政大資科專題演講

端對端加密系統的安全性

April. 24, 2023

中研院資創中心 研究助技師 李政池

ziv@citi.sinica.edu.tw

即時通訊應用軟體 資安 事件（LINE為例）

- **[2021年05月03日]**

LINE爆資安漏洞　又有7家日企認了！用戶個資「讓中國隨意看」(https://www.ettoday.net/news/20210503/1973128.htm)

- **[2021年03月19日]**

日本LINE驚傳漏洞/駭客付錢就能攔截你的簡訊/ 難以根除的傀儡網路Emotet採用多層次網路架構/逾 100 萬台 iPhone 安裝 的通話錄音程式有竊聽漏洞
(https://blog.trendmicro.com.tw/?p=67477)

- **[2021年03月17日]**

日本 LINE 驚傳資安漏洞！中國工程師能偷看用戶訊息
(https://3c.ltn.com.tw/news/43609)

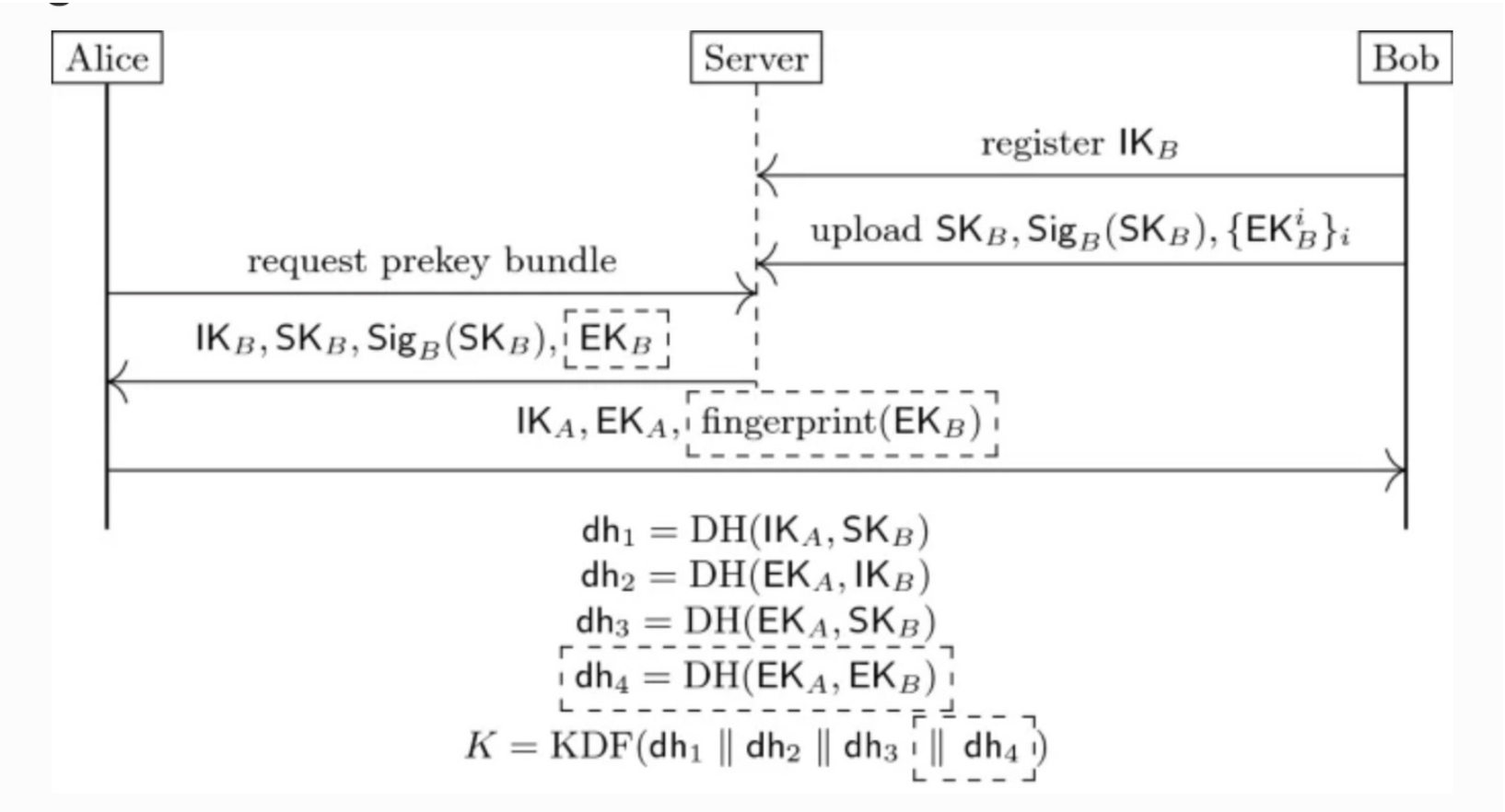
行動通訊 安全 隱憂

- 日本政府2021宣布擬停用 LINE
- 台灣明令禁止官方使用 WeChat、微信等中國開發產品
- 即時通訊軟體 Telegram、WhatsApp、Signal、FB、Twitter
- 台灣是 LINE 重度的使用者
- 資料外洩？
- What if 中國國企併購LINE!!

SKI+ Secure Messenger：On-Going Project

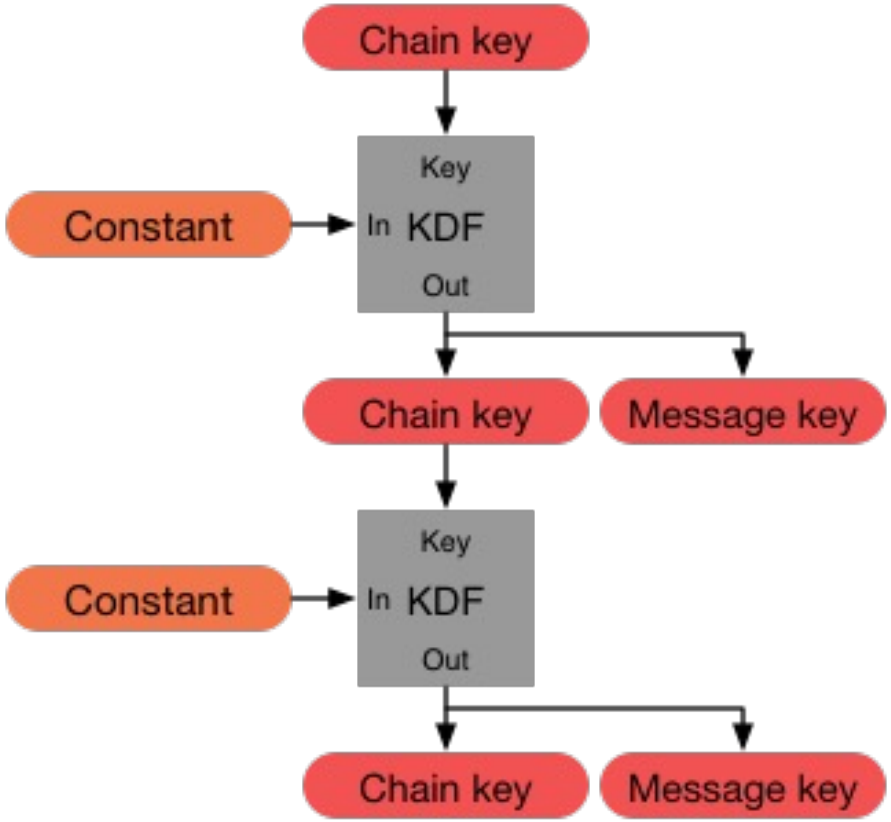
- **Design Goals**
  - Establish exclusively self-contained **core** technology for building end-to-end secure messaging system (SMS)
  - Design a software security module **(SSM)**, which is upgradable
  - Deploy the SMS server and provide end-to-end encryption service
- Subsystems
  - Cross-platform software security module design
  - Instant messaging server development
  - Android/iOS messaging application development
  - Desktop (PC) messaging application development
  - **Enterprise (on-premises) SMS**

X3DH Key Agreement Protocol

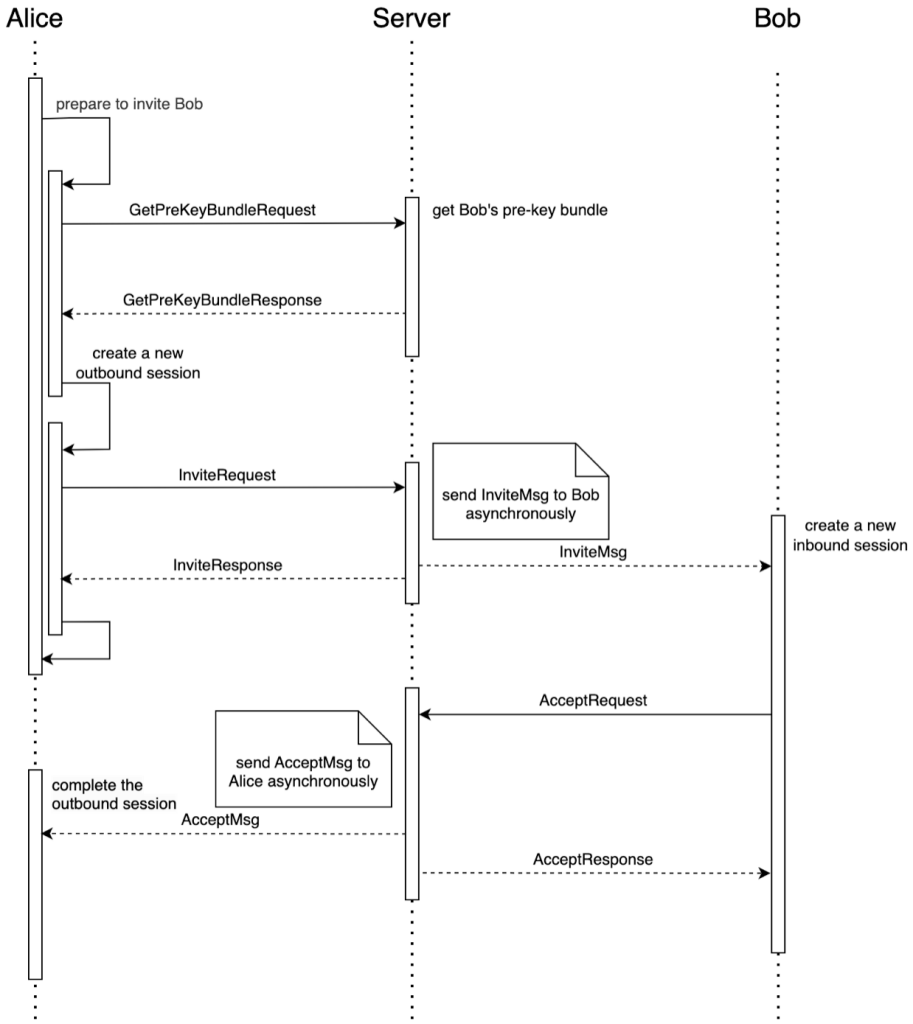


In the case of PQC:
apply SIDH(Supersingular Isogeny Diffie-Hellman protocol) ?

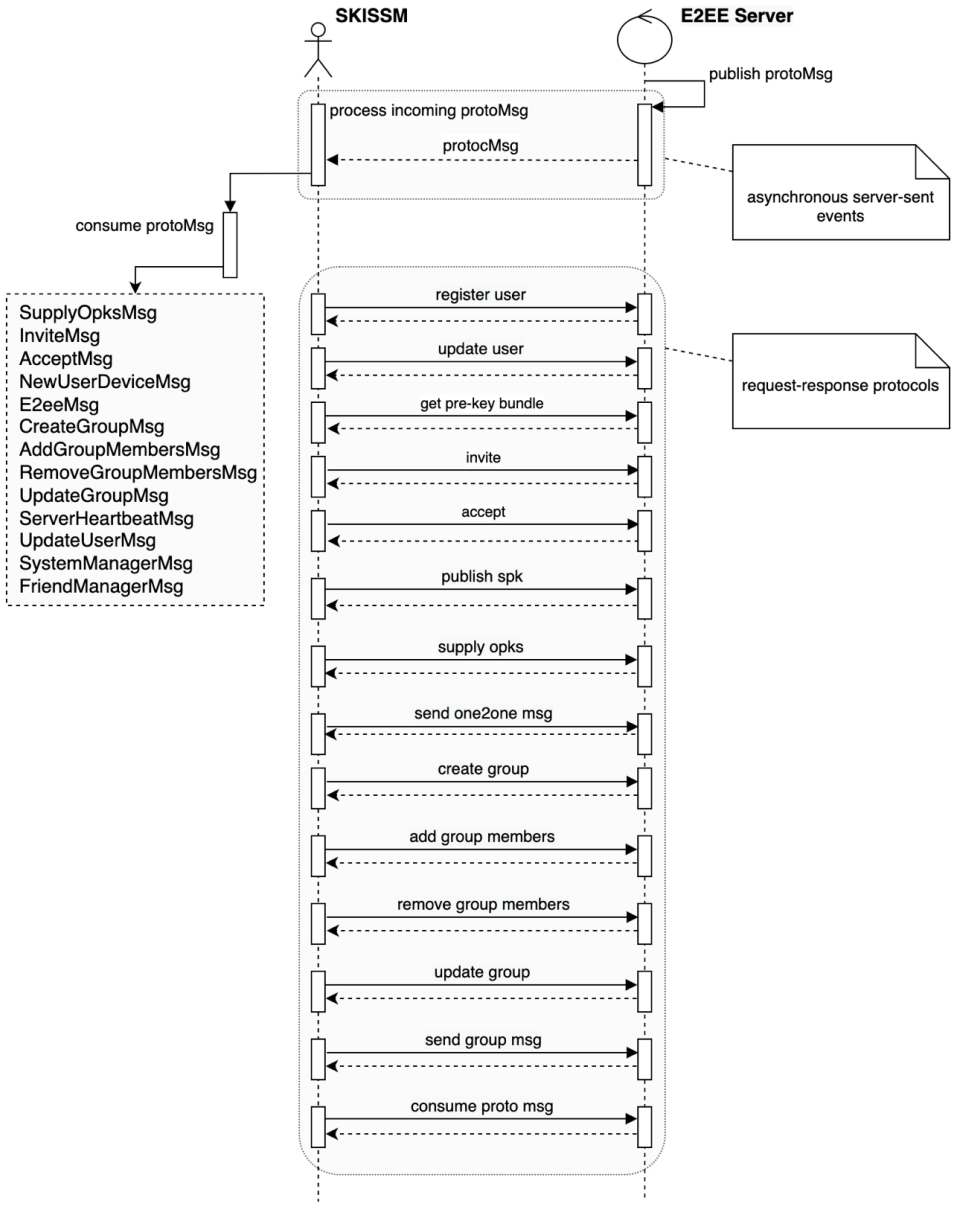
Double Ratchet Algorithm



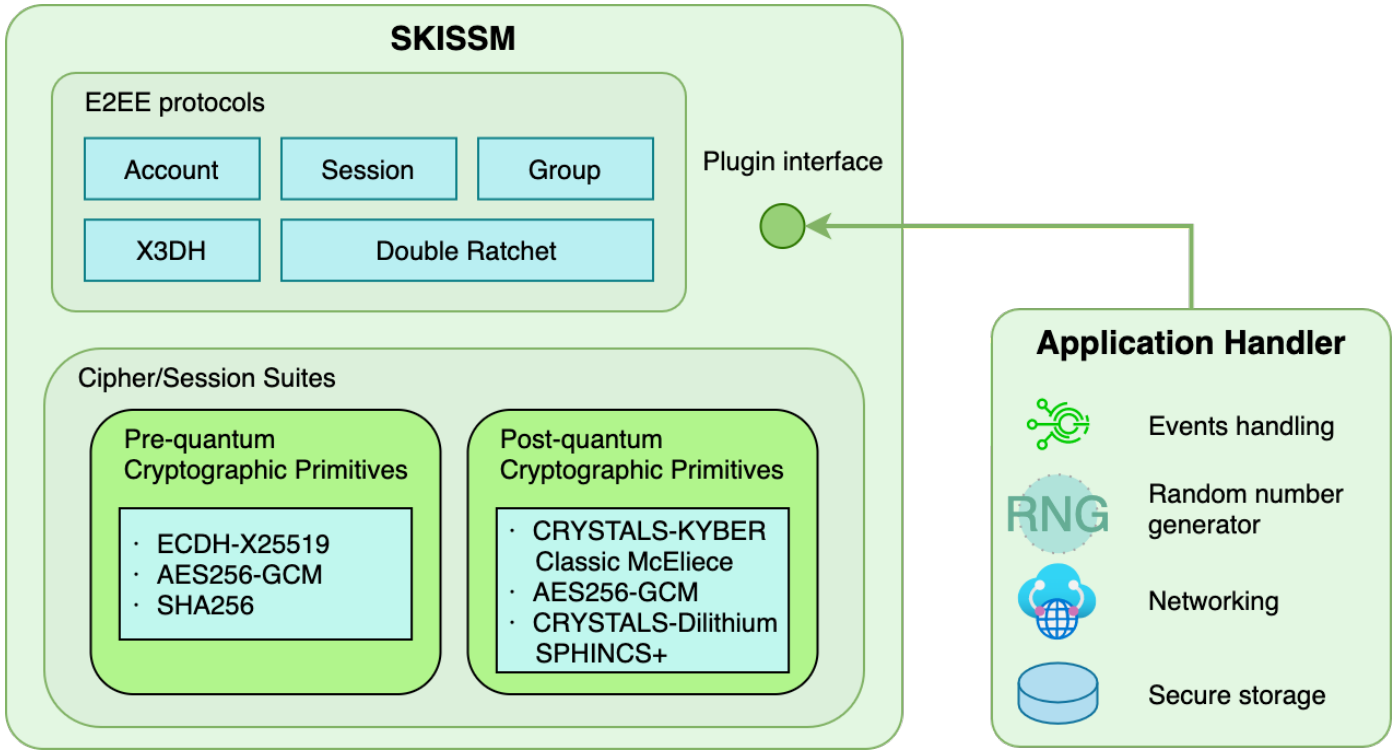
Invite and Accept Protocol



E2EE Protocols



開源 端對端 加密模組 SKISSM 軟體架構



- SKISSM GitHub project 網址
  https://github.com/ziv-e2eelab-org/skissm

SKI+

自主研發 MIT 產品

SKI+ 由中研院資創中心所開發的端對端加密通訊軟體， SKI+ 訊息的加密及解密計算均於終端設備(手機)完成，伺服器無法取得加解密細節，為一款國內開發對使用者隱私保障的通訊系統。

Play 商店　Apple Store　電腦版

SKI+ Secure Messenger is Online

Play Store

App Store

電腦版

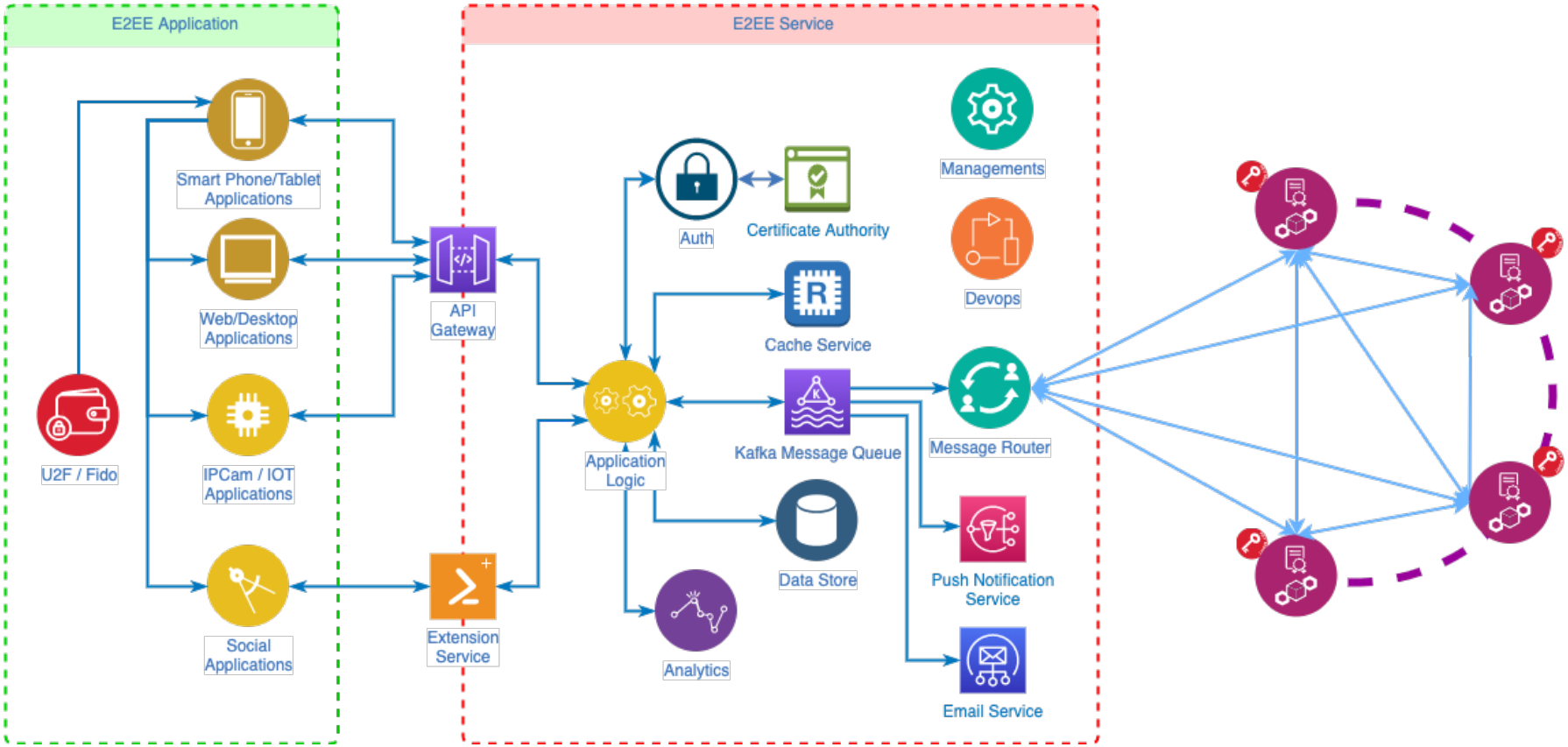
https://file.e2eelab.org/release/

Comparisons

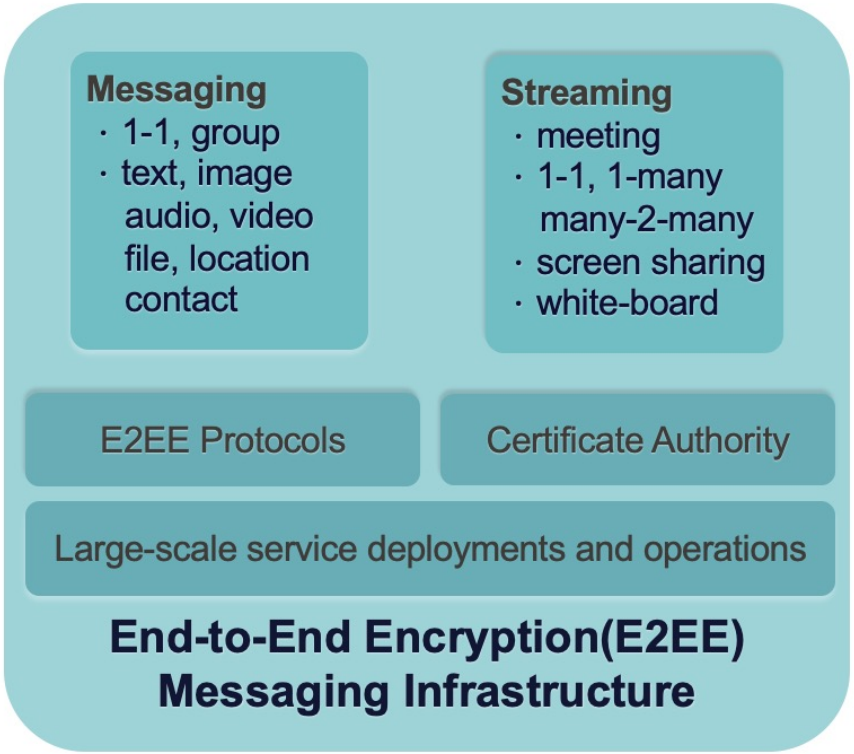
	Facebook	Line	Telegram	What's app	Signal	SKI+
E2EE support	yes, but manual	only for txt and voice streaming	yes, but manual	yes, by default	yes, by default	yes, by default
E2EE algorithm	unknown	Letter sealing	MTProto	Signal protocol	Signal protocol	SSM developed by Academia Sinica
Group message encryption	no	under 50 members	no	yes	yes	yes
Message backup	backup non-private chat	backup unencrypted messages	backup unencrypted messages	no	no	no
Open source	no	no	client	no	yes	in-preparation
Private key change notification	no	no	no	yes, but manual	yes, by default	change not allowed
Public key fingerprint verification	yes	yes	yes	yes for 1-1, not for group	yes	yes
Profit making organizations / funders	Facebook / analyze user data / adv.	Line / analyze user data / adv.	non-profit / Original founder / user donations	Facebook / analyze user data / adv.	non-profit / user donations	non-profit / Academia Sinica
Information provided upon government request for investigation	name, start date, last event time, ip, email	registration info, msg info, unencrypted message	ip, phone num	name, start date, last event time, ip, email	start date, last event time	ip, phone num

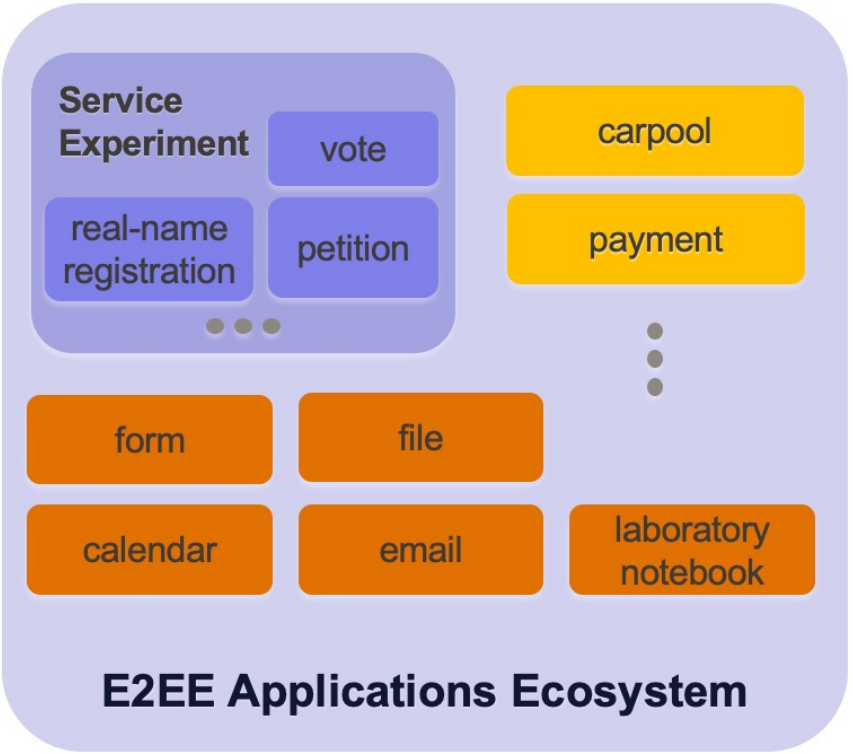
參考天下雜誌 (2020-07-09)
https://futurecity.cw.com.tw/article/1553

新版SKI+可延伸端對端加密微服務架構



E2EE Applications





端對端加密即時通 SKI+ 研發專案

成為開源的即時通訊軟體

歡迎共同 研究開發 SKI+專案

Thanks !  a