Инструкция по эксплуатации системы ZAS Telephone

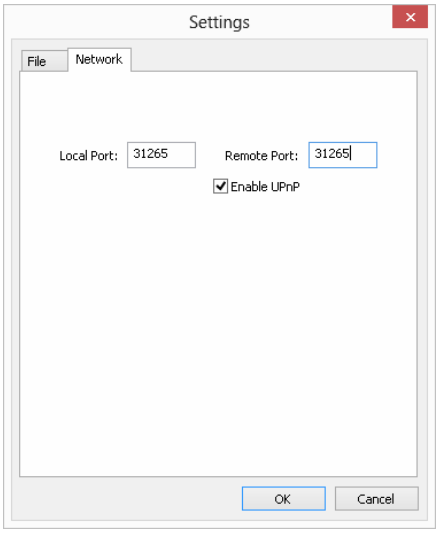
ZAS-telephone - бессерверная сеть, предназначенная для осуществления конфиденциальных телефонных звонков (voice) и обмена текстовыми сообщениями (chat) по защищенному каналу с шифрованием. Шифрование осуществляется от одного компьютера до другого; таким образом, перехватить информацию, идущую по каналу, невозможно.

Программа не требует инсталляции. Все необходимые файлы находятся в текущей директории. Программа не создает записей в реестре и/или файлов в других местах на компьютере. Возможен запуск программы с USB флеш-драйва на гостевом компьютере.

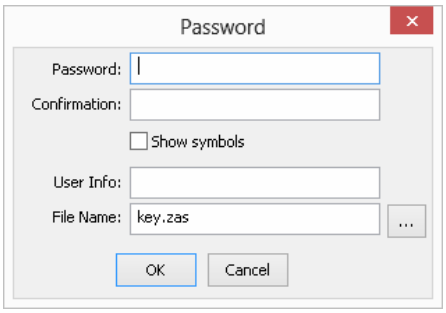
Системные требования: PC, Windows XP и выше.

Руководство администратора

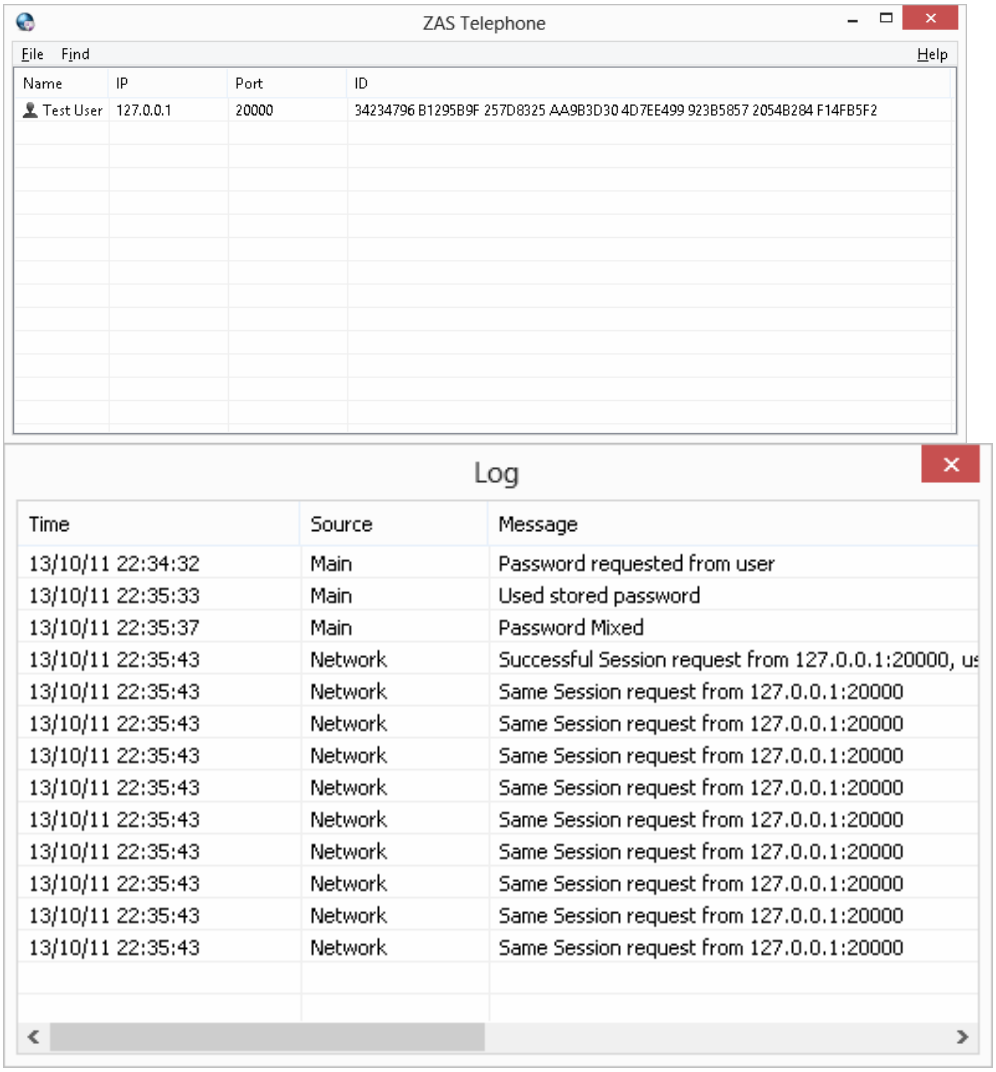
Стандартным портом работы программы является 31265. Протокол обмена UDP. Нужно настроить маршрутизатор для передачи данных с произвольного внешнего порта на IP адрес и указанный порт компьютера где установлена программа. Можно переназначить порты в меню настроек на произвольные (local port – номер открываемого порта компьютера где запущена программа, Remote port – номер порта на маршрутизаторе). Если установить галочку Enable UPnP то программа будет пытаться установить port forwarding. Если маршрутизатор настроен вручную, то галочку следует убрать и поле Remote port игнорируется.



Кроме этого нужно сгенерировать ключ в меню file/generate key. Ввести пароль, подтверждение пароля, имя пользователя (будет отображаться в списке у подключенных клиентов) и имя файла с ключом.



На этом настройка закончена. При подключении клиентов они будут появляться в списке Network и информация о сетевом обмене будет отображаться в окне лога.

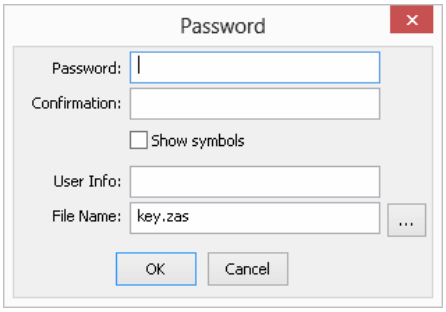


Руководство пользователя

Программа содержит три списка пользователей: главный список, в который можно добавить людей, с которыми чаще всего происходит общение. В этом списке иконка в первом столбце означает доверенный или неизвестный пользователь, во втором столбце – пользователь в сети или не в сети. Сетевой список (Network) в котором перечислены пользователи с которыми когда либо было установлено соединение с момента запуска программы и список KADEMLIA в котором

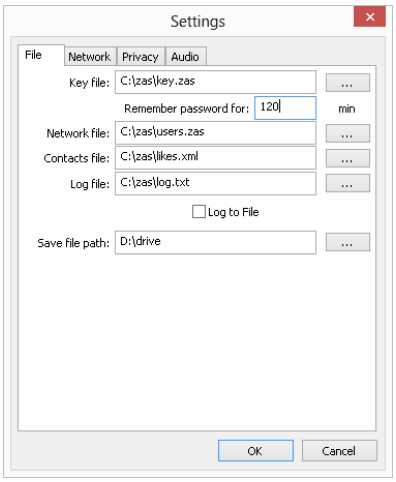
перечислены пользователи по группам (текущая запомненная часть сети). По умолчанию виден только главный список пользователей.

Для работы программы в первую очередь необходимо один раз сгенерировать ваш ключ в меню file/generate key. Ввести пароль, подтверждение пароля, имя пользователя (будет отображаться в списке у подключенных клиентов) и имя файла с ключом.



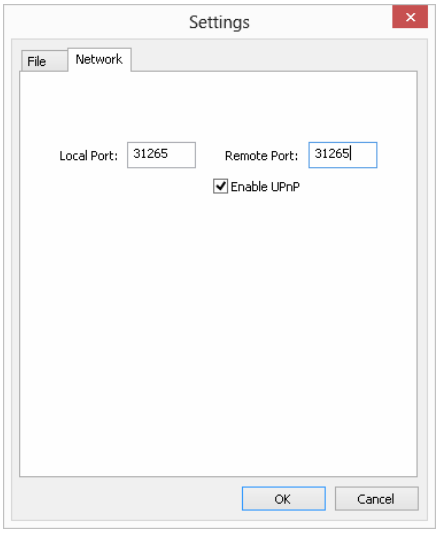
Все остальные параметры будут поставлены автоматически при первом запуске программы. При первом запуске программы файл со списком серверов создастся автоматически. Также его можно скачать с сайта zas-comm.ru.

Его в дальнейшем можно редактировать, добавляя строчки в xml формате <node ip="184.60.28.1" port="31265" url="boot.zas-comm.ru" />. Имена и пути всех файлов задаются в меню file/settings.



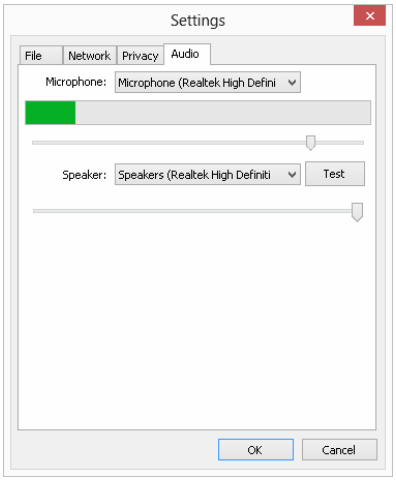
Здесь key file – имя файла с ключом, Remember password for – запомнить введенный пользователем пароль на указанное число минут (0 – помнить до закрытия программы), Network file – файл со списком серверов, Contacts file – файл со списком пользователей в главном списке программы, Log file – имя лог-файла, Log to File – записывать лог в файл, Save file path – путь куда сохранять принятые файлы по умолчанию.

В меню настройки соединения (Network) можно указать локальный и удаленный порт. Галочка Enable UPnP устанавливает перебрасывание (port forwarding) с внешнего порта маршрутизатора на локальный порт компьютера.

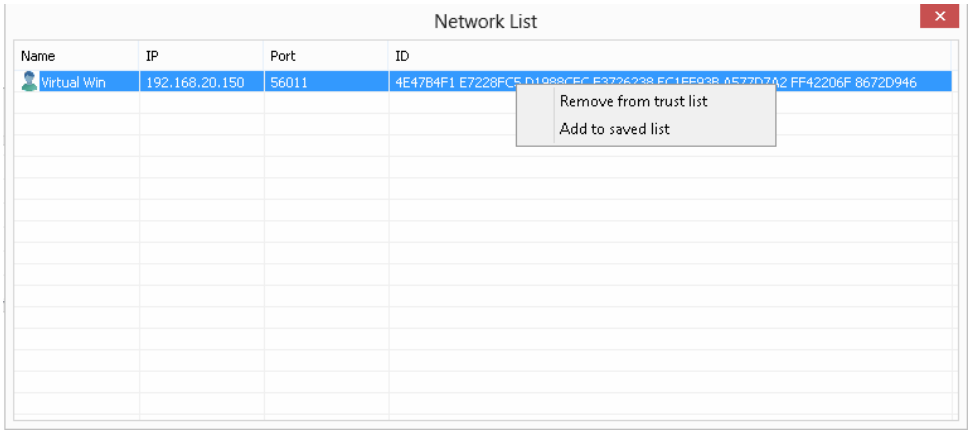


Настройки приватности (Privacy): Allow text and voice from anyone – разрешить автоматическое открытие диалога при получении текстового сообщения или звонка от любого пользователя сети или только от того кто в главном списке; Show communication requests – показывать запрос на установления соединения (может быть запрошен из меню при нажатии правой кнопкой мышки на пользователе из главного списка); Accept file transfer from anyone – разрешать запрос на передачу файлов от любого пользователя.

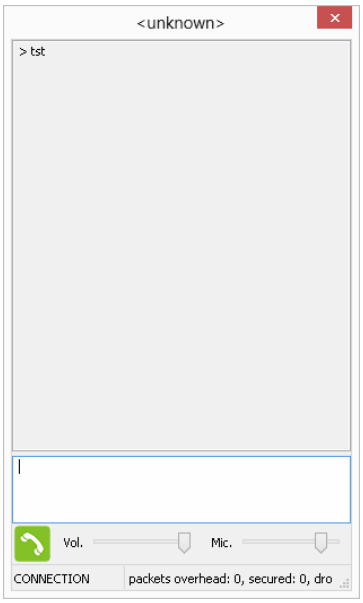
Аудио настройки (говорят сами за себя):



Когда все настройки сделаны (или использованы по умолчанию) нужно запустить соединение с сервером нажав кнопку file/bootstrap (bootstrap запускается автоматически при старте программы). Информация о прохождении соединения будет указана в окне лога. В конечном итоге в списке Network появятся пользователи, с которыми происходил обмен данными. Если нажать правкой кнопкой мышки на имя пользователя, то появится возможность добавить его в главный лист (main list).

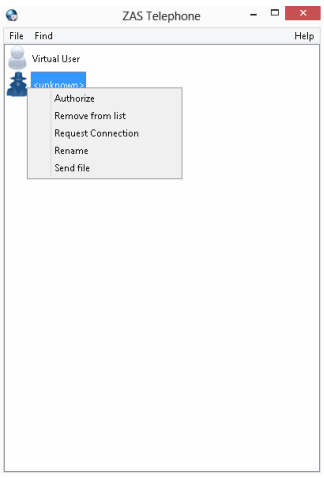


Двойной клик на имени пользователя в любом из списков открывает диалоговое окно в котором можно написать сообщение или позвонить, нажав кнопку Dial. Все сообщения и звуковой канал зашифрованы ключами. Справа от кнопки Dial находятся регуляторы громкости динамиков и чувствительности микрофона. В заголовке окна указано имя пользователя, с которым происходит общение.



В строке состояния отображается текущее состояние соединения и количество посланных, принятых зашифрованных пакетов, отклоненных пакетов и пакетов для установки соединения.

Пользователи в главном списке имеют изменяющуюся иконку в зависимости от состояния. Черная – пользователь не авторизован, серая – пользователь не в сети, синяя – пользователь в сети. По нажатию правой кнопки мышки на пользователе из главного списка можно выбрать следующие команды: Authorize – авторизовать (с подтверждением), Remove from list – удалить из листа, Request connection – запросить соединение (единственный способ связаться с пользователем если вы не в его списке и в настройках приватности не установлено разрешение принимать сообщения от всех пользователей). Rename – переименовать пользователя, send file – послать файл.



Принцип построения системы

Сетевая иерархия системы построена на принципах Kademlia широко используемой в различных сетях с распределенной инфраструктурой. В системе нет централизованного сервера, каждый из узлов сети хранит информацию о части сети и выдает ее по запросу. В качестве идентификаторов узлов используются 256-битные следы (fingerprint) используемых ключей. Таким образом, никакой узел не может выдать себя за другой узел, если не владеет секретным ключом с этим

следом. Безопасность программы основана, в том числе, на трудности сгенерировать ключ с заданным следом за разумное количество времени. Но даже выдав себя за другого пользователя, злоумышленник не сможет подслушать передаваемую информацию правильному пользователю, т.к. уникальные ключи генерируются на этапе установления соединения. Однако для нормальной работы программы после запуска необходимо установить связь с хотя бы одним узлом (bootstrap сервер) и получить список узлов с него. В качестве таких серверов могут использоваться любые узлы системы, но предпочтительно указывать те, которые всегда включены, например zas-comm.ru:31625. В процессе работы программа накапливает данные о пользователях и сохраняет их в файле, указанном в параметре Network file. Пользователь может добавлять свои сервера в этот файл и удалять существующие. В данном файле записи могут быт в виде URL:port или IP:port.

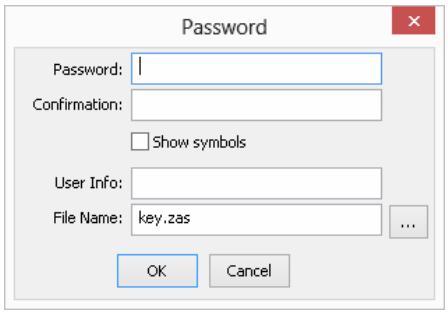
Каждый узел в сети хранит и обновляет информацию о части сети разделенные в группы по степени близости ID узлов. В каждой группе содержится до N (параметр компиляции) записей. Под записью понимается сочетание ID,IP,port. Количество узлов в некоторых группах никогда не достигают числа N по причине отсутствия возможных ID с соответствующим расстоянием до узла. При получении поискового запроса от другого узла ему пересылаются все записи с наиболее близкой к запрашиваемому узлу группы. Если в данном ответе не содержится информация о искомом узле Подробнее о принципах построения сети можно узнать в описании Kademlia.

Перед любым запросом или ответом устанавливается зашифрованный канал связи между узлами и сессия хранится до выключения программы или переустановки соединения. Все поисковые запросы, не говоря уже о пользовательских данных, передаются через зашифрованный канал связи, однако сам факт коммуникации между узлами может быть обнаружен злоумышленником.

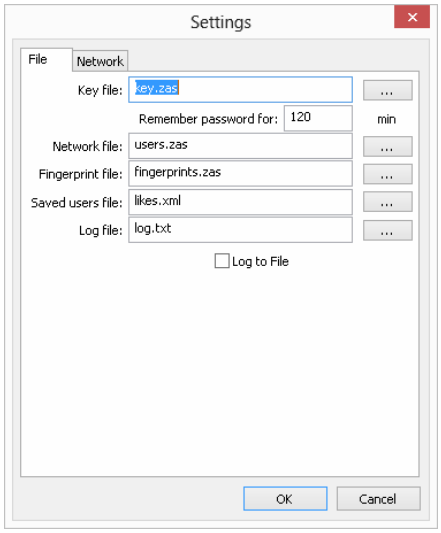
Непосредственное соединение двух пользователей

Возможна работа программы с индивидуальным соединением двух (или более) определенных пользователей. Для этого необходимо:

1. каждому из пользователей сгенерировать новый ключ (меню File/Generate Key)

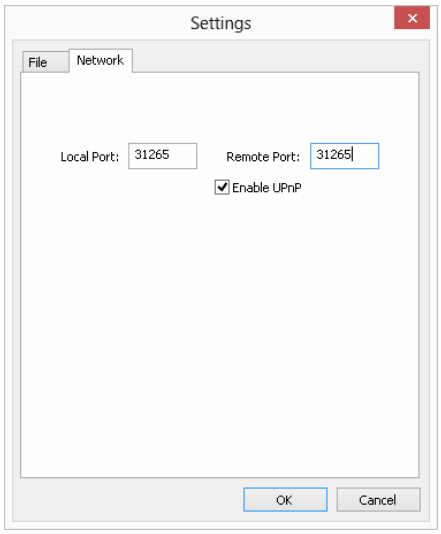


или указать в настройках (меню File/settings) файл с существующим ключом

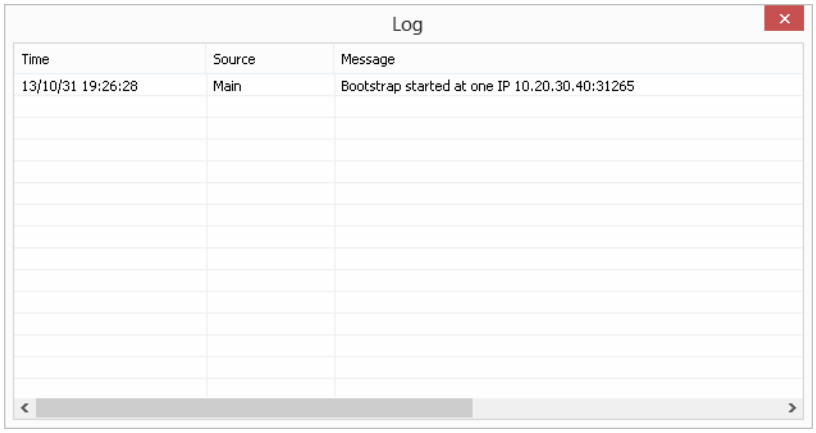


2. В настройках одной из программ прописать в файле пользователей ip и порт либо url и порт в xml формате <node ip="184.60.28.1" port="31265" url="boot.zas-comm.ru" />. Порт можно оставить по умолчанию 31256 на обоих программах.

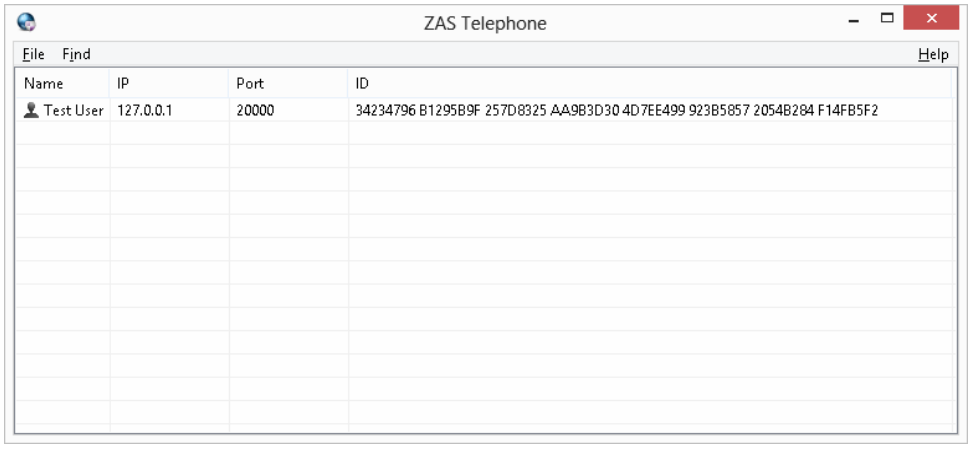
3. На обеих сторонах нужно либо вручную разрешить в маршрутизаторе перебрасывание портов (port forwarding) либо установить галочку UPnP в сетевых настройках программы (меню File/settings вкладка Network).



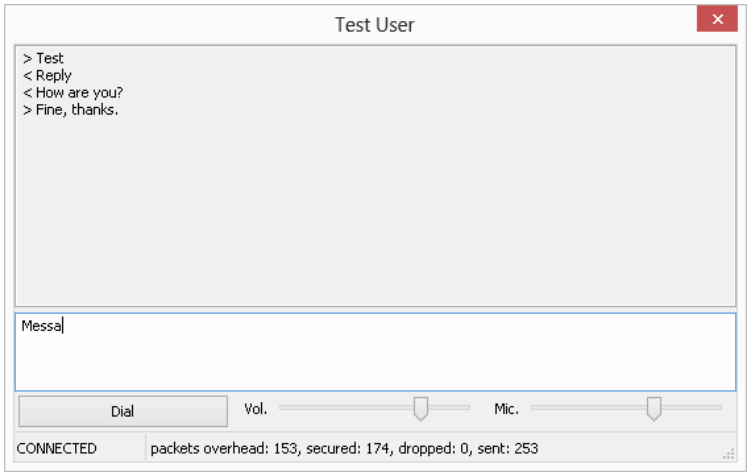
4. Далее выбираем команду File/bootstrap в той программе, в которой настраивали IP адрес в пункте 2 и видим сообщение в логе о том что началась установка соединения.



5. Если все настроено правильно, то через несколько секунд в списке пользователей Network и KADEMLIA обеих программ появится второй абонент. Это означает что между пользователями уже установлено зашифрованное соединение и весь дальнейший обмен информацией будет секретным.



6. Далее в любой из программ по двойному клику на абоненте в любом списке можно запустить диалоговое окно и начать текстовое общение или звуковое по нажатию кнопки dial



О безопасности

ZAS обеспечивает безопасность и конфиденциальность информации, при условии что компьютер не захвачен троянами, и секретный ключ не попал в руки противника. Также, имейте в виду, что никакая программа не может защитить вас от прямого подслушивания и подсматривания.

Не исключено наличие багов и уязвимостей в самой программе. Регулярно обновляйте версию.

ZAS не обеспечивает сокрытия вашего IP адреса и адреса вашего корреспондента; таким образом, сторонним наблюдателям может быть известно о факте связи между вами; хотя неизвестно содержание связи.

Для шифрования используются алгоритмы IDEA и XTEA, разработанные неправительственными организациями и выдержавшие множество проверок. Начальный обмен на открытых ключах происходит по схеме Диффи - Хеллмана с использованием 4096-битных чисел.

Любая система на открытых ключах подвержена атакам типа "человек в середине". Это значит, что при первом разговоре с вашим абонентом вы должны верифицировать ID друг друга и добавить в главный список.

ZAS концептуально не использует PKI, так как PKI контроллируется.

Вы можете использовать open-source программу ZAS с зашифрованным каналом связи для личных и коммерческих целей. Программа поставляется как есть. Мы старались все сделать хорошо и правильно, однако мы не берем на себя никаких обязательств и не даем никаких гарантий. Используйте на свой страх и риск.

Пожелания, предложения и замеченные баги присылайте на адрес zas@zas-comm.ru