

OpenPGP v ČR

Roman Pavlík, TNS a. s.

<rp@tns.cz>

Trusted Network Solutions, a.s.

Praha, 5. března 2002

Historie PGP

- 1991 PGP 1.0 (Phillip R. Zimmermann) MD4, RSA.
- 1991-1993 PGP 2.0, PGP 2.1, PGP 2.2 – bugfix releases.
- 1993 PGP 2.3[a] int. freeware, MD5, IDEA, RSA, změna způsobu podpisu zprávy, nekompatibilita s PGP 2.[0-2]
- 1993 PGP 2.4.x (ViaCrypt), komerční verze, ADK.
- 1994 PGP 2.5 (MIT), US freeware – získán souhlas s implementací algoritmu RSA, nekompatibilita.
- 1995-1998 PGP 2.6ui (různí autoři), dlouhé RSA klíče (až 8192 bitů), odstraněny problémy s DH/DSS (PGP 2.64).
- 1996 PGP 2.6.3i (Ståle Schumacher), pokus o sjednocení verzí.

PGP 1.0 byla kryptograficky slabá a nekompatibilní s jakoukoli jinou verzí. Touto verzí začal spor Phillipa R. Zimmermanna (PRZ) s vlastníkem autorských práv k algoritmu RSA a později také s vládou Spojených států (pro podezření z porušení exportních omezení ITAR*).

Phillip R. Zimmermann udělil licenci na vývoj a prodej komerční verze společnosti ViaCrypt.

Rychlý vývoj se ustálil – mimo území Spojených států byla užívána freewarová verze PGP 2.3a,[†] ve Spojených státech se prodávala komerční verze PGP 2.4.x.

PGP 2.4.x byla určena pro komerční užití, poprvé se zde objevila možnost vynutit si šifrování dalším „firemním“ klíčem. Tento princip byl později použit ve vyšších verzích PGP pod názvem Additional Decryption Key (ADK).

MIT se snažil vyřešit licenční problém PGP ve Spojených státech, výsledkem bylo získání RSA licence pro PGP 2.5 freeware, licenční ujednání ale nařizovalo nekompatibilitu s dosud užívanými implementacemi RSA v PGP.

V roce 1996 vytvořil Ståle Schumacher z vývojové větve PGP 2.6 verzi PGP 2.6.3i s cílem opravit chyby a sjednotit verze – na dlouho dobu nejpoblárnější verze.

*International Traffic in Arms Regulations (ITAR) – pravidla regulace mezinárodního obchodu se zbraněmi.

[†]Autoři algoritmu RSA, Rivest, Shamir a Adleman, publikovali výsledky své práce dříve, než získali na algoritmus patent. Tento postup znemožnil získání patentu ve většině zemí s výjimkou Spojených států kde je možné patent získat i na dílo, které již bylo představeno veřejnosti.

Historie PGP

1995-1996 PGP 4.0, PGP 4.5 (ViaCrypt) komerční verze, samostatný podpisový a šifrovací klíč, částečná podpora DH klíčů (PGP 4.5.1), Netscape plugin.

1996 PGP Inc. kupuje ViaCrypt.

1997 PGP 5.0 (PGP Inc., MIT), DH/DSS, RSA (komerční verze), SHA-1, MD5, IDEA, 3DES, CAST. **Ve verzi 5.0i bezpečnostní chyba – neinteraktivně vytvořené klíče s použitím /dev/random neobsahují dostatek entropie.**

1997 Vzniká pracovní skupina IETF – první draft OpenPGP.

1997 NAI kupuje PGP, Inc.

V letech 1995 a 1996 pokračoval ViaCrypt ve vývoji komerční verze PGP, vznikl plugin pro Netscape, byla přidána možnost vytvořit klíč určený pouze pro šifrování a další klíč určený pouze pro podepisování.

Začátkem roku 1996 bylo uzavřeno vyšetřování PRZ bez vznesení jakéhokoliv obvinění. Po urovnání sporu založil PRZ společnost PGP, Inc., která koupila ViaCrypt, dosavadního výrobce komerční verze. V té době začala práce na nové verzi PGP s cílem nahradit algoritmus RSA a přidat podporu pro symetrické šifry CAST128 a TripleDES. Verze nesla pracovní označení PGP 3.0, ale na trh byla uvedena pod označením PGP 5.0.

PGP 5.0 byla první verzí, která podporovala DH/DSS klíče, symetrickou šifru CAST a vzorkování SHA1. Nejen použité algoritmy, ale i výsledný formát zprávy je nekompatibilní s PGP 2.6.x. PGP 5.0 pro operační systémy Microsoft Windows a MacOS obsahovala grafické rozhraní a byla integrována do prostředí těchto operačních systémů. Zdrojové kódy řádkové verze byly dostupné a snadno přeložitelné na jiných (otevřených) operačních systémech.

PGP 5.0 se stala základem pro práci návrh formátu OpenPGP, která započala v roce 1997.

V roce 1997 se společnost PGP, Inc. stala cílem akvizice společností Network Associates, která vznikla fúzí McAfee a Network General se snahou vytvořit silnou softwarovou firmu zaměřenou na bezpečnost dat.*

*Společnost Network Associates získala ve stejném roce akvizicí i společnost Trusted Information Systems, Inc., výrobce „legendárního“ FWTK i jeho komerční verze – firewallu Gauntlet.

Historie PGP

- 1997 G10 0.0 (Werner Koch), The GNU Encryption and Signing Tool.
- 1998 PGP 5.5x (NAI Inc.), additional decryption key.
- 1998 PGP 6.0 (NAI Inc.), RSA, PGPDisk, DRK, ADK.
- 1998 Seminář EurOpenu na téma PGP, PRZ v Praze.
- 1998 OpenPGP standard, RFC 2440.
- 1999 PGP 6.5 (NAI Inc.) PGPnet (IPSec/IKE). NAI používali značku PGP pro další produkty (PGP e-ppliance server). PGP 6.5.3 byla první verze, kterou bylo možné exportovat v binární podobě. NAI nezveřejnili zdrojové kódy.

Werner Koch zveřejnil kód G10 verze 0.0 22. 12. 1997. Základy GnuPG byly položeny. Cílem bylo vytvořit nástroj kompatibilní s PGP, avšak s GNU licenci. Werner Koch začal na projektu GnuPG pracovat v době „největší slávy“ PGP.

Společnost NAI doplnila do PGP vlastnosti známé z předešlých komerčních verzí od ViaCryptu, ve verzi PGP 5.5x bylo hlavní novinkou možnost používat Additional Decryption Key (ADK), princip uživatelé komerčních verzí znali již z PGP 2.4.x z roku 1993.

V další verzi, PGP 6.0, NAI doplnili plnou podporu RSA klíčů včetně možnosti jejich generování. Doplněn byl také virtuální driver disku pro operační systémy Microsoft Windows a MacOS, který prováděl transparentní šifrování/dešifrování dat ukládaných na pevný disk.

V roce 1998 byl zveřejněn standard OpenPGP (RFC 2440). Cesta k výrobě software plně kompatibilního s PGP byla volná.

Verze PGP 6.5 byla pokusem společnosti NAI integrovat řadu dalších funkcí, které s původním cílem PGP jen pramálo souvisely, jako byl zejména PGPnet – implementace IPSec/IKE pro operační systém Microsoft Windows. PGP 6.5.3 se zapsala do historie jako první verze, k níž NAI nezveřejnili zdrojové kódy a také jako první verze, pro kterou již neplatila exportní omezení a mohla být ze Spojených států legálně vyvezena. V té době se NAI pokusila marketingově využít popularitu značky PGP a pod tímto označením začala nabízet např. PGP e-ppliance, což byl firewall Gauntlet prodáváný společně se servery Sun Microsystems. S původním PGP již tento produkt neměl společného vůbec nic.

Historie PGP

- 1999 GnuPG 1.0 (Werner Koch), první verze pro provozní podmínky, nástupce G10.
- 2000 PGP 7.0 (NAI Inc.) Personal Firewall, Personal IDS, nový formát RSA klíče – podpora ADK, NAI poskytovali zdrojové kódy, do binární podoby nelze přeložit.
- 2001 PRZ odešel ze společnosti Network Associates.
-
8. 3. 2002 **Vývoj PGP Desktop zastaven.** (Neúspěch NAI nalézt kupce pro celou produktovou řadu PGP Desktop.)

GnuPG 1.0 (G10 existoval do verze 0.2.7, verze 0.2.8 byla dokončena s novým názvem, The GNU Privacy Guard, GnuPG) byla první stabilní implementací standardu OpenPGP s GNU licencí. Podporovala algoritmy DSA, Elgamal, vzorkovací funkce MD5, RIPEMD a SHA1 a symetrické algoritmy CAST, 3DES a AES. Umožňovala snadné přidání dalších algoritmů prostřednictvím konceptu „extension modules“. Tak byla přidána podpora pro RSA (mimo území Spojených států) a symetrického algoritmu IDEA (pro země, kde nebyl tento algoritmus patentován).

V roce 2000 uvedla NAI PGP 7.0, do které integrovali „personal firewall“, paketový filtr pro Microsoft Windows na „personal IDS“. Protože v roce 2000 vypršela platnost patentu RSA (patent byl časově omezen), nic nebránilo jeho volnému užití. NAI ve verzi PGP 7.0 uvedlo plnou podporu RSA klíčů pro verze PGP 2.6.x i nový formát RSA klíčů, který umožňoval vytvořit RSA klíč určený pouze pro šifrování a RSA klíč určený pouze pro podepisování. Na rozdíl od verze PGP 4.5 od společnosti ViaCrypt z roku 1996 se ve verzi PGP 7.0 společně s novými RSA klíči používala symetrická šifra CAST a vzorkování pomocí SHA1. PGP 7.0 bylo opět dostupné včetně zdrojových kódů, které však nejsou úplné. (NAI obnovili poskytování zdrojových kódů od verze PGP 6.5.8, z nichž však již nebylo možné získat binární verzi.)

Phill R. Zimmermann opustil v roce 2001 společnost Network Associates. Ve svém prohlášení ujistil uživatele PGP, že až do verze 7.0.3, která byla jako poslední uvedena za jeho působení ve společnosti NAI, neobsahovalo PGP žádná „zadní vrátka“.

V březnu 2002 NAI rozeslali některým zákazníkům dopis, ve kterém oznámili, že se nepodařilo nalézt kupce pro produktovou řadu PGP a s vývojem produktu PGP desktop NAI končí. PGP desktop je převedeno do režimu „maintenance mode“ – servisní smlouvy nebudou po skončení platnosti obnoveny.

Algoritmy PGP a GnuPG

Algoritmy	PGP 2.6.x	PGP [56].x	PGP 7.x	GnuPG 1.0.6
RSA	2048	2048	2048*	2048 [†]
DSA	–	1024	1024	1024
ELGamal	–	4096	4096	4096
MD5	<i>ano</i>	ano	ano	ano
RIPEDM	ne	ano	ano	ano
SHA-1	ne	<i>ano</i>	<i>ano</i>	<i>ano</i>
IDEA	<i>ano</i>	ano	ano	(ano)
CAST	ne	<i>ano</i>	<i>ano</i>	<i>ano</i>
3DES	ne	ano	ano	ano
AES	ne	ne	ano	ano

PGP 2.6.x není kompatibilní s formátem OpenPGP. PGP [567].x a GnuPG emulují formát zpráv pro zajištění zpětné kompatibility s PGP 2.6.x. Jednou z nutných podmínek dosažení kompatibility je dostupnost příslušného algoritmu pro zajištění kompatibility mezi verzemi.

Na obrázku jsou *zvýrazněným písmem* vyznačeny algoritmy, které se v příslušné verzi PGP anebo GnuPG použijí implicitně.

GnuPG velmi přísně dodržuje GNU licenci. Proto neobsahuje podporu algoritmu IDEA interně – ve Spojených státech a většině západní Evropy je algoritmus IDEA chráněn patentem.

*PGP verze 7.x zavádí nový formát RSA klíčů o velikosti až 4096 bitů. Plná podpora těchto klíčů v GnuPG 1.0.7 včetně možnosti jejich generování.

[†]GnuPG 1.0.6 podporuje import RSA klíčů pro zajištění kompatibility s PGP 2.6.x, nepodporuje generování těchto klíčů.

GnuPG a IDEA

- PGP 2.6.3[i] používá jiný formát zpráv než OpenPGP, RSA klíče, šifra IDEA, MD5 hash.
- GnuPG formát PGP 2.6.3[i] emuluje (dostupné jen šifrování nebo podepisování).
- Symetrický algoritmus IDEA chráněn patentem, není součástí GnuPG (striktní dodržování GNU licence).
- **IDEA není v ČR patentován**, GnuPG extension modul pro šifru IDEA
<http://www.gpg.cz/rp/GnuPG/extensions/idea.c>

PGP 2.6.3[i] byla velmi populární a rozšířená verze, někteří uživatelé ji používají dodnes. Pro dosažení kompatibility s touto verzí je nutné:

- podporovat zprávy ve formátu PGP 2.6.x (RFC 1991), GnuPG podporuje emulaci tohoto formátu – podpora pro šifrování nebo podepisování, GnuPG nepodporuje přímo šifrování a podepisování zpráv ve formátu PGP 2.6x;
- podporovat RSA klíče, šifrovací algoritmus IDEA a vzorkovací funkci MD5.

GnuPG interně podporuje RSA klíče a vzorkovací funkci MD5. Přímou nepodporuje algoritmus IDEA, který je chráněn patentem ve Spojených státech (patent vyprší 25. května 2010), Japonsku (patentová přihláška podána 16. května 1991, patent zatím nebyl vydán), Rakousku, Francii, Německu, Itálii, Holandsku, Španělsku, Švédsku, Švýcarsku a Velké Británii (patent vyprší 16. května 2011). Algoritmus IDEA lze za velmi specifických podmínek použít pro nekomerční užití, licence je dostupná na <http://www.media-crypt.com/>.

Algoritmus IDEA není na území ČR chráněn patentem, podporu lze do GnuPG přidat prostřednictvím rozšiřujících modulů (extension modules). IDEA modul je dostupný na výše uvedené adrese. Na stejné adrese je k dispozici RSA modul, který po zapracování RSA přímo do GnuPG slouží spíše pro inspiraci při vytváření vlastního modulu.

GnuPG a PGP 2.6.x

- standardní import klíčenky PGP 2.6.x plně podporován.
- šifrování pro PGP 2.6.x

```
gpg --rfc1991 --cipher-algo idea --compress-algo 1  
--encrypt --recipient alice tajny.txt
```
- podepisování pro PGP 2.6.x

```
gpg --local-user 0x24E2C409 --sign document
```
- podepisování a šifrování: vytvoření podpisu
v samostatném souboru, převedení zprávy do formátu PGP
paketu, spojení podpisu a PGP paketu, zašifrování. Viz.
<http://www.gnupg.cz/gph/en/pgp2x.html>

Pro šifrování zprávy do formátu PGP 2.6.x je nutné použít přepínače specifikující emulaci formátu podle RFC 1991, zvolit šifrovací algoritmus IDEA a kompresní algoritmus kompatibilní s PGP 2.6.x. Ve verzi GnuPG 1.0.7 bude nový přepínač `--pgp2`, který nastaví výše uvedené přepínače. Nesmí být použity jiné než RSA klíče pro formát PGP 2.6.x, v opačném případě nebude zpráva verzí PGP 2.6.x dešifrovatelná.

Podpisování zprávy pro formát PGP 2.6.x se neliší od běžného podepisování pomocí GnuPG. I zde je nutno používat výhradně RSA klíče v3.

Dešifrování a verifikace zprávy ve formátu PGP 2.6.x se nijak neliší od dešifrování či verifikace zprávy ve formátu OpenPGP, tedy `gpg soubor.pgp`.

Podpisování a šifrování pro PGP 2.6.x je nutné provést ve čtyřech krocích:

1. vytvoření podpisu zprávy v samostatném souboru:

```
foo% gpg --detach-signature --recipient alice --local-user 0x24E2C409 \  
soubor.txt
```
2. převedení zprávy do formátu PGP paketu

```
foo% gpg --store -z 0 --output soubor.lit soubor.txt
```
3. spojení podpisu a PGP paketu

```
foo% cat soubor.sig soubor.lit | gpg --no-options --no-literal --store \  
--compress-algo 1 --output soubor.z
```
4. zašifrování klíčem příjemce

```
foo% gpg --rfc1991 --cipher-algo idea --no-literal --encrypt \  
--recipient alice --output soubor.pgp soubor.z
```


Keyserver PKSD

Keyservery pgp.net používají pksd-0.94 (Marc Horowitz)

- implementace není kompatibilní s OpenPGP
 - servery nepodporují více než jeden subklíč;
 - servery nepodporují revokační certifikáty.
 - implementace není robustní (dnes již více než 1,6M klíčů)
 - nekonzistentní databáze (jisté klíče nelze vyhledat).
-
- vývoj OpenPGP serverů www.keyserver.net,
www.cryptnet.net, www.fi.muni.cz/~xbanszel
 - diskuze o distribuovaném modelu

Veřejné PGP klíče jsou uloženy v síti serveru klíčů pgp.net, které nijak neřeší jejich autentičnost – slouží pouze jako databáze veřejných klíčů.

Původní práce Marca Horowitze vznikla dříve než byl popsán OpenPGP standard, s tímto standardem není kompatibilní. Na server klíčů není možné uložit klíč, který má více subklíčů než jeden.

Velikost databáze narostla do nečekaných rozměrů, v pksd dočasně vyřešeno rozložením do více souborů. Stav je nevyhovující – databáze je nekonzistentní, nepodporuje konkurenční přístup. Vývoj pksd nepokračuje.

Existuje několik nových implementací OpenPGP keyservru.

- www.keyserver.net – komerční implementace, zdrojové kódy nejsou dostupné, není dále vyvíjen;
- www.cryptnet.net – GPL licence, implementováno nad SQL databází PostgreSQL, nedostatečný výkon;
- www.fi.muni.cz/~xbanszel – diplomová práce Martina Banzela, dokončena první fáze, zatím není určeno pro provozní podmínky.

Vzhledem k rychle rostoucímu počtu klíčů se uvažuje o distribuovaném modelu databáze veřejných PGP klíčů – mj. snaha snížit komunikační zátěž PGP keyservrů.

Analýza pubringu

březen 2002:

Počet klíčů uložených na keyserveru: 1 413 462.

Počet UID uložených na keyserveru: 1 611 963.

Počet klíčů podepsaných alespoň jedním cizím klíčem: 155 667.

Algoritmy	# klíčů	% z celku
RSA	140 524	9,9418 %
DSA/ELGamal	1 272 731	90,0435 %
ELGamal	219	0,0155 %

Analýza databáze serveru klíčů z března 2002 ukazuje vzrůstající zájem o OpenPGP. Z údajů je alarmující velice nízký počet klíčů, které byly podepsány klíčem jiného subjektu. Jen 10% klíčů používá model „pavučiny důvěry“.*

Tabulka zastoupení jednotlivých klíčů vyvrací fámu o RSA klíči formátu PGP 2.6.x jakožto nejpobulárnějším druhu PGP klíčů. Je zajímavé, že existuje skupina uživatelů PGP 2.6.3i, kteří bez racionálního důvodu odmítají přechod na OpenPGP (GnuPG).

*Více informací o „pavučině důvěry“ viz. příspěvek Wernera Kocha nebo publikace The GNU Privacy Handbook.

OpenPGP v ČR

Rychlý růst popularity PGP

prosinec 1997 200 klíčů v doméně .cz

prosinec 1998 1 200 klíčů v doméně .cz

březen 2002 9 578 klíčů v doméně .cz (0,59 % všech PGP klíčů)

GnuPG v ČR

srpen 2000 české zrcadlo GnuPG <http://www.gnupg.cz/>

prosinec 2001 dokončena lokalizace (Magda Procházková)

<ftp://ftp.gnupg.cz/pub/local/cs.po>

duben 2002 seminář EurOpenu na téma GnuPG

V prosinci 1998 byl v příspěvku Josefa Pojsla „PGP v České republice“ na semináři EurOpenu prezentován graf nárůstu klíčů v doméně .cz. Graf znázorňoval exponenciální růst počtu klíčů a tím i popularity PGP v České republice.

Údaje z března 2002 tento trend potvrzují a to i přes strastiplné období, kterým PGP nepochybně prošlo. Díky existenci otevřeného standardu OpenPGP a vynikající stabilitě GPL implementace, GnuPG, lze očekávat i nadále rychle rostoucí počet klíčů.

Servery <http://www.gnupg.cz> a <ftp://ftp.gnupg.cz> jsou v provozu od srpna 2000, a jsou zrcadlem serverů [gnupg.org](http://www.gnupg.org). V době vánoc 2001 byla dokončena práce na lokalizaci GnuPG 1.0.6 (použita čeština ISO-8859-2). Připomínky k překladu lze zasílat na adresu gnupg-lokalizace@gnupg.cz. Česká lokalizace bude součástí distribuce GnuPG verze 1.0.7.

V roce 2002 se připravuje testovací provoz nového serveru OpenPGP klíčů v ČR.

Reference

- [1] <http://www.gnupg.cz/docs.html>
Dokumentace k projektu GnuPG, RFC2440,
PGP 5–GnuPG HowTo, Replacing PGP 2.x with GnuPG.
- [2] <http://www.pgpi.com/>
Freeware PGP, dokumentace PGP, řada odkazů.
- [3] <http://dtype.org/keyanalyze/>
Analýza databáze PGP klíčů z keyserverů.
- [4] <http://www.gpg.cz/rp/GnuPG/>
LaTeXová verze The GNU Privacy handbook, IDEA a RSA
moduly pro GnuPG, lokalizace.