VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

UŽITÍ PROTOKOLU ACP PRO PLATEBNÍ SYSTÉMY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

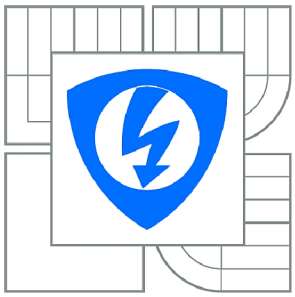
AUTOR PRÁCE
AUTHOR

JAROSLAV KUNC

BRNO 2014

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

UŽITÍ PROTOKOLU ACP PRO PLATEBNÍ SYSTÉMY

ACP PROTOCOL IN PAYMENT SYSTEMS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

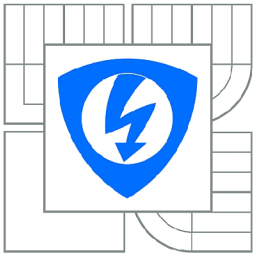
AUTOR PRÁCE — JAROSLAV KUNC

AUTHOR

VEDOUCÍ PRÁCE — Ing. IVO STRAŠIL

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Jaroslav Kunc	***ID:***	147451
Ročník:	3	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Užití protokolu ACP pro platební systémy

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je vypracovat scénáře užití protokolu ACP v platebních systémech.

Práce bude obsahovat:
- analýzu nyní užívaných protokolů pro platební systémy (zejm. pro platby po internetu) se zaměřením na bezpečnostní problémy a problémy použitelnosti,
- diskuzi cílů vývoje nového systému s co nejvyšší mírou interoperability a bezpečnosti. Diskuzi k anonymitě plateb,
- základní scénáře transakcí nového protokolu pro internetové a mobilní platby. Posouzení praktické použitelnosti nového protokolu z hlediska bezpečnosti, datové a výpočetní resp. časové náročnosti transakcí a obtížnosti implementace.

DOPORUČENÁ LITERATURA:

[1] BURDA, K. Univerzální rámec pro řízení přístupu v počítačových sítích. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2011, roč. 2011, č. 9, s. 1-6. ISSN: 1213- 1539.
[2] BURDA, K.; LEŽÁK, P. Aplikace univerzálního rámce řízení přístupu. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2012, roč. 2012, č. 28, s. 1-5. ISSN: 1213- 1539.
[3] ČÍKA, P. Protokol pro zabezpečení elektronických transakcí - SET. Elektrorevue - Internetový časopis (http://www.elektrorevue.cz), 2006, roč. 2006, č. 45, s. 1 (s.)ISSN: 1213- 1539.

Termín zadání:	10.2.2014	***Termín odevzdání:***	4.6.2014

Vedoucí práce: Ing. Ivo Strašil
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

ABSTRAKT

Bakalářská práce se zaměřuje na protokol pro kryptografické systémy v platebních systémech vyvinutých na ÚTKO. V práci jsou zahrnuty analýzy nyní používaných protokolů pro elektronické platební systémy. Práce popisuje základní princip protokolů AAA (autorizace, autentizace a účtování) a základní princip protokolu ACP. Práce obsahuje diskuzi cílů nového systému pro platební transakce a diskuzi anonymity plateb. Dalším úkolem této práce je vypracovat scénáře pro užití protokolu ACP v elektronických platebních systémech a zhodnotit tyto scénáře.

KLÍČOVÁ SLOVA

AAA, ACP, elektronické platební systémy, internetové platební systémy, protokoly pro platební systémy

ABSTRACT

Bachelor's thesis focuses on the protocol for the cryptographic systems in payment systems developed for ÚTKO. The thesis analyses now used protocols for electronic payment systems. The thesis describes the basic principle of AAA protocols (Authentication, Authorization and Accounting) and the basic principle of ACP protocol. The thesis includes a discussion of the objectives of the new system for payment transactions and discussion about anonymity of this transactions. The next object of this thesis is to develop scenarios inclusive protocol ACP in electronic payment systems and evaluate this scenarios.

KEYWORDS

AAA, ACP, electronic payment systems, internet payment systems, protocols for payment systems

KUNC, Jaroslav *Užití protokolu ACP pro platební systémy*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 41 s. Vedoucí práce byl Ing. Ivo Strašil.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Užití protokolu ACP pro platební systémy“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Ivo Strašilovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

(podpis autora)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Již od počátku vývoje lidstva je zájem o jednoduché a bezpečné obchodování. Dnes, v 21. století pro nás představuje jednoduchost a rychlost elektronika ve spojení s internetem.

V dnešní době existuje již celá řada systémů (protokolů) pro elektronické obchodování, nicméně tyto systémy jsou nezastupitelné a nejsou schopny vzájemné spolupráce. Proto se na VUT Brně (ústav telekomunikací) zrodila myšlenka na vytvoření univerzálního přístupového rámce, který by se dal univerzálně využít pro všechny druhy elektronického platebního styku.

Díky vzniku této myšlenky byl vytvořen protokol ACP (Access Control Protocol), který se zaměřuje právě na univerzální rámec a jeho komunikaci mezi portály AAA (Authentication, Authorization a Accounting). V tomto systému ACP se počítá se zavedením AAA portálu na každém zařízení, které se účastní transakce. Aby tento stav mohl vzniknout, je potřeba samotné AAA portály definovat již v samotném operačním systému daného zařízení.

V první kapitole této práce jsou uvedeny základní požadavky na elektronické platební systémy. Požadavky jsou rozděleny na všeobecné, funkční, bezpečnostní a na požadavky na autorizaci. Dále jsou v kapitole rozebrány protokoly pro elektronické platební systémy (Secure Electronic Transaction, VISA 3D-Secure, Secure Sockets Layer, Open Financial Exchange, atd.) a internetové platební systémy (PayPay, PayPal, Moneybookers, PaySec).

Ve druhé kapitole je uveden teoretický úvod AAA systémů, tedy systémů pro správnou autentizaci, autorizaci a účtování. Je zde popsána funkce systému AAA, dále pak rozšiřenost protokolů AAA a je zde rozebrán univerzální rámec systémů AAA. V této kapitole je rozebrán i protokol ACP, jsou zde rozebrány formáty zpráv a popsány jednotlivé pole, použité v ACP. Dále jsou zde uvedeny typy zpráv ACP a k čemu v komunikaci slouží.

Ve třetí kapitole jsou diskutovány cíle vývoje nového systému s co nejvyšší mírou interoperability a bezpečnosti. V kapitole je uvedena diskuze anonymity plateb z pohledu všech subjektů elektronické platební transakce. Dále v kapitole nalezneme specifikace na ideální platební systém a také na reálný systém. Nakonec jsou v kapitole zrealizovány základní scénáře pro elektronické transakce s použitím protokolu ACP.

1 ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

1.1 Požadavky na elektronické platební systémy

1.1.1 Všeobecné požadavky

Všeobecně je od elektronických platebních systémů očekáváno, že budou spolehlivé, rychlé, bezpečné a jejich provoz bude vyžadovat minimální náklady. Od elektronických platebních systémů je také očekáváno, že usnadní práci jejich uživatelům. Například, že se zákazník nebude muset dostavit fyzicky na místo, kde chce nakupovat, nebude muset navštívit bankomat, aby měl peníze fyzicky u sebe, ale například prostřednictvím internetu přepraví své peníze ze svého klientského účtu na účet obchodníka, který zakoupené zboží pošle například poštou. Dále mezi všeobecné požadavky patří schopnost systému pracovat nezávisle na jiných systémech a také nezávisle na operačním systému uživatele.

1.1.2 Bezpečnostní požadavky

Mezi základní požadavky na elektronické platební systémy patří bezpečnostní požadavky. Každý, kdo využívá jakýkoliv druh elektronické platby, se zajímá o její vysokou bezpečnost. Jde především o to, že zákazník nemá při elektronické platbě své peníze fyzicky v ruce, ani nevidí konkrétního obchodníka, kterému své peníze dává, tudíž je zapotřebí tyto transakce zabezpečit vhodným způsobem. Mezi základní způsoby zabezpečení patří použití šifrovacích klíčů a dalších autentizačních technik. Klienti používající platby po internetu vystavují své peníze jistému riziku jejich odcizení, proto vývojáři platebních systémů musí brát v potaz tyto rizika. Z tohoto důvodu vzniká celá řada platebních systémů, které se snaží minimalizovat rizika zneužití elektronických platebních systémů. Mezi základní bezpečnostní vlastnosti patří:

- Integrita – Platební systém nesmí umožnit, aby se peníze převáděly z prostředků neautentizovaného uživatele. Měl by odmítnout i přijetí platby bez souhlasu (ochrana například proti uplácení).
- Utajenost – Údaje transakce (totožnost zákazníka, totožnost obchodníka, celková suma, atd.) by měly být třetí straně utajeny.
- Autentizace – Je nejdůležitější složka v platebních systémech, jde o ověření identity uživatele. Mezi základní druhy autentizace patří autentizace heslem a digitálním podpisem.

- Dostupnost – Možnost provádět platby, kdykoliv je třeba.
- Spolehlivost přenášených dat – Transakce musí být atomické – buď se transakce provede celá, nebo se neprovede nic. Ztráta peněžních prostředků kvůli chybě hardware či software je naprosto neakceptovatelná.
- Interoperabilita – Vzájemná kompatibilita protokolu mezi různými hardwarovými a softwarovými systémy.

1.1.3 Požadavky na autorizaci

Autorizace je klíčovou částí elektronické transakce. Jedná se v podstatě o překážku mezi uživatelem a aktivem – penězi. Od ideálního platebního systému se očekává, že autorizace bude bezchybná a k danému aktivu bude připuštěna skutečně jen oprávněná osoba. Při elektronické platbě je potřeba předání si autentizačních údajů mezi účastníky, běžně prostřednictvím internetu (tzn. otevřenou sítí). Naprostou samozřejmostí je tuto komunikaci šifrovat (použití kryptografie – metody utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí) nebo přenášet zabezpečeným kanálem. Náhled třetí strany do této komunikace je nepřípustný, celá autentizace by pak neměla žádný smysl. Přehled dnes používaných autentizačních prostředků internetovými bankami:

- Uživatelské jméno a heslo – K potvrzení identity slouží znalost uživatelského jména a hesla. Bezpečnost je mimo jiné závislá na zvoleném hesle.
- Certifikát – Je vystaven bankovním ústavem, prakticky se jedná o soubor uložený na libovolném médiu.
- Kalkulátor – Elektronické zařízení, generující jednorázová hesla. Zařízení jsou synchronizována se systémem banky, aby byly generovány stejné klíče.
- Autentizace pomocí SMS – Metoda generování náhodných hesel. Hesla jsou zasílána na mobilní telefon účastníka, ten je předá bance prostřednictvím webové aplikace banky.

1.1.4 Funkční požadavky

Mezi základní funkční požadavky patří flexibilita, to znamená, že platební systém by měl být schopen správně fungovat na více zařízeních. Čím více přístrojů dokáže platební systém využívat, tím lépe. Dalším funkčním požadavkem je použitelnost. Platební systém by měl být jednoduchý na použití, přehledný a intuitivní. Jeho software by měl jít snadno nainstalovat, aktualizovat a v případě potřeby i snadno

vyměnit za nový platební systém. Dále by při výpadku měl systém zajistit, aby nedošlo k újmě na žádném účastníkovi platby. Měla by být zajištěna dostupnost a stálost systému.

1.2 Protokoly pro elektronické platební systémy

1.2.1 Secure Electronic Transaction (SET)

SET je protokol, který zabezpečuje elektronické platební transakce, především se stará o správnou autentizaci, tedy ověření komunikujících stran. SET je vyvinut společnostmi Visa a MasterCard, jako metoda pro bezpečné karetní transakce přes otevřenou síť. Tento protokol je v podstatě řada zpráv, které se vyměňují mezi třemi základními entitami, a to držitelem karty, obchodníkem a platební bránou.

SET využívá tyto mechanismy:

- **Šifrování symetrickým klíčem**

  Vysílač i přijímač sdílí jeden stejný klíč. Těmito klíči lze šifrovat či dešifrovat data, která se mezi nimi odesílají. Nevýhodou je, že se klíč musí mezi přijímačem a vysílačem poslat bezpečnou cestou. Mezi nejznámější symetrické šifrovací mechanismy patří DES, 3-DES a AES.

- **Šifrování veřejným klíčem**

  Jde o asymetrické šifrování, které pro svou funkci používá dva klíče, veřejný a soukromý. Princip je takový, že vysílač šifruje zprávu pomocí veřejného klíče, příjemce ji pak dešifruje vlastním soukromým klíčem. Nejznámějším algoritmem pro šifrovaní veřejným klíčem je RSA.

- **Hašovací funkce**

  Jde o doplňkové zabezpečení, výsledkem této metody je takzvaný haš, neboli digitální otisk (tj. posloupnost určité délky). Z vypočítaného haše ze vstupních dat už nelze získat data zpět. Mezi nejznámější hašovací funkce patří MD5 a SHA1.

- **Digitální podpis**

  Ověřuje digitální informace. Používá dva algoritmy, jeden pro podepisování, druhý pro ověřování. Používá se zpravidla pro haš zprávy. Funguje tak, že haš se zašifruje soukromým klíčem odesílatele. Příjemce pak z přijaté zprávy

vytvoří haš a porovná ho s hašem od odesílatele. Pokud se shodují, je jisté, že zpráva nebyla změněna.

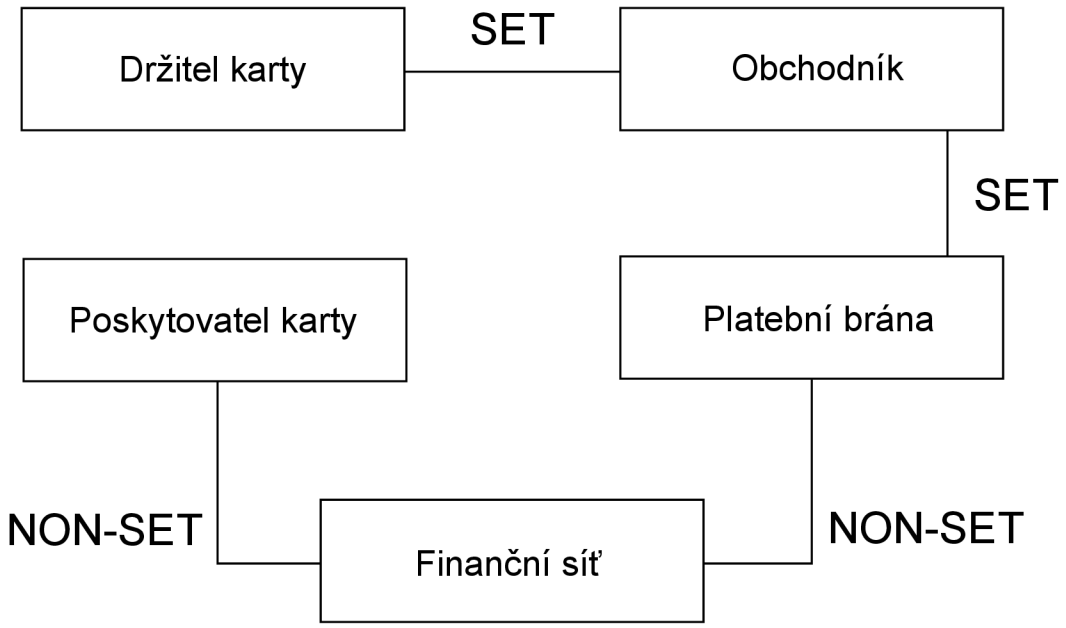
- **Digitální obálka**

  Slouží pro zabezpečený přenos symetrického klíče od vysílače k přijímači. Princip spočívá v zašifrování symetrického klíče veřejným klíčem příjemce. Výsledkem je zašifrovaný klíč, který je odeslán příjemci. Příjemce klíč dešifruje pomocí svého soukromého klíče, tím získá symetrický klíč, který se poté používá při další komunikaci.

Průběh základní transakce SET:

1. Držitel karty zašle obchodníkovi zprávu 1, kde žádá přiřazení unikátního identifikačního čísla transakce.
2. Obchodník posílá držiteli karty zprávu 2, která obsahuje přiřazené identifikační číslo. Společně s ID posílá i svůj certifikát a certifikát platební brány.
3. Držitel karty ověří přijaté certifikáty a posílá obchodníkovi zprávu 3, která obsahuje IO – informace k objednávce (ID transakce, PurchAmt) a PI – platební instrukce (ID transakce, PayAmt, účet). PurchAmt označuje očekávanou částku, kterou má držitel zaplatit, zatímco PayAmt je částka, kterou držitel karty naznačuje, že je ochoten zaplatit. Informace k objednávce jsou určeny obchodníkovi, zatímco platební instrukce platební bráně. Zpráva je zašifrována náhodně vygenerovaným symetrickým klíčem. Tento klíč je ještě zašifrován veřejným klíčem (digitální obálka).
4. Obchodník obdrží od držitele karty zašifrované zprávy IO a PI. Obchodník dešifruje IO, zkontroluje IO a zašifruje IO veřejným klíčem. V tomto kroku IO reprezentuje ID transakce a AuthAmt. AuthAmt označuje částku, o kterou obchodník žádá. Zašifrovanou PI s dvojitým podpisem a s digitální obálkou obchodník předá společně s IO platební bráně a ve zprávě 4 žádá po bráně autorizaci a získání aktiv.
5. Platební brána autorizuje držitele karty, zkontroluje hodnoty OI a PI, provede účtovací operace a ve zprávě 5 vrátí výsledek obchodníkovi. Platební brána podepíše výsledek svým soukromým klíčem.
6. Obchodník obdrží výsledek a ten pak ve zprávě 6 odešle držiteli karty.

Pozn.: Všimněme si, že jakmile obchodník dešifruje zprávu 3, může si libovolně změnit jakékoliv pole v IO. Výsledkem by mohlo být, že AuthAmt bude vyšší než PayAmt. To by znamenalo, že částka, kterou obchodník žádá by byla větší než částka, kterou je držitel karty ochoten zaplatit. Proto dochází u platební brány ke kontrole shody IO a PI.



Obr. 1.1: Diagram použití SET

Závěr

Uživatel SETu musí být držitelem platební karty. SET vyžaduje existenci infrastruktury kreditních karet. SET není univerzální platební protokol, je omezen na platební karty. Dále nezajišťuje tok financí od jednoho klienta ke druhému. Nutnou podmínkou pro používaní protokolu je vlastnictví digitálního certifikátu vydaného certifikační autoritou. Digitální certifikát musí vlastnit každý subjekt transakce. Při platbě kartou exituje jisté riziko zneužití údajů, protože držitel karty posílá číslo své karty přimo obchodníkovi. Jako symetrická šifra je použit 56-bitový DES a jako asymetrická 1024-bitový RSA. DESem jsou šigrovány jen méně důležité údaje.

1.2.2 Visa 3D-Secure

Jedná se o zabezpečený 3-doménový protokol, viz obr. 1.2.

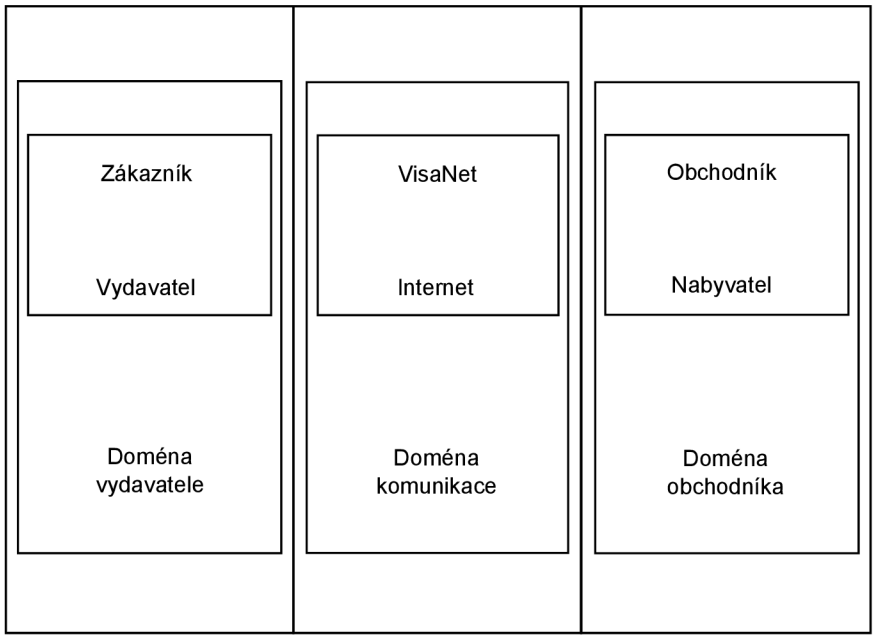
- Doména vydavatele
- Doména nabyvatele
- Doména vzájemné komunikace

Průběh základní transakce:

1. Držitel VISA karty pošle obchodníkovi číslo své kreditní karty.
2. Obchodník si zjistí status kreditní karty pomocí VISA adresáře.
3. Visa adresář se podle karetního rozsahu odkáže na příslušný Access Control Server (ACS), zda-li je karta řádně registrována.
4. ACS pošle přes VISA adresář odpověď obchodníkovi.
5. Obchodní pošle ACS požadavek na autentizaci.
6. ACS autentizuje nakupujícího, tuto autentizaci podepíše a pošle obchodníkovi.
7. Obchodník zkontroluje autentizaci a pokračuje autorizací k platbě.
8. Banka obchodníka autorizuje požadavek bankce zákazníka.

Závěr

Bezpečnost protokolu 3D-Secure je zajištěna spojením pomocí SSL. 3D-Secure ověřuje totožnost zákazníka, který je držitelem karty. Dále bezpečnost 3D-Secure spočívá v ověřování držitele karty přímo u banky obchodníka, internetový obchod tedy nemá přístup k informacím, jako je číslo karty zákazníka, což je velká výhoda tohoto protokolu. SSL zajišťuje pravost účastníků pomocí digitálních certifikátů. Výhodou 3D-Secure je, že držitel platební karty nemusí používat dodatečný software na svém počítači, nicméně je třeba registrace uživatele u vydavatele platební karty, nebo použití jiného autentizačního mechanismu. Funguje na principu centralizovaného autentizačního přístupu. To znamená, že všechny obchodníkovy komponenty jsou směrovány do VISA adresáře, který udržuje informace o všech uživatelích. Požadavek dále směřuje jen na určitého uživatele. 3D-Secure je mechanismus autentizace



Obr. 1.2: 3-D Secure, zobrazení tří domén

držitele karty. MasterCard nebo VISA mají v databázi všechny karty a na základě autentizace se provádí jejich kontrola. Výsledek autentizace je předán zpět do platební brány.

1.2.3 Secure Sockets Layer (SSL)

Jedná se o mezivrstvový protokol. Nachází se mezi vrstvou transportní a aplikační. Slouží k zabezpečení datových přenosů pomocí šifrování a autentizace komunikujících stran. Bezpečnost SSL je řešena vytvořením zabezpečeného kanálu. Data přenášená v tomto kanálu jsou šifrovaná a teoreticky by zvenčí neměla být viditelná.

Princip SSL

SSL k bezpečné komunikaci používá asymetrické šifry. Každá z komunikujících stran má dvojici klíčů, tedy veřejný a soukromý. Pokud veřejným klíčem zašifrujeme nějakou zprávu, tak je zajištěno, že ji bude moci dešifrovat pouze majitel použitého veřejného klíče svým soukromým klíčem. Pro výměnu klíčů se požívají algoritmy, jako například RSA, DSA nebo Fortezza, pro symetrickou šifru RC2, RC4 nebo IDEA, pro haš se používá MD nebo SHA.

1.2.4 Open Financial Exchange (OFX)

OFX se stará o výměnu finančních dat prostřednictvím internetu. Používá SGML ke strukturování a formátování informací posílaných mezi aplikacemi. Ve verzi 1.0.2 již používá http (Hypertext Transfer Protokol). Verze 2 je celá postavena na XML. Vše funguje na bázi požadavek – odpověď. K ověření identity se v OFX používá heslo a k ověření autorizace certifikáty. OFX podporuje i Secure Sockets Layer (SSL), což je kryptografický protokol. SSL šifruje zprávy a zajišťuje jejich integritu a autentizaci.

Hlavními bezpečnostními prvky jsou: utajenost, integrita, autentizace. Příjemce si může ověřit totožnost odesílatele. OFX využívá hašování, takže se dá ověřit, jestli daná zpráva v komunikaci nebyla změněna. OFX je volně přístupná, takže ji může využívat jakákoliv instituce.

Data v OFX jsou strukturována podle DTD (Document Type Definition). Skládají se z podepsaných elementů pro každou žádost i odpověď. Tyto elementy jsou následované dalšími elementy nazývanými message sets. Každá tato sada se skládá z menších zpráv, jako např. požadavek na bankovní vyrovnání.

1.2.5 The Bank Internet Payment System (BIPS)

Klienti mohou posílat zabezpečené platební instrukce prostřednictvím internetu. Klient posílá platební instrukce na platební server ve své bance a to pomocí e-mailu nebo webového rozhraní. BIPS překládá informace z e-mailu a webového rozhraní do bankovních platebních transakcí. BIPS server má roli brány k mnoha existujícím bankovním systémům.

Transakce

Zákazník posílá pomocí e-mailu či webového rozhraní platební instrukce na platební server. BIPS server překládá instrukce do bankovních platebních transakcí. Tyto instrukce posílá přes finanční síť příslušnému bankovnímu systému. BIPS používa k autentizaci veřejné klíče. Klíče se používají jak na vytváření podpisů, tak k šifrování citlivých dat. Každá instrukční zpráva je digitálně podepsána odesílatelem a zahrnuje odesílatelův certifikát a unikátní transakční identifikátor. Podpisy jsou kódovány jako ASCII znaky. Na vyšší úrovni je platební instrukce podobná elektronickému šeku, a to tak, že je digitálně podepsána plátcem, ale v tomto případě je přímo poslána do jeho banky místo příjemci.

1.2.6 Network payment protocol (NPP)

NPP platební protokol je postaven na BIPS protokolu. Ke skrytí částí NPP zpráv je možno použít symetrického šifrování.

Transakce

Klient nakupuje na internetových stránkách (e-shopu) obchodníka. Po vložení zboží do košíku dojde až k platbě. Elektronická peněženka detekuje platební stránku obchodníka. Elektronická peněženka, nainstalována u klienta, čte dále informace o transakci. Peněženka pak požádá o zaslání autentizačních informací. Tento požadavek odešle na SPA server do banky zákazníka. Server banky zákazníka porovná autentizační informace o zákazníkovi s informacemi uloženými ve své databázi. Když je vše v pořádku vygeneruje se unikátní autorizační token a ten je zaslán peněžence klienta. Peněženka předá token serveru obchodníka. Obchodník odešle autorizační požadavek spolu s AAV do své banky. Banka obchodníka posílá autorizační požadavek a token do banky zákazníka. Po úspěšné autorizaci je nákup dokončen. Obchodník potvrdí transakci a dodá bankovní doklad zákazníkovi.

1.2.7 Homebanking computer interface (HBCI)

Přenos dat v HBCI je prováděn pomocí síťového rozhraní. HBCI zpráva se skládá z hlavičky, podpisové hlavičky, jednoho či více obchodních segmentů, podpisového traileru a traileru samotné zprávy. Pro verifikaci a šifrování používá RSA. Dále je potřeba heslo uživatele pro přístup do bankovního systému. Každý klient má svůj elektronický podpis. Pracuje se dvěma klíči, soukromým a veřejným. Soukromý klíč je uložen na uživatelově PC. Banka pak používá veřejný klíč uživatele k jeho autentizaci a kontrole jeho podpisu.

1.3 Internetové platební systémy

1.3.1 Nejpoužívanější internetové platební systémy

Internetové platební systémy jsou v podstatě virtuální peněženky. Těmito systémy je možno na internetu platit a také platby přijímat. Jde o velmi levné, rychlé a ve většině případů i spolehlivé transakce. Samozřejmostí jsou platby na mezinárodní úrovni. Peníze je možno posílat mezi libovolnými účty a bankami, ať už jde o české či cizí. Velkou výhodou je, že účty v internetových systémech lze zakládat zdarma a i jejich vedení je zdarma. Z tohoto důvodu je pro klienta finančně i časově dostupné mít internetových účtů více. Systémy samotné jsou relativně bezpečné, především

proto, že na ně bylo spácháno už mnoho útoků a proto se tyto systémy neustále zdokonalují, nicméně je velice nevhodné nechávat na těchto internetových účtech uložené velké částky a už vůbec ne celoživotní úspory, protože tyto systémy mohou stejně jako bankovní domy zkrachovat.

PayPal

Jde o nejrozšířenější transakčně-platební systém na světě, používaný ve velkém množství e-shopů. Je dostupný i uživatelům v ČR, nicméně uživatelské rozhraní český jazyk nepodporuje. PayPal se vyznačuje jednoduchostí registrace i používáním uživatelského účtu. Zřízení účtu je zdarma, stejně tak i vedení účtu, poplatky za transakce jsou nízké. U PayPalu nelze převádět peníze na cizí účty. PayPal účet je prakticky nezbytný pro uživatele, kteří chtějí nakupovat na eBay.com. Velkou výhodou je rychlost a to, že s obdrženými prostředky lze ihned disponovat.

PayPay

PayPay nabízí stejné funkce jako PayPal, nicméně nabízí o něco širší možnosti použití. Má složitější způsob registrace, ověřuje e-mailovou adresu a číslo mobilního telefonu. PayPay umožňuje platit, ale i žádat peníze. Chybí možnost využití pro dary. Existuje desktopová aplikace PayPay Desktop.

MoneyBookers

Nezbytnou součástí registrace do systému MoneyBookers je vyplnění sady údajů, celá registrace je zdlouhavá, povinné jsou i otázky, které jsou pro internetové platby naprosto zbytečné. Aktivace účtu je prostřednictvím internetu. Stránku MoneyBookers lze sice přepnout do českého jazyka, ale překlad je značně nezdařilý. MoneyBookers si za vklad peněz pomocí karty nárokuje poplatek ve výši 1,9% částky.

PaySec

PaySec je český systém, jde spíše o elektronickou peněženku, než o systém pro online platby. Nabití peněz na účet lze realizovat převodem z bankovního účtu nebo platební kartou. Nabití platební kartou je však doprovázeno poplatkem ve výši 2 % vložené částky. Výhodou PaySecu je jeho rozšířenost v ČR.

1.4 Závěrečné zhodnocení elektronických platebních protokolů

1.4.1 Použitelnost

Výše uvedené protokoly nejsou schopny vzájemné spolupráce. Žádný z nich nevyužívá univerzální rámec, který by se dal aplikovat na všechny typy platební transakce. Každý protokol se specializuje jen na svůj přesný scénář platební transakce.

Některé platební protokoly (SET, 3D-Secure) vyžadují vlastnictví kreditní karty a nelze tak k penězům přistupovat jen na základě autentizace jejich komunikátoru/certifikátu. Žádný z těchto protokolů není schopen zajistit všechny druhy placení za zboží, jako například koupě elektronické jízdenky přímo na zastávce, koupě limonády v automatu, internetový nákup v e-shopu, nákup v kamenné prodejně či převod prostředků z účtu na účet.

Internetové systémy (PayPay, PayPal, atd.) jsou schopny práce výhradně prostřednictvím internetu a online e-shopingu. Navíc je potřeba registrace klienta do jejich systému.

1.4.2 Bezpečnost

Bezpečnosti je v nyní používaných protokolech dosáhnuto pomocí šifrování zpráv, a to za pomoci veřejných klíčů. Veřejné klíče používají digitální certifikáty. Digitální certifikáty bývají obsaženy na všech zařízeních, které jsou součástí platební transakce.

Platební protokoly využívající kreditní karty (SET a 3D-Secure) nesou vždy riziko zneužití karet. Zvláště v protokolu SET jsou pak údaje z kreditní karty předávány přímo obchodníkovi, což je nežádoucí.

Používanou metodou pro šifrování zpráv je 1024-bitový RSA. Podle samotných tvůrců by prolomení takovéto asymetrické šifry vyžadovalo vysoké výpočetní operace a i tak by dešifrování trvalo i 100 let. Dále protokoly využívají jako symetrickou šifru 56-bitový DES, nicméně tato šifra je použita jen pro zabezpečení méně důležitých dat.

2 SYSTÉMY TYPU AAA A PROTOKOL ACP

2.1 Systémy typu AAA

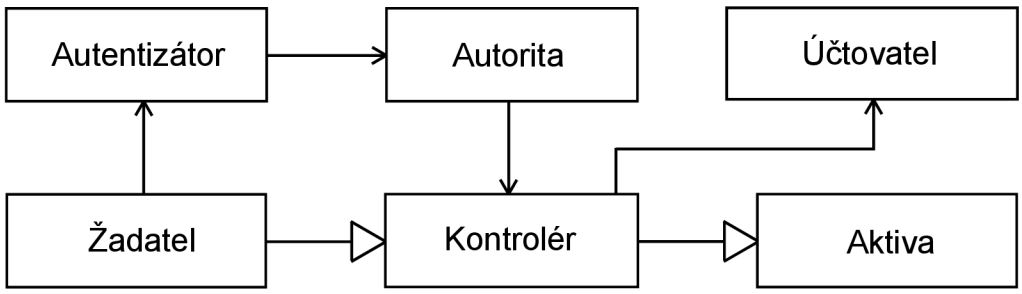
2.1.1 Základní princip AAA

Zkratka AAA pochází z anglických slov Authentication, Authorization a Accounting, což znamená autentizace, autorizace a účtování. Hlavním účelem systému AAA je zajištění řízení přístupu uživatelů sítě k prostředkům sítě a vedení záznamů o těchto přístupech. Tyto prostředky se nazývají aktiva (zařízení sítě nebo poskytované služby).

V systémech AAA je přístup založen na identitě uživatele. Každý uživatel má přiřazenou jedinečnou identitu a jsou mu dána přístupová práva.

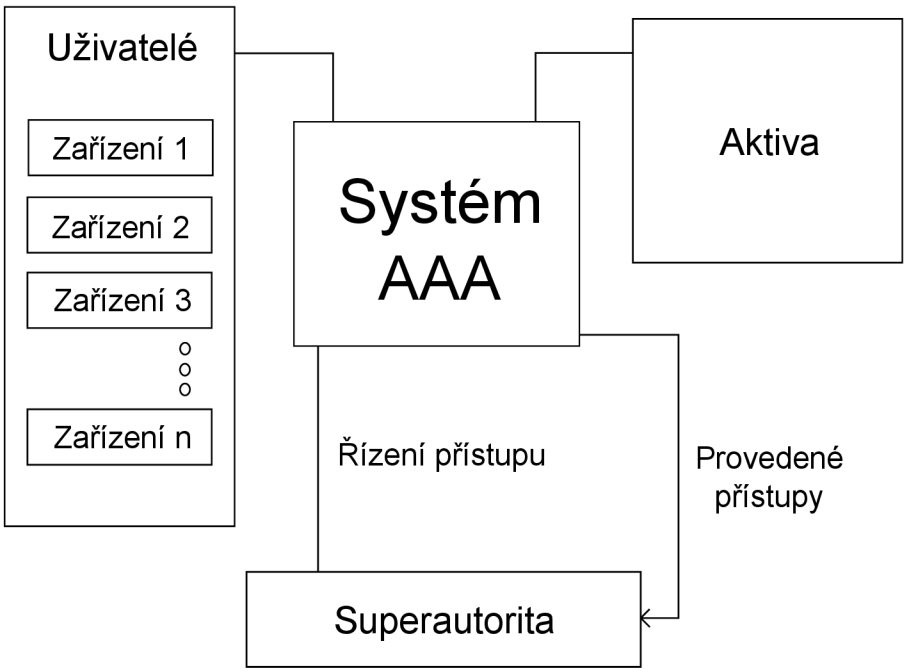
V systému AAA lze definovat tyto základní entity (obr. 2.1):

- Žadatel - zajišťuje řízení systému AAA
- Kontrolér - řídí přístup uživatele k aktivům
- Autentizátor - provádí ověření identity žadatele
- Autorita - rozhoduje o přístupu k aktivům
- Účtovatel - vede záznamy o přístupech k aktivům



Obr. 2.1: Základní entity v AAA

Systém AAA funguje tak, že uživatel zažádá o přístup k aktivům, poté proběhne autentizace, kde mezi sebou komunikují žadatel a autentizátor. Výsledek autentizace je pak předán autoritě. Pokud je autentizace úspěšná, zkontroluje autorita práva uživatele. Na základě práv vytvoří autorita dvě zprávy, nařízení pro kontrolér a oprávnění pro žadatele. Nařízení popisují přístupová práva žadatele. Oprávnění poskytují informace o právech uživatele. Funkce viz obr. 2.2.



Obr. 2.2: Diagram funkce systému AAA

2.1.2 Rozšířenost protokolů AAA

V současné době se využívá hned několik protokolů typu AAA. Jsou to například protokoly RADIUS, Diameter, Open ID a ve firemních systémech například Kerberos. Existuje celá řada systémů pro řízení přístupu, nicméně tyto systémy používají různé komunikační protokoly s různými typy autentizace, tudíž jsou tyto systémy AAA nezastupitelné a nejsou schopny spolupracovat. Tyto systémy mají také různé úrovně zabezpečení.

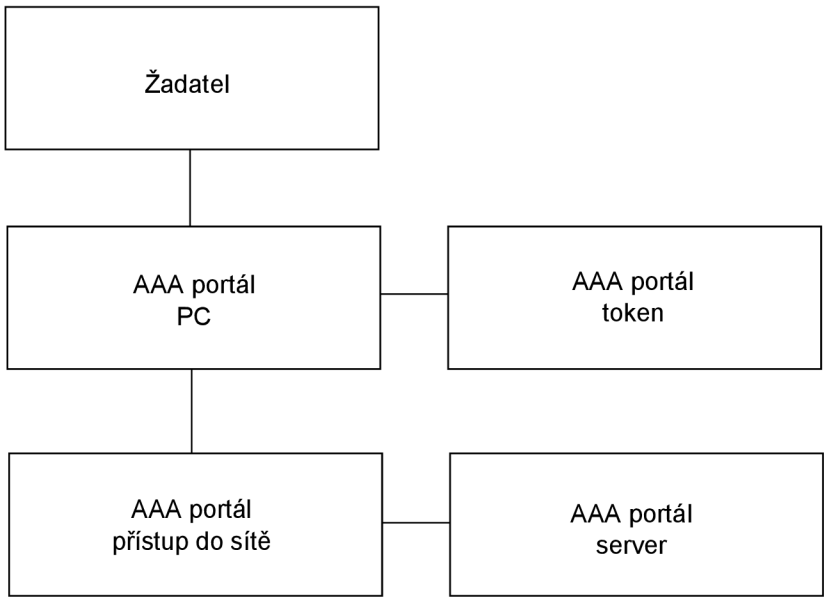
2.1.3 Univerzální rámec systémů AAA

Z hlediska systémů AAA lze rozlišovat tři základní typy prvků:

- Servery - poskytují vzdálené služby uživatelům
- Počítače uživatelů - poskytují možnost využívat lokální služby
- Autentizační zařízení - umožňují uživatelům prokázat svoji identitu

V tomto rozdělení typů prvků jsou aktivem serverů právě poskytované služby, aktivem počítačů jsou důvěrná data a aktivem autentizačních zařízení jsou autentizační faktory uživatele. Pro řízení přístupu k těmto aktivům lze implemetovat autonomní systém AAA do každého z prvků sítě. Tento autonomní systému se nazýva

AAA portál, ten obsahuje všechny prvky systému. Implementace portálu AAA je podstatou pro návrh univerzálního přístupového rámce. Protokol pro řízení přístupu pro komunikaci mezi portály budeme nazývat ACP. Tato zkratka znamená Access Control Protocol, tedy protokol pro řízení přístupu. Grafické zobrazení univerzálního rámce, viz obr. 2.3.



Obr. 2.3: Diagram univerzálního rámce

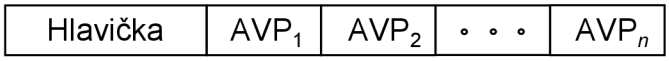
Zprávy protokolu ACP budou přenositelné na jakékoliv vrstvě. Pro vetšinu přenosů ACP bude využit protokol TLS, neboli Transport Layer Security, dále protokol EAPoL, neboli EAP over LAN a také přenos přes USB rozhraní zařízení. TLS protokol využívá autentizaci komunikujících stran založenou na kryptografii a veřejném klíči. TLS umožňuje zabezpečenou komunikaci ACP protokolu mezi systémy AAA. Protokol EAPoL umožňuje přenos autentizačních zpráv při přístupu uživatelů do lokálních sítí. Protokol ACP bude protokolem EAPoL přenositelný právě proto, že oba mají podobný formát zpráv.

2.2 Protokol ACP

Protokol ACP je schopen zajistit komunikaci mezi více uzly a také flexibilní komunikaci pro potřeby systému AAA, tedy pro autentizaci, autorizaci a účtování. Komunikace mezi uzly bude řešena pomocí ad-hoc sítě pro danou transakci. Bezpečné spoje budou zajištěny TLS spoji nebo jinými fyzicky bezpečnými linkami. Celá komunikace bude vyžadovat síťovou adresaci a možnost tranzitování zpráv. Komunikace v rámci ACP bude mít dva hlavní aktéry:

- Iniciátor – uzel, který inicioval (zahájil) transakci, tedy žádající uzel.
- Adresát – uzel, na který je vznášen požadavek.

Iniciátor nejčastěji žádá adresáta o přístup k aktivům, či o provedení autentizace. Adresát mu na základě autentizace přístup umožní či přístup odmítne.



Obr. 2.4: Formát zprávy ACP

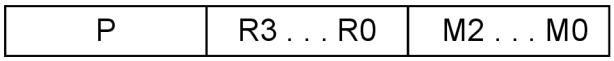
Popis polí ACP:

- Hlavička (7 B)
- AVP (Attribute-Value Pair) – viz obr. 2.7

Obr. 2.5: Formát pole Hlavička

Popis pole Hlavička:

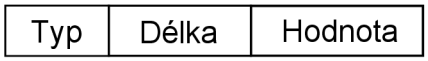
- Kód (1 B)
- Identifikátor (3 B) – unikátní identifikace transakce
- Délka (3 B) – délka celé zprávy v Bytech (oktetech)



Obr. 2.6: Formát pole Kód

Popis pole Kód:

- P (1 b) – P bit (určuje, že jde o ACP)
- R3 ... R0 (4 b) – bity pro budoucí použití, všechny nastaveny na 0
- M2 ... M0 (3 b) – určuje o jaký typ zprávy se jedná



Obr. 2.7: Formát pole AVP

Popis pole AVP:

- Typ (1 B) – Identifikuje typ AVP.
- Délka (2 B) – Pole popisující délku Hodnoty.
- Hodnota (0 až 65535 B) – Pole, popisující příslušnou hodnotu typu AVP.

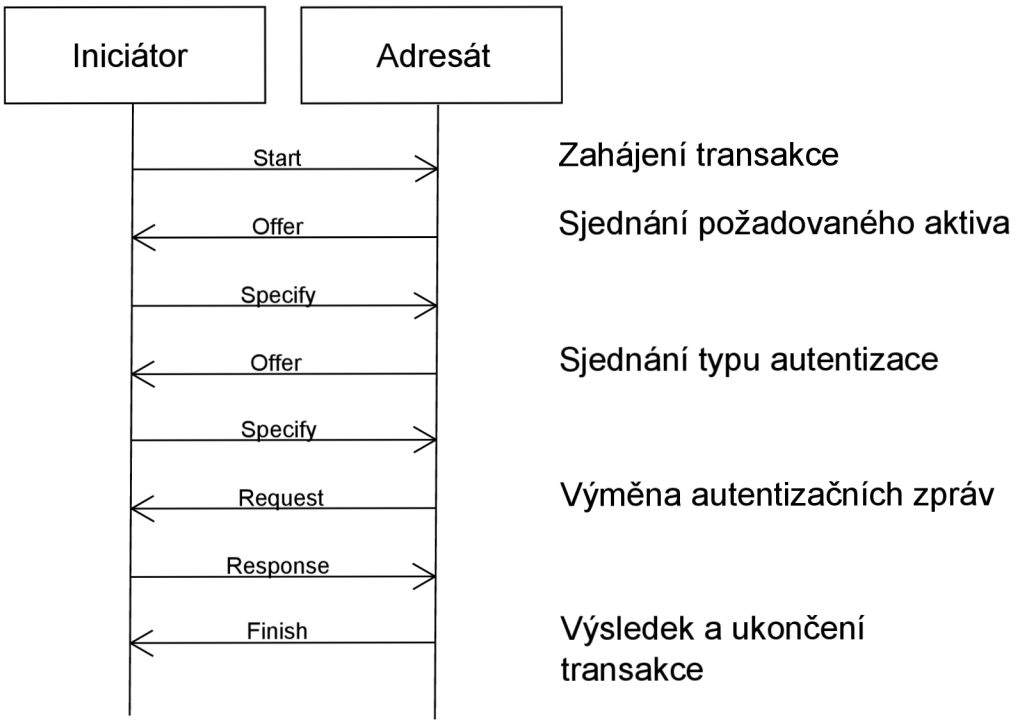
Existují tři typy AVP polí:

- Krátké AVP (SAVP) – Obsahuje data kratší než 2^8 B
- Dlouhé AVP (LAVP) – Obsahuje data kratší než 2^{16} B
- Kontejnerové AVP (CAVP) – Obsahuje jeden nebo více AVP typů

Protokol ACP definuje šest typů zpráv:

- Start – Úvodní zpráva transakce, odesílaná iniciátorem.
- Finish – Zpráva ukončující transakci, odesílaná adresátem.
- Offer – Zpráva obsahující nabídku aktiv, odesílaná adresátem.
- Specify – Reakce na zprávu offer, odesílaná adresátem.
- Request – Zpráva odesílaná adresátem v rámci autentizace.
- Response – Zpráva odesílaná iniciátorem v rámci autentizace.

Schéma základní transakce protokolu ACP je zobrazeno na obr. 2.8.



Obr. 2.8: Základní transakce ACP

3 SPECIFIKACE A SCÉNÁŘE UŽITÍ PROTOKOLU ACP

3.1 Diskuze cílů vývoje nového systému

Hlavním cílem nového systému by mělo být vytvoření univerzálního rámce pro práci ve všech dnes užívaných scénářích pro platební transakce. Tak abychom pomocí jednoho protokolu/systému byli schopni zajistit jak mikroplatby, tak i převody větších sum. Systém by měl zajistit univerzálnost a umožnit jak platby v kamenném obchodě, tak i online nákupy v e-shopu a mikroplatby, jako například koupě parkovného přímo na parkovišti. Nový systém by měl být schopen zastoupit všechny systémy, které jsou doposud používané a měl by být schopen je nahradit.

Nový elektronický platební systém, používající protokol ACP by měl být schopen pracovat na každém zařízení, na které se vhodně naimplementuje AAA portál, podporující zprávy ACP. Takovýto portál by mohl být vhodně implementován například softwarovou aplikací, nebo přímo do internetového prohlížeče. Nový systém by měl zajišťovat interoperabilitu, tudíž by měl být schopen pracovat na jakémkoliv zařízení bez ohledu na použitý operační systém (Windows, Linux, Mac OS, atd.). Systém by měl být bezpečný a to tak, aby nemohlo dojít k ohrožení aktiva. Vhodné by bylo vést každou transakci zabezpečeným TLS spojením. Kanál TLS by mohl být použit i k samotné autentizaci. Takovýto způsob by vyžadoval vlastnictví certifikátů na obou stranách komunikace. Bezpečnost systému by měla být zajištěna nejenom s ohledem na možné nositele hrozby, ale také proti pádu systému samotného. Z toho plyne, že celý systém musí být atomický (buď se vyřídí celá transakce nebo nic). Konkrétně u elektronického šeku by mohla být obsažena doba platnosti. Při pádu systému by byly peníze blokovány jen do doby (zvolená doby platnosti šeku), než by vypršela platnost šeku. Pak by je měl mít zákazník opět k dispozici.

3.2 Diskuze anonymity plateb

Nakupování fyzicky (přímo v kamenné prodejně) umožňuje nakupování anonymně. Je přirozené, že většina zákazníků vyžaduje anonymitu i při elektronickém obchodování. Proto by měl nový systém zachovat tyto požadavky. Už jen proto, že ne každý ze subjektů transakce musí vědět o všech prvcích dané komunikace.

V elektronických platebních systémech nemusí každý ze subjektů transakce vědět o všech prvcích komunikace. Vhodné by bylo, aby každý subjekt komunikace znal jen ta data, která skutečně potřebuje k tomu, aby byl dokončen převod peněz, takže aby obchodník dostal zaplaceno a zákazník dostal službu, kterou si zaplatil. Mělo

by být samozřejmostí utajení obsahu celé transakce subjektům, které se transakce vůbec neúčastní. V nejlepším případě by vůbec neměli o transakci vědět.

V následujícím textu je shrnuto (v závislosti na daném subjektu transakce), které informace jsou pro daný subjekt důležité, a které jsou naopak nežádoucí. Tato diskuze neuvažuje právní nařízení pro elektronické transakce, zabývá se čistě anonymitou každého účastníka transakce, jakožto prvkem proti zneužití informací komunikujících stran.

Základní subjekty elektronické transakce:

- Zákazník
- Obchodník
- Banka zákazníka
- Banka obchodníka

Z pohledu zákazníka: Zákazník tvoří v elektronické transakci žadatele o službu, kterou mu poskytuje obchodník. Zákazník musí vědět, kam posílá své peníze (číslo účtu obchodníka) a jakou částku posílá. Na konci transakce by měl dostat potvrzení o úspěšnosti transakce. Není nutné, aby znal obsah komunikace, kterou si mezi sebou posílají banka zákazníka a obchodníka.

Z pohledu obchodníka: Obchodník tvoří v transakci poskytovatele služby. Obchodníka v tomto případě zajímá odměna za jeho služby, tedy finanční vyrovnání. Obchodník musí obdžet potvrzení o výsledku transakce. Obchodník by neměl znát identitu zákazníka, nemusí tedy vědět komu službu prodává. V případě jedné větší objednávky, která se rozdělí mezi jednotlivé subzákazníky, by obchodník neměl znát ani množství služby, které připadá jednotlivému subzákazníkovi. Obchodník nesmí znát obsah komunikace, která probíhá mezi zákazníkem a bankou zákazníka. V případě, že by znal obsah této komunikace, by celá autentizace téměř postrádala význam. Obchodník by se pak mohl volně vydávat za zákazníka a manipulovat s jeho aktivy.

Z pohledu banky zákazníka: Banka zákazníka tvoří v transakci autentizační server, tudíž si musí ověřit identitu zákazníka (tedy svého klienta). Na základě autentizace zná banka číslo účtu zákazníka a ví odkud peníze čerpat a jakou částku posílá. Musí také znát číslo účtu obchodníka, aby věděla, kam prostředky poslat.

Z pohledu banky obchodníka: Banka obchodníka musí znát číslo účtu obchodníka (tedy svého klienta) a částku, která mu bude na účet připsána. Banka

obchodníka nesmí znát obsah komunikace, která probíhá mezi zákazníkem a bankou zákazníka. Z toho plyne, že nemusí znát ani identitu zákazníka.

3.3 Specifikace navrhovaného systému

Navrhovaný systém bude používat ochranu TLS spojením, dále pak certifikaci veřejným klíčem. Navrhovaný systém bude používat AAA portály na každém zařízení. AAA portál na zařízení může být řešen pomocí softwarové (dále již SW) aplikace nebo může být implementován přímo do internetového prohlížeče, kde bude komunikovat prostřednictvím protokolu http/https. Systém by měl být schopen pracovat na libovolném hardwarovém zařízení (dále již HW) (smartphone, PC, tablet, server, atd.), které obsahuje AAA portál. SW portál na zařízení by měl umět pracovat s NFC (Near Field Comunication) a také s QR kódy. Tato funkce by zlepšila použitelnost celého systému, zejména by klientovi systému usnadnila práci.

3.3.1 Kritéria ideálního systému

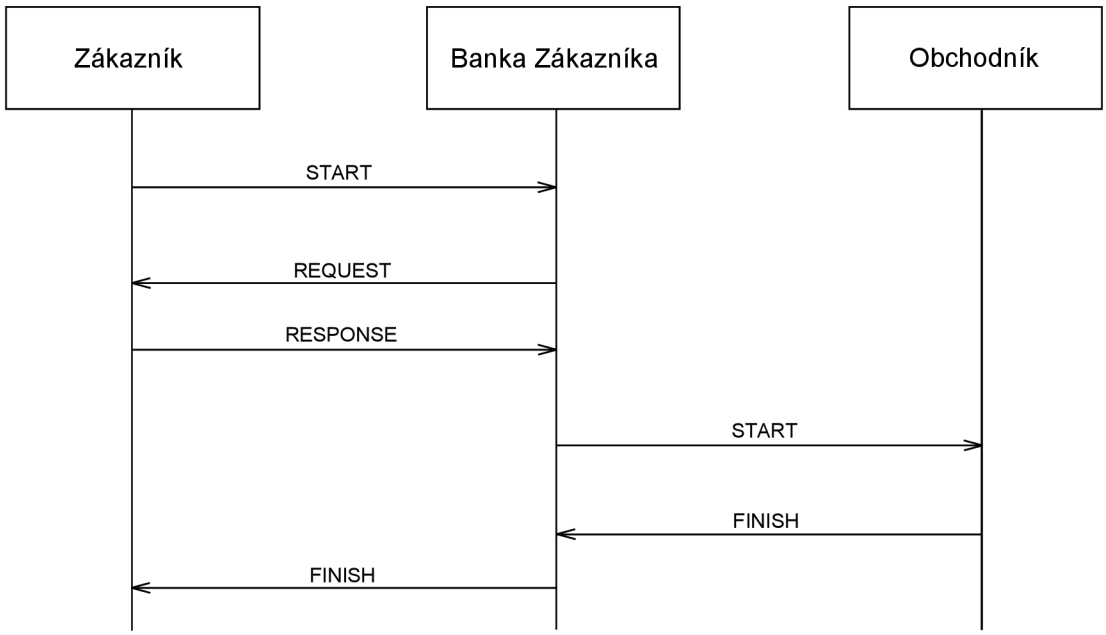
- Elektronická transakce v ideálním systému by měla proběhnout okamžitě.
- Systém by měl být schopný odolat jakékoliv hrozbě.
- Transakce by měly být utajené všem subjektům, které se neúčastní komunikace/transakce.
- Systém by měl být přenositelný na jakékoliv HW zařízení.
- Systém by měl být přenositelný na jakýkoliv operační systém.
- SW implementace by měla být nainstalována již v samotném operačním systému.
- Systém by měl být nepřetržitě dostupný.
- Aplikace by měla být jednoduše ovladatelná (intuitivní) i pro uživatele, který nemá zkušenosti s používáním podobných způsobů platby.
- Systém musí provést transakci atomicky, to znamená, že se transakce musí úspěšně zdařit ve všech bodech komunikace.

3.3.2 Kritéria reálného systému

- Elektronická transakce by měla proběhnout nejlépe v řádech stovek milisekund.
- Systém by měl být schopný odolat jakékoliv hrozbě. Minimálně však všem doposud známým typům útoku.
- Pokud by se nepodařilo utajit komunikaci při probíhající transakci, měla by být komunikace vhodně šifrována, aby třetí strana nezaznamenala nic jiného než spoustu nic neříkajících symbolů.
- Systém by měl být přenositelný na jakékoliv HW zařízení.
- Systém by měl být přenositelný na jakýkoliv operační systém.
- Instalace SW implementace by měla být jednoduchá a měla by nás sama navést (tzn. i bez předchozích zkušeností s instalací).
- Systém by měl být nepřetržitě dostupný.
- Aplikace by měla být jednoduše ovladatelná (intuitivní) i pro uživatele, který nemá zkušenosti s používáním podobných způsobů platby.
- Systém musí provést transakci atomicky, to znamená, že se transakce musí úspěšně zdařit ve všech bodech komunikace. V případě nějakého problému musí být vše zabezpečeno tak, aby žádná strana transakce nebyla poškozena.

3.4 Scénář zajišťující mikroplatbu

3.4.1 Základní schéma transakce



Obr. 3.1: Průběh mikroplatby

3.4.2 Popis transakce

V tomto scénáři budeme uvažovat zákazníka, který si bude kupovat například kafe z automatu. Zákazník v tomto scénáři disponuje chytrým komunikačním zařízením (smartphone, tablet). Zákazník má od své banky přiděleny dva soukromé klíče a to ZB pro komunikaci mezi zákazníkem a bankou a AZB pro autentizaci zákazníka u banky. Objednávka zákazníka bude v tomto případě zadána pevně, to znamená, že v ní bude přímo uvedeno co objednává v podobě kódu zboží, který bude znát zákazníkova banka.

Zákazník nejprve přijde k automatu, který disponuje technologií IEEE 802.11 podporující pouze zprávy typu ACP. Připojí se svým zařízením na tento automat a smartphonem vyfotí QR kód přidělený k danému druhu kávy. ACP portál na jeho zařízení může být řešen SW aplikací. Tato aplikace vyhodnotí QR kód.

Následně probíhá komunikace ACP takto:

1. Zákazník posílá zprávu START obsahující identifikátor banky, identifikátor zákazníka a typ požadovaného aktiva.
2. Portál banky zjistí podle identifikátoru zákazníka klíče ZB a AZB.
3. Portál banky v tuto chvíli provede autentizaci a to tak, že zašle zákazníkovi zprávu REQUEST, která obsahuje typ zvoleného aktiva + náhodné číslo.
4. Zákazník zkontroluje aktivum a pomocí klíče AZB zašifruje hodnotu aktiva a náhodného čísla. Tento řetězec posílá bance jako zprávu RESPONSE.
5. Banka provede stejný výpočet jako zákazník a zkontroluje hodnotu výpočtu s výpočtem obdrženým od zákazníka. Pokud se hodnoty shodují, je autentizace úspěšná.
6. Portál banky naváže komunikaci s portálem obchodníka, tato komunikace bude probíhat v trvalém spojení TLS, tudíž už je komunikace autentizovaná. Banka tedy posílá zprávu START, která obsahuje typ požadovaného aktiva.
7. Portál obchodníka posílá zprávu FINISH, která obsahuje dané aktivum, což bude jednorázový kód, který zákazník vloží klávesnicí do automatu, za což obdrží své kafe.
8. Portál banky kód zašifruje klíčem AZ a ve zprávě FINISH jej odešle portálu zákazníka.
9. Komunikátor zprávu klíčem AZ dešifruje a zákazník zadá kód do automatu.
10. Banka zákazníka pošle danou částku na účet obchodníka hned při dalším zúčtovacím obdobím.

3.4.3 Datové/časové nároky

Celkem bude odesláno šest ACP zpráv.

Pro zprávy budou zvoleny tyto typy AVP:

START	NAME_PRO_G, NAME_SUP_L, ASSET_L
REQUEST	ASSET_L, INIT
RESPONSE	HMAC
START	ASSET_L
FINISH	PROVE
FINISH	ENC

Všechny zprávy budou obsahovat hlavičku – 6 krát 56 b, celkem 336 b.

Zpráva START bude obsahovat identifikátor zákazníka a banky, což bude číslo zákazníkova účtu a kód banky, tedy 10 + 4 číslice – do 50b, dále kód aktiva, což

bude osmimístné číslo, tedy do 32 b.

Zpráva REQUEST bude obsahovat kód aktiva, což bude osmimístné číslo, tedy do 32 b a náhodné číslo o velikosti 256 b.

Zpráva RESPONSE bude obsahovat zašifrovaný řetězec o délce 256 b.

Druhá zpráva START bude obsahovat kód aktiva, což bude osmimístné číslo, tedy do 32 b.

Zpráva FINISH bude obsahovat aktivum, velikost 256 b.

Druhá zpráva FINISH bude obsahovat zašifrované aktivum, velikost 256 b.

Velikosti zpráv jsou jen orientační a celkově bude transakce vyměňovat okolo 1500 b.

Při rychlosti 8 kb/s by měla celá transakce proběhnout do 200 ms.

Hodnota 200 ms je hrubý odhad a i kdyby se doba transakce nějakým způsobem vyšplhala až na 1 sekundu, tak zákazník by stejně neměl šanci tuto dobu poznat.

3.4.4 Praktická použitelnost

Tento scénář je možno aplikovat na různé druhy menších plateb. Scénář je popsán pro platbu kafe z automatu, ale mohl by se uplatnit i na platbu parkovného, platbu jízdenky MHD nebo na jakoukoliv jinou platbu převádějící malý finanční obnos.

3.4.5 Bezpečnost

Bezpečnost komunikace mezi bankou a zákazníkem je řešena použitím šifrování soukromým klíčem. Šifrování provede banka i zákazník a následně jsou obě hodnoty bankou porovnány.

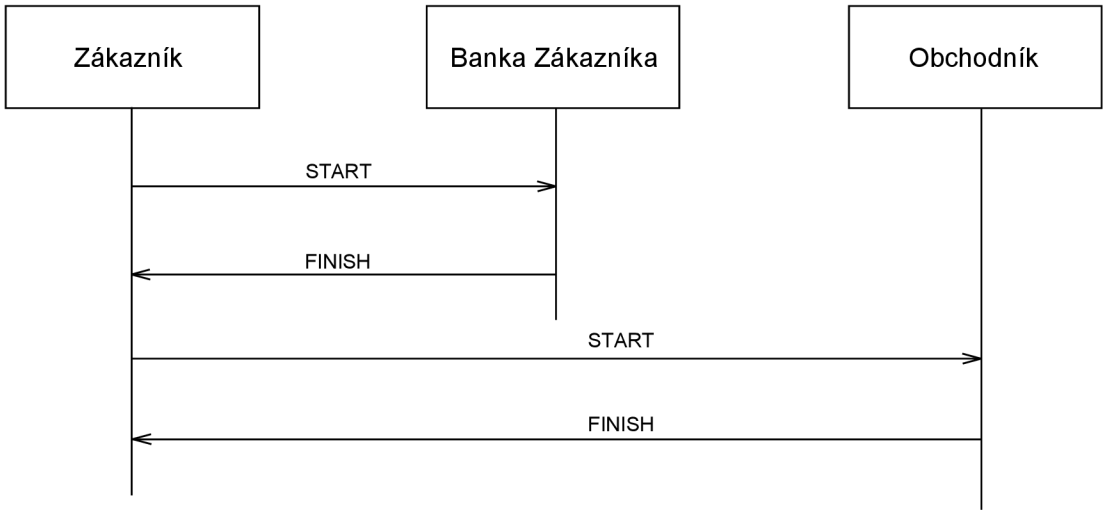
Komunikace mezi bankou zákazníka a obchodníkem probíhají v zabezpečeném TLS kanále. Celé toto zabezpečení naprosto dostačuje při použití scénáře na převod mikroplateb.

3.4.6 Porovnání s doposud používanými protokoly

Tento scénář narozdíl od jiných protokolů pro elektronické transakce nevyžaduje po zákazníkovi vlastnictví kreditní/debetní karty. Jeho zabezpečení je úměrné velikosti placené částky. Transakce je rychlá a dá se použít podstatně univerzálněji, než umožňují ostatní protokoly.

3.5 Scénář platby online

3.5.1 Popis transakce



Obr. 3.2: Průběh online platby

Scénář uvažuje zákazníka, který vlastní chytré mobilní komunikační zařízení, nebo přímo PC. ACP portál na zařízení může být implementován přímo do webového prohlížeče. Zákazník si nejprve vybere své zboží na internetových stránkách e-shopu obchodníka. Obchodník zákazníkovi zašle fakturu prostřednictvím jeho webových stránek (například pomocí https).

Následně probíhá komunikace ACP takto:

1. Autentizace zákazníka proběhne už v samotném navázání spojení a to tak, že se mezi zákazníkem a bankou zákazníka vytvoří bezpečný TLS kanál, ke kterému jsou zapotřebí soukromé šifrovací klíče zákazníka. Od teď už celá komunikace beží šifrovaně.
2. Zákazník posílá zprávu START obsahující jedinečné ID transakce, které zákazníkovi vygeneruje jeho implementace ACP portálu, dále číslo bankovního účtu obchodníka a danou částku, jakožto typ požadovaného aktiva.
3. Banka zákazníka už autentizovala zákazníka a tak přejde k autorizaci a následně pošle elektronický šek. Tím je ukončena komunikace mezi bankou a zákazníkem.
4. V tomto bodě se naváže další TLS kanál, tentokrát mezi zákazníkem a obchodníkem a celá další komunikace již probíhá šifrovaně.

5. Zákazník pošlě elektronický šek obchodníkovi.
6. Obchodník zkontroluje údaje a podpis banky.
7. Pokud je vše v pořádku, pošle obchodník potvrzení o přijetí platby zákazníkovi a zboží je mu následně posláno například poštou.

Elektronický šek je tvořen unikátním ID šeku přiděleného bankou, která šek vydala. Šek obsahuje účet zákazníka, účet obchodníka, danou částku a měnu. Dále je opatřen digitálním podpisem dle ITU X.509.

Potvrzení o přijetí platby je realizováno několika znaky. V podstatě se jedná o větu, že vše proběhlo v pořádku.

3.5.2 Praktická použitelnost

Tento typ scénáře je možno uplatnit na různé online nákupy prostřednictvím e-shopu. Obchodník obdrží za svou službu elektronický šek, který má stejnou funkci jako papírový šek. Šek si pak vyzvedne ve své bance. Protože při tomto scénáři může být převáděno větších sum, bude šek obsahovat i číslo účtu obchodníka, aby nemohl šek vybrat nikdo jiný. Šek by měl obsahovat číslo účtu obchodníká plus číslo účtu zákazníka, identifikátor šeku pro znemožnění dvojtého vybrání šeku a částku. Částka a účet obchodníka musí být viditelné obchodníkovi, aby se z účtu dozvěděl, zda má obdržet správnou částku. Účet zákazníka by měl být bankou zákazníka zašifrovaný, aby jej mohla dešifrovat jen banka obchodníka pomocí jejího soukromého klíče.

3.5.3 Datové/časové nároky

Celkem budou odeslány dvě ACP zprávy START a dvě zprávy FINISH.

Pro zprávy budou zvoleny tyto typy AVP:

START	NAME_PRO_G, NAME_SUP_L, ASSET_L
FINISH	SIG
START	SIG
FINISH	AVP RESULT

Všechny zprávy budou obsahovat hlavičku – 4 krát 56 b, celkem 224 b.

Zpráva START bude obsahovat číslo účtu obchodníka, tedy 10 + 4 číslice – do 50b, dále částku, což může být až šestimístné číslo s desetinou čárkou, tedy do 32 b + měna (do 20b,).

Zpráva FINISH bude obsahovat šek s podpisem banky, velikost 512 b.

Druhá zpráva START bude obsahovat také šek s podpisem banky, velikost 512 b.

Zpráva FINISH bude obsahovat potvrzení o platbě, v podstatě několik znaků, velikost až 256 b.

Velikosti zpráv jsou jen orientační a celkově bude transakce vyměňovat okolo 1600 b.

Při rychlosti 8 kb/s by měla transakce proběhnout do 210 ms. Je potřeba přičíst navázání dvou TLS spojení, takže zhruba dvakrát 70 ms

Celkově se tedy dostáváme na hodnotu zhruba 350 ms. Hodnota 350 ms je hrubý odhad a i kdyby se doba transakce nějakým způsobem vyšplhala až na 1 sekundu, tak zákazník by stejně neměl šanci tuto dobu poznat.

3.5.4 Bezpečnost

Prakticky celá ACP komunikace probíhá prostřednictvím zabezpečeného TLS spojení, takže se dá považovat za dostatečně zabezpečenou i pro převody vyšších částek.

3.5.5 Porovnání s doposud používanými protokoly

Tento scénář narozdíl od jiných protokolů pro elektronické transakce také nevyžaduje po zákazníkovi vlastnictví kreditní/debetní karty. Transakce je rychlá i při navazování TLS spojení a scénář jde použít univerzálně pro všechny typy internetového obchodování.

4 ZÁVĚR

V první kapitole jsem nejprve provedl analýzu protokolů, které zajišťují elektronické platební transakce. Z analýzy se dá vyvodit, že nyní používané protokoly pro elektronické platební transakce nejsou schopny vzájemné spolupráce a jsou vzájemně nezastupitelné. Navíc mají rozdílnou úroveň zabezpečení.

V druhé kapitole jsem vytvořil teoretický úvod, který rozebírá funkci systémů AAA. Dále jsou zde popsány jednotlivé entity systémů AAA a je zde rozebrán protokol ACP. V kapitole jsou dále obsaženy jednotlivé pole rámce ACP s popisem jejich významu a typy zpráv ACP.

V třetí části jsou popsány cíle vývoje nového systému s co nejvyšší mírou interoperability a bezpečnosti. Tato část pojednává o vytvoření univerzálího rámce, který by se dal použít na všechny typy platebního styku. Dále jsou zde specifikovány parametry jak ideálního, tak reálného systému pro platby pomocí ACP

Dále jsou ve třetí části uvedeny základní scénáře platební transakce s použití ACP a to konkrétně scénář pro mikroplatby a scénář pro online nákupy. Podařilo se vytvořit scénáře, které jsou zabezpečeny pomocí TLS nebo použitím soukromých klíčů.

Protokol ACP vznikl s potřebou po univerzálním přístupovém rámci, který by byl schopen funkce komunikace prakticky na každém harwarovém i softwarovém zařízení, obsahující AAA portál. Scénáře byly vypracovány s ohledem na rychlost a bezpečnost komunikace.

Platební systémy využívající protokol ACP a protokol samotný má podle mě své opodstatnění a to hlavně co se týče univerzálnosti použití. Myslím, že protokol ACP přináší výhody a věřím, že v praxi by se dočkal svého uplatnění, zvláště, pokud by se podařilo zajistit kompatibilitu systému na jakémkoliv zařízení obsahující ACP portál.

LITERATURA

[1] BURDA, K.; STRAŠIL, I.; PELKA, T.; STANČÍK, P. *Access Control Protocol (ACP); Access Control Protocol (ACP). RFC draft.* Dostupné z URL: <http://tools.ietf.org/html/draft-kaaps-acp-01>.

[2] BURDA, K. *Univerzální rámec pro řízení přístupu v počítačových sítích. Elektrorevue - Internetový časopis* 2011, roč. 2011, č. 9, s. 1-6. ISSN: 1213-1539 Dostupné z URL: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/univerzalni-ramec-pro-rizeni-pristupu-v-pocitacovych-sitich/>.

[3] BURDA, K.; LEŽÁK, P. *Aplikace univerzálního rámce řízení přístupu. Elektrorevue - Internetový časopis,* 2012, roč. 2012, č. 28, s. 1-5. ISSN: 1213-1539 Dostupné z URL: <http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/35/aplikace-univerzalniho-ramce-rizeni-pristupu/>.

[4] BURDA, K. *AAA systémy a protokoly. Elektrorevue - Internetový časopis,* 2009. ISSN: 1213-1539 Dostupné z URL: <http://www.elektrorevue.cz/cz/clanky/informacni-technologie/25/aaa-systemy-a-protokoly-1/>.

[5] ČÍKA, P. *Protokol pro zabezpečení elektronických transakcí - SET. Elektrorevue - Internetový časopis,* 2006, roč. 2006, č. 45, s. 1 (s.) ISSN: 1213-1539 Dostupné z URL: <http://www.elektrorevue.cz/clanky/06045/index.html>.

[6] Hsiao-Cheng Yu; Kuo-Hua Hsi; Pei-Jen Kuo. *Electronic payment systems: an analysis and comparison of types,* 2002, Volume 24, Issue 3, Pages 331-347. ISSN: 0160-791X Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S0160791X0200012X>.

[7] Gritzalis, S.; Spinellis, D.; Georgiadis, P. *Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification, Computer Communications,* 1999, Volume 22, Issue 8, Pages 697-709. ISSN: 0160-791X Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S0140366499000304>.

[8] LYBACK, D. *Agent Trade Servers in Financial Exchange Systems,* 2004, Volume 4, Issue 3, Pages 329-339. Dostupné z URL: <http://dl.acm.org/citation.cfm?id=1013206>.

[9] Rathour, S. *Review of 3-D Secure Protocol,* 2013, Volume 1, Issue 8. ISSN: 2319-6386 Dostupné z URL: <http://dl.acm.org/citation.cfm?id=1013206>.

[10] Lu, S.; Smolka, S.A., *Model checking the secure electronic transaction (SET) protocol,* 1999. Dostupné z URL: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=805074&tag=1>.

[11] BURDA, K.; STRAŠIL, I. *Zabezpečovací systémy. Brno: Vysoké učení technické v Brně,* 2012. s. 1-187. ISBN: 978-80-214-4441-6.

[12] *Protokoly pro elektronické platební systémy.* In: [online]. [cit. 2014-01-02].

Dostupné z URL: <http://www.security-portal.cz/clanky/protokoly-pro-elektronické-platební-systémy>.

[13] PIJÁK, Michal. *Elektronické platební systémy.* 2003. Diplomová práce. Masarykova univerzita v Brně. Dostupné z URL: <http://www.fi.muni.cz/usr/staudek/vyuka/security/e_payment/index.html#2-4-4>.

[14] SLABÝ, P. *Implementace technologie SET.* 2000. Diplomová práce. České vysoké učení technické. Dostupné z URL: <http://www1.fs.cvut.cz/cz/u12110/set-demo/Diplomka.htm>.

[15] WAIC, V. *Srovnání internetových platebních systémů.* In: [online]. [cit. 2014-01-02]. Dostupné z URL: <http://www.zive.cz/clanky/srovnani-internetovych-platebnich-systemu/mpenize-a-prekvapivy-vitez/sc-3-a-144190-ch-63058/default.aspx#articleStart>.

[16] Internetové platební systémy - Paypal, Paypay, MoneyBookers a další. In: [online]. [cit. 2014-01-02].

Dostupné z URL: <http://penize.org/internetove/systemy/platebni/>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AAA Authentication, Authorization and Accounting – autentizace, autorizace a účtování

AAV Adeno Associated Virus

ACP Access Control Protocol – protokol pro řízení přístupu

ACS Access Control Server – server pro řízení přístupu

AVP Attribute-Value Pair

BIPS The Bank Internet Payment System

DES Data Encryption Standard – symetrická šifra

EAP Extensible Authentication Protocol – rozšiřitelný autentizační protokol

EAPoL EAP over LAN – EAP přes lokální síť

HBCI Homebanking Computer Interface

HTTP Hypertext Transfer Protokol

LAN Lokal Area Network – lokální síť

NPP Network payment protocol

OFX Open Financial Exchange

PC Personal Computer – osobní počítač

PIN Personal Identification Number

RSA Rivest, Shamir, Adleman – šifra s veřejným klíčem

SET Secure Electronic Transaction – protokol pro zabezpečení elektronických transakcí

SGML Standard Generalized Markup Language

SSL Secure Sockets Layer

TLS Transport Layer Security

XML Extensible Markup Language