測試與評估表	
Cryptomator	
1. 工具概述	
姓名:	Cryptomator
類別:	加密
目的:	為儲存在雲端的文件提供客戶端加密
測試日期	2025年4月22日
文件翻譯日期:	2025年8月14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:	V1.15.3
2. 安裝和設定	
作業系統相容性	Windows、macOS、Linux、Android、iOS
安裝手冊:	Yes
安裝步驟:	• 下載地址https://cryptomator.org/ • 標準安裝(基本使用無需高級配置) • 可選:透過套件管理器安裝(brew / apt)

提及是否需要命令列設定或特殊配置	無需命令列設置
常見安裝問題及修復:	● 安裝被 Microsoft Defender SmartScreen 或 macOS Gatekeeper 阻止 ○ 點選“更多資訊”>“繼續執行” ○ 或者, 在Windows 安全性 > 應用程式和瀏覽器控制 ● 缺少 Java 運行時或不相容的 JDK ○ 確保已安裝並正確配置 Java 17+ 或 JDK 23 ● Cryptomator 開啟時沒有可見介面或無回應選單 ○ 重置應用程式配置 ○ 刪除或重新命名使用者設定檔(例如 Cryptomator.cfg ○ Windows: %LocalAppData%\Cryptomator\Cryptomator.cfg ○ macOS:~/Library/Application Support/Cryptomator/
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 ● 測試步驟:使用所有主要功能驗證工具的核心功能, 追蹤任何故障或錯誤。 ☐ 該工具基本上無法使用, 存在許多損壞的功能和缺陷。 ☐ 一些功能損壞或出現錯誤 ☐ 小錯誤或問題 ☐ 基本功能正常, 幾乎沒有錯誤或沒有錯誤 ☑ 功能齊全, 無任何錯誤 網路依賴: ● 允許完全存取先前同步的保險庫和文件解密。 ● 加密和解密完全在本地進行。 在地化和語言支持 ● 提供超過 50 種語言版本, 包括中文(簡體和繁體)、日語和韓語。 ● 有一個活躍的開源社群做出貢獻。	5

	• 社群回饋會定期整合到發布版本中，並為語言包提供良好的版本支援。 移動無障礙 • 可作為 Android 和 iOS 的行動應用程式。	
非技術用戶的可用性	易於安裝和部署 • 一鍵下載，設定密碼後 • 有下載步驟的影片和圖片教學 • 3分鐘安裝。 使用者入門體驗 • 包括應用程式內工具提示和首次啟動應用程式時的簡短教學。 • 指導新用戶建立保險庫並加密文件 所需的技術經驗水平 • 在無需編程的用戶也可以安裝並開始使用該工具 • 介面是可視化的，菜單驅動的	4.3

安全和隱私強度	加密標準
	• E2EE 使用
	• AES-GCM（256 位元）：用於文件內容和文件頭加密。
	• ECDH-ES（橢圓曲線 Diffie-Hellman 暫時靜態）：用於金鑰交換，具體來說，以 JSON Web 加密（JWE）格式包裝使用者金鑰和裝置特定的機密。
	• PBES2-HS256+A128KW：用於從使用者密碼衍生帳戶金鑰（基於密碼的金鑰包裝）。
	
	已知強度彈性
	• 做不依賴中心化服務，允許私有/自架部署
	• 加密詮釋資料，提供一定程度的合理的否認。
	• 如果伺服器流量受到監控，詮釋資料外洩
	• 沒有內建的規避工具
	• 有任何已知的弱點或風險嗎？
	與已知標準的比較
	• 與業界標準高度一致：
	  • 使用 NIST 認可的演算法（AES-GCM、ECDH）
	  • 金鑰輪換和前向保密機制反映了最佳實踐
	
	資料最小化
	• 零知識架構
	隱私權政策的可近性和清晰度
		4.2

	● 僅收集必要的個人資料 ● 用戶可以請求存取、更正或刪除他們的資料。 ● 無第三方廣告追蹤器 ● 為法律和履行目的保留最少的必要資料	
維護/永續性	社群支持 ● 用戶可以在官方社群論壇上發布問題並獲得協助。 ● GitHub 問題：公開錯誤回報、功能請求和開發人員回復 ● 提供清晰、維護良好的指南和常見問題解答 ● 付費用戶（例如透過應用程式商店購買）可以獲得優先支援。 開發活躍狀態 ● 每週/每月更新 ● 快速回應的開發團隊 資金和贊助 ● Skymatic GmbH（核心開發公司）。 ● 用戶貢獻：直接捐贈、GitHub 贊助商和應用程式商店購買。 ● 沒有大型非政府組織或政府資助者 ● 下載量和每日用戶數均超過 39 萬	4.6
性能/有效性和可靠性	測試環境設定： ● 裝置**：**惠普 Envy x360 ○ 第 13 代Intel® i7 CPU ○ 16 GB RAM ● **Windows 11** ● 網路：4G網絡 使用者體驗觀察 ● 非常流暢，加載速度很快 速度和反應能力： ● 載入時間短，使用過程中無延遲 資源使用： ● 1% CPU 使用率 ● 138.0 MB RAM 網路效能： ● 不適用－該工具可離線用於加密文件 可靠性 ● Cryptomator 已接受知名網路安全公司 Cure53 的公開審計。2017 年 7 月，Cure53 對 Cryptomator 的核心庫進行了白盒加密審計。	4

	• Cure53 的總結論是 C密碼器攻擊面很小，不會對長期完整性造成威脅	
部署注意事項：	開源與透明度： • 完全開源 雲端部署與本地部署： • 在桌面和行動裝置上本地運行 • 不需要雲端基礎設施 • 對於雲端儲存集成，使用者必須安裝其雲端提供者的同步用戶端（例如 Dropbox、OneDrive）或透過 WebDAV 連線。 依賴項： • 使用 Java 和 JavaFX • 依賴關係在 GitHub 儲存庫 部署後維護 • 桌面和行動應用程式得到積極維護且易於更新 • 具有清晰的模組化結構，可進行分叉，因此修改起來相當容易 合併/可持續性： • 鼓勵透過 GitHub Discussions 進行社群討論和開發者參與	
4. 測試場景		
• 將文檔儲存在加密	• 使用 Cryptomator 建立新的保險庫 • 儲存各種文件類型（PDF、Word 文件、圖像） • 僅當保管庫解鎖時才可存取文件	
• 跨多個裝置的保險庫	• 在我的 iOS 裝置上安裝了 Cryptomator 應用程序，以測試跨平台的保險庫可訪問性。 • 為了將保險庫同步到 iOS 應用程序，我必須透過 Google Drive 連接它，因為行動應用程式需要基於雲端的保險庫 • 在 iOS Cryptomator 應用程式上同步我的 Google Drive 帳戶後，我就能夠在筆記型電腦上查看我建立的保險庫。 • 儘管它依賴雲端同步來訪問，但其可在桌面和行動平台之間互通	
5. 見解和建議		
主要發現	優勢： • 本機優先加密：客戶端加密意味著您的資料在到達雲端之前就已加密。	

	● 跨平台:適用於 Windows、macOS、Linux、Android 和 iOS。 ● 零知識:該應用程式永遠無法存取您的密碼 ● 如果密碼遺失, 允許恢復保險庫 弱點: ● 沒有內建同步;完全依賴第三方雲端同步客戶端 ● 行動付費功能:雖然桌面版本是免費的, 但 iOS 和 Android 應用程式需要購買 ● 需要在雲端儲存中手動建立保險庫
建議的改進	透過使用更強的密碼熵來改進預設設置
替代工具:	Veracrypt
授權	GPLv3
成本/資源影響	總成本: ● 桌面平台(Windows、macOS、Linux): ○ 免費使用**GPLv3** 授權 ● 移動平台: ○ Android:透過 Play Store 或 ProxyStore 購買付費應用程式(19.99 歐元, 含增值稅) ○ iOS:免費唯讀模式 ○ 完全存取權限 19.99 歐元(終身許可, 含增值稅)
為什麼這對威權環境中的公民社會有用?	● Cryptomator 對使用者裝置上的文件進行加密, 因此即使雲端基礎設施受到中國等專制政府的監控或破壞, 實際文件內容仍然無法存取。 ● Cryptomator 不需要註冊或基於雲端的登錄, 這意味著它不會將用戶活動與可識別的帳戶綁定 ● 它適用於 Windows、macOS、Linux、Android 和 iOS, 使公民團體能夠在不同裝置和平台上保護其文件 ● 由於所有加密和解密都在本地進行, 因此專制政權無法攔截傳輸中的資料或依賴雲端儲存中的後門 ● 由於 Cryptomator 不依賴集中式身份驗證伺服器或專有網絡, 因此政府更難阻止或破壞其使用