Testing & Evaluation Sheet

Signal

1. Tool Overview

Name:	Signal
Category:	Communication, Privacy
Purpose:	Secure messaging app designed to provide end-to-end encrypted communication, allowing users to send messages, make voice and video calls, and share files while maintaining privacy and security.
Date	3/27/2025
Status:	Deployed ☑ Operational - Actively running/maintained □ In Testing - Currently being evaluated or piloted □ Inactive/Deprecated - No longer maintained or functional
Deployment Architecture:	□ A standalone software - Runs entirely locally (e.g., runs on computer and doesn't depend on external server) □ A locally hosted service with separate server and client component - Run both backend/frontend yourself (e.g., backend could be on a local network, or self-hosted on cloud) ☑ A service with a local client that's hosted by a third party - You install a client on your device, but it connects to and depends on a remote server (e.g., Signal: install app (client), but Signal's servers handle message relaying, etc.) □ A service that is hosted by a third party but can also be self-hosted
Version:	V. 7.51.0.0

2. Installation & Setup

OS Compatibility	Signal is available for Android, iOS, Windows, macOS, and Linux and can be downloaded from their respective app stores or official sources. (To use the Signal desktop app, Signal must first be installed on your phone)
Installation Manual:	Yes

Installation Steps:	● Provided download instructions: https://signal.org/download/ ● Step by step instructions here: https://docs.cryptomator.org/desktop/getting-started/ ● Creating an account on your phone is simple—just follow the on-screen instructions. ● A QR code appears when linking your Signal account from your phone to the desktop version.
Mention if command-line setup or special configurations are needed	For End Users (Windows/macOS/Linux/Android/iOS): - No command-line setup or special configuration is required. Installation is done via app stores or official website with a simple graphical installer. For Developers or Advanced Users: - Command-line tools may be used to build from source or interact with Signal services (e.g., Signal-CLI for sending messages via terminal). This requires Java and configuration of your environment. Self-Hosting: - Hosting Signal's full backend services is not publicly supported due to complexity and reliance on Signal's centralized infrastructure.
Common Installation Issues & Fixes:	N/A
User Documentation:	Yes
Required Technical Knowledge	Beginner

3. Testing & Evaluation

Category	Details	Score
Operational Functionality:	**Functionality** ● No bugs or broken features noticed **Internet Dependence:** ● It does not have offline functionality ● Messaging and Voice Calls: Signal will work on 2G and 3G networks for text messages and voice calls. However, voice call quality may be significantly affected on 2G, as it has much lower bandwidth compared to 3G. 3G can handle basic voice calls reasonably well, but the performance may still degrade compared to 4G or Wi-Fi.	4.7

	● 5G or LTE works perfectly fine, but dependent on file size **Localization & Language Support** ● There are 68 languages available, with English, Simplified & Traditional Mandarin **Mobile Accessibility** ● It is very mobile friendly, as one of their main selling points is that they have a phone version	
Usability for Non-Technical Users	**Ease of Installation & Deployment** ● Easy to install ● Installation is under 5 minutes **User Onboarding Experience** ● They provide installation guides ● They have an in depth FAQ page **Technical Experience Level Required** ● The interface is visual and menu-driven	5.0
Security & Privacy Strength	**Encryption Standards** ● End-To-End Encryption (E2EE) ● All attachments, images, files are encrypted before upload. ● Two Factor Authentication (2FA) ● Safety Numbers (Key Verification) ● Uses ZRTP (Zimmerman Real-Time Transport Protocol) for end-to-end encrypted key exchange (third parties can not intercept video/audio). ● Signal uses Sealed Sender: Hides user's identity for Signal servers (Signal doesn't even know who sent the message just that a message was sent) ● Only stores timestamps of when a user was last online with no other logs or details. **Censorship resilience** ● "Signal provides a built-in censorship circumvention feature and also includes support for a simple TLS proxy that can bypass these blocks in many circumstances and let people communicate privately" **Vulnerability: Its Resilience against known threats** ● Reviewed by independent organizations such as Cure53, Mozilla, and Electronic Frontier Foundation and constantly rated as one of the most secure messaging apps **Comparison with Known Standards**	5.0

	● Reviewed by independent organizations such as Cure53, Mozilla, and Electronic Frontier Foundation (EFF) and constantly rated as one of the most secure messaging apps. **Data Minimization** ● Does not store user messages, contacts, or conversation logs and only available data upon request is the date of the user's last connection. **Privacy Policy Accessibility and Clarity** ● They have a clear data handling policy, which is linked to the bottom of all of their webpages. ● https://signal.org/legal/#privacy-policy	
Maintenance/Sustainability	**Community support** ● They have a decently large community, with members posting multiple times per day ● https://community.signalusers.org/c/general/7 ● There is also a large reddit community where many people post **Development active status** ● Publicly available update logs in appstore ● Development team responds within anywhere from an hour to a day **Funding and Sponsorship** ● Donations from individuals ● $22,000,000 dollars in 2023	5.0
Performance / Effectiveness & Reliability	**Testing Environment Setup:** ● Device: Macbook Pro (14 inch, M4 Chip), 10-core CPU, 24 GB Memory ● OS: 15.2 Sequoia ● Network: Wifi **User Experience Observations** ● Signal runs smoothly on macOS with fast app launch and seamless synchronization across linked devices. ● High responsiveness during typical use—sending/receiving messages, media, and voice/video calls happen without noticeable delay. ● Clean and minimalist UI that's intuitive even for first-time users. ● Prompt and reliable message notifications, including read receipts and typing indicators. **Resource Usage:** ● Before Stress Testing ○ CPU: 0.05 - 0.08 % ○ Memory: 235 MB	5.0

	● After: ○ CPU: 8% ○ Memory: 324 MB **Network Performance:** ● Latency (Round-Trip Time - RTT): ● Min: 7.760 ms ● Avg: 13.110 ms ● Max: 19.892 ms ● Std Dev: 4.334 ms ● Packet Loss: 0.0% (All packets successfully reached the server and returned.) **Interpretation:** ● Low Latency: An average of 13.1 ms is very good, meaning Signal's servers respond quickly. ● Stable Connection: Minimal variation (4.3 ms standard deviation) suggests a reliable network. ● No Packet Loss: Ensures smooth messaging/calling with no dropped data. **Fast Local Network Response:** ● First few hops (inside Soochow University, Taiwan) have low latency (~2-10 ms). ● Network infrastructure is stable ● Efficient Routing Through TWIX (Taiwan Internet Exchange): ● Hops 6-10 go through 192.192.x.x (TWIX or other local ISPs). ● No unusual delays or bottlenecks in Taiwan. **Stable Latency:** ● The highest delay recorded was 23.77 ms (Hop 9). ● No signs of packet loss or excessive rerouting. **Reliability** ● Community is large and well reviewed ● Also been reviewed by 3rd party audits revealing no security flaws	
Deployment Considerations:	**Open Source & Transparency:** ● Yes, they have a github ● Anyone can verify Signal's implementation and cryptographic protocols. The code is open for scrutiny, and the cryptographic mechanisms it uses (such as the Signal Protocol for end-to-end encryption) have been widely reviewed by security	

	researchers. This transparency allows the community to review the code, find vulnerabilities, and contribute improvements. ● https://github.com/signalapp/Signal-Desktop **Cloud vs. Local Deployment:** ● Signal is already deployed ● Can be run locally on the users software **Dependencies:** ● Does not require dependencies **Post-Deployment Maintenance** ● Tool is easy to maintain ● There is a setting for automatic updates **Merge/Sustainability:** ● If you want to customize the E2EE or other layers of encryption, this gets more complicated as it could introduce new vulnerabilities ● Otherwise if you just want to add new features, this is easy to do as it's built on a modular architecture which makes it easier to understand the components and their interactions. This allows deployers and developers to modify specific parts of the code without affecting the entire application. For instance, if you want to modify the messaging functionality or user interface, you can do so by working within the specific modules that manage these aspects. ● It is very open to contributions, but it mentions to start small, as the PR requests that are more likely to be reviewed and accepted are the ones that make small, easily reviewed changes with clear and specific intentions.	
4. Testing Scenarios		
Scenario 1: Sending & receiving messages	● Was able to both send and receive messages including people in different countries ● Able to use emojis and reactions ● Able to create group chats ● Disappearing messages work as expected	
Scenario 2: Device Linking	● Able to link desktop signal to a phone. Able to use both softwares	

Scenario 3: Offline Sending Messages	● Able to draft messages offline, but not able to send messages [this is to be expected] ● Once getting back online, it is quick to send the message

5. Insights & Recommendations

Key Findings	**Strengths:** ● Strong security ● Minimal data collection ● 3rd party audited ● Multi-platform support **Weaknesses:** ● Centralized server ● No cloud backup ● Higher bandwidth usage due to encryption ● Might be blocked in some countries
Suggested Improvements	● User Interface Improvements: UI changes to improve clarity and navigation ● The user interface is intuitive and no changes are necessary ● Documentation: Step-by-step installation guides, tutorials for technical users ● Good documentation for installation ● Alternative Tools: [If better tools exist, list them] ● Since it is very difficult and complex to self-host there are other alternatives like Matrix (Element), Jitsi Meet, and Wire.
Alternative Tools:	Since it is very difficult and complex to self-host there are other alternatives like Matrix (Element), Jitsi Meet, and Wire.
License	GNU Affero General Public License
Cost/Resource Implications	**Total Cost of Ownership:** ● Limited time cost, as downloading it is simple ● Maintaining is simple and straightforward ● No subscriptions needed
Why is this useful to civil societies in authoritarian environments?	● Signal is freely available on Android, iOS, Windows, macOS, and Linux. It requires no technical expertise to install or use, and its visual interface is intuitive, which makes it usable for a wide range of activists ● Authoritarian governments often compel platforms to hand over user data or monitor communication logs. Signal is

	designed to store virtually no user data—it doesn’t keep chat histories, contact info, or conversation metadata. ● CSOs operating in high-risk environments often need to coordinate efforts across multiple members without compromising safety. Signal’s support for secure group chats, disappearing messages, and device verification through safety numbers helps ensure that only trusted individuals can access shared information. ● An activist in Tibet, working with an international human rights group, can use Signal to send interview transcripts, photos, and documents securely to colleagues abroad, without fear that Chinese authorities can intercept or trace the communication. Although China blocks Signal's servers, the app includes a built-in censorship circumvention feature using TLS proxies. These proxies disguise Signal traffic to look like normal HTTPS traffic (e.g., visiting a website), which helps bypass government firewalls. To use Signal in Tibet or elsewhere in China, the activist can set up the app with a proxy (provided by trusted contacts or Signal’s official community), and continue to message safely.