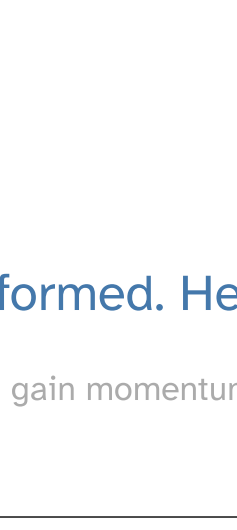


Everything You Think You Know About Delta Chat Is Wrong

Last updated on 2026-06-05

[#chat](#) [#delta](#) [#email](#) [#messaging](#) [#pgp](#) [#security](#)*I am smitten with Delta Chat...*

Delta Chat has been making massive strides lately and I think you should consider using it as your full time secure messenger.

"But Email..."

No, You Are Wrong

"PGP is ..."

Slow Down. You've Been Misinformed. Hear Me Out...

Whenever a Delta Chat discussion is about to gain momentum in a social forum there's always someone who has to step in and say something like

Armchair Expert

Actually, email is bad and this will never work so nobody should use it.

It keeps happening over and over.

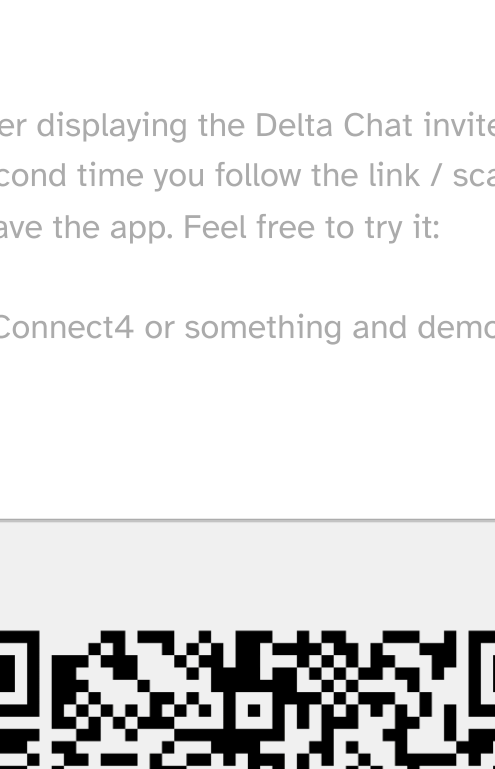
This blog post is commonly used to reinforce the position: [Stop Using Encrypted Email](#).

It's honestly a good blog post; metadata *is* as important as content.

Too bad none of that matters with Delta Chat + Chatmail. No user metadata is exposed. 🙄

Everybody Hates Email

In the technology world "email" is a four letter word that usually receives a negative reaction. It also soured my first impression. Nobody wants to make their email experience noisier than it already is.



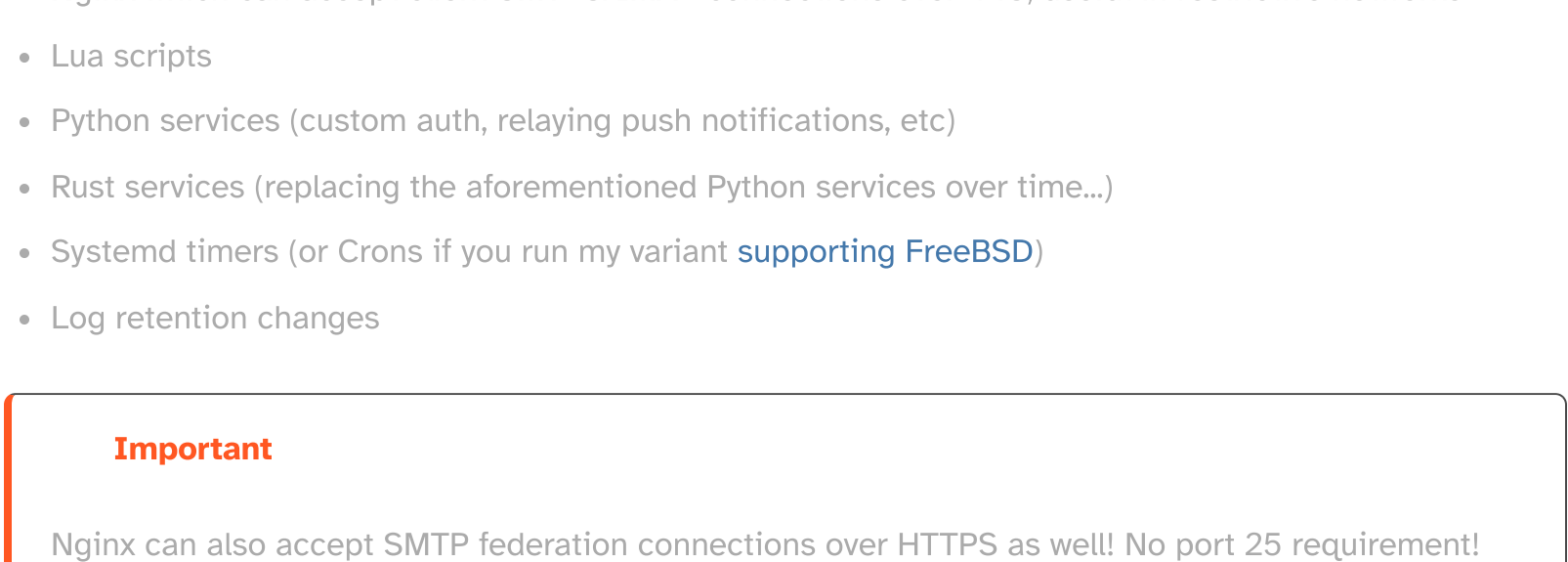
Repeat After Me

Nobody wants more email.

Agreed. So take a deep breath. You will not use your normal email address with Delta Chat. In fact, you should not even try unless there is no other possible way for you to use the software. If you want more technical details about this thing first before you even try it, [skip ahead](#).

Ok I'm Interested

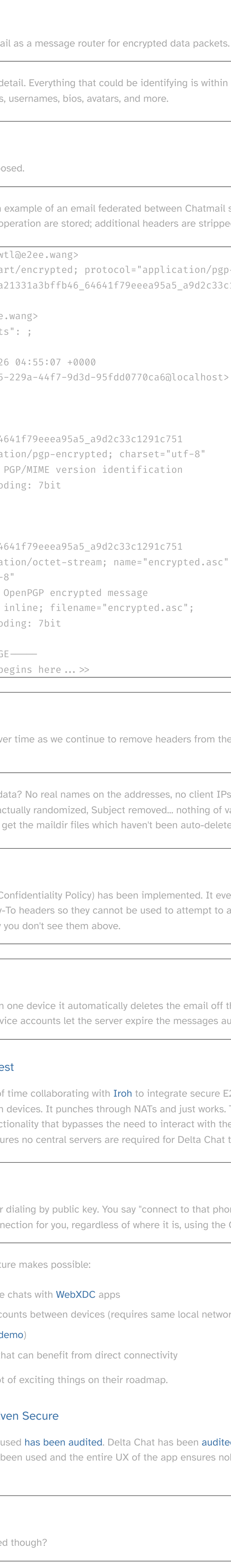
Cool. First time users will scan an invite QR code or follow the equivalent link ("Send me a message") I have shared below. The page will look like this:



This is what users see if they don't have Delta Chat installed yet. Users should open the app to create a profile before proceeding. They will not be asked to choose a username or password or 2FA. It's very simple.

Then users can return to their browser displaying the Delta Chat invite webpage and connect with the second Open Chat button. Or the second time you follow the link / scan the QR code it will connect users immediately because they already have the app. Feel free to try it:

[Send me a message](#), I'll play you in Connect4 or something and demo Delta Chat's features for you if I'm awake.



Chatmail Fixes Almost Everything...

Delta Chat developed a messaging-optimized email server stack called **Chatmail**. Anyone can deploy a Chatmail server. But what is it exactly?

- Dovecot, **patched** to reduce latency on deliveries (long story, old hack, never should have existed)
- Postfix (requires TLSv1.3 for submission, >=TLSv1.2 for federation)
- DKIM
- Nginx which can accept client SMTPS/IMAP connections over 443, useful in restrictive networks
- Lua scripts
- Python services (custom auth, relaying push notifications, etc)
- Rust services (replacing the aforementioned Python services over time...)
- Systemd timers (or Crons if you run my variant [supporting FreeBSD](#))
- Log retention changes

Important

Nginx can also accept SMTP federation connections over HTTPS as well! No port 25 requirement! This is very alpha but it's live on some servers and of course would require all Chatmail servers to support it to completely ditch normal port 25 federation.

That's about it, but the devil is in the details.

The services have very specific configurations which eliminate the need for spam filtering because the accounts are not enumerable and Chatmail to Chatmail is always going to be encrypted: users cannot send unencrypted emails.

Note

No Spam filtering required. Users cannot send unencrypted emails.

You can run a Chatmail server anywhere. You do not have to worry about having a "clean" IP address: none of the Chatmail servers are going to check your reputation. Message deliveries generally happen in well over a second, so it's just as fast as any other messenger. If you want, you can run a server and never open port 25 to achieve a private non-federating Delta Chat server. This is a completely valid use case.

Hint

Delta Chat only uses email as a message router for encrypted data packets.

This is the most important detail. Everything that could be identifying is within the encrypted data: the chat subject, group chat IDs, usernames, bios, avatars, and more.

Important

No user metadata is exposed.

Don't believe me? Here's an example of an email federated between Chatmail servers. Before the MIME headers required for basic operation are stored; additional headers are stripped right after storage.

```
Return-Path: <1tmgk6wtl@e2ee.wang>
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
    boundary="18a21331a3bffb46_64641f79eeea95a5_a9d2c33c1291c751"
MIME-Version: 1.0
From: <1tmgk6wtl@e2ee.wang>
To: "hidden-recipients";
Subject: [ ... ]
Date: Mon, 30 Mar 2026 04:55:07 +0000
Message-ID: <b2ee6b55-229a-44f7-9d3d-95fdd0770ca6@localhost>
Chat-Version: 1.0

--18a21331a3bffb46_64641f79eeea95a5_a9d2c33c1291c751
Content-Type: application/pgp-encrypted; charset="utf-8"
Content-Description: PGP/MIME version identification
Content-Transfer-Encoding: 7bit

Version: 1

--18a21331a3bffb46_64641f79eeea95a5_a9d2c33c1291c751
Content-Type: application/octet-stream; name="encrypted.asc";
    charset="utf-8"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc";
Content-Transfer-Encoding: 7bit

-----BEGIN PGP MESSAGE-----
<< encrypted base64 begins here... >>
```

Note

I update this example over time as we continue to remove headers from the Chatmail relay server storage.

Where's the sensitive metadata? No real names on the addresses, no client IPs. Received and DKIM headers scrubbed, Date is actually randomized, Subject removed... nothing of value here. Go ahead and seize the server, they'll only get the maildir files which haven't been auto-deleted yet and no useful logs.

Attention!

RFC9788 HCP (Header Confidentiality Policy) has been implemented. It even protects the References and In-Reply-To headers so they cannot be used to attempt to associate messages by thread/group. That's why you don't see them above.

Tip

If your account is only on one device it automatically deletes the email off the server after downloading it. Multi-device accounts let the server expire the messages automatically.

... And Iroh Fixes The Rest

Delta Chat has spent a lot of time collaborating with **Iroh** to integrate secure E2EE P2P communications between users and your own devices. It punches through NATs and just works. The Iroh connection can then be used for lots of functionality that bypasses the need to interact with the email servers. This is yet another innovation that ensures no central servers are required for Delta Chat to work.

How It Works

Iroh gives you an API for dialing by public key. You say "connect to that phone" and Iroh will find and maintain the fastest connection for you, regardless of where it is, using the QUIC protocol.

Examples of things this feature makes possible:

- Realtime P2P apps in the chats with [WebXDC](#) apps
 - Securely transferring accounts between devices (requires same local network for security purposes)
 - Audio/Video calls ([tech demo](#))
 - Any future functionality that can benefit from direct connectivity
- The team definitely has a lot of exciting things on their roadmap.

But I Heard PGP Isn't Even Secure

The **Rust PGP library** being used **has been audited**. Delta Chat has been **audited multiple times**. A very specific subset of PGP has been used and the entire UX of the app ensures nobody has to be aware of PGP.

Curious User

What crypto is being used though?

Currently it's using the same base cryptography implementation that Signal uses (ed25519-dalek Rust crate). Delta Chat generates an Ed25519/Curve25519 identity key and encryption subkeys. The symmetric cipher used for session keys is AES-128.

Curious User

Does it have Perfect Forward Secrecy and PQC encryption?

Not at this time for normal messaging. Both the TLS connections between client/server, server/server federation, and when using Iroh are protected with PFS, but the messages themselves are not. The term "Perfect Forward Secrecy" is a confusing way to describe the desired functionality. The Delta Chat team prefers to call this "Reliable Deletion". Signal users did not have PFS / Reliable Deletion on iOS until **iOS 26.4.2**, so even Signal users were not truly protected. As you can imagine, this is a very difficult problem due to how complicated our OSes and devices are.

Important

2026 update: PFS and PQC are coming soon! The Delta Chat team announced **AutoCrypt v2** at FOSDEM.

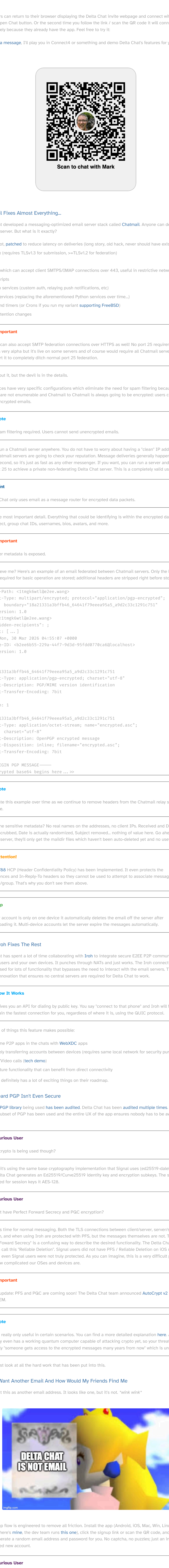
Note

PFS is really only useful in certain scenarios. You can find a more detailed explanation [here](#). Also nobody even has a working quantum computer capable of attacking crypto yet, so your threat model is really "someone gets access to the encrypted messages many years from now" which is unlikely.

Please, just look at all the hard work that has been put into this.

I Don't Want Another Email And How Would My Friends Find Me

Don't treat this as another email address. It looks like one, but it's not. *"wink wink"*



The signup flow is engineered to remove all friction. Install the app (Android, iOS, Mac, Win, Linux), choose a server (here's [mine](#), the dev team runs [this one](#)), click the signup link or scan the QR code, and that's it. It will generate a random email address and password for you. No captcha, no puzzles; just an instantly provisioned new account.

Curious User

Wait, instant anonymous email accounts?

Ok, so this is where things get confusing for people.

Chatmail servers offer free, instant email address signup. The mechanism is literally "try to login with a random email address and password" and if the account doesn't exist it's registered immediately. This is done through the aforementioned custom auth integration with Dovecot.

Curious User

That's terrible, you're basically creating an open relay and we suffered from enough spam due to those.

Remember, you can't send an email that isn't encrypted. Spammers don't send encrypted mails. This is completely useless to them.

Curious User

I won't even know my own account details?

You never really need to know what it is. If you want, you can find the address and password in the app settings.

Now that you have an account, use your invite QR code or link and send it to your friends however you want: regular email, SMS, another chat platform, print it on a postcard. All they have to do is click the link or scan the code. They'll be prompted to install the app if they don't have it, but then they'll instantly be connected to you as a contact. You can even share a link or QR code to a group chat.

Please try it. And if you have more questions about the security or operation of the app, how push notifications work securely and anonymously, etc read the very extensive [FAQ](#).

Alternative Clients?

Delta Chat has done a wonderful job of building a robust cross-platform library in Rust which enables them to deliver the same functionality on each platform. You get the same quality experience on all of the supported OSes so there is no worry about which clients support which features. One alternative client for Android is [ArcaneChat](#), which uses the same **core** as the official Delta Chat app.

You can find additional information about alternative clients [on this page](#).

Really -- Why Email?

Inventing a new protocol for instant messaging is a lot of work. XMPP could be great, but it's very fragmented. Everything needed to build a secure messaging system on top of email already existed, and we know the existing software scales and is battle hardened from years of deployment.

There are also certain benefits of using email: it's harder for a country to block it if they want to prohibit secure messengers that do not have mandatory backdoors. They'd have to block all known Chatmail servers, but new ones can be deployed very quickly. You can also add new relays (email addresses) in your settings -- using a completely different new Chatmail server -- and your contacts will instantly update the address they use to reach you as soon as they receive your first message because your key did not change. This is a feature called **AEAP** - Advanced Email Address Porting. There has been discussion about the possibility of auto-rotating your identity which I feel is a powerful concept that will have a huge impact on privacy tools for the masses.

Does It Have My Favorite Messenger Features?

I hope so. Maybe the biggest limitation right now is that sharing large media files (~ > 32MB) is not well supported -- you may have to use one of the large-file-transfer web services unless your relay has increased the max message sizes.

- Group chats
- Broadcast groups (like Telegram channels)
- Inline attachments (audio/video)
- Voice messages
- Location sharing (edit: being reworked, but you can share location and there is a map to view)
- Very good support for multiple accounts/profiles
- Search (tested with accounts that have 400k+ messages, works fast)
- Disappearing messages
- Notification muting
- Presence (only sorta; more like a "recently seen")
- Very friendly on unreliable networks
- Custom chat backgrounds
- Invite links/codes can be deactivated/regenerated
- Contact sharing (to introduce users to each other securely)
- Message editing
- Deletes which happen across all your devices / "delete for everyone"
- Multiple relays (servers/chatmail addresses) can be attached to an account. Your contacts will recognize you from your PGP public key automatically and learn your new address
- Audio/Video calls via WebRTC, not Iroh at this time (beta, available on Desktop, Android and iOS -- working well though!)

Note

Markdown was previously mentioned, but it was first added to Desktop and has been removed as a new cross-platform text renderer is being designed. It should be functional with ArcaneChat on Android, though.

What Aren't You Telling Me?

There are a few shortcomings coming from other messengers. Some of these missing features are in the core and will be released soon. But a few things I think people should be aware of at time of writing:

- When you use your account on multiple devices, there isn't a way to revoke access right now. Be mindful about this.
- Groups are meant to be between people you can trust as they do not have ACLs yet. Anyone can add or remove anyone else, change the group name/subject, avatar.
- Joining a group chat shows no history, so it can look dead/empty
- Link previews do not exist (yet)
- No typing notifications (definitely possible with Iroh, but some people consider this an anti-feature anyway)

How Can I Contribute?

You can **contribute** code, translations, help support the community on the forum, or even run a Chatmail server (it's really cheap and low resource!). You can also **help fund the dev team** making this possible.

Corrections AKA Some Things I Thought I Knew Were Wrong

A few details escaped review:

- Location sharing isn't P2P/realtime as it is intended to be stateful and needs to work reliably if the other users receiving them have multiple devices or intermittent network connectivity. They are broadcast once every 60 seconds using the normal SMTP transport if the location has not changed since last transmission.

State syncing is also utilising SMTP for similar reasons as a device could be offline for days at a time. Having a reliable channel to communicate the state is important. It could use Iroh when they're known to be online, and this is being explored.

SPF records are encouraged for compatibility with classic email servers, but Chatmail does not validate SPF.

Published by feld on 2025-03-07

[« Delta Chat Bots Made Easy](#)

[ACME HTTP-01 for a Cluster of Web Servers »](#)