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

ELEKTRONICKÉ BANKOVNICTVÍ

E-BANKING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE BRONISLAV VLK
AUTHOR

VEDOUCÍ PRÁCE doc. Ing. VÁCLAV ZEMAN, Ph.D.
SUPERVISOR

BRNO 2008

VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ
Fakulta elektrotechniky
a komunikačních technologií
Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Vlk Bronislav
Ročník: 3

ID: 74617
Akademický rok: 2007/08

NÁZEV TÉMATU:

Elektronické bankovnictví

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a systematicky popište soudobé elektronické bankovní systémy. V práci se zaměřte na vysvětlení principů a na uvedení základních vlastností těchto systémů. Proveďte průzkum a srovnání elektronických bankovních systémů používaných v České republice. Srovnání proveďte z pohledu uživatele i provozovatele.

DOPORUČENÁ LITERATURA:

[1] DOSTÁLEK, L. VOHNOUTOVÁ, M. Velký pruvodce infrastrukturou PKI. Computer Press, Brno 2006, ISBN: 80-251-0828-7
[2] SAVARD, J. G. A Cryptographic Compendium, Press, 2000, available on www.quadibloc.com

Termín zadání: 11.2.2008

Termín odevzdání: 4.6.2008

Vedoucí projektu: doc. Ing. Václav Zeman, Ph.D.

prof. Ing. Kamil Vrba, CSc.
předseda oborové rady

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací

UPOZORNĚNÍ:

LICENČNÍ SMLOUVA

POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bronislav Vlk

Bytem: Stroupežnického 361/13, 79604, Prostějov

Narozen/a (datum a místo): 14.9.1973, Prostějov

(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 60200 Brno 2

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):

   ☐ disertační práce

   ☐ diplomová práce

   ☑ bakalářská práce

   jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP: Elektronické bankovnictví

Vedoucí/školitel VŠKP: doc. Ing. Václav Zeman, Ph.D.

Ústav: Ústav telekomunikací

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

☑ tištěné formě - počet exemplářů 1

☑ elektronické formě - počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

.....	.....
Nabyvatel	Autor

Abstrakt

Název práce:	**Elektronické bankovnictví**
Příjmení a jméno:	**Vlk Bronislav**
Ústav:	**Ústav telekomunikací**
Obor:	**Teleinformatika**
Vedoucí práce:	**Doc. Ing. Václav Zeman, Ph.D.**
Počet stran:	**53**
Počet příloh:	**0**
Rok obhajoby:	**2008**

Bakalářská práce je zaměřena na komparaci elektronického bankovnictví. Srovnávání jednotlivých typických znaků vybraných bank poskytlo informace, které je možné využít k výběru finančního ústavu uživatelem (klientem).

První část práce popisuje elektronické bankovnictví a jeho zabezpečení (šifrování, hash, elektronický podpis a protokoly). Druhá část této práce analyzuje zabezpečení elektronického bankovnictví pomocí daných kritérií.

Klíčová slova

Elektronické bankovnictví

Šifrování a kryptografie

Autentizace a autorizace

Elektronický podpis

Protokoly

Abstract

Title:	**E-banking**
Name:	**Vlk Bronislav**
Department:	**Department of Telecommunications**
Specialization:	**Teleinformatics**
Supervisor:	**Doc. Ing. Václav Zeman, Ph.D.**
Number of pages:	**53**
Number of attachments:	**0**
Year of defence :	**2008**

My work is focused on a comparison of electronic banking. Comparing typical individual characters selected banks provided information which can be used to select a financial institution user (client).

The first part describes the work of electronic banking and its security (encryption, hash, electronic signature and protocols). The second part of this work analyzes the security of electronic banking via the above criteria.

Keywords

E-banking

Encryption and cryptography

Authentication and authorization

Electronic signature

Protocols

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma Elektronické bankovnictví 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 jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 28. 5. 2008 .....

(podpis autora)

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D., za velmi užitečnou metodickou pomoc a cenné rady při zpracování semestrální práce.

Obsah str.

Úvod

Vývoj lidstva s sebou nese pokrok ve všech jeho oblastech. Ne vždy však posun vpřed bývá jen pozitivní. Moderní technický pokrok na jedné straně usnadňuje a urychluje lidstvu práci. Na straně druhé mívá i negativní dopad. K jednomu z nich právem náleží ochrana dat klienta banky.

V době internetu již není možná existence bank bez poskytování internetových služeb. Ba dokonce lze konstatovat, že oblast internetového bankovnictví je jedna z nejrychleji se rozvíjejících oblastí na českém finančním trhu. Možnost využívat rychlého a pohodlného způsobu spravování svých finančních prostředků je velmi lákavá, řadě klientů ušetří čas i peníze. Ovšem přináší i rizika, týkající se bezpečné ochrany účtu.

Cílem mé bakalářské práce je popsat principy současných elektronických bankovních systémů, včetně jejich základních vlastností.

Nevyhnutelnou podmínkou pro fungování elektronického bankovnictví je jeho bezpečnost. Na tu jsem se ve své práci zaměřil nejvíce. Proto dalším cílem práce je průzkum a srovnání elektronických bankovních systémů používaných v České republice.

1 Elektronické bankovnictví

Elektronické (též přímé) bankovnictví je založeno na elektronické vzájemné výměně dat mezi bankou a klientem. Z důvodu velkého růstu e-transakcí (transakcí uskutečněných přes internet) stoupá i velká poptávka po kvalitním a bezpečném elektronickém bankovnictví. Banky se snaží vycházet vstříc požadavkům klientů. Ti kladou vysoké nároky na bezpečnost předávaných informací. Cílem bank je co nejsnáze spravovat peníze na bankovním účtu klienta. Od toho se odvíjí i to, aby banky měly co nejmenší náklady, které neustále rostou.

Klient - uživatel může využívat pro svou správu účtu v bance např. mobilní telefon, internetový prohlížeč (např. Microsoft Internet Explorer, Mozilla Firefox, Apple Safari či Opera ASA), přístup k internetu a případně pro kvalitnější zabezpečení

účtu např. čipovou kartu, certifikát, mobil či PIN kalkulátor (bližší popis v kapitole 2.10 Autentizace a autorizace).

Banky se snaží prosadit různou filozofii přístupu klienta k datům. K dispozici je několik druhů klientů:

- Tlustý – Klient má v sobě více funkcí a vykonává část logiky aplikace. Nabízí tak přídavnou hodnotu k efektivnějšímu zpracování. Nedochází však k úspoře TCO (náklady na vlastnictví programů - Total Cost of Ownership), protože se musí udržovat aplikační část na klientech. S každým upgradem se musí aktualizovat všechny klienty.
- Tenký - Klient je určen pro spojení uživatele s databázi pomocí Internetu nebo sítě LAN s nižšími přenosovými pásmy. Na klienta je odesílána pouze obrazovka a aplikační logika je zpracovávána na serveru.
- Dedikovaný – specializovaný klient je přímo připojen do databáze, kde modifikuje data v reálném čase. Typicky je tento klient používán pro velký počet uživatelů nad výkonnou komunikační infrastrukturou.
- Mobilní. – Klient modifikuje data v lokální databázi s následnou synchronizací do centrální databáze. Typickým příkladem jsou laptopy a handheldy. Tento klient je určen pro uživatele v „poli“, kterým stačí pouze přístup k menšímu objemu specifických dat.

Tenkých klientů může být celá řada a nejčastěji se používá:

- Tenký klient pro Windows, zajišťující přístup k datům pomocí WWW prohlížeče. Klient je určen pro velký počet internetových a intranetových uživatelů.
- Tenký klient pro Javu, který umožňuje přístup javovským aplikacím, přistup k databázím zejména v ne-Windowsovském prostředí např. Sun Solaris. Klient je rovněž určen pro velký počet internetových a intranetových uživatelů.
- Tenký klient pro HTML, který využívá protokolu HTML k zobrazení uživatelského rozhraní. Klient je určen pro menší počet internetových uživatelů.
- Tenký klient pro WML, který zajišťuje bezdrátové spojení do databáze pomocí protokolu WAP (Wireless application protocol). Uživatelské rozhraní na WAP zařízení je specifikováno pomocí WML a XML. WAP server převádí data http na wireless protocol (WAP).

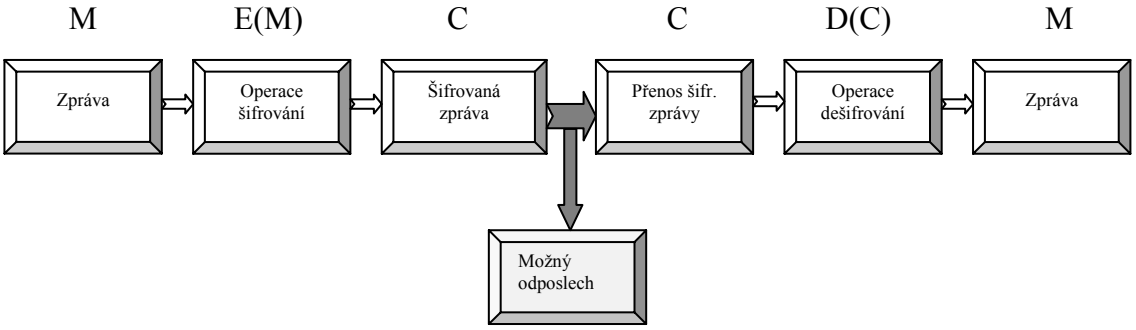
- Tenký klient se specializovaným protokolem pro zobrazování. Příkladem mohou být technologie firmy Citrix (ICA) nebo Terminal Server firmy Microsoft. Specializované protokoly řeší opravu chyb, obnovu, šifrování a kompresi dat. Všechny tyto funkce jsou zajištěny i na malých přenosových pásmech. Řešení firmy Citrix má navíc k dispozici podporu pro šifrované přenosy mezi specializovanou SSL bránou pod názvem Citrix Secure Gateway. S tímto produktem získalo řešení certifikaci na FIPS 140-1. Je zajištěna také přímá podpora protokolu IPSec. Vlastní klient je k dispozici na všechny známé operační systémy Windows, Linux, Solaris, Macintosh a další.

2 Zabezpečení elektronického bankovnictví

2.1 Šifrování a kryptografie

Kryptografie je nauka o šifrách známá již z dob starověku. Používání kódů a šifer sloužilo k ukrytí smyslu důležitých informací a v průběhu dějin nabývala kryptografie stále většího významu. Slovo kryptografie pochází z řečtiny – kryptós (je skrytý) a gráphein (psát).

Šifrování je způsob, jak zvýšit zabezpečení zprávy či souboru zašifrováním vlastního obsahu zprávy. Takto zašifrovanou zprávu smí číst jen ta osoba, která vlastní šifrovací klíč. Použití kódování dat nám zajišťuje vyšší bezpečnost, ale může způsobit i pocit falešného bezpečí.



obr. 1 Přenos dat šifrovaným kanálem

Kryptografické metody obecně využívají tzv. "klíč", pomocí kterého tajná data šifrují a posléze opět dešifrují. Současně některé metody umožňují nebo i vynucují použití více klíčů různých pro šifrování a dešifrování.

Většina moderních algoritmů je založena na matematické teorii čísel. Tzv. kryptografická transformace T je libovolné prosté zobrazení množiny celých čísel na množinu celých čísel. Kryptografický systém je pak parametrický systém kryptografických transformací $T^K = (Tk : k \in K)$, kde k je klíč a K je prostor klíčů. Podle použití způsobu práce s klíči se kryptografické metody dělí na symetrické a asymetrické.

2.2 Symetrické šifry

Symetrická kryptografie (též "konvenční kryptografie" či angl. "conventional cryptography") používá stejný klíč jak pro šifrování, tak pro dešifrování zprávy.

Vstupem je tedy nějaký text ze stanovené abecedy a klíč. Šifrovací funkcí se za pomoci klíče text převede na šifrovaný text, který může být odeslán příjemci zprávy. Příjemce pak použije dešifrovací funkci se stejným klíčem a tím získá původní text. Důležité je, že pro dešifrování musí mít příjemce k dispozici stejný klíč, jakým byl text šifrován. Je tedy třeba zajistit bezpečný způsob doručení klíče, aby se tento klíč nedostal do nepovolaných rukou.

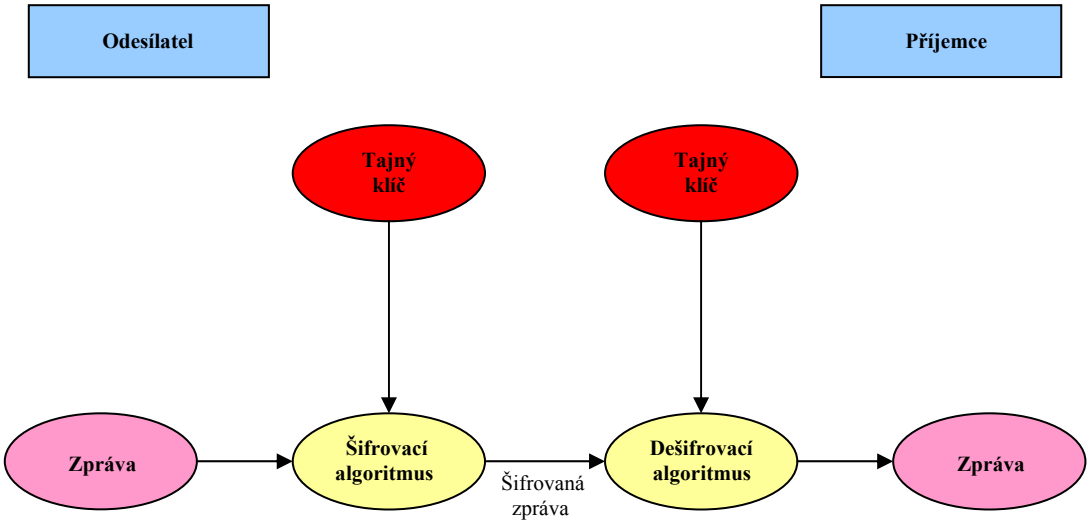
Pro šifrování se používají funkce, u kterých platí, že při znalosti vstupního a šifrovaného textu je velmi obtížné vygenerovat klíč, ač vlastní šifrování a dešifrování pomocí tohoto klíče je rychlá záležitost. Obtížnost eventuálního zjištění klíče záleží zejména na vlastní délce klíče. Šifrovaná zpráva musí odolat hrubému útoku silou, který předpokládá vyzkoušení všech možných klíčů. Pokud je klíč délky 8 bitů, existuje 2^8 (256) možných klíčů. Před několika lety se podařilo rozbít šifru DES s 56ti-bitovým klíčem. V dnešní době se užívají běžně klíče velikosti 128 bitů, kdy zjištění takového klíče by teoreticky trvalo asi 10^{39} let. To znamená že i při současném trendu vývoje IT budou klíče s touto délkou ještě nějakou chvíli použitelné.

Mezi symetrické metody kryptografie patří např. již zmíněný algoritmus DES (délka klíče 56 bitů) či jeho nástupce 3DES (násobný DES – klíč 3x delší než DES, tj. 168 bitů) anebo další, jako jsou BlowFish (proměnná délka klíče až 256 bitů) a IDEA

(délka klíče 128 bitů), CAST (délka klíče 128 bitů), CIFER (délka klíče 16 bitů) a AES (délka klíče 128, 192 či 256 bitů).
Výhody a nevýhody symetrické kryptografie:

- Výhodou symetrických metod je jejich rychlost. Dají se také velmi dobře využít pro šifrování dat, která se nikam neposílají (zašifrují se dokumenty na počítači, aby je nikdo nemohl číst).
- První nevýhodou je, že pokud chceme s někým šifrovaně komunikovat, musíme si předem bezpečným kanálem předat klíč. To někdy může být obrovský problém. Druhá nevýhoda je počet klíčů. Chceme-li zajistit, aby mohli tajně spolu komunikovat 2 osoby, je zapotřebí 1 klíče. Pro 3 osoby jsou to již 3 klíče, pro 4 osoby 6 klíčů, obecně počet klíčů = n*(n-1)/2, kde n je počet osob. Při vyšším počtu osob tak začíná být správa klíčů problémem.

Algoritmus DES má šifrovací klíč délky 56 bitů. Tento však je již nedostačující a byl nahrazen algoritmem 3DES s klíčem 112 bitů nebo 168 bitů (112=2x56 nebo 168=3x56 – 56 je délka šifrovacího klíče algoritmu DES). Další algoritmy jsou algoritmy s délkou klíče 128 bitů (IDEA, RC2, RC4 atd.). V současné době je nejpoužívanější algoritmus AES s délkou klíče 128, 192 nebo 256 bitů. Jedná se o blokové šifry, které se šifrují/dešifrují po blocích o velikosti např. 8 B. Jestliže je vstupující blok kratší, musí se dorovnat na 8 B, aby útočník nemohl zaměnit pořadí jednotlivých zašifrovaných bloků (obr. 2). Obsah předchozího bloku se nesmí dostat do bloku následujícího, aby nedocházelo k přehazování šifrovaných bloků. Mluvíme o tzv. módu šifry.



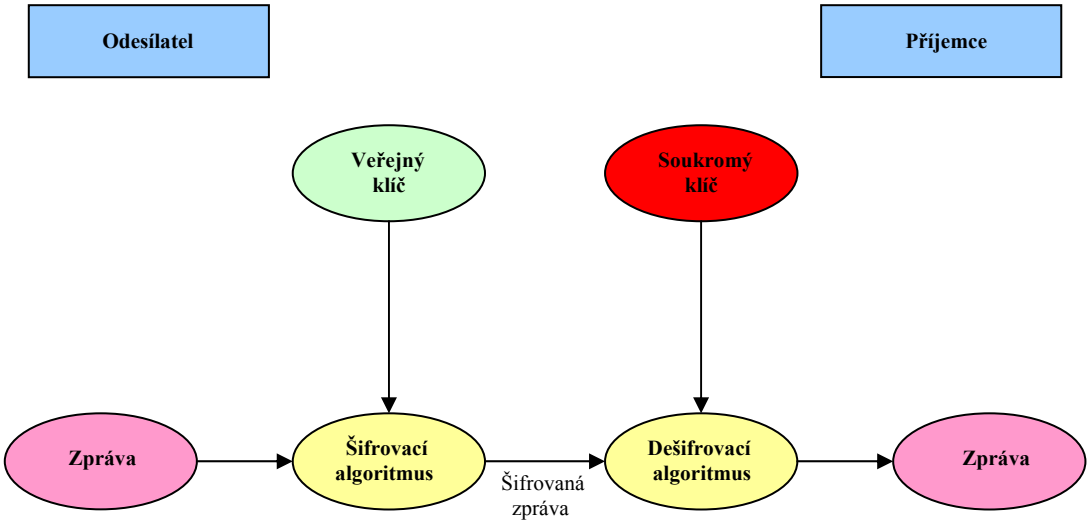
obr. 2 Symetrická šifra

Často používané módy jsou např. módy CBC (Cipher block chaining mode) či ECB (Electronic codeblock mode). Jestliže chceme vyjádřit algoritmus s konkrétním módem, mluvíme např. o DES-CBC, DES-ECB, IDEA-CBC či IDEA-ECB atd.

2.3 Asymetrické šifry

Druhou skupinou kryptografických metod je tzv. "asymetrická kryptografie" (též angl. "public key cryptography").

Asymetrické šifry oproti šifrám symetrickým používají vždy pár šifrovacích klíčů ("kaypair"). Jeden klíč pro šifrování a druhý pro dešifrování. U asymetrických šifer nemluvíme o šifrovacím a dešifrovacím klíči, ale o veřejném ("public key") a soukromém klíči ("private key"). Nejznámějším asymetrickým šifrovacím algoritmem je algoritmus RSA.



obr. 3 Asymetrická šifra

Příjemce si musí vygenerovat dvojici klíčů: veřejný klíč a soukromý klíč. Soukromý klíč si příjemce uloží do důvěryhodného úložiště klíčů (na pevný disk, čipovou kartu atd.), který si musí střežit. Veřejný klíč může příjemce poskytnout třetí straně, aniž by se bál dešifrování zprávy. Odesílatel po přijetí veřejného klíče od příjemce šifruje zprávu právě tímto veřejným klíčem. Příjemce dešifruje přijatou zprávu svým soukromým klíčem a získá původní zprávu.

Důležitou vlastností asymetrického algoritmu je, že za použití veřejného klíče lze snadno šifrovat text, ale naopak na základě veřejného klíče je velice obtížné získat původní zprávu.

Veřejný klíč je skutečně veřejný, tj. pokud uživatel chce, aby mu někdo mohl poslat zašifrovanou zprávu, musí nejprve dát k dispozici tento svůj veřejný klíč. Ten použije odesílatel pro zašifrování tajné zprávy a šifru odešle. Pro dešifrování pak potřebuje příjemce mít druhý klíč z páru, soukromý klíč, který jediný lze použít pro dešifrování. Klíčový pár se většinou tvoří zároveň. Algoritmus uživateli vygeneruje oba klíče, veřejný klíč uživatel zveřejní a soukromý klíč si dobře uschová.

S délkou klíče asymetrických metod je to trochu jinak, než u symetrických šifer. Asymetrické šifry většinou pracují se specifickým druhem čísel, např. s prvočísly. Při záškodníkových pokusech o rozkódování se pak stačí zabývat jen tímto oborem čísel a tedy i počet bitů klíče je třeba oproti symetrickým metodám patřičně navýšit, aby byla zachována požadovaná míra bezpečnosti.

Bezpečná délka šifrovacích klíčů pro algoritmus RSA je min. 1024 bitů. Často se však používají klíče dlouhé 2048 či 4096 bitů. Mezi nejznámější asymetrické metody patří algoritmy DH (Diffie-Hellman; 1976), RSA (Rivest-Shamir-Aleman; 1977) a DSA (digital signature algorithm; 1991).

Algoritmus Diffie-Hellmanův (DH) se však nehodí pro asymetrické šifrování, ale k bezpečnému stanovení tajných klíčů či sdílených tajemství.
Obecně platí, že asymetrické šifrovací algoritmy jsou výpočetně mnohem náročnější než symetrické algoritmy.

Výhody a nevýhody asymetrické kryptografie

- Hlavní výhodou je to, že není třeba nikam posílat soukromý klíč a tak nemůže dojít k jejímu vyzrazení. Naproti tomu veřejný klíč je možné dát k dispozici všem. Je třeba méně klíčů než u symetrických metod – pro komunikaci několika osob postačí pro každou osobu jen jeden pár klíčů.
- Nevýhodou asymetrických metod je jejich rychlost. Tyto metody jsou až 1000 x pomalejší než metody symetrické. Další nevýhodou asymetrické kryptografie je nutnost ověření pravosti klíče, tj. stoprocentní identifikace majitele veřejného klíče. Pro tyto účely existují např. certifikační úřady, které zjednodušeně řečeno udržují databázi osob s ověřenou totožností a jejich veřejných klíčů. V teoretickém případě nabourání takového úřadu však může záškodník např. zaměnit klíče u různých registrovaných osob a tak nic netušící uživatel zakóduje tajnou zprávu veřejným klíčem záškodníka místo klíčem skutečného adresáta.

Vzhledem k pomalosti asymetrických metod šifrování se často využívá kombinace obou metod, kdy se z každé metody využívají její přednosti. Tajný klíč symetrické metody je např. zašifrován veřejným klíčem asymetrické metody, čímž je zajištěno jeho bezpečné předání adresátovi. Tajným klíčem pak lze šifrovat vlastní tajnou zprávu.

Někdy postačuje samotná symetrická kryptografie – a to v případě, že si obě strany dokážou jiným bezpečným způsobem předat tajný klíč.

Další místo využití je např. v případě jednoho uživatele, který si chce ochránit své vlastní soubory před zneužitím tak, aby je mohl otevřít jen on sám.

2.4 Autentizace pomocí asymetrické kryptografie

Podstatou asymetrického šifrovacího systému jsou dva různé klíče – jeden veřejný (pro šifrování) a druhý soukromý (pro dešifrování). Veřejný klíč je určen k volnému šíření a je distribuován všem osobám, se kterými komunikujeme. Naproti tomu soukromý klíč musí zůstat přísně utajen u jeho vlastníka, který by jej měl chránit jako oko v hlavě. To, co bylo zašifrováno veřejným klíčem, lze dešifrovat pouze soukromým klíčem. Jeden jediný klíč nelze použít k zašifrování i opětovnému dešifrování. Důvodem této vlastnosti asymetrických algoritmů jsou použité matematické funkce, jejichž reverzní výpočet je prakticky neproveditelný. Asymetrické šifrovací algoritmy jsou v porovnání se symetrickými obecně výrazně pomalejší. Asymetrické kryptosystémy (např. RSA, ECPKC, LUC), kryptografické protokoly i metody digitálních podpisů používají komplikované operace s dlouhými čísly, které by standardnímu PC nebo běžné čipové kartě trvaly příliš dlouho. Proto se často šifruje klasickými symetrickými systémy (např. DES, IDEA, WinCros). Asymetrickými systémy se šifrují pouze relativně krátké použité symetrické klíče.

V praxi se nejčastěji používá algoritmus RSA a algoritmy na bázi eliptických křivek (ECC). Autory RSA jsou Rivest-Shamir-Adleman. Stupeň jeho bezpečnosti je odvislá od použité délky klíče. Pro vytváření elektronického podpisu se standardně používají klíče s minimální délkou 1024 bitů. Samotný algoritmus vznikl v roce 1977 a do podzimu roku 2000 byl chráněn patentem. Jeho prolomení závisí na schopnosti útočníkova systému řešit úlohy faktorizace velkých čísel. Ve srovnání s DES je RSA samozřejmě podstatně pomalejší. Při softwarových realizacích se uvádí, že je to přibližně 100 krát, při hardwarových realizacích dokonce 1000 až 10000krát. RSA je součástí řady používaných norem.

Vývoj několika posledních let v této oblasti do značné míry naznačuje, že budoucnost bude patřit spíše algoritmům na bázi eliptických křivek (ECC). Jedná se o moderní algoritmy založené na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. Výhodou ECC oproti RSA je především řádově větší bezpečnost při použití výrazně kratšího klíče. K dosažení stejné bezpečnosti, jako má RSA s klíčem o délce 2048 bitů, potřebujeme eliptický klíč s délkou pouze asi 160 až 180 bitů. Existují i hybridní šifry, které kombinují jak symetrické algoritmy, tak asymetrické algoritmy.

Je tedy daleko výhodnější data zašifrovat symetrickým algoritmem a náhodným klíčem, který je vygenerován jako jedinečný pouze pro danou relaci. Ten posléze zašifrovat pomocí asymetrického algoritmu a přibalit k zašifrovaným datům. Celý „balíček“ je pak odeslán příjemci, který nejprve dešifruje symetrický klíč a teprve s jeho pomocí samotná data. Tímto způsobem funguje drtivá většina softwaru používajícího asymetrickou kryptografii (včetně např. PGP).

2.5 Hash (otisk)

Hash funkce je transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je pak řetězec znaků s pevnou délkou, tzv. hash nebo také otisk. Hash funkce se často používají v kryptografii, kde se však na její kvalitu kladou další kritéria.

Co tedy očekáváme od kvalitní hash funkce:

- vstup může být jakékoli délky
- výstup musí mít pevnou délku
- hodnota hash musí být jednoduše vypočitatelná pro jakýkoli vstupní řetězec
- funkce je jednosměrná (ireverzibilní)
- funkce je bez kolizí

Funkce je jednosměrná, pokud je nemožné jednoznačně najít k otisku původní text. Funkce je slabě bezkolizní, pokud k danému textu není výpočetně možné vymyslet jiný text, který bude mít stejný otisk.
Funkce je silně bezkolizní, pokud není výpočetně možné najít dva různé texty se stejným otiskem.

Mezi dnes běžně používané algoritmy patří SHA-1 a MD5. Hash funkce jsou nepostradatelnou součástí elektronického podpisu.

Základní princip hashe spočívá v tom, že výsledný hash je zhuštěným otiskem, který identifikuje původní zprávu. Hashování nachází spoustu různých uplatnění, například při kontrole integrity dat nebo jako součást schémat digitálního podpisu.

Kódy pro ověřování zpráv pomocí algoritmů hash (HMAC) označují pakety za účelem ověření, zda jsou přijaté informace shodné s odeslanými informacemi. Tato funkce se nazývá integrita a je nejdůležitější při výměně dat prostřednictvím nezabezpečených médií.

Kódy HMAC zajišťují integritu pomocí algoritmu hash s klíčem, což je výsledek matematického výpočtu u zprávy, který využívá funkci (algoritmus) hash v kombinaci se sdíleným tajným klíčem.

Algoritmus hash je kryptografický kontrolní součet neboli kontrolní součet MIC (Message Integrity Code), který musí obě strany vypočítat, aby mohla být zpráva ověřena. Odesílající počítač například používá k výpočtu kontrolního součtu u zprávy funkci hash a sdílený klíč, které zahrne do paketu. Přijímající počítač musí provést stejnou funkci hash u přijaté zprávy a sdíleného klíče a porovnat ji s původní hodnotou (zahrnutou do paketu od odesílatele). Pokud se zpráva během přenosu změnila, budou se hodnoty algoritmu hash lišit a paket bude odmítnut.

Hash vypočtený ze zprávy, která je zřetězená, se velmi často nazývá MAC (Message Authentication Code). MAC se používá v protokolech SSL/TLS, protokolu IPsec a např. v autentizačních kalkulátorech pro tvoru jednorázových hesel. MAC se někdy označuje jako „symetrický podpis“.

Pojem hashovací funkce se vyvinul z pojmu jednosměrné funkce v návaznosti na kryptografické aplikace. Norma ISO/IEC 10118 popisuje jednak obecné přístupy, jednak některé konkrétní technologie. V současné době jsou nejpoužívanějšími hashovacími funkcemi následující:

SHA-1 (norma z roku 1995 [1],

MD5 (RFC1321: The MD5 Message-Digest Algorithm. R. Rivest. April 1992.),

RIPEMD [2] - evropské schéma hashovací funkce.

Některé další byly navrženy v rámci projektu Cryptonessie a i NIST si vzhledem k AES pospíšil s předběžnou verzí **SHA-512**, což je hashovací funkce umožňující výstupy v délce až 512 bitů [3] atd.

Blízkou třídou norem jsou dokumenty popisující tzv. autentizační kódy zpráv (MAC - Message Authentication Code) - ISO/IEC 9797.

Staršími, dnes již ojediněle používanými hashovacími funkcemi jsou MD2 a MD4 (obě vycházejí z dílny RSA Security- RFC 1319 a RFC 1320).

Algoritmus MD5 (Message-Digest algorithm 5) je velmi rozšířený hash o velikosti 128 bitů. MD5 je popsána v internetovém standardu RFC 1321. Prosadila se do mnoha aplikací, např. pro kontrolu integrity souborů nebo ukládání hesel.

Algoritmus MD5 byl vytvořen v roce 1991 (Ronaldem Rivestem), aby nahradil dřívější hašovací funkci MD4. V roce 1996 byla objevena vada v návrhu MD5, a i když nebyla zásadní, kryptologové začali raději doporučovat jiné algoritmy, jako je například SHA-1 (i když ani ten již dnes není považován za bezchybný). V roce 2004 byly nalezeny daleko větší chyby a od použití MD5 v bezpečnostních aplikacích se upouští.

Algoritmus MD5 provede čtyři průchody datových bloků (algoritmus MD4 provedl pouze tři průchody) za použití různých číselných konstant pro jednotlivá slova ve zprávě během každého průchodu. Počet 32bitových konstant použitých během výpočtu algoritmu MD5 je 64, takže algoritmus MD5 nakonec vytvoří 128bitový algoritmus hash, který se používá pro kontrolu integrity. I když je algoritmus MD5 náročnější na prostředky, poskytuje silnější integritu než algoritmus MD4.

Algoritmus SHA1 (Secure Hash Algorithm 1) byl vyvinut v institutu NIST (National Institute of Standards and Technology), jak je uvedeno ve standardu Federal Information Processing Standard (FIPS) PUB 180-1. Proces výpočtu algoritmu SHA se velmi podobá procesu výpočtu algoritmu MD5. Výsledkem výpočtu algoritmu SHA1 je 160bitový algoritmus hash, který se používá pro kontrolu integrity. Delší algoritmus hash poskytuje lepší zabezpečení, proto je algoritmus SHA bezpečnější než algoritmus MD5.

Velikost vstupu je omezena hodnotou 2^{64}. Algoritmus SHA-1 poskytuje 80 bitové zabezpečení, což v praxi znamená, že při standardním útoku na haš délky 160 bitu je třeba $2^{160/2}$ operací k nalezení kolize. Tento algoritmus je využíván především v oblasti digitálního podepisování a v oblasti ověřování integrity dat.

V současné době se považují algoritmy MD-5 a SHA-1 za slabé a nedostačující. Nahrazují je algoritmy vytvářející delší hashe např. SHA-224 (hash dlouhý 28 B), SHA-256 (hash 32 B), SHA-384 (hash 48 B) či otisk SHA-512 (hash 64 B) – podobný hashy SHA-256, někdy nazývaný jako SHA-2.

2.6 Elektronický podpis

Zajímavou aplikací asymetrických metod kryptografie je tzv. elektronický podpis. Pro použití elektronického podpisu potřebujeme nejprve nějakou známou hashovaní funkci (např. MD5 nebo SHA-1). Známou v tom smyslu, aby všichni adresáti, kteří budou chtít ověřit pravost naší zprávy tuto funkci znali (resp. ji znal program, který ověření provede). Hash funkce udělá z naší zprávy tzv. otisk (angl. "message digest") nebo se výsledek také dá nazvat jakýmsi kontrolním součtem zprávy. Tento otisk má vždy stejnou délku bez ohledu na délku vstupní zprávy (128 či 160 bitů). Jednou z vlastností této hashovací funkce je fakt, že prakticky není možné z otisku zpětné získání původní zprávy a zároveň je i velmi nepravděpodobné nalezení jiné zprávy, která by použitím hashovaní funkce dala stejný otisk.

Jestliže takto vzniklý otisk podepíšeme svým soukromým klíčem (nejčastěji se používá algoritmus DSA viz. níže), vznikne nám kýžený elektronický podpis. Podpis pak přiložíme k původní zprávě a zprávu i s touto přílohou odešleme. Příjemce zprávu otevře, a pomocí stejné hashovací funkce vypočítá její otisk. Pomocí veřejného klíče odesílatele dále získá obsah elektronického podpisu. Je-li tento rozkódovaný obsah totožný s otiskem přijaté zprávy, je identita odesílatele potvrzena, jelikož nikdo jiný, než vlastník soukromého klíče nemohl elektronický podpis s touto vlastností vytvořit.

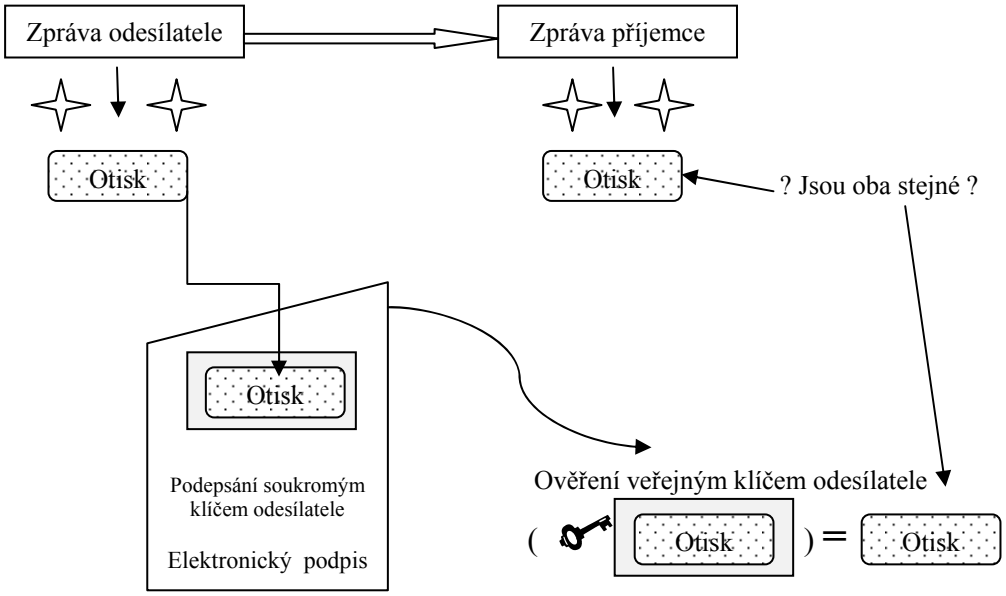
Hashovaní funkce se používá z důvodu, aby přikládaný elektronický podpis nebyl příliš velký. Pokud by odesílatel svým soukromým klíčem podepsal celou zprávu, elektronický podpis by byl minimálně jednou tak velký a tedy finální zpráva s podpisem by zvětšila objem minimálně na dvojnásobek. V případě použití hashovaní funkce je zaručena stejná funkčnost, avšak s minimální datovou přítěží k původní zprávě.

Elektronický podpis je mechanismus pro zajištění integrity odesílaných dat (například zadání transakcí) a bezpečné ověření jejich odesilatele. Elektronický podpis se používá jako komunikační prostředek např. právě pro internetové bankovnictví.

Verifikace (ověřování) se provádí ve třech krocích (obr. 4):

- Příjemce spočte otisk z přijaté zprávy.
- Příjemce získá z přijatého elektronického podpisu pomocí veřejného klíče odesílatele otisk zprávy.
- Příjemce porovná výsledek získaný z bodu 1 s výsledkem získaným z bodu 2.

Jestliže jsou výsledky stejné, pak ten, kdo vlastní soukromý klíč odesílatele, je právě ověřený odesílatel. Z toho plyne, že zpráva nebyla během přenosu pozměněna.



obr. 4 Verifikace elektronického podpisu

Elektronický podpis provádí důkaz pravosti na základě vlastního soukromého klíče. Svůj vlastní soukromý klíč je nutné chránit.

Na rozdíl od šifrování se používá elektronický podpis klíče odesílatele (nikoli příjemce).

Elektronický podpis je chápán jako podpis vytvořený na základě asymetrické kryptografie.

Na elektronický podpis existují v různých zemích různé pohledy. V některých zemích je elektronický podpis chápán jako plnohodnotná náhrada rukou psaného textu a v jiných zemích je chápán jen k autentizaci dokumentu.

V členských zemích EU je problematika elektronického podpisu řešena formou „Směrnice evropského parlamentu a rady 1999/93/ES“ ze dne 13. prosince 1999. V české legislativě se jedná o zákon „O elektronickém podpisu“ č. 227/2000 Sb. Tento zákon byl novelizován zákony 226/2002 Sb., 517/2002 Sb. a 440/2004 Sb.

Samotný elektronický podpis lze přirovnat spíše k efektu, kterým je identifikace a autentizace např. autora určitého dokumentu. Elektronický podpis je založen na metodách asymetrickém šifrování.

Elektronický podpis musí splňovat:

- jeho základní vlastností je nepopiratelnost
- je prakticky nemožné jej zfalšovat
- lze jednoduše ověřit jeho autenticitu
- jeho použitím je zaručena neporušenost zprávy (resp. zjištění jejího porušení)
- v kombinaci se šifrováním je zpráva chráněna před vyzrazením obsahu
- navíc může obsahovat časovou značku a být tak jednoznačně určen v čase

Elektronický podpis – sestavení a ověření

Pokud chceme vytvořit elektronický podpis určitého souboru, musíme nejprve určit jeho HASH. Jakýkoliv soubor nebo e-mailovou zprávu lze v podstatě chápat jako „obyčejný“ soubor čísel, na který aplikujeme HASH algoritmus. Na jeho výstupu získáme číslo o dané délce jednoznačně reprezentující vstupní data – otisk souboru. HASH je následně zašifrován pomocí soukromého klíče podepisující osoby a elektronický podpis je na světě. Poněkud zjednodušeně řečeno je HASH podepsán privátním klíčem elektronickým podpisem. Ten se pak může přidat k podepisovaným datům nebo může být transformován do podoby samostatného souboru (extra signature). Zpravidla se k němu ještě přidává i digitální certifikát podepsané osoby, který může posloužit adresátovi k ověření podpisu.

Ověření podpisu probíhá analogicky k jeho vytvoření. Příjemce jednak znovu vypočte HASH z původního souboru a jednak jej ověřuje pomocí certifikátu odesílatele z podpisu. Certifikát buď již má ověřující osoba k dispozici nebo si jej může třeba stáhnout z webu certifikační autority, která jej vydala. Samotné ověření pak spočívá v porovnání obou HASHů. Pokud jsou stejné, je zřejmé, že podepsanou osobou je skutečně ta, která to o sobě tvrdí (vlastník certifikátu, který jediný má k dispozici privátní klíč). Pokud se HASH liší, může to znamenat pokus o padělání podpisu, pozměnění souboru cestou nebo cokoliv jiného, co ve svém důsledku vedlo k porušení nebo pozměnění dat či podpisu samotného.

Digitální certifikát se skládá ze dvou základních komponent: veřejného klíče a osobních dat jeho vlastníka. Celistvost certifikátu je zaručena elektronickým podpisem, které může vytvořit sám jeho vlastník pomocí soukromého klíče z tohoto klíčového

páru (self-signedcertificate) nebo certifikační autorita svým soukromým klíčem. Z hlediska důvěryhodnosti má logicky větší váhu digitální certifikát vydaný certifikační autoritou, která ručí za ověření identity jeho vlastníka. Kromě již zmiňovaných obsahují certifikáty také další údaje, jako je doba vypršení platnosti certifikátu (expirace), jméno vydávající certifikační autority, evidenční číslo certifikátu, certifikační cesta (posloupnost certifikátů certifikační autority, které jsou potřebné k ověření pravosti certifikátu), případně ještě další doplňující údaje.

Certifikační autoritu si můžeme představit jako jistou formu notářského úřadu, figurujícího mezi komunikujícími stranami, o které by se dalo říci, že spojuje veřejný klíč s uživatelem a ozřejmuje jeho autenticitu. Základním dokumentem, kterým se certifikační autorita řídí, je certifikační politika. Český zákon O elektronickém podpisu stanovuje řadu požadavků a náležitostí, které musí poskytovatel certifikačních služeb splňovat. Například ručí do stanovené výše za případné škody vzniklé vlastním pochybením, má omezené možnosti dalšího podnikání atp. U nás například společnost První certifikační, Certifikační autorita Czechia ad.

Pokud budeme chtít elektronický podpis používat i pro zabezpečení vlastní komunikace, je i zde k dispozici více možných řešení. V podstatě můžeme využít možností, které nám nabízí operační systém a další nástroje Windows, a podepisovat e-maily přímo v Outlooku. Nebo můžeme využít software od jiného výrobce, který bývá zpravidla pro uživatele daleko více transparentní a dává jim větší možnosti kontroly nad klíčovými páry i šifrovanými/podepisovanými daty.

2.7 Autentizace uživatele

Autentizaci uživatele je možno provést:

- Uživatel něco má (autentizační kalkulátor, čipovou kartu či např. mobilní telefon)
- Uživatel něco ví (heslo, PIN)
- Uživatel něčím je - má např. biometrické vlastnosti (otisky prstů, struktura oční sítnice či duhovky, tvar obličeje apod.)
- Uživatel něco umí (podepsat se)

Snahou je kombinovat mezi všemi metodami. Vedle autentizace (prokazování totožnosti) se používá i termín autorizace. Zatímco autentizaci prokážeme, o koho se jedná, autorizaci přiřazujeme role či oprávnění, která má v jednotlivých aplikacích.

V PKI se pro autentizaci využívá certifikát veřejného klíče a pro autorizaci pak atributové certifikáty.

Autentizační metody:

Stálá hesla – přístupové heslo. Na straně serveru bývá znehodnocené jednocestnou funkcí proti zneužití. Stálé heslo však může být odposlechnuto či vylákáno pomocí podvrženého serveru.

Jednorázová hesla – řeší problém s odposlechem hesla během přenosu. Používá se mnoho algoritmů pro jednorázová hesla, např. seznam jednorázových hesel, kombinace jednorázových hesel a stálým (PIN) nebo číslování hesel – systém vyžaduje určité heslo ze seznamu.

a) Rekurentní algoritmus – využívá jednocestné funkce, např. otisk.
b) Sdílené tajemství – důkaz pravosti dokumentu. Generují se jednorázová hesla.
c) Symetrická šifra – klient sdílí se serverem symetrický šifrovací klíč.

Biometrika – používá se biometrických vlastností člověka. Nejlevnějším je otisk prstů. Ten lze omezit na 300 – 600 bajtů. Využití biometrických vlastností je největší např. otevírání dveří, k přístupu k PC apod. Nejlepšího využití nachází biometrika v kombinaci s čipovou kartou. Pomocí otisků prstů a PIN otevřeme přístup k soukromému klíči na čipové kartě a následně využijeme soukromého klíče na této kartě k autentizaci.

Shamirův algoritmus – tento je určen pro ochranu aktiva (šifrovacího klíče, sdíleného tajemství apod.). Část sdíleného tajemství či šifrovacího klíče uložíme např. na ***n*** čipových karet a tyto rozdáme ***n*** držitelům karet. Jestliže chceme tajemství rekonstruovat, musí se sejít ***k*** držitelů karet.

2.8 Protokoly

Protokol definuje pravidla komunikace. Komunikuje s partnerskou vrstvou jiného uzlu.

Protokol může být standardizovaný (podle RGC, IEEE, CCITT, ISO, apod.) nebo soukromý.

Zahrnuje:

- proceduru navázání spojení
- adresování
- přenos dat
- zpracování chyb
- řízení toku komunikace
- přidělování prostředků

Popis šifrování dat: Jakmile jsou ověřeny obě strany (klient i banka), může klient pracovat s internetovým bankovnictvím. Slabým článkem je i komunikační cesta, po které proudí výměna dat. Ta může být odposlouchávána, pozdržena, přečtena a pozměněna. Z toho důvodu jsou data oběma směry šifrována. K tomuto obousměrnému šifrování se mohou používat protokoly např. SSL, IPsec apod.

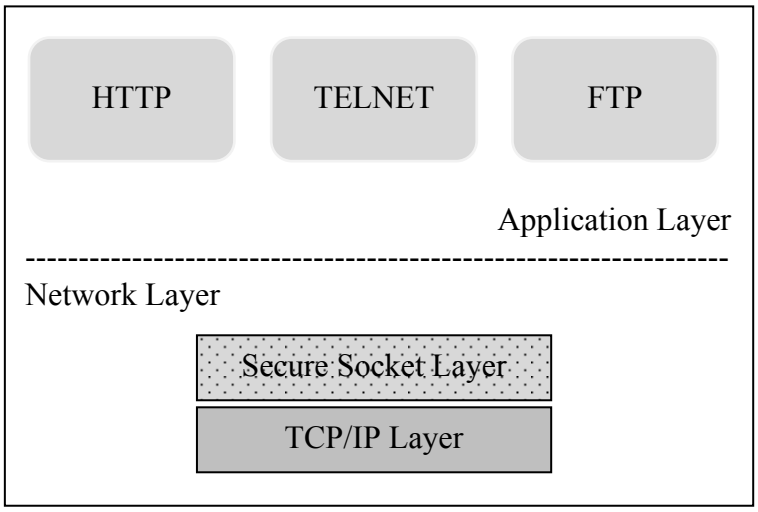
Protokol SSL

Protokol SSL (Secure Socket Layer) vytvořila firma Netscape. Firma Microsoft vytvořila podobný protokol PCT. V praxi se však ujal protokol SSL verze 3. Avšak oficiálním protokolem internetu se stal protokol TLS (Transport Layer Security) protokol, který je obdobou protokolu SSL verze 3.

Protokoly TLS a SSL jsou si podobné, avšak klient TLS se nedomluví se serverem SSL a naopak. Proto klient i server musejí být nakonfigurováni pro podporu protokolu SSL nebo protokolu TLS.

Protokol SSL zajišťuje soukromí a spolehlivost pro komunikující aplikace, chrání data před odposloucháváním, zfalšováním a paděláním.

Na obr. 5 je vidět uspořádání pozice protokolu SSL v modelu TCP/IP. SSL je podvrstvou mezi TCP/IP a aplikací. Podvrstva SSL zajišťuje šifrování PDU (Protokol Data Unit) aplikační vrstvy.



obr. 5 Pozice protokolu SSL v TCP/IP modelu

Komunikace protokolem SSL/TLS mezi klientem a serverem je plně duplexní, tj. skládá se z komunikace od klienta na server a v opačném směru ze serveru na klienta. Pro šifrování se používá symetrická šifra. Server předá klientovi svůj veřejný klíč. Po přijetí klientem jsou data dešifrována a použita. O šifrování se stará webový prohlížeč. Činnost je zobrazena pomocí žlutého visacího zámku v prohlížeči na staré liště. Takto je uživatel informován, že jeho komunikace probíhá bezpečně (šifrovaně).

Informace o použitém certifikátu máme možnost přečíst poklikem na ikonu visacího zámku.

SSL je protokol dělený na vrstvy.

Dvě vrstvy jsou hlavní:

- SSL Handshake Protocol je zodpovědný za vytvoření bezpečné komunikace mezi klientem a serverem. To je dáno na základě ověření a odsouhlasení šifrovacího algoritmu a klíčů.
- SSL Record Protocol je zodpovědný za zabalení dat protokolů vyšší vrstvy (např. HTTP, Telnet, FTP a další).

Hlavní přínosy SSL:

Bezpečnost šifrování – hlavním přínosem protokolu SSL je ustavení bezpečného spojení mezi dvěma komunikujícími uzly. Jakmile jsou iniciačním algoritmem vyměněny bezpečné klíče, je používáno symetrické šifrování.

Spolehlivost - přenos zprávy obsahuje kontrolu integrity dat prostřednictvím entity nazývané MAC (Message Authentication Code).

Interoperabilita - rozdílné aplikace různých programátorů by měly být schopny úspěšné výměny parametrů bez znalosti šifry aplikace druhé strany.

Rozšiřitelnost - struktura SSL umožňuje implementaci nových metod šifrování a výměny veřejných klíčů.

Relativní efektivita - šifrovací operace jsou dost náročné na vytížení procesoru; SSL se snaží tuto zátěž kompenzovat přídavnými funkcemi jako je např. komprimace dat nebo kešování spojení (umožní omezení počtu spojení iniciovaných vždy od začátku).

Protokol IPsec

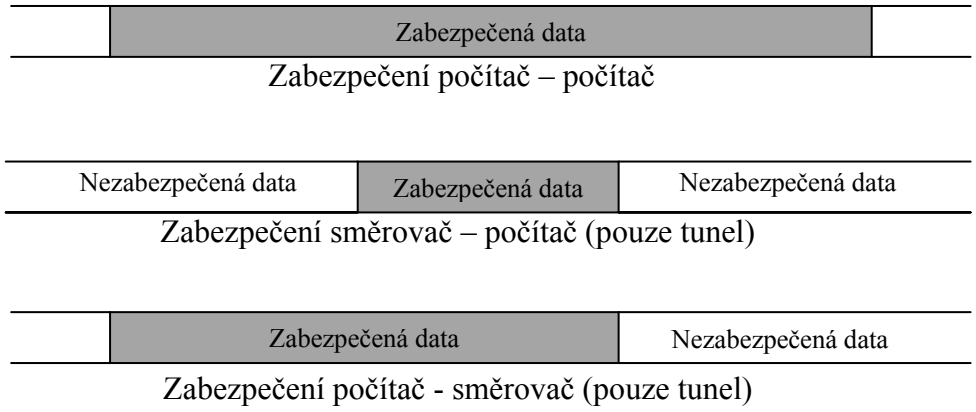
Protokol IPsec patří mezi protokoly specifikující zabezpečení komunikace na úrovní protokolu IP tzn. zabezpečení jednotlivých IP datagramů. V architektuře OSI se jedná o zabezpečení na síťové vrstvě. Výhodou tohoto zabezpečení je to, že se děje na úrovni operačního systému. Aplikace tímto nemusí o zabezpečení ani vědět a nemusí být upravovány, IPsec však nezabezpečuje data mezi uživateli či aplikacemi na týmž počítači.

Zabezpečení nemusí vždy probíhat na úrovni operačního systému vlastního počítače. Může se provádět na úrovni hraničního směrovače naší sítě.

IPsec je specifikován v RFC-2401 až RFC-2412. V minulosti firma CISCO zavedla svůj vlastní standard pod názvem Cisco Encryption Technology (CET). Dnes firma Cisco podporuje jak formát CET tak IPsec. Současně spolupracuje s firmou Microsoft v oblasti IPsec.

Na obr. 6 jsou znázorněny základní modely komunikace IPsec, kde komunikace může být zabezpečena:

- Mezi dvěma koncovými počítači (nepoužívá se).
- Mezi dvěma směrovači. Na obou koncích sítě máme podnikovou LAN či WAN, a komunikace probíhá přes Internet. Jestliže máme více takových sítí, pak komunikace probíhá pomocí tunelů.
- Mezi počítačem a směrovačem. Např. zaměstnanec přistupuje z domova, či na cestách pomocí internetu, do podnikové sítě (intranetu).



obr. 6 Základní modely komunikace IPsec

Ověřování - při přijetí paketu může dojít k ověření, zda vyslaný paket odpovídá odesílateli či zda vůbec existuje.

Šifrování - obě strany se předem dohodnou na formě šifrování paketu. Poté dojde k zašifrování celého paketu krom IP hlavičky, případně celého paketu a bude přidána nová IP hlavička.

Základní protokoly:

Authentication Header (AH) - zajišťuje autentizace odesílatele a příjemce, integritu dat v hlavičce, ale vlastní data nejsou šifrována.

Encapsulation payload security (ESP) - přidává šifrování paketů

Nevýhodou protokolu IPsec je, že je příliš složitý a implementace je náchylná k chybám. IPsec se rozšířil díky návaznosti na protokol IP verze 6.

Jestliže je na konci zabezpečené sítě směrovač, používá se výhradně tunel. Jednotlivé modely lze kombinovat.

2.9 Autentizace a autorizace

Ověření uživatele, neboli tzv. autentizace uživatele, je jednou z hlavních oblastí zabezpečení elektronického bankovnictví. Banka má pomocí autentizace uživatele (uživatele) jistotu, že ověřovaný uživatel je klientem banky.

Pro ověřování klientů používají banky v České republice nejčastěji tyto způsoby autentizace:

a) Uživatelské jméno a heslo

Ověření pomocí uživatelského jména a hesla je nejčastějším prvkem zabezpečení. Jedná se však o nejslabší zabezpečení. I když se většina bank snaží, aby heslo obsahovalo různá písmena, číslice či kombinaci znaků, stále se jedná o nejjednodušší zabezpečení.

b) Certifikát

Uživatel má vydaný platný osobní certifikát (bankou autorizovaný veřejný RSA klíč uživatele, délky 1024 bitů). Tento certifikát se používá pro navázání komunikace se serverem banky a pro podepisování aktivních operací uživatele.

Veškerá komunikace probíhá v protokolu SSL (SSL – Secure Socket Layer). Všechna data jsou šifrována silným symetrickým šifrovacím algoritmem a to standardně s využitím 128-bit šifrovacího klíče – typ a případně délka použitého šifrovacího klíče závisí na nastavení na straně uživatele, šifrovací klíč je jedinečný - platný pro dané připojení k serveru banky.

Pro podepisování aktivních operací uživatelem se používá elektronický podpis (k vytvoření elektronického podpisu se používá osobní certifikát uživatele – RSA algoritmus).

Osobní certifikát může mít uživatel uložený ve svém počítači, na disketě, na přenosném paměťovém médiu (flash disk) či na čipové kartě.

Přístup k osobnímu certifikátu uživatele je chráněn heslem, které si určuje a které zná pouze uživatel, nebo PINem v případě čipové karty.

Zabezpečení vnitřní sítě uživatele při přístupu na síť Internet si zajišťuje uživatel a je nezávislé na aplikaci internetových bank.

c) Čipová karta

Klientský certifikát je uložený na čipové kartě a umožňuje generovat jedinečný klíč, který ověřuje platnost prováděných operací. Čipovou kartu s certifikátem je potřeba vložit do čtečky čipových karet v počítači. Klientský certifikát se používá jak

pro přihlášení do služby internetového bankovnictví, tak pro autorizaci aktivních transakcí.

Platný klientský certifikát na čipové kartě je podmínkou pro jeho využití pro přihlášení do aplikace a autorizaci transakcí v internetovém bankovnictví.
Certifikát uložený na čipové kartě má z bezpečnostních důvodů omezenou platnost na 12 měsíců. Zbývající platnost certifikátu se může ověřit na obrazovce . Před vypršením platnosti certifikátu je nutné certifikát prostřednictvím správce certifikátu obnovit.
V případě, že se certifikát nevyužívá, může se jeho platnost odvolat.

d) SMS kód

Každý přístup do elektronického bankovnictví pomocí mobilního telefonu je zajištěn bankovním pinem, který si uživatel může kdykoliv změnit.

Pro přihlášení na účet nebo zadávání transakcí je třeba připojit bezpečnostní kód, kterým se potvrdí oprávněnost pracovat s účtem a správnost údajů v zadané transakci. Tento kód se jednoduše zasílá bezpečnou SMS (uživatelem povolenou, schválenou) zprávou na displej telefonu a klient banky jej pouze přepíše do příslušné kolonky ve formuláři operace.

Pro šifrování dat v GSM sítích se používá symetrický algoritmus A5 (existuje v několika variantách). Tímto algoritmem jsou šifrována pouze data mezi telefonem a základnovou stanicí (BTS). Z toho vyplývá, že organizace spravující infrastrukturu GSM má přístup k dešifrovaným datům (samotný operátor u SMS uchovává minimálně informace o odesílateli a příjemci zprávy a datum). Šifrování přenášených dat však není povinná vlastnost sítě a není obtížné ji také obejít. Proto jsou zprávy odesílané v rámci GSM bankingu navíc šifrované SIM toolkitem se sdíleným symetrickým klíčem uloženým v bance a na SIM kartě.

e) Autentizační kalkulátor

Autentizační kalkulátor je zařízení, které umožňuje zvýšit bezpečnost služeb přímého bankovnictví. Tento kalkulátor se používá pro generování dvou typů kódů. Autentizační kód uživatele slouží k jeho identifikaci, podobně jako třeba heslo (PIN). Úroveň bezpečnosti při použití autentizačního kódu uživatele je však podstatně vyšší. Autentizační kód zprávy (MAC) se používá pro zabezpečení zpráv – příkazů, které uživatel odesílá do banky.

Způsob využití autentizačního kalkulátoru vychází z principu jednotlivých služeb přímého bankovnictví.

Autentizační kalkulátor je proti svému zneužití sám chráněn bezpečnostním heslem - PIN. Pro první použití kalkulátoru je nastaveno prvotní PIN.

Autentizační kalkulátor má neomezenou platnost používání.

Autentizační kód uživatele

Kalkulátor generuje posloupnost kódů v závislosti na interních parametrech kalkulátoru (unikátních pro každý kalkulátor). Obě komunikující strany znají interní parametry kalkulátoru, přičemž je zajištěno, že tyto parametry nejsou známy třetí straně. Na základě předchozích kódů nelze (bez znalosti interních parametrů kalkulátoru) vypočítat (ani předpovědět) kód následující.

Odesilatel (uživatel) vygeneruje pomocí svého kalkulátoru autentizační kód, který předá příjemci (například bance). Autentizační server příjemce vypočte očekávaný kód a porovnáním ověří identitu odesilatele.

Autentizační kód zprávy (MAC)

Funkce generování autentizačního kódu zprávy (MAC) je v principu podobná generování autentizačního kódu uživatele. Interní parametry kalkulátoru jsou pro generování MAC doplněny vybranými údaji zprávy (částka, číslo účtu protistrany apod.). Odesilatel vygeneruje autentizační kód (MAC) a spolu se zprávou jej předá příjemci. Příjemce vypočte očekávaný kód a porovnáním ověří identitu odesilatele a integritu zprávy (pokud byl modifikován některý z chráněných údajů, tj. údajů zadaných pro výpočet kódu, kód nebude odpovídat).

2.10 Zabezpečení na straně klienta

Může se zdát, že se v datech přenášených mezi bankou a uživatelem, žádné důležité informace neskrývají. To je však omyl. Je zapotřebí si uvědomit, jaká výměna dat může mezi bankou a uživatelem probíhat.

Možné informace přenášené mezi bankou a uživatelem:

- vstupní data z klávesnice, myši, tabletu či z dotykové obrazovky)
- obsah zobrazovaných oken
- řídicí a stavové informace
- data k ověření přístupových práv

Největší riziko nesou data z klávesnice (např. psaní hesla) Řešením je, že musíme data šifrovat.

Pro klasickou (textovou) terminálovou emulaci se všeobecně zavedl systém Secure Shell (SSH), který je na systému GNU/Linux reprezentován variantou OpenSSH.

Jednou z významných oblastí použití SSH je také zabezpečení přenosu dat. K tomu, abychom mohli využít SSH k šifrování dat, je třeba jednak donutit aplikace, aby toto šifrování používaly, a současně zajistit bezproblémové ověření přístupových práv. Na straně banky (tam, kde poběží aplikace) musí být k dispozici (nainstalován) SSH server a musí být "použitelný" - tedy spuštěný jako démon nebo spouštěný pomocí inetd, resp. xinetd. Na PC, u kterého uživatel sedí, musí být nainstalován SSH klient. Při správném nastavení (viz dále) pak proces probíhá následovně:

1. Uživatel se přihlásí na klientský stroj pomocí ssh.
2. Je-li nastavena proměnná DISPLAY, systém SSH vykoná automaticky následující kroky.
3. Vytvoří se spojení s reálným (vzdáleným) X serverem pomocí šifrovaného kanálu.
4. Šifrovaným kanálem se přenášejí i data pro ověření totožnosti ("reálné" ověření identity se však provádí na klientském stroji, původní autentizační data se na server nepřenášejí).
5. Na straně klienta se vytvoří virtuální X server (X proxy) a nastaví se na něj proměnná DISPLAY.
6. Spouštěné aplikace využívají implicitně tento virtuální server a data tedy putují šifrovaným kanálem.
7. Po skončení relace ssh opět automaticky zruší X proxy, vrátí proměnnou DISPLAY na původní hodnotu a zlikviduje uložená autentizační data.

Pro šifrování SSH existuje několik dobrých důvodů, proč tuto technologii používat:

- kvalitní šifrování, výběr z několika různých algoritmů (3DES, Blowfish, ARS a další)
- řada metod autentizace (založených hlavně na RSA), včetně ověřování totožnosti serveru
- zabudovaná komprese přenášených dat
- šifrované kanály ("tunely") pro X i další služby (na SSH lze vybudovat i jednoduchou virtuální privátní síť)
- plnohodnotná náhrada klientských aplikací typu telnet, rsh, rlogin, rcp apod.
- podpora spolupráce se systémem Kerberos

Jsou vytvořeny obecné zásady, které by měl každý znát (a leckdo také zná, byť se jimi třeba neřídí):

- **princip minimality práv** - každý uživatel (nebo každý program) má mít jen taková práva, která jsou nezbytně nutná pro jeho činnost
- **princip nedůvěry** - každé síťové prostředí musí být vždy považováno za nebezpečné z hlediska všech možných bezpečnostních rizik; každý program musí být považován za (bezpečnostně) děravý
- **princip implicitního zákazu** - implicitním chováním musí být odepření přístupu; je-li podmínek přístupu více, každá se musí uplatnit tímto způsobem
- **princip bezpečného zotavení** - při výjimečné situaci (chybě apod.) musí být reakcí odepření přístupu; nelze predikovat úmysly uživatele/programu

Při hodnocení bezpečnosti samozřejmě musíme brát v úvahu také ekonomická hlediska - nejen investici do zabezpečení, ale také systémovou režii (zátěž systému vzniklou zabezpečením).

3 ANALÝZA ELEKTRONICKÉHO BANKOVNICTVÍ

3.1 Dílčí analýza

Bankovní data jsou velmi citlivou záležitostí, proto jí banky věnují náležitou pozornost. Zabezpečení bankovních informací můžeme rozdělit do několika kategorií:

- identifikace banky
- šifrování údajů
- internetové prohlížeče
- ověření uživatele
- zabezpečení transakcí
- cena zabezpečení
- bezpečnostní zásady.

3.2 Identifikace banky

Je nutné si ověřovat identifikaci nejen zákazníka, ale i samotného bankovního ústavu. V České republice je u všech bank použit protokol SSL. Bankovní ústav se prokáže internetovému prohlížeči ověřeným SSL certifikátem, který obsahuje identifikační údaje potřebné pro ověření totožnosti banky.

Všechny mnou ověřované banky používají délku šifrovaného klíče 128 bitů. Většina bank (83,4%) používá jako certifikační autoritu fy VeriSign. Ve dvou případech se jedná o První certifikační autoritu (ČSOB a Poštovní spořitelna). ČSOB je vlastníkem Poštovní spořitelny, a proto je jejich elektronické bankovnictví podobné.

Banka	Délka šifrovacího klíče	Veřejný klíč	Algoritmus podpisu	Vystavitel	Uložení klíčů
BAWAG Bank CZ, a.s.	128	1024	sh1RSA	Verisign	-
Citibank, a.s.	128	1024	sha1RSA	Verisign	-
Česká spořitelna, a.s .	128	1024	sha1RSA	Verisign	-
Československá obchodní banka, a.s.	128	1024	sha1RSA	I.CA	-
eBanka, a.s.	128	1024	sha1RSA	Verisign	-
GE Money Bank, a.s.	128	1024	sha1RSA	Verisign	-
ING Bank N.V.	128	1024	sha1RSA	Verisign	-
Komerční banka, a.s.	128	1024	sha1RSA	Verisign	čipová karta
Poštovní spořitelna, a.s.	128	1024	sha1RSA	I.CA	-
Raiffeisenbank, a. s.	128	1024	sha1RSA	Verisign	-
UniCredit Bank Czech Republic, a.s.	128	1024	sha1RSA	Verisign	-
Volksbank CZ, a.s.	128	1024	sha1RSA	VeriSign	-

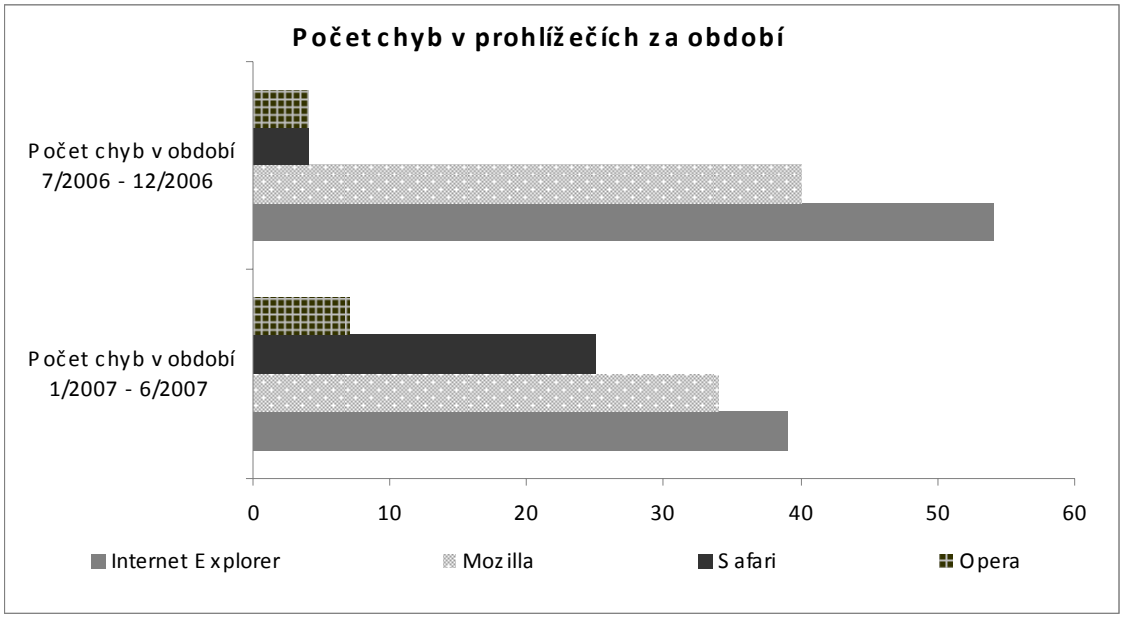
Tab.1 Identita banky

3.3 Internetové prohlížeče

Z uživatelské části je nejdůležitější internetový prohlížeč. Proto jsem se zabýval i jeho bezpečností. Internetový prohlížeč by měl být nenapadnutelný a vhodně zabezpečen. K zabezpečení se používají antivirové programy, odstraňovače spyware či malware. Dalším důležitým krokem je, aby uživatel používal bezpečný a ověřený počítač, který má k dispozici jen on sám. Internetový prohlížeč může být ohrožen jednou z bezpečnostních děr, která vznikne v průběhu vývoje. Útočník tak může přesměrovat obsah stránky na jiný server, tzv. podvrhnutí stránky. Uživatel by měl pravidelně aktualizovat svůj operační systém a internetový prohlížeč. Včasným záplatováním může předejít velkým škodám.

Internetový prohlížeč	Počet chyb v období 1/2007 - 6/2007	Počet chyb v období 7/2006 - 12/2006	+ Opraveno chyb - Nové chyby
Internet Explorer	39	54	15
Mozilla	34	40	6
Safari	25	4	-21
Opera	7	4	-3

Tab. 2 Počet chyb v prohlížečích za období



Graf 1 Počet chyb v prohlížečích za období

3.4 Ověření uživatele

V České republice bankovní ústavy používají k ověřování tzv. autentizaci nejčastěji přihlašování pomocí uživatelského jména a hesla (celkem v devíti případech). Dalším velmi častým autentizačním procesem je přihlašování pomocí autentizačního kalkulátoru či certifikátu (shodně ve čtyřech případech).

Mimo tyto přihlašovací procedury se osvědčilo přihlašování pomocí certifikátu uloženého na čipové kartě (tři případy), či pomocí kódu zaslaného na mobilní telefon formou bezpečné SMS (ve dvou případech).

Autentizace uživatelským jménem a heslem:

Základním typem autentizace je přihlášení pomocí přiděleného klientského čísla a hesla. Heslo zadané klientem se na server neposílá v čitelné podobě, posílá se jeho hash. Hesla musejí být alespoň x-znaků dlouhá a musejí obsahovat určitou kombinaci písmen či číslic. Samozřejmostí je citlivost na velikost písmen. Hesla mohou být až x-znaků dlouhá. Aplikace kontroluje interval od poslední změny hesla a doporučuje klientovi jeho změnu. Změnu hesla je možné provést přímo v aplikaci po přihlášení, pro změnu je nutné znát staré heslo. Po x-pokusech o změnu hesla a nezadání správného

starého hesla dojde k zablokování uživatele a odhlášení z aplikace. Např. Česká spořitelna, a.s. používá v internetovém bankovnictví na stránkách www.servis24.cz možnost napsat heslo pomocí grafické klávesnice. Grafická klávesnice není na obrazovce na pevném místě, zobrazuje se náhodně posunutá. Cílem grafické klávesnice je omezit nebezpečí odposlechnutí hesla pomocí keylogeru.

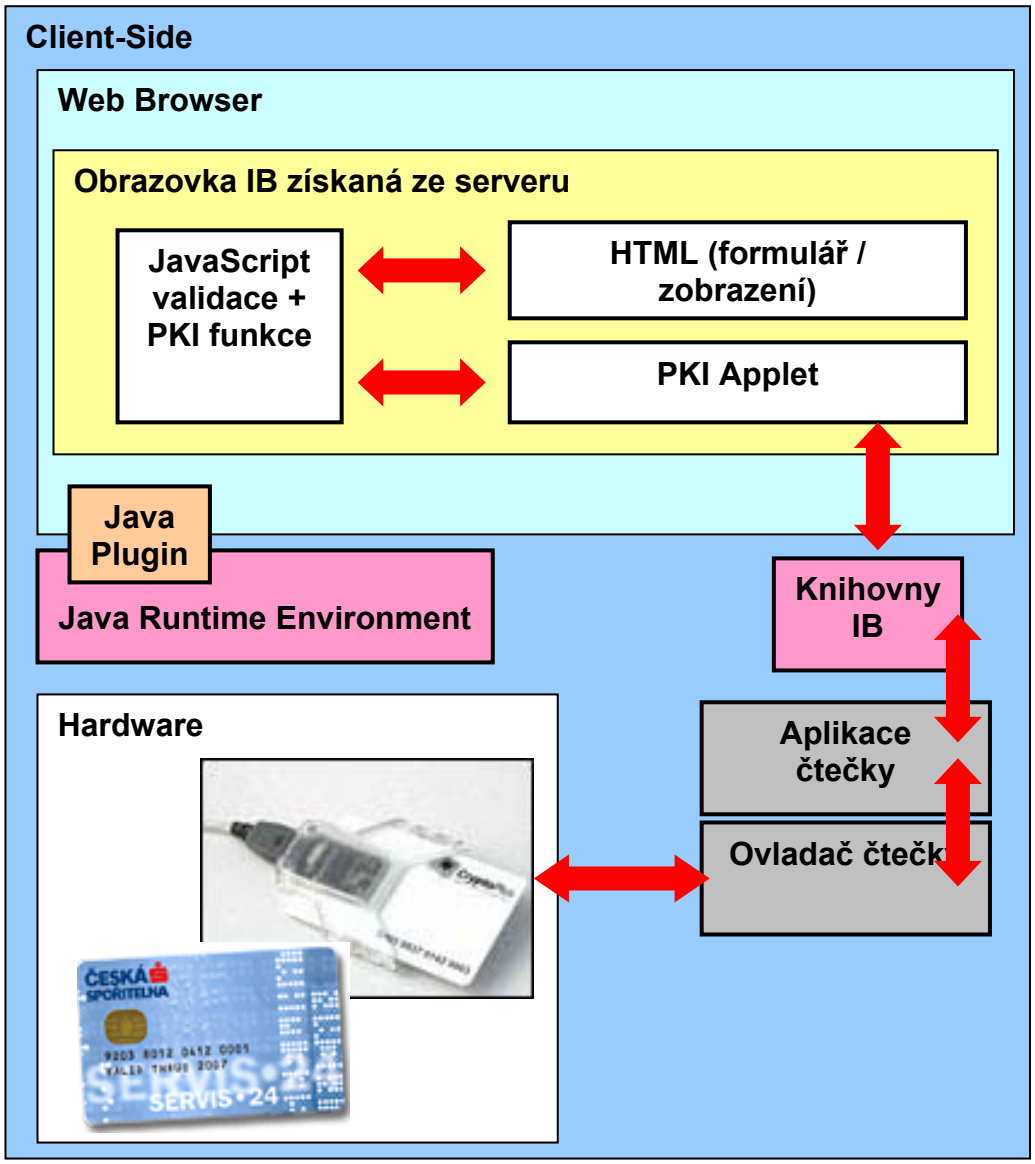
Autentizace autentizačním kalkulátorem:

Autentizační kalkulátor neboli AK je forma vyšší bezpečnosti. AK vypadá jako kalkulačka, má jednoznačné identifikační číslo a integrované hodiny reálného času. Umí na základě času a případně dalších zadaných parametrů transakce vygenerovat číselný kód platný jen omezenou dobu, jehož platnost ověřuje speciální komponenta na straně banky. Zadáním vygenerovaného číselného kódu se dá potvrdit transakce nebo je použitelný i jako doplňková bezpečnost při přihlášení. Nevýhodou AK je nutnost ručního zadávání parametrů transakce do kalkulačky, což je použitelné jen pro několik základních typů transakcí, jako je příkaz k úhradě nebo inkasu.

Autentizace klientským certifikátem:

Další formou vyšší bezpečnosti je osobní certifikát uložený na čipové kartě, označovaný jako PKI (Public Key Infrastructure). Tento způsob je považovaný za nejbezpečnější a současně nejsnáze použitelný. Používá se nejen k potvrzování transakcí ale také k plnohodnotnému přihlášení, není tedy současně nutné zadávat jméno a heslo jako u AK. Osobní certifikát je vydáván nejčastěji I. Certifikační Autoritou, zkratkou ICA. Certifikát se vydává na období 1 rok a po vypršení platnosti je nutné vystavit nový za poplatek přes 300 korun. Čipová karta funguje nejen jako bezpečné úložiště klíčů ale obsahuje také procesor zajišťující generování certifikátů a veškeré algoritmy pro šifrování a dešifrování dat. Pro přístup k uloženým klíčům je nutné zadat pin. Pro práci s čipovou kartou je potřeba k počítači připojit čtečku čipových karet. Čtečky existují od několika výrobců a připojují se většinou přes rozhranní USB. Aby bylo možné používat čipovou kartu z prohlížeče Internetových stránek, musí být na počítači nainstalováno několik SW komponent. Připojení čtečky do systému zajistí ovladač čtečky dodaný jejím výrobcem. Integrace šifrovacích funkcí do operačního systému má na starosti aplikace čipové karty. Poslední důležitou součástí bývá Applet spouštěný v prohlížeči jako součást obrazovky, která nějakým způsobem manipuluje s daty. Pro správnou funkci appletu je nutná Java, přesněji JRE. Mezi

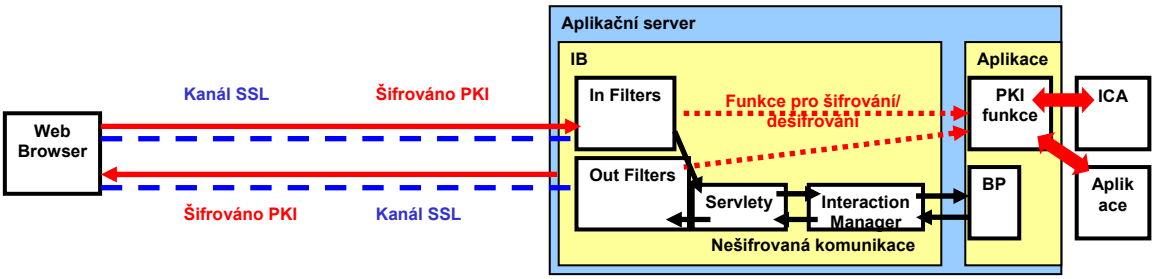
HTML stránkou a Appletem se data předávají pomocí JavaSriptu. Klient dostane veškeré HW i SW vybavení na pobočce banky a většinou si PKI zprovozní sám. Se správným fungováním PKI je spojená řada problémů, například odstranění knihoven při automatické aktualizaci Javy nebo nekompatibilita některých funkcí appletu s Javou.



obr. 7 Certifikát na čipové kartě

Veškerá komunikace prohlížeče s bankou probíhá šifrovaně protokolem SSL, aby nikdo nemohl důvěrná data cestou odchytit a prohlížet. PKI přidává navíc ještě jednu úroveň šifrování. To se ale nepoužívá všude, pouze na data zadávaná klientem. Autorizace vyšší bezpečností při použití PKI spočívá v tom, že klient odesílaná data podepíše privátním certifikátem z čipové karty. Právě kvůli podepsání musí klient na

žluté konfirmační obrazovce zadat pin. Podpis se kontroluje na straně banky proti veřejnému klíči klienta. Podepsaná data se navíc uschovají pro případ pozdějších reklamací. Internetové bankovní aplikace obsahují vestavěnou podporu pro manipulaci s certifikáty, takzvaný Správce certifikátů.



obr. 8 Správce certifikátů

Banka	*Uživatelské jméno a heslo*	*Certifikát*	*Čipová karta*	*SMS kód*	*PIN kalkulátor*
BAWAG Bank CZ, a.s.	ano		od 1/2008		
Citibank, a.s.					ano
Česká spořitelna, a.s .	ano		ano		ano
Československá obchodní banka, a.s.	ano		ano		
eBanka, a.s.		ano		ano	ano
GE Money Bank, a.s.	ano	ano		ano	
ING Bank N.V.	ano				
Komerční banka, a.s.		ano	ano		
Poštovní spořitelna, a.s.	ano				
Raiffeisenbank, a. s.	ano				
UniCredit Bank Czech Republic, a.s.	ano				ano
Volksbank CZ, a.s.	ano	ano			

Tab. 3 Autentizace

Zvláště u autentizace uživatelským jménem a heslem je důležitá jejich tvorba a podmínky na ně kladené. Uživatelské jméno a heslo je osobním tajemstvím uživatele a ten si je musí chránit. Nejčastější minimální délka uživatelského hesla je 8-10 znaků. U hesla je to rovněž délka minimálně 8 znaků (písmena či číslice). Podmínky kladené na tvorbu uživatelských jmen a hesel jsou v tabulce č. 4.

Banka	Uživatelské jméno	Heslo	
		Minimální délka	Musí obsahovat
BAWAG Bank CZ, a.s.	8 číslic	8 znaků	číslice, písmeno
Citibank, a.s.	8 - 30 číslic	8 znaků	číslice, písmeno
Česká spořitelna, a.s.	10 číslic	8 - 30 znaků	min 2 čísla a 2 písmena, zbytek libovolné
Československá obchodní banka, a.s.	8 číslic	5 znaků	Číslice
eBanka, a.s.	10 znaků	10 pro Osobní eKonto; 11 pro Mobilní eKonto	Číslice
GE Money Bank, a.s.	číslo účtu	5 - 10 znaků	libovolná kombinace
ING Bank N.V.	1 - 9	8 znaků	libovolná kombinace
Komerční banka, a.s.	certifikát	8 znaků	libovolná kombinace
Poštovní spořitelna, a.s.	8 číslic	5 znaků	Číslice
Raiffeisenbank, a. s.	8 - 15 znaků	8 - 15 znaků	číslice, písmeno
UniCredit Bank Czech Republic, a.s.	6 - 8 znaků	8 znaků	Číslice
Volksbank CZ, a.s.	8 číslic	8 znaků	číslice, písmeno

Tab. 4 Tvorba uživatelského jména a hesla

V případě, že uživatel zadá chybně heslo, má několik pokusů na opravu. Nejčastěji se vyskytuje možnost max. tří špatných pokusů, po kterých se internetové bankovnictví zablokuje (viz. tab. 5).

Banka	Počet pokusů do zablokování přístupu k účtu
BAWAG Bank CZ, a.s.	6
Citibank, a.s.	3 + 2 otázky
Česká spořitelna, a.s .	3
Československá obchodní banka, a.s.	3
eBanka, a.s.	3
GE Money Bank, a.s.	3 / 3 *
ING Bank N.V.	3
Komerční banka, a.s.	3 / 3 **
Poštovní spořitelna, a.s.	3
Raiffeisenbank, a. s.	6
UniCredit Bank Czech Republic, a.s.	3
Volksbank CZ, a.s.	6

* uživatelské jméno a heslo / certifikát
* při vstupu na účet přes certifikát se po třech pokusech jen zavře okno prohlížeče / čipová karta se zablokuje

Tab. 5 Počet pokusů do zablokování přístupu k účtu

Odblokování hesla u různých bankovních ústavů se provádí např. telefonicky, na pobočce či pomocí internetového chatu např. GE Money Bank.. Nejčastějším typem

odblokování je zavolání do call center bank (telefonicky). Což je výhodné např. pro uživatele, kteří jsou v zahraničí.

Banka	*Nejjednodušší způsob odblokování účtu*
BAWAG Bank CZ, a.s.	faxová žádost
Citibank, a.s.	telefonicky - ověření čísla karty, 2 čísla z 6 místného PINu
Česká spořitelna, a.s .	telefonicky - klientské číslo, bezpečnostní heslo a bezpečnostní kód
Československá obchodní banka, a.s.	na pobočce - při zablokování čipové karty se vydá nová
eBanka, a.s.	na pobočce - při zablokování autentizačního kalkulátoru
GE Money Bank, a.s.	na pobočce, chat, telefonicky
ING Bank N.V.	Telefonicky
Komerční banka, a.s.	telefonicky - při zablokování čipové karty
Poštovní spořitelna, a.s.	na pobočce
Raiffeisenbank, a. s.	telefonicky, na pobočce
UniCredit Bank Czech Republic, a.s.	telefonicky, na pobočce
Volksbank CZ, a.s.	Telefonicky

Tab. 6 Odblokování účtu

Další důležitým kritériem pro výběr vhodné banky, je doba do automatického odhlášení uživatele z internetového bankovnictví. Nejčastějším časem pro automatické odhlášení z internetového bankovnictví je 10 minut.

Banka	*Doba do automatického odhlášení klienta*
BAWAG Bank CZ, a.s.	5 min.
Citibank, a.s.	10 min.
Česká spořitelna, a.s .	10 min.
Československá obchodní banka, a.s.	20 min.
eBanka, a.s.	není určena
GE Money Bank, a.s.	10 min.
ING Bank N.V.	10 min.
Komerční banka, a.s.	20 min.
Poštovní spořitelna, a.s.	20 min.
Raiffeisenbank, a. s.	neuvedena
UniCredit Bank Czech Republic, a.s.	20 min.
Volksbank CZ, a.s.	10 min.

Tab. 7 Doba odpojení

3.5 Autorizace transakcí

Samotné transakce lze autorizovat podobně jako u autentizace čtyřmi způsoby. Nejčastější je autorizace pomocí SMS kódu. Toto zabezpečení je i z hlediska technologického poměrně „levná a bezpečná“ záležitost. Složitějším ale zároveň dosti využívaným zabezpečením transakcí je klientský certifikát (ve čtyřech případech). Další způsob zabezpečení transakcí je prostřednictvím čipové karty či autentizačního kalkulátoru.

Banka	*Certifikát*	*Čipová karta*	*SMS kód*	*PIN kalkulátor*
BAWAG Bank CZ, a.s.	Ano	-	-	-
Citibank, a.s.	-	-	-	-
Česká spořitelna, a.s .	-	Ano	Ano	Ano
Československá obchodní banka, a.s.	-	Ano	Ano	-
eBanka, a.s.	Ano	-	Ano	Ano
GE Money Bank, a.s.	Ano	-	Ano	-
ING Bank N.V.	-	-	-	-
Komerční banka, a.s.	Ano	Ano	-	-
Poštovní spořitelna, a.s.	-	-	Ano	-
Raiffeisenbank, a. s.	Ano	-	Ano	-
UniCredit Bank Czech Republic, a.s.	-	-	-	Ano
Volksbank CZ, a.s.	Ano	-	-	-

Tab. 8 Autorizace transakcí

Celkem sedm bank informuje dostatečně uživatele internetového bankovnictví na svých stránkách o certifikačních pravidlech a postupech práce s certifikáty viz. tab. 9. Mezi důležité informace patří způsob a postup jak získat certifikát, co je k získání třeba a jak a kde se odvolat, za co banka ručí a za co ne. Dále sem patří pravidla chování a povinnosti banky, ale i samotného uživatele.

Banka	Zveřejněná pravidla banky na internetových stránkách banky
BAWAG Bank CZ, a.s.	Ne
Citibank, a.s.	Ano
Česká spořitelna, a.s .	Ano
Československá obchodní banka, a.s.	Ano
eBanka, a.s.	Ano
GE Money Bank, a.s.	Ano
ING Bank N.V.	Ne
Komerční banka, a.s.	Ano
Poštovní spořitelna, a.s.	Ano
Raiffeisenbank, a. s.	Ne
UniCredit Bank Czech Republic, a.s.	Ne
Volksbank CZ, a.s.	Ne

Tab. 9 Zveřejněná pravidla banky

3.6 Cena zabezpečení pro uživatele

Důležitým faktorem pro výběr vhodné banky je cena za služby elektronického bankovnictví. Nejlevnější ale vždy neznamená nejlepší. Vyšší úroveň zabezpečení stojí banky nemalé peníze. Všechny banky neúčtují vstupní poplatek za zřízení účtu. U vedení účtu je cena určena podle různě nabízených balíčků za služby a s tím spojené zpoplatnění služby. Je na uživateli, pro jakou službu či balíček se rozhodne podle vlastních potřeb.

Banka	Zřízení účtu	Vedení účtu
BAWAG Bank CZ, a.s.	0 Kč	30 Kč
Citibank, a.s.	0 Kč	99 Kč
Česká spořitelna, a.s .	0 Kč	25 Kč *
Československá obchodní banka, a.s.	0 Kč	40 Kč
eBanka, a.s.	0 Kč	0 / 20 / 89 Kč **
GE Money Bank, a.s.	0 Kč	39 Kč
ING Bank N.V.	0 Kč	0 Kč
Komerční banka, a.s.	0 Kč	44 Kč
Poštovní spořitelna, a.s.	0 Kč	0 Kč
Raiffeisenbank, a. s.	0 Kč	35 Kč
UniCredit Bank Czech Republic, a.s.	0 Kč	50 Kč
Volksbank CZ, a.s.	0 Kč	30 Kč

* sporožirové účty včetně telebankingu
** mob. elek. klíč / internet. elek. klíč / osobní elek. klíč

Tab. 10 Cena za vedení a zřízení

U nadstandardního zabezpečení je u služeb nabízených bankami například zpoplatněn nákup autentizačního (PIN) kalkulátoru, či čipové karty včetně čtečky.

Banka	Nadstandardní zabezpečení (aktivace / zřízení)	
	PIN kalkulátor	Čipová karta + čtečka
BAWAG Bank CZ, a.s.	-	-
Citibank, a.s.	-	-
Česká spořitelna, a.s .	-	990 Kč
Československá obchodní banka, a.s.	0 Kč	100 + 500 Kč
eBanka, a.s.	89 Kč / za měsíc	-
GE Money Bank, a.s.	-	-
ING Bank N.V.	-	-
Komerční banka, a.s.	-	390 + 1000 Kč
Poštovní spořitelna, a.s.	-	-
Raiffeisenbank, a. s.	-	-
UniCredit Bank Czech Republic, a.s.	50 Kč / za měsíc	-
Volksbank CZ, a.s.	-	-

Tab. 11 Cena za nadstandard

U bank, které nabízejí podpisové certifikáty, je důležité znát cenu za obnovu certifikátu. Nejdražší je v tomto případě Česká spořitelna, a.s., eBanka, a.s. či ČSOB, a.s.

Banka	Obnova certifikátu
BAWAG Bank CZ, a.s.	0 Kč
Citibank, a.s.	-
Česká spořitelna, a.s .	320 Kč
Československá obchodní banka, a.s.	100 Kč
eBanka, a.s.	200 Kč
GE Money Bank, a.s.	0 Kč
ING Bank N.V.	-
Komerční banka, a.s.	0 Kč
Poštovní spořitelna, a.s.	-
Raiffeisenbank, a. s.	0 Kč
UniCredit Bank Czech Republic, a.s.	-
Volksbank CZ, a.s.	0 Kč

Tab. 12 Obnova certifikátu

V neposlední řadě je dobré vědět výši zpoplatnění zasílání zpráv, např. prostřednictvím e-mailu, SMS, faxu či dopisu. Nejlevnější varianta je zasílání zpráv na e-mail a rovněž formou SMS zpráv.

Uvedené ceny za služby jsou ceny pro uživatele internetového bankovnictví.

Banka	Zasílání zpráv			
	E-mail	SMS	Fax	Dopis
BAWAG Bank CZ, a.s.	-	-	-	-
Citibank, a.s.	-	-	-	-
Česká spořitelna, a.s .	0 Kč	1 Kč	10 Kč	15 Kč + poštovné
Československá obchodní banka, a.s.	1 Kč	1 Kč	-	-
eBanka, a.s.	0 Kč	3,90 Kč	20 Kč	20 Kč
GE Money Bank, a.s.	-	2,50 Kč	6 Kč	-
ING Bank N.V.	-	-	-	-
Komerční banka, a.s.	0 Kč	1,50 Kč	0 Kč	35 Kč
Poštovní spořitelna, a.s.	0 Kč	3 Kč	-	-
Raiffeisenbank, a. s.	1 Kč	3 Kč	-	-
UniCredit Bank Czech Republic, a.s.	0 Kč	0 / 1,90 Kč *	-	-
Volksbank CZ, a.s.	-	-	-	-

* Konto Pohoda (v balíčku je 5 SMS zdarma), každá další SMS je za 1,90 Kč

Tab. 13 Zasílání zpráv

3.7 Bezpečnostní zásady

Ochranný systém internetového bankovnictví musí účinně plnit svou funkci v celém rozsahu a data uživatelů nemohou být při komunikaci s bankou nikým zneužita. Proto je doporučeno dodržovat jednoduché bezpečnostní zásady:

1) Využívat aktivně kombinace všech bezpečnostních prvků služeb elektronického bankovnictví (heslo, autorizační SMS, limity účtu, zasílání SMS zpráv o nových aktivních transakcích, autentizační kalkulátor, klientský certifikát, čipovou kartu).
2) Chránit důsledně přihlašovací údaje (klientské číslo a heslo) před dalšími osobami.
3) Heslo nevolit snadno odhadnutelné (např. 12345678). Doporučuje se heslo, které je kombinací alfanumerických znaků. Heslo musí obsahovat alespoň dva numerické znaky a alespoň dva alfa znaky.
4) Heslo pro internetové bankovnictví se doporučuje často obměňovat.
5) Využívat autorizační SMS, když to umožňuje samotné internetové bankovnictví.
6) Využívat možnosti aktivace zasílání SMS o transakcích zadaných pomocí přihlašovacích údajů.
7) Uživatelům, kteří provádějí aktivní transakce ve veřejných prostorách, je doporučeno používat pro přihlášení jeden z typů vyššího zabezpečení.
8) Nedoporučuje se přihlašovat do internetového bankovnictví v nedůvěryhodném prostředí, tedy tam, kde není plně zajištěno uživatelovo soukromí a kde zadávání uživatelových přihlašovacích údajů může někdo odpozorovat.
9) Po odhlášení z internetového bankovnictví uživatel musí zavřít všechny stávající okna prohlížeče a pro další případnou práci otevřít prohlížeč znovu.
10) Uživatel nesmí nikdy sdělovat přihlašovací údaje (uživatelské jméno a heslo) při ústní a telefonické komunikaci a neuvádět jej v písemné komunikaci (dopis; e-mail). Heslo je jen uživatelovo a je v jeho zájmu, aby jej neznal nikdo jiný: ani kolegové v práci či rodinní příslušníci. Heslo nesdělujte ani operátorovi podpory služeb internetového bankovnictví různých bank.

Banka je chráněna proti napadnutí svých systémů účinnou kombinací hardwarových a softwarových obranných prvků, jakými jsou firewally, detektory průniku nebo oddělením jednotlivých informačních systémů od přístupu z Internetu.

Účinnost těchto ochran je pravidelně kontrolována v souladu se zásadami bezpečnostní politiky banky.

Doporučení pro uživatele IB: v případě pochybností je vhodné volat banku, a to na telefonní číslo z tištěných materiálů banky či telefonního seznamu. Telefonní číslo uvedené na falešné e-mailové výzvě nebo na stránkách, kam uživatelova zpráva odkáže, může vést k podvodníkovi.

Uživateli je doporučeno vybírat takovou banku, která používá dostatečné metody autorizace (například SMS, čipová karta). Nesmí se instalovat neznámé programy, není dobré navštěvovat nedůvěryhodné stránky, je nutné používat aktualizovaný antivirový program a osobní firewall.

3.8 Trendy a vývoj elektronického bankovnictví

Banky se snaží nabídnout svým klientům co nejrozmanitější způsoby komunikace s jejich účty. Přesto ale elektronické bankovnictví rozhodně neznamená konec bankovních poboček. Jedním z důvodů je i to, že zájem o využívání nových komunikačních kanálů – jak internetu, tak mobilních technologií – roste. Ale existuje část obyvatelstva, která nebude ochotna tyto nové technologie přijmout. Je hypotéza, která tvrdí, že moderní banky budou své pobočky postupně přetvářet na spíše konzultantsko-prodejní místa. Do banky by tak klient přišel jen v případě, že potřebuje přímou radu. Běžné operace bude totiž provádět sám za pomocí moderní technologie odkudkoli a kdykoli.

Na vývoj bankovních produktů neustále působí řada vlivů a souvislostí. Trendy vývoje bankovních produktů se můžeme pokusit předpokládat v podstatě ze dvou hledisek - z pohledu banky jako podnikatelského subjektu nebo jako finančních zprostředkovatelů na finančním trhu. Z pohledu banky jako podnikatelského subjektu budou vývoj bankovních produktů ovlivňovat snahy o snížení obchodních rizik, snížení nákladů, zvýšení efektivnosti, podílu na trhu, kvality poskytovaných služeb včetně komunikace s bankou. Z pohledu postavení banky na finančním trhu je nutno odvozovat

předpoklad vývoje bankovních produkt ze současných trendů na světových finančních trzích.

V poslední době, v souvislosti s rychlým vývojem informačních a bankovních technologií, dochází k různým změnám v počtu, struktuře, vlastnictví a zaměření finančních institucí.

Je dosti pravděpodobné, že vzhledem k rozvoji moderních komunikačních technologií bude jednou mobilní a elektronické bankovnictví úplnou samozřejmostí. Doba, ve které byla banka jako budova, ve které klienti vyřizují své transakce, neodmyslitelnou součástí bankovnictví, se pomalu začíná blížit ke svému konci.

V České republice brání rozvoji elektronického bankovnictví zejména jistý konzervatizmus hlavně starších lidí. Jejich odstup od nových technologií brání progresivním novým komunikačním kanálům v rozvoji a usnadnění komunikace klienta s bankou. Do jisté míry zde hraje svou roli i určitý strach z bankrotu bank. Rozvoji nových technologií také brání i nedostatečného pokrytí populace internetovým připojením.

Elektronická komerce na internetu velmi úzce souvisí s elektronickým bankovnictvím. Především v platbách přes internet vidím velký potenciál dalšího vývoje.

Jistě nemalou překážkou ve vývoji komunikačních technologií ve spojení s elektronickým bankovnictvím je jejich zabezpečení. Dokud nebude vyvinut dostatečně bezpečný kanál, který by současně využívala podstatná část klientů, bude mít elektronické bankovnictví stále kam směřovat.

4 Závěr

Jestliže se uživatel rozhodne pro základní balíček zabezpečení, pro tzv. autentizaci přihlašovacím jménem a heslem, dostane službu, která je ekonomicky levnější. Zvýšení bezpečnosti např. autentizačním kalkulátorem, čipovou kartou nebo certifikátem je jistě bezpečnější, ale i dražší. Uživatel však získá lepší pocit, že jeho finance jsou bezpečně spravovány bankou.

Mezi banky s nejlepším zabezpečením jistě patří Česká spořitelna, a.s., Komerční banka, a.s., eBanka, a.s. a GE Money Bank, a.s. Jedním z důvodů proč jsem určil tyto banky mezi nejlepšími je bezesporu samotný přístup bank k problematice bezpečnosti internetového bankovnictví. Je to dáno hlavně počtem aktivních uživatelů (klientů) bank, kteří mají přístup do internetového bankovnictví. Výše uvedené banky používají více možností autentizace do internetového bankovnictví (Komerční banka, a.s. – dvě autentizace a Česká spořitelna, a.s., eBanka, a.s. a GE Money Bank, a.s dokonce tři metody autentizace). Toto se týká i autorizace transakcí (Komerční banka, a.s. a GE Money Bank, a.s mají dvě autorizace transakcí a Česká spořitelna, a.s. a eBanka, a.s. dokonce tři metody autorizace transakcí).

Vstup na účet je nejméně chráněn u BAWAG Bank CZ, a.s., Citibank, a.s., ING Bank N.V. či Raiffeisenbank, a. s., kde si uživatel nemůže zvolit lepší zabezpečení. To je dáno počtem možností autentizace a autorizace transakcí.

Aktivní transakce jsou chráněny o něco lépe. Nejlépe dopadly banky, které nabízejí i nejlepší zabezpečení. Jsou to Česká spořitelna, a.s., Komerční banka, a.s., eBanka, a.s. a GE Money Bank, a.s.

Internetové bankovnictví může být zabezpečeno sebelépe, ale bez dodržování základních pravidel uživatelů, může docházet k zneužití internetového bankovnictví. Doporučuji dodržovat desatero, které je uvedeno v oddíle 3.7 Bezpečnostní zásady.

Literatura

[1] http://csrc.nist.gov/fips/fip180-1.pdf

[2] ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/ripemd/

[3] http://csrc.nist.gov/cryptval/shs/sha256-384-512.pdf

[4] Přádka M., Kala J., *Elektronické bankovnictví*, Computer Press Praha 2000, str. 73-83

[5] Dostálek L., Vohnoutová M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu,* Computer Press, a.s. Brno 2006, str. 21-36

[6] Dostálek L., *Velký průvodce protokoly TCP/IP: Bezpečnost*, Computer Press Praha 2001, str. 389-397, 461-463, 485-487

[7] Rosa T., *Co je dobré vědět, když mluvíte o šifrování a kódování*, http://digiweb.ihned.cz/c3-17121110-i00000_d-co-je-dobre-vedet-kdyz-mluvite-o-sifrovani-a-kodovani

[8] Krčmář P., *Existuje bezpečný prohlížeč?*, http://www.root.cz/clanky/existuje-bezpecny-prohlizec/

[9] Symantec Internet Security, *Threat Report, Trends for January–June 07, Volume XII, Published September 2007*, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

[10] Wikipedie, *IPsec*, http://cs.wikipedia.org/wiki/IPsec

[11] Nykodýmová H., *Jak je to s bezpečností internetového bankovnictví?*, http://www.lupa.cz/clanky/jak-je-to-s-bezpecnosti-internetoveho-bankovnictvi/

[12] Odvárka P., *SSL protokol (3) - SSL Handshake Protocol*, http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=171&clanekID=183

[13] *Úvod do teorie šifrování*, http://st.vse.cz/~XRENP01/index.htm

[14] Zámečník P., Krčmář P., *Analýza zabezpečení internetového bankovnictví v České republice*, http://www.iinfo.cz/tiskove-centrum/tiskove-zpravy/mesec-bezpecnost-internetoveho-bankovnictvi/