

Competitive Analysis – Aegis Link vs Threema

1. Overview of Competitor

2.

Threema is a privacy-focused messaging app that offers:

End-to-end encryption (E2EE)

Anonymous usage (no phone or email required)

Paid, non-ad-based model

Swiss-based data protection

Open source code

3. Feature Comparison

Comparing the features of Threema and Aegis Link you can see that Threema is a more fully implemented system, but does have minimal data storage.

Feature Comparison Table:

Feature	Aegis Link (PoC)	Threema
Encryption	E2EE (default)	E2EE (default)
Data Storage	No persistent storage	Minimal metadata storage
Identity System	Aegis ID (public key based)	Threema ID (random identifier)
Registration	No personal data required	No phone/email required
Group Messaging	Not implemented	Fully supported
Offline Messaging	Not implemented	Supported
Platform Support	Limited (PoC) (planned extensions for mobile)	iOS, Android, Desktop
Monetisation	One-time payment (planned, mobile only)	One-time purchase
Open Source	Fully Open Source	Partially open source

4. Where Aegis is strong

- Aegis has zero-knowledge architecture, with no server-side storage at all
- It is fully privacy-by-design from inception
- Minimal data footprint exists, being only the Aegis ID and the keys
- Simpler architecture providing a bare-bones approach to privacy

5. Where Aegis is weak

- Aegis lacks certain key features which are available in Threema, including multiple platform support, group chats, and offline delivery.
- Less tested in comparison to Threema
- Weaker encryption practises

Aegis Link is a privacy-first proof of concept that prioritises zero-knowledge, allowing for users to have completely private and secure conversations with absolutely no oversight, while Threema is a fully realised, user-ready implementation of similar principles, with minimal metadata being collected.

When compared to other products such as Signal and WhatsApp, both Threema and Aegis Link prioritise anonymity and minimal data exposure, shifting the focus from convenience and large-scale connectivity toward privacy-first communication and user-controlled data.