Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

table of contents

Signiert von: Heinrich Georg Elsigan
Datum: 08.04.2025 16:35:09

TRUST

Dieses Dokument ist digital signiert!
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

thanks to

Normally, thanks to are always at the end of each paper,
but the people or organizations I benefited from while trying to make AES strong again are more important than a simple proof of concept showing that it works, except on my raw experimental test form.

https://www.bouncycastle.org/

https://www.schneier.com/

https://github.com/dotnet/

https://github.com/microsoft

https://git.lysator.liu.se/nettle/nettle (real easy to read c/c++ code)

source code of secure chat is available at GitHub

https://github.com/heinrichelsigan/chat-ipv6

secure chat Winx86/x64 client download

go to https://cqrxs.eu/download/ and choose latest version.

Attention, version before March 2025 have a ***3-fish over Aes-Engine*** encryption bug, because 3-fish uses AES default block size and key length and Bouncy Castle Aes-Engine parameters. It works, but settings AES default engine for 3-fish, isn't so serious and please download version after March 30.

Besten Dank und freundliche Grüße,

(Heinrich Elsigan)

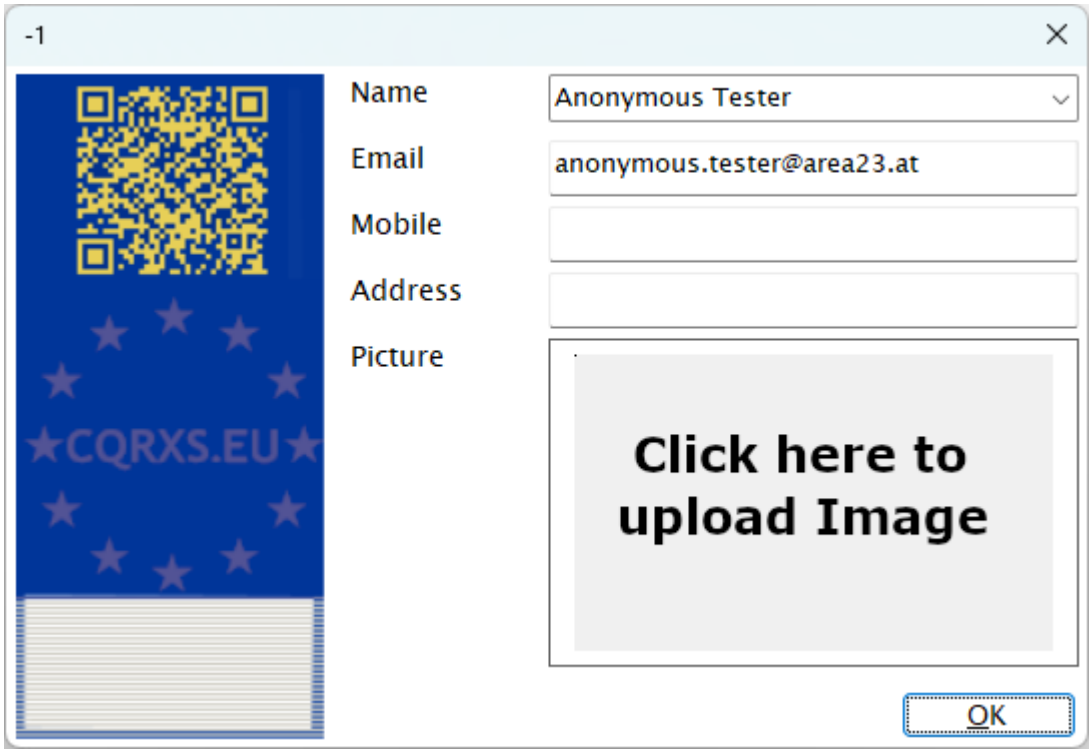
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

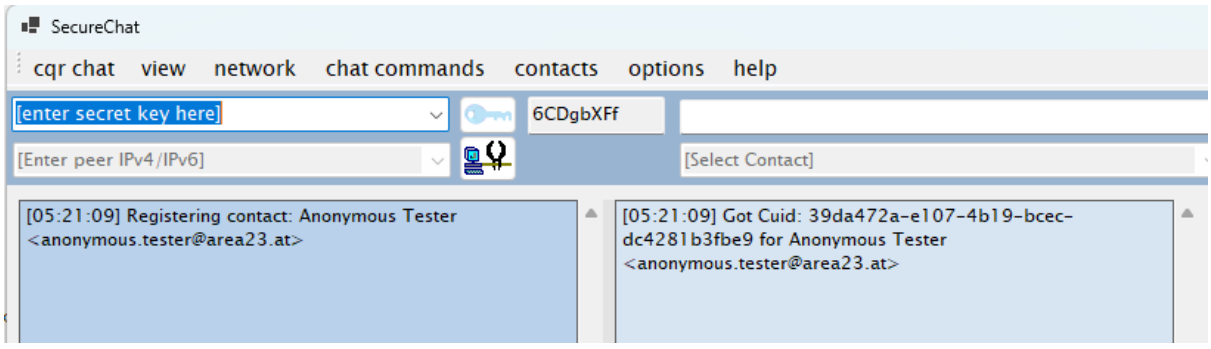
UID ATU72804824

Wien, 9. März 2025

secure chat startup

First, when starting application, you have to enter some kind of nickname and a valid email address. You can upload a picture, but it will not be transferred for now.





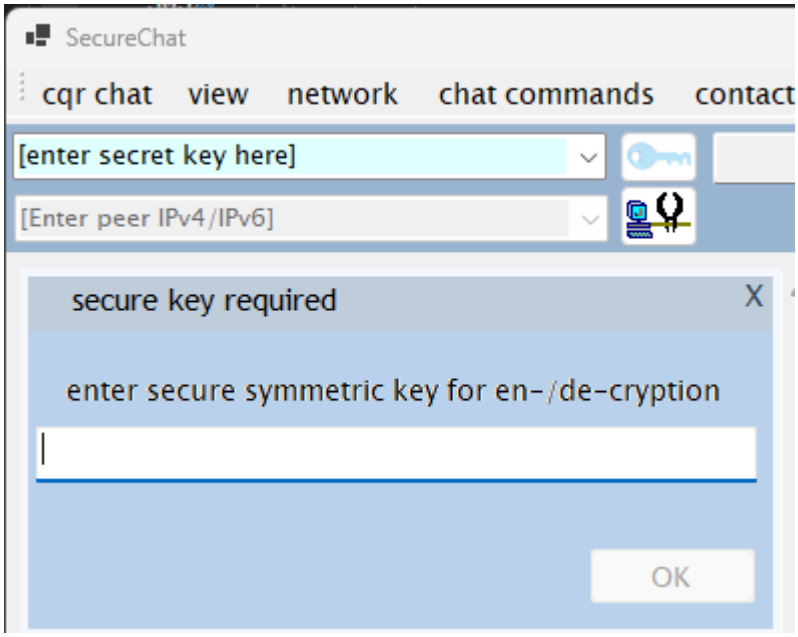
After starting Secure Chat Windows Client, you must enter a shared secure key for all modes.

Unless you don't enter at least 2 characters, you will asked again to enter a secure key.

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025



Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

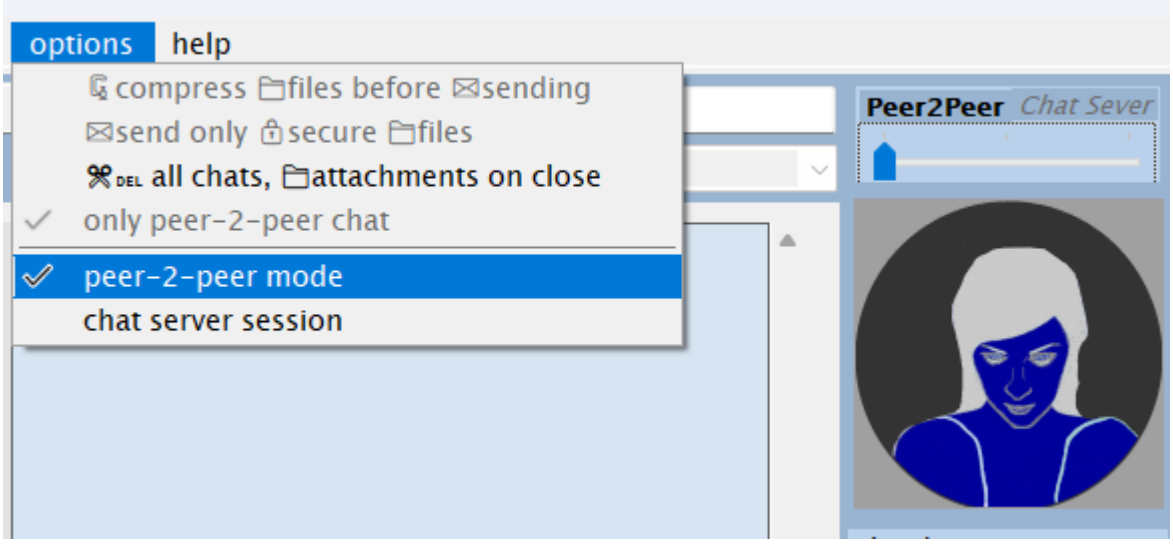
Wien, 9. März 2025

secure chat modes

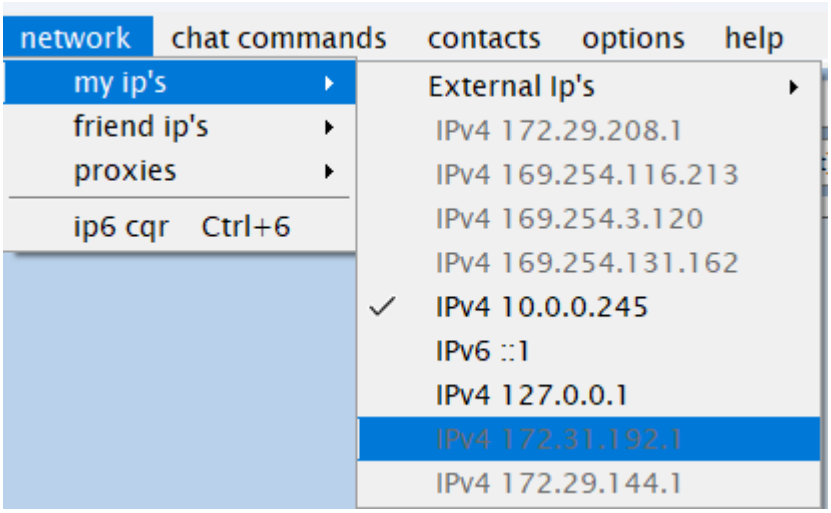
Secure chat supports 2 modes.

peer-2-peer mode

In peer-2-peer mode, no connection to cqrxs.eu server is made and chat msg will be send peer to peer between to chat clients. Each chat client opens a server socket on interface ifx:7777 to receive messages. You can choose only 1 network interface, where chat application should listen and switch between different interfaces



By default, the network interface with connection to the internet is chosen,
if IPv6 is available with route to ::0 access to internet, IPv6 address will be selected by default.



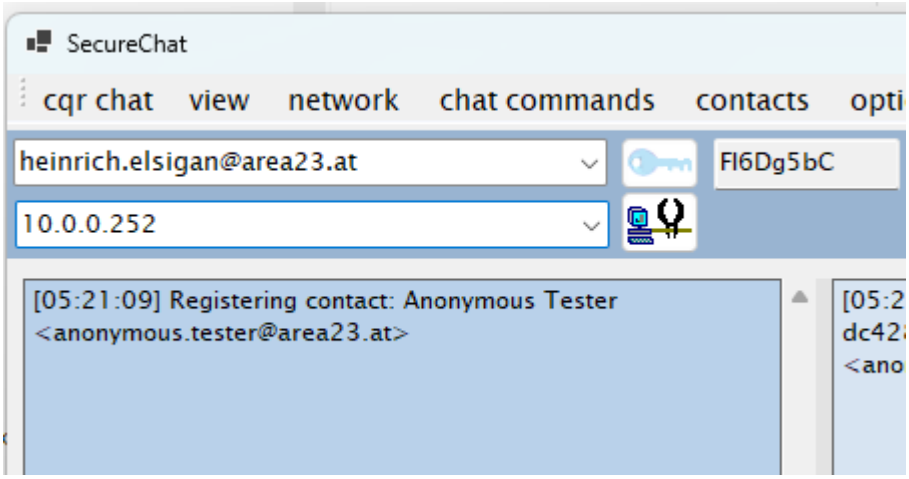
Grayed addresses don't have a route to **0/0** or **::0** at the moment, you can choose them.
Loopback adapters aren't grayed, you can choose them to chat via loopback with yourself. (echo lo).

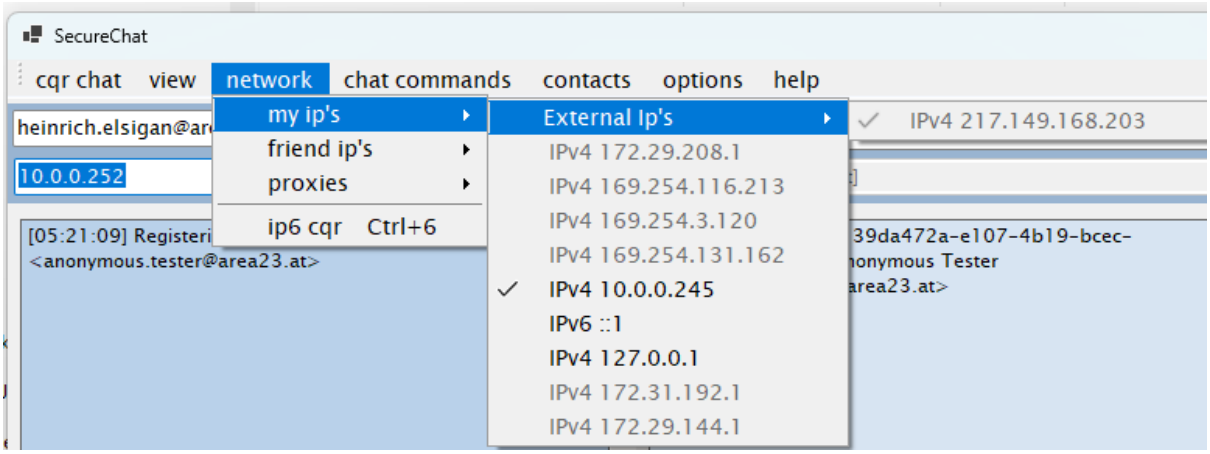
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

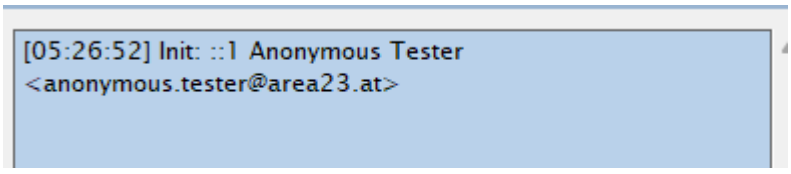
Wien, 9. März 2025

Then enter in IP-Address Box a valid over interface, you choosed before, reachable IP, where your partner has also a secure chat app running.

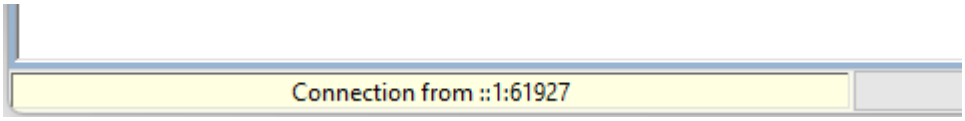




When partner ip is connectable and a socket connection to partner IP port 7777 could be established, then you will get a notification.



See more information at status label at bottom.



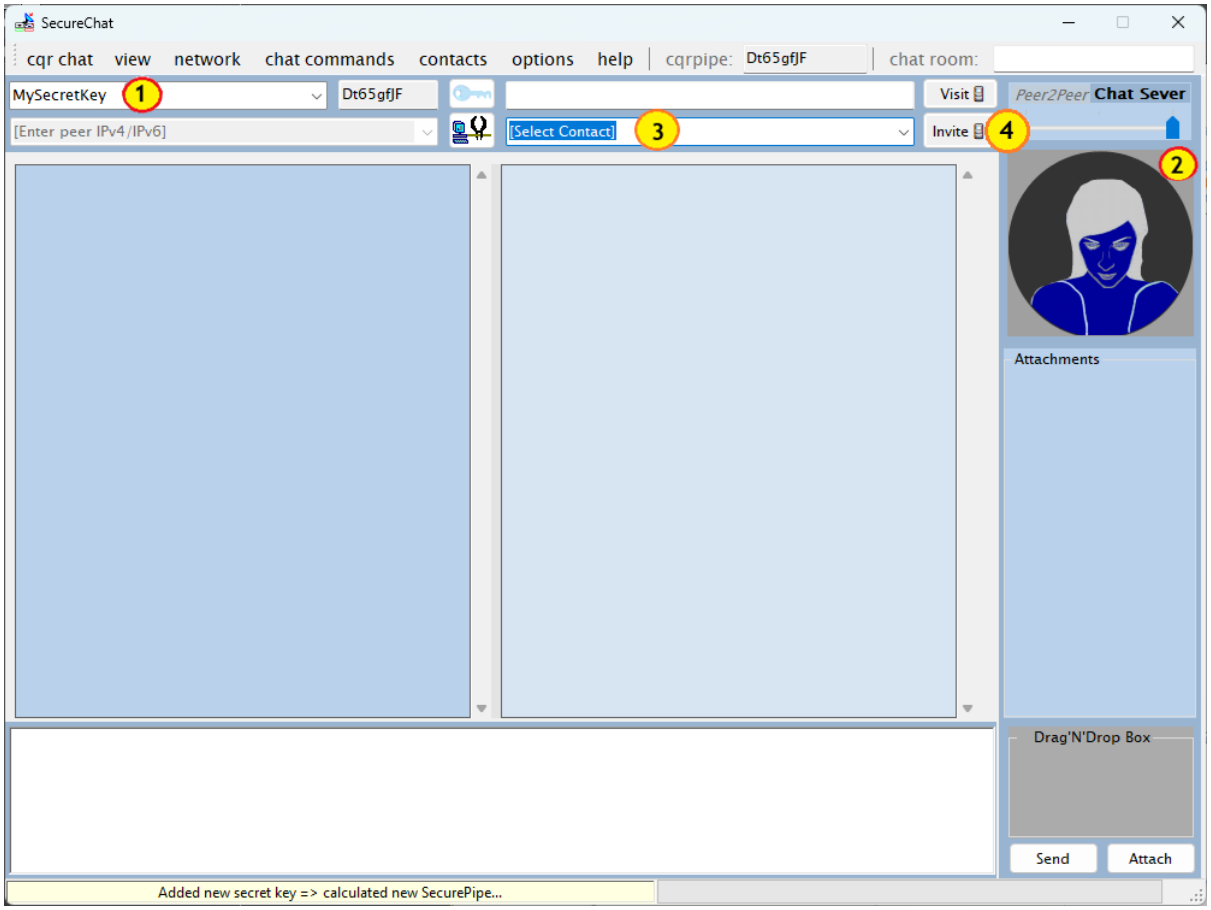
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

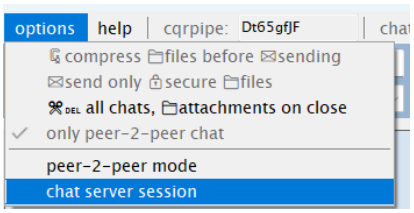
Wien, 9. März 2025

chat server session mode

secure chat app connects to WS on AWS in spain: https://cqrxs.eu/cqrsrv/cqrjd/CqrService.asmx
In chat server session mode, you must import contacts first, see section import contacts.

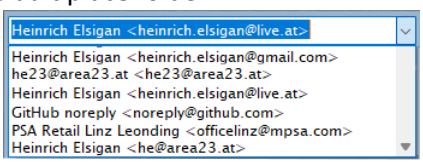


(1) No matter if ***peer-2-peer*** or ***chat-server*** mode, you need to enter first a shared key.
(2) After entering shared key, toogle at right top mode to ***chat-server***



or select in menu options “chat server session”:

(3) When most contacts has been imported or added manually,
go to *Contacts ComboBox*, where [Select Contact] is default placeholder.



Select contact, which you want to invite to chat room:

(4) When chosen and selected contact to invite, click Invite Button

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

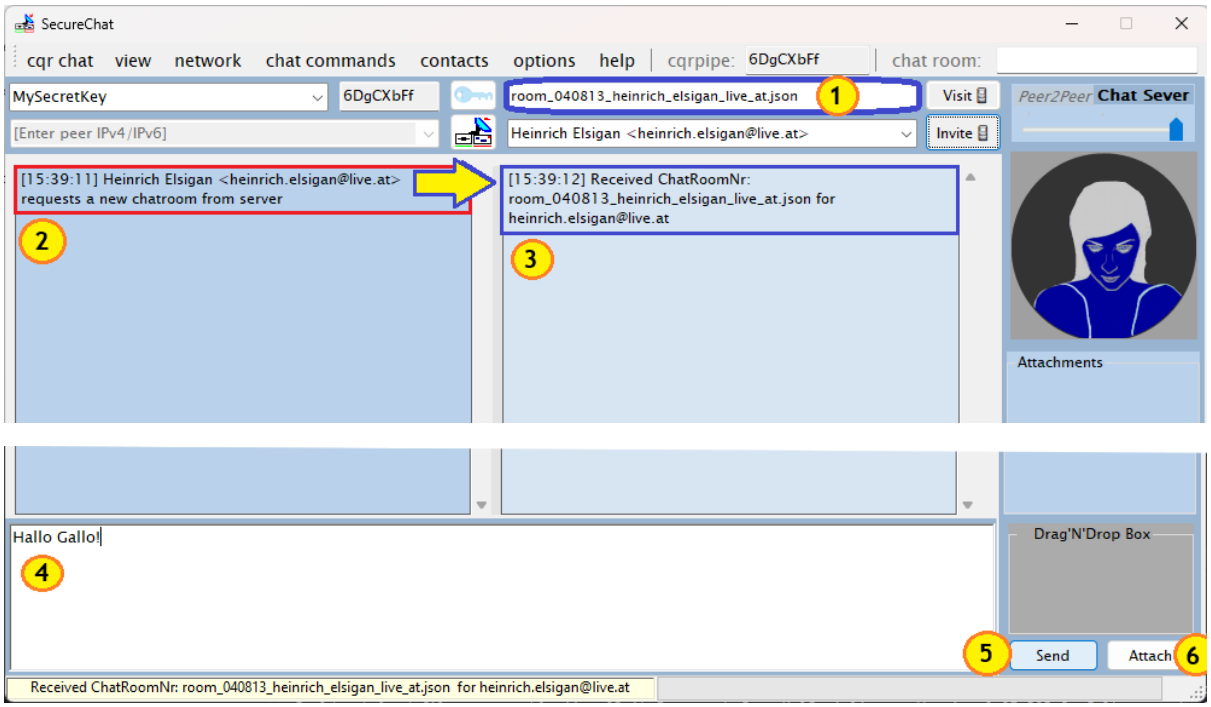
requesting successfully a new session chat room

After pressing the invite button, a new chat room invite request with your and invited person contact data will be send to AWS WS in spain.

When retrieving a successfully response, full chat room name will be set at *room number* Textbox (1).

In source chat textarea (2) the original request will be appended.

In case of success, received chat room number and invited person will be noticed in destination chat textarea (3)



(4) In **Textbox** *chat* you can enter now, some free chat sentences,
(5) Click **Button** *Send* to send your message to the chat room mentioned above,
(6) Click **Button** *Attach* to attach images, documents or any other files. (please not too large).

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

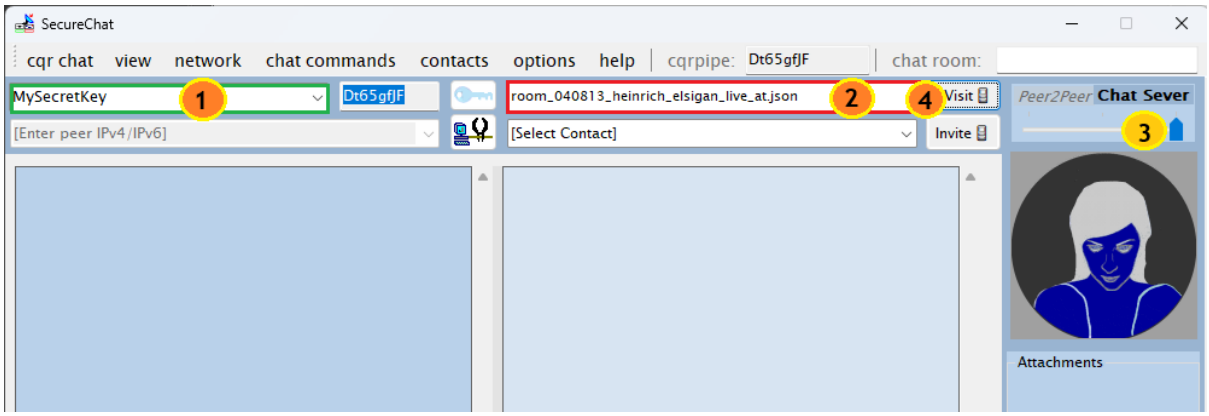
UID ATU72804824

Wien, 9. März 2025

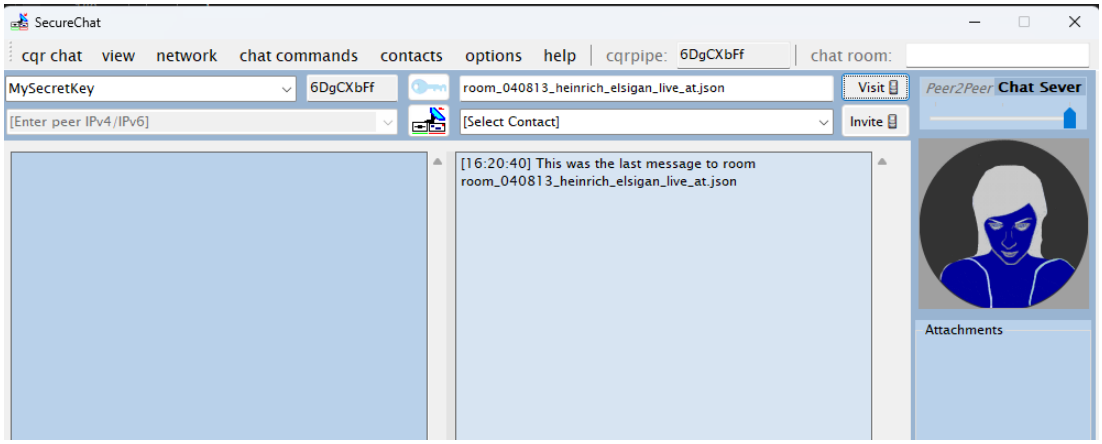
starting visiting a chat room, that someone other has created

When a college, co-employer or friend invited you to a chatroom, you must wait until he/she sends ***shared key*** and ***chat room number*** via Email, SMS, told it to you by phone-call or at launch meeting.

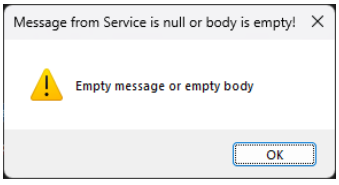
(1) Enter shared key to encrypt / decrypt both symmetrically with same key / hash.
(2) Enter ***chat room number*** you have received from your contact and please write it fully out with extension *.json*, otherwise chatroom will not be found.
(3) Toogle SecureChat mode *to chat server session*.
(4) Click *Visit* **Button** to connect to chat room.



When entered shared key and chat room number matche, then you will get the last message, that was send to that chat room, before you begin visit.



When a new chat room constains no messages or attachment at all, because it's new and was opened / requested some seconds ago, you will get this Windows Dialog Info, when visiting it:



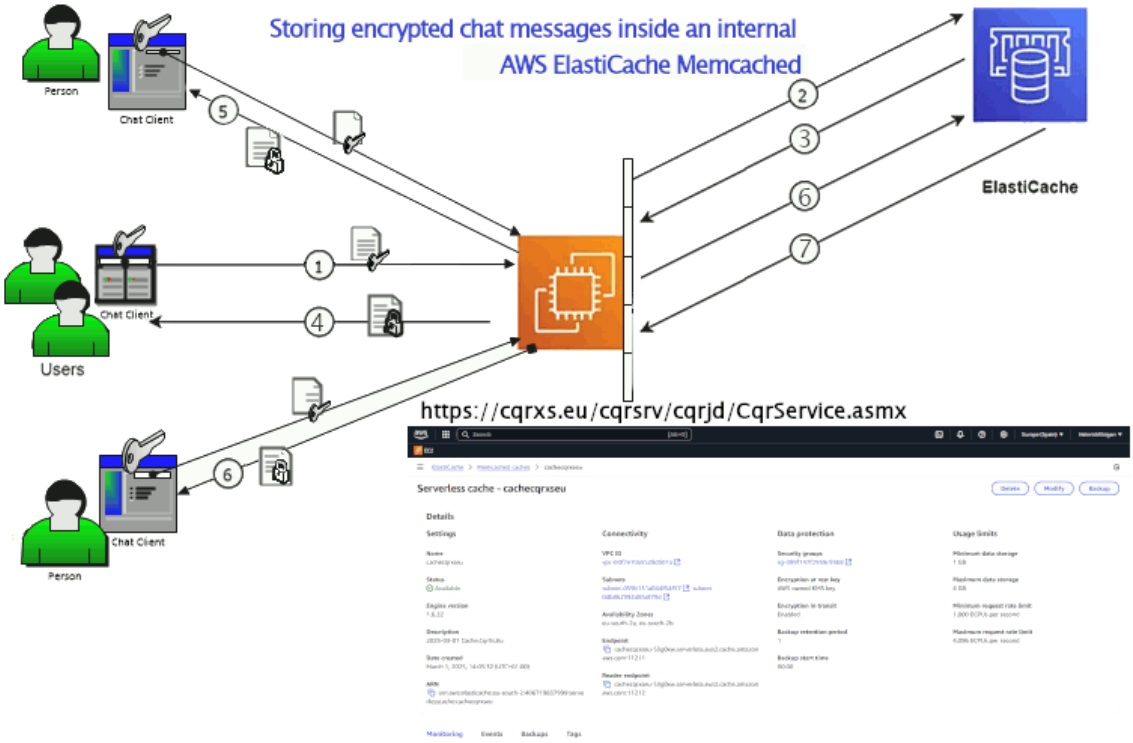
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

chat server mode technical description

Communication is over webservice on https://cqrxs.eu



https://valkey.io/commands/randomkey/

https://cqrxs.eu/cqrsrv/cqrjd/CqrService.asmx

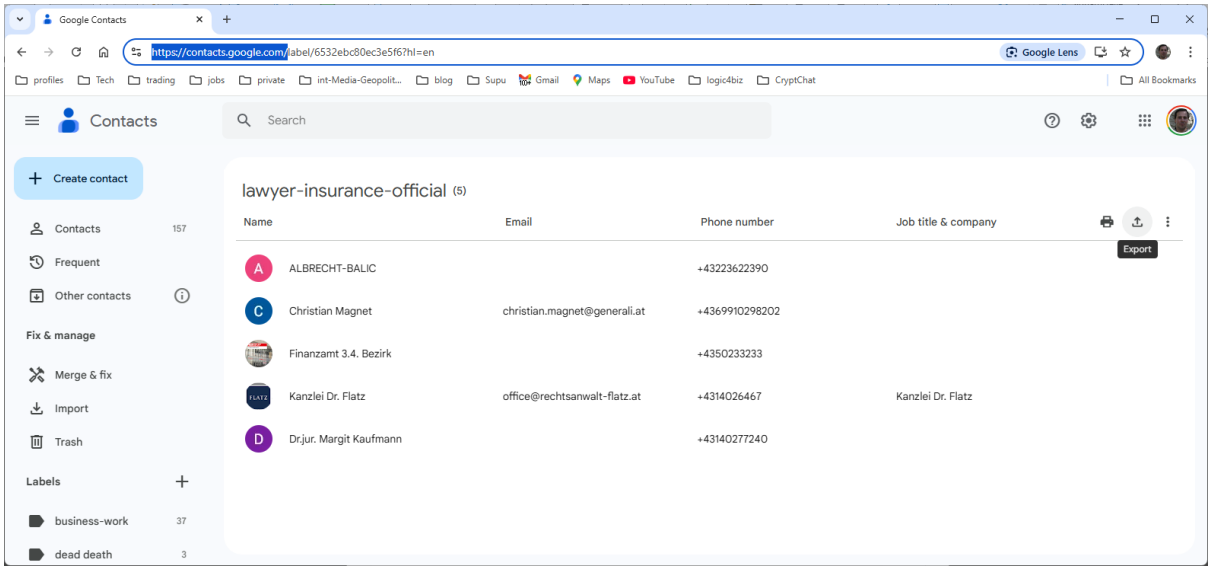
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

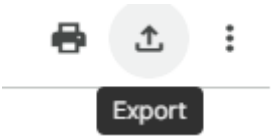
UID ATU72804824

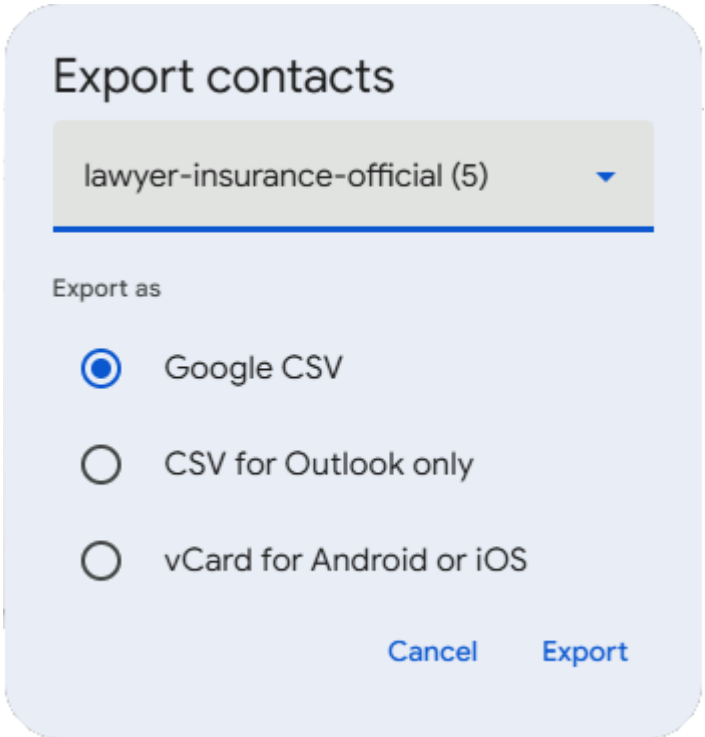
Wien, 9. März 2025

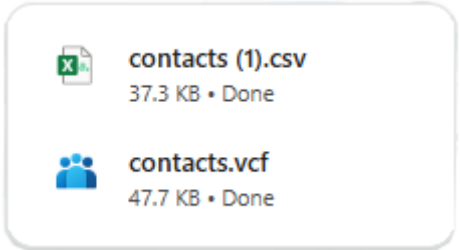
importing contacts from Google

Go to https://contacts.google.com/ and choose contacts label, that you will export or choose all.



Then click on  export contacts.





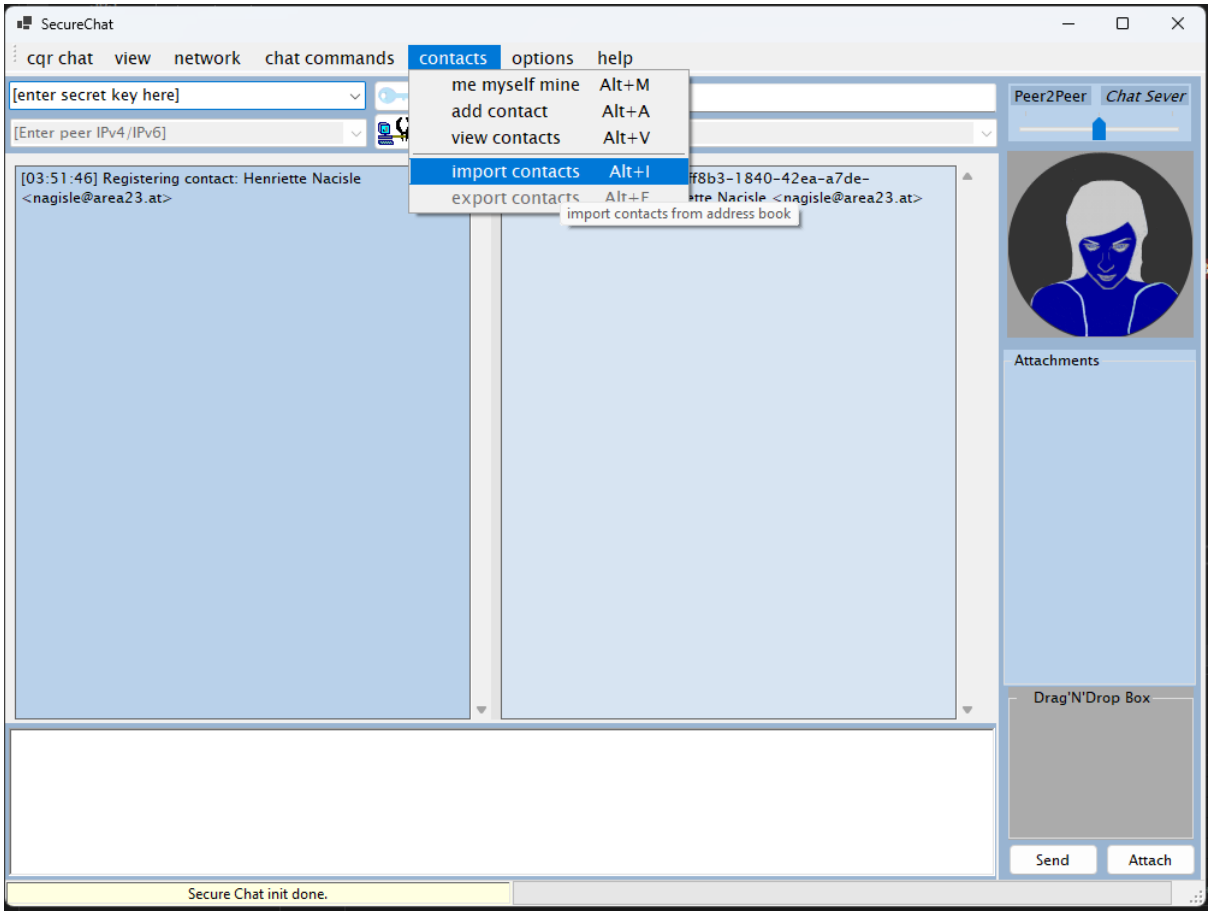
You can choose either **Google CSV** or **CSV for Outlook only** or **vCard for Android or IOS**.

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

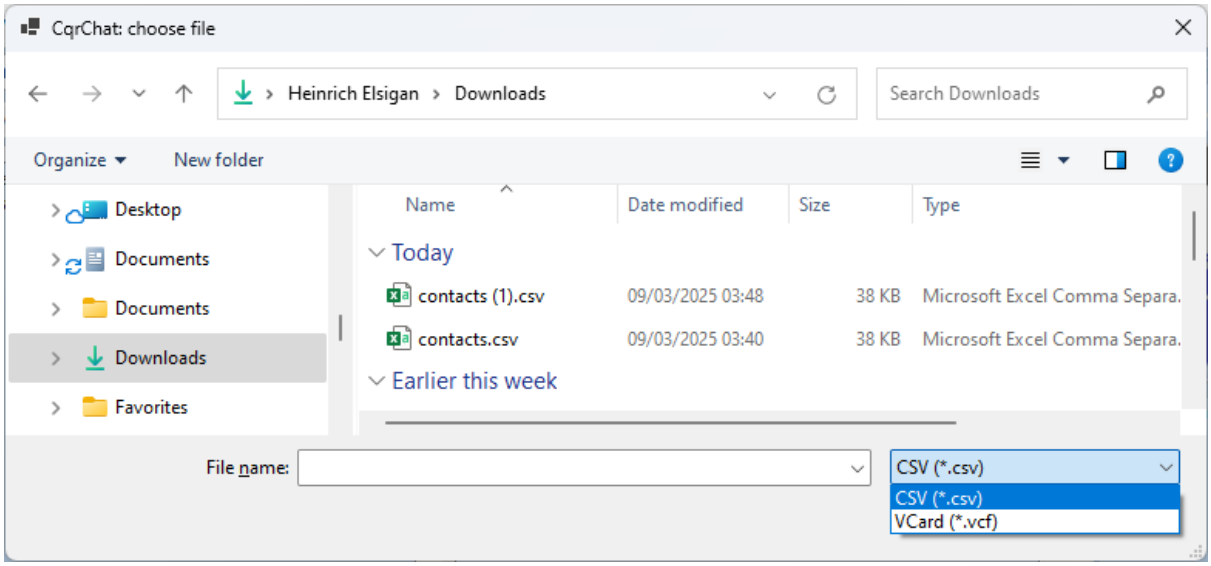
UID ATU72804824

Wien, 9. März 2025

When starting Secure Chat Winx86/x64 Client, choose menu contacts => import contacts or **ALT-i**.



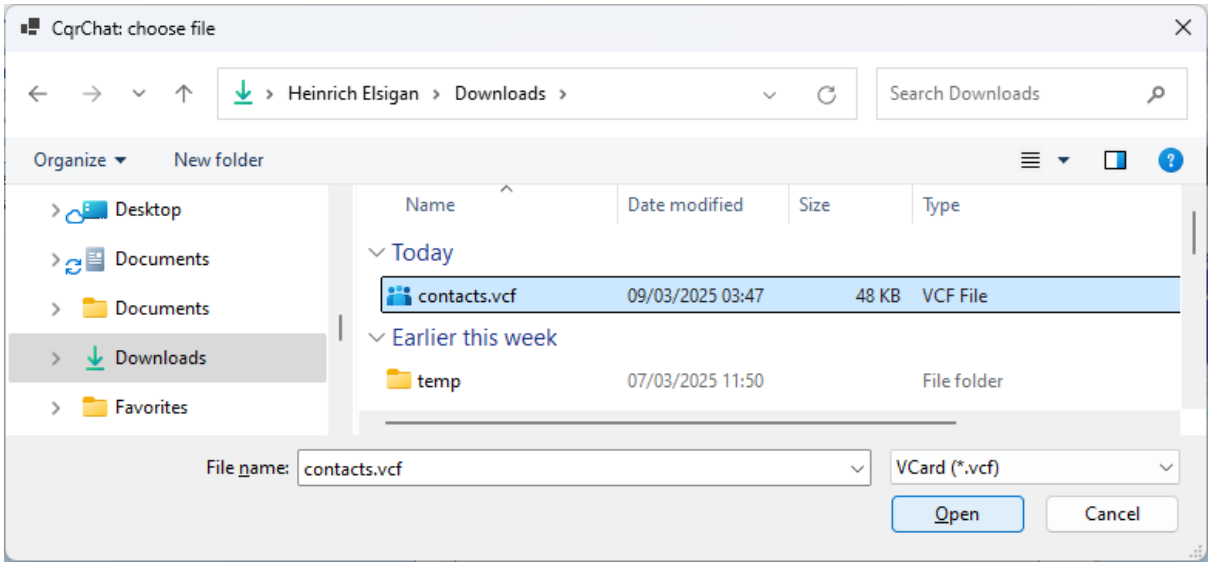
You can select between CSV (*.csv) and VCard (*.vcf) format. CSV (*.csv) is default selected.



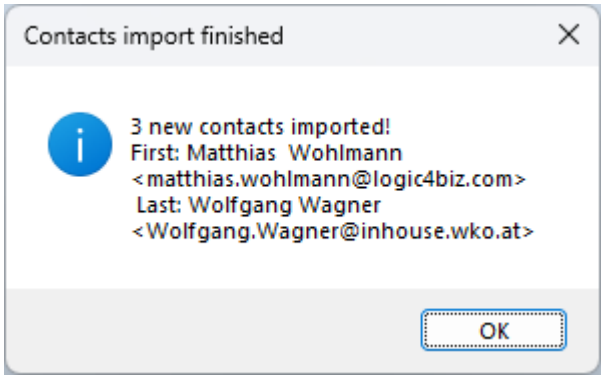
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025



Only contacts, with existing E-Mail Address will be imported.



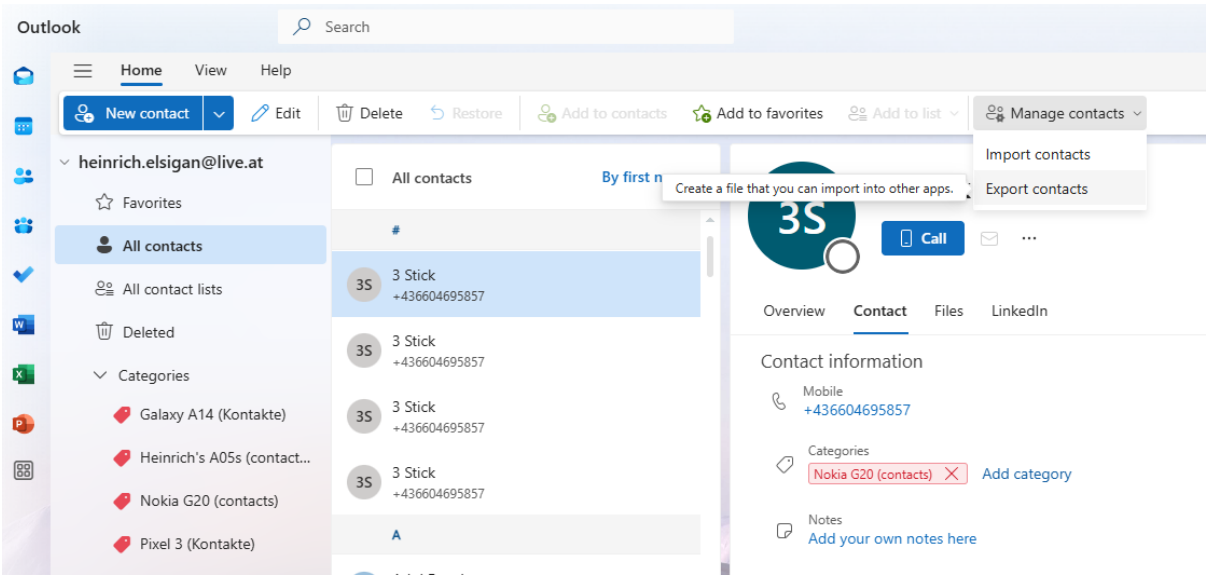
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

importing contacts from MS Outlook

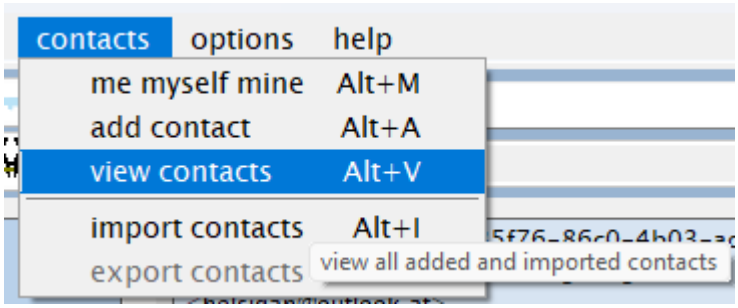
Open MS Outlook and click on then choose Export contacts in Manage contacts



Contacts will be exported to a csv file.
After export import contacts as same as described in section Google before.

viewing imported contacts

Click on menu contacts => view contacts or ALT-v



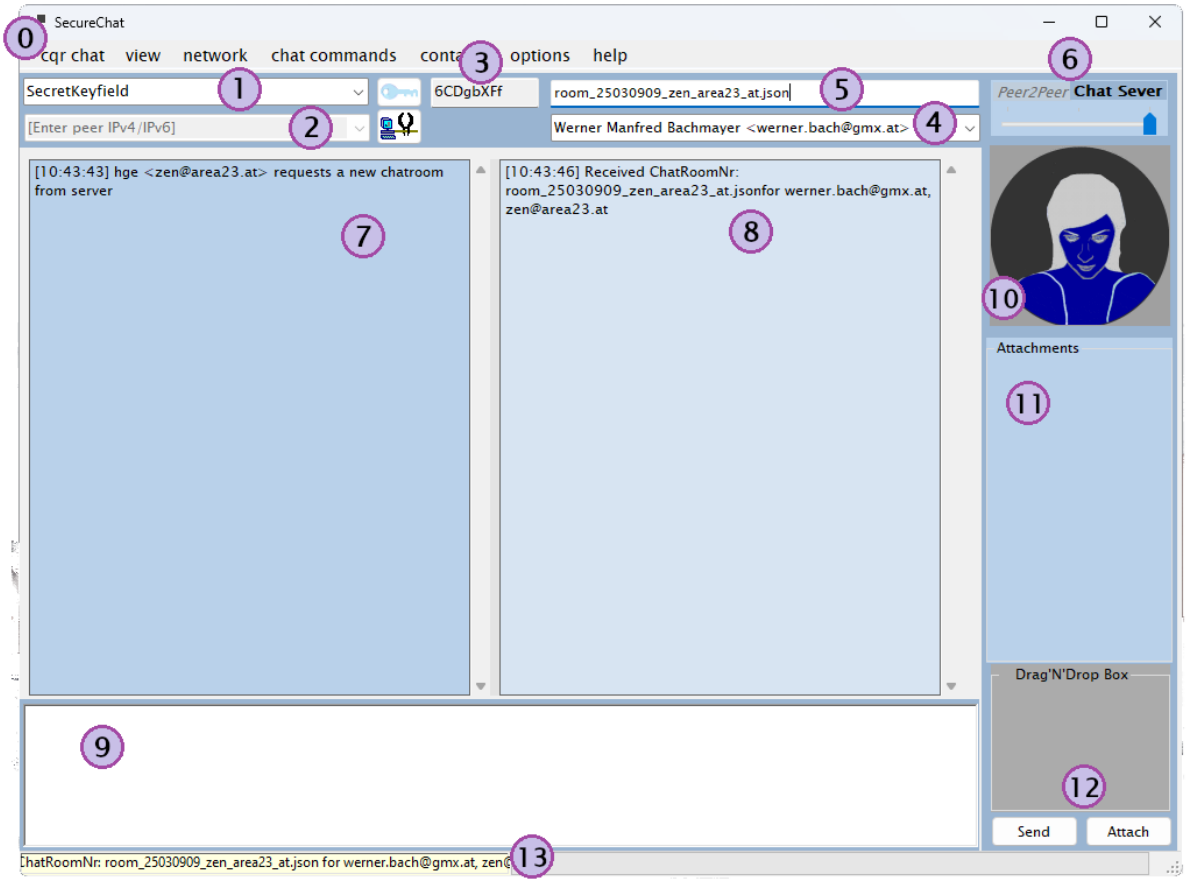
Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

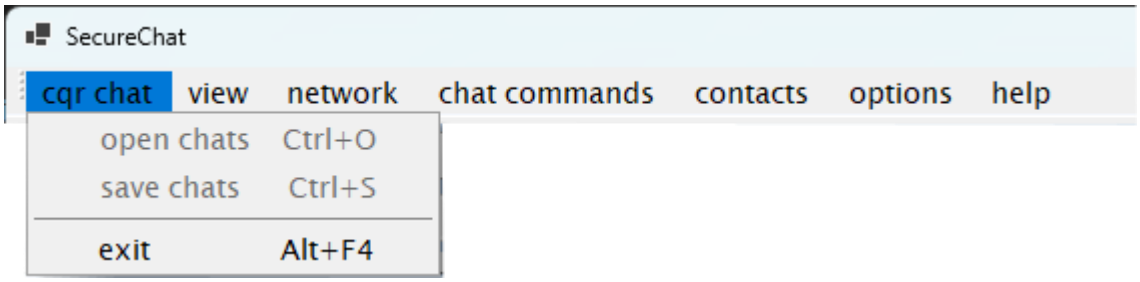
Wien, 9. März 2025

controls in secure chat win-form

Description and usage of different controls on Windows Forms



0. Menu see section Menu later



1. Secure key Texbox 

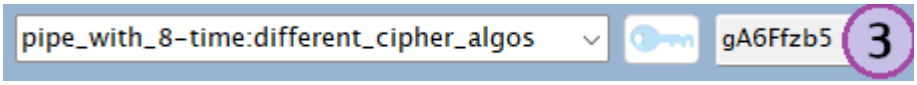
You and your chat partner must enter the ***same*** **secret key** for symmetric 8-fime encryption ppipeline.

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

2. IP-Address of your partner 

that is reachable from your selected network interface. (example above with loopback ipv4)
3. Internal hash for symmetric cipher algorithms


g	Ghost28147
A	AES AES Galois field
6	Cast6
F	3-Fish (Bruce Schneier on ThreeFish)
f	2-Fish (Bruce Schneier on TwoFish)
z	Zenmatrix (my own easy fast symmetric cipher algo)
b	Blowfish (Bruce Schneier)
5	RC532

Name: Heinrich Elsigan
Adresse: Theresianumgasse 6/28, 1040 Vienna, Austria
Telefon: +43 650 7527928
E-Mail: heinrich.elsigan@gmail.com he@area23.at

UID ATU72804824

Wien, 9. März 2025

```
switch (cipher)
{
    case CipherEnum.Aes: return 'A';

    case CipherEnum.BlowFish: return 'b';
    case CipherEnum.Camellia: return 'C';
    case CipherEnum.Cast6: return '6';
    case CipherEnum.Des3: return 'D';
    case CipherEnum.Fish2: return 'f';
    case CipherEnum.Fish3: return 'F';
    case CipherEnum.Gost28147: return 'g';

    case CipherEnum.Idea: return 'I';
    case CipherEnum.RC532: return '5';
    case CipherEnum.Seed: return 's';
    case CipherEnum.Serpent: return 'S';
    case CipherEnum.SkipJack: return 'J';
    case CipherEnum.Tea: return 't';
    case CipherEnum.XTea: return 'X';

    case CipherEnum.ZenMatrix: return 'z';

    case CipherEnum.Cast5: return 'c';
    case CipherEnum.Rijndael: return 'a';
    case CipherEnum.Noekeon: return 'N';
    case CipherEnum.RC2: return '2';
    case CipherEnum.RC564: return 'R';
    case CipherEnum.RC6: return 'r';
    case CipherEnum.Tnepres: return 'T';

    case CipherEnum.ZenMatrix2: return 'Z';

    case CipherEnum.Des: return '$';
    case CipherEnum.Rsa: return '%';
    default: break;
}
```

4. ChatRoomNumber every member of your chat room session has to add.
   When using Server Session Chat mode, every invited person has to add both Secure Key and Chatroom Number.
   Please remark, that cqrxs.eu don't spams and you have to tell via phone call or SMS both secret key and exactly spelled Chatroom number.
5.