第一版

2022-11-08

TEEMA

行 業 標 準

資通訊產品供應鏈資安標準

第一部：晶片安全

Security Standard for ICT Product Supply Chain

Part 1：IC Chip Security

V1.0

台灣區電機電子工業同業公會　發行
TAIWAN ELECTRICAL AND ELECTRONIC MANUFACTURERS' ASSOCIATION

目錄

前言

半導體技術的發展，使電子元件快速地微小化並應用於各種資訊及通訊設備中，資通訊技術(Information and Communication Technology, ICT)因此得以快速發展。ICT 技術已成為構建現代社會的基礎，被大量使用於國防軍事系統，以及與國民生計相關的關鍵基礎設施。對於此類應用而言，若其安全性(security)遭到威脅，可能導致嚴重的生命及財產損失，故確保資訊安全是部署此類 ICT 應用的先決條件。

經過數十年的全球化發展，ICT 供應鏈逐漸分散於世界各地，而此趨勢在 ICT 產品尤為明顯。在 ICT 採購全球化的趨勢下，確保 ICT 產業供應鏈安全成為棘手的問題。典型的 ICT 產品主要是由微控制器(MCU)或微處理器(MPU)、儲存裝置、通訊模組/裝置、作業系統、應用程式等軟硬體元件(component)所組成，目的是提供各種設備正常運作所需的功能。供應商(如 OEM 業者)通常通過選擇合適的硬體和軟體元件，將其構建成提供特定服務的設備。

在 ICT 供應鏈中，各種軟硬體、應用程式、資訊服務，多少會使用外部供應商技術元件。由於這些軟硬體元件很可能來自不同的第三方供應商，因此該供應鏈中的相關元件，可能會對 ICT 產品產生資安威脅，進而使最終組成的設備，其安全性(security)受到質疑。由於 ICT 產品供應商可能無法有效掌握所有外部技術元件的安全性，一旦駭客能攻擊產業供應鏈中的環節，將對 ICT 產品的安全性產生深遠的影響。

在 ICT 產品中，資訊安全性須經由各種安全功能來確保，故負責各種精密運算的晶片，其安全性成為各種關鍵設備正常運作的先決條件。我國半導體產業在全球 ICT 供應鏈中佔有重要地位，如何確保所提供的 ICT 產品符合一定的安全標準規範，成為受關注的焦點。因此在數位發展部數位產業署及經濟部技術處的支持下，制定本標準。

本標準制定之目的為協助終端使用者(如地方政府等相關單位)，增進其所採購之 ICT 產品資安防護能力，並藉此引領 ICT 與其相關物聯網應用廠商，導入資安防護設計概念與技術。

本標準係依台灣區電機電子工業同業公會(TEEMA)之規定，經標準及安規委員會審定，由公會公布之產業標準。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，公會不負責任何或所有此類專利權、商標權與著作權之鑑別。

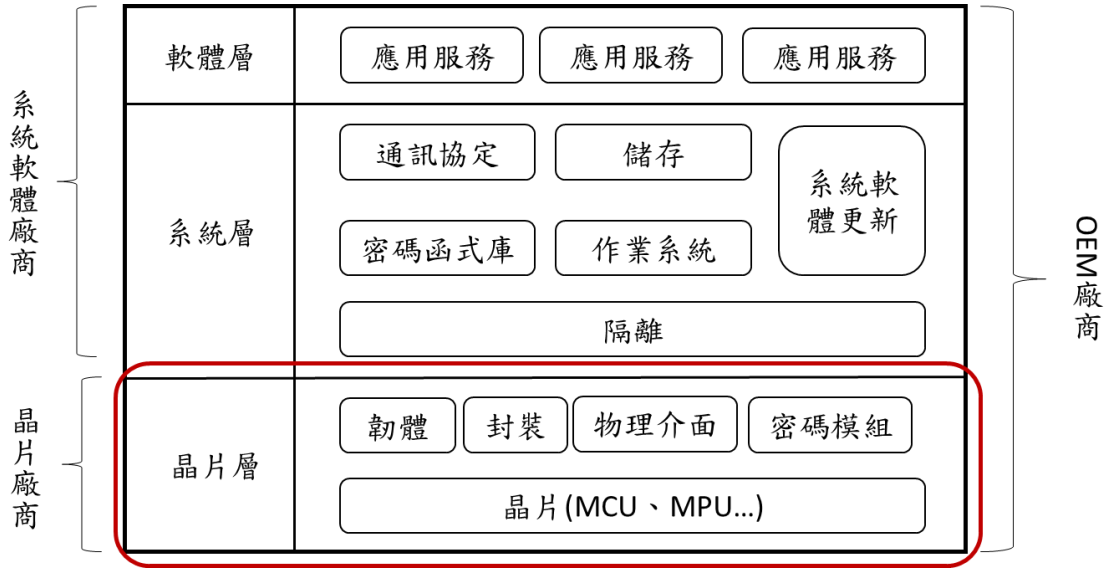
1. 適用範圍

ICT 產品通常可分為最基礎的晶片層，及建構其上的系統層及軟體層，並由不同的廠商負責開發相關的軟硬體元件。依組成 ICT 產品的三個層級，其安全要求可分為「第一部：晶片安全標準」及「第二部：系統軟體安全標準」。本標準之適用範圍，為組成 ICT 產品的各種硬體元件，且這些元件會對產品產生潛在資安風險。

適用於本標準的廠商及其在供應鏈中扮演的角色如下：

- 晶片廠商：於晶片層專注研發晶片、韌體及 bootROM 等，因此適用於本標準。
- OEM 廠商：構思和開發基於本標準的設備，例如選擇符合本標準的硬體，並在硬體上選用合適的系統及軟體，開發相關的應用程序或函式庫等，以組裝構建成提供特定服務的設備。由於 OEM 廠商通常會將各種軟硬體元件(例如處理器和軟體)，組合或整合到其銷售的解決方案中，因此同時適用第一部及第二部安全標準。

本標準適用範圍為 ICT 產品的晶片層，其在供應鏈中對應之層級，參見下圖 1 紅框所示。



資料來源：本團隊自行整理

圖 1 適用範圍示意圖

由於晶片是各種運算的核心，一旦發生資安問題，將直接影響上層系統軟體運作的安全性，因此第一部晶片安全標準規定晶片層的安全要求，包括執行核心運算的微控制器/微處理器，應在矽前(pre-silicon)階段避免晶片設計含有可疑電路、於矽後(post-silicon)階段應防範非侵入式的旁通道攻擊，並規定了晶片封裝、韌體及除錯介面等相關的安全要求。因晶片層為 ICT 產品的最底層，提供上層系統軟體運作的基礎安全環境，故「第一部 晶片安全」標準可以進行獨立的認證。

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

ISO/IEC 17825:2016 Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

3. 用語及定義

下列用語及定義適用於本標準。

3.1 測試(Testing)

指在測試實驗室依照測試規範標準程序進行測試，並簽發正式的測試報告(test report)告知委託者測試結果。

3.2 驗證(Certification)

由公正之第三方針對產品、過程或是服務符合標準之認可。

3.3 測試實驗室(Testing Laboratory)

指通過 ISO/IEC 17025 認證的測試實驗室(以下簡稱實驗室)，使用本標準定義的測試方法，作為檢驗待測物是否滿足本標準所定義的通過條件之標準。

3.4 關鍵安全參數(Critical Security Parameter，CSP)

係指一旦外洩或修改可能危及密碼模組安全性的安全相關資訊，例如：密鑰(secret key)、私鑰(private key)、通行碼(password)、PIN 碼(Personal Identification Number)、憑證(certificate)、工作模式(operation mode)或其它機敏資訊。

3.5 敏感性資料(Sensitive Data)

係指使用者運行待測物時產生的機敏文件(如商業資料等)。

3.6 個人資料(Personal Data)

係指指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.7 金鑰(Key)

在密碼學中，金鑰係指某個用來完成加密、解密、完整性查驗、進行數位簽章等密碼學應用的秘密值(secret value)，例如：密鑰(secret key)、私鑰(private key)、公鑰(public key)。

3.8 晶片(Integrated Circuit/Chip，IC)

晶片或積體電路(IC)，係指設計用於執行處理和/或儲存功能的極小型之電子電路。

3.9 硬體實例(Hardware Instance)

係指產品中具有相似生命週期的實體或虛擬設備(device)或元件(component)，例如晶片在其 Flash 快閃記憶體中有一塊受保護區域(memory region)，並包含一個 128 位的唯一識別 ID，此區域可視為實例。Trustzone 中的 Secure World 及 Normal World，即為兩個不同的實例，並可以根據當前 session 所需在 Secure 和 Normal World 進行切換。

3.10 物理維護 (Physical Maintenance)

當使用者拆卸晶片蓋板(covers)及打開晶片封裝，或透過 JTAG、UART、USB 等物理介面進行除錯 (debug)時，皆視為對晶片進行物理維護。

3.11 時序分析 (Timing Analysis，TA)

晶片中的每個邏輯運算都需要時間來執行或回應，並且所需時間會因輸入值而異。透過精確測量每個運算所花費的時間，攻擊者可能藉此破解密碼系統，獲取加解密演算法使用的密鑰、私鑰、通行碼、PIN 碼等。

3.12 簡單功耗分析 (Simple Power Analysis，SPA)

由於在密碼模組上運行的每個算式與指令，都是按順序執行的，通過監控密碼模組執行過程中的功率消耗變化，對指令執行或邏輯電路活動模式，進行直接分析，如果指令序列與金鑰有關，則這些指令造成的波形變化被分析後，可能導致金鑰外洩等的安全問題，且 SPA 只需要少量的功耗紀錄就可以進行攻擊。

3.13 簡單電磁分析 (Simple Electromagnetic Analysis，SEMA)

SEMA 採用與 SPA 相同的方法，通過觀察電磁輻射記錄(EM trace)的變化推估密鑰。根據金鑰位元是 0 或 1 而執行不同運算的密碼演算法，容易受 SEMA 攻擊，攻擊者可以透過觀察加密的整個過程推斷出金鑰。

3.14 差分功耗分析 (Differential Power Analysis，DPA)

DPA 需要大量的電壓變化紀錄，來比對功率消耗和資料的相依性。DPA 不需要了解太多關於待測物的詳細知識，即使記錄的軌跡包含雜訊，一旦收集足夠的功耗紀錄，攻擊者就可以採用兩組資料的多筆功耗紀錄(trace)，然後計算這些紀錄的平均值之差，將雜訊抵消，以找出金鑰。

3.15 差分電磁分析 (Differential Electromagnetic Analysis，DEMA)

DEMA 是一種進階攻擊，透過利用多筆電磁輻射記錄，來提高捕獲訊號的真實度(fidelity)，適用於不可能進行簡單電磁分析攻擊，或無法提供足夠的訊息的情況。DEMA 攻擊比簡單電磁分析攻擊更為複雜，但可以在不需要太多有關待測物的知識情況下，有效分析密碼系統的旁通道弱點。

3.16 相依性(Dependency)

相依性是一種度量，用以衡量兩個變量(variables)相互影響的程度。於本標準中，係指加密模組在不同輸入值(變量)情況下，即使用(a) 隨機的 CSP 和固定的明文字串，及(b) 隨機的明文字串和固定的 CSP，是否會產生加密所需執行時間的不同，例如當碰上輸入值位元“0”時，加密的時間將縮短，反之遇上位元“1”時，則加密時間稍為延長。透過統計加密模組在不同輸入值情況下，即可判斷晶片於設計之初，是否有對加密模組進行時序攻擊的防護，避免攻擊者可以透過時序這類旁通道資訊，推論出加密模組當下正在計算位元“0”或“1”。

3.17 半導體封裝 (Semiconductor Package)

半導體封裝(以下簡稱封裝)，是一種用於容納、包覆一個或多個半導體元件或積體電路的載體/外殼，外殼的材料可以是金屬、塑料、玻璃、或者是陶瓷。封裝可為裸晶/晶粒(1)提供一定的衝擊/劃傷保護；(2)提供與外部電路連接的引腳或觸點；(3)將晶粒工作產生的熱量帶走。

3.18 矽前(Pre-silicon)

晶片設計者透過硬體描述語言(如 Verilog 或 VHDL)描述晶片電路或硬體，利用硬體描述語言模擬器確認電路功能無誤後，經由邏輯合成器把這些使用硬體描述語言的設計轉換成邏輯閘層級的設計。之後透過自動擺放及繞線軟體，針對對應的邏輯

閘元件布局進行擺放及繞線，最後經過相關電路及布局的設計準則驗證後，即完成矽前階段的工作任務，此時將產出晶片布局設計圖。

3.19 矽後(Post-silicon)

於矽後階段，晶片設計者把晶片布局設計圖，交由晶片製造商或晶圓代工廠製做晶片。晶圓代工廠將把設計好的電路圖，實際轉移到半導體晶圓上(wafer)上，經過一連串的程序後，在晶圓表面上形成積體電路(IC)，再切割成一片一片的裸晶/晶粒(Die)，待完成封裝，形成最終的晶片(Chip)。

3.20 塗層(Coating)

係指透過半導體封裝的鈍化技術，利用有機聚合物等材質形成保形塗層或密封塗層，防止環境或其它物理損壞對晶片造成傷害。

3.21 差分錯誤分析(Differential Fault Analysis，DFA)

係指待測物在加解密過程中，攻擊者選擇合適時間與位置，進行錯誤注入(例如改變晶片的電壓)，干擾加解密運算，使晶片中的暫存器在加解密過程中產生錯誤，通過對正確密文輸出和錯誤密文輸出的差異比較，分析取得晶片內部的機敏資料，如金鑰等。

3.22 電磁錯誤注入(Electromagnetic Fault Injection，EMFI)

EMFI 為一種局部性高精度的攻擊手段，攻擊者通過將電磁探頭置於加密電路附近，在合適的時間產生一個脈衝信號干擾晶片內部關鍵的訊號線路，使得電路運行出錯，例如讓暫存器發生位元翻轉(bit flip) ，以產生所需的效果，如跳過身份驗證步驟、繞過安全啟動(secure boot)、提升特權或更改加密運算的輸出等。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

每個產品都有獨特的功能和安全要求，為了對接國際資安標準(如：SESIP)，減少產品安全認證的障礙，本標準針對晶片層定義了三個安全等級(security level)。晶片層的元件應先滿足較低安全等級之要求，始可進級高階等級之測試。

各安全等級說明如下：

- 1 級： 1 級安全匯集了產品在晶片層最重要的資安基線(security baseline)，可以防範一些最常見的資安漏洞。送測廠商依產品資安功能填寫調查問卷(questionnaire)，以便測試實驗室可以透過受審查廠商所完成的問卷及所檢附之證據，評估其所開發的元件是否已滿足基線安全標準之要求。
- 2 級： 2 級安全標準用以證明元件可以防範由遠端發起的網路攻擊(cyber attack)，並且攻擊者在被偵測到之前將無法對元件進行大規模的重複攻擊，因此元件遭受物理攻擊的傷害範圍有限，故讓廠商可以提供適用於許多大眾市場解決方案的安全保證。2 級安全由測試實驗室對待測元件進行獨立評估和審查。測試實驗室使用漏洞分析和滲透測試等方法，來確認待測元件是否已滿足標準要求。
- 3 級： 3 級安全標準專為希望對其開發的高價值資產元件，進行獨立評估的晶片供應商而設計。此安全等級讓 OEM 廠商相信該元件，可以提供駭客於本地端(local)針對硬體攻擊的保護。3 級安全由測試實驗室對待測元件進行獨立評估，確保元件可以防範複雜的硬體攻擊，例如駭客對元件具有物理存取權限。

其中，第三欄安全等級中的安全要求可分為 M 及 O 兩類，如下所述：

- M：此項目為強制性(Mandatory)的安全要求。
- O：可自選的(Optional)安全要求項目，可用於強化產品的安全性。

表 1 晶片安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 晶片安全	5.1.1 晶片本體	送測單位自我評估並提供佐證資料，實驗室書審	—	5.1.1.1 (M) 5.1.1.2 (M) 5.1.1.3 (O) 5.1.1.4 (O)
	5.1.2 晶片設計		—	5.1.2.1 (O)
	5.1.3 晶片密碼模組保護		—	5.1.3.1 (M) 5.1.3.2 (M) 5.1.3.3 (O)
5.2 物理介面安全	5.2.1 除錯介面		5.2.1.1 (M) 5.2.1.2 (O)	—
	5.2.2 功能保護		—	5.2.2.1 (M)
5.3 硬體元件安全	5.3.1 晶片身份		5.3.1.1 (M) 5.3.1.2 (M) 5.3.1.3 (M)	—
	5.3.2 硬體運行狀態		5.3.2.1 (M) 5.3.2.2 (M)	—
	5.3.3 安全更新		5.3.3.1 (M)	—
	5.3.4 安全重置		5.3.4.1 (M) 5.3.4.2 (O) 5.3.4.3 (O)	—
	5.3.5 安全隔離		5.3.5.1 (M)	5.3.5.2 (M)
5.4 密碼安全	5.4.1 演算法安全		5.4.1.1(M)	—
	5.4.2 金鑰安全		5.4.2.1(M) 5.4.2.2 (M)	—
	5.4.3 亂數產生器安全		5.4.3.1 (M)	—
5.5 韌體安全	5.5.1 韌體保護		5.5.1.2 (M) 5.5.1.3 (M) 5.5.1.4 (M) 5.5.1.5 (M)	5.5.1.1 (M)

資料來源：本團隊自行整理

安全等級總表如表 1 所示，第一欄為安全構面，包括晶片安全及物理介面安全等；第二欄為安全要求分項，係依各安全構面設計對應之安全要求；第三欄為安全

等級，按各安全要求分項之驗證結果，作為安全等級評估標準。本安全等級總表各欄的關連性，應依循本節 5.1 至 5.5 之技術規範內容。

4.1.1 安全構面

(a) 5.1 晶片安全：產品應具備抵禦入侵及偵測入侵的能力，此外，安全的晶片設計、強韌的封裝材料均應視為晶片安全要求標的。

(b) 5.2 物理介面安全：產品提供之除錯介面應具備足夠之安全防護。

(c) 5.3 硬體元件安全：產品硬體元件的身份，應可被正確辨識(identity verification)，並可進行安全更新與出廠重置(factory reset)。

(d) 5.4 密碼安全：產品所使用之密碼演算法、金鑰與亂數產生器等，均應具備足夠之安全強度。

(e) 5.5 韌體安全：產品所使用的韌體，應確保其機密性、真實性與完整性。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個或以上之安全要求。

4.1.3 安全等級

安全等級依(1)晶片層應具備之安全要求、(2)技術實現複雜度綜合考量，分為 1 級、2 級、3 級三個等級，並對應所應符合的安全要求分項。安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求，應先滿足所有較低安全等級中的強制性安全要求。若廠商在 2 級與 3 級中，實施(implement) 了一個或多個選擇(optional)的安全要求，則安全等級分別為 2+級、3+級。若廠商在 2 級的基礎上，額外滿足了 3+級的安全要求，亦應視為 2 級。

5. 安全要求

本節詳盡載明產品為滿足安全功能應採取的共通方法，產品所對應之安全等級，應符合本節安全要求。

5.1 晶片安全

5.1.1 晶片本體

5.1.1.1 產品在執行密碼運算的過程中，不應因相異的CSP值而使處理時間產生差異，以防止透過時序分析，找出執行時間與 CSP 之間的相依性。(3 級)

5.1.1.2 產品在執行密碼運算的過程中，應防止攻擊者透過簡單功耗分析或簡單電磁分析，找出密碼運算的執行序列(operation sequence)。(3 級)

5.1.1.3 產品在執行密碼運算的過程中之紀錄，應防止攻擊者透過差分功耗分析或差分電磁分析，找出產品所使用的 CSP。(3 級)

5.1.1.4 產品在執行密碼運算的過程中，應防止攻擊者透過差分錯誤分析或電磁錯誤注入，造成待測物產生穩定的異常輸出，或待測物發生潛在的 CSP 洩漏問題。(3 級)

5.1.2 晶片設計

5.1.2.1 產品不應存在疑似硬體木馬的電路設計。(3 級)

5.1.3 晶片密碼模組保護

5.1.3.1 產品密碼模組元件，應由包含標準鈍化技術的生產級元件組成，且進行物理維護時不會外洩明文 CSP。(3 級)

5.1.3.2 產品密碼模組元件，應覆蓋不透明的硬式防篡改塗層或封裝材料，並於遭受竄改時，可保留篡改或移除模組的證據。(3 級)

5.1.3.3 產品密碼模組元件應具有被篡改之回應機制。(3 級)

5.2 物理介面安全

5.2.1 除錯介面

5.2.1.1 產品除錯介面存取應具備身份鑑別功能，且無法遭到濫用(如：存取使用者身份權限以外的其它資料)，以確保資料的安全性。(2 級)

5.2.1.2 產品除錯介面之身分鑑別功能，應具備適當的身份角色權限，且無法使用非法方式進行身份提權。(2 級)

5.2.2 功能保護

5.2.2.1 產品應具備偵測或防止物理攻擊之能力，避免造成非安全功能中的必要功能異常(如：網路時間協定無法運作、電源指示燈號異常等)。(3 級)

5.3 硬體元件安全

5.3.1 晶片身份

5.3.1.1 產品應擁有唯一性識別資訊，並可被正確辨識。(2 級)

5.3.1.2 產品硬體實例均應擁有唯一性識別資訊，並可被正確辨識。(2 級)

5.3.1.3 產品應提供查驗其真實性的機制，確保產品不是非法的複製品(clone)。(2 級)

5.3.2 硬體運行狀態

5.3.2.1 產品應在啟動(start-up)期間，查驗產品真實性與完整性。(2 級)

5.3.2.2 產品應提供可辨識的已知運行狀態，讓使用者可以隨時查驗產品目前的運行狀態是否安全。(2 級)

5.3.3 安全更新

5.3.3.1 產品應在使用者環境中，提供安全的韌體更新功能。(2 級)

5.3.4 安全重置

5.3.4.1 產品應提供出廠重置(factory reset)功能，銷毀產品中所儲存的使用者資料。(2 級)

5.3.4.2 產品應提供退役功能，銷毀產品中的應用程式、敏感性資料及個人資料，並且使產品無法再使用。(2 級)

5.3.4.3 當發生故障需要檢修時，產品應提供產品返還供應商功能，銷毀產品中的敏感性資料及個人資料，且讓供應商無法復原遭銷毀的資料。(2 級)

5.3.5 安全隔離

5.3.5.1 產品應提供應用程式與硬體安全功能之間的有效隔離機制，以避免攻擊者在應用程式上執行的惡意行為，可以破壞產品的其它安全功能。(2 級)

5.3.5.2 產品應提供硬體元件之間的有效隔離功能，以避免含有弱點的元件成為攻擊跳板，對其它元件造成損害。(3 級)

5.4 密碼安全

5.4.1 演算法安全

5.4.1.1 產品所使用的各種密碼運算，如加密、解密、數位簽章等，應使用符合國際標準要求，或資安產業慣例使用之密碼演算法，例如，NIST SP 800-140C 所核可的同等或以上等級之密碼演算法。(2 級)

5.4.2 金鑰安全

5.4.2.1 產品所使用的金鑰產生演算法，應使用符合國際標準要求之密碼演算法，例如 NIST SP 800-133 Rev. 2。(2 級)

5.4.2.2 儲存在 KeyStore 中的 CSP，應保護其真實性、完整性及機密性。(2 級)

5.4.3 亂數產生器安全

5.4.3.1 產品所使用的亂數產生演算法，應符合國際標準要求，或公認資安產業慣例，例如，NIST SP 800-90A、NIST SP 800-90B 或 AIS31 所核可的同等或以上等級之密碼演算法，且所產生之亂數，應通過 NIST SP 800-22 隨機性測試。(2 級)

5.5 韌體安全

5.5.1 韌體保護

5.5.1.1 韌體不應被萃取分析出明文 CSP。(3 級)

5.5.1.2 韌體應具備完整性查驗機制，且使用之演算法，應使用符合國際標準要求，或公認之資安產業慣例使用之演算法。(2 級)

5.5.1.3 韌體應具備真實性查驗機制，且用於真實性查驗之金鑰應受到保護。(2 級)

5.5.1.4 韌體應具備完整性查驗機制，以防止使用者利用遭竄改之韌體進行更新。(2 級)

5.5.1.5 韌體應具備真實性查驗機制，以防止使用者利用偽造之韌體進行更新。(2 級)

附錄 A ：驗證結果重用

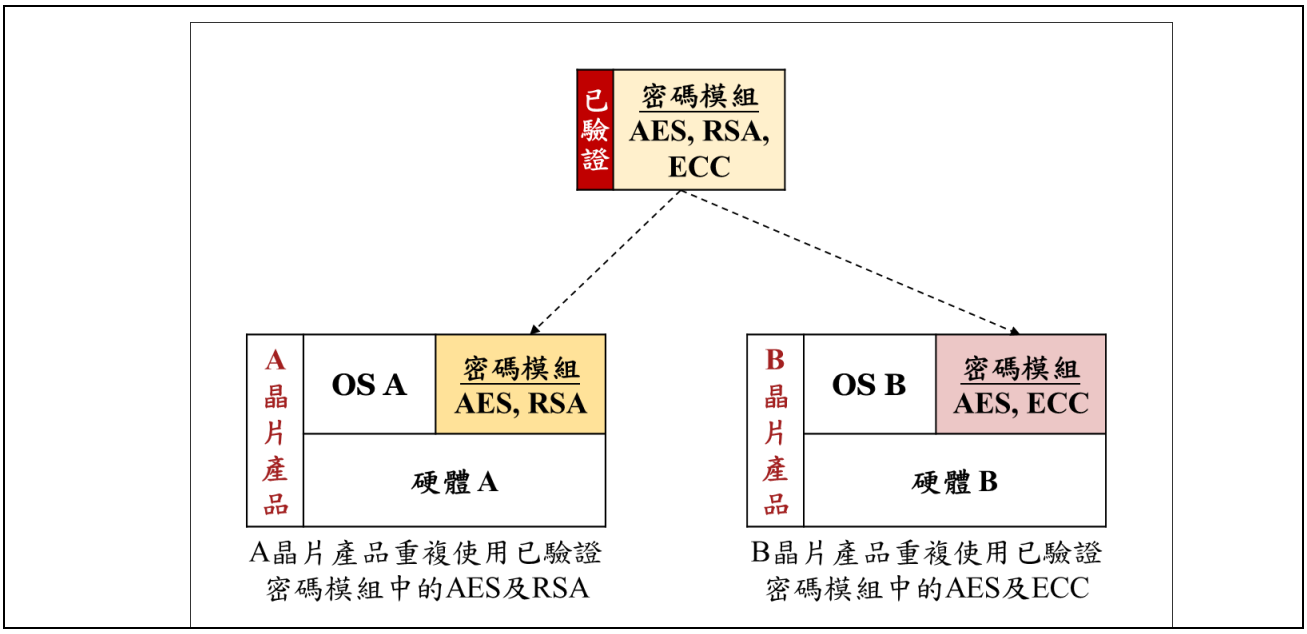
ICT 產品通常很複雜，通常是通過組合多個硬體和軟體元件來構建而成，其中包括保護關鍵資產的安全元件。本標準定義了獨立評估晶片及元件，並可在任何的 ICT 產品中重複使用驗證結果。這些驗證結果可以來自本標準，也可以來自其它兼容的外部驗證結果，例如：重複使用 CC (Common Criteria)的驗證結果。

A.1. 驗證結果重用

ICT 產品通常包括以下元件：

- 硬體：如處理單元、記憶體、並可能包括安全元件、直接或間接可讓攻擊者利用的網路介面等
- 作業系統：為在硬體上運行應用程式的基礎
- 網路連接層：允許將產品連接到後端或其它產品

上述這些組成 ICT 產品的軟硬體元件，一般上會在不同產品中重複使用。系統及 OEM 廠商通常通過選擇合適的硬體和軟體元件(可能來自不同的第三方供應商)，然後用其構建成 ICT 產品。該供應鏈中的每個供應商都應提供元件的資安測試結果，並取得驗證機構的認可，最後由系統及 OEM 廠商負責確保最後的 ICT 產品是安全的。在 ICT 產品的構建整合過程中，維護相關重要軟硬體元件的安全性可能非常複雜，因此這些元件的供應商都需要使用一致的方法來確保所提供元件的安全性。



資料來源：本團隊自行整理

圖 2 已驗證元件重複使用示意圖

本標準包括重複使用(reuse)已獲驗證的元件，減少重複測試的成本浪費。如上圖 2 所示，已驗證的密碼模組 AES、RSA 及 ECC 可分別被 ICT 產品 A、產品 B 重複使用。甲實驗室在測試ICT 產品A、產品B時，若可以確認產品內使用的密碼模組，已被合格的乙實驗室測試通過並取得驗證機構的之認可，則可以直接採納乙實驗室的測試結果，不需重複測試。甲實驗室僅需對其它的元件如 OS A(OS B)及硬體 A(硬體 B)進行測試。

已驗證結果的重複使用，對驗證時間冗長，成本高，過程繁瑣的產品(元件)至關重要，近年來已成為國際認驗證標準的新趨勢。例如：2020 年 7 月，應歐洲執委會(European Commission)的要求，歐盟網路與資訊安全局(European Union Agency for Network and Information Security，ENISA)提供了基於現行資訊技術安全評估共同準則(Common Criteria)的歐洲網路安全驗證規範(Common Criteria based European Cybersecurity Certification Scheme，EUCC)方案草案，以供公眾諮詢。 EUCC 方案直接提及了驗證結果的可重用性概念，特別是：

「作為新驗證的一部分，應可以重複使用其它 ICT 產品驗證的評估結果。因此，申請人可以向符合性評鑑機構(Conformity Assessment Body，CAB)提供先前的評估結果，包括與產品生命週期或申請人的補丁管理方法相關的評估結果，以作為重新使

用的證據。當提供的證據符合 CAB 要求的證據要求，且證據的真實性可以確認時，CAB 應將這些結果用於其評估任務中。」

產品元件的各種組合和驗證結果重複的使用，將有利於快速發展的各種 ICT 產品，相關優勢如下：

- 可重用性：將已驗證元件應用在各種不同 ICT 產品，可協助送測單位節省測試時間和成本。
- 縮短上市時間：對於目前正將產品送測的單位而言，本標準對其沒有直接的影響，但對購買已驗證元件的產品製造商將受益於降低測試成本和縮短上市時間。如果製造商重複使用已驗證的元件進行開發，初始的測試成本可以分攤在不同的專案項目，且減少的測試時間可縮短後續產品的上市時間。
- 安全始於設計(Security by design)：當系統及 OEM 廠商使用已驗證的元件進行終端 ICT 產品整合時，由於該元件安全性已由其它資安專家確認，因此終端 ICT 產品可利用已經過驗證的元件來確保安全性。

在不影響測試品質的情況下，元件的可組合性和驗證結果重用是實現上述目標的重要機制。然而，在所有情況下，驗證結果的重複使用都將特別著重於每個元件的安全整合指引(secure integration guidance)。對整合各已驗證元件的 ICT 產品而言，相關的測試將著重於確認安全整合指引及組合規則(composition rule)是否被嚴格遵守。但無論如何，在驗證結果可重複使用情況下，測試工作量都將遠遠低於在新 ICT 產品中，對所有元件進行重新測試。

使用本標準作為核心測試方法，供應商可以通過重複使用元件供應商在測試其產品期間提供的證據，清楚地了解其整合第三方元件時所應掌握的前提條件及安全整合指引。故本標準是一種有利於組合的測試方法，允許對單獨或組合產品元件的測試，讓通過這樣方式完成的元件驗證結果在不同的產品組合中仍然適用。

總的來說，本標準旨在減少驗證的高複雜性和成本，讓送測單位的有限資源分配可以滿足對高級功能快速增長的需求，且降低終端使用者遭受各種資安威脅的機率。

A.2. 攻擊和威脅

針對 ICT 產品的攻擊可分為 3 大類威脅模型，這些威脅模型進一步構成了本標準所制定的測項，說明如下：

- 遠端網路威脅

  ICT 產品的最小威脅模型是僅具有遠端(無物理)存取權限的攻擊者在攻擊階段嘗試連接到產品。攻擊者在進行攻擊前，可以針對目標 ICT 產品進行任何類型的攻擊探究，包括事先購買該產品嘗試進行物理攻擊，以鑑別產品中可被遠端利用的資安弱點。

- 物理威脅

  當攻擊者可以物理存取 ICT 產品時，就可能透過旁通道攻擊、JTAG 介面的弱點等，從中發掘產品的物理漏洞。攻擊者對 ICT 產品的典型物理威脅包括產品部署在物理保護環境之外，及可能的臨時性物理存取(如邪惡女僕攻擊，evil maid attack)，攻擊者可在供應鏈運送過程中臨時物理存取最終使用者的產品。

- 不受信任的軟體

  不受信任的軟體可能由終端使用者或外部人員載入到產品上，並且可能影響 ICT 產品、其元件或應用程式，因此測試規範應包含這類威脅模型的測項。

ICT 產品普遍受到遠端、物理及不受信任的軟體威脅，因此本標準專注於 ICT 產品的安全要求，為 ICT 產品的安全測試奠定基礎。

參考資料

(1) Arm Limited, Platform Security Model v1.1 (JSADEN014), Jan. 2021.
(2) Arm Limited, PSA Certified Level 1 Questionnaire version 2.1 (JSADEN001), Oct. 2020.
(3) GlobalPlatform Technology, SESIP Profile for Secure MCUs and MPUs v0.0.0.7 (GPT_SPE_150), Jun. 2021.
(4) Security Evaluation Standard for IoT Platforms (SESIP) v1.0 (GP_FST_070)
(5) FIPS 140-3 Security Requirements for Cryptographic Modules
(6) ISO/IEC 15408:2008 Information technology — Security techniques — Evaluation criteria for IT security
(7) ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules

版本修改紀錄

版本	時間	摘要
V1.0	2022/07/25	初版
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-

修改紀錄表

修正條文	現行條文

台灣區電機電子工業同業公會
TAIWAN ELECTRICAL AND ELECTRONIC MANUFACTURERS' ASSOCIATION
Tel：886-2-87926666 Fax：886-2-87926088
http://www.teema.org.tw