

Evaluation Systems & Common Criteria

中英雙語解釋 / Bilingual Explanation

購買安全產品的挑戰 / The Challenge of Buying Security Products

- **理想流程**：選購安全產品理論上應包含：
 - *The ideal process:*
 - 評估自身需求，確定安全要求。
 - *Assess needs to determine requirements.*
 - 識別能滿足這些要求的產品。
 - *Identify the product that will meet those requirements.*
 - 購買並部署該產品。
 - *Purchase the product and deploy it.*
- **現實問題**：大多數客戶缺乏有效執行這些步驟的專業知識。他們難以判斷產品的安全聲明是否屬實，或產品是否真正符合其需求。
 - *The problem: Most customers lack the expertise to perform these steps effectively. They struggle to verify security claims or if a product truly fits their needs.*
- **解決方案**：建立一個標準化的、由獨立專家團隊執行的評估與認證流程，為安全產品提供一個經認證的信任等級，幫助消費者做出明智決策。
 - *A solution: Provide a standardized process of independent evaluation by expert teams to provide a certified level of confidence for security products.*

評估方法論 / Evaluation Methodology

一個評估標準通常提供以下內容：

An evaluation standard typically provides:

1. 一組定義安全功能的「功能要求」：說明產品「能做什麼」（例如，支援哪些加密演算法、存取控制方法）。
 - *A set of **functional requirements** defining security functionality: What the product "does" (e.g., supported encryption algorithms, access control methods).*
2. 一組建立功能要求所需的「保證要求」：說明產品「如何被可信地建造和測試」，以確保其功能被正確實現且沒有重大漏洞。這涉及開發流程、測試深度、文件完整性等。

- A set of **assurance requirements** needed for establishing confidence that the functional requirements are met. This addresses how the product is "trustworthily built and tested" (development process, testing rigor, documentation).
3. 一套用於判定產品是否滿足要求的「評估方法學」：指導評估人員如何進行測試與審查。
- A **methodology** for determining that the functional requirements are met. Guides evaluators on how to test and review.
4. 一個表示評估結果的「信任等級度量」：以清晰的分級（如等級1-4、EAL1-EAL7）來表示產品的整體可信度。
- A **measure of the evaluation result** indicating the trustworthiness of the evaluated system, often as a clear rating (e.g., Level 1-4, EAL1-EAL7).

密碼模組認證標準範例：FIPS 140-2 / Example: Cryptographic Module Certification - FIPS 140-2

對於密碼功能，美國聯邦機構被要求使用經過國家安全局（NSA）批准或通過 FIPS 140-2（《密碼模組安全要求》）驗證的產品。這是一個廣受國際認可的標準。

For cryptographic functions, U.S. federal agencies must use products validated to FIPS 140-2 (Security Requirements for Cryptographic Modules). This is a widely recognized international standard.

- **核心做法**：約有150家供應商將其密碼模組交由獨立實驗室進行合規性/一致性測試，以獲得認證。
 - Core practice: Vendors have independent labs test their modules for compliance.
- **分級制度**：FIPS 140-2定義了四個安全等級，用於保護敏感但非機密資訊的密碼設備。
 - Grading system: FIPS 140-2 defines four security levels for cryptographic devices.

FIPS 140-2 安全等級詳解 / FIPS 140-2 Security Levels Explained

- **等級 1 - 基本安全**
 - Level 1 - Basic Security
 - **要求**：至少使用一種經批准的密碼演算法或函數。必須在生產級設備上執行（例如，使用未經評估作業系統的通用電腦）。
 - Requirements: At least one approved algorithm. Must run on production-grade equipment (e.g., a general-purpose computer with an unevaluated OS).
 - **典型應用**：個人軟體加密工具、基礎的網路安全協定。
 - Typical use: Personal software encryption tools, basic network security protocols.

- 等級 2 - 增強型安全

- *Level 2 - Enhanced Security*
- 要求：包含等級1所有要求，並增加：
 - *Requirements: All Level 1, plus:*
- 實體安全：具備防竄改塗層、封條或防撬鎖。
 - *Physical security: Tamper-evident coatings/seals or pick-resistant locks.*
- 身份驗證：提供基於角色的驗證。
 - *Authentication: Role-based authentication.*
- 軟體密碼學：允許在多使用者系統中使用軟體密碼學，前提是底層作業系統需符合 Common Criteria EAL2或更高保證等級。
 - *Software crypto: Allowed in multi-user systems if the OS meets Common Criteria EAL2 or higher.*

- 等級 3 - 高度安全

- *Level 3 - High Security*
- 要求：包含等級2所有要求，並增加：
 - *Requirements: All Level 2, plus:*
- 實體安全：增強型防竄改與對抗措施（許多商業產品可達到）。
 - *Physical security: Enhanced tamper-resistance and countermeasures.*
- 身份驗證：基於身份的驗證。
 - *Authentication: Identity-based authentication.*
- 作業系統：底層作業系統需在特定Common Criteria保護綱要下達到EAL3等級。
 - *Operating System: Underlying OS must be EAL3 under a specific Common Criteria Protection Profile.*

- 等級 4 - 最高級安全

- *Level 4 - Highest Security*
- 要求：包含等級3所有要求，並增加：
 - *Requirements: All Level 3, plus:*
- 實體安全：對密碼模組提供完整的保護外殼，能偵測並回應未授權的實體存取嘗試，並在偵測到竄改時立即清零所有金鑰。
 - *Physical security: Complete protective envelope to detect/respond to physical access attempts, including **immediate zeroization of keys upon tampering**.*
- 環境保護：提供針對惡劣環境條件（如極端電壓、溫度）的保護。
 - *Environmental protection: Protection against environmental compromise.*

- **軟體/韌體**：模組的軟體/韌體元件可在符合Common Criteria EAL4或更高等級的通用作業系統上執行。
 - *Software/Firmware: Can run on a general-purpose OS meeting EAL4 or higher.*
- **典型應用**：用於高價值交易、軍事通信或惡劣物理環境中的硬體安全模組。
 - *Typical use: Hardware Security Modules for high-value transactions, military comms, or harsh environments.*

共同準則簡介 / A Note on Common Criteria

FIPS 140-2中多次提及的**共同準則**是一個更通用、國際化的IT安全產品評估標準（ISO/IEC 15408）。它使用**評估保證等級**來衡量產品開發與測試過程的嚴謹度。FIPS 140-2在較高等級中引用CC，是為了對運行密碼模組的軟體平台（如作業系統）的「保證等級」提出要求。

The Common Criteria (CC) is a more general, international standard for evaluating IT security products. It uses Evaluation Assurance Levels (EALs) to measure development rigor. FIPS 140-2 references CC at higher levels to require a certain *assurance level* for the software platform running the crypto module.

小測試 / Quick Test

問題：一家線上銀行正在為其新的「行動銀行App」選擇後端使用的密碼函式庫，以保護用戶的交易資料。該函式庫將部署在銀行的標準Linux伺服器機房內。銀行最關注的是防止軟體邏輯漏洞導致金鑰洩露，並確保加密操作的正確性。根據FIPS 140-2標準的精神與等級描述，銀行採購團隊應優先關注該密碼函式庫產品的哪一項認證或特性？

選項 / Options:

1. 該產品是否通過**FIPS 140-2 等級4**認證，因為這是最高等級，能確保金鑰在物理竄改時被立即清除。
 - *Whether the product is certified to FIPS 140-2 Level 4, as it's the highest level and ensures immediate key zeroization upon physical tampering.*
2. 該產品是否通過**FIPS 140-2 等級1**認證，因為它只需要使用批准演算法，且能在通用的Linux系統上運行，成本最低、部署最靈活。
 - *Whether the product is certified to FIPS 140-2 Level 1, as it only requires approved algorithms and can run on generic Linux, offering the lowest cost and most flexible deployment.*
3. 該產品是否通過**FIPS 140-2 等級2**（或更高）認證，並且其執行所依賴的Linux作業系統發行版本本身，是否在一個相關的Common Criteria保護綱要下達到了**EAL2**或更高的評估保證等級。
 - *Whether the product is certified to FIPS 140-2 Level 2 (or higher), and whether the*

Linux OS distribution it relies on has been evaluated to EAL2 or higher under a relevant Common Criteria Protection Profile.

4. 該產品供應商是否擁有ISO 9001品質管理體系認證，以證明其公司具有標準化的生產與管理流程。
- *Whether the product vendor holds an ISO 9001 Quality Management System certification, to prove the company has standardized production and management processes.*

答案與解析 / Answer & Analysis:

- **正確答案：3**
 - *Correct Answer: 3*
- **解析：**
 - 銀行的核心關切是**軟體邏輯正確性與金鑰的邏輯保護**，而非機房內的**實體竄改**（那屬於**實體安全範疇**）。因此，需要關注的是**密碼模組在軟體環境下的安全保證**。
 - *The bank's core concern is software logic correctness and logical key protection, not physical tampering within the data center (which is a physical security concern). Thus, the focus should be on the crypto module's security assurance in a software environment.*
 - **選項1**過度針對**實體安全**。等級4主要針對可能遭受物理攻擊的環境（如放置在**公共區域**的ATM），其**金鑰清零機制**主要回應物理觸發器。對於放置在**安全機房**內的**伺服器軟體庫**而言，這並非**最關鍵**的要求，且**成本過高**。
 - *Option 1 over-emphasizes physical security. Level 4 targets physically exposed devices. Its key zeroization is physically triggered. For a software library in a secure data center, this is not the most critical requirement and is cost-ineffective.*
 - **選項2**的要求**過低**。等級1僅**保證使用正確的演算法**，但**完全沒有對其運行的軟體平台（作業系統）提出任何安全保證要求**。在一個**未經評估**、可能存在**未知漏洞**的**作業系統**上運行**密碼軟體**，**金鑰**仍有**很高風險**從**記憶體**中被**其他惡意程序**竊取，這正是**銀行**所擔憂的。
 - *Option 2 sets the bar too low. Level 1 only ensures correct algorithms but imposes no assurance requirements on the underlying OS. Running crypto software on an unevaluated, potentially vulnerable OS poses a high risk of key theft from memory by other processes, which is exactly the bank's concern.*
 - **選項3**是**精準**的答案。FIPS 140-2從**等級2**開始，明確要求：若在**多使用者系統**中使用**軟體密碼學**，其**作業系統**需**達到CC EAL2或更高**。這直接回應了**銀行**的擔憂——EAL2評估意味著**作業系統**經過了**更嚴格的設計審查和測試**，降低了其**本身存在嚴重漏洞**的風險，從而為其上運行的**密碼模組**提供了一個**更可信的執行環境**。這正是在**軟體環境**中提

升「保證等級」的具體體現。

- *Option 3 is precise. Starting at Level 2, FIPS 140-2 explicitly requires that for software crypto in multi-user systems, the OS must meet CC EAL2 or higher. This directly addresses the bank's concern — an EAL2 evaluation means the OS has undergone more rigorous design review and testing, reducing the risk of critical flaws and providing a more trusted environment for the crypto module. This is the concrete embodiment of improving "assurance" in a software context.*
 - 選項4 (ISO 9001) 是通用的品質管理認證，與產品本身的安全特性或保證等級沒有直接關係。一個流程合規的公司仍可能生產出有安全漏洞的產品。它不能替代專門的安全產品評估認證。
 - *Option 4 (ISO 9001) is a generic quality management certification, not directly related to the security features or assurance level of the product itself. A process-compliant company can still produce products with security flaws. It is not a substitute for a dedicated security product evaluation certification.*
-

中英雙語解釋 / Bilingual Explanation

購買安全產品的挑戰 / The Challenge of Buying Security Products

- **理想流程**：選購安全產品理論上應包含：
 - *The ideal process:*
 - 評估自身需求，確定安全要求。
 - *Assess needs to determine requirements.*
 - 識別能滿足這些要求的產品。
 - *Identify the product that will meet those requirements.*
 - 購買並部署該產品。
 - *Purchase the product and deploy it.*
 - **現實問題**：大多數客戶缺乏有效執行這些步驟的專業知識。他們難以判斷產品的安全聲明是否屬實，或產品是否真正符合其需求。
 - *The problem: Most customers lack the expertise to perform these steps effectively. They struggle to verify security claims or if a product truly fits their needs.*
 - **解決方案**：建立一個標準化的、由獨立專家團隊執行的評估與認證流程，為安全產品提供一個經認證的信任等級，幫助消費者做出明智決策。
 - *A solution: Provide a standardized process of independent evaluation by expert teams to provide a certified level of confidence for security products.*
-

一個評估標準通常提供以下內容：

An evaluation standard typically provides:

1. 一組定義安全功能的「功能要求」：說明產品「能做什麼」（例如，支援哪些加密演算法、存取控制方法）。
 - *A set of **functional requirements** defining security functionality: What the product "does" (e.g., supported encryption algorithms, access control methods).*
2. 一組建立功能要求所需的「保證要求」：說明產品「如何被可信地建造和測試」，以確保其功能被正確實現且沒有重大漏洞。這涉及開發流程、測試深度、文件完整性等。
 - *A set of **assurance requirements** needed for establishing confidence that the functional requirements are met. This addresses how the product is "trustworthily built and tested" (development process, testing rigor, documentation).*
3. 一套用於判定產品是否滿足要求的「評估方法學」：指導評估人員如何進行測試與審查。
 - *A **methodology** for determining that the functional requirements are met. Guides evaluators on how to test and review.*
4. 一個表示評估結果的「信任等級度量」：以清晰的分級（如等級1-4、EAL1-EAL7）來表示產品的整體可信度。
 - *A **measure of the evaluation result** indicating the trustworthiness of the evaluated system, often as a clear rating (e.g., Level 1-4, EAL1-EAL7).*

密碼模組認證標準範例：FIPS 140-2 / Example: Cryptographic Module Certification - FIPS 140-2

對於密碼功能，美國聯邦機構被要求使用經過國家安全局（NSA）批准或通過 **FIPS 140-2**（《密碼模組安全要求》）驗證的產品。這是一個廣受國際認可的標準。

*For cryptographic functions, U.S. federal agencies must use products validated to **FIPS 140-2** (Security Requirements for Cryptographic Modules). This is a widely recognized international standard.*

- **核心做法**：約有150家供應商將其密碼模組交由獨立實驗室進行合規性/一致性測試，以獲得認證。
 - *Core practice: Vendors have independent labs test their modules for compliance.*
- **分級制度**：FIPS 140-2定義了四個安全等級，用於保護敏感但非機密資訊的密碼設備。
 - *Grading system: FIPS 140-2 defines four security levels for cryptographic devices.*

FIPS 140-2 安全等級詳解 / FIPS 140-2 Security Levels Explained

- 等級 1 - 基本安全

- *Level 1 - Basic Security*
- **要求：**至少使用一種經批准的密碼演算法或函數。必須在生產級設備上執行（例如，使用未經評估作業系統的通用電腦）。
 - *Requirements: At least one approved algorithm. Must run on production-grade equipment (e.g., a general-purpose computer with an unevaluated OS).*
- **典型應用：**個人軟體加密工具、基礎的網路安全協定。
 - *Typical use: Personal software encryption tools, basic network security protocols.*

- 等級 2 - 增強型安全

- *Level 2 - Enhanced Security*
- **要求：**包含等級1所有要求，並增加：
 - *Requirements: All Level 1, plus:*
- **實體安全：**具備防竄改塗層、封條或防撬鎖。
 - *Physical security: Tamper-evident coatings/seals or pick-resistant locks.*
- **身份驗證：**提供基於角色的驗證。
 - *Authentication: Role-based authentication.*
- **軟體密碼學：**允許在多使用者系統中使用軟體密碼學，前提是底層作業系統需符合Common Criteria EAL2或更高保證等級。
 - *Software crypto: Allowed in multi-user systems if the OS meets Common Criteria EAL2 or higher.*

- 等級 3 - 高度安全

- *Level 3 - High Security*
- **要求：**包含等級2所有要求，並增加：
 - *Requirements: All Level 2, plus:*
- **實體安全：**增強型防竄改與對抗措施（許多商業產品可達到）。
 - *Physical security: Enhanced tamper-resistance and countermeasures.*
- **身份驗證：**基於身份的驗證。
 - *Authentication: Identity-based authentication.*
- **作業系統：**底層作業系統需在特定Common Criteria保護綱要下達到EAL3等級。
 - *Operating System: Underlying OS must be EAL3 under a specific Common Criteria Protection Profile.*

- 等級 4 - 最高級安全

- *Level 4 - Highest Security*
- 要求：包含等級3所有要求，並增加：
 - *Requirements: All Level 3, plus:*
- 實體安全：對密碼模組提供完整的保護外殼，能偵測並回應未授權的實體存取嘗試，並在偵測到竄改時立即清零所有金鑰。
 - *Physical security: Complete protective envelope to detect/respond to physical access attempts, including immediate zeroization of keys upon tampering.*
- 環境保護：提供針對惡劣環境條件（如極端電壓、溫度）的保護。
 - *Environmental protection: Protection against environmental compromise.*
- 軟體/韌體：模組的軟體/韌體元件可在符合Common Criteria EAL4或更高等級的通用作業系統上執行。
 - *Software/Firmware: Can run on a general-purpose OS meeting EAL4 or higher.*
- 典型應用：用於高價值交易、軍事通信或惡劣物理環境中的硬體安全模組。
 - *Typical use: Hardware Security Modules for high-value transactions, military comms, or harsh environments.*

共同準則簡介 / A Note on Common Criteria

FIPS 140-2中多次提及的**共同準則**是一個更通用、國際化的IT安全產品評估標準（ISO/IEC 15408）。它使用**評估保證等級**來衡量產品開發與測試過程的嚴謹度。FIPS 140-2在較高等級中引用CC，是為了對運行密碼模組的軟體平台（如作業系統）的「保證等級」提出要求。

*The **Common Criteria (CC)** is a more general, international standard for evaluating IT security products. It uses **Evaluation Assurance Levels (EALs)** to measure development rigor. FIPS 140-2 references CC at higher levels to require a certain *assurance level* for the software platform running the crypto module.*

小測試 / Quick Test

問題：一家線上銀行正在為其新的「行動銀行App」選擇後端使用的密碼函式庫，以保護用戶的交易資料。該函式庫將部署在銀行的標準Linux伺服器機房內。銀行最關注的是防止軟體邏輯漏洞導致金鑰洩露，並確保加密操作的正確性。根據FIPS 140-2標準的精神與等級描述，銀行採購團隊應優先關注該密碼函式庫產品的哪一項認證或特性？

選項 / Options:

1. 該產品是否通過 **FIPS 140-2 等級4** 認證，因為這是最高等級，能確保金鑰在物理竄改時被立即清除。

- Whether the product is certified to **FIPS 140-2 Level 4**, as it's the highest level and ensures immediate key zeroization upon physical tampering.
2. 該產品是否通過 **FIPS 140-2 等級1** 認證，因為它只需要使用批准演算法，且能在通用的 Linux系統上運行，成本最低、部署最靈活。
- Whether the product is certified to **FIPS 140-2 Level 1**, as it only requires approved algorithms and can run on generic Linux, offering the lowest cost and most flexible deployment.
3. 該產品是否通過 **FIPS 140-2 等級2 (或更高)** 認證，並且其執行所依賴的Linux作業系統發行版本本身，是否在一個相關的Common Criteria保護綱要下達到了**EAL2或更高的評估保證等級**。
- Whether the product is certified to **FIPS 140-2 Level 2 (or higher)**, and whether the **Linux OS distribution** it relies on has been evaluated to **EAL2 or higher** under a relevant Common Criteria Protection Profile.
4. 該產品供應商是否擁有ISO 9001品質管理體系認證，以證明其公司具有標準化的生產與管理流程。
- Whether the product vendor holds an ISO 9001 Quality Management System certification, to prove the company has standardized production and management processes.

答案與解析 / Answer & Analysis:

- 正確答案：3
 - *Correct Answer: 3*
- 解析：
 - 銀行的核心關切是軟體邏輯正確性與金鑰的邏輯保護，而非機房內的實體竄改（那屬於實體安全範疇）。因此，需要關注的是密碼模組在軟體環境下的安全保證。
 - *The bank's core concern is **software logic correctness and logical key protection**, not physical tampering within the data center (which is a physical security concern). Thus, the focus should be on the crypto module's **security assurance in a software environment**.*
 - 選項1 過度針對實體安全。等級4主要針對可能遭受物理攻擊的環境（如放置在公共區域的ATM），其金鑰清零機制主要回應物理觸發器。對於放置在安全機房內的伺服器軟體庫而言，這並非最關鍵的要求，且成本過高。
 - *Option 1 over-emphasizes physical security. Level 4 targets physically exposed devices. Its key zeroization is physically triggered. For a software library in a secure data center, this is not the most critical requirement and is cost-ineffective.*
 - 選項2 的要求過低。等級1僅保證使用正確的演算法，但完全沒有對其運行的軟體平台

(作業系統) 提出任何安全保證要求。在一個未經評估、可能存在未知漏洞的作業系統上運行密碼軟體，金鑰仍有很高風險從記憶體中被其他惡意程序竊取，這正是銀行所擔憂的。

- *Option 2 sets the bar too low. Level 1 only ensures correct algorithms but imposes no assurance requirements on the underlying OS. Running crypto software on an unevaluated, potentially vulnerable OS poses a high risk of key theft from memory by other processes, which is exactly the bank's concern.*
- 選項3是精準的答案。FIPS 140-2從等級2開始，明確要求：若在多使用者系統中使用軟體密碼學，其作業系統需達到CC EAL2或更高。這直接回應了銀行的擔憂——EAL2評估意味著作業系統經過了更嚴格的設計審查和測試，降低了其本身存在嚴重漏洞的風險，從而為其上運行的密碼模組提供了一個更可信的執行環境。這正是在軟體環境中提升「保證等級」的具體體現。
 - *Option 3 is precise. Starting at Level 2, FIPS 140-2 explicitly requires that for software crypto in multi-user systems, the OS must meet CC EAL2 or higher. This directly addresses the bank's concern — an EAL2 evaluation means the OS has undergone more rigorous design review and testing, reducing the risk of critical flaws and providing a more trusted environment for the crypto module. This is the concrete embodiment of improving "assurance" in a software context.*
- 選項4 (ISO 9001) 是通用的品質管理認證，與產品本身的安全特性或保證等級沒有直接關係。一個流程合規的公司仍可能生產出有安全漏洞的產品。它不能替代專門的安全產品評估認證。
 - *Option 4 (ISO 9001) is a generic quality management certification, not directly related to the security features or assurance level of the product itself. A process-compliant company can still produce products with security flaws. It is not a substitute for a dedicated security product evaluation certification.*

中英雙語解釋 / Bilingual Explanation

共同準則的緣起與架構 / The Origin and Structure of the Common Criteria

- **背景：**過去，對安全系統評估標準的需求導致許多國家發展出各自的國家標準（如美國的TCSEC、歐洲的ITSEC）。這些標準互不相容，造成國際貿易壁壘和重複評估。
 - *Background: The need for secure systems evaluation criteria led to incompatible national standards (e.g., TCSEC in the U.S., ITSEC in Europe), creating trade barriers and redundant evaluations.*
- **解決方案：**共同準則應運而生，它是一個由約26個國家（包括美國、加拿大、英國、德

國、法國、日本等主要經濟體) 共同簽署、認可的國際標準 (ISO/IEC 15408) 。它旨在提供一個通用、一致的評估框架。

- *Solution: The Common Criteria (CC) emerged as an international standard (ISO/IEC 15408) signed and recognized by about 26 countries, providing a common, consistent evaluation framework.*
- CC 體系組成：
 - *The CC Framework Consists of:*
 - CC 核心文件：定義了安全功能與保證要求、評估概念及等級。
 - *The CC documents: Define security functional/assurance requirements, concepts, and levels.*
 - CC 評估方法學：為評估者提供具體的技術指南。
 - *The CC Evaluation Methodology (CEM): Provides technical guidance for evaluators.*
 - 國家評估體系：各簽約國根據CC原則制定的本國具體實施與認證方案。
 - *National Schemes: Country-specific implementation and certification schemes based on CC principles.*
- 關鍵優勢：在一個簽約國完成的評估（達到特定等級），其結果在其他所有簽約國均得到相互承認，大幅促進了安全產品的國際流通。
 - *Key Advantage: Evaluations (to a certain level) by one signing country are mutually recognized by all others, greatly facilitating international trade of security products.*

核心術語與評估類型 / Core Terminology and Evaluation Types

任何關於CC的討論都充滿縮寫。以下是最關鍵的幾個：

Any discussion of the CC is acronym-heavy. Here are the most critical ones:

- **TOE**：評估對象。指提交進行評估的特定產品或系統。
 - *TOE (Target of Evaluation): The specific product or system submitted for evaluation.*
- **ST**：安全目標。一份定義了TOE具體安全要求、並說明其如何滿足這些要求的文件。它是本次評估的依據。
 - *ST (Security Target): A document specifying the security requirements for the TOE and how it meets them. It's the basis for evaluation.*
- **PP**：保護綱要。一份針對某一類產品或系統（如防火牆、智慧卡）的、與實現無關的通用安全要求規範。它是撰寫ST的模板或參照。

- *PP (Protection Profile): A generic, **implementation-independent** security specification for a category of products/systems (e.g., firewalls, smart cards). It serves as a template for writing an ST.*
- **EAL：評估保證等級**。衡量TOE在開發和測試過程中所達到的**保證**（即「可信度」）等級，共分為EAL1到EAL7。等級越高，意味著開發過程越嚴格、文件越完備、測試越深入。
 - *EAL (Evaluation Assurance Level): A scale (EAL1 to EAL7) measuring the **assurance** (i.e., confidence) level achieved in the TOE's development and testing. Higher EAL means more rigorous process, documentation, and testing.*

CC下的兩種主要評估類型：

Two main types of evaluations under the CC:

1. **保護綱要評估**：對一份PP文件本身進行評估，確認其定義的通用要求是完整、一致且適合的。這就像評估一個「藍圖」的質量。
 - *Evaluation of a Protection Profile (PP): Assessing the **PP document itself** to ensure its generic requirements are complete, consistent, and suitable. It's like evaluating the quality of a "blueprint".*
2. **安全目標評估**：對一個具體的產品（TOE）根據其ST文件進行評估，確認產品確實滿足了ST中聲明的所有安全要求。這是針對「最終建築物」的驗收。
 - *Evaluation against a Security Target (ST): Assessing a **specific product (TOE)** against its **ST** to confirm it meets all claimed security requirements. This is the "building inspection" for the final product.*

保護綱要與安全目標詳解 / Protection Profile vs. Security Target

- **保護綱要**：
 - *Protection Profile (PP):*
 - **性質：通用規範**。描述一類產品（如「企業防火牆」）應該具備的安全特性，不綁定於任何特定廠商的實現。
 - *Nature: A **generic specification**. Describes what security features a class of products should have, independent of any vendor's implementation.*
 - **內容**：包括該類產品面臨的**威脅**、運行的**環境假設**、要達成的**安全目標**，以及具體的**IT安全要求**（功能和保證要求）。
 - *Content: Includes **threats**, **environmental assumptions**, **security objectives**, and specific **IT security requirements** for that product category.*
 - **範例**：目前存在約50多份已註冊的PP，涵蓋防毒軟體、生物辨識、防火牆、入侵偵測系統、作業系統、PKI等。

- Examples: Approximately 50 registered PPs exist for antivirus, biometrics, firewalls, IDS, operating systems, PKI, etc.

- 安全目標：

- Security Target (ST):
- 性質：產品特定文件。由產品供應商為其具體的TOE撰寫，說明「這個產品」提供了哪些安全功能來滿足需求。
 - Nature: A **product-specific document**. Written by the vendor for its **specific TOE**, stating what security functions "this product" provides.
- 與PP的關係：ST可以聲明其符合某個已評估的PP（即「基於PP」），這意味著該產品旨在滿足該PP的所有要求。ST也可以是完全獨立定義的。
 - Relationship to PP: An ST can claim **conformance** to an evaluated PP (i.e., "PP-based"), meaning the product aims to meet all requirements of that PP. An ST can also be independently defined.
- 內容：除類似PP的結構外，還包括TOE安全功能摘要（具體說明產品如何實現要求）以及符合PP的聲明（如有）和基本原理（證明要求的完整性和TOE滿足要求的能力）。
 - Content: In addition to a structure similar to a PP, it includes a **TOE Summary Specification** (how the product implements requirements), **PP Conformance Claims**, and a **Rationale**.

小測試 / Quick Test

問題：某政府機構計劃採購一批用於處理敏感公務的「智慧卡」。在招標規格中，他們要求產品必須通過「共同準則」認證。為了最有效地確保採購到的產品具備足夠且一致的安全性，並能在國際合作專案中互認，該機構在撰寫招標文件時，應採取以下哪種最明確的規格要求方式？

選項 / Options:

1. 要求投標產品必須通過 **EAL4+** 的 Common Criteria 評估。
 - *Require that the bidding product must have passed a Common Criteria evaluation at **EAL4+**.*
2. 要求投標產品必須通過基於 **【智慧卡IC平台保護綱要】** 的 Common Criteria 評估，且評估保證等級不低於 **EAL4**。
 - *Require that the bidding product must have passed a Common Criteria evaluation based on the **[Smart Card IC Platform Protection Profile]**, with an Evaluation*

3. 要求投標產品供應商提供其自行撰寫並經過評估的 **安全目標** 文件，且該ST中聲明的安全功能符合機構的內部需求清單。
 - *Require the vendor to provide its own evaluated **Security Target** document, and that the security functions claimed in the ST align with the agency's internal requirements checklist.*
4. 要求投標產品必須在其原產國獲得國家級的資訊安全產品銷售許可證。
 - *Require that the bidding product must have obtained a national-level information security product sales license in its country of origin.*

答案與解析 / Answer & Analysis:

- **正確答案：2**
 - *Correct Answer: 2*
- **解析：**
 - 本題的關鍵在於如何利用CC框架來實現採購的確定性與可比性。單純指定一個EAL等級，或接受廠商自定的ST，都可能無法保證產品滿足該類產品（智慧卡）的完整安全需求。
 - *The key is using the CC framework for **procurement certainty and comparability**. Simply specifying an EAL level or accepting a vendor's own ST may not guarantee the product meets the **complete** security needs for that product category (smart cards).*
 - 選項1只指定了保證等級（EAL4），但沒有指定功能要求。不同廠商的智慧卡，即使都達到EAL4，其實現的安全功能（如支援的加密演算法、防側信道攻擊能力、記憶體保護機制）可能差異巨大。EAL4只代表「開發過程有多嚴謹」，不直接代表「產品有什麼安全功能」。
 - *Option 1 only specifies the **Assurance Level (EAL4)**, but not the **Functional Requirements**. Different vendors' smart cards at EAL4 could have vastly different security features. EAL4 indicates "how rigorously it was built," not directly "what security features it has".*
 - 選項2是最佳實踐。它同時指定了：
 - *Option 2 represents best practice. It specifies both:*
 - **功能要求集：**通過引用一份業界公認、經過評估的**保護綱要**，明確了智慧卡這類產品必須滿足的**完整安全功能要求**。這確保了所有合格產品在安全功能上具備可比性和完備性。
 - *Functional Requirements: By referencing a recognized, evaluated **Protection Profile**, it defines the **complete set of security functions** a smart card must have, ensuring comparability and completeness among*

qualified products.

- **保證等級**：要求不低於**EAL4**，確保產品的開發和測試過程達到了一定的嚴謹度，從而對其實現上述功能的能力產生足夠信心。
 - *Assurance Level: Requiring at least EAL4 ensures the product's development and testing process was rigorous enough to inspire confidence in its ability to implement those functions.*
- 這種「PP + EAL」的組合，為採購提供了清晰、客觀、可驗證且國際互認的標準。
 - *This "PP + EAL" combination provides a clear, objective, verifiable, and internationally recognized standard for procurement.*
- **選項3**的問題在於，廠商自定的ST可能只包含了對其產品有利的部分功能，而刻意避開或弱化了一些實現成本高但重要的要求（如抗物理攻擊）。這導致不同廠商的ST之間無法直接比較，採購方需要耗費大量精力進行對比審查，失去了CC標準化所帶來的效率優勢。
 - *Option 3's flaw is that a vendor's own ST may only include features favorable to its product, omitting costly but important requirements. This makes comparison between vendors difficult and loses the efficiency benefits of CC standardization.*
- **選項4**與國際通用的CC認證無關。國家銷售許可可能基於不同的、非國際互認的標準，無法保證產品的安全特性符合國際共識，也無法在其他簽約國獲得承認。
 - *Option 4 is unrelated to the internationally recognized CC certification. A national sales license may be based on different, non-mutually recognized standards, failing to ensure the product meets international security consensus or gains recognition in other CC countries.*