測試與評估表

Signal

1. 工具概述

姓名:	Signal
類別:	溝通、隱私
目的:	安全訊息應用程式旨在提供端對端加密通信，允許用戶發送訊息、進行語音和視訊通話以及共享文件，同時保持隱私和安全。
測試日期:	2025年3月27日
文件翻譯日期:	2025年8月16日
地位:	已部署 ☑ 營運中 - 積極運作/維護 ☐ 測試中 - 目前正在評估或試行 ☐ 不活躍/棄用 - 不再維護或運行
部署架構:	☐ 獨立軟體 - 完全在本地運行（例如，在電腦上運行並且不依賴外部伺服器） ☐ 具有獨立伺服器和用戶端元件的本機主機服務 - 自行執行後端/前端（例如，後端可以在本機網路上，也可以在雲端自行託管） ☑ 由第三方託管的本機用戶端服務 - 您在裝置上安裝用戶端，但它連接並依賴遠端伺服器（例如，Signal：安裝應用程式（用戶端），但 Signal 的伺服器處理訊息中繼等） ☐ 由第三方託管但也可以自行託管的服務
版本:	V. 7.51.0.0

2. 安裝和設定

作業系統相容性	Signal 適用於 Android、iOS、Windows、macOS 和 Linux 系統，可從各自的應用程式商店或官方管道下載。（要使用 Signal 桌面應用，必須先在手機上安裝 Signal）
安裝手冊:	Yes
安裝步驟:	● 提供下載說明：https://signal.org/download/

	● 此處有逐步說明：https://docs.cryptomator.org/desktop/getting-started/ ● 在手機上建立帳戶很簡單——只需按照螢幕上的指示操作即可。 ● 將您的 Signal 帳戶從手機連結到桌面版本時會出現QR Code。
提及是否需要命令列設定或特殊配置	對於最終用戶（Windows/macOS/Linux/Android/iOS）： - 無需命令列設定或特殊配置。安裝可透過應用程式商店或官方網站使用簡單的圖形安裝程式完成。 對於開發人員或進階使用者： - 命令列工具可用於從原始程式碼建置或與 Signal 服務互動（例如，用於透過終端機發送訊息的 Signal-CLI）。這需要 Java 和環境配置。 自託管： - 由於複雜性和對 Signal 集中式基礎架構的依賴，Hosting Signal 的完整後端服務未被公開支援。
常見安裝問題及修復：	不適用
使用者文件：	Yes
所需的技術知識	初學者

3. 測試與評估

類別	細節	分數
操作功能：	功能 ● 未發現任何錯誤或損壞的功能 網路依賴： ● 它沒有離線功能 ● 簡訊和語音通話：Signal 可在 2G 和 3G 網路上發送簡訊和撥打語音電話。然而，由於 2G 網路的頻寬遠低於 3G 網絡，因此語音通話品質可能會受到顯著影響。3G 網路可以很好地處理基本的語音通話，但與 4G 或 Wi-Fi 相比，其效能可能仍會有所下降。 ● 5G 或 LTE 運作良好，但取決於檔案大小 在地化和語言支持 ● 提供 68 種語言，包括英文、簡體中文和繁體中文 移動無障礙 ● 它非常適合行動設備，因為它們的主要賣點之一是有手機版本	4.7

非技術用戶的可用性	易於安裝和部署 ● 易於安裝 ● 安裝時間不到 5 分鐘 使用者入門體驗 ● 他們提供安裝指南 ● 他們有一個詳細的常見問題頁面 所需的技術經驗水平 ● 介面是可視化的，菜單驅動的	5.0
安全和隱私強度	加密標準 ● 端對端加密（E2EE） ● 所有附件、圖像、檔案在上傳前都經過加密。 ● 雙重認證（2FA） ● 安全號碼（金鑰驗證） ● 使用 ZRTP（Zimmerman 即時傳輸協定）進行端對端加密金鑰交換（第三方無法攔截視訊/音訊）。 ● Signal 使用密封寄件者：隱藏 Signal 伺服器的使用者身分（Signal 甚至不知道是誰發送了訊息，只是知道訊息已發送） ● 僅儲存使用者上次線上的時間戳，不儲存其他日誌或詳細資訊。 審查彈性 ● “Signal 提供了內建的審查規避功能，還支援簡單的 TLS 代理，可以在許多情況下繞過這些阻止並允許人們進行私密通信” 漏洞：抵禦已知威脅的能力 ● 經 Cure53、Mozilla 和電子前沿基金會等獨立機構審核，並持續被評為最安全的訊息應用程式之一 與已知標準的比較 ● 經過 Cure53、Mozilla 和電子前沿基金會 (EFF) 等獨立組織的審查，並持續被評為最安全的訊息應用程式之一。 資料最小化 ● 不儲存使用者訊息、聯絡人或對話日誌，且唯一可應要求提供的資料是使用者上次連線的日期。 隱私權政策的可近性和清晰度 ● 他們有明確的資料處理政策，該政策連結到所有網頁的底部。 ● https://signal.org/legal/#privacy-policy	5.0
維護/永續性	社群支持 ● 他們有一個相當大的社群，成員每天發布多次帖子 ● https://community.signalusers.org/c/general/7	5.0

	● 還有一個大型的 reddit 社群，許多人在那裡發布開發活躍狀態 ● 應用程式商店中公開的更新日誌 ● 開發團隊會在一小時到一天的時間內回應 資金和贊助 ● 個人捐款 ● 2023年為2,200萬美元	
性能/有效性和可靠性	測試環境設定： ● 設備：Macbook Pro（14 英寸，M4 晶片），10 核心 CPU，24 GB RAM ● 作業系統：15.2 Sequoia ● 網路：Wifi 使用者體驗觀察 ● Signal 在 macOS 上運作順暢，具有快速應用程式啟動和跨連結裝置無縫同步的功能。 ● 典型使用期間回應速度很快——發送/接收訊息、媒體和語音/視訊通話沒有明顯的延遲。 ● 簡潔的使用者介面，即使對於初次使用的使用者來說也很直覺。 ● 及時可靠的訊息通知，包括已讀回執和輸入指示器。 資源使用： ● 壓力測試前 ○ CPU：0.05 - 0.08% ○ 記憶體：235 MB ● 後： ○ CPU：8% ○ 記憶體：324 MB 網路效能： ● 延遲（往返時間 - RTT）： ● 最小值：7.760 毫秒 ● 平均：13.110 毫秒 ● 最大：19.892 毫秒 ● 標準差：4.334 毫秒 ● 資料包遺失：0.0%（所有資料包成功到達伺服器並返回。） 解釋： ● 低延遲：平均 13.1 毫秒非常好，這意味著 Signal 的伺服器回應速度很快。 ● 穩定連線：最小變化（4.3 毫秒標準差）表示網路可靠。 ● 無資料包遺失：確保訊息傳遞/通話順暢，無資料遺失。 快速本地網路回應：	5.0

	• 前幾跳（台灣東吳大學內）的延遲較低（~2-10 毫秒）。 • 網路基礎架構穩定 • 透過 TWIX（台灣網路交換中心）進行高效率路由： • 跳數 6-10 通過 192.192.x.x（TWIX 或其他本地 ISP）。 • 台灣沒有出現異常延誤或瓶頸。 穩定延遲： • 記錄的最大延遲為 23.77 毫秒（跳 9）。 • 沒有資料包遺失或過度重新路由的跡象。 可靠性 • 社群規模龐大，評價良好 • 也經過第三方審計，未發現任何安全漏洞	
部署注意事項：	開源與透明度： • Yes，有 github • 任何人都可以驗證 Signal 的實作和加密協定。其程式碼已開放供審查，其使用的加密機制（例如用於端對端加密的 Signal 協定）已得到安全研究人員的廣泛審查。這種透明性使社群能夠審查程式碼、發現漏洞並貢獻改進。 • https://github.com/signalapp/Signal-Desktop 雲端部署與本地部署： • 已部署 • 可以本地運行 依賴項： • 不需要依賴 部署後維護 • 工具易於維護 • 有一個自動更新的設置 合併/可持續性： • 如果您想自訂 E2EE 或其他加密層，這會變得更加複雜，因為它可能會引入新的漏洞 • 如果您只是想添加新功能，這很容易做到，因為它基於模組化架構，更容易理解元件及其互動。這使得部署人員和開發人員可以修改程式碼的特定部分，而不會影響整個應用程式。例如，如果您想要修改訊息傳遞功能或使用者介面，您可以在管理這些方面的特定模組中進行操作。 • 它對貢獻非常開放，但它提到從小處著手，因為更有可能被審查和接受的 PR 請求是那些做出小	

	的、易於審查的更改並具有明確和具體意圖的請求。	
4. 測試場景		
場景 **1**:發送和接收訊息	● 能夠發送和接收來自不同國家的人的消息 ● 能夠使用表情符號和反應 ● 能夠創建群聊 ● 消失的訊息按預期工作	
場景二:設備關聯	● 能夠連結桌面端或手機端。可以兩邊使用	
場景三:離線傳送訊息	● 可以離線起草訊息, 但無法發送訊息[這是可以預料的] ● 一旦恢復上線, 就可以快速發送訊息	
5. 見解和建議		
主要發現	優勢: ● 強大的安全性 ● 最少的資料收集 ● 第三方審核 ● 多平台支援 弱點: ● 集中式伺服器 ● 沒有雲端備份 ● 由於加密, 頻寬使用率更高 ● 在某些國家/地區可能會被屏蔽	
建議的改進	● 使用者介面改進:使用者介面改進以提高清晰度和導航 ● 使用者介面直觀, 無需更改 ● 文件:逐步安裝指南、技術使用者教學課程 ● 良好的安裝文檔 ● 替代工具:[如果有更好的工具, 請列出] ● 由於自架網站非常困難且複雜, 因此還有其他替代方案, 如 Matrix（Element）、Jitsi Meet 和 Wire。	
替代工具:	由於自架網站非常困難且複雜, 因此還有其他替代方案, 如 Matrix（Element）、Jitsi Meet 和 Wire。	
授權	GNU APGLv3	
成本/資源影響	總成本: ● 下載簡單, 時間成本有限	

	● 維護簡單直接 ● 無需訂閱
為什麼這對威權環境中的公民社會有用？	● Signal 在 Android、iOS、Windows、macOS 和 Linux 平台上均可免費使用。安裝和使用無需任何技術專業知識，其直覺的可視化介面使其適用於各類活動人士。 ● 專制政府經常強迫平台交出使用者資料或監控通訊日誌。Signal 的設計幾乎不儲存任何用戶資料——它不保存聊天記錄、聯絡資訊或對話詮釋資料。 ● 在高風險環境中工作的公民團體通常需要在不影響安全的情況下協調多名成員的工作。Signal 支援安全群組聊天、閱後即焚訊息以及透過安全號碼進行裝置驗證，有助於確保只有受信任的個人才能存取共享資訊。 ● 一位在西藏與國際人權組織合作的活動人士，可以使用 Signal 安全地向海外同事發送採訪記錄、照片和文件，而無需擔心中國當局攔截或追蹤通訊。儘管中國封鎖了 Signal 的伺服器，但該應用程式內建了使用 TLS 代理程式的審查規避功能。這些代理商會將 Signal 流量偽裝成正常的 HTTPS 流量（例如造訪網站），從而協助繞過政府防火牆。要在西藏或中國其他地區使用 Signal，該活動人士可以設定該應用程式的代理（由可信任聯絡人或 Signal 官方社群提供），並繼續安全地發送訊息。