出國報告（出國類別：開會）

2025 臺灣資安產業荷蘭拓銷出國報告

單位名稱：數位發展部數位產業署
姓名職稱：林俊秀　署長
　　陳宇志　技正

派赴國家：荷蘭（海牙）
出國期間：114 年 9 月 27 日~114 年 10 月 4 日
報告日期：114 年 12 月 16 日

摘要

數位發展部數位產業署（以下簡稱本署）為展示臺灣資安能量、拓展歐洲市場，於 2025 年 9 月組團赴荷蘭參與海牙資安週（Cyber Security Week）及 ONE Conference。此行主軸為深化臺荷資安合作，開拓國際通路，透過政府交流、論壇發聲與企業媒合，展現臺灣資安政策與技術實力。代表團由本署林俊秀署長擔任領隊，與後量子資安產業聯盟、工業技術研究院、資訊工業策進會，共同帶領匯智安全科技、歐生全創新、東擎科技、來毅數位及全景軟體等 5 家國內資安業者進行拓銷，期間除舉辦臺荷企業媒合會，並拜會荷蘭國鐵（NS）、歐盟資安供應商（ESET）及資訊與電信主要用戶協會（BTG）等潛在合作單位，以協助業者鏈結系統整合商與採購方。同時拜會荷蘭資安相關政府與產業組織，以掌握歐洲市場趨勢與合作資源，並評估「地平線歐洲」（Horizon Europe）、「數位歐洲」（Digital Europe）等歐盟計畫參與機會，建立長期投資與研發合作框架，為期 8 天的展示、交流與媒合，有效深化雙邊產業夥伴關係

目錄

圖目錄

壹、目的

為了因應全球資安新局勢並推進臺灣資安產業進入歐洲市場，數位發展部數位產業署（以下簡稱本署）於 2025 年 9 月率領臺灣代表團，參與荷蘭的兩大國際盛事：海牙資安週（Cyber Security Week）與歐洲指標性資安會議 ONE Conference，以「深化臺荷資安合作，開啟國際市場新通路」為主軸，透過官方對話、論壇案例分享及企業媒合等多元活動，藉此展現臺灣資安產業的實力與創新能量，積極尋求歐洲市場的曝光與合作機會。

本署近年來透過臺荷雙方持續不斷的互訪與會議合作，已與荷蘭建立穩定的雙邊交流機制。自 2023 年起便定期參與海牙資安週活動，建立與荷蘭政府及產業界的聯繫管道；同時，荷蘭政府代表亦多次應邀來臺，在 CYBERSEC 臺灣資安大會上分享經驗，有效深化雙方的互信與合作基礎。本次出訪承繼過往交流成果，目標將雙方合作層次升級，著重於拓展產業媒合、推動技術驗證以及資源整合等具體合作項目。本次荷蘭拓銷行程之核心目的包含：

1.提升國際能見度與策略聯盟深化：運用海牙資安週（Cyber Security Week）與具指標性的 ONE Conference 等國際資安平臺，展現臺灣在資安政策推動與後量子密碼（Post-quantum cryptography, PQC）等關鍵技術發展的整體實力。此舉不僅有效擴大了「資安臺灣」的品牌曝光度，同時也成功強化既有的臺荷資訊安全聯盟合作關係，為雙方未來持續推動高層對話與深化產業鏈結，奠定了堅實的合作基礎。

2.協助廠商鏈結合作夥伴、拓展歐洲市場：透過舉辦臺荷資安交流媒合會，並拜會荷蘭國鐵（NS）、歐盟資安供應商（ESET）與資訊與電信主要用戶協會（BTG）等指標性潛在需求方，從而協助我國資安業者與荷蘭當地的系統整合商、代理商及潛在採購單位建立聯繫，促進實質合作洽談，以建立進入歐洲市場的通路節點。

3.掌握歐洲市場趨勢與合作資源：藉由主動拜會荷蘭資安相關政府單位與重要產業組織，蒐集歐洲市場在導入資安標準、產業生態發展現況以及特定應用需求等關鍵情報。同時，積極尋求荷蘭當地的投資、合作與落地支持等資源，以協助臺灣資安業者規劃精準、具可行性的市場布局策略。

4.建立長期資金與合作框架：於 ONE Conference 申辦臺荷資安圓桌論壇，藉由臺荷雙方資安議題交流與研究合作機制探討等多元互動，評估協助產業申請歐盟「地平線歐洲」（Horizon Europe）、「數位歐洲」（Digital Europe）計畫等創新補助資源的可行性，藉此為未來雙邊長期的技術合作、聯合研發投資，以及市場驗證等工作，建立穩固且可持續的資金與合作基礎。

貳、行程

日期	時間	行程
09/27（六）	23:30	搭乘中華航空自臺灣/桃園機場起飛
09/28（日）	07:35－11:15	於捷克/布拉格機場轉機
	12:50	抵達荷蘭/阿姆斯特丹機場
	18:00	晚餐
	20:00	搭車前往住宿飯店 CheckIn
09/29（一）	10:00－11:30	出席海牙資安週開幕式-International Kick-off Cybersecurity Week
	11:30－12:30	拜會荷蘭國家資安中心（NCC-NL）
	14:00－15:00	拜會進駐 HSD Campus 廠商
	15:00	搭車前往駐荷蘭台北代表處
	16:30－17:30	拜會駐荷蘭台北代表處
	18:00	出席臺荷交流晚宴
	21:00	搭車前往住宿飯店
09/30（二）	09:00	出席 ONE Conference 開幕式與主題演講
	09:15－10:20	拜會海牙市政府
	10:25	ONE Conference 新創攤位參觀
	11:00	出席會議議程
	13:30－15:00	拜會歐盟資安供應商（ESET）
	15:00－15:50	出席後量子資安產業聯盟（PQC-CIA）李召集人之專題演講
	16:10－17:10	拜會荷蘭應用科學研究機構（TNO）
	17:15－17:35	拜會 Topsector ICT
	18:30－20:30	出席 ONE Conference － International Cyber Business Event
	21:00	搭車前往住宿飯店

日期	時間	行程
10/01（三）	10:00－12:00	出席 ONE Conference Side Event - Taiwan－Netherlands Cybersecurity Roundtable
	13:20	搭車前往荷蘭國鐵（NS）
	14:00－16:30	拜會荷蘭國鐵（NS）
	18:00	晚餐
	20:00	搭車前往住宿飯店
10/02（四）	10:00	出席臺荷資安交流媒合會
	10:30－11:30	拜會資訊與技術執行機構（ICTU）
	14:00－15:30	拜會資訊與電信主要用戶協會（BTG）
	18:00	晚餐
	20:00	搭車前往住宿飯店
10/03（五）	07:00	搭車前往機場
	11:00	搭乘中華航空自荷蘭/阿姆斯特丹機場起飛
10/04（六）	06:00	抵達臺灣/桃園機場。

參、團員名單

一、 數位發展部

	姓名	單位	職稱
1	林俊秀	數位發展部數位產業署	署長
2	陳宇志	數位發展部數位產業署	技正

二、 隨隊成員

	姓名	單位	職稱
1	黃維中	財團法人工業技術研究院	副所長
2	邱苑慈	財團法人工業技術研究院	副經理
3	林宜萱	財團法人工業技術研究院	副經理
4	蕭榮興	財團法人資訊工業策進會	主任

肆、執行過程及內容

(一) 參與海牙資安週開幕式與 Delegations Leader Pitch

1.**時間**：9 月 29 日 （一） 10:00－11:30

2.**地點**：荷蘭海牙 HSD Campus 7F
（Wilhelmina van Pruisenweg 104, 2595 AN Den Haag）

3.**與會人員**：

臺方	數位發展部數位產業署 後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長
其他國際代表團	西班牙、瑞典、捷克、匈牙利、法國、愛爾蘭、英國、美國及加拿大等 9 個國家代表團。

4.**主題**：海牙資安週啟動活動，各國代表團皆會參加，透過主辦方介紹荷蘭資源及計畫簡介、快速媒合等活動，協助各訪團快速掌握在荷蘭合作機會。上午 10:50 Delegations leaders pitch，臺灣代表團作為首個分享單位，由署長代表本團進行簡介，宣傳 CYBER TAIWAN Side Event、臺荷資安交流媒合活動等。

5.**議程**：

時間	主題	備註
10:00－10:30	Registration and networking	
10:30－10:35	Welcome by Municipality of The Hague, city of Peace, Justice and Security	
10:25－10:40	Introduction Security Delta （HSD） by Joris den Bruinen	

時間	主題	備註
10:40 – 10:50	Topsector ICT	
10:50 – 11:30	**Delegations leaders pitch**	**署長代表介紹（3 分鐘）**
11:30 – 11:45	Coffee break	
11:45 – 12:10	Doing business in The Netherlands & the Dutch cybersecurity landscape	
12:10 – 12:15	Speed Dating Explanation	
12:15 – 13:30	Lunch	
13:30 – 14:30	Speed Dating Round 1（3x20mins at moderated standing tables）	5 家業者參加
14:30 – 15:00	Coffee break	
15:00 – 16:00	Speed Dating Round 2（3x20mins at moderated standing tables）	5 家業者參加
16:00 – 17:00	Final words from moderator & Networking drinks	
17:00	End of Programme	

6.活動重點摘述：

海牙資安週於海牙市政府與海牙資安三角洲（HSD）的共同主持下正式展開。開場旨在協助國際與會者快速掌握荷蘭資安政策、生態與市場脈動，並透過新增的 Delegation Leaders Pitch 使 10 個國家代表團得以在 3 分鐘內簡述其定位與合作方向。此環節使整體活動更具國際能見度，而下午的快速媒合（Speed Dating）則進一步促成代表團與在地企業的精準對接。儘管活動形式多元，但整體焦點仍聚焦於荷蘭官方所欲推動的核心議題，包括國際合作、供應鏈安全、Secure-by-Design 及資安人才培育等，呈現荷蘭在全球資安生態中的戰略布局。

開幕致詞首先由 InnovationQuarter 代表歡迎各國與會者，並強調資安週作為國際交流平台的重要性。接著海牙市副市長以「和平與正義之都」的城市角色闡述海牙在歐洲資安領域的地位，同時呼應歐洲資安月及多項新活動所帶動的城市能量。HSD 總監則強調資安跨越國界、需以全球信任與合作為基礎，並提出以知識、資金、人才與市場為核心的四大支持架構，以及與非營利組織 ECSO（European Cyber Security Organisation）合作推動「Made in Europe」標章，彰顯歐洲自主供應鏈的重要性。隨後，Topsector ICT 的分享進一步勾勒荷蘭「2035 Secure-by-Design」願景，從產業建構、自主安全技術、供應鏈韌性到人才發展，呈現荷蘭面向未來的數位韌性策略。

在國際代表團分享環節中，由臺灣率先分享，此不僅提升現場能見度，也突顯我國在全球 ICT 與半導體供應鏈中的關鍵地位。署長介紹臺灣在後量子密碼（PQC）、SEMI E187 標準、OT 資安技術、數位信任架構與物聯網安全認證等領域的具體成果，並預告將於 ONE Conference 進行 PQC 專題分享及舉辦臺荷資安圓桌會議，展現臺荷深化合作的強烈意願。緊接著，加拿大、捷克、法國與匈牙利等代表也陸續分享各國技術強項與合作期待，涵蓋威脅情報、AI 合規、零信任架構、後量子技術、滲透測試及安全服務等領域，凸顯歐洲資安市場在多元議題下的高度開放性與合作需求。

整體而言，海牙資安週開幕式呈現強烈的國際互動氛圍與策略意涵。荷蘭藉此展現其在政策引導、產業生態與城市韌性上的整合力，而各國代表團則以多樣化的技術與產業優勢提供合作契機。其中，臺灣作為首位發言的代表團，不僅成為焦點，也使我國在國際場合上的專業形象更加鮮明。開幕式整體內容從政策、產業到技術層面展現出跨國協作的可能性，為後續幾日的活動奠定良好基礎。

圖 1：代表團於荷蘭海牙 HSD Campus 合影

圖 2：代表團於海牙資安週合影

圖 3：海牙市副市長 Saskia Bruines 於海牙資安週進行開場致詞

圖 4：海牙資安三角洲（HSD）Joris den Bruinen 主任致詞

圖 5：TopsectorICT　Stephanie Ottenheijm計畫經理致詞

圖 6：海牙資安週開幕式活動現場剪影

圖 7：林俊秀署長以臺灣代表團團長身份上台致詞

圖 8：林俊秀署長於致詞時介紹代表團成員

圖 9：法國代表團代表致詞

圖 10：加拿大代表團代表致詞

(二) ONE Conference – 參與開幕式及研討會、新創攤位參觀

■ ONE Conference 開幕式

1.**時間**：9 月 30 日 （二） 09:00－09:15

2.**地點**：荷蘭海牙 World Forum - KWA 會議室 @ Lobby 層
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員**：

臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：本年度 ONE Conference 聚焦法規與政策、公私協力、供應鏈資安、地緣政治等 8 大元素，匯集演講、攤位等，共來自 55 國、2000 多名與會者進行交流。

5.**議程**：

時間	主題
09:00 – 09:15	ONE Conference – Opening

6.**活動重點摘述**：

本次大會由 Irene Rompa 開場，她在荷蘭科技生態系統中領導加速器、促進荷蘭新創企業的國際擴張並組織大型創新活動。同時任職於 Quantum Delta NL，致力於擴大荷蘭量子技術生態系統。

Irene Rompa 以過去 5 年投入荷蘭量子科技生態的背景切入，提醒與會者，地緣政治因素影響合作夥伴的可信度，公私部門需重新檢視跨境雲與供應商風險；由國家出資或支持的攻擊者，其手法已從間諜轉為破壞行動，從海底電纜、GPS 干擾到工控資安系統皆面臨更具策略性的風險。她同時指出多數組織仍欠缺基本資安防護，荷蘭國家資安中心（National Cyber Security Centrum, NCSC）反映許多單位的工業控

制系統資安防禦都未完善。討論的焦點已從「資料外洩」轉向「資料竊取與關鍵服務中斷」對社會的衝擊；OT 安全的重要性已與 IT 等量齊觀。合規方面，NIS2 與網路韌性法案持續主導對話，供應鏈韌性與中小供應商責任外溢成關鍵。

海牙市長 Jan van Zanen 則以主辦城市首長角度致詞，他從城市角色出發，強調海牙作為「和平與正義之都」及國會與政府中樞，長期負責大型國安與外交活動，並孕育出歐洲具代表性的資安生態 HSD（The Hague Security Delta）。他指出地方治理同樣面臨政治人物安全、示威管理與民生系統（供水、供電、醫療）之資安韌性課題。市府正推動企業網站健全、反詐教育與社區課程以提升公私部門與居民的資安意識。今年會場設置「人才匯聚（Talent Hub）」與首次「資本區（Capital Area）」，號召產學研與投資人連結，促進創新落地。希望在地生態的「人才x技術x資本」要素需同時到位，透過公私協作強化城市與國家的數位韌性。

從歐洲因應地緣政治風險的經驗可供臺灣參考，以應對數位威脅與供應鏈韌性挑戰。面對灰色地帶攻擊與滲透威脅時，透過公私協作培育自主資安技術、強化本地供應鏈能量，並結合相關計畫資源與國際投資合作，打造具韌性的資安產業生態，提升國家整體防護與數位主權能量。

圖 11：ONE Conference 開幕活動現場

■ ONE Conference 新創攤位參觀

1.時間：9 月 30 日 （二） 10:25－10:50

2.地點：荷蘭海牙 World Forum - Ariane 會議室 @ Lobby 層
（Churchillplein 10, 2517 JW Den Haag）

3.與會人員：

臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任

4.活動重點摘述：

(1)圖靈 Turing Space - 專注於去中心化身份技術，以促進跨境信任
Turing Space 是專注於 TrustTech 的新創公司，致力於推動數位身分與電子憑證的應用，服務對象涵蓋 WHO、UNHCR 以及 12 國、550 個政府及機構。公司分布於荷蘭、日本、臺灣與美國，核心技術採用去中心化識別碼（DID）與可驗證憑證（VC），協助政府、企業與個人簡化跨境與跨產業的驗證流程。其亮點包括：高度安全且具互操作性的數位身分解決方案、能有效串接不同國家與產業場域，以及在國際治理與民生應用上皆具實績，對了解去中心化身份在全球治理、政府服務及產業應用的挑戰，具有高度參考價值。

(2)Cyemptive technologies - 提供預防性與主動式資安解決方案
Cyemptive Technologies 是提供「預防性」與「軍用級」資安解決方案的新創公司，核心團隊來自 NSA、微軟與日立，其核心技術 CyberSlice© 能在威脅造成損害前阻止攻擊，包括零日攻擊，無需事後修復。其主要產品包括 ZeroStrike 端到端保護套件、CyberScan 檔案掃描防勒索，以及 Command 系列全面防護方案，並與資安保險公司合作，降低客戶風險與理賠頻率。

圖 12：圖靈 Turing Space 在新創攤位區展示

■ ONE Conference 研討會

1.**時間**：9 月 30 日 （二） 11:00－12:30、15:00－15:50

2.**地點**：**荷蘭海牙 World Forum**
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員**：

臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任

4.**參與緣由**：透過參與大會議程有關供應鏈安全及軍民協防等議題演講，蒐集荷蘭相關做法並作為後續推動策略方向參考。

5.**重點摘述**：

(1) PQC 遷移論壇 PQC Migration Survival Panel

量子電腦預計在未來 10 至 15 年內具備破解現行公鑰機制的能力，使「先儲存、後解密」（store now, decrypt later）的風險已提前浮

現。歐洲多國與美國因此陸續啟動後量子密碼（Post-Quantum Cryptography, PQC）推動計畫，並以 2035 年前全面淘汰具量子脆弱性的既有演算法為共同目標。荷蘭亦在此議題上積極部署，包括由荷蘭國家情報與安全總局（AIVD）、荷蘭應用科學研究機構（TNO）以及荷蘭數學與電腦科學研究中心（CWI）共同發布 PQC 遷移手冊，並成立跨部門遷移工作小組，協助政府與產業建立具體的轉換路徑。

與會專家強調，PQC 遷移的關鍵在於組織層級的推動，而非僅限技術本身。董事會的支持至關重要，因此須將技術議題轉譯為清晰的業務案例、轉換路線圖及成本效益分析，以促成決策共識。專家亦指出，本次遷移可視為推動「密碼學敏捷性（crypto-agility）」的重要契機，要求未來供應商在產品設計時即具備演算法可替換、金鑰可調整及向後相容等能力，使系統能因應後續標準更新與新威脅。

在具體做法上，荷方建議以「化繁為簡」的方式循序推進，由高風險且相對容易切入的內部系統進行轉換，並依「診斷（資產盤點與監測）→規劃→執行」的流程逐步改善。同時，也需根據應用情境選擇純 PQC 或混合架構（hybrid），並評估效能、延遲與相容性等因素。會中亦提及，多數網路通訊與資料交換協定已開始導入 PQC，例如 TLS 1.3 與部分端到端加密通訊（如 Signal）均已採取 PQC 或混合模式部署，顯示產業遷移已進入實質啟動階段，整體轉換時程壓力相當迫切。

對臺灣而言，PQC 不僅是技術升級，更是產業政策與監管推動的「時間賽局」。本署 2025 年已公布後量子密碼遷移指引，持續帶動相關政府機關與單位啟動評估密碼安全，後續應持續在指引中探討「密碼學敏捷性」之規劃原則；推動後量子加密工具、與互通性試驗場域，協助機關與企業獲得安全可靠工具。加速示範場域（政府服務、金融支付、物聯網終端）與國際對接（導入歐盟/美國框架），以形塑在地解決方案並進行實地驗證。

(2) Bridging the CRA Gap: Lifecycles vs. Expectations

隨著歐盟《網路韌性法案》（Cyber Resilience Act, CRA）於 2024 年 12 月 10 日正式生效，各會員國陸續建置監督機構、技術驗證與合格評估程序、檢查機制及罰則制度等落地架構，此一制度化過程勢必影響臺灣物聯網產品外銷歐盟市場的要求與合規成本。本場次由台夫特理工大學（TU Delft）Lorenz Kustosch 博士分享相關研究，著重於具備數位元件之產品是否能在其預期壽命期間維持安

全性並持續受到支援，並探討 CRA 設定的最低要求與消費者實際期待之間的落差。

根據該研究所進行的跨國消費者調查，智慧裝置使用年限的普遍期待明顯高於 CRA 所設定的至少 5 年安全支援門檻。智慧照明、家用路由器與智慧恆溫器多被期望可使用 4 年以上，而太陽能逆變器的平均預期壽命更達 10 年，有些受訪者甚至提出 15 至 20 年的使用需求。此外，超過半數的消費者認為設備在整個生命週期內都應持續獲得軟體更新，以確保安全維運。然而，調查亦顯示，多數用戶其實無法判斷家中常見物聯網設備（如路由器、掃地機器人、智慧燈具）是否仍在接收安全更新，反映出用戶端資訊缺乏透明度的問題尤為明顯。

講者指出，目前要求使用者登入各設備介面逐一查核更新狀態的方式並不實際，難以作為確保產品安全維運的可行手段。儘管 CRA 已要求製造商負有資訊揭露義務，但在實際操作上，仍需更直覺、易辨識的標示與資訊呈現機制，以協助終端用戶做出較為明確的採購與維護決策。整體而言，該研究顯示，未來物聯網設備的安全維運不僅是法規問題，也涉及市場期待與使用者資訊可得性的提升，對臺灣輸歐產品亦具重要參考意義。

本場議題突顯物聯網產品「資安維運責任」的重要性，與本署推動的物聯網設備資安標準與測試規範方向一致。未來可持續強化具數位元素產品安全支援年限之揭露義務，並公開揭露「更新有效期」與「漏洞修補機制」，透過認驗證與標章制度與國際標準的對接，提升國產物聯網設備在國際市場的信任度與韌性，形成具出口競爭力的安全供應鏈體系。

(3) Accelerating PQC Deployment through PPP

本場次由臺灣後量子資安產業聯盟李維斌召集人演講，聚焦抗量子電腦攻擊、後量子加密及後量子遷移議題，此議題在荷蘭也是備受關注，透過公開演講，不僅可加強曝光臺灣資安能量，更分享臺灣如何以公私協力方式推動相關議題與進展，有助於推動臺荷或臺歐盟國家合作。

本場演講以「臺灣後量子密碼公私協力方式推動現況」為主軸，說明全球面臨量子計算威脅下，密碼系統轉型的緊迫性。李維斌召集人指出，臺灣在本署推動下，採取自上而下（政府、金融、關鍵基

礎設施）與自下而上（製造、通訊、醫療等產業）雙軌並進策略，透過需求端示範與供應端創新共同驅動 PQC 落地。並介紹了我國首部《臺灣後量子密碼遷移指引》，並說明指引主要參考 NIST SP 1800-38 系列與 FIPS 203/204/205 標準，配合 MOSCA、CARAF、PASTA 等風險評估方法，建構完整遷移流程。此外，本署亦推動產官學合作建立 PQC 晶片標準化平台與安全評估工具（PQ-SAT），以提升國內產業的密碼敏捷性與自主測試能量。李維斌召集人強調，PQC 導入不僅是技術升級，更是國家資安韌性的關鍵工程，需兼顧加密效能與供應鏈協作。

圖 13：專家於 PQC 遷移論壇發表看法

圖 14：Lorenz Kustosch 從網路韌性法案探討物聯網產品資安必要性

圖 15：後量子資安產業聯盟李維斌召集人分享臺灣 PQC 公私協力推動現況

(三) ONE Conference – International Cyber Business Event

1.**時間：**9 月 30 日 （二） 18:30–20:30

2.**地點：荷蘭海牙 Marriot Hotel**
（Johan de Wittlaan 30, 2517 JR Den Haag）

3.**與會人員：**

臺方	數位發展部數位產業署 後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長
其他國際代表團	全球資安領袖、荷蘭創業家、新創與成長型企業

4.**主題：**ONE Conference 專屬國際資安交流活動，本團有申請 Taiwan Stand 以提升曝光及交流機會。

5.**活動重點摘述：**
相對白天大會活動聚焦技術分享及如何以技術解決社會議題等（禁止商業行為及行銷），晚會活動則是鼓勵參與之全球資安領袖、荷蘭創業家、新創與成長型企業間商業交流的活動，並可申請攤位（一小型立桌及 LOGO 識別牌），增加露出及交流機會。本團有申請 Taiwan Stand，由團隊與 5 家業者以 30 分鐘一班的方式，輪流於攤位駐點。

現場人潮眾多、環境較為熱絡，雖較難進行深入洽談或立即觸發商機，但活動形式有助於與白天正式會議中結識的潛在合作夥伴，在輕鬆氣氛中再次互動，從聊天中更熟悉彼此，為後續合作奠定基礎。

此整體活動安排順暢，Taiwan Stand 的設計與位置有效提升了代表團的曝光與交流成效。此外，透過 SECPAAS Cyber Taiwan 官方 LinkedIn 頻道的策略性社群推廣，進一步擴大了臺灣代表團在國際舞台上的能見度與專業形象。

場地配置

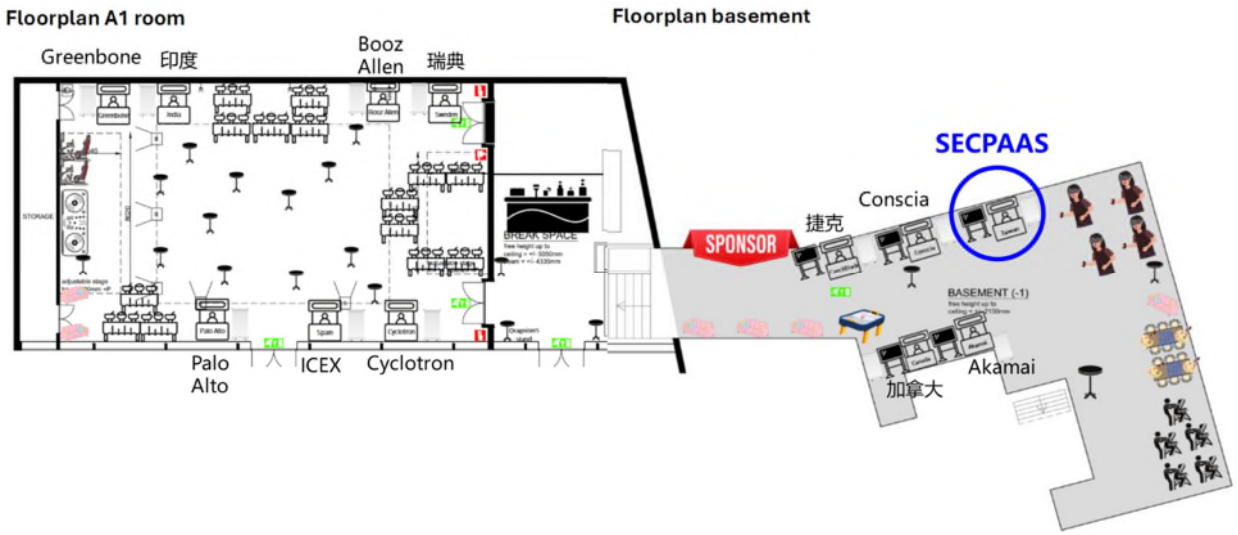


圖 16：Business Event 場地配置

SECPAAS 攤位規劃

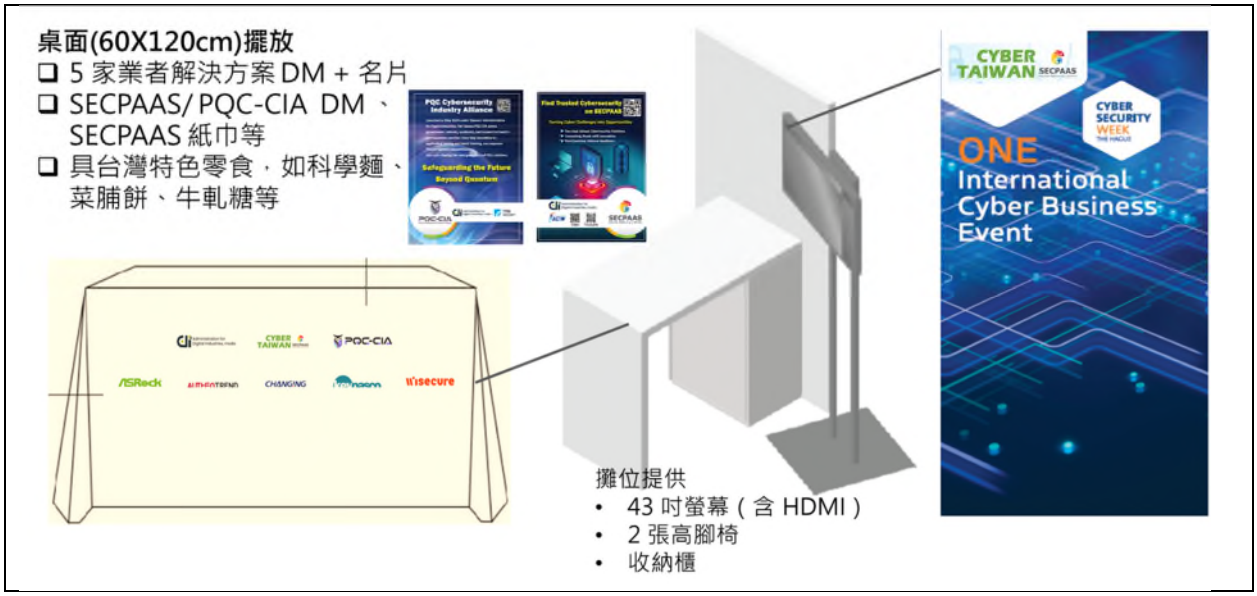


圖 17：Taiwan Stand SECPAAS 攤位規劃

圖 18：Taiwan Stand 擺設

圖 19：林俊秀署長與來毅於 Taiwan Stand 合影

圖 20：全景代表於 Taiwan Stand 與參觀者合影

圖 21：International Cyber Business Event 其他參與攤位

(四) ONE Conference – Taiwan–Netherlands Cybersecurity Roundtable

1.**時間**：10 月 1 日 （三） 10:00–12:00

2.**地點**：**荷蘭海牙 World Forum - Kilimanjaro 2 @ 樓層 2**
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員**：

荷方	EZ 荷蘭經濟部 ・數位經濟司司長 Leah Postma ・資安產業聚落協調員 Brenda van der Wal ・數位信任中心 Anouk de Rooij 荷蘭國家資安中心 NCC-NL ・公共部門顧問 Nina Huijberts 海牙資安三角洲 HSD ・主任 Joris den Bruinen CFLW 總經理 Mark van Staalduinen 現場蒞臨來賓……等
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：藉由雙方分享政府補助資源，加深臺荷資訊安全聯盟交流合作，以協助推動臺荷雙邊資安技術合作。

5.**議程**：

時間	主題	主講者
10:00–10:05	開場致詞	林俊秀署長
10:05–10:10	在地方治理中嵌入資安	來毅數位 林政毅執行長

時間	主題	主講者
10:10－10:15	以人為本的身分識別，打造更安全的數位社會	歐生全 Peter Sun 歐洲業務總監
10:15－10:20	後量子 HSM 與零信任基礎	匯智安全 鄭嘉信執行長
10:20－10:25	保護現代社會的數位骨幹	東擎科技 廖重欽歐洲業務總監
10:25－10:30	建立數位信任	全景軟體 陳俊良副總經理
探索臺灣—荷蘭資安技術合作與驗證機會		
10:35－10:45	HSD 研究報告：聚焦臺灣、新加坡、日本、南韓的資安發展藍圖	海牙資安三角洲 Joris den Bruinen 主任
10:45－10:55	臺荷資安聯盟成果	CFLW Mark van Staalduinen 總經理
10:55－12:00	自由交流	

6.**活動緣由：**

(1) 本次圓桌會議目的為建立一個涵蓋產業、政府、學術和研究的合作平台，促進臺荷雙邊資安技術共同合作與推廣。並探討共同申請臺灣與歐盟的補助計畫可能性，以進一步強化雙邊資安技術合作研發之深度。

(2) 本署於去年出訪 ONE Conference 期間，促成臺荷雙邊成立「臺荷資訊安全聯盟」，包含 CFLW、HSD 及 Keypasco 等 3 家荷方代表，及來毅數位、池安量子、振生半導體、幻雲資訊和圖靈等 5 家臺方代表加入聯盟，並在本署與荷蘭經濟部數位經濟局（DDE － EZ）代表見證下，簽署合作備忘錄，已奠定初步合作基礎，例如今（2025）年資安大會期間 CFLW、HSD 等荷方成員代表也再度來臺，並邀請荷蘭國鐵資安長及 ElecticIQ 等有興趣與臺灣合作的代表一同參與交流。

本次活動希望可在雙邊合作基礎下，進一步聚焦在如何結合雙方政府計畫資源，共同支持雙方資安技術整合及落地驗證。

7.**活動重點摘述：**

本次會議主要延續並深化臺荷雙邊資訊安全的交流與合作，並探討如何結合雙方政府資源，共同推動資安技術的合作與推廣。署長在開場致詞中強調，面對日益嚴峻的數位威脅，政府、學研與產業之間的跨域合作至關重要。荷蘭經濟部數位經濟司司長則明確指出，資安是一個集體挑戰（collective challenge），任何一方的弱點都可能影響全球數位供應鏈的安全，因此雙方應建立長遠且多面向的合作機制，共同提升資安韌性。

5 家臺灣資安廠商輪流分享他們如何用資安技術解決全球共通問題後，交流環節聚焦在幾個重點議題，包含後量子密碼技術（PQC）的挑戰與遷移策略。量子運算對現有加密技術的威脅已越來越近，面臨駭客「先擷取資料，後解密」（Harvest Now, Decrypt Later）的風險。臺灣代表團分享了 PQC 聯盟在推動標準化方面的努力，並提出了混合式遷移模式（Hybrid Mode），建議將現有的傳統加密演算法與新的 PQC 演算法結合使用，以應對長期的量子威脅。由於 PQC 遷移過程預計將是長達 10 年以上的漫長旅程，建議企業在採購新設備時，應將具備「PQC Ready」的能力納為關鍵考量因素。討論中也特別提到，對於 OT 設備（營運技術設備）等難以隨意替換或更新的關鍵基礎設施，更需要謹慎處理過渡期的風險與更新挑戰。

另外有關臺荷合作機制部分，荷蘭國家資安中心（NCC-NL）的代表指出，該中心可作為歐盟資安能力中心（ECCC）在荷蘭的對口，提供歐洲層級的資金機會，特別是來自如「地平線歐洲」（Horizon Europe）或「數位歐洲」（Digital Europe）計畫等，這些計畫涵蓋資安創新、PQC 和 AI 等領域。非歐盟國家如臺灣，可以參考瑞士或以色列等國家的做法，透過公私學研夥伴關係，以「關聯成員」（associated partner）的身分加入這些跨國專案。雙方應專注於共同投入資源，在聯合研究與開發專案上展開合作，建立共同的技術路線圖，以期實現實質互惠的長期合作關係。此外，荷方也強調，資安領域的標準化過程（如歐盟的 CRA 法案）通常非常緩慢，因此必須主動進行跨國合作，以應對不斷變化的威脅。

圖 22：林俊秀署長於會前與荷蘭經濟部數位經濟司司長（左一）交流

圖 23：Taiwan－Netherlands Cybersecurity Roundtable 與會者合影

(五) 拜會荷蘭國家資安中心（NCC-NL）

1.**時間**：9 月 29 日 （一） 11:30－12:30

2.**地點**：荷蘭海牙 RVO-HQ building
（Pr. Beatrixlaan 2, 2595 AL Den Haag）

3.**與會人員**：

荷方	荷蘭企業署（RVO）： ・國際創新合作主任 Gabriëlle van Zoeren 荷蘭國家資安中心（RVO/NCC-NL） ・主任 Jurriën Norder ・歐盟事務顧問 Lodewijk Noordzij ・公共部門顧問 Nina Huijberts ・DEP 聯盟建構顧問 Emi Metselaar 國際研究與創新合作部門（RVO/Team IRIS） ・顧問 Eddy Schipper 任務與技術合作部門（RVO/Team MATCH） ・顧問 Bob Hengeveld
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：了解歐盟創新資金關注的資安議題，以及對後量子遷移的看法，另透過歐盟資安相關法規制定趨勢，從中尋求臺灣資安業者切入歐洲市場的機會。

5.**議程：**

時間	主題	主講者
11:30－11:40	開場/雙方與會者介紹	Gabriëlle van Zoeren 國際創新合作主任 林俊秀署長
11:40－11:55	RVO/NCC-NL 簡介	NCC-NL 主任 Jurriën Norder
11:55－12:25	雙方交流議題： 1. NCC-NL 在協助產業鏈結「地平線歐洲」（Horizon Europe）或「數位歐洲」（Digital Europe）計畫上有什麼方式？臺灣的資安業者是否也能透過貴單位找到合作機會？ 2. 請益歐盟資安法規（CRA、NIS2、CSA、EUCC 等）的政策推進方向，以及荷蘭政府協助企業落地的策略，並提供臺灣業者進入歐洲市場所需的法規資訊、資安檢測生態地圖及建議。 3.歐盟 CRA 法案已經對資通訊產品的資訊安全提出規範，荷蘭政府如何協助資通訊廠商符合 CRA 的規範？可以提供臺灣參考	
12:25－12:30	全體與會者合影	林俊秀署長代表致贈禮物

6.**拜會重點摘述：**

荷蘭國家資安中心（Netherlands Cybersecurity Coordination Centre, NCC-NL）在今年正式承接資安研究與創新平台 dcypher 的功能後，成為荷蘭推動資安研究、創新與跨部門協作的核心機構。本次會議以臺荷多年合作為起點，從雙方既有的 Globalstars 計畫與「地平線歐洲」（Horizon Europe）共同專案，延伸至歐盟最新資安法規與未

來研發合作模式的討論。會議由荷蘭企業署（Rijksdienst voor Ondernemend Nederland, RVO）國際創新合作主任 Gabriëlle van Zoeren 開場，她回顧自 2019 年以來雙方在資安、積體光學與光纖感測等領域的合作成果，並強調荷方高度重視與臺灣的長期夥伴關係，希望在全球挑戰日益複雜的背景下，持續攜手打造更安全且具韌性的數位環境。

而 NCC-NL 主任 Jurriën Norder 所提出的歐盟資安監管趨勢，尤其是《網路韌性法案》（Cyber Resilience Act, CRA）預計於 2026 年正式生效。該法案要求所有含數位元件的產品在完整生命週期中皆維持資安韌性與漏洞管理能力，對出口歐盟的臺灣製造業與資通產業產生直接影響。在法規脈絡之外，荷方也介紹 NCC-NL 所提供的補助與支援機制，包括 SECURE 專案與「網路安全創新基金」Cybersecurity Innovation Fund（CIF-NL），及推動國際創新合作的多層級工具，如前期探索任務（Fact-finding Missions）等。然而，依照「歐盟控股原則」，非歐盟企業需在歐盟境內設立子公司並符合控股資格方可直接申請歐盟層級資金。因此他建議臺灣企業可考慮以「地平線歐洲」（Horizon Europe）或「數位歐洲」（Digital Europe）計畫的「關聯成員」（associated partner）方式參與，以強化研發合作與資金接軌。

在研發合作模式的討論中，署長特別關注 NCC-NL 與歐盟補助機制是否有適用跨國企業的研發合作。荷方回應 NCC-NL 的服務對象包括公部門、學術研究機構與私部門企業，而補助設計特別重視企業主導的創新案」，政府則扮演資金與制度架構的促成者，多數補助計畫皆由企業主導並可邀請學研單位共同參與。因此若臺荷企業共同聚焦資安或數位韌性領域，原則上可納入 NCC-NL 或歐盟計畫的可行支援範圍。RVO 也提到正籌備與臺灣的新一波雙邊合作計畫，而資安是荷蘭十大關鍵技術領域之一，顯示此領域具高度成長潛力。

在會議總結時，雙方皆認為成功的國際研發合作應建立在穩固的夥伴關係之上。歐盟與荷蘭目前提供層級多元的研發資助機制，包括 Horizon Europe、Digital Europe、Eureka、Globalstars 與 Bilateral Programme 等，均能支持跨國企業及研究機構投入創新研發。臺荷雙方在光子技術（photonics）與高科技領域已有多年合作基礎，未來以資安技術作為深化合作的新方向意義重大。雙方一致認為，可透過 RVO 與荷蘭在臺辦事處作為後續對接與合作的主要窗口，持續推動共同研發與跨國創新。

圖 24：拜會荷蘭國家資安中心 RVO/NCC-NL 會議

(六) 拜會進駐 HSD Campus 廠商

1.**時間：**9 月 29 日 （一） 14:00－15:00

2.**地點：荷蘭海牙 HSD Campus 6F**
（Wilhelmina van Pruisenweg 104, 2595 AN Den Haag）

3.**與會人員：**

臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈 資策會：蕭榮興主任 台灣企業國際化協助網絡：許秀芳執行長

4.**主題：**拜會進駐 HSD 的臺灣廠商以及其合作夥伴 CFLW。

5.**議程：**

時間	**主題**	**主講者**
14:30－14:45	拜會來毅數位/Keypasco	林政毅執行長
14:45－15:10	拜會 CFLW	Dr. Mark van Staalduinen, Managing Director & Founder

6.**參觀重點摘述：**

來毅數位科技股份有限公司（LYDSEC Digital Technology Co., Ltd.）成立於 2012 年 5 月 10 日，總部位於臺北，專注於資訊安全軟體的研發與銷售，主打「Keypasco」身分認證與管理方案，涵蓋多因子驗證（MFA）、FIDO 認證及企業級安全解決方案。公司自創立起即以國際市場為目標，除臺灣外已在瑞典設立研發子公司，並於日本、香港、美國及荷蘭等地設有據點，服務橫跨至少 16 個國家，涵蓋金融、政府機構、電商、智慧製造等多元產業。來毅數位積極推動國際合作，2024 年與荷蘭資安平台 HSD 及 CFLW 簽署臺荷資安合作備忘錄，並於 2025 年 1

月 27 日成立荷蘭分公司 Keypasco Europe BV，此舉有助於深化其歐洲市場布局，展現了公司以臺灣為基地、放眼全球的資安領導地位。

CFLW Cyber Strategies 是荷蘭在地的全球網路情報（cyber intelligence）服務商，聚焦暗網威脅監控、加密資產/區塊鏈犯罪分析、AI 與新興技術下的數位犯罪偵察等。當天由創辦人 Dr. Mark van Staalduinen（總經理暨創辦人）接待與介紹他們如何以 Dark Web Monitor 等工具協助政府與產業對抗網路犯罪。其核心產品與服務主要包含：

（1）Dark Web Monitor 針對暗網論壇/市集的情資蒐集、關鍵字與威脅指標（IOC）追蹤，產出可行動情報，服務政府、金融與企業客戶。
（2）Crypto-Asset Analytics：追蹤鏈上資金流與非法交易樣態，支援執法與監管調查。
（3）分析與取證：結合 AI 與開源情報技術，分析釣魚與資料外洩情資，追蹤新興科技犯罪並協助政府與企業進行數據取證與資安威脅偵測。

CFLW 是 2024 年簽署臺荷資安合作備忘錄（MOU）的發起單位之一，Dr.Mark 也於 2025 年應邀來台參加臺灣資安大會，目前已與來毅數位展開專案合作。

圖 25：來毅數位在 HSD Campus 辦公室

(七) 拜會駐荷蘭台北代表處

1.**時間：**9 月 29 日 （一） 16:30－17:30

2.**地點：荷蘭海牙 駐荷蘭台北代表處**
（Van Stolkweg 23, 2585 JM Den Haag）

3.**與會人員：**

駐荷蘭台北代表處	田中光大使、劉公漢副參事、吳怡真組長、陳昇裕秘書、蔡博名秘書
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 工研院：黃維中副所長、邱苑慈 資策會：蕭榮興主任

4.**主題：**了解荷蘭政策及產業趨勢，尋求後續臺灣資安業者可於荷蘭拓銷的資源鏈結。

5.**議程：**

時間	主題	主講者
16:30－16:40	開場/雙方與會者介紹	田中光大使 林俊秀署長
16:40－17:20	雙方交流議題： 1. 本署目前與荷方資安交流規劃 2. 荷蘭在資安政策的趨勢為何？ 3. 荷方如何協助外國廠商赴當地投資或拓銷的官方單位（含聯絡窗口）及資源有哪些？	
17:20－17:30	全體與會者合影	林俊秀署長代表致贈禮物

6.**拜會緣由：**
拜會駐荷蘭台北代表處旨在就我國與荷方在資安領域既有合作基礎上，進一步強化政策與產業鏈結，並瞭解荷蘭資安產業發展趨勢與投資環境。近年本署與荷蘭海牙資安三角洲（HSD）互動密切，除邀請荷方貴賓訪

台及參與 ONE Conference 外，臺灣廠商如來毅、圖靈及立端已於當地設立據點，成為深化雙邊合作的實例。為促進我國資安產業在歐洲市場的落地與拓展，此次特別拜會海牙市政府、荷蘭經濟部（EZ）及 Topsector ICT 等單位，期透過駐處協助，掌握荷方資安政策走向、產業發展重點與相關落地資源，作為未來臺灣業者切入歐洲市場及參與歐盟補助計畫的重要依據。

同時，荷蘭政府於 2022 年發布《荷蘭 2022－2028 資安戰略》，提出提升公私部門資安韌性、推動安全創新、應對跨國威脅及培育資安人才等四大方向，並設立「網路安全創新基金」（CIF-NL）以鼓勵中小企業投入資安研發。代表團期盼透過駐處協助，進一步瞭解荷方相關政策及官方投資推廣單位（如荷蘭投資局 NFIA）的運作與資源，建立我國廠商落地荷蘭的合作管道，並推動後續在人才交流、技術合作及情資共享等面向的長期合作機制。

7.**拜會重點摘述：**

本署於會中感謝駐荷蘭台北代表處的協助與安排，並指出本署的任務之一，是推動臺灣資安產業發展與國際布局。臺荷交流歷史悠久，從早期農業往來發展至今日以高科技為主軸的深層合作，其中台積電（TSMC）與艾司摩爾（ASML）於全球半導體價值鏈中長期合作的模式，更突顯雙方產業互補與戰略夥伴關係的重要性。鑒於歐盟積極推動「Chips Act（晶片聯盟）」，意欲重塑歐洲半導體生態，本署認為臺灣應把握此政策契機，特別在 AI 與資安領域深化與歐洲夥伴的合作，以建立兼具技術深度與韌性的長期夥伴關係。

近年臺灣在後量子密碼（PQC）技術已於產業落地實作，並與荷蘭研究機構具互補發展潛力，未來可成為雙邊合作的技術基礎。同時，SEMI E187 工控設備資安標準正逐步成為全球半導體供應鏈的共同規範，預期將強制要求包括 ASML 在內的設備商遵循，這為臺灣資安廠商提供切入國際市場的關鍵機會。另外隨著以色列等傳統競爭對手因國際情勢受限，臺灣的資安技術與可信形象更具優勢，應積極強化在歐洲市場的品牌能見度與合作布局。

駐荷蘭台北代表處田中光大使認為資安議題技術性高，駐處可扮演「引薦者」與「協調者」角色，協助鏈結荷蘭政府與產業夥伴，推動公私協力合作。署長則呼應，應以經濟實力作為外交價值之支撐，透過產業成果推動「價值外交」，展現臺灣的國際貢獻與實質影響力。最後經濟組

組長建議 10 月底至 11 月初間舉辦臺荷署長級及次長級對話，除探討經貿、創新、AI 與半導體外，也可將資安列為重要合作議題，並納入「Globalstars」計畫框架。此舉可促使雙方企業共同申請政府補助與概念驗證（PoC）專案，以落實具體合作。此外，亦建議代表團未來與荷方交流時，應明確呈現合作能帶來的實際效益與互惠成果，建立長期且務實的夥伴關係。

圖 26：代表團與駐荷蘭台北代表處成員合影

(八) 拜會海牙市政府

1.**時間：**9 月 30 日 （二） 09:15－10:20

2.**地點：荷蘭海牙 World Forum - Nile 會議室 @ 樓層 1**
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員：**

荷方	海牙市政府 ・市長 Jan van Zanen ・資安長（CISO）Lilian Knippenberg ・數位策略師 Daan Rijnders ・國際事務政策顧問 Pit Scheer
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 台灣企業國際化協助網絡：許秀芳執行長

4.**主題：**尋求後續臺灣資安業者及後量子在荷蘭拓銷的資源鏈結。

5.**議程：**

時間	主題	主講者
09:15－09:25	開場/雙方與會者介紹	海牙市政府 Jan van Zanen 市長 林俊秀署長
09:25－09:30	臺荷資安交流歷程與合作規劃	陳宇志技正
09:30－09:35	全體與會者合影	林俊秀署長代表致贈禮物

時間	主題	主講者
09:35－10:20	雙方交流議題： 1. HSD 的成立與發展 2. 就海牙的城市創新與數位治理交換意見 3. 請益臺灣資安業者可鏈結荷蘭計畫資源的可行性及方式 4. 了解 Hack the Hague 活動未來規劃，表達臺灣組隊參與意願外，及探討其與臺灣其他駭客競賽活動鏈結之可行性	

6.**拜會重點摘述：**

本署此次拜會的核心目的在於聚焦臺荷雙方於資安、後量子密碼（PQC）技術、資安產業鏈交流與城市資安治理等領域的合作方向，並就未來計畫進行具體討論。我方首先說明臺灣在資安推動的現況與策略，由於臺灣是全球受網路攻擊最頻繁的地區之一，政府正積極推動零信任架構與量子後密碼技術的落實。同時，已建立多項資安認證制度，包括物聯網產品資安標章、應用程式安全檢測制度，以及與 SEMI 合作制定的半導體設備資安標準 SEMI E187。此外，臺灣也引入 CMMC 架構，以提升國防供應鏈的資安能量。

在研發與創新合作方面，荷方亦舉出 EclecticIQ 與臺灣 TeamT5 的成功合作案例，強調臺荷在資安技術上的互補性已具相當基礎，可作為拓展雙邊合作模式的參考。雙方就多項國際合作機制進行交流，包括 Eureka、Globalstars 及臺歐 ICT 對話等平台，透過這些框架可促進臺荷企業與新創共同申請國際研發案，荷蘭方則由荷蘭企業署（RVO）及荷蘭科研基金會（NOW）為對接的資助來源。

雙方一致認為可先以後量子密碼（PQC）作為合作起點，結合產官學能量展開聯合研發與示範。署長建議可邀請荷蘭 PQC 領域專家赴臺進行聯合實證，再於荷蘭落地應用。荷方則提及歐盟「數位歐洲」（Digital Europe）計畫目前有 PQC 相關徵案，雙方可此為切入點，共同參與國際研發計畫。

在城市資安合作部分，海牙市政府都市發展與經濟事務局局長 Marijn Fraanje 及現任資安長 Lilian Knippenberg 介紹了該市每年舉辦的

「Hack The Hague」活動。該活動以協作式弱點揭露（CVD）為核心，結合學生、專業駭客及企業力量，透過實際演練來提升城市資安韌性與公民資安意識。署長亦分享臺灣今年於臺南舉辦首屆「Hack Tainan」城市駭客活動成果，雙方有意推動「Hack The Hague × Hack Tainan」串聯活動，並促進資安社群交流、專家互訪及經驗分享。

雙方最後達成多項後續合作初步共識，包括持續推動後量子密碼聯合研發與實證、規劃城市資安駭客活動合作與教育交流、強化供應鏈及半導體產業資安合作，以及透過雙邊或歐洲資助計畫建立長期合作機制，深化臺荷兩地在資安與創新領域的夥伴關係。

圖 27：代表團與海牙市政府代表於會場會議室交流

圖 28：代表團與海牙市政府代表合影

(九) 拜會歐盟資安供應商（ESET）

1.**時間：**9 月 30 日 （二） 13:30－15:00

2.**地點：荷蘭海牙 Marriot Hotel - Executive Boardroom 會議室**
（Johan de Wittlaan 30, 2517 JR Den Haag）

3.**與會人員：**

荷方	ESET ・Martin Talian, 首席企業方案長
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題：**了解 ESET 企業會員資安需求，介紹臺灣後量子推動內容及廠商資安能量，提供雙方交流機會。

5.**議程：**

時間	主題	主講者
13:30－13:40	開場及與會者介紹	林俊秀署長
13:40－13:55	ESET 簡介	Martin Talian, 首席企業方案長
13:55－14:10	PQC-CIA 成果及案例簡介	黃維中副所長
14:10－14:40	臺灣資安解決方案簡介	資安業者各約 6 分鐘
14:40－14:55	Q&A 交流時間	
14:55－15:00	全體與會者合影	林俊秀署長代表致贈禮物

6.**拜會緣由：**

ESET 為歐盟最大的資安供應商之一，在全球已超過 200 個國家與地區設有業務。本次交流的 Martin Talian 過去與資策會國合中心因歐銀專案有合作，未來將協助推動 ESET 亞太地區市場業務，因此有意願了解我國資安解決方案，故安排本次活動促進雙邊交流。

7.**拜會重點摘述：**

與歐盟資安供應商（ESET）的拜會交流，主要目的是讓臺灣資安產業與歐洲資安巨頭建立聯繫，並探討具體的合作機會。ESET 首席企業方案長 Martin 先生在會中向臺灣代表團介紹了公司的策略與技術優勢。ESET 成立於 1992 年，總部位於斯洛伐克，是歐洲最大的私營資安公司之一，業務範圍涵蓋全球超過 200 個國家與地區。Martin 先生指出，ESET 作為歐洲主要專注於研究且由歐洲人擁有的資安公司（他稱之為「Ferrari 引擎」），正將重點從單純的軟體供應商轉移到開發企業級的專業領域解決方案。這些解決方案涵蓋國防、政府、醫療保健和金融機構等關鍵產業。ESET 的核心實力在於其大規模的威脅情報網絡，透過超過 1 億個設備，為其 AI 和研究服務提供巨大的輸入數據，使其在資安研究能力上處於領先地位。

臺灣代表團藉此機會展示了具備國際競爭力的資安解決方案，以尋求與 ESET 在技術整合與市場推廣上的互補與合作。署長在開場時，即強調臺灣在後量子密碼技術（PQC）、工控資安（OT cybersecurity）和零信任架構（Zero-Trust architecture）上的推動成果。隨團的 5 家臺灣業者提供了具體的解決方案亮點：匯智安全科技（WiSECURE）展示可整合 PQC 演算法的晶片與高效能硬體安全模組（HSM），並與 Google 合作提供雲端加密方案；歐生全創新（AuthenTrend）以生物辨識 FIDO2 無密碼技術結合 PQC，強化量子時代的身分驗證安全；東擎科技（ASRock Industrial）提供符合 IEC 62443 工控資安標準的嵌入式硬體產品，滿足歐洲 NIS2 與 CRA 法規；來毅數位（Keypasco）以雙通道多因子驗證（MFA）機制實現零信任網路架構，有效防禦中間人攻擊；全景軟體（Changing）則以 CG Trust 平台整合 FIDO 身分與設備識別，並可與 EDR/SIEM 系統串接，具備金融業 PKI 應用經驗並規劃導入 PQC 技術。整體展示展現臺灣資安產業在端點防護、身份驗證與工控安全等領域的完整能量與國際合作潛力。

ESET 的核心實力在於其大規模的威脅情報網絡，透過超過 1 億個設備的輸入數據，使其在資安研究能力上處於領先地位。從 Martin 先生的回饋與提問中，可觀察到對方的核心關注重點，包括工控資安分層防護與

資料保護機制的實務可行性。另 Martin 先生也於會中明確表達，他們正在尋找 OT（營運技術）資安和網路資安方面的合作夥伴，並可為特定區域提供定制化的威脅研究服務。

圖 29：代表團與 Martin 先生合影

(十) 拜會荷蘭應用科學研究機構（TNO）

1.**時間：**9 月 30 日 （二） 16:10－17:10

2.**地點：荷蘭海牙 World Forum - Everest 2 @ 樓層 2**
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員：**

荷方	TNO ・Dr. Thomas Attema 密碼學研究員 ・Dr. Michiel van der Veen 資安事業總監
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 台灣企業國際化協助網絡：許秀芳執行長

4.**拜會緣由：**雙方就後量子遷移指引的實證策略、經驗，以及產業辦理遷移的不足之處進行交流，以尋求合作機會。

5.**拜會重點摘述：**

荷蘭應用科學研究組織（Netherlands Organisation for Applied Scientific Research, TNO）是荷蘭規模最大的應用科學研究機構，並於 2023 年與荷蘭國家情報與安全總局（AIVD）、荷蘭數學與電腦科學研究中心（CWI）共同發布後量子密碼（Post-Quantum Cryptography, PQC）遷移指引，2024 年 12 月也推出第二版，納入最新的標準進展、工具模組與政策框架。本次與會的 Thomas Attema 是該指引的主要撰寫者之一，同時也是 TNO 的密碼學研究員，其研究涵蓋從風險評估、策略規劃到遷移執行的完整流程。在技術落地上，他特別著重於如何在既有通訊協定上進行「混合模式」部署、提升密碼學敏捷性（crypto-agility），並兼顧新技術在效能與隱私需求上的平衡，使 PQC 不僅是抵禦量子威脅的替代方案，也能符合實際應用的運作需求。

Attema 在簡報中提出由「認知→行動→協作→後續」構成的推動路徑，作為組織推動 PQC 遷移的全生命週期方法。首先，需透過系列活動與溝通機制提升決策層與技術社群間的共同語言，使組織充分理解量子風險與遷移必要性；其次，將 PQC 遷移手冊落實到資產盤點、風險分級、

敏捷化改造與混合部署等具體步驟；最後，建立跨域協作機制，讓學研、政府、關鍵領域業者與解決方案供應商共同參與測試與驗證；最終階段則需透過國家與歐盟的政策框架銜接標準制定與市場採購，形成可持續的合規與測試能量。Attema 強調 PQC 遷移並非僅是替換演算法，而是同時牽涉治理與技術的系統性轉型工程，需搭配成熟的工具套件、可驗證的混合方案與具體的進度衡量指標，並在政策與採購層面嵌入相關實施條件，以降低跨金融、物聯網與關鍵基礎設施等領域的轉換阻力。

在技術層面上，Attema 也指出 PQC 遷移常被誤以為只是加密標準的轉換，但實務上首要挑戰在於「設定優先順序」。因此，他提醒組織在啟動 PQC 遷移前，必須先完成加密資產盤點，以掌握基礎設施中各類加密技術的使用情形，並據以進行後續策略規劃。此外，組織需建立明確的治理架構，以管理整體轉型過程，並與供應商共同討論如何實現真正具備彈性的加密敏捷性；同時透過階段性評估檢視遷移進度，以確認技術與流程上的改變是否朝正確方向推進。整體而言，本場拜會呈現荷蘭在 PQC 遷移上的高度成熟性，也為其他國家推動量子時代密碼轉換提供具有參考價值的作法。

圖 30：代表團與 TNO 代表合影

(十一)　拜會 Topsector ICT

1.**時間：**9 月 30 日 （二） 17:15－17:35

2.**地點：荷蘭海牙 World Forum - Everest 2 @ 樓層 2**
（Churchillplein 10, 2517 JW Den Haag）

3.**與會人員：**

荷方	Topsector ICT ・主任 Frits Grotenhuis ・國際合作專案經理 Tijs Koops
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 台灣企業國際化協助網絡：許秀芳執行長

4.**拜會緣由：**了解 Topsector ICT 現有資安相關計畫資源，以及其國際合作模式，探詢臺灣如何加入或合作。

5.**拜會重點摘述：**

Topsector 是荷蘭政府推動的國家級策略之一，聚焦九大核心產業領域，包含水科技、農業與食品、化工、高科技系統與材料、能源、物流、創意產業、生命科學與健康及資訊與通訊科技（ICT）。而 Topsector ICT 主要任務為致力於推動人工智慧、資安、資料科學等關鍵數位技術的創新發展，並將其應用於醫療、能源、永續與安全等領域，同時強化人才培育與國際合作，帶動荷蘭的數位轉型與產業競爭力。

本次主要與 Topsector ICT Frits Grotenhuis 主任交流，其表示 Topsector ICT 也類似臺灣資安推動方向，建立專案如 Cybersecurity for the Netherlands（CS4NL），透過跨部門、跨產業與跨研究單位的公私合夥模式，專注於「系統與產業鏈韌性」（system and chain resilience）研究，尤其聚焦於能源、醫療、農業等關鍵領域。在補助政策上，推出專門扶植中小企業的競賽與補助，例如 2025 年的 SME Call，提供 400 萬歐元扶植「Cybersecurity Technologies」或「AI/Data」等優先技術研發，並強化實用研發與產業落地。強化產研

鏈結加強，企業與研究機構合作規模提升，逐漸轉為供應鏈層級的韌性安全，希望藉此擴展國際市場與出口機會。

圖 31：代表團與 Topsector ICT 代表交流

(十二)　拜會荷蘭國鐵（NS）

1.**時間**：10 月 1 日 （三） 14:00－16:30

2.**地點**：**荷蘭國鐵 Leidschendam 據點**
（Westvlietweg 4, The Hague, 2266 LA, NL）

3.**與會人員**：

荷方	荷蘭國鐵代表： ・資安執行副總裁暨資安長 Dimitri Van Zantvliet ・副資安長 Joseph Mager ・資深 OT 資安管理員與 PQC 專家 Erwin Kooi ・製造經理 Erik Ziessen
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 荷蘭在台辦事處：陳廷彥資深事務官 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：尋求臺灣資安業者與荷蘭國鐵的合作機會，並探討與荷蘭國鐵 PQC 技術交流機會。

5.**議程**：

時間	主題	主講者
14:00－14:15	代表團抵達荷蘭國鐵，前往會議室	
14:15－14:30	荷蘭國鐵致歡迎詞，雙方與會者介紹，雙方致贈禮物	NS 資安長 Dimitri Van Zantvliet 林俊秀署長
14:30－14:50	荷蘭國鐵資安作為簡介	NS 資安長 Dimitri Van Zantvliet
14:50－15:00	PQC-CIA 聯盟成果及檢測工具介紹	蕭榮興主任

時間	主題	主講者
15:00－15:30	臺灣資安解決方案簡介	資安業者（各 6 分鐘）
15:30－15:50	製造與營運管理介紹	NS 製造經理 Erik Ziessen
15:50－16:30	荷蘭國鐵作業場域介紹	（需先換鞋）
16:30	結束拜會	

6.**拜會緣由：**

荷蘭國鐵（NS）為荷蘭主要國營鐵路運營商，負責該國超過 90%的城際與地區鐵路服務。荷蘭國鐵資安長 Dimitri van Zantvliet 於今（2025）年 4 月資安大會期間來台，並參觀臺灣資安館，對臺灣業者的解決方案已有初步了解。4 月 18 日亦參加臺荷交流會議，對歐生全、來毅、匯智等方案內容已有初步認識。此次臺灣代表團回訪，持續尋求臺灣資安業者與荷蘭國鐵的合作機會，並探討與荷蘭國鐵 PQC 技術交流機會。

7.**拜會重點摘述：**

本場拜會除了讓 5 家臺灣資安業者有機會輪流向荷蘭國鐵展示資安方案，尋求合作機會外，荷蘭國鐵（NS）也由 Dimitri 分享其資安治理架構，其以鐵道 200 年歷史強調安全與風險管理的核心地位。NS 目前以「十個安全／資安領域」統整乘客安全、運務流程、軌道環境與數位系統等治理面向，並完成三輪組織調整，使資安部門提升至直接向董事會報告，與財務風險同級，反映其在關鍵基礎設施中的重要性。資源配置優先集中於「第一線運營安全與服務持續」，並透過情資、事故檢討與回饋強化整體韌性。

在供應鏈與資料治理方面，NS 過去曾遭遇重大資安事件，促使其重新審視外部依賴與脆弱點，並將事件教訓納入治理流程。近期更因北約高峰會期間多起釣魚、憑證竊取與入侵嘗試，加深其對關鍵基礎設施需具備高敏感度與復原能力的認知。NS 也強調未來將展開演算法與關鍵元件的系統化盤點與替換，在 NIS 等法規框架下，資安要求已全面融入鐵道運務規範。技術面則導入 AI 於 OT／IT 系統中，例如運用遠端監控與預測性維護協助工程團隊提前掌握狀態，並利用 AI 熱像與影像辨識技術取代部分高風險巡檢作業。

在後量子密碼（PQC）議題上，NS 雖不處理國家級最高機敏資料，但仍涉及大量一般性機敏資訊，因此將於明年啟動全面加密資產盤點，並評估替換高風險設備來源，以降低供應鏈曝險，建立更完整的可稽核加密基礎。

參訪 NS 維修基地與中控室時，團隊觀察到 NS 已透過標準作業程序與遠端監控流程整合維修運作，並採用 A－D 健康等級管理車隊。現場以 IoT 感測、機器學習影像分析與 VR/3D 技術輔助檢修與訓練，使作業逐步從依賴現場聽辨轉向數據驅動與遠端模式，提升安全性與效率。

對臺灣資安業者而言，本次拜訪旨在了解鐵道與關鍵基礎設施場域的資安需求，由於荷蘭國鐵關注 IT/OT 安全、供應鏈安全、資安事件響應等議題，臺灣廠商的解決方案包含安全合規的工控伺服器、多因子驗證、金鑰管理解決方案、微型化/PQC ready 的 HSM 等解決方案，都能對焦到荷蘭國鐵的資安需求，可持續與荷蘭國鐵安排產品實證之合作討論。

圖 32：荷蘭國鐵資安長 Dimitri van Zantvliet 歡迎代表團來訪

圖 33：代表團與荷蘭國鐵成員合影

(十三)　拜會資訊與電信主要用戶協會（BTG）

1.**時間**：10 月 2 日 （四） 14:00－15:30

2.**地點**：荷蘭海牙 HSD Campus 6F Mini Plaza
（Wilhelmina van Pruisenweg 104, 2595 AN Den Haag）

3.**與會人員**：

荷方	BTG ・商務經理 Max Vlap ・BTG 會員廠商 ・FoxCrypto 資安架構師 Sander Dorigo ・FoxCrypto 專案經理 Ivon Janssen ・Scalys 創辦人暨執行長 Hans Klos ・恩荷芬理工大學（TU Twente）助理教授 Monika Trimoska 世界創新科技與服務聯盟（WITSA） ・荷蘭分會會長 Frits Bussemaker 荷蘭內政暨王國關係部（BZK） ・量子安全加密政府計畫（QvC-NL）計畫經理 Pieter Schneider ・資安、量子運算與人工智慧專家 Mine Temurhan ・夥伴關係經理 Cecilia van der Pol
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：了解 BTG 企業會員資安需求，介紹臺灣後量子推動內容及廠商資安能量，提供雙方交流機會。

5.**議程：**

時間	主題	主講者
14:00－14:10	開場/雙方與會者介紹	林俊秀署長
14:10－14:25	BTG 及 WITSA 簡介	Frits Bussemaker 會長
14:25－15:00	臺灣資安解決方案簡介	業者各約 6 分鐘
15:00－15:25	Q&A 交流時間	
15:25－15:30	全體與會者合影	林俊秀署長代表致贈禮物

6.**拜會緣由：**

資訊與電信主要用戶協會（BTG）是荷蘭 ICT 領域重要產業公協會，擁有約 180 個會員，涵蓋政府機構、商業公司、知識機構、ICT 服務供應商及電信業者。此次交流旨在了解 BTG 企業會員的資安需求，並介紹臺灣在後量子密碼技術（PQC）方面的推動內容與資安能量，以尋求雙方具體的合作機會。BTG 協會本身高度重視並聚焦於荷蘭的數位韌性、零信任（Zero Trust）、PQC 以及物聯網安全（IoT security）等關鍵議題。BTG 會長 Petra Claessen 也積極參與荷蘭政府針對 5G、AI 和資安等政策議題的討論，凸顯了 BTG 在荷蘭數位基礎設施安全上的重要影響力。此次交流透過中華軟體公會引薦，希望增加與荷蘭 ICT 領域的廠商或 SI、資訊服務業者交流合作機會。

7.**拜會重點摘述：**

資訊與電信主要用戶協會（BTG）為世界資訊科技與服務聯盟（WITSA）的成員之一。WITSA 為一個匯聚全球約 80 至 90 個 IT 產業協會的國際組織，致力於促進全球資通訊產業的合作與政策交流。當日由 WITSA 荷蘭分會會長 Frits Bussemaker 代表 BTG，與署長一起開場，並代表 BTG 進行簡介，說明其主要職責為代表荷蘭參與 WITSA，並為 BTG 會員建立全球性的對話與合作平台。Frits 會長指出，BTG 的工作除了匯集國際組織間的對話，並在荷蘭政府層級倡議對新興數位技術的關注。

Frits 特別提到臺灣曾主辦 WITSA 首屆 AI 峰會，討論了全球層面的 AI 政策決策與安全維護。本次交流活動被定調為 BTG 與 WITSA 的共同活動，強調透過這個全球性的 IT 產業網絡，臺灣資安業者能夠與荷蘭主要 ICT/電信業者建立更廣泛聯繫的可能性。此外，BTG 會員多來自金融、交通、能源等關鍵基礎設施產業，其資安需求與挑戰為本次討論的主要議題。當日臺灣的 5 家資安業者分別簡介自身技術與產品，分享臺灣在關鍵基礎設施資安防護的應用經驗。雙方並就產業現況與資安挑戰交換意見，BTG 亦簡介其會員對資安解決方案的關注方向。此次交流有助於瞭解荷方產業的實際需求，並為未來雙邊在數位技術與資安議題上的持續對話奠定基礎。

圖 34：林俊秀署長於活動開始致歡迎詞

圖 35：Frits Bussemaker 會長代表簡介 BTG 及 WITSA

圖 36：代表團與所有與會交流貴賓合影

(十四)　臺荷資安交流媒合會

1.**時間**：10 月 2 日 （四） 10:00－13:00

2.**地點**：荷蘭海牙 HSD Campus 6F Mini Plaza
（Wilhelmina van Pruisenweg 104, 2595 AN Den Haag）

3.**與會人員**：

荷方	・荷蘭代理商 Sinteg ・資安科技公司 MODAT ・區塊鏈新創公司 DigiCorp Labs ・半導體與 AI/IoT 技術分銷公司 Macnica ATD Europe（ASUS 合作夥伴，主要市場在法國與日本） ・雲端通訊解決方案供應商 Talksome ・華碩 ASUS AIoT ・協助中小企業國際拓銷的顧問公司 BZB Europe ・AI 威脅防禦技術新創公司 DeepCytes Lab
臺方	數位發展部數位產業署
	後量子資安產業聯盟：李維斌召集人 工研院：黃維中副所長、邱苑慈、林宜萱 資策會：蕭榮興主任 資安業者：5 家資安業者，共 8 位 台灣企業國際化協助網絡：許秀芳執行長

4.**主題**：臺灣資安業者與荷蘭當地系統整合商之交流媒合商談。

5.**議程**：

時間	主題	主講者
09:30－10:00	來賓報到	
10:00－10:02	開場	主持人
10:02－10:05	敬邀署長致歡迎詞	林俊秀署長
10:05－10:10	全體合影	
10:10－12:10	媒合活動（最多交流 5 輪，每場 15 分鐘）	5 張桌（每家 1 張）

時間	主題	主講者
12:10－13:00	午餐自由交流（備輕食及飲料）	

6.**活動辦理緣由：**希望透過臺荷雙方交流媒合洽談，促進雙方探索技術整合、通路合作與商機拓展的可能性，強化雙方跨境合作基礎。

7.**活動重點摘述：**

為協助參與業者有更多機會與當地系統整合商或代理商等媒合對談，而安排本次活動，除了透過當地合作夥邀請及宣傳，本場活動也被列入海牙資安週的系列活動之一，因此當天除了原先邀請的貴賓，也吸引其他感興趣的貴賓前來參加。彙整廠商回饋意見如下：

歐生全表示，本次媒合會促成多場具潛力的洽談，特別是與 Macnica（日本／法國）及 Sinteg（荷蘭/北非）等代理商與系統整合商的互動，雙方在產品與市場面向上具高度互補性，被視為極具合作潛力的夥伴

來毅科技表示，本次媒合會安排精準、效率高，成功協助公司建立多項初步商業連結，媒合成果具延續性，未來將以概念驗證（PoC）專案形式，持續深化與潛在夥伴的合作，包括 Macnica、ASUS、Sinteg、Deepcytes（英國）與 Talksome（荷蘭）等，展現明確的後續合作意向。

匯智安全表示，荷蘭 ICTU 團隊對公司產品在無人機安全應用上的潛力表達高度興趣，雙方規劃後續線上會議以討論技術合作細節。Sinteg 則看好公司全系列 HSM（硬體安全模組）產品的應用潛力，並有意協助推進非洲市場，目前雙方透過電子郵件持續交流。同時，荷蘭資安通路商 BZB Europe 亦表達協助拓展當地業務之意願，雙方正討論具體推廣策略。

全景軟體表示，與 Sinteg 的會談氣氛良好，對方對公司產品表達高度興趣，雙方建立直接聯繫管道，並有意就具體應用場景進行後續接洽。

東擎科技則表示會後將另與 DigiCorp Labs（荷蘭）、ICTU 及 DeepCytes 安排後續會議，以延續媒合成果並探索進一步合作機會。

總括而言，廠商回饋意見顯示本次媒合會有助於臺灣資安廠商接軌歐洲市場，開啟更多具潛力的合作對話，已為未來商機拓展奠定良好基礎。

圖 37：D 桌東擎（左）、B 桌歐生全（右）媒合剪影

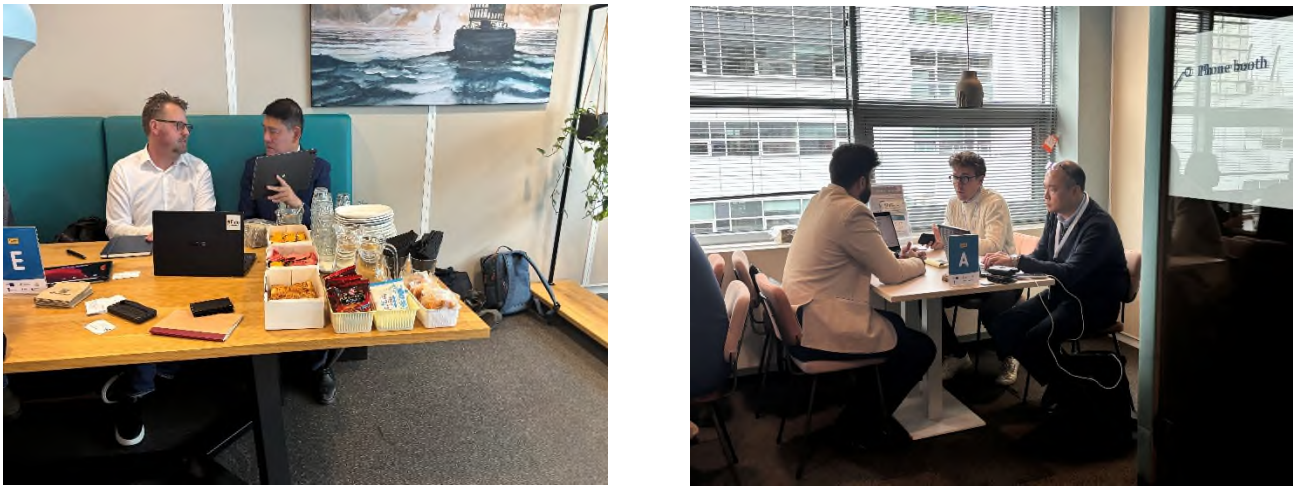


圖 38：E 桌全景（左）、A 桌來毅（右）媒合剪影

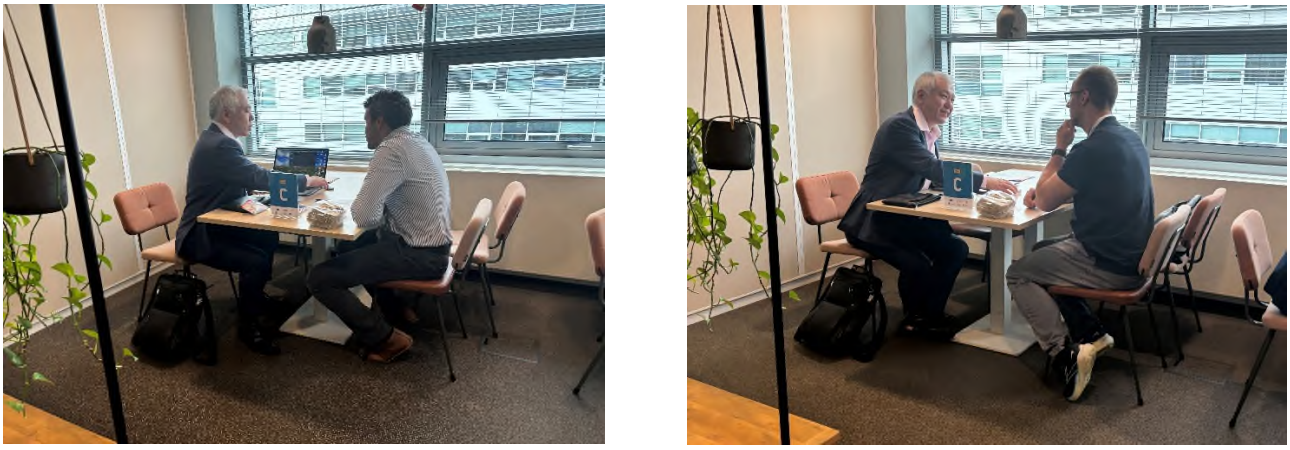


圖 39：C 桌匯智安全媒合剪影

圖 40：代表團與荷方業者於臺荷資安交流媒合會合影

伍、 心得與建議

本次赴荷蘭的資安代表團，確實達成臺灣資安產業實踐「強化臺荷資安合作、拓展國際市場通路」的核心目標。透過參與歐洲指標性的「海牙資安週」及相關交流活動，臺灣團隊成功展示自身的資安技術能力，並增進國際交流，特別是在開幕式的 Delegations Leaders Pitch 活動中，臺灣作為首個受邀分享的國家，向各訪團展示具資安韌性供應鏈、後量子密碼（PQC）、工控資安（OT）及零信任架構等領域的技術實力。這為臺灣資安解決方案在推廣歐洲市場奠定堅實基礎。

在官方交流層面，團隊在荷期間拜會荷蘭企業署（RVO）、荷蘭國家資安中心（NCC-NL）及海牙市政府等進行對話，其中海牙市政府對後量子資安（PQC）議題表達明確的合作興趣，更重要的是，荷蘭官方單位提醒臺灣廠商必須及早關注已通過生效的歐盟《網路韌性法案》（CRA），該法案將對所有出口至歐盟的「含數位元件產品」產生強制性的法遵要求與漏洞通報義務，成為臺灣資通訊產品銷歐的關鍵門檻，此訊息有助於讓臺灣廠商提前調整產品策略。此外，在當前國際地緣政治變化下，駐荷蘭台北代表處亦指出，臺灣應把握傳統競爭對手（如以色列）受限的契機，強化在歐洲市場的品牌能見度與合作布局。

在研究與前瞻技術領域部分，此次與荷蘭應用科學研究機構（TNO）深入聚焦於 PQC 遷移策略，雙方就 PQC 遷移指引、導入實證策略以及密碼學敏捷性（crypto agility）的推動方式進行了技術交流。TNO 亦對我國「後量子資安產業聯盟（PQC-CIA）」採取的公私協力模式表示關注與肯定。PQC-CIA 於 ONE Conference 大會期間，透過專題演講分享我國以公私協力模式加速 PQC 應用部署的推動經驗，獲得正面迴響，顯示臺灣在推動前瞻技術應用的模式具有參考價值。

本次行程為臺灣業者帶來了實質的商業合作機會。在關鍵基礎設施領域拜會荷蘭國鐵（NS），介紹臺灣廠商的解決方案，如符合標準的工控伺服器（東擎）、PQC-ready 硬體安全模組（匯智）以及多因子驗證方案，能夠精準對應荷蘭國鐵在 IT/OT 安全與供應鏈脆弱性方面的迫切需求。此外，透過與 ESET 等歐洲主要資安供應商及 Macnica、Sinteg 等系統整合商的會面，為臺灣廠商開拓更廣的歐洲（包括荷蘭、法國、英國等）通路與合作夥伴關係，參與廠商在活動後已展開後續追蹤與洽談，為實質商機奠定了基礎。

本署今年再次帶領廠商參與海牙資安週與 ONE Conference。儘管 ONE Conference 本質上並非商業媒合活動，但其在荷蘭資安生態系中的地位極為關鍵，亦為荷蘭政府、產業界、研究機構及多國代表匯聚的重要交流場域。此行顯示，本次代表團成功深化雙方的信任關係，在此平台上仍能有效鏈結歐洲生態系，並協助我國業者於荷蘭落地或拓展合作。因此，建議仍可持續參與相關活動，以延續既有互動成果並深化國際夥伴關係，後續的深化合作與戰略佈局至關重要，以下幾點作為未來參考：

1.強化官方支持與在地化落地：積極透過荷蘭官方單位及荷蘭在台辦事處，為臺灣資安廠商提供更具體且在地化的法規、投資與拓銷支持，將能加速臺灣廠商融入歐洲生態系。另可持續與海牙市政府就資安社群活動進行交流，關注明年「Hack The Hague」的辦理情形，並推動臺灣優質團隊參賽交流。與駐荷蘭台北代表處交流時提及未來可邀請荷蘭外交部資安特使來臺，參加 CYBERSEC 臺灣資安大會等國際會議，以強化政府層級對話。

2.技術合作由策略分享轉向聯合實證：此次在許多官方拜會及產業交流的過程中，屢次提及後量子密碼（PQC）相關議題，在與 TNO 的交流中已在 PQC 遷移策略有初步共識，未來可將合作重點從單純的策略分享，提升至聯合專案合作。如雙方可共同爭取 ITEA 專案，以 PQC 業者在數位信任上的案例內容進行實證，從而共同確立技術標準與應用典範。同時，未來應持續關注歐盟 CRA 的具體標準與通報義務，並加強推動臺灣物聯網設備資安標準與歐盟標準的對接。

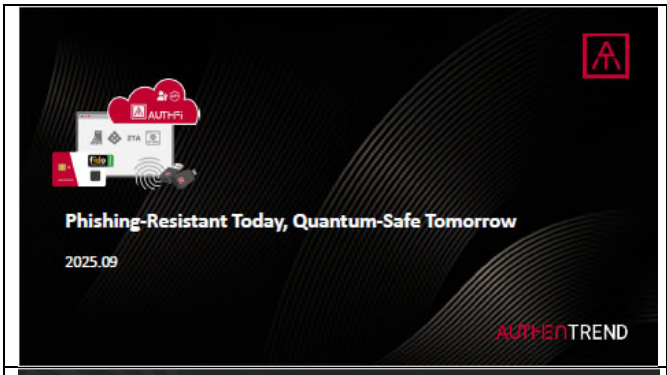
3.市場策略轉向產業整合性解決方案：參團業者普遍反映，未來市場對資安產品的需求將從單一產品轉向針對特定產業的整合性解決方案。鑑於 BTG（大型 ICT 與電信用戶協會）成員（如金融、交通、能源）表明對 OT 安全和關鍵基礎設施防護的迫切需求，建議未來可引導臺灣資安業者開發整合性資安解決方案，以滿足歐洲大型客戶對完整、高韌性防護體系的需求。因此，在未來的媒合活動中，應強化雙邊對話與需求分享，從而提升合作的精準度與最終的實質成效。

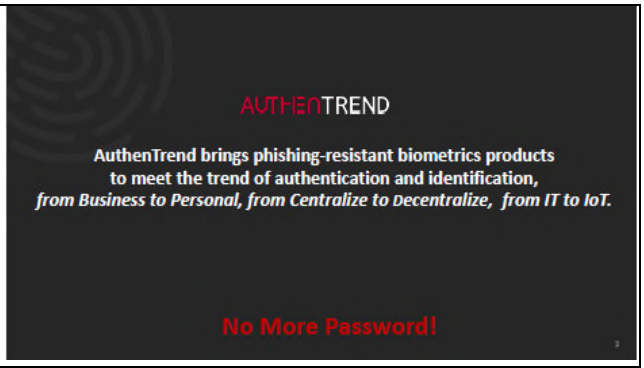
附件：參與資安拓銷之廠商簡報

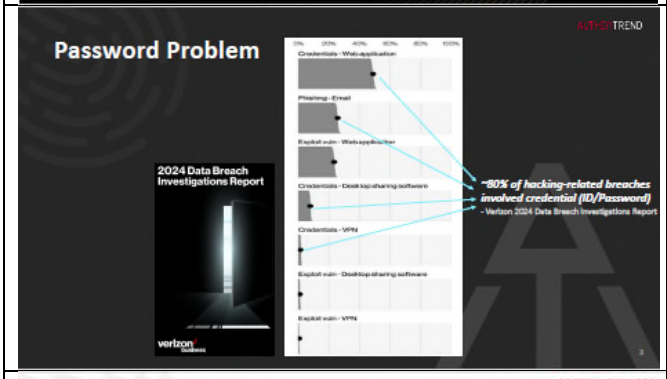
1．東擎科技


ASRock
Industrial
COCREATE AN INTELLIGENT WORLD
Thank You!

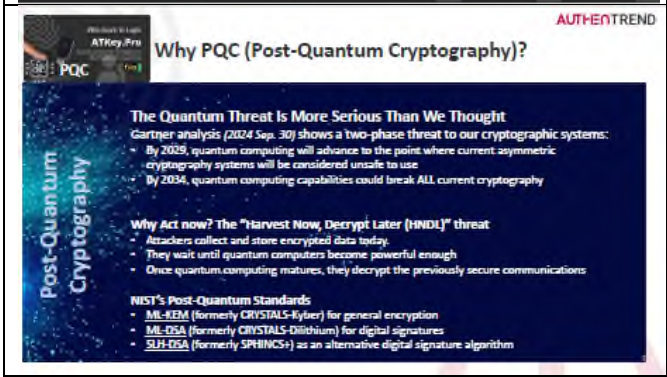
2．歐生全創新

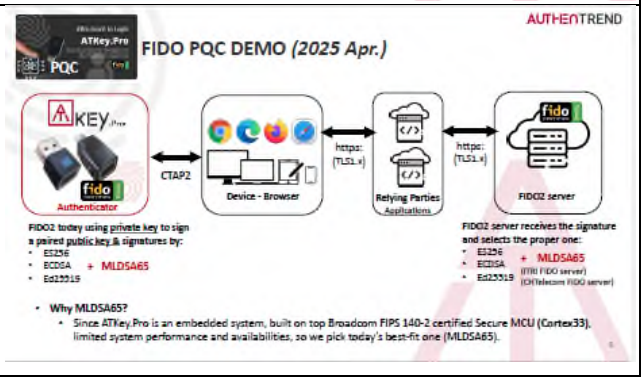

AUTHFi
Phishing-Resistant Today, Quantum-Safe Tomorrow
2025.09
AUTHENTREND

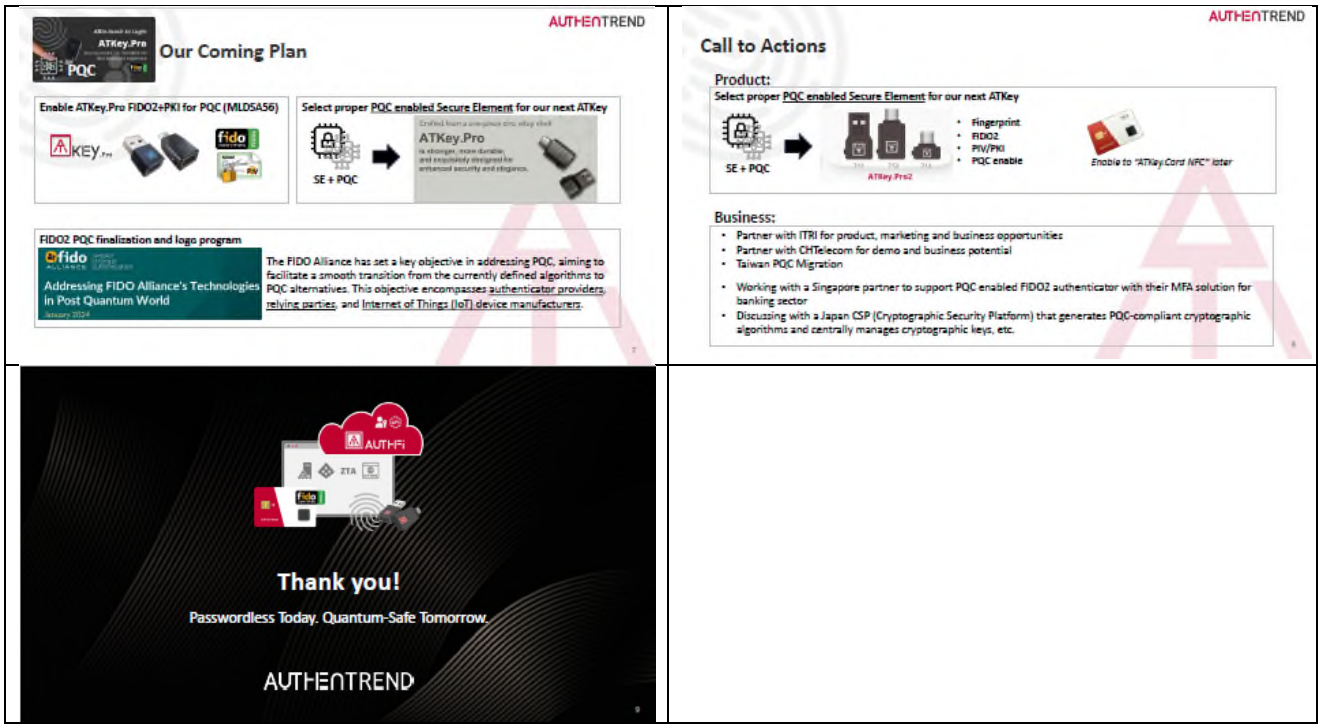

AUTHENTREND
AuthenTrend brings phishing-resistant biometrics products
to meet the trend of authentication and identification,
from Business to Personal, from Centralize to Decentralize, from IT to IoT.
No More Password!


Password Problem
2024 Data Breach
Investigations Report
verizon
~80% of hacking-related breaches
involved credential (ID/Password)
- Verizon 2024 Data Breach Investigations Report


AUTHENTREND
Why Password Issue Always?
Password is "Share-secret",
no matter Server, Client or
transmission, all with the risks
being hacked (Phishing, man-in-the-
middle, server attack, ...)
Phishing
Hackers Don't Hack,
They Log In
An estimated 3.4 billion phishing emails a day
are sent by cyber criminals


ATKey.Pro
PQC
AUTHENTREND
Why PQC (Post-Quantum Cryptography)?
Post-Quantum Cryptography
The Quantum Threat Is More Serious Than We Thought
Gartner analysis (2024 Sep. 30) shows a two-phase threat to our cryptographic systems:
By 2029, quantum computing will advance to the point where current asymmetric cryptography systems will be considered unsafe to use
By 2034, quantum computing capabilities could break ALL current cryptography
Why Act now? The "Harvest Now, Decrypt Later (HNDL)" threat
Attackers collect and store encrypted data today.
They wait until quantum computers become powerful enough
Once quantum computing matures, they decrypt the previously secure communications
NIST's Post-Quantum Standards
ML-KEM (formerly CRYSTALS-Kyber) for general encryption
ML-DSA (formerly CRYSTALS-Dilithium) for digital signatures
SLH-DSA (formerly SPHINCS+) as an alternative digital signature algorithm


ATKey.Pro
PQC
AUTHENTREND
FIDO PQC DEMO (2025 Apr.)
Authenticator
CTAP2
Device - Browser
https:
(TLS1.x)
Relying Parties
Applications
https:
(TLS1.x)
FIDO2 server
FIDO2 today using private key to sign
a paired public key & signatures by:
ES256
ECDSA + MLDSA65
Ed25519
FIDO2 server receives the signature
and selects the proper one:
ES256
ECDSA + MLDSA65
Ed25519
(ITRI FIDO server)
(CHTelecom FIDO server)
Why MLDSA65?
Since ATKey.Pro is an embedded system, built on top Broadcom FIPS 140-2 certified Secure MCU (Cortex33), limited system performance and availabilities, so we pick today's best-fit one (MLDSA65).


AUTHENTREND
Our Coming Plan
Enable ATKey.Pro FIDO2+PKI for PQC (MLDSA56)
Select proper PQC enabled Secure Element for our next ATKey
SE + PQC
ATKey.Pro
FIDO2 PQC finalization and logo program
Addressing FIDO Alliance's Technologies in Post Quantum World
The FIDO Alliance has set a key objective in addressing PQC, aiming to facilitate a smooth transition from the currently defined algorithms to PQC alternatives. This objective encompasses authenticator providers, relying parties, and Internet of Things (IoT) device manufacturers.
AUTHENTREND
Call to Actions
Product:
Select proper PQC enabled Secure Element for our next ATKey
SE + PQC
Fingerprint
FIDO2
PIV/PKI
PQC enable
Enable to "ATKey.Card NFC" later
Business:
Partner with ITRI for product, marketing and business opportunities
Partner with CHTelecom for demo and business potential
Taiwan PQC Migration
Working with a Singapore partner to support PQC enabled FIDO2 authenticator with their MFA solution for banking sector
Discussing with a Japan CSP (Cryptographic Security Platform) that generates PQC-compliant cryptographic algorithms and centrally manages cryptographic keys, etc.
Thank you!
Passwordless Today. Quantum-Safe Tomorrow.
AUTHENTREND

3．全景軟體


CHANGING
TPEX:8272
CHANGING Briefing
Profile
Founded in 1998, a member of the Wistron Group
Deeply engaged in cybersecurity and authentication technologies
Employee : 180
Headquarters : Hsinchu, Taiwan
Office : Taipei, Taiwan
Core Value
Verification of People, Will, and Things
Certified Solution, Continuous Innovation
Taiwan National Information of Cyber Security (NICS) ZTA User / Device certified
Authentication solutions with FIDO and OATH certifications
Taiwan Ministry of Digital Affairs (moda) Electronic Signature solution registration
ISO 27001 certification
Customer involves Banks, Securities, Insurance, Government, Healthcare, Defense, and Enterprise
1000+ Customers

We focus on Verification of People, Will, and Things

Authentication

Seamless protection of critical resources, from OTP, MFA, FIDO to ZTA

Digital Transformation

Integrating AI-OCR and image processing technologies to achieve end-to-end document lifecycle management

Solutions

Cybersecurity

Compliance with financial and government regulations, delivering high-level cybersecurity service

IoT Security

Driving IoT development by integrating trust, certificate management, and ecosystem connectivity

Secure Authentication

Authentication

- IDExpert MFA Solutions
  OTP / FIDO / PKI
- CGFIDO FIDO Solutions
  UAF / FIDO2 / Passkey
- CGTrust ZTA Solutions
  800-207 / ZTMM
  FIDO(User) / TPM(Device)
  Risk Detect and Blocking

IDEXPERT / CGFIDO / CGTrust

Tech / FinTech Cybersecurity

Cybersecurity

- FXML Net-Bank Transactions Security Solution
- Financial Fast-ID Solution
- eKYC Solution
- Stock Place an Order Security Solution
- Mobile PKI Solution.
- Classic / PQC Key Management System
- Data / Privacy Protection System
- HSM Application Gateway System

Digital Transform Application

Digital Transformation

Electronic Signature

eSigning a contract, e-form, and receipt reduces time and improves the audit trail and security.

- FastSIGN
- EazySIGN

AI-OCR

Using AI to improve OCR, from ID recognition to Document information retrieval. It can be the foundation of eKYC and speed up the online application procedure.

- FastID
- FastDOC

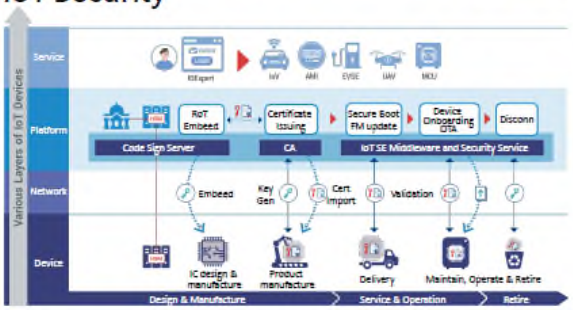
Image MGT System

Long-time archiving and protecting enterprise digitalized documents. An authorized user can retrieve anytime and keep the audit trail.

- DIMS (Digital Image MGT Sys)
- CIS (Clinical Information Sys)

IoT Security

IoT Security



Future Strategy

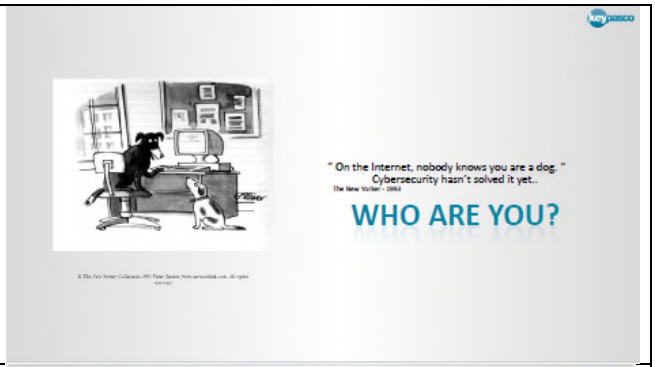
- Passkey replaces Password
- Solution to Cloud and SaaS
- PQC Migration
- IoT secuirty with compliance

CHANGING

THANK YOU

4．來毅數位科技

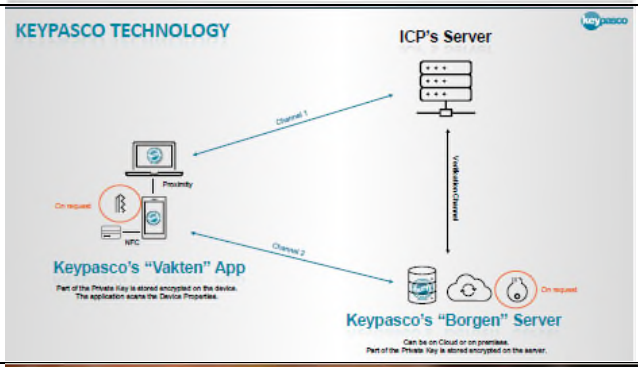

Keypasco
Your DeviceID as unique as your DNA
2025-10-02 Den Haag, Netherlands
Fabio Bordignon , fabio.bordignon@keypasco.com
Chengi Lin, chengi@iydsec.com


" On the Internet, nobody knows you are a dog. "
Cybersecurity hasn't solved it yet..
WHO ARE YOU?

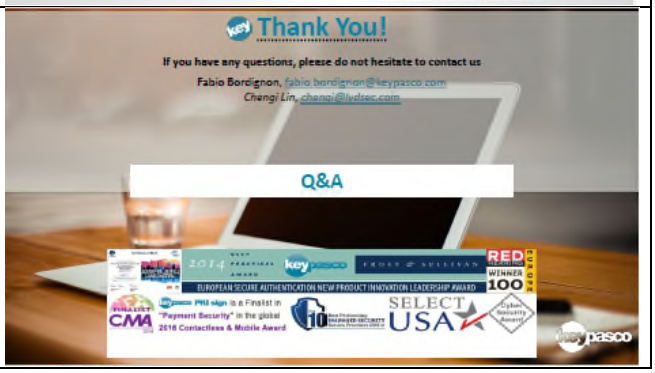

Password Software Cert
OTP Tokens
OTP Apps
USB Key, PKI
SMS OTP
FIDO2, UAF
Phishing
VNC
MiTM
ARE EVOLVING
MiTB
SMS Hijacking
??????


CHALLENGES OF CURRENT SOLUTION
In last 40 years, technology shifts and diversifying online services are escalating, as well the cost of Cybersecurity breaches.
RISK
The attack fronts are multi-dimensional; Threats are evolving; Fraud cost are escalating
HOW CAN WE STOP THIS EVIL-SPIRAL?


Non-Distributed Credentials
DeviceID
2 Channels Structure
Risk Engine
Partial Key
Proximity & NFC Features
Sign What You See

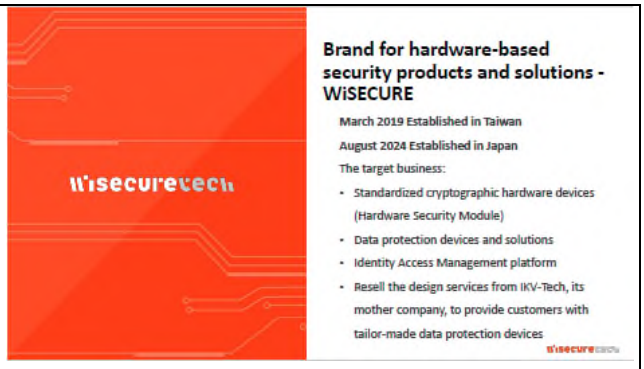

KEYPASCO TECHNOLOGY
ICP's Server
Keypasco's "Vakten" App
Keypasco's "Borgen" Server

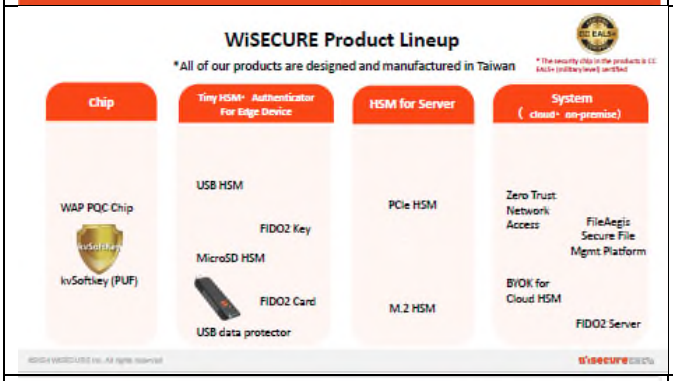

fido alliance


Thank You!
If you have any questions, please do not hesitate to contact us
Fabio Bordignon, fabio.bordignon@keypasco.com
Chengi Lin, chengi@iydsec.com
Q&A

5．匯智安全科技

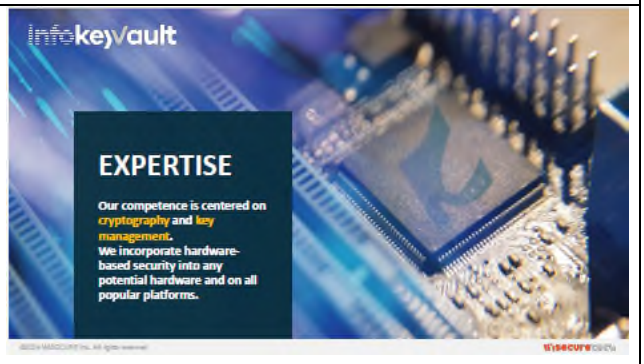

About WiSECURE
Security wisely empowered
wisecuretech

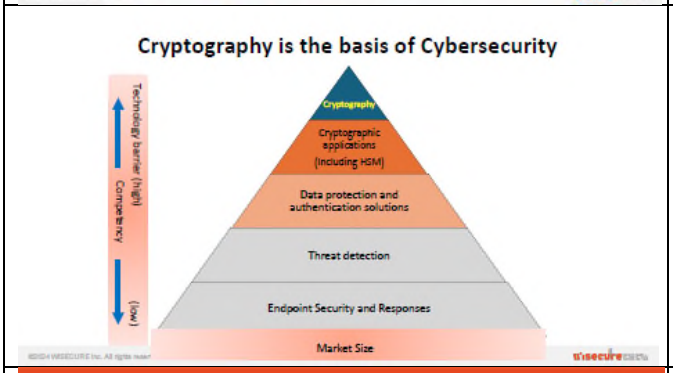

wisecuretech
Brand for hardware-based security products and solutions - WiSECURE
March 2019 Established in Taiwan
August 2024 Established in Japan
The target business:
Standardized cryptographic hardware devices (Hardware Security Module)
Data protection devices and solutions
Identity Access Management platform
Resell the design services from IKV-Tech, its mother company, to provide customers with tailor-made data protection devices


WiSECURE Product Lineup
*All of our products are designed and manufactured in Taiwan
Chip
WAP PQC Chip
kvSoftkey (PUF)
Tiny HSM・Authenticator For Edge Device
USB HSM
FIDO2 Key
MicroSD HSM
FIDO2 Card
USB data protector
HSM for Server
PCIe HSM
M.2 HSM
System (cloud・on-premise)
Zero Trust Network Access
FileAegis Secure File Mgmt Platform
BYOK for Cloud HSM
FIDO2 Server

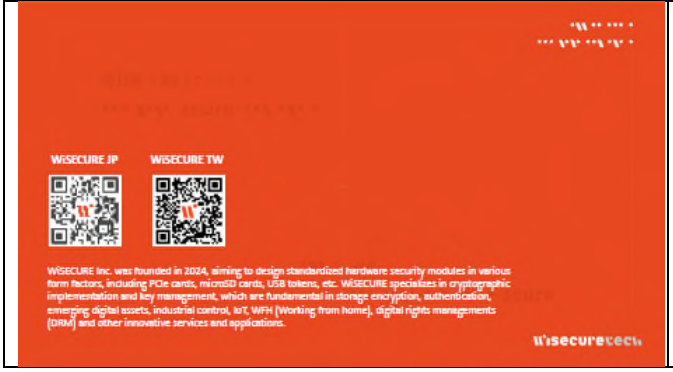

We are a Google Global Partner
Client-Side Encryption (CSE) using our USB HSMs
Google Workspace
The Solution for Data Sovereignty!


WiSECURE is 100% Subsidiary of ...
Trust
Secure
Relief
infokeyvault
We are a Data Security company providing reliable hardware products and designs for:
Military,
Taiwan government,
Aerospace vehicle communication,
Device vendors, and
Enterprise


infokeyvault
EXPERTISE
Our competence is centered on cryptography and key management.
We incorporate hardware-based security into any potential hardware and on all popular platforms.


Cryptography is the basis of Cybersecurity
Technology barrier (high)
Complexity
(low)
Cryptography
Cryptographic applications (including HSM)
Data protection and authentication solutions
Threat detection
Endpoint Security and Responses
Market Size


WAP PQC Secure Processor
The world's first groundbreaking PQC chip!
Submitting FIPS 140-3 CAVP CMVP (Level 3)


WiSECURE JP
WiSECURE TW
WiSECURE Inc. was founded in 2024, aiming to design standardized hardware security modules in various form factors, including PCIe cards, microSD cards, USB tokens, etc. WiSECURE specializes in cryptographic implementation and key management, which are fundamental in storage encryption, authentication, emerging digital assets, industrial control, IoT, WFH (Working from home), digital rights managements (DRM) and other innovative services and applications.
wisecuretech