物聯網與 M2M 的最佳安全搭檔 — *iBadge* 裝置識別方案

雲端技術與行動裝置的潮流，啟動了物聯網與 M2M (Machine-to-Machine) 的新紀元！但無所不在的資安威脅隨之而來、處處威脅您的商機。銓安智慧科技 (IKV) 的 ***iBagde 裝置識別方案***，將是您的裝置在聯網時的最佳**識別防護**利器。

連網裝置具備以下特性：

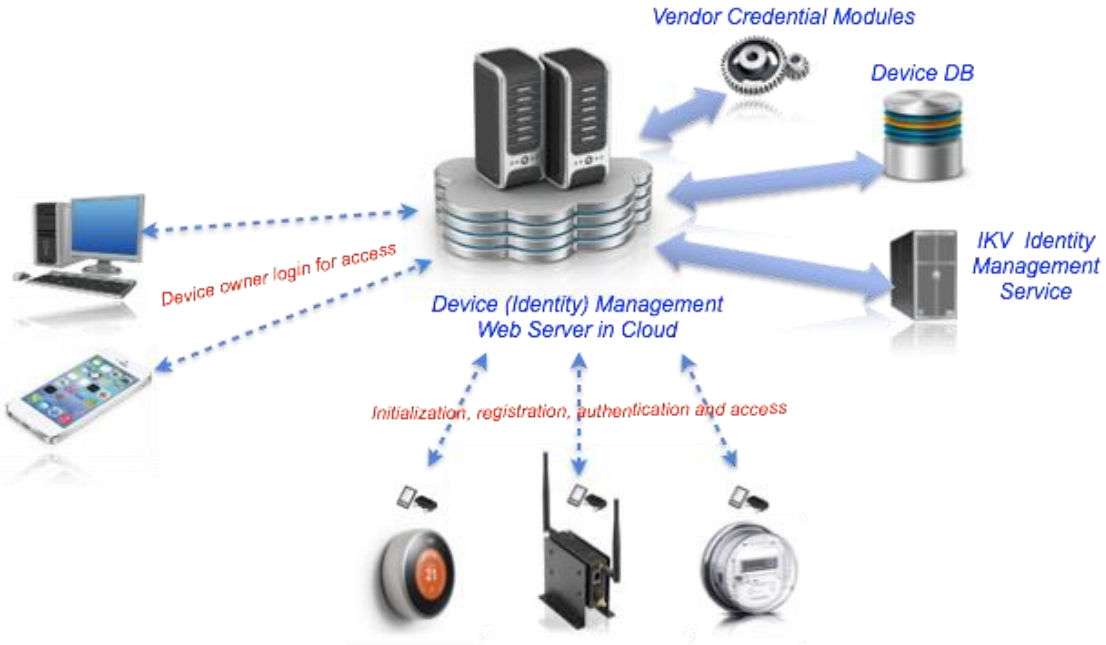
- 運算效能有限
- 注重省電
- 製作成本較低
- 有自動連網與資料處理的裝置智慧 (device intelligence)
- 具有實現雲端應用服務的前置資料搜集處理之使命

這些特性從裝置製造商或應用服務商的觀點，產生以下影響：

1. 裝置專屬資料 (如 MAC 位置、裝置識別代號等) 的人工燒錄成本與管理成本增高
2. 生產數量龐大，後續管理相較以往困難度提高
3. 軟硬體結構簡單，沒有差異化
4. 無法在裝置韌體內設計複雜的保護機制

以上特性對於運用大量連網裝置，以推動後端加值應用來尋求獲利的廠商，成為難以承受的困擾，有如一道無形高牆，阻礙營利！分析上述問題的核心，便是連網裝置缺乏有效率的方法建立並管理裝置識別資訊。

iBadge 裝置識別方案 使用價格合理的硬體認證晶片 (authentication chip) 搭配高強度的公鑰密碼系統進行裝置認證識別，並提供位於雲端管理與認證裝置的配套系統，使配備認證晶片的連網裝置立刻成為物聯網或 M2M 網路架構內**保證獨一無二的終端**，應用服務商將可利用此堅固的基礎，對裝置設計更多完善的保護與安全機制，確保您在雲端的服務可以**安全無虞地獲利**！

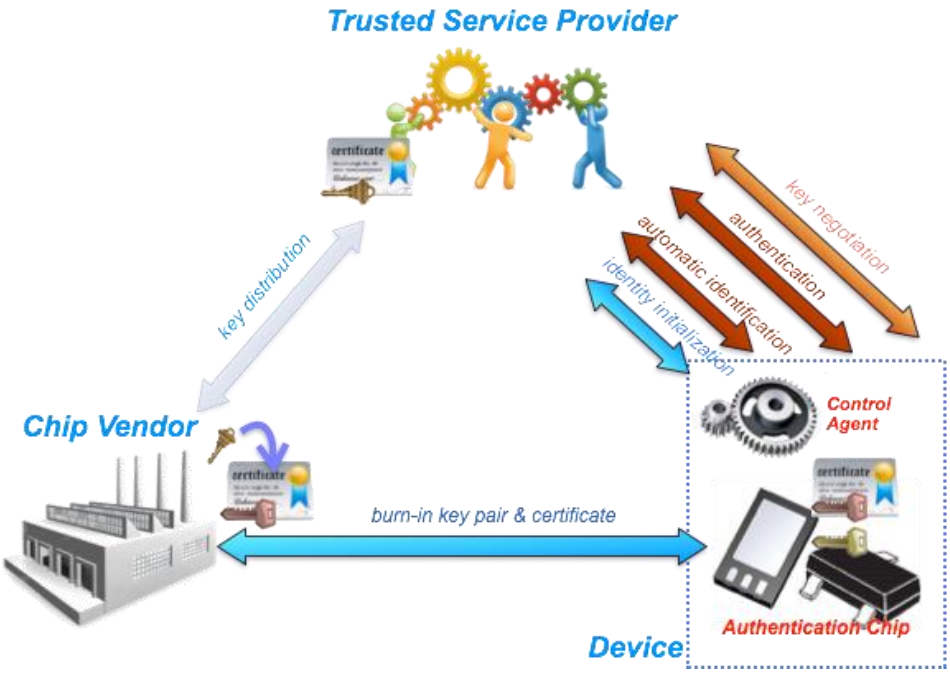


裝置搭配 ***iBadge 裝置識別方案*** 之後，可具備以下能力：

- 生產階段無需人工介入，認證晶片內含全球獨一無二之識別代號與認證密鑰
- 裝置端韌體無需進行複雜密碼運算，可以安全無虞地與位於連網後端應用程式直接進行認證與資料加解密
- 可透過瀏覽器與智慧手機 App 與裝置連線進行管理
- 可經由方案提供的後端模組，輕鬆管理裝置識別代號與其他對應之獨特資訊

運用 ***iBadge 裝置識別方案*** 將可進行以下應用：

- 裝置認證 (device authentication)，保證連網存取應用之裝置皆納管
- 控管韌體更新服務 (controlled device update)，確保接受更新服務之裝置皆為合法授權
- 聯網互通 (device inter-communication)，使裝置與裝置、裝置對使用者，皆可安全溝通，無隱私資料流失之威脅
- 防止山寨裝置 (anti-counterfeit)，確保後端服務或中介 (gateway) 軟硬體被仿冒者運用



iBadge 裝置識別方案 之特點：

- 認證晶片於晶圓封測時燒錄唯一識別代號與密鑰，為業界唯一在供應鏈管理層次保證安全與唯一性之產品
- 使用橢圓曲線公鑰系統 (ECC) 進行強認證 (strong authentication) ，安全無虞
- 裝置端控制模組 (control agent) 移植簡單，省電性能佳，可與您的各式裝置進行整合
- 識別認證完成產生僅一次使用的『會談密鑰 (session key) 』可進一步對資料加密或產生完整性檢查碼，成為連網裝置安全之基石
- 提供應用後端連網伺服器所需之認證支援，包括認證程式庫與認證服務 (web service) 、裝置識別代號資料庫、裝置與連網伺服器 HTTP 連線介面、裝置管理流程 API，可快速將具備識別功能之裝置與您的應用服務整合

iBadge 裝置識別方案 提供 Wi-Fi 模組完整解決方案，採用該模組之客戶可直接連網進行識別，無需額外進行整合。目前持續與其他 2.4G/PAN (BLE, ZigBee,…) 通訊模組廠商產品進行整合，亦竭誠歡迎相關通訊產品廠商洽談合作。

IKV-Tech (InfoKeyVault Technology, 銓安智慧科技股份有限公司) 為台灣少數專注於硬體資訊安全產品與解決方案之科技服務公司，透過專業與創意，協助全球客戶保護珍貴的數位資產。***iBadge 裝置識別方案*** 為專門針對物聯網應用所提供之硬體識別解決方案，如需進一步產品咨詢，請電洽或電郵與我們聯繫，將有專人為您解說並提供進一步產品資訊。

電郵: ikvinfo@email.ikv-tech.com

網址: http://www.ikv-tech.com/

聯繫我們: http://www.ikv-tech.com/contact-us