Security objectives for the IoT Secure Communications Module (Cont.)

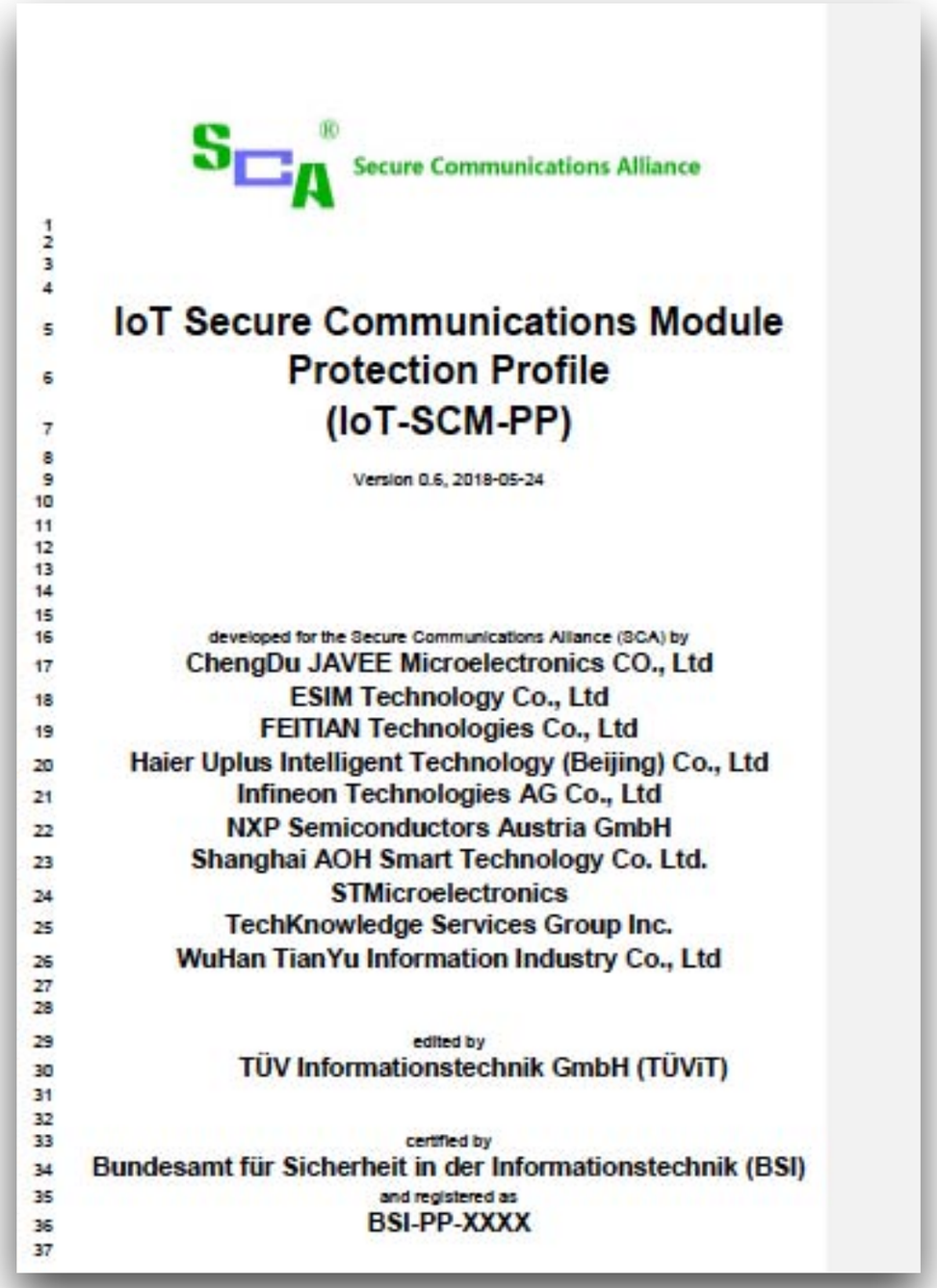
- **Cryptographic keys protection 秘鑰保護**
  - **Countermeasures against disclosing cryptographic keys stored in the TOE by performing timing analysis on operations with those keys shall be employed by the TOE.**
- **Securely Update 安全更新**
  - **The TOE shall provide functionality to securely update its firmware or parts thereof, protected concerning authenticity and confidentiality.**
- **Utilise Secured Elements 下列作業，必須使用通過安全認證之安全元件**
  - **The TOE shall use and rely on an IoT SE, which is evaluated and certified according to Protection Profile IoT-SE-PP, for the following operations:**
    - **Generation of a signature or MAC over data to be sent to the IoT Device Admin as a proof of authenticity, using the Device Authentication Key (DAK) stored in the IoT SE;**
    - **Verification of authenticity of data sent by the IoT Device Admin by verification of the corresponding signature or MAC coming with those data, using the Admin Authentication Key (AAK) stored in the IoT SE;**
    - **Random number generation.**

Security objectives for the SCM Operational Environment

- **Integration: IoT 開發商”必須”將認證通過之安全通信模塊 (IoT SCM) 整合到 IoT 產品當中，並且將 SCM 作為 IoT 產品與安全元件 (IoT SE) 之間唯一的連線通道**
  - **The IoT device manufacturer shall integrate the IoT SCM TOE into the IoT host device in a way that without significant physical modifications the IoT SCM TOE can only be used in connection with its intended IoT host device and IoT SE.**
- **No Bypass: 開發商必須確保“所有的通信”都只能透過 SCM 進行**
  - **The IoT device manufacturer shall implement the IoT host device in a way that all communication with external network devices will be mediated via the IoT SCM TOE only, i.e. by construction, communication of the IoT application with external network devices shall only be possible if mediated by the TOE.**
- **Firmware Keys 確保韌體映射檔案必須受到保護**
  - **Regardless of which type SCM-FAK is, it shall be only shared for firmware updates for those IoT SCM products, which can install/execute identical SCM FW Update Images; for IoT SCM products which cannot, different product-specific SCM-FAK shall be generated and used by the IoT SCM developer.**

IoT Secure Communications Module Protection Profile (IoT-SCM-PP) - EAL2 augmented by ALC_FLR.1

- secure channel functionality for communication to external network devices, regardless whether those are located in the same LAN as the IoT device or in some WAN (typically the internet);
- enforcement of strong cryptographic protection concerning authentication of channel endpoints, and confidentiality-protection and authenticity-protection of data transferred;
- allowing the IoT application to connect/communicate only to/ with those network addresses, which have been configured by the remote IoT SCM administrator and securely transferred into the TOE;
- blocking the IoT application from any non-allowed incoming connections, from non-authentic communication data and from communication data, which were not meeting the enforced minimum cryptographic protection level;
- providing cryptographic services and random numbers to the IoT application;
- secure update of the IoT SCM firmware; and furthermore
- enabling communication of the administrator of the IoT SE with the IoT SE and enabling firmware updates of the IoT SE.


Secure Communications Alliance

IoT Secure Communications Module Protection Profile (IoT-SCM-PP)

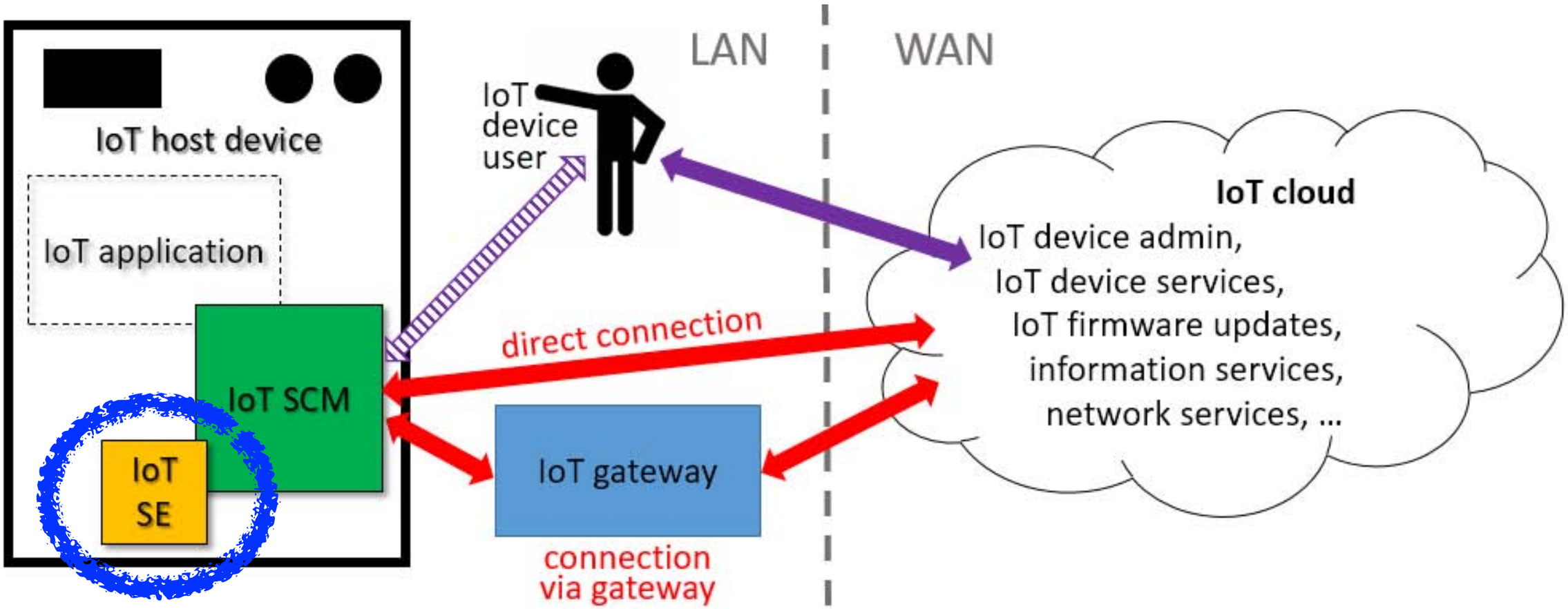
Version 0.6, 2018-05-24

developed for the Secure Communications Alliance (SCA) by
ChengDu JAVEE Microelectronics CO., Ltd
ESIM Technology Co., Ltd
FEITIAN Technologies Co., Ltd
Haier Uplus Intelligent Technology (Beijing) Co., Ltd
Infineon Technologies AG Co., Ltd
NXP Semiconductors Austria GmbH
Shanghai AOH Smart Technology Co. Ltd.
STMicroelectronics
TechKnowledge Services Group Inc.
WuHan TianYu Information Industry Co., Ltd

edited by
TÜV Informationstechnik GmbH (TÜViT)

certified by
Bundesamt für Sicherheit in der Informationstechnik (BSI)
and registered as
BSI-PP-XXXX

IoT Secure Element Protection Profile (IoT-SE-PP)



Threats to the IoT SE

- **Impersonation 假扮/冒充認可的 IoT 設備接收或發送信息**
  - **An attacker may try to send data to the IoT device the IoT SE TOE is integrated in, impersonating the IoT device admin, or to send data to the IoT device admin, impersonating the TOE, without the respective receiving party being able to detect that.**
- **Modification 竄改 (modify) / 重送 (replay) SE 與 IoT 設備之間的通信內容**
  - **An attacker may try to intercept communication between the IoT device the IoT SE TOE is integrated in and the IoT device admin to modify or replay transmitted IoT device data or IoT admin data, without the respective receiving party being able to detect that.**
- **Disclosure IoT 設備與 SE 之間的通信遭到竊聽遭到**
  - **An attacker may try to intercept communication between the IoT device the IoT SE TOE is integrated in and the IoT device admin to gain knowledge about transmitted IoT device data or IoT admin data.**
- **Illegal KeyAccess IoT 秘鑰遭到竄改與誤用**
  - **An attacker may try to read out private or secret keys from the IoT SE TOE by logical means. An attacker may try to modify keys stored inside the TOE by logical means. An attacker might try to use keys stored in the TOE for cryptographic operations these are not intended for.**

Security objectives for the IoT Secure Element

- **Data authenticity 數據認證**
  - **The TOE shall provide functionality of data authenticity protection by adding electronic signatures or message authentication codes (MACs) to data to be sent to the IoT device admin, and by verification of electronic signatures or message authentication codes (MACs) of data received from the IoT device admin.**
- **Data confidentiality protection 數據加密保護**
  - **The TOE shall provide functionality of data confidentiality protection by encryption of data sent to the IoT device admin, and by decryption of ciphertext data received from the IoT device admin. The encryption mechanism(s) used shall provide security strength of at least 100 bits.**
- **Key Access 秘鑰保護**
  - **The TOE shall not allow disclosure of secret or private cryptographic keys by logical means. The TOE shall restrict entering and updates of any kind of cryptographic keys (or key certificates, if used) by logical means to the IoT device admin. The TOE shall not allow keys being used in cryptographic operations they are not intended for.**

Security objectives for the IoT Secure Element (cont.)

- **Securely Update 安全更新**
  - **The TOE shall provide functionality to securely update its firmware or parts thereof, protected concerning authenticity and confidentiality.**
- **Physical Protection 物理保護儲存在 TOE 的資產**
  - **The TOE shall protect all its assets stored internally from disclosure and undetectable modification, substitution and/or deletion by physical means, including physical probing or modification, information-leakage analysis and fault-injection methods.**
- **Strong RNG 有品質的隨機數**
  - **The TOE shall provide a cryptographically strong random number generator suitable for any kind of application up to the generation of ephemeral keys for DSA or ECDSA, based on a TOE-internal entropy source.**

Security objectives for the SE Operational Environment

- **Integration: IoT 開發商”必須”將認證通過之安全元件 (IoT SE) 整合到 IoT 產品當中，並且將 SE 作為 IoT 產品與安全通信模塊 (IoT SCM) 之間唯一的連線通道**
  - **The IoT device manufacturer shall integrate the IoT SE TOE into the IoT host device in a way that without significant physical modifications the IoT SE TOE can only be used in connection with its intended IoT host device and IoT SCM.**
- **SE Keys: 秘鑰產生、管理**
- **Firmware Keys 確保韌體映射檔案必須受到保護**
  - **Regardless of which type SE-FAK is, it shall only be shared for firmware updates for those IoT SE products, which can install/execute identical SE FW update images; for IoT SE products which cannot, different product-specific SE-FAK shall be generated and used by the IoT SE developer.**

IoT Secure Element Protection Profile (IoT-SE-PP) - EAL4 augmented by AVA_VAN.4 and ALC_FLR.1

- **Storage and usage of device-individual cryptographic keys for**

  authentication of the TOE against network devices and remote users, and
  authentication of data protected sent from the IoT host device via the TOE to connected network devices and remote IoT device users;

- **Access control concerning usage and update of keys stored/used in the TOE;**

- **Entropy generation and random bit generation as a service for the IoT host device;**

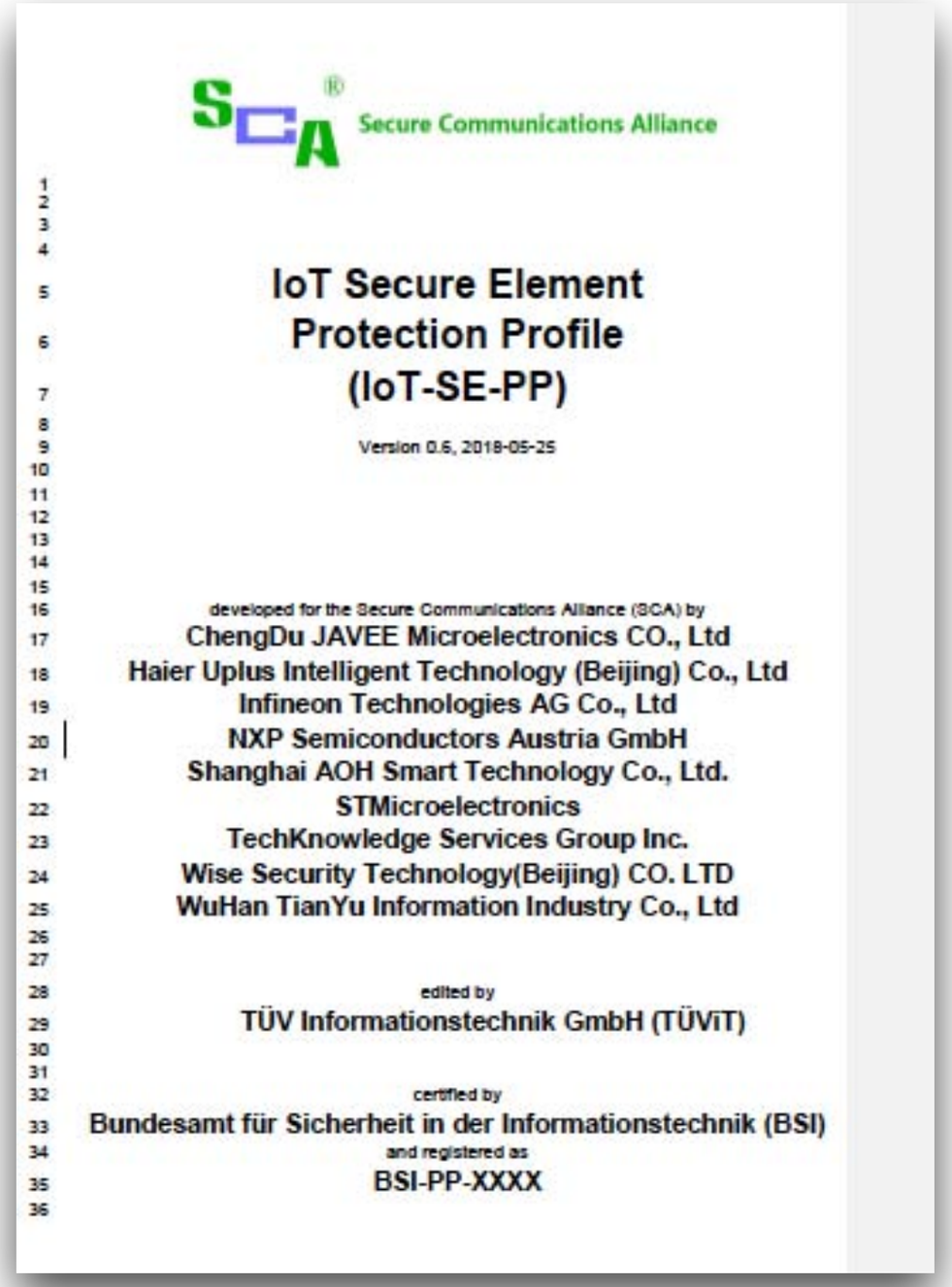
- **Secure update of TOE firmware;**

- **Protection of internally stored assets from disclosure or modification by physical probing, physical modification, information leakage analysis and fault-injection techniques.**

- **Optional Functionality, this PP does not require the following security functionality for the IoT SE TOE, though it might be – among others – added by the ST author:**

  - **Generation of cryptographic keys for TOE-internal or TOE-external use (if used, the random number generator of the TOE shall be used as a basis);**

  - **Access-controlled storage as a service functionality for IoT SCM and/or IoT host device.**



Secure Communications Alliance

IoT Secure Element
Protection Profile
(IoT-SE-PP)

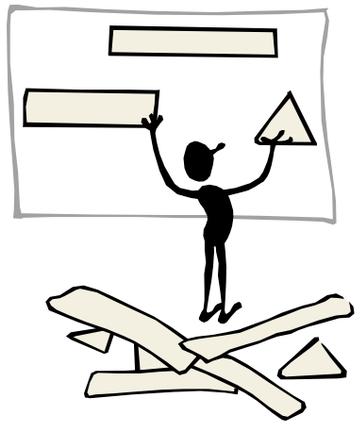
Version 0.6, 2018-05-25

developed for the Secure Communications Alliance (SCA) by
ChengDu JAVEE Microelectronics CO., Ltd
Haier Uplus Intelligent Technology (Beijing) Co., Ltd
Infineon Technologies AG Co., Ltd
NXP Semiconductors Austria GmbH
Shanghai AOH Smart Technology Co., Ltd.
STMicroelectronics
TechKnowledge Services Group Inc.
Wise Security Technology(Beijing) CO. LTD
WuHan TianYu Information Industry Co., Ltd

edited by
TÜV Informationstechnik GmbH (TÜViT)

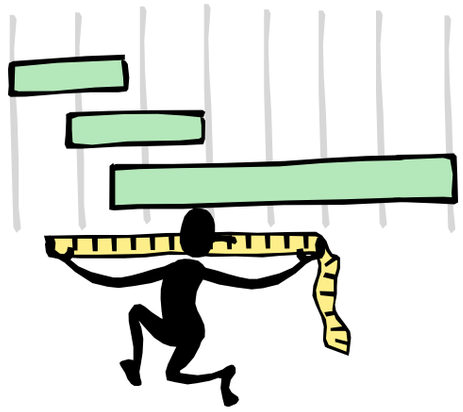
certified by
Bundesamt für Sicherheit in der Informationstechnik (BSI)
and registered as
BSI-PP-XXXX

信息技術安全評估規劃



in parallel

與開發同步



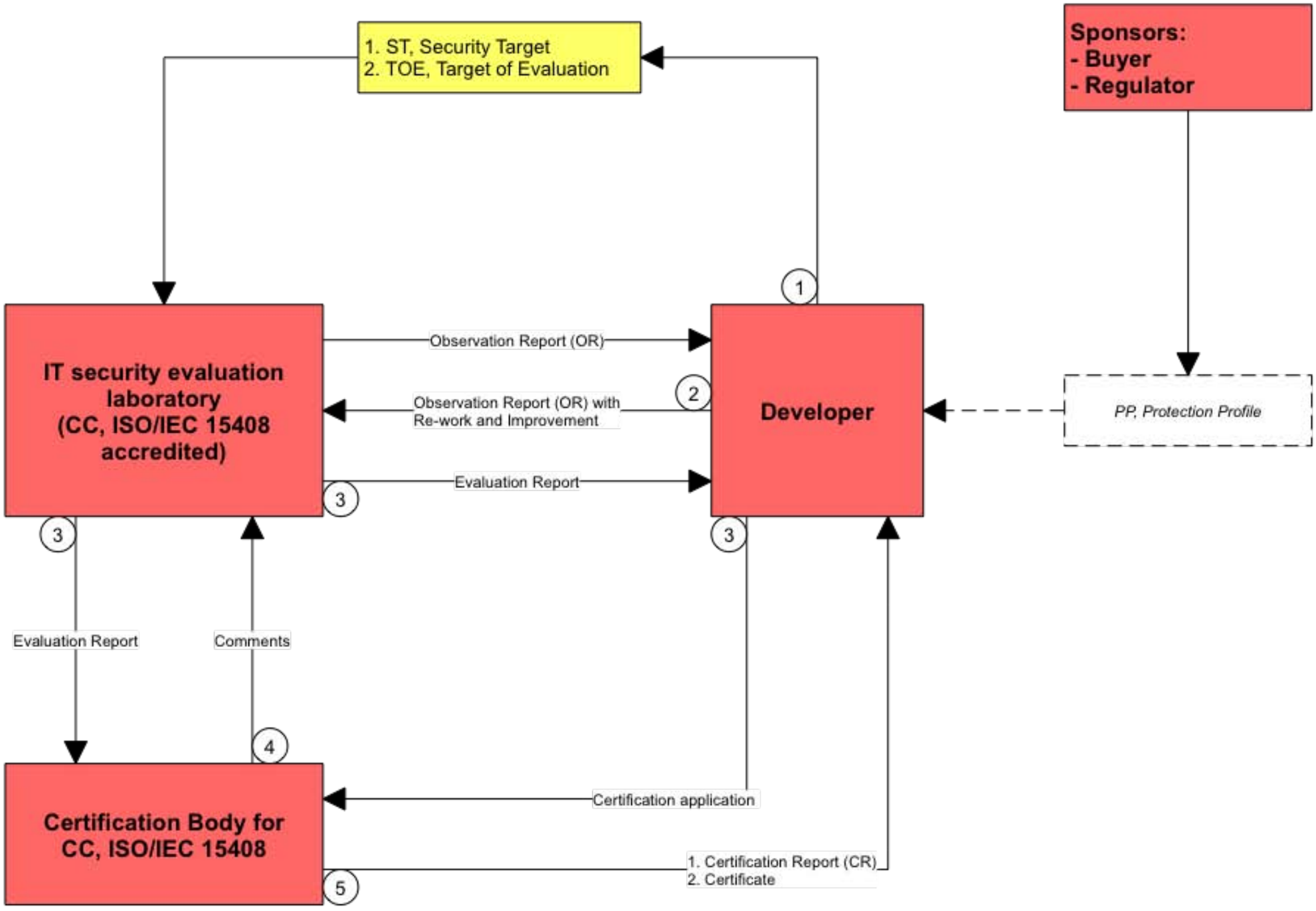
after TOE development has finished

評估對象開發完成後

Re-Evaluation / Maintenance

重新認證與維護

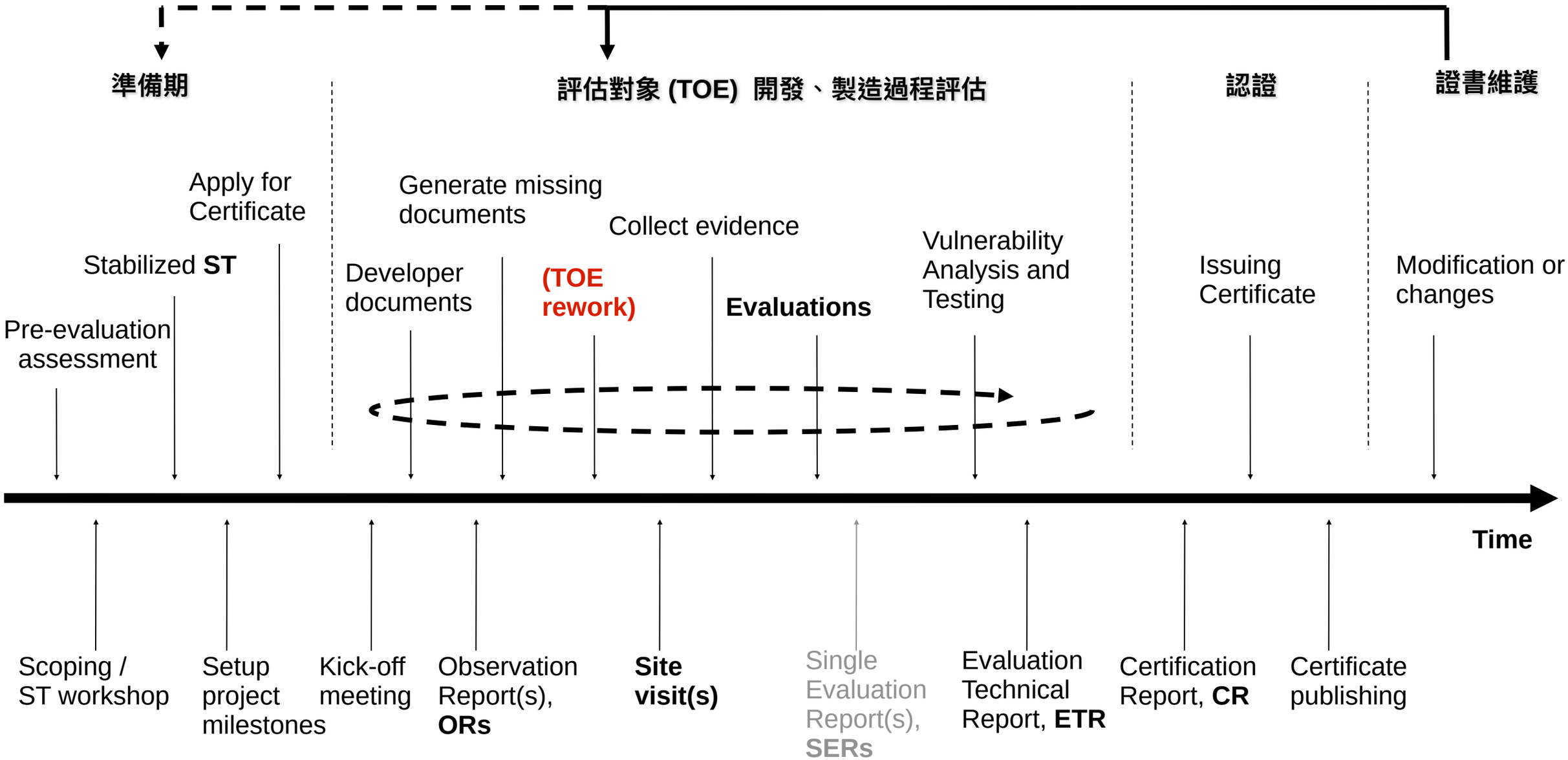
信息技術安全評估、認證過程



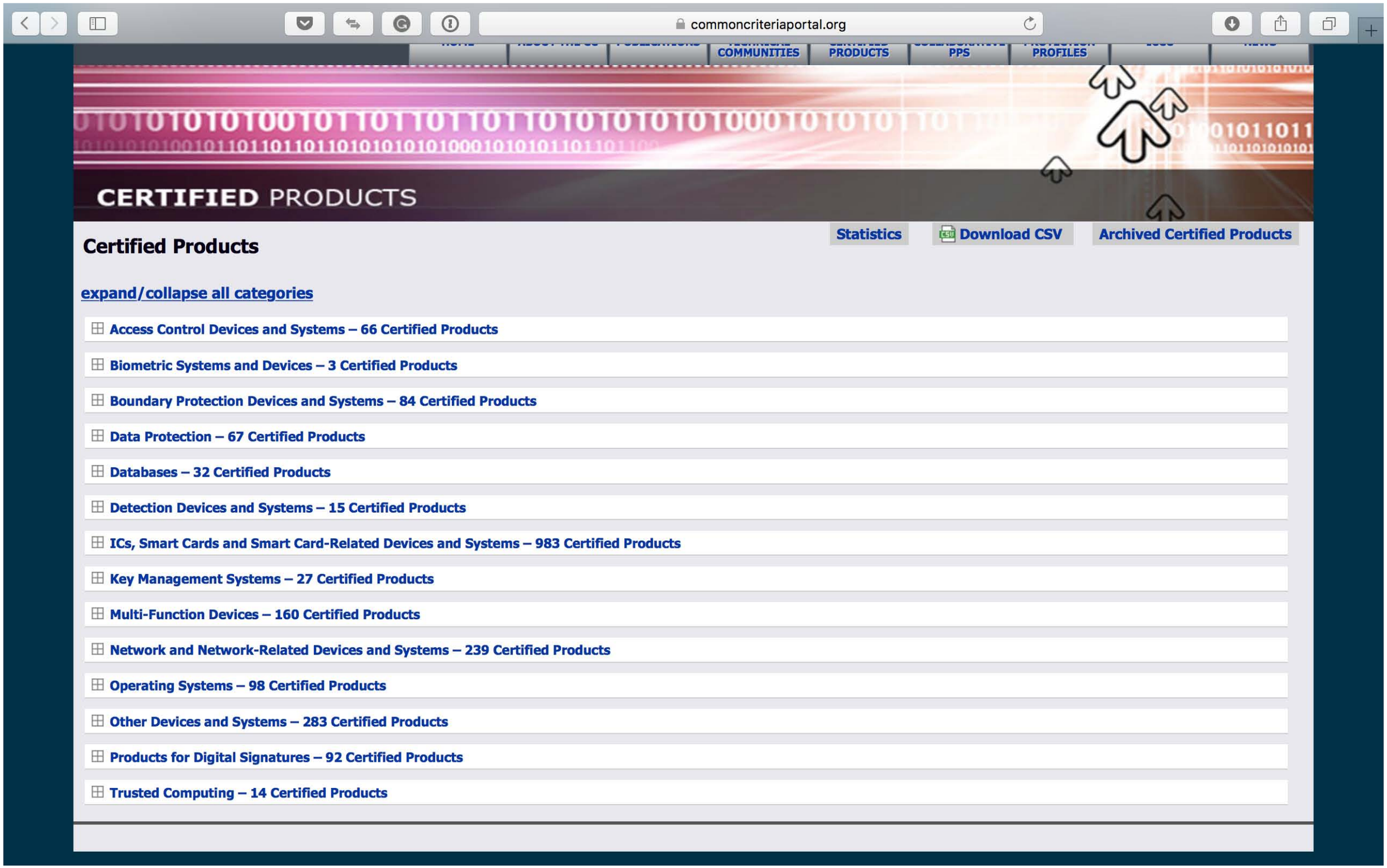
信息技術安全評估文檔類別

- 組織安全政策
- 設計文件：功能、架構、自我保護、原始設計圖或源代碼 (EAL4 以上)、開發工具
- 配置管理
- 測試文件：測試計畫、分析、結果、深度、廣度
- 安全詳細操作、使用、生成說明
- 安全開發流程、環境安全管理與控制文檔
- 脆弱性分析、評估文檔
- 其他支持性文檔，例如，原廠安全開發手冊

信息技術安全評估項目管理 (up to EAL4)



國際信息技術安全認證註冊



- **End 終**

