

ENIGMA 3

Deine Nachrichten. Dein Server. Niemand sonst.

Über 60 Millionen Nachrichten wurden von jemand anderem gelesen. EncroChat, Sky ECC und ANOM haben bewiesen, woran es liegt — nicht an der Verschlüsselung, am **Betreiber**. Enigma 3 zieht ihn aus dem Bild: Ihre Nachrichten, Ihr Server, niemand sonst. Durchgehend Ende-zu-Ende verschlüsselt — kein Konzern, keine Cloud, keine Telemetrie.

🔒 Ende-zu-Ende verschlüsselt

🏠 100 % selbst gehostet

⏱️ Selbstlöschende Nachrichten

📞 Verschlüsselte Anrufe

🖥️ Windows · Linux · Android · Web

WARUM ENIGMA 3

— Vertrauen Sie niemandem. Am wenigsten einem Anbieter.

Drei „abhörsichere" Dienste der Welt sind an einem einzigen Punkt gescheitert — nicht an der Verschlüsselung, am Betreiber. Die Zahlen stammen aus offiziellen Europol-, Eurojust- und Staatsanwaltschaftsmeldungen.

ENCROCHAT · 2020

60 Mio.

gelesene Nachrichten · 700 Mio. € beschlagnahmt · **6.500+ Festnahmen**

60.000 Geräte, verkauft als „absolut abhörsicher". Die Polizei musste keine Kryptografie knacken: Über das **Update-Programm des Anbieters** erhielt jedes Gerät einen Späher. Die Nutzer wussten nicht, dass ihre Gespräche jahrelang mitliefen — bis die Ermittler sie längst lasen.

SKY ECC · 2021

700 Mio. €

beschlagnahmt · Dutzende Festnahmen auf drei Kontinenten

Server in Frankreich und Kanada beschlagnahmt, Gründer verhaftet. Der entscheidende Unterschied zu EncroChat: **Der Anbieter hielt die Schlüssel selbst** — und gab sie an die Behörden heraus. Ein „sicheres" System, dessen Hersteller mitsamt Schlüsselbuch aushilfsbereit ist.

ANOM · 2021

300+

Verurteilungen · 40 Tonnen Drogen sichergestellt

Kein Fehler, kein Hack — **das Produkt war die Ermittlung**. Im Rahmen der Operation Trojan Shield, verdeckt vom FBI, lief zwei Jahre lang jede Nachricht über Server, die Ermittlern gehörten. Wer ANOM kauft, kauft keinen Schutz — er mietet eine Beweismittelmaschine.

Der gemeinsame Fehler: Nie war die Verschlüsselung schuld — **immer der Betreiber.** Wer den Server hält, hält die Schlüssel, ohne ein einziges Verfahren zu brechen.

Der Alltag, verglichen

	WhatsApp	Telegram	Signal	ENIGMA 3
Server gehört	Meta	dem Anbieter	Foundation (USA)	**Ihnen**
Inhalte liest	Anbieter (optional Backup)	Anbieter (bei „Cloud-Chats“)	niemand — außer eigenen Backups	**niemandem**
Metadaten	bei Meta	beim Anbieter	bei Signal, minimiert	**auf Ihrer Hardware**
Identität	Telefonnummer	Telefonnummer oder Nutzername	Telefonnummer Pflicht	**Nutzername, ohne Telefonzwang**
Kündigung	Anbieter löscht Ihre Daten	Anbieter löscht Ihre Daten	löscht nach 30 Tagen Inaktivität	**Sie sind der Betreiber**

Das Prinzip: Enigma 3 hat keine Herstellerinstanz zum Übernehmen, kein Update-Programm zum Missbrauchen, keine Schlüssel bei jemand anderem. Die Beschlagnahme, die bei EncroChat alles war, ist hier die leere Festplatte.

WAS KOSTET VERTRAUEN

— Privatsphäre hat einen Preis — ehrliche Zahlen

	WHATSAPP / TELEGRAM	TEAMS / SLACK	ENIGMA 3
Was Sie zahlen	0 € — mit Ihren Daten, Ihrer Reichweite, Ihren Gewohnheiten	Abo pro Person und Monat	**Einmalig: ein eigener Server. Kein Abo, keine Gebühr pro Person.**
Wem der Server gehört	dem Anbieter	dem Anbieter	**Ihnen**
Wer die Inhalte liest	der Anbieter — wann immer er will	der Anbieter — wann immer er will	**niemandem. Nur Ihre Geräte.**
Metadaten	beim Anbieter, mit Klarnamen	beim Anbieter, mit Klarnamen	**bei Ihnen — der Server sieht nur, wer wann mit wem schreibt.**
Wenn der Zugang streikt	weg — der Anbieter entscheidet	weg — der Anbieter entscheidet	**Sie entscheiden. Immer.**

🤝 Ihr Betreiber — ohne Vertrauenslücke

Aufsetzen, Updates und Backups übernimmt Ihr Betreiber — Sie chatten einfach. Und hier steht die Garantie, die es sicher macht: **Selbst der Betreiber kann keine einzige Nachricht, keinen Schlüssel, kein Passwort lesen.** Er kann es technisch nicht — die Schlüssel liegen auf Ihren Geräten, der Server sieht nur Chiffretext. Was er sieht, ist die Verbindung, nie der Inhalt.

📜 Datenschutz, den Sie Behörden zeigen können

Serverhoheit bei Ihnen, Auftragsverarbeitung selbst geregelt, keine Datenübertragung ins Ausland, keine Konzern-AGB, die Sie nicht steuern. **DSGVO ist hier kein Versprechen — sie ist die Bauart.** Und Sie können jederzeit weg: Server platt machen, Schlüssel zerstören, nichts bleibt. Kein Lock-in.

SO LIEST SICH DAS IM ALLTAG

Drei Gruppen. Drei gute Gründe.

👨‍👩‍👧 Die Familiengruppe

Enkelbilder, Urlaub, die schweren Gespräche — sie bleiben im eigenen Archiv des Hauses. Nicht gelesen, nicht für Werbung, nicht „nur zur Zustellung". Der Server gehört zum Haus, nicht zum Konzern.

💼 Die Firma

Projekte, Angebote, Kalkulationen — auf einem Server, den ein Mensch übersieht, statt in einer Cloud, deren Backup bei anderen Firmen landet. Vertraulich heißt hier: **bei Ihnen** — nicht bei einer Datenschutz-Zentrale, die im Zweifel zustimmt.

⚖️ Vertrauliche Arbeit

Praxis, Redaktion, Verein, Gewerbe — wer Geheimnis wahrt, lagert nicht aus. Bei Enigma 3 entscheidet nur Ihr Server, wer etwas lesen kann. Und der Server steht bei Ihnen, nicht bei Meta, nicht bei Microsoft, nicht bei einem Rechenzentrum, dessen Kundenliste Sie nicht kennen.

Was eine Beschlagnahme bringt

🔒 Der Tag, an dem die Polizei kommt

Angenommen, Ihr Server wird beschlagnahmt — morgen, ohne Vorwarnung. Was dabei auf dem Tisch liegt: **Tabytes Chiffretext. Kein einziger gelesene Satz, kein Kanalname, kein Profilname, keine Reaktion.** Die Schlüssel liegen auf den Geräten, nicht auf dem Server — und weil der Server sie nie hatte, kann er sie auch nicht hergeben. Was bleibt, ist die nackte Verbindung: wer wann mit wem sprach. Was besprochen wurde: niemals.

Und die Geräte schweigen nicht: **neues Gerät, Passwort-Reset — jeder Vorfall alarmiert alle anderen Geräte des Kontos.** Wer nicht Sie war, wird mit „Das war nicht ich“ widerrufen. Ein Angreifer, der Ihr Konto übernehmen will, wird am selben Tag sichtbar. Genau umgekehrt war es bei EncroChat: Dort lasen es Tausende Beamte, ohne dass die Nutzer es merkten. Der Unterschied ist nicht Glück — es ist die Frage, wessen Server.

KRYPTOGRAFIE STATT VERTRAUEN

„Unknackbar“ — warum der Satz hier kein Marketing ist

Es gibt zwei Arten, Sicherheit zu verkaufen: eine, die man nachprüfen kann — und eine, die man glauben muss.

🧮 Die Mathematik

AES-256 hat **2^{256} mögliche Schlüssel** — mehr Varianten, als das Universum Teilchen hat. Ausprobieren ist nicht teuer, sondern physikalisch unmöglich: alle Rechner der Erde über die Lebensdauer der Sonne — kein einziger Treffer. Deshalb schützen Staaten ihre Geheimnisse damit: nicht aus Mut, aus Mathematik.

🔬 Die Prüfung

X3DH, Double Ratchet, AES-256-GCM — keine Erfindung, der man vertrauen muss, sondern seit Jahrzehnten öffentliches Gut: tausend Kryptologen, Standard-Dokumente, im Einsatz bei Signal, iMessage und Banken. Nach Kerckhoffs muss Sicherheit funktionieren, wenn jeder das Verfahren kennt. Bei Enigma 3 ist die Bauart offen dokumentiert — die Sicherheit hängt am Schlüssel, nicht am Verfahren.

⚠️ Die Bruchstelle — und warum sie hier fehlt

Noch nie wurde AES geknackt, X3DH gebrochen oder der Double Ratchet überwunden. **Jeder Fall gelesener Chats — EncroChat, Sky ECC, ANOM — scheiterte nie an der Mathematik, sondern am Rand:** ein Betreiber, der Schlüssel aushändigt, ein Update-Programm, das zum Späher wird, ein Produkt, das selbst die Hintertür war. Enigma 3 zieht diese Ränder ab: Server bei Ihnen, Schlüssel auf Ihren Geräten, Alarm bei jedem neuen Gerät, Widerruf bei jedem Reset. Was übrig bleibt, ist die Mathematik allein.

Was „unknackbar“ nicht meint: die Metadaten (wer wann mit wem), Ihr eigenes Gerät und die Rechtslage, falls Sie zur Herausgabe Ihrer Schlüssel gezwungen werden. Alles andere — Inhalt, Namen, Reaktionen, Anhänge — bleibt Chiffretext.

IM VERGLEICH

— Gegen das Feld — Signal, Matrix, Session, SimpleX

Alle vier sind gute Messenger. Der Unterschied ist nicht der Algorithmus — den teilen sie — sondern wem die Server gehören, was nach dem Löschen bleibt und wer im Vorfeld angreifen kann.

	Signal	Matrix	Session	SimpleX	**Enigma 3**
Server gehört	Foundation (USA)	Betreiber, föderiert	Oxen-Konsortium	Serverbetreiber	**Ihnen**
Zugang	Telefonnummer Pflicht	E-Mail, Server frei	Seed-Satz	ohne Identität	**Nutzername + Einladungscode**
Echtes Löschen	Retention des Servers	Soft-Mask, Betreiber muss liefern	nach Zustellung	nach Zustellung	**Crypto-Shredding, auch im Backup**
Timer verlängerbar?	Server setzt Frist	Betreiber setzt Frist	—	—	**nein — steht im Chiffretext**
Stille Mitleser?	—	Server kann still Mitglieder hinzufügen	—	—	**Senden pausiert bis zur Bestätigung**

🎯 Kein Massenziel — und keine Landkarte

Wer Signal, WhatsApp oder Telegram angreifen will, erfindet nichts — es ist schon gebaut: ein Werkzeug für eines von hundert Millionen **identischen** Geräten, und alle sind betroffen. So kippten EncroChat und Sky ECC. **Für Enigma 3 existiert kein solcher Werkzeugkasten.** Der Code ist nicht öffentlich, er läuft nirgends millionenfach — niemand, dem Behörden ihr Handwerkszeug vorab abnehmen könnten, hat ihn unter echten Nutzern gewendet. Es gibt keine Landkarte, an der man ansetzen könnte. Ein vorbereiteter Angriff läuft ins Leere: Er muss einzeln, bei Null, für genau Ihren Server geführt werden — ohne Vorlauf, ohne Trefferliste.

Ehrlich statt beworben: Ihr Betreiber sieht die Verbindung — wer, wann, wo. Was Sie senden, nie. Alles andere ist ein Versprechen, das man nachprüfen kann.

SICHERHEIT

— Verschlüsselt bis unters Dach — als Voreinstellung

Sie müssen nichts einstellen. Alles Folgende ist Standard ab der ersten Nachricht:

🔐 Ende-zu-Ende-Verschlüsselung

Direktnachrichten: X3DH + Double Ratchet (wie Signal) mit Vorwärtsgeheimheit und Selbstheilung. **Kanäle und Gruppen:** Sender Keys, rotiert bei jedem Austritt. **Anhänge:** AES-256-GCM, Dateiname und Typ im Chiffretext. Der Server speichert und vermittelt **nur Chiffretext** — er kann nichts lesen.

📞 Verschlüsselte Anrufe — auf Ihrem Server

Sprach- und Videoanrufe mit Bildschirmfreigabe, je Anruf eigener Schlüssel. Neuer Schlüssel bei jedem Teilnehmerwechsel. **Der LiveKit-Server läuft bei Ihnen** — was Signal und WhatsApp nur bei deren Rechenzentren tun, passiert hier auf Ihrer Hardware. Auf Wunsch komplett ohne LiveKit-Kontainer.

⏱️ Selbstlöschende Nachrichten

Lebensdauer je Nachricht wählbar: 1 h · 7 h · 24 h · 3 · 7 · 30 Tage. Der Timer steht im verschlüsselten Inhalt — **der Server kann ihn nicht verlängern.**

🔥 Unwiederbringliche Löschung

Crypto-Shredding: Jede Nachricht hat einen eigenen Schlüssel. Löschen zerstört den Schlüssel — Kopien auf Server und Backup sind danach **unlesbar**. Es gibt keine eingebauten Backups, die Löschung aushebeln.

📱 Geräte & Sicherheitsnummern

Eigener Schlüssel pro Gerät. Geräte einsehen und widerrufen, Alarm bei neuem Gerät, optionales Auto-Entfernen. Sicherheitsnummern zum Vergleichen — so schließen Sie aus, dass niemand unbemerkt zuhört. **Ein neues Gerät liest Älteres nicht** — die Schlüssel dazu wurden für es nie erzeugt.

🔑 Lokaler Tresor

Biometrie oder PIN versiegeln die Schlüssel auf dem Gerät (Argon2id). Die PIN ist 8-stellig und am Desktop Pflicht. Android nutzt den Keystore, Windows DPAPI. Ohne PIN findet sich nur Chiffretext.

🔐 Zwei-Stufen-Login (TOTP)

Zusätzlich zum Passwort ein sechsstelliger Einmal-Code aus der Authenticator-App — eingerichtet unter Einstellungen → Sicherheit. Feste **Backup-Codes** helfen, wenn das Gerät nicht griffbereit ist. Angemeldet wird nur mit **Anmeldename und Passwort** — das System speichert und versendet keinerlei E-Mail-Adressen; der Zugang kommt per Einladungscode des Betreibers.

DAS SICHERHEITSMODELL

— Wer sieht was — und wer kann was nicht

Server-Betreiber	Sieht **Metadaten** (wer, wann, welcher Raum, Größe). **Kann nicht:** Inhalte, Anhänge oder Anrufe lesen — der Server sieht nur Chiffretext.
Angreifer im Netz	Sieht nur eine TLS-Verbindung. **Kann keine** Inhalte lesen.
Gestohlenes Gerät	Ohne PIN/Passwort nur Chiffretext. Schlüssel sind hardwaregestützt versiegelt.
Push-Anbieter	Erhält nur Zeitpunkt und Zielgerät — **niemals den Inhalt** einer Nachricht.
Server-Beschlagnahme	Ohne die Geräte-Schlüssel der Nutzer: **keine einzige lesbare Nachricht.**

VOREINSTELLUNGEN

Sauber voreingestellt — kompromisslos

- ✓ **Nur Einladung:** Wer mitmacht, entscheidet der Betreiber per Einladungslink.
- ✓ **12 Zeichen** Mindest-Passwort, Anmelde-Drosselung mit wachsender Sperrzeit, hartes Passwort-Schloss nach Fehlversuchen.
- ✓ **Anmeldung nur mit Anmeldename und Passwort** — optional zwei Stufen mit Einmal-Code (TOTP) und Backup-Codes. Es werden keine E-Mail-Adressen gespeichert oder versendet.
- ✓ **HTTPS mit HSTS** und strenger Content Security Policy — der Server lehnt Klartext rundherum ab.
- ✓ **Metadaten-Rauschen entfernt:** EXIF, GPS und XMP verschwinden beim Bild-Upload — ein Foto, das Sie senden, ist genau das: ein Bild. Kein Formular.
- ✓ **Bots, SSO und Webhooks gibt es nicht:** keine API-Key-Tür, kein Login über fremde Anbieter, kein automatischer Post-Verteiler — die Bauart ist ohne diese Einfallstore gebaut.
- ✓ **Neues Gerät statt Alarm:** bringt ein Kontakt nur ein neues Gerät hinzu, zeigt die App den Hinweis „Neues Gerät“ mit Bestätigung — kein Angriffsalarm. Echte Schlüsselwechsel bleiben die rote Warnung; beides hält das Senden bis zur Bestätigung an.
- ✓ **Keine Telemetrie, kein Crash-Reporting, kein Hintergrund-Download.**
- ✓ **Nach dem Löschen** bleibt nur ein inhaltsloser Löschnachweis — kein Inhalt, kein Text.

Ehrlich statt beworben: Kommunikationspartner, Zeitpunkte und Raumgrößen bleiben als Metadaten sichtbar — auf Ihrer eigenen Hardware, nicht bei einem Konzern. Was Sie senden, sieht niemand. Enigma 3 ersetzt Versprechen durch überprüfbare Technik.

KRYPTOGRAFIE

Ende-zu-Ende-Verschlüsselung — wie es im Detail funktioniert

Grundlage sind geprüfte Standard-Verfahren: WebCrypto mit NIST P-256 (ECDH, ECDSA), HKDF/HMAC-SHA-256 und AES-256-GCM. Private Schlüssel verlassen das Gerät nie.

🤝 Austausch: X3DH

Der Absender holt das **Prekey-Bündel** des Empfängergeräts und prüft dessen Signatur gegen den gepinnten Signaturschlüssel (TOFU). Ergebnis ist ein gemeinsamer Geheimnis — nur für diese zwei Geräte.

🔁 Direktnachrichten: Double Ratchet

Jede Nachricht hat einen **eigenen Schlüssel**. Der symmetrische Ratchet liefert Vorwärtsgeheimheit, der Diffie-Hellman-Ratchet **Selbstheilung** nach einer Kompromittierung. Auch die Header sind verschlüsselt. Replay-Schutz inklusive. Jede Nachricht wird für alle vorhandenen Geräte verschlüsselt — **ein späteres Gerät liest Älteres nicht**; die Schlüssel existieren für es nicht.

👥 Gruppen & Kanäle: Sender Keys

Jedes Gerät führt pro Raum eine signierte Schlüsselkette. Verteilt wird **über die verschlüsselten Einzel-Sitzungen** — nur bestätigte Mitglieder erhalten Schlüssel. Rotation bei jedem Austritt, spätestens nach 7 Tagen. Neue Mitglieder lesen Älteres **nicht** mit.

📞 Anrufe & Anhänge

Anrufe: LiveKit Insertable Streams. Die Geräte vereinbaren den Anrufschlüssel untereinander und verpacken ihn an die Gerätschlüssel der Teilnehmer — der Server erzeugt, speichert oder ausgibt ihn nie selbst. **Anhänge:** AES-256-GCM über den Ratchet bzw. Sender Key — Dateiname und Typ liegen im Chiffretext.

Schlüssel pro Gerät (jedes Gerät erzeugt eigene)

Identitätsschlüssel (ECDH P-256)	Basis der Sicherheitsnummer — dauerhaft pro Gerät
Signaturschlüssel (ECDSA P-256)	Signiert das Signed Prekey, beim ersten Kontakt gepinnt (TOFU)
Signed Prekey & Einmal-Prekeys	Für den X3DH-Austausch, werden erneuert und nach Verbrauch nachgefüllt

DURCHSETZUNG & VERTRAUEN

— Was der Server ablehnt — und was der Client beobachtet

🚫 Der Server weist Klartext ab

`CreateMessage`, `UpdateMessage`, `CreateUpload` und Bildbeschreibungen antworten mit `e2ee_required` — ohne Chiffretext, in Direktnachrichten, Gruppen und Kanälen. Diese Pflicht ist **nicht abschaltbar**. Alte Klartext-Nachrichten werden beim Start zerstört: Schlüssel geschreddert, Speicher sicher überschrieben.

🚪 Keine stillen Lauscher

Der Client merkt sich die zuerst gesehene Mitgliederliste. Später hinzugefügte Mitglieder bleiben **ausstehend**, bis Sie sie bestätigen oder ihre Sicherheitsnummer prüfen. Der Server darf neue Mitglieder melden — aber keine Schlüssel unbemerkt aushändigen.

⚠️ Gerätewarnungen (TOFU)

Geräte-Schlüssel werden beim Erstkontakt gepinnt. **Ein neues Gerät** zeigt nur den Hinweis „Neues Gerät“ mit Bestätigung — **kein Alarm**. Ein echter Schlüsselwechsel bleibt die rote Warnung. Beides hält das Senden bis zur Bestätigung an. Neue Anmeldungen warnen **Ihre anderen Geräte** mit Name und Zeit — Widerruf per Klick.

🧹 Kontrolliertes Löschen

Systemereignisse (Beitritte, Anrufe, Raumänderungen) sind sofort oder automatisch löschbar; der Server überschreibt gespeicherte Ereignisse sicher. Nach dem Löschen bleibt nur ein inhaltsloser Löschnachweis.

🔒 Harte Vorgaben

- ✓ **Nur mit Einladung** registrieren
- ✓ **12 Zeichen** Mindest-Passwort
- ✓ Anmelde-Drosselung mit wachsender Sperrzeit
- ✓ **Absolute Sitzungslaufzeit** (Standard 12 h)
- ✓ HTTPS mit HSTS, strenge CSP, kein Einbetten
- ✓ Auto-Entfernen untätiger Geräte nach 30–365 Tagen (optional)

🧨 Entfernt, nicht abgeschaltet

- ✓ **Keine Bots** — API-Keys, MCP, Webhooks entfernt; Bot-Konten beim Start widerrufen
- ✓ **Kein SSO/OAuth** — Passwort-Anmeldung bleibt immer aktiv
- ✓ **Keine Link-Vorschauen** — der Server sähe die URL in Klartext
- ✓ **Keine Telemetrie, kein Crash-Reporting**

GERÄTESICHERHEIT

— Schlüssel unter Verschluss — und wer warnen kann

🔑 Der Tresor (App-Sperre)

PIN oder Passphrase leitet per **Argon2id** (am Desktop 256 MiB, bestehende Tresore ziehen automatisch hoch) einen Schlüssel ab, der einen zufälligen 256-Bit-Datenschlüssel umhüllt — versiegelt mit einem gerätespezifischen Geheimnis. Alle Tresoreinträge sind mit **AES-GCM** versiegelt. Android: Keystore/StrongBox, iOS: Secure Enclave, Windows: DPAPI. Beim Sperren, Timeout und App-Ende wird der Schlüssel aus dem Speicher verworfen. Falsche PIN: exponentielle Sperre, optional Tresor-Wipe nach N Versuchen (wählbar: 3, 5, 10, 25, 50; die Stufe „stark“ erzwingt 8-stellige PIN und Löschen nach 5). Beim Tippen zeigt eine Einschätzung, wie schnell eine kopierte Datenbank die PIN prüfen könnte.

✅ Verifizieren statt hoffen

Sicherheitsnummer je Person — persönlich oder per QR-Code verglichen. Danach gilt die Person als verifiziert. In Gruppen per Schloss in der Kopfzeile für jedes Mitglied. Verifizierte Geräte werden bei Schlüsseländerung **rot markiert**, bis Sie bestätigen — Senden bleibt dann pausiert.

📱 Geräte im Blick

Alle Geräte des Kontos mit Nachrichtenschlüsseln sichtbar, einzeln widerrufbar. Neues Gerät? Ihre anderen Geräte erhalten eine **Alarm-Nachricht** („Das war ich nicht?“). Optionales Auto-Entfernen: Geräte, die 30/60/90/180 Tage inaktiv waren, werden mitsamt Schlüsseln widerrufen.

🚪 Keine stillen Mitleser

Der Client merkt sich die erste gesehene Mitgliederliste. Der Server kann neue Mitglieder nur **angeben** — Schlüssel gibt es erst nach Ihrer Bestätigung. So kann niemand unbemerkt eingeschleust werden. Sessions laufen mit **absoluter Laufzeit** (Standard z. B. 12 h), nicht nur nach Untätigkeit.

METADENSCHUTZ · STUFE 1

Verschlüsselung versteckt den Inhalt — Stufe 1 nimmt die Metadaten dazu

Der Gegner hier: der Server-Betreiber oder jeder, der eine Kopie der Server-Daten erhält. Stufe 1 entfernt die Metadaten, die der Server nicht braucht, und macht den Rest ungenauer. Experimentell, standardmäßig an, ohne Einstellung.

🏷️ Verschlüsselte Kanalnamen

Der Client verschlüsselt **Kanalname und Beschreibung** mit den Sender Keys des Raums; der Server speichert nur Chiffretext und einen neutralen Platzhalter (🔒 `#4f2a9c01d7`). Der Klartextname erreicht den Server nie — eine spätere Umbenennung im Klartext wird abgelehnt (fail closed). Wer lesen kann, liest den Namen; Geräte ohne Schlüssel sehen den Platzhalter. Alte Klartext-Einträge löscht die Migration.

📏 Größen-Padding

Jede verschlüsselte Nachricht und Bearbeitung wird vor der Verschlüsselung auf eine feste Größenstufe gepolstert (Padmé-Regel, ≥256 Byte, höchstens ~12 % Mehrkosten, unsichtbare Markerzeichen). **Der Server erkennt nicht, ob eine kurze Antwort oder ein langer Satz geht.** Anhänge nutzen schon immer Größenstufen.

⌨️ Typing-Abschaltung

Einstellungen → Datenschutz & Sicherheit: „Schreibanzeigen senden“ aus heißt, dieses Gerät sendet keine — während Sie die der anderen weiter sehen. Die Wahl gilt pro Gerät und Server, nie zentral gespeichert.

🪪 Verschlüsselte Profilnamen

Anzeigename und Bild sind Ende-zu-Ende verschlüsselt; der Server sieht nur Chiffretext und einen stabilen Platzhalter. Wer in einem Raum mit Ihnen lesen kann, erhält den Freischlüssel automatisch — auch Geräte, die später beitreten.

😊 Verschlüsselte Reaktionen

Neue Reaktionen laufen wie die Nachricht selbst: der Server speichert nur Kennung und Chiffretext und erkennt weder Menge noch Emoji. Ältere Reaktionen aus Klartext-Zeit bleiben lesbar.

🧾 Minimale Server-Logs

Die Prozess-Logs schreiben standardmäßig **keine Benutzer-IDs, Anmelde- oder Anzeigenamen, Raumnamen, E-Mails oder IPs** — Identitätsfelder stehen als `[redacted]`. Audit-Einträge behalten keinen IP- oder User-Agent-Hash, außer der Betreiber schaltet ihn scharf — dann mit rotierendem Schlüssel (Standard 24 h). Die Sitzungsliste zeigt die grobe Geräteklasse („Firefox on Windows“).

KONTROLLE

— Ihr Konto, Ihr Server — mit den harten Buttons

🔑 Passkey-Anmeldung (WebAuthn)

Anmeldung ohne Passwort: Der Server speichert nur das **öffentliche Credential**, der private Schlüssel bleibt auf Ihrem Gerät. Auf HTTPS-Servern sind Passkeys **standardmäßig an** — Passwort-Anmeldung bleibt immer erhalten und lässt sich nicht abschalten. Ein **Passwort-Reset warnt alle Geräte des Kontos** — so sehen Sie sofort, ob jemand Ihr Konto zwischenzeitlich genutzt hat. Jede Zeremonie nutzt einen fünf Minuten gültigen Nonce, der **höchstens einmal** verifiziert. Ein neuer oder entfernter Passkey alarmiert Ihre anderen Sitzungen; Entfernen widerruft bestehende Credentials wie ein Passwortwechsel. Die Relying Party wird aus der öffentlichen HTTPS-URL abgeleitet — Credentials gelten nie über den Server-Herkunftsbereich hinaus.

📡 Aktive Sitzungen: wer online ist

Einstellungen → Sicherheit zeigt **jedes Gerät, das bei Ihrem Konto angemeldet ist**: Beschreibung, Anmeldeart, Anmeldezeitpunkt, letzte Nutzung, ein **Online-Marker** und „dieses Gerät“. Online heißt eine live bestehende Echtzeitverbindung, pro Sitzung mit 60-Sekunden-Herzschlag — nicht geraten. Jede Sitzung außer der aktuellen lässt sich mit **einem Klick abmelden**. Gestohlener Laptop oder vergessener Browser lassen sich gezielt abmelden — ohne das Konto anzufassen.

📱 Geräte & Schlüssel in der Hand

Einstellungen → „Geräte mit Nachrichtenschlüsseln“ zeigt jedes Gerät Ihres Kontos; jedes ist **einzeln widerrufbar**. Ein widerrufenes Gerät wird abgemeldet, verliert Sitzungen und Tokens und erhält **keine neuen Sender Keys** — künftige Nachrichten lassen es aus. Neue Anmeldungen alarmieren Ihre anderen Geräte mit Name und Zeitpunkt und der Option „**Das war ich nicht**“ zum sofortigen Widerrufen. Betreiber können Auto-Entfernen nach Untätigkeit (30–365 Tage) einrichten; entfernte Geräte werden mitsamt Schlüsseln vollständig widerrufen.

Buttons für die harten Fälle

🗑️ Alles löschen — der Admin-Button

Administratoren finden in **Admin → Sicherheit → selbstlöschende Nachrichten** einen Danger-Button: „Alle Nachrichten löschen“. Ein Vorgang räumt **jede Nachricht in jedem Raum, Thread und jeder Direktnachricht** — inklusive Reaktionen, Bearbeitungen, Anhänge und Link-Vorschauen. Dieselbe Mechanik wie der Ablauf-Wischer: jeder Nachrichtenschlüssel geschreddert, Körperereignisse gelöscht, Anhang-Bytes entfernt, Projektionen aktualisiert, bis zu acht Räume parallel als Hintergrundjob. **Konten, Räume, Mitgliedschaften, Geräte, Schlüssel und Einstellungen bleiben.** Endgültig, im Audit-Protokoll ohne Nachrichteninhalt.

🧹 Alle *eigenen* Nachrichten löschen

Nutzer haben diese Kraft über ihre eigenen Daten ebenfalls: Einstellungen → Selbstlöschende Nachrichten → „Alle meine Nachrichten löschen“. Der Server zieht jeden je geschriebenen Beitrag zurück — auch aus verlassenen Räumen und Thread-Antworten, neueste zuerst. Mitgliedschaft bleibt; Inhalt, Reaktionen, Pins, Such-Einträge, Benachrichtigungen und Anhänge gehen. Kryptografisch geschreddert, nicht versteckt.

⚙️ Admin → Sicherheit: was dort steht

Eine eigene Seite **Sicherheit** mit drei Bereichen. **Zugang:** gesperrte Benutzernamen, die der Server bei der Registrierung ablehnt; jeder OAuth-Client auf Standard, vertraut oder gesperrt stellbar. **Aufbewahrung:** Danger-Button „Alle Nachrichten löschen“ (Hintergrundjob mit Fortschritt); Systemmeldungen sofort löschen oder der Nachrichtenlebensdauer folgen lassen, sicher überschrieben. **Sitzungen:** absolute Sitzungslaufzeit (z. B. 12 h); **inaktive Geräte automatisch entfernt nach 30, 60, 90, 180 Tagen oder 1 Jahr** — widerrufen, Schlüssel, Sitzungen und Tokens, auch das letzte Gerät eines Kontos. Dazu: Einladung-Links mit Ablauf, Passwort-Policy, Anmelde-Drosselung, Branding, Audit-Protokoll ohne Inhalt, IP-Watch-Diagnose.

AUSSTATTUNG

Ein Messenger, der alles kann — verschlüsselt

💬 Voller Chat

Räume, Threads, Gruppen und Kanäle, Erwähnungen, Reaktionen, Markdown, angeheftete Nachrichten, Dateianhänge — alles Ende-zu-Ende verschlüsselt. Lesebestätigungen beidseitig abschaltbar.

🖼️ Dateien & Medien

Bilder, Dokumente, Videos — Ende-zu-Ende verschlüsselt, Metadaten automatisch entfernt.

📞 Konferenzen

Sprach- und Videoanrufe mit Bildschirmfreigabe, je Anruf verschlüsselt.

🔔 Benachrichtigungen

Push nur ohne Inhalt — Ihr Text geht nie über fremde Server.

🛡️ Verifizierung

Sicherheitsnummern je Person, Geräteübersicht, Warnung bei neuen Geräten.

🧹 Kontrollierte Löschung

Systemmeldungen sofort oder automatisch löschen — Server überschreibt sicher.

Überall zu Hause

🪟 **Windows 10/11 (x64)**	Installer, behält bei Updates alle Daten und Schlüssel.
🐧 **Linux x86_64 / arm64**	AppImage — ausführen und loslegen.
🤖 **Android 7+**	Signierte APK, mit Biometrie-Sperre und Keystore-Tresor.
📱 **iPhone / iPad**	Nutzung über die Web-App im Safari.
🌐 **Browser**	Web-App direkt vom eigenen Server.

LOSLEGEN

In drei Schritten zum eigenen Chat

1. **Server starten**
   Ein Linux-Rechner oder eine VM. Ein einziges **setup.sh** führt Sie durch die Einrichtung: Domains, Cloudflare und Docker — ohne Docker-Wissen, es fragt alles ab und richtet es ein. Sie brauchen eine Domain. Mehr Routine braucht es nicht.

2. **App installieren**
   Desktop-App, APK oder Web-App öffnen und **Serveradresse eintragen**. Anmeldung nur per Einladung — so entscheidet Ihr Betreiber, wer dabei ist.

3. **Sicher loslegen**
   Erste Direktnachricht, Sicherheitsnummer vergleichen, ersten Anruf testen. Alles Weitere ist Voreinstellung.

Wichtig zu wissen: Enigma 3 ist selbst gehostete Software für Menschen, die Kontrolle übernehmen wollen — kein kostenloser Fernwartungs-Dienst. Sie brauchen eine eigene Linux-Maschine und eine Domain; Aufsetzen und Betrieb übernimmt Ihr Betreiber. **Warum gibt es das?** Weil wir es selbst nutzen — kein Investor, kein datenhungriges Geschäftsmodell dahinter. **Es gibt immer nur die letzte Version** — keine veralteten Pakete im Umlauf. Technische Details, Sicherheitsmodell und Installation sind vollständig offen dokumentiert.

Wechseln Sie. Reden Sie weiter.

Nachrichten, die bei Ihnen bleiben — auf Hardware, die Ihnen gehört.