

# Ahtapot

## Şifreli Mail Gönderme/Alma

### Thunderbird & Enigmail & GPG

## Bileşenler

**Thunderbird:** Açık kaynak masaüstü e-posta gönderme/alma istemcisidir.

**Enigmail:** Thunderbird eklentisidir. Bu eklenti ile GPG aracını kullanarak şifreli e-posta gönderilir ve şifrelenmiş e-postalar okunabilir. Bu araç ile anahtarlarınızı yönetebilir ve anahtar sunucularına sorgu yapabilir ve kendi anahtarınızı anahtar sunucularına gönderebilirsiniz.

**GNU Privacy Good(GPG):** OpenPGP standartlarına uygun olarak kendi anahtar çiftini oluşturmak için GNU Project tarafından geliştirilmiş anahtarlama aracıdır. Gizli ve genel olmak üzere iki anahtar oluşturulur.

**Gizli Anahtar(PrivateKey):** Çok dikkatli bir şekilde saklanması gereken ve başka birileri ile paylaşılması gereken bir anahtardır. Anahtar üretilirken kullanılan şifre ile gelen/giden e-postalar okunabilir. Bu şifrenin de çok dikkatli seçilmesi ve unutulmaması gerekmektedir.

**Genel Anahtar(PublicKey):** E-posta gönderdiğiniz alıcılarınızın, sizden gelen e-postaları okuyabilmesi için ihtiyacı olduğu anahtardır. Bu anahtarı sizden e-posta eki olarak temin edebilirler veya anahtar sunucularında paylaşıldı ise buralardan arama yaparak bulabilirler.

**Anahtar Sunucuları(SKS):** GPG aracı veya **Enigmail**'i kullanarak üretilen kişisel anahtar çiftinizin **Genel Anahtar**ının paylaşıldığı ve saklandığı sunuculardır. Bu sunuculara **Genel Anahtar**ınızı göndererek sizden şifreli e-posta alan kişiler, gönderdiğiniz e-postayı okuyabilmek için bu sunucularda arama yapar ve **Genel Anahtar**ınıza ulaşırlar.

**Pgpkeyserver-lite:** SKS sunucularında web tabanlı **Genel Anahtar** araması yapılmasını sağlayan uygulamadır. Bu web uygulaması arayüzünden kendi **Genel Anahtar**ınızı da yükleyebilirsiniz.

## Enigmail Kurulumu

Enigmail GPG aracını kullanarak anahtar çiftinizi oluşturur.

GPG aracı neredeyse bütün Linux dağıtımlarında yüklü gelmektedir.

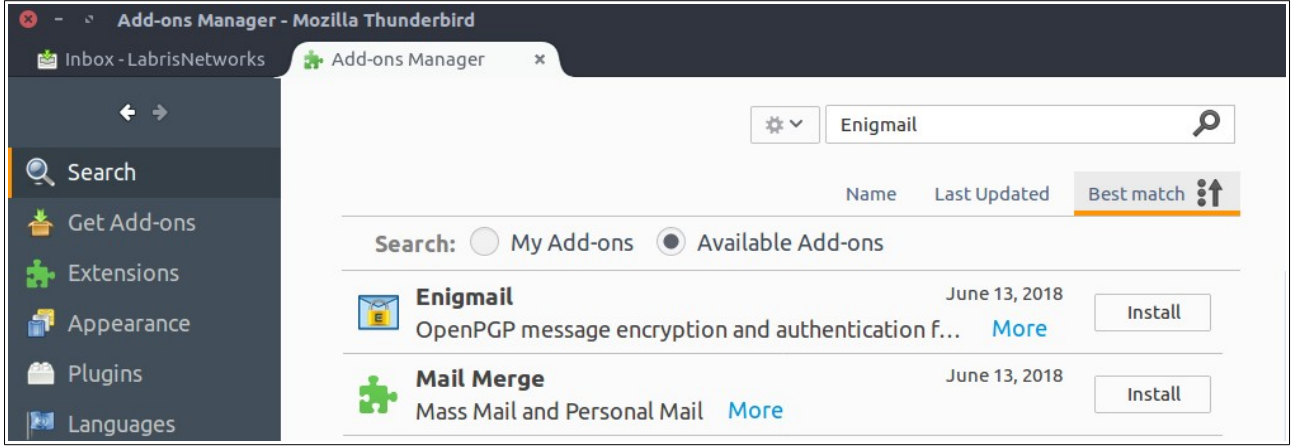
Windows için aşağıdaki linkteki "Simple installer for GnuPG modern" (GnuPG modern için basit kurucu) linkinin yanındaki "Download" (İndir) butonuna tıklayarak GPG kurucusunu indirebilirsiniz.

<https://gnupg.org/download/index.html#sec-1-2>

Kurulum için thunderbird eklenti yöneticisi menüsüne girilir.

1- Araçlar > Eklentiler

2- Sol taraftak **Eklentiler** menüsüne basılır ve sağ üst köşede arama alanına **Enigmail** yazılır.

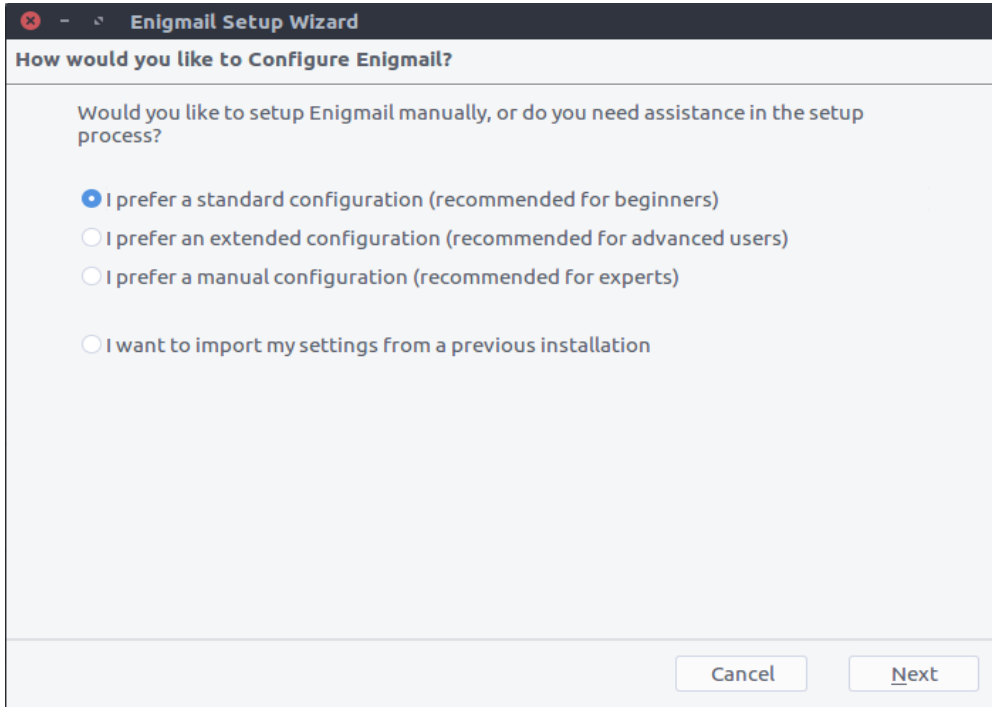


3- Enigmail eklentisi **Kur** butonuna basılarak kurulur.

4- Eklenti kurulduktan sonra thunderbird yeniden başlatılır ve kurulum sihirbazı ile ilk yapılandırma yapılır.

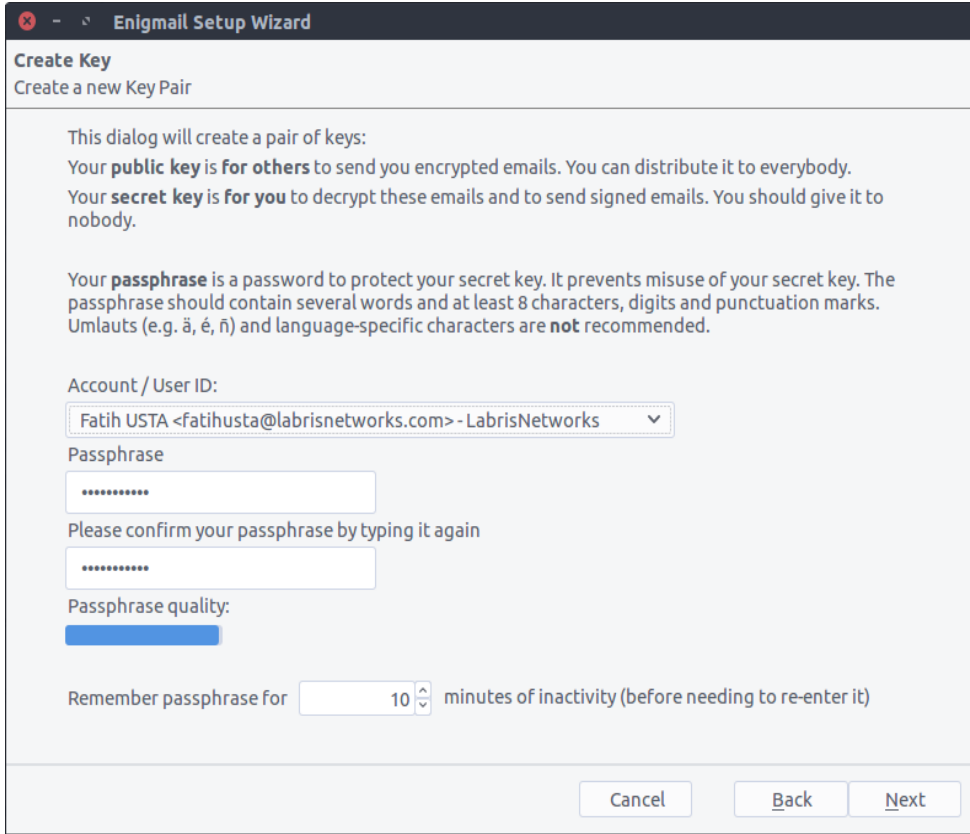
## Enigmail kurulum sihirbazı ayarları ve Anahtar Üretme

1- Enigmail kurulum sihirbazında aşağıdaki seçenek seçilir ve **next** denir.



**Not:** Bu işlemten sonra ubuntu sistemlerde GPG'yi bulamadığına veya versiyonu uyuşmadığına dair bir hata verir ise `/usr/bin/gpg2` yolu gösterilir.

2- E-posta hesabınız için anahtar oluşturulur. Bunun için **güçlü** bir **şifre** belirlenir ve **next** denir.



**Create Key**  
Create a new Key Pair

This dialog will create a pair of keys:  
Your **public key** is **for others** to send you encrypted emails. You can distribute it to everybody.  
Your **secret key** is **for you** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your secret key. It prevents misuse of your secret key. The passphrase should contain several words and at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Account / User ID:  
Fatih USTA <fatihusta@labrisnetworks.com> - LabrisNetworks

Passphrase  
.....

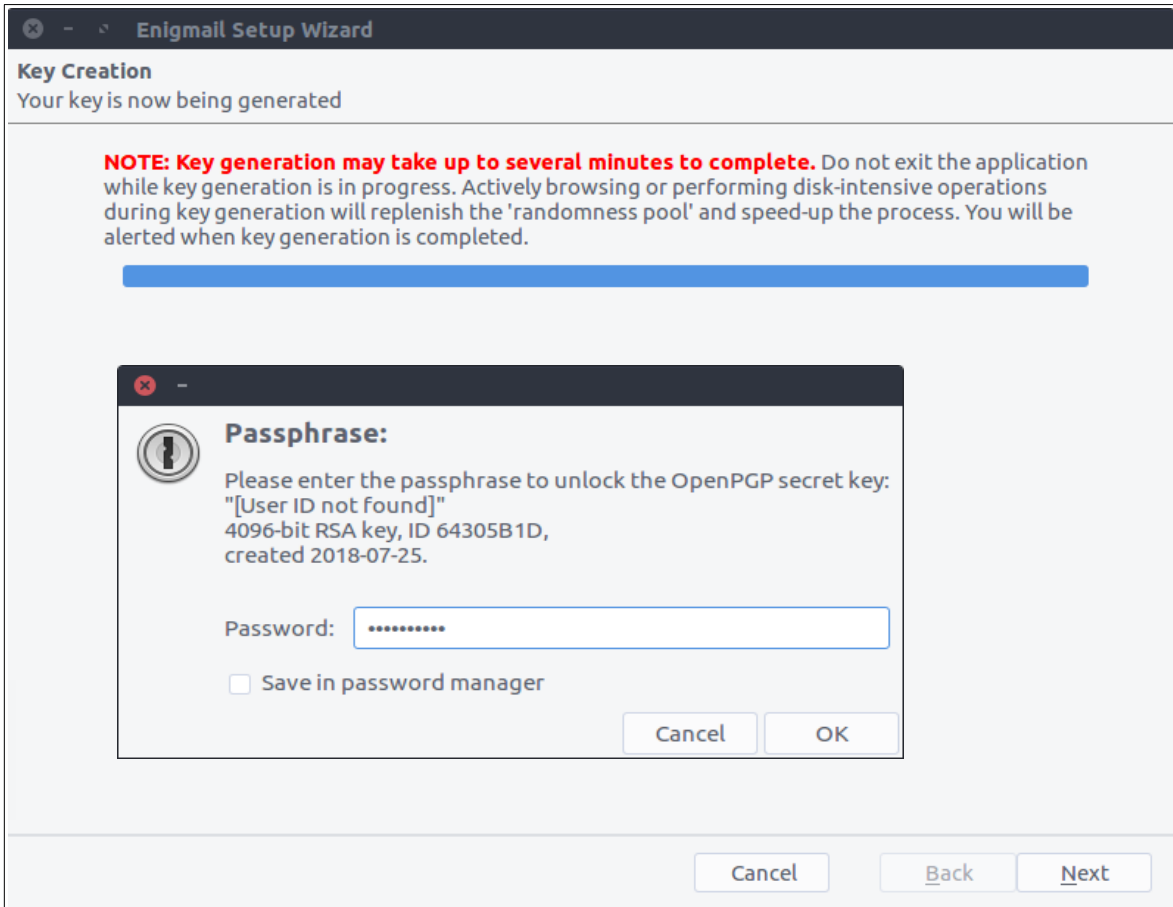
Please confirm your passphrase by typing it again  
.....

Passphrase quality:  
.....

Remember passphrase for 10 minutes of inactivity (before needing to re-enter it)

Cancel Back Next

3- Anahtar oluşturma aşamasında tekrar parolanızı giriniz.



**Key Creation**  
Your key is now being generated

**NOTE: Key generation may take up to several minutes to complete.** Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

.....

**Passphrase:**  
Please enter the passphrase to unlock the OpenPGP secret key:  
"[User ID not found]"  
4096-bit RSA key, ID 64305B1D,  
created 2018-07-25.

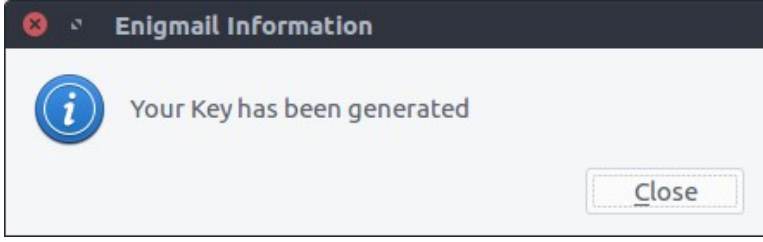
Password: .....

☐ Save in password manager

Cancel OK

Cancel Back Next

4- Anahtar oluřturma iřlemi bařarılı bir řekilde tamamlandıęında ařaęıdaki mesaj grntlenir.



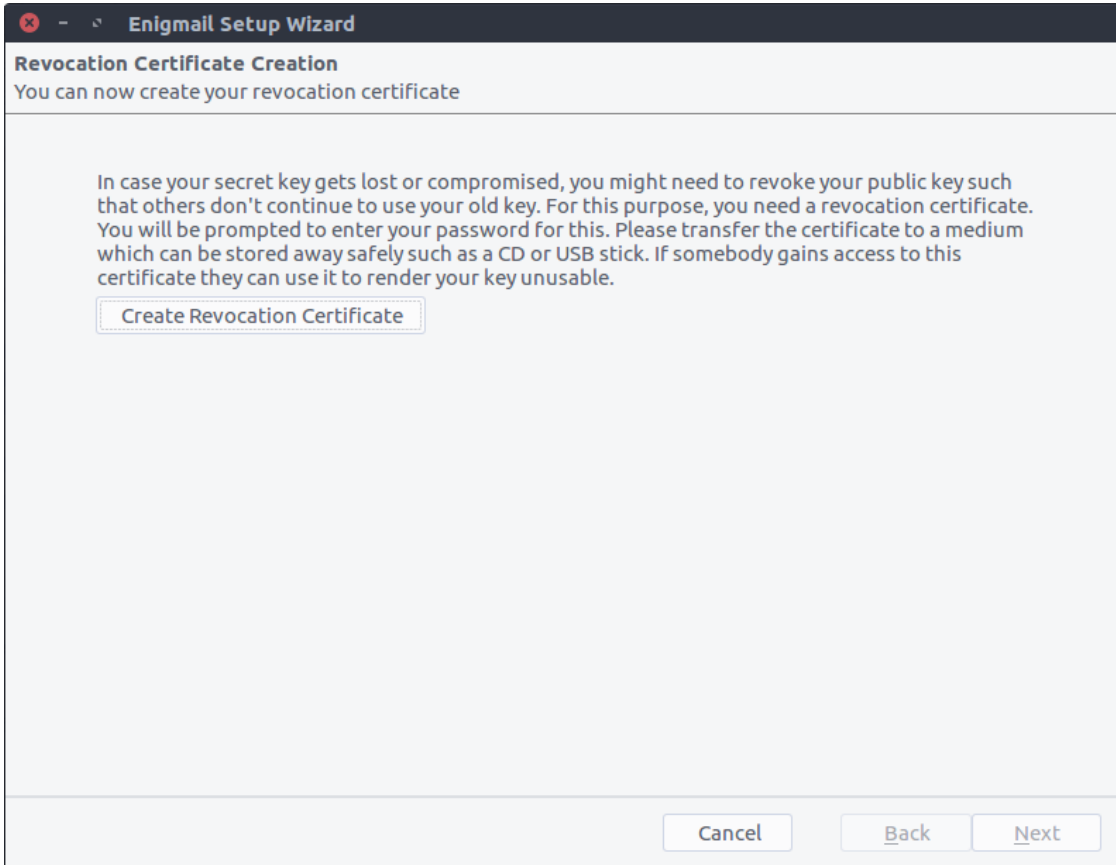
5- **Next** butonuna basılır ve iptal sertifikası(Revocation Certificate) oluřturulur.

Bir iptal sertifikası (revocation certificate) retmelisiniz ki, belli bir anahtar geerlilięini yitirdięinde bařkaları haberdar edebilesiniz. Bu řu durumlarda olabilir:

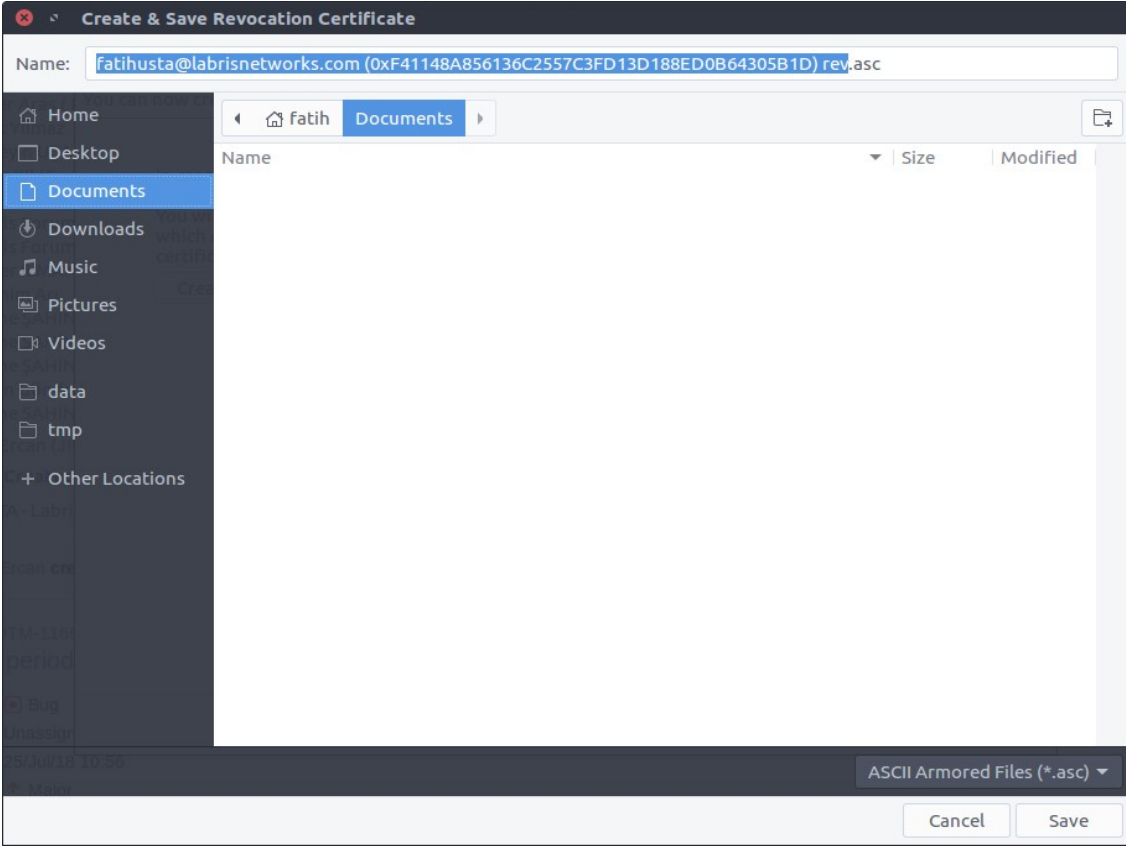
- Anahtar iftini kullanmayı bıraktıęınızda
- Gizli anahtarı kaybettięinizde
- Gizli anahtarın parolasını unuttuęunuzda
- Gizli anahtarın ele geirildięine veya bařkalarıyla paylařıldıęına inandięınızda.

Genel anahtarınızı bir anahtar sunucuya yklemeyi planlıyorsanız bir iptal sertifikası retmeniz zellikle **nemlidir**. Bir anahtarı ykledikten sonra bařka bir řekilde "**silmenin**" yolu yoktur ve eski ya da gzden ıkarılmıř anahtarların bir anahtar sunucuda bekletilerek insanların kafasını karıřtırmasını istemezsiniz.

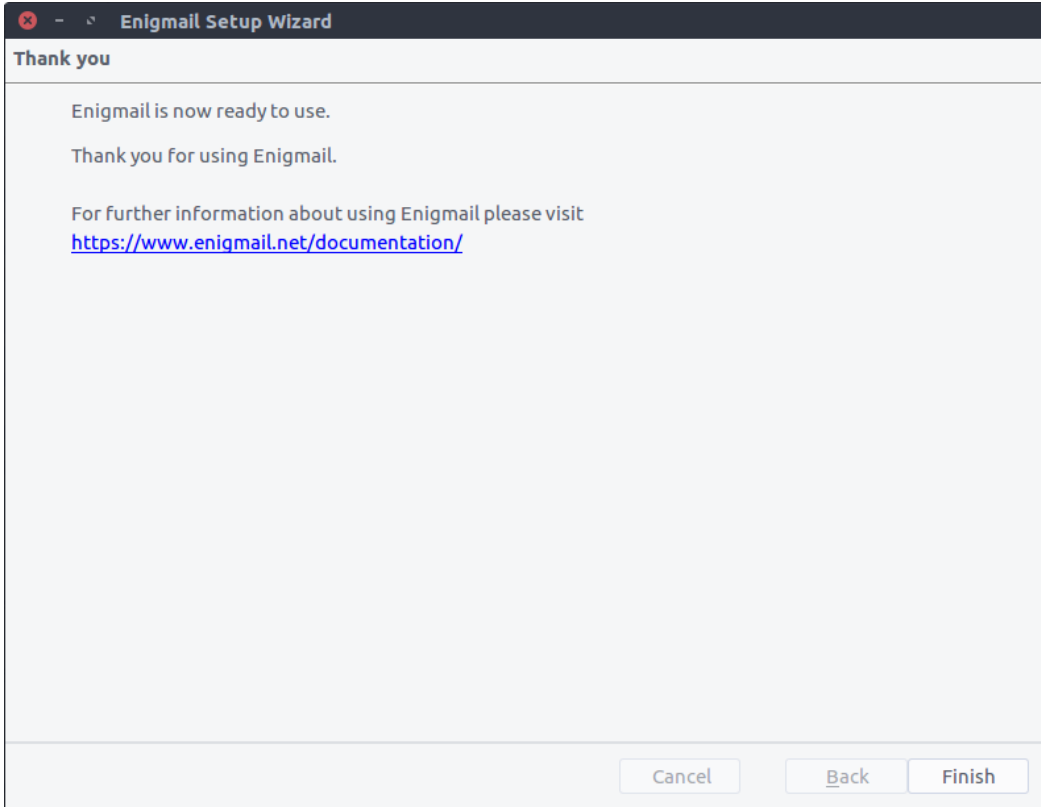
Create Revocation Certificate butonuna basılır.



6- Sertifikanın kayıt edileceği dizin seçilir ve **save** denir. Bu işlemden sonra çıkan mesaja **close/ok** denir. Eğer şifre sorarsa başta belirlenen şifre girilir.



7- Kurulum tamamlandıktan sonra **Finish** butonuna basılır.



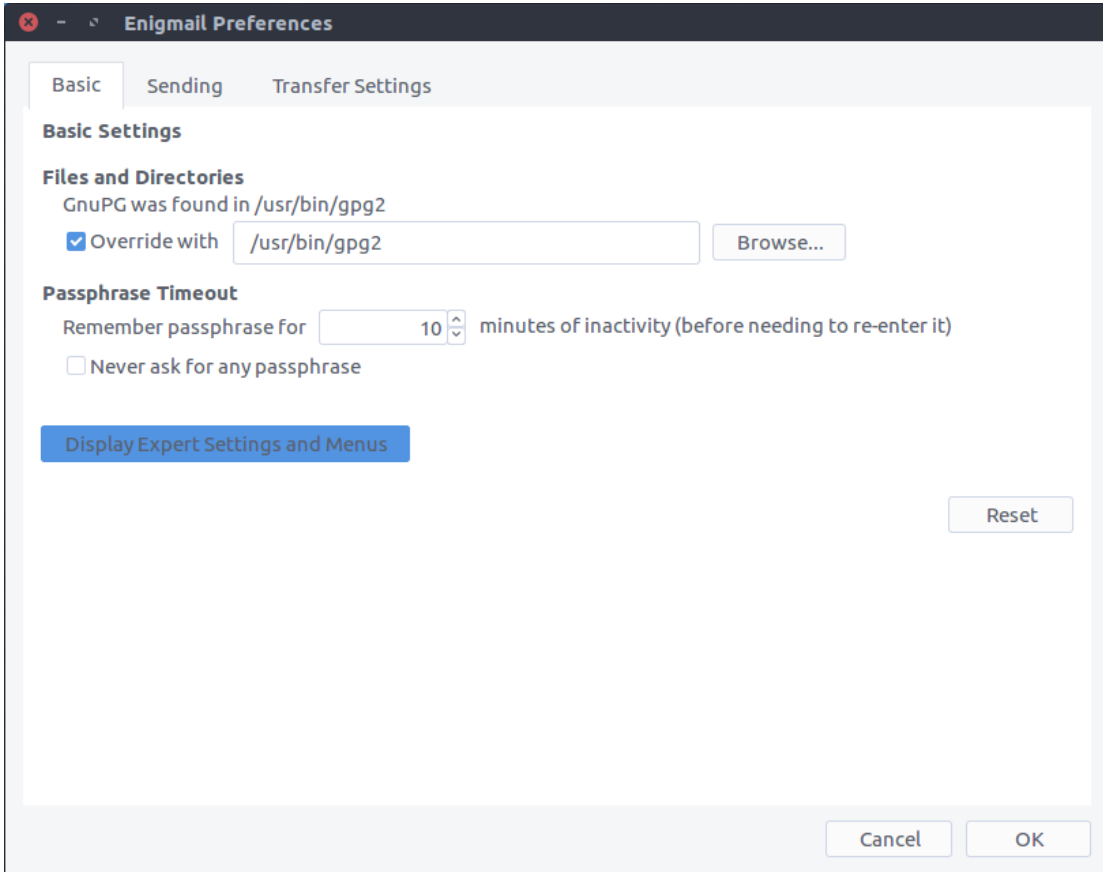
# Enigmail Anahtar Sunucusu(SKS) Ayarları

Enigmail ayarlarında anahtar sunucusu tanımlarını yaparak istenilen sunuculardan sorguların yapılması ve size ait **Genel Anahtarlarınızın** bu adreslere yüklenmesi sağlanabilir.

Bunun için thunderbird menu çubuğundan aşağıdaki yol takip edilerek enigmail ayarlarına ulaşılır.

1- Menü Çubuğu>Enigmail>Preferences

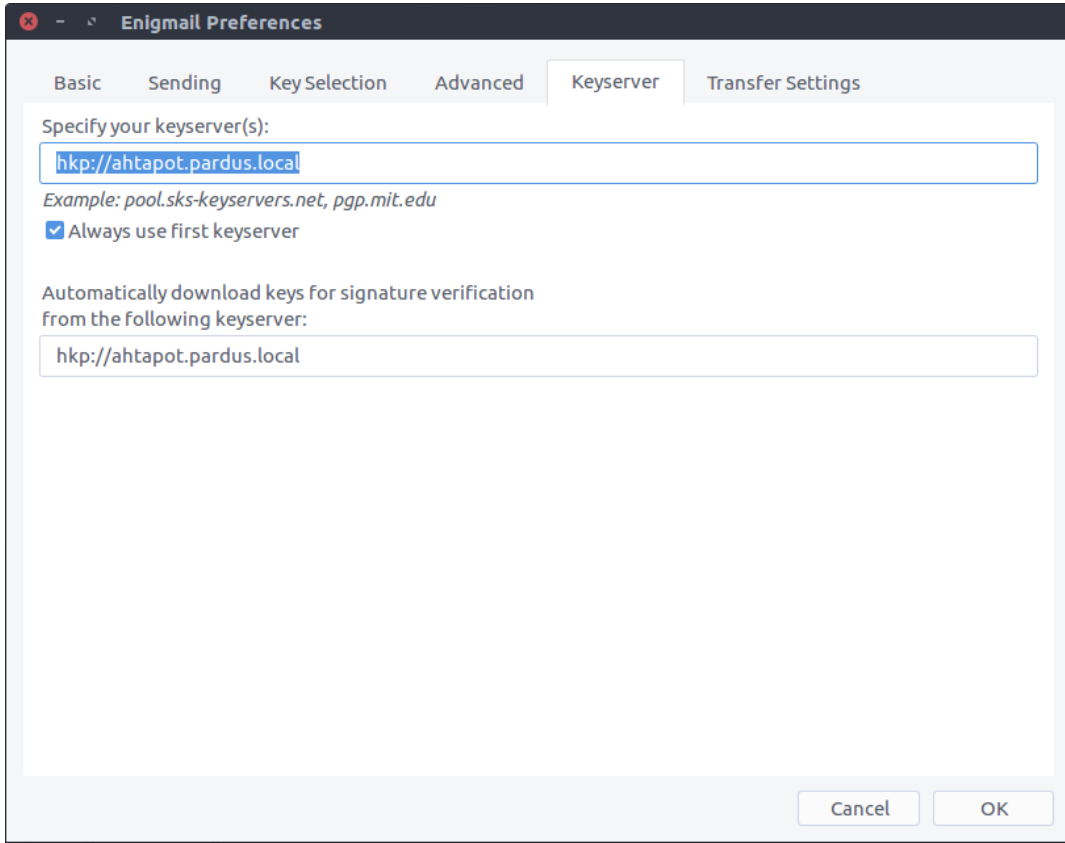
2- Gelişmiş özellikler açılır. Bunun için **Basic** tabında **Display Expert Settings and Menus** butonuna basılır.



3- Yeni menüde **Keyserver** tabına basılır. Daha sonra **anahtar sunucusu(sks)** tanımları aşağıdaki gibi yapılır. Sunucudan otomatik indirme kısmı opsiyonel olarak tanımlanır.

**Anahtar sunucusu adresi(fqdn):** hkp://ahtapot.pardus.local

Not: Anahtar sunucusu adresinin isim çözümlemesinin doğru yapıldığından emin olunur.

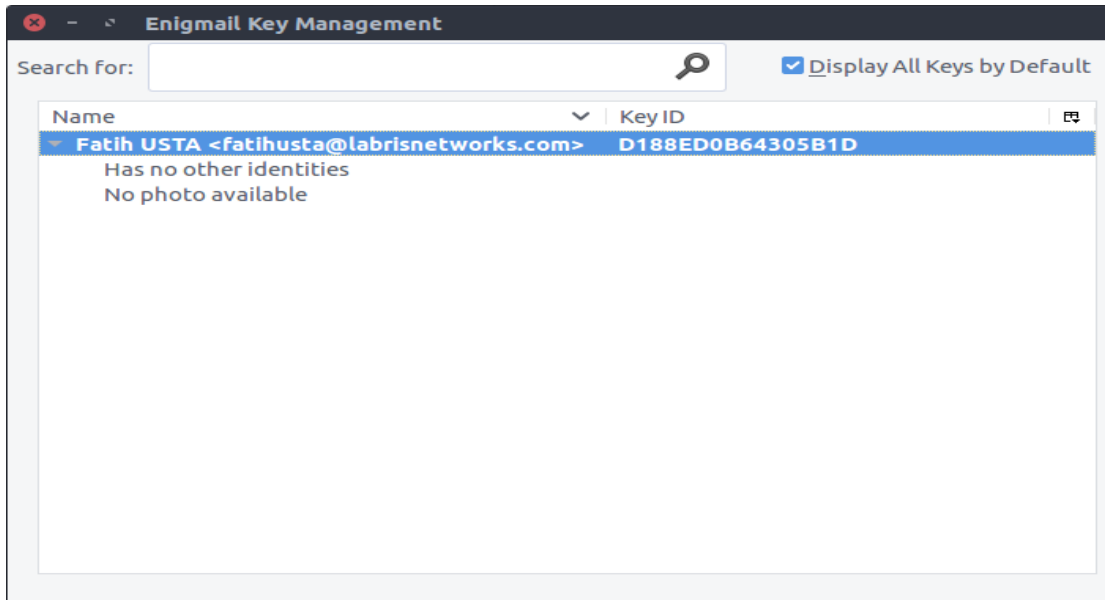


## Anahtar Özelliklerini görüntüleme ve Yönetme

Enigmail anahtar yönetimi menüsünde **Genel Anahtarlar** görüntülenir. Bu menüden **Genel Anahtar**ınızı anahtar sunucusuna gönderme, silme, devredışı bırakma, iptal etme vb. işlemler yapılabilir.

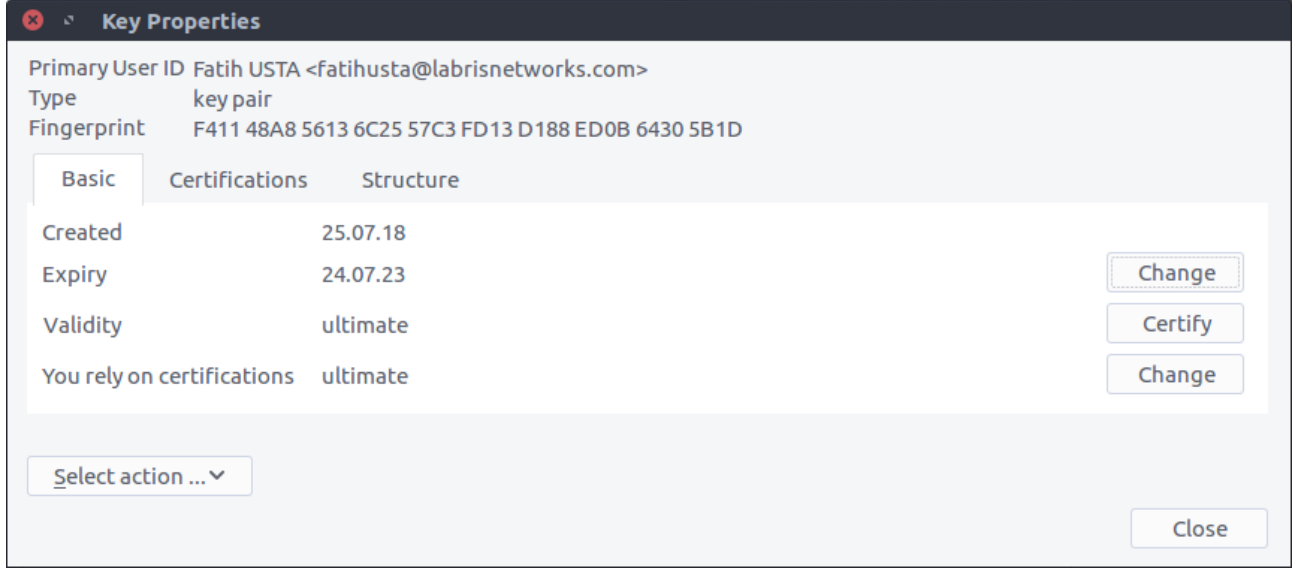
Bunun için; Menü Çubuğu>Enigmail>Key Management

Bu ekranda menü çubuğunu kullanarak veya ilgili anahtarın üzerine sağ klik yaparak işlemler yapılabilir.



## Anahtar Özellikleri

Anahtar özelliklerini görüntülemek için çift tıklanabilir veya sağ klik > key properties veya menu çubuğundan view > key properties denebilir.



The image shows a 'Key Properties' dialog box with a dark header. It contains the following information:

- Primary User ID: Fatih USTA <fatihusta@labrisnetworks.com>
- Type: key pair
- Fingerprint: F411 48A8 5613 6C25 57C3 FD13 D188 ED0B 6430 5B1D

Below this information are three tabs: 'Basic' (selected), 'Certifications', and 'Structure'. The 'Basic' tab contains a table with the following data:

Created	25.07.18	
Expiry	24.07.23	<button>Change</button>
Validity	ultimate	<button>Certify</button>
You rely on certifications	ultimate	<button>Change</button>

At the bottom left is a 'Select action ...' dropdown menu, and at the bottom right is a 'Close' button.

## Genel Anahtarın E-posta Eki Olarak Gönderilmesi

Şifreli e-posta gönderilmeden önce **Genel Anahtar**ın alıcılar ile paylaşılması gerekir.

E-posta eki olarak genel anahtarınızı göndermek için;

1- Yeni posta oluşturulur ve alıcı adresi yazılır. Varsa iletmek istediğiniz mesaj e-posta içerisinde belirtilir.

2- Mail gönderilmeden önce Genel Anahtar Ek olarak eklenir.

Bunun için; Menu Çubuğu > Enigmail > **Attach My Public Key** işaretlenir.

3- Mail gönderilir.

4- **Alıcı** mailin ekinde yer alan Genel Anahtar Anahtar yönetimi uygulamasına dahil eder.

Bunun için; Gelen mailin eki üzerinde **sağ klik yapılır** ve **Import OpenPGP key** denir ve çıkan mesaja **OK** denir.

Not: Alıcının enigmail veya benzeri bir araç kullanması gerekir.

## Genel Anahtarın Tanımlı Anahtar Sunucularına Gönderilmesi

Şifreli e-postaların alıcılar tarafından okunabilmesi için **Genel Anahtar** e-posta eki olarak alıcılara yollanabilir veya anahtar sunucularına yüklenerek herkesle paylaşılabilir.

Bunun için **Key Management** menüsünde ilgili anahtarınıza sağ klik yaparak **Upload Public Keys To Keyserver** seçeneğine basılır. (Menü Çubuğu>Keyserver>Upload Public Keys)



## Anahtar Sunucuları ile Senkronizasyon

Tanımlı anahtar sunucularındaki bütün anahtarları senkronize etmek için aşağıdaki adımlar takip edilir.

Not: Genele açık sunuculardaki veri tabanı boyutu 20GB civarında olabilir.

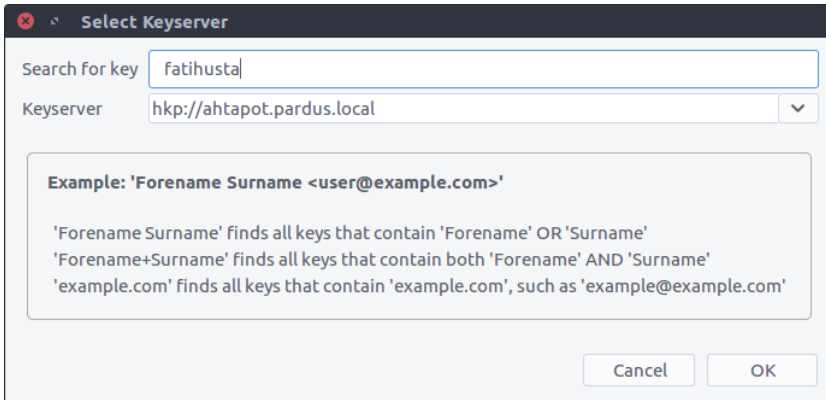
Bunun için **Key Management** menüsünde sağ klik yaparak **Refresh Public Keys From Keyserver** seçeneğine basılır. (Menü Çubuğu>Keyserver>Refresh All Public Keys)

## Anahtar Sunucusunda Genel Anahtar Arama ve Ekleme

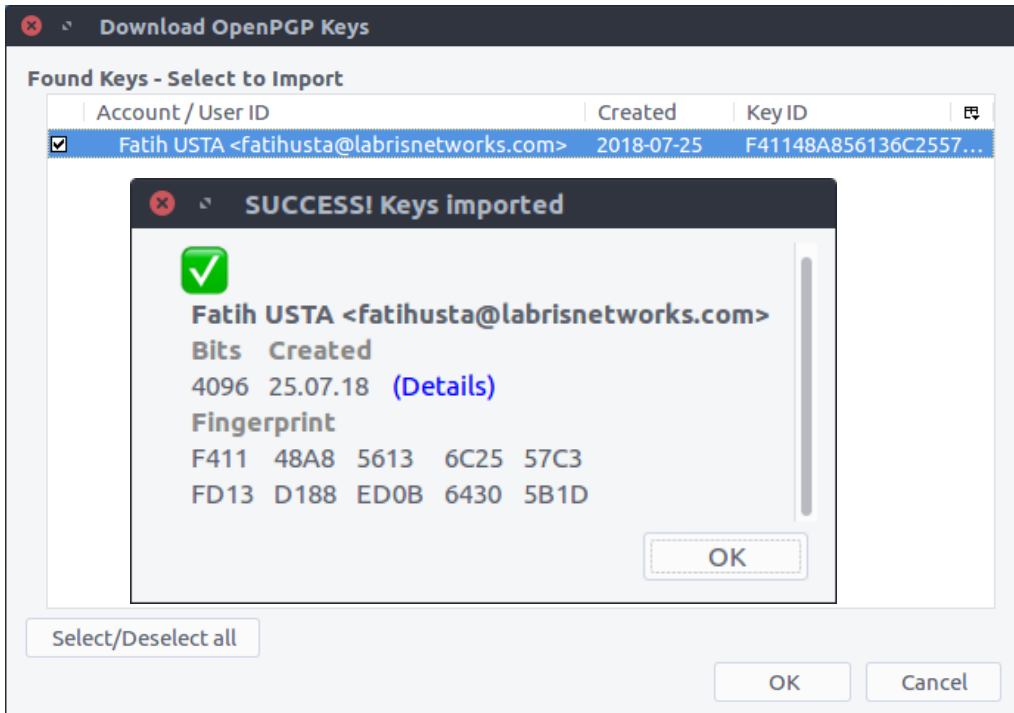
Anahtar sunucusundaki bütün Genel Anahtarları dahil etmek yerine sadece ilgili gönderici'ye ait **Genel Anahtar** dahil edilebilir.

Bunun için; Key Management > Menü Çubuğu > Keyserver > Search For Keys

Arama alanına göndericinin e-posta adresi veya adı ve/veya soyadı yazılarak arama yapılır.



Arama sonuçlarında ilgili e-posta adresine ait **Genel Anahtar** Seçilir ve **OK** denir.

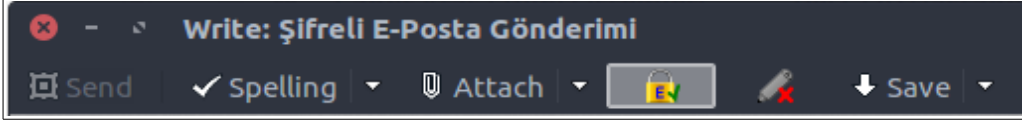


Anahtar başarılı bir şekilde eklendiğinde yukarıdaki gibi görünür. **Details** kısmına basılarak ilgili anahtara ait detaylar görüntülenebilir.

# Şifreli Mail Gönderimi

Şifreli mail gönderimi yapmak için aşağıdaki adımlar izlenir.

- 1- Yeni e-posta oluşturun.
- 2- Alıcıları tanımlanır ve gönderilmesi gereken e-posta yazılır.
- 3- Gönderilmeden önce E-posta gönderme ekranındaki kilit simgesine basılır. Bu sayede giden mail şifrelenmiş olarak gönderilir.



- 4- Mail gönderimi sırasında anahtarınızın şifresini girmeniz gerekir.
- 5- Eğer e-posta imzalanmak isteniyor ise kilit simgesi yanındaki **kalem** simgesine basılır.

Öntanımlı olarak şifreli mail gönderimi için hesap ayarları bölümündeki ayarlar kullanılabilir.

Bunun için; Thunderbird Menü Çubuğu > Edit > Account Settings yolu takip edilir.

Açılan pencerede ilgili hesap için **OpenPGP Security** menüsü seçilir.

Aşağıdaki gibi ayarlar yapılabilir.

