USE CASE - SECURE MESSAGING PLATFORM

比最安全的加密通訊更安全

μSD/X 整合安全通訊 App-Signal

守護行動裝置端點安全的μSD/X，以硬體 Micro SD 卡為基礎架構，能與安全通訊軟體整合，保護關鍵私鑰不外洩，強化安全性且無損通訊效率。本文以知名通訊軟體Signal實作整合，作為安全通訊用例。

通訊軟體 Signal 之安全機制

有別於其他即時通訊軟體 (Instant Messaging, IM)，Signal [1] 無論端點或伺服器都提供完整開源 (open source) 程式。使用者雙方透過伺服器互相溝通，搭配 X3DH (Extended Triple Diffie-Hellman) [2] 進行密鑰交換，私鑰毋須離開使用者環境也能各自計算出密鑰協議，有效降低私鑰外洩風險。此外，當雙方傳遞訊息時，每次對話都更換一次性密鑰 (One-Time Message Key)，即使該一次性密鑰被破解，過去的訊息、對方回應的訊息、未來再發送的訊息，這三者安全性都不受到影響。由於此演算法流程像是只能單向旋轉的棘輪，因此稱作雙棘輪演算法 (Double Ratchet Algorithm) [3]。

來自個人裝置的安全風險

雖然 Signal 加密機制設計完備，最重要的私鑰仍儲存於個人裝置內，導致此強調安全的開源程式仍存在許多風險。例如：其他應用程式後門與木馬程式竊取私鑰、作業系統本身安全性的隱憂、裝置運行時的功率消耗或電磁輻射等，相關物理特徵洩漏後，遭旁通道攻擊 SCA (Side-Channel Attack)，導致危害密鑰安全等。

而另一個容易成為駭客目標的，便是存放於 Signal 資料庫上完整的對話紀錄。Signal 的開源伺服器不存取任何使用者的通訊紀錄，所有紀錄皆被存放於使用者的個人裝置上。匯智安全科技研發團隊，根據 2019 年發表的國際期刊 [4] 實作後證實，可輕易取得手機內 KeyStore service 的資料庫內容，包含完整的對話紀錄。

μSD/X 保護核心密鑰與資料庫隱私

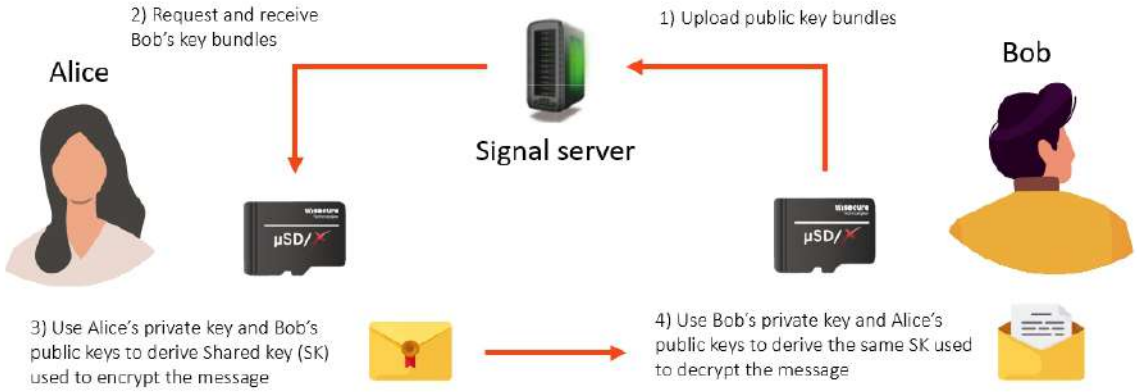
μSD/X 可輕鬆與 Signal 跨平台應用程式整合，將其私鑰儲存、密鑰交換、訊息加解密等服務，轉移至 μSD/X 的安全模組內。並且可將資料庫密鑰加密，確保該加密密鑰安全存放於 μSD/X 硬體內，不因前述的各種風險而被竊取。其內含「具備高防護能力之安全晶片 Infineon SLE 97 [5]」，並設計防範旁通道攻擊的演算法實作，包括 Signal 所採用之最新密鑰協議、新一代數位簽章標準 FIPS 186-5（橢圓曲線數位簽章 EdDSA)[6]、雙棘輪演算法等。使用者只要將 μSD/X 放入手機，便可在硬體防護的基礎之上，使用 Signal 進行安全通訊，亦能保護資料庫的對話紀錄安全。透過 μSD/X 管理私鑰完整生命週期，包括私鑰生成、配送、銷毀、簽章，並能抵禦旁通道攻擊，徹底保護密鑰與機敏訊息。

應用情境——µSD/X 如何確保密鑰安全

當 Signal 搭配 µSD/X 執行加密通訊服務時，初次啟動 µSD/X 即創建用於帳號綁定的身分密鑰 IK (Identity Key)、簽章準密鑰 SPK (Signed Prekey)、每次對話使用的一次性預共享密鑰 OPK (One-Time Pre Keys) 等。這些密鑰無法在未授權狀態下被取出，運算時毋須也無法離開 µSD/X 硬體。

假設 Alice 使用 Signal 加密通訊傳送訊息給 Bob，有µSD/X 支援之 Signal 加密通訊流程如下：

1. 為使用 X3DH 計算出共用密鑰進行通訊，Bob 首先將 IK、SPK 與 OPK(s) 三者所對應之公鑰所組成的公鑰組 (Key Bundle)，從µSD/X 匯出上傳 Signal 伺服器。
2. Alice 從 Signal 伺服器取得 Bob 公鑰組後，再使用 Bob 的公鑰組，和自己的私鑰一起代入 X3DH 演算法，在 µSD/X 中運算得出共用密鑰。
3. Alice 以此共用密鑰，將要傳送給 Bob 的機密訊息加密後，連同 Alice 自己的身分公鑰、隨機產生的一次性公鑰，一起傳給 Bob。Bob 用同樣方法計算出共用密鑰後，即可解密看見 Alice 訊息內容。



實際客戶案例

目前 µSD/X 已成功應用於客戶的加密通訊上，提供語音與數據通訊的密鑰交換與加解密服務，並使用美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 最新的橢圓曲線簽章標準 EdDSA。有別於市面上其他 mobile token，µSD/X 具備高效能加解密與高傳輸速度，可快速計算密鑰協議，保護密鑰安全。匯智安全科技因同時具備客製化演算法能力，成為客戶首選。

參考資料

[1] https://signal.org/#page-top
[2] https://signal.org/docs/specifications/x3dh/
[3] https://signal.org/docs/specifications/doubleratchet/
[4] Kamil KACZYŃSKI, "Security Analysis of Signal Arduino Database Protection Mechanisms,"International Journal on Information Technologies & Security, № 4 (vol. 11), 2019.
[5] https://www.infineon.com/cms/en/product/security-smart-card-solutions/security-controllers/sle-97/
[6] https://en.wikipedia.org/wiki/EdDSA

Wisecure Technologies