

# Delta Chat UX testing Kyiv Oct 2018

**Final Version: March 2019**

Ksenia Ermoshina, Vadym Hudyma



# Table of Contents

Introduction.....	3
About the writers of this report.....	3
Key findings.....	4
Detailed findings.....	6
Task 1 - Create an account and start chatting.....	6
Task 2 – Group chat.....	9
Task 3 - Verification and verified group chat.....	15
Task 4 - Backups, Import/export of the keys.....	17
Other feedback and requests.....	19
Appendix: User reaction synthetic tables.....	20
Task 1.....	20
Task 2.....	21
Task 3.....	22
Task 4.....	23

# Introduction

Delta Chat user-testing took place in Kyiv<sup>1</sup> on October 30 and 31, 2018 and included 12 testers, 10 coming from journalistic and NGO activist user-groups, and 2 being local tech enthusiasts, though not specialists in secure messaging or cryptography.

Based on our prior needfinding, we first designed our user-testing tables, that featured 4 big tasks. Each big task included smaller step-by-step actions for users to follow, and a series of reactions to choose from. We picked 5 basic emojis, from very happy to angry, as well as offering “no answer” when users preferred to skip emotional reactions.

The testing sessions took 2 hours each. They started with a very brief introduction to Delta Chat that did not include any technical explanations or anything that could potentially influence users’ behavior or attitude towards the app. We then distributed 4 tables to each user, turning the sheets blank side to the top, so that they could not anticipate the tasks and thus would be less biased.

While users were completing the tasks we did not give any recommendations or advice unless they reported being really stuck and explicitly asked for help. We took notes on all reactions and spontaneous observations that users shared while working on their tasks. Every time a big task was finished, we asked users to take a short break and asked each of them for a few comments in freestyle: all emotions, reactions, swearing and laughter were welcome. These were noted by hand but also recorded with an offline recorder Zoom h4n, with explicit permission obtained from the testers before the start of the session.

After all four tasks were complete, we asked users if they had any general comments, and noted these last remarks. Some of the testers subsequently joined us together with Delta Chat developers for further informal discussions. One of the interesting and important outcomes for us was the longer-term engagement with some of these testers, who have now become more or less active advisors and test groups that will be involved further in upcoming happenings such as the Delta-Xyiv gathering in Spring 2019. Their organizations having quite explicit needs and requirements, and we have been working with them to narrow down our development priorities. The next iteration of user-tests will thus include some of the users from these first tests, and a group of new users, to compare perceptions of the app progress versus fresh experiences and impressions.

## About the writers of this report

Ksenia Ermoshina has been involved in the Autocrypt community since December 2016, first as a researcher focused on secure messaging protocols and usages and as an active user of PETs. Her role has progressively evolved leading to her engagement with Delta Chat’s development team as a “usability” person, though also reflecting upon her personal user-experiences as an activist, and helping with community-growing, local organizing, ensuring constant feedback between the DeltaChat team, high-risk user groups and a more “tech-

<sup>1</sup> See the report about Delta-Xi Kyiv gathering here: <https://delta.chat/en/2018-11-17-deltaxi>

oriented” group of testers. Ksenia’s research on digital security for Crimean activists and journalists highlighted the focus on Ukraine as the country where DeltaChat found its main testing playground and community connections.

Vadym Hudima has long-term experience as a digital security trainer working with high-risk users, NGO activists and journalists in Ukraine, including risk groups working on the frontlines in war-torn zones of the country. Vadym joined the DeltaChat effort around spring 2018, and has been working to feed his expertise as a trainer, namely with risk assessment and threat-modelling, into designing more informed and detailed use-cases for DeltaChat. His immediate knowledge of the Ukrainian context helped prepare and conduct Delta Chat’s need-finding research to discover real user perspectives.

## Key findings

*As a preliminary notice:* the immediate results of this testing were shared with the Delta Chat developer team already during the Kyiv gathering in October 2018. Many of our immediate recommendations confirmed developers’ expectations, as well as corresponded with some of the open issues on our GitHub page and topics raised on the User Support forum. Many of the recommendations have since been implemented and are present in the newest Delta Chat v 0.200. Some of the fundamental features, such as verified groups, have undergone heavy redevelopment, with the implementation of ‘rpgp’. We will emphasize this progress further in this report. However, we think it’s important to share our key findings and detailed findings that may be of interest for other secure messaging and email app developers, designers and users.

- While Delta Chat Android app has proven itself to be quite usable, some of its features require better explanation. **Wording** stays one of the most important aspects to work on. The wording is a challenge for Delta Chat, also because of its **decentralized** nature, as users are generally more used to centralized messaging apps that store users’ data on their own centralized servers.
- Our tests and more general research on secure messaging show that users’ behaviour have been quite deeply **formatted by the most popular apps**, such as Signal, WhatsApp and Facebook Messenger. Many of the expectations for Delta Chat usability come from these patterns, and while some of them should be progressively modified (towards building **better UX/UI paths for decentralized tools**), others should be met, at least for the nearest future.
- For example, users expressed concerns about “permissions” and access of Delta Chat to their contact lists, gallery, camera and so on. We recommend to **modify the default permission messages** in order to make them more explicit to the users, namely, emphasizing Delta Chat’s “serverless” nature (e.g. explaining that the app does not store anything on a centralized Delta Chat own server). Another aspect related to this is the “real password”. Testers were confused about trusting Delta Chat with their real email password.
- Therefore, we recommend to **use graphic elements, videos and other visuals**,

within the app's FAQ and on the Delta Chat blog, to explain Delta Chat's features, such as "no phone number required", "no Delta Chat own servers", "end-to-end encryption" and others. Our additional recommendation is to make the FAQ accessible offline within the app.

- The app's "**contact**" **management** is another interesting challenge that we recommend to work on. There is a certain user reaction pattern that we call "**fear of the contact book**": it is a concern expressed by many users who do not want to merge their Delta Chat app-specific contacts with their phone address book. Our recommendation is to make interactions between Delta Chat and the phone address book more explicit (see the FAQ-related recommendations). Our second recommendation is to show how a contact was added (e.g. "phone address book", "directly added" or "introduced as member of a group").
- Finally, we recommend to provide a **simpler and shorter path** to add and delete a contact, as well as an easy way to switch between group chats and one-to-one chats. Here, major progress has been made in v.0.200 towards giving users optional paths for adding new contacts, however some challenges persist that we detail in the findings below.
- **Verified groups** are another challenge for Delta Chat usability. One of our concrete recommendations is to change the color scheme within a verified chat (for example, to a darker theme). These expectations come from Facebook's "Secret chat" function. We also recommend to **work on a visual/graphic element** for better explanation of the "verification" process.

# Detailed findings

## Task 1 - Create an account and start chatting

### Account creation process

Several users expected to have a separate “sign up” button, however, they saw only a “login” form. Almost all users were confused that they had to enter their real email login details from their pre-existing email account(s), and not to create a new app-specific password for Delta Chat. They expressed concern about Delta Chat having access to their emails.

5 users out of 11 experienced problems with IMAP settings. They asked for better explanations about why exactly they could not log in.

### Recommendations

For the account creation process, we recommend to add separate pages for login and password, in order to give more screen space to add explanations. Key elements to elucidate include:

- Delta Chat does not have servers and does not share passwords with anyone, as they stay on the device; maybe mention on the login screen that Delta Chat acts as an e-mail client;
- Delta needs you to use an existing email account or register with a (trusted) email provider;
- Probably give a link to the FAQ or Delta Chat’s website section with a “white list” of providers that are known to have no or very few issues with handling Autocrypt headers;

For IMAP settings we recommend to:

- Include links to the FAQ/help;
- Add direct links to appropriate IMAP settings for the most widely used email providers.

### Sending a message to a new contact, replying to new messages

When mistyping an email address, users did not get any notifications about the fact that the email was sent to a wrong contact, or not delivered at all.

Many users were irritated that the app asked permission to access their contacts several times. However the newer Android versions (8+) and iOS repeatedly ask for permissions to basically everything. Therefore, while we need to take user reactions to permissions into account, we might better focus efforts on what defaults should be chosen or even propose

different preselected option sets for users with different threat models (regular vs high-risk).

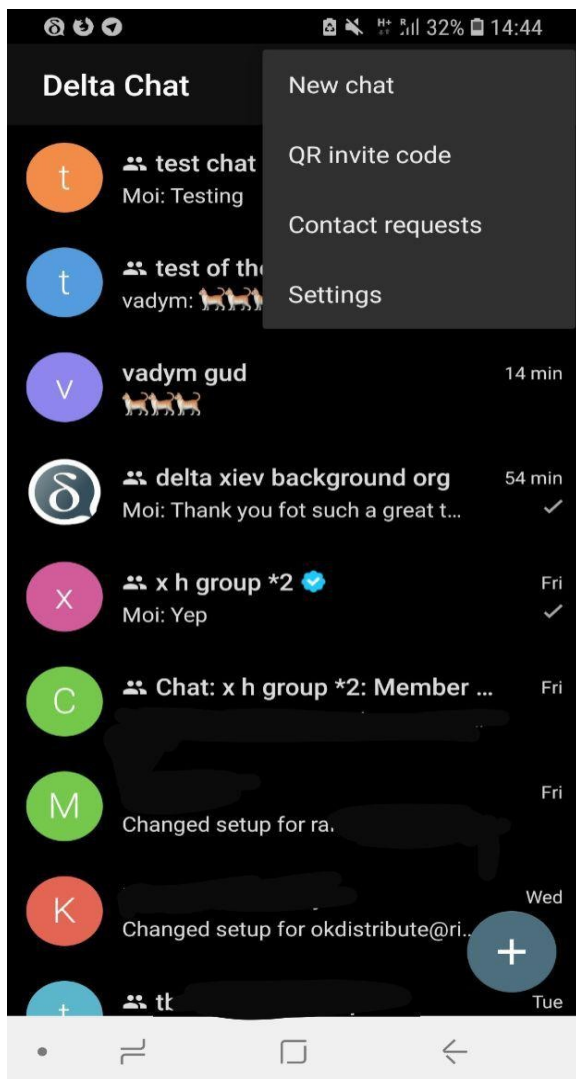
When asked to send a new message to one of our test accounts, several users tried to get there **using the “plus” button**. They were confused to see only the two options “new group” and “new verified group” there. Given that “new chat” is commonplace in most messengers, these expectations are understandable.

Some users said they would like to be able to chat with a person without creating a new contact. This may be a security feature for those who want to send just a few messages without adding metadata and leaving traces of a contact on their device. This may come from the more general “fear of the contact book” and the centralization of social graph that is attributed to it. It may also come from Signal experiences: during Rennes usability testing that happened on February 8, 2019<sup>2</sup>, regular Signal users said they did not like to “merge” their phone contact book with Signal contacts.

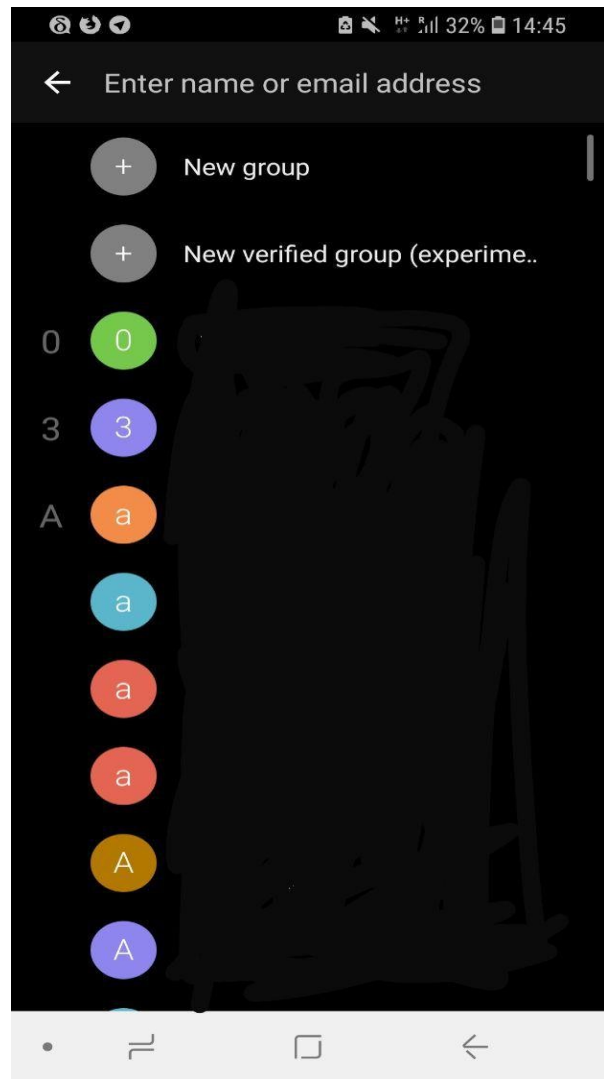
## **Recommendations**

- Explain that Delta Chat does not actually need access to the phone’s address book and has its own contact book; If possible, give a user a way to write a message without adding an email to the contact list;
- Think of a workaround for the “delivery notification” in case of a wrong recipient;
- Rethink the paradigm “contacts / new chats” [what is shown first to the user?] Maybe show a “speech bubble” instead of “+”;
- Adding a “new chat” option directly under the “plus” button (see screenshot 2) is a good option, as this path seems to be quite expected. Currently there is a way to start a new chat using this, but it is three steps away from the initial “plus” button screen.

2 We have conducted a Delta Chat usability session at the Transcyberian cryptoparty during the Festival of Digital Freedoms in Rennes, on February 9, 2019. See: <https://fdln.insa-rennes.fr/simaginer/soiree-transcyberien-bring-back-the-party-into-cryptoparty/>



Screenshot 1: Current way to start a new chat under "three dots" menu - v 0.101.0



Screenshot 2: Current options under the "+" button. It could be good to put "New Chat" directly here.

## Message delivery, deletion and encryption

Users at the smaller Rennes UX workshop (Feb 2019) expressed strong critiques of the default start message. They were concerned with the phrase "some messages may be sent unencrypted" and said they would prefer to have more exact information about this, for example, explaining that the first message will be unencrypted, as encryption will begin with the second. They also wanted to see warning signs if a message is sent unencrypted ("like it is in Riot.im").

Users said it was unclear for them if messages were deleted on the other side as well, saying they did not understand the "deleted on the server" message, and it "looked like Viber, that deletes from everywhere":

*"I do not understand if it is just me who does not have the message when I delete it. Or all participants. It is very important, if I want it to be like OTR. It is*



*so important for me that I would base my choice of a messenger on that” [a tester]*

Users noticed that it was unclear why they had to press for a long time on the message to delete it, saying this would not be very usable in case of mobility. Also, users could not figure out how to forward a message from one chat to another, with almost everyone reporting errors. Finally, users indicated that they would like the ability to edit messages.

### **Recommendations:**

- Improve wording about encryption in the default start message; create a UI sign for “unencrypted”;
- Add a comprehensive section on message deletion and storage in the FAQ and in the app itself; e.g. consider using the wording of WhatsApp, which uses these Delete options: “Delete for All” / “Delete for me” / “Cancel”.

### Sharing, forwarding, creating and deleting media files :

Users did not have particular problems with sending attachments through Delta Chat, or taking a new photo from within the app. While during the Kyiv usability testing several users encountered errors when trying to share an image from their Gallery or forwarding images from one chat to another, during our subsequent internal tests with different providers, we got no errors for these actions (versions v.0.101.1 and v.0.97.1) and can consider this as fixed.

When users wanted to delete a photo taken from within Delta Chat, they could not find it in their gallery (they were expecting a separate “Delta Chat” folder, as it is for Telegram for example). Some users underlined that it was good feature. Users liked that the app was asking if they wanted to save pictures to the device memory, as they reported sometimes saving pictures accidentally when using other apps, which they felt was not secure. However, users found it was hard to save images because they had to open them fully.

Users said they would like to be aware of the consequences of giving Delta Chat access to their camera and gallery.

### **Recommendations:**

- Add the ability to save from the preview. Add the ability to choose where to save;
- Add explanation that Delta only stores media files locally and has no own centralized server;

## Task 2 – Group chat

### Group chat creation and contact management

While the majority of users did not have problems with creating a new chat, some aspects of group chat creation were criticized: some users tried to create a group chat using the “three dots” on the right top of the screen instead of the plus button on the bottom. A user said that,

when clicking on the name of the chat, they were expecting to see list of chat members, but they saw settings instead.

Adding a new chat member was not clear for the majority of the users. Many users noticed one had to take a step back when adding a new member to the group instead of the usual “Ok” or “Done”. Some users said they did not understand where to look for the list of members. Some said they found it weird that they were not in the list of group chat members. Filtering of contacts was missing, and users were confused to see contacts from their phone book among Delta Chat contacts.

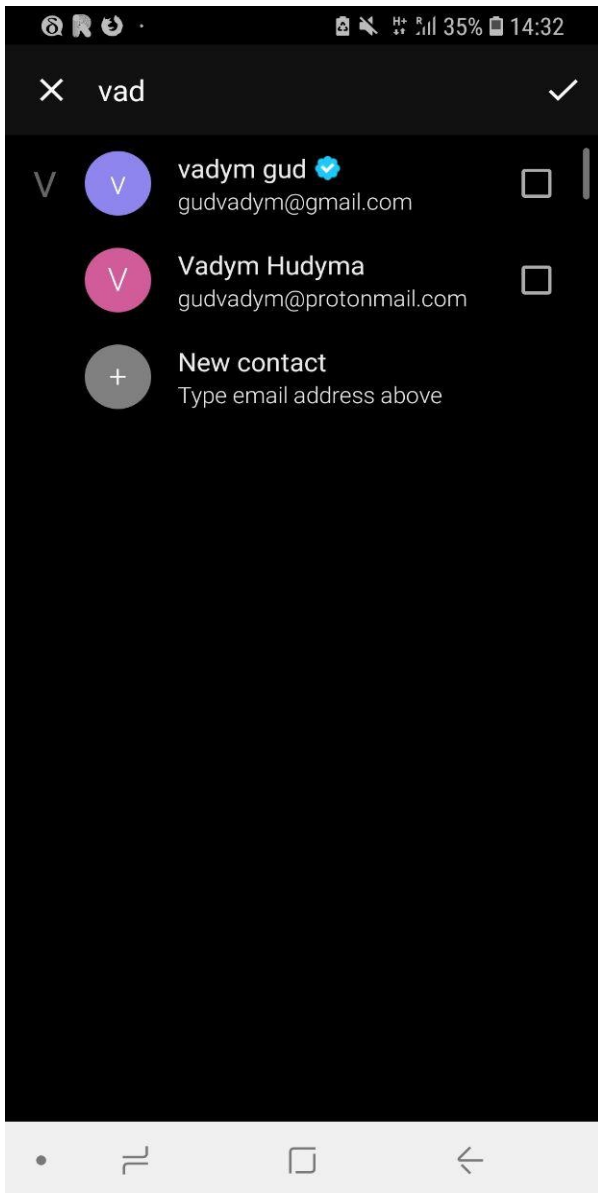
Sharing and forwarding images from the gallery caused a few errors. However, the tests conducted by us internally with the v0.97.1 and v.0.101.1 did not show these errors anymore.

Users requested an easier way to switch between group chats and one-to-one chats.

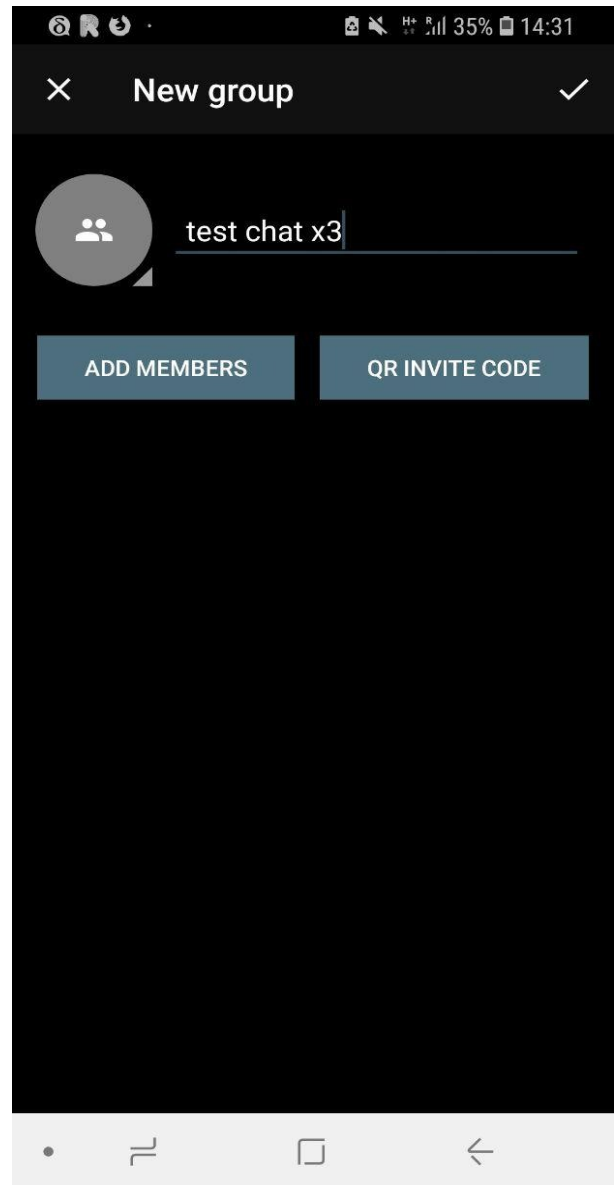
### **Recommendations:**

- Streamline the “add new member” feature;
- Rewrite the welcome message in the group chat, to more precisely communicate about encryption and risks of having some messages unencrypted;
- Devise a different organization of contacts;

**Progress notice:** In the v.0.100.1 the “add new member” process has become overall much easier. See screenshots:



*Screenshot 4: contact selection process for creating a new group. The tick in the right upper corner is added in the v.0.101.0 which makes the process much smoother.*

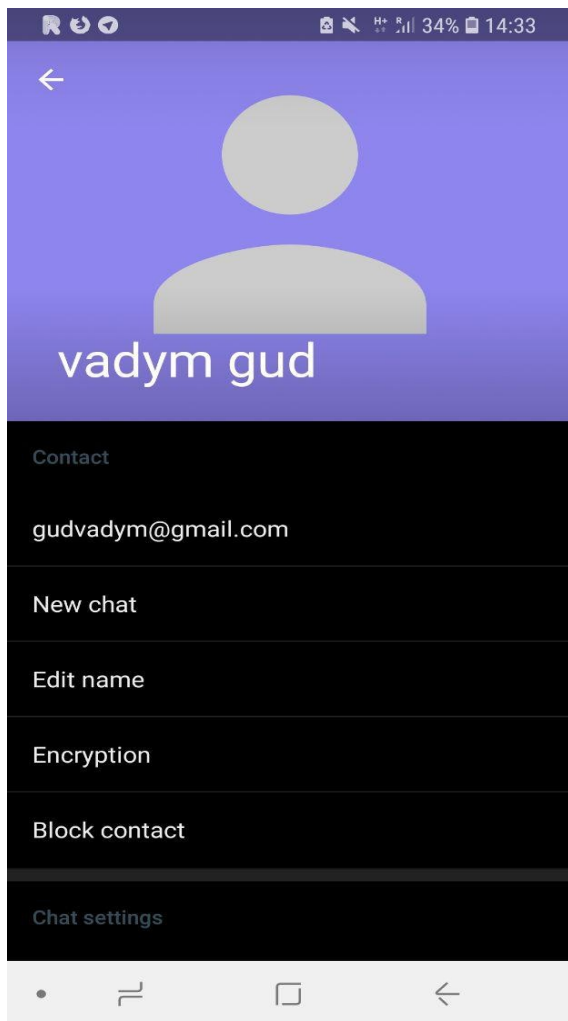


*Screenshot 5: The “new group” process has become easier with the “Add members” / QR Invite code buttons.*

- Users recommended a path to switch from group chat to 1-to-1 by clicking on the icon to go to the “profile of the contact” to start chatting.

**Progress notice:** This was implemented in the v.0.101.0 (see screenshot 6). However, the

UI could be made more explicit (e.g. the clickable elements, such as “New chat” may be visually different from the “contact information” such as the email address).



*Screenshot 6: “Contact profile” page under v.0.101.0 - the “new chat” option could be accentuated as a “button”.*

## Deleting members and chats, leaving chats

When removing members from group chats some users took the wrong path, and tried to click on the “two people” icon on the top right of the chat screen. Other users suggested that an easier way to delete members would be to click on the contact’s circle userpic. In v.0.101.0 and above it is already possible to “block contact” via this path, but not to remove it from a group chat.

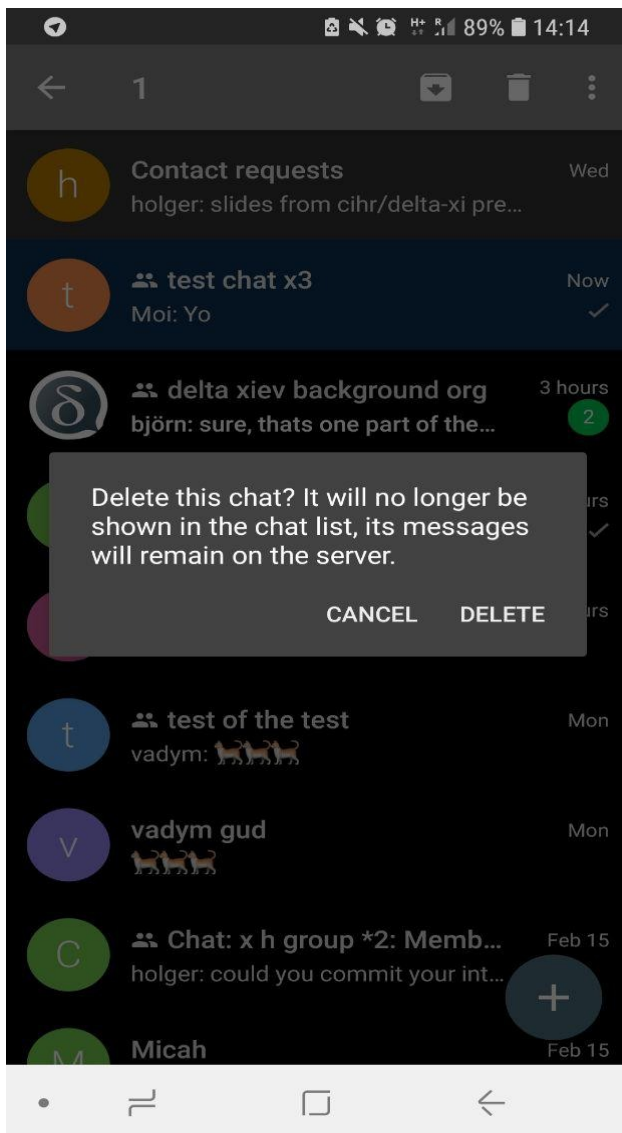
Users also requested a warning question: “Do you really want to delete this member from the group chat?” because they said they could do it accidentally. It was unclear to users about who had the rights to remove participants. Other users reported that after deleting a member they saw 4 members in total, but other group chat participants still saw 5.

Users were really confused with the fact that the chat continued to exist after they deleted it, even when they were themselves the chat’s creator. Many users reported continuing to receive messages after having left a chat. Users also found it weird to still see the group chat in their list of chats after having left it. For high-risk users it is important to underline the separation between “deletion” and “leaving” a group: in a situation of an arrest, a person may think that deleting a group chat would help stop receiving messages, however, other group members can continue sending messages that will arrive on the users’ device, even though the previous history of the deleted chat will not be accessible anymore.

**Progress notice:** In the version v.0.101.0 deleting a group removes it from your client. When a member sends a message in the deleted group, a user can still get it, however all the previous history is cleared.

### **Recommendations:**

- Add a new path for deleting members by clicking on the contact’s circle userpic;
- Add a warning question “Do you really want to delete this member from the group chat?”
- Add security reminder as a message after chat deletion: “You may still access the group messages and content. If you deleted this chat for security reasons, we recommend you also "leave group chat";



Screenshot 7: Deletion notification message. We suggest to rephrase it giving the user a choice to “clear messages” or “leave chat and clear messages”.

## Task 3 - Verification and verified group chat

### Meaning of verification

There was a lot of confusion around the meaning of “verification”, as well as about the verification process itself. It appears that users understand verification as a social event, not as device or account verification in itself. For example, one user interpreted the task to “verify your neighbour” in terms of social verification: he asked his neighbour to give his email address and confirm it was genuinely his email.

### QR code scanning

Many users found face-to-face QR verification as the only verification method to be too restrictive. The test showed that it limits access to verified groups for users with bad or damaged cameras. Some users said that they would like to have a remote verification process, specifically for situations where face-to-face meeting was out of the question.

#### **Progress notice:**

Under the v0.101.0 users have the ability to access “fingerprints” of their contacts under “contact’s profile → encryption”, so potentially comparing fingerprints in a more traditional way could be another solution to “verify” a contact. However, this path is not obvious and sends us back to the traditional key-based verification process, which may differ from Delta Chat’s main paradigm.

There was also a lot of confusion around placement of verification action buttons (“Scan QR code”/“Show QR verification code”). Users generally expected them to be on the same page or menu.

#### **Progress notice:**

In v0.101.0 the QR-code invite is also placed under “New group” which is very convenient (see screenshot 5 above).

Many users were confused that verification required verification from both parties and was not a one-way action. We may want to look either for a technical solution or just add some “action required” message after verification is completed.

Some users search for this feature on the “View profile” page or by tapping on the profile icon in “contacts”, which also suggests that the verification process is expected to be connected to a profile in the UI.

Currently while the verification is being executed, users see a message saying “Please wait”. It would be good to modify this phrase, adding an explanation: e.g. “Verification is in process, please wait”.

#### **Recommendations**

- In order to solve the problem of inability to scan QR code, some other way of

verification should be introduced. Manual entry could be a good solution, as well as ability to easily share or copy+paste it in case some at-distance verification is needed;

- Users proposed to have a “secret question” to be able to verify a person remotely.
- We would suggest to have both verification action buttons (“Scan QR code”/“Show QR verify code”) placed somewhere near each other. Also naming of the “Scan QR code” button should be changed into something suggesting its connection to a verification process and should be more consistent - for example “Scan QR verify code”.
- Generally, changing the wording around verification is something to think about further;
- Verification needs either streamlining or an onboarding process for new users. One of the tools that could be used for that is a visual / short comic illustration that can be included in the FAQ and in a dedicated blog post.
- We might want to add more detailed information about verified groups in the FAQ that currently refers only to a rather complex technical documentation [[“CounterMITM”](#)];

## Verified Group Creation

Users mentioned that the difference between regular and verified group chats was not clear UI-wise. They also expressed a very strong need for a clear separation between contacts that had been verified by them and other contacts in the verified group chat.

Many users expressed their dissatisfaction with a very long verification process and no feedback during the waiting process, as well as the lack of a ‘success’ message after verification succeeded.

During simultaneous verification many users were stuck in an infinite verification loop because they were trying to verify someone who was already being verified by another member of the group.

Users were confused by the inability to forward messages from one verified chat to another. If this is expected behaviour, some clarification in the error messages is required.

The need to be able to delete messages on all devices involved in a given conversation was greatly amplified in a verified group setting, which was perceived as “more secure”.

## **Recommendations**

- Introduce clear UI separation between verified and unverified contacts as well as between contacts added by users themselves or through other verified contacts; Additional information about which contact verified this particular contact may be useful as well;
- Introduce better UI separation between normal group chats and verified group chats



(e.g. colour scheme change);

- Add a success message after verification is completed;
- Replace indeterminate spinning wheel with a determinate one as a progress indicator, or even go for a percentage bar if we're expecting this process to take more than 10 seconds on slower mobile phones or in situations with bad internet connection<sup>3</sup>.
- Consider adding a more explicit message (e.g. "Verification in process. Please wait" instead of just "Please wait"). The same concern was expressed for video uploads during testing in Rennes, France (to add the counter / progress indicator of the upload);
- The ability to sort and search through contacts based on their verification status may also be a useful feature;

## Task 4 - Backups, Import/export of the keys

Most users were extremely confused while trying to find the backup button. The overwhelming majority of users also failed to import the backup during the new login setup, as the text "Import backup" was very small and did not look to be clickable. Many users were also unsatisfied that there were no options for choosing where to save their backup. Some users said the language settings were not respected after importing a backup.

The majority of users were also confused that they were supposed to enter their secret (PIN, figure or password) from their device when exporting a backup (*"it's as if an external service has access to my device"*).

Exporting and importing keys was not always easy: not all users understood what "keys" actually were; some requested to have an option to choose the path where to save keys including an external device.

While Autocrypt setup wasn't specifically tested in this round of user-testing, some users were also confused about the specific role of "Autocrypt setup" and usage of this feature.

### **Recommendations:**

- Change the UI of the "Import backup" feature on the login screen: either to proactively ask users to search for a backup on a device or otherwise nudge users to import it, as it seems to be preferred behaviour in most cases;
- Creation of the backup also needs a more noticeable placement, either directly in Settings or even as a regular reminder to the user;
- Explanation of the limits of Delta Chat access to users' devices should be made more explicit in the FAQ and within the app itself, to limit confusion of users when they are asked to enter the PIN from their phone for exporting backups.

<sup>3</sup> See this research by the Nielsen Norman Group on "response time": <https://www.nngroup.com/articles/response-times-3-important-limits/>

- Option to save backups in user-defined locations should also be introduced, including external storages, both offline and online. This may be a useful addition, especially considering the use-case of device failure and quickly spreading usage of full-disk encryption on most modern mobile devices, which makes easy backup recovery impossible. In order to eliminate the associated risks of external storage, this may be an option for opt-in during the initial Delta Chat setup.

## Other feedback and requests

During the session users requested additional features and expressed other concerns. Everyone shared the need for ephemeral messaging and an auto-delete function. A human rights activist suggested the following features for her work:

- to create different conversations with the same person tagged by topics;
- to use a collaborative editor or easy access to something like a Google Doc or Google Drive;
- to have an additional password for verified groups.

Several users mentioned:

- a “broadcasting” function - the ability to select contacts by clicking on them and to send one message to all of them at once;
- an ability to hide Delta Chat under an icon that does not look like a messaging app;
- easily generated throw-away accounts for field missions;

Other needs expressed by users:

- the ability to delete chats by contact, in case one member of a chat is arrested;
- to click on a contact and delete all conversations with this person, including conversations from his or her phone;

Features that did not make sense to users:

- Most users do not need or do not understand the need for archiving conversations. It may make sense to drop this at some point or at least not invest much work in it.






It is interesting that users said they would expect a more specific UI, not a copy of Signal or Telegram. Some of them were expecting a new UI from a new messenger.

An interesting suggestion, that goes together with the general Delta Chat approach to inclusiveness, is to make the UI customizable for people with disabilities or particularities (e.g. left-handed). A left-handed tester suggested to have an opt-in ability to have his messages on the left side of the screen and incoming messages on the right side.






During a testing session in Rennes, France, we received suggestions on improving the FAQ section and putting it within the app. Currently the FAQ/help opens up in the default Android browser, even if users have set up Firefox or Chrome as their default browsers. Users expressed concerns with having to go online to search for FAQ/help, because they might be in a situation of bad connectivity and would like to be able to search through FAQ on their devices.

# Appendix: User reaction synthetic tables






## Task 1

Reactions						n/a
1. Create an account	1	1	4	1	4	1
2. Send a message to [test accounts]	4	4,5	0	2,5	1	0
3. Reply to received messages	6	2	2	2	1	0
4. Send existing image to [test accounts]	5	4	1	1	0	1
5. Save received image	4	1	4	1	3	0
6. Share the image with [test accounts]	0	2	1	4	5	0
7. Take a new photo with Delta Chat and send it to [test accounts]	4	4	3	0	0	1
8. Delete this photo	3	3	2	1	3	0






## Task 2

Reactions						n/a
1. Create a group chat with [test accounts]	2	3	1	3	0	3
2. Add [another test account] and one of your neighbors	2	7	1	2	0	0
3. Send a message to this group chat	7	5	0	0	0	0
4. Reply to received message	2	4	1	0	0	5
5. Delete member [test account] from the group chat	6	2	3	0	1	0
6. Leave the group	5	5	1	1	0	0

### Task 3

Reactions						n/a
1. Verify contact of 1 person next to you and [test account-1] or [test account-2]	0	2	3	3	5	1
2. Create a verified group	3	4	0	2,5	1,5	1
3. Start chatting	5	5	1	0	0	1
4. Delete a message	2	3	3	0	3	1
5. Archive any chat	5	3	2	0	0	1
6. Unarchive this chat	5	5	2	0	0	0
7. Delete any chat	6	4	1	0	1	0

## Task 4

Reactions						n/a
1. Create a backup of your chats	2	1	4	1	4	0
2. Export secret key	1	4	4	1	2	0
3. « Delete your account» - Delete the app data	3	4	0	0	1	4
4. Import backup	3	1	0	4	2	2
5. Import secret key	2	3	3	0	3	1
6. Start chatting	3	1	0	1	3	3