Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

GPG útmutató a biztonságos kommunikációhoz

2012. január

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalomjegyzék

Bevezető

Napjainkban az informatika világában egyre nagyobb hangsúlyt kap a biztonság, legyen szó személyek, intézmények, vagy informatikai eszközök, információk és adatok biztonságáról. Ezt szem előtt tartva a PTA CERT-Hungary (Nemzeti Hálózatbiztonsági Központ) az alábbi dokumentumban ismerteti a PGP/GPG-vel kapcsolatos legfontosabb információkat, amely az intézményen belüli és az intézmények közötti elektronikus levelezést teheti még biztonságosabbá. A dokumentumban foglaltakat alkalmazva jelentősen csökkenthető az elektronikus levelek információinak és csatolmányainak kompromittálódása. A dokumentum a https://www.accessnow.org/page/-/docs/GPG_Guide_for_Secure_Communications.pdf alapján készült.

Miért érdemes általában titkosítást, azon belül pedig GPG-t használni?

Az adatok és a kommunikáció titkosítása sok funkciót tölt be, amely növeli a biztonságot. Egyrészt biztosítja, hogy a nem biztonságos hálózatokon, például az interneten vagy a telefonhálózaton továbbított - és elfogott - adatokat ne lehessen elolvasni (titkosság). Másrészt lehetőséget biztosít annak igazolására, hogy egy információ, amelyet úgy tűnik, hogy egy megbízható ismerős küldött, valóban tőle jött-e (hitelesítés), és az információt nem módosították-e illetéktelenül (sértetlenség). Talán túlzásnak tűnik, hogy a nem biztonságos kommunikáció nagyobb veszélyt jelenthet, mint például egy rally-n vagy egy krízistérségben való tényleges jelenlét, de a szervezetek munkatársai könnyű célponttá válhatnak, ha a terveket nem biztonságos kommunikációs csatornákon beszélik meg, és a későbbi helyszínek ismertté válnak. A kommunikáció nem az egyetlen, de nagyon fontos terület, ahol figyelmet kell fordítani a biztonságra (például üzleti titok).

A GPG (GNU Privacy Guard) egy széles körben elismert, jól bevált, alapos vizsgálatnak alávetett titkosító szoftver. PGP (Pretty Good Privacy) alapokra épül, és a (későbbiekben ismertetett) nyilvános kulcsú titkosítási technikákat alkalmazza a titkosításhoz és a hitelesítéshez. A leggyakrabban használt asztali számítógépes és/vagy laptopos operációs rendszerek (Windows, Mac, Linux) mindegyikéhez vannak verziói, továbbá a Firefox és Chrome böngészőkön keresztüli webmail hozzáféréshez, valamint az iPhone, iPad és Android alapú intelligens mobil eszközökhöz is elkészültek már vagy most készülnek a verziók. Bár elsősorban e-mailekhez használatos, más alkalmazások, például levelezési listák, valamint fájlok és fájlrendszerek titkosításához is kiválóan alkalmazható.

Ez az útmutató a GPG telepítését és használatát, valamint a nyilvános kulcsú titkosítással kapcsolatos alapvető tudnivalókat ismerteti.

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMA6qp8+hrrSkyAQf/VP/ojB3mNxeVLnmdBDObeVPjopN3G5ICv1PfDm+Iezhi
jTsBFKqg/l36wwOrTFJTgKjfNm1qlyOg4R+WYSzdf7tZBosDWmnWDrrFUfOIEBsF
AxIEjDOFXsXyVOs1RD886mVlRXvRDunYfq6/N38/JTZ4DDbEzi94vxcfZbse4xGO
LPDRpIlMs3aPMAcFUyfopLHon+5tun4kPptLpv7qns1GG+by8iIgYl1wytyTSWBE
uPZjVmwgfpoGNVX+6oj4p3sbbIW4W9ipCdjUylW9fcCSDdQXYPhA/d2j5Fq3b4P2
OfVvTHveFdFOrwey3QqPoS85+BdhPadxrAKjtCvke4UCDAMnm/6+HKa4fgEP/iXS
G8kyLM+TEFxion51gYEdQf+qJpaOKiTdUvpYsf8oMGlbM9O/KX4hdGbe/XwUiJnj
nCye5uEOtrOP2MEaAAnkLO7B/JdwCgetFYq9qybYgE/s+3WH8gbJhl9W63eTUjGS
7doI8+fSQI6yINhbJkE2hj7pPjcOfGa/d+OvbEfXi8mXOdxlaSTW/thVHcbIa5Jg
Mb3yUNkQhAQ7BoHfMzz6Yn28lOeult2Y7qaHnbJ6b5NPpCTVDAaJQn/X+qtQBul4
T2BU3Fecwn86lPYYEsaWIBGGouYufVNykeYqJvc93BbEK/iVkPCzOJ86ccETiaAS
545b/dpKtGTDnogOSmhYCEO7tzAx3WiUDCAUO3xOb5cCd7YkdywtkgCyyFbV9KPB
Z61aaCJQoNnpB66xgJDDfNV8RdpZjEUjIxDDLNLEOpmgEFWC5/jf8p4jZML1csDr
```

Üzenet szövege GPG-vel való titkosítás után.

A jó gyakorlat fő elemei

Megszokásból titkosítani kell minden kommunikációt. Így a felhasználó nem feledkezik meg róla, amikor tényleg fontos a titkosítás használata. Ráadásul ha az üzenetek csak egy része kerül titkosításra, akkor ezek az üzenetek válnak az esetleges megfigyelések célpontjává.

Titokban kell tartani a titkos kulcsot. Amennyiben a kulcs biztonsága veszélybe került, vissza kell vonni és újat kell generálni helyette. Titokban kell tartani a titkos kulcsot védő jelszót, és ha ennek biztonsága veszélybe kerül, minél előbb meg kell változtatni, a kulcsokat pedig vissza kell vonni.

Ajánlott közzé tenni a nyilvános kulcsot minél szélesebb körben, és megfelelő aláírási eljárások alkalmazásával ajánlott aláíratni minél több emberrel (a kulcsot aláíró személy felé az Ön személyazonosságát és a kulcs integritását egyaránt igazolnia kell). Ezért, ha más szervezetek tagjaival van a GPG-t használó felhasználónak találkozója, mindig érdemes megragadni a lehetőséget, hogy aláírják egymás kulcsait.

Igazolja a levelezőpartnerek személyazonosságát oly módon, hogy ismert kulcsszerverekről letölti a nyilvános kulcsot, és ellenőrzi az aláírásokat.

Alaptelepítés

Az alaptelepítés miden platform esetében ugyanazokból a lépésekből áll:

- Le kell tölteni az adott platformhoz való GPG-t és azokat a kiegészítő szoftvereket, amelyekre szüksége van;
- Ki kell csomagolni és telepíteni a GPG-t és a kiegészítő szoftvereket;
- Futtatni kell a GPG-t, és generálni szükséges egy kulcspárt (egy nyilvános és egy titkos kulcsot);
- Ki kell választani a titkos kulcsot védő jelszót, amely könnyen megjegyezhető és könnyen begépelhető, de nehezen kitalálható;
- Meg kell adni az esetleges további beállításokat a telepített szoftverben;

» Exportálni kell a nyilvános kulcsot ASCII armored formátumban, és lehetőleg meg kell kérni valakit, aki igazolni tudja a GPG-t használó felhasználó személyazonosságát, hogy aláírásával az felhasználó kulcsaként hitelesítse a kulcsot;
» Fel kell tölteni az aláírt nyilvános kulcsot egy vagy több kulcsszerverre;
» Fel kell jegyezni a kulcs lejárati dátumát, és be kell állítani, hogy a meghosszabbításról vagy újragenerálásról előzetes figyelmeztetést kapjon;
» Létre kell hozni visszavonási (revoke) tanúsítványt, amelyet tökéletesen biztos helyen kell tartani, hogy azonnal fel lehessen tölteni, amikor a felhasználó titkos kulcsa esetleg veszélybe kerül (például az eszközt, amelyen a felhasználó titkos kulcsa tárolásra került, ellopják vagy elveszíti), vagy ha a felhasználó elfelejtette a jelszót. Minden esetben el kell távolítani azokról az eszközökről, amelyeken a felhasználó a titkos kulcsait tárolja.

Az egyes platformokra vonatkozó részletes telepítési utasítások a dokumentum végén találhatók.

A GPG használat közben

Windows-felhasználók figyelmébe: Az alábbiakban ismertetett parancsok közül némelyikhez parancssort kell indítani. Amennyiben telepítésre került a GPG Kleopatra modulja vagy egy más grafikus kezelőfelületet, akkor ott is végre lehet hajtani ezeket a műveleteket.

- XP esetében a Start menüre kattintva, ki kell választani a Futtatás (Run) parancsot, és a következőt begépelni:
  command.com
  Választható a Programok (Programs) / Kellékek (Accessories) / Parancssor (Command Prompt) megoldás is a parancssori ablak eléréséhez.
- A Vista és a Windows 7 nem tünteti fel a Futtatás (Run) opciót a Start menüben; azt külön kell aktiválni. Ehhez a Start gombra kattintva, ki kell választani a Tulajdonságok (Properties) elemet, majd a Start menü (Start Menu) fület és a Testreszabás (Customize) elemet. Az újonnan megjelenő ablakban egy hosszú lista látható különböző választási lehetőségekkel. Lefelé görgetve, meg kell keresni a Futtatás parancs (Run Command) elemet, és ezt aktívvá tenni a négyzet bejelölésével. Végül az OK gombra kell kattintani, majd az Alkalmaz (Apply) gombra. A Futtatás elemnek ezután meg kell jelennie a Start menüben, és be lehet írni a
  command.com
  parancsot, akárcsak XP-ben.

Mac OS X felhasználók figyelmébe: Az alábbiakban ismertetett parancsok némelyikéhez parancssort kell indítani. Ehhez az Applications / Utilities / Terminal elemet kell választani.
A parancssor (más néven „konzol”) megnyitása után a parancsok minden platform esetében megegyeznek.

Jelszóválasztás

A jó, nehezen feltörhető jelszó kiválasztása nagyon fontos, ugyanis ez a leggyengébb láncszem a GPG biztonsági rendszerben. Bárki, aki megszerzi a jelszót és a titkos kulcsot, hozzáférhet minden kommunikációhoz, és – ami még ennél is rosszabb – megszemélyesítheti az érintett felhasználót

megbízható ismerősei előtt. A jelszavaknak, mivel azokat sokszor kell használni, könnyen gépelhetőnek, könnyen megjegyezhetőnek és nehezen kitalálhatónak kell lenniük. Bár általában elfogadható, ha ugyanazt a jelszót használják a kevésbé fontos weboldalakon (például új weboldalak regisztrációs rendszereiben), úgy a titkos kulcs a legbizalmasabb adat, amelyet mindig szigorúan védeni kell. Egyedi jelszót kell választani, és kivételes elővigyázatossággal kell őrizni. Amennyiben a leghalványabb jele is van annak, hogy a jelszó illetéktelen személy birtokába került, a kulcsokat mielőbb vissza kell vonni. Utána, amint biztonságos helyzetben van a felhasználó (biztonságos hálózat, biztonságos rendszer, biztonságos billentyűzet), új kulcsokat kell generálni és új jelszót kell létrehozni.

Jelszóként ne használják nevüket, a szervezetük nevét, saját címüket vagy szervezetük címének valamely részletét, háziállatuk, házastársuk, gyermekük, iskolájuk nevét, illetve semmiféle olyan információt, amely a felhasználóval kapcsolatos és esetleg fellelhető az interneten (még az állítólagosan titkos részeken, például a zárolt Facebook oldalon lévő információkat sem). Ne legyen használva továbbá olyan önálló szavak, amelyek bármely nyelv szótárában megtalálhatók, ugyanis ezek könnyen feltörhetők.

Sok tankönyv szerint azok a jelszavak a legbiztonságosabbak, amelyeket véletlenszerűen generáltak, illetve megfelelnek bizonyos szabályoknak, például meghatározott hosszúságúak, és legalább egy nagybetűt és egy számot tartalmaznak. Az ilyen módszerekkel létrehozott jelszavakat nehéz pontosan megjegyezni és nehéz beírni a billentyűzeten; sok ember számára problémát jelent, hogy megjegyezzen akár egyetlen, 22 véletlenszerű karakterből álló karakterláncot is, ezért leírja, ami igen veszélyes gyakorlat lehet.

Jobban használható az a stratégia, hogy egy megjegyezhető mondatot hoz létre a felhasználó, amelyben természetesen vannak nagybetűk, szóközök és írásjelek is, amelyet nagyon nehezen lehetne kitalálni.

Amennyiben a jelszó biztonsága bármikor veszélybe kerül (tehát egy másik személy megismeri), akkor vissza kell vonni a kulcsot, új kulcsot kell generálni, le kell védeni egy teljesen új jelszóval, és megfelelő figyelmeztetéseket kell kiadni, hiszen ezek után feltételezni kell, hogy a régi kulccsal bonyolított kimenő és bejövő kommunikáció nem biztonságos többé.

Amennyiben bármikor meg kell változtatni a jelszót - például mert nehéz beírni vagy a felhasználó szeretné még biztonságosabbá tenni -, meg kell nyitni egy parancssort, és a következő parancsot begépelni:

gpg --edit-key <mykey>

Az <mykey> helyébe írja be a kulcs azonosítószámát vagy pedig az ahhoz tartozó e-mail cím egy részletét.

A parancssorba írja be ezt a parancsot:

passwd

Utána be kell írni a régi jelszót, majd pedig kétszer az új jelszót (egyszer meg kell adni, egyszer meg kell erősíteni). A parancssorba írja be ezt a parancsot:

save

Ezután nem szabad elfelejteni frissíteni biztonsági másolatokat vagy más telepítéseket, hogy ezek is az új jelszóval legyenek konfigurálva.

E-mail

Érdemes megszokásból titkosítani minden e-mailt, két okból is. Egyrészt ha a felhasználó csak a bizalmas üzeneteket titkosítja, ezek azonnal kitűnnek és célponttá válnak bárki számára, aki figyeli a kommunikációját. Másrészt ha a felhasználó szelektíven titkosít, nagy az esélye, hogy egyszer elfelejt majd titkosítani egy fontos dolgot.

Szerencsére a levelező szoftverekben az összes e-mail titkosítása egy négyzet bejelölésével vagy más egyszerű művelettel beállítható.

Thunderbird (Windows és GNU/Linux) esetében le kell tölteni és telepíteni kell az Enigmail plug-int. A Thunderbird ezután kiegészül egy OpenPGP menüvel, ahonnan a legtöbb GPG funkció beállítható és működtethető. Kulcsok generálásához, szerkesztéséhez vagy visszavonásához, illetve a jelszó megváltoztatásához a GPG Kleopatra modulját, parancssort vagy más windowsos kezelőfelületet kell használni.

Outlook (Windows) - csak 2003 SP2 vagy későbbi vagy 2007 - esetében a GpgOL plug-inre lesz szükség, amelyet a Gpg4win fel fog telepíteni. Az Outlook következő megnyitásakor az Extrák (Extras) / Beállítások (Options) ablakban megjelenik egy GpgOL fül, ahonnan konfigurálni lehet a GPG-t. Az S/MIME támogatást kell választani, és a titkosítást és az üzenetek aláírását alapértelmezésként kell beállítani.

Web alapú levelezés

Amíg meg nem jelenik a Firefox-hoz és Chrome-hoz való PGP/GPG plug-inek első verziója, addig a kizárólag webböngészőn keresztül működtethető szolgáltatásokhoz nem igazán lehet GPG titkosítást használni.

Amennyiben azonban a rendszer engedi a TLS-en keresztüli biztonságos kapcsolatot IMAP és/vagy POP3 protokollal (mint a G-mail és a Hotmail esetében), akkor az összes e-mailes interakció a helyi gépen, szabványos levelezőklienssel (például Thunderbird segítségével) történhet. Ebben a felállásban minden e-mail letöltődik a felhasználó gépre, hogy azok dekódolásra és elolvasásra kerüljenek, majd ez után pedig a felhasználó megírja, titkosítja, majd feltölti és elküldi a választ. A webböngészőből nem lehet elolvasni a titkosított üzeneteket, illetve nem lehetséges igazolni az aláírásokat.

Olyan webes levelezőrendszerek esetében, amelyek ezt a felállást nem teszik lehetővé, esetleg létre lehet hozni egy szűrőt, amely automatikusan átirányítja az e-maileket egy másik fiókra, amely

támogatja a PGP/GPG titkosítást. Ennek a lehetőségnek nincs sok előnye (mivel a kulcsok az e-mail címhez kötődnek). Mivel sok ilyen szolgáltatás a továbbítást is tiltja, javasoljuk, hogy a titkosított levelekhez más szolgáltatást használjon.

Fájlok és fájlrendszerek

A GPG egyedi fájlok vagy egész fájlrendszerek titkosítására is használható.

Minden platform esetében ezt a parancsot kell használni:

gpg -c <filename>

Ezután kétszer be kell írni a jelszót (egyszer meg kell adni, egyszer meg kell erősíteni). A jelszónak nem kell ugyanannak a jelszónak lennie, amely a titkos kulcsokat védi. Nem szabad elveszíteni a jelszót, mert különben nem lehet a fájl tartalmát dekódolni. Végül a fájl nem titkosított változatának törlése szükséges.

A fájl visszafejtése a következő paranccsal történik:

gpg <filename.gpg>

Ezután meg kell adni ugyanazt a jelszót, amelyet a fájl titkosításakor használt.

Windows rendszereken a Windows Intézőben jobb egérgombbal rá kell kattintani egy vagy több fájlnévre, és a felugró menüben ki kell választani az Encrypt (kódolás) parancsot, vagy pedig meg kell nyitni a Kleopatrát, ott a File / Encrypt menüt kell választani, és a párbeszédablakban böngészéssel meg kell keresni az adott fájlokat. A dekódolás (decrypt) szintén ezekben a menükben található.

Amennyiben a felhasználó a teljes merevlemezt szeretné titkosítani, a GPG-vel ez is megoldható, bár a szoftvert elsősorban nem erre a célra találták ki. Javasoljuk, inkább a Truecrypt (www.truecrypt.org) program, illetve Macintoshon a beépített merevlemez-titkosítás használatát.

Bizalmas fájlok titkosítása

A GPG egyik szépsége, hogy egy fájl úgy is titkosítható, hogy csak az általunk megnevezett személy tudja megnyitni és elolvasni. Ehhez a fájlt a címzett nyilvános kulcsával kell titkosítani az alábbi parancs beírásával, ahol a „Bob” szót a címzett e-mail címének egy részletével, a „my-file.txt”-t pedig a titkosítani kívánt fájl nevével kell helyettesíteni:

gpg --recipient <Bob> --encrypt <my-file.txt>

Amennyiben a felhasználó szeretné beilleszteni a teljes fájlt egy egyszerű szöveges e-mailbe, hogy elküldje a címzettnek, akkor a parancsot az ASCII armor opcióval is kell egészíteni:

gpg --recipient Bob --armor --output your-file.asc --encrypt my-file.txt

Bob az alábbi paranccsal tudja visszafejteni a fájlt:

gpg --decrypt <the-file.gpg>

Levelezési listák

A GPG titkosítási rendszer az általános célú, „egy az egyhez” típusú e-mailezést és a levelezési listákat is támogatja. Titkosított levelezési lista futtatásához először telepíteni kell egy GPG-képes listaszervert. A rendelkezésre álló rendszerek között említendő a Schleuder (http://schleuder2.nadir.org/), a GPG-Ezmlm (http://www.synacklabs.net/projects/crypt-ml/) és a RedIRIS. Ezenkívül a GNU Mailman (www.list.org) listaszervert is lehet úgy módosítani, hogy GPG-képes legyen (http://non-gnu.uvt.nl/mailman-pgp-smime/).

Kulcskezelés

Biztonság

Mindig biztonságban kell tartani a titkos kulcsot! A titkos kulcshoz csak az azt használó (és létrehozó) felhasználónak szabad hozzáférnie.

Kulcsgenerálás

Az első kulcspár - egy nyilvános és egy titkos kulcs - generálását az alapértelmezett opciókkal kell elvégezni. Azonban nem árt egy kicsit többet tudni a kulcsok működéséről és a választható lehetőségekről. Ezek megértéséhez hasznos lehet, ha a felhasználó általánosságban rendelkezik ismeretekkel a titkosítás működésével kapcsolatban.

A titkosítási rendszer erősségét - vagyis azt, hogy mennyire nehéz feltörni a kódot - három tényező határozza meg: **1)** mennyire erős a kódolatlan szöveg (cleartext) titkosításához használt algoritmus, illetve módszer; **2)** milyen hosszú a kulcs, amelyet az algoritmus az üzenet titkosításához használ; és **3)** mennyire körültekintően és helyesen működteti a felhasználó a rendszert. A mindennapi életből vett analógiával az algoritmus a zár típusa - például zárbetét vagy lakat -, a kulcs pedig az adott zárba illő kulcs. Feltételezve, hogy feltörésálló algoritmusról van szó - márpedig a GPG által használt algoritmusok eddig ellenálltak a hozzáértők feltörési kísérleteinek -, minél hosszabb a kulcs, annál tovább tart az adott üzenet dekódolása a kulcs megfejtésére irányuló ismételt próbálkozásokkal („nyers erővel”, vagyis az összes lehetőség végigpróbálásával – brute force). Ez a valószínűséggel magyarázható: minél hosszabb a kulcs, annál kevésbé valószínű, hogy brute force támadással, azaz a lehetőségek egymás utáni próbálgatásával meg lehet találni a megfelelőt.

Ennek azonban egy másik oldala is van: minél hosszabb a kulcs, annál több időt vesz igénybe a titkosítás és a dekódolás. A GPG nem engedi a 768 bit-nél rövidebb kulcsok létrehozását. Jelenleg az 2048 bit tűnik ésszerű kompromisszumnak; a biztonságos hosszúság növekedése követni fogja a könnyen hozzáférhető feldolgozó kapacitás növekedését.

Kulcsgeneráláshoz a következő parancsot kell használni (a parancssor megnyitásáról „A GPG használat közben” című fejezetben volt szó):

gpg --gen-key

A GPG különböző választható kulcstípusokat ajánl fel - az alapértelmezést kell elfogadni, amely DSA és ElGamal. Ilyenkor a GPG nemcsak egy, hanem két kulcspárt generál, az egyik az aláírásokhoz használandó elsődleges (vagy mester-) kulcspár, a másik pedig a másodlagos kulcspár vagy alkulcs, amely csak üzenetek és más adatok titkosításához használható. A későbbiekben több alkulcsot is fel lehet venni, ha szükséges.

Az alkulcsok és további felhasználói azonosítók felvételével kapcsolatban a GNU Privacy Guard kézikönyv „Kulcskomponensek felvétele és törlése” című fejezete ad bővebb felvilágosítást.

Kulcscsere

Amikor a felhasználó nyilvános kulcsszerverhez kapcsolódik, hogy feltöltse a kulcsát vagy letöltse és igazolja egy ismerős kulcsát - amit meg kell tennie -, akkor (hkp protokollon keresztül) nem titkosított módon kapcsolódik. Ez kétféle kockázatot hordoz magában: egyrészt a hálózat üzemeltetője figyelni tudja a felhasználó forgalmát, ha meg akarja tudni, hogy kivel szándékozik kommunikálni; másrészt közbeékelődéses (Man-In-The-Middle - MITM) támadással valaki hamis kulcsra cserélheti ki az igazit. Nem árt tudni, hogy ilyen típusú támadások is előfordulhatnak.

Amikor csak lehet, az ujjlenyomatok (fingerprint) összehasonlításával a felhasználó bizonyosodjon meg a felől, hogy a partner igazi kulcsa van a birtokunkban.

Ez akkor is problémát jelent, ha a feltelepített (Enigmailt használó) Thunderbird úgy van beállítva, hogy biztonságos proxyt, például Tor-t (www.torproject.org) használjon. A probléma helyi HTTP proxy, például Polipo (http:www.pps.jussieu.fr/~jch/software/polipo/) használatával is megoldható. Miután letöltésre és telepítésre került, ezt a két sort kell beírni a Thunderbird konfigurációba:

socksParentProxy = "localhost:9050"
socksProxyType = socks5

Ezután a következő opciót kell hozzáadni a GPG parancssorhoz (vagy be kell állítani az Enigmail speciális beállításai között):

--keyserver-options http-proxy=http://localhost:8123

Kulcsok és lejárati dátumok

Amikor a felhasználó a kulcsokat generálja, a GPG beállítja a lejárati dátumot. Ezt fel kell jegyezni és feltétlenül figyelemmel kísérni ezt a dátumot, hogy még időben meg lehessen hosszabbítani vagy újra lehessen generálni a kulcsokat. Nyitni kell tehát egy parancssort és a következő parancsot kell begépelni:

gpg --edit-key <mykey>

Az <mykey> helyébe a kulcs azonosítószámát vagy pedig az e-mail címnek egy részletét kell begépelni. A GPG megkeresi a kulcsot, kilistázza a paramétereit, és egy újabb parancssort nyit meg. Ekkor a következő parancsot kell begépelni:

expire

ezután a rendszer rákérdez az új lejárati dátum részleteire.

Amennyiben a felhasználó lekési a dátumot, és lejárnak a kulcsai, még mindig meghosszabbíthatja őket, de csak egy jóval bonyolultabb eljárással.

A GPG felajánlja azt a beállítást is, hogy a kulcsok soha ne járjanak le.

Ez a beállítás azonban több okból sem ajánlott. Amennyiben közeli lejárati dátumot állít be a felhasználó, az segítséget jelenthet például olyan helyzetben, amikor nem tudja feltölteni a visszavonási tanúsítványt.

Az egyes alkulcsokat egyenként kell megújítani, és az eredeti telepítés óta létrehozott alkulcsoknak is különböző lejárati dátumai lesznek.

A következő példában, amely a GNU Privacy Guard kézikönyvében is szerepel, Chloé-nak két felhasználói azonosítója, egy nyilvános kulcsa és három alkulcsa van. Az elsődleges kulcs és az egyik alkulcs soha nem jár le, a másik két alkulcsnak azonban van lejárati dátuma:

```
chloe% gpg --edit-key chloe@cyb.org
Secret key is available.
pub 1024D/26B6AAE1 created: 1999-06-15 expires: never
trust: -/u
sub 2048g/0CF8CB7A created: 1999-06-15 expires: never
sub 1792G/08224617 created: 1999-06-15 expires: 2002-06-14
sub 960D/B1F423E7 created: 1999-06-15 expires: 2002-06-14
(1) Chloe (Jester) <chloe@cyb.org>
(2) Chloe (plebian) <chloe@tel.net>
Command>
```

Írja be a következő parancsot

toggle

a parancssorba, ha a felhasználó saját titkos kulcsairól szeretne hasonló információkat lekérni.

A kulcsok visszavonása

Amennyiben ellopják vagy a felhasználó elveszíti a számítógépét vagy okostelefonját (vagy bármely egyéb eszközét, például biztonsági másolatokhoz használt lemezét vagy USB stick-jét), amelyen megtalálható a titkos kulcsa, akkor a lehető leghamarabb vissza kell vonni a kulcsot és új kulcsokat

kell generálni. Amennyiben követte a fenti utasításokat és a GPG telepítésekor létrehozott egy visszavonási tanúsítványt, úgy nincs más dolga, mint feltölteni a visszavonási tanúsítványt a nyilvános kulcsszerverre. Amennyiben nem így járt el, akkor a kulcs visszavonásához az alábbi parancsot kell kiadnia, feltéve, hogy még hozzáfér a titkos kulcsához:

gpg --gen-revoke <mykey>

A felhasználó itt megjelölheti a visszavonás okát (például „key compromised”, azaz „kulcs kompromittálódás”), és be kell írnia a jelszavát. A <mykey> helyébe a kulcs azonosítószámát vagy a kulcspár azonosítására szolgáló felhasználói azonosító valamelyik részletét kell beírni.

A felhasználó cserébe kap egy ASCII-armored blokkot, amelyet fel kell töltenie a nyilvános kulcsszerverekre. Amennyiben a felhasználó a telepítés során generál visszavonási tanúsítványt, azt biztos helyen kell tartania - ha szükséges, ki kell nyomtatni, és széfben tárolni -, mivel a visszavonási tanúsítványt bárki közzéteheti, és a kulcsát utána már nem tudja új kommunikációra használni.

A visszavont kulcs a régi kommunikáció visszafejtésére még felhasználható. Azonban a felhasználó részéről az addigi levelezőpartnereit (lehetőleg minél többet) értesíteni kell arról, hogy a kulcsa visszavonásra került, és meg kell adni számukra azt a helyet, ahonnan letölthetik az új nyilvános kulcsot.

A felhasználó őrizze különös gonddal a visszavonási tanúsítványt (mivel azt bárki feltöltheti egy nyilvános kulcsszerverre, és használhatatlanná teheti a kulcsot), és lehetőség szerint ne ugyanazon a helyen tárolja, mint a titkos kulcsot, nehogy egyszerre kerüljenek illetéktelen kézbe. Megfelelő tárolási megoldás lehet a biztonságosan őrzött kinyomtatott dokumentum (mert rövid), a CD vagy az USB-meghajtó. A visszavonási tanúsítványt ki kell törölni annak a gépnek a GPG mappájából, amelyen a kulcs generálódott.

Az alkulcsokat egyenként is vissza lehet vonni a „revkey” paranccsal. Ennek módját és a figyelembe veendő szempontokat a GNU Privacy Guard kézikönyv „Kulcskomponensek visszavonása” című fejezete ismerteti.

A GPG szolgáltatásai

Titkosság

A titkosság biztosítja, hogy csak a címzett olvashatja el az üzenet tartalmát. A GPG a következőképpen biztosítja a titkosságot.

Alice e-mailt ír Bobnak a munkaállomásán. Szintén lokálisan, az Alice munkaállomására telepített GPG egyszer használatos, véletlenszerű szimmetrikus kulcsot generál, amelyet arra használ, hogy egy gyors szimmetrikus kulcsalgoritmus segítségével titkosítsa az üzenetet. A GPG ezután Bob nyilvános kulcsával titkosítja a szimmetrikus kulcsot és hozzáadja az üzenethez. Bonyolultnak

hangzik, de a lényeg a nyilvánoskulcs infrastruktúra (PKI) előnyeinek és a szimmetrikus titkosítás gyorsaságának kombinálása: a folyamat második, titkosítási része sokkal erőforrás igényeseb, de a szimmetrikus kulcs kis mérete miatt jól kezelhető. Amikor Bob megkapja az üzenetet, titkos kulcsával dekódolja a szimmetrikus kulcsot, majd a szimmetrikus kulccsal dekódolja a üzenet törzsét. Mivel a titkosítás és a dekódolás teljes egészében lokálisan történik a küldő és a fogadó számítógépen, nincs szükség közvetítőre az üzenet vagy a kulcs titkosságának megőrzéséhez (így közbeékelődéses - man-in-the-middle - támadás sem fordulhat elő).

Hitelesítés

A hitelesítés az a funkció, amellyel Alice igazolni tudja, hogy a Bob-tól jövő e-mailek valóban Bob-tól származnak, függetlenül attól, hogy Alice ismeri-e Bob igazi kilétét a való életben. Meg kell jegyezni, hogy a GPG semmilyen módon nem köt egy adott kulcsot egy ténylegesen létező entitáshoz; csak azt tudja igazolni, hogy minden e-mailt ugyanazzal a titkos kulccsal titkosítottak, amely feltételezhetően ugyanahhoz a személyhez tartozik. A GPG-ben a hitelesítés a következőképpen történik.

Bob összeállítja az Alice-nek szánt üzenetet, és egyirányú titkosítási függvénnyel létrehozza az üzenet „hash” (lásd a fogalomtárat) értékét, illetve kivonatát (digest). Ezt követően a titkos kulcsával titkosítja a hash értéket. Alice (vagy bárki más) úgy tudja igazolni Bob aláírását, hogy a feladó nyilvános kulcsával visszafejti a hash értéket, majd az e-mail tartalmának ugyanazon az egyirányú matematikai függvényen való átfuttatásával egy második hash-t hoz létre, majd összehasonlítja a kettőt. A hash-ek egyezése esetén Alice biztos lehet abban, hogy Bob pontosan azt az üzenetet küldte, mivel Bob nyilvános kulcsa vissza tudta fejteni a hash értéket, és a hash érték bizonyítja, hogy az aláírás az adott üzenethez tartozik.

Azonosítás

Az azonosítás azt jelenti, hogy igazolni lehet, miszerint egy adott e-mail címre küldött, illetve onnan érkező üzenetek egy meghatározott, azonosítható, a való életben is létező emberhez jutnak el, illetve tőle származnak. Az azonosítás a GPG-ben két eljárás valamelyikével történik.

Az egyik a nyilvános kulcsok aláírásának gyakorlatával megteremtett bizalmi háló (web of trust). Amennyiben elegendő számú ember ír alá egy adott nyilvános kulcsot, akkor az adott nyilvános kulcs és az adott e-mail cím összetartozása igen erős lesz. Ez úgy teremthető meg, hogy Alice feltölti nyilvános kulcsát egy nyilvános kulcsszerverre, és időt és gondot fordít arra, hogy kiépítse maga körül a bizalmi hálót, mégpedig úgy, hogy minél több ember számára igazolja személyazonosságát, és kriptográfiailag - Alice nyilvános kulcsának aláírásával - igazoltatja velük. Célravezető lehet, hogy a szervezetek tagjai találkozóik alkalmával ragadják meg a lehetőséget egymás kulcsainak igazolására és aláírására.

A másik módszer, hogy Alice és Bob személyesen találkoznak, és betekintenek egymás azonosító dokumentumaiba, majd a GPG titkosítási rendszerrel igazolják, hogy a másik birtokában van a titkos kulcsnak, amely kriptográfiailag egyezik az adott e-mail címhez tartozó nyilvános kulccsal.

Sértetlenség

A sértetlenség (integritás) azt jelenti, hogy igazolni lehet, miszerint a feladótól származó, nem titkosított e-mail tartalmát útközben senki nem módosította. A sértetlenség a GPG-ben a hitelesítésnél megismert eljárással biztosítható, amely egyidejűleg azt is bizonyítja, hogy az üzenet tartalmát, azaz az egyirányú matematikai hash függvény bemenetét, útközben nem lehetett módosítani. Ellenkező esetben a két hash nem egyezne.

Letagadhatatlanság

A letagadhatatlanság azt jelenti, hogy a feladó később nem tagadhatja le, hogy ő írta az üzenetet, illetve nem tagadhatja le az üzenetben tett nyilatkozatát vagy ígéretét. A GPG a következő eljárással biztosítja a letagadhatatlanságot.

Alice bizonygatja, hogy nem ő küldte azt az üzenetet, amelyről Bob azt hiszi, hogy Alice-től jött. Bob igazolja az üzenet aláírását Alice nyilvános kulcsával, és ellenőrzi, hogy a nyilvános kulcs érvényes-e az adott üzenetre. Amennyiben mindkét feltétel teljesül, akkor az üzenet csak Alice-től származhat, hiszen csak ő tudta az adott titkos/nyilvános kulcspárral megfelelően aláírni az adott e-mail címről jövő üzenetet.

Bizalom

A nyilvánoskulcs infrastruktúra (PKI), amelyet a GPG titkosítási rendszert használó személyek hoznak létre, azzal teremti meg a bizalmat, hogy harmadik személyek számára egyértelművé teszi, hogy a rendszeren belül egy vagy több személy megbízik egy másik személyben. A következőkben elmagyarázzuk, miként épül fel a bizalmi háló a GPG-ben.

Ha Alice megbízik Bob-ban, Carol pedig megbízik Alice-ben, akkor Alice át tudja ruházni bizalmát Bob-ra, így átvitt értelemben Carol is megbízhat Bob-ban. A folyamat akkor indul el, amikor Bob feltölti nyilvános kulcsát egy nyilvános kulcsszerverre. Alice először igazolja Bob személyazonosságát. Alice ezt úgy teheti meg, hogy személyesen találkozik Bobbal, és ellenőrzi Bob személyazonosító okmányait, az igazolás azonban sokszor azon alapul, hogy a két személy régóta ismeri egymást. Alice ezután titkos kulcsával aláírja Bob nyilvános kulcsát, majd az aláírt kulcsot feltölti egy kulcsszerverre. Mostantól bárki, aki ellenőrizni akarja, bizonyítani tudja - Alice nyilvános GPG kulcsával -, hogy Alice aláírta Bob nyilvános kulcsát, ami annak jele, hogy Alice megbízik Bob-ban.

Ahhoz, hogy Carol arra a következtetésre jusson, hogy Bob valószínűleg az, akinek mondja magát, és olyan személy, akiben megbízhat, Bob-nak fel kellett töltenie nyilvános kulcsát egy nyilvános kulcsszerverre, majd időt és gondot kellett fordítania arra, hogy kiépítse a nyilvános kulcsa körülötti bizalmi hálót, azaz másokkal aláíratta és a kulcsszerverre visszatöltette a nyilvános kulcsát. Carol közvetlenül a GPG titkosítási rendszerből is bizonyos mértékig következtethet arra, hogy Bob megbízható, még mielőtt Bob bármit is írna neki egy üzenetben: Carol átnézheti azok listáját, akik az illető nyilvános kulcsának aláírásával jelezték, hogy megbíznak benne. Carol igazolni tudja az illetőbe vetett bizalom hitelességét, azonban még el kell döntenie, hogy ezek a kapcsolatok elegendőek-e ahhoz, hogy meggyőzzék arról, hogy Bob valóban az, akinek mondja magát. Ez nem

csupán darabszám kérdése; Carol döntése, hogy megbízhat-e Bob-ban vagy sem, nagyrészt attól is függ, hogy kik azok a személyek, akik Bob kulcsát aláírták. Ez sok esetben személyes döntés; Carol e helyett vagy kiegészítésképpen a GPG titkosítási rendszerbe épített bizalmi értékeket is használhatja annak számszerűsítésére, hogy a rendszer milyen mértékben hiszi el, hogy Bob valóban az, akinek mondja magát.

KRIPTOGRÁFIAI TULAJDONSÁG	TITKOSÍTÁS / VISSZAFEJTÉS	ALÁÍRÁS / IGAZOLÁS	NYILVÁNOS SZERVER
HITELESÍTÉS	-	IGEN	-
SÉRTETLENSÉG	-	IGEN	-
LETAGADHATATLANSÁG	-	IGEN	-
TITKOSSÁG	IGEN	-	-
BIZALOM ÁTRUHÁZÁSA	IGEN*	IGEN	IGEN
MEGBÍZHATÓSÁGRA KÖVETKEZTETÉS	IGEN*	IGEN	IGEN

** Nem feltétlenül fontos titkosítást használni, amikor aláírjuk valaki nyilvános kulcsát, illetve nem feltétlenül kell kommunikálnunk valakivel, azonban ezekkel a lépésekkel meggyőződhetünk róla, hogy az e-mail fiók felett rendelkező személy ugyanaz a személy-e, akinek az e-mail címhez tartozó GPG titkos kulcs védelmét szolgáló jelmondat a birtokában van.*

Biztonsági házirendek

E-mail

Az emberek szerint az e-mail arra szolgál, hogy magánbeszélgetéseket folytassanak egy vagy több másik személlyel. Mégis a felhasználók nagyon ritkán tesznek lépéseket az e-mailek titkosságának megerősítése érdekében, és a GPG-vel kapcsolatban általában az az első kérdésük, hogy „Miért kéne titkosítani az e-maileket?”.

A helyzet az, hogy az e-mail, ahogy ma használják, a képeslap digitális megfelelője. Az 1990-es évek elejétől sok biztonsági szakértő gondolja úgy, hogy az internetes közösségnek alapbeállításként kellene használnia a titkosítást; az e-mail üzenetek titkosításakor virtuálisan ugyanazt tesszük, mint amikor a papírra írt leveleket borítékba zárjuk.

Sok felhasználó számára az e-mail protokollok működése egyszerűen megérthető: a feladó kliense kapcsolódik a kimenő SMTP (egyszerű levélátviteli protokoll) szerveréhez, ez a szerver közvetlenül kapcsolódik a címzett bejövő levelező szerveréhez, és a címzett kliense közvetlenül ugyanehhez a bejövő levelező szerverhez kapcsolódik. Ez ugye csak három kapcsolódás, és mindegyik közvetlen kapcsolódás? Tévedés. A helyzet valójában az, hogy a három átvitel lebonyolítása érdekében a levélforgalmat általában úgy irányítják, hogy az talán egy tucatnyi vagy még annál is több számítógépen keresztülmegy. Bárki, aki e számítógépek bármelyikéhez adminisztrátori hozzáféréssel rendelkezik, elolvashatja az átmenő e-maileket - amíg az e-mail üzeneteket kódolatlan

formában továbbítják, márpedig általában ez a helyzet. A titkosítás biztosítja, hogy az üzenetek tartalmát akkor se lehessen elolvasni, ha a több tucat adminisztrátor közül valaki elfogja az üzeneteket. A biztonsági szakértők általános véleménye, hogy a titkosításnak már több éve *de facto* szabvánnyá kellett volna válnia. Mivel ez nem történt meg, a felhasználóknak nemcsak saját és szervezete érdekében, hanem a összes internethasználó érdekében is segítenie kell abban, hogy azzá válhasson.

BCC

A BCC („blind carbon copy") a titkos másolatot jelenti, vagyis hogy úgy lehet elküldeni az e-mail üzenet másolatát valakinek, hogy a többi címzett nem tud róla.

A BCC mezőt kizárólag akkor kell használni, ha körözvényszerű e-mailt küldünk sok ember számára. Ebben a szituációban ha BCC használatára kerül sor egyszerű CC („carbon copy"), azaz „Másolatot kap" helyett, az egyes címzettek inkognitóban maradhatnak a listán szereplő többi személy előtt és mindazok előtt, akik hozzáférhetnek a levelezési lista archívumához. Nyilvános listák esetében biztosítani kell, hogy a listatagok ne kerüljenek fel a spam listákra.

Egyéb helyzetekben nem illendő használni a BCC mezőt, különösen akkor nem, ha a beszélgetést titkosítással védik. Egy e-mail beszélgetéslánc résztvevői feltételezik, hogy az e-mailt transzparensen, kizárólag a látható, kifejezetten feltüntetett címzettek számára küldik. Ez különösen igaz a titkosított beszélgetésláncokra, hiszen a beszélgetéslánc titkosítása azt a nyomatékos üzenetet küldi, hogy a beszélgetés csak ismert címzetteknek szól, és az e-maileket mindenki más előtt rejtve kell tartani. Amennyiben valaki más BCC-be kerül, úgy előtte is ismertté válik az, aminek szigorúan magánbeszélgetésnek kellene lennie, továbbá meghiúsul a transzparencia elve, és elveszíthetővé válik a beszélgetésláncban részt vevő többi fél bizalma (ha a résztvevők megtudják - például a BCC-zett személy válaszol a beszélgetésláncra -, megromolhat velük a kapcsolat).

A tájékozottság növelése - a GPG ujjlenyomat használata

Mivel a teljes nyilvános kulcs ormótlanul nézne ki e-mail aláírásként vagy egy névjegyen, a GPG-nek egy olyan funkciója is van, amellyel kompaktabb változatot, úgynevezett „ujjlenyomat"-ot lehet generálni. GPG ujjlenyomat generálásához a parancssori utasításokkal el kell menni abba a könyvtárba, ahol a GPG telepítve van, és a következő parancsot kell kiadni:

gpg --fingerprint <keyID>

és a <keyID> helyébe be kell írni a kulcs számát vagy pedig az ahhoz tartozó e-mail cím egy részletét.
Ajánlott minél többször használni az ujjlenyomatot: feltüntetni a névkártyán, és használni szokásos aláírásként a nem titkosított e-mailekben. Ily módon jobban tudatosítható azokban, akikkel a felhasználó érintkezik, hogy a GPG fontos dolog és elérhető, és elősegítheti a szélesebb körben való elterjedését. A névkártyán szereplő ujjlenyomat is segítséget jelenthet a kulcs aláírásában.

A titkosítás használata

Bizalmas információk

Mindig titkosítani kell az e-mailben küldött bizalmas információkat! Amennyiben az üzenet címzettjei közül még nem mindenki telepített fel PGP/GPG-t, biztatni kell őket, hogy tegyék meg, és segíteni nekik a folyamatban.

Titkosítás kérése

Amennyiben valaki kódolatlanul küld a felhasználó számára bizalmas információkat, udvariasan meg kell kérni, hogy a későbbiekben minden információt titkosítva küldjön. Amennyiben nem tudja hogyan kell, segíteni kell neki a folyamatban.

Beszélgetéslánc titkosítása

Amennyiben a felhasználó több levelezőpartnere is részt vesz egy hosszabb e-mail megbeszélésben, mindegyiküknek ügyelnie kell arra, hogy minden résztvevő számára titkosítva küldjék a továbbításokat és a válaszokat.

Csatolmányok

Ügyelni kell arra, hogy a titkosított e-mailekhez csatolt mellékletek is titkosítva legyenek.

Ezt kétféleképpen lehet megtenni. Egyik lehetőség: a fájlt az e-mailhez csatolni, utána a GPG MIME használatával titkosítani az egész e-mailt, a csatolmányt és minden mást. Másik lehetőség: először titkosítani önmagában a fájlt a parancssorból vagy egy GPG segédprogramból, utána csatolni az e-mailhez, és titkosítani az e-mail törzsét (amennyiben az e-mail nem tartalmaz bizalmas információt, akkor kódolatlanul is el lehet küldeni az e-mail törzsét, azonban célszerű rutinszerűen titkosítani minden e-mailt). Az elsőként említett lehetőséget nem minden e-mail kliens támogatja, és az a legvalószínűbb, hogy a gyakorlatban a második lehetőséget fogja használni a felhasználó.

Tárgysor

A GPG nem titkosítja a forgalmi adatokat (lásd alább), amelyek a feladó és a címzett adatait és az e-mail tárgysorát tartalmazzák. A tárgysort különös gonddal kell megszövegezni, hogy ne áruljon el semmilyen bizalmas információt az e-mail tartalmáról, de mégis felkeltse a címzett figyelmét.

Forgalmi adatok

Egy adott üzenet tartalma sokszor kevésbé árulkodó, mint magának az üzenetnek az adatai (metaadatok): ki küldte, ki kapta meg, mikor, hol, és a levelezőpartnerek milyen gyakran kommunikálnak egymással. Az ilyen típusú adatokat, amelyek általában az e-mail üzenetek fejlécében (valamint az internetszolgáltatók és a felhasználók által látogatott más címek szolgáltatóinak naplóiban) szerepelnek, „forgalmi adatok”-nak is szokták nevezni, és sok országban,

de leginkább az EU-ban törvények szabályozzák, hogy ezeket az adatokat bűnüldözési célból és biztonsági okokból több hónaptól akár több évig terjedő ideig meg kell őrizni.

Egy elgondolkodtató üzenet: Vegyél paradicsomot.

Egy ilyen üzenet jelentőségét nem lehet megítélni, ha semmilyen információ nem áll rendelkezésre a levelezőpartnerek viszonyáról. Amennyiben naponta több tucatszor kommunikálnak egymással, valószínűleg házastársakról van szó. Amennyiben az egyik egy tömegrendezvényeken felbukkanó hírhedt bajkeverő, akkor valószínűleg a következő eseményre „fegyverkeznek fel". Amennyiben egy élelmiszer áruház vezetői, akkor az üzenet bizalmas üzleti információkat is tartalmazhat.

Célszerű figyelembe venni tehát, hogy bár a GPG védi az üzenet tartalmát, a forgalmi adatok védelméről egyáltalán nem gondoskodik. A forgalmi adatok védelméhez és az anonimitás megőrzéséhez olyan eszközre van szükség, mint például a Tor (http://www.torproject.org), amelyet kifejezetten erre a célra fejlesztettek ki.

Letöltések ellenőrzése

Sok weboldal elérhetővé tesz egy olyan hash-t, amellyel ellenőrizni lehet, hogy a letöltött fájlokat nem módosították-e illetéktelenül (például úgy, hogy kémprogramot vagy más kártékony szoftvert csempésztek bele).

Minden platform esetében ezt a parancsot kell beírni a parancssorba:

gpg --verify <filename>

A GPG összehasonlítja az aláírásokat, és jelentést készít arról, hogy egyeznek-e.

Windows alatt két másik választási lehetőség is van. A Windows Intézőben jobb gombbal rá kell kattintani a fájlnévre, és a felugró menüben a GpgEX / Verify parancsot kell választani, illetve meg kell nyitni a Kleopatrát, és a File menüben a Decrypt / Verify parancsot kell választani. Mindkét esetben ugyanaz a grafikus felület jelenik meg; a megfelelő négyzetek bejelölése után a Decrypt/Verify parancsra kattintva lehet továbblépni. A következő képernyő közölni fogja, hogy az aláírások megegyeznek-e.

A letöltések ellenőrzésével kapcsolatban további információk találhatók GnuPG sértetlenség-ellenőrzésről szóló oldalán: http://www.gnupg.org/download/integrity_check.html.

Kulcskezelés, aláírás és biztonság

Hitelesítés

Mindig alá kell írni az üzeneteket, amikor a címzettnek fontos tudnia, hogy az információ a kitől származik.

Sértetlenség, URL linkek és e-mail mellékletek

Alá kell írni az üzenetet, amennyiben fontos, hogy bizonyítható legyen az, hogy az üzenetben lévő információt útközben nem módosították. Ilyen helyzet többek között akkor fordulhat elő, ha olyan e-maileket küld a felhasználó, amelyekben külső forrásokra mutató URL-ek vannak, vagy amelyekhez mellékletek vannak csatolva.

URL-ek esetében fontos megbizonyosodni a felől, hogy útközben nem módosították-e, azaz nem cserélték-e ki egy rosszindulatú helyre vezető linkre.

A csatolmányok alkalmazása azért kockázatos, mert azt harmadik fél olyan csatolmányra cserélheti ki az üzenet továbbítása közben, amely kártékony kódot tartalmaz. Ez titkosított csatolmányok esetében is igaz, hiszen a rosszindulatú harmadik felet semmi nem akadályozza abban, hogy a helyettesítő csatolmányt a címzett nyilvános kulcsával titkosítsa. A feladónak tehát alá kell írnia a csatolmányt, és az aláírást is csatolnia kell az e-mailhez, vagy pedig az e-mailt és a csatolmányt összecsomagolja MIME-mal, majd az egész becsomagolt levelet aláírja.

Letagadhatatlanság

amennyiben fontos az, hogy egy e-mailben tett ígéretet a későbbiekben ne lehessen visszavonni, meg kell kérni a feladót, hogy a kérdéses üzenetet GPG-vel írja alá.

Bizalmi hálózat

Az azonosság igazolása

Amennyiben a felhasználó olyan valakivel találkozik, aki tudvalevőleg PGP/GPG-t használ, meg kell ragadnia a lehetőséget, és a GPG bizalmi hálójának szélesítése céljából a megbeszélés napirendi pontjai közé felvenni a személyazonosság igazolását és a kulcsaláírást. A régóta szoros kapcsolatban álló embereknek - függetlenül attól, hogy személyesen tudnak-e találkozni vagy sem -, szintén érdemes aláírniuk egymás kulcsait, hiszen az ő esetükben nincs szükség fizikai jelenlétre egymás személyazonosságának igazolásához.

Bizalomértékelés

Az is növelheti a bizalmi háló értékét, ha kulcsaláíráskor a felhasználó értékeli, hogy mennyire bízik meg azokban a személyekben, akiknek a kulcsát aláírja. Az értékelésnek nemcsak azt kell tükröznie, hogy a felhasználó meg van győződve arról, hogy a másik az, akinek mondja magát, hanem azt is, hogy általánosságban mennyire bízik meg bennük. A GPG-ben erre is van egy mechanizmus. Elő kell hívni a GPG kulcsszerkesztőjét az alábbi paranccsal:

gpg -key-edit <keyID>

A **<keyID>** helyébe annak az e-mail címnek egy részletét kell beírni, amelyhez az a kulcs tartozik, amelynek a megbízhatósági szintjét kell szerkeszteni.

A parancssorba a következő parancsot kell begépelni:

trust

A GPG egy menüt ajánl fel, amelyből módosítani lehet az érintett személy megbízhatósági szintjét.

A saját „kulcscsomó” kibővítése

Rutinszerűen ellenőrizni kell, hogy az új partnernek van-e az e-mail címükhöz kapcsolódó PGP/GPG kulcsa. Amennyiben a partnernek van érvényes nyilvános kulcsa, későbbi felhasználás céljából hozzá kell adni személyes „kulcscsomóhoz”.

A bizalom ellenőrzése

Amennyiben első alkalommal kommunikál a felhasználó egy olyan személlyel, aki GPG titkosítási rendszert használ, mindig ellenőrizni kell az illetőbe vetett bizalmat. A bizalmi háló akkor hasznos, ha használják.

A nyilvános kulcsú titkosításról

A nyilvános kulcsú titkosítás az idegenek közti spontán kommunikáció biztonságosságát célzó bevált módszer. Bár ugyanezt az elméletet az 1970-es évek közepén a brit GCHQ is titokban kidolgozta, a találmányt általában Whitfield Diffie, Martin Hellman és Ralph Merkle nevéhez kötik, akik 1976-ban tették közzé először a módszer leírását. 1978-ban Ron Rivest, Adi Shamir és Leonard Adleman RSA néven közzétette az első olyan algoritmust, amely az aláírást és a titkosítást egyaránt támogatta. Az RSA Data Security céget, amely jelenleg az EMC egyik divíziója, az RSA algoritmus kereskedelmi hasznosítása céljából hozták létre. A PGP az RSA egy korai megvalósítása volt, bár a PGP és a GPG más algoritmusokat is támogat.

A nyilvános kulcsú titkosítás nem egyedi („szimmetrikus”) kulcson, hanem két egymást kiegészítő kulcs (kulcspár) használatán alapul. A kulcspár bármelyik tagja vissza tudja fejteni a másik kulccsal titkosított anyagokat; mindegyik tud úgy titkosítani anyagokat, hogy azt csak a másik kulccsal lehessen dekódolni. Az egyik kulcs titokban marad, és azt csak a tulajdonosa ismeri. A másik kulcs nyilvános, és a lehető legszélesebb körben terjesztve van.

Ebben a rendszerben ha Bob szeretne olyan információt küldeni Alice-nek, amelyet csak Alice tud elolvasni, akkor Bob az üzenetet Alice nyilvános kulcsával titkosítja (amelyet egy kulcsszerverről tud letölteni vagy akár egy könyvből is ki tud másolni); Alice a titkos kulcsával tudja dekódolni és elolvasni az üzenetet. Hasonlóképpen, ha Alice szeretné bebizonyítani Bob-nak, hogy megírt egy adott üzenetet, akkor ha az üzenetet a saját titkos kulcsával titkosítja, és a saját nyilvános kulcsával dekódolja, ez bizonyítékul szolgál Bob számára, hogy Alice volt az üzenet szerzője. E struktúra alapján sokféle variációt lehet különböző helyzetekre alkalmazni: Bob például egyszerre használhatja saját titkos kulcsát és Alice nyilvános kulcsát az üzenet titkosításához, hogy az üzenet tőle származó üzenetként legyen hitelesítve, és csak Alice tudja elolvasni.

Az RSA algoritmust 1978-ban szabadalmaztatták, de a rendszer magánszemélyek általi mindennapos használata csak az 1990-es évek első felében vetődött fel reális lehetőségként, amikor a számítástechnikai feldolgozó kapacitás már elég olcsó és elterjedt volt. Az 1990-es évek első felében sok politikai vita zajlott a digitális jogokért harcoló szervezetek és a titkosítást katonai fegyvernek tartó kormányok között. A kormánypolitikusok olyan elképzeléseket támogattak, mint például a kulcsletét (tehát hogy a magánszemélyeknek egy kormányadatbázisban kellett volna elhelyezniük a titkos kulcsuk másolatát), valamint a behozatali/kiviteli korlátozások, amit azzal indokoltak, hogy az erős titkosítás elterjedése megnehezítené a bűnüldöző szervek és a biztonsági szolgálatok arra irányuló erőfeszítéseit, hogy megvédjék a közösséget a szervezett bűnözéstől és más veszélyektől. Az elektronikus kereskedelem terjedésével azonban az erős titkosítás békeidőkben való használata túl nagy jelentőséget kapott ahhoz, hogy továbbra is ragaszkodjanak ehhez a politikához, és a legtöbb országban megszüntették ez említett korlátozásokat.

A web bizalmi hálója

Mindennapjainkban úgy használjuk a bizalmi hálókat, hogy tudatosan nem is gondolunk rájuk. Meghatározott viszonteladótól veszünk autót, mert egy barátunk őt ajánlotta. Friss ételt rendelünk egy olyan étteremben, amit soha nem láttunk vagy amiről soha nem hallottunk, mert bízunk abban, hogy az egészségügyi hatóságok megvizsgálták a csirkét. Általánosabb értelemben feltételezzük, hogy aki boltot nyit, az bérleti szerződést kötött egy bérbeadóval, és felelősségre vonható a rendőrség részéről, ha megalapozott teszünk panaszt teszünk az áruval kapcsolatban, amit eladott nekünk.

A bizalmi háló olyan mechanizmus, amely lehetővé teszi, hogy idegenek is megbízzanak egymásban, mert bizonyítékot tud szolgáltatni arra, hogy mások is bíznak bennük. A digitális világban például az eBay is egy bizalmi hálózat, amely a visszajelzések osztályozásával lehetővé teszi, hogy a felhasználók bizalmat szavazzanak egymásnak a soha nem látott nagyszámú ismeretlennel való kereskedés alapján. Amennyiben a felhasználó meglátja egy olyan eBay felhasználó összesített pontszámát, aki sok sikeres tranzakciót bonyolított le, és folyamatosan magas pontszámokat kap, akkor nagyfokú bizalmat érezhet iránta, és úgy gondolja, hogy biztonságos üzletet köthet vele.

Ez az egyszerű magyarázat elrejti a tényt, hogy még a fizikai világban is sokszor árnyaltabb a kép. Egy használtautó kereskedőnek lehet olyan híre, hogy „becsapja” az embereket, de ez alapján nem teljesen egyértelmű, hogy valóban törvényt szeg-e, vagy csak ügyesen végzi a munkáját, és olyan dolgot is el tud adni, ami végül nem felel meg az igényeinknek. A bizalmi háló ezeken a árnyaltabb területeken érvényesül igazán.

A bizalmi hálózatok csak akkor működnek, ha az alapul szolgáló mechanizmusokat is bizalom övezi. A felhasználónak biztosnak kell lennie abban, hogy a személy, akivel dolga van, pontosan azonosítható. Ez azt is jelenti, hogy az illető, miután kötelezettséget vállalt egy üzenetben vagy egy tranzakcióban, később nem tagadhatja le, hogy részt vett benne. Egy olyan rendszer, mint például az eBay, biztonságos és zárt környezet, és olyan cég tulajdonában van, amely általában jóindulatú a felhasználókkal szemben. Azonban az internet általában véve egy nyitott közösség, és ebben az értelemben más mechanizmusokra kell hagyatkoznunk, ha ugyanilyen fokú bizalmat szeretnénk kiépíteni.

Nyilvános kulcsú titkosítással nyitott közösségekben is megteremthető a bizalmi háló. A nyilvános kulcsú titkosítás úgy van megalkotva, hogy a résztvevők digitálisan aláírhassák a kommunikációjukat és a tranzakcióikat, és ebből következően akkor is biztosak lehessenek abban, hogy XY valóban XY, ha semmilyen módon nem tudják XY-t egy tényleges személyhez társítani. A kriptográfiai aláírás biztosítja a letagadhatatlanságot, tehát a résztvevő nem tagadhatja le, hogy létrehozott egy üzenetet vagy tranzakciót, ha az adott tranzakción lévő aláírás megegyezik az ő aláírásával. A PGP (Pretty Good Privacy) és GPG (GNU Privacy Guard) e-mail titkosító rendszer elősegíti a nyitott közösségek bizalmi hálóinak kiépítését.

A GPG-ről

A GNU Privacy Guard (GPG) egy nyilvános kulcsú titkosításra szolgáló ingyenes, nyílt forráskódú szoftveralkalmazás, amelyet a Free Software Foundation GNU szoftverprojektje keretében fejlesztettek ki és terjesztenek. A PGP („Pretty Good Privacy”) kriptográfiai szoftvercsomag egyik alternatívája. A GPG megfelel az RFC 4880-nak, amely az OpenPGP-re vonatkozó IETF-szabvány specifikációját tartalmazza, és együttműködik a PGP-vel és más OpenPGP-kompatibilis rendszerekkel. A GPG első változata 1999 szeptemberében jelent meg.

A sebesség és hatékonyság érdekében a GPG nemcsak nyilvános kulcsú titkosítást, hanem egy sor más kriptográfiai mechanizmust, többek között például szimmetrikus kulcsokat és hash függvényeket is használ. Ez a sokoldalú megközelítés rugalmas titkosítási rendszert eredményez, amely különféle célokra használható. Elsősorban az e-mailek védelmét szolgálja, de levelezési listák, kiválasztott fájlok és teljes fájlrendszerek, valamint másfajta protokollokon keresztüli kommunikáció (például a Jabber és hasonló népszerű kliensek plugin-eken keresztüli azonnali üzeneteinek) védelmére is használható.

Egy titkosító szoftver rejtjelelemzéssel szembeni ellenálló képességére az a legfontosabb garancia, hogy alávetik a kriptográfiai közösség szigorú és alapos vizsgálatának. A PGP és a GPG eddig (20, illetve 12 éve) sikeresen állja a próbát, erősnek és biztonságosnak tekinthető.

További források

GNU Privacy Guard Kézikönyv:
Gpg4win Compendium (PDF): http://wald.intevation.org/frs/download.php/775/gpg4win-compendium-en-3.0.0-beta1.pdf

Fogalomtár

Hash függvény: A kriptográfiai hash (zagyvalék) vagy digest egy egyirányú matematikai függvény, amely adatblokkból fix bithosszúságú karakterláncot hoz létre. Annak bizonyítására használják, hogy egy üzenet tartalma nem változott meg, ugyanis az üzeneten végrehajtott legapróbb változás is gyakran egészen drámai módon megváltoztatja a hash-t; az üzenetet nem lehet rekonstruálni a hash-ből; és két eltérő üzenetből sem generálható egyforma hash. Jól ismert hash függvények: MD4, MD5, SHA-1 és SHA-2.

Kulcsszerver: A kulcsszerver a nyilvános kulcsok másolatait tárolja, hogy innen bárki letölthessen, és olyan üzenetek hitelesítésére használja fel, amelyek láthatólag egy meghatározott személytől származnak. Új kulcspár generálásakor fel kell tölteni a nyilvános kulcsot, és frissíteni kell, amikor aláírásra kerül azokkal a személyekkel, akik igazolni tudják a felhasználó személyazonosságát, és szorosabban kapcsolatba tudják hozni a nyilvános kulcsával.

Letagadhatatlanság: A nyilvános kulcsú titkosítás egyik fontos jellemzője, hogy ha egy üzenetet egy adott személy a titkos kulcsával aláírt (ami abból tudható, hogy az üzenetet az adott személy nyilvános kulcsával vissza lehet fejteni), akkor az illető később nem tagadhatja le, hogy az üzenet tőle származik.

PKI (nyilvánoskulcs infrastruktúra): Kulcsszerverek és tanúsítványok ökoszisztémája, amely a nyilvános kulcsokat gondozza és hitelesíti.

Nyilvános kulcsú titkosítás: 1976-ban, az olcsó számítógépek és a számítógépes hálózatok megjelenésével egyértelmű igény mutatkozott egy olyan technika iránt, amely biztosítja az idegenek közötti biztonságos spontán kommunikációt. A megoldás, amelyet hivatalosan Whitfield Diffie, Martin Hellman és Ralph Merkle nevéhez kötnek, de tőlük függetlenül a brit GCHQ önállóan is feltalált, az egyedi szimmetrikus kulcs helyett egy egyszerre generált kulcspárt használ, amelyben az egyik kulcs titkos marad, a másik pedig nyilvános (és a lehető legszélesebb körben publikált).

Aláírás: A nyilvános kulcsú titkosításban az e-mail üzenet aláírása hitelesíti az üzenetet és egyértelműen azonosítja a feladót. Az aláírás előállítása egyirányú kriptográfiai függvénnyel történik, amely létrehozza az üzenet digitális hash-ét, és a feladó titkos kulcsával titkosítja a hash-t. Amennyiben az üzenet aláírása ezzel a módszerrel történik, a címzett a feladó nyilvános kulcsával (amely bizonyítja a feladó személyazonosságát) dekódolni tudja az üzenetet, majd lefuttatja ugyanazt a kriptográfiai függvényt az üzeneten, hogy egy másik hash-t generáljon, és azt összehasonlítsa a dekódolt hash-el (annak bizonyítására, hogy az üzeneten nem történt módosítás).

Szimmetrikus kulcsú titkosítás: A titkosítás 1980-as évekig meghatározó formája, a szimmetrikus kulcsú titkosítás ugyanazt az egy kulcsot használja a kommunikáció titkosítására és visszafejtésére. A módszer hátránya, hogy ha két idegen szeretne biztonságosan kommunikálni egymással, akkor először át kell adniuk a másiknak a kulcs másolatát. A GPG-ben a gyorsaság miatt a teljes üzeneteket titkosító egyszer használatos kulcsok (session keys) szimmetrikusak, a nyilvános/titkos kulcspárt pedig az egyszer használatos kulcsok kicserélésére és aláírás céljára használják.

Bizalmi háló: A nyilvános kulcsú titkosítás feltalálásáig a bizalom főként hierarchikus volt, és a hatóságokon alapult. Egy bank például kibocsáthatott akkreditívet (letter of credit), amelyet egy idegen a megbízhatósága jeléül bemutathatott a jövőbeli külföldi üzleti partnereinek. A GPG ehelyett inkább a „hat lépés” elméletre támaszkodik, és azt feltételezi, hogy az emberek megbíznak azokban, akiket ismernek. Tehát amikor a felhasználó nyilvános kulcsot generál, meg kell kérnie azokat az embereket, akiket ismer, vagy akikkel igazolni tudja mind a személyazonosságát, mind pedig a magát a kulcsát, hogy írják alá a kulcsot. Ahogy egyre többen írják alá a kulcsot, annál megbízhatóbbá válik a kulcs az egész hálózat számára, részben a számok miatt (ahogy az eBay

hírneve is nő), részben pedig azért, mert a kulcsot aláíró emberek közül egyesek személyes vagy szakmai kapcsolatba kerülnek azokkal, akik a kulcsot használni szeretnék. Az így kialakuló bizalmi láncolat a világhálóhoz hasonlóan lassanként hálózattá, bizalmi hálóvá terebélyesedik.

Részletes telepítési útmutató platformonként

Windows

A Gpg4win telepítőcsomagban található modulokkal különböző e-mail kliensekbe lehet integrálni a GPG-t. A dokumentum további része a Thunderbird-re és az Outlook-ra koncentrál, mert ez a két levelező kliens az egyik legterjedtebb.

A Gpg4win telepítése

Le kell tölteni a Gpg4win programot a http://www.gpg4win.org/download.html oldalról, és elmenteni el egy olyan helyre, ahol könnyen megtalálható.

Futtatni kell a fájl, így a letöltött fájlra duplán kell kattintani.

A Gpg4win telepítéshez való kicsomagolása ugyanúgy történik, mint bármely más szokásos Windows szoftver esetében. A program fel fogja szólítani a felhasználót, hogy válassza ki a nyelvet, majd ezután megjelenik a szoftver leírását tartalmazó indítóképernyő és a licencszerződés.

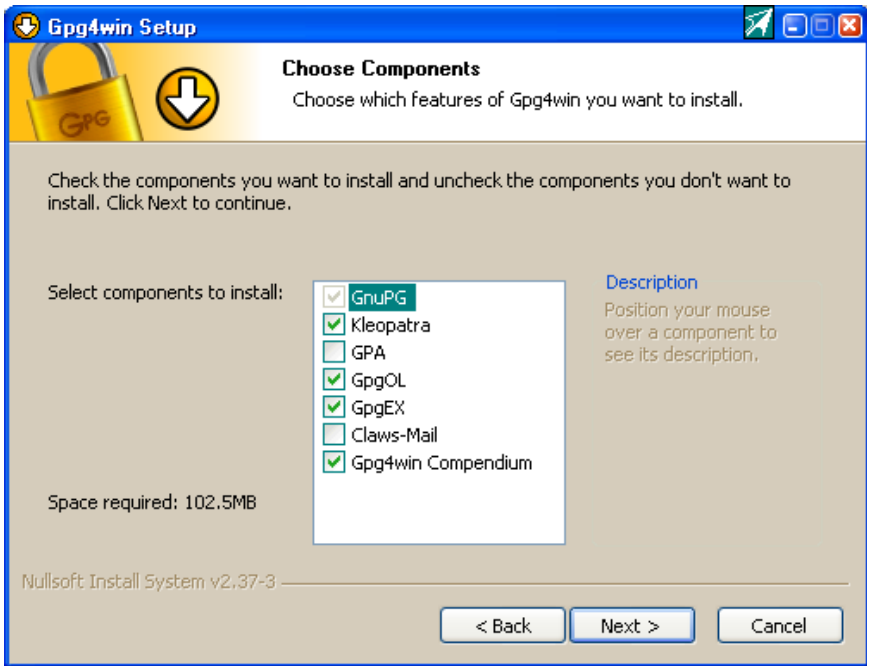
Ezután ki kell választani azokat a komponenseket, amelyeket telepíteni szükséges. A GnuPG kötelező. A program alapértelmezés szerint a következő modulokat telepíti:

- Kleopatra - kulcsok és tanúsítványok kezelésére szolgáló modul;
- GpgOL - a Gpg4win-t az Outlook 2003/2007-be integrálja;
- GpgEX - a Gpg4win-t a Windows Explorer-be integrálja, hogy Intéző ablakból is lehessen fájlokat titkosítani;
- Gpg4win Compendium - a szoftver használati utasítása és egy remek eszköz.

Egyéb felajánlott modulok:

- GPA - a Kleopatra alternatívája kulcs- és tanúsítványkezeléshez;
- Claws-Mail – alternatív e-mail kliens, amely jól egyesíthető a Gpg4win-nel.

Amennyiben a Gpg4win Outlook termékkel kerül használatra, és Outlook 2003 SP2 vagy későbbi verzió, illetve 2007 fut a gépen XP, 32 bites Vista vagy 32 bites Windows 7 alatt, akkor a GPG Outlook-ba integrálásához feltétlenül be kell jelölni a GpgOL melletti négyzetet. A GpgOL nem fut a Vista és a Windows 7 64 bites verziói alatt.

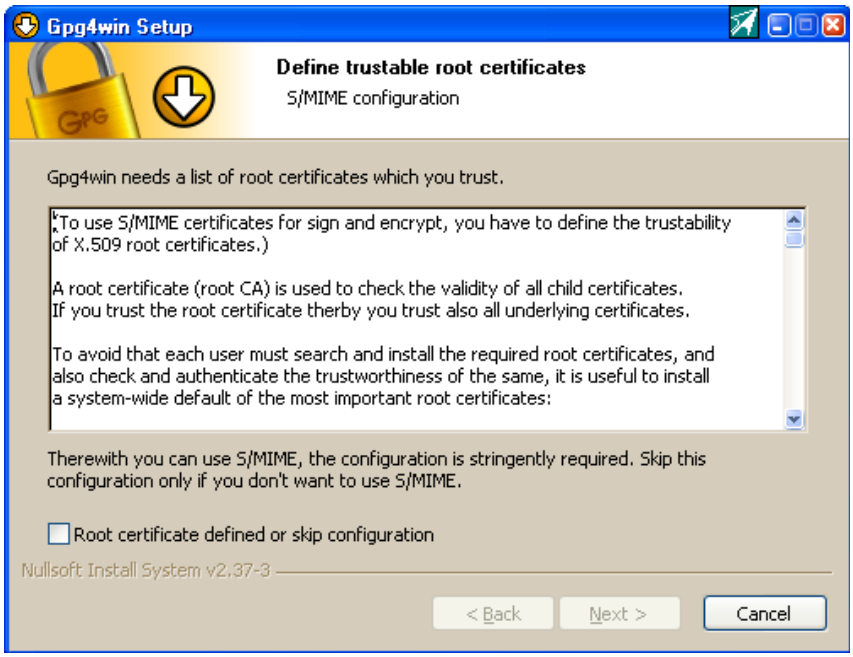


Alapértelmezés szerint a szoftver a következő könyvtárba települ:

C:\Program Files\GNU\GnuPG

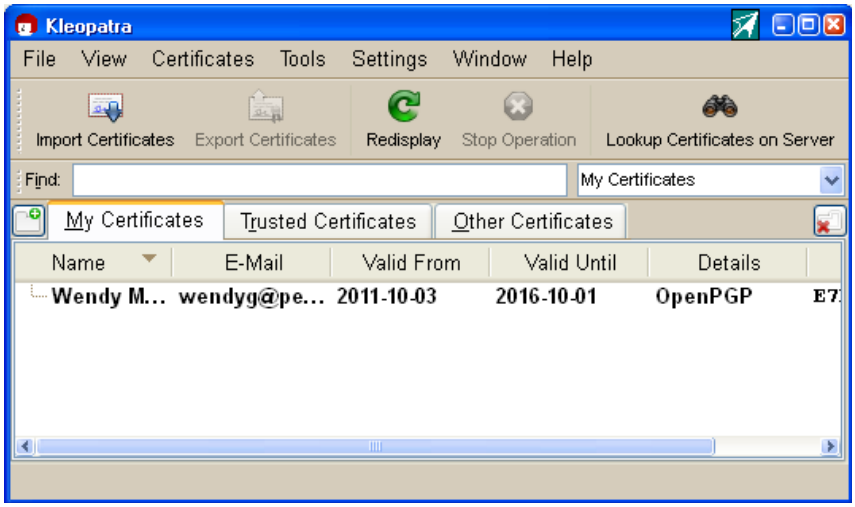
de tetszés szerint másik könyvtárat is lehet választani. A program megkérdezi a felhasználótól, hogy szeretne-e ikont elhelyezni az asztalon, illetve parancsot a Start menüben és/vagy gyorsindítási ikont eszköztáron, majd a telepítés folytatódik.

A szoftver létrehoz egy C:\Documents and Settings\<felhasználónév>\Application Data\gnupg könyvtárat is. Ez a könyvtár fogja tárolni a felhasználó és levelezőpartnerei kulcsait, és ugyanebben a könyvtárban lehet biztonsági másolatot készíteni, ha a felhasználó szeretne másolatot megőrizni a kulcscsomójából. A telepítés befejezése után a Gpg4win felkéri a felhasználót, hogy hozzon létre megbízható gyökértanúsítványokat. Ezt csak akkor kell megtenni, ha S/MIME használatára kerül a sor. Egyelőre elegendő bejelölni a négyzetet a konfiguráció átugrásához.



Az alaptelepítés ezzel befejeződött.

Ezután kulcspárt kell generálni. Ezt a Kleopatra-ban lehet elvégezni, amelynek a telepítéskor megadott választástól függően meg kell jelennie az asztalon vagy a Start menü új csoportjában. Ha nem látható, akkor meg kell keresni azt a könyvtárat, ahová a GPG telepítésre került, és kétszer rá kell kattintani a Kleopatra.exe fájlra. A kulcspár generálásához a File / New / Certificate parancsra kell kattintani, és a Kleopatra végigvezeti a felhasználót a folyamaton.



Körültekintően kell kiválasztani a jelszót! (Ahogy a fentiekben olvasható.)

Visszavonási tanúsítványt is szükséges generálni, ezt egy biztonságos helyre kell másolni, és kitörölni abból a könyvtárból, amelyben a kulcsok tárolódnak.

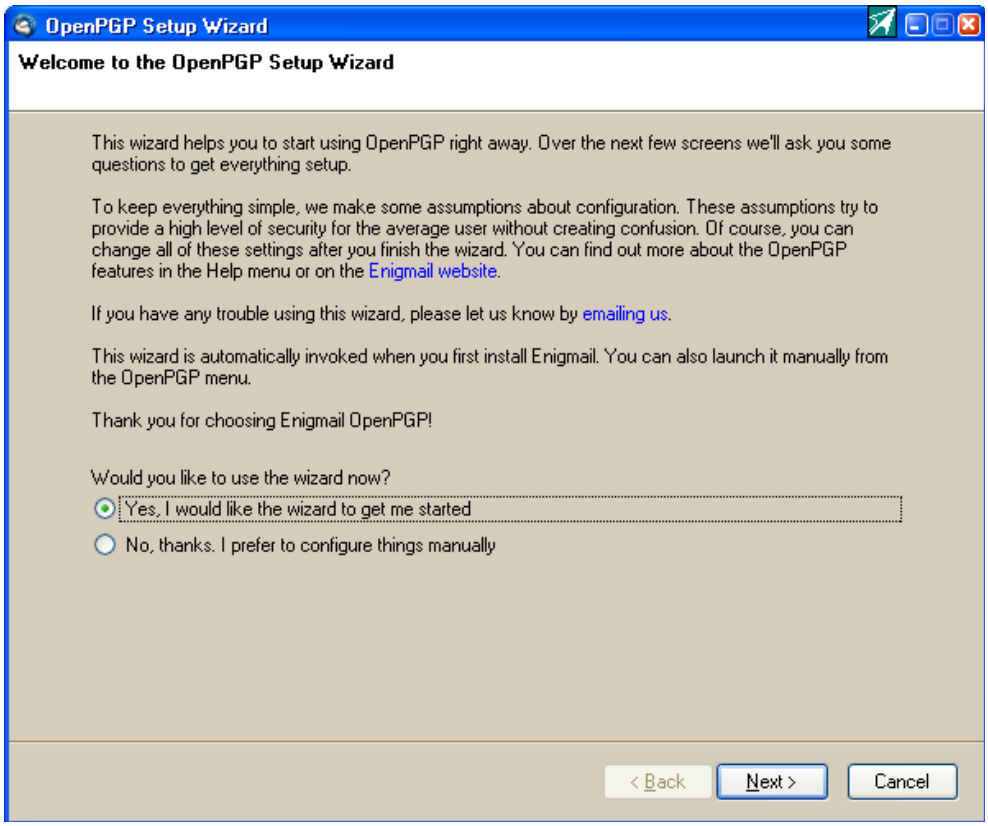
Az e-mail szoftver innen fogja elővenni.

Windows - Thunderbird

Le kell tölteni az Enigmailt a http://enigmail.mozdev.org/download/index.php.html oldalról. Meg kell győződni arról, hogy a megfelelő verzió kerül letöltésre az adott Thunderbird verzióhoz (a Thunderbird verziója a Súgó menüben, a Névjegyben ellenőrizhető).

A Thunderbird-ön belül az Eszközök menüt kell lenyitni, és Bővítmények lehetőséget kiválasztani. A Telepítésre kell kattintani a bal alsó sarokban, majd arra a helyre navigálni, ahol az Enigmail kiegészítő telepítve lett, majd ezt ki jelölni. A többit a Thunderbird elvégzi. A Thunderbird újraindítása után egy OpenPGP feliratú új menü meg megjelenni a eszköztáron, amely minden szükséges funkciót tartalmaz a GPG működtetéséhez: kell-e titkosítani az e-mailt, ha igen, akkor mikor, mennyi ideig maradjon aktív a jelszó, mielőtt újra be kell gépelni; hozzáférés a nyilvános kulcsszerverekhez a partnerek kulcsainak letöltése és saját kulcsok feltöltése céljából. A Thunderbird Enigmail OpenPGP menüjén keresztül akár mások nyilvános kulcsai is aláírhatók és feltölthetők.

Az OpenPGP menüben ki kell választani a Telepítővarázslót, amely segít az Enigmail konfigurálásában.



Windows - Outlook

Amennyiben a telepítéskor bejelölésre került a GpgOL jelölőnégyzetet, akkor a Gpg4win feltelepítette a plugin-t, és az Outlook következő megnyitásakor egy GpgOL feliratú menü is meg fog jelenni. Azonban: A GpgOL csak Outlook 2003-mal és 2007-tel működik. Az Outlook régebbi vagy újabb (2010-es) verzióival nem. Mivel az Outlook egy zárt forráskódú szoftver, a GPG integrálása nem megy zökkenőmentesen, mint a nyílt forráskódú szoftverek esetében.

Ez azonban talán sokkal inkább a fejlesztők, mint a felhasználók problémája. Amennyiben a GpgOL beállítások fülre kattint a felhasználó, jelölőnégyzeteket fog látni arra vonatkozóan, hogy szeretné-e aktiválni az S/MIME támogatást (jelölje be), szeretné-e alapértelmezés szerint titkosítani az új üzeneteket (igen), és szeretné-e alapértelmezés szerint aláírni az új üzeneteket (igen). Ezeket a beállításokat az üzenetenként is meg lehet adni.

Ajánlott, hogy az „Üzenetek megjelenítése HTML formátumban” négyzetet ne legyen bejelölve (így néhány üzenet olvashatatlan lesz), továbbá érdemes üresen hagyni a titkosított e-mailek mellékletként való megjelenítése melletti négyzetet is.

Elképzelhető, hogy szükség lesz néhány változtatásra az Outlook használatának módjával kapcsolatban.

- Ne legyen használva a Microsoft Word terme üzenetek írására!
- Ne készüljön és ne legyen küldve HTML üzenet (a titkosítás és visszafejtés során minden formázás elveszhet).

Ezeket a Beállítások menüben, az E-mailek formázása fülre kattintva lehet elérni és bejelölni. „Csak szöveg" formátumra szükséges állítani az üzenet formátumát.

Ubuntu (és a többi népszerű linux disztribúció nagy része) Thunderbird használatával

A GPG-nek már telepítve kell lennie, így csak a Thunderbird-öt kell telepíteni, és a „Windows - Thunderbird” részben szereplő utasításokat kell követni.

MAC OS X

http://gpgtools.org/
Mac-hez a következő oldalon találhatók más grafikus kezelőfelületek:
http://www.gnupg.org/related_software/frontends.html#mac.

Anroid

Az Android Privacy Guard (APG) programot és a K-9 e-mail klienst a Market-ről lehet letölteni. Használatát a http://thialfihar.org/projects/apg/ oldal ismerteti.

IOS (iPad, iPhone)

Csak dekódolás (érintetlen) iPhone-on - oPenGP Lite - http://pgp.wiredpig.us/2010/pgpgpg-on-iphone/

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel.: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937