# nymphemeral Documentation

Release 1.3.2

Felipe Dau and David R. Andersen

February 12, 2017

#### Contents

1	What is nymphemeral?         1.1       Overview	<b>1</b> 1
2	Installation (On a Debian Wheezy/Ubuntu Trusty system)2.1Main Dependencies2.2Connections2.3Mixmaster2.4News Server	<b>3</b> 3 4 6 9
3	Usage3.1Files Structure3.2GPG Keyring3.3Launching nymphemeral3.4Creating a Nym3.5Decrypting Messages3.6Sending Messages3.7Configuring the Nym3.8Unread Messages Counter	<b>11</b> 11 12 13 14 17 19 23 25
4	Other         4.1       Changelog         4.2       Feedback and Contact         4.3       Acknowledgements	<b>27</b> 27 29 30

# What is nymphemeral?

## **1.1 Overview**

nymphemeral is a tool made for users searching for secure and anonymous communication on the internet.

It is a GUI client that relies on a pseudonym remailer that communicates to its users by posting messages to a shared mailbox, a Zax-type nym server. Both the server and the client apply an ephemeral encryption layer on their messages based on the Axolotl Ratchet protocol, providing forward and future secrecy to the conversation.

#### 1.1.1 Features

- Manages pseudonym actions: creation, configuration and deletion, as well as message dispatch and retrieval
- Communicates with the new nymserv, a Zax-type nym server with forward and future secrecy
- · Uses python-gnupg and pyaxo for encryption
- · Uses aampy to retrieve messages from alt.anonymous.messages
- Sends messages through Mixmaster, sendmail, or outputs the resulting ciphertexts to be sent manually
- Supports End-to-End Encryption

#### 1.1.2 Current Release

The current version of nymphemeral is 1.4.2, a beta, released 2016-03-21.

#### 1.1.3 Limitations

#### **Regular Zax-type**

nymphemeral does not support the regular Zax-type nym server. It only supports the new nymserv, adding or expecting an ephemeral encryption layer in its messages.

#### **Mixmaster**

Although it is supported (and the use is encouraged), nymphemeral is not a *Mixmaster* GUI. It does enable the users to send their messages to the nym server automatically via *Mixmaster*, but it cannot be used to send regular email.

nymphemeral is a **nym client** and the only way to exchange messages is to send every message to the nym server, to be processed and then remailed to the recipient. *Mixmaster* is just one of the output methods.

**Important:** nymphemeral 1.3.3 was updated to use pyaxo 0.4 that follows the latest (Oct 1, 2014) version of the protocol, which changed the order of the ratcheting. For that reason, old conversations (created with nymphemeral < 1.3.3) might not work properly after the update. We suggest that users update nymphemeral and restart their conversations by changing their nyms' ephemeral keys. The *Configuring the Nym* section explains how that can be done.

# Installation (On a Debian Wheezy/Ubuntu Trusty system)

# 2.1 Main Dependencies

Make sure that you have the following:

```
sudo apt-get install python-dev python-tk # If using Debian/Ubuntu
sudo yum install python-devel tkinter # If using Fedora
```

If you use pip and setuptools (probably installed automatically with *pip*), you can easily install nymphemeral with:

sudo pip install nymphemeral

The other dependencies used by nymphemeral such as pyaxo, python-dateutil and python-gnupg will be automatically downloaded and installed. You can go to *Other Dependencies*.

If you do not use *pip*, you at least have to install *setuptools*. It provides a few features needed by nymphemeral and will also automatically install the dependencies mentioned above. After making sure you have *setuptools*, install with:

```
git clone https://github.com/felipedau/nymphemeral
cd nymphemeral/
sudo python setup.py install
```

nymphemeral and its dependencies should be installed.

#### 2.1.1 Other Dependencies

nymphemeral will be ready for use after installation via either of the two methods described in *Main Dependencies*. However, you should follow the instructions from *Connections*, install *Mixmaster* and have a *News Server* running to be able to use all of its features.

#### 2.1.2 Updating

If you installed nymphemeral with *pip*, you can also use it for updates:

```
sudo pip install --upgrade nymphemeral
```

# 2.2 Connections

We recommend using stunnel, Tor and socat along with nymphemeral when downloading and sending messages. If you are a Whonix user, you should go to connections-whonix.

#### 2.2.1 Stunnel

stunnel adds TLS to your connections. You can install it with:

sudo apt-get install stunnel4

To configure *stunnel*, you can use the .conf file we provide with nymphemeral. Copy that file to the directory where *stunnel* looks for config files (which is usually /etc/stunnel):

sudo curl https://raw.githubusercontent.com/felipedau/nymphemeral/master/connections/stunnel.conf -o

Open /etc/default/stunnel4 and enable stunnel automatic startup by switching ENABLE to 1:

```
# Change to one to enable stunnel automatic startup
ENABLED=1
```

And start it with:

sudo service stunnel4 start

You should get the following message:

```
Starting SSL tunnels: [Started: /etc/stunnel/stunnel.conf] stunnel.
```

#### Tunelling

From the last sections of the .conf file:

```
[nntps-client]
client = yes
accept = 127.0.0.1:119
connect = 127.0.0.1:10063
[ssmtp-client]
protocol = smtp
client = yes
accept = 127.0.0.1:2525
connect = 127.0.0.1:2526
```

Note that:

- The NNTP client is used to download messages. Whenever it accesses port 119, *stunnel* will connect it to port 10063, adding *TLS*.
- The SMTP client is used to send messages. Whenever it accesses port 2525, *stunnel* will connect it to port 2526, adding *TLS*.

#### 2.2.2 Tor

*Tor* is a low-latency communication system used to hide your traffic. If you wish to have the latest stable version you should use this option. If that is not the case, simply install it with:

sudo apt-get install tor

#### 2.2.3 Socat

*socat* manages the last part of the process, which will make the connections from your machine to the servers via *Tor*. You can install it with:

sudo apt-get install socat

A script should be used to make the connection itself. Copy both socat scripts we provide with nymphemeral:

```
curl https://raw.githubusercontent.com/felipedau/nymphemeral/master/connections/socnews.sh -o ~/socne curl https://raw.githubusercontent.com/felipedau/nymphemeral/master/connections/socsmtp.sh -o ~/socs
```

And enable them to be executed:

```
chmod +x ~/socnews.sh ~/socsmtp.sh
```

#### **News Server**

From the socnews.sh file:

socat TCP-Listen:10063, bind=localhost, fork SOCKS4A:localhost:news.mixmin.net:563, socksport=9050 > /de

Note that *socat* accepts connections through port 10063 (the one that *stunnel* connects to) and then connects to the news server at *mixmin.net* via *Tor* through port 9050.

```
Run it with:
```

~/socnews.sh

#### **SMTP Server**

From the socsmtp.sh file:

```
socat TCP-Listen:2526,bind=localhost,fork SOCKS4A:localhost:lnwxejysejqjlm31.onion:2525,socksport=90
```

Note that *socat* accepts connections through port 2526 (the one that *stunnel* connects to) and then connects to the Jeremy Bentham Remailer SMTP server at anemonee.mooo.com via *Tor* through port 9050.

#### Run it with:

~/socsmtp.sh

You could also use other SMTP servers, such as these ones:

```
mail.mixmin.net
mail.allpingers.net
```

**Note:** You can use whatever NNTP/SMTP servers you would like. We chose to use those for convenience, but you are totally free to configure other ones or setup your own.

**Important:** You do not need to start *stunnel* or *Tor* again, but the scripts have to be executed every time the system starts up or whenever you wish to use nymphemeral.

### 2.3 Mixmaster

This section describes how to compile the new large-key version of *Mixmaster* on a *Debian Wheezy* system. If you already have **Mixmaster 3** installed and configured you can go to *Pre-installed Mixmaster*. If you are a Whonix user, you should go to mixmaster-whonix.

Most of the content of this section was taken from this post by the Jeremy Bentham Remailer Admin. The instructions should be helpful for building *Mixmaster* on other flavors of linux as well. See *Ubuntu Loader Changes* for a change if using *Ubuntu*.

#### 2.3.1 Preliminaries

First, you need to install the packages required by Mixmaster and OpenSSL:

```
sudo apt-get install build-essential libpcre3-dev wget \
zliblg-dev libncurses5-dev curl perl bc dc bison libbison-dev
```

#### 2.3.2 Build OpenSSL

Then you need to compile a version of *OpenSSL* that contains the *IDEA* cipher. Grab the most recent version (make sure it is version 1.0.1g or later!) from the OpenSSL download page.

Extract the tarball (substituting your version for 1.0.1g):

```
tar xvf openssl-1.0.1g.tar.gz
```

Build the distribution:

```
cd openssl-1.0.1g
./config
make
make test
sudo make install
```

Note that this installs *OpenSSL* into /usr/local/ssl. Symlink the new *OpenSSL* installation into your normal lib and include directories so that the *Mixmaster* install script can find them. Note that the sudo mv instructions below will only work if you have previous copies of the files installed. If you get an error along the lines of mv: cannot stat libssl.a or similar, just ignore it - you did not have a file there to move:

```
cd /usr/lib
sudo mv libssl.a libssl.a.old
sudo ln -s /usr/local/ssl/lib/libssl.a libssl.a
sudo mv libcrypto.a libcrypto.a.old
sudo ln -s /usr/local/ssl/lib/libcrypto.a libcrypto.a
cd /usr/include
sudo mv openssl openssl.old
sudo ln -s /usr/local/ssl/include/openssl openssl
```

#### 2.3.3 Build Mixmaster

Download Mixmaster 3.0.3.

Be sure to verify the SHA256 hash of the downloaded file. You can do this by executing the command:

sha256sum mixmaster-3.0.3b.tar.gz

The output should match the following hex number:

4cd6121e49cddba9b0771d453fa7b6cf824bee920af36206d1414388a47708de

Extract the *Mixmaster* tarball:

tar xvf mixmaster-3.0.3b.tar.gz

Run the Install script:

cd mixmaster-3.0.3b ./Install

Answer the questions posed by the script:

- You can just press enter when it prompts for the installation directory. It will be installed at ~/Mix
- Do not worry about the *OpenSSL* version questions 1.0.1g+ is so new the script does not know about it select the default **YES**
- Your new version of OpenSSL does have AES encryption, so answer YES to that question as well
- As we are going to only use *Mixmaster* as a client (with nymphemeral), answer **NO** to the question about running a remailer

Mixmaster should be installed successfully.

#### **Ubuntu Loader Changes**

If you are using *Ubuntu* and see the following compile error:

```
gcc mix.o rem.o rem1.o rem2.o chain.o chain1.o chain2.o nym.o pgp.o pgpdb.o pgpdata.o pgpget.o pgpcro
/usr/bin/ld: /usr/local/ssl/lib/libcrypto.a(dso_dlfcn.o): undefined reference to symbol 'dlclose@@GL'
/lib/x86_64-linux-gnu/libdl.so.2: error adding symbols: DSO missing from command line
collect2: error: ld returned 1 exit status
make: *** [mixmaster] Error 1
Error: The compilation failed. Please consult the documentation (section `Installation problems').
```

you should make the following changes to the Install script, due to modifications Ubuntu has made to the loader.

On line 402 of the Install script, change:

LDFLAGS=

to:

LDFLAGS="-ldl"

#### 2.3.4 Getting New Remailer Stats

Before you can use *Mixmaster*, you need to update the stats. We are going to use the pinger from the Jeremy Bentham Remailer, but the process should be similar to other pingers you wish to use.

An easy way to do this **securely** is with *curl*. First, create a file called update.sh in your ~/Mix directory, with the following contents:

```
#!/bin/bash
export SSL_CERT_DIR=$HOME/Mix/certs
rm pubring.asc pubring.mix mlist.txt rlist.txt
curl --cacert ./certs/anemone.pem https://anemone.mooo.com/stats/mlist.txt -o mlist.txt
curl --cacert ./certs/anemone.pem https://anemone.mooo.com/stats/rlist.txt -o rlist.txt
curl --cacert ./certs/anemone.pem https://anemone.mooo.com/stats/pubring.mix -o pubring mix
curl --cacert ./certs/anemone.pem https://anemone.mooo.com/stats/pubring.mix -o pubring mix
```

Change the script to executable mode:

chmod +x update.sh

Next, create the ~/Mix/certs directory and add anemone.mooo.com's certificate:

```
mkdir ~/Mix/certs
cd ~/Mix/certs
wget http://anemone.mooo.com/anemone.pem
```

Now that you have downloaded the certificate file, you can securely update your remailer stats by simply:

cd ~/Mix ./update.sh

You should update the remailer stats at least once a day when using Mixmaster.

### 2.3.5 Config File

*Mixmaster* just needs to be configured through the ~/Mix/mix.cfg file. A very simple config file could be written as follows:

```
CHAIN *,*,*,*,*
SMTPRELAY localhost
SMTPPORT 2525
HELONAME anonymous.invalid
REMAILERADDR anonymous@anonymous.invalid
```

#### Chain

The CHAIN is the path that your messages will take before being delivered. In the configuration above, the messages are going to pass by five mixes, and finally get to the actual target. You can use any sequence and number of mixes in the chain, passing their names or simply  $\star$  (which means that it could be any mix), separated by commas.

**Note:** Adding more mixes to the chain will probably increase the latency to deliver your messages. That is actually not a bad thing, but you should decide how long you are willing to wait to exchange messages.

#### **SMTP Server**

If you followed *Connections*, you remember that we will use port 2525 to reach an SMTP server. Using the options SMTPRELAY and SMTPPORT will tell *Mixmaster* to use that specific connection. Finally, as part of the protocol you need to provide a HELONAME and a REMAILERADDR. As we want to be anonymous, we provide an invalid address.

Note: nymphemeral should be ready to tunnel via Tor messages sent using Mixmaster!

### 2.3.6 Pre-installed Mixmaster

Although we encorage the use of the *Mixmaster* version installed with this section, improved with **4096-bit RSA** (and other features), you are allowed to use any derivative of **Mixmaster 3**. As long as you use that version and nymphemeral is able to find both paths to the binary and config file, you are fine. Configuring these paths is explained later on *[mixmaster]*.

# 2.4 News Server

**Zax-type** nym servers deliver messages to their nyms by posting them on a news group. aampy is the tool underneath nymphemeral that downloads those messages via a news server. The default news server configured in nymphemeral.cfg is set to localhost, port 119. This default is useful if you use stunnel to encrypt the connection between localhost:119 and your actual news server, exactly what was done on *Connections*. If you followed that section, you do not need to configure anything.

Note: nymphemeral should be ready to tunnel your news feed via Tor!

If you want to connect directly to the news server, you should edit nymphemeral.cfg and change the address and port of the news server appropriately. Unfortunately, the **python 2.7 nntplib** module does not support connections over SSL/TLS.

# Usage

# 3.1 Files Structure

After installing the client, run nymphemeral at the command line and it will create the following files and directories inside the base directory (~/.config/nymphemeral):

- \*.gpg: GPG keyring files
- nymphemeral.cfg: Config file that stores preferences and paths used by the client. This file is not encrypted and does not have sensitive data
- hSub files that store the hSub passphrases of the nyms
  - encrypted\_hsubs.txt: File encrypted to every nym (with asymmetric encryption) by one that has access to it
  - hsubs.txt: File used to store (temporarily) the hSub passphrases of new nyms that still do not have access to the encrypted one
- db: Database directory that stores the conversation states of all the nyms. These databases are protected with symmetric encryption (using the passphrases the user provided when creating each nym)
- messages: Directory that stores the read and unread messages
  - unread: Directory that stores the messages downloaded from the news group, that are already encrypted with ephemeral encryption from the server
  - read: Directory that stores the messages the user chose to save, that are encrypted with asymmetric encryption, where the nym encrypted to itself

### 3.1.1 Configuring nymphemeral

You can modify nymphemeral.cfg per your liking. We will not describe the whole file, but only the options relevant to the user that belong to the following sections:

#### [gpg]

Although this option can be modified through the GUI, you can toggle use\_agent between True/False to use the GPG Agent when signing/decrypting messages. (Default: True)

#### [main]

The value of logger\_level can be modified to control what nymphemeral logs on the console. These values are the same ones used by Python's logging module. You can choose from:

debug
info
warning
error
critical

**Example:** debug is the most sensitive level. When it is set, every message will be logged from debug to critical. (Default: warning)

#### [mixmaster]

This section defines the paths nymphemeral searches for *Mixmaster's* binary and config file. Values defined on this section will be checked before the default paths *Mixmaster* usually uses for both compiled (as instructed on *Mixmaster*) and installed (with the package manager) versions:

Option	Compiled	Installed
binary	~/Mix/mixmaster	mixmaster
cfg	~/Mix/mix.cfg	~/.Mix/mix.cfg

If your *Mixmaster* installation is different from these values, you must change the binary and cfg options accordingly. nymphemeral calls --version on the binary and checks for the existence of the config file. Only after checking that *Mixmaster* is some derivative of **Mixmaster 3** and the config file is found, it assumes it is installed and working. Finally it searches for the *mix chain* to be displayed on the GUI, but will not prevent *Mixmaster* to be used if it is not found.

#### [newsgroup]

If you already have a news server running, replace group, server and port with its information. Otherwise, visit *News Server* to find out how to create one using *socat* and *stunnel*.

Important: Changes made to nymphemeral.cfg will only take effect by restarting the client.

# 3.2 GPG Keyring

nymphemeral has its own GPG keyring within its base directory and it does not access information from the user keyring. Therefore, if you are going to use End-to-End Encryption, you have to manually add the respective key to the keyring.

More information regarding End-to-End Encryption can be found in the *Sending Messages* and *Decrypting Messages* sections.

#### 3.2.1 Adding Key

Considering you will encrypt a message to a user whose public key is in the pkey.asc file in the home directory. You can add it to nymphemeral's keyring with:

```
gpg --homedir ~/.config/nymphemeral --import ~/pkey.asc
```

Now you can type its UID or fingerprint when encrypting the message.

Similarly, you can also add private keys to the keyring if you expect to receive messages encrypted to a specific key you have. Either the GPG Agent or nymphemeral will automatically prompt you for a passphrase and decrypt the message.

## 3.2.2 Default Keys

nymphemeral's package includes the public keys of the nym.now.im server and the nymphemeral nym. By importing the former to the client keyring you are able to create and use nyms on that server, and if you need to contact us, the latter allows you to send end-to-end encrypted messages to nymphemeral@nym.now.im. In order to import them you should click Import Default Keys in the Nym Servers window (presented in *Managing Servers*).

The included keys can be found in the nymphemeral.keyring module as .asc files and a detached signature of *nym.now.im*'s public key signed by the Jeremy Bentham Remailer Admin can be used to verify the nym-now-im-server.asc file.

# 3.3 Launching nymphemeral

▼ nymphemeral 1.3.2 - + ×
nymphemeral
Address
tester@nym.now.im
Passphrase
******
Manage Servers
☑ Use GPG Agent
Output Method
Send via Mixmaster
Mix Chain: *,*,*,*,*
Send via Email
Display Output in Message Window
Start Session

Fig. 3.1: Login Window

The client is launched with:

nymphemeral

### 3.3.1 First Time Use

When you launch nymphemeral for the first time, you must import a server public key in order to create and use nyms.

#### 3.3.2 Managing Servers

You can import the *Default Keys* as well as add, modify or delete any server public key whenever you want by clicking Manage Servers in the login window.

### 3.3.3 Starting Session

To start a session, in the login window, fill in the Address and Passhphrase fields, choose the output method that you would like to use and click Start Session. If you wish to create a nym, you can follow the same steps - nymphemeral asks if a nym is being created when the address is not found in the keyring.

### 3.3.4 GPG Agent

If it is enabled, the GPG Agent's dialogs will be displayed when you need to sign/decrypt messages, prompting you for a passphrase. If you decide not to enable it, nymphemeral's own dialogs will be used.

### 3.3.5 Output Method

When **Mixmaster** is installed and configured, clicking the Send via Mixmaster radio button on the login screen will route all messages to the nymserv through the Mixmaster network automatically.

If you have **sendmail** configured and running on your machine, you can also choose to send messages to the nymserv as regular email via the Send via Email radio button automatically.

If you would rather send messages manually, select the Display Output in Message Window radio button and then copy the encrypted message from the message window for transmission. If you choose this option it is your responsibility to send the encrypted message to the server. When this last method is being used, the client assumes that the message will get to the server. Therefore, when you finish the creation process, the nym information will be written to disk right away as well as it will be deleted when you confirm to delete the nym.

**Important:** Regardless the method that is being used, information about the message that has just been created is displayed in the first lines of the text box from the current tab.

# 3.4 Creating a Nym

Back to the login window, when you click Start Session and the nym server's public key is already in the keyring, then the client will search for the nym address that was given. If the nym is not found, you will be asked if you wish to create it and you will be directed to the Create Nym tab in the main window. To create a nym, you must provide the following information:

Ŧ	Public Key Manager –	+ ×
-New Serve	er Public Key	
BEGI	N PGP PUBLIC KEY BLOCK	$\Delta$
Version:	N/A	
mQINBFNcN	lowBEAD9Uq+w7qoERG9CjSEbly8a1tbCGpgGolJi8PMIo9H21ArtuYd0	
eaPoTiv6Z	/SBie45jynRJKow8WTLvCW5Ko+AVblRi+3u9cKboDS1rYb3soU+Q9N1	
th3PMsqYe	tKmIUFM3xdVLhlMNvSrf8qzi8vA05KpCc5MibLIYuiVxJRwIzHa8Xwn	
rersBk4RJ	BoC/kXhB2MdjiEDJi+evMrX8dFC9LTjcCYy3yn03wUai9Rb3Vl23BH8	
7ji1mn6AH	IDxs0Koqe73uP3Q4aGWQ0ycyNr/LeMQ+yauBTHA4mx9ZT7JRJbRNBI9D	
91Rp37qWX	Mqvcv3eVORPxvcsJIqHoh2omih4V6YdRlGePAwB0qnnMGdDo9sWMms8	
xX/nI+X0x	EMTNfhjaLCSQKWJ05a41KFo6Mzs8hwbVRp0zsQvBIJlUMpJasShEBX/	
Bud10ad4G	yXS7YgBuQOcUjgzTQmoujM8qZZpprhGubtcO5KrXzB+jGjFibjbTHBZ	
sC87/0Eeh	2gHbXhe3i9Pck3U5OufCFiB23lTLzhj55P31x/4mZ0oGcg/ozWytdai	
rorMg/ekt	9p05T0vYHqqbuT4tis47xtItmsr9vDQiCOuMIo82CdNat6mb9erB0Jg	
vJItsFJ57	4nFm0HvQApwkLHbtpVJCwhy5ZRnn6AZYH0VEdYStrCbytvHEwARAQAB	
tB50eW0g0	J2VydmVyIDxjb25maWdAbnltLm5vdy5pbT6JAj4EEwECACgFAlNcNowC	
GWMFCQPC2	WAGCWKIBWMCBNUIAGKKCWQWAGMBAN4BAN6AAAOJEH] L/8qmLNNeZuOP	
/0B4UKDV2	3JAZ3+PX56m2yPWD5KK2/KJAK1T6KWENUG5NZ2AD4B08yQ5+ZGZLaKn	
V/tg1qLwy	<pre>/jU/AWNCMPUA1912tpYCWHLNE5/1KWUAUM/alPpk1LeAU/cu+4g1Fdd4 //lliafa00f6ipkl.lashuDyb040llKamduUpbC0EC0am3uX/Ula7i0sEC4</pre>	
J1F3J2yH/	HUJESP98TUIPKLJFSDVDXN848UKMMOUUDSUFLUOMSVX/HLZZIUFFSA	
10/14VPU]	uvz1+KwKJ3514Q2/0+10J+Jv2QQ10V540JNQJ2NQKWXV9NC001g0ND/	
	.utrc54mJ1FVQ9FF41meDLuVmg3LrAQ01Wt1mq2Bt12m4V923mmA+1tJ	
lowor,bumb5	.0012viih10+220CL30111v0LA11L750vd1h50A291BT1000A2vCD026182	$\checkmark$
	Save	

Fig. 3.2: Key Manager Window

	Nym Servers	- +
Nym Servers		
nym.now.im		

Fig. 3.3: Server Manager Window



Fig. 3.4: Nym Not Found Dialog

### 3.4.1 Pseudonymous Name

The Pseudonymous Name field is the name you are going to give to the nym.

## 3.4.2 Duration

You must provide the duration of the nym's key. Once the key expires, the nym expires as well. The Duration must be in the same format used by **GPG** (e.g. 1w, 2m, or 3y).

# 3.4.3 Ephemeral Key

The Axolotl Ratchet protocol derives a master key from the handshake to start a conversation. Since there is already a secure channel between you and the server (using its PGP key), the user can go ahead and send a master key to skip that extra step. That key is the Ephemeral Key you need to provide. It can be any random string since it is ephemeral and will be used only on the first round of message exchange until the ratcheting starts.

**Tip:** nymphemeral will automatically generate one by default, but you can uncheck Auto-generate and provide a key that you generated.

## 3.4.4 hSub Passphrase

Using a **hashed subject (hSub)** is the easiest way of setting up subject identification for your nym to retrieve messages. An hSub is made of two parts, where the first is a random number and the second is the hash of that same random number and a passphrase. As the hashing is a one-way function, no one can identify the owner of the message. However, as you know your nym's hSub passphrase, you can hash it with the random number of every message, and if the result collides with the second part of the hSub, that message was sent to your nym. More on hSub by Zax.

Saving your hSubs allows nymphemeral to retrieve messages from all your nyms at once. You just need to know how the encryption of the hSub passphrases file works:

The first nym that you create will encrypt its hSub passphase and can only be decrypted by itself. The next nym to be created will save its hSub passphrase in plaintext and will not be able to access the encrypted file until you re-log in with the first nym. Then, it will encrypt both passphrases to both nyms and if you create a third nym, those two other nyms can encrypt the passphrases to the third one and so on.

**Tip:** nymphemeral will automatically generate one by default, but you can uncheck Auto-generate and provide a key that you generated.

Note: Although the hSub Passphrase is not required to use a nym, this client works better if you use one and we decided to make it a required field. If you feel that it should allow nyms without an hSub, let us know.

### 3.4.5 Create Nym

Finally, click Create Nym. The text box will display the output message. Read it to see if the message was sent successfully. The nym will be created and the other tabs will be enabled.

<ul> <li>nymphemeral 1.3.2</li> </ul>	- + ×
Inbox Send Message Configure Nym Unread Counter Create Nym	
Ephemeral Key mIRGq/5xmmHWZ1aJvD1cF2ZY8ZnL17uUktTq8a/RFeQnQQ	
hSub Passphrase	
a/Ri1+QfPO8Wcsn9bluXtoD8RWilaFvQfJ+Ugo6+JE7HcQ	
Name	
Tester	
Duration	
6m	
Create Nym	
Nym Creation Headers and Configuration	
Be prepared to wait	V
tester@nym.now.im	Change Nym

Fig. 3.5: Create Nym Tab

# 3.5 Decrypting Messages

After the nym is created, go to the Inbox tab. There you can click Retrieve Messages to start **aampy** and if there are messages sent to you that are tied to your hSub key, they will be displayed in the Messages list box. Clicking on one of the messages will decrypt it and display it in the Body tab and its headers in the Headers tab. If you wish to keep the message, click Save to Disk. You can also click Reply Message and you will be directed to the Send Message tab.

**Note:** Clicking on undecrypted messages will delete them when the process is done. If it fails to decrypt then it is useless. If it succeeds, then it becomes useless due to the Axolotl ratchet protocol. You can go to pyaxo to read more about it.

Ŧ		ny	mphemeral 1.3.2		- + ×
nbox	Send Message	Configure Nym	Unread Counter	Create Nym	
Ephe	emeral Kev				
mIR	Gq/5xmmHWZ1a	JvD1cF2ZY8ZnL	17uUktTq8a/RFeQ	nQQ	
hSul	Passphrase				
a/Ri1	L+QfPO8Wcsn9b	luXtoD8RWilaFvQ	) fJ+Ugo6+JE7HcQ		
Nam	e				
Test	er				
Dura	ation				
6m					
			[	1	
			Create Nym		
⊢Nyn	n Creation Heade	ers and Configura	tion		
hQII 7060 eDpa FNU Bett a0b0 Sjsl 2yF <sup>+</sup> 4sg chS2 6wH2 n9/1 Ebgl UtTr USL4 rdAl Gbas 25E <sup>+</sup>	4A1cKgY2431N9AK JpoNv90GcrFKM 4DUUG65Xsm8Cpv 4tPL0F3ayKZ7K9 4bcx72cgeX2xti 3son14Ht/bluNbuy 39RKn1Bf580J02 4G0bx1d0y49Rta 4G0bx1d0y49Rta 4Gbbx1d0y49Rta 4Gbbx1d0y49Rta 4Gbbx1d0y49Rta 4Gbbx1d0y49Rta 50KWD51y41F0A1 50KWD51y41F0A1 50KW151y160A3 50KW	//9F0-BusGWtb47 loHv+K95Pxa2zz6 vrDFqT7tT2iUNX %krvDkt09Yk0rR 20PEryVwi95tA4 %KrUDt09Yk0rR 20U2rrWJqEv4H (MGT129n9YtdaU MGT129n9YtdaU MGT529h9YtdaU MGT529h9YtdaU MG756Pq3 3RJ0Mmr5oxK E33Msp0J55at5 1MK94wAaUlmXLx +EGSUULVMF148 HMY32rarMmFaGt	v7R7FHph4Dr j sX00 iKzbmL/mXhj7EF83 pKhEKP0nAchth6T MUxoJ7UTK0lm7m Jq6yMqu-hx5VLf1 hkn1DLC80CQn3ii IBMJLMAwq29nhf1 iBMJLMAwq29nhf1 iITmJRVC1R76pn Ulq2yMUzAAvu50 yKFCTfU21X0SKb qDX+UMDmXLSKn-dU rxx92vTF6KC2cpp J4TrX229T1611E V/3Af113D0ur73e	rRCtweTthWiWxsr iAXDrxlXujai/oSV 7mwJPPwct77bIXr2 iveYGU2CHGOT4IcQ HFaGVKmJMZMOjjAM/ bi6ILMd7yEKJBPLL IVUNatXsTL9mdYyRN Wdjx40C8iDJNRNWT zneVSuRII28tBZpv updsv5lcZzagutFeB wUQlidddMkr4ny2LS blVIGcCKJf5baDBS KCVUys9NGEZAFrV4 MMSGKDbE7tTPfU9 icJywxX/dMtFBBucL 89F2NrTXLv+X7M6 ky79sjqlJQD1h9aH HajFeQLVZWSGEV/ SxeBhgqRZ20WLN7p	M
tester	anvm now im				Change Nym

Fig. 3.6: Creation Message

Inbox       Send Message         Retrieve Messages         Messages         Undecrypted message         arget@nym.now.im:Lipsum         Body         Headers         Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa a comassa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	<b>T</b>	nymphemeral 1.3.2	- + ×
Retrieve Messages         Undecrypted message         larget@nym.now.im: Lipsum         Body         Headers         Annean at libero nec lectus cursus consectetur. Cras in efficitur frelis. Fusce tristique arcu sed dui scelerisque tincidunt.         Phaellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa a cmassa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Inbox	Send Message Configure Nym Unread Counter	
Retrieve Messages         Undecrypted message         Larget@nym.now.im: Lipsum         Body         Headers         Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa succipi tultricis in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Messages         Undecrypted message         larget@nym.now.im: Lipsum         Body         Headers         Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipi tultricis in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Re	trieve Messages	
Undecrypted message  arget@nym.now.im:Lipsum  Body Headers  Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus tigula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa succipit ultricis in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Mes	sages	
Body       Headers         Aenean at libero nec lectus cursus consectetur. Cras in efficitur         felis. Fusce tristique arcu sed dui scelerisque tincidunt.         Phasellus tigula augue, auctor non consectetur sit amet, sagittis         vivera massa. Aenean et luctus ante, quis dictum neque. Curabitur         id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci         eu metus rutrum euismod. Aliquam erat volutpat.	Und	ecrypted message	4
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	targ	et@nym.now.im: Lipsum	
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus tigula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricis in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus tigula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa a cmassa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum meque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus tigula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa succipit ultricis in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body Headers Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Body   Headers           Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt.         Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus antee, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.			
Aenean at libero nec lectus cursus consectetur. Cras in efficitur felis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus ligula augue, auctor non consectetur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Bod	y Headers	
Telis. Fusce tristique arcu sed dui scelerisque tincidunt. Phasellus tigula augue, auctor non consecteur sit amet, sagittis viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Aene	an at libero nec lectus cursus consectetur. Cras in efficitur	A .
viverra massa. Aenean et luctus ante, quis dictum neque. Curabitur id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	Phas	s. Fusce tristique arcu sed dui scelerisque tincidunt.	
id massa ac massa suscipit ultricies in eget lorem. Etiam ac orci eu metus rutrum euismod. Aliquam erat volutpat.	vive	erra massa. Aenean et luctus ante, quis dictum neque. Curabitur	
eu metus rutrum euismoo. Aliquam erat volutpat.	id n	assa ac massa suscipit ultricies in eget lorem. Etiam ac orci	
	eun	etus rutrum euismod. Aliquam erat volutpat.	
Politi fun Pith			7
Dalata from Diala			
Leiele Irom Lisk Reply Messade	De	lete from Disk	Reply Message
hepty message			
tester@nym_now_imChange Nym	tester	anym now im	Change Nym

Fig. 3.7: Body Tab

~		ny	mphemeral 1.3.2	- + ×
Inbox	Send Message	Configure Nym	Unread Counter	
Re	etrieve Messages			
Mes	sages	20		
targ	ecrypted messa et@nym.now.im	ge : Lipsum		
Bod	y Headers			
Fro	n: target@nym.n ject: Lipsum	iov. im		
De	elete from Disk			Reply Message
tester	@nym.now.im			Change Nym

Fig. 3.8: Headers Tab

#### 3.5.1 End-to-End Encryption

If someone has sent you an End-to-End Encrypted message, when you click on the message to decrypt it, after removing the encryption layers that were added by the nym server, either the GPG Agent or nymphemeral will prompt you for a passphrase if the key is found in the keyring:

If the key is not found or the authentication fails, the ciphertext will be displayed, allowing you to decrypt it manually.

**Note:** You should read the *GPG Keyring* section to add the keys involved in the End-to-End Encryption to nymphemeral's keyring.

# 3.6 Sending Messages

Sending a message is simple. Fill in the Target Email Address, Subject and Message fields and click Send.

#### 3.6.1 Optional Headers

In the Headers text box, other headers can be added to the message in the format:

```
HeaderA: InformationA
HeaderB: InformationB
```

-	Enter Passphrase —	×			
Ø	Enter Passphrase				
£/13	You need a passphrase to unlock the secret key for user: "Tester <tester@nym.now.im>" 4096-bit RSA key, ID 817AEC8B, created 2015-05-13</tester@nym.now.im>				
	Password:				
	Cancel Unlock				



<ul> <li>nymphemeral 1.3.2</li> </ul>	- + ×
Inbox Send Message Configure Nym Unread Counter	
Target Email Address	
target@nym.now.im	
Subject	
A plain text message	
Headers (Optional)	
Message	EX.
Praesent non tortor finibus, imperdiet justo quis, dapibus mi. Nam gravida, felia et commodo vestibulum, enim dui tincidunt risus, sed pretium nisl metus a purus. Morbi mollis sollcitudin risus, non iaculis libero porta vehicula. Vivamus nec maximus turpis, vel vehicula tortor. Donec tempor libero vitae venenatis malesuada. Duis faucibus urna sit amet risus tristique dictum. Maecenas eleifend est enim, mattis suscipit ligula vestibulum non. Phasellus ut turpis condimentum, gravida dolor ac, ultricies mauris. Suspendisse vitae libero at mi pharetra placerat.	
	_
	N4
Target (IIIDs or Fingerprints)	Signer
	Signer
Throw Key IDs	
Send	
tester@nym.now.im	Change Nym

Fig. 3.10: Send Message Tab

box Send Message Configure Nym Unread Counter Target Email Address target@nym.now.im Subject A plain text message Headers (Optional)  Message Send the following message to send@nym.now.im It has been copied to the clipboardBEGIN PGP MESSAGE Version: Gnub6 v1 h0IMA1cKgY2431N9ARAAtP43c00CiV+3VdpBqB50Wt15m/uK0YcXX0FcyIv0iK9 v0jxwjUX0CF8J7bAM7c+YeM239ET15gNgeMTmMkddnmBrdzJ6MTUH21BiJUg4 USXfx+XPD1amF6/45KLW7r78BHk18arM94pF36K54FH31V42BH454FH448FH344FH32CH2FH344SH444FH32CH2FH344SH44FH32CH2FH344SH44FH32CH2FH344SH44FH32CH2FH344SH44FH32CH2FH344SH454FH448FH345FH31V42BH454FH448FH344FH342BH454FH448FH344FH342BH454FH448FH344FH342BH454FH448FH344FH342BH454FH448FH344FH344SH448FH44FH342BH454FH448FH344FH344SH448FH344FH345FH4	Ŧ		ny	mphemeral 1.3.2		-	+	×
Target Email Address target@nym.now.im Subject A plain text message Headers (Optional)  Message Send the following message to send@nym.now.im It has been copied to the clipboardBEGIN PGP MESSAGE Version: GnuPG v1 h0IMAIcKgvZa3IN9ARAAtP43c0OCiV+3VdpBqBSoWwt15m/uK0YcXX0FcyIV0iK9 v0/xwjUAVCP8J7baN7c+VerX39ET15gyMgeMTmkIddhombFdzJ6WT0LM21BiJug+ USXfx+XPDid9jAquUSbnRaJmFG/45KLMyrnz78BHki183ew6MhfPpICnobFbGkfR YPv23IOvG57E6x500G5PV1tG78BJRrtowntEUB04ab21/WBq1yEduv/4BH=ryx gwesndSJNg-dMJJKLryJXUITpFwcCInn2FNo+HVM21BiJug+ UVmrfBy9/adMJJKLryJXUITpFwcCInn2FNo+HVM21BiJug+ VPV23IOvG57E6x500G5PV1tG78BJRrtowntEUB04ab21/WBq1yEduv/4BH=ryx gwesndSJNg-dMJJKLryJXUITpFwcCInn2FNo+HVM21BiJug+ UVmrfBy9/adMJJKLryJXUITpFwcCInn2FNo+HVM21BiJug+ Ster@nym.now.im ster@nym.now.im Change Nym	nbox	Send Message	Configure Nym	Unread Counter				
Target Email Address target@nym.now.im Subject A plain text message Headers (Optional)  Message Send the following message to send@nym.now.im It has been copied to the clipboardBEGIN PGP MESSAGE Version: GnuPG v1 h0IMalcKgY243IN9ARAAtP43c0OCiV+3V4BgBg5oNwt15m/uK0YCXX0FcyTv0iK9 v0jxvjUAVQcF8J7baH7c+YeMZ39ET1SgWgeMTmkIddnmbFdzJ6WTQLM21BiJug+ ISXfx+XPDid9JAqMJSNhalmF6/45KLNyrnz78Bkki183ew6MhfPpIcNobFbKfR YPv23L0vGs57E6x500GSPV1tG78BJRrtownKtEUooLabzH7W8Q1yEdUv/4BMs+gx gwesndSJNgA/MJMKLryJ7UX1FpKwcLINPR20p1F76865+MRigOrcB UttwK402Fzaj6Az60L18AxMx-mev9fjikdausu+j4LR0ZIzk/QL4L3bURIFuT4P ve500sxvE75EqR2jn72toxsKaMV4QBRPd6Pd0f1Y8ZCG77ACna6f17Kke0jNy 697nFChpi/k18DfZ8DLSYT+qN6f80HtMrc26ZL3BjNSvjnMau+10DcHffic6ghf9 x4MWvA3PL0N3XXdqmk1ZkeE5115FJV8FE47trbbbCG8m/VULHjnjULh03krD5 6gf7R8U-MyddMkmLefbfJsNR1FPJPFR6555 TU2DYTM0FDLnqEE6hbx2gr242Pi+13TaJ9BiK1KRLr1+H6iXBMNKTZMatsq+dX eSUBFFDe/nkp+ddBmueHVPB1gM6BIxNPjPJRvE0QKG0MJb1aa5956xJvUJPR Fnrow Key IDs Send								
target@nym.now.im         Subject         A plain text message         Headers (Optional)         Image: Source of the state of th	Targ	et Email Addres	5					
Subject A plain text message Headers (Optional) Message Send the following message to send@nym.now.im It has been copied to the clipboard BEGIN PGP MESSAGE Version: GnuPG v1 h0IMA1cKgY2431N9ARAAtP43c00CiV+3VdpBqB50Wt15m/uK0YcXX0FcyIv0iK9 v0jxwjUAVQcF8J7baM7c+YeM239ET15gWgeMTmMkddnmbFd2J6WTQLM21BiJUg+ 1SXf+xPRDiaJmFc/4SKLWnr27BBHK183ex6MHfPpIcnobFb6KfR YPv2310vb57E6x50065PV1tG78BJRrtownKEU00Lab2N7W8qJyEdUw/4BM+spx gwesnd5JNp4/MUJNKLry/JXUXTFFwcLInz7DeJK183ex6MHfPpIcnobFb6KfR YPv2310vb57E6x50065PV1tG78BJRrtownKEU00Lab2N7W8qJyEdUw/4BM+spx gwesnd5JNp4/MUJNKLry/JXUXTFFwcLInz7DeJK183ex6MHfPjEnchoFb6KfR YPv2316vb57E6x5005FV1tG78BJRrtownKEU00Lab2N7W8qJyEdUw/4BM+spx gwesnd5JNp4/MUJNKLry-IndyF8dHkndcz2DeJJF78057WHT0F20F3 UUtwk402Fzaj6Az60LBAXMv=meyPgf1kdausH;4LR0Z1k/QL41A3bURIFuT4P ve50gSxVeTD5F1gRZjnY2bUgBuvdvexI5negd2n1En/juJxD5f1Nzf5SwqKrM TGgVEKHJLSgMLa7MnfgHR0bfuzFDhHjjq1sJVKFh6UM7+ejLq3Xn5t0gk7q11x UTWMFBy9/4uJP69WF5L1zptoxsKaMP4q6RPddf1V22KCq7YACn4Gf17RkeojNy 697nChp1/k10072BUJST+n0%f8dHtn-c22LJ3JBVSVm4u=102MFH1c6cdpF9 x4MWvA3PL0N3XKdqm12kE65115FJV8FE47trbbbC68Bm/UPLHjnjULh03RrD5 6gF178U3-VMABMEKSeF15 TU20YUM0FDLnq1E6h52q7242P1+n3TaJ9BiXLRLr1+H61XBMNFVT2Wat5q+dX eq5U0FfDe/nkp+ddBmDueHVP0JM6BIxnPjFJRVE0QKG0Nhp1aa5056xuJVUIPR End-to-End Encryption (Recommended) Target (UUDs or Fingerprints) Signer Throw Key IDs Send	targ	et@nym.now.im						
A plain text message Headers (Optional)  Message Send the following message to send@nym.now.im It has been copied to the clipboardBEGIN PGP MESSAGE Version: GnuPG v1 h0IMAIcKy72A31N9ARAAtP43c00CiV+3VdpBqB5oWwt15m/uK0YcXX0FcyIV0iK9 v0jxwjUAVQCF0J7bAM7c+VeM239ET15gWgeeMTmMkddnmbFdzJ6WT0LM21BiJug+ ISKfx+XP0idjAmuU5hmAmFc/JSKUMyra72BBHklBaveMHtPfgLChobFbkKfR YPv23lGvG557E6x509G5PV1tG78BJRrtovnKtEU00LabzN7WBq1yEdUw/4BMs+gx gwesnd5JNpa/dmJJMkLryj7XUL7mx72BBHklBaveMHtPfgLChobFbkKfR YPv23lGvG557E6x509G5PV1tG78BJRrtovnKtEU00LabzN7WBq1yEdUw/4BMs+gx gwesnd5JNpa/dmJJMkLryj7XUL7mx72BBHklBaveMHtPfgLChobFbkKfR YPv23lGvG557E6x509G5PV1tG78BJRrtovnKtEU00LabzN7WBq1yEdUw/4BMs+gx gwesnd5JNpa/dmJJMkLryj7XUL7mwCIAn2FNox4NM4m2Dp1F76aS+MNfj0rCB UtuK4027z18fklBaVtnyFMM2TLaptoxSkAMP4q6RP6dJTB2XCqC7YACn4Gf17RkeojNy 697nFChpi/k1087ZbNL7m4N6f80Htmc2ZL3J8JKSUM44L10x6Bf11ZkVCqF74LabBRKL5eT5 TU20YruM0FDLnqIE6h5x2gr242Pi+n3TaJ9HiXtsRr1+HH5XBMNRVTXWatsq+dX eQ5U0FfDe/nkp+ddBmDueHVP0IgM6BIxnPjFRvEQ6QKGDNhp1aa59056xuJvUIPR End-to-End Encryption (Recommended) Target (UUDs or Fingerprints) Signer Throw Key IDs Send	Subj	ect						
Headers (Optional)       Image: Content of Conte	A pla	ain text message	2					
Message         Send the following message to send@nym.now.im         It has been copied to the clipboard        BEGIN PGP MESSAGE         Version: GnuPG v1         h0JMALCKgYZ431W9ARAAtP43c00ciV+3VdpBqBsOW+t1sm/uK0YcXX0FcyTv0ik9         v0jwxjUAVQcFBJ7baH7c+YeMZ39ET1SgWgeeMTmMkddmmbfdzJ30WTQLMZ1BiJug+         LSXfx+XPDidjAqu/SDnka1mFG/45KLWyrnz7BBHki1B3ew6MhfPpIchonbFb6kfR         YPvz310vGs57E6x500GSPV1tG7BBJRrtovnKtEU004Lab2N7W6Q1yEdUw/4BMs+gx         gwesndSJNgA/dmJMKLryJXUXTFpwcKlmDzPlp1F76a65+MH3jOrCB         UtUsk/402Fzaj6Az60L18AxMx-mev9fjikdausu+j4LR0ZIzk/QL4LAbURIFuT4P         ve500sxvE75lqR2jn/Y20UgtBuvdvextBregd2n1En/jul+XD5j11XF5SwqKrM         T6gvFkNJLSSgMLa7MnRg+HRDbfuzFDhHjjq1sjVKrh6UM7-ejLq3XnSt0gk7qLX         v1MwFBy9/4JUJ96WFSLIZTpoxKsMAVP4gBRPddfVBX2CQC77ACnA6f17RkeojNy         6977R5Chpi/k18DfZ8DLSYT+qN6f80tHwnc262LJ8jNSvjnMau+100cHffic6gbf9         x4MWvA3PL0N3XXdqmk1ZkeE6111sTpV8FE47trbbbC68Bm/VPLHjnjULh03krD5         6977R5Chpi/k18DfZ8DLSYT+qN6f80tHwnc262LJ8jNSvjnMau+100cHffic6gbf9         x4MWvA3PL0N3XXdqmk1ZkeE611sTpV8FE47trbbbC68Bm/VPLHjnjULh03krD5         6977R5Chp2/nkydBMxmuT91p30K3kmJ020H3pV07JT8MBKNESE55         TU2DYTM0FDLnqIE6hbx2gr242P1+n3Ta)9BiXk1RLr1+H6iXBMNNTXWatSq+dX         eSUBFTDe/nkp+ddBm0ueHVPB1gN68IxnPjPjRvE0QKG0K0Np1aa5956xuJvUIPR         = End-to-End Encryption (Recommended)         Target       (UIDs or Fingerprints) <t< td=""><td>Hea</td><td>ders (Ontional)-</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Hea	ders (Ontional)-						
Message         Send the following message to send@nym.now.im         It has been copied to the clipboard        BEGIN PGP MESSAGE         Version: GnuPG v1         h0[MalcKgY243]N9ARAAtP43c00CiV+3VdpBqB50Wtl5m/uK0YcXX0FcyIv0ik9         v0]xvjJuVQcF8J7baM7c+VeM239E115gWgeoMTmMddhmbFd2J6WTQLM21BiJug+         ISXfx+XPDigiAqu/SbnRaimFc/4SKLNYnr27BBHkl18asweMhfPpIcnobFb6kfR         YPv23L6v6s57E6x50065PV1tG78BJRrtovnKtEU00Lab2N7W6q1yEdUw/4BM+sqx         gwesndS1Mpa/dvJNKLry/JVUTFpWctlTapPlpF76a6S+NRijOrc8         UttwK402Fzaj6Az60L1BAxMv:mevPg1ikdausu+j4LR0Z1zk/0(41A3bUR]ErIT4P         ve500sxvDf5lR2jn/YDUg1BuUdvex1Stnegd2n1En/jul+X05f1LR75SwqKrM         TG69FK0JLSSgMLa7WnRg+HR0bfu2FDHHjjq1sjVkFh6UM7+ejLq3XnSt0gk7q1Ix         UthwK402Fzaj6Az60L1BAxMv:mevPg1kdausu+j4LR0Z1zk/0(41A3bUR]ErIT4P         ve500sxvDf5lR2jn/YDUg1BuUdvex1C2CL3L3jNSt0jWau+10QcHffic6dpH9         c697nFcDrjArk0KxmmuT0mg6mX5gm1jo2Dd1yB2/XCqC7VAnGf17Rkv05St0gk7q1Ix         UfWrMVA3PL0N3Xxdqmk1ZkeE611sTpV8FE47rtbbbC68Bm/UPLHjnjULh03RD5         c697nFcDrjArk0KxmmuT0mg6mX5gm1jo2Dd1p3PD02TBBMBKNESF5         TU2DYrUM0FDLnqIE6h6x2gr242Pi+n3TaJ9BiXsRLr1H6iXBMNRVTzWatsq+dX         c65UBFFDe/nkp+ddBm0ueHVP01gM6BixnPjPjRvE0QKG0Nhp1aa59056xuJvUIPR         End-to-End Encryption (Recommended)         Target       (UIDs or Fingerprints)         Signer         Throw Key IDs		ders (opcional)						
Message         Send the following message to send@nym.now.im         It has been copied to the clipboard        BEGIN PGP MESSAGE         Version: EnuB6 v1         h0IMA1cKgvZ431N9ARAAtP43c00CiV+3VdpBq85oWxt15m/uK0YcXX0FcyIv0iK9         v0jxwjUAV0cF8J7baM7c+YeMZ39ET15gWgeoMTmMkddnmbFdzj6WT0LM21BiJUg+         LSXfx+XPDigjAqu/SbnRaumFc/4SKLWynr278BHkiL8aveoMH*fpE1cnobFbokfR         YPv2310vb57E6x59065PV1LG78BJRrtownKEUb0Lab2N7W6Q1yEdUw/4BMs-qx         gwesnd5JN8p/dmVJNKLryj/XUXTpFwcfLinzPhorF2L36X5+MRj0rc8         Uttx4002Fzaj6Az60L1BAArtx+mevPgfikdausu+j4LRoZIzk/QL41A3bUR1FuT4P         ve5005kWc1D5F1gR2jnr2bugBuwdwexI5neg201En/juJ+X05F1JNR15SwqKrH         T6gvFKH1J5SgML37hnG3+HKD61uzFDhijj1j15jVKF16dW7Pe1jQ3Xn5BWkj7d1x         UftwK402Fzaj6Az60L1BAArtx+mevPgfikdausu+j4LRoZIzk/QL41A3bUR1FuT4P         ve5005kWc1D5F1gR2jnr2bugBuwdwexI5neg20LaFn/juJ+X05HMRVTzWa15gkr4Tk         V6gvFKH1J5B0720L57T+N96169tH-nc25LJ3JNSV3MWau+100cHfic6gbf9         x4MWvA3PL0N3Xxdqmk1ZkeE611157DV8FE47trbbbC68Bm/UPL1jnjULh03RrD5         GefT78U3-V90kWmnu0Th9pGwk38m_1026Mq3P0207ERBABMRLSEF5         TU2OV ruM0FDLnq1E6h6x2gr242P1+n3TaJ9BiK1xRLr1+H61XBMNRVTzWa15q+dX         eQSU0FfDe/nkp+ddBmDueHVP01gM6BIxnPjPjRvE0QKG0Nhp1aa59505kuJVUIPR         End-to-End Encryption (Recommended)         Target       (UIDs or Fingerprints)         Signer       Send								
Message         Send the following message to send@nym.now.im         It has been copied to the clipboard        BEGIN PGP MESSAGE         Version: GnuPG v1         h0IMALcKgvZ431N9ARAAtP43c00CiV+3VdpBqB50Wwt15m/uK0YcXX0FcyIv0iK9         v0jw.juXUGVF637DsM7-c+VeX239ET15gWgeoMTmWdddnmbFdzJ6WT0LM21BiJug+         LSXfx+XPDid9jAgwU5bnRaJmE6/4SKLWyrnz78BHki183ew6MhfPpICnobFb6KfR         YPv31Gvc57E6x9006PVL1G78B3RtrtowREtU06LabzNWq01yEdUW/4BNs-qx         yesnd5JNpa/dmVJNKLryj/XUXTpFwcIkn2FNox+NN4mZD+p1F76a65+MRj0rcB         UltwK4Q2Fzaj6az60L18Axfbx-mevPg1ikdausu+J4EnoZ1zk/Q4LA3DbRIFuT4P         ve5Q0sxVcFDslqR2jn/YzDuStawKavAgRePdd1YB2KCq77Acn46f17KkeojNy         697nFCbji/k1B0FZB0L5YT-qN6F8BtHmc22EJ3BjNSyjmWau+J0DcMffic6dpf9         x4MPVvASPL0N3XKdmk1Zzbc5LSTF4F611sTpWFE4F47trbbC6BMFNVTzB4stq4X         e50UBF1Ce/hykHedBidBuHPDF1jfjlovGKGNKDNh1aa580566xuJvUIPR         =End-to-End Encryption (Recommended)         Target       (UIDs or Fingerprints)       Signer         Throw Key IDs       Send							_	
Message         Send the following message to send@nym.now.im         It has been copied to the clipboard        BEGIN PGP MESSAGE         Version: GnuPG v1         h0IMAIcKgVZ431W9ARAAtP43c00CiV+3VdpBqB5oWwt15m/uK0YcXX0FcyIV0iK9         v0jxwj1aVCeB7Jbx0/r-4VP429ET15gWge0MTmkIddnmbfdzJ0WT0LM21BiJug+         LSXfx+XPDid9jAqwU5bnRaJmFG/45KLMyrnz78BHki183ew6MhfPpICnobFbGkfR         YPv2310vGs7E6x500GSPV1tG78BJRrtowntEUD0Lab2t/NW6Q1yEdUw/4BM+ayx         gwesndsJNpa/dm/JMKLryJNUXTpFwc/InzFNox+NMWarDup1F78665X+MRj0rcB         UttwK402rzaj6Az60LBAxMx+mevPgfikdausu+j4LR0Z1zky(U4LA3bURIFuT4P         ve500sXvE75LgR2jn/ZXDUgtBuvdvexLSTBegd2n1En/j1VJ+N5filLX75SwqKrM         T6gvEKHJLS5gHLa7MnRg+HRDbfuzFDhHjj1j1j1j1j1j1j1j1vJ+N5filLX7FSwqKrM         YG9JFL021x4D4UAW2mnu0Tm9GinX2Bmljj220hj4j201718g92202rRABMBKLSeT5         TU20YrUM0FDLnqLE6bhx2gr242P1+n3TaJ98lXx1RLr1+H6iXBMNVT2WatSq+dX         ve5U05FFDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNMNNT2WatSq=dX         ve5U05FFDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNMNNT2WatSq=dX         ve5U05FFDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNNNNT2WatSq=dX         ve5U05FFDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNNNNT2WatSq=dX         ve5U05FFDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNNNNT2WatSq=dX         VE5U05FDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNNNNT2WatSq=dX         VE5U05FDe/nkp+ddBm0zeHVP013g08LrnP j6JkvE0QKGNNNP1aa59056xuJvU1PR         End-to-End Encryption (Recommended)								
Send the following message to send@nym.now.im       It has been copied to the clipboard         It has been copied to the clipboard       It has been copied to the clipboard         Version: GnuPG v1       hQIMALCKgY2431N9ARAAtP43c00CiV+3VdpBq85oWrt15m/uKQYCXX0FcyIv0ik9         v0jxwjUAVQcF8J7baM7c+YeM239ET15gWgeoMTmKddhmbFd2j6WTQLM21BjJug+       ItsXf+xXP0id9jAqu/SbnatmFc/45KLMYnrz78Bktil8aew6MhfPpIchobFbokfR         YPv231Gv6s57E6x5005FV1tG78BJRrtownKEU00Lab2N7W0g1yEdUw/4BM4sqx       gwesndS1Mpa/dmVJMKLry1/XUTFpwctLinzPtDvFt7865A+MRigTcCB         UUtwK402Fzaj6Az60L18AxMv-mevPg1ikdausu+j4LRoZ1zk/0(41A3bUR1FuT4P       ve500sxvE75SwqKrM         T6gvFkNJLS5gHLa7hwRg+HRDbfuzFDhHjjj15jVKrh6UM7-ejLq3Xn5t0gk7qIIx       Ufwk7By9/4uJP69WFSLI2ptoxskaMvP4q6RPdd1VB2KcqC7YACnd61TRkeojNy         697nFchp1/kla0f28DL57t-qM6f80tHwnc262LJ3jNSvjmMau+1Q0cHf1ic6qbf9       x4MMvA3PL0N3XKdqmk12keE611sTpV8FE47trbbbC68Bm/UPLHjnjULh03RrD5         6gf178U3-M9KdWxmnutThp6jGWtBIxNPjPjRvE0QKG0Nhp1aa59o56xuJvUJPR       ve500svE755         e6U50FfDe/nkp+dd8mbueHVP01gM68IxNPjPjRvE0QKG0Nhp1aa59o56xuJvUJPR       ve         e6U60FfDe/nkp+dd8mbueHVP01gM68IxNPjPjRvE0QKG0Nhp1aa59o56xuJvUJPR       ve         e7       Signer       Signer         ster@nym.now.im       Change Nym	Mes	sage					- 17	ī
It has been topied to the clipboard        BEGIN PGP MESSAGE         Version: Enub6 v1         h0IMAlcKgYZ431N9ARAAtP43c00CiV+3VdpBq850Wrt15m/uK0YcXX0FcyIv0iK9         v0jxxjUAV0cF8J7baM7c+YeMZ39ET15gNgeeMTmMkddnmbFdzjBWT0LM21BiJug+         ISXf+xXPDidjAqu/SbnAzmFc/4SKLWPra72BBHk1BaseMHFfpE1cnbFb6kfR         YPv2310v6s57E6x59065PV1tG78BJRrtownKEUb0Lab2N7W6Q1yEdUw/4BMs-qx         gwesndSiNga/dml3NkLryfXUXTpFwctUnAZPDiF76dS5+MRj0rc8         UttwK402Fzaj6Az60L1BAxMxmmevPgfikdausu+j4LRoZIzk/QL41A3bUR1FuT4P         ve50QsXveTD5F1gR2jnrZbUgtBuvdvexIsnegQaTaEn/juJ+X05F1JR25SwRtM1         G97nChpi,K18072BJL5T+noN51B4ENdvexZbnBg9Z0azFRABMBKLSFT5         TU20VruM0FDLnqE6h6x2gr242Pi+n3TaJ9BiK1xRLr1+H6iXBMNRVT2Wat5q+dX         egSU0FfDe/nkp+ddBmDueHVP01gN6BIxnPjFRe0KQK0Nbp1aa59056xuJvUPR         End-to-End Encryption (Recommended)         Target       (UIDs or Fingerprints)         Signer       Send	Sen	d the following	g message to se	nd@nym.now.im			- P	
Version: GnuPG v1     Version: GnuPG v1       hQIMALCKGYZ43.IN9ARAAtP43c00CiV+3VdpBq85oWxt15m/uKQYcXX0FcyIv0iK9     v0 vvi JuXQCFaJ7baYr-vPKZ39ET15gWgeoMTmMdddnmbFdzJ6WTQLM21BiJug+       LSXFx+XPDid9jAquUSbnRaJmE6/4SKLMyrnz78BHki183ew6MhTPpLCnobFb6KfR     Pvr231cw557E6x5005PV1CHG78BJRtruorNRE1U06LabzWMQ1YdBN+qg       gwesnd5JNpa/dmVJNKLryj/XUXTpFwcTLnZFNox+NN4m2D+p1F7a65S+WRj0rC8     LUtwK402Fzaj6Az60LIBAxMx+mevPgfikdausu+j4LRoZIzK/QL41A3buRIFuTAP       ve5Q0sXveTD5F1gRZjnrZbUgtBuvdvexJIsnegdzn1En/juJ+X05f1JNzfSswqKrM     T6gvEKhJLSSgNLa7Mng+HRObfuzFDhHjjq1sjVKrh6UM7-ejLq3Xn5tgk7q1LX       UtwK409JP2012052052052052052052052052052052052052052	l I I I	las been copre	a to the ctipbo	aru				
Version: GnuPG v1 h0IMALckgVZ431N9ARAAtP43c00CiV+3VdpBqB50wtb15m/uK0YcXX0FcyIv0iK9 v0jxyjUAVCF8J7baWr-vPeMZ39ET15gWge0MTmkIddhmbFdzJ6WT0LM21BiJug+ LSXfx+RPDid9jAqukISbnRaJmE6/4SKLMyrm27BBHki183ew6MtPpICnobFb6kfR YPv2310vG57F6x5006SPV1tG7B3JRrtovnKEEU00LabzN7WBq1yEduv/ABH+9x gwesndSJNpa/dmVJNKLryjXUXTpFwc/In2FNoxElNabzP1F78a6S+WR30rcE LUtwK402Fzaj6Az60L1BAXMtxmevPgfiKdausu+j4LR0ZIzk/QL4LA5bURIFuT4P ve5Q05xVE7D51gR2j1YZDtoxSkMVP4qBRPeM2dT9ZKCG7YACn6fTRRkeojNy 697nFChpi/k18Df2B0LSYT-qN6F8BHtMnc26ZL3BjNSvjnNau+100cHffic6qhf9 xAMWvA3PL0N3XKdgmk1ZkeE61isTpV8F47trbbC6BMS/WLM10yLN03RrDS 697nFChpi/k18Df2B0LSYT-qN6F8BHtMnc26ZL3BjNSvjnNau+100cHffic6qhf9 xAMWvA3PL0N3XKdgmk1ZkeE61isTpV8F47trbbC6BMS/WUH3jNULN03RrDS 695UpFfDe/nkp+dd8mDueHVP19J6B1XHrD19 jPjKvE0QKG0Nhp1aa59056xuJvUJPR FEnd-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send		-BEGIN PGP ME	SSAGE					
hQIMA1cKgYZ431N9ARAAtP43c00CiV+3VdpBqB50Wrt15m/uKQYcXX0FcyIv0ik9 v0jxwjUAVQcF8J7baM7c+YeMZ39ET15gWgeoMTmKdddnmbfd2J8WTQLM21BJUg+ LSXf+xFD10jAqu/SbnAamFc/45KLMYnrz78Bht(182ew6MhfPp1chobFbkfR YPvZ3L0v6557E6x5005FV1tG78BJRrtovnKtEU00Lab2N7W0g1yEdUv/4BM5+gx gwesndS1Dng/dm/JNKLryf/XUTFpwctInzPtoxPup1F76865+MRj0rc6 UUtwK402Fzaj6Az60L18AxHvmevPg1kdausu+j4LRoZIzk/QL41A3bURIFuT4P veS00svrtD51qR2jn72UgUtgUudvexL50FbHjja1sjVKrh6UM7+ejLa3Xn5t0gk7qL1X UUfwK189/4uJP65WF5L1zptoxsKaMvP4q6RP0dd1VB2KCqC7VAcnd61TRkeojNy 697nFchp1/k180728DL59T+qN6780tHunc262LJ3jNSvjmNarL0QcHff1c6qbf9 x4MMvA3PL0N3XKdqmk1ZkeE611sTpV8FE47rtbbbC68Bm/UPLHjnjULh03RrD5 6gf178U3-M96NkmnQtHp6GNk3Bmj1020Maj920ozFRABMBKLSeT5 TU2DYTW0FDLnqE6h6x2gr242Pi+n3TaJ9BiK1RLr1H6iXBMNNT2Watsq+dX e05U8FfDe/nkp+dd8m0ueHVP01gN68IxnPjPjRvE0QKG0Nhp1aa59o56xuJvUJPR =End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs	Ver	sion: GnuPG v1						
voj xs julvõg-F8JTbah7-×YeM239ETI SgNgeoHTmNdddmnbFdz joKYTQLM218i Jug+ 1SKf+×YPDidjaquUShnAsimFc/ASKLMYPra72BBHkl BaseM6Hf Pg1CnobFbkKfR YPv23LGvGs57E6x5006SPV1tG78BJRrtovnKtEU08LabzN7W8q1yEdUw/4BMs+gx gwesnd5JNpa/dm2JNRtryj XUXTPMvCILnZFNox+NN4m2D+p1F76aS+MRJ 0rCB Utuk4Q02F28Jd2012BA/tNsmerYg1ikdausu+14RezDz12K/Q141AbDRFLT7AP ve50Q5xVeTD5FLgR2jnYZbUgtBuvdvexI5negQ12En/jJJ+X05f1JNz7SSwqKrM TGgVEKHJLSSGNL37NKG+MRDfuzZDhHj jq15jVKF16MUr4ejLg3NnStQ8K7qL UTWwfBy9/4JJ969WFSLIzptoxSk4MP4q6RP6dJTVB2KCqC7VACn46f17RkeojNy 697nFChpi/k10872NL37tr-Nof6B9tHmc22LJ3BJKSD17Mau+1Q0cHf16cdghf9 x4MWvA3PL0N3XKdqmk1ZkeE61115TpV8FE47trbbbC68Bm/UPLHjnjULh03RrD5 69F178U3-V90kkmnUTDF0gGMx38m1j020hq1yP071RBMRNL5eF5 TU20YruM0FDLnq1E6h6x2gr242Pi+n3TaJ9BiKixRLr1+H6iXBMNRVT2Natsq+dX eQ5U0FfDe/nkp+dd8mDueHVP0JM6BIxnPjPRvEQ6QKGDNhp1aa59056xuJvUIPR =Ind-to-End Encryption (Recommended) Target (UUDs or Fingerprints) Signer Throw Key IDS Send	hoi	MA1cKaYZ43lN9A	RAAtP43c00CiV+3	VdpBa85oWwtl5m/uK0YcXX0F	cvIv0ik9			
LSXfx4XPDid9jAquUSbnRaJmE6/4SKLMyrnz78BHki183ew6MhfPpICnobFb6kfR YPv23[cv657E6x9065PV1678BJRftvonKEU061ab2NWABU49Bv4px gwesnd5JNpa/dmVJNKLryj/XUXTpFwcILn2FNovxHNMm2D+D1F76a6S+WRGJrC4B LUtwK402Fzaj6Az60LI8AxMx+mevPgfikdausu+j4LRoZIzK/QL41A3bURIFUT4P ve5Q0sXveTD5F1gR2jnrZbUgtBuvdvexI5negd2n1En/ju1+XDsf1JNzfSSwqKrM T6gvEKHJLS5gNLa7MnRg+HRDbfuzFDhHjjqLsjVKrh6UM7+ejLq3Xn5tgk7q1Lx UfwHFBy9/4uJ965WF51LgrtoxSkMV4PdqRPR0df1YB2KCG77KArd6f17RkeojNy 697nFChpi/k18Df28DL5YT-qW6f80Hmc26ZL38jNSvjnNau+100cHffic6dpf9 x4MMVvA3PL0N3XKdmk1Z+KE6F1iJSTpVRFE47trbbC608Mr/UEHjnjULh03RrD5 6gF178U3+vB0kWzmu0Th9g6mXx8gm1jo26hq1VP01718g9g2oozFR8AMBKL5ET5 TU2DYruM0FDLnqIE6h6x2gr242Pi+n3TaJyBiKixRLr1+H6iXBMNVT2Natsq+dX eGSUBFfDe/nkp+dd8mDueHVP01gK68LrnP i jNxC90KG0Mhp1aa59o56xuJvUIPR Fend-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send ster@nym.now.im Change Nym	v0j:	wjUAVQcF8J7bal	M7c+YeMZ39ET15g	WgeoMTmNdddnmbFdzJ6WTQLM	21BiJug+			
YPv231GvGs57E6x500GSPV1tG78BJRrtovnKtEU00Lab2/NW6Q1yEdUv/4BMs+qx gwesndSJMp4/dMJNKLryJXUxTpFwcKInDzPloF76a65+MRjOrC8 UUtwK402F2aj6Az60L38AXMx+mev9f3ikdausu+j4LRoZIzk/QL4LA5bURIFuT4P ve500sxvErD51gR2jrJX2bUgtBuvdvexE15megd2n1En/jul+XDsf1jLX7SSwqKrM T6gvEkUJLS5gMLa7MnRg+HRDbfuzEDhHjjq1sjVKrh6UM7+ejLq3XnSt0gk7qL1x UthwFBy9/4uJB6WFSLIzptoxKsMAVP4BRPM2dfU38Zkcg77XAnd6f17RkeojNy 697nFChpi/k18DfZ8DL5YT+qN6f80tHwnc262LJ8jNSvjnMau+1QDcMffic6qbf9 x4MMvA3PL0N3XKdqmk1ZkeE61L1sTpV8fE47trbbbC68m/UPLHjnjULh03RrD5 6gf718U3-VM6Wkmnut0ThegGmX8gm1j02Md1yP071Bd9g20ozFR8MMRKLSeT5 TU2DYTM0FDLnq1E6h6x2gr242P1+n3TaJ9BiXtRLr1+H6iXBMNVT2WatSq+dX eGSU6FfDe/nkp+d68m0ueHVPB1gN68IxnPjPjRvE0QKG0Nhp1aa59o56xuJvU1PR =End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs	lsx	fx+XPDid9jAqwU	5bnRaJmFG/4SKLM	yrnz78BHkil83ew6MhfPpICn	obFbGkfR			1
gre sinch by Academic V/ Acade	YPV:	231GVGS5/E6X50	Q6SPVLtG/8BJRrt	0VNKTEU00LabzN/W8q1yEdUw Tkn2ENov:NN4mzD:n1E76a65	/4BMs+gx			
ve500sxveTd5F10R21jn72bUgtBuvdvexI3negd2nEn/jUJ+XD6F11Nz75SwqKrM T6gvEKHJLSSgMLa7WnRg+HRDbfuzFDHHj jq15jVKh6UM7+ejLq3XnSt0gK7q11x UfwrfBy9/4UJP69WFSL1zptoxsKaHvP4q6RP6ddYB2KCqC7VACn46f17RkeojNy 697nFChpi/K18Df28DLSYT-qN6f80Hmc26ZLJ8jNSvjnNau+10DcMffic6qbf9 x4MWVA3PL0NXXdqml2KEE611sT5pV8F47trbbC68MWJPLHj njULh03RrD5 6gFT78U3+V90kWzmu0Th9gGmXx8gm1j026hq1VP01718g9g2oozFR8AMBKLSET5 T120YrUM6PL0nqE6h6x2g742P1+n3134pK1xRL-1HH5XBMNK7V4Watsq-dX e05U8FfDe/nkp+dd8mDueHVP019M68IxnPjPjRvE60KGDNhp1aa59o56xuJvU1PR Fend-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs ster@nym.now.im Change Nym	lUt	vK402Fzai6Az60	LI8AxMx+mevPafi	kdausu+i4LRoZIzk/OL4lA3b	URLFuT4P			
TGgUEKHJLSSgMLa7WnRg+HRDbfuzPDhHjjqLsjVKrh6UM7+ejLq3XnStgk7qLIX       UTwhFBy9/4Ju3P6WFSLIZptoxsKaMVP4qRRPddTYB2Kcq7YACn4GfTRKeojNy       697nEChpi/kl8Df2B0LSYT-qN6F80H4mc26ZL38jNSvjmKau+100cHffic6qhf9       xAMPVvA3PL0N3XKdgmkLZkeE6li1sTpV8fE47trbbC6GBm/UPLhjnjULN03RrDS       6971R013+V8QkWzmnuQTh9GmXx8gmIj020hq1yP01718g9g2oozFR8AWBKLSeTS       TU2DYTW0FDLnqLE6h6x2gr242P1+n3TaJ9B1K1xRLr1+H6iXBMNKVTzWa1Sq4dX       eSUB6FDe_nkp+dd8mDueHPP1gh6B1LmP1 Pj RvE0QKG0NhP1aaS9056xuJvU1PR       -End-to-End Encryption (Recommended)       Target     (UIDs or Fingerprints)       Signer       Throw Key IDs       Send	ve5	QsXveTD5FlgRZ	jnYZbUgtBuvdvex	I5negd2n1En/juJ+XDsfi1Nz	fSSwqKrM			
UTWATBY9/4UJP69WF5L12pT0xStAWVP4QeRV60dJY82KCqC/7ACn4Gf17Rke0jWy 697nChp1;K180f28DLS7T=AWF61Bf0HcaC2LJ3BjKSyTMau+1Q0eRHf1c6qbf9 x4MWvA3PL0N3XKdqmk12keE611157pV8fE47trbbbC68Bm/UPLHjnjULh03RrD5 6qF178U3-VP0KVzm017D6gcMx3gm1j02f0Ap1yP0718d9g20ozFR8AWBKL5eT5 TU20YruM0FDLnq1E6h6x2gr242Pi+n3TaJ9BiK1xRLr1+H6iXBMNRVT2WatSq+dX eqSU0FfDe/nkp+dd8mDueHVP01gN68IxnPjPjRvE0QKGDNhp1aa59056xuJvU1PR End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send	T6g	vEKHJLSSgMLa7W	nRg+HRDbfuzFDhH	jjq1sjVkFh6UM7+ejLq3XnSt	0gk7qlIx			
x4MWVA9L0N3XXdgmk1ZkeE6111sTpV8Fe47trbbC6088m/UPLHjnjULh03KrD5 6gFt78U3+VB0kWzmuQTh9gGmX88gm1j0Zbhq1yP01718g9gZooZFR8AMBKL5eT5 TU2DYTWR0FDInqTE6h6x2g7242P1+n313yBik1xRt1-HH6X38NNRT4Watsq+dX eQSU0FfDe/nkp+dd8mDueHVP019N681xnPjPjRvE0QKGDNhp1aa59056xuJvU1PR End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send	01W	vfBy9/4uJP69WF FCbpi/k18Df78	SLIZPTOXSKaMVP4	q6RP0dd1YB2KCqC/YACn4Gfl nc267L18iNSvinWau+10DcMf	/RkeojNy fic6abf9			
GpET2RU3+vBQkWzmiuQTh9gGmXx8pm1j02Phq1718g9g2oozFR6AM8KLSET5       TU2DYruM0FDLnqTE6h6x2gr242Pi+n31aJ9KiX:RLr1+H6iXBMNRV1Netsq+dX       eSU06FDer/nkp+dd8mDueHVP01gN681xnPjPjRvE0QKG0Nhp1aa59o56xuJvU1PR       End-to-End Encryption (Recommended)       Target     (UIDs or Fingerprints)       Signer       Throw Key IDs       Send	x4M	VvA3PL0N3XKdq	nk1ZkeE61iIsTpV	8fE47trbbbCG8Bm/UPLHjnjU	LhQ3RrDS			
TU2DYTWOFDLnqIE6hx2gr242Pi+n3TaJ9BiKisRLr1+H6iXBMNVT2WatSq+dX eqSUBFfDe/nkp+dd8mbueHVPB1gN6BIxNPjPjRvE0QKGDNhp1aa59o56xuJvU1PR End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send ster@nym.now.im Change Nym	6gF	l78U3+vBQkWzmn	uQTh9gGmXx8gmIj	oZ0hq1yP01718g9gZoozFRBA	WBKLSeT5			
Education (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send ester@nym.now.im Change Nym	TU2	OYruMOFDLnqIE6	h6x2gr242Pi+n3T	aJyBiKixRLr1+H6iXBMNRvTz	Watsq+dX			
End-to-End Encryption (Recommended) Target (UIDs or Fingerprints) Signer Throw Key IDs Send ester@nym.now.im Change Nym	EQ.		ibdenti orgitoorx		AUD VOI IN			1
Target (UIDs or Fingerprints) Signer Throw Key IDs Send ster@nym.now.im Change Nym	End	l-to-End Encrypt	ion (Recommend	ed)				
Throw Key IDs Send ster@nym.now.im Change Nym	Ta	rget	((	IIDs or Fingerprints)		Signe	er	
Throw Key IDs  Send  ster@nym.now.im  Change Nym								
Send Send Change Nym		Throw Key IDs						
ster@nym.now.im Change Nym								
ster@nym.now.im Change Nym				Send				
	ester	@nym.now.im				Change N	lym	1

Fig. 3.11: Sent Message

#### Example

I know a server that allows me to post messages to *Usenet*. I provide its email address in the Target Email Address and as I wish to post to *alt.privacy.anon-server*, I type the following header in the Headers text box:

Newsgroups: alt.privacy.anon-server

The server will process the message and the post should arrive in the news group.

#### 3.6.2 End-to-End Encryption

The End-to-End Encryption section enables the user to encrypt and/or sign messages. The Target and Signer fields can receive either an UID or fingerprint. If more than one key is found for that query, nymphemeral will ask the user to be more specific, to avoid ambiguity.

There is also the option to use the Throw Key IDs checkbox, so that **if** someone obtains the ciphertext, they will not even be able to find out whom the message was encrypted to, because the key ID was removed. Therefore, when someone receives that message, they will have to use all of their keys to attempt to decrypt it.

If the message is being signed, either the GPG Agent or nymphemeral will prompt you for a passphrase to unlock the secret key:

**Note:** You should read the *GPG Keyring* section to add the keys involved in the End-to-End Encryption to nymphemeral's keyring.

	nymphemeral 1.3.2	- + :
box Send Message Config	gure Nym Unread Counter	
Target Email Address		
target@nym.now.im		
Subject		
E2E encrypted message		
Headors (Ontional)		
Treaders (optional)		
Message		
Aliquam bibendum, enim	ut vestibulum maximus, lorem eros	
hendrerit nulla, at tin	cidunt lorem metus eu ex.	
End-to-End Encryption (Re	commended)	
Target	(UIDs or Fingerprints)	Signer
target	817AEC8B	
Throw Key IDs		
	Send	

Fig. 3.12: End-to-End Encryption

•	Enter Passphrase – ×			
B	Enter Passphrase			
	You need a passphrase to unlock the secret key for user: "Tester <tester@nym.now.im>" 4096-bit RSA key, ID 817AEC8B, created 2015-05-13</tester@nym.now.im>			
	Password:			
	Cancel Unlock			



#### 3.6.3 Message Structure

It is important to know how the contents of your message are handled. For example, if you composed the following message:

```
To: recipient@domain
Subject: Foo
```

It would be encrypted to the server (with both asymmetric and ephemeral encryption layers) and would become the following message to be transmitted:

```
To: send@server
-----BEGIN PGP MESSAGE-----
<ciphertext>
-----END PGP MESSAGE-----
```

If someone intercepted the message, they would only learn that you sent a message to send@server, which would remail it to someone else. However, they learn nothing about the original message, because it is encrypted to the server. Now, when the server receives and decrypt it, the original message is accessed:

```
To: recipient@domain
Subject: Foo
```

Bar

Bar

That is the reason that another layer (end-to-end encryption) should be added. That way, when the server removes its encryption layer, it would only have access to the headers:

```
To: recipient@domain
Subject: Foo
-----BEGIN PGP MESSAGE-----
<ciphertext>
-----END PGP MESSAGE-----
```

It is called "end-to-end" because only the ends of the transmission (you and the recipient) can access the data. That last encryption layer must be removed by the recipient, to finally obtain the plaintext of the message. The last thing you should know is that the headers cannot be encrypted. Therefore, make sure to use non sensitive information for the **subject** and **optional headers** you might add.

# 3.7 Configuring the Nym

On the Configure Nym tab you can modify the Pseudonymous Name, Ephemeral Key and hSub key of your nym (both keys can be automatically generated by nymphemeral). Clicking on Configure will create the message that will be sent to the server. If you wish to not use your nym anymore, click Delete Nym.

Tip: If you believe that the server is not processing your messages, try to change the Ephemeral Key so that the databases will be synced.



Fig. 3.14: Configure Nym Tab

*		ny	nphemeral 1.3.2	- +
Inbox	Send Message	Configure Nym	Unread Counter	
Nyr	ns With Unread	Messages		
aice	@nymserver.ne	t(1)		4
bob	@domain.org(2)			
test	er@nym.now.im	(1)		
				17
tester	@nvm.now.im			Change Nym

Fig. 3.15: Unread Counter Tab

# 3.8 Unread Messages Counter

On the Unread Counter tab there is a list of nyms with unread messages, so you do not need to log in with all your nyms to check if they have new messages (as long as you are retrieving messages with a nym that has access to the encrypted hSub passphrases).

# Other

# 4.1 Changelog

### 4.1.1 nymphemeral 1.4.2, released 2016-03-21

- Make the login interface more intuitive and close #21
- Minor interface enhancements
- Require setuptools only
- Include default keys and close #29
- Organize imports and close #37

## 4.1.2 nymphemeral 1.4.1, released 2016-02-13

- Add nymphemeral's own method to check a nym's passphrase
- Fix issue when retrieving nyms due to a change to python-gnupg
- · Enable auto-generation of ephemeral and hSub keys
- Add method to retrieve a specific nym
- Add expiration attributes to the Nym class and display the expiration date on the GUI

## 4.1.3 nymphemeral 1.4, released 2015-12-19

- Make a proper entry point to launch the GUI
- Close #24 by using versioneer for version management

## 4.1.4 nymphemeral 1.3.6, released 2015-12-17

- Fix issue #26 to format the key info of nyms without expiration
- Fix issue #30 to not crash nymphemeral when a mix chain is not found
- Add an Updating section to the docs
- Do not call the package manager to install dependencies

#### 4.1.5 nymphemeral 1.3.5, released 2015-09-09

- Improve the logger level
- Add more information to the installation sections
- Define which attributes and methods of Client are private
- Improve the code (add constants, simplify methods, remove redundancy)
- Fix bug to save new databases in the db directory

### 4.1.6 nymphemeral 1.3.4, released 2015-07-22

- Improve recognition of the Mixmaster installation
- Clarify nymphemeral's features and limitations
- Add instructions for Whonix

#### 4.1.7 nymphemeral 1.3.3, released 2015-07-18

- Use pyaxo 0.4
- Use Python's logging module
- Slightly improve aampy's performance
- Improve parsing of the config file
- Improve and add more input validation
- Bug fixes and code improvements

### 4.1.8 nymphemeral 1.3.2, released 2015-05-13

- Add End-to-End encryption
  - Encrypt
  - Throw key IDs
  - Sign
  - Support GPG agent
- Redesign aampy

#### 4.1.9 nymphemeral 1.3.1, released 2015-03-03

- Create client module
- Modify the GUI to be a layer between the user and the client

#### 4.1.10 nymphemeral 1.2.3, released 2015-02-14

• Remove dependency links processing from pip install

#### 4.1.11 nymphemeral 1.2.2.1, released 2014-11-14

• Remember the output method being used

### 4.1.12 nymphemeral 1.2.1, release 2014-11-10

- Append date to the title of the messages in the 'inbox'
- Encrypt hSub passphrases
- Support headers added by the user at the top of the message being composed
- Add the 'In-Reply-To' header to the reply

# 4.2 Feedback and Contact

Please use the GitHub issue tracker to leave suggestions, feature requests, bug reports, complaints or any contribution to nymphemeral. If you feel the need to talk about something else, send messages to nymphemeral@nym.now.im. You can also use its public key for end-to-end encryption:

```
----BEGIN PGP PUBLIC KEY BLOCK----
mQINBFa+ivYBEAC217YY5svarWao9DLA0Zem5E1gs1B8ttKxNdWh3RJjDk3XL0Qs
1zlRI8QAgNpReQVACNXpglu1x1bpZ+AwS1HjC4W0v8BrgOYWSrhyg0h8yr0IZ3fk
Bybrx6aZ3uH1z4oY1vfRy48maT+4L1qmliH72DRh7ic+Mscy/wU0ufAsnH2uQKo6
ViJ6TB8ra7DarftNRyTNNAnMjQuUiLfX2ZHAtqzDs3FJ0wD/zfdwE/x/0dRztP86
YTbTJIB104CU86rfDXqmE2UDqCFaxcoKY/6XLNymsVVdG/TLS50H0wIqUep3iG++
/HDhCiTlVKCsYdDolSWiJ27lUn3chSvuMBELTQZqQ0SQnBd17Fn1aYcZwMklojNG
C5xHVHWENng1Jjj0UGKEzX7PvzyH/IyDcqjPJa2R5MHXC1VC1BKVE9uEGvjGoZnT
bdOYkAZGEpGmpaWDecNV38Xhfjb4DkG/zYb19kDEvLNP7/KwmCgaFJw+F5PEnZ7K
cC09MZrD7cyyYaDi/mdym++yE1p/hv8ohzCev6xsJ2+QISzkEC2ceC/1sgfMt+hS
w6Jws/qf0LejFv0lGpHqUYz0WYFZVxT1X6wa8cZIVF55D1wFT4o7onfLDsjjTMkJ
yt1CpitYQqXALIfBb8hp9sG4xkuV5ZL9wMYtnbZUen7xb3qEYM2GQDJqoQARAQAB
tCRueW1waGVtZXJhbCA8bnltcGhlbWVyYWxAbnltLm5vdy5pbT6JAj4EEwECACqF
Ala+ivYCGyMFCQlmAYAGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEMY7xouz
msjh0sYP/3avkGR4oU6Iq57wFkHjkKuSI81hkY0x223J3OoCJc5CcggyN4huy4fy
+OHf5rcaRosjmPlk/jRbEuK3TVNsc5RsHGAk/rg8KUUEXnhDAAv1vXYISinwc2FV
80Nv2qUTMv9imrC/w+fJYjY3RccH7YADWzV4tn9E0E0vjHh3LqY2p11djKyvnZod
cKkZ+NdKsUAU6xh3HbGoFPssYRos/xBNk6oHXEtPtCEZ4pfHjqV2k6yR0QpXabgS
36FdTF0Hh6CyvQJ9pD5CLloPEqivubTF++jNh7++2riKu0XKW2ns7vw3pt189ZIt
QdYoVVGnFTq011bW5nfrhzB9d00JHX8i8oNFW5WEzFh8sB7sRygmLpGzEOPeoCNE
PBB2360xlsCNGDtjXYRbkqyLoujiimFweN4ZapmIB+MSxYyAxxZ7BvOD/Y0Y2266
togL0LdBXU/khegUJvLteBS08iH+Y1iKLhhC4tAkvldKsJ0bCjnMynuxqFreD7hU
uXQ4liTu5o4FPZw9Vk+DOceEOeNYya7rdKC6d57C2H9MfrZRl717BXQArYCNAn89
f2phyOxgiWk/Af+NlwfWb0XFiFZBywTZlkK7SS0+/xf7EZqWgL3q/U2WRZs01ZBQ
T+iJBmraQNBGjWwm6rZvslhFAs127K9BadinS2lfx5rBJeW7TlqOuQINBFa+ivYB
EADEWeia6RWeUbypav1YZrYZp3jYrM/QjxqXRFtsXUkjaK91ndkHB1rwqWyLiWOc
k/YePlXXyQtvR52Ldfzs056vIQz2uIJGVSpn/oOn7SFBrTtsvuzHltbe4nzMQLlP
MF3zwGTqG9SRNxzviE/rSkqfnzRvUNV/uq/ySKrUo4tgvHVUyO+G/j7Lva1ZJWaZ
VWUf5QXFH39a46+uKd1lvIN3UMpIX9vNHs9MOCMSRCdtOwP9Su8SztFRTjAq2PRb
/NmehmRfpC/vVtriyyn85t8IcTczTx02t290CNB76FlyFFreOimzGYjRfg40its3
IctttDVP82sOMjozE+A4IUXchTPcb5QhGTTjgxHUGxaScMBlJpb+zH7OXKzvELAL
W8Ft4yZH6bXo4ONnw0M/S9+upXqkclPHoCd5lq85wkvJTM2UiNdtnn4doBKQaGb0
fM1HtXRWvCS1m+aYNboE8eq51SjJaa2X0Sjsk6dWMvldK6hIE8+IFHayUdfdnSwH
DRbUDZtyxKURAd8z9tMHaGVr6BG8fNmE+xbNdAca4iN2CLWUHMkeFvmrlQf0iZxJ
6jeBHSM9eA59gSKL5olDAIJK8vVHjkTKDWnnZ9e61E0eWWF5H4yPTABNctRJjrAN
```

```
iv5D05FK6NOods56JsBXdlhtuF/TITFjbQYKpSJofeyDxQARAQABiQIlBBgBAgAP
BQJWvor2AhsMBQkJZgGAAAoJEMY7xouzmsjhW5IQAI+pnQkoUG+vu4hcuW//9vsD
XDHerjkUUC1QvKAML1Ijkb/tKmkBgk/EgAFffBaG50DPaXAW8MhC4Q6/9vmR8Stj
T5cHwGuHdo7aJbD4F3G71HMJsI2W0vhRzx/LaLaPITklCz7Ink69hRsy49vr8tx
ZAkkaEq28RSXZGodLd/RQQ+o27hZbc0kKabspajj++yg9yrM6OauM+/xl6C46dFI
s+7drK8fZisiJdegN982RgjuNaVtcGpoRdFuJ9QJoJ8ZVcnsyBV0AX/3Pg/I3leY
DNY+g98MrkysoS4k0nPifumuqXp/coc/d9X2H5prMOVbKr5pvP9G7pOCZn0Kzi/W
YUCVEdO2AiEDVUEt/1+8fLm+dIy8nf1nlTgy6bnFTnJ8lndf+4bpiAGBSjby8H5A
hx3qHy7EKkaN4Z/bBuvsL0D9Sfu2/ngMEyTLhg0UYru4kauYwZEBotj9Ax6oRBLw
ALV1PAg28klEq3d05+ehD18VMkzQrI6XZv1tX2vwu0AeGvIrSy+9Hs+RuEZTFbQT
dQUnLc2tRTUgWnsqNefG7gBSYzu8IRmNNv+Y4reyN+qDRUVj2J10YPMhEnRgtr6z
R9T6jR8Eh+PorYbfchv5uyeyb1iiWfntfESP6qpwkoI3Dr986JI60MEYTWuAlwIn
Y27t5vjdCGe7mIVrTCri
=/TNE
-----END PGP PUBLIC KEY BLOCK-----
```

# 4.3 Acknowledgements

- Thanks to rxcomm for the new nymserv, nym.now.im, pyaxo, aampy and for assisting on the development of this client
- Thanks to crooks (Zax) for the original nymserv software
- Thanks to tych0 for assisting on fixes and improvements
- Thanks to HulaHoopWhonix (from the Whonix team) for testing and providing awesome feedback, such as bug reports, feature requests and suggestions