物聯智慧股份有限公司
ThroughTek Co., Ltd.

物聯智慧
資安白皮書

2023/06/30

目錄

1. 物聯智慧介紹

物聯智慧股份有限公司 (6565.TW，以下簡稱 TUTK 或本公司) 2008 年於台灣台北成立，為物聯網雲端服務平台解決方案商，積極致力於裝置連線技術與雲端服務平台開發。初期專注於開發設定容易、操作簡單之對點連線技術，主要應用於消費型影像監控產品之上。隨著物聯網浪潮興起，應用於多樣硬體產品之軟體連線解決方案需求持續增加，物聯智慧因累積了豐富的軟硬體整合經驗，進一步推出 Kalay 雲端服務平台，為欲投入物聯網發展之企業型客戶擴大服務範疇。

Kalay 雲端服務平台以優異的點對點(P2P)連線技術為基礎，可跨越各式作業系統運作，再以靈活而有彈性的模組化服務，協助品牌商或硬體製造商的產品延伸雲端應用附加價值。物聯智慧以核心之 Kalay 平台與全球主要 OEM/ODM 廠、品牌商、系統整合商，以至晶片商建立緊密合作關係，能因應不同類型客戶之需求，協助快速導入產品開發，加速產品上市時程，更能有效節省營運成本。Kalay 平台可開放 API 與第三方服務對接，使客戶擁有更多元的商業服務模式，現階段提供包含影像傳輸、雲端錄影、資料蒐集及分析、遠端控制及管理硬體裝置、訊息推播等十多種功能模組，可依照不同市場及客戶需求，彈性選擇方案組合。

圖: Kalay 雲端服務平台生態系

1.1 KALAY 雲端平台簡介

以點對點 (P2P) 連線技術為基礎，開發多種模組化功能為平台主幹，協助客戶以軟韌體整合開發各種物聯網產品，讓產品兼具操作簡易、連網穩定性及安全性。

Kalay 雲端平台廣泛應用於各種應用領域，可依客戶需求提供**客製化服務**、**專案服務**或為產品開發**應用程式(app)**，協助客戶的智慧產品或服務能快速進入消費市場。

此外，還可整合採用以 Kalay 雲端平台核心技術所開發之**雲端影像管理系統(Cloud VMS)**、**Hausetopia app**、或 **IoT 設備管理平台(DMP)** 等方案來豐富服務範疇。

1.2 KALAY 雲端平台主要特點

透過 Kalay 雲端平台，用戶可以建立一個可靠、安全、可彈性擴展的物聯網解決方案。它提供了設備連接、數據管理、應用開發和安全保護等關鍵

功能，幫助用戶更好地利用物聯網技術，實現智能化和高效的物聯網應用。Kalay 平台的主要功能包括：

- 設備連接與管理：Kalay 平台以優異的設備連線軟體技術為核心，提供了設備連接和管理的功能，使設備能夠與雲端平台快速進行連線和通訊。它支持多種通訊協議和連接方式，如 Wi-Fi、藍牙、Z-Wave、乙太網路等，以適應市場上各式類型多元的設備。
- 數據採集與分析：Kalay 平台可以從連接的設備中即時收集數據，並提供數據存儲和分析的能力。這使得用戶可以獲取設備生成的數據並進行深入分析，從中獲得有價值的資料洞察和決策支持。
- 應用開發與部署：Kalay 平台提供應用開發的工具和環境，使開發者能夠快速構建和部署物聯網應用程式。它支持多種開發語言和框架，並提供豐富的 API 和 SDK，讓開發者能夠輕鬆地整合和擴展功能。
- 安全與隱私保護：Kalay 平台注重安全和隱私保護，採用了多重安全措施來保護設備和數據的安全性。它提供身份驗證、數據加密、訪問控制等功能，以確保只有授權的用戶可以訪問和操作設備和數據。

2. 安全責任歸屬

保障用戶端及設備端的資料安全是一切雲端服務的根本，用戶使用手機控制裝置，端到端之間透過網路傳輸重要數據，TUTK 作為物聯網雲端平台服務的先驅者，必須為客戶嚴格把關，從雲端伺服器、軟韌體技術、加密驗證機制多重防護，本公司以最高標準落實數據安全保護，並持續關注和採用最新的安全技術和措施，以確保客戶的數據得到最佳的保護。

2.1 責任歸屬

TUTK 負責雲端平台之運營服務和數據交換的安全管理，並對雲端平台和伺服器的安全性負責。然，客戶若自行開發 app、自行架設/維護伺服器或

硬體對接本公司軟體技術(包含使用本公司 SDK)，則由客戶自行保障其應用及數據的安全性，包括硬體、伺服器和 app 的安全規範。除了下表內所列項目以外，由客戶自行負責。

類型	由 TUTK 託管、代管			
伺服器	阿里雲	Google Cloud	Amazon	IDC/Telecoms
責任	TUTK 與雲平台服務商共同承擔			
app、雲平台	TUTK 標準版及全功能客製化			
責任	TUTK 承擔			

2.2 TUTK 提供的安全責任

TUTK 使用全球知名的雲端主機服務商，例：Amazon, Google, 阿里雲...等公司，並且依據客戶需求來調配主機服務地區，以確保客戶的服務品質及設備連線的安全性。

此外，與各雲主機服務商共同合作，確保提供客戶的連線具有高度安全性，主要包含保護客戶數據的安全、避免漏洞利用和駭客攻擊、保證設備管理和升級的安全等。

另外有關用戶隱私資料，本公司了解客戶及用戶重視並關心自己的隱私權益，從物聯智慧提供的隱私保護政策說明文件了解本公司如何做到對客戶及用戶的承諾。

2.3 客戶自身的安全責任

當使用 TUTK 的解決方案時，客戶應嚴格遵守本公司的說明文件，配置安全和對接的要求。同時，客戶也必須確保其伺服器、客戶端或硬體產品本身的安全性。對於客戶採用 TUTK 的 SDK 所自行開發的 app/平台，本公司僅能提供技術支援，無法為其整體提供安全保障。對於 TUTK 代為修改

或客制化的 app/平台所涉及的數據安全、隱私政策聲明及法律規定等相關訊息，客戶必須自行負責。

3. TUTK 的國際合規及認證

TUTK 作為全球化的物聯網 (IoT) 雲端解決方案提供商，所提供的產品和服務均符合國際資訊安全合規和認證要求。以下為本公司的國際合規及取得之認證：

3.1 ISO/IEC 27001

ISO 27001 是國際標準組織 (ISO) 制定的資訊安全管理體系 (ISMS) 標準。透過該認證，證明本公司已建立和實施全面的資訊安全管理體系，該體系能夠確保本公司的資訊安全性、可用性和完整性。

ISO 27001 資安認證包括了以下三方面：

風險管理：通過評估和管理風險，能夠確保數據、系統和服務的安全性。

安全控制：確保系統和服務符合最新的安全控制要求，對未授權的存取和使用進行防範。

審計和監控：通過專門的審計和監控機制，確保資訊安全管理體系的持續有效性。

經由 ISO 27001 認證，TUTK 展現了其對客戶和合作夥伴在資訊安全方面的承諾和專業能力，也體現本公司在安全管理上的持續優化和改進，在國際上得到承認和接受。

3.2 GDPR（歐洲通用數據保護條例）

General Data Protection Regulation （歐洲通用數據保護條例，以下簡稱 GDPR）是歐盟於 2018 年 5 月 25 日實施的一項數據保護法規。它是一項旨在保護個人數據隱私和權利的法規，同時要求組織在處理和保護個人數據時遵守特定的法律要求。以下為幾個重要的規範：

數據保護：作為一家提供 IoT 和連接設備解決方案的公司，TUTK 可能處理和存儲大量的個人數據。根據 GDPR 規範，個人數據的處理需要符合特定的法律要求，包括合法性、透明性、目的限制、數據最小化、準確性和安全性等。透過遵守 GDPR 合規準則，本公司可以確保適當保護個人數據，減少數據洩露和違反隱私保護的風險。

用戶權利保護：根據 GDPR，個人數據主體擁有特定的權利，例如訪問、更正、刪除、限制處理和數據可攜性等。作為數據處理者，本公司可以實施相應的流程和控制措施，以確保用戶能夠有效行使其權利。這可以增加用戶對本公司的信任，並提高 TUTK 在遵守隱私和數據保護方面的形象。

風險管理：遵守 GDPR 可以幫助本公司進行風險評估和管理，並確保採取適當的技術和措施來保護個人數據免受未經授權的訪問、洩露或損壞。

3.3 CCPA（加州消費者隱私保護法）

California Consumer Privacy Act（加州消費者隱私法，以下簡稱 CCPA），於 2020 年 1 月 1 日生效。該法案旨在保護加利福尼亞州居民的個人資訊隱私權利。CCPA 為消費者提供了一些權利保障，包括：

訪問個人資訊：消費者可以向組織請求訪問他們收集的個人資訊。

刪除個人資訊：消費者可以要求組織刪除他們的個人資訊。

資訊披露：組織需要在收集個人資訊時提供有關其收集和使用目的的透明資訊。

不售出個人資訊 : 消費者可以選擇禁止組織將其個人資訊出售給第三方。

TUTK 遵守 CCPA 合規準則，即表示本公司已經採取了一系列措施，以確保客戶的個人資訊隱私得到充分的保護和尊重。落實符合 CCPA 的要求即展現本公司對客戶個人資訊隱私的重視，為客戶與用戶提供了額外的信心和保障。

3.4 其他

本公司對於資安合規非常重視，採取了一系列措施來確保客戶的數據和資訊安全。以下是本公司在資安合規方面的做法：

遵守相關法律法規：本公司遵循適用的資安法規，包括但不限於 GDPR（歐洲通用數據保護條例）、CCPA（加州消費者隱私法）和其他適用的隱私保護法律。

數據加密：本公司採用的數據加密技術可妥善保護數據在傳輸和存儲過程中的安全。通過使用加密協議和安全算法，本公司確保敏感數據的保密性和完整性。

訪問控制：本公司實施嚴格的訪問控制權管理措施，只有經過授權的員工才能訪問和處理客戶數據。本公司限制對數據的訪問權限，以確保僅有因執行業務所需的人員可經手處理相關數據。

安全審查與監控：本公司進行定期的安全審查和監控，以確保系統和網路受到及時的監控和保護。本公司監測潛在的安全威脅和異常活動，並採取相應的應對和防範措施。

員工培訓與意識：本公司提供全體員工必要的資安教育訓練，加強員工對於資安合規的意識和理解。本公司鼓勵員工遵守最佳的資安實踐，並定期充實其相關知識和技能。

通過這些資安合規措施，本公司公司致力於保護客戶的數據安全和隱私。本公司將繼續投入資源和努力，不斷改進本公司的資安措施，以應對不斷演變的威脅和風險。

4. TUTK 技術資安合規

技術資安合規是指確保公司在技術實施和運營中符合相關的安全法規和標準。以下是本公司在技術資安合規方面的做法。

4.1 安全開發實踐

本公司遵循安全開發生命週期（SDL）和最佳實踐，確保在軟體和系統開發過程中考慮安全性。本公司進行代碼審查和漏洞掃描，以減少潛在的安全漏洞和弱點。相關做法如下：

- 安全編碼准則：本公司制定了安全編碼准則，明確了在開發過程中應遵循的安全最佳實踐和規範。這包括輸入驗證、輸出編碼、安全配置和錯誤處理等方面的准則，以減少常見的安全漏洞。
- 安全審查：本公司進行代碼審查，以識別潛在的安全漏洞和弱點。透過定期的代碼審查，能及早發現和修復安全問題，確保代碼品質和安全性。
- 安全測試：本公司進行系統級和應用級的安全測試，包括黑盒測試和白盒測試等。透過模擬攻擊和安全漏洞的測試，可評估系統的安全性，以及時發現和修復潛在的漏洞。
- 安全培訓：本公司為技術開發團隊提供安全培訓，使他們瞭解常見的安全威脅和攻擊技術，並掌握相應的防禦措施。這有助於提高開發人員的安全意識和技能，以確保他們在開發過程中對於確保安全性能有周延的思慮。

4.2 身份驗證機制和訪問控制措施

本公司採用多重身份驗證機制，確保只有經過授權的用戶才能訪問系統和數據。本公司實施嚴格的訪問控制策略，包括角色和權限管理，以確保僅限於所需的權限。所有伺服器都需要 PKI 金鑰訪問，並且只發放給有限的人員或經授權的管理員。

- 24 小時自動/手動監控，以發現伺服器上的異常訪問和行為
- 全球不同地點的伺服器，確保沒有單點故障
- 定期更新系統，為潛在的安全漏洞更新
- 不斷測試和掃描任何意外漏洞

4.3 雲端存儲服務

本公司所運營的全球伺服器位於可信賴的雲服務提供商，包括 AWS、Google 和阿里雲...等。透過將伺服器托管在這些資料中心，能夠充分利用其先進的安全措施和嚴格的訪問政策，確保客戶數據的機密性和安全性。

TUTK 致力於採取最佳安全實踐，持續監控和更新系統及伺服器，以確保客戶數據得到最高水平的保護。包括定期評估和強化安全措施，採用加密技術保護數據的傳輸和存儲，實施嚴格的身份驗證和訪問控制措施，以及採取預防和應急措施應對潛在的安全威脅。

4.4 應用軟體

- 執行先進的 AWS 或 Softlayer 安全服務，提供攻擊檢測、預防和分析
- 對所有不必要的端口進行嚴格的基於規則的防火牆封鎖；只對特定的訪問協議開放
- 大規模的日誌分析，用於伺服器加固和資源優化
- 與趨勢科技安全服務的進一步合作

4.5 數據通訊

本公司在數據傳輸和安全方面採取了多種加密和保護措施，以確保設備與雲服務之間，以及雲之間的安全連接和數據傳輸。以下是本公司採用的安全措施：

- HTTPS 連接 : 使用 HTTPS 協議來保護通訊的安全性，確保設備與雲服務之間的通訊是經過加密的。通過在 HTTP 通訊上加密 SSL/TLS 協議層，保護數據在傳輸過程中的機密性和完整性。
- 資料加密：本公司採用 AES256 （Advanced Encryption Standard 256-bit）對稱加密算法，使用 256 位金鑰進行數據加密和解密。AES256 具有更高的金鑰長度和更強的安全性，廣泛應用於保護敏感數據的安全性。它通過多層加密操作來保護數據的機密性，並且需要正確的金鑰才能進行解密。
- 安全通訊 : 根據設備的能力和配置情形，可選擇使用 TLS 1.2 或 DTLS 1.2 進行安全通訊，TLS 1.2 和 DTLS 1.2 都是用於保護網絡通訊的協議，提供加密、完整性驗證和身份認證等功能。TLS 1.2 適用於可靠的傳輸協議 (如 TCP)，而 DTLS 1.2 適用於基於不可靠傳輸協議 (如 UDP) 的即時通訊和數據傳輸。針對 TLS 及 DTLS，本公司也規劃定期升級版本。
- 數據包加擾：本公司支持使用的設備對數據包進行加擾。加擾技術可以增加數據的隨機性和複雜性，以提高安全性，使其更難以被未經授權的人員解析和破解。

透過以上的加密和保護措施，本公司致力於確保設備之間的數據傳輸是安全的，並保護客戶數據的機密性和完整性。本公司不斷研究和採用最新的安全技術和算法，以應對不斷變化的安全威脅，並提供可靠的數據保護方案。

5. 資安事件反應小組（PSIRT）

資安事件反應小組（PSIRT）負責處理與本公司產品有關的安全事件，包括評估，緩解和公開報告本公司產品的資安問題。

資安事件反應小組的任務是解決產品的資安問題。 如果經由內部測試、研究人員或客戶所通報的資安問題，本公司將立即評估資安事件，如果問題確認，本公司將與研發團隊解決此資安問題。

為了保護用戶，本公司將不會披露所有資安問題的詳細資訊，而僅在發布修補程序或解決方法之前才發布此資安問題。

Follow Us On

or visit www.throughtek.com