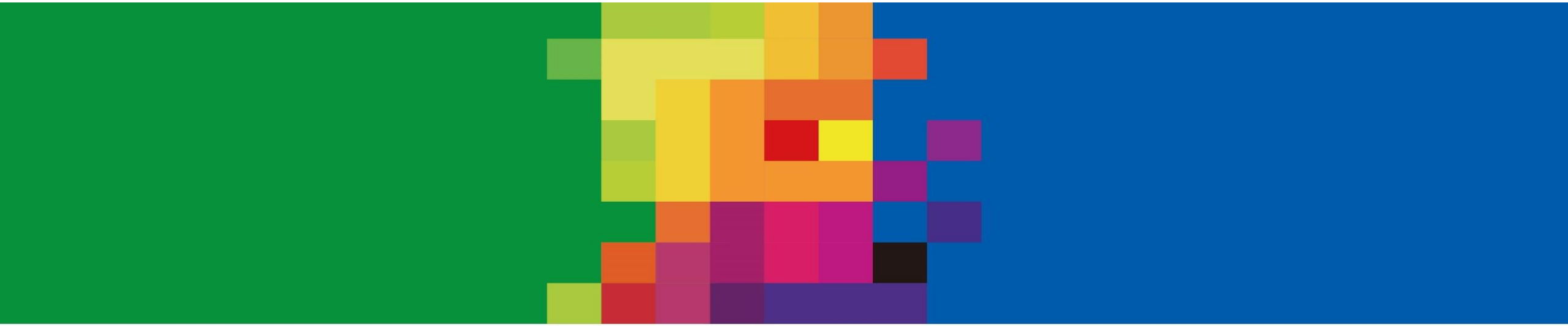
TLS憑證效期縮短：
券商內部因應挑戰與自動化之路

臺灣網路認證股份有限公司(TWCA)
CA研發處 蔡家宏處長



TWCA 臺灣網路認證

TWID 身分識別中心

客戶市場

- 保險
- 證券 期貨
- 銀行
- 投信 投顧
- 電信
- 政府
- 電商 電支
- 新創

TWID 身分識別中心

服務藍圖

參與國際組織

CA/BROWSER FORUM

fido ALLIANCE

Adobe

TWID 服務

1 多元身分識別

提供多種身分識別工具來證明客戶身分

2 信物管理

依據身分識別，提供不同等級的信物(如 SSL/TLS)

3 電子簽署

透過信物對內容進行電子簽章，行使用戶對內容的意思表示之確認

4 資料共享

提供授權擷取或申請交付兩種資料取得方案

身分核驗夥伴

◆ 網站身分識別

- 加入國際 Root Program，具備多元發證能力
- 目前 **SSL 相關憑證發行量逾 32,000 張**，展現市場採用與服務可靠度
- 國際設備廠商合作，如 QNAP
- **2025 年 3 月**，協助政府單位導入網站憑證，強化政府網站的 **資安防護與數位韌性**。

SSL 憑證 ： 3.2 萬
金融憑證 ： 2,300 萬

Mobile ID：3,000 萬

中華電信　台灣大哥大　遠傳

票交所： 28 家銀行晶片卡
eDDA 26 家網銀帳密

TLS 也有分級？

- 在提到分級之前，我們先來談談核發 TLS 憑證前的兩大驗證：
  - **組織驗證**：確認申請者所在組織合法存在
  - **網域驗證**：確認申請者可以控制該網域
    - HTTP 驗證
    - DNS 驗證
  - 都是 Challenge-Response 概念的驗證方式
    - CA 隨機產生 token，申請者將 token 放到指定地方供 CA 驗證
    - 放在該站台下，稱之為 HTTP 驗證
    - 產生一筆DNS record (TXT) 放置 token，稱之為 DNS 驗證

TLS 也有分級？

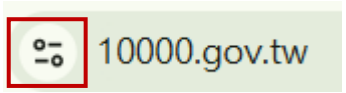
- TLS 憑證依照其驗證強度

憑證級別	驗證	適合情境
DV (Domain Validation)	需要過網域驗證	個人站台
OV(Organization Validation)	需要通過組織驗證及網域驗證	一般企業
EV (Extended Validation)	需要通過組織驗證及網域驗證 (組織驗證有更嚴格審查要求， 例如司法管轄權所在地)	金融產業

- **DV 憑證即表示憑證僅經過網域驗證即簽發，為信賴等級最低之憑證，被釣魚網站大量使用**
- **OV 及 EV 憑證需要經過組織驗證，合法之組織才可簽發，也提供企業信譽之保障**

TLS 也有分級？

- 正版
  - https://10000.gov.tw
- 盜版
  - https://10000gov.vip
  - https://10.000gov.tw
  - …



憑證檢視者：10000.gov.tw

一般(G) 詳細資訊(D)

核發對象

一般名稱 (CN)	10000.gov.tw
組織 (O)	政府機關-財政部國庫署
組織單位 (OU)	<不是憑證的一部分>

發行者

一般名稱 (CN)	TWCA Secure SSL Certification Authority
組織 (O)	TAIWAN-CA
組織單位 (OU)	<不是憑證的一部分>

有效期間

發行日期	2025年9月16日 星期二 上午10:54:27
到期日	2026年9月16日 星期三 晚上11:59:59

SHA-256 指紋

憑證	e3e1b2a46542992b07c88c7c19575542ca11ae0fe64a079399bd839c2150cfd9
公開金鑰	59a1b328d606933ac4ab80165f03b9360d32d06859244b83efc702457f32d1e1

什麼是 CA/Browser Forum (CABF)

- 是一個由 CA 和瀏覽器共同組成的行業組織，負責制定**公共憑證**的相關規範，這些規範稱之為 Baseline Requirement (BR)，包含：
  - TLS 憑證
  - S/MIME 憑證
  - CodeSign 憑證

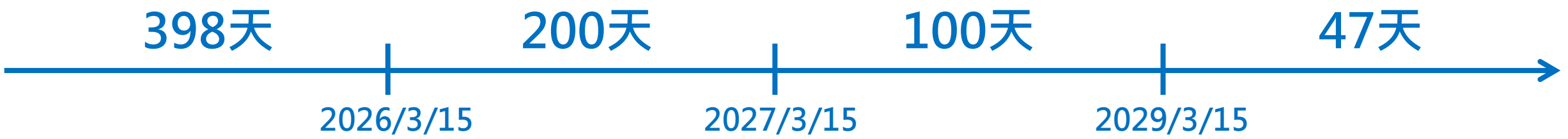
- 所有 CABF 規範條文的制定與異動都需要經過組織成員投票表決
  - TWCA 也是成員之一，過去也參與了許多重要的議案投票

- CA 必須嚴格遵守 CABF 所制定的 BR，若有違反之情事，輕則憑證限期廢止(5 日內)，重則 CA 被瀏覽器移除信任

- 除了 CABF 制定的 BR 規範外，各瀏覽器也會制訂更嚴格的規範，若有違反之情事，瀏覽器可以單方面移除信任
  - Chrome、Mozilla、Apple、Microsoft

TLS 憑證效期縮短期程

- 2025/4/12 CABF 投票通過，TLS 憑證效期將逐年縮短
  - 基於安全因素 (**金鑰破解風險、憑證廢止空窗期、PQC 密碼敏捷性議題**)
  - **已經是決議，不可逆，必定會施行**



- 過去憑證效期為一年，未來將逐年縮短最終至 47 天
- 人工產製金鑰、上傳 CSR 、手動佈署憑證，負擔將會倍增

→ 盡早導入憑證自動化解決方案，使用支援 ACME 自動化協議之 CA

自動化協定或標準的選擇

- 由於目標是自動化，勢必需要將原來人工作業轉化為 AP 作業
  - 透過 ACME 憑證自動化協議
    - RFC 8555 國際標準
    - 為了 TLS 憑證而訂定
    - 廣泛被全球 CA 採用
  - 其他憑證相關標準
    - SCEP、CMP、EST 等較早期的協定
    - 並不是為了 TLS 憑證所量身打造
    - 部分 CA 有支援
  - 透過 CA 自行開發 API
    - 客戶需要單獨與 CA 整合
    - CA 可以提供 ACME 無法支援之功能

目前導入首選會是 ACME

什麼是 ACME？為什麼選擇 ACME？

- Automatic Certificate Management Environment – 自動化憑證管理協定
  - 旨在解決憑證自動化申請、網域驗證、續期。
  - 國際標準：RFC 8555 (2019/3)。
    - RFC 8657、RFC 9773
  - 目前已經廣泛被主流 CA 採用。
    - Chrome 要求所有 CA 要支援。

- ACME 特色
  - 標準的 Client –Server 架構。
  - 用戶透過 Agent (client) 向 CA (server) 申請憑證。
    - Agent 實作 ACME 協定，例如 Certbot、acme.sh、Lego、Posh-ACME、simple-ACME、自行實作…
    - CA 實作 ACME 協定，例如 TWCA 。
  - 金鑰產製、CSR 產製、網域驗證等作業均涵蓋於 ACME 協定範疇。
  - 支援 HTTP 以及 DNS 網域驗證方式。
  - 安全機制：Agent 產生並註冊非對稱金鑰，針對交易訊息做簽章達到身分識別。

ACME 可以做到哪些自動化？

憑證申請流程	未導入自動化前	是否可以透過 ACME 完成？
產製金鑰	使用工具產生 (例如 OpenSSL)	自動化，內含在 ACME 協定中
產製 CSR	使用工具產生 (例如 OpenSSL)	自動化，內含在 ACME 協定中
上傳 CSR	將 CSR 貼入 CA 提供之窗口 (或使用選擇檔案方式上傳)	自動化，內含在 ACME 協定中
組織驗證	由 CA 自行完成，自動為主，必要時人工	由 CA 自行完成，不包含在 ACME 協定中
網域驗證	HTTP、DNS、EMAIL、甚至電話驗證，透過人工方式放置 token	自動化，內含在 ACME 協定中 (僅支援 HTTP 及 DNS 驗證，自動化放置 token)
核發憑證	CA 核發憑證後將憑證檔案寄給用戶	自動化，內含在 ACME 協定中
憑證佈署	用戶自行取得憑證檔案，依照不同 web server 進行憑證佈署	由用戶端 Agent 或其他方式完成，不包含在 ACME 協定中

自動化的關鍵

- 完整自動化解決方案必須包含 **自動化憑證申請 + 自動化憑證佈署**
  - ACME 幾乎已經可以做到大部分的自動化作業，唯獨憑證佈署
  - 券商導入自動化方案的關鍵在於 **自動化憑證佈署**

若僅能自動化申請憑證，只做了一半 !!

怎麼做到憑證自動續期的呢？

- 在過去，憑證即將到期前會通知用戶，用戶再自行產製金鑰、上傳CSR、取得憑證並安裝

- 導入 ACME 自動化解決方案後，大部分 Agent 都具備自動續期功能
  - 原理就是有一個排程定期檢查憑證是否即將到期，若即將到期就主動執行自動申請

- 憑證續期作業不再需要人為介入
  - 但是也要有其他機制來降低排程未執行的風險

主流的自動化解決方案

- Agent Base 解決方案
  - 每台[註1]憑證主機安裝 Agent，例如使用 Certbot 或是 TWCA 提供之 MSSLAgent[註2]
  - 主要透過腳本方式支援基本的憑證佈署功能
  - 適合環境單純的中小企業

- 專門的 CLM 平台
  - KeyFactor、Venafi (CyberArk)、appviewX 或各大 CA 自行開發等
  - 有 Agent Base (每台憑證主機安裝 agent) 也有集中式管理 (地端安裝專用主機)
  - 針對不同主機或設備的憑證佈署支援度較高
  - 提供管理介面供管理人員對所有憑證主機進行操作
  - 費用較為高昂，適合環境複雜的大型企業

- 客戶自行開發
  - 透過 Agent 完成自動化申請憑證
  - 自動化佈署透過自行開發或整合 (例如透過 Ansible)
  - 可依企業內部實際情況做功能調整
  - 適合自主掌握程度或具有開發能力的企業

[註1]是否每台憑證主機都要安裝 Agent 視環境以及驗證方法決定
[註2]由 TWCA 基於 Certbot 專案，修正其原始碼弱點所包裝的 Agent 軟體

券商可能會面臨的困難

- 憑證申請程序的轉變
  - 現況申請憑證透過人工行政程序 (例如需要公文簽核)

- 資安考量
  - 資安政策不允許在憑證主機安裝 Agent
  - 憑證主機無法對外，或是讓外部連入
  - 無法自動化進行網域驗證 (HTTP 或 DNS 驗證放置 token)
    - Agent 或 CLM 平台權限不足
  - CLM 平台無法佈署憑證至各憑證主機

- 憑證綁定
  - 礙於國內法規要求，行動 APP 需要綁定 TLS 憑證
  - 憑證效期縮短將會導致 APP 頻繁換版
  - 國際趨勢已經不建議這樣做，也有一些替代方案與建議[註1] [註2]

- 盤點困難
  - 組織內部現況有多少站台使用憑證無法統一盤點
    - 分屬不同單位
    - 同時向多間 CA 申請憑證

[註1] https://www.digicert.com/blog/certificate-pinning-what-is-certificate-pinning
[註2] https://blog.cloudflare.com/why-certificate-pinning-is-outdated/

針對券商的建議：

即刻起就要開始進行內部評估！

- 憑證使用狀況盤點
  - 現行憑證數量、站台數量、應用數量盤點
  - 現行憑證申請及安裝流程盤點
  - 憑證安裝的主機及設備類型盤點
- 制度的盤點
  - 內部行政程序盤點
  - 資安政策、法規要求盤點
- 對於 ACME 自動化方案有深入了解
  - 研究並了解其原理架構
  - 組成專門的跨部門小組，而非單一部門負責
- 自動化方案評估
  - Agent、CLM 或是自行開發

以國內現況，我們評估
未來 1 年是評估及導入關鍵期
2027/3/15 憑證效期縮短為 100 天
屆時若是人工作業已達到 四倍 工作量

TWCA 臺灣網路認證

TWID 身分識別中心

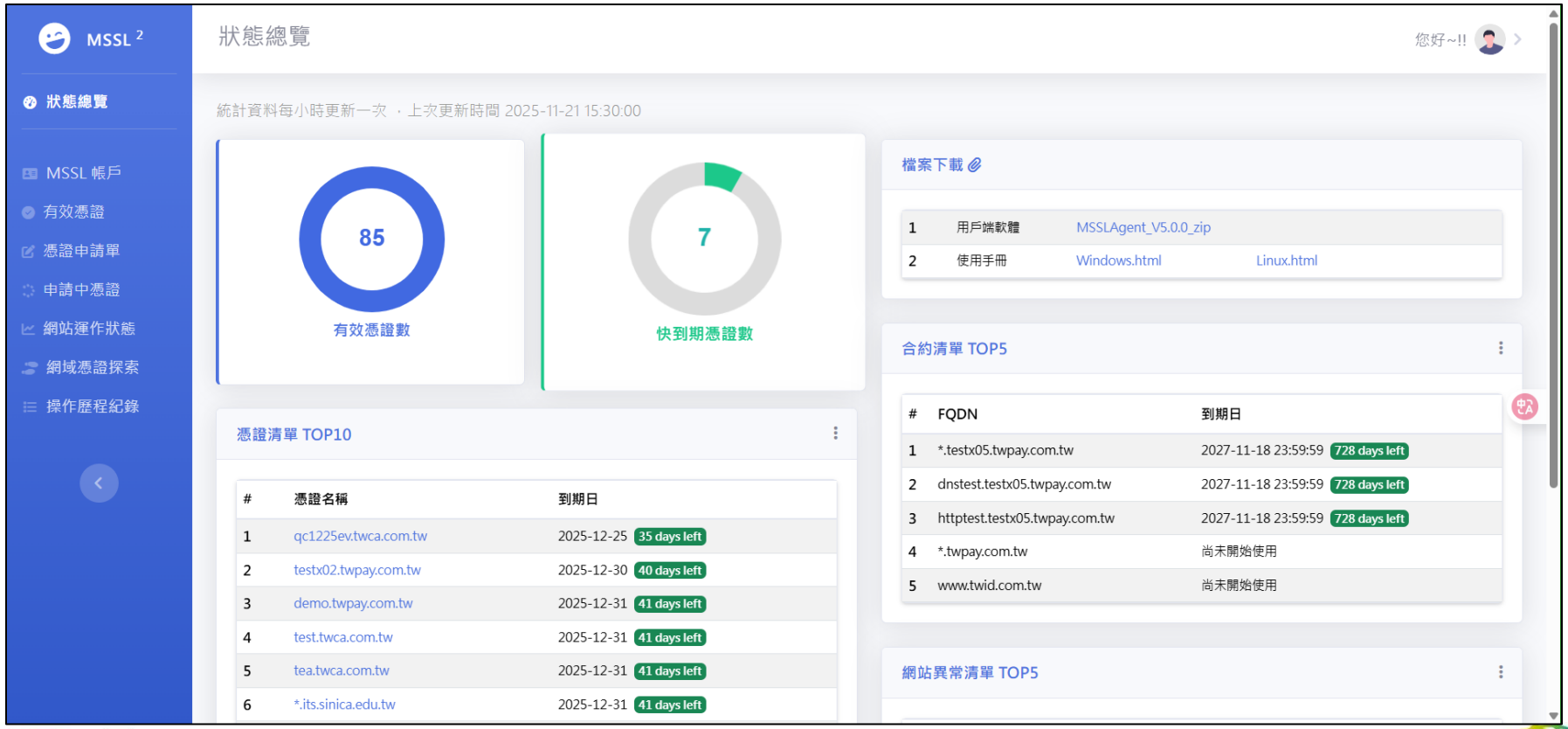
TWCA 的解決方案

- TWCA 已經支援 ACME 協定
  - 滿足國際標準
  - 持續與 CLM 大廠介接

- 可透過 MSSLAgent 與 TWCA 進行憑證申請 + 佈署
  - MSSLAgent 底層使用知名主流之 Certbot 工具，完全相容 ACME 協定
  - 可以完成基本憑證佈署
    - IIS、Nginx、Apache
  - 可自行撰寫佈署腳本
    - 使用 deploy hook 機制
    - 自主彈性高
  - 說明
    - https://twiddemo.twca.com.tw/acme/msslagent.html

TWCA 的解決方案

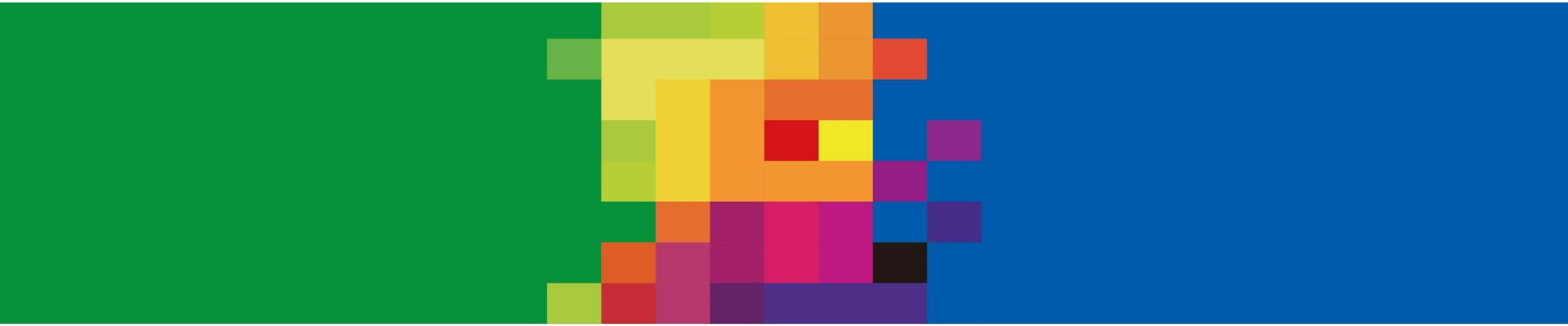
- MSSL 2.0 憑證管理服務
  - 可視化的 UI 介面協助用戶管理憑證
  - 預計 2026 Q1 推出



總結

- 憑證效期縮短已成定局，券商內部導入憑證自動化流程刻不容緩。
- 過去 TWCA 專注於憑證簽發，憑證佈署由用戶自行完成，為了達成完整憑證自動化作業流程，憑證佈署將成為關鍵。
- 建議即刻起立刻進行盤點，並且評估最佳的憑證自動化解決方案。
- TWCA 已經支援 ACME 協定，並且透過 MSSLAgent 可以更進一步幫助客戶進行基本的自動化導入，同時我們也即將推出 MSSL 2.0，強化憑證管理服務。

感謝聆聽



TWCA 臺灣網路認證

TWID 身分識別中心