

AEGIS — Commercialization Assessment

What this is. An honest appraisal of what it would take to sell AEGIS, what it would cost, and which routes are actually viable. Written to help you decide, not to encourage the decision.

Not legal or financial advice. Export control, lawful-intercept obligations, and liability exposure are jurisdiction-specific and consequential. Retain a lawyer with encryption-export and platform-regulation experience *before* distributing anything, and an accountant before modelling seriously. The figures here are planning ranges with stated assumptions, not quotes.

1. The uncomfortable market facts

Secure messaging is one of the hardest consumer categories that exists. Before anything else, weigh these:

Consumer willingness to pay is close to zero. Signal is free and operates on roughly \$50M/year of donations and a \$50M founding loan; WhatsApp is free and monetized by an owner with other revenue. A paid app competes against excellent free products.

The network effect is brutal and asymmetric. A messenger's value to a user is approximately zero until the people they message are on it. This is why the category is littered with technically superior failures. It is the single biggest reason not to sell a consumer messenger.

Comparable outcomes. Threema (~€5 one-time, Swiss, privacy-branded) is one of the few consumer-paid successes and remains a modest business. Wire and Wickr both pivoted from consumer to enterprise/government; Wickr was acquired by AWS. Silent Circle and Blackphone struggled commercially despite strong technology. **The consistent pattern: the money is in B2B and government, not consumer.**

Your specific disadvantage: cover traffic costs bandwidth *continuously, per idle user*, so unit economics get worse with scale in a way normal SaaS does not. Quantify this early (see §5) — it may determine the entire business model.

Your specific advantage: post-quantum readiness is becoming a *procurement requirement*, not a nice-to-have. NIST standardized ML-KEM/ML-DSA, and US federal guidance pushes migration through the early 2030s. "Harvest now, decrypt later" is a real, fundable concern for organizations with long-lived secrets. **This is your wedge, and it is time-limited — the advantage erodes as incumbents ship PQ.** Signal already deployed PQXDH.

2. Regulatory and legal path

Export control (do this before distributing)

Encryption software is controlled under the U.S. Export Administration Regulations (ECCN 5D002) and equivalent Wassenaar-derived regimes elsewhere. Mass-market and publicly available software usually qualifies for **License Exception ENC**, but eligibility typically requires a self-classification report or a CCATS submission to the Bureau of Industry and Security, and open-source publication has its own notification treatment. Costs are modest (counsel time, roughly \$5–15k); the risk of skipping it is not. **Non-US founders:** your own national regime applies too, and some are stricter.

Lawful intercept and platform regulation

AEGIS is designed so the operator *cannot* identify who talks to whom. That is the product — and it is precisely what several regimes are pressing against: the UK Online Safety Act's technology notices, EU proposals around client-side scanning, and traceability mandates in India. Signal has publicly stated it would exit markets rather than comply. **Decide your position on this before you take money**, because it constrains which markets you can sell into and it is the question every investor and enterprise buyer will ask.

Liability

If you market to at-risk users — journalists, activists, dissidents — and the system fails, the harm is severe and irreversible. Terms of service do not fully insulate you from claims of reckless misrepresentation. Practical mitigations: publish the audit, state limitations plainly *in the product*, carry tech E&O insurance, and never make claims beyond §3 of the due-diligence document.

Other

Trademark search and registration for the name (AEGIS is heavily used — expect a rename). Privacy policy and DPA for GDPR/CCPA even though you hold little data. App-store policies (both stores permit E2EE messengers; both require disclosures). Dependency license inventory before distribution.

3. Three viable routes

Route A — Open-source protocol + commercial support (recommended)

Publish the code and whitepaper; monetize integration, licensing, audits, and support. In security, open source is a credibility requirement, not a giveaway; closed-source crypto is treated as a red flag. - **Revenue:** consulting (\$200–400/hr), integration contracts (\$50–250k), dual-licensing for closed products, sponsored feature

development. - **Cost to start:** lowest of the three. Effectively the audit plus your time. - **Risk:** modest ceiling; income is labour-linked. - **Why it fits:** your asset is a defensible *design*, and the paper plus audit is what converts it into reputation, which is what sells services.

Route B — B2B/regulated-sector product

Sell to organizations with a compliance-driven reason to care: defense contractors, legal, healthcare, finance with long-lived secrets, NGOs and news organizations. -

Pricing: \$15-60/seat/month, or six-figure site licences. - **Requirements:** SSO/SCIM, audit logging (carefully — logging fights the privacy model), admin policy controls, on-prem or sovereign deployment, SOC 2 Type II (~\$30-60k plus 6-12 months), and often FIPS-validated crypto modules for government work. - **Why it works:** the buyer is not choosing against free WhatsApp; they are choosing against a compliance failure. Network effects are contained inside the customer's org — **this neutralizes the category's worst problem.** - **This is where the money is if you want a company.**

Route C — Consumer paid app

One-time purchase (Threema model) or subscription. - **Reality check:** requires mobile apps, 24/7 infrastructure, support, marketing against free incumbents, and a solution to the cold-start problem. - **Recommendation:** do not start here. Consider it only after Route A or B has produced reputation and revenue.

4. What "production" actually requires

Beyond the hardening checklist, a sellable product needs:

Area	Work
Mobile	Native iOS + Android clients. The largest single line item. Rewrite the protocol in Rust with FFI bindings, or reimplement per platform.
Push notifications	Architecturally awkward: APNs/FCM see delivery events. Options are silent pushes with local fetch, or persistent connections that cost battery. Every private messenger fights this.
Infrastructure	Relay fleet across jurisdictions, directory authorities, monitoring, incident response, abuse handling.
Media	Attachments, images, voice notes; then encrypted calls via WebRTC with its own metadata problems.
Onboarding	Contact discovery without uploading address books — a genuinely hard privacy problem (Signal uses SGX enclaves, contested).
Support & ops	Account recovery under forward secrecy, device migration, on-call.
Compliance	SOC 2, possibly FIPS 140-3 validated crypto for government sales.

5. Cost and timeline model

Assumptions: senior engineers at \$150–200k/year fully loaded (US); a small team; sequential phases; no marketing spend until Phase 3. Adjust downward substantially for non-US or solo work.

Phase	Scope	Duration	Cost
0 • Hardening	P0+P1 from the checklist; native PQ crypto; CI	2–3 months	\$40–80k (1 engineer) or your own time
1 • Audit	External cryptographic + implementation audit, remediation, publish report	2–3 months	\$30–100k audit + \$20–40k remediation
2 • Formal methods <i>(optional but differentiating)</i>	Tamarin/ProVerif model	1–2 months	\$30–60k specialist
3 • Product	Mobile clients, media, push, onboarding, ops	9–18 months	\$400k–1.2M (3–5 people)
4 • Compliance	SOC 2 Type II; export classification; counsel	6–12 months (parallel)	\$50–120k
Infrastructure	Relays, directories, monitoring	ongoing	\$2–15k/month at modest scale

Realistic totals. Route A: **\$60–150k and 4–6 months** to a credible, audited, published protocol you can sell services around. Route B: **\$600k–1.5M and 18–24 months** to a sellable enterprise product. Route C: everything in Route B plus marketing, with a materially lower probability of success.

The number that decides your model: bandwidth cost per idle user per month under constant-rate cover traffic. Measure it before writing a business plan. At one 16 KB packet every 0.5 s, a single always-on client emits roughly 80 GB/month in each direction — clearly untenable as-is, so production must either lengthen the cover interval dramatically, shrink packets, or make cover traffic adaptive. **This is the most important open question for the business, and it is a protocol-design question, not a sales one.**

6. Recommended sequence

1. **Rename.** Clear trademark before building a brand.
2. **Do P0 hardening.** Two weeks. The API-auth and key-storage issues would embarrass you in any review.
3. **Publish.** Open-source the code, release the whitepaper, submit to PETS, USENIX Security, or Real World Crypto. Academic scrutiny is free, high-quality review — and rejection feedback is itself valuable.

4. **Measure the cover-traffic economics.** This determines whether the design scales commercially. Publish the numbers.
5. **Get the audit.** Publish the report *including findings*. Doing this openly is a stronger trust signal than a clean summary.
6. **Then choose:** services (Route A) or a B2B product (Route B), based on what the reception tells you about demand.

Do not: market to at-risk users pre-audit; claim anonymity properties the user population cannot support (see gap G2); keep the source closed; or make "unbreakable"/"quantum-proof" claims. In this field, overclaiming is the fastest way to lose the credibility that is your only real asset.

7. Honest assessment

What you have: an unusually complete research prototype with a coherent, defensible thesis, real implemented metadata defences, a working application, and a written specification. That is a genuine accomplishment and more than most projects at this stage have.

What you do not have: an audit, mobile clients, production key management, operational infrastructure, a distribution channel, or evidence that anyone will pay. The technology is the *smallest* remaining problem.

The most likely good outcome is not a consumer app. It is that AEGIS becomes a credible, cited, open specification with an audit behind it, and that credibility becomes consulting, licensing, or an enterprise product in a niche that has a compliance-driven reason to buy — or an acquisition by someone who needs post-quantum messaging expertise and wants the team.

The most likely bad outcome is spending a year building mobile apps for a consumer product nobody switches to. The graveyard is full of technically superior messengers.

If you want a business, go where the buyer has a budget and a mandate. If you want impact, publish and let the design influence systems with distribution you will never have. Both are worthwhile. Building a paid consumer messenger is the one path where the odds are genuinely poor.