

Security benchmark of messaging applications

Signal, WhatsApp, Telegram, Matrix-based solutions (such as Element, Tchap or Citadel), Threema, SimpleX and Olvid: what do messaging apps that call themselves "secure" actually guarantee? A criterion-by-criterion review, for everyone to verify.

"objective and measurable arguments that anyone can verify for themselves"

A benchmark of secure messaging applications, by the designers of Olvid.

benchmark.olvid.io

Our approach

"Secure." "Private." "End-to-end encrypted." These words now appear on many consumer messaging apps. But what do they really mean? Behind a seemingly identical promise lie radically different security models: not all of them protect the user against the same adversaries.

Some solutions simply assert their security; others, such as Signal or Olvid, back it up with detailed technical justifications. These justifications are necessary — they allow a community of experts to analyze, discuss, and even challenge or refute the vendors' claims — but they are not sufficient: security concerns all users, while only the most knowledgeable are in a position to judge it.

These arguments must therefore be made accessible to the widest audience without distorting them: keep it simple without being simplistic. Misleading the end user would not only be dishonest; it would be potentially dangerous, since nobody knows in advance their profile, their context, or the risks they are exposed to.

We do not aim to be exhaustive, nor to catalog every messaging app on the market, but to shed light on structural weaknesses, too often overlooked, specific to certain operating models. **We therefore immediately ruled out the messaging apps that have no end-to-end encryption at all (Teams, Google Chat, Slack or Discord), where the operator has direct access to all exchanged data.**

As the designers of Olvid, one of the solutions examined here, we obviously have a bias. We will therefore stick, as far as possible, to objective and measurable arguments that anyone can verify for themselves.

An attentive reader will notice that Olvid checks almost every box in the table. It is tempting to see this as a tailor-made benchmark. We accept that suspicion, and we invite the reader to dispel it themselves: the relevance of each criterion is argued independently of whichever solution satisfies it. **If Olvid meets almost all of them, it is because we first defined the fundamental security criteria, and then designed Olvid to meet them. Not the other way around.**

The results

How each messaging application scores against each criterion

Criterion	Olvid	Signal	WhatsApp	Telegram	Matrix-based*	SimpleX	Threema
End-to-end encryption	✓	✓	✓	✗	⚡	✓	✓
End-to-end authentication	✓	✗	✗	✗	✗	✗	✗
End-to-end security	✓	✗	✗	✗	✗	✗	✗
No identity substitution	✓	✗	✗	✗	✗	✓	✓
Open source client	✓	✓	✗	✓	✓	✓	✓
End-to-end multi-device	✓	✓	✓	✗	✗	⊖	✓
Minimal personal data	✓	✗	✗	✗	✗	✓	⚡
No contact discovery and spam	✓	⚡	✗	✗	✗	✓	⚡
Post-quantum encryption	✗ planned for 2027	✓	✗	✗	✗	⚡	✗

Legend: ✓ Good ⚡ Partial ✗ Poor ⊖ Not applicable

* Element, Tchap, Citadel

To read this table properly, you need to understand each criterion, which we summarize further down by stating what it guarantees and what you are exposed to without it. Each summary is complemented by a dedicated page that explains in more detail why the criterion is essential to the security of a messaging app. A separate page lists some of the criteria we excluded and explains why we did so. Finally, each application is analyzed, with a criterion-by-criterion justification of the results we give it.

The criteria

End-to-end encryption

WHAT THIS CRITERION GUARANTEES: Your messages are encrypted before they leave your device, and only those who hold the keys they were encrypted for can read them. You still need to make sure that those keys really belong to your correspondents (that is what the End-to-end authentication criterion is about).

WITHOUT IT: Anyone with access to the server (operator, hacker, authority) can read all conversations in full.

End-to-end authentication

WHAT THIS CRITERION GUARANTEES: You are always certain of the identity of the person you are writing to, without having to take the operator's word for it.

WITHOUT IT: The operator, or anyone who compromises it, can impersonate any of your contacts, and encryption does not protect you from that.

End-to-end security

WHAT THIS CRITERION GUARANTEES: You know who you are talking to, and you know that nobody else can listen in, not even the operator. In other words, you are having a genuinely private conversation.

WITHOUT IT: One of the two guarantees is missing, and the other loses most of its value. Perfect encryption to the wrong person protects nothing.

No identity substitution

WHAT THIS CRITERION GUARANTEES: The trust established with a contact remains valid over time; their identity cannot be silently replaced.

WITHOUT IT: A malicious operator, or in some cases the interception of a single SMS, is enough to take control of an account and impersonate its owner with all of their contacts.

Open source client

WHAT THIS CRITERION GUARANTEES: The messaging app's security promises can be verified by a third party.

WITHOUT IT: There is no way to confirm that the application really does what it claims; you have to take the vendor's word for it.

End-to-end multi-device

WHAT THIS CRITERION GUARANTEES: You use your profile on all your devices, and only a device that is already legitimate can authorize a new one.

WITHOUT IT: Either you are limited to a single device per account, or the server decides which devices receive your conversations, and nothing stops it from adding one it controls.

Minimal personal data

WHAT THIS CRITERION GUARANTEES: The operator knows nothing about you. Data it does not hold can be neither hacked nor sold.

WITHOUT IT: Your messaging app is tied to your real identity, and that link is exposed to leaks and cross-referencing.

No contact discovery and spam

WHAT THIS CRITERION GUARANTEES: Nobody can find you or reach out to you unless you want them to.

WITHOUT IT: Anyone who knows your number can contact you: spam, phishing and, in the worst cases, attacks that require no action on your part.

Post-quantum encryption

WHAT THIS CRITERION GUARANTEES: Your communications recorded today cannot be decrypted tomorrow, on the day a sufficiently powerful quantum computer exists.

WITHOUT IT: An adversary who records your encrypted communications today will be able to decrypt them retroactively as soon as they have such a computer.



READ MORE

benchmark.olvid.io

Comments, corrections, suggestions? Email us at benchmark@olvid.io.

© 2026 Olvid · Unless otherwise noted, the content of this site is licensed under CC BY-ND 4.0. · 1 October 2026