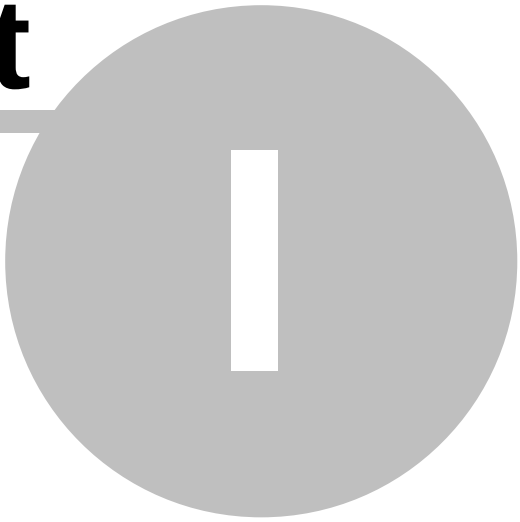
# Cryptia common guide

# Table of Contents

# Part



# 1 The Quick Start: introduction

## 1.1 Preface

The Quick Start comprises the first several sections of this manual which should be read in series (most probably it will not take longer than twenty minutes). After you will have finished reading them, you will be able to grasp basic principles of Cryptia's functionality and make an effective use of the program. Consult further sections of this manual if you seek an in-depth understanding of program's principles or want more control over the encryption process. In case you have any questions concerning a particular Cryptia's function, it is recommended to search this manual for relevant words.

## 1.2 System requirements

To install Cryptia 0.9 for Windows a computer with at least
- Windows XP
- 512 MB of RAM and 1 GB processor
is required.

Mac OS version requires Mac OS X 10.6 Snow Leopard or newer.

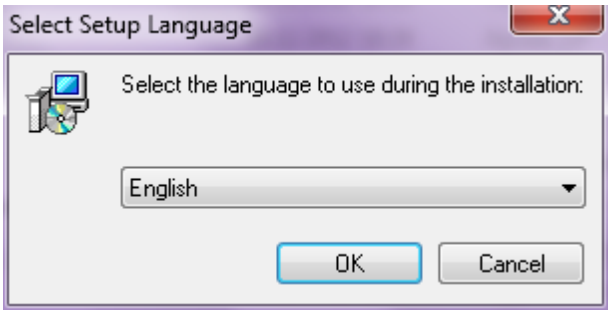
Cryptia client is available for installation on smart phones — visit www.cryptia.com for up-to-date compatibility list.

# Part II

# 2 The Quick Start: installation

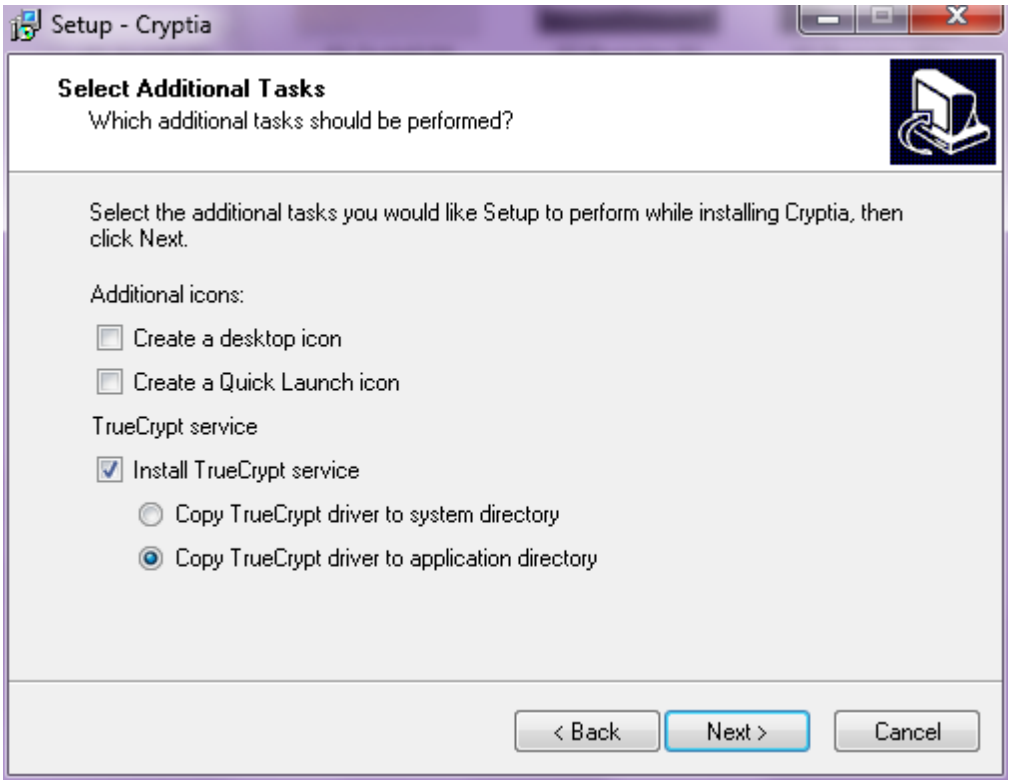
## 2.1 Windows installation

Run the application you downloaded from cryptia.com — its name should be cryptia_setup_win32.exe. Default location for this file is your downloads folder (e.g. *C:\Users\[user's name]\Downloads*\). Alternatively, you may run the file directly from your browser's download list.




In the first window you should choose a language to be used in the installation process. This language will also be used as default when you run Cryptia for the first time. You will be able to change the program's language later.


The installation is fairly typical and you may have encountered a similar process during the installation of any other Windows program. You will be required to: read and accept the terms of license agreement; name a folder to extract program files to (make sure you have write access to this folder); choose a name for Windows Start menu folder and a location for the program's shortcuts. There is only one option that requires further clarification.




Truecrypt is a utility driver that enables support of encrypted file containers (in Cryptia we call them Encrypted storage). Encrypted storage is a virtual drive that stores files received by an account associated with it. The disk is mounted only when the account is connected to the server and its contents are encrypted. It is recommended to proceed with TrueCrypt drivers installation, otherwise the encrypted storage functionality will be disabled. You may choose to install the driver either to OS driver directory or to the program's folder. The former setup is more stable in case you want to reinstall the client, the latter may be useful if you aim for portability.

## 2.2 Mac OS installation

Mount the downloaded installation file named *cryptia_setup_mac.dmg* and launch the mounted image. After the window opens, drag the file *Cryptia.app* on the *Applications* folder alias. Unmount the image. The program is ready to be run.

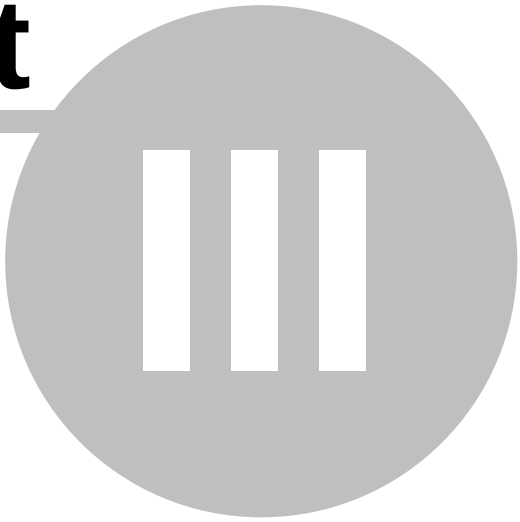

## 2.3 Portable client for Windows

Cryptia uses an encrypted file called **adressbook.cdb** to store your address book and message history; the file **cryptia.ini** contains program preferences (see this topic for information concerning this file). Both files are located in your personal folder, default location of which is *C:\Users\[User name]\AppData\Roaming\Cryptia*. You may choose to move these files to the program's folder — in this case Cryptia will become portable, which means that the client may be stored on a removable media (e.g. flash stick or external hard drive) in a ready-to-use state. You would be able to work with the same copy of Cryptia client using it on as many computers as you like and none of them would have any traces of the program's usage on it. Also, running on different computers, Cryptia will maintain the contact list and message history (which would be separate on each computer otherwise).

However, we recommend setting a complex daily password to encrypt the address book and message history stored on the media.

Only one instance of Cryptia may be running on a device at a time, thus you would not be able to run portable client and a regular one together. Please note, that Cryptia allows multiple accounts to be opened simultaneously by a single client.

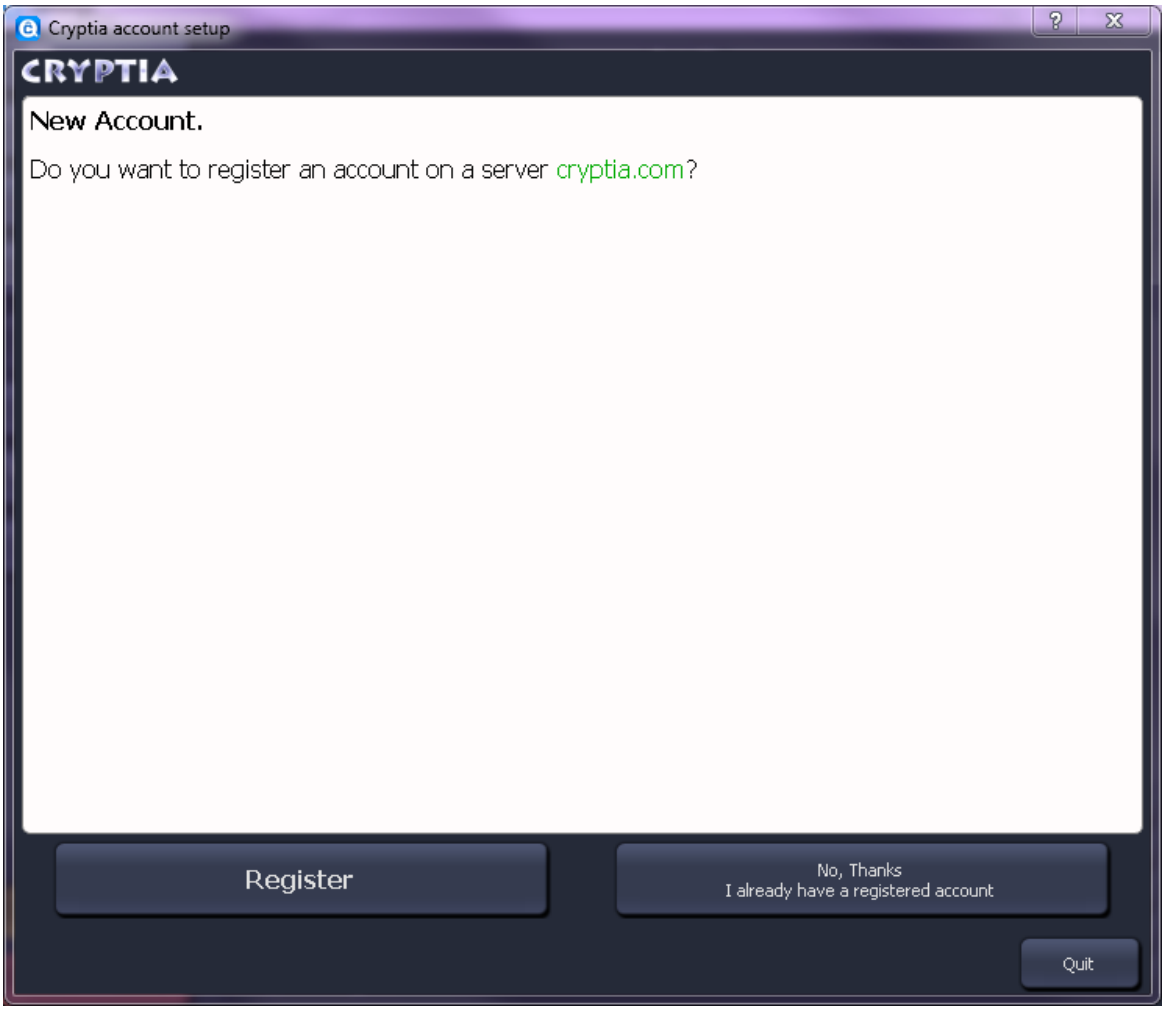
# Part



# 3 The Quick Start: registering a new account

## 3.1 The first launch. Registering a new account

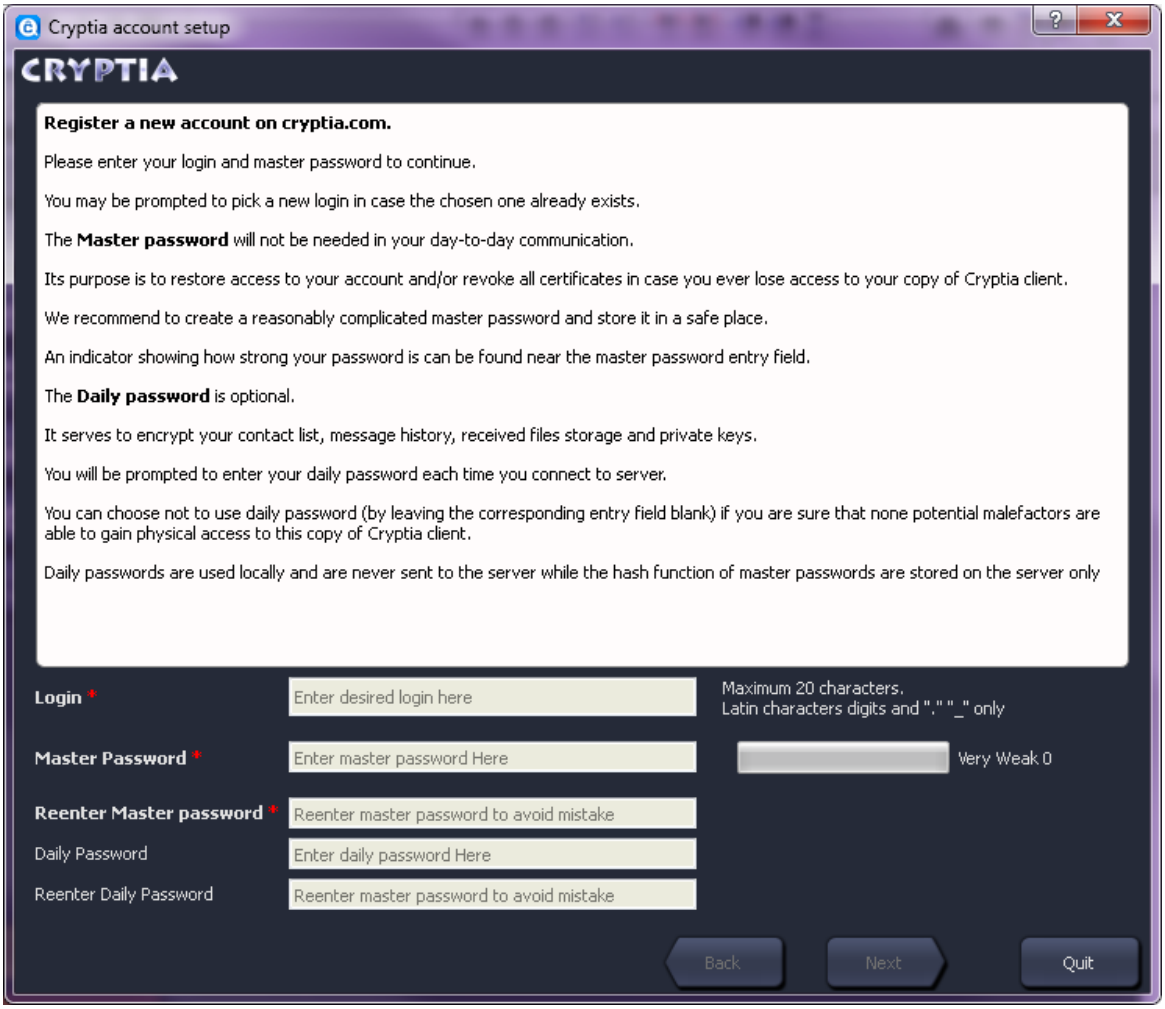
Run the program as soon as installation is completed. If there are no accounts set up on this computer you will see the welcome screen.




As the Quick Start section of the manual is intended for perusal by lead-off Cryptia users, the registration process will be described next. Click the *Register* button to continue. This window can be accessed in the future by using the Add account option in the *Settings*.

## 3.2 Master password and daily password

Study the information provided in the following window thoroughly — there you would find the basic principles of account security covered. The functions of **Master-password** and **daily passwords** are also explained in this memo.




Please note, that you should never forget your Master password, otherwise you will lose control of your account - either retrieving the lost Master password or creating a new one is impossible. These strict measures are necessary to ensure adequate security of your account.

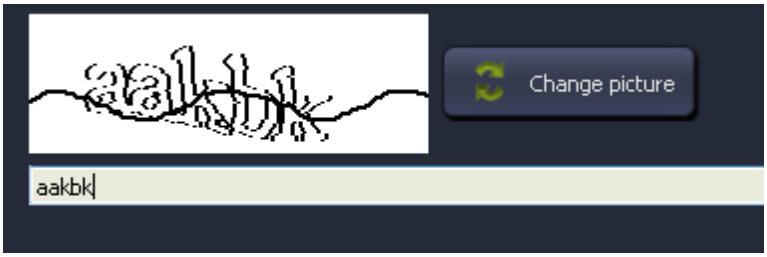
You can leave the daily password entry filed blank — however, this decision may leave you defenseless in case a malefactor gains physical access to your copy of Cryptia client. Therefore we recommend you to specify a daily password, particularly if you are using a portable client.

The information associated with the account - including message history and contact list - will be stored locally on the device that runs Cryptia. If you are using multiple Cryptia clients on different devices, every copy of the client would have its own daily password. However, daily passwords used on different copies may be identical. Alternatively, if you wish, you may choose not create a daily password on your home computer and use it at work.

Whenever you might forget your daily password or a malefactor might gain an access to your account, you would be able to revoke all your key pairs using your master password, rendering all your daily passwords ineffective. You would be prompted to specify a new daily password when creating a key pair. See this link for more information regarding key pairs..

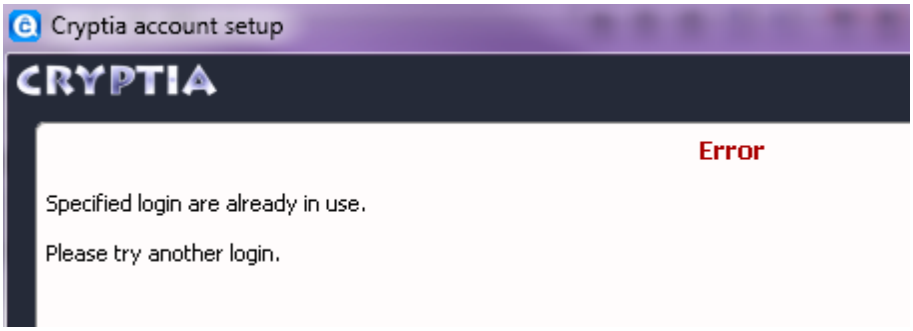

Enter the desired login, then enter both master password and daily password twice. There is a security meter located to the right of the master password entry field — it shows whether the specified master password is secure. Passwords employing lower case letters, capital letters, digits and punctuation marks together are considered stronger.

Click *Next*> when finished.




Every time you create a new account you would need to complete CAPTCHA by typing the text you see on a picture. CAPTCHA is required to protect the server from spam attacks. If you are having trouble reading the distorted picture, try changing it by clicking the corresponding button. Click Next> as soon as you complete the test.

After CAPTCHA is resolved successfully, the login is being checked. In case the login you have chosen already exists, you would be prompted to specify a new one.

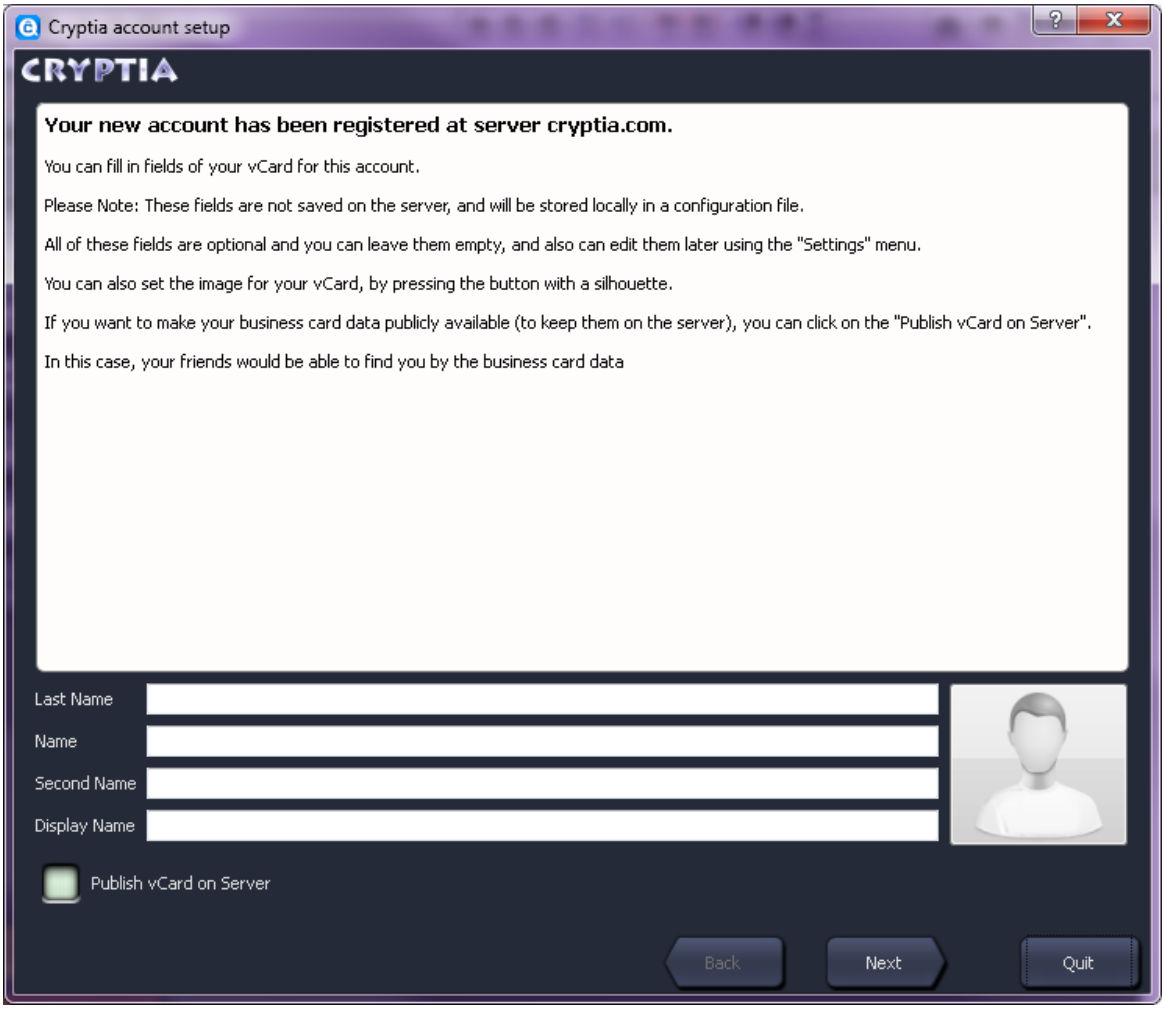



The login you specified is registered on the server immediately after being verified to be unique.

## 3.3 The Calling card

A **Calling card** contains the information about you which you would like to share with other users. It includes your name, your photo (or any other image that suits you) and an alias which is displayed in other users' contact lists next to your photo. Neither of these is mandatory.

There are several ways to transfer your calling card data to other users. In case you choose to publish your vCard on the server, the data will be visible to anyone who performs a search query on your login. Alternatively, you may either grant a permission to transfer your calling card upon establishing a new contact or export the card in a *.vCard file to be sent to the recipient via email or any other means of communication. Please note that your calling card can be similarly exported to a file by users that have it in their contact list.




To add a photo or any other image to the calling card, simply click a silhouette to the right. You may skip this step for now completely by pressing *Next>*. The program's *Settings* window will provide you with an ability to create, edit or publish your vCard at any time.

## 3.4 Encrypted storage

To finish creating your account you will need to set up an Encrypted storage. Encrypted storage is a container that stores the files transferred to you and encrypts them using your Daily password. The files will not be encrypted if you haven't created a Daily password for this account.

The container mounts as a virtual disk when the account is connected to the server and unmounts on disconnect. CryptiaGuardian is a background process (you can find it in the Task manager) that ensures a timely unmounting of the drive even in case of emergency crash of the Cryptia client. Any files may be copied and moved to and from this drive as long as it remains mounted; the files transferred to you are saved here. You also have the option to mount the countainer without having the account connect to the server.


Here you should specify the location and size of the container file. Please note, that a large container file may require a lot of time to be created — 50 megabytes set by default should be sufficient for most cases. You can create another container - larger, if need be - and associate it with the account at any time.

If you already have a container file (previuosly created using Cryptia or TrueCrypt program), you may

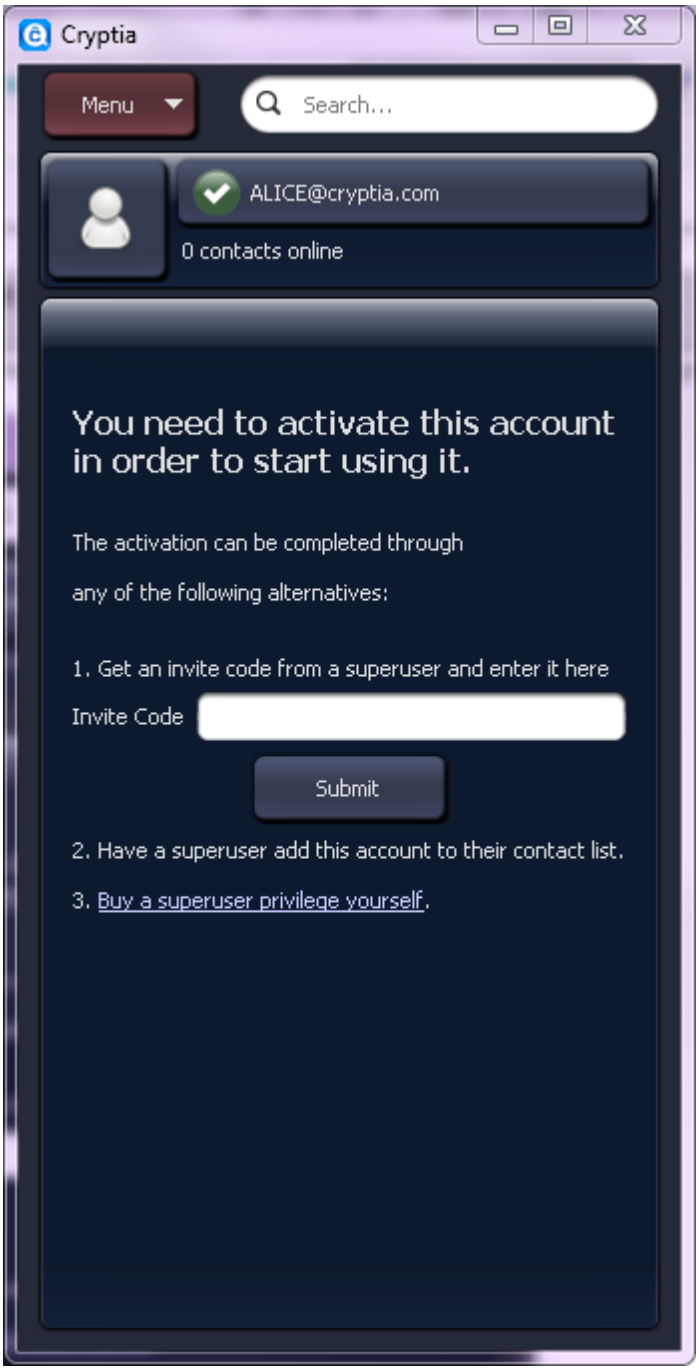
choose not to create a container file and associate it with your account later, using the *Settings*. However, single container file may be associated to only one Cryptia account at a time. In case an account does not have a container associated with it, the files are saved to a folder specified in the Interface tab of the *Settings* window.

# Part IV

# 4 The Quick Start: overview of the program

## 4.1 Account activation

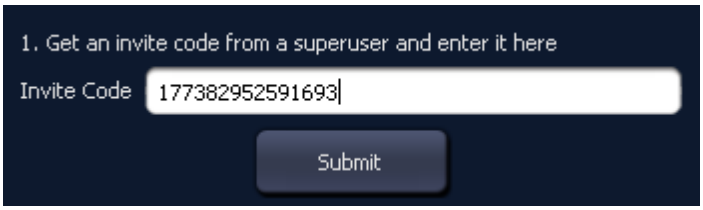
Being at beta-testing stage, Cryptia requires every account to be activated after registration. Before you activate your account, the main window will look like this:




The activation process is tied to super-users, which are people actively participating in beta-testing. You may contact a super-user that acquainted you with Cryptia to have him include your account to

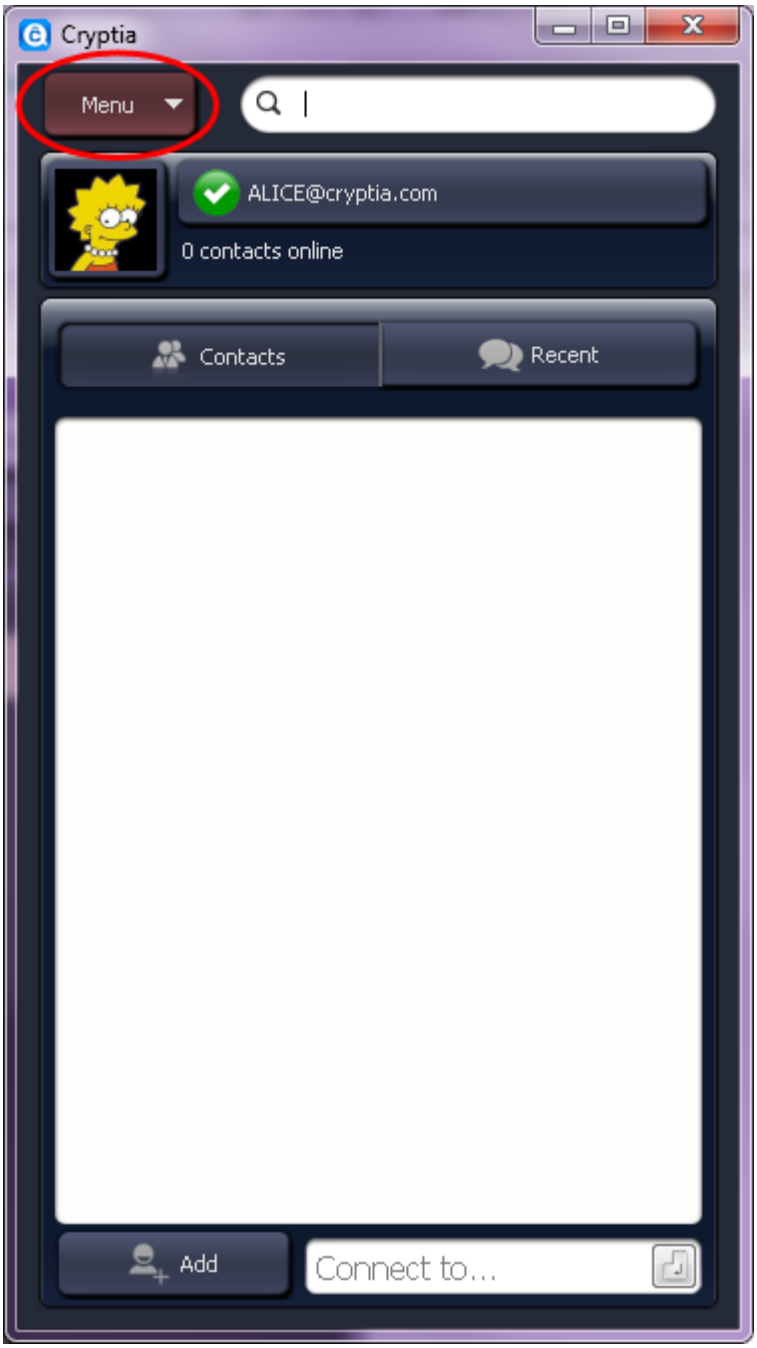
his or her contacts. You will then have your account activated automatically and obtain the first entry to your contact list.


The alternative solution is the invite code, which the super-user will generate and send to you. To activate the account, you should submit the code to the server.

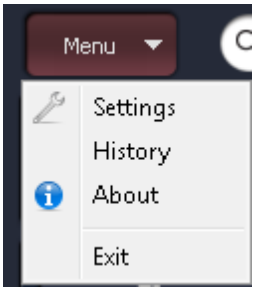



You can also discover more about super-user privilege and purchase it for yourself, if you want to, after following the link in the window, pictured above. If you are unable to activate your account, contact us for troubleshooting via any means provided by cryptia.com website.

## 4.2 The Main window

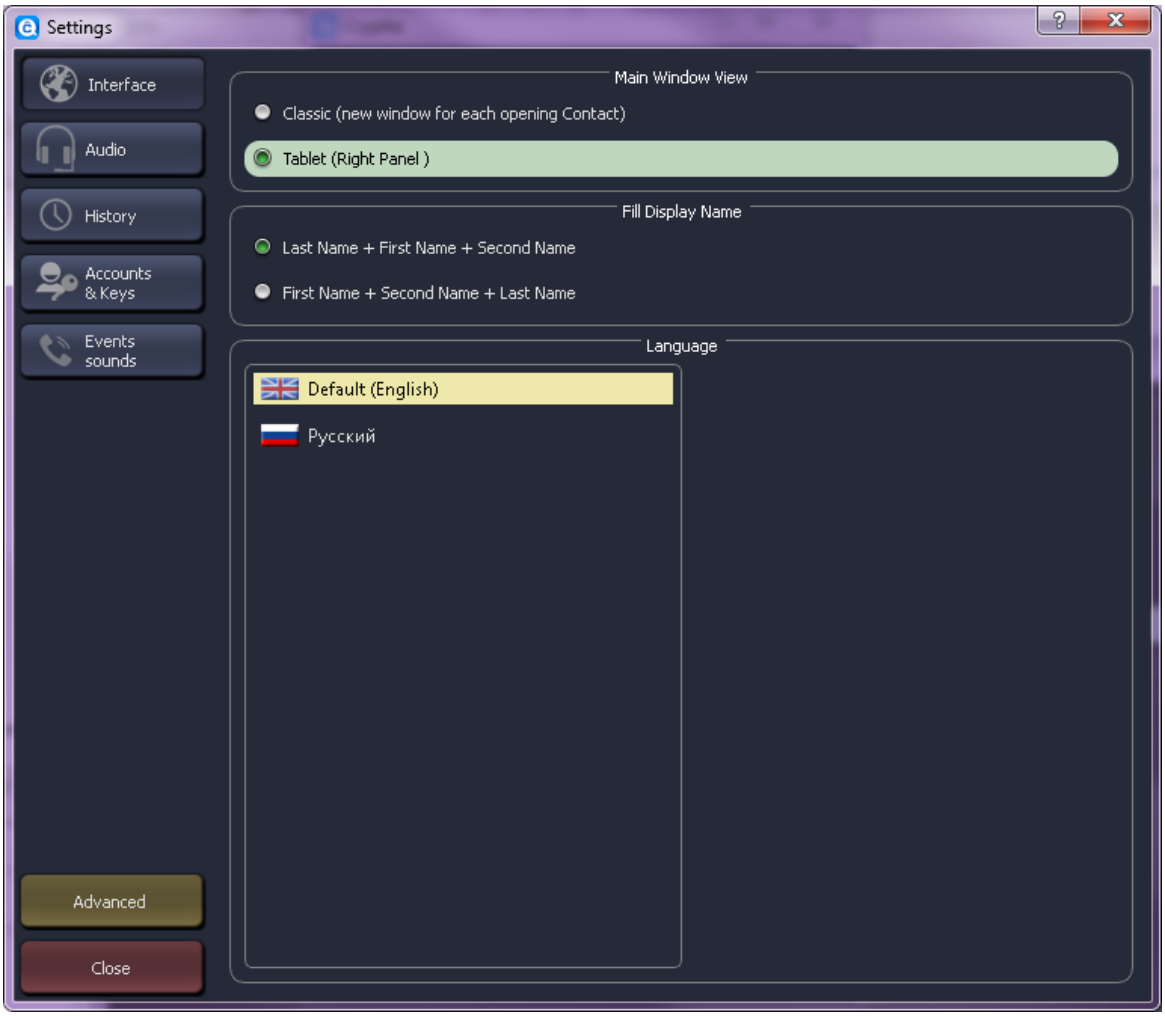



As soon as your account is created, you will see the main window of the program. You will find its detailed description in a further section of this manual. Right now you should open the *Menu* drop-down list in the upper left corner of the window and choose *Settings* there.




## 4.3 Languages

Program's language may be the thing that requires foremost attention. The default setting is the language the program's installer had been using – if you want to change it, see that the top bookmark on the left, *Interface,* is selected.



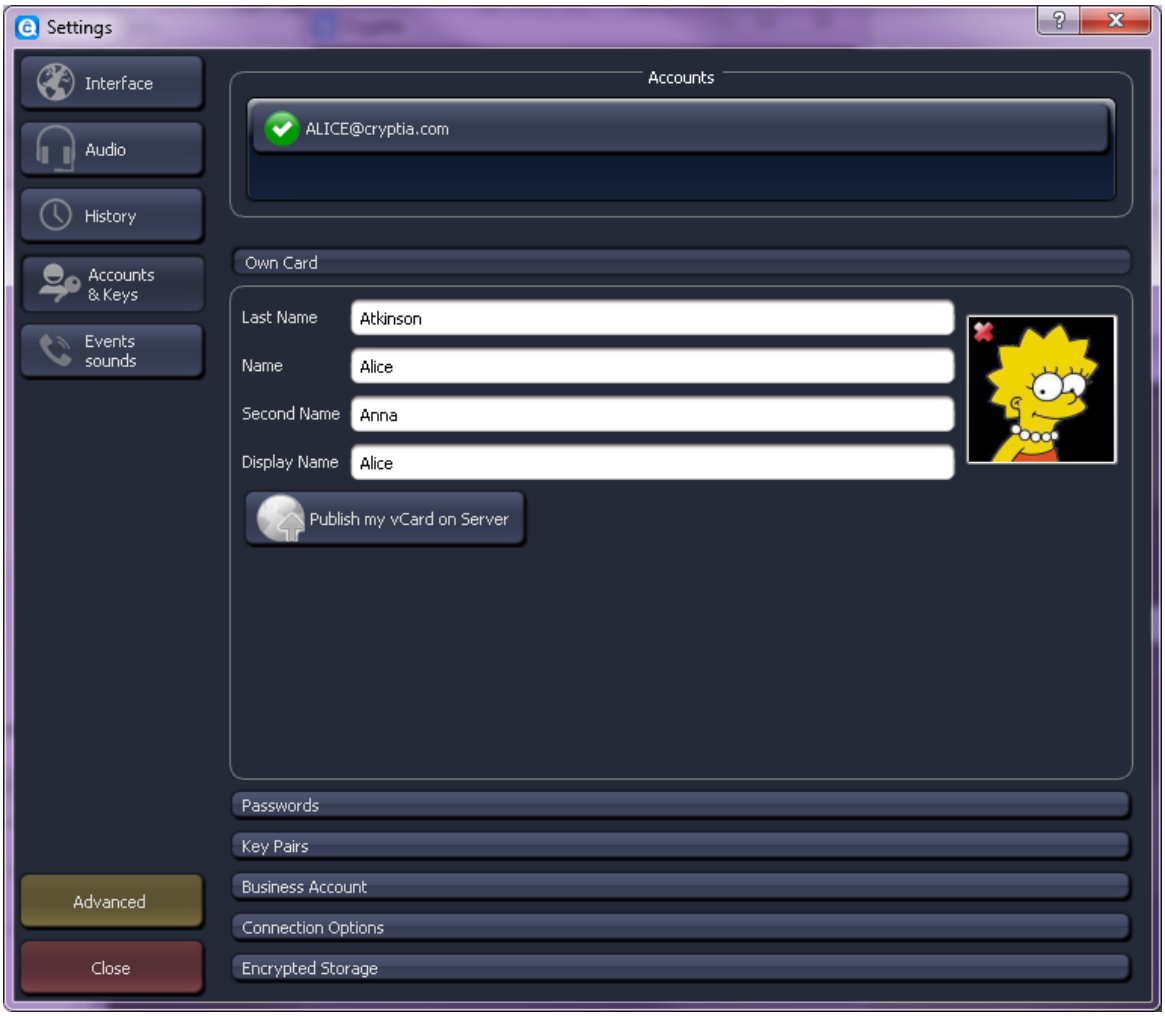

There is a list of languages in the center of the window pictured. You should seek out the familiar flag in case you are unable to understand the language the program is currently using.

Other options offered by this window are the layout of the main window and the storage folder for

received files (make sure you have the necessary write access — see link for details). More information about the Interface tab is provided here.

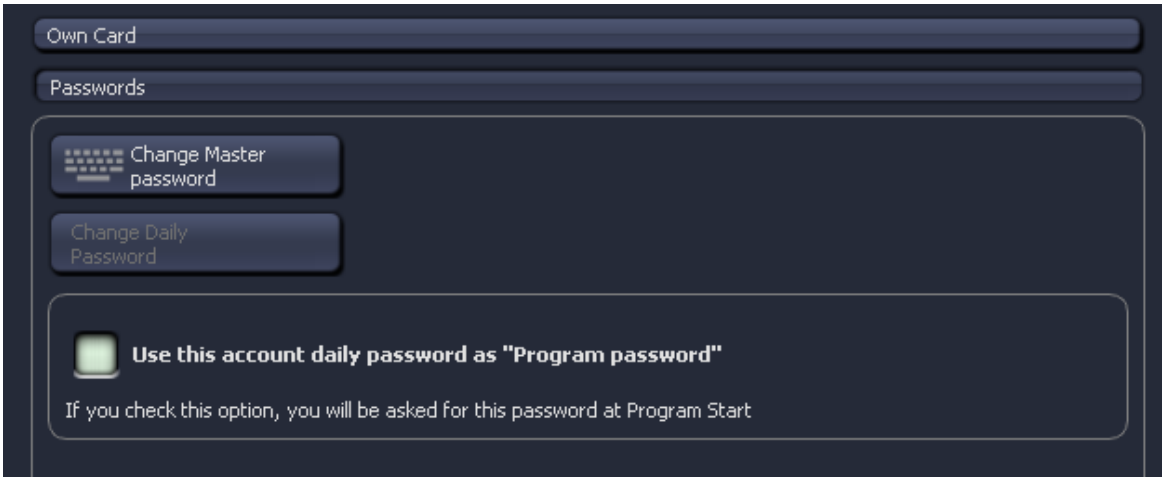
## 4.4 Calling card and password editing

Take a look on the tabs located leftwards of the *Settings* window and click on the *Accounts & Keys* tab. The resulting layout is pictured below.




It's very easy to modify your calling card. As you write in the entry fields and add an image (by clicking the silhouette to the right) changes are saved automatically. The function of *publishing a vCard on the server* is already mentioned – it makes your calling card details visible to the users that searched for your account name. To unpublish a published calling card simply clear all entry fields and click on *Publish vCard on the server* button again. There are other ways to transfer a calling card to another user – see this topic for more information concerning the possibilities.

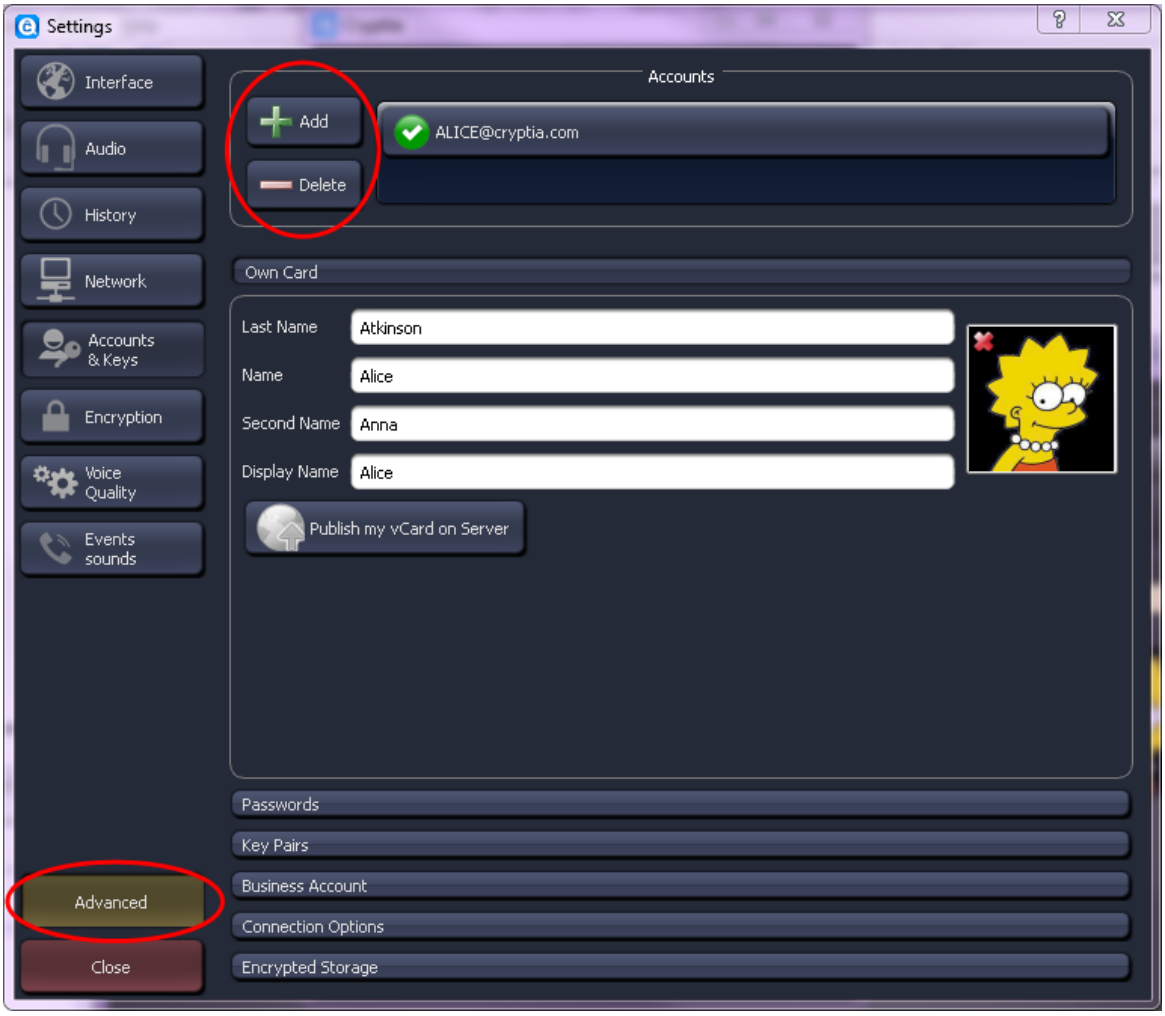
Notice the five bars to the bottom of your calling card details. These are the buttons that lead to the **additional panels** of the Accounts & Keys tab. These panels will be described thoroughly in the following chapters of the manual. At the moment click on *Passwords* to reveal the passwords panel.




You can change any of your passwords using the buttons located here. Naturally, you would need to specify the corresponding old password before doing so. The checkbox below defines whether you would be prompted for a password as you start Cryptia.

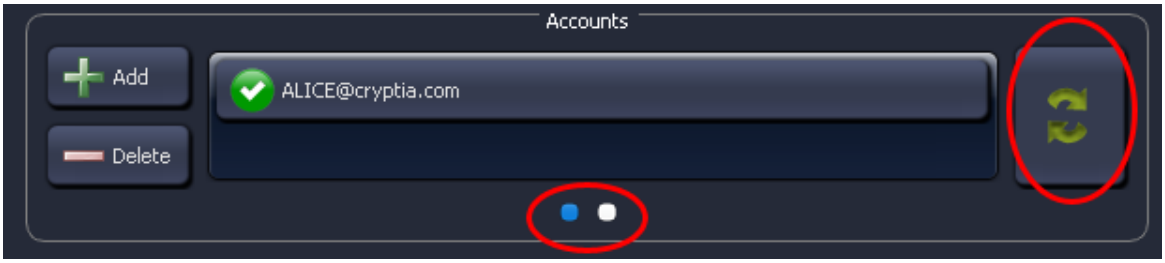
## 4.5 Adding accounts

Make sure you have *Accounts & Keys* tab of the *Settings* window opened. Take a look to the lower left corner of the window – the *Advanced* button will open some new options for you. Click on it.




As you can see on the picture, two new buttons have appeared to the left of the status bar in the *Accounts & Keys* tab. Using these buttons you are able to **Add** and **Remove accounts** to and from this particular copy of Cryptia.

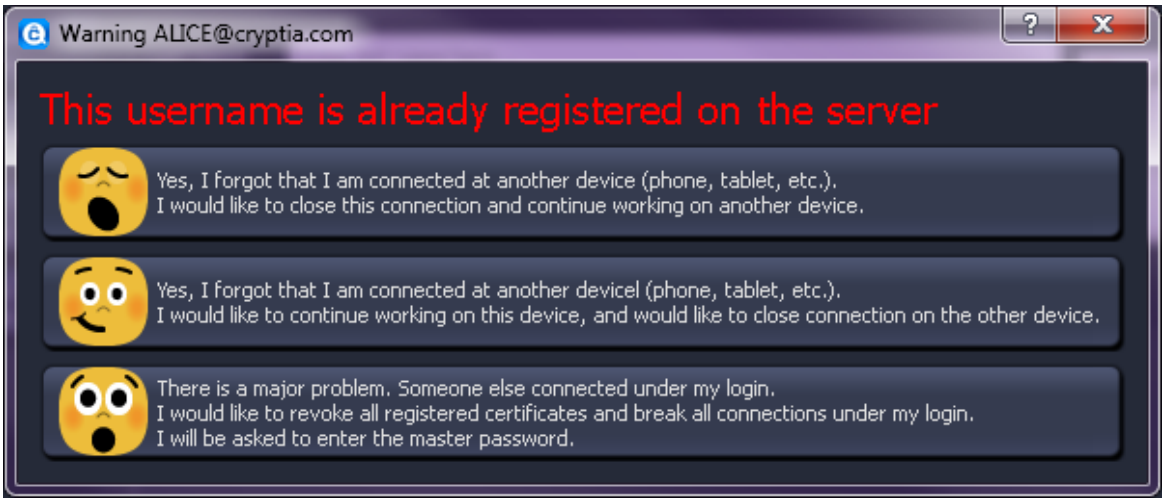
After you click on *+Add* button, already familiar Cryptia Account Setup window will open in which you can either register a new Cryptia account or add an already existing one to this computer. Thus multiple accounts can be used on a single computer as well as one account can be accommodated on several computers.




As soon as there's more than one account associated with this client, several new options appear. The button to the right of the status bar switches the active account by scrolling all accounts added to this computer. The white dots below the status bar represent accounts consecutively added to the computer. Clicking a dot will make a corresponding account active. Cryptia main window contains similar dots. Note, that the settings you specify in this window apply only to the account which is currently active.

To remove an account from this computer, click on the *-Remove* button. Removing the account also deletes message history and contact list associated with it. The action is irreversible as such information is never stored anywhere but on your computer. You would not be able to restore the information deleted this way even if you add the account again.

**Nota bene.** Whereas a Cryptia client can have several accounts logged in and connected to server at a time, an account can be logged in on a single client exclusively. Whenever you try to log in the account that is already being connected to the server, you will be presented with the following options:

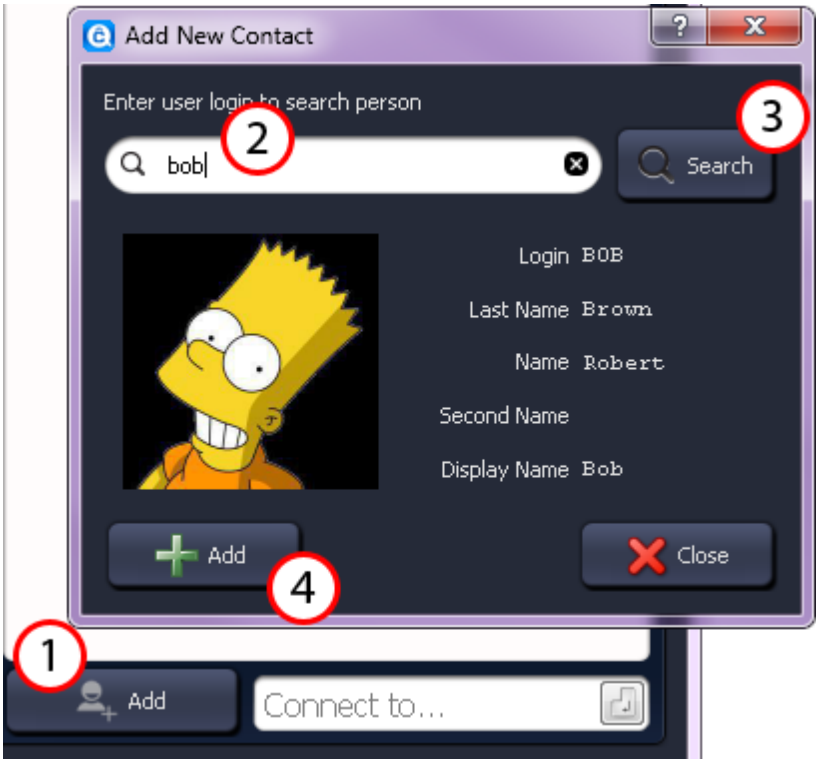


# Part V

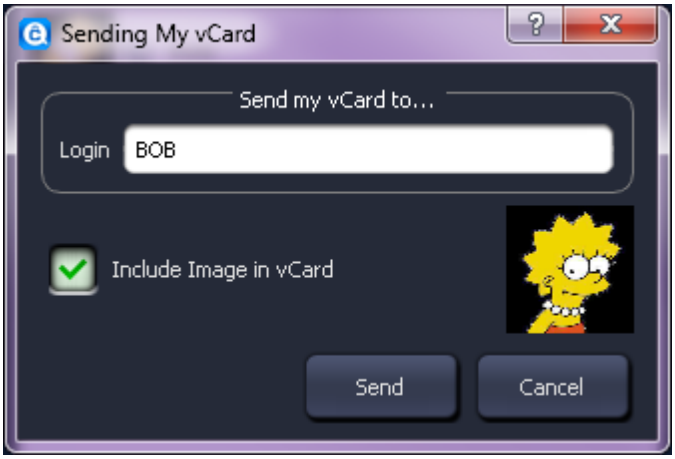
# 5 The Quick Start: conversation

## 5.1 Adding a contact

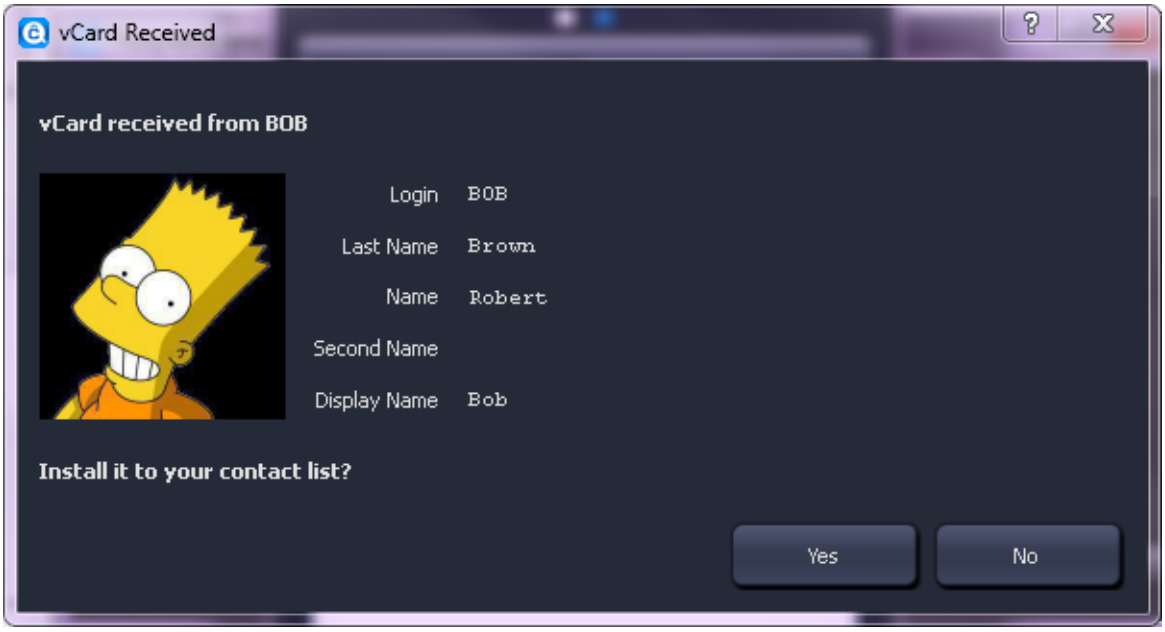
Cryptia establishes a direct connection with another user each time you converse with him or her. To open such a connection you will need to have this user's calling card while the user should have yours. Thus adding a new contact in Cryptia is essentially a calling card exchange.




Let's go back to the program's main window. Click the Add contact (1) button in the lower left corner of the window. A new window opens in which you should enter the target account name (2) and click on Search (3). If the user has chosen to publish his calling card on a server you will see its details here. Click on +Add to add this information to your contact list.




Afterwards, you are prompted to confirm sending your calling card to the user. If the user is online, he or she will receive your calling card immediately and will have to confirm that he would like to talk to you. I the user is not online at the moment, the calling card will be received as soon as he or she logs in.

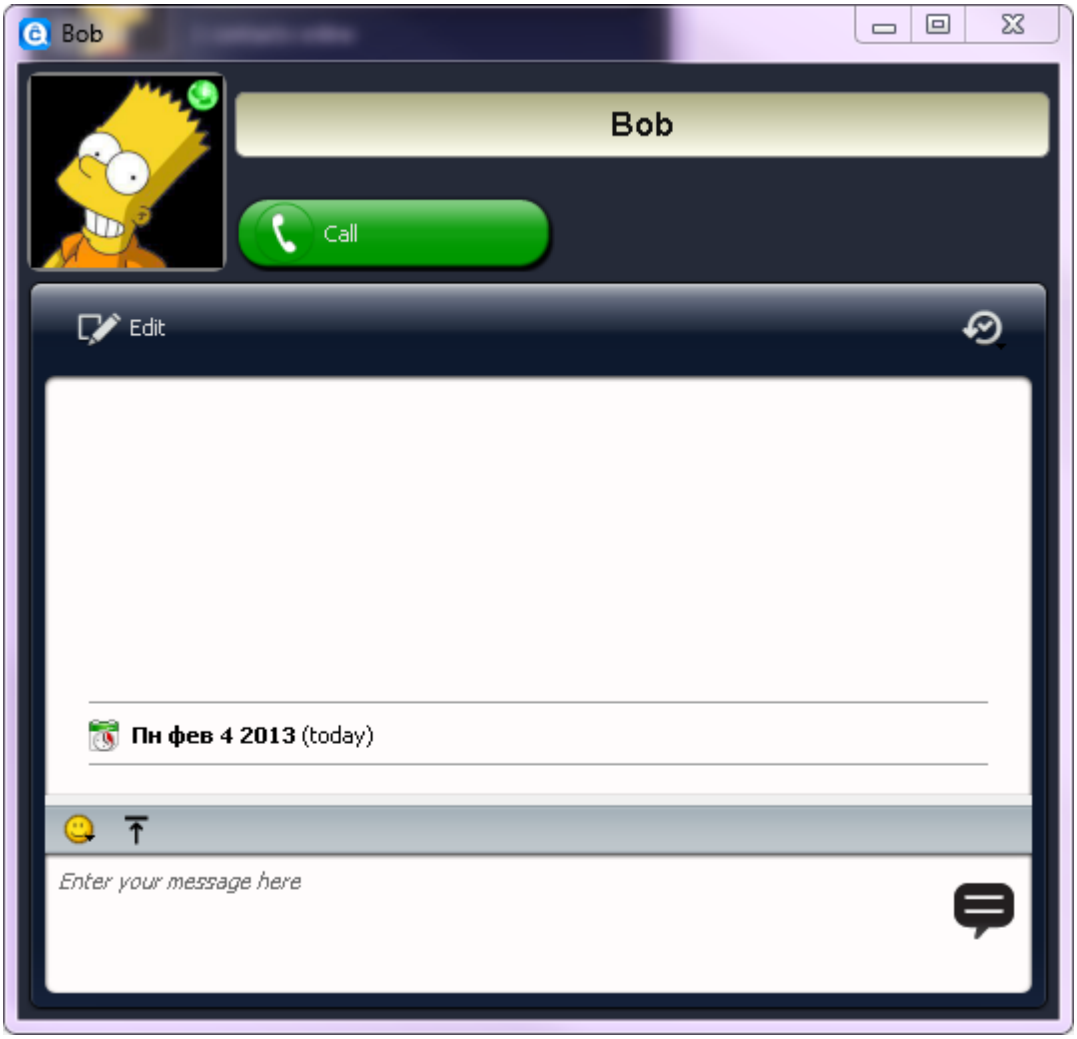



Once both parties have confirmed their intentions, you will be able to see the online indicator next to the user's name in your contact list. The indicator looks like a circle, and if it's green, you are able to start a conversation:


**Nota bene.** If you don't want to send your calling card information through the network, you can export it to a file and manage the transfer via any means you like..

## 5.2 The conversation

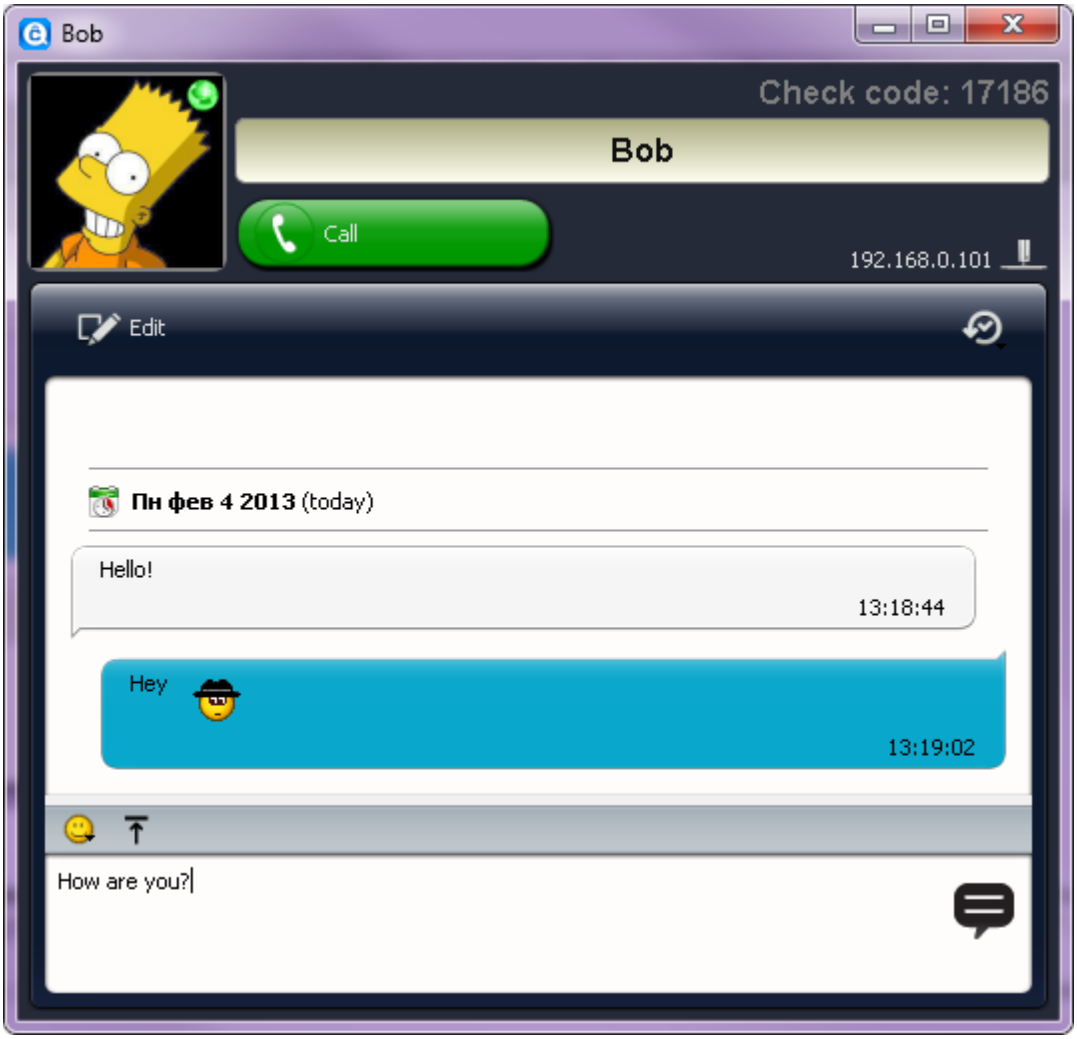
Double-click on a name in your contact list. The connection window will open.




An green circle in the upper right corner of the user's portrait indicates the user is online and you are able to establish a connection with him or her. Cryptia requires both parties to be online at the same time because the connection is established directly and no relay servers are used.

As soon as you write a text message, send a file or click a *Voice call* button, the connection procedure will start. Business-account users have an unlimited number of connections per day, while nonpaying users are restricted to connections with up to five other nonpaying users per day (it need not be the same five users every day and no restrictions apply for conversations with business-account users).

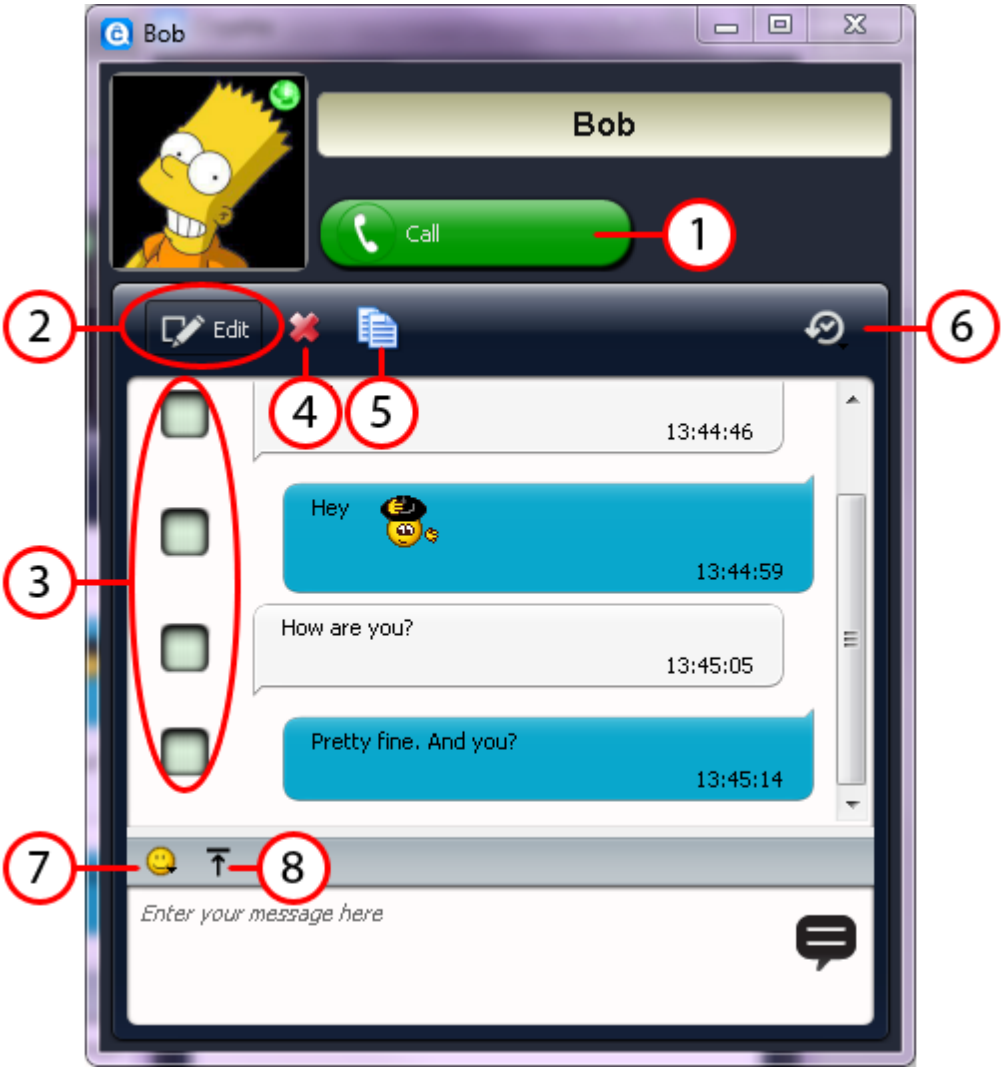
Use an entry field in the lower part of the window to write down and send a message and note the additional information that will appear after the connection will have been established:




The most important part is the **check code**, as it indicates whether the connection is confidential and secure against eavesdropping. Compare the code you have with the one the person you are talking to has – they should match unless your connection is being subject to "man-in-the-middle" attack.

As soon as you close the window, the connection is terminated. To continue your conversation you will have to restart the connection.

Here is the conversation window in detail:



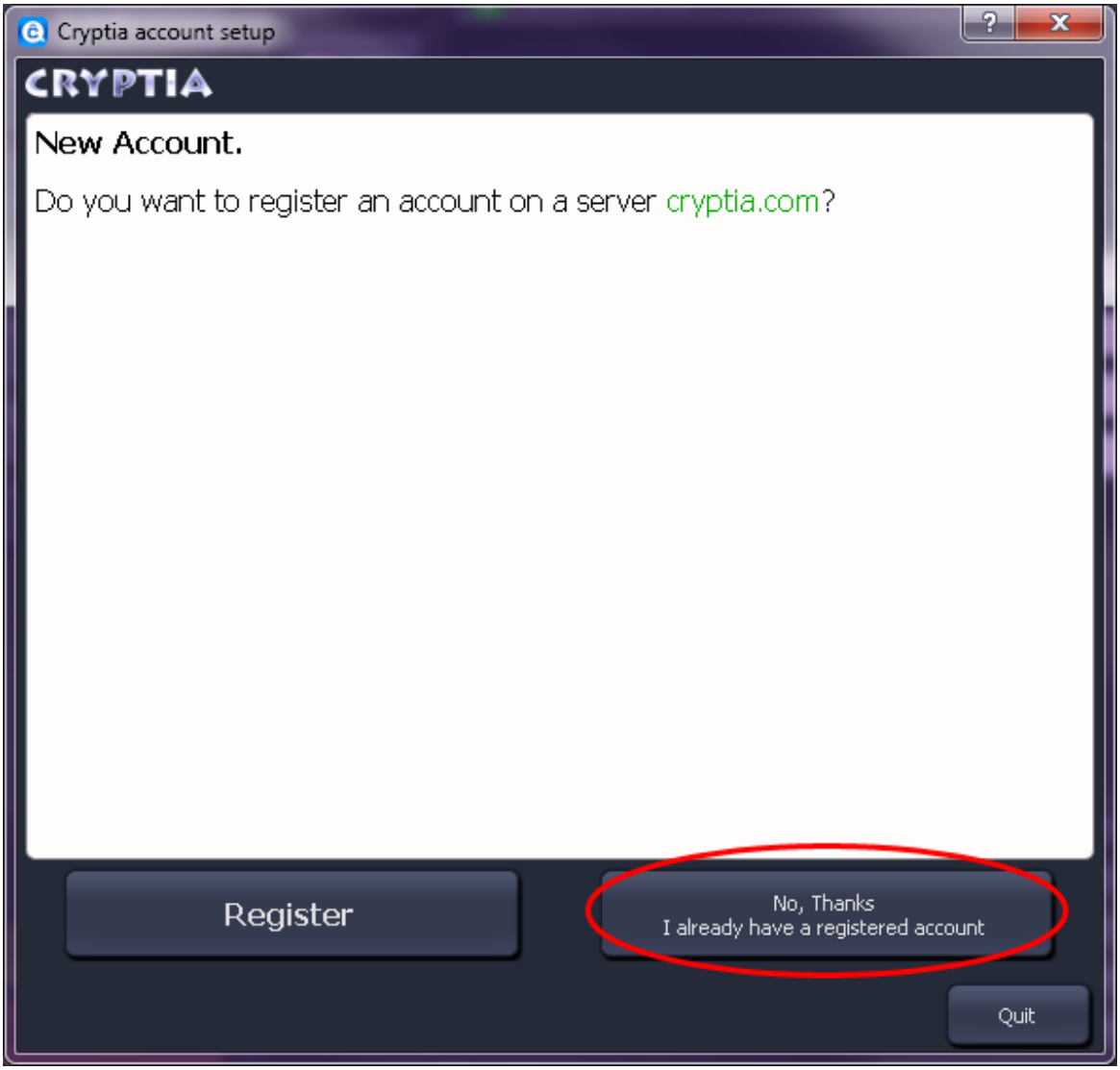

At the upper part of the window there is a green button labeled as Call (1), which serves to initiate voice connection. The Edit button (2), located below the portrait of your interlocutor, reveals editing tools, allowing to select a particular message (3), delete it (4) or copy it to the clipboard (5). The drop-down list labeled with the clock (6) can be used to filter messages based on the time of posting.

The gray bar to the top of the text entry field contains two buttons. The button to the left (7) lets you add animated emoticons to your text messages, while the rightmost (8) opens file selection dialog (default for your OS) in which you choose files to be sent to your interlocutor. The files can be sent to you in a similar way. All files you receive are saved to the Encrypted storage, and if it's unavailable - to the folder, designated in the *Interface* tab of the *Settings* window. Make sure the storage has enough free space available and you have the necessary write access.

# Part VI

# 6 Accounts

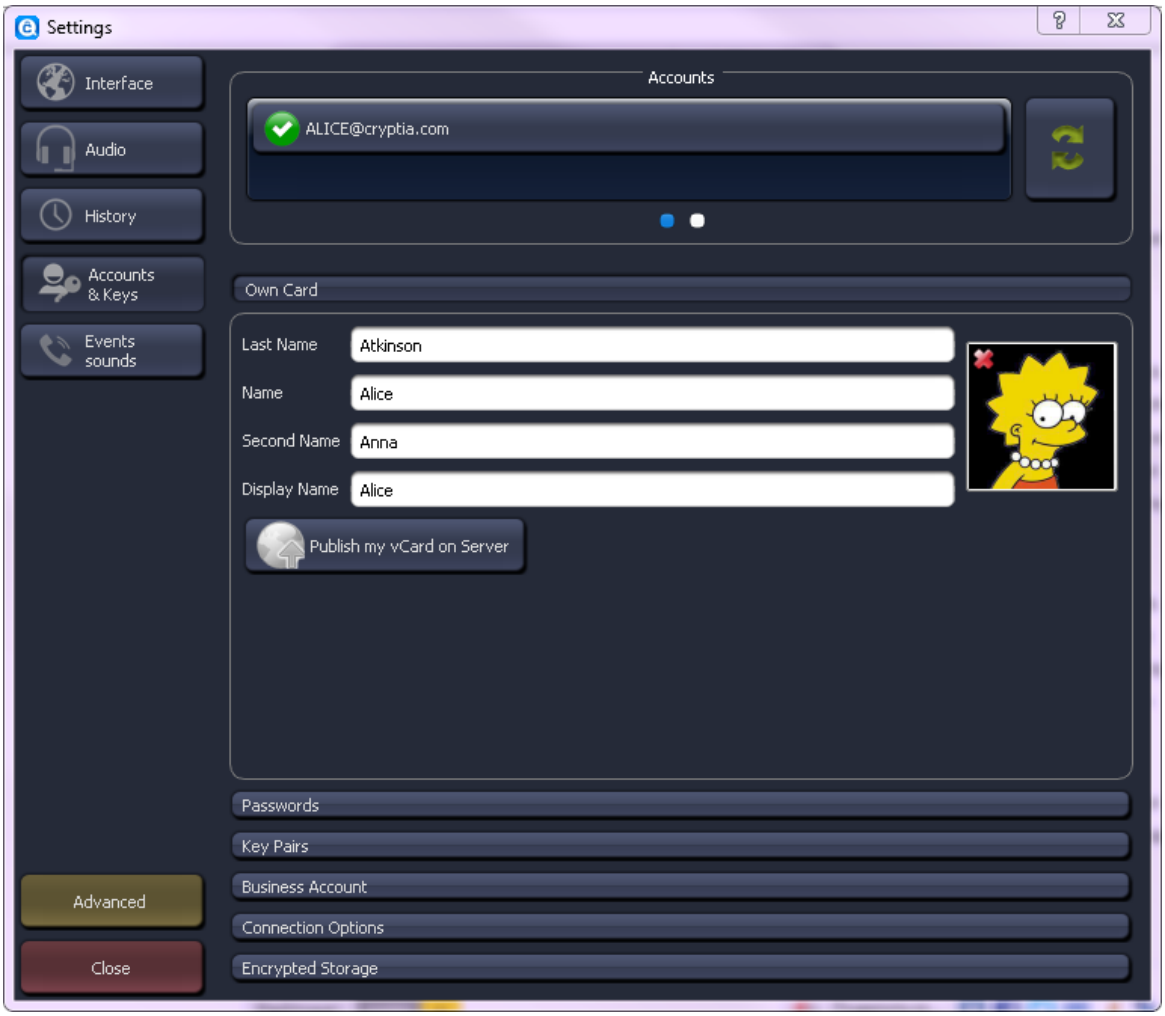
## 6.1 Adding an already registered account. Different account servers.



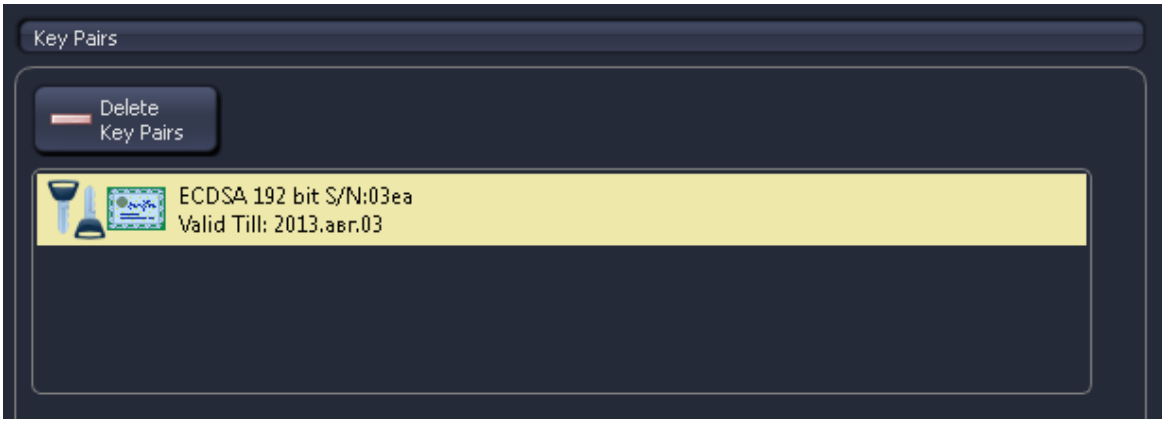

Cryptia account setup window lets you add an account you prevoiusly created on another computer. Click on the *No thanks, I already have a registered account* button. The dialog is essentially similar to the one where you registered a new account - all you need is to remember the Master password you created for this account and designate a new Daily password to be used on this computer. Note, that the Daily password may be different from those you used for the account on another computers and devices.


In case the account's server is different from cryptia.com (which may be true for corporate accounts; if you used Cryptia client to create an account, the server is always cryptia.com), type the server's adress into the entry field that becomes visible after you click on the *Another server* checkbox.

## 6.2 Key pairs




The picture above shows the *Accounts tab* of the *Settings window*. Some of the functions - namely adding, removing and scrolling accounts, calling card panel and password editing panel - had been described in the Quick start. The topic you are reading now is dedicated to the *Key Pair Management* panel while the next few topic of the manual will go through the remainder of the panels in the *Accounts* tab. Note that settings you choose in the *Accounts tab* are applied only to the account currently active (which is shown on the status bar on the top of the window), thus different accounts have independent settings.



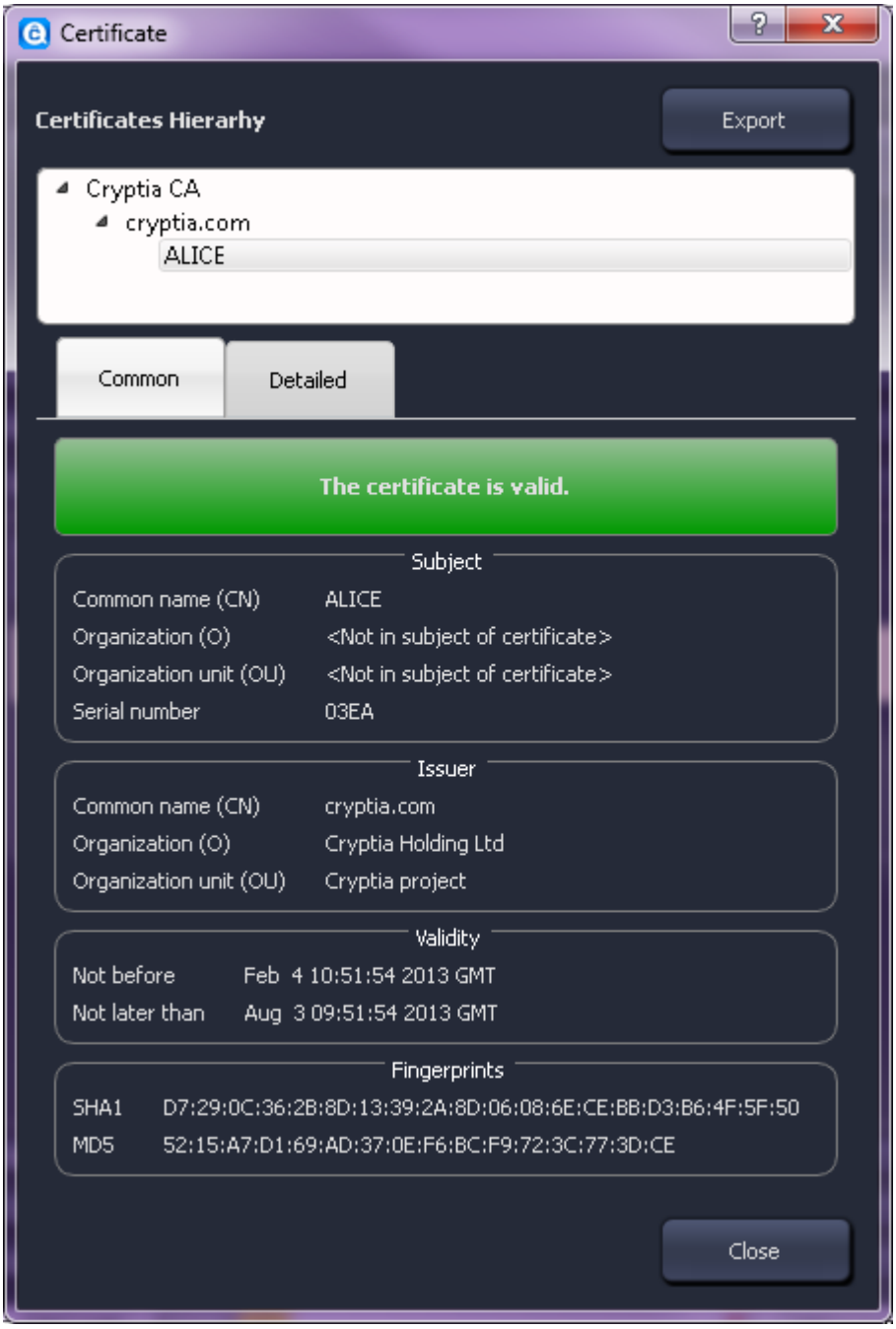

A key pair is a tool that verifies the authenticity of a connection with server or with another user. The pair is separated into two keys, a **public** and a **private** one. The former is sent to the recipient and can be authenticated using the latter, which is stored as a file on the sender's computer. Then the public key is applied to encrypt a message, and the private counterpart is required to decrypt it. The public key technology is a cornerstone of modern cryptography.

A Cryptia account has at least one separate key pair stored on each computer dedicated to client-server interaction - its private key is protected by the account's Daily password (if it's present on the computer). The client also stores multiple key pairs that are used to establish a connection with, and transfer messages to and from other Cryptia users.

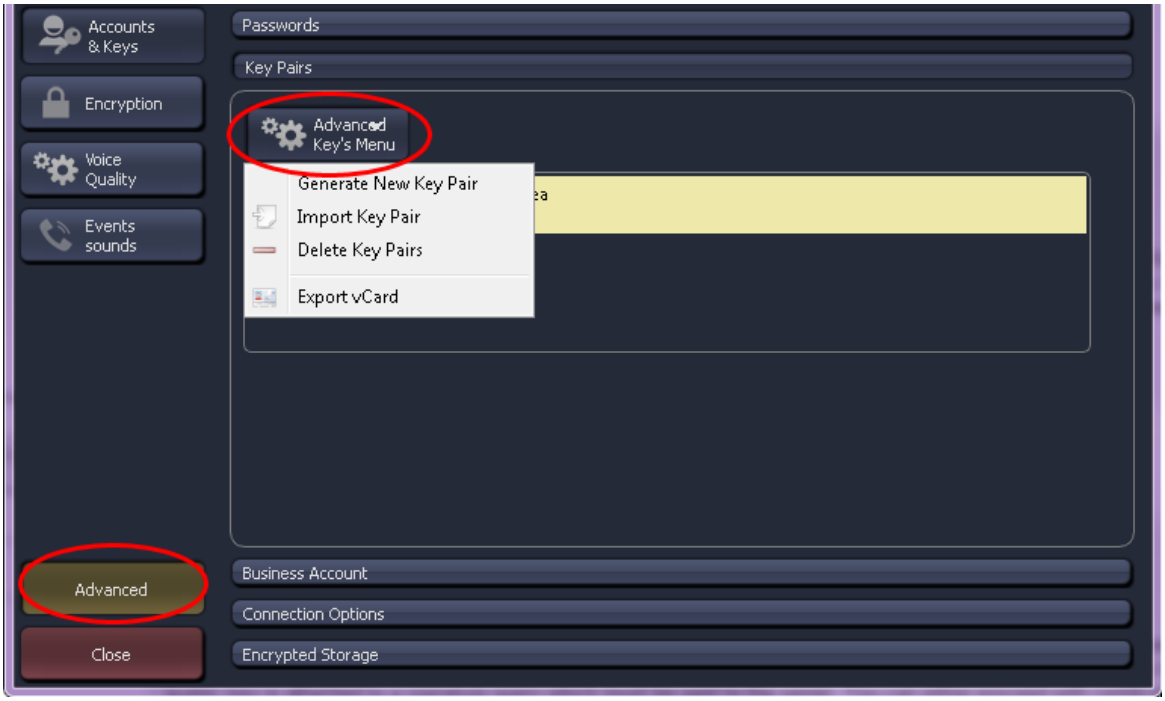
A **certificate** is essentially a public key that is signed by the issuer. The credibility of a certificate (i. e. of a public key) can be confirmed by an acknowledged signature. *Key Pair Management* panel contains a list of all certificates stored on this computer. The icons shows the current status of an associated key pair. Possible states are as follows:

| | |
|---|---|
|  | A newly generated key pair which has not yet been authenticized by a certificate. |
|  | A key pair with valid certificate. |
|   | A key pair which had its certificate revoked. You are not able to use this key pair it may only be deleted. See Manual Section "Cetificate Revokation and Invisible Mode" for details. |
|  | A key pair which had its certificate denied. It is unlikely to happen if you used Cryptia or OpenSSL to generate a key pair. Most probably, you had imported a damaged certificate file or the public key encryption algorithm is not supported on your computer. |
|  | Certificate revokation in progress. You cannot use the key pair, netiher you will not be able to delete it before you complete the certificate revokation process. |

Double-click on the key pair in the list to view the information about it.




If you have *Advanced layout* switched on (check the button in the lower left corner of the window), the *Advanced Key Management* drop-down menu will replace the *Delete Key Pairs* button above the list of certificates. It allows to create, import or delete a key pair. Besides, you can *export a *.vCard file* that contains your calling card and any certificates of your choice. Thus you are able to conduct a public key transfer on your own. A user that received the *.vCard file from you can import your calling card along with all attached certificates using the Contact info window.

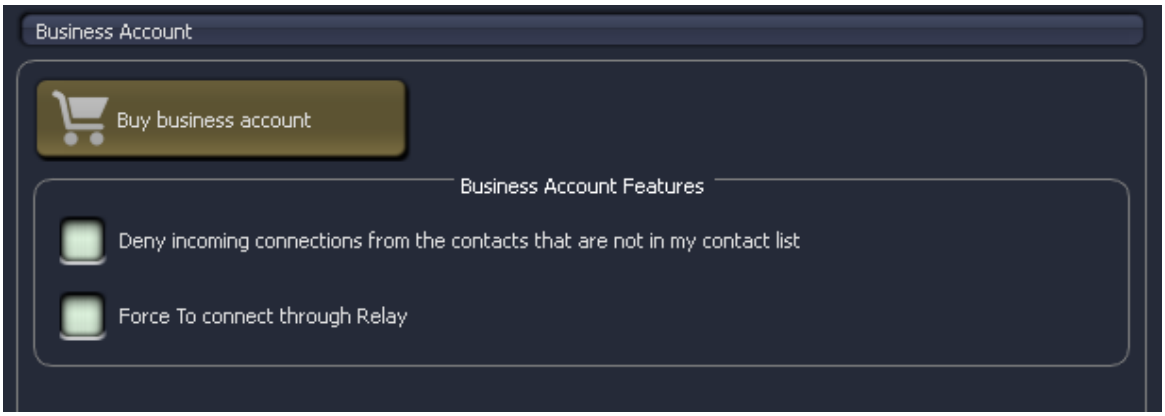



When generating a new key pair you can select a creation algorithm - RSA, DSA or ECDSA and define its parameters, such as key length or elliptic curve type. The generation may take time from few seconds to ten minutes or more. As soon as the pair is generated, the private key is encrypted and saved to your computer, and the public key is attached to a signature query which must be sent to the server. You can either proceed with certificate signing immediately or send the query later.

## 6.3 Business accounts

As mentioned above, non-paid Cryptia users are restricted only to five non-paid users per day which they can converse with. The restriction is lifted for business account users. Furthermore, conversations with business account users are not counted towards non-paid user's limit.

Business account is also required to perform a one-time connection (see one-time connection box of the Main Window). Business account users can deny one-time connections towards them by checking the *Deny incoming connections from users not present in my contact list* box in the *Business Account* panel of the *Accounts* tab.

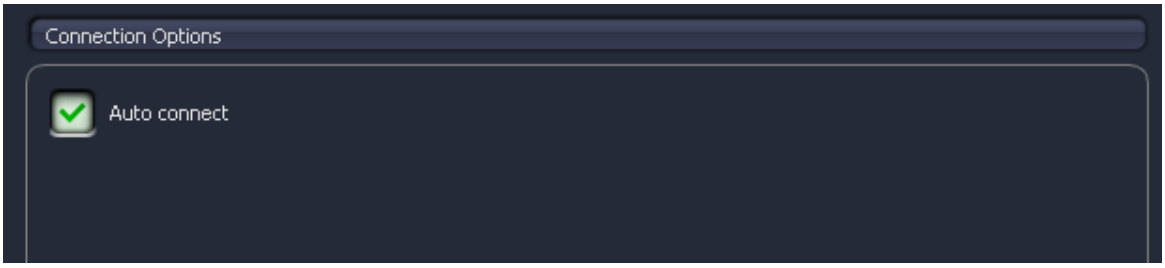


The second option of this panel will force the client to *always use a relay server* when establishing connection even if direct connection is possible. Your IP-address will not be visible, your interlocutor will see the IP-address of a relay server instead. Whenever both parties switched this option on, two relay servers will be used.

Note that Cryptia client may use a relay server on its own accord when making a connection if it is not possible to establish a direct one.

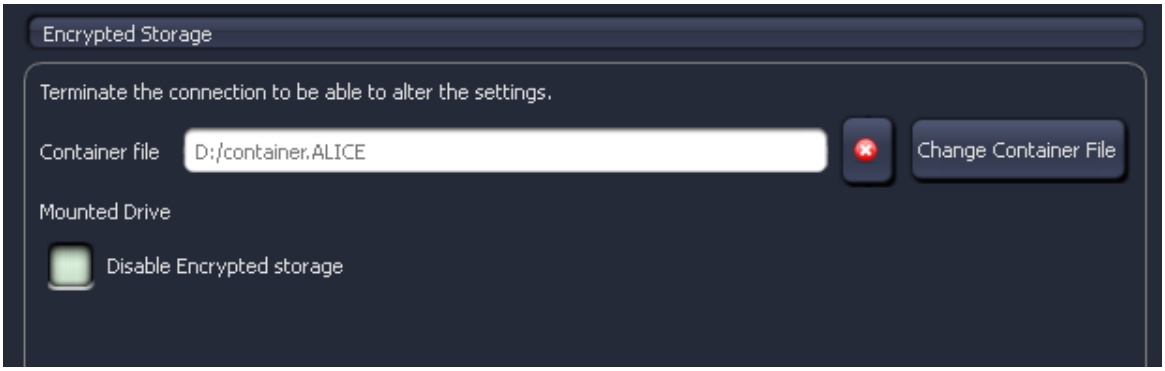
Clicking on the *Buy the Business account* button in the panel will redirect you to the webpage where you will be able to complete the purchase.

## 6.4 Automatic login on program start




*Connection options* panel of the *Accounts* tab contains only one possible setting. If it is checked, Cryptia client will connect the account to the server immediately after the program starts. However, it is possible only when the private key is not encrypted, i. e. you have no Daily password set for this account.

## 6.5 Encrypted storage management



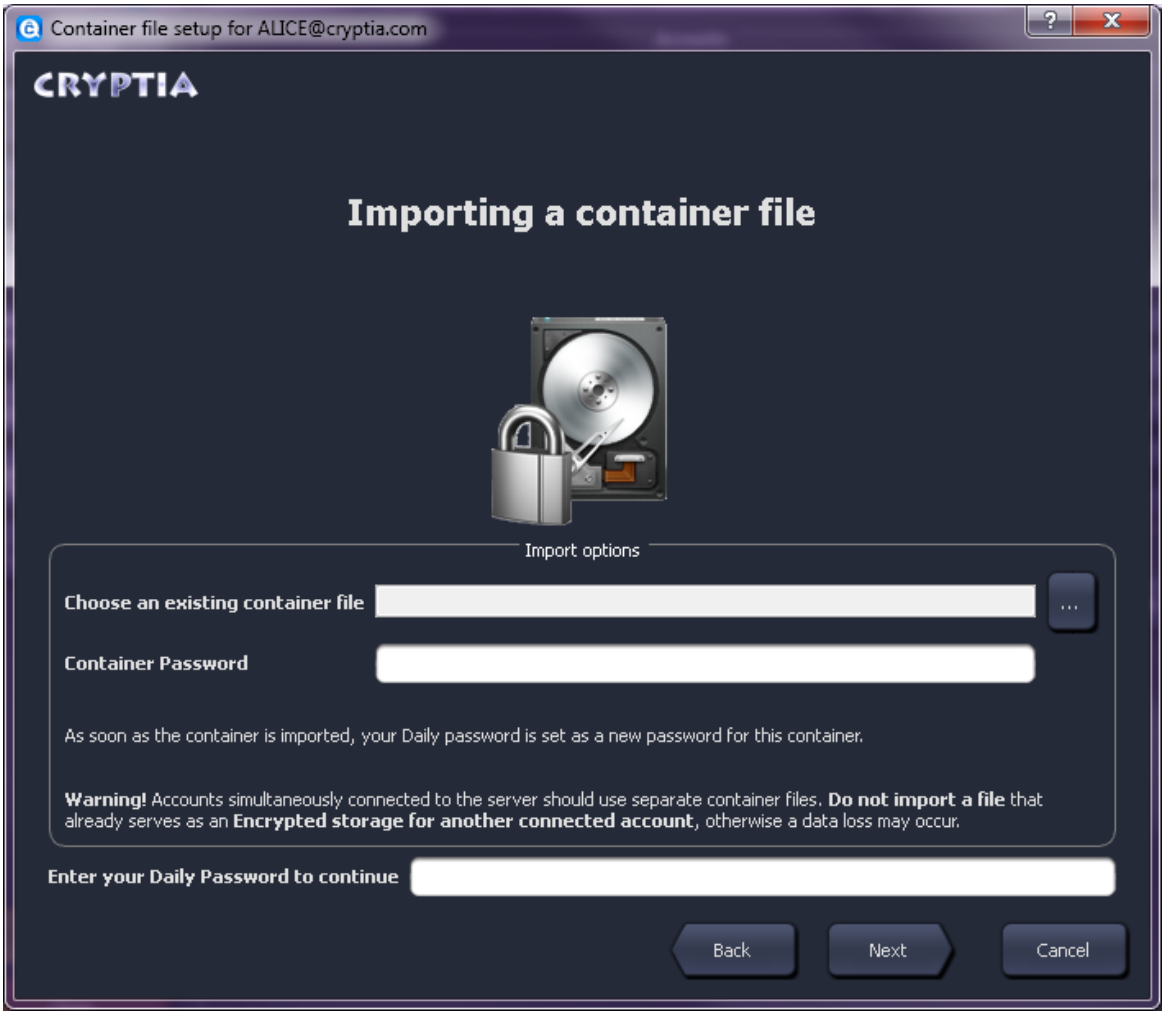

*Encrypted Storage* panel of the *Accounts* tab allows to set up the container file for your Encrypted storage. The setting are only changeable if the account is disconnected from the server.

Below the container file path an indicator showing the label of a mounted virtual disc (if you are using Windows) is located. To the right of the path line there are two buttons - the first disconnects a container from the account while the second allows to set up a new file. If you choose to desconnect a container file from the account, the file itself will not be removed - you'll have to do it by yourself if you want the data deleted. The *Disable Encrypted storage* checkbox temporarily disconnects the storage from the account when switched on, and reconnects the container automatically when

switched off.

The *Change container File* button will open up the following window:


The process of creating a new container file has already been described in the Quick Start. Importing an existing file looks like this:




You should enter the path to the container file and the password it is encrypted with.

If you have created the file using TrueCrypt, enter the password in <brackets>. E. g. in case the password you defined when creating the container was My_Password, you should enter <My_Password> here. We do hope the password you set was a bit more reliable though.

If the container file you are going to add was created by Cryptia, type in the Daily password of the account which the container was created for.

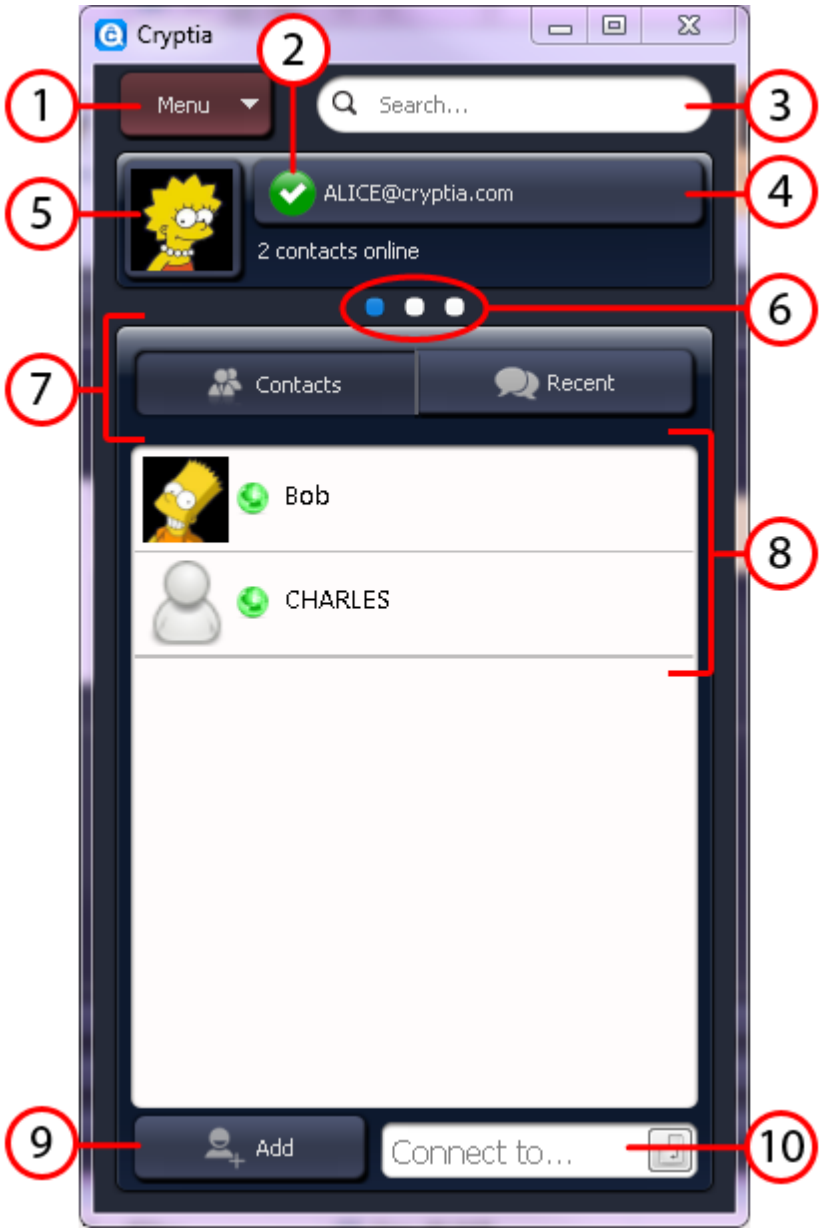
After the import, the container file is re-encrypted with the Daily password of the active account (i. e. the account you are connecting the container to). You need to type the Daily password into the entry field at the bottom of the window.

**Do not connect the container to two or more account at the same time!** Make the file you are importing is not set as Encrypted storage of other accounts, otherwise an irrepairable data loss may occur.

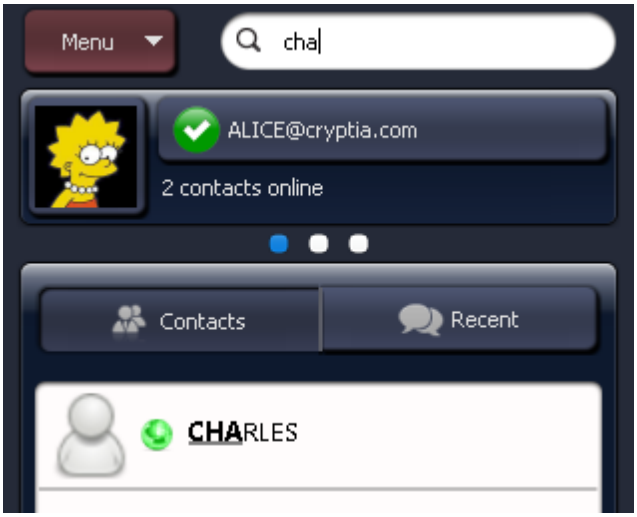
# Part VII

# 7 Main Window, contact list and message history

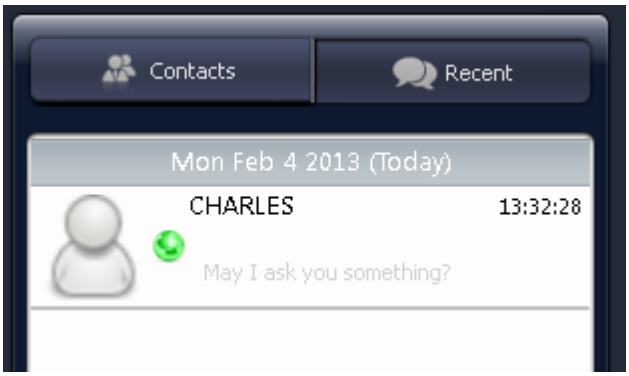
## 7.1 Main window in detail




1) A drop-down menu leading to *Settings*, *Message history* and *About* box. You can open the latter to find out the program's version number.
2, 4) The connection status icon and the status bar (see the next topic)
3) The contact list filter that picks out the contacts according to the filter query you typed in. After you have typed a text string, your contact list will show only the contacts that contain that string. The filter will not reset if you scroll through the accounts using the white dots below the status bar (6), so you can search multiple contact lists that way.




5) The portrait you added to your calling card. Clicking on it will open the *Accounts* tab of the *Settings* window.
6) The account tokens are white dots that correspond to accounts consecutively added to this computer. Clicking on a dot will make the respective account active.
7) A switch that determines what kind of entries the contact list comprises. It can be either **contacts**, sorted alphabetically, or **conversations**, sorted by time, from newer to older. Here's how the contact list looks like after you click on the recent switch:




8) The contact list. Double click on a contact to start a conversation. Right-clicking on a contact will bring up a context menu.
9) The *Add contact* button.
10) One-time conversation box. It starts a conversation with a user that is not present in your contact list - to do so enter the user's login and press enter. To use this feature you need either to have a business account or start a one-time conversation with business account user.

## 7.2 Connection status


The status bar is located at the top of the Main window (it also can be found at the top of Accounts tab in the Settings window). It shows the name of the active account and the status of its connection

to the server. Clicking on the status bar will either terminate the connection if the account is online, or start the login procedure in case the account os offline. The icon to the left of the account name is the connection status, which can be as follows:


Online

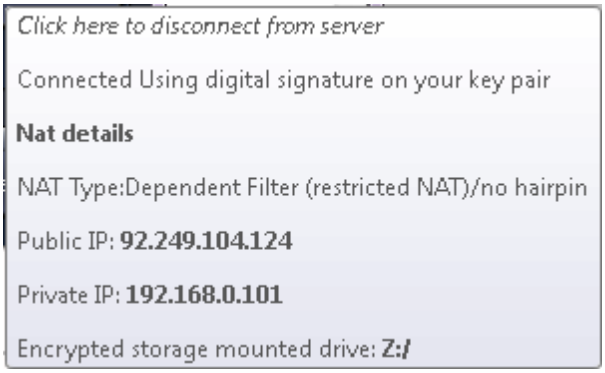

Connection error


Logging in

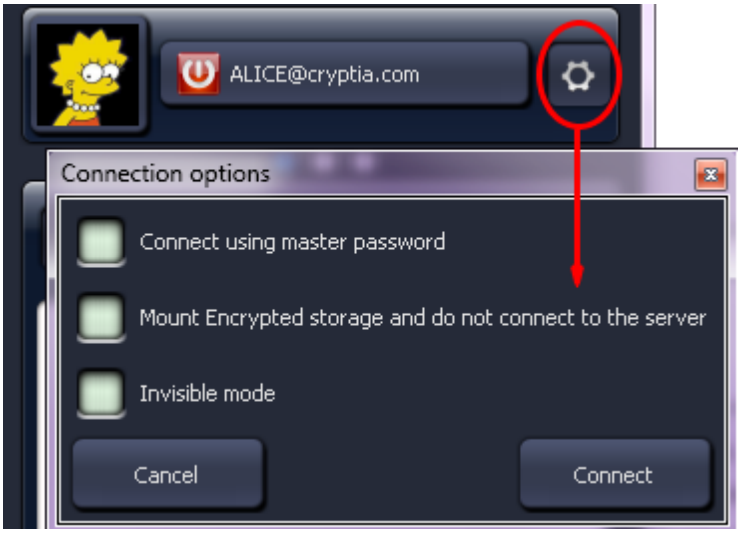

Offline, terminated by user


Offline, but Encrypted storage is mounted

You can also hover a mouse pointer over the status bar to reveal a tooltip with more information.




## 7.3 Certificate revocation and invisible mode




Click on the status bar to terminate the connection to the server. The termination makes an additional button, labeled with a cogwheel, appear (see picture above). The button also shows up in case the account failed to connect to the server. Click on the cogwheel button to open the *Connection options* window.

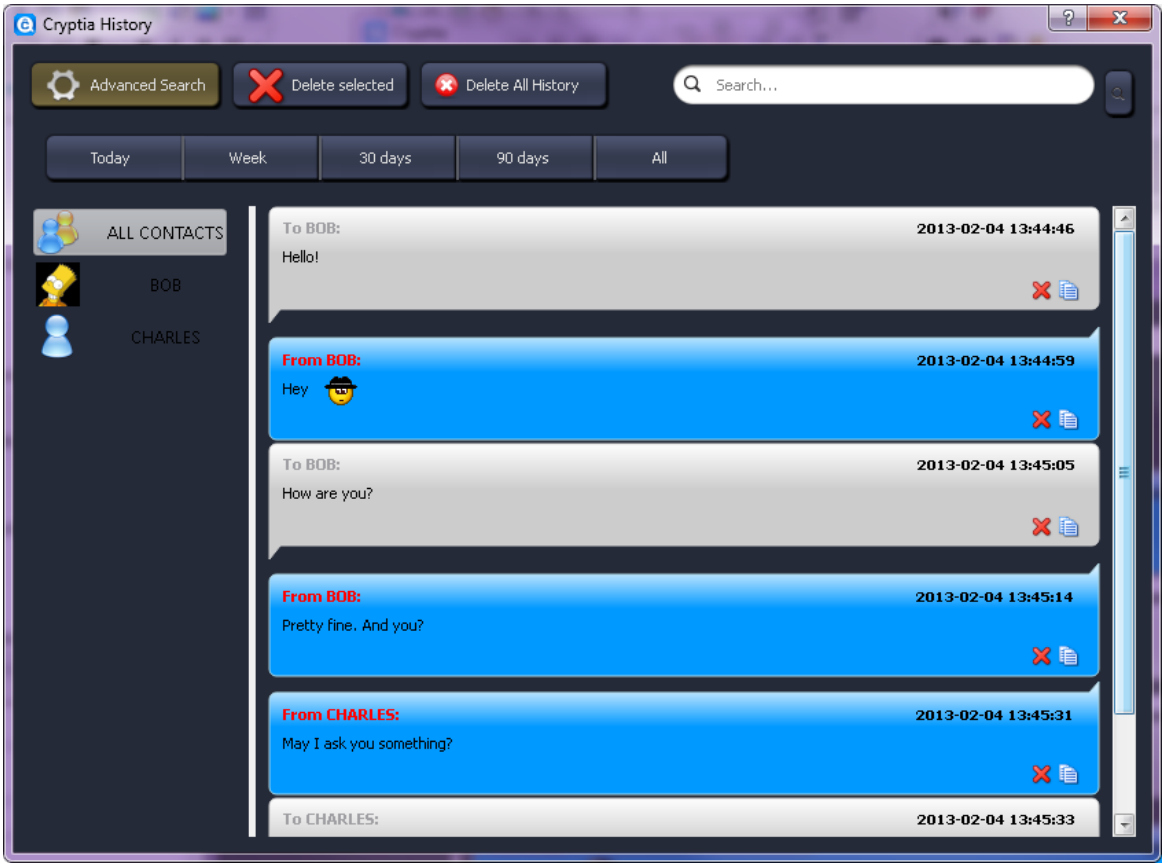

If you logged in using your Master password, you would not be able to make calls, send files or converse, the only options available to you would be key pair management and password changing. If you suspect that **somebody has stolen any of your private keys** and received access to your account, you are able to *revoke all your certificates* as soon as you log in using your Master password - this will render Daily passwords to this account on all devices void.

*Invisible mode* determines whether the users that have you in their contact list will see your online status.

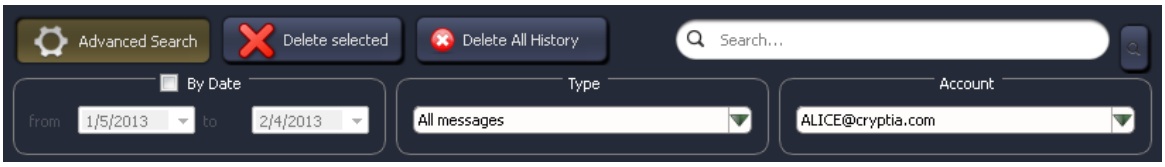
Here you can also *mount the Encrypted storage without connecting to the server.*

## 7.4 Message history

Apart from the *Settings* window, the drop-down menu, which is located at the top left corner of Cryptia's *Main window*, opens *Message History*. The latter keeps record of text chat, error and other server messages, as well as sent and received files log. Voice calls are not recorded.

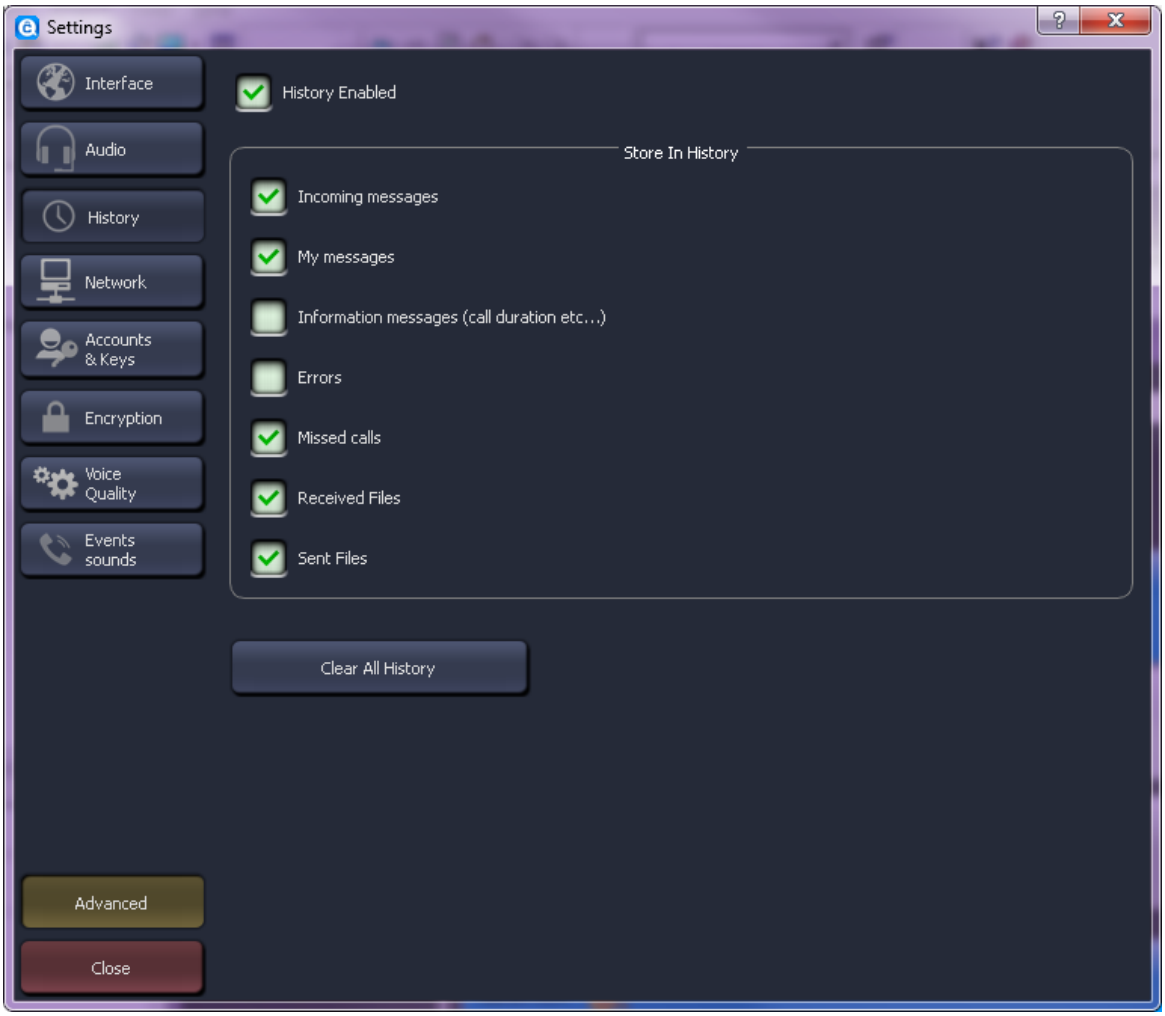



The options this window provides are self-explanatory. Filtered messages are shown in the center, each message may be deleted or copied to clipboard using the corresponding icons. Names list on the left allows to filter messages by the user you have had conversation with. More options, such as message search and date filter, are located at the top of the window.




*Advanced search* includes more precise date filter as well as message type (i. e. text chat, service info, file transfer logs etc.) filter. Note that Cryptia stores history for all accounts added to this computer. The *Account* drop-down menu found under the *Advanced Search* allows to filter messages by the specific account to which these messages are related.

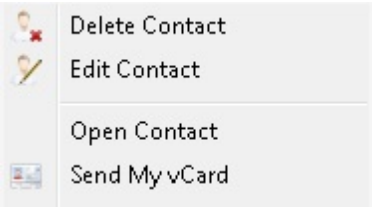
## 7.5 Message history serrings




The following tab of the *Settings* window contains control options over which messages should be kept in the history log. Make sure you have the *Advanced* mode turned on to see the options. The button below erases everything currently recorded.

## 7.6 Account info

Let's return to Cryptia's *Main window.* As you right-click on the contact in the list, a context menu appears:



The two bottom items had already been described in the Quick start. If you choose to *Delete a contact*, the contact will be removed from the computer you are currently working on along with associated message history and certificates. The information deleted will not be restored in case you add this contact again.

*Editing a contact* takes place in a separate window which will open up as you choose the appropriate option in the context menu. *Display name* defines the alias that will show up in the contact list. The ring tone is an audio (.mp3 or .wav) file which will play every time the user starts a conversation with you. After clicking on the *Advanced* button, the layout of the *Contact editing* window will change as follows:


Advanced contact editing includes certificates and key-agreement protocol parameter cache associated with this account.

Certificates that applied in establishing a secure connection with this particular account can either be transferred along with a calling card or installed manually. Click on the *Add* button in the

*Certificates* panel to do the latter. Click on a the *Details* button to review the certificate you selected. Note that it is impossible to verify a certificate unless you are connected to the server.

Key-agreement protocol parameters (Diffie-Hellman or Diffie-Hellman on elliptic curves) are transferred from the initiator to the receiving party during the initiation of the first conversation. These parameters are stored in the cache and subsequently reused in the later conversations. The parameters are transferred via the server; although the public transfer of these parameters poses no threat, you can import them using this menu (provided the other party generates and exports them via Encryption tab in the *Settings* window).

The next topic covers .vCard files import and export.

## 7.7 Bypassing the server in calling card exchange

In case another user decided not to publish their calling card on the server, Cryptia will not have any information about them apart their login. This user can either transfer the calling card to you while being added to your contact list or send you the .vCard file that contains the Calling card and certificates you should import. To do the latter, click on the *Import vCard* button during the Contact editing (see previous topic). Here you can also export the Calling card of the user whose contact you are editing to a vCard file you can transfer to a third party.


To export your own calling card to a file, use the Key pairs panel of the *Accounts* tab in the *Settings* window. Click on the *Advanced key management* drop-down menu to see the function required.

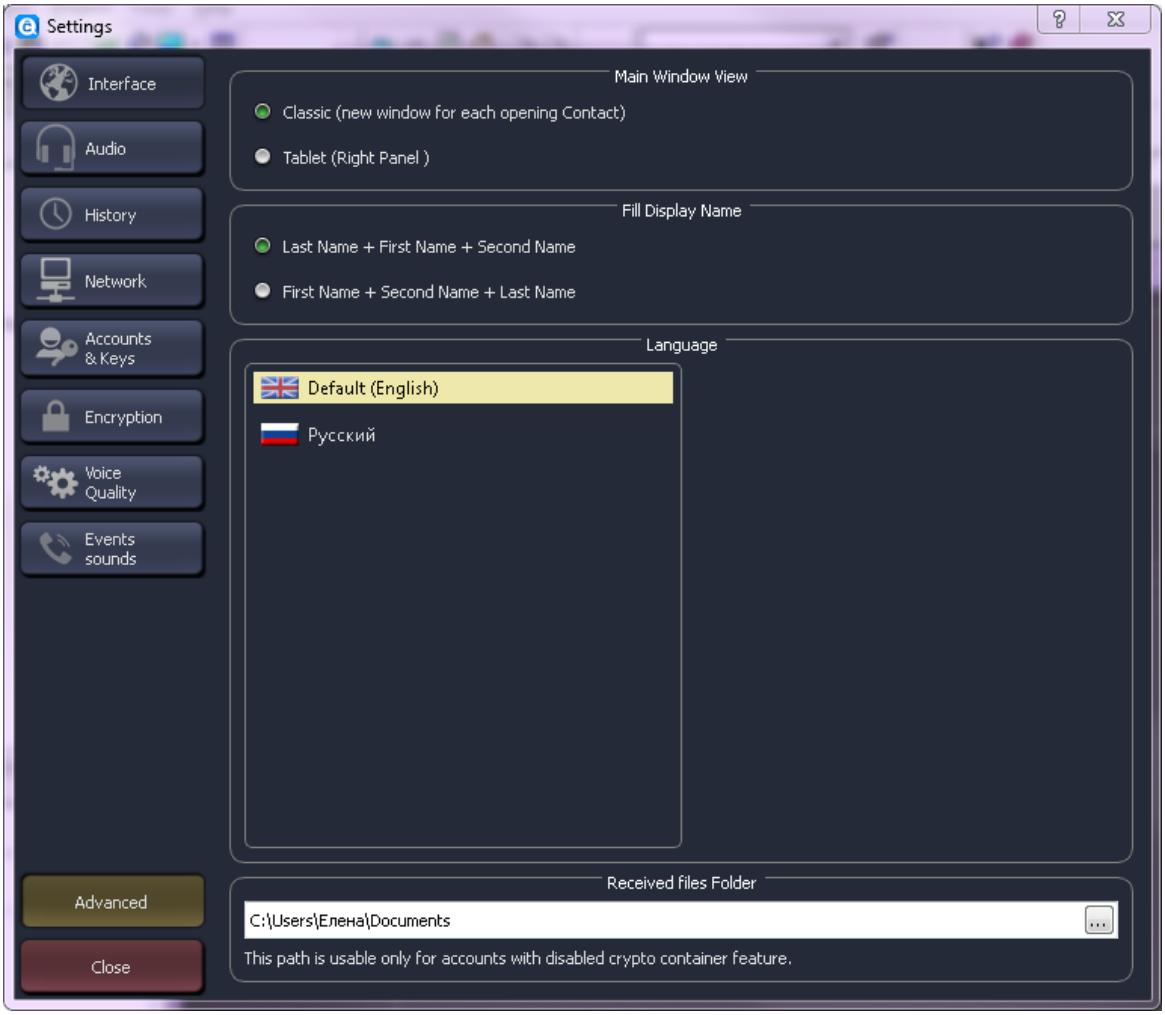
# Part VIII

# 8 Settings

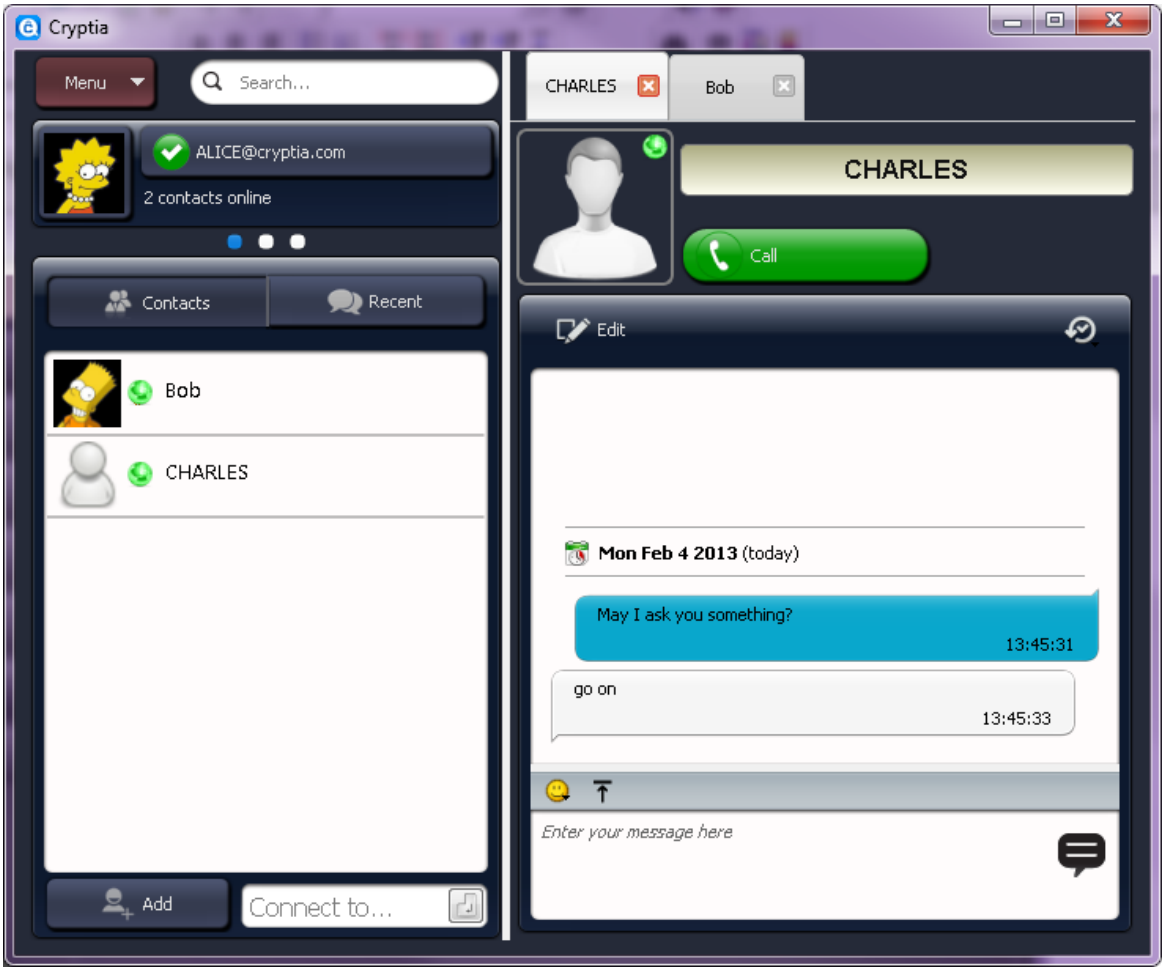
## 8.1 Preface on Settings

The section covers all tabs of the Settings window besides the Accounts tab (described here and here) and the History tab (described here).
If the layout you see in this manual does not match the one you see on your computer, make sure you have Advanced mode (the button in the lower left corner) switched on - most likely the item you miss belongs to extended settings. Note that the layout may also be different according to the Operating System you have on your computer.

## 8.2 Interface settings



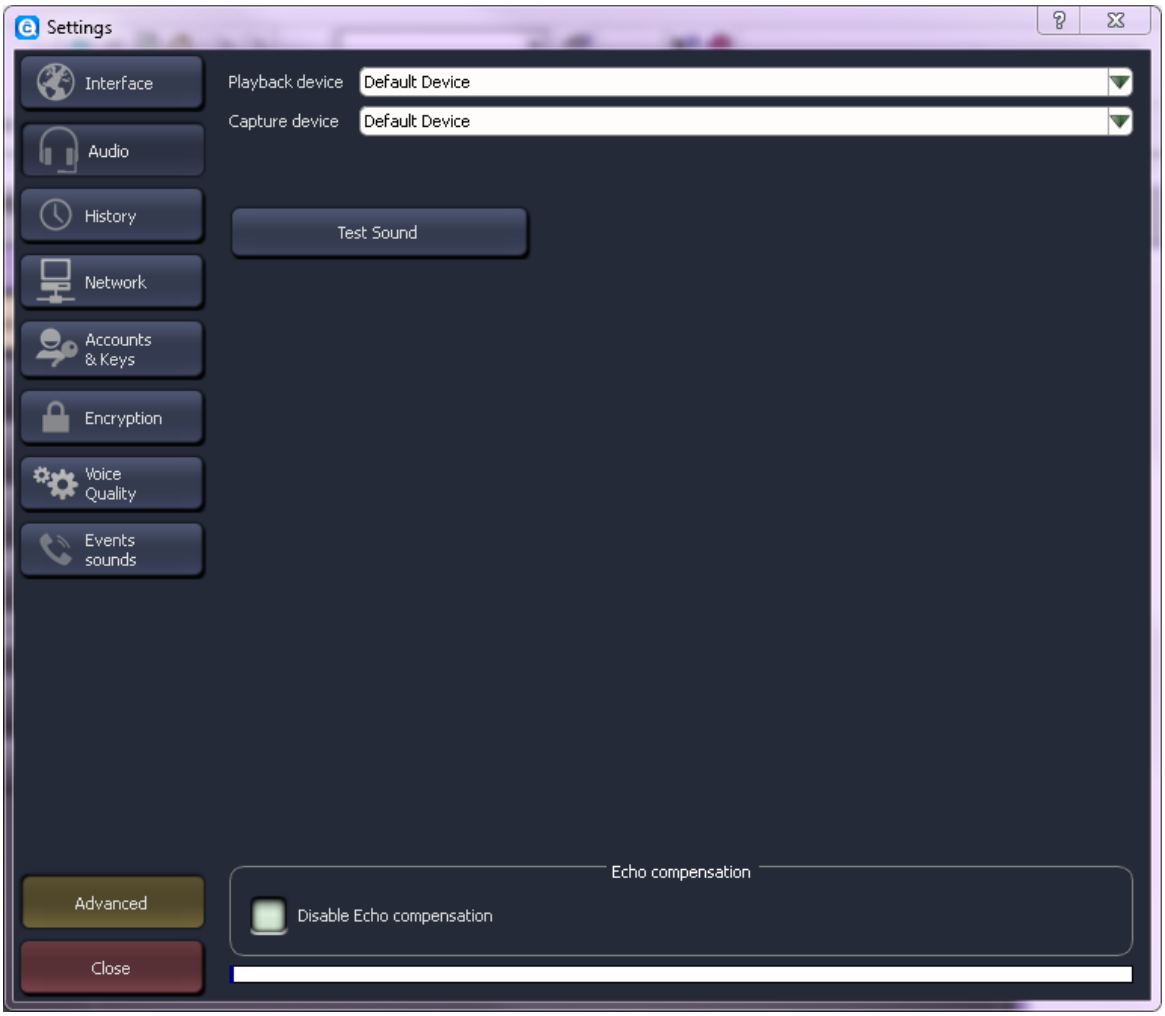

The Interface tab has already been described in the Quick Start under the subject of language selection. Additionally you can define the following options: a) *the order* in which the *names* (first, middle and last) of another user *are displayed* in your contact list, unless you specified an alias; b) *the layout of Cryptia's Main window.* The latter determines whether a conversation started will require a separate window to be opened or will use the same Main window.



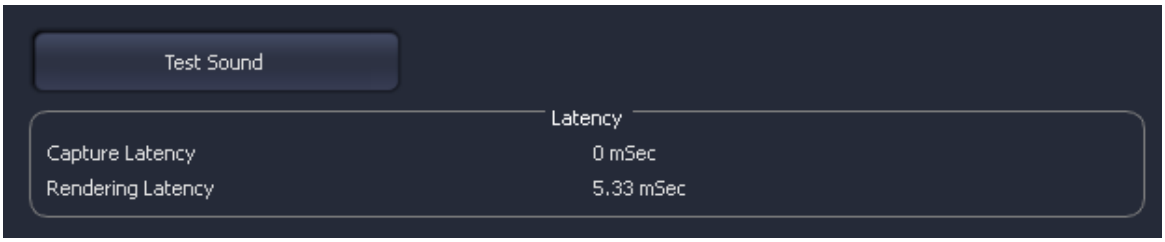

On the screenshot above you can see Cryptia's Main window in *Tablet* layout. Tabs on the top of the right side of the window contain opened conversations - the arrangement which may be more convenient for having several conversations at a time. Also, this layout may be more familiar for some users.

*Advanced settings* include *the path which files you receive are saved to* in case Encrypted storage is unavailable. Make sure you have write access that allows you to save files at the destination specified.

## 8.3 Audio settings

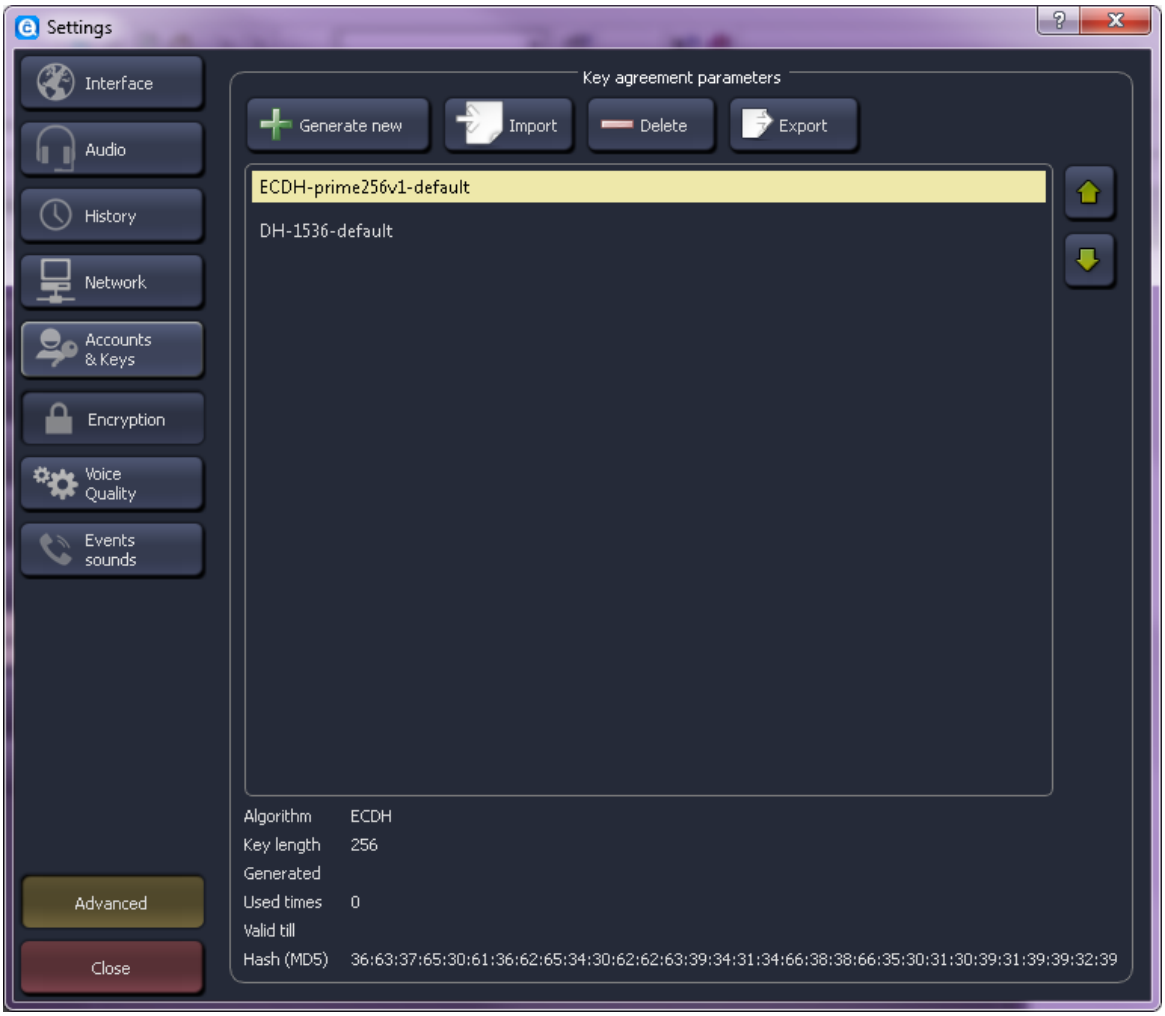



This tab allows to select a sound device to be used by Cryptia for *recording* and for *playback*, provided you have more than one. You can also disable echo cancellation if you want to preserve the computer's processing resourses. Note that if you are using headphones or audio headset for voice communication, there is absolutely no need in echo cancellation.



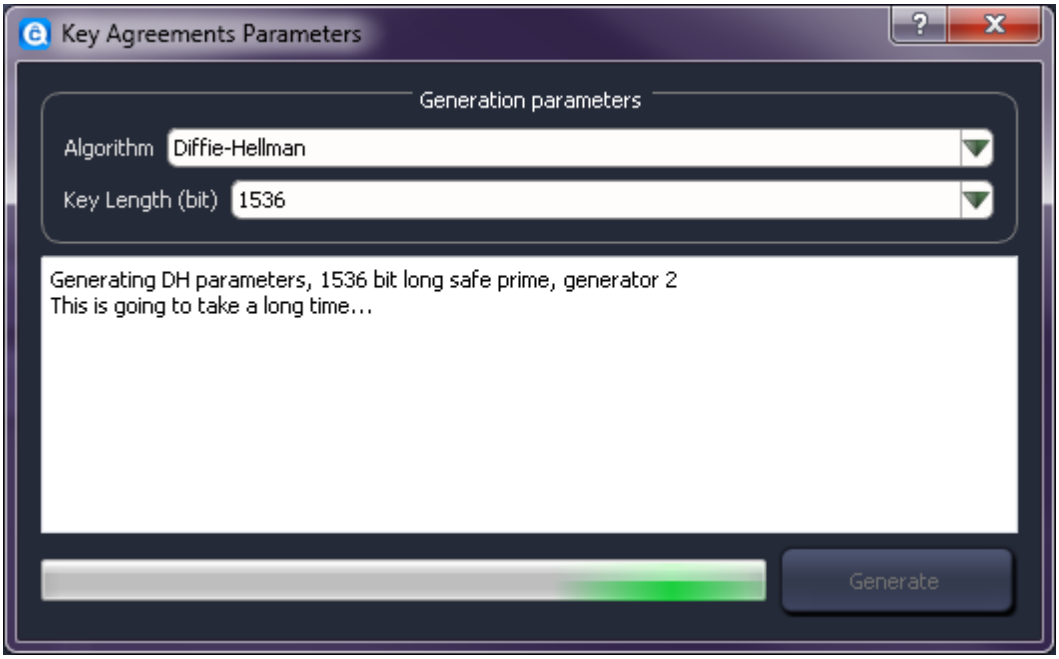

Clicking on the *Test Sound* button will trigger an automatic audio device test, and mesured latency value will be displayed.

## 8.5 Encryption settings




Key agreement algorithms are necessary for establishing an outcoming connection. You may have several algorithms set up, and they will be used in the order specified in this tab. The priority goes from top to bottom, and the arrows to the right allow to set up the order.

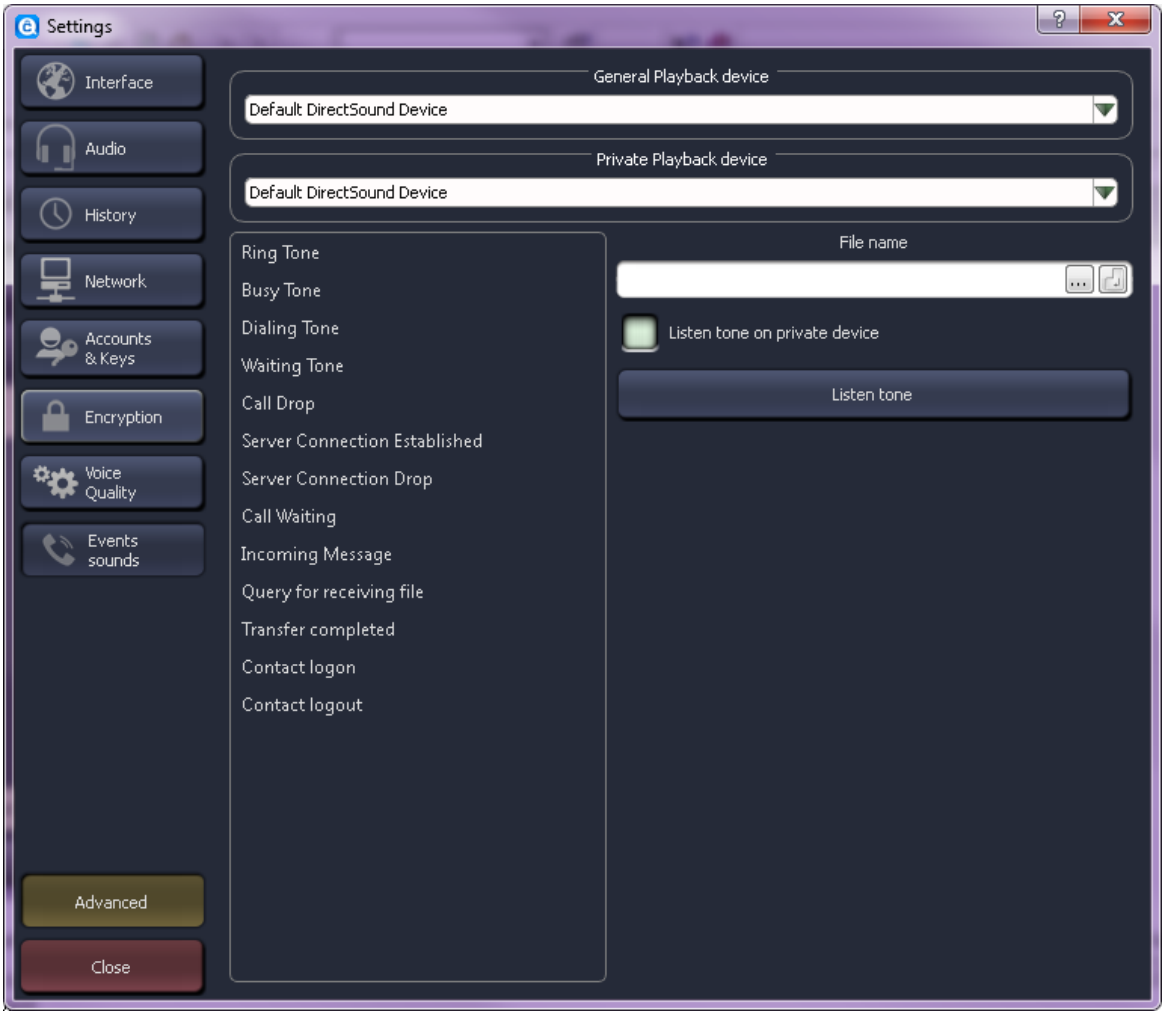
To ensure maximum efficiency you may want to have at least one set of parameters on Diffie-Hellman algorithm and one on Diffie-Hellman on ellyptic curves. To generate a new set, use the Generate new button at the top of the window. Similarly to key pairs, the parameter set generation may take any time from couple of seconds to dozens of minutes, depending on the algorithm you specified.




You can also import a parameter set generated by another program and export a set to a file which another user will install to their cache manually (use this if you want to bypass the public transfer of parameters).

## 8.7 Event sound settings

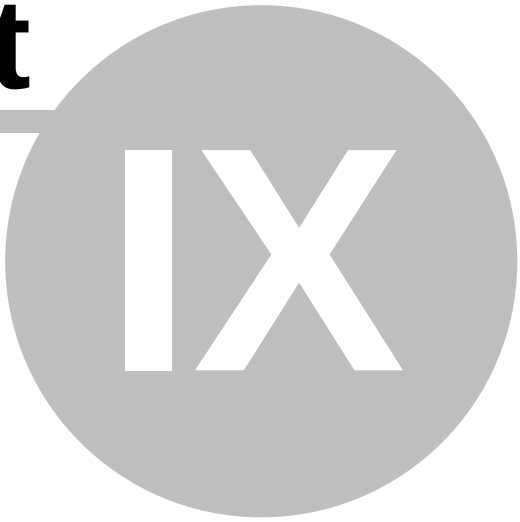
This tab allows to select an audio device which will be used for the playback of event signals and choose the particular audio files which will be the signals.




The list on the left present various events which may trigger a signal. The Listen button on the right allows a preview of a current event sound. Entry field above the button contains a path for the sound file (.wav and .mp3 file formats are supported), and the button with an ellipsis opens browse window.

Return button ( ) resets the default sound for this event.

# Part



# 9 Advanced

## 9.1 Cryptia.ini editing

**The most advanced and obscure settings may be defined only by changing the cryptia.ini file** (see here on topic of file's location). **The reason is that non-expert user should not be able to alter the program into complete inoperability. You should know what you are doing and hold full responsibility on Cryptia's functioning. We also recommend to back up a copy of the file before any advanced editing starts.**

### Rerouting

You can replace the file's contents with a new path for a configuration file. This may be helpful if you want to use a folder with different access rights, e. g. in Linux.

```
[redirect]
cryptia.ini=new path/cryptia.ini
```

### Address book file rerouting

Under the [your_computer_name] section create a following line:

```
addressBook=<Full or relative path to the file>
```

In case no path defined, Cryptia will search for it in its program folder, then in the personal folder (in Windows the default path is C:\users\[username]\Appdata\Roaming\Cryptia). If the search fails, the file will be created in the latter location.

### Force predefined UDP ports

If you enable this option, Cryptia will occupy the specified range of UDP ports to prevent them from being taken by other programs. In some cases, particularly when a restriction on UDP (apart from DNS query) is enforced by the network administrator and you need to program an exception, or when you have a symmetric router and want to forward ports, you can predefine UDP ports by inseting following lines:

```
[serverConnections]
forceToPorts=true
firstPreprogrammedPort=41000
lastPreprogrammedPort=41010
```

Otherwise, this option will be disabled. Also, when this option is turned on, NAT settings will not take any effect.

### Connection timeout

The server is set to terminate the connection with the account after 60 seconds of inactivity. To keep the connection, a special packet named keepAlive is transferred by client. The default interval between keepAlive packets is 45 seconds, but you can change the timing by altering the following lines:

```
[serverConnections]
```

```
keepAliveTimeout=45000
```

## Symmetric encryption algorithms

Supported encryption algorithms may be listed (in the order of preference) under the [encryption] section. For instance:

```
[encryption]
supportedVoiceCiphers=aes-256;camellia-256;cast-5;seed;des3;bf;
supportedDataCiphers=aes-256;camellia-256;cast-5;seed;
```

You may add any algorithm that openSSL library, which is supplied with Cryptia (or installed to your OS), supports.

In case no algorithm is specified, aes-256, which is the default algorithm, is implied. If you don't include aes-256 to the list, Cryptia client will be unable to establish a conversation with other users, unless they alter their settings appropriately (by including compatible algorithms to their supported encryption algorithm list).

Back Cover