財團法人電信技術中心出國報告

參加 2023 法國歐洲電信標準協會資安研討會(ETSI Security Conference 2023)

單位名稱：財團法人電信技術中心
姓名職稱：牛愛元 助理工程師
何柏逸 助理工程師
派赴國家：法國
出國期間：2023 年 10 月 14 日至 2023 年 10 月 21 日止

摘要

2023 年 ETSI Cyber Security conference(歐洲電信標準協會年度網路安全活動)會議於 2023 年 10 月 16 至 19 日於法國 ETSI 總部 Sophia Antipolis 科技園區舉辦，本次會議集結了來自世界各地，並擁有不同專業知識領域的學者進行講座，其中包括 Google、Samsung 等大型團隊共同參與。

本次會議主題的重心放在全球安全標準的實施，主要內容為人工智慧、5G、物聯網、零信任架構等各個領域上的應用，與過往不同的是還添加了許多不同的主題，像是如何招募下一代的網路安全菁英，以及如何讓網路安全的意識傳達給消費者。

透過參與本次會議，公司可以獲取各國標準及法規的更新資訊，並獲取更新內容對公司目前技術上的應用，進而提升公司在產業中的競爭力。

目錄

圖目錄

表目錄

壹、目的

本次會議聚集了來自世界各國的技術專家及標準制定委員，會議過程由ETSI 團隊進行主持，本次會議自 10 月 16 日開始，至 10 月 19 日結束，共為期四天。前半段的主題放在全球網路安全、各國安全標準制定、資料保護和隱私、零信任機制、供應鏈管理、量子安全密碼學，後半段則是針對人工智慧、5G 等技術主題進行演講。

本中心為執行數位發展部「112 年度建立主動式防禦強化通傳網路防護韌性計畫工項」補助計劃案，並由中心指派何柏逸及牛愛元兩位助理工程師至法國出席，參與 ETSI Cyber Security conference(歐洲電信標準協會年度網路安全活動)會議，了解國際間對於各應用領域資安規範擬定的狀況、新興技術如量子密碼學或是 6G 未來的發展，期能蒐集解決方案或是參考制定規範的方法，協助提升我國資安防護能力，並和國際資安趨勢接軌。

貳、行程

表 1、出差行程表

日期	行程
2023 年 10 月 14(六)至 15 日(日)	啟程，前往法國尼斯
2023 年 10 月 16(一)	參加 ETSI Security Conference 2023- 1. 全球網路安全 (Global Cyber Security) 2. 各國制定規範之情況 (Regulation State of the Nation) 3. 由技術面探討規範、資料保護與隱私 (Regulation, Data Protection and Privacy, Technical Aspects)
2023 年 10 月 17(二)	參加 ETSI Security Conference 2023- 1. 零信任、供應鏈和開源 (Zero Trust, Supply Chain & Open Source) 2. 物聯網及認證 (IoT & Certification) 3. 量子安全密碼學 (Quantum Safe Cryptography Session)
2023 年 10 月 18(三)	參加 ETSI Security Conference 2023- 1. 吸引下個世代的工程師與投資未來 (Experiences of Attracting Next Generation of Engineers and Investing in Future) 2. 物聯網及認證 (IoT and Certification Session) 3. 物聯網和行動認證 (IoT & Mobile Certification) 4. 5G 實際應用 - 第 1 部分 (5G in the Wild - Part 1)
2023 年 10 月 19(四)	參加 ETSI Security Conference 2023- 1. 5G 實際應用 - 第 2 部分 (5G in the Wild - Part 2) 2. 6G 的未來

	(6G Futures) 3. 擴增實境與人工智慧 (Augmented Reality and AI)
2023年10月20(五)至21(六)	返回台灣

參、 會議過程及內容

一、 第一天

(一) 全球網路安全(GLOBAL CYBER SECURITY)

開場的主題演講由歐盟網絡安全局、Google 和前 Intel 夥伴分享關於全球網路安全(Cyber Security)的趨勢以及該如何做到研究和實務相互結合。在演講中提到，網路安全的廣義定義為網路空間中安全和營運的策略、政策和標準，包括國際參與、事件應對、執法、資訊保全、外交以及對全球資訊基礎設施安全和穩定至關重要的其他領域。

Information Security Forum(ISF)提到 2017 時主要的威脅領域為：

1. 連接(Connectivity)：

   過度依賴連結和電子流程會導致攻擊（來自 DDoS、勒索軟體、內部人員等的威脅）帶來災難性後果。

2. 信任(Trust)：

   對資訊完整性的信任正在削弱（來自誤報、虛假資訊、虛假區塊鏈等的威脅）。

3. 控制(Controls)：

   智慧科技的發展和相互衝突的監管指導削弱了控制（監控、人工智慧等）。

而 2023 年面臨的威脅則是，組織建立自主防禦來對抗 AI 攻擊，排除了人類的監督，並使受到攻擊後的恢復變得更加困難。身分變得更有價值，威脅行為的主要目的為竊取私密資料。

在安全標準化這部分遇到了新的難題，包括編制標準的人員由專業團隊變為志願招募、許多標準中框架和流程的比例變高、新標準的制定時間漫長，而在全

球化的角度來看，不斷變化的地緣政治局勢或監管要求，導致國際安全標準需要調整的次數越來越頻繁，而有些標準甚至互不相容。

對此，講者提了幾點可以幫助標準制定的觀點:

1. 許多技術和流程都值得標準化，但可能沒有足夠的資源來實現所有技術的標準化，可以使用決定專案優先順序的工具來協助。
2. 制定監測採用情況的機制，以確保將努力用於最需要的地方。在發布完整版本之前建立使用標準新元素的流程。
3. 新的攻擊和技術可能會使既有的安全方法失效。我們可以開發一個「快速回應」框架，以確保安全標準的持續有效性。
4. 妥善利用工具和自動化，並與開源專案加強合作，可以緩解產品和制定標準之間時程的不一致。

接下來提到了一些關於物聯網的標準，如下圖:

圖 1、物聯網安全標準

資料來源：Google

最後，講者提到制定標準時有幾點通則可以採用，如正常化(Normalization)可以保證產品格式統一，達到全球通用；而資訊全面透明(Full Transparency)、資料隱私(Data Privacy)則可以使消費者更加安心的購買。

下一階段由歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)、OpenPolicy、Verizon 和網路安全中心(Center of Internet Security, CIS)介紹全球的網路安全。

首先，由 ETSI 的代表介紹 ETSI 於網路安全領域中所擔任的腳色。ETSI 是一個獨立、非營利的組織，有超過 900 個會員(如圖 2)，並分別來自 60 個以上不同的國家，會員包括製造商、網路業者等中小企業以及政府單位或學術研究機構，協會包括了許多專家和新創企業人士，ETSI 制定適用於全球的資訊與通訊技術(ICT)標準。

圖 2、ETSI 會員

參考來源：現場拍攝

ETSI 的網路安全技術委員會(Technical Committee on Cybersecurity, TC CYBER)於 2014 年創立，和量子安全密碼學工作團隊一起致力於產業安全挑戰以及安全政策和立法，以解決全球網路安全問題，其中包括網路安全生態系統、關鍵基礎設施安全、消費者物聯網和移動設備隱私與安全、網路安全，以及網路安全工具和指南等。

除此之外，ETSI 內還有許多小組分別負責不同領域的安全議題，小組名稱和其負責領域如下所示：

- 3GPP SA3：行動網路安全
- ISG NFV：確保網路功能虛擬化安全
- TC ITS：智慧交通系統
- ISG ETI：加密流量集成

- TC SAI：確保人工智慧安全
- TC ESI：數位簽章與信任服務
- TC SET：智慧卡與安全元件
- ISG QKD：量子金鑰分配
- TC LI：合法攔截和保留數據
- ISG PDL：授權的分散式帳本

而為了有效的制定合適的標準，ETSI 內的成員需要常常溝通，保持資訊開放、透明化，參考眾多成員的意見以達成共識，採用威脅分析、風險評估、測試或評估規範，並和其他組織互相合作(如圖 3、圖 4)，如國際標準化組織(International Organization for Standardization, ISO)、國際電工委員會(International Electrotechnical Commission, IEC) 、歐盟網絡安全局(European Network and Information Security Agency, ENISA)等，以此確保制定出的安全標準可為國際通用。

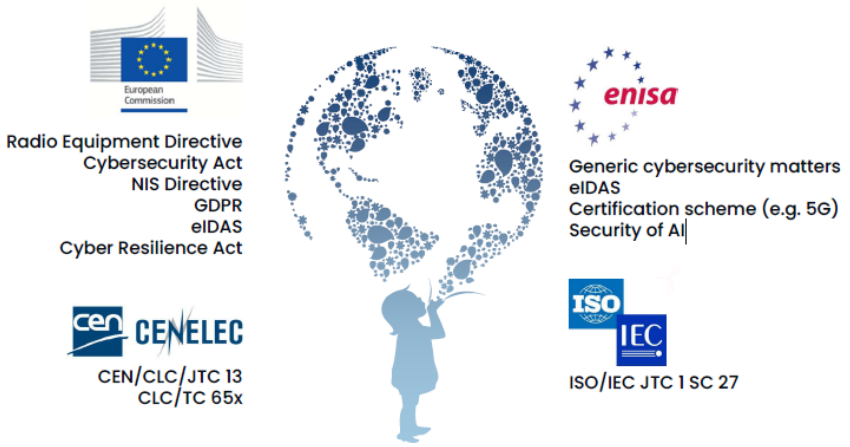


圖 3、與 ETSI 合作的組織(1)

參考來源：ETSI

圖 4、與 ETSI 合作的組織(2)

參考來源：ETSI

而簡報中也分別提到了一些當前正在保護的技術和系統，以及一些新興、尚未完成保護的領域，對於新興領域，ETSI 也在致力於完成新的法案，例如於 2022 年九月提出的資安韌性法草案 Cyber Resilience Act(CRA)，並呼籲成員們一起協助審視和修訂：

1. 正在保護的包括：
    - 行動/無線系統（5G、TETRA、DECT、RRS、RFID...）
    - 網路功能虛擬化
    - 智慧交通系統
    - 廣播
    - 人工智慧
    - 物聯網（oneM2M）
2. 新興領域：
    - 合法攔截和保留數據
    - 數位簽章與信任服務
    - 授權的分散式帳本
    - 智慧卡/安全元件
    - 安全演算法
    - 量子金鑰分發

- 量子安全密碼學
- 人工智慧

接下來第二部分由 Open Policy 由產品安全面來講述如何將安全標準及規則和市場機會連結。首先，Open Policy 是第一個由人工智慧所驅動的政策平台，透過系統自動分析、自然語言處理(Natural Language Processing, NLP)、統整市場情報，使得使用者在資訊變化甚快、眾多不同安全標準的現今，以簡單明瞭的方式理解不斷變化的情勢，降低進入市場前所需耗費的努力。講者同時也舉例了光是物聯網安全政策就有很多不同標準(如圖 5)。

圖 5、不斷發展的物聯網安全政策格局

參考來源：Open Policy

因此，如果利用更有效的 AI 技術來建立一個標準監控技術，將可以達到以下幾點效益：

1. 控制評估與互相辨認
2. 第三方監控
3. 報告和測試
4. 新控制措施的建議
5. OT 與 IT 有效融合
6. 全面的企業風險管理
7. 風險透明化

第三個講題由 Verizon 公司的夥伴分享後量子領域在網路標準生態系統(如下圖)。

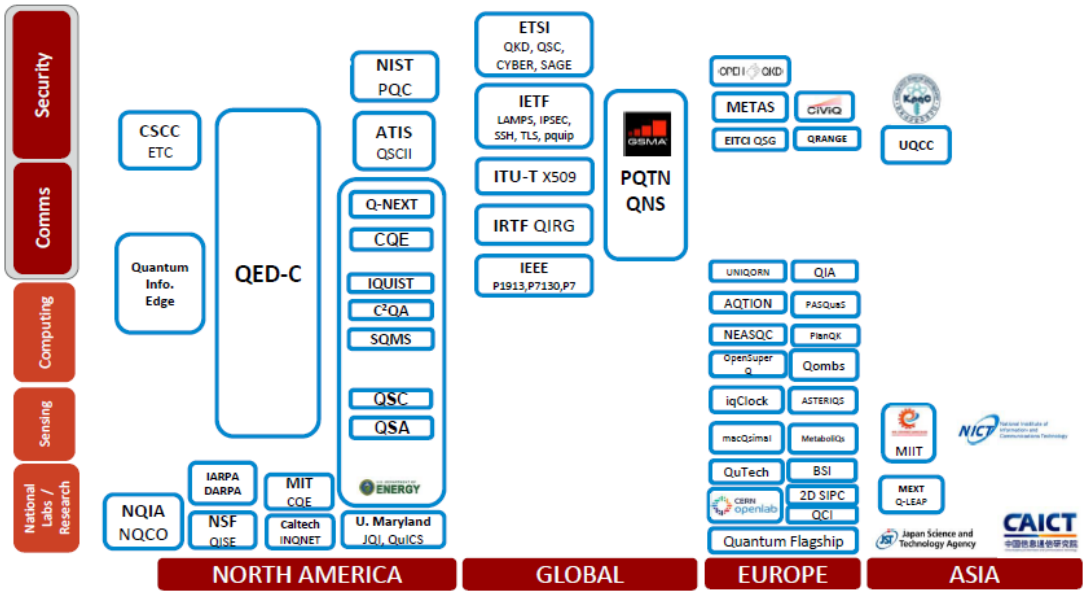


圖 6、後量子領域生態系統一覽圖

參考來源：Verizon

目前 ETSI 有許多標準提到後量子領域，如以下列所示：

- “Quantum Safe Cryptography and Security [Introduction]” (WP No.8)
- “Quantum-safe algorithmic framework” (QSC 001)
- “Case Studies and Deployment Scenarios” (QSC 003)
- “Quantum-Safe threat assessment” (QSC 004),
- “Limits to Quantum Computing applied to symmetric key sizes” (QSC 006)
- “Quantum-Safe Key Exchanges” (TR 103 570) / “QS-Hybrid Key Exchanges” (TS 103 744)
- “Critical Security Controls for Effective Cyber Defense ”(TR 103 305)

- “Migration strategies and recommendations to Quantum Safe schemes” (TR 103 619)
- “Migration to QSC for ITS” (TR 103 949)

這也說明了後量子安全領域正在興起中，各國開始關注並制定相關標準。後量子安全領域將會在後續研討會中提到更多細節。

最後，由網路安全中心(Center for Internet Security, CIS)的成員介紹軟體物料清單的重要性(Software Bill of Materials, SBOM)。首先，講者提到美國第 14028 號行政命令-改善國家網路安全(Executive Order 14028: Improving the Nation’s Cybersecurity)，為了提升軟體供應鏈安全，要求供應商須提供軟體物料清單給購買者;《聯邦食品、藥品和化妝品法案》第 524B 條「確保設備的網路安全」(Federal Food, Drug, and Cosmetic Act, Section 524B)中要求包含連接到網路的軟體的醫療設備提供 SBOM，其中包括商業、開源和現成軟體元件的數據；而歐盟的網路彈性法案(CRA)也強調了 SBOM 的重要性。軟體物料清單是將軟體中所有使用到的元件都記錄下來，使得供應鏈更方便管理所使用到的元件、確保其安全性，而美國聯邦政府要求 SBOM 清單至少必須包含以下元素：

1. 供應商名稱
2. 元件名稱
3. 元件版本
4. 唯一 ID
5. 依賴關係
6. SBOM 作者
7. 時間戳記

製作 SBOM 的好處包括紀錄軟體組建的詳細訊息、確保軟體的執照版本未過期、追蹤軟體版本並確保軟體為最新版。此外，SBOM 的格式可以被機器讀取，也有助於後續的自動化，方便整合在現有的工具中、漏洞查詢等等。目前 SBOM 有

三種格式，分別為：

1. Software Package Data eXchange (SPDX)

   此格式為 Linux Foundation 發起的。

2. CycloneDX

   是一個輕量級的軟體物料清單標準。

3. Software Identification (SWID) tags

   為一個標準化的 XML 格式。

而 SBOM 的實踐與程序包含以下幾點：

1. 頻率：如果更新軟體，那麼供應商就必須更新 SBOM。
2. 深度：必須列出足夠詳細的所有頂級依賴關係，以便遞迴地查找傳遞依賴關係。
3. 已知的未知因素：數據應明確地說明元件是否已清楚列舉依賴關係、抑或是已經沒有更多依賴關係，降低未知。
4. 分發和交付：及時提供且必須設定適當的存取權限。
5. 存取控制：提供者可以決定 SBOM 要設為公開或私人，但訪問控制的條款必須預先提供。
6. 包容錯誤：由於目前關於 SBOM 網路安全行政法規尚未成熟，因此各組織被要求對於 SBOM 發生錯誤要給予理解與包容。

最後，講者於總結時提到 SBOM 目前還在進步的階段中，鼓勵大家多加認識並運用，且不要讓完美成為進步的敵人，SBOM 的「最低要求」必須持續進步才可以達成 SBOM 的根本效益。

(二)　各國的規範制定狀況 Regulation State of the Nation

本階段的講題主要聚焦於各國訂定規範的情況，分別由 ETSI、印度電信工程中心、Schneider Electric 的講者來分享。

首先，由 ETSI 的夥伴概述歐盟網路安全監管工具和 ETSI 支援的事項。歐盟由 27 個成員國組成、7 個決策機構和 50 多個專門機構組成，其中政策與立法由歐洲議會、歐洲理事會、歐盟理事會、歐盟委員會負責，而補充機構包含歐洲法院、歐洲中央銀行、審計院。值得特別一提的是，歐盟有額外設立一個常設機構叫做歐盟網路安全局 (European Union Agency for Cybersecurity, ENISA)，其致力於提升歐洲整體網路安全水準，主要負責網路安全相關事務，包含實施網路與資訊安全指令。

歐盟發布主要網路安全措施有下列幾項：

- 網路與資訊安全 Measures for a high common level of cybersecurity (NIS2)
- Resilience of Critical Entities Directive (CER)
- 數位營運韌性法案 Digital Operational Resilience Act (DORA)
- 通訊技術認證 Communications Technology Certification (CSA, EUCC)
- 一般資料保護規則 General Data Protection Regulation (GDPR)
- 資安韌性法草案 Cyber Resilience Act (CRA) [proposed]
- 人工智慧法案 AI Act [proposed]
- 數位服務法案 Digital Services Act (DSA)

第二個主題由印度的電信工程中心(Telecommunication Engineering Centre, TEC)分享在印度的物聯網安全。TEC 是國家標準機構，負責處理電信

和 ICT 相關產業、與國際電信聯盟電信標準化部門 (ITU-T)協調，並也有加入 ETSI、oneM2M 和 3GPP 標準化活動。

再來，講者提到印度在 M2M、物聯網和 5G 等領域中有一些政策上的貢獻，例如在 2018 發布的國家數位通訊政策(National Digital Communication Policy, NDCP-2018)便有許多突出的特點：

1. 確保 50 億台連網設備的永續生態系統發展。
2. 簡化許可和監管框架，同時確保 IoT/ M2M/ 未來服務和網路元素採用適當的安全框架，並納入國際最佳實踐。
3. 開發加速部署 M2M 服務的框架，同時保護 M2M 設備的安全和攔截。
4. 為新興技術及其在通訊領域的應用制定路線圖，例如 5G、人工智慧、機器人、物聯網、雲端運算和 M2M。
5. 建立多方主導的協作機制，協調工業 4.0 轉型。
6. 開發農業、智慧城市、智慧交通網路、智慧電錶、耐用消費產品等領域的物聯網/M2M 連接服務市場。

第三個主題由 Schneider Electric 的夥伴提供，首先會先講到各國在制定標準時的情況，再來會提到國際間的標準制定。首先，講者提到碎片化會造成進步的阻礙，而美國、歐洲或亞洲各國各自進行安全相關標準的訂定將會使得這個狀況加劇（如圖 7）。

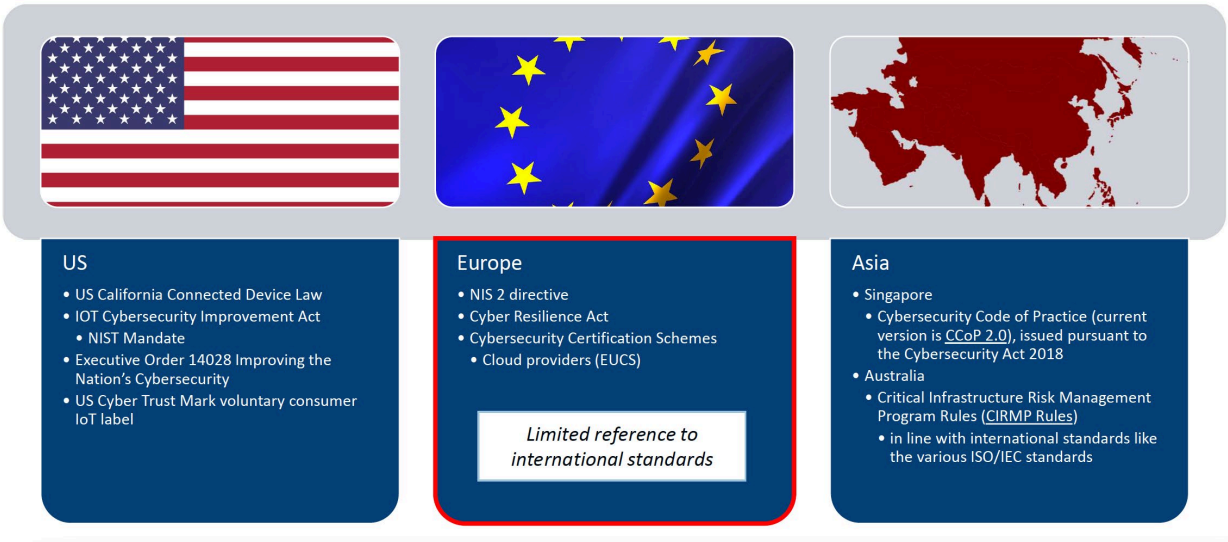


圖 7、美國、歐洲和亞洲的標準訂定情況

參考來源：Schneider Electric

因此各國之間的溝通與討論才是更有效率的做法，各國應致力於共同訂定國際標準，同時使國際標準也能支持各國各自的規範。講者也提到了一些關鍵點，幫助各國如何有效地實施國際標準：

1. 確保產業全球競爭力和創新至關重要。
2. 避免公告機構的瓶頸所造成進入區域市場的延誤。
3. 協調網路安全要求並達成互相認可的協議。
4. 避免讓中小型企業落後（這將會導致失去創新的企業）。
5. 降低合規成本，進而降低產品成本。

而制定國際標準也有一些要點，可以避免花重複的力氣、降低制定標準所需成本，例如重複使用現有的成熟國際標準、重複使用合格評估、認證和證據，並由歐洲電子技術標準委員會（CEN-CENELEC）在國際標準的基礎上製定協調標準的角色。講者分別舉例了標準之間互相參考、沿用的例子，如下兩張圖，分別是物聯網標準相互關聯示意圖和 PSWG 情境下各階段適用之標準：

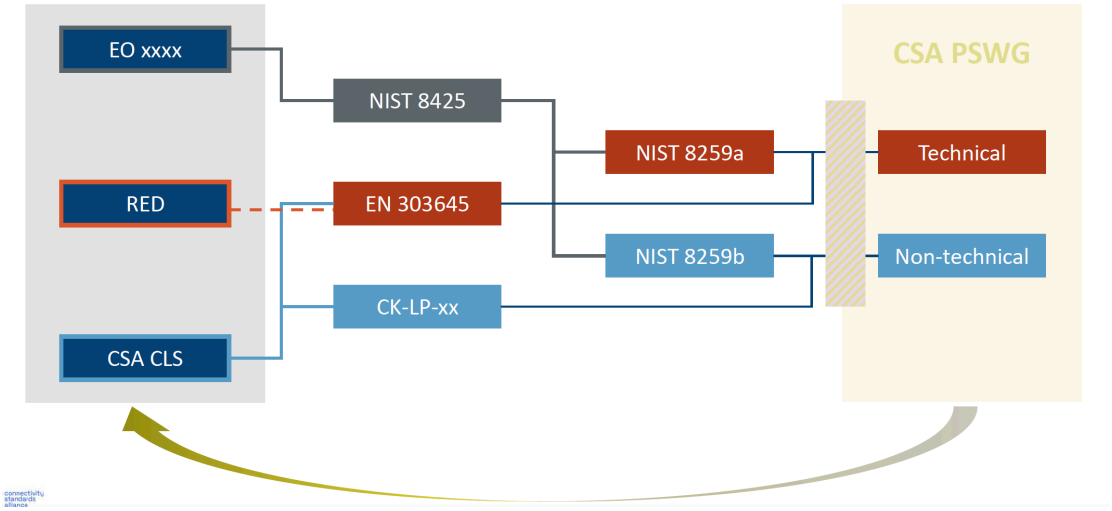


圖 8、物聯網標準相互關聯示意圖

參考來源：Schneider Electric

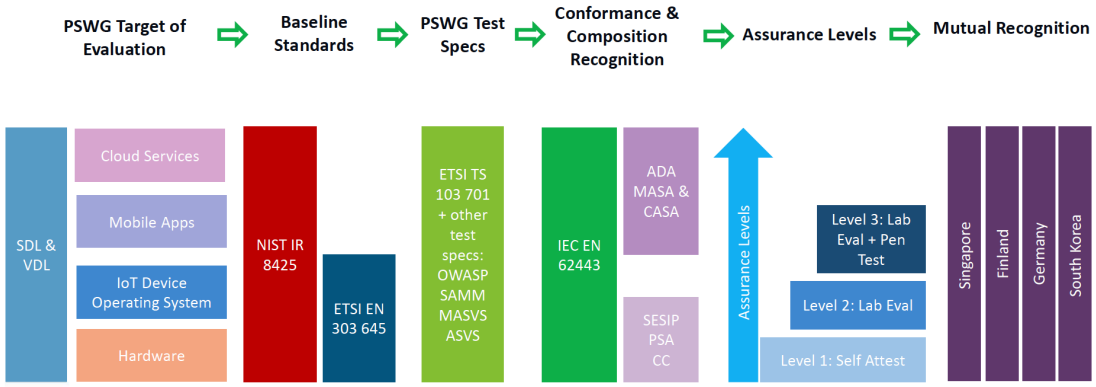


圖 9、PSWG 情境下各階段適用之標準

參考來源：Schneider Electric

(三)　從技術面探討規範、資料保護和隱私 Regulation, Data Protection and Privacy, Technical Aspects

這個階段將由技術面介紹規範、資料保護與隱私，首先由義大利那布勒斯帕特諾普大學的講者來分享如何在不犧牲資料可用性的情況下確保資料隱私性。講者提到了一個叫做 ENCRYPT 的方法，它是一個具有擴展性且實用的隱私保護框架，可以使使用者以符合 GDPR 的方式處理在聯合跨境資料空間的資料。在此框架內，將為公民和終端使用者開發一個推薦引擎，並根據數據的敏感性以及安全程度和整體系統性能，為他們提供有關隱私保護技術的個人化建議。這個專案主要有以下目標：

1. 提升隱私保護技術的適用性與效能，實現符合 GDPR 要求的敏感資料跨境聯合處理，開發整合服務平台。
2. 提高隱私保護技術的使用者友善性，促進所有相關參與者識別、理解、選擇和採用。
3. 促進並從本質上支援不同組織和不同部門之間類似資料類型的隱私保護處理的互通性。
4. 促進符合 GDPR 的歐洲通用資料空間並促進網路威脅情報資訊的交流，並與相關倡議和專案進行聯絡。
5. 為了確保開發的解決方案的適用性，透過與最終用戶共同設計它們，並驗證最小的現實用例，包括帶有個人資料的聯合資料基礎設施。
6. 透過傳播和利用開源專案成果，加強隱私保護解決方案的開源開發者和研究人員的生態系統。

二、 第二天

(一)零信任、供應鏈和開源 Zero Trust, Supply Chain & Open Source

一開始講者先提到加密流量整合(Encrypted Traffic Integration, ETI)所面臨的問題，如下列所示：

- 使用加密已成為增強通訊安全性的預設方法
- 加密會使使用者面臨惡意流量的威脅：
    - 由於隱藏在加密後面而無法辨識的流量，網路業者無法再過濾掉以保護最終用戶。
    - 端對端加密可能會限制網路管理、反詐騙、網路安全和監管監控系統管理流入、流經和流出網路的資料和通訊的能力。
    - 加密流量無法被授權檢查
    - 加密本身並不能保護端點免於攻擊

ETI 的角色是實現對影像等資料的合理授權訪問，而無需由 ETSI 對內容進行價值判斷，確保網路營運商不會參與傳輸非法內容。確保網路營運商能夠合理存取每個協定層標頭，以優化網路功能。

零信任架構的意思在於當尚未確定這個系統或是用戶是可信前，全部都先假設期不可信任，因此在這個架構底下，證明自己可信任才能使得系統透明和可擴展。

(二)物聯網和認證 IoT & Certification

這個主題探討物聯網和認證，並介紹了 ETSI EN 303 645 物聯網產品安全/隱私保護標準，這個標準是由 ETSI 在 2019 年所發布，其宗旨為確保物聯網裝置安全，並保護消費者的隱私。

講者首先提到 ETSI EN 303 645 和 ETSI TS 103 645 的發展趨勢(如圖 10)，從開始發展以來，仍不斷和其他標準合作或是引用其他標準做滾動修正，以達到在歐洲和更廣泛的全球市場建立共同基準線的目標，並將所有消費者物聯網設備的安全門檻從接近零提高到較良好的水平，包含通用制定的安全性和資料保護要求，以創建必要的靈活性，並涵蓋所有消費者物聯網領域。

圖 10、ETSI EN 303 645 和 ETSI TS 103 645 之發展趨勢

參考來源：ETSI

而 ETSI 也制定了規範物聯網各種裝置的標準，完整地確保整個物聯網環境安全，規範如下圖所示：

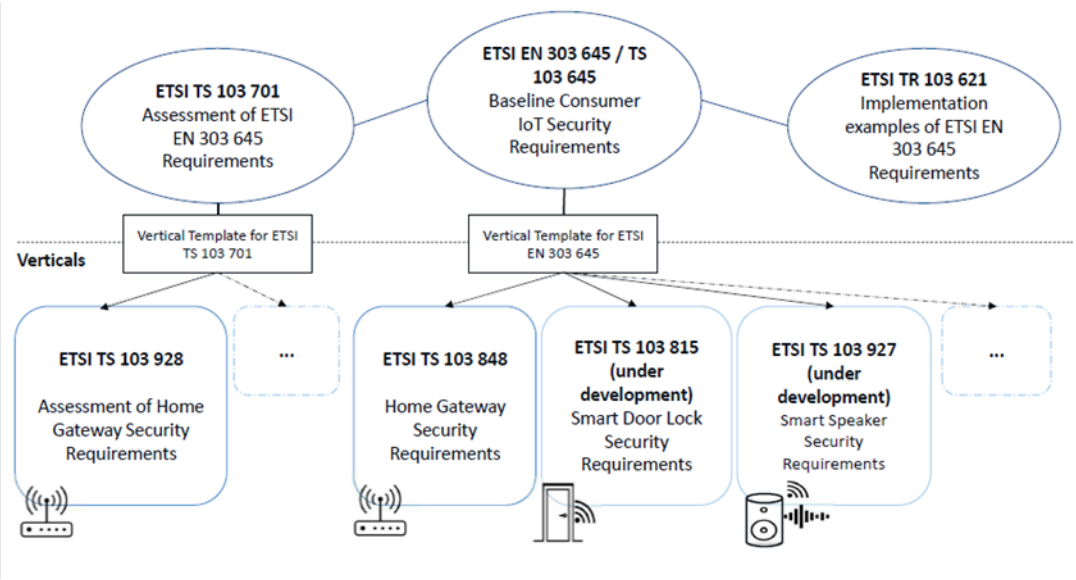


圖 11、ETSI 制定之物聯網相關標準

參考來源：ETSI

(三)　量子安全密碼學 Quantum Safe Cryptography Session

本階段主題為量子安全密碼學的安全標準制定，將會分別提到美國國家標準暨技術研究院(National Institute of Standards and Technology，簡寫為NIST)和 ETSI 為量子安全密碼學所指定的標準、達到量子安全的方法及安全量子通訊等議題。

首先，由 NIST 的代表介紹 NIST 制定密碼學和後量子密碼學 (Post-quantum cryptography，縮寫 PQC)相關標準(如圖 12)。NIST 從 2016 年便開始著手擬訂制定標準、蒐集要求，並發起密碼學競賽，希望能選出可以抵抗量子電腦威脅的演算法，並將演算法納入標準中。於 2017-2022 這六年間，陸續舉辦了多次研討會邀請各方專家討論，並進行了 3 輪競賽，而到了 2022 年，NIST 公布了獲選的 4 種加密法及 3 種候選的密鑰封裝演算法。目前已在 2023 年公告了標準草案，蒐集大眾的意見，並預計在 2024 發布第一版 PQC 標準。

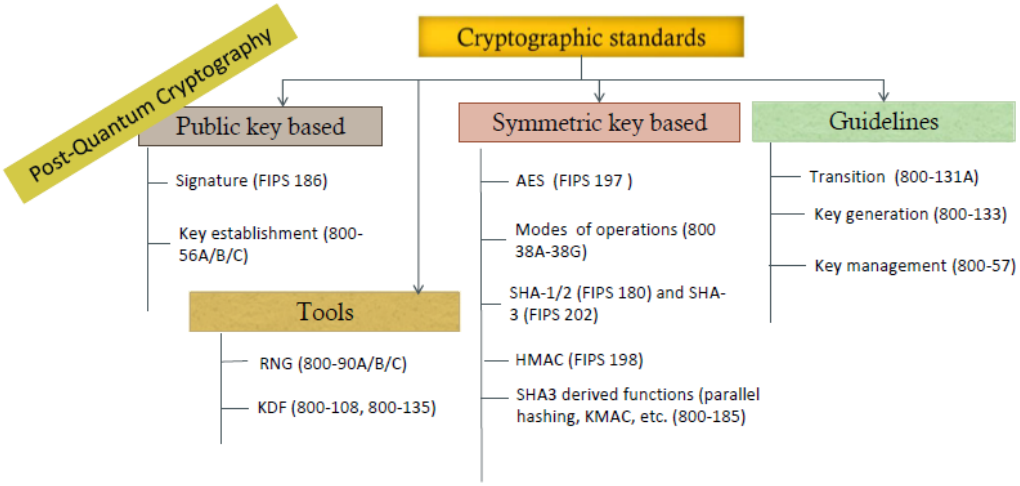


圖 12、NIST 所制定之密碼學和後量子密碼學標準

參考來源：NIST

截至 2022 年 NIST 公布入選的四種演算法如下：

1. CRYSTALS-KYBER
   - 基於網格密碼學(Lattice-based)的密鑰封裝機制(Key Encapsulation Mechanism, KEM)
   - FIPS 203 草案「基於網格的密鑰封裝機制標準」(“Module-Lattice-based Key-Encapsulation Mechanism Standard”, ML-KEM) 中被指定
2. CRYSTALS-DILITHIUM
   - 基於網格密碼學的數位簽章演算法
   - FIPS 204 草案「基於網格的智慧簽章標準」(“Module-Lattice-Based Digital Signature Standard”, ML-DSA) 中被指定
3. SPHINCS+
   - 基於無狀態雜湊 (Stateless hash-based)的簽章演算法
   - FIPS 205 草案「基於無狀態雜湊的簽章標準」(“Stateless Hash-Based Digital Signature Standard”, SLH-DSA) 中被指定
4. FALCON
   - 基於網格密碼學的數位簽章演算法
   - 將會在 FIPS 206 草案中被指定

而第四輪比賽的候選者演算法如下：

1. Classic McEliece
   - NIST 對其安全性充滿信心
   - 最小的密文，但最大的公鑰
   - NIST 希望獲得有關 Classic McEliece 特定案例的回饋
2. BIKE
   - 在第四輪候選人中擁有最具競爭力的表現
   - NIST 鼓勵大家對 IND-CCA 安全性進行審查
3. HQC

- 提供強大的安全保證和成熟的解密失敗率分析
- 比 BIKE 更大的公鑰和密文大小

從入選的密碼學名單中，可以看出許多演算法是基於網格密碼學，因此 NIST 目前也在積極的徵求不是基於網格密碼學的演算法，以為標準添加更多元的演算法，防止採用單一密碼學，若在未來出現新的攻擊面，會全面無法使用。此外，NIST 也在找尋其他具有短簽章和可以快速驗證的簽章演算法。

接下來由 ETSI 介紹目前已制定的與量子密碼相關的技術規範(Technical Specification, TS)、技術報告(Technical Report, TR)，以及正在進行中的工作項目，如下列所示：

1. 已完成的項目有：
   - QSC Migration; ITS and C-ITS migration study, ETSI TR 103 949 (2023-05)
   - State Management for Stateful Authentication Mechanisms, ETSI TR 103 692 (2021-11)
   - Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)
   - Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)
   - Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)
   - Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)
2. 目前進行中(鼓勵 ETSI 會員一起參與修訂工作)：
   - Quantum-Safe Hybrid Key Exchanges, RTS/CYBER-QSC-0019 (TS 103 744)

- Impact of Quantum Computing on Cryptographic Security Proofs, DTR/ CYBERQSC-0020
- Deployment Considerations for Hybrid Schemes, DTR/CYBER-QSC-0021
- Impact of Quantum Computing on Symmetric Cryptography, DTR/CYBER-QSC-0022

再來由 Toshiba 的講者講解量子密鑰分發(Quantum Key Distribution, 縮寫 QKD)以及 ETSI，量子密鑰分發為一種安全通訊方法，其有一個獨特的特點是，只要有第三方試圖竊聽密碼，那麼原本通訊的雙方便會發現，這種通訊方法是利用量子力學的基本原理，透過量子疊加態來傳輸資訊。講者列舉了三種 QKD 的協定如圖 13，分別講述了不同情境的密鑰傳輸方式。

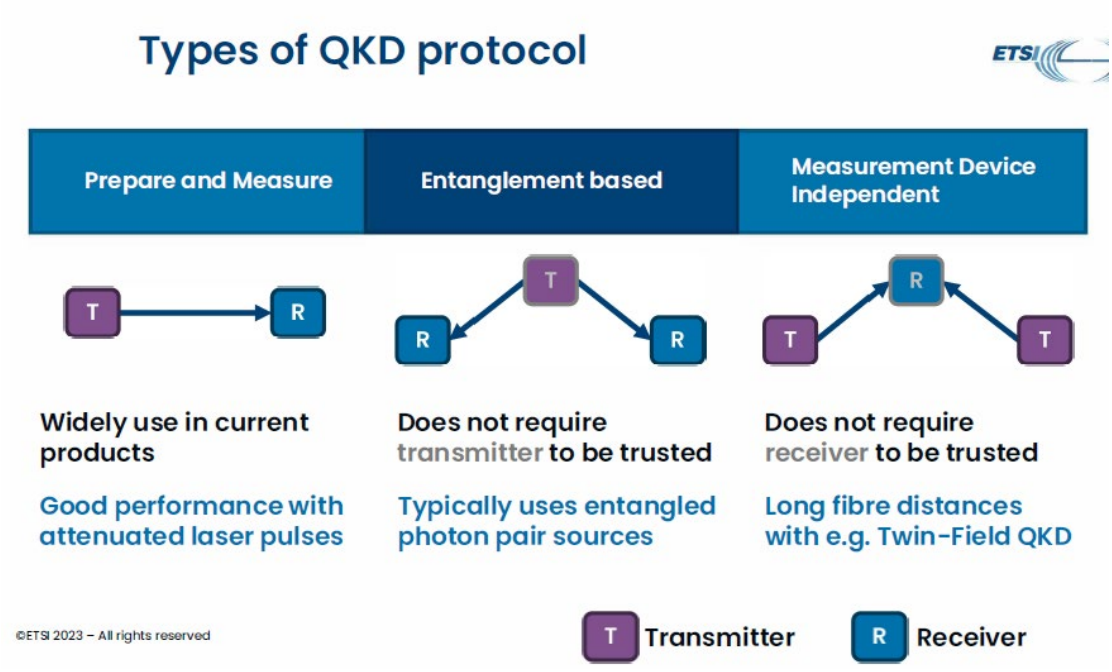


圖 13、三種量子密鑰分發協定

參考來源：TOSHIBA

三、 第三天

(一) 多元化之路：英國的 CyberFirst 專案如何塑造下一代網路安全專業人員 (The path to diversity: How the UK’s CyberFirst project is shaping the next generation of cyber security professionals)

本議題是由來自 NCSC(National Cyber Security Centre)為第三天帶來首場開幕演講。

本篇主要探討的內容為多元化及包容性對公司帶來的影響，講者認為企業不能對每件事情只採取單一文化的看法及解決措施，若公司能夠強化多元化及包容性，便能創造出適應性更強及更有效率的團隊，多元化將被視為競爭優勢。

為了增進多元化及包容性，NCSC 提出了一項名為 CyberFirst 的計畫，旨在招募並培育各種有才華的年輕人，引領他們進入網路安全的職業領域。CyberFirst 活動的目的是激發並鼓勵來自各個背景的學生考慮從事網路安全職業，並提供 CyberFirst 獎學金。

該計畫內容於 2015 年由英國政府通訊總部贊助並推出，主要計畫內容為針對 14 至 18 歲的學生實施網路相關知識教學，並提供助學金。

最後講者認為職場的正向文化是非常重要的，也提到了下幾個點作為結尾

1. 改善外部招募的作法吸引多元化的人才。
2. 用實際行動消除組織內部少數民族及性別上的薪資差距。
3. 透過培訓及強化資訊來支持內部員工，並打造一個完全包容的環境。
4. 希望透過 CyberFirst 的計畫，能夠吸引每年參與的女性人數。
5. 與弱勢社區機構的學生合作，共同創建一個完整的網路安全社區。

(二)　吸引下個世代的工程師與投資未來 Experiences of Attracting Next Generation of Engineers and Investing in Future

接下來是由來自 ISC2 **以及 ETSI 的會員發展總監進行兩個主題的演講。**

第一部份探討議題認為全球對資訊和系統安全的專業人員的需求正不斷增長，根據統計目前正有約 550 萬名資安人員，但實際的資安人員需求為 950 萬名。根據研究統計全球有 67%的企業表示他們嚴重缺乏網路安全人員來預防及解決網路安全相關的問題，30%的企業表示他們有適量的網路安全人員來預防及解決網路安全相關的問題，但僅有 2%的企業表示他們有充足的網路安全人員來預防及解決網路安全相關的問題。

講者認為的解決方案為雇用在資安產業上的實習生及初階員工，初階員工及實習生在薪資上的支出較低且可以將日常任務分派給他們，從而解放高階員工不必在日常任務中花費太多時間，他們的想法也能為企業帶來創新思維及創造力。實習生及初階員工的分配工作內容如下圖所示：

圖 14、實習生及初階員工的分配工作內容

參考來源：ISC2

最後講者也提到在招募實習生及初階員工時所需注意的特質:

表 2、實習生及初階員工時所需注意的特質

非技術性技能	性格特徵
團隊合作能力	解決問題
獨立工作能力	想像力及創造力
管理專案的經驗	分析性思維
服務客戶的經驗	學習慾望
表達能力	批判性思維

強調透過在職培訓的方式,適當的給予壓力讓員工能夠學習到如何在高壓下解決問題的能力,並利用導師制的方式每天配發任務及進度報告,透過這些方式可以讓新進人員能夠快速地跟上腳步,並成為公司重要的資產。

第二部份 ETSI 將重點放在 ICT 的標準化教育計畫的推廣方面,此計畫於 2016 年發起,目前參與機構包括德國、法國、義大利、西班牙等歐洲國家, 此計畫的目的及目標在於增進學生在 ICT 標準化教育的知識、向來自各地各領域的人員提供教育訓練及分享資訊的細節。

(三)　物聯網及認證 IoT and Certification Session

本議題是由來自 ETSI 程序委員、RISE 研究機構、FSCOM 以及 BT 的物聯網系統解決架構小組進行演講。

第一部份提到強制性控制涉及一套控制技巧，也在其他拘禁情境中使用，如人質事件和人口販運，以覆蓋自主權和自我感覺，使一個人陷入困境。在親密關係中，強制性控制的背景下，對新型電信應用（如智慧型手機、平板電腦、社交媒體、可穿戴裝置、智慧型音箱、遠端系統、互聯網連接的汽車、互聯網連接的家電、智慧門鎖、）的濫用通常被稱為消費者物聯網（IoT）啟用的虐待。

針對強制性控制的危害，講者提出了幾項預防性的概念:

- 消費者智慧型產品中不應有通用預設密碼。
- 設備製造商應該建立和維護漏洞揭露政策。
- 設備製造商應該明確說明產品軟體安全更新的時間。
- 在設計過程中加入隱私和安全性。
- 公司在收集和分享位置數據之前應得到用戶的許可。

最後講者提到的創傷知情設計可被定義為認識和理解人們的創傷如何影響他們的經歷。知情的設計致力於發現和設計的過程中避免加劇這種創傷，並建立解決方案，可以透過設計後的聊天機器人模擬虐待的情境，可以向受虐者提供有效的資訊做參考。

第二部份專注於介紹物聯網軟體設備的認證方式，根據統計超過 99%的漏洞是軟體產生的，因此訂定了一個高水準的物聯網網路認證機構，首先設備供應商須將設備的安全狀態傳給符合性評估機構(CAB)，通過後頒發證書，在物聯網軟體認證需求中有五個必要的條件，數位保證必須是基於加密的，而非口頭或手動保證，過程必須要自動化且不應太複雜，認證應能夠與未來更新後的軟體並用，證書的有效性及可靠性應易被驗證，認證過程本身應是安全的。

以下為物聯網設備遠端認證架構圖:

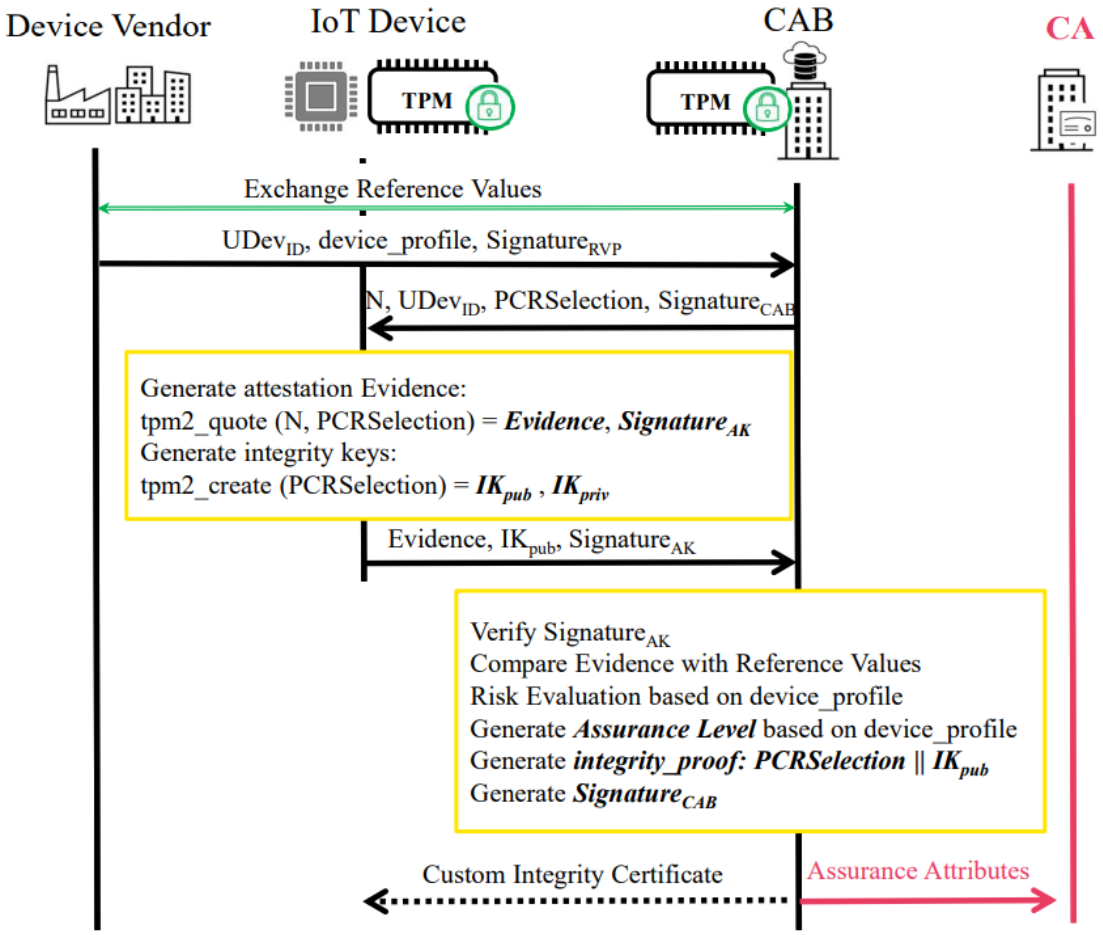


圖 15、物聯網設備遠端認證架構

參考來源: RISE

AutoCert 的遠端認證基於 RATS(遠端認證程序)架構。在設備被認證之前，物聯網設備擁有者負責產生與設備軟體相對應的參考值並將其安全地傳送給驗證方。在遠端認證開始之前，物聯網擁有者向 CAB 發送帶有 UDevID 和物聯網設備的 device_profile 的簽名請求。CAB 發送了一個帶有隨機 nonce N 和 PCRSelection 的簽名認證請求給物聯網設備。TPM2_Quote 功能用於產生憑證。具有密碼學強度隨機產生的 nonce N 辨別憑證並確定其是否為新的，並防止重送攻擊。而後建議物聯網設備產生一個完整性金鑰對 IK，並將其與憑證一起發送以創建一個完整性證明。IK 是一個 RSA 金鑰，使用 PCRSelection 和 TPM2_Create 功能產生的 IKpriv 和 IKpub。由於設備上的安全關鍵性軟體的任何更改都會使

用 TPM2_PCR_Extend 進行記錄，因此在創建 IK 時使用此 PCRSelection 確保如果設備的軟體狀態發生更改，則該金鑰將無效。有效的 TPM(信賴平台模組)產生的認證金鑰 AK 用於簽署 TPM 產生的憑證。它用於第三方驗證特定物聯網設備上的 TPM 產生的金鑰和數據的方式。在收到憑證後，CAB 驗證隨附的簽名並將憑證與參考值進行比較。根據認證結果並使用適當的風險評估機制，對認證方的保證等級根據 device_profile 進行計算。認證的結果和保證級別由 CAB 用於確保軟體狀態的完整性。

第三部份重點介紹成立於 2016 年的 AIOTI(物聯網創新聯盟)，旨在促進和支持在物聯網、邊緣運算和其他融合技術領域的合作。AIOTI 成員在數位價值鏈上推動業務、政策、標準化、研究和創新發展，以支持歐洲的數位化和競爭力。

講者將這次主題放在星閃(NearLink)技術的安全上，星閃技術是由華為研發的近距離連接技術，星閃的架構主要分為三層，實體層為核心層，負責高頻訊號的傳輸及接收、資料連接層負責資料的打包及解包、網路層負責資料路由的轉發；主要技術模式分為低功耗接入技術(SLE)及基礎接入技術(SLB)，低功耗接入技術主打低功耗、低延遲、高可靠性，資料傳輸率為 12Mbps 可應用於無線耳機、滑鼠等技術，基礎接入技術模式專注於高速率、高容量、高精確度，資料傳輸可達 1.2Gbps 可應用於視訊的傳輸、大型檔案分享等技術。

下圖為三者之間在各層的安全機制比較，可以看出星閃技術在強制雙向認證方面、安全儲存方面皆比其他兩項成熟，但講者也提到目前星閃技術在功能上或許遠超藍芽及 WIFI，但目前還位於開發階段尚未成熟，且在成本考量上遠高於 WIFI 及藍芽，因此該如何推廣此技術將會是 NearLink 目前所面臨最大的挑戰之一。

		NearLink	Bluetooth 5.3	Wi-Fi (WPA3)
Application-layer security	Configuration	√	Undefined	Undefined
	Mechanism	√	Undefined	Undefined
	Requirements	√	Undefined	Undefined
Transport-layer security	Blocklist & trustlist protection	√	√	Undefined
	Mandatory two-way authentication	√	Customizable (No authn. for Just work mode)	Customizable (No authn. for Open mode)
	Strong credentials	√	Password complexity undefined	Password complexity undefined
	GM cryptography	√ (ZUC, SM2, SM3)	×	×
	Independent on/off between encryption & complete insurance	√	× (Simultaneous on/off)	× (Simultaneous on/off)
	No. signaling messages	Context present: 5 Context absent: 2	Context present: 10+ Context absent: 4	Context present: 8+ Context absent: 8+
Device security	Secure storage	√	Undefined	Undefined
	Domain-based security isolation	√	Undefined	Undefined

圖 16、各層的安全機制

參考來源：FSCOM

第四部份是針對 oneM2M 做主要介紹，oneM2M 是個全世界互聯網通用的規格編程由 8 個世界領先的 ICT 標準制定組織組成，主要是：ARIB，ATIS，CCSA，ETSI，TIA，TSDSI，TTA 和 TTC。涵蓋領域包括建築、API 編譯、保全、電子科技、電子裝置等等；

針對 oneM2M 的安全性，主要支援的領域為身分認證、建立安全小組、授權、遠端配置，附加的領域為身分保護、敏感性資料處裡、設備安全管理，下圖為 oneM2M 的安全框架，可以看到 oneM2M 提供了一組通用的安全功能，保護物聯網設備及應用程式減少及防止攻擊。

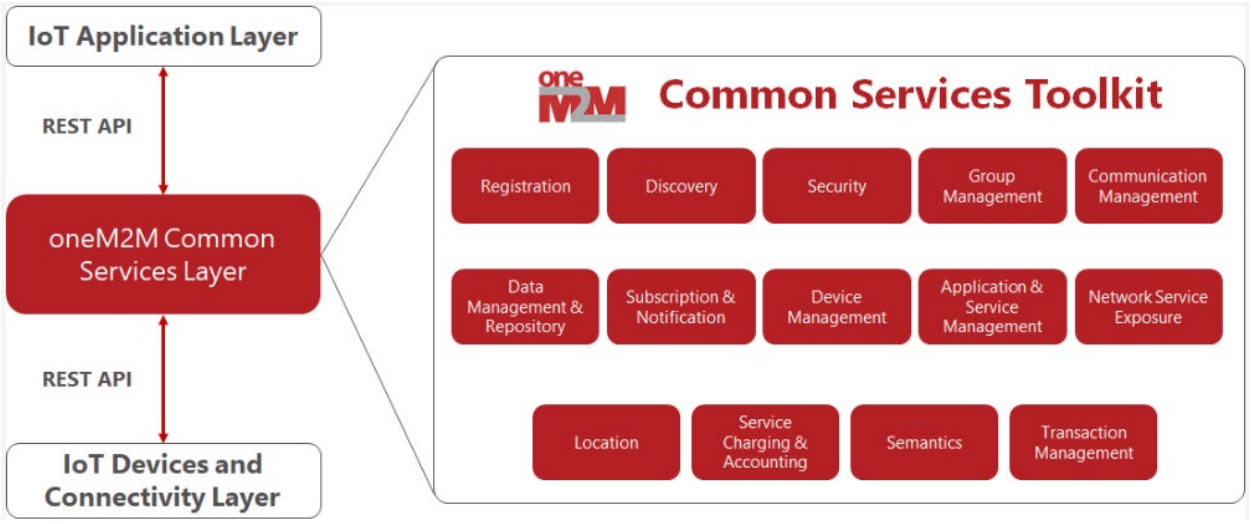


圖 17、oneM2M 的安全框架

參考來源: oneM2M

(四)　物聯網和行動認證 IoT & Mobile Certification

本議題是由來自義大利電信研發部、Google Android Security and Privacy 團隊、Google Android Security and Privacy 策略小組進行演講。

第一部份提到消費者行動裝置保護輪廓(TS 103 732 v1.1.1)於 2021 年 11 月發布,其定義智慧型手機和平板電腦的安全和保障、降低潛在風險並保護用戶,其中包含了使用者身分驗證、TOE(評估目標)軟體安全更新、以不同的安全等級保護使用者資料、應用程式的權限管理、生物特徵安全認證等。

ETSI 如何對 Protection Profile 進行認證？

1. 使用專家任務組機制來資助評估和認證活動。
2. 在 STF 646 工作方針的開發和批准之後，ETSI 針對專業知識機構進行評估，並選擇了 ANSSI 作為認證機構，Thales ITSEF 作為評估實驗室。
3. Thales ITSEF 在 2023 年 6 月完成了評估，結果為通過。
4. 評估報告已於 2023 年 6 月交付給 ANSSI 和 ETSI。
5. 認證機構於 2023 年 8 月批准了 Thales ITSEF 的評估報告，並且認證現在正在進行，以完成認證流程。
6. ETSI TC CYBER 在 ETSI TC CYBER #35 會議期間批准了 CMDPP 交付成果的最終版本以及 STF 646 里程碑 A 和 B 文件。

消費者行動裝置保護輪廓是一個可單獨用於智慧型手機、平板電腦等行動裝置通用標準評估的工具，ANSSI 針對保護輪廓的認證支持/允許製造商對其移動設備提供的安全性進行一致且具有最新技術基準的認證/評估，該計畫目前由 GSMA 的 FASG 裝置安全小組開發中。

最後講者提到 TS 103 732 系列將來的發展，TS 103 732 系列的持續演進 - 與多用戶相關的模組（TS 103 732-3）和預安裝應用程序（TS 103 732-4）的安全要求正在 ETSI TC CYBER 中進行開發，但未來可能會新增其他模組。TC CYBER 可能會處理來自 GSMA MDCert 開發的額外安全要求。

第二部份提到安全性、隱私和數據保護已成為消費者購買新智慧型手機時最關心的議題之一。消費者無法了解大多數設備安全更新的時間有多長，生物辨識技術有多強大，以及其他非常基本的安全功能。這導致了資訊缺乏，因為大多數消費者是從價格和功能比較網站上了解各種智慧型手機的功能。

根據目前的市場分析，現有的智慧型手機安全標準只有三組，分別為 BSI、CC/NIAP、ETSI TS 103 732，且目前沒有行業運行消費者智慧型手機安全認證計畫。

GSMA MDSCert 主要的工作內容

- 分析了現有的 GSMA 認證計劃，如 ESA 和 NESAS，以查看我們是否能夠輕鬆利用它們現有的治理、流程和程序
- 調查了市場/監管對於不同保證水平的需求，並提出了一些建議，以提供足夠的靈活性並直接對應到現有和未來的法規（即歐盟 CSA）
- 定義了使用這一認證計劃的人物角色，如消費者、政策制定者、科技媒體、一般媒體和其他利益相關者
- 進行差距分析，並通過與 ETSI TC Cyber 的協議，提供了大量關於 TS 103 732 的回饋，形成了保護配置文件的 2.x 版本
- 進行了一項針對消費者的研究，涵蓋了 11 個市場，有超過 22,000 名參與者。

最後講者提到該如何將認證的資訊傳遞給大家，當中包含宣傳標章的外觀及標籤的內容分析，在產品包裝的側面可能會印有二維條碼及標誌，消費者可以透過掃描後，獲取相關標籤認證的資訊。

第三部份提到隨著時代的進步，物聯網產品設備在全世界已達數十億台，也意味著物聯網網路安全的議題正被大家關注著，目前約有 20 幾個監管機構正在制定相關的物聯網網路安全法規，但他們制定的法規並不同步，且容易發生衝突，從下圖可以看出各國所遵照的標準並不同步，為此 CSA 正成立安全工作小組

(PSWG)解決此一問題。

Region	IoT Device Security Spec	Mandatory/ voluntary	Certification	Labeling	Key Standard Referenced
Asia					
Australia	Under development	Voluntary	Yes	Yes	ETSI EN 303 645
China	Yes	Mandatory	No	No	None
India	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Japan	Yes	Voluntary	No	No	NIST, ETSI EN 303 645
Singapore	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
South Korea	Yes	Voluntary	Yes	Yes	ITU X.1352
Thailand	Under development	Voluntary	No	No	None
Vietnam	Yes	Voluntary	No	No	ETSI EN 303 645
Europe					
France	Yes	Voluntary	No	No	ETSI EN 303 645
Germany	Yes	Voluntary	Yes	Yes	ETSI EN 303 645
Spain	No	Voluntary	No	No	None
UK	Yes	Mandatory	Yes	Yes	ETSI EN 303 645
Americas					
Brazil	Yes	Mandatory	Yes	Yes	ETSI EN 303 645, ISO/IEC 27402
US	Yes	Voluntary	Yes	Yes	NIST IR 8425

圖 18、各國所遵照的標準

參考來源: Google Android Security and Privacy

安全工作小組(PSWG)的目的為確保物聯網產品的安全及隱私、可以定義多個安全等級、授予監管機構和消費者認可的標章、開放式且廣泛參與。

最後講者提到此計畫目前會先關注在美國 NISTIR 8425、歐洲 ETSI EN 303 645 及 ISO 27402，並努力彙整這些標準。此計畫將於 2024 年 1 月啟動。

(五)　5G in the Wild - Part 1

本議題是由來自 ETSI 小組、Deloitte Tohmatsu Cyber 團隊進行演講。

本次會議主題環繞在 3GPP 的技術規則小組(TSGs)，該小組的工作內容為負責技術標準及規範的制定，下圖為各技術小組的工作內容。

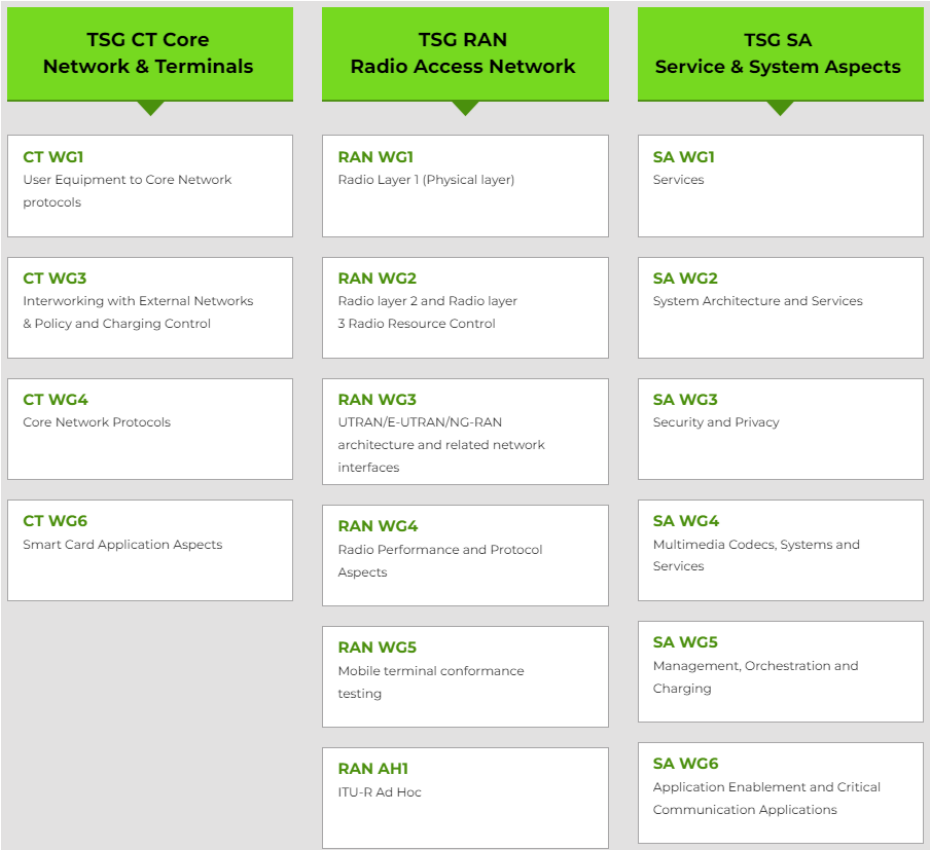


圖 19、技術小組的工作內容

參考來源:ETSI

- TSG RAN:AI/ML 空中介面、MIMO、Duplex、環境物聯網、NTN、SON/MDT、XR 等技術進行研究。
- TSG SA:衛星存取、能源效率、延展實境及元宇宙等技術研究。

3GPP 目前在 5G 計畫中發布了五項計畫分別為 Releases15 ~19，其內容為:

Release15:發布新的無線接入技術:5G NR

Release16:為消費者帶來更高的資料處理速度及可靠度

Release17:注重於毫米波(mmWave)擴展、5G 終端支援 RedCap 新技術(NR-Light)、終端增強、非地面網路(NTN)、網路拓撲擴展。

Release18:著重於移動寬頻、設備、網路的演進，將於 2024 年完成。

Release19:預計 2024 年開始進行。

最後講者總結 3GPP 的研究流程領域複雜，Release19 的內容目前還在討論中，未來將考慮加入新的部門進行研究， Release18 及 Release19 將在未來幫助 6G 技術的發展奠定重要的基礎。

第二部份講者提到 5G 手機網路利用眾多網路技術,被設計成能在雲端運作,並具有更大的對外開放性。因此，為了確保 5G 手機網路的成功和成本效益，採用資訊科技安全技術是至關重要的，5G 技術是一項重大技術的轉變，這也為電信商帶來新的風險。儘管將 5G 視為另一個世代可能很容易，但其高度整合、技術多樣性，帶來了在攻擊的情境下如何管理的一大挑戰。

通用零件的增加使得網路安全小組需要重新思考網路安全的運作模式,例如身分和存取管理、加密、憑證可信任 CA、作業系統、資料庫等，因此講者提出一項統一的框架做整合。

講者最後提到目前正利用現有的框架建構一個統一的控制框架，將 NIST 及 ISO 的框架維持不變，並加入 3GPP、GSMA、CSI、ENISA 的資料，並將重複的資料刪除，並說明使用單一控制框架帶來的好處為每個資產受到相同的控制，以便消除潛在弱點。

四、 第四天

(一) 5G in the Wild - Part 2

為最後一天上午帶來演講的是來自 ETSI ISG NFV 安全工作小組、TCA eUICC 小組。

首先 NFV 小組針對 NFV 功能進行介紹，網路功能虛擬化(NFV)的概念是將傳統或特殊化的硬體(路由器、交換器、防火牆等功能)利用此技術進行虛擬化，並整合於共用的伺服器，藉此網路的設備將被取代並大幅減少設備成本。

NFV 的架構包含了三點，第一為虛擬網路功能（VNF）用以提供網路功能的應用，第二為網路功能虛擬化基礎架構（NFVi），其包含了平台上的基礎架構元件（運算、儲存、連網），從而支援運行網路應用所需的軟體或容器管理平台，第三點則是管理、自動化和網路編排（MANO），用於管理 NFV 基礎架構。

講者提到 ETSI 目前正在研究的 ETSI NFV 第五版中，主要專注在整合及生態系統的部分，並擴展目前的介面及建模和新的功能。

針對 NFV 安全相關的作業，目前 ETSI 正進行的部分為:

- NFV-SEC 020:身分管理及安全規範
- NFV-SEC 022: API 存取的存取令牌(Token)規範
- NFV-SEC 023:容器安全規範
- NFV-SEC 024:安全管理規範
- NFV-SEC 025:端到端 NFV 及 NS(信號網路)管理安全規範
- NFV-SEC 026:隔離及信任域的相關規範

第二部份主要將焦點轉移至ETSI SET規劃的兩個平台UICC及SSP，UICC(通用積體電路卡)的主要功能包括存儲用戶的身份資訊、管理訪問移動網路的權限，以及支援不同的應用程式，如付款、身份證明等。它是移動設備與無線網路之間的一個重要接口，有助於確保設備的安全性和身份辨識，SSP(智慧安全平台)

於 2015 年由 ETSI SET 提出，用於託管安全的應用程序，但目前還在規劃當中。

講者提出 UICC 正考慮使用 MIPI 標準如下圖，I3C BUS 支援多種裝置之間的通訊，同時具有互換性和能夠向後兼容 I2C（Inter-Integrated Circuit）協定。它被設計為一種高效能、低功耗、低成本的解決方案，特別適用於移動設備、物聯網（IoT）裝置和其他嵌入式系統。I3C BUS 提供了更高的傳輸速率、更低的功耗以及更靈活的裝置管理，使其成為一種先進的序列通訊標準。

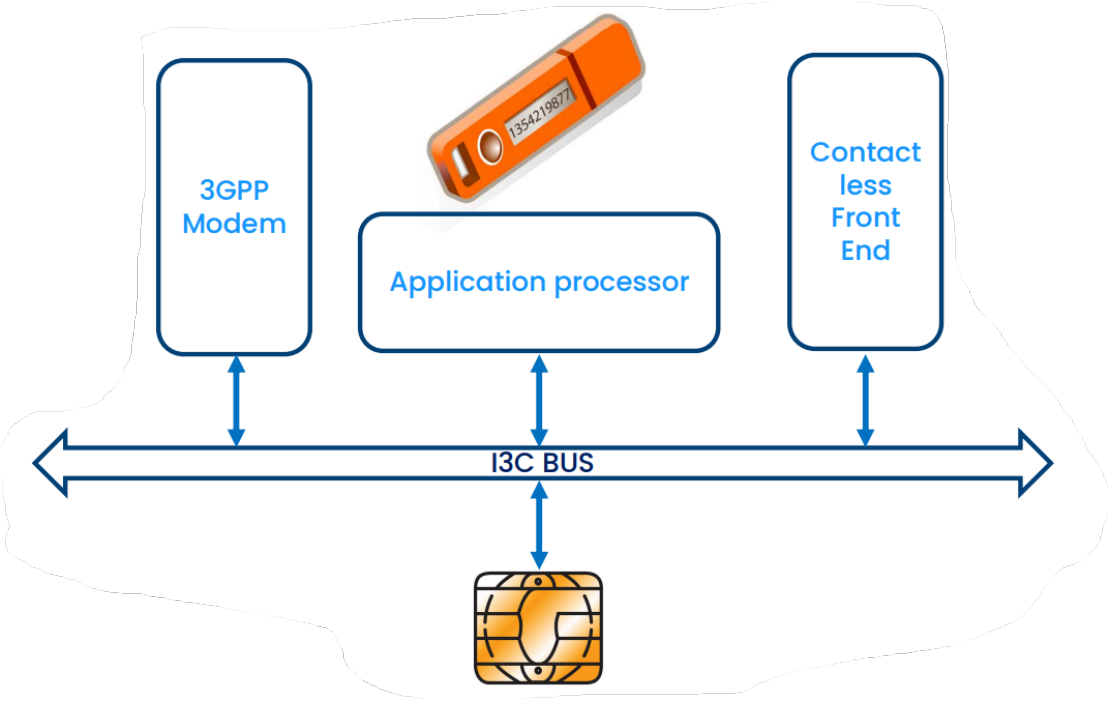


圖 20、MIPI 標準

參考來源: eUICC

(二)　6G 的未來（6G Futures）

本議題由來自 Samsung R&D Institute UK 團隊進行主題演講。

此部份主要將主題內容放在 6G 技術的介紹以及目前可能會遇到的安全要求，講者提到目前 6G 技術仍處於研發階段，但目標會放在三個階段，第一為確保有足夠的無線容量以實現更高的資料傳輸速度，並應用於虛擬實境、擴增實境、混合實境等技術，第二為使用更新更可靠的感測器、執行器、智慧組件為使用者帶來更好的使用環境體驗，最後一點為數位複製品技術，在虛擬世界中複製物理實體並與其互動，並無時間或空間的限制。

講者針對 6G 安全提出自己的看法並歸類於下圖中:

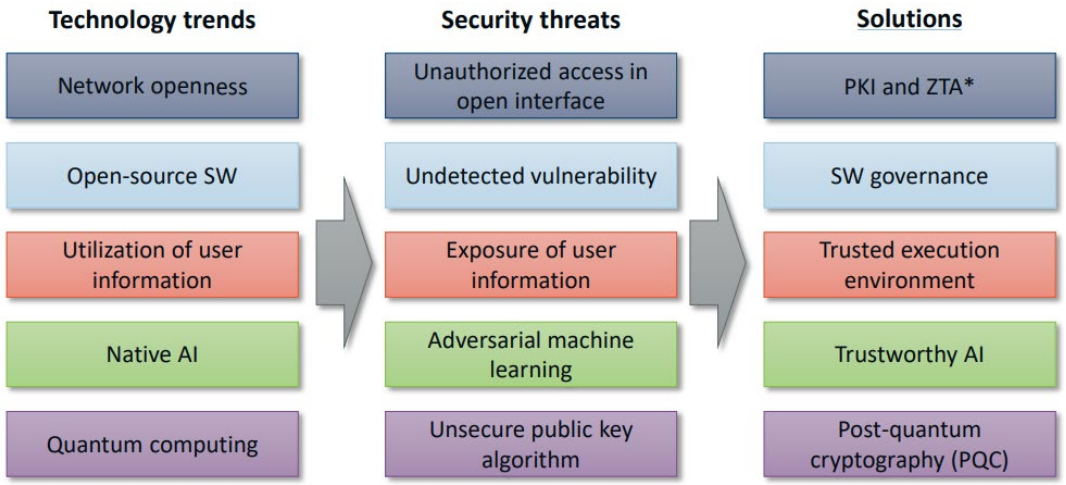


圖 21、6G 安全

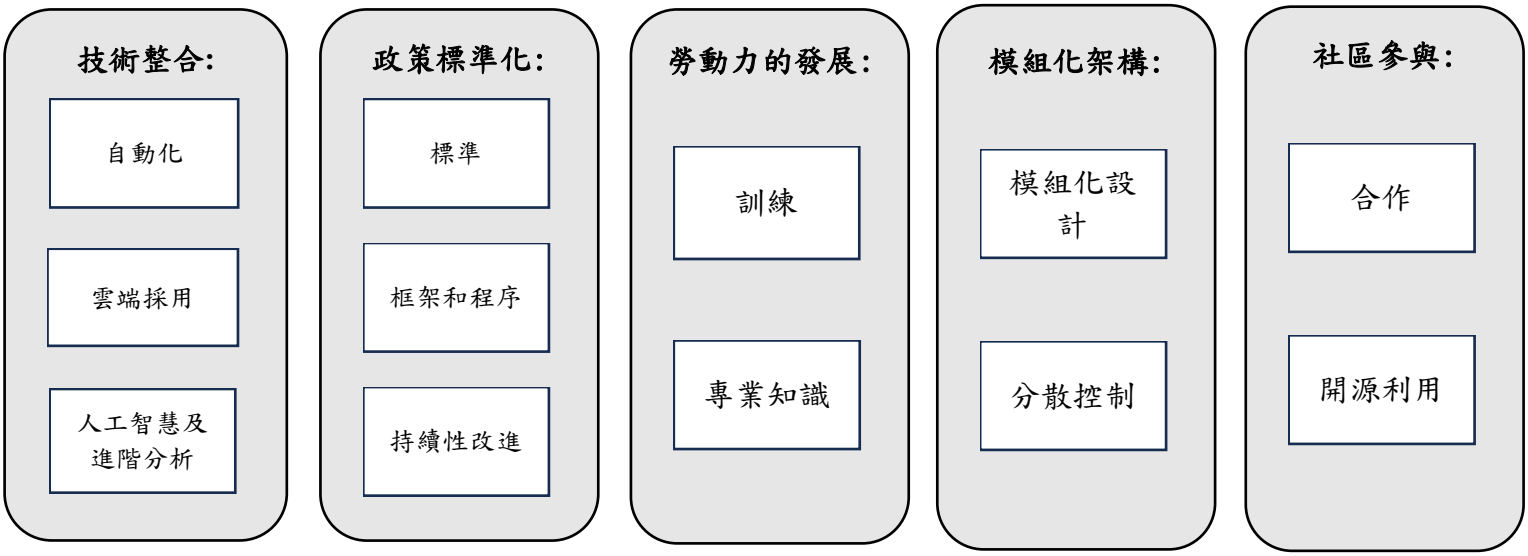
參考來源: Samsung

(三)　擴增實境與人工智慧 (Augmented Reality and AI)

本次會議最後一個主題演講是由 AI Shield 團隊、ETSI 程序委員會、trustilio 團隊、ENISA 團隊針對 AI 技術應用進行演講。

本講座首先探討的主題為 AI 是否為可增強的?講者認為直到我們創新與增進他，否則沒有辦法，儘管有可用性的技術及工具，完成 AI 應用架構仍然花了三十年的時間。

下表為 AI 應用架構:



從早期的 AI 1.0 到 AI 3.0 人工智慧的進步與風險同步增長，從最一開始的機器學習到現今的生成式人工智慧，在每一階段中都有發生嚴重的資安事件(如下表):

表 3、各階段中所發生之資安事件

機器學習	Twitter 使用微軟開發的聊天機器人 Tay 在不到一天的時間學習了多個種族歧視的詞彙，並自發性的在對話中產生。
深度學習	Tesla 在 2022 年感恩節期間因車主開啟全自動駕駛模式而引連環車禍。
生成式學習	三名南韓三星員工在無意間向 Chatgpt 洩漏公司機密，一名分享半導體資料中的原始碼、另一名分享機密代碼用來修復

	設備缺陷、最後一名提交了整份會議紀錄請求 Chatgpt 最彙整。

從 AI 2.0 到 AI 3.0 我們須注意的風險有哪些不同?很明顯在者兩者之間所需注意的資安意識是有很明顯的差異存在(如表 4)

表 4、AI 2.0 到 AI 3.0 風險比較

AI 2.0:OWASP 機器學習所帶來的十項資安風險	AI 3.0:OWASP 所歸納出前十項大型語言模型風險
ML01:2023 對抗式攻擊	LLM01:提示注入攻擊
ML02:2023 資料毒化攻擊	LLM02:不安全的輸出處裡
ML03:2023 模型逆向攻擊	LLM03:訓練資料毒化
ML04:2023 成員推理攻擊	LLM04:模型阻斷服務
ML05:2023 模型竊取	LLM05:供應鏈漏洞
ML06:2023 損壞封包攻擊	LLM06:敏感性資料揭露
ML07:2023 遷移學習攻擊	LLM07:不安全外掛程式設計
ML08:2023 模型扭轉攻擊	LLM08:過度代理
ML09:2023 輸出完整性攻擊	LLM09:過度信賴
ML10:2023 神經網路重編程	LLM10:模型竊取

利害關係人的心聲:

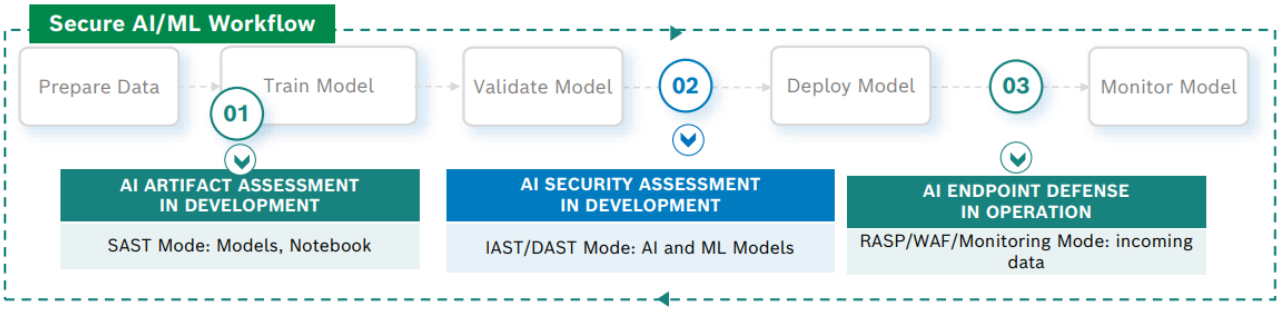
站在買方、高階主管、IT 管理者立場:我希望確保我的產品可靠、安全且值得信賴，以讓我的顧客感到安心。

站在使用者、人工智慧及機器學習開發商、安全經理人立場:我們只想專注在建立好的模型，不想擔心在其他安全相關問題。

根據顧能公司(Gartner)的調查，生成式 AI 已成為企業正面臨的新興風險，五家企業中有兩家違反 AI 隱私，四家企業中有一家面臨惡意攻擊，因此對於開

發者及使用者來說，在輸入資料時的穩健性是非常重要的一件事情，畢竟對攻擊者來說，攻擊手法的難度是非常低的，但攻擊者能夠獲取的利益卻是可觀的。

最後演講者提到自己對人工智慧及機器學習工作流程看法，並說明下個世代的人工智慧安全應具備的能力如下圖:



Legends	Capabilities	Application Security Context
01	SAST	Static Application Security Testing (e.g. code scan, artefacts scan, etc.)
02	IAST/DAST	Interactive/Dynamic Application Security Testing (e.g. application run time probing)
03	RASP/WAF/Monitoring	Real time application security protection / Web Application Firewall / Monitoring

圖 22、人工智慧安全應具備的能力

參考來源: AI Shield

第二部份講座的內容著重於 ETSI 人工智慧的運作內容及推動因素、ETSI 如何代表解決這些人工智慧的問題。

重要訊息:

1. 行業規範 ISG SAI 將於 2023 年關閉，並於 2023 年 12 月以 TC SAI 的角色重啟。
2. 2024 年 4 月 5-7 日 ETSI 將舉辦人工智慧標準化現況、實施、展望會議。

講者首先介紹到人工智慧系統在網路安全領域面臨多項挑戰，以下為幾項較為關鍵的挑戰。

1. 透明度和可解釋性不足：人工智慧系統運作如同一個“黑盒子”，難以理解它們如何做出決策。
2. 過度依賴人工智慧：過度依賴人工智慧系統可能會在這些系統遭到破壞時產生漏洞。

3．偏見和歧視：人工智慧系統可能會無意中延續其訓練數據存在的偏見，導致歧視性的結果。

4．易受攻擊：網路罪犯可以操縱人工智慧系統，可能破壞企業系統並造成重大損害的威脅。

5．缺乏人類監督：在缺乏適當的人類監督的情況下，人工智慧系統可能會做出產生意外後果的決策。

6．高成本：實施和維護人工智慧安全系統的成本高昂。

7．隱私擔憂：人工智慧系統通常需要大量數據，這可能引發隱私擔憂。

講者提到最重要的問題是政府階層的看法是保護公民的重要關鍵，將頒布法令針對提供惡意人工智慧程式的提供者及開發商造成的損害進行承擔責任的賠償。

目前的人工智慧是人造的，未來的人工智慧將會有所分歧，不再是人造的（機器通過從其失誤中“學習”，設計下一代機器，幾代後人類生成的基礎就會失去），要管理人工智慧，不僅需要管理人工智慧本身，人類社會如何與“不同”的智慧互動也必須加以管理，人工智慧和人類都需要考慮如何共同合作。

目前正由三個 ETSI 小組及一個監督小組來解決以下三點問題:

TC SAI:所有人工智慧的安全形式，著重於機器學習。

TC CYBER:將 SAI 的建議納入風險分析法(TS 102 165-1)與對策架構(TS 102 165-2)。

TC MTS:探討人工智慧和測試的作用。

OCG AI 協調整個 ETSI 的政策及其他事務。

最後講者總結人工智慧本身不是問題，它是一種希望利用新技術來擴展可以實現的範疇的願望的症狀，人工智慧可以被應用為 X 光掃描辨識癌症，也可能被有心人士用為破壞性的圖像如 Deepfake，因此工具的應用及意圖才是最重要的。

第三部份講者將主題放在人工智慧網路安全框架(FAICP)上，FAICP 是由

ENISA 於 2023 年 6 月發表，目的在於增強人工智慧的產品的彈性和安全性。

FAICP 的設計目標及原則:

目標：

建立一個針對確保資訊通訊技術基礎設施和託管的人工智慧所需的良好資訊安全實踐框架（FAICP），同時考慮人工智慧生命周期的所有階段（從系統概念到退役），以及人工智慧供應鏈的所有元素、相關行為者、流程和技術。

設計原則:

- 兼容性:以過去的經驗為基礎並在其之上建構。
- 全面性:考慮 ICT 基礎設施中的人工智慧系統，並包括在人工智慧系統及其個別元件周圍和內部所需的所有資訊之安全實踐。
- 多用途:適用於不同行業的人工智慧利益相關者。
- 國際性:包括歐洲和國際間的努力、標準和建議。

FAICP 所帶來的影響:

效益:

協助利益相關者辨別現有的標準和最佳實踐，以確保其人工智慧系統，並識別其安全需求，監控並強制執行這些需求的合規性。

受益人:

以下各方：開發者、整合者、供應商、供應鏈業務合作夥伴、人工智慧系統使用者、供應鏈、歐盟國家主管機關。

下圖為講者整理出的相關規範:

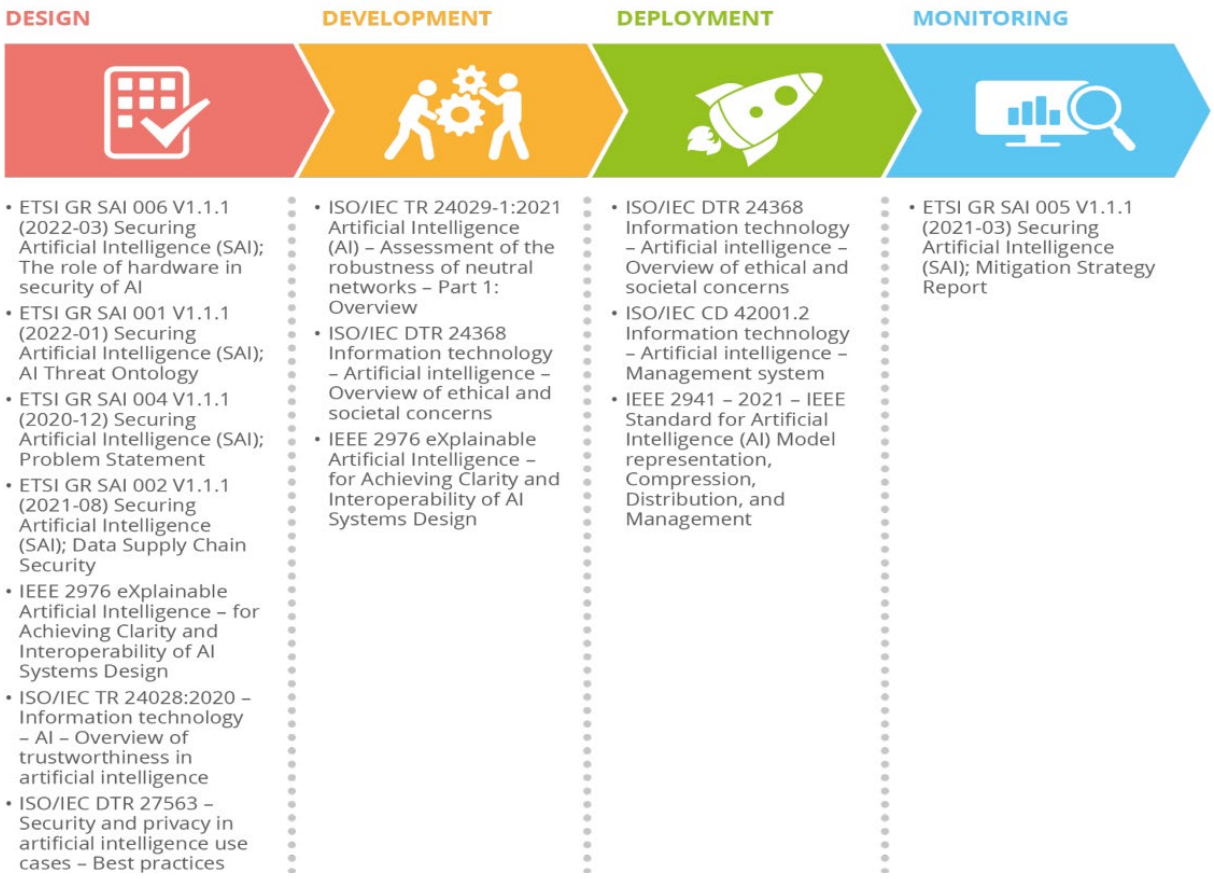


圖 23、相關規範

參考來源：trustilio

最後講者提到 FAICP 所面臨的挑戰:

- 資料的互通性
- 長期風險（由於人工智慧系統在部署後繼續學習，風險持續存在）
- 動態風險測量/指標（靜態測量不切實際）
- 全球人工智慧道德框架（被全球接受的道德標準）
- 跨學科、多視角的方法是必要的
- 從政策要求到設計原則

最後一部份演講針對 ENISA 進行介紹，最先探套的部份為 ENISA 主要的運作內容為:

1. 貢獻於歐盟資訊安全領域的戰略研究議程（《資訊安全法》第 11 條）。

2．為歐洲資訊安全能力中心（ECCC）提供建議，制定戰略議程和工作計畫

3．支持在歐盟成員國實施，並與主要利益相關者和研究界保持討論。

網路安全研究趨勢及未來展望

技術方面:

- 先進的計算（下一代微處理器、邊緣計算、高性能計算、量子計算）
- 通用計算（下一代物聯網、嵌入式計算系統）
- 人工智慧（大型語言模型）
- 下一代通訊技術
- 太空技術
- 虛擬實境

非技術性方面

- 數字主權及支持其的相關資訊安全條件
- 隱私和倫理
- 供應鏈安全，量子安全準備
- 假新聞和假訊息，網路犯罪，資訊安全和混合戰爭之間的模糊邊界（例如高級持續性威脅（APT）的重要性，與非民主國家的關係以及駭客的操縱，Pegasus間諜軟體，以及其他與戰爭有關的神秘事件...）
- 關鍵基礎設施在混合戰爭和攻擊背景下的關鍵角色
- 國際合作，例如全球資訊安全的協調。

人工智慧在網路保險領域具有重大變革，但存在著重大的障礙。

挑戰：

- 用於訓練人工智慧和機器學習模型的數據來源是保險公司需要克服的主要挑戰。數據的可用性和品質是重要因素。它們可能妨礙高級統計方法和機器學習/人工智慧在網路風險建模中的應用。
- 人工智慧模型中的偏見可能導致人工智慧系統的歧視行為
- 方法必須是可解釋的、公平/無偏的，以提供經過驗證的效益。黑盒子人工智

慧系統中固有的（人類和算法的）偏見威脅了保險業內的信任。

最後講者總結與人工智慧標準化活動相關的網路研究：

- 標準和法規可以塑造創新和更廣泛的採用，例如，品質標準可以降低與新技術相關的風險，並促進競爭。
- 標準所涵蓋的領域正在擴大（例如，人工智慧和大數據）；標準在採用和擴散階段也很重要。
- 支持研究活動，以評估如何將人工智慧轉化為用於認證涉及人工智慧的產品、流程和服務的標準。
- 開發一個考慮多種惡意企圖、案例的標準化框架是一項關鍵挑戰。

肆、 心得及建議

在本次會議中，邀請了來自許多國家和機構分享各自領域的資安趨勢，包括了零信任架構、量子安全密碼學、培育人才、人工智慧以及 5G 等主體，講者們宣導了一些相關的資安落實方法以及標準制定的方法，值得我國政府在未來擬訂資安相關政策或標準制定時參考借鏡。

首先，在制定安全標準時，可以將技術和流程標準化，避免花費過多的力氣做重複的事，例如參考沿用先前已制定好的標準、妥善利用自動化工具以避免產品和標準制定的速率不一。

軟體物料清單(SBOM)也是一項需要持續精進並運用的，目前美國聯邦政府為了防範因使用來源不明的軟體元件而導致發生漏洞，已經強制供應商需要提供 SBOM 表。隨著運用開源或第三方軟體元件的情形越來越頻繁，確保軟體元件的組成透明度，並藉此提升管理漏洞的方便程度，變成至關重要的事。政府應參考國際作法，持續向國內製造商宣導 SBOM 的重要性，並提供相關的協助與諮詢服務。

其次，零信任機制也是現下十分熱門的概念，在現今網路環境日益複雜、邊界不明確的情形下，一慮採取不信任，這個方法可以防範許多不必要的攻擊。而零信任之概念也可以應用到日常環境中，即在遇到不確定的狀況時，都需先驗證其安全性再選擇使用，避免因大意而造成被攻擊的局面。我們可以在各個方面加強使用這種機制，並使國人養成零信任的習慣，在取用資料或點選連結時，先驗證可信度，提升國人資安意識。

本次安全會議亦提到量子密鑰分發，這將是一個全新的安全通訊方法，雖然目前美國 NIST 仍未公布最終版 PQC 的相關規範，但是面對新的演算法轉換，NIST 亦呼籲全球政府、企業或組織可以開始著手研究新的演算法，因為這將會使全球公鑰系統大幅更換，我國政府和企業也應該開始注重新的量子加密法。

第三天以較有趣的開場演講作為主題，目前全世界的資安人員僅有 550 萬名，但實際需求人員為 950 萬名，在台灣有許多公司並不注重於資安的治理，許多中小企業抱持著不想投入過多成本的心態對資訊安全抱持著置之不理的態度，一旦造成損失頂多也自認倒楣，並不會顧慮到公司資料外洩所帶來的嚴重性，然而如何提升下一代的網路安全意識，這部分也是台灣需要加強的地方，隨著智慧型手機及電腦的普及，擁有智慧型手機的年齡層逐漸降低，若沒有從小灌輸資安的意識，青少年可能在裝置操作中，無意將自身的個資外洩。目前國外針對這部分已經實施 ETSI ICT 標準化教育計畫，以及 NCSC 的 CyberFirst 計畫等，這些計畫為提升年輕人的資安意識帶來很大的轉變，也能從中找尋及培養資安人才，這部分可以供台灣作為參考，將資安意識帶進校園，以避免年輕族群個資外洩，進而成為攻擊者的目標。

隨著 Chatgpt 的出現，生成式人工智慧已成為近期最熱門的話題之一，聊天機器人的技術也是大家近期最關注的話題，但隨著些技術的成長，隨之帶來的攻擊手法也不斷地在更新，人工智慧會透過人類提供的資料進行學習，伴隨者好壞的龐大資訊量，如果生成式人工智慧模型在訓練數據中可能會出現包含見訊息，它們可能學會生成具有歧視性的內容。這可能加劇社會中不平等的現象，並對特定族群造成不良影響。生成式人工智慧模型在訓練過程中使用大量的個人數據，這些數據可能包括文字、圖像或其他敏感訊息。如果這些模型被濫用，可能導致個人隱私的外洩。因此在教育上，必須讓員工了解到使用生成式人工智慧時必須注意的部分，當中包括不能將公司機密輸入進行提問，公司也應教育員工使用生成式人工智慧的風險，以及其可能帶來的危害。

伍、 相關照片及資料

圖 24、ETSI 外部

參考來源：現場拍攝

圖 25、研討會會議室

參考來源：現場拍攝

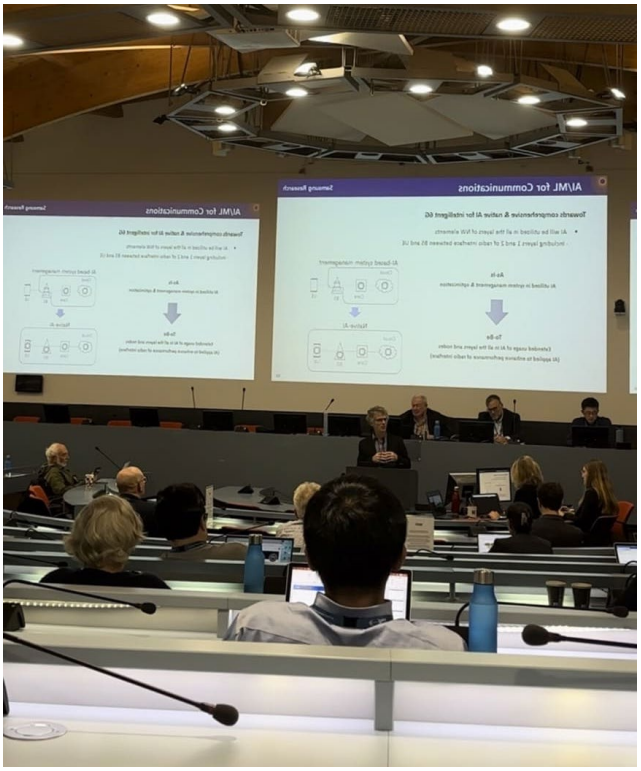


圖 26、研討會演講(1)

參考來源：現場拍攝

圖 27、研討會演講(2)

參考來源：現場拍攝