Crypto-World

Informační sešit GCUCMP

Ročník 2, číslo 11/2000 20.listopadu 2000

11/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>230 e-mail výtisků)

OBSAH : **Str.**

A. Soutěž
Mgr. Pavel Vondruška (NBÚ)

Část III. - Jednoduchá transpozice
Luštění jednoduché transpozice - úplná tabulka (metodika)

Jednoduchá transpozice je jedna ze základních metod šifrování. Po jednoduché záměně se tak seznámíme s druhým nejdůležitějším systémem. Troufám si tvrdit, že většina šifrových systémů vychází právě z těchto dvou postupů. Ostatně prvky typu SHIFT apod. v blokových šifrách jsou vlastně jen transpozicí jednotlivých bitů. Vraťme se však k tomuto systému. Transpozice je "přeskupení" otevřeného textu podle nějakých pravidel - tato pravidla se nazývají klíčem. Výsledný šifrový text zachovává frekvenci hlásek příslušného jazyka. Zpřetrhány jsou pouze bigramové vazby a tím je ukryt význam původního textu. V takovémto textu se tedy nevyskytují dlouhá opakování, je zachována frekvence hlásek příslušného jazyka, neodpovídají bigramové frekvence, nelze provést dělbu na samohlásky a souhlásky. Poměr samohlásek a souhlásek je v textu zachován a je přibližně v poměru 40 : 60. Tento systém se používal ještě za druhé světové války a v některých méně vyspělých státech i v celkem nedávné době. Používala se však určitá modifikace, která velice znesnadňuje luštění - tzv. dvojitá neúplná transpozice. Text je nejprve vepsán do tabulky určitého rozměru, zde jsou podle prvého klíče sloupce rozházeny a dále je text převeden do tabulky o jiných rozměrech, která není ovšem v posledním řádku zcela vyplněna (!) a opět jsou sloupce podle druhého klíče přeskupeny. V případě, že rozměry tabulek (počet sloupců) jsou 30 a více, je ke zpětné transformaci nutné použít složitější postupy, kde se již bez počítačů neobejdeme a v některých případech může být tento systém (např. ve spojení s jednoduchou záměnou) celkem použitelnou šifrou určenou např. pro náhradní spojení, kdy nelze z nějakého důvodu použít kvalitní speciální šifrátor.

Vraťme se k jednoduché transpozici využívající úplnou tabulku. Získáme šifrový text rozepsaný jako obvykle do pětimístných skupin. Pořídíme frekvenci a zjistíme, že odpovídá frekvenci jazyka. Nejsou zde velká opakování a jsou zde skupiny samohlásek a souhlásek. Toto by mohlo naznačovat, že se jedná o transpozici. V případě, že se jedná o jednoduchou transpozici s úplnou tabulkou, postupujeme takto:

Určení rozměru tabulky

Spočteme délku šifrového textu a snažíme se určit pravděpodobný rozměr tabulky. Ten zjistíme tak, že délku šifrového textu rozložíme na součin prvočísel a z nich kombinujeme pravděpodobnou velikost tabulky. Máme-li např. šifrový text délky 120, pak jsou možné následující velikosti tabulek :
120= 2*2*2*3*5

Tabulky :
počet sloupců * počet řádků
málo pravděpodobné (bylo by příliš lehké k řešení) : 1*120, 2*60 , 3*40, 4*30, 6*20
složité : 120*1, 60* 2 ,
tabulky : 8*15, 15*8, 12*10, 10*12, 20*6, 30*4, 40*3

Šifrový text se vepíše do "podezřelých" tabulek. Poznamenejme, že text se vepisuje po sloupcích (!), viz. příklad na konci textu.

Dříve, než přejdeme k vlastnímu luštění, můžeme si do značné míry ověřit, zda námi zvolená tabulka je správná. Zjistíme to na poměru souhlásek a samohlásek v jednotlivých řádcích tabulky. I zde by měl být přibližně zachován poměr samohlásky : souhlásky = 40 : 60. Která z tabulek splňuje tento poměr pro většinu svých řádků, ta je nejpravděpodobnější tabulkou a zde začneme s pokusem o vyluštění původního textu.

Luštění

Samotné luštění není nijak složité. Ti z vás, kteří luští tzv. lištovky v různých časopisech, tento postup již prakticky znají. Pokud nemáme k dispozici vhodný program a jsme příliš pohodlní si jej napsat, nezbývá než sloupce tabulky rozstříhat a přeskupovat tak, abychom se snažili zohlednit bigramové četnosti (např. PR, ST) a samohláskové a souhláskové vazby, a to ve všech řádcích najednou. Postupně tedy k sobě přikládáme vhodné sloupky, až dostaneme celé bloky otevřeného text (čte se po řádcích). Bloky pak jen přeskupíme a máme hledaný výsledek.

Vše si prakticky ještě zopakujeme na následujícím cvičném příkladě.

Cvičný šifrový příklad na jednoduchou transpozici - úplná tabulka

OTSEC NCNUX ATONO TOUTO KXUJU AILBX UVPTD HSEOL KYREN EPSUK
ZELID RZPAU (60 znaků)

Určení velikosti tabulky
ne : 1*60 , 2*30, 3*20, 4*15,
možné tabulky : 15*4, 20*3, 10*6, 6*10

Prozradím, že tento text byl úmyslně volen tak, aby ani poměr samohlásky: souhlásky nedal zcela jednoznačnou odpověď na rozměr tabulky, v praxi ovšem takovéto případy většinou nenastávají, tento příklad měl pouze komplikovat samotné luštění žákům, kterým jsem příklad předložil a nechtěl jsem, aby jednoduše zjistili správnou velikost tabulky. Sledujte, jak se šifrový text plní do tabulky. Začátečníkům někdy toto činí potíže a zapisují jej omylem do řádků místo do sloupců.

rozměr 20*3
očekávaný poměr 8/12

OECXOTTXULUTSLREUEDP 8/12
TCNANOOUABVDEKEPKLRA 8/12
SNUTOUKJIXPHOYNSZIZU 8/12

rozměr 15*4
očekávaný poměr 6 / 9

OCUOOKUBPSKNULZ 6/9
TNXNUXAXTEYEKIP 6/9
SCAOTUIUDORPZDA 7/8
ENTTOJLVHLESERU 5/10

rozměr 10*6
očekávaný poměr 4/6

OCOTUUSRUD	5/5
TNNOAVEEKR	4/6
SUOKIPONZZ	4/6
EXTXLTLEEP	3/7
CAOUBDKPLA	4/6
NTUJXHYSIU	4/6

ukázka 6*10
očekávaný poměr 2,4 / 3,6

OAKUKZ	3/3
TTXVYE	2/4
SOUPRL	2/4
ENJTEI	3/3
COUDND	2/4
NTAHER	2/4
COISPZ	2/4
NULESP	2/4
UTBOUA	4/2
XOXLKU	2/4

Nejpravděpodobnějšími tabulkami jsou rozměry 20*3 a 6*10, následují rozměry 10*6 a nejhůře z testu vyšel rozměr 15*4.

Správný rozměr je 6*10. Vzhledem k malému počtu sloupců již není problém je správně seřadit a dostaneme příslušný otevřený text :

UKAZKO
VYTEXT
PROLUS
TENIJE
DNODUC
HETRAN
SPOZIC
ESUPLN
OUTABU
LKOUXX

Takže hledaným textem je :

UKAZKOVY TEXT PRO LUSTENI JEDNODUCHE TRANSPOZICE S UPLNOU TABULKOU XX

Klíčem je pak postup, jak přeskupit sloupce otevřeného textu na sloupce šifrového textu.

Na příkladě si můžeme všimnout, že při zápisu do tabulky byl doplněn text tak, aby zcela vyplnil i poslední řádek pomocí XX. Pro různé uživatele, kteří systém používají, může být doplnění tabulky na úplnou tabulku charakteristické. Text by měl být doplněn náhodně, ale často se používá nějaký ustálený způsob, který kryptoanalytikovi (pokud jej zjistí) pomáhá v luštění. Např. se používá doplňování pomocí X nebo písmena abecedy nebo se doplní podpis apod. Všechna tato doplnění jsou špatná a mohou vést ke snadné kompromitaci systému (určení velikosti tabulky a umístění některých sloupků). Znalost takovýchto maličkostí usnadní chápání podstatně složitějších problémů, se kterými se v kryptologii můžeme setkat. Připomeňme v této souvislosti analogii s nevhodným doplňováním dat pro šifrování symetrických klíčů podle normy PKCS#1, v. 1.5 .

Nyní již můžeme vyhlásit soutěžní úlohu III.kola

Úlohou třetího kola je vyluštění přiloženého šifrového textu. Jedná se o jednoduchou transpozici - použita byla úplná tabulka. Rozměr tabulky musíte určit. Text je v češtině, v mezinárodní abecedě = 26 znaků A-Z (bez háčků a čárek) a bez mezer, je rozdělen do skupin po 5-ti znacích. Prozradím, že se jedná o text, který se vyskytl na stránkách našeho e-zinu.

SIFROVY TEXT

IRJYE VDIPI AVIVZ NTUKM EORZN EOTYE KKLPI TTNNC EIPAE COSMN EOPRL KEPEP LAPTE NNEDO SOTNK ENOPT LBOAO TROVR OEEIN REEEK UTSHX EOORM YIJAJ PZOED DEDOD UCSTS ONZOA IKSCU JPPES NISBV FEIIK AEUVU EJOOO DNMKS EORKB YMOAU ELPNO DKOOO JUNST ZIUOU EEJVG EEDZA ACEDM KKEEI RNETV

Zaslání celého textu 10 bodů.
Losování III.kola bude 8.12.2000 (18.00 hod).

****

Pravidla soutěže

Soutěž probíhá ve čtyřech kolech. V sešitech 9/2000 až 12/2000 je uveřejněna jedna soutěžní úloha a současně je uveden doprovodný text k dané úloze. Řešitelé, kteří zašlou do data, které bude u každé úlohy uvedeno, správné řešení, budou slosováni a dva vybraní získají cenu kola. **I po tomto datu však lze správná řešení dále zasílat a získat tak hlavní výhru!**

Dne 15.12.2000 bude soutěž ukončena a z řešitelů, kteří získali nejvíce bodů, bude vylosován celkový vítěz. **Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže později, např. až v prosinci, a řešení všech úloh odešle najednou v časovém limitu do 15.12.2000**; přijde jen o možnost být vylosován jako vítěz příslušného kola.

Dne 20.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol a jméno celkového vítěze; uveřejníme také menší statistiku k celé soutěži. Ceny do soutěže věnovaly firmy PVT a.s. a AEC spol. s r.o. (jednotlivá kola), Globe CZ (cena pro celkového vítěze).

Cenou v jednotlivých kolech je bezplatná registrace vašeho veřejného klíče u certifikační autority (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců (cena cca 300,- Kč). Hlavní cenou je registrace domény prvního řádu + hosting na webu u firmy GLOBE CZ (v běžné hodnotě 5000,- Kč).

Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa, případně pouze pseudonym).

Stav po II.kole

Pseudonym	I.kolo datum /bodů	II.kolo datum /bodů	III.kolo datum/bodů	IV.kolo datum/bodů	CELKEM
J.M.	12.9 /10 ☒				
Mirek Š.	12.9 /10	17.10/10			
Petr T.	12.9 /10	18.10/10			
Bohumír Š.	12.9 /10	18.10/10			
Martin K.	12.9 /10				
František K.	12.9 /10				
Tomáš V.	13.9 /10 ⏢	31.10/10			
Jan J.	13.9 /10	17.10/10			
Josef D.	18.9 /10				
Honza K.	18.9 /10				
Vašek V.	2.10/10				
Michal B.	4.10/10	18.10/10 ⏢			
Láďa R.	4.10/10	24.10/10 ☒			
Martin V.	18.10/10				
Karel Š.		24.10/10			
Ivan L.		19.10/10			

Legenda : cena kola - certifikát u AEC ⏢
cena kola - certifikát u PVT ☒

B. Působnost zákona o elektronickém podpisu a výklad hlavních pojmů (Informace o přednášce)

Mgr. Pavel Vondruška (NBÚ)

Dne 1.listopadu uspořádalo ***Sdružení pro bezpečnost informačních technologií a informačních systémů*** **(BITIS, http://www.mujweb.cz/veda/bitis) a spolek *Česká technika*** ve velké zasedací síni rektorátu ČVUT přednášku na aktuální téma "Působnost zákona o elektronickém podpisu a výklad hlavních pojmů". Večera se zúčastnilo přes 40 odborníků z České a Slovenské republiky. Po mé úvodní hodinové přednášce následovala hodinová diskuse, do které se zapojila celá řada účastníků. Diskuse byla velice zajímavá a nesla se ve zcela nekonfliktním duchu. Z diskuse vyplynulo, že při realizaci celého systému používání elektronického podpisu čeká všechny zúčastněné subjekty ještě dlouhá a náročná cesta. V diskusi vystoupila i ředitelka odboru elektronického podpisu ÚOOÚ paní Mgr. Dagmar Bosáková, která přítomné seznámila se stavem příprav vyhlášek k paragrafu 6 a 17 Zákona o elektronickém podpisu. Akce připomínala spíše klubový večer. K této příjemné atmosféře přispělo pěkné prostředí a drobné občerstvení, které účastníkům zajistil spolek Česká technika (doc.Chaloupka).

Jako připomínku této akce zde uvádím otisk dvou fólií použitých v úvodní přednášce. Jedná se o připomenutí, jak se vytváří elektronický podpis datové zprávy a jak probíhá ověření podpisu u přijaté elektronicky podepsané datové zprávy. Přesto, že se jedná o dvě zcela zřejmé situace, byl o tyto fólie zájem - dají se totiž dobře využít při vysvětlení těchto pojmů. Ostatní fólie byly věnovány pojmům zákona (roztřídění typů podpisů, poskytovatelů certifikačních služeb, práva a povinnosti podepisující se osoby a ÚOOÚ). Soubor všech fólií - v elektronické podobě - lze získat zasláním žádosti na adresu pavel.vondruska@post.cz , předmět folie.

Obsah přednášky

1. Účinnost a požadavky na jednotlivé subjekty a jejich odpovědnost (podepisující se osoba, osoba spoléhající se na elektronický podpis, organizace, veřejná moc, poskytovatel certifikačních služeb)
2. Typy elektronických podpisů (elektronický podpis, zaručený a kvalifikovaný elektronický podpis)
3. Typy poskytovatelů certifikačních služeb a certifikátů (PCS, kvalifikovaný certifikát, PCS vydávající kvalifikované certifikáty, akreditovaný PCS)
4. Některé problémy spojené s aplikací zákona v praxi
5. Diskuse

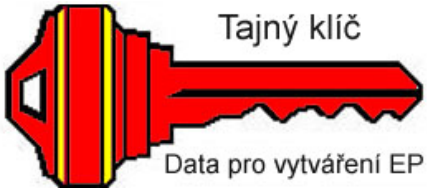
Použité zkratky :

ZoEP	- Zákon o elektronickém podpisu č.227/2000
EP	- elektronický podpis
ZEP	- zaručený elektronický podpis
QP	- kvalifikovaný podpis
QC	- kvalifikovaný certifikát
PCS	- poskytovatel certifikačních služeb
PCS-QC	- poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
APCS	- akreditovaný poskytovatel certifikačních služeb
PBVP	- prostředek pro bezpečné vytváření podpisů
PBOP	- prostředek pro bezpečné ověřování podpisů
ÚOOÚ	- Úřad pro ochranu osobních údajů

ELEKTRONICKÝ PODPIS

DATOVÁ ZPRÁVA " T "

Toto je text, který budu chtít podepsat. Nyní ukáži jak se to dělá. Celý postup je velice jednoduchý. Hash, asymetrická šifra, data pro vytváření EP klíč,certifikát.



HASH

SHA-1
MD5

AB 09 12 C2 4F 12 A5 4C D1 FF " H1 "
128/160 bitů

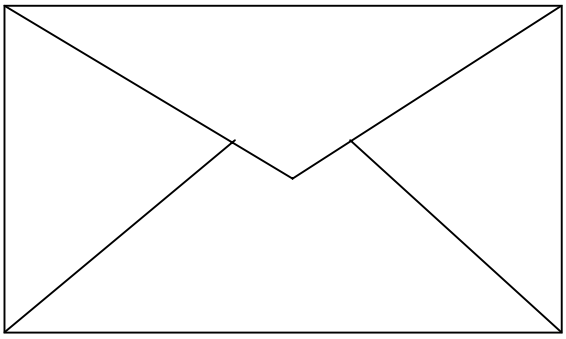
PCS

ASYMETRICKÁ ŠIFRA

RSA, DSA, ECC

1

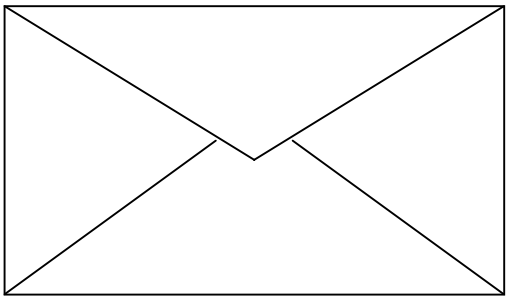
3



ELEKTRONICKÝ PODPIS DATOVÉ ZPRÁVY " T "

2

ELEKTRONICKÝ PODPIS - OVĚŘENÍ



" T "

Toto je text, který budu chtít podepsat. Nyní ukáži jak se to dělá. Celý postup je velice jednoduchý. Hash, asymetrická šifra, data pro vytváření EP klíč,certifikát.

Elektronický podpis "T"

ASYMETRICKÁ ŠIFRA

HASH
SHA-1
MD5

AB 09 12 C2 4F 12 A5 4C D1 FF " H1 "

H2 = H1

AB 09 12 C2 4F 12 A5 4C D1 FF " H2 "

128/160 bitů

IDENTIFIKACE
NEPORUŠENOST
NEPOPIRATELNOST

OVĚŘENÍ PLATNOSTI u PCS
AKCEPTOVÁN ?
ZNEPLATNĚN (CRL)?
POZASTAVENA
PLATNOST ?
ZRUŠEN (úřadem) ?

P C S

C. Rozjímání nad ZoEP, zvláště pak nad paragrafem 11
Mgr. Pavel Vondruška (NBÚ)

Zákon o elektronickém podpisu vstoupil v platnost 1.10.2000. Zákon doplní prováděcí vyhlášky k § 6 a k § 17 . K vydání těchto vyhlášek je zmocněn ÚOOÚ. Na tomto úřadu vznikl odbor elektronického podpisu, který má za úkol vyhlášky připravit. Odbor má v současné době tři lidi. Pokud nemají být tyto vyhlášky bezzubé a tedy mají nastavit správné podmínky (především bezpečnostní parametry) k hodnocení poskytovatelů certifikačních služeb, kteří chtějí vydávat kvalifikované certifikáty nebo být přímo akreditovanými poskytovateli certifikačních služeb, je zřejmé, že musí být připraveny s náležitou erudicí a znalostí věci. Dr.Neuwirt jmenoval odbornou komisi, která má za úkol připravit podklady k těmto vyhláškám. Dnes, kdy píši tyto řádky, vyšel v EU další opravený draft (celkem již desátý !) věnovaný hodnocení poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty. Jedná se tedy o materiály velice živé a stále se ještě měnící.

Jakmile bude text vyhlášky touto odbornou skupinou připraven, bude Úřadem předložen k připomínkám nejprve odborníkům - především z firem, které se problematikou elektronického podpisu aktivně zabývají - a po té celé veřejnosti k diskusi. Po zapracování připomínek se bude čekat na možnost zveřejnění těchto vyhlášek ve Sbírce zákonů. Tady pravděpodobně bude nutná novela zákona č.101/2000, kterým Úřad vznikl . **V současné době je totiž Úřad sice zákonem č. 227/2000 zmocněn k přípravě těchto vyhlášek, ale není ústředním orgánem státní správy a tedy nemůže ve Sbírce zákonů publikovat a vlastně tak nemůže tuto vyhlášku vydat….**

Vraťme se k zákonu o elektronickém podpisu. Při seznamování se s jednotlivými paragrafy mne zaujalo, že z celkového počtu 28 paragrafů není jeden z nich - a to paragraf 11 - uveden názvem paragrafu. Tento paragraf je také co do počtu řádků nejkratší. Ovšem obsah je velice důležitý. Podívejme se na tento paragraf trochu blíže.

§ 11

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

Otázka 1

Především mne napadla otázka, co je vlastně oblast veřejné moci? Na koho se tedy dikce tohoto zákona vztahuje?
V jednom z připravovaných dokumentů jsem našel následující odpověď:
Tento paragraf se vztahuje na státní orgány, orgány samosprávy, jiné orgány veřejné moci, Kancelář Prezidenta ČR, Kancelář Poslanecké sněmovny Parlamentu ČR, Kancelář senátu Parlamentu ČR a Kancelář Veřejného ochránce práv.

Otázka 2

Druhá otázka, která mne při přečtení tohoto paragrafu napadla, je tato : co se míní spojením … v oblasti orgánů veřejné moci …? Zde je možných více výkladů:

- uvnitř jednoho každého z orgánů veřejné moci
- v komunikaci mezi jednotlivými orgány veřejné moci
- v komunikaci mezi občanem a některým z orgánů veřejné moci
- veškerá komunikace orgánů veřejné moci (uvnitř orgánu, mezi jednotlivými orgány, občan - orgány veřejné moci)

Tuto otázku zodpovídá doc.Smejkal takto:

… pokud zákon říká "v oblasti", znamená to samozřejmě vždy, kdy se jedná o komunikaci, kde alespoň na jedné straně se nachází orgán veřejné moci. Jinak by toto ustanovení bylo formulováno zřejmě jinak, např. "orgány veřejné moci mohou používat..." a především, takovýto výklad by postrádal jakokoliv logiku vzhledem k požadavkům, které na komunikaci v rámci procesních právních předpisů po novele provedené ZoEP máme.
Doslovná citace (včetně překlepu) z : Vladimír Smejkal, rubrika Zprávy (11.11.2000), Vyjádření ÚOOÚ, http://www.e-podpisy.cz/ .

Citaci zde uvádím takto pečlivě vzhledem ke zlověstné poznámce, která na příslušné adrese vítá každého návštěvníka:

"Obsah všech stránek nacházejících se na tomto serveru pod jménem e-podpisy.cz a epodpisy.cz je chráněn platnými českými zákony, a to především autorským zákonem. Jakékoliv rozmnožování, rozšiřování, předávání, transformování, upravování, prodej, pronájem, půjčování nebo jiný způsob poskytování autorských děl zde se nacházejících další osobě, případně sdělování díla veřejnosti jakýmkoliv způsobem včetně rozšiřování prostřednictvím dálkového přístupu např. prostřednictvím sítě Internet, jakož i zhotovení rozmnoženiny pro osobní potřebu nad rámec zákonných oprávnění vyplývajících z autorského zákona je porušováním autorských práv a současně trestným činem. Citace z autorských děl a jiných dokumentů, zde uveřejněných, jsou možné pouze s uvedením autora, názvu a pramene."

Důsledky tohoto paragrafu

Účinnost ZoEP (zde a dále budeme používat zkratky, které byly zavedeny v předchozím článku) je od 1.10.2000 a ani k tomuto paragrafu nebylo přijato přechodné ustanovení. Tedy již vstoupil v platnost.

Při komunikaci v oblasti veřejné moci v současné době není možné použít jiný podpis než zaručený elektronický podpis (ZEP) založený na kvalifikovaném certifikátu (QC), který vydal akreditovaný poskytovatel certifikačních služeb (APCS).

Důsledek 1 ☺

Pokud budeme brát doslova dikci tohoto zákona, znamená to, že se úředníci orgánů veřejné moci již nesmí ručně podepisovat ? Mají přece nařízeno používat pouze ZEP s QC od APCS ! Takže pokud od 1.10.2000 se nějaký úředník podepíše pod nějaký dokument, porušil tím ZoEP č.227/2000. Snad se dá tento rozpor vyřešit konstatováním, že zde mělo být uvedeno: v případě použití elektronického podpisu má být použito zaručeného elektronického podpisu …. Odůvodnit se to dá slovy, vždyť celý ZoEP se týká elektronického podepisování tak, proč to zde zdůrazňovat …Ovšem pravdou je, že dikce paragrafu je jednoznačná a tyto podpisy zakazuje.

Důsledek 2

Pod e-mail, fax (odesílaný z PC) apod. již nesmí být napsán podpis z klávesnice či vložen oskenovaný podpis. Dle definice je totiž i takovýto postup elektronickým podpisem (§ 2, písmeno a), ale není zaručeným elektronickým podpisem (§ 2, písmeno b). Úředník nebo občan, který zasílá elektronickou datovou zprávu nějakému orgánu veřejné moci, se tedy nemůže do tohoto dokumentu podepsat - nebyl by to totiž zaručený elektronický podpis … a tedy by porušil zákon.

Důsledek 3

Dokud nebudou vydány prováděcí vyhlášky (a ty jak již víme budou, až to bude moci ÚOOÚ vykonat) - nebudou známa pravidla k hodnocení poskytovatele, který vydává kvalifikované certifikáty. Teprve po splnění těchto podmínek lze zažádat Úřad o akreditaci a o zařazení do seznamu akreditovaných poskytovatelů certifikačních služeb (při splnění podmínek § 10). Jenže k tomu, aby mohl někdo splnit podmínky kladené na PCS, je nutné mít např. bezpečné prostředky pro vytváření elektronického podpisu a ověřovací prostředky. K

hodnocení těchto prostředků je potřeba vybudovat síť testovacích laboratoří (nebo zajistit uznávání zahraničních certifikátů těchto zařízení). K využívání v oblasti veřejné moci je prostě potřeba získat kvalifikovaný certifikát od akreditovaného poskytovatele certifikačních služeb a to bude možné až za nějaký čas… Do té doby nelze požadavek paragrafu 11 zajistit a tak splnit.

Informace 1

K zařazení paragrafu 11 pravděpodobně vedla snaha zajistit podpisům v oblasti veřejné moci co největší důvěru - bezpečnost. V tom případě mohl být dokonce stanoven požadavek na použití kvalifikovaného podpisu (§ 3, odstavec 2), který je chápán v EU jako ekvivalent vlastnoručního podpisu. K tomu, aby byl nějaký podpis kvalifikovaný (tedy splnil podmínku paragrafu 3, odstavec 2), musí být mimo požadavku, že se jedná o zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem, který vydává kvalifikovaný certifikát (nemusí být tedy akreditovaný), navíc splněn požadavek, že podpis byl vytvořen pomocí bezpečného podpisového prostředku. Na druhou stranu v případě přísné dikce paragrafu 11 - … je možné používat pouze … by to mohl být spíše další problém. Řešení by byla drahá a odrazovala by v používání tohoto způsobu komunikace. Mnohem výhodnější by bylo umožnit orgánům veřejné moci vyhlašovat bezpečnostní profily pro jednotlivé konkrétní agendy - tedy vyhlásit akceptovatelný způsob podpisu příjemcem (jak se o tom uvažuje v EU) - pro různé agendy. Např. při e-mail dotazu typu - zda má úřad otevřeno ve středu odpoledne - se zdá splnění požadavků paragrafu 11 poněkud přehnaně úzkostlivé a bránící elektronické komunikaci na místo její podpory.

Důsledek 4

Žádný z orgánů veřejné moci již nemůže např. pro svoji potřebu v rámci vnitřní pošty používat nebo budovat svá řešení (např. levné a zcela vyhovující řešení pomocí instalace serveru Windows 2000 se zapnutou službou certifikační autority). Takováto řešení nejsou založena na poskytování služeb akreditovaného poskytovatele certifikačních služeb (APCS) dle přísné dikce paragrafu 11. Takže i pro tuto vnitřní službu si musí každý z orgánů veřejné moci zajistit certifikáty od nějakého APCS a tomu za tyto služby pravidelně platit. Další možností je vybudování vlastního PCS a po splnění podmínek vyhlášky a ZoEP zažádat o akreditaci na ÚOOÚ. Tato cesta je ovšem velice nákladná; při splnění všech podmínek § 6 a § 10 se bude pohybovat v desítkách miliónů Kč. Navíc z paragrafu 10 písmeno 6 v případě, že někdo poskytuje služby jako APCS, plyne, že jiné než taxativně vyjmenované služby ani provádět nemůže - tedy např. svoji činnost jako orgán veřejné moci (§10 písmeno 6 : Kromě činností uvedených v tomto zákoně může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec (doplním, že znalec čehokoli - např. hub)). Je zde sice možnost výjimky, ale není dále stanoveno, jak při udělení či neudělení má Úřad postupovat. Vyvozuji z toho, že pravděpodobně může být výjimka - (stát se akreditovaným poskytovatelem certifikačních služeb a poskytovat jiné služby než advokát, notář nebo znalec) - udělována nebo neudělována libovolně na základě nálady úředníka ÚOOÚ nebo třeba podle čísla žádosti (lichým se udělí, sudým ne…).

Informace 2 ☺

Paragraf 11 je právně nevymahatelný, neboť za jeho porušení nebo nedodržování nejsou stanoveny v ZoEP č.227/2000 žádné sankce.

Uvědomuji si, že výše uvedené důsledky paragrafu 11 nejsou na první pohled zřejmé a předpokládám, že ani nebyly míněny tak, jak jsem právě popsal. Ovšem zákon je zákon… A tak se těším na fronty u APCS, kde stojí přede mnou úředníci z BIS, Vojenské

kontrarozvědky nebo Jednotky rychlého nasazení se svými doklady, aby uzavřeli smlouvu s příslušným akreditovaným poskytovatelem certifikačních služeb. Možná, že tato data budou nakonec zajímavější a cennější než samotná data k vytváření elektronického podpisu.

Na závěr si asi čtenář klade otázku, jak se vlastně paragraf 11 do ZoEP dostal? Pokusím se najít odpověď uvedením následující zkrácené historie vzniku ZoEP č.227/2000.

Fakta z historie vzniku ZoEP č.227/2000.

V lednu tohoto roku předložili poslanci Vladimír Mlynář (US), Ivan Langer (ODS), Stanislav Gross (ČSSD) a Cyril Svoboda (KDU-ČSL) návrh zákona o elektronickém podpisu. Tento text připravil SPIS ve spolupráci s doc. Smejkalem a doc.Matesem. Dne 26. ledna 2000 byl tento návrh většinou poslaneckých hlasů postoupen do druhého čtení.

Před tímto druhým čtením Úřad pro státní informační systém a SPIS iniciovaly vznik expertní skupiny nezávislých odborníků a požádaly ji o zpracování odborných připomínek k textu poslaneckého návrhu zákona formou pozměňovacích návrhů tak, aby byl uveden do souladu se Směrnicí Evropské unie o elektronických podpisech schválenou 30.listopadu 1999 a o odstranění nedostatků, na které odborná veřejnost poukazovala (vyplývající především z jiného pojetí samotné definice elektronického podpisu a z nutného působení více druhů poskytovatelů certifikačních služeb).

Tato odborná skupina se sešla se zástupci SPISU a ÚSISU na pracovním víkendovém shromáždění v Třešti (26.2. - 27.2.2000) a v následujících dnech zpracovávala odborné připomínky k textu. Z textu přijatého v prvém čtení bylo ponecháno po těchto úpravách přibližně 18% z původního textu. Konečný produkt, který z těchto jednání vzešel (návrh Zákona o elektronickém podpisu), byl předán 7.3.2000 panu poslanci Mlynářovi, který jej předložil Hospodářskému výboru parlamentu.

Paragraf 11 ani jeho obdoba v této zpracované a předané verzi nebyl uveden. V legislativním procesu došlo následně i k některým dalším dílčím změnám.

Zákon byl přijat 29. června 2000. Jako autor předlohy je ve sbírce zákonů uveden Parlament. Tento přístup k autorství je podle mne správný, neboť autorství jakéhokoliv odborníka, který návrh Zákona o elektronickém podpisu připravoval, je totiž mírně řečeno pochybné. Z původního návrhu zbylo přibližně osmnácti procentní torzo a text vložený odbornou skupinou zase vycházel ze znění a zásad Směrnice EU. Autory jsou v pravém slova smyslu všichni ti, kteří pomocí pozměňovacích návrhů zákon upravili - tedy poslanci Parlamentu. Zákon vstoupil v platnost 1.10.2000.

Na úplný závěr uvedu ještě jednu doslovnou citaci :

"Generování pochybností okolo výkladu § 11, který od samého počátku velmi vadí některým lobujícím firmám, je významným signálem o tom, že se těmto lobbystům již podařilo zřejmě proniknout do činnosti ÚOOÚ." Vladimír Smejkal, rubrika Zprávy (11.11.2000), Vyjádření ÚOOÚ, http://www.e-podpisy.cz/ .

Takovéto konstatování je bezobsažné a problémy kolem paragrafu 11 neřeší. Předpokládám, že teprve nařízení vlády, kterým se využití elektronického podpisu upravuje v oblasti veřejné moci, tyto problémy nějakým způsobem odstraní nebo alespoň uvede na pravou míru. **Tento článek nevznikl jako snaha o "generování pochybností", ale snaží se pojmenovat problémy, které paragraf 11 může v sobě obsahovat. Pokud jsou tyto problémy malicherné - tím lépe, pokud ne - je potřebné se s nimi nějakým objektivním způsobem vypořádat.**

D. Kryptografie a normy

Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)

Díl 3.
Normy PKCS (Public-Key Cryptographic Standards) - PKCS #5.

Úvod

Dnešní část seriálu bude věnována PKCS #5**,** tj. vlastně problematice práce s heslem. Nejedná se však o popsání cest jak volit správné heslo (délka, používané znaky), abychom se vyhnuli slovníkovým útokům, resp. útokům obdobného charakteru. Cílem normy je popsat způsoby, dle kterých lze bezpečně z daného hesla odvozovat tajný klíč (použitý např. pro zašifrování soukromého klíče).

PKCS #5

Jako ostatní normy z řady PKCS má i pětka svojí historii. První její verze se objevila v únoru 1991. V současnosti platí verze 2, která rovněž prošla několika drafty, aby nakonec byla vydána jako rfc2898 (lit. [1]). Autorem tohoto dokumentu je známý odborník, pracovník firmy RSA Security Burt Kaliski.

Dokument obsahuje doporučení pro následující tři schémata:

- funkce pro odvozování klíčů (key derivation functions);
- šifrovací schémata;
- schémata pro autentizaci zpráv.

Vše doplňuje popis technik dle syntaxe ASN.1. Doporučení jsou formulována pro obecné (tj. nekonkretizované) aplikace v počítačích a komunikačních systémech a jsou poměrně flexibilní.

Funkce pro odvozování klíčů

Úkolem této funkce (funkce pro odvozování klíčů) je vytvořit nový (odvozený) klíč z původního (základního) klíče a dalších parametrů. Tímto základním klíčem je zde míněno heslo a ostatními parametry jsou tzv. sůl (salt – tato by měla být generována náhodně a měla by být minimálně 64 bitů dlouhá) a stav čítače. K odvození klíčů je použita pak hashovací funkce (obvykle MD5 či SHA-1). Délka odvozeného klíče je omezena délkou výstupu hashovací funkce (tj. pro MD5 to je 128 bitů, pro SHA-1 to je 160 bitů).

Poznámka. V návaznosti na chystanou normu AES se již objevila – zatím ve velice předběžné verzi – hashovací funkce SHA-512, jejíž výstup , jak název napovídá, má délku 512 bitů.

V dokumentu PKCS#5 je heslem míněn oktetový řetězec (řetězec osmibitových znaků) libovolné délky. Obvykle je pro kódování běžného textu použito nějaké standardní pravidlo (ASCII či UTF-8).

Obecný přístup ke kryptografii používající hesla kombinuje heslo se „solí“ a takto je odvozován klíč. „Sůl“ je pak jakýmsi parametrem velké množiny klíčů a nemusí být utajována. I když protivník může zkonstruovat množinu všech možných hesel (slovníkový útok), bude pro něj obtížné zkonstruovat množinu všech možných klíčů – pro každé heslo existuje velké množství klíčů. Protivník tudíž je nucen prohledávat hesla pro každou konkrétní „sůl“.

Používán je i následující přístup, který má za cíl zvýšit výpočetní nároky totálních zkoušek. Při odvození klíče se použije dlouhá série iterací (např. výpočet pomocí hashovací

funkce), řekněme 1000 a zatímco osoba znající správné heslo je schopná provést tento počet iterací, osoba, která zkouší různá hesla již není schopna pro každou z možností toto provést.

V materiálu PKCS#5 jsou popsány dvě funkce pro odvozování klíčů z hesla: PBKFD1 a PBKFD2. První z nich již není doporučována pro nové aplikace, zde proto bude popsána pouze druhá funkce PBKFD2.

Postup výpočtu DK:

DK = PBKDF2 (P, S, c, dkLen)

1. l = CEIL (dkLen / hLen) ,
   r = dkLen - (l - 1) * hLen .

Zde l je počet hLen-oktetových bloků DK (zaokrouhlený nahoru), r je počet oktetů posledního bloku, CEIL(x) – nejmenší celé číslo větší než x.

2. Postupně pro každý blok DK spočteme

   T_1 = F (P, S, c, 1) ,
   T_2 = F (P, S, c, 2) ,
   ...
   T_l = F (P, S, c, l) ,

   kde F je xor (mod 2) součet

   F (P, S, c, i) = U_1 \xor U_2 \xor ... \xor U_c

   a

   U_1 = PRF (P, S || INT (i)) ,
   U_2 = PRF (P, U_1) ,
   ...
   U_c = PRF (P, U_{c-1}) .

   INT (i) je 4-oktetové kódování celého čísla i, nejvýznačnější oktet je první.

3. Konkantenací těchto bloků (prvních dkLen oktetů) získáme odvozený klíč.

   DK = T_1 || T_2 || ... || T_l<0..r-1>

Zde PRF je vhodná pseudonáhodná funkce, hLen je délka jejího výstupu, P je heslo, S je „sůl“, c stav čítače, dkLen je zamýšlená délka klíče (nejvýše (2^32 - 1) * hLen) a DK je získaný odvozený klíč.

Šifrovací schémata vycházející z hesla

Typickým využitím těchto schémat je ochrana soukromého klíče, kde příslušná zpráva obsahuje informaci o soukromém klíči (dle PKCS#8).

Opět existují dva popsané postupy, první se opírá o využití PKBDF1 v kombinaci s blokovou šifrou (jako jsou DES, RC2 v módu CBC). Zde bude popsán pouze druhý postup opírající se o PBKDF2 (v rfc2898 je pak popsáno užití se šifrovým algoritmem RC5).

PBES2:

A.Zašifrování zprávy M pomocí hesla P (výsledkem je šifrový text C):

1. Spočteme DK = KDF (P, S, c, dkLen) .
2. Zašifrujeme zprávu M (odpovídajícím algoritmem) s pomocí klíče DK.

(zde P je heslo, S je sůl, c je stav čítače a dkLen určuje délku odvozeného klíče DK, M je zpráva).

B.Dešifrování šifrového textu C heslem P pro získání otevřeného textu M:

1. Spočteme DK = KDF (P, S, c, dkLen) .
2. Dešifrujeme zprávu M (odpovídajícím algoritmem) s pomocí klíče DK.

Schema pro autentizaci zprávy

Toto schéma obsahuje vytvoření MAC (autentizační kód zprávy) a verifikaci tohoto kódu. MAC je přitom vytvářen pomoci klíče a verifikace MAC probíhá využitím téhož klíče. V kryptografii opírající se o používání hesla je tímto klíčem samo heslo. Je popsáno jediné schéma PBMAC1.

A.Vytváření MAC:

1.Stejnou cestou jako výše (předešlý odstavec) spočteme odvozený klíč.
DK = KDF (P, S, c, dkLen) .
2. Zpráva M je zpracována odpovídajícím schématem pro autentizaci zprávy při využití odvozeného klíče DK a je získán autentizační kód T.

B. Ověření MAC probíhá analogickou cestou.

Schématem pro autentizaci zprávy zde může být např. HMAC-SHA-1 opírající se o využití hashovací funkce SHA-1. Klíč v tomto schématu má proměnlivou délku a autentizační kód T má délku 160 bitů (FIPS-180-1).

Shrnutí

Postupy v materiálu rfc2898 patří mezi dnes běžně užívané metody práce s heslem. Nejsou to však cesty jediné. V článcích [2] , v podkladových materiálech skupiny P1363 (Study Group on Password-Based Authenticated-Key-Exchange Methods) lze nalézt celou řadu novodobých postupů pro práci s heslem. Vzhledem k tomu, že těchto materiálů je povícero (minimálně pět, je však možné, že před zpracováním příslušného dokumentu ještě nějaké přibudou) byl by výklad těchto technik značně obsáhlý.

Odkazuji zainteresovaného čtenáře proto přímo na tyto články – již rozpracovaný dokument P1363a (Amendment, současná verze - Draft 5) se těmito technikami zabývat nebude. Výjimkou je definice funkce KDF2 (funkce pro odvození klíčů), která se od výše popsané funkce PKBDF2 liší v některých detailech a samozřejmě v obecnějším použití.

Teprve nově vzniklá skupina (The IEEE P1363 Study Group for Future Public-Key Cryptography Standards) bude zpracovávat dokument, který by měl obsahovat návrh postupů pro práci s heslem (tato skupina byla zformována teprve na počátku tohoto roku a zatím nevydala žádný dokument - resp. draft).

Za zmínku však stojí materiál [2.6]. Jeho obsahem však není popis ještě konkrétní volba postupů a technik, ale popisuje spíše cíle, které bude sledovat budoucí standardizace.

Literatura

[1] rfc 2898, Burt Kaliski: PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

[2] *návrhy pro P1363:*

[2.1] Taekyoung Kwon: Ultimate Solution to Authentication via Memorable Password

[2.2] David Jablon: Strong Password-Only Authenticated Key Exchange

[2.3] Thomas Wu:The Secure Remote Password Protocol

[2.4] Philip MacKenzie and Ram Swaminathan: Secure Network Authentication with Password Identification

[2.5] Mihir Bellare and Phillip Rogaway :The AuthA Protocol for Password-Based Authenticated Key Exchange

Následující materiál shrnuje podmínky, jaké by měla splňovat chystaná norma.

[2.6] Bellare, Jablon, Krawczyk, MacKenzie, Rogaway, Swaminathan & Wu : Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange Methods

E. **Letem šifrovým světem**

Informace pro odběratele e-zinu. Prosím nepřehlédněte změnu e-mail spojení. Od 1.12.2000 nastupuji na ÚOOÚ, kde se budu zabývat problémy spojenými s elektronickým podpisem. Moje e-mail adresa tedy bude cca od 4.12.2000 vondruskap@uoou.cz (upřesním dodatečně). Adresa pavel.vondruska@post.cz je stále platná.

1. Pro zájemce o bezpečnost mobilních telefonů doporučuji nově publikovaný článek autorů Slobodana Petroviče a Amparo Fúster-Sabatera. Je zde zveřejněna kryptoanalýza algoritmu A5/2 (slabší verze A5/1, který se užívá v mobilních telefonech i na našem území). Publikovaná metoda dokazuje, že složitost je jen dvě na sedmnáctou http://eprint.iacr.org/2000/052.pdf .

2. Jako bývalý šachista si nemohu odpustit zprávu ze šachového světa. Zápas o mistra světa mezi Garry Kasparovem a jeho bývalým žákem Vladimirem Kramnikem skončil vítězstvím pětadvacetiletého Kramnika ! Garry Kasparov patnáct let neprohrál zápas s žádným člověkem (1x prohrál s počítačem). Nyní v zápase na šestnáct partií 2x prohrál a 13x remizoval (stav před poslední partií). Kramnik je sympatický vysoký mladý sebevědomý muž. Na závěr jedna z jeho vět, kterou jsem si zapamatoval: "Nelze srovnávat šachy s politikou. Šachisté zápasí čestně, v politice nevítězí vždy moudřejší nebo výjimečnější."

3. Pokud potřebujete informace o stavu zákonodárství v oblasti elektronického podpisu (resp. digitálního podpisu) , pak můžete využít informace na URL adrese http://rechten.kub.nl/simone/ds-lawsu.htm . Jsou zde uvedeny informace ze všech států světa. Bohužel aktualizace - alespoň v případě České republiky - není příliš dobrá. Na serveru je uvedeno, že poslední aktualizace byla provedena 17.10.2000.

4. Také nevěříte elektronickému podpisu ? Nelíbí se Vám skutečnost, že se nepodepisujete vy osobně, ale podepisuje vás počítač, který může být značně nedůvěryhodný? Pak vás jistě zaujme článek známého odborníka, kryptologa Bruce Schneiera "Why Digital Signatures Are Not Signatures" . Článek vyšel 15.11.2000 ve známém elektronickém časopise Crypto-Gramm , http://www.counterpane.com .

5. Zajímavý článek o skutečné kybernetické válce mezi hackery z Izraele a Palestiny si můžete přečíst na http://www.zdnet.com/zdnn/stories/news/0,4586,2647934,00.html

6. Další zajímavý článek od B.Scneiera a C.Ellisona "10 Risks of PKI" lze získat na URL adrese : http://www.counterpane.com/pki-risks.html

7. Legendární Enigma, která byla ukradena z muzea v Bletchley Parku (viz zpráva v minulém čísle), byla vrácena na své místo http://news.bbc.co.uk/hi/english/uk/newsid_977000/977127.stm

8. O čem jsme psali před rokem ?
   Crypto-World 11/99 http://www.mujweb.cz/veda/gcucmp/casopis/crypto11_99.html
   A. Jak je to s bezpečností eliptických kryptosystémů ? (Ing. Pinkava)
   B. Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4
   C.Y2Kcount.exe - Trojský kůň v počítačích
   D.Matematické principy informační bezpečnosti (Dr. Souček)

F. Závěrečné informace

1.Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL , na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp .

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2.Registrace / zrušení registrace

Pokud máte zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3.Spojení

běžná komunikace, zasílání příspěvků

p.vondruska@nbu.cz	-	do 30.11.2000
vondruskap@uoou.cz	-	od 3.12.2000 (?)
pavel.vondruska@post.cz	-	osobní poštovní adresa, registrace odběratelů
pavel.vondruska@sms.paegas.cz	-	zasílání SMS