



科技日新月異，人和機器溝通的模式也隨之改變，同樣地，機器和機器溝通的方式歷經了革命。M2M 是無法抵擋的趨勢，傳輸過程的安全議題也隨著駭客攻擊事件頻傳而浮上檯面。設備之間傳輸不受駭客威脅是 M2M 和 IoT 時代的必要課題。

iBadge USB Token 實現 M2M 在 USB 介面的安全防護。嵌入 USB 的安全晶片實現了資料加密、設備身分認證和訊息驗證等政府及民間廣泛採用的密碼演算法。使用者不費吹灰之力便能有效控管物聯網設備，並確保手機、伺服器、電腦、雲端和設備之間通訊的安全。



### 用途

- 設備和雲端的身分驗證

安全晶片出廠前便燒錄了一對公私鑰以及獨一無二的身分驗證碼。其身分驗證密碼演算法採用 163 位元 ECC 橢圓曲線密碼演算法，一次性非揮發記憶體 (NVM) 可讀寫 500 bytes 使用者資訊。搭配雲端認證系統，唯有插入 iBadge USB Token 的設備才獲准進行通訊。

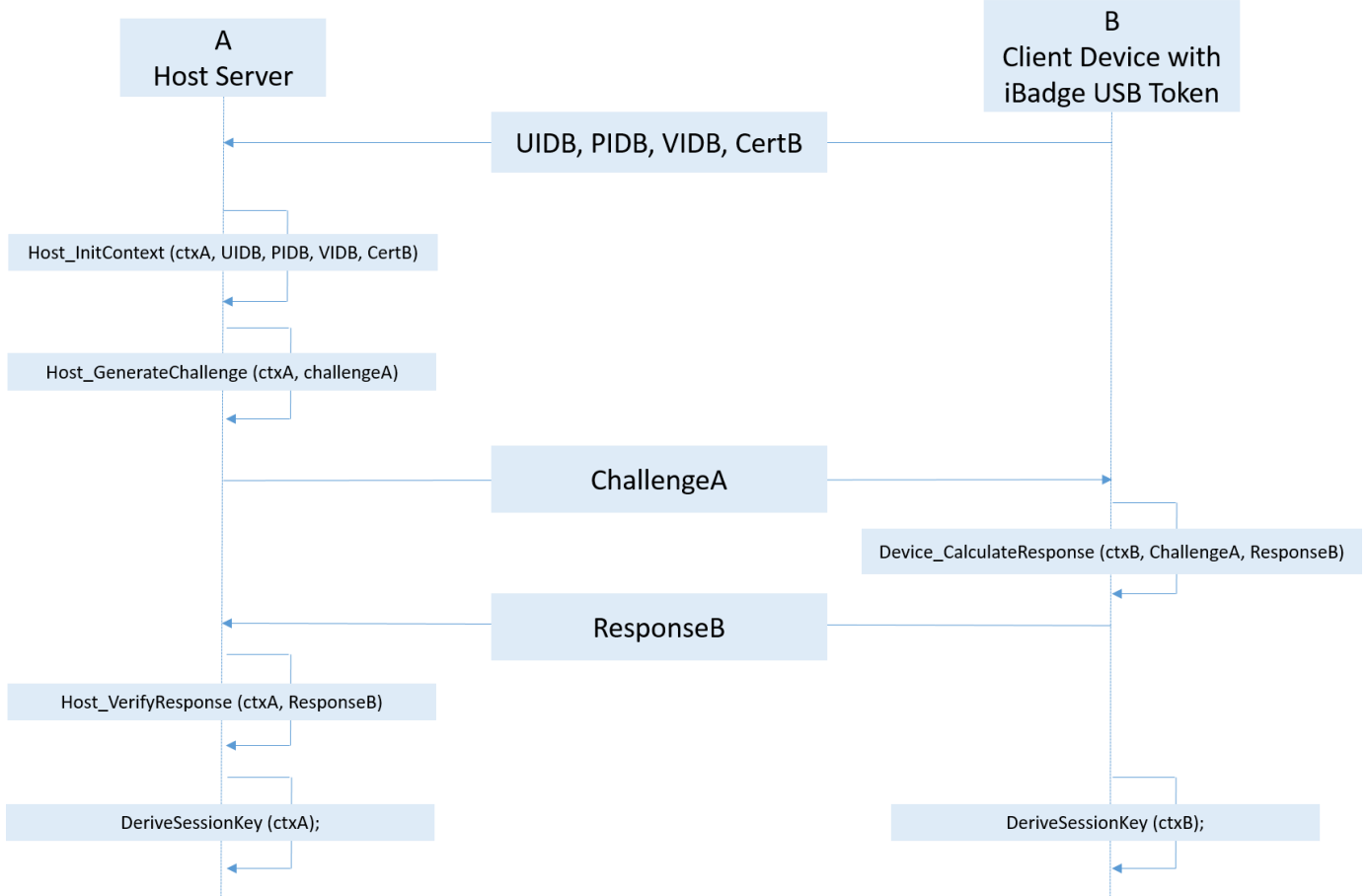
- 訊息加解密以防止駭客竊聽

透過先進加密標準 (AES) 密碼演算法實現了通訊雙方的訊息保密性。

支援 ECB, CBC, CTR, CFB 和 OFB 區塊加密模式。

# Technical Details

The illustration of authentication



iBadge USB Token Specification	
Interface	USB2.0 / USB1.1
API for Supported OS	Android 4.2+, Windows, Linux (SCSI)
Standard	Mass Storage Class

iBadge Secure Chip Specification	
Secure Chip	iBadge Strong Authentication Secure Chip KV-L S10
Ambient Temperature	Min 25.0°C Max 85.0°C
Integration Interface	MIPI® Battery Interface (BIF) Easy-to-implement single-wire host interface
Cryptographic Algorithm	Strong asymmetric cryptography with Elliptic Curve Cryptography (ECC) 163-bit key length
Unique Identifier	Increased security with asymmetric cryptography and chip-individual keys

USB Token Function	
Encryption	Crypto Algorithm: AES-256 Operation Modes: ECB, CBC, CTR, CFB and OFB
Authentication	Asymmetric Cryptography with ECC 163-bit Key



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。如需進一步產品諮詢，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。

TEL: +886-2-23643228  
ikvinfo@email.ikv-tech.com  
9F., No.68, Sec. 4, Roosevelt Rd.,  
Zhongzheng Dist., Taipei City