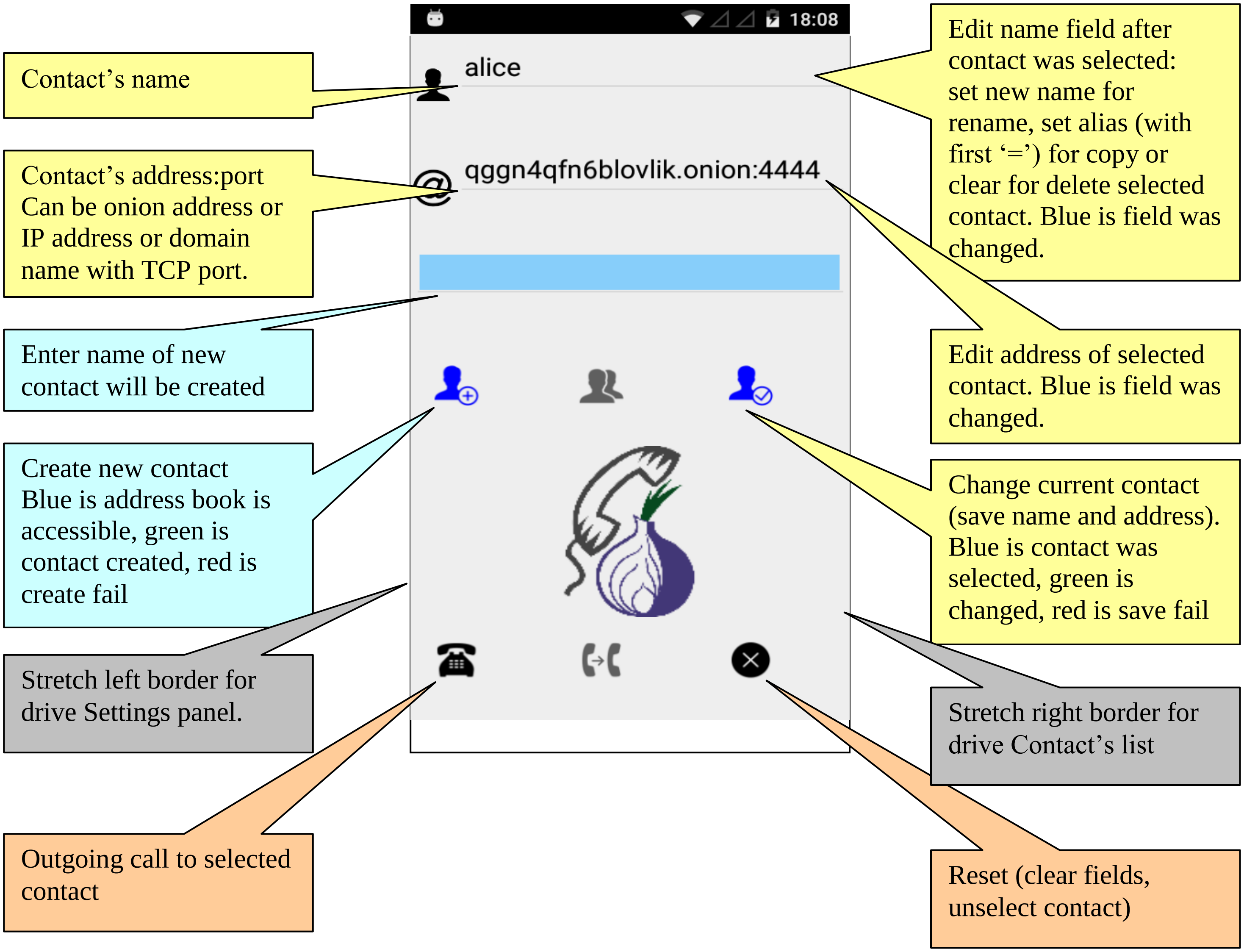
Torfone for Android

1. Install APK, first run Torfone, input password (1-31 chars, default is ‘password’) on blue field and press ‘OK’ button (top-left). Note: you can’t change this password later!
2. Wait for initializing. Stretch left screen border to open Settings panel. Copy your onion address generated by Tor on first start. You will send this address to your friends.
3. Get onion address from you friend.
4. Create temporary contact: press “New” button (top-left), input any contact’s name in blue field (avoid locals characters: not all Androids support correctly) up to 15 chars and press “New” button once more. New contact will be created.
5. Stretch right screen border to open Contacts list. Tap on created contact (select it). Close Contact’s list.
6. Paste or enter onion address of your friend in address field. Press “Change” button (top-right) for save.
7. Now you can call to you friend: open Contact’s list, select contact and press “Call” button (bottom-left). Wait for connecting over Tor.
8. On incoming call you friend press “Call” button (bottom-left) for answer. For terminate call press “Cancel” button (bottom-right).
9. During first call exchange your contacts: parties open Contact’s list and click on ‘*Myself’ entry for sending his contact to remote. Received contact will be add to address book with generated name as ‘+’ then current session ID then key fingerprint.
10. After call you can compare session IDs must be the same on both sides for ensure session was safe.
11. You must rename received contact to any other name without ‘+’ on the start. After this you will authenticate himself to this contact on incoming call.
12. You can delete temporary contact created manually: select it, erase name field and press “Change” button (top-right). Contact will be deleted from book.
13. Authenticated call has smaller latency: two onion connecting will be used in parallel.
14. You CAN switch to un-anonymous direct P2P UDP connecting: both parties must press “Direct” button (bottom-middle) for start NAT traversal. Button will be green on success.

Main panel



18:08

alice

qggn4qfn6blovlik.onion:4444

Contact’s name

Contact’s address:port
Can be onion address or IP address or domain name with TCP port.

Enter name of new contact will be created

Create new contact
Blue is address book is accessible, green is contact created, red is create fail

Stretch left border for drive Settings panel.

Outgoing call to selected contact

Edit name field after contact was selected: set new name for rename, set alias (with first ‘=’) for copy or clear for delete selected contact. Blue is field was changed.

Edit address of selected contact. Blue is field was changed.

Change current contact (save name and address). Blue is contact was selected, green is changed, red is save fail

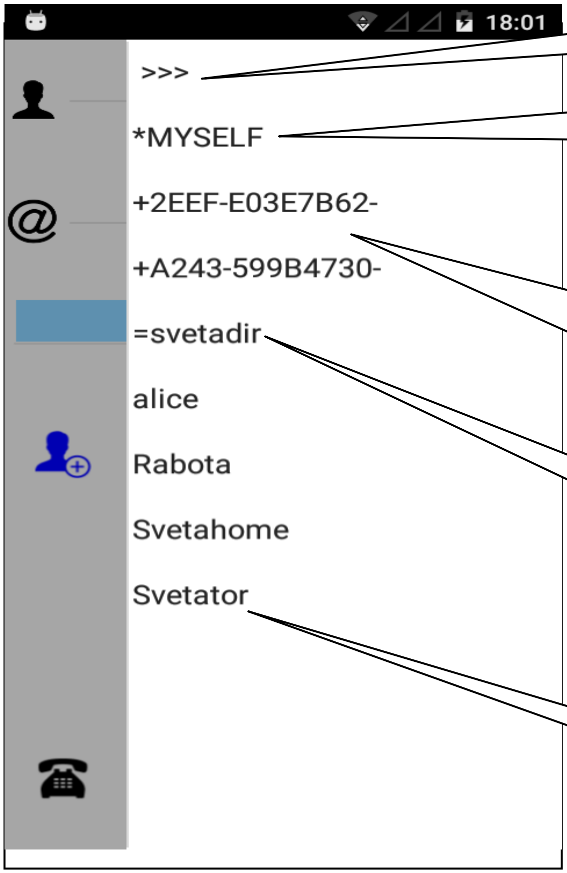
Stretch right border for drive Contact’s list

Reset (clear fields, unselect contact)

Contact's list

Tap contact for selection in idle state. You can modify selected contact or provide outgoing call to it.

Tap contact for sending to remote side during a call. You can send *MYSELF or any other contact from your book. Name of contact in your book will not be reveal: on remote side new name will be generated automatically. Contact's address and key will be copied to address book of remote party.



18:01

>>>

*MYSELF

+2EEF-E03E7B62-

+A243-599B4730-

=svetadir

alice

Rabota

Svetahome

Svetator

Close list, go back to main phone panel

Me (our onion address generated by Tor with specified listening port)

Contact received from remote during call. Name was generated as '+', session code and key's fingerprint

Alias (copy of contact with different name / address but same key). Name must start as '='

Created or renamed contact

Note 1: on incoming call outputs name of parent contact, not aliases (contacts with first symbol '='). If parent contact was deleted then outputs first found alias.

Note 2: for contacts with first symbol '+' (received from remote/not renamed or created manually) Torfone will not be authenticate himself on incoming call (for protect own identity from scanning by unknown contacts). Rename received contact only if you trust this sender.

Settings:

Our onion address:port Set '?' for show actual onion generated by Tor

SOCKS5 port of internal Tor. Set '0' for disable internal Tor.

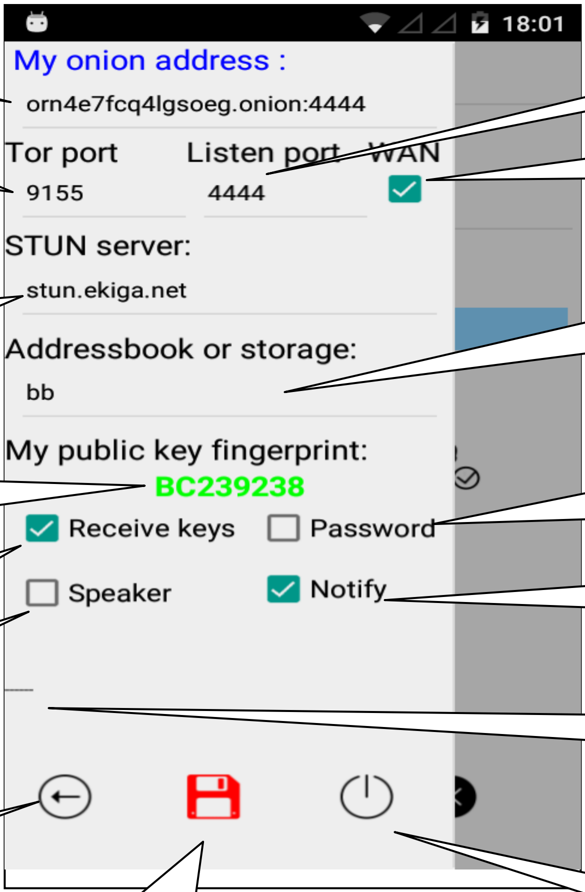
STUN server for NAT traversal. Uses only for optional switch to P2P UDP connecting

Fingerprint of our public key generated on first start. Green is TCP listener is OK, red is fail.

Allow automatically receiving of contacts during call.

Set media voice path (loudspeaker) instead earphone.

Close Settings panel, go back to main phone panel



My onion address :

orn4e7fcq4lgsoeg.onion:4444

Tor port	Listen port	WAN
9155	4444	☑

STUN server:

stun.ekiga.net

Addressbook or storage:

bb

My public key fingerprint:

BC239238

☑ Receive keys □ Password

□ Speaker ☑ Notify

TCP listening port. Can be set in range 1024 – 65535 as a part of your address.

Listen incoming connecting from Internet. If unchecked only connects from Tor will be listened

Encrypted Storage file name in public documents folder. Specify serial device name for use external storage (USB or Bluetooth token).

Enter password any time application is started. If uncheck password will be saved in application private file space.

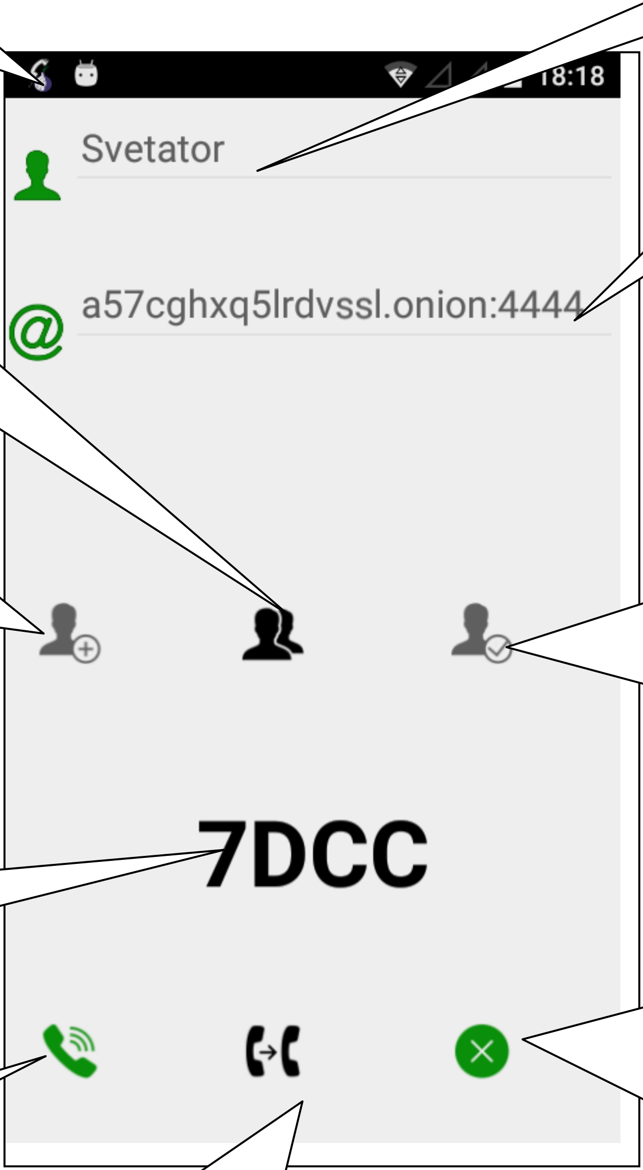
Android notification of incoming calls

Some technical information for debugging.

Exit application (for restart). Note Tor is run as demon so still work after exiting Torfone.

Save settings to ini file. Red after some changes (modified fields are blue). Red Apply icon after setting was saved. Black on unchanged.

Torfone during call:



Svetator

a57cghxq5lrdvssl.onion:4444

7DCC

Notification of incoming call. Stretch panel down and press notification for open Torfone running in background and answer.

Comparing pre-shared secret. Press, input secret in blue field and press again. Other party must do the same.
Blue is other party already input secret and wait your secret.
Green is secret matches.
Red is secrets are different.

Green: contact received from remote party;
Blue: remote party send contact but you deny receiving on Settings panel;
Red: remote party send contact but it is already exists in your book.

Session ID (Short Authentication string). Must be the same on both sides. Compare for ensure call is safe (not intercepted or corrupted).

Answer incoming call. Talk / Mute during call. After changing voice path during call press twice for apply new settings.

Red is outgoing call.
Green is incoming call from Tor
Blue is incoming call from Internet.

Name of remote party (as specified in your address book). Icon will be green if key is matches: this call is trusted.

Address of remote party (as specified in your address book). Icon will be green if onion address is confirmed by Tor

Still Black: not authenticated call
Blue: Remote party is authenticated (contact exist in you book) but onion address is not confirmed (unaccusable or thi is direct call from/to IP address).
Green: Both remote party contact and his onion address are authenticated.
Red: remote party know you but you not have this contact in you book (possible scanning or you delete this contact).

Reset incoming or outgoing call on any stage.

Red is physical outgoing TCP connecting.
Blue is physical incoming TCP connecting.
Green is both outgoing and incoming connections: only for authenticated onion calls acceptor connects to originator in parallel. During this call more slower path can be periodically reconnected for decreasing latency.

Switch to direct P2P UDP connecting. Both parties must tap for initiate NAT traversal.
Red after you allow P2P connecting.
Blue after remote party allow P2P connecting.
Green if P2P is success (not always possible due restricted NATs on both sides).