

ENIGMA 3

Deine Nachrichten. Dein Server. Niemand sonst.

Der selbst gehostete Messenger mit durchgehender Ende-zu-Ende-Verschlüsselung: Nachrichten, Anhänge und Anrufe. Kein Konzern, keine Cloud, keine Telemetrie — alles läuft auf Ihrer eigenen Hardware.

- 🔒 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.

Bekannte Messenger versprechen: „Wir schützen Ihre Daten.“ Dieses Versprechen hängt vom Vertrauen ab — im Betreiber, im Unternehmen, in dessen Mitarbeitern. Die bekanntesten „abhörsicheren“ Dienste der Welt sind genau daran gescheitert:

💥 EncroChat (2020) · Sky ECC (2021) · ANOM (2021)

EncroChat: Polizei drang in die **Server des Herstellers** ein — nicht in die Verschlüsselung — und schob allen 60.000 Geräten ein Update unter, das die Schlüssel abschöpfte: **60 Mio. gelesene Nachrichten**, 700 Mio. € beschlagnahmt, **6.500+ Festnahmen** (Sirus). **Sky ECC:** Server beschlagnahmt, Gründer festgenommen — die Schlüssel lagen beim Anbieter. **ANOM:** verdeckte FBI-Operation, **das Produkt selbst war die Hintertür**, 300+ Verurteilungen. Belege: offizielle Europol-, Eurojust- und Staatsanwaltschaftsmeldungen. **Der gemeinsame Fehler:** Der Betreiber war die schwache Stelle. Enigma 3 entfernt sie — der Server läuft bei Ihnen.

Das Prinzip: Enigma 3 hat keine Herstellerinstanz, die man übernehmen kann. Was wichtig ist, passiert auf Ihrer Hardware. Sie entscheiden, wer was lesen darf — wenn Sie wollen: niemand.

Der Alltag, verglichen

	WhatsApp	Telegram	**Enigma 3**
Server gehört	Meta	dem Anbieter	**Ihnen**
Lesezugriff	Anbieter (optional Backup)	Anbieter (bei „Cloud-Chats“)	**niemandem**
Metadaten	bei Meta	beim Anbieter	**auf Ihrer Hardware**
Kündigung	Anbieter löscht Ihre Daten	Anbieter löscht Ihre Daten	**Sie sind der Betreiber**

Für wen ist das?

Richtig für Sie, wenn …
… Sie Familien- oder Team-Nachrichten nicht bei einem Konzern parken wollen.
… Ihr Verein oder Ihre Praxis DSGVO nicht erklären, sondern einfach lassen will.
… Sie WhatsApp-Klonen entkommen wollen, ohne auf vertraute Funktionen zu verzichten.
… Sie die Wahl zwischen „zu einfach“ und „Konzern-Dschungel“ leid sind.

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.

🔑 Lokaler Tresor

Biometrie oder PIN versiegeln die Schlüssel auf dem Gerät (Argon2id). Android nutzt den Keystore, Windows DPAPI. Ohne PIN findet sich nur Chiffretext.

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.**

Sauber voreingestellt — kompromisslos

- ✓ **Nur Einladung:** Wer mitmacht, entscheidet der Betreiber per Einladungslink.
- ✓ **12 Zeichen** Mindest-Passwort, Anmelde-Drosselung mit wachsender Sperrzeit.
- ✓ **HTTPS mit HSTS** und strenger Content Security Policy — der Server lehnt Klartext rundherum ab.
- ✓ **Metadaten-Rauschen entfernt:** EXIF, GPS und XMP werden beim Bild-Upload automatisch gelöscht.
- ✓ **Keine Bots, kein SSO, keine Webhooks:** konsequent entfernt, weil sie die Verschlüsselung aufbrechen würden.
- ✓ **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. Wer die Web-App vom Server lädt, muss dem Server vertrauen — Desktop- und Android-App reduzieren dieses Risiko. 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.

👥 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, Medienschlüssel pro Anruf, verpackt an die Gerätschlüssel der Teilnehmer. **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. Abweichungen markieren Nachrichten als „**Neues Gerät**“, färben das Schloss rot, und Sie können bestätigen oder prüfen. 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** (64 MiB, t=3) einen Schlüssel ab, der einen zufälligen 256-Bit-Datenschlüssel umhüllt. 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.

✅ 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. Passkeys sind optional — Passwort-Anmeldung bleibt immer erhalten und lässt sich nicht abschalten. 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, SMTP und Docker — ohne Docker-Wissen, es fragt alles ab und richtet es ein. Sie brauchen eine Domain und ein SMTP-Postfach. 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. Der Betrieb erfordert eine eigene Linux-Maschine und eine Domain. Technische Details, Sicherheitsmodell und Installation sind vollständig offen dokumentiert.

Wechseln Sie. Reden Sie weiter.

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