Session Private Messaging Review
A Private Messaging Solution
19 January 2021

It protects your metadata, encrypts your communications, and makes sure your messaging activities leave no digital trail behind.

Bottom line

Session is the only messaging app the author has found that's end-to-end private encrypted, easy to use, multi-platform and highly decentralized without any central company or other attack vulnerability. It's only serious problem is the limited private group size, for now, but this can be worked around somewhat. The Lokinet implementation should soon allow this to be resolved.

Discussion

For the first time since last April, Session (formerly Loki) private messaging was revisited after Robert Braxman mentioned it recently in "Best Secure Instant Messaging Apps for 2021" at https://lbry.tv/@RobBraxmanTech:6/message-final:9

I highly recommend checking it out. Most questions are answered in their FAQ at GetSession.org/faq/

Below is my review for Linux, Android and Windows 7 installs

Installed the latest Session from GetSession.org on a Linux laptop. It was incredibly easy using the AppImage file which is also used to open the app. Instructions about what to do with this type of executable file are at AppImage.org (example for file named Subsurface*.AppImage). It would be nice to have in an obvious instruction link by the Linux download link. I renamed Session's AppImage file to something easy to enter at the command prompt after changing to that directory. The terminal screen remains open with Session node activity streaming.

Secret messaged my user ID found in my profile (icon at upper left) to a few skilled friends along with the install link. After receiving their first message, their user ID was available to save as a contact within the program. It took a moment to find the message entry field in the lower right.

Sending voice messages is easy after entering settings/privacy to enable mic access. Select the microphone icon left of the text entry and the voice window appears with the mic rolling. To end the message, select the mic icon again. Then you will have the send icon available to the left of the text entry field. There are no volume controls within the program.

The limit is 20 users in a closed group. This will increase very soon. Meanwhile, a work around would be for a larger group to be broken up into groups of 20 or less. A few users who are usually online could be in all of the groups and act as bridges, forwarding messages between groups. This is open source, so maybe someone will come out with a bot for this.

The **Android** setup has an option for "Fast Mode" through google notification servers which they say doesn't expose messages or who is messaged. I'm not comfortable with that and went with "Slow Mode" with full metadata protection. "Slow" was about 20-seconds to receive a short voice message.

The recovery phrase is not automatically displayed and can be copied while offline later from the settings screen. Have a session ID from someone, or Session on another device, ready to paste in for your first message. From there it’s pretty straightforward.

The **windows** setup is very easy, bypassing the recovery phrase copying which is available in the setup screen. Select + at the top, paste the receiving Session ID, and it’s ready to send. A pretty nice user interface.

Note: Session IDs are not currently shared across devices. They did, but had issues. This is a high priority feature to resume.

Overall, I’m happy with the user experience. The level of privacy and high decentralization which Session achieves is outstanding. I encourage people to try it out. PrivacyTools evaluation has been requested for its recommendation. In the Session FAQ it states, “Session’s desktop, Android, and iOS clients are currently undergoing a security audit by Quarkslab. The results of the audit will be published once it is completed.”

If I know you, you can secret message me on Telegram or Signal for my Session ID.

Mike Silver