E-mail-önvédelem: kézikönyv a megfigyelés elleni harchoz GnuPG titkosítással

PCLinuxOS Magazine – 2021. augusztus

A **Free Software Foundation**-tól utánnyomás
A képek a Creative Commons Attribution 4.0 licenc alapján felhasználva
A szöveg felhasználása a Creative Commons Attribution-ShareAlike 4.0 licenc alapján

A tömeges megfigyelés sérti az alapvető jogainkat és kockázatossá teszi a szabad beszédet. A leírás alapszintű önvédelmi képességre oktat: az e-mail titkosításra. A végére érve képes leszel titkosított e-maileket küldeni és fogadni, biztosítva, hogy az e-mailjeidet lehallgató ügynök, vagy megszerző tolvaj ne tudja elolvasni. Mindössze egy internetre kapcsolt számítógépre, egy e-mailfiókra és körülbelül negyven percre van szükség.

Még ha nincs is rejtegetni valód, a titkosítás segít megvédeni a veled kommunikálók személyes terét és megnehezíti a tömeges megfigyelő rendszerek életét. Ha van valami fontos elrejteni valód, jó helyen jársz; ezek ugyanazok az eszközök, amiket a kiszivárogtatók használnak a személyiségük védelmére, miközben feltárják az emberi jogok megsértését, a korrupciót és más bűnügyeket.

A titkosítás használata mellett, szükség van a rólunk gyűjtött adatok mennyiségének csökkentése melletti politikai harcra is, de alapvető első lépés önmagunk védelme és a kommunikáción megfigyelésének lehető legnehezebbé tétele. Ez a leírás segít ebben. Kezdők számára készült, de ha már ismered a GnuPG alapjait, vagy gyakorlott szabad szoftver felhasználó vagy, akkor tetszeni fognak a haladó tippek és a barátaid oktatására a leírás.

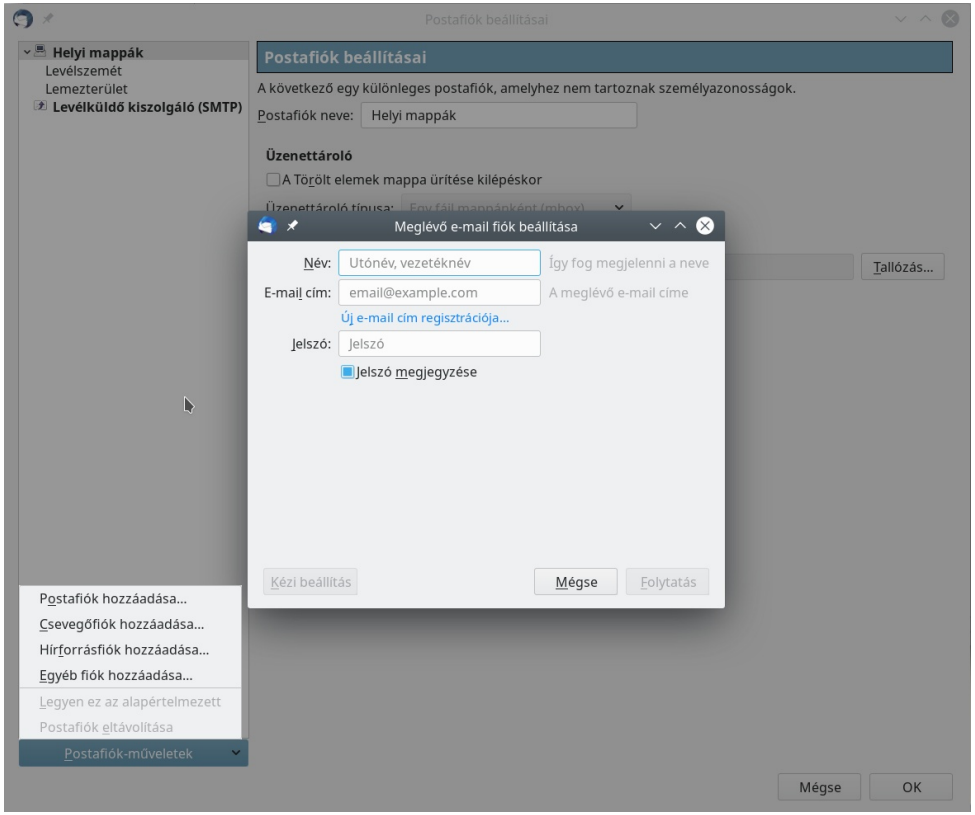
1. szakasz: szedd össze a darabokat

A leírás szabad licencű szoftverekre támaszkodik, amik teljesen átláthatóak és bárki lemásolhatja vagy saját változatot készíthet belőle. Ez sokkal jobban véd a megfigyeléstől, mint a jogvédett szoftverek (Windows, MacOS). Továbbiakat az fsf.org-on olvashatsz.

A legtöbb GNU/Linux operációs rendszeren ott van a GnuPG, így ezeknél nem kell telepíteni. MacOS-t és Windows-t futtatók a GnuPG letöltése lépéseit később olvashatják. A titkosítási rendszered beállítása előtt legyen a gépen telepített levelező program. Sok GNU/Linux disztribúción már ott van az Icedove, ami esetleg „Thunderbird” néven található. Az ilyen programokkal a webböngészős eléréstől (mint Gmail) eltérő módon férhetsz hozzá ugyanahhoz az e-mail fiókhoz, de további lehetőségeket is kínálnak.

Ha már van e-mail programod, akkor átugorhatsz a 2. lépéshez.

1.a lépés: levelező program beállítása az e-mail-fiókhoz



Nyisd meg a leveleződet és kövesd a varázslót (lépésről, lépésre vezet), ami beállítja magát az e-mail-fiókodhoz. Általában „Postafiók beállításai → Postafiók hozzáadása”. A levelező szerver beállításait a rendszergazdától vagy a postafiók segítségnyújtási részénél kapod meg.

Hibaelhárítás

A varázsló nem indul el. A varázsló kézzel is indítható, de az ehhez tartozó menüopciót elnevezése levelezőtől függően más lehet. Az indítógomb a program főmenüjében, az „Új” vagy hasonló néven, mint „Postafiók hozzáadása” vagy „Új/Létező postafiók” található.

A varázsló nem találja a postafiókot vagy nem tölti le a leveleket. Mielőtt feltúrnád a netet, előbb kérdezd meg olyanoktól a helyes beállításokat, akik szintén az általad használt e-mail-rendszert használják.

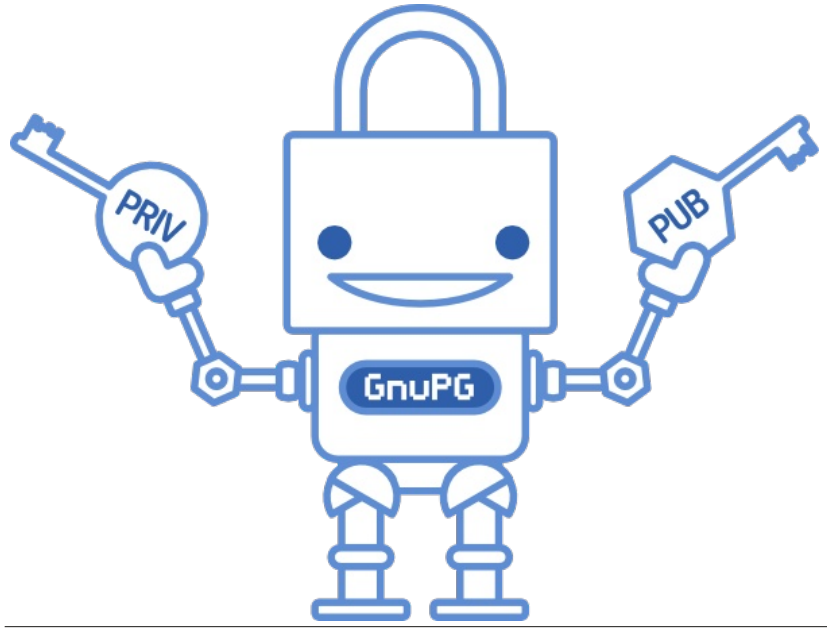
Nem találom a menüt. Sok levelezőben a főmenüt egy ikon rejti, amiben egymás fölött elhelyezkedő három vízszintes vonal látható.

1.b lépés: készítsd elő a terminált és telepítsd a gnupg-t

Ha GNU/Linux-os gépet használsz, akkor a GnuPG már a gépeden kell legyen és a 2. lépésre ugorhatsz.

GnuPG, OpenPG, ez micsoda?

A GnuPG, GPG, GNU Privacy Guard, OpenPG és a PGP kifejezéseket általában felváltva használják. Technikai értelemben a titkosítási szabvány az OpnePGP (Pretty Good Privacy) és a szabványt érvényesítő program pedig a GNU Privacy Guard (röviden GPG vagy GnuPG). A legtöbb levelező rendelkezik GnuPG felülettel. A GnuPG újabb változata a GnuPG2.



2. szakasz: készítsd el a kulcsodat

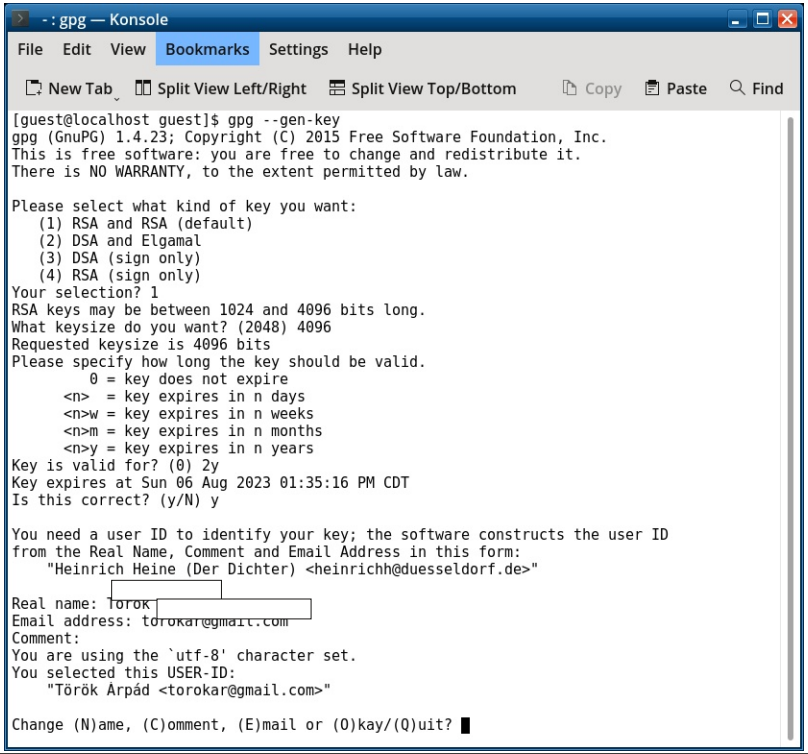
A GnuPG-rendszer használatához kell egy nyilvános (public) és egy privát kulcspár. Mindkettő hosszú, véletlenszerűen generált, számokból és betűkből álló, egyedi karaktersor. A nyilvános és privát kulcsodat egy speciális matematikai függvény köti össze.

A publikus kulcsod nem olyan, mint egy igazi kulcs, mivel egy keyserver-nek hívott nyílt, online könyvtárban van. Az emberek letöltik és GnuPG-vel használva titkosítják a neked szóló üzenetet. A keyserver-t tekintsd telefonkönyvnek; aki neked akar e-mailt küldeni, megkeresheti a nyilvános kulcsodat.

A privát kulcsod sokkal inkább olyan, mint egy tényleges kulcs, mivel magadnál tartod (a gépeden). A GnuPG-t és a privát kulcsot együtt használva bontod ki a neked küldött titkosított üzeneteket. **Soha, semmilyen körülmények között se oszd meg senkivel a privát kulcsodat.**

A kódolás és dekódolás mellett a kulcsokat használhatod az üzenetek aláírására és mások aláírásának hitelessége ellenőrzésére. A következő szakaszban ezt részletesebben áttekintjük.

2.a lépés: készíts egy kulcspárt



Nyiss terminált Ctrl + Alt + t (GNU/linux alatt) vagy keresd meg az alkalmazások között és a következő kóddal hozd létre a kulcspárodat:

Terminál parancssorát használjuk a kulcspár létrehozására GnuPG programmal. A terminál a GNU/Linux operációs rendszerben telepítve kell legyen, macOS és Windows OS használata esetén a „Terminal" (macOS) vagy a „PowerShell" (Windows) programot használd, amiket az 1. szakaszban is használtunk.

 # gpg --gen-key a folyamat elindítása

A kérdésre, hogy milyen kulcsot akarsz csinálni, válaszd az alapopciót az „**(1) RSA and RSA**"-t.

A kulcs mérete (keysize) legyen: **4096** az erős kulcshoz.

Lejáratra 2 évet javaslunk: **2y** (2 years).

A promptot követve állítsd be a személyes adataidat.

Állítsd be a jelszavadat

A „Passphrase" nevű ablakban írj be egy erős jelszót! Kézzel is megteheted vagy választhatod a Diceware (kockadobás) módszert. A kézi bevitel gyorsabb, de nem annyira biztonságos. A Diceware használata lassabb és dobókocka is kell, de támadók számára sokkal nehezebben kitalálható jelszót eredményez. Használatához Micah Lee írásában olvasd el a „Biztonságos jelszó készítése Diceware-rel" részt.
Ha úgy döntesz, magad készíted a jelszót, akkor valami megjegyezhető, de legalább 12 karakter hosszúságú valamit találj ki, ami legalább egy kis- és egy nagybetűt, illetve legalább egy számot vagy írásjelet tartalmaz. Sose használj olyan jelszót, amit máshol már alkalmaztál. Ne használj semmilyen azonosítható sablont, mint születésnap, telefonszám, kis kedvenc neve, dalszöveg, könyvidézet és a többi.

Hibaelhárítás

GnuPG nincs telepítve. GPG nincs telepítve. Ellenőrizheted, hogy ez van-e a **gpg --version** paranccsal. Ha GnuPG nincs telepítve, ez a legtöbb GNU/Linux rendszerben ilyen, vagy hasonló eredményt ad: **Command 'gpg' not found, but can be installed with** (parancs nem található, de telepíthető a következő paranccsal) **su- apt-get install gnupg**. Az utasítás szerint telepítsd a programot.

Túl sokáig tartott a jelszavam létrehozása. Így van rendjén. Fontos a jelszavadról gondoskodni. Amikor készen állsz, csak kövesd a lépéseket az elejétől kezdve, hogy létrehozd a kulcsodat.

Hogy nézhetem meg a kulcsomat? A következő parancsot add ki, hogy lásd a kulcsokat: **gpg --list-keys**. Ott kell lennie a tieidnek, miként Edwardénak is (3. szakasz). Ha csak a saját kulcsodra vagy kíváncsi a **gpg --list [e-mail címed]**-t írd be. Szintén használható a **gpg --list-secret-key** a privát kulcsod megtekintésére.

További források. A folyamattal kapcsolatos további információkért a The GNU Privacy Handbook-hoz is fordulhatsz. Mindenképp az „RSA and RSA"-nál (alapbeállítás) maradj, mivel az újabb és sokkal biztonságosabb, mint az amit a kézikönyv javasol. Arra is ügyelj, hogy a kulcsod legalább 4096 bit legyen, ha biztonságban akarsz lenni.

Haladó

Haladó kulcspárok. Amikor a GnuPG új kulcspárt készít, leválasztja a titkosítási funkciót az aláírási funkciótól al-kulcsok segítségével. Az al-kulcsok körültekintő használatával a GnuPG-s személyazonosságod sokkal nagyobb biztonságban tartható és a kulcs megrongálódása esetén gyorsabban helyreállítható. Alex Cabal és a Debian wikije jól leírja biztonságos al-kulcsos rendszer felállításának módját.

2.b lépés: a létrehozás utáni néhány fontos lépés

```
fsfesd@esd:~$ gpg --gen-revoke F0F7F0C06A2A3242674584876E4BEA8C4862BA58 > revoke.asc

sec  rsa4096/6E4BEA8C4862BA58 2021-07-13 FSF ESD <esd@fsf.org>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
>
Reason for revocation: Key has been compromised
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!


fsfesd@esd:~$ gpg --send-key F0F7F0C06A2A3242674584876E4BEA8C4862BA58
gpg: sending key 6E4BEA8C4862BA58 to hkps://hkps.pool.sks-keyservers.net
```

Feltöltjük a kulcsodat egy keyserver-re, így akik titkosított üzenetet akarnak neked küldeni, letölthetik a nyilvános kulcsodat az Internetről. A feltöltéshez a menüben sok keyserver közül választhatsz, de ezek egymás másolatai, így lényegtelen, melyiket használod. Ugyanakkor, új kulcs feltöltése után, beletelhet pár órába, mire szinkronizálnak.

Másold ki a keyID-dat (kulcsazonosító): a **gnupg --list-key [e-mail címed]** kiírja a publikus („pub”) kulcsod információit, közte a keyID-t, ami egyedi szám- és betűsor. Másold ki a keyID-t, hogy a következő parancsban használhasd.

Töltsd fel a kulcsot egy szerverre: **gpg --send-key [keyID]**

Exportáld a kulcsodat egy fájlba

A következő parancsot kiadva exportáld a titkos kulcsodat, hogy következő lépés során importálhasd azt a leveleződbe. Elkerülendő a kulcsod kompromittálódását, biztos helyen tárold és gondoskodj arról, hogy átvitel esetén az megbízható módon történjen. A kulcsok exportálása a következő paranccsal történhet:

$ gpg --export-secret-keys -a [keyid] > my_secret_key.asc

$ gpg --export -a [keyid] > my_public_key.asc

Visszavonási tanúsítvány létrehozása

Arra az esetre, ha elvesztenéd a kulcsodat, vagy napvilágra kerülne, készíts egy tanúsítványt és a számítógépeden egy biztonságos helyre mentsd (a 6.c lépést nézd meg a visszavonási tanúsítvány biztonságos tárolásáról). Ez a lépés alapvetően fontos az e-mailes önvédelmed szempontjából, ahogy azt az 5. szakasz részletesebben is kifejti.

Másold ki a keyID-dat : a **gnupg --list-key [e-mail címed]** kiírja a publikus („pub”) kulcsod információit, közte a keyID-t, ami egyedi szám- és betűsor. Másold ki a keyID-t, hogy a következő parancsban használhasd.

generálj visszavonási tanúsítványt: **gpg --gen-revoke --output revoke.asc [keyID]**

A prompt a különböző visszahívási okokat ajánl fel választáshoz. Javasoljuk az **1 „key has been compromised”** (kulcsot kompromittálódott) használatát.

Nem kell, de be lehet írni okot, majd Enter-t nyomva vigyél be egy üres sort és hagyd jóvá a választásodat.

Hibaelhárítás

Úgy tűnik, hogy a kulcsom nem működik, vagy „Permission denied”-ot kapok. Mint minden fájl vagy könyvtár, a pgp kulcsok engedélyfüggőek. Ha a hozzáférés nincs jól beállítva, a rendszered nem fogadja el a kulcsot. A következő lépéseket követve ellenőriz és frissítsd a jogosultságokat.

Hozzáférés ellenőrzése: **ls -l ~/.gnupg/***

Állíts be olvasási, írási, futtatási engedélyt csak magadnak, senki másnak: ez a javasolt jogosultság a könyvtáradra. A következő kódot használhatod: **chmod 700 ~/.gnupg**.

Állíts be olvasási, írási engedélyt csak magadnak, senki másnak: ez a javasolt jogosultság a könyvtáradban a kulcsokra. A következő kódot használhatod: **chmod 600 ~/.gnupg/***.

Ha (valamilyen okból) a ~/.gnupg-n belül készítettél saját könyvtárat, akkor arra a könyvtárra futtatási engedélyt is kell adnod. A könyvtárak megnyitásához futtatási engedély kell. A hozzáféréssel kapcsolatos további információkért ezt a részletes tájékoztató kézikönyvet tanulmányozd.

Haladó

Továbbiak a keyserver-ekről. Ebben a kézikönyvben további információkat olvashatsz a keyserver-ekről. Az sks weblap tartalmaz egy listát a magas szinten együttműködő keyserver-ekről. A kulcsodat a számítógépedre közvetlenül is exportálhatod.

A kulcsaid átvitele: A következő parancsokat használd a kulcsaid átvitelére. Ahhoz, hogy a kulcsaid nyilvánosságra kerülését elkerüld, biztos helyen tárold és gondoskodj arról, hogy átvitel esetén, az megbízható módon történjék. Kulcs importálása és exportálása a következő parancsokkal lehetséges:

```
$ gpg --export-secret-keys -a keyid > az_en_privat_kulcsom.asc
$ gpg --export -a keyid > my_public_key.asc
$ gpg --import my_private_key.asc
$ gpg --import my_public_key.asc
```

Győződj meg arról, hogy a keyID megfelelő, ha igen, akkor lépj tovább és adj **ultimate** trust (legmagasabb szintű megbízhatóság) neki:

```
$ gpg --edit-key [your@email]
```

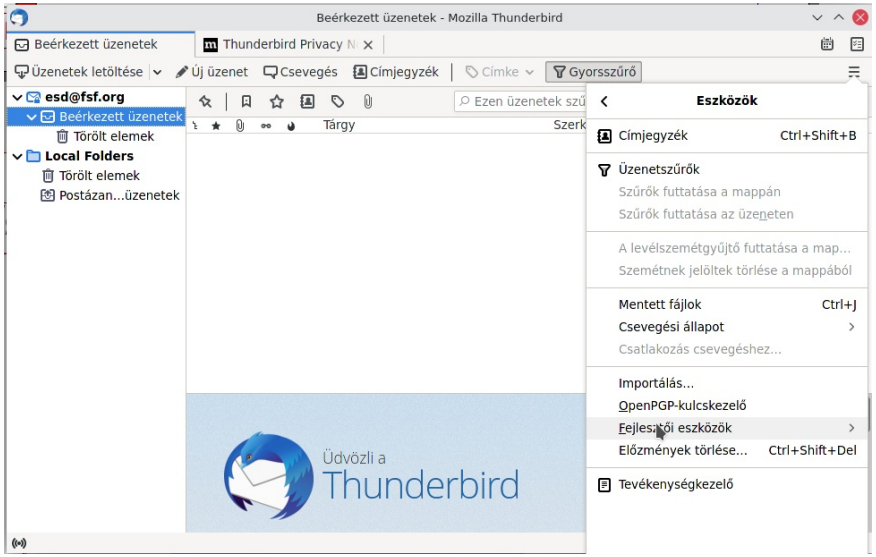
Mivel ez a te kulcsod, az **ultimate**-t válaszd. Senki más kulcsa ne kapjon ultimate trust-ot.

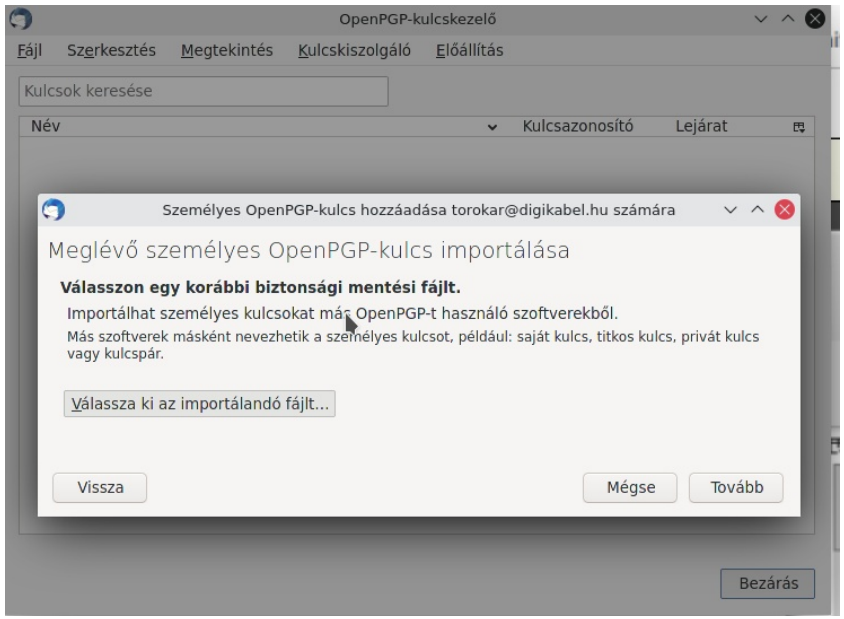
A 2.b hibaelhárítási szakaszban továbbiakat olvashatsz az engedélyekről. Átvitel során a kulcsaid engedélyei esetleg megkeveredhetnek, ami hibát eredményezhet. Könnyen elkerülhető, ha a könyvtárak és a fájlok jogosultsága megfelelő.

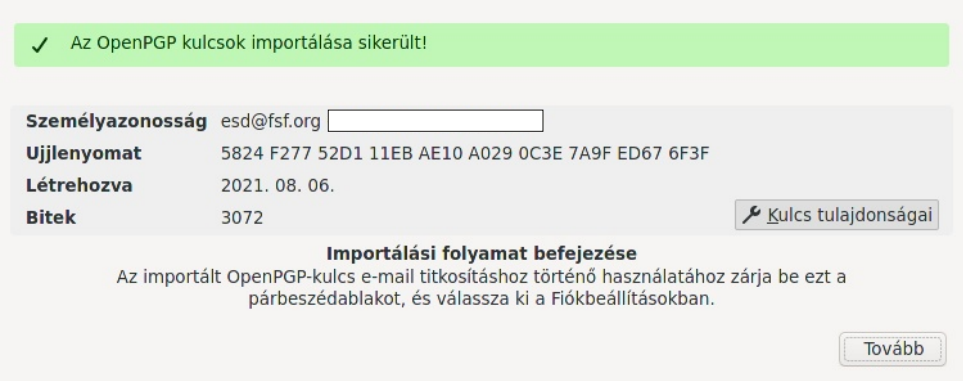
3. szakasz: az e-mail-titkosítás beállítása

Az Icedove (vagy Thunderbird) levelező program tartalmaz PGP-funkciót, ami a munkát nagyon egyszerűvé teszi. Végigvezetünk a lépéseken, amivel a kulcsodat ezekbe az e-mail-kliensekbe integrálhatod és használatod.

3.a lépés: állítsd be a titkosítást az e-mailbe







Ha az e-mailed titkosítását beállítottad, akkor bekapcsolódhatsz az Interneten folyó titkosított forgalomban. Először importáltatjuk a leveleződdel a titkos kulcsodat és azt is megtanuljuk, hogyan szerezzük be mások publikus kulcsait a szerverekről, így küldeni és fogadni is tudsz titkosított e-mailt.

Nyisd meg a levelezőt és használd az „Eszközök → **OpenPGP Kulcskezelő**”-t.

A „Fájl → **Titkos kulcsok importálása fájlból**” pontnál.

Válaszd ki a a 2.b lépésnél az exportálásakor [az_en_privat_kulcsom.asc] néven mentett fájlt.

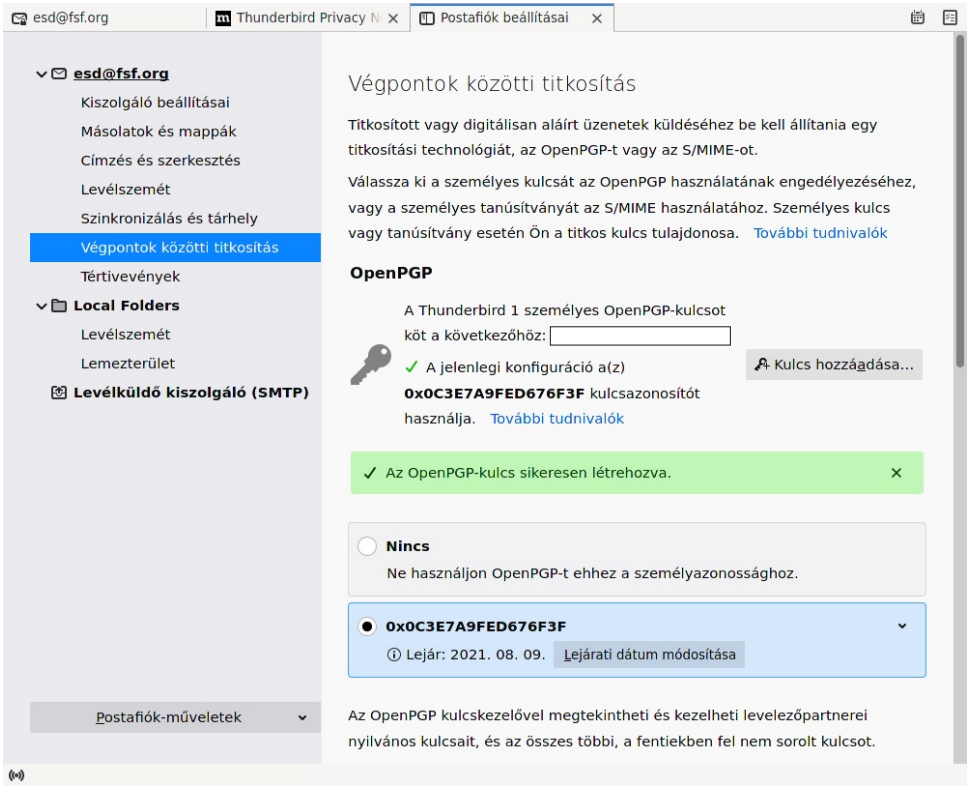
Nyisd meg a jelszavaddal.

Egy "OpenPGP kulcsok importálása sikeres" feliratú nyugtázó ablakot kapsz.

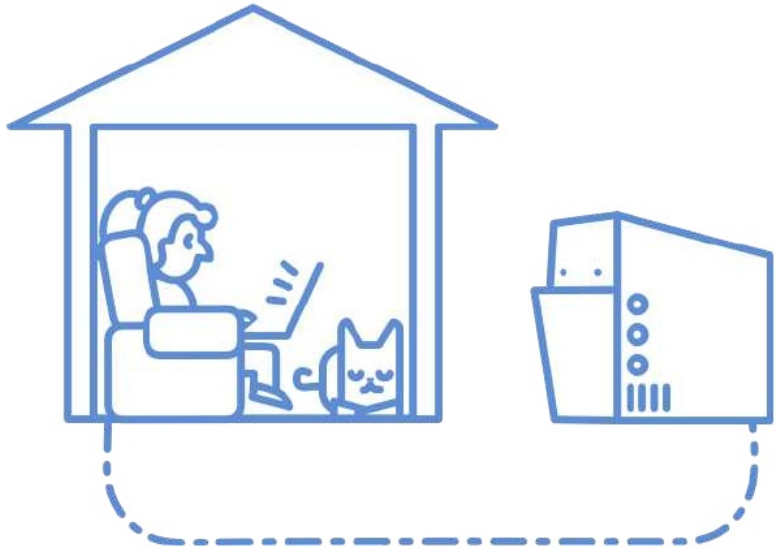
Lépj a „Szerkesztés” (Icedove-ban) vagy az „Eszközök” (Thunderbird-ben) → Postafiók beállításai” → Titkosítás a végpontok között”-be és ellenőrizd, hogy a te kulcsodat importálta-e és válaszd a „Privát kulcsként kezeld”-et.

Hibaelhárítás

Nem vagyok biztos, hogy az importálás rendben történt-e. Nézz be a „Postafiók beállításai → Titkosítás a végpontok között”-be („Szerkesztés” (Icedove) vagy „Eszközök” (Thunderbird)). Itt meggyőződhetsz, hogy a „személyes kulcsod az üzenethez kapcsolva van” látható-e. Ha nem, akkor újrapróbálhatod a Kulcs hozzáadása opcióval. Gondoskodj arról, hogy a kulcsfájl megfelelő, aktív és titkos legyen.

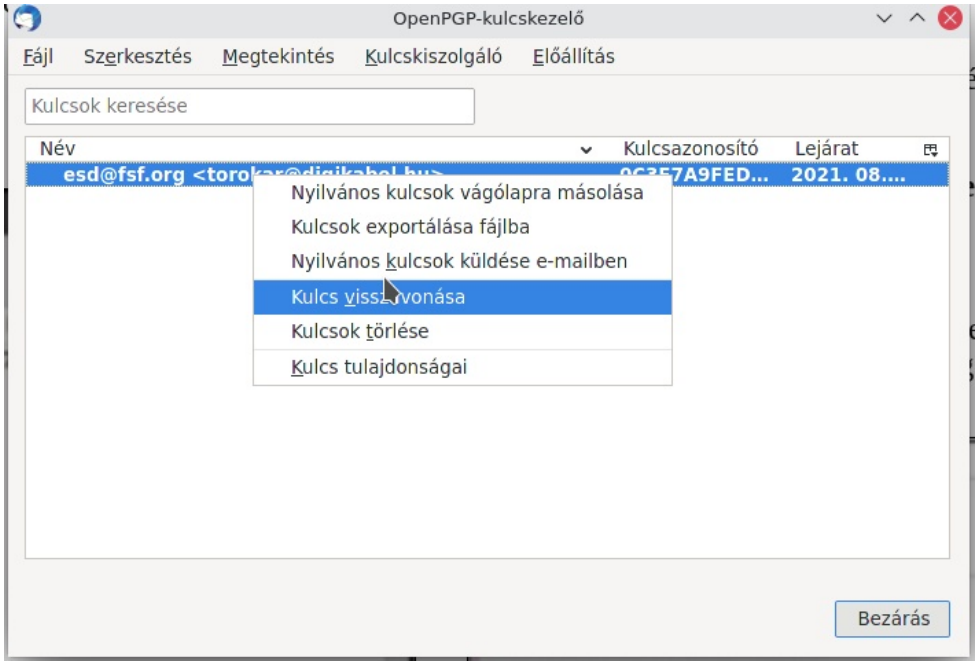


4. szakasz: próbáld ki!



Mosst lefuttatsz egy ellenőrző üzenetváltást az FSF Edward nevű programjával, ami tudja, hogyan kell a titkosítást használni. A külön jelzettek kivételével, valós, élő személlyel a kommunikáció lépései ugyanezek.

4.a lépés: küldd el Edwardnak a publikus kulcsodat.



Ez speciális lépés, valós személlyel levelezéskor nem szükséges. A levelező programodban a lépj az „Eszközök → OpenPGP kulcskezelő”-höz. A megjelenő listában látnod kell a kulcsodat. Jobb kattintás a kulcsodon és válaszd a **Publikus kulcs küldése e-mailben**-t. Ez készít egy új üzenetvázlatot, mintha az „Új üzenet” gombot lenyomtad volna, de mellékletben ott a publikus kulcsfájlod.

Címezd az üzeneted **edward-en@fsf.org**-nak. Legalább egy szót (bármi, amit csak akarsz) írj be a tárgy mezőbe és a szövegtörzsbe is. Ne küldd még el.

Szeretnénk, hogy Edward képes legyen megnyitni az üzenetet a kulcsfájllal, ezért az első üzenetünket titkosítatlanul kell elküldenünk. Gondoskodj arról, hogy a „Biztonság” lenyílóban a titkosítás ki legyen kapcsolva, válaszd a „Ne titkosítsa” pontot. Ha nincs titkosítás, nyomj meg a Küldés-t.

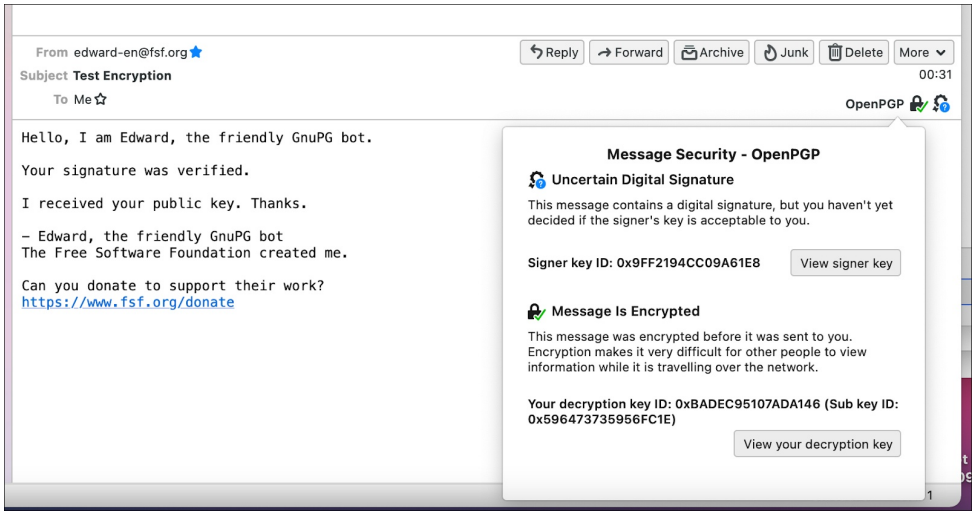
Két-három percbe beletelhet, mire Edward válaszol. Ezalatt, lépj tovább és néz meg ennek a leírásnak a „Használd helyesen” részét. Mihelyst megjött a válasz, jöhet a következő lépés. Innentől pontosan ugyanazt csinálod, amit valós személlyel levelezve tennél.

Edward válaszát megnyitva a GnuPG kérheti a jelszavadat, mielőtt a személyes kulcsodat használná a megfejtésre.

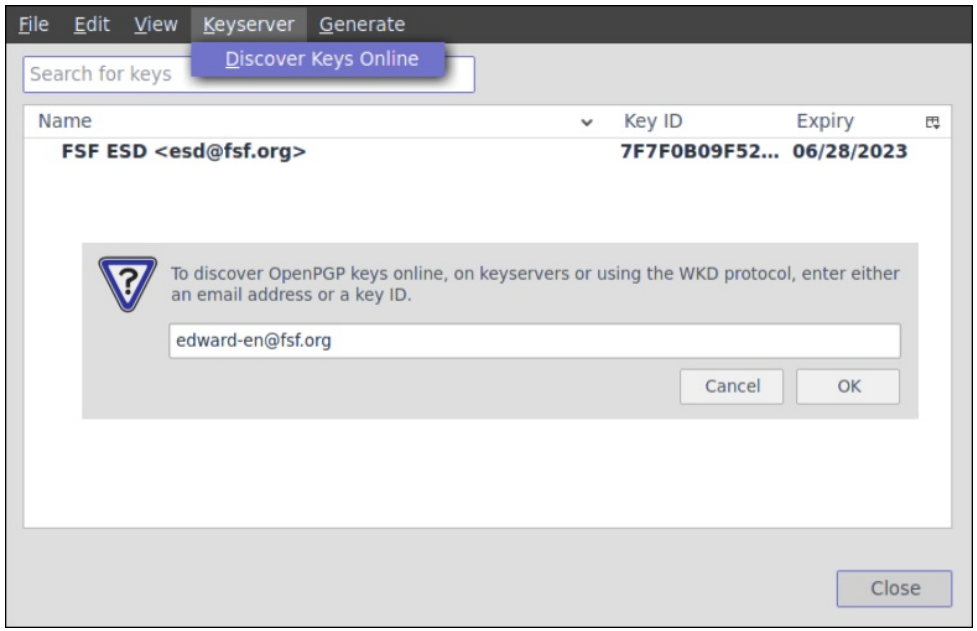
4.b lépés: titkosított e-mail ellenőrzése

Szerezd meg Edward kulcsát

Edward számára küldendő e-mail-hez kell a publikus kulcsa, ezért most azt le kell tölteni egy keyserver-ről. Kétféleképpen is megteheted:



1. opció: az első üzenetedre Edwardtól kapott válasz e-mail tartalmazza Edward publikus kulcsát. Az e-mail jobb oldalánál, nem sokkal az írási terület fölött találsz egy „OpenPGP” gombot, rajta egy lakattal és mellette egy kis kerékkel. Kattints rá és válaszd a „Felfedezés”-t a „Az üzenetet olyan kulccsal küldték, amivel még nem rendelkezel” szöveg mellett. Ekkor egy felnyíló jelenik meg, Edward kulcsának részleteivel.



2. opció: nyisd meg az OpenPGP kulcskezelőt és a „Kulcskiszolgáló”-nál válaszd a Kulcsok felfedezése online. Itt írd be Edward e-mail-címét és importáld Edward kulcsát.

Az **Elfogadott (nem megerősített)** opció hozzáadja a kulcsot a kulcskezelődhöz és most már használható kódolt e-mailek küldésére és Edward digitális aláírásának hitelesítésére.

A megnyíló, Edward kulcsának importálását megerősítő ablakban számos, a kulcsához társított e-mailt láthatsz. Ez így jó; biztonsággal importálhatod a kulcsot.

Mivel titkosítottad az e-mailt Edward publikus kulcsával, Edward privát kulcsa kell a kibontáshoz. Egyedül Edward rendelkezik a privát kulcsával, őt kivéve senki sem tudja dekódolni.

Küldj Edwardnak kódolt e-mailt

Írjál egy új e-mailt a levelező programoddal edward-en@fsf.org-nak címezve. A tárgy „Encrytpion test” vagy valami hasonló legyen és írj a szövegtörzsbe is.

Ez alkalommal, gondoskodj arról, hogy a kódolás legyen bekapcsolva a „Biztonság”-nál a „**Titkosítás megkövetelve**”. Ha a kódolás be van kapcsolva, üsd le „Küldés”-t.

Hibaelhárítás

„Címzett nem érvényes, nem megbízható vagy nem található”. Kódolt e-mailt akarsz küldeni olyannak, akinek még nem rendelkezel a publikus kulcsával. Ügyelj arra, hogy a kulcs kulcskezelődbe importálásánál a fenti lépéseket pontosan kövesd. Nyisd meg az OpenPGP kulcskezelőt, hogy meggyőződj a címzett meglétéről.

Nem lehet e-mailt küldeni. A következő üzenetet kapod, amikor megpróbálod elküldeni a titkosított e-maileded: „Unable to send this message with end-to-end encryption, because there are problems with the keys of the following recipients: edward-en@fsf.org.” Ez általában azt jelenti, hogy a kulcsot „nem elfogadott (ellenőrizetlen)” opcióval importáltad. Lépj a kulcs „tulajdonságai”-hoz úgy, hogy jobb billentyűvel kattintasz rajta az OpenPGP kulcskezelőjében és válaszd az „Igen, nem nyugtáztam, de ez a megfelelő kulcs”-ot az az ablak alján az „Elfogadás” opcióban. Küldd el újra az e-mailt.

Nem találom Edward kulcsát. Zárd be azokat a felnyílókat, amik a Küldés óta jelentek meg. Győződj meg arról, hogy csatlakozva vagy-e az Internethez és próbáld újra. Ha nem működik, ismételt meg az eljárást, másik keyserver-t választva, amikor választani kell.

Kódolatlan üzenet az Elküldött mappában. Noha, a más kulcsával kódolt üzenet nem tudod kibontani, a leveleződ automatikusan ment egy másolatot a te publikus kulcsoddal kódolva, amit az Elküldött elemek mappában úgy láthatsz, mint egy normál e-mailt. Ez normális és nem jelenti azt, hogy az üzeneted kódolatlanul ment volna el.

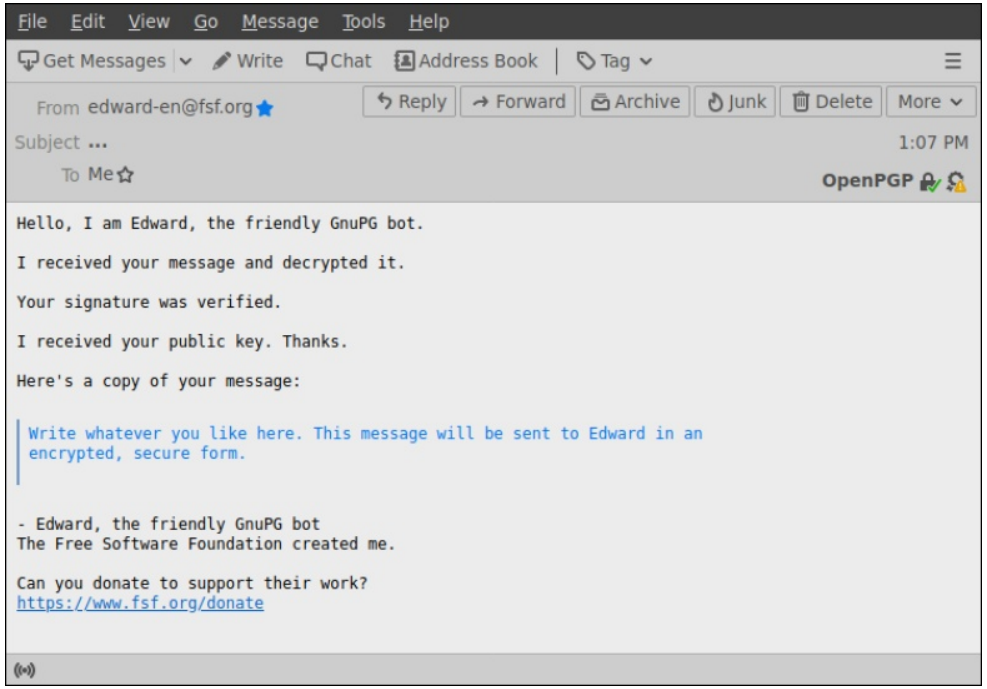
Haladó

Kódolj üzeneteket parancssorból. Kódolhatsz és dekódolhatsz üzeneteket és fájlokat parancssorból is, ha azt szereted jobban. Az --armor opció a titkosított kimenetet a szokásos karakterkészlettel jeleníti meg.

Fontos: biztonsági tippek

Noha az üzeneted titkosított is, a tárgy nem, tehát ne helyezz el ott személyes információkat. A küldő és fogadó címek szintén kódolatlanok, vagyis egy megfigyelő rendszer képes kitalálni, hogy kivel tartasz kapcsolatot. A megfigyelő ügynökök tudni fogják, hogy GnuPG-t használsz, még ha nem is tudja kitalálni, mit mondasz. Amikor mellékletet küldesz, az aktuális e-mail jellegétől függetlenül kiválaszthatod, hogy kódolod-e, vagy sem.

A potenciális támadásokkal szembeni nagyobb biztonság érdekében kikapcsolhatod a HTML-t. Helyette az üzenet törzsét írhatod sima szövegként. Ahhoz, hogy Icedove, vagy Thunderbird esetén ezt elérd, lépj a Nézet → Szövegtörzs mint→ Sima szöveg.



4.c lépés: válasz fogadása

Amikor Edward megkapja az üzenetet, a privát kulcsával dekódolja, majd válaszol neked.

Két-három percet eltarthat, mire Edward válaszol. Ezalatt, ugorj előre a leírásban és nézd meg a **Használd jól** részt.

Edward kódolt e-mailt küldve válaszol, így jelezve, hogy az e-mailedet megkapta és dekódolta. A leveleződ automatikusan dekódolja Edward üzenetét.

Az üzenetben az OpenPGP gombban a lakat fölött zöld pipával jelzi, hogy az üzenet titkosított és egy kis, narancssárga figyelmeztető jel mutatja, hogy a kulcs elfogadva, de nincs megerősítve. Ha nem fogadtad el a kulcsot, egy kis kérdőjelet láthatsz ott. A promptra kattintva a gombon, szintén a kulcs jellemzőihez jutsz el.

4.d lépés: aláírt tesztüzenet küldése

A GnuPG-ben lehetőség van üzenetek és fájlok aláírására, igazolva, hogy azok tőled származnak és nem módosultak menet közben. Ezek az aláírások erősebbek, mint az unokatestvérük a toll és papír – nem lehet hamisítani, mivel a privát kulcsod nélkül nem lehet ilyeneket készíteni (újabb ok, amiért biztos helyen kell tartanod a privát kulcsodat).

Bárkinek aláírhatsz üzenetet, így ez a legjobb módja az emberekkel tudatni, hogy GnuPG-t használsz és biztonságos kommunikációt folytathatnak veled. Ha nincs GnuPG-jük, el tudják olvasni az üzenetedet és láthatják az aláírásodat. Amennyiben van GnuPG-jük, azt is tudják ellenőrizni, hogy az aláírásod valódi-e.

Hogy Edwardnak aláírt e-mailt küldj, fogalmazz meg egy üzenetet az e-mail-címére és kattints a ceruza ikonra a lakat ikonja mellett, ami aranyra változik. Ha aláírsz egy üzenetet, a GnuPG kérni fogja a jelszót, mielőtt elküldené, mivel ki kell nyitnia a privát kulcsodat az aláíráshoz.

A „Postafiók beállításai → Végpontok közötti titkosítás” beállítható, hogy alapból hozzáadja a digitális aláírást.

4.e lépés: válasz fogadása

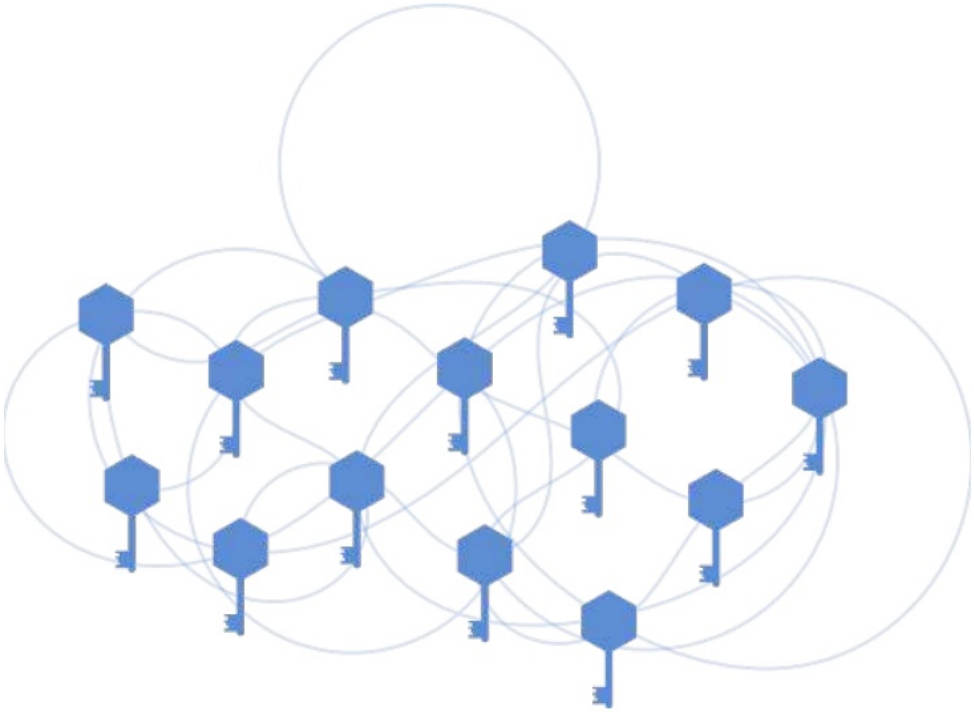
Amikor Edward megkapja az e-mailedet, a publikus kulcsoddal (amit a 3. lépésnél küldtél meg neki) hitelesíti, hogy az általad küldött üzenetet nem módosították és titkosít neked egy választ.

Két-három percet eltarthat, mire Edward válaszol. Ezalatt, ugorj előre a leírásban és nézd meg a leírásban a **Használd jól** szakaszt.

Edward válasza titkosítva érkezik, mivel titkosítást szeret használni, amikor csak lehet. Ha minden a tervek szerint megy, azt kell üzennie, hogy „Your signature was verified”. Ha a aláírt tesztüzeneted titkosított volt, először azt jelzi.

Amikor kézhez kapod Edward e-mailjét és megnyitod, az e-mail-kliensed automatikusan érzékeli, hogy a publikus kulcsoddal lett kódolva és a privát kulcsoddal dekódolja azt.

5. lépés: ismerd meg a Web of Trust-ot



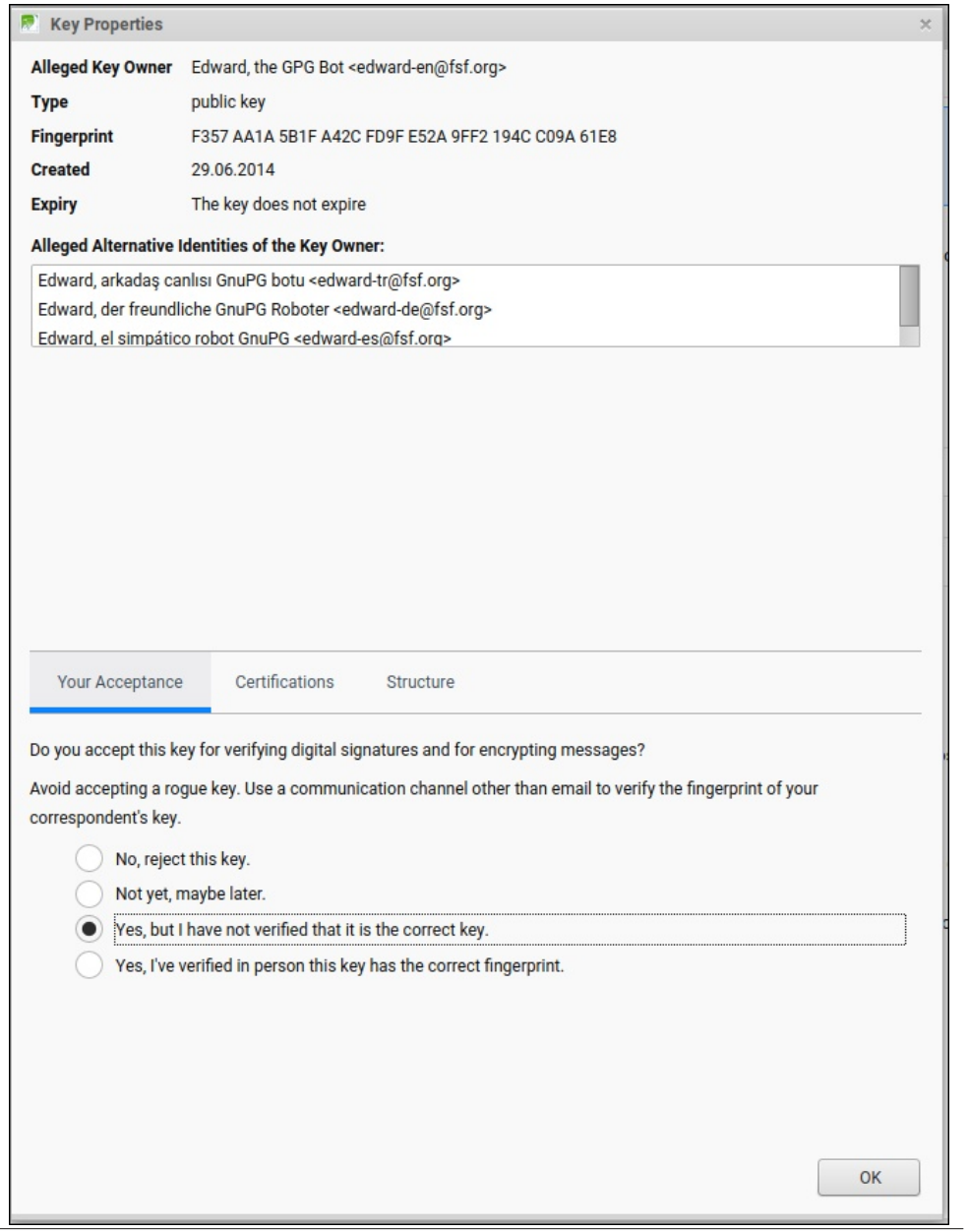
Az e-mail-titkosítás erőteljes technológia, de van egy gyengesége: kell valamilyen módszer annak ellenőrzésére, hogy valaki publikus kulcsa tényleg az övé-e. Máskülönben nem lehetne megakadályozni, hogy egy támadó a barátod nevével készítsen egy e-mail-címet, hozzá egy kulcsot és megszemélyesítse számodra a barátodat. Ezért, a szabad szoftver programozói, akik kidolgozták a titkosítást, kialakították a kulcsaláírást rendszerét és a Web of Trust-ot.

Más kulcsának aláírásával közlöd a nyilvánossággal, hogy tanúsítod, az hozzá tartozik és nem valaki máshoz.

Kulcsok aláírása és üzenetek aláírása ugyanazt a típusú matematikai műveletet alkalmazza, de teljesen eltérő eredményre vezethet. Jó gyakorlat általában aláírni az e-maileket, de ha alkalmanként aláírod mások kulcsát, előfordulhat, hogy véletlenül hitelt adsz valamilyen imposztornak.

Akik a publikus kulcsodat használják, láthatják, ki írta alá. Ha már elég sokáig használtad a GnuPG-t, a kulcsodhoz több száz aláírás tartozhat. Az olyan kulcsot, amin sok olyan aláírása szerepel, akikben megbízol (trust), sokkal megbízhatóbbnak tekintheted. A Web of Trust (bizalom hálózata) GnuPG-t használók egysége, akiket az aláírásaikon keresztül kifejezett bizalom köt össze egymással.

5. lépés: írj alá kulcsot



A levelező programod menüjében keresd meg az OpenPG Kulcskezelőt és Edward kulcsánál válaszd a jobb kattintással elérhető **tulajdonságokat**.

Az „Elfogadás” pontnál választhatod az **„Igen, meggyőződtem, hogy ehhez a kulcshoz a megfelelő ujjlenyomat tartozik”** opciót.

Azt jelentetted ji, hogy „Hiszem, hogy Edward publikus kulcsa tényleg Edwardhoz tartozik.” Ez nem jelent túl sokat, mivel Edward nem valós személy, de jó eljárás és valós személyek esetében fontos. Továbbiakat olvashatsz személy kulcsának aláírásáról az „ID ellenőrzése aláírás előtt” szakaszban.

Kulcsok azonosítása: ujjlenyomatok és ID-k (azonosítók)

Az emberek publikus kulcsait általában a kulcs ujjlenyomata alapján azonosítják, ami egy karakterlánc, mint az F357AA1A5B1FA42CFD9FE52A9FF2194CC09A61E8 (Edward kulcsánál). Megnézheted a saját és mások nyilvános kulcsának ujjlenyomatát a Kulcskezelőben az adott kulcs jobb kattintásos menüjében a jellemzők kiválasztásával. Jó módszer, hogy az e-mail-címed megosztásakor, azzal együtt az ujjlenyomatodat is megosztod, így amikor a keyserver-ről letöltik a kulcsodat, ellenőrizhetik, hogy az megfelelő-e.

Szoktak a publikus kulcsokra egy rövidebb keyID-vel (kulcs azonosító) is hivatkozni. A keyID azonnal látható a Kulcskezelő ablakában. Régebben ezeket a nyolckarakteres keyID-ket használták azonosításra, amik egy időben biztonságosak voltak, de ma már nem megbízhatóak. Az ujjlenyomat egészét vizsgálnod kell, amikor ellenőrzöd, hogy a kulcs megfelel-e ahhoz a személyhez, akivel kapcsolatot keresel. Sajnos gyakori hamisítási módszer, amikor valaki szándékosan úgy készít kulcsot, hogy az ujjlenyomatának utolsó nyolc karaktere megegyezzen valaki máséval.

Fontos: mire vigyázzunk, amikor kulcsot írunk alá?

Valaki kulcsának aláírása előtt meg kell győződni, hogy ténylegesen hozzá tartozik -e és valóban az, akinek mondja magát. Ideális esetben a bizalom az idők folyamán az illetővel tartott kapcsolatból és üzenetváltásokból, illetve az illető és mások közötti kapcsolatot látva alakul ki. Bármikor kulcsot írsz alá, kérd a teljes publikus kulcs ujjlenyomatának bemutatását és nem csak a rövidebb keyID-ét. Ha fontosnak tartod valaki kulcsát aláírni, akivel találkoztál, kérj tőle hivatalos igazolványt és győződj meg, hogy az igazolványon szereplő név egyezik-e a publikus kulcs nevével.

Haladó

Foglalkozz a Web of Trust-tal. Sajnos a bizalom nem terjed a felhasználók körében olyan módon, ahogy sokan gondolják. A GnuPG-közösség erősítésének egyik legjobb módja, a Web of Trust megértése és a körülmények által megengedett lehető legtöbb személy kulcsának körültekintő aláírása.

6. szakasz: használd jól

Mindenki egy kicsit másképp használja a GnuPG-t, de az e-mail biztonságáért fontos néhány alapvető lépés betartása. Ha nem követed, azzal a veled kommunikáló személyek privát létét kockáztatod csakúgy, mint a sajátodét és károsítod a Web of Trust-ot.

Mikor titkosítsak? Mikor írjak alá?

Minél több levelet tudsz titkosítani, annál jobb. Ha csak alkalmanként titkosítasz e-maileket, minden kódolt levél felkeltheti a megfigyelő rendszer érdeklődését. Ha az összes, vagy a legtöbb e-mailt kódolod, a megfigyelést végzők nem tudják, hol kezdjenek hozzá. Ez nem jelenti azt, hogy az e-mailek alkalmankénti titkosítása nem hasznos – nagyszerű kezdés és a tömeges megfigyelést sokkal nehezebbé teszi.

Hacsak nem akarod elleplezni magad (ami további védelmi eljárásokat igényel), semmi sem szól az ellen, hogy az összes üzenetet aláírd, függetlenül, hogy kódolt-e vagy sem. Miközben lehetővé teszed a GnuPG-vel rendelkezőknek, hogy ellenőrizzék, a levél tőled jött-e, az aláírás finoman jelzi a többieknek, GnuPG-t használsz és támogatod a biztonságos kapcsolattartást. Ha gyakran küldesz aláírt levelet olyanoknak, akik nem ismerik a GnuPG-t, érdemes egy, erre a leírásra mutató hivatkozást is csatolni a szabványos aláírásodba (szöveges és nem kriptográfiai félét).

E-mail-önvédelem: kézikönyv a megfigyelés elleni harchoz GnuPG titkosítással

Óvakodj az érvénytelen kulcsoktól

A GnuPG biztonságosabbá teszi a levelezést, de fontos figyelni az érvénytelen kulcsokra, amik rossz kezekbe kerülhetnek. Érvénytelen kulccsal titkosított e-mailt a figyelő programok esetleg elolvashatják.

A leveleződben lépj vissza Edward által küldött első titkosított e-mailhez. Mivel Edward a te publikus kulcsoddal írta alá, egy zöld pipát láthatsz az OpenPGP gombon.

GnuPG-t használva váljon szokásoddá ennek a gombnak a figyelése. A program ott jelzi, ha olyan e-mailt kapsz, amit nem megbízható kulccsal írtak alá.

Másold biztos helyre a visszahívási tanúsítványodat

Emlékszel, amikor elkészítetted és mentetted a kulcsaidat, a GnuPG készített egy visszavonási tanúsítványt? Ideje a tanúsítványt a legbiztonságosabb tárolóba kimásolni – egy flash meghajtó, lemez vagy merevlemez otthon egy biztonságos helyen tárolva jó lehet, és nem egy eszközön, amit magaddal szoktál vinni. A legbiztonságosabb ismert módszer a visszavonási tanúsítvány kinyomtatása és biztos helyen tárolása.

Ha a privát kulcsod akármikor elveszik, vagy ellopják, szükséged lesz erre a tanúsítványra, hogy tudasd az emberekkel, nem használod többé azt a kulcspárt.

Fontos: azonnal intézkedj, ha valaki megszerzi a privát kulcsodat.

Ha elveszted a privát kulcsodat vagy más birtokába jut (mondjuk lopással vagy a géped feltörésével), fontos, hogy azonnal visszahívd, mielőtt bárki más használná a titkosított üzenteid olvasására, vagy az aláírásod hamisítására. Ebben a leírásban nem tárgyaljuk a kulcs visszahívását, ezeket az instrukciókat követheted. Miután a visszahívás megtörtént, készíts új kulcsot és az új kulcsoddal együtt küldj egy e-mail mindenkinek, akinél általában használod a kulcsodat, hogy biztosan tudjanak róla.

Webmail és a Gnupg

Ha webböngészővel nézed az e-maileded, akkor webmailt használsz, egy levelezőt, amit távoli weblapon tárolnak. A webmaillel ellentétben az asztali levelező a számítógépeden fut. Mivel a webmail nem képes dekódolni a titkosított e-mailt, titkosított formájában fogja mutatni. Ha alapvetően webmail-t használsz, tudni fogod, hogy meg kell nyitni a leveleződet, amikor kódolt üzenetet kapsz.

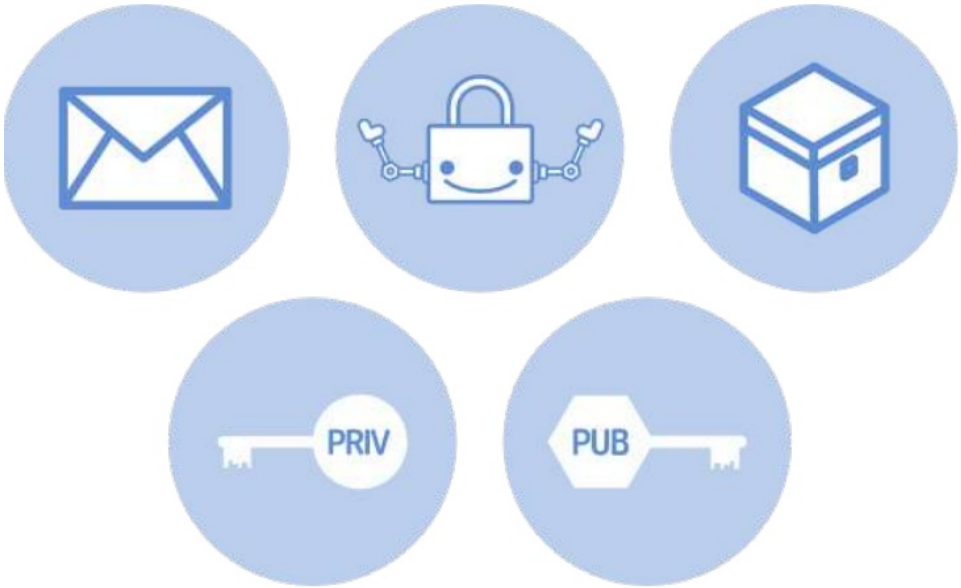
A publikus kulcsod képezze az online azonosságod részét

Először is add a publikus kulcsodat az e-mail-aláírásodhoz, majd írj egy e-mailt legalább öt barátodnak, tudatva velük, hogy épp most állítottad be a GnuPG-t és említsd meg nekik a publikus kulcsodat. Készíts hivatkozást ehhez a leíráshoz és kérd őket a csatlakozásra. Ne feledd, van még egy csodás tájékoztató rajz is.

Kezdd el kiírni a publikus kulcsodat mindenhova, ahol csak látható az e-mail-címed: közösségi médián a profilodba, blogba, weblapra vagy névjegyedre. (A Free Software Foundation-nál, mi a munkatársak oldalaira rakjuk ki.) Olyan hozzáállást kell kialakítani, hogy hiányérzetünk legyen, amikor publikus kulcs ujjlenyomata nélküli e-mail-címet látunk.

E-mail-önvédelem: kézikönyv a megfigyelés elleni harchoz GnuPG titkosítással

7. szakasz: következő lépés



Most végére értél a GnuPG e-mail-titkosítás, a tömeges megfigyelés elleni lépések alapjainak. A következő lépések segítenek, hogy a legtöbbet hozd ki a befektetett munkádból.

Csatlakozz a mozgalomhoz

Most tettél egy hatalmas lépést afelé, hogy megvédd az online személyes teredet. De az, hogy mindenki egyedül cselekszik, nem elég. A tömeges megfigyelés megbuktatásához mozgalmat kell alapítani a számítógép-felhasználók függetlensége és szabadsága érdekében. Csatlakozz a Free Software Foundation közösségéhez, hogy hasonló gondolkodású emberekkel találkozz és dolgozz a változásért.

GNU Social

Mastodon

Twitter

Olvasd el, hogy a GNU Social és a Mastodon miért jobb mint a Twitter és miért nem használunk Facebook-ot.

Vezess be új embereket az e-mail-önvédelembe

Megérteni és beállítani e-mail-titkosítást félelmetes feladat sokaknak. Hogy bevonhassuk őket, könnyítsd meg a publikus kulcsod elérését és ajánlj fel a segítséged a titkosításban. Íme néhány javaslat:

- # Tarts e-mail önvédelmi oktatást a barátaidnak és a közösségnek, az oktató anyagunk alapján.

- # A megosztási oldalunkkal készíts e-mailt néhány barátodnak és kérd fel, hogy csatlakozzanak a titkosított e-mail-használatban. Ne felejtsd el csatolni a GnuPG publikus kulcsod ujjlenyomatát, hogy könnyen letölthessék a kulcsodat.

- # Tedd ki a publikus kulcsod ujjlenyomatát mindenhol, ahol az e-mail-címedet meg szoktad jelentetni. Néhány jó hely: az e-mail-aláírásod (szöveges típusú és nem a titkosítási), a közösségi médiaprofil, blog, weblapok vagy névjegy. Mi, a Free Software Foundation-nál a „munkatársak” oldalra rakjuk ki a sajátunkat

Védd jobban a digitális életedet

Tanulj a megfigyelést nehezítő technológiákról a levelezés, a merevlemezes tárolás, az online megosztás és hasonlók tekintetében a Free Software Directory’s Pack-ból és a prism-break.org-tól.

Ha Windowst, Mac OS-t vagy más jogvédett operációs rendszert használsz, ajánljuk, hogy válts szabad szoftveres operációs rendszerre, mint a GNU/Linux. Ez sokkal nehezebbé teszi a támadóknak, hogy belépjenek a számítógépedbe egy rejtett hátsó bejáraton. Nézd meg a Free Software Foundation által támogatott GNU/Linux verziókat.

Opcionális: egészítsd ki az e-mail-védelmedet Tor-ral

Az Onion Router (Tor) hálózata az internetes kommunikációt többrétegű titkosításba csomagolja és sokszorosan körbeutaztatja a világban. Jól használva a Tor összezavarja a helyi megfigyelőket és a világméretű megfigyelő apparátust. GnuPG titkosítással együtt használva a legjobb eredményt adja.

Ahhoz, hogy a leveleződ Tor-on keresztül küldje és fogadja az üzeneteket, telepítsd a Torbirdy kiegészítőt a Kiegészítők menün keresztül.

Mielőtt a Tor-on keresztül néznéd meg az üzeneteidet, mindenképpen legyél tisztában a kapcsolódó biztonsági kérdésekkel. Ez a tájékoztató rajz, amit egy Electronic Frontier Foundation-os barátunk készített, bemutatja, hogy a Tor miképpen véd meg téged.

E-mail-önvédelem: kézikönyv a megfigyelés elleni harchoz GnuPG titkosítással

A magazin szerkesztőjének megjegyzése: *a PCLinuxOS Magazine korábban foglalkozott az OpenPGP használatával e-mail titkosítására egy, 2013 novemberében YouCanToo által írt, Mailvelope OpenPGP titkosítás OpenPGP-vel című cikkben. Ezt a cikket is szabadon felhasználhatod forrásként, hogy felgyorsítsd a PGP használatát e-mail titkosítására. Meggyőződésünk, hogy ennek a két írásnak felhasználásával képes leszel kialakítani egy e-mail-titkosítási eljárást, ami az igényeidnek és helyzetednek megfelel.*