

SKI+ 即時通

本院覽號

公告日期

智財權狀態

32T-1080108

know-how

摘要

SKI+ 是跨平台手機即時通訊軟體。目前支援 IOS 和 Android 平台。設計與開發是將訊息的私密與安全性視為最優先考量。我們提供了點對點加密，公鑰加密對於一對一及群組通訊，拒絕來者通訊（設為黑名單）以及帳號轉移等功能。我們的加解密核心模組有1、可跨平台使用。2、密文資料格式及加解密工具要可版本化。3、核心模組的應用層須建立共同介面，並將不同平台介接實作獨立抽離在其它不同平台上組合使用。

技術優勢

- 相較於現有的即時通訊，包括科技大廠如(Facebook)或其它以安全性（國家）為主要訴求（如Threema, 宣稱伺服器的地點在瑞士境內），SKI+是以"可信賴的受託中介者"的角色，並以中央研究院為發展基地開始。
- 期望能以非營利且以使用者安全為主目標，以中研院資訊創新研究中心出品，讓使用者能產生信任感，即"可靠機構的信任機制"。畢竟目前所有以訊息安全性為考量的即時通，不只著重於資料安全的實作技術，也要讓使用者"信任"即時通的提供者不會將他們的資料外洩或作為其他營利用途。例如在金鑰的產生/交換/保存/銷毀, 在伺服器備份是否是加密，提供者可否有使用者的私鑰等。都是牽涉到"信任"的議題。

應用範圍

- 個人手機私密通訊。
- 公司商用機密通訊軟體。
- 線上雲端服務加強保密安全機制。
- 電子郵件附件保密防護機制。
- 個人資料及圖片、文件、影音保密防護傳送。

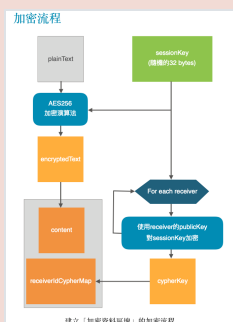


圖1.加密流程

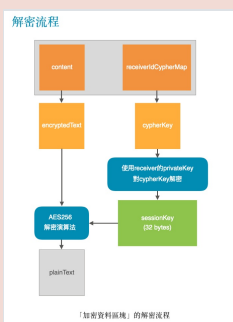


圖2.解密流程

創作人

李德財等



中央研究院
ACADEMIA SINICA