HowTo: YubiKey NEO as PGP smartcard

Our tutorial explains how PGP software works and how you can use PGP to encrypt your mailbox.org e-mails. The reliability of the OpenPGP encryption depends largely on the secrecy and secure storage of your private key. If you use GnuPG on more than one device, someone else could create a copy of your secret private key, especially if you share the device with other users, and if any of them happen to have administrative permissions on the operating system.

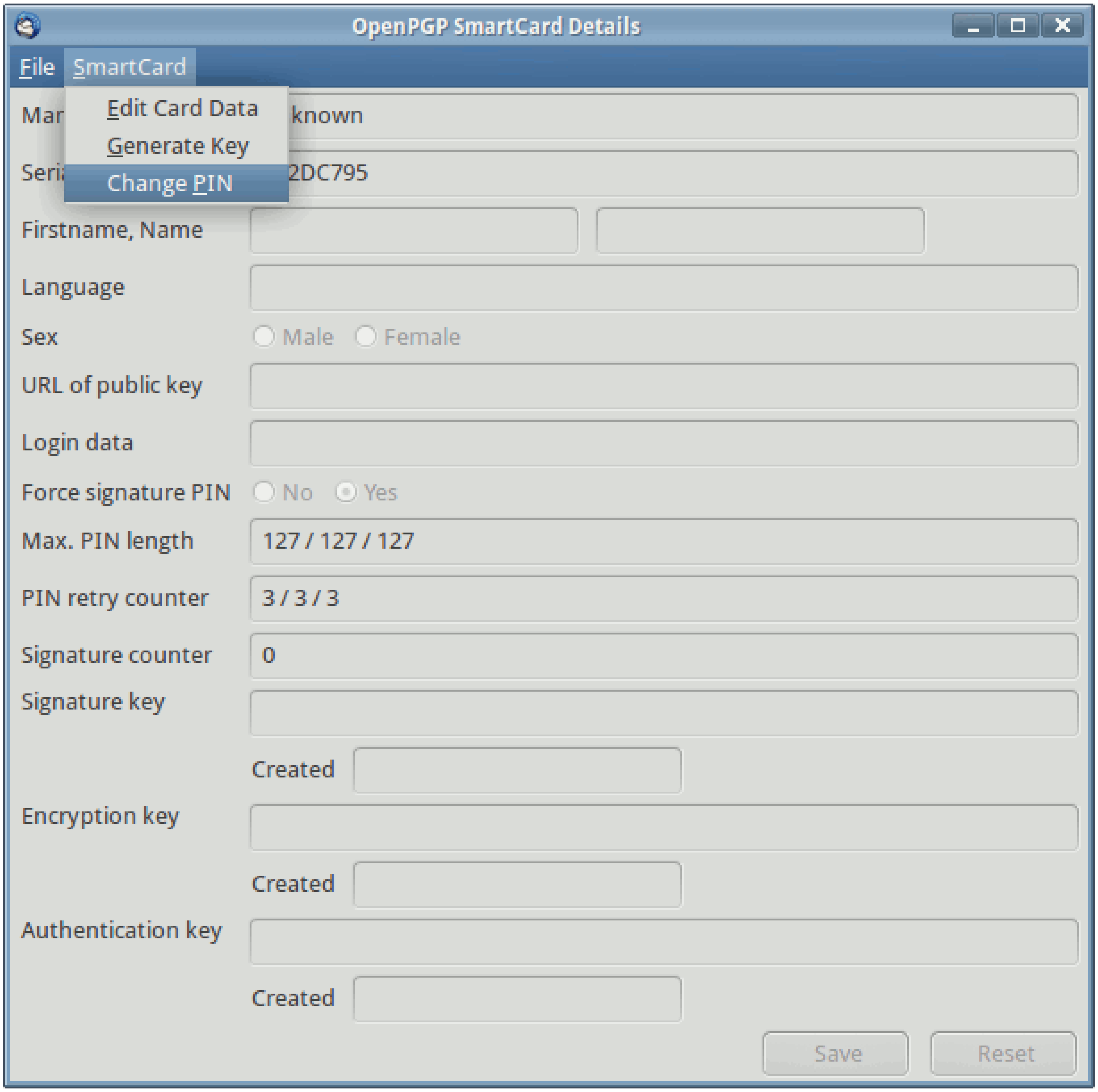
Smartcards facilitate the secure use of GnuPG in such scenarios. Here, the private key is stored exclusively on the smartcard and will never leave its secure environment. Did you know that the **YubiKey 5**, which you can use for logging in securely to mailbox.org with OTP, does already come with a smartcard for OpenPGP included?

Before this smartcard can be used, the related functionality on the YubiKey needs to be enabled first. To do this, you need to download the tool ***ykpersonalize*** from the Yubico Website and install it on your computer. If you are a user of Ubuntu or Fedora, then you should be able to find it in a repository. After the installation is complete, open a command line interface or terminal and run the following command to enable the smartcard:

```
> ykpersonalize -m82
```

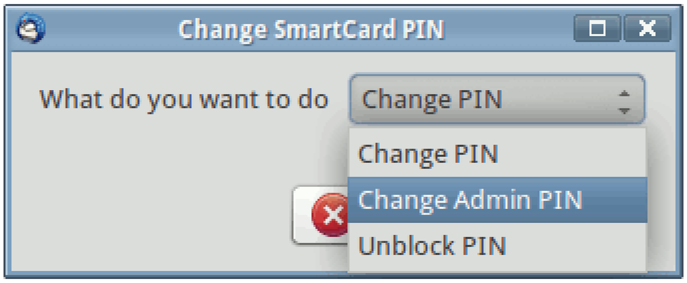
How to manage your smartcard using Thunderbird and Enigmail

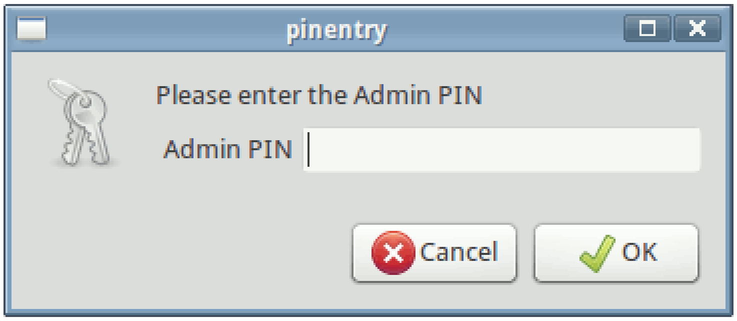
The smartcard on the YubiKey 5 can only be used in connection with a local e-mail client. We recommend Mozilla Thunderbird with the Enigmail add-on enabled. Enigmail is fully compatible with the functionality provided by the smartcard, and you can manage your smartcard settings from the Enigmail menu in Thunderbird.



Mar	known
Seri	2DC795
Firstname, Name	
Language	
Sex	○ Male ○ Female
URL of public key	
Login data	
Force signature PIN	○ No ● Yes
Max. PIN length	127 / 127 / 127
PIN retry counter	3 / 3 / 3
Signature counter	0
Signature key	
Created	
Encryption key	
Created	
Authentication key	
Created	

The first thing to do after enabling the smartcard is to change the existing 6-digit PIN, as well as the 8-digit Admin-PIN. The factory settings for these numbers are **123456** for the PIN and **12345678** for the Admin-PIN.





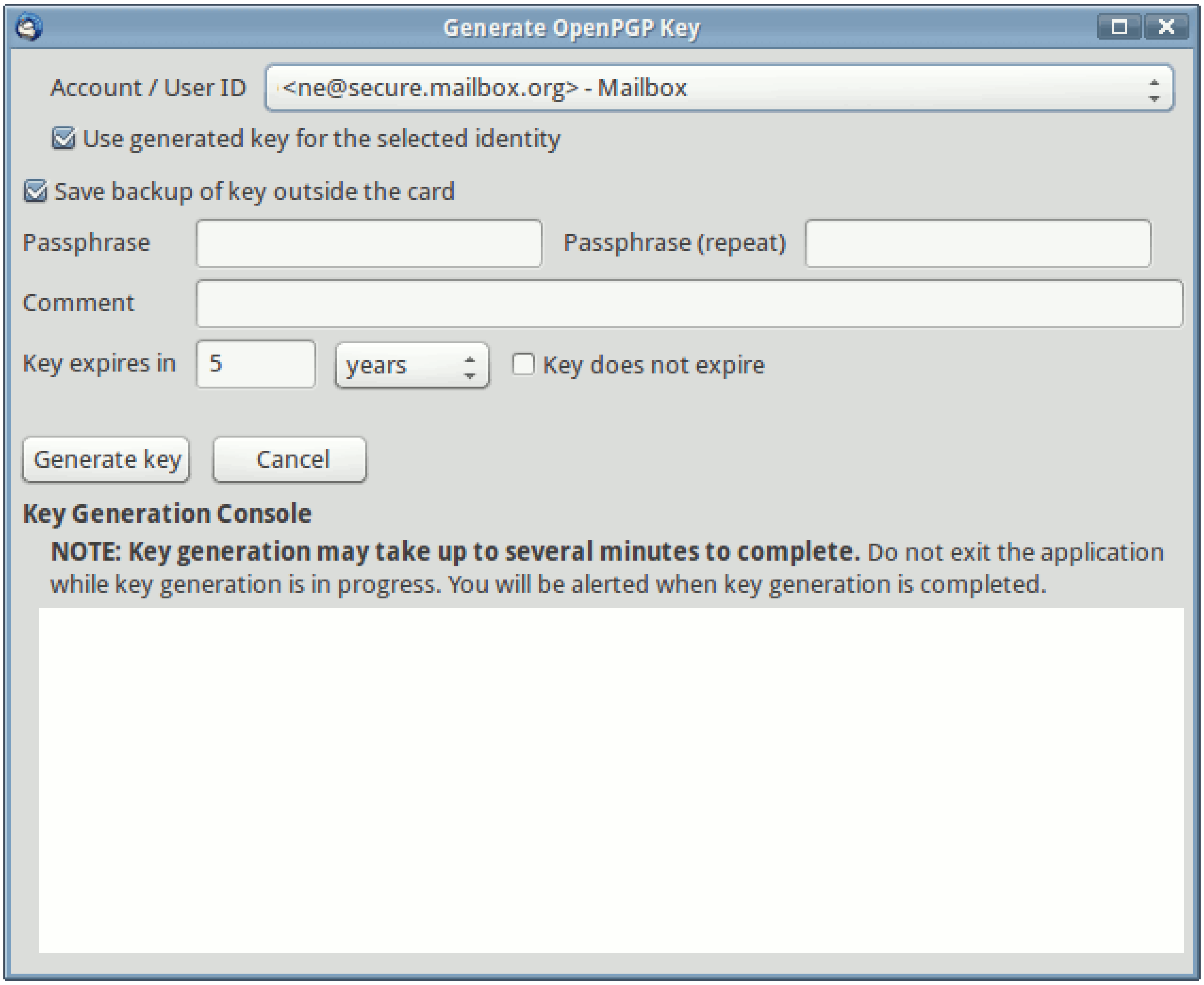
Please enter the Admin PIN

Please note the following security mechanisms on the smartcard:

1. If you enter the wrong PIN three times in a row, the smartcard will be locked automatically. However, it can be unlocked again by entering the Admin-PIN.
2. If you enter the wrong Admin-PIN three times running, the smartcard will be disabled permanently and can no longer be used.

Once you have chosen a new PIN and Admin-PIN, the smartcard can be personalised further. For instance, you can enter a name, or the download URL for your public PGP key.

The last remaining step is to generate the relevant keys on the smartcard. Select an e-mail account and create the keys for this account. Immediately afterwards, create a backup of your keys to store someplace else. This is important because you might need another copy of the keys to set up a replacement YubiKey NEO, in case your current smartcard gets damaged. **You must do the backup at this stage because later any direct access to the private key on the smartcard will be restricted.** The backup files should be kept in a safe place, and preferably not on the computer that you normally use your smartcard with.



Generate OpenPGP Key

Account / User ID: <ne@secure.mailbox.org> - Mailbox

☑ Use generated key for the selected identity

☑ Save backup of key outside the card

Passphrase: Passphrase (repeat):

Comment:

Key expires in: 5 years ☐ Key does not expire

Key Generation Console

NOTE: Key generation may take up to several minutes to complete. Do not exit the application while key generation is in progress. You will be alerted when key generation is completed.

Whenever you use an application that needs access to your private key (e.g., to decrypt messages or to sign e-mails in Thunderbird), your YubiKey 5 must be connected to your device. You will be asked for the PIN and entering this will grant the application access to your private key, and whatever cryptographic operation has been requested will then be performed on the YubiKey.

Related Articles

- Is there going to be transport encryption for my e-mail
- How to use two-factor authentication - 2FA
- Can I trust the staff at mailbox.org
- How to set up Mailvelope
- PGP key management