

cMessenger

Sovereign-routed private messaging vs. consumer messengers and Tor — across privacy, sovereign routing, file transfer, and infrastructure trust.

Consumer messengers ship excellent end-to-end encryption but route through the operator's home jurisdiction; Tor anonymises transport but is not a messenger. **cMessenger** lets the sender choose the relay jurisdiction per message and per file, lets the recipient publish inbound jurisdiction filters, and runs every relay on a node that is already protected by the Interlace® Inline Engine on the wire.

Sovereign-routing per message and per file.

Sender picks the relay jurisdiction every time; recipient publishes inbound jurisdiction filters. No other messenger does either.

Per-message Path Diffusion.

Every message is its own atomic routing decision. Reassembly cost grows with conversation length; no probe ever sees the whole picture.

Every relay protected by the Interlace® Inline Engine.

Wire-speed XDP/eBPF filtering and the SOC behavioural engine on the infrastructure carrying your messages — not just on the cryptographic envelope.

Legend · ✓ supported · ✗ not supported · ◐ partial · — not applicable

Capability	Signal	WhatsApp	Telegram	FB Msgr	Discord	SimpleX	Tor	cMessenger
PRIVACY & IDENTITY								
End-to-end encryption by default	✓	✓	✗ cloud	✓	✗ text	✓	— transport	✓
No personal identifier (phone / email) required	✗ phone	✗ phone	✗ phone	✗ FB acct	✗ email	✓	✓	✓
Browser-only access — no app install	✗	◐ web tied to phone	✓	✓	✓	✗	✗ Tor Browser	✓
No central server retains message bodies	✗	✗	✗	✗	✗	◐ queue	— transport	✓
SOVEREIGN ROUTING								

Capability	Signal	WhatsApp	Telegram	FB Msgr	Discord	SimpleX	Tor	cMessenger
Sender chooses relay jurisdiction per message	X	X	X	X	X	X	ExitNodes config	✓
Per-message routing independence (Path Diffusion)	X	X	X	X	X	X	✓ per-stream circuit	✓
Recipient-defined inbound jurisdiction filters	X	X	X	X	X	X	X	✓
Operator-controlled jurisdictional policy	X US central	X Meta	X	X Meta	X	X federated	X volunteer	✓
FILE TRANSFER								
E2E-encrypted file attachments	✓	✓	secret chats	✓	X	✓	— overlay app	✓
Sovereign-routed file attachments (per-file path choice)	X	X	X	X	X	X	X	✓
INFRASTRUCTURE TRUST								
Wire-speed XDP/eBPF inline filtering on every relay	X	X	X	X	X	X	X	✓
SOC behavioural engine + self-learning reputation across global mesh	X	X	X	X	X	X	X	✓
Hashcash PoW anti-abuse (no SMS / CAPTCHA / bot detection)	X	X	X	X	X	X	✓ Tor PoW	✓

Tor is a transport-layer anonymity network, not a messaging service in itself; values reflect what Tor provides plus a typical overlay (OnionShare / Cwtch / Ricochet). **SimpleX** is federated and supports self-hosting of SMP queue servers, but does not expose per-message jurisdictional choice or inline-heuristic protection on relays. **Telegram**'s Cloud Chats are not E2E; only Secret Chats are. **Discord** rolled out E2E voice in 2024 but text and file content remain server-stored in plaintext.

READ THE FULL CMESSENGER PAGE

cMessenger deep-dive: interlaceresearch.com/solutions/messaging

Platform overview: interlaceresearch.com/platform

No phone, no email, no account required. Generate a cryptographic keypair in the browser and start sending. info@subpico.com