



Handleiding & Documentatie

Deze Handleiding & Documentatie is geschreven door Greenhost.

Vragen en opmerkingen kunnen worden gestuurd naar support@publeaks.nl.

Inhoudsopgave

Over Publeaks.....	3
Stichting Publeaks.....	3
Netwerk Democratie.....	4
Hermes Centrum voor Transparantie en Digitale Rechten.....	4
Het Internet Protection Lab.....	4
Greenhost.....	5
Hoe Publeaks is opgezet.....	6
Het platform.....	6
Tor netwerk.....	6
PGP versleuteling van bestanden.....	7
Een laptop met Tails Linux.....	8
Wachtwoorden.....	8
Opdrachten workshop.....	10
Handleidingen receiver.....	12
Opstarten laptop en inloggen.....	12
Een encrypted persistent volume aanmaken.....	14
Het aanmaken van een PGP sleutelpaar.....	17
Het publieke deel van de PGP key in publeaks zetten.....	22
Ophalen van een tip.....	30
Decrypten van een toegezonden bestand.....	33
Metadata verwijderen van bestanden.....	36
Backups.....	37
Backup maken van de PGP sleutel.....	37
Updaten van Tails.....	39

Over Publeaks

In iedere samenleving vinden misstanden plaats en zijn er tipgevers die misschien informatie hebben of kennis van zaken die niet in de haak zijn. Misstanden waarvan zij vinden dat ze moeten worden onderzocht, om er een einde aan te maken of misschien om er een bredere discussie mee los te maken.

Publeaks is een omgeving die deze tipgevers in staat stelt om veilig en anoniem informatie te lekken naar de pers. De tipgever kan zelf selecteren naar welke van de aangesloten mediaorganisaties hij of zij de stukken wil sturen en de ontvangende journalist kan berichten achterlaten voor de aanbieder.

De journalist besluit zelfstandig tot verificatie, nader onderzoek of publicatie. De pers heeft als opdracht om te controleren, om te publiceren, om aan de orde te stellen. De pers is daar toe uitgerust. Journalisten zijn professionals die onderzoeken, doorvragen, wederhoor toepassen en ze hebben een medium waarmee ze zaken naar buiten kunnen brengen.

Natuurlijk is lekken niet zonder risico, maar Publeaks maakt het zo veilig mogelijk. Zo zorgt het systeem er voor dat de afzender, locatie en andere gegevens van het versturen van documentatie niet te herleiden is.

Publeaks.nl is een samenwerking tussen de stichting Publeaks, het Hermes Centrum voor Transparantie en Digitale Rechten, het Internet Protection Lab en Greenhost.

Stichting Publeaks

De Stichting Publeaks wil de journalistieke infrastructuur versterken en het journalistieke vermogen door middel van het ondersteunen van geanonimiseerde communicatie tussen burgers en persorganen.

Het bestuur van de stichting Publeaks.nl bestaat uit:

- Teun Gautier
- Mieke van Heesewijk – Directeur Netwerk Democratie

- Corine de Vries – Lid van Hoofredactie De Volkskrant

De stichting heeft geen enkele toegang tot de inhoud van stukken of rol in de relaties tussen journalist en aanbieder van informatie. De stichting heeft slechts tot doel om de infrastructuur beschikbaar te maken. De stichting, noch een andere (rechts-)persoon heeft toegang tot de gegevens op het systeem waar het informatie over aanbrenger betreft of de eventueel verzonden stukken.

De stichting heeft een zeer beperkte begroting die wordt opgebracht door de deelnemende persbedrijven, fondsen en donaties.

Stichting Puleaks is bereikbaar via info@puleaks.nl

Netwerk Democratie

Netwerk Democratie is mede verantwoordelijk voor de idee-ontwikkeling en realisatie van Puleaks.nl. De stichting Netwerk Democratie zet zich in voor een veerkrachtige democratie waarin burgers meer betrokken zijn en, met behulp van technologie, actief bijdragen.

www.netdem.nl

Hermes Centrum voor Transparantie en Digitale Rechten

Het Hermes Centrum voor Transparantie en Digitale Rechten heeft de software Globaleaks ontwikkeld. Globaleaks is een open source project gericht op het creëren van een wereldwijd, anoniem, censuur-bestendig, klokkenluiders platform.

In samenwerking met Puleaks is de Globaleaks software aangepast en vertaald. Het resultaat van die samenwerking is puleaks.nl.

www.logioshermes.org

Het Internet Protection Lab

Het Internet Protection Lab is verantwoordelijk voor het technisch projectmanagement van Puleaks.nl. Het Internet Protection Lab biedt overal ter wereld concrete en gerichte steun aan journalisten, bloggers en activisten die bedreigd worden. Door het bieden van internetverbindingen, expertise van

beveiligde webhosting, maken ze hun werk veiliger en effectiever.

www.internetprotectionlab.net

Greenhost

Greenhost is verantwoordelijk voor de hosting en ondersteuning van Publeaks.

De basis van Greenhost is groene hosting en al meer dan 10 jaar loopt Greenhost hierin voorop. Greenhost is betrokken bij maatschappelijk relevante kwesties zoals duurzaamheid en digitale vrijheid. Dankzij eigen innovaties hebben ze 70% minder systemen nodig. Daarnaast gebruiken ze uitsluitend hernieuwbare energiebronnen.

Greenhost zet zich in voor een open en vrij internet en de bescherming van haar gebruikers. Greenhost staat pal voor vrijheid van informatie, privacy en openbaarheid van bestuur. Ze houden als enige provider niet bij wanneer u met wie mailt en maken gebruik van vrije en open software. Ze sponsoren meerdere organisaties die zich inzetten voor vrijheid, duurzaamheid en cultuur, zoals Free Press Unlimited en Publeaks.

www.greenhost.nl

Tel. 020-4890444

Hoe Publeaks is opgezet

Het platform

Het primaire doel van het Publeaks platform is te zorgen dat tipgevers anoniem kunnen blijven als zij dat willen. Daartoe heeft Publeaks een systeem opgezet dat op verschillende manieren zorgt dat de identiteit van een tipgever niet bekend wordt. Zo maakt het Publeaks gebruik van het Tor netwerk en worden bestanden alleen versleuteld met PGP opgeslagen.

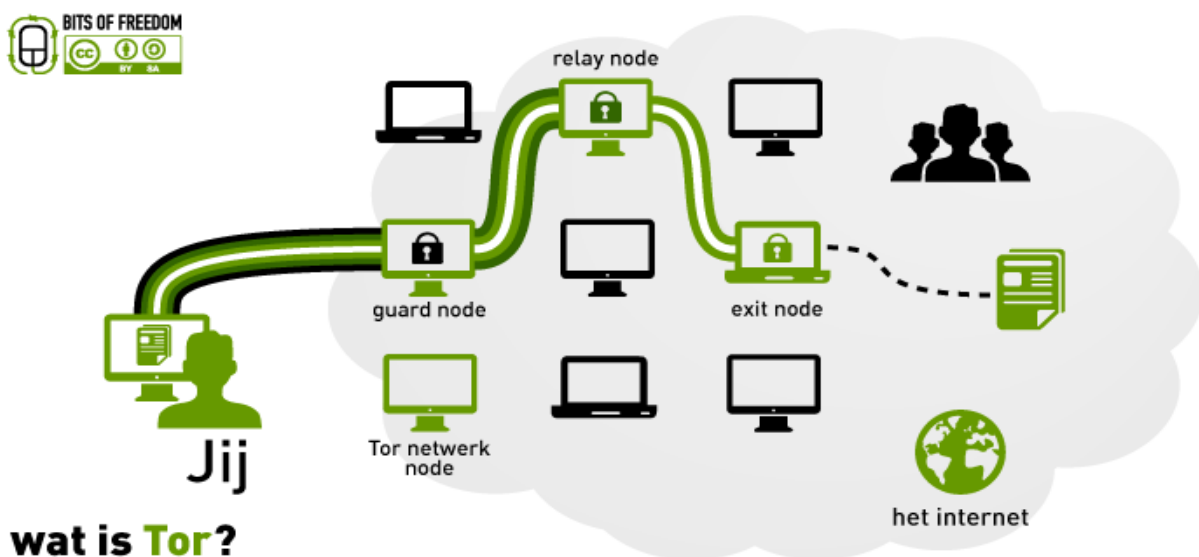
Hierbij moet worden opgemerkt dat geen enkele techniek feilloos is, dus ook die van Publeaks niet. Wel heeft Publeaks, mede door gebruik te maken van de nieuwste technieken, het voor de tipgevers zo veilig mogelijk gemaakt.

Tor netwerk

Bezoekers van de Publeaks website wordt daarvoor aangeraden dit alleen te doen via het Tor netwerk en dit geldt nog extra voor eventuele tipgevers. Het Tor netwerk is namelijk ontworpen om je anoniem op internet te kunnen begeven en zo ook anoniem Publeaks te bezoeken.

Hoe werkt Tor?

Het anonimiseren werkt doordat Tor op zijn weg naar het internet eerst driemaal een willekeurige en versleutelde verbinding maakt met een node in het Tor netwerk. De website die wordt bezocht kan daardoor bijna onmogelijk herleiden wie feitelijk de website bezoekt.



Bij het Publeaks platform is het niet alleen de gebruiker die van Tor gebruik maakt, maar ook de server zelf. Niet alleen de gebruiker is dan anoniem, maar ook de server. Hierdoor is het op de server van Publeaks niet alleen onmogelijk om te achterhalen wie bestanden naar de Publeaks server heeft geüpload, maar ook dat niemand kan achterhalen waar de server fysiek staat. Daardoor is toegang krijgen tot de server en de data daarop een stuk moeilijker.

Mocht een bezoeker zelf niet direct gebruik van het Tor netwerk willen of kunnen maken, dan werkt de normale Publeaks website als proxy naar het Tor netwerk. De verbinding met de website is dan beveiligd met SSL en vanaf daar wordt dan via het Tor netwerk een verbinding opgezet met de Publeaks server waar de data wordt opgeslagen.

PGP versleuteling van bestanden

Bestanden die worden geüpload naar de server worden daar versleuteld met PGP opgeslagen. Daarvoor worden alleen die PGP sleutels gebruikt die horen bij de media waarvan de tipgever heeft aangegeven dat deze er zijn informatie aan wil geven. Dus alleen die media en niemand anders kan daarna nog die bestanden ontsleutelen.

Hoe werkt PGP?

PGP is een zogenoemde asymmetrische encryptie methode die werkt met sleutelparen. Elk sleutelpaar bestaat uit twee sleuteldelen, een publiek deel en een privé deel. De publieke sleutel wordt gebruikt voor het versleutelen van data en het privé deel voor het ontsleutelen van data.



Doordat je de publieke sleutel alléén gebruikt om data te versleutelen, kun je deze sleutel zonder problemen aan iedereen geven. Jij bent vervolgens de enige die de daarmee versleutelde data met jouw privé sleutel kan ontsleutelen. Deze versleutelde data kan dus veilig worden opgeslagen of worden verstuurd, zonder het gevaar dat iemand anders dit kan lezen of

gebruiken.

Het is dus zeer van belang dat de privé sleutel veilig wordt bewaard en van een zeer goed wachtwoord wordt voorzien.

Wat is het verschil tussen PGP en GPG?

PGP en GPG (ook wel GnuPG) hebben beide dezelfde oorsprong en dezelfde functionaliteit. Het belangrijkste verschil is dat PGP betaalde software is en GPG vrij beschikbare open-source software is. Linux maakt standaard gebruik van de GPG.

Een laptop met Tails Linux

De journalist gebruikt voor het ophalen van de tips een speciaal daarvoor geconfigureerde laptop met Tails Linux. Deze laptop biedt de mogelijkheid om in een veilige omgeving bestanden te anonimiseren voordat ze de wereld in worden gebracht.

Tails is een Linux versie die speciaal is ontwikkeld om je veilig en anoniem op het internet te begeven. De standaard browser is daarom van Tor voorzien. Tails is ook minder kwetsbaar voor malafide software, doordat de installatie niet zomaar is aan te passen en het telkens 'schoon' wordt opgestart.

Voor de journalisten is de anonimiteit misschien wat minder van belang, zij maken er tenslotte geen geheim van dat ze gebruik maken van Publeaks, maar de extra veiligheid die Tails biedt is wel erg belangrijk. De laptop laat geen sporen achter van wat een journalist op het systeem heeft gedaan en het systeem biedt de mogelijkheid om data versleuteld op te slaan. Hierdoor kunnen ontvangen bestanden veilig worden gedownload, van eventuele (meta)data worden ontdaan en worden bewaard en bewerkt, zonder gevaar dat er iets van uitlekt. Voor het verwijderen van metadata is er speciale software op de laptop aanwezig die de journalist hierbij kan helpen.

Wachtwoorden

Voor het Publeaks platform worden meerdere wachtwoorden gebruikt, namelijk voor de account op de Publeaks website, voor de versleutelde opslag op de laptop en voor de PGP sleutel. Het is natuurlijk erg belangrijk om hier goede en sterke wachtwoorden te gebruiken.

Wat is een veilig wachtwoord?

Het belangrijkste bij een goed wachtwoord is de lengte, het is daarom ook beter om van een wachtzin te spreken dan van een wachtwoord. Gebruik in elk geval wachtwoorden van minimaal 12 karakters, maar meer is beter. Daarnaast is het natuurlijk goed om een combinatie te hebben van kleine letters, hoofdletters, cijfers en overige tekens, maar lengte wint het van complexiteit. Een wachtwoord “Zwaaien Ziet Zwaan” is daarom een beter wachtwoord dan “Q\$4e”.

Wachtwoord vergeten?

Er zitten in PGP en de versleutelde opslag op de Tails usb-stick géén achterdeurtjes of workarounds. Als een wachtwoord kwijt is, dan is daar helemaal niets meer aan te doen. Alle data die dan nog met de desbetreffende sleutel is versleuteld, moet als verloren worden beschouwd.

Wel is het mogelijk een nieuwe publieke PGP sleutel aan te maken en naar de Publeaks website te uploaden. Dit kan op dezelfde manier gebeuren als de eerste keer dat de PGP sleutels werd aangemaakt en zoals in het hoofdstuk “Het aanmaken van een PGP sleutelpaar” in de handleiding wordt beschreven. Bij nieuwe tips wordt dan gebruik gemaakt van deze nieuwe sleutel waarvan het wachtwoord dan natuurlijk wel bekend is. Eventueel kan een tipgever worden gevraagd de documenten nogmaals te uploaden, zodat deze alsnog beschikbaar komen.

Opdrachten workshop

1. Steek eerst de usb in de laptop en start daarna pas de laptop. Log vervolgens in.
2. Maak een encrypted persistent volume aan.
3. Herstart en log in met *Use persistent storage Yes*.
4. Maak een PGP sleutelpaar aan.
5. Log in op <https://secure.publeaks.nl>
6. Voeg je aangemaakte PGP key toe aan je *voorkeuren*. (Log daarna uit.)

De stappen 1 t/m 6 zijn noodzakelijk om het systeem te configureren en je in staat te stellen tips te ontvangen. De overige stappen zijn interessant als je wilt leren hoe het systeem werkt.

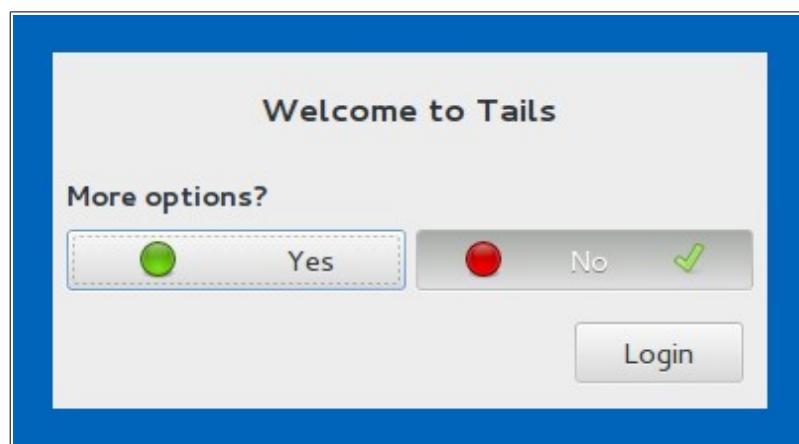
7. Upload een bestand via de website (en sla de code op die je krijgt!)
8. Bekijk de e-mail melding die je binnen hebt gekregen.
9. Log als jezelf in op de website en bekijk de tip die je hebt opgestuurd.
10. Geef een reactie op deze tip.
11. Download het bestand dat je had geüpload en decrypt het op je laptop.
12. Lees de reactie die je eerder gaf en schrijf een antwoord terug.
13. Upload een extra bestand. (Log daarna uit.)
14. Bekijk de nieuwe e-mail melding die je binnen hebt gekregen.
15. Log weer als jezelf in en bekijk de gewijzigde tip.
16. Log in als tipgever met de code die je eerder hebt opgeslagen.
17. Download het nieuwe bestand en decrypt het.

Handleidingen receiver

Opstarten laptop en inloggen

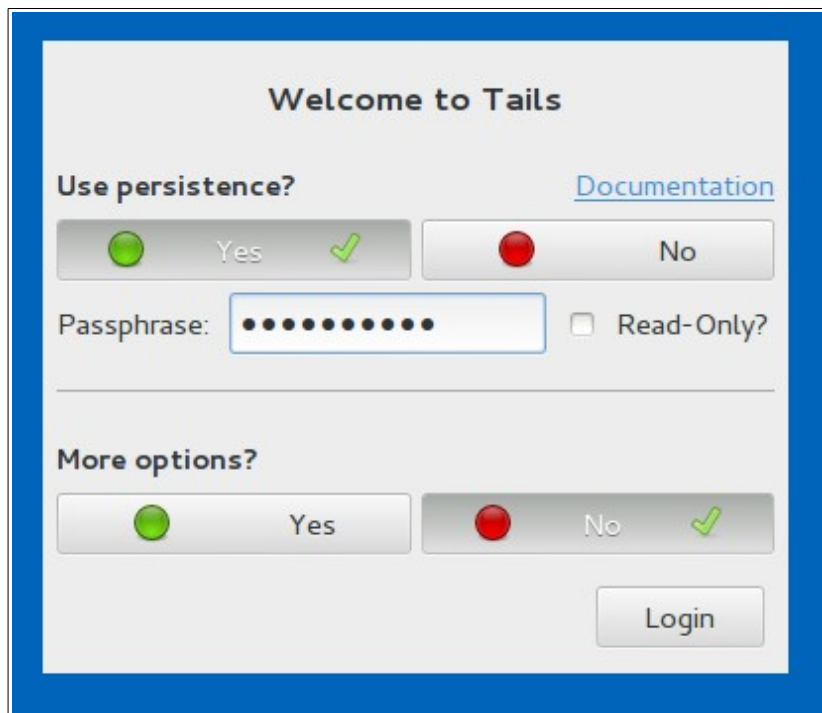
Steek eerst de USB-stick met de Linux versie 'Tails' in de laptop en zet daarna pas de laptop aan.

De eerste keer dat de laptop wordt opgestart ziet het login scherm eruit zoals hieronder. Er is dan nog geen persistent volume.



Klik dan op *Login* om in te loggen.

Als er wel een persistent volume is aangemaakt ziet het login scherm eruit zoals hieronder. Je kunt dan een wachtwoord invoeren om toegang te krijgen tot de persistent volume. (Hoe je een persistent volume aanmaakt staat beschreven in de volgende stap.)



Klik onder *Use persistence?* op *Yes* en voer daarna het wachtwoord van de persistent volume in.

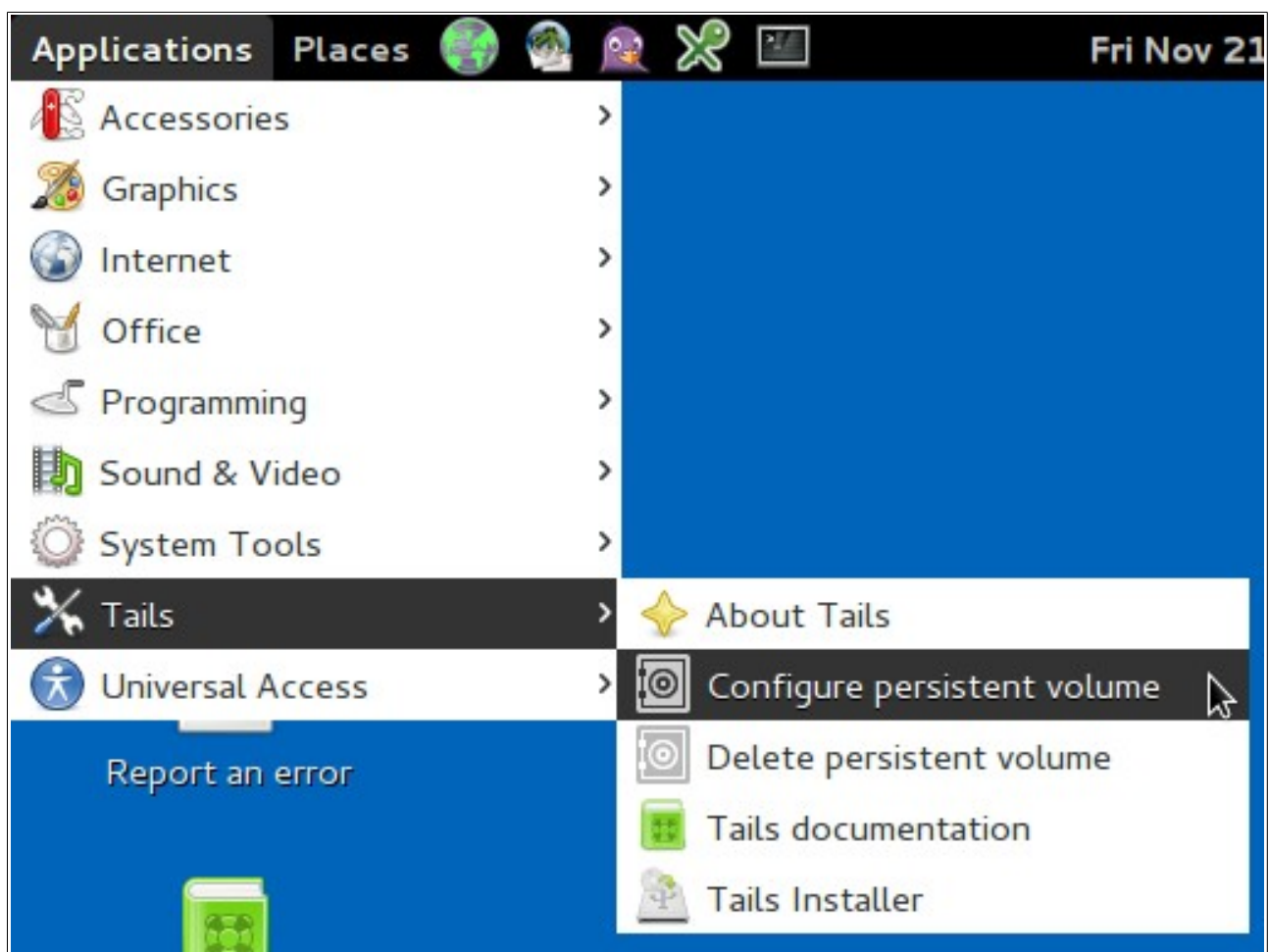
Klik daarna op *Login* om in te loggen.

Een encrypted persistent volume aanmaken

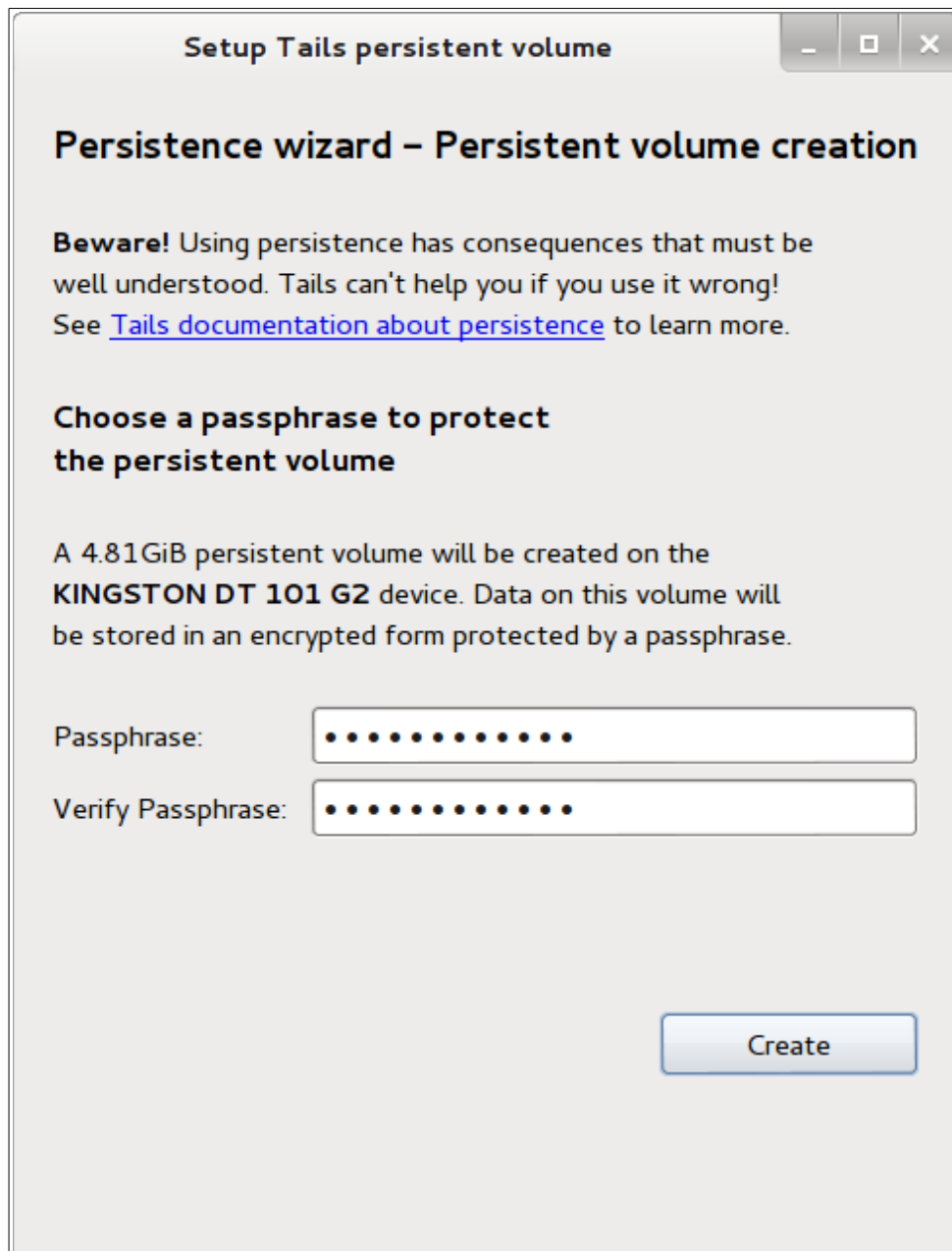
Standaard bewaard Tails geen gegevens, alles wat er op de laptop wordt gedaan, wordt vergeten en verwijderd als deze wordt afgesloten. Voor het gebruik met Publeaks willen we ook bestanden kunnen bewaren en in elk geval moet de PGP sleutel ergens worden opgeslagen.

Daarom wordt er allereerst een encrypted persistent volume op de USB-stick aangemaakt. Dit is een versleutelde plek op de USB-stick waar veilig data kan worden opgeslagen.

Start de laptop en log in.



Start *Configure persistent volume*

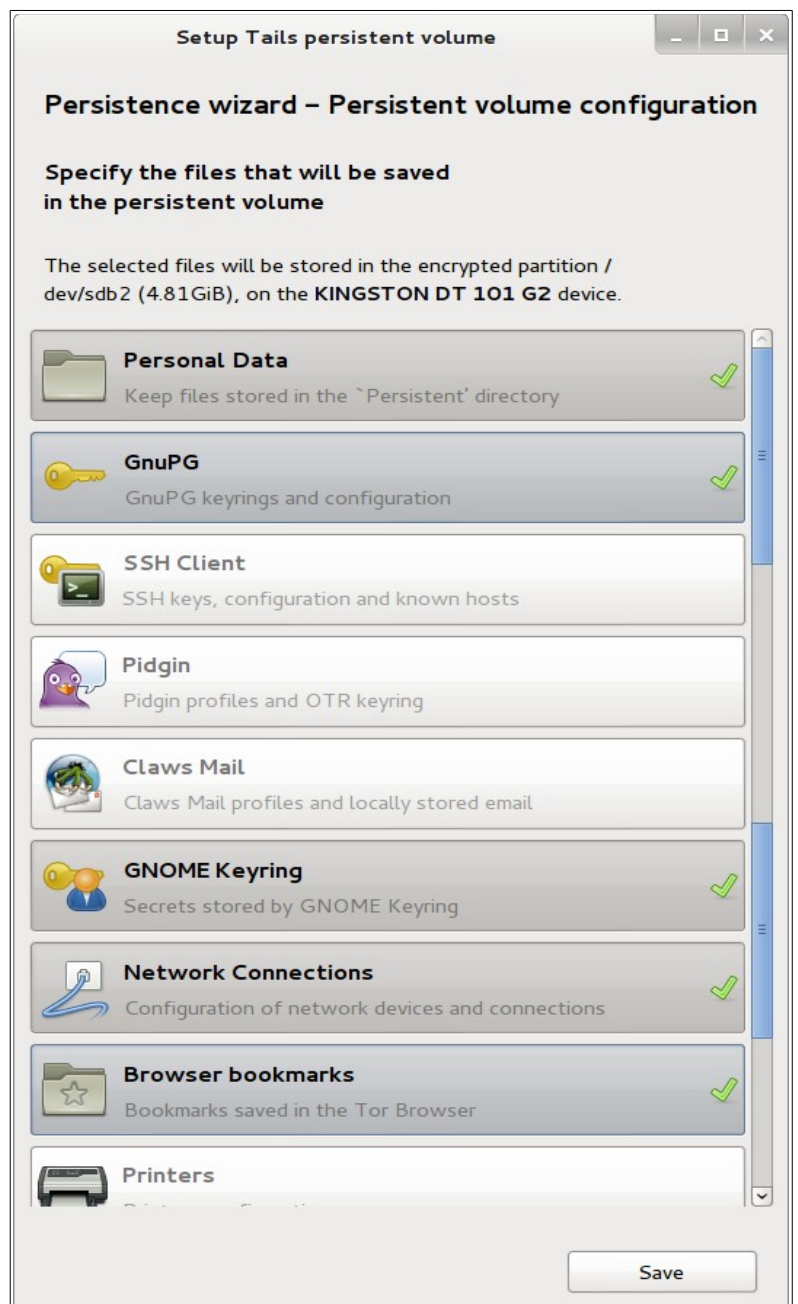


Voer tweemaal een goede wachtzin in en klik op *Create*

Selecteer de volgende onderdelen:

- Personal Data
- GnuPG
- GNOME Keyring
- Network Connections
- Browser bookmarks

klik daarna op **Save**.



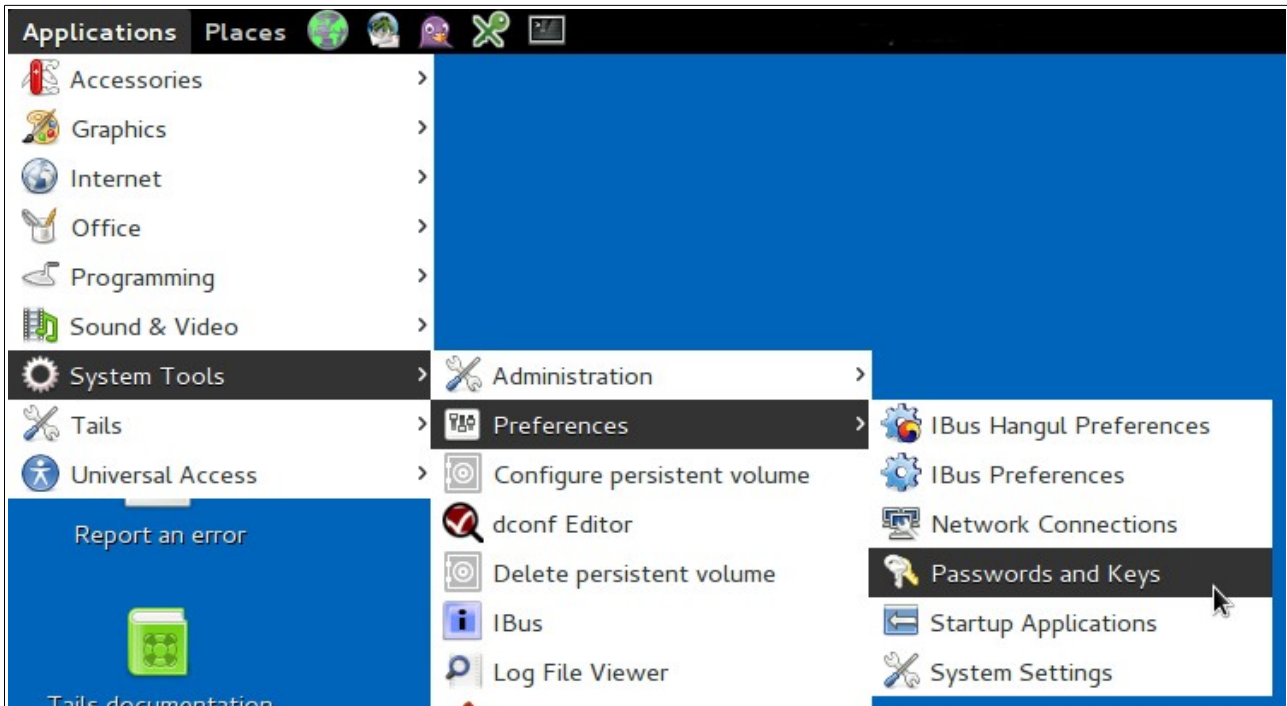
Sluit vervolgens dit programma af door op het kruisje te klikken
en start de laptop opnieuw op.

Na opnieuw opstarten krijgt u het eerder getoonde inlogscherm waarin u kunt kiezen voor de persistent volume.

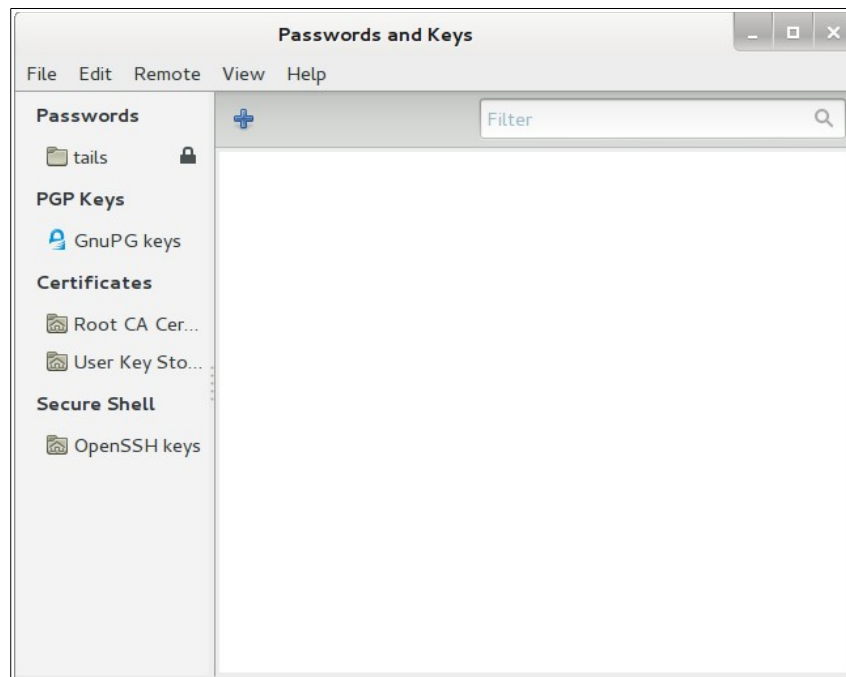
Het aanmaken van een PGP sleutelpaar

Om bestanden veilig op de server op te slaan worden deze voordat ze worden opgeslagen eerst met behulp van PGP versleuteld. Om dat te kunnen doen moeten de gebruikers van Publeaks natuurlijk wel een PGP sleutel hebben. Daarom wordt hier uitgelegd hoe een PGP sleutelpaar kan worden aangemaakt.

N.B. Zorg dat je bent ingelogd met *Use persistence?* op Yes!



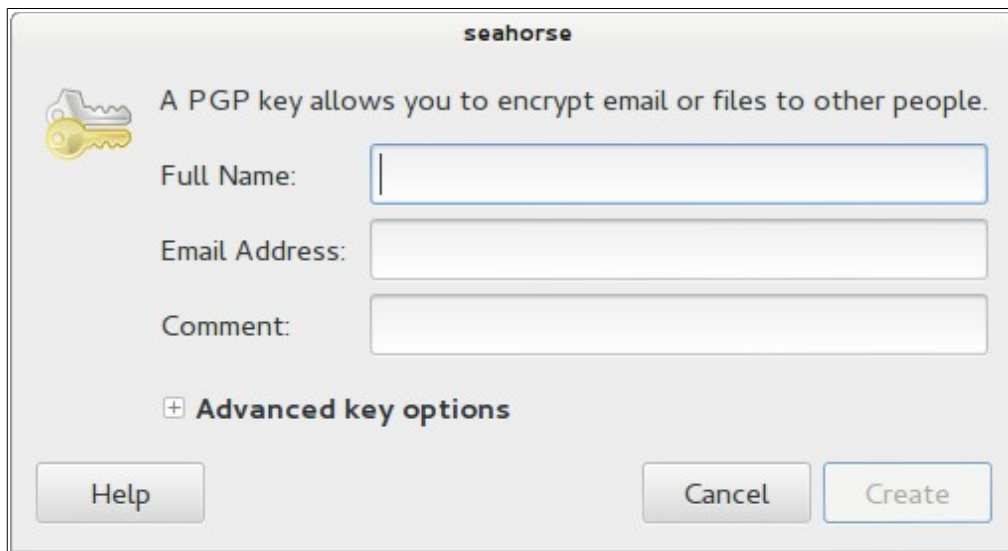
Start *Passwords and Keys*




Klik op *File* en dan *New*



Klik *PGP Key* en dan *Continue*



seahorse

 A PGP key allows you to encrypt email or files to other people.

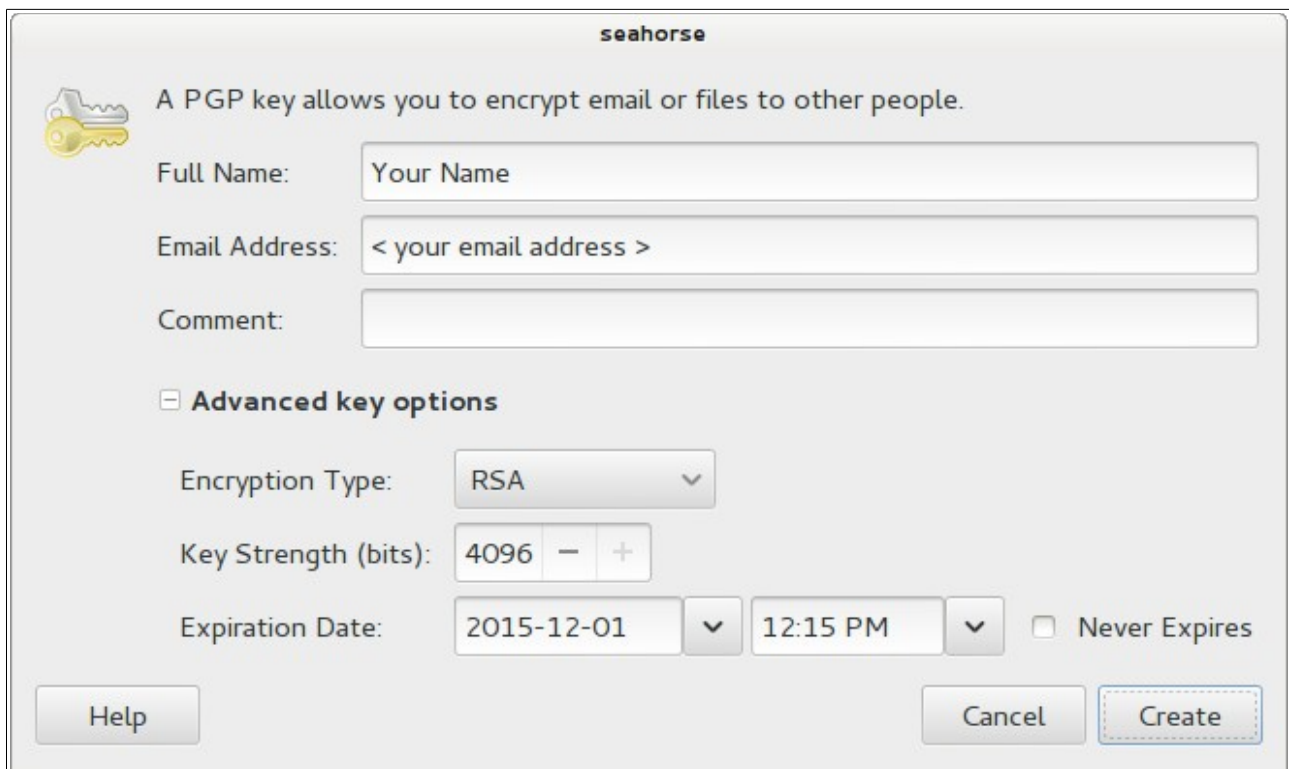
Full Name:

Email Address:


Comment:

☐ **Advanced key options**

Klik op *Advanced key options*



seahorse

 A PGP key allows you to encrypt email or files to other people.

Full Name:

Email Address:

Comment:

☒ **Advanced key options**

Encryption Type: ▼

Key Strength (bits): - +

Expiration Date: ▼ ▼ ☐ Never Expires

Vul de volgende gegevens in en klik *Create*

Full Name: Je volledige naam of naam van het medium

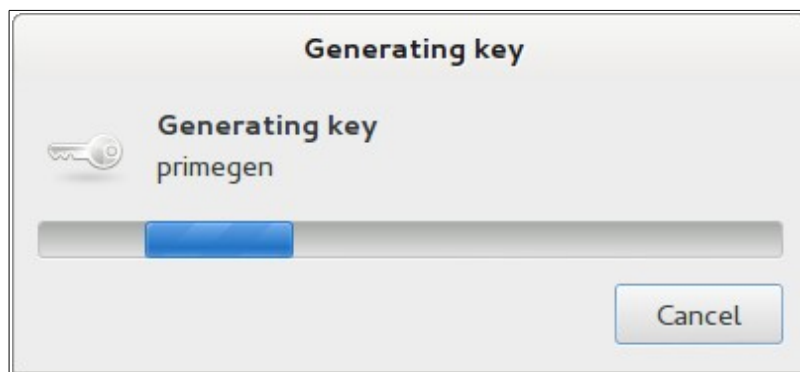
Email Address: het e-mail adres dat je voor Publeaks gebruikt

Zet de Key Strength op 4096

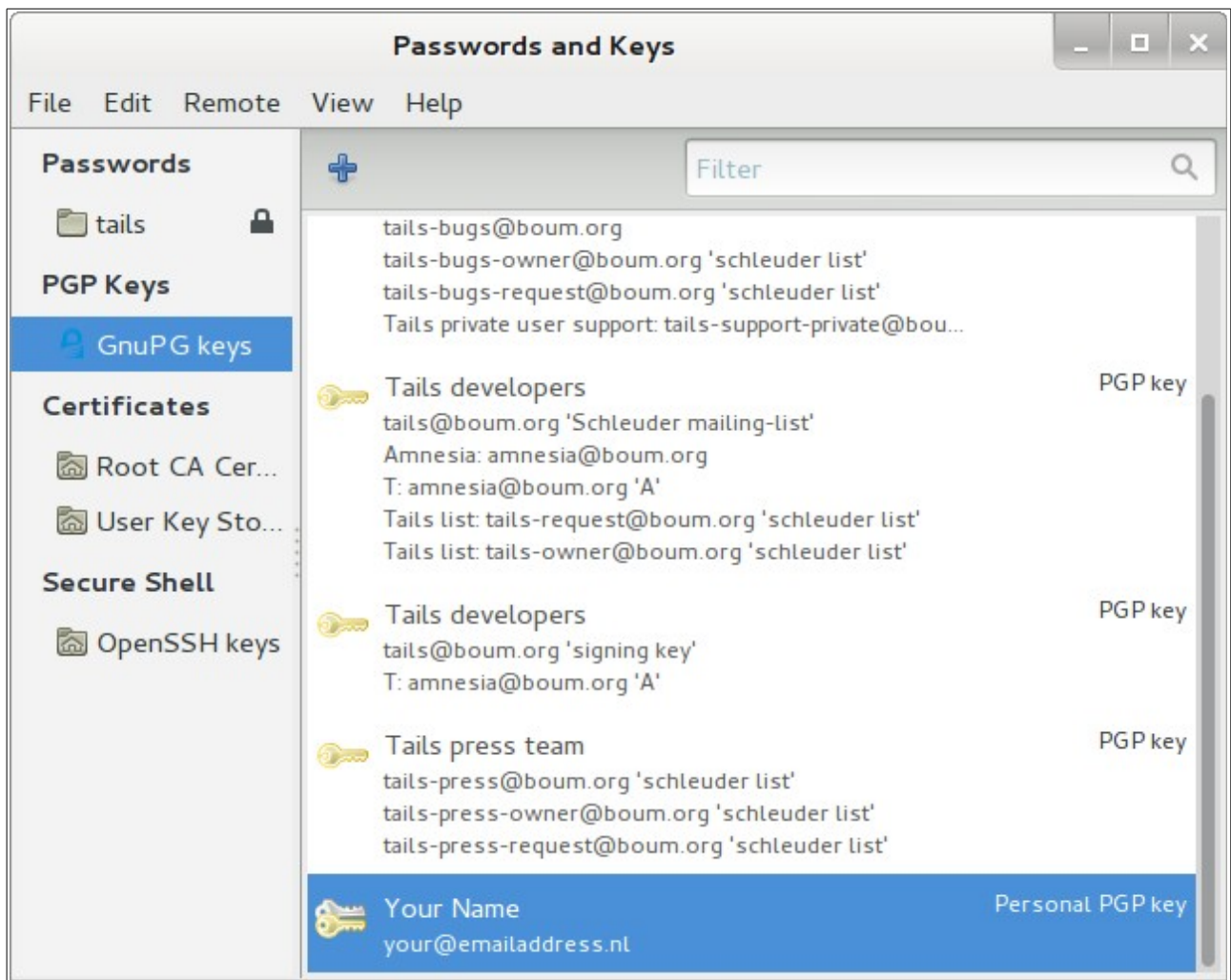
Zet de Expiration Date op één jaar in de toekomst.



Vul een goede passphrase in en klik *OK*



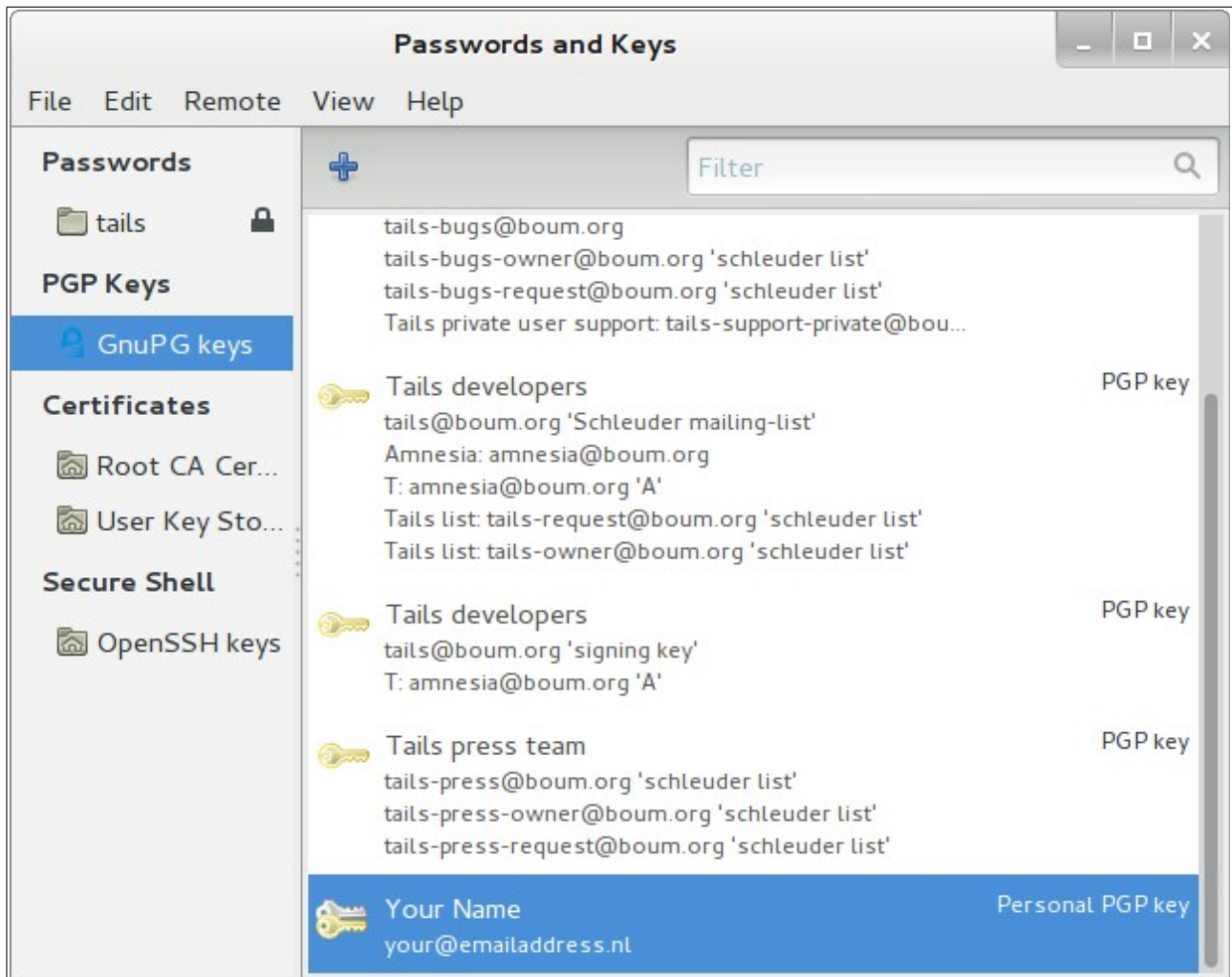
Het genereren van de keys kan soms lang duren.



De aangemaakte keys zijn te vinden onder *GnuPG keys*

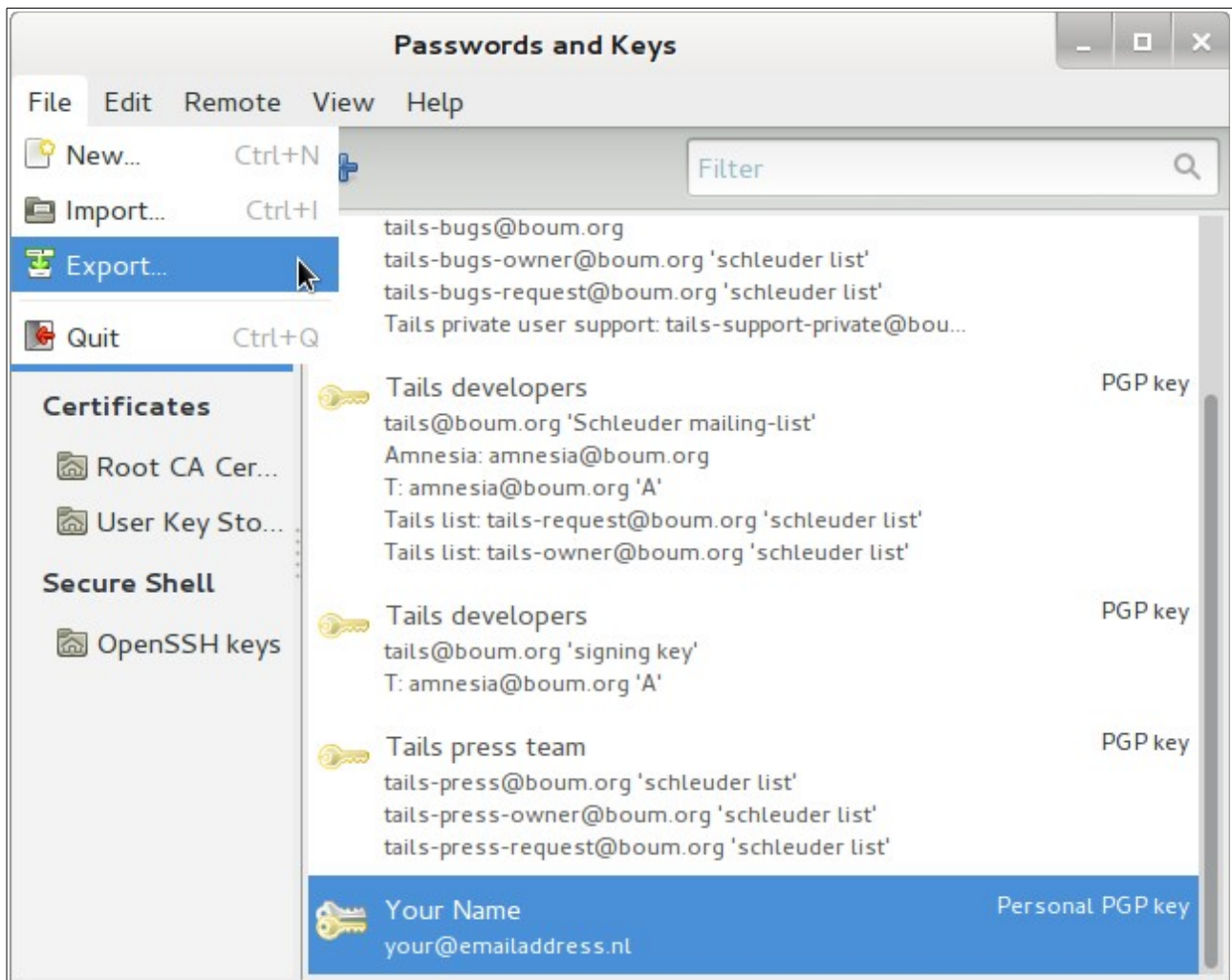
Het publieke deel van de PGP key in publeaks zetten

Om op de server bestanden te versleutelen, moeten de publieke sleutels beschikbaar zijn. Hieronder wordt uitgelegd hoe het publieke deel van het PGP sleutelpaar kan worden geüpload.

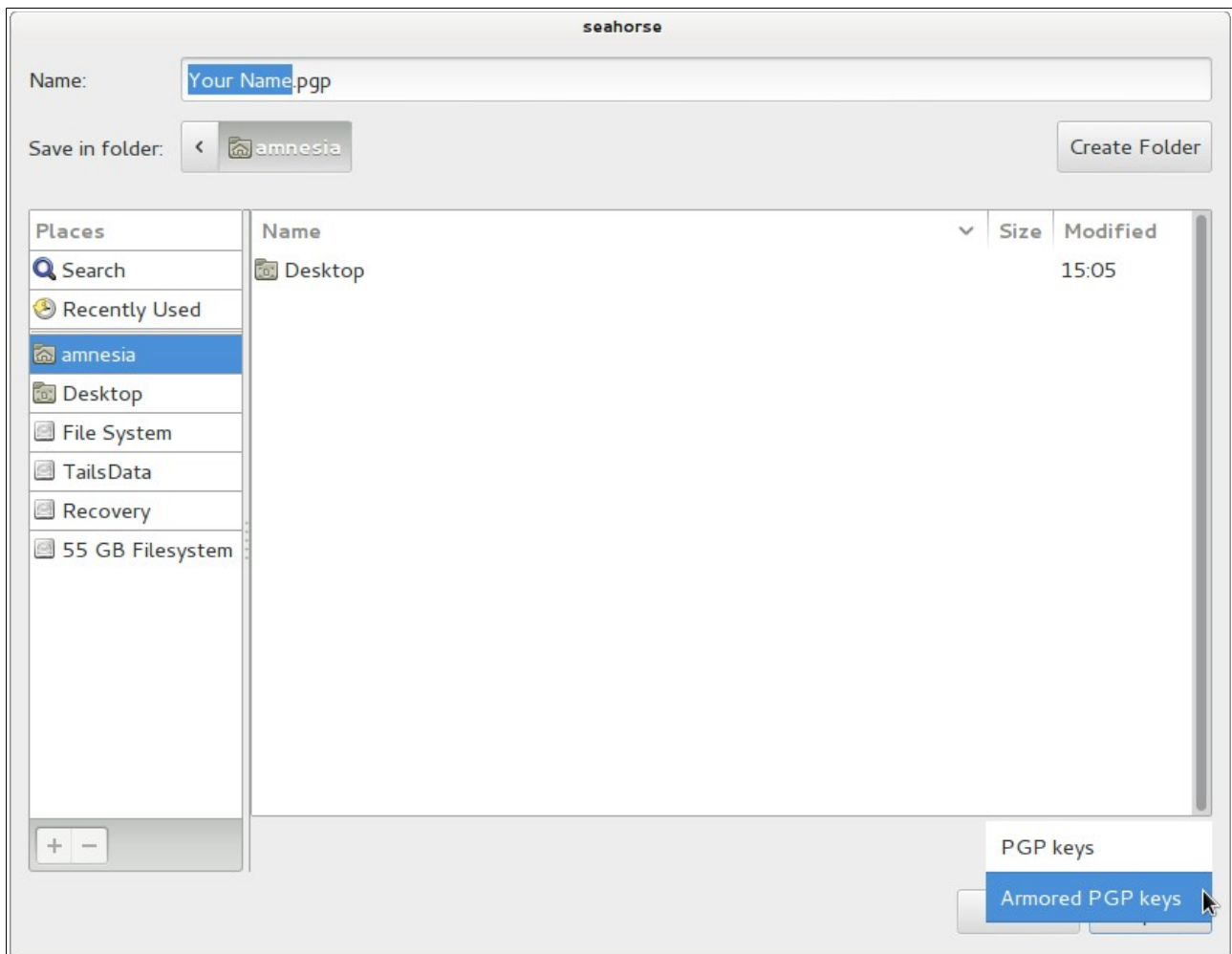


Start *Passwords and Keys* (als deze niet meer actief is)

en selecteer jouw *Personal PGP key*



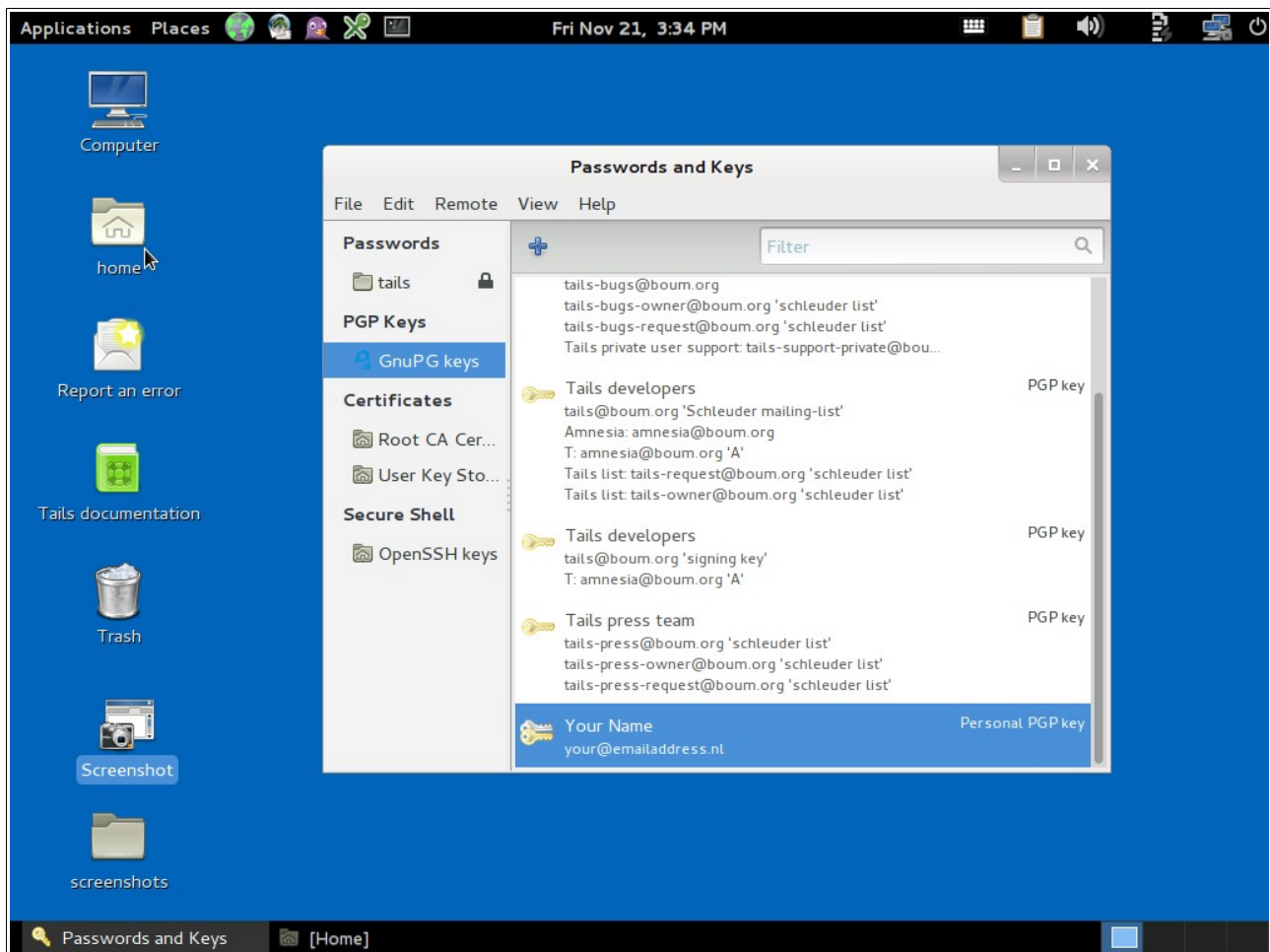
Klik *File* en dan *Export*



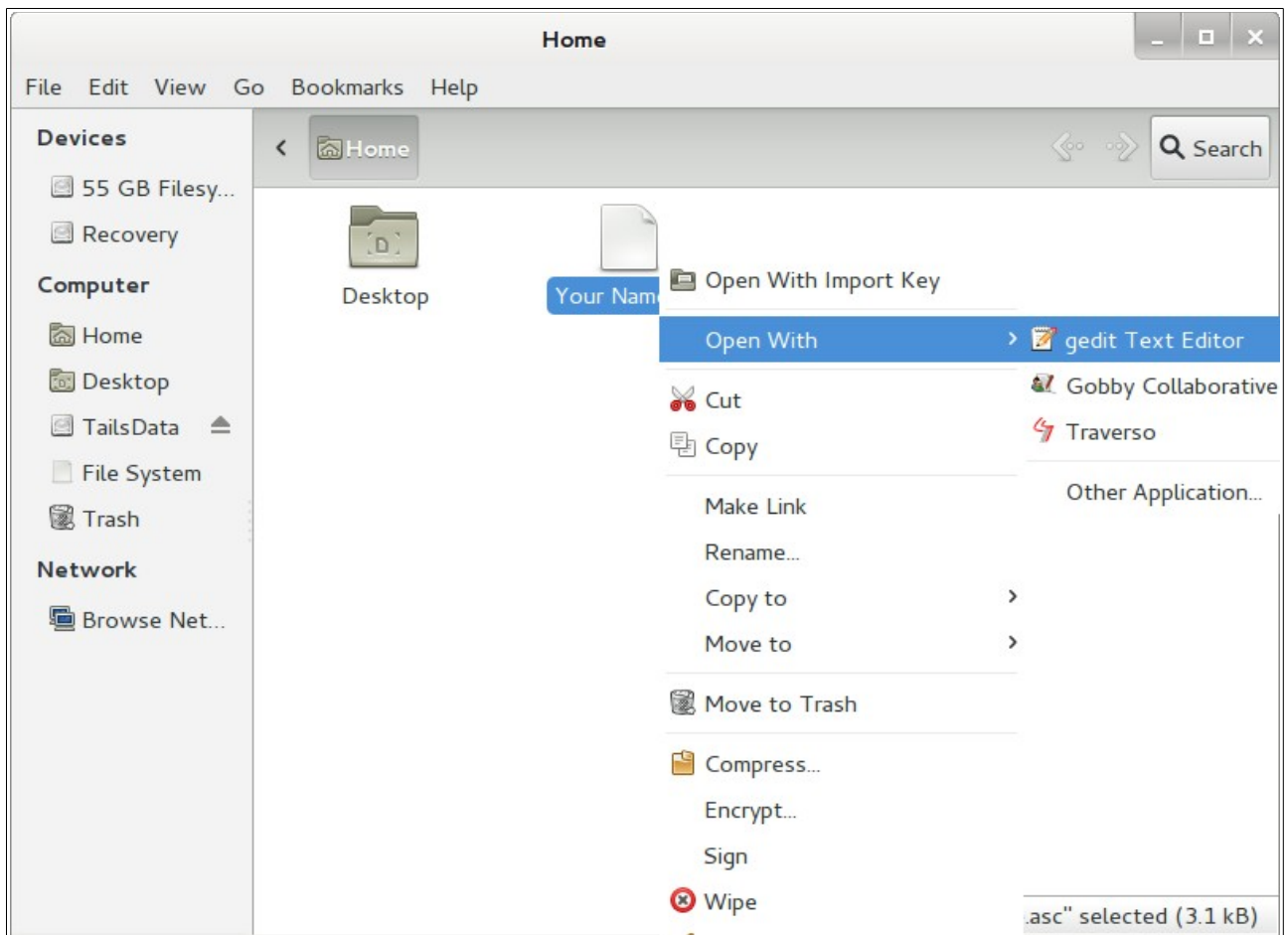
Selecteer de map *amnesia*

Verander rechtsonder de setting naar *Armored PGP keys*

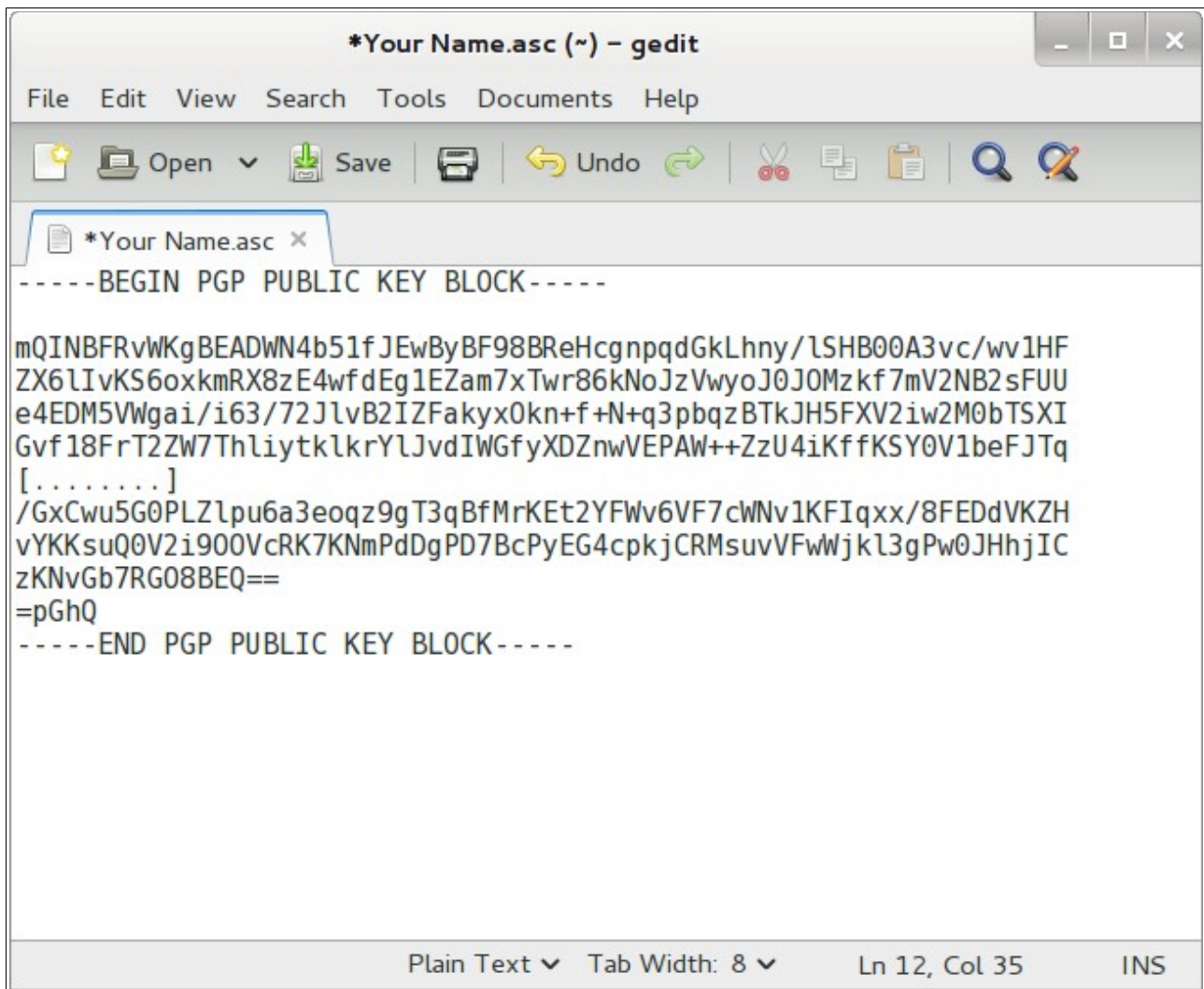
Klik daarna op *Export*



Dubbelklik *home* op de desktop



Rechtermuisklik op de eerder geëxporteerde key
en open het bestand met *gedit Text Editor*



The screenshot shows a gedit text editor window titled '*Your Name.asc (~) - gedit'. The menu bar includes File, Edit, View, Search, Tools, Documents, and Help. The toolbar contains icons for Open, Save, Undo, and other standard editing functions. The text area contains a PGP public key block, starting with '-----BEGIN PGP PUBLIC KEY BLOCK-----' and ending with '-----END PGP PUBLIC KEY BLOCK-----'. The key data is a long string of characters. The status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 12, Col 35', and 'INS'.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFRvWKgBEADWN4b51fJEwByBF98BReHcgnpqdGkLhny/LSHB00A3vc/wv1HF
ZX6lIvKS6oxkmRX8zE4wfdEg1EZam7xTwr86kNoJzVwyoJ0JOMz kf7mV2NB2sFUU
e4EDM5VWgai/i63/72JlvB2IZFakyx0kn+f+N+q3pbqzBTkJH5FXV2iw2M0bTSXI
Gvf18FrT2ZW7Thliyt klkrYlJvdIWGfyXDZnwVEPAW++ZzU4iKffKSY0V1beFJTq
[ ..... ]
/GxCwu5G0PLZlpu6a3eoqz9gT3qBfMrKEt2YFwv6VF7cWNv1KFIqxx/8FEDdVKZH
vYKKsuQ0V2i900VcRK7KNmPdDgPD7BcPyEG4cpkjCRMsuvVFwWjkl3gPw0JHhjiC
zKNvGb7RG08BEQ==
=pGhQ
-----END PGP PUBLIC KEY BLOCK-----
```

Kopieer **alle** tekst in gedit

inclusief -----BEGIN PGP PUBLIC KEY BLOCK----- en -----END PGP PUBLIC KEY BLOCK-----

Start op de laptop de browser en ga naar <https://secure.publeaks.nl>



Log in door te klikken op *Login pagina* en je gebruikersnaam en wachtwoord in te voeren.



Klik op *Voorkeuren*



Klik op het tabblad *Encryptie instellingen*
en klik op *CONFIGUREER EEN PGP SLEUTEL*

— CONFIGUREER EEN PGP SLEUTEL

Plak hier de PGP-sleutel:

✓ UPDATE NOTIFICATIE EN ENCRYPTIE INSTELLINGEN

Plak de eerder gekopieerde public PGP key in het veld.

N.B. Als het veld reeds een PGP key bevat, verwijder deze dan eerst voor de eigen key te plakken.

Klik daarna op *UPDATE NOTIFICATIE EN ENCRYPTIE INSTELLINGEN*.

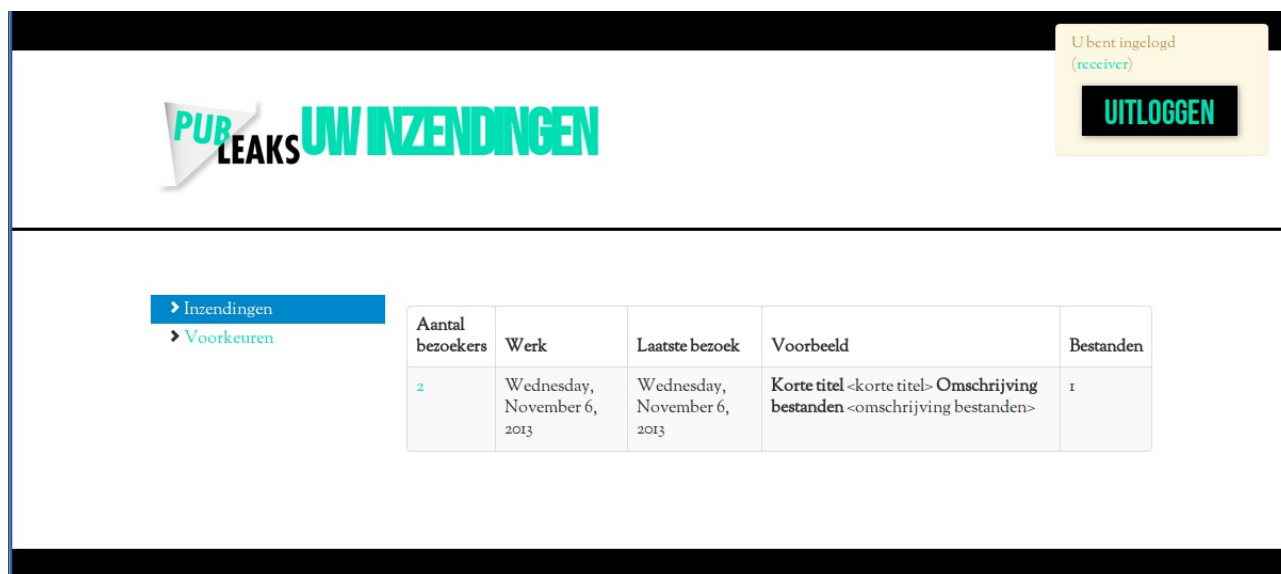
Ophalen van een tip

Start op de laptop de browser en ga naar <https://secure.publeaks.nl>

BENT U EEN DEELNEMENDE JOURNALIST?

Dit is de **Login pagina**.

Log in door te klikken op *Login pagina* en je gebruikersnaam en wachtwoord in te voeren.



The screenshot shows the Publeaks dashboard. At the top left is the 'PUB LEAKS UW INZENDINGEN' logo. At the top right, a yellow box indicates 'U bent ingelogd (receiver)' with a black 'UITLOGGEN' button. On the left, a sidebar contains a blue 'Inzendingen' button and a teal 'Voorkeuren' button. The main area features a table with the following data:

Aantal bezoekers	Werk	Laatste bezoek	Voorbeeld	Bestanden
2	Wednesday, November 6, 2013	Wednesday, November 6, 2013	Korte titel <korte titel> Omschrijving bestanden <omschrijving bestanden>	1

Nadat je bent ingelogd toont de website de verschillende tips die je hebt ontvangen.

Klik op het getal dat onder *Toegang* staat om de desbetreffende tip te bekijken.

Uitleg van de verschillende kolommen:

- *Aantal bezoekers*: Het aantal maal dat deze tip door die media organisatie is bekeken.

- *Werk*: De datum waarop de tip is ingediend.
- *Laatste bezoek*: De datum waarop je de tip voor het laatst hebt bekeken.
- *Voorbeeld*: Korte informatie over de inhoud van de tip.
- *Bestanden*: Het aantal bestanden dat in de tip is geüpload.

U bent ingelogd
(receiver)

UITLOGGEN

STATUSOVERZICHT VERZONDEN DOCUMENTEN

Categorie details [klik om te sluiten](#)

een misstand

This this has been submitted at Wednesday, November 6, 2013

Korte titel (Geef een korte titel.)

<korte titel>

Omschrijving bestanden (Geef een zo volledig mogelijke omschrijving van de bestandstypen.)

<omschrijving bestanden>

Volledige beschrijving (Geef een zo volledige omschrijving van de documenten.)

<volledige beschrijving>

Reacties

REAGEER

Bestanden

[Toon alleen de bestanden die nog niet gedownload zijn](#)

Ⓢ

DOWNLOAD (2/5)

bestand.png.pgp

[Laat de sha256 checksums zien](#)

Lijst ontvangers

Naam	Omschrijving	Aantal bezoekers
Greenhost		2

Op de statusoverzicht pagina staat alle relevant informatie over de ingezonden tip:

- *Categorie details*: Op dit moment is er slechts één categorie.
- *Korte titel*: De titel die de tipgever aan upload heeft gegeven.
- *Omschrijving bestanden*: Omschrijving van de bestanden door de tipgever.
- *Volledige omschrijving*: Omschrijving van de tip door de tipgever.
- *Bestanden*: De bestanden die de tipgever heeft gestuurd en hoe vaak ze

zijn gedownload.

N.B. Bestanden kunnen maximaal 3 keer worden gedownload.

- *Reacties*: Een lijst van reacties van zowel de journalisten als van de tipgever.

Een reactie geven kan door in het lege veld te schrijven en te klikken op Voeg een commentaar toe.

N.B. De tipgever krijgt geen meldingen, hij moet zelf kijken of er (nieuwe) berichten zijn.

N.B. Niet alleen de tipgever, maar ook de andere ontvangers kunnen deze reacties lezen.

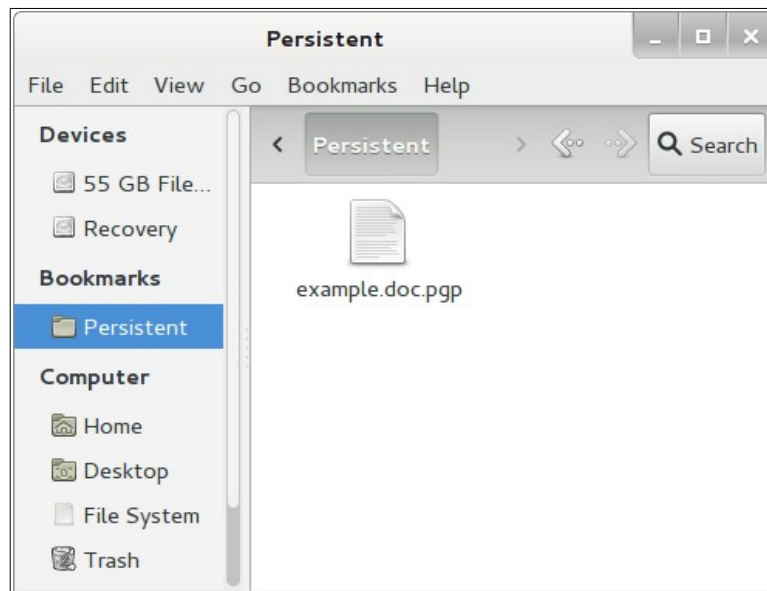
- *Lijst ontvangers*: Een overzicht van welke media deze tip hebben ontvangen en hoe vaak die desbetreffende media de tip hebben bekeken.

Decrypten van een toegezonden bestand

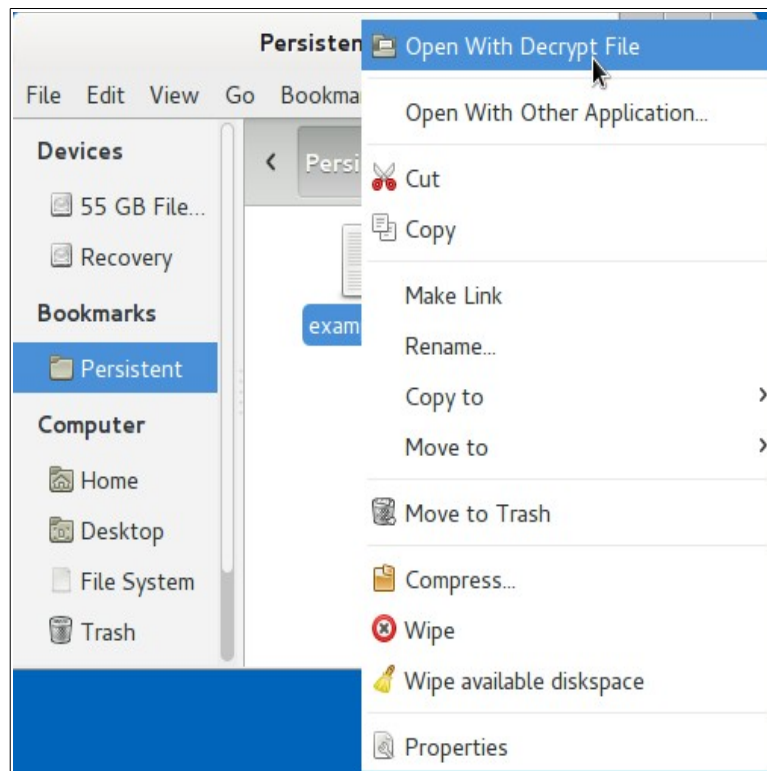
Download het bestand dat je wilt decrypten en sla dit op je laptop op in de map *Persistent*.

N.B. Bestanden die niet in de map *Persistent* worden opgeslagen verdwijnen als de laptop wordt herstart.

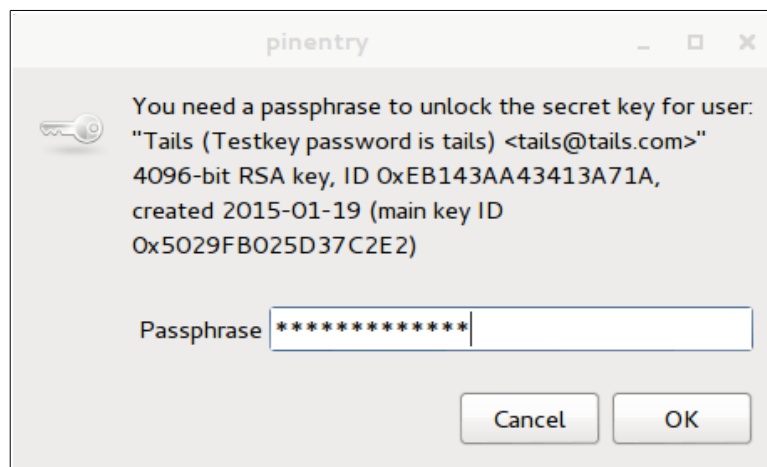
Open de filebrowser, bijvoorbeeld door op de map *Home* op de desktop te klikken.



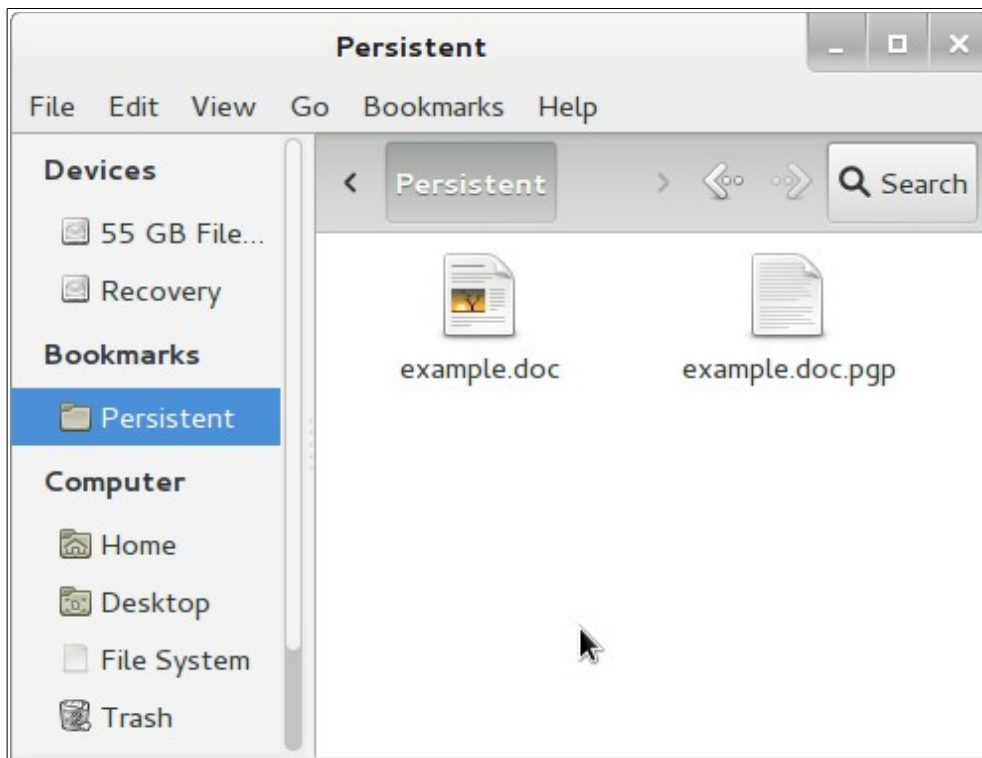
N.B. De bestanden die encrypt zijn met PGP hebben meestal de extensie .pgp, maar dat hoeft niet het geval te zijn.



Rechtermuisklik op het bestand dat je wilt decrypten.



Voer het wachtzin van je PGP-key in en klik op OK.



Kies eventueel de locatie waar je het gedecrypte bestand op wilt slaan.

Metadata verwijderen van bestanden

In bestanden staat vaak metadata over de gebruiker die het bestand heeft gemaakt of bewerkt. Deze gegevens zouden mogelijkheid de identiteit van de tipgever kunnen verraden. Daarom is het verstandig om de metadata en andere herkenbare informatie van bestanden eerst te verwijderen voordat ze elders, buiten deze versleutelde laptops, worden gebruikt.

N.B. Dat een bestand geen metadata meer bevat, betekend natuurlijk niet dat de inhoud van het bestand niet alsnog de identiteit van de tipgever kan verraden.

Let daarom ook op mogelijke (onzichtbare) watermerken in de documenten. Het gaat hier te ver om uitgebreid op watermerken in te gaan, maar wees bewust van het bestaan en wees voorzichtig.

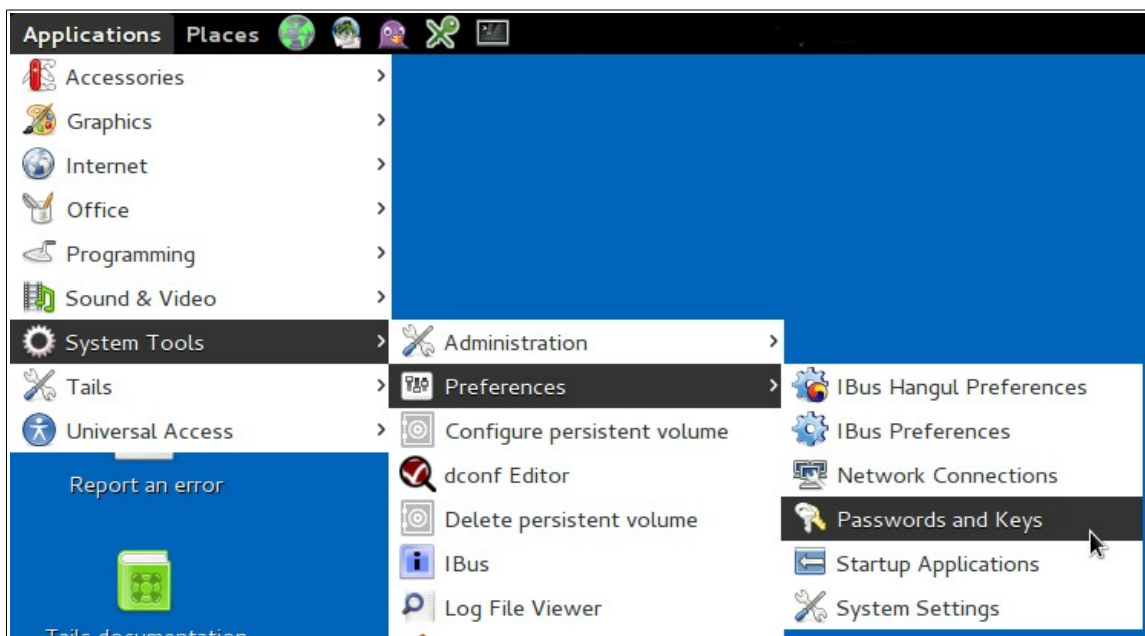
Backups

Zoals bij alle techniek is ook hier nooit uit te sluiten dat er een keer een defect in de apparatuur op zal treden. Daarom worden door ons dagelijks backups van de servers gemaakt. Voor de laptops ligt die verantwoordelijkheid bij de journalisten die een laptop in beheer hebben. Het is aan de journalisten zelf om te bepalen of het nodig is om deze backup wel of niet te maken.

N.B. Wees voorzichtig met backups van gevoelige data!

Alle data die op de usb-stick staat is veilig opgeslagen in een versleuteld volume. Als er een backup wordt gemaakt, dan is het mogelijk dat deze op een onversleutelde plek wordt opgeslagen. De PGP sleutel is zelf ook beveiligd met een wachtwoord, maar andere data op de usb-stick heeft deze extra beveiliging niet. Het is daarom verstandig om zeer voorzichtig te zijn bij het maken van een backup van gevoelige data.

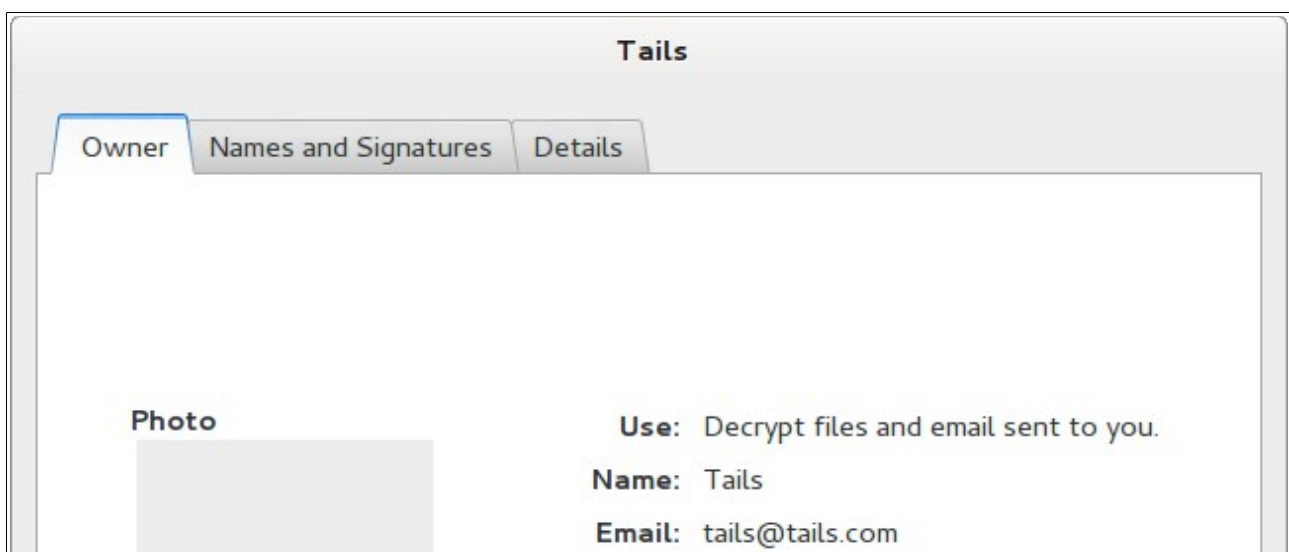
Backup maken van de PGP sleutel



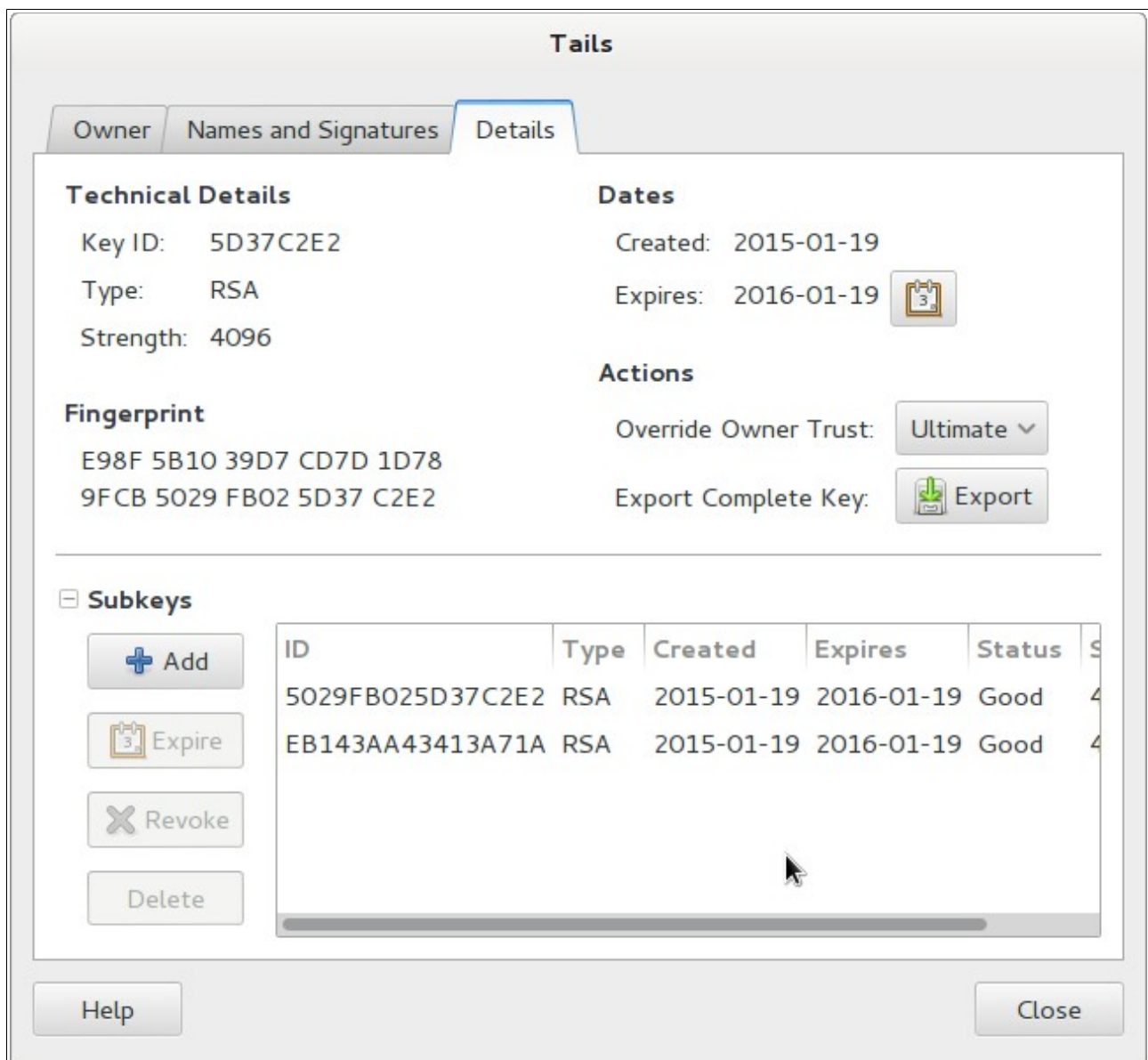
Start *Passwords and Keys*



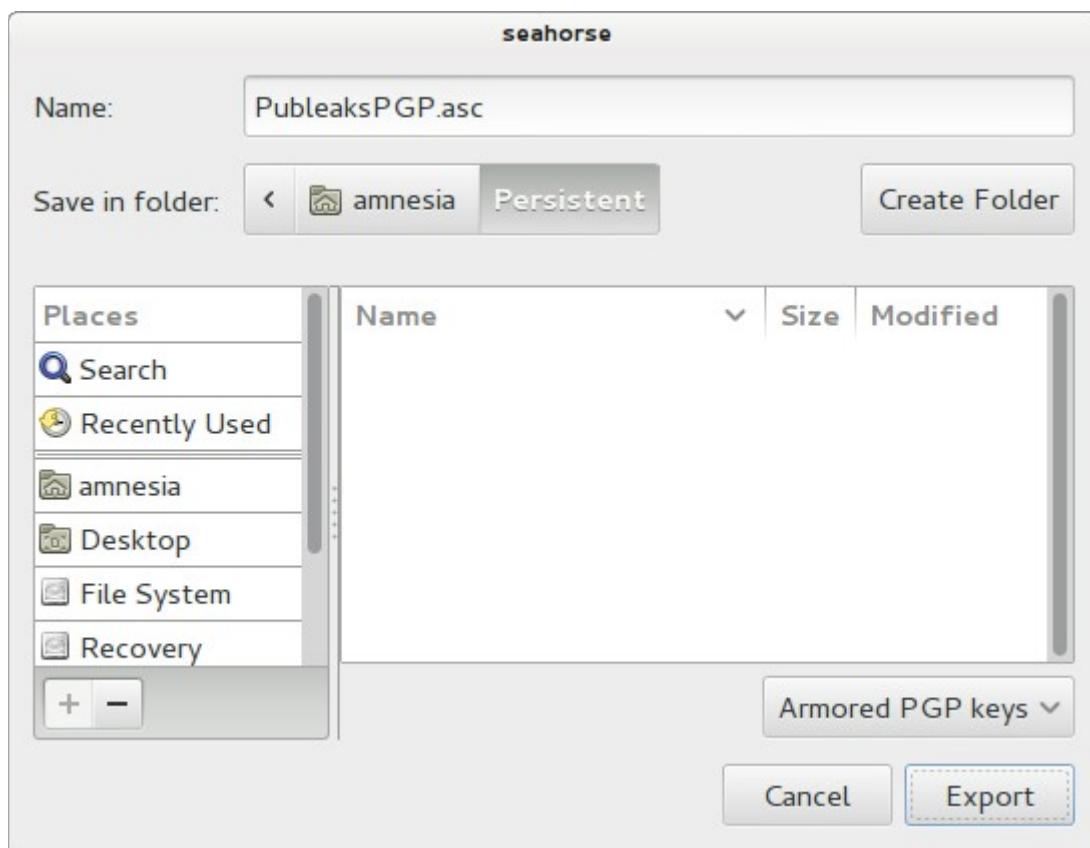
Dubbelklik uw *Personal PGP key*



Klik op *Details*



Klik op *Export* (daarmee exporteert u de *Complete Key*)



Selecteer waar u de keys op wilt slaan, geef het een naam en klik op *Export*

Updaten van Tails

Zoals bij elk systeem worden ook voor Tails met enige regelmaat nieuwe versies gemaakt. Deze nieuwe versies kunnen verbeteringen en uitbreidingen bevatten, maar belangrijker is dat ze mogelijk ook beveiligingsproblemen oplossen. Het is dus belangrijk om zoveel mogelijk de laatste versie van Tails te gebruiken.

Sinds Tails 1.2 zoekt Tails automatisch naar updates wanneer verbinding met internet wordt gemaakt. Daarna kunt u kiezen of u eventuele updates wel of niet wilt installeren.

N.B. Om automatisch te kunnen updaten heeft Tails minimaal 2GB intern geheugen nodig. Niet alle laptops die door Publeaks zijn uitgegeven beschikken over genoeg geheugen en kunnen dus (nog) niet automatisch updaten.