---

title: SimpleX platform

revision: 07.02.2023

| Updated 07.02.2023 | Languages: EN, FR, CZ |

SimpleX platform - motivation and comparison

Problems

Existing chat platforms and protocols have some or all of the following problems:

- Lack of privacy of the user profile and contacts (meta-data privacy).
- No protection (or only optional protection) of E2EE implementations from MITM attacks via provider.
- Unsolicited messages (spam and abuse).
- Lack of data ownership and protection.
- Complexity of usage for all non-centralized protocols to non-technical users.

The concentration of the communication in a small number of centralized platforms makes resolving these problems quite difficult.

Proposed solution

Proposed stack of protocols solves these problems by making both messages and contacts stored only on client devices, reducing the role of the servers to simple message relays that only require authorization of messages sent to the queues, but do NOT require user authentication - not only the messages but also the metadata is protected because users do not have any identifiers assigned to them - unlike with any other platforms.

See SimpleX whitepaper for more information on platform objectives and technical design.

Why use SimpleX

SimpleX unique approach to privacy and security

Everyone should care about privacy and security of their communications - even ordinary conversations can put you in danger.

Full privacy of your identity, profile, contacts and metadata

Unlike any other existing messaging platform, SimpleX has no identifiers assigned to the users - it does not use phone numbers (like Signal or WhatsApp), domain-based addresses (like email, XMPP or Matrix), usernames (like Telegram), public keys or even random numbers (like all other messengers) to identify its users - we do not even know how many people use SimpleX.

To deliver the messages instead of user identifiers that all other platforms use, SimpleX uses the addresses of unidirectional (simplex) message queues. Using SimpleX is like having a different email address or a phone number for each contact you have, but without the hassle of managing all these addresses. In the near future SimpleX apps will also change the message queues automatically, moving the conversations from one server to another, to provide even better privacy to the users.

This approach protects the privacy of who are you communicating with, hiding it from SimpleX platform servers and from any observers. You can further improve your privacy by configuring your network access to connect to SimpleX servers via some overlay transport network, e.g. Tor.

The best protection against spam and abuse

As you have no identifier on SimpleX platform, you cannot be contacted unless you share a one-time invitation link or an optional temporary user address. Even with the optional user addresses, while they can be used to send spam contact requests, you can change or completely delete it without losing any of your connections.

Complete ownership, control and security of your data

SimpleX stores all user data on client devices, the messages are only held temporarily on SimpleX relay servers until they are received.

We use portable database format that can be used on all supported devices - we will soon add the ability to export the chat database from the mobile app so it can be used on another device.

Unlike servers of federated networks (email, XMPP or Matrix), SimpleX servers do not store user accounts, they simply relay messages to the recipients, protecting the privacy of both parties. There are no identifiers or encrypted messages in common between sent and received traffic of the server, thanks to the additional encryption layer for delivered messages. So if anybody is observing server traffic, they cannot easily determine who is communicating with whom (see SimpleX whitepaper for the known traffic correlation attacks).

Users own SimpleX network

You can use SimpleX with your own servers and still communicate with people using the servers that are pre-configured in the apps or any other SimpleX servers.

SimpleX platform uses an open protocol and provides SDK to create chat bots, allowing implementation of services that users can interact with via SimpleX Chat apps – we are really looking forward to see what SimpleX services can be built.

If you are considering developing with the SimpleX platform, whether for chat bot services for SimpleX app users or to integrate the SimpleX Chat library into your mobile apps, please get in touch for any advice and support.

Comparison with other protocols

	SimpleX chat	Signal, big platforms	XMPP, Matrix	P2P protocols
Requires user identifiers	No = private	Yes[1]	Yes[2]	Yes[3]
Possibility of MITM	No = secure	Yes[4]	Yes	Yes
Dependence on DNS	No = resilient	Yes	Yes	No
Single operator or network	No = decentralized	Yes	No	Yes[5]
Central component or other network-wide attack	No = resilient	Yes	Yes[2]	Yes[6]

1. Usually based on a phone number, in some cases on usernames.
2. DNS based.
3. Public key or some other globally unique ID.
4. If operator's servers are compromised.
5. While P2P networks and cryptocurrency-based networks are distributed, they are not decentralized - they operate as a single network, with a single namespace of user addresses.
6. P2P networks either have a central authority or the whole network can be compromised - see the next section.

Comparison with P2P messaging protocols

There are several P2P chat/messaging protocols and implementations that aim to solve privacy and centralisation problem, but they have their own set of problems that makes them less reliable than the proposed design, more complex to implement and analyse and more vulnerable to attacks.

1. P2P networks use some variant of DHT to route messages/requests through the network. DHT implementations have complex designs that

have to balance reliability, delivery guarantee and latency. The proposed design has both better delivery guarantees and lower latency (the message is passed multiple times in parallel, through one node each time, using servers chosen by the recipient, while in P2P networks the message is passed through `O(log N)` nodes sequentially, using nodes chosen by the algorithm).

2. The proposed design, unlike most P2P networks, has no global user identifiers of any kind, even temporary.

3. P2P itself does not solve MITM attack problem, and most existing solutions do not use out-of-band messages for the initial key exchange. The proposed design uses out-of-band messages or, in some cases, pre-existing secure and trusted connections for the initial key exchange.

4. P2P implementations can be blocked by some Internet providers (like BitTorrent). The proposed design is transport agnostic - it can work over standard web protocols, and the servers can be deployed on the same domains as the websites.

5. All known P2P networks are likely to be vulnerable to Sybil attack, because each node is discoverable, and the network operates as a whole. Known measures to reduce the probability of the Sybil attack either require a centralized component or expensive proof of work. The proposed design, on the opposite, has no server discoverability - servers are not connected, not known to each other and to all clients. The SimpleX network is fragmented and operates as multiple isolated connections. It makes network-wide attacks on SimpleX network impossible - even if some servers are compromised, other parts of the network can operate normally, and affected clients can switch to using other servers without losing contacts or messages.

6. P2P networks are likely to be vulnerable to DRDoS attack. In the proposed design clients only relay traffic from known trusted connection and cannot be used to reflect and amplify the traffic in the whole network.