第一版

2022-11-08

TEEMA

行 業 標 準

資通訊產品供應鏈資安標準

第二部：系統軟體安全

Security Standard for ICT product Supply Chain

Part 2：System Software 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。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 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，提供 ICT 產品所需要的安全服務，來確保運行在晶片層上的作業系統及軟體之安全性。而系統層及軟體層也常為駭客首要攻擊的層面，利用遠端、應用程式介面等方式，進行 ICT 產品的入侵及攻擊。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我國 ICT 供應鏈業者，增進其所開發之 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。

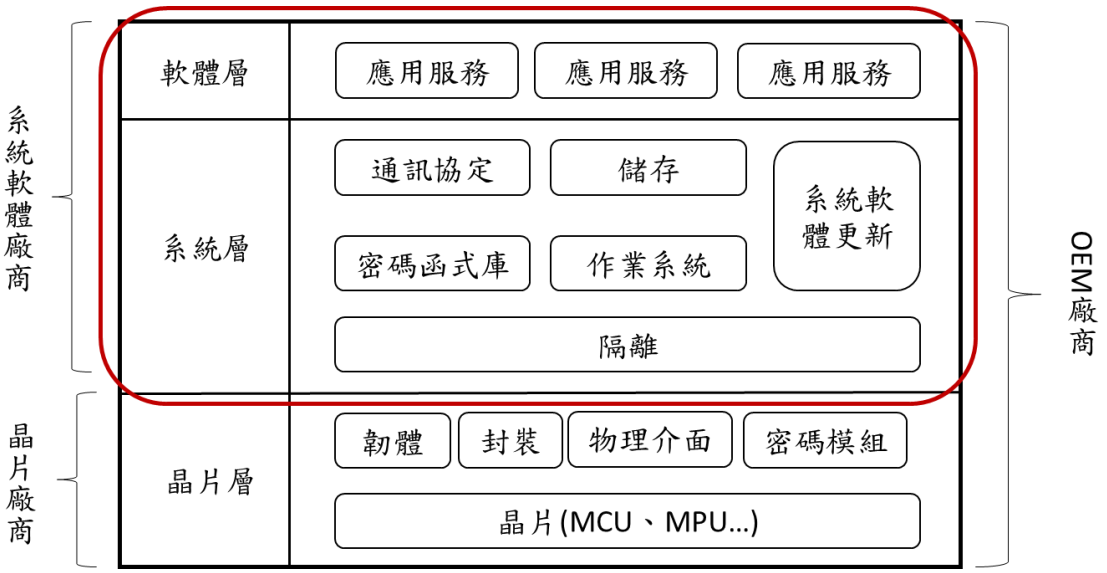
本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

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

本標準在供應鏈中對應之層級，參見下圖 1 紅框所示。適用於本系列標準的廠商及其在供應鏈中扮演的角色如下：

- 軟體系統廠商：於系統層及軟體層負責開發作業系統(如即時作業系統 RTOS)、通訊模組、密碼函式庫(crypto library)、產品所需的應用服務，如 Apps 等，其安全性建構於安全的晶片層。
- 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。



資料來源：本團隊自行整理

圖 1 適用範圍示意圖

本標準規定了系統層及軟體層的安全要求，包括密碼安全、儲存安全、通訊安全等。

由於系統層的運作仰賴安全的晶片層，因此系統層的資安標準認證，應基於已通過「第一部 晶片安全」標準認證的晶片層。對於專注開發應用服務的軟體層廠商，所開發的應用服務欲通過本資安標準認證，應同時基於已通過認證的系統層及晶片層。

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。

[1] 資通訊產品供應鏈資安標準 第一部：晶片安全 v1.0

3. 用語及定義

「資通訊產品供應鏈資安標準 第一部：晶片安全 v1.0」所述，及下列用語及定義適用於本標準。

3.1 部件(Part)

係指應用程式相對獨立的組成部份(application part)，例如 module、process、applet 等。

3.2 增長計數器(Only-increasing Counter)

係指儲存特定事件或過程發生次數的元件。

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，本標準針對系統軟體層定義了三個安全等級(security level)。系統軟體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 級安全基線匯集了產品在系統軟體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標準要求。
- 2 級：2 級安全標準用以證明系統軟體元件可以滿足大部份產品的要求，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的系統軟體元件進行獨立評估和審查。測試實驗室使用弱點掃描、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，進行獨立評估的系統軟體供應商而設計。此安全等級讓 OEM 廠商相信該元件除了提供進階的安全功能外，也可以防禦複雜的駭客攻擊。3 級安全由測試實驗室對待測元件進行獨立評估，確保系統軟體元件進階的安全功能可以防範複雜的攻擊，例如駭客利用有弱點的元件當作攻擊跳板，攻擊其它系統軟體元件。

由於系統軟體層的運作應基於安全的晶片層，故系統軟體層應使用相同安全等級，或更高等級的晶片層。換句話說，晶片層安全等級，應至少等於或大於系統軟體層欲通過的安全等級。例如：欲通過 2 級資安認證的系統軟體層，其底層採用的晶片層，應先通過 2 級或 3 級的資安認證。若系統軟體層搭配的晶片層僅通過 2 級資安認證，系統軟體層應僅能取得 2 級資安認證，無法取得 3 級的資安認證。

第三欄安全等級中的安全要求可分為 M 及 O 兩類，說明如下：

- 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 系統軟體安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 系統軟體元件安全	5.1.1 系統軟體身份	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)	—
	5.1.2 系統軟體運行狀態		5.1.2.1 (M)	—
	5.1.3 安全更新		5.1.3.1 (M)	—
5.2 密碼安全	5.2.1 演算法安全		5.2.1.1 (M)	—
	5.2.2 金鑰安全		5.2.2.1 (M) 5.2.2.2 (M)	—
	5.2.3 亂數產生器安全		5.2.3.1 (M)	—
5.3 軟體安全	5.3.1 安全隔離		—	5.3.1.1 (M)
	5.3.2 安全狀態		5.3.2.1 (M)	5.3.2.2 (O)
	5.3.3 安裝/更新/卸載安全		5.3.3.1 (M) 5.3.3.2 (M) 5.3.3.3 (M)	—
5.4 儲存安全	5.4.1 資料保護		5.4.1.1 (M) 5.4.1.2 (M) 5.4.1.3 (M)	—
	5.4.2 資料安全銷毀		—	5.4.2.1 (M)
	5.4.3 日誌保全		5.4.3.1 (M)	—
	5.4.4 增長紀錄保全		—	5.4.4.1 (O)
5.5 通訊安全	5.5.1 協定安全		5.5.1.1 (M) 5.5.1.2 (M) 5.5.1.3 (M)	—
5.6 韌體安全	5.6.1 韌體內容安全		5.6.1.1 (M) 5.6.1.2 (M)	5.6.1.3 (M)
	5.6.2 韌體保護		5.6.2.1 (M) 5.6.2.2 (M)	—

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
			5.6.2.3 (M) 5.6.2.4 (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，包括系統軟體元件安全及密碼安全等；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 5.6 之技術規範內容。

4.1.1 安全構面

(a) 5.1 系統軟體元件安全：產品的唯一性識別資訊應可被正確辨識(identity verification)，並可進行安全更新。

(b) 5.2 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。

(c) 5.3 軟體安全：產品之應用程式應具備安全保護機制。

(d) 5.4 儲存安全：產品儲存的資料，應確認其真實性、完整性及機密性，並確認資料必要時能安全銷毀。

(e) 5.5 通訊安全：產品應使用符合資安規範的安全通訊協定與保護措施。

(f) 5.6 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，並且不應存取可被利用的弱點或漏洞。

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以上之安全要求。

4.1.3 安全等級

安全等級依(1)系統軟體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。其對應之列即其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。若廠商在各別安全等級中，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 系統軟體元件安全

5.1.1 系統軟體身份

5.1.1.1 產品應擁有唯一性識別資訊，並可被正確辨識。(2 級)

5.1.2 系統軟體運行狀態

5.1.2.1 產品應提供可辨識的已知運行狀態。(2 級)

5.1.3 安全更新

5.1.3.1 產品應在使用者環境中，提供安全的產品更新功能。(2 級)

5.2 密碼安全

5.2.1 演算法安全

5.2.1.1 產品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)

5.2.2 金鑰安全

5.2.2.1 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)

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

5.2.3 亂數產生器安全

5.2.3.1 產品應使用符合國際標準要求，或公認資安產業慣例之亂數產生演算法，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)

5.3 軟體安全

5.3.1 安全隔離

5.3.1.1 產品應提供應用程式元件的隔離功能，使得攻擊者即使可以在應用程式某部件(application part)上執行惡意行為，也無法損害應用程式其它部件的機密性和完整性。(3 級)

5.3.2 安全狀態

5.3.2.1 產品應具備驗證應用程式真實性之能力。(2 級)

5.3.2.2 產品應提供應用程式可辨識的已知運行狀態，例如燈號、警示訊息、圖示等。(3 級)

5.3.3 安裝/更新/卸載安全

5.3.3.1 產品應在使用者環境，及不安全的產品生產現場中，提供安全的應用程式安裝功能。(2 級)

5.3.3.2 產品應在使用者環境中，提供安全的應用程式安全更新功能。(2 級)

5.3.3.3 產品應提供安全卸載功能，銷毀應用程式資料，以防止潛在攻擊者透過物理接觸，獲取敏感性資料及個人資料。(2 級)

5.4 儲存安全

5.4.1 資料保護

5.4.1.1 應用程式儲存的所有資料，應受到真實性和完整性的保護。(2 級)

5.4.1.2 產品應使用加密方式保護儲存資料的機密性和完整性。(2 級)

5.4.1.3 所有儲存在產品直接控制之外，且非屬例外列表所含的資料，應受到保護。(2 級)

5.4.2 資料安全銷毀

5.4.2.1 記憶體中已刪除的資料應確實被清除，且無法復原。(3 級)

5.4.3 日誌保全

5.4.3.1 產品應提供安全的日誌產生及儲存方式。(2 級)

5.4.4 增長紀錄保全

5.4.4.1 產品應提供可靠的增長計數器(only-increasing counter)，並避免計數器數值遭受竄改或刪除。(3 級)

5.5 通訊安全

5.5.1 協定安全

5.5.1.1 產品所使用的安全通道協定，應符合安全規範，如 TLS 1.2 的 TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384 等。(2 級)

5.5.1.2 產品所實施(implement)使用的通信協定，應與宣告者相符。 (2 級)

5.5.1.3 產品應僅提供必要運行所需的網路服務。(2 級)

5.6 韌體安全

5.6.1 韌體內容安全

5.6.1.1 韌體中不應含有明文 CSP，及未經宣告之 IP、URL 及 email。(2 級)

5.6.1.2 韌體不應存在漏洞評鑑系統 CVSS v3 中，嚴重性等級評比為高之資安風險漏洞。(2 級)

5.6.1.3 韌體於執行逆向工程後，不應存在原始碼、目的碼，或即時編譯程式碼(just-in-time compiled code)。(3 級)

5.6.2 韌體保護

5.6.2.1 韌體應具備完整性驗證機制，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之最佳演算法。(2 級)

5.6.2.2 韌體應具備真實性驗證機制，且用於真實性之金鑰應受到保護。(2 級)

5.6.2.3 韌體應具備完整性保護機制，以防止使用者將遭竄改之韌體進行更新。(2 級)

5.6.2.4 韌體應具備真實性保護機制，以防止使用者將偽造之韌體進行更新。(2 級)

附錄 A：驗證結果重用

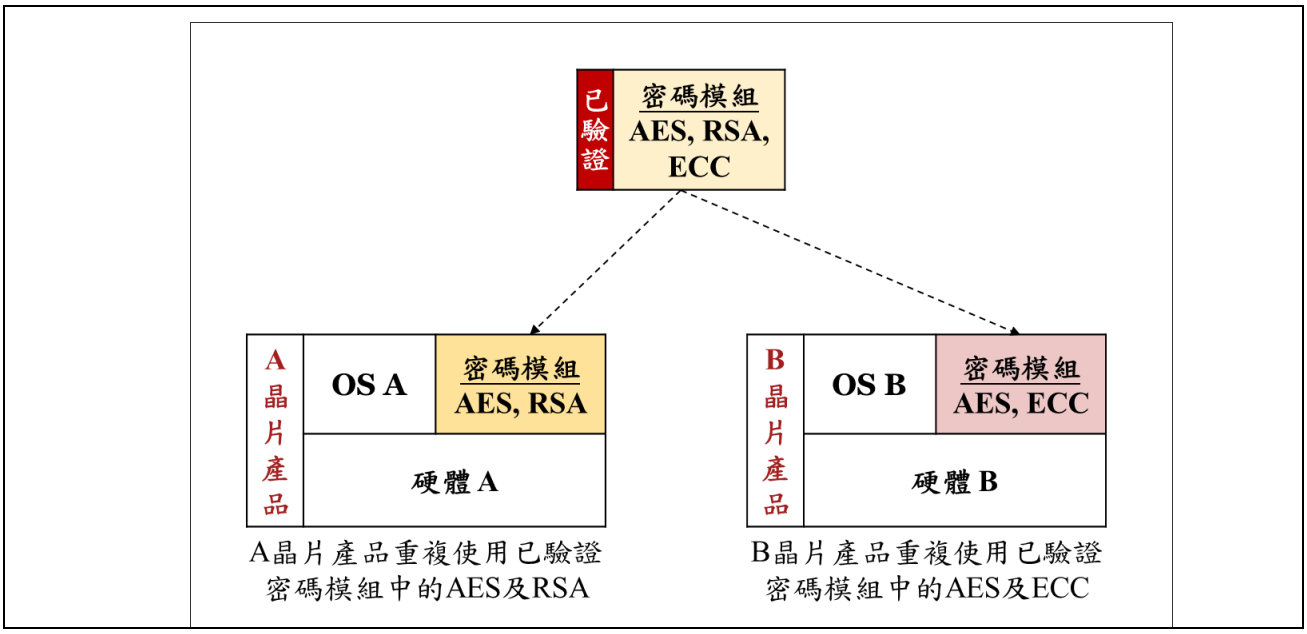
ICT 產品通常很複雜，通常是通過組合多個硬體和軟體元件來構建而成，其中包括保護關鍵資產的安全元件。本標準定義了獨立評估系統軟體及元件的方法，並可在任何的 ICT 產品中重複使用驗證結果。這些驗證結果可以來自本標準，也可以來自其它兼容的外部驗證結果，例如：重複使用 CC (Common Criteria)的驗證結果。

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 1 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.

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