



# PGP šifrovanie e-mailov a súborov

[Dokument naposledy aktualizovaný: júl 2019]

PGP šifrovanie (iniciály názvu Pretty Good Privacy) je jedným z vhodných spôsobov, ako ochrániť dôvernosť a integritu svojich správ a dát. Využíva asymetrické šifry, teda máme páry kľúčov. Na šifrovanie máme verejný kľúč a na dešifrovanie súkromný. Ak použijeme vhodnú veľkosť šifrovacích kľúčov a dodržíme zásady ich bezpečného používania, naše správy prakticky nebude možné dešifrovať, aj keby ich útočník odchytil.

## Ako to funguje?

Šifrovanie:

Verejným kľúčom príjemcu zašifruje odosielateľ správu / dáta a dešifrovať ich môže len príjemca - majiteľ súkromného kľúča.

Podpisovanie:

Odosielateľ podpisuje správu svojim súkromným kľúčom a príjemca verejným kľúčom odosielateľa overí jeho autenticitu.



Tieto dve operácie môžeme používať súčasne, aj samostatne. Pre tieto operácie sa odporúča používať rôzne páry kľúčov. Našťastie mnohé implementácie PGP vytvárajú podkľúče určené samostatne pre šifrovanie a podpisovanie automaticky.

Pre používanie odlišných párov kľúčov existujú viaceré dôvody. Jedným z nich sú širšie možnosti manažovania kľúčových párov. Predstavme si firmu, v ktorej zamestnanci používajú PGP šifrovanie a podpisovanie e-mailov. Ak napríklad zamestnanec odíde z firmy, jeho nadriadený si potrebuje zachovať prístup k jeho pracovnej e-mailovej komunikácii, teda potrebuje súkromný šifrovací kľúč





zamestnanca. Podpisový kľúč zamestnanca však musí byť zneplatnený, aby ho niekto iný nemohol zneužiť. Oddeleným párom kľúčov môžeme tiež nastaviť rôzne dátumy expirácie.

## Parametre kľúčov a "best practices"

- Odporúčaná veľkosť RSA kľúčov je 4096 bitov. Môžeme použiť aj ECC kľúče, no kvôli väčšej kompatibilite a z praktického hľadiska porovnateľnej bezpečnosti sa v tomto návode budeme sústrediť na RSA.
- Minimálna veľkosť RSA kľúča pre zachovanie rozumnej miery bezpečnosti: 2048 bitov.
- Odporúčaná maximálna veľkosť RSA kľúča pre zachovanie rozumnej použiteľnosti: 4096 bitov.
- Odporúčaná doba platnosti (primárne kľúče aj podkľúče): maximálne 2 roky.
- Doba platnosti môže byť v prípade potreby predĺžená pomocou súkromného primárneho kľúča.
- Je potrebné používať silné heslo (**passphrase**), ktoré nebudeme ukladať do Thunderbirdu a pod.
- <u>Bezpečné zdieľanie verejných kľúčov</u> napríklad výmenou podpísaných e-mailov, správou cez sociálne siete, alebo cez komunikačné aplikácie ako Signal, či WhatsApp, prípadne repozitáre verejných kľúčov ako Keybase.io; pričom iným kanálom je následne potrebné vymeniť si odtlačok prsta kľúča. Ak je to možné, ideálna výmena kľúčov je na osobnej úrovni.
- Nastavenie šifrovania predmetu správy a príloh (zapnutie štandardu PGP/MIME).
- Po skončení platnosti kľúčového páru ho revokujte.

## Bezpečnosť

Ako sme spomenuli vyššie, mnohé implementácie PGP automaticky vytvárajú podkľúče s odlišným použitím. Štandardne pri vytváraní nového kľúčového páru dostaneme:

- Primárny pár s právami podpisovať správy a certifikovať kľúče iných ľudí
- Podkľúč s právom šifrovať správy

Primárny kľúč teda predstavuje našu identitu. Môžeme ním vytvárať a zneplatňovať ďalšie podkľúče. Preto potrebujeme chrániť jeho súkromnú časť. Jednou z možností je vytvoriť si sadu kľúčov pre bežné použitie, ktorú si môžeme nahrať na všetky naše zariadenia. Vytvoríme druhý podkľúč a priradíme mu podpisové právo. Primárny kľúč si bezpečne zálohujeme a v bežnej sade kľúčov z neho odstránime súkromnú časť. Tak získame túto sadu kľúčov:

- Verejná časť primárneho kľúča (bez práv)
- Podkľúč s právom šifrovať správy
- Podkľúč s právom podpisovať správy

V prípade úniku takejto sady útočník nemôže vytvárať a zneplatňovať podkľúče, meniť ich dobu expirácie, vytvárať revokačné certifikáty, ani certifikovať kľúče iných ľudí. My však vieme uniknuté kľúče zneplatniť a vytvoriť si nové. Klient Kleopatra, ktorým sa budeme nižšie zaoberať, k januáru





2019 takéto sady kľúčov vytvárať nedokázal, no cez konzolu si vieme vlastnú sadu vytvoriť priamo cez nástroj GPG/GPG2. Návod nájdete nižšie, alebo aj napríklad <u>tu</u> a <u>tu</u>.

Vhodnou formou ochrany kľúčového páru je nastavenie doby expirácie. Ak by sa útočník dostal k podkľúču, tento bude zneplatnený po uplynutí expiračnej doby. Dobu expirácie je možné predlžovať len s použitím súkromnej časti primárneho kľúča. Tiež v prípade, že stratíte prístup ku svojmu kľúču, je vhodné, aby bol po istom čase automaticky zneplatnený.

Dôležitým bezpečnostným prvkom PGP kľúčov je heslo (**passphrase**). Ak sa útočník dostane k súkromnému kľúču obete, má zatiaľ v rukách len jeho zašifrovanú podobu. Používanie silného hesla môže zamedziť úspešnému zneužitiu kľúča, nakoľko techniky ako brute-force, či slovníkový útok, sú voči nemu neefektívne. Pre vytvorenie silného hesla odporúčame aplikovať všeobecné "best practices". Z bezpečnostného hľadiska je vhodné heslo neukladať do e-mailového klienta, ale radšej ho pri každom použití kľúča ručne vypísať.

## Dôveryhodnosť a overovanie PGP kľúčov

Keď získate verejný kľúč inej osoby, je vhodné overiť si, že jej skutočne patrí kontrolou "odtlačku prsta" (fingerprint) jej verejného kľúča. Môže sa totiž stať, že útočník využije techniku "man-in-themiddle" a podhodí vám svoj vlastný kľúč. Odtlačok prsta je vhodné obdržať iným kanálom, ako samotný kľúč, ideálne osobne, alebo telefonicky. Tento potom vieme porovnať s odtlačkom prsta kľúča.

Verejné kľúče vo svojej databáze môžete následne overovať (certifikovať) podpísaním svojim súkromným kľúčom. Takéto verejné kľúče pokladáte za plne overené. Aby ste však nemuseli veľké množstvo kľúčov a kľúče cudzích osôb overovať sami, existuje tzv. "web of trust" prístup. Ak kľúč, ktorý si chcete pridať do svojej databázy pred vami overili používatelia, ktorým veríte, že ho overili správne, môžete ho automaticky pokladať za overený. Vo vašej databáze máte možnosť nastaviť mieru dôvery / dôveryhodnosť kľúčom iných používateľov. Svojmu kľúču nastavíte úplnú dôveru, ostatným kľúčom podľa vášho uváženia úplnú, čiastočnú, žiadnu, prípadne neznámu mieru dôvery.

Konkrétnu politiku dôvery a overovania si môžete nastaviť podľa svojich preferencií. Ak napríklad cudzí kľúč podpísali traja ľudia, ktorým dôverujete len čiastočne, môžete ho považovať za plne overený. Ak ho podpísal jeden, alebo dvaja čiastočne dôveryhodní používatelia, kľúč pokladáte len za čiastočne overený. Podrobnejší popis problematiky môžete nájsť <u>tu</u>.





### Návod pre open-source softvér Enigmail pre Thunderbird

#### Inštalácia softvéru

 V e-mailovom klientovi Mozilla Thunderbird kliknite na menu a vyberte "Doplnky" -> "Doplnky". V ľavej lište vyberte "Rozšírenia" a vyhľadajte "Enigmail". Nájdený modul pridajte do programu Thunderbird.

	U-UI 5 THEMES COLL	S ections more	Q enigmail →
lter Results	Searc	h Results for "enigmail"	
CATEGORY All Add-ons	» Sort by	Relevance   Most Users   Top Rated   Newest   More *	
WORKS WITH Any Thunderbird All Systems	»	Enigmail FEATURED OpenPGP message encryption and authentication for Thunderbird and SeaMonkey. ***** (223): 134,075 users	+ Add to Thunderbird
TAG All Tags 92 matching results	»	Mail Redirect         TEATURED           Allow to redirect (a.k.a., "remail") mail messages to o recipients.         ************************************	+ Add to Thunderbird
	-	Mail Merge         REQUIRES RESTART         FEATURED           Mass Mail and Personal Mail         ************************************	+ Add to Thunderbird
	alat	EditEmailSubject (Edit email Subject) TOURISSESTART This module allows you to change/edit email subjec *****	+ Add to Thunderbird
	٩	Expression Search / GMailU ROUMESENA Powerful message searching through expressions. Tromfred totom' to see all messages from Fred to in the current view. Support regular expressions' ar click to search:	at + Add to Thunderbird Type Tom nd

2) Pri inštalácii vám pravdepodobne Enigmail oznámi, že nemáte nainštalovaný program GnuPG (Gpg4win). Môžete si ho nainštalovať vlastnoručne, alebo to necháte na Thunderbird – riaďte sa pokynmi. Pri inštalácii Gpg4win odporúčame vybrať aj komponent Kleopatra (ak používate MS Outlook, môžete pridať aj komponent GpgOL pre jeho podporu a pre rýchle šifrovanie súborov môžete využiť komponent GpgEX, ktorý pridá položku do kontextového menu (ktoré sa zobrazí po kliknutí pravým tlačítkom na súbor)).



ÚRAD PODPREDSEDU VLÁDY SR PRE INVESTÍCIE A INFORMATIZÁCIU	CSIRT.SK
d Newest More	
in and authentica	Choose Components Choose which features of Gpg4win you want to install.
7. Check the component install. Click Next to co	s you want to install and uncheck the components you don't want to ontinue.
Select components to ail") mail message	install: GrupG Gra Gra Gra Gra Gra Gra Gra Gr
IXT FEATURED Space required: 95.7%	ив
Gpg4win-3,1.5	
email Subjecty	Add to Thunderbird
ange/edit email subjects	

Vytváranie PGP kľúčov (bez primárneho kľúča určeného len na certifikáciu)

[Expertný návod pre vytvorenie zväzku kľúčov v odporúčanej konfigurácii nájdete v nasledujúcej podkapitole.]

- 1) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Správa kľúčov"
- 2) Kliknite na "Vytvoriť" -> "Nový pár kľúčov"

								Ē		83	
🐺 Get Messages 🔽 🧨 Write 🗸	Chat	Address Book	0	Tag 🗸 🎖 Quick Filte	r	Q Search «Ctr	!+K>			Ð	
a 🕎 Local Folders آن Trash اه Outbox	Thu	nderbird Ma	il -	Local Folde	s				•		
	Aco	counts									
	٥	View settings for	his a	account							
		Set up an account	:								
		🖂 Email 🛛 🖳 Ch	at	Rewsgroups	Feeds	🗚 ExQuilla					
		Create a new cale	nd	🗊 Enigmail Key Manag	ement					-	
				Eile Edit View Keys Search for: 🔎	erver Gener	ite New <u>K</u> ey Pair	☑ <u>D</u> isplay All Keys by	/ Default			
				Name		<ul> <li>Key ID</li> </ul>			Blacklist		EŞ.
	Ad	vanced Featur	es								
	Q	Search messages									
	4 fe	Manage message	fil								





3) Vyberte e-mail, ktorému chcete kľúče priradiť. Vytvorte si heslo a nastavte platnosť kľúčov maximálne na 2 roky. V záložke "Rozšírené…" zvoľte typ a veľkosť kľúča. Použitie eliptickej krivky by malo poskytnúť vyššiu rýchlosť a väčšiu bezpečnosť, no pokulhávať môže kompatibilita s príjemcami vašich správ. RSA je však tiež z praktického hľadiska pokladané za dostatočne bezpečné, pričom vylúčime riziko nekompatibility. V tomto prípade volíme veľkosť kľúča 3072, alebo 4096 bitov.

	🕤 Generate OpenPGP Key
Enigmail Key Management	Account / User ID 🔻
<u>File Edit View K</u> eyserver <u>G</u> enerate	Use generated key for the selected identity
Search for: 🔎	No passphrase
Name ^ Key ID	Passphrase Passphrase (repeat)
	Key expiry Advanced
	Key expires in 2 years T 🖾 Key does not expire
	Generate key Cancel
	Key Generation
	NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

- 4) Kliknite na "Generate key". Program začne generovať kľúč, no nič nehlási. Počkajte, kým sa ukáže oznámenie o ukončení. Proces urýchlite, ak počas neho budete vykonáva diskovo náročné operácie, nakoľko tým dodáte zdroj náhodnosti.
- 5) Po ukončení sa v rámci oznámenia zobrazí aj otázka, či chcete vytvoriť revokačný certifikát. Toto je vhodné, nakoľko v prípade straty či odcudzenia súkromného kľúča použijete tento certifikát na zneplatnenie kľúča. Uložte si ho na bezpečné miesto, ideálne offline úložisko. Podobne si zálohujte aj váš nový PGP kľúč.

## Nahrávanie verejných kľúčov na keyserver

Svoj verejný PGP kľúč môžete nahrať na vybraný keyserver, čo je služba, ktorá umožňuje jeho zdieľanie s verejnosťou. Používateľ, ktorý Vás bude chcieť šifrovane kontaktovať, tak získa ľahký prístup k tejto možnosti.

- 1) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Predvoľby"
- 2) Kliknite na "Zobraz Expertné nastavenia a menu"





oudsielanie in	uniter settings		
Základné nastavenia			
Súbory a zložky			
GnuPG bolo nájdené v	C:\Program Files (x86)\G	nuPG\bin\gpg.exe	
Použiť toto		Hľadať	
Passphrase Timeout			
Pamätať si heslo poča	s 5 📮 minutes of	inactivity (before needing	to re-enter it)
Zobraz Expertné nasta	venia a menu		Predvolené
Zobraz Expertné nasta	venia a menu		Predvolené
Zobraz Expertné nasta	venia a menu		Predvolené

3) Kliknite na záložku "Keyserver" a nastavte adresy serverov, ktoré chcete používať -> potvrďte. Ak si neviete vybrať keyserver, môžete použiť napríklad <u>pgp.mit.edu</u>, alebo <u>hkp://pool.sks-keyservers.net</u>. Väčšie keyserveri sa medzi sebou často synchronizujú, teda k samotnému výberu môžeme pristupovať voľnejšie.

Nastavenia Enigmail	
Základné Odosielanie Výber kľúča Rozšírené Keyserver Transfer Settings	
Zvoľte Vaše keyserver(y):	
hkps://hkps.pool.sks-keyservers.net, hkps://keys.mailvelope.com, hkps://pgp.mit.edu	
Example: pool.sks-keyservers.net, pgp.mit.edu	
✓ Always use first keyserver	
Automaticky sťahovať kľúče pre overenie podpisu	
z nasledujúceho keyservera:	
OK Zrušiť	

- 4) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Správa kľúčov"
- 5) Vyberte menu "Keyserver" odtiaľto môžete odoslať svoje verejné kľúče na nastavený keyserver (označte vybrané a zvoľte "Odoslať verejné kľúče"), aktualizovať svoju databázu, či hľadať kľúče, ktoré v nej ešte nemáte





۲		Správa kľúčov Enigmail	- • ×
<u>S</u> úbor <u>U</u> praviť <u>Z</u> obraziť	<u>K</u> eyserver	<u>V</u> ytvoriť	_
Hľadať 🔎	Obn	oviť vyb <u>r</u> ané verejné kľúče Ctrl+R	dľúče
Meno	<u>H</u> ľad	ať kľúče	
Þ	<u>O</u> do:	slať verejné kľúče	^
Þ	Uplo	ad to your provider's Web Key Directory	
Þ.	Obn	p <u>v</u> iť všetky verejné kľúče	
Þ	<u>N</u> ájd	i kľúče pre všetky kontakty	
Þ			
incident <incident@csi< p=""></incident@csi<>	rt.sk>	EC5177D3E4E11CE2	
Þ			
Þ			
			~

Pridávanie alternatívnych e-mailov do kľúčov

- 1) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Správa kľúčov"
- 2) Dvojklikom na vybraný kľúč otvorte okno, kam môžete pridávať nový e-mail
- 3) Vľavo dole kliknite na "Vyberte akciu..." a vyberte "Spravovať ID užívateľa"

9	Správa kľúčov Enigmail – 🗖 🗙	
Súbor Upraviť Zobraziť Keyserver V	Vlastnosti kľúča	×
HTadat' D	Hlavné ID užívateľa incident <incident@csirt.sk> Typ pár kľúčov Odtlačok prstu DFB9 E478 4304 CB18 AF97 E49D EC51 77D3 E4E1 1CE2 Also known as: CSIRT.SK <info@csirt.gov.sk></info@csirt.gov.sk></incident@csirt.sk>	
	incident <incident@csirt.gov.sk> Incident <incident@csirt.sk></incident@csirt.sk></incident@csirt.gov.sk>	
p inclaent <inclaent@csirt.sk> ▷ ▷</inclaent@csirt.sk>	Základné Certifications Structure	
D D D	Koniec platnosti Validity neznámy	Change
Р Р Б	You rely on certifications plne dôveryhodný	Change
	Vyberte akciu •	
	Spravovať 10 užívateľa Pridaj fotografiu Zmeniť heslo Zneplatniť Klúč Vytvoriť a uložiť revokačný certifikát	Zatvoriť

- 4) Kliknite "Pridať", vyplňte položky "meno" a "e-mail" a potvrďte
- 5) Teraz môžete zmeniť primárny e-mail kľúča (je prvý v poradí) jeho označením a kliknutím na "Nastaviť hlavnú"





dtlačok prstu DFB9 Also known as:	47B 4304 CB18 AF97 E49D EC51 77D3 E4E1 1CE2	
CSIRT.SK < info@csirt.	Zmeniť primárne ID užívateľ	'a ×
incident <incident@c Incident <incident@c< td=""><td>Zmeniť kľúč: incident &lt; incident@csirt.sk&gt; - 0xEC</td><td>5177D3E4E11CE2</td></incident@c<></incident@c 	Zmeniť kľúč: incident < incident@csirt.sk> - 0xEC	5177D3E4E11CE2
ákladné Certification	Dostupné   Eringinian Fridat i Diazvarcia incident < Meno CSIRT.SK - F-mail	
Koniec platnosti	incident < OK Zruš	śiť Change
Validity	Pridať Nastaviť hlavnú Zneplatniť	Certify
You rely on certificati		Zatvoriť okno

Import a export kľúčov

- 1) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Správa kľúčov"
- Pre import kľúča Kliknite na "Súbor" -> "Importovať kľúče zo súboru" a vyberte súbor s kľúčom, ktorý chcete pridať do databázy (štandardne sa stretnete s príponami .asc a .gpg)

0			Sp	práva kľúčov Enigmail 🛛 🚽 🗖	
<u>S</u> úbor	<u>Upraviť Z</u> obraziť mportovať kľúče zo s	<u>K</u> eyserver súboru	<u>V</u> ytvoriť	☑ Štandardne zobraz všetky kľúče	
1	Exportovať kľúče do s Poslať verejné kľúče ( Vytvoriť email na ozn	súboru e-mailom ačené kľúče		<ul> <li>ID kľúča</li> </ul>	CQ ^
	Create <u>A</u> utocrypt Seti Spravovať S <u>m</u> artCard Znova načítať vy <u>r</u> ovn	up Message  ávaciu pamä	iť kľúčov		
1	<u>Z</u> avrieť <u>K</u> oniec		Ctrl+W		
					*

3) Pre export kľúča najprv kliknite na kľúč, ktorý chcete exportovať. Následne kliknite na "Súbor" -> "Exportovať kľúče do súboru". Pozorne vyberte, či chcete exportovať len verejné kľúče, alebo aj súkromné. Dbajte na to, aby ste zdieľali len svoje verejné kľúče. Súkromné kľúče patria len vám. Nikdy ich s nikým nezdieľajte, ani ich neposielajte e-mailom, ani žiadnym iným nechráneným kanálom.





5	Správa kľúčov Enigi	mail	- • ×
úbor <u>U</u> praviť <u>Z</u> obraziť <u>K</u> ey <b>⊣ľadať</b> _∕∕	server Vytvorit'	raz všetky kľúče	
Meno	<ul> <li>ID kľúča</li> </ul>		E\$
			^
×			
	Potvro	denie Enigmail	×
> incident cincident@csirt.sk	0		
	Prajete si do uloženého súbol	ru s kľúčom OpenPGP zahrnúť i sú	ikromný kľúč?
Þ. a	Exportovať iba verejné kľúče	Exportovať <u>s</u> úkromné kľúče	Zrušiť
>			
Þ.			
			~
1.5			

Nastavenie dôveryhodnosti kľúčov a ich podpisovanie / overovanie

- 1) Otvorte v menu klienta Thunderbird okno "Enigmail" -> "Správa kľúčov"
- 2) Dvojklikom otvorte vlastnosti vybraného PGP kľúča (tu môžete okrem iného nájsť odtlačok prsta kľúča pre porovnanie s informáciou od jeho majiteľa)
- 3) Pre nastavenie dôveryhodnosti kliknite v záložke "Základné" na poslednú položku "Change" a vyberte mieru dôveryhodnosti (viď časť Dôveryhodnosť a overovanie PGP kľúčov)

Vlastnosti kľúča	×
Hlavné ID užívateľa incident «incident@csirt.sk> Typ pár kľúčov Odtlačok prstu DERO FATR 4304 CR18 AF97 F40D FC51 77D3 F4F1 1CF2	Enigmail - Nastaviť dôveryhodnosť vlastníka Dôveryhodnosť kľúča: incident <incident@csirt.sk> - 0xE</incident@csirt.sk>
Also known as:     CSIRT.SK <info@csirt.gov.sk>       Incident <incident@csirt.gov.sk>     ``       Incident <incident@csirt.sk>     ``       Zákładné Certifications Structure     ``       Vytvorený     ``       Koniec platnosti     ``       Validity     neznámy</incident@csirt.sk></incident@csirt.gov.sk></info@csirt.gov.sk>	Ako je kľúč dôveryhodný? Neviem Nedôverujem Dôverujem iba čiastočne © Plne dôverujem Change Change Change OK Certify
You rely on certifications plne dôveryhodný	Change
Vyberte akciu •	Zatvoriť

 Pre podpísanie, resp. overenie kľúča kliknite v záložke "Základné" na prostrednú položku – "Certify", vyberte kľúč, ktorým chcete podpisovať a mieru, do akej ste podpisovaný kľúč overili





Vlastnosti kľúča		×	
Hlavné ID užívateľa incident <incident@csirt.sk> Typ pár kľúčov</incident@csirt.sk>	1		Enigmail - podpísať kľúč
Odtlačok prstu DFB9 E47B 4304 CB18 AF97 E49D EC51 77D3 E4E1 1CE2 Also known as:		Kľúč k podpisu: Odtlačok prstu:	incident ≺incident@csirt.sk> - 0xEC5177D3E4E11CE2 DFB9 E47B 4304 CB18 AF97 E49D EC51 77D3 E4E1 1CE2
CSIRT.SK <info@csirt.gov.sk> ^ incident <incident@csirt.gov.sk> Incident <incident@csirt.sk> v</incident@csirt.sk></incident@csirt.gov.sk></info@csirt.gov.sk>		Also known as:	CSIRT.SK <info@csirt.gov.sk> incident <incident@csirt.gov.sk> Incident <incident@csirt.sk></incident@csirt.sk></incident@csirt.gov.sk></info@csirt.gov.sk>
Základné Certifications Structure		Kľúč k podpisovaniu:	incident <incident@csirt.sk> - 0xEC5177D3E4E11CE2</incident@csirt.sk>
Výtvorený Koniec platnosti	Change	– Ako dôkladne ste ovu	Note: you have to set owner trust to ultimate for your own keys to be shown here. Poznámka: niektoré uživateľské ID kľúča 0xEC5177034E11CE2 sú podpisané zvoleným tajným kľúčom. svíjíča ja kľúča knoj chrzeta podpisárají zná tíň oza usedensi podpis
Validity neznámy	Certify	Nebudem odpov     Vôbec sem nesko	edať otroloval/a
You rely on certifications plne dôveryhodný	Change	O Vykonal/a som o	rientačnú kontrolu
		○ Vykonal/a som d	ôkladnú kontrolu
Vyberte akciu *	Zatvoriť	🗌 Lokálny podpis (ni	e je možné exportovat) OK Zrušiť

## Používanie PGP kľúčov v klientovi Thunderbird

Modul Enigmail pridá do lišty nástrojov okna určeného na písanie správy ikony visiaceho zámku a ceruzky. Ak chcete e-mail zašifrovať, kliknite na zámok (zafarbí sa a namiesto červeného krížika sa pri ňom objaví zelená kvačka). Ak chcete správu podpísať, kliknite na ceruzku (správa sa podobne, ako zámok). Pri odosielaní správy si od vás Thunderbird vyžiada heslo k vášmu PGP kľúču.

## Nastavenie automatického podpisovania a šifrovania

- 1) Kliknite v hlavnom menu klienta Thunderbird na položku "Možnosti" -> "Nastavenie účtov"
- 2) Pre vybrané e-mailové konto kliknite na položku "OpenPGP Security"
- 3) Pre automatické podpisovanie vyberte podľa vašej preferencie z položiek "podpíš nezašifrované správy" a "podpíš zašifrované správy"
- 4) Je odporúčané nastaviť šifrovanie konceptov správ pri ich ukladaní na disk

	Nastavenie účtov
	Signing/Encryption Options
Nastavenie servera Kópie a priečinky Písanie a adresovanie Nevyžiadaná pošta Synchronizácia a úložný priestor OpenPGP Security Potvrdenia o prečítaní	Podporu podpisovania a šifrovania pomocou OpenPGP zaisťuje Enigmail. Potrebujete mať nainštalovaný GnuPG (gpg), aby bolo možné túto funkciu použiť. ✓ Povoliť podporu OpenPGP (Enigmail) pre túto identitu O Použiť «-mailovú adresu tejto identity k určeniu kľúča OpenPGP ④ Použiť určený ID kľúč OpenPGP (0x1234ABCD): [0xDFB9E47B4304CB18A] Vyberte kľúč
<ul> <li>Bezpecnost</li> <li>Bincident@csirt.sk</li> <li>Nastavenie servera</li> <li>Kópie a priečinky</li> <li>Písanie a adresovanie</li> <li>Nevyžiadaná pošta</li> <li>Surschercistica s (dielár á niedze)</li> </ul>	Message Composition Autocrypt Predvolené nastavenia vytvárania správy Vždy šifrovať správy Štandardne podpisovať správy Vždy použiť PGP/MIME
OpenPGP Security Potvrdenia o prečítaní Bezpečnosť	Po aplikácii štandardných nastavení a pravidiel: □ podpíš nezašifrované správy ☑ podpíš zašifrované správy ☑ Zašifruj koncepty správ pri ukladaní
Nastavenie servera Kópie a priečinky Písanie a adresovanie	If both, Enigmail and S/MIME encryption are possible, then: O Prefer S/MIME  Prefer Enigmail (OpenPGP)
Nevyžiadaná pošta Synchronizácia a úložný priestor OpenPGP Security Potvrdenia o prečítaní v Akcje s účtami •	Rozšírené Enigmail nastavenia
	OK Zrušiť





5) Vyberte, ktorý štandard má Enigmail použiť, ak je dostupný S/MIME, aj OpenPGP. Štandardne vyberieme OpenPGP. Diskusiu o rozdieloch týchto štandardov môžete nájsť tu.

#### Výmena PGP kľúča

- 1) Kliknite v hlavnom menu klienta Thunderbird na položku "Možnosti" -> "Nastavenie účtov"
- 2) Pre vybrané e-mailové konto kliknite na položku "OpenPGP Security"
- 3) Kliknite na položku "Vyberte kľúč"
- 4) Zvoľte PGP kľúč, ktorý chcete pre tento e-mail používať. Takto môžete napríklad vymeniť expirovaný kľúč za nový.

		Nastavenie účtov			×	
Nastavenie servera Kópie a priečinky Písanie a adresovanie Nevyžiadaná pošta Synchronizácia a úložný priestor OpenPGP Security Potvrdenia o prečítaní Bezpečnosť	Signing/ Podporu po GnuPG (gpg Povoliť ) Použiť O Použiť OxDFB9E4 Message C	/Encryption Options odpisovania a šifrovania pomocou OpenPGP zr g), aby bolo možné túto funkciu použiť. podporu OpenPGP (Enigmail) pre túto identitu 'e-mailovú adresu tejen GPC (0x1234ABCD): 'rDtává (D kľúč OpenGPC (0x1234ABCD): '784304CB18A Vyberte kľúč 'omonsition Autosvet	aisťuje Enigmail. Potrebuje a a OpenPGP	te mat' nainšta	lovaný	
Nastavenie servera Kópie a priečinky Písanie a adresovanie Nevyžiadaná pošta Synchronizácia a úložný priestor OpenPGP Security Potvrdenia o prečítaní Bezpečnosť Nastavenie servera Kópie a priečinky Písanie a adresovanie Nevyžiadaná pošta Synchronizácia a úložný priestor OpenPGP Security Potvrdenia o prečítaní	Predv Vž. Šta Vž. Po apl po Za If both Pre	Vyberte su Určiť kľúč OpenPGP pre šifrovanie Hľadať Ďincident <incident@csirt.sk></incident@csirt.sk>	Platnosť	Vytvorený Selectrové	ID kľúča 0xEC5177D3E4E11	CE2
		<u>Q</u> bnoviť zoznam kľúčov			Vybe	erte kľúč Zrušiť





## Návod pre generovanie kľúčov pomocou GnuPG cez konzolu (odporúčaná konfigurácia)

# Obmedzenie používania slabého hašovacieho algoritmu SHA1:

Prednastavené algoritmy použité novo vygenerovanými kľúčmi je možné definovať v ~/.gnupg/gpg.conf (ak neexistuje, vytvoríme ho):

personal-digest-preferences SHA512,SHA384,SHA256,SHA224

Pre bezpečné podpisovanie explicitne nastavíme bezpečný algoritmus v ~/.gnupg/gpg.conf: Cert-digest-algo SHA256 (prípadne "digest-algo SHA256")

Bližšie informácie nájdete napríklad <u>tu</u>.

# Vytvorenie primárneho (master) kľúča:

Počas generovania primárneho kľúčového páru bude treba špecifikovať heslo k privátnemu kľúču – toto heslo bude používané len pri vytváraní alebo modifikácii podkľúčov – odporúčame použiť silné, no dobre zapamätateľné heslo (**passphrase**).

\$ gpg --expert --full-gen-key (alebo gpg -expert -gen-key, pre GnuPG verzie 1) gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want: (1) RSA and RSA (default)

(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(7) DSA (set your own capabilities)
(8) RSA (set your own capabilities)
(9) ECC and ECC
(10) ECC (sign only)
(11) ECC (set your own capabilities)

Your selection? 8

Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Sign Certify Encrypt

(S) Toggle the sign capability

(E) Toggle the encrypt capability

(A) Toggle the authenticate capability

(Q) Finished

Your selection? **S** 

Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Certify Encrypt





(S) Toggle the sign capability(E) Toggle the encrypt capability

(A) Toggle the authenticate capability

(Q) Finished

Your selection? **E** 

Possible actions for a RSA key: Sign Certify Encrypt Authenticate Current allowed actions: Certify

(S) Toggle the sign capability

- (E) Toggle the encrypt capability
- (A) Toggle the authenticate capability
- (Q) Finished

Your selection? **Q** RSA keys may be between 1024 and 4096 bits long. What keysize do you want? (2048) **4096** Requested keysize is 4096 bits Please specify how long the key should be valid. 0 = key does not expire <n> = key expires in n days <n>w = key expires in n weeks <n>m = key expires in n weeks <n>y = key expires in n years Key is valid for? (0) **2y** Key expires at Fri 02 Apr 2021 03:51:47 PM CEST Is this correct? (y/N) **y** 

GnuPG needs to construct a user ID to identify your key.

Real name: Janko Mrkvicka Email address: janko.mkrvicka@csirt.sk Comment: You selected this USER-ID: "Janko Mrkvicka <janko.mkrvicka@csirt.sk>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? **O** We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number generator a better chance to gain enough entropy. gpg: key 0xA9B3110ED21FA171 marked as ultimately trusted





gpg:	revocation	certificate	stored	as	'/home/janko/.gnupg/openpgp-
revocs.d	I/D44CA7BBB71DA	3735157D764A9	B3110ED21F	A171.rev'	
public a	nd secret key creat	ed and signed.			
gpg: che	cking the trustdb				
gpg: ma	rginals needed: 3	completes neede	ed: 1 trust mo	odel: PGP	
gpg: der	oth: 0 valid: 5 sig	ned: 0 trust: 0-	. 0a. 0n. 0m. (	)f. 5u	

gpg: next trustdb check due at 2021-03-04

pub rsa4096/0xA9B3110ED21FA171 2019-04-03 [] [expires: 2021-04-02]

Key fingerprint = D44C A7BB B71D A373 5157 D764 A9B3 110E D21F A171

uid [ultimate] Janko Mrkvicka <janko.mkrvicka@csirt.sk>

# Konfigurácia primárneho (master) kľúča - nastavenie použitia iba silných algoritmov:

\$ gpg --expert --edit-key 0xA9B3110ED21FA171 gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec rsa4096/0xA9B3110ED21FA171
 created: 2019-04-03 expires: 2021-04-02 usage: C
 trust: ultimate validity: ultimate
[ultimate] (1). Janko Mrkvicka <janko.mkrvicka@csirt.sk>

## gpg> setpref SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP Uncompressed

Set preference list to:

Cipher: AES256, AES192, AES, CAST5, 3DES Digest: SHA512, SHA384, SHA256, SHA224, SHA1 Compression: ZLIB, BZIP2, ZIP, Uncompressed Features: MDC, Keyserver no-modify Really update the preferences? (y/N) y

sec rsa4096/0xA9B3110ED21FA171

created: 2019-04-03 expires: 2021-04-02 usage: C

trust: ultimate validity: ultimate

[ultimate] (1). Janko Mrkvicka <janko.mkrvicka@csirt.sk>

#### gpg> **save**

Vygenerovaný kľúčový pár je vhodné / potrebné zazálohovať na offline médium. Takisto jeho heslo.





#### <u># Pridanie identity ku kľúču:</u>

#### \$ gpg --expert --edit-key 0xA9B3110ED21FA171

gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec rsa4096/0xA9B3110ED21FA171
created: 2019-04-03 expires: 2021-04-02 usage: C
trust: ultimate validity: ultimate
ssb rsa4096/0x67A1C966778BAE55
created: 2019-04-03 expires: 2021-04-02 usage: S
ssb rsa4096/0xFCBFA27BBBF1180C
created: 2019-04-03 expires: 2021-04-02 usage: E
[ultimate] (1). Janko Mrkvicka <janko.mkrvicka@csirt.sk>

gpg> **adduid** Real name: **Janko Mrkvicka** Email address: **janicko@csirt.sk** Comment: You selected this USER-ID: "Janko Mrkvicka <janicko@csirt.sk>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

sec rsa4096/0xA9B3110ED21FA171 created: 2019-04-03 expires: 2021-04-02 usage: C trust: ultimate validity: ultimate ssb rsa4096/0x67A1C966778BAE55 created: 2019-04-03 expires: 2021-04-02 usage: S ssb rsa4096/0xFCBFA27BBBF1180C created: 2019-04-03 expires: 2021-04-02 usage: E [ultimate] (1) Janko Mrkvicka <janko.mkrvicka@csirt.sk>

#### gpg> **save**

Ak máme záujem špecifikovať, ktorá identita je primárna, je to možné pomocou:

\$ gpg --expert --edit-key 0xA9B3110ED21FA171 gpg> uid 2 #t.j. poradové číslo identity gpg> primary





#### gpg> **save**

# \$ gpg --list-secret-keys /home/mrkvicka/.gnupg/pubring.gpg

-----

# sec rsa4096/0xA9B3110ED21FA171 2019-04-03 [C] [expires: 2021-04-02] Key fingerprint = D44C A7BB B71D A373 5157 D764 A9B3 110E D21F A171

uid [ultimate] Janko Mrkvicka <janko.mkrvicka@csirt.sk>

# Vytvorenie podpisového a šifrovacieho podkľúča:

Počas generovania podkľúča bude treba špecifikovať heslo k privátnemu kľúču. Toto heslo sa bude používať pri práci s e-mailmi. Odporúčame vygenerovať silné a zároveň jednoducho napísateľné heslo (**passphrase**). Toto heslo by malo byť odlišné od hesla ku primárnemu kľúču.

Počas generovania budete vyzvaní taktiež na zadanie hesla k privátnemu primárnemu kľúču, ktorý musí byť odomknutý, aby bolo možné podpísať práve generovaný podkľúč.

## \$ gpg --expert --edit-key 0xA9B3110ED21FA171

gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec rsa4096/0xA9B3110ED21FA171
 created: 2019-04-03 expires: 2021-04-02 usage: C
 trust: ultimate validity: ultimate
[ultimate] (1). Janko Mrkvicka <janko.mkrvicka@csirt.sk>

## gpg> **addkey**

Please select what kind of key you want: (3) DSA (sign only) (4) RSA (sign only) (5) Elgamal (encrypt only) (6) RSA (encrypt only) (7) DSA (set your own capabilities) (8) RSA (set your own capabilities) (10) ECC (sign only) (11) ECC (set your own capabilities) (12) ECC (encrypt only) (13) Existing key Your selection? **4** RSA keys may be between 1024 and 4096 bits long. What keysize do you want? (2048) **4096** Requested keysize is 4096 bits





sec rsa4096/0xA9B3110ED21FA171
created: 2019-04-03 expires: 2021-04-02 usage: C
trust: ultimate validity: ultimate
ssb rsa4096/0x67A1C966778BAE55
created: 2019-04-03 expires: 2021-04-02 usage: S
[ultimate] (1). Janko Mrkvicka <janko.mkrvicka@csirt.sk>

#### gpg> **save**

Obdobným spôsobom sa generuje šifrovací podkľúč - možnosť (6) RSA (encrypt only).

# Finálna podoba vygenerovaných kľúčov:

\$ gpg --list-secret-keys 0xA9B3110ED21FA171

\_\_\_\_\_

sec rsa4096/0xA9B3110ED21FA171 2019-04-03 [C] [expires: 2021-04-02] Key fingerprint = D44C A7BB B71D A373 5157 D764 A9B3 110E D21F A171 uid [ultimate] Janko Mrkvicka <janko.mkrvicka@csirt.sk> uid [ultimate] Janko Mrkvicka <janicko@csirt.sk> ssb rsa4096/0x67A1C966778BAE55 2019-04-03 [S] [expires: 2021-04-02] Key fingerprint = 8F7D 0B0D 7186 1597 E477 EC8D 67A1 C966 778B AE55 ssb rsa4096/0xFCBFA27BBBF1180C 2019-04-03 [E] [expires: 2021-04-02] Key fingerprint = 4C92 815E B824 B057 DC91 4076 FCBF A27B BBF1 180C

<u># Export primárnych kľúčov aj všetkých podkľúčov:</u>
 Pre export všetkých kľúčov:
 \$ gpg --export-secret-keys --armor --output
 /media/janko/BACKUP/janko.mrkvicka\_allkeys\_secret.gpg 0xA9B3110ED21FA171

Pre export verejných kľúčov:





## \$ gpg --export --armor --output /media/janko/BACKUP/janko.mrkvicka\_allkeys\_public.gpg 0xA9B3110ED21FA171

<u># Export podkľúčov:</u>

## \$ gpg --export-secret-subkeys --armor --output ./janko.mrkvicka\_subkeys\_secret.gpg 0xA9B3110ED21FA171

Po zazálohovaní kľúčov (najmä primárneho kľúčového páru), tento potrebujeme vymazať z pracovného počítača.

\$ gpg --delete-secret-keys 0xA9B3110ED21FA171 gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

sec rsa4096/0xA9B3110ED21FA171 2019-04-03 Janko Mrkvicka <janko.mkrvicka@csirt.sk>

Delete this key from the keyring? (y/N) **y** This is a secret key! - really delete? (y/N) **y** 

Nasleduje dialóg potvrdzujúci vymazávanie kľúča aj všetkých podkľúčov. Ak si chceme ponechať podkľúče, stačí nepotvrdiť ich vymazanie.





## Vytváranie PGP kľúčov v open-source softvéri Kleopatra

1) V programe Kleopatra otvorte v menu položku "File" -> "New Key Pair..."

💼 к	leopatra		
<u>F</u> ile	<u>View</u> <u>C</u> ertificates	<u>T</u> ools <u>S</u> ettings	<u>W</u> indow <u>H</u> elp
<u>ه</u> ب	<u>N</u> ew Key Pair	Ctrl+N	e, e Q
Q	Lookup on Server	Ctrl+Shift+I	port Certify Lookup on Server Notepad
<u>₽₹</u>	Import	Ctrl+I	
	Export Export Secret Keys Print Secret Key	Ctrl+E	Welcome to Meanstra 2.1.4-maduin-2.1.5
ini Ka	Publish on Server Decrypt/Verify Sign/Encrypt Sign/Encrypt Folder	Ctrl+Shift+E	Vieconine to Keopatra 5.1.+ gpg+win-5.1.5  Kleopatra is a front-end for the crypto software <u>GnuPG</u> .  For most actions you need either a public key (certificate) or your own private key.  • The private key is needed to decrypt or sign.
	C <u>r</u> eate Checksum Files <u>V</u> erify Checksum Files		The public key can be used by others to verify your identity or encrypt to you. You can learn more about this on <u>Wikipedia</u> .
	<u>C</u> lose	Ctrl+W	
	Quit	Ctrl+Q	New Key Pair

2) Vyberte formát "OpenPGP key pair"

🖪 Kleopatra		
<u>File View Certificates Tools Setting</u>	s <u>W</u> indow <u>H</u> elp	
File Yiew Certificates Iools Setting		
	<ul> <li>OpenPGP key pairs are certified by continning the Imgerpant of the public key.</li> <li>Create <u>a</u> personal X.509 key pair and certification request X.509 key pairs are certified by a certification authority (CA). The generated request needs to be sent to a CA to finalize creation.</li> </ul>	
	Next Cancel	

3) Zadajte svoje meno a e-mail, ktorému chcete kľúče priradiť. Otvorte položku "Advanced Settings…". Zvoľte si typ a veľkosť kľúča. Použitie eliptickej krivky by malo poskytnúť vyššiu rýchlosť a väčšiu bezpečnosť, no pokulhávať môže kompatibilita s príjemcami vašich správ. RSA je však v dnešnej dobe z praktického hľadiska pokladané za dostatočne bezpečné, pričom vylúčime riziko nekompatibility. V tomto prípade volíme veľkosť kľúča 3072, alebo 4096 bitov. Zvoľte použitie – podpisovanie, či šifrovanie. Nastavte platnosť kľúčov maximálne na 2 roky.





R Kleopatra File View Certificates Tools	Settings Window Help	
Elle View Certificates Tools       Advanced Settings - Kleopatra       Technical Details       Key Material       RSA       4096 bits       I + RSA       4096 bits       (default) ~       I + Elgamal       248 bits       4095 bits       I - Cottificate       U - Certificate       I - Roryption       Authentication       Valid untiti       2/1/2021	Settings Window Hep	2 E2 , dick on (optional) (optional)

4) Skontrolujte údaje a vytvorte si heslo

		0 /	8 2
G	Key Pair Creatio	on Wizard	
	Review Para	meters	
	Please review the	parameters before proceeding.	
	Name: Email Address: Key Type: Key Strength: Usage: Subkey Type: Subkey Type: Subkey Strength Subkey Usage: Valid Until:	Fero Tarba fero.taraba@email.sk RSA 4096 bits Encrypt, Sign RSA a: 4096 bits Encrypt Monday, February 01, 2021	
	✓ Show all detai	s	
			<u>C</u> reate <u>Cancel</u>





ify	 Import			0		•		X §
		6 ка	ey Pair Creation Wiza	ard				
	pinentr	y-qt Please enter protect your Passphrase: Repeat: Quality:	the passphrase to new key heslo@vesl0#nie heslo@vesl0#nie 100% QK Car	¶∕* mcel	es large am	ounts of rand	lom numbers. This	: may require
							Next	<u>C</u> ancel

5) Kľúčový pár je vhodné zálohovať na bezpečné miesto, ideálne offline úložisko

💼 Kleopatra				
<u>F</u> ile <u>V</u> iew <u>C</u> ertificates <u>T</u> ools <u>S</u> ett	ings <u>W</u> indow <u>H</u> elp			
Sign/Encrypt Decrypt/Verify Impor	Key Pair Creation Wizard			
Search <alt+q></alt+q>	Key Pair Successfully Created		All Certificates	
Name	Rey Fun Successiony created	d From	Valid Until	Details
Fero Tarba	Your new key pair was created successfully. Please find details on the result and some suggested next steps below. Result Key pair created successfully. Fingerprint: 16DBB8AEEEFE01F1984EEB1233584643A6FE401F	19	2/1/2021	OpenPGP
	Make a Backup Of Your Key Par           Send Public Key By EMail           Upload Public Key To Directory Service			
4	Enish			Þ





## Čo s PGP kľúčom po expirácii?

Kľúče po expirácii ich platnosti je potrebné revokovať a opätovne nahrať na keyserver (resp. ak bol nahrávaný), aby reflektoval túto situáciu. Kľúče, ktoré sú dnes pokladané za prakticky neprelomiteľné, môžu byť prelomené v budúcnosti vďaka rastúcemu výpočtovému výkonu a novým algoritmom. Expirovaný no nerevokovaný kľúč tak môže byť zneužitý útočníkmi, ktorí si navyše vedia jednoducho spätne nastaviť podpisovú hierarchiu, a tak pridať kľúču zdanie legitímnosti.

Šifrovací podkľúč je vhodné odložiť aj po jeho expirácii a revokácii, nakoľko ho môžeme použiť na čítanie starej pošty. Tak isto revokovaným podpisovým kľúčom vieme overiť svoje podpisy na starých správach, no nemôžeme ním podpisovať nové.