

Comparatif de la sécurité des messageries

Signal, WhatsApp, Telegram, les solutions Matrix (comme Element, Tchap ou Citadel), Threema, SimpleX et Olvid : que garantissent vraiment les messageries qui se disent « sécurisées » ? Un examen critère par critère, que chacun peut vérifier.

« des arguments objectifs et mesurables, que chacun pourra vérifier par lui-même »

Un comparatif de la sécurité des messageries, par les concepteurs d'Olvid.

benchmark.olvid.io

Notre démarche

« Sécurisée. » « Privée. » « Chiffrée de bout en bout. » Ces mots s'affichent aujourd'hui sur bon nombre de messageries grand public. Mais que recouvrent-ils réellement ? Derrière une promesse en apparence identique se cachent des modèles de sécurité radicalement différents : tous ne protègent pas l'utilisateur contre les mêmes adversaires.

Certaines solutions se contentent d'affirmer leur sécurité ; d'autres, à l'image de Signal ou d'Olvid, l'étayent par des justifications techniques détaillées. Ces justifications sont nécessaires — elles permettent à une communauté d'experts d'analyser, de discuter, voire de contester ou d'invalidier les prétentions des éditeurs — mais elles ne suffisent pas : la sécurité concerne tous les utilisateurs, alors que seuls les plus avertis ont les moyens d'en juger.

Il faut donc rendre ces arguments accessibles au plus grand nombre sans les trahir : faire simple sans être simpliste. Tromper l'utilisateur final ne serait pas seulement malhonnête ; ce serait potentiellement dangereux, car nul ne connaît à l'avance son profil, son contexte, ni les risques auxquels il est exposé.

Nous ne cherchons pas à être exhaustifs, ni à recenser toutes les messageries du marché, mais à mettre en lumière des faiblesses structurelles, trop souvent ignorées, propres à certains modes de fonctionnement. **Nous avons ainsi écarté d'emblée les messageries dépourvues de tout chiffrement de bout en bout (Teams, Google Chat, Slack ou Discord), où l'opérateur accède directement à l'ensemble des données échangées.**

En tant que concepteurs d'Olvid, l'une des solutions étudiées ici, nous avons évidemment un parti pris. Nous nous en tiendrons donc, autant que possible, à des arguments objectifs et mesurables, que chacun pourra vérifier par lui-même.

Un lecteur attentif remarquera qu'Olvid coche presque toutes les cases du tableau. La tentation est grande d'y voir un comparatif taillé sur mesure. Nous assumons ce soupçon et invitons le lecteur à le lever lui-même : la pertinence de chaque critère est argumentée indépendamment de la solution qui le satisfait. **Si Olvid les remplit presque tous, c'est parce que nous avons d'abord défini les critères de sécurité fondamentaux, puis conçu Olvid pour y répondre. Pas l'inverse.**

Les résultats

La note de chaque application de messagerie pour chaque critère

Critère	Olvid	Signal	WhatsApp	Telegram	Basées sur Matrix*	SimpleX	Threema
Chiffrement de bout en bout	✓	✓	✓	✗	⚠	✓	✓
Authentification de bout en bout	✓	✗	✗	✗	✗	✗	✗
Sécurité de bout en bout	✓	✗	✗	✗	✗	✗	✗
Pas de substitution d'identité	✓	✗	✗	✗	✗	✓	✓
Client open source	✓	✓	✗	✓	✓	✓	✓
Multi-appareil de bout en bout	✓	✓	✓	✗	✗	⊖	✓
Données personnelles minimales	✓	✗	✗	✗	✗	✓	⚠
Pas de découverte d'utilisateurs ni de spam	✓	⚠	✗	✗	✗	✓	⚠
Chiffrement post-quantique	✗	✓	✗	✗	✗	⚠	✗

prévu pour 2027

Légende : ✓ Bon ⚠ Partiel ✗ Mauvais ⊖ Non applicable

* Element, Tchap, Citadel...

Pour apprécier ce tableau, il faut comprendre chaque critère, que nous résumons plus bas en précisant ce qu'il garantit et ce à quoi l'on s'expose sans lui. Chaque résumé est complété par une page dédiée qui explique plus précisément en quoi ce critère est essentiel à la sécurité d'une messagerie. Une page dédiée liste quelques-uns des critères que nous avons écartés en expliquant pourquoi nous l'avons fait. Enfin, chaque application est analysée en justifiant, critère par critère, les résultats que nous lui attribuons.

Les critères

Chiffrement de bout en bout

CE QUE CE CRITÈRE GARANTIT : Vos messages sont chiffrés avant de quitter votre appareil, et seuls les détenteurs des clés pour lesquelles ils ont été chiffrés peuvent les lire. Reste à s'assurer que ces clés sont bien celles de vos correspondants (c'est l'objet du critère Authentification de bout en bout).

SANS LUI : Toute personne ayant accès au serveur (opérateur, pirate, autorité) peut lire l'intégralité des conversations.

Authentification de bout en bout

CE QUE CE CRITÈRE GARANTIT : Vous êtes systématiquement certain de l'identité de la personne à qui vous écrivez, sans devoir croire l'opérateur sur parole.

SANS LUI : L'opérateur, ou quiconque le compromet, peut se faire passer pour n'importe lequel de vos contacts, et le chiffrement ne vous en protège pas.

Sécurité de bout en bout

CE QUE CE CRITÈRE GARANTIT : Vous savez à qui vous parlez, et vous savez que personne d'autre ne peut écouter, pas même l'opérateur. Autrement dit, vous avez une réelle conversation privée.

SANS LUI : L'une des deux garanties manque, et l'autre perd l'essentiel de sa valeur. Un chiffrement parfait vers la mauvaise personne ne protège rien.

Pas de substitution d'identité

CE QUE CE CRITÈRE GARANTIT : La confiance établie avec un contact reste valable dans le temps ; son identité ne peut pas être remplacée silencieusement.

SANS LUI : Une malveillance de l'opérateur, ou dans certains cas l'interception d'un simple SMS, suffit à prendre le contrôle d'un compte et à se substituer à son propriétaire auprès de tous ses contacts.

Client open source

CE QUE CE CRITÈRE GARANTIT : Les promesses de sécurité de la messagerie sont vérifiables par un tiers.

SANS LUI : Impossible de confirmer que l'application fait réellement ce qu'elle annonce ; il faut croire l'éditeur sur parole.

Multi-appareil de bout en bout

CE QUE CE CRITÈRE GARANTIT : Vous utilisez votre profil sur tous vos appareils, et seul un appareil déjà légitime peut en autoriser un nouveau.

SANS LUI : Soit vous êtes limité à un seul appareil par compte, soit c'est le serveur qui décide quels appareils reçoivent vos conversations, et rien ne l'empêche d'en ajouter un qu'il contrôle.

Données personnelles minimales

CE QUE CE CRITÈRE GARANTIT : L'opérateur ne sait rien de vous. Une donnée qu'il ne détient pas ne peut être ni piratée, ni revendue.

SANS LUI : Votre messagerie est reliée à votre identité réelle, et ce lien est exposé aux fuites et aux recoupements.

Pas de découverte d'utilisateurs ni de spam

CE QUE CE CRITÈRE GARANTIT : Personne ne peut vous trouver ni vous solliciter sans que vous l'ayez voulu.

SANS LUI : Quiconque connaît votre numéro peut vous contacter : spam, hameçonnage et, dans les pires cas, attaques ne nécessitant aucune action de votre part.

Chiffrement post-quantique

CE QUE CE CRITÈRE GARANTIT : Vos échanges enregistrés aujourd'hui ne pourront pas être déchiffrés demain, le jour où un ordinateur quantique suffisamment puissant existera.

SANS LUI : Un adversaire qui enregistre aujourd'hui vos communications chiffrées pourra les déchiffrer rétroactivement dès qu'il disposera d'un tel ordinateur.



LIRE LA SUITE

benchmark.olvid.io

Une remarque, une correction, une suggestion ? Écrivez-nous à benchmark@olvid.io.

© 2026 Olvid · Sauf mention contraire, le contenu de ce site est sous licence CC BY-ND 4.0. · 1er octobre 2026