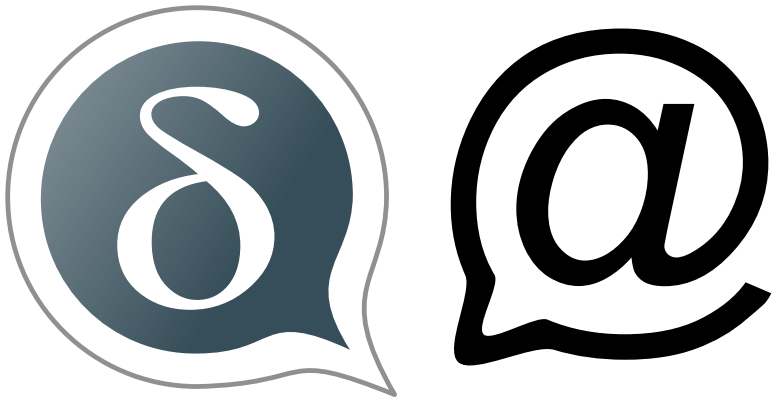
Usable end-to-end security with Delta Chat and Chatmail



holger krekel (he/they)

Usable security

- Measuring by actual security outcomes (not protocols!)
- Any security oriented feature requires UX/UI first
- Assume Dialogues/Warnings/Icons are ignored

Overview on security in this talk

- Chatmail relays (message transport)
- Delta Chat apps (multi-device end points)

Discussion/questions tomorrow during long morning session

Classic email providers 🤒

- Users need to know address and password
- Personal data needed for address registration
- Providers store and transmit cleartext messages
- Rate limits not suitable for chatting
- Slow and unreliable because of spam checking
- No mobile push notifications
- gmail/outlook/apple/… gatekeeping/tracking/processing

insecure, cumbersome, expensive to operate

Self-hosted email provider 😯

- Better privacy
- No push notifications (could be done, needs work)
- Mixing cleartext/e2ee is detrimental to usable security outcomes
- **Limits of cleartext interoperability** (Gmail/Outlook/Gmx/... Gatekeeping)

Chatmail relays rely on cryptographic security 🤩

- Strict TLS and DKIM enforced
- E2E-encryption enforced: cleartext messages/subjects rejected
- Reliable: No Spam-checking or IP reputation magic

Chatmail Relays are for ephemeral message transport

- Ad-hoc: login to get and use a (random) address
- Ephemeral: messages removed after download from client(s)
- Address is removed after <configurable> days without login

Chatmail Relays are near-zero-state

If a chatmail relay VPS is catastrophically lost:

- point DNS to a new VPS, setup again
- voila :) previous users can continue to chat

Chatmail Relays have near-zero cost

- Relays unconditionally forget messages
- Relays are cryptographically interoperable with other relays (and well-behaving classic servers)
- After setup it's near-zero per month maintenance cost
- RasPi or Cheapest VPS can serve some 1000's of users

Yearly costs all citizens of France: ~66.6K EUR (0.1 cent per user)

Delta Chat end-point security: Usability

- Instant onboarding with chatmail relays enforces E2EE
- Strict TLS by default, autodiscover of provider addresses/ports
- Automatic key management and verification
- **No questions about keys**

Delta Chat end-point security: Protocols

- Strict TLS between apps and servers by default
- Autocrypt 1.1 (key spec + automatic in-band address/key binding)
- SecureJoin (Out-of-band security against network/MITM attacks)
- Metadata minimization / IETF "Header Protection" draft

Delta Chat end-point security: Implementation

Apps and bots use async "chatmail core" Rust library which implements:

- all cryptography (rPGP, RustCrypto etc.)
- networking and message transport,
- contact, group, message, blob etc. management
- a statically linked binary speaking Json-RPC via stdin/stdout

OpenPGP implementation: rPGP

- Full-rust implementation of OpenPGP RFC 9580
- Never had any of the "another vulnerability" gpg-related issues
- Security audited (last in 2025)
- Using same ed25519-signing code as Signal
- rPGP has community traction outside Delta Chat usage

Wire-Interoperable cryptography matters!

Delta Chat metadata seen on transport layer

- Sender
- Recipients
- Date
- Autocrypt header with PGP public key

R&D security/resilience NEXT STEPS

- Don't leak cryptographic identity to transport layer
- "Sealed Sender" (unauthenticated sending)
- Multiple transport addresses for chat profiles
- Migrate to OpenPGP V6 and PQC
- "Remote-wipe" feature to mitigate device-seizure
- "Forward Secrecy" to mitigate hostile servers

Thursday morning session for details

Delta Chat usable security changes in July releases

- **Chat Identity based on cryptography, not email address**
- Chats remains E2EE forever, can never drop back to cleartext
- E2EE messages get no icon (cleartext chats/messages are marked)

Webxdc apps

- webxdc apps are zip files, containing all assets
- can be attached and started in any chat
- can not access the internet, use end-to-end messaging only
- Delta integrates Iroh P2P library for realtime channels
- "Live Chat" app offers strictly ephemeral chatting with PFS

Links

- https://github.com/chatmail/
- https://github.com/deltachat/
- https://github.com/rpgp/rpgp
- https://securejoin.delta.chat

See you tomorrow at the morning session or elsewhere!