

Signal

	Service contains risks and is suitable for some use cases. (Read more)
	The service is produced entirely or partly outside EU/ETA area. The customer is responsible for fulfillment of European data privacy and information security requirements. (Read more)

Signal

<https://signal.org/>

Signal is an encrypted communications application for Android, iOS, mac, Windows and Linux platforms. It uses the Internet to send one-to-one and group messages, which can include images and video messages, and make one-to-one voice and video calls. Signal uses standard cellular mobile numbers as identifiers, and uses end-to-end encryption to secure all communications to other Signal users.

Signal is the successor of an encrypted voice calling app called RedPhone and an encrypted texting program called TextSecure, after 2015 it has been called Signal. Signal is developed by Open Whisper Systems. Source code of Signal is published under [GPLv3](#) license.

Terms of service & Privacy policy

- TOS: (version: Updated May 25, 2018) <https://signal.org/legal/#terms-of-service>
- Privacy policy: (version: Updated May 25, 2018) <https://signal.org/legal/#privacy-policy>

Evaluation (23 December 2020)

- + End to end encryption
- + Interoperability with other messaging software
- + Encryption for messages and phone calls
- + The complete source code of the Signal clients is available on GitHub under a free software license
- + Free licensing enables interested parties to examine the code
- + Possibility for Group Conversations
- + Enclosing Multimedia is possible
- Signal demands that the primary device is a Android or iOS phone, with an Internet connection

Login

- Login happens with one's mobile number. The service will be activated via SMS. The service is used via the mobile app.
- Signal demands that the primary device is a Android or iOS phone, with an Internet connection

Support

- <https://support.signal.org/hc/en-us>

Service Provider

- Signal.org <https://signal.org/>

- Signal is developed by a software group called Open Whisper Systems. The group is funded by a combination of donations and grants, and all of its products are published as free and open-source software.

Similar services

- WhatsApp, Telegram, Chatsecure, Bleep

Common notes:

In this service Mobile Apps will send so called end to end (forward secrecy, end-to-end), encrypted messages, service quite is alike with WhatsApp, which is probably more known by public. Service is well protected for Man-In-the-Middle attacks and eavesdropping.

Revenue logic: The group is funded by a combination of donations and grants and crowd funding, and all of its products are published as free and open-source software. Different Foundations also support Open Whisper System. Technical description of Signal can be found: <http://support.whispersystems.org>

Security and Privacy: All program code can be reviewed at GitHub. Signal may be the only one this kind of software, which code can be reviewed entirely (including Proxy Servers. ?)

Service uses centralized Proxy Server which transmits messages and checks from users address book if communication contacts are using Signal. Location and composition of Proxies are not available, probably those are in U.S but messages stay encrypted in transmission. Some data for example time stamps, public encryption key, PUSH-ID and IP address may be captured by authorities.

Possible communication companies are compared using users address books from mobile phones and users address books from Signal's customer database. Comparison algorithm is said to be one way procedure in a way users address book can not be exposed from server.