ZAS Telephone System User Guide

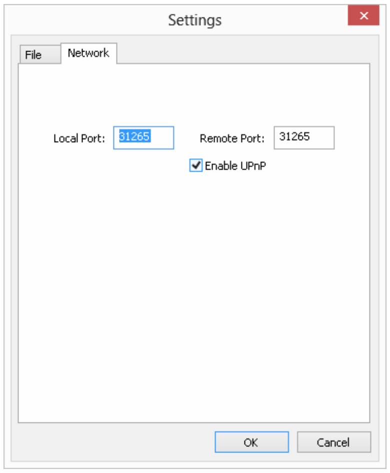
ZAS communicator is open source software, which provides secure voice communication, file transfer and real time text messaging over the Internet. The communication channel is encrypted from one end to the other, so it is impossible to intercept information.

The software runs as standalone application; no installation is necessary. All program files are located in the current folder. The software does not create any records in Windows registry or any files at other locations. You can run ZAS from USB flash drive on guest computer.

System requirements: PC, Windows XP or higher.

Administrator's Guide

The program communicates by UDP using default port 31265 (port could be modified). If you are behind NAT, you have to set up router port forwarding from any external node to IP address and port of computer with application. You can set local and external port to any available in system (local port – port number of computer which runs ZAS software, Remote port – external port number (on the router)). You can set up port forwarding automatically by checking 'Enable UPnP' checkbox. If you prefer setting up port forwarding manually, then 'Enable UPnP' box should be unchecked.

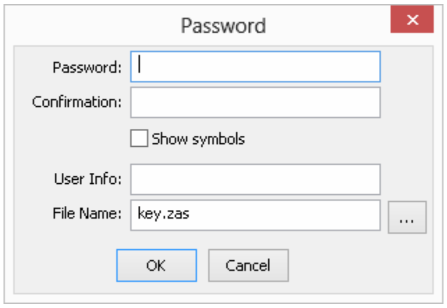


Local Port: 31265

Remote Port: 31265

☑ Enable UPnP

First thing to do is generating your secret key: by menu FILE->generate key. It will request to enter your password and confirm password. You can also enter any information to identify yourself in the network into user information field (this will be shown in the list with connected nodes) and key file name.



Password:

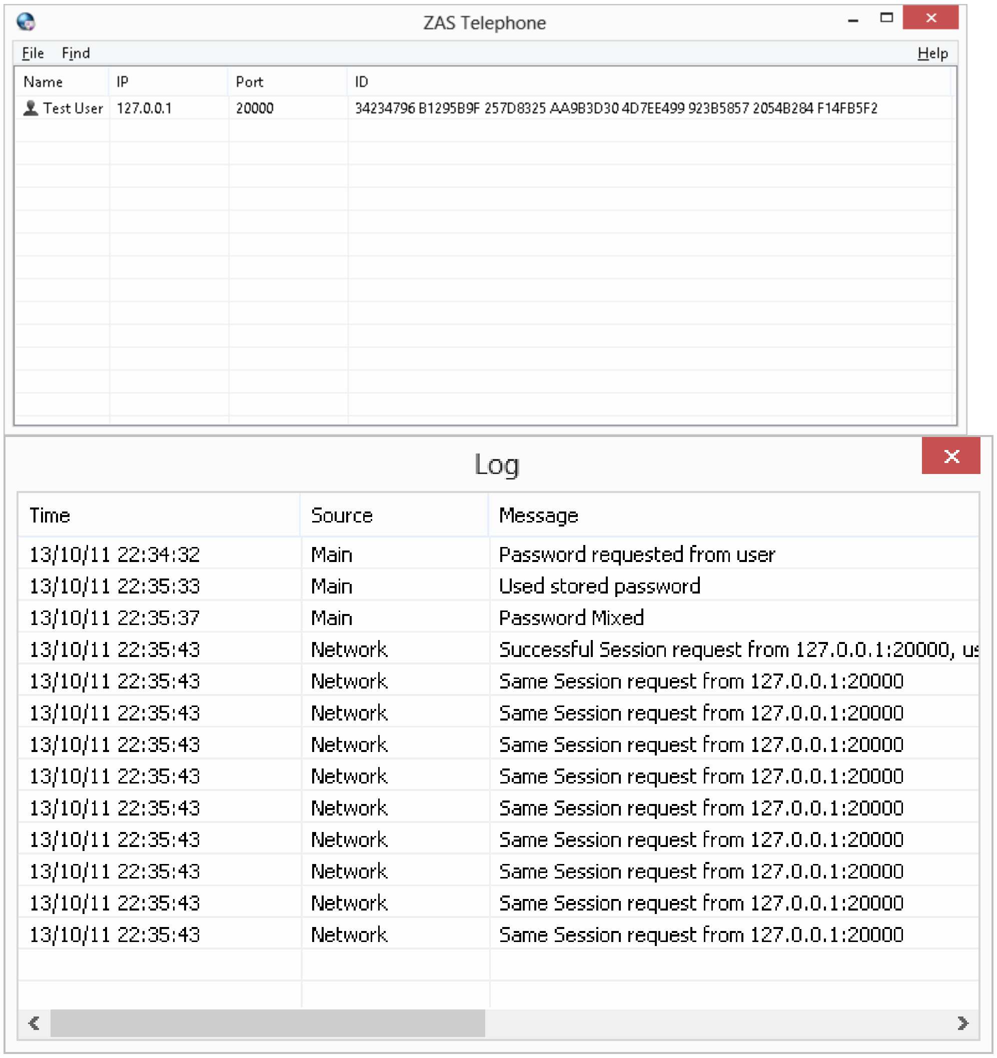
Confirmation:

□ Show symbols

User Info:

File Name: key.zas

That’s it. When a user will connect the information will be updated in the list and shown in the log window.



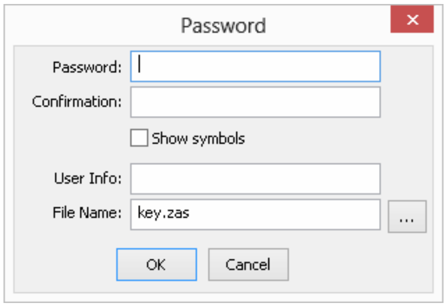
Name	IP	Port	ID
Test User	127.0.0.1	20000	34234796 B1295B9F 257D8325 AA9B3D30 4D7EE499 923B5857 2054B284 F14FB5F2

```
Time                Source    Message
13/10/11 22:34:32   Main      Password requested from user
13/10/11 22:35:33   Main      Used stored password
13/10/11 22:35:37   Main      Password Mixed
13/10/11 22:35:43   Network   Successful Session request from 127.0.0.1:20000, us
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
13/10/11 22:35:43   Network   Same Session request from 127.0.0.1:20000
```

User Guide

The program has tree lists with user: main list with users you are saved for frequent communication. Network list with users who had connection with us from launch of application. Kademlia list with nodes in groups who represent our vision of the network according with KAD architecture (see description below). By default you see only main list.

Before communication start you have to generate your secret key by menu FILE->generate key. Then it would require entering and confirming your password. You can also enter any information to identify yourself in the network into user information field (this will be shown in the list with connected nodes) and key file name.



Password:

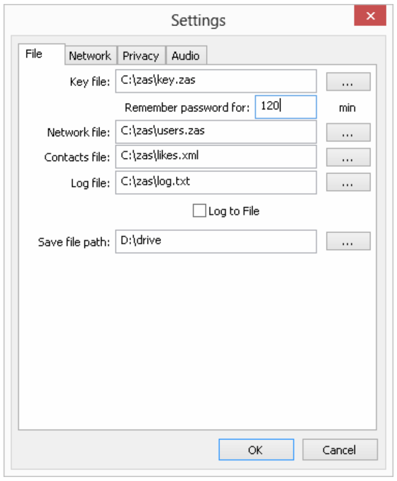
Confirmation:

□ Show symbols

User Info:

File Name: key.zas

All other parameters will be set to default values at first run. The program keeps known node list in xml file that will be created automatically at first launch. You can add additional nodes in the list with IP address or URL and port number (look for examples in the file) <node ip="184.60.28.1" port="31265" url="boot.zas-comm.ru" />.. File paths can be changed in the menu file/settings. File can be downloaded from zas-comm.ru.



Key file: C:\zas\key.zas

Remember password for: 120 min

Network file: C:\zas\users.zas

Contacts file: C:\zas\likes.xml

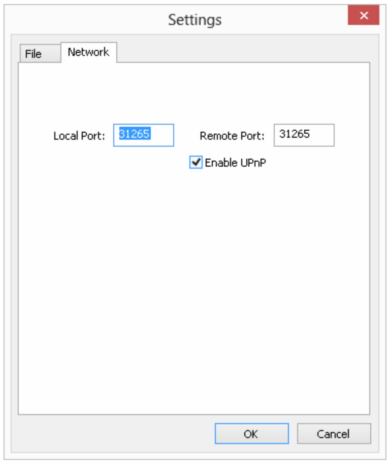
Log file: C:\zas\log.txt

□ Log to File

Save file path: D:\drive

Here key file – secret key file name, Remember password for – cache key user password for required amount of minutes, Network file – file with recent users list in xml format, Contacts file – users in main window (with whom you are more likely to talk), Log file – log file name, Log to File – enable logging to file, Save file path – default path for transferred files.

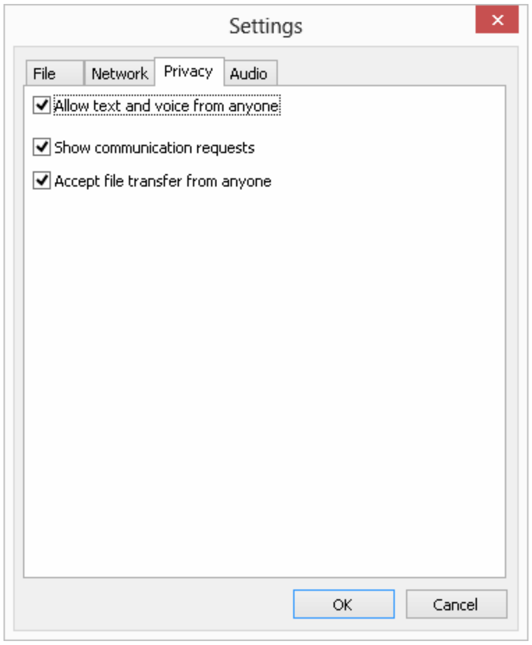
Network tab is to set local and external port for connection if you don't like default settings. Check box Enable will try to set port forwarding from external port of router to local computer port. It will notify in case of failure.



Local Port: 31265 Remote Port: 31265

☑ Enable UPnP

Privacy settings: Allow text and voice from anyone – anyone can send text or call (otherwise only users from main list); Show communication requests – another user can send communication request from right mouse button menu and it can be shown or not; Accept file transfer from anyone – accept files from anyone or only from users in main list.

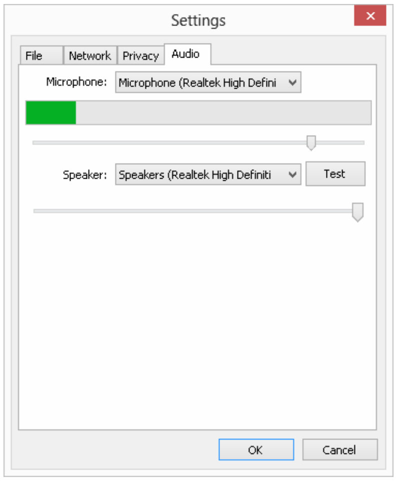


☑ Allow text and voice from anyone

☑ Show communication requests

☑ Accept file transfer from anyone

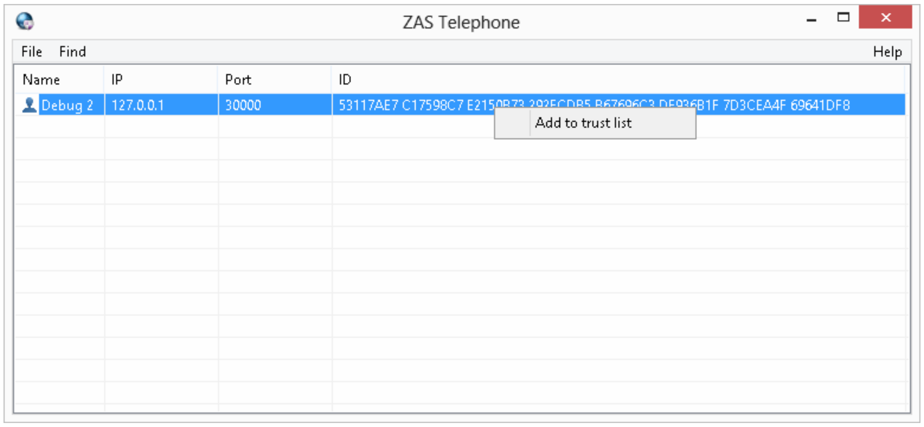
Audio settings (it’s clear):



Microphone: Microphone (Realtek High Defini

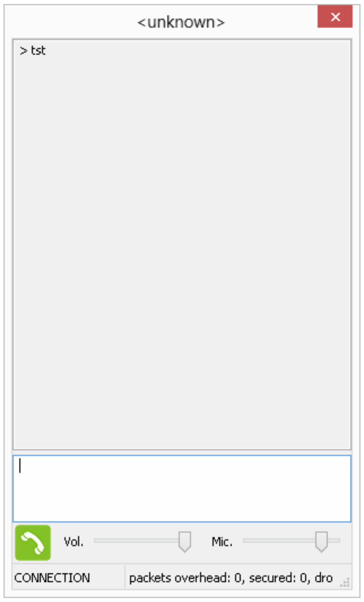
Speaker: Speakers (Realtek High Definiti

When everything is set up (or used default settings) you have to connect to the network by the menu file/bootstrap. Information about connection will be displayed in log window. Finally user list will be populated with nodes which are currently online. Mouse right button click on the node will give you opportunity do add the node in main list. If you don't trust user anymore you can remove him/her from list by the same way. You can add users from Network and KADEMLIA lists to the main list. You can remove user from main list just click right mouse button.



Name	IP	Port	ID
Debug 2	127.0.0.1	30000	53117AE7 C17598C7 E2150B73 292FCDB5 B67696C3 DF936B1F 7D3CEA4F 69641DF8

Mouse double click will open dialog box where you can write a message or make voice call (press Dial for that). All messaging and the voice channel are always encrypted. There are controls for volume and microphone speech level on the right side from Dial button. You can see the name of the user in window's caption.

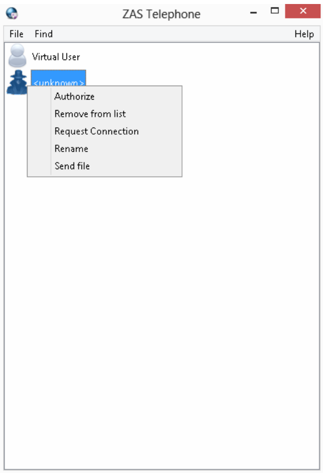


> tst

CONNECTION | packets overhead: 0, secured: 0, dro

In the status bar you can see connection status and number of packets sent and received, and the network maintenance overhead.

Users in the main menu have different icon (it depends on status). Black – unauthorized user, grey – user is offline, blue – user is online. Mouse right button click will show the menu: Authorize – authorize with confirmation, Remove from list – delete from list, Request connection – the only one way to communicate with user with no-anyone privacy setting is communication request (it can be also disabled, see privacy settings). Rename – rename the user locally, send file – send request for file transfer.



System Architecture

The network architecture is based on the serverless approach known as Kademlia. There are no dedicated servers in the system. Every node keeps information about part of the network and provides this information to another nodes by request. A node is identified by 256-bit fingerprint of its unique secret key. So a node can't impersonate another node as long as it haven't got secret key with exactly the same fingerprint. The program security is based on the fact that it's impossible to generate the key with required fingerprint in any reasonable amount of time. But even if the enemy would try to impersonate a valid system user he won't be able to decode any information; as the key exchange occurs at connection establishing phase.

For normal operation, a connection with at least one active node (bootstrap) is required. That node will send list of known users. This bootstrap can be any node in system. The list of known nodes is collected automatically during normal operation of ZAS software.

For the very first start it's better to set bootstrap node which is always online like zas-comm.ru:31625. You can also manually modify file with Network data by adding new nodes and removing old ones.

Additional information about networking principles could be found in the Internet by searching on key word "Kademlia".

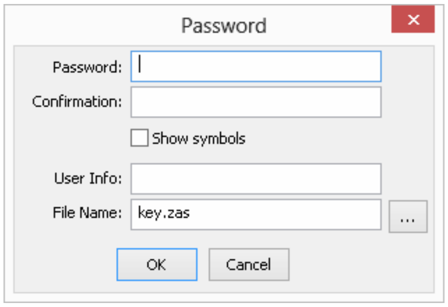
Before start of any communication in the network secured channel is established and session is kept until the program is terminated or the connection is reset. Encrypted channels always transfer all of the networking data such as search requests etc.. Although the fact of communication between nodes is visible, the information content can't be monitored.

Direct connection mode

ZAS could be used for direct connection between just two private users or small group of users.

Here is how:

1. Users have to create their own keys (menu FILE->Generate Key)



Password

Password:

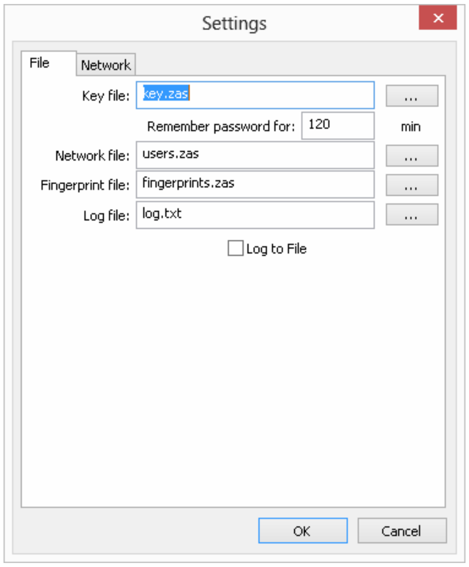
Confirmation:

□ Show symbols

User Info:

File Name: key.zas

Or select file name with existing keys (menu FILE->settings)



Settings

File | Network

Key file: key.zas

Remember password for: 120 min

Network file: users.zas

Fingerprint file: fingerprints.zas

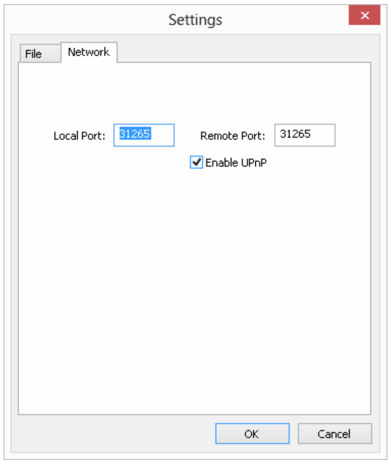
Log file: log.txt

□ Log to File

2. Set IP address and port in xml file with user list on one of the computers. The default port is 31256 however you can modify it to anything you like.

   <node ip="193.34.9.170" port="31265" />.

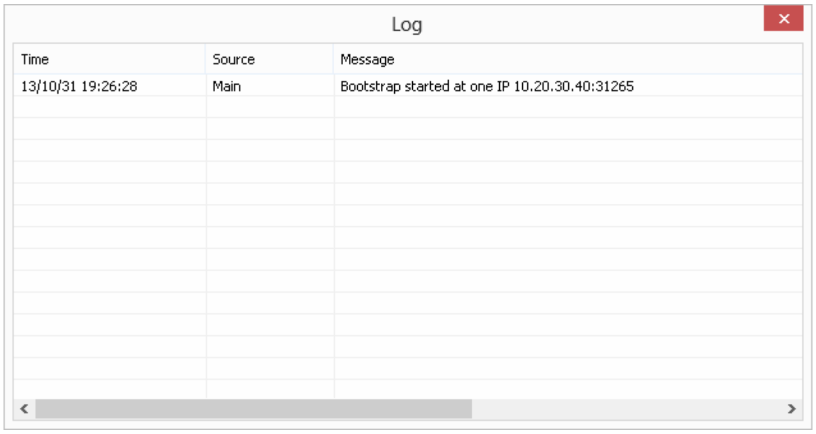
Set up router port forwarding or enable UpnP on both sides (menu FILE->settings Network).



Local Port: 31265 Remote Port: 31265

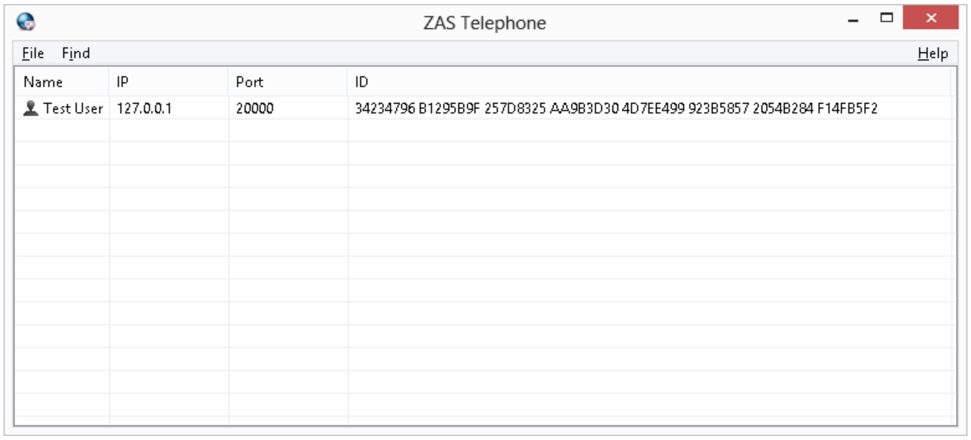
☑ Enable UPnP

3. Next click File/bootstrap in the program with was set up with IP address at step 2. There will be information about bootstrapping on the log window.



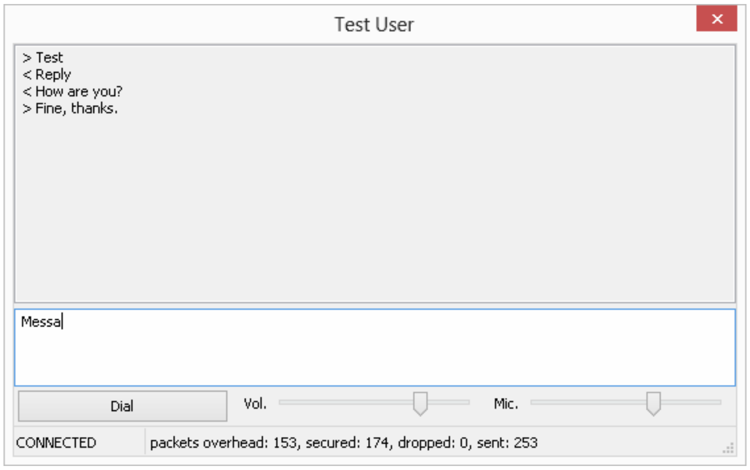
Time	Source	Message
13/10/31 19:26:28	Main	Bootstrap started at one IP 10.20.30.40:31265

4. If everything is OK then opposite user will be shown in user list. It means that secured connection is established and all other communication will be encoded.



Name	IP	Port	ID
Test User	127.0.0.1	20000	34234796 B1295B9F 257D8325 AA9B3D30 4D7EE499 923B5857 2054B284 F14FB5F2

5. Next in any of the programs you can double click user name and start communication



```
> Test
< Reply
< How are you?
> Fine, thanks.
```

Messa

CONNECTED packets overhead: 153, secured: 174, dropped: 0, sent: 253

Security

ZAS provides strong security if your computer is clean from malware or viruses and if the enemies didn't steal your secret key. However keep in mind that no software can protect you from direct eavesdropping.

There is certain possibility of bugs and vulnerabilities in the ZAS software itself. Always keep the software updated to the latest revision. Updating the software is your task; we won't remind you about new versions.

ZAS does not hide your IP address and address of your correspondent. So outside observers can recognize the fact of communication between two of you, but they can't obtain the information itself.

ZAS encryption is based on IDEA and XTEA algorithms. Those algorithms were developed by non-government entities, survived fair amount of analysis and considered proven by time. The initial key exchange is by Diffie-Hellman algorithm using 4096-bit safe primes.

Any system based on open key cryptography is vulnerable to "man-in-the-middle" attacks. Therefore it is necessary for you to verify your correspondent ID and add him to the trust list (make authorized).

ZAS doesn't use PKI, because governments control PKI.

You are free to use open-source ZAS-telephone for any private or commercial purpose. The program is distributed "as is". We make our best effort to create good software, however we don't assume any liabilities and we won't give any guarantees. Use ZAS communicator at your own risk.

Feedback, suggestions and bug reports: zas@zas-comm.ru