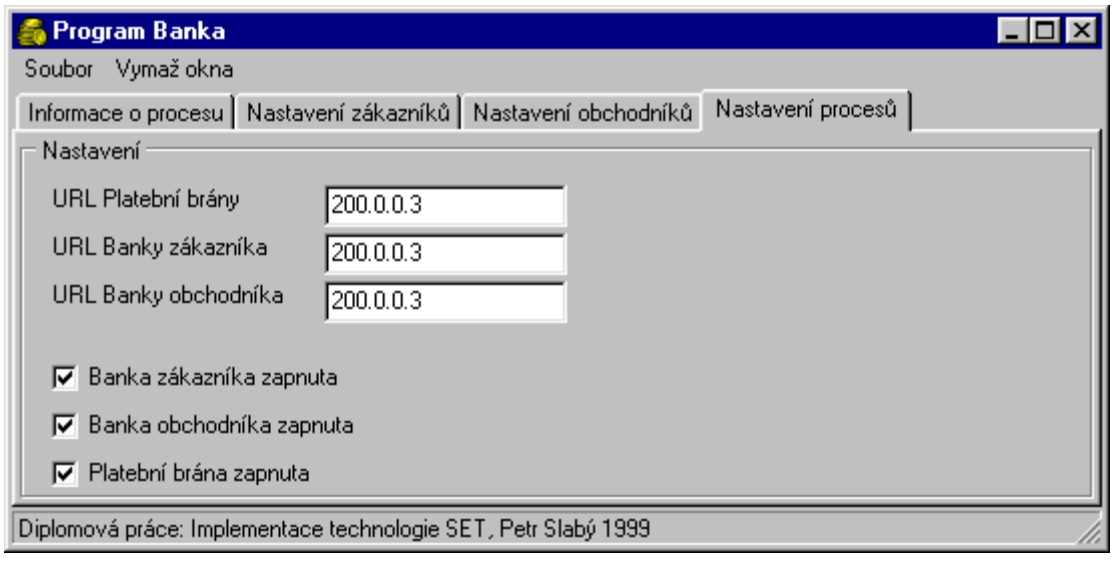
4.3.1.3 Banka

Tento program je složen ze tří částí – Banka zákazníka, Banka obchodníka a Platební brána.



obrázek 53 - Program Banka

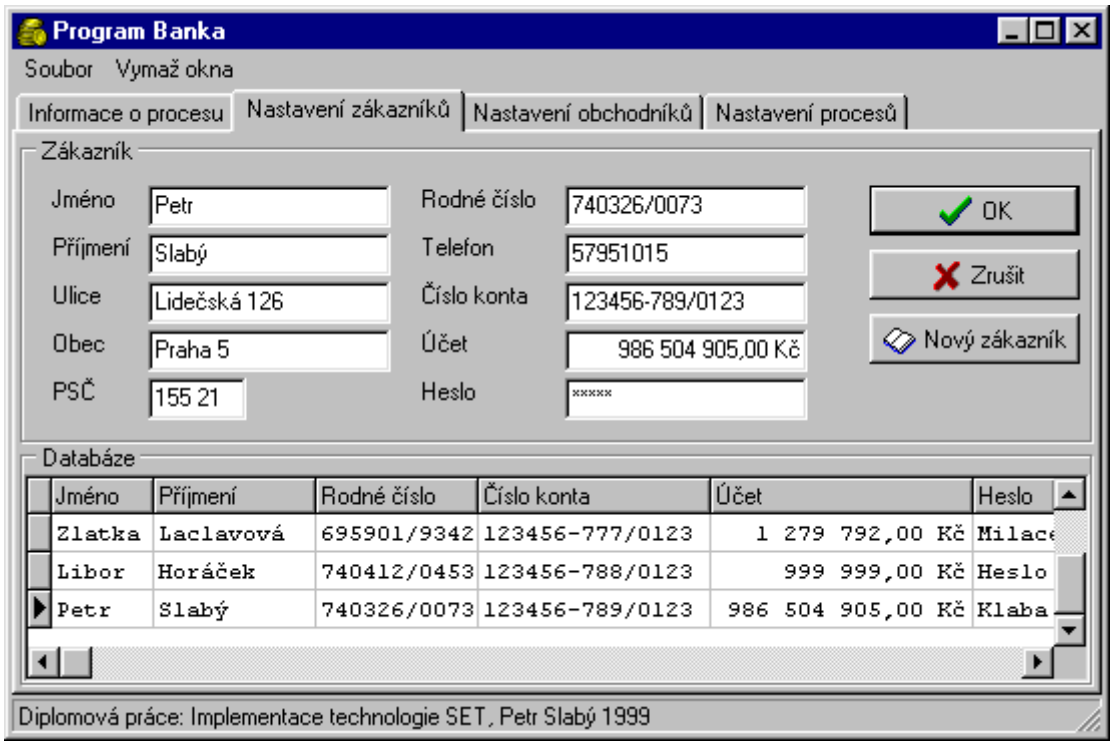
Pro správnou funkci tohoto systému musí být spuštěny všechny tři části. Každá z těchto částí se dá vypnout, ale je nutné tento program



obrázek 54 - Program Banka - nastavení procesů

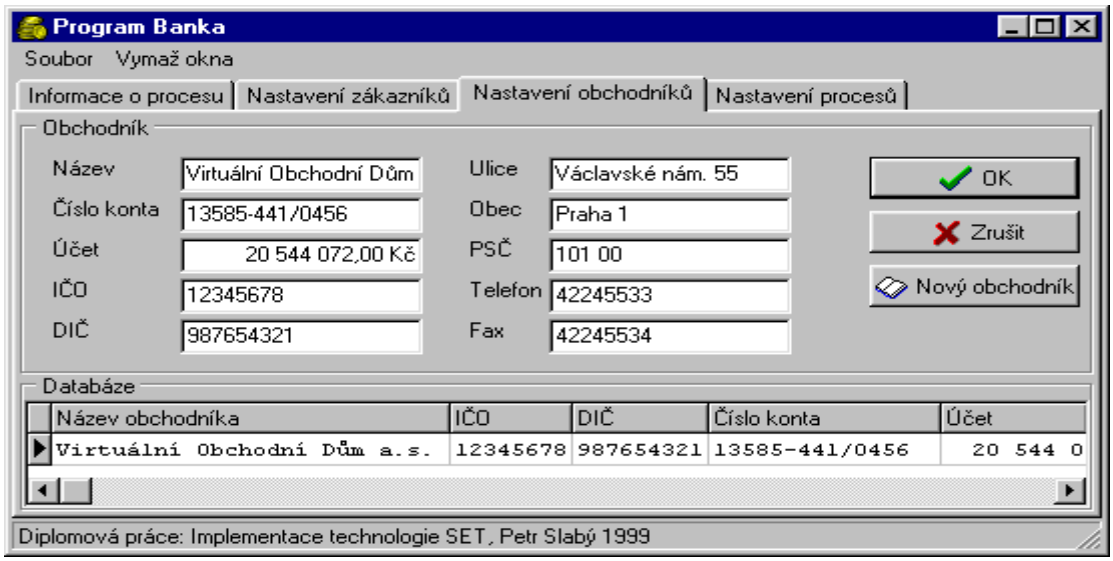
spustit na jiném počítači. Poté je ale zapotřebí správně nakonfigurovat URL adresy všech subjektů.

Banka zákazníka reprezentuje banku, kde má každý zákazník svůj účet. V bance se zadávají noví zákazníci. Dále se mohou editovat nebo rušit. Banka ověřuje solventnost zákazníků a zaznamenává všechny jejich platební transakce.



obrázek 55 - Program Banka - nastavení zákazníků

Banka obchodníka reprezentuje banku, kde má každý obchodník svůj účet. V bance se zadávají nebo mažou noví obchodníci. Banka zaznamenává všechny platební transakce obchodníků.



obrázek 56 - Program Banka - nastavení obchodníků

Platební brána je program, který dává příkazy bance zákazníka a bance obchodníka k převodu peněz z účtu zákazníka na účet obchodníka.

4.3.1.4 CGI

Tento program generuje WWW stránky Virtuálního Obchodního Domu a posílá MIME zprávu s objednaným zbožím internetovému prohlížeči, který po přijetí této zprávy zaktivuje peněženku.

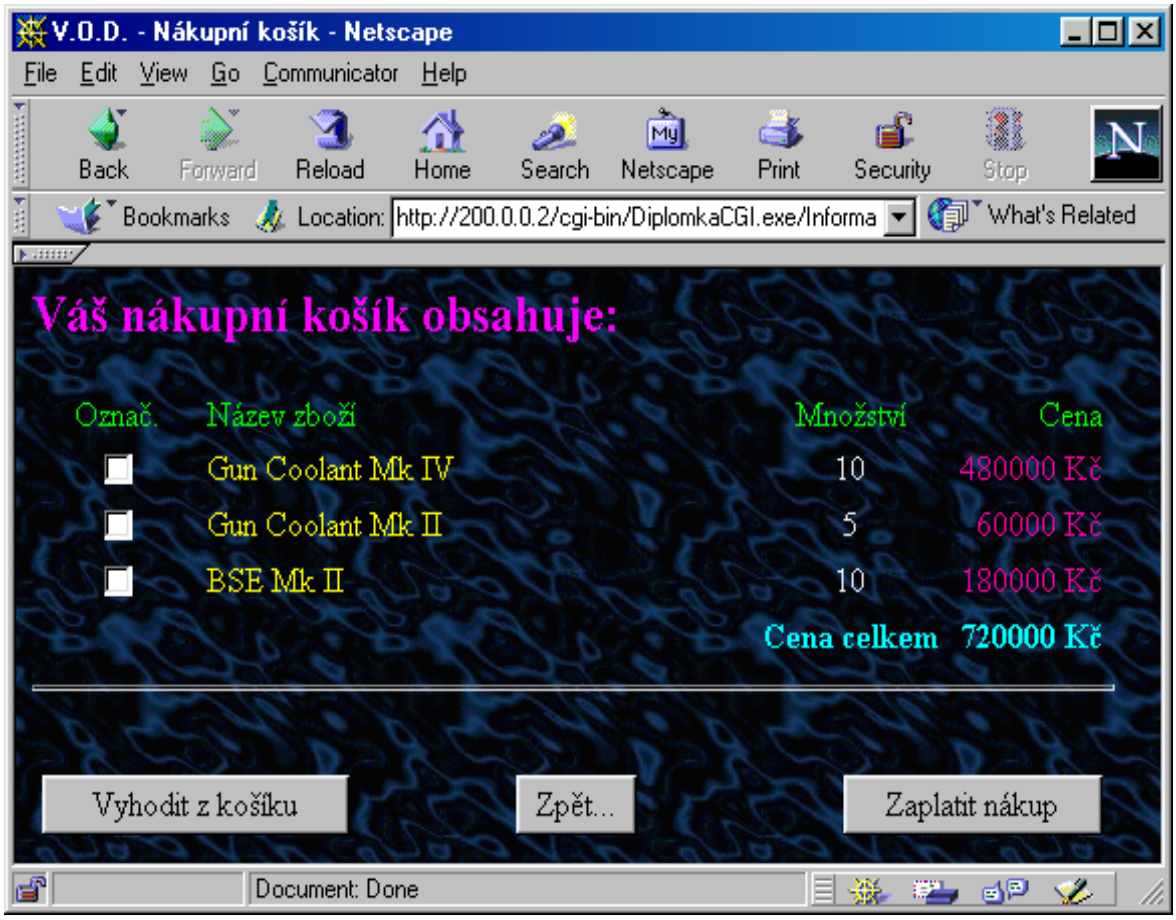
MIME zpráva zaslaná ze serveru obchodníka WWW prohlížeči zákazníka, který po jejím přijetí aktivuje elektronickou peněženku a ta ji zpracuje:

```
Mime version: 1.0
Content-Type: text/plain
Content-Length: 0
Content-Transfer-Encoding: binary
SET-Initiation-Type: Payment
SET-Version: 0.0
SET-SET-URL: http://200.0.0.2/cgi-bin/DiplomkaCGI.exe/PlatitSETem
SET-Success-URL: http://200.0.0.2/cgi-bin/DiplomkaCGI.exe/Uspech
SET-Failure-URL: http://200.0.0.2/cgi-bin/DiplomkaCGI.exe/Chyba

Gun Coolant Mk IV;10;480000
Gun Coolant Mk II;5;60000
BSE Mk II;10;180000
```

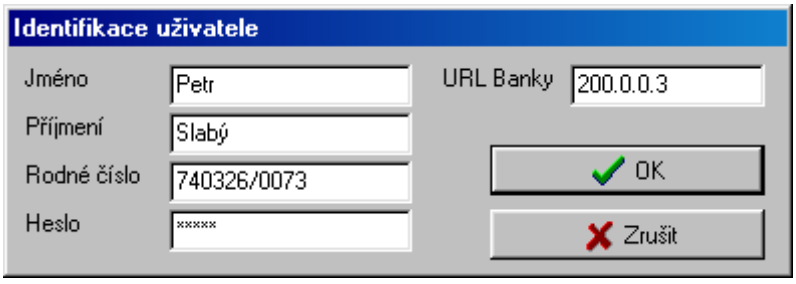
4.4 Popis funkce a toku dat

4.4.1 Popis funkce



obrázek 57 - V.O.D. - nákupní košík

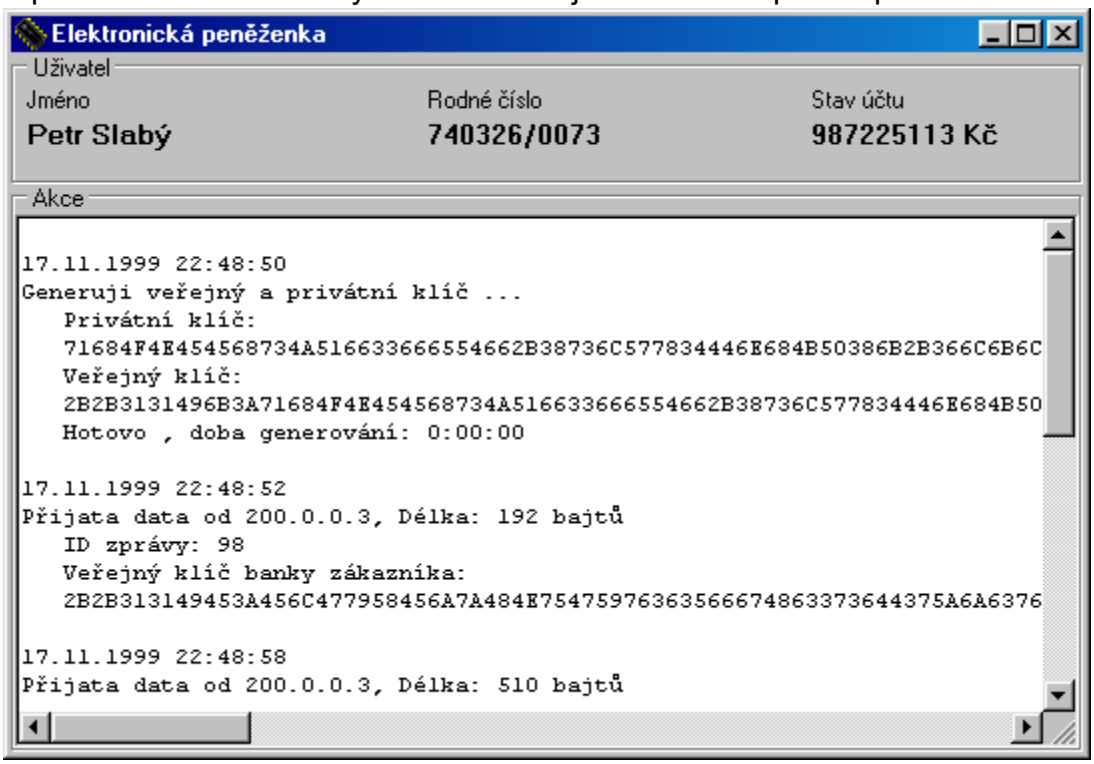
Po klepnutí na tlačítko „Zaplatit“ se zaktivuje Peněženka. Nejprve je nutné zadat jméno, příjmení, rodné číslo a heslo. Do políčka URL banky se musí zadat URL adresa banky zákazníka.



obrázek 58 - Inicializace peněženky

Po klepnutí na tlačítko OK se spustí vlastní platební transakce. Z uvedených údajů se vypočte hashovací kód, který je později použit pro identifikaci zákazníka. Vymění si s bankou zákazníka veřejné klíče a pošle

bance symetrický klíč. Poté u banky zákazníka zjistí zůstatek na účtu daného zákazníka a URL platební brány. Dále zjistí z objednaného zboží celkovou cenu a porovná jí se zůstatkem na účtu. Je-li dostatečný zůstatek na účtu, tak se pokračuje dále, jinak se transakce přeruší. Spojí se s platební bránou a vymění si veřejné klíče a pošle platební bráně



obrázek 59 - Peněženka

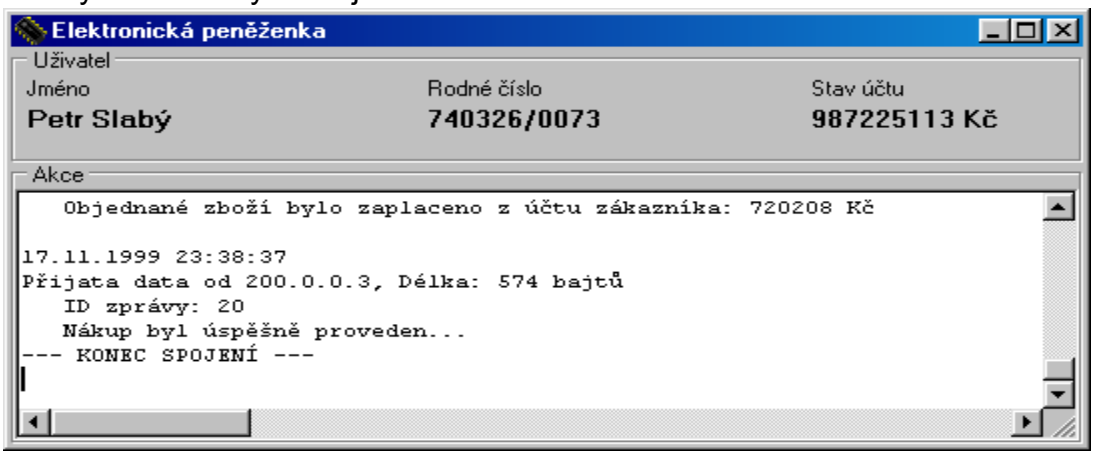
symetrický klíč. Dále se spojí s obchodníkem a také si vymění veřejné klíče a pošle obchodníkovi symetrický klíč. Poté vygeneruje dvojitou zprávu. Jedna část je zakódována veřejným klíčem platební brány a druhá část veřejným klíčem obchodníka. V první části je hashovací kód zákazníka a v druhé části je objednané zboží od obchodníka.

Obchodník dvojitou zprávu přijme dekóduje svojí část, určí celkovou cenu objednávky a objednané zboží. Vymění si s bankou obchodníka veřejné klíče a pošle bance symetrický klíč. Od banky obchodníka zjistí URL platební brány. Vymění si s platební bránou veřejné klíče a pošle jí symetrický klíč. Vloží do dvojité zprávy svůj hashovací kód zakódovaný veřejným klíčem platební brány. Pošle platební bráně dvojitou zprávu a poté ještě celkovou cenu objednaného zboží.

Platební brána přijme dvojitou zprávu a dekóduje obě části zprávy a tak dostane identifikační kódy zákazníka a obchodníka. S bankou zákazníka si vymění veřejné klíče a pošle bance zákazníka symetrický klíč. Dále pošle bance identifikační kód zákazníka a obratem dostane číslo účtu zákazníka. Poté pošle bance zákazníka částku k převedení z účtu zákazníka na účet obchodníka. S bankou obchodníka si vymění veřejné klíče a pošle bance obchodníka symetrický klíč. Poté pošle bance obchodníka identifikační kód obchodníka a obratem dostane číslo účtu obchodníka. Dále pošle bance obchodníka částku, kterou má připsat na konto obchodníka. Bance zákazníka pošle číslo účtu obchodníka.Jestliže nedošlo k žádné chybě

během přenosů zpráv a jejich zpracování, tak platební brána všem účastníkům transakce rozešle zprávu o úspěšném ukončení transakce.

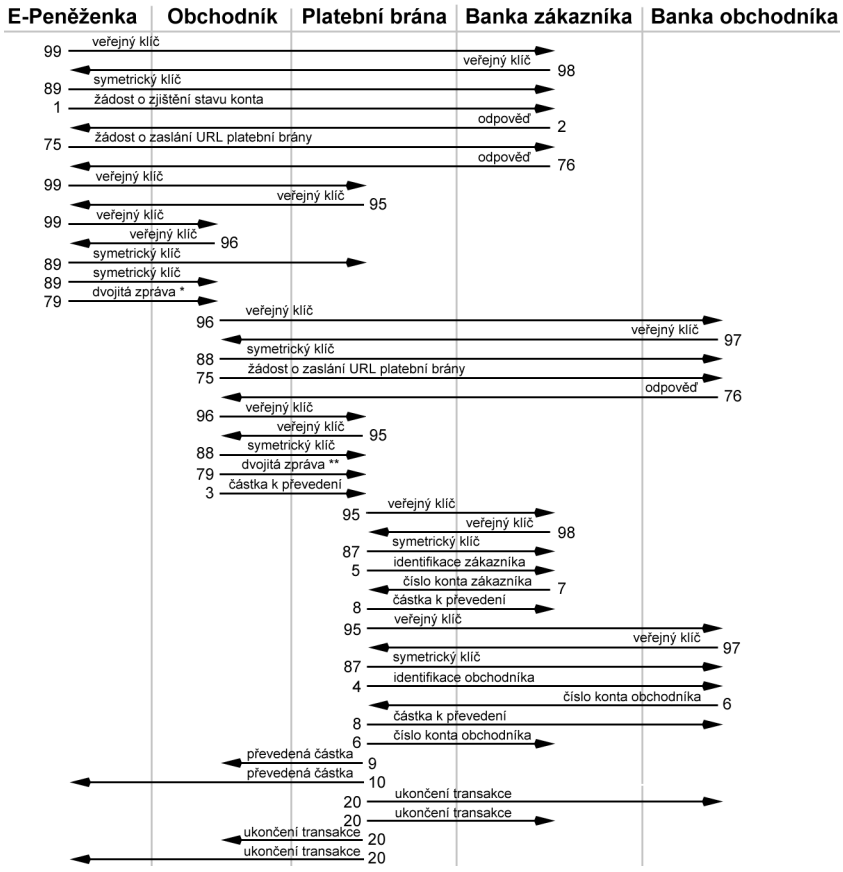
Jestliže ale během zpracování došlo k nějaké chybě, tak subjekt u kterého došlo k chybě, rozešle zprávu s chybovým hlášením všem do té doby zúčastněným subjektům a transakce se ukončí.



obrázek 60 - Peněženka - ukončení transakce

4.4.2 Tok dat

Na následujícím obrázku je zobrazen tok dat při platbě v platebním systému.



obrázek 61 - Tok dat při platbě

Šipka znázorňuje směr toku dat. Na začátku každé šipky je číslo, které je identifikačním číslem zprávy. Nad šipkou je vždy informace o datech.

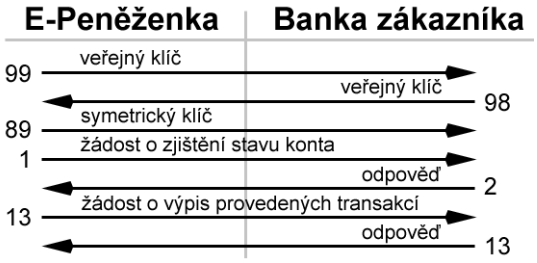
V následující tabulce je seznam všech identifikačních čísel zpráv. ID označuje číslo zprávy, odpověď A resp. N značí, že zpráva vyžaduje resp. nevyžaduje odpověď.

ID	*Odpověď*	*Obsah zprávy*	*Vysvětlení*
1	A	Hash kód zákazníka	Žádost o zjištění stavu účtu
2	N	Stav účtu	Odpověď se zprávou o stavu účtu
3	N	Částka	Částka k převedení na účet
4	A	Hash kód obchodníka	Žádost o identifikaci obchodníka
5	A	Hash kód zákazníka	Žádost o identifikaci zákazníka
6	N	Číslo konta obchodníka	Odpověď na žádost o identifikaci obchodníka
7	N	Číslo konta zákazníka	Odpověď na žádost o identifikaci zákazníka
8	N	Částka	Žádost o uskutečnění převodu
9	N	Částka	Informace o uskutečněném převodu (pro obchodníka)
10	N	Částka	Informace o uskutečněném převodu (pro zákazníka)
13	A	Hash kód zákazníka Výpis plateb	Výpis provedených plateb ***
20	N		Úspěšný konec transakce
21	N	Chybové hlášení	Chyba od zákazníka
22	N	Chybové hlášení	Chyba od obchodníka
23	N	Chybové hlášení	Chyba od banky zákazníka
24	N	Chybové hlášení	Chyba od banky obchodníka
25	N	Chybové hlášení	Chyba od platební brány
75	A		Žádost o URL platební brány
76	N	URL platební brány	Odpověď na žádost o URL platební brány
79	N	2 části: hash kód zákazníka a hash kód obchodníka	Dvojitá zpráva
87	N	Symetrický klíč	Symetrický klíč zákazníka
88	N	Symetrický klíč	Symetrický klíč obchodníka
89	N	Symetrický klíč	Symetrický klíč platební brány
95	A	Veřejný klíč	Veřejný klíč platební brány
96	A	Veřejný klíč	Veřejný klíč obchodníka
97	A	Veřejný klíč	Veřejný klíč banky obchodníka
98	A	Veřejný klíč	Veřejný klíč banky zákazníka
99	A	Veřejný klíč	Veřejný klíč zákazníka

tabulka 2 - Přehled posílaných zpráv

Pozn.:
** - Dvojitá zpráva obsahuje v první části hash kód zákazníka a v druhé soupis objednávaného zboží.*
*** - Dvojitá zpráva obsahuje v první části hash kód zákazníka a v druhé části hash kód obchodníka.*
**** - Při výpisu provedených plateb se ve zprávě žádosti posílá hash kód zákazníka a obratem se dostává zpráva ve které je seznam provedených plateb.*

Na následujícím obrázku je zobrazen tok dat při výpisu plateb.



obrázek 62 - Tok dat při výpisu transakcí

4.4.3 Formáty zpráv

Každá zpráva má tuto strukturu:

- ID zprávy – hexadecimální číslo (2 bajty)
- Délka zprávy – hexadecimální číslo (4 bajty)
- Zpráva – řetězec hexadecimálních čísel (proměnná délka)

4.4.3.1 Veřejný klíč

Při odeslání se veřejný klíč převede na řetězec dvojic znaků, přičemž každá dvojice znaků odpovídá hexadecimálnímu číslu jednoho ASCII znaku veřejného klíče. Tzn., že se posílá zpráva s dvojnásobnou délkou než je délka samotného veřejného klíče. Po tomto převodu se přidá hlavička zprávy, tj. ID zprávy a délka zprávy.

Po přijmutí zprávy s takto převedeným veřejným klíčem se musí odpovídajícím způsobem veřejný klíč rekonstruovat.

4.4.3.2 Symetrický klíč

Před odesláním symetrického klíče se symetrický klíč zakóduje pomocí veřejného klíče příjemce a převede se na hexadecimální formát. Poté se přidá hlavička zprávy a zpráva se odešle.

Po přijmutí zprávy se zakódovaným symetrickým klíčem se zpráva převede z hexadecimálního formátu na ASCII formát a dekóduje se pomocí privátního a veřejného klíče příjemce.

4.4.3.3 Jednoduchá zpráva

Nejdříve se vypočte message digest (MD5) ze zprávy a poté se tento digest zakóduje veřejným klíčem příjemce. Tímto je vytvořen digitální podpis. Vytvoří se obálka, která obsahuje délku zprávy (4 bajty), samotnou zprávu, délku digitálního podpisu (4 bajty) a digitální podpis. Tato obálka se poté zakóduje symetrickým klíčem (metoda Triple DES) a převede se na hexadecimální formát. Nakonec se připojí hlavička a zpráva se odešle.

Po přijmutí zakódované zprávy se obálka převede z hexadecimálního formátu na ASCII a dekóduje se symetrickým klíčem. Z obálky se vyjme zpráva a digitální podpis, který se následně převede na ASCII formát. Digitální podpis se dekóduje pomocí privátního a veřejného klíče příjemce. Ze zprávy se vypočte nový message digest a porovná se s dekódovaným message digestem ze zprávy. Jestliže si tyto hodnoty odpovídají, pak je vše v pořádku. Jestliže si ale neodpovídají, pak je zpráva nahrazena zprávou s chybovým hlášením.

4.4.3.4 Dvojitá zpráva

Vytvoření dvojité zprávy je analogické jako vytvoření jednoduché zprávy, ale s tím rozdílem, že odesílaná zpráva je složená ze dvou jednoduchých zpráv.

Dekódování dvojité zprávy je trochu složitější, protože se nedekódují obě zprávy najednou, ale pouze jedna a druhá se pouze oddělí od první. Dekódování první zprávy je analogické jako dekódování jednoduché zprávy. Druhá zpráva se musí dekódovat zvlášť, protože se musí zajistit to, aby některý příjemce mohl dekódovat pouze jednu zprávu a některý mohl dekódovat obě zprávy. Na dekódování druhé zprávy je použita funkce k dekódování jednoduché zprávy.

5. Porovnání s jinými platebními systémy

Elektronické platební systémy v současnosti používané na Internetu, zejm. v prostředí WWW, jsou v základě elektronickými ekvivalenty tradičních forem plateb. Patří mezi ně elektronické šeky, elektronická hotovost a elektronické kreditní karty. Výjimku tvoří tzv. mikroplatby.

Na vývoji těchto systémů se stejnou měrou podílejí university, výzkumná pracoviště, komerční organizace i bankovní sektor. Zdá se však, že šanci na globální uplatnění mají především systémy zaváděné renomovanými finančními institucemi, které již v reálném světě disponují důvěrou veřejnosti.

5.1 Mikroplatby

Velmi ojedinělým způsobem provádění plateb prostřednictvím Internetu, je tzv. systém mikroplateb. Jako jediný z již představených platebních metod nemá ekvivalent mezi konvenčními platebními prostředky a je specifickou formou platby právě v prostředí veřejných sítí.

V reálném světě je nejvhodnější formou pro krytí transakcí s velmi nízkou hodnotou hotovostní platba. Provedení jakékoli platby hotovostí je ale na spodní hranici omezeno hodnotou mince s nejnižší nominální hodnotou. Jakákoli transakce nesmí klesnout pod tuto spodní mez. V případech, kdy by jednotlivé transakce nedosáhly této výše, se používá předplatné, jehož podstatnou nevýhodou je omezení přístupu ke službám těm zákazníkům, kteří mají zájem využívat poskytované služby jen příležitostně či se nejdříve přesvědčit o jejich kvalitě. Právě v prostředí veřejně přístupných sítí se nabízí rozsáhlá škála služeb, jejichž provozování je závislé na překonání těchto bariér.

Mikroplatební systémy umožňují efektivní transfer velmi malých obnosů v rámci jediné transakce. Z toho vyplývají i nároky na tyto systémy. Zaprvé je nutné udržet náklady na komunikaci mezi zúčastněnými stranami na absolutním minimu. Server musí být schopen provádět velmi vysoké množství transakcí. Úspěšný mikroplatební systém z tohoto důvodu nesmí operovat s kryptografickými technikami náročnými na počítačové zpracování. Systémy používané pro provádění plateb prostřednictvím elektronických šeků, kreditních karet či elektronické hotovosti vyžadují ověření platby ze strany prodejce před jejím samotným provedením, čímž se zvyšují režijní náklady. Vzhledem k velmi nízkým obnosům přenášeným tímto způsobem, nemají mikroplatební systémy zakomponovány žádné nebo jen velmi slabé bezpečnostní mechanismy.

Na poli mikroplatebních systémů dominují v dnešní době na trhu zejména systémy Millicent a SubScrip. Na příkladu systému Millicent lze demonstrovat základní model fungování systémů mikroplateb.

5.1.1 MILLICENT

Millicent je decentralizovaný mikroplatební systém vyvinutý firmou Digital Equipment, umožňující provádění plateb dosahujících alespoň desetiny amerického centu. Vyznačuje se efektivitou zpracování dat a maximální flexibilitou. Může být uplatněn v řadě aplikací.

Bezpečnost odpovídající potřebám mikroplatebního systému je zajištěna pomocí jednoduché digestivní funkce. Bezpečnostní protokol je

definován tak, že náklady spojené s uskutečněním podvodu jsou vyšší, než hodnota pořizovaných služeb.

obrázek 63 - Schéma systému MILLICENT

5.1.1.1 Proces provádění plateb

Spotřebitel zakoupí scrip zvoleného zprostředkovatele.

Za použití scripu zprostředkovatele, spotřebitel zakoupí scrip prodejce. (Tento krok odpadá v případě, že zákazník již platný scrip prodejce vlastní.) Hodnota scripu prodejce nesmí překročit hodnotu zprostředkovatelského scripu ve vlastnictví spotřebitele.

Zprostředkovatel zašle spotřebiteli scrip prodejce a nový zprostředkovatelský scrip v hodnotě zůstatku na účtu zákazníka.(Tento krok odpadá v případě, že zákazník již platný scrip prodejce vlastní.)

Spotřebitel zašle prodejci spolu s objednávkou zboží/služeb prodejní scrip (scrip daného prodejce).

Prodejce provede kontrolu duplikace prodejního scripu. Poté zašle zákazníkovi objednanou zakázku a nový prodejní scrip v hodnotě odpovídající zůstatku.

5.1.1.2 Bezpečnost

Systém Millicent existuje ve třech variantách protokolů, v jejichž rámci je k základnímu modelu přičleněna bezpečnostní nadstavba odpovídající různým požadavkům na bezpečnost komunikace mezi zúčastněnými stranami (a zohledňující odlišnou míru bezpečnosti různých sítí.)

1. Prostý scrip

Je nejjednodušším protokolem systému Millicent. Veškerá komunikace probíhá bez použití jakýchkoli bezpečnostních aparátů.

Není vyloučeno napadení scripu neoprávněnými osobami a jeho následné zneužití.

2. Kryptograficky ošetřený scrip

Spotřebitel a prodejce používají při vzájemné komunikaci prostředky symetrického kódování. Vzhledem k velmi malým částkám přenášeným v systému Millicent, je možno považovat použití kryptografických technik za neúměrně náročné. Nevýhody (vyšší nároky na zpracování a náročnější komunikace s uživatelem) v tomto případě převyšují výhody (vyšší bezpečnost a zachování soukromí).

3. Scrip s podpisem

Ochraňuje scrip před zcizením a to bez použití kryptografických technik. Podpis se generuje hashovací funkcí scripu, tajného uživatelského identifikátoru a požadavku. Tento podpis je vytvořen zákazníkem a je zaslán spolu se scripem a objednávkou prodejci. Prodejce, který je schopen odvodit uživatelský identifikátor, je schopen provést kontrolu autenticity podpisu. Jakákoli změna, ke které došlo neoprávněným zásahem, způsobí odlišnost obou podpisů. Jestliže se podpisy neshodují, prodejce odmítne provést požadovanou transakci.

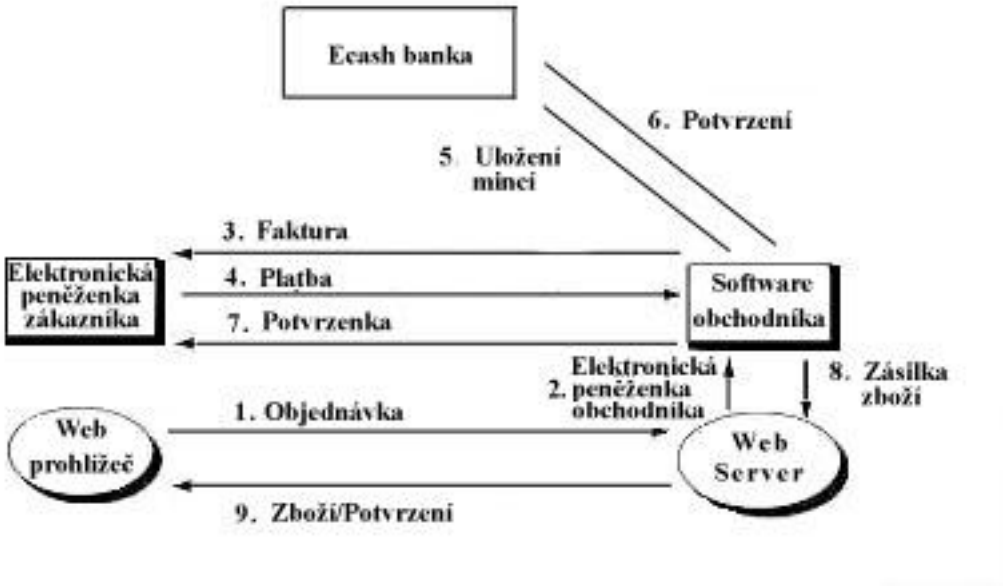
5.2 Elektronická hotovost

Celosvětově nejrozšířenější tradiční platební formou je platba hotovostí. K její mimořádné oblibě přispívá zejména její všeobecná přijatelnost, jistota řádného uskutečnění platby, anonymita a neexistence poplatků za transakce. Snahy nalézt elektronickou obdobu takového platebního styku, která by zachovávala tyto výhody a přitom splňovala požadavky vyplývající z využití ve virtuálním prostředí, vyústily ve vznik hned několika projektů, z nichž se nejúspěšněji prosazují zejména tři: Ecash, CAFE a NetCash. Základní princip fungování elektronických hotovostních plateb demonstruji na příkladu systému Ecash.

5.2.1 ECASH

Ecash, též zvaný Digicash, je produktem firmy Digicash se sídlem v USA a Holandsku. Jeho hlavním kvalitativním rysem je uplatnění mechanismů, zajišťujících zcela anonymní a bezpečné platby na Internetu.

V systému Ecash tvoří základní jednotky spotřebitelé (klienti), obchodníci a banky (výhradně banky zapojené do sítě Ecash služeb). U těchto bank vedou své účty jak spotřebitelé, tak obchodníci.



obrázek 64 - Schéma systému ECash

5.2.1.1 Ecash mince

Mince jsou jednotky používané v systému Ecash jako platidlo. Spotřebitelé mohou elektronickou formou “vybrat" část úspor ze svých bankovních kont tak, že tyto peníze převedou ve formě tzv. mincí (coins, dále pouze mince) do své elektronické peněženky (tzv. cyberwallet), uložené na pevném disku počítače. Každé minci je přiřazeno sériové číslo. To je vygenerováno samotným spotřebitelem za pomoci softwaru zabezpečujícího aplikaci elektronické peněženky. Sériová čísla jsou

generována náhodným výběrem a jsou dostatečně vysoká, aby pravděpodobnost výskytu dvou stejných čísel byla snížena na přijatelné minimum. Po přiřazení sériových čísel k mincím, jsou tato čísla ošetřena tak, že jsou při dalších krocích skryta a chráněna proti přečtení. Mince s takto zastřenými sériovými čísly jsou posléze zaslány zpět do Ecash banky, ve které má uživatel veden svůj účet. Banka opatří mince tzv. podpisem naslepo a mince odešle zpět ke spotřebiteli, který před jejich použitím opětovně zčitelní sériová čísla.

Banka svým podpisem stvrzuje platnost mince i její hodnotu, kterou stanovuje sám spotřebitel. Vzhledem k nečitelnosti sériového čísla a k použití podpisu naslepo tak banka nemá kontrolu nad skutečnou hodnotou, kterou spotřebitel minci přiřadil. Banka má k dispozici pouze žádost spotřebitele o podepsání těchto mincí s jejich údajnou hodnotou. Z tohoto důvodu musí banka při ochraně proti padělání hodnot mincí používat při podpisu naslepo sadu soukromých kryptografických podpisových klíčů, z nichž každý je určen vždy právě pro jednu hodnotovou kategorii mince. Jen v této hodnotě je pak minci možno použít. Aby bylo možno při platbě minci verifikovat, je její součástí i veřejný kryptografický podpisový klíč banky, ve které byla podepsána.

5.2.1.2 Proces platby

Spotřebitel zašle objednávku zboží obchodníkovi.

Obchodník poté odešle fakturu. Faktura obsahuje detailní informace o množství objednaného zboží, měnu, ve které má být proplacena, datum, jméno obchodníkovy Ecash banky a identifikační číslo jeho účtu u této banky. Faktura je odeslána bez použití jakýchkoli ochranných mechanismů.

Rozhodne-li se spotřebitel zaplatit požadovanou sumu, zašle software pro aplikaci elektronické peněženky automaticky požadovaný počet mincí, v případě potřeby vybere z bankovního účtu dostatečný obnos pro tvorbu nových mincí.

Spotřebitel zašle mince přesně odpovídající fakturované hodnotě obchodníkovi. (Suma odeslaná prodejci a fakturovaný obnos se musí přesně shodovat. V systému Ecash není možné z důvodu uchování anonymity kupce, vracet peníze nazpět.)

5.2.1.3 Bezpečnost

Bezpečnost systému Ecash je zajištěna nasazením mechanismů symetrické i asymetrické kryptografie. Ochrany uvnitř systému, zejm. kontroly proti použití neplatných mincí, je dosaženo verifikací, kterou provádí banka ve své databázi použitých mincí. Tato databáze je zároveň slabinou systému Ecash. Při hromadnějším využívání systému Ecash by nutně docházelo k přetížení a k nepřijatelnému prodloužení doby odezvy při zpracování dat.

5.3 Elektronické šeky

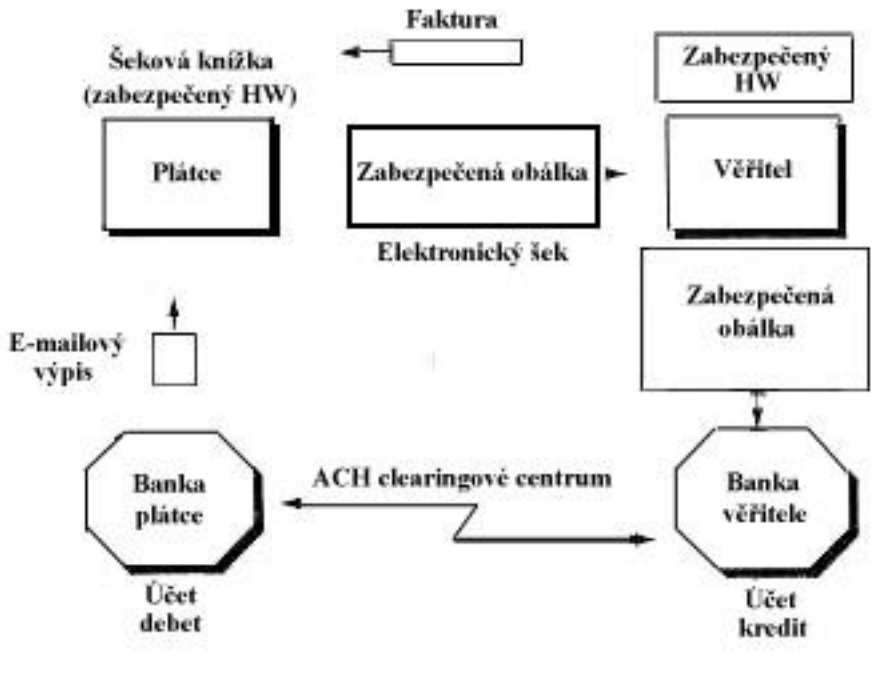
Zatímco ve Spojených státech amerických se platební šeky těší velké oblibě, v Evropě jejich používání soustavně klesá. Důvodem tohoto poklesu popularity je především finanční náročnost zpracování tohoto typu plateb a obtíže spojené s navrácenými, neproplatitelnými šeky. Tyto nedostatky je možno překonat elektronickou variantou platebních šeků, která by umožňovala převod finančních obnosů z účtu plátce (směnečníka) na účet věřitele formou okamžitého převodu při transakci. Z pohledu bank je přitom žádoucí maximální možnou měrou využít již zavedených sítí využívaných pro mezibankovní peněžní transfer.

Dosud byla vyvinuta řada systémů pro platby elektronickými platebními šeky. Mezi nimi je možno jmenovat zejména Netbill, Netcheque či projekt Konsorcia pro technologii finančních služeb (The Financial Services Technology Consortium - FSTC). Toto konsorcium se skládá ze zástupců amerických bank, výzkumných institucí a vládních organizací. Jeho cílem je přispívat k posilování amerického finančního průmyslu. Podpora projektu ze strany předních amerických bankovních domů, dává tomuto projektu velkou naději na úspěch a rozšíření v praxi.

5.3.1 Projekt FSTC

Projekt elektronických platebních šeků FSTC zdůrazňuje co nejefektivněji využít stávající bankovní infrakstrukturu s cílem propojení tradičních a nových bankovních služeb.

Elektronická forma šeků se oproti jejich tradiční podobě vyznačuje značnou flexibilitou při zpracování. Je možno provádět okamžité ověření dostupnosti finančních zdrojů. Vyšší míra bezpečnosti je zajištěna ratifikací



obrázek 65 - Schéma systému FSTC

digitálních podpisů. Modifikací polí dat na elektronickém šeku lze vystavovat různé typy šeků (např. změnou v poli “Měna" vznikne cestovní šek). Elektronické šeky mohou být snáze zakomponovány do procesu elektronických objednávek a fakturací.

Plátce zašle řádně vyplněný šek spolu s certifikátem a digitálním podpisem v bezpečnostní elektronické obálce věřiteli. Forma elektronické obálky není specifikována v rámci konceptu FSTC a může existovat v řadě variant přizpůsobených různým potřebám, případnému technickému vybavení platebních stran (např. varianta pro e-mail, pro kryptograficky ošetřený interaktivní dialog atd.). Věřitel indosuje šek prostřednictvím speciálního hardwarového zařízení a odešle jej své bance k proplacení. Samotný proces zpracování elektronického šeku bankou je zcela identický s procesem proplacení šeku prostřednictvím běžného automatizovaného clearingového centra (ACH) nebo metodou předložení elektronického šeku.

Model projektu FSTC vychází z předpokladu, že každá ze stran účastnící se platby formou elektronického šeku, je registrována některou z institucí poskytujících veřejné identifikační klíče.

Klíčovou podmínkou v projektu FSTC je vlastnictví elektronické šekové knížky uložené na bezpečném hardwarovém zařízení. Funkcí tohoto zařízení je bezpečné uchovávání tajného soukromého klíče a certifikátu vystaveného některou z certifikačních autorit a registrace vystavených a indorsovaných elektronických šeků.

5.3.1.1 Proces provádění plateb

Rychlý přenos dat o elektronických šecích mezi zúčastněnými stranami v prostředí počítačových sítí je základem architektury projektu FSTC. V praxi je možno uplatnit tento koncept ve čtyřech různých modifikacích, scénářích odpovídajících různým úrovním zabezpečení jednotlivých stran požadovaným hardwarovým vybavením.

Scénáře:

- Deposit-and-clear
- Cash-and-transfer
- Lockbox
- Funds transfer

5.4 Přímé bankovnictví - HomeBanking

Přímé bankovnictví znamená poskytování bankovních služeb, dostupných klientovi, pomocí přímých komunikačních kanálů, které umožňují bezprostřední přístup k zadávání bankovních operací, objednávání služeb nebo práci s účty.

5.4.1 Expandia banka

Expandia banka využívá těchto informačních kanálů:

- telefon (standartně nebo krátké textové zprávy GSM-SMS)
- fax
- Internet

5.4.1.1 Bezpečnost

K zabezpečení proti zneužití či zkreslení přenášených informací slouží klientovi jeho osobní „Elektronický klíč“, který má rozměry malé kapesní kalkulačky a klient jej tedy může mít vždy při sobě. Zadáním osobního identifikačního čísla (PIN) uvede klient Elektronický klíč do činnosti a ten sám vygeneruje jedinečný autentizační kód. Autentizační kód a klientské číslo umožní klientovi přihlásit se do systému banky.

Elektronický klíč je vyráběn francouzskou firmou ActivCard. Slouží k autentizaci klienta a banky a navíc k certifikaci dat posílaných klientem do banky. Využívá principu symetrického šifrování.

Pro šifrování na Internetu je aplikováno SSL3 (s klíčem 128 bitů) a pro asymetrické šifrování a digitální podpisy je implementována technologie RSA. Expandia banka získala povolení certifikační autority Verisign, opravňující k používání 128 bitové šifry.

Aby byl zabráněn přístup jakéhokoliv neautorizovaného subjektu do prostředí banky, je vnitřní prostor chráněn systémem hardwarových a softwarových ochranných zdí. Ochranné zdi (firewally) jsou vždy umístněny před všechny systémy používané v bance. Firewally umožní přístup pouze těm klientům, kteří splňují definované pravidlo. Pokud se objeví jiný požadavek nesplňující zadanou podmínku, firewall přístup odmítne.

Aby se útočník z Internetu proboural až k centrálnímu počítači je technicky nemožné. Na centrální systém je aplikována řada po sobě jdoucích ochran. V této řadě serverů jsou použité i jiné platformy operačních systémů, které od sebe mají odlišné vlastnosti. V rámci přístupové větve také dochází ke změně komunikačního protokolu TCP/IP používaného na Internetu na zcela odlišný komunikační protokol, což technicky znemožňuje přímé napojení na klientský systém. Každý ze systémů je on-line monitorován a každá neobvyklá operace je zaznamenána.

6. Závěr

Domnívám se, že v časovém horizontu 5 až 10 let může elektronické obchodování získat dominantní roli. Překážky, které v současné době ještě stojí v cestě rozvoji elektronického obchodu (legislativní, bezpečnostní, platební apod.) budou poměrně rychle překonány. K tempu odstraňování těchto bariér přispívá, podle mého názoru, zejména silná motivace komerční i vládní sféry, kteřé se snaží získat pro své firmy a občany co nejpevnější postavení v nově vznikající oblasti potenciálně vysokých příjmů.

Nesdílím ovšem futuristické představy těch, kteří se domnívají, že elektronické obchodování v budoucnosti zcela vytlačí "tradiční formy obchodu". Domnívám se, že obchod bude vždy i projevem sociální aktivity člověka uskutečňované v přímém kontaktu mezi členy společnosti. Tento přímý kontakt jedinců zůstane podle mého názoru nenahraditelnou lidskou potřebou, která se bude projevovat i v obchodních aktivitách.

Česká republika by neměla přehlédnout pohyby sil v této oblasti a plně si uvědomit rozsah příležitostí, které elektronické obchodování nabízí. Naše postavení není vůbec srovnatelné se situací v USA či Evropské unie, ale právě snahy o začlenění do evropských struktur by nás měly ještě více motivovat ke zlepšení situace v oblasti, kterou tyto regiony považují za jednu z klíčových v jejich budoucím vývoji. To znamená zejména zlepšit situaci v oblasti telekomunikací, vytvořit co nejpříhodnější legislativní zázemí pro rozvoj elektronického obchodu, stále a intensivněji zlepšovat vybavení škol a universit výpočetní technikou (včetně připojení na Internet), podporovat aktivity rozšiřující obecné povědomí široké veřejnosti (a podnikatelské sféry zejména) o možnostech elektronického obchodu a maximálně podporovat iniciativy komerčních subjektů směřujících k rozvoji elektronického obchodu u nás. Velkou inspirací by pro nás mohly být obdobné snahy v Evropské unii deklarované ve zprávě komisaře Bangemanna a týkající se celkové informatizace společnosti. Nepochybuji, že úsilí, které do této oblasti vložíme, se nám v budoucnosti mnohonásobně vyplatí.

Myslím si, že platební systém který jsem vytvořil, tak jak je napsaný by měl splňovat většinu bezpečnostních kritérií kladených na elektronický obchod. To ovšem neznamená, že sada těchto protokolů je dokonalá. Během práce na systému, i během implementace, mě napadala různá vylepšení, která jsem si už ovšem z časových důvodů nemohl dovolit.

Otázku, kterou si můžeme položit je význam této práce. Nepředstírám, že v této fázi jde o význam pouze teoretický. Jde hlavně o ověření možnosti použití kryptografie s veřejným klíčem v oblasti elektronického obchodu. To možné je. V průběhu práce se objevovaly výhody kryptografie s veřejným klíčem, ale také zápory jejího využití.

Mezi výhody lze počítat jednoduchost vyměňování klíčů bez použití jakékoli další technologie. Tato výhoda se zvláště projeví při případné výměně šifrovacích klíčů banky. To je vlastnost, které u symetrického kódování nemohu nikdy dosáhnout. Dalším kladem je bezesporu vysoká bezpečnost algoritmů asymetrické kryptografie, která je v této aplikační oblasti obzvláště potřebná.

Nevýhodou je relativně velká délka jednotlivých zpráv, která je závislá na velikosti modulu asymetrických šifrovacích klíčů. Jestliže máme modul o délce

1024 b, tak po zašifrování bude nejkratší zpráva (i kdyby měla původně 1 bit) dlouhá 128 oktetů. Z toho vyplývá vyšší náročnost na přenosové médium oproti použití symetrické kryptografie. To by se v určitých prostředích mohlo negativně projevit na výkonnosti celého systému.

7. Příloha

7.1 Slovník pojmů

Acquirer Banka obchodníka. Je to finanční instituce zakládající konta obchodníkům a zpracovávající autorizace platebních karet a plateb.

Brand Značka. Finanční instituce založená společnostmi vydávající platební karty, která chrání a inzeruje značku. Zakládá a uvádí v platnost pravidla pro použití a příjem jejich platebních karet a obstarává sítě propojující finanční instituce.

Cardholder Zákazník. V prostředí elektronického obchodu, spotřebitelé a obchodní nákupčí vzájemně spolupracující s obchodníky z osobních počítačů. Zákazník používá platební kartu, která mu byla vydána jeho bankou (issuer).

Certifikační autorita (CA) Je to obvykle všeobecně známá instituce vytvářející a vydávající certifikáty uživatelům.

DES Data Encryption Standart. Standard kódování dat.

Digitální certifikát Je veřejný klíč spojený s údaji o osobě, a obojí je digitálně podepsané třetí důvěryhodnou stranou, jejíž veřejný klíč je znám.

IBM Společnost, která je největším dodavatelem technologie SET.

Issuer Banka zákazníka. Je to finanční instituce zakládající konta pro zákazníky a vydává platební karty. Garantuje platbu pro autorizované transakce s platební kartou ve shodě s pravidly společnosti vydávající platební karty a lokální legislativou.

Mastercard Společnost zabývající se obchodem, jejíž standarty jsou používány pro platební karty.

Merchant Obchodník. Nabízí zboží k prodeji nebo poskytuje služby za úhradu. Se SETem obchodník může nabízet zákazníkům bezpečné elektronické interakce. Jestliže chce přijímat platební karty musí mít smlouvu s bankou obchodníka (acquirer).

Message digest Je to řetězec znaků (pevné délky) z jednocestné hashovací funkce, jejíž vstupem je daná zpráva (proměnné délky).

Microsoft Outlook Softwarový produkt firmy Microsoft Corporation. Je to prohlížeč Internetové pošty.

MIME Multipurpose Internet Message Extensions. Používá se pro kódování obálek pro platební zprávy, které podporuje Internetový prohlížeč.

MIPS Million Instructions Per Second. Milion instrukcí za vteřinu. Zkratka udávající výkonnost procesoru.

MOTO Mail Order / Telephone Order. Nákup na dobírku poštou.

Netscape Communicator Softwarový produkt firmy Netscape Communications Corporation. Je to Internetový prohlížeč.

Payment gateway Platební brána. Je to zařízení ovládané bankou obchodníka nebo navrhnuté třetí stranou ke zpracování platebních zpráv obchodníka včetně platebních instrukcí zákazníka.

Private key Tajný (privátní) klíč. Je to kryptografický klíč používaný ve spolupráci s veřejným klíčem. Není určen pro veřejné použití. Tento klíč je používán pro tvorbu digitálních podpisů nebo dekódování zpráv a souborů.

Public key Veřejný klíč. Je to kryptografický klíč používaný ve spolupráci s tajným klíčem. Je volně šiřitelný. Je používán ke kontrole podpisů vytvořených tajným klíčem. Je také používán ke kódování zpráv nebo souborů, které pak mohou být dekódovány pouze správným tajným klíčem.

RSA Rivest Shamir Adleman. RSA je také příklad veřejného klíče.

SET Secure Electronic Transaction. Je to komunikační protokol pro provedení bezpečné platby mezi držitelem platební karty a obchodníkem v prostředí nezabezpečené komunikační sítě.

SSL Secure Socket Layer. Zajišťuje bezpečný přenos libovolných dat mezi dvěma subjekty.

Third party Třetí strana. Banky zákazníků a obchodníků občas vyberou ke zpracování transakcí platebních karet třetí stranu.

VISA Společnost zabývající se obchodem, jejíž standarty jsou používány pro platební karty.

7.2 Literatura

1. **SET Book 1: Business description v1.0, 1997**
   Zdroj: http://www.setco.org
   Pozn.: Základní informace o SET protokolu.

2. **SET Book 2: Pogrammer's Guide v1.0, 1997**
   Zdroj: http://www.setco.org
   Pozn.: Informace o programování a strukturách SET protokolu.

3. **WWW.SET.CZ**
   Pozn.: Informace o technologii SET a vývoj technologie v ČR.

4. **WWW.VISA.COM**
   Pozn.: Společnost vydávající platební karty.

5. **WWW.MASTERCARD.COM**
   Pozn.: Společnost vydávající platební karty.

6. **WWW.KOBA.CZ**
   Pozn.: První banka ve střední Evropě s technologií SET.

7. **WWW.TORRY.RU**
   Pozn.: Stránka s komponentami pro Delphi.

8. **H. Škorpíková: Využití Internetu v oblasti obchodu, 1998**
   Zdroj: CD-ROM z časopisu ComputerWorld
   Pozn.: Diplomová práce

9. **D. Cvrček: Platební protokol elektronické peněženky s veřejným klíčem, 1997**
   Zdroj: http://www.fee.vutbr.cz/~cvrcek/diplomka/
   Pozn.: Diplomová práce

10. **WWW.EBANKA.CZ**
    Pozn.: Banka poskytující službu HomeBanking.

7.3 Obsah

1. ÚVOD 2

1.1 ÚVOD DIPLOMOVÉ PRÁCE 2
1.2 PLATEBNÍ STYK 3
1.2.1 Co jsou bezhotovostní platby z účtu 3
1.2.2 Co je platební karta 4
1.3 BEZPEČNOST DAT 6
1.3.1 Symetrické šifrování 6
1.3.2 Asymetrické šifrování 6
1.3.3 Digitální podpis 7
1.3.4 Digitální certifikát 9
1.3.5 Kombinace symetrické a asymetrické šifry 10
1.3.6 Poznámka k existenci asymetrické šifry 10

2. SET 12

2.1 ÚVOD DO SETU 12
2.2 BEZPEČNOST SETU 14
2.3 POSTUP PŘI PLACENÍ SETEM V OBCHODNÍM DOMĚ 15
2.4 DETAILNÍ POPIS PROCESU PLATBY SETEM 18
2.4.1 Úvod k popisu 18
2.4.2 Funkce certifikační autority 19
2.4.3 Získání certifikátu 20
2.4.3.1 Certifikace zákazníka 20
2.4.3.2 Certifikace obchodníka 21
2.4.3.3 Certifikace platební brány 21
2.4.3.4 Certifikace banky obchodníka 21
2.4.3.5 Certifikace banky zákazníka 21
2.4.3.6 Hierarchie zabezpečení 22
2.4.4 Registrace zákazníka 22
2.4.4.1 Krok č. 1 23
2.4.4.2 Krok č. 2 24
2.4.4.3 Krok č. 3 24
2.4.4.4 Krok č. 4 25
2.4.4.5 Krok č. 5 26
2.4.4.6 Krok č. 6 27
2.4.4.7 Krok č. 7 28
2.4.5 Registrace obchodníka 29
2.4.5.1 Krok č. 1 30
2.4.5.2 Krok č. 2 30
2.4.5.3 Krok č. 3 30
2.4.5.4 Krok č. 4 32
2.4.5.5 Krok č. 5 33
2.4.6 Nákupní žádost 33
2.4.6.1 Krok č. 1 34
2.4.6.2 Krok č. 2 34
2.4.6.3 Krok č. 3 34
2.4.6.4 Krok č. 4 36
2.4.6.5 Krok č. 5 37
2.4.7 Autorizace platby 38
2.4.7.1 Krok č. 1 38
2.4.7.2 Krok č. 2 39
2.4.7.3 Krok č. 3 40
2.4.8 Uskutečnění platby 41
2.4.8.1 Krok č. 1 42
2.4.8.2 Krok č. 2 42
2.4.8.3 Krok č. 3 43

3. VÝVOJ SETU 45

3.1 VÝVOJ V ČESKÉ REPUBLICE 45
3.1.1 Historie 45

3.2 VÝVOJ VE SVĚTĚ ... 48
3.2.1 Historie ... 48
3.3 JAK ZÍSKAT SET JAKO ZÁKAZNÍK ... 50
3.3.1 Konkrétně v České republice ... 50
3.3.2 Obecně kdekoliv ... 50
3.3.3 Obdržení certifikátu ... 50
3.4 JAK ZÍSKAT SET JAKO OBCHODNÍK ... 55

4. NÁVRH EXPERIMENTÁLNÍHO SYSTÉMU ... 56

4.1 POŽADAVKY NA PLATEBNÍ SYSTÉM ... 56
4.1.1 Obchodní požadavky ... 56
4.1.2 Technické požadavky ... 57
4.1.2.1 Důvěrnost informací ... 58
4.1.2.2 Integrita dat ... 58
4.1.2.3 Autentizace ... 58
4.1.2.4 Neodmítnutelnost odpovědnosti ... 59
4.2 TEORETICKÉ ŘEŠENÍ ... 60
4.2.1 Bezpečnostní požadavky ... 60
4.2.1.1 Vstupní hashovací algoritmus ... 60
4.2.1.2 Symetrické kódování ... 60
4.2.1.3 Asymetrické kódování ... 60
4.2.1.4 Digitální podpis ... 60
4.3 PROGRAMOVÉ ŘEŠENÍ ... 61
4.3.1.1 Peněženka ... 61
4.3.1.2 Obchodník ... 61
4.3.1.3 Banka ... 62
4.3.1.4 CGI ... 64
4.4 POPIS FUNKCE A TOKU DAT ... 65
4.4.1 Popis funkce ... 65
4.4.2 Tok dat ... 67
4.4.3 Formáty zpráv ... 69
4.4.3.1 Veřejný klíč ... 69
4.4.3.2 Symetrický klíč ... 69
4.4.3.3 Jednoduchá zpráva ... 69
4.4.3.4 Dvojitá zpráva ... 70

5. POROVNÁNÍ S JINÝMI PLATEBNÍMI SYSTÉMY ... 71

5.1 MIKROPLATBY ... 71
5.1.1 MILLICENT ... 71
5.1.1.1 Proces provádění plateb ... 72
5.1.1.2 Bezpečnost ... 72
5.2 ELEKTRONICKÁ HOTOVOST ... 74
5.2.1 ECASH ... 74
5.2.1.1 Ecash mince ... 74
5.2.1.2 Proces platby ... 75
5.2.1.3 Bezpečnost ... 75
5.3 ELEKTRONICKÉ ŠEKY ... 76
5.3.1 Projekt FSTC ... 76
5.3.1.1 Proces provádění plateb ... 77
5.4 PŘÍMÉ BANKOVNICTVÍ - HOMEBANKING ... 78
5.4.1 Expandia banka ... 78
5.4.1.1 Bezpečnost ... 78

6. ZÁVĚR ... 79

7. PŘÍLOHA ... 81

7.1 SLOVNÍK POJMŮ ... 81
7.2 LITERATURA ... 83
7.3 OBSAH ... 84
7.4 SEZNAM OBRÁZKŮ ... 87
7.5 SEZNAM TABULEK ... 88

7.4 Seznam obrázků

obrázek 1 - Příkaz k úhradě ... 3
obrázek 2 - Schéma platby v kamenném obchodě ... 4
obrázek 3 - Symetrické šifrování ... 6
obrázek 4 - Asymetrické šifrování ... 7
obrázek 5 - Message digest - odesílatel ... 7
obrázek 6 - Message digest - příjemce ... 8
obrázek 7 - Certifikační autorita ... 10
obrázek 8 - Platební systém se SETem ... 12
obrázek 9 - Platba SETem ... 15
obrázek 10 - Inicializace peněženky ... 16
obrázek 11 - Peněženka účty ... 16
obrázek 12 - Ověření obchodníka ... 17
obrázek 13 - Peněženka - účty ... 17
obrázek 14 - Hierarchie zabezpečení ... 22
obrázek 15 - Registrace zákazníka ... 23
obrázek 16 - Registrace zákazníka - krok č. 1 ... 23
obrázek 17 - Registrace zákazníka - krok č. 2 ... 24
obrázek 18 - Registrace zákazníka – krok č. 3 ... 25
obrázek 19 - Registrace zákazníka – krok č. 4 ... 25
obrázek 20 - Registrace zákazníka - krok č. 5 ... 27
obrázek 21 - Registrace zákazníka - krok č. 6 ... 28
obrázek 22 - Registrace zákazníka - krok č. 7 ... 29
obrázek 23 - Registrace obchodníka ... 29
obrázek 24 - Registrace obchodníka - krok č. 1 ... 30
obrázek 25 - Registrace obchodníka - krok č. 2 ... 30
obrázek 26 - Registrace obchodníka - krok č. 3 ... 31
obrázek 27 - Registrace obchodníka - krok č. 4 ... 32
obrázek 28 - Registrace obchodníka - krok č. 5 ... 33
obrázek 29 - Nákupní žádost ... 33
obrázek 30 - Nákupní žádost - krok č. 1 ... 34
obrázek 31 - Nákupní žádost - krok č. 2 ... 34
obrázek 32 – Nákupní žádost – krok č. 3 ... 36
obrázek 33 - Nákupní žádost - krok č. 4 ... 37
obrázek 34 - Nákupní žádost - krok č. 5 ... 37
obrázek 35 - Autorizace platby ... 38
obrázek 36 - Autorizace platby – krok č. 1 ... 38
obrázek 37 - Autorizace platby – krok č. 2 ... 40
obrázek 38 - Autorizace platby – krok č. 3 ... 41
obrázek 39 - Uskutečnění platby ... 41
obrázek 40 - Uskutečnění platby - krok č. 1 ... 42
obrázek 41 - Uskutečnění platby - krok č. 2 ... 43
obrázek 42 - Uskutečnění platby - krok č. 3 ... 44
obrázek 43 - Inicializace peněženky ... 51
obrázek 44 - Zadání hesla ... 51
obrázek 45 – Přidání nové karty ... 51
obrázek 46 - Peněženka účty ... 52
obrázek 47 - Zadání hash kódu ... 52
obrázek 48 - Registrace certifikátu – krok č. 1 ... 53
obrázek 49 - Registrace certifikátu – krok č. 2 ... 53
obrázek 50 - Inicializace peněženky ... 54
obrázek 51 - Peněženka účty ... 54
obrázek 52 - Program Obchodník ... 61
obrázek 53 - Program Banka ... 62
obrázek 54 - Program Banka - nastavení procesů ... 62
obrázek 55 - Program Banka - nastavení zákazníků ... 63
obrázek 56 - Program Banka - nastavení obchodníků ... 63
obrázek 57 - V.O.D. - nákupní košík ... 65

obrázek 58 - Inicializace peněženky *65*
obrázek 59 - Peněženka *66*
obrázek 60 - Peněženka - ukončení transakce *67*
obrázek 61 - Tok dat při platbě *67*
obrázek 62 - Tok dat při výpisu transakcí *69*
obrázek 63 - Schéma systému MILLICENT *72*
obrázek 64 - Schéma systému ECash *74*
obrázek 65 - Schéma systému FSTC *76*

7.5 Seznam tabulek

tabulka 1 - Symboly použité v diagramech *19*
tabulka 2 - Přehled posílaných zpráv *68*